# Cisco Çözümlerini Uygulama ve Yönetme (CCNA 200-301) Sınavına Hazırlık Rehberi

Cemal Taner

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Cisco Çözümlerini Uygulama ve Yönetme (CCNA 200-301) Sınavına Hazırlık Rehberi
Cemal Taner
30 Ağustos 2020
ISBN: 1230004089636

**Bu e-kitap Cemal Taner tarafından hazırlanmıştır. İzin alınmaksızın kısmen veya tamamen alıntı yapılamaz, kopyalanamaz, çoğaltılamaz ve yayınlanamaz.**

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# İÇİNDEKİLER

1. Bölüm: Network'e Giriş

2.Bölüm: Temel Switch-Anahtar ve End Device-Uç Cihaz Yapılandırması

3.Bölüm: Ağ Protokolleri ve Modelleri

4.Bölüm: Fiziksel Katman

5.Bölüm: Sayı Sistemleri

6.Bölüm: Veri Bağlantısı Katmanı

7.Bölüm: Ethernet Anahtarlama

8.Bölüm: Ağ Katmanı

9. Bölüm: Adres Çözümleme

10.Bölüm: Temel Router-Yönlendirici Yapılandırması

11.Bölüm: IPv4 ve IPv6 Adresleme

12.Bölüm:ICMP

13.Bölüm: Taşıma Katmanı

14. Bölüm: Uygulama Katmanı

15. Bölüm: Ağ Güvenliği Temelleri

16. Bölüm: Küçük Bir Ağ Oluşturma

17.Bölüm: Gelişmiş Cihaz Yapılandırmaları

18.Bölüm: Anahtarların Çalışma Prensipleri

19.Bölüm: VLAN'lar

20.Bölüm: İnter VLAN Routing

21.Bölüm: STP

22.Bölüm: Etherchannel

23. Bölüm: DHCP

24.Bölüm: SLAAC ve DHCPv6

25.Bölüm: Varsayılan Ağ Geçidi Yedekliliği (FHRP)

26.Bölüm: LAN Güvenliği

27. Bölüm: Güvenli Anahtar Yapılandırması

28. Bölüm: Kablosuz Ağ Teknolojileri

29.Bölüm: Kablosuz Ağ Yapılandırmaları

30.Bölüm: Yönlendirme Prensipleri

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

31.Bölüm: Statik Yönlendirme

32.Bölüm:OSPFv2 ve Yapılandırması

33.Bölüm: Ağ Güvenliği

34.Bölüm: ACL

35.Bölüm: NAT

36.Bölüm:WAN Teknolojileri

37.Bölüm: VPN ve IPsec

38.Bölüm: QoS

39.Bölüm: Ağ Yönetimi

40.Bölüm: Network Tasarımı

41.Bölüm: Ağ Sorunlarını Giderme

42.Bölüm: Ağ Sanallaştırma

43.Bölüm: Ağ Otomasyonu

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 1. Bölüm: Network'e Giriş

## 1.1.Network Components- Ağ Bileşenleri

### 1.1.1. Ağda Bilgisayar Rolleri

Ağdaki her bilgisayara ana bilgisayar (host) veya uç cihaz (end devices) denir.

Sunucular, uç cihazlara bilgi sağlayan bilgisayarlardır:

- email servers-eposta sunucu
- web servers-web sunucu
- file server-dosya sunucu

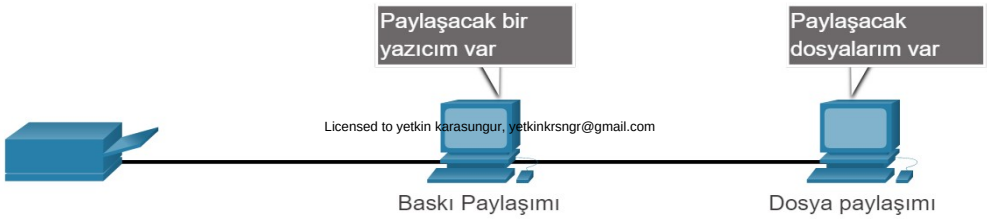
İstemciler, bilgi almak için sunuculara istek gönderen bilgisayarlardır:

- web sunucusundan web sayfası
- bir e-posta sunucusundan e-posta talep ederler.

| Sunucu Tipi | Açıklama |
|---|---|
| Email | E-posta sunucusu, e-posta sunucusu yazılımını çalıştırır. İstemciler, sunucudaki e-postalara erişmek için Microsoft Outlook gibi posta istemci yazılımlarını kullanır. |
| Web | Web sunucusu web sunucusu yazılımını çalıştırır. İstemciler, sunucudaki web sayfalarına erişmek için Windows Internet Explorer gibi tarayıcı yazılımlarını kullanır. |
| File | Dosya sunucusu şirket ve kullanıcı dosyalarını merkezi bir konumda saklar. İstemci aygıtları bu dosyalara Windows Dosya Gezgini gibi istemci yazılımlarıyla erişir. |

### 1.1.2 Peer-to-Peer-Eşler Arası Ağlar

Eşler Arası Ağda bir aygıtın istemci ve sunucu olması mümkündür. Bu tür ağ tasarımı yalnızca çok küçük ağlar için önerilir.

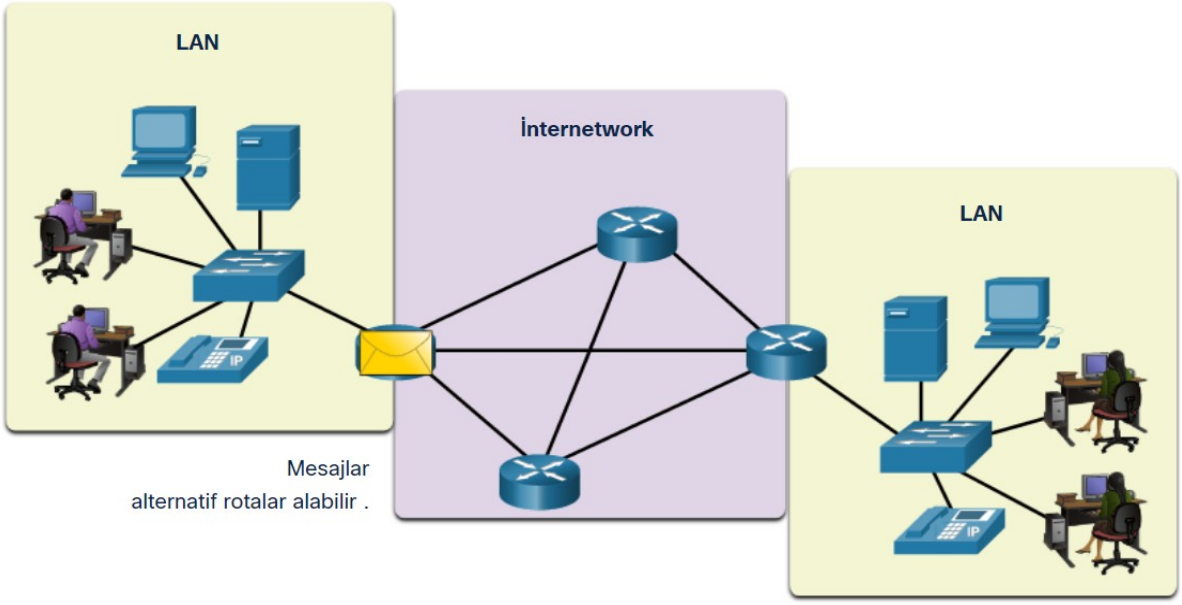



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Avantajları | Dezavantajları |
|---|---|
| Kurulumu kolay | Merkezi yönetim yok |
| Daha az karmaşık | Güvenli değil |
| Daha az maliyet | Ölçeklenebilir değil |
| Basit görevler için kullanılır: dosya aktarma ve yazıcıları paylaşma | Daha yavaş performans |

### 1.1.3.End Devices-Uç Cihazlar

Bir uç cihaz, mesajın nereden geldiğini veya nereden alındığını gösterir. Veriler bir uç cihazdan çıkar, ağ üzerinden akar ve başka bir uç cihaza gelir.

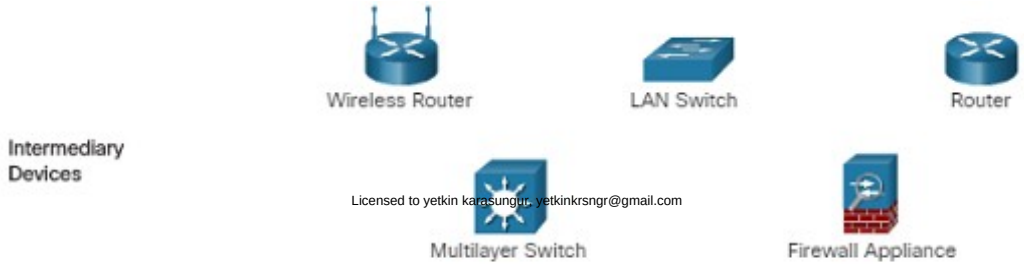



### 1.1.4.Intermediary Network Devices-Aracı Ağ Cihazları

Bir aracı ağ cihazı, uç cihazları birbirine bağlar. Örnek olarak anahtarlar(switch), kablosuz erişim noktaları (wireless access point)), yönlendiriciler(router) ve güvenlik duvarları (firewall) gösterilebilir.

Bir ağdan veriler akarken  bir aracı ağ cihaiz verilerin yönetimi de dahil olmak üzere aşağıdakileri görevleri yerine getirir:

- Veri sinyallerini yeniden oluşturma ve yeniden iletme.
- Ağda hangi yolların var olduğu hakkında bilgi bulundurma.
- Diğer aygıtları hatalar ve iletişim hataları konusunda bilgilendirme.

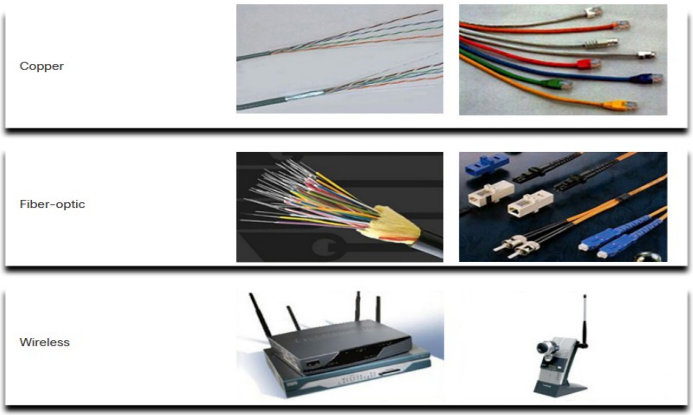



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 1.1.5.Network Media-Ağ Medyası

Bir ağdaki iletişim, bir mesajın kaynaktan hedefe gitmesini sağlayan bir ortam aracılığıyla gerçekleştirilir.

| Media Tipleri | Açıklama |
|---|---|
| Copper-Bakır Kablo | Elektriksel darbeleri kullanır |
| Fiber Optic | Işık darbelerini kullanır. |
| Kablosuz iletim (Wireless) | Elektromanyetik dalgaların belirli frekanslarının modülasyonunu kullanır. |



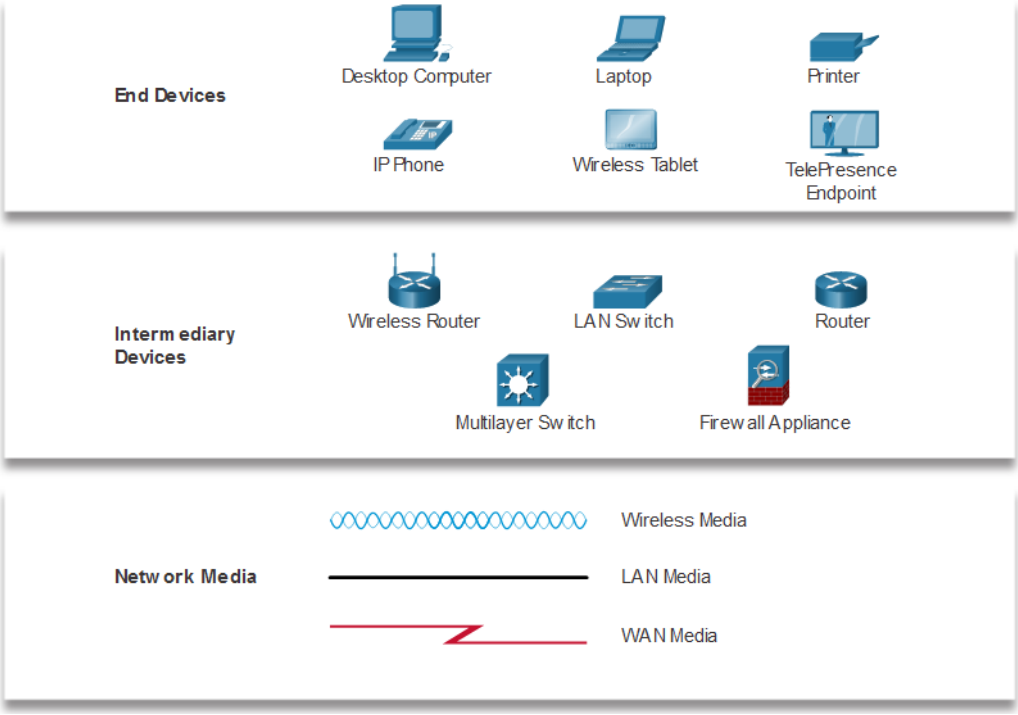

## 1.1.6.Network Representations-Ağ Gösterimleri

Genellikle topoloji diyagramları olarak adlandırılan ağ diyagramları, ağ içindeki aygıtları temsil etmek için sembolleri kullanır.

Bilmeniz gereken önemli terimler şunları içerir:

- Ağ arayüz kartı-Network Interface Card (NIC)
- Fiziksel Port-Physical Port
- Arayüz,arabirim-Interface

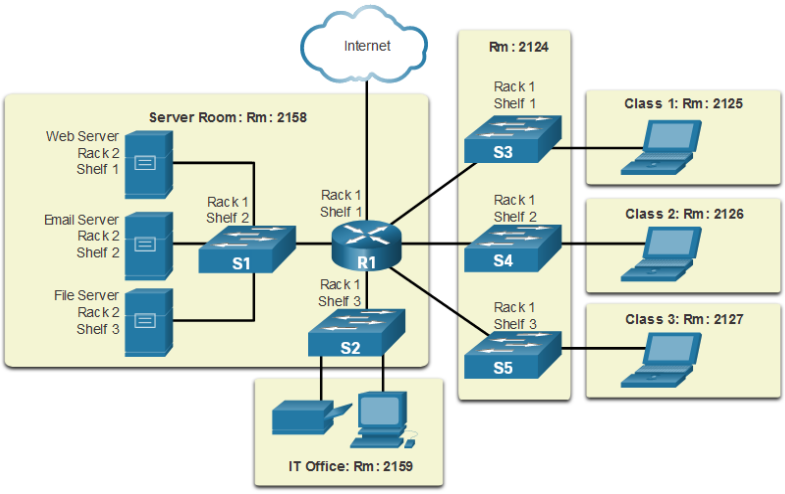
Not: Genellikle, bağlantı noktası (port) ve arabirim (interface) terimleri birbirinin yerine kullanılır



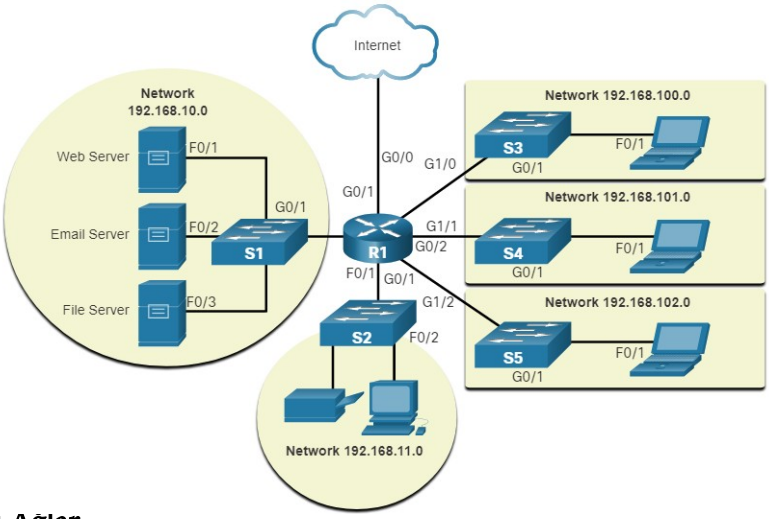

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 1.1.7.Topology Diagrams-Topoloji Diyagramları

Fiziksel topoloji diyagramları, ara cihazların fiziksel konumunu ve kablo kurulumunu gösterir.




Mantıksal (Logical) topoloji diyagramları aygıtları, bağlantı noktalarını ve ağın adresleme şemasını gösterir.




## 1.2. Ağ Türleri

### 1.2.1.Çok Boyutlu Ağlar

Small Home Networks –birkaç bilgisayarı birbirine ve İnternete bağlar.

Small Office/Home Office – bir ev veya uzak ofis içindeki bilgisayarın şirket ağına bağlanmasını sağlar

Medium to Large Networks – birçok konumda yüzlerce veya binlerce birbirine bağlı bilgisayar bulunur

World Wide Networks – İnternet gibi yüz milyonlarca bilgisayarı birbirine bağlar

Small Home

SOHO

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Medium/Large

World Wide

### 1.2.2. LAN ve WAN

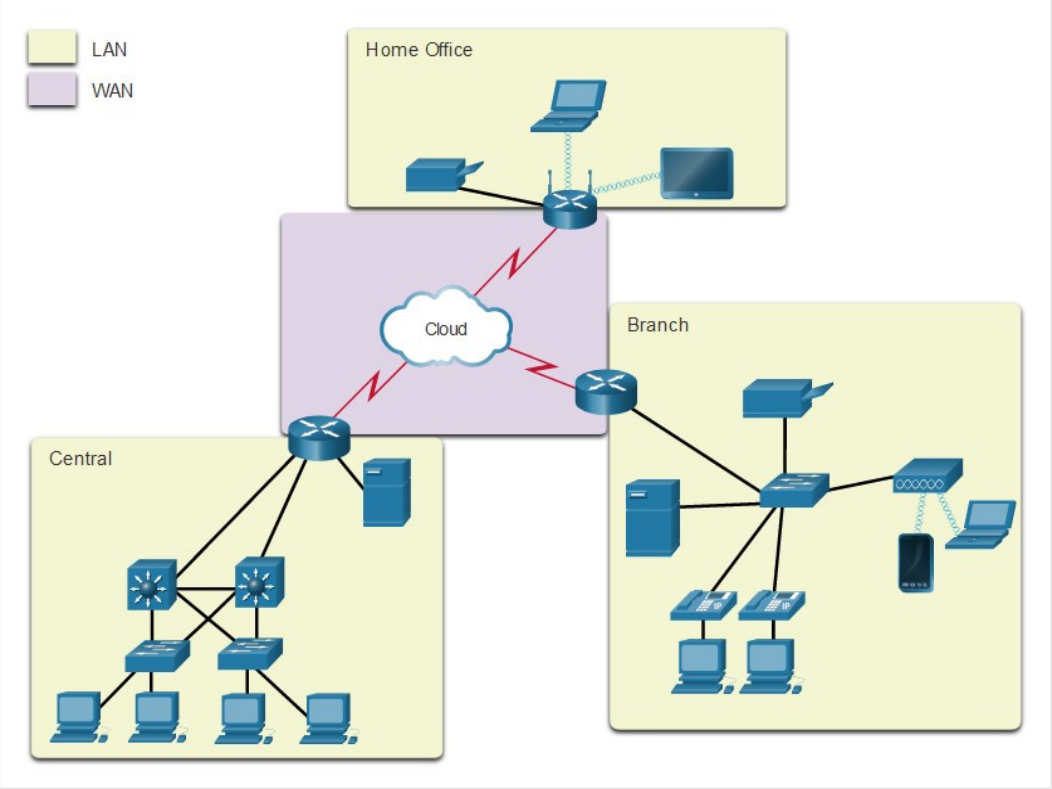
Ağ altyapıları, aşağıdakiler bakımından büyük farklılıklar gösterir:

- Kapsanan alanın büyüklüğü
- Bağlı kullanıcı sayısı
- Mevcut hizmetlerin sayısı ve türleri
- Sorumluluk alanı

En yaygın iki ağ türü:

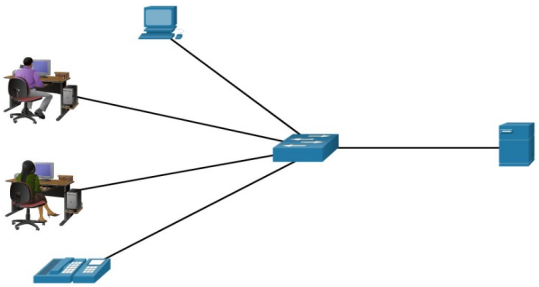
Local Area Network (LAN)

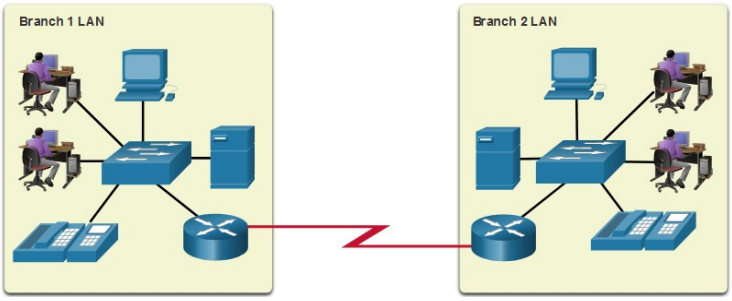
Wide Area Network (WAN).




LAN, küçük bir coğrafi alana yayılan bir ağ altyapısıdır.

WAN, geniş bir coğrafi alana yayılan bir ağ altyapısıdır.






| LAN | WAN |
|---|---|
| Sınırlı bir alanda uç cihazları birbirine bağlar. | Geniş coğrafi bölgelerde LAN'ları birbirine bağlar. |
| Tek bir kuruluş veya kişi tarafından yönetilir. | Genellikle bir veya daha fazla servis sağlayıcı tarafından yönetilir. |
| Dahili cihazlara yüksek hızlı bant genişliği sağlar. | Genellikle LAN'lar arasında daha düşük hız bağlantıları sağlar. |

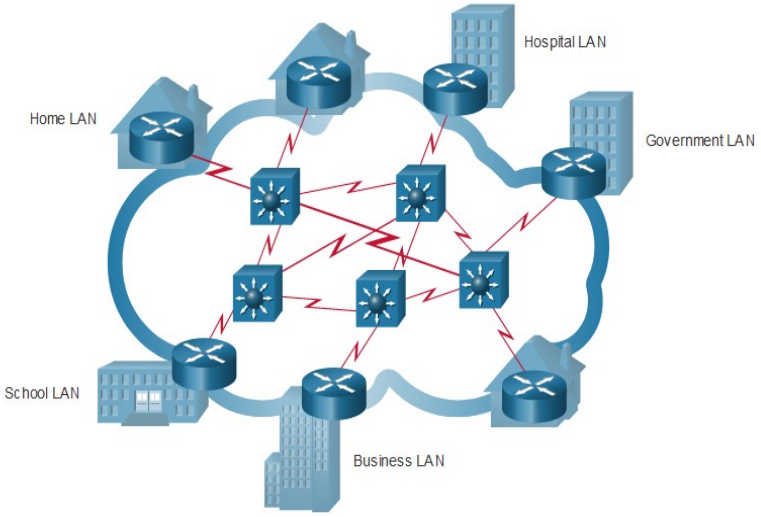
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 1.2.3.İnternet

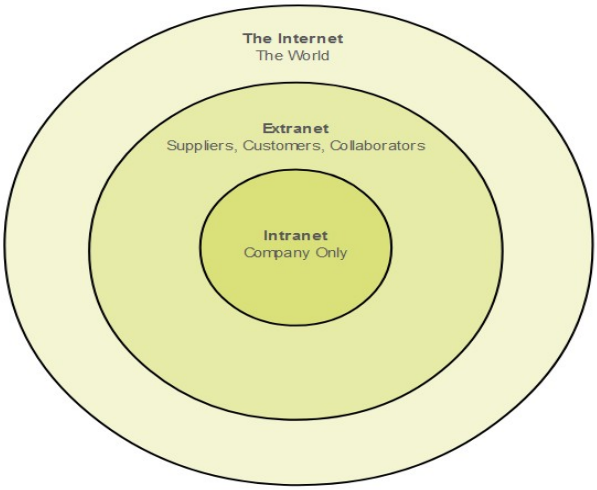
İnternet, dünya çapında birbirine bağlı LAN ve WAN toplamıdır. LAN'lar WAN'lar kullanılarak birbirine bağlanır. WAN'lar oluşturulurken bakır teller, fiber optik kablolar ve kablosuz iletim kullanabilir.

İnternet herhangi bir kişiye veya gruba ait değildir. İnternet üzerindeki yapının korunmasına yardımcı olmak için aşağıdaki gruplar geliştirilmiştir:

- IETF
- ICANN
- IAB




### 1.2.4.Intranets ve Extranets




Bir intranet, yalnızca kuruluş üyeleri veya yetkilendirilmiş diğer kişiler tarafından erişilebilir olması amaçlanan bir kuruluşun içindeki özel LAN ve WAN toplamıdır.

Bir kuruluş, ağlarındaki verilerine erişmesi gereken farklı bir kuruluşta çalışan kişiler için ağlarına güvenli erişim sağlamak amacıyla bir extranet kullanabilir.

## 1.3.İnternet Bağlantıları

### 1.3.1.İnternet Erişim Teknolojileri

Kullanıcıları ve kuruluşları internete bağlamanın birçok yolu vardır:

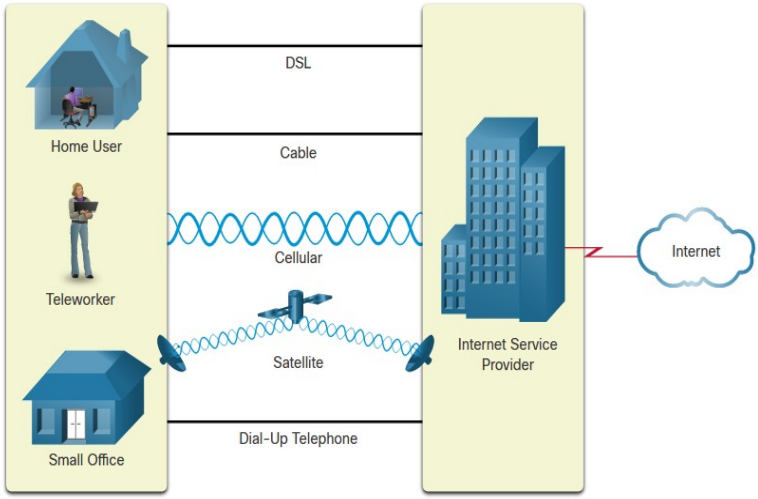
Ev kullanıcıları ve küçük ofisler için popüler hizmetler arasında geniş bant kablo, geniş bant dijital abone hattı (DSL), kablosuz WAN'lar ve mobil hizmetler bulunur.

Kuruluşların IP telefonları, video konferansı ve veri merkezi depolamasını desteklemek için daha hızlı bağlantılara ihtiyaçları vardır.

Business-class ara bağlantıları genellikle servis sağlayıcılar (SP) tarafından sağlanır ve şunları içerebilir: business DSL, kiralık hatlar ve Metro Ethernet.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 1.3.2.Ev ve Küçük Ofis İnternet Bağlantıları

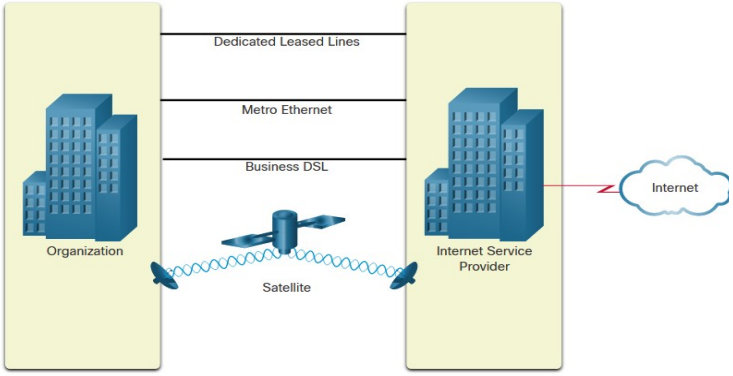



| Bağlantı | Açıklama |
|---|---|
| Cable-Kablo | yüksek bant genişliği, her zaman açık, kablolu televizyon servis sağlayıcıları tarafından sunulan internet. |
| DSL | yüksek bant genişliği, her zaman açık, bir telefon hattı üzerinden çalışan internet bağlantısı. |
| Cellular-Hücresel | internete bağlanmak için bir cep telefonu şebekesi kullanır. |
| Satellite-Uydu | İnternet Servis Sağlayıcıları olmayan kırsal alanlara büyük fayda sağlar. |
| Dial-up telephone - Çevirmeli bağlantı | modem kullanan ucuz, düşük bant genişliği seçeneği, her zaman açık değil. |

### 1.3.3.İşletmeler İçin İnternet Bağlantıları

Kurumsal iş bağlantıları şunları gerektirebilir:

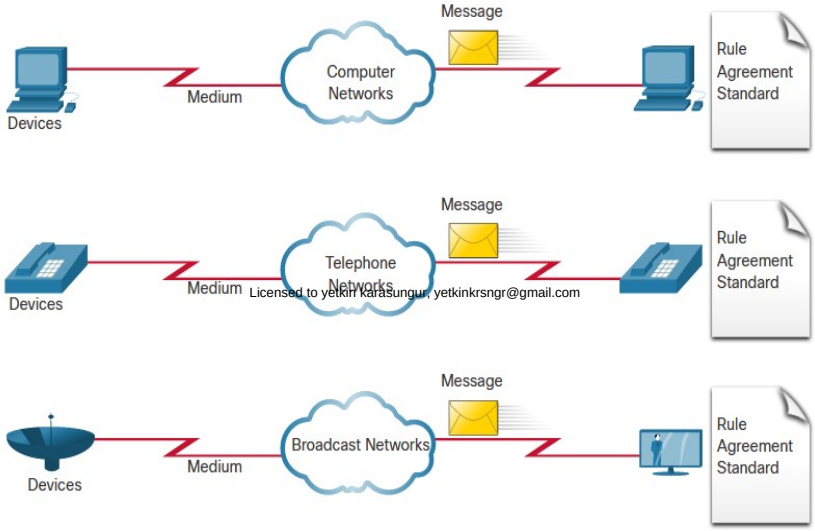
- daha yüksek bant genişliği
- özel bağlantılar
- yönetilen hizmetler




| Bağlantı Türü | Açıklama |
|---|---|
| Dedicated Leased Line | Bunlar, uzak ofisleri özel ses ve / veya veri ağına bağlayan servis sağlayıcının ağı içinde ayrılmış devrelerdir. |
| Ethernet WAN | Bu, LAN erişim teknolojisini WAN'a genişletir. |
| DSL | Business DSL, Simetrik Dijital Abone Hatları (SDSL) dahil olmak üzere çeşitli formatlarda mevcuttur. |
| Satellite | Bu, kablolu bir çözüm olmadığında bağlantı sağlayabilir. |

### 1.3.4. Birleşik Ağlar

Birleştirilmiş ağlardan önce bir kuruluş, telefon, video ve veri için ayrı ayrı kablolardan oluşan hizmetler kullanıyordu. Bu ağların her biri sinyali taşımak için farklı teknolojiler kullanırdı ve bu teknolojilerin her biri farklı kurallar ve standartlar kullanırdı.

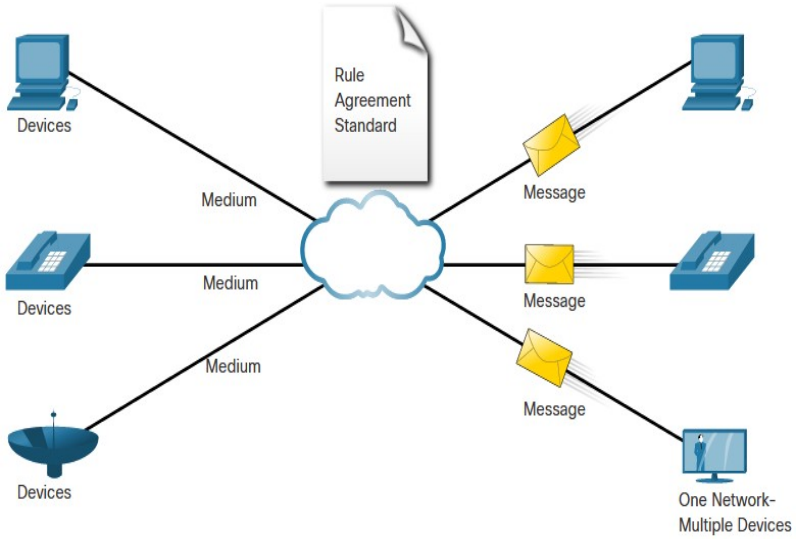



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Birleşik veri ağları, aşağıdakiler dahil olmak üzere bir bağlantıda birden çok hizmet taşır:

- data
- voice
- video

Birleşik ağlar, aynı ağ altyapısı üzerinden veri, ses ve video sağlayabilir. Ağ altyapısı aynı kurallar ve standartları kullanır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 2.Bölüm: Temel Switch( Anahtar) ve End Device( Uç Cihaz) Yapılandırması

**Bu bölümde anlatılanları uygulamak için Cisco Packet Tracer Programını İndirmelisiniz.**

Ücretsiz Packet Tracer 101 Eğitimi için Youtube kanalımı ziyaret edebilirsiniz.

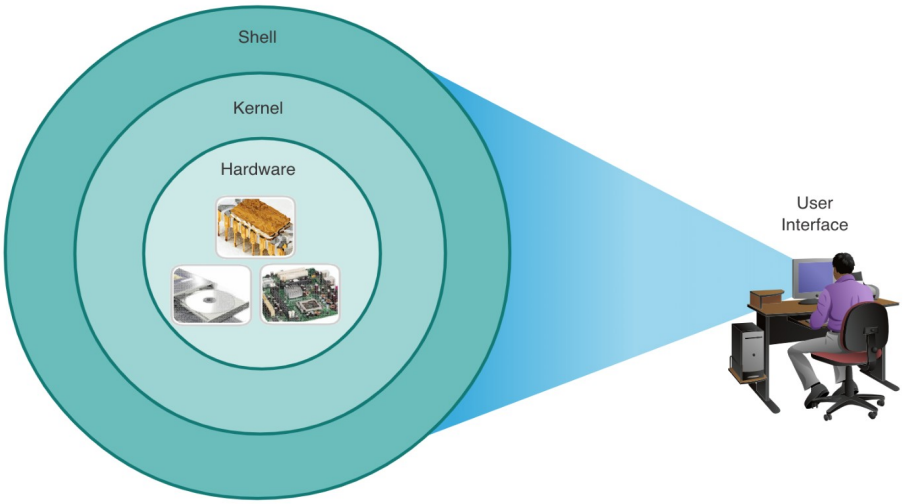
## 2.1.Cisco IOS ( Internetwork Operating System)Access-Cisco IOS Erişimi

### 2.1.1.Operating Systems-İşletim Sistemleri

Shell-Kullanıcıların bilgisayardan belirli görevler istemesine izin veren kullanıcı arabirimi. Bu istekler CLI veya GUI arabirimleri aracılığıyla yapılabilir.

Kernel- Bir bilgisayarın donanımı ve yazılımı arasında iletişim kurar ve donanım kaynaklarının yazılım gereksinimlerini karşılamak için nasıl kullanıldığını yönetir.

Hardware- Temel elektronik dahil bir bilgisayarın fiziksel bölümü.




### 2.1.2.GUI

GUI(Grafic User Interface), kullanıcının grafik simgeler, menüler ve pencereler içeren bir ortam kullanarak sistemle etkileşime girmesini sağlar. Bir GUI daha kullanıcı dostudur ve sistemi kontrol eden temel komut yapısı hakkında daha az bilgi gerektirir.

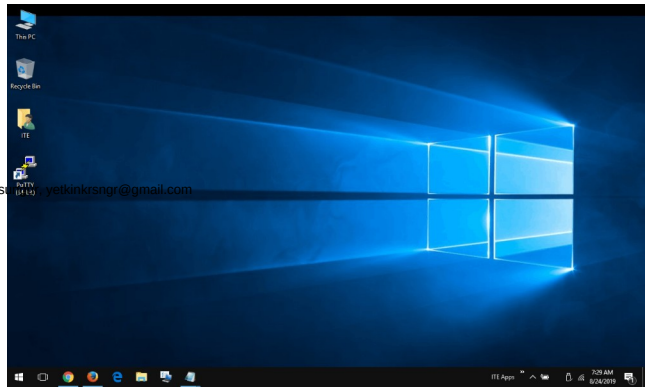
GUI örnekleri: Windows, macOS, Linux KDE, Apple iOS ve Android.

GUI'ler hata verebilir, çökebilir veya belirtildiği gibi çalışmayabilir. Bu nedenlerle, ağ cihazlarına tipik olarak bir CLI üzerinden erişilir.

### 2.1.3.İşletim Sisteminin Amacı

PC işletim sistemi kullanıcının aşağıdakileri yapmasını sağlar:

- Seçimler yapmak ve programları çalıştırmak için fare kullanma
- Metin ve metin tabanlı komutları girme
- Çıkışı bir monitörde görüntüleme



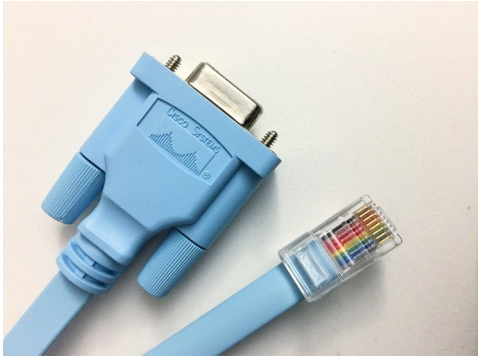
Licensed to yetkin karasu yetkinkrsngr@gmail.com

- CLI (Command Line Interface) tabanlı ağ işletim sistemi, bir ağ teknisyeninin aşağıdakileri yapmasını sağlar:
- CLI tabanlı ağ programlarını çalıştırmak için bir klavye kullanma
- Metin ve metin tabanlı komutlar girmek için klavye kullanma
- Çıkışı bir monitörde görüntüleme

```
analyst@secOps ~]$ ls
Desktop  Downloads  lab.support.files  second_drive
[analyst@secOps ~]$
```

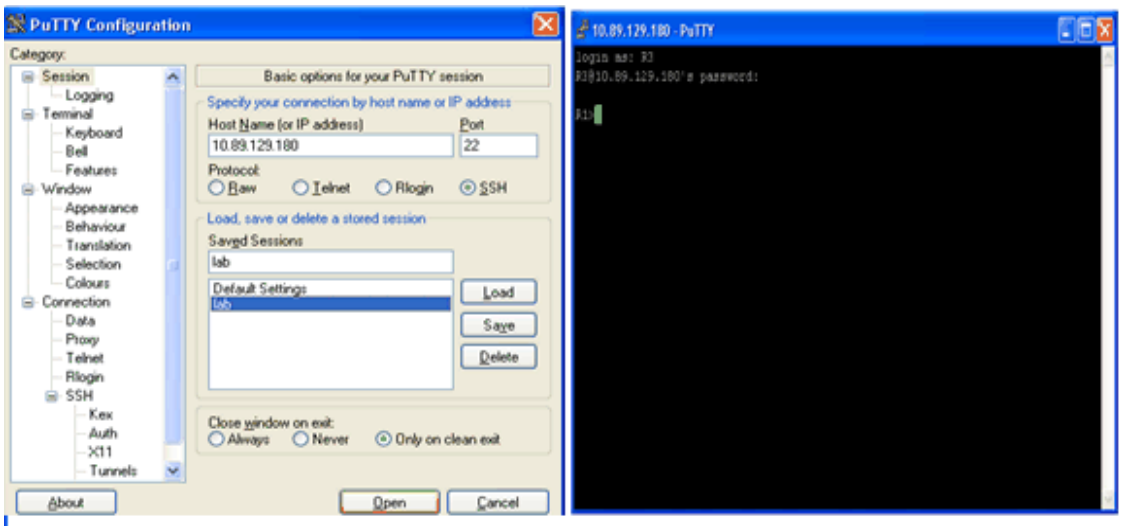
## 2.1.4.Erişim Yöntemleri

Console – İlk yapılandırmaları gerçekleştirmek veya  bakım yapmak amacıyla bir aygıta erişmek için kullanılan bir fiziksel yönetim bağlantı noktası.



Secure Shell (SSH) –Ağ üzerinden sanal arabirim aracılığıyla bir aygıta güvenli bir uzaktan CLI bağlantısı kurar. (Not: Bu, bir cihaza uzaktan bağlanmak için önerilen yöntemdir.

Telnet –Ağ üzerinden bir aygıta güvenli olmayan bir uzak CLI bağlantısı kurar. (Not: Kullanıcı kimlik doğrulaması, şifreler ve komutlar ağ üzerinden düz metin olarak gönderilir.)

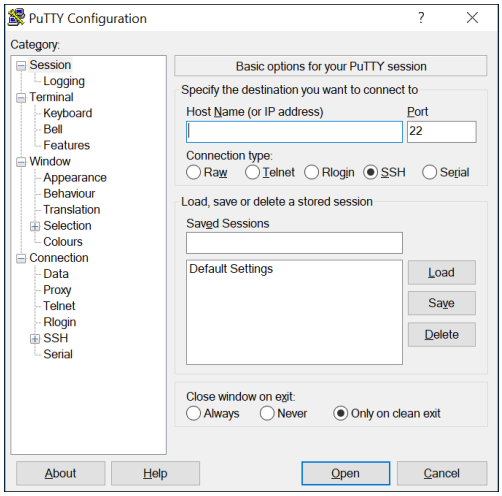


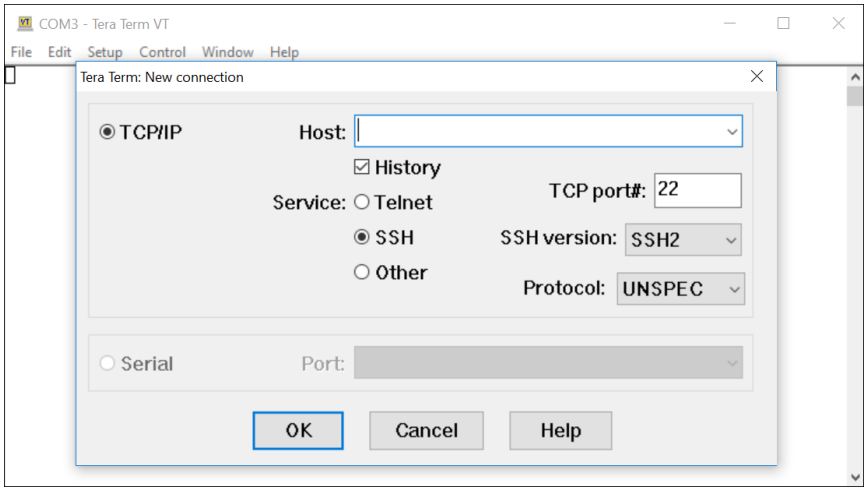

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 2.1.5.Terminal Emülasyon Programları

Terminal emülasyon programları, bir ağ aygıtına bir konsol bağlantı noktası veya SSH / Telnet bağlantısıyla bağlanmak için kullanılır.

PuTTY, Tera Term ve SecureCRT gibi seçebileceğiniz birçok terminal emülasyon programı vardır.




## 2.2.Cisco IOS'da Gezinme

### 2.2.1.Birincil Komut Modları

User EXEC Mode:

Yalnızca sınırlı sayıda temel izleme (show) komutuna erişime izin verir

> Sembolü ile biten CLI istemi ile tanımlanır

```
Router>
```

Privileged EXEC Mode:
Tüm komutlara ve özelliklere erişim sağlar
# Sembolü ile biten CLI istemi ile tanımlanır

```
Router#
```

### 2.2.2.Configuration Mode and Subconfiguration Modes-Yapılandırma Modu ve Alt Yapılandırma Modları

**Global Configuration Mode:**

Cihazdaki yapılandırma seçeneklerine erişmek için kullanılır

```
Switch(config)#
```

**Line Configuration Mode:**

Konsol, SSH, Telnet veya AUX erişimini yapılandırmak için kullanılır

```
Switch(config-line)#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Interface Configuration Mode:**

Switch bağlantı noktasını veya yönlendirici arabirimini yapılandırmak için kullanılır

```
Switch(config-if)#
```

## 2.2.3.IOS Modları Arasında Gezinme

**Privileged EXEC Mode:**

Kullanıcı EXEC modundan ayrıcalıklı EXEC moduna geçmek için enable komutunu kullanın.

```
Switch> enable
Switch#
```

**Global Configuration Mode:**

Genel yapılandırma moduna girmek için configure terminal komutunu kullanın. Ayrıcalıklı EXEC moduna geri dönmek için exit komutunu kullanın.

```
Switch(config)#
Switch(config)#exit
Switch#
```

**Line Configuration Mode:**

Hat yapılandırma moduna girmek için line komutunu ve ardından yönetim satırı türünü kullanın. Genel yapılandırma moduna geri dönmek için exit komutunu kullanın.

```
Switch(config)#line console 0
Switch(config-line)#exit
Switch(config)#
```

**Subconfiguration Modes:**

Genel yapılandırma moduna geri dönmek üzere herhangi bir alt yapılandırma modundan çıkmak için exit komutunu kullanın. Ayrıcalıklı EXEC moduna geri dönmek için end komutunu veya Ctrl + Z tuş bileşimini kullanın.

```
Switch(config)#line console 0
Switch(config-line)#end
Switch#
```

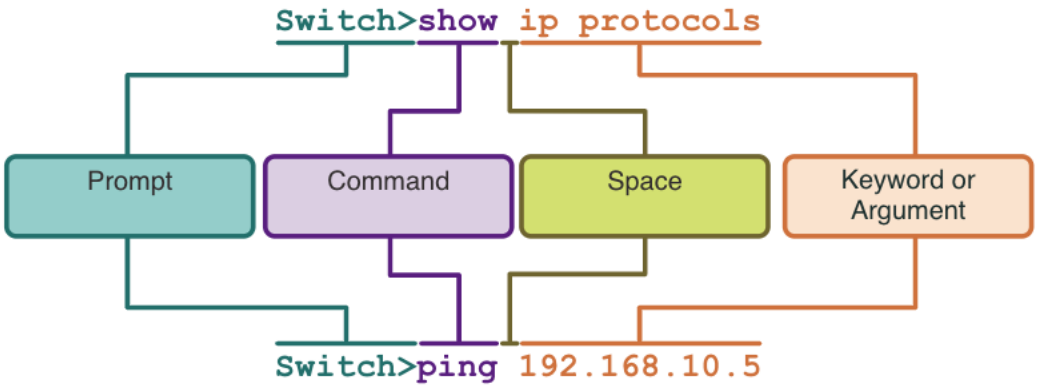
Doğrudan bir alt yapılandırma modundan diğerine geçmek için, istediğiniz alt yapılandırma modu komutunu yazın. Örnekte, komut istemi (config-line) # yerine (config-if) # olarak değişir.

```
Switch(config-line)#interface FastEthernet 0/1
Switch(config-if)#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 2.3.Komut Yapısı

### 2.3.1.Temel IOS Komut Yapısı




Keyword – Bu, işletim sisteminde tanımlanan belirli bir parametredir (şekilde, ip protocols).

Argument-Bu önceden tanımlanmamıştır; kullanıcı tarafından tanımlanan bir değer veya değişkendir (şekilde,192.168.10.5).

### 2.3.2.IOS Komut Sözdizimi Kontrolü

Bir komut bir veya daha fazla bağımsız değişken gerektirebilir. Bir komut için gereken anahtar sözcükleri ve bağımsız değişkenleri belirlemek için komut sözdizimine bakın.

Kalın yazılmış metin, gösterildiği gibi girilen komutları ve anahtar kelimeleri gösterir.

İtalik metin, kullanıcının değeri sağladığı bir bağımsız değişkeni belirtir.

| Kural | Açıklama |
|---|---|
| **boldface** | Kalın yazı metni, gösterildiği gibi tam olarak girdiğiniz komutları ve anahtar kelimeleri gösterir. |
| *italics* | İtalik metin, değer verdiğiniz bağımsız değişkenleri belirtir. |
| [x] | Köşeli ayraçlar isteğe bağlı bir öğeyi (anahtar sözcük veya bağımsız değişken) gösterir. |
| {x} | Parantezler gerekli bir öğeyi (anahtar kelime-keyword veya bağımsız değişken-argument) gösterir. |
| [x {y \| z }] | Köşeli parantez içindeki köşeli ayraçlar ve dikey çizgiler, isteğe bağlı bir öğe içinde gerekli bir seçeneği belirtir. Boşluklar, komutun bölümlerini açıkça tanımlamak için kullanılır. |

Komut sözdizimi, bir komut girilirken kullanılması gereken biçimi sağlar.

Komut ping ve kullanıcı tanımlı argüman hedef cihazın ip adresidir.

Örneğin, ping 10.10.10.5

```
ping ip-address
```

Komut traceroute ve kullanıcı tanımlı argüman hedef cihazın ip adresidir.
Örneğin, traceroute 192.168.254.254

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
traceroute ip-address
```

Bir komut birden çok bağımsız değişkenle kullanılıyorsa, bu komutun şu şekilde temsil edildiğini görebilirsiniz:

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

## 2.3.3.Cisco IOS Yardım Özellikleri

IOS'ta iki tür yardım bulunur: bağlama duyarlı yardım(context-sensitive) ve komut sözdizimi denetimi (command syntax check.).

Bağlama duyarlı yardım, şu soruların yanıtlarını hızlı bir şekilde bulmanızı sağlar:

Her komut modunda hangi komutlar kullanılabilir?

Hangi komutlar belirli karakterlerle veya karakter grubuyla başlar?

Belirli komutlar için hangi bağımsız değişkenler ve anahtar kelimeler kullanılabilir?

```
Router#ping ?
  WORD  Ping destination address or hostname
  ip    IP echo
  ipv6  IPv6 echo
```

Komut sözdizimi denetimi, kullanıcı tarafından geçerli bir komutun girildiğini doğrular.

Yorumlayıcı girilen komutu anlayamazsa, komutta neyin yanlış olduğunu açıklayan geri bildirim sağlar.

```
Switch#interface fastEthernet 0/1
                 ^
% Invalid input detected at '^' marker.
```

## 2.3.4.Kısayol Tuşları ve Komutların Kısa Yazımı

IOS CLI, yapılandırmayı, izlemeyi ve sorun gidermeyi kolaylaştıran kısayol tuşları ve kısayollar sağlar.

Komutlar ve anahtar kelimeler, benzersiz bir seçimi tanımlayan minimum karakter sayısına kadar kısaltılabilir. Örneğin, **configure** komutu **conf** ile başlayan tek komut olduğu için **configure** komutu **conf** olarak kısaltılabilir.

```
Router#con
% Ambiguous command: "con"
Router#con?
configure  connect
```

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Aşağıdaki tablo, komut satırı düzenlemesini geliştirmek için tuş vuruşlarının kısa bir listesidir.

| Keystroke-Tuş Vuruşu | Description-Açıklama |
|---|---|
| **Tab** | Kısmi komut adı girişini tamamlar. |
| **Backspace** | İmlecin solundaki karakteri siler. |
| **Left Arrow** or **Ctrl+B** | İmleci bir karakter sola taşır. |
| **Right Arrow** or **Ctrl+F** | İmleci bir karakter sağa taşır. |
| **Up Arrow** or **Ctrl+P** | En son komutlardan başlayarak arabellekteki geçmiş komutları çağırır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bir komut çıkışı terminal penceresinde görüntülenenden daha fazla metin ürettiğinde, IOS bir "--More--" istemi görüntüler. Aşağıdaki tabloda, bu istem görüntülendiğinde kullanılabilecek tuş vuruşları açıklanmaktadır.

Aşağıdaki tablo, bir işlemden çıkmak için kullanılabilecek komutları listelemektedir.

| Keystroke | Description |
|---|---|
| **Enter** Key | Sonraki satırı görüntüler. |
| **Space** Bar | Bir sonraki ekranı görüntüler. |
| Any other key | Ayrıcalıklı EXEC moduna geri dönerek görüntüleme dizesini sonlandırır. |

| Keystroke | Description |
|---|---|
| **Ctrl-C** | Herhangi bir yapılandırma modundayken, yapılandırma modunu bitirir ve ayrıcalıklı EXEC moduna geri döner. |
| **Ctrl-Z** | Herhangi bir yapılandırma modundayken, yapılandırma modunu bitirir ve ayrıcalıklı EXEC moduna geri döner. |
| **Ctrl-Shift-6** | DNS aramalarını, traceroute izlemesini, ping'i vb. iptal etmek için kullanılan çok amaçlı kesme tuşları |

## 2.4. Temel Cihaz Yapılandırması

### 2.4.1.Cihaz İsimleri

Herhangi bir cihazdaki ilk yapılandırma komutu, ona benzersiz bir hostname vermek olmalıdır.

Varsayılan olarak, tüm cihazlara fabrika varsayılan adı atanır. Örneğin, bir Cisco IOS anahtarı "Switch" dir.

```
Switch# configure terminal
Switch(config)# hostname Sw-Floor-1
Sw-Floor-1(config)#
```

Cihazları Adlandırma Klavuzu:

- Bir harf veya rakamla başlar
- Boşluk içermez
- Bir harf veya rakamla biter
- Yalnızca harf, rakam ve tire kullanılır
- 64 karakterden kısa olmalıdır.

Not: Anahtarı varsayılan ayara döndürmek için, **no hostname** global config komutunu kullanın.

### 2.4.2.Parola Kuralları

Zayıf veya kolayca tahmin edilebilen şifrelerin (parola) kullanılması bir güvenlik sorunudur.

Tüm ağ aygıtları, ayrıcalıklı EXEC, kullanıcı EXEC ve parolalarla uzaktan Telnet erişimini güvenceye alarak yönetim erişimini sınırlamalıdır. Ayrıca, tüm parolalar şifrelenmeli ve yasal bildirimler (banner) sağlanmalıdır.

**Parola Kuralları:**

Sekiz karakterden daha uzun parolalar kullanın.

Büyük ve küçük harfler, sayılar, özel karakterler ve / veya sayısal dizilerin bir kombinasyonunu kullanın.

Tüm cihazlar için aynı parolayı kullanmaktan kaçının.

Sık kullanılan kelimeleri kullanmayın çünkü kolayca tahmin edilebilirler.

Not:Bu kitapta laboratuvarların çoğunda **cisco** veya **class** gibi basit parolalar kullanır. Bu parolalar zayıf ve kolayca tahmin edilebilir olarak kabul edilir ve gerçek dünya üretim ortamlarında kullanılmamalıdır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 2.4.3.Parolaları Yapılandırma

Kullanıcı EXEC modu erişimini koruma:

Önce global konfigürasyon modunda line consol 0 komutunu kullanarak hat konsolu yapılandırma moduna girin.

Ardından, **password** *parola* komutunu kullanarak kullanıcının EXEC modu şifresini belirtin.

Son olarak, login komutunu kullanarak EXEC kullanıcı erişimini etkinleştirin. Örnekta parola olarak "cisco" verilmiştir.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line console 0
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Ayrıcalıklı EXEC modu erişimini koruma:

Önce global yapılandırma moduna girin.

Ardından, **enable secret** *parola* komutunu kullanın. Örnekta parola olarak "class" verilmiştir.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# enable secret class
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

VTY hattı erişiminin güvenliğini sağlama:

İlk olarak global konfigürasyon modunda **line vty 0 15** komutunu kullanarak VTY konfigürasyon moduna girin.

Ardından, **password** *parola* komutunu kullanarak VTY parolasını belirtin.

Son olarak, login komutunu kullanarak VTY erişimini etkinleştirin.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# line vty 0 15
Sw-Floor-1(config-line)# password cisco
Sw-Floor-1(config-line)# login
Sw-Floor-1(config-line)# end
Sw-Floor-1#
```

Not: VTY hatları cihaza Telnet veya SSH kullanarak uzaktan erişim sağlar. Çoğu Cisco anahtarı, 0 ila 15 numaralı 16 VTY hattını destekler.

### 2.4.4.Parolaları Şifreleme

Startup-config ve running-config dosyaları parolaların çoğunu düz metin olarak görüntüler.

Tüm düz metin parolaları şifrelemek için, **service password-encryption** genel yapılandırma komutunu kullanın.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# service password-encryption
Sw-Floor-1(config)# exit
Sw-Floor-1#
```

Aygıttaki parolaların artık şifreli olduğunu doğrulamak için **show running-config** komutunu kullanın.

```
Sw-Floor-1# show running-config
!

!
line con 0
password 7 094F471A1A0A
login
!
Line vty 0 4
Password 7 03095A0F034F38435B49150A1819
Login
!
!
end
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 2.4.5.Banner Mesajları

Başlık mesajı, yetkisiz personelin cihaza erişmeye çalışmasını önlemek için önemlidir.

Bir ağ cihazında günün banner mesajını oluşturmak için **banner motd # the message of the day #** global config komutunu kullanın.

```
Sw-Floor-1# configure terminal
Sw-Floor-1(config)# banner motd #Authorized Access Only!#
```

Banner, cihaza erişim denemelerinde görüntülenecektir.

```
Press RETURN to get started.



Authorized Access Only!

User Access Verification

Password:
```

Not: Komut sözdizimindeki "#" sınırlayıcı karakter olarak adlandırılır. Mesajdan önce ve sonra girilir.

## 2.5.Yapılandırmaları Kaydetme

### 2.5.1.Yapılandırma Dosyaları

**Aygıt yapılandırmasını depolayan iki sistem dosyası vardır:**

**startup-config**-Bu, NVRAM'de saklanan kayıtlı yapılandırma dosyasıdır. Başlatma veya yeniden başlatma sırasında cihaz tarafından kullanılacak tüm komutları içerir. Flaş, cihaz kapalıyken içeriğini kaybetmez.

**running-config**- Bu, Rasgele Erişim Belleğinde (RAM) saklanır. Mevcut yapılandırmayı yansıtır. Çalışan bir yapılandırmayı değiştirmek, bir Cisco cihazının çalışmasını hemen etkiler. RAM geçici bir bellektir. Cihaz kapatıldığında veya yeniden başlatıldığında tüm içeriğini kaybeder.

Çalışan yapılandırmada yapılan değişiklikleri başlangıç yapılandırma dosyasına kaydetmek için **copy running-config startup-config** ayrıcalıklı EXEC modu komutunu kullanın.

```
Router#show startup-config
Using 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

### 2.5.2.Çalışan Yapılandırmaları Değiştirme

**Çalışan yapılandırmada yapılan değişiklikler istenen etkiye sahip değilse ve çalışan yapılandırma henüz kaydedilmemişse, cihazı önceki yapılandırmasına geri yükleyebilirsiniz. Bunu yapmak için şunları yapabilirsiniz:**

Değiştirilen komutları tek tek kaldırın.

Aygıtı ayrıcalık EXEC modunda **reload** komutunu kullanarak yeniden yükleyin. Not: Bu, cihazın kısa bir süre çevrimdışı kalmasına neden olacağından ağ kesintisine neden olur.

Licensed to yetkin karasungur, yetkinksngr@gmail.com

İstenmeyen değişiklikler startup-config dosyasına kaydedildiyse, EXEC modunda **erase startup-config** komutunu kullanarak tüm yapılandırmaların temizlenmesi gerekebilir.

```
Router# reload
Proceed with reload? [confirm]
Initializing Hardware ...
```

Startup-config dosyasını sildikten sonra, running-config dosyasını RAM'den silmek için cihazı yeniden yükleyin.

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
%SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Router#
```

## 2.6.Bağlantı Noktaları ve Adresler

### 2.6.1.IP Adresleri

IP adreslerinin kullanılması, cihazların birbirlerini bulmasını ve internette uçtan uca iletişim kurmasını sağlayan başlıca araçtır.

IPv4 adresinin yapısına noktalı ondalık gösterim adı verilir ve 0 ile 255 arasında dört ondalık sayı ile gösterilir.

IPv4 alt ağ maskesi, adresin ağ kısmını ana bilgisayar bölümünden ayıran 32 bitlik bir değerdir. IPv4 adresiyle birleştiğinde, alt ağ maskesi cihazın hangi alt ağa üye olduğunu belirler.

Varsayılan ağ geçidi adresi, ana bilgisayarın internet dahil uzak ağlara erişmek için kullanacağı yönlendiricinin IP adresidir.

IPv6 adresleri 128 bit uzunluğundadır ve onaltılık değerlerden oluşan bir dize olarak yazılmıştır. Her dört bit tek bir onaltılık sayı ile temsil edilir; toplam 32 onaltılık değer vardır. Dört onaltılık basamaklı gruplar iki nokta üst üste ":" ile ayrılır.

IPv6 adresleri büyük / küçük harfe duyarlı değildir ve küçük veya büyük harfle yazılabilir.

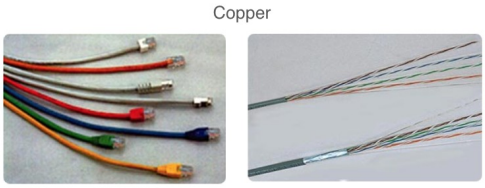
### 2.6.2.Arayüz ve Portlar

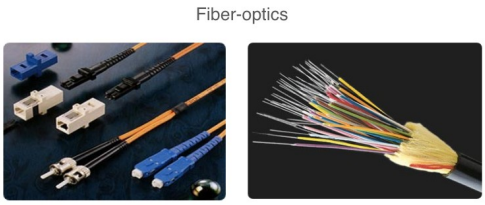
Ağ iletişimleri, son kullanıcı aygıt arabirimlerine, ağ aygıtı arabirimlerine ve bunları bağlayan kablolara bağlıdır.

Ağ ortamı türleri arasında bükümlü çift bakır kablolar, fiber optik kablolar, koaksiyel kablolar veya kablosuz bulunur.

Farklı ağ ortamı türlerinin farklı özellikleri ve avantajları vardır. Çeşitli ortam türleri arasındaki bazı farklar şunlardır:

- Medyanın başarıyla sinyal alabileceği mesafe
- Medyanın kurulacağı ortam
- Veri miktarı ve aktarılma hızı
- Medya ve kurulum maliyeti



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 2.7.IP Adreslemesini Yapılandırma

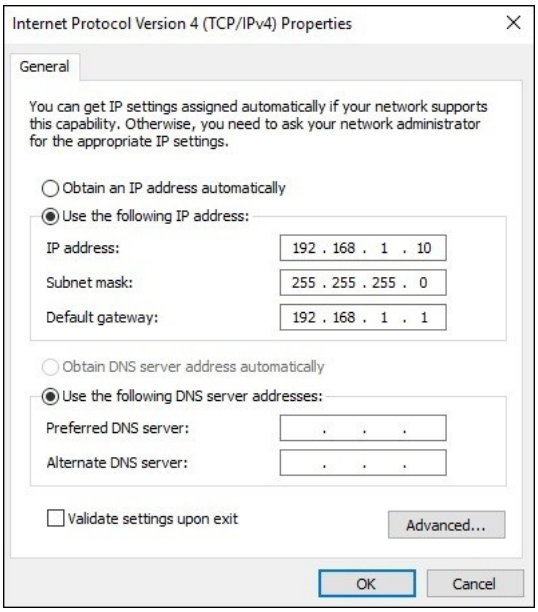
### 2.7.1.Uç Cihazlar için Manuel IP Adresi Yapılandırması

Ağdaki uç cihazların ağdaki diğer cihazlarla iletişim kurmak için bir IP adresine ihtiyacı vardır.

IPv4 adres bilgileri manuel olarak veya Dinamik Ana Bilgisayar Yapılandırma Protokolü-Dynamic Host Configuration Protocol (DHCP) kullanılarak otomatik olarak son cihazlara girilebilir.

Windows PC'de bir IPv4 adresini manuel olarak yapılandırmak için, Denetim Masası> Ağ Paylaşım Merkezi> Bağdaştırıcı ayarlarını değiştir'i seçin ve bağdaştırıcıyı seçin. Sonra sağ tıklayın ve Yerel Alan Bağlantısı Özelliklerini görüntülemek için Özellikler'i seçin.

Ardından, Internet Protokolü Sürüm 4 (TCP / IPv4) Özellikleri penceresini açmak için Özellikler'i tıklatın. Ardından IPv4 adresini ve alt ağ maskesi bilgilerini ve varsayılan ağ geçidini yapılandırın.



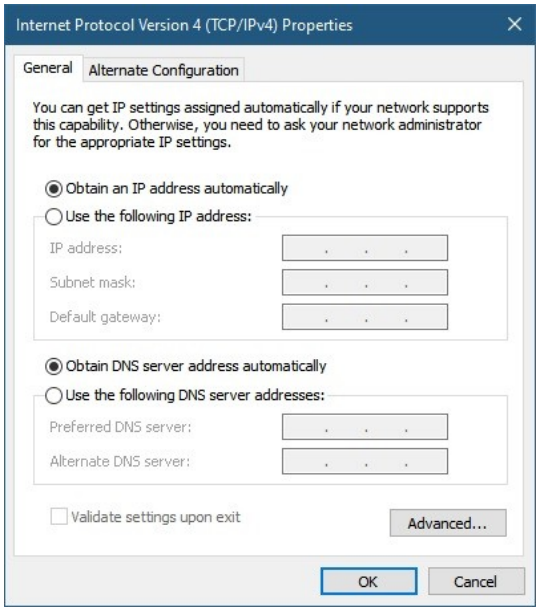

### 2.7.2.Uç Cihazlar için Otomatik IP Adresi Yapılandırması

DHCP, DHCP özellikli her uç cihaz için otomatik IPv4 adres yapılandırmasını etkinleştirir.

Uç cihazlar genellikle otomatik IPv4 adres yapılandırması için DHCP kullanılarak yapılandırılır.

Windows PC'de bir IPv4 adresini manuel olarak yapılandırmak için, Denetim Masası> Ağ Paylaşım Merkezi> Bağdaştırıcı ayarlarını değiştir'i seçin ve bağdaştırıcıyı seçin. Sonra sağ tıklayın ve Yerel Alan Bağlantısı Özelliklerini görüntülemek için Özellikler'i seçin.

Ardından, Internet Protokolü Sürüm 4 (TCP / IPv4) Özellikleri penceresini açmak için Özellikler'i tıklayın, ardından Otomatik olarak bir IP adresi al'ı ve DNS sunucusu adresini otomatik olarak al'ı seçin.




### 2.7.3.Anahtar Sanal Arayüz Yapılandırması

Anahtara uzaktan erişmek için SVI'da bir IP adresi ve bir alt ağ maskesi yapılandırılmalıdır.

Bir anahtarda bir SVI yapılandırmak için:

**interface vlan 1** komutunu genel yapılandırma modunda girin.

Sonra **ip address ip-address subnet-mask** komutunu kullanarak bir IPv4 adresi atayın.

Son olarak, **no shutdown** komutunu kullanarak sanal arabirimi etkinleştirin.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address 192.168.1.20 255.255.255.0
Switch(config-if)# no shutdown
```

# 3.Bölüm: Ağ Protokolleri ve Modelleri

## 3.1.Kurallar

### 3.1.1.İletişimin Temelleri

Ağlar boyut ve karmaşıklık bakımından farklılık gösterebilir. Bir bağlantıya sahip olmak yeterli değildir, cihazlar birbirleri nasıl iletişim kuracaklarını kararlaştırmalıdır.

Herhangi bir iletişimin üç unsuru vardır:

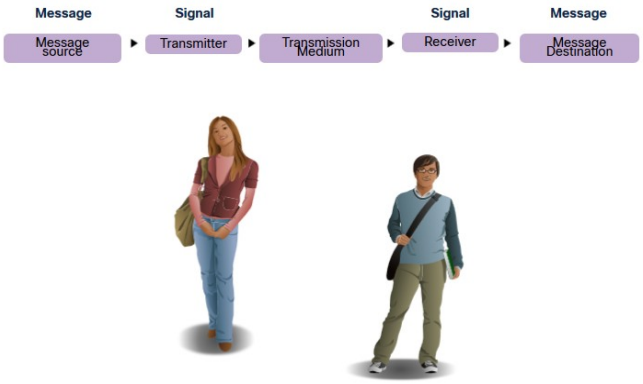
Bir kaynak (gönderici) olacak.

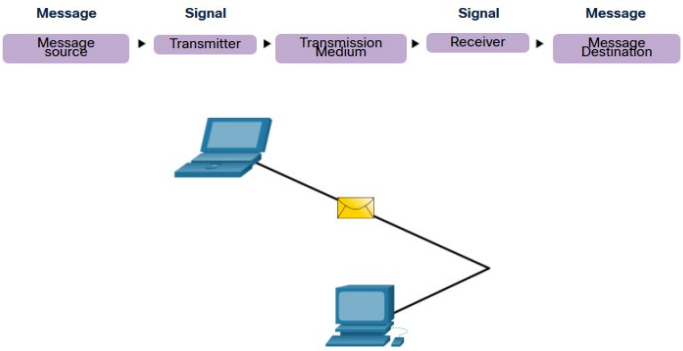
Bir hedef (alıcı) olacaktır.

İletişim yolunun gerçekleşmesini sağlayan bir kanal (medya) olacaktır.

### 3.1.2.İletişim Protokolleri

- Tüm iletişim protokollere tabidir.
- Protokoller iletişimin izleyeceği kurallardır.
- Bu kurallar protokole bağlı olarak değişecektir.




Protokoller aşağıdaki gereksinimleri sağlamalıdır:

- Tanımlanmış bir gönderen ve alıcı
- Ortak dil ve dilbilgisi
- Teslimat hızı ve zamanlaması
- Onay veya onay şartları

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

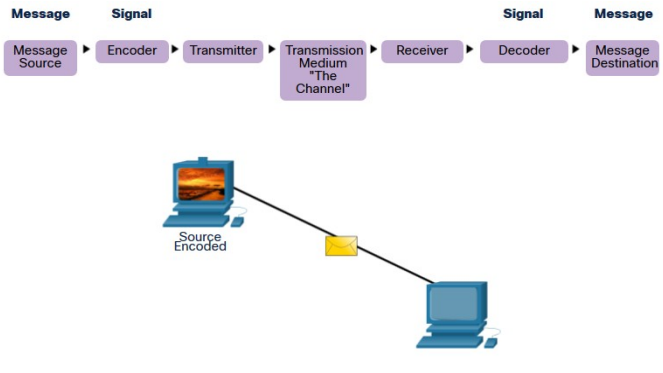
### 3.1.3.Ağ Protokolü Gereksinimleri

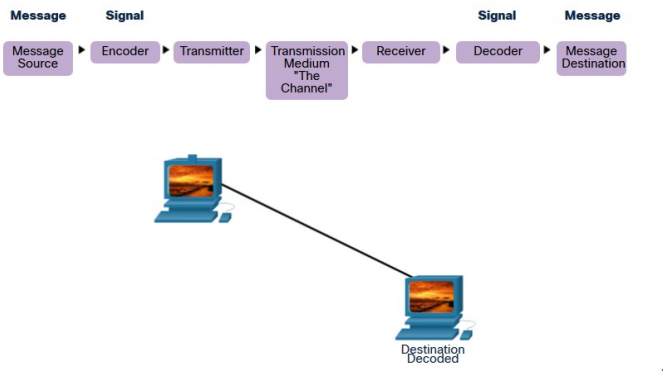
Ortak bilgisayar protokolleri aynı şekilde çalışmalı ve aşağıdaki gereksinimleri içermelidir:

- Mesaj kodlama
- Mesaj biçimlendirme ve kapsülleme
- Mesaj boyutu
- Mesaj zamanlaması
- Mesaj iletim seçenekleri

### 3.1.4.Mesaj Kodlama

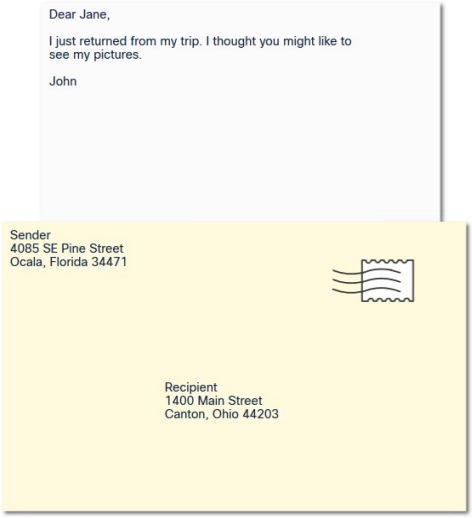
- Kodlama, bilgiyi iletim için kabul edilebilir başka bir forma dönüştürme işlemidir.
- Kod çözme, bilgiyi yorumlamak için bu işlemi tersine çevirir.
-

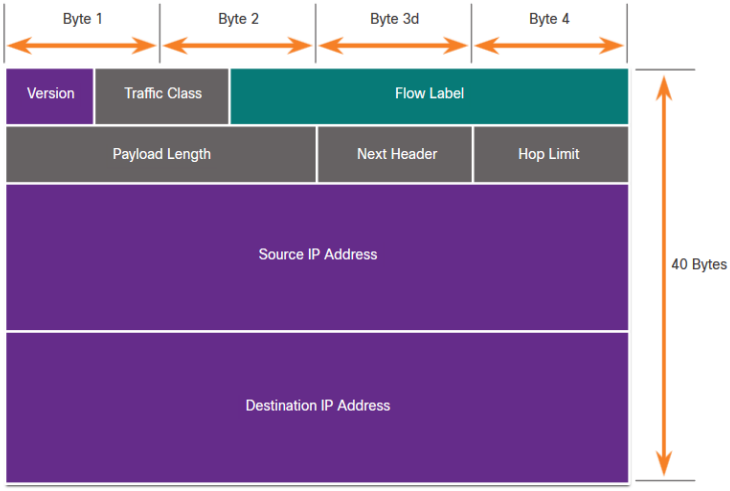



### 3.1.5.Mesaj Biçimlendirme ve Kapsülleme(Encapsulation)

- Bir mesaj gönderildiğinde, belirli bir biçim veya yapı kullanmalıdır.
- Mesaj biçimleri, mesajın türüne ve mesajı iletmek için kullanılan kanala bağlıdır.



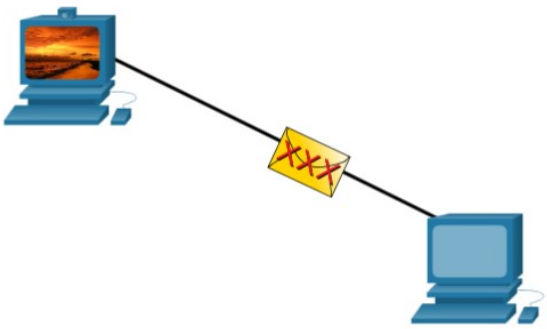



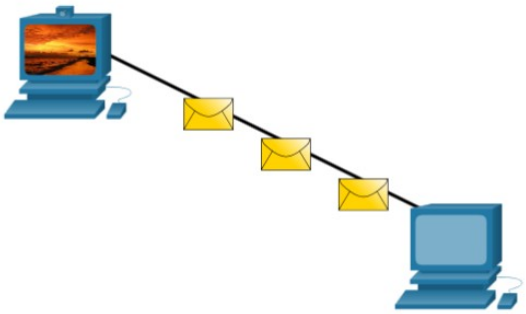

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 3.1.6.Mesaj Boyutu

Bilgisayarlar arasındaki kodlama, ortam için uygun bir biçimde olmalıdır.

- Ağ üzerinden gönderilen mesajlar bitlere dönüştürülür
- Bitler bir ışık, ses veya elektrik impulsları desenine kodlanır.
- Hedef ana bilgisayar, mesajı yorumlamak için sinyallerin kodunu çözmelidir.





### 3.1.7.Mesaj Zamanlaması

Mesaj zamanlaması aşağıdakileri içerir:

**Flow Control –** Veri aktarım hızını yönetir ve ne kadar bilgi gönderilebileceğini ve aktarılma hızını tanımlar.

**Response Timeout –** Bir cihazın hedeften bir yanıt duymadığında ne kadar bekleyeceğini yönetir.

**Access method -** Birinin ne zaman mesaj gönderebileceğini belirler.

"Collisions-Çarpışmalar" gibi konuları düzenleyen çeşitli kurallar olabilir. Bu, aynı anda birden fazla cihaz trafik gönderdiğinde ve mesajların bozulduğu zamandır.

Bazı protokoller proaktiftir ve çarpışmaları önlemeye çalışır; diğer protokoller reaktiftir ve çarpışma meydana geldikten sonra bir kurtarma yöntemi oluşturur.

### 3.1.8.Mesaj Teslim Seçenekleri

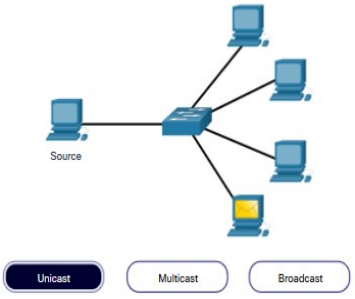
Mesaj teslimi aşağıdaki yöntemlerden biri olabilir:

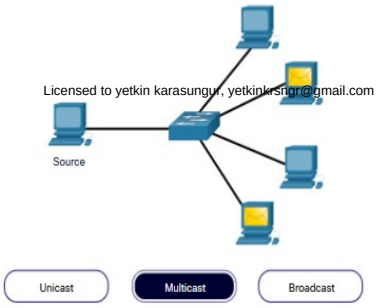
**Unicast –Tekli Yayın** bire bir iletişim

**Multicast –Çoklu Yayın** birdene bir gruba (hepsine değil)

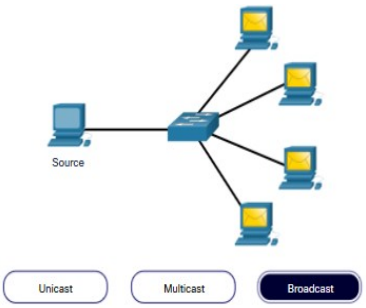
**Broadcast –Yayın** birden herkese

**Not:** Yayınlar (broadcast) IPv4 ağlarında kullanılır, ancak IPv6 için bir seçenek değildir. Daha sonra IPv6 için ek dağıtım seçeneği olarak "Anycast" ı da göreceğiz.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



## 3.2.1.Ağ Protokolüne Genel Bakış

Ağ protokolleri, ortak bir kurallar kümesi tanımlar.

Aşağıdakilere uygulanabilir:

- Software
- Hardware
- Her ikisi

Protokollerin kendilerine ait:

Fonksiyonları
Formatları
Kuraları

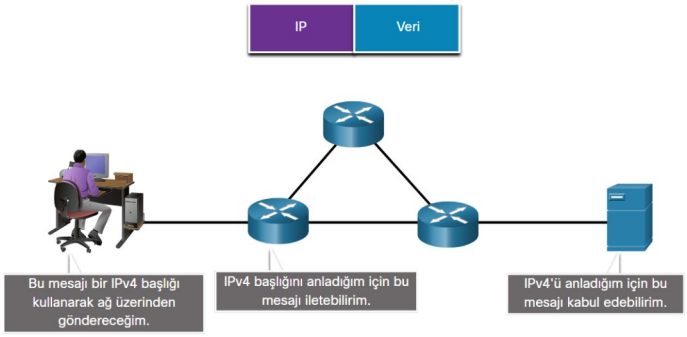
vardır

| Protokol Tipi | Açıklama |
|---|---|
| Network Communications | iki veya daha fazla cihazın bir veya daha fazla ağ üzerinden iletişim kurmasını sağlama |
| Network Security | kimlik doğrulama, veri bütünlüğü ve veri şifreleme sağlama |
| Routing | yönlendiricilerin rota bilgilerini değiş tokuş etmesini, yol bilgilerini karşılaştırmasını ve en iyi yolu seçmesini sağlama |
| Service Discovery | cihazların veya hizmetlerin otomatik tespiti için kullanılır |

## 3.2.2.Ağ Protokolü İşlevleri

Cihazlar iletişim kurmak için kararlaştırılan protokolleri kullanır.

Protokoller bir veya daha fazla fonksiyona sahip olabilir.

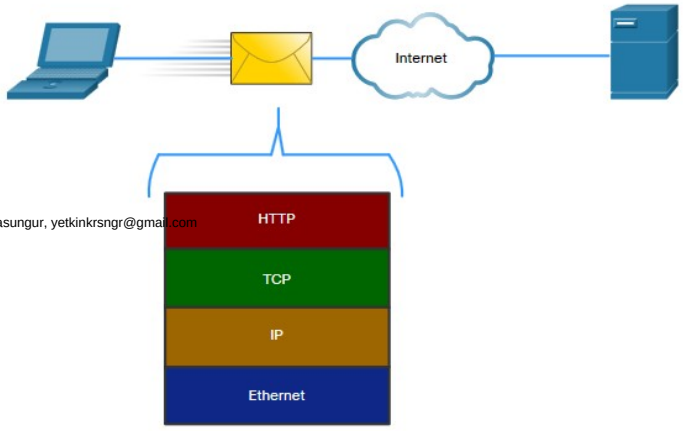



| Fonksiyon | Açıklama |
|---|---|
| Addressing-Adresleme | Göndereni ve alıcıyı tanımlar (MAC Adresi, IP Adresi) |
| Reliability-Güvenilirlik | Garantili teslimat sağlar |
| Flow Control-Akış Kontrolü | Veri akışlarını verimli bir oranda sağlar |
| Sequencing-Sıralama | İletilen her veri segmentini benzersiz şekilde etiketler |
| Error Detection-Hata Tespiti | Verilerin iletim sırasında bozulup bozulmadığını belirler |
| Application Interface-Uygulama Arayüzü | Ağ uygulamaları arasında süreçler arası iletişim |

## 3.2.3.Protokol Etkileşimi

Ağlar çeşitli protokollerin kullanılmasını gerektirir.

Her protokolün kendi işlevi ve biçimi vardır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Protocol | Function |
|---|---|
| Hypertext Transfer Protocol (HTTP) | ▪ Bir web sunucusunun ve bir web istemcisinin etkileşim şeklini yönetir<br>▪ İçeriği ve biçimi tanımlar |
| Transmission Control Protocol (TCP) | ▪ Tek tek konuşmaları yönetir<br>▪ Garantili teslimat sağlar<br>▪ Akış denetimini yönetir |
| Internet Protocol (IP) | Mesajları göndericiden alıcıya global olarak iletir |
| Ethernet | Aynı Ethernet Yerel Alan Ağı'nda (LAN) bir NIC'den başka bir NIC'ye mesaj gönderir |

## 3.3.Protokol Aileleri

### 3.3.1.Network Protokol Aileleri

Protokoller diğer protokollerle çalışabilmelidir.

Protokol Aileleri:

- Bir iletişim fonksiyonunu yerine getirmek için gerekli bir grup birbiriyle ilişkili protokol kümesidir
- Bir sorunu çözmeye yardımcı olmak için birlikte çalışan kurallar kümesidir

Protokoller katmanlar olarak görüntülenir:

- Daha Yüksek Katmanlar
- Alt Katmanlar - verilerin taşınmasıyla ilgilenir ve üst katmanlara hizmet sunar

### 3.3.2.Network Protokollerinin Gelişimi

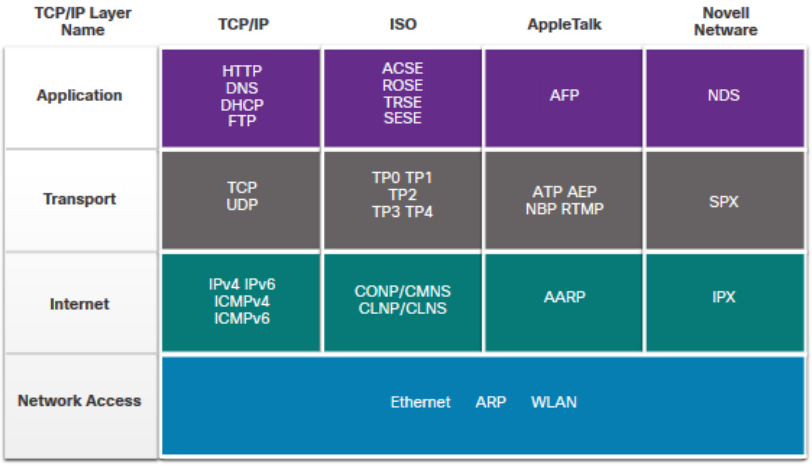
Önde gelen birkaç protokol ailesi vardır.

**Internet Protocol Suite & TCP/IP-** En yaygın protokol paketi ve Internet Engineering Task Force- İnternet Mühendisliği Görev Gücü tarafından sürdürülür (IETF)

**Open Systems Interconnection (OSI) protocols-** International Organization for Standardization - International Telecommunications Union - Uluslararası Standartlar Örgütü (ISO) ve Uluslararası Telekomünikasyon Birliği (ITU) tarafından geliştirilmiştir.

**AppleTalk-** Apple Inc.'in tescilli paketi sürümü

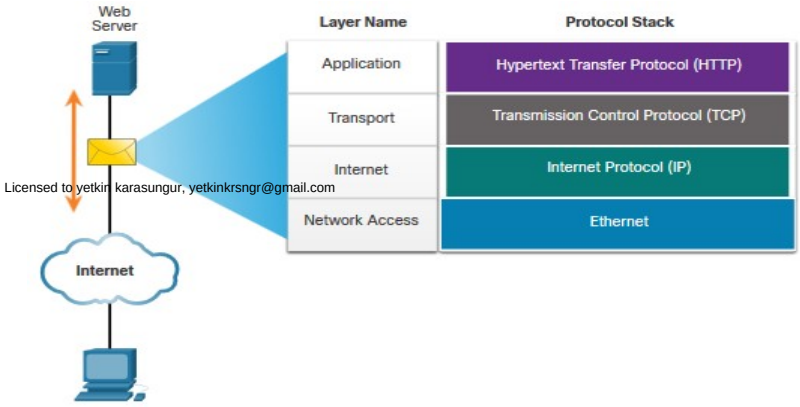
**Novell NetWare-** Novell Inc. tarafından geliştirilen özel paket




### 3.3.3.TCP / IP Protokol Ailesi

TCP / IP protokolleri uygulama, aktarım-taşıma ve internet katmanlarında çalışır.

En yaygın ağ erişim katmanı LAN protokolleri Ethernet ve WLAN'dır (kablosuz LAN).



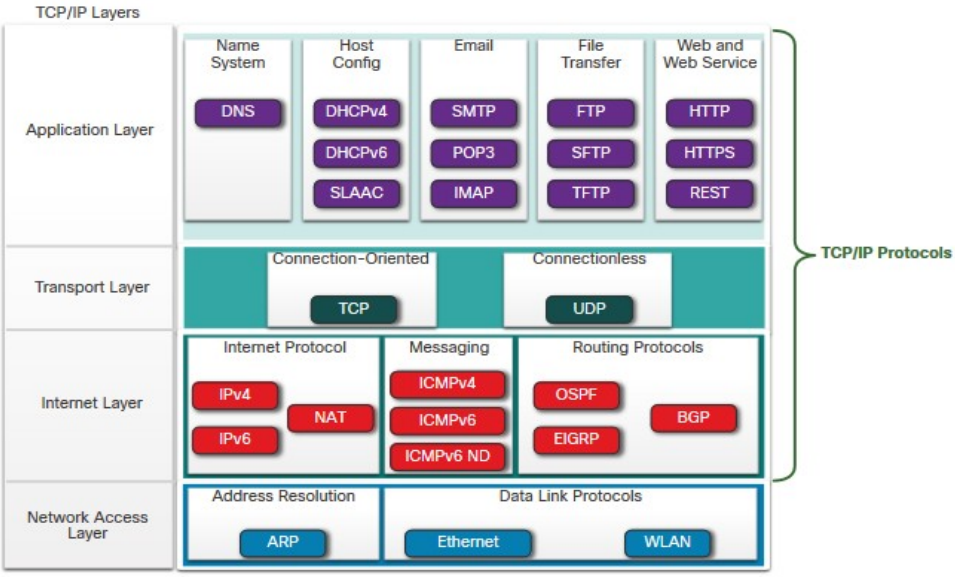

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

TCP / IP, internet tarafından kullanılan protokol paketidir ve birçok protokol içerir.

TCP/IP:

Herkesin erişimine açık olan ve herhangi bir satıcı tarafından kullanılabilen açık bir standart protokol paketidir.

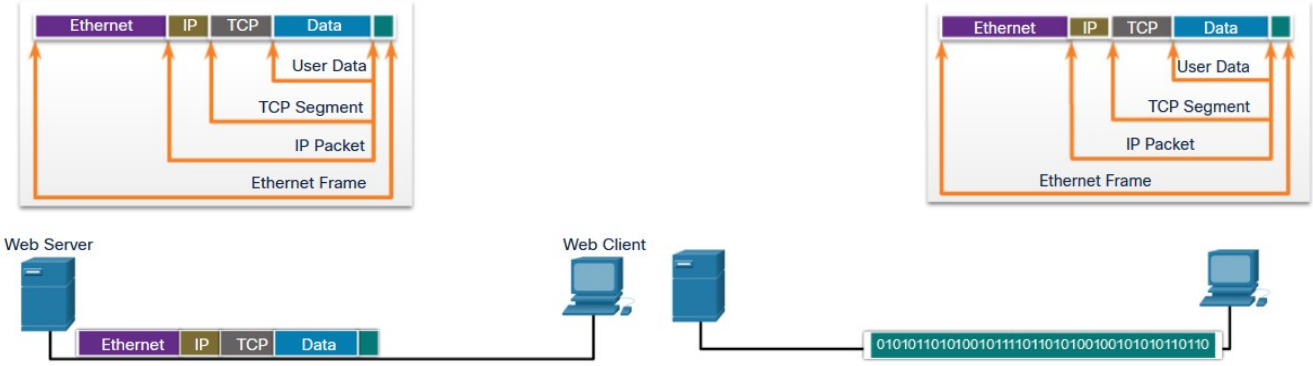
Ağ endüstrisi tarafından onaylanan ve birlikte çalışabilirliği sağlamak için bir standart kuruluşu tarafından onaylanan standartlara dayalı bir protokol paketidir.




### 3.3.4.TCP / IP İletişim Süreci

İstemciye bir web sayfasını kapsülleyen ve gönderen bir web sunucusu.

Web tarayıcısının web sayfasını kapsülden çıkaran bir istemci




## 3.4.Standart Kuruluşluları

### 3.4.1.Açık Standartlar

Açık standartlar şunları teşvik eder:

birlikte çalışabilirlik

rekabet

yenilik

Standart organizasyonları:

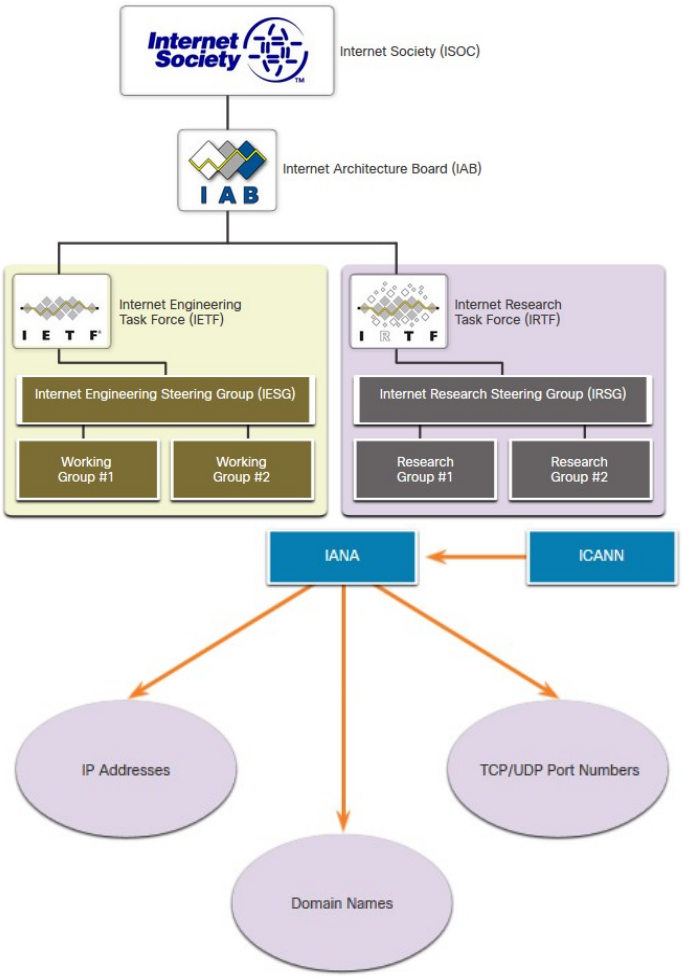
satıcı bağımsız

kar amacı gütmeyen kuruluşlar

açık standartlar konseptini geliştirmek ve teşvik etmek amacıyla kurulmuştur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 3.4.2.İnternet Standartları




Internet Society (ISOC) - İnternetin açık gelişimini ve evrimini teşvik eder

Internet Architecture Board (IAB) - İnternet standartlarının yönetimi ve geliştirilmesinden sorumlu

Internet Engineering Task Force (IETF) - İnternet ve TCP / IP teknolojilerini geliştirir, günceller ve bakımını yapar

Internet Research Task Force (IRTF) - İnternet ve TCP / IP protokolleri ile ilgili uzun vadeli araştırmalara odaklanmıştır

TCP / IP'nin geliştirilmesi ve desteklenmesi ile ilgili standart kuruluşlar

**Internet Corporation for Assigned Names and Numbers (ICANN)** - IP adresi tahsisini, alan adlarının yönetimini ve diğer bilgilerin atanmasını koordine eder

**Internet Assigned Numbers Authority (IANA)** - ICANN için IP adresi tahsisini, alan adı yönetimini ve protokol tanımlayıcılarını denetler ve yönetir

## 3.4.3.Elektronik ve İletişim Standartları

**Institute of Electrical and Electronics Engineers(IEEE, telafuzu "I-triple-E") -** güç ve enerji, sağlık, telekomünikasyon ve ağ alanlarında standartlar oluşturur.

**Electronic Industries Alliance (EIA)**- elektrik kabloları, konektörler ve ağ ekipmanlarını monte etmek için kullanılan 19 inç raflarla ilgili standartlar geliştirir

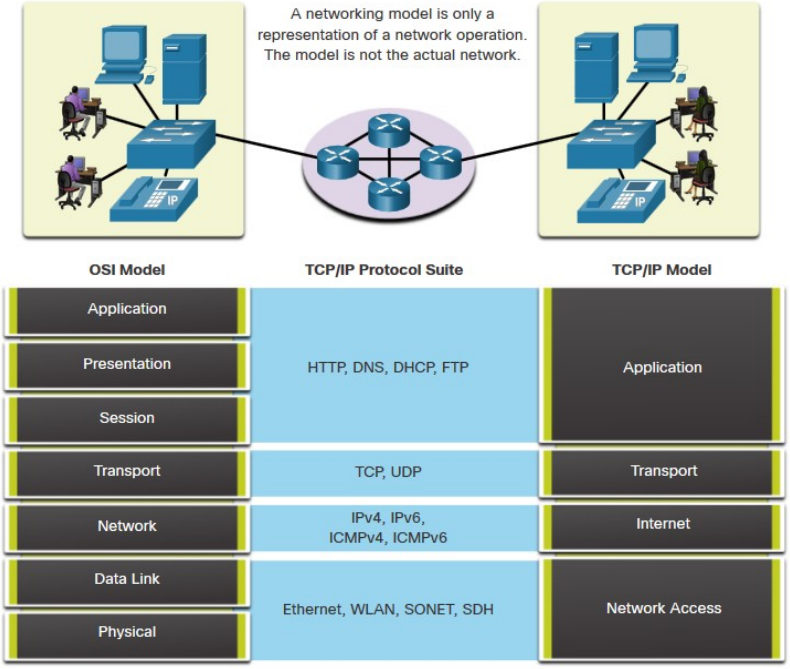
**Telecommunications Industry Association (TIA)**- radyo cihazlarında, hücresel kulelerde, IP Üzerinden Ses (VoIP) cihazlarında, uydu iletişiminde ve daha fazlasında iletişim standartları geliştirir

**International Telecommunications Union-Telecommunication Standardization Sector (ITU-T**) - video sıkıştırma, İnternet Protokol Televizyonu (IPTV) ve dijital abone hattı (DSL) gibi geniş bant iletişim standartlarını tanımlar

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 3.5. Referans Modelleri

### 3.5.1.Katmanlı Model Kullanmanın Yararları




Bir ağın nasıl işlediği gibi karmaşık kavramları açıklamak ve anlamak zor olabilir. Bu nedenle katmanlı bir model kullanılır.

İki tane katmanlı model ağ işlemlerini tanımlar:

Open System Interconnection (OSI) Reference Model

TCP/IP Reference Model

**Katmanlı bir model kullanmanın faydaları şunlardır:**

Belirli bir katmanda çalışan protokollerin üzerinde çalıştıkları bilgileri ve üst ve alt katmanlar için tanımlı bir arayüzü olduğu için protokol tasarımına yardımcı olur

Farklı satıcıların ürünleri birlikte çalışabildiği için rekabeti teşvik eder

Bir katmandaki teknoloji veya yetenek değişikliklerinin yukarıdaki ve altındaki diğer katmanları etkilemesini önler (Ipv4>IPv6)

Ağ işlevlerini ve yeteneklerini tanımlamak için ortak bir dil sağlar

### 3.5.2.The OSI Reference Model

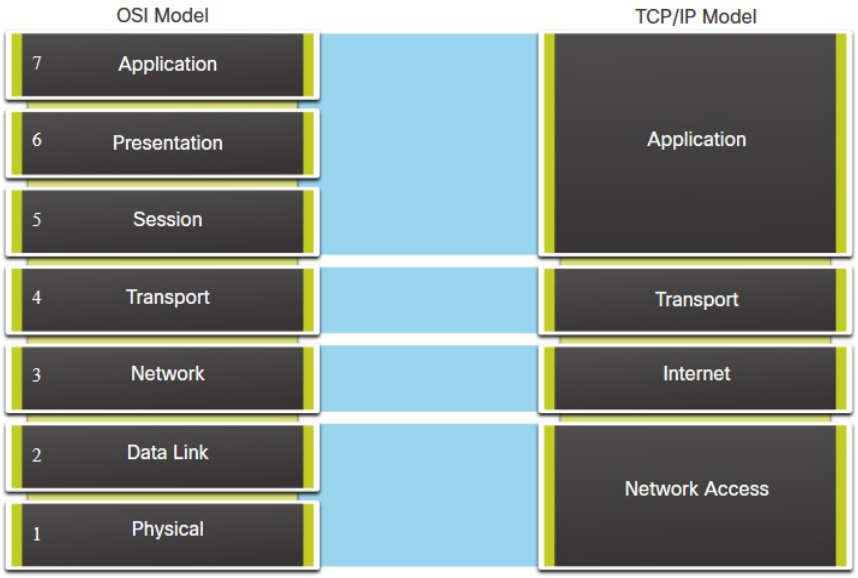
| OSI Model Layer | Description |
|---|---|
| 7 - Application | İşlemler arası iletişim için kullanılan protokolleri içerir. |
| 6 - Presentation | Uygulama katmanı hizmetleri arasında aktarılan verilerin ortak temsilini sağlar. |
| 5 - Session | Sunum katmanına ve veri alışverişini yönetmeye yönelik hizmetler sunar. |
| 4 - Transport | İletişim için verileri bölümlere ayırma, aktarma ve yeniden birleştirme hizmetlerini tanımlar. |
| 3 - Network | Ağ üzerinden veri parçalarını değiştirmek için hizmetler sağlar. |
| 2 - Data Link | Ortak bir ortam üzerinden veri çerçeveleri alışverişi yöntemlerini açıklar. |
| 1 - Physical | Fiziksel bağlantıları etkinleştirme, sürdürme ve devre dışı bırakma yöntemlerini açıklar. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 3.5.3.The TCP/IP Reference Model

| TCP/IP Model Layer | Description |
|---|---|
| **Application** | Verileri kullanıcıya gösterir ayrıca kodlama ve iletişim denetimini temsil eder. |
| **Transport** | Farklı ağlardaki çeşitli cihazlar arasındaki iletişimi destekler. |
| **Internet** | Ağ üzerinden en iyi yolu belirler. |
| **Network Access** | Ağı oluşturan donanım cihazlarını ve medyayı kontrol eder. |

### 3.5.4. İki Modelin Karşılaştırılması



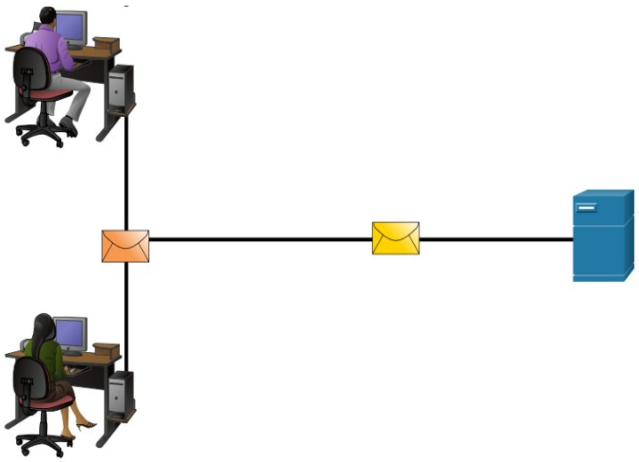

OSI modeli, ağ erişim katmanını ve TCP / IP modelinin uygulama katmanını birden çok katmana böler.

TCP / IP protokol paketi, fiziksel bir ortam üzerinden iletim yaparken hangi protokollerin kullanılacağını belirtmez.

OSI Katman 1 ve 2, medyaya erişmek için gerekli prosedürleri ve ağ üzerinden veri göndermek için fiziksel araçları tanımlar.

## 3.6.Veri Kapsülleme

### 3.6.1.Mesajları Bölümleme



Bölümleme, mesajları daha küçük birimlere bölme işlemidir. Çoğullama, bölümlere ayrılmış verilerin çoklu akışlarını alma ve bunları bir araya getirme işlemidir.

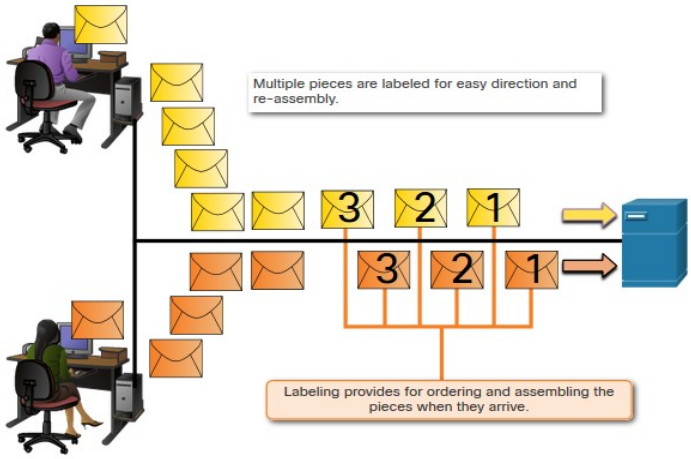
Mesajları bölümlere ayırmanın iki temel avantajı vardır:

**Hızı artırır** - Bir iletişim bağlantısı olmadan ağ üzerinden büyük miktarlarda veri gönderilebilir.

**Verimliliği artırır** - Veri akışının tamamı değil, yalnızca hedefe ulaşamayan segmentlerin yeniden iletilmesi gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

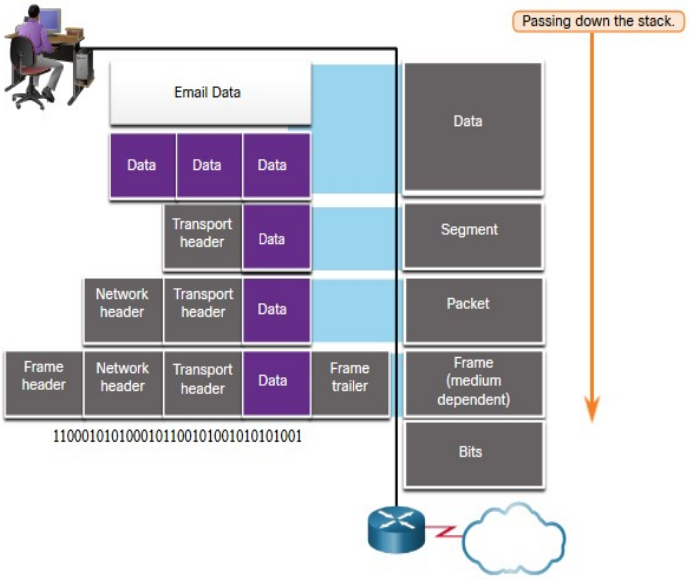
### 3.6.2.Mesajları-İletileri Sıralama




İletileri sıralama, iletinin hedefte yeniden biraraya getirilebilmeleri için segmentleri numaralandırma işlemidir.

TCP, tek tek segmentlerin sıralanmasından sorumludur.

### 3.6.3.Protocol Data Units(PDU)-Protokol Veri Birimleri




Kapsülleme(encapsulation), protokollerin ve bilgilerinin verilere aktarıldığı süreçtir.

Sürecin her aşamasında, bir PDU'nun yeni işlevlerini yansıtan farklı bir adı vardır.

PDU'lar için evrensel bir adlandırma kuralı yoktur, bu derste PDU'lar TCP / IP paketinin protokollerine göre adlandırılır.

Yığından geçen PDU'lar aşağıdaki gibidir:

Data (Data Stream)

Segment

Packet

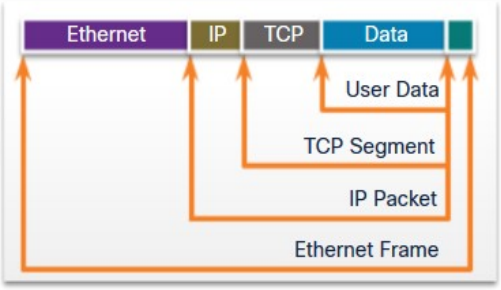
Frame

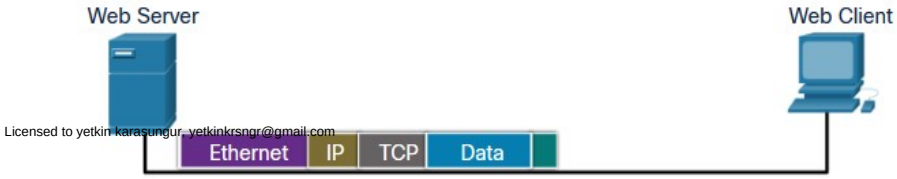
Bits (Bit Stream)

### 3.6.4.Encapsulation Example-Kapsülleme Örneği

Kapsülleme yukarıdan aşağıya bir işlemdir.

Yukarıdaki seviye işlemini gerçekleştirir ve ardından modelin bir sonraki seviyesine geçirir. Bu işlem, bit akışı (1 ve 0'lar) olarak gönderilinceye kadar her katman tarafından tekrarlanır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 3.6.5.De-encapsulation Example-Kapsül Açma Örneği

Veriler yığında yukarı doğru hareket ettikçe kapsülden çıkarılır.

Bir katman işlemini tamamladığında, bu katman başlığını çıkarır ve işlenecek bir sonraki seviyeye geçirir. Bu, uygulamanın işleyebileceği bir veri akışı olana kadar her katmanda tekrarlanır.

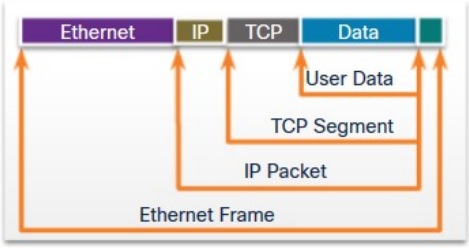
Received as Bits (Bit Stream)

Frame

Packet

Segment

Data (Data Stream)



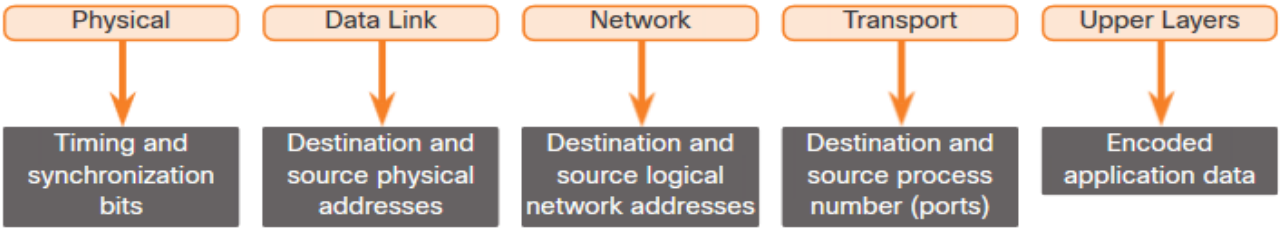
## 3.7.Veri Erişimi

### 3.7.1.Adresler

**Hem veri bağlantısı hem de ağ katmanları, verileri kaynaktan hedefe iletmek için adreslemeyi kullanır.**

**Network layer source and destination addresses**- IP paketini orijinal kaynaktan nihai hedefe teslim etmekten sorumludur.

**Data link layer source and destination addresses** – Veri bağlantı çerçevesini bir ağ arabirim kartından (NIC) aynı ağdaki başka bir NIC'ye iletmekten sorumludur.



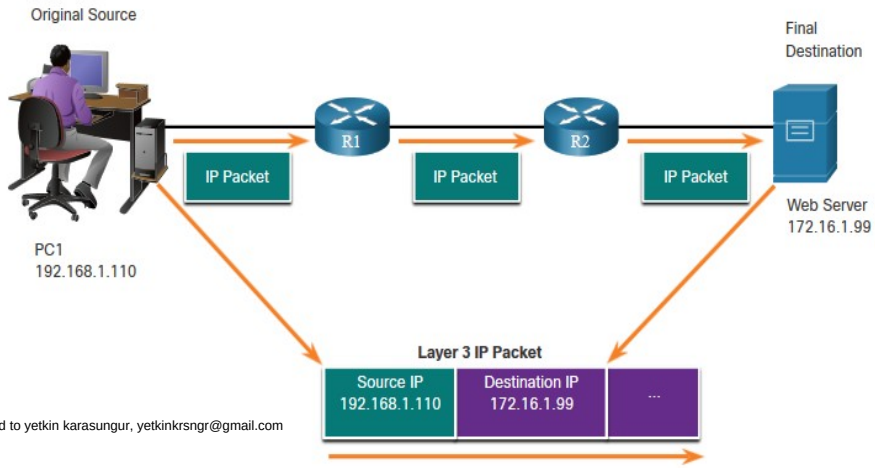

### 3.7.2.Layer 3 Logical Address-Katman 3 Mantıksal Adresler

IP paketi iki IP adresi içerir:

**Source IP address** - Gönderen cihazın IP adresi, paketin orijinal kaynağı.

**Destination IP address** - Alıcı cihazın IP adresi, paketin son varış yeri.

Bu adresler aynı bağlantıda veya uzakta olabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**IP adresi iki bölüm içerir:**

**Network portion (IPv4) or Prefix (IPv6)-Ağ kısmı (IPv4) veya Önek (IPv6)**

Adresin en sol kısmı, IP adresinin üye olduğu ağ grubunu gösterir.

Her LAN veya WAN aynı ağ kısmına sahip olacaktır.

**Host portion (IPv4) or Interface ID (IPv6)**-Ana bilgisayar bölümü (IPv4) veya Arayüz Kimliği (IPv6)

Adresin geri kalan kısmı, grup içindeki belirli bir cihazı tanımlar.

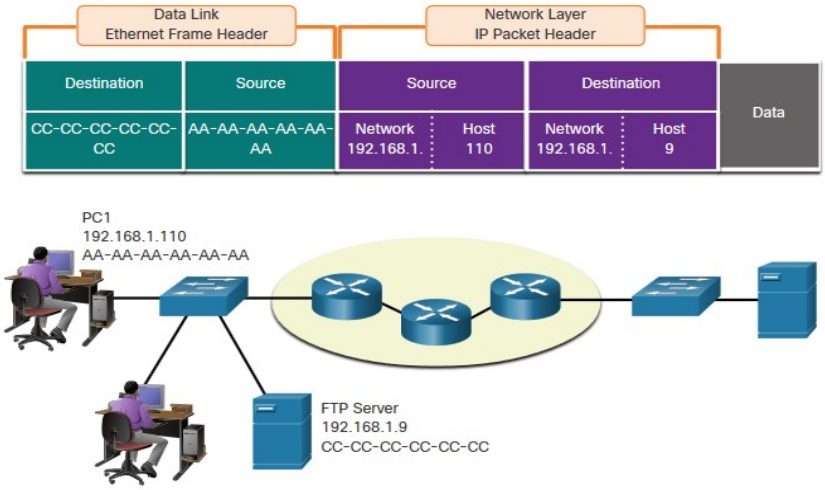
Bu bölüm, ağdaki her cihaz için benzersizdir.

## 3.7.3.Aynı Ağdaki Cihazlar

Aygıtlar aynı ağda olduğunda, kaynak ve hedef adresin ağ bölümünde aynı numaraya sahip olacaktır. (Subnetmask sayesinde)

PC1 – 192.168.1.110

FTP Server – 192.168.1.9



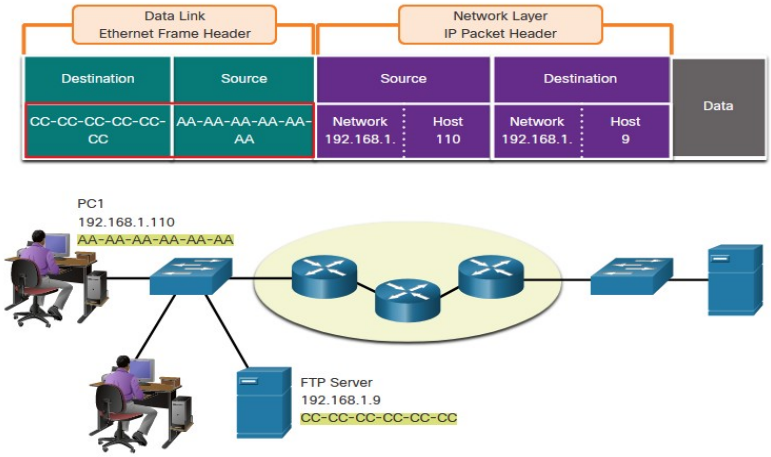

## 3.7.4.Veri Bağlantı Katmanı (Data Link) Adreslerinin Rolü: Aynı IP Ağı

Aygıtlar aynı Ethernet ağında olduğunda, veri bağlantı çerçevesi hedef NIC'nin MAC adresini kullanır.

MAC adresleri fiziksel olarak Ethernet NIC içine yerleştirilmiştir ve yerel adresleme yöntemidir.

Kaynak MAC adresi bağlantıdaki göndericinin adresi olacaktır.

Hedef MAC adresi, nihai hedef uzak olsa bile her zaman kaynakla aynı bağlantıda olacaktır.



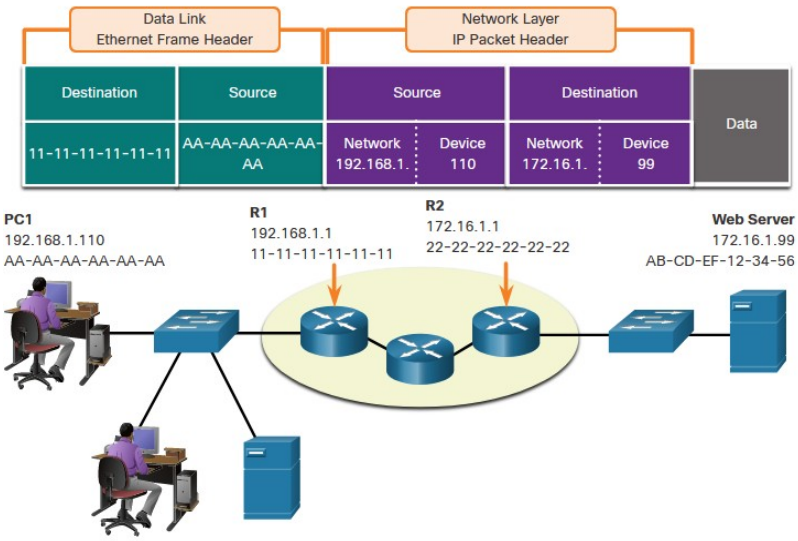

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 3.7.5.Farkı Ağlardaki Cihazlar

Kaynak ve hedefin farklı bir ağ bölümü varsa, bu farklı ağlarda oldukları anlamına gelir.

PC1 – 192.168.1

Web Server – 172.16.1

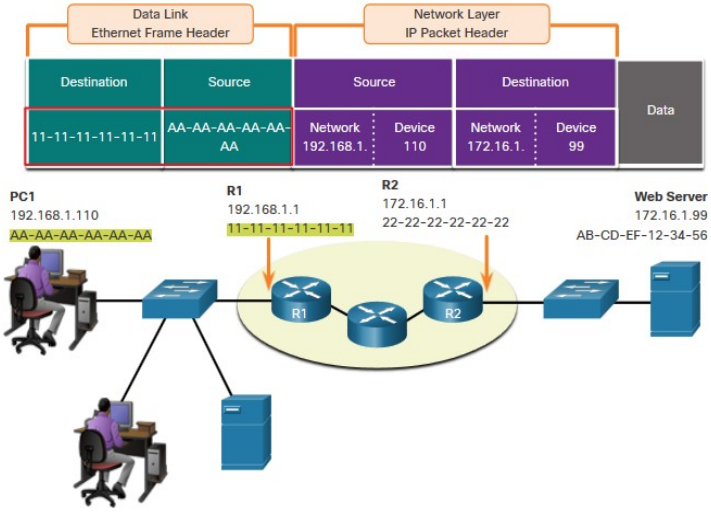



Son hedef uzak ağda olduğunda, Katman 3, Katman 2'ye yönlendirici adresi olarak da bilinen yerel varsayılan ağ geçidi IP adresini sağlar.

Varsayılan ağ geçidi (DGW), bu LAN'ın bir parçası olan ve diğer tüm uzak yerlere "kapı" veya "ağ geçidi" olacak olan yönlendirici arabirimi IP adresidir.

LAN üzerindeki tüm cihazlara bu adres hakkında bilgi verilmelidir, aksi takdirde trafiği yalnızca LAN ile sınırlandırılır.

PC1'deki Katman 2 varsayılan ağ geçidine (Yönlendirici) iletildiğinde, yönlendirici daha sonra bilgileri gerçek hedefe alma yönlendirme işlemini başlatabilir.




**Veri bağlantısı adreslemesi yerel adresleme olduğundan her bağlantı için bir kaynak ve hedef olacaktır.**

İlk segment için MAC adresleme:

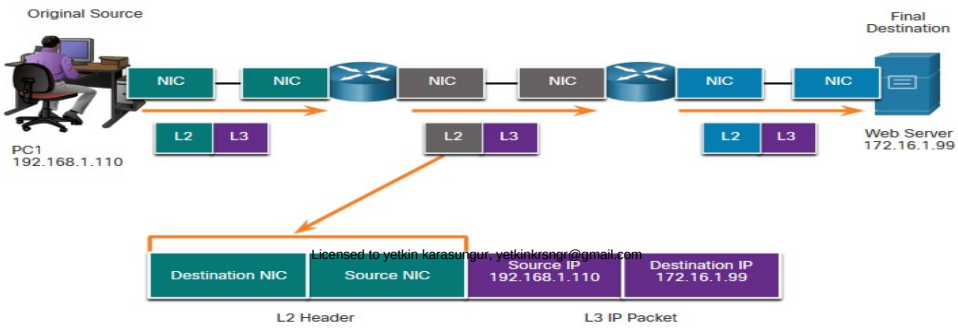
Kaynak - AA-AA-AA-AA-AA-AA (PC1) Çerçeveyi gönderir.

Hedef - 11-11-11-11-11-11 (R1- Varsayılan Ağ Geçidi MAC) Çerçeveyi alır.

İkinci atlama için MAC adresi:

Kaynak – (First Router- exit interface) frame gönderir

Hedef – (Second Router) frame alır

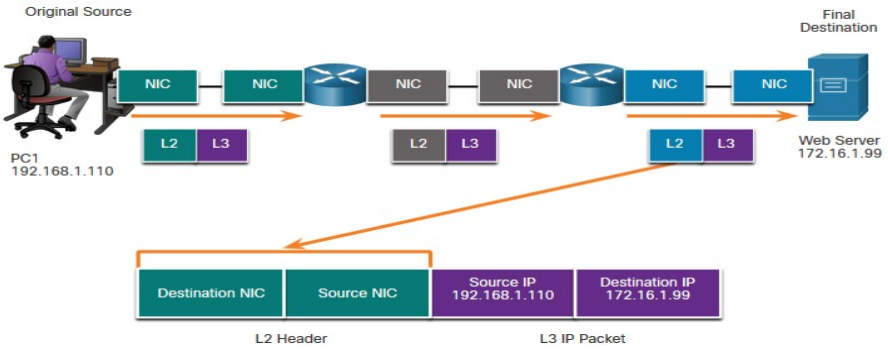



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Son segment için MAC adresleme:

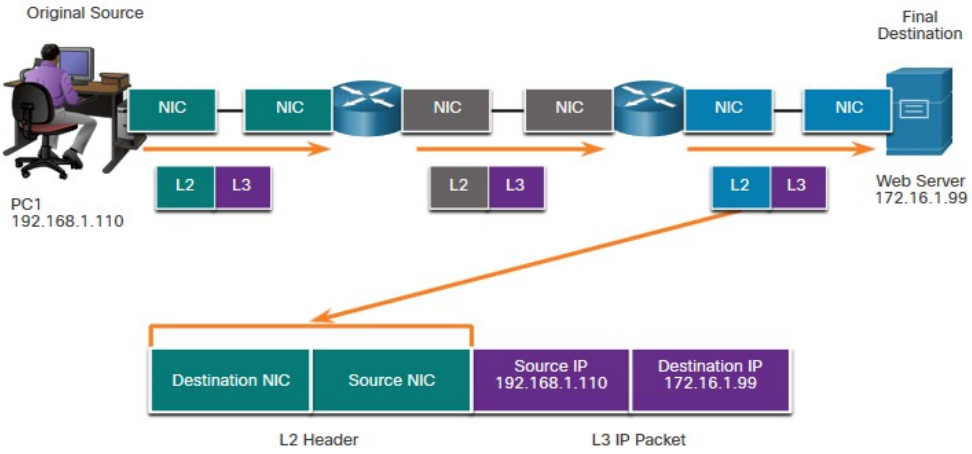
Source – (Second Router- exit interface) frame gönderir

Destination – (Web Server NIC) frame alır




Paketin değiştirilmediğine, ancak çerçevenin değiştirildiğine dikkat edin, bu nedenle L3 IP adreslemesi, L2 MAC adresi gibi segmentten segmente değişmez.

L3 adresleme global olduğundan ve nihai hedef hala Web Sunucusu olduğu için aynı kalır.




**Not:** L2 yerel adresleme bağlantıdan bağlantıya veya atlamadan atlamaya değişirken, L3 adresleme aynı kalır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 4.Bölüm: Fiziksel Katman

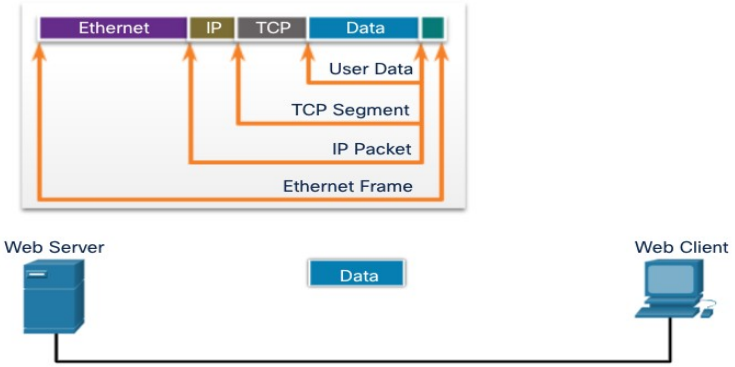
## 4.1.Fiziksel Katmanın Amacı

### 4.1.1.Fiziksel Bağlantı

Herhangi bir ağ iletişimi gerçekleşmeden önce, yerel ağla fiziksel bir bağlantı kurulmalıdır. Ağın kurulumuna bağlı olarak bu bağlantı kablolu veya kablosuz olabilir. Bu genellikle bir şirket ofisi veya ev ağı için geçerlidir. Ağ Arabirim Kartı-Network Interface Card (NIC) bir cihazı ağa bağlar. Bazı cihazlarda yalnızca bir NIC bulunabilirken, diğerlerinde birden fazla NIC bulunabilir (örneğin, Kablolu ve / veya Kablosuz). Tüm fiziksel bağlantılar aynı düzeyde performans sunmaz.

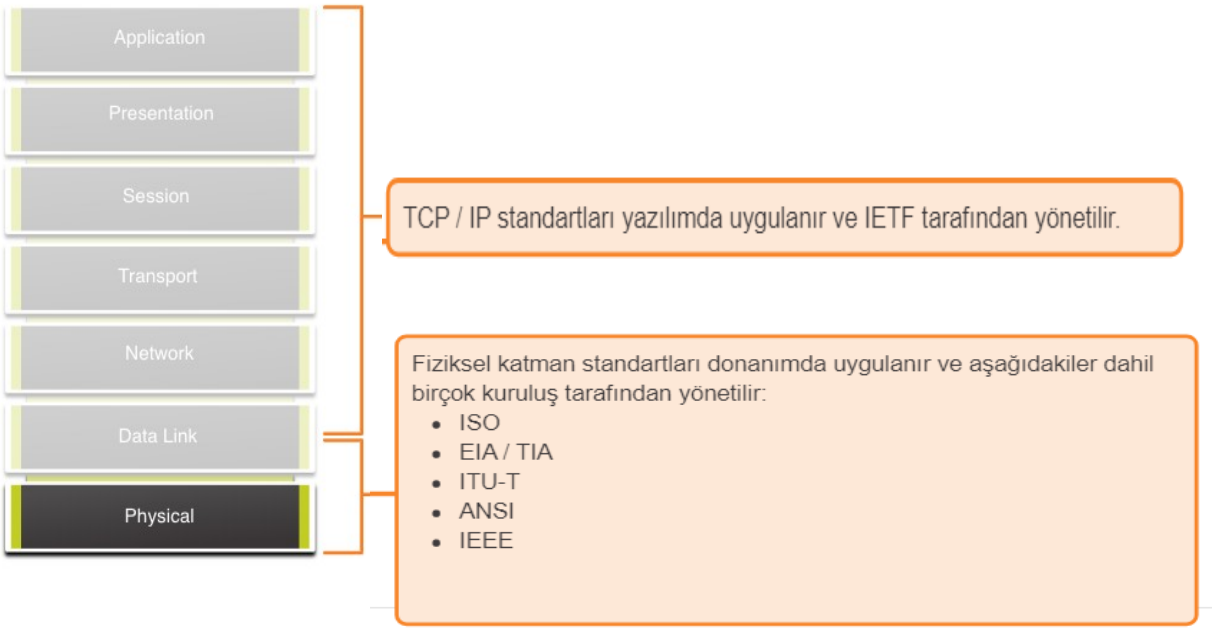
### 4.1.2.Physical Layer-Fiziksel Katman

Ağ ortamındaki bitleri aktarır.Veri Bağlantı Katmanı'ndan tam bir çerçeveyi kabul eder ve bunu yerel ortama iletilen bir dizi sinyal olarak kodlar Bu, kapsülleme sürecindeki son adımdır. Hedefe giden yoldaki bir sonraki aygıt bitleri alır ve çerçeveyi yeniden kapsüller, ardından onunla ne yapacağına karar verir.




## 4.2.Fiziksel Katman Özellikleri

### 4.2.1.Fiziksel Katman Standartları




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 4.2.2.Fiziksel Bileşenler

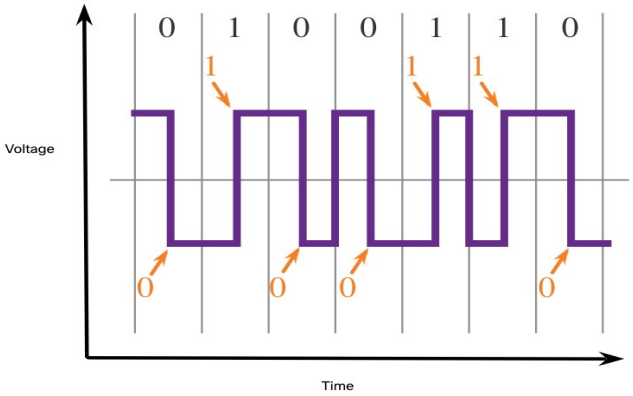
Fiziksel Katman Standartları üç işlevsel alanı ele alır:

- Fiziksel Bileşenler
- Kodlama
- Sinyal

Fiziksel Bileşenler, bitleri temsil eden sinyalleri ileten donanım aygıtları, ortam ve diğer konektörlerdir. NIC'ler, arabirimler ve konektörler, kablo malzemeleri ve kablo tasarımları gibi donanım bileşenlerinin tümü fiziksel katmanla ilişkili standartlarda belirtilmiştir.

### 4.2.3.Encoding-Kodlama

Kodlama, bit akışını ağ yolundaki bir sonraki aygıt tarafından tanınan bir biçime dönüştürür. Bu "kodlama", bir sonraki cihaz tarafından tanınabilecek öngörülebilir modeller sunar. Kodlama yöntemlerine örnek olarak Manchester (şekilde gösterilmektedir), 4B / 5B ve 8B / 10B verilebilir.




### 4.2.4.Bandwidth-Bant Genişliği

Bant genişliği, bir ortamın  taşıyabileceği veri kapasitesidir. Dijital bant genişliği, belirli bir süre içinde bir yerden başka bir yere akabilecek veri miktarını ölçer; saniyede kaç bit iletilebilir. Fiziksel medya özellikleri, mevcut teknolojiler ve fizik yasaları mevcut bant genişliğinin belirlenmesinde rol oynar.

| Bant Genişliği Birimi | Kısaltma | Karşılığı |
|---|---|---|
| Bits per second | bps | 1 bps = fundamental unit of bandwidth |
| Kilobits per second | Kbps | 1 Kbps = 1,000 bps = $10^3$ bps |
| Megabits per second | Mbps | 1 Mbps = 1,000,000 bps = $10^6$ bps |
| Gigabits per second | Gbps | 1 Gbps – 1,000,000,000 bps = $10^9$ bps |
| Terabits per second | Tbps | 1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps |

## 4.3.Bakır Kablolama

### 4.3.1.Bakır Kablolamanın Özellikleri

Bakır kablolama, günümüzde ağlarda kullanılan en yaygın kablolama türüdür. Ucuzdur, kurulumu kolaydır ve elektrik akımı akışına karşı düşük dirence sahiptir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Sınırlamalar:

- Zayıflama - elektrik sinyalleri ne kadar uzun hareket ederse o kadar zayıflar.

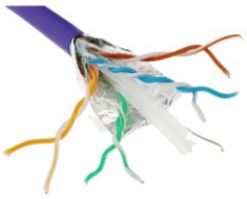
- Elektrik sinyali, veri sinyallerini (Elektromanyetik Girişim-Electromagnetic Interference (EMI) ve Radyo Frekansı Girişimi -Radio Frequency Interference(RFI) ve Çapraz İletişim-Crosstalk) bozabilecek iki kaynaktan gelen girişime duyarlıdır.

Azaltma:

- Kablo uzunluğu sınırlarına sıkı sıkıya bağlı kalmak zayıflamayı azaltacaktır.
- Bazı bakır kablolar metalik ekranlama ve topraklama kullanarak EMI ve RFI'yı azaltır.
- Bazı bakır kablolar, karşı devre çifti kablolarını birlikte bükerek çapraz karışmayı azaltır.

## 4.3.2.Bakır Kablo Çeşitleri

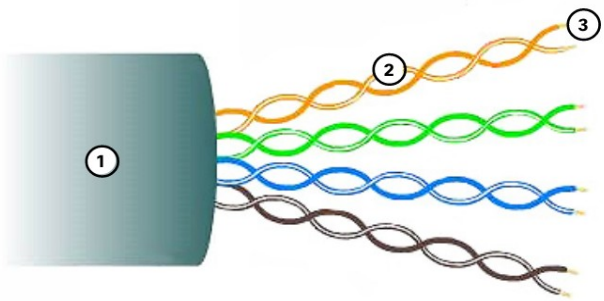
Unshielded Twisted-Pair (UTP) Cable



Shielded Twisted-Pair (STP) Cable

Coaxial Cable

## 4.3.3.Unshielded Twisted Pair (UTP)-Korumasız Çift Bükümlü (UTP)

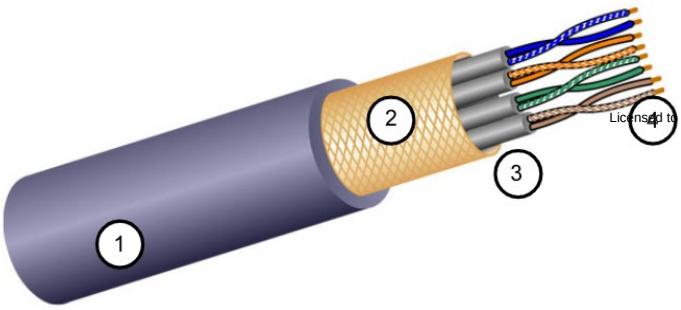



UTP en yaygın ağ ortamıdır.
RJ-45 konektörlerle sonlandırılır
Ana bilgisayarları ara ağ aygıtlarıyla birbirine bağlar.

UTP'nin Temel Özellikleri
1)Dış kılıf bakır telleri fiziksel hasarlardan korur.
B2)ükülü çiftler sinyali parazitten korur.
3)Renk kodlu plastik yalıtım, telleri birbirinden elektriksel olarak izole eder ve her çifti tanımlar.

## 4.3.4.Shielded Twisted Pair (STP)-Korumalı Çift Bükümlü

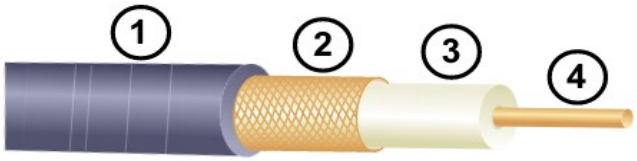
UTP'den daha iyi gürültü koruması
UTP'den daha pahalı
UTP'den daha zor kurulum
RJ-45 konektörlerle sonlandırılır
Ana bilgisayarları ara ağ aygıtlarıyla birbirine bağlar




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

STP'nin Temel Özellikleri
1)Dış kılıf bakır telleri fiziksel hasarlardan korur
2)Örgülü veya folyo ekran EMI / RFI koruması sağlar
3)Her bir kablo çifti için folyo ekran EMI / RFI koruması sağlar
4)Renk kodlu plastik yalıtım telleri birbirinden elektriksel olarak izole eder ve her çifti tanımlar

### 4.3.5.Coaxial Cable-Koaksiyel Kablo



Aşağıdakilerden oluşur:
1)Küçük fiziksel hasarları önlemek için dış kablo kılıfı
2)Dokuma bakır örgü veya metalik folyo, devrede ikinci tel ve iç iletken için bir kalkan görevi görür.
3)Esnek plastik yalıtım tabakası
4)Elektronik sinyalleri iletmek için bir bakır iletken kullanılır.

Koaksiyel kablo ile kullanılan farklı tipte konnektörler vardır.

Aşağıdaki durumlarda yaygın olarak kullanılır:
Kablosuz kurulumlar - kablosuz cihazlara anten takılmasında
Kablolu İnternet Kurulumu - Müşteri binaları kablolaması

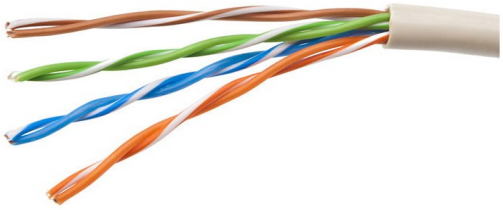
## 4.4.UTP Kablolama

### 4.4.1.UTP Kabloların Özellikleri

UTP, birlikte bükülmüş ve esnek bir plastik kılıf içine yerleştirilmiş dört çift renk kodlu bakır tel içerir. Ekranlama kullanılmaz. UTP, çapraz iletişimi (crostalk-parazit) sınırlamak için aşağıdaki özelliklere dayanır:

Cancellation-İptal - Bir çift kablodaki her tel karşı kutup kullanır. Bir tel negatif, diğer tel pozitif. Birlikte bükülürler ve manyetik alanlar EMI / RFI dışında ve birbirlerini etkili bir şekilde iptal eder.

Her telde foot (30,48 cm) başına bükülme cinsinden değişim - Her tel, kablodaki teller arasında çapraz karışmayı önlemeye yardımcı olan farklı bir miktarda bükülür.



### 4.4.2.UTP Kablolama Standartları ve Konnektörleri

UTP standartları TIA / EIA tarafından belirlenir.

TIA / EIA-568 aşağıdakileri standartlaştırır:

Kablo Çeşitleri

Kablo Uzunlukları

Konektörler

Kablo sonlandırması

Test Yöntemleri

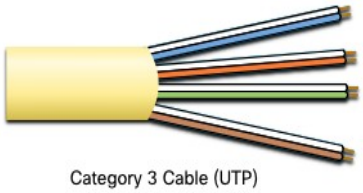
Bakır kablolama için elektrik standartları, kabloyu performansına göre derecelendiren IEEE tarafından belirlenir. Örnekler:

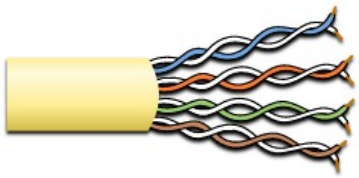
Category 3

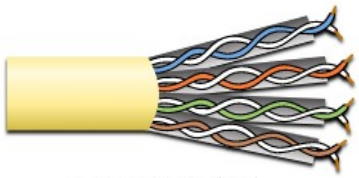
Category 5 and 5e

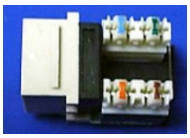
Category 6

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

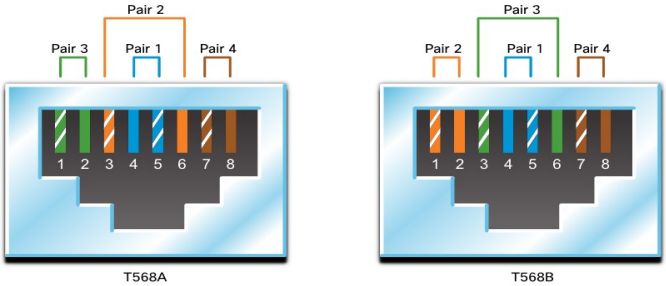

Category 3 Cable (UTP)


Category 5 and 5e Cable (UTP)


Category 6 Cable (UTP)



### 4.4.3.Düz(Straight-through) ve Çapraz(Crossover) UTP Kabloları




| Cable Type | Standard | Application |
|---|---|---|
| Ethernet Straight-through | Both ends T568A or T568B | Host to Network Device |
| Ethernet Crossover * | One end T568A, other end T568B | Host-to-Host, Switch-to-Switch, Router-to-Router |
| * Kablo türünü ve tam bağlantıyı algılamak için Otomatik MDIX kullanan çoğu NIC'ten dolayı Eski Olarak Kabul Edilir | | |
| Rollover | Cisco Proprietary | Bir bağdaştırıcı kullanarak seri bağlantı noktasını Yönlendirici veya Anahtar Konsolu Bağlantı Noktasına bağlama |

## 4.5.Fiber Optik Kablolama

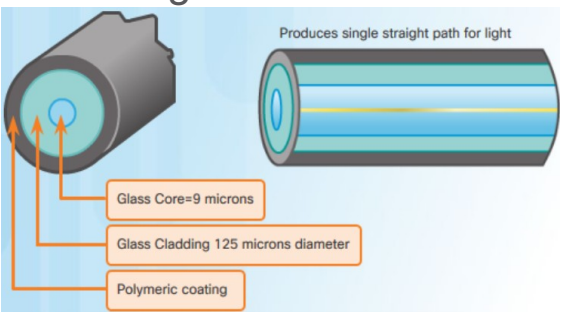
### 4.5.1.Fiber Optik Kabloların Özellikleri

Pahalı olması nedeniyle UTP kadar yaygın değil
Bazı ağ senaryoları için ideal
Diğer ağ ortamlarından daha yüksek bant genişliğinde daha uzun mesafelerde veri iletir
Zayıflamaya karşı daha az hassastır ve EMI / RFI'ya tamamen bağışık değildir
Esnek ve ince cam liflerdinden yapılmıştır
Bitleri ışık darbeleri olarak kodlamak için bir lazer veya LED kullanır
Fiber optik kablo, minimum sinyal kaybı ile iki uç arasında ışık iletmek için bir dalga kılavuzu görevi görür

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

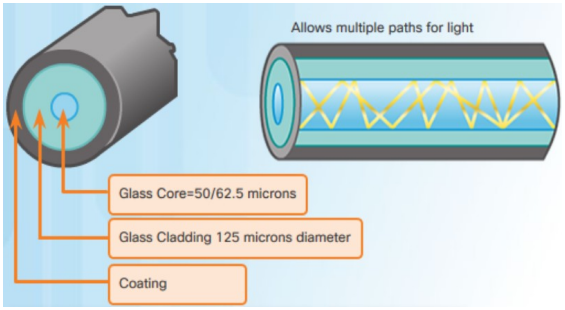
### 4.5.2.Fiber Optik Çeşitleri

Single-Mode Fiber




Çok küçük çekirdek
Pahalı lazerler kullanır
Uzun mesafe uygulamaları

Multimode Fiber




Daha büyük çekirdek
Daha ucuz LED'ler kullanır
LED'ler farklı açılardan iletiyor
550 metrede 10 Gbps'ye kadar

Dispersiyon, ışık atımının zamanla yayılmasını ifade eder. Artan dağılım, sinyal gücünün artması anlamına gelir. MMF'nin SMF'den daha fazla dağılımı vardır, MMF için maksimum kablo mesafesi 550 metredir.

### 4.5.3.Fiber Optik Kablo Kullanımı

Fiber optik kablolama şu sektörlerde kullanılmaktadır:

**Enterprise Networks -** Omurga kablolama uygulamaları ve birbirine bağlı altyapı cihazları için kullanılır
**Fiber-to-the-Home (FTTH) -** Evlere ve küçük işletmelere her zaman açık geniş bant hizmetleri sunmak için kullanılır
**Long-Haul Networks -** Servis sağlayıcılar tarafından ülkeleri ve şehirleri bağlamak için kullanılır
**Submarine Cable Networks -** Okyanus ötesi mesafelere kadar zorlu sualtı ortamlarında hayatta kalma yeteneğine sahip güvenilir yüksek hızlı, yüksek kapasiteli çözümler sağlamak için kullanılır.

Bu derste odak noktamız, işletme içinde fiber optik kullanımıdır.

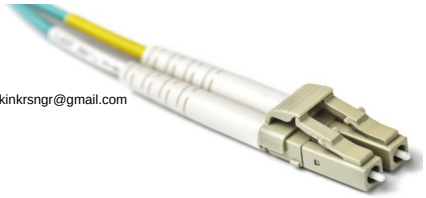
### 4.5.4.Fiber-Optic Konnektörler

Straight-Tip (ST) Connectors

Lucent Connector (LC) Simplex Connectors

Subscriber Connector (SC) Connectors

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



Duplex Multimode LC Connectors

### 4.5.5.Fiber Patch Cords

SC-SC MM Patch Cord

LC-LC SM Patch Cord

ST-LC MM Patch Cord

ST-SC SM Patch Cord

Sarı kablo kılıfı tek modlu fiber kablolar ve turuncu çok modlu fiber kablolar içindir.

### 4.5.6.Fiber Bakır Karşılaştırılması

Optik fiber öncelikle veri dağıtım tesisleri arasında yüksek trafikli, noktadan noktaya bağlantılar ve çok katlı kampüslerdeki binaların birbirine bağlanması için omurga kablolaması olarak kullanılır.

| Uygulama Sorunu | UTP Kablolama | Fiber Optik Kablolama |
|---|---|---|
| Bant genişliği desteği | 10 Mb/s - 10 Gb/s | 10 Mb/s - 100 Gb/s |
| Uzaklık | Nispeten kısa (1-100 metre) | Nispeten uzun (1-100.000 metre) |
| EMI ve RFI'ya bağışıklık | Düşük | Yüksek |
| Elektrik tehlikelerine karşı bağışıklık | Düşük | Yüksek |
| Medya ve konektör maliyetleri | Düşük | Yüksek |
| Gerekli Kurulum becerileri | Düşük | Yüksek |
| Güvenlik önlemleri | Düşük | Yüksek |

## 4.6.Kablosuz (Wireless) Medya

### 4.6.1.Kablosuz Ortamın Özellikleri

Radyo veya mikrodalga frekanslarını kullanarak ikili basamakları temsil eden elektromanyetik sinyaller taşır. Bu, en büyük hareketlilik seçeneğini sunar.

Kablosuz ağın bazı sınırlamaları:

**Kapsama alanı-Coverage area**-Etkili kapsama alanı, dağıtım yerinin fiziksel özelliklerinden önemli ölçüde etkilenebilir.

**Girişim-Interference**- Kablosuz parazite karşı hassastır ve birçok yaygın cihaz tarafından bozulabilir.

**Güvenlik-Security**- Kablosuz iletişim kapsama alanı, fiziksel bir ortam dizisine erişim gerektirmez, böylece herkes erişebilir.

**Paylaşılan Medya-Shared medium**- WLAN'lar yarı çift yönlü olarak çalışır, yani bir seferde yalnızca bir aygıt gönderebilir veya alabilir. WLAN'a aynı anda erişen birçok kullanıcı, her kullanıcı için daha düşük bant genişliğine neden olur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 4.6.2.Kablosuz Ortam Türleri

Kablosuz veri iletişimi için IEEE ve telekomünikasyon endüstrisi standartları, hem veri bağlantısını hem de fiziksel katmanları kapsar. Bu standartların her birinde, fiziksel katman özellikleri şunları gerektirir:

- Veriden radyo sinyali kodlama yöntemleri
- İletim frekansı ve gücü
- Sinyal alımı ve kod çözme gereksinimleri
- Anten tasarımı ve yapımı

Wireless Standards-Kablosuz Standartlar:

- **Wi-Fi (IEEE 802.11)** - Kablosuz LAN (WLAN) teknolojisi
- **Bluetooth (IEEE 802.15)** - Kablosuz Kişisel Alan ağı-Wireless Personal Area network (WPAN) standardı
- **WiMAX (IEEE 802.16)** - Geniş bant kablosuz erişim sağlamak için noktadan çok noktaya topoloji kullanır
- **Zigbee (IEEE 802.15.4)** - Öncelikle Nesnelerin İnterneti (IoT) uygulamaları için düşük veri hızı, düşük güç tüketimi iletişimi sağlar

### 4.6.3.Wireless LAN

Genel olarak, bir Kablosuz LAN (WLAN) aşağıdaki cihazları gerektirir:

**Wireless Access Point (AP)** - Kullanıcılardan gelen kablosuz sinyalleri yoğunlaştırır ve mevcut bakır tabanlı ağ altyapısına bağlar.

**Wireless NIC Adapters** - Ağdaki bilgisayarlara kablosuz iletişim yeteneği sağlar.

Bir dizi WLAN standardı vardır. WLAN ekipmanı satın alırken uyumluluk ve birlikte çalışabilirlik sağlar.

Ağ Yöneticileri, WLAN'ları yetkisiz erişime ve hasara karşı korumak için katı güvenlik politikaları ve süreçleri geliştirmeli ve uygulamalıdır.

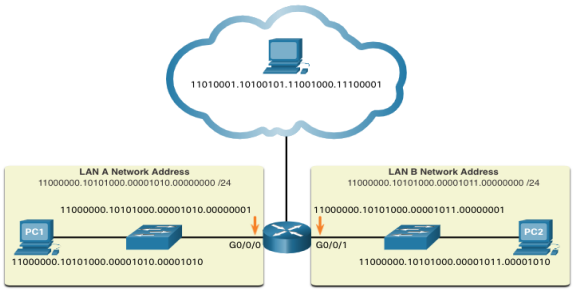
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

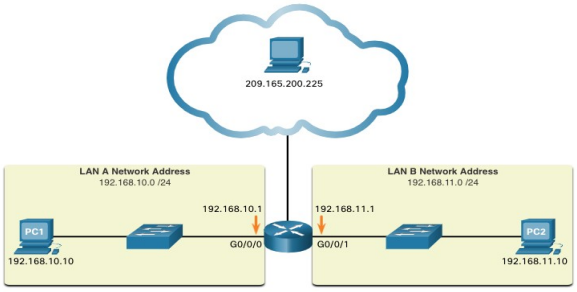
# 5.Bölüm: Sayı Sistemleri

## 5.1.Binary Number System-İkili Sayı Sistemi

### 5.1.1.İkili Sayı Sistemi ve IPv4 Adresleri

- İkili numaralandırma sistemi bit denilen 1 ve 0'lardan oluşur
- Ondalık numaralandırma sistemi 0-9 arasındaki rakamlardan oluşur
- Bilgisayarlar, sunucular ve ağ ekipmanları birbirini tanımlamak için ikili adresleme kullanır
- Her adres, sekizli adı verilen (oktet) dört bölüme ayrılmış 32 bitlik bir dizeden oluşur.
- Her sekizli bir nokta ile ayrılmış 8 bit (veya 1 bayt) içerir.
- İnsanlar tarafından kullanım kolaylığı için, bu noktalı gösterim noktalı ondalık sayıya(desimal) dönüştürülür.




### 5.1.2.Binary Positional Notation-İkili Konumsal Gösterim

Konumsal gösterim, bir rakamın, rakamlar dizisinde yer aldığı "konuma" bağlı olarak farklı değerleri temsil ettiği anlamına gelir.

Ondalık konumsal gösterim sistemi aşağıdaki tablolarda gösterildiği gibi çalışır.

| Taban | 10 | 10 | 10 | 10 |
|---|---|---|---|---|
| Sayının Konumu | 3 | 2 | 1 | 0 |
| Hesaplanan | ($10^3$) | ($10^2$) | ($10^1$) | ($10^0$) |
| Pozisyon Değeri | 1000 | 100 | 10 | 1 |

| | Bin | Yüz | On | Bir |
|---|---|---|---|---|
| Sayının Konumu | 1000 | 100 | 10 | 1 |
| Ondalık Sayı (1234) | 1 | 2 | 3 | 4 |
| Hesaplanan | 1 x 1000 | 2 x 100 | 3 x 10 | 4 x 1 |
| Onları topla… | 1000 | + 200 | + 30 | + 4 |
| Sonuç | **1,234** | | | |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

İkili konumsal gösterim sistemi aşağıdaki tablolarda gösterildiği gibi çalışır.

| Taban | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
|---|---|---|---|---|---|---|---|---|
| Sayının Konumu | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
| Hesaplanan | ($2^7$) | ($2^6$) | ($2^5$) | ($2^4$) | ($2^3$) | ($2^2$) | ($2^1$) | ($2^0$) |
| Konum Değeri | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

| Positional Value | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| Binary Number (11000000) | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| Hesaplanan | 1x128 | 1x64 | 0x32 | 0x16 | 0x8 | 0x4 | 0x2 | 0x1 |
| Onları Topla | 128 | + 64 | + 0 | + 0 | + 0 | + 0 | + 0 | + 0 |
| Sonuç | **192** | | | | | | | |

## 5.1.3.İkiliden Ondalığa Dönüştürme

11000000.10101000.00001011.00001010 sayısını ondalığa dönüştürün.

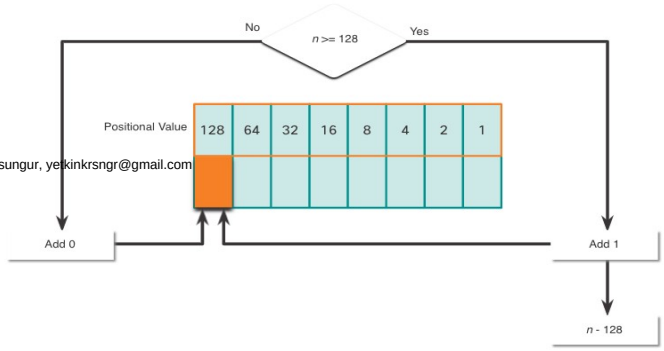
| Konum Değeri | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | |
|---|---|---|---|---|---|---|---|---|---|
| **Binary Number (11000000)** | **1** | **1** | **0** | **0** | **0** | **0** | **0** | **0** | 192 |
| Hesaplanan | 1x128 | 1x64 | 0x32 | 0x16 | 0x8 | 0x4 | 0x2 | 0x1 | |
| Onları Topla... | 128 | + 64 | + 0 | + 0 | + 0 | + 0 | + 0 | + 0 | |
| **Binary Number (10101000)** | **1** | **0** | **1** | **0** | **1** | **0** | **0** | **0** | 168 |
| Hesaplanan | 1x128 | 0x64 | 1x32 | 0x16 | 1x8 | 0x4 | 0x2 | 0x1 | |
| Onları Topla... | 128 | + 0 | + 32 | + 0 | + 8 | + 0 | + 0 | + 0 | |
| **Binary Number (00001011)** | **0** | **0** | **0** | **0** | **1** | **0** | **1** | **1** | 11 |
| Hesaplanan | 0x128 | 0x64 | 0x32 | 0x16 | 1x8 | 0x4 | 1x2 | 1x1 | |
| Onları Topla... | 0 | + 0 | + 0 | + 0 | + 8 | + 0 | + 2 | + 1 | |
| **Binary Number (00001010)** | **0** | **0** | **0** | **0** | **1** | **0** | **1** | **0** | 10 |
| Hesaplanan | 0x128 | 0x64 | 0x32 | 0x16 | 1x8 | 0x4 | 1x2 | 0x1 | |
| Onları Topla... | 0 | + 0 | + 0 | + 0 | + 8 | + 0 | + 2 | + 0 | |

192.168.11.10

## 5.1.4.Ondalıktan İkiliye Dönüştürme

İkili konum değeri tablosu, noktalı ondalık IPv4 adresini ikiliye dönüştürmede yararlıdır.

128 konumunda başlayın (en önemli bit).
Sekizlik (n) ondalık sayısı 128'e eşit veya daha büyük mü?
Hayırsa, 128 konum değerine bir ikili 0 kaydedin ve 64 konum değerine gidin.
Evetse, 128 konum değerine bir ikili 1 kaydedin, ondalık sayıdan 128 çıkarın ve 64 konum değerine gidin.
Bu adımları 1 konum değeri üzerinden tekrarlayın.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Örnek:** Ondalık 168'i ikiliye dönüştürün

168> 128 mi?

Evet, 128 konumuna 1 girin ve 128 çıkarın (168-128 = 40)

40> 64 mü?

Hayır, 64 konumuna 0 girin ve devam edin

40> 32 mi?

Evet, 32 konumuna 1 girin ve 32 çıkarın (40-32 = 8)

8> 16 mı?

Hayır, 16 konumuna 0 girin ve devam edin

8> 8 mi?

Eşit. 8 konumuna 1 girin ve 8 çıkarın (8-8 = 0)

Değer kalmadı. Kalan ikili konumlara 0 girin

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |

Ondalık 168, ikili olarak 10101000 olarak yazılır.

## 5.2.Hexadecimal Number System-Onaltılı Sayı Sistemi

### 5.2.1.Onaltılık Sayılar ve IPv6 Adres

IPv6 adreslerini anlamak için onaltılık sayıyı ondalığa ve tam tersine çevirebilmeniz gerekir.
Onaltılık, 0 ile 9 arasındaki rakamları ve A - F arasındaki harfleri kullanan, temel on altı numaralandırma sistemidir.
Bir değeri, tek bir onaltılık basamak olarak ifade etmek, dört ikili bite göre daha kolaydır.
Onaltılık sayılar IPv6 adreslerini ve MAC adreslerini temsil etmek için kullanılır.

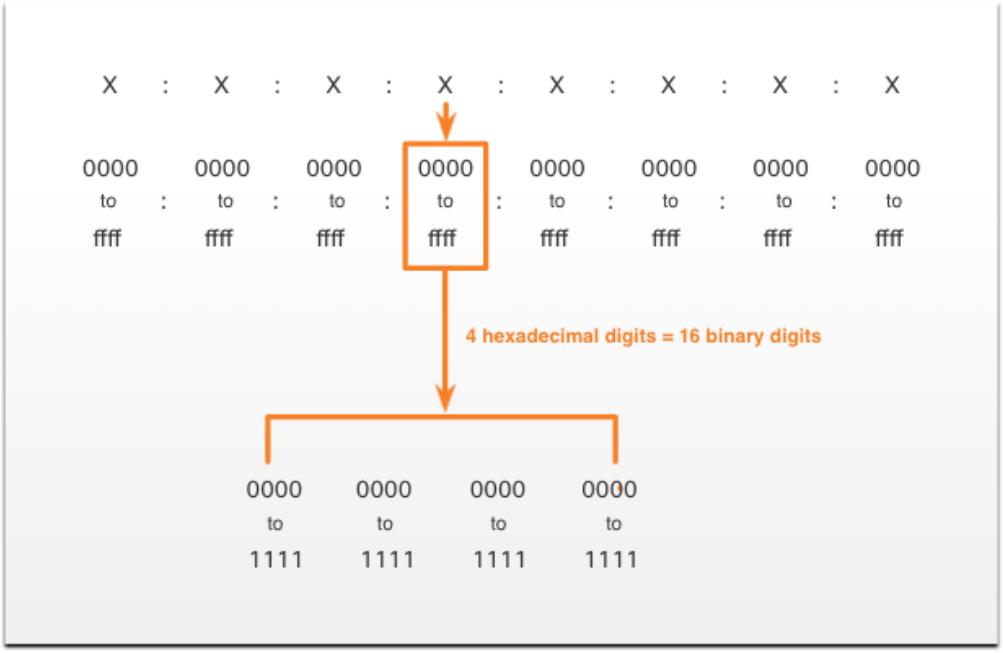
| Decimal | Binary | Hexadecimal |
|---|---|---|
| 0 | 0000 | 0 |
| 1 | 0001 | 1 |
| 2 | 0010 | 2 |
| 3 | 0011 | 3 |
| 4 | 0100 | 4 |
| 5 | 0101 | 5 |
| 6 | 0110 | 6 |
| 7 | 0111 | 7 |
| 8 | 1000 | 8 |
| 9 | 1001 | 9 |
| 10 | 1010 | A |
| 11 | 1011 | B |
| 12 | 1100 | C |
| 13 | 1101 | D |
| 14 | 1110 | E |
| 15 | 1111 | F |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

IPv6 adresleri 128 bit uzunluğundadır. Her 4 bit bir tek onaltılık sayı ile temsil edilir. Bu, IPv6 adresini toplam 32 onaltılık değer yapar.

Şekil, her bir X dört onaltılık değeri temsil eden bir IPv6 adresi yazmak için tercih edilen yöntemi göstermektedir.

Her dört onaltılık karakter grubuna onaltılı (hextet) denir.




## 5.2.2.Ondalıktan Onaltılıya Dönüşümler

Ondalık sayıları onaltılık değerlere dönüştürmek için listelenen adımları izleyin:

- Ondalık sayıyı 8 bitlik ikili dizelere dönüştürün.
- İkili dizeleri en sağdan başlayarak dörtlü gruplar halinde bölün.
- Her dört ikili sayıyı eşdeğer onaltılık basamağa dönüştürün.

Örneğin, 168 üç adımlı işlem kullanılarak onaltılık biçime dönüştürülmüştür.

- 168, ikili sayı sisteminde 10101000'dir.
- 10101000 dört ikili basamaklı iki grupta , 1010 ve 1000 olarak ayrılır
- 1010, hex A ve 1000, hex 8'dir, bu nedenle 168, onaltılık olarak A8'dir.

## 5.2.3.Onaltılıdan Ondalık Dönüşüm

Onaltılık sayıları ondalık değerlere dönüştürmek için listelenen adımları izleyin:

- Onaltılık sayıyı 4 bitlik ikili dizelere dönüştürün.
- En sağdan başlayarak 8 bit ikili gruplama oluşturun.
- Her 8 bitlik ikili gruplamayı eşdeğer ondalık basamağına dönüştürün.

Örneğin, D2 üç adımlı işlem kullanarak ondalık sayıya dönüştürülür:

- D2 4-bit ikili dizgilerde 1101 ve 0010'dur.
- 1101 ve 0010, 8 bitlik bir grupta 11010010'dur.
- İkili olarak 11100010 ondalık olarak 210'a eşittir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Desimal To Binary

**Örnek: Ondalık 112 sayısını ikilik olarak yazınız.**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |

**112>128**
**128 den küçük olduğu için 128 basamağı 0**
**112>64**
**64 basamağı 1**
**112-64=48**
**48>32 olduğu için 32 basamağı 1**
**48-32=16**
**16>=16 olduğu için 16 basamağı 1**
**16-16=0**
**diğer basamakların hepsi 0**

**Sonuç: 01110000**

## Binary To Desimal

**Örnek: 11011011 ikilik sayısını ondalık olarak yazınız**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 128 | 64 | 0 | 16 | 8 | 0 | 2 | 1 |

**128+64+16+8+2+1=**

**Sonuç: 219**

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# Hexadesimal To Desimal

**Örnek: 1A Hexadesimal sayısını desimal olarak yazınız.**

**Hexadesimal 1 = 0001 ikiliye eşittir**
**Hexadesimal A = 1010 ikiliye eşittir.**

**İkisini bir araya getirir oktet yaparsak 00011010 olur. Bunu da desimale çevirelim.**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 16 | 8 | 0 | 2 | 0 |

**16+8+2+1=26**

**Sonuç:26**

# Desimal To Hexadesimal

**Örnek: 240 ondalık sayısını hexadesimal olarak yazınız.**

**240 sayısını önce ikiliye çeviriyoruz.**

**240>128**
**128 basamağı 1**
**240-128= 112**
**112>64**
**64 basamağı 1**
**112-64=48**
**48>32**
**32 basamağı 1**
**48-32=16**
**16>=16**
**16 basamağı 1**
**16-16=0**
**geri kalan basamaklar 0**

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

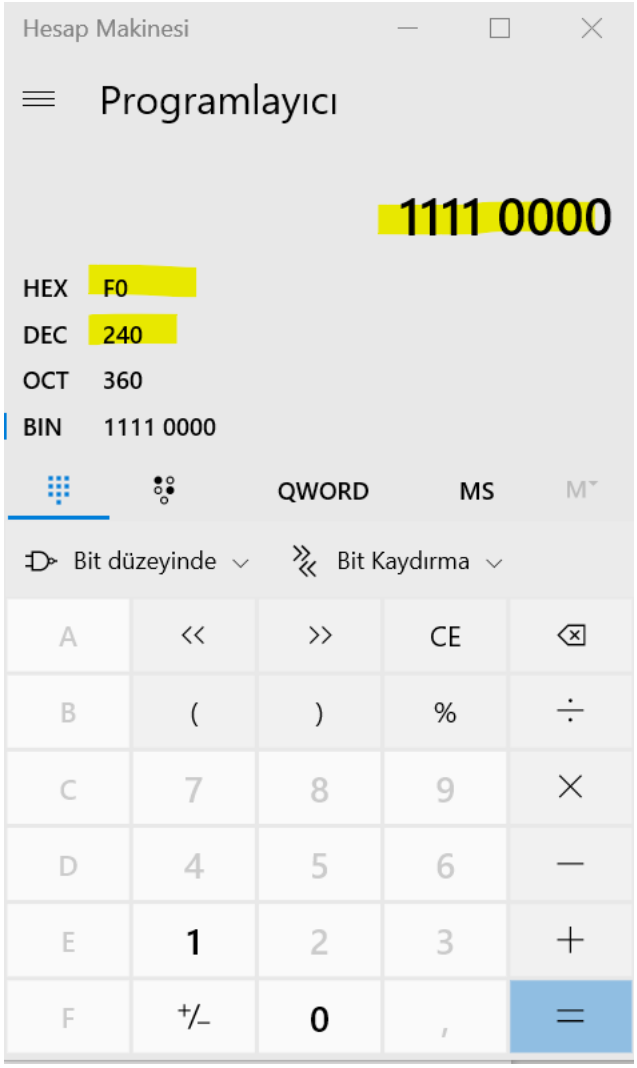
**11110000 olarak bulunur.**

**Bu sayıyı iki tane 4 lü olarak yazalım.**

**1111 0000**
**1111 =F**
**0000=0**
**Sonuç: F0**

**Arkadaşlar benzer örnekleri kendiniz farklı sayılar ile yapınız ve Windows'taki hesap makinesi ile yaptıklarınızı doğrulayınız.**

**W**




**www.cemaltaner.com.tr**

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 6.Bölüm: Data Link Layer-Veri Bağlantısı Katmanı

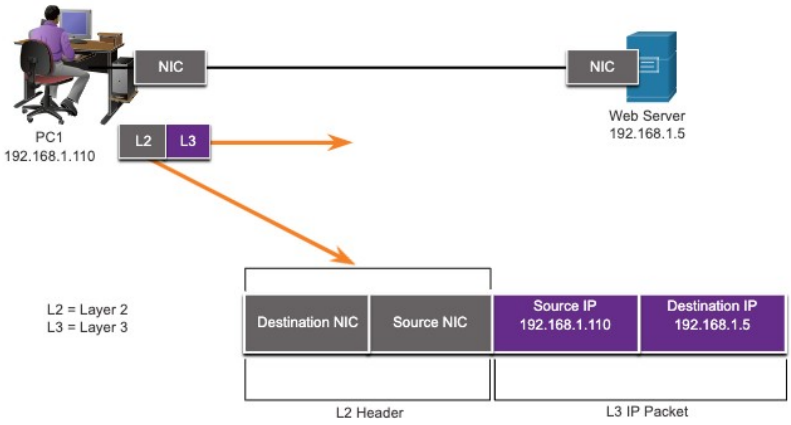
## 6.1.Veri Bağlantısı Katmanının Amacı

### 6.1.1.Veri Bağlantısı Katmanı

Veri Bağlantısı katmanı, uç cihaz ağ arayüz kartları (NIC) arasındaki iletişimden sorumludur.

Üst katman protokollerinin fiziksel katman ortamına erişmesine izin verir ve Katman 3 paketlerini (IPv4 ve IPv6) Katman 2 Çerçeveleri (Frame) alır.

Ayrıca hata algılama gerçekleştirir ve bozuk çerçeveleri reddeder.



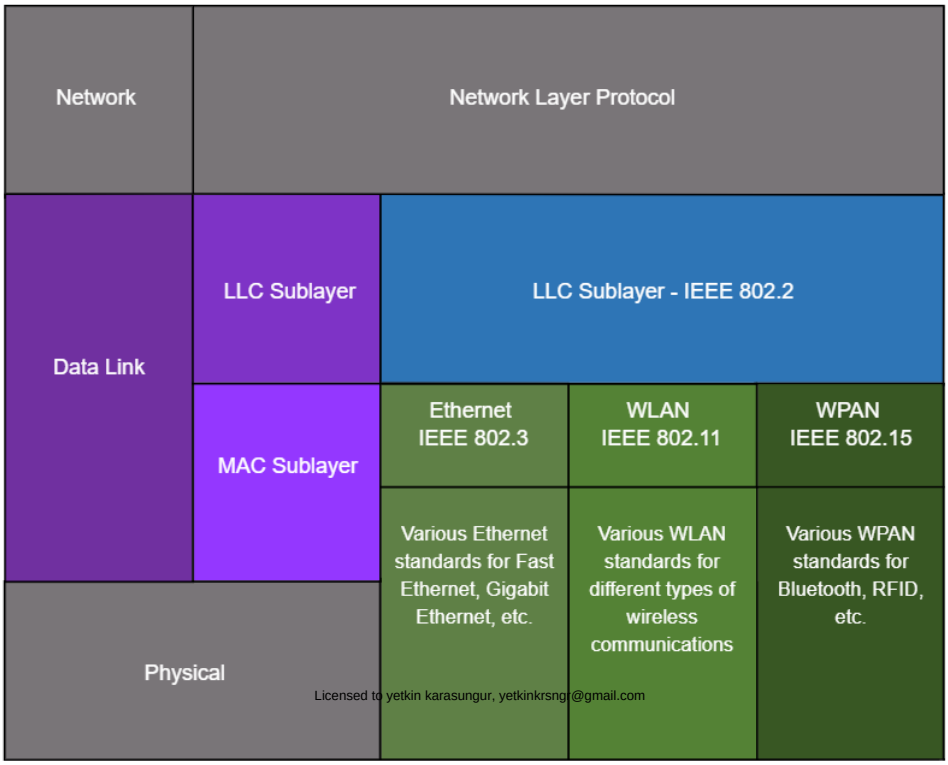

### 6.1.2.EEE 802 LAN / MAN Veri Bağlantısı Alt Katmanları

IEEE 802 LAN / MAN standartları ağ türüne (Ethernet, WLAN, WPAN, vb.) özeldir.

Veri Bağlantı Katmanı iki alt katmandan oluşur. Mantıksal Bağlantı Kontrolü-Logical Link Control (LLC) ve Medya Erişim Kontrolü-Media Access Control (MAC).

LLC alt katmanı, üst katmanlardaki ağ yazılımı ile alt katmanlardaki aygıt donanımı arasında iletişim kurar.

MAC alt katmanı, veri kapsülleme ve medya erişim kontrolünden sorumludur.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 6.1.3.Medyaya Erişim Sağlama

Düğümler arasında değiş tokuş edilen paketlerde çok sayıda veri bağlantısı katmanı ve ortam geçişi görülebilir.

Yol üzerindeki her sekmede, bir yönlendirici dört temel Katman 2 işlevi gerçekleştirir:

Ağ ortamından bir çerçeve kabul eder.

Kapsüllenmiş paketi ortaya çıkarmak için çerçeveyi kapsülden çıkarır.

Paketi yeni bir çerçeveye yeniden kapsüller.

Yeni çerçeveyi bir sonraki ağ segmentine iletir.

### 6.1.4.Veri Bağlantı Katmanı Standartları

Veri bağlantı katmanı protokolleri mühendislik kuruluşları tarafından tanımlanır:

- Institute for Electrical and Electronic Engineers (IEEE).
- International Telecommunications Union (ITU).
- International Organizations for Standardization (ISO).
- American National Standards Institute (ANSI).

## 6.2.Topolojiler

### 6.2.1.Physical and Logical Topologies-Fiziksel ve Mantıksal Topolojiler

Bir ağın topolojisi, ağ aygıtlarının ve aralarındaki bağlantıların düzenlenmesi ve ilişkisidir.

Ağları tanımlarken kullanılan iki tür topoloji vardır:

Physical topology – fiziksel bağlantıları ve cihazların nasıl birbirine bağlandığını gösterir.

Logical topology – aygıt arabirimleri ve IP adresleme şemalarını kullanan aygıtlar arasındaki sanal bağlantıları tanımlar.

### 6.2.2.WAN Topolojileri

**Üç yaygın fiziksel WAN topolojisi vardır:**

**Point-to-point** – en basit ve en yaygın WAN topolojisi. İki uç nokta arasındaki kalıcı bağlantıdan oluşur.

**Hub and spoke** – merkezi bir sitenin şubelerle noktadan noktaya bağlantı kurduğu yıldız topolojisine benzer.

**Mesh** – yüksek kullanılabilirlik sağlar ancak her uç sistemin diğer uç sistemlere bağlanmasını gerektirir.

### 6.2.3.LAN Topolojileri

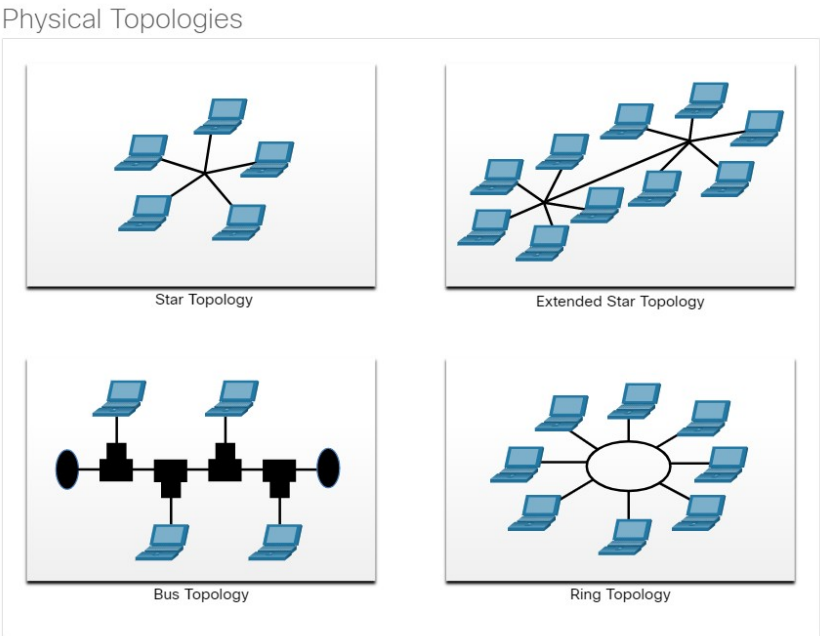
LAN'lardaki uç cihazlar genellikle bir yıldız veya genişletilmiş yıldız topolojisi kullanılarak birbirine bağlanır. Yıldız ve genişletilmiş yıldız topolojilerinin kurulumu kolaydır, iyi ölçeklendirilebilir ve sorun gidermesi kolaydır.

Erken Ethernet ve Eski Token Ring teknolojileri iki ek topoloji sağlar:

**Bus** – Tüm uç sistemler birlikte zincirlenir ve her iki uçta sonlandırılır.

**Ring** – Her uç sistem bir halka oluşturmak için kendi komşularına bağlanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 6.2.4.Half and Full Duplex Communication-Yarım ve Tam Çift Yönlü İletişim

### Half-duplex communication

Paylaşılan bir ortamda aynı anda yalnızca bir cihazın göndermesine veya almasına izin verir.

Ethernet hub'larına sahip eski veri yolu topolojilerinde ve WLAN'larda kullanılır.

### Full-duplex communication

Her iki cihazın da paylaşılan bir ortamda aynı anda iletim ve alma izni verir.

Ethernet anahtarları tam çift yönlü modda çalışır.

## 6.2.5.Access Control Methods-Erişim Kontrol Yöntemleri

### Contention-based access-Çekişme tabanlı erişim

Ortamın kullanımı için yarışan, yarı çift yönlü çalışan tüm düğümler. Örnekler:

Eski veri yolu topolojisi Ethernet'te kullanılan, çarpışma algılama-Carrier sense multiple access with collision detection (CSMA / CD) ile taşıyıcı algılamalı çoklu erişim.

Kablosuz LAN'larda kullanıldığı gibi, çarpışmadan kaçınma-Carrier sense multiple access with collision avoidance (CSMA / CA) ile taşıyıcı algılamalı çoklu erişim.

### Controlled access-Kontrollü erişim

Her bir düğümün ortam üzerinde kendi zamanı olduğu belirleyici erişim.

Token Ring ve ARCNET gibi eski ağlarda kullanılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 6.2.6.Contention-Based Access – CSMA/CD

**CSMA/CD**

- Eski Ethernet LAN'lar tarafından kullanılır.
- Bir seferde yalnızca bir aygıtın gönderdiği veya aldığı yarı çift yönlü modda çalışır.
- Bir cihazın ne zaman gönderebileceğini ve aynı anda birden fazla cihaz gönderilirse ne olacağını yönetmek için bir çarpışma algılama (collision detection) işlemi kullanır.

**CSMA/CD collision detection process**:

- Aynı anda iletim yapan cihazlar, paylaşılan ortamda sinyal çarpışmasına neden olur.
- Cihazlar çarpışmayı algılar.
- Aygıtlar rastgele bir süre bekler ve verileri yeniden iletir.

### 6.2.7.Contention-Based Access – CSMA/CA

**CSMA/CA**

- IEEE 802.11 WLAN'lar tarafından kullanılır.
- Bir seferde yalnızca bir aygıtın gönderdiği veya aldığı yarı çift yönlü modda çalışır.
- Bir cihazın ne zaman gönderebileceğini ve aynı anda birden fazla cihaz gönderilirse ne olacağını yönetmek için bir çarpışma önleme işlemi kullanır.

**CSMA/CA collision avoidance process**:

- İletim sırasında, cihazlar iletim için gereken süreyi de içerir.
- Paylaşılan ortamdaki diğer aygıtlar zaman süresi bilgilerini alır ve ortamın ne kadar süre kullanılamayacağını bilir.

## 6.3.Data Link Frame-Veri Bağlantı Çerçevesi

### 6.3.1.Frame-Çerçeve

**Veri, bir çerçeve oluşturmak için bir başlık ve bir artbilgi veri bağlantı katmanı tarafından kapsüllenir.**

Bir veri bağlantı çerçevesi üç bölümden oluşur:

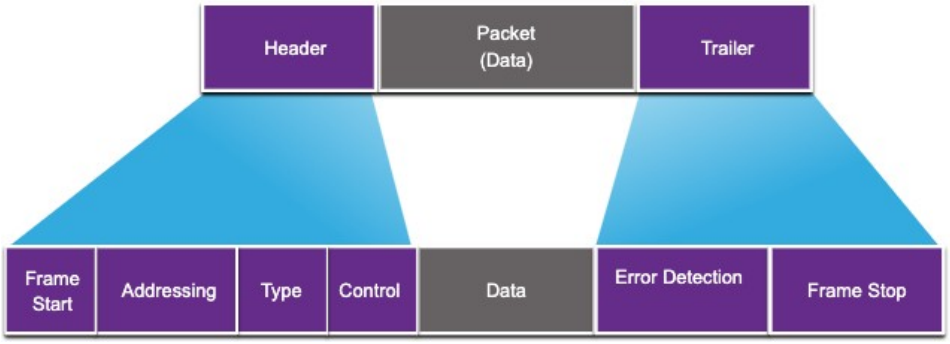
- Header-Başlık
- Data-Veri
- Trailer-Artbilgi

Üstbilgi ve artbilgi alanları veri bağlantı katmanı protokolüne göre değişir.

Çerçevede taşınan kontrol bilgisi miktarı erişim kontrol bilgisi ve mantıksal topolojiye göre değişir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

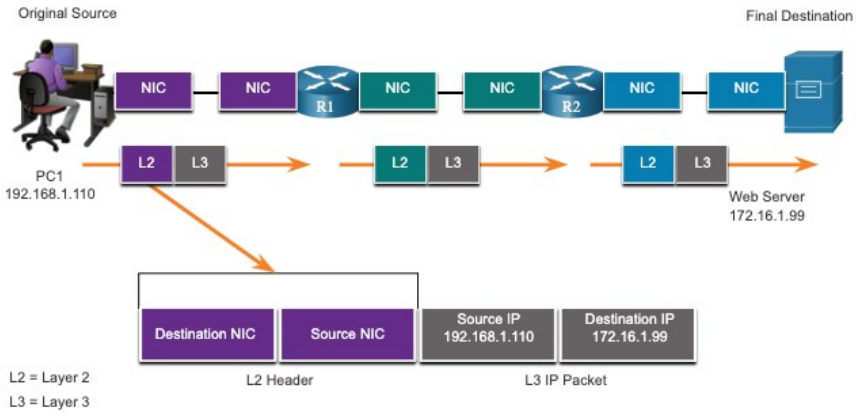
## 6.3.2.Frame Fields-Çerçeve Alanları




| Field-Alan | Description-Açıklama |
|---|---|
| Frame Start and Stop | Çerçevenin başlangıcını ve sonunu tanımlar |
| Addressing | Kaynak ve hedef düğümleri gösterir |
| Type | Kapsüllenmiş Katman 3 protokolünü tanımlar |
| Control | Akış kontrol hizmetlerini tanımlar |
| Data | Çerçeve taşıma yükünü içerir |
| Error Detection | İletim hatalarını belirlemek için kullanılır |

## 6.3.3.Layer 2 Addresses-Katman 2 Adresler

- Fiziksel adres olarak da bilinir.
- Çerçeve başlığında bulunur.
- Yalnızca bağlantıdaki bir çerçevenin yerel teslimi için kullanılır.
- Çerçeveyi ileten her cihaz tarafından güncellenir.




## 6.3.4.LAN and WAN Frames-LAN ve WAN Çerçeveleri

Mantıksal topoloji ve fiziksel medya kullanılan veri bağlantısı protokolünü belirler:

- Ethernet
- 802.11 Wireless
- Point-to-Point (PPP)
- High-Level Data Link Control (HDLC)
- Frame-Relay

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

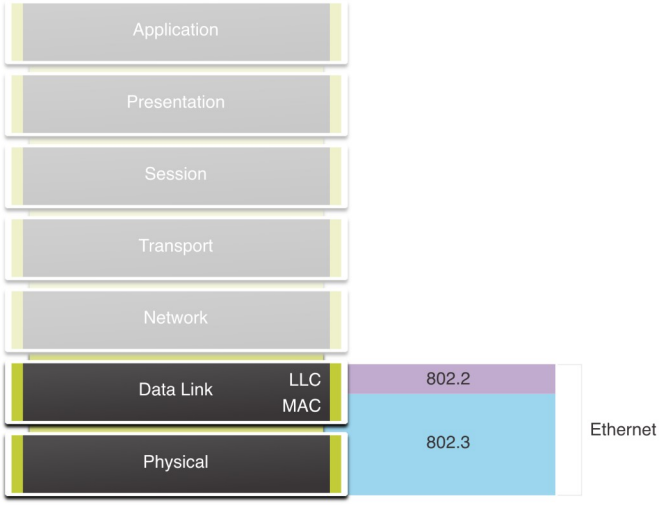
Her protokol, belirtilen mantıksal topolojiler için ortam erişim denetimi gerçekleştirir.

# 7.Bölüm: Ethernet Anahtarlama

## 7.1.Ethernet Frames-Ethernet Çerçeveleri

### 7.1.1.Ethernet Encapsulation-Ethernet Kapsülleme

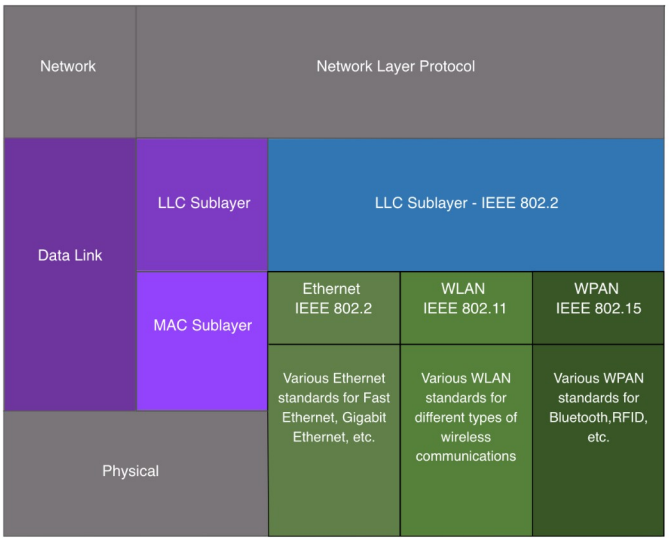
Ethernet, veri bağlantı katmanında ve fiziksel katmanda çalışır. IEEE 802.2 ve 802.3 standartlarında tanımlanan bir ağ teknolojileri ailesidir.




### 7.1.2.Data Link Sublayers-Veri Bağlantısı Alt Katmanları

Ethernet de dahil olmak üzere 802 LAN / MAN standartları, çalışmak için veri bağlantı katmanının iki ayrı alt katmanını kullanır:

- LLC Sublayer: (IEEE 802.2) Çerçeve için hangi ağ katmanı protokolünün kullanıldığını belirlemek için bilgileri çerçeveye yerleştirir.
- MAC Sublayer: (IEEE 802.3, 802.11, or 802.15) Veri kapsülleme ve medya erişim kontrolünden sorumludur ve veri bağlantı katmanı adresleme sağlar.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 7.1.2.1.MAC Sublayer

MAC alt katmanı, verilerin kapsüllenmesinden ve medyaya erişilmesinden sorumludur.

**Data Encapsulation**

IEEE 802.3 veri kapsüllemesi aşağıdakileri içerir:

- **Ethernet frame**- Bu, Ethernet çerçevesinin iç yapısıdır.
- **Ethernet Addressing**- Ethernet çerçevesi, Ethernet çerçevesini aynı LAN üzerinde Ethernet NIC'den Ethernet NIC'ye iletmek için hem kaynak hem de hedef MAC adresi içerir.
- **Ethernet Error detection**- Ethernet çerçevesi, hata tespiti için kullanılan bir çerçeve kontrol dizisi (FCS) artbilgi içerir.

**Medya Erişimi**

IEEE 802.3 MAC alt katmanı, bakır ve fiber de dahil olmak üzere çeşitli ortam türleri üzerinde farklı Ethernet iletişim standartları için özellikler içerir.

Bir veri yolu topolojisi veya hub kullanan eski Ethernet, paylaşılan, yarı çift yönlü bir ortamdır. Yarım dubleks ortam üzerindeki Ethernet, çekişmeli tabanlı erişim yöntemi, taşıyıcı algılamalı çoklu erişim / çarpışma algılama - carrier sense multiple access/collision detection (CSMA / CD) kullanır.

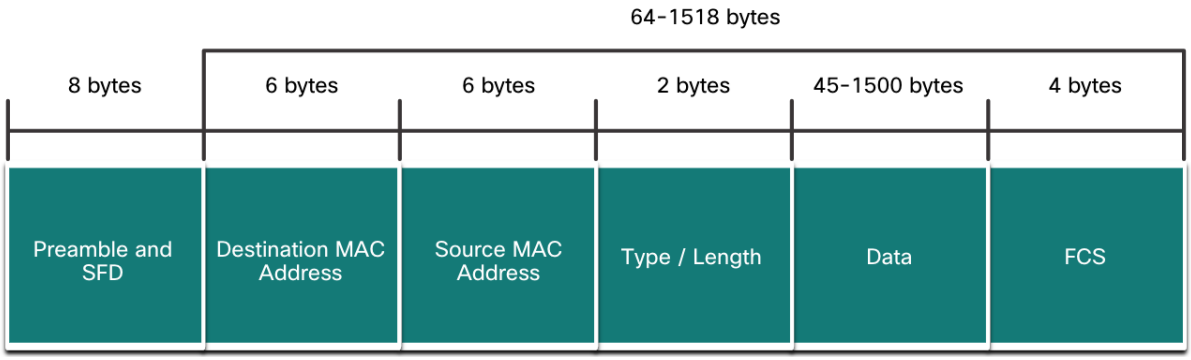
Günümüzün Ethernet LAN'larında tam çift yönlü çalışan anahtarlar kullanılır. Ethernet anahtarlarıyla tam çift yönlü iletişim için CSMA / CD aracılığıyla erişim kontrolü gerektirmez.

### 7.1.3.Ethernet Frame Fields-Ethernet Çerçeve Alanları

Minimum Ethernet çerçeve boyutu 64 bayt ve maksimum 1518 bayttır. Çerçevenin boyutu tanımlanırken giriş alanı dahil edilmez.

Uzunluğu 64 bayttan kısa olan çerçeveler “collision fragment -çarpışma parçası” veya “runt frame-kırpık çerçeve” olarak kabul edilir ve otomatik olarak atılır. 1500 bayttan fazla veri içeren kareler “jumbo” veya “baby giant frames-bebek dev çerçeveleri” olarak kabul edilir.

İletilen bir çerçevenin boyutu minimumdan küçük veya maksimumdan büyükse, alıcı cihaz çerçeveyi düşürür (drop). Düşen kareler, çarpışmaların veya diğer istenmeyen sinyallerin sonucu olabilir. Geçersiz sayılırlar. Jumbo çerçeveleri genellikle çoğu Fast Ethernet ve Gigabit Ethernet anahtarı ve NIC tarafından desteklenir.

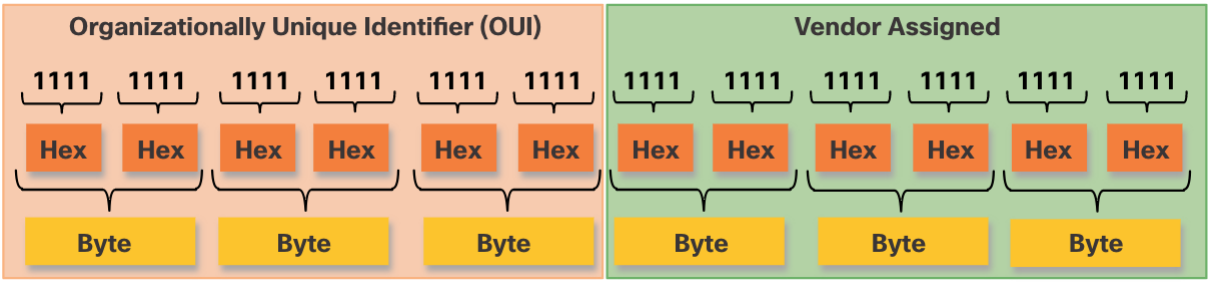



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 7.2.Ethernet MAC Address-Ethernet MAC Adresi

### 7.2.1.MAC Adresi ve Onaltılı Sayı Sistemi

- Ethernet MAC adresi, 12 onaltılık değer kullanılarak ifade edilen 48 bitlik bir ikili değerden oluşur.
- 8 bitin (bir bayt) ortak bir ikili gruplama olduğu göz önüne alındığında, ikili 00000000 ila 11111111, onaltılı olarak 00 ila FF aralığı olarak temsil edilebilir,
- Onaltılık kullanırken, 8 bitlik gösterimi tamamlamak için her zaman baştaki sıfırlar görüntülenir. Örneğin, 0000 1010 ikili değeri 0A olarak onaltılık olarak temsil edilir.
- Onaltılık sayılar, genellikle belgelerdeki ondalık ve onaltılık değerler arasında ayrım yapmak için 0x (örn., 0x73) öncesinde yer alan değerle temsil edilir.
- Onaltılık ayrıca bir alt simge 16 veya onaltılık sayı ve ardından bir H (örn., 73H) ile temsil edilebilir.
- Bir Ethernet LAN'da, her ağ cihazı aynı, paylaşılan ortama bağlanır. MAC adresleme, OSI modelinin veri bağlantı katmanında cihaz tanımlama için bir yöntem sağlar.
- Ethernet MAC adresi, 12 onaltılık basamak kullanılarak ifade edilen 48 bitlik bir adrestir. Bir bayt 8 bite eşit olduğundan, bir MAC adresinin 6 bayt uzunluğunda olduğunu da söyleyebiliriz.
- Tüm MAC adresleri Ethernet cihazına veya Ethernet arayüzüne özgü olmalıdır. Bunu sağlamak için, Ethernet aygıtları satan tüm satıcıların, kuruluşa özgü tanımlayıcı (OUI) adı verilen benzersiz bir 6 onaltılık (yani 24 bit veya 3 bayt) kod almaları için IEEE'ye kaydolmaları gerekir.
- Bir Ethernet MAC adresi, 6 onaltılık satıcı OUI kodunun ardından 6 onaltılık satıcı tarafından atanan bir değerden oluşur.




### 7.2.2.Çerçeve İşleme

Bir cihaz bir mesajı Ethernet ağına iletirken, Ethernet başlığında bir Kaynak MAC adresi ve bir Hedef MAC adresi bulunur.

Bir NIC bir Ethernet çerçevesi aldığında, hedef MAC adresini RAM'de depolanan fiziksel MAC adresiyle eşleşip eşleşmediğini kontrol eder. Eşleşme yoksa, cihaz çerçeveyi atar. Bir eşleşme varsa, çerçeveyi kapsülleme işleminin gerçekleştiği OSI katmanlarından geçirir.

**Not:**Hedef MAC adresi, ana bilgisayarın üyesi olduğu bir yayın veya çok noktaya yayın grubu ise Ethernet NIC'leri de çerçeveleri kabul eder.

Ethernet çerçevesinin kaynağı veya hedefi olan herhangi bir aygıtta Ethernet NIC ve dolayısıyla MAC adresi bulunur. Buna iş istasyonları, sunucular, yazıcılar, mobil cihazlar ve yönlendiriciler dahildir.

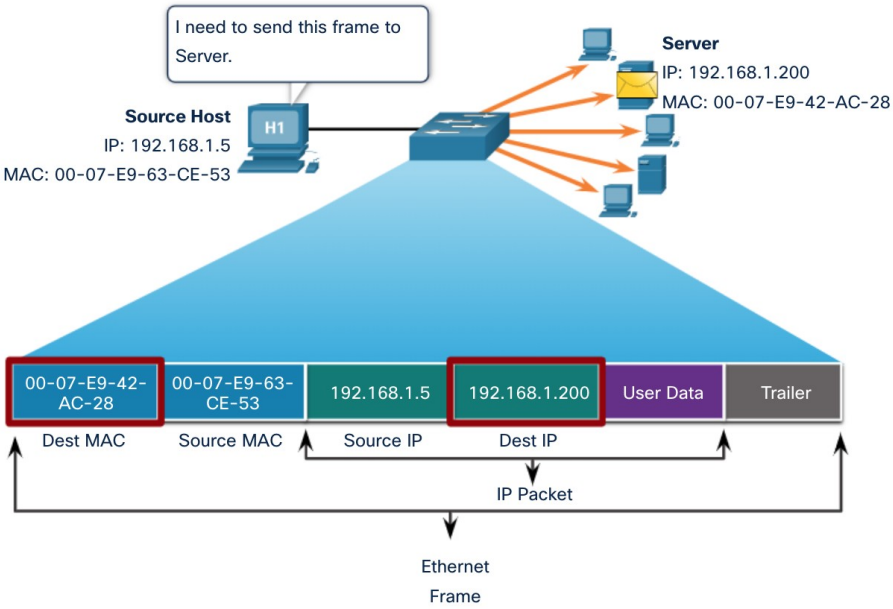
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 7.2.3.Unicast MAC Address-Tek Noktaya Yayın MAC Adresi

Ethernet'te, Katman 2 tek noktaya yayın, yayın ve çok noktaya yayın iletişimleri için farklı MAC adresleri kullanılır.

- Tek noktaya yayın MAC adresi, bir çerçeve tek bir verici aygıttan tek bir hedef aygıta gönderildiğinde kullanılan benzersiz adrestir.
- Bir kaynak ana bilgisayarın bir IPv4 adresiyle ilişkili hedef MAC adresini belirlemek için kullandığı işlem Adres Çözümleme Protokolü-Address Resolution Protocol (ARP) olarak bilinir. Bir kaynak ana bilgisayarın bir IPv6 adresiyle ilişkili hedef MAC adresini belirlemek için kullandığı işlem, Komşu Bulma-Neighbor Discovery (ND) olarak bilinir.

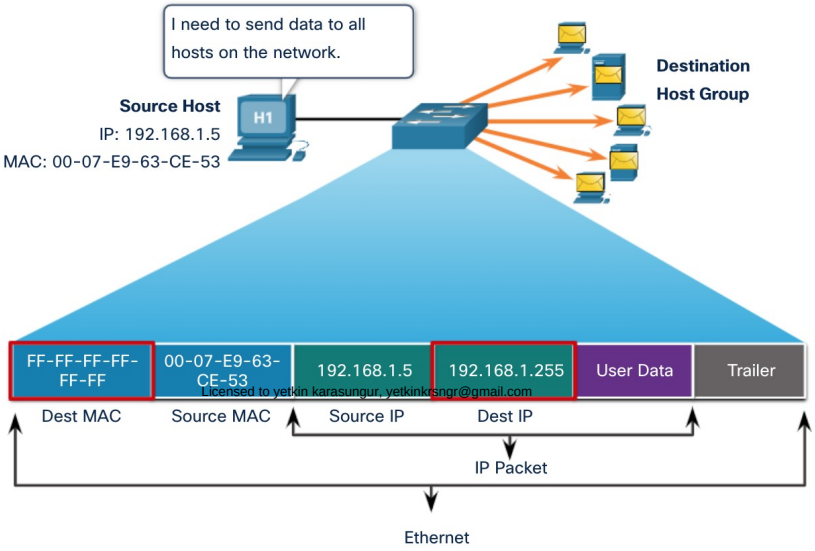
Not:Kaynak MAC adresi her zaman tek noktaya yayın adresi olmalıdır.




### 7.2.4.Broadcast MAC Address-Yayın MAC Adresi

Ethernet LAN'daki her aygıt tarafından bir Ethernet yayın çerçevesi alınır ve işlenir. Bir Ethernet yayınının özellikleri aşağıdaki gibidir:

- Onaltılık (FF-FF-FF-FF-FF-FF) hedef MAC adresi onaltılıktır (ikili formatta 48 adet 1).
- Gelen bağlantı noktası dışındaki tüm Ethernet anahtar bağlantı noktalarına iletilir. Bir yönlendirici tarafından iletilmez.
- Kapsüllenmiş veriler bir IPv4 yayın paketiyse, bu paketin ana bilgisayar bölümünde hepsinin (1'ler-255) bulunduğu bir hedef IPv4 adresi içerdiği anlamına gelir. Adresteki bu numaralandırma, o yerel ağdaki (yayın etki alanı) tüm ana bilgisayarların paketi alıp işleyeceği anlamına gelir.

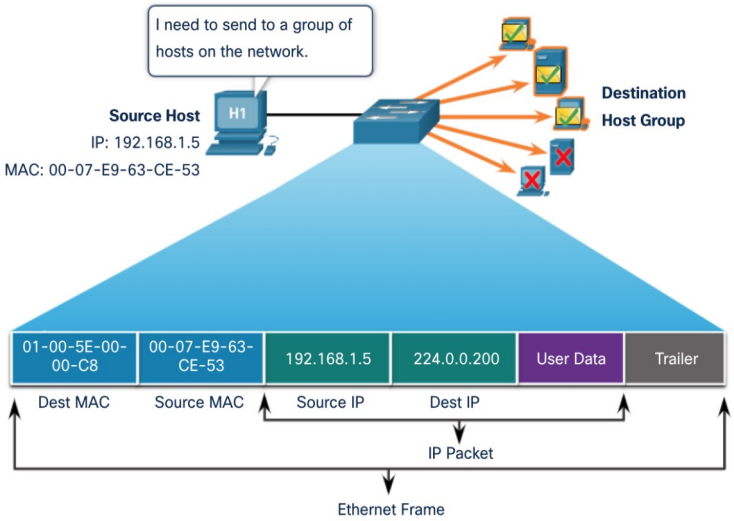



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 7.2.5.Multicast MAC Address-Çok Noktaya Yayın MAC Adresi

Bir Ethernet çok noktaya yayın çerçevesi, aynı çok noktaya yayın grubuna ait bir grup aygıt tarafından alınır ve işlenir.

- Kapsüllenmiş veriler bir IPv4 çok noktaya yayın paketi olduğunda 01-00-5E hedef MAC adresi ve kapsüllenmiş veriler bir IPv6 çok noktaya yayın paketi olduğunda 33-33 hedef MAC adresi vardır.
- Kapsüllenmiş verilerin IP olmadığı zaman için Yayılan Ağaç Protokolü (STP) gibi başka ayrılmış çok noktaya yayın hedef MAC adresleri vardır.
- Anahtar çok noktaya yayın gözetleme için yapılandırılmadığı sürece, gelen bağlantı noktası dışındaki tüm Ethernet anahtar bağlantı noktalarının altında kalmıştır. Yönlendirici çok noktaya yayın paketlerini yönlendirecek şekilde yapılandırılmadığı sürece bir yönlendirici tarafından iletilmez.
- Çok noktaya yayın adresleri bir adres grubunu temsil ettiğinden (bazen ana bilgisayar grubu da denir), bunlar yalnızca bir paketin hedefi olarak kullanılabilir. Kaynak her zaman tek noktaya yayın adresi olacaktır.
- Tek noktaya yayın ve yayın adreslerinde olduğu gibi, çok noktaya yayın IP adresi karşılık gelen bir çok noktaya yayın MAC adresi gerektirir.




## 7.3.The MAC Address Table-MAC Adres Tablosu

### 7.3.1.Switch Fundamentals-Anahtar Temelleri

Katman 2 Ethernet anahtarı, yönlendirme kararları vermek için Katman 2 MAC adreslerini kullanır. IPv4 paketi, ARP mesajı veya IPv6 ND paketi gibi çerçevenin veri bölümünde taşınan verilerin (protokolün) tamamen farkında değildir. Anahtar, yönlendirme kararlarını yalnızca Katman 2 Ethernet MAC adreslerine dayanarak alır.

Ethernet anahtarı, gelen bağlantı noktası dışındaki tüm bağlantı noktalarını bitleri yineleyen eski Ethernet hub'larının aksine her adres için bir yönlendirme kararı vermek üzere MAC adres tablosunu inceler.

Bir anahtar açıldığında MAC adres tablosu boştur.

Not: MAC adres tablosuna bazen içerik adreslenebilir bellek-content addressable memory (CAM) tablosu denir.

### 7.3.2.Switch Learning and Forwarding-Anahtar Öğrenme ve Yönlendirme

Examine the Source MAC Address (Learn)-Kaynak MAC Adresini İncele (Öğren)

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bir anahtara giren her çerçevede yeni bilgiler öğrenilir. Bunu çerçevenin kaynak MAC adresini ve çerçevenin anahtara girdiği bağlantı noktası numarasını inceleyerek yapar. Kaynak MAC adresi tabloda yoksa, gelen bağlantı

noktası numarasıyla birlikte tabloya eklenir. Kaynak MAC adresi varsa, anahtar o giriş için yenileme zamanlayıcısını günceller. Varsayılan olarak, Ethernet anahtarlarının çoğu tabloda bir girişi 5 dakika (300 sn) tutar.

**Not**: Kaynak MAC adresi tabloda ancak farklı bir bağlantı noktasında varsa, anahtar bunu yeni bir giriş olarak kabul eder. Giriş aynı MAC adresi kullanılarak ancak daha güncel bağlantı noktası numarasıyla değiştirilir.

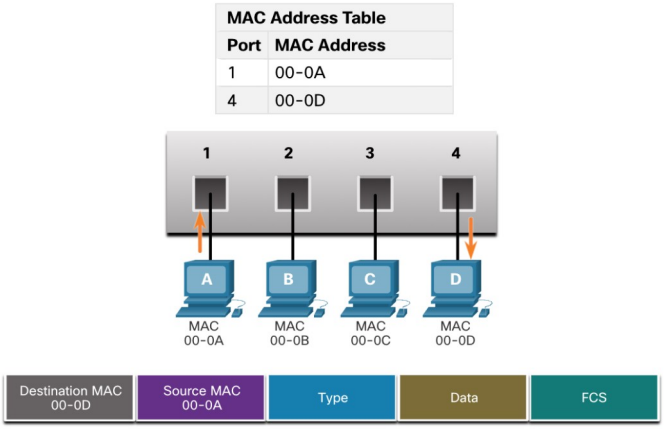
**Find the Destination MAC Address-Hedef MAC Adresini Bulun (Forward)**

Hedef MAC adresi tek noktaya yayın adresiyse, anahtar çerçevenin hedef MAC adresi ile MAC adres tablosundaki bir giriş arasında bir eşleşme arar. Hedef MAC adresi tabloda ise, çerçeveyi belirtilen bağlantı noktasından iletir. Hedef MAC adresi tabloda yoksa, anahtar çerçeveyi gelen bağlantı noktası dışındaki tüm bağlantı noktalarından iletir. Buna bilinmeyen tek noktaya yayın denir.

**Not**: Hedef MAC adresi bir yayın veya çok noktaya yayınsa, çerçeve gelen bağlantı noktası dışındaki tüm bağlantı noktalarına da taşmış olur.

### 7.3.3.Filtering Frames- Çerçeveleri Filtreleme

Bir anahtar farklı aygıtlardan çerçeveler aldığından, her çerçevenin kaynak MAC adresini inceleyerek MAC adres tablosunu doldurabilir. Anahtarın MAC adres tablosu hedef MAC adresini içeriyorsa, çerçeveyi filtreleyip tek bir bağlantı noktasını iletebilir.




## 7.4.Switch Speeds and Forwarding Methods-Anahtar Hızları ve Yönlendirme Yöntemleri

### 7.4.1.Cisco Anahtarlarında Çerçeve Yönlendirme Yöntemleri

Anahtarlar, ağ bağlantı noktaları arasında veri geçişi için aşağıdaki yönlendirme yöntemlerinden birini kullanır:

**Store-and-forward switching-Depola ve ilet anahtarlama**- Bu çerçeve yönlendirme yöntemi tüm çerçeveyi alır ve CRC'yi hesaplar. CRC geçerliyse, anahtar giden arabirimi belirleyen hedef adresi arar. Ardından çerçeve doğru bağlantı noktasından iletilir.

**Cut-through switching-Çapraz kesimli anahtarlama**- Bu çerçeve yönlendirme yöntemi, çerçeveyi tamamen alınmadan önce iletir. Çerçevenin iletilebilmesi için en azından çerçevenin hedef adresi okunmalıdır.

Deopla ve ilet anahtarlamasının büyük bir avantajı, bir çerçevi yaymadan önce hatalar olup olmadığını belirlemesidir. Bir çerçevede bir hata algılandığında, anahtar çerçeveyi atar. Çerçeveleri hatalı olarak atmak, bozuk veriler tarafından tüketilen bant genişliği miktarını azaltır.

Trafik önceliklendirmesi için çerçeve sınıflandırmasının gerekli olduğu yakınsak ağlarda hizmet kalitesi (QoS) analizi için depola ve ileri anahtarlama gereklidir. Örneğin, IP üzerinden ses (VoIP) veri akışlarının web tarama trafiğine göre önceliği olmalıdır.

Bilgisayar Ağları Kurumsal Ağ Tasarımı ve Yönetimi Uygulamaları

### 7.4.1.1.Cut-Through Switching-Çapraz Kesimli Anahtarlama

Çapraz kesimli anahtarlamasında, aktarım tamamlanmamış olsa bile, anahtar alındığı anda verilere etki eder. Anahtar, hedef MAC adresini okumak için yeterli çerçeveyi tamponlar, böylece verileri hangi bağlantı noktasına iletmesi gerektiğini belirleyebilir. Anahtar, çerçeve üzerinde herhangi bir hata kontrolü gerçekleştirmez.

Çapraz kesimli anahtarlamanın iki çeşidi vardır:

**Fast-forward switching-Hızlı İleri Anahtarlama** -Hedef adresi okuduktan sonra bir paketi hemen ileterek en düşük gecikme seviyesini sunar. Hızlı ileri anahtarlama, tüm paket alınmadan iletilmeye başladığı için, paketlerin hatalı olarak geçirildiği zamanlar olabilir. Hedef NIC, teslim alındıktan sonra hatalı paketi atar. Hızlı ileri anahtarlama, tipik anahtarlama yöntemidir.

**Fragment-free switching-Parçasız anahtarlama** -Depola ve ilet anahtarının yüksek gecikmesi ve yüksek bütünlüğü ile hızlı iletme anahtarının düşük gecikmesi ve azaltılmış bütünlüğü arasındaki bir uzlaşma, anahtar iletmeden önce çerçevenin ilk 64 baytında bir hata denetimi depolar ve gerçekleştirir. Çoğu ağ hatası ve çarpışma ilk 64 bayt sırasında oluştuğu için, çerçeveyi iletmeden önce bir çakışma oluşmaz.

### 7.4.2.Duplex and Speed Settings-Çift Taraflı ve Hız Ayarları

Bir anahtardaki en temel ayarlardan ikisi, her bir ayrı ayrı bağlantı noktası için bant genişliği ("hız") ve çift yönlü(duplex) ayarlarıdır. Çift yönlü ve bant genişliği ayarlarının anahtar bağlantı noktası ile bağlı aygıtlar arasında eşleşmesi önemlidir.

Ethernet ağında iletişim için kullanılan iki tür dubleks ayarı vardır:

**Full-duplex**- Bağlantının her iki ucu aynı anda gönderebilir ve alabilir.

**Half-duplex**- Aynı anda yalnızca bağlantının bir ucu veri gönderilebilir.

Autonegotiation-Otomatik anlaşma, çoğu Ethernet anahtarı ve NIC'de bulunan isteğe bağlı bir işlevdir. İki cihazın otomatik olarak en iyi hız ve dupleks özelliklerini görüşmesini sağlar.

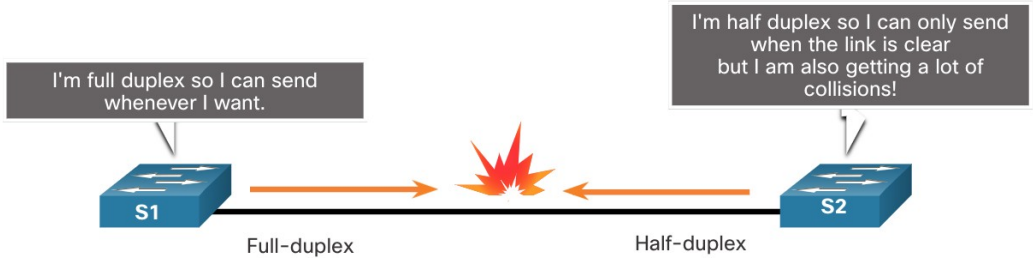
**Not**: Gigabit Ethernet bağlantı noktaları yalnızca tam çift yönlü (full-duplex) olarak çalışır.

### 7.4.3.Duplex and Speed Settings

Duplex mismatch-Çift yönlü uyumsuzluk, 10/100 Mbps Ethernet bağlantılarındaki performans sorunlarının en yaygın nedenlerinden biridir. Bağlantıdaki bir bağlantı noktası yarı çift yönlü çalışırken, diğer bağlantı noktası tam çift yönlü çalışırken çalışır.

Bu, bir bağlantıdaki bir veya her iki bağlantı noktası sıfırlandığında ve otomatik anlaşma işlemi her iki bağlantı ortağının da aynı yapılandırmaya sahip olmasıyla sonuçlanmaz.

Kullanıcılar bir bağlantının bir tarafını yeniden yapılandırıp diğerini yeniden yapılandırmayı unuttuğunda da ortaya çıkabilir. Bir bağlantının her iki tarafında otomatik anlaşma var veya iki tarafında da kapalı olmalıdır. En iyi uygulama, her iki Ethernet anahtar bağlantı noktasını tam çift yönlü olarak yapılandırmaktır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 7.4.4.Auto-MDIX

Cihazlar arasındaki bağlantılar bir zamanlar çapraz veya düz kablo kullanılmasını gerektiriyordu. Gereken kablo tipi, birbirine bağlanan cihazların tipine bağlıdır.

**Not**:Yönlendirici ve ana bilgisayar arasındaki doğrudan bağlantı, çapraz bağlantı gerektirir.

Çoğu anahtar aygıt artık otomatik orta bağımlı arabirim geçişi (auto-MDIX-medium dependent interface crossover ) özelliğini desteklemektedir. Etkinleştirildiğinde, anahtar bağlantı noktasına takılı kablonun türünü otomatik olarak algılar ve arayüzleri buna göre yapılandırır.

Otomatik MDIX özelliği, Cisco IOS Sürüm 12.2 (18) SE veya daha yenisini çalıştıran anahtarlarda varsayılan olarak etkindir. Ancak, özellik devre dışı bırakılabilir. Bu nedenle, her zaman doğru kablo türünü kullanmalısınız ve auto-MDIX özelliğine güvenmemelisiniz.

Auto-MDIX, mdix otomatik arabirim yapılandırma komutu kullanılarak yeniden etkinleştirilebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 8.Bölüm: Ağ Katmanı

## 8.1.Ağ Katmanı Özellikleri

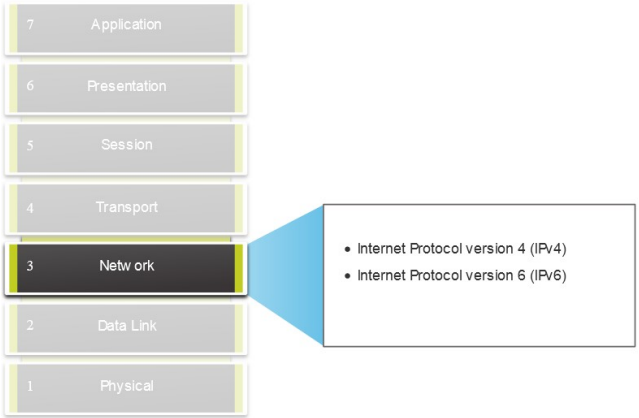
### 8.1.1.Ağ Katmanı

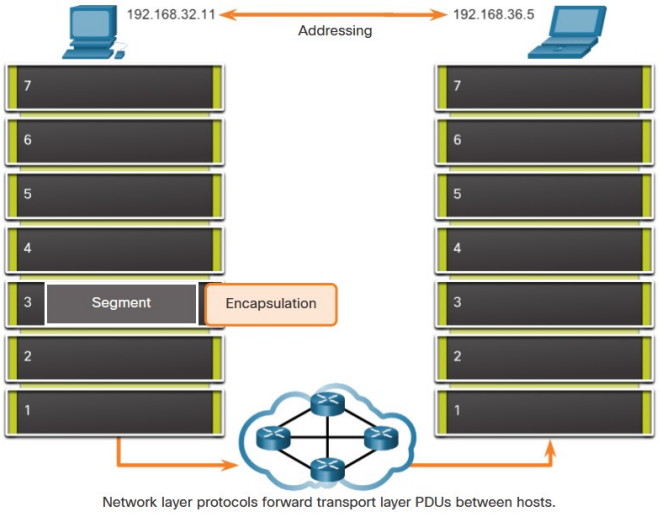
Uç cihazların (host) veri alışverişine izin veren hizmetler sunar

IP sürüm 4 (IPv4) ve IP sürüm 6 (IPv6), temel ağ katmanı iletişim protokolleridir.

Ağ katmanı dört temel işlem gerçekleştirir:

- Addressing end devices-Uç Cihazların Adreslenmesi
- Encapsulation-Kapsülleme
- Routing-Yönlendirme
- De-encapsulation-Kapsül Açma

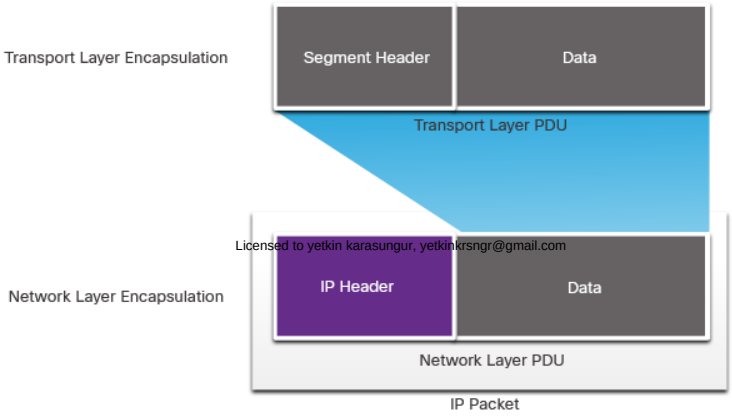



### 8.1.2.IP Encapsulation- IP Kapsülleme

- IP, taşıma katmanı segmentini  kapsüller (içine alır).
- IP, IPv4 veya IPv6 paketi kullanabilir ve katman 4 segmentini etkilemez.
- IP paketi ağ üzerinden geçerken tüm katman 3 cihazları tarafından incelenecektir.
- IP adresleme, kaynaktan hedefe değişmez.

  Not: NAT adreslemeyi değiştir ancak daha sonraki bir modülde açıklanacaktır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 8.1.3.IP'nin Özellikleri

IP'nin düşük ek yüke sahip olması amaçlanmıştır ve şu şekilde tanımlanmıştır:

- Connectionless-Bağlantısız
- Best Effort-En İyi Çaba
- Media Independent-Medyadan Bağımsız

### 8.1.3.1.Connectionless

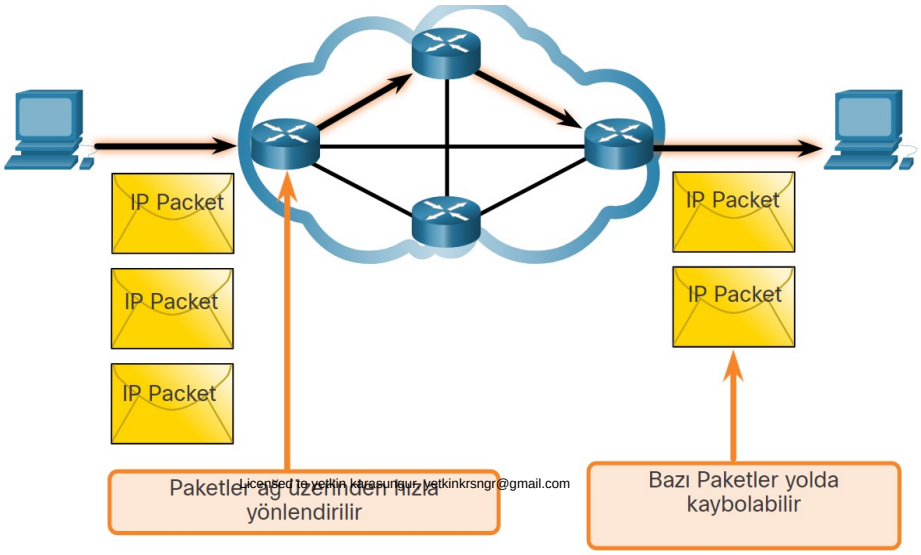
IP Bağlantısızdır

- IP, paketi göndermeden önce hedefle bağlantı kurmaz.
- Hiçbir kontrol bilgisi gerekmez (senkronizasyonlar, alındı bildirimleri, vb.).
- Hedef, paket geldiğinde alacaktır, ancak IP tarafından hiçbir ön bildirim gönderilmez.
- Bağlantıya yönelik trafiğe ihtiyaç varsa, başka bir protokol bunu ele alır (genellikle taşıma katmanındaki TCP).

### 8.1.3.2.Best Effort

IP is Best Effort- IP En İyi Çaba Gösterir

- IP, paketin teslimini garanti etmez.
- Alınmayan verileri yeniden göndermek için bir mekanizma olmadığından IP ek yükü azaltmıştır.
- IP onay beklemez.
- IP, diğer cihazın çalışır durumda olup olmadığını veya paketi alıp almadığını bilmez.




Licensed to yetkin kerasundur yetkinkrsngr@gmail.com

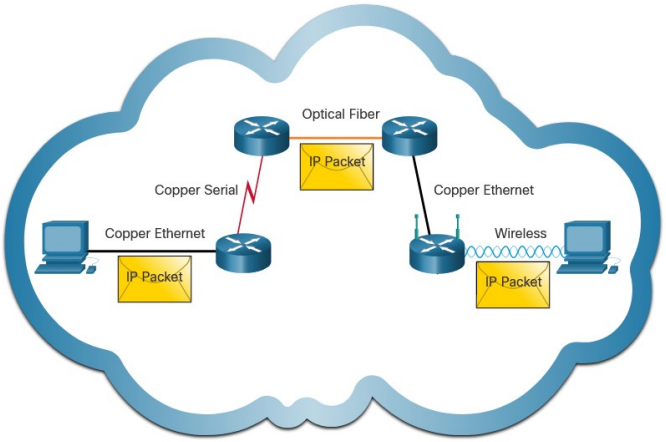
### 8.1.3.3.Media Independent

IP güvenilir değil:

- Teslim edilemeyen veya bozuk paketleri yönetemez veya düzeltemez.
- Bir hatadan sonra IP yeniden iletilemiyor.
- IP, paketleri  yeniden sıralayamıyor.
- IP, bu işlevler için diğer protokollere güvenmelidir. (TCP)

IP medyadan bağımsızdır:

- IP, veri bağlantı katmanında gerekli olan çerçeve türüyle veya fiziksel katmandaki ortam türüyle ilgilenmez.
- IP, herhangi bir ortam türü üzerinden gönderilebilir: bakır, fiber veya kablosuz.




Ağ katmanı, Maksimum İletim Birimi'ni-Maximum Transmission Unit (MTU) kuracaktır.

- Ağ katmanı bunu veri bağlantı katmanı tarafından gönderilen kontrol bilgilerinden alır.
- Ağ daha sonra MTU boyutunu belirler.

Parçalanma, Katman 3'ün IPv4 paketini daha küçük birimlere bölmesidir.

- Parçalanma gecikmeye neden olur.
- IPv6 paketleri parçalamaz.

Örnek: Yönlendirici Ethernet'ten daha küçük bir MTU ile yavaş bir WAN'a gider

## 8.2.IPv4 Packet(Datagram)-IPv4 Paketi

### 8.2.1.IPv4 Packet Header-IPv4 Paket Başlığı

IPv4, ağ katma8nı için birincil iletişim protokolüdür.

Ağ başlığının birçok amacı vardır:

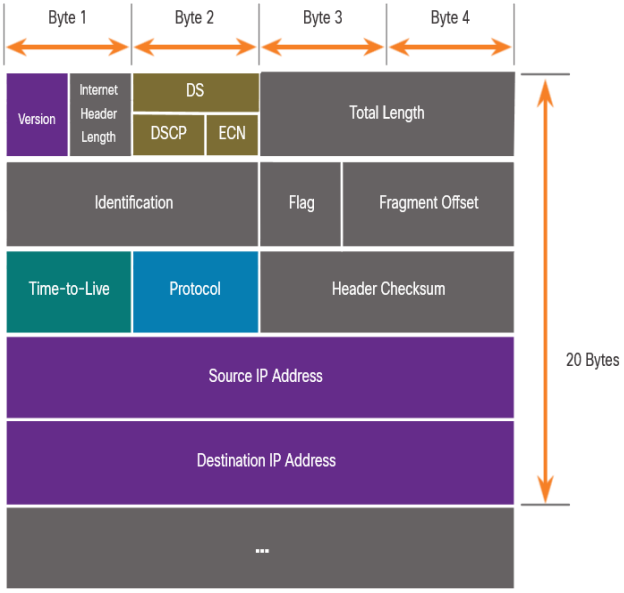
Paketin doğru yönde (varış yerine) gönderilmesini sağlar.

Çeşitli alanlarda ağ katmanı işlemesi için bilgiler içerir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Üstbilgideki bilgiler, paketi işleyen tüm katman 3 aygıtları tarafından kullanılır

### 8.2.2.IPv4 Paket Başlık (Üstbilgisi-Header) Alanları




IPv4 ağ başlığı özellikleri:

- Ikili olarak gösterilir.
- Çeşitli bilgi alanları içerir
- Diyagram soldan sağa, satır başına 4 bayt okunur
- En önemli iki alan kaynak ve hedeftir (IP adresi).

Protokollerin bir veya daha fazla işlevi olabilir.

**IPv4 başlığındaki önemli alanlar:**

| Function | Description |
|---|---|
| **Version** | IPv4 için 4 bit = 0100 |
| **Differentiated Services** | QoS: DiffServ - DS alanı veya daha eski IntServ - ToS veya Hizmet Türü-Type of Service için kullanılır |
| **Header Checksum** | IPv4 üstbilgisindeki bozulmayı algılama |
| **Time to Live (TTL)** | Katman 3 sekme sayımı. Sıfır olduğunda, yönlendirici paketi atar. |
| **Protocol** | Kimlik sonraki seviye protokolü: ICMP, TCP, UDP, vb. |
| **Source IPv4 Address** | 32 bit source address |
| **Destination IPV4 Address** | 32 bit destination address |

## 8.3.IPv6 Paketi

### 8.3.1.Limitations of IPv4-IPv4'ün Sınırlamaları

IPv4'ün üç temel sınırlaması vardır:

- IPv4 adresinin tükenmesi - Temel olarak IPv4 adreslememiz bitti.
- Uçtan uca bağlantı eksikliği - IPv4'ün bu kadar uzun süre dayanmasını sağlamak için özel adresleme ve NAT oluşturuldu. Bu, genel seslendirme ile doğrudan iletişimi sona erdirdi.
- Artan ağ karmaşıklığı - NAT geçici çözüm anlamına geliyordu ve ağ üstbilgileri adreslemesini değiştirmenin bir yan etkisi olarak ağ üzerinde sorunlar yaratıyor. NAT gecikme ve sorun giderme sorunlarına neden olur.

**IPv6,** İnternet Mühendisliği Görev Gücü (IETF) tarafından geliştirilmiştir.

IPv6, IPv4'ün sınırlamalarının üstesinden gelir.

IPv6'nın sağladığı iyileştirmeler:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

- **Daha fazla adres alanı** – 128 bit adres alanı 340 andesilyon IP adresi sağlar.
- **Gelişmiş paket kullanımı** – daha az alana sahip basitleştirilmiş başlık

- **NAT ihtiyacını ortadan kaldırır** – çok fazla adresleme olduğundan, özel adreslemeyi dahili olarak kullanmaya ve paylaşılan bir genel adresle eşleştirilmesine gerek yoktur

IPv4 and IPv6 Address Space Comparison

| Number Name | Scientific Notation | Number of Zeros |
|---|---|---|
| 1 Thousand | 10^3 | 1,000 |
| 1 Million | 10^6 | 1,000,000 |
| 1 Billion | 10^9 | 1,000,000,000 |
| 1 Trillion | 10^12 | 1,000,000,000,000 |
| 1 Quadrillion | 10^15 | 1,000,000,000,000,000 |
| 1 Quintillion | 10^18 | 1,000,000,000,000,000,000 |
| 1 Sextillion | 10^21 | 1,000,000,000,000,000,000,000 |
| 1 Septillion | 10^24 | 1,000,000,000,000,000,000,000,000 |
| 1 Octillion | 10^27 | 1,000,000,000,000,000,000,000,000,000 |
| 1 Nonillion | 10^30 | 1,000,000,000,000,000,000,000,000,000,000 |
| 1 Decillion | 10^33 | 1,000,000,000,000,000,000,000,000,000,000,000 |
| 1 Undecillion | 10^36 | 1,000,000,000,000,000,000,000,000,000,000,000,000 |

Legend
There are 4 billion IPv4 addresses
There are 340 undecillion IPv6 addresses

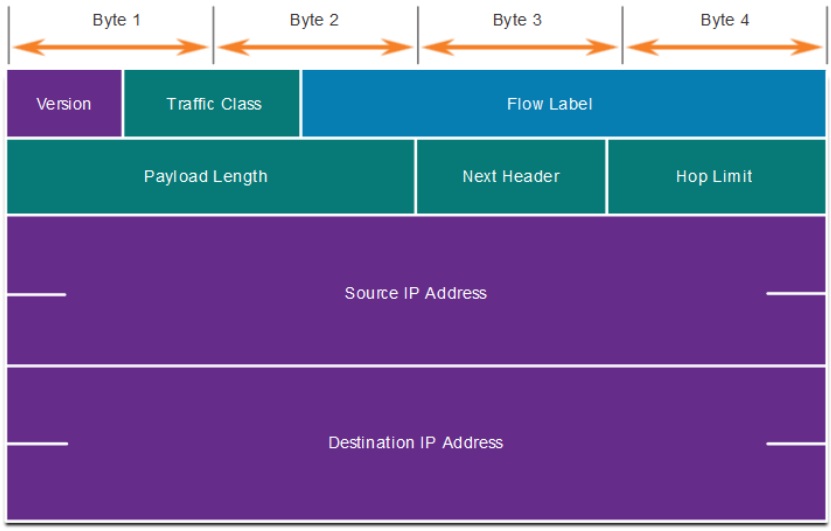
## 8.3.2.IPv6 Paket Başlığındaki Alanlar

IPv6 başlığı basitleştirilmiştir, ancak daha küçük değildir.

Başlık 40 Bayt veya sekizli uzunluğunda sabitlenmiştir.

Performansı artırmak için bazı IPv4 alanları kaldırıldı:

- Flag
- Fragment Offset
- Header Checksum




**Mor aynı kalan alanlar, yeşil adı değişen alanlar, mavi yeni eklenen alanlar.**

**IPv6 başlığındaki önemli alanlar:**

| Function | Description |
|---|---|
| **Version** | Ipv6 için 4 bit = 0110 |
| **Traffic Class** | QoS için kullanılır: DiffServ - DS alanına eşdeğerdir |
| **Flow Label** | Cihazı aynı akış etiketlerini aynı şekilde işlemesi için bilgilendirir, 20 bit alan |
| **Payload Length** | Bu 16 bit alan, IPv6 paketinin veri bölümünün uzunluğunu veya yükünü gösterir |
| **Next Header** | Kimlik sonraki seviye protokolü: ICMP, TCP, UDP, vb. |
| **Hop Limit** | Ipv4teki TTL alanı  Katman3 atlama sayısı |
| **Source IPv4 Address** | 128 bit source address |
| **Destination IPV4 Address** | 128 bit destination address |

**Not:** IPv4'ün aksine, yönlendiriciler IPv6 paketlerini parçalamaz.

## 8.4.HOST ROTALARI

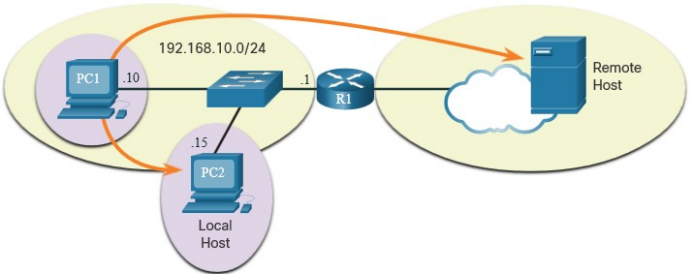
### 8.4.1.Host Yönlendirme Kararı

Paketler her zaman kaynağında oluşturulur.

Her ana cihaz  kendi yönlendirme tablosunu oluşturur.

Bir ana bilgisayar aşağıdakilere paket gönderebilir:

- Kendisi – 127.0.0.1 (IPv4), ::1 (Ipv6)
- Local Hosts –hedef aynı LAN'da
- Remote Hosts – cihazlar aynı LAN'da değil




Kaynak aygıt, hedefin yerel mi yoksa uzak mı olduğunu belirler

Belirleme yöntemi:

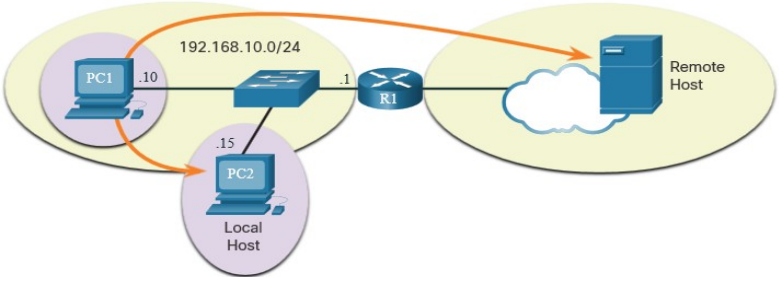
IPv4 – Kaynak, hedef IP adresiyle birlikte kendi IP adresini ve Alt ağ maskesini kullanır

IPv6 – Kaynak, yerel yönlendirici tarafından bildirilen ağ adresini ve ön ekini kullanır

Yerel trafik, bir ara aygıt tarafından işlenecek ana bilgisayar arabirimine dökülür.

Uzak trafik doğrudan LAN üzerindeki varsayılan ağ geçidine yönlendirilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 8.4.2.Default Gateway-Varsayılan Ağ Geçidi

Bir yönlendirici veya katman 3 anahtarı varsayılan bir ağ geçidi olabilir.

Varsayılan ağ geçidinin (DGW) özellikleri:

- LAN'ın geri kalanıyla aynı aralıkta bir IP adresine sahip olmalıdır.
- LAN'dan veri kabul edebilir ve LAN'dan trafiği iletebilir.
- Diğer ağlara yönlendirebilir.

Bir aygıtta varsayılan ağ geçidi veya hatalı bir varsayılan ağ geçidi yoksa, trafik LAN'dan ayrılamaz.

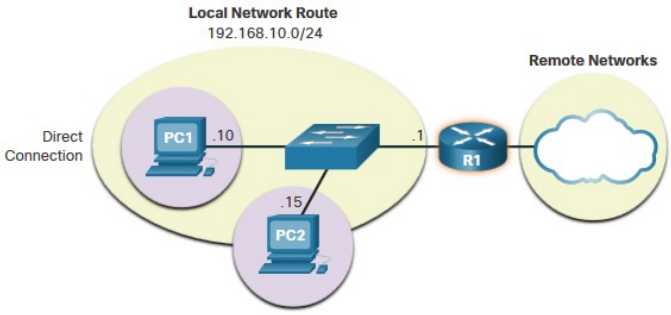
### 8.4.2.1.A Host Routes to the Default Gateway-Varsayılan Ağ Geçidi Host Rotaları

Ana makine (host) varsayılan ağ geçidini (DGW) statik olarak veya IPv4'teki DHCP aracılığıyla bilecektir.

IPv6, DGW'yi bir yönlendirici istemi (RS) aracılığıyla gönderir veya manuel olarak yapılandırılabilir.

DGW, yönlendirme tablosundaki son çare güzergahı olacak statik yoldur.

Uzaktaki ağlara trafik göndermek istiyorsa, LAN üzerindeki tüm cihazların yönlendiricinin DGW'sine ihtiyacı olacaktır.




### 8.4.2.2.Host Routing Tables

Windows'ta PC yönlendirme tablosunu görüntülemek için netstat -r komutunu kullanın

Bu iki komut tarafından görüntülenen üç bölüm:

Interface List – Tüm arayüzler ve MAC adresleri

IPv4 Routing Table

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

IPv6 Routing Table

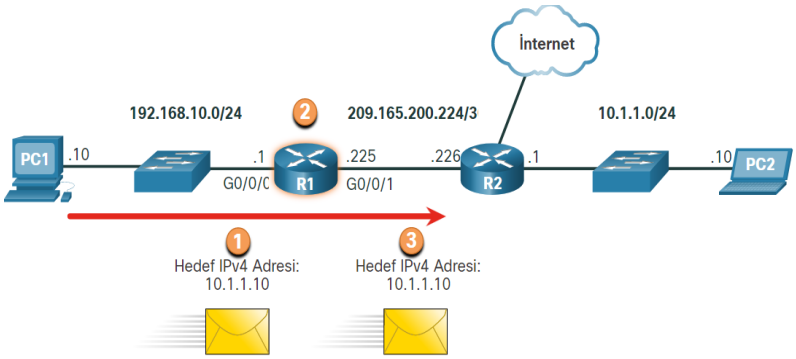
IPv4 Routing Table for PC1

```
C:\Users\PC1> netstat -r

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.10.1  192.168.10.10      25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     306
      192.168.10.0    255.255.255.0         On-link    192.168.10.10     281
    192.168.10.10  255.255.255.255         On-link    192.168.10.10     281
   192.168.10.255  255.255.255.255         On-link    192.168.10.10     281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1     306
        224.0.0.0        240.0.0.0         On-link    192.168.10.10     281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1     306
  255.255.255.255  255.255.255.255         On-link    192.168.10.10     281
```

## 8.5.Yönlendirmeye Giriş

### 8.5.1.Yönlendirici Paket Yönlendirme Kararı

Yönlendirici çerçeveyi(frame) ana cihazdan (host) aldığında ne olur?




R1 Routing Table

| Route | Next Hop or Exit Interface |
|---|---|
| 192.168.10.0 /24 | G0/0/0 |
| 209.165.200.224/30 | G0/0/1 |
| **10.1.1.0/24** | **via R2** |
| Default Route 0.0.0.0/0 | via R2 |

1. Paket, R1 yönlendiricisinin Gigabit Ethernet 0/0/0 arabirimine gelir. R1 katmab 2 ethernet başlığını kapsülden çıkarır.
2. R1, paketin hedef IPv4 adresini inceler ve IPv4 yönlendirme tabslosunda en iyi eşleşmeyi arar. Rota girişi bu paketin R2 yönlendiricisine iletileceğini gösterir.
3. R1 paketi yeni bir ethernet başlığı ( kullanılan WAN protokolüne göre değişir) içine kapsüller ve R2'ye iletir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 8.5.2.IP Router Routing Table-IP Yönlendirici Yönlendirme Tablosu

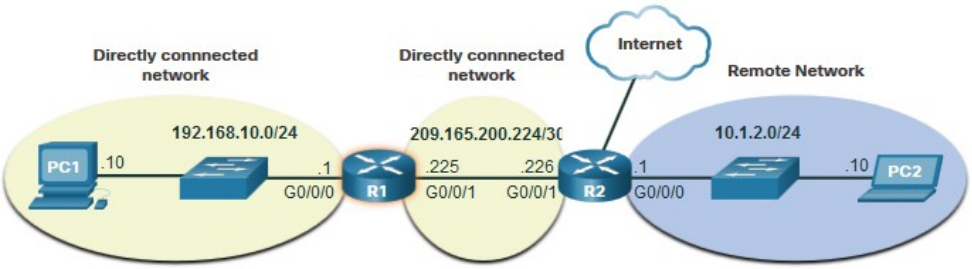
Yönlendirme tablosu üç tür rota girişi depolar:

**Directly Connected-Doğrudan bağlı ağlar** – Arabirimin etkin olması ve adreslemesinin olması koşuluyla, bu yollar yönlendirici tarafından otomatik olarak eklenir.

**Remote** – Yönlendiricinin doğrudan bağlantısı olmayan ve öğrenilebilecek yollar şunlardır:

- Manually-Manüel olarak – Statik rota ile
- Dynamically-Dimanik(otomatik) – yönlendiricilerin bilgilerini birbirleriyle paylaşmasını sağlamak için bir yönlendirme protokolü kullanarak

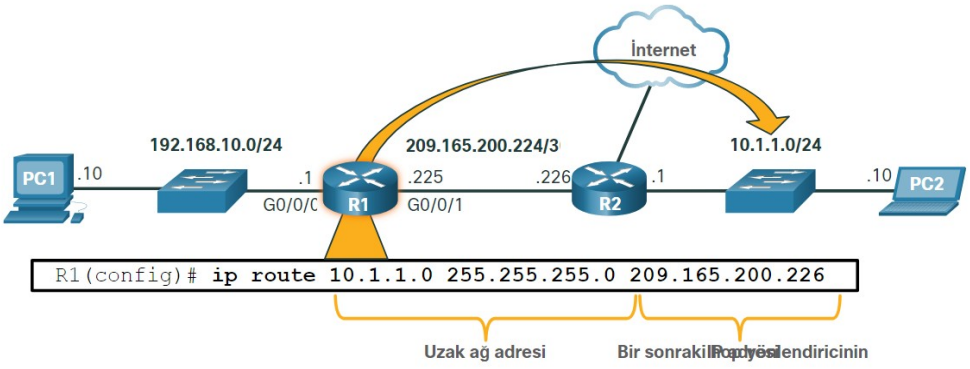
**Default Route-Varsayılan Rota** – bu, yönlendirme tablosunda bir eşleşme olmadığında tüm trafiği belirli bir yöne yönlendirir




## 8.5.3.Static Routing

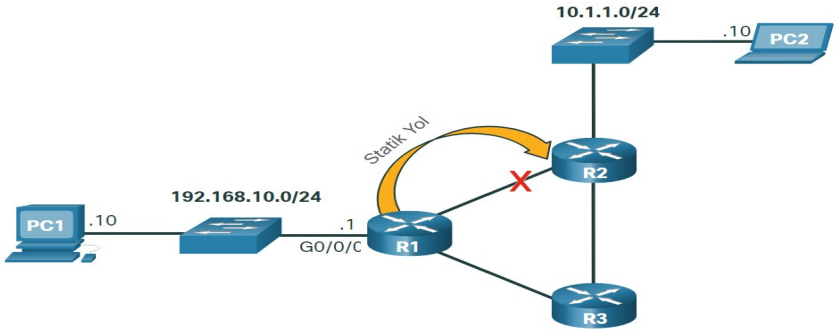
Statik Rota Özellikleri:

- Manuel olarak yapılandırılmalıdır
- Topolojide bir değişiklik olduğunda yönetici tarafından manuel olarak ayarlanmalıdır
- Yedeksiz küçük ağlar için iyi
- Genellikle varsayılan bir rotayı yapılandırmak için dinamik bir yönlendirme protokolü ile birlikte kullanılır




R1, 10.1.1.0/24 ağına ulaşmak için statik bir yolla manuel olarak yapılandırılır. Bu yol değişirse, R1 için yeni bir statik yol gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



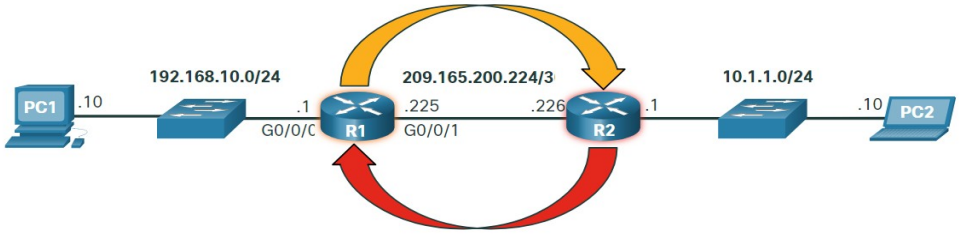

R1 ile R2 arasındaki rota artık mevcut değilse, R3 yoluyla yeni bir statik yol yapılandırılmalıdır. Statik bir yol, topoloji değişiklikleri için otomatik olarak ayarlanmaz.

## 8.5.4.Dynamic Routing

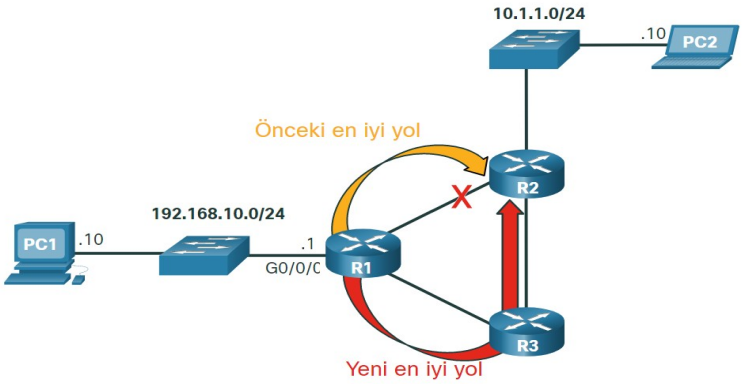
Dinamik Rotalar Otomatik Olarak:

- Uzak ağları keşfeder
- Güncel bilgileri korur
- Hedefe giden en iyi yolu seçer
- Bir topoloji değişikliği olduğunda yeni en iyi yolları bulur

Dinamik yönlendirme, diğer yönlendiricilerle statik varsayılan yolları da paylaşabilir.




- R1, R2'ye 192.168.10.0/24 ağı hakkında bilgi vermek için yönlendirme protokolü OSPF'yi kullanıyor.
- R2, R1'e 10.1.1.0/24 ağı hakkında bilgi vermek için yönlendirme protokolü OSPF'yi kullanıyor.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

R1, R2 ve R3, dinamik yönlendirme protokolü OSPF'yi kullanıyor. Bir ağ topolojisi değişikliği varsa, yeni bir en iyi yolu bulmak için otomatik olarak ayarlanabilirler.

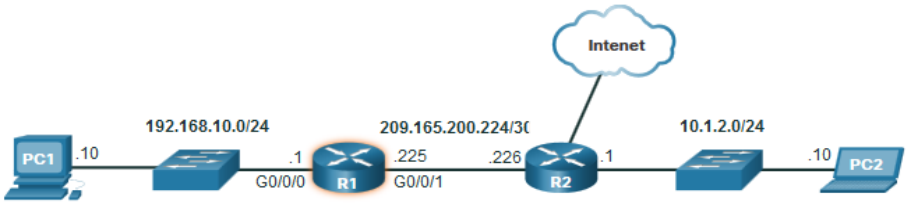
## 8.5.5.IPv4 Yönlendirme Tablosuna Giriş

**show ip route** komutu aşağıdaki rota kaynaklarını gösterir:

- L - Doğrudan bağlı yerel arayüz IP adresi
- C - Doğrudan bağlı ağ
- S - Statik yol bir yönetici tarafından manuel olarak yapılandırıldı
- O - OSPF
- D – EIGRP (EIGRP DUAL algoritmasını kullanır ve kod olarak DUAL'in D'si alınmıştır)

Bu komut rota türlerini gösterir:

- Directly Connected – C and L
- Remote Routes – O, D, etc.
- Default Routes – S*




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*    0.0.0.0/0 [1/0] via 209.165.200.226, GigabitEthernet0/0/1
      10.0.0.0/24 is subnetted, 1 subnets
O        10.1.1.0 [110/2] via 209.165.200.226, 00:02:45, GigabitEthernet0/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 9. Bölüm: Adres Çözümleme

## 9.1.MAC ve IP

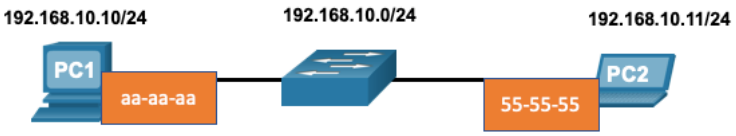
### 9.1.1.Aynı Ağdaki Hedef

**Ethernet LAN üzerindeki bir aygıta atanmış iki birincil adres vardır:**

**Layer 2 physical address (the MAC address)**– Aynı Ethernet ağında NIC - NIC iletişimi için kullanılır.

**Layer 3 logical address (the IP address)**– Paketi kaynak aygıttan hedef aygıta göndermek için kullanılır.

Katman 2 adresleri, aynı ağdaki bir NIC'den başka bir NIC'ye çerçeveleri göndermek için kullanılır. Bir hedef IP adresi aynı ağ üzerindeyse, hedef MAC adresi hedef cihazın adresi olacaktır.



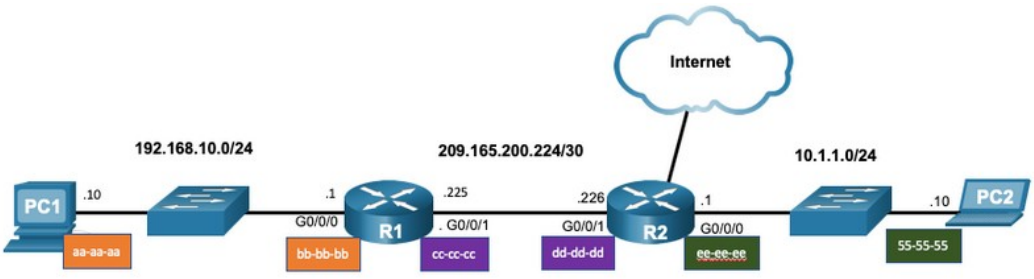

| Destination MAC | Source MAC | Source IPv4 | Destination IPv4 |
|---|---|---|---|
| 55-55-55 | aa-aa-aa | 192.168.10.10 | 192.168.10.11 |

### 9.1.2.Uzak Ağdaki Hedef

Hedef IP adresi uzak bir ağda olduğunda, hedef MAC adresi varsayılan ağ geçidinin adresidir.

ARP, IPv4 tarafından bir cihazın IPv4 adresini NIC cihazının MAC adresiyle ilişkilendirmek için kullanılır.

ICMPv6, bir aygıtın IPv6 adresini NIC aygıtının MAC adresiyle ilişkilendirmek için IPv6 tarafından kullanılır.




| Destination MAC | Source MAC | Source IPv4 | Destination IPv4 |
|---|---|---|---|
| bb-bb-bb | aa-aa-aa | 192.168.10.10 | 10.1.1.10 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

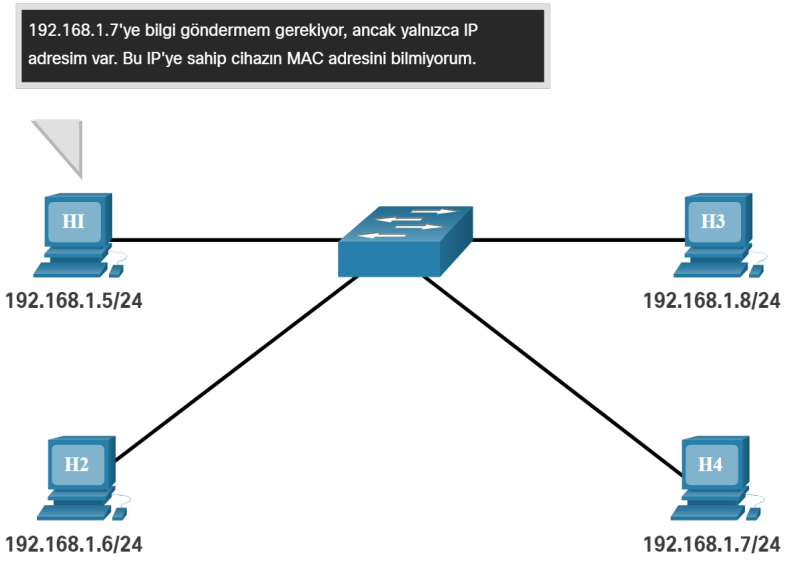
## 9.2.ARP

### 9.2.1.Genel Bakış

Bir cihaz, IPv4 adresini bildiğinde yerel bir cihazın hedef MAC adresini belirlemek için ARP'yi kullanır.

ARP iki temel işlev sunar:

- IPv4 adreslerini MAC adreslerine çözümleme
- MAC adresi eşleşmelerinin IPv4  ARP tablosu bakımı




### 9.2.2.ARP İşlevleri

Bir çerçeve(frame) göndermek için, aygıt ARP tablosunda bir hedef IPv4 adresi ve karşılık gelen bir MAC adresi arar.

Paketin hedef IPv4 adresi aynı ağdaysa, aygıt hedef IPv4 adresi için ARP tablosunda arama yapacaktır.

Hedef IPv4 adresi farklı bir ağdaysa, aygıt varsayılan ağ geçidinin IPv4 adresi için ARP tablosunda arama yapacaktır.

Aygıt IPv4 adresini bulursa, ilgili MAC adresi çerçevedeki hedef MAC adresi olarak kullanılır.

ARP tablo girişi bulunmazsa, aygıt bir ARP isteği gönderir.

### 9.2.3.ARP Tablosundan Girdileri Kaldırma

ARP tablosundaki girişler kalıcı değildir ve belirli bir süre sonra bir ARP önbellek zamanlayıcısı sona erdiğinde kaldırılır.

ARP önbellek zamanlayıcısının süresi işletim sistemine bağlı olarak değişir. yeni Windows işletim sistemleri ARP tablo girdilerini şekilde gösterildiği gibi 15 ila 45 saniye arasında saklar.

ARP tablosu girdileri yönetici tarafından manuel olarak da kaldırılabilir. *arp -d* komutuyla

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 9.2.4.Ağ Aygıtlarındaki ARP Tabloları

**`show ip arp`** komutu bir Cisco yönlendiricide ARP tablosunu görüntüler.

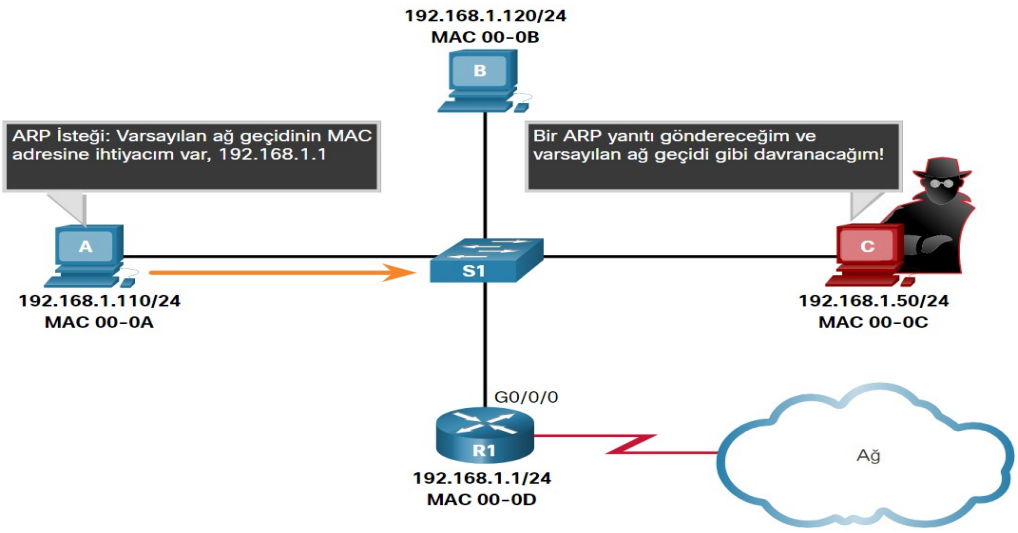
**`arp -a`** komutu, bir Windows 10 bilgisayarda ARP tablosunu görüntüler.

```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1           -   a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
```

```
C:\Users\PC> arp -a

Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
```

### 9.2.5.ARP Sorunları - ARP Yayınları ve ARP Kimlik Sahtekarlığı

ARP istekleri yerel ağdaki her cihaz tarafından alınır ve işlenir.
Aşırı ARP yayınları performansta bir miktar azalmaya neden olabilir.
ARP yanıtları, bir ARP zehirlenmesi saldırısı gerçekleştirmek için bir tehdit aktörü tarafından taklit edilebilir.
Kurumsal düzey anahtarlar, ARP saldırılarına karşı koruma için azaltma tekniklerini içerir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

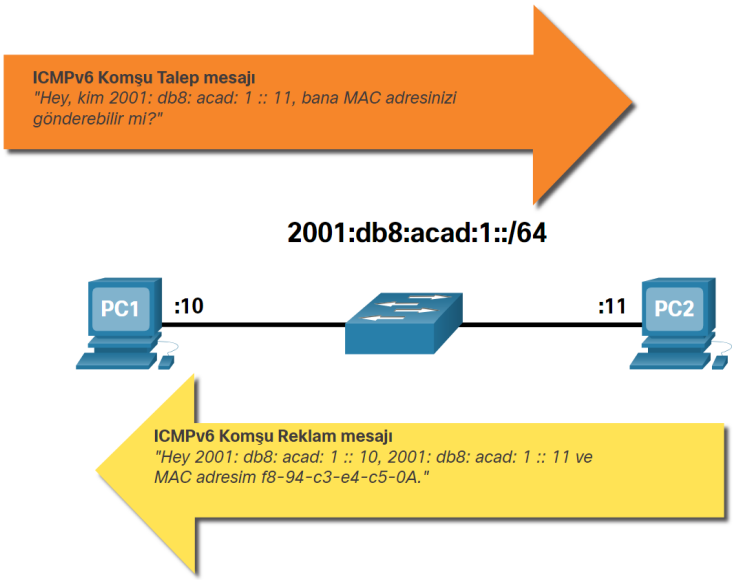
## 9.3.IPv6 Komşu Keşfi (Neighbor Discovery)

### 9.3.1.IPv6 Neighbor Discovery Messages-IPv6 Komşu Keşfi Mesajları

IPv6 Komşu Bulma (ND) protokolü şunları sağlar:

- Adres çözümlemesi
- Yönlendirici keşfi
- Yönlendirme hizmetleri
- ICMPv6 Komşu İstemi-Neighbor Solicitation (NS) ve Komşu Reklamı (Tanıtımı)-Neighbor Advertisement (NA) iletileri, adres çözünürlüğü gibi aygıttan aygıta iletiler için kullanılır.
- ICMTPv6 Yönlendirici İstemi-Router Solicitation(RS) ve Yönlendirici Reklamı-Router Advertisement (RA) mesajları, yönlendirici keşfi için aygıtlar ve yönlendiriciler arasındaki mesajlaşma için kullanılır.
- ICMPv6 yönlendirme mesajları, yönlendiriciler tarafından bir sonraki atlama seçimi için kullanılır.

### 9.3.2.IPv6 Neighbor Discovery – Address Resolution-IPv6 Komşu Bulma - Adres Çözümleme




IPv6 aygıtları, bilinen bir IPv6 adresinin MAC adresini çözmek için ND kullanır.

ICMPv6 Komşu Talep mesajları özel Ethernet ve IPv6 çok noktaya yayın adresleri kullanılarak gönderilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 10.Bölüm: Temel Router-Yönlendirici Yapılandırması

## 10.1.Configure Initial Router Settings-Yönlendirici İlk Ayarlarını Yapılandırma

### 10.1.1.Temel Yönlendirici Yapılandırma Adımları

Aygıt adını yapılandırın.

```
Router(config)# hostname hostname
```

Ayrıcalıklı EXEC modunu güvenli hale getirin.

```
Router(config)# enable secret password
```

Güvenli kullanıcı EXEC modu.

```
Router(config)# line console 0
Router(config-line)# password password
Router(config-line)# login
```

Uzak Telnet / SSH erişimini güvenli hale getirin.

```
Router(config)# line vty 0 4
Router(config-line)# password password
Router(config-line)# login
Router(config-line)# transport input {ssh | telnet}
```

Tüm düz metin parolaları şifreleyin.

```
Router(config)# service password encryption
```

Yasal bildirimde bulunun ve yapılandırmayı kaydedin.

```
Router(config)# banner motd # message #
Router(config)# end
Router# copy running-config startup-config
```

### 10.1.2.Örnek Yapılandırma

```
R1(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# transport input ssh
telnet
R1(config-line)# exit
R1(config)# service password encryption
R1(config)# banner motd #
Enter TEXT message. End with a new line
and the #
****************************************
*******
WARNING: Unauthorized access is
prohibited!
****************************************
******
R1(config)# exit
R1# copy running-config startup-config
```

## 10.2.Configure Interfaces-Arabirimleri(Arayüz) Yapılandırma

### 10.2.1.Yönlendirici Arayüzlerini Yapılandırma

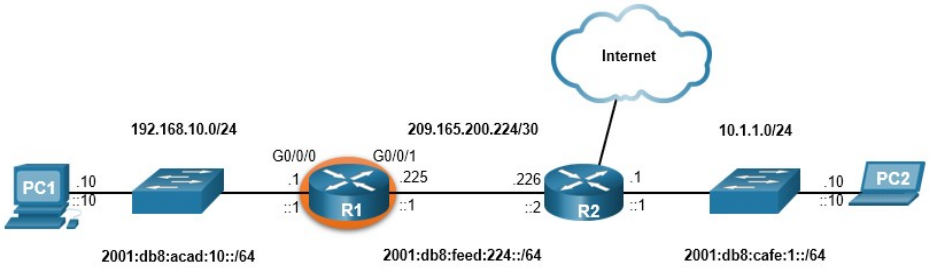
Bir yönlendirici arabiriminin yapılandırılması, aşağıdaki komutları içerir:

```
Router(config)# interface type-and-number
Router(config-if)# description description-text
Router(config-if)# ip address ipv4-address subnet-mask
Router(config-if)# ipv6 address ipv6-address/prefix-length
Router(config-if)# no shutdown
```

- Arabirime bağlı ağ hakkında bilgi eklemek için **description** komutunu kullanmak iyi bir uygulamadır.
- **no shutdown** komutu arabirimi etkinleştirir.

### 10.2.2.Yönlendirici Arayüzlerini Yapılandırma Örneği

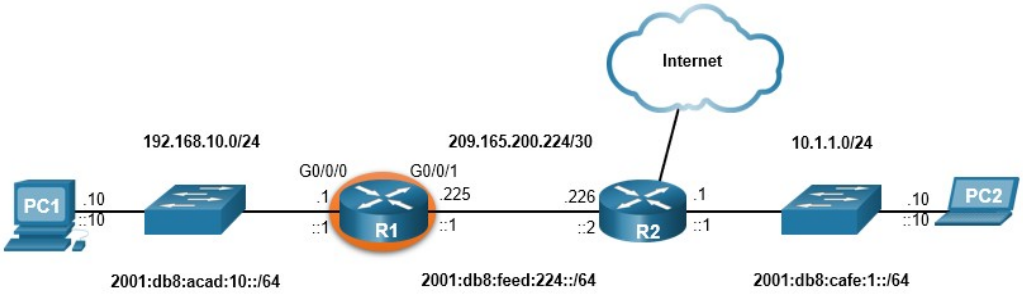
Şekilde R1'de G0 / 0/0 arayüzünü yapılandırma komutları aşağıda gösterilmiştir:




```
R1(config)# interface gigabitEthernet 0/0/0
R1(config-if)# description Link to LAN
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:10::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:43:53.435: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to
down
*Aug  1 01:43:56.447: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to
up
*Aug  1 01:43:57.447: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

R1'de G0 / 0/1 arayüzünü yapılandırma komutları aşağıda gösterilmiştir:




```
R1(config)# interface gigabitEthernet 0/0/1
R1(config-if)# description Link to R2
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:feed:224::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
*Aug  1 01:46:29.170: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Aug  1 01:46:32.171: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to up
*Aug  1 01:46:33.171: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1,
changed state to up
```

## 10.2.3. Verify Interface Configuration-Arayüz Yapılandırmasını Doğrulama

Arayüz yapılandırmasını doğrulamak için **show ip interface brief** IPv6 için de **show ipv6 interface brief** komutlarını kullanın:

```
R1#  show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   209.165.200.225 YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
```

```
R1#  show ipv6 interface brief
GigabitEthernet0/0/0       [up/up]
    FE80::201:C9FF:FE89:4501
    2001:DB8:ACAD:10::1
GigabitEthernet0/0/1       [up/up]
    FE80::201:C9FF:FE89:4502
    2001:DB8:FEED:224::1
Vlan1                      [administratively down/down]
    unassigned
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 10.2.4.Configure Verification Commands-Yapılandırma Doğrulama Komutları

Aşağıdaki tablo, arayüz yapılandırmasını doğrulamak için kullanılan **show** komutlarını özetler.

| Komutlar | Açıklama |
|---|---|
| `show ip interface brief`<br>`show ipv6 interface brief` | Tüm arabirimleri, IP adreslerini ve geçerli durumlarını görüntüler. |
| `show ip route`<br>`show ipv6 route` | RAM'de depolanan IP yönlendirme tablolarının içeriğini görüntüler. |
| `show interfaces` | Aygıttaki tüm arabirimlerin istatistiklerini görüntüler. Yalnızca IPv4 adres bilgilerini görüntüler. |
| `show ip interfaces` | Bir yönlendiricideki tüm arabirimler için IPv4 istatistiklerini görüntüler. |
| `show ipv6 interfaces` | Bir yönlendiricideki tüm arabirimler için IPv6 istatistiklerini görüntüler. |

**show ip route** komutu ile IPv4 yönlendirme tablosunun içeriği ve **show ipv6 route** komutu ile IPv6 yönlendirme tablosunun içeriği görüntülenir.

```
R1# show ip route
< output omitted>
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, GigabitEthernet0/0/1
L        209.165.200.225/32 is directly connected, GigabitEthernet0/0/1
R1#
```

```
R1# show ipv6 route
<output omitted>
C   2001:DB8:ACAD:10::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:10::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:FEED:224::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:FEED:224::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**show interfaces** komutu ile tüm arayüzlerin istatistiklerini görüntüleyin:

```
R1# show interfaces gig0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4321-2x1GE, address is a0e0.af0d.e140 (bia  a0e0.af0d.e140)
  Description: Link to LAN
  Internet address is 192.168.10.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 100Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:35, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output     drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1180 packets input, 109486 bytes, 0 no buffer
     Received 84 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles

<output omitted>

R1#
```

**show ip interface** komutuyla yönlendirici arabirimleri için IPv4 istatistiklerini görüntüleyin:

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP Flow switching is disabled

<output omitted>

R1#
```

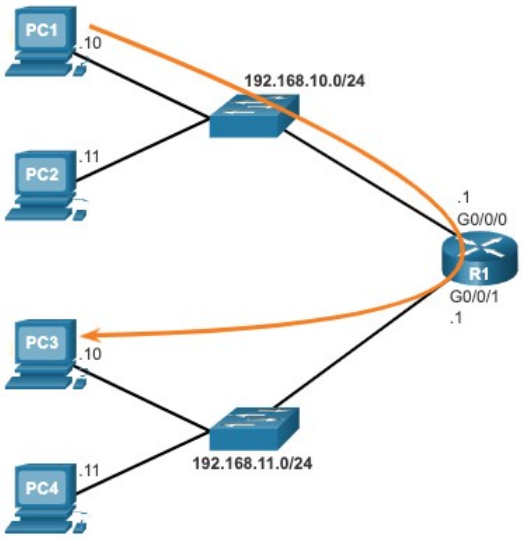
**show ipv6 interface** komutuyla yönlendirici arabirimleri için IPv6 istatistiklerini görüntüleyin:

```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::868A:8DFF:FE44:49B0
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:10::1, subnet is 2001:DB8:ACAD:10::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF44:49B0
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND NS retransmit interval is 1000 milliseconds

R1#
```

## 10.3.Configure the Default Gateway-Varsayılan Ağ Geçidini Yapılandırma

### 10.3.1.Bilgisayardaki Varsayılan Ağ Geçidi

Bir ana bilgisayar başka bir ağdaki bir aygıta bir paket gönderdiğinde varsayılan ağ geçidi kullanılır.
Varsayılan ağ geçidi adresi genellikle ana bilgisayarın yerel ağına bağlı yönlendirici arabirim adresidir.
PC3'e ulaşmak için PC1, PC3'ün IPv4 adresine sahip bir paketi adresler, ancak paketi varsayılan ağ geçidine, R1'in G0 / 0/0 arayüzüne iletir.

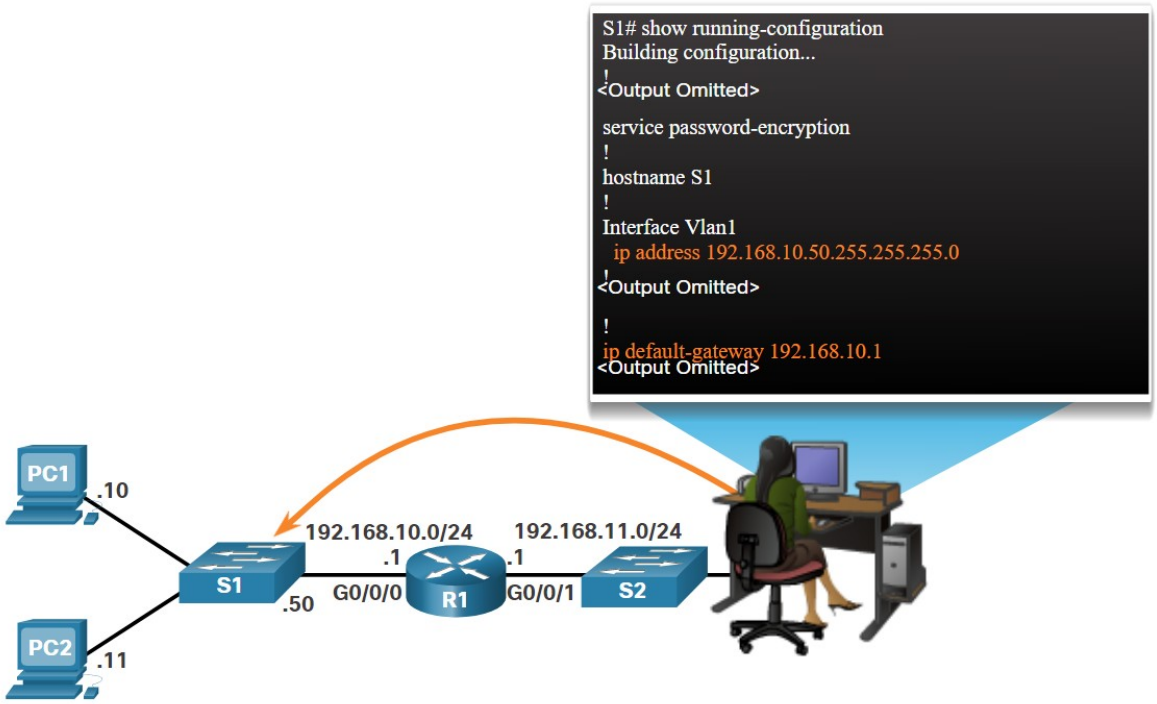



**Not**: Bilgisayarın ve yönlendirici arabiriminin IP adresi aynı ağda olmalıdır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 10.3.2.Anahtardaki Varsayılan Ağ Geçidi

Bir anahtarın, anahtarı başka bir ağdan uzaktan yönetmek için yapılandırılmış bir varsayılan ağ geçidi adresi olmalıdır.
Bir anahtarda IPv4 varsayılan ağ geçidini yapılandırmak için **ip default-gateway** *ip-address* genel yapılandırma komutunu kullanın.



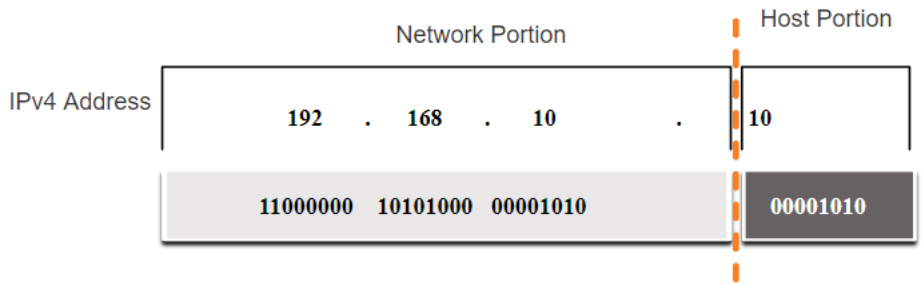

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 11.Bölüm: IPv4 ve IPv6 Adresleme

## 11.1.IPv4 Adres Yapısı

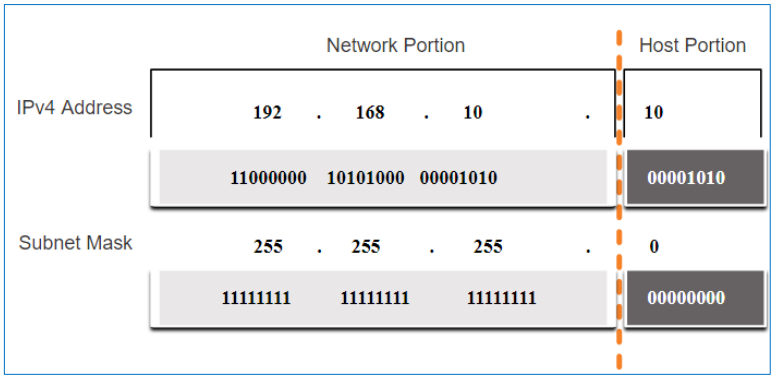
### 11.1.1.Network and Host Portions-Ağ ve Ana Bilgisayar Bölümleri

IPv4 adresi, bir ağ bölümü ve bir ana bilgisayar bölümünden oluşan 32 bit hiyerarşik bir adrestir.
Ağ bölümünü ana makine bölümüne karşı belirlerken, 32 bit akışına bakmalısınız.
Ağ ve ana bilgisayar bölümlerini belirlemek için bir alt ağ maskesi kullanılır.




### 11.1.2.Subnet Mask-Alt Ağ Maskesi

Bir IPv4 adresinin ağ ve ana bilgisayar bölümlerini tanımlamak için, alt ağ maskesi soldan sağa, her bit için IPv4 adres biti ile karşılaştırılır.
Ağı ve ana bilgisayar bölümlerini tanımlamak için kullanılan bu işleme ANDing (ANDleme) adı verilir.

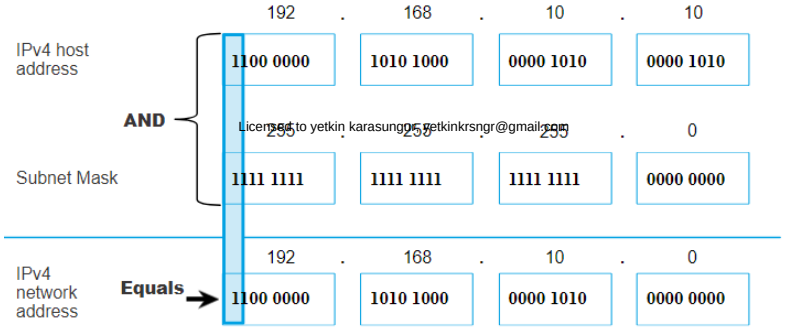



Ağ adresinin belirlenmesinde mantıksal AND Boolean işlemi kullanılır.

Mantıksal AND, sadece 1 AND 1'in 1 ürettiği ve diğer herhangi bir kombinasyonun 0 ile sonuçlandığı iki bitin karşılaştırılmasıdır.

1 AND 1 = 1,  0 AND 1 = 0,  1 AND 0 = 0,  0 AND 0 = 0  1 = True and 0 = False

Ağ adresini tanımlamak için, ana bilgisayar IPv4 adresi, ağ adresini tanımlamak için alt ağ maskesi ile mantıksal olarak AND'lenir.



Licensed to yetkin karasungur yetkinkrsngr@gmail.com

## 11.1.3.Prefix Length-Önek Uzunluğu

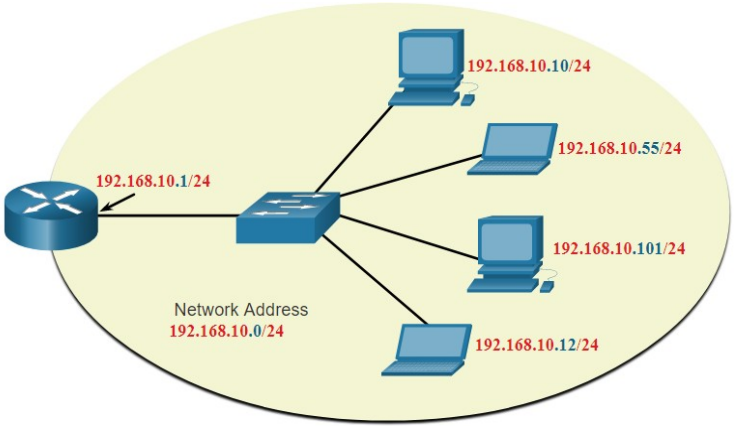
Bir önek uzunluğu, bir alt ağ maskesi adresini tanımlamak için kullanılan daha kolay bir yöntemdir.
Önek uzunluğu, alt ağ maskesinde 1 olarak ayarlanan bit sayısıdır.
"slash notation( eğik çizgi gösterimi)" ile yazılır, alt ağ maskesindeki 1 olan bit sayısını sayın ve eğik çizgi sonrasına ekleyin.

| Subnet Mask | 32-bit Address | Prefix Length |
|---|---|---|
| 255.0.0.0 | 11111111.00000000.00000000.00000000 | /8 |
| 255.255.0.0 | 11111111.11111111.00000000.00000000 | /16 |
| 255.255.255.0 | 11111111.11111111.11111111.00000000 | /24 |
| 255.255.255.128 | 11111111.11111111.11111111.10000000 | /25 |
| 255.255.255.192 | 11111111.11111111.11111111.11000000 | /26 |
| 255.255.255.224 | 11111111.11111111.11111111.11100000 | /27 |
| 255.255.255.240 | 11111111.11111111.11111111.11110000 | /28 |
| 255.255.255.248 | 11111111.11111111.11111111.11111000 | /29 |
| 255.255.255.252 | 11111111.11111111.11111111.11111100 | /30 |

## 11.1.4.Network, Host, and Broadcast Addresses-Ağ, Ana Bilgisayar ve Yayın Adresleri

Her ağda üç tür IP adresi bulunur:

- Network address
- Host addresses
- Broadcast address



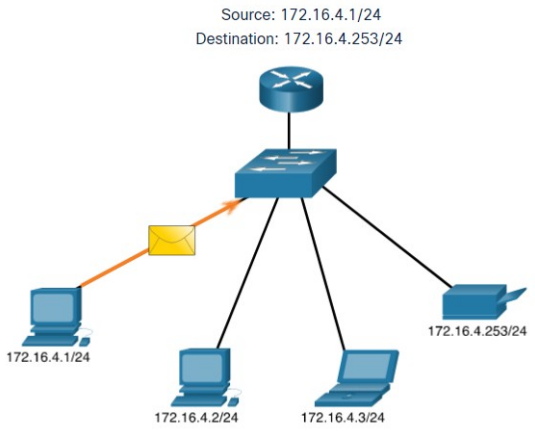

| | Network Kısmı | Host Kısmı | Host Bits |
|---|---|---|---|
| Subnet mask<br>**255.255.255.**0 or **/24** | 255 255 255<br>11111111 11111111 11111111 | 0<br>00000000 | |
| Network address<br>**192.168.10.**0 or **/24** | 192 168 10<br>11000000 10100000 00001010 | 0<br>00000000 | Hepsi 0 |
| First address<br>**192.168.10**.1 or **/24** | 192 168 10<br>11000000 10100000 00001010 | 1<br>00000001 | 0 veya 1'ler |
| Last address<br>**192.168.10**.254 or **/24** | 192 168 10<br>11000000 10100000 00001010 | 254<br>11111110 | 0 veya 1'ler |
| Broadcast address<br>**192.168.10**.255 or **/24** | 192 168 10<br>11000000 10100000 00001010 | 255<br>11111111 | Hepsi 1 |

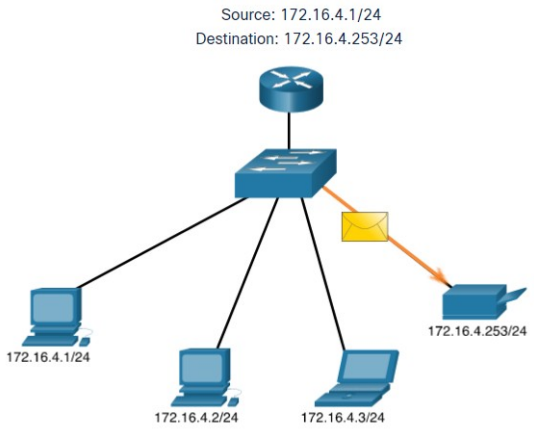
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.2.IPv4 Unicast, Broadcast, Multicast

### 11.2.1.Unicast

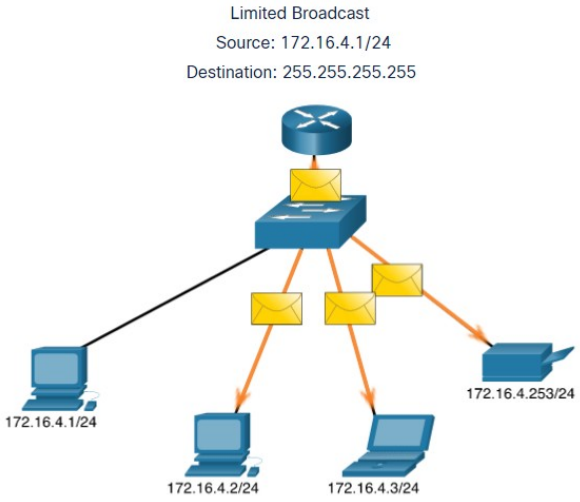
Tek noktaya yayın iletimi bir hedef IP adresine bir paket gönderir.
Örneğin, 172.16.4.1'deki bilgisayar yazıcıya 172.16.4.253'te tek noktaya yayın paketi gönderir.

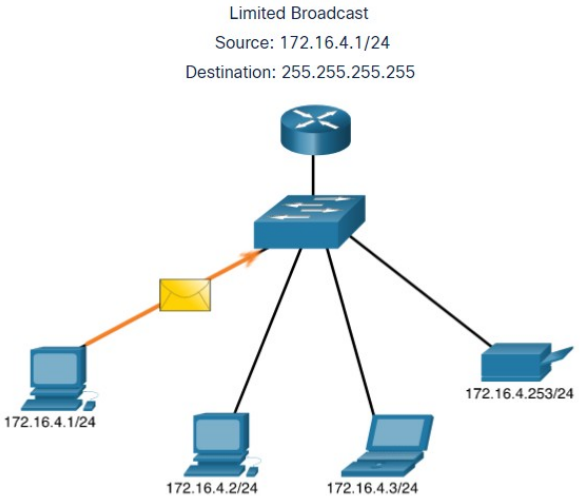



### 11.2.2.Broadcast

Yayın iletimi diğer tüm hedef IP adreslerine bir paket gönderir.
Örneğin, 172.16.4.1'deki bilgisayar tüm IPv4 ana bilgisayarlarına bir yayın paketi gönderir.

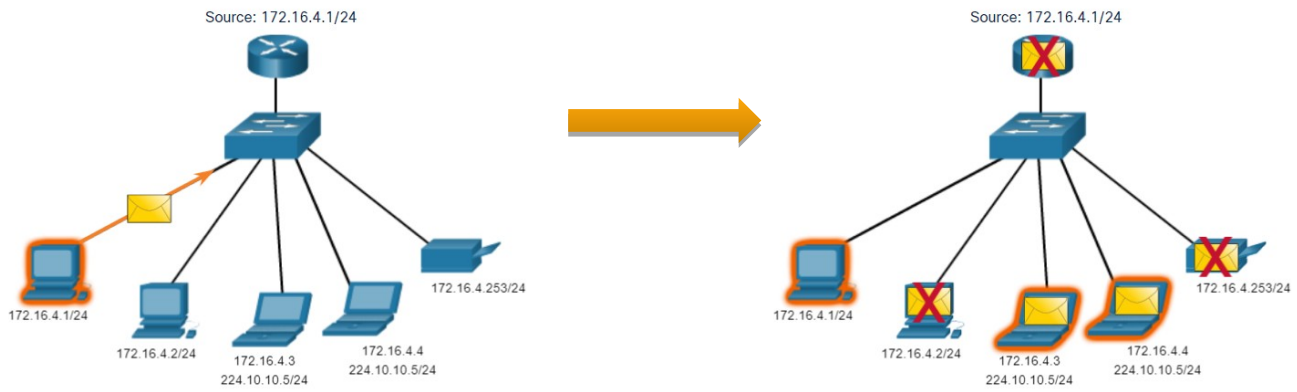



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 11.2.3.Multicast

Çok noktaya yayın iletimi, çok noktaya yayın adres grubuna bir paket gönderir.
Örneğin, 172.16.4.1'deki PC, çok noktaya yayın grubu adresine ( 224.10.10.5) çok noktaya yayın paketi gönderir.




## 11.3.IPv4 Adres Türleri

### 11.3.1.Public and Private IPv4 Addresses-Genel ve Özel IPv4 Adresleri

RFC 1918'de tanımlandığı gibi, genel IPv4 adresleri küresel olarak internet servis sağlayıcısı (ISP) yönlendiricileri arasında yönlendirilir.
Özel adresler, çoğu kuruluş tarafından dahili ana bilgisayarlara IPv4 adresleri atamak için kullanılan yaygın adres bloklarıdır.

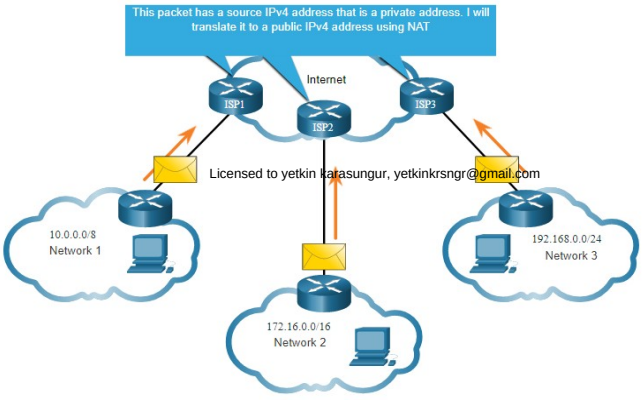
Özel IPv4 adresleri benzersiz değildir ve herhangi bir ağda dahili olarak kullanılabilir.
Ancak, özel adresler global olarak yönlendirilemez.

| Network Address and Prefix | RFC 1918 Private Address Range |
|---|---|
| 10.0.0.0/8 | 10.0.0.0 - 10.255.255.255 |
| 172.16.0.0/12 | 172.16.0.0 - 172.31.255.255 |
| 192.168.0.0/16 | 192.168.0.0 - 192.168.255.255 |

### 11.3.2.Routing to the Internet-İnternete yönlendirme

Ağ Adresi Çevirisi-Network Address Translation(NAT) özel IPv4 adreslerini genel IPv4 adreslerine çevirir.
NAT genellikle internete bağlanan kenar yönlendiricide (edge router) etkinleştirilir.

Dahili özel adresi (internal private address) genel bir (public global) global IP adresine çevirir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.3.3.Özel Kullanım IPv4 Adresleri

```
C:\Users\NetAcad> ping 127.0.0.1
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

Loopback addresses-Geri Döngü Adresleri

- 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- Genellikle 127.0.0.1 olarak tanımlanır
- TCP / IP'nin çalışıp çalışmadığını test etmek için bir ana bilgisayarda kullanılır.

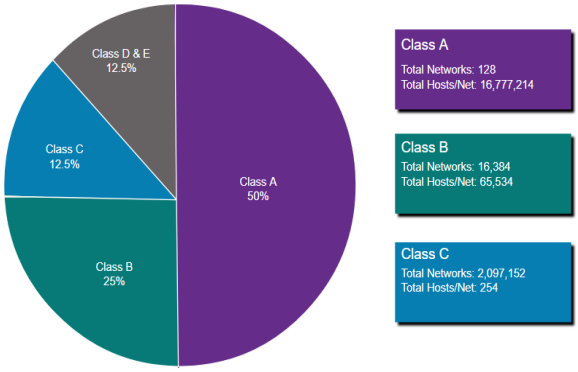
Link-Local addresses-Yerel Bağlantı adresleri

- 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- Genellikle Otomatik Özel IP Adresleme-Automatic Private IP Addressing(APIPA) adresleri veya kendinden atanan adresler olarak bilinir.
- Windows DHCP istemcileri tarafından, kullanılabilir DHCP sunucusu olmadığında kendi kendini yapılandırmak için kullanılır.

## 11.3.4.Legacy Classful Addressing-Eski Sınıflı Adresleme

RFC 790 (1981) belli sınıflarda (Class) IPv4 adresleri tahsis etti

- Class A (0.0.0.0/8 to 127.0.0.0/8)
- Class B (128.0.0.0 /16 – 191.255.0.0 /16)
- Class C (192.0.0.0 /24 – 223.255.255.0 /24)
- Class D (224.0.0.0 to 239.0.0.0)
- Class E (240.0.0.0 – 255.0.0.0)

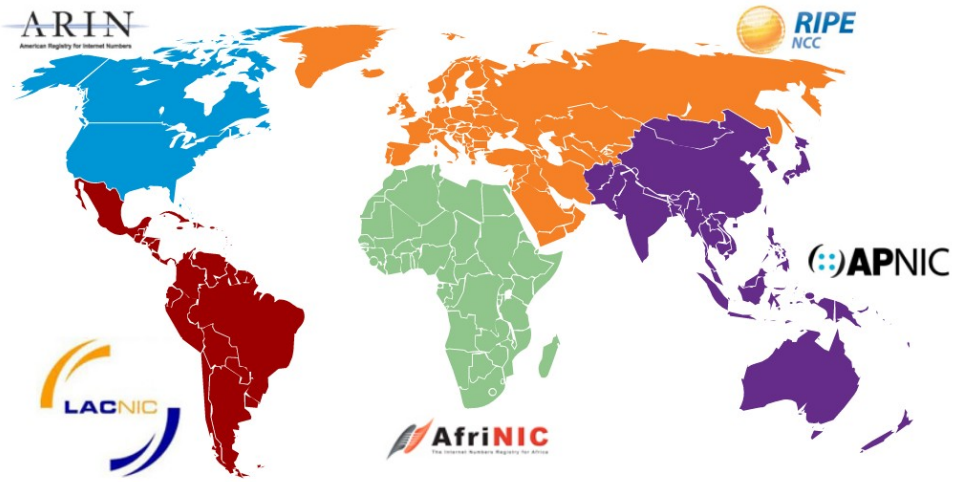



Sınıflı adresleme birçok Ipv4 adresin boşa gitmesine neden oldu.

Sınıfsal adres tahsisi, sınıf kurallarını (A, B, C) göz ardı eden sınıfsız (classless) adresleme ile değiştirildi.

## 11.3.5.Assignment of IP Addresses-IP Adreslerinin Atanması

İnternet Atanmış Numaralar Kurumu-Internet Assigned Numbers Authority (IANA), IPv4 ve IPv6 adres bloklarını beş Bölgesel İnternet Kaydı- Regional Internet Registries kurumu aracılığıyla (RIR) yönetir ve tahsis eder. RIR'lar, daha küçük ISP'lere ve kuruluşlara IPv4 adres blokları sağlayan İSS'lere IP adresleri tahsis etmekten sorumludur.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

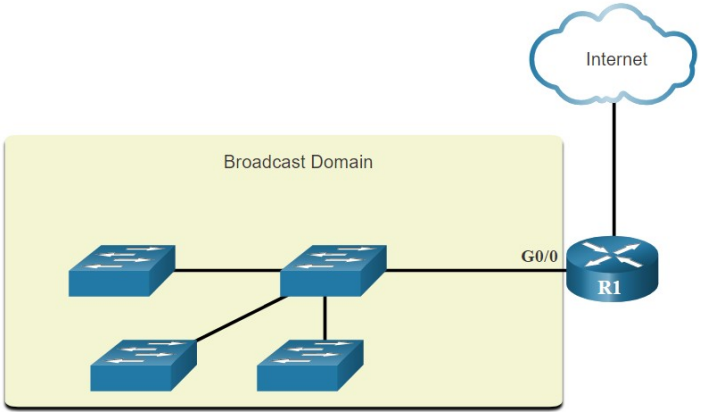
## 11.4.Network Segmentation-Ağ Bölümleme

### 11.4.1.Broadcast Domains and Segmentation-Yayın Alanları ve Bölümleme

Birçok protokol yayınları (broadcast) veya çok noktaya yayınları kullanır (örneğin, ARP diğer aygıtları bulmak için yayınları kullanır, ana bilgisayarlar bir DHCP sunucusu bulmak için yayınları kullanır.)

Anahtarlar, trafiği alındığı arabirim dışındaki tüm arabirimlere yayıyor.

- Yayınları durduran tek cihaz bir yönlendiricidir.
- Yönlendiriciler yayınları yaymaz.
- Her yönlendirici arabirimi bir yayın etki alanına bağlanır ve yayınlar yalnızca o belirli yayın etki alanında yayılır.



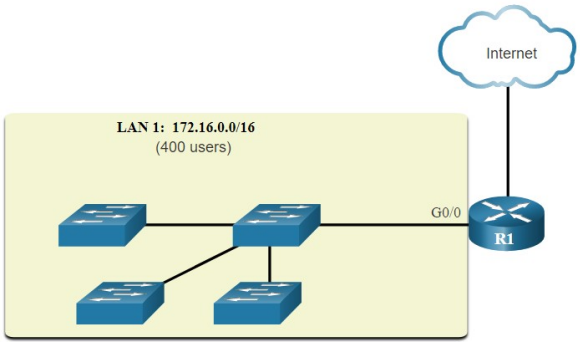

### 11.4.2.Büyük Yayın Alanlarıyla İlgili Sorunlar

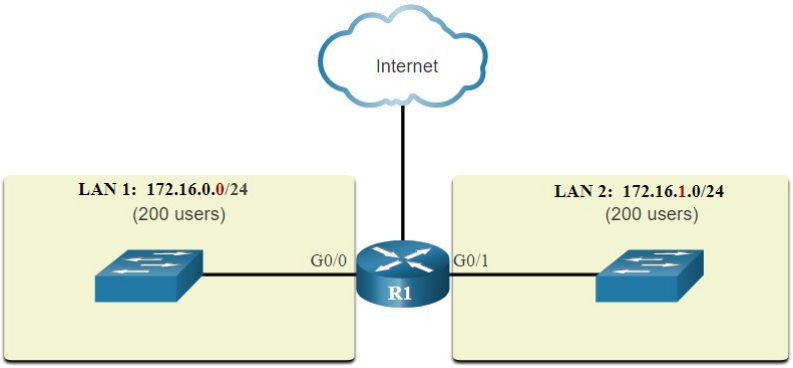
Geniş bir yayın alanıyla ilgili bir sorun, bu ana bilgisayarların aşırı yayın üretebilmesi ve ağı olumsuz etkileyebilmesidir.

Çözüm, alt ağ (subnetting) adı verilen bir işlemde daha küçük yayın etki alanları oluşturmak için ağın boyutunu azaltmaktır.

Ağ adresi 172.16.0.0 /16'yı her biri 200 kullanıcıdan iki alt ağına bölmek: 172.16.0.0 /24 ve 172.16.1.0 /24.

Yayınlar yalnızca daha küçük yayın alanlarında yayılır.



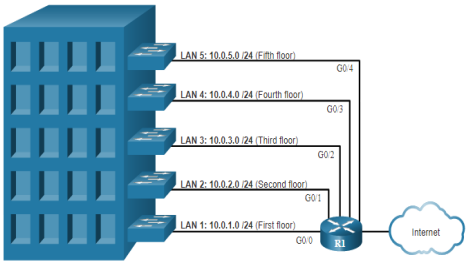

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 11.4.3.Ağları Bölümlere Ayırma Nedenleri

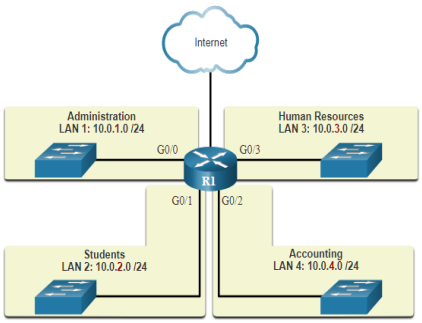
- Alt ağ Subnetting), genel ağ trafiğini azaltır ve ağ performansını iyileştirir.
- Alt ağlar arasında güvenlik politikaları uygulamak için kullanılabilir.
- Alt ağ, anormal yayın trafiğinden etkilenen cihaz sayısını azaltır.

Alt ağlar aşağıdakiler dahil çeşitli nedenlerle kullanılır:

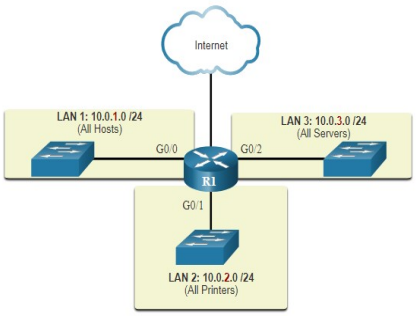
Location




Grup veya İşlev




Cihaz Tipi




## 11.5.Subnet an IPv4 Network-IPv4 Ağları Alt Ağlara Bölme

### 11.5.1.Subnet on an Octet Boundary-Sekizli Sınırda Alt Ağ

IPv4 alt ağları, ağ bitleri olarak bir veya daha fazla ana bilgisayar biti kullanılarak oluşturulur. Bu, ek ağ bitleri oluşturmak için adresin ana bilgisayar bölümünden bazı bitleri ödünç almak için alt ağ maskesinin genişletilmesiyle yapılır. Ne kadar çok ana bilgisayar biti ödünç alınırsa, o kadar çok alt ağ tanımlanabilir. Alt ağların sayısını artırmak için ödünç alınan daha fazla bit, alt ağ başına ana bilgisayar sayısını azaltır.

Ağlar en kolay şekilde / 8, / 16 ve / 24 sekizli sınırında alt ağlara bağlanır. Tablo bu önek uzunluklarını tanımlar.Daha uzun önek uzunlukları kullanmanın alt ağ başına ana bilgisayar sayısını azalttığına dikkat edin.

| Prefix Length | Subnet Mask | Subnet Mask in Binary (n = network, h = host) | # of hosts |
|---|---|---|---|
| /8 | **255**.0.0.0 | **nnnnnnnn**.hhhhhhhh.hhhhhhhh.hhhhhhhh<br>**11111111**.00000000.00000000.00000000 | 16,777,214 |
| /16 | **255.255**.0.0 | **nnnnnnnn.nnnnnnnn**.hhhhhhhh.hhhhhhhh<br>**11111111.11111111**.00000000.00000000 | 65,534 |
| /24 | **255.255.255**.0 | **nnnnnnnn.nnnnnnnn.nnnnnnnn**.hhhhhhhh<br>**11111111.11111111.11111111**.00000000 | 254 |

Sekizli sınırında alt ağ oluşturmanın ne kadar yararlı olabileceğini anlamak için aşağıdaki örneği düşünün. Bir kuruluşun iç ağ adresi olarak 10.0.0.0/8 özel adresini seçtiğini varsayalım. Bu ağ adresi, tek bir yayın etki alanındaki 16.777.214 ana bilgisayarı bağlayabilir. Açıkçası, tek bir alt ağda 16 milyondan fazla ana bilgisayara sahip olmak ideal değildir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Kuruluş ayrıca 10.0.0.0/8 adresini tabloda gösterildiği gibi / 16 sekizli sınırında alt ağa bağlayabilir. Bu, kuruluşa, 65.534 ana bilgisayarı bağlayabilen her alt ağ ile 256 adede kadar alt ağ (yani 10.0.0.0/16 - 10.255.0.0/16) tanımlama

yeteneği sağlar. İlk iki sekizlinin adresin ağ bölümünü belirlerken, son iki sekizlinin ana bilgisayar IP adresleri için olduğuna dikkat edin.

**Tabloda 10.0.0.0/8 /16 alt ağ maskesi kullanılarak alt ağlar oluşturulmuştur.**

| **Subnet Address** (256 Possible Subnets) | **Host Range** (65,534 possible hosts per subnet) | **Broadcast** |
|---|---|---|
| **10.0**.0.0/**16** | **10.0**.0.1 - **10.0**.255.254 | **10.0**.255.255 |
| **10.1**.0.0/**16** | **10.1**.0.1 - **10.1**.255.254 | **10.1**.255.255 |
| **10.2**.0.0/**16** | **10.2**.0.1 - **10.2**.255.254 | **10.2**.255.255 |
| **10.3**.0.0/**16** | **10.3**.0.1 - **10.3**.255.254 | **10.3**.255.255 |
| **10.4**.0.0/**16** | **10.4**.0.1 - **10.4**.255.254 | **10.4**.255.255 |
| **10.5**.0.0/**16** | **10.5**.0.1 - **10.5**.255.254 | **10.5**.255.255 |
| **10.6**.0.0/**16** | **10.6**.0.1 - **10.6**.255.254 | **10.6**.255.255 |
| **10.7**.0.0/**16** | **10.7**.0.1 - **10.7**.255.254 | **10.7**.255.255 |
| ... | ... | ... |
| **10.255**.0.0/**16** | **10.255**.0.1 - **10.255**.255.254 | **10.255**.255.255 |

**Tabloda 10.0.0.0/8 /24 alt ağ maskesi kullanılarak alt ağlar oluşturulmuştur.**

| **Subnet Address** (65,536 Possible Subnets) | **Host Range** (254 possible hosts per subnet) | **Broadcast** |
|---|---|---|
| **10.0.0**.0/**24** | **10.0.0**.1 - **10.0.0**.254 | **10.0.0**.255 |
| **10.0.1**.0/**24** | **10.0.1**.1 - **10.0.1**.254 | **10.0.1**.255 |
| **10.0.2**.0/**24** | **10.0.2**.1 - **10.0.2**.254 | **10.0.2**.255 |
| … | … | … |
| **10.0.255**.0/**24** | **10.0.255**.1 - **10.0.255**.254 | **10.0.255**.255 |
| **10.1.0**.0/**24** | **10.1.0**.1 - **10.1.0**.254 | **10.1.0**.255 |
| **10.1.1**.0/**24** | **10.1.1**.1 - **10.1.1**.254 | **10.1.1**.255 |
| **10.1.2**.0/**24** | **10.1.2**.1 - **10.1.2**.254 | **10.1.2**.255 |
| … | … | … |
| **10.100.0**.0/**24** | **10.100.0**.1 - **10.100.0**.254 | **10.100.0**.255 |
| ... | ... | ... |
| **10.255.255**.0/**24** | **10.255.255**.1 - **10.2255.255**.254 | **10.255.255**.255 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Alternatif olarak, kuruluş 10.0.0.0/8 ağını tabloda gösterildiği gibi / 24 sekizli sınırında alt ağ oluşturmayı seçebilir. Bu, kuruluşun her biri 254 ana bilgisayarı bağlayabilen 65.536 alt ağ tanımlamasına olanak tanır. / 24 sınırı, makul

sayıda ana bilgisayarı ve sekizli sınırında uygun şekilde alt ağları barındırdığı için alt ağ oluşturmada çok popülerdir.

**Bir /24 ağına alt ağ sağlamanın altı yolunu görmek için tabloya bakın.**

| Prefix Length | Subnet Mask | Subnet Mask in Binary (n = network, h = host) | # of subnets | # of hosts |
|---|---|---|---|---|
| /25 | 255.255.255.128 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh<br>11111111.11111111.11111111.**1**0000000 | **2** | 126 |
| /26 | 255.255.255.192 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh<br>11111111.11111111.11111111.**11**000000 | **4** | 62 |
| /27 | 255.255.255.224 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh<br>11111111.11111111.11111111.**111**00000 | **8** | 30 |
| /28 | 255.255.255.240 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh<br>11111111.11111111.11111111.**1111**0000 | **16** | 14 |
| /29 | 255.255.255.248 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh<br>11111111.11111111.11111111.**11111**000 | **32** | 6 |
| /30 | 255.255.255.252 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh<br>11111111.11111111.11111111.**111111**00 | **64** | 2 |

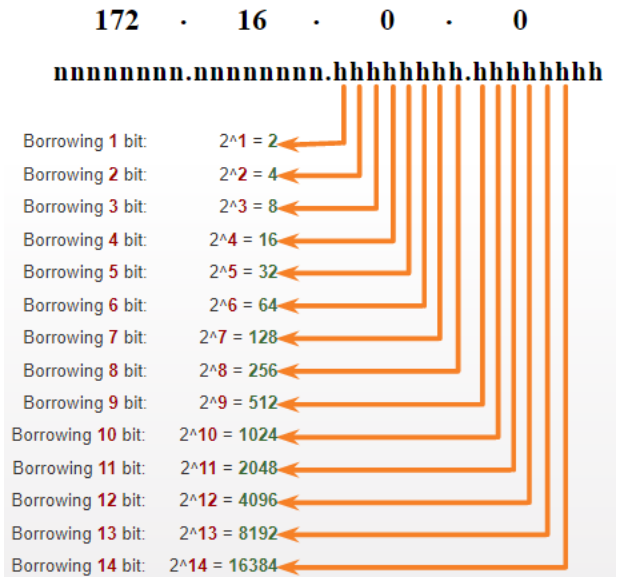
**Tablo, bir /16 önekinin alt ağ oluşturması için olası tüm senaryoları vurgular.**

| Prefix Length | Subnet Mask | Network Address (n = network, h = host) | # of subnets | # of hosts |
|---|---|---|---|---|
| /17 | 255.255.**128**.0 | nnnnnnnn.nnnnnnnn.**n**hhhhhhh.hhhhhhhh<br>11111111.11111111.**1**0000000.00000000 | **2** | 32766 |
| /18 | 255.255.**192**.0 | nnnnnnnn.nnnnnnnn.**nn**hhhhhh.hhhhhhhh<br>11111111.11111111.**11**000000.00000000 | **4** | 16382 |
| /19 | 255.255.**224**.0 | nnnnnnnn.nnnnnnnn.**nnn**hhhhh.hhhhhhhh<br>11111111.11111111.**111**00000.00000000 | **8** | 8190 |
| /20 | 255.255.**240**.0 | nnnnnnnn.nnnnnnnn.**nnnn**hhhh.hhhhhhhh<br>11111111.11111111.**1111**0000.00000000 | **16** | 4094 |
| /21 | 255.255.**248**.0 | nnnnnnnn.nnnnnnnn.**nnnnn**hhh.hhhhhhhh<br>11111111.11111111.**11111**000.00000000 | **32** | 2046 |
| /22 | 255.255.**252**.0 | nnnnnnnn.nnnnnnnn.**nnnnnn**hh.hhhhhhhh<br>11111111.11111111.**111111**00.00000000 | **64** | 1022 |
| /23 | 255.255.**254**.0 | nnnnnnnn.nnnnnnnn.**nnnnnnn**h.hhhhhhhh<br>11111111.11111111.**1111111**0.00000000 | **128** | 510 |
| /24 | 255.255.**255.0** | nnnnnnnn.nnnnnnnn.**nnnnnnnn**.hhhhhhhh<br>11111111.11111111.**11111111**.00000000 | **256** | 254 |
| /25 | 255.255.**255.128** | nnnnnnnn.nnnnnnnn.**nnnnnnnn.n**hhhhhhh<br>11111111.11111111.**11111111.1**0000000 | **512** | 126 |
| /26 | 255.255.**255.192** | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nn**hhhhhh<br>11111111.11111111.**11111111.11**000000 | **1024** | 62 |
| /27 | 255.255.**255.224** | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnn**hhhhh<br>11111111.11111111.**11111111.111**00000 | **2048** | 30 |
| /28 | 255.255.**255.240** | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnn**hhhh<br>11111111.11111111.**11111111.1111**0000 | **4096** | 14 |
| /29 | 255.255.**255.248** | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnn**hhh<br>11111111.11111111.**11111111.11111**000 | **8192** | 6 |
| /30 | 255.255.**255.252** | nnnnnnnn.nnnnnnnn.**nnnnnnnn.nnnnnn**hh<br>11111111.11111111.**11111111.111111**00 | **16384** | 2 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.5.2./16 önekiyle 100 Alt Ağ Oluşturma

En az 100 alt ağ gerektiren ve dahili ağ adresi olarak 172.16.0.0/16 özel adresini seçen büyük bir kuruluşu düşünün.
Şekil, üçüncü sekizli ve dördüncü sekizliden bit ödünç alırken oluşturulabilecek alt ağların sayısını görüntüler.
Şu anda ödünç alınabilecek en fazla 14 ana bilgisayar biti olduğuna dikkat edin (yani, son iki bit ödünç alınamaz).
Kuruluş için 100 alt ağ gereksinimini karşılamak için, 7 bitin (yani, $2^7$ = 128 alt ağ) ödünç alınması gerekir.




## 11.5.3./8 önekiyle 1000 Alt Ağ Oluşturma

Ağ adresi 10.0.0.0/8 kullanarak istemcileri için 1000 alt ağ gerektiren küçük bir ISS düşünün, bu da ağ kısmında 8 bit ve alt ağdan ödünç almak için kullanılabilir 24 ana bilgisayar biti olduğu anlamına gelir.
Şekil, ikinci ve üçüncü bitlerden ödünç bit alınarak oluşturulabilecek alt ağ sayısını görüntüler.
Şu anda ödünç alınabilecek en fazla 22 ana bilgisayar biti olduğuna dikkat edin (yani, son iki bit ödünç alınamaz).
Kuruluş için 1000 alt ağ gereksinimini karşılamak için, 10 bit (yani, $2^{10}$=1024 alt ağlar) ödünç alınması gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.6.Gereksinimleri Karşılayacak Alt Ağ

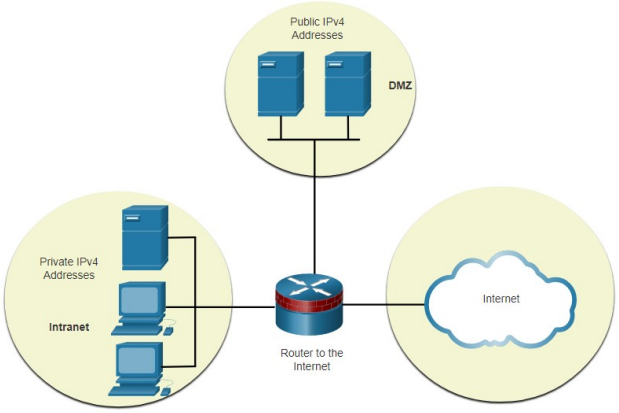
### 11.6.1.Özel Alt Ağ  ve Genel IPv4 Adres Alanı

Kurumsal ağlarda şunlar bulunur:

- Intranet - Bir şirketin genellikle özel IPv4 adreslerini kullanan dahili ağı.
- DMZ – Sunucuların İnternete çıktığı bölge.
- DMZ'deki cihazlar genel IPv4 adreslerini kullanır.

Bir şirket, 10.0.0.0/8 ve alt ağı / 16 veya / 24 ağ sınırında kullanabilir.

DMZ cihazlarının genel IP adresleriyle yapılandırılması gerekir.




### Kullanılmayan Ana Bilgisayar IPv4 Adreslerini En Aza İndirin ve Alt Ağları En Üst Düzeye Çıkarın

Alt ağları planlarken dikkat edilmesi gereken iki önemli husus vardır:
Her ağ için gereken ana bilgisayar adresi sayısı
Gerekli alt ağların sayısı

| Prefix Length | Subnet Mask | Subnet Mask in Binary (n = network, h = host) | # of subnets | # of hosts |
|---|---|---|---|---|
| /25 | 255.255.255.128 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**n**hhhhhhh<br>11111111.11111111.11111111.**1**0000000 | **2** | 126 |
| /26 | 255.255.255.192 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nn**hhhhhh<br>11111111.11111111.11111111.**11**000000 | **4** | 62 |
| /27 | 255.255.255.224 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnn**hhhhh<br>11111111.11111111.11111111.**111**00000 | **8** | 30 |
| /28 | 255.255.255.240 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnn**hhhh<br>11111111.11111111.11111111.**1111**0000 | **16** | 14 |
| /29 | 255.255.255.248 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnn**hhh<br>11111111.11111111.11111111.**11111**000 | **32** | 6 |
| /30 | 255.255.255.252 | nnnnnnnn.nnnnnnnn.nnnnnnnn.**nnnnnn**hh<br>11111111.11111111.11111111.**111111**00 | **64** | 2 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

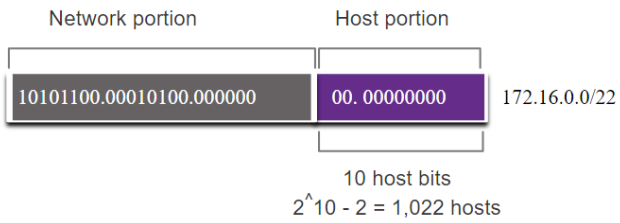
## Örnek: Verimli IPv4 Alt Ağları

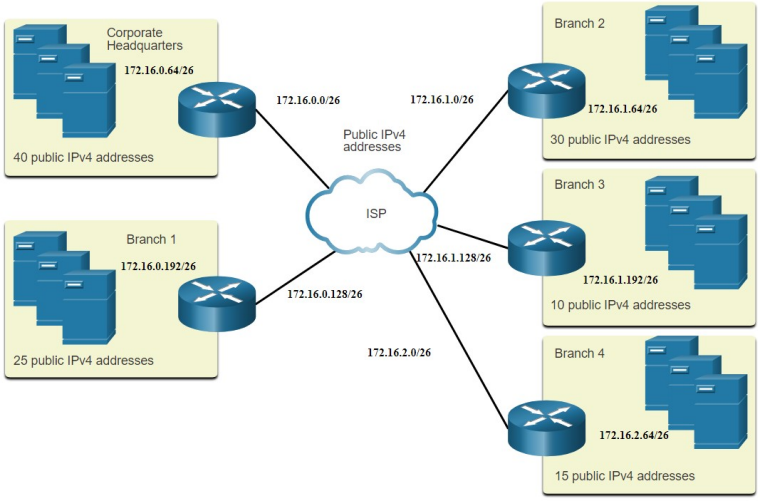
Bu örnekte, şirket merkezi, ISS'si tarafından 1.022 ana bilgisayar adresi sağlayan 172.16.0.0/22 (10 ana bilgisayar biti) genel ağ adresi tahsis edilmiştir.

Beş site vardır ve bu nedenle beş internet bağlantısı vardır, bu organizasyonun en büyük 40 en küçük 10 alt adrese ihtiyaç duyan 10 alt ağa sahip olması gerekir.

Bir /26 (yani, 255.255.255.192) alt ağ maskesi ile 10 alt ağ tahsis edilir. ($2^4$=16 toplam subnet elde edilir. 4 host biti alındı.)

$2^6$-2=62 her subnetteki maks IP sayısı



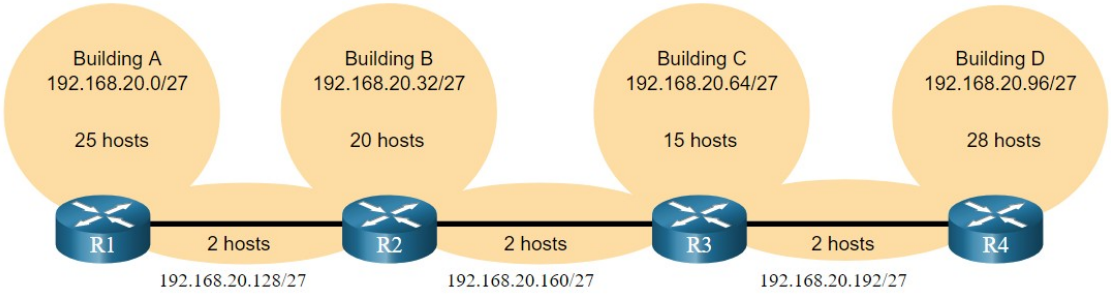




## 11.7.VLSM

### 11.7.1.IPv4 Adreslerin Korunması

Topoloji göz önüne alındığında, 7 alt ağ gereklidir (yani, dört LAN ve üç WAN bağlantısı) ve en fazla ana bilgisayar 28 ana bilgisayar ile Bina D'de bulunur.

A / 27 maskesi, 30 ana bilgisayar IP adresi ve 8 alt ağ sağlar ve bu nedenle bu topolojiyi destekler.

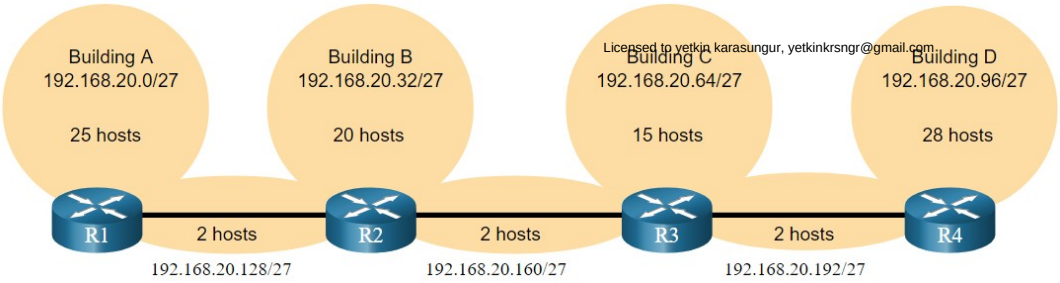



Ancak, noktadan noktaya WAN bağlantıları yalnızca iki adres gerektirir ve bu nedenle toplam 84 kullanılmayan adres olur bu da bir israftır.

Host portion
2^5 – 2 = 30 host IP addresses per subnet

30 – 2 = 28
Each WAN subnet wastes 28 addresses

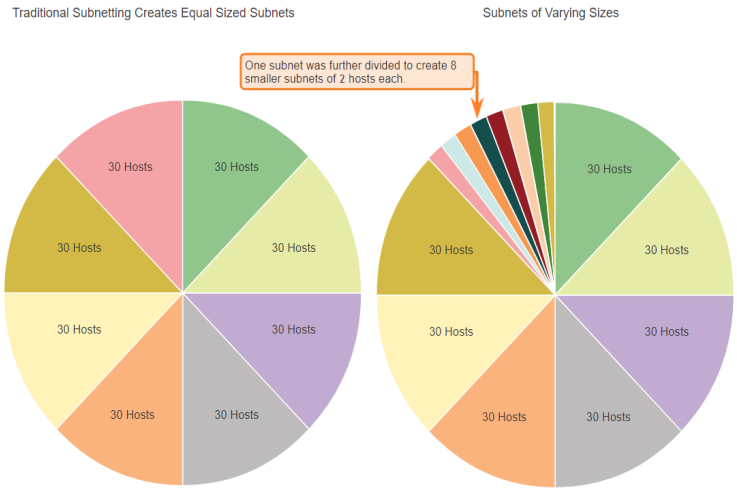
28 x 3 = 84
84 addresses are unused




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

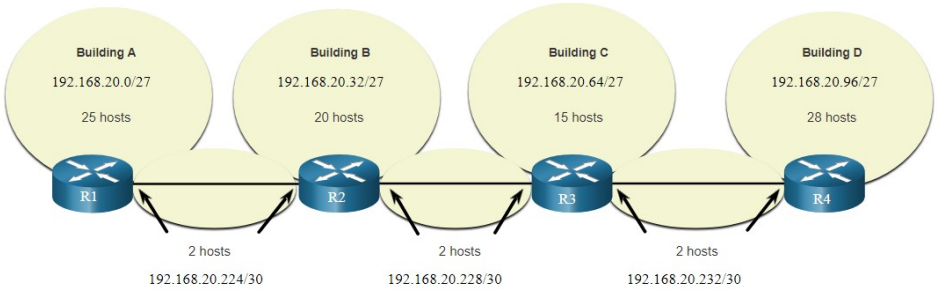
## 11.7.2.VLSM(Variable Lenght SubnetMask)

Sol taraf geleneksel alt ağ şemasını (yani aynı alt ağ maskesi) gösterirken, sağ taraf VLSM'nin bir alt ağı alt ağa bağlamak ve son alt ağı sekiz / 30 alt ağa bölmek için nasıl kullanılabileceğini gösterir.

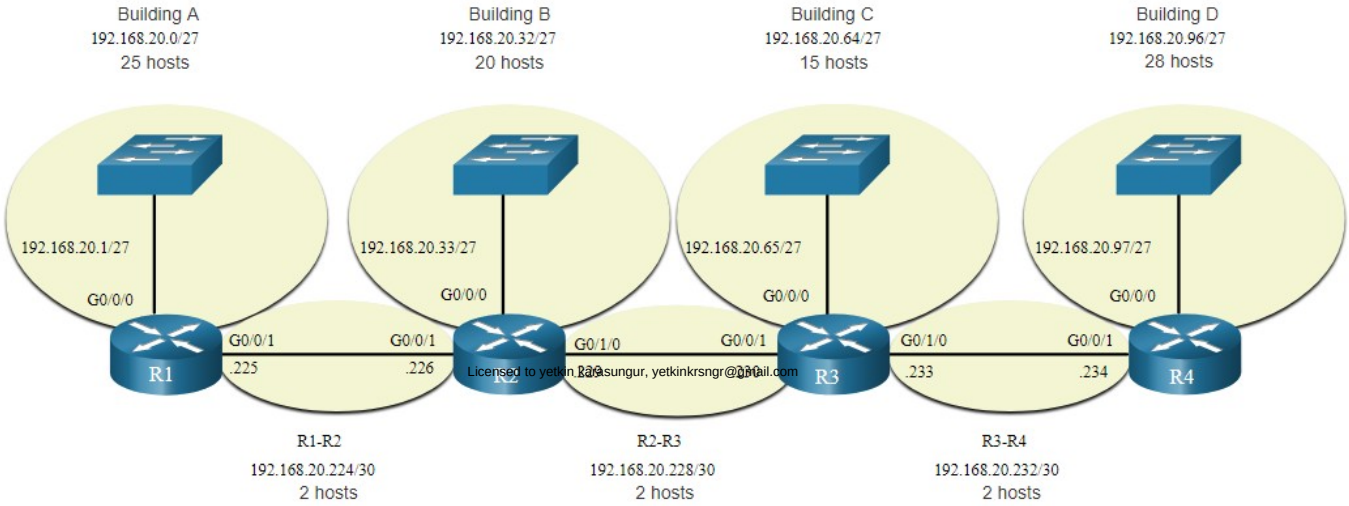



VLSM kullanırken, her zaman en büyük alt ağın ana bilgisayar gereksinimlerini karşılayarak başlayın ve en küçük alt ağın ana bilgisayar gereksinimleri karşılanana kadar alt ağa devam edin.

VLSM ile ortaya çıkan topoloji uygulandı.




VLSM alt ağları kullanılarak, LAN ve internet yönlendirici ağları, mantıksal topoloji diyagramında gösterildiği gibi israf olmadan yapılandırılabilir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.8.IPv6 Addressing-IPv6 Adresleme

### 11.8.1.IPv4 Sorunları

IPv4 adresleri tükeniyor. IPv6, IPv4'ün halefidir. IPv6'nın çok daha büyük bir 128 bit adres alanı vardır.

IPv6'nın geliştirilmesi, IPv4 sınırlamaları ve diğer geliştirmeler için düzeltmeler de içeriyordu.

Artan internet nüfusu, sınırlı bir IPv4 adres alanı, NAT ve IoT ile ilgili sorunlar ile IPv6'ya geçişin zamanı geldi.

### 11.8.2.IPv4 ve IPv6 Birlikte Varlığı

Hem IPv4 hem de IPv6 yakın gelecekte bir arada olacak ve geçiş birkaç yıl sürecek.

IETF, ağ yöneticilerinin ağlarını IPv6'ya geçirmelerine yardımcı olmak için çeşitli protokoller ve araçlar oluşturmuştur. Bu göç teknikleri üç kategoriye ayrılabilir:

Dual stack -Aygıtlar hem IPv4 hem de IPv6 protokol yığınlarını aynı anda çalıştırır.

Tunneling – IPv6 paketini bir IPv4 ağı üzerinden taşıma yöntemi. IPv6 paketi bir IPv4 paketinin içinde kapsüllenir.

Translation - Ağ Adresi Çevirisi 64 (NAT64), IPv6 özellikli cihazların IPv4 için NAT'a benzer bir çeviri tekniği kullanarak IPv4 özellikli cihazlarla iletişim kurmasını sağlar.

## 11.9.IPv6 Adres Gösterimi

### 11.9.1.IPv6 Adres Formatı

IPv6 adresleri 128 bit uzunluğundadır ve onaltılık olarak yazılmıştır.

IPv6 adresleri büyük / küçük harfe duyarlı değildir ve küçük veya büyük harfle yazılabilir.

IPv6 adresi yazmak için tercih edilen biçim x: x: x: x: x: x: x: x'dir ve her "x" dört onaltılık (hekstet) değerden oluşur.

IPv6'da, bir onaltılık (hekstet), 16 bitlik veya dört onaltılık değere sahip bir segmenti belirtmek için kullanılan resmi olmayan terimdir.

Tercih edilen biçimde IPv6 adreslerine örnekler:

```
2001:0db8:0000:1111:0000:0000:0000:0200
2001:0db8:0000:00a3:abcd:0000:0000:1234
```

## 11.9.2.Sadeleştirme Kuralları

#### Kural 1 - Baştaki Sıfırı At

IPv6 adreslerinin gösterimini azaltmaya yardımcı olan ilk kural, önde gelen 0'ları (sıfırlar) atlamaktır.

Örnekler:

01ab, 1ab olarak gösterilebilir

09f0, 9f0 olarak gösterilebilir

0a00, a00 olarak gösterilebilir

00ab ab olarak gösterilebilir

Not: Bu kural yalnızca baştaki 0'lar için geçerlidir, arkadaki 0'lar için DEĞİLDİR, aksi takdirde adres belirsiz olacaktır.

Licensed to yekin karasungur, yekinkrsngr@gmail.com

| Type | Format |
|---|---|
| Preferred | 2001 : **0**db8 : **000**0 : 1111 : **000**0 : **000**0 : **000**0 : **0**200 |
| No leading zeros | 2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200 |

### Kural 2 - Çift Kolon

Bir çift kolon (::) tüm sıfırlardan oluşan bir veya daha fazla 16 bit hextet'in tek, bitişik dizesinin yerini alabilir.
Örnek:
2001:db8:cafe:1:0:0:0:1 (baştaki 0'lar atlandı) 2001:db8:cafe:1::1 olarak gösterilebilir.

Not: Çift kolon (: :) bir adres içinde yalnızca bir kez kullanılabilir, aksi takdirde birden fazla olası adres olabilir.

| Type | Format |
|---|---|
| Preferred | 2001 : **0**db8 : **000**0 : 1111 : **0000** : **0000** : **0000** : **0**200 |
| Compressed | 2001:db8:0:1111::200 |

## Alıştırmalar:

| Preferred format | fe80 | 0000 | 0000 | 0000 | 6678 | 9101 | 0000 | 34ab |
|---|---|---|---|---|---|---|---|---|
| Omit leading zeroes | fe80 | 0 | 0 | 0 | 6678 | 9101 | 0 | 34ab |
| Compressed format | fe80::6678:9101:0:34ab | | | | | | | |

| Preferred format | 2001 | 0db8 | 0000 | 1234 | 5678 | 9101 | 1112 | 1113 |
|---|---|---|---|---|---|---|---|---|
| Omit leading zeroes | 2001 | db8 | 0 | 1234 | 5678 | 9101 | 1112 | 1113 |
| Compressed format | 2001:db8::1234:5678:9101:1112:1113 | | | | | | | |

| Preferred format | 2001 | 0000 | 0db8 | 1111 | 0000 | 0000 | 0000 | 0200 |
|---|---|---|---|---|---|---|---|---|
| Omit leading zeroes | 2001 | 0 | db8 | 1111 | 0 | 0 | 0 | 200 |
| Compressed format | 2001:0:db8:1111::200 | | | | | | | |

| Preferred format | fe80 | 0000 | 0000 | 0000 | 0000 | 0000 | 0101 | 1111 |
|---|---|---|---|---|---|---|---|---|
| Omit leading zeroes | fe80 | 0 | 0 | 0 | 0 | 0 | 101 | 1111 |
| Compressed format | fe80::101:1111 | | | | | | | |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.10.IPv6 Adres Tipleri

### 11.10.1.Unicast, Multicast, Anycast

IPv6 adresleri üç kategoride incelenebilir:

Unicast – Tek noktaya yayın, IPv6 etkin bir aygıttaki bir arabirimi benzersiz olarak tanımlar.

Multicast – Çok noktaya yayın, birden çok hedefe tek bir IPv6 paketi göndermek için kullanılır.

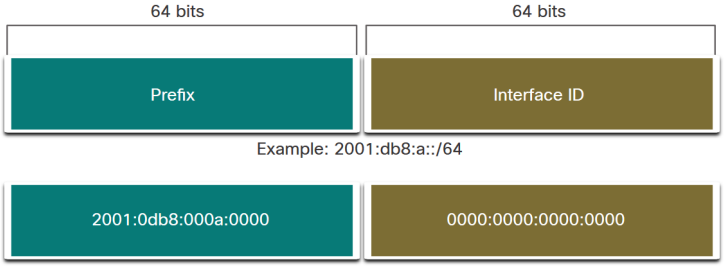
Anycast – Bu, birden fazla cihaza atanabilen herhangi bir IPv6 tek noktaya yayın adresidir. Herhangi bir yayın adresine gönderilen bir paket, bu adrese sahip en yakın cihaza yönlendirilir.

Not: IPv4'ün aksine, IPv6'nın bir yayın(broadcast) adresi yoktur. Ancak, esas olarak aynı sonucu veren bir IPv6 tüm düğümler çok noktaya yayın (all-nodes multicast address ) adresi vardır.

### 11.10.2.IPv6 Prefix Uzunluğu

Ön ek uzunluğu, eğik çizgi gösteriminde temsil edilir ve bir IPv6 adresinin ağ bölümünü belirtmek için kullanılır.

IPv6 önek uzunluğu 0 ila 128 arasında olabilir. LAN'lar ve diğer birçok ağ türü için önerilen IPv6 önek uzunluğu / 64'tür.



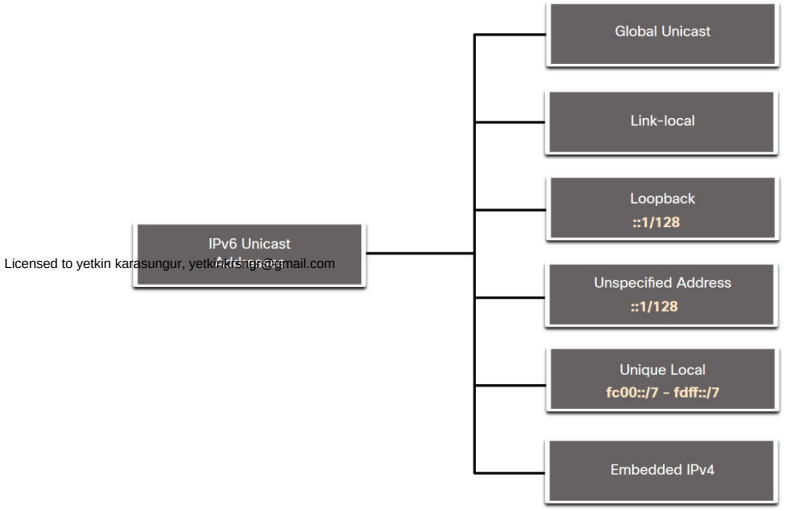

Not: Çoğu ağ için 64 bit Arayüz Kimliği kullanılması önemle tavsiye edilir. Bunun nedeni, durum bilgisi olmayan adres otomatik yapılandırmasının- stateless address autoconfiguration (SLAAC) Arabirim Kimliği için 64 bit kullanmasıdır. Ayrıca alt ağ oluşturmayı ve yönetmeyi kolaylaştırır.

### 11.10.3.Types of IPv6 Unicast Addresses-IPv6 Tek Noktaya Yayın Adresi Türleri

Yalnızca tek bir adresi olan IPv4 cihazlarının aksine, IPv6 adreslerinin genellikle iki tek noktaya yayın (unicast ) adresi vardır:

**Global Unicast Address (GUA)** – Bu, genel (public) bir IPv4 adresine benzer. Bunlar dünya çapında benzersiz, internete yönlendirilebilir adreslerdir.

**Link-local Address (LLA)** - IPv6 özellikli her aygıt için gereklidir ve aynı yerel bağlantıdaki diğer aygıtlarla iletişim kurmak için kullanılır. LLA'lar yönlendirilemez ve tek bir bağlantıyla sınırlıdır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.10.4Unique Local Address-Benzersiz Yerel Adres

**IPv6 benzersiz yerel adresleri (fc00 :: / 7 - fdff :: / 7 aralığı) IPv4 için RFC 1918 özel(private) adresleriyle benzerlik gösterir, ancak önemli farklılıklar vardır:**

- Benzersiz yerel adresler, bir site içinde veya sınırlı sayıda site arasında yerel adresleme için kullanılır.
- Benzersiz yerel adresler, asla başka bir ağa erişmesi gerekmeyen cihazlar için kullanılabilir.
- Benzersiz yerel adresler global olarak yönlendirilmez veya global bir IPv6 adresine çevrilmez.

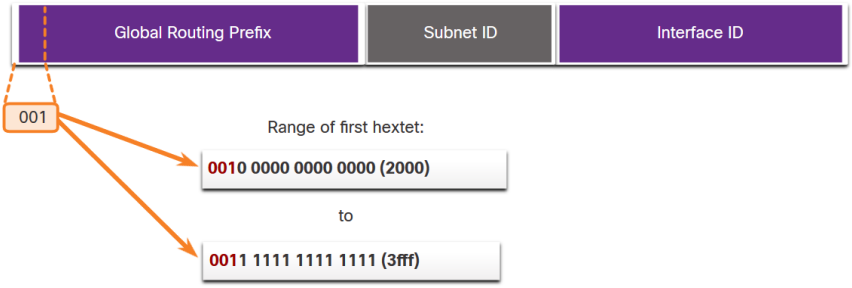
**Not**: Birçok site, ağlarını potansiyel güvenlik risklerinden korumak veya gizlemek için RFC 1918 adreslerinin özel niteliğini kullanır. Bu asla Unique Local Adreslerin kullanım amacı değildir.

## 11.10.5.IPv6 GUA

**IPv6 genel tek noktaya yayın adresleri (GUA'lar) genel olarak benzersizdir ve IPv6 internetinde yönlendirilebilir.**

Şu anda, yalnızca ilk üç biti 001 veya 2000 :: / 3 olan GUA'lar atanmaktadır.

Şu anda kullanılabilir olan GUA'lar ondalık 2 veya 3 ile başlar (Bu, kullanılabilir toplam IPv6 adres alanının yalnızca 1 / 8'i).




**Global Routing Prefix:**

Genel yönlendirme öneki, ISS gibi sağlayıcı tarafından atanan adresin müşteriye veya siteye önek veya ağ kısmıdır. Global yönlendirme öneki, ISS politikalarına bağlı olarak değişir.

**Subnet ID:**

Alt Ağ Kimliği alanı, Genel Yönlendirme Öneki ve Arabirim Kimliği arasındaki alandır. Alt Ağ Kimliği bir kuruluş tarafından kendi sitesindeki alt ağları tanımlamak için kullanılır.

**Interface ID:**

IPv6 arabirim kimliği, bir IPv4 adresinin ana bilgisayar bölümüne eşdeğerdir. Çoğu durumda 64 bit arabirim kimliği oluşturan /64 alt ağın kullanılması şiddetle önerilir.

## 11.10.6.IPv6 LLA

**IPv6 bağlantı yerel adresi (LLA), bir aygıtın aynı bağlantıdaki (alt ağ-subnet) diğer IPv6 etkin aygıtlarla iletişim kurmasını sağlar.**

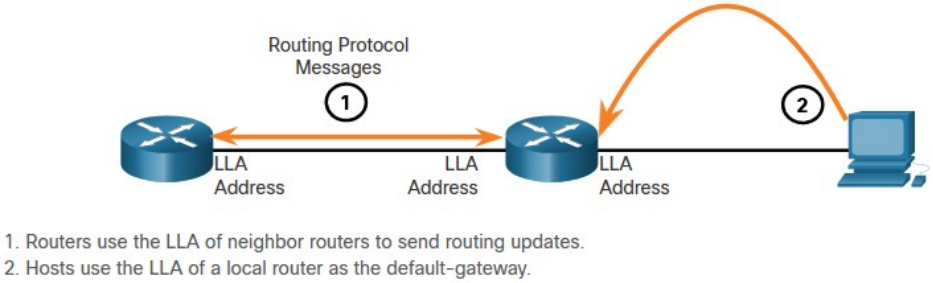
Kaynağı veya hedefi LLA olan paketler yönlendirilemez.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

IPv6 özellikli her ağ arabiriminin bir LLA'sı olmalıdır.

Bir LLA bir arabirimde manuel olarak yapılandırılmazsa, aygıt otomatik olarak bir tane oluşturur.

IPv6 LLA'lar fe80 :: / 10 aralığındadır.




## 11.11.GUA ve LLA Statik Yapılandırma

### 11.11.1.Yönlendiricideki Statik GUA Yapılandırması

**Cisco IOS'taki çoğu IPv6 yapılandırma ve doğrulama komutu, IPv4 benzerleri gibidir. Çoğu durumda, tek fark komutlar içinde ip yerine ipv6 kullanılmasıdır.**

Bir arabirimde IPv6 GUA'sını yapılandırma komutu: **ipv6 address** *ipv6-address/prefix-length.*

Örnek, R1'deki G0 / 0/0 arabiriminde bir GUA yapılandırmak için komutları gösterir:

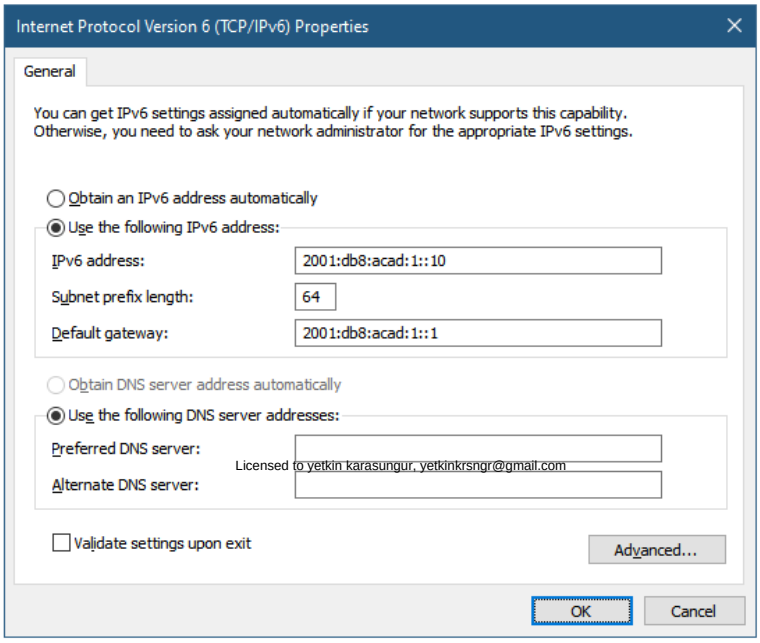
```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
```

### 11.11.2.Windows Ana Bilgisayarında Statik GUA Yapılandırması

IPv6 adresini bir ana bilgisayarda elle yapılandırmak, IPv4 adresini yapılandırmaya benzer.

Yönlendirici arayüzünün GUA veya LLA'sı varsayılan ağ geçidi olarak kullanılabilir. En iyi uygulama LLA kullanmaktır.

Not: DHCPv6 veya SLAAC kullanıldığında, yönlendiricinin LLA değeri otomatik olarak varsayılan ağ geçidi adresi olarak belirtilir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 11.11.3.Yerel Tek Noktaya Bağlantı Yayın Adresinin Statik GUA Yapılandırması

LLA'yı manuel olarak yapılandırmak, tanınabilir ve hatırlanması daha kolay bir adres oluşturmanıza olanak tanır.

LLA'lar **ipv6 address** *ipv6-link-local-address* **link-local** komutu kullanılarak el ile yapılandırılabilir.

Örnek, R1'deki G0 / 0/0 arabiriminde bir LLA yapılandırma komutlarını gösterir

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address fe80::1:1 link-local
R1(config-if)# no shutdown
R1(config-if)# exit
```

**Not**: Her bağlantıda aynı LLA, o bağlantıda benzersiz olduğu sürece yapılandırılabilir. Genel uygulama, yönlendiriciyi ve belirli arabirimi tanımlamayı kolaylaştırmak için yönlendiricinin her arabiriminde farklı bir LLA oluşturmaktır.

## 11.12.IPv6 GUA'ları için Dinamik Adresleme

### 11.12.1.RS ve RA Mesajları

**Aygıtlar, GUA adreslerini Internet Denetim İletisi Protokolü sürüm 6-Internet Control Message Protocol version 6(ICMPv6) iletileri aracılığıyla dinamik olarak alır.**

IPv6 yönlendiricilerini bulmak için ana bilgisayar aygıtları tarafından Yönlendirici İstemi-Router Solicitation(RS) iletileri gönderilir

Yönlendirici Tanıtım-Router Advertisement (RA) iletileri, bir IPv6 GUA'ı nasıl edineceklerine ve aşağıdakiler gibi yararlı ağ bilgileri sağlama konusunda ana bilgisayarları bilgilendirmek için yönlendiriciler tarafından gönderilir:

- Network prefix ve prefix length
- Default gateway address
- DNS addresses ve domain name

RA, IPv6 GUA yapılandırmak için üç yöntem sağlayabilir:

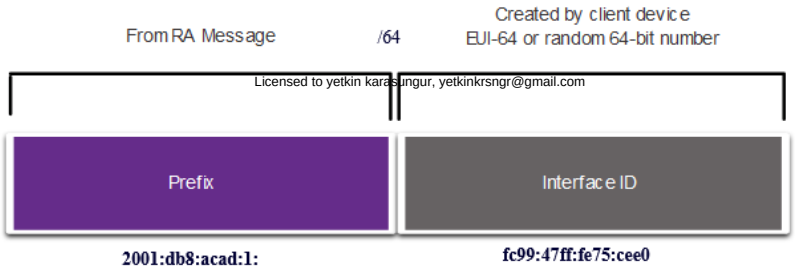
- SLAAC
- SLAAC with stateless DHCPv6 server
- Stateful DHCPv6 (no SLAAC)

### Yöntem 1: SLAAC

SLAAC, bir cihazın DHCPv6 hizmetleri olmadan bir GUA yapılandırmasına izin verir.

Aygıtlar, yerel yönlendiricinin ICMPv6 RA iletilerinden bir GUA yapılandırmak için gerekli bilgileri alır.

Ön ek RA tarafından sağlanır ve aygıt bir arabirim kimliği oluşturmak için EUI-64 veya rasgele oluşturma yöntemini kullanır.



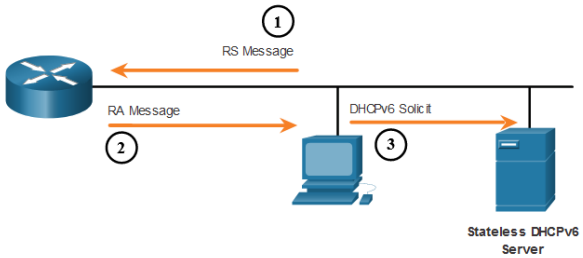

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Yöntem 2: SLAAC ve Stateless DHCP

**Bir RA, bir aygıta hem SLAAC hem de durumsuz-Stateless DHCPv6 kullanmasını söyleyebilir.**

RA mesajı, cihazların aşağıdakileri kullanmasını önerir:

- SLAAC kendi IPv6 GUA'sını oluşturacak
- Varsayılan ağ geçidi adresi olarak RA kaynağı IPv6 adresi olan yönlendirici LLA
- DNS sunucusu adresi ve etki alanı adı (domain name) gibi diğer bilgileri almak için durum bilgisi olmayan bir DHCPv6 sunucusu



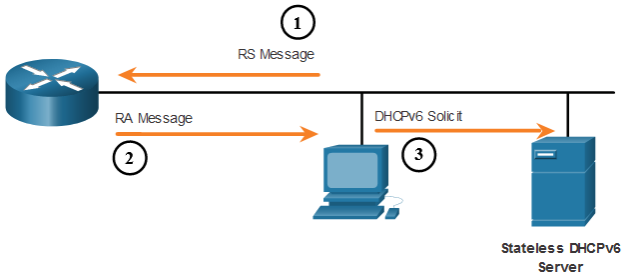

## Yöntem 3: Stateful DHCPv6

**RA, bir aygıta yalnızca durum bilgisi olan DHCPv6 kullanmasını söyleyebilir.**

Durum bilgisi olan DHCPv6, IPv4 için DHCP'ye benzer. Bir aygıt, durum bilgisi olan bir DHCPv6 sunucusundan otomatik olarak bir GUA, önek uzunluğu ve DNS sunucularının adreslerini alabilir.

RA mesajı, cihazların aşağıdakileri kullanmasını önerir:

- Varsayılan ağ geçidi adresi için RA kaynağı IPv6 adresi olan yönlendirici LLA.
- GUA, DNS sunucusu adresi, etki alanı adı ve diğer gerekli bilgileri almak için durum bilgisi olan bir DHCPv6 sunucusu.




## 11.12.2.EUI-64 Process vs. Randomly Generated-EUI-64 Süreci ve Rastgele Üretilmesi

RA iletisi, durum bilgisi olmayan DHCPv6'ya sahip SLAAC veya SLAAC olduğunda, istemcinin kendi arabirim kimliğini oluşturması gerekir.

Arabirim kimliği EUI-64 işlemi veya rasgele oluşturulmuş 64 bit sayı kullanılarak oluşturulabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

IEEE, aşağıdakileri gerçekleştiren Genişletilmiş Benzersiz Tanımlayıcı-Extended Unique Identifier (EUI) veya değiştirilmiş EUI-64 işlemini tanımladı:

İstemcinin 48 bit Ethernet MAC adresinin ortasına 16 bitlik bir değer (onaltılık olarak) eklenir.

İstemci MAC adresinin 7. biti ikili 0'dan 1'e çevrilir.

Örnek:

| | |
|---|---|
| 48-bit MAC | fc:99:47:75:ce:e0 |
| EUI-64 Interface ID | fe:99:47:ff:fe:75:ce:e0 |

İşletim sistemine bağlı olarak, aygıt MAC adresini ve EUI-64 işlemini kullanmak yerine rastgele oluşturulmuş bir arayüz kimliği kullanabilir. (mahremiyet sorunları)

Windows Vista'dan başlayarak, Windows EUI-64 ile oluşturulan yerine rasgele oluşturulmuş bir arayüz kimliği kullanır.

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
Default Gateway . . . . . : fe80::1
C:\>
```

Not: Herhangi bir IPv6 tek noktaya yayın adresinin benzersizliğini sağlamak için, istemci Yinelenen Adres Algılama-Duplicate Address Detection (DAD) olarak bilinen bir işlemi kullanabilir. Bu, kendi adresi için bir ARP isteğine benzer. Yanıt yoksa, adres benzersizdir.

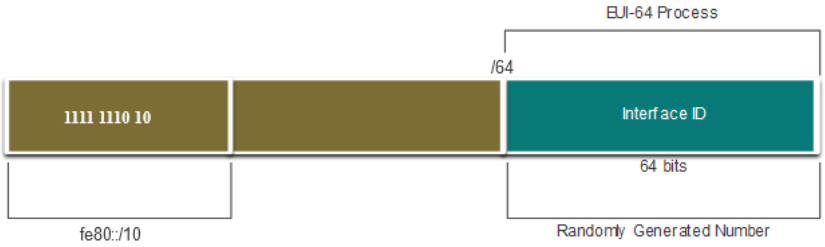
## 11.13.IPv6 LLA'lar için Dinamik Adresleme

### 11.13.1.Dynamic LLAs

Tüm IPv6 arabirimlerinde IPv6 LLA bulunmalıdır.

IPv6 GUA'lar gibi LLA'lar da dinamik olarak yapılandırılabilir.

Şekilde, LLA'nın EUI-64 işlemi veya rasgele oluşturulan 64 bit sayı kullanılarak fe80 :: / 10 öneki ve arabirim kimliği kullanılarak dinamik olarak oluşturulduğu gösterilmektedir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 11.13.2.Dynamic LLAs on Windows

Windows gibi işletim sistemleri, hem SLAAC tarafından oluşturulan bir GUA hem de dinamik olarak atanmış bir LLA için aynı yöntemi kullanır.

### EUI-64 Generated Interface ID:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:fc99:47ff:fe75:cee0
Link-local IPv6 Address . . . . . : fe80::fc99:47ff:fe75:cee0
Default Gateway . . . . . . . . . : fe80::1
C:\>
```

### Random 64-bit Generated Interface ID:

```
C:\> ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:50a5:8a35:a5bb:66e1
   Link-local IPv6 Address . . . . . : fe80::50a5:8a35:a5bb:66e1
   Default Gateway . . . . . . . . . : fe80::1
C:\>
```

### 11.13.3.Cisco Yönlendiricide Dynamic LLA

Cisco yönlendiricileri, arabirime bir GUA atandığında otomatik olarak bir IPv6 LLA oluşturur. Varsayılan olarak, Cisco IOS yönlendiricileri IPv6 arabirimlerindeki tüm LLA'ların arabirim kimliğini oluşturmak için EUI-64 kullanır.

R1'in G0 / 0/0 arayüzünde dinamik olarak yapılandırılmış bir LLA örneği:

```
R1# show interface gigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is ISR4221-2x1GE, address is 7079.b392.3640 (bia 7079.b392.3640)
(Output omitted)
R1# show ipv6 interface brief
GigabitEthernet0/0/0 [up/up]
FE80::7279:B3FF:FE92:3640
2001:DB8:ACAD:1::1
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 11.14.IPv6 Çok Noktaya Yayın Adresleri

### 11.14.1.Assigned IPv6 Multicast Addresses-Atanmış IPv6 Çok Noktaya Yayın Adresleri

IPv6 çok noktaya yayın adresleri ff00 :: / 8 önekine sahiptir. İki tür IPv6 çok noktaya yayın adresi vardır:

Well-Known multicast addresses-İyi bilinen çok noktaya yayın adresleri

Solicited node multicast addresses-İstenen düğüm çok noktaya yayın adresleri

Not: Çok noktaya yayın adresleri kaynak adresler değil, yalnızca hedef adresler olabilir.

#### Well-Known IPv6 Multicast Addresses

**İyi bilinen IPv6 çok noktaya yayın adresleri atanır ve önceden tanımlanmış aygıt grupları için ayrılmıştır.**

İki yaygın IPv6 Atanmış çok noktaya yayın grubu vardır:

**ff02::1 All-nodes multicast group** - Bu, IPv6 etkin tüm cihazların katıldığı çok noktaya yayın grubudur. Bu gruba gönderilen bir paket bağlantı veya ağdaki tüm IPv6 arabirimleri tarafından alınır ve işlenir.

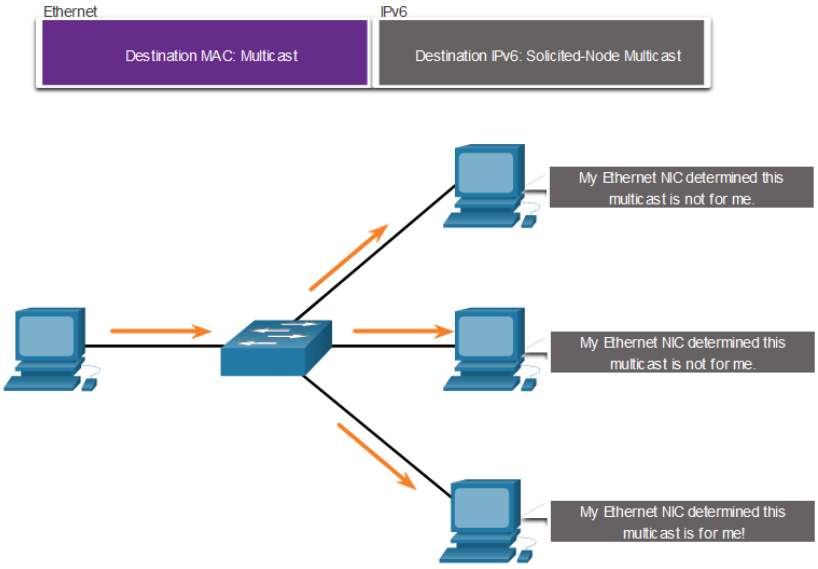
**ff02::2 All-routers multicast group** - Bu, tüm IPv6 yönlendiricilerinin katıldığı çok noktaya yayın grubudur. Bir yönlendirici, **ipv6 unicast-routing** genel yapılandırma komutuyla IPv6 yönlendiricisi olarak etkinleştirildiğinde bu grubun üyesi olur.

#### Solicited-Node IPv6 Multicast

İstenen düğüm çok noktaya yayın adresi, tüm düğümler çok noktaya yayın adresine benzer.

İstenen düğüm çok noktaya yayın adresi, özel bir Ethernet çok noktaya yayın adresine eşlenir.

Ethernet NIC, cihazın IPV6 paketinin amaçlanan hedefi olup olmadığını görmek için IPv6 işlemine göndermeden hedef MAC adresini inceleyerek çerçeveyi filtreleyebilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

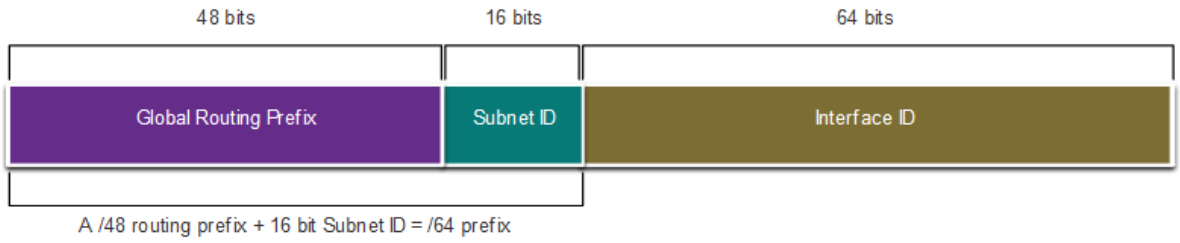
## 11.15.IPv6 Ağlarda Subnetting

### 11.15.1.Subnet Kimliğini (Subnet ID) Kullanma

IPv6, alt ağlar göz önünde bulundurularak tasarlanmıştır.

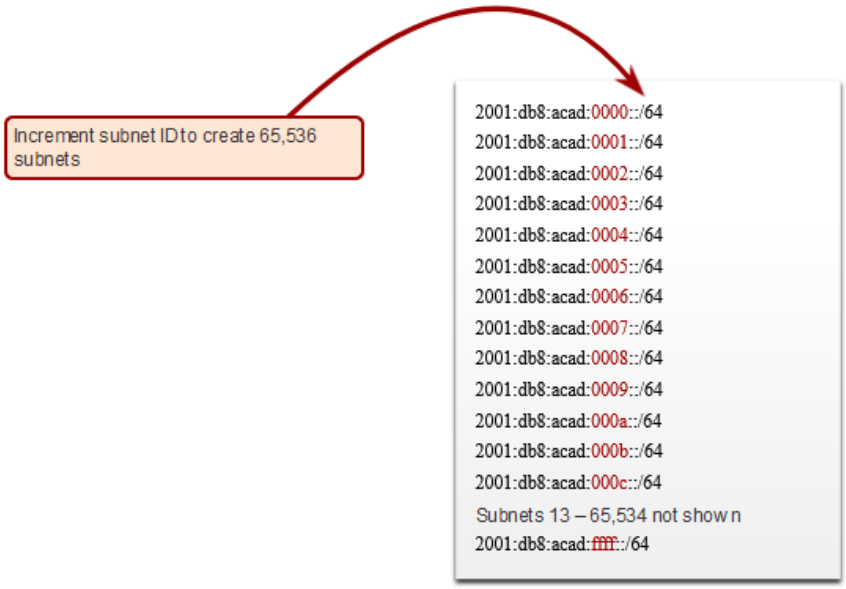
Alt ağlar oluşturmak için IPv6 GUA'sında ayrı bir alt ağ kimliği alanı kullanılır.

Alt ağ kimliği alanı, Genel Yönlendirme Öneki ve arayüz kimliği arasındaki alandır.




**Örnek:** 2001:db8:acad::/48 küresel yönlendirme öneki 16 bit subnet kimliği ile verildiğinde

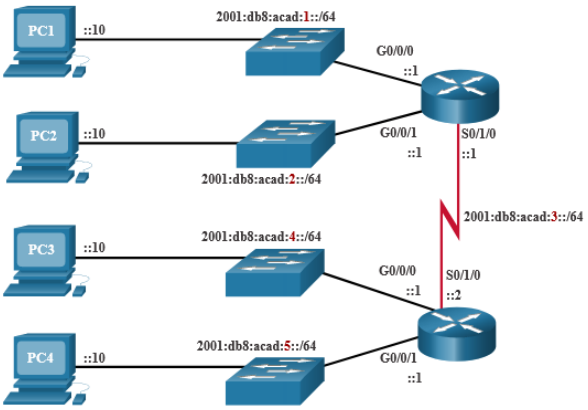
- 65.536/64 alt ağa izin verir
- Genel yönlendirme öneki tüm alt ağlar için aynıdır.
- Her alt ağ için yalnızca alt ağ kimliği onaltılık değeri, onaltılı olarak artar.

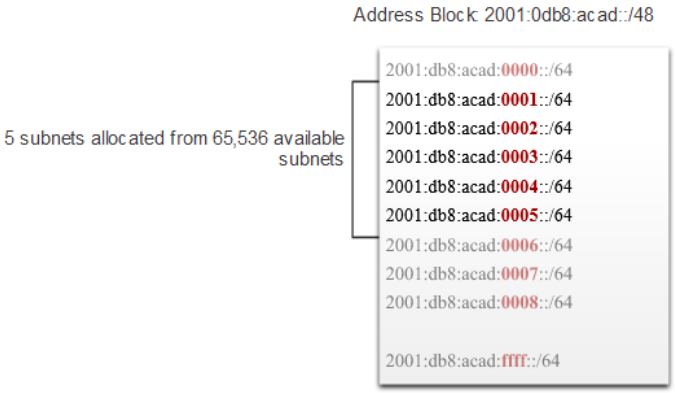



Aşağıdaki örnek topoloji, her bir LAN için ve R1 ile R2 arasındaki seri bağlantı için bir tane olmak üzere beş alt ağ gerektirir.

Beş IPv6 alt ağı, 0001 ila 0005 alt ağ kimliği alanı ile ayrılmıştır. Her / 64 alt ağı, gerekenden daha fazla adres sağlayacaktır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Örnek, R1'deki yönlendirici arabirimlerinin her birinin farklı bir IPv6 alt ağında olacak şekilde yapılandırıldığını gösterir.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/1/0
R1(config-if)# ipv6 address 2001:db8:acad:3::1/64
R1(config-if)# no shutdown
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 12.Bölüm: ICMP(Internet Control Message Protocol)

## 12.1.ICMP Mesajları

### 12.1.1.ICMPv4 ve ICMPv6 Mesajları

Internet Denetim İletisi Protokolü-Internet Control Message Protocol ( (ICMP), belirli koşullarda IP paketlerinin işlenmesiyle ilgili sorunlar hakkında geri bildirim sağlar.

ICMPv4, IPv4 için mesajlaşma protokolüdür. ICMPv6, IPv6 için mesajlaşma protokolüdür ve ek işlevler içerir.

Hem ICMPv4 hem de ICMPv6 için ortak ICMP iletileri şunları içerir:

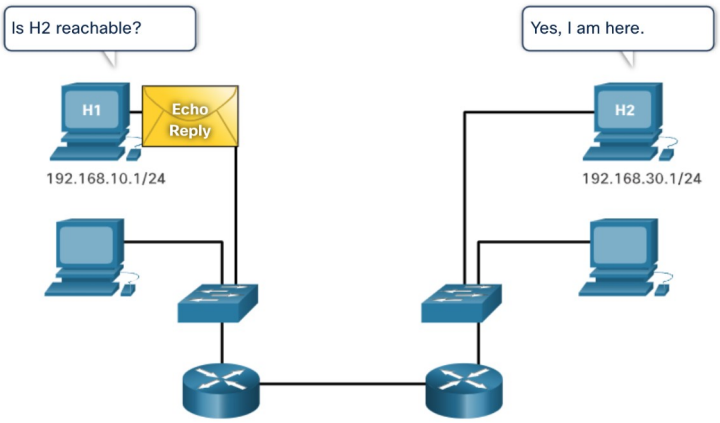
- Host reachability-Host Erişilebilirliği
- Destination or Service Unreachable-Hedef veya Hizmete Erişilemiyor
- Time exceeded-Zaman aşıldı (İstek zaman aşımına uğradı)

Not: ICMPv4 iletileri gerekli değildir ve güvenlik nedeniyle bir ağda genellikle izin verilmez. Örneğin Windows işletim sisteminde ICMP yankı isteğine cevap dönmez. Güenlik duvarından açmak gerekir.

### 12.1.2.Host Reachability

ICMP Yankı İletisi-ICMP Echo Message, bir IP ağındaki bir ana bilgisayarın ulaşılabilirliğini test etmek için kullanılabilir.

Örnekte:Yerel ağda bir bilgisayar, başka bir bilgisayara ICMP Yankı İsteği-ICMP Echo Request gönderir. Hedef bilgisayar ulaşılabilir durumdaysa, Yankı Yanıtı-Echo Reply. ile yanıt verir.




### 12.1.3.Destination or Service Unreachable

Bir hedefe veya hizmete erişilemez olduğunu bildirmek için bir ICMP Hedef Ulaşılamıyor-ICMP Destination Unreachable iletisi kullanılabilir.

ICMP mesajı, paketin neden teslim edilemediğini gösteren bir kod içerecektir.

ICMPv4 için birkaç Hedef Erişilemeyen kodu aşağıdaki gibidir:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

0 - Net unreachable

1 - Host unreachable

2 - Protocol unreachable

3 - Port unreachable

### 12.1.4.Time Exceeded

Bir paketteki Yaşam Süresi-Time to Live (TTL) alanı 0'a düşürüldüğünde, kaynak ana bilgisayara bir ICMPv4 Zaman Aşıldı-Time Exceeded mesajı gönderilir.

ICMPv6 da Zaman Aşıldı mesajı gönderir. IPv4 TTL alanı yerine ICMPv6, paketin süresinin dolup dolmadığını belirlemek için IPv6 Atlama Sınırı-Hop Limit alanını kullanır.

```
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.
Reply from 192.168.1.1: TTL expired in transit.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Not: Zaman Aşıldı mesajları traceroute aracı tarafından kullanılır.

## 12.1.5.ICMPv6 Mesajları

ICMPv6, Komşu Keşif Protokolü'nün (Neighbor Discovery-ND veya NDP) bir parçası olarak dört yeni protokol de dahil olmak üzere ICMPv4'te bulunmayan yeni özelliklere ve gelişmiş işlevlere sahiptir.

IPv6 yönlendiricisi ile IPv6 aygıtı arasında dinamik adres ataması da dahil olmak üzere mesajlaşma aşağıdaki gibidir:

- Router Solicitation (RS) message
- Router Advertisement (RA) message

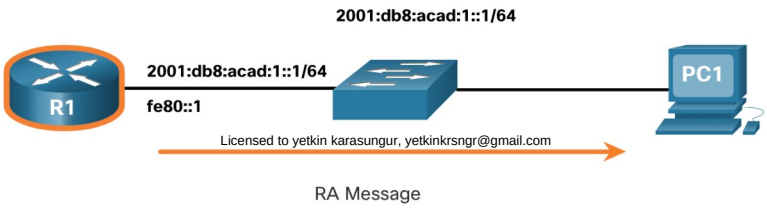
Yinelenen adres algılama ve adres çözünürlüğü dahil (IPV4 teki ARP gibi) IPv6 aygıtları arasındaki mesajlaşma aşağıdaki gibidir:

- Neighbor Solicitation (NS) message
- Neighbor Advertisement (NA) message

RA iletileri IPv6 etkin ana bilgisayarlara adres bilgileri sağlamak için her 200 saniyede IPv6 etkin yönlendiriciler tarafından gönderilir.

RA iletisi, ana bilgisayar için önek, önek uzunluğu, DNS adresi ve etki alanı adı gibi adres bilgilerini içerebilir.

Durum Bilgisi Olmayan Adres Otomatik Yapılandırma-Stateless Address Autoconfiguration (SLAAC) kullanan bir ana bilgisayar, varsayılan ağ geçidini, RA'yı gönderen yönlendiricinin bağlantı yerel adresine ayarlar.



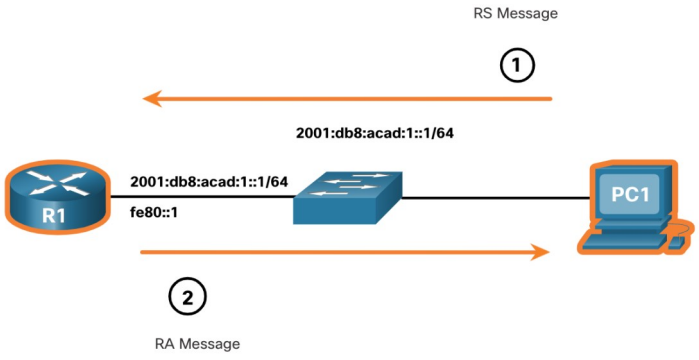
IPv6 özellikli bir yönlendirici de RS mesajına yanıt olarak bir RA mesajı gönderir.

Şekilde PC1, IPv6 adres bilgilerinin dinamik olarak nasıl alınacağını belirlemek için bir RS mesajı gönderir.

R1, RS'ye bir RA mesajıyla yanıt verir.

PC1 bir RS mesajı gönderir, “Merhaba, ağayeni katıldım. Ağda bir IPv6 yönlendirici var mı? IPv6 adres bilgilerimi nasıl dinamik olarak alacağımı bilmem gerekiyor. ”

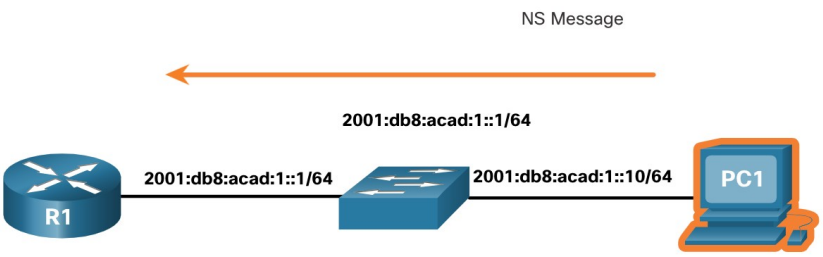
R1, bir RA mesajıyla yanıt verir. “Merhaba tüm IPv6 özellikli cihazlar. Ben R1 ve bir IPv6 genel tek noktaya yayın adresi oluşturmak için SLAAC kullanabilirsiniz. Önek 2001: db8: acad: 1 :: / 64'tür. Bu arada, varsayılan yerel ağ geçidi olarak fe80 :: 1 bağlantı yerel adresimi kullan. "




Genel bir IPv6 tek noktaya yayın veya  yerel bağlantı (link local) tek noktaya yayın adresi atanmış bir aygıt, IPv6 adresinin benzersiz olmasını sağlamak için çift(yinelenen) adres algılama-duplicate address detection  (DAD) gerçekleştirebilir.

Bir adresin benzersizliğini kontrol etmek için, cihaz hedef IPv6 adresi olarak kendi IPv6 adresine sahip bir NS mesajı gönderir.

Ağdaki başka bir aygıt bu adrese sahipse, gönderen aygıta adresin kullanımda olduğunu bildiren bir NA iletisi ile yanıt verir.



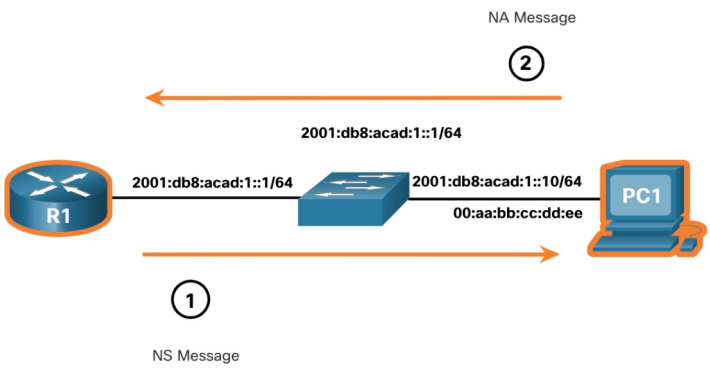

Not: DAD gerekli değildir, ancak RFC 4861, DAD'nin tek noktaya yayın-unicast adreslerinde gerçekleştirilmesini önerir.

Hedefin MAC adresini belirlemek için, cihaz istenen düğüm adresine bir NS mesajı gönderir.

Mesaj bilinen (hedeflenen) IPv6 adresini içerecektir. Hedeflenen IPv6 adresine sahip aygıt, Ethernet MAC adresini içeren bir NA mesajıyla yanıt verecektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Şekilde, R1, 2001: db8: acad: 1 :: 10'a MAC adresini soran bir NS mesajı gönderir. PC! De NA ile cevap verir.




## 12.2.Ping ve Traceroute Testleri

### 12.2.1.Ping – Bağlantı Testi

**Ping** komutu, ana bilgisayarlar arasındaki bağlantıyı test etmek için ICMP yankı isteği ve yankı yanıt mesajlarını kullanan ve hedefe başarı oranını ve ortalama gidiş-dönüş süresini içeren bir özet sunan bir IPv4 ve IPv6 test yardımcı programıdır.

Zaman aşımı süresi içinde bir yanıt alınmazsa, ping yanıt alınmadığını belirten bir mesaj sağlar.

ICMP Yankı İsteği gönderilmeden önce adres çözümlemesinin (ARP veya ND) yapılması gerekiyorsa, ilk ping için zaman aşımına uğraması yaygındır.

```
S1#ping 192.168.20.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.20.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

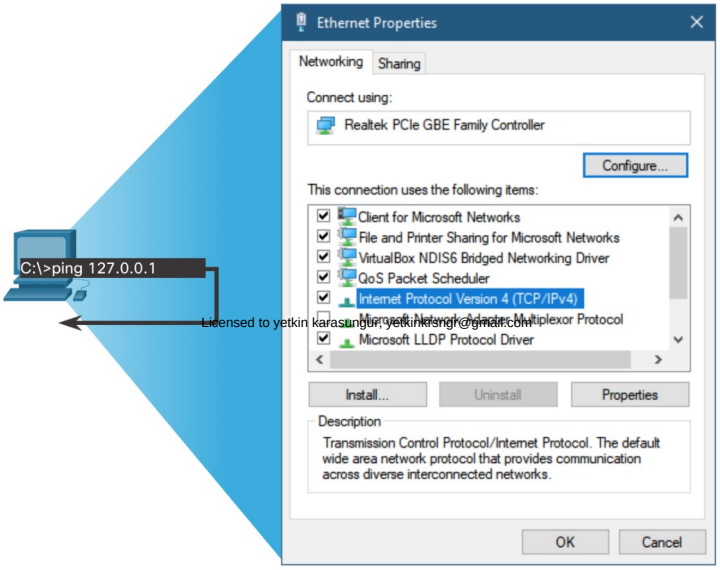
```
R1#ping 2001:db8:acad:1::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:db8:acad:1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms
```

### 12.2.2.Loopback (Geri Döngü) Adresine Ping

Ping, yerel ana bilgisayarda IPv4 veya IPv6'nın dahili yapılandırmasını test etmek için kullanılabilir. Bunu yapmak için, IPv4 için 127.0.0.1 yerel geri döngü adresine ping işlemi uygulayın (IPv6 için :: 1).

IPv4 için 127.0.0.1 veya IPv6 için :: 1 yanıtı, IP'nin ana bilgisayara düzgün bir şekilde yüklendiğini gösterir.

Bir hata mesajı, TCP / IP'nin ana bilgisayarda çalışmadığını gösterir.



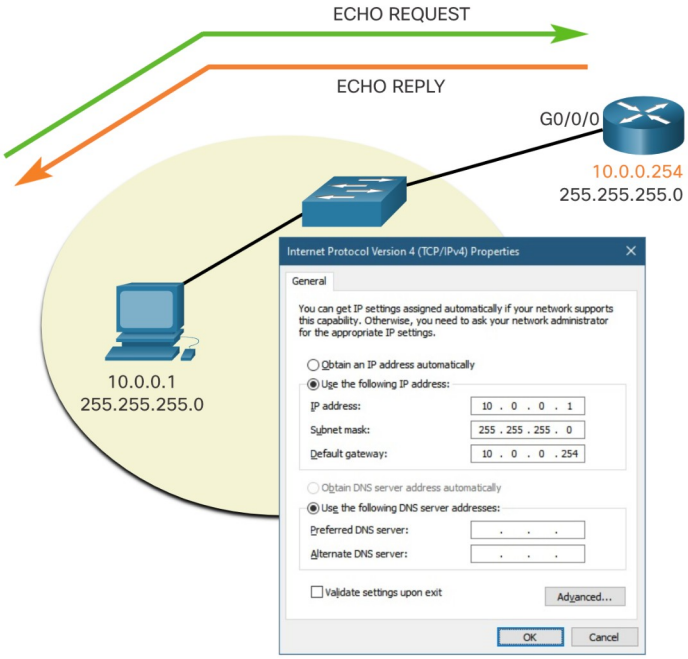
Licensed to yetkin karasungur, yetkinkesngr@gmail.com

## 12.2.3.Ping the Default Gateway-Varsayılan Ağ Geçidine Ping

Ping komutu, bir ana bilgisayarın yerel ağda iletişim kurma yeteneğini test etmek için kullanılabilir.

Varsayılan ağ geçidi adresi genellikle yönlendirici normalde her zaman çalışır durumda olduğundan kullanılır.

- Varsayılan ağ geçidine yapılan başarılı bir ping, varsayılan ağ geçidi olarak hizmet veren ana bilgisayarın ve yönlendirici arabiriminin her ikisinin de yerel ağda çalıştığını gösterir.
- Varsayılan ağ geçidi adresi yanıt vermezse, yerel ağda çalıştığı bilinen başka bir ana bilgisayarın IP adresine bir ping gönderilebilir.

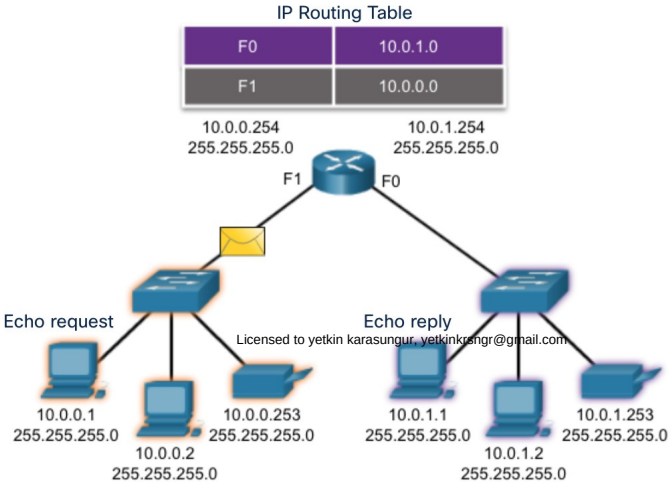



## 12.2.4.Ping a Remote Host-Uzak Hosta Ping

Ping, yerel bir ana bilgisayarın uzak bir ağ üzerinden(İnternet) iletişim kurma yeteneğini test etmek için de kullanılabilir.

Yerel bir ana makine, uzak ağdaki bir ana bilgisayara ping atabilir. Ağ üzerinde başarılı bir ping işlemi uzak ağdaki host ile arasındaki iletişimi doğrular.

**Not**: Birçok ağ yöneticisi ICMP iletilerinin girişini sınırlar veya yasaklar, bu nedenle ping yanıtının olmaması güvenlik kısıtlamalarından kaynaklanabilir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 12.2.5. Traceroute – Yol Testi

Traceroute (tracert), iki ana bilgisayar arasındaki yolu test etmek ve bu yol boyunca başarıyla ulaşılan atlamaların(hop) bir listesini sağlamak için kullanılan bir yardımcı programdır.

Traceroute, yol boyunca her bir sıçrama için gidiş-dönüş süresi sağlar ve bir atlamanın yanıt veremediğini gösterir. Kaybolan veya yanıtlanmamış bir paketi belirtmek için yıldız işareti (*) kullanılır.

Bu bilgiler, yoldaki sorunlu bir yönlendiriciyi bulmak için kullanılabilir veya yönlendiricinin yanıt vermeyecek şekilde yapılandırıldığını gösterebilir.

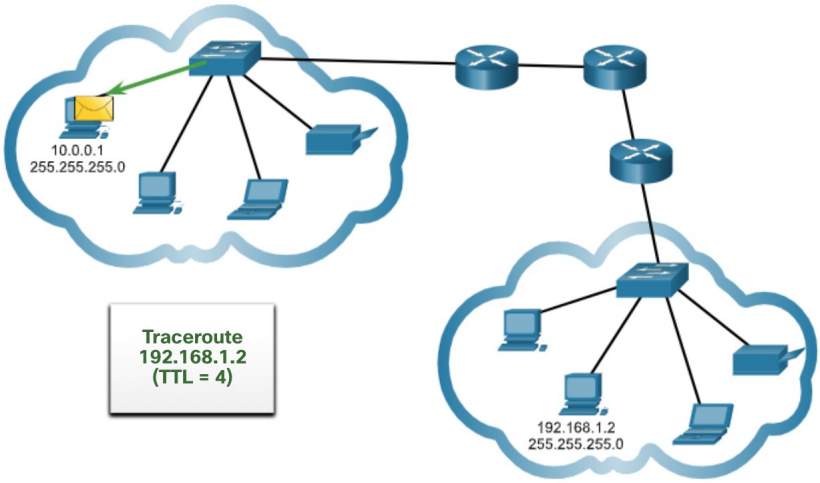
```
R1#traceroute 192.168.40.2
Type escape sequence to abort.
Tracing the route to 192.168.40.2

  1   192.168.10.2    1 msec    0 msec    0 msec
  2   192.168.20.2    2 msec    1 msec    0 msec
  3   192.168.30.2    1 msec    0 msec    0 msec
  4   192.168.40.2    0 msec    0 msec    0 msec
```

Not: Traceroute, Katman 3 üstbilgilerinde IPv4'teki TTL alanının ve IPv6'daki Atlama Sınırı-Hop Limit alanının işlevini ve ICMP Zaman Aşıldı-Time Exceeded iletisini kullanır.

Traceroute'tan gönderilen ilk iletinin TTL alan değeri 1 olacaktır. Bu, TTL'nin ilk yönlendiricide zaman aşımına uğramasına neden olur. Bu yönlendirici daha sonra ICMPv4 Zaman Aşıldı iletisiyle yanıt verir.

Traceroute daha sonra her bir mesaj dizisi için TTL alanını (2, 3, 4 ...) aşamalı olarak artırır. Bu, paketler yolda daha fazla zaman aşımına uğradığından iz (trace) her atlamanın adresini sağlar.

TTL alanı hedefe ulaşılana kadar artırılmaya devam eder veya önceden belirlenmiş bir maksimum değere artırılır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 13.Bölüm: Taşıma Katmanı

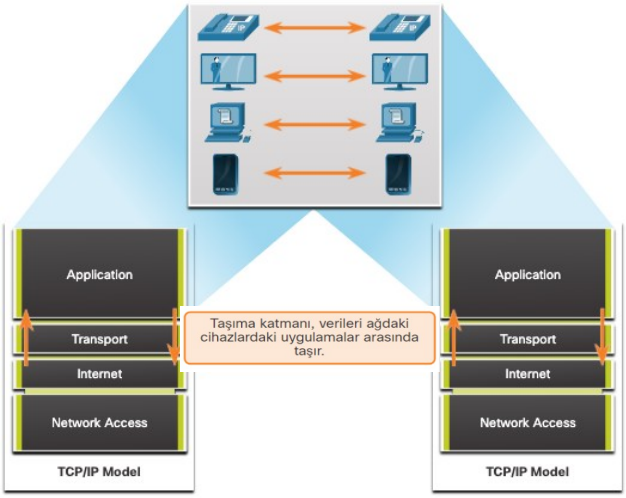
## 13.1.Verilerin Taşınması

### 13.1.1.Taşıma Katmanının Rolü

Taşıma katmanı:

Farklı ana bilgisayarlarda çalışan uygulamalar arasındaki mantıksal iletişimden sorumludur.

Uygulama katmanı ve ağ aktarımından sorumlu olan alt katmanlar arasındaki bağlantı sağlar.




### 13.1.2.Taşıma Katmanı Sorumlulukları

Taşıma katmanı aşağıdaki sorumluluklara sahiptir:

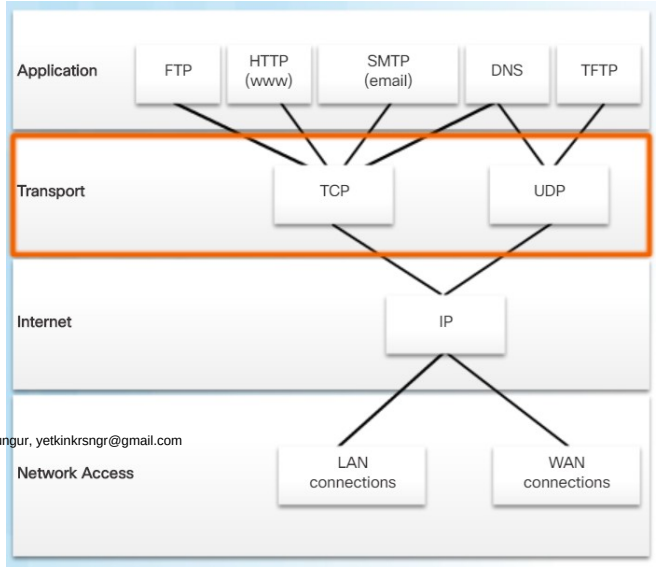
- Tek tek görüşmeleri izleme
- Verileri bölümlere ayırma ve segmentleri yeniden birleştirme
- Başlık bilgisi ekler
- Birden fazla konuşmayı tanımlar, ayırır ve yönetir
- Aynı ağda farklı iletişim konuşmalarının araya eklenmesi için segmentasyon ve çoklama kullanır

### 13.1.3.Taşıma Katmanı Protokolleri

IP, paketlerin teslimatının veya taşınmasının nasıl gerçekleştiğini belirtmez.

Aktarım katmanı protokolleri iletilerin ana bilgisayarlar arasında mesajların nasıl aktarılacağını belirler ve bir konuşmanın güvenilirlik gereksinimlerini yönetmekle sorumludur.

Aktarım katmanı TCP ve UDP protokollerini içerir.

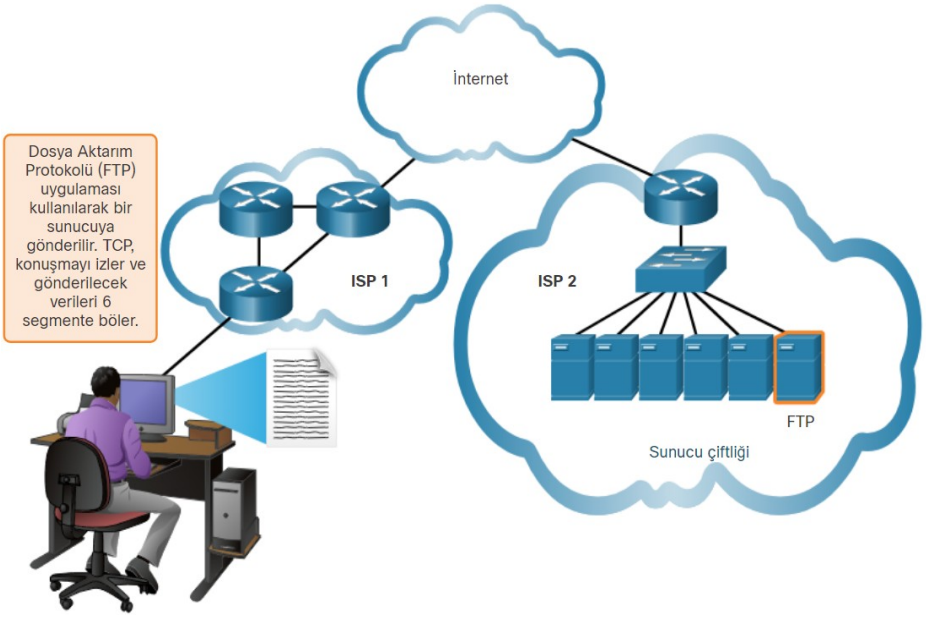



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 13.1.4.Transmission Control Protocol(TCP)

TCP güvenilirlik ve akış kontrolü sağlar. TCP temel işlemleri:

- Belirli bir uygulamadan belirli bir ana bilgisayara aktarılan veri segmentlerinin numaralandırma ve izleme
- Alınan verileri onaylama
- Onaylanmamış verileri belirli bir süre sonra yeniden iletme
- Yanlış sırada gelebilecek verileri sıralama
- Alıcı tarafından kabul edilebilir verimli bir hızda veri gönderme

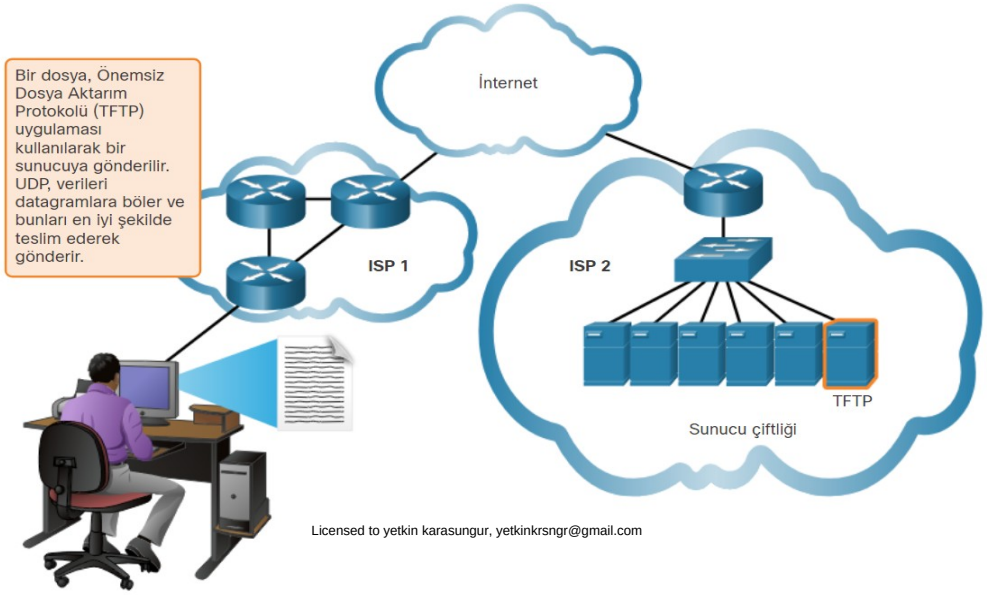



## 13.1.5.User Datagram Protocol (UDP)

UDP, uygun uygulamalar arasında çok az ek yük ve veri kontrolü ile datagramları taşımak için temel işlevleri sağlar.

UDP bağlantısız bir protokoldür.

UDP en iyi çaba dağıtım protokolü olarak bilinir, çünkü verinin hedefe ulaştığına dair bir bildirim yoktur.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 13.1.6.Doğru Uygulama için Doğru Taşıma Katmanı Protokolü

Bazı uygulamalar ağ üzerinden iletim sırasında bazı veri kayıplarını tolere edebilir, ancak iletimdeki gecikmeler kabul edilemez. Bu uygulamalar için UDP daha iyi bir seçimdir çünkü daha az ağ ek yükü gerektirir. IP üzerinden Ses (VoIP) gibi uygulamalar için UDP tercih edilir. Onaylar ve yeniden iletim, iletimi yavaşlatır ve sesli konuşmayı kabul edilemez hale getirir.

UDP, verilerin minimum düzeyde olduğu ve yeniden iletimin hızlı bir şekilde yapılabildiği istek ve yanıt uygulamaları tarafından da kullanılır. Örneğin, alan adı hizmeti (DNS) bu tür işlem için UDP kullanır. İstemci, bir DNS sunucusundan bilinen bir alan adı için IPv4 ve IPv6 adreslerini ister. İstemci önceden belirlenmiş bir süre içinde yanıt almazsa, talebi tekrar gönderir.

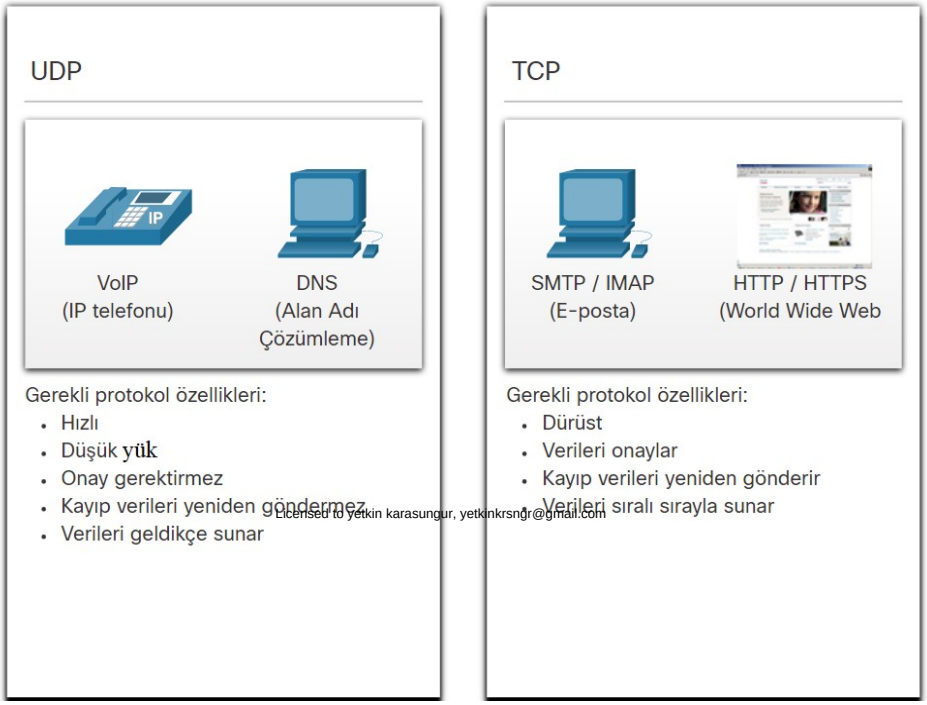
Örneğin, bir canlı video akışının bir veya iki bölümü ulaşamazsa, akışta anlık bir kesinti yaratır. Bu, görüntüde veya seste bozulma olarak görünebilir, ancak kullanıcı tarafından fark edilmeyebilir. Hedef cihazın kayıp verileri hesaba katması gerekiyorsa, yeniden iletimler beklerken akış gecikebilir ve bu nedenle görüntü veya sesin büyük ölçüde bozulmasına neden olabilir. Bu durumda, alınan segmentlerle mümkün olan en iyi medyayı oluşturmak ve güvenilirlikten vazgeçmek daha iyidir.

Diğer uygulamalar için, tüm verilerin ulaşması ve doğru sırada işlenebilmesi önemlidir. Bu tür uygulamalar için, taşıma protokolü olarak TCP kullanılır. Örneğin, veritabanları, web tarayıcıları ve e-posta istemcileri gibi uygulamalar, gönderilen tüm verilerin hedefe orijinal durumunda ulaşmasını gerektirir. Eksik herhangi bir veri bir iletişimi bozarak onu eksik veya okunamaz hale getirebilir. Örneğin, web üzerinden bankacılık bilgilerine erişirken tüm bilgilerin doğru bir şekilde gönderilip alındığından emin olmak önemlidir.

Uygulama geliştiricileri, uygulamaların gereksinimlerine bağlı olarak hangi taşıma protokolü türünün uygun olduğunu seçmelidir. Video, TCP veya UDP üzerinden gönderilebilir. Depolanan ses ve video akışını sağlayan uygulamalar genellikle TCP kullanır. Uygulama, kullanıcı deneyimini daha iyi kontrol etmek için ara belleğe alma, bant genişliği araştırması ve tıkanıklık kontrolü gerçekleştirmek için TCP kullanır.

Gerçek zamanlı video ve ses genellikle UDP kullanır, ancak aynı zamanda TCP veya hem UDP hem de TCP kullanabilir. Bir video konferans uygulaması varsayılan olarak UDP kullanabilir, ancak birçok güvenlik duvarı UDP'yi engellediğinden, uygulama TCP üzerinden de gönderilebilir.

Depolanan ses ve video akışını sağlayan uygulamalar TCP kullanır. Örneğin, ağınız isteğe bağlı bir filmi izlemek için gereken bant genişliğini aniden destekleyemezse, uygulama kayıttan yürütmeyi duraklatır. Duraklatma sırasında, TCP akışı yeniden kurmak için çalışırken bir "arabelleğe alınıyor ..." mesajı görebilirsiniz. Tüm segmentler sırayla olduğunda ve minimum bant genişliği geri yüklendiğinde, TCP oturumunuz devam eder ve film oynatılmaya devam eder.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 13.2.TCP'ye Genel Bakış

### 13.2.1.TCP Özellikleri

**Establishes a Session - Bir Oturum Oluşturur** - TCP, herhangi bir trafiği iletmeden önce kaynak ve hedef cihazlar arasında müzakere eden ve kalıcı bir bağlantı (veya oturum) oluşturan bağlantı odaklı bir protokoldür.

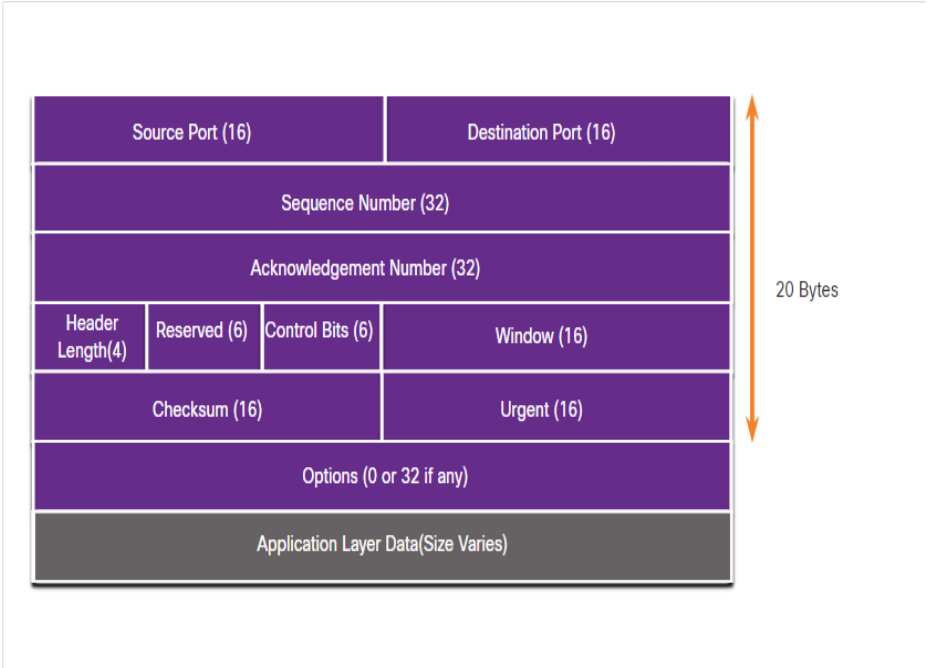
**Ensures Reliable Delivery - Güvenilir Teslimatı Sağlar** - Birçok nedenden dolayı, bir segmentin ağ üzerinden iletildiği için tamamen bozulması veya kaybolması mümkündür. TCP, kaynak tarafından gönderilen her bölümün hedefe ulaşmasını sağlar.

**Provides Same-Order Delivery – Aynı-Sırayla Teslimatı Sağlar** - Ağlar farklı iletim hızlarına sahip olabilen birden fazla rota sağlayabildiğinden, veriler yanlış sırada gelebilir.

**Supports Flow Control - Akış Kontrolünü Destekler -** Ağ ana bilgisayarlarının sınırlı kaynakları vardır (yani, bellek ve işlem gücü). TCP, bu kaynakların fazlakullanıldığının farkında olduğunda, gönderen uygulamanın veri akış hızını azaltmasını isteyebilir.

### 13.2.2.TCP  Header-TCP Başlığı

TCP, iletişim oturumunun durumunu izlediği anlamına gelen özel bir protokoldür. TCP hangi bilgileri gönderdiğini ve hangi bilgilerin kabul edildiğini kaydeder. Bir TCP segmenti, uygulama katmanı verilerini kapsüllerken 20 bayt (yani 160 bit) ek yük ekler. Şekil, bir TCP başlığındaki alanları göstermektedir.



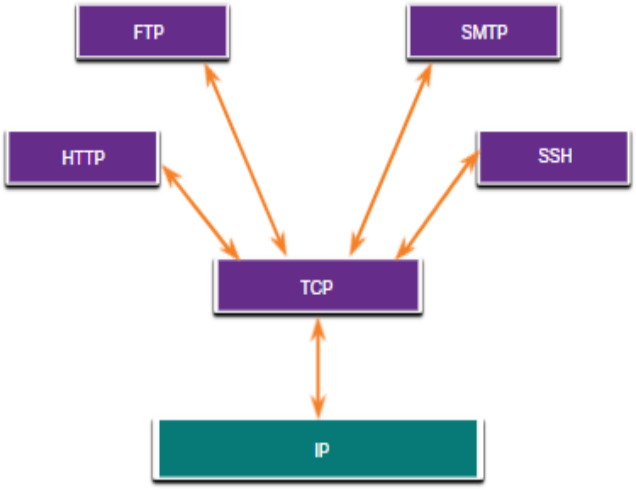

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 13.2.3.TCP Başlık Alanları

| TCP Header Field | Description |
|---|---|
| **Source Port** | Kaynak uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bit alan. |
| **Destination Port** | Hedef uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bit alan. |
| **Sequence Number** | Verilerin yeniden birleştirilmesi amacıyla kullanılan 32 bitlik alan. |
| **Acknowledgment Number** | Verilerin alındığını ve kaynaktan sonraki baytın beklendiğini belirtmek için kullanılan 32 bit alan. |
| **Header Length** | TCP segmenti başlığının uzunluğu gösterir "data offset" olarak bilinen bir 4-bit alandır. |
| **Reserved** | Gelecekte kullanılmak üzere ayrılmış 6 bitlik bir alan. |
| **Control bits** | TCP segmentinin amacını ve işlevini gösteren bit kodlarını veya bayrakları içeren 6 bitlik bir alan kullanılır. |
| **Window size** | Bir kerede kabul edilebilecek bayt sayısını belirtmek için kullanılan 16 bit alan. |
| **Checksum** | Segment başlığı ve verilerinin hata kontrolü için kullanılan 16 bit alan. |
| **Urgent** | İçerdiği verilerin acil olup olmadığını belirtmek için kullanılan 16 bitlik bir alan. |

### 13.2.4.TCP Kullanan Uygulamalar

TCP, TCP / IP protokol paketinin farklı katmanlarının nasıl belirli rollere sahip olduğuna dair iyi bir örnektir. TCP, veri akışını segmentlere bölmek, güvenilirlik sağlamak, veri akışını kontrol etmek ve segmentleri yeniden düzenlemekle ilişkili tüm görevleri yerine getirir. TCP, uygulamayı bu görevlerden herhangi birini yönetme zorunluluğundan kurtarır. Şekilde gösterilenler gibi uygulamalar, basitçe veri akışını taşıma katmanına gönderebilir ve TCP hizmetlerini kullanabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 13.3.UDP'ye Genel Bakış

### 13.3.1.UDP Özellikleri

UDP'nin özellikleri şunlardır:

- Veriler alınma sırasına göre yeniden oluşturulur.
- Kaybolan segmentler yeniden gönderilmez.
- Oturum kuruluşu yoktur.
- Gönderen, kaynakların kullanılabilirliği hakkında bilgilendirilmez.

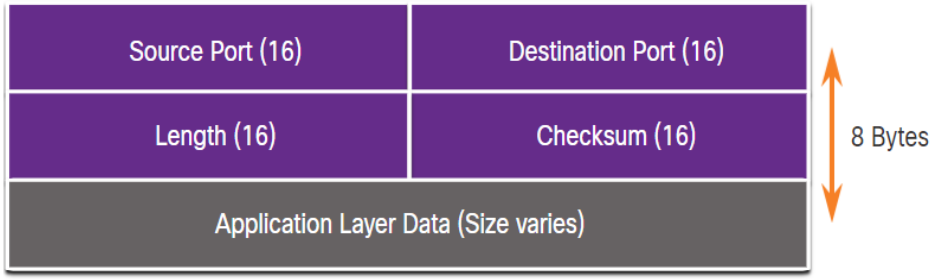
### 13.3.2.UDP Başlığı

UDP, durum bilgisiz bir protokoldür, yani ne istemci ne de sunucu iletişim oturumunun durumunu takip etmez. Taşıma protokolü olarak UDP kullanılırken güvenilirlik gerekiyorsa, uygulama tarafından ele alınmalıdır.

Ağ üzerinden canlı video ve ses iletmenin en önemli gereksinimlerinden biri, verilerin hızla akmaya devam etmesidir. Canlı video ve ses uygulamaları, minimum düzeyde veya farkedilebilir bir etki olmadan bazı veri kayıplarını tolere edebilir ve UDP'ye mükemmel şekilde uygundur.

UDP'deki iletişim bloklarına datagramlar veya segmentler denir. Bu datagramlar, taşıma katmanı protokolü tarafından en iyi çaba olarak gönderilir.

UDP başlığı, TCP başlığından çok daha basittir çünkü yalnızca dört alanı vardır ve 8 bayt (yani 64 bit) gerektirir. Şekil, bir UDP başlığındaki alanları gösterir.




### 13.3.3.UDP Başlık Alanları

Tablo, bir UDP başlığındaki dört alanı tanımlar ve açıklar.

| UDP Header Field | Description |
|---|---|
| **Source Port** | Kaynak uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bit alan. |
| **Destination Port** | Hedef uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bit alan. |
| **Length** | UDP datagram başlığının uzunluğunu belirten 16 bit alan. |
| **Checksum** | Datagram başlığı ve verilerinin hata kontrolü için kullanılan 16 bitlik alan. |

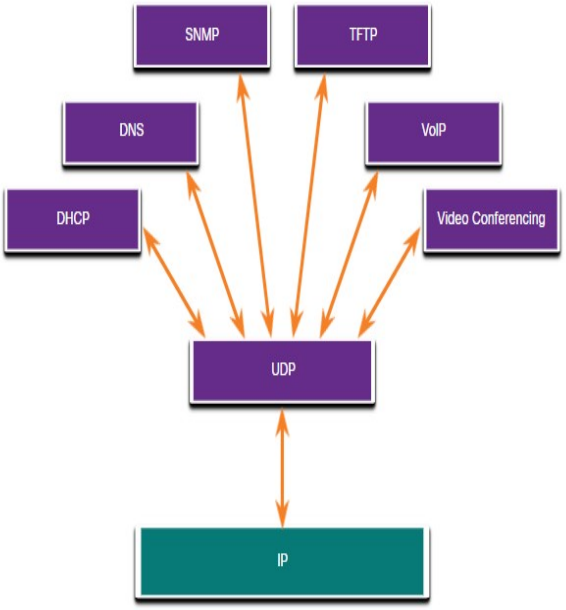
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 13.3.4.UDP kullanan uygulamalar

UDP'ye en uygun üç tür uygulama vardır:

**Canlı video ve multimedya uygulamaları -** Bu uygulamalar bazı veri kayıplarını tolere edebilir ancak çok az gecikme gerektirir veya hiç geciktirmez. Örnekler VoIP ve canlı video akışını içerir.
**Basit istek ve yanıt uygulamaları -** Bir toplantı sahibinin istek gönderdiği ve yanıt alabileceği veya alamayacağı basit işlemlere sahip uygulamalar . Örnekler arasında DNS ve DHCP bulunur.
**Güvenilirliği tek başına idare eden uygulamalar** - Akış kontrolü, hata tespiti, onaylar ve hata kurtarmanın gerekli olmadığı veya uygulama tarafından ele alınabildiği tek yönlü iletişimler. Örnekler arasında SNMP ve TFTP bulunur.

Şekil, UDP gerektiren uygulamaları tanımlar.




## 13.4.Port Numaraları

### 13.4.1.Birden Çok Ayrı İletişim

TCP ve UDP aktarım katmanı protokolleri, aynı anda birden çok konuşmayı yönetmek için bağlantı noktası numaralarını kullanır.

Kaynak bağlantı noktası numarası, yerel ana bilgisayardaki kaynak uygulama ile ilişkilendirilirken, hedef bağlantı noktası numarası uzak ana bilgisayardaki hedef uygulama ile ilişkilendirilir.

Örneğin, bir ana bilgisayarın bir web sunucusundan bir web sayfası isteği başlattığını varsayın. Ana bilgisayar web sayfası isteğini başlattığında, kaynak bağlantı noktası numarası, konuşmayı benzersiz bir şekilde tanımlamak için ana bilgisayar tarafından dinamik olarak oluşturulur. Bir ana bilgisayar tarafından üretilen her istek, dinamik olarak oluşturulmuş farklı bir kaynak bağlantı noktası numarası kullanır. Bu süreç, aynı anda birden fazla konuşmanın gerçekleşmesine izin verir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

İstekte, hedef bağlantı noktası numarası, hedef web sunucusundan talep edilen hizmet türünü tanımlayan şeydir. Örneğin, bir istemci hedef bağlantı noktasında 80 numaralı bağlantı noktasını belirttiğinde, mesajı alan sunucu web hizmetlerinin talep edildiğini anlar.

Bir sunucu, bağlantı noktası 21'de FTP bağlantısı sunarken, bağlantı noktası 80'deki web hizmetleri gibi aynı anda birden fazla hizmet sunabilir.

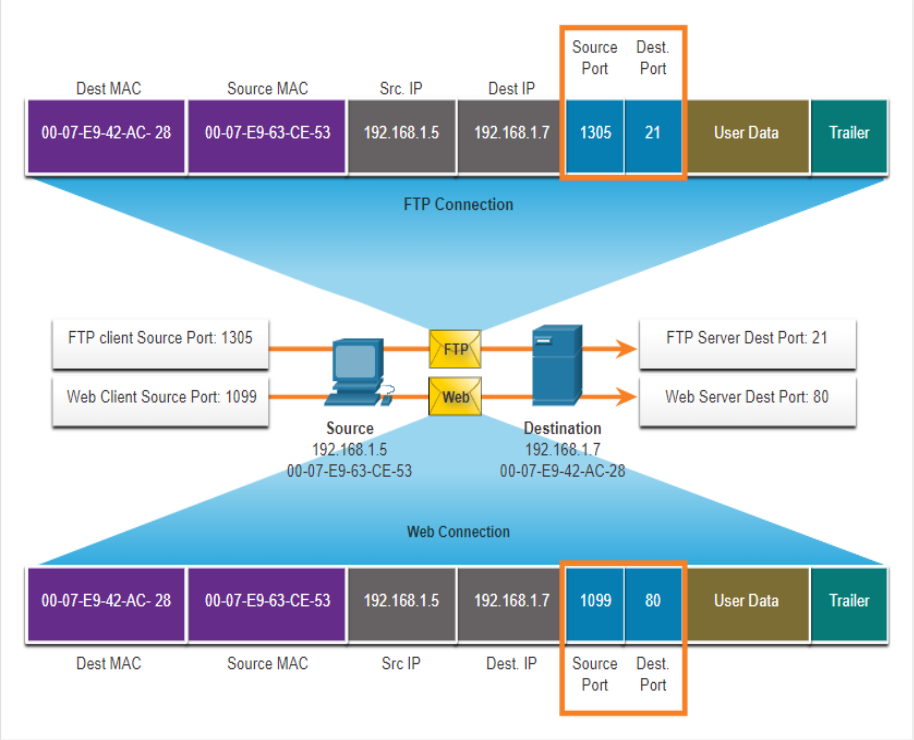
## 13.4.2.Soket Çiftleri

Kaynak ve hedef bağlantı noktaları segmentin içine yerleştirilir.

Bölümler daha sonra bir IP paketi içinde kapsüllenir.

Kaynak IP adresi ile kaynak bağlantı noktası numarasının veya hedef IP adresi ile hedef bağlantı noktası numarasının kombinasyonu **soket** olarak bilinir.

Soketler, bir istemci üzerinde çalışan birden çok işlemin birbirinden ayırt edilmesini ve sunucu işlemine yapılan birden çok bağlantının birbirinden ayırt edilmesini sağlar.




## 13.4.3.Port Numarası Grupları

Internet Assigned Numbers Authority(IANA), 16 bit port numaraları dahil olmak üzere çeşitli adresleme standartlarını atamaktan sorumlu standartlar organizasyonudur. Kaynak ve hedef bağlantı noktası numaralarını tanımlamak için kullanılan 16 bit, 0 ile 65535 arasında bir bağlantı noktası aralığı sağlar.

IANA, sayı aralığını aşağıdaki üç bağlantı noktası grubuna ayırmıştır.

Bazı istemci işletim sistemleri, kaynak bağlantı noktalarını atamak için dinamik bağlantı noktası numaraları yerine kayıtlı bağlantı noktası numaralarını kullanabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Port Group | Port Aralığı | Açıklama |
|---|---|---|
| **Well-known Ports**<br>**İyi bilinen portlar** | **0 to 1,023** | • Bu bağlantı noktası numaraları, web tarayıcıları, e-posta istemcileri ve uzaktan erişim istemcileri gibi yaygın veya popüler hizmetler ve uygulamalar için ayrılmıştır.<br>• Ortak sunucu uygulamaları için iyi bilinen tanımlanmış bağlantı noktaları, istemcilerin gereken ilişkili hizmeti kolayca tanımlamasını sağlar. |
| **Registered Ports**<br>**Kayıtlı portlar** | **1,024 to 49,151** | • Bu bağlantı noktası numaraları IANA tarafından belirli işlemlerle veya uygulamalarla kullanmak isteyen bir kuruluşa atanır.<br>• Bu işlemler, iyi bilinen bir bağlantı noktası numarası alacak olan yaygın uygulamalar yerine, öncelikle kullanıcının yüklemeyi seçtiği bireysel uygulamalardır.<br>• Örneğin, Cisco, RADIUS sunucu kimlik doğrulama işlemi için 1812 numaralı bağlantı noktasını kaydetmiştir. |
| **Private** and/ or **Dynamic Ports**<br>**Özel ve dinamik atanan portlar** | **49,152 to 65,535** | • Bu bağlantı noktaları geçici bağlantı noktaları olarak da bilinir.<br>• Bir hizmete bağlantı başlatıldığında istemcinin işletim sistemi genellikle bağlantı noktası numaralarını dinamik olarak atar.<br>• Dinamik bağlantı noktası daha sonra iletişim sırasında istemci uygulamasını tanımlamak için kullanılır. |

## Well-Known Port Numbers

| Port Number | Protocol | Application |
|---|---|---|
| **20** | TCP | File Transfer Protocol (FTP) - Data |
| **21** | TCP | File Transfer Protocol (FTP) - Control |
| **22** | TCP | Secure Shell (SSH) |
| **23** | TCP | Telnet |
| **25** | TCP | Simple Mail Transfer Protocol (SMTP) |
| **53** | UDP, TCP | Domain Name Service (DNS) |
| **67** | UDP | Dynamic Host Configuration Protocol (DHCP) - Server |
| **68** | UDP | Dynamic Host Configuration Protocol - Client |
| **69** | UDP | Trivial File Transfer Protocol (TFTP) |
| **80** | TCP | Hypertext Transfer Protocol (HTTP) |
| **110** | TCP | Post Office Protocol version 3 (POP3) |
| **143** | TCP | Internet Message Access Protocol (IMAP) |
| **161** | UDP | Simple Network Management Protocol (SNMP) |
| **443** | TCP | Hypertext Transfer Protocol Secure (HTTPS) |

Açıklanamayan TCP bağlantıları büyük bir güvenlik tehdidi oluşturabilir. Netstat komutu, bağlantıları doğrulamak için önemli bir araçtır.

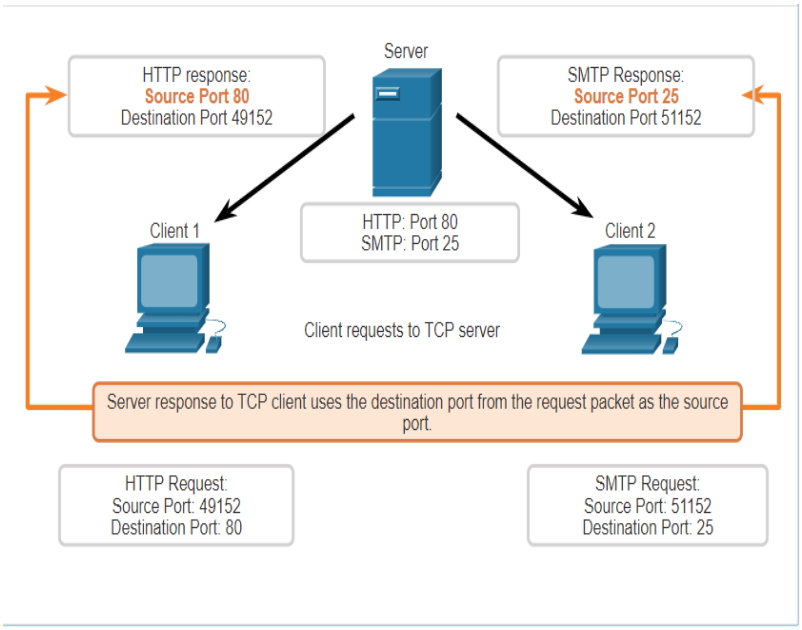
```
C:\Users\A>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.8.144:49674    51.105.249.239:https   ESTABLISHED
  TCP    192.168.8.144:49761    a23-213-166-60:https   CLOSE_WAIT
  TCP    192.168.8.144:49762    a23-213-166-60:https   CLOSE_WAIT
  TCP    192.168.8.144:49763    a23-213-166-60:https   CLOSE_WAIT
  TCP    192.168.8.144:49764    a23-213-166-60:https   CLOSE_WAIT
  TCP    192.168.8.144:49765    a23-213-166-60:https   CLOSE_WAIT
  TCP    192.168.8.144:49766    a23-213-166-60:https   CLOSE_WAIT
  TCP    192.168.8.144:49767    a104-96-150-51:http    CLOSE_WAIT
```

## 13.5.TCP İletişim Süreci

### 13.5.1.TCP Sunucu İşlemleri

Bir sunucuda çalışan her uygulama işlemi bir bağlantı noktası numarası kullanacak şekilde yapılandırılmıştır.

- Tek bir sunucunun, aynı taşıma katmanı hizmetleri içinde aynı bağlantı noktası numarasına atanmış iki hizmeti olamaz.
- Belirli bir bağlantı noktasına atanan etkin bir sunucu uygulaması açık olarak kabul edilir; bu, taşıma katmanının söz konusu bağlantı noktasına adreslenen bölümleri kabul ettiği ve işlediği anlamına gelir.
- Doğru sokete gönderilen herhangi bir istemci isteği kabul edilir ve veriler sunucu uygulamasına iletilir.

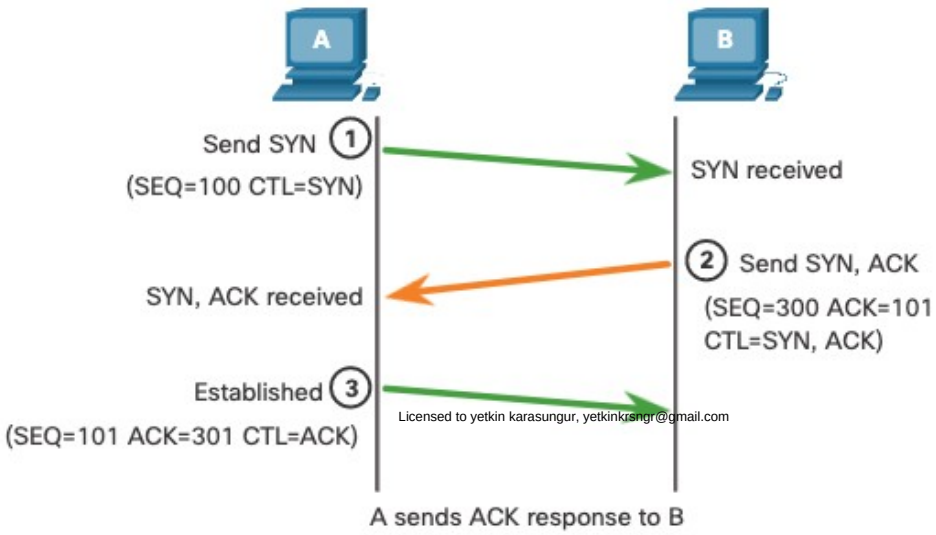



### 13.5.2.TCP Bağlantısı Kurulumu

Adım 1: Başlatan istemci, sunucuyla bir istemciden sunucuya-client-to-server iletişim oturumu ister.

Adım 2: Sunucu, istemciden sunucuya iletişim oturumunu onaylar ve sunucudan istemciye-server-to-client iletişim oturumu ister.

Adım 3: Başlatan istemci, sunucudan istemciye-server-to-client iletişim oturumunu onaylar.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

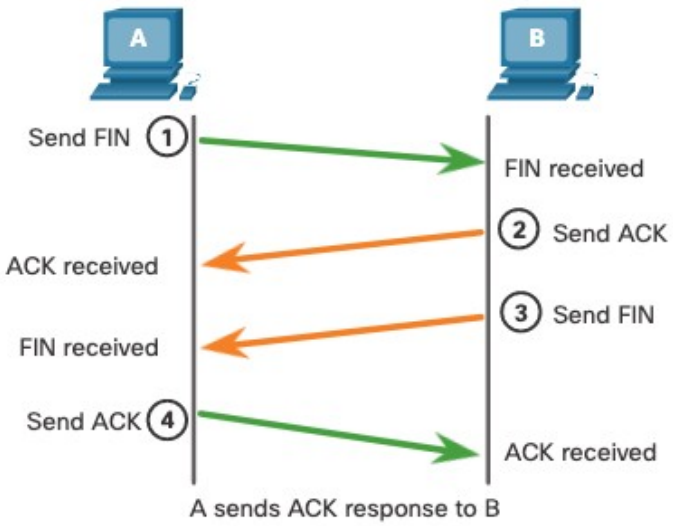
### 13.5.3.Oturum Sonlandırma

Adım 1: İstemci akışta gönderilecek daha fazla veriye sahip olmadığında, FIN bayrağı ayarlanmış bir segment gönderir.

Adım 2: Sunucu, oturumu istemciden sunucuya sonlandırmak için FIN'nin alındığını onaylamak için bir ACK gönderir.

Adım 3: Sunucu, istemciye sunucudan istemciye oturumu sonlandırmak için bir FIN gönderir.

Adım 4: İstemci, sunucudan FIN'i onaylamak için bir ACK ile yanıt verir.



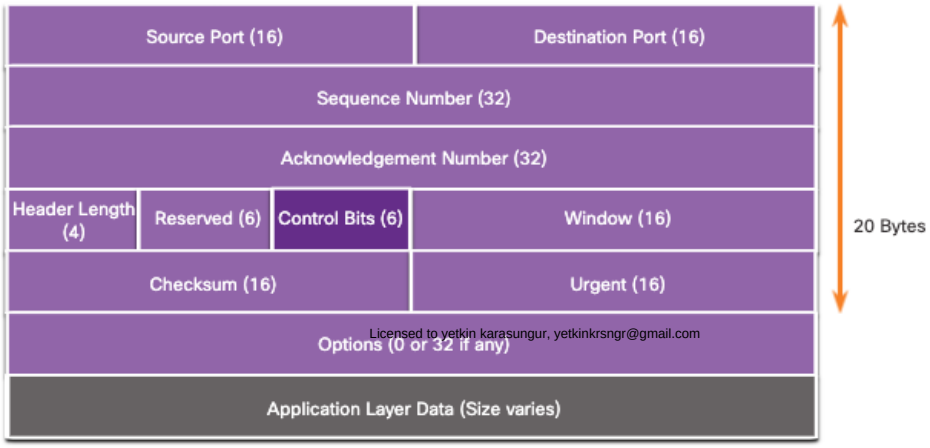

### 13.5.4.TCP Üç Yönlü El Sıkışma Analizi

Ana bilgisayarlar durumu korur, bir oturumdaki her veri segmentini izler ve TCP başlığındaki bilgileri kullanarak hangi verilerin alındığı hakkında bilgi alışverişinde bulunur. TCP, her bağlantının iki tek yönlü iletişim oturumunu temsil ettiği tam çift yönlü bir protokoldür. Bağlantı kurmak için, ana bilgisayarlar üç yönlü bir anlaşma yapar. Şekilde gösterildiği gibi, TCP başlığındaki kontrol bitleri bağlantının ilerlemesini ve durumunu gösterir.

Üç yönlü el sıkışmanın işlevleri şunlardır:

- Hedef aygıtın ağda mevcut olduğunu belirler.
- Hedef aygıtın etkin bir hizmete sahip olduğunu ve başlatan istemcinin kullanmayı planladığı hedef bağlantı noktası numarasındaki istekleri kabul ettiğini doğrular.
- Hedef cihaza, kaynak istemcinin bu port numarası üzerinde bir iletişim oturumu kurmayı planladığını bildirir.

İletişim tamamlandıktan sonra oturumlar kapatılır ve bağlantı sonlandırılır. Bağlantı ve oturum mekanizmaları, TCP güvenilirlik işlevini etkinleştirir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

TCP segment başlığının Kontrol Bitleri-Control Bits alanındaki altı bit aynı zamanda bayraklar(flags) olarak da bilinir. Bayrak, açık veya kapalı olarak ayarlanmış bir bittir.

Altı kontrol biti bayrağı aşağıdaki gibidir:

URG - Acil işaretçi alanı önemli
ACK - Bağlantı kurulmasında ve oturum sonlandırmada kullanılan onay bayrağı
PSH - İtme işlevi
RST - Bir hata veya zaman aşımı meydana geldiğinde bağlantıyı sıfırlayın
SYN - Bağlantı kurulumunda kullanılan sıra numaralarını senkronize edin
FIN - Gönderenden daha fazla veri yok ve oturum sonlandırmada kullanılmıyor

## 13.6.Güvenilirlik ve Akış Kontrolü

### 13.6.1.TCP Güvenilirlik- Garantili ve Sıralı Teslim

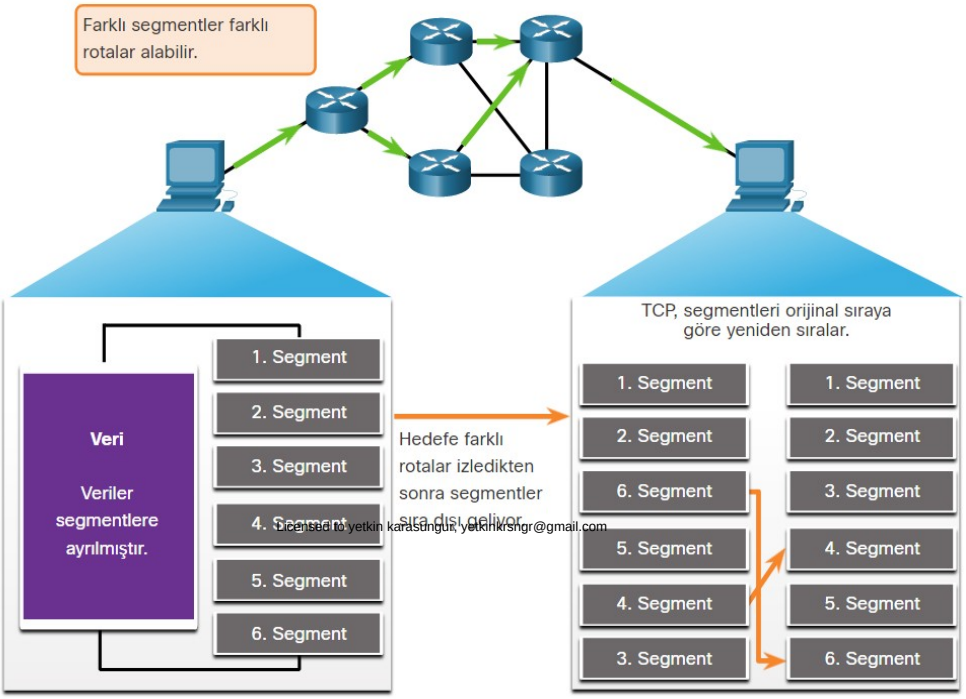
TCP'nin bazı uygulamalar için daha iyi protokol olmasının nedeni, UDP'den farklı olarak bırakılan paketleri yeniden göndermesi ve teslimattan önce uygun sıralarını belirtmek için paketleri numaralandırmasıdır. TCP, paket akışının korunmasına da yardımcı olabilir, böylece aygıtlar aşırı yüklenmez.

TCP kesimlerinin hedeflerine ulaşmadığı zamanlar olabilir. Diğer zamanlarda, TCP segmentleri sıra dışı gelebilir. Orijinal mesajın alıcı tarafından anlaşılabilmesi için tüm verilerin alınması ve bu bölümlerdeki verilerin orijinal sıraya göre yeniden birleştirilmesi gerekir. Bu hedefe ulaşmak için her paketin başlığında sıra numaraları atanır. Sıra numarası, TCP segmentinin ilk veri baytını temsil eder.

Oturum kurulumu sırasında, bir ilk sıra numarası (ISN) belirlenir. Bu ISN, alıcı uygulamaya iletilen baytların başlangıç değerini temsil eder. Veriler, oturum sırasında iletildikçe, sıra numarası, iletilen bayt sayısı kadar artar. Bu veri bayt takibi, her segmentin benzersiz şekilde tanımlanmasını ve onaylanmasını sağlar. Eksik segmentler daha sonra belirlenebilir.

ISN birde başlamaz, ancak etkin bir şekilde rastgele bir sayıdır. Bu, belirli türdeki kötü niyetli saldırıları önlemek içindir. Basit olması için, bu bölümdeki örnekler için 1 ISN kullanacağız.

Segment sıra numaraları, şekilde gösterildiği gibi alınan segmentlerin nasıl yeniden birleştirileceğini ve yeniden sıralanacağını gösterir.



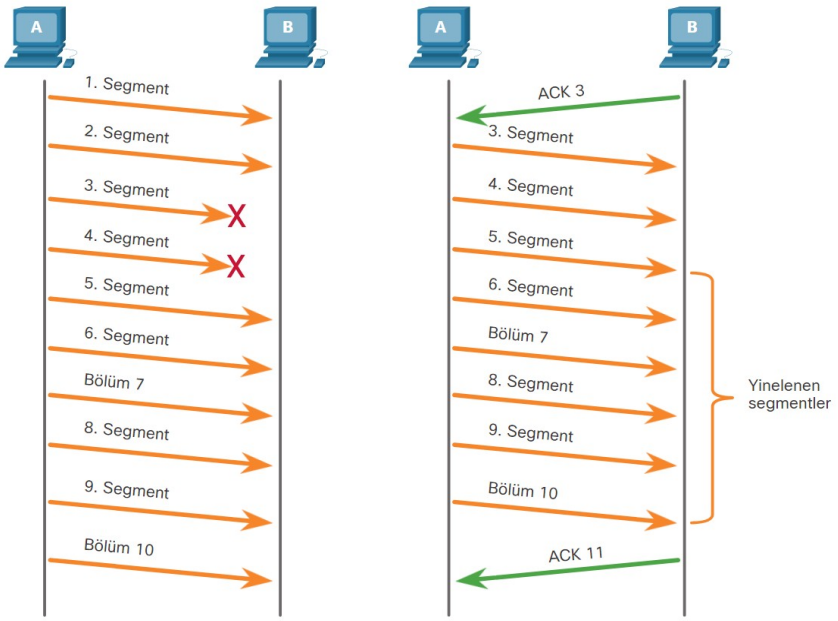
Licensed to: yetkin karasungur, yetkinkrsngr@gmail.com

## 13.6.2.TCP Güvenilirliği - Veri Kaybı ve Yeniden İletimi

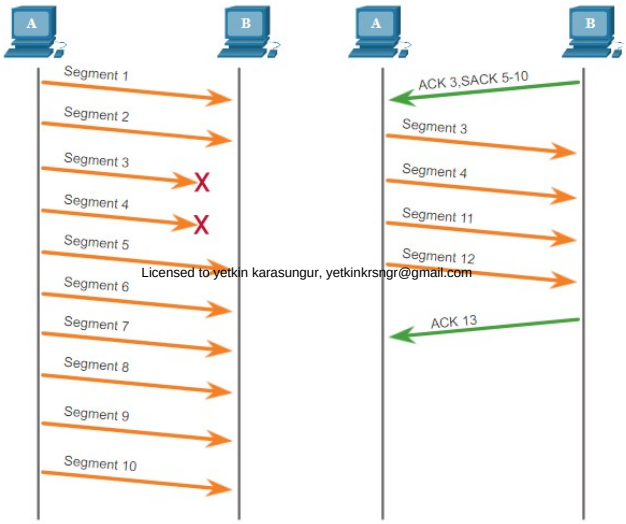
Bir ağ ne kadar iyi tasarlanırsa tasarlansın, zaman zaman veri kaybı meydana gelir. TCP, bu segment kayıplarını yönetme yöntemleri sağlar. Bunların arasında, onaylanmamış veriler için segmentleri yeniden iletme mekanizması vardır.

Sıra (SEQ) numarası ve alındı (ACK) numarası, iletilen bölümlerde bulunan veri baytlarının alındığını teyit etmek için birlikte kullanılır. SEQ numarası, iletilmekte olan segmentteki ilk veri baytını tanımlar. TCP, alıcının almayı beklediği bir sonraki baytı belirtmek için kaynağa geri gönderilen ACK numarasını kullanır. Buna beklenti kabulü denir.

Daha sonraki geliştirmelerden önce, TCP yalnızca beklenen bir sonraki baytı kabul edebiliyordu. Örneğin, şekilde, basitlik için segment numaralarını kullanarak, ana bilgisayar A, segmentleri 1'den 10'a kadar ana bilgisayar B'ye gönderir. 3. Ana bilgisayar A, başka herhangi bir segmentin gelip gelmediğini bilmiyor. Bu nedenle, Ana Bilgisayar A, 3 ila 10 arasındaki segmentleri yeniden gönderecektir. Tüm yeniden gönderilen segmentler başarılı bir şekilde ulaşırsa, 5 ila 10 arasındaki segmentler kopyalar olacaktır. Bu, gecikmelere, tıkanıklığa ve verimsizliklere yol açabilir.




Bugün ana bilgisayar işletim sistemleri tipik olarak, üç yönlü el sıkışma sırasında görüşülen, seçici onay-selective acknowledgment (SACK) adı verilen isteğe bağlı bir TCP özelliğini kullanır. Her iki ana bilgisayar SACK'i destekliyorsa, alıcı, kesintili bölümler dahil olmak üzere hangi bölümlerin (baytların) alındığını açıkça onaylayabilir. Bu nedenle, gönderen ana bilgisayarın yalnızca eksik verileri yeniden iletmesi gerekir. Örneğin, sonraki şekilde, yine basitlik için bölüm numaralarını kullanarak, ana bilgisayar A, bölümler 1 ila 10'u ana bilgisayar B'ye gönderir. Bölüm 3 ve 4 dışındaki tüm bölümler gelirse, ana bilgisayar B, bölüm 1 ve 2'yi aldığını kabul edebilir. (ACK 3) ve 5 ile 10 arasındaki segmentleri (SACK 5-10) seçici olarak onaylayın. Ana bilgisayar A'nın yalnızca 3. ve 4. segmentleri yeniden göndermesi gerekir.

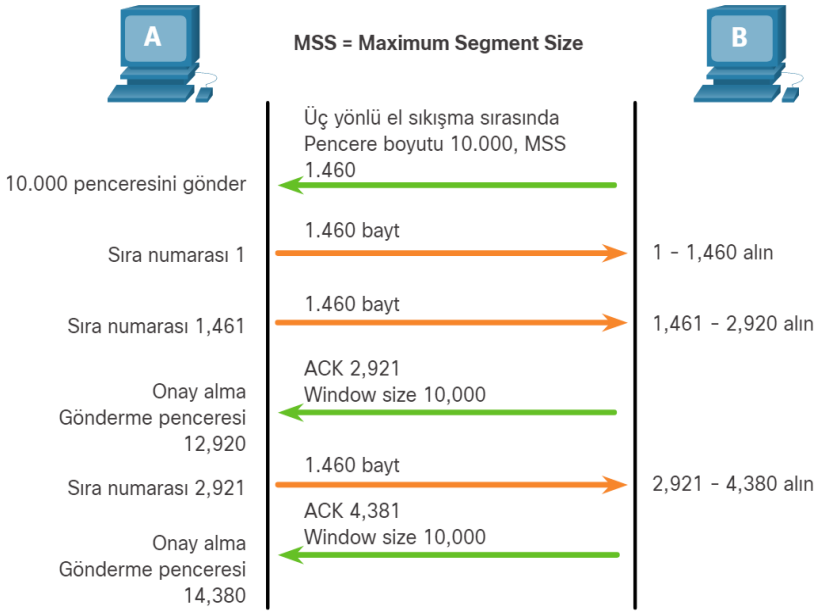



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 13.6.3.TCP Akış Kontrolü – Pencere Boyutu ve Kabul Bildirimleri

TCP ayrıca akış denetimi için mekanizmalar sağlar. Akış kontrolü, hedefin güvenilir bir şekilde alabileceği ve işleyebileceği veri miktarıdır. Akış denetimi, belirli bir oturum için kaynak ve hedef arasındaki veri akış hızını ayarlayarak TCP iletiminin güvenilirliğini korumaya yardımcı olur. Bunu başarmak için, TCP başlığı pencere boyutu adı verilen 16 bitlik bir alan içerir.

Şekil, pencere boyutu ve alındı bildirimlerinin bir örneğini göstermektedir.




Pencere boyutu, bir alındı bildirimi beklenmeden gönderilebilecek bayt sayısını belirler. Kabul numarası, bir sonraki beklenen baytın numarasıdır.

Pencere boyutu, bir TCP oturumunun hedef cihazının bir seferde kabul edebileceği ve işleyebileceği bayt sayısıdır. Bu örnekte, TCP oturumu için PC B başlangıç pencere boyutu 10.000 bayttır. İlk bayt, bayt numarası 1'den başlayarak, son bayt PC A'nın bir onay almadan gönderebileceği bayt 10.000'dir. Bu, PC A'nın gönderme penceresi olarak bilinir. Pencere boyutu her TCP segmentine dahil edilir, böylece hedef, ara bellek kullanılabilirliğine bağlı olarak pencere boyutunu herhangi bir zamanda değiştirebilir.

Üç yönlü el sıkışma sırasında TCP oturumu kurulduğunda ilk pencere boyutu üzerinde anlaşmaya varılır. Kaynak cihaz, hedefin pencere boyutuna bağlı olarak hedef cihaza gönderilen bayt sayısını sınırlamalıdır. Ancak kaynak cihaz, baytların alındığına dair bir onay aldıktan sonra, oturum için daha fazla veri göndermeye devam edebilir. Tipik olarak hedef, bir alındı bildirimi ile yanıtlamadan önce pencere boyutunun alınmasını tüm baytların alınmasını beklemeyecektir. Baytlar alındıkça ve işlendikçe, hedef, kaynağa ek bayt göndermeye devam edebileceğini bildirmek için alındı bildirimleri gönderecektir.

Örneğin, PC B'nin bir alındı bildirimi göndermeden önce 10.000 baytın tamamının alınmasını beklememesi normaldir. Bu, PC A'nın, PC B'den alındı bildirimleri alırken gönderme penceresini ayarlayabileceği anlamına gelir. Şekilde gösterildiği gibi, PC A, bir sonraki beklenen bayt olan 2,921 alındı bildirimi aldığında. PC A gönderme penceresi 2.920 bayt artıracaktır. Bu, gönderme penceresini 10.000 bayttan 12.920'ye değiştirir. PC A, 12.920'deki yeni gönderme penceresinden fazlasını göndermediği sürece PC B'ye 10.000 bayta kadar daha göndermeye devam edebilir.

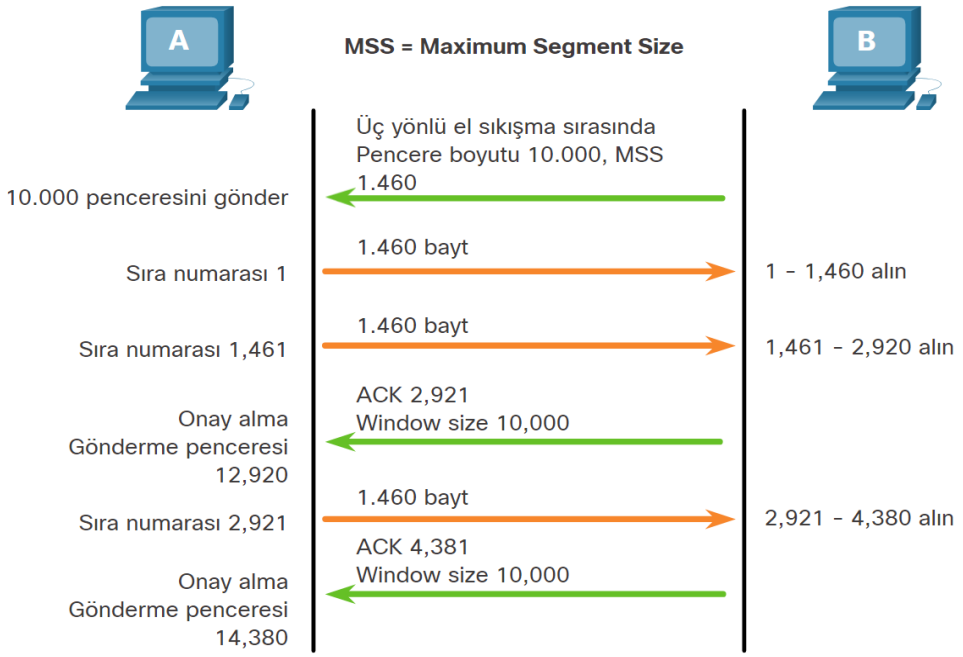
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Alınan baytları işlerken onaylar gönderen bir hedef ve kaynak gönderme penceresinin sürekli ayarlanması, kayan pencereler olarak bilinir. Önceki örnekte, PC A'nın gönderme penceresi başka bir 2.921 bayta 10.000'den 12.920'ye kadar artar veya kayar.

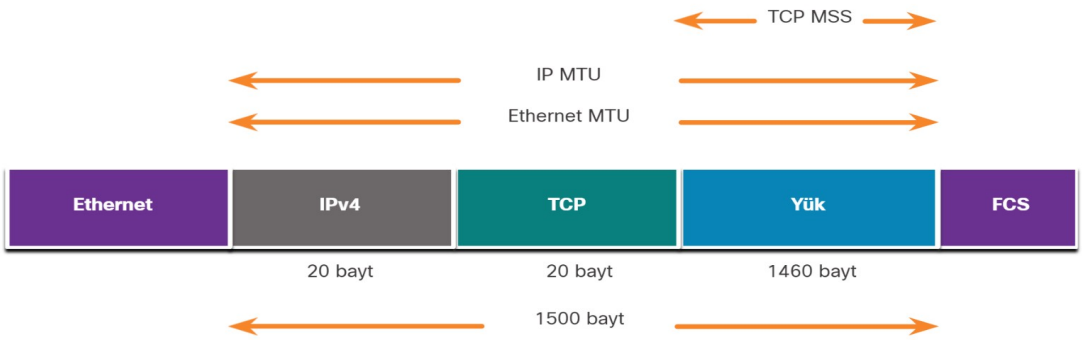
Hedefin arabellek alanının kullanılabilirliği azalırsa, bir bildirim almadan göndermesi gereken bayt sayısını azaltmak için kaynağa bilgi vermek için pencere boyutunu azaltabilir.

## 13.6.4.TCP Akış Kontrolü - Maksimum Segment Boyutu

Şekilde, kaynak her TCP segmenti içinde 1.460 bayt veri iletiyor. Bu, genellikle hedef aygıtın alabileceği Maksimum Segment Boyutudur (MSS). MSS, bir aygıtın tek bir TCP segmentinde alabileceği en büyük veri miktarını bayt cinsinden belirten TCP başlığındaki seçenekler alanının bir parçasıdır. MSS boyutu TCP başlığını içermez. MSS, genellikle üç yönlü el sıkışma sırasında dahil edilir.




IPv4 kullanılırken yaygın bir MSS 1.460 bayttır. Bir ana bilgisayar, IP ve TCP başlıklarını Ethernet maksimum iletim biriminden (MTU) çıkararak MSS alanının değerini belirler. Bir Ethernet arayüzünde, varsayılan MTU 1500 bayttır. 20 baytlık IPv4 başlığını ve 20 baytlık TCP üstbilgisini çıkararak, şekilde gösterildiği gibi varsayılan MSS boyutu 1460 bayt olacaktır.

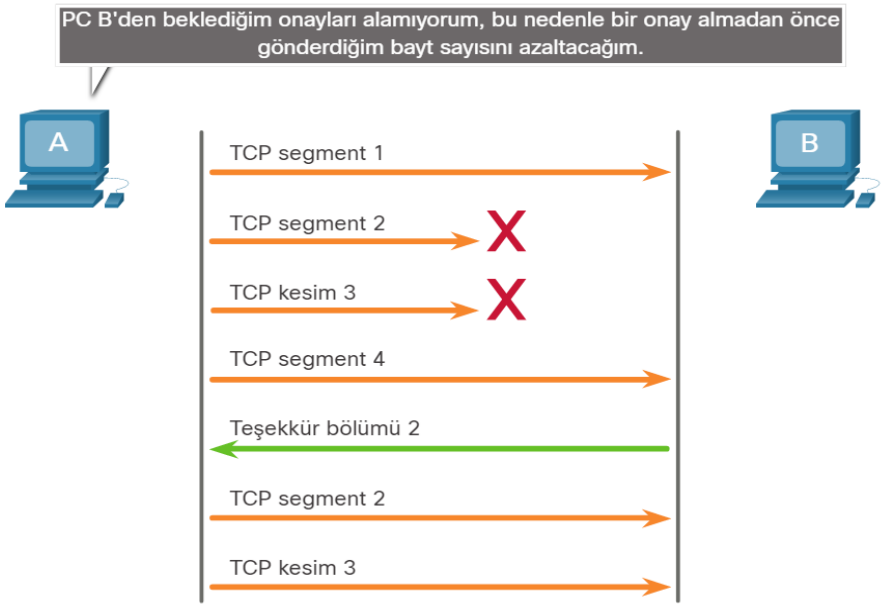



## 13.6.5.TCP Akış Kontrolü - Tıkanıklık Önleme

Bir ağda tıkanıklık olduğunda, aşırı yüklenmiş yönlendirici tarafından paketlerin atılmasıyla sonuçlanır.

Tıkanıklığı önlemek ve kontrol etmek için TCP, birkaç tıkanıklık işleme mekanizması, zamanlayıcı ve algoritma kullanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

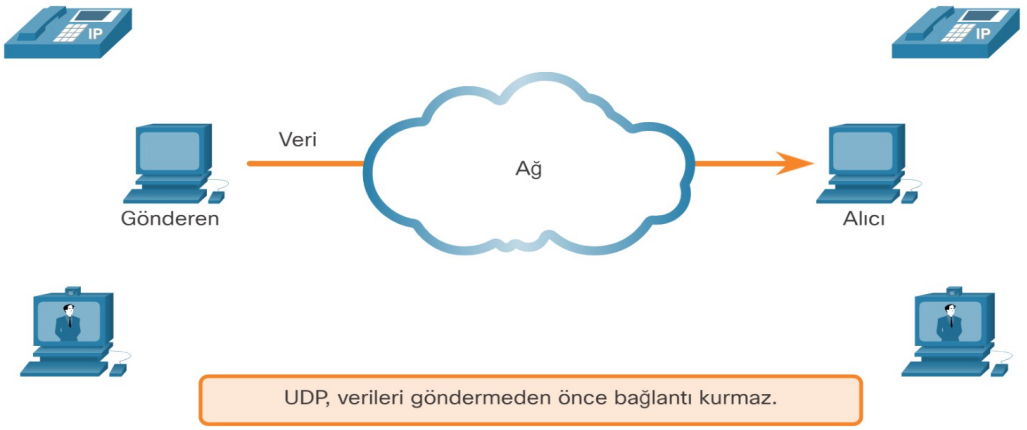



Onay numaraları bir sonraki beklenen bayt içindir ve bir segment için değildir. Kullanılan segment numaraları, açıklama amacıyla basitleştirilmiştir.

## 13.7.UDP İletişimi

### 13.7.1.UDP Düşük Ek Yük ve Güvenilirlik

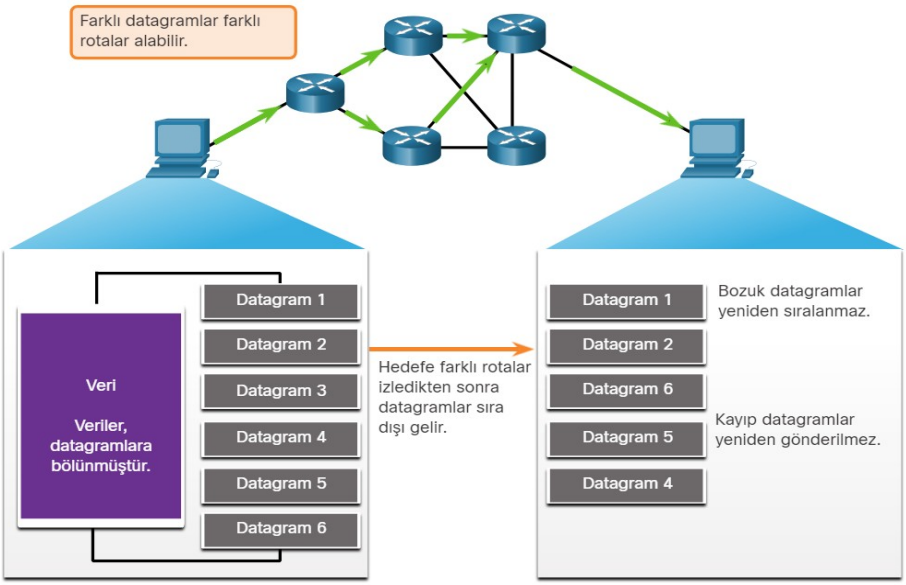
UDP bir bağlantı kurmaz. UDP, küçük bir datagram başlığı ve ağ yönetimi trafiği olmadığı için düşük ek yük ile veri aktarımı sağlar.




### 13.7.2.UDP Veri Biriminin Yeniden Birleştirilmesi

UDP sıra numaralarını TCP'nin yaptığı gibi izlemez.
UDP'nin datagramları iletim sıralarına göre yeniden sıralaması mümkün değildir.
UDP, verileri alındığı sıraya göre yeniden birleştirir ve uygulamaya iletir.

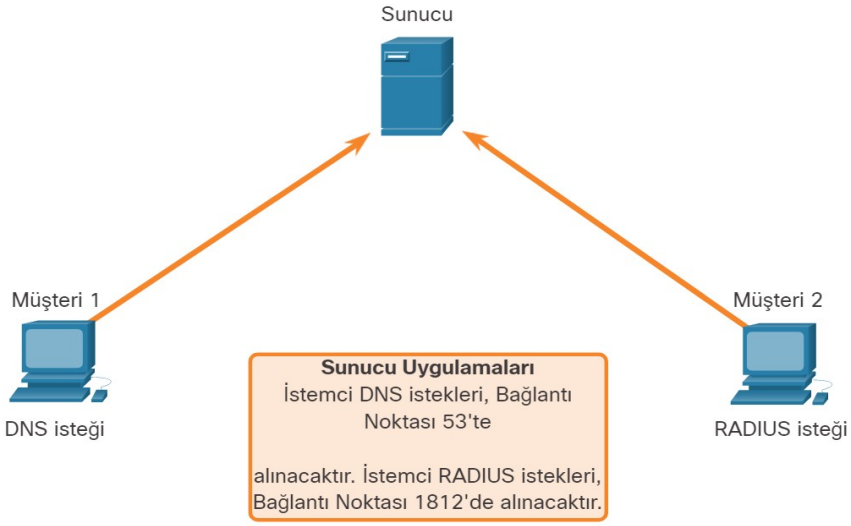
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 13.7.3.UDP Sunucu İşlemleri ve İstekleri

UDP tabanlı sunucu uygulamalarına iyi bilinen veya kayıtlı bağlantı noktası numaraları atanır.

UDP, bu portlardan biri için hedeflenmiş bir datagram alır, uygulama verilerini port numarasına göre uygun uygulamaya iletir.




## 13.7.4.UDP İstemci İşlemleri

UDP istemci işlemi, bağlantı noktası numaraları aralığından dinamik olarak bir bağlantı noktası numarası seçer ve bunu konuşma için kaynak bağlantı noktası olarak kullanır.
Hedef bağlantı noktası genellikle sunucu işlemine atanan iyi bilinen veya kayıtlı bağlantı noktası numarasıdır.
İstemci kaynak ve hedef bağlantı noktalarını seçtikten sonra, işlemdeki tüm datagramların başlığında aynı bağlantı noktası çifti kullanılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 14. Bölüm: Uygulama Katmanı

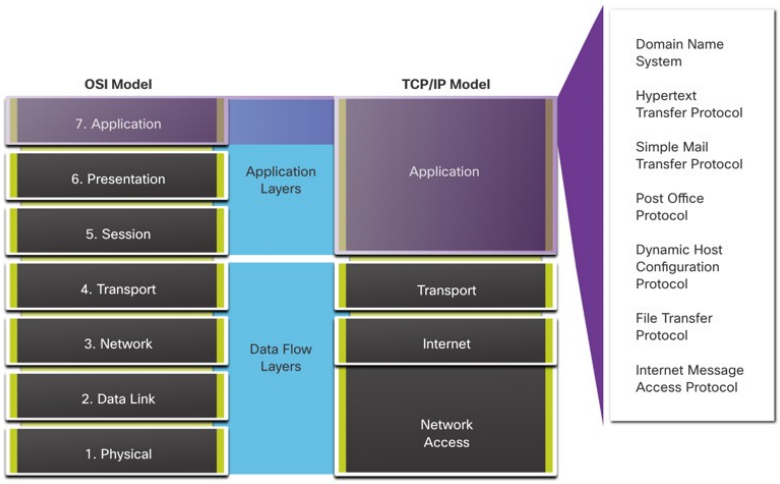
## 14.1.Application, Presentation,Session

### 14.1.1.Application Layer-Uygulama Katmanı

OSI modelinin üst üç katmanı (uygulama, sunum ve oturum) TCP / IP uygulama katmanının işlevlerini tanımlar.

Uygulama katmanı, iletişim kurmak için kullanılan uygulamalar ile mesajların iletildiği temel ağ arasındaki arayüzü sağlar.

En çok bilinen uygulama katmanı protokollerinden bazıları HTTP, FTP, TFTP, IMAP ve DNS'dir.



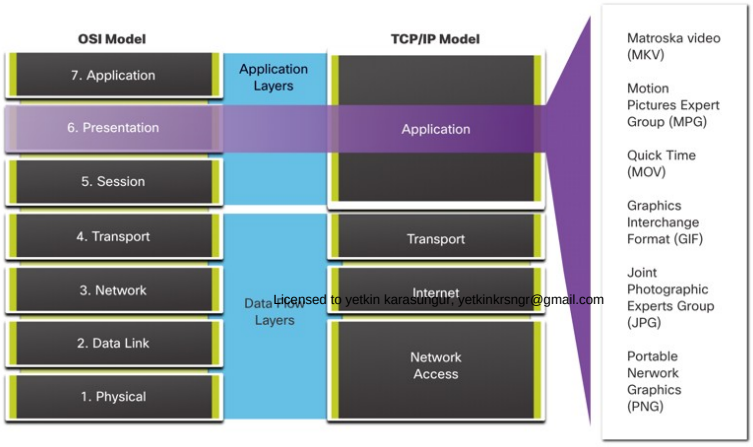

### 14.1.2.Presentation&Session Layer-Sunum-Oturum Katmanı

Sunum katmanının işlevleri:

- Kaynak aygıttaki verileri, hedef aygıt tarafından alınacak şekilde uyumlu bir biçimde biçimlendirme veya sunma
- Verileri hedef cihaz tarafından açılabilecek şekilde sıkıştırma
- Verileri iletmek için şifreleme ve alındıktan sonra verilerin şifresini çözme

Oturum katmanının işlevleri:

- Kaynak ve hedef uygulamalar arasında iletişim  oluşturur ve korur.
- İletişim kurmak, bunları etkin tutmak ve kesintiye uğrayan veya uzun süre boşta kalan oturumları yeniden başlatmak için bilgi alışverişini yönetir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 14.1.3.TCP/IP Application Layer Protocols- Uygulama Katmanı Protokolleri

TCP / IP uygulama protokolleri, birçok yaygın internet iletişim işlevi için gerekli format ve kontrol bilgilerini belirtir.

Uygulama katmanı protokolleri, bir iletişim oturumu sırasında hem kaynak hem de hedef aygıtlar tarafından kullanılır.

İletişimin başarılı olması için, kaynak ve hedef ana bilgisayarda uygulanan uygulama katmanı protokollerinin uyumlu olması gerekir.

Name System
DNS - Domain Name System (or Service)
TCP, UDP client 53
Cisco.com gibi alan adlarını IP adreslerine çevirir.

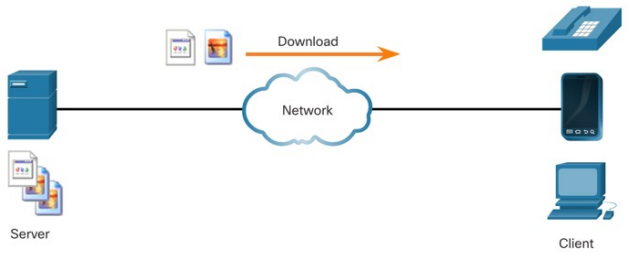
Host Config
DHCP - Dynamic Host Configuration Protocol
UDP client 68, server 67
IP adreslerini yeniden kullanılacak şekilde dinamik olarak atar

Web
HTTP - Hypertext Transfer Protocol
TCP 80, 8080
World Wide Web'de metin, grafik görüntü, ses, video ve diğer multimedya dosyalarını alıp vermek için bir dizi kural

## 14.2.Sunucu İstemci&Eşler Arası Ağlar

### 14.2.1.Client-Server Model

- İstemci ve sunucu işlemlerinin uygulama katmanında olduğu kabul edilir.
- İstemci / sunucu modelinde, bilgi isteyen aygıta istemci-client, isteğe yanıt veren aygıta sunucu-server denir.
- Uygulama katmanı protokolleri, istemciler ve sunucular arasındaki istek ve yanıtların biçimini tanımlar.

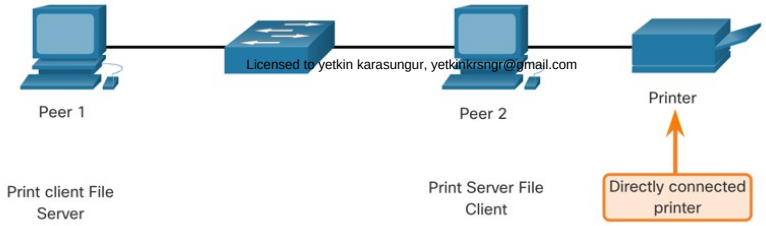



### 14.2.2.Peer-to-Peer Networks

Eşler arası (P2P) ağda, iki veya daha fazla bilgisayar bir ağ aracılığıyla bağlanır ve özel bir sunucuya sahip olmadan kaynakları (yazıcılar ve dosyalar gibi) paylaşabilir.

Bağlı her uç cihaz (eş olarak bilinir) hem sunucu hem de istemci olarak işlev görebilir.

Bir bilgisayar aynı anda başka bir işlem için istemci görevi görürken bir işlem için sunucu rolünü üstlenebilir. İstemci ve sunucunun rolleri isteğe bağlı olarak belirlenir.

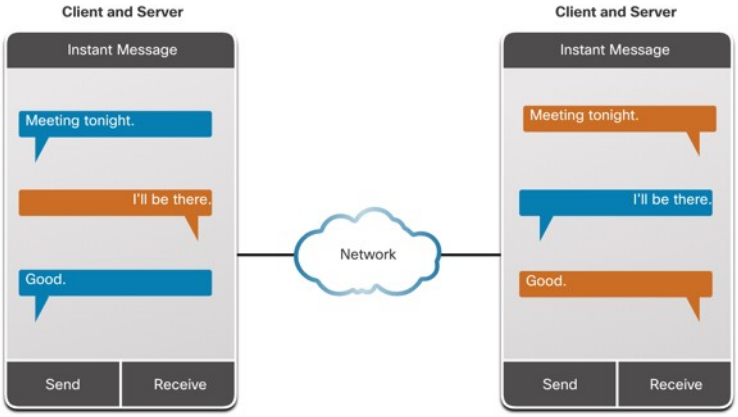



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 14.2.3.Peer-to-Peer Applications

Bir P2P uygulaması, bir cihazın aynı iletişim içinde hem istemci hem de sunucu olarak hareket etmesini sağlar.

Bazı P2P uygulamaları, her eşin başka bir eşte depolanan kaynağın yerini almak için bir dizin sunucusuna eriştiği karma bir sistem kullanır.




### Ortak P2P Uygulamaları

P2P uygulamalarında, uygulamayı çalıştıran ağdaki her bilgisayar, uygulamayı çalıştıran ağdaki diğer bilgisayarlar için bir istemci veya sunucu görevi görebilir.

Ortak P2P ağlarına örnek:

- BitTorrent
- Direct Connect
- eDonkey
- Freenet

## 14.3.Web-Email Protocols

### 14.3.1.Hypertext Transfer Protocol-Hypertext Markup Language

Bir web adresi veya Tekdüzen Kaynak Konum Belirleyicisi-Uniform Resource Locator (URL) bir web tarayıcısına yazıldığında, web tarayıcısı web hizmetiyle bağlantı kurar. Web hizmeti, HTTP protokolünü kullanan sunucuda çalışıyor.

Web tarayıcısının ve web sunucusunun nasıl etkileşime girdiğini daha iyi anlamak için bir web sayfasının tarayıcıda nasıl açıldığını inceleyin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

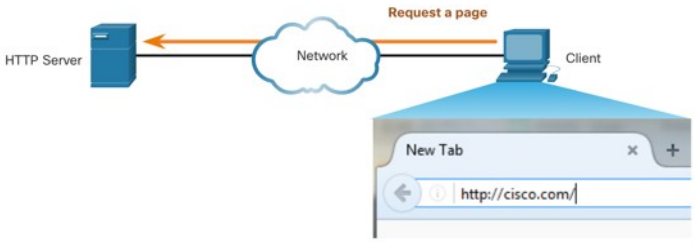
Adım 1 :

Tarayıcı, URL'nin üç bölümünü yorumlar:

http (protokol veya şema)
www.cisco.com (the server name)
index.html (istenen belirli dosya adı)

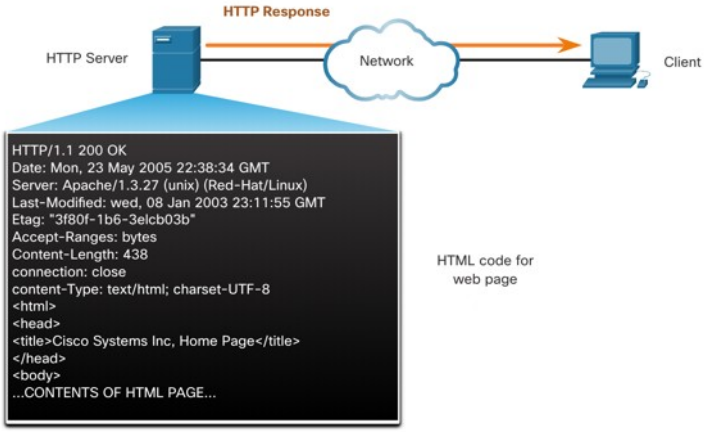
Adım 2
Tarayıcı daha sonra www.cisco.com adresini sunucuya bağlanmak için kullandığı sayısal bir IP adresine dönüştürmek için bir ad sunucusu ile kontrol eder.

İstemci, sunucuya bir GET isteği göndererek sunucuya bir HTTP isteği başlatır ve index.html dosyasını ister.

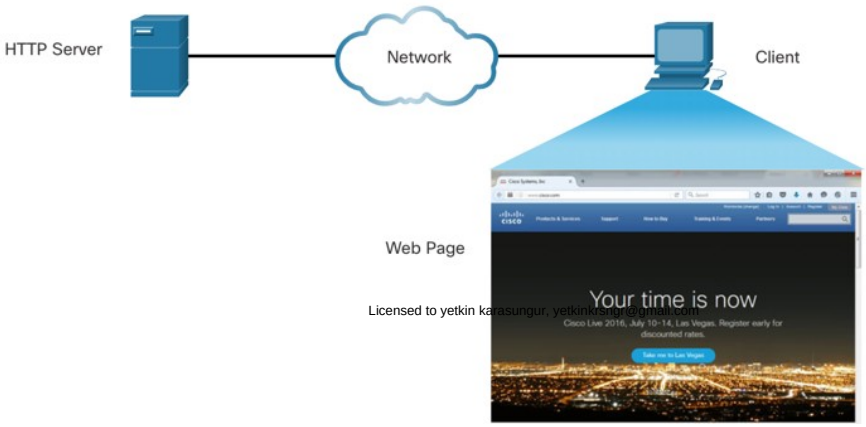



Adım 3

İsteğe yanıt olarak, sunucu bu web sayfasının HTML kodunu tarayıcıya gönderir.




Adım 4
Tarayıcı, HTML kodunun şifresini çözer ve tarayıcı penceresi için sayfayı biçimlendirir.




Licensed to yetkin karasungur, yetkinkarasungur@gmail.com

## 14.3.2.HTTP-HTTPS

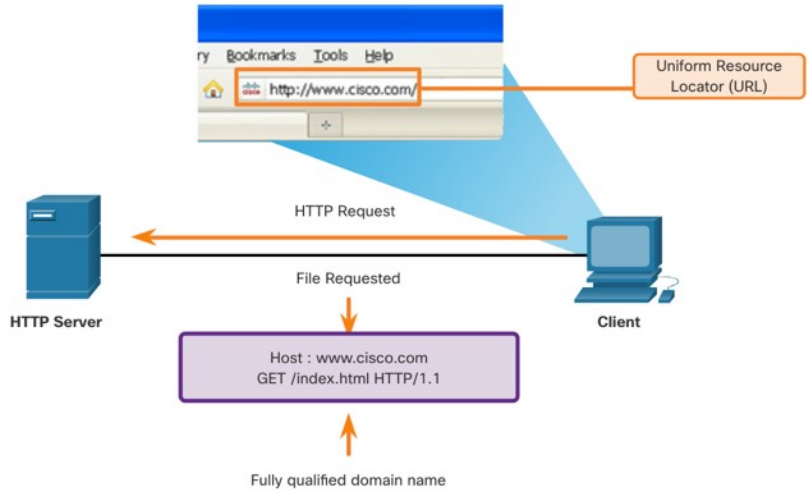
HTTP, bu iletişim için kullanılan mesaj türlerini belirten bir istek / yanıt protokolüdür.

Üç yaygın mesaj türü GET, POST ve PUT'dur:

GET-Bu, istemci için bir istemci isteğidir. Bir istemci (web tarayıcısı) HTML sayfaları istemek için web sunucusuna GET mesajını gönderir.

POST-Bu, veri dosyalarını form sunucusu gibi web sunucusuna yükler.

PUT-Bu, web sunucusuna görüntü gibi kaynakları veya içeriği yükler.




HTTP güvenli bir protokol değildir. İnternet üzerinden gönderilen güvenli iletişim için HTTPS kullanılmalıdır.

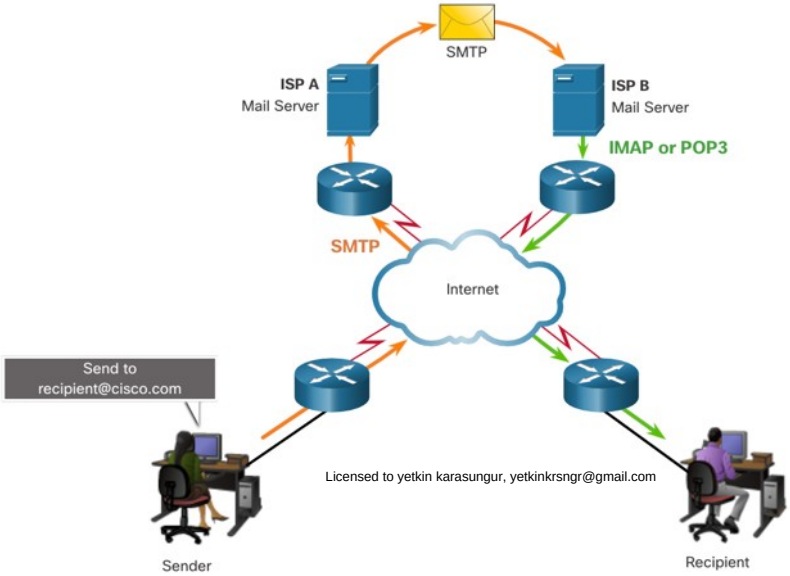
## 14.3.3.Email Protocols

E-posta, bir ağ üzerinden elektronik mesaj gönderme, saklama ve alma yöntemidir. E-posta mesajları, posta sunucularındaki veritabanlarında depolanır. E-posta istemcileri, e-posta göndermek ve almak için posta sunucularıyla iletişim kurar.

İşlem için kullanılan e-posta protokolleri:

Simple Mail Transfer Protocol (SMTP) – posta göndermek için kullanılır.

Post Office Protocol (POP) & IMAP – istemcilerin posta alması için kullanılır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

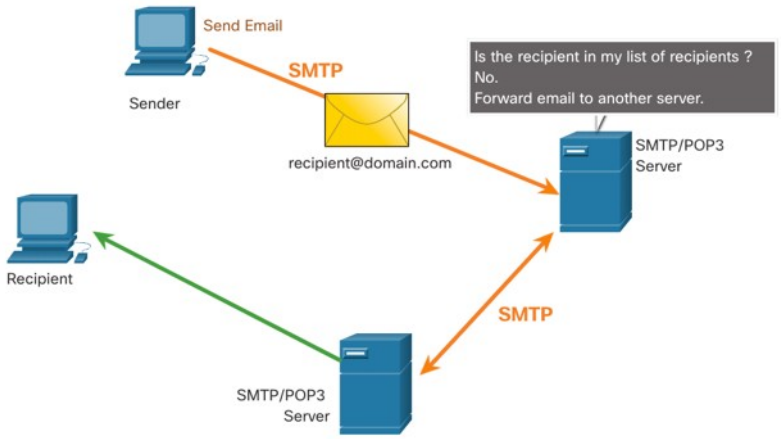
## SMTP, POP,IMAP

Bir istemci e-posta gönderdiğinde, istemci SMTP işlemi bilinen bağlantı noktası 25'teki bir sunucu SMTP işlemine bağlanır.

Bağlantı kurulduktan sonra, istemci e-postayı bağlantı üzerinden sunucuya göndermeye çalışır.

Sunucu iletiyi aldığında, alıcı yerelse iletiyi yerel bir hesaba yerleştirir veya iletiyi teslim edilmek üzere başka bir posta sunucusuna iletir.

Hedef e-posta sunucusu çevrimiçi olmayabilir veya meşgul olabilir. Öyleyse, SMTP daha sonra gönderilecek iletileri biriktirir.

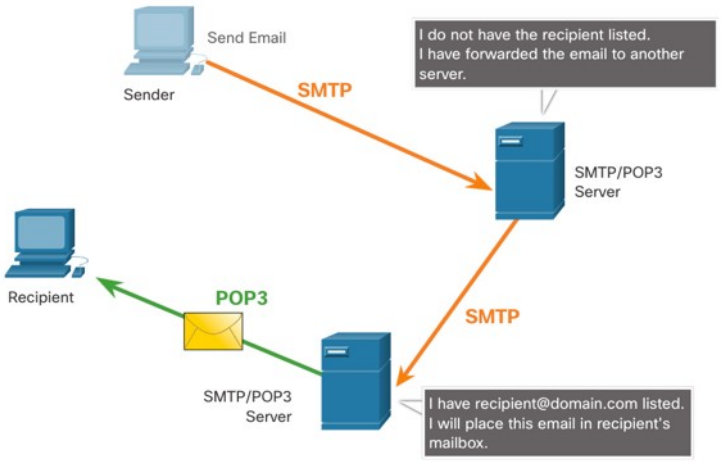



SMTP mesaj biçimleri için bir mesaj başlığı (alıcı e-posta adresi ve gönderen e-posta adresi) ve bir mesaj gövdesi gerekir.

POP, bir uygulama tarafından bir posta sunucusundan posta almak için kullanılır. POP kullanılarak sunucudan istemciye posta indirildiğinde, iletiler sunucuda silinir.
Sunucu, istemci bağlantı istekleri için TCP bağlantı noktası 110'u pasif olarak dinleyerek POP hizmetini başlatır. Bir istemci hizmeti kullanmak istediğinde, sunucuyla bir TCP bağlantısı kurma isteği gönderir.

Bağlantı kurulduğunda, POP sunucusu bir karşılama mesajı gönderir.

İstemci ve POP sunucusu daha sonra bağlantı kapatılana veya sonlandırılana kadar komut ve yanıt alışverişinde bulunur.



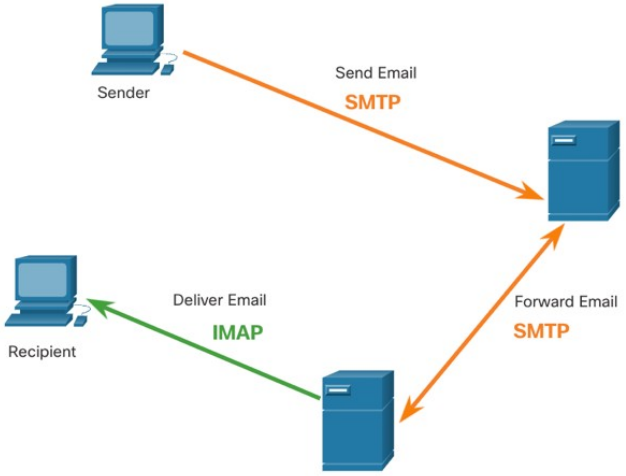

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

POP iletileri saklamadığından, merkezi bir yedekleme çözümüne ihtiyaç duyan küçük işletmeler için önerilmez.

IMAP, e-posta mesajlarını alma yöntemini tanımlayan başka bir protokoldür.

POP'un aksine, kullanıcı bir IMAP sunucusuna bağlandığında, mesajların kopyaları istemci uygulamasına indirilir. Orijinal mesajlar manuel olarak silinene kadar sunucuda tutulur.

Kullanıcı bir mesajı silmeye karar verdiğinde, sunucu bu eylemi senkronize eder ve mesajı sunucudan siler.



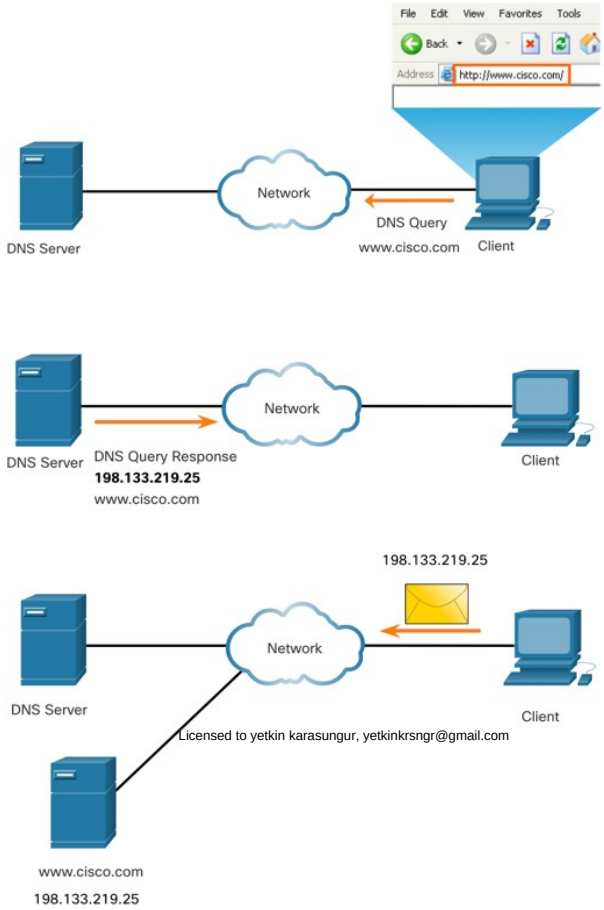

## 14.4.IP Adresleme Hizmetleri

### 14.4.1.Domain Name Service

Alan adları-Domain names, sayısal IP adreslerini basit ve tanınabilir bir ada dönüştürmek için oluşturuldu.

http://www.cisco.com gibi tam nitelikli alan adları (FQDN'ler), insanların hatırlaması için 198.133.219.25'ten daha kolaydır.

DNS protokolü, kaynak adlarını gerekli sayısal ağ adresiyle eşleşen otomatik bir hizmet tanımlar. Sorguların, yanıtların ve verilerin biçimini içerir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## DNS Mesaj Biçimi

DNS sunucusu, adları çözümlemek için kullanılan farklı türde kaynak kayıtları saklar. Bu kayıtlar kaydın adını, adresini ve türünü içerir.

Bu kayıt türlerinden bazıları aşağıdaki gibidir:

- **A**-Bir uç cihaz IPv4 adresi
- **NS**-Yetkili bir isim sunucusu
- **AAAA**- Bir uç cihazIPv6 addresi (pronounced quad-A)
- **MX**- E-posta değişim kaydı

İstemci bir sorgu yaptığında, sunucu DNS işlemi önce adı çözümlemek için kendi kayıtlarına bakar. Saklanan kayıtlarını kullanarak adı çözümleyemezse, adı çözümlemek için diğer sunucularla iletişim kurar.

Bir eşleşme bulunup orijinal istekte bulunan sunucuya geri döndükten sonra, sunucu aynı adın tekrar istenmesi durumunda numaralandırılmış adresi geçici olarak saklar.

DNS, sunucular arasında aynı ileti biçimini kullanır; her tür istemci sorgusu ve sunucu yanıtları, hata iletileri ve kaynak kaydı bilgilerinin aktarımı için bir soru, yanıt, yetki ve ek bilgilerden oluşur.

| DNS mesaj bölümü | Açıklama |
|---|---|
| Question | İsim sunucusu için soru |
| Answer | Soruyu cevaplayan kaynak kayıtları |
| Authority | Bir otoriteye işaret eden kaynak kayıtları |
| Additional | Ek bilgi tutan kaynak kayıtları |

## DNS Hiyerarşisi

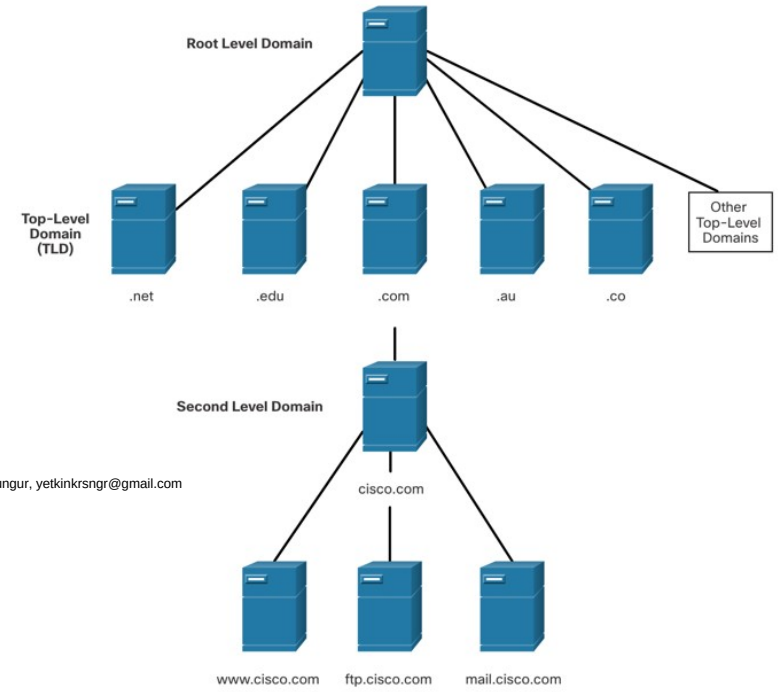
DNS, ad çözümlemesi sağlamak üzere bir veritabanı oluşturmak için hiyerarşik bir sistem kullanır.

Her DNS sunucusu belirli bir veritabanı dosyasını tutar ve yalnızca tüm DNS yapısının bu küçük kısmı için ad-IP eşlemelerini yönetmekten sorumludur.

Bir DNS sunucusu, DNS bölgesi içinde olmayan bir ad çevirisi için istek aldığında, DNS sunucusu isteği çeviri için uygun bölge içindeki başka bir DNS sunucusuna iletir.

Üst düzey-top-level (TLD) alanlara örnekler:

- .com- a business or industry
- .org- a non-profit organization
- .au- Australia




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## nslookup komutu

Nslookup, kullanıcının belirli bir ana bilgisayar adını çözmek için aygıtta yapılandırılmış DNS sunucularını el ile sorgulamasına olanak tanıyan bir bilgisayar işletim sistemi yardımcı programıdır.

Bu yardımcı program, ad çözümleme sorunlarını gidermek ve ad sunucularının geçerli durumunu doğrulamak için de kullanılabilir.

Nslookup komutu verildiğinde, ana makineniz için yapılandırılmış varsayılan DNS sunucusu görüntülenir.

Bir ana bilgisayarın veya alanın adı nslookup komut istemine girilebilir.

```
C:\Users> nslookup
Default Server:  dns-sj.cisco.com
Address:  171.70.168.183
> www.cisco.com
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    origin-www.cisco.com
Addresses:  2001:420:1101:1::a
          173.37.145.84
Aliases:  www.cisco.com
> cisco.netacad.net
Server:  dns-sj.cisco.com
Address:  171.70.168.183
Name:    cisco.netacad.net
Address:  72.163.6.223
>
```

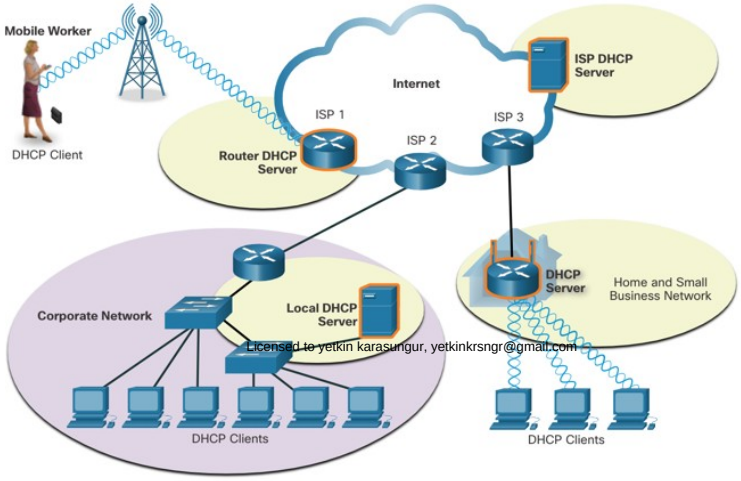
## 14.4.2.Dynamic Host Configuration Protocol

IPv4 hizmeti için Dinamik Ana Bilgisayar Yapılandırma Protokolü-Dynamic Host Configuration Protocol (DHCP), IPv4 adreslerinin, alt ağ maskelerinin, ağ geçitlerinin ve diğer IPv4 ağ parametrelerinin atanmasını otomatikleştirir.

DHCP, statik adreslemeye kıyasla dinamik adresleme olarak kabul edilir. Statik adresleme IP adresi bilgilerinin manuel olarak girilmesidir.

Bir ana bilgisayar ağa bağlandığında, DHCP sunucusuyla iletişim kurulur ve bir adres istenir. DHCP sunucusu, havuz adı verilen yapılandırılmış adreslerden bir adres seçer ve bunu ana bilgisayara atar (kiralar-lease).

Birçok ağ hem DHCP hem de statik adresleme kullanır. DHCP, son kullanıcı aygıtları gibi genel amaçlı ana makineler için kullanılır. Statik adresleme, ağ geçidi yönlendiricileri, anahtarlar, sunucular ve yazıcılar gibi ağ aygıtları için kullanılır.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not: IPv6 için DHCP (DHCPv6), IPv6 istemcileri için benzer hizmetler sağlar. Ancak, DHCPv6 varsayılan bir ağ geçidi adresi sağlamaz. Bu, yalnızca yönlendiricinin Yönlendirici Reklamı(RA) mesajından dinamik olarak elde edilebilir.

DHCP Süreci:

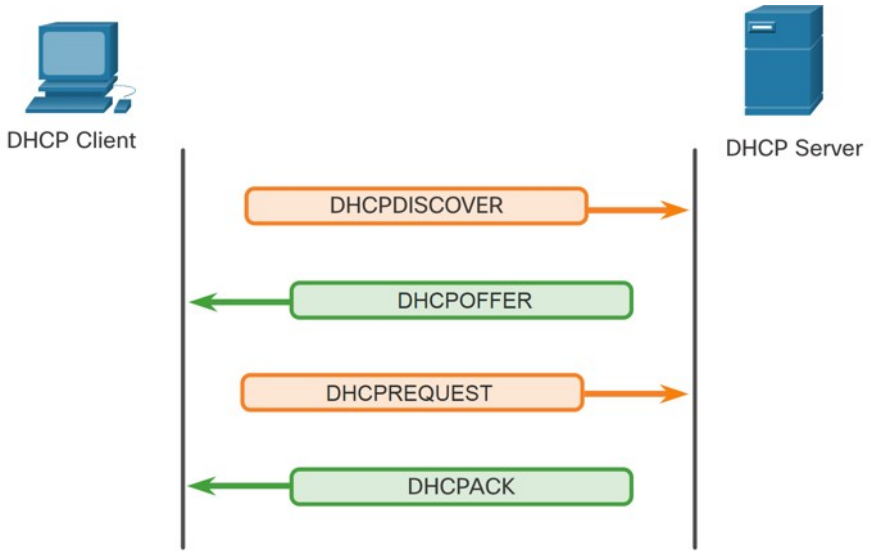
IPv4, DHCP yapılandırılmış bir aygıt önyükleme yaptığında veya ağa bağlandığında, istemci ağdaki kullanılabilir DHCP sunucularını tanımlamak için bir DHCP bulma (DHCPDISCOVER) iletisi yayınlar.

Bir DHCP sunucusu, istemciye kiralama sağlayan bir DHCP teklif (DHCPOFFER) mesajıyla yanıt verir. (İstemci ağdaki birden çok DHCP sunucusu nedeniyle birden fazla teklif alırsa, bir tane seçmelidir.)

İstemci, istemcinin kabul ettiği açık sunucuyu ve kiralama teklifini tanımlayan bir DHCP isteği (DHCPREQUEST) iletisi gönderir.

Sunucu daha sonra istemciye kiralama işleminin sonlandırıldığını bildiren bir DHCP onayı (DHCPACK) iletisi döndürür.

Teklif artık geçerli değilse, seçilen sunucu DHCP negatif alındı bildirimi (DHCPNAK) iletisiyle yanıt verir ve işlem yeni bir DHCPDISCOVER iletisiyle başlamalıdır.

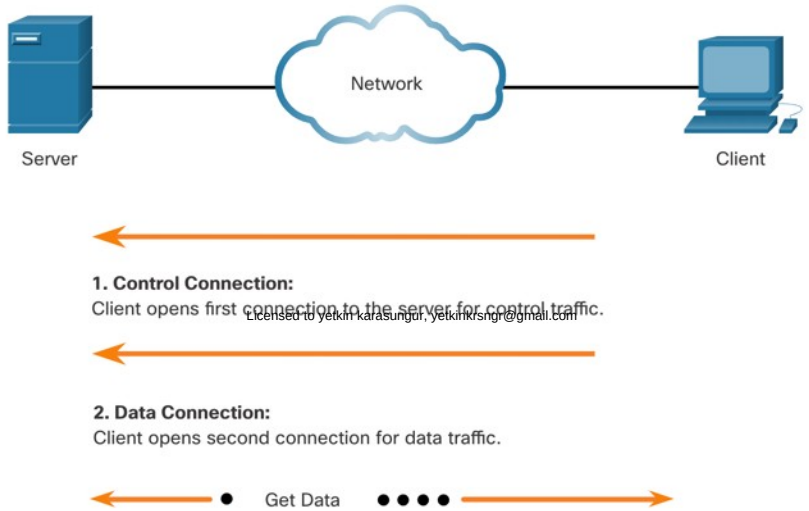



Not:DHCPv6, DHCPv4'tekine benzer bir dizi iletiye sahiptir. DHCPv6 mesajları SOLICIT, ADVERTISE, INFORMATION REQUEST ve REPLY'dir.

## 14.5.Dosya Paylaşım Hizmetleri

### 14.5.1.File Transfer Protocol

FTP, bir istemci ile bir sunucu arasında veri aktarımına izin verecek şekilde geliştirilmiştir. FTP istemcisi, bir FTP sunucusundan veri göndermek ve almak için kullanılan bir bilgisayarda çalışan bir uygulamadır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Adım 1 - İstemci, TCP bağlantı noktası 21'i kullanarak trafiği kontrol etmek için sunucuya ilk bağlantıyı kurar. Trafik, istemci komutları ve sunucu yanıtlarından oluşur.
Adım 2 - İstemci, TCP bağlantı noktası 20'yi kullanarak gerçek veri aktarımı için sunucuya ikinci bağlantıyı kurar. Bu bağlantı aktarılacak her veri olduğunda oluşturulur.

Adım 3 - Veri aktarımı her iki yönde de yapılabilir. İstemci verileri sunucudan indirebilir (çekebilir) veya istemci sunucuya veri yükleyebilir (gönderebilir).

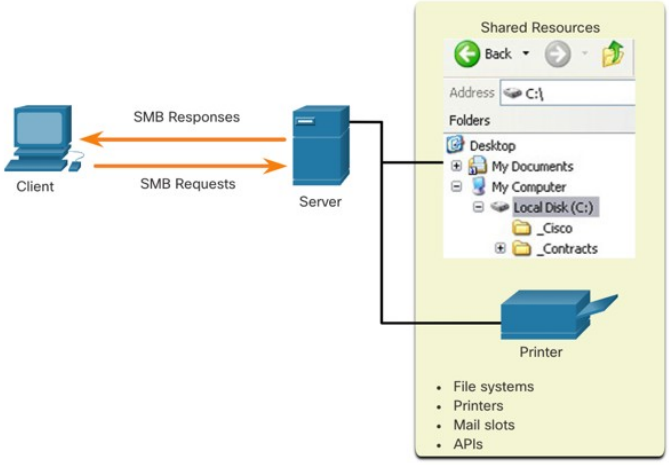
## 14.5.2.Server Message Block-Sunucu İleti Bloğu

Sunucu İleti Bloğu-Server Message Block (SMB) bir istemci / sunucu, istek yanıtı dosya paylaşım protokolüdür. Sunucular kendi kaynaklarını ağdaki istemciler için kullanılabilir hale getirebilir.

SMB mesajlarının üç işlevi:

- Oturumları başlatma, kimlik doğrulaması yapma ve sonlandırma
- Dosya ve yazıcı erişimini kontrol etme
- Bir uygulamanın başka bir cihaza / cihazdan mesaj göndermesine veya almasına izin verme

FTP tarafından desteklenen dosya paylaşımının aksine, istemciler sunuculara uzun vadeli bir bağlantı kurar. Bağlantı kurulduktan sonra, istemci kullanıcı, kaynak istemci ana bilgisayarında yerelmiş gibi sunucudaki kaynaklara erişebilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 15. Bölüm: Ağ Güvenliği Temelleri

## 15.1.Security Threats and Vulnerabilities-Güvenlik Tehditleri ve Güvenlik Açıkları

### 15.1.1.Tehdit Türleri

Bir ağa yapılan saldırılar yıkıcı olabilir ve hasar veya önemli bilgi veya varlıkların çalınması nedeniyle zaman ve para kaybına neden olabilir. Davetsiz misafirler ağa yazılım açıkları, donanım saldırıları veya birinin kullanıcı adını ve şifresini tahmin ederek erişebilir. Yazılımı değiştirerek veya yazılım açıklarından yararlanarak erişim sağlayan davetsiz misafirlere tehdit aktörleri-oyuncuları-threat actors denir.

Tehdit oyuncusu ağa eriştikten sonra dört tür tehdit ortaya çıkabilir:

- Information Theft-Bilgi Hırsızlığı
- Data Loss and manipulation-Veri Kaybı ve Değiştirme
- Identity Theft-Kimlik Hırsızlığı
- Disruption of Service-Hizmetin Kesilmesi

### 15.1.2.Güvenlik Açıkları Türleri

Güvenlik açığı, bir ağdaki veya bir aygıttaki zayıflık derecesidir. Bir dereceye kadar güvenlik açığı, yönlendiriciler, anahtarlar, masaüstü bilgisayarlar, sunucular ve hatta güvenlik aygıtlarında bulunur. Genellikle, saldırı altındaki ağ aygıtları, sunucular ve masaüstü bilgisayarlar gibi uç noktalardır.

Üç ana güvenlik açığı veya zayıflık vardır:

- Teknolojik Güvenlik Açıkları TCP / IP Protokolü zayıflıkları, İşletim Sistemi Zayıflıkları ve Ağ Ekipmanı zayıflıklarını içerebilir.
- Yapılandırma Güvenlik Açıkları, güvenli olmayan kullanıcı hesaplarını, kolayca tahmin edilen şifreleri olan sistem hesaplarını, yanlış yapılandırılmış internet hizmetlerini, güvenli olmayan varsayılan ayarları ve yanlış yapılandırılmış ağ ekipmanını içerebilir.
- Güvenlik Politikası Güvenlik açıkları arasında yazılı bir güvenlik politikası eksikliği, politika, kimlik doğrulama sürekliliği eksikliği, uygulanmayan mantıksal erişim denetimleri, yazılım ve donanım kurulumu ve politikaya uymayan değişiklikler ve var olmayan bir olağanüstü durum kurtarma planı yer alabilir.

Bu güvenlik açıklarının üç kaynağı da bir ağı veya cihazı kötü amaçlı kod saldırıları ve ağ saldırıları da dahil olmak üzere çeşitli saldırılara açık bırakabilir.

### 15..1.3.Fiziksel Güvenlik

Ağ kaynakları fiziksel olarak tehlikeye atılabilirse, bir tehdit aktörü ağ kaynaklarının kullanımını durdurabilir. Dört fiziksel tehdit sınıfı aşağıdaki gibidir:

**Hardware threats** -Bu, sunuculara, yönlendiricilere, anahtarlara, kablo tesisine ve iş istasyonlarına fiziksel hasarları içerir.

**Environmental threats** -Bu, aşırı sıcaklıkları (çok sıcak veya çok soğuk) veya aşırı nem (çok ıslak veya çok kuru) içerir.

Licensed to unknown

**Electrical threats** -Buna gerilim ani artışları, yetersiz besleme gerilimi ve güç kaybı dahildir.

**Maintenance threats -**Buna, anahtar elektrik bileşenlerinin (elektrostatik deşarj), kritik yedek parçaların eksikliği, kötü kablolama ve kötü etiketleme dahildir.

## 15.2.Network Attacks-Ağ Saldırıları

### 15.2.1.Types of Malware-Kötü Amaçlı(Zararlı) Yazılım Türleri

Kötü amaçlı yazılım, verilere, ana bilgisayarlara veya ağlara zarar vermek, bozmak, çalmak veya "kötü" veya gayri meşru eylemlere neden olmak için özel olarak tasarlanmış kod veya yazılımdır. Aşağıdakiler kötü amaçlı yazılım türleridir:

**Viruses** -Bilgisayar virüsü, kendisinin bir kopyasını başka bir programa ekleyip başka bir programa dahil olarak yayılan bir kötü amaçlı yazılım türüdür. Bir bilgisayardan diğerine yayılır ve seyahat ederken enfeksiyonlar bırakır.

**Worms** - Bilgisayar solucanları virüslere benzer, çünkü kendilerinin işlevsel kopyalarını çoğaltırlar ve aynı tür hasara neden olabilirler. Virüs bulaşmış bir anasistem dosyasının yayılmasını gerektiren virüslerin aksine, solucanlar bağımsız bir yazılımdır ve çoğaltmak için bir anasistem programı veya insan yardımı gerektirmez.

**Trojan Horses** -Meşru görünen zararlı bir yazılım parçasıdır. Virüslerden ve solucanlardan farklı olarak, Truva atları diğer dosyalara bulaşarak çoğalmaz. Kendi kendini kopyalarlar. Truva atları, e-posta eki açma veya İnternet'ten dosya indirme ve çalıştırma gibi kullanıcı etkileşimi yoluyla yayılmalıdır.

### 15.2.2.Keşif Saldırıları

Kötü amaçlı kod saldırılarına ek olarak, ağların çeşitli ağ saldırılarına karşı kurban olması da mümkündür. Ağ saldırıları üç ana kategoride sınıflandırılabilir:

**Reconnaissance attacks**-Sistemlerin, hizmetlerin veya güvenlik açıklarının keşfi ve eşlenmesi.

**Access attacks**-Verilerin, sistem erişiminin veya kullanıcı ayrıcalıklarının yetkisiz olarak değiştirilmesi.

**Denial of service**-Ağların, sistemlerin veya hizmetlerin devre dışı bırakılması veya bozulması.

Keşif saldırıları için dış tehdit aktörleri, belirli bir şirkete veya kuruma atanan IP adres alanını kolayca belirlemek için nslookup ve whois yardımcı programları gibi internet araçlarını kullanabilir. IP adresi alanı belirlendikten sonra, bir tehdit aktörü etkin adresleri tanımlamak için halka açık IP adreslerine ping atabilir.

### 15.2.3.Erişim Saldırıları

Erişim saldırıları, web hesaplarına, gizli veritabanlarına ve diğer hassas bilgilere erişmek için kimlik doğrulama hizmetlerinde, FTP hizmetlerinde ve web hizmetlerindeki bilinen güvenlik açıklarından yararlanır.

Erişim saldırıları dört tipte sınıflandırılabilir:

**Password attacks -** Kaba kuvvet, truva atı ve paket koklayıcı kullanılarak uygulanır

**Trust exploitation -** Bir tehdit aktörü, bir sisteme erişmek için yetkisiz ayrıcalıklar kullanır ve muhtemelen hedefi tehlikeye atar.

**Port redirection**: - Tehdit oyuncusu, başka hedeflere yönelik saldırıların temeli olarak güvenliği ihlal edilmiş bir sistem kullanır. Örneğin, tehlikeye giren bir ana bilgisayar A. Host A'ya bağlanmak için SSH (bağlantı noktası 22) kullanan bir tehdit aktörü, ana bilgisayar B tarafından güvenilir ve bu nedenle tehdit aktörü buna erişmek için Telnet'i (bağlantı noktası 23) kullanabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Man-in-the middle -** Tehdit aktörü, iki taraf arasında geçen verileri okumak veya değiştirmek için iki meşru taraf arasında konumlandırılır.

### 15.2.4.Denial of Service Attacks-Hizmet Engelleme Saldırısı

Hizmet reddi (DoS) saldırıları en yaygın saldırı türüdür ve ortadan kaldırılması en zor olanlarıdır. Bununla birlikte, uygulama kolaylığı ve potansiyel olarak önemli hasar nedeniyle, DoS saldırıları güvenlik yöneticilerinin özel ilgisini hak ediyor.

- DoS saldırıları birçok şekilde olabilir. Nihayetinde, sistem kaynaklarını tüketerek yetkili kişilerin bir hizmeti kullanmasını engellerler. DoS saldırılarını önlemeye yardımcı olmak için işletim sistemleri ve uygulamalar için en son güvenlik güncellemelerinden haberdar olmak önemlidir.
- DoS saldırıları büyük bir risktir çünkü iletişimi keser ve önemli ölçüde zaman ve para kaybına neden olurlar. Bu saldırıların vasıfsız bir tehdit oyuncusu tarafından bile yürütülmesi nispeten kolaydır.
- DDoS, DoS saldırısına benzer, ancak birden çok koordineli kaynaktan gelir. Örneğin, bir tehdit aktörü, zombiler olarak bilinen virüslü ana bilgisayarlar ağı oluşturur. Bir zombi ağına botnet denir. Tehdit oyuncusu, zombilerin botnet'ine DDoS saldırısı gerçekleştirmesini bildirmek için bir komut ve kontrol (C&C) programı kullanır.

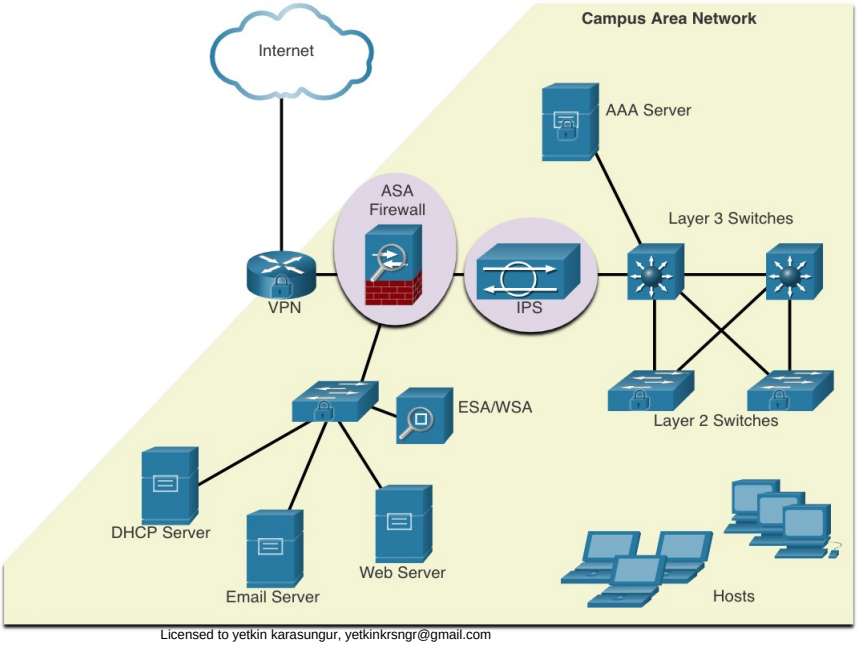
## 15.3.Network Attack Mitigations-Ağ Saldırılarını Azaltma

### 15.3.1.Derinlemesine Savunma Yaklaşımı

Ağ saldırılarını azaltmak için, önce yönlendiriciler, anahtarlar, sunucular ve ana makineler de dahil olmak üzere aygıtları güvenli hale getirmelisiniz. Çoğu kuruluş, güvenliğe yönelik derinlemesine bir savunma yaklaşımı (katmanlı bir yaklaşım olarak da bilinir) kullanır. Bu, birlikte çalışan ağ cihazları ve hizmetlerinin bir kombinasyonunu gerektirir.

Bir kuruluşun kullanıcılarını ve varlıklarını TCP / IP tehditlerine karşı korumak için çeşitli güvenlik aygıtları ve hizmetleri uygulanır:

- VPN
- ASA Firewall
- IPS
- ESA/WSA
- AAA Server




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 15.3.2. Yedekleri Sakla

Cihaz yapılandırmalarını ve verilerini yedeklemek, veri kaybına karşı korunmanın en etkili yollarından biridir. Yedeklemeler, güvenlik ilkesinde tanımlandığı şekilde düzenli olarak gerçekleştirilmelidir. Veri yedeklemeleri, ana tesiste bir şey olursa yedekleme ortamını korumak için genellikle tesis dışında depolanır.

Tabloda yedekleme konuları ve açıklamaları gösterilmektedir.

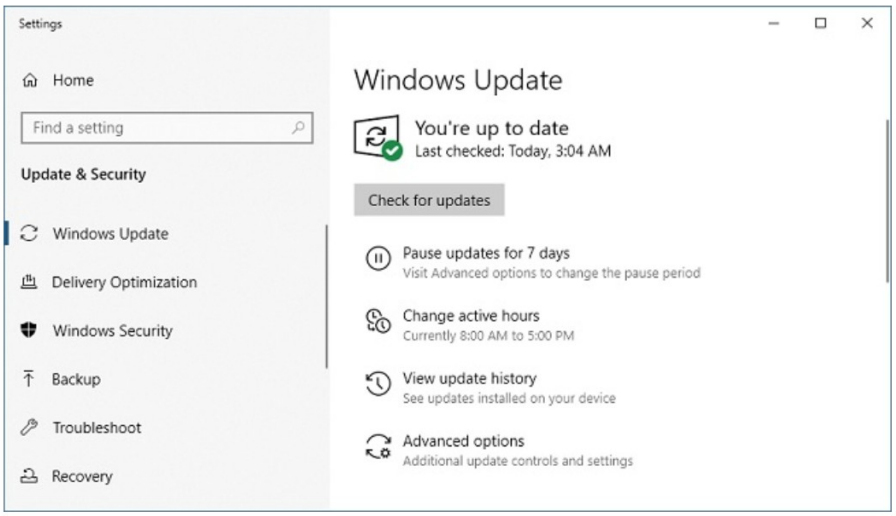
| Önem | Açıklama |
|---|---|
| Frequency | • Güvenlik ilkesinde tanımlandığı şekilde düzenli olarak yedekleme yapın.<br>• Tam yedeklemeler zaman alabilir, bu nedenle sık sık değiştirilen dosyaların kısmi yedekleriyle aylık veya haftalık yedeklemeler gerçekleştirin. |
| Storage | • Verilerin bütünlüğünü sağlamak ve dosya geri yükleme prosedürlerini doğrulamak için her zaman yedeklemeleri doğrulayın. |
| Security | • Yedeklemeler, güvenlik politikasının gerektirdiği şekilde günlük, haftalık veya aylık rotasyonda onaylanmış bir tesis dışı depolama yerine taşınmalıdır. |
| Validation | Yedeklemeler güçlü parolalar kullanılarak korunmalıdır. Verileri geri yüklemek için parola gerekirtirmelidir. |

### 15.3.3. Upgrade, Update, and Patch-Yükseltme, Güncelleme ve Yama

Yeni kötü amaçlı yazılımlar yayınlandıkça, kuruluşların virüsten koruma yazılımının en son sürümlerine güncellemesi gerekir.

Solucan saldırısını azaltmanın en etkili yolu, işletim sistemi satıcısından güvenlik güncelleştirmelerini karşıdan yükleyip tüm savunmasız sistemleri yamamaktır.

Kritik güvenlik yamalarının yönetimine yönelik bir çözüm, tüm son sistemlerin güncellemeleri otomatik olarak indirdiğinden emin olmaktır.




### 15.3.4. Authentication, Authorization, Accounting

Kimlik doğrulama, yetkilendirme ve hesap yönetimi (AAA veya "triple A") ağ güvenlik hizmetleri, ağ aygıtlarında erişim denetimi kurmak için birincil çerçeve sağlar.

AAA, bir ağa kimin erişmesine izin verildiğini (kimlik doğrulaması), ağa erişirken (yetkilendirirken) hangi eylemleri gerçekleştirdiğini ve oradayken neler yapıldığını (muhasebe) kaydetmenin bir yoludur.

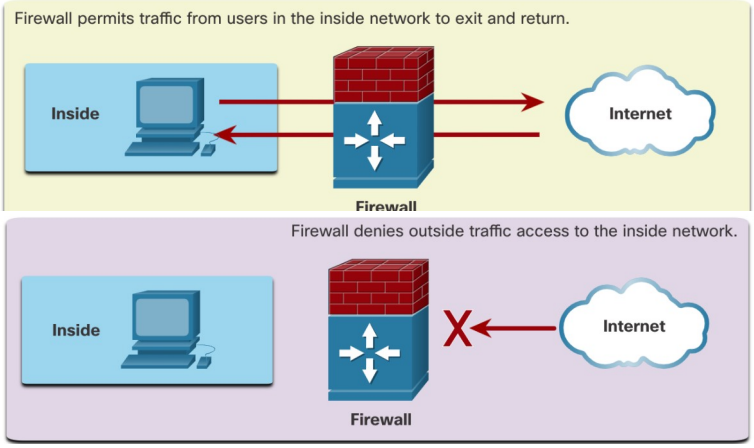
AAA kavramı, kredi kartı kullanımına benzer. Kredi kartı kimin kullanabileceğini, kullanıcının ne kadar harcayabileceğini belirler ve kullanıcının hangi parayı harcadığını hesaba katar.

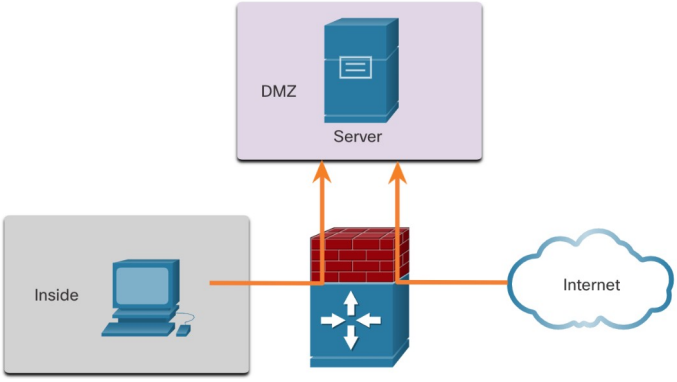
Yüksek Öğrenim Kredi ve Yurtlar Kurumu

## 15.3.5.Firewalls-Ateş Duvarı-Güvenlik Duvarı

Ağ güvenlik duvarları iki veya daha fazla ağ arasında bulunur, aralarındaki trafiği kontrol eder ve yetkisiz erişimi önlemeye yardımcı olur.

Güvenlik duvarı, dış kullanıcıların belirli hizmetlere kontrollü erişimine izin verebilir. Örneğin, dış kullanıcılar tarafından erişilebilen sunucular genellikle askersizleştirilmiş-silahsızlaştırılmış bölge-demilitarized zone (DMZ) olarak adlandırılan özel bir ağda bulunur. DMZ, bir ağ yöneticisinin o ağa bağlı ana bilgisayarlar için belirli politikalar uygulamasını sağlar.




## 15.3.6.Güvenlik Duvarı Çeşitleri

Güvenlik duvarı ürünleri çeşitli şekillerde üretilmiştir. Bu ürünler, bir ağa neyin erişmesine izin verileceğini veya neyin reddedileceğini belirlemek için farklı teknikler kullanır. Bunlar aşağıdakileri içerir:

**Packet filtering**- IP veya MAC adreslerine dayalı erişimi önler veya izin verir

**Application filtering**- Bağlantı noktası numaralarına göre belirli uygulama türlerine erişimi engeller veya izin verir

**URL filtering**- Belirli URL'lere veya anahtar kelimelere göre web sitelerine erişimi engeller veya izin verir

**Stateful packet inspection** (SPI)- Gelen paketler, dahili ana bilgisayarlardan gelen isteklere yasal yanıtlar olmalıdır. İstenmeyen paketler, özellikle izin verilmedikçe engellenir. SPI ayrıca hizmet reddi (DoS) gibi belirli saldırı türlerini tanıma ve filtreleme özelliğini de içerebilir.

## 15.3.7.Endpoint Security-Uç Nokta Güvenliği

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Uç nokta veya ana bilgisayar, ağ istemcisi olarak çalışan tek bir bilgisayar sistemi veya cihazdır. Yaygın uç noktaları dizüstü bilgisayarlar, masaüstü bilgisayarlar, sunucular, akıllı telefonlar ve tabletlerdir.

Uç nokta cihazlarının güvenliğini sağlamak, bir ağ yöneticisinin insan doğasını içerdiği için en zorlu işlerden biridir. Bir şirketin iyi belgelenmiş politikaları olmalı ve çalışanlar bu kuralların farkında olmalıdır.

Çalışanların ağın doğru kullanımı konusunda eğitilmesi gerekir. Politikalar genellikle virüsten koruma yazılımı ve ana bilgisayar saldırılarının önlenmesini içerir. Daha kapsamlı uç nokta güvenlik çözümleri ağ erişim kontrolüne dayanır.

## 15.4.Device Security-Cihaz Güvenliği

### 15.4.1.Cisco AutoSecure

Bir aygıta yeni bir işletim sistemi yüklendiğinde güvenlik ayarları varsayılan değerlere ayarlanır. Çoğu durumda, bu güvenlik seviyesi yetersizdir. Cisco yönlendiricileri için, Cisco AutoSecure özelliği sistemin güvenliğinin sağlanmasına yardımcı olmak için kullanılabilir.

Ayrıca, çoğu işletim sistemi için uygulanması gereken bazı basit adımlar vardır:

- Varsayılan kullanıcı adları ve şifreler derhal değiştirilmelidir.
- Sistem kaynaklarına erişim yalnızca bu kaynakları kullanma yetkisi olan kişilerle sınırlandırılmalıdır.
- Gereksiz servisler ve uygulamalar mümkün olduğunda kapatılmalı ve kaldırılmalıdır.
- Genellikle, üreticiden gönderilen cihazlar bir süre bir depoda durur ve en güncel yamalar kurulmamıştır. Uygulamadan önce herhangi bir yazılımı güncellemek ve güvenlik yamalarını yüklemek önemlidir.

### 15.4.2.Passwords-Parolalar(Şifre Değil!)

Ağ cihazlarını korumak için güçlü parolalar kullanmak önemlidir. İzlenmesi gereken standart yönergeler şunlardır:

- En az sekiz, tercihen 10 veya daha fazla karakterden oluşan bir şifre kullanın.
- Şifreleri karmaşık hale getirin. İzin veriliyorsa, büyük ve küçük harf, sayı, sembol ve boşluk karışımı ekleyin.
- Tekrar, ortak sözlük sözcükleri, harf veya sayı dizileri, kullanıcı adları, akraba veya evcil hayvan adları, doğum tarihleri, kimlik numaraları, ata adları veya diğer kolay tanımlanabilir bilgi parçaları gibi biyografik bilgilere dayalı şifrelerden kaçının.
- Bir şifreyi kasten yanlış yazınız. Örneğin, Smith = Smyth = 5mYth veya Güvenlik = 5ecur1ty.
- Parolaları sık sık değiştirin. Parola bilmeden tehlikeye atılırsa, tehdit oyuncusunun parolayı kullanma fırsatı sınırlıdır.
- Parolaları bir yere yazmayın ve masa veya monitör gibi bariz yerlerde bırakmayın.

Cisco yönlendiricilerinde, parolalar için önde gelen boşluklar yoksayılır, ancak ilk karakterden sonraki boşluklar dikkate alınmaz. Bu nedenle, güçlü bir parola oluşturmanın bir yolu boşluk çubuğunu kullanmak ve birçok kelimeden oluşan bir cümle oluşturmaktır. Buna parola denir. Bir parolanın hatırlanması genellikle basit bir paroladan daha kolaydır. Ayrıca tahmin etmek daha uzun ve daha zordur. Cisco123 yerine aralarda boşluk tuşuna basılmış C i s c o 1 2 3 tercih edilmeli.

### 15.4.3.Ek Parola Güvenliği

Parolaların cisco yönlendirici ve anahtar üzerinde aşağıdakiler de dahil olmak üzere gizli kalmasını sağlamaya yardımcı olmak için atılabilir birkaç adım vardır:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tüm düz metin parolaları **service password-encryption** komutuyla şifreleyin.

Parolaları **security passwords min-length** komutuyla kabul edilebilir bir parola uzunluğuyla belirleyin.

Kaba kuvvet saldırılarını engellemek için **login block-for#attempts#within#** komutunu kullanın.

**exec-timeout** komutuyla belirli bir süre sonra etkin olmayan, ayrıcalıklı bir EXEC modu erişimini devre dışı bırakın.

```
Router(config)# service password-encryption
Router(config)# security password min-length 8
Router(config)# login block-for 120 attempts 3 within 60
Router(config)# line vty 0 4
Router(config-line)# password cisco
Router(config-line)# exec-timeout 5 30
Router(config-line)# transport input ssh
Router(config-line)# end
Router#
Router# show running-config | section line vty
line vty 0 4
 password 7 03095A0F034F
 exec-timeout 5 30
 login
Router#
```

## 15.4.4.Enable SSH-SSH'ı Etkinleştir

Aşağıdaki adımları kullanarak bir Cisco cihazını SSH'yi destekleyecek şekilde yapılandırmak mümkündür:

1. Benzersiz bir cihaz ana bilgisayar adı(hostname) yapılandırın. Bir cihazın varsayılandan farklı bir ana bilgisayar adı olmalıdır.
2. IP etki alanı adını (domain name) yapılandırın. Genel yapılandırma modunda **ip-domain name** komutunu kullanarak ağın IP etki alanı adını yapılandırın.
3. SSH trafiğini şifrelemek için bir anahtar oluşturun. SSH, kaynak ve hedef arasındaki trafiği şifreler. Ancak bunu yapmak için,**crypto key generate rsa general-keys modulus** global yapılandırma komutu kullanılarak benzersiz bir kimlik doğrulama anahtarının oluşturulması gerekir. Modül bitleri anahtarın boyutunu belirler ve 360 bit ila 2048 bit arasında yapılandırılabilir. Bit değeri ne kadar büyük olursa, anahtar o kadar güvenli olur. Bununla birlikte, daha büyük bit değerlerinin bilgilerin şifrelenmesi ve şifresinin çözülmesi daha uzun sürer. Önerilen minimum modül uzunluğu 1024 bittir.
4. Yerel bir veritabanı girişi doğrulayın veya oluşturun. **username** genel yapılandırma komutunu kullanarak yerel bir veritabanı kullanıcı adı girişi oluşturun.
5. Yerel veritabanında kimlik doğrulaması yapın. Yerel veritabanıında vty satırının kimliğini doğrulamak için **login local** yapılandırma komutunu kullanın.
6. Vty gelen SSH oturumlarını etkinleştir. Varsayılan olarak, vty satırlarında giriş oturumuna izin verilmez. Telnet ve SSH dahil olmak üzere **transport input[ssh | telnet]** komutuyla birden çok giriş protokolü belirtebilirsiniz

## 15.4.5.Kullanılmayan Hizmetleri Devre Dışı Bırak

Cisco yönlendiricileri ve anahtarları, ağınızda gerekli olabilecek veya olmayabilecek etkin hizmetlerin bir listesiyle başlar. CPU döngüleri ve RAM gibi sistem kaynaklarını korumak için kullanılmayan hizmetleri devre dışı bırakın ve tehdit aktörlerinin bu hizmetleri kullanmasını önleyin.

Varsayılan olarak açık olan hizmetlerin türü, IOS sürümüne bağlı olarak değişir. Örneğin, IOS-XE'de genellikle yalnızca HTTPS ve DHCP bağlantı noktaları açık olacaktır. Bunu **show ip port all** komutuyla doğrulayabilirsiniz.

IOS-XE öncesi IOS sürümleri **show control-plane host open-ports** komutunu kullanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 16. Bölüm: Küçük Bir Ağ Oluşturma

## 16.1.Küçük Ağdaki Aygıtlar

### 16.1.1.Küçük Ağ Topolojileri

İşletmelerin çoğunluğu küçüktür İş ağlarının çoğu da küçüktür.

Küçük bir ağ tasarımı genellikle basittir.

Küçük ağlar genellikle DSL, kablo veya Ethernet bağlantısı ile sağlanan tek bir WAN bağlantısına sahiptir.

Büyük ağlar, ağ cihazlarının bakımı, güvenliği ve sorunlarının giderilmesi ve kurumsal verilerin korunması için bir BT departmanı gerektirir. Küçük ağlar yerel bir BT teknisyeni veya sözleşmeli bir uzman tarafından yönetilir.

### 16.1.2.Küçük Bir Ağ için Cihaz Seçimi

Büyük ağlar gibi, küçük ağlar da kullanıcı gereksinimlerini karşılamak için planlama ve tasarım gerektirir. Planlama, tüm gereksinimlere, maliyet faktörlerine ve dağıtım seçeneklerine gereken önem verilmesini sağlar. İlk tasarım hususlarından biri, ağı desteklemek için kullanılacak aracı cihazların türüdür.

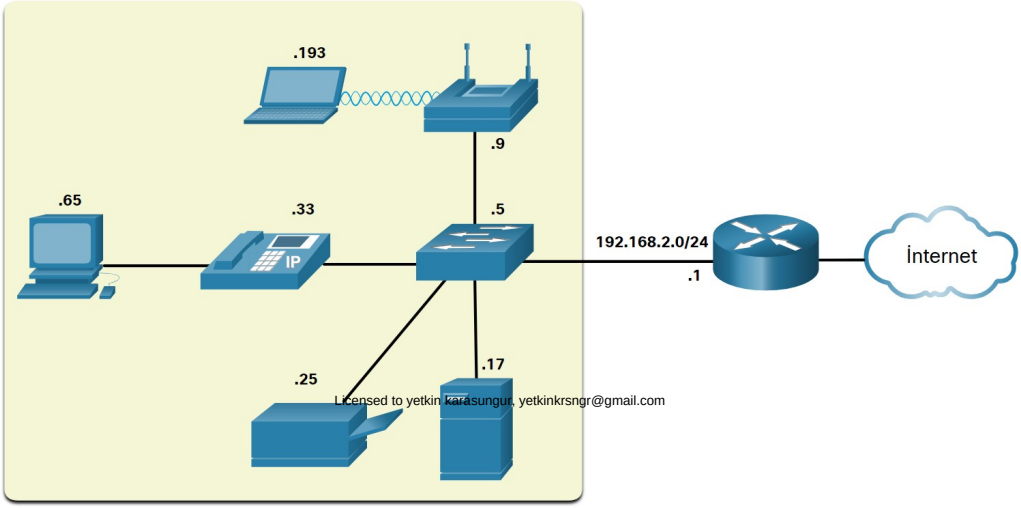
Ağ aygıtlarını seçerken dikkate alınması gereken faktörler şunlardır:

- maliyet
- bağlantı noktası / arabirim hızı ve türleri
- genişletilebilirliği
- işletim sistemi özellikleri ve hizmetleri

### 16.1.3.Küçük Ağ için IP Adresleme

Bir ağı uygularken, bir IP adresleme şeması oluşturun ve kullanın. Bir ağdaki tüm ana bilgisayarların ve cihazların benzersiz bir adresi olmalıdır. IP adresleme şemasını dikkate alacak cihazlar aşağıdakileri içerir:

- Son kullanıcı cihazları - Bağlantı sayısı ve tipi (kablolu, kablosuz, uzaktan erişim)
- Sunucular ve çevre birimleri aygıtları (örneğin, yazıcılar ve güvenlik kameraları)
- Anahtarlar ve erişim noktaları dahil aracı cihazlar



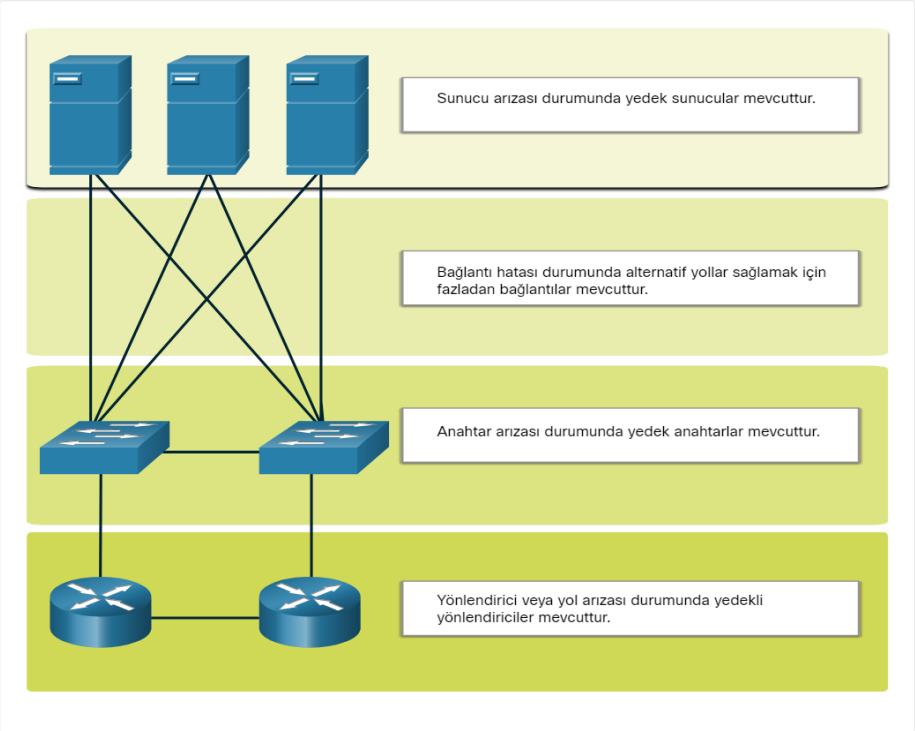
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aygıt türüne göre bir IP adresleme düzeni planlamanız, belgelemeniz ve korumanız önerilir. Planlı bir IP adresleme düzeninin kullanılması, bir aygıt türünü belirlemeyi ve sorunları gidermeyi kolaylaştırır.

### 16.1.4.Redundancy in a Small Network-Küçük Ağda Yedeklilik(Fazlalık-Artıklık)

Yüksek derecede güvenilirlik sağlamak için ağ tasarımında yedeklilik gereklidir. Artıklık, tek hata noktalarının ortadan kaldırılmasına yardımcı olur.

Artıklık, yinelenen ekipmanların kurulmasıyla gerçekleştirilebilir. Kritik alanlar için yinelenen ağ bağlantıları sağlayarak da gerçekleştirilebilir.

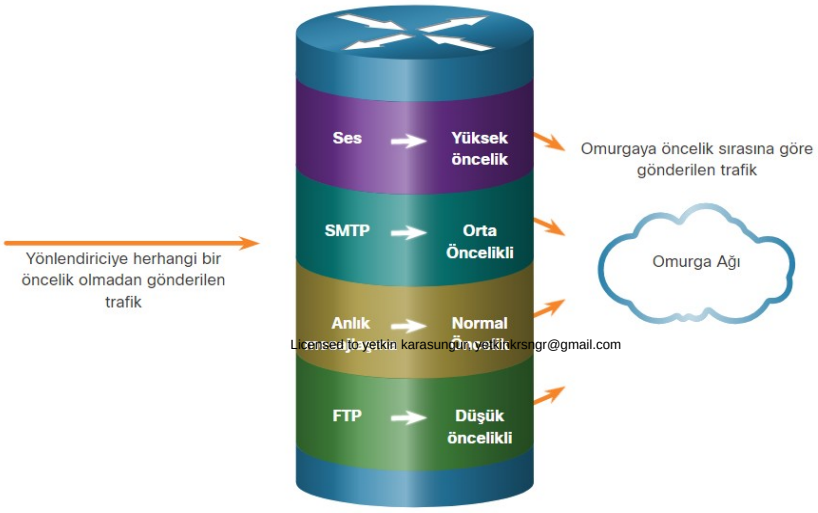



### 16.1.5.Trafik Yönetimi

İyi bir ağ tasarımının amacı, çalışanların verimliliğini artırmak ve ağ kesintilerini en aza indirmektir.

Küçük bir ağdaki yönlendiriciler ve anahtarlar, ses ve video gibi gerçek zamanlı trafiği, diğer veri trafiğine göre uygun bir şekilde destekleyecek şekilde yapılandırılmalıdır. İyi bir ağ tasarımı hizmet kalitesini (QoS) uygulayacaktır.

Öncelik sıralamanın dört kuyruğu vardır. Yüksek öncelikli kuyruk her zaman önce gönderilir.



Licensed to yetkin karasungur yetkinkrsngr@gmail.com

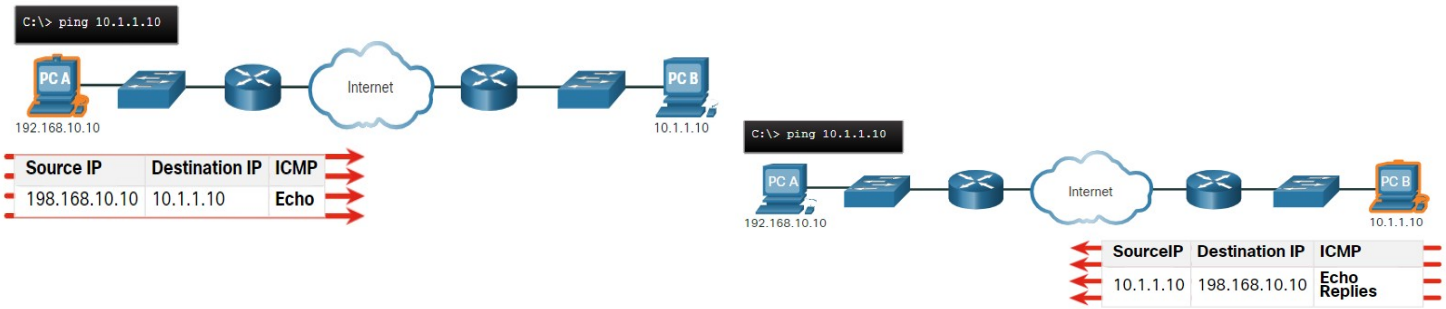
## 16.2.Bağlantıyı Doğrulama

### 16.2.1.Ping ile Bağlantıyı Doğrulayın

Ağınız küçük ve yeni olsun ya da mevcut bir ağı ölçeklendiriyor olsanız da, bileşenlerinizin birbirine ve internete düzgün bir şekilde bağlandığını her zaman doğrulamak isteyebilirsiniz.

Çoğu işletim sisteminde bulunan ping komutu, kaynak ve hedef IP adresi arasındaki Katman 3 bağlantısını hızlı bir şekilde test etmenin en etkili yoludur.

Ping komutu, Internet Denetim İletisi Protokolü- Internet Control Message Protocol (ICMP) yankı- echo ( (ICMP Tür 8) ve yankı yanıtı-echo reply (ICMP Tür 0) iletilerini kullanır.




Komut çıkışında gösterildiği gibi, PC A, PC-B'den Katman 3 ağ bağlantısını doğrulayan yankı yanıtları almıştır.

```
C:\Users\PC-A> ping 10.1.1.10
Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time=47ms TTL=51
Reply from 10.1.1.10: bytes=32 time=60ms TTL=51
Reply from 10.1.1.10: bytes=32 time=53ms TTL=51
Reply from 10.1.1.10: bytes=32 time=50ms TTL=51
Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 47ms, Maximum = 60ms, Average = 52ms
C:\Users\PC-A>
```

Çıktı, PC A ve PC B arasındaki Katman 3 bağlantısını doğrular.

Cisco IOS **ping** komutu çıktısı, bir Windows ana bilgisayarından farklılık gösterir. Örneğin, IOS pingi çıktıda gösterildiği gibi beş ICMP yankı mesajı gönderir.

```
R1# ping 10.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
```

Dikkat edin **!!!!!** çıktı karakterleri. IOS **ping** komutu, alınan her ICMP yankı yanıtı için bir gösterge görüntüler. Tablo, **ping** komutundaki en yaygın çıktı karakterlerini listeler .

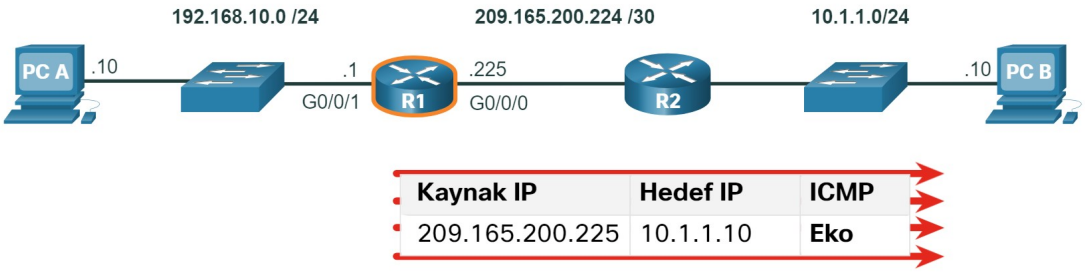
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## IOS Ping Göstergeleri

| Element | Description |
|---|---|
| ! | • Ünlem işareti, yankı yanıt mesajının başarıyla alındığını gösterir.<br>• Kaynak ve hedef arasındaki Katman 3 bağlantısını doğrular. |
| . | • Bir süre, yankı yanıt mesajını beklerken sürenin dolduğu anlamına gelir.<br>• Bu, yol boyunca bir yerde bir bağlantı sorununun oluştuğunu gösterir. |
| U | • Büyük U harfi, ICMP Tip 3 “hedefe ulaşılamıyor” hata iletisiyle yanıtlanan yol boyunca bir yönlendiriciyi belirtir.<br>• Olası nedenler arasında, yönlendiricinin hedef ağın yönünü bilmemesi veya hedef ağdaki ana makineyi bulamaması bulunmaktadır. |

# Gelişmiş (Extended) Ping

Standart bir ping , ping kaynağı olarak hedef ağa en yakın arayüzün IP adresini kullanır . Örnekte gösterildiği gibi, R1'deki ping 10.1.1.10 komutunun kaynak IP adresi G0 / 0/0 arayüzünün (yani 209.165.200.225) adresi olacaktır.




Cisco IOS, ping komutunun "genişletilmiş" bir modunu sunar . Bu mod, kullanıcının komut işlemiyle ilgili parametreleri ayarlayarak özel ping türleri oluşturmasına olanak tanır.

Genişletilmiş ping, ayrıcalıklı EXEC modunda hedef IP adresi olmadan ping yazılarak girilir . Daha sonra genişletilmiş pingi özelleştirmeniz için size birkaç komut verilecektir .

Not: Enter tuşuna basılması , belirtilen varsayılan değerleri kabul eder.

```
R1# ping
Protocol [ip]:
Target IP address: 10.1.1.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Ingress ping [n]:
Source address or interface: 192.168.10.1
DSCP Value [0]:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0x0000ABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
R1#
```

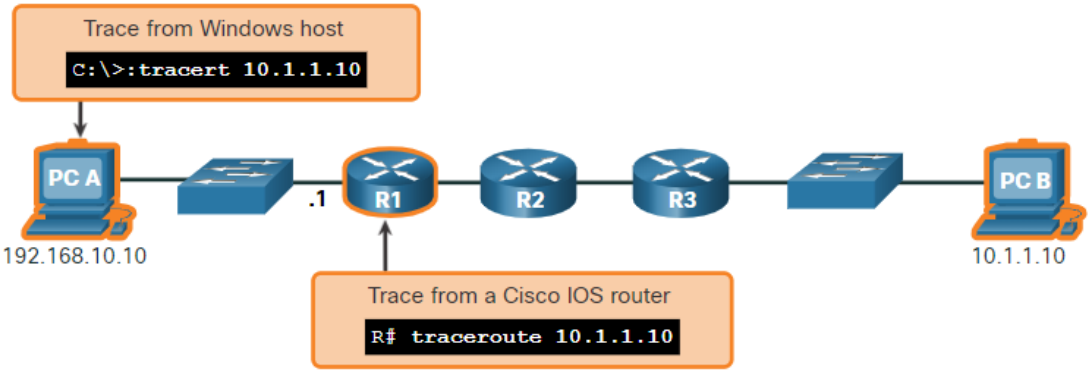
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 16.2.2. Traceroute ile Bağlantıyı Doğrulama

Ping komutu, Katman 3 bağlantı sorunu olup olmadığını hızlı bir şekilde belirlemek için kullanışlıdır. Ancak, sorunun yol boyunca nerede bulunduğunu tanımlamaz.

Traceroute, ağdaki Katman 3 sorunlu alanların bulunmasına yardımcı olabilir. Bir paket bir ağ üzerinden yönlendirilirken izleme(trace), atlamaların(yönlendiricilerin) bir listesini döndürür.

Trace komutunun sözdizimi işletim sistemleri arasında değişiklik gösterir.




Bir Windows 10 bilgisayarında tracert komutunun örnek çıktısı aşağıdadır.
Not: Windows'ta bir tracert'i kesmek için Ctrl-C tuşlarını kullanın.

Tek başarılı yanıt R1'deki ağ geçidinden geldi. Yıldız işaretiyle (*) gösterildiği gibi bir sonraki sekmeye izleme istekleri zaman aşımına uğradı, yani bir sonraki atlama yönlendiricisinin yanıt vermediği veya ağ yolunda bir hata olduğu anlamına gelir. Bu örnekte R1 ve R2 arasında bir sorun var gibi görünmektedir.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.10 over a maximum of 30 hops:
  1     2 ms     2 ms     2 ms  192.168.10.1
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
^C
C:\Users\PC-A>
```

Aşağıdakiler R1'den traceroute komutunun örnek çıktılarıdır:

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 10.1.1.10 1 msec 0 msec
R1#
```

```
R1# traceroute 10.1.1.10
Type escape sequence to abort.
Tracing the route to 10.1.1.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 0 msec 1 msec
  2 209.165.200.230 1 msec 0 msec 1 msec
  3 *  *  *
  4 *  *  *
  5 *
```

Solda, tracert PC B'ye başarılı bir şekilde ulaşabileceğini doğruladı.
Sağ tarafta, 10.1.1.10 ana makinesi mevcut değildi ve çıktıda yanıtların zaman aşımına uğradığı yıldız işaretleri gösteriliyor. Zaman aşımları, olası bir ağ sorununu gösterir.
Cisco IOS'ta bir tracert'i kesmek için Ctrl-Shift-6 tuşlarını kullanın.

kasimbozdogan@kasimbozdogan.com kasimbozdogan@gmail.com

## Genişletilmiş Traceroute

Genişletilmiş ping komutu gibi, genişletilmiş bir traceroute komutu da vardır. Yöneticinin komut işlemiyle ilgili parametreleri ayarlamasını sağlar.

Windows tracert komutu, komut satırındaki seçenekler aracılığıyla birkaç parametrenin girilmesine izin verir. Ancak, genişletilmiş traceroute IOS komutu gibi yönlendirilmez. Aşağıdaki çıktıda Windows tracert komutu için kullanılabilir seçenekler gösterilmektedir:

```
C:\Users\PC-A> tracert /?
Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name
Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
C:\Users\PC-A>
```

Cisco IOS genişletilmiş **traceroute** seçeneği, kullanıcının komut işlemiyle ilgili parametreleri ayarlayarak özel bir izleme türü oluşturmasını sağlar.

Genişletilmiş traceroute, hedef IP adresi olmadan traceroute yazarak ayrıcalıklı EXEC moduna girilir. IOS, tüm farklı parametrelerin ayarlanmasıyla ilgili bir dizi bilgi istemi sunarak komut seçeneklerinde size yol gösterecektir.

Not: Enter'a basmak belirtilen varsayılan değerleri kabul eder ve uygular.

```
R1# traceroute
Protocol [ip]:
Target IP address: 10.1.1.10
Ingress traceroute [n]:
Source address: 192.168.10.1
DSCP Value [0]:
Numeric display [n]:
Timeout in seconds [3]:
Probe count [3]:
Minimum Time to Live [1]:
Maximum Time to Live [30]:
Port Number [33434]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Type escape sequence to abort.
Tracing the route to 192.168.10.10
VRF info: (vrf in name/id, vrf out name/id)
  1 209.165.200.226 1 msec 1 msec 1 msec
  2 209.165.200.230 0 msec 1 msec 0 msec
  3  *
    10.1.1.10 2 msec 2 msec
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 16.3.Ana Bilgisayar (Host) ve IOS Komutları

### 16.3.1.Windows Bilgisayarda IP Yapılandırması

Windows 10'da, dört önemli ayarı hızlı bir şekilde görüntülemek için IP adresi ayrıntılarına Ağ ve Paylaşım Merkezi'nden erişebilirsiniz: adres, maske, yönlendirici ve DNS. Veya bir Windows bilgisayarın komut satırından ipconfig komutunu verebilirsiniz.

MAC adresini ve aygıtın Katman 3 adreslemesiyle ilgili bir dizi ayrıntıyı görüntülemek için **ipconfig / all** komutunu kullanın.

Bir ana bilgisayar DHCP istemcisi olarak yapılandırılmışsa, IP adresi yapılandırması **ipconfig / release** ve **ipconfig / renew** komutları kullanılarak yenilenebilir.

Windows PC'lerde DNS İstemcisi hizmeti, önceden çözümlenmiş adları bellekte depolayarak DNS ad çözümlemesinin performansını da en iyi duruma getirir. **ipconfig / displaydns** komutu, bir Windows bilgisayar sistemindeki tüm önbelleğe alınmış DNS girdilerini görüntüler.

```
C:\Users\PC-A> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : PC-A-00H20
   Primary Dns Suffix  . . . . . . . : cisco.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cisco.com
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 192.168.10.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

```
C:\Users\PC-A> ipconfig /release
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   Default Gateway . . . . . . . . . :
(Output omitted)
C:\Users\PC-A> ipconfig /renew
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.124
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
(Output omitted)
C:\Users\PC-A>
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
C:\Users\PC-A> ipconfig /displaydns
Windows IP Configuration
(Output omitted)
    netacad.com
    ----------------------------------------
    Record Name . . . . . : netacad.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 602
    Data Length . . . . . : 4
    Section . . . . . : Answer
    A (Host) Record . . . : 54.165.95.219
(Output omitted)
```

## 16.3.2.Linux Bilgisayarda IP Yapılandırması

Bir Linux makinesinde GUI kullanarak IP ayarlarını doğrulama, Linux dağıtımına ve masaüstü arayüzüne bağlı olarak değişir.

Komut satırında, o anda etkin olan arabirimlerin durumunu ve IP yapılandırmalarını görüntülemek için **ifconfig** komutunu kullanın.

Linux'ta **ip adresss** komutu adresleri ve özelliklerini görüntülemek için kullanılır. IP adresleri eklemek veya silmek için de kullanılabilir.

Not: Görüntülenen çıktı Linux dağıtımına bağlı olarak değişebilir.

```
[analyst@secOps ~]$ ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:b5:d6:cb
          inet addr: 10.0.2.15  Bcast:10.0.2.255  Mask: 255.255.255.0
          inet6 addr: fe80::57c6:ed95:b3c9:2951/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1332239 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105910 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1855455014 (1.8 GB)  TX bytes:13140139 (13.1 MB)
lo: flags=73  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

## 16.3.3.MacOS Bilgisayarda IP Yapılandırması

Mac ana bilgisayarının GUI'sinde, IP adresleme bilgilerini almak için Ağ Tercihleri> Gelişmiş'i açın.

**ifconfig** komutu, komut satırındaki arabirim IP yapılandırmasını doğrulamak için de kullanılabilir.

Ana bilgisayar IP ayarlarını doğrulamak için diğer kullanışlı macOS komutları arasında networketup -listallnetworkservices ve networketup -getinfo <network service> bulunur.

```
MacBook-Air:~ Admin$ networksetup -listallnetworkservices
An asterisk (*) denotes that a network service is disabled.
iPhone USB
Wi-Fi
Bluetooth PAN
Thunderbolt Bridge
MacBook-Air:~ Admin$
MacBook-Air:~ Admin$ networksetup -getinfo Wi-Fi
DHCP Configuration
IP address: 10.10.10.113
Subnet mask: 255.255.255.0
Router: 10.10.10.1
Client ID:
IPv6: Automatic
IPv6 IP address: none
IPv6 Router: none
Wi-Fi ID: c4:b3:01:a0:64:98
MacBook-Air:~ Admin$
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 16.3.4.arp Komutu

arp komutu Windows, Linux veya Mac komut isteminden yürütülür. Komut o anda ana bilgisayarın ARP önbelleğinde bulunan tüm cihazları listeler.

**arp -a** komutu bilinen IP adresini ve MAC adresi bağlayıcısını görüntüler. ARP önbelleği yalnızca son erişilen cihazlardan gelen bilgileri görüntüler.

```
C:\Users\PC-A> arp -a
Interface: 192.168.93.175 --- 0xc
  Internet Address      Physical Address      Type
  10.0.0.2              d0-67-e5-b6-56-4b     dynamic
  10.0.0.3              78-48-59-e3-b4-01     dynamic
  10.0.0.4              00-21-b6-00-16-97     dynamic
  10.0.0.254            00-15-99-cd-38-d9     dynamic
```

ARP önbelleğinin doldurulduğundan emin olmak için, bir aygıta ARP tablosunda bir giriş olacak şekilde ping atın.

Ağ yöneticisinin önbelleği güncellenmiş bilgilerle yeniden doldurmak istemesi durumunda, önbellek **netsh interface ip delete arpcache** komutu kullanılarak temizlenebilir.

**Not: netsh interface ip delete arpcache komutunu** kullanabilmek için ana bilgisayarda yönetici erişimine ihtiyacınız olabilir.

## 16.4.Sorun Giderme Metotları

### 16.4.1.Temel Sorun Giderme Yaklaşımları

| Adım | Açıklama |
|---|---|
| **Adım 1. Sorunu Belirleyin** | • Bu, sorun giderme işleminin ilk adımıdır.<br>• Araçlar bu adımda kullanılabilse de, sorun yaşayan kullanıcı ile bir konuşma genellikle çok yararlıdır. |
| **Adım 2. Olası Sebepler Teorisi Oluşturma** | • Sorun tanımlandıktan sonra, olası nedenler teorisini oluşturmaya çalışın.<br>• Bu adım genellikle soruna birkaç olası sebepten daha fazlasını verir. |
| **Adım 3. Nedeni Belirlemek için Teoriyi Test Edin** | • Olası nedenlere dayanarak, sorunun nedeninin hangisi olduğunu belirlemek için teorilerinizi test edin.<br>• Bir teknisyen testi çözmek ve sorunu çözüp çözmediğini görmek için hızlı bir düzeltme uygulayabilir.<br>• Hızlı bir düzeltme sorunu çözmezse, kesin nedeni belirlemek için sorunu daha ayrıntılı bir şekilde araştırmanız gerekebilir. |
| **Adım 4. Bir Eylem Planı Oluşturun ve Çözümü Uygulayın** | Sorunun kesin nedenini belirledikten sonra, sorunu çözmek için bir eylem planı oluşturun ve çözümü uygulayın. |
| **Adım 5. Çözümü Doğrulayın ve Önleyici Önlemler Uygulayın** | • Sorunu giderdikten sonra, tam işlevselliği doğrulayın.<br>• Mümkünse, önleyici tedbirler alın. |
| **Adım 6. Bulguları, Eylemleri ve Sonuçları Belgeleyin** | • Sorun giderme işleminin son adımında, bulgularınızı, eylemlerinizi ve sonuçlarınızı belgeleyin.<br>• Bu, ileride başvurmak için çok önemlidir. |

### 16.4.2.debug komutu

IOS **debug** (hata ayıklama) komutu, yöneticinin işletim sistemi sürecini, protokolünü, mekanizmasını ve olay iletilerini gerçek zamanlı olarak analiz için görüntülemesini sağlar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tüm hata ayıklama komutları ayrıcalıklı EXEC modunda girilir. Cisco IOS, hata ayıklama çıktısının yalnızca ilgili özelliği veya alt özelliği içerecek şekilde daraltılmasına izin verir. Hata ayıklama komutlarını yalnızca belirli sorunları gidermek için kullanın.

Tüm hata ayıklama komut seçeneklerinin kısa bir açıklamasını listelemek için **debug ?** komutunu ayrıcalıklı EXEC modunda komut satırında kullanın.

Belirli bir hata ayıklama özelliğini kapatmak için, hata ayıklama komutunun önüne **no** anahtar kelimesini ekleyin

Alternatif olarak, komutun **undebug** formunu ayrıcalıklı EXEC modunda girebilirsiniz.

Tüm etkin hata ayıklama komutlarını bir kerede kapatmak için, **undebug all** komutunu kullanın.

**Dikkat!!!Önemli miktarda çıktı üretebildikleri ve sistem kaynaklarının büyük bir bölümünü kullanabildikleri için bazı hata ayıklama komutlarını kullanırken dikkatli olun. Yönlendirici, hata ayıklama mesajlarını görüntülemekle o kadar meşgul olabilir ki, ağ işlevlerini gerçekleştirmek için yeterli işlem gücüne sahip olamaz, hatta hata ayıklamayı kapatmak için komutları işleyemez.**

Örneğin, bir Cisco yönlendiricideki ICMP mesajlarının durumunu izlemek için , örnekte gösterildiği gibi **debug ip icmp** komutunu kullanın .

```
R1# debug ip icmp
ICMP packet debugging is on
R1#
R1# ping 10.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
R1#
*Aug 20 14:18:59.605: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.606: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.608: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.609: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
*Aug 20 14:18:59.611: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1#
```

## 16.5.Sorun Giderme Senaryoları

### 16.5.1.Duplex Operation and Mismatch Issues-Çift Yönlü İşlem ve Uyumsuzluk Sorunları

Birbirine bağlanan Ethernet arabirimleri, en iyi iletişim performansı ve bağlantıda verimsizlik ve gecikmeden kaçınmak için aynı dubleks modda(full-full veya half-half) çalışmalıdır.

Ethernet otomatik anlaşma-autonegotiation özelliği yapılandırmayı kolaylaştırır, sorunları en aza indirir ve birbirine bağlanan iki Ethernet bağlantısı arasındaki bağlantı performansını en üst düzeye çıkarır. Bağlı cihazlar önce desteklenen yeteneklerini duyurur ve ardından her iki uç tarafından desteklenen en yüksek performans modunu seçer.

Bağlı iki aygıttan biri tam çift yönlü, diğeri yarım çift yönlü çalışıyorsa, çift yönlü uyumsuzluk oluşur. Veri iletişimi çift yönlü uyumsuzluğa sahip bir bağlantı üzerinden gerçekleşecek olsa da, bağlantı performansı çok düşük olacaktır.

Dubleks uyumsuzluklarına genellikle yanlış yapılandırılmış bir arabirim veya nadir durumlarda başarısız bir otomatik anlaşma yapılır. Aygıtlar arasındaki iletişim hala devam ettiği için dupleks uyumsuzluklarının giderilmesi zor olabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 16.5.2.IOS Aygıtlarında IP Adresleme Sorunları

Yanlış IPv4 atamasının iki yaygın nedeni, manuel atama hataları veya DHCP ile ilgili sorunlardır.

Ağ yöneticileri genellikle sunucular ve yönlendiriciler gibi aygıtlara IP adreslerini el ile atamak zorundadır. Atama sırasında bir hata yapılırsa, cihazla iletişim sorunlarının oluşması muhtemeldir.

Bir IOS aygıtında, ağ arabirimlerine hangi IPv4 adreslerinin atandığını doğrulamak için **show ip interfaces** veya **show ip interfaces brief** komutlarını kullanın. Örneğin, gösterildiği gibi **show ip interfacebrief** komutunun verilmesi, R1'deki arabirim durumunu doğrular.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   209.165.200.225 YES manual up                    up
GigabitEthernet0/0/1   192.168.10.1    YES manual up                    up
Serial0/1/0            unassigned      NO  unset  down                  down
Serial0/1/1            unassigned      NO  unset  down                  down
GigabitEthernet0       unassigned      YES unset  administratively down down
R1#
```

### 16.5.3. Uç Cihazlarda (Host) IP Sorunlarını

Windows tabanlı makinelerde, aygıt bir DHCP sunucusuyla iletişim kuramadığında, Windows otomatik olarak 169.254.0.0/16 aralığına ait bir adres atar. Bu özelliğe Otomatik Özel IP Adresleme-Automatic Private IP Addressing (APIPA) adı verilir.

APIPA adresine sahip bir bilgisayar ağdaki diğer cihazlarla iletişim kuramayacaktır, çünkü bu cihazlar büyük olasılıkla 169.254.0.0/16 ağına ait olmayacaktır.

Not: Linux ve OS X gibi diğer işletim sistemleri APIPA kullanmaz.

Aygıt DHCP sunucusuyla iletişim kuramıyorsa, sunucu belirli ağ için bir IPv4 adresi atayamaz ve aygıt iletişim kuramaz.

Windows tabanlı bir bilgisayara atanan IP adreslerini doğrulamak için **ipconfig** komutunu kullanın.

### 16.5.4.Varsayılan Ağ Geçidi Sorunları

Bir uç aygıt için varsayılan ağ geçidi, uç aygıtla aynı ağa ait olan ve trafiği diğer ağlara yönlendirebilen en yakın ağ aygıtıdır. Bir aygıtta yanlış veya var olmayan bir varsayılan ağ geçidi adresi varsa, uzak ağlardaki aygıtlarla iletişim kuramaz.

IPv4 adresleme sorunlarına benzer şekilde, varsayılan ağ geçidi sorunları yanlış yapılandırma (manuel atama durumunda) veya DHCP sorunları (otomatik atama kullanılıyorsa) ile ilgili olabilir.

Windows tabanlı bilgisayarlarda varsayılan ağ geçidini doğrulamak için ipconfig komutunu kullanın.

Yönlendiricide, yönlendirme tablosunu listelemek için **show ip route** komutunu kullanın ve varsayılan yol olarak bilinen varsayılan ağ geçidinin ayarlandığını doğrulayın. Bu yol, paketin hedef adresi yönlendirme tablosundaki diğer yollarla eşleşmediğinde kullanılır.

```
C:\Users\PC-A> ipconfig
Windows IP Configuration
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
(Output omitted)
```

Licensed to yetkin korasungur, yetkinkrsngr@gmail.com

### 16.5.5.DNS Sorunlarını Giderme

Kullanıcıların bir internet bağlantısının çalışmamasını yanlışlıkla DNS'nin kullanılabilirliği ile ilişkilendirmesi yaygındır.

DNS sunucusu adresleri manuel veya otomatik olarak DHCP üzerinden atanabilir.

Şirketler ve kuruluşların kendi DNS sunucularını yönetmesi yaygın olsa da, adları çözümlemek için erişilebilir herhangi bir DNS sunucusu kullanılabilir.

Cisco, kimlik avı ve bazı kötü amaçlı yazılım sitelerini filtreleyerek güvenli DNS hizmeti sağlayan OpenDNS sunar. OpenDNS adresleri 208.67.222.222 ve 208.67.220.220'dir. Web içeriği filtreleme ve güvenlik gibi gelişmiş özellikler aileler ve işletmeler tarafından kullanılabilir.

Windows bilgisayarı tarafından hangi DNS sunucusunun kullanıldığını doğrulamak için **ipconfig / all** komutunu kullanın.

```
C:\Users\PC-A> ipconfig /all
(Output omitted)
Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : F8-94-C2-E4-C5-0A
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a4aa:2dd1:ae2d:a75e%16(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.10(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : August 17, 2019 1:20:17 PM
   Lease Expires . . . . . . . . . . : August 18, 2019 1:20:18 PM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 100177090
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 208.67.222.222
   NetBIOS over Tcpip. . . . . . . . : Enabled
(Output omitted)
```

**Nslookup** komutu bilgisayarlar için kullanışlı bir DNS sorun giderme aracıdır. Nslookup ile kullanıcı elle DNS sorguları yapabilir ve DNS yanıtını analiz edebilir.

```
C:\Users\PC-A> nslookup
Default Server:  Home-Net
Address:  192.168.1.1
> cisco.com
Server:  Home-Net
Address:  192.168.1.1
Non-authoritative answer:
Name:    cisco.com
Addresses:  2001:420:1101:1::185
          72.163.4.185
> 8.8.8.8
Server:  Home-Net
Address:  192.168.1.1
Name:    dns.google
Address:  8.8.8.8
>
> 208.67.222.222
Server:  Home-Net
Address:  192.168.1.1
Name:    resolver1.opendns.com
Address:  208.67.222.222
>
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 17.Bölüm: Gelişmiş Cihaz Yapılandırmaları

## 17.1.İlk Ayarlarla Bir Anahtarı Yapılandırma

### 17.1.1Switch Boot Sequence- Anahtar Öyükleme Sırası

Bir Cisco anahtarı açıldıktan sonra, aşağıdaki beş adımlı önyükleme sırasından geçer:

Adım 1: İlk olarak, anahtar ROM'da depolanan bir açılışta otomatik sınama-power-on self-test (POST) programı yükler. POST CPU alt sistemini kontrol eder. CPU, DRAM ve flash aygıtının flash dosya sistemini oluşturan kısmını test eder.

Adım 2: Ardından, anahtar önyükleme yükleyic-boot loader  yazılımını yükler. Önyükleme yükleyicisi, POST başarıyla tamamlandıktan hemen sonra çalıştırılan ROM'da depolanan küçük bir programdır.

Adım 3: Önyükleme yükleyicisi düşük seviyeli CPU başlatma işlemini gerçekleştirir. Fiziksel belleğin nereye eşlendiğini, bellek miktarını ve hızını kontrol eden CPU kayıtlarını başlatır.

Adım 4: Önyükleme yükleyicisi, sistem kartındaki flash dosya sistemini başlatır.

Adım 5: Son olarak, önyükleme yükleyicisi varsayılan bir IOS işletim sistemi yazılım görüntüsünü bulur ve belleğe yükler ve IOS'ye geçişin kontrolünü verir.

#### 17.1.1.boot system komutları

Anahtar, BOOT ortam değişkenindeki bilgileri kullanarak otomatik olarak önyükleme yapmaya çalışır. Bu değişken ayarlanmazsa, anahtar bulabileceği ilk yürütülebilir dosyayı yüklemeye ve yürütmeye çalışır.

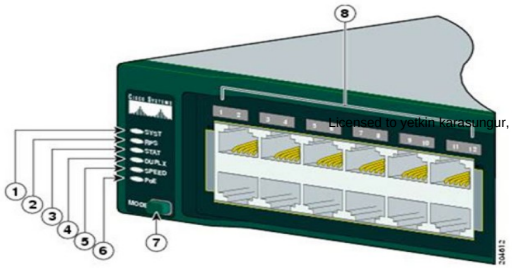
IOS işletim sistemi daha sonra startup-config dosyasında bulunan Cisco IOS komutlarını kullanarak arabirimleri başlatır. Startup-config dosyasına config.text adı verilir ve flash içinde bulunur.

Örnekte, BOOT ortam değişkeni önyükleme sistemi genel yapılandırma modu komutu kullanılarak ayarlanır. IOS'nin farklı bir klasörde bulunduğuna ve klasör yolunun belirtildiğine dikkat edin. Geçerli IOS önyükleme dosyasının neye ayarlandığını görmek için **show boot** komutunu kullanın.

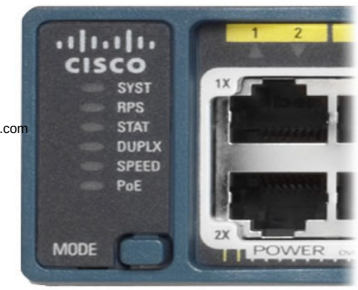
```
S1(config)# boot system flash:/c2960-lanbasek9-mz.150-2.SE/c2960-lanbasek9-mz.150-2.SE.bin
```

| Command | Definition |
|---|---|
| **boot system** | Ana komut |
| **flash:** | Depolama cihazı |
| **c2960-lanbasek9-mz.150-2.SE/** | Dosya sistemine giden yol |
| **c2960-lanbasek9-mz.150-2.SE.bin** | IOS dosya ismi |

### 17.1.2.Anahtar LED Göstergeleri




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



**System LED (SYST): Sistemin güç alıp almadığını ve düzgün çalışıp çalışmadığını gösterir.**
**Redundant Power Supply LED (RPS):** RPS durumunu gösterir.
**Port Status LED (STAT):** Yeşil olduğunda, varsayılan bağlantı noktası durum modunun seçildiğini gösterir. Bağlantı noktası durumu daha sonra her bağlantı noktasıyla ilişkilendirilen led anlaşılabilir.
**Port Duplex LED (DUPLX):** Yeşil renkte, bağlantı noktası dupleks modunun seçildiğini gösterir. Bağlantı noktası dupleks özelliği daha sonra her bağlantı noktasıyla ilişkili led tarafından anlaşılabilir.
**Port Speed LED (SPEED):** Yeşil renkte, bağlantı noktası hız modunun seçildiğini gösterir. Bağlantı noktası hızı daha sonra her bağlantı noktasıyla ilişkili led tarafından anlaşılabilir.
**Power over Ethernet LED (PoE):** Anahtar PoE'yi destekliyorsa gösterir. Anahtardaki bağlantı noktalarının PoE durumunu gösterir.

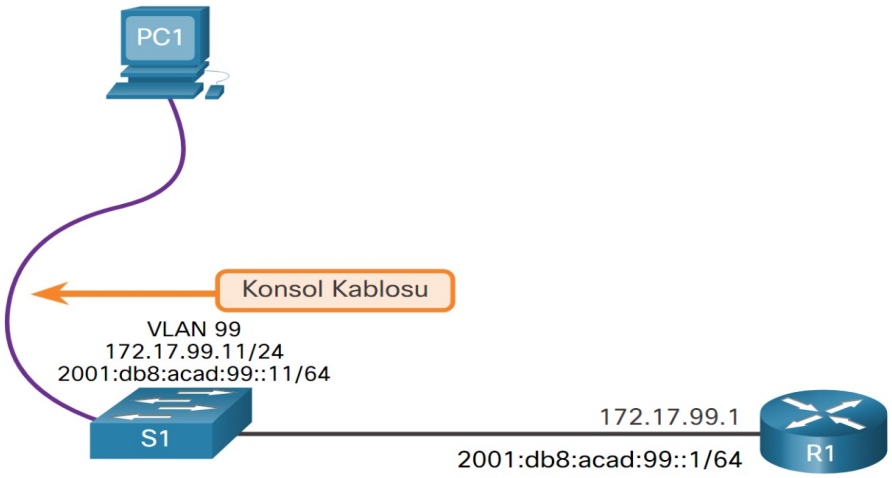
Mod düğmesi farklı modlar arasında geçiş yapmak için kullanılır - STAT, DUPLEX, SPEED ve PoE gibi

## 17.1.3.Anahtar Yönetim Erişimi

Uzaktan yönetim erişimi için bir anahtar hazırlamak için anahtarın bir IP adresi ve bir alt ağ maskesi ile yapılandırılması gerekir.

Anahtarı uzak bir ağdan yönetmek için, anahtarın varsayılan bir ağ geçidi ile yapılandırılması gerekir. Bu, ana cihazlarda IP adresi bilgilerinin yapılandırılmasına çok benzer.

Şekilde, S1'deki anahtar sanal arabirimine-switch virtual interface (SVI) bir IP adresi atanmalıdır. SVI, anahtardaki fiziksel bir bağlantı noktası değil, sanal bir arabirimdir. Bir PC'ye bağlanmak için anahtarın başlangıçta yapılandırılabilmesi için bir konsol kablosu kullanılır.




## 17.1.4.Anahtar SVI Yapılandırma Örneği

Varsayılan olarak, anahtar yönetimini VLAN 1 üzerinden kontrol edecek şekilde yapılandırılmıştır. Tüm bağlantı noktaları varsayılan olarak VLAN 1'e atanır. Güvenlik nedeniyle, VLAN yönetimi için VLAN 1 dışında bir VLAN kullanmak en iyi uygulama olarak kabul edilir,

Adım 1: Yönetim Arayüzünü Yapılandırma: VLAN arayüzü yapılandırma modunda, anahtarın yönetim SVI'sına bir IPv4 adresi ve alt ağ maskesi uygulanır.

Not: VLAN 99 için SVI, VLAN 99 oluşturulana ve VLAN 99 ile ilişkili bir anahtar bağlantı noktasına bağlı olan bir aygıt olana kadar “yukarı-up / yukarı-up” olarak görünmez.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not: Anahtarın IPv6 için yapılandırılması gerekebilir. Örneğin, IOS sürüm 15.0 çalıştıran bir Cisco Catalyst 2960 üzerinde IPv6 adreslemesini yapılandırabilmeniz için, **sdm prefer dual-ipv4-and-ipv6 default** genel yapılandırma komutunu girmeniz gerekir ve ardından anahtarı **reload** komutu ile yeniden yükleyin.

| Görev | IOS Commands |
|---|---|
| Genel yapılandırma moduna girin. | S1# **configure terminal** |
| SVI için arayüz yapılandırma moduna girin. | S1(config)# **interface vlan 99** |
| Yönetim arayüzü IPv4 adresini yapılandırın. | S1(config-if)# **ip address 172.17.99.11 255.255.255.0** |
| Yönetim arayüzü IPv6 adresini yapılandırın | S1(config-if)# **ipv6 address 2001:db8:acad:99::1/64** |
| Yönetim arayüzünü etkinleştirin. | S1(config-if)# **no shutdown** |
| Ayrıcalıklı EXEC moduna dönün. | S1(config-if)# **end** |
| Çalışan yapılandırmayı başlangıç yapılandırmasına kaydedin. | S1# **copy running-config startup-config** |

### Adım 2: Varsayılan Ağ Geçidini Yapılandırma

Doğrudan bağlı olmayan ağlardan uzaktan yönetilecekse, anahtar varsayılan bir ağ geçidi ile yapılandırılmalıdır.

Not: Varsayılan ağ geçidi bilgilerini bir yönlendirici reklamı (RA) mesajından alacağından, anahtar bir IPv6 varsayılan ağ geçidi gerektirmez.

| Görev | IOS Commands |
|---|---|
| Genel yapılandırma moduna girin. | S1# **configure terminal** |
| Anahtar için varsayılan ağ geçidini yapılandırın. | S1(config)# **ip default-gateway 172.17.99.1** |
| Ayrıcalıklı EXEC moduna dönün. | S1(config-if)# **end** |
| Çalışan yapılandırmayı başlangıç yapılandırmasına kaydedin. | S1# **copy running-config startup-config** |

### Adım 3: Yapılandırmayı Doğrulayın

**show ip interface brief** ve **show ipv6 interface brief** komutları, hem fiziksel hem de sanal arabirimlerin durumunu belirlemek için yararlıdır. Gösterilen çıktı, VLAN 99 arabiriminin bir IPv4 ve IPv6 adresiyle yapılandırıldığını onaylar.

Not: SVI'ya uygulanan bir IP adresi yalnızca anahtara uzaktan yönetim erişimi içindir; bu, anahtarın Katman 3 paketlerini yönlendirmesine izin vermez.

```
S1# show ip interface brief
Interface      IP-Address      OK? Method   Status    Protocol
Vlan99         172.17.99.11    YES manual   down      down
(output omitted)
S1# show ipv6 interface brief
Vlan99                 [down/down]
    FE80::C27B:BCFF:FEC4:A9C1
    2001:DB8:ACAD:99::11
(output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 17.2.Anahtar Bağlantı Noktalarını Yapılandırma

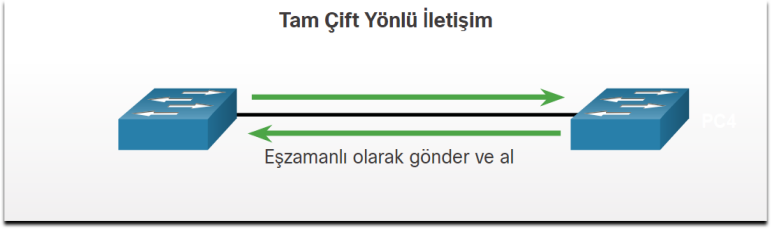
### 17.2.1.Duplex Communication-Çift Yönlü(Dupleks) İletişim

Tam çift yönlü-Full-duplex iletişim, bağlantının her iki ucunun da aynı anda veri iletmesine ve almasına izin vererek bant genişliği verimliliğini artırır. Bu, çift yönlü iletişim olarak da bilinir ve mikrosegmentasyon gerektirir.

Bir anahtar bağlantı noktasına bağlı yalnızca bir aygıt varsa ve tam çift yönlü modda çalışırken mikrosegmentli bir LAN oluşturulur. Tam çift yönlü modda çalışan bir anahtar bağlantı noktasıyla ilişkili bir çarpışma alanı yok.

Tam çift yönlü iletişimin aksine, yarım çift yönlü-Half-duplex iletişim tek yönlüdür. Yarı çift yönlü iletişim performans sorunları oluşturur, çünkü veriler bir seferde yalnızca bir yönde akabilir ve bu da genellikle çarpışmalara-collisions neden olur.

Gigabit Ethernet ve 10 Gb NIC'lerin çalışması için tam çift yönlü bağlantılar gerekir. Tam çift yönlü modda, NIC üzerindeki çarpışma algılama devresi devre dışı bırakılır. Tam çift yönlü, her iki yönde de yüzde 100 verimlilik sunar (gönderme ve alma). Bu, belirtilen bant genişliğinin potansiyel kullanımının iki katına çıkmasına neden olur.



### 17.2.2.Fiziksel Katmanda Anahtar Bağlantı Noktalarını Yapılandırma

Anahtar bağlantı noktaları, özel çift yönlü ve hız ayarlarıyla manuel olarak yapılandırılabilir. İlgili arayüz yapılandırma komutları dublex ve speed.

Cisco Catalyst 2960 ve 3560 anahtarlarındaki anahtar bağlantı noktaları için hem dubleks hem de hız-speed için varsayılan ayar otomatiktir. 10/100/1000 bağlantı noktaları, 10 veya 100 Mbps'ye ayarlandığında yarı veya tam çift yönlü modda çalışır ve 1000 Mbps (1 Gbps) olarak ayarlandığında yalnızca tam çift yönlü modda çalışır.

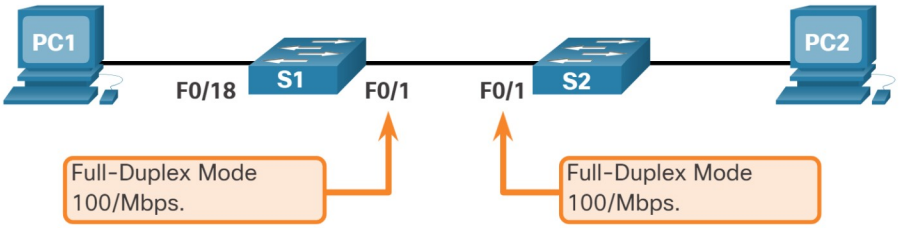
Otomatik anlaşma-Autonegotiation , bağlantı noktasına bağlanan aygıtın hız ve dubleks ayarları bilinmiyorsa veya değişebilirse yararlıdır. Sunucular, özel iş istasyonları veya ağ cihazları gibi bilinen cihazlara bağlanırken, en iyi uygulama hız ve dupleks ayarlarını manuel olarak yapmaktır.

Anahtar bağlantı noktası sorunlarını giderirken, dubleks ve hız ayarlarının kontrol edilmesi önemlidir.

Not: Çift yönlü mod için uyumsuz ayarlar ve anahtar bağlantı noktalarının hızı bağlantı sorunlarına neden olabilir. Otomatik anlaşma-Autonegotiation hatası, eşleşmeyen ayarlar oluşturur.

1000BASE-SX bağlantı noktaları gibi tüm fiber optik bağlantı noktaları yalnızca önceden ayarlanmış bir hızda çalışır ve her zaman tam çift yönlüdür

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




| Görev | IOS Commands |
|---|---|
| Genel yapılandırma moduna girin. | S1# **configure terminal** |
| Arayüz yapılandırma moduna girin. | S1(config)# **interface FastEthernet 0/1** |
| Arayüz dubleksini yapılandırın. | S1(config-if)# **duplex full** |
| Arayüz hızını yapılandırın. | S1(config-if)# **speed 100** |
| Ayrıcalıklı EXEC moduna dönün. | S1(config-if)# **end** |
| Çalışan yapılandırmayı başlangıç yapılandırmasına kaydedin. | S1# **copy running-config startup-config** |

## 17.2.4.Auto-MDIX

Otomatik çapraz orta bağımlı arabirim -automatic medium-dependent interface crossover (auto-MDIX) etkinleştirildiğinde, anahtar arabirimi gerekli kablo bağlantı türünü (düz  veya çapraz) otomatik olarak algılar ve bağlantıyı uygun şekilde yapılandırır.

Otomatik MDIX özelliği olmayan anahtarlara bağlanırken, sunucular, iş istasyonları veya yönlendiriciler gibi aygıtlara bağlanmak için düz kablolar kullanılmalıdır. Çapraz kablo anahtarlar, diğer anahtarlara veya tekrarlayıcılara bağlamak için kullanılmalıdır.

Otomatik MDIX etkinken, diğer cihazlara bağlanmak için her iki kablo türü kullanılabilir ve arabirim başarıyla iletişim kurmak için otomatik olarak ayarlanır.

Yeni Cisco anahtarlarında, **mdix auto** interface yapılandırma modu komutu özelliği etkinleştirir. Bir arabirimde auto-MDIX kullanılırken, özelliğin düzgün çalışması için arabirim hızı ve dupleks otomatik olarak ayarlanmalıdır.

```
S1(config-if)# mdix auto
```

Not: auto-MDIX özelliği, Catalyst 2960 ve Catalyst 3560 anahtarlarında varsayılan olarak etkindir, ancak eski Catalyst 2950 ve Catalyst 3550 anahtarlarında kullanılamaz.

Belirli bir arabirimin auto-MDIX ayarını incelemek için **phy** anahtar sözcüğüyle **show controllerers ethernet-controller** komutunu kullanın.

```
S1# show controllers ethernet-controller fa0/1 phy | include MDIX
 Auto-MDIX           :  On    [AdminState=1    Flags=0x00052248]
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 17.2.5.Switch Verification Commands-Anahtar Doğrulama Komutları

| Task-Görev | IOS Commands |
|---|---|
| Arayüz durumunu ve yapılandırmasını görüntüleyin. | S1# **show interfaces** [*interface-id*] |
| Mevcut başlangıç yapılandırmasını görüntüleyin. | S1# **show startup-config** |
| Mevcut çalışan konfigürasyonu görüntüleyin. | S1# **show running-config** |
| Flash dosya sistemi ile ilgili bilgileri görüntüleyin. | S1# **show flash** |
| Sistem donanım ve yazılım durumunu görüntüleyin. | S1# **show version** |
| Girilen komut geçmişini görüntüleyin. | S1# **show history** |
| Bir arabirim hakkındaki IP bilgilerini görüntüleyin. | S1# **show ip interface** [*interface-id*]<br>OR<br>S1# **show ipv6 interface** [*interface-id*] |
| MAC adres tablosunu görüntüleyin. | S1# **show mac-address-table**<br>OR<br>S1# **show mac address-table** |

## Verify Switch Port Configuration-Anahtar Bağlantı Noktası Yapılandırmasını Doğrulama

**show running-config** komutu, anahtarın doğru yapılandırıldığını doğrulamak için kullanılabilir. S1'deki kısaltılmış örnek çıktıdan, bazı önemli bilgiler şekilde gösterilmiştir:

- Yönetim-management VLAN 99 ile yapılandırılmış
  Fast Ethernet 0/18 arayüzü-port
- 172.17.99.11 255.255.255.0 IPv4 adresiyle yapılandırılmış VLAN 99
- Varsayılan ağ geçidi 172.17.99.1 olarak ayarlanmış

```
S1# show running-config
Building configuration...
Current configuration : 1466 bytes
!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
!
(output omitted)
!
interface Vlan99
 ip address 172.17.99.11 255.255.255.0
 ipv6 address 2001:DB8:ACAD:99::1/64
!
ip default-gateway 172.17.99.1
```

**show interfaces** komutu, anahtarın ağ arabirimlerinde durum ve istatistik bilgilerini görüntüleyen yaygın olarak kullanılan başka bir komuttur. **show interfaces** komutu, ağ cihazlarını yapılandırırken ve izlerken sıklıkla kullanılır.

**show interfaces fastEthernet 0/18** komutu, FastEthernet 0/18 arabiriminin yukarı-up / yukarı-up olduğunu, yani çalışır durumda olduğunu gösterir. Daha aşağıdaki çıktı, dubleksin full ve hızın 100 Mbps olduğunu gösterir.

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Network Access Layer Issues-Ağ Erişim Katmanı Sorunları

**show interfaces** komutunun çıktısı, yaygın medya sorunlarını tespit etmek için kullanışlıdır. Bu çıktının en önemli parçalarından biri, örnekte gösterildiği gibi hat-line ve veri bağlantısı-data link protokolü durumunun gösterilmesidir.

İlk parametre (FastEthernet0 / 18 yukarı-up) donanım katmanını belirtir ve arabirimin bir taşıyıcı algılama sinyali alıp almadığını gösterir. İkinci parametre (hat protokolü yukarı-up) veri bağlantı katmanını belirtir ve veri bağlantı katmanı protokol bilgilerinin alınıp alınmadığını gösterir. Show interfaces komutunun çıktısına bağlı olarak, olası sorunlar aşağıdaki gibi giderilebilir:

Arayüz çalışıyorsa ve hat protokolü-line protocol çalışmıyorsa, bir sorun vardır. Bir kapsülleme türü uyuşmazlığı olabilir, diğer uçtaki arabirim hatayla devre dışı bırakılmış olabilir veya bir donanım sorunu olabilir.

Hat protokolü ve arabirim kapalıysa, bir kablo takılı değildir veya başka bir arabirim sorunu vardır. Örneğin, arka arkaya bağlantıda, bağlantının diğer ucu yönetimsel olarak kapalı olabilir.

Arayüz yönetimsel olarak kapalıysa, etkin yapılandırmada manuel olarak devre dışı bırakılmıştır (**shutdown** komutu verilmiştir).

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)MTU 1500 bytes, BW 100000
Kbit/sec, DLY 100 usec,
```

**show interfaces** komut çıkışı, burada gösterildiği gibi FastEthernet0 / 18 arabirimi için sayaçları ve istatistikleri görüntüler:

```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0025.83e6.9092 (bia 0025.83e6.9092)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2295197 packets input, 305539992 bytes, 0 no buffer
     Received 1925500 broadcasts (74 multicasts)
     0 runts, 0 giants, 0 throttles
     3 input errors, 3 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 74 multicast, 0 pause input
     0 input packets with dribble condition detected
     3594664 packets output, 436549843 bytes, 0 underruns
     8 output errors, 1790 collisions, 10 interface resets
     0 unknown protocol drops
     0 babbles, 235 late collision, 0 deferred
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bazı medya hataları, devrenin arızalanmasına neden olacak kadar şiddetli değildir, ancak ağ performansı sorunlarına neden olur. Tablo, show interfaces komutu kullanılarak tespit edilebilen bu yaygın hatalardan bazılarını açıklar.

| Hata Tipi | Açıklama |
|---|---|
| **Input Errors** | Toplam hata sayısı. runts, giants, no buffer, CRC, frame, overrun, ve ignored sayılarını içerir. |
| **Runts** | Ortam için minimum paket boyutundan daha küçük oldukları için atılan paketler. Örneğin, 64 bayttan az olan herhangi bir Ethernet paketi bir runt olarak kabul edilir. |
| **Giants** | Ortam için maksimum paket boyutunu aştığı için atılan paketler. Örneğin, 1.518 bayttan büyük herhangi bir Ethernet paketi dev-giants olarak kabul edilir. |
| **CRC** | CRC hataları, hesaplanan sağlama toplamı-checksum alınan sağlama toplamıyla aynı olmadığında oluşturulur. |
| **Output Errors** | İncelenen arayüzden datagramların son iletimini engelleyen tüm hataların toplamı. |
| **Collisions** | Ethernet çarpışması nedeniyle yeniden iletilen mesaj sayısı. |
| **Late Collisions** | 512 bit frame iletildikten sonra meydana gelen bir çarpışma |

### Interface Input and Output Errors-Arayüz Giriş ve Çıkış Hataları

"Girdi hataları-Input errors" incelenen arabirimde alınan datagramlardaki tüm hataların toplamıdır. Buna runts, giants, CRC, no buffer, frame, overrun, ve ignored sayıları dahildir. Show interfaces komutundan bildirilen girdi hataları aşağıdakileri içerir:

**Runt Frames**-64 baytlık izin verilen minimum uzunluktan daha kısa olan Ethernet çerçevelerine runt denir. Arızalı NIC'ler aşırı runt çerçevelerinin olağan nedenidir, ancak çarpışmalardan da kaynaklanabilirler.

**Giants**- İzin verilen maksimum boyuttan büyük Ethernet çerçevelerine giant denir.

**CRC errors**- Ethernet ve seri arabirimlerde, CRC hataları genellikle bir ortam veya kablo hatasını gösterir. Yaygın nedenler arasında elektrik paraziti, gevşek veya hasarlı bağlantılar veya yanlış kablolama bulunur. Çok sayıda CRC hatası görürseniz, bağlantıda çok fazla gürültü var ve kabloyu incelemelisiniz. Ayrıca gürültü kaynaklarını aramalı ve ortadan kaldırmalısınız.

"Çıktı hataları-Output errors", incelenen arayüzden datagramların son iletimini engelleyen tüm hataların toplamıdır. Show interfaces komutuyla bildirilen çıktı hataları aşağıdakileri içerir:

**Collisions**- Yarım-half dubleks işlemlerde çarpışmalar normaldir. Ancak, tam çift yönlü iletişim için yapılandırılmış bir arabirimde çakışmaları asla görmemelisiniz.

**Late collisions**- Geç-late bir çarpışma, çerçevenin 512 biti iletildikten sonra meydana gelen bir çarpışmayı ifade eder. Aşırı kablo uzunlukları geç çarpışmaların en yaygın nedenidir. Diğer bir yaygın neden, dubleks yanlış yapılandırılmasıdır.

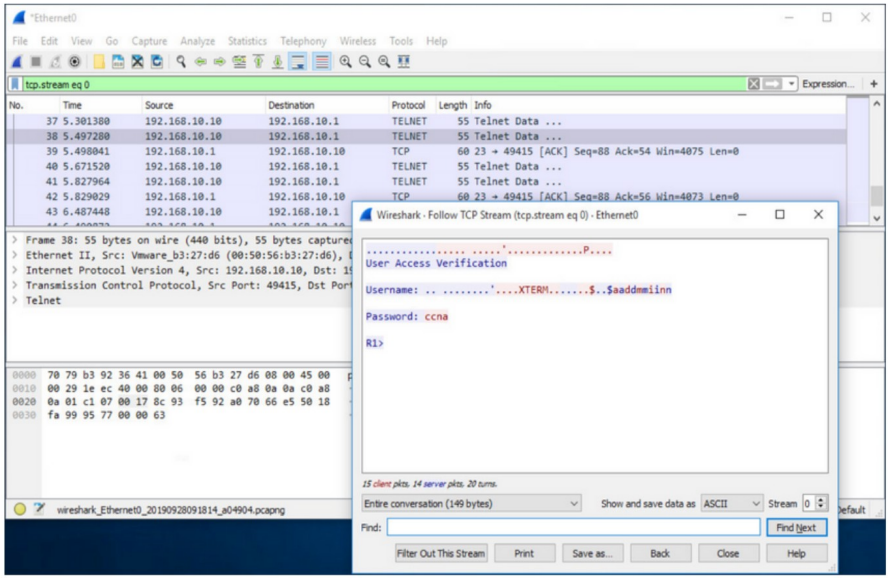
## 17.3.Güvenli Uzaktan Erişim

### 17.3.1.Telnet

Telnet, TCP bağlantı noktası 23'ü kullanır. Hem oturum açma kimlik doğrulamasının (kullanıcı adı ve parola) hem de iletişim kuran cihazlar arasında iletilen verilerin güvenli olmayan düz metin iletimini kullanan eski bir protokoldür.

Bir tehdit aktörü Wireshark kullanarak paketleri izleyebilir. Örneğin, şekilde tehdit aktörü bir Telnet oturumundan **admin** kullanıcı adını ve **ccna** parolasını ele geçirdi.

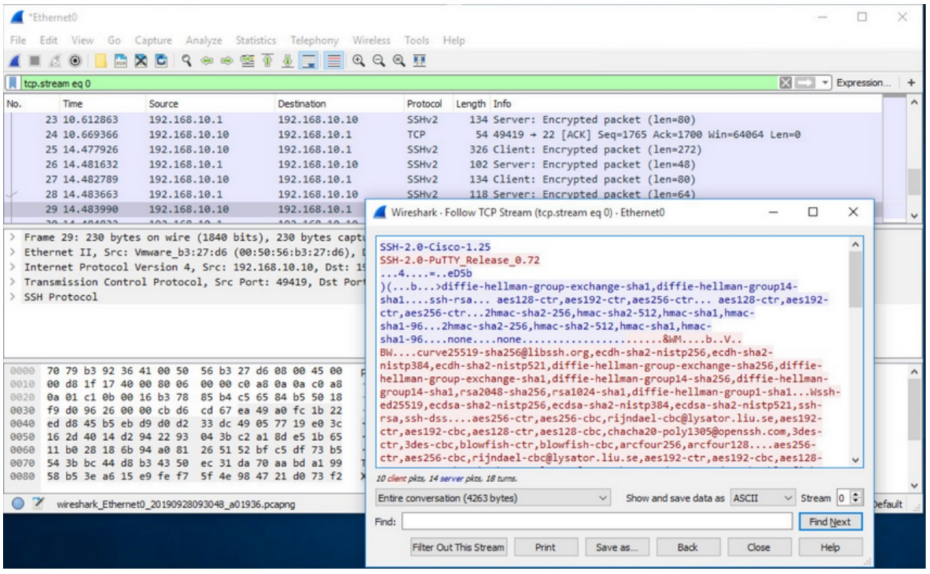
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 17.3.2.SSH (Secure Shell)

Güvenli Kabuk-Secure Shell (SSH), TCP bağlantı noktası 22 kullanan güvenli bir protokoldür. Uzak bir aygıta güvenli (şifreli) bir yönetim bağlantısı sağlar. SSH, yönetim bağlantıları için Telnet'in yerini almalıdır. SSH, bir cihazın kimliği doğrulandığında (kullanıcı adı ve şifre) güçlü şifreleme sağlayarak ve aynı zamanda iletişim kuran cihazlar arasında iletilen veriler için uzaktan bağlantılar için güvenlik sağlar.

Şekilde bir SSH oturumunun Wireshark yakalaması gösterilmektedir. Tehdit aktörü, yönetici aygıtının IP adresini kullanarak oturumu izleyebilir. Bununla birlikte, Telnet'ten farklı olarak, SSH ile kullanıcı adı ve parola şifrelenir.




## Anahtarın SSH'yi Desteklediğini Doğrulayın

Catalyst 2960 anahtarında SSH'yi etkinleştirmek için, anahtarın şifreleme (şifreli) özellikleri ve yetenekleri dahil olmak üzere IOS yazılımının bir sürümünü kullanıyor olması gerekir. Anahtarın şu anda hangi IOS çalıştığını görmek için anahtarda **show version** komutunu kullanın. “K9” kombinasyonunu içeren bir IOS dosya adı, şifreleme (şifreli) özelliklerini ve yeteneklerini destekler.

Örnek, show version komutunun çıktısını gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE7, RELEASE SOFTWARE (fc1)
```

### 17.3.3.SSH Yapılandırması

SSH'yi yapılandırmadan önce, anahtarın benzersiz bir ana bilgisayar adı(hostname) ve doğru ağ bağlantısı ayarlarıyla minimum düzeyde yapılandırılması gerekir.

Adım 1: SSH desteğini doğrulama - Anahtarın SSH'yi desteklediğini doğrulamak için show ip ssh komutunu kullanın. Anahtar, şifreleme özelliklerini destekleyen bir IOS çalıştırmıyorsa, bu komut tanınmaz.

```
S1# show ip ssh
```

Adım 2: IP etki alanını yapılandırın – **ip domain-name** genel yapılandırma modu komutunu kullanarak ağın IP etki alanı adını yapılandırın.

```
S1(config)# ip domain-name cisco.com
```

Adım 3: RSA anahtar çiftleri oluşturun - RSA anahtar çifti oluşturmak otomatik olarak SSH'yi etkinleştirir. Anahtarda SSH sunucusunu etkinleştirmek ve bir RSA anahtar çifti oluşturmak için **cyrpto key generate rsa** global yapılandırma modu komutunu kullanın.

```
S1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024
```

Not: RSA anahtar çiftini silmek için, **crypto key zeroize rsa** global yapılandırma modu komutunu kullanın. RSA anahtar çifti silindikten sonra SSH sunucusu otomatik olarak devre dışı bırakılır.

4. Adım: Kullanıcı kimlik doğrulamasını yapılandırın - SSH sunucusu yerel olarak veya bir kimlik doğrulama sunucusu kullanarak kullanıcıların kimliğini doğrulayabilir. Yerel kimlik doğrulama yöntemini kullanmak için, **username *username* secret *password*** genel yapılandırma modu komutunu kullanarak bir kullanıcı adı ve parola çifti oluşturun.

```
S1(config)# username admin secret ccna
```

Adım 5: vty satırlarını yapılandırın - **transport input ssh** yapılandırma modu komutunu kullanarak vty satırlarındaki SSH protokolünü etkinleştirin. Yerel kullanıcı adı veritabanından SSH bağlantıları için yerel kimlik doğrulaması istemek için **line vty** global yapılandırma modu komutunu ve ardından **login local** yapılandırma modu komutunu kullanın.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local
S1(config-line)# exit
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Adım 6: SSH sürüm 2'yi etkinleştir - Varsayılan olarak, SSH hem sürüm 1 hem de 2'yi destekler. Her iki sürümü de desteklerken bu, **show ip ssh** çıktısında destekleyici sürüm 2 olarak gösterilir. **ip ssh version 2** genel yapılandırma komutunu kullanarak SSH sürümünü etkinleştirin .

```
S1(config)# ip ssh version 2
```

## SSH'in Çalıştığını Doğrulayın

Bir bilgisayarda, bir SSH sunucusuna bağlanmak için PuTTY gibi bir SSH istemcisi kullanılır. Örneğin, aşağıdakilerin yapılandırıldığını varsayın:

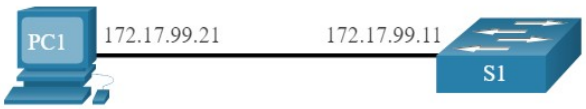
S1 anahtarında SSH etkin

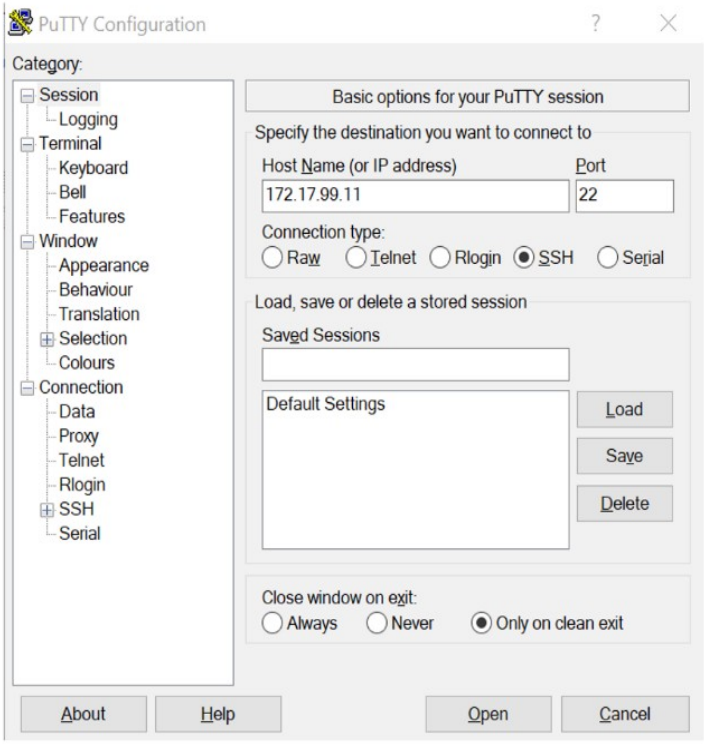
S1 anahtarında IPv4 adresi 172.17.99.11 olan VLAN 99 arabirimi (SVI)

IPv4 adresli PC1 172.17.99.21

Bir terminal emülatörü kullanarak, PC1'den S1'in SVI VLAN IPv4 adresine bir SSH bağlantısı başlatın.

Bağlandığında, kullanıcıdan örnekte gösterildiği gibi bir kullanıcı adı ve parola istenir. Önceki örnekteki yapılandırma kullanılarak, kullanıcı adı admin ve şifre ccna girilir. Doğru kombinasyonu girdikten sonra, kullanıcı SSH üzerinden Catalyst 2960 anahtarındaki komut satırı arabirimine (CLI) bağlanır.




```
Login as: admin
Using keyboard-interactive
Authentication.
Password:
S1> enable
Password:
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

SSH sunucusu olarak yapılandırdığınız aygıtta SSH'nin sürüm ve yapılandırma verilerini görüntülemek için **show ip ssh** komutunu kullanın. Örnekte, SSH sürüm 2 etkinleştirilmiştir.

```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
To check the SSH connections to the device, use the show ssh command as shown.
S1# show ssh
%No SSHv1 server connections running.
Connection Version Mode Encryption  Hmac               State          Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started       admin
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started       admin
S1#
```

## 17.4.Yönlendirici Yapılandırması

### 17.4.1.Yönlendirici Ayarlarını Yapılandırma

Cisco yönlendiricileri ve Cisco anahtarları birçok benzerliğe sahiptir. Benzer bir mod işletim sistemini, benzer komut yapılarını ve aynı komutların çoğunu desteklerler. Ayrıca, her iki cihaz da benzer başlangıç yapılandırma adımlarına sahiptir. Örneğin, aşağıdaki yapılandırma görevleri her zaman gerçekleştirilmelidir. Örnekte gösterildiği gibi, cihazı diğer yönlendiricilerden ayırt etmek için adlandırın ve parolaları yapılandırın.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# hostname R1
R1(config)# enable secret class
R1(config)# line console 0
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# line vty 0 4
R1(config-line)# password cisco
R1(config-line)# login
R1(config-line)# exit
R1(config)# service password-encryption
R1(config)#
```

Bir banner'ı, örnekte gösterildiği gibi, yetkisiz erişime ilişkin yasal bildirim sağlayacak şekilde yapılandırın.

```
R1(config)# banner motd $ Authorized Access Only! $
R1(config)#
```

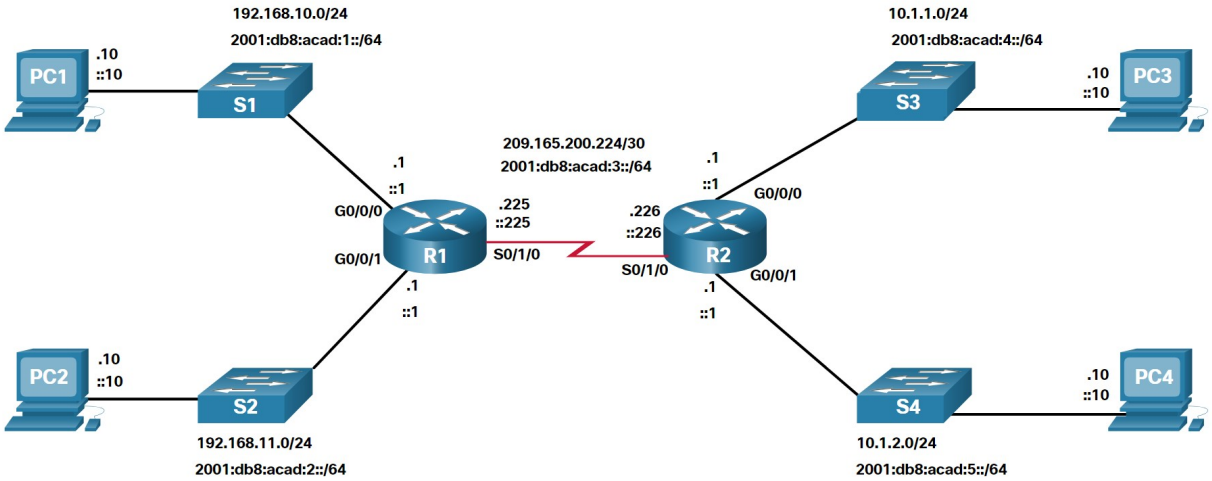
Değişiklikleri örnekte gösterildiği gibi yönlendiriciye kaydedin.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 17.4.2.Dual Stack Topology-Çift Yığın Topolojisi

Anahtarlar ve yönlendiriciler arasındaki ayırt edici özelliklerden biri, her biri tarafından desteklenen arabirimlerin türüdür. Örneğin, Katman 2 anahtarları LAN'ları destekler; bu nedenle, birden fazla FastEthernet veya Gigabit Ethernet bağlantı noktasına sahiptir. Şekildeki çift yığın topolojisi, yönlendirici IPv4 ve IPv6 arabirimlerinin yapılandırmasını göstermek için kullanılır.




## Yönlendirici Arayüzlerini Yapılandırma

Yönlendiriciler LAN'ları ve WAN'ları destekler ve farklı ağ türlerini birbirine bağlayabilir; bu nedenle, birçok arabirimi desteklerler. Örneğin, G2 ISR'lerde seri, DSL ve kablo arabirimleri de dahil olmak üzere diğer ağ arabirimi türlerini barındırmak için bir veya iki tümleşik Gigabit Ethernet arabirimi ve Yüksek Hızlı WAN Arabirim Kartı-High-Speed WAN Interface Card (HWIC) yuvası vardır.

Bir arayüzün kullanılabilir olması için gerekenler:

En az bir IP adresiyle yapılandırılmış olmalı -**ip-address subnet-mask** ve **ipv6 address ipv6-address/prefix** arabirimi yapılandırma komutlarını kullanın.

Etkinleştirilmiş olmalı - Varsayılan olarak, LAN ve WAN arabirimleri etkin değildir. (shutdown). Bir arabirimi etkinleştirmek için, **no shutdown** komutu ile etkinleştirilmelidir. (Bu, arabirimi açmaya benzer.) Fiziksel katmanın etkin olabilmesi için arayüz başka bir cihaza (hub, anahtar veya başka bir yönlendirici) bağlı olmalıdır.

Açıklama - İsteğe bağlı olarak, arabirim 240 karaktere kadar kısa bir açıklama ile de yapılandırılabilir. Her arabirimde bir açıklama yapılandırmak iyi bir uygulamadır. Üretim ağlarında, arayüz açıklamalarının faydaları, sorun giderme ve bir üçüncü taraf bağlantı ve iletişim bilgilerinin tanımlanmasında yardımcı oldukları için hızla fark edilir.

Aşağıdaki örnek, R1 üzerindeki arayüzlerin konfigürasyonunu gösterir.

```
R1(config)# interface gigabitethernet 0/0/0
R1(config-if)# ip address 192.168.10.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# description Link to LAN 1
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ip address 192.168.11.1 255.255.255.0
R1(config-if)# ipv6 address 2001:db8:acad:2::1/64
R1(config-if)# description Link to LAN 2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 209.165.200.225 255.255.255.252
R1(config-if)# ipv6 address 2001:db8:acad:3::225/64
R1(config-if)# description Link to R2
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### IPv4 Loopback Interfaces-IPv4 Geri Döngü Arabirimleri

Cisco IOS yönlendiricilerinin bir başka yaygın yapılandırması, geri döngü arabirimini- loopback interface etkinleştirmektir.

Geri döngü arabirimi, yönlendiricinin içinde bulunan mantıksal bir arabirimdir. Fiziksel bir bağlantı noktasına atanmaz ve hiçbir zaman başka bir aygıta bağlanamaz. Yönlendirici çalıştığı sürece otomatik olarak "yukarı" duruma getirilen bir yazılım arayüzü olarak kabul edilir.

Geridöngü arabirimi, bir Cisco IOS aygıtının test edilmesinde ve yönetilmesinde kullanışlıdır, çünkü en az bir arabirimin her zaman kullanılabilir olmasını sağlar. Örneğin, yönlendiricinin arkasındaki ağları taklit ederek, iç yönlendirme süreçlerini test etmek gibi test amaçları için kullanılabilir.

Geridöngü arabirimleri, ek arabirimler oluşturmak için laboratuvar ortamlarında da yaygın olarak kullanılır. Örneğin, yapılandırma uygulaması ve sınama amacıyla daha fazla ağ simüle etmek için bir yönlendiricide birden çok geri döngü arabirimi oluşturabilirsiniz. Her geri döngü arabiriminin IPv4 adresi benzersiz olmalı ve diğer arabirimler tarafından kullanılmamalıdır. Bu müfredatta, internete bir bağlantıyı simüle etmek için genellikle geri döngü arayüzü kullanırız.

Geri döngü adresini etkinleştirmek ve atamak kolaydır:

```
R1(config)# interface loopback 0
R1(config-if)# ip address 10.0.0.1 255.255.255.0
R1(config-if)# exit
R1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0, changed state to up
```

## 17.5.Doğrudan (Direkt) Bağlı Ağları Doğrulama

### 17.5.1.Arayüz Doğrulama Komutları

Bir arabirimin çalışmasını ve yapılandırmasını doğrulamak için kullanılabilecek birkaç show komutu vardır.

Aşağıdaki komutlar özellikle bir arabirimin durumunu hızlı bir şekilde tanımlamak için kullanışlıdır:

**show ip interface brief** ve **show ipv6 interface brief** - Bunlar, arabirimin IPv4 veya IPv6 adresi ve geçerli çalışma durumu dahil tüm arabirimler için bir özet görüntüler.

**show running-config interface** *interface-id*- Bu, belirtilen arabirime uygulanan komutları görüntüler.

**show ip route** ve **show ipv6 route**-Bunlar, RAM'de depolanan IPv4 veya IPv6 yönlendirme tablosunun içeriğini görüntüler. Cisco IOS 15'te, etkin arayüzler yönlendirme tablosunda 'C' (Bağlı-Connected) veya 'L' (Yerel-Local) kodu ile tanımlanan ilgili iki girişle görünmelidir. Önceki IOS sürümlerinde, yalnızca 'C' koduna sahip tek bir giriş görünür.

### Arayüz Durumunu Doğrulama

**show ip interface brief** ve **show ipv6 interface brief** komutlarının çıktıları, yönlendiricideki tüm arabirimlerin durumunu hızlı bir şekilde ortaya çıkarmak için kullanılabilir. Örneklerde gösterildiği gibi, arayüzlerin durumu "yukarı-up" ve protokolün de "yukarı-" olması belirtildiği gibi aktif ve çalışır durumda olduğunu doğrular. Farklı bir çıkış, konfigürasyonda veya kablolarda bir sorun olduğunu gösterir.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      YES unset  administratively down down
R1# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:1::1
GigabitEthernet0/0/1   [up/up]
    FE80::7279:B3FF:FE92:3131
    2001:DB8:ACAD:2::1
Serial0/1/0            [up/up]
    FE80::7279:B3FF:FE92:3130
    2001:DB8:ACAD:3::1
Serial0/1/1            [down/down]     Unassigned
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## IPv6 Yerel Bağlantı ve Çok Noktaya Yayın Adreslerini Doğrulama

**show ipv6 interface brief** komutunun çıktısı, arabirim başına yapılandırılmış iki IPv6 adresi görüntüler. Adreslerden biri, elle girilen IPv6 genel tek noktaya yayın adresidir. FE80 ile başlayan diğer adres, arabirimin yerel bağlantı tek noktaya yayın adresidir. Genel bir tek noktaya yayın adresi atandığında otomatik olarak bir bağlantı yerel adresi arabirime eklenir. Bir bağlantı yerel adresine sahip olmak için bir IPv6 ağ arabirimi gerekir, ancak genel bir tek noktaya yayın adresi olması gerekmez.

**show ipv6 interface gigabitethernet 0/0/0** komutu, arabirim durumunu ve arabirime ait tüm IPv6 adreslerini görüntüler. Bağlantı yerel adresi ve genel tek noktaya yayın adresiyle birlikte çıktı, örnekte gösterildiği gibi FF02 önekinden başlayarak arabirime atanan çok noktaya yayın adreslerini içerir.

```
R1# show ipv6 interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::7279:B3FF:FE92:3130
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
    FF02::1:FF92:3130
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
```

**show running-config interface** komutunun çıktısı, gösterildiği gibi belirtilen arabirime uygulanan geçerli komutları görüntüler.

Daha ayrıntılı arabirim bilgilerini toplamak için aşağıdaki iki komut kullanılır:

**show interfaces**-Aygıttaki tüm arabirimler için arabirim bilgilerini ve paket akış sayısını görüntüler.

**show ip interface ve show ipv6 interface**-Bir yönlendiricideki tüm arabirimler için IPv4 ve IPv6 ile ilgili bilgileri görüntüler.

```
R1 show running-config interface gigabitethernet 0/0/0
Building configuration...
Current configuration : 158 bytes
!
interface GigabitEthernet0/0/0
 description Link to LAN 1
 ip address 192.168.10.1 255.255.255.0
 negotiation auto
 ipv6 address 2001:DB8:ACAD:1::1/64
end
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Rotaları Doğrulama

**Show ip route** ve **show ipv6 route** komutlarının çıktıları, örnekte gösterildiği gibi, doğrudan bağlı üç ağ girişini ve üç yerel ana bilgisayar yolu arabirim girişini gösterir.

Yerel ana bilgisayar yolunun yönetimsel mesafesi 0'dır. Ayrıca IPv4 için / 32 maskesi ve IPv6 için / 128 maskesi vardır. Yerel ana bilgisayar yolu, yönlendiricideki IP adresine sahip olan yollar içindir. Yönlendiricinin söz konusu IP'ye gönderilen paketleri işlemesine izin vermek için kullanılır.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP

Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0
R1# show ipv6 route
IPv6 Routing Table - default - 7 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Yönlendirme tablosundaki bir yolun yanındaki "C", bunun doğrudan bağlı bir ağ olduğunu gösterir. Yönlendirici arabirimi genel bir tek noktaya yayın adresiyle-global unicast address yapılandırıldığında ve “yukarı / yukarı” durumunda olduğunda, IPv6 öneki ve önek uzunluğu IPv6 yönlendirme tablosuna bağlı bir rota olarak eklenir.

Arabirime uygulanan IPv6 genel tek noktaya yayın adresi de yönlendirme tablosuna yerel bir yol olarak yüklenir. Yerel yolun / 128 öneki vardır. Yerel yollar, yönlendirme tablosu tarafından yönlendiricinin arabirim adresi olan paketleri etkin bir şekilde işlemek için kullanılır.

## Show Komut Çıktısını Filtreleme

Birden çok çıktı ekranı oluşturan komutlar varsayılan olarak 24 satırdan sonra duraklatılır. Duraklatılmış çıktının sonunda--More-- - metni görüntülenir. Enter tuşuna basıldığında sonraki satır görüntülenir ve boşluk çubuğuna basıldığında sonraki sayfa kümesi görüntülenir. Görüntülenecek satır sayısını belirtmek için terminal length komutunu kullanın. 0 (sıfır) değeri, yönlendiricinin çıkış ekranları arasında duraklamasını önler.

CLI'daki kullanıcı deneyimini geliştiren bir diğer kullanışlı özellik de show çıktısının filtrelenmesidir. Filtreleme komutları, çıktının belirli bölümlerini görüntülemek için kullanılabilir. Filtreleme komutunu etkinleştirmek için, show komutundan sonra bir dikey çizgi (|) karakteri girin ve ardından bir filtreleme parametresi ve bir filtreleme ifadesi girin.

Kerem Aydın Yetkin (kerem@ayt.io)

| (pipe) işaretinden  sonra yapılandırılabilen dört filtreleme parametresi vardır:

- section - Filtreleme ifadesiyle başlayan bölümün tamamını gösterir.
- include - Filtreleme ifadesiyle eşleşen tüm çıktı satırlarını içerir.
- exclude - Filtreleme ifadesiyle eşleşen tüm çıktı satırlarını hariç tutar.
- begin - Filtreleme ifadesiyle eşleşen satırdan başlayarak belirli bir noktadaki tüm satırları gösterir

Örnekte gösterildiği gibi section ifadesiyle başlayan tüm bölümü gösterir.

```
R1# show running-config | section line vty
line vty 0 4
 password 7 110A1016141D
 login
 transport input all
```

Örnekte gösterildiği gibi, filtreleme ifadesiyle eşleşen tüm çıktı satırlarını içerir.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      NO  unset  down                  down
R1#
R1# show ip interface brief | include up
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
```

Örnekte gösterildiği gibi, filtreleme ifadesiyle eşleşen tüm çıktı satırlarını hariç tutar.

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
Serial0/1/1            unassigned      NO  unset  down                  down
R1#
R1# show ip interface brief | exclude unassigned
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.10.1    YES manual up                    up
GigabitEthernet0/0/1   192.168.11.1    YES manual up                    up
Serial0/1/0            209.165.200.225 YES manual up                    up
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Örnekte gösterildiği gibi, filtreleme ifadesiyle eşleşen satırdan başlayarak belirli bir noktadaki tüm çıktı satırlarını gösterir.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, GigabitEthernet0/0/0
L        192.168.10.1/32 is directly connected, GigabitEthernet0/0/0
      192.168.11.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.11.0/24 is directly connected, GigabitEthernet0/0/1
L        192.168.11.1/32 is directly connected, GigabitEthernet0/0/1
      209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C        209.165.200.224/30 is directly connected, Serial0/1/0
L        209.165.200.225/32 is directly connected, Serial0/1/0
```

## Komut Geçmişi Özelliği

Komut geçmişi özelliği, geri çağrılacak yürütülmüş komutların listesini geçici olarak depoladığı için yararlıdır.

Geçmiş arabelleğindeki komutları geri çağırmak için Ctrl + P veya Yukarı Ok tuşuna basın. Komut çıkışı en son komutla başlar. Art arda eski komutları geri çağırmak için tuş sırasını tekrarlayın. Geçmiş arabelleğindeki daha yeni komutlara geri dönmek için Ctrl + N veya Aşağı Ok tuşuna basın. Art arda yeni komutları çağırmak için tuş sırasını tekrarlayın.

Varsayılan olarak komut geçmişi etkindir ve sistem geçmiş arabelleğindeki son 10 komut satırını yakalar. Arabellek içeriğini görüntülemek için **show history** privileged EXEC komutunu kullanın.

Yalnızca geçerli terminal oturumu sırasında geçmiş arabelleğinin kaydettiği komut satırı sayısını artırmak da pratiktir. Arabellek boyutunu artırmak veya azaltmak için **terminal history size** kullanıcı EXEC komutunu kullanın.

```
R1# terminal history size 200
R1# show history
  show ip int brief
  show interface g0/0/0
  show ip route
  show running-config
  show history
  terminal history size 200
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 18.Bölüm: Anahtarların Çalışma Prensipleri

## 18.1.Frame Forwarding-Çerçeve İletme

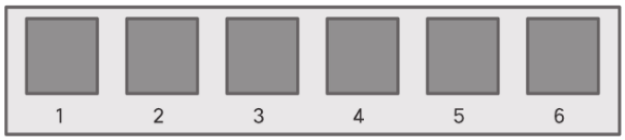
### 18.1.1.Ağda Anahtarlama

Çerçeveleri anahtarlama ve iletme kavramı, ağ iletişimi ve telekomünikasyonda evrenseldir. LAN'larda, WAN'larda ve genel anahtarlamalı telefon ağında (PSTN) çeşitli anahtar türleri kullanılır.

Bir anahtarın trafiği nasıl yönlendireceğine dair karar, o trafiğin akışına göre verilir. Arayüze giren ve çıkan çerçevelerle ilişkili iki terim vardır:

Giriş - Bu, bir çerçevenin aygıta girdiği bağlantı noktasını tanımlamak için kullanılır.
Çıkış - Bu, çerçevelerin cihazdan çıkarken kullanacağı bağlantı noktasını tanımlamak için kullanılır.
Bir LAN anahtarı, trafiği anahtar üzerinden iletirken başvurulan bir tabloyu tutar. Bir LAN anahtarının tek zekası, trafiği iletmek için tablosunu kullanma yeteneğidir. Bir LAN anahtarı, bir Ethernet çerçevesinin giriş bağlantı noktasına ve hedef MAC adresine göre trafiği iletir. Bir LAN anahtarı ile, MAC adresleri ve bağlantı noktaları arasındaki sıkı ilişkiyi tanımlayan yalnızca bir ana anahtarlama tablosu vardır; bu nedenle, belirli bir hedef adresine sahip bir Ethernet çerçevesi, girdiği giriş bağlantı noktasından bağımsız olarak her zaman aynı çıkış bağlantı noktasından çıkar.

Not : Bir Ethernet çerçevesi, alındığı bağlantı noktasından asla iletilmeyecektir.




Port Table

| Destination Addresses | Port |
|---|---|
| EE | 1 |
| AA | 2 |
| BA | 3 |
| EA | 4 |
| AC | 5 |
| AB | 6 |

### 18.1.2.Switch MAC Adres Tablosu

Bir anahtar, entegre devrelerden ve anahtar aracılığıyla veri yollarını kontrol eden eşlik eden yazılımdan oluşur. Anahtarlar, ağ iletişimlerini anahtar aracılığıyla uygun bağlantı noktasından hedefe doğru yönlendirmek için hedef MAC adreslerini kullanır.

Bir anahtarın bir çerçeveyi iletmek için hangi bağlantı noktasını kullanacağını bilmesi için önce her bağlantı noktasında hangi aygıtların bulunduğunu öğrenmesi gerekir. Anahtar, bağlantı noktalarının cihazlarla ilişkisini öğrendikçe, MAC adres tablosu adı verilen bir tablo oluşturur. Bu tablo, yüksek hızlı arama uygulamalarında kullanılan özel bir bellek türü olan içerik adreslenebilir bellekte -Content Addressable Memory (CAM) saklanır. Bu nedenle, MAC adres tablosu bazen CAM tablosu olarak da adlandırılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

LAN anahtarları, MAC adres tablosunu koruyarak gelen veri çerçevelerinin nasıl işleneceğini belirler. Anahtar, bağlantı noktalarının her birine bağlı her aygıtın kaynak MAC adresini kaydederek MAC adres tablosunu doldurur. Anahtar, o aygıta atanmış olan bağlantı noktasından belirli bir aygıta yönelik çerçeveler göndermek için MAC adres tablosundaki bilgilere başvurur.

## Anahtar Öğren ve İlet Yöntemi

Bir anahtara giren her Ethernet çerçevesinde aşağıdaki iki aşamalı işlem gerçekleştirilir.

Adım 1. Öğrenin - Kaynak MAC Adresini İnceleme

Bir anahtara giren her çerçeve, öğrenilecek yeni bilgiler için kontrol edilir. Bunu, çerçevenin kaynak MAC adresini ve çerçevenin anahtara girdiği bağlantı noktası numarasını inceleyerek yapar:

- MAC adresi tablosunda kaynak MAC adresi yoksa, MAC adresi ve gelen bağlantı noktası numarası tabloya eklenir.
- Kaynak MAC adresi mevcutsa, anahtar bu giriş için yenileme zamanlayıcısını günceller. Varsayılan olarak, çoğu Ethernet anahtarı tablodaki bir girişi beş dakika tutar. Kaynak MAC adresi tabloda ancak farklı bir bağlantı noktasında mevcutsa, anahtar bunu yeni bir giriş olarak değerlendirir. Giriş, aynı MAC adresi kullanılarak, ancak daha güncel bağlantı noktası numarasıyla değiştirilir.

Adım 2. İlet - Hedef MAC Adresini İnceleme

Hedef MAC adresi bir tek noktaya yayın adresiyse, anahtar çerçevenin hedef MAC adresi ile MAC adres tablosundaki bir giriş arasında bir eşleşme arayacaktır:

- Hedef MAC adresi tablodaysa, çerçeveyi belirtilen bağlantı noktasının dışına iletecektir.
- Hedef MAC adresi tabloda değilse, anahtar, çerçeveyi gelen bağlantı noktası dışındaki tüm bağlantı noktalarını iletir. Buna bilinmeyen tek noktaya yayın denir. Hedef MAC adresi bir yayın veya çok noktaya yayın ise, çerçeve ayrıca gelen bağlantı noktası dışındaki tüm bağlantı noktalarının dışına taşınır.

## İletme Yöntemlerini Değiştirme

Anahtarlar, Katman 2 yönlendirme kararlarını çok hızlı bir şekilde verir. Bunun nedeni, uygulamaya özel entegre devrelerdeki (ASIC'ler) yazılımdır. ASIC'ler, cihazdaki çerçeve işleme süresini azaltır ve cihazın performansı düşürmeden artan sayıda çerçeveyi yönetmesine izin verir.

Katman 2 anahtarları, çerçeveler arasında geçiş yapmak için iki yöntemden birini kullanır:

**Depola ve ilet** - Bu yöntem, çerçevenin tamamını aldıktan sonra çerçevede bir iletim kararı verir ve döngüsel artıklık denetimi (CRC) olarak bilinen matematiksel bir hata kontrol mekanizması kullanarak çerçeveyi hatalar için kontrol eder. Sakla ve ilet anahtarlama, Cisco'nun birincil LAN anahtarlama yöntemidir.

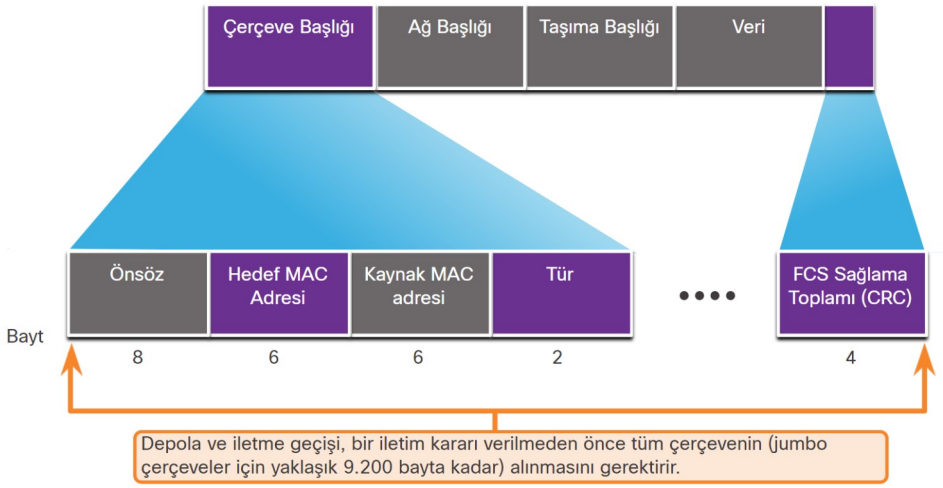
Depola ve ilet (Store-and-Forward)anahtarlama, kestirmeden anahtarlamadan farklı olarak, aşağıdaki iki temel özelliğe sahiptir:

Hata kontrolü - Giriş portundaki tüm çerçeveyi aldıktan sonra, anahtar, datagramın son alanındaki çerçeve kontrol dizisi (FCS) değerini kendi FCS hesaplamalarıyla karşılaştırır. FCS, çerçevenin fiziksel ve veri bağlantısı hatalarından arınmış olmasını sağlamaya yardımcı olan bir hata kontrol sürecidir. Çerçeve hatasız ise, anahtar çerçeveyi ileri götürür. Aksi takdirde çerçeve düşer.

Otomatik arabelleğe alma - Depola ve ilet anahtarları tarafından kullanılan giriş bağlantı noktası arabelleğe alma işlemi, herhangi bir Ethernet hızı karışımını desteklemek mümkün kılar. Örneğin, 1 Gb / sn arabirimden gönderilmesi gereken 100 Mbps Ethernet bağlantı noktasına giden bir gelen çerçevenin işlenmesi, kaydet ve ilet yönteminin kullanılmasını gerektirir. Giriş ve çıkış bağlantı noktaları arasındaki hızlarda herhangi bir uyumsuzluk

licensed to halil karasunay, yalidikkar@gmail.com

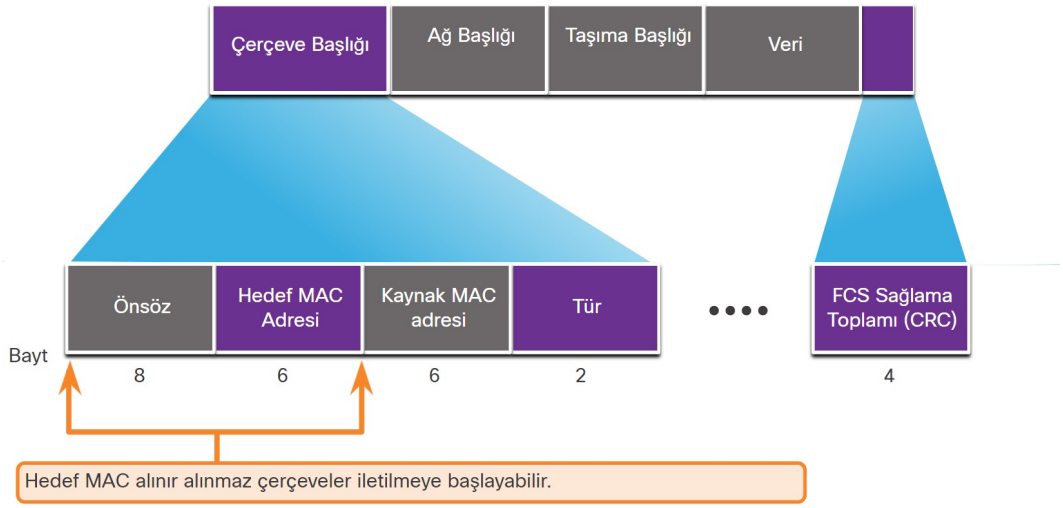
olduğunda, anahtar tüm çerçeveyi bir arabellekte depolar, FCS kontrolünü hesaplar, çıkış bağlantı noktası arabelleğine iletir ve sonra gönderir.
Şekil, depolayıp iletmenin Ethernet çerçevesine dayalı olarak nasıl bir karar verdiğini göstermektedir.




**Kestirmeden(Cut-Through) anahtarlama** - Bu yöntem, gelen çerçevenin hedef MAC adresi ve çıkış bağlantı noktası belirlendikten sonra yönlendirme sürecini başlatır.

Depola ve ilet anahtarlama yöntemi, FCS denetimini geçmeyen çerçeveleri bırakır. Bu nedenle, geçersiz çerçeveleri iletmez.

Bunun tersine, kestirmeden anahtarlama yöntemi, hiçbir FCS denetimi gerçekleştirilmediğinden geçersiz çerçeveleri iletebilir. Bununla birlikte, kestirmeden iletme, hızlı çerçeve değiştirme gerçekleştirme özelliğine sahiptir. Bu, anahtarın, şekilde gösterildiği gibi, çerçevenin hedef MAC adresini MAC adres tablosunda arar aramaz bir iletme kararı verebileceği anlamına gelir.




Anahtarın, yönlendirme kararını vermeden önce çerçevenin geri kalanının giriş bağlantı noktasına girmesini beklemesi gerekmez.

Parçasız anahtarlama, anahtarın çerçeveyi yalnızca Tür alanını okuduktan sonra iletmeye başladığı, değiştirilmiş bir geçiş anahtarlama biçimidir. Parçasız anahtarlama, gecikmede neredeyse hiç artış olmaksızın kesmeye göre daha iyi hata kontrolü sağlar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Geçiş anahtarlamasının daha düşük gecikme hızı, onu 10 mikrosaniye veya daha az işlemden işleme gecikmeleri gerektiren son derece zorlu, yüksek performanslı bilgi işlem (HPC) uygulamaları için daha uygun hale getirir.

Kesmeli anahtarlama yöntemi, hatalı çerçeveleri iletebilir. Ağda yüksek bir hata oranı (geçersiz çerçeveler) varsa, geçiş geçişi bant genişliği üzerinde olumsuz bir etkiye sahip olabilir ve dolayısıyla bant genişliğini hasarlı ve geçersiz çerçevelerle tıkayabilir.

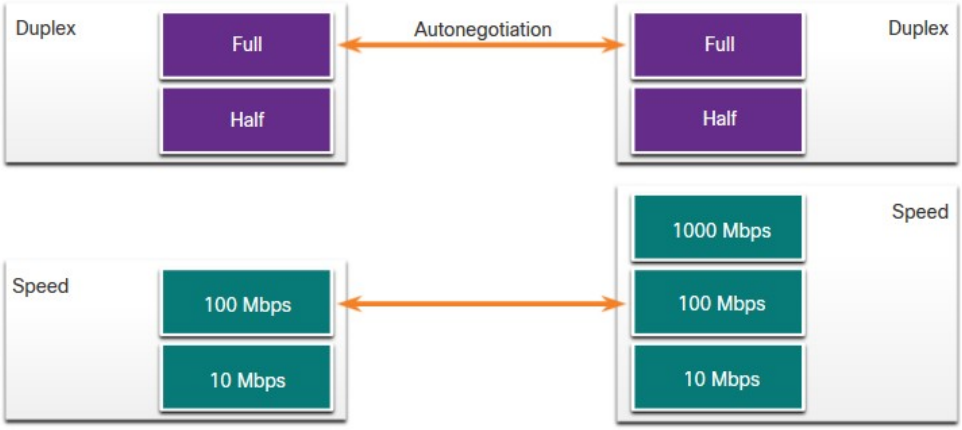
## 18.2.Anahtar Etki Alanları

### 18.2.1Collision Domains-Çarpışma Etki Alanları

Eski hub tabanlı Ethernet segmentlerinde, ağ cihazları paylaşılan ortam için rekabet etti. Cihazlar arasında aynı bant genişliğini paylaşan ağ segmentleri, çarpışma alanları olarak bilinir. Aynı çarpışma alanındaki iki veya daha fazla cihaz aynı anda iletişim kurmaya çalıştığında, bir çarpışma meydana gelecektir.

Bir Ethernet anahtarı bağlantı noktası yarı çift yönlü çalışıyorsa, her segment kendi çarpışma etki alanında bulunur. Anahtar bağlantı noktaları tam çift yönlü olarak çalışırken hiçbir çarpışma etki alanı yoktur. Bununla birlikte, bir anahtar bağlantı noktası yarı çift yönlü çalışıyorsa, bir çakışma alanı olabilir.

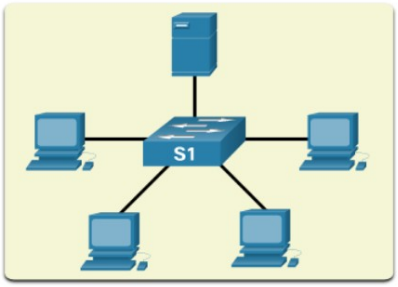
Varsayılan olarak, Ethernet anahtarı bağlantı noktaları, bitişik cihaz tam çift yönlü olarak da çalışabildiğinde tam çift yönlü otomatik olarak anlaşır. Anahtar bağlantı noktası eski bir hub gibi yarı çift yönlü çalışan bir aygıta bağlıysa, anahtar bağlantı noktası yarı çift yönlü olarak çalışacaktır. Yarı çift yönlü olması durumunda, anahtar bağlantı noktası bir çarpışma alanının parçası olacaktır.

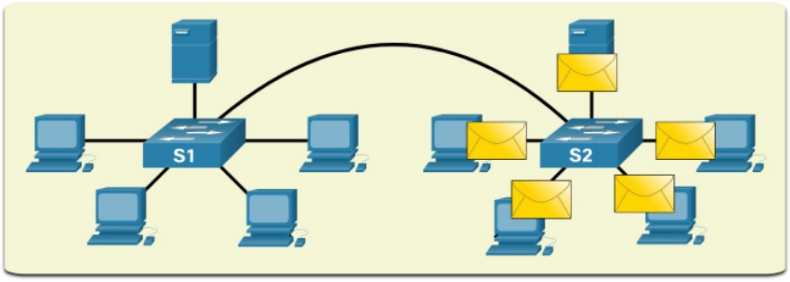



### 18.2.2.Broadcast Domains-Yayın Etki Alanları

Yayın etki alanı, LAN'daki tüm Katman 1 veya Katman 2 aygıtlarına kadar uzanır.
MAC katmanı olarak da adlandırılan yayın alanını yalnızca bir katman 3 cihazı (yönlendirici) kırar.
Yayın alanı, LAN üzerindeki yayın trafiğini alan tüm cihazlardan oluşur.
Katman 2 anahtarı yayını aldığında, giriş arayüzü hariç tüm arayüzlerden taşar.
Çok fazla yayın tıkanıklığa ve düşük ağ performansına neden olabilir.
Katman 1 veya katman 2'deki aygıtların artırılması yayın alanının genişlemesine neden olur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 19.Bölüm: VLAN’lar

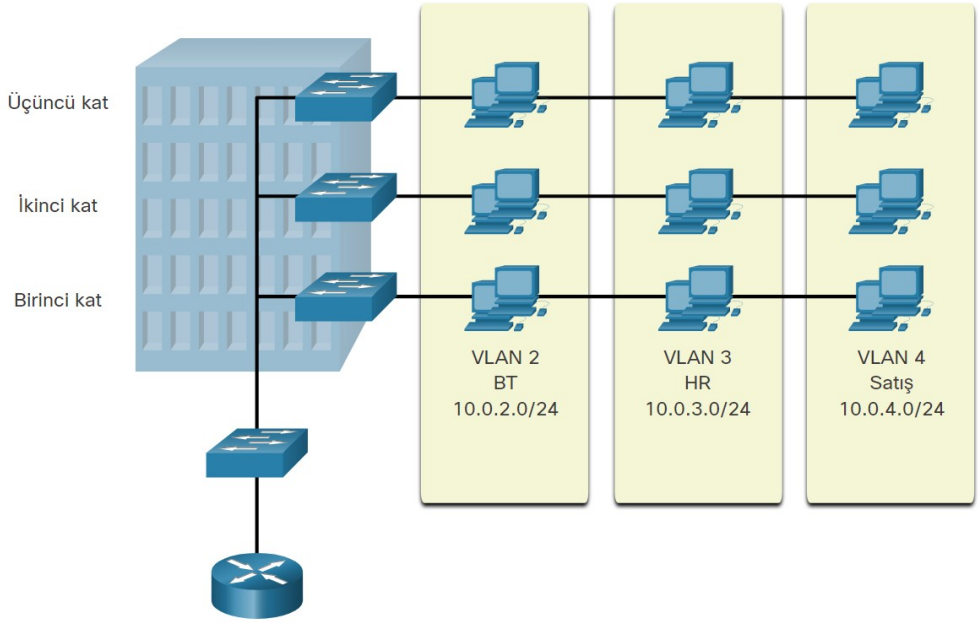
## 19.1.VLAN’lara Genel Bakış

### 19.1.1VLAN (Virtual LAN) Nedir?

Sanal LAN'lar (VLAN'lar), anahtarlı bir ağda bölümleme ve organizasyonel esneklik sağlar. Bir VLAN içindeki bir grup cihaz, her cihaz aynı kabloya bağlıymış gibi iletişim kurar. VLAN'lar, fiziksel bağlantılar yerine mantıksal bağlantılara dayanır.

Şekilde gösterildiği gibi, anahtarlamalı bir ağdaki VLAN'lar, çeşitli departmanlardaki (yani BT, İK ve Satış) kullanıcıların, kullanılan fiziksel anahtardan veya bir kampüs LAN'ındaki konumdan bağımsız olarak aynı ağa bağlanmasını sağlar.

Şekil, her katta bir anahtar bulunan 3 katlı bir binayı göstermektedir. Anahtarlar, bir yönlendiriciye bağlı başka bir anahtara bağlanır. Her katın kendisine bağlı birden fazla ana bilgisayarı vardır. Üç kata yayılan ve her katta birden çok ana bilgisayar içeren üç VLAN vardır. VLAN'lar şunlardır: VLAN 2, IT, 10.0.2.0/24; VLAN 3, HR, 10.0.3.0/24; VLAN 4, Satış, 10.0.4.0/24.




VLAN'lar, bir yöneticinin ağları, kullanıcıların veya cihazların fiziksel konumuna bakılmaksızın işlev, ekip veya uygulama gibi faktörlere göre bölümlere ayırmasına izin verir. Her VLAN, ayrı bir mantıksal ağ olarak kabul edilir. Bir VLAN içindeki cihazlar, diğer VLAN'larla ortak bir altyapıyı paylaşsalar bile, kendi bağımsız ağları içindeymiş gibi davranırlar. Herhangi bir anahtar bağlantı noktası bir VLAN'a ait olabilir.

Tek noktaya yayın, yayın ve çok noktaya yayın paketleri yalnızca paketlerin kaynaklandığı VLAN içindeki uç cihazlara iletilir ve taşınır. VLAN'a ait olmayan cihazlar için hedeflenen paketler, yönlendirmeyi destekleyen bir cihaz aracılığıyla iletilmelidir.

Birden çok IP alt ağı, birden çok VLAN kullanılmadan, anahtarlamalı bir ağda bulunabilir. Ancak cihazlar aynı Katman 2 yayın alanında olacaktır. Bu, ARP isteği gibi herhangi bir Katman 2 yayının, yayını almak istemeyenler bile anahtarlanmış ağdaki tüm cihazlar tarafından alınacağı anlamına gelir.

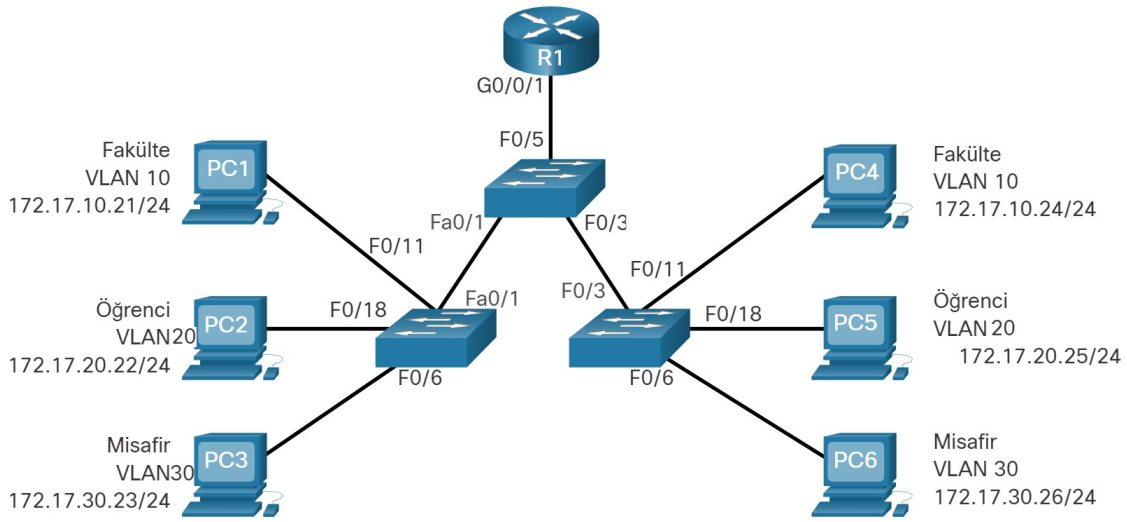
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bir VLAN, birden çok fiziksel LAN segmentine yayılabilen mantıksal bir yayın alanı oluşturur. VLAN'lar, büyük yayın alanlarını daha küçük alanlara ayırarak ağ performansını iyileştirir. Bir VLAN'daki bir cihaz bir yayın Ethernet çerçevesi gönderirse, VLAN'daki tüm cihazlar çerçeveyi alır ancak diğer VLAN'lardaki cihazlar almaz.

Ağ yöneticileri, VLAN'ları kullanarak, belirli kullanıcı gruplamalarına göre erişim ve güvenlik politikaları uygulayabilir. Her bir anahtar bağlantı noktası yalnızca bir VLAN'a atanabilir (bir IP telefona veya başka bir anahtara bağlı bir bağlantı noktası hariç).

## 19.1.2.VLAN Tasarımının Faydaları

Anahtarlamalı bir ağdaki her VLAN, bir IP ağına karşılık gelir. Bu nedenle, VLAN tasarımı, hiyerarşik bir ağ adresleme şemasının uygulanmasını dikkate almalıdır. Hiyerarşik ağ adresleme, IP ağ numaralarının ağı bir bütün olarak dikkate alacak şekilde ağ segmentlerine veya VLAN'lara uygulanması anlamına gelir. Şekilde gösterildiği gibi, bitişik ağ adresi blokları ağın belirli bir alanındaki aygıtlar için ayrılır ve yapılandırılır.




| Avantajları | Açıklama |
|---|---|
| Daha Küçük Yayın Alanları | LAN'ı bölmek yayın alanlarının sayısını azaltır |
| Geliştirilmiş Güvenlik | Yalnızca aynı VLAN'daki kullanıcılar birlikte iletişim kurabilir |
| Geliştirilmiş BT Verimliliği | VLAN'lar benzer gereksinimlere sahip cihazları gruplar ör. fakülte öğrenciler vb. |
| Düşük Maliyet | Bir anahtar birden fazla grubu veya VLAN'ı destekleyebilir |
| Daha iyi performans | Küçük yayın alanları trafiği azaltır ve bant genişliğini artırır |
| Daha Basit Yönetim | Benzer gruplar benzer uygulamalara ve diğer ağ kaynaklarına ihtiyaç duyacaktır |

## 19.1.3.VLAN ÇEŞİTLERİ

### Varsayılan-Default VLAN

Bir Cisco anahtarındaki varsayılan VLAN, VLAN 1'dir. Bu nedenle, başka bir VLAN'da olacak şekilde açıkça yapılandırılmadıkça tüm anahtar bağlantı noktaları VLAN 1'dedir. Varsayılan olarak, tüm Katman 2 kontrol trafiği VLAN 1 ile ilişkilidir.

Licensed to yetkin karasuluğlu, yetkinkrsglu@gmail.com

VLAN 1 hakkında unutulmaması gerekenler:

- Tüm bağlantı noktaları varsayılan olarak VLAN 1'e atanır.
- Yerel VLAN, varsayılan olarak VLAN 1'dir.
- Yönetim VLAN'ı varsayılan olarak VLAN 1'dir.
- VLAN 1 yeniden adlandırılamaz veya silinemez.
- Örneğin, **show vlan brief** çıktısında, tüm bağlantı noktaları şu anda varsayılan VLAN 1'e atanmıştır. Hiçbir doğal (native) VLAN açık bir şekilde atanmamıştır ve başka hiçbir VLAN etkin değildir; bu nedenle ağ, yönetim (management) VLAN ile aynı şekilde doğal VLAN ile tasarlanır. Bu bir güvenlik riski olarak kabul edilir.

```
Switch# show vlan brief
VLAN Name             Status   Ports
---- ---------------- -------  -------------------
1    default          active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                               Fa0/5, Fa0/6, Fa0/7, Fa0/8
                               Fa0/9, Fa0/10, Fa0/11, Fa0/12
                               Fa0/13, Fa0/14, Fa0/15, Fa0/16
                               Fa0/17, Fa0/18, Fa0/19, Fa0/20
                               Fa0/21, Fa0/22, Fa0/23, Fa0/24
                               Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

### Veri VLANI

Veri VLAN'ları, kullanıcı tarafından oluşturulan trafiği ayırmak için yapılandırılmış VLAN'lardır. Ağı kullanıcı veya cihaz gruplarına ayırdıkları için kullanıcı VLAN'ları olarak adlandırılırlar. Modern bir ağ, organizasyon gereksinimlerine bağlı olarak birçok veri VLAN'ına sahip olacaktır. Veri VLAN'larında ses ve ağ yönetimi trafiğine izin verilmemesi gerektiğini unutmayın.

### Doğal (Native) VLAN

Bir VLAN'dan gelen kullanıcı trafiği, başka bir anahtara gönderildiğinde VLAN kimliğiyle etiketlenmelidir. Trunk bağlantı noktaları, etiketli trafiğin iletimini desteklemek için anahtarlar arasında kullanılır. Spesifik olarak, bir 802.1Q ana hat-trunk portu, çerçevenin ait olduğu VLAN'ı tanımlamak için Ethernet çerçeve başlığına 4 baytlık bir etiket ekler.

Bir anahtarın ayrıca bir ana hat bağlantısı üzerinden etiketsiz trafik göndermesi gerekebilir. Etiketsiz trafik bir anahtar tarafından oluşturulur ve eski cihazlardan da gelebilir. 802.1Q ana bağlantı noktası, yerel VLAN'a etiketsiz trafik yerleştirir. Bir Cisco anahtarındaki doğal VLAN, VLAN 1'dir (yani varsayılan VLAN).

Doğal VLAN'ı, VLAN 1 ve diğer VLAN'lardan farklı olarak kullanılmayan bir VLAN olarak yapılandırmak en iyi uygulamadır. Aslında, anahtarlı etki alanındaki tüm ana hat bağlantı noktaları için doğal VLAN rolünü yerine getirmek üzere sabit başka bir VLAN tahsis etmek tavsiye edilen bir uygulamadır.

### Yönetim (Management)VLANI

Yönetim VLAN'ı, SSH, Telnet, HTTPS, HTTP ve SNMP dahil olmak üzere ağ yönetimi trafiği için özel olarak yapılandırılmış bir veri VLAN'dır. Varsayılan olarak, VLAN 1, Katman 2 anahtarında yönetim VLAN'ı olarak yapılandırılır.

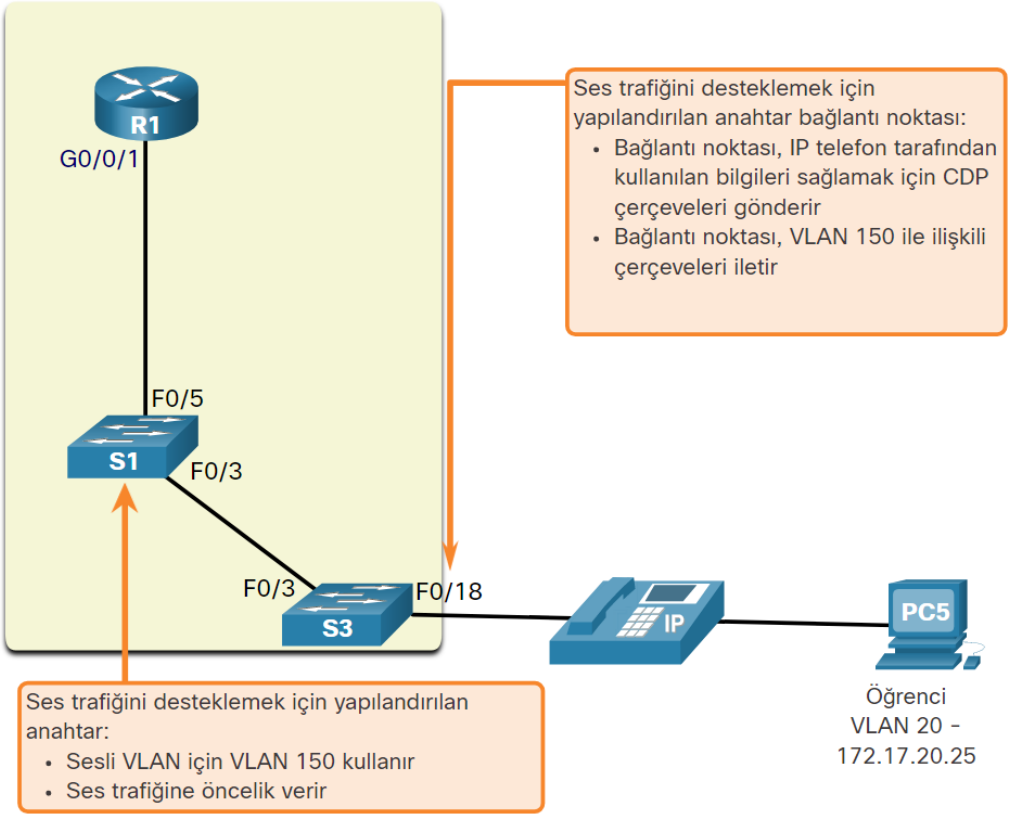
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Ses (Voice) VLANI**

IP üzerinden Ses'i (VoIP-Voice over ) desteklemek için ayrı bir VLAN gereklidir. VoIP trafiği aşağıdakileri gerektirir:

Ses kalitesini sağlamak için garantili bant genişliği
Diğer ağ trafiği türlerine göre iletim önceliği
Ağ üzerindeki sıkışık alanların etrafına yönlendirilme yeteneği
Ağda 150 ms'den daha az gecikme
Bu gereksinimleri karşılamak için, tüm ağ VoIP'yi destekleyecek şekilde tasarlanmalıdır.

Şekilde VLAN 150, ses trafiğini taşımak üzere tasarlanmıştır. Öğrenci bilgisayarı PC5, Cisco IP telefonuna ve telefon S3 anahtarına bağlıdır. PC5, öğrenci verileri için kullanılan VLAN 20 içindedir.




## 19.2.Çok Anahtarlı Bir Ortamdaki VLAN'lar

### 19.2.1.VLAN Trunklarını Tanımlama

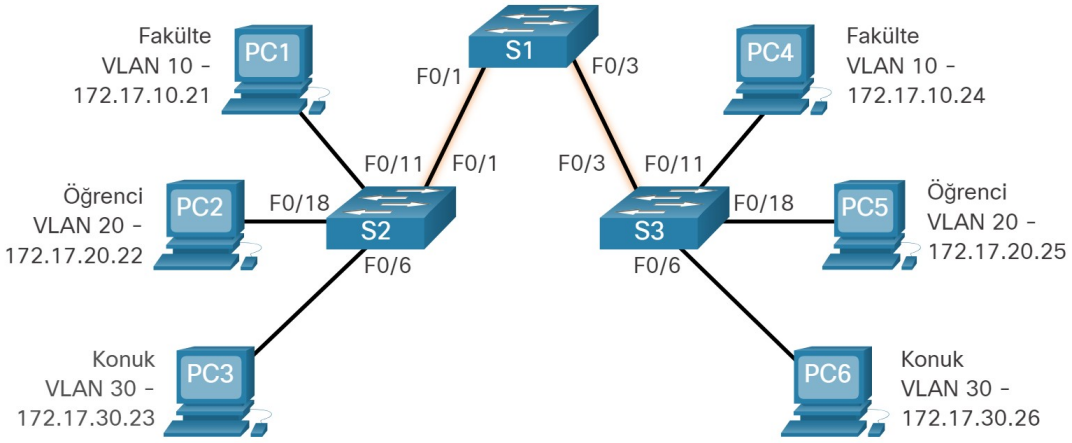
VLAN'lar, VLAN ana hatları (trunk) olmadan pek kullanışlı olmazdı. VLAN bağlantıları, tüm VLAN trafiğinin anahtarlar arasında yayılmasına izin verir. Bu, farklı anahtarlara bağlı ancak aynı VLAN'daki cihazların bir yönlendiriciden geçmeden iletişim kurmasını sağlar.

Bir ana hat, birden fazla VLAN taşıyan iki ağ cihazı arasındaki noktadan noktaya bir bağlantıdır. Bir VLAN trunk, VLAN'ları tüm ağ boyunca genişletir. Cisco, Hızlı Ethernet, Gigabit Ethernet ve 10-Gigabit Ethernet arayüzlerindeki ana hatları koordine etmek için IEEE 802.1Q'yu destekler.

Licensed to yetkin.kerasunud yetkin.kerasu@gmail.com

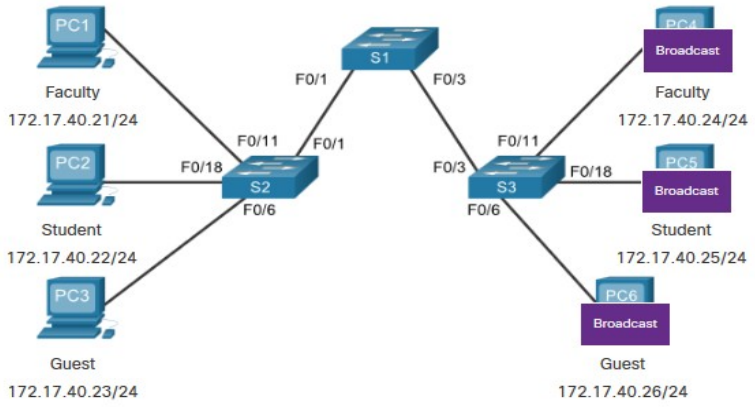
Bir VLAN trunk, belirli bir VLAN'a ait değildir. Bunun yerine, anahtarlar ve yönlendiriciler arasında çoklu VLAN'lar için bir kanaldır. Bir ana hat, bir ağ cihazı ile sunucu veya uygun bir 802.1Q özellikli NIC ile donatılmış başka bir cihaz arasında da kullanılabilir. Varsayılan olarak, bir Cisco Catalyst anahtarında, tüm VLAN'lar bir ana hat bağlantı noktasında desteklenir.

Şekilde, S1 ve S2 anahtarları ile S1 ve S3 arasındaki vurgulanan bağlantılar, ağ üzerinden VLAN'lar 10, 20, 30 ve 99'dan (yani doğal VLAN) gelen trafiği iletmek üzere yapılandırılmıştır. Bu ağ, VLAN bağlantıları olmadan çalışamaz.




## VLAN'lar Olmadan Ağ

Bir anahtar bağlantı noktalarından birinde bir yayın çerçevesi aldığında, çerçeveyi yayının alındığı bağlantı noktası dışındaki tüm diğer bağlantı noktalarının dışına iletir. Şekilde, tüm ağ aynı alt ağda (172.17.40.0/24) yapılandırılır ve hiçbir VLAN yapılandırılmaz. Sonuç olarak, fakülte bilgisayarı (PC1) bir yayın çerçevesi gönderdiğinde, S2 anahtarı bu yayın çerçevesini tüm bağlantı noktalarına gönderir. Sonunda tüm ağ yayını alır çünkü ağ tek bir yayın etki alanıdır.



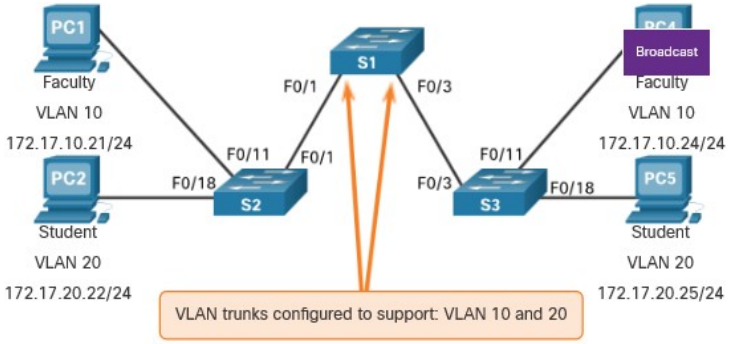

PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.

## VLAN'lı Ağ

VLAN'lar, ayrı anahtar bağlantı noktaları ile ilişkilendirilir ve bunlar üzerinde yapılandırılır. Bu bağlantı noktalarına bağlı cihazlarda VLAN kavramı yoktur. Ancak, bu cihazlar IP adresleme ile yapılandırılmıştır ve belirli bir IP ağının üyeleridir. VLAN ve IP ağı arasındaki bağlantı burada görünür. VLAN, bir IP ağına (veya alt ağa) eşdeğerdir. VLAN'lar anahtar üzerinde yapılandırılırken, IP adresleme cihazda yapılandırılır.

Licensed to yetkin kasungur, yetkinkrsngr@gmail.com

Fakülte cihazları VLAN 10'a atanır ve öğrenci cihazları VLAN 20'ye atanır. Fakülte bilgisayarı PC1'den S2'yi değiştirmek için bir yayın çerçevesi gönderildiğinde, anahtar yayın çerçevesini yalnızca VLAN 10'u desteklemek üzere yapılandırılan anahtar bağlantı noktalarına iletir.




PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.

S2 ve S1 anahtarları (F0 / 1 bağlantı noktaları) ve S1 ile S3 (F0 / 3 bağlantı noktaları) arasındaki bağlantıyı oluşturan bağlantı noktaları, ana hatlardır (trunk )ve ağdaki tüm VLAN'ları desteklemek üzere yapılandırılmıştır.

S1, yayın çerçevesini F0 / 1 bağlantı noktasında aldığında, S1, bu yayın çerçevesini, bağlantı noktası F0 / 3 olan VLAN 10'u desteklemek için yapılandırılmış diğer tek bağlantı noktasından iletir. S3 yayın çerçevesini F0 / 3 bağlantı noktasında aldığında, bu yayın çerçevesini F0 / 11 bağlantı noktası olan VLAN 10'u desteklemek için yapılandırılmış diğer tek bağlantı noktasını iletir. Yayın çerçevesi, fakülte bilgisayarı PC4 olan VLAN 10'da yapılandırılan ağdaki diğer tek bilgisayara ulaşır.

VLAN'lar bir anahtarda uygulandığında, belirli bir VLAN'daki bir ana bilgisayardan tek noktaya yayın, çok noktaya yayın ve yayın trafiğinin iletimi, o VLAN'da bulunan cihazlarla sınırlıdır.

## VLAN Etiketleme

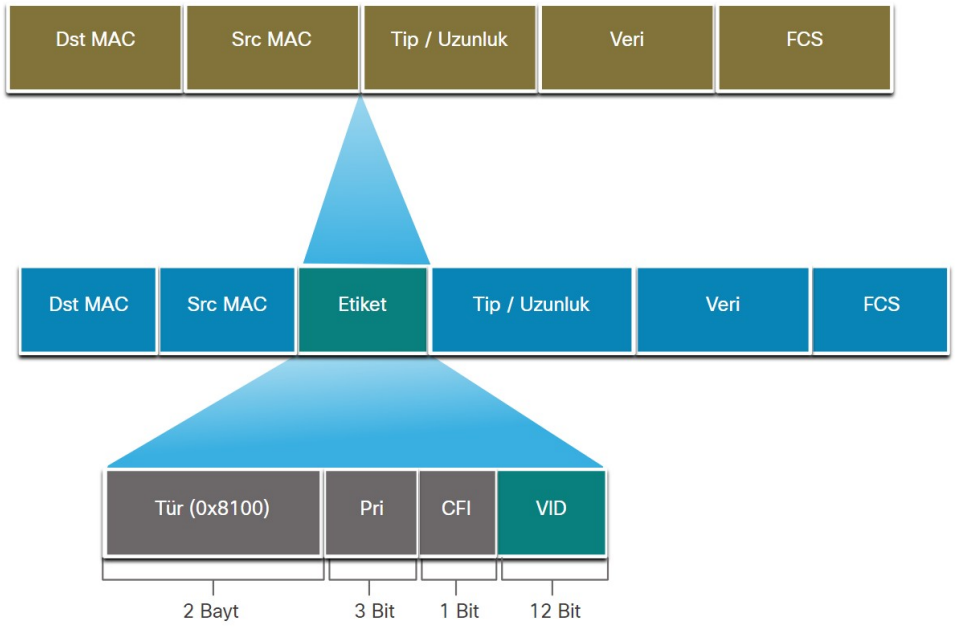
Standart Ethernet çerçeve başlığı, çerçevenin ait olduğu VLAN hakkında bilgi içermez. Bu nedenle, Ethernet çerçeveleri bir trunk üzerine yerleştirildiğinde, ait oldukları VLAN'lar hakkındaki bilgiler eklenmelidir. Etiketleme adı verilen bu işlem, IEEE 802.1Q standardında belirtilen IEEE 802.1Q başlığı kullanılarak gerçekleştirilir. 802.1Q başlığı, çerçevenin ait olduğu VLAN'ı belirten orijinal Ethernet çerçeve başlığına eklenen 4 baytlık bir etiket içerir.

Anahtar, erişim(access) modunda yapılandırılan ve bir VLAN atanan bir bağlantı noktasındaki bir çerçeve aldığında, anahtar çerçeve başlığına bir VLAN etiketi ekler, Çerçeve Kontrol Sırasını (FCS) yeniden hesaplar ve etiketli çerçeveyi bir ana bağlantı noktasından gönderir.

### VLAN Etiketi Alan Ayrıntıları

Şekilde gösterildiği gibi, VLAN etiketi kontrol bilgisi alanı bir Tür alanı, bir Öncelik alanı, bir  Biçim Tanımlayıcı alanı ve VLAN Kimliği alanından oluşur:

Tür - Etiket protokol kimliği (TPID) değeri olarak adlandırılan 2 baytlık bir değer. Ethernet için onaltılık 0x8100 olarak ayarlanmıştır.
Kullanıcı önceliği - Seviye veya hizmet uygulamasını destekleyen 3 bitlik bir değer.
Canonical Format Identifier (CFI) - Token Ring çerçevelerinin Ethernet bağlantıları üzerinden taşınmasını sağlayan 1 bitlik bir tanımlayıcı.
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com
VLAN Kimliği (VID) - 4096'ya kadar VLAN kimliğini destekleyen 12 bitlik bir VLAN kimlik numarası.
Anahtar, etiket kontrol bilgi alanlarını ekledikten sonra, FCS değerlerini yeniden hesaplar ve yeni FCS'yi çerçeveye ekler.




## Doğal (Native) VLAN'lar ve 802.1Q Etiketleme

IEEE 802.1Q standardı, ana hat bağlantıları için doğal bir VLAN belirler ve bu varsayılan VLAN 1'dir. Etiketsiz bir çerçeve bir ana hat bağlantı noktasına ulaştığında doğal VLAN'a atanır. Anahtarlar arasında gönderilen yönetim çerçeveleri, genellikle etiketlenmemiş trafik örneğidir. İki anahtar arasındaki bağlantı bir ana hat ise, anahtar etiketsiz trafiği doğal VLAN'da gönderir.

## Doğal VLAN'da Etiketli Çerçeveler

Birleştirmeyi destekleyen bazı cihazlar, doğal VLAN trafiğine bir VLAN etiketi ekler. Doğal VLAN'da gönderilen kontrol trafiği etiketlenmemelidir. Bir 802.1Q ana bağlantı noktası, doğal VLAN ile aynı olan VLAN kimliğine sahip etiketli bir çerçeve alırsa, çerçeveyi bırakır. Sonuç olarak, bir Cisco anahtarındaki bir anahtar bağlantı noktasını yapılandırırken, cihazları doğal VLAN'da etiketli çerçeveler göndermeyecek şekilde yapılandırın. Doğal VLAN'da etiketli çerçeveleri destekleyen diğer satıcıların cihazları arasında IP telefonları, sunucular, yönlendiriciler ve Cisco olmayan anahtarlar bulunur.

## Doğal VLAN'daki Etiketsiz Çerçeveler

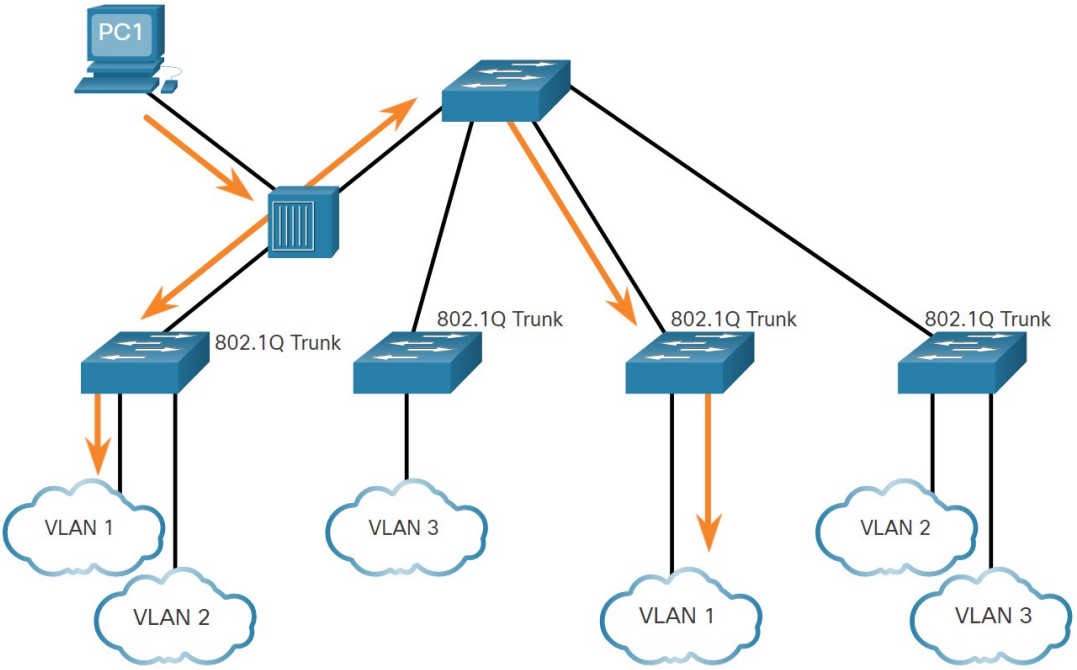
Bir Cisco anahtar ana bağlantı noktası etiketsiz çerçeveler aldığında (iyi tasarlanmış bir ağda alışılmadık bir durumdur), bu çerçeveleri doğal VLAN'a iletir. Doğal VLAN ile ilişkili herhangi bir cihaz yoksa (bu alışılmadık değildir) ve başka ana hat portu yoksa (bu da alışılmadık değildir), çerçeve düşürülür. Varsayılan doğal VLAN, VLAN 1'dir. Bir 802.1Q ana bağlantı noktası yapılandırılırken, doğal VLAN kimliğinin değeri varsayılan bir Bağlantı Noktası VLAN Kimliği (PVID) olarak atanır. 802.1Q bağlantı noktasından gelen veya çıkan tüm etiketlenmemiş trafik, PVID değerine göre iletilir. Örneğin, VLAN 99 doğal VLAN olarak yapılandırılırsa, PVID 99 olur ve tüm etiketlenmemiş trafik VLAN 99'a iletilir. Doğal VLAN yeniden yapılandırılmamışsa, PVID değeri VLAN 1 olarak ayarlanır.

Şekilde, PC1 bir hub ile 802.1Q devre bağlantısına bağlanmıştır.

Şekil, doğal VLAN üzerindeki etiketsiz trafik akışını gösteren bir ağ topolojisidir. Şeklin üst kısmında bir anahtar var. Anahtar, her birine bir 802.1Q devre bağlantısı yoluyla aşağıda dört diğer anahtara bağlanır. Üstteki anahtar ile en soldaki anahtar arasında, ana PC1'in bağlı olduğu bir hub bulunur. En soldaki anahtarın VLAN 1'de bir bağlantı noktası ve VLAN 2'de bir bağlantı noktası vardır. Soldan ikinci anahtarın VLAN 3'te bir bağlantı noktası vardır. Soldan üçüncü anahtarın VLAN 1'de bir bağlantı noktası vardır. Sağdaki anahtarın bir VLAN 2'de bağlantı noktası ve VLAN 3'te bir bağlantı noktası. Turuncu oklar, PC1 akışlarından hub'a gönderilen trafiği ve onu her iki bağlı

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

anahtara gönderen trafiği gösterir. En soldaki anahtar, onu VLAN 1'deki bağlantı noktasına gönderir. Üstteki anahtar, onu soldan üçüncü anahtara gönderir ve bu da onu VLAN 1'e bağlı bağlantı noktasından dışarı gönderir.




PC1, anahtarların ana bağlantı noktalarında yapılandırılan doğal VLAN ile ilişkilendirdiği ve buna göre ilettiği etiketlenmemiş trafiği gönderir. PC1 tarafından alınan ana hattaki etiketli trafik bırakılır. Bu senaryo, birkaç nedenden ötürü zayıf ağ tasarımını yansıtır: bir hub kullanır, bir ana hat bağlantısına bağlı bir ana bilgisayara sahiptir ve anahtarların doğal VLAN'a atanmış erişim bağlantı noktalarına sahip olduğu anlamına gelir. Ayrıca, eski senaryoları yönetmenin bir yolu olarak doğal VLAN'lar için IEEE 802.1Q spesifikasyonunun motivasyonunu da göstermektedir.

## Ses VLAN'ı Etiketleme

VoIP'i desteklemek için ayrı bir ses VLAN'ı gereklidir. Bu, hizmet kalitesi (QoS- quality of service ) ve güvenlik politikalarının ses trafiğine uygulanmasını sağlar.

Bir Cisco IP telefonu doğrudan bir anahtar bağlantı noktasına bağlanır. Bir IP ana bilgisayarı, ağ bağlantısı elde etmek için IP telefona da bağlanabilir. Cisco IP telefonuna bağlı erişim portu, iki ayrı VLAN kullanacak şekilde yapılandırılabilir. Bir VLAN, ses trafiği içindir ve diğeri, ana bilgisayar trafiğini desteklemek için bir veri VLAN'dır. Anahtar ve IP telefonu arasındaki bağlantı, hem ses VLAN trafiğini hem de veri VLAN trafiğini taşımak için bir ana hat bağlantısını simüle eder.

Özellikle, Cisco IP Phone, entegre üç bağlantı noktalı bir 10/100 anahtarı içerir. Bağlantı noktaları, aşağıdaki cihazlara özel bağlantılar sağlar:

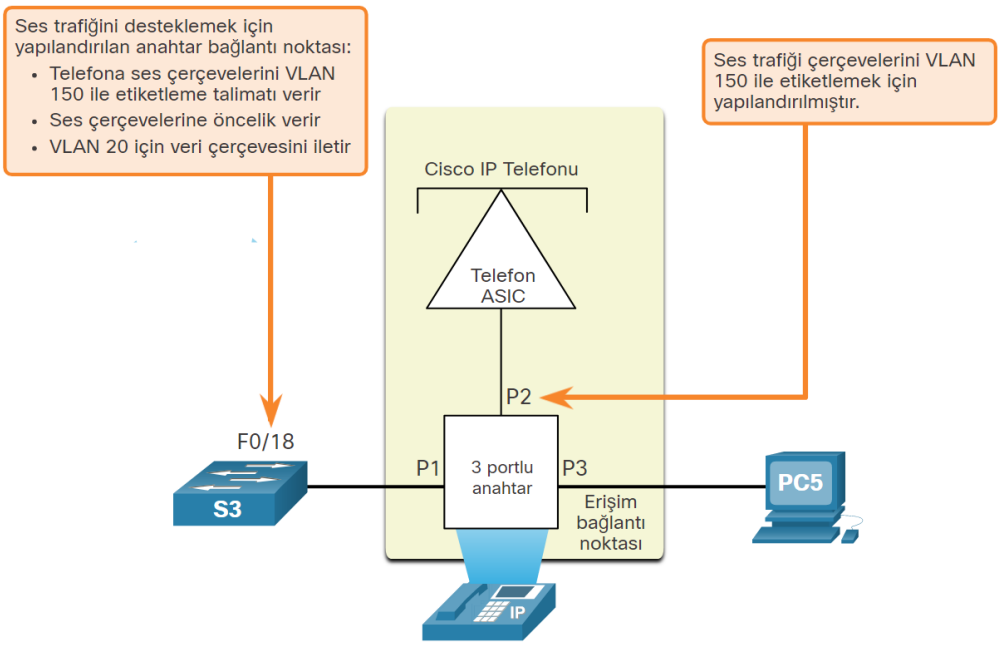
- Port 1, anahtara veya diğer VoIP cihazına bağlanır.
- Port 2, IP telefon trafiğini taşıyan dahili bir 10/100 arayüzdür.
- Port 3 (erişim portu) bir PC'ye veya başka bir cihaza bağlanır.

Anahtar erişim portu, takılı IP telefonuna üç yoldan biriyle ses trafiği göndermesi talimatını veren CDP paketleri gönderir. Kullanılan yöntem, trafik türüne göre değişir:

- Sesli VLAN trafiği, uygun bir Katman 2 hizmet sınıfı (CoS) öncelik değeri ile etiketlenmelidir
- Erişim VLAN trafiği, Katman 2 CoS öncelik değeri ile de etiketlenebilir
- Erişim VLAN etiketlenmemiş (Katman 2 CoS öncelik değeri yok)

Licensed to yetkin karasungur, yetkinkrsng@gmail.com

Şekilde, öğrenci bilgisayarı PC5 bir Cisco IP telefonuna ve telefon S3 anahtarına bağlanmıştır. VLAN 150, ses trafiğini taşımak için tasarlanmıştır, PC5 ise öğrenci verileri için kullanılan VLAN 20'dedir.




## Ses VLAN'ı Doğrulama Örneği

**show interface fa0/18 switchport** komutu için örnek çıktı gösterilmektedir. Örnek çıktıdaki vurgulanan alanlar, veri için yapılandırılmış bir VLAN (VLAN 20) ve ses için yapılandırılmış bir VLAN (VLAN 150) ile yapılandırılmış F0 / 18 arayüzünü gösterir.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)
```

# 19.3.VLAN YAPILANDIRMASI

## 19.3.1.Catalyst Anahtarlarda VLAN Aralıkları

Farklı Cisco Catalyst anahtarları, çeşitli sayıda VLAN'ı destekler. Desteklenen VLAN'ların sayısı, çoğu kuruluşun ihtiyaçlarını karşılayacak kadar büyüktür. Örneğin, Catalyst 2960 ve 3650 Serisi anahtarlar 4.000'den fazla VLAN'ı destekler. Bu anahtarlardaki normal aralıklı VLAN'lar 1 ila 1.005 arasında numaralandırılmıştır ve genişletilmiş aralıklı VLAN'lar 1.006 ila 4.094 arasında numaralandırılmıştır. Şekil, Cisco IOS Sürüm 15.x çalıştıran bir Catalyst 2960 anahtarındaki varsayılan VLAN'ları gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
Switch# show vlan brief

VLAN Name             Status   Ports
---- ---------------- -------  -------------------
1    default          active   Fa0/1, Fa0/2, Fa0/3, Fa0/4
                               Fa0/5, Fa0/6, Fa0/7, Fa0/8
                               Fa0/9, Fa0/10, Fa0/11, Fa0/12
                               Fa0/13, Fa0/14, Fa0/15, Fa0/16
                               Fa0/17, Fa0/18, Fa0/19, Fa0/20
                               Fa0/21, Fa0/22, Fa0/23, Fa0/24
                               Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

### Normal Aralık VLAN'lar

Aşağıdakiler normal aralıklı VLAN'ların özellikleridir:

- Tüm küçük ve orta ölçekli işletme ve kurumsal ağlarda kullanılırlar.
- 1 ile 1005 arasında bir VLAN ID ile tanımlanırlar.
- 1002'den 1005'e kadar olan kimlikler, eski ağ teknolojileri (yani, Token Ring ve Fiber Dağıtılmış Veri Arayüzü) için ayrılmıştır.
- Kimlikler 1 ve 1002 - 1005 otomatik olarak oluşturulur ve kaldırılamaz.
- Yapılandırmalar, anahtar flaş belleğinde vlan.dat adlı bir VLAN veritabanı dosyasında saklanır.
- Yapılandırıldığında, VLAN bağlantı protokolü (VTP), VLAN veritabanının anahtarlar arasında senkronize edilmesine yardımcı olur.

### Genişletilmiş Aralık VLAN'lar

Aşağıdakiler, genişletilmiş menzilli VLAN'ların özellikleridir:

- Servis sağlayıcılar tarafından birden çok müşteriye hizmet vermek için ve genişletilmiş VLAN kimliklerine ihtiyaç duyacak kadar büyük küresel kuruluşlar tarafından kullanılırlar.
- 1006 ile 4094 arasında bir VLAN Kimliği ile tanımlanırlar.
- Yapılandırmalar varsayılan olarak çalışan yapılandırmada kaydedilir.
- Normal aralıklı VLAN'lardan daha az VLAN özelliğini desteklerler.
- Genişletilmiş menzilli VLAN'ları desteklemek için VTP şeffaf (transparent) mod yapılandırması gerektirir.

Not : 4096, IEEE 802.1Q başlığının VLAN ID alanında 12 bit olduğundan, Catalyst anahtarlarında kullanılabilen VLAN sayısı için üst sınırdır.

## 19.3.2.VLAN Oluşturma Komutları

Normal aralıklı VLAN'ları yapılandırırken, yapılandırma ayrıntıları anahtardaki flash bellekte vlan.dat adlı bir dosyada saklanır. Flash bellek kalıcıdır ve **copy running-config startup-config** komutunu gerektirmez. Ancak, diğer ayrıntılar genellikle bir Cisco anahtarında VLAN'ların oluşturulduğu anda yapılandırıldığı için, çalışan yapılandırma değişikliklerini başlangıç yapılandırmasına kaydetmek iyi bir uygulamadır.

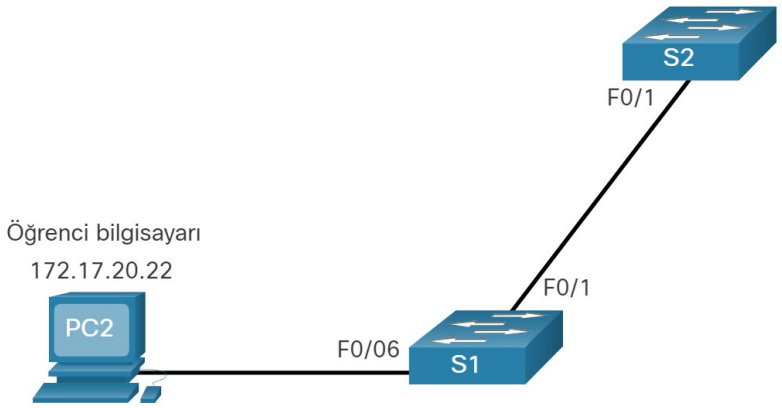
Tablo, bir anahtara VLAN eklemek ve ona bir ad vermek için kullanılan Cisco IOS komut sözdizimini gösterir. Her VLAN'ı adlandırmak, anahtar yapılandırmasında en iyi uygulama olarak kabul edilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Görev | IOS Komutları |
|---|---|
| Genel yapılandırma moduna girin. | Switch# **configure terminal** |
| Geçerli bir kimlik numarasına sahip bir VLAN oluşturun. | Switch(config)# **vlan** *vlan-id* |
| VLAN'ı tanımlamak için benzersiz bir ad belirtin. | Switch(config-vlan)# **name** *vlan-name* |
| Ayrıcalıklı EXEC moduna dönün. | Switch(config-vlan)# **end** |

### VLAN Oluşturma Örneği

Topolojide, öğrenci bilgisayarı (PC2) henüz bir VLAN ile ilişkilendirilmemiştir, ancak VLAN 20'ye ait olan 172.17.20.22 IP adresine sahiptir.




Örnek, öğrenci VLAN'ının (VLAN 20) S1 anahtarında nasıl yapılandırıldığını gösterir.

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

Not : Tek bir VLAN kimliği girmeye ek olarak, virgülle ayrılmış bir dizi VLAN kimliği veya vlan vlan-id komutu kullanılarak kısa çizgilerle ayrılmış bir dizi VLAN kimliği girilebilir . Örneğin, **vlan 100,102,105-107** global konfigürasyon komutunu girmek 100, 102, 105, 106 ve 107 VLAN'ları oluşturacaktır .

### 19.3.4.VLAN Bağlantı Noktası Atama Komutları

Bir VLAN oluşturduktan sonraki adım, VLAN'a bağlantı noktaları atamaktır.

Tablo, bir bağlantı noktasını erişim bağlantı noktası olarak tanımlamak ve bunu bir VLAN'a atamak için sözdizimini gösterir. **switchport mode access** komutu isteğe bağlıdır, ancak şiddetle güvenlik açısından en iyi uygulama olarak tavsiye edilir. Bu komutla, arayüz erişim (access) moduna geçer. Erişim modu, bağlantı noktasının tek bir VLAN'a ait olduğunu ve bir ana hat bağlantısı (trunk) olmak için anlaşmayacağını belirtir.

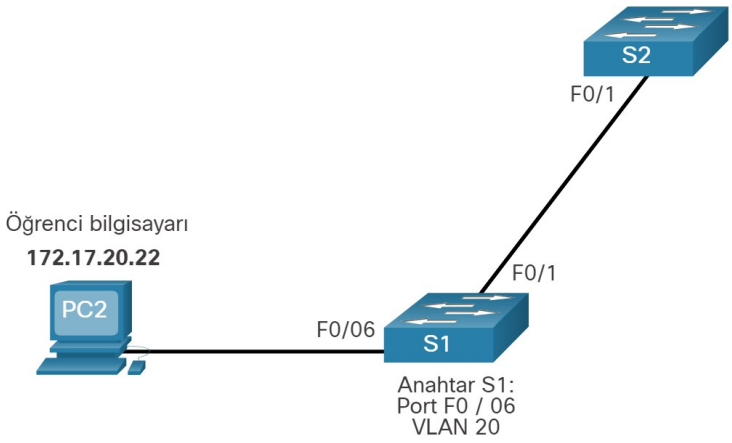
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Görev | Komutlar |
|---|---|
| Genel yapılandırma moduna girin. | Switch# **configure terminal** |
| Arayüz yapılandırma moduna girin. | Switch(config)# **interface** *interface-id* |
| Bağlantı noktasını erişim moduna ayarlayın. | Switch(config-if)# **switchport mode access** |
| Bağlantı noktasını bir VLAN'a atayın. | Switch(config-if)# **switchport access vlan** *vlan-id* |
| Ayrıcalıklı EXEC moduna dönün. | Switch(config-if)# **end** |

Not : Birden çok arabirimi aynı anda yapılandırmak için **interface range** komutunu kullanın.

### VLAN Bağlantı Noktası Atama Örneği

Şekilde, S1 anahtarı üzerindeki F0 / 6 bağlantı noktası bir erişim bağlantı noktası olarak yapılandırılmıştır ve VLAN 20'ye atanmıştır. Bu bağlantı noktasına bağlı herhangi bir cihaz VLAN 20 ile ilişkilendirilecektir. Bu nedenle, örneğimizde PC2, VLAN 20 içindedir.




Örnek, S1'in F0 / 6'yı VLAN 20'ye atamak için yapılandırmasını gösterir.

```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
```

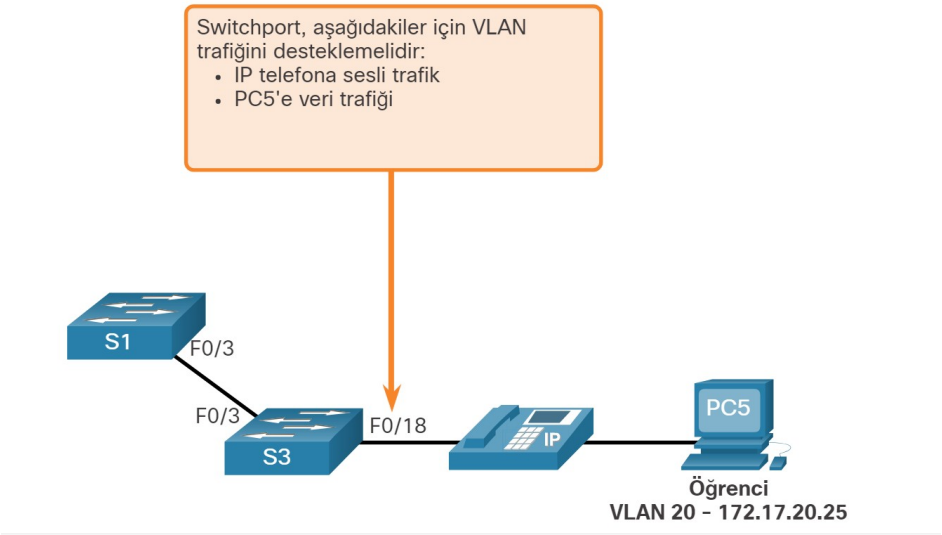
VLAN'lar son cihazda değil anahtar bağlantı noktasında yapılandırılır. PC2, anahtar bağlantı noktasında yapılandırılan VLAN ile ilişkili bir IPv4 adresi ve alt ağ maskesi ile yapılandırılır. Bu örnekte, VLAN 20'dir. VLAN 20 diğer anahtarlarda yapılandırıldığında, ağ yöneticisinin diğer öğrenci bilgisayarlarını PC2 (172.17.20.0/24) ile aynı alt ağda olacak şekilde yapılandırması gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 19.3.5. VERİ VE SES VLANLARI

Bir erişim bağlantı noktası aynı anda yalnızca bir veri VLAN'ına ait olabilir. Bununla birlikte, bir bağlantı noktası aynı zamanda bir ses VLAN ile ilişkilendirilebilir. Örneğin, bir IP telefona ve bir uç cihaza bağlı bir bağlantı noktası iki VLAN ile ilişkilendirilebilir: biri ses için, diğeri veri için.

Şekildeki topolojiyi bakınız. PC5, S3'teki FastEthernet 0/18 arayüzüne bağlanan Cisco IP telefonuna bağlanır. Bu konfigürasyonu uygulamak için bir veri VLAN'ı ve bir ses VLAN'ı oluşturulur.




### Veri ve Ses VLAN Örneği

Bir bağlantı noktasına bir ses VLAN'ı atamak için **switchport voice vlan** *vlan-id* arabirim yapılandırma komutunu kullanın.

Ses trafiğini destekleyen LAN'larda tipik olarak hizmet kalitesi (QoS) de etkinleştirilmiştir. Ses trafiği, ağa girer girmez güvenilir olarak etiketlenmelidir. **mls qos trust [cos | device cisco-phone | dscp | ip-precedence]** arabirim yapılandırma komutu, bir arabirimin güvenilir durumunu ayarlamak ve trafiği sınıflandırmak için paketin hangi alanlarının kullanıldığını belirtmek için kullanılır.

Örnekteki yapılandırma iki VLAN'ı (yani, VLAN 20 ve VLAN 150) oluşturur ve ardından S3'ün F0 / 18 arayüzünü VLAN 20'de bir anahtar bağlantı noktası olarak atar. Ayrıca, VLAN 150'ye ses trafiğini atar ve temelde QoS sınıflandırmasını etkinleştirir. IP telefonu tarafından atanan hizmet sınıfı (CoS)'dir.

```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# end
S3#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**switchport access vlan** komutu anahtarda olmayan bir VLAN'ı oluşturur ve portu o VLAN'a atar. Örneğin, VLAN 30, anahtarın show çıkışında mevcut değildir . Eğer **switchport access vlan 30** komutu daha önce yapılandırmamış herhangi arabirimde girilirse, ardından anahtarın çıktısı aşağıdaki gibidir:

```
% Access VLAN does not exist. Creating vlan 30
```

Burada VLAN 30'un öncesinde mevcut olmadığı ama şimdi oluşturulduğu bildirilir.

## 19.3.6.VLAN BİLGİLERİNİ DOĞRULAMA

Bir VLAN yapılandırıldıktan sonra, VLAN yapılandırmaları Cisco IOS show komutları kullanılarak doğrulanabilir . Bunun için :
**show vlan** komutunu kullanın. Söz diziminin tamamı:
**show vlan [brief | id vlan-id | name vlan-name | summary]**

Tabloda **show vlan** komut seçenekleri açıklanmaktadır.

| Görev | Komut Parametresi |
|---|---|
| VLAN adını, durumunu ve bağlantı noktalarını satır başına bir VLAN görüntüler. | **brief** |
| Tanımlanan VLAN ID numarası hakkındaki bilgileri görüntüler. | **id** *vlan-id* |
| Tanımlanan VLAN adı ile ilgili bilgileri görüntüler. Vlan adı, 1 ila 32 karakter arasında bir ASCII dizesidir. | **name** *vlan-name* |
| VLAN özet bilgilerini görüntüleme. | **summary** |

```
S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0
```

Diğer yararlı komutlar şunlardır **show interfaces interface-id switchport and the show interfaces vlan vlan-id** komutu. Örneğin **show interfaces fa0/18 switchport** komutu FastEthernet 0/18 bağlantı noktasının veri ve ses VLAN'larına doğru şekilde atandığını doğrulamak için kullanılabilir.

```
S1# show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 150
Administrative private-vlan host-association: none
(Output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 19.3.7.VLAN PORT ÜYELİĞİNİ DEĞİŞTİRME

VLAN bağlantı noktası üyeliğini değiştirmenin birkaç yolu vardır.

Anahtar erişim bağlantı noktası yanlış bir şekilde bir VLAN'a atanmışsa, **switchport access vlan** *vlan-i*d arabirim yapılandırma komutunu doğru VLAN kimliğiyle yeniden girin . Örneğin, Fa0 / 18'in yanlış bir şekilde VLAN 20 yerine varsayılan VLAN 1'de olacak şekilde yapılandırıldığını varsayın. Bağlantı noktasını VLAN 20 olarak değiştirmek için, **switchport access vlan 20'**yi girmeniz yeterlidir .

Bir bağlantı noktasının üyeliğini varsayılan VLAN 1'e geri döndürmek için, gösterildiği gibi **no switchport access vlan** arayüz yapılandırma modu komutunu kullanın.

Örneğin çıktıda, Fa0 / 18, **show vlan brief** komutuyla onaylandığı gibi varsayılan VLAN 1'de olacak şekilde yapılandırılır .

```
S1(config)# interface fa0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1#
S1# show vlan brief
VLAN Name                 Status    Ports
---- ------------------ --------- -------------------------------
1    default            active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                  Gi0/1, Gi0/2
20   student            active
1002 fddi-default       act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default    act/unsup
1005 trnet-default      act/unsup
```

VLAN 20'nin kendisine bağlantı noktası atanmamış olmasına rağmen hala aktif olduğuna dikkat edin.

## 19.3.8.VLANLARI SİLME

**no vlan** *vlan-id* komutu ile ilgili bir VLAN'i silebilirsiniz.
Dikkat: Bir VLAN'ı silmeden önce, tüm üye bağlantı noktalarını farklı bir VLAN'a yeniden atayın.

**delete flash: vlan.dat** veya **delete vlan.dat** komutları ile tüm VLAN'ları silebilirsiniz

Tüm VLAN'ları sildikten sonra anahtarı yeniden yükleyin.(reload)

Not: Fabrika varsayılanına geri yüklemek için - tüm veri kablolarını çıkarın, başlangıç yapılandırmasını silin ve vlan.dat dosyasını silin, ardından cihazı yeniden yükleyin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 19.4.VLAN TRUNKLARI

### 19.4.1.TRUNK YAPILANDIRMA KOMUTLARI

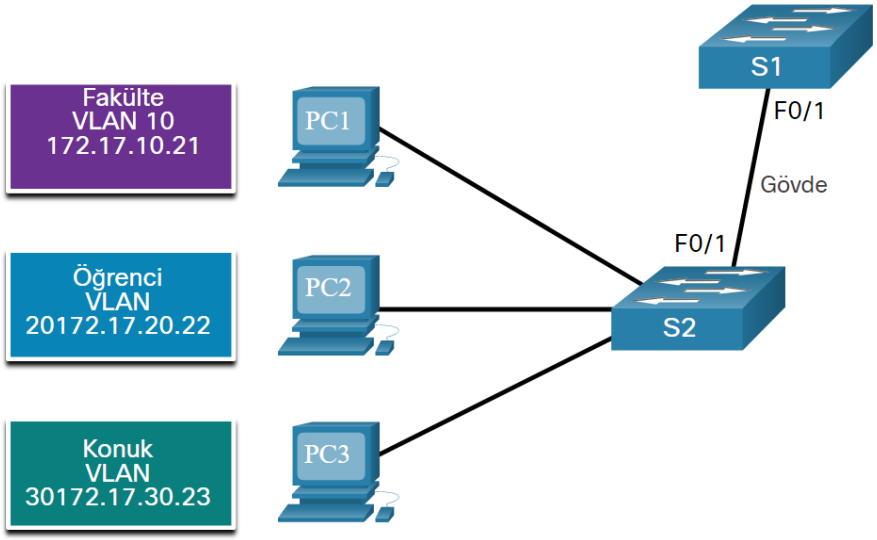
Artık VLAN'ları yapılandırıp doğruladığınıza göre, VLAN bağlantılarını yapılandırma ve doğrulama zamanı. Bir VLAN ana hattı, tüm VLAN'lar için trafik taşıyan iki anahtar arasındaki bir Katman 2 bağlantısıdır (izin verilen VLAN listesi manuel veya dinamik olarak kısıtlanmadıkça).

Ana hat bağlantılarını etkinleştirmek için, birbirine bağlanan portları tabloda gösterilen arayüz yapılandırma komutları setiyle yapılandırın.

| Görev | IOS Komutu |
|---|---|
| Genel yapılandırma moduna girin. | Switch# **configure terminal** |
| Arayüz yapılandırma moduna girin. | Switch(config)# **interface** *interface-id* |
| Bağlantı noktasını trunk moduna ayarlayın. | Switch(config-if)# **switchport mode trunk** |
| Doğal VLAN'ı VLAN 1 dışında bir şeye ayarlayın | Switch(config-if)# **switchport trunk native vlan** *vlan-id* |
| Ana hat (trunk) bağlantıda izin verilecek VLAN'ların listesini belirtin. | Switch(config-if)# **switchport trunk allowed vlan** *vlan-list* |
| Ayrıcalıklı EXEC moduna dönün. | Switch(config-if)# **end** |

### TRUNK YAPILANDIRMA ÖRNEĞİ

Şekilde, VLAN'lar 10, 20 ve 30 Fakülte, Öğrenci ve Misafir bilgisayarlarını (PC1, PC2 ve PC3) destekler. Anahtar S1 üzerindeki F0 / 1 bağlantı noktası, bir ana hat bağlantı noktası olarak yapılandırılır ve trafiği VLAN'lar 10, 20 ve 30 için iletir. VLAN 99, yerel-doğal VLAN olarak yapılandırılır.




Her VLAN ile ilişkili alt ağlar şunlardır:

- VLAN 10 - Fakülte / Personel - 172.17.10.0/24
- VLAN 20 - Öğrenciler - 172.17.20.0/24
- VLAN 30 - Misafirler - 172.17.30.0/24
- VLAN 99 - Yerel - 172.17.99.0/24

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Örnek, S1 anahtarındaki F0 / 1 bağlantı noktasının ana hat bağlantı noktası olarak yapılandırılmasını gösterir. Yerel-Doğal VLAN, VLAN 99 olarak değiştirilir ve izin verilen VLAN listesi 10, 20, 30 ve 99 ile sınırlandırılır.

```
S1(config)# interface fastEthernet 0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

Not : Bu yapılandırma, ana bağlantılarda otomatik olarak 802.1Q kapsüllemeyi kullanan Cisco Catalyst 2960 anahtarlarının kullanıldığını varsayar. Diğer anahtarlar, kapsüllemenin manuel konfigürasyonunu gerektirebilir. Bir ana hat bağlantısının her iki ucunu da her zaman aynı yerel VLAN ile yapılandırın. 802.1Q ana hat yapılandırması her iki uçta da aynı değilse, Cisco IOS Yazılımı hataları rapor eder.

## 19.4.2.TRUNK YAPILANDIRMASINI DOĞRULAYIN

Anahtar çıkışı, S1 anahtarındaki anahtar bağlantı noktası F0 / 1 yapılandırmasını görüntüler. Yapılandırma, **show interfaces interface-ID switchport** komutuyla doğrulanır .

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (VLAN0099)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

En üstte vurgulanan alan, F0 / 1 bağlantı noktasının yönetici modunun ana hat(trunk) olarak ayarlandığını gösterir . Bağlantı noktası, trunk modunda. Bir sonraki vurgulanan alan, yerel VLAN'ın VLAN 99 olduğunu doğrular. Çıkışın daha aşağısında, altta vurgulanan alan, VLAN 10, 20, 30 ve 99'un trunkta etkinleştirildiğini gösterir.

Not : Çok işlevli ana hat arabirimleri için başka bir yararlı komut, **show interface trunk** komutudur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 19.4.3.TRUNK'U VARSAYILAN DURUMA SIFIRLAMA

**no switchport trunk allowed vlan** ve **no switchport trunk native vlan** izin verilen VLANları kaldırmak ve trunkın yerli-doğal VLAN sıfırlamak için kullanılan komutlardır. Varsayılan duruma sıfırlandığında, trunk tüm VLAN'lara izin verir ve yerel-doğal VLAN olarak VLAN 1'i kullanır. Örnek, bir trunk arayüzünün tüm trunk özelliklerini varsayılan ayarlara sıfırlamak için kullanılan komutları gösterir.

```
S1(config)# interface fa0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
```

```
The show interfaces f0/1 switchport command reveals that the trunk has been reconfigured to a default
state.
```

```
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
(output omitted)
```

Bu örnek çıktı, S1 anahtarındaki F0 / 1 anahtar bağlantı noktasından trunk özelliğini kaldırmak için kullanılan komutları gösterir. **show interfaces f0/1 switchport** komutu F0 / 1 arayüzünün statik erişim moduna geçtiğini gösterir.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces fa0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
(output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 19.5.DİNAMİK TRUNK PROTOKOLÜ

## 19.5.1.DTP NEDİR?

Bazı Cisco anahtarlarının, komşu bir cihazla otomatik olarak bağlantı kurmalarına izin veren özel bir protokolü vardır. Bu protokole Dinamik Bağlantı Protokolü -Dynamic Trunking Protocol (DTP) denir. DTP, bir ağ yöneticisi için yapılandırma sürecini hızlandırabilir. Ethernet ana hat arabirimleri farklı kanal modlarını destekler. Bir arabirim, ana hat oluşturmaya veya devre dışı bırakmaya veya komşu arabirimle trunk oluşturma konusunda anlaşmaya ayarlanabilir. Trunk görüşmesi, ağ cihazları arasında yalnızca noktadan noktaya çalışan DTP tarafından yönetilir.

DTP, Catalyst 2960 ve Catalyst 3650 Serisi anahtarlarda otomatik olarak etkinleştirilen Cisco'ya özel bir protokoldür. DTP, ana hat anlaşmasını yalnızca komşu anahtardaki bağlantı noktası DTP'yi destekleyen bir ana hat modunda yapılandırılmışsa yönetir. Diğer satıcılardan gelen anahtarlar DTP'yi desteklemez.

Dikkat : Bazı ağlar arası çalışma cihazları, DTP çerçevelerini hatalı bir şekilde iletebilir ve bu da yanlış yapılandırmalara neden olabilir. Bunu önlemek için, DTP'yi desteklemeyen cihazlara bağlı Cisco anahtar arayüzlerinde DTP'yi kapatın.

Cisco Catalyst 2960 ve 3650 anahtarları için varsayılan DTP yapılandırması dynamic auto dur.

Bir Cisco anahtarından DTP'yi desteklemeyen bir cihaza trunk oluşturmayı etkinleştirmek için, **switchport mode trunk** ve **switchport nonegotiate** yapılandırma modu komutlarını kullanın. Bu, arabirimin bir ana hat olmasına neden olur, ancak DTP çerçeveleri oluşturmayacaktır.

```
S1(config-if)# switchport mode trunk
S1(config-if)# switchport nonegotiate
```

Dinamik bağlantı protokolünü yeniden etkinleştirmek için **switchport mode dynamic auto** komutunu kullanın.

```
S1(config-if)# switchport mode dynamic auto
```

İki anahtarı birbirine bağlayan bağlantı noktaları, **switchport mode trunk** ve **switchport nonegotiate** komutlarıyla tüm DTP reklamlarını yok sayacak şekilde yapılandırılırsa , bağlantı noktaları ana bağlantı noktası modunda kalacaktır. Bağlanan bağlantı noktaları dynamic auto olarak ayarlanırsa, bir ana hat üzerinde anlaşmazlar ve erişim modu durumunda kalarak etkin olmayan bir ana hat bağlantısı oluştururlar.

Bir bağlantı noktasını ana hat modunda olacak şekilde yapılandırırken, **switchport mode trunk** komutunu kullanın. O zaman trunkın hangi durumda olduğu konusunda bir belirsizlik yoktur; her zaman açıktır.

### Arayüz Anlaşma Modları

**switchport mode** komutunun ek seçenekleri vardır.
DTP anlaşmasını durdurmak için **switchport nogotiate** arayüz yapılandırma komutunu kullanın. **Show interface interface_id switchport** komutu ile kapatma doğrulanır.

| Seçenek | Açıklama |
|---|---|
| **access** | Kalıcı erişim modu ve komşu bağlantıyı bir erişim bağlantısına dönüştürmek için anlaşma yapar |
| **dynamic auto** | Komşu arabirim trunk veya desirable modda ayarlanmışsa trunk arabirimi oluşur |
| **dynamic desirable** | Aktif olarak diğer otomatik veya desirable arayüzler ile müzakere ederek bir trubk olmak ister |
| **trunk** | Kalıcı trunk modu ve komşu bağlantıyı bir trunkbağlantısına dönüştürmek için anlaşma yapar |

Licensed to yetik karasunoyr yetikrksnor@gmail.com

## DTP Yapılandırmasının Sonuçları

Tablo, Catalyst 2960 anahtar bağlantı noktalarına bağlı bir ana hat bağlantısının zıt uçlarındaki DTP yapılandırma seçeneklerinin sonuçlarını gösterir. En iyi uygulama, mümkün olduğunda ana hat bağlantılarını statik olarak yapılandırmaktır.

| | Dynamic Auto | Dynamic Desirable | Trunk | Access |
|---|---|---|---|---|
| **Dynamic Auto** | Access | Trunk | Trunk | Access |
| **Dynamic Desirable** | Trunk | Trunk | Trunk | Access |
| **Trunk** | Trunk | Trunk | Trunk | Sınırlı bağlantı |
| **Access** | Access | Access | Sınırlı bağlantı | Access |

## DTP Modunu Doğrulama

Varsayılan DTP modu, Cisco IOS Yazılım sürümüne ve platforma bağlıdır. Geçerli DTP modunu belirlemek için , çıktıda gösterildiği gibi **show dtp interface** komutunu verin.

```
S1# show dtp interface fa0/1
DTP information for FastEthernet0/1:
TOS/TAS/TNS: ACCESS/AUTO/ACCESS
TOT/TAT/TNT: NATIVE/NEGOTIATE/NATIVE
Neighbor address 1: C80084AEF101
Neighbor address 2: 000000000000
Hello timer expiration (sec/state): 11/RUNNING
Access timer expiration (sec/state): never/STOPPED
Negotiation timer expiration (sec/state): never/STOPPED
Multidrop timer expiration (sec/state): never/STOPPED
FSM state: S2:ACCESS
# times multi & trunk 0
Enabled: yes
In STP: no
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 20.Bölüm: Inter VLAN Routing

## 20.1.Inter-VLAN Yönlendirme İşlemi

### 20.1.1.Inter-VLAN Yönlendirme Nedir?

VLAN'lar anahtarlı Katman 2 ağlarını çeşitli nedenlerle bölümlere ayırmak için kullanılır. Nedeni ne olursa olsun, bir VLAN'daki ana bilgisayarlar, yönlendirme hizmetleri sağlamak için bir yönlendirici veya Katman 3 anahtarı olmadığı sürece başka bir VLAN'daki ana bilgisayarlarla iletişim kuramaz.

Inter-VLAN yönlendirme, ağ trafiğini bir VLAN'dan başka bir VLAN'a iletme işlemidir.

Üç adet VLAN arası yönlendirme seçeneği vardır:

**Legacy Inter-VLAN routing**- Bu eski bir çözüm. İyi ölçeklenmez.

**Router-on-a-Stick**-Bu, küçük ve orta ölçekli ağlar için kabul edilebilir bir çözümdür.

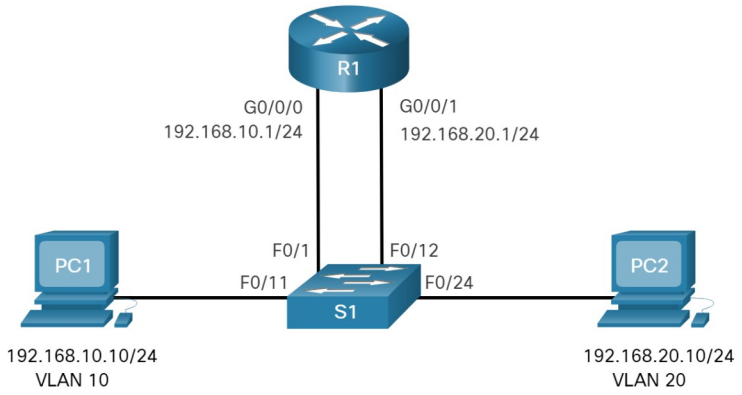
**Layer 3 switch using switched virtual interfaces (SVIs)**- Bu, orta ve büyük ölçekli kuruluşlar için en ölçeklenebilir çözümdür.

### Eski VLANlar Arası Yönlendirme

İlk VLAN arası yönlendirme çözümü, birden fazla Ethernet arabirimine sahip bir yönlendirici kullanmaya dayanıyordu. Her yönlendirici arabirimi farklı VLAN'lardaki bir anahtar bağlantı noktasına bağlanmıştır. Yönlendirici arabirimleri, VLAN alt ağındaki yerel ana bilgisayarlara varsayılan ağ geçidi olarak işlev görür.

Fiziksel arayüzler kullanan eski VLAN arası yönlendirme çalışır, ancak önemli bir sınırlaması vardır. Yönlendiricilerin sınırlı sayıda fiziksel arabirimi olduğundan makul ölçüde ölçeklendirilemez. VLAN başına bir fiziksel yönlendirici arabirimi gerektirmesi, yönlendiricinin fiziksel arabirim kapasitesini hızla tüketir.

Not: Bu VLAN arası yönlendirme yöntemi artık anahtarlamalı ağlarda uygulanmaz ve yalnızca açıklama amaçlıdır.




### Router-on-a-Stick Inter-VLAN Routing(RoaS)

router-on-a-stick ’VLAN arası yönlendirme yöntemi, eski VLAN arası yönlendirme yönteminin sınırlamasının üstesinden gelir. Bir ağdaki birden çok VLAN arasındaki trafiği yönlendirmek için yalnızca bir fiziksel Ethernet arabirimi gerekir.

Video serisi ayrıntılarına ulaşmak için tarayınız

Cisco IOS yönlendirici Ethernet arabirimi, 802.1Q devre olarak yapılandırılır ve Katman 2 anahtarındaki bir devre bağlantı noktasına bağlanır. Özellikle, yönlendirici arabirimi yönlendirilebilir VLAN'ları tanımlamak için alt arabirimler kullanılarak yapılandırılır.

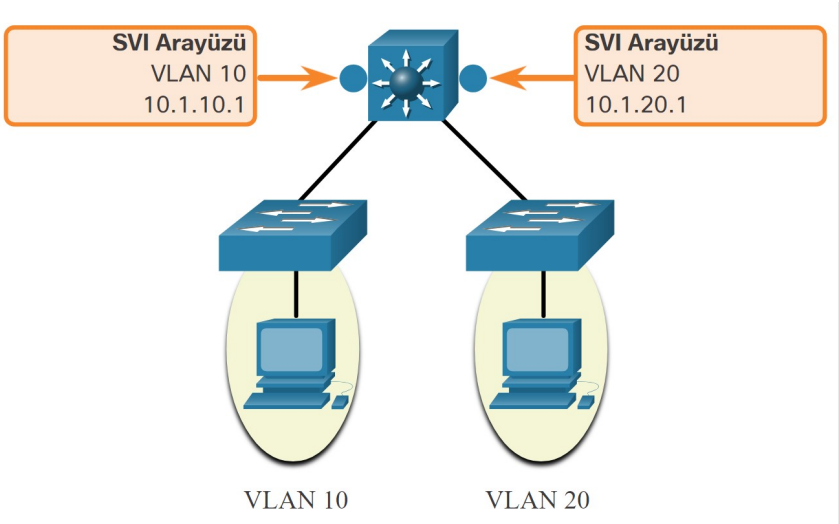
Yapılandırılan alt arabirimler, yazılım tabanlı sanal arabirimlerdir. Her biri tek bir fiziksel Ethernet arabirimiyle ilişkilidir. Alt arabirimler bir yönlendiricideki yazılımda yapılandırılır. Her alt arabirim bağımsız olarak bir IP adresi ve VLAN ataması ile yapılandırılır. Alt arabirimler, VLAN atamalarına karşılık gelen farklı alt ağlar için yapılandırılır. Bu mantıksal yönlendirmeyi kolaylaştırır.

VLAN etiketli trafik yönlendirici arayüzüne girdiğinde, VLAN alt arayüzüne iletilir. Hedef IP ağ adresine göre bir yönlendirme kararı verildikten sonra, yönlendirici trafik için çıkış arayüzünü belirler. Çıkış arabirimi 802.1q alt arabirimi olarak yapılandırılmışsa, veri çerçeveleri yeni VLAN ile VLAN etiketlenir ve fiziksel arabirimi geri gönderir

**Not: router-on-a-stick yöntemi 50 VLAN'ın ötesine geçmez.**

## Katman 3 Anahtarında Inter-VLAN Yönlendirme

VLAN arası yönlendirme gerçekleştirmenin modern yöntemi, Katman 3 anahtarları ve anahtarlı sanal arabirimler (SVI) kullanmaktır. SVI, şekilde gösterildiği gibi Katman 3 anahtarı üzerinde yapılandırılan sanal bir arabirimdir.




Not : Katman 3 anahtarı(Layer 3 switch ), Katman 2 ve Katman 3'te çalıştığı için çok katmanlı anahtar (multilayer switch ) olarak da adlandırılır. Ancak, bu kursta Katman 3 anahtarı terimini kullanıyoruz.

Inter-VLAN SVI'lar, yönetim VLAN arayüzünün yapılandırıldığı şekilde oluşturulur. SVI, anahtarda bulunan bir VLAN için oluşturulur. Sanal olmasına rağmen, SVI, VLAN için bir yönlendirici arayüzünün yapacağı aynı işlevleri gerçekleştirir. Spesifik olarak, söz konusu VLAN ile ilişkili tüm anahtar bağlantı noktalarına veya bu bağlantı noktalarından gönderilen paketler için Katman 3 işleme sağlar.

Aşağıdakiler, VLAN arası yönlendirme için Katman 3 anahtarları kullanmanın avantajlarıdır:

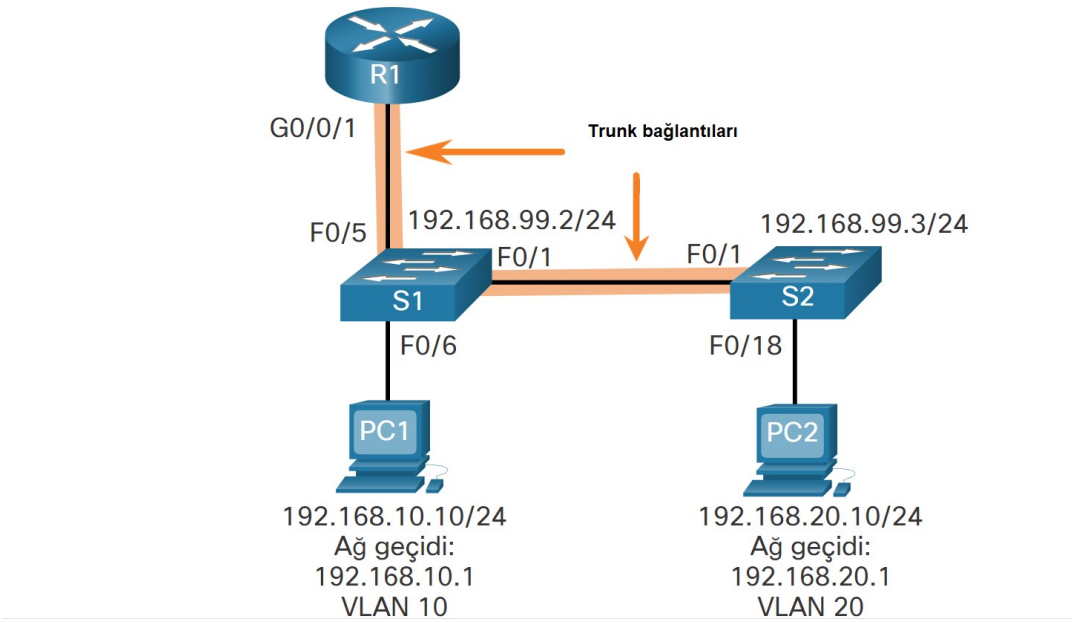
- Her şey donanım anahtarlamalı ve yönlendirilmiş olduğundan, çubuk üzerindeki yönlendiriciden çok daha hızlıdırlar.
- Yönlendirme için anahtardan yönlendiriciye harici bağlantılara gerek yoktur.
- Katman 2 EtherChannels, bant genişliğini artırmak için anahtarlar arasında ana hat bağlantıları olarak kullanılabildiğinden tek bir bağlantıyla sınırlı değildir.
- Gecikme çok daha düşüktür, çünkü verilerin farklı bir ağa yönlendirilmesi için anahtardan çıkması gerekmez.
- Yönlendiricilerden daha yaygın olarak bir kampüs LAN'ında konuşlandırılırlar.

Licensed to yetkin kansungur, yetkinksngr@gmail.com

Tek dezavantaj, Katman 3 anahtarlarının daha pahalı olmasıdır.

## 20.2. RoaS Yapılandırması

### 20.2.1 Örnek Topoloji




Şekilde, R1 GigabitEthernet 0/0/1 arabirimi S1 FastEthernet 0/5 bağlantı noktasına bağlanmıştır. S1 FastEthernet 0/1 bağlantı noktası S2 FastEthernet 0/1 bağlantı noktasına bağlanır. Bunlar, VLAN'lar içinde ve arasındaki trafiği iletmek için gerekli olan devre-trunk bağlantılarıdır.
VLAN'lar arasında geçiş yapmak için, R1 GigabitEthernet 0/0/1 arayüzü tabloda gösterildiği gibi mantıksal olarak üç alt arayüze ayrılmıştır. Tablo ayrıca anahtarlarda yapılandırılacak üç VLAN'ı gösterir.
R1, S1 ve S2'nin başlangıçtaki temel yapılandırmalara sahip olduğunu varsayın. Şu anda, PC1 ve PC2 ayrı ağlarda oldukları için birbirlerine ping atamazlar. Sadece S1 ve S2 birbirlerine ping atabilir, ancak PC1 veya PC2 tarafından erişilemezler, çünkü aynı zamanda farklı ağlardalar.
Aygıtların birbirlerine ping atmasını sağlamak için, anahtarların VLAN'lar ve trunklarla yapılandırılması ve yönlendiricinin VLAN arası yönlendirme için yapılandırılması gerekir.

S1'i VLAN'larla ve trunklarla yapılandırmak için aşağıdaki adımları tamamlayın:

Adım 1. VLAN'ları oluşturun ve adlandırın.

Adım 2. Her VLAN için yönetim arayüzünü (SVI) oluşturun.

Adım 3. Erişim bağlantı noktalarını yapılandırın.

Adım 4. Trunk bağlantı noktalarını yapılandırın.

**1 . VLAN'ları oluşturun ve adlandırın.**

İlk olarak, VLAN'lar oluşturulur ve adlandırılır. VLAN'lar yalnızca VLAN alt yapılandırma modundan çıktıktan sonra oluşturulur.

```
S1(config)# vlan 10
S1(config-vlan)# name LAN10
S1(config-vlan)# exit
S1(config)# vlan 20
S1(config-vlan)# name LAN20
S1(config-vlan)# exit
S1(config)# vlan 99
S1(config-vlan)# name Management
S1(config-vlan)# exit
S1(config)#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**2 . Yönetim arayüzünü oluşturun.**

Daha sonra, R1'in varsayılan ağ geçidi ile birlikte VLAN 99'da yönetim arayüzü oluşturulur.

```
S1(config)# interface vlan 99
S1(config-if)# ip add 192.168.99.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# ip default-gateway 192.168.99.1
S1(config)#
```

**3 . Erişim bağlantı noktalarını yapılandırın.**

Daha sonra, PC1'e bağlanan Fa0 / 6 portu, VLAN 10'da bir erişim portu olarak konfigüre edilir. PC1'in doğru IP adresi ve varsayılan ağ geçidi ile yapılandırıldığını varsayın.

```
S1(config)# interface fa0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

**4 . Trunk bağlantı noktalarını yapılandırın.**

Son olarak, S2'ye bağlanan Fa0 / 1 ve R1'e bağlanan Fa05 bağlantı noktaları, ana hat bağlantı noktaları olarak yapılandırılır.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# exit
S1(config)# interface fa0/5
S1(config-if)# switchport mode trunk
S1(config-if)# no shut
S1(config-if)# end
*Mar  1 00:23:43.093: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
*Mar  1 00:23:44.511: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to
up
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### S2 VLAN ve Trunking Yapılandırması

S2 için konfigürasyon S1'e benzer.

```
S2(config)# vlan 10
S2(config-vlan)# name LAN10
S2(config-vlan)# exit
S2(config)# vlan 20
S2(config-vlan)# name LAN20
S2(config-vlan)# exit
S2(config)# vlan 99
S2(config-vlan)# name Management
S2(config-vlan)# exit
S2(config)#
S2(config)# interface vlan 99
S2(config-if)# ip add 192.168.99.3 255.255.255.0
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# ip default-gateway 192.168.99.1
S2(config)# interface fa0/18
S2(config-if)# switchport mode access
S2(config-if)# switchport access vlan 20
S2(config-if)# no shut
S2(config-if)# exit
S2(config)# interface fa0/1
S2(config-if)# switchport mode trunk
S2(config-if)# no shut
S2(config-if)# exit
S2(config-if)# end
*Mar  1 00:23:52.137: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
```

## R1 Alt Arayüz (Sub İnterface)Yapılandırması

RoaS yönlendirici yöntemi, yönlendirilecek her VLAN için bir alt arabirim-subinterface oluşturmanızı gerektirir. İnterface_id subinterface_id genel yapılandırma modu komutu kullanılarak bir alt arabirim oluşturulur. Alt arabirim sözdizimi, fiziksel arabirimdir, bunu bir nokta ve bir alt arabirim numarası izler. Gerekli olmasa da, alt arayüz numarasının VLAN numarası ile eşleştirilmesi gelenekseldir.
Daha sonra her bir alt arayüz aşağıdaki iki komutla yapılandırılır:
encapsulation dot1q vlan_id [native] - Bu komut, alt arayüzü belirtilen vlan-id'den 802.1Q kapsüllenmiş trafiğe yanıt verecek şekilde yapılandırır. Native anahtar kelime seçeneği yalnızca yerel VLAN'ı VLAN 1 dışında bir şeye ayarlamak için eklenir.
ip address ip-address subnet-mask - Bu komut, alt arabirimin IPv4 adresini yapılandırır. Bu adres genellikle tanımlanan VLAN için varsayılan ağ geçidi görevi görür.
Yönlendirilecek her VLAN için işlemi tekrarlayın. Yönlendirmenin gerçekleşmesi için her yönlendirici alt yüzeyine benzersiz bir alt ağda bir IP adresi atanmalıdır. Tüm alt arabirimler oluşturulduğunda, no shutdown arabirimi yapılandırma komutu kullanarak fiziksel arabirimi etkinleştirin. Fiziksel arabirim devre dışı bırakılmışsa, tüm alt arabirimler devre dışı bırakılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 20.3.Katman 3 Anahtarlarını Kullanarak VLAN Arası Yönlendirme

### 20.3.1.Layer 3 Switch Inter-VLAN Yönlendirme

Modern, kurumsal ağlar, gereksinimleri karşılamak için kolayca ölçeklenemediği için nadiren RoaS yönlendirici kullanır. Bu çok büyük ağlarda, ağ yöneticileri VLAN arası yönlendirmeyi yapılandırmak için Katman 3 anahtarlarını kullanır.

RoaS yönlendirici yöntemini kullanan VLAN'lar arası yönlendirme, küçük ila orta ölçekli bir kuruluş için uygulanması kolaydır. Bununla birlikte, büyük bir kuruluş, VLAN arası yönlendirme sağlamak için daha hızlı ve çok daha ölçeklenebilir bir yöntem gerektirir.

Kurumsal kampüs LAN'ları, VLAN arası yönlendirme sağlamak için Katman 3 anahtarları kullanır. Katman 3 anahtarları, yönlendiricilerden daha yüksek paket işleme hızları elde etmek için donanım tabanlı anahtarlama kullanır. Katman 3 anahtarları, kurumsal dağıtım katmanı kablolama dolaplarında da yaygın olarak uygulanır.

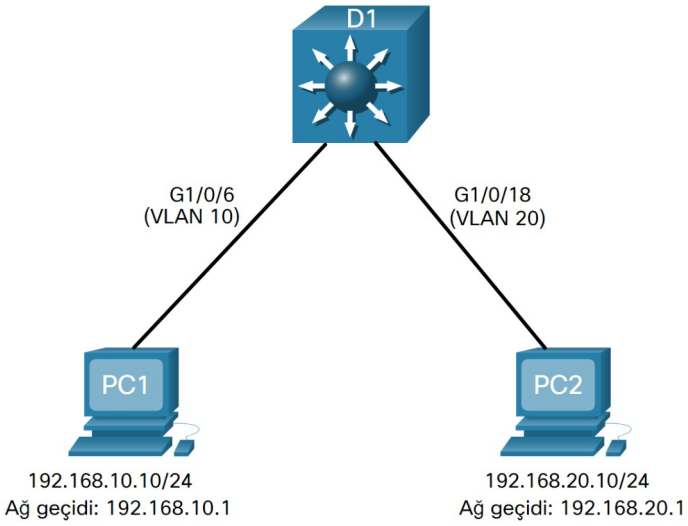
Katman 3 anahtarının yetenekleri şunları içerir:

- Birden çok anahtarlamalı sanal arabirim (SVI) kullanarak bir VLAN'dan diğerine yönlendirin.
- Katman 2 anahtar portunu Katman 3 arayüzüne (yani yönlendirilmiş bir porta) dönüştürün. Yönlendirilmiş bir bağlantı noktası, bir Cisco IOS yönlendiricisindeki fiziksel bir arabirime benzer.

VLAN arası yönlendirme sağlamak için Katman 3 anahtarları SVI'leri kullanır. SVI'lar, bir Katman 2 anahtarında yönetim SVI'sini oluşturmak için kullanılan aynı **interface vlan** *vlan-id* komutu kullanılarak yapılandırılır . Yönlendirilebilir VLAN'ların her biri için bir Katman 3 SVI oluşturulmalıdır.

### 20.3.2.Örnek Topoloji

Şekilde, Katman 3 anahtarı D1, farklı VLAN'lardaki iki ana bilgisayara bağlıdır. PC1, VLAN 10'da ve PC2, VLAN 20'de gösterildiği gibi. Katman 3 anahtarı, iki ana bilgisayara VLAN arası yönlendirme hizmetleri sağlayacaktır.




D1 VLAN IP Adresleri

| VLAN Arayüzü | IP adresi |
|---|---|
| 10 | 192.168.10.1/24 |
| 20 | 192.168.20.1/24 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Katman 3 Anahtar Yapılandırması

S1'i VLAN'lar ve trunking ile yapılandırmak için aşağıdaki adımları tamamlayın:

1. Adım . VLAN'ları oluşturun.

2. Adım . SVI VLAN arayüzlerini oluşturun.

3. Adım . Erişim bağlantı noktalarını yapılandırın.

4. adım . IP yönlendirmeyi etkinleştirin.

### 1 . VLAN'ları oluşturun.

İlk olarak, çıktıda gösterildiği gibi iki VLAN oluşturun.

```
D1(config)# vlan 10
D1(config-vlan)# name LAN10
D1(config-vlan)# vlan 20
D1(config-vlan)# name LAN20
D1(config-vlan)# exit
D1(config)#
```

### 2 . SVI VLAN arayüzlerini oluşturun.

VLAN'lar 10 ve 20 için SVI'yı yapılandırın. Yapılandırılan IP adresleri, ilgili VLAN'lardaki ana bilgisayarlara varsayılan ağ geçitleri olarak hizmet edecektir. Her iki SVI'da hat protokolünü gösteren bilgi mesajlarının yukarı doğru değiştiğine dikkat edin.

```
D1(config)# interface vlan 10
D1(config-if)# description Default Gateway SVI for 192.168.10.0/24
D1(config-if)# ip add 192.168.10.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
D1(config)# int vlan 20
D1(config-if)# description Default Gateway SVI for 192.168.20.0/24
D1(config-if)# ip add 192.168.20.1 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
*Sep 17 13:52:16.053: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
*Sep 17 13:52:16.160: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up
```

### 3 . Erişim bağlantı noktalarını yapılandırın.

Ardından, ana bilgisayarlara bağlanan erişim bağlantı noktalarını yapılandırın ve bunları ilgili VLAN'larına atayın.

```
D1(config)# interface GigabitEthernet1/0/6
D1(config-if)# description Access port to PC1
D1(config-if)# switchport mode access
D1(config-if)# switchport access vlan 10
D1(config-if)# exit
D1(config)#
D1(config)# interface GigabitEthernet1/0/18
D1(config-if)# description Access port to PC2
D1(config-if)# switchport mode access
D1(config-if)# switchport access vlan 20
D1(config-if)# exit
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**4 . IP yönlendirmeyi etkinleştirin.**

Son olarak, trafiğin VLAN'lar 10 ve 20 arasında değiş tokuş edilmesini sağlamak için **ip routing** genel yapılandırma komutuyla IPv4 yönlendirmesini etkinleştirin . Bu komut, IPv4 için bir Katman 3 anahtarında VANlar arası yönlendirmeyi etkinleştirmek üzere yapılandırılmalıdır.

```
D1(config)# ip routing
D1(config)#
```

## Layer 3 Switch Inter-VLAN Yönlendirme Doğrulaması

Katman 3 anahtarı kullanan VLAN'lar arası yönlendirme, çubuk üzerinde yönlendirici yönteminden daha basit yapılandırılır. Yapılandırma tamamlandıktan sonra, ana bilgisayarlar arasındaki bağlantı test edilerek yapılandırma doğrulanabilir.

Bir ana bilgisayardan, ping komutunu kullanarak başka bir VLAN'daki bir ana bilgisayara olan bağlantıyı doğrulayın . İlk olarak ipconfig Windows host komutunu kullanarak mevcut ana bilgisayar IP yapılandırmasını doğrulamak iyi bir fikirdir . Çıktı, IPv4 adresini ve PC1'in varsayılan ağ geçidini doğrular.

```
C:\Users\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
  Connection-specific DNS Suffix . :
  Link-local IPv6 Address          : fe80::5c43:ee7c:2959:da68%6
  IPv4 Address                     : 192.168.10.10
  Subnet Mask                      : 255.255.255.0
  Default Gateway                  : 192.168.10.1
C:\Users\PC1>
```

Ardından, çıktıda gösterildiği gibi ping Windows ana bilgisayar komutunu kullanarak PC2 ile bağlantıyı doğrulayın . Ping çıkışı başarılıysa VLANlar arası yönlendirme operasyonunu onaylar.

```
C:\Users\PC1> ping 192.168.20.10
Pinging 192.168.20.10 with 32 bytes of data:
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Reply from 192.168.20.10: bytes=32 time<1ms TTL=127
Ping statistics for 192.168.20.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\PC1>
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 20.4.Katman 3 Anahtarında Yönlendirme

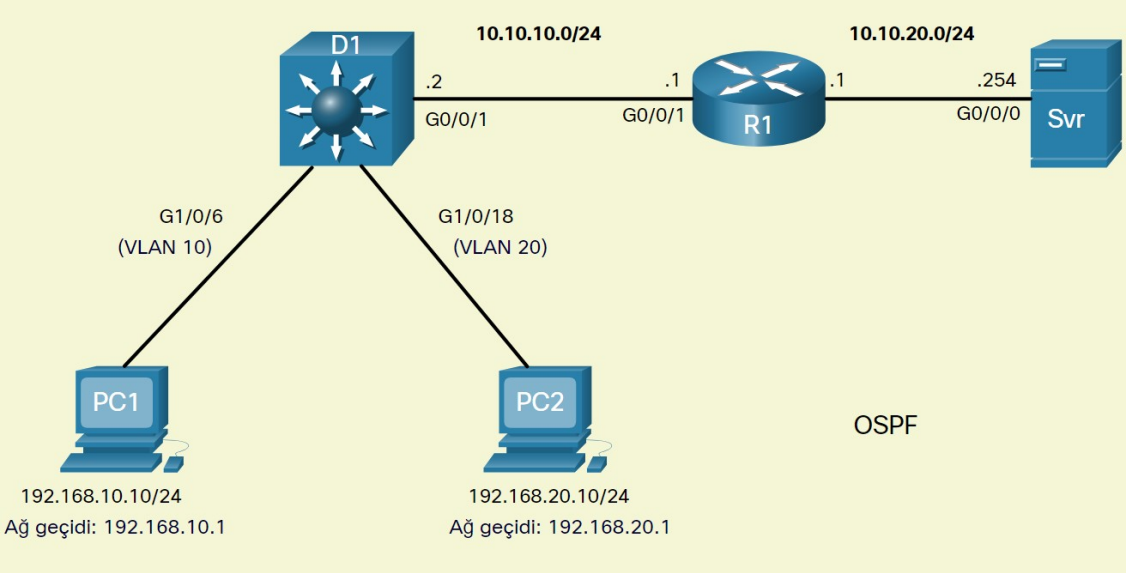
VLAN'lara diğer Katman 3 cihazları tarafından erişilebilecekse, bunlar statik veya dinamik yönlendirme kullanılarak tanıtılmalıdır. Bir Katman 3 anahtarında yönlendirmeyi etkinleştirmek için, yönlendirilmiş bir bağlantı noktası yapılandırılmalıdır.

Katman 3 anahtarında, başka bir Katman 3 cihazına bağlı Katman 2 bağlantı noktasındaki anahtar bağlantı noktası özelliği devre dışı bırakılarak yönlendirilmiş bir bağlantı noktası oluşturulur. Özellikle, bir Katman 2 bağlantı noktasında anahtar bağlantı noktası olmayan arabirim yapılandırma komutunu yapılandırmak, bunu Katman 3 arabirimine dönüştürür. Daha sonra arayüz, bir yönlendiriciye veya başka bir Katman 3 anahtarına bağlanmak için bir IPv4 yapılandırmasıyla yapılandırılabilir.

### 20.4.1.Örnek Topoloji

Şekilde, önceden yapılandırılmış D1 Katman 3 anahtarı artık R1'e bağlanmıştır. R1 ve D1, OSPF yönlendirme protokolü etki alanı içindedir. Inter-VLAN'ın D1'de başarıyla uygulandığını varsayın. R1'in G0 / 0/1 arayüzü de yapılandırılmış ve etkinleştirilmiştir. Ek olarak, R1, iki ağını (10.10.10.0/24 ve 10.20.20.0/24) tanıtmak için OSPF kullanıyor.

Not : OSPF yönlendirme yapılandırması başka bir kursta ele alınmıştır. Bu modülde, OSPF yapılandırma komutları size tüm etkinliklerde ve değerlendirmelerde verilecektir. Katman 3 anahtarında OSPF yönlendirmesini etkinleştirmek için yapılandırmayı anlamanız gerekmez.




#### Katman 3 Anahtarında Yönlendirme Yapılandırması

D1'i R1 ile yönlendirmek üzere yapılandırmak için aşağıdaki adımları tamamlayın:

1. Adım . Yönlendirilen bağlantı noktasını yapılandırın.

2. Adım . Yönlendirmeyi etkinleştirin.

3. Adım . Yönlendirmeyi yapılandırın.

4. adım . Yönlendirmeyi doğrulayın.

5. Adım . Bağlantıyı doğrulayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 1 . Yönlendirilen (routed) bağlantı noktasını yapılandırın.

G1 / 0 / 1'i yönlendirilmiş bir bağlantı noktası olacak şekilde yapılandırın, ona bir IPv4 adresi atayın ve etkinleştirin.

```
D1(config)# interface GigabitEthernet1/0/1
D1(config-if)# description routed Port Link to R1
D1(config-if)# no switchport
D1(config-if)# ip address 10.10.10.2 255.255.255.0
D1(config-if)# no shut
D1(config-if)# exit
D1(config)#
```

### 2 . Yönlendirmeyi etkinleştirin.

IPv4 yönlendirmesinin **ip routing** genel yapılandırma komutuyla etkinleştirildiğinden emin olun .

```
D1(config)# ip routing
D1(config)#
```

### 3 . Yönlendirmeyi yapılandırın.

OSPF yönlendirme protokolünü, R1'e bağlı ağ ile birlikte VLAN 10 ve VLAN 20 ağlarını tanıtmak için yapılandırın. R1 ile bir bitişiklik kurulduğunu bildiren mesaja dikkat edin.

```
D1(config)# router ospf 10
D1(config-router)# network 192.168.10.0 0.0.0.255 area 0
D1(config-router)# network 192.168.20.0 0.0.0.255 area 0
D1(config-router)# network 10.10.10.0 0.0.0.3 area 0
D1(config-router)# ^Z
D1#
*Sep 17 13:52:51.163: %OSPF-5-ADJCHG: Process 10, Nbr 10.20.20.1 on GigabitEthernet1/0/1 from LOADING to
FULL, Loading Done
D1#
```

### 4 . Yönlendirmeyi doğrulayın.

D1'deki yönlendirme tablosunu doğrulayın. D1'in artık 10.20.20.0/24 ağına bir rotası olduğuna dikkat edin.

```
D1# show ip route | begin Gateway
Gateway of last resort is not set
      10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
C        10.10.10.0/30 is directly connected, GigabitEthernet1/0/1
L        10.10.10.2/32 is directly connected, GigabitEthernet1/0/1
O        10.10.20.0/24 [110/2] via 10.10.10.1, 00:00:06, GigabitEthernet1/0/1
      192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.10.0/24 is directly connected, Vlan10
L        192.168.10.1/32 is directly connected, Vlan10
      192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.20.0/24 is directly connected, Vlan20
L        192.168.20.1/32 is directly connected, Vlan20
D1#
```

### 5 . Bağlantıyı doğrulayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

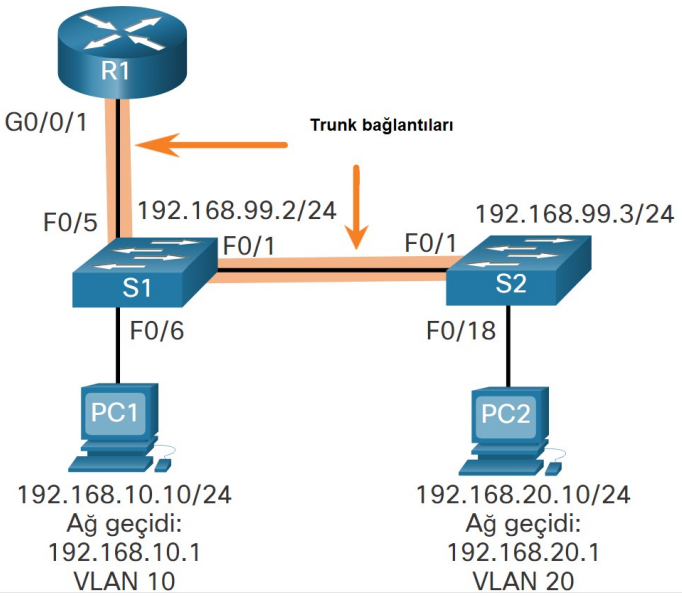
Şu anda, PC1 ve PC2, R1'e bağlı sunucuya ping atabilir.

## 20.5.Inter Vlan Yönlendirme Sorunlarını Giderme

VLAN'lar arası bir yapılandırmanın çalışmayabilmesinin birkaç nedeni vardır. Hepsi bağlantı sorunları ile ilgilidir. İlk olarak, bir kablonun yanlış bağlantı noktasına bağlanabileceği sorunları çözmek için fiziksel katmanı kontrol edin. Bağlantılar doğruysa, VLAN arası bağlantının başarısız olmasının diğer yaygın nedenleri için tablodaki listeyi kullanın.

| Sorun Tipi | Nasıl Düzeltilir | Nasıl Doğrulanır |
|---|---|---|
| Missing VLANs<br>Eksik VLAN'lar | • Varsa VLAN'ı oluşturun (veya yeniden oluşturun).<br>• Ana makine bağlantı noktasının doğru VLAN'a atandığından emin olun. | **show vlan [brief]**<br>**show interfaces switchport**<br>**ping** |
| Switch Trunk Port Issues<br>Anahtar Bağlantı Noktası Sorunları | • Trunkların doğru yapılandırıldığından emin olun.<br>• Bağlantı noktasının bir trunk bağlantı noktası olduğundan ve etkinleştirildiğinden emin olun. | **show interface trunk**<br>**show running-config** |
| Switch Access Port Issues<br>Erişim Bağlantı Noktası Sorunlarını Değiştirme | • Erişim portuna doğru VLAN'ı atayın.<br>• Bağlantı noktasının bir erişim bağlantı noktası olduğundan ve etkinleştirildiğinden emin olun.<br>• Ana makine yanlış alt ağda yanlış yapılandırılmış. | **show interfaces switchport**<br>**show running-config interface**<br>**ipconfig** |
| Router Configuration Issues<br>Yönlendirici Yapılandırma Sorunları | • Yönlendirici alt arayüzü IPv4 adresi yanlış yapılandırılmış.<br>• Yönlendirici alt arayüzü VLAN ID'sine atanmıştır. | **show ip interface brief**<br>**show interfaces** |

### 20.5.1.Örnek Topoloji




| Router R1 Subinterfaces | | |
|---|---|---|
| **Subinterface** | **VLAN** | **IP Address** |
| G0/0/0.10 | 10 | 192.168.10.1/24 |
| G0/0/0.20 | 20 | 192.168.20.1/24 |
| G0/0/0.30 | 99 | 192.168.99.1/24 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Eksik VLAN'lar

VLAN'lar arası bağlantı sorunu, eksik bir VLAN'dan kaynaklanıyor olabilir. VLAN oluşturulmamışsa, yanlışlıkla silinmişse veya ana hat bağlantısında izin verilmiyorsa eksik olabilir.

Örneğin, PC1, **show vlan brief** komut çıktısında gösterildiği gibi şu anda VLAN 10'a bağlıdır .

```
S1# show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
10   LAN10                            active    Fa0/6
20   LAN20                            active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1#
```

Şimdi, aşağıdaki çıktıda gösterildiği gibi, VLAN 10'un yanlışlıkla silindiğini varsayın.

```
S1(config)# no vlan 10
S1(config)# do show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
20   LAN20                            active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1(config)#
```

VLAN 10'un artık çıktıda eksik olduğuna dikkat edin. Ayrıca Fa0 / 6 bağlantı noktasının varsayılan VLAN'a yeniden atanmadığına dikkat edin. Bunun nedeni, bir VLAN'ı sildiğinizde, bu VLAN'a atanan bağlantı noktalarının devre dışı kalmasıdır. Siz onları yeni bir VLAN'a atayana veya eksik VLAN'ı yeniden oluşturana kadar VLAN ile ilişkili (ve dolayısıyla devre dışı) kalırlar.

VLAN üyeliğini doğrulamak için **show interface interface-id switchport** komutunu kullanın.

```
S1(config)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Eksik VLAN'ın yeniden oluşturulması, aşağıdaki çıktıda gösterildiği gibi ana bilgisayarları otomatik olarak ona yeniden atayacaktır.

```
S1(config)# vlan 10
S1(config-vlan)# do show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
20   LAN20                            active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1(config-vlan)#
```

VLAN'ın beklendiği gibi oluşturulmadığına dikkat edin. Bunun nedeni, aşağıdaki çıktıda gösterildiği gibi, VLAN'ı oluşturmak için VLAN alt yapılandırma modundan çıkmanız gerektiğidir.

```
S1(config-vlan)# exit
S1(config)# vlan 10
S1(config)# do show vlan brief
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/2, Fa0/3, Fa0/4, Fa0/7
                                                Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                                Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                                Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                Fa0/24, Gi0/1, Gi0/2
10   VLAN0010                         active    Fa0/6
20   LAN20                            active
99   Management                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S1(config)#
```

Şimdi VLAN'ın listeye dahil edildiğine ve Fa0 / 6'ya bağlı ana bilgisayarın VLAN 10'da olduğuna dikkat edin.

## Trunk Bağlantı Noktası Sorunları

VLAN arası yönlendirme için bir başka sorun, yanlış yapılandırılmış anahtar bağlantı noktalarını içerir. Eski bir VLAN arası çözümde, bu, bağlanan yönlendirici bağlantı noktası doğru VLAN'a atanmadığında ortaya çıkabilir.

Ancak, bir RoAs yönlendirici çözümünde en yaygın neden, yanlış yapılandırılmış bir ana hat bağlantı noktasıdır.

Örneğin, PC1'in yakın zamana kadar diğer VLAN'lardaki ana bilgisayarlara bağlanabildiğini varsayalım. Bakım günlüklerine hızlı bir bakış, S1 Katman 2 anahtarına yakın zamanda rutin bakım için erişildiğini ortaya çıkardı. Bu nedenle, sorunun bu anahtarla ilgili olabileceğinden şüpheleniyorsunuz.

S1'de, R1'e bağlanan bağlantı noktasının (yani, F0 / 5) gösterildiği gibi **show interfaces trunk** komutunu kullanarak bir ana hat bağlantısı olarak doğru şekilde yapılandırıldığını doğrulayın .

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
S1# show interfaces trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
S1#
```

R1'e bağlanan Fa0 / 5 portu çıktıda gizemli bir şekilde eksik. Gösterildiği gibi show running-config interface fa0 / 5 komutunu kullanarak arayüz yapılandırmasını doğrulayın .

```
S1# show running-config interface fa0/5
Building configuration...
Current configuration : 96 bytes
!
interface FastEthernet0/5
 description Trunk link to R1
 switchport mode trunk
 shutdown
end
S1#
```

Gördüğünüz gibi, bağlantı noktası yanlışlıkla kapatıldı. Sorunu düzeltmek için, bağlantı noktasını yeniden etkinleştirin ve çıkışta gösterildiği gibi trunk durumunu doğrulayın.

```
S1(config)# interface fa0/5
S1(config-if)# no shut
S1(config-if)#
*Mar  1 04:46:44.153: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
S1(config-if)#
*Mar  1 04:46:47.962: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to
up
S1(config-if)# do show interface trunk
Port        Mode             Encapsulation  Status        Native vlan
Fa0/1       on               802.1q         trunking      1
Fa0/5       on               802.1q         trunking      1
Port        Vlans allowed on trunk
Fa0/1       1-4094
Fa0/5       1-4094
Port        Vlans allowed and active in management domain
Fa0/1       1,10,20,99
Fa0/5       1,10,20,99
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       1,10,20,99
Fa0/1       1,10,20,99
S1(config-if)#
```

Anahtarlar arası bağlantının VLAN arası yönlendirmeyi kesintiye uğratma riskini azaltmak için, yedek bağlantılar ve alternatif yollar ağ tasarımının bir parçası olmalıdır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Erişim (Access) Portu Sorunları

Anahtar erişim bağlantı noktası yapılandırmasında bir sorundan şüphelenildiğinde, yapılandırmayı incelemek ve sorunu tanımlamak için doğrulama komutlarını kullanın.

PC1'in doğru IPv4 adresine ve varsayılan ağ geçidine sahip olduğunu, ancak kendi varsayılan ağ geçidine ping atamayacağını varsayın . PC1'in bir VLAN 10 bağlantı noktasına bağlanması gerekiyor.

**show interfaces** interface-id switchport komutunu kullanarak S1'deki bağlantı noktası yapılandırmasını doğrulayın.

```
S1# show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

Fa0 / 6 bağlantı noktası, "statik access" ile belirtildiği gibi bir erişim bağlantı noktası olarak yapılandırılmıştır. Ancak, VLAN 10'da olacak şekilde yapılandırılmamış gibi görünüyor. Arayüzün yapılandırmasını doğrulayın.

```
S1# show running-config interface fa0/6
Building configuration...
Current configuration : 87 bytes
!
interface FastEthernet0/6
 description PC-A access port
 switchport mode access
end
S1#
```

Fa0 / 6 bağlantı noktasını VLAN 10'a atayın ve bağlantı noktası atamasını doğrulayın.

```
S1# configure terminal
S1(config)# interface fa0/6
S1(config-if)# switchport access vlan 10
S1(config-if)#
S1(config-if)# do show interface fa0/6 switchport
Name: Fa0/6
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (VLAN0010)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
(Output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

PC1 artık diğer VLAN'lardaki ana bilgisayarlarla iletişim kurabilir.

## Yönlendirici Yapılandırma Sorunları

RoAS yönlendirici yapılandırma sorunları genellikle alt arayüz yanlış yapılandırmalarıyla ilgilidir. Örneğin, yanlış bir IP adresi yapılandırılmış veya alt arayüze yanlış VLAN Kimliği atanmış.

Örneğin, R1, VLAN 10, 20 ve 99'daki kullanıcılar için VLAN arası yönlendirme sağlamalıdır. Ancak, VLAN 10'daki kullanıcılar başka herhangi bir VLAN'a erişemez.

Anahtar bağlantı bağlantısını doğruladınız ve her şey yolunda görünüyor. Show ip interface brief komutunu kullanarak alt arayüz durumunu doğrulayın .

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES unset  administratively down down
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
Gi0/0/1.10             192.168.10.1    YES manual up                    up
Gi0/0/1.20             192.168.20.1    YES manual up                    up
Gi0/0/1.99             192.168.99.1    YES manual up                    up
Serial0/1/0            unassigned      YES unset  administratively down down
Serial0/1/1            unassigned      YES unset  administratively down down
R1#
```

Alt arayüzlere doğru IPv4 adresleri atanmıştır ve işlevseldir.

Alt arayüzlerin her birinin hangi VLAN'larda olduğunu doğrulayın. Bunu yapmak için, show interfaces komutu kullanışlıdır, ancak çok sayıda ek gereksiz çıktı üretir. Komut çıktısı, çıktıda gösterildiği gibi IOS komut filtreleri kullanılarak azaltılabilir.

```
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  100.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  99.
R1#
```

Bazı seçilmiş anahtar sözcüklerle birlikte boru (pipe) sembolü (|), komut çıktısını filtrelemeye yardımcı olan kullanışlı bir yöntemdir. Bu örnekte, yalnızca "Gig" veya "802.1Q" harflerini içeren satırların görüntüleneceğini belirtmek için include anahtar sözcüğü kullanılmıştır. Bu arada show interface arayüz çıkışı doğal listelenen, bu filtreler kullanılarak arabirimler ve atanan bir VLAN yoğunlaştırılmış listesi üretir.

G0 / 0 / 1.10 arayüzünün VLAN 10 yerine yanlış bir şekilde VLAN 100'e atandığına dikkat edin. Bu, gösterildiği gibi R1 GigabitEthernet 0/0 / 1.10 alt arayüzünün yapılandırmasına bakılarak onaylanır.

```
R1# show running-config interface g0/0/1.10
Building configuration...
Current configuration : 146 bytes
!
interface GigabitEthernet0/0/1.10
 description Default Gateway for VLAN 10
 encapsulation dot1Q 100
 ip address 192.168.10.1 255.255.255.0
end
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bu sorunu düzeltmek için, **encapsulation dot1q 10** alt arabirim yapılandırma modu komutunu kullanarak G0 / 0 / 1.10 alt arabirimini doğru VLAN'da olacak şekilde yapılandırın.

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# interface gigabitEthernet 0/0/1.10
R1(config-subif)# encapsulation dot1Q 10
R1(config-subif)# end
R1#
R1# show interfaces | include Gig|802.1Q
GigabitEthernet0/0/0 is administratively down, line protocol is down
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  1., loopback not set
GigabitEthernet0/0/1.10 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  10.
GigabitEthernet0/0/1.20 is up, line protocol is up
  Encapsulation 802.1Q Virtual LAN, Vlan ID  20.
GigabitEthernet0/0/1.99 is up, line protocol is up
R1#
```

Alt arayüz doğru VLAN'a atandığında, bu VLAN üzerindeki cihazlar tarafından erişilebilir ve yönlendirici, VLAN arası yönlendirme gerçekleştirebilir.

Doğrulama ile yönlendirici yapılandırma sorunları hızla giderilerek, VLAN arası yönlendirmenin düzgün çalışmasına izin verilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 21.Bölüm: STP

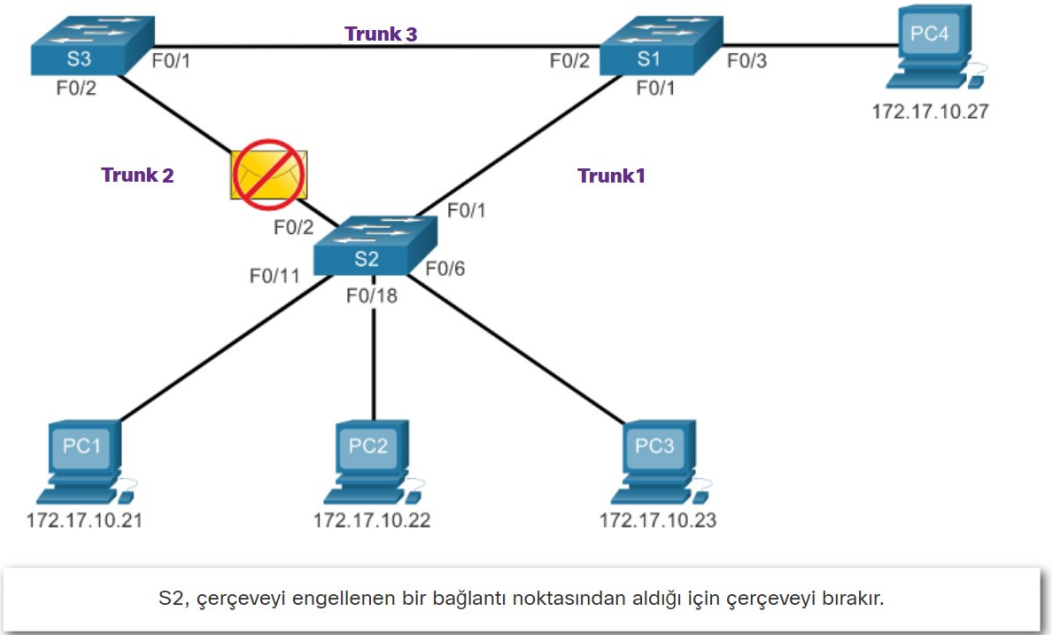
## 21.1.STP'nin Amacı

### 21.1.1.Katman 2 Ağlarda Artıklık

Bu konu, Katman 2 ağındaki döngülerin nedenlerini kapsar ve kapsayan ağaç protokolünün nasıl çalıştığını kısaca açıklar. Artıklık, tek hata noktalarını ortadan kaldırmak ve ağ hizmetlerinin bozulmasını önlemek için hiyerarşik tasarımın önemli bir parçasıdır. Yedekli ağlar fiziksel yolların eklenmesini gerektirir, ancak mantıksal yedeklilik de tasarımın bir parçası olmalıdır. Verilerin ağda geçiş yapması için alternatif fiziksel yollara sahip olmak, yol kesintisine rağmen kullanıcıların ağ kaynaklarına erişmesini mümkün kılar. Ancak, anahtarlanan bir Ethernet ağındaki yedek yollar hem fiziksel hem de mantıksal Katman 2 döngülerine neden olabilir.
Ethernet LAN'lar, herhangi iki aygıt arasında tek bir yol bulunan döngüsiz bir topoloji gerektirir. Ethernet LAN'daki bir döngü, bir bağlantı kesilene ve döngü kopana kadar Ethernet çerçevelerinin yayılmasının devam etmesine neden olabilir.

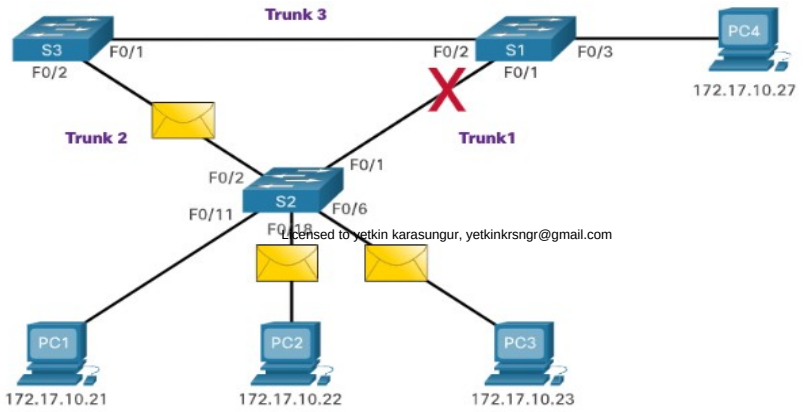
### 21.1.2.Spanning Tree Protokolü

Yayılma Ağacı Protokolü (STP), döngü içermeyen bir Katman 2 topolojisi oluştururken fazlalık sağlayan bir döngü önleme ağ protokolüdür. IEEE 802.1D, STP için orijinal IEEE MAC Köprüleme standardıdır.




### STP Yeniden Hesaplama

STP, daha önce engellenen bağlantı noktalarını yeniden hesaplayıp açarak ağdaki bir arızayı telafi eder.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Artıklı (Redundant) Anahtar Bağlantılarıyla İlgili Sorunlar

Yol yedekliliği(artıklığı-fazlalığı), tek bir arıza noktası olasılığını ortadan kaldırarak birden çok ağ hizmeti sağlar. Bir Ethernet ağındaki iki cihaz arasında birden fazla yol olduğunda ve anahtarlarda kapsayan ağaç uygulaması olmadığında, bir Katman 2 döngüsü oluşur. Katman 2 döngüsü, MAC adres tablosu kararsızlığına, bağlantı doygunluğuna ve anahtarlarda ve son cihazlarda yüksek CPU kullanımına neden olarak ağın kullanılamaz hale gelmesine neden olabilir.

Katman 3 protokollerinden, IPv4 ve IPv6'dan farklı olarak, Katman 2 Ethernet, sonsuz döngülü çerçeveleri tanıyan ve ortadan kaldıran bir mekanizma içermez. Hem IPv4 hem de IPv6, bir Katman 3 ağ cihazının bir paketi yeniden iletme sayısını sınırlayan bir mekanizma içerir. Bir yönlendirici, her IPv4 paketinde TTL'yi (Yaşam Süresi) ve her IPv6 paketinde Atlama Sınırı alanını azaltacaktır. Bu alanlar 0'a düşürüldüğünde, bir yönlendirici paketi bırakacaktır. Ethernet ve Ethernet anahtarları, bir anahtarın Katman 2 çerçevesini yeniden iletme sayısını sınırlamak için karşılaştırılabilir bir mekanizmaya sahip değildir. STP, Katman 2 Ethernet için bir döngü önleme mekanizması olarak özel olarak geliştirilmiştir.

## Katman 2 Döngüler(loops)

STP etkinleştirilmeden, Katman 2 döngüleri oluşarak yayın, çok noktaya yayın ve bilinmeyen tek noktaya yayın çerçevelerinin sonsuz döngüye girmesine neden olabilir. Bu, bir ağı çok kısa bir süre içinde, bazen sadece birkaç saniye içinde kapatabilir. Örneğin, bir ARP İsteği gibi yayın çerçeveleri, orijinal giriş bağlantı noktası dışında tüm anahtar bağlantı noktalarına iletilir. Bu, bir yayın alanındaki tüm cihazların çerçeveyi alabilmesini sağlar. Çerçevenin dışarı iletileceği birden fazla yol varsa, sonsuz bir döngü ortaya çıkabilir. Bir döngü oluştuğunda, bir anahtardaki MAC adres tablosu, yayın çerçevelerinden gelen güncellemelerle sürekli olarak değişecek ve bu da MAC veritabanı kararsızlığına neden olacaktır. Bu, yüksek CPU kullanımına neden olabilir ve bu da anahtarın çerçeveleri iletememesine neden olur.

Döngülerden etkilenen tek çerçeve türü yayın çerçeveleri değildir. Döngülü bir ağa gönderilen bilinmeyen tek noktaya yayın çerçeveleri, hedef cihaza yinelenen çerçevelerin ulaşmasına neden olabilir. Bilinmeyen bir tek noktaya yayın çerçevesi, anahtarın MAC adres tablosunda hedef MAC adresine sahip olmaması ve çerçeveyi giriş bağlantı noktası hariç tüm bağlantı noktalarını dışarı iletmesi gerektiğidir.

## Yayın Fırtınası (Broadcast Storm)

Bir yayın fırtınası, belirli bir süre boyunca ağı ezip geçen, anormal derecede yüksek sayıda yayındır. Yayın fırtınaları, anahtarları ve uç cihazları ezici bir şekilde birkaç saniye içinde devre dışı bırakabilir. Yayın fırtınalarına, hatalı bir NIC gibi bir donanım sorunu veya ağdaki bir Katman 2 döngüsü neden olabilir.

ARP İstekleri gibi bir ağda Katman 2 yayınları çok yaygındır. Katman 2 döngüsünün ağ üzerinde hemen ve devre dışı bırakan sonuçları olması muhtemeldir. Katman 2 çok noktaya yayın, genellikle anahtar tarafından bir yayınla aynı şekilde iletilir. Dolayısıyla, IPv6 paketleri hiçbir zaman Katman 2 yayını olarak iletilmese de, ICMPv6 Komşu Keşfi Katman 2 çoklu yayınlarını kullanır.

Katman 2 döngüsüne yakalanan bir ana bilgisayara ağdaki diğer ana bilgisayarlar erişilemez. Ek olarak, MAC adres tablosundaki sürekli değişiklikler nedeniyle, anahtar tek noktaya yayın çerçevelerini hangi bağlantı noktasından ileteceğini bilemez. Önceki animasyonda, anahtarlar PC1 için listelenen yanlış bağlantı noktalarına sahip olacaktır. PC1 için hedeflenen bilinmeyen tek noktaya yayın çerçevesi, tıpkı yayın çerçevelerinde olduğu gibi ağın etrafında döngüler oluşturur. Ağ etrafında döngü yapan daha fazla çerçeve, sonunda bir yayın fırtınası yaratır.

Bu sorunların yedekli bir ağda ortaya çıkmasını önlemek için, anahtarlarda bir tür kapsayan ağaçların etkinleştirilmesi gerekir. Katman 2 döngülerinin oluşmasını önlemek için Cisco anahtarlarında yayılma ağacı (STP) varsayılan olarak **etkindir.**

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 21.2.Spanning Tree Algoritması

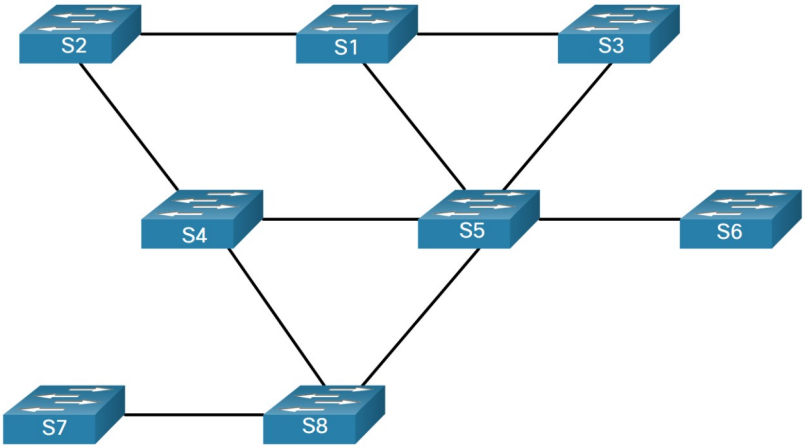
STP, o yıllarda Digital Equipment Corporation'da çalışan Radia Perlman tarafından icat edilen ve 1985 tarihli "Genişletilmiş Bir Ağda Yayılan Ağacın Dağıtılmış Hesaplaması için Algoritma"- "An Algorithm for Distributed Computation of a Spanning Tree in an Extended LAN." başlıklı makalesinde yayınlanan bir algoritmaya dayanmaktadır. Genişleyen ağaç algoritması (STA), diğer tüm anahtarların tek bir en düşük maliyetli yolu belirlediği tek bir kök köprüyü seçerek döngüsüz bir topoloji oluşturur.

Döngü önleme protokolü olmadan, döngüler meydana gelir ve yedekli bir anahtar ağını çalışmaz hale getirir.

STA tarafından döngü nasıl önlenir adım adım görelim.

### STA Senaryo Topolojisi

Bu STA senaryosu, birden çok anahtar arasında yedekli bağlantılara sahip bir Ethernet LAN kullanır.

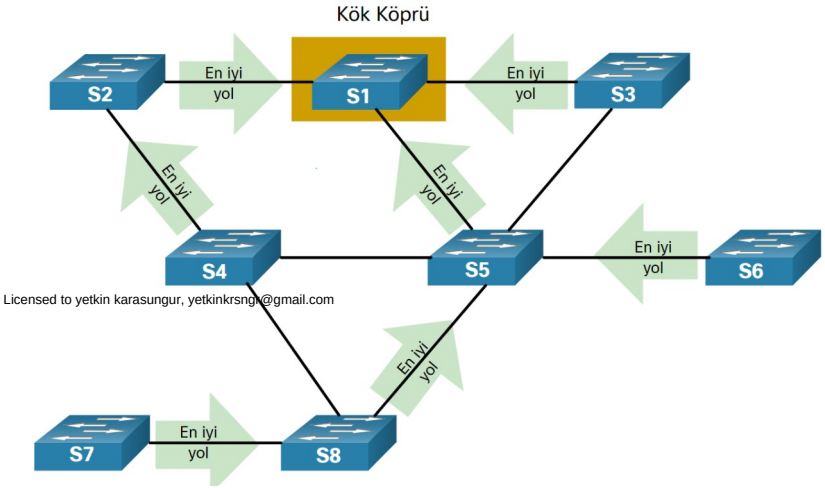



STP, stratejik olarak yerleştirilmiş "engelleme durumu" bağlantı noktalarını kullanarak ağ üzerinden döngü içermeyen bir yol yapılandırarak döngülerin oluşmasını önler. STP'yi çalıştıran anahtarlar, önceden engellenen bağlantı noktalarının engelini dinamik olarak kaldırarak ve trafiğin alternatif yolları geçmesine izin vererek hataları telafi edebilir.

### Kök Köprüyü seçin

Kapsayan ağaç algoritması, tek bir kök köprü (root bridge) seçilerek başlar. Şekil, S1 anahtarının temel köprü olarak seçildiğini göstermektedir. Bu topolojide, tüm bağlantılar eşit maliyetlidir (aynı bant genişliği). Her anahtar, kendisinden kök köprüye tek ve en düşük maliyetli bir yol belirleyecektir.

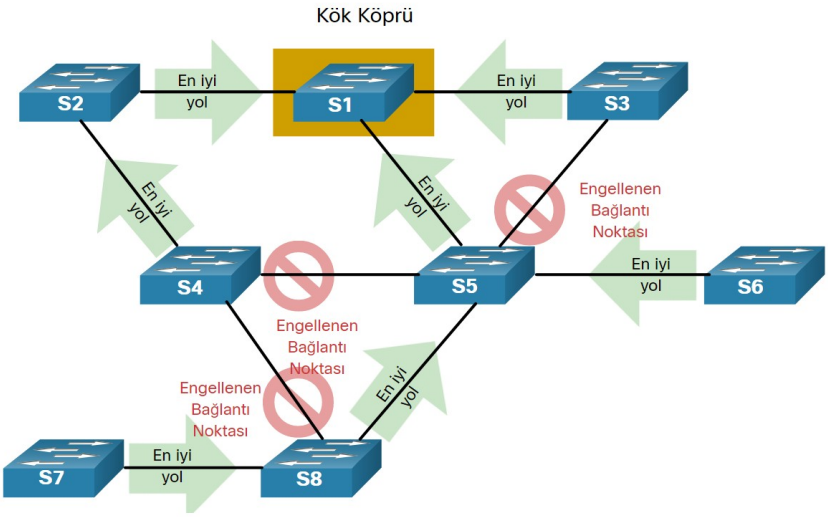
Not : STA ve STP, anahtarları köprüler olarak ifade eder. Bunun nedeni, Ethernet'in ilk günlerinde anahtarlara köprü olarak atıfta bulunulmasıdır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Gereksiz Yolları Engelle

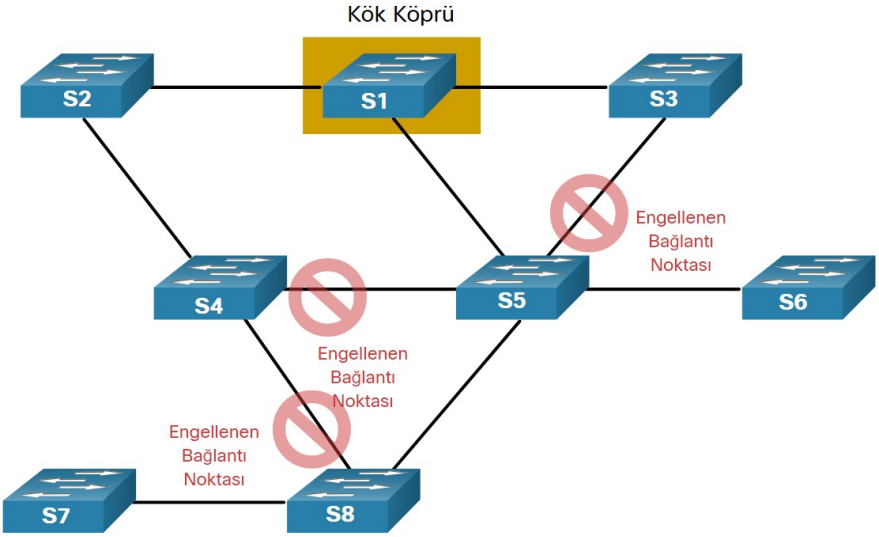
STP, şekilde gösterildiği gibi bir döngüye neden olabilecek yedekli yolları kasıtlı olarak bloke ederek ağdaki tüm hedefler arasında yalnızca bir mantıksal yol olmasını sağlar. Bir bağlantı noktası engellendiğinde, kullanıcı verilerinin bu bağlantı noktasına girmesi veya çıkması engellenir. Yedekli yolların engellenmesi, ağdaki döngüleri önlemek açısından kritik önem taşır.




S4, S5 ve S8 anahtarları, kök köprüye giden yedekli yolları engelledi.

## Döngüsüz Topoloji

Engellenen bir bağlantı noktası, şekilde gösterildiği gibi, bu bağlantıyı iki anahtar arasında iletmeyen bir bağlantı haline getirme etkisine sahiptir. Bunun, ağacın köküne bağlanan bir ağaçtaki dallara benzer şekilde, her anahtarın kök köprüye yalnızca tek bir yola sahip olduğu bir topoloji oluşturduğuna dikkat edin.



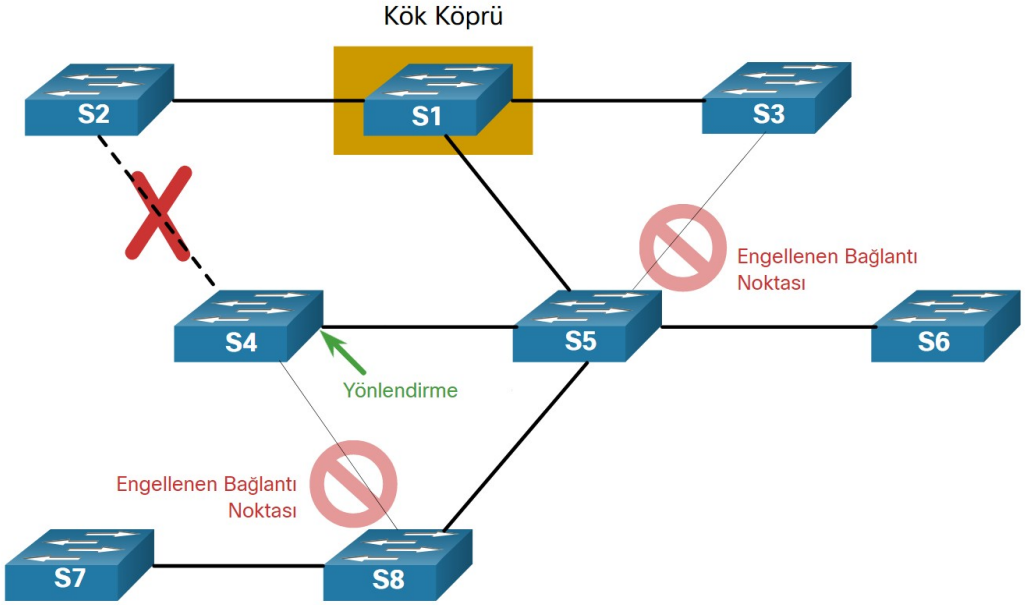

Her anahtarın artık kök köprüye yalnızca bir yönlendirme yolu vardır.

## Bağlantı Hatası Yeniden Hesaplamaya Neden Oluyor

Fiziksel yollar, artıklık sağlamak için hala mevcuttur, ancak bu yollar döngülerin oluşmasını önlemek için devre dışı bırakılmıştır. Bir ağ kablosu veya anahtar arızasını telafi etmek için yol gerekli olursa, STP, yolları yeniden hesaplar ve yedek yolun etkin hale gelmesine izin vermek için gerekli bağlantı noktalarının engelini kaldırır. STP yeniden hesaplamaları, ağa yeni bir anahtar veya yeni anahtarlar arası bağlantı eklendiğinde de gerçekleşebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Şekil, S2 ve S4 anahtarları arasında STP'nin yeniden hesaplamasına neden olan bir bağlantı hatasını göstermektedir. S4 ve S5 arasındaki önceden yedek bağlantının şimdi bu hatayı telafi etmek için ilettiğine dikkat edin. Her anahtar ile kök köprü arasında hala yalnızca bir yol vardır.




## 21.3.STP Nasıl Çalışır?

### 21.3.1.Döngüsüz Topolojiye Doğru

Artık döngülerin nasıl oluşturulduğunu ve bunları önlemek için kapsayan ağaç STP protokolünü kullanmanın temellerini biliyorsunuz. Bu konu sizi adım adım STP'nin işleyişine götürecektir. STA'yı kullanarak STP, dört adımlı bir süreçte döngü içermeyen bir topoloji oluşturur:

1. Kök köprüyü seçin.
2. Kök bağlantı noktalarını seçin.
3. Belirlenen bağlantı noktaları seçildi.
4. Alternatif (engellenmiş) bağlantı noktaları seçin.

STA ve STP işlevleri sırasında, anahtarlar kendileri ve bağlantıları hakkında bilgi paylaşmak için Köprü Protokolü Veri Birimlerini-Bridge Protocol Data Units (BPDU'lar) kullanır. BPDU'lar, kök köprüyü, kök bağlantı noktalarını, belirlenmiş bağlantı noktalarını ve alternatif bağlantı noktalarını seçmek için kullanılır. Her BPDU, BPDU'yu hangi anahtarın gönderdiğini tanımlayan bir köprü kimliği-bridge ID (BID) içerir. BID, kök köprü ve bağlantı noktası rolleri dahil olmak üzere STA kararlarının çoğunun alınmasında rol oynar. Şekilde gösterildiği gibi, BID bir öncelik (priority) değeri, genişletilmiş bir sistem kimliği- extended system IDve anahtarın MAC adresini içerir. En düşük BID değeri, bu üç alanın birleşimiyle belirlenir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

BID, Köprü Önceliğini, Genişletilmiş Sistem Kimliğini ve anahtarın MAC Adresini içerir.

### Köprü Önceliği

Tüm Cisco anahtarları için varsayılan öncelik değeri 32768 ondalık değeridir. Aralık, 4096'lık artışlarla 0 ila 61440 arasındadır. Daha düşük bir köprü önceliği tercih edilir. 0 olan bir köprü önceliği, diğer tüm köprü önceliklerinden önceliklidir.

### Genişletilmiş Sistem Kimliği

Genişletilmiş sistem kimliği değeri, bu BPDU için VLAN'ı tanımlamak üzere BID'deki köprü öncelik değerine eklenen ondalık bir değerdir.

IEEE 802.1D'nin ilk uygulamaları, VLAN kullanmayan ağlar için tasarlandı. Tüm anahtarlar arasında tek bir ortak yayılan ağaç vardı. Bu nedenle, eski anahtarlarda, genişletilmiş sistem kimliği BPDU'lara dahil edilmiyordu. Ağ altyapısı segmentasyonu için VLAN'lar yaygınlaştıkça, 802.1D, 12 bitlik VLAN kimliğinin BPDU çerçevesine dahil edilmesini gerektiren VLAN desteği içerecek şekilde geliştirildi. VLAN bilgileri, genişletilmiş sistem kimliği kullanılarak BPDU çerçevesine dahil edilir.

Genişletilmiş sistem kimliği, daha sonraki STP uygulamalarının farklı VLAN setleri için farklı kök köprülere sahip olmasına izin verir. Bu, bir VLAN setinin farklı bir kök köprü kullanan farklı bir VLAN seti tarafından kullanılması için bir STP topolojisinde yedekli, iletmeyen bağlantılara izin verebilir.

### Mac Adresi

İki anahtar aynı öncelik ile yapılandırıldığında ve aynı genişletilmiş sistem kimliğine sahip olduğunda, onaltılık olarak ifade edilen en düşük değere sahip MAC adresine sahip anahtar, daha düşük BID'ye sahip olacaktır.

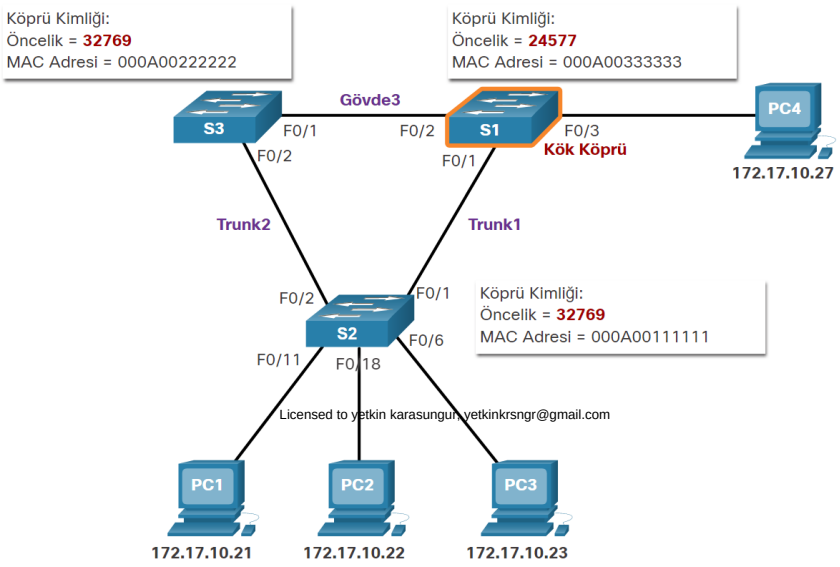
## 1. Kök Köprüyü seçin

STA, tek bir anahtarı temel köprü olarak belirler ve tüm yol hesaplamaları için referans noktası olarak kullanır. Anahtarlar, kök köprünün seçilmesiyle başlayarak döngü içermeyen topoloji oluşturmak için BPDU'ları değiştirir.

Bir seçim süreci, hangi anahtarın temel köprü olacağını belirler. Yayın alanındaki tüm anahtarlar seçim sürecine katılır. Bir anahtar başlatıldıktan sonra, her iki saniyede bir BPDU çerçeveleri göndermeye başlar. Bu BPDU çerçeveleri, gönderen anahtarın BID'sini ve Kök Kimliği olarak bilinen kök köprünün BID'sini içerir.

En düşük BID'ye sahip anahtar, kök köprü olacaktır. İlk başta, tüm anahtarlar, kendi BID'leri Kök Kimliği olarak ayarlanmış olarak kendilerini kök köprü olarak ilan eder. Sonunda, anahtarlar en düşük BID'ye sahip olan ve bir kök köprü üzerinde anlaşacak olan BPDU'ların değişimi yoluyla öğrenir.

Şekilde S1, en düşük BID'ye sahip olduğu için temel köprü olarak seçilmiştir.

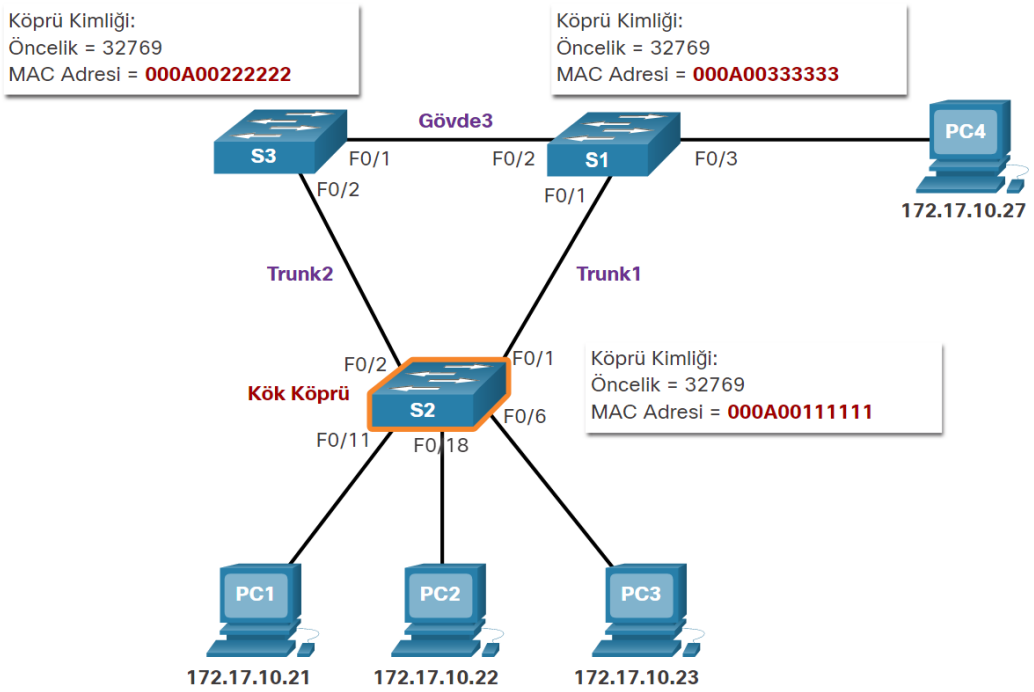


Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Varsayılan BID 32768 olduğundan, iki veya daha fazla anahtarın aynı önceliğe sahip olması mümkündür. Önceliklerin aynı olduğu bu senaryoda, en düşük MAC adresine sahip anahtar, kök köprü haline gelecektir. Kök köprü kararının ağ gereksinimlerini en iyi şekilde karşıladığından emin olmak için, yöneticinin istenen kök köprü anahtarını daha düşük bir öncelikle yapılandırması önerilir.

Şekilde, tüm anahtarlar 32769 ile aynı önceliğe göre yapılandırılmıştır. Burada MAC adresi, hangi anahtarın kök köprü olacağı konusunda belirleyici faktör haline gelir. En düşük onaltılık MAC adresi değerine sahip anahtar, tercih edilen kök köprüdür. Bu örnekte, S2, MAC adresi için en düşük değere sahiptir ve bu kapsayan ağaç örneği için kök köprü olarak seçilmiştir.

Not : Örnekte, tüm anahtarların önceliği 32769'dur. Değer, 32768 varsayılan köprü önceliğine ve her anahtarla (32768 + 1) ilişkili genişletilmiş sistem kimliğine (VLAN 1 ataması) dayanmaktadır.




## Kök Yol (Root Port)Maliyetini Belirleyin

Belirli bir kapsayan ağaç örneği için kök köprü seçildiğinde, STA, yayın etki alanındaki tüm hedeflerden kök köprüye giden en iyi yolları belirleme sürecini başlatır. Dahili kök yol maliyeti olarak bilinen yol bilgisi, anahtardan kök köprüye giden yol boyunca tüm bağımsız bağlantı noktası maliyetlerinin toplamı tarafından belirlenir.

Not : BPDU, kök yol maliyetini içerir. Bu, gönderen anahtardan kök köprüye giden yolun maliyetidir.

Bir anahtar BPDU'yu aldığında, dahili kök yolu maliyetini belirlemek için segmentin giriş bağlantı noktası maliyetini ekler.

Varsayılan bağlantı noktası maliyetleri, bağlantı noktasının çalıştığı hız ile tanımlanır. Tablo, IEEE tarafından önerilen varsayılan bağlantı noktası maliyetlerini gösterir. Cisco anahtarları varsayılan olarak, hem STP hem de RSTP için kısa yol maliyeti olarak da bilinen IEEE 802.1D standardı tarafından tanımlanan değerleri kullanır. Bununla birlikte, IEEE standardı, 10 Gb / sn bağlantılar ve daha hızlı kullanılırken uzun yol maliyeti olarak da bilinen IEEE-802.1w'de tanımlanan değerlerin kullanılmasını önerir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

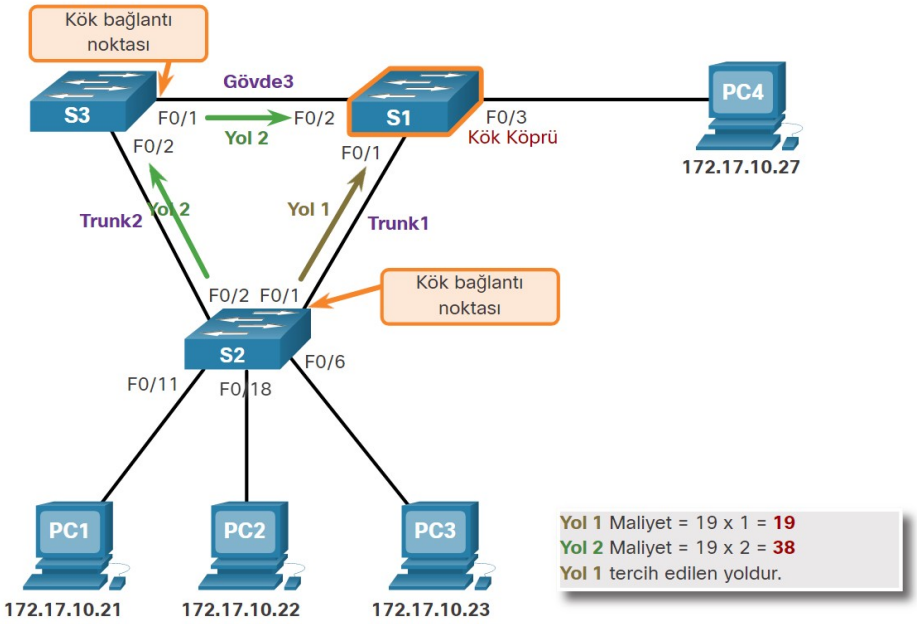
| Bağlantı hızı | STP Maliyeti: IEEE 802.1D-1998 | RSTP Maliyeti: IEEE 802.1w-2004 |
|---|---|---|
| 10 Gb / sn | 2 | 2.000 |
| 1 Gb / sn | 4 | 20.000 |
| 100 Mb / sn | 19 | 200.000 |
| 10 Mb / sn | 100 | 2.000.000 |

Anahtar bağlantı noktalarının kendileriyle ilişkili varsayılan bir bağlantı noktası maliyeti olmasına rağmen, bağlantı noktası maliyeti yapılandırılabilir. Ayrı bağlantı noktası maliyetlerini yapılandırma yeteneği, yöneticiye kök köprüye uzanan ağaç yollarını manuel olarak kontrol etme esnekliği sağlar.

## 2. Kök Bağlantı Noktalarını (Root Port) Seçin

Kök köprü belirlendikten sonra, kök bağlantı noktasını seçmek için STA algoritması kullanılır. Kök olmayan her anahtar bir kök bağlantı noktası seçecektir. Kök bağlantı noktası, genel maliyet (en iyi yol) açısından temel köprüye en yakın bağlantı noktasıdır. Bu toplam maliyet, dahili kök yolu maliyeti olarak bilinir.

Dahili kök yolu maliyeti, şekilde gösterildiği gibi, temel köprüye giden yol boyunca tüm bağlantı noktası maliyetlerinin toplamına eşittir. En düşük maliyetli yollar tercih edilir ve diğer tüm gereksiz yollar engellenir. Örnekte, yol 1 üzerinden S2'den temel köprü S1'e dahili kök yol maliyeti 19 iken (IEEE tarafından belirlenen bağımsız bağlantı noktası maliyetine göre) yol 2'ye göre dahili kök yol maliyeti 38'dir. temel köprü için toplam yol maliyeti, tercih edilen yoldur ve F0 / 1, S2'deki kök bağlantı noktası olur.




## 3. Seçilmiş-Belirtilmiş (Designated) Bağlantı Noktaları

Kapsayan ağacın döngü önleme kısmı bu sonraki iki adımda belirginleşir. Her anahtar bir kök bağlantı noktası seçtikten sonra, anahtarlar belirlenen bağlantı noktalarını seçecektir.

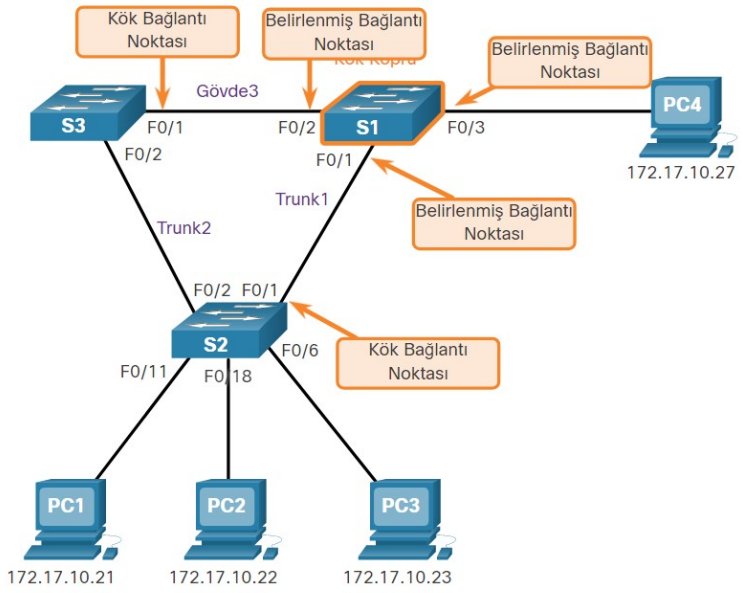
İki anahtar arasındaki her segmentin bir belirlenmiş portu olacaktır. Belirtilen bağlantı noktası, segment üzerindeki (iki anahtarlı), kök köprüye dahili kök yol maliyetine sahip bir bağlantı noktasıdır. Diğer bir deyişle, belirlenen bağlantı noktası, kök köprüye giden trafiği almak için en iyi yola sahiptir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Kök bağlantı noktası veya belirlenmiş bağlantı noktası olmayan şey, alternatif veya engellenen bağlantı noktası olur. Sonuç, her anahtardan kök köprüye tek bir yoldur.

## Kök Köprü Üzerindeki Belirlenmiş Bağlantı Noktaları

Temel köprü üzerindeki tüm bağlantı noktaları, şekilde gösterildiği gibi belirlenmiş bağlantı noktalarıdır. Bunun nedeni, temel köprünün kendisi için en düşük maliyete sahip olmasıdır.

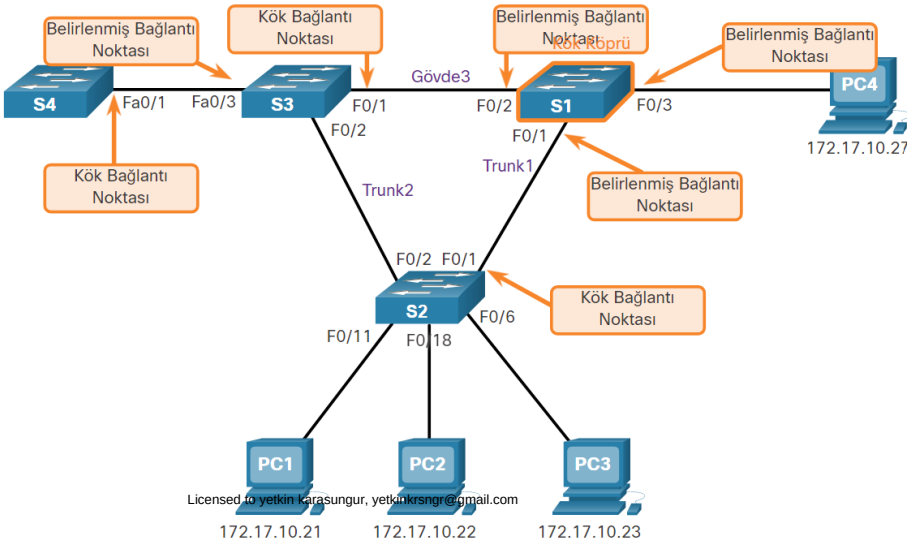



Kök köprü üzerindeki tüm bağlantı noktaları belirlenmiş bağlantı noktalarıdır.

## Kök Bağlantı Noktası Olduğunda Belirlenmiş Bağlantı Noktası

Bir segmentin bir ucu bir kök bağlantı noktasıysa, diğer ucu belirlenmiş bir bağlantı noktasıdır. Bunu göstermek için, şekil S4 anahtarının S3'e bağlı olduğunu gösterir. S4'teki Fa0 / 1 arayüzü, kök bağlantı noktasıdır çünkü kök köprüye giden en iyi ve tek yola sahiptir. Segmentin diğer ucundaki S3 üzerindeki Fa0 / 3 arayüzü bu nedenle belirlenen port olacaktır.

Not : Uç cihazların (ana bilgisayarların) takılı olduğu tüm anahtar bağlantı noktaları belirlenmiş bağlantı noktalarıdır.

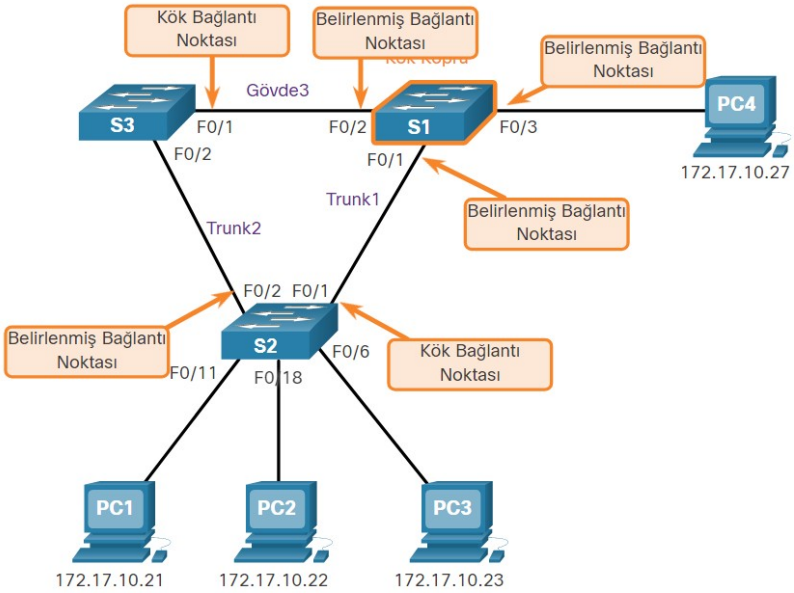



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

S4'teki Fa0 / 1 arabirimi, bir kök bağlantı noktasıdır çünkü S3'ün Fa0 / 3 arabirimi, belirlenmiş bir bağlantı noktasıdır.

### Kök Bağlantı Noktası Olmadığında Belirlenen Bağlantı Noktası

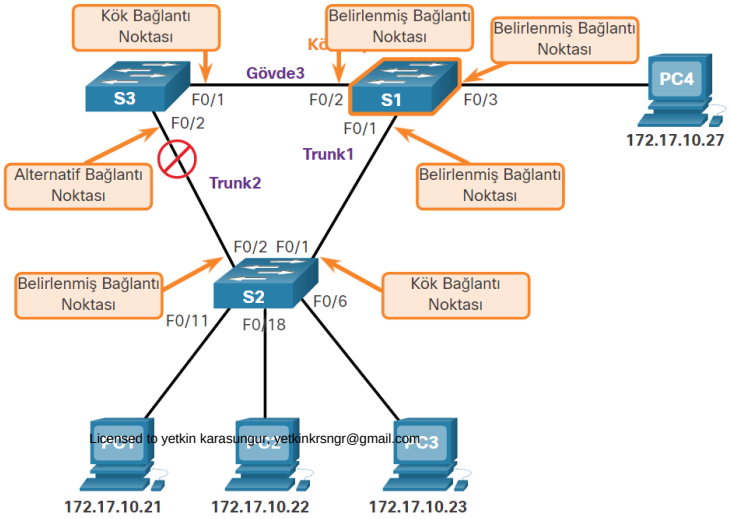
Bu, iki anahtar arasında yalnızca anahtarlardan hiçbirinin kök köprü olmadığı bölümler bırakır. Bu durumda, anahtar üzerindeki, kök köprüye giden en düşük maliyetli yola sahip bağlantı noktası, segment için belirlenmiş bağlantı noktasıdır. Örneğin, şekilde, son segment, S2 ve S3 arasındakidir. Hem S2 hem de S3, kök köprüye aynı yol maliyetine sahiptir. Kapsayan ağaç algoritması, köprü kimliğini bir bağ kırıcı olarak kullanacaktır. Şekilde gösterilmemesine rağmen, S2 daha düşük bir BID'ye sahiptir. Bu nedenle, S2'nin F0 / 2 portu belirlenmiş port olarak seçilecektir. Belirtilen bağlantı noktaları yönlendirme durumundadır.




S2'nin Fa0 / 2 arayüzü, S3 ile segmentte belirlenmiş porttur.

## 4. Alternatif (Engellenen) Bağlantı Noktaları Seçin

Bir bağlantı noktası bir kök bağlantı noktası veya belirlenmiş bir bağlantı noktası değilse, o zaman alternatif (veya yedek) bir bağlantı noktası olur. Döngüleri önlemek için alternatif bağlantı noktaları ve yedek bağlantı noktaları atma-discard veya engelleme-blocking durumundadır. Şekilde, STA alternatif rolde S3 üzerinde F0 / 2 bağlantı noktasını yapılandırmıştır. S3 üzerindeki F0 / 2 bağlantı noktası engelleme durumundadır ve Ethernet çerçevelerini iletmeyecektir. Diğer tüm anahtarlar arası bağlantı noktaları yönlendirme durumundadır. Bu, STP'nin döngü önleme kısmıdır.




S3'ün Fa0 / 2 arabirimi bir kök bağlantı noktası veya belirlenmiş bir bağlantı noktası değildir, bu nedenle alternatif veya engellenmiş bir bağlantı noktası olur.

## Birden Çok Eşit Maliyet Yolundan Bir Kök Bağlantı Noktası Seçin

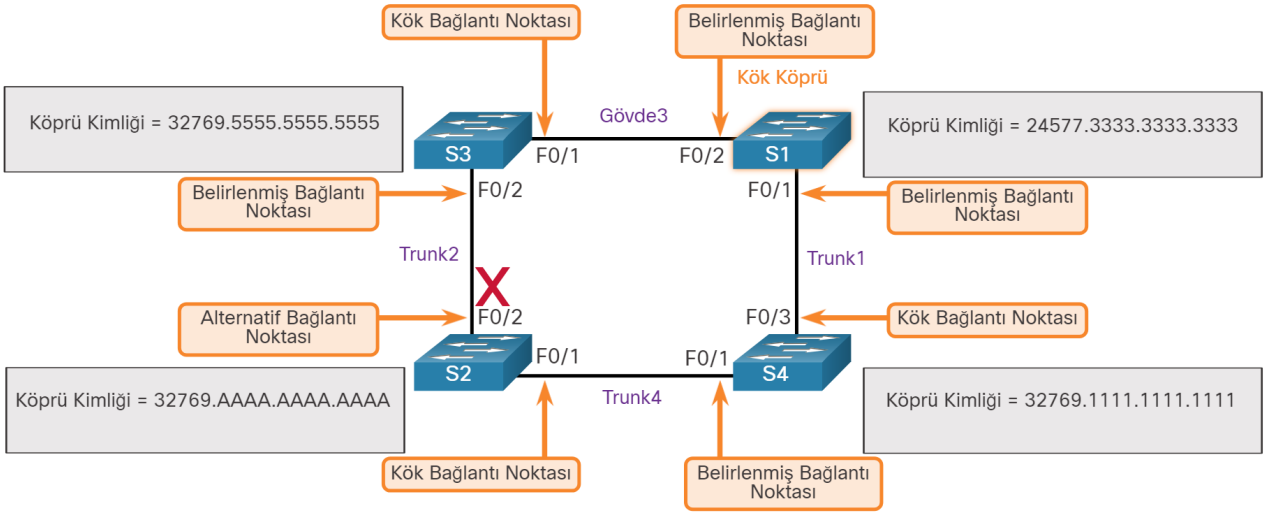
Kök bağlantı noktası ve belirlenen bağlantı noktaları, kök köprüye giden en düşük yol maliyetine dayanır. Ancak, anahtarın kök köprüye birden çok eşit maliyetli yolu varsa ne olur? Bir anahtar, bir kök bağlantı noktasını nasıl belirler?

Bir anahtarın kök köprüye eşit maliyetli birden çok yolu olduğunda, anahtar aşağıdaki kriterleri kullanarak bir bağlantı noktası belirler:

- En düşük gönderen BID
- En düşük gönderen bağlantı noktası önceliği
- En düşük gönderen bağlantı noktası kimliği

### 1 . En Düşük Gönderen BID

Şekilde, kök köprü olarak S1 anahtarı dahil olmak üzere dört anahtarlı bir topoloji gösterilmektedir. Bağlantı noktası rolleri incelendiğinde, S3 anahtarındaki F0 / 1 bağlantı noktası ve S4 anahtarındaki F0 / 3 bağlantı noktası, ilgili anahtarları için kök köprüye en düşük maliyetli yola (kök yol maliyeti) sahip oldukları için kök bağlantı noktaları olarak seçilmiştir. S2 iki bağlantı noktasına sahiptir, F0 / 1 ve F0 / 2, temel köprüye eşit maliyetli yollarla. Bu durumda, bağın kopması için komşu anahtarların köprü kimlikleri S3 ve S4 kullanılacaktır. Bu, gönderenin BID olarak bilinir. S3'ün BID'si 32769.5555.5555.5555 ve S4'ün BID'si 32769.1111.1111.1111'dir. S4 daha düşük bir BID'ye sahip olduğundan, S4'e bağlı bağlantı noktası olan S2'nin F0 / 1 bağlantı noktası kök bağlantı noktası olacaktır.

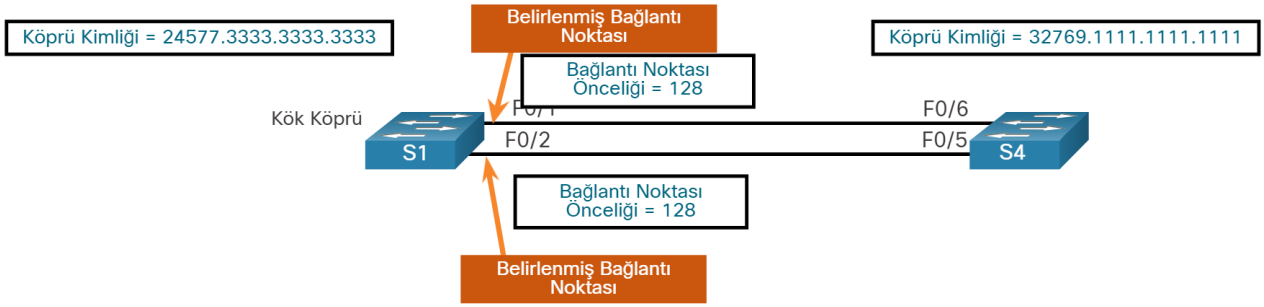



### 2 . En Düşük Gönderen Bağlantı Noktası Önceliği

Sonraki iki kriteri göstermek için, topoloji, aralarında iki eşit maliyetli yol bulunan iki anahtarın bağlandığı bir topoloji olarak değiştirilir. S1, kök köprüdür, bu nedenle her iki bağlantı noktası da belirlenmiş bağlantı noktalarıdır.

S4, temel köprüye eşit maliyetli yollara sahip iki bağlantı noktasına sahiptir. Her iki bağlantı noktası da aynı anahtara bağlı olduğundan, gönderenin BID'si (S1) eşittir. Yani ilk adım berabere.

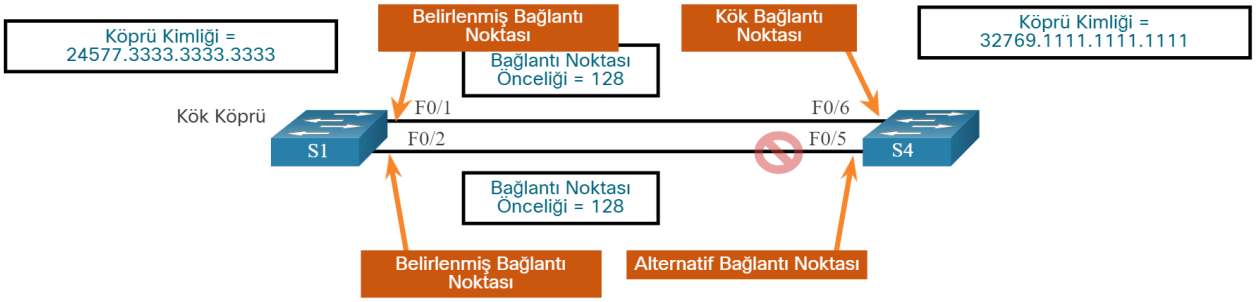
Listede bir sonraki, gönderenin (S1) bağlantı noktası önceliği. Varsayılan bağlantı noktası önceliği 128'dir, bu nedenle S1'deki her iki bağlantı noktası da aynı bağlantı noktası önceliğine sahiptir. Bu aynı zamanda bir berabere. Bununla birlikte, S1 üzerindeki bağlantı noktalarından herhangi biri daha düşük bir bağlantı noktası önceliğiyle yapılandırılmışsa, S4 bitişik bağlantı noktasını iletim durumuna geçirecektir. S4 üzerindeki diğer bağlantı noktası bir engelleme durumu olacaktır.




### 3 . En Düşük Gönderen Bağlantı Noktası Kimliği

Son bağ bozucu, en düşük gönderenin bağlantı noktası kimliğidir. S4 anahtarı, S1 üzerindeki F0 / 1 ve F0 / 2 bağlantı noktalarından BPDU'ları aldı. Kararın alıcının bağlantı noktası kimliğine değil, gönderenin bağlantı noktası kimliğine bağlı olduğunu unutmayın. S1'deki F0 / 1'in bağlantı noktası kimliği, F0 / 2 bağlantı noktasından daha düşük olduğu için, S4 anahtarındaki F0 / 6 bağlantı noktası kök bağlantı noktası olacaktır. Bu, S1'deki F0 / 1 bağlantı noktasına bağlı S4'teki bağlantı noktasıdır.

S4 üzerindeki F0 / 5 bağlantı noktası, alternatif bir bağlantı noktası haline gelecek ve STP'nin döngü önleme parçası olan engelleme durumuna yerleştirilecektir.




## STP Zamanlayıcıları ve Port Durumları

STP yakınsaması aşağıdaki gibi üç zamanlayıcı gerektirir:

- Merhaba Zamanlayıcısı(Hello Timer ) - Merhaba zamanı, BPDU'lar arasındaki aralıktır. Varsayılan 2 saniyedir ancak 1 ile 10 saniye arasında değiştirilebilir.
- İleri Gecikme Zamanlayıcısı (Forward Delay Timer ) - İleri gecikme, dinleme ve öğrenme durumunda harcanan süredir. Varsayılan 15 saniyedir ancak 4 ile 30 saniye arasında değiştirilebilir.
- Maksimum Yaş Zamanlayıcısı (Max Age Timer ) - Maksimum yaş, STP topolojisini değiştirmeye çalışmadan önce bir anahtarın beklediği maksimum süredir. Varsayılan 20 saniyedir, ancak 6 ile 40 saniye arasında değiştirilebilir.

Not : Varsayılan zamanlar, STP alanı için bu zamanlayıcıların değerini belirleyen kök köprüde değiştirilebilir.

STP, yayın alanı boyunca mantıksal döngü içermeyen yolu kolaylaştırır. Kapsayan ağaç, BPDU çerçevelerinin birbirine bağlı anahtarlar arasında değiş tokuşu ile öğrenilen bilgiler aracılığıyla belirlenir. Bir anahtar bağlantı noktası, geçiş sırasında tam topoloji hakkında bilgi olmadan doğrudan engelleme durumundan yönlendirme durumuna geçiş yaparsa, bağlantı noktası geçici olarak bir veri döngüsü oluşturabilir. Bu nedenle, STP, şekilde gösterildiği gibi dördü operasyonel bağlantı noktası durumu olan beş bağlantı noktasına sahiptir. Devre dışı durumunun işlevsel olmadığı kabul edilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Port Durumu | Açıklama |
|---|---|
| Engelleme (Blocking) | Bağlantı noktası, alternatif bir bağlantı noktasıdır ve çerçeve iletmeye katılmaz. Bağlantı noktası, kök köprünün konumunu ve kök kimliğini belirlemek için BPDU çerçevelerini alır. BPDU çerçeveleri ayrıca her bir anahtar bağlantı noktasının son etkin STP topolojisinde hangi bağlantı noktası rollerini üstlenmesi gerektiğini belirler.20 saniyelik Maks Yaş zamanlayıcısıyla, komşu anahtardan beklenen bir BPDU almayan bir anahtar bağlantı noktası, engelleme durumuna geçecektir. |
| Dinleme (Listening)) | Engelleme durumundan sonra, bir bağlantı noktası dinleme durumuna geçecektir. Bağlantı noktası, köke giden yolu belirlemek için BPDU'ları alır. Anahtar bağlantı noktası ayrıca kendi BPDU çerçevelerini iletir ve bitişik anahtarlara anahtar bağlantı noktasının aktif topolojiye katılmaya hazırlandığını bildirir. |
| Öğrenme (Learning) | Bir anahtar bağlantı noktası, dinleme durumundan sonra öğrenme durumuna geçiş yapar. Öğrenme durumu sırasında, anahtar bağlantı noktası BPDU'ları alır ve işler ve çerçeve iletmeye katılmaya hazırlanır.Ayrıca MAC adres tablosunu doldurmaya başlar. Bununla birlikte, öğrenme durumunda, kullanıcı çerçeveleri hedefe iletilmez. |
| İletme (Forearding) | Yönlendirme durumunda, bir anahtar bağlantı noktası aktif topolojinin bir parçası olarak kabul edilir.Anahtar bağlantı noktası, kullanıcı trafiğini iletir ve BPDU çerçevelerini gönderir ve alır. |
| Devre dışı | Devre dışı durumdaki bir anahtar bağlantı noktası, yayılma ağacına katılmaz ve çerçeveleri iletmez.Devre dışı durumu, anahtar bağlantı noktası yönetimsel olarak devre dışı bırakıldığında ayarlanır. |

## Her Port Durumunun Operasyonel Detayları

| Port Durumu | BPDU | MAC Adres Tablosu | Veri Çerçevelerini İletme |
|---|---|---|---|
| Engelleme | Sadece al | Güncelleme yok | Hayır |
| Dinleme | Al ve gönder | Güncelleme yok | Hayır |
| Öğrenme | Al ve gönder | Tablo güncelleniyor | Hayır |
| Yönlendirme | Al ve gönder | Tablo güncelleniyor | Evet |
| Devre dışı | Hiçbiri gönderilmedi veya alınmadı | Güncelleme yok | Hayır |

## 21.4.STP'nin Farklı Versiyonları

Şimdiye kadar, Yayılan Ağaç Protokolü terimini ve yanıltıcı olabilecek STP kısaltmasını kullandık. Pek çok profesyonel bunları, Rapid Spanning Tree Protocol (RSTP) ve Multiple Spanning Tree Protocol (MSTP) gibi çeşitli yayılan ağaç uygulamalarına başvurmak için kullanır. Kapsayan ağaç kavramlarını doğru bir şekilde iletmek için, bağlamda yayılma ağacının uygulanmasına veya standardına başvurmak önemlidir.

Kapsayan ağaç için en son standart, Yerel ve metropolitan alan ağları için IEEE standardı olan IEEE-802-1D-2004'te bulunur: Ortam Erişim Kontrolü (MAC) Köprüleri. Standardın bu sürümü, standartla uyumlu anahtarların ve köprülerin, orijinal 802.1d standardında belirtilen eski STP protokolü yerine Hızlı Yayılma Ağacı Protokolünü (RSTP) kullanacağını belirtir. Bu müfredatta, orijinal Yayılan Ağaç Protokolü bir tartışmanın bağlamı olduğunda, karışıklığı önlemek için "orijinal 802.1D kapsayan ağaç" ifadesi kullanılır. İki protokol, döngü içermeyen yol için aynı terminolojiyi ve yöntemleri paylaştığından, birincil odak noktası mevcut standart ve Cisco tescilli STP ve RSTP uygulamaları olacaktır.

Tabloda gösterildiği gibi, orijinal IEEE 802.1D spesifikasyonundan bu yana genişleyen ağaç protokollerinin çeşitli çeşitleri ortaya çıkmıştır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| STP Türü | Açıklama |
|---|---|
| STP | Bu, yedekli bağlantılara sahip bir ağda döngü içermeyen bir topoloji sağlayan orijinal IEEE 802.1D sürümüdür (802.1D-1998 ve öncesi). Ortak Genişleme Ağacı (CST) olarak da adlandırılır, VLAN'ların sayısından bağımsız olarak tüm köprülü ağ için bir kapsayan ağaç örneğini varsayar. |
| PVST + | VLAN Başına Genişleme Ağacı (PVST +), ağda yapılandırılan her VLAN için ayrı bir 802.1D kapsayan ağaç örneği sağlayan bir Cisco STP geliştirmesidir. PVST +; PortFast, UplinkFast, BackboneFast, BPDU koruması, BPDU filtresi, kök koruması ve döngü korumasını destekler. |
| RSTP | Hızlı Yayılma Ağacı Protokolü (RSTP) veya IEEE 802.1w, STP'den daha hızlı yakınsama sağlayan bir STP evrimidir. |
| 802.1D-2004 | Bu, IEEE 802.1w'yi içeren STP standardının güncellenmiş bir sürümüdür. |
| Hızlı PVST + | Bu, PVST + kullanan ve VLAN başına ayrı bir 802.1w örneği sağlayan bir Cisco RSTP geliştirmesidir.Her ayrı örnek, PortFast, BPDU koruması, BPDU filtresi, kök koruması ve döngü korumasını destekler. |
| MSTP | Çoklu Genişleme Ağacı Protokolü (MSTP), önceki Cisco tescilli Çoklu Örnek STP (MISTP) uygulamasından esinlenen bir IEEE standardıdır. MSTP, birden çok VLAN'ı aynı kapsayan ağaç örneğine eşler. |
| MST | Çoklu Genişleme Ağacı (MST), MSTP'nin 16 adede kadar RSTP örneği sağlayan ve aynı fiziksel ve mantıksal topolojiye sahip birçok VLAN'ı ortak bir RSTP örneğinde birleştiren Cisco uygulamasıdır.Her örnek PortFast, BPDU koruması, BPDU filtresi, kök koruması ve döngü korumasını destekler. |

IOS 15.0 veya üstünü çalıştıran Cisco anahtarları, varsayılan olarak PVST + çalıştırın. Bu sürüm, eski belirlenmemiş bağlantı noktalarının yerine alternatif bağlantı noktaları gibi IEEE 802.1D-2004'ün birçok özelliğini içerir. Hızlı yayılan ağaç protokolünü çalıştırmak için anahtarların hızlı yayılan ağaç modu için açıkça yapılandırılması gerekir.

## RSTP Kavramları

RSTP (IEEE 802.1w), geriye dönük uyumluluğu korurken orijinal 802.1D'nin yerini alır. 802.1w STP terminolojisi esas olarak orijinal IEEE 802.1D STP terminolojisiyle aynı kalır. Çoğu parametre değiştirilmeden bırakılmıştır. Orijinal STP standardına aşina olan kullanıcılar, RSTP'yi kolayca yapılandırabilir. Bağlantı noktası rollerini ve topolojiyi belirlemek için hem STP hem de RSTP için aynı yayılma ağacı algoritması kullanılır.

RSTP, Katman 2 ağ topolojisi değiştiğinde kapsayan ağacın yeniden hesaplanma hızını artırır. RSTP, düzgün yapılandırılmış bir ağda bazen birkaç yüz milisaniye kadar kısa bir sürede çok daha hızlı yakınsama sağlayabilir. Bir bağlantı noktası, alternatif bir bağlantı noktası olacak şekilde yapılandırılırsa, ağın yakınsamasını beklemeden hemen bir yönlendirme durumuna geçebilir.

Not : Rapid PVST +, RSTP'nin VLAN bazında Cisco uygulamasıdır. Rapid PVST + ile her VLAN için bağımsız bir RSTP örneği çalışır.

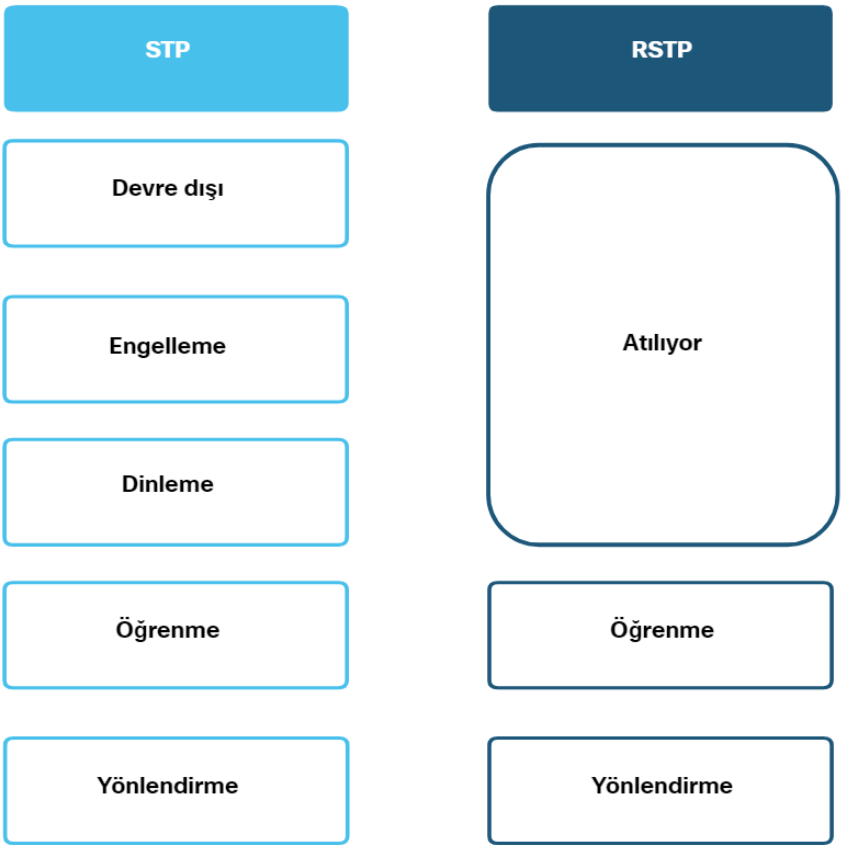
## RSTP Bağlantı Noktası Durumları ve Bağlantı Noktası Rolleri

STP ve RSTP arasındaki bağlantı noktası durumları ve bağlantı noktası rolleri benzerdir.

### STP ve RSTP Bağlantı Noktası Durumları

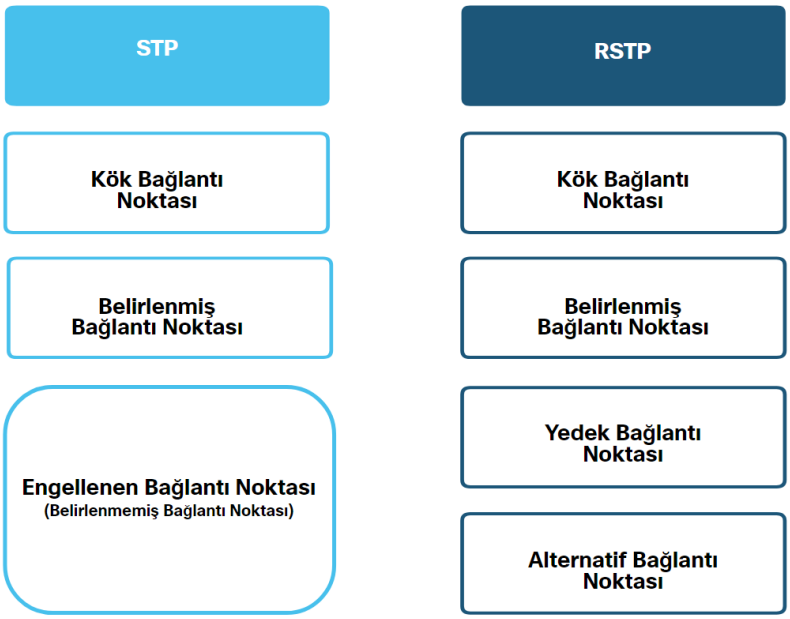
Şekilde gösterildiği gibi, RSTP'de STP'deki üç olası çalışma durumuna karşılık gelen yalnızca üç bağlantı noktası durumu vardır. 802.1D devre dışı, engelleme ve dinleme durumları benzersiz bir 802.1w atma-discard durumunda birleştirilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## STP ve RSTP Bağlantı Noktası Rolleri

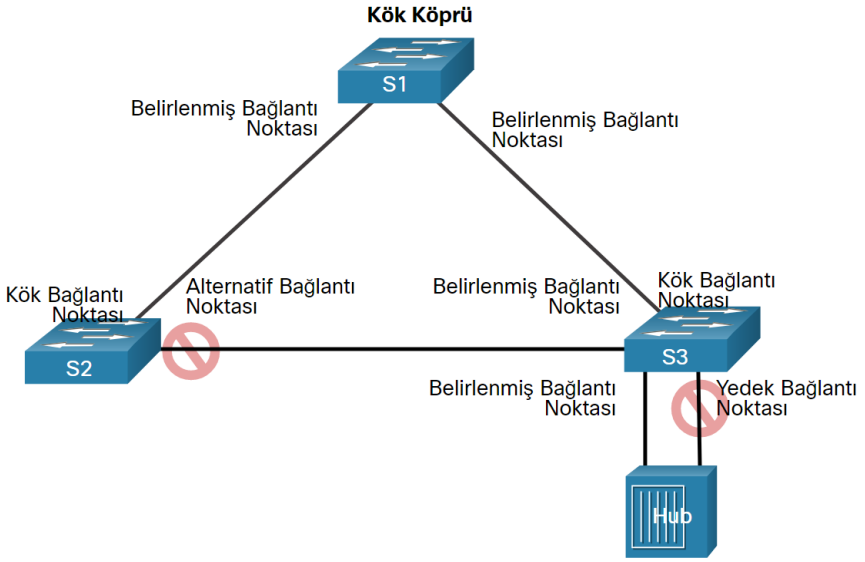
Şekilde gösterildiği gibi, kök bağlantı noktaları ve belirlenmiş bağlantı noktaları hem STP hem de RSTP için aynıdır. Ancak, STP'nin engelleme durumuna karşılık gelen iki RSTP bağlantı noktası rolü vardır. STP'de, engellenen bir bağlantı noktası, atanmış veya kök bağlantı noktası olarak tanımlanır. RSTP'nin bu amaç için iki bağlantı noktası rolü vardır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### RSTP Alternatif ve Yedek Bağlantı Noktaları

Şekilde gösterildiği gibi, alternatif bağlantı noktası, temel köprüye giden alternatif bir yola sahiptir. Yedekleme bağlantı noktası, hub gibi paylaşılan bir ortama yedeklemedir. Yedekleme bağlantı noktası daha az yaygındır çünkü hub'lar artık eski cihazlar olarak kabul edilmektedir.

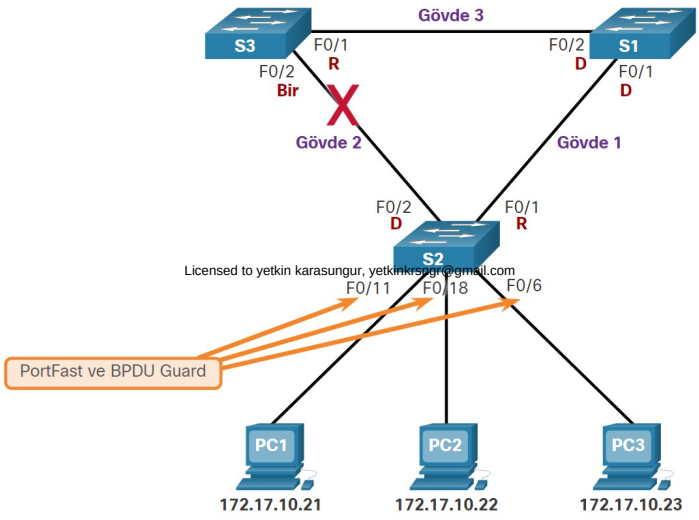



## PortFast ve BPDU Guard

Bir cihaz bir anahtar bağlantı noktasına bağlandığında veya bir anahtar açıldığında, anahtar bağlantı noktası hem dinleme hem de öğrenme durumlarından geçer ve her seferinde İleri Gecikme zamanlayıcısının süresinin dolmasını bekler. Bu gecikme, her bir durum, dinleme ve öğrenme için toplam 30 saniye için 15 saniyedir. Bu gecikme, bir DHCP sunucusunu bulmaya çalışan DHCP istemcileri için bir sorun oluşturabilir. Bağlı ana bilgisayardan gelen DHCP mesajları, 30 saniyelik İleri Gecikme zamanlayıcıları için iletilmez ve DHCP işlemi zaman aşımına uğrayabilir. Sonuç, bir IPv4 istemcisinin geçerli bir IPv4 adresi almayacağıdır.

Not : Bu, istemcilerde ICMPv6 Yönlendirici Talep mesajları gönderirken meydana gelebilse de, yönlendirici ICMPv6 Yönlendirici Tanıtım mesajları göndermeye devam edecek, böylece aygıt adres bilgilerini nasıl elde edeceğini bilecektir.

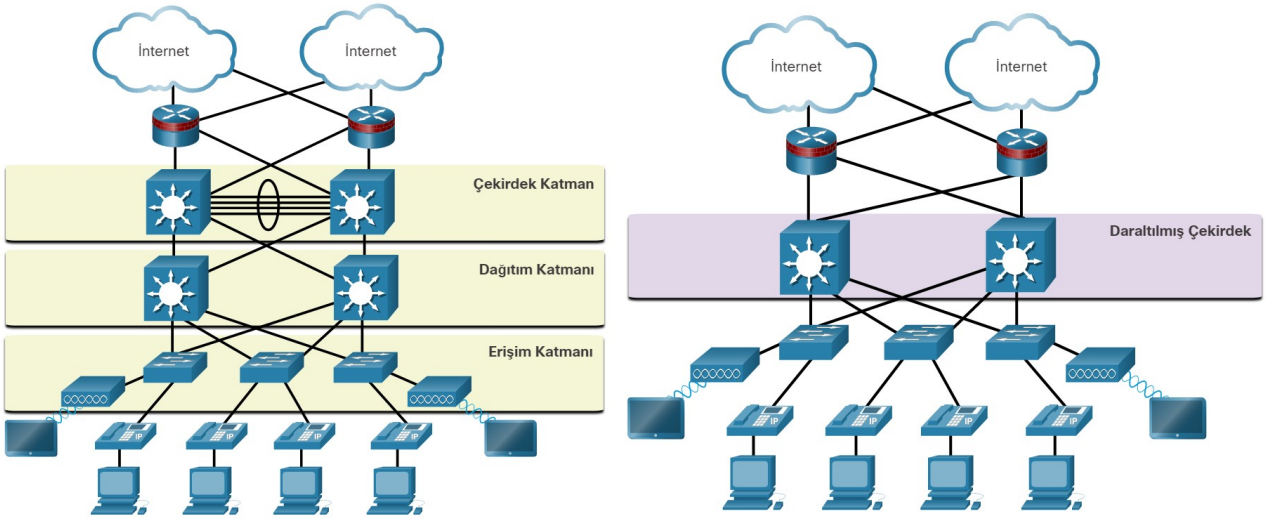
PortFast ile bir anahtar bağlantı noktası yapılandırıldığında, bu bağlantı noktası, olağan 802.1D STP geçiş durumlarını (dinleme ve öğrenme durumları) atlayarak ve 30 saniyelik bir gecikmeden kaçınarak hemen engellemeden yönlendirme durumuna geçer. IEEE 802.1D STP'nin her VLAN'da birleşmesini beklemek yerine, DHCP istemcileri gibi bu bağlantı noktalarına bağlı aygıtların ağa hemen erişmesine izin vermek için erişim bağlantı noktalarında PortFast'ı kullanabilirsiniz. PortFast'in amacı, erişim bağlantı noktalarının yayılma ağacının birleşmesini beklemesi gereken süreyi en aza indirmek olduğu için, yalnızca erişim bağlantı noktalarında kullanılmalıdır. PortFast'i başka bir anahtara bağlanan bir bağlantı noktasında etkinleştirirseniz, genişleyen bir ağaç döngüsü oluşturma riskiniz vardır. PortFast yalnızca uç cihazlara bağlanan anahtar bağlantı noktalarında kullanım içindir.



Geçerli bir PortFast yapılandırmasında, BPDU'lar PortFast özellikli anahtar bağlantı noktalarında asla alınmamalıdır, çünkü bu bağlantı noktasına başka bir köprü veya anahtarın bağlı olduğunu gösterir. Bu potansiyel olarak genişleyen bir ağaç döngüsüne neden olur. Bu tür bir senaryonun oluşmasını önlemek için Cisco anahtarları, BPDU koruması adı verilen bir özelliği destekler. Etkinleştirildiğinde, BPDU koruması, herhangi bir BPDU alındığında anahtar bağlantı noktasını derhal hatalı devre dışı (hata devre dışı) durumuna getirir. Bu, bağlantı noktasını etkin bir şekilde kapatarak olası döngülere karşı koruma sağlar. BPDU koruma özelliği, bir yöneticinin arabirimi manuel olarak hizmete sokması gerektiğinden geçersiz yapılandırmalara güvenli bir yanıt sağlar.

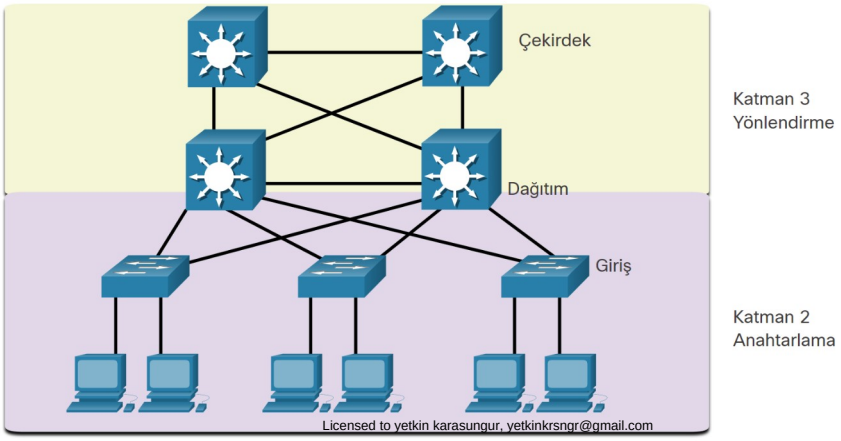
## STP'ye Alternatifler

STP, bir Ethernet döngü önleme protokolüydü ve hala da öyle. Yıllar geçtikçe, kuruluşlar LAN'da daha fazla dayanıklılık ve kullanılabilirlik gerektirdi. Ethernet LAN'ları, şekilde gösterildiği gibi, tek bir yönlendiriciye bağlı birkaç birbirine bağlı anahtardan erişim, dağıtım ve çekirdek katman anahtarlarını içeren karmaşık bir hiyerarşik ağ tasarımına geçti.



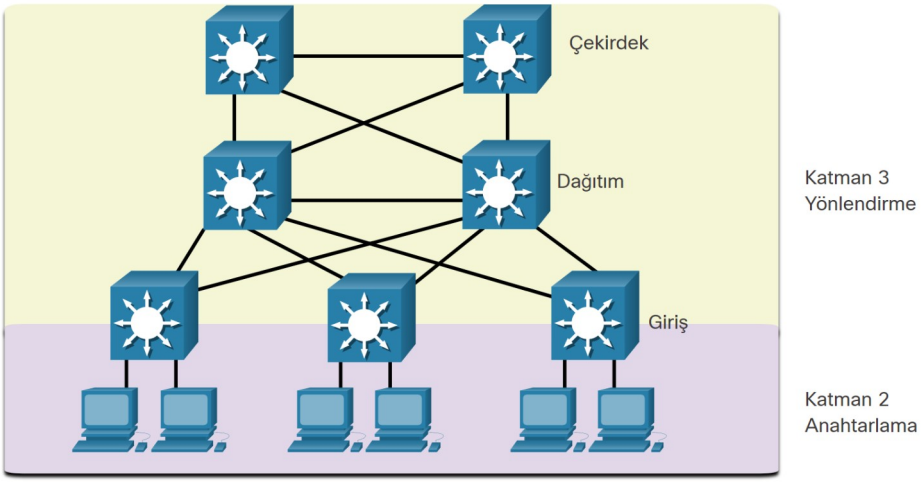

Uygulamaya bağlı olarak, Katman 2 sadece erişim katmanını değil, aynı zamanda dağıtımı ve hatta çekirdek katmanları da içerebilir. Bu tasarımlar, yüzlerce veya hatta binlerce VLAN içeren yüzlerce anahtar içerebilir. STP, RSTP ve MSTP'nin bir parçası olarak iyileştirmelerle eklenen fazlalık ve karmaşıklığa adapte olmuştur.

Ağ tasarımının önemli bir yönü, topolojide bir arıza veya değişiklik olduğunda hızlı ve öngörülebilir yakınsamadır. Kapsayan ağaç, Katman 3'teki yönlendirme protokolleri tarafından sağlanan aynı verimlilikleri ve öngörülebilirlikleri sunmamaktadır. Şekil, yönlendirme yapan dağıtım ve çekirdek çok katmanlı anahtarlarla geleneksel bir hiyerarşik ağ tasarımını göstermektedir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Katman 3 yönlendirmesi, bağlantı noktalarını engellemeden topolojide yedekli yollar ve döngüler sağlar. Bu nedenle, bazı ortamlar, cihazların erişim katmanı anahtarına bağlandığı yerler dışında her yerde Katman 3'e geçiş yapmaktadır. Başka bir deyişle, erişim katmanı anahtarları ve dağıtım anahtarları arasındaki bağlantılar, bir sonraki şekilde gösterildiği gibi, Katman 2 yerine Katman 3 olacaktır.




STP büyük olasılıkla kuruluşta bir döngü önleme mekanizması olarak kullanılmaya devam edecek olsa da, erişim katmanı anahtarlarında, aşağıdaki diğer teknolojiler de kullanılmaktadır:

- Çoklu Sistem Bağlantı Toplama-Multi System Link Aggregation (MLAG)
- En Kısa Yol Köprüleme-Shortest Path Bridging (SPB)
- Çok Sayıda Bağlantının Şeffaf Ara Bağlantısı-Transparent Interconnect of Lots of Links (TRILL)

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 22.Bölüm: Etherchannel

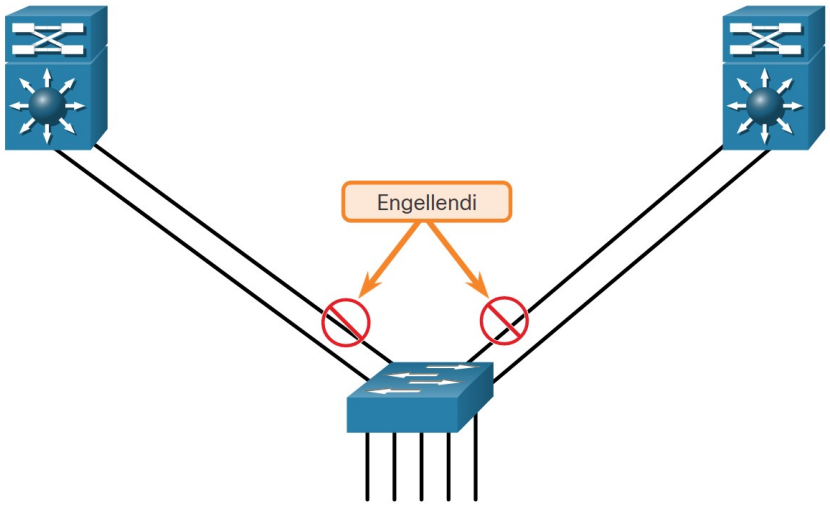
## 22.1.Bağlantı Toplama

Aygıtlar arasında, tek bir bağlantıyla sağlanandan daha fazla bant genişliği veya yedekliliğin gerekli olduğu senaryolar vardır. Bant genişliğini artırmak için cihazlar arasında birden fazla bağlantı bağlanabilir. Ancak, Cisco anahtarları gibi Katman 2 cihazlarında varsayılan olarak etkinleştirilen Yayılma Ağacı Protokolü (STP), şekilde gösterildiği gibi anahtarlama döngülerini önlemek için yedek bağlantıları engelleyecektir.

STP tarafından engellenmeyecek cihazlar arasında fazlalık bağlantılara izin veren bir bağlantı toplama teknolojisi gereklidir. Bu teknoloji, EtherChannel olarak bilinir.

EtherChannel, birden fazla fiziksel Ethernet bağlantısını tek bir mantıksal bağlantıda gruplayan bir bağlantı toplama teknolojisidir. Anahtarlar, yönlendiriciler ve sunucular arasında hata toleransı, yük paylaşımı, artırılmış bant genişliği ve artıklık sağlamak için kullanılır.

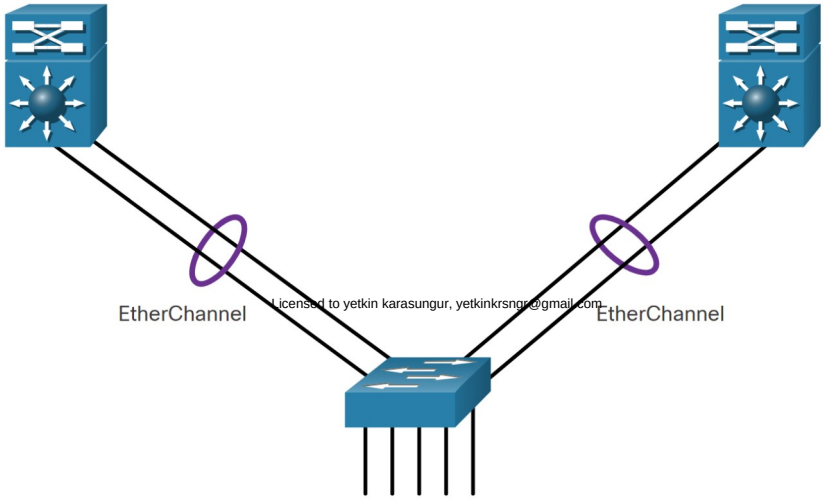
EtherChannel teknolojisi, anahtarlar arası iletişimin genel hızını artırmak için anahtarlar arasındaki fiziksel bağlantıların sayısını birleştirmeyi mümkün kılar.




STP, varsayılan olarak fazlalık bağlantıları engeller.

## 22.2.EtherChannel

EtherChannel teknolojisi, ilk olarak Cisco tarafından, birkaç Hızlı Ethernet veya Gigabit Ethernet bağlantı noktasını tek bir mantıksal kanalda gruplandıran bir LAN anahtar-geçiş tekniği olarak geliştirilmiştir. Bir EtherChannel yapılandırıldığında, ortaya çıkan sanal arabirime bağlantı noktası kanalı adı verilir. Fiziksel arayüzler, şekilde gösterildiği gibi bir bağlantı noktası kanalı arayüzünde birlikte paketlenmiştir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 22.2.3.EtherChannel'in Avantajları

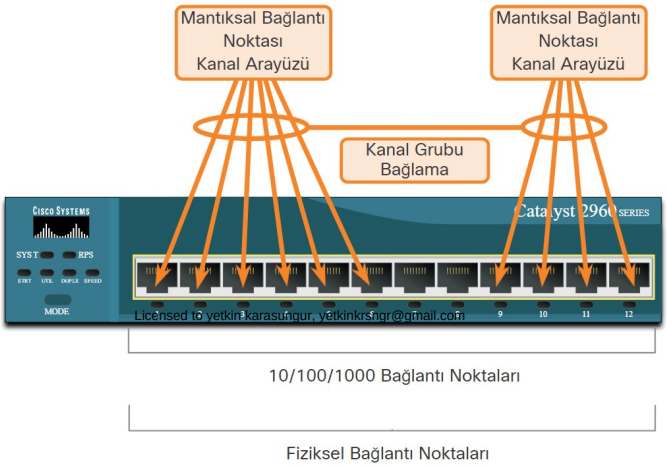
EtherChannel teknolojisinin aşağıdakiler dahil birçok avantajı vardır:

- Çoğu yapılandırma görevi, her bir bağlantı noktası yerine EtherChannel arabiriminde yapılabilir ve bağlantılar boyunca yapılandırma tutarlılığı sağlanır.
- EtherChannel, mevcut anahtar bağlantı noktalarına dayanır. Daha fazla bant genişliğine sahip olmak için bağlantıyı daha hızlı ve daha pahalı bir bağlantıya yükseltmeye gerek yoktur.
- Yük dengeleme, aynı EtherChannel'in parçası olan bağlantılar arasında gerçekleşir. Donanım platformuna bağlı olarak, bir veya daha fazla yük dengeleme yöntemi uygulanabilir. Bu yöntemler, fiziksel bağlantılar üzerinden kaynak MAC ve hedef MAC yük dengelemesini veya kaynak IP ve hedef IP yük dengelemesini içerir.
- EtherChannel, tek bir mantıksal bağlantı olarak görülen bir toplama oluşturur. İki anahtar arasında birkaç EtherChannel paketi bulunduğunda, STP, anahtarlama döngülerini önlemek için paketlerden birini engelleyebilir. STP yedek bağlantılardan birini engellediğinde, tüm EtherChannel'ı engeller. Bu, o EtherChannel bağlantısına ait tüm bağlantı noktalarını engeller. Yalnızca bir EtherChannel bağlantısının olduğu yerlerde, EtherChannel'daki tüm fiziksel bağlantılar etkindir çünkü STP yalnızca bir (mantıksal) bağlantı görür.
- EtherChannel, genel bağlantı tek bir mantıksal bağlantı olarak görüldüğü için yedeklilik sağlar. Ek olarak, kanal içindeki bir fiziksel bağlantının kaybı topolojide bir değişiklik yaratmaz. Bu nedenle, genişleyen bir ağaç yeniden hesaplaması gerekli değildir. En az bir fiziksel bağlantının mevcut olduğunu varsayarsak; EtherChannel, EtherChannel içindeki kayıp bir bağlantı nedeniyle toplam verimi düşse bile işlevsel kalır.

## 22.2.4.Uygulama Kısıtlamaları

EtherChannel, aşağıdakiler dahil olmak üzere belirli uygulama kısıtlamalarına sahiptir:

- Arayüz türleri karıştırılamaz. Örneğin, Hızlı Ethernet ve Gigabit Ethernet tek bir EtherChannel içinde karıştırılamaz.
- Şu anda her bir EtherChannel, sekiz adede kadar uyumlu şekilde yapılandırılmış Ethernet bağlantı noktasından oluşabilir. EtherChannel, bir anahtar ile başka bir anahtar veya ana bilgisayar arasında 800 Mbps'ye (Hızlı EtherChannel) veya 8 Gbps'ye (Gigabit EtherChannel) kadar tam çift yönlü bant genişliği sağlar.
- Cisco Catalyst 2960 Katman 2 anahtarı şu anda altı adede kadar EtherChannel'ı desteklemektedir. Bununla birlikte, yeni IOS'lar geliştirildikçe ve platformlar değiştikçe, bazı kartlar ve platformlar bir EtherChannel bağlantısı içinde artan sayıda bağlantı noktasını destekleyebilir ve ayrıca artan sayıda Gigabit EtherChannel'ı destekleyebilir.
- Ayrı EtherChannel grup üye bağlantı noktası yapılandırması her iki cihazda da tutarlı olmalıdır. Bir tarafın fiziksel bağlantı noktaları ana hat olarak yapılandırılırsa, diğer tarafın fiziksel bağlantı noktaları da aynı yerel VLAN içinde ana hatlar olarak yapılandırılmalıdır. Ek olarak, her EtherChannel bağlantısındaki tüm bağlantı noktaları, Katman 2 bağlantı noktaları olarak yapılandırılmalıdır.
- Her EtherChannel, şekilde gösterildiği gibi mantıksal bir port kanal arayüzüne sahiptir. Bağlantı noktası kanal arayüzüne uygulanan bir konfigürasyon, o arayüze atanan tüm fiziksel arayüzleri etkiler.



## 22.2.5.Otomatik Anlaşma (AutoNegotiation) Protokolleri

EtherChannels, iki protokolden biri, Port Aggregation Protocol (PAgP) veya Link Aggregation Control Protocol (LACP) kullanılarak müzakere yoluyla oluşturulabilir. Bu protokoller, benzer özelliklere sahip bağlantı noktalarının, bitişik anahtarlarla dinamik görüşme yoluyla bir kanal oluşturmasına izin verir.

Not : PAgP veya LACP olmadan statik veya koşulsuz bir EtherChannel'i yapılandırmak da mümkündür.

## PAgP Protokolü

PAgP ("Pag - P" olarak telaffuz edilir), EtherChannel bağlantılarının otomatik olarak oluşturulmasına yardımcı olan Cisco'ya özel bir protokoldür. Bir EtherChannel bağlantısı PAgP kullanılarak yapılandırıldığında, PAgP paketleri, bir kanalın oluşturulması için görüşmek üzere EtherChannel özellikli bağlantı noktaları arasında gönderilir. PAgP, eşleşen Ethernet bağlantılarını belirlediğinde, bağlantıları bir EtherChannel'da gruplandırır. EtherChannel, kapsama ağacına tek bir bağlantı noktası olarak eklenir.

PAgP etkinleştirildiğinde EtherChannel'i de yönetir. PAgP paketleri her 30 saniyede gönderilir. PAgP, yapılandırma tutarlılığını kontrol eder ve iki anahtar arasındaki bağlantı eklemelerini ve arızalarını yönetir. Bir EtherChannel oluşturulduğunda, tüm portların aynı tip konfigürasyona sahip olmasını sağlar.

Not : EtherChannel'da, tüm bağlantı noktalarının aynı hıza, çift yönlü ayarlara ve VLAN bilgilerine sahip olması zorunludur. Kanalın yaratılmasından sonra herhangi bir port-kanal değişikliği, toplanan kanal portlarını da değiştirir.

PAgP, her bir tarafın konfigürasyonunu tespit ederek ve bağlantıların uyumlu olmasını sağlayarak EtherChannel bağlantısını oluşturmaya yardımcı olur, böylece EtherChannel bağlantısı gerektiğinde etkinleştirilebilir. PAgP için modlar aşağıdaki gibidir:

- Açık (On)- Bu mod, arayüzü PAgP'siz kanala zorlar. Açık modunda yapılandırılan arayüzler PAgP paketlerini değiştirmez.
- PAgP Desirable- Bu PAgP modu, arayüzün PAgP paketleri göndererek diğer arayüzlerle görüşmeleri başlattığı aktif bir görüşme durumuna bir arayüze yerleştirir.
- PAgP auto - Bu PAgP modu, arayüzün aldığı PAgP paketlerine yanıt verdiği ancak PAgP anlaşmasını başlatmadığı pasif bir anlaşma durumuna bir arayüze yerleştirir.

Modlar her iki tarafta da uyumlu olmalıdır. Bir taraf otomatik modda olacak şekilde yapılandırılmışsa, diğer tarafın EtherChannel anlaşmasını başlatmasını beklerken, pasif duruma getirilir. Diğer taraf da otomatik olarak ayarlanmışsa, görüşme asla başlamaz ve EtherChannel oluşmaz. Tüm modlar no komutu kullanılarak devre dışı bırakılırsa veya hiçbir mod yapılandırılmazsa, EtherChannel devre dışı bırakılır.

Açık modu, arayüzü herhangi bir görüşme yapmadan manuel olarak bir EtherChannel'a yerleştirir. Yalnızca diğer taraf da açık olarak ayarlanmışsa çalışır. Diğer taraf PAgP aracılığıyla parametreler üzerinde anlaşma sağlayacak şekilde ayarlanmışsa, EtherChannel formu oluşmaz çünkü açık moduna ayarlanan taraf anlaşmaz.

İki anahtar arasında anlaşma olmaması, EtherChannel'daki tüm bağlantıların diğer tarafta sona erdiğinden veya diğer anahtarda PAgP uyumluluğunun olduğundan emin olmak için kontrol yapılmadığı anlamına gelir.

## PAgP Modu Ayarları Örneği

Şekildeki iki anahtara bakınız. S1 ve S2'nin PAgP kullanarak bir EtherChannel oluşturup oluşturmadığı, kanalın her iki tarafındaki mod ayarlarına bağlıdır.

Licensed to yetkin karasungur, yetkinkarasungur@gmail.com

Tablo, S1 ve S2'deki çeşitli PAgP modları kombinasyonunu ve bunun sonucunda ortaya çıkan kanal kurulumunu gösterir.

**PAgP Modları**

| S1 | S2 | Kanal Kurulumu |
|---|---|---|
| On | On | Evet |
| On | Desirable/Auto | Hayır |
| Desirable | Desirable | Evet |
| Desirable | Auto | Evet |
| Auto | Desirable | Evet |
| Auto | Auto | Hayır |

## 22.2.6.LACP Protokolü

LACP, birkaç fiziksel bağlantı noktasının tek bir mantıksal kanal oluşturmak için paketlenmesine izin veren bir IEEE spesifikasyonunun (802.3ad) bir parçasıdır. LACP, bir anahtarın LACP paketlerini diğer anahtara göndererek otomatik bir paket üzerinde anlaşmasına izin verir. Cisco EtherChannel ile PAgP'ye benzer bir işlevi yerine getirir. LACP bir IEEE standardı olduğundan, çok satıcılı ortamlarda EtherChannel'ları kolaylaştırmak için kullanılabilir. Cisco cihazlarında her iki protokol de desteklenir.

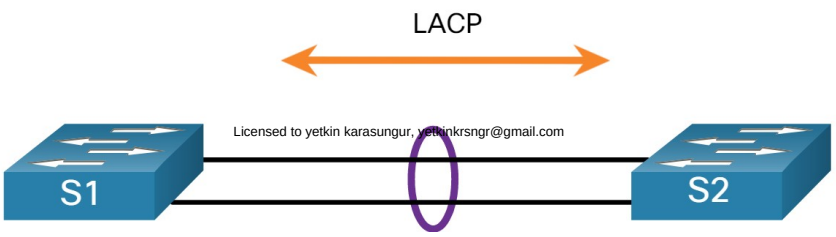
Not : LACP başlangıçta IEEE 802.3ad olarak tanımlanmıştır. Ancak, LACP artık yerel ve metropolitan alan ağları için daha yeni olan IEEE 802.1AX standardında tanımlanmaktadır.

LACP, PAgP ile aynı müzakere avantajlarını sağlar. LACP, her bir tarafın konfigürasyonunu algılayarak ve uyumlu olduklarından emin olarak EtherChannel bağlantısını oluşturmaya yardımcı olur, böylece EtherChannel bağlantısı gerektiğinde etkinleştirilebilir. LACP için modlar aşağıdaki gibidir:

Açık(On) - Bu mod, arayüzü LACP'siz kanala zorlar. Açık modunda yapılandırılan arayüzler LACP paketlerini değiştirmez.
LACP etkin(active) - Bu LACP modu, bir bağlantı noktasını etkin bir anlaşma durumuna yerleştirir. Bu durumda, bağlantı noktası, LACP paketleri göndererek diğer bağlantı noktaları ile görüşmeleri başlatır.
LACP pasif (passive) - Bu LACP modu, bir bağlantı noktasını pasif anlaşma durumuna yerleştirir. Bu durumda, bağlantı noktası aldığı LACP paketlerine yanıt verir, ancak LACP paket görüşmesini başlatmaz.
PAgP'de olduğu gibi, EtherChannel bağlantısının oluşması için modların her iki tarafta da uyumlu olması gerekir. Açık modu tekrarlanır, çünkü EtherChannel konfigürasyonunu koşulsuz olarak PAgP veya LACP dinamik anlaşması olmadan oluşturur.

LACP, sekiz aktif bağlantıya ve ayrıca sekiz bekleme bağlantısına izin verir. Mevcut aktif bağlantılardan birinin başarısız olması durumunda bir bekleme bağlantısı etkin hale gelecektir.

**LACP Modu Ayarları Örneği**
Şekildeki iki anahtarlara bakınız. S1 ve S2'nin LACP kullanarak bir EtherChannel oluşturup oluşturmayacağı, kanalın her iki tarafındaki mod ayarlarına bağlıdır.



Licensed to yetkin karasungur, yetinkrsngr@gmail.com

Tablo, S1 ve S2'deki LACP modlarının çeşitli kombinasyonunu ve bunun sonucunda oluşan kanal kurulum sonucunu gösterir.

**LACP Modları**

| S1 | S2 | Kanal Kurulumu |
|---|---|---|
| Açık | Açık | Evet |
| Açık | Aktif/ pasif | Hayır |
| Aktif | Aktif | Evet |
| Aktif | Pasif | Evet |
| Pasif | Aktif | Evet |
| Pasif | Pasif | Hayır |

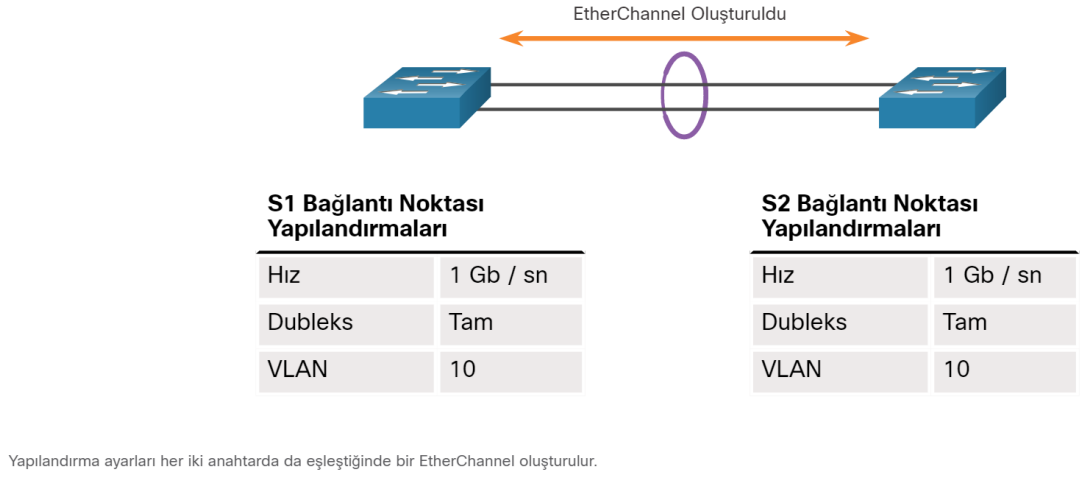
## 22.3.Etherchannel Yapılandırması

### 22.3.1.Yapılandırma Yönergeleri

Artık EtherChannel'in ne olduğunu bildiğinize göre, bu konu onu nasıl yapılandıracağınızı açıklıyor. Aşağıdaki yönergeler ve kısıtlamalar, EtherChannel'i yapılandırmak için kullanışlıdır:

- EtherChannel desteği - Tüm Ethernet arabirimleri, arabirimlerin fiziksel olarak bitişik olması gerekmeden EtherChannel'i desteklemelidir.
- Hız ve çift yönlü - Bir EtherChannel'daki tüm arayüzleri aynı hızda ve aynı çift yönlü modda çalışacak şekilde yapılandırın.
- VLAN eşleşmesi - EtherChannel paketindeki tüm arabirimler aynı VLAN'a atanmalı veya bir ana hat olarak yapılandırılmalıdır (şekilde gösterilmiştir).
- VLAN aralığı - Bir EtherChannel, bir kanal EtherChannel'daki tüm arabirimlerde aynı izin verilen VLAN aralığını destekler. İzin verilen VLAN aralığı aynı değilse, arabirimler otomatik veya istenen moda ayarlandıklarında bile bir EtherChannel oluşturmazlar .

Şekil, bir EtherChannel'in S1 ve S2 arasında oluşmasına izin verecek bir konfigürasyonu göstermektedir.



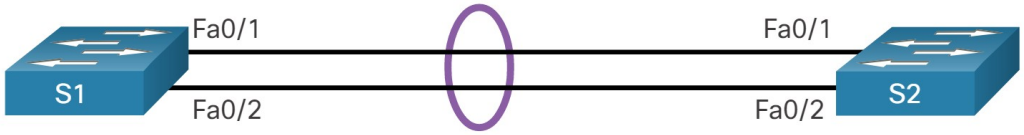

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bu ayarların değiştirilmesi gerekiyorsa, bunları bağlantı noktası kanalı arabirimi yapılandırma modunda yapılandırın. Bağlantı noktası kanalı arayüzüne uygulanan herhangi bir konfigürasyon aynı zamanda bireysel arayüzleri de etkiler. Ancak, ayrı arabirimlere uygulanan konfigürasyonlar, bağlantı noktası kanalı arabirimini etkilemez. Bu nedenle, bir EtherChannel bağlantısının parçası olan bir arayüzde konfigürasyon değişiklikleri yapmak, arayüz uyumluluk sorunlarına neden olabilir.

Bağlantı noktası kanalı erişim modunda, ana hat modunda (en yaygın) veya yönlendirilmiş bir bağlantı noktasında yapılandırılabilir.

## LACP Yapılandırma Örneği

EtherChannel varsayılan olarak devre dışıdır ve yapılandırılmalıdır. Şekildeki topoloji, LACP kullanılarak bir EtherChannel konfigürasyon örneğini göstermek için kullanılacaktır.




EtherChannel'ı LACP ile yapılandırmak için aşağıdaki üç adım gerekir:

Adım 1. **interface range** global konfigürasyon modu komutunu kullanarak EtherChannel grubunu oluşturan arayüzleri belirtin . **range** anahtar kelimesi birkaç arayüzü seçip hepsini yapılandırmanıza izin verir.

Adım 2. Arayüz aralığı konfigürasyon modunda **channel-group identifier mode active** komutuyla port kanal arayüzünü oluşturun . Tanımlayıcı, bir kanal grubu numarasını belirtir. **mode activ**e anahtar kelimeleri bir LACP EtherChannel yapılandırma olarak bunu tanımlar.

Adım 3. Port kanal arayüzünde Katman 2 ayarlarını değiştirmek için, **interface port-channel** komutunu ve ardından arayüz tanımlayıcısını kullanarak port kanalı arayüz konfigürasyon moduna girin . Örnekte S1, bir LACP EtherChannel ile yapılandırılmıştır. Bağlantı noktası kanalı, belirtilen izin verilen VLAN'larla bir ana hat arabirimi olarak yapılandırılır.

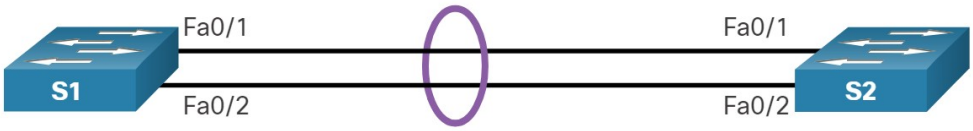
```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config)# interface port-channel 1
S1(config)# switchport mode trunk
S1(config)# switchport trunk allowed vlan 1,2,20
```

## 22.4.Etherchannel Yapılandırması Doğrulama

Her zaman olduğu gibi, ağınızdaki cihazları yapılandırırken, yapılandırmanızı doğrulamanız gerekir. Sorunlar varsa, bunları giderebilmeniz ve düzeltmeniz de gerekecektir. Bu konu size doğrulama komutlarının yanı sıra bazı yaygın EtherChannel ağ sorunları ve bunların çözümlerini verir.

Doğrulama komutu örnekleri, şekilde gösterilen topolojiyi kullanacaktır.

Licensed to yetkin kırasaoğlu ketkikrsnr@gmail.com




**show interfaces port-channel** komutu port kanal arayüzünün genel durumunu görüntüler. Şekilde, Port Channel 1 arayüzü yukarı yani etkin durumdadır.

```
S1# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is c07b.bcc4.a981 (bia c07b.bcc4.a981)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
(output omitted)
```

Aynı cihaz üzerinde birkaç bağlantı noktası kanalı arabirimi yapılandırıldığında, bağlantı noktası kanalı başına bir satır bilgi görüntülemek için **show etherchannel summary** komutunu kullanın. Çıkışta, anahtarın yapılandırılmış bir EtherChannel'ı vardır; grup 1 LACP kullanır.

Arabirim paketi FastEthernet0 / 1 ve FastEthernet0 / 2 arabirimlerinden oluşur. Grup bir Katman 2 EtherChannel'dır ve port kanal numarasının yanındaki SU harfleriyle belirtildiği gibi kullanımdadır.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/1(P)    Fa0/2(P)
```

Çıktıda gösterildiği gibi, belirli bir bağlantı noktası kanalı arabirimi hakkındaki bilgileri görüntülemek için **show etherchannel port-channel** komutunu kullanın. Örnekte, Bağlantı Noktası Kanal 1 arabirimi iki fiziksel arabirimden oluşur: FastEthernet0 / 1 ve FastEthernet0 / 2. Aktif modda LACP kullanır. Uyumlu bir konfigürasyona sahip başka bir anahtara düzgün şekilde bağlanmıştır, bu nedenle bağlantı noktası kanalının kullanımda olduğu söylenir.

```
S1# show etherchannel port-channel
                Channel-group listing:
                ----------------------
Group: 1
----------
                Port-channels in the group:
                ---------------------------
Port-channel: Po1    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:01h:02m:10s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Load share deferral = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             0
  0     00     Fa0/2    Active             0
Time since last port bundled:    0d:00h:09m:30s    Fa0/2
```

Licensed to

Bir EtherChannel paketinin herhangi bir fiziksel arayüz üyesinde, **show interfaces etherchannel** komutu, çıktıda gösterildiği gibi EtherChannel'daki arayüzün rolü hakkında bilgi sağlayabilir. FastEthernet0 / 1 arayüzü, EtherChannel paket 1'in bir parçasıdır. Bu EtherChannel'in protokolü LACP'dir.

```
S1# show interfaces f0/1 etherchannel
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                            LACP port     Admin     Oper    Port
Port      Flags   State     Priority      Key       Number  State
Fa0/1     SA      bndl      32768         0x1       0x1     0x102       0x3D
Partner's information:
                  LACP port                         Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age     key    Key    Number  State
Fa0/1     SA      32768     c025.5cd7.ef00  12s     0x0    0x1    0x102   0x3Dof the port in the current
state: 0d:00h:11m:51sllowed vlan 1,2,20
```

## 22.5.EtherChannel Yapılandırmalarında Sık Karşılaşılan Sorunlar

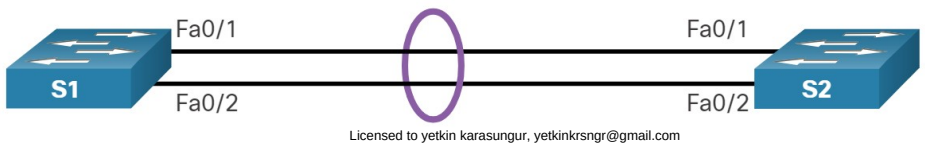
Bir EtherChannel içindeki tüm arabirimler aynı hız ve çift yönlü mod yapılandırmasına, ana hatlarda yerel ve izin verilen VLAN'lara ve erişim bağlantı noktalarında VLAN'a erişime sahip olmalıdır. Bu yapılandırmaların sağlanması, EtherChannel ile ilgili ağ sorunlarını önemli ölçüde azaltacaktır. Yaygın EtherChannel sorunları şunları içerir:

- EtherChannel'da atanan bağlantı noktaları aynı VLAN'ın parçası değildir veya ana hat olarak yapılandırılmamıştır. Farklı yerel VLAN'lara sahip bağlantı noktaları bir EtherChannel oluşturamaz.
- Trunking, EtherChannel'ı oluşturan bazı bağlantı noktalarında yapılandırıldı, ancak hepsinde değil. EtherChannel'i oluşturan bağımsız bağlantı noktalarında trank modunu yapılandırmanız önerilmez. Bir EtherChannel üzerinde bir trank yapılandırırken, EtherChannel'daki trunking modunu doğrulayın.
- İzin verilen VLAN aralığı aynı değilse, PAgP otomatik veya istenen moda ayarlandığında bile portlar bir EtherChannel oluşturmaz .
- PAgP ve LACP için dinamik anlaşma seçenekleri, EtherChannel'in her iki ucunda da uyumlu şekilde yapılandırılmamıştır.

Not : PAgP veya LACP'yi DTP ile karıştırmak kolaydır, çünkü bunların tümü ana hat bağlantılarındaki davranışı otomatikleştirmek için kullanılan protokollerdir. PAgP ve LACP, bağlantı birleştirme (EtherChannel) için kullanılır. DTP, ana hat bağlantılarının oluşturulmasını otomatikleştirmek için kullanılır. Bir EtherChannel trunk yapılandırıldığında, tipik olarak önce EtherChannel (PAgP veya LACP) ve ardından DTP yapılandırılır.

## Etherchannel Sorun Giderme Örneği

Şekilde, S1 ve S2 anahtarlarındaki F0 / 1 ve F0 / 2 arayüzleri bir EtherChannel ile bağlanmıştır. Ancak, EtherChannel çalışmıyor.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Adım 1. EtherChannel Özet Bilgilerini Görüntüleyin

**Show etherchannel summary** komutunun çıktısı , EtherChannel'in çalışmadığını gösterir.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SD)         -      Fa0/1(D)    Fa0/2(D)
```

### Adım 2. Bağlantı Noktası Kanal Yapılandırmasını Görüntüleyin

**show run | begin interface port-channel** , daha ayrıntılı çıktısı, S1 ve S2'de yapılandırılmış uyumsuz PAgP modlarının olduğunu gösterir.

```
S1# show run | begin interface port-channel
interface Port-channel1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode on
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode on
!=====================================
S2# show run | begin interface port-channel
interface Port-channel1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
!
interface FastEthernet0/1
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode desirable
!
interface FastEthernet0/2
 switchport trunk allowed vlan 1,2,20
 switchport mode trunk
 channel-group 1 mode desirable
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 3. Adım: Yanlış Yapılandırmayı Düzeltin

Sorunu düzeltmek için, EtherChannel'daki PAgP modu **desirable** olarak değiştirildi.

Not : EtherChannel ve STP birlikte çalışmalıdır. Bu nedenle, EtherChannel ile ilgili komutların girildiği sıra önemlidir, bu nedenle doğrudan değiştirilmenin aksine Port-Channel 1 arayüzünün kaldırıldığını ve daha sonra kanal grubu komutuyla yeniden eklendiğini görüyorsunuz . Yapılandırmayı doğrudan değiştirmeye çalışırsanız, STP hataları ilişkili bağlantı noktalarının engelleme veya hata devre dışı bırakma durumuna geçmesine neden olur.

```
S1(config)# no interface port-channel 1
S1(config)# interface range fa0/1 - 2
S1(config-if-range)# channel-group 1 mode desirable
Creating a port-channel interface Port-channel 1
S1(config-if-range)# no shutdown
S1(config-if-range)# exit
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

### Adım 4. EtherChannel'in Çalışır durumda olduğunu doğrulayın

EtherChannel artık **show etherchannel summary** komutunun çıktısı ile doğrulanarısa aktif olduğu görülür. .

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         PAgP      Fa0/1(P)    Fa0/2(P)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 23.Bölüm:DHCP

## 23.1.DHCP Kavramları

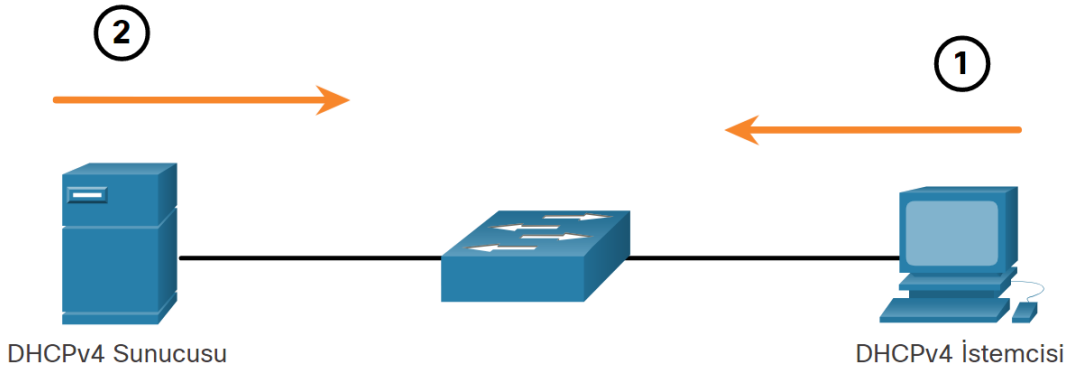
### 23.1.1.DHCP Sunucu ve İstemci

Dinamik Ana Bilgisayar Yapılandırma Protokolü v4-Dynamic Host Configuration Protocol (DHCPv4), IPv4 adreslerini ve diğer ağ yapılandırma bilgilerini dinamik olarak atar. Masaüstü istemcileri tipik olarak ağ düğümlerinin çoğunu oluşturduğundan, DHCPv4 ağ yöneticileri için son derece kullanışlı ve zaman kazandıran bir araçtır.

Özel bir DHCPv4 sunucusu ölçeklenebilir ve yönetimi nispeten kolaydır. Bununla birlikte, küçük bir şubede veya SOHO konumunda, bir Cisco yönlendirici, özel bir sunucuya ihtiyaç duymadan DHCPv4 hizmetleri sağlayacak şekilde yapılandırılabilir. Cisco IOS yazılımı, isteğe bağlı, tam özellikli bir DHCPv4 sunucusunu destekler.

DHCPv4 sunucusu, sunucu tarafından seçilen sınırlı bir süre için veya istemcinin artık adrese ihtiyacı kalmayana kadar bir adres havuzundan bir IPv4 adresini dinamik olarak atar veya kiralar.

İstemciler, idari olarak tanımlanmış bir süre için sunucudan bilgileri kiralar. Yöneticiler, DHCPv4 sunucularını farklı aralıklarla kiralamaların zaman aşımına uğraması için ayarlamak üzere yapılandırır. Kira, genellikle 24 saat ile bir hafta arasında veya daha uzun bir süredir. Kira süresi sona erdiğinde, müşterinin genellikle aynı adresi yeniden tahsis etmesine rağmen, istemci başka bir adres istemelidir.




1. DHCPv4 kiralama işlemi, istemcinin bir DHCP sunucusunun hizmetlerini talep eden bir mesaj göndermesiyle başlar.
2. Mesajı alan bir DHCPv4 sunucusu varsa, bir IPv4 adresi ve olası diğer ağ yapılandırma bilgileriyle yanıt verecektir.

#### DHCPv4 İşlemi

DHCPv4 bir istemci / sunucu modunda çalışır. Bir istemci bir DHCPv4 sunucusuyla iletişim kurduğunda, sunucu bu istemciye bir IPv4 adresi atar veya kiralar. İstemci, kiralama süresi dolana kadar bu kiralık IPv4 adresiyle ağa bağlanır. İstemci, kira sözleşmesini uzatmak için periyodik olarak DHCP sunucusuyla iletişim kurmalıdır. Bu kiralama mekanizması, taşınan veya kapatılan istemcilerin artık ihtiyaç duymadıkları adresleri tutmamalarını sağlar. Bir kira süresi sona erdiğinde, DHCP sunucusu adresi gerektiği gibi yeniden tahsis edilebileceği havuza geri gönderir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

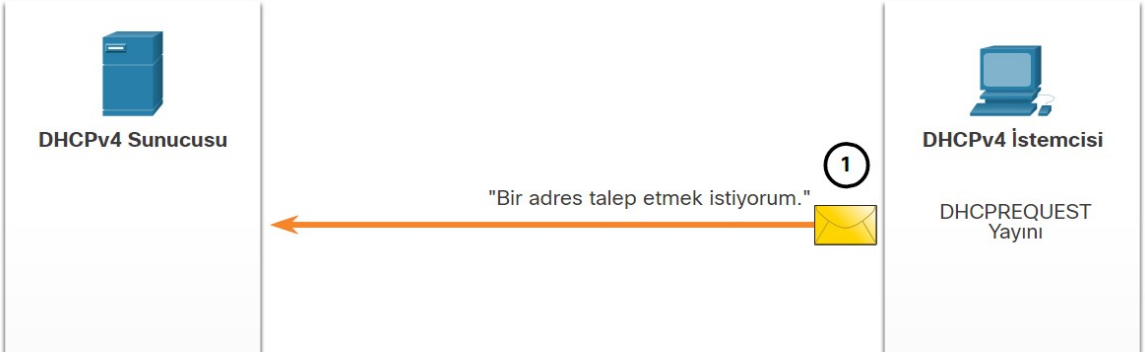
## Adres Atama Adımları

İstemci önyükleme yaptığında (veya başka bir şekilde bir ağa katılmak istediğinde), bir ip kiralamak için dört aşamalı bir süreç başlatır:

DHCP Keşfi (DHCPDISCOVER)
DHCP Teklifi (DHCPOFFER)
DHCP İsteği (DHCPREQUEST)
DHCP Alındı Bildirimi (DHCPACK)

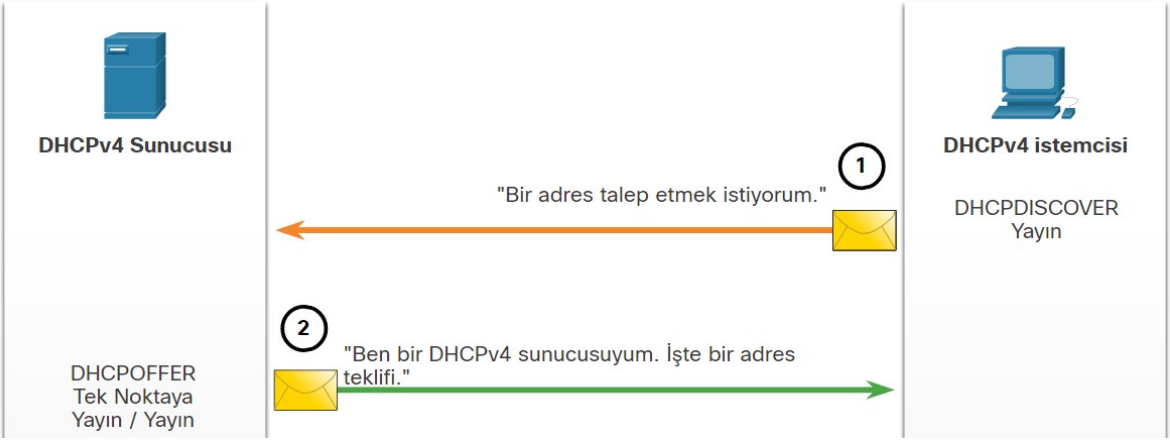
### Adım 1. DHCP Keşfi (DHCPDISCOVER)

İstemci, mevcut DHCPv4 sunucularını keşfetmek için kendi MAC adresine sahip bir yayın DHCPDISCOVER mesajı kullanarak işlemi başlatır. İstemci açılışta geçerli IPv4 bilgisine sahip olmadığından, sunucuyla iletişim kurmak için Katman 2 ve Katman 3 yayın adreslerini kullanır. DHCPDISCOVER mesajının amacı, ağdaki DHCPv4 sunucularını bulmaktır.




### Adım 2. DHCP Teklifi (DHCPOFFER)

DHCPv4 sunucusu bir DHCPDISCOVER mesajı aldığında, istemciye kiralamak için kullanılabilir bir IPv4 adresi ayırır. Sunucu ayrıca, talepte bulunan istemcinin MAC adresinden ve istemcinin kiralanan IPv4 adresinden oluşan bir ARP girişi oluşturur. DHCPv4 sunucusu, talep eden istemciye  DHCPOFFER mesajını gönderir.

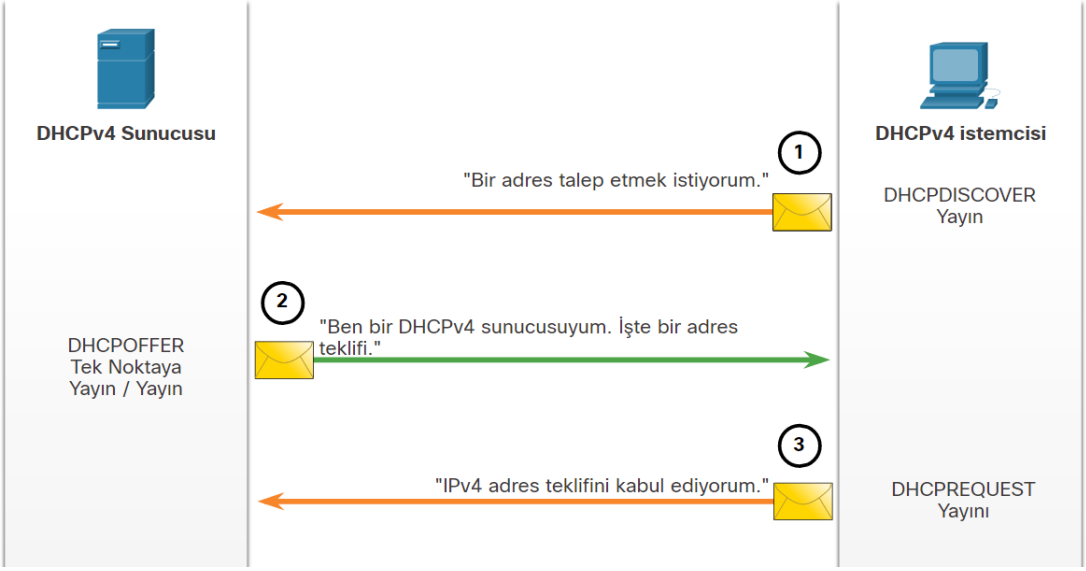



### Adım 3. DHCP İsteği (DHCPREQUEST)

İstemci sunucudan DHCPOFFER'ı aldığında, bir DHCPREQUEST mesajı gönderir. Bu mesaj hem kira başlangıcı hem de kira yenileme için kullanılır. Kira oluşturma için kullanıldığında, DHCPREQUEST, sunduğu parametreler için seçilen sunucuya bağlayıcı bir kabul bildirimi ve müşteriye bağlayıcı bir teklif sunabilecek diğer sunucular için örtük bir reddetme işlevi görür.

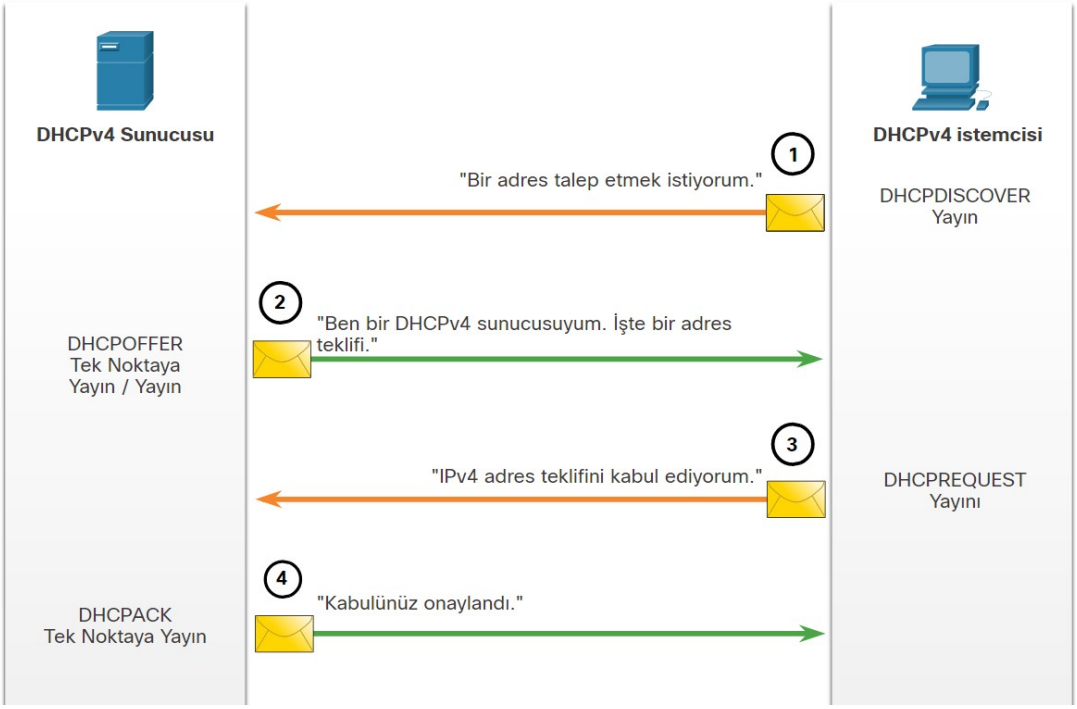
Licensed to yetkin karasungur, yetkinkrshgr@gmail.com

Birçok kurumsal ağ, birden çok DHCPv4 sunucusu kullanır. DHCPREQUEST mesajı, bu DHCPv4 sunucusunu ve diğer DHCPv4 sunucularını kabul edilen teklif hakkında bilgilendirmek için bir yayın biçiminde gönderilir.




### Adım 4. DHCP Alındı Bildirimi (DHCPACK)

DHCPREQUEST mesajını aldıktan sonra, sunucu, halihazırda kullanılmadığından emin olmak için bu adrese bir ICMP pingiyle kira bilgilerini doğrulayabilir, istemci kirası için yeni bir ARP girişi oluşturacak ve bir DHCPACK mesajı ile yanıt verecektir. DHCPACK mesajı, mesaj tipi alanındaki bir değişiklik dışında DHCPOFFER'ın bir kopyasıdır. İstemci DHCPACK mesajını aldığında, yapılandırma bilgisini günlüğe kaydeder ve atanan adres için bir ARP araması gerçekleştirebilir. ARP'ye yanıt gelmezse, istemci IPv4 adresinin geçerli olduğunu bilir ve kendi adresi olarak kullanmaya başlar.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Kira Sözleşmesini Yenileme Adımları**

Kira süresinin sona ermesinden önce, müşteri, şekilde gösterildiği gibi DHCPv4 sunucusuyla kira sözleşmesini yenilemek için iki aşamalı bir süreç başlatır:

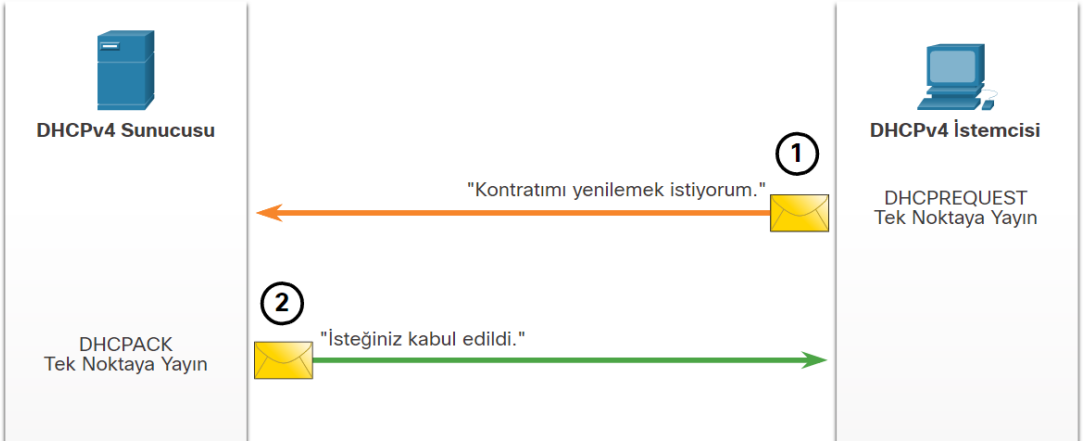
1 . DHCP İsteği (DHCPREQUEST)

Kira süresi sona ermeden önce, istemci, ilk olarak IPv4 adresini sunan DHCPv4 sunucusuna doğrudan bir DHCPREQUEST iletisi gönderir. Bir DHCPACK belirli bir süre içinde alınmazsa, istemci başka bir DHCPREQUEST yayınlar, böylece diğer DHCPv4 sunucularından biri kira süresini uzatabilir.

2 . DHCP Alındı Bildirimi (DHCPACK)

DHCPREQUEST mesajını aldığında, sunucu bir DHCPACK göndererek kira bilgilerini doğrular.

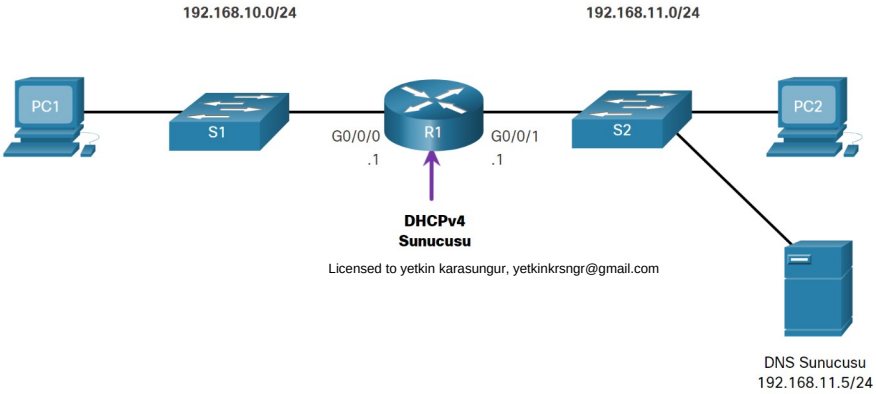
Not : Bu mesajlar (öncelikle DHCPOFFER ve DHCPACK), IETF RFC 2131'e göre tek noktaya yayın veya yayın olarak gönderilebilir.




## 23.2.Cisco IOS DHCP Sunucusunu Yapılandırma

### 23.2.1.Cisco IOS DHCPv4 Sunucusu

Artık DHCPv4'ün nasıl çalıştığı ve işinizi nasıl biraz daha kolaylaştırabileceği konusunda temel bir anlayışa sahipsiniz. Ayrı bir DHCPv4 sunucunuz yoksa, bu konu size bir Cisco IOS yönlendiricisinin bir Cisco IOS DHCP yönlendiricisi gibi davranması için nasıl yapılandırılacağını gösterecektir. Cisco IOS yazılımını çalıştıran bir Cisco yönlendirici, bir DHCPv4 sunucusu görevi görecek şekilde yapılandırılabilir. Cisco IOS DHCPv4 sunucusu, yönlendirici içindeki belirli adres havuzlarından DHCPv4 istemcilerine IPv4 adresleri atar ve yönetir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Cisco IOS DHCPv4 Sunucusunu Yapılandırma Adımları

Bir Cisco IOS DHCPv4 sunucusunu yapılandırmak için aşağıdaki adımları kullanın:

1. Adım . IPv4 adreslerini hariç tutun.
2. Adım . DHCPv4 havuz adı tanımlayın.
3. Adım . DHCPv4 havuzunu yapılandırın.

### Adım 1. IPv4 Adreslerini Hariç Tutun

DHCPv4 sunucusu olarak işlev gören yönlendirici, belirli adresleri dışlayacak şekilde yapılandırılmadığı sürece bir DHCPv4 adres havuzundaki tüm IPv4 adreslerini atar. Tipik olarak, bir havuzdaki bazı IPv4 adresleri, statik adres atamaları gerektiren ağ cihazlarına atanır. Bu nedenle, bu IPv4 adresleri başka cihazlara atanmamalıdır. IPv4 adreslerini dışlamak için komut sözdizimi aşağıdaki gibidir:

```
Router(config)# ip dhcp excluded-address low-address [high-address]
```

Tek bir adres veya bir adres aralığı, aralığın düşük adresi ve yüksek adresi belirtilerek hariç tutulabilir . Dışarıda bırakılan adresler, yönlendiricilere, sunuculara, yazıcılara ve manuel olarak yapılandırılmış veya yapılandırılacak diğer cihazlara atanan adresler olmalıdır. Komutu birden çok kez de girebilirsiniz.

### Adım 2. DHCPv4 Havuz Adı Tanımlayın

Bir DHCPv4 sunucusunun yapılandırılması, atanacak bir adres havuzunun tanımlanmasını içerir.

Örnekte gösterildiği gibi, **ip dhcp pool pool-name** komutu belirtilen ada sahip bir havuz oluşturur ve yönlendiriciyi Router (dhcp-config) # istemiyle tanımlanan DHCPv4 yapılandırma moduna geçirir.

Havuzu tanımlamak için kullanılan komut sözdizimi aşağıdaki gibidir:

```
Router(config)# ip dhcp pool pool-name
Router(dhcp-config)#
```

### Adım 3. DHCPv4 Havuzunu Yapılandırın

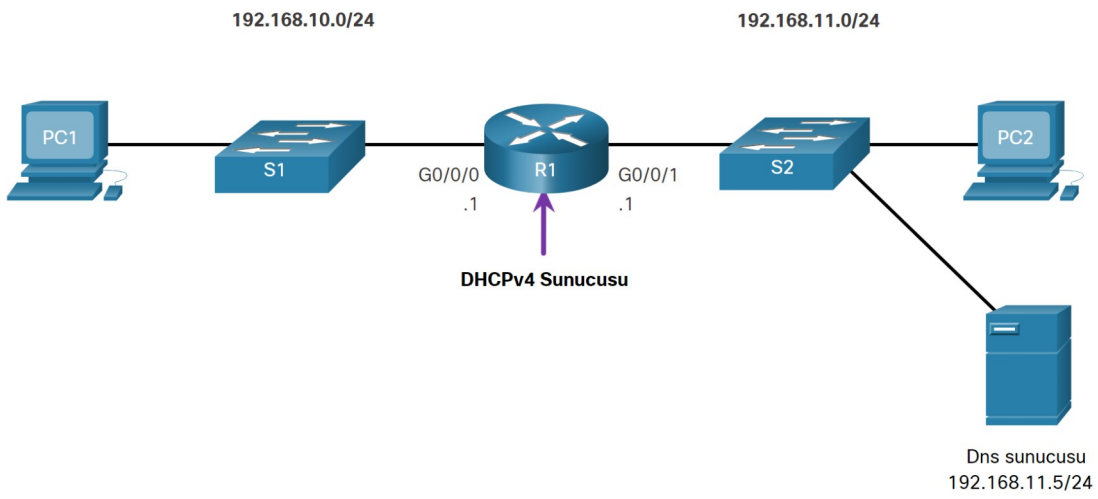
Aşağıdaki tablo, DHCPv4 havuzu yapılandırmasını tamamlamak için gereken görevleri listeler.
Adres havuzu ve varsayılan ağ geçidi yönlendiricisi yapılandırılmalıdır. Kullanılabilir adres aralığını tanımlamak için **network** ifadesini kullanın . **default-router** varsayılan ağ geçidi yönlendirici tanımlamak için kullanılan komuttur. Tipik olarak, ağ geçidi, istemci cihazlara en yakın yönlendiricinin LAN arayüzüdür. Bir ağ geçidi gereklidir, ancak birden fazla ağ geçidi varsa sekize kadar adres listeleyebilirsiniz.
Diğer DHCPv4 havuz komutları isteğe bağlıdır. Örneğin, bir DHCPv4 istemcisinin kullanabildiği DNS sunucusunun IPv4 adresi, **dns-server** komutu kullanılarak yapılandırılır . **domain-name** komutu alan adı tanımlamak için kullanılır. DHCPv4 kiralama süresi, **lease** komutu kullanılarak değiştirilebilir . Varsayılan kira değeri bir gündür. **netbios-name-server** komutu NetBIOS WINS sunucusu tanımlamak için kullanılır.

| Görev | IOS Komutu |
|---|---|
| Adres havuzunu tanımlayın. | `network network-number [mask \| / prefix-length]` |
| Varsayılan yönlendiriciyi veya ağ geçidini tanımlayın. | `default-router address [ address2….address8]` |
| Bir DNS sunucusu tanımlayın. | `dns-server address [ address2…address8]` |
| Alan adını tanımlayın. | `domain-name domain` |
| DHCP kiralamasının süresini tanımlayın. | `lease days [hours [ minutes]] \| infinite}` |
| NetBIOS WINS sunucusunu tanımlayın. | `netbios-name-server address [ address2… address8]` |

Licensed to yetkin{kadirgulu5yetkin@hotmail.com}

## Yapılandırma Örneği

Örnek konfigürasyonun topolojisi şekilde gösterilmiştir.




Örnek, R1'i 192.168.10.0/24 LAN için bir DHCPv4 sunucusu yapmak için yapılandırmayı gösterir.

```
R1(config)# ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)# ip dhcp excluded-address 192.168.10.254
R1(config)# ip dhcp pool LAN-POOL-1
R1(dhcp-config)# network 192.168.10.0 255.255.255.0
R1(dhcp-config)# default-router 192.168.10.1
R1(dhcp-config)# dns-server 192.168.11.5
R1(dhcp-config)# domain-name example.com
R1(dhcp-config)# end
R1#
```

## DHCPv4 Doğrulama Komutları

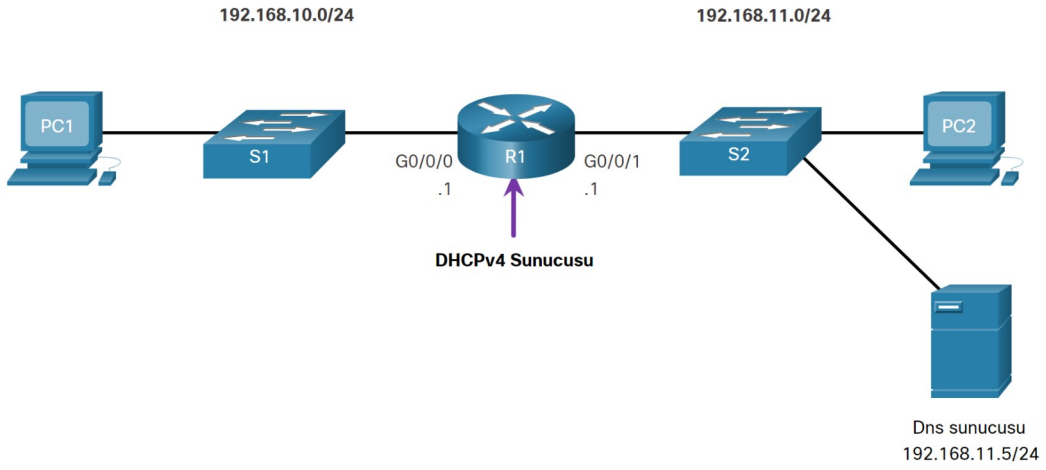
Cisco IOS DHCPv4 sunucusunun çalıştığını doğrulamak için tablodaki komutları kullanın.

| Komut | Açıklama |
|---|---|
| `show running-config \| section dhcp` | Yönlendiricide yapılandırılan DHCPv4 komutlarını görüntüler. |
| `show ip dhcp binding` | DHCPv4 hizmeti tarafından sağlanan tüm IPv4 adreslerinin MAC adresi bağlamalarının bir listesini görüntüler. |
| `show ip dhcp server statistics` | Gönderilen ve alınan DHCPv4 mesajlarının sayısıyla ilgili sayım bilgilerini görüntüler. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## DHCPv4'ün Çalışır durumda olduğunu doğrulama

Şekilde gösterilen topoloji, örnek çıktıda kullanılmıştır. Bu örnekte, R1, DHCPv4 hizmetleri sağlayacak şekilde yapılandırılmıştır. PC1'e güç verilmemiştir ve bu nedenle bir IP adresine sahip değildir.




Aşağıdaki komutların çıktısı, PC1'in IPv4 adresleme bilgilerini DHCPv4 sunucusundan aldığını varsayar. Bir Windows PC'yi bir DHCPDISCOVER mesajı göndermeye zorlamak için **ipconfig / renew** komutunu girmeniz gerekebilir.

## DHCPv4 Yapılandırmasını doğrulayın

Örnekte gösterildiği gibi, **show running-config | section dhcp** komut çıkışı, R1'de yapılandırılan DHCPv4 komutlarını görüntüler. | section parametresi yalnızca DHCPv4 yapılandırmasıyla ilişkili komutları görüntüler.

```
R1# show running-config | section dhcp
ip dhcp excluded-address 192.168.10.1 192.168.10.9
ip dhcp excluded-address 192.168.10.254
ip dhcp pool LAN-POOL-1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.11.5
 domain-name example.com
```

DHCPv4 Atamalarını Doğrulayın

Örnekte gösterildiği gibi, DHCPv4'ün çalışması **show ip dhcp binding** komutu kullanılarak doğrulanabilir . Bu komut, DHCPv4 hizmeti tarafından sağlanan tüm IPv4 adreslerinin MAC adresi bağlantılarının bir listesini görüntüler.

```
R1# show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address       Client-ID/              Lease expiration        Type       State      Interface
                 Hardware address/
                 User name
192.168.10.10    0100.5056.b3ed.d8       Sep 15 2019 8:42 AM     Automatic  Active
GigabitEthernet0/0/0
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### DHCPv4 İstatistiklerini Doğrula

**show ip dhcp server statistics** çıktısı, mesajların yönlendirici tarafından alındığını veya gönderildiğini doğrulamak için kullanılır. Bu komut, gönderilen ve alınan DHCPv4 mesajlarının sayısıyla ilgili sayım bilgilerini görüntüler.

```
R1# show ip dhcp server statistics
Memory usage         19465
Address pools        1
Database agents      0
Automatic bindings   2
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   0
Renew messages       0
Workspace timeouts   0
Static routes        0
Relay bindings       0
Relay bindings active        0
Relay bindings terminated    0
Relay bindings selecting     0
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         4
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
```

### DHCPv4 İstemcisinin IPv4 Adreslemesini Aldığını Doğrulayın

İpconfig / all PC1'de verilen komut, örnekte görüldüğü gibi TCP / IP parametreleri,. PC1, 192.168.10.0/24 ağ kesimine bağlandığından, bu havuzdan otomatik olarak bir DNS son eki, IPv4 adresi, alt ağ maskesi, varsayılan ağ geçidi ve DNS sunucusu adresi aldı. DHCP'ye özgü yönlendirici arayüz yapılandırması gerekmez. Kullanılabilir DHCPv4 havuzuna sahip bir ağ kesimine bir PC bağlanırsa, bilgisayar uygun havuzdan otomatik olarak bir IPv4 adresi alabilir.

```
C:\Users\Student> ipconfig /all
Windows IP Configuration
   Host Name . . . . . . . . . . . . : ciscolab
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained  . . . . . . . . . : Saturday, September 14, 2019 8:42:22AM
   Lease Expires   . . . . . . . . . : Sunday, September 15, 2019 8:42:22AM
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCP Server . . . . . . . . . . . : 192.168.10.1
   DNS Servers . . . . . . . . . . . : 192.168.11.5
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Cisco IOS DHCPv4 Sunucusunu devre dışı bırakma

DHCPv4 hizmeti varsayılan olarak etkindir. Hizmeti devre dışı bırakmak için, **no service dhcp** global yapılandırma modu komutunu kullanın. Örnekte gösterildiği gibi, DHCPv4 sunucu işlemini yeniden etkinleştirmek için **service dhcp** global yapılandırma modu komutunu kullanın. Parametreler yapılandırılmamışsa hizmetin etkinleştirilmesinin hiçbir etkisi yoktur.

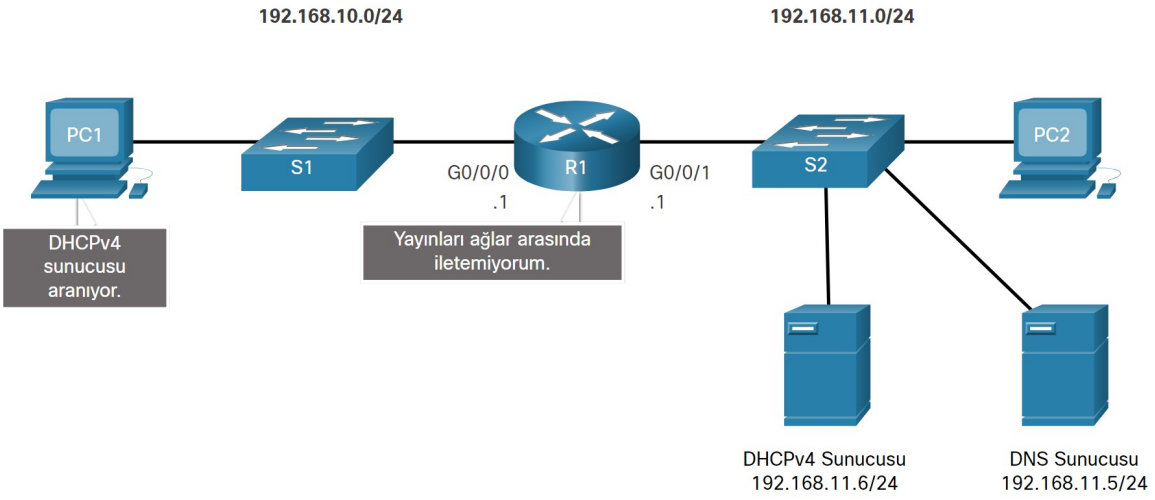
```
R1(config)# no service dhcp
R1(config)# service dhcp
R1(config)#
```

Not : DHCP bağlantılarının temizlenmesi veya DHCP hizmetinin durdurulması ve yeniden başlatılması, ağda geçici olarak atanan çift IP adreslerine neden olabilir.

## DHCPv4 Geçişi (Relay Agent)

Karmaşık bir hiyerarşik ağda, kurumsal sunucular genellikle merkezi olarak konumlandırılır. Bu sunucular ağ için DHCP, DNS, TFTP ve FTP hizmetleri sağlayabilir. Ağ istemcileri genellikle bu sunucularla aynı alt ağda değildir. İstemciler sunucuları bulmak ve hizmetleri almak için genellikle yayın mesajlarını kullanır.

Şekilde, PC1, bir yayın mesajı kullanarak bir DHCPv4 sunucusundan bir IPv4 adresi almaya çalışıyor. Bu senaryoda, R1 bir DHCPv4 sunucusu olarak yapılandırılmamıştır ve yayını iletmez. DHCPv4 sunucusu farklı bir ağda bulunduğu için PC1, DHCP kullanarak bir IP adresi alamaz. R1, DHCPv4 mesajlarını DHCPv4 sunucusuna aktaracak şekilde yapılandırılmalıdır.




Bu senaryoda, bir ağ yöneticisi PC1 için IPv4 adresleme bilgilerini yenilemeye çalışıyor.

### ipconfig / release

PC1 bir Windows bilgisayardır. Ağ yöneticisi, ipconfig / release komutunu kullanarak tüm geçerli IPv4 adresleme bilgilerini bırakır . IPv4 adresinin serbest bırakıldığına ve hiçbir adresin gösterilmediğine dikkat edin.

```
C:\Users\Student> ipconfig /release
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   Default Gateway . . . . . . . . . :
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### ipconfig / renew

Daha sonra, ağ yöneticisi IPv4 adresleme bilgilerini ipconfig / renew komutuyla yenilemeye çalışır . Bu komut PC1'in bir DHCPDISCOVER mesajı yayınlamasına neden olur. Çıktı, PC1'in DHCPv4 sunucusunu bulamadığını gösterir. Yönlendiriciler yayınları iletmediği için istek başarılı olmaz.

Ağ yöneticisi, tüm alt ağlar için R1 üzerine DHCPv4 sunucuları ekleyebilir. Ancak bu, ek maliyet ve idari ek yük yaratacaktır.

```
C:\Users\Student> ipconfig /renew
Windows IP Configuration
An error occurred while renewing interface Ethernet0 : unable to connect to your DHCP server. Request
has timed out.
```

### ip helper-address

Daha iyi bir çözüm, R1'i **ip helper-address** *adres* arabirimi yapılandırma komutuyla yapılandırmaktır. Bu, R1'in DHCPv4 yayınlarını DHCPv4 sunucusuna geçirmesine neden olur. Örnekte gösterildiği gibi, yayını PC1'den alan R1 üzerindeki arabirim, DHCPv4 adresini 192.168.11.6'daki DHCPv4 sunucusuna geçirmek için yapılandırılmıştır.

```
R1(config)# interface g0/0/0
R1(config-if)# ip helper-address 192.168.11.6
R1(config-if)# end
R1#
```

### show ip interface

R1 bir DHCPv4 aktarma aracısı olarak yapılandırıldığında, DHCPv4 hizmeti için yayın isteklerini kabul eder ve ardından bu istekleri tek noktaya yayın olarak 192.168.11.6 IPv4 adresine iletir. Ağ yöneticisi , yapılandırmayı doğrulamak için **show ip interface** komutunu kullanabilir.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is 192.168.11.6
(output omitted)
```

### ipconfig / all

Çıktıda gösterildiği gibi, PC1 artık ipconfig / all komutuyla doğrulanan DHCPv4 sunucusundan bir IPv4 adresi alabilir .

```
C:\Users\Student> ipconfig /all
Windows IP Configuration

Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   IPv4 Address. . . . . . . . . . . : 192.168.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

Licensed to [illegible] ...tkinkrsngr@gmail.com

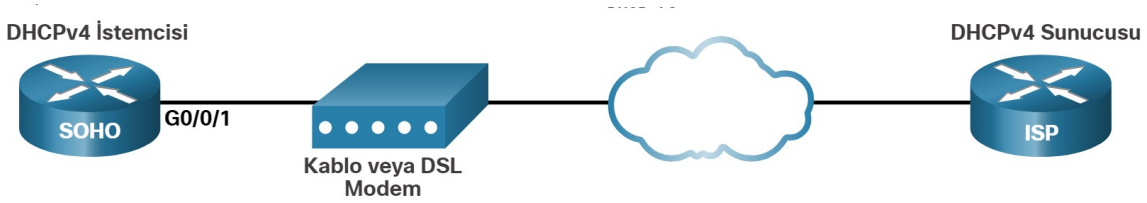
## DHCPv4 İstemcisi olarak Cisco Router

ISS'niz aracılığıyla bir DHCP sunucusuna erişiminizin olabileceği senaryolar vardır. Bu durumlarda, bir Cisco IOS yönlendiricisini DHCPv4 istemcisi olarak yapılandırabilirsiniz. Bu konu, bu süreçte size yol gösterir.

Bazen, küçük bir ofis veya ev ofisteki (SOHO) ve şube sitelerindeki Cisco yönlendiricilerinin, istemci bilgisayarlara benzer şekilde DHCPv4 istemcileri olarak yapılandırılması gerekir. Kullanılan yöntem ISP'ye bağlıdır. Bununla birlikte, en basit yapılandırmasında, Ethernet arabirimi bir kablo veya DSL modeme bağlanmak için kullanılır.

Bir Ethernet arabirimini DHCP istemcisi olarak yapılandırmak için **ip address dhcp** arabirim yapılandırma modu komutunu kullanın.

Şekilde, G0 / 0/1 arabirimi **ip address dhcp** komutuyla yapılandırıldıktan sonra, bir ISP'nin belirlenmiş müşterilere 209.165.201.0/27 ağ aralığından IP adresleri sağlayacak şekilde yapılandırıldığını varsayalım .




### Yapılandırma Örneği

Bir Ethernet arabirimini DHCP istemcisi olarak yapılandırmak için örnekte gösterildiği gibi **ip address dhcp** arabirim yapılandırma modu komutunu kullanın. Bu yapılandırma, ISP'nin belirli müşterilere IPv4 adresleme bilgileri sağlayacak şekilde yapılandırıldığını varsayar.

```
SOHO(config)# interface G0/0/1
SOHO(config-if)# ip address dhcp
SOHO(config-if)# no shutdown
Sep 12 10:01:25.773: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0/0/1 assigned DHCP address
209.165.201.12, mask 255.255.255.224, hostname SOHO
```

**show ip interface g0/0/1** komutu arabirimin yukarı-up olduğunu ve adres DHCPv4 sunucusu tarafından tahsis edildiğini doğruladı.

```
SOHO# show ip interface g0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  Internet address is 209.165.201.12/27
  Broadcast address is 255.255.255.255
  Address determined by DHCP
(output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

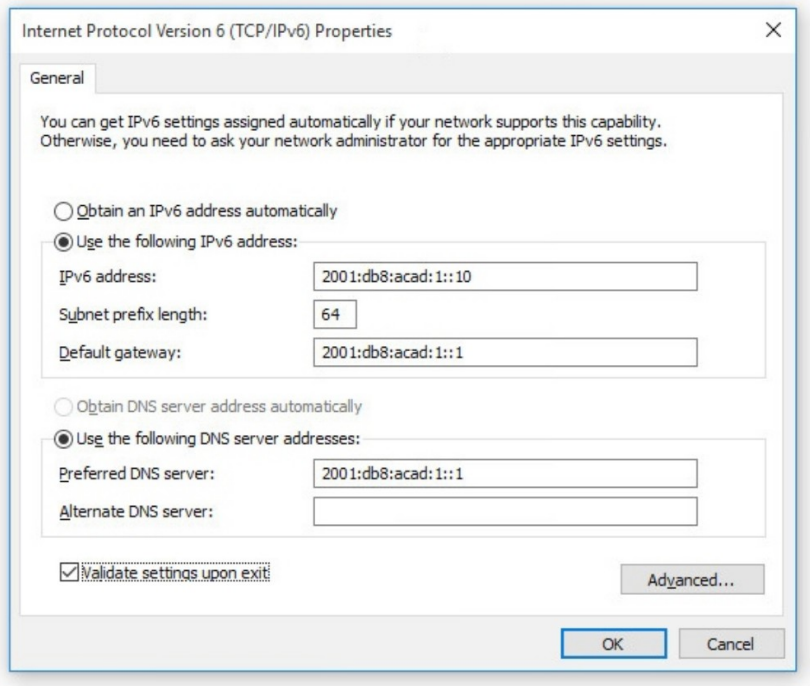
# 24.Bölüm: SLAAC ve DHCPv6

## 24.1.IPv6 GUA Ataması

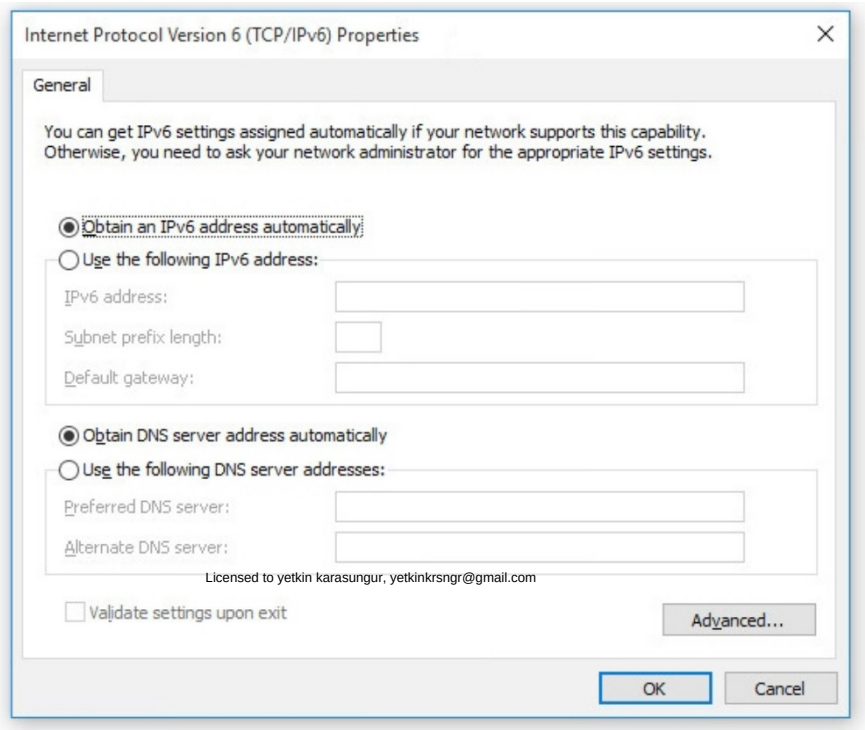
### 24.1.1.IPv6 Ana Bilgisayar Yapılandırması

Bir yönlendiricide, bir IPv6 genel tek noktaya yayın adresi (GUA), **ipv6 address** *ipv6-address/prefix-length* arabirim yapılandırma komutu kullanılarak manuel olarak yapılandırılır .

Bir Windows ana bilgisayarı, şekilde gösterildiği gibi bir IPv6 GUA adresi yapılandırmasıyla manuel olarak da yapılandırılabilir.




Bir IPv6 GUA'sını manuel olarak girmek, zaman alıcı olabilir ve bir şekilde hataya açık olabilir. Bu nedenle, çoğu Windows ana bilgisayarı, şekilde gösterildiği gibi, dinamik olarak bir IPv6 GUA yapılandırması edinecek şekilde etkinleştirilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## IPv6 Ana Bilgisayar Bağlantısı-Yerel Adresi(Local Address)

Otomatik IPv6 adresleme seçildiğinde, ana bilgisayar arabirimdeki IPv6 adres bilgilerini otomatik olarak almaya ve yapılandırmaya çalışacaktır. Ana bilgisayar, arayüzde alınan İnternet Kontrol Mesajı Protokolü sürüm 6 (ICMPv6) Yönlendirici Bildirimi (RA) mesajı ile tanımlanan üç yöntemden birini kullanacaktır. Ana bilgisayarla aynı bağlantıda bulunan bir IPv6 yönlendiricisi, ana bilgisayarlara IPv6 adres bilgilerini nasıl elde edeceklerini öneren RA mesajları gönderir. IPv6 bağlantı-yerel adresi, önyüklendiğinde ve Ethernet arabirimi etkin olduğunda ana bilgisayar tarafından otomatik olarak oluşturulur. Örnek ipconfig çıktısı, bir arabirim üzerinde otomatik olarak oluşturulan bir yerel bağlantı adresini-Link Local Address (LLA) gösterir.

Şekilde, arabirimde IPv6 GUA olmadığına dikkat edin. Bunun nedeni, bu örnekte, ağ kesiminin ana bilgisayar için ağ yapılandırma talimatlarını sağlayacak bir yönlendiriciye sahip olmaması veya ana bilgisayarın statik IPv6 adresinde yapılandırılmamış olmasıdır.

Not: Ana bilgisayar işletim sistemleri, bazen bir "%" ve bir sayı ile eklenen bir yerel bağlantı adresi gösterecektir. Bu, Bölge Kimliği veya Kapsam Kimliği (Zone ID - Scope ID) olarak bilinir. İşletim sistemi tarafından LLA'yı belirli bir arayüzle ilişkilendirmek için kullanılır.

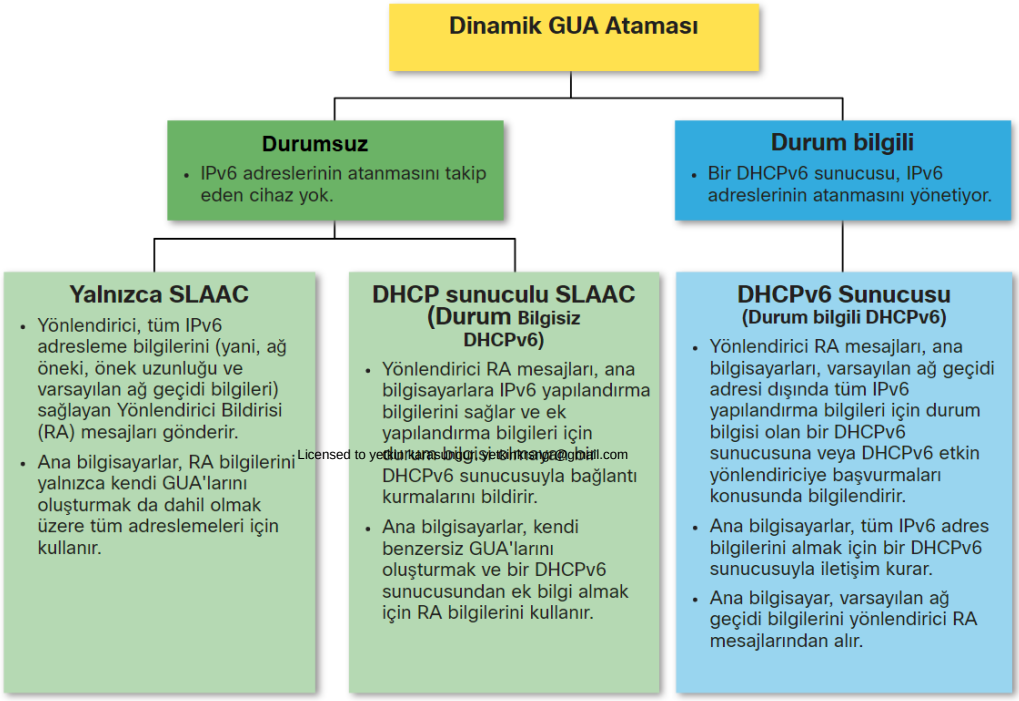
```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . :
   Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
   IPv4 Address. . . . . . . . . . . : 169.254.202.140
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :
C:\PC1>
```

## IPv6 GUA Ataması

IPv6, bir ana bilgisayarın IPv6 yapılandırmasını nasıl elde edebileceğini basitleştirmek için tasarlanmıştır. Varsayılan olarak, IPv6 etkin bir yönlendirici IPv6 bilgilerini duyurur. Bu, bir ana bilgisayarın IPv6 yapılandırmasını dinamik olarak oluşturmasına veya almasına olanak tanır.

IPv6 GUA, şekilde gösterildiği gibi, durum bilgisi olmayan ve durum bilgisi olan hizmetler kullanılarak dinamik olarak atanabilir.

Bu modüldeki tüm durum bilgisi olmayan ve durum bilgisi olan yöntemler, ana bilgisayara IPv6 yapılandırmasının nasıl oluşturulacağını veya alınacağını önermek için ICMPv6 RA mesajlarını kullanır. Ana bilgisayar işletim sistemleri RA'nın önerisini takip etse de, asıl karar nihayetinde ana bilgisayara bağlıdır.



Licensed to yedum.karabuguyetkinsag@gmail.com

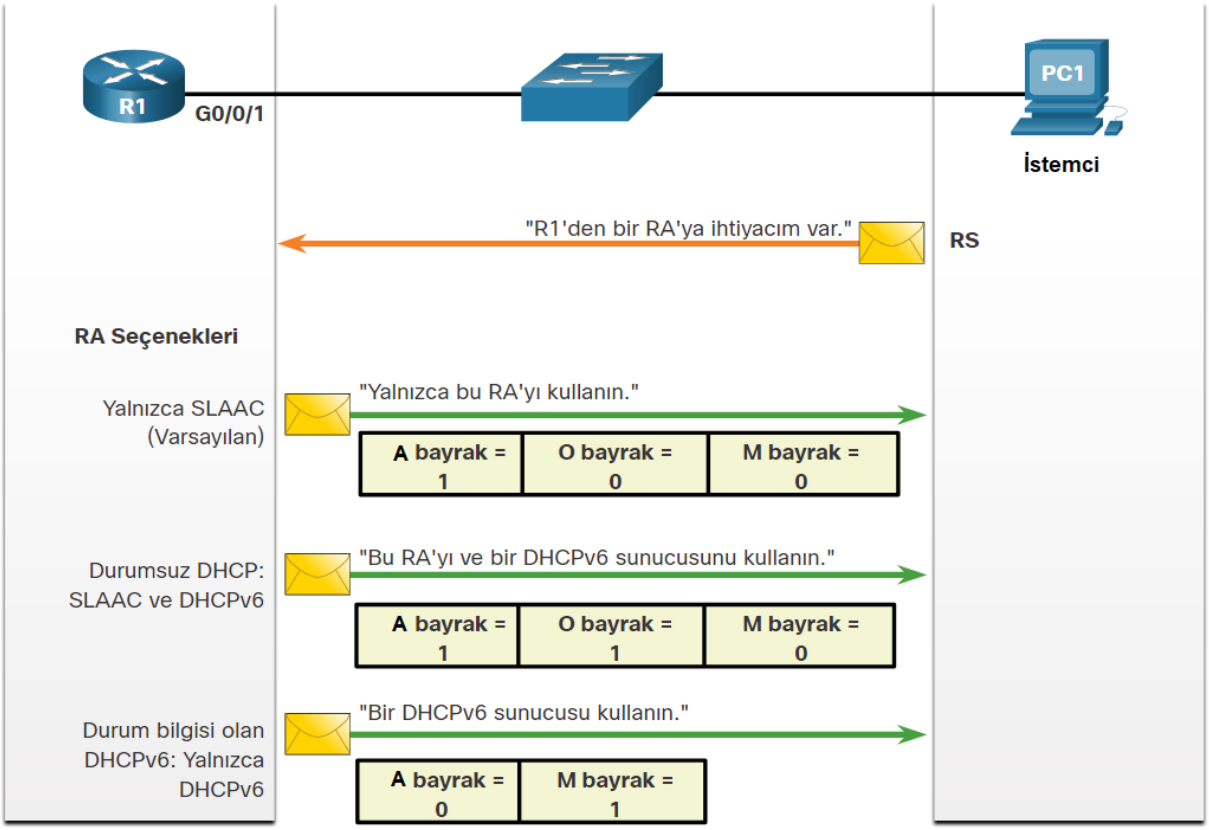
## Üç RA Mesaj Bayrağı(Flag)

Bir istemcinin IPv6 GUA'yı nasıl elde edeceğine ilişkin karar, RA mesajındaki ayarlara bağlıdır.

Bir ICMPv6 RA mesajı, bir ana bilgisayarın kullanabileceği dinamik seçenekleri tanımlayan aşağıdaki gibi üç bayrak içerir:

A Bayrağı (A flag) - Bu Otomatik Adres Yapılandırma bayrağıdır. Bir IPv6 GUA oluşturmak için Durumsuz Adres Otomatik Yapılandırması'nı (SLAAC) kullanın.
O bayrağı - Bu, Diğer Yapılandırma bayrağıdır. Diğer bilgiler, durum bilgisi olmayan bir DHCPv6 sunucusundan alınabilir.
M bayrağı - Bu, Yönetilen Adres Yapılandırması bayrağıdır. IPv6 GUA almak için durum bilgisi olan bir DHCPv6 sunucusu kullanın.
A, O ve M bayraklarının farklı kombinasyonlarını kullanan RA mesajları, ana bilgisayarı mevcut dinamik seçenekler hakkında bilgilendirir.

Şekil bu üç yöntemi göstermektedir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 24.2.SLAAC (Stateless Address Auto Configuration)

### 24.2.1.SLAAC Nedir?

Her ağın bir DHCPv6 sunucusu yoktur veya erişime ihtiyacı yoktur. Ancak IPv6 ağındaki her cihazın bir GUA'ya ihtiyacı vardır. SLAAC yöntemi, ana bilgisayarların bir DHCPv6 sunucusunun hizmetleri olmadan kendi benzersiz IPv6 genel tek noktaya yayın adreslerini oluşturmasını sağlar.

SLAAC, durumsuz bir hizmettir. Bu, hangi IPv6 adreslerinin kullanıldığını ve hangilerinin mevcut olduğunu bilmek için ağ adresi bilgilerini saklayan hiçbir sunucu olmadığı anlamına gelir.

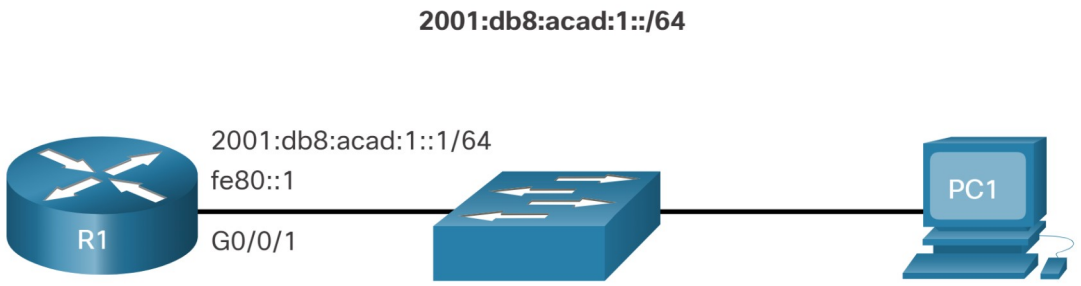
SLAAC, normalde bir DHCP sunucusu tarafından sağlanacak adresleme ve diğer yapılandırma bilgilerini sağlamak için ICMPv6 RA mesajlarını kullanır. Bir ana bilgisayar, RA'da gönderilen bilgilere göre IPv6 adresini yapılandırır. RA mesajları, her 200 saniyede bir IPv6 yönlendirici tarafından gönderilir.

Bir ana bilgisayar, IPv6 etkin bir yönlendiricinin ana bilgisayara bir RA göndermesini isteyen bir Yönlendirici Talep- Router Solicitation(RS) mesajı da gönderebilir.

SLAAC yalnızca SLAAC olarak veya DHCPv6 ile SLAAC olarak konuşlandırılabilir.

### SLAAC'ı etkinleştirme

Durum bilgisi olmayan dinamik GUA tahsisi sağlamak için SLAAC'ın nasıl etkinleştirildiğini görmek için aşağıdaki topolojiye bakın.




R1 GigabitEthernet 0/0/1, belirtilen IPv6 GUA ve bağlantı yerel adresleriyle yapılandırıldığını varsayalım.

Show ipv6 interface komutunun çıktısı , G0 / 0/1 arayüzündeki mevcut ayarları görüntüler.

Vurgulandığı gibi, R1'e aşağıdaki IPv6 adresleri atanmıştır:

Bağlantı yerel IPv6 adresi - fe80 :: 1
GUA ve alt ağ - 2001: db8: acad: 1 :: 1 ve 2001: db8: acad: 1 :: / 64
IPv6 tüm düğümler grubu - ff02 :: 1

```
R1# show ipv6 interface G0/0/1
GigabitEthernet0/0/1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Description: Link to LAN
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
(output omitted)
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yönlendirici arabiriminde bir IPv6 yapılandırması olsa da, SLAAC kullanan ana bilgisayarlara adres yapılandırma bilgilerini içeren RA'lar göndermek için henüz etkinleştirilmemiştir.

RA mesajlarının gönderilmesini etkinleştirmek için, bir yönlendiricinin çıktıda gösterildiği gibi **ipv6 unicast-routing** genel yapılandırma komutunu kullanarak IPv6 tüm yönlendiriciler grubuna katılması gerekir.

```
R1(config)# ipv6 unicast-routing
R1(config)# exit
R1#
```

IPv6 tüm yönlendiriciler grubu, IPv6 çok noktaya yayın adresi ff02 :: 2'ye yanıt verir. Çıktıda gösterildiği gibi bir yönlendiricinin etkinleştirilip etkinleştirilmediğini doğrulamak için **show ipv6 interfaces** komutunu kullanabilirsiniz.

IPv6 özellikli bir Cisco yönlendirici, RA mesajlarını IPv6 tüm düğümler çoklu yayın adresine her 200 saniyede bir ff02 :: 1 gönderir.

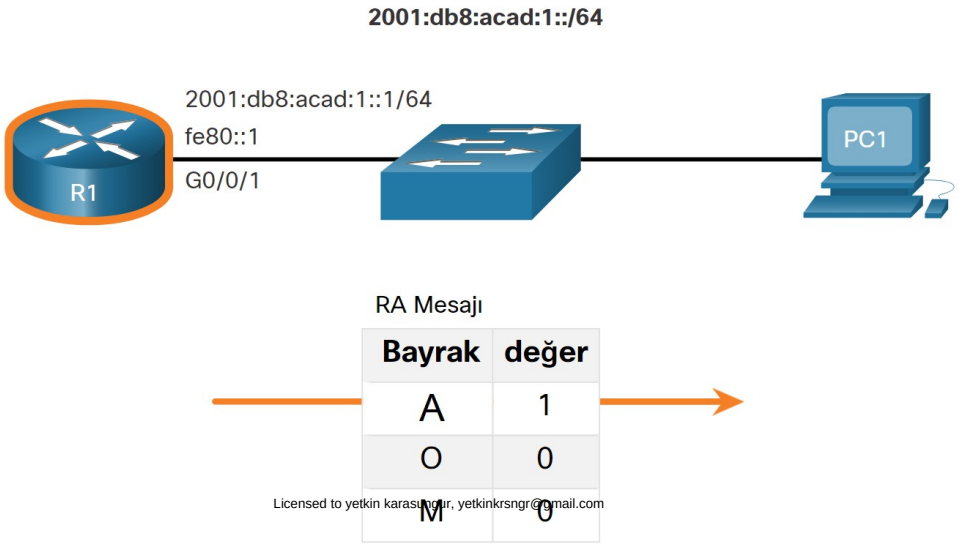
```
R1# show ipv6 interface G0/0/1 | section Joined
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
R1#
```

## Yalnızca SLAAC Yöntemi

Yalnızca SLAAC yöntemi, **ipv6 unicast-routing** komutu yapılandırıldığında varsayılan olarak etkinleştirilir . Yapılandırılmış bir IPv6 GUA'ya sahip tüm etkin Ethernet arayüzleri, şekilde gösterildiği gibi, A bayrağı 1'e ve O ve M bayrakları 0'a ayarlanmış RA mesajları göndermeye başlayacaktır.

A = 1 bayrak o RA'da önek reklamı kullanarak kendi IPv6 GUA oluşturmak o istemcinin işidir. İstemci, Genişletilmiş Benzersiz Tanımlayıcı-Extended Unique Identifier yöntemini (EUI-64) kullanarak kendi Arabirim Kimliğini oluşturabilir veya rastgele oluşturabilir.

O = 0 ve M = 0 istemci talimat bayrakları özellikle RA mesajında bilgileri kullanmak için. RA, ön ek, önek uzunluğu, DNS sunucusu, MTU ve varsayılan ağ geçidi bilgilerini içerir. DHCPv6 sunucusundan daha fazla bilgi alınamaz.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Örnekte, PC1, IPv6 adresleme bilgilerini otomatik olarak almak üzere etkinleştirilmiştir. A, O ve M bayraklarının ayarları nedeniyle, PC1, R1 tarafından gönderilen RA mesajında
bulunan bilgileri kullanarak yalnızca SLAAC gerçekleştirir.

Varsayılan ağ geçidi adresi, R1 için LLA olan RA mesajının kaynak IPv6 adresidir. Varsayılan ağ geçidi yalnızca RA mesajından otomatik olarak alınabilir. Bir DHCPv6 sunucusu bu bilgiyi sağlamaz.

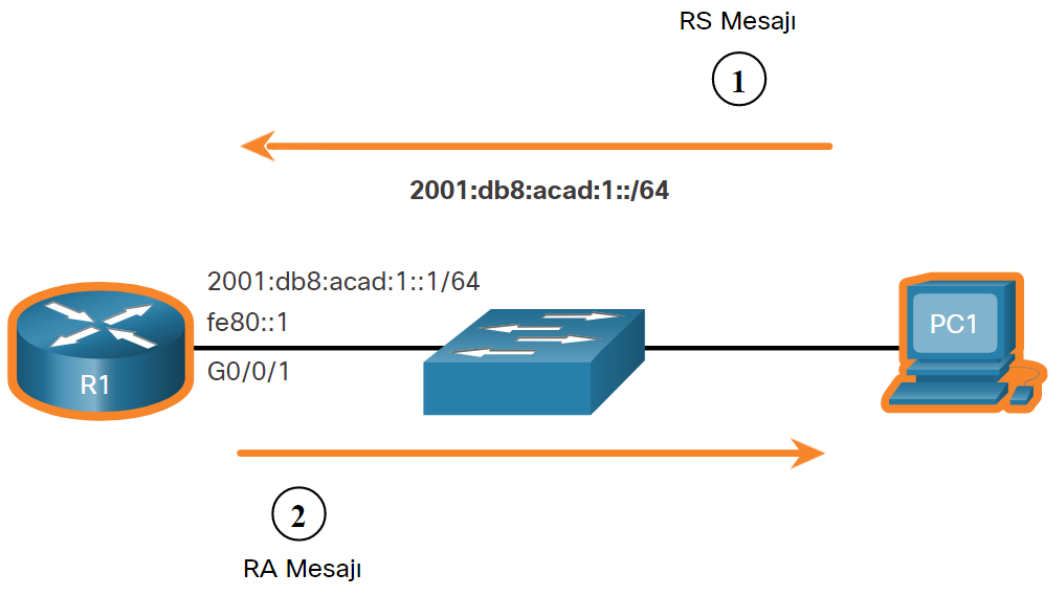
```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
   Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
   IPv4 Address. . . . . . . . . . . : 169.254.202.140
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
C:\PC1>
```

## ICMPv6 RS Mesajları

Bir yönlendirici, her 200 saniyede bir RA mesajları gönderir. Ancak, bir ana bilgisayardan bir RS mesajı alırsa bir RA mesajı da gönderecektir.

Bir istemci, adres bilgilerini otomatik olarak alacak şekilde yapılandırıldığında, ff02 :: 2'nin IPv6 tüm yönlendiricilerinin çok noktaya yayın adresine bir RS mesajı gönderir.

Şekil, bir ana bilgisayarın SLAAC yöntemini nasıl başlattığını göstermektedir.




1. PC1 yeni başlatıldı ve henüz bir RA mesajı almadı. Bu nedenle, bir RA talebinde bulunan ff02 :: 2'nin IPv6 tüm yönlendiricilerinin çok noktaya yayın adresine bir RS mesajı gönderir.
2. R1, IPv6 tüm yönlendiriciler grubunun bir parçasıdır ve RS mesajını almıştır. Yerel ağ önekini ve önek uzunluğunu içeren bir RA üretir (örn., 2001: db8: acad: 1 :: / 64). Daha sonra RA mesajını ff02 :: 1'in IPv6 tüm düğümlü çok noktaya yayın adresine gönderir. PC1 bu bilgiyi benzersiz bir IPv6 GUA oluşturmak için kullanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Arabirim Kimliği Oluşturmak için Ana Bilgisayar (Host)İşlemi

SLAAC kullanarak, bir ana bilgisayar genellikle 64 bit IPv6 alt ağ bilgilerini yönlendirici RA'sından alır. Ancak, kalan 64 bit arabirim tanımlayıcısını (ID) iki yöntemden birini kullanarak oluşturması gerekir:

Rastgele oluşturulmuş - 64 bit arabirim kimliği, istemci işletim sistemi tarafından rastgele oluşturulur. Bu, şu anda Windows 10 ana bilgisayarları tarafından kullanılan yöntemdir.
EUI-64 - Ana bilgisayar, 48 bit MAC adresini kullanarak bir arayüz kimliği oluşturur. Ana bilgisayar, adresin ortasına fffe'nin onaltılık değerini ekler ve arabirim kimliğinin yedinci bitini çevirir. Bu, arabirim kimliğinin ikinci onaltılık basamağının değerini değiştirir. Bazı işletim sistemleri, gizlilik endişeleri nedeniyle EUI-64 yöntemi yerine rastgele oluşturulmuş arabirim kimliğini varsayılan olarak kullanır. Bunun nedeni, ana bilgisayarın Ethernet MAC adresinin EUI-64 tarafından arabirim kimliğini oluşturmak için kullanılmasıdır.

Not : Windows, Linux ve Mac OS, kullanıcının arabirim kimliğinin üretimini rastgele oluşturulacak şekilde değiştirmesine veya EUI-64'ü kullanmasına izin verir.

Örneğin, aşağıdaki ipconfig çıktısında Windows 10 PC1 ana bilgisayarı, R1 RA'da bulunan IPv6 alt ağ bilgilerini kullandı ve çıktıda vurgulandığı gibi rastgele bir 64 bit arabirim kimliği oluşturdu.

```
C:\PC1> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c
   Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21
   IPv4 Address. . . . . . . . . . . : 169.254.202.140
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
C:\PC1>
```

## Yinelenen Adres Algılama-Duplicate Address Detection

İşlem, ana bilgisayarın bir IPv6 adresi oluşturmasını sağlar. Bununla birlikte, adresin ağda benzersiz olacağının garantisi yoktur.

SLAAC, durumsuz bir süreçtir; bu nedenle, bir ana bilgisayar, yeni oluşturulan bir IPv6 adresinin kullanılmadan önce benzersiz olduğunu doğrulama seçeneğine sahiptir. Yinelenen Adres Algılama (DAD) işlemi, IPv6 GUA'nın benzersiz olmasını sağlamak için bir ana bilgisayar tarafından kullanılır.

DAD, ICMPv6 kullanılarak uygulanır. DAD gerçekleştirmek için, ana bilgisayar, istenen düğüm çok noktaya yayın adresi adı verilen, özel olarak oluşturulmuş bir çok noktaya yayın adresine sahip bir ICMPv6 Komşu Talep (NS) iletisi gönderir. Bu adres, ana bilgisayarın son 24 bitlik IPv6 adresini çoğaltır.

Başka hiçbir cihaz NA mesajıyla yanıt vermezse, adresin benzersiz olması neredeyse garanti edilir ve ana bilgisayar tarafından kullanılabilir. Ana bilgisayar tarafından bir NA alınırsa, adres benzersiz değildir ve işletim sisteminin kullanılacak yeni bir arayüz kimliği belirlemesi gerekir.

İnternet Mühendisliği Görev Gücü (IETF), DAD'nin yalnızca SLAAC kullanılarak oluşturulup oluşturulmadığına, durum bilgisi olan DHCPv6 kullanılarak elde edilip edilmediğine bakılmaksızın tüm IPv6 tek noktaya yayın adreslerinde kullanılmasını önerir. DAD zorunlu değildir çünkü 64 bitlik bir arabirim kimliği 18 kentilyon olasılık sağlar ve bir çoğaltma olasılığı uzaktadır. Ancak, çoğu işletim sistemi, adresin nasıl yapılandırıldığına bakılmaksızın tüm IPv6 tek noktaya yayın adreslerinde DAD gerçekleştirir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 24.3.DHCPv6

### 24.3.1.DHCPv6 İşlem Adımları

Durum bilgisi olmayan DHCPv6, gerekli tüm bilgilerin ana bilgisayara sağlandığından emin olmak için SLAAC'ın bölümlerini kullanır. Durum bilgisi olan DHCPv6, SLAAC gerektirmez.

DHCPv6 sağladıkları bakımdan DHCPv4'e benzer olsa da, iki protokol birbirinden bağımsızdır.

Not : DHCPv6, RFC 3315'te tanımlanmıştır.

Ana bilgisayar, RA'da durum bilgisi olmayan DHCPv6 veya durum bilgisi olan DHCPv6 belirtildikten sonra DHCPv6 istemci / sunucu iletişimini başlatır.

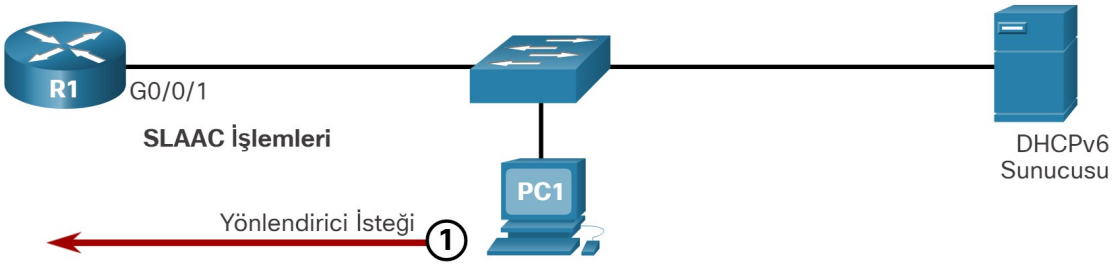
Sunucudan istemciye DHCPv6 iletileri UDP hedef bağlantı noktası 546'yı kullanırken istemciden sunucuya DHCPv6 iletileri UDP hedef bağlantı noktası 547'yi kullanır.

DHCPv6 işlemleri için adımlar aşağıdaki gibidir:

- İstemci bir RS mesajı gönderir.
- Yönlendirici bir RA mesajıyla yanıt verir.
- Ana bilgisayar bir DHCPv6 SOLICIT mesajı gönderir.
- DHCPv6 sunucusu bir ADVERTISE mesajıyla yanıt verir.
- Ana bilgisayar, DHCPv6 sunucusuna yanıt verir.
- DHCPv6 sunucusu bir REPLY mesajı gönderir.

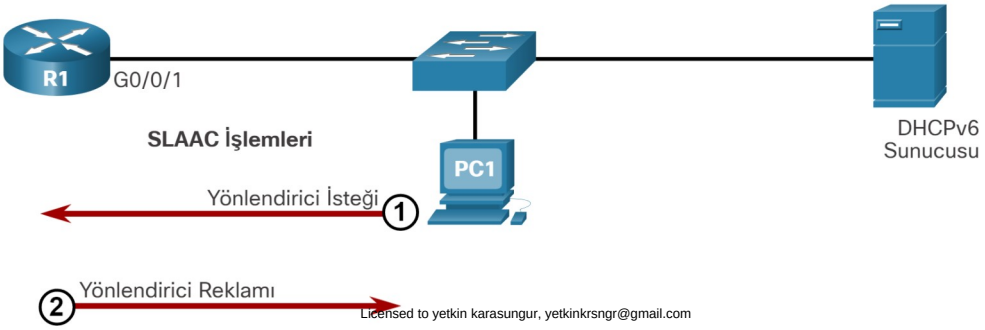
**Adım 1. İstemci bir RS mesajı gönderir.**

PC1, tüm IPv6 etkin yönlendiricilere bir RS mesajı gönderir.




**Adım 2. Yönlendirici bir RA mesajı ile yanıt verir.**

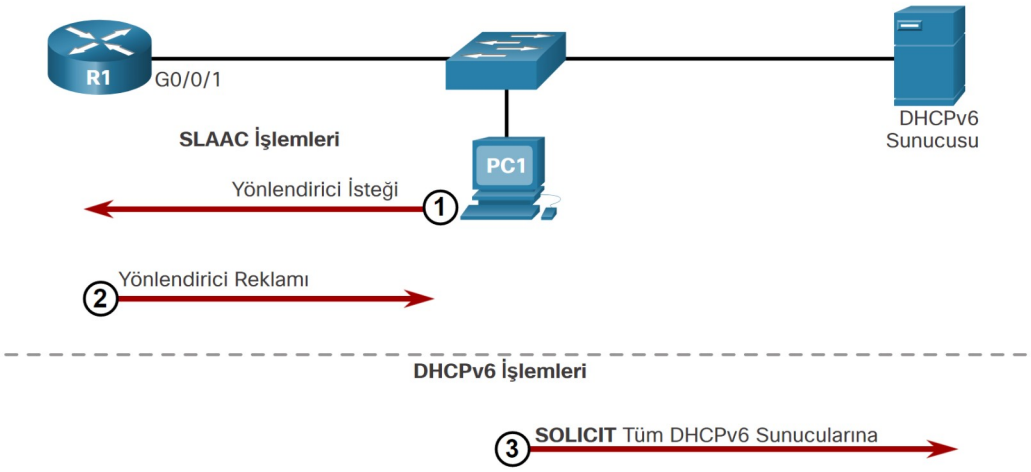
R1, RS'yi alır ve istemcinin bir DHCPv6 sunucusuyla iletişim başlatacağını belirten bir RA ile yanıt verir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

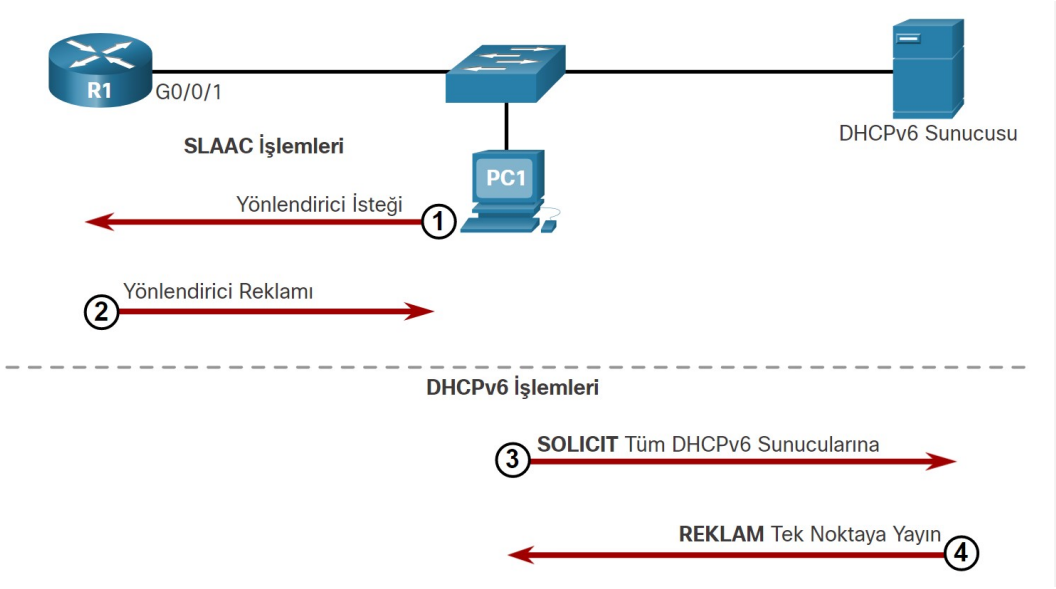
**Adım 3. Ana bilgisayar bir DHCPv6 SOLICIT mesajı gönderir.**

Artık bir DHCPv6 istemcisi olan istemcinin bir DHCPv6 sunucusu bulması gerekir ve ayrılmış IPv6 çok noktaya yayın tüm DHCPv6 sunucuları adresine bir DHCPv6 SOLICIT iletisi gönderir: ff02 :: 1: 2. Bu çok noktaya yayın adresinin bağlantı yerel kapsamı vardır, bu da yönlendiricilerin iletileri diğer ağlara iletmediği anlamına gelir.




**Adım 4. DHCPv6 sunucusu bir ADVERTISE mesajıyla yanıt verir.**

Bir veya daha fazla DHCPv6 sunucusu, bir DHCPv6 ADVERTISE tek noktaya yayın mesajıyla yanıt verir. ADVERTISE mesajı, DHCPv6 istemcisine sunucunun DHCPv6 hizmeti için uygun olduğunu bildirir.

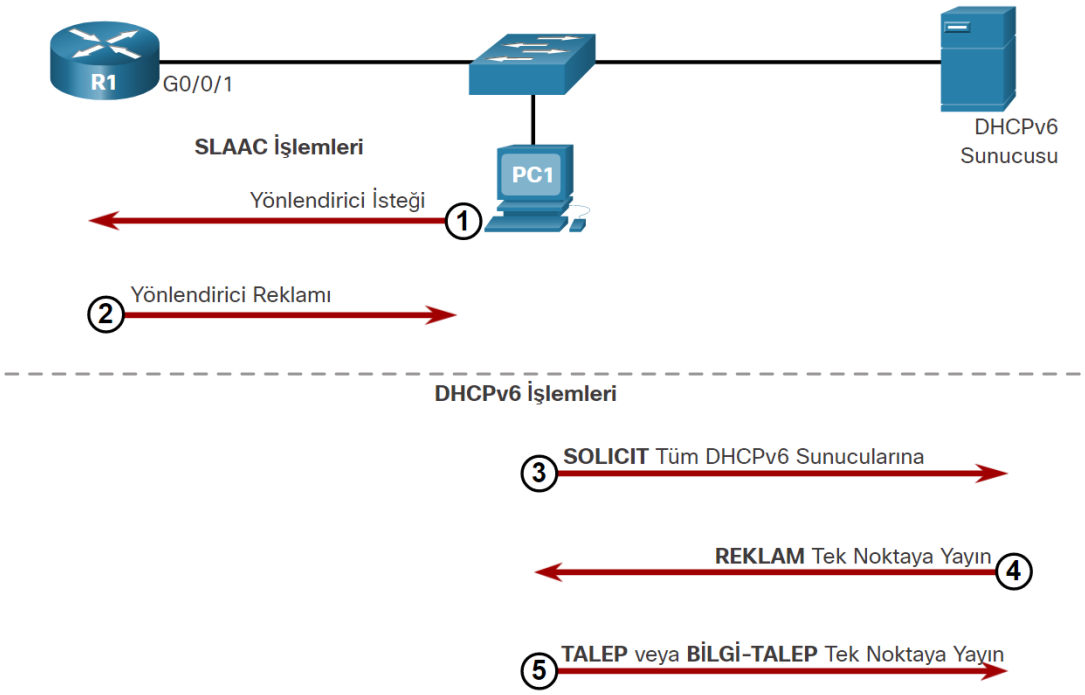



**Adım 5. Ana bilgisayar, DHCPv6 sunucusuna yanıt verir.**

PC1 yanıtı, durum bilgisi olan veya olmayan DHCPv6 kullanıp kullanmadığına bağlıdır:

Durumsuz DHCPv6 istemcisi - İstemci, RA mesajındaki öneki ve kendi oluşturduğu bir Arayüz Kimliğini kullanarak bir IPv6 adresi oluşturur. İstemci daha sonra DHCPv6 sunucusuna ek yapılandırma parametreleri (örneğin, DNS sunucusu adresi) talep eden bir DHCPv6 BİLGİ-TALEP mesajı gönderir.
Durum bilgisi olan DHCPv6 istemcisi - İstemci, gerekli tüm IPv6 yapılandırma parametrelerini almak için DHCPv6 sunucusuna bir DHCPv6 İSTEĞİ iletisi gönderir.

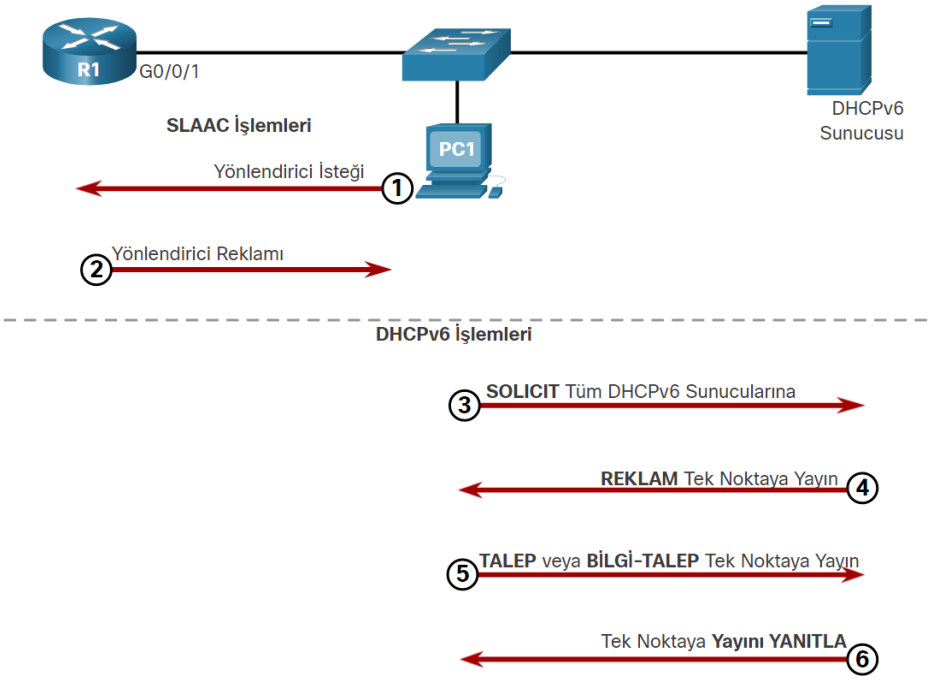
© Licensed to yetkin kahsunur, yetkinkrsngr@gmail.com




**Adım 6. DHCPv6 bir REPLY-YANITLA mesajı gönderir.**

Sunucu istemciye bir DHCPv6 REPLY tek noktaya yayın mesajı gönderir. Mesajın içeriği, bir TALEP veya BİLGİ-TALEP mesajına yanıt verip vermediğine bağlı olarak değişir.

Not : İstemci, varsayılan ağ geçidi adresi olarak RA'nın kaynak IPv6 Link-local adresini kullanacaktır. Bir DHCPv6 sunucusu bu bilgiyi sağlamaz.



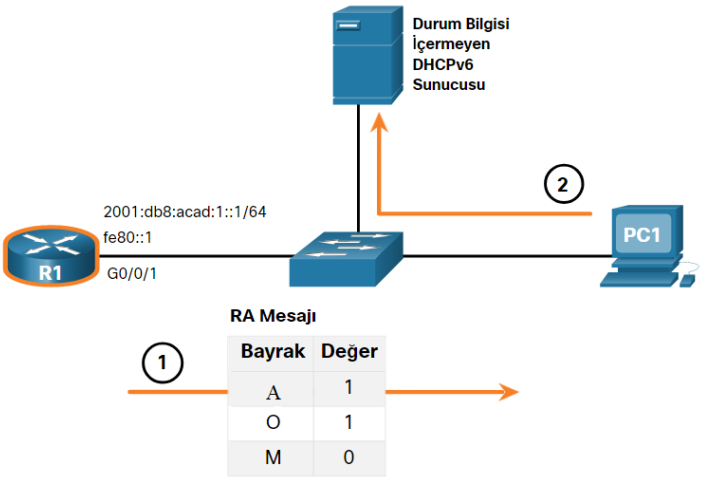

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Durumsuz DHCPv6 İşlemi

Durum bilgisi olmayan DHCPv6 sunucusu, yalnızca bir DNS sunucusunun IPv6 adresi gibi ağdaki tüm cihazlar için aynı olan bilgileri sağlar.

Bu işlem, durum bilgisi olmayan DHCPv6 olarak bilinir, çünkü sunucu herhangi bir istemci durum bilgisini (yani, kullanılabilir ve tahsis edilmiş IPv6 adreslerinin bir listesi) tutmamaktadır. Durum bilgisi olmayan DHCPv6 sunucusu, IPv6 adresleri değil, yalnızca istemciler için yapılandırma parametreleri sağlıyor.

Şekil, durum bilgisiz DHCPv6 işlemini göstermektedir.




1. PC1, durum bilgisi olmayan bir DHCP RA mesajı alır. RA mesajı, ağ önekini ve önek uzunluğunu içerir. Durum bilgisi olan DHCP için M bayrağı varsayılan değer 0'a ayarlanmıştır. A = 1 bayrağı istemciye SLAAC kullanmasını bildirir. O = 1 bayrağı, istemciye durum bilgisiz bir DHCPv6 sunucusundan ek yapılandırma bilgilerinin alınabileceğini bildirir.
2. İstemci, ek bilgi (örneğin, DNS sunucusu adresleri) almak için durum bilgisiz bir DHCPv6 sunucusu arayan bir DHCPv6 SOLICIT mesajı gönderir.

## Bir Arayüzde Durum Bilgisiz DHCPv6'yı Etkinleştirme

Durum bilgisiz DHCPv6, **ipv6 nd other-config-flag** arabirim yapılandırma komutu kullanılarak bir yönlendirici arabiriminde etkinleştirilir . Bu, O bayrağını 1'e ayarlar.

Vurgulanan çıktı, RA'nın alıcı ana bilgisayarlara durum bilgisi olmayan otomatik yapılandırmayı (A bayrağı = 1) kullanmasını ve başka bir yapılandırma bilgisi (O bayrağı = 1) almak için bir DHCPv6 sunucusuna başvurmasını söyleyeceğini doğrular.

Not: Arabirimi  varsayılan SLAAC tek seçenek (O bayrak = 0) değerine sıfırlamak için **no ipv6 nd other-config-flag** komutunu kullanabilirsiniz.

```
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
R1#
```

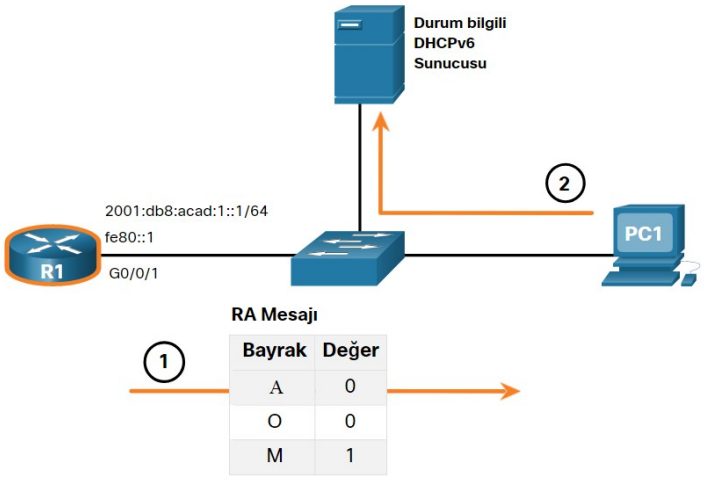
Lisanslı İp Yetkin Karasungur, yetkinkrsngr@gmail.com

### Durum bilgili DHCPv6 İşlemi

Bu seçenek en çok DHCPv4'e benzer. Bu durumda, RA mesajı istemciye, RA'nın kaynak IPv6 bağlantı-yerel adresi olan varsayılan ağ geçidi adresi dışında, tüm adresleme bilgilerini durum bilgisi olan bir DHCPv6 sunucusundan almasını söyler.

Bu, durum bilgisi olan DHCPv6 olarak bilinir çünkü DHCPv6 sunucusu IPv6 durum bilgilerini korur. Bu, IPv4 için adres ayıran bir DHCPv4 sunucusuna benzer.

Şekil, durum bilgisi olan DHCPv6 işlemini gösterir.




1. PC1, O bayrağı 0'a ve M bayrağı 1'e ayarlanmış bir DHCPv6 RA mesajı alır; bu, PC1'e tüm IPv6 adresleme bilgilerini durum bilgisi olan bir DHCPv6 sunucusundan alacağını belirtir.
2. PC1, durum bilgisi olan bir DHCPv6 sunucusu arayan bir DHCPv6 SOLICIT mesajı gönderir.

Not : A = 1 ve M = 1 ise, Windows gibi bazı işletim sistemleri SLAAC kullanarak bir IPv6 adresi oluşturur ve durum bilgisi olan DHCPv6 sunucusundan farklı bir adres alır. Çoğu durumda, A bayrağının manuel olarak 0'a ayarlanması önerilir.

### Bir Arayüzde Durum Bilgili DHCPv6'yı Etkinleştirme

Durum bilgisi olan DHCPv6, **ipv6 nd managed-config-flag** arabirimi yapılandırma komutu kullanılarak bir yönlendirici arabiriminde etkinleştirilir . Bu, M bayrağını 1'e ayarlar. **ipv6 nd prefix default no-autoconfig** arabirim komutu, A bayrağını 0 olarak ayarlayarak SLAAC'yi devre dışı bırakır.

Örnekte vurgulanan çıktı, RA'nın ana bilgisayara tüm IPv6 yapılandırma bilgilerini bir DHCPv6 sunucusundan (M bayrağı = 1) almasını söyleyeceğini doğrular.

```
R1(config)# int g0/0/1
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# ipv6 nd prefix default no-autoconfig
R1(config-if)# end
R1#
R1# show ipv6 interface g0/0/1 | begin ND
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use DHCP to obtain routable addresses.
R1#
```

## 24.4.DHCPv6 Sunucusunu Yapılandırma

### 24.4.1.DHCPv6 Yönlendirici Rolleri

Cisco IOS yönlendiricileri güçlü cihazlardır. Daha küçük ağlarda, bir DHCPv6 sunucusu, istemci veya aktarma aracısına sahip olmak için ayrı cihazlara sahip olmanız gerekmez. Bir Cisco IOS yönlendiricisi, DHCPv6 sunucu hizmetleri sağlayacak şekilde yapılandırılabilir.

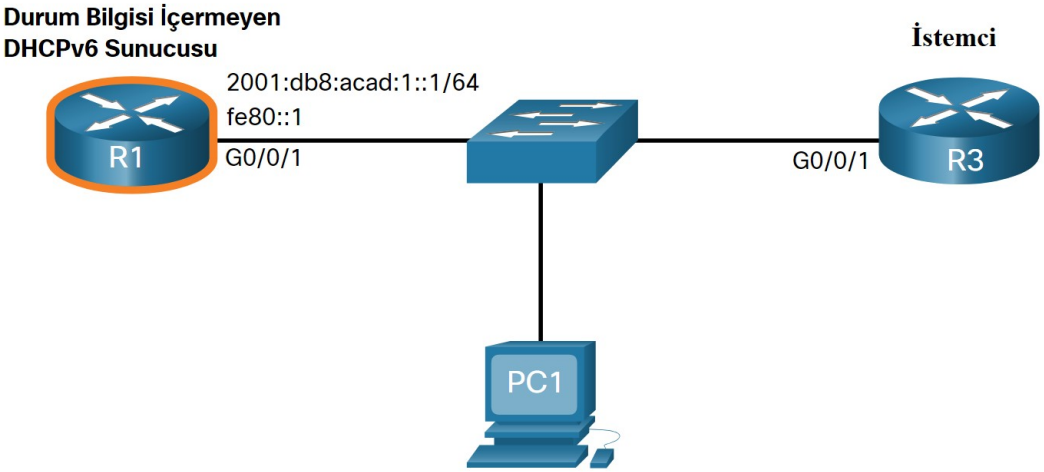
Özellikle aşağıdakilerden biri olacak şekilde yapılandırılabilir:

**DHCPv6 Sunucusu** - Yönlendirici, durum bilgisi olmayan veya durum bilgisi olan DHCPv6 hizmetleri sağlar.
**DHCPv6 İstemcisi** - Yönlendirici arayüzü, bir DHCPv6 sunucusundan bir IPv6 IP yapılandırması alır.
**DHCPv6 Aktarma Aracısı (Relay Agent)** - Yönlendirici, istemci ve sunucu farklı ağlarda bulunduğunda DHCPv6 yönlendirme hizmetleri sağlar.

**Durum Bilgisiz DHCPv6 Sunucusunu Yapılandırma**

Durum bilgisi olmayan DHCPv6 sunucusu seçeneği, yönlendiricinin RA mesajlarında IPv6 ağ adresleme bilgilerini duyurmasını gerektirir. Ancak, istemcinin daha fazla bilgi için bir DHCPv6 sunucusuna başvurması gerekir.

Durum bilgisi olmayan DHCPv6 sunucu yönteminin nasıl yapılandırılacağını öğrenmek için örnek topolojiye bakın.




Bu örnekte, R1, ana bilgisayar IPv6 yapılandırması ve DHCPv6 hizmetleri için SLAAC hizmetleri sağlayacaktır.

Bir yönlendiriciyi durum bilgisi olmayan bir DHCPv6 sunucusu olarak yapılandırmak ve doğrulamak için beş adım vardır:

1. Adım . IPv6 yönlendirmesini etkinleştirin.
2. Adım . DHCPv6 havuz adı tanımlayın.
3. Adım . DHCPv6 havuzunu yapılandırın.
4. adım . DHCPv6 havuzunu bir arabirime bağlayın.
5. Adım . Ana makinelerin IPv6 adresleme bilgilerini aldığını doğrulayın.

Usefeed to vetkin karakuhutu, vetkinfrentu@gmail.com

**Adım 1. IPv6 yönlendirmesini etkinleştirin.**

**ipv6 unicast-routing** komutu IPv6 yönlendirme sağlamak için gereklidir. Yönlendiricinin durum bilgisiz bir DHCPv6 sunucusu olması gerekli olmasa da, yönlendiricinin ICMPv6 RA mesajlarını yayması gerekir.

```
R1(config)# ipv6 unicast-routing
R1(config)#
```

**Adım 2. Bir DHCPv6 havuz adı tanımlayın.**

**ipv6 dhcp pool** POOL-NAME global yapılandırma komutunu kullanarak DHCPv6 havuzunu oluşturun . Bu, **Router(config-dhcpv6)#** ile belirtildiği gibi DHCPv6 havuzu alt yapılandırma moduna girer .

Not: Havuz adının büyük harf olması gerekmez. Ancak, büyük harfli bir ad kullanmak, konfigürasyonda görmeyi kolaylaştırır.

```
R1(config)# ipv6 dhcp pool IPV6-STATELESS
R1(config-dhcpv6)#
```

**Adım 3. DHCPv6 havuzunu yapılandırın.**

R1, komut çıktısında gösterildiği gibi, DNS sunucusu adresi ve etki alanı adı dahil olmak üzere ek DHCP bilgileri sağlayacak şekilde yapılandırılacaktır.

```
R1(config-dhcpv6)# dns-server 2001:db8:acad:1::254
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)# exit
R1(config)#
```

**Adım 4. DHCPv6 havuzunu bir arabirime bağlayın.**

DHCPv6 havuzu, çıktıda gösterildiği gibi **ipv6 dhcp server** POOL-NAME arabirim yapılandırma komutu kullanılarak arabirime bağlanmalıdır.

Yönlendirici, bu arabirimdeki durum bilgisi olmayan DHCPv6 isteklerine havuzda bulunan bilgilerle yanıt verir. O bayrağının, **ipv6 nd other-config-flag** arabirim komutu kullanılarak 0'dan 1'e manuel olarak değiştirilmesi gerekir . Bu arabirim üzerinden gönderilen RA mesajları, ek bilgilerin durum bilgisi olmayan bir DHCPv6 sunucusundan alınabileceğini gösterir. A bayrağı varsayılan olarak 1'dir ve istemcilere kendi GUA'larını oluşturmak için SLAAC'ı kullanmalarını söyler.

```
R1(config)# interface GigabitEthernet0/0/1
R1(config-if)# description Link to LAN
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 nd other-config-flag
R1(config-if)# ipv6 dhcp server IPV6-STATELESS
R1(config-if)# no shut
R1(config-if)# end
R1#
```

**Adım 5. Ana bilgisayarların IPv6 adresleme bilgilerini aldığını doğrulayın.**

License to yetkin karasungur (yetkinkrsngr@gmail.com)

Bir Windows ana bilgisayarında durum bilgisiz DHCP'yi doğrulamak için **ipconfig / all** komutunu kullanın. Örnek çıktı, PC1'deki ayarları görüntüler.

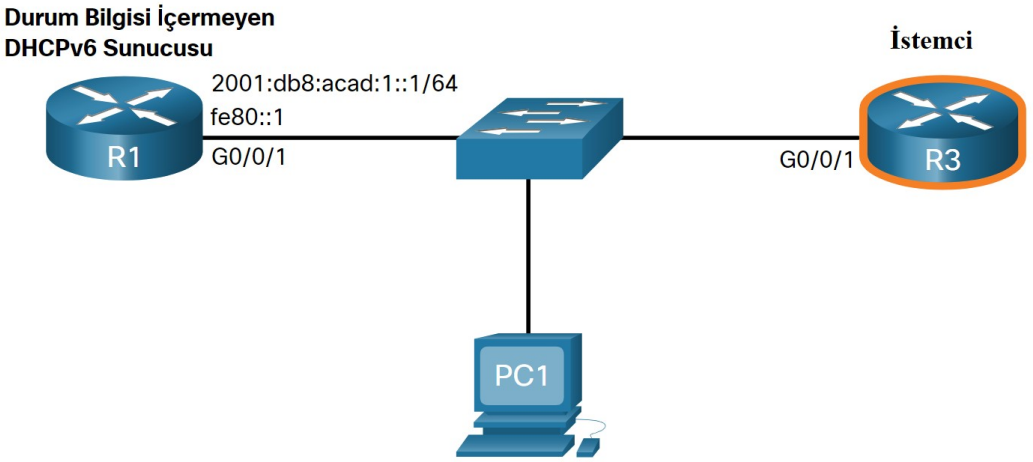
Çıktıda, PC1'in IPv6 GUA'sını 2001: db8: acad: 1 :: / 64 önekini kullanarak oluşturduğuna dikkat edin. Ayrıca, varsayılan ağ geçidinin R1'in IPv6 bağlantı yerel adresi olduğuna dikkat edin. Bu, PC1'in IPv6 yapılandırmasını R1'in RA'sından aldığını doğrular.

Vurgulanan çıktı, PC1'in alan adını ve DNS sunucusu adres bilgilerini durum bilgisi olmayan DHCPv6 sunucusundan öğrendiğini doğrular.

```
C:\PC1> ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:1de9:c69:73ee:ca8c (Preferred)
   Link-local IPv6 Address . . . . . : fe80::fb:1d54:839f:f595%21(Preferred)
   IPv4 Address. . . . . . . . . . . : 169.254.102.23 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
   DHCPv6 IAID . . . . . . . . . . . : 318768538
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 2001:db8:acad:1::254
   NetBIOS over Tcpip. . . . . . . . : Enabled
C:\PC1>
```

## Durum Bilgisi İçermeyen DHCPv6 İstemcisi Yapılandırma

Bir yönlendirici ayrıca bir DHCPv6 istemcisi olabilir ve DHCPv6 sunucusu olarak çalışan bir yönlendirici gibi bir DHCPv6 sunucusundan bir IPv6 yapılandırması alabilir. Şekilde, R1 durum bilgisi olmayan bir DHCPv6 sunucusudur.




Bir yönlendiriciyi durum bilgisi olmayan bir DHCPv6 sunucusu olarak yapılandırmak ve doğrulamak için beş adım vardır.

1. Adım . IPv6 yönlendirmesini etkinleştirin.
2. Adım . İstemci yönlendiriciyi bir LLA oluşturmak için yapılandırın.
3. Adım . İstemci yönlendiriciyi SLAAC kullanacak şekilde yapılandırın.
4. adım . İstemci yönlendiricisine bir GUA atandığını doğrulayın.
5. Adım . İstemci yönlendiricinin diğer gerekli DHCPv6 bilgilerini aldığını doğrulayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Adım 1. IPv6 yönlendirmesini etkinleştirin.**

DHCPv6 istemci yönlendiricisinde **ipv6 unicast-routing** yönlendirmesinin etkinleştirilmesi gerekir.

```
R3(config)# ipv6 unicast-routing
R3(config)#
```

**Adım 2. İstemci yönlendiriciyi bir LLA oluşturmak için yapılandırın.**

İstemci yönlendiricinin bir bağlantı yerel adresine sahip olması gerekir. Global tek noktaya yayın adresi yapılandırıldığında, yönlendirici arabiriminde bir IPv6 bağlantı yerel adresi oluşturulur. Ayrıca, **ipv6 enable** arabirimi yapılandırma komutu kullanılarak bir GUA olmadan da oluşturulabilir . Cisco IOS, rastgele bir Arayüz Kimliği oluşturmak için EUI-64 kullanır.

Çıktıda, **ipv6 enable** komutu, R3 istemci yönlendiricisinin Gigabit Ethernet 0/0/1 arayüzünde yapılandırılır.

```
R3(config)# interface g0/0/1
R3(config-if)# ipv6 enable
R3(config-if)#
```

**Adım 3. İstemci yönlendiriciyi SLAAC kullanacak şekilde yapılandırın.**

İstemci yönlendiricinin, IPv6 yapılandırması oluşturmak için SLAAC kullanacak şekilde yapılandırılması gerekir. **ipv6 address autoconfig** komutu SLAAC kullanarak adresleme IPv6 otomatik yapılandırmayı sağlar.

```
R3(config-if)# ipv6 address autoconfig
R3(config-if)# end
R3#
```

**Adım 4. İstemci yönlendiricisine bir GUA atandığını doğrulayın.**

Ana bilgisayar yapılandırmasını gösterildiği gibi doğrulamak için **show ipv6 interface brief** komutunu kullanın. Çıkış, R3 üzerindeki G0 / 0/1 arayüzüne geçerli bir GUA atandığını doğrular.

Not : Arayüzün işlemi tamamlaması birkaç saniye sürebilir.

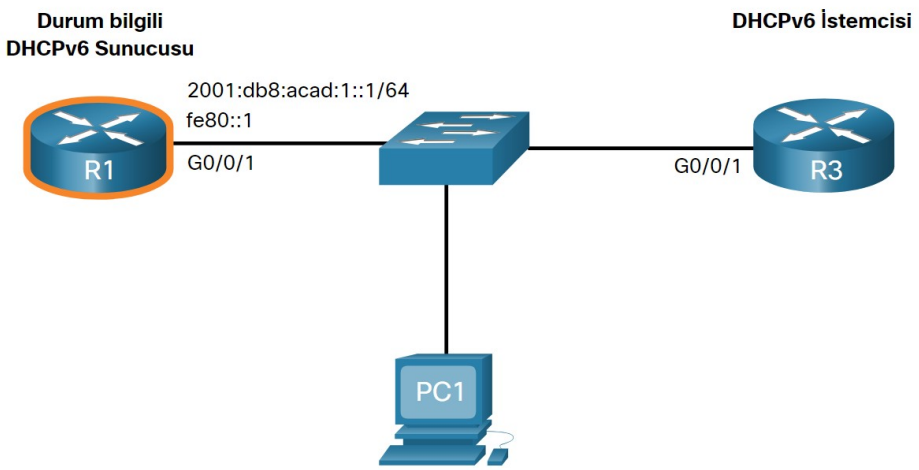
```
R3# show ipv6 interface brief
GigabitEthernet0/0/0   [up/up]
    unassigned
GigabitEthernet0/0/1   [up/up]
    FE80::2FC:BAFF:FE94:29B1
    2001:DB8:ACAD:1:2FC:BAFF:FE94:29B1
Serial0/1/0            [up/up]
    unassigned
Serial0/1/1            [up/up]
    unassigned
R3#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Durum Bilgili DHCPv6 Sunucusunu Yapılandırma

Durum bilgisi olan DHCP sunucusu seçeneği, IPv6 etkin yönlendiricinin ana bilgisayara gerekli tüm IPv6 ağ adresleme bilgilerini almak için bir DHCPv6 sunucusuna başvurmasını söylemesini gerektirir.

Şekilde, R1, yerel ağdaki tüm ana bilgisayarlara durum bilgisi olan DHCPv6 hizmetleri sağlayacaktır. Durum bilgisi olan bir DHCPv6 sunucusunu yapılandırmak, durum bilgisi olmayan bir sunucuyu yapılandırmaya benzer. En önemli fark, durum bilgisi olan bir DHCPv6 sunucusunun ayrıca bir DHCPv4 sunucusuna benzer IPv6 adresleme bilgilerini içermesidir.




Bir yönlendiriciyi durum bilgisi olmayan bir DHCPv6 sunucusu olarak yapılandırmak ve doğrulamak için beş adım vardır:

1. Adım . IPv6 yönlendirmesini etkinleştirin.
2. Adım . DHCPv6 havuz adı tanımlayın.
3. Adım . DHCPv6 havuzunu yapılandırın.
4. adım . DHCPv6 havuzunu bir arabirime bağlayın.
5. Adım . Ana makinelerin IPv6 adresleme bilgilerini aldığını doğrulayın.

### Adım 1. IPv6 yönlendirmesini etkinleştirin.

**ipv6 unicast-routing** komutu IPv6 yönlendirme sağlamak için gereklidir.

```
R1(config)# ipv6 unicast-routing
R1(config)#
```

### Adım 2. Bir DHCPv6 havuz adı tanımlayın.

**ipv6 dhcp pool** POOL-NAME global yapılandırma komutunu kullanarak DHCPv6 havuzunu oluşturun .

```
R1(config)# ipv6 dhcp pool IPV6-STATEFUL
R1(config-dhcpv6)#
```

### Adım 3. DHCPv6 havuzunu yapılandırın.

R1, komut çıktısında gösterildiği gibi IPv6 adresleme, DNS sunucu adresi ve etki alanı adı sağlayacak şekilde yapılandırılacaktır. Durum bilgisi olan DHCPv6 ile, tüm adresleme ve diğer yapılandırma parametreleri DHCPv6 sunucusu tarafından atanmalıdır. **address prefix** komutu sunucu tarafından tahsis edilecek adres havuzunu

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

belirtmek için kullanılır. Durum bilgisi olan DHCPv6 sunucusu tarafından sağlanan diğer bilgiler, çıktıda gösterildiği gibi tipik olarak DNS sunucusu adresini ve etki alanı adını içerir.

Not : Bu örnek, DNS sunucusunu Google'ın genel DNS sunucusuna ayarlıyor.

```
R1(config-dhcpv6)# address prefix 2001:db8:acad:1::/64
R1(config-dhcpv6)# dns-server 2001:4860:4860::8888
R1(config-dhcpv6)# domain-name example.com
R1(config-dhcpv6)#
```

**Adım 4. DHCPv6 havuzunu bir arabirime bağlayın.**

Örnek, GigabitEthernet 0/0/1 arayüzünün R1 üzerindeki tam konfigürasyonunu gösterir.

DHCPv6 havuzu, **ipv6 dhcp server** POOL-NAME arabirim yapılandırma komutu kullanılarak arabirime bağlanmalıdır.

- M bayrağı, **ipv6 nd managed-config-flag** arabirim komutu kullanılarak 0'dan 1'e manuel olarak değiştirilir .
- A bayrağı, **ipv6 nd prefix default no-autoconfig** arabirim komutu kullanılarak manuel olarak 1'den 0'a değiştirilir . A bayrağı 1'de bırakılabilir, ancak Windows gibi bazı istemci işletim sistemleri SLAAC kullanarak bir GUA oluşturur ve durum bilgisi olan DHCPv6 sunucusundan bir GUA alır. A bayrağının 0 olarak ayarlanması, istemciye bir GUA oluşturmak için SLAAC kullanmamasını söyler.
- **ipv6 dhcp server** komutu arabirimine DHCPv6'yı havuzu bağlar. R1 artık bu arabirimde durum bilgisi olan DHCPv6 isteklerini aldığında havuzda bulunan bilgilerle yanıt verecektir.

Not: M bayrağını varsayılan 0'a geri ayarlamak için **no ipv6 nd managed-config-flag** komutunu kullanabilirsiniz. **no ipv6 nd prefix default no-autoconfig** komutu A bayrağını varsayılan 1'e geri ayarlar.

```
R1(config)# interface GigabitEthernet0/0/1
R1(config-if)# description Link to LAN
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# ipv6 nd managed-config-flag
R1(config-if)# ipv6 nd prefix default no-autoconfig
R1(config-if)# ipv6 dhcp server IPV6-STATEFUL
R1(config-if)# no shut
R1(config-if)# end
R1#
```

**Adım 5. Ana bilgisayarların IPv6 adresleme bilgilerini aldığını doğrulayın.**

Bir Windows ana bilgisayarında doğrulamak için, durum bilgisi olmayan DHCP yapılandırma yöntemini doğrulamak için ipconfig / all komutunu kullanın. Çıkış, PC1'deki ayarları görüntüler. Vurgulanan çıktı, PC1'in IPv6 GUA'sını durum bilgisi olan bir DHCPv6 sunucusundan aldığını gösterir.

```
C:\PC1> ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:1:a43c:fd28:9d79:9e42 (Preferred)
   Lease Obtained. . . . . . . . . . : Saturday, September 27, 2019, 10:45:30 AM
   Lease Expires . . . . . . . . . . : Monday, September 29, 2019 10:05:04 AM
   Link-local IPv6 Address . . . . . : fe80::192f:6fbc:3db:b749%6(Preferred)
   Autoconfiguration IPv4 Address. . : 169.254.102.73 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
   DHCPv6 IAID . . . . . . . . . . . : 318768538
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888
   NetBIOS over Tcpip. . . . . . . . : Enabled
C:\PC1>
```

**DHCPv6 Sunucusu Doğrulama Komutları**

Bir yönlendiricide DHCPv6 işlemini doğrulamak için **show ipv6 dhcp pool** ve **show ipv6 dhcp binding** komutlarını kullanın.

**show ipv6 dhcp pool** komutu DHCPpv6 havuzu ve parametreleri doğrular . Komut ayrıca aktif istemcilerin sayısını da tanımlar. Bu örnekte, IPV6-STATEFUL havuzunun şu anda 2 istemcisi vardır, bu da PC1 ve R3'ün IPv6 genel tek noktaya yayın adreslerini bu sunucudan aldığını gösterir.

Bir yönlendirici, durum bilgisi olan DHCPv6 hizmetleri sağladığında, atanmış IPv6 adreslerinin bir veritabanını da tutar.

```
R1# show ipv6 dhcp pool
DHCPv6 pool: IPV6-STATEFUL
  Address allocation prefix: 2001:DB8:ACAD:1::/64 valid 172800 preferred 86400 (2 in use,  0 conflicts)
  DNS server: 2001:4860:4860::8888
  Domain name: example.com
  Active clients: 2
R1#
```

İstemcinin IPv6 bağlantı yerel adresini ve sunucu tarafından atanan genel tek noktaya yayın adresini görüntülemek için **show ipv6 dhcp binding** komutunu kullanın.

Çıktı, R1 üzerindeki mevcut durum bilgili bağlamayı görüntüler. Çıktıdaki ilk istemci PC1 ve ikinci istemci R3'tür.

Bu bilgiler, durum bilgisi olan bir DHCPv6 sunucusu tarafından tutulur. Durum bilgisi olmayan bir DHCPv6 sunucusu bu bilgiyi saklamaz.

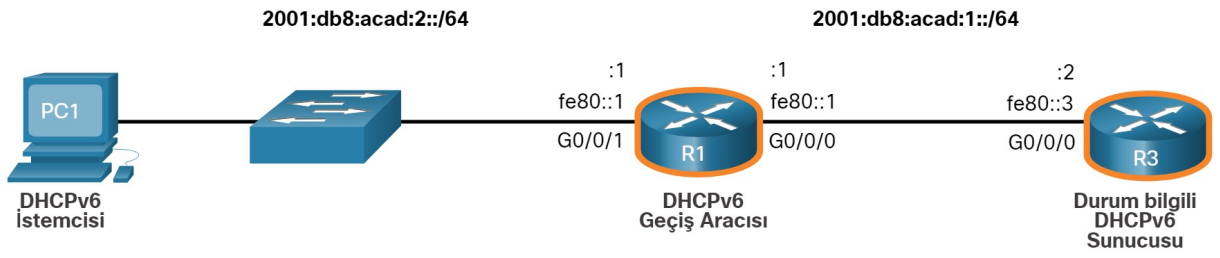
```
R1# show ipv6 dhcp binding
Client: FE80::192F:6FBC:9DB:B749
  DUID: 000100012514818300505 6B327D6
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x03000C29, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:1:A43C:FD28:9D79:9E42
             preferred lifetime 86400, valid lifetime 172800
             expires at Sep 27 2019 09:10 AM (171192 seconds)
Client: FE80::2FC:BAFF:FE94:29B1
  DUID: 0003000100FCBA9429B0
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x00060001, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:1:B4CB:25FA:3C9:747C
             preferred lifetime 86400, valid lifetime 172800
             expires at Sep 27 2019 09:29 AM (172339 seconds)
R1#
```

## 24.2.DHCPv6 Aktarma Aracısını Yapılandırma

DHCPv6 sunucusu istemciden farklı bir ağda bulunuyorsa, IPv6 yönlendiricisi DHCPv6 aktarma aracısı olarak yapılandırılabilir. Bir DHCPv6 aktarma aracısının yapılandırması, bir IPv4 yönlendiricisinin DHCPv4 geçişi olarak yapılandırılmasına benzer.

Şekilde R3, durum bilgisi olan bir DHCPv6 sunucusu olarak yapılandırılmıştır. PC1, 2001: db8: acad: 2 :: / 64 ağındadır ve IPv6 yapılandırmasını almak için durum bilgisi olan bir DHCPv6 sunucusunun hizmetlerini gerektirir. R1'in DHCPv6 Geçiş Aracısı olarak yapılandırılması gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Bir yönlendiriciyi DHCPv6 aktarma aracısı olarak yapılandırmak için komut sözdizimi aşağıdaki gibidir:

```
Router(config-if)# ipv6 dhcp relay destination ipv6-address [interface-type interface-number]
```

Bu komut, DHCPv6 istemcilerine bakan arayüzde yapılandırılır ve çıktıda gösterildiği gibi sunucuya ulaşmak için DHCPv6 sunucu adresini ve çıkış arayüzünü belirtir. Çıkış arabirimi, yalnızca sonraki atlama adresi bir LLA olduğunda gereklidir.

```
R1(config)# interface gigabitethernet 0/0/1
R1(config-if)# ipv6 dhcp relay destination 2001:db8:acad:1::2 G0/0/0
R1(config-if)# exit
R1(config)#
```

### DHCPv6 Aktarma Aracısını Doğrulayın

DHCPv6 aktarma aracısı, **show ipv6 dhcp interface** komutu kullanılarak doğrulanabilir . Bu, G0 / 0/1 arayüzünün relay agent modunda olduğunu doğrulayacaktır.

```
R1# show ipv6 dhcp interface
GigabitEthernet0/0/1 is in relay mode
  Relay destinations:
    2001:DB8:ACAD:1::2
    2001:DB8:ACAD:1::2 via GigabitEthernet0/0/0
R1#
```

R3'te , herhangi bir ana bilgisayara IPv6 yapılandırması atanıp atanmadığını doğrulamak için **show ipv6 dhcp binding** komutunu kullanın.

Bir istemci bağlantı yerel adresine bir IPv6 GUA'nın atandığına dikkat edin. Bunun PC1 olduğunu varsayabiliriz.

```
R3# show ipv6 dhcp binding
Client: FE80::5C43:EE7C:2959:DA68
  DUID: 0001000124F5CEA2005056B3636D
  Username : unassigned
  VRF : default
  IA NA: IA ID 0x03000C29, T1 43200, T2 69120
    Address: 2001:DB8:ACAD:2:9C3C:64DE:AADA:7857
            preferred lifetime 86400, valid lifetime 172800
            expires at Sep 29 2019 08:26 PM (172710 seconds)
R3#
```

Son olarak, IPv6 yapılandırmasına atandığını onaylamak için PC1'de ipconfig / all kullanın . Gördüğünüz gibi, PC1 gerçekten de IPv6 yapılandırmasını DHCPv6 sunucusundan almıştır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
C:\PC1> ipconfig /all
Windows IP Configuration
Ethernet adapter Ethernet0:
   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:db8:acad:2:9c3c:64de:aada:7857 (Preferred)
   Link-local IPv6 Address . . . . . : fe80::5c43:ee7c:2959:da68%6(Preferred)
   Lease Obtained  . . . . . . . . . : Saturday, September 27, 2019, 11:45:30 AM
   Lease Expires . . . . . . . . . . : Monday, September 29, 2019 11:05:04 AM
   IPv4 Address. . . . . . . . . . . : 169.254.102.73 (Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::1%6
   DHCPv6 IAID . . . . . . . . . . . : 318768538
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-F3-76-75-54-E1-AD-DE-DA-9A
   DNS Servers . . . . . . . . . . . : 2001:4860:4860::8888
   NetBIOS over Tcpip. . . . . . . . : Enabled
C:\PC1>
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 25.Bölüm: Varsayılan Ağ Geçidi Yedekliliği -First Hop Redundancy Protocols(FHRP)

## 25.1.First Hop Redundancy Protocols

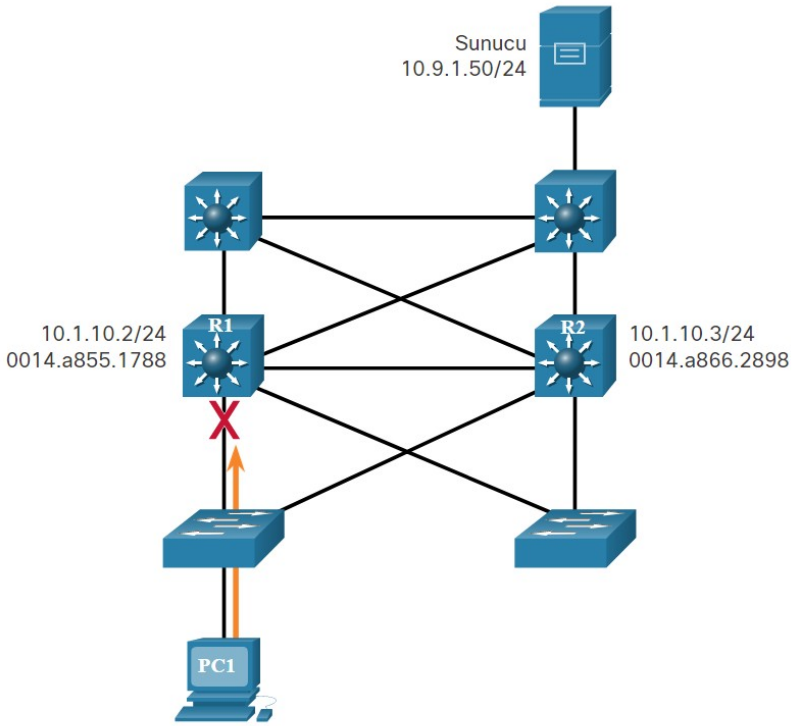
### 25.1.1.Varsayılan Ağ Geçidi Sınırlamaları

Bir yönlendirici veya yönlendirici arabirimi (varsayılan ağ geçidi görevi gören) başarısız olursa, bu varsayılan ağ geçidi ile yapılandırılan ana bilgisayarlar dış ağlardan izole edilir. İki veya daha fazla yönlendiricinin aynı VLAN'lara bağlandığı anahtarlamalı ağlarda alternatif varsayılan ağ geçitleri sağlamak için bir mekanizma gereklidir. Bu mekanizma, ilk atlama artıklık protokolleri (FHRP'ler) tarafından sağlanır.

Anahtarlamalı bir ağda, her istemci yalnızca bir varsayılan ağ geçidi alır. Paketleri yerel segmentin dışına taşımak için ikinci bir yol olsa bile, ikincil bir ağ geçidi kullanmanın bir yolu yoktur.

Şekilde, R1, paketleri PC1'den yönlendirmekten sorumludur. R1 kullanılamaz hale gelirse, yönlendirme protokolleri dinamik olarak birleşebilir. R2 artık, R1'den geçebilecek dış ağlardan gelen paketleri yönlendiriyor. Ancak, iş istasyonlarından, sunuculardan ve varsayılan ağ geçidi olarak R1 ile yapılandırılmış yazıcılardan gelen trafik dahil olmak üzere, R1 ile ilişkili iç ağdan gelen trafik yine de R1'e gönderilir ve bırakılır.

Not : Yönlendirici yedekliliği konusundaki tartışmanın amaçları doğrultusunda, bir Katman 3 anahtarı ile dağıtım katmanındaki bir yönlendirici arasında işlevsel bir fark yoktur. Uygulamada, bir Katman 3 anahtarının, anahtarlı bir ağdaki her VLAN için varsayılan ağ geçidi olarak çalışması yaygındır. Bu tartışma, kullanılan fiziksel cihazdan bağımsız olarak yönlendirme işlevine odaklanmaktadır.




PC1 varsayılan ağ geçidine ulaşamıyor.

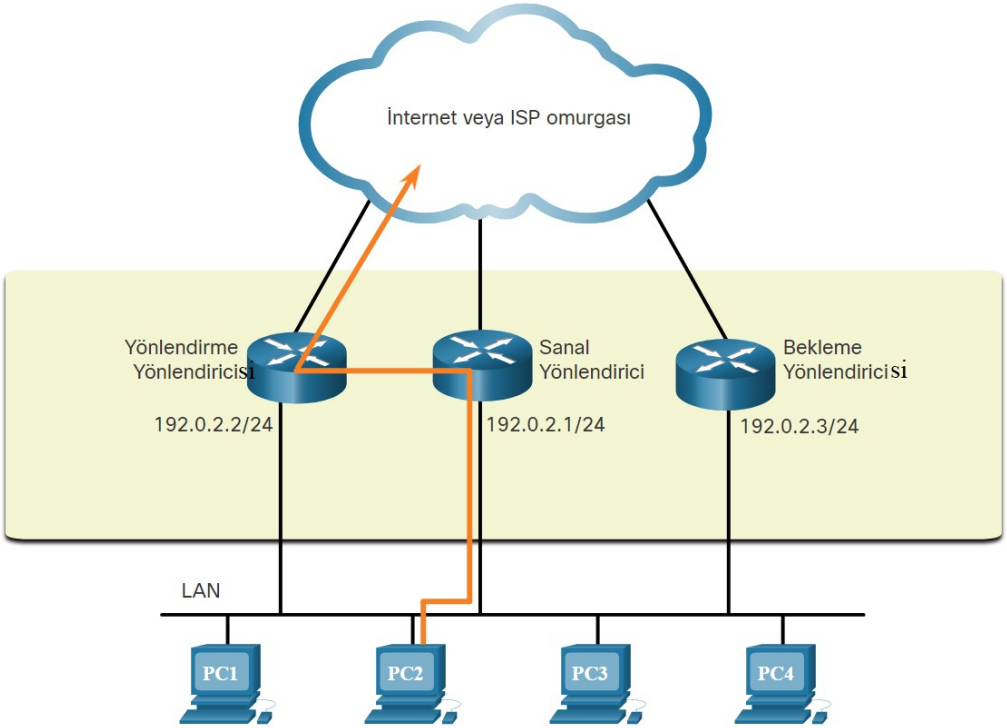
Uç cihazlar genellikle varsayılan bir ağ geçidi için tek bir IPv4 adresiyle yapılandırılır. Ağ topolojisi değiştiğinde bu adres değişmez. Bu varsayılan ağ geçidi IPv4 adresine ulaşılamazsa, yerel aygıt paketleri yerel ağ kesiminin dışına gönderemez ve diğer ağlardan etkin bir şekilde bağlantısını keser. Bu segment için varsayılan bir ağ geçidi olarak hizmet edebilecek yedek bir yönlendirici mevcut olsa bile, bu cihazların yeni bir varsayılan ağ geçidinin adresini belirleyebileceği dinamik bir yöntem yoktur.

Not : IPv6 cihazları, varsayılan ağ geçidi adreslerini dinamik olarak ICMPv6 Yönlendirici Reklamından alır. Ancak IPv6 cihazları, FHRP kullanılırken yeni varsayılan ağ geçidine daha hızlı bir yük devretme avantajından yararlanır.

## 25.1.2.Yönlendirici Yedekliliği

Varsayılan ağ geçidinde tek bir hata noktasını önlemenin bir yolu, sanal bir yönlendirici uygulamaktır. Bu tür yönlendirici yedekliliğini uygulamak için, birden çok yönlendirici, şekilde gösterildiği gibi, tek bir yönlendiricinin yanılsamasını LAN üzerindeki ana bilgisayarlara sunmak üzere birlikte çalışmak üzere yapılandırılır. Bir IP adresini ve bir MAC adresini paylaşarak, iki veya daha fazla yönlendirici tek bir sanal yönlendirici görevi görebilir.

Fiziksel ağ topolojisi dört bilgisayar, üç yönlendirici ve bir İnternet veya ISS omurga bulutu gösterir. Dört bilgisayar ve üç yönlendirici bir LAN'a bağlıdır. Üç yönlendiricinin de her birinin Ineternet veya IPS omurgasına giden bir bağlantısı vardır. IP adresi 192.0.2.1/24 olan bir yönlendirme yönlendiricisi vardır. IP adresi 192.0.2.100/24 olan bir sanal yönlendirici var. IP adresi 192.0.2.2/24 olan bir yedek yönlendirici var. PC2'den gönderilen bir paketi temsil eden bir ok, 192.0.2.100 IP adresindeki sanal yönlendiriciye, ardından 192.0.2.1 IP adresli yönlendirme yönlendiricisine ve ardından İnternet veya ISP omurgasına gider.




Sanal yönlendiricinin IPv4 adresi, belirli bir IPv4 segmentindeki iş istasyonları için varsayılan ağ geçidi olarak yapılandırılır. Çerçeveler ana cihazlardan varsayılan ağ geçidine gönderildiğinde, ana bilgisayarlar varsayılan ağ geçidinin IPv4 adresiyle ilişkili MAC adresini çözmek için ARP'yi kullanır. ARP çözünürlüğü, sanal yönlendiricinin MAC adresini döndürür. Sanal yönlendiricinin MAC adresine gönderilen çerçeveler daha sonra sanal yönlendirici grubu içinde o anda aktif olan yönlendirici tarafından fiziksel olarak işlenebilir. Tek bir sanal yönlendiricinin MAC veya IP adresine gönderilen çerçeveleri işlemekten sorumlu cihazlar olarak iki veya daha fazla yönlendiriciyi tanımlamak için bir protokol kullanılır. Ana cihazlar, sanal yönlendiricinin adresine trafik gönderir. Bu trafiği ileten fiziksel yönlendirici, ana cihazlara şeffaftır.

Bir artıklık protokolü, trafiğin iletilmesinde hangi yönlendiricinin etkin rol alması gerektiğini belirleyen mekanizma sağlar. Ayrıca, yönlendirme rolünün ne zaman bir yedek yönlendirici tarafından devralınması gerektiğini de belirler. Bir yönlendirme yönlendiricisinden diğerine geçiş, uç cihazlar için şeffaftır.

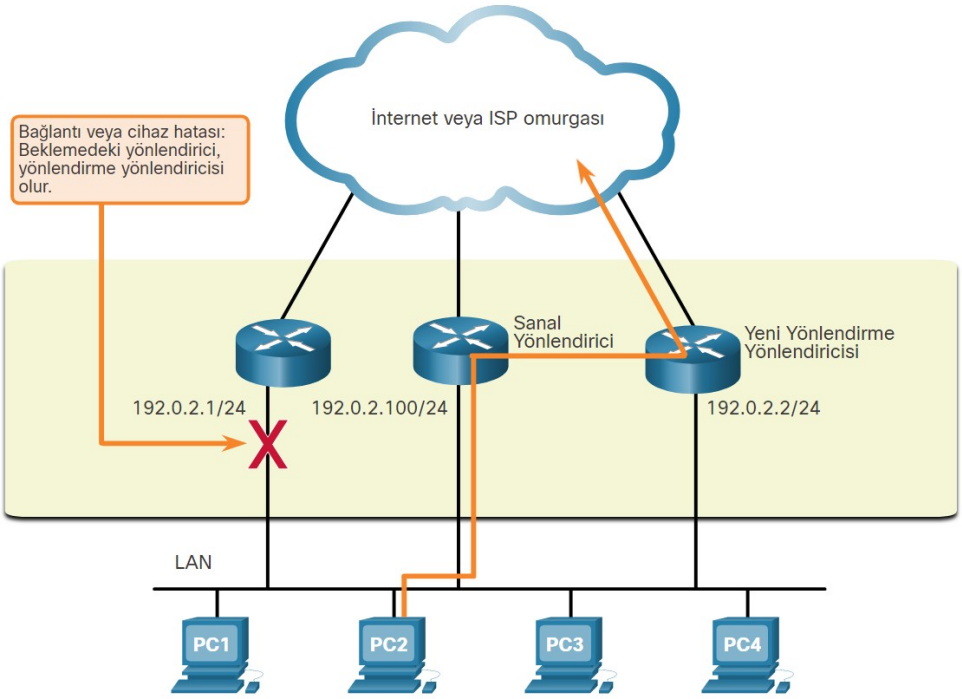
Bir ağın, varsayılan ağ geçidi olarak işlev gören bir aygıtın arızasından dinamik olarak kurtulma yeteneği, ilk atlama artıklığı olarak bilinir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Yönlendirici Yük Devretme Adımları

Etkin yönlendirici başarısız olduğunda, yedeklilik protokolü, şekilde gösterildiği gibi, bekleme yönlendiricisini yeni etkin yönlendirici rolüne geçirir. Aktif yönlendirici arızalandığında meydana gelen adımlar şunlardır:

1. Beklemedeki yönlendirici, yönlendirme yönlendiricisinden Merhaba (Hello) mesajlarını görmeyi durdurur.
2. Bekleme yönlendiricisi, yönlendirme yönlendiricisinin rolünü üstlenir.
3. Yeni yönlendirme yönlendiricisi, sanal yönlendiricinin hem IPv4 hem de MAC adreslerini üstlendiğinden, ana cihazlar hizmette kesinti görmez.




## FHRP Seçenekleri

Bir üretim ortamında kullanılan FHRP, büyük ölçüde ağın ekipmanına ve ihtiyaçlarına bağlıdır. Tablo, FHRP'ler için mevcut tüm seçenekleri listeler.

| FHRP Seçenekleri | Açıklama |
|---|---|
| Çalışırken Bekleme Yönlendirici Protokolü (Hot Standby Router Protocol - HSRP) | HRSP, ilk atlama IPv4 cihazının şeffaf yük devretmesine izin vermek için tasarlanmış, Cisco'ya ait bir FHRP'dir.HSRP, bir IPv4 varsayılan ağ geçidi adresiyle yapılandırılmış ağlarda IPv4 ana bilgisayarları için ilk atlama yönlendirme yedekliliği sağlayarak yüksek ağ kullanılabilirliği sağlar.HSRP, aktif bir cihaz ve bir bekleme cihazı seçmek için bir grup yönlendiricide kullanılır.Bir grup cihaz arayüzünde, aktif cihaz, paketleri yönlendirmek için kullanılan cihazdır;bekleme cihazı, aktif cihaz arızalandığında veya önceden ayarlanmış koşullar karşılandığında devreye giren cihazdır.HSRP bekleme yönlendiricisinin işlevi, HSRP grubunun çalışma durumunu izlemek ve etkin yönlendirici arızalanırsa hızlı bir şekilde paket iletme sorumluluğunu üstlenmektir. |
| IPv6 için HSRP | Bu, HSRP ile aynı işlevselliği sağlayan ancak bir IPv6 ortamında Cisco'ya ait bir FHRP'dir. Bir HSRP IPv6 grubu, HSRP grup numarasından türetilen sanal bir MAC adresine ve HSRP sanal MAC adresinden türetilen sanal bir IPv6 bağlantı yerel adresine sahiptir.HSRP grubu etkin olduğunda, HSRP sanal IPv6 bağlantı yerel adresi için periyodik yönlendirici ilanları (RA) gönderilir.Grup inaktif hale geldiğinde, bu RA'lar son bir RA gönderildikten sonra durur. |

Cemal Köyetekin tarafından yetkilendirilmiştir(cemalkoyetekin@gmail.com)

| FHRP Seçenekleri | Açıklama |
|---|---|
| Sanal Yönlendirici Yedeklilik Protokolü sürüm 2 (Virtual Router Redundancy Protocol-VRRPv2) | Bu, bir veya daha fazla sanal yönlendiricinin sorumluluğunu bir IPv4 LAN üzerindeki VRRP yönlendiricilere dinamik olarak atayan tescilli olmayan bir seçim protokolüdür.Bu, çoklu erişim bağlantısı üzerindeki birkaç yönlendiricinin aynı sanal IPv4 adresini kullanmasına izin verir.Bir VRRP yönlendiricisi, VRRP protokolünü bir LAN'a bağlı bir veya daha fazla başka yönlendirici ile birlikte çalıştırmak üzere yapılandırılır.Bir VRRP konfigürasyonunda, bir yönlendirici sanal yönlendirici yöneticisi olarak seçilir, diğer yönlendiriciler ise sanal yönlendirici yöneticisinin başarısız olması durumunda yedek görevi görür. |
| VRRPv3 | Bu, IPv4 ve IPv6 adreslerini destekleme yeteneği sağlar.VRRPv3, çok satıcılı ortamlarda çalışır ve VRRPv2'den daha ölçeklenebilirdir. |
| Ağ Geçidi Yük Dengeleme Protokolü (Gateway Load Balancing Protocol-GLBP) | Bu, HSRP ve VRRP gibi başarısız bir yönlendiriciden veya devreden veri trafiğini koruyan ve aynı zamanda bir grup yedekli yönlendirici arasında yük dengelemeye (yük paylaşımı da denir) izin veren Cisco'ya özel bir FHRP'dir. |
| IPv6 için GLBP | Bu, GLBP ile aynı işlevselliği sağlayan ancak bir IPv6 ortamında Cisco'ya ait bir FHRP'dir. IPv6 için GLBP, bir LAN üzerinde tek bir varsayılan ağ geçidi ile yapılandırılmış IPv6 ana bilgisayarları için otomatik yönlendirici yedeklemesi sağlar. LAN üzerindeki birden çok ilk atlama yönlendiricisi, IPv6 paket iletme yükünü paylaşırken tek bir sanal ilk atlama IPv6 yönlendiricisi sunmak için bir araya gelir. |
| ICMP Yönlendirici Bulma Protokolü (ICMP Router Discovery Protocol-IRDP) | RFC 1256'da belirtilen IRDP, eski bir FHRP çözümüdür. IRDP, IPv4 ana bilgisayarlarının diğer (yerel olmayan) IP ağlarına IPv4 bağlantısı sağlayan yönlendiricileri bulmasına izin verir. |

## 25.2.HSRP

### 25.2.1.HSRP'ye Genel Bakış

Cisco, varsayılan yönlendiriciniz başarısız olursa dış ağ erişimini kaybetmemek için IPv6 için HSRP ve HSRP sağlar.

HSRP, ilk atlama IP cihazının şeffaf yük devretmesine izin vermek için tasarlanmış, Cisco'ya ait bir FHRP'dir.

HSRP, bir IP varsayılan ağ geçidi adresiyle yapılandırılmış ağlarda IP ana bilgisayarları için ilk atlama yönlendirme yedekliliği sağlayarak yüksek ağ kullanılabilirliği sağlar. HSRP, aktif bir cihaz ve bir bekleme cihazı seçmek için bir grup yönlendiricide kullanılır. Bir grup cihaz arayüzünde, aktif cihaz, paketleri yönlendirmek için kullanılan cihazdır; bekleme cihazı, aktif cihaz arızalandığında veya önceden ayarlanmış koşullar karşılandığında devreye giren cihazdır. HSRP bekleme yönlendiricisinin işlevi, HSRP grubunun çalışma durumunu izlemek ve etkin yönlendirici arızalanırsa hızlı bir şekilde paket iletme sorumluluğunu üstlenmektir.

#### HSRP Önceliği ve Önalım (Priority-Preemption)

Etkin ve yedek yönlendiricilerin rolü, HSRP seçim süreci sırasında belirlenir. Varsayılan olarak, sayısal olarak en yüksek IPv4 adresine sahip yönlendirici, etkin yönlendirici olarak seçilir. Ancak ağınızı şansa bırakmaktansa normal koşullarda nasıl çalışacağını kontrol etmek her zaman daha iyidir.

#### HSRP Önceliği- Priority

HSRP önceliği, aktif yönlendiriciyi belirlemek için kullanılabilir. En yüksek HSRP önceliğine sahip yönlendirici, etkin yönlendirici olacaktır. Varsayılan olarak HSRP önceliği 100'dür. Öncelikler eşitse, sayısal olarak en yüksek IPv4 adresine sahip yönlendirici etkin yönlendirici olarak seçilir.

Bir yönlendiriciyi etkin yönlendirici olacak şekilde yapılandırmak için, **standby priority** arabirim komutunu kullanın. HSRP önceliğinin aralığı 0 ila 255'tir.

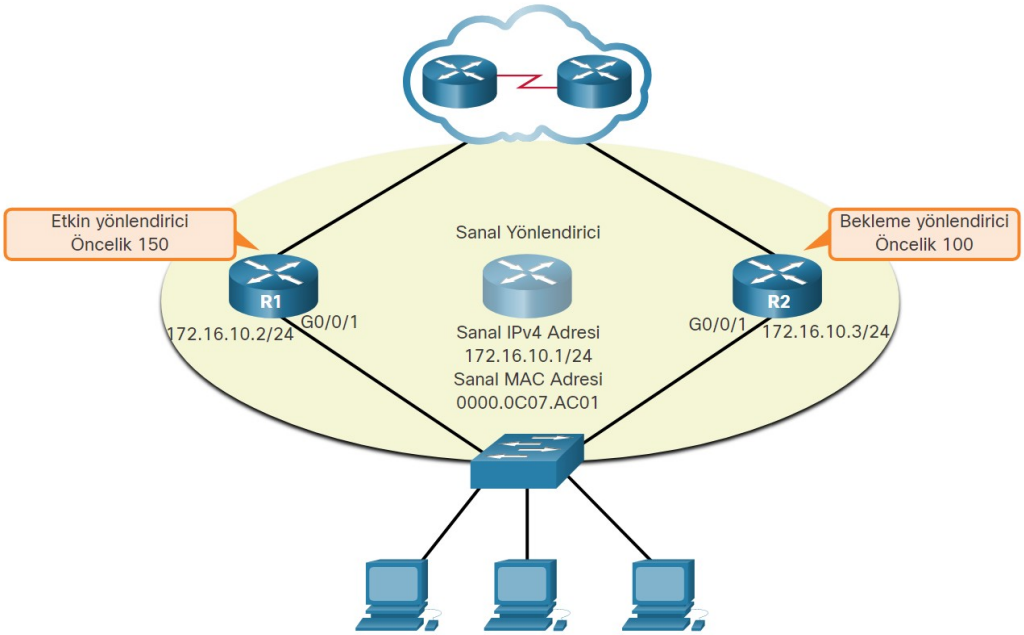
Lisanslı Ağ Kullanıcısı: [illegible]@gmail.com

## HSRP Önalım- Preemption

Varsayılan olarak, bir yönlendirici etkin yönlendirici olduktan sonra, başka bir yönlendirici daha yüksek bir HSRP önceliğiyle çevrimiçi gelse bile etkin yönlendirici olarak kalacaktır.

Yeni bir HSRP seçim sürecini, daha yüksek öncelikli bir yönlendirici çevrimiçi olduğunda gerçekleşmeye zorlamak için, **standby preempt** arabirim komutu kullanılarak önleme etkinleştirilmelidir . Preemption, bir HSRP yönlendiricisinin yeniden seçim sürecini tetikleme yeteneğidir. Önceden alma etkinleştirildiğinde, daha yüksek bir HSRP önceliğine sahip çevrimiçi olarak gelen bir yönlendirici, etkin yönlendirici rolünü üstlenir.

Preemption, yalnızca daha yüksek bir önceliğe sahipse bir yönlendiricinin etkin yönlendirici olmasına izin verir. Önleme için etkinleştirilmiş, eşit önceliğe sahip ancak daha yüksek bir IPv4 adresi olan bir yönlendirici, etkin bir yönlendiriciyi engellemez. Şekildeki topolojiye bakın.




R1, 150 HSRP önceliğiyle yapılandırılırken, R2'nin varsayılan HSRP önceliği 100'dür. Preemption, R1'de etkinleştirildi. Daha yüksek bir önceliğe sahip olan R1, etkin yönlendiricidir ve R2, yedek yönlendiricidir. Yalnızca R1'i etkileyen bir güç kesintisi nedeniyle, etkin yönlendirici artık kullanılamaz ve hazır yönlendirici R2, etkin yönlendiricinin rolünü üstlenir. Güç geri geldikten sonra, R1 tekrar çevrimiçi olur. R1 daha yüksek bir önceliğe sahip olduğundan ve ön alım etkinleştirildiğinden, yeni bir seçim sürecini zorlayacaktır. R1, etkin yönlendiricinin rolünü yeniden üstlenecek ve R2, yedek yönlendiricinin rolüne geri dönecektir.

Not : Önleme devre dışı bırakıldığında, seçim işlemi sırasında çevrimiçi olarak başka yönlendirici yoksa, ilk başlatan yönlendirici etkin yönlendirici olacaktır.

## HSRP Durumları ve Zamanlayıcıları

Bir yönlendirici, segment için trafiği iletmekten sorumlu olan aktif HSRP yönlendiricisi veya beklemede, aktif yönlendirici başarısız olursa aktif rolü üstlenmeye hazır pasif bir HSRP yönlendiricisi olabilir. Bir arabirim HSRP ile yapılandırıldığında veya mevcut bir HSRP yapılandırmasıyla ilk kez etkinleştirildiğinde, yönlendirici, HSRP grubunda hangi durumu üstleneceğini belirleme işlemine başlamak için HSRP merhaba paketleri gönderir ve alır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tablo, HSRP durumlarını özetlemektedir.

| HSRP Durumu | Açıklama |
|---|---|
| İlk-initial | Bu duruma bir konfigürasyon değişikliği yoluyla veya bir arayüz ilk kez kullanılabilir olduğunda girilir. |
| Öğren-Learn | Yönlendirici sanal IP adresini belirlemedi ve henüz aktif yönlendiriciden bir merhaba mesajı görmedi. Bu durumda, yönlendirici aktif yönlendiriciden haber bekler. |
| Dinle-Listen | Yönlendirici sanal IP adresini bilir, ancak yönlendirici ne etkin yönlendirici ne de yedek yönlendiricidir. Bu yönlendiricilerden gelen merhaba mesajlarını dinler. |
| Konuş-Speak | Yönlendirici periyodik merhaba mesajları gönderir ve aktif ve / veya yedek yönlendiricinin seçimine aktif olarak katılır. |
| Yedek-Standby | Yönlendirici, bir sonraki etkin yönlendirici olmaya adaydır ve düzenli aralıklarla merhaba mesajları gönderir. |
| Aktif | Yönlendirici seçimi kazandı. |

Etkin ve yedek HSRP yönlendiricileri, varsayılan olarak her 3 saniyede bir HSRP grubu çoklu yayın adresine (V1 224.0.0.2 veya V2 224.0.0.102 ) merhaba paketleri gönderir. Bekleme yönlendiricisi, etkin yönlendiriciden 10 saniye sonra bir merhaba mesajı almazsa etkin hale gelecektir. Yük devretmeyi veya önceliklendirmeyi hızlandırmak için bu zamanlayıcı ayarlarını düşürebilirsiniz. Ancak, CPU kullanımının artmasını ve gereksiz bekleme durumu değişikliklerinden kaçınmak için merhaba zamanlayıcıyı 1 saniyenin altına veya tutma zamanlayıcısını 4 saniyenin altına ayarlamayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 26.Bölüm: LAN Güvenliği

## 26.1.Uç Nokta Güvenliği

### 26.1.1.Bugünkü Ağ Saldırıları

Haber medyası genellikle kurumsal ağlara yapılan saldırıları kapsar. Güncel saldırılarla ilgili güncel bilgileri bulmak için internette "en son ağ saldırıları" araması yapmanız yeterlidir. Büyük olasılıkla, bu saldırılar aşağıdakilerden birini veya birkaçını içerecektir:

**Dağıtılmış Hizmet Reddi (Distributed Denial of Service-DDoS):** Bu, bir kuruluşun web sitesine ve kaynaklarına halkın erişimini azaltmak veya engellemek amacıyla zombi adı verilen birçok cihazdan koordineli bir saldırıdır.

**Veri İhlali -Data Breach:** Bu, bir kuruluşun veri sunucularının veya ana bilgisayarlarının gizli bilgileri çalmak için tehlikeye atıldığı bir saldırıdır.

**Kötü Amaçlı Yazılım - Malware :** Bu, bir kuruluşun ana bilgisayarlarına çeşitli sorunlara neden olan kötü amaçlı yazılımların bulaştığı bir saldırıdır. Örneğin, şekilde gösterilen WannaCry gibi fidye yazılımı, bir ana bilgisayardaki verileri şifreler ve bir fidye ödenene kadar buna erişimi kilitler.

### 26.1.2.Ağ Güvenliği Cihazları

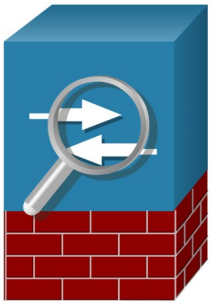
#### VPN Özellikli Yönlendirici

VPN özellikli bir yönlendirici, bir genel ağ üzerinden ve kurumsal ağdaki uzak kullanıcılara güvenli bir bağlantı sağlar. VPN hizmetleri güvenlik duvarına entegre edilebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**NGFW**

NGFW, durum bilgisi içeren paket denetimi, uygulama görünürlüğü ve denetimi, yeni nesil saldırı önleme sistemi (NGIPS), gelişmiş kötü amaçlı yazılım koruması (AMP) ve URL filtreleme sağlar.



**NAC**

Bir NAC cihazı, kimlik doğrulama, yetkilendirme ve muhasebeleştirme(AAA) hizmetlerini içerir. Daha büyük kuruluşlarda, bu hizmetler, çok çeşitli kullanıcılar ve cihaz türleri arasında erişim politikalarını yönetebilen bir cihaza dahil edilebilir. Cisco Identity Services Engine (ISE), bir NAC cihazı örneğidir.

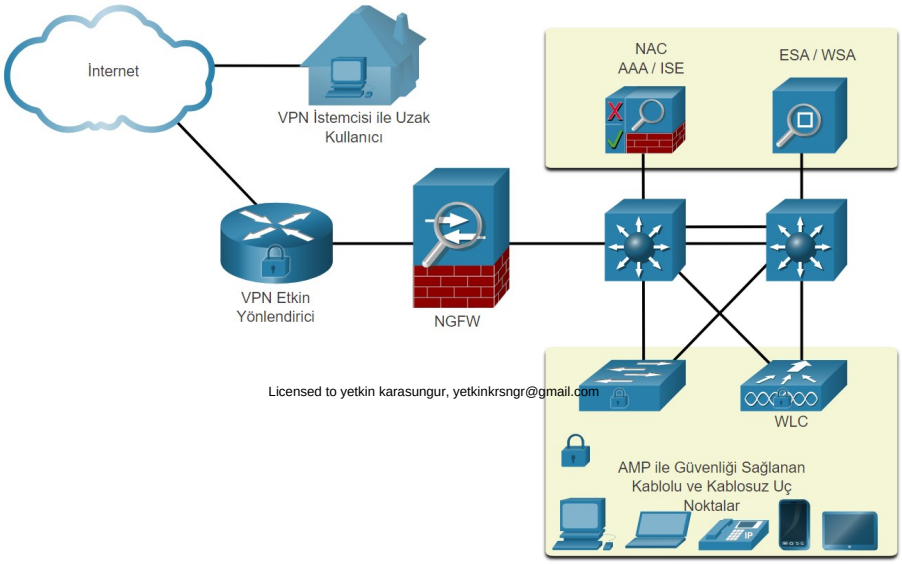
## 26.1.3.Uç Nokta Koruması

Anahtarlar, kablosuz LAN denetleyicileri (WLC'ler) ve diğer erişim noktası (AP) aygıtları gibi LAN aygıtları uç noktaları birbirine bağlar. Bu cihazların çoğu, bu bölümde  anlatılan LAN ile ilgili saldırılara karşı hassastır.

Ancak birçok saldırı ağın içinden de kaynaklanabilir. Dahili bir ana bilgisayara sızılırsa, tehdit aktörünün sunucular ve hassas veriler gibi kritik sistem cihazlarına erişim kazanması için bir başlangıç noktası olabilir.

Uç noktalar, genellikle dizüstü bilgisayarlar, masaüstü bilgisayarlar, sunucular ve IP telefonlarından oluşan ana bilgisayarların yanı sıra, genellikle kendi cihazlarınızı getirin (BYOD'ler) olarak adlandırılan, çalışanların sahip olduğu cihazlardır. Uç noktalar, e-posta veya web taraması yoluyla yapılan kötü amaçlı yazılımlarla ilgili saldırılara özellikle duyarlıdır. Bu uç noktalar tipik olarak virüsten koruma / kötü amaçlı yazılımdan koruma, ana bilgisayar tabanlı güvenlik duvarları ve ana bilgisayar tabanlı izinsiz girişi önleme sistemleri (HIPS'ler) gibi geleneksel ana bilgisayar tabanlı güvenlik özelliklerini kullanır. Ancak günümüzde uç noktalar en iyi şekilde NAC, ana bilgisayar tabanlı AMP yazılımı, bir e-posta güvenlik aracı (ESA) ve bir web güvenlik aracı (WSA) kombinasyonu ile korunmaktadır. Gelişmiş Kötü Amaçlı Yazılım Koruması (AMP) ürünleri, Uç Noktalar için Cisco AMP gibi uç nokta çözümlerini içerir.

Şekil, bu bölümde anlatılan tüm ağ güvenlik cihazlarını ve uç nokta çözümlerini temsil eden basit bir topolojidir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 26.2.Giriş Kontrolü

### 26.2.1.Yerel Parola ile Kimlik Doğrulama

Ağ aygıtlarında birçok kimlik doğrulama türü gerçekleştirilebilir ve her yöntem farklı güvenlik düzeyleri sunar. Uzaktan erişim kimlik doğrulamasının en basit yöntemi, aşağıdaki örnekte vty satırlarında gösterildiği gibi konsolda, vty hatlarında ve aux bağlantı noktalarında bir oturum açma ve parola kombinasyonu yapılandırmaktır. Bu yöntem, uygulanması en kolay olanıdır, ancak aynı zamanda en zayıf ve en az güvenlidir. Bu yöntem hiçbir sorumluluk sağlamaz ve şifre düz metin olarak gönderilir. Şifreyi bilen herkes cihaza giriş yapabilir.

```
R1(config)# line vty 0 4
R1(config-line)# password ci5c0
R1(config-line)# login
```

SSH, daha güvenli bir uzaktan erişim biçimidir:

- İletim sırasında her ikisi de şifrelenen bir kullanıcı adı ve şifre gerektirir.
- Kullanıcı adı ve şifre yerel veritabanı yöntemiyle doğrulanabilir.
- Bir kullanıcı oturum açtığında kullanıcı adı kaydedildiği için daha fazla hesap verebilirlik sağlar.

Aşağıdaki örnek, SSH'yi ve uzaktan erişimin yerel veritabanı yöntemlerini gösterir.

```
R1(config)# ip domain-name example.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)# username Admin secret Str0ng3rPa55w0rd
R1(config)# ssh version 2
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
R1(config-line)# login local
```

Yerel veritabanı yönteminin bazı sınırlamaları vardır:

- Kullanıcı hesapları her cihazda yerel olarak yapılandırılmalıdır. Yönetilmesi gereken birden çok yönlendirici ve anahtar bulunan büyük bir kurumsal ortamda, her cihazda yerel veritabanlarını uygulamak ve değiştirmek zaman alabilir.
- Yerel veritabanı yapılandırması, geri dönüş kimlik doğrulama yöntemi sağlamaz. Örneğin, yönetici o cihazın kullanıcı adını ve şifresini unutursa ne olur? Kimlik doğrulama için hiçbir yedekleme yöntemi olmadığından, şifre kurtarma tek seçenek haline gelir.

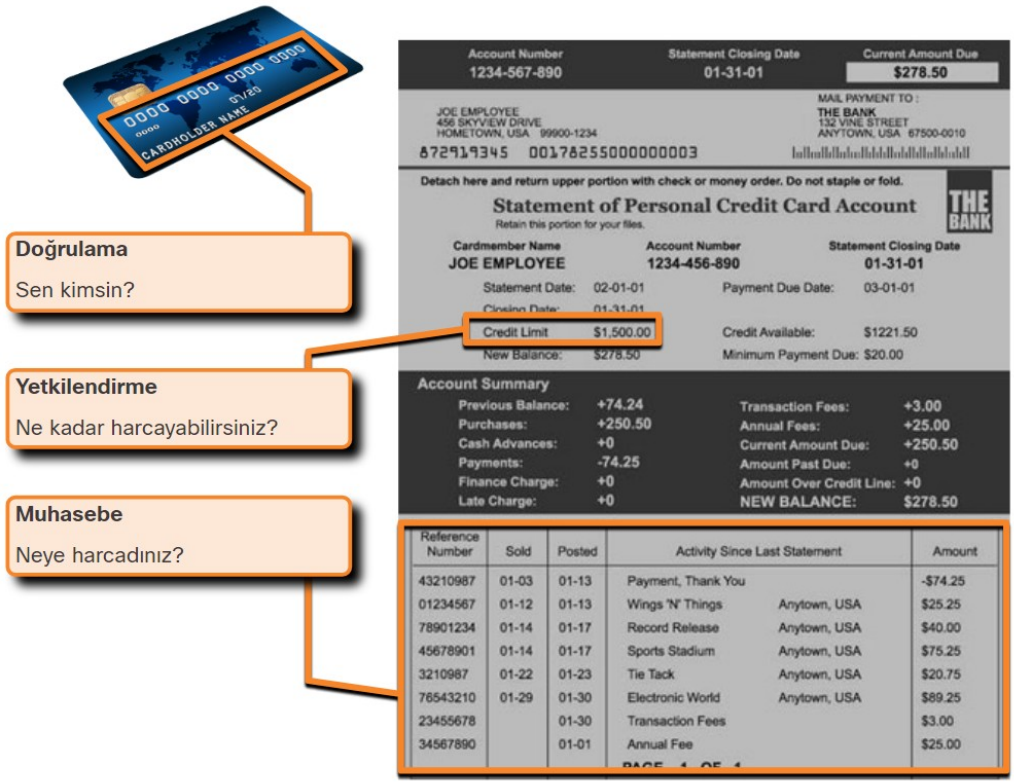
Daha iyi bir çözüm, tüm cihazların merkezi bir sunucudan aynı kullanıcı adı ve şifre veritabanına başvurmasını sağlamaktır.

### 26.2.2.AAA Bileşenleri

AAA, Kimlik Doğrulama, Yetkilendirme ve Muhasebeleştirme anlamına gelir. AAA kavramı, şekilde gösterildiği gibi bir kredi kartı kullanmaya benzer. Kredi kartı, onu kimin kullanabileceğini, o kullanıcının ne kadar harcayabileceğini tanımlar ve kullanıcının satın aldığı ürün veya hizmetlerin hesabını tutar.

AAA, bir ağ cihazında erişim kontrolü kurmak için birincil çerçeveyi sağlar. AAA, bir ağa kimlerin erişmesine izin verildiğini (kimlik doğrulama), oradayken ne yapabileceklerini (yetkilendirme) ve ağa erişirken (hesaplama) hangi eylemleri gerçekleştirdiklerini denetlemenin bir yoludur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

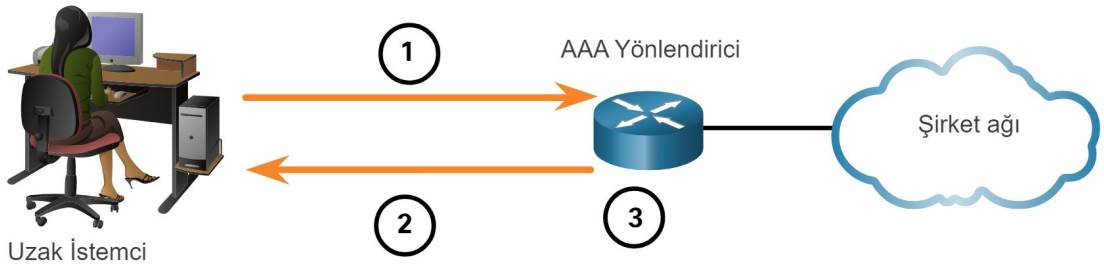



## Kimlik Doğrulama

Yerel ve sunucu tabanlı, AAA kimlik doğrulamasını uygulamanın iki yaygın yöntemidir.

### Yerel AAA Kimlik Doğrulaması

Yerel AAA, kullanıcı adlarını ve parolaları Cisco yönlendirici gibi bir ağ cihazında yerel olarak depolar. Kullanıcılar, şekilde gösterildiği gibi yerel veri tabanına göre kimlik doğrulama yapar. Yerel AAA, küçük ağlar için idealdir.

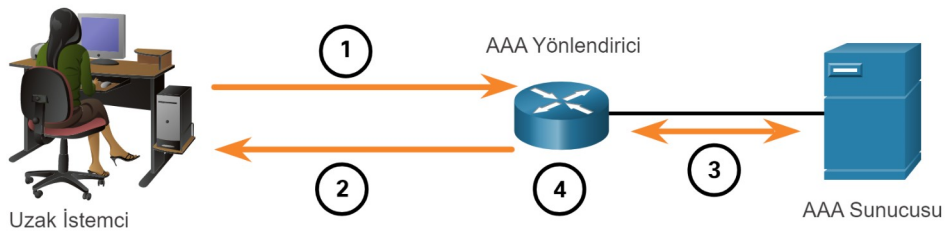



1. İstemci, yönlendiriciyle bir bağlantı kurar.
2. AAA yönlendirici, kullanıcıdan bir kullanıcı adı ve parola ister.
3. Yönlendirici, yerel veritabanını kullanarak kullanıcı adı ve parolayı doğrular ve kullanıcının yerel veritabanındaki bilgilere dayalı olarak ağa erişimi sağlanır.

### Sunucu Tabanlı AAA Kimlik Doğrulaması

Sunucu tabanlı yöntemle yönlendirici, şekilde gösterildiği gibi merkezi bir AAA sunucusuna erişir. AAA sunucusu, tüm kullanıcılar için kullanıcı adlarını ve şifreleri içerir. Yönlendirici, AAA sunucusuyla iletişim kurmak için Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti (Remote Authentication Dial-In User Service-RADIUS) veya Terminal Erişim Denetleyicisi Erişim Kontrol Sistemi (Terminal Access Controller Access Control System - TACACS +) protokollerini kullanır. Birden fazla yönlendirici ve anahtar olduğunda, sunucu tabanlı AAA daha uygundur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

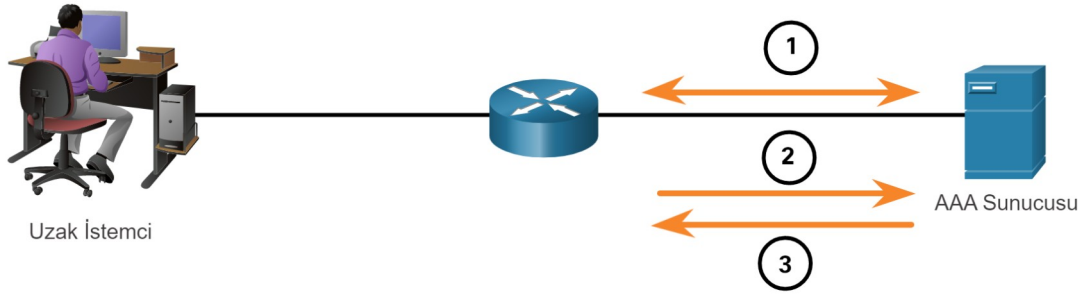



1. İstemci, yönlendiriciyle bir bağlantı kurar.
2. AAA yönlendirici, kullanıcıdan bir kullanıcı adı ve parola ister.
3. Yönlendirici, bir AAA sunucusu kullanarak kullanıcı adı ve parolayı doğrular.
4. Kullanıcıya, uzak AAA sunucusundaki bilgilere dayalı olarak ağa erişim sağlanır.

## Yetkilendirme

AAA yetkilendirmesi otomatiktir ve kullanıcıların kimlik doğrulamasından sonra ek adımlar gerçekleştirmesini gerektirmez. Yetkilendirme, kullanıcıların kimlik doğrulaması yapıldıktan sonra ağda neler yapıp yapamayacağını yönetir.

Yetkilendirme, kullanıcının ağa erişimini tanımlayan bir dizi öznitelik kullanır. Bu öznitelikler, şekilde gösterildiği gibi, AAA sunucusu tarafından o kullanıcı için ayrıcalıkları ve kısıtlamaları belirlemek için kullanılır.

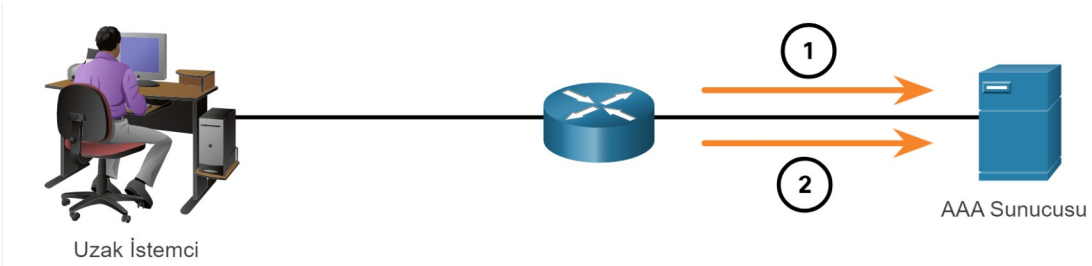



1. Bir kullanıcının kimliği doğrulandığında, yönlendirici ile AAA sunucusu arasında bir oturum kurulur.
2. Yönlendirici, istemcinin talep ettiği hizmet için AAA sunucusundan yetkilendirme ister.
3. AAA sunucusu, yetkilendirme için bir BAŞARILI / BAŞARISIZ yanıtı döndürür.

## Muhasebeleştirme

AAA muhasebeleştirme, kullanım verilerini toplar ve raporlar. Bu veriler, denetim veya faturalama gibi amaçlar için kullanılabilir. Toplanan veriler, bağlantı başlatma ve durdurma sürelerini, yürütülen komutları, paket sayısını ve bayt sayısını içerebilir.

Muhasebenin birincil kullanımı, onu AAA kimlik doğrulaması ile birleştirmektir. AAA sunucusu, şekilde gösterildiği gibi, kimliği doğrulanmış kullanıcının cihazda tam olarak ne yaptığının ayrıntılı bir kaydını tutar. Bu, kullanıcı tarafından verilen tüm EXEC ve yapılandırma komutlarını içerir. Günlük, kullanıcı adı, tarih ve saat ve kullanıcı tarafından girilen gerçek komut dahil olmak üzere çok sayıda veri alanı içerir. Bu bilgi, cihazlarda sorun giderirken kullanışlıdır. Ayrıca, bireylerin ne zaman kötü niyetli eylemlerde bulunduğuna dair kanıt sağlar.



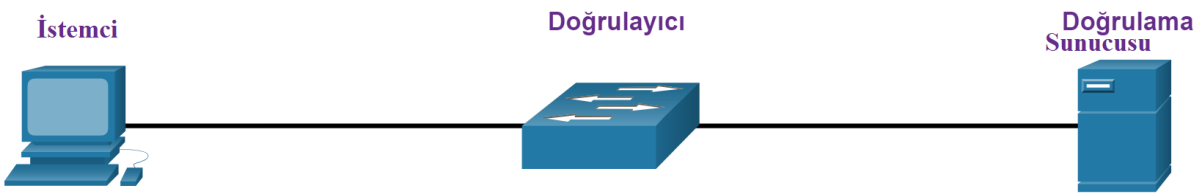

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

1. Bir kullanıcının kimliği doğrulandığında, AAA hesaplama süreci, hesap oluşturma sürecini başlatmak için bir başlangıç mesajı oluşturur.
2. Kullanıcı bitirdiğinde, bir durdurma mesajı kaydedilir ve hesaplama süreci sona erer.

## 802.1X

EEE 802.1X standardı, bağlantı noktası tabanlı bir erişim kontrolü ve kimlik doğrulama protokolüdür. Bu protokol, yetkisiz iş istasyonlarının genel erişimli anahtar bağlantı noktaları aracılığıyla bir LAN'a bağlanmasını kısıtlar. Kimlik doğrulama sunucusu, anahtar veya LAN tarafından sunulan herhangi bir hizmeti kullanıma sunmadan önce bir anahtar bağlantı noktasına bağlı her iş istasyonunun kimliğini doğrular.

802.1X bağlantı noktası tabanlı kimlik doğrulamayla, ağdaki aygıtlar şekilde gösterildiği gibi belirli rollere sahiptir.




İstemci (İstemci) - Bu, kablolu veya kablosuz cihazlar için mevcut olan 802.1X uyumlu istemci yazılımı çalıştıran bir cihazdır.
Anahtar (Kimlik Doğrulayıcı) - Anahtar, istemci ile kimlik doğrulama sunucusu arasında bir aracı görevi görür. İstemciden kimlik bilgileri ister, bu bilgiyi kimlik doğrulama sunucusuyla doğrular ve istemciye bir yanıt gönderir. Kimlik doğrulayıcı görevi görebilecek başka bir cihaz da kablosuz erişim noktasıdır.
Kimlik doğrulama sunucusu - Sunucu, istemcinin kimliğini doğrular ve anahtara veya kablosuz erişim noktasına istemcinin LAN'a ve geçiş hizmetlerine erişme yetkisi olup olmadığını bildirir.

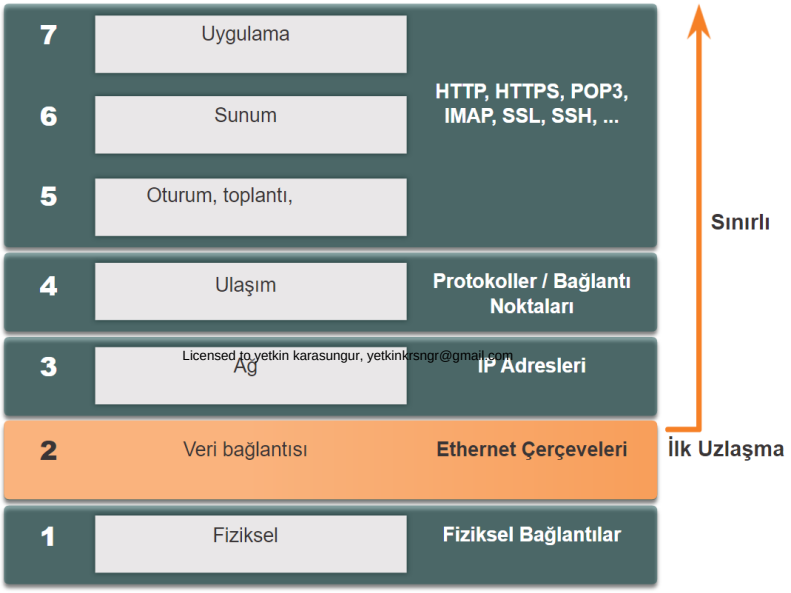
## 26.3.Katman 2 Güvenlik Tehditleri

### 26.3.1.Katman 2 Güvenlik Açıkları

OSI referans modelinin birbirinden bağımsız çalışan yedi katmana bölündüğünü hatırlayın. Şekil, her bir katmanın işlevini ve yararlanılabilecek çekirdek öğeleri göstermektedir.

Ağ yöneticileri, Katman 3'teki öğeleri Katman 7'ye kadar korumak için rutin olarak güvenlik çözümleri uygularlar. Bu öğeleri korumak için VPN'ler, güvenlik duvarları ve IPS cihazları kullanırlar. Bununla birlikte, 2. Katman tehlikeye atılırsa, üstündeki tüm katmanlar da etkilenir. Örneğin, dahili ağa erişimi olan bir tehdit aktörü 2. Katman çerçevelerini ele geçirirse, yukarıdaki katmanlarda uygulanan tüm güvenlik işe yaramaz. Tehdit unsuru, Katman 2 LAN ağ altyapısına çok fazla zarar verebilir.

Diyagram, OSI katmanlarıyla ilgili numarayı, adı ve diğer bilgileri yukarıdan aşağıya gösterir: 7 - uygulama, 6- sunum, 5 - oturum, 4 - taşıma, 3 - Ağ, 2 - veri bağlantısı ve 1 - fiziksel . Yukarıdaki tüm katmanların da tehlikeye atıldığını gösteren bir ok ile 2. katmanda Ethernet çerçevelerinin ilk uzlaşmasını gösterir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 26.3.2.Saldırı Kategorileri

Güvenlik, yalnızca sistemdeki en zayıf halka kadar güçlüdür ve Katman 2, bu zayıf halka olarak kabul edilir. Bunun nedeni, LAN'ların geleneksel olarak tek bir organizasyonun idari kontrolü altında olmasıdır. Yerel ağımıza bağlı tüm kişilere ve cihazlara doğal olarak güvendik. Bugün, BYOD ve daha karmaşık saldırılarla, LAN'larımız sızmaya karşı daha savunmasız hale geldi. Bu nedenle, Katman 3 ila Katman 7'yi korumaya ek olarak, ağ güvenliği uzmanlarının Katman 2 LAN altyapısına yönelik saldırıları da azaltması gerekir.

Katman 2 altyapısına yapılan saldırıları azaltmanın ilk adımı, Katman 2'nin temelindeki işlemi ve Katman 2 altyapısının oluşturduğu tehditleri anlamaktır.

Katman 2 LAN altyapısına yönelik saldırılar tabloda anlatılmıştır.

Layer 2 Saldırıları

| Kategori | Örnekler |
|---|---|
| MAC Tablo Saldırıları | MAC adresi taşma saldırılarını içerir. |
| VLAN Saldırıları | VLAN atlama ve VLAN çift etiketleme saldırılarını içerir. Ayrıca, ortak bir VLAN'daki cihazlar arasındaki saldırıları da içerir. |
| DHCP Saldırıları | DHCP açlığı ve DHCP sahtekarlığı saldırılarını içerir. |
| ARP Saldırıları | ARP sahtekarlığı ve ARP zehirlenmesi saldırılarını içerir. |
| Adres Sahteciliği Saldırıları | MAC adresi ve IP adresi sahtekarlığı saldırılarını içerir. |
| STP Saldırıları | Yayılma Ağacı Protokolü manipülasyon saldırılarını içerir. |

## 26.3.3.Saldırı Azaltma Teknikleri

Tablo, Katman 2 saldırılarının azaltılmasına yardımcı olmak için Cisco çözümlerine genel bir bakış sağlar.

| Çözüm | Açıklama |
|---|---|
| Port Güvenliği | MAC adresi taşma saldırıları ve DHCP açlık saldırıları dahil olmak üzere birçok saldırı türünü önler. |
| DHCP Gözetleme | DHCP açlığını ve DHCP sahtekarlığı saldırılarını önler. |
| Dinamik ARP Denetimi (DAI) | ARP sahtekarlığını ve ARP zehirlenme saldırılarını önler. |
| IP Kaynak Koruması (IPSG) | MAC ve IP adresi sahtekarlığı saldırılarını önler. |

Bu Katman 2 çözümleri, yönetim protokolleri güvenli değilse etkili olmayacaktır. Örneğin, yönetim protokolleri Syslog, Basit Ağ Yönetimi Protokolü (SNMP), Önemsiz Dosya Aktarım Protokolü (TFTP), telnet, Dosya Aktarım Protokolü (FTP) ve diğer yaygın protokollerin çoğu güvenli değildir; bu nedenle aşağıdaki stratejiler önerilir:

- Her zaman bu protokollerin SSH, Güvenli Kopya Protokolü (SCP), Güvenli FTP (SFTP) ve Güvenli Yuva Katmanı / Taşıma Katmanı Güvenliği (SSL / TLS) gibi güvenli varyantlarını kullanın.
- Cihazları yönetmek için bant dışı yönetim ağını kullanmayı düşünün.
- Yönetim trafiğinden başka hiçbir şeyin bulunmadığı özel bir yönetim VLAN'ı kullanın.
- İstenmeyen erişimi filtrelemek için ACL'leri kullanın.

### MAC Adres Tablosu Saldırısı

Bu konuda, odak noktası hala anahtarlar, özellikle MAC adres tabloları ve bu tabloların saldırılara karşı nasıl savunmasız olduğu üzerinedir.

Zekeriya Köylü Murat Sungur, yetkinterg@gmail.com

İletme kararları vermek için, Katman 2 LAN anahtarının, alınan çerçevelerdeki kaynak MAC adreslerine dayalı bir tablo oluşturduğunu hatırlayın. Şekilde gösterilen tabloya MAC adres tablosu denir. MAC adres tabloları bellekte saklanır ve çerçeveleri daha verimli bir şekilde iletmek için kullanılır.

```
S1# show mac address-table dynamic
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0001.9717.22e0    DYNAMIC     Fa0/4
   1    000a.f38e.74b3    DYNAMIC     Fa0/1
   1    0090.0c23.ceca    DYNAMIC     Fa0/3
   1    00d0.ba07.8499    DYNAMIC     Fa0/2
S1#
```

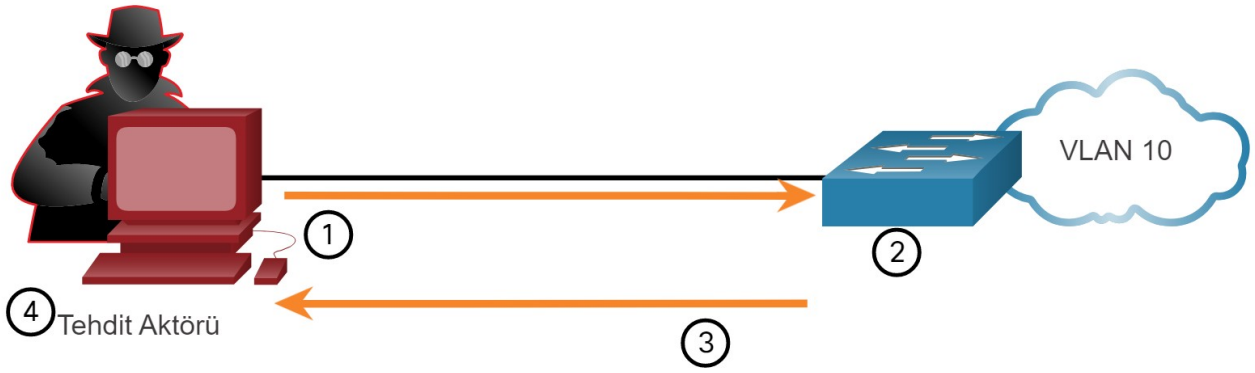
## MAC Adres Tablosu Taşması

Tüm MAC tablolarının sabit bir boyutu vardır ve sonuç olarak, bir anahtar, MAC adreslerini depolayacak kaynakları tüketebilir. MAC adresi taşma saldırıları, anahtar MAC adres tablosu dolana kadar anahtarı sahte kaynak MAC adresleriyle bombardıman ederek bu sınırlamadan yararlanır.

Bu gerçekleştiğinde, anahtar çerçeveyi bilinmeyen bir tek noktaya yayın olarak değerlendirir ve MAC tablosuna başvurmadan aynı VLAN üzerindeki tüm bağlantı noktalarından gelen tüm trafiği doldurmaya başlar. Bu koşul artık bir tehdit aktörünün yerel LAN veya yerel VLAN üzerindeki bir ana bilgisayardan diğerine gönderilen tüm kareleri yakalamasına olanak tanır.

Not : Trafik yalnızca yerel LAN veya VLAN içinde taşınır. Tehdit aktörü yalnızca tehdit aktörünün bağlı olduğu yerel LAN veya VLAN içindeki trafiği yakalayabilir.

Şekil, bir tehdit aktörünün bir MAC adres tablosunu aşmak için ağ saldırısı aracı macof'u nasıl kolayca kullanabileceğini göstermektedir .




1. Tehdit unsuru VLAN 10'a bağlıdır ve birçok rastgele kaynak ve hedef MAC ve IP adresini hızla oluşturmak için **macof** kullanır .
2. Kısa bir süre içinde, anahtarın MAC tablosu dolar.
3. MAC tablosu dolduğunda, anahtar aldığı tüm kareleri doldurmaya başlar. **Macof** çalışmaya devam ettiği sürece , MAC tablosu dolu kalır ve anahtar, VLAN 10 ile ilişkili her bağlantı noktasından gelen tüm çerçeveleri **doldurmaya** devam eder.
4. Tehdit aktörü daha sonra VLAN 10'a bağlı tüm cihazlardan kareleri yakalamak için paket koklama yazılımı kullanır.

Tehdit aktörü macof'un çalışmasını durdurursa veya keşfedilir ve durdurulursa, anahtar sonunda tablodaki eski MAC adresi girişlerini yaşlandırır ve yeniden bir anahtar gibi davranmaya başlar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### MAC Adres Tablosu Saldırısını Azaltma

Macof gibi araçları bu kadar tehlikeli yapan şey, bir saldırganın çok hızlı bir şekilde bir MAC tablosu taşma saldırısı oluşturabilmesidir. Örneğin, bir Catalyst 6500 anahtarı, MAC adres tablosunda 132.000 MAC adresi depolayabilir. Macof gibi bir araç , bir anahtara saniyede 8.000 adede kadar sahte çerçeve ekleyebilir; birkaç saniye içinde bir MAC adres tablosu taşma saldırısı oluşturmak mümkündür. Şekil bir Linux ana bilgisayarında macof komutunun örnek bir çıktısını gösterir .

```
# macof -i eth1
36:a1:48:63:81:70 15:26:8d:4d:28:f8 0.0.0.0.26413 > 0.0.0.0.49492: S 1094191437:1094191437(0) win 512
16:e8:8:0:4d:9c da:4d:bc:7c:ef:be 0.0.0.0.61376 > 0.0.0.0.47523: S 446486755:446486755(0) win 512
18:2a:de:56:38:71 33:af:9b:5:a6:97 0.0.0.0.20086 > 0.0.0.0.6728: S 105051945:105051945(0) win 512
e7:5c:97:42:ec:1 83:73:1a:32:20:93 0.0.0.0.45282 > 0.0.0.0.24898: S 1838062028:1838062028(0) win 512
62:69:d3:1c:79:ef 80:13:35:4:cb:d0 0.0.0.0.11587 > 0.0.0.0.7723: S 1792413296:1792413296(0) win 512
c5:a:b7:3e:3c:7a 3a:ee:c0:23:4a:fe 0.0.0.0.19784 > 0.0.0.0.57433: S 1018924173:1018924173(0) win 512
88:43:ee:51:c7:68 b4:8d:ec:3e:14:bb 0.0.0.0.283 > 0.0.0.0.11466: S 727776406:727776406(0) win 512
b8:7a:7a:2d:2c:ae c2:fa:2d:7d:e7:bf 0.0.0.0.32650 > 0.0.0.0.11324: S 605528173:605528173(0) win 512
e0:d8:1e:74:1:e 57:98:b6:5a:fa:de 0.0.0.0.36346 > 0.0.0.0.55700: S 2128143986:2128143986(0) win 512
```

Bu saldırı araçlarının tehlikeli olmasının bir başka nedeni de, yalnızca yerel anahtarı etkilemekle kalmaz, aynı zamanda diğer bağlı Katman 2 anahtarlarını da etkileyebilir. Bir anahtarın MAC adres tablosu dolduğunda, diğer Katman 2 anahtarlarına bağlı olanlar dahil tüm bağlantı noktalarına basmaya başlar.

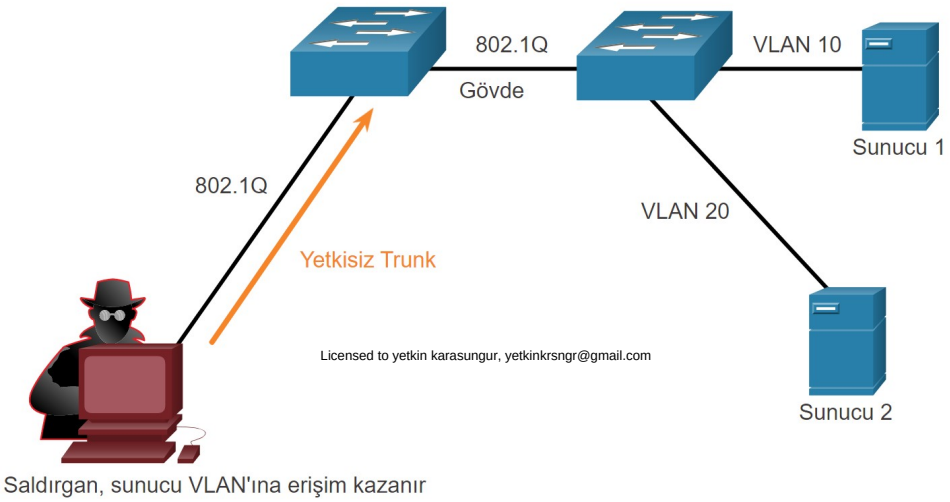
MAC adres tablosu taşma saldırılarını azaltmak için ağ yöneticilerinin bağlantı noktası güvenliğini uygulaması gerekir. Bağlantı noktası güvenliği, bağlantı noktasında yalnızca belirli sayıda kaynak MAC adresinin öğrenilmesine izin verecektir.

## 26.4.LAN Saldırıları

### 26.4.1.VLAN Atlama Saldırıları

Bir VLAN atlama saldırısı, bir VLAN'dan gelen trafiğin bir yönlendirici yardımı olmadan başka bir VLAN tarafından görülmesini sağlar. Temel bir VLAN atlamalı saldırıda, tehdit aktörü bir ana bilgisayarı, çoğu anahtar bağlantı noktasında varsayılan olarak etkinleştirilen otomatik bağlantı noktası bağlantı noktası özelliğinden yararlanacak bir anahtar gibi davranacak şekilde yapılandırır.

Tehdit aktörü, ana bilgisayarı bağlantı anahtarıyla bağlantı anahtarıyla 802.1Q sinyalizasyonunu ve Cisco'ya ait Dinamik Bağlantı Protokolü (DTP) sinyalizasyonunu sahte yapacak şekilde yapılandırır. Başarılı olursa, anahtar şekilde gösterildiği gibi, ana bilgisayarla bir ana hat bağlantısı kurar. Artık tehdit aktörü anahtardaki tüm VLAN'lara erişebilir. Tehdit aktörü, VLAN'lar arasında etkin bir şekilde atlayarak herhangi bir VLAN üzerinden trafik gönderip alabilir.

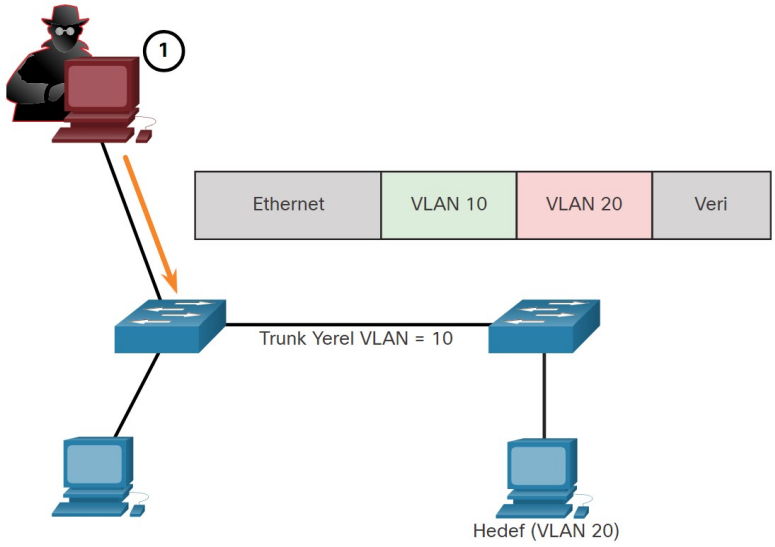


## 26.4.2.VLAN Çift Etiketleme Saldırısı

Belirli durumlarda bir tehdit aktörü, halihazırda bir 802.1Q etiketine sahip çerçevenin içine gizli bir 802.1Q etiketi yerleştirebilir. Bu etiket, çerçevenin, orijinal 802.1Q etiketinin belirtmediği bir VLAN'a gitmesine izin verir.

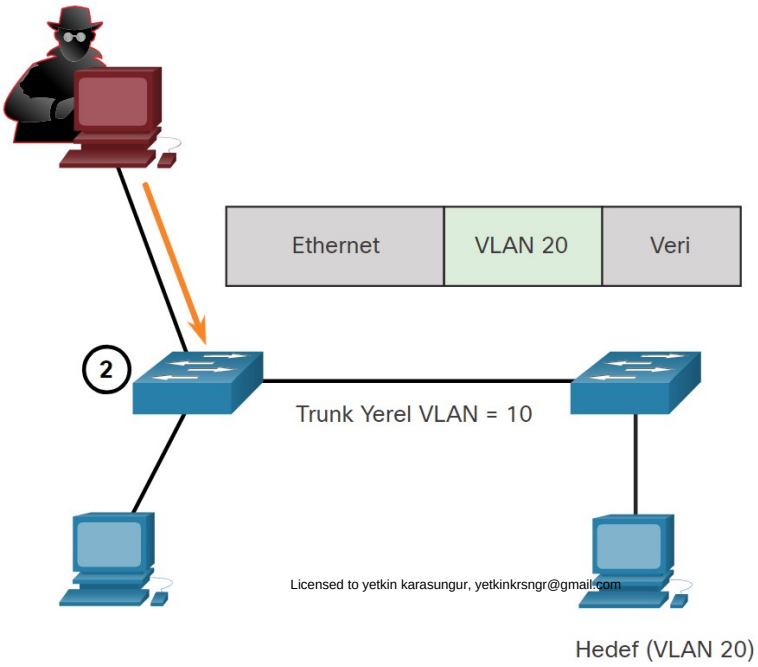
### Aşama 1

Tehdit aktörü, anahtara çift etiketli bir 802.1Q çerçeve gönderir. Dış başlık, ana hat bağlantı noktasının yerel VLAN'ıyla aynı olan tehdit aktörünün VLAN etiketine sahiptir. Bu örneğin amaçları için, bunun VLAN 10 olduğunu varsayın. İç etiket, bu örnekte, VLAN 20 kurban VLAN'dır.



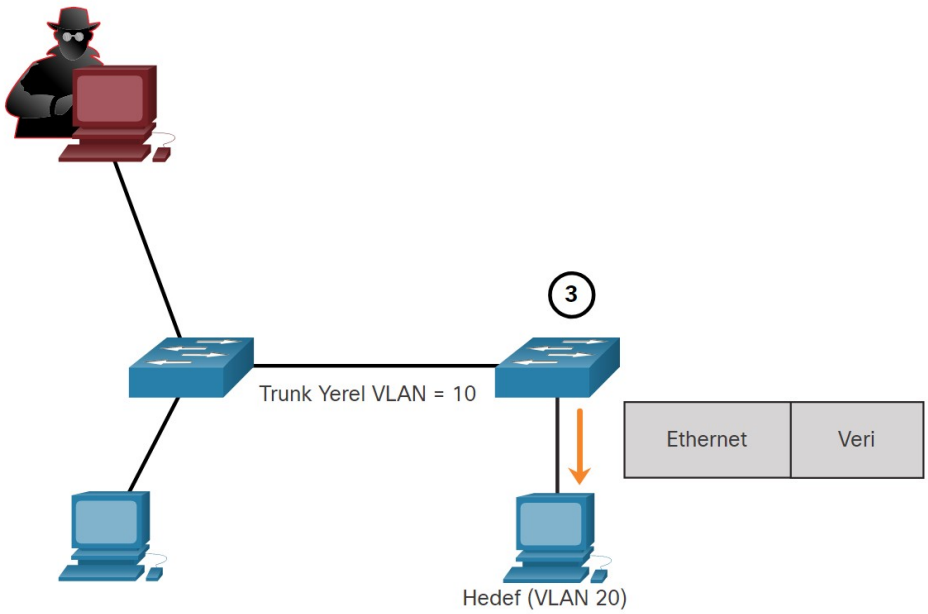

### Aşama 2

Çerçeve, ilk 4 bayt 802.1Q etiketine bakan ilk anahtara ulaşır. Anahtar, çerçevenin yerel VLAN olan VLAN 10'a yönelik olduğunu görüyor. Anahtar, VLAN 10 etiketini çıkardıktan sonra paketi tüm VLAN 10 bağlantı noktalarını iletir. Çerçeve, yerel VLAN'ın bir parçası olduğu için yeniden etiketlenmez. Bu noktada, VLAN 20 etiketi hala sağlamdır ve ilk anahtar tarafından incelenmemiştir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Çerçeve, VLAN 10 için olması gerektiğine dair hiçbir bilgisi olmayan ikinci anahtara ulaşır. Yerel VLAN trafiği, 802.1Q spesifikasyonunda belirtildiği gibi gönderen anahtar tarafından etiketlenmez. İkinci anahtar yalnızca tehdit aktörünün yerleştirdiği dahili 802.1Q etiketine bakar ve çerçevenin hedef VLAN olan VLAN 20'ye yönelik olduğunu görür. İkinci anahtar, hedef için mevcut bir MAC adres tablosu girişi olup olmamasına bağlı olarak çerçeveyi hedefe gönderir veya onu taşırır.




Bir VLAN çift etiketleme saldırısı tek yönlüdür ve yalnızca saldırgan, ana bağlantı noktasının yerel VLAN'ıyla aynı VLAN'da bulunan bir bağlantı noktasına bağlandığında çalışır. Buradaki fikir, çift etiketlemenin saldırganın bir VLAN üzerindeki ana bilgisayarlara veya sunuculara veri göndermesine izin vermesidir, aksi takdirde bir tür erişim kontrolü yapılandırması tarafından engellenir. Muhtemelen dönüş trafiğine de izin verilecek ve böylece saldırgana normalde engellenen VLAN'daki cihazlarla iletişim kurma yeteneği verilecek.

**VLAN Saldırısını Azaltma**

VLAN atlama ve VLAN çift etiketleme saldırıları, önceki bir modülde tartışıldığı gibi aşağıdaki ana hat güvenlik yönergeleri uygulanarak önlenebilir:

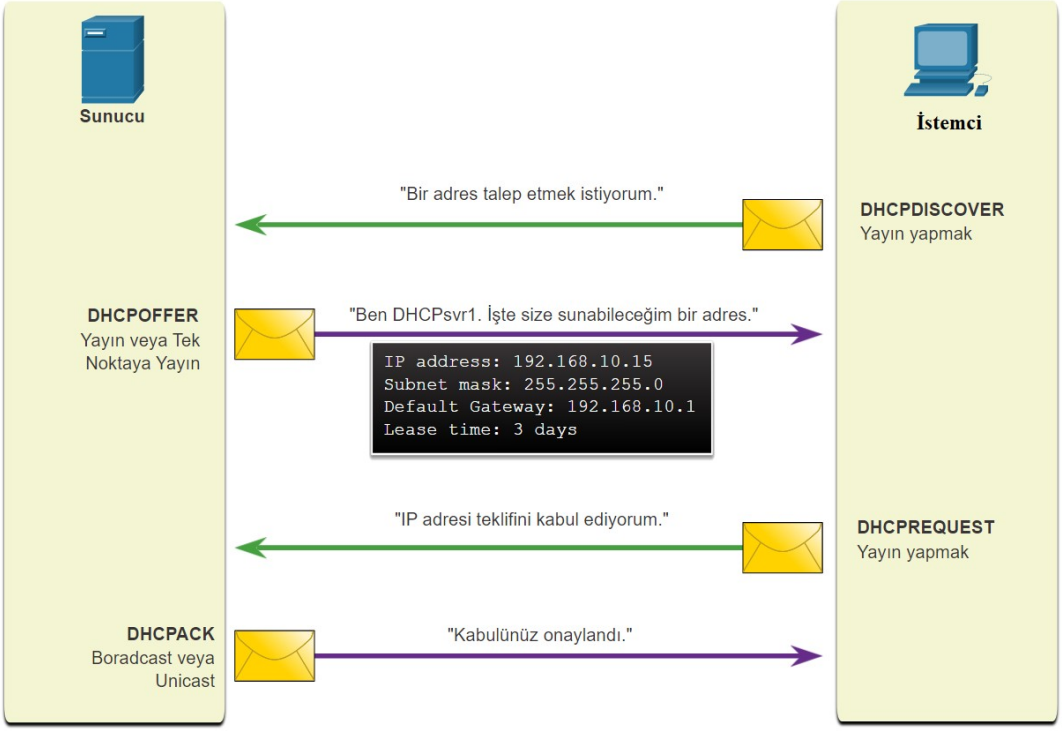
- Tüm erişim bağlantı noktalarında trunk oluşturmayı devre dışı bırakın.
- Ana hat bağlantılarında otomatik trunkı (DTP) devre dışı bırakın, böylece ana hatlar manuel olarak etkinleştirilmelidir.
- Yerel VLAN'ın yalnızca ana hat bağlantıları için kullanıldığından emin olun.

## 26.5.DHCP Saldırıları

### 26.5.1.DHCP Mesajları

DHCP sunucuları, istemcilere IP adresi, alt ağ maskesi, varsayılan ağ geçidi, DNS sunucuları ve daha fazlasını içeren IP yapılandırma bilgilerini dinamik olarak sağlar. İstemci ile sunucu arasındaki DHCP mesaj alışverişinin sırasının bir incelemesi şekilde gösterilmektedir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 26.5.2.DHCP Saldırıları

İki tür DHCP saldırısı, DHCP açlığı ve DHCP sahtekarlığıdır. Her iki saldırı da DHCP gözetleme uygulanarak hafifletilir.

### DHCP Starvation Saldırısı

DHCP Starvation saldırısının amacı, istemcileri bağlamak için bir DoS oluşturmaktır. DHCP açlık saldırıları, Gobbler veya Yersinia gibi bir saldırı aracı gerektirir.

Gobbler veya Yersinia, kiralanabilir IP adreslerinin tüm kapsamına bakma yeteneğine sahiptir ve hepsini kiralamaya çalışır. Özellikle, sahte MAC adresleriyle DHCP keşif mesajları oluşturur.

### DHCP Spoofing Saldırısı

Ağa sahte bir DHCP sunucusu bağlandığında ve yasal istemcilere yanlış IP yapılandırma parametreleri sağladığında bir DHCP sahtekarlığı saldırısı gerçekleşir. Kötü niyetli bir sunucu, çeşitli yanıltıcı bilgiler sağlayabilir:

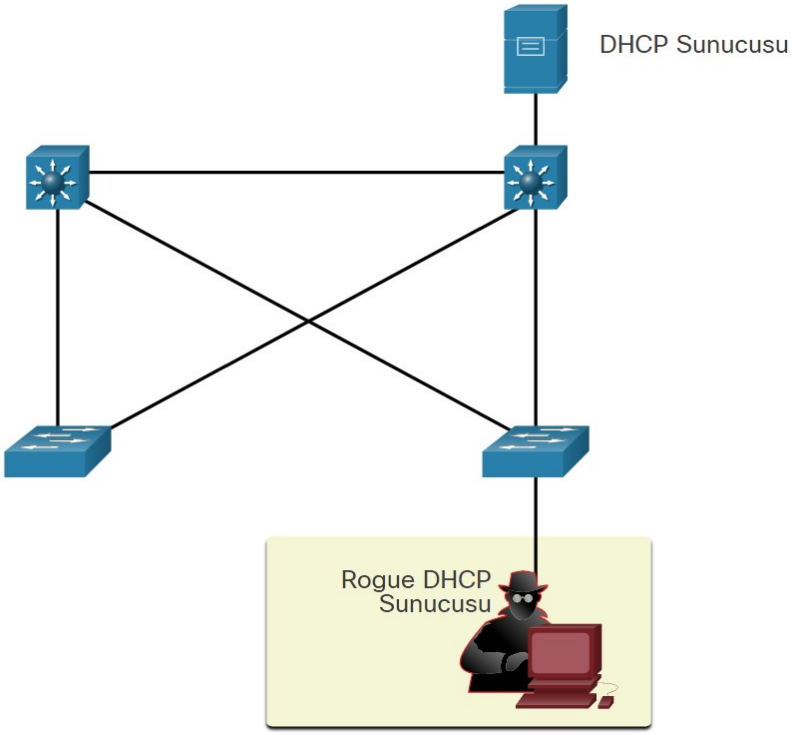
- Yanlış varsayılan ağ geçidi - Sahtesunucu, bir ortadaki adam saldırısı oluşturmak için geçersiz bir ağ geçidi veya ana bilgisayarının IP adresini sağlar. İzinsiz giren kişi ağ üzerinden veri akışını engellediği için bu tamamen fark edilmeyebilir.
- Yanlış DNS sunucusu - Sahte sunucu, kullanıcıyı sahte bir web sitesine yönlendiren yanlış bir DNS sunucusu adresi sağlar.
- Yanlış IP adresi - Sahte sunucu, DHCP istemcisinde etkili bir şekilde DoS saldırısı oluşturan geçersiz bir IP adresi sağlar.

### Aşama 1

Tehdit Aktörü, Rogue-Sahte DHCP Sunucusunu Bağlar

Bir tehdit aktörü, hileli bir DHCP sunucusunu hedef istemcilerle aynı alt ağ ve VLAN'lardaki bir anahtar bağlantı noktasına başarıyla bağlar. Sahte sunucunun amacı, istemcilere yanlış IP yapılandırma bilgisi sağlamaktır.

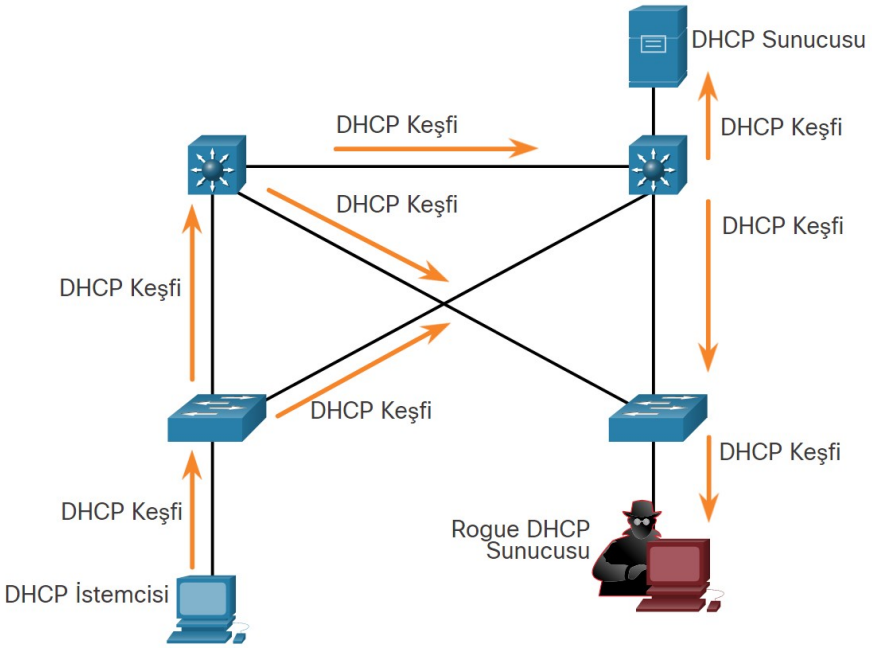
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




**Aşama 2**

İstemci DHCP Keşif Mesajlarını Yayınlar

Meşru bir istemci ağa bağlanır ve IP yapılandırma parametreleri gerektirir. Bu nedenle, istemci, bir DHCP sunucusundan bir yanıt arayan bir DHCP Bulma isteği yayınlar. Her iki sunucu da mesajı alacak ve yanıt verecektir.

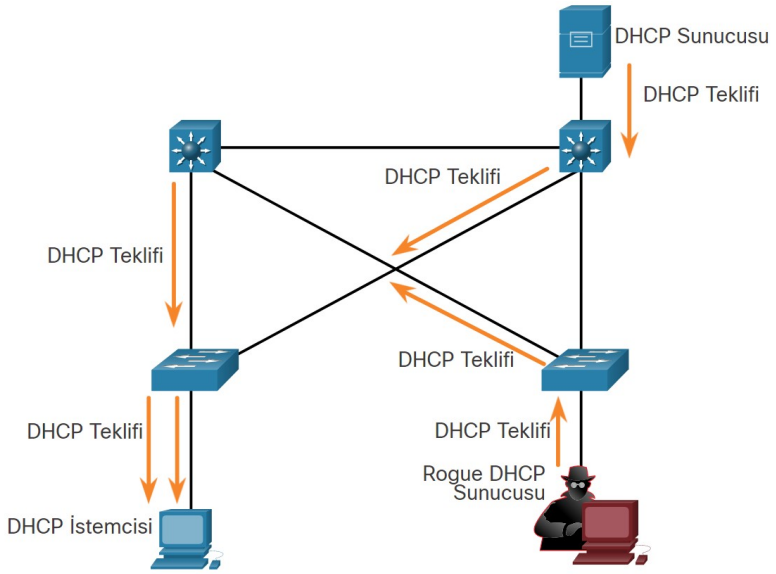



**Aşama 3**

Meşru ve Sahte DHCP Yanıtı

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

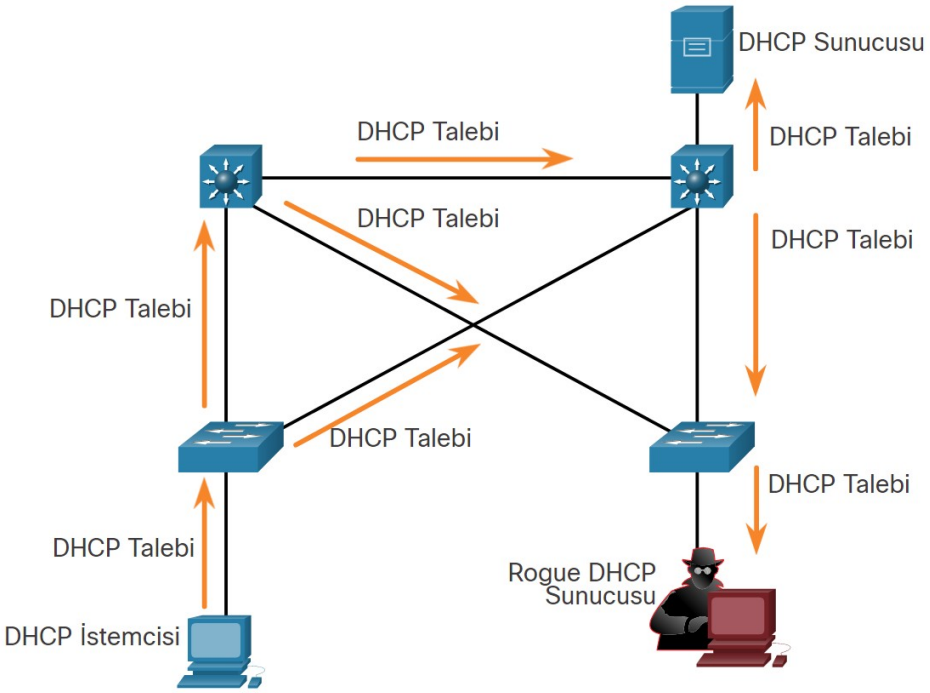
Meşru DHCP sunucusu, geçerli IP yapılandırma parametreleriyle yanıt verir. Ancak sahte sunucu, tehdit aktörü tarafından tanımlanan IP yapılandırma parametrelerini içeren bir DHCP teklifiyle de yanıt verir. İstemci alınan ilk teklife cevap verecektir.




**Aşama 4**

İstemci Rogue DHCP Teklifini Kabul Ediyor

İlk önce sahte teklif alındı ve bu nedenle istemci, tehdit aktörü tarafından tanımlanan IP parametrelerini kabul eden bir DHCP isteği yayınlar. Meşru ve dolandırıcı sunucu isteği alacaktır.

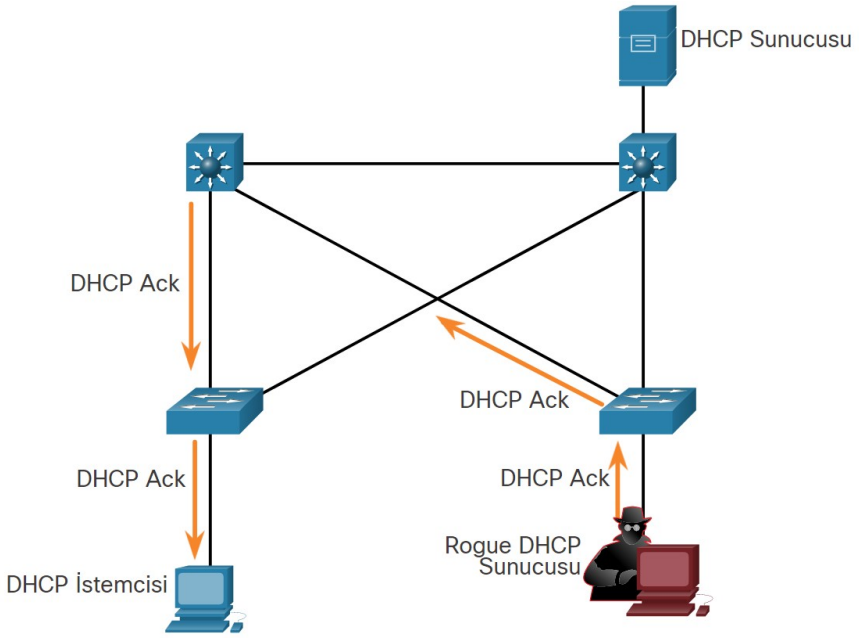



**Aşama 5**

Rogue Server Onayları

Sahte sunucu, istemciye isteğini kabul etmek için tek noktaya bir yanıt gönderir. Meşru sunucu, istemciyle iletişimi kesecektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




DHCP saldırıları DHCP Snooping yapılandırmasıyla azaltılabilir.

## 26.6.ARP Saldırıları

Belirli bir IPv4 adresine sahip bir ana bilgisayarın MAC adresini belirlemek için yayın yapan ARP İsteklerini barındıracağını hatırlayın. Bu genellikle varsayılan ağ geçidinin MAC adresini keşfetmek için yapılır. Alt ağdaki tüm ana bilgisayarlar ARP İsteğini alır ve işler. ARP İsteğinde eşleşen IPv4 adresine sahip ana bilgisayar bir ARP Yanıtı gönderir.

ARP RFC'ye göre, bir istemcinin "nedensiz-gratuitous ARP" adı verilen istenmeyen bir ARP İsteği göndermesine izin verilir. Bir ana bilgisayar karşılıksız bir ARP gönderdiğinde, alt ağdaki diğer ana bilgisayarlar, ücretsiz ARP'de bulunan MAC adresini ve IPv4 adresini kendi ARP tablolarında saklar.

Buradaki sorun, bir saldırganın sahte bir MAC adresi içeren ücretsiz bir ARP mesajını bir anahtara gönderebilmesi ve anahtarın MAC tablosunu buna göre güncellemesidir. Bu nedenle, herhangi bir ana bilgisayar, seçtikleri herhangi bir IP ve MAC adresi kombinasyonunun sahibi olduğunu iddia edebilir. Tipik bir saldırıda, bir tehdit aktörü, tehdit aktörünün MAC Adresi ve varsayılan ağ geçidinin IPv4 adresiyle alt ağdaki diğer ana bilgisayarlara istenmeyen ARP Yanıtları gönderebilir.

İnternette, dsniff, Cain & Abel, ettercap, Yersinia ve diğerleri dahil ARP ortadaki adam saldırıları oluşturmak için kullanılabilen birçok araç bulunmaktadır. IPv6, Katman 2 adres çözümlemesi için ICMPv6 Komşu Bulma Protokolünü kullanır. IPv6, IPv6'nın sahte bir ARP Yanıtını engellemesine benzer şekilde, Komşu Bildirimi sahtekarlığını azaltmaya yönelik stratejiler içerir.

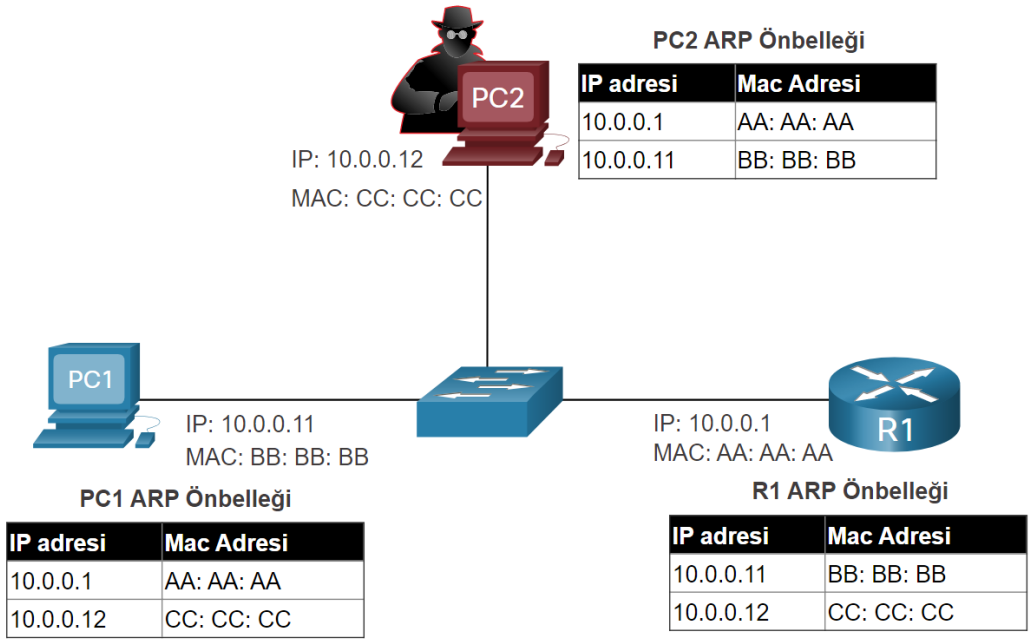
ARP sahtekarlığı ve ARP zehirlenmesi, DAI(Dynamic ARP Isnpection) uygulanarak hafifletilir.

### Aşama 1

Yakınsanmış MAC Tabloları ile Normal Durum

Her aygıt, LAN üzerindeki diğer aygıtlar için doğru IPv4 ve MAC adreslerini içeren doğru bir MAC tablosuna sahiptir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



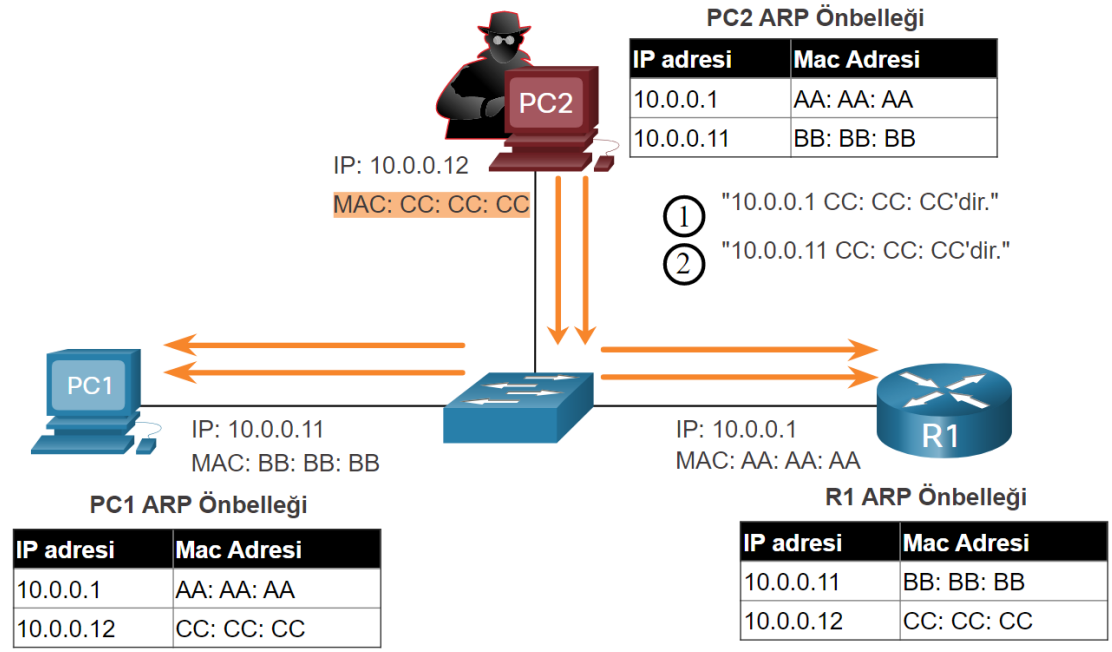

Not: MAC adresleri basitlik açısından 24 bit olarak gösterilmiştir.

**Aşama 2**

ARP Spoofing Saldırısı

Tehdit aktörü, varsayılan ağ geçidi olarak R1'i değiştirmek amacıyla iki sahte nedensiz ARP Yanıtı gönderir:

İlki, LAN üzerindeki tüm cihazlara, tehdit aktörünün MAC adresinin (CC: CC: CC) R1'in IPv4 adresi 10.0.0.1 ile eşleştiğini bildirir.
İkincisi, tehdit aktörünün MAC adresinin (CC: CC: CC) PC1'in IPv4 adresi 10.0.0.11 ile eşleştiğini LAN üzerindeki tüm cihazlara bildirir.



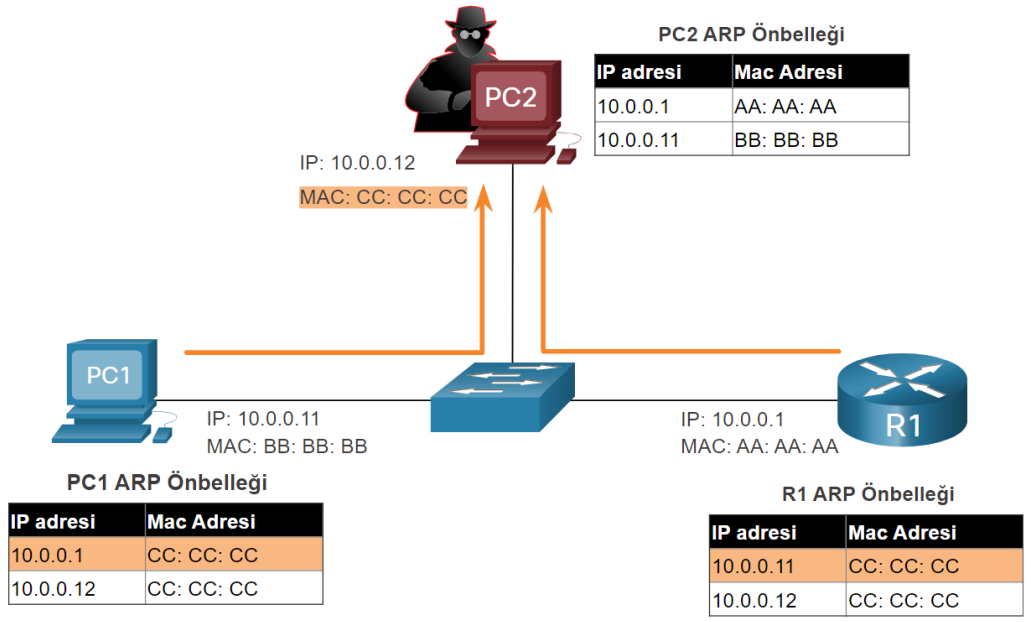

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not: MAC adresleri basitlik açısından 24 bit olarak gösterilmiştir

**Aşama 3**

Ortadaki Adam Saldırısı ile ARP Zehirleme Saldırısı

R1 ve PC1, birbirlerinin MAC adresi için doğru girişi kaldırır ve bunu PC2'nin MAC adresiyle değiştirir. Tehdit aktörü şimdi alt ağdaki tüm cihazların ARP önbelleklerini zehirledi. ARP zehirlenmesi, çeşitli ortadaki adam saldırılarına yol açarak ağ için ciddi bir güvenlik tehdidi oluşturur.

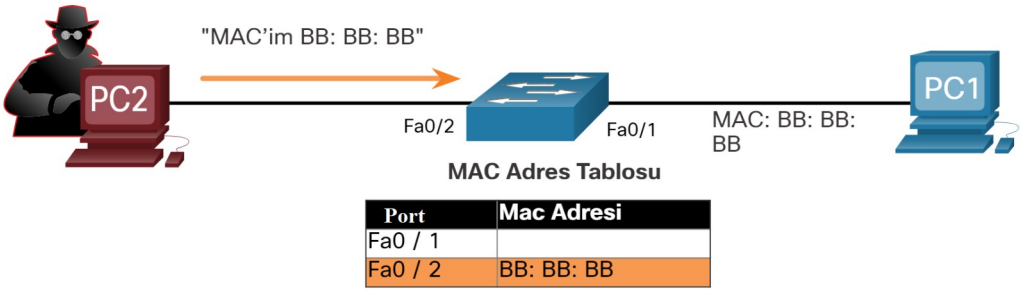



Not: MAC adresleri basitlik açısından 24 bit olarak gösterilmiştir.

## Adres Sahtekarlığı Saldırısı

IP adresleri ve MAC adresleri, çeşitli nedenlerle sahte olabilir. IP adresi sahtekarlığı, bir tehdit aktörünün alt ağdaki başka bir cihazın geçerli bir IP adresini ele geçirmesi veya rastgele bir IP adresi kullanmasıdır. IP adresi sahtekarlığının azaltılması, özellikle IP'nin ait olduğu bir alt ağ içinde kullanıldığında zordur.

MAC adresi sahtekarlığı saldırıları, tehdit aktörleri ana bilgisayarlarının MAC adresini bir hedef ana bilgisayarın bilinen başka bir MAC adresiyle eşleşecek şekilde değiştirdiğinde meydana gelir. Saldıran ana bilgisayar daha sonra yeni yapılandırılmış MAC adresiyle ağ boyunca bir çerçeve gönderir. Anahtar çerçeveyi aldığında, kaynak MAC adresini inceler. Anahtar, mevcut MAC tablosu girişinin üzerine yazar ve MAC adresini şekilde gösterildiği gibi yeni porta atar. Daha sonra, hedef ana bilgisayar için belirlenen çerçeveleri yanlışlıkla saldıran ana bilgisayara iletir.




Not: MAC Adresleri, basitlik açısından 24 bit olarak gösterilmiştir

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Hedef ana bilgisayar trafik gönderdiğinde, anahtar, MAC adresini orijinal bağlantı noktasına yeniden hizalayarak hatayı düzeltir. Anahtarın bağlantı noktası atamasını doğru durumuna döndürmesini engellemek için, tehdit aktörü anahtara sürekli olarak çerçeveler gönderecek bir program veya komut dosyası oluşturabilir, böylece

anahtar yanlış veya sahte bilgileri korur. Katman 2'de, bir anahtarın MAC adreslerinin kaynağını doğrulamasına izin veren bir güvenlik mekanizması yoktur, bu da onu sahtekarlığa karşı bu kadar savunmasız kılar.

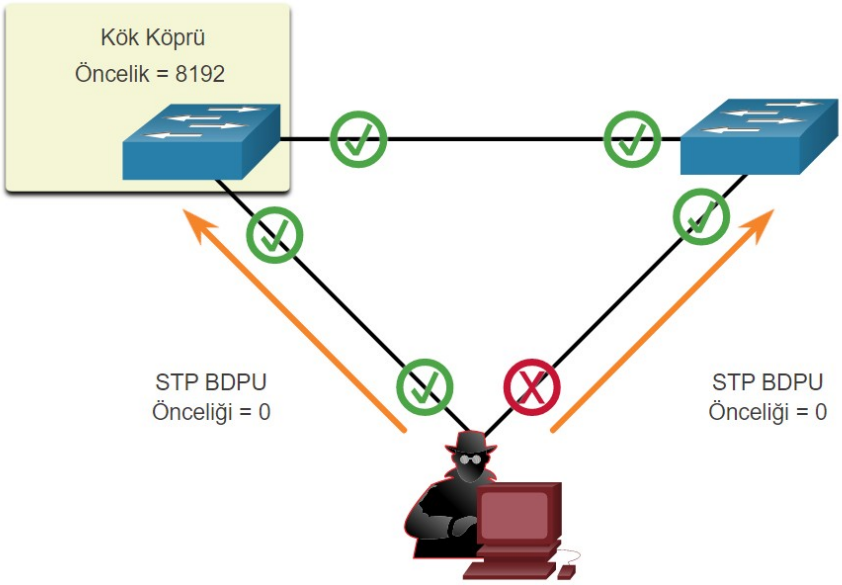
IP ve MAC adresi sahtekarlığı, IPSG (IP Source Guard) uygulanarak azaltılabilir.

## 26.7.STP Saldırısı

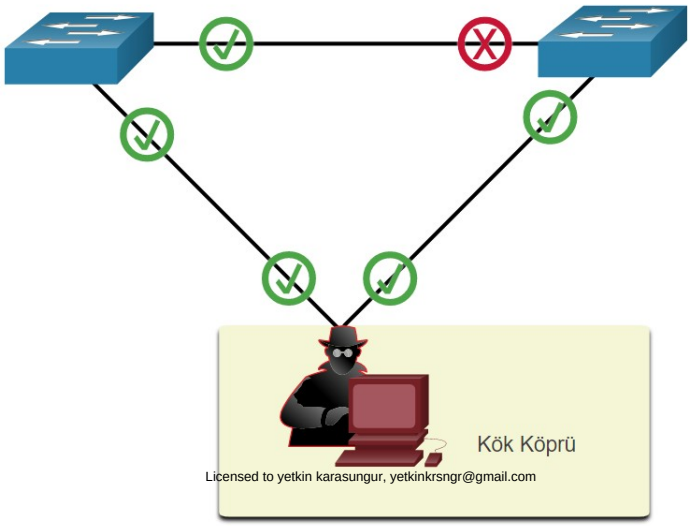
Ağ saldırganları, kök köprüyü (root bridge) taklit ederek ve bir ağın topolojisini değiştirerek bir saldırı gerçekleştirmek için Yayılan Ağaç Protokolünü (STP) manipüle edebilir. Saldırganlar, ana bilgisayarlarının kök köprüler gibi görünmesini sağlayabilir; ve bu nedenle, hemen değiştirilen etki alanı için tüm trafiği yakalayın.

Bir STP manipülasyon saldırısı gerçekleştirmek için saldıran ana bilgisayar, şekilde gösterildiği gibi genişleyen ağaç yeniden hesaplamalarını zorlayacak konfigürasyon ve topoloji değişikliklerini içeren STP köprü protokolü veri birimlerini (BPDU'lar) yayınlar. Saldıran ana bilgisayar tarafından gönderilen BPDU'lar, temel köprü olarak seçilme girişiminde daha düşük bir köprü önceliğini duyurur.

Not : Bu sorunlar, herhangi bir kötü niyet olmaksızın birisi ağa bir Ethernet anahtarı eklediğinde de ortaya çıkabilir.




Başarılı olursa, saldıran ana bilgisayar şekilde gösterildiği gibi temel köprü haline gelir ve artık başka türlü erişilemeyen çeşitli çerçeveleri yakalayabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 26.8.CDP Saldırıları

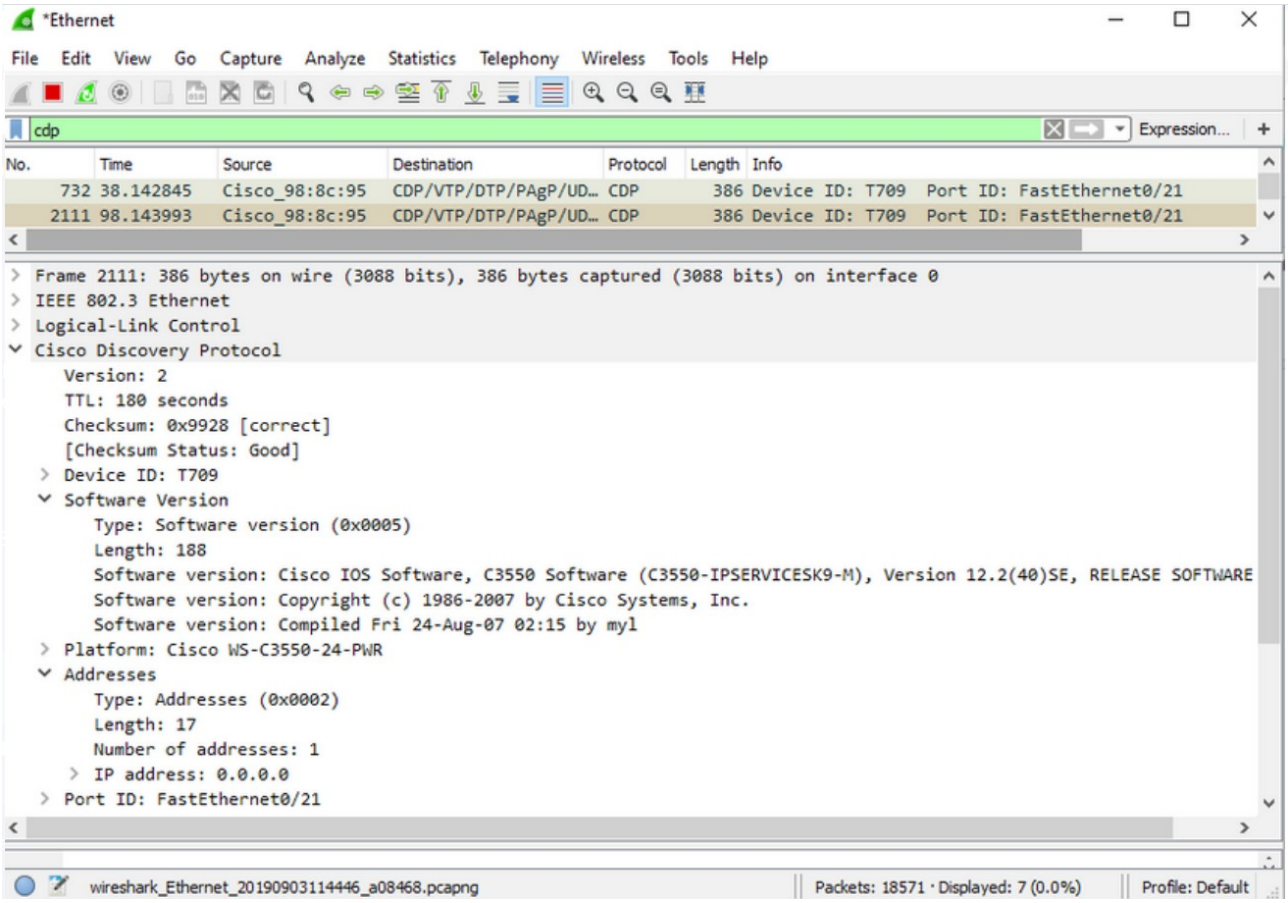
Cisco Keşif Protokolü (CDP), tescilli bir Katman 2 bağlantı keşif protokolüdür. Varsayılan olarak tüm Cisco cihazlarında etkindir. CDP, diğer CDP etkin aygıtları otomatik olarak keşfedebilir ve bağlantılarının otomatik olarak yapılandırılmasına yardımcı olabilir. Ağ yöneticileri ayrıca ağ aygıtlarını yapılandırmaya ve sorun gidermeye yardımcı olması için CDP kullanır.

CDP bilgileri, düzenli, şifrelenmemiş çok noktaya yayınla CDP etkin bağlantı noktalarına gönderilir. CDP bilgileri, aygıtın IP adresini, IOS yazılım sürümünü, platformu, yetenekleri ve yerel VLAN'ı içerir. CDP mesajını alan cihaz, CDP veritabanını günceller.

CDP bilgileri, ağ sorunlarını gidermede son derece yararlıdır. Örneğin CDP, Katman 1 ve 2 bağlantısını doğrulamak için kullanılabilir. Bir yönetici doğrudan bağlı bir arabirime ping atamazsa, ancak yine de CDP bilgilerini alıyorsa, sorun büyük olasılıkla Katman 3 yapılandırmasıyla ilgilidir.

Bununla birlikte, CDP tarafından sağlanan bilgiler bir tehdit aktörü tarafından ağ altyapısı açıklarını keşfetmek için de kullanılabilir.

Şekilde, örnek bir Wireshark yakalaması bir CDP paketinin içeriğini görüntüler. Saldırgan, cihaz tarafından kullanılan Cisco IOS yazılım sürümünü belirleyebilir. Bu, saldırganın o IOS sürümüne özgü herhangi bir güvenlik açığı olup olmadığını belirlemesine olanak tanır.




CDP yayınları şifrelenmemiş ve kimliği doğrulanmamış olarak gönderilir. Bu nedenle, bir saldırgan doğrudan bağlı Cisco cihazlarına sahte cihaz bilgileri içeren hazırlanmış CDP çerçeveleri göndererek ağ altyapısına müdahale edebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

CDP'nin kötüye kullanımını azaltmak için, CDP'nin aygıtlarda veya bağlantı noktalarında kullanımını sınırlayın. Örneğin, güvenilmeyen cihazlara bağlanan uç bağlantı noktalarında CDP'yi devre dışı bırakın.

Bir aygıtta CDP'yi genel olarak devre dışı bırakmak için, **no cdp run** global yapılandırma modu komutunu kullanın. CDP'yi global olarak etkinleştirmek için **cdp run** global yapılandırma komutunu kullanın.

Bir bağlantı noktasında CDP'yi devre dışı bırakmak için, **no cdp enable** arabirim yapılandırma komutunu kullanın. Bir bağlantı noktasında CDP'yi etkinleştirmek için **cdp enable** arabirim yapılandırma komutunu kullanın.

Not : Bağlantı Katmanı Bulma Protokolü (LLDP) de keşif saldırılarına karşı savunmasızdır. LLDP'yi genel olarak devre dışı bırakmak için **no lldp run** global yapılandırma komutunu kullanın . Arayüz üzerinde LLDP'yi devre dışı bırakmak için, **no lldp transmit** ve **no lldp receive** arabirim yapılandırma komutunlarını kullanın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 27. Bölüm: Güvenli Anahtar Yapılandırması

## 27.1.Bağlantı Noktası Güvenliğini (Port Security) Uygulama

### 27.1.1.Kullanılmayan Portlar

Katman 2 cihazları, bir şirketin güvenlik altyapısındaki en zayıf halka olarak kabul edilir. Katman 2 saldırıları, bilgisayar korsanlarının dağıtması en kolay olanlardandır, ancak bu tehditler bazı yaygın Katman 2 çözümleriyle azaltılabilir.

Anahtar üretimde kullanım için dağıtılmadan önce tüm anahtar bağlantı noktaları (arabirimler) güvenli hale getirilmelidir. Bir bağlantı noktasının nasıl güvenli hale getirildiği, işlevine bağlıdır.

Ağın yetkisiz erişimden korunmasına yardımcı olmak için birçok yöneticinin kullandığı basit bir yöntem, bir anahtardaki tüm kullanılmayan bağlantı noktalarını devre dışı bırakmaktır. Örneğin, bir Catalyst 2960 anahtarında 24 bağlantı noktası varsa ve kullanımda olan üç Hızlı Ethernet bağlantısı varsa, kullanılmayan 21 bağlantı noktasını devre dışı bırakmak iyi bir uygulamadır. Kullanılmayan her bağlantı noktasına gidin ve Cisco IOS **shutdown** komutunu verin. Bir bağlantı noktasının daha sonra yeniden etkinleştirilmesi gerekiyorsa, **no shutdown** komutuyla etkinleştirilebilir .

Bir dizi bağlantı noktasını yapılandırmak için **interface range** komutunu kullanın.

```
Switch(config)# interface range type module/first-number - last-number
```

Örneğin, S1'de Fa0 / 8'den Fa0 / 24'e kadar portları kapatmak için aşağıdaki komutu girmelisiniz.

```
S1(config)# interface range fa0/8 - 24
S1(config-if-range)# shutdown
%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to administratively down
(output omitted)
%LINK-5-CHANGED: Interface FastEthernet0/24, changed state to administratively down
S1(config-if-range)#
```

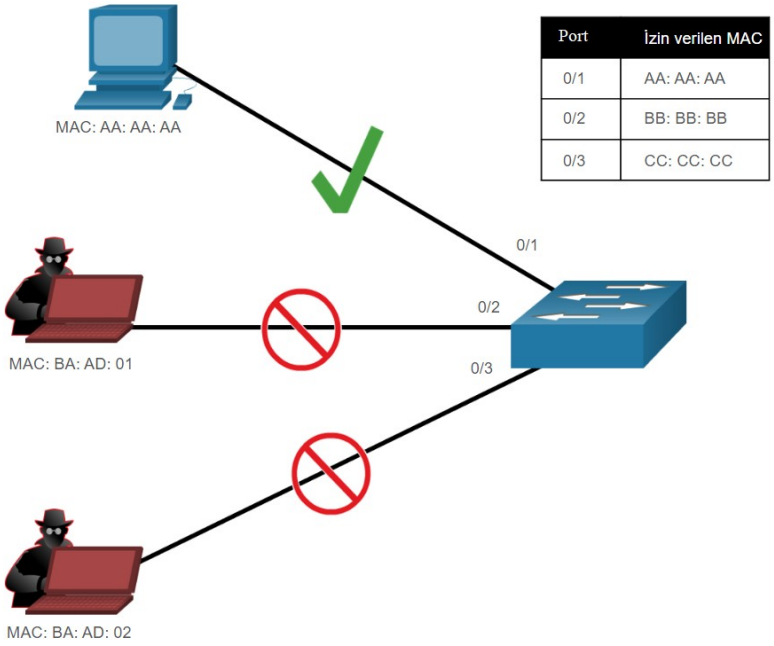
### 27.1.2.MAC Adres Tablosu Saldırılarını Azaltma

MAC adres tablosu taşma saldırılarını önlemenin en basit ve en etkili yöntemi, bağlantı noktası güvenliğini (Port Security) sağlamaktır.

Bağlantı noktası güvenliği, bir bağlantı noktasında izin verilen geçerli MAC adreslerinin sayısını sınırlar. Bir yöneticinin bir bağlantı noktası için MAC adreslerini manuel olarak yapılandırmasına veya anahtarın sınırlı sayıda MAC adresini dinamik olarak öğrenmesine izin vermesine olanak tanır. Bağlantı noktası güvenliğiyle yapılandırılan bir bağlantı noktası bir çerçeve aldığında, çerçevenin kaynak MAC adresi, bağlantı noktasında manuel olarak yapılandırılan veya dinamik olarak öğrenilen güvenli kaynak MAC adresleri listesiyle karşılaştırılır.

Bir bağlantı noktasında izin verilen MAC adreslerinin sayısı bir ile sınırlandırılarak, şekilde gösterildiği gibi ağa yetkisiz erişimi kontrol etmek için bağlantı noktası güvenliği kullanılabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




| Port | İzin verilen MAC |
|---|---|
| 0/1 | AA: AA: AA |
| 0/2 | BB: BB: BB |
| 0/3 | CC: CC: CC |

**Not** : MAC adresleri basitlik açısından 24 bit olarak gösterilmiştir.

## 27.1.3.Bağlantı Noktası Güvenliğini Etkinleştirme

Örnek yapılandırmaya dikkat edin. **switchport port-security** komutu reddedildi. Bunun nedeni, bağlantı noktası güvenliğinin yalnızca manuel olarak yapılandırılmış erişim bağlantı noktalarında veya elle yapılandırılan ana hat-trunk bağlantı noktalarında yapılandırılabilmesidir. Varsayılan olarak, Katman 2 anahtar bağlantı noktaları dinamik otomatik (trunking açık) olarak ayarlanmıştır. Bu nedenle, örnekte bağlantı noktası, anahtar bağlantı noktası modu **switchport mode access** yapılandırma komutuyla yapılandırılır.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security
Command rejected: FastEthernet0/1 is a dynamic port.
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# end
S1#
```

FastEthernet 0/1 için geçerli bağlantı noktası güvenlik ayarlarını örnekte gösterildiği gibi görüntülemek için **show port-security interface** komutunu kullanın. Bağlantı noktası güvenliğinin nasıl etkinleştirildiğine, bağlantı noktası durumunun Güvenli-kapalı(Secure-Down) olduğuna, yani bağlı cihaz olmadığı ve ihlal olmadığı, ihlal modunun Kapat (Shutdown) ve maksimum MAC adresi sayısının 1 olduğuna dikkat edin. bağlantı noktası, anahtar bağlantı noktası durumu Secure-up'ı görüntüler ve anahtar, aygıtın MAC adresini güvenli bir MAC olarak otomatik olarak ekler. Bu örnekte, bağlantı noktasına hiçbir cihaz bağlı değildir.

```
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bağlantı noktası güvenliği etkinleştirildikten sonra, örnekte gösterildiği gibi diğer bağlantı noktası güvenlik özellikleri yapılandırılabilir.

```
S1(config-if)# switchport port-security ?
  aging        Port-security aging commands
  mac-address  Secure mac address
  maximum      Max secure addresses
  violation    Security violation mode <cr>
S1(config-if)# switchport port-security
```

## 27.1.4.MAC Adreslerini Sınırlama ve Öğrenme

Bir bağlantı noktasında izin verilen maksimum MAC adresi sayısını ayarlamak için aşağıdaki komutu kullanın:

```
Switch(config-if)# switchport port-security maximum value
```

Varsayılan bağlantı noktası güvenlik değeri 1'dir. Yapılandırılabilecek maksimum güvenli MAC adresi sayısı anahtara ve IOS'a bağlıdır. Bu örnekte, maksimum 8192'dir.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security maximum ?
  <1-8192>  Maximum addresses
S1(config-if)# switchport port-security maximum
```

Anahtar, üç yoldan biriyle güvenli bir bağlantı noktasındaki MAC adreslerini öğrenecek şekilde yapılandırılabilir:

### 1 . Elle-Manuel (Manually ) Yapılandırılmış

Yönetici, bağlantı noktasındaki her güvenli MAC adresi için aşağıdaki komutu kullanarak manuel olarak statik bir MAC adresi / adresleri yapılandırır:

```
Switch(config-if)# switchport port-security mac-address mac-address
```

### 2 . Dinamik Olarak Öğrenilmiş

Ne zaman **switchport port-security** komutu girilirse, bağlantı noktasına bağlı aygıt için MAC otomatik sabitlenir fakat başlangıç yapılandırması için eklenmez. Anahtar yeniden başlatılırsa, bağlantı noktasının aygıtın MAC adresini yeniden öğrenmesi gerekecektir.

### 3 . Dinamik Olarak Öğrenilmiş - Yapışkan-Sticky

Yönetici, aşağıdaki komutu kullanarak anahtarın MAC adresini dinamik olarak öğrenmesini ve bunları çalışan yapılandırmaya "yapıştırmasını" etkinleştirebilir:

```
Switch(config-if)# switchport port-security mac-address sticky
```

Çalışan yapılandırmanın kaydedilmesi, dinamik olarak öğrenilen MAC adresini NVRAM'a kaydedecektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aşağıdaki örnek, Fa0 / 1 bağlantı noktasına bağlı bir ana bilgisayar ile FastEthernet 0/1 için eksiksiz bir bağlantı noktası güvenlik yapılandırmasını gösterir. Yönetici maksimum 2 MAC adresi belirler, bir güvenli MAC adresini manuel olarak yapılandırır ve ardından bağlantı noktasını maksimum 2 güvenli MAC adresine kadar ek güvenli

MAC adreslerini dinamik olarak öğrenecek şekilde yapılandırır. Yapılandırmayı doğrulamak için **show port-security interfaces** ve **show port-security address** komutunu kullanın.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport port-security
S1(config-if)# switchport port-security maximum 2
S1(config-if)# switchport port-security mac-address aaaa.bbbb.1234
S1(config-if)# switchport port-security mac-address sticky
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1# show port-security address
               Secure Mac Address Table
-------------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                     (mins)
----    -----------       ----                          -----   -------------
1    a41f.7272.676a    SecureSticky                 Fa0/1        -
1    aaaa.bbbb.1234    SecureConfigured             Fa0/1        -
-------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max  Addresses limit in System (excluding one mac per port) : 8192
S1#
```

## 27.1.5.Port Güvenliği Eskimesi

Bağlantı noktası güvenliği eskimesi, bir bağlantı noktasındaki statik ve dinamik güvenli adreslerin yaşlanma (aging) süresini ayarlamak için kullanılabilir. Bağlantı noktası başına iki tür yaşlandırma desteklenir:

- Mutlak -Absolute: Bağlantı noktasındaki güvenli adresler, belirtilen eskime süresinden sonra silinir.
- Hareketsizlik - Inactivity :Bağlantı noktasındaki güvenli adresler, yalnızca belirtilen eskime süresi boyunca etkin değillerse silinir.

Mevcut güvenli MAC adreslerini manuel olarak silmeden güvenli bir bağlantı noktasındaki güvenli MAC adreslerini kaldırmak için eskimeyi kullanın. Yaşlanma süresi sınırları, yeni MAC adresleri eklenirken bile geçmiş güvenli MAC adreslerinin kalmasını sağlamak için artırılabilir. Statik olarak yapılandırılmış güvenli adreslerin eskimesi, bağlantı noktası bazında etkinleştirilebilir veya devre dışı bırakılabilir.

Güvenli bağlantı noktası için statik yaşlanmayı etkinleştirmek veya devre dışı bırakmak ya da eskime süresini veya türünü ayarlamak için s**witchport port-security aging** komutunu kullanın.

```
Switch(config-if)# switchport port-security aging { static | time time | type {absolute | inactivity}}
```

Komut için parametreler tabloda açıklanmıştır.

| Parametre | Açıklama |
|---|---|
| statik | Bu bağlantı noktasında statik olarak yapılandırılmış güvenli adresler için yaşlanmayı etkinleştirin. |
| time *time* | Bu bağlantı noktası için eskime süresini belirtin. Aralık 0 - 1440 dakikadır. Zaman 0 ise, bu bağlantı noktası için eskime devre dışı bırakılır. |
| type absolute | Mutlak yaşlanma süresini ayarlayın. Bu bağlantı noktasındaki tüm güvenli adresler, belirtilen süreden (dakika olarak) tam olarak sonra eskir ve güvenli adres listesinden kaldırılır. |
| type inactivity | Hareketsizlik yaşlanma türünü ayarlayın. Bu bağlantı noktasındaki güvenli adresler, yalnızca belirtilen süre boyunca güvenli kaynak adresinden veri trafiği yoksa eskir. |

Not : MAC adresleri basitlik açısından 24 bit olarak gösterilmiştir.

Örnek, eskime türünü 10 dakikalık hareketsizlik olarak yapılandıran ve yapılandırmayı doğrulamak için **show port-security interface** komutunu kullanan bir yöneticiyi gösterir .

```
S1(config)# interface fa0/1
S1(config-if)# switchport port-security aging time 10
S1(config-if)# switchport port-security aging type inactivity
S1(config-if)# end
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

## 27.1.6.Port Güvenliği İhlal Modları

Bağlantı noktasına bağlı bir aygıtın MAC adresi, güvenli adresler listesinden farklıysa, bağlantı noktası ihlali oluşur. Varsayılan olarak, bağlantı noktası hata devre dışı durumuna girer.

Bağlantı noktası güvenlik ihlali modunu ayarlamak için aşağıdaki komutu kullanın:

```
Switch(config-if)# switchport port-security violation { protect | restrict | shutdown}
```

Aşağıdaki tablolar, bir anahtarın yapılandırılmış ihlal moduna göre nasıl tepki verdiğini gösterir.

### Güvenlik İhlali Modu Açıklamaları

| Mod | Açıklama |
|---|---|
| kapat-shutdown (varsayılan) | Bağlantı noktası hemen hata devre dışı durumuna geçer, bağlantı noktası LED'ini kapatır ve bir syslog mesajı gönderir. İhlal sayacını artırır. Güvenli bir bağlantı noktası hata devre dışı durumdayken, bir yöneticinin **shutdown** ve **no shutdown** komutu girerek onu yeniden etkinleştirmesi gerekir. |
| kısıtlamak-restrict | Maksimum değerin altına düşmek veya maksimum değeri artırmak için yeterli sayıda güvenli MAC adresini kaldırana kadar, bağlantı noktası bilinmeyen kaynak adresli paketleri bırakır. Bu mod, Güvenlik İhlali sayacının artmasına neden olur ve bir sistem günlüğü mesajı oluşturur. |
| korumak-protect | Bu, güvenlik ihlali modları arasında en az güvenlidir. Maksimum değerin altına düşmek veya maksimum değeri artırmak için yeterli sayıda güvenli MAC adresini kaldırana kadar, port, MAC kaynak adresleri bilinmeyen paketleri bırakır. Sistem günlüğü mesajı gönderilmez. |

Licensed to yetkin karasungur, yetkinkrshgr@gmail.com

### Güvenlik İhlali Modu Karşılaştırması

| İhlal Modu | Rahatsız Edici Trafiği Atar | Sistem Günlüğü Mesajı Gönderir | İhlal Sayacını Artırır | Bağlantı Noktasını Kapatır |
|---|---|---|---|---|
| Koru | Evet | Hayır | Hayır | Hayır |
| Kısıtla | Evet | Evet | Evet | Hayır |
| Kapat | Evet | Evet | Evet | Evet |

Aşağıdaki örnek, bir yöneticinin güvenlik ihlalini "kısıtla" olarak değiştirdiğini göstermektedir. **Show port-security interface** komutunun çıktısı , değişikliğin yapıldığını doğrular.

```
S1(config)# interface f0/1
S1(config-if)# switchport port-security violation restrict
S1(config-if)# end
S1#
S1# show port-security interface f0/1
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Restrict
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7272.676a:1
Security Violation Count   : 0
S1#
```

### Hata Devre Dışı (Error Disable )Durumdaki Bağlantı Noktaları

Bağlantı noktası güvenlik ihlali kapatıldığında ve bir bağlantı noktası ihlali meydana geldiğinde ne olur? Bağlantı noktası fiziksel olarak kapatılır ve hata devre dışı bırakılır ve bu bağlantı noktasında trafik gönderilmez veya alınmaz.

Şekilde, bağlantı noktası güvenlik ihlali varsayılan kapatma ayarına döndürülmüştür. Daha sonra a41f.7272.676a MAC adresine sahip ana bilgisayarın bağlantısı kesilir ve Fa0 / 1'e yeni bir ana bilgisayar takılır.

Konsolda bağlantı noktası güvenliği ile ilgili bir dizi mesajın nasıl üretildiğine dikkat edin.

```
S1(config)# int fa0/1
S1(config-if)# switchport port-security violation shutdown
S1(config-if)# end
S1#
*Mar  1 00:24:15.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
*Mar  1 00:24:16.606: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
*Mar  1 00:24:19.114: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:24:20.121: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
S1#
*Mar  1 00:24:32.829: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/1, putting Fa0/1 in
err-disable state
*Mar  1 00:24:32.838: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC
address a41f.7273.018c on port FastEthernet0/1.
*Mar  1 00:24:33.836: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
down
*Mar  1 00:24:34.843: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to down
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Örnekte, **show interface** komutu bağlantı noktası durumunu hatalı devre dışı olarak tanımlar . **Show port-security interface** komutunun çıktısı artık bağlantı noktası durumunu Secure-up yerine Secure-shutdown olarak gösteriyor. Güvenlik İhlali sayacı 1 artar.

```
S1# show interface fa0/1 | include down
FastEthernet0/18 is down, line protocol is down (err-disabled)
(output omitted)
S1# show port-security interface fa0/1
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 10 mins
Aging Type                 : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 1
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : a41f.7273.018c:1
Security Violation Count   : 1
S1#
```

Yönetici, güvenlik ihlaline neyin neden olduğunu belirlemelidir. Güvenli bir bağlantı noktasına yetkisiz bir aygıt bağlanırsa, bağlantı noktası yeniden etkinleştirilmeden önce güvenlik tehdidi ortadan kaldırılır.

Bir sonraki örnekte, ilk ana bilgisayar Fa0 / 1'e yeniden bağlanır. Bağlantı noktasını yeniden etkinleştirmek için önce **shutdown** komutunu kullanın, ardından örnekte gösterildiği gibi bağlantı noktasını çalışır hale getirmek için **no shutdown** komutunu kullanın.

```
S1(config)# interface fa0/1
S1(config-if)# shutdown
S1(config-if)#
*Mar  1 00:39:54.981: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively
S1(config-if)# no shutdown
S1(config-if)#
*Mar  1 00:40:04.275: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:40:05.282: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to
up
S1(config-if)#
```

### Bağlantı Noktası Güvenliğini Doğrulama

Bir anahtarda bağlantı noktası güvenliğini yapılandırdıktan sonra, bağlantı noktası güvenliğinin doğru ayarlandığını doğrulamak için her arabirimi kontrol edin ve statik MAC adreslerinin doğru şekilde yapılandırıldığından emin olun.

### Tüm Arayüzler için Port Güvenliği

Anahtarın bağlantı noktası güvenlik ayarlarını görüntülemek için **show port-security** komutunu kullanın. Örnek, **switchport port-security** komutuyla yalnızca bir bağlantı noktasının yapılandırıldığını gösterir.

```
S1# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
--------------------------------------------------------------------------
      Fa0/1              2            2                  0         Shutdown
--------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Belirli Bir Arayüz için Port Güvenliği

Daha önce ve bu örnekte gösterildiği gibi, belirli bir arayüzün ayrıntılarını görüntülemek için **show port-security interface** komutunu kullanın.

```
S1# show port-security interface fastethernet 0/1
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 10 mins
Aging Type                  : Inactivity
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
Total MAC Addresses         : 2
Configured MAC Addresses    : 1
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : a41f.7273.018c:1
Security Violation Count    : 0
S1#
```

### Öğrenilen MAC Adreslerini Doğrulama

MAC adreslerinin konfigürasyona "yapıştığını" doğrulamak için, FastEthernet 0/19 örneğinde gösterildiği gibi **show run** komutunu kullanın.

```
S1# show run interface fa0/1
Building configuration...

Current configuration : 365 bytes
!
interface FastEthernet0/1
 switchport mode access
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky a41f.7272.676a
 switchport port-security mac-address aaaa.bbbb.1234
 switchport port-security aging time 10
 switchport port-security aging type inactivity
 switchport port-security
end
```

### Güvenli MAC Adreslerini Doğrulama

Tüm anahtar arayüzlerinde manuel olarak yapılandırılan veya dinamik olarak öğrenilen tüm güvenli MAC adreslerini görüntülemek için, örnekte gösterildiği gibi **show port-security address** komutunu kullanın.

```
S1# show port-security address
               Secure Mac Address Table
----------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                   (mins)
----    -----------       ----                          -----   -------------
   1    a41f.7272.676a    SecureSticky                  Fa0/1        -
   1    aaaa.bbbb.1234    SecureConfigured              Fa0/1        -
----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 8192
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 27.2.VLAN Saldırılarını Azaltma

### 27.2.1.VLAN Saldırıları

Bir VLAN atlama saldırısı üç yoldan biriyle başlatılabilir:

- Anahtarın trunking moduna girmesine neden olmak için saldıran ana bilgisayardan DTP mesajlarının sahteciliği. Saldırgan buradan hedef VLAN ile etiketlenmiş trafiği gönderebilir ve ardından anahtar paketleri hedefe teslim eder.
- Bir sahte anahtarın tanıtılması ve trunk etkinleştirilmesi. Saldırgan daha sonra kurban anahtarındaki tüm VLAN'lara sahte anahtardan erişebilir.
- Başka bir VLAN atlamalı saldırı türü, çift etiketleme (veya çift kapsüllenmiş) saldırıdır. Bu saldırı, çoğu anahtardaki donanımın çalışma şeklinden yararlanır.

### 27.2.2.VLAN Atlama Saldırılarını Azaltmak için Yapılması Gerekenler
### VLAN atlama saldırılarını azaltmak için aşağıdaki adımları kullanın:

Adım 1 : Anahtar bağlantı noktası modu **switchport mode access** arabirimi yapılandırma komutunu kullanarak bağlantı noktalarında DTP (otomatik bağlantı) görüşmelerini devre dışı bırakın .

Adım 2 : Kullanılmayan bağlantı noktalarını devre dışı bırakın ve kullanılmayan bir VLAN'a yerleştirin.

Adım 3 : **Switchport mode trunk** komutunu kullanarak bir trunking portundaki trunk bağlantısını manuel olarak etkinleştirin .

Adım 4 : **Switchport nonegotiate** komutunu kullanarak trunk hat bağlantı noktalarında DTP (otomatik bağlantı) görüşmelerini devre dışı bırakın .

Adım 5 : **Switchport trunk native vlan** *vlan _ number* komutunu kullanarak DoğalVLAN'ı VLAN 1 dışında bir VLAN'a ayarlayın .

Örneğin, şunları varsayalım:

- 0/1 ile fa0 / 16 arasındaki FastEthernet bağlantı noktaları, etkin erişim bağlantı noktalarıdır
- 0/17 ile 0/20 arasındaki FastEthernet bağlantı noktaları şu anda kullanımda değil
- 0/21 ile 0/24 arasındaki FastEthernet bağlantı noktaları, trunk hat bağlantı noktalarıdır.

VLAN atlaması, aşağıdaki yapılandırma uygulanarak azaltılabilir.

```
S1(config)# interface range fa0/1 - 16
S1(config-if-range)# switchport mode access
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/17 - 20
S1(config-if-range)# switchport mode access
S1(config-if-range)# switchport access vlan 1000
S1(config-if-range)# shutdown
S1(config-if-range)# exit
S1(config)#
S1(config)# interface range fa0/21 - 24
S1(config-if-range)# switchport mode trunk
S1(config-if-range)# switchport nonegotiate
S1(config-if-range)# switchport trunk native vlan 999
S1(config-if-range)# end
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

- FastEthernet bağlantı noktaları 0/1 - 0/16, erişim bağlantı noktalarıdır ve bu nedenle, bunları açık bir şekilde bağlantı noktalarına erişim sağlayarak devre dışı bırakılır.
- 0/17 - 0/20 FastEthernet bağlantı noktaları kullanılmayan bağlantı noktalarıdır ve devre dışı bırakılır ve kullanılmayan bir VLAN'a atanır.
- 0/21 - 0/24 FastEthernet bağlantı noktaları trunk hat bağlantılarıdır ve DTP devre dışı bırakılmış ana hatlar manuel olarak etkinleştirilir. Doğal VLAN ayrıca varsayılan VLAN 1'den kullanılmayan bir VLAN 999'a değiştirilir.

## 27.3.DHCP Saldırılarını Azaltma

### 27.3.1.DHCP Saldırısının İncelemesi

DHCP açlık-starvation saldırısının amacı, istemcileri bağlamak için bir Hizmet Reddi (DoS) oluşturmaktır. DHCP açlık saldırıları, Gobbler veya Yersinia gibi bir saldırı aracı gerektirir. Gobbler gönderilen her DHCP isteği için benzersiz bir kaynak MAC adresi kullandığından, DHCP açlık saldırılarının bağlantı noktası güvenliği kullanılarak etkili bir şekilde azaltılabileceğini hatırlayın.

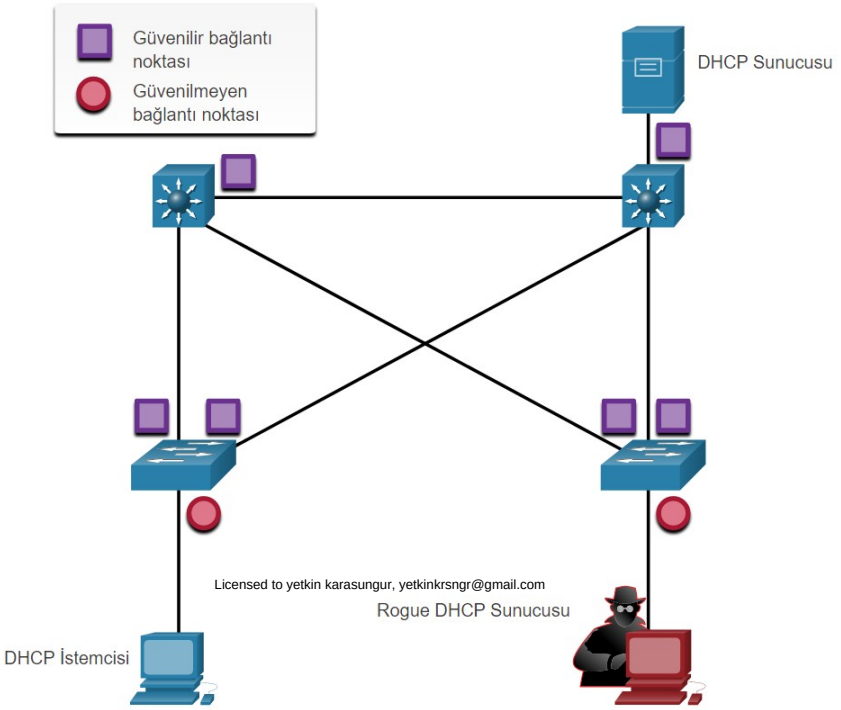
Ancak, DHCP sahtekarlığı saldırılarının azaltılması daha fazla koruma gerektirir. Gobbler, gerçek arayüz MAC adresini kaynak Ethernet adresi olarak kullanmak üzere yapılandırılabilir, ancak DHCP yükünde farklı bir Ethernet adresi belirtebilir. Bu, bağlantı noktası güvenliğini etkisiz hale getirecektir çünkü kaynak MAC adresi meşru olacaktır.

DHCP sahtekarlığı saldırıları, güvenilir bağlantı noktalarında DHCP gözetleme-snooping kullanılarak hafifletilebilir.

### 27.3.2.DHCP Gözetleme-Snooping

DHCP gözetleme, kaynak MAC adreslerine dayanmaz. Bunun yerine, DHCP gözetleme, DHCP mesajlarının yönetimsel olarak yapılandırılmış güvenilen veya güvenilmeyen bir kaynaktan gelip gelmediğini belirler. Daha sonra DHCP iletilerini filtreler ve güvenilmeyen kaynaklardan gelen DHCP trafiğinin hızını sınırlandırır.

Yönetim kontrolünüz altındaki anahtarlar, yönlendiriciler ve sunucular gibi cihazlar güvenilir kaynaklardır. Güvenlik duvarının dışındaki veya ağınızın dışındaki herhangi bir cihaz güvenilmeyen bir kaynaktır. Ek olarak, tüm erişim bağlantı noktaları genellikle güvenilmeyen kaynaklar olarak kabul edilir. Şekilde, güvenilir ve güvenilmeyen bağlantı noktalarının bir örneği gösterilmektedir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

DHCP gözetlemeyi etkinleştirdikten sonra sahte DHCP sunucusunun güvenilmeyen bir bağlantı noktasında olacağına dikkat edin. Varsayılan olarak tüm arabirimler güvenilmez olarak kabul edilir. Güvenilir arabirimler, tipik olarak meşru bir DHCP sunucusuna doğrudan bağlı ana hat bağlantıları ve bağlantı noktalarıdır. Bu arabirimler açıkça güvenilir olarak yapılandırılmalıdır.

Güvenilmeyen bir bağlantı noktasındaki bir aygıtın kaynak MAC adresini ve DHCP sunucusu tarafından o aygıta atanan IP adresini içeren bir DHCP tablosu oluşturulur. MAC adresi ve IP adresi birbirine bağlıdır. Bu nedenle, bu tabloya DHCP gözetleme bağlama tablosu (DHCP snooping binding table) denir.

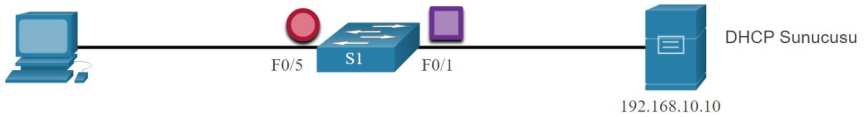
## 27.3.3.DHCP Gözetlemeyi Uygulama Adımları

DHCP gözetlemeyi etkinleştirmek için aşağıdaki adımları kullanın:

- 1. Adım . **ip dhcp snooping** genel yapılandırma komutunu kullanarak DHCP gözetlemeyi etkinleştirin .
- 2. Adım . Güvenilen bağlantı noktalarında **ip dhcp snooping trust** arabirimi yapılandırma komutunu kullanın.
- 3. Adım . **ip dhcp snooping limit rate** arabirim yapılandırma komutunu kullanarak güvenilmeyen bağlantı noktalarında saniyede alınabilecek DHCP keşif mesajlarının sayısını sınırlayın .
- 4. adım . **ip dhcp snooping** *vlan* genel yapılandırma komutunu kullanarak, VLAN veya bir dizi VLAN ile DHCP gözetlemeyi etkinleştirin .

## 27.3.4.DHCP Snooping Yapılandırma Örneği

Bu DHCP gözetleme örneğinin referans topolojisi şekilde gösterilmektedir. F0 / 5'in bir PC'ye bağlandığı için güvenilmeyen bir bağlantı noktası olduğuna dikkat edin. F0 / 1, DHCP sunucusuna bağlandığı için güvenilir bir bağlantı noktasıdır.



Aşağıda, S1'de DHCP gözetlemesinin nasıl yapılandırılacağına dair bir örnek verilmiştir. DHCP gözetlemenin ilk olarak nasıl etkinleştirildiğine dikkat edin. Daha sonra, DHCP sunucusuna giden yukarı akış arabirimine açıkça güvenilir. Daha sonra, F0 / 5 ile F0 / 24 arasındaki FastEthernet bağlantı noktaları aralığı varsayılan olarak güvenilmezdir, bu nedenle hız sınırı saniyede altı paket olarak ayarlanır. Son olarak, DHCP gözetleme, VLANS 5, 10, 50, 51 ve 52'de etkinleştirilir.

```
S1(config)# ip dhcp snooping
S1(config)# interface f0/1
S1(config-if)# ip dhcp snooping trust
S1(config-if)# exit
S1(config)# interface range f0/5 - 24
S1(config-if-range)# ip dhcp snooping limit rate 6
S1(config-if-range)# exit
S1(config)# ip dhcp snooping vlan 5,10,50-52
S1(config)# end
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

DHCP gözetlemesini doğrulamak için **show ip dhcp snooping** ayrıcalıklı EXEC komutunu kullanın ve örnekte gösterildiği gibi DHCP bilgisi alan istemcileri görüntülemek için **show ip dhcp snooping binding** komutunu kullanın.

Not : DHCP gözetleme, bir sonraki konu olan Dinamik ARP Denetimi (DAI) için de gereklidir.

```
S1# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
5,10,50-52
DHCP snooping is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:
Insertion of option 82 is enabled
   circuit-id default format: vlan-mod-port
   remote-id: 0cd9.96d2.3f80 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:
Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
FastEthernet0/1            yes        yes             unlimited
  Custom circuit-ids:
FastEthernet0/5            no         no              6
  Custom circuit-ids:
FastEthernet0/6            no         no              6
  Custom circuit-ids:
S1# show ip dhcp snooping binding
MacAddress         IpAddress       Lease(sec) Type          VLAN Interface
------------------ --------------- ---------- ------------- ---- --------------------
00:03:47:B5:9F:AD  192.168.10.11   193185     dhcp-snooping 5    FastEthernet0/5
```

## 27.4.ARP Saldırılarını Azaltmak

### 27.4.1.Dinamik ARP Denetimi (Dynamic ARP Inspection)

Tipik bir ARP saldırısında, bir tehdit aktörü, tehdit aktörünün MAC Adresi ve varsayılan ağ geçidinin IP adresi ile alt ağdaki diğer ana bilgisayarlara istenmeyen ARP istekleri gönderebilir. ARP sahtekarlığını ve bunun sonucunda ortaya çıkan ARP zehirlenmesini önlemek için, bir anahtarın yalnızca geçerli ARP İstekleri ve Yanıtlarının iletildiğinden emin olması gerekir.

Dinamik ARP incelemesi (DAI), DHCP gözetleme gerektirir ve aşağıdakileri yaparak ARP saldırılarını önlemeye yardımcı olur:

- Geçersiz veya gereksiz ARP İsteklerini aynı VLAN'daki diğer bağlantı noktalarına iletmemek.
- Güvenilmeyen bağlantı noktalarında tüm ARP İsteklerini ve Yanıtlarını yakalamak.
- Yakalanan her paketin geçerli bir IP-MAC bağlantısı için doğrulanması.
- ARP zehirlenmesini önlemek için geçersiz kaynaklardan gelen ARP İsteklerini düşürme ve günlüğe kaydetme.
- Yapılandırılan ARP paketlerinin DAI sayısı aşılırsa arabirimin hata-devre dışı bırakılması.

### 27.4.2.DAI Uygulama Yönergeleri

ARP sahtekarlığı ve ARP zehirlenmesi olasılığını azaltmak için aşağıdaki DAI uygulama yönergelerini izleyin:

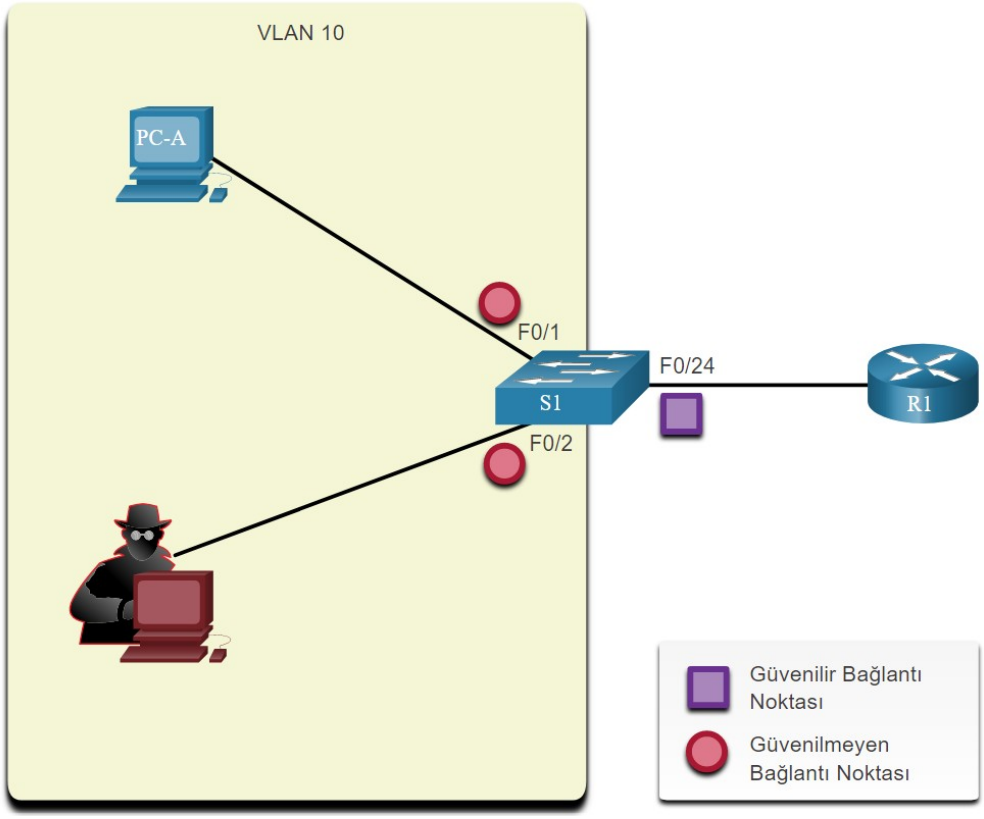
Lisansınız yetkili kullanıcıyı, yetkili kullanıcıyı tanımlamaktadır.

- DHCP gözetlemeyi global olarak etkinleştirin.
- Seçili VLAN'larda DHCP gözetlemeyi etkinleştirin.

- Seçili VLAN'larda DAI'yi etkinleştirin.
- DHCP gözetleme ve ARP incelemesi için güvenilir arabirimleri yapılandırın.

Genel olarak, tüm erişim anahtarı bağlantı noktalarını güvenilmeyen olarak yapılandırmanız ve diğer anahtarlara bağlı tüm yukarı bağlantı bağlantı noktalarını güvenilir olarak yapılandırmanız önerilir.

Şekildeki örnek topoloji, güvenilir ve güvenilmeyen bağlantı noktalarını tanımlar.




## 27.4.3.DAI Yapılandırma Örneği

Önceki topolojide, S1, VLAN 10'da iki kullanıcıyı birbirine bağlamaktadır. DAI, ARP sahtekarlığı ve ARP zehirlenmesi saldırılarını azaltacak şekilde yapılandırılacaktır.

Örnekte gösterildiği gibi, DHCP gözetleme etkinleştirilir çünkü DAI, DHCP gözetleme bağlama tablosunun çalışmasını gerektirir. Ardından, VLAN10'daki PC'ler için DHCP gözetleme ve ARP incelemesi etkinleştirilir. Yönlendiriciye giden yukarı bağlantı bağlantı noktası güvenilirdir ve bu nedenle DHCP gözetleme ve ARP incelemesi için güvenilir olarak yapılandırılır.

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10
S1(config)# ip arp inspection vlan 10
S1(config)# interface fa0/24
S1(config-if)# ip dhcp snooping trust
S1(config-if)# ip arp inspection trust
```

DAI ayrıca hem hedef hem de kaynak MAC ve IP adreslerini kontrol edecek şekilde yapılandırılabilir:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Hedef MAC - Ethernet başlığındaki hedef MAC adresini ARP gövdesindeki hedef MAC adresine göre kontrol eder.
Kaynak MAC - Ethernet başlığındaki kaynak MAC adresini ARP gövdesindeki gönderen MAC adresi ile karşılaştırır.

IP adresi - 0.0.0.0, 255.255.255.255 adresleri ve tüm IP çok noktaya yayın adresleri dahil olmak üzere, ARP gövdesini geçersiz ve beklenmeyen IP adresleri için kontrol eder.

**ip arp inspection validate {[src-mac] [dst-mac] [ip]}** global konfigürasyon komutu ARP paketlerini düşürmek için yapılandırmak DAI için kullanılır. ARP paketlerinin gövdesindeki MAC adresleri Ethernet başlığında belirtilen adreslerle eşleşmediğinde kullanılabilir. Aşağıdaki örnekte yalnızca bir komutun nasıl yapılandırılabileceğine dikkat edin. Bu nedenle, birden çok **ip arp inspection validate** komutlarının girilmesi , önceki komutun üzerine yazılır. Birden fazla doğrulama yöntemi eklemek için, aşağıdaki çıktıda gösterildiği ve doğrulandığı gibi aynı komut satırına girin.

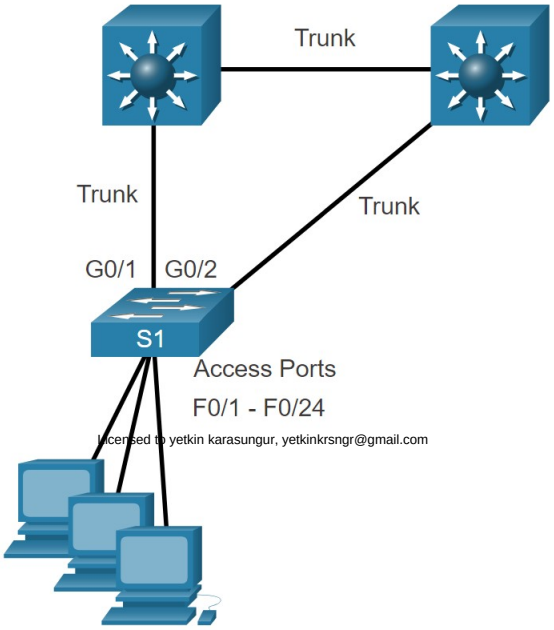
```
S1(config)# ip arp inspection validate ?
dst-mac  Validate destination MAC address
  ip       Validate IP addresses
  src-mac  Validate source MAC address
S1(config)# ip arp inspection validate src-mac
S1(config)# ip arp inspection validate dst-mac
S1(config)# ip arp inspection validate ip
S1(config)# do show run | include validate
ip arp inspection validate ip
S1(config)# ip arp inspection validate src-mac dst-mac ip
S1(config)# do show run | include validate
ip arp inspection validate src-mac dst-mac ip
S1(config)#
```

## 27.5.STP Saldırılarını Azaltmak

### 27.5.1.PortFast ve BPDU Guard

Ağ saldırganlarının, kök köprüyü taklit ederek ve bir ağın topolojisini değiştirerek bir saldırı gerçekleştirmek için Yayılan Ağaç Protokolünü (STP) manipüle edebileceğini hatırlayın. Yayılan Ağaç Protokolü (STP) manipülasyon saldırılarını azaltmak için PortFast ve Köprü Protokolü Veri Birimi-Bridge Protocol Data Unit (BPDU) Korumasını kullanın:

- **PortFast** - PortFast, dinleme ve öğrenme durumlarını atlayarak, erişim portu olarak yapılandırılmış bir arabirimi hemen bir engelleme durumundan yönlendirme durumuna getirir. Tüm son kullanıcı bağlantı noktalarına uygulayın. PortFast yalnızca uç cihazlara bağlı bağlantı noktalarında yapılandırılmalıdır.
- **BPDU Koruması** - BPDU koruması hemen hatası, BPDU alan bir bağlantı noktasını devre dışı bırakır. PortFast gibi, BPDU koruması da yalnızca uç cihazlara bağlı arabirimlerde yapılandırılmalıdır.
- Şekilde, S1 için erişim portları PortFast ve BPDU Guard ile yapılandırılmalıdır.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 27.5.2.PortFast'ı Yapılandırma

PortFast, erişim bağlantı noktalarının STP'nin birleşmesini beklemesi gereken süreyi en aza indirmek için STP dinleme ve öğrenme durumlarını atlar. Başka bir anahtara bağlanan bir bağlantı noktasında PortFast etkinleştirilirse, bir kapsayan ağaç döngüsü oluşturma riski vardır.

PortFast, **spanning-tree portfast** yapılandırma komutu kullanılarak bir arabirimde etkinleştirilebilir . Alternatif olarak, Portfast, **spanning-tree portfast default** global konfigürasyon komutu kullanılarak tüm erişim portlarında global olarak konfigüre edilebilir.

PortFast'in global olarak etkinleştirilip etkinleştirilmediğini doğrulamak için **show running-config | begin span** komutunu veya **show spanning-tree summary** komutunu başlatın. PortFast'in bir arabirimde etkinleştirilip etkinleştirilmediğini doğrulamak için , aşağıdaki örnekte gösterildiği gibi **show running-config interface** arabirim türü / numarası komutunu kullanın. show spanning-tree interface type/number detail komutu da doğrulama için kullanılabilir.

PortFast etkinleştirildiğinde uyarı mesajlarının görüntülendiğine dikkat edin.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a single
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
%Portfast has been configured on FastEthernet0/1 but will only
 have effect when the interface is in a non-trunking mode.
S1(config-if)# exit
S1(config)# spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
 should now disable portfast explicitly on switched ports leading to hubs,
 switches and bridges as they may create temporary bridging loops.
S1(config)# exit
S1# show running-config | begin span
spanning-tree mode pvst
spanning-tree portfast default
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
(output omitted)
```

## 27.5.3.BPDU Guard'ı Yapılandırma

PortFast etkinleştirilse bile, arabirim BPDU'ları dinlemeye devam edecektir. Beklenmeyen BPDU'lar yanlışlıkla veya ağa bir anahtar eklemek için yetkisiz bir girişimin parçası olabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

BPDU Korumasının etkin olduğu bir bağlantı noktasında herhangi bir BPDU alınırsa, bu bağlantı noktası hata devre dışı (error disable)bırakılır. Bu, bağlantı noktasının kapatıldığı ve manuel olarak yeniden etkinleştirilmesi

veya **errdisable recovery cause bpduguard** global yapılandırma komutu aracılığıyla otomatik olarak kurtarılması gerektiği anlamına gelir .

BPDU Guard, **spanning-tree bpduguard enable** arabirimi yapılandırma komutu kullanılarak bir bağlantı noktasında etkinleştirilebilir . Alternatif olarak, tüm PortFast özellikli bağlantı noktalarında BPDU korumasını global olarak etkinleştirmek için **spanning-tree portfast bpduguard default** genel yapılandırma komutunu kullanın.

Kapsayan ağacın durumu hakkındaki bilgileri görüntülemek için, **show spanning-tree summary** komutunu kullanın. Örnekte, PortFast varsayılan ve BPDU Koruması, erişim modu olarak yapılandırılan bağlantı noktaları için varsayılan durum olarak etkinleştirilmiştir.

Not : Tüm PortFast özellikli bağlantı noktalarında BPDU Korumasını her zaman etkinleştirin.

```
S1(config)# interface fa0/1
S1(config-if)# spanning-tree bpduguard enable
S1(config-if)# exit
S1(config)# spanning-tree portfast bpduguard default
S1(config)# end
S1# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
Extended system ID           is enabled
Portfast Default             is enabled
PortFast BPDU Guard Default  is enabled
Portfast BPDU Filter Default is disabled
Loopguard Default            is disabled
EtherChannel misconfig guard is enabled
UplinkFast                   is disabled
BackboneFast                 is disabled
Configured Pathcost method used is short
(output omitted)
S1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 28. Bölüm: Kablosuz Ağ Teknolojileri

## 28.1.Kablosuz Ağlara Giriş

### 28.1.1.Kablosuz Ağların Faydaları

Kablosuz LAN (Wireless LAN-WLAN), genellikle evlerde, ofislerde ve kampüs ortamlarında kullanılan bir tür kablosuz ağdır. Ağlar hareket halindeki insanları desteklemelidir. İnsanlar bilgisayarlar, dizüstü bilgisayarlar, tabletler ve akıllı telefonlar kullanarak ağa bağlanır. Kablolu LAN'lar, servis sağlayıcı ağları ve cep telefonu ağları gibi ağ erişimi sağlayan birçok farklı ağ altyapısı vardır. Ancak ev ve iş ortamlarında mobiliteyi mümkün kılan şey WLAN'dır.

Kablosuz altyapısı olan işletmelerde, ekipman her değiştiğinde veya bir çalışanı bir bina içerisine yerleştirirken, ekipmanı veya laboratuvarı yeniden düzenlerken veya geçici yerlere veya proje sahalarına taşınırken maliyet tasarrufu sağlanabilir. Kablosuz bir altyapı, hızla değişen ihtiyaçlara ve teknolojilere uyum sağlayabilir.

### 28.1.2.Kablosuz Ağ Türleri

Kablosuz ağlar, Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) standartlarına dayanır ve genel olarak dört ana türe ayrılabilir: WPAN, WLAN, WMAN ve WWAN.

**Kablosuz Kişisel Alan Ağları** (Wireless Personal-Area Networks-WPAN) - Kısa menzilli bir ağ için düşük güçlü vericiler kullanır, genellikle 20 ila 30 ft. (6 ila 9 metre). Bluetooth ve ZigBee tabanlı cihazlar WPAN'larda yaygın olarak kullanılmaktadır. WPAN'lar, 802.15 standardına ve 2,4 GHz radyo frekansına dayanır.

**Kablosuz LAN'lar** (WLAN) - Genellikle 300 fit'e kadar olan orta büyüklükteki bir ağı kapsamak için vericileri kullanır. WLAN'lar bir evde, ofiste ve hatta bir kampüs ortamında kullanıma uygundur. WLAN'lar 802.11 standardına ve 2,4 GHz veya 5 GHz radyo frekansına dayanır.

**Wireless MANs** (WMAN) - Daha geniş bir coğrafi alan üzerinde kablosuz hizmet sağlamak için vericileri kullanır. WMAN'ler, bir metropol şehre veya belirli bir bölgeye kablosuz erişim sağlamak için uygundur. WMAN'ler belirli lisanslı frekansları kullanır.

**Kablosuz Geniş Alan Ağları** (Wireless Wide-Area Networks -WWAN'lar) - Geniş bir coğrafi alanda kapsama alanı sağlamak için vericileri kullanır. WWAN'lar ulusal ve küresel iletişim için uygundur. WWAN'lar ayrıca belirli lisanslı frekansları kullanır.

### 28.1.3.Kablosuz Teknolojiler

Kablosuz teknoloji, veri göndermek ve almak için lisanssız radyo spektrumunu kullanır. Lisanssız spektruma, kullandıkları cihazda bir kablosuz yönlendirici ve kablosuz teknolojisi olan herkes erişebilir.

**Bluetooth** - 300 ft. (100m) mesafeye kadar iletişim kurmak için bir cihaz eşleştirme işlemi kullanan bir IEEE 802.15 WPAN standardı. Akıllı ev cihazlarında, ses bağlantılarında, otomobillerde ve kısa mesafeli bağlantı gerektiren diğer cihazlarda bulunabilir. İki tür Bluetooth radyosu vardır:

- Bluetooth Düşük Enerji (Bluetooth Low Energy-BLE) - Bu, ağ topolojisi dahil olmak üzere büyük ölçekli ağ cihazlarına kadar birçok ağ teknolojisini destekler.
- Bluetooth Temel Hız / Gelişmiş Hız (Bluetooth Basic Rate/Enhanced Rate-BR / EDR) - Bu, noktadan noktaya topolojileri destekler ve ses akışı için optimize edilmiştir.

**WiMAX** (Worldwide Interoperability for Microwave Access) WiMAX, DSL ve kablo ile rekabet eden geniş bant kablolu internet bağlantılarına bir alternatiftir. Ancak, genellikle henüz bir DSL veya kablo sağlayıcısına bağlı olmayan alanlarda kullanılır. 50 km'ye (30 mil) kadar yüksek hızlı kablosuz geniş bant erişimi sağlayan bir IEEE 802.16 WWAN standardıdır. WiMAX, Wi-Fi'ye benzer şekilde çalışır, ancak daha yüksek hızlarda, daha büyük

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com.

mesafelerde ve daha fazla sayıda kullanıcı için. Cep telefonu kulelerine benzer bir WiMAX kulesi ağı kullanır. WiMAX vericileri ve hücresel vericiler, şekilde gösterildiği gibi aynı kule üzerinde alanı paylaşabilir.

**Hücresel Geniş Bant** - Hücresel 4G / 5G, öncelikle cep telefonları tarafından kullanılan kablosuz mobil ağlardır, ancak otomobillerde, tabletlerde ve dizüstü bilgisayarlarda da kullanılabilir. Hücresel ağlar, hem veri hem de sesli iletişim taşıyan çok erişimli ağlardır. Bir hücre sitesi, belirli bir alanda sinyalleri ileten hücresel bir kule tarafından oluşturulur. Birbirine bağlanan hücre siteleri hücresel ağı oluşturur. İki tür hücresel ağ, Global Mobil Sistem (GSM) ve Kod Bölmeli Çoklu Erişim'dir (Code Division Multiple Access-CDMA). GSM uluslararası olarak tanınırken, CDMA esas olarak ABD'de kullanılmaktadır.

4. Nesil mobil ağ (4G), mevcut mobil ağdır. 4G, önceki 3G ağlarının 10 katı hızlar sunar. Yeni 5G, 4G'den 100 kat daha yüksek hızlar sunma ve ağa her zamankinden daha fazla cihaz bağlama vaadini taşıyor.

**Uydu Geniş Bant** - Belirli bir coğrafi konumsal Dünya yörünge uydusu ile hizalanmış yönlü bir uydu çanağı kullanılarak uzak sitelere ağ erişimi sağlar. Genellikle daha pahalıdır ve net bir görüş alanı gerektirir. Tipik olarak, kırsal ev sahipleri ve kablo ve DSL'nin bulunmadığı işletmeler tarafından kullanılır.

## 28.1.4.802.11 Standartları

Kablosuz iletişim dünyası çok geniştir. Bununla birlikte, belirli işle ilgili beceriler için Wi Fi'nin belirli yönlerine odaklanmak istiyoruz. Başlamak için en iyi yer, IEEE 802.11 WLAN standartlarıdır. Bu standartlar, kablosuz bağlantılar için radyo frekanslarının nasıl kullanıldığını tanımlar. Standartların çoğu, kablosuz aygıtların belirtilen radyo frekansında (2,4 GHz veya 5 GHz) kablosuz sinyalleri iletmek ve almak için bir antene sahip olduğunu belirtir. Daha yüksek hızlarda gönderip alan yeni standartlardan bazıları, erişim noktalarının (AP'ler) ve kablosuz istemcilerin çoklu giriş ve çoklu çıkış (MIMO) teknolojisini kullanan birden çok antene sahip olmasını gerektirir. MIMO, iletişim performansını iyileştirmek için hem verici hem de alıcı olarak birden fazla anten kullanır. Verimi artırmak için sekiz adede kadar gönderme ve alma anteni kullanılabilir.

Yıllar içinde IEEE 802.11 standardının çeşitli uygulamaları geliştirilmiştir. Tablo bu standartları vurgulamaktadır.

| IEEE WLAN Standardı | Radyo frekansı | Açıklama |
|---|---|---|
| 802.11 | 2,4 GHz | • 2 Mbps'ye kadar hızlar |
| 802.11a | 5 GHz | • 54 Mbps'ye kadar hızlar<br>• küçük kapsama alanı<br>• bina yapılarına nüfuz etmede daha az etkilidir<br>• 802.11b ve 802.11g ile birlikte çalışmaz |
| 802.11b | 2,4 GHz | • 11 Mbps'ye kadar hızlar<br>• 802.11a'dan daha uzun menzil<br>• bina yapılarına daha iyi nüfuz edebilme |
| 802.11g | 2,4 GHz | • 54 Mbps'ye kadar hızlar<br>• azaltılmış bant genişliği kapasitesi ile 802.11b ile geriye dönük uyumlu |
| 802.11n | 2,4 GHz 5 GHz | • veri hızları, 70 m'ye (230 fit) kadar mesafe aralığı ile 150 Mbps ile 600 Mbps arasındadır<br>• AP'ler ve kablosuz istemciler, MIMO teknolojisini kullanan birden çok |

izinsiz çoğaltılamaz ve dağıtılamaz

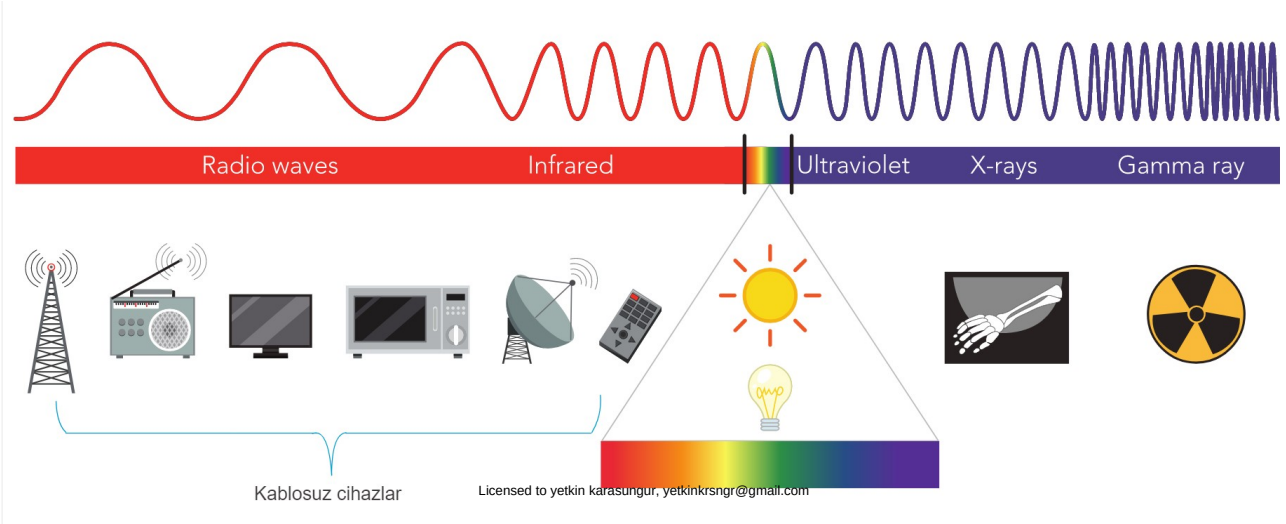
| IEEE WLAN Standardı | Radyo frekansı | Açıklama |
|---|---|---|
| | | anten gerektirir<br>• sınırlayıcı veri hızlarına sahip 802.11a / b / g cihazlarla geriye dönük uyumlu |
| 802.11ac | 5 GHz | • MIMO teknolojisini kullanarak 450 Mbps ile 1.3 Gbps (1300 Mbps) arasında değişen veri hızları sağlar<br>• Sekiz adede kadar anten desteklenebilir<br>• sınırlayıcı veri hızlarına sahip 802.11a / n cihazlarla geriye dönük uyumlu |
| 802.11ax | 2,4 GHz 5 GHz | • 2019'da yayınlanan en son standart<br>• Wi-Fi 6 veya Yüksek Verimli Kablosuz (HEW) olarak da bilinir<br>• gelişmiş güç verimliliği, daha yüksek veri oranları, artırılmış kapasite sağlar ve birçok bağlı cihazı yönetir<br>• şu anda 2,4 GHz ve 5 GHz kullanarak çalışır, ancak bu frekanslar kullanılabilir olduğunda 1 GHz ve 7 GHz kullanır<br>• Daha fazla bilgi için internette Wi-Fi Generation 6'yı arayın |

## Radyo Frekansları

Tüm kablosuz cihazlar, elektromanyetik spektrumun radyo dalgaları aralığında çalışır. WLAN ağları 2,4 GHz frekans bandında ve 5 GHz bandında çalışır. Kablosuz LAN aygıtlarında, şekilde gösterildiği gibi radyo dalgaları aralığının belirli frekanslarına ayarlanmış vericiler ve alıcılar bulunur. Özellikle aşağıdaki frekans bantları 802.11 kablosuz LAN'lara tahsis edilmiştir:

2,4 GHz (UHF) - 802.11b / g / n / ax
5 GHz (SHF) - 802.11a / n / ac / ax

## Elektromanyetik Spektrum



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Kablosuz Standart Kuruluşları

Standartlar, farklı üreticiler tarafından üretilen cihazlar arasında birlikte çalışabilirliği sağlar. Uluslararası olarak, WLAN standartlarını etkileyen üç kuruluş ITU-R, IEEE ve Wi-Fi Alliance'dır.

ITU: Uluslararası Telekomünikasyon Birliği (ITU), radyo frekansı spektrumunun ve uydu yörüngelerinin ITU-R aracılığıyla tahsisini düzenler. ITU-R, ITU Radyo Haberleşme Sektörü anlamına gelir.

IEEE:IEEE, bir radyo frekansının bilgi taşımak için nasıl modüle edildiğini belirtir. IEEE 802 LAN / MAN standart ailesi ile yerel ve metropolitan alan ağları (MAN) standartlarını korur. IEEE 802 ailesindeki baskın standartlar 802.3 Ethernet ve 802.11 WLAN'dır.

Wi-Fi Alliance :Wi-Fi Alliance, kendini WLAN'ların büyümesini ve kabulünü teşvik etmeye adamış küresel, kar amacı gütmeyen bir endüstri ticaret birliğidir. Amacı, satıcıları endüstri normlarına ve standartlara uygunluk konusunda onaylayarak 802.11 standardına dayalı ürünlerin birlikte çalışabilirliğini iyileştirmek olan bir satıcılar birliğidir.

## 28.2.WLAN Bileşenleri

### 28.2.1.Kablosuz NIC'ler

Kablosuz dağıtımlar, bir radyo vericisi ve aynı radyo frekanslarına ayarlanmış bir radyo alıcısı olan en az iki cihaz gerektirir:

- Kablosuz NIC'lere sahip son cihazlar
- Kablosuz yönlendirici veya kablosuz AP gibi bir ağ cihazı

Kablosuz iletişim kurmak için dizüstü bilgisayarlar, tabletler, akıllı telefonlar ve hatta en yeni otomobiller, bir radyo vericisi / alıcısı içeren entegre kablosuz NIC'ler içerir. Bununla birlikte, bir cihazda entegre bir kablosuz NIC yoksa, şekilde gösterildiği gibi bir USB kablosuz adaptör kullanılabilir.

### 28.2.2.Kablosuz Ev Yönlendiricisi

Bir son cihazın ilişkilendirdiği ve kimlik doğrulaması yaptığı altyapı cihazının türü, WLAN'ın boyutuna ve gereksinimine göre değişir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Örneğin, bir ev kullanıcısı tipik olarak kablosuz cihazları, şekilde gösterildiği gibi küçük, kablosuz bir yönlendirici kullanarak birbirine bağlar. Kablosuz yönlendirici şu işlevi görür:

- Erişim noktası - Bu, 802.11a / b / g / n / ac kablosuz erişim sağlar.
- Anahtar - Bu, kablolu cihazları birbirine bağlamak için dört bağlantı noktalı, tam çift yönlü, 10/100/1000 Ethernet anahtarı sağlar.
- Yönlendirici - Bu, internet gibi diğer ağ altyapılarına bağlanmak için varsayılan bir ağ geçidi sağlar.

Kablosuz yönlendirici, genellikle küçük bir işletme veya konut kablosuz erişim cihazı olarak uygulanır. Kablosuz yönlendirici, paylaşılan hizmet seti tanımlayıcısını (SSID) içeren işaretler göndererek kablosuz hizmetlerini tanıtır. Aygıtlar kablosuz olarak SSID'yi keşfeder ve yerel ağa ve internete erişmek için onunla ilişkilendirmeye ve kimlik doğrulamaya çalışır.

Çoğu kablosuz yönlendirici ayrıca, yüksek hızlı erişim, video akışı desteği, IPv6 adresleme, hizmet kalitesi (QoS), yapılandırma yardımcı programları ve yazıcıları veya taşınabilir sürücüleri bağlamak için USB bağlantı noktaları gibi gelişmiş özellikler de sağlar.

Ek olarak, ağ hizmetlerini genişletmek isteyen ev kullanıcıları, Wi-Fi menzil genişleticileri uygulayabilir. Bir cihaz, genişleticiye kablosuz olarak bağlanabilir, bu da iletişimlerinin kablosuz yönlendiriciyle tekrarlanmasını artırır.

## 28.2.3.Kablosuz Erişim Noktaları (Acess Point)

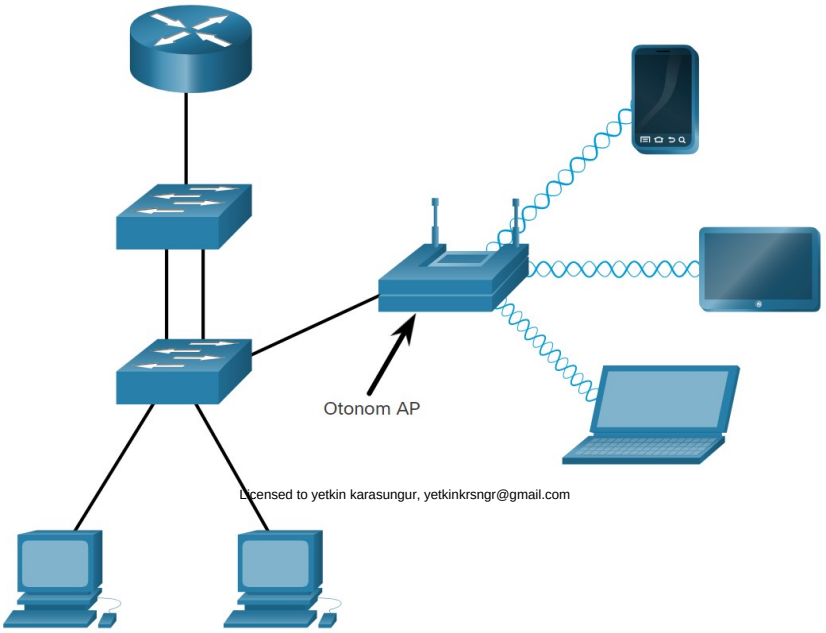
Menzil genişleticilerin kurulumu ve yapılandırması kolay olsa da, en iyi çözüm, kullanıcı cihazlarına özel kablosuz erişim sağlamak için başka bir kablosuz erişim noktası kurmaktır. Kablosuz istemciler, SSID'lerini tanıtan yakındaki AP'leri keşfetmek için kablosuz NIC'lerini kullanır. İstemciler daha sonra bir AP ile ilişkilendirmeye ve kimlik doğrulamaya çalışır. Kimlik doğrulandıktan sonra, kablosuz kullanıcıların ağ kaynaklarına erişimi olur.

## 28.2.4.AP Kategorileri

AP'ler, otonom AP'ler veya denetleyici tabanlı AP'ler olarak kategorize edilebilir.

### Otonom AP'ler

Bunlar, şekilde gösterildiği gibi bir komut satırı arayüzü veya bir GUI kullanılarak yapılandırılan bağımsız cihazlardır. Otonom AP'ler, kuruluşta yalnızca birkaç AP'nin gerekli olduğu durumlarda kullanışlıdır. Ev yönlendiricisi, özerk bir AP'nin bir örneğidir çünkü AP yapılandırmasının tamamı cihazda bulunur. Kablosuz talep artarsa, daha fazla AP gerekli olacaktır. Her AP, diğer AP'lerden bağımsız olarak çalışacak ve her bir AP, manuel yapılandırma ve yönetim gerektirecektir. Çok sayıda AP'ye ihtiyaç duyulsaydı, bu zor bir hal alırdı.

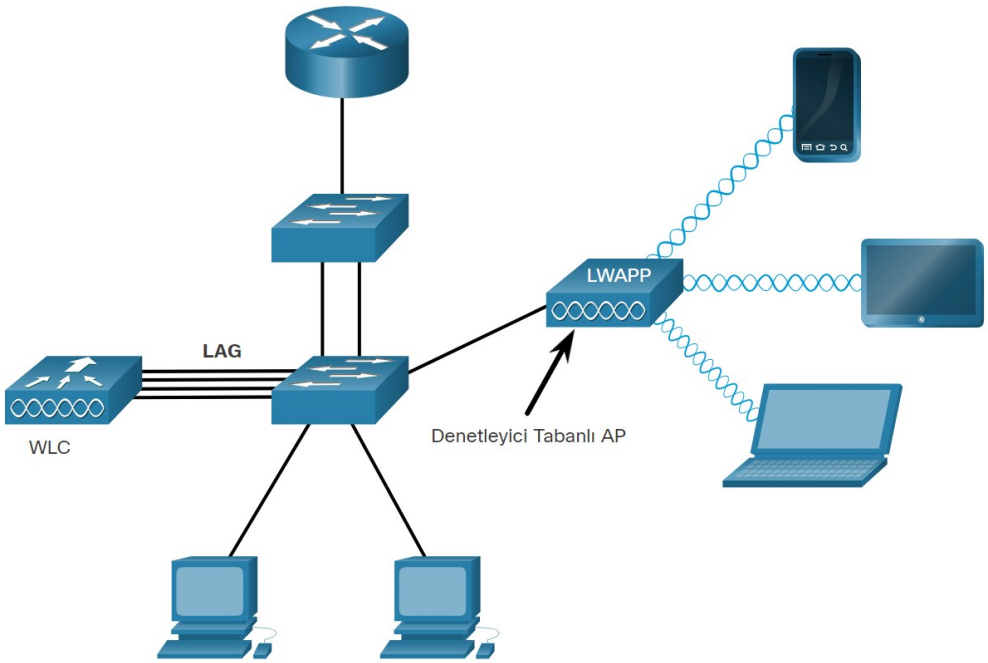



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Denetleyici tabanlı AP'ler**

Bu cihazlar ilk yapılandırma gerektirmez ve genellikle hafif AP'ler (lightweight-LAP'ler) olarak adlandırılır. LAP'ler, sonraki şekilde gösterildiği gibi bir WLAN denetleyicisi (WLAN controller-WLC) ile iletişim kurmak için Hafif Erişim Noktası Protokolünü (Lightweight Access Point Protocol-LWAPP) kullanır. Denetleyici tabanlı AP'ler, ağda birçok AP'nin gerekli olduğu durumlarda kullanışlıdır. Daha fazla AP eklendikçe, her AP otomatik olarak yapılandırılır ve WLC tarafından yönetilir.

Şekilde WLC'nin anahtarlama altyapısına bağlı dört porta sahip olduğuna dikkat edin. Bu dört bağlantı noktası, onları bir araya toplamak için bir bağlantı toplama grubu (link aggregation group-LAG) olarak yapılandırılmıştır. EtherChannel'in çalışmasına çok benzer şekilde, LAG artıklık ve yük dengeleme sağlar. Anahtar üzerindeki WLC'ye bağlı tüm bağlantı noktalarının trunking olması ve EtherChannel açık olarak yapılandırılması gerekir. Ancak, LAG tam olarak EtherChannel gibi çalışmaz. WLC, Bağlantı Noktası Toplama Protokolünü (PaGP) veya Bağlantı Toplama Kontrol Protokolünü (LACP) desteklemez.




## 28.2.5.Kablosuz Antenler

Çoğu işletme sınıfı AP, tam işlevli birimler yapmak için harici antenlere ihtiyaç duyar.

**Çok Yönlü Antenler:** Şekilde gösterilen gibi çok yönlü antenler 360 derecelik kapsama sağlar ve evler, açık ofis alanları, konferans odaları ve dış alanlarda idealdir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Yönlü Antenler:** Yönlü antenler, radyo sinyalini belirli bir yönde odaklar. Bu, antenin işaret ettiği yönde AP'ye giden ve gelen sinyali güçlendirir. Bu, bir yönde daha güçlü bir sinyal gücü ve diğer tüm yönlerde daha düşük sinyal gücü sağlar. Yönlü Wi-Fi antenlerinin örnekleri arasında Yagi ve parabolik çanak antenler bulunur.

**Çoklu Giriş Çoklu Çıkış** (Multiple Input Multiple Output-MIMO), IEEE 802.11n / ac / ax kablosuz ağları için mevcut bant genişliğini artırmak için çoklu antenler kullanır. Verimi artırmak için sekiz adede kadar gönderme ve alma anteni kullanılabilir.

## 28.3.WLAN Nasıl Çalışır

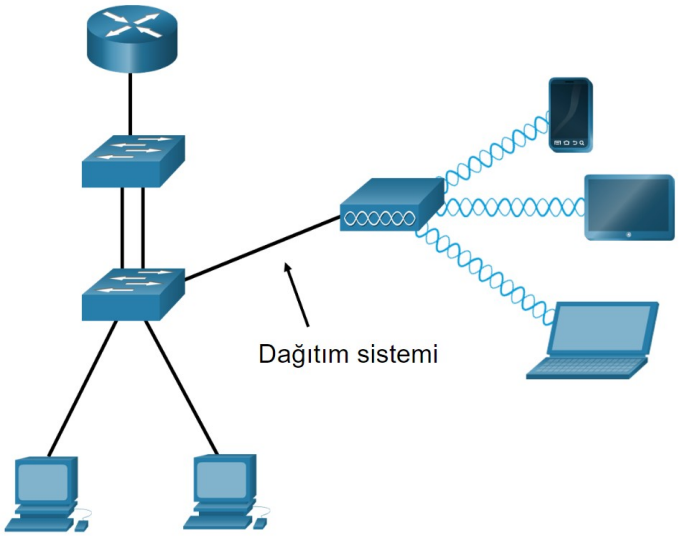
### 28.3.1.802.11 Kablosuz Topoloji Modları

Kablosuz LAN'lar çeşitli ağ topolojilerini barındırabilir. 802.11 standardı iki ana kablosuz topoloji modunu tanımlar: Ad hoc modu ve Altyapı modu. İnternet paylaşımı (Tethering) da bazen hızlı kablosuz erişim sağlamak için kullanılan bir moddur.

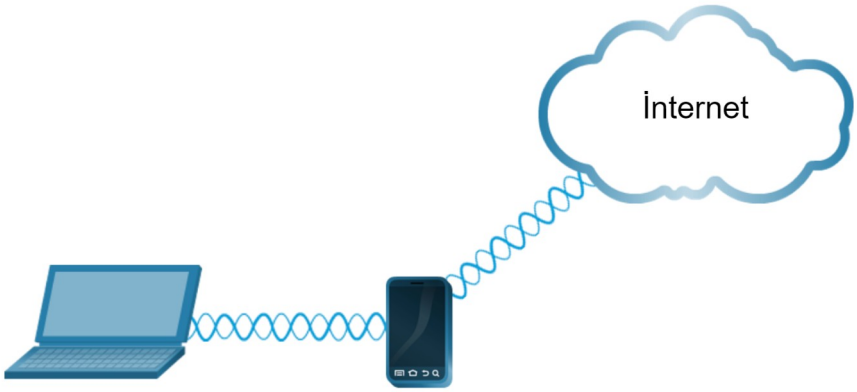
Ad hoc modu - Bu, iki cihazın AP'ler veya kablosuz yönlendiriciler kullanmadan eşler arası (P2P) kablosuz olarak bağlandığı zamandır. Örnekler, Bluetooth veya Wi-Fi Direct kullanarak birbirlerine doğrudan bağlanan kablosuz istemcileri içerir. IEEE 802.11 standardı, bağımsız bir temel hizmet kümesi (IBSS) olarak geçici bir ağı ifade eder.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Altyapı modu - Bu, kablosuz istemcilerin WLAN'lar gibi bir kablosuz yönlendirici veya AP aracılığıyla birbirine bağlandığı zamandır. AP'ler, Ethernet gibi kablolu dağıtım sistemini kullanarak ağ altyapısına bağlanır.




İnternet paylaşımı - Özel topolojinin bir çeşidi, hücresel veri erişimi olan bir akıllı telefon veya tabletin kişisel bir etkin nokta oluşturmak için etkinleştirilmesidir. Bu özelliğe bazen tethering denir. Hotspot, genellikle bir akıllı telefonun bir Wi-Fi yönlendiricisinin kablosuz hizmetlerini sağlamasını sağlayan geçici bir hızlı çözümdür. Diğer cihazlar internet bağlantısını kullanmak için akıllı telefonla bağlantı kurabilir ve kimlik doğrulaması yapabilir.




## 28.3.2.BSS ve ESS

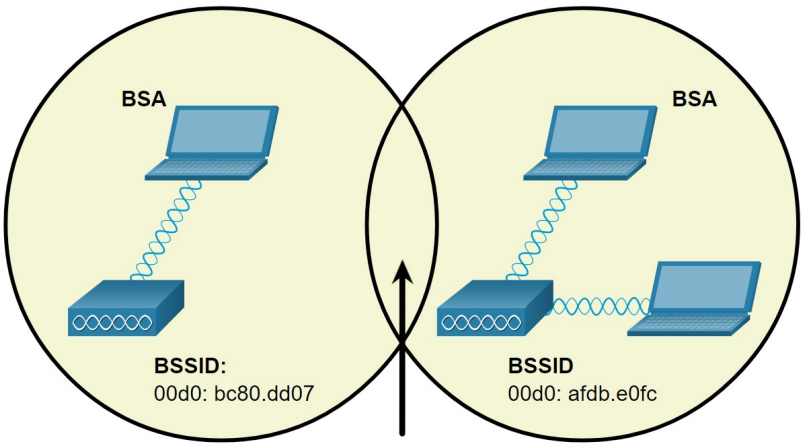
Altyapı modu iki topoloji yapı bloğunu tanımlar: Bir Temel Hizmet Kümesi ( Basic Service Set-BSS) ve bir Genişletilmiş Hizmet Kümesi (Extended Service Set-ESS).

### Temel Servis Seti

Bir BSS, tüm ilişkili kablosuz istemcileri birbirine bağlayan tek bir AP'den oluşur. Şekilde iki BSS gösterilmektedir. Daireler, Temel Hizmet Alanı (BSA) olarak adlandırılan BSS'nin kapsama alanını gösterir. Bir kablosuz istemci BSA'nın dışına çıkarsa, artık BSA içindeki diğer kablosuz istemcilerle doğrudan iletişim kuramaz.

AP'nin Katman 2 MAC adresi, Temel Hizmet Kümesi Tanımlayıcısı (BSSID) olarak adlandırılan her bir BSS'yi benzersiz şekilde tanımlamak için kullanılır. Bu nedenle, BSSID, BSS'nin resmi adıdır ve her zaman yalnızca bir AP ile ilişkilendirilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



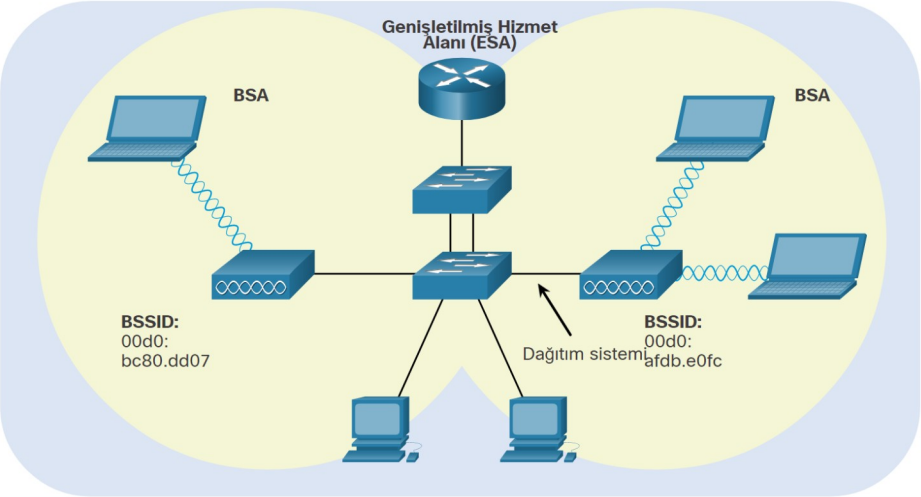

Bağlantı kaybı olmadan BSA'lar arasında dolaşım sağlamak için% 10 ila 15 örtüşme

**Genişletilmiş Servis Seti**

Tek bir BSS yetersiz kapsama sağladığında, iki veya daha fazla BSS ortak bir dağıtım sistemi (DS) aracılığıyla bir ESS'ye birleştirilebilir. ESS, kablolu bir DS ile birbirine bağlanan iki veya daha fazla BSS'nin birleşimidir. Her ESS bir SSID ile tanımlanır ve her BSS kendi BSSID'si ile tanımlanır.

Bir BSA'daki kablosuz istemciler artık aynı ESS içindeki başka bir BSA'daki kablosuz istemcilerle iletişim kurabilir. Gezici mobil kablosuz istemciler bir BSA'dan diğerine (aynı ESS içinde) geçebilir ve sorunsuz bir şekilde bağlanabilir.

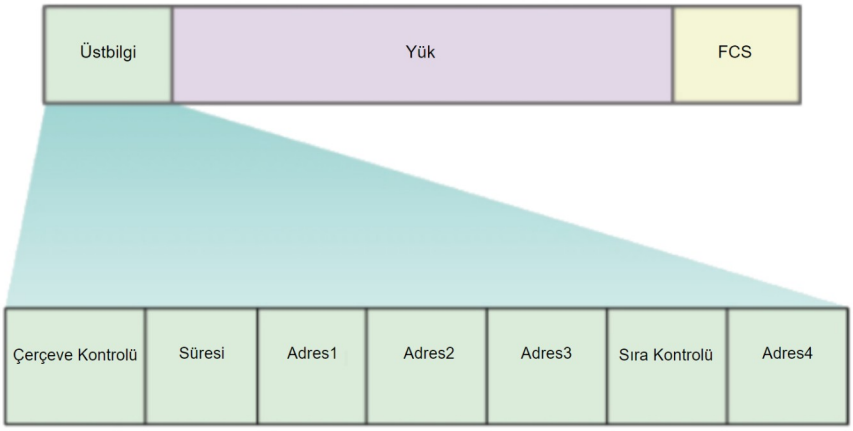
Şekildeki dikdörtgen alan, bir ESS'nin üyelerinin iletişim kurabileceği kapsama alanını tasvir etmektedir. Bu alana Genişletilmiş Hizmet Alanı ( Extended Service Area-ESA) denir.




## 28.3.3.802.11 Çerçeve Yapısı

Tüm Katman 2 çerçevelerinin bir başlık, yük ve Çerçeve Kontrol Sırası (Frame Check Sequence-FCS) bölümünden oluştuğunu hatırlayın. 802.11 çerçeve formatı, şekilde gösterildiği gibi daha fazla alan içermesi dışında Ethernet çerçeve formatına benzer.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Tüm 802.11 kablosuz çerçeveleri aşağıdaki alanları içerir:

- Çerçeve Kontrolü - Bu, kablosuz çerçevenin türünü tanımlar ve protokol sürümü, çerçeve türü, adres türü, güç yönetimi ve güvenlik ayarları için alt alanlar içerir.
- Süre - Bu genellikle bir sonraki çerçeve iletimini almak için gereken kalan süreyi belirtmek için kullanılır.

Kablosuz bir cihazdan:

- 
- Adres 1 Alıcı Adresi - AP'nin MAC adresi.
- Adres 2 Gönderici Adresi - Gönderenin MAC adresi.
- Adres 3 SA / DA / BSSID - hedefin kablosuz veya kablolu cihaz olabilecek MAC adresi.

AP'den:

- Adres 1 Alıcı Adresi - gönderenin MAC adresi.
- Adres 2 Verici Adresi - AP'nin MAC adresi.
- Adres 3 SA / DA / BSSID - kablosuz hedefin MAC adresi.
- Sıra Kontrolü - Bu, sıralamayı ve parçalanmış kareleri kontrol etmeye yönelik bilgileri içerir.
- Adres4 - Bu genellikle eksiktir çünkü yalnızca geçici modda kullanılır.
- Yük - Bu, aktarım verilerini içerir.
- FCS - Bu, Katman 2 hata kontrolü için kullanılır.

## 28.3.4.CSMA / CA

WLAN'lar yarı çift yönlü, paylaşılan medya yapılandırmalarıdır. Yarı çift yönlü, herhangi bir anda yalnızca bir müşterinin iletebileceği veya alabileceği anlamına gelir. Paylaşılan medya, kablosuz istemcilerin tümünün aynı radyo kanalı üzerinden gönderip alabileceği anlamına gelir. Bu bir sorun yaratır çünkü bir kablosuz istemci gönderirken işitemez ve bu da bir çarpışmanın tespit edilmesini imkansız hale getirir.

Bu sorunu çözmek için, WLAN'lar, ağda nasıl ve ne zaman veri gönderileceğini belirleme yöntemi olarak, çarpışma önleme (CSMA / CA-collision avoidance ) ile taşıyıcı algılama çoklu erişimini kullanır. Bir kablosuz istemci şunları yapar:

- Boşta olup olmadığını görmek için kanalı dinler, yani kanalda o anda başka bir trafik olmadığını algılar. Kanal aynı zamanda taşıyıcı olarak da adlandırılır.
- Şebekeye özel erişim istemek için AP'ye (RTS) mesajı gönderme isteği gönderir.
- AP'den gönderime erişim izni veren bir gönderi silme (CTS) mesajı alır.
- Kablosuz istemci bir CTS mesajı almazsa, işlemi yeniden başlatmadan önce rastgele bir süre bekler.
- CTS'yi aldıktan sonra verileri iletir.
- Tüm iletimler onaylandı. Bir kablosuz istemci bir onay almazsa, bir çarpışma olduğunu varsayar ve süreci yeniden başlatır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 28.3.5.Kablosuz İstemci ve AP İlişkilendirilmesi

Kablosuz cihazların bir ağ üzerinden iletişim kurması için, önce bir AP veya kablosuz yönlendirici ile ilişkilendirmeleri gerekir. 802.11 işleminin önemli bir parçası, bir WLAN'ı keşfetmek ve ardından ona bağlanmaktır. Kablosuz cihazlar, aşağıdaki üç aşamalı süreci tamamlar:

- Kablosuz bir AP keşfetme
- AP ile kimlik doğrulama
- AP ile ilişkilendirme

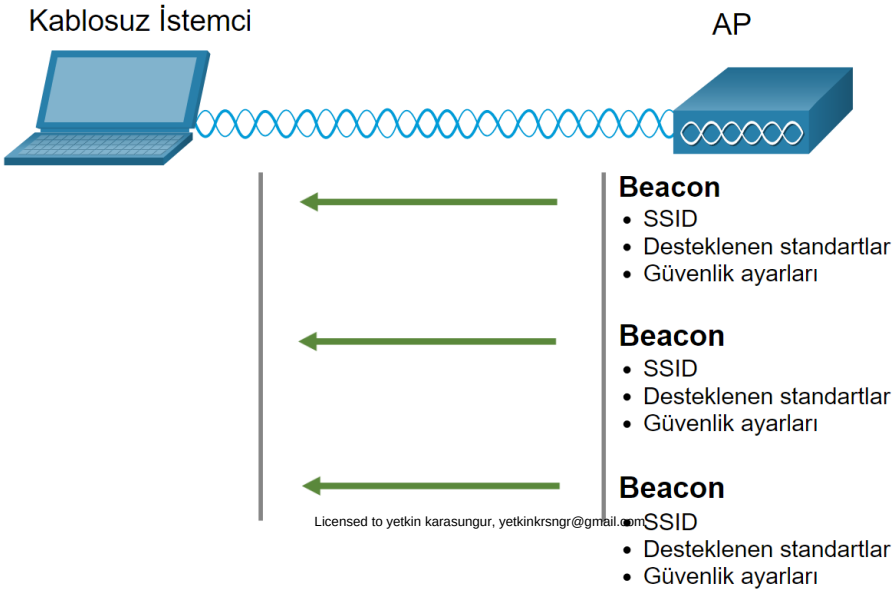
Başarılı bir ilişkiye sahip olmak için, bir kablosuz istemci ve bir AP'nin belirli parametreler üzerinde anlaşması gerekir. Başarılı bir ilişkilendirmenin görüşülmesini sağlamak için parametrelerin daha sonra AP'de ve ardından istemcide yapılandırılması gerekir.

- **SSID** - SSID adı, bir istemcideki kullanılabilir kablosuz ağlar listesinde görünür. Trafiği bölümlere ayırmak için birden çok VLAN kullanan daha büyük kuruluşlarda, her SSID bir VLAN ile eşlenir. Ağ yapılandırmasına bağlı olarak, bir ağdaki birkaç AP ortak bir SSID'yi paylaşabilir.
- **Şifre** - Bu, kablosuz istemcinin AP'de kimlik doğrulaması yapması için gereklidir.
- **Ağ modu** - Bu, 802.11a / b / g / n / ac / ad WLAN standartlarını ifade eder. AP'ler ve kablosuz yönlendiriciler Karma modda çalışabilir, yani birden çok standart aracılığıyla bağlanan istemcileri aynı anda destekleyebilirler.
- **Güvenlik modu** - Bu, WEP, WPA veya WPA2 gibi güvenlik parametresi ayarlarını ifade eder. Her zaman desteklenen en yüksek güvenlik seviyesini etkinleştirin.
- **Kanal ayarları** - Bu, kablosuz verileri iletmek için kullanılan frekans bantlarını ifade eder. Kablosuz yönlendiriciler ve AP'ler, radyo frekansı kanallarını tarayabilir ve uygun bir kanal ayarını otomatik olarak seçebilir. Başka bir AP veya kablosuz cihazla parazit olması durumunda kanal manuel olarak da ayarlanabilir.

## 28.3.6.Pasif ve Aktif Keşif Modu

Kablosuz cihazlar bir AP veya kablosuz yönlendiriciyi bulmalı ve bunlara bağlanmalıdır. Kablosuz istemciler bir tarama (araştırma) işlemi kullanarak AP'ye bağlanır. Bu süreç pasif veya aktif olabilir.

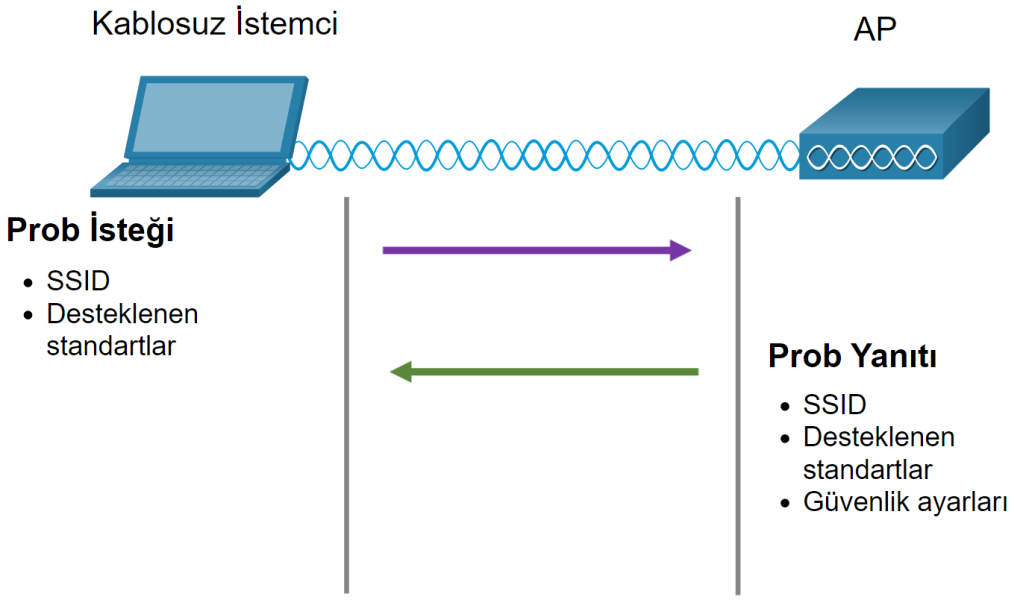
Pasif modda AP, SSID'yi, desteklenen standartları ve güvenlik ayarlarını içeren yayın işaretçisi çerçevelerini periyodik olarak göndererek hizmetini açıkça ilan eder. İşaretin birincil amacı, kablosuz istemcilerin belirli bir alanda hangi ağların ve AP'lerin mevcut olduğunu öğrenmesine izin vermektir. Bu, kablosuz istemcilerin hangi ağı ve AP'yi kullanacağını seçmesine olanak tanır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Etkin-Aktif modda, kablosuz istemciler SSID'nin adını bilmelidir. Kablosuz istemci, birden çok kanalda bir yoklama isteği çerçevesi yayınlayarak işlemi başlatır. Araştırma talebi, desteklenen SSID adını ve standartları içerir. SSID ile yapılandırılan AP'ler, SSID'yi, desteklenen standartları ve güvenlik ayarlarını içeren bir araştırma yanıtı gönderir. Bir AP veya kablosuz yönlendirici işaret çerçevelerini yayınlamayacak şekilde yapılandırılmışsa aktif mod gerekebilir.

Bir kablosuz istemci, yakındaki WLAN ağlarını keşfetmek için bir SSID adı olmadan bir araştırma isteği de gönderebilir. İşaret çerçevelerini yayınlamak için yapılandırılan AP'ler, kablosuz istemciye bir araştırma yanıtı ile yanıt verir ve SSID adını sağlar. SSID yayınlama özelliği devre dışı bırakılmış AP'ler yanıt vermiyor.

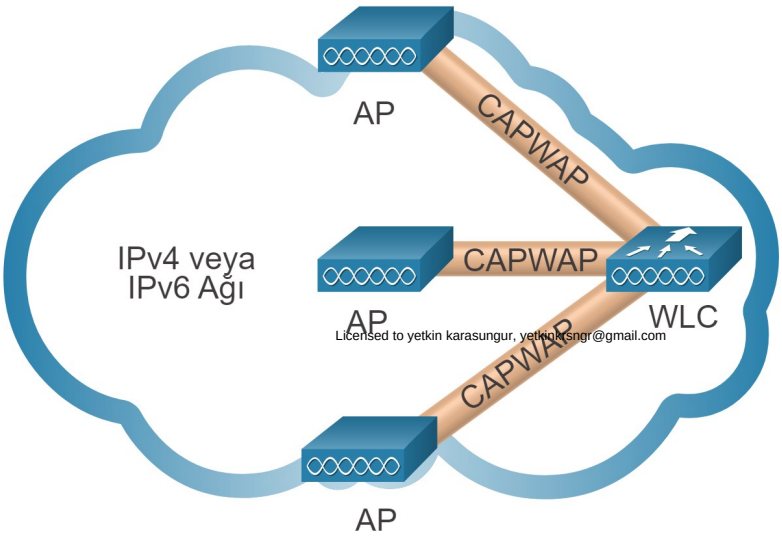



## 28.4.CAPWAP (Control and Provisioning of Wireless Access Points) Nedir?

### 28.4.1.CAPWAP'a Giriş

CAPWAP, bir WLC'nin birden çok AP ve WLAN'ı yönetmesini sağlayan bir IEEE standart protokolüdür. CAPWAP ayrıca, bir AP ve bir WLC arasında WLAN istemci trafiğinin kapsüllenmesinden ve iletilmesinden sorumludur.

CAPWAP, LWAPP'ye dayanır ancak Datagram Aktarım Katmanı Güvenliği- Datagram Transport Layer Security (DTLS) ile ek güvenlik sağlar. CAPWAP, Kullanıcı Datagram Protokolü (UDP) bağlantı noktalarında tüneller oluşturur. CAPWAP, şekilde gösterildiği gibi IPv4 veya IPv6 üzerinden çalışabilir, ancak varsayılan olarak IPv4'ü kullanır.



Licensed to yetkin karasungur, yetkinksngr@gmail.com

IPv4 ve IPv6, UDP bağlantı noktaları 5246 ve 5247'yi kullanır. Bağlantı noktası 5246, AP'yi yönetmek için WLC tarafından kullanılan CAPWAP kontrol mesajları içindir. 5247 numaralı bağlantı noktası, CAPWAP tarafından kablosuz istemcilerden gelen ve giden veri paketlerini kapsüllemek için kullanılır. Ancak, CAPWAP tünelleri, paket başlığında farklı IP protokolleri kullanır. IPv4, IP protokolü 17'yi ve IPv6, IP protokolü 136'yı kullanır.

### 28.4.2.Bölünmüş MAC Mimarisi

CAPWAP'ın temel bileşenlerinden biri, bölünmüş medya erişim denetimi (MAC) kavramıdır. CAPWAP bölünmüş MAC konsepti, normalde bağımsız AP'ler tarafından gerçekleştirilen tüm işlevleri yerine getirir ve bunları iki işlevsel bileşen arasında dağıtır:

- AP MAC İşlevleri
- WLC MAC İşlevleri

Tablo, her biri tarafından gerçekleştirilen bazı MAC işlevlerini göstermektedir.

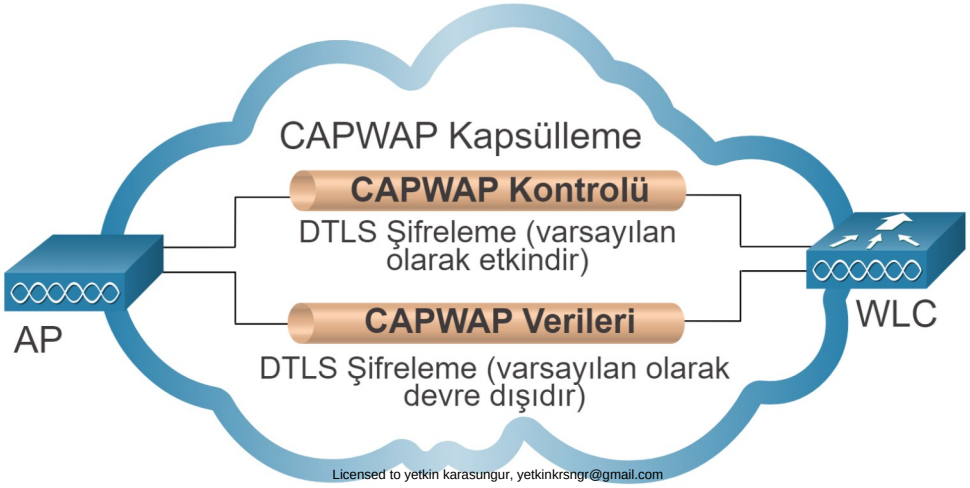
| AP MAC İşlevleri | WLC MAC İşlevleri |
|---|---|
| İşaretler ve araştırma yanıtları | Doğrulama |
| Paket alındı bildirimleri ve yeniden iletimler | Gezici istemcilerin ilişkilendirilmesi ve yeniden ilişkilendirilmesi |
| Çerçeve kuyruğa alma ve paket önceliklendirme | Diğer protokollere çerçeve çevirisi |
| MAC katmanı veri şifreleme ve şifre çözme | 802.11 trafiğinin kablolu bir arayüzde sonlandırılması |

### 28.4.3.DTLS Şifreleme

DTLS, AP ile WLC arasında güvenlik sağlayan bir protokoldür. Şifreleme kullanarak iletişim kurmalarına olanak tanır ve gizli dinlemeyi veya kurcalanmayı önler.

DTLS, CAPWAP kontrol kanalının güvenliğini sağlamak için varsayılan olarak etkindir, ancak şekilde gösterildiği gibi veri kanalı için varsayılan olarak devre dışı bırakılmıştır. AP ile WLC arasında değiş tokuş edilen tüm CAPWAP yönetimi ve kontrol trafiği, kontrol düzlemi gizliliği sağlamak ve Man-In-the-Middle (MITM) saldırılarını önlemek için varsayılan olarak şifrelenir ve güven altına alınır.

CAPWAP veri şifreleme isteğe bağlıdır ve AP başına etkindir. Veri şifreleme, bir AP'de etkinleştirilmeden önce WLC'ye DTLS lisansının yüklenmesini gerektirir. Etkinleştirildiğinde, tüm WLAN istemci trafiği, WLC'ye iletilmeden önce AP'de şifrelenir ve bunun tersi de geçerlidir.

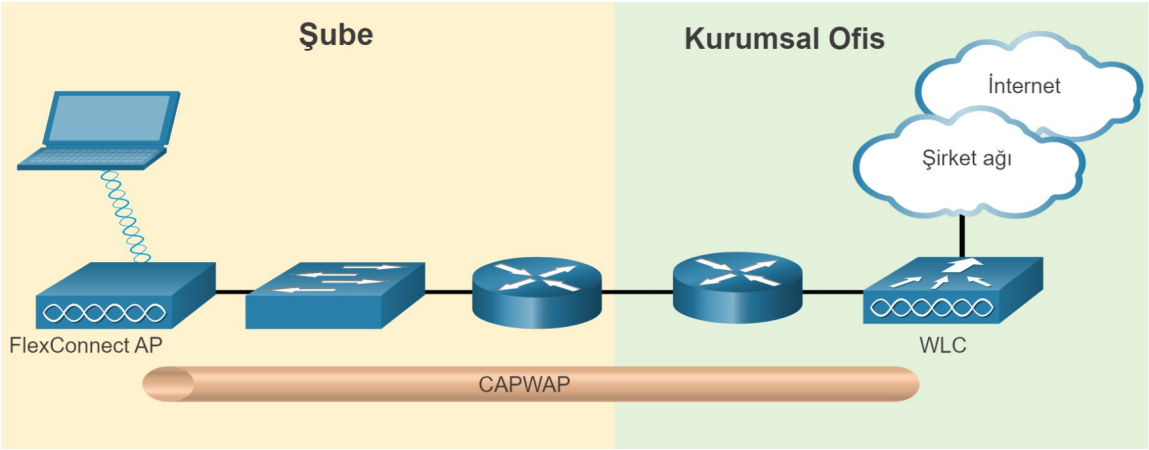


### 28.4.4.FlexConnect AP'ler

FlexConnect, şube ofisleri ve uzak ofis dağıtımları için kablosuz bir çözümdür. Her ofise bir denetleyici dağıtmadan, bir WAN bağlantısı aracılığıyla kurumsal ofisten bir şubedeki erişim noktalarını yapılandırmanıza ve kontrol etmenize olanak tanır.

FlexConnect AP için iki çalışma modu vardır.

**Bağlantı modu** - WLC'ye erişilebilir. Bu modda FlexConnect AP, WLC ile CAPWAP bağlantısına sahiptir ve şekilde gösterildiği gibi CAPWAP tüneli üzerinden trafik gönderebilir. WLC, tüm CAPWAP işlevlerini yerine getirir.
**Bağımsız mod** - WLC'ye erişilemez. FlexConnect, WLC ile CAPWAP bağlantısını kaybetti veya başarısız oldu. Bu modda, bir FlexConnect AP, istemci veri trafiğini yerel olarak değiştirmek ve istemci kimlik doğrulamasını yerel olarak gerçekleştirmek gibi bazı WLC işlevlerini üstlenebilir.



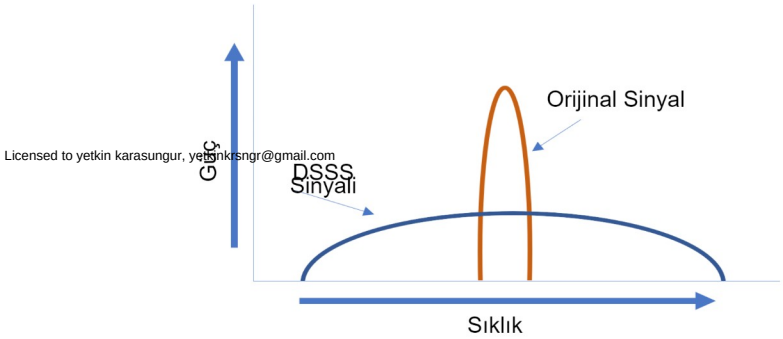

## 28.5.Kanal Yönetimi

### 28.5.1.Frekans Kanalı Doygunluğu

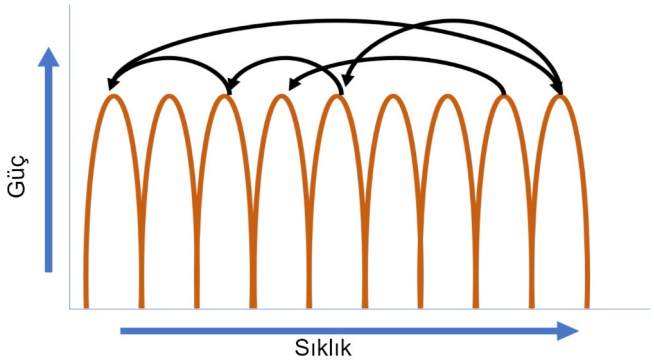
Kablosuz LAN cihazlarında, iletişim kurmak için radyo dalgalarının belirli frekanslarına ayarlanmış vericiler ve alıcılar bulunur. Yaygın bir uygulama, frekansların aralıklar olarak tahsis edilmesidir. Bu tür aralıklar daha sonra kanal adı verilen daha küçük aralıklara bölünür.

Belirli bir kanala olan talep çok yüksekse, o kanalın aşırı doygun hale gelme olasılığı yüksektir. Kablosuz ortamın doygunluğu, iletişimin kalitesini düşürür. Yıllar geçtikçe, kablosuz iletişimi geliştirmek ve doygunluğu azaltmak için bir dizi teknik oluşturuldu. Bu teknikler, kanalları daha verimli bir şekilde kullanarak kanal doygunluğunu azaltır.

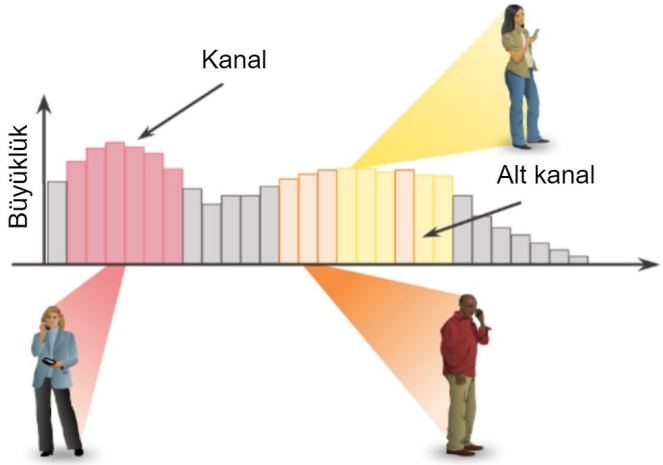
**Direct-Sequence Spread Spectrum (DSSS)** - Bu, bir sinyali daha büyük bir frekans bandına yaymak için tasarlanmış bir modülasyon tekniğidir. Yaygın spektrum teknikleri, düşmanların bir iletişim sinyalini kesmesini veya bozmasını daha zor hale getirmek için savaş sırasında geliştirildi. Bunu, şekilde gösterildiği gibi, sinyalin fark edilebilir tepe noktasını etkili bir şekilde gizleyen daha geniş bir frekansa yayarak yapar. Uygun şekilde yapılandırılmış bir alıcı, DSSS modülasyonunu tersine çevirebilir ve orijinal sinyali yeniden oluşturabilir. DSSS, 802.11b aygıtları tarafından, aynı 2,4 GHz frekansını kullanan diğer aygıtların neden olduğu paraziti önlemek için kullanılır.



**Frequency-Hopping Spread Spectrum (FHSS)** - Bu, iletişim için yayılmış spektrum yöntemlerine dayanır. Birçok frekans kanalı arasında bir taşıyıcı sinyali hızla değiştirerek radyo sinyallerini iletir. FHSS ile, gönderen ve alıcının hangi kanala atlanacağını "bilmek" için senkronize edilmesi gerekir. Bu kanal atlama işlemi, kanalların daha verimli kullanılmasına izin vererek kanal tıkanıklığını azaltır. FHSS, orijinal 802.11 standardı tarafından kullanılmıştır. Telsizler ve 900 MHz kablosuz telefonlar da FHSS kullanır ve Bluetooth FHSS kullanır.

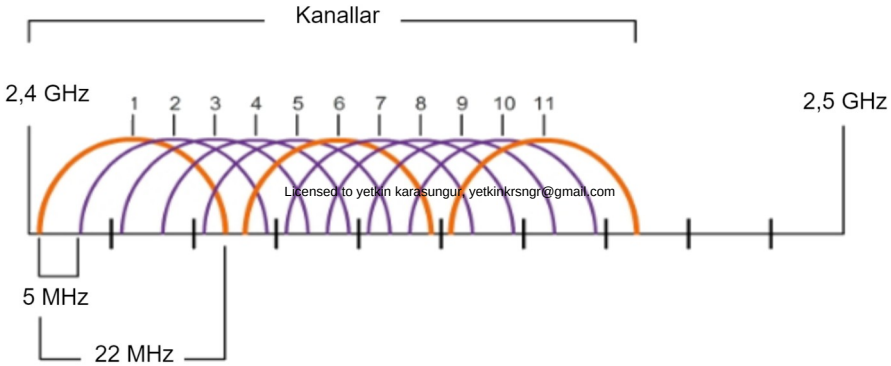



**Orthogonal Frequency-Division Multiplexing (OFDM)** -Bu, tek bir kanalın bitişik frekanslarda birden fazla alt kanal kullandığı bir frekans bölmeli çoğullama alt kümesidir. Bir OFDM sistemindeki alt kanallar, birbirine tam olarak ortogonaldir ve alt kanalların karışmadan üst üste gelmesine izin verir. OFDM, 802.11a / g / n / ac dahil bir dizi iletişim sistemi tarafından kullanılır. Yeni 802.11ax, Ortogonal frekans bölmeli çoklu erişim- Orthogonal frequency-division multiaccess(OFDMA) adı verilen bir OFDM varyasyonunu kullanır.




**28.5.2.Kanal Seçimi**

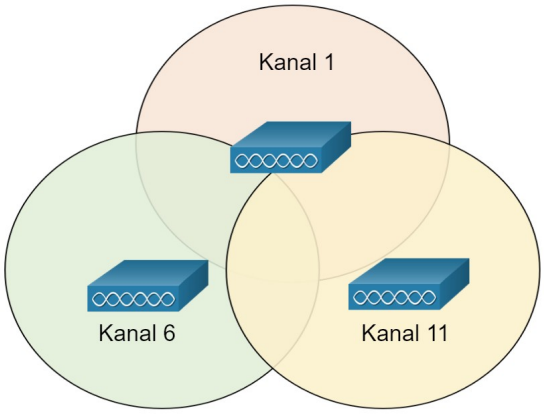
Birden çok AP gerektiren WLAN'lar için en iyi uygulama, çakışmayan kanalları kullanmaktır. Örneğin, 802.11b / g / n standartları 2,4 GHz ila 2,5 GHz spektrumunda çalışır. 2,4 GHz bant, birden çok kanala bölünmüştür. Her kanala 22 MHz bant genişliği tahsis edilir ve sonraki kanaldan 5 MHz ile ayrılır. 802.11b standardı, şekilde gösterildiği gibi Kuzey Amerika için 11 kanalı tanımlar (Avrupa'da 13 ve Japonya'da 14).



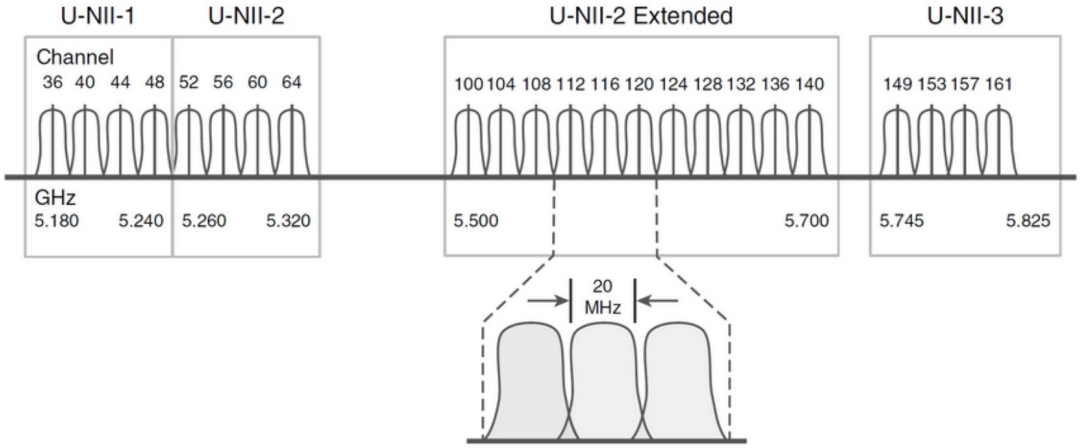
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Parazit, bir sinyal başka bir sinyal için ayrılmış bir kanalla çakıştığında meydana gelir ve olası bozulmaya neden olur. Birden çok AP gerektiren 2,4 GHz WLAN'lar için en iyi uygulama, çoğu modern AP bunu otomatik olarak yapsa da, çakışmayan kanalları kullanmaktır. Üç bitişik AP varsa, şekilde gösterildiği gibi **1., 6. ve 11.** kanalları kullanın.

**802.11b / g / n için 2.4 GHz Çakışmayan Kanallar**

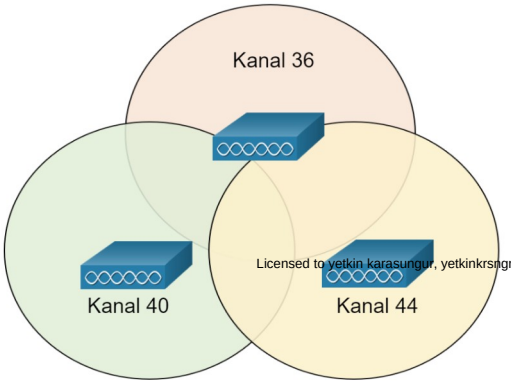



5 GHz standartları 802.11a / n / ac için 24 kanal vardır. 5 GHz bandı üç bölüme ayrılmıştır. Her kanal bir sonraki kanaldan 20 MHz ile ayrılır. Şekilde, 5 GHz bandı için 24 Lisanssız Ulusal Bilgi Altyapısı (U-NNI) 24 kanalının tamamı gösterilmektedir. Her bir kanalın frekansının kuyruklarında hafif bir çakışma olsa da, kanallar birbirine karışmaz. 5 GHz kablosuz, çok sayıda örtüşmeyen kablosuz kanal nedeniyle yoğun nüfuslu kablosuz ağlardaki kablosuz istemciler için daha hızlı veri iletimi sağlayabilir.




2,4 GHz WLAN'larda olduğu gibi, şekilde gösterildiği gibi birbirine bitişik birden çok 5 GHz AP'yi yapılandırırken engellemeyen kanalları seçin.

**802.11a / n / ac için 5 GHz Etkileşimsiz Kanallar**




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 28.6. Kablosuz Ağ Güvenliği

### 28.6.1.Kablosuz Ağ Güvenliğine Genel Bakış

WLAN, bir AP menzilinde bulunan ve onunla ilişkilendirilecek uygun kimlik bilgilerine açık olan herkese açıktır. Kablosuz bir NIC ve kırma teknikleri bilgisiyle, bir saldırganın bir WLAN'a erişmek için işyerine fiziksel olarak girmesi gerekmeyebilir.

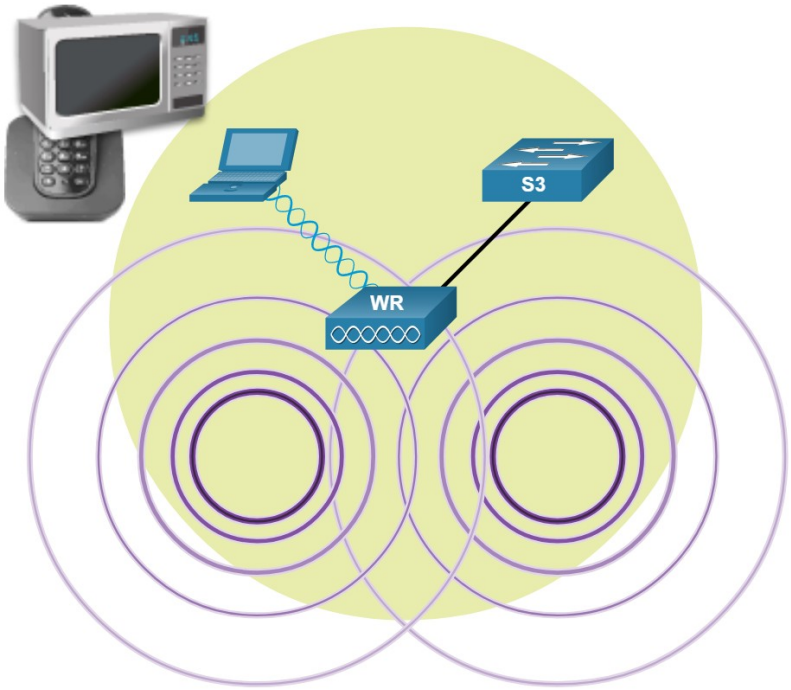
Saldırılar yabancılar, hoşnutsuz çalışanlar ve hatta istemeden çalışanlar tarafından oluşturulabilir. Kablosuz ağlar, özellikle aşağıdakiler de dahil olmak üzere çeşitli tehditlere karşı hassastır:

**Verilerin ele geçirilmesi** - Kablosuz veriler, dinleyiciler tarafından okunmasını önlemek için şifrelenmelidir.
**Kablosuz saldırganlar** - Ağ kaynaklarına erişmeye çalışan yetkisiz kullanıcılar, etkili kimlik doğrulama teknikleriyle caydırılabilir.
**Hizmet Reddi (DoS) Saldırıları** - WLAN hizmetlerine erişim, yanlışlıkla veya kötü niyetle tehlikeye atılabilir. DoS saldırısının kaynağına bağlı olarak çeşitli çözümler mevcuttur.
**Rogue-Sahte AP'ler** - İyi niyetli bir kullanıcı tarafından veya kötü niyetli amaçlarla kurulan yetkisiz AP'ler, yönetim yazılımı kullanılarak tespit edilebilir.

### DoS Saldırıları

Kablosuz DoS saldırıları şunların sonucu olabilir:

**Yanlış yapılandırılmış cihazlar** - Yapılandırma hataları WLAN'ı devre dışı bırakabilir. Örneğin, bir yönetici yanlışlıkla bir yapılandırmayı değiştirebilir ve ağı devre dışı bırakabilir veya yönetici ayrıcalıklarına sahip bir davetsiz misafir kasıtlı olarak bir WLAN'ı devre dışı bırakabilir.
**Kablosuz iletişime kasıtlı olarak müdahale eden kötü niyetli bir kullanıcı -** Amacı, kablosuz ağı tamamen veya hiçbir yasal cihazın ortama erişemeyeceği noktaya kadar devre dışı bırakmaktır.
**Kazayla etkileşim -** WLAN'lar, şekilde gösterildiği gibi mikrodalga fırınlar, telsiz telefonlar, bebek kameraları vb. diğer kablosuz cihazlardan kaynaklanan girişime eğilimlidir. 2,4 GHz bandı, 5 GHz bandından daha fazla parazite eğilimlidir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

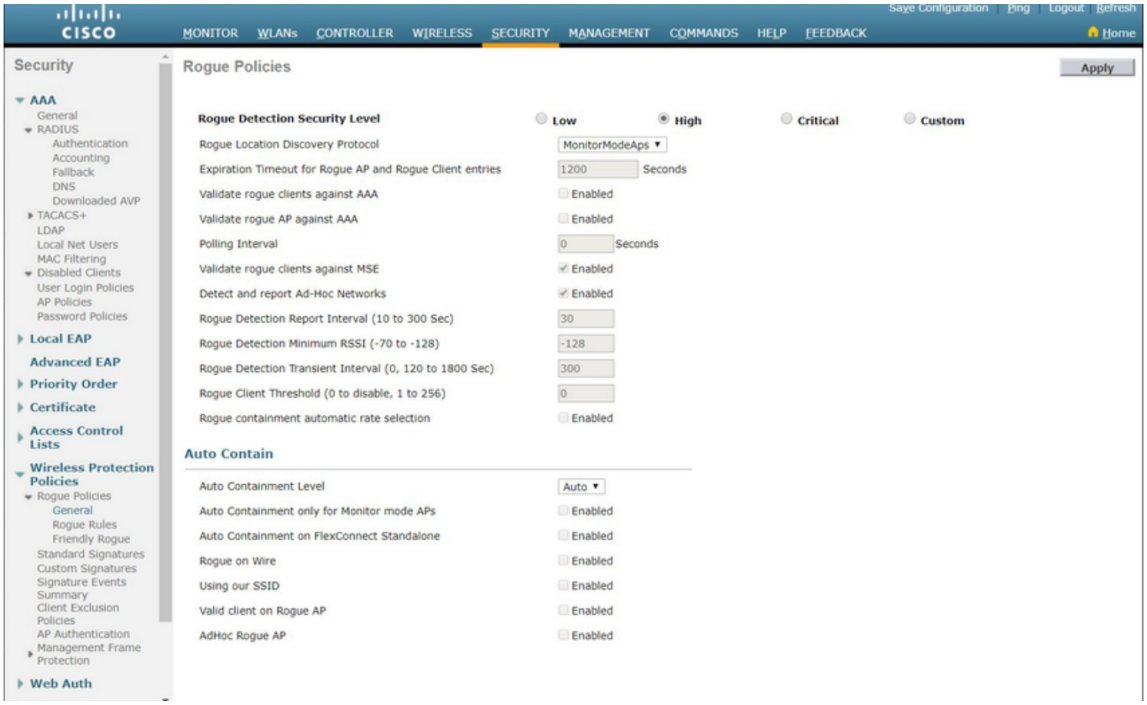
## Yetkisiz Erişim Noktaları

Sahte AP, kurumsal bir ağa açık yetkilendirme olmaksızın ve kurumsal politikaya aykırı olarak bağlanan bir AP veya kablosuz yönlendiricidir. Tesislere erişimi olan herkes güvenli bir ağ kaynağına erişime izin verebilecek, pahalı olmayan bir kablosuz yönlendirici kurabilir.

Bağlandıktan sonra sahte AP, bir saldırgan tarafından MAC adreslerini yakalamak, veri paketlerini yakalamak, ağ kaynaklarına erişmek veya ortadaki adam saldırısı başlatmak için kullanılabilir.

Kişisel bir ağ erişim noktası da hileli AP olarak kullanılabilir. Örneğin, güvenli ağ erişimine sahip bir kullanıcı, yetkili Windows ana bilgisayarının bir Wi-Fi AP olmasını sağlar. Bunu yapmak, güvenlik önlemlerini atlatır ve diğer yetkisiz cihazlar artık ağ kaynaklarına paylaşılan bir cihaz olarak erişebilir.

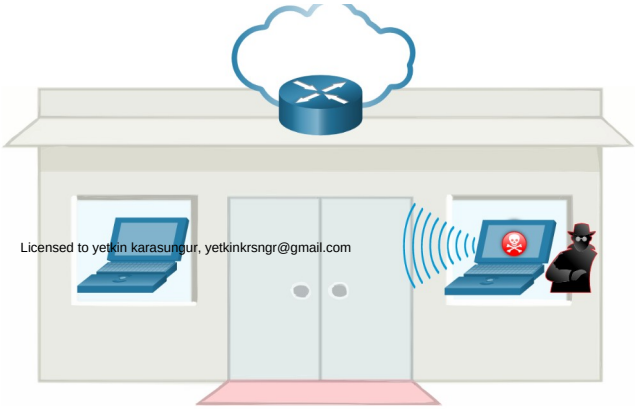
Sahte AP'lerin kurulumunu önlemek için, kuruluşlar WLC'leri şekilde gösterildiği gibi sahte AP politikalarıyla yapılandırmalı ve yetkisiz AP'ler için radyo spektrumunu aktif olarak izlemek için izleme yazılımı kullanmalıdır.



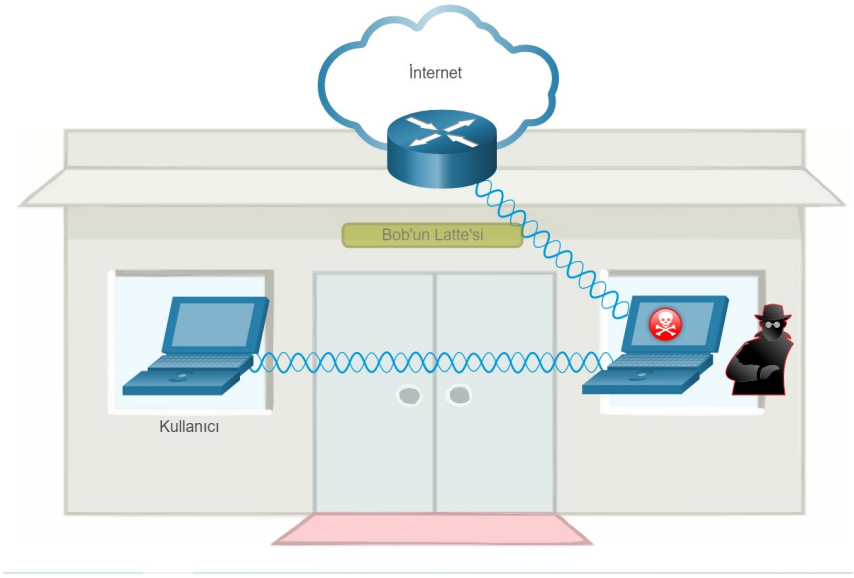

## Ortadaki Adam Saldırısı

Bir ortadaki adam (MITM) saldırısında, bilgisayar korsanı, iki taraf arasında geçen verileri okumak veya değiştirmek için iki meşru varlık arasında konumlandırılır. Bir MITM saldırısı oluşturmanın birçok yolu vardır.

Popüler bir kablosuz MITM saldırısına "kötü ikiz (evil twin) AP" saldırısı adı verilir; burada bir saldırgan, sahte bir AP'yi tanıtır ve bunu şekilde gösterildiği gibi meşru bir AP ile aynı SSID ile yapılandırır. Havaalanları, kafeler ve restoranlar gibi ücretsiz Wi-Fi sunan konumlar, açık kimlik doğrulaması nedeniyle bu tür saldırılar için özellikle popüler noktalardır.



Bir WLAN'a bağlanmaya çalışan kablosuz istemciler, kablosuz erişim sunan aynı SSID'ye sahip iki AP görürler. Sahte AP'nin yakınındakiler daha güçlü sinyali bulur ve büyük olasılıkla onunla ilişkilendirilir. Kullanıcı trafiği artık, verileri yakalayan ve şekilde gösterildiği gibi meşru AP'ye ileten sahte AP'ye gönderilir. Meşru AP'den geri dönüş trafiği sahte AP'ye gönderilir, yakalanır ve ardından şüphelenmeyen kullanıcıya iletilir. Saldırgan, kullanıcının parolalarını, kişisel bilgilerini çalabilir, cihazına erişim sağlayabilir ve sistemi tehlikeye atabilir.




Bir MITM saldırısı gibi bir saldırıyı yenmek, WLAN altyapısının karmaşıklığına ve ağdaki etkinliği izleme konusundaki uyanıklığa bağlıdır. Süreç, WLAN'daki yasal aygıtların tanımlanmasıyla başlar. Bunu yapmak için kullanıcıların kimliklerinin doğrulanması gerekir. Tüm yasal cihazlar bilindikten sonra, ağ anormal cihazlar veya trafik için izlenebilir.

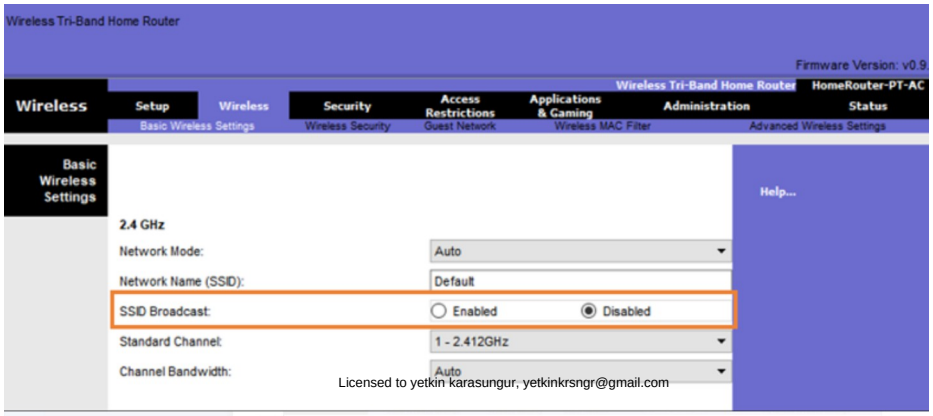
## 28.6.2.SSID Gizleme ve MAC Adresi Filtreleme

Kablosuz sinyaller, tavanlar, zeminler, duvarlar, evin dışı veya ofis alanı gibi katı maddelerden geçebilir. Sıkı güvenlik önlemleri olmadan, bir WLAN kurmak, Ethernet bağlantı noktalarını her yere, hatta dışarıya koymakla eşdeğer olabilir.

Kablosuz davetsiz misafirleri dışarıda tutma ve verileri koruma tehditlerini ele almak için, iki erken güvenlik özelliği kullanıldı ve çoğu yönlendirici ve AP'de hala mevcuttur: SSID gizleme ve MAC adresi filtreleme.

### SSID Gizleme

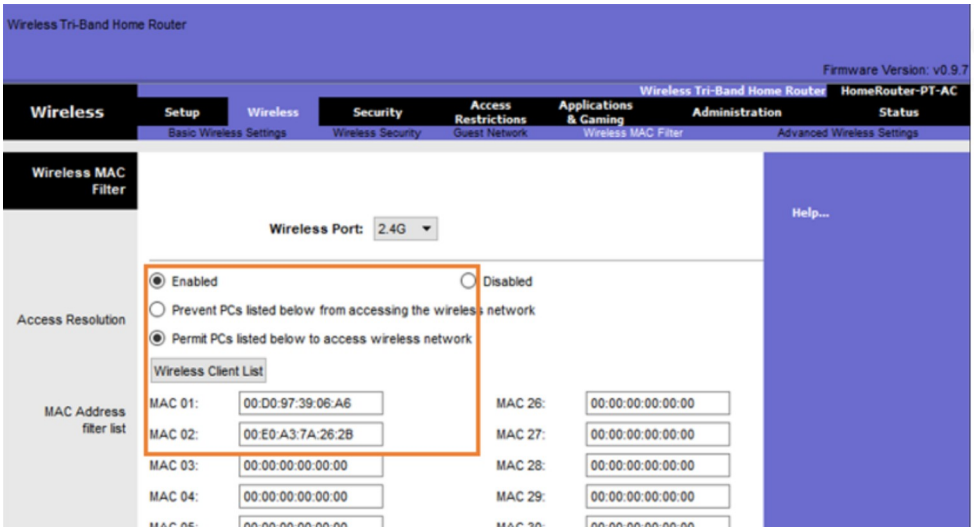
AP'ler ve bazı kablosuz yönlendiriciler, şekilde gösterildiği gibi SSID işaret çerçevesinin devre dışı bırakılmasına izin verir. Kablosuz istemciler, ağa bağlanmak için SSID'yi manuel olarak yapılandırmalıdır.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**MAC Adresleri Filtreleme**

Bir yönetici, fiziksel MAC donanım adreslerine göre istemcilerin kablosuz erişimine manuel olarak izin verebilir veya reddedebilir. Şekilde yönlendirici, iki MAC adresine izin verecek şekilde yapılandırılmıştır. Farklı MAC adreslerine sahip cihazlar, 2.4GHz WLAN'a katılamayacaktır.



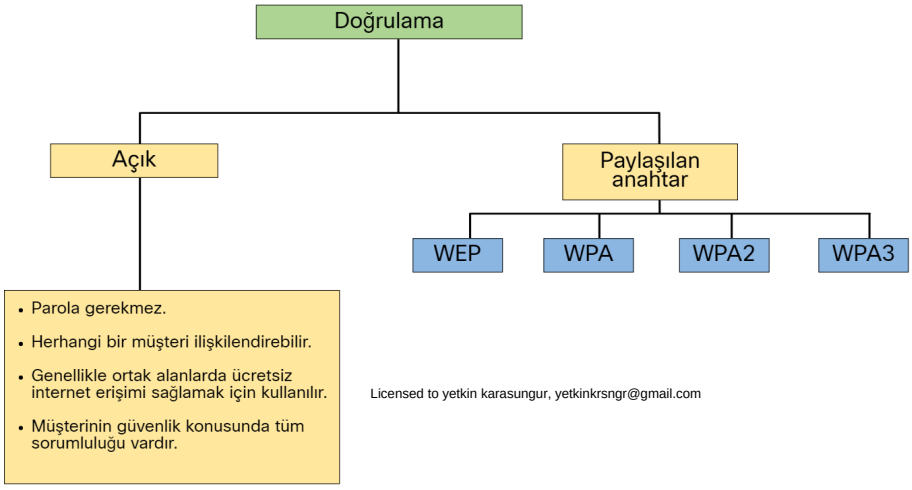

## 28.6.3.802.11 Orijinal Kimlik Doğrulama Yöntemleri

Bu iki özellik çoğu kullanıcıyı caydırsa da gerçek şu ki, ne SSID gizlemesi ne de MAC adres filtrelemesi kurnaz bir davetsiz misafirin önüne geçemez. AP'ler bunları yayınlamasa bile SSID'ler kolayca keşfedilir ve MAC adresleri sahte olabilir. Bir kablosuz ağın güvenliğini sağlamanın en iyi yolu, kimlik doğrulama ve şifreleme sistemleri kullanmaktır.

Orijinal 802.11 standardıyla iki tür kimlik doğrulama tanıtıldı:

**Açık sistem kimlik doğrulaması** - Herhangi bir kablosuz istemci kolayca bağlanabilmeli ve yalnızca kafeler, oteller gibi ücretsiz internet erişimi sağlayanlar ve uzak bölgeler gibi güvenliğin önemli olmadığı durumlarda kullanılmalıdır. Kablosuz istemci, güvenli bir şekilde bağlanmak için bir sanal özel ağ (VPN) kullanmak gibi güvenlik sağlamaktan sorumludur. VPN'ler, kimlik doğrulama ve şifreleme hizmetleri sağlar. VPN'ler bu konunun kapsamı dışındadır.

**Paylaşılan anahtar kimlik doğrulaması** - Bir kablosuz istemci ile AP arasındaki verileri doğrulamak ve şifrelemek için WEP, WPA, WPA2 ve WPA3 gibi mekanizmalar sağlar. Ancak, bağlanmak için parolanın her iki taraf arasında önceden paylaşılması gerekir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 28.6.3.1.Paylaşılan Anahtar Kimlik Doğrulama Yöntemleri

Tabloda açıklandığı gibi kullanılabilen dört paylaşımlı anahtar kimlik doğrulama tekniği vardır. WPA3 cihazlarının mevcudiyeti her yerde bulunana kadar, kablosuz ağlar WPA2 standardını kullanmalıdır.

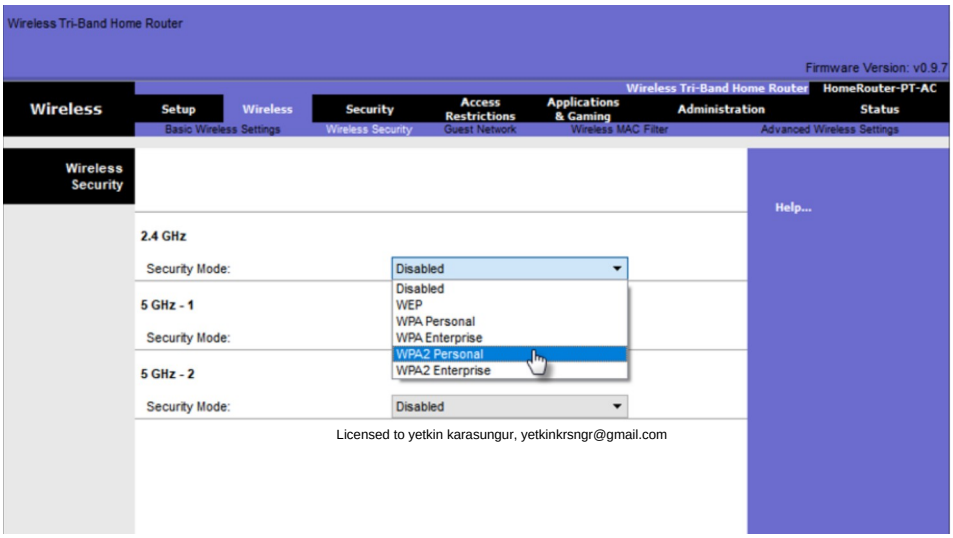
| Kimlik Doğrulama Yöntemi | Açıklama |
|---|---|
| Kabloluya Eşdeğer Gizlilik - Wired Equivalent Privacy (WEP) | Verileri Rivest Cipher 4 (RC4) şifreleme yöntemini kullanarak sabit bir anahtarla güvence altına almak için tasarlanmış orijinal 802.11 spesifikasyonu. Ancak, paketleri değiştirirken anahtar asla değişmez. Bu, hacklemeyi kolaylaştırır. WEP artık tavsiye edilmemektedir ve asla kullanılmamalıdır. |
| Wi-Fi Korumalı Erişim - Wi-Fi Protected Access (WPA) | WEP kullanan ancak verileri çok daha güçlü Geçici Anahtar Bütünlük Protokolü-Temporal Key Integrity Protocol (TKIP) şifreleme algoritmasıyla güvence altına alan bir Wi-Fi Alliance standardı. TKIP, her paketin anahtarını değiştirerek hacklemeyi çok daha zor hale getirir. |
| WPA2 | WPA2, kablosuz ağların güvenliğini sağlamak için mevcut endüstri standardıdır. Şifreleme için Gelişmiş Şifreleme Standardını-Advanced Encryption Standard (AES) kullanır. AES şu anda en güçlü şifreleme protokolü olarak kabul edilmektedir. |
| WPA3 | Yeni nesil Wi-Fi güvenliği. WPA3 özellikli tüm cihazlar en son güvenlik yöntemlerini kullanır, eski eski protokollere izin vermez ve Korumalı Yönetim Çerçevelerinin (PMF) kullanılmasını gerektirir. Ancak, WPA3'e sahip cihazlar henüz yaygın değildir. |

### Bir Ev Kullanıcısının Kimliğini Doğrulama

Ev yönlendiricilerinin tipik olarak kimlik doğrulama için iki seçeneği vardır: WPA ve WPA2. WPA2, ikisinin en güçlüsüdür. Şekil, iki WPA2 kimlik doğrulama yönteminden birini seçme seçeneğini göstermektedir:

**Kişisel-Personal -** Ev veya küçük ofis ağları için tasarlanmıştır, kullanıcılar önceden paylaşılan bir anahtar (PSK) kullanarak kimlik doğrulaması yapar. Kablosuz istemciler, önceden paylaşılan bir parola kullanarak kablosuz yönlendiriciyle kimlik doğrulaması yapar. Özel bir kimlik doğrulama sunucusu gerekmez.
**Kurumsal-Enterprise -** Kurumsal ağlar için tasarlanmıştır, ancak bir Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti (RADIUS) kimlik doğrulama sunucusu gerektirir. Kurulumu daha karmaşık olsa da ek güvenlik sağlar. Cihazın RADIUS sunucusu tarafından doğrulanması ve ardından kullanıcıların kimlik doğrulama için Genişletilebilir Kimlik Doğrulama Protokolü (EAP) kullanan 802.1X standardını kullanarak kimlik doğrulaması yapmaları gerekir.

Şekilde, yönetici kablosuz yönlendiriciyi 2,4 GHz bandında WPA2 Kişisel kimlik doğrulama ile yapılandırıyor.



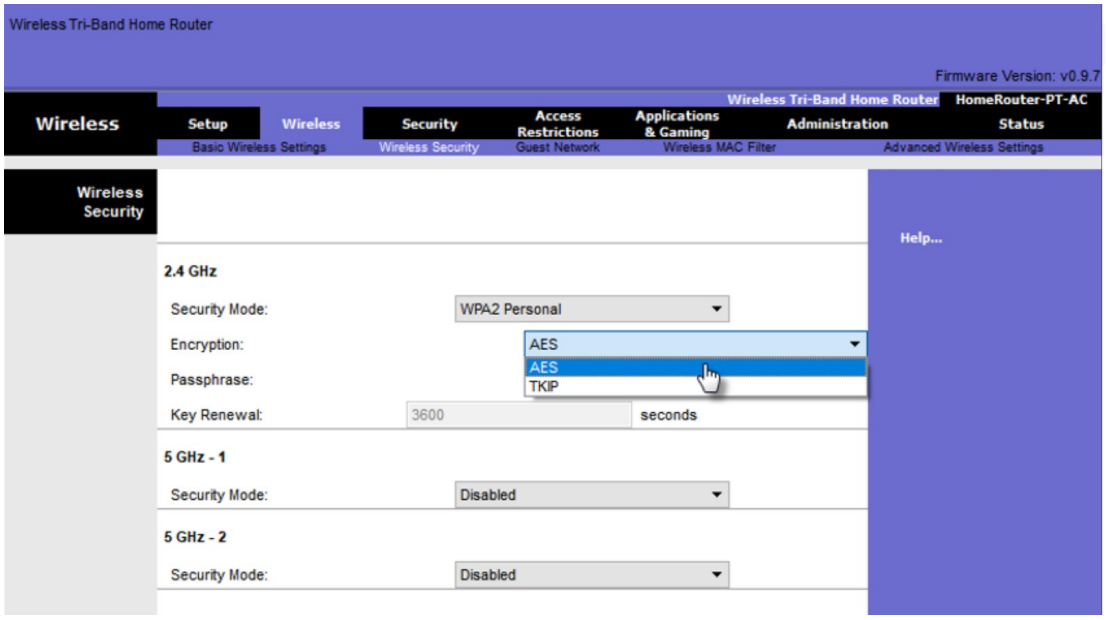
## 28.6.4.Şifreleme Yöntemleri

Verileri korumak için şifreleme kullanılır. Bir saldırgan şifrelenmiş verileri ele geçirmişse, makul bir süre içinde bunları deşifre edemezler.

WPA ve WPA2 standartları aşağıdaki şifreleme protokollerini kullanır:

**Temporal Key Integrity Protocol (TKIP)** - TKIP, WPA tarafından kullanılan şifreleme yöntemidir. 802.11 WEP şifreleme yöntemiyle ilişkili orijinal kusurları ele alarak eski WLAN ekipmanı için destek sağlar. WEP kullanır, ancak Katman 2 yükünü TKIP kullanarak şifreler ve mesajın değiştirilmediğinden emin olmak için şifreli pakette bir Mesaj Bütünlüğü Kontrolü (MIC) gerçekleştirir.
**Gelişmiş Şifreleme Standardı (AES)** - AES, WPA2 tarafından kullanılan şifreleme yöntemidir. Çok daha güçlü bir şifreleme yöntemi olduğu için tercih edilen yöntemdir. Hedef ana bilgisayarların şifrelenmiş ve şifrelenmemiş bitlerin değiştirilip değiştirilmediğini tanımasına olanak tanıyan Blok Zincirleme İleti Kimlik Doğrulama Kodu Protokolü (CCMP) ile Sayaç Şifreleme Modunu kullanır.

Şekilde, yönetici kablosuz yönlendiriciyi 2,4 GHz bandında AES şifrelemeli WPA2 kullanacak şekilde yapılandırıyor.



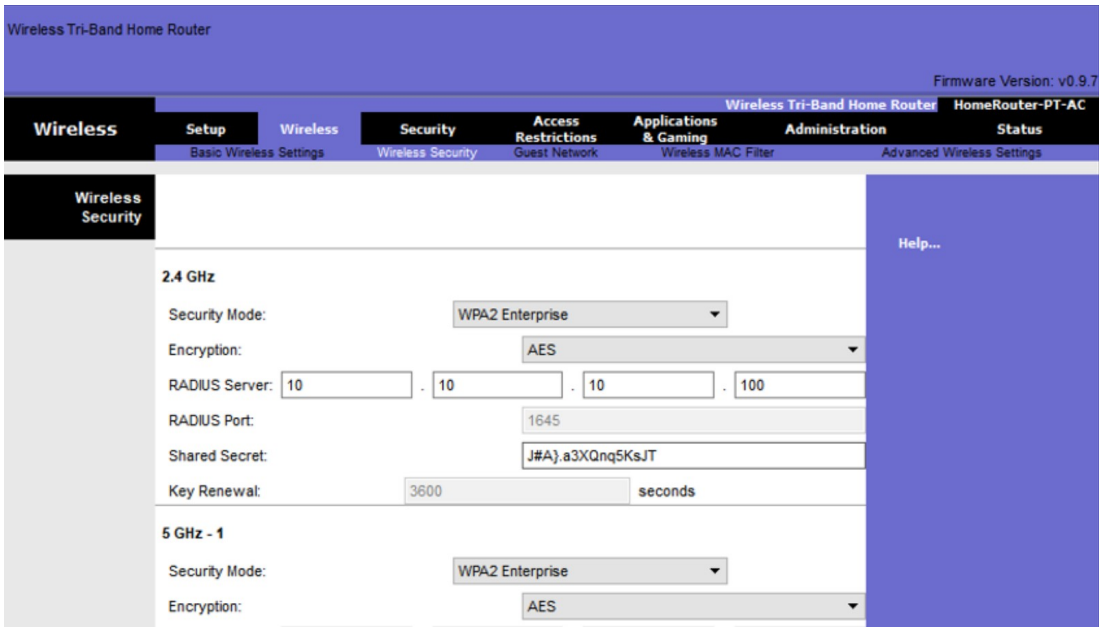

## Kurumsal Kimlik Doğrulama

Daha katı güvenlik gereksinimlerine sahip ağlarda, kablosuz istemcilere bu tür erişim izni vermek için ek bir kimlik doğrulama veya oturum açma gerekir. Kurumsal güvenlik modu seçimi bir Kimlik Doğrulama, Yetkilendirme ve Hesap Oluşturma (AAA) RADIUS sunucusu gerektirir.

**RADIUS Sunucusu IP adresi** - Bu, RADIUS sunucusunun erişilebilir adresidir.
**UDP bağlantı noktası numaraları** - RADIUS Kimlik Doğrulaması için resmi olarak atanan UDP bağlantı noktaları 1812 ve RADIUS Hesabı için 1813, ancak şekilde gösterildiği gibi 1645 ve 1646 UDP bağlantı noktalarını kullanarak da çalışabilir.
**Paylaşılan anahtar** - AP'nin RADIUS sunucusuyla kimliğini doğrulamak için kullanılır.

Şekilde, yönetici kablosuz yönlendiriciyi AES şifrelemesini kullanarak WPA2 Kurumsal kimlik doğrulama ile yapılandırmaktadır. RADIUS sunucusu IPv4 adresi, kablosuz yönlendirici ve RADIUS sunucusu arasında kullanılacak güçlü bir parola ile de yapılandırılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Paylaşılan anahtar, kablosuz bir istemcide yapılandırılması gereken bir parametre değildir. Yalnızca AP'nin RADIUS sunucusuyla kimlik doğrulaması yapması gerekir. Kullanıcı kimlik doğrulama ve yetkilendirme, son kullanıcılar için merkezi, sunucu tabanlı kimlik doğrulaması sağlayan 802.1X standardı tarafından gerçekleştirilir.

802.1X oturum açma işlemi, AP ve RADIUS sunucusuyla iletişim kurmak için EAP kullanır. EAP, ağ erişimini doğrulamak için bir çerçevedir. Güvenli bir kimlik doğrulama mekanizması sağlayabilir ve daha sonra TKIP veya AES şifrelemesini kullanarak kablosuz şifreleme oturumu için kullanılabilen güvenli bir özel anahtar üzerinde anlaşabilir.

## WPA3

WPA2 artık güvenli kabul edilmiyor. WPA3, varsa, önerilen 802.11 kimlik doğrulama yöntemidir. WPA3 dört özellik içerir:

- WPA3-Kişisel
- WPA3-Kurumsal
- Açık Ağlar
- Nesnelerin İnterneti (IoT) İlk Katılımı

### WPA3-Kişisel

WPA2-Kişiselde, tehdit aktörleri bir kablosuz istemci ile AP arasındaki "el sıkışmasını" dinleyebilir ve PSK'yı denemek ve tahmin etmek için kaba kuvvet saldırısı kullanabilir. WPA3-Personal, IEEE 802.11-2016'da belirtilen bir özellik olan Eşzamanlı Eşitlik Doğrulaması'nı (SAE) kullanarak bu saldırıyı engeller. PSK asla açığa çıkmaz ve tehdit aktörünün tahmin etmesini imkansız hale getirir.

### WPA3-Kurumsal

WPA3-Enterprise, hala 802.1X / EAP kimlik doğrulamasını kullanır. Ancak, 192 bitlik bir şifreleme paketinin kullanılmasını gerektirir ve önceki 802.11 standartları için güvenlik protokollerinin karıştırılmasını ortadan kaldırır. WPA3-Enterprise, yüksek güvenlikli Wi-Fi ağlarında yaygın olarak kullanılan Commercial National Security Algorithm (CNSA) Suite'e uyar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Açık Ağlar

WPA2'deki açık ağlar, kullanıcı trafiğini kimliği doğrulanmamış, açık metin olarak gönderir. WPA3'te, açık veya halka açık Wi-Fi ağları hala herhangi bir kimlik doğrulama kullanmaz. Ancak, tüm kablosuz trafiği şifrelemek için Fırsatçı Kablosuz Şifreleme-Opportunistic Wireless Encryption (OWE) kullanırlar.

## IoT İlk Katılım

WPA2, aygıtları önce yapılandırmadan hızlı bir şekilde yerleşik hale getirmek için Wi-Fi Korumalı Kurulum-Wi-Fi Protected Setup (WPS) içermesine rağmen, WPS çeşitli saldırılara karşı savunmasızdır ve önerilmez. Dahası, IoT cihazları tipik olarak başsızdır (headless ), yani yapılandırma için yerleşik GUI'ye sahip olmadıkları ve kablosuz ağa bağlanmak için herhangi bir kolay yönteme ihtiyaç duydukları anlamına gelir. Aygıt Sağlama Protokolü-Device Provisioning Protocol (DPP) bu ihtiyacı karşılamak için tasarlanmıştır. Her bir başsız aygıtın sabit kodlanmış bir genel anahtarı vardır. Anahtar genellikle aygıtın dışına veya paketine Hızlı Yanıt (QR) kodu olarak damgalanmıştır. Ağ yöneticisi QR kodunu tarayabilir ve cihazı hızlı bir şekilde yerleştirebilir. WPA3 standardının tam olarak bir parçası olmasa da, DPP zamanla WPS'nin yerini alacaktır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 29.Bölüm: Kablosuz Ağ Yapılandırmaları

## 29.1.Uzak Site WLAN Yapılandırması

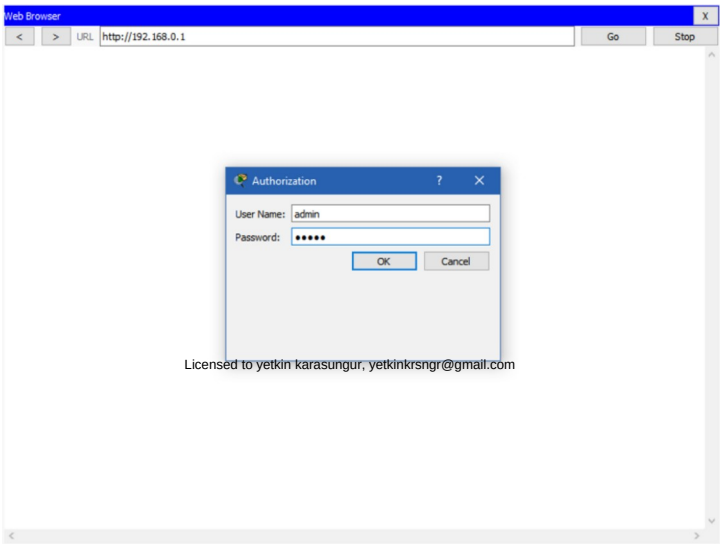
### 29.1.1.Kablosuz Yönlendirici

Uzaktan çalışanlar, küçük şubeler ve ev ağları genellikle küçük bir ofis ve ev yönlendiricisi kullanır. Bu yönlendiriciler genellikle kablolu istemciler için bir anahtar, bir internet bağlantısı için bir bağlantı noktası (bazen "WAN" olarak adlandırılır) ve kablosuz istemci erişimi için kablosuz bileşenler içerdiğinden, bazen entegre yönlendirici olarak adlandırılır.

#### Kablosuz Yönlendiricide Oturum Açma

Çoğu kablosuz yönlendirici, kutudan çıkar çıkmaz hizmete hazırdır. Ağa bağlanacak ve hizmet sağlayacak şekilde önceden yapılandırılırlar. Örneğin, kablosuz yönlendirici, bağlı cihazlara otomatik olarak adresleme bilgisi sağlamak için DHCP kullanır. Ancak, kablosuz yönlendiricinin varsayılan IP adresleri, kullanıcı adları ve şifreleri internette kolayca bulunabilir. Bu bilgiyi sağlayan birçok web sitesinin bir listesini görmek için sadece "varsayılan kablosuz yönlendirici IP adresi" veya "varsayılan kablosuz yönlendirici şifreleri" arama ifadesini girin. Örneğin, şekildeki kablosuz yönlendirici için kullanıcı adı ve şifre "admin" dir. Bu nedenle, ilk önceliğiniz güvenlik nedenleriyle bu varsayılanları değiştirmek olmalıdır.

Kablosuz yönlendiricinin konfigürasyon GUI'sine erişmek için bir web tarayıcısı açın. Adres alanına kablosuz yönlendiricinizin varsayılan IP adresini girin. Varsayılan IP adresi, kablosuz yönlendiriciyle birlikte gelen belgelerde bulunabilir veya internette arama yapabilirsiniz. Şekilde, birçok üretici için ortak bir varsayılan olan IPv4 adresi 192.168.0.1 gösterilmektedir. Bir güvenlik penceresi, yönlendirici GUI'sine erişim yetkisi ister. Admin kelimesi genellikle varsayılan kullanıcı adı ve şifre olarak kullanılır. Yine, kablosuz yönlendiricinizin belgelerini kontrol edin veya internette arama yapın.



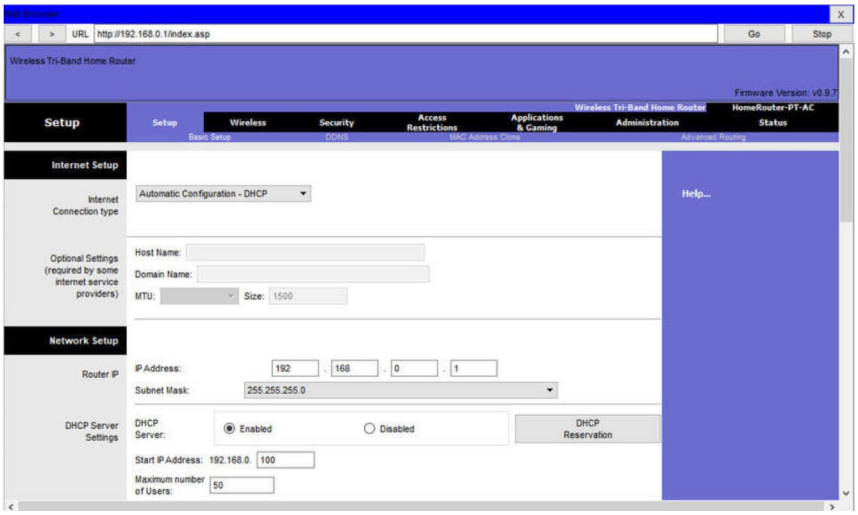
## 29.1.2.Temel Ağ Kurulumu

Temel ağ kurulumu aşağıdaki adımları içerir:

1. Bir web tarayıcısından yönlendiricide oturum açın.
2. Varsayılan yönetici şifresini değiştirin.
3. Yeni yönetici parolası ile oturum açın.
4. Varsayılan DHCP IPv4 adreslerini değiştirin.
5. IP adresini yenileyin.
6. Yeni IP adresiyle yönlendiricide oturum açın.

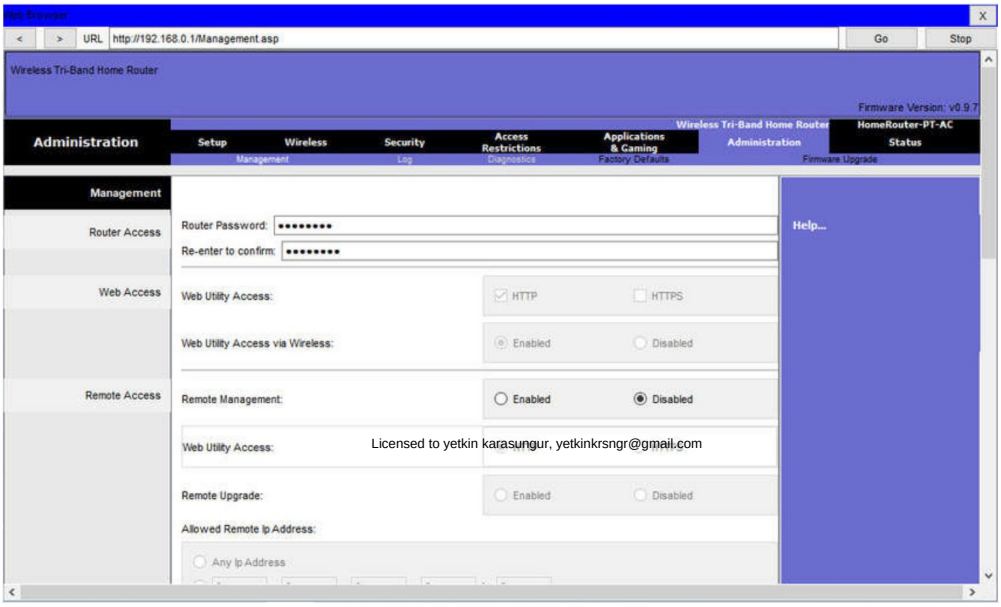
**1 . Bir web tarayıcısından yönlendiricide oturum açın.**

Oturum açtıktan sonra bir GUI açılır. GUI, çeşitli yönlendirici yapılandırma görevlerinde gezinmenize yardımcı olacak sekmelere veya menülere sahip olacaktır. Başka bir pencereye geçmeden önce genellikle bir pencerede değiştirilen ayarları kaydetmek gerekir. Bu noktada, varsayılan ayarlarda değişiklik yapmak en iyi uygulamadır.




**2 . Varsayılan yönetici şifresini değiştirin.**

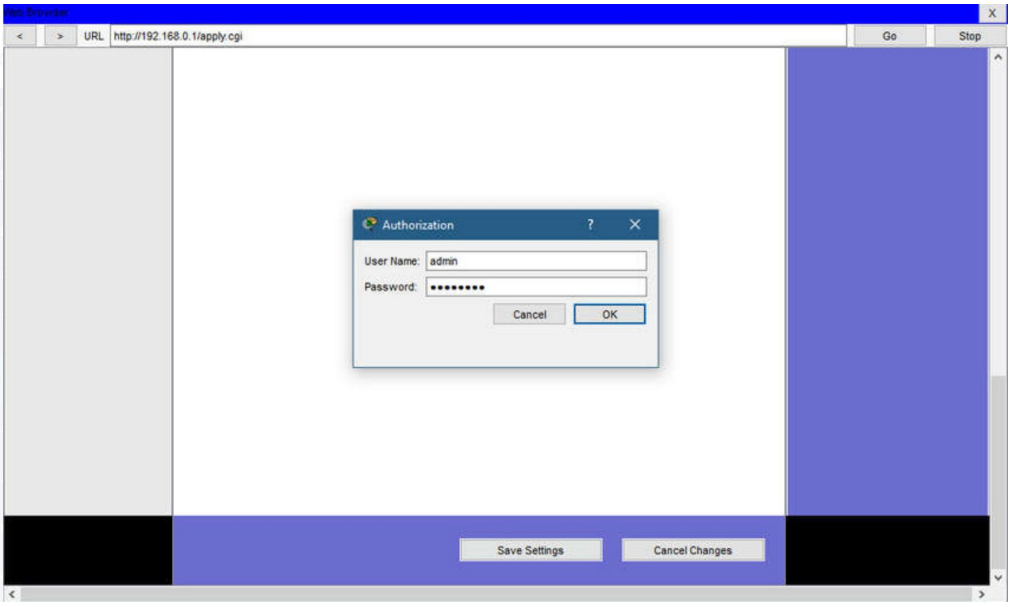
Varsayılan oturum açma parolasını değiştirmek için yönlendiricinin GUI'sinin yönetim bölümünü bulun. Bu örnekte, Yönetim sekmesi seçilmiştir. Yönlendirici şifresinin değiştirilebileceği yer burasıdır. Örnekteki gibi bazı cihazlarda, yalnızca şifreyi değiştirebilirsiniz. Yapılandırdığınız yönlendiricinin varsayılan kullanıcı adı ne olursa olsun kullanıcı adı **admin** olarak kalır.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**3 . Yeni yönetici şifresiyle oturum açın.**

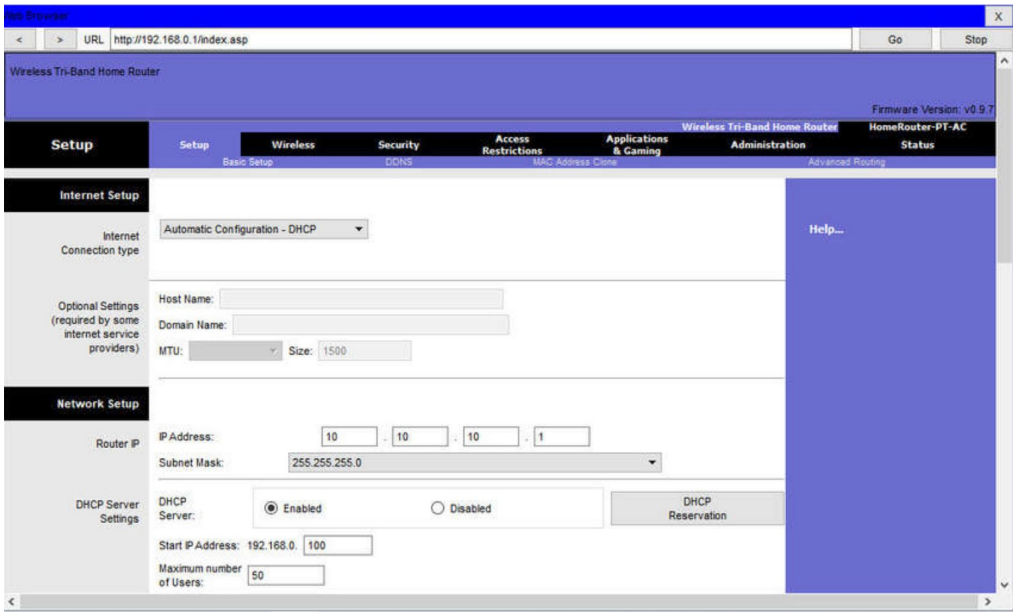
Yeni parolayı kaydettikten sonra, kablosuz yönlendirici yeniden yetkilendirme isteyecektir. Örnekte gösterildiği gibi kullanıcı adını ve yeni şifreyi girin.




**4 . Varsayılan DHCP IPv4 adreslerini değiştirin.**

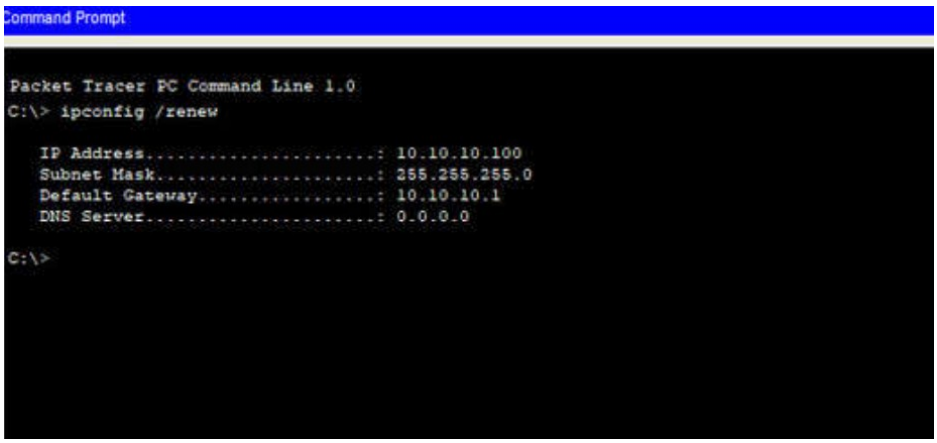
Varsayılan yönlendirici IPv4 adresini değiştirin. Ağınız içinde özel IPv4 adresleme kullanmak en iyi uygulamadır. Örnekte 10.10.10.1 IPv4 adresi kullanılmıştır, ancak seçtiğiniz herhangi bir özel IPv4 adresi olabilir.

**5.IP adresini yenileyin.**



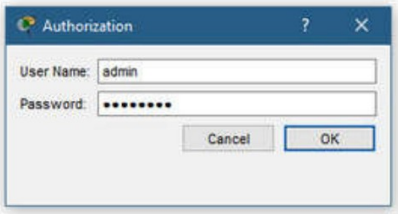

Kaydet'e (Save) tıkladığınızda, kablosuz yönlendiriciye erişimi geçici olarak kaybedersiniz. Bir komut penceresi açın ve örnekte gösterildiği gibi ipconfig / renew komutuyla IP adresinizi yenileyin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




**6 . Yeni IP adresiyle yönlendiricide oturum açın.**

Yönlendirici yapılandırma GUI'sine örnekte gösterildiği gibi yeniden erişim kazanmak için yönlendiricinin yeni IP adresini girin. Artık yönlendiriciyi kablosuz erişim için yapılandırmaya devam etmeye hazırsınız.




## 29.1.3.Temel Kablosuz Kurulum

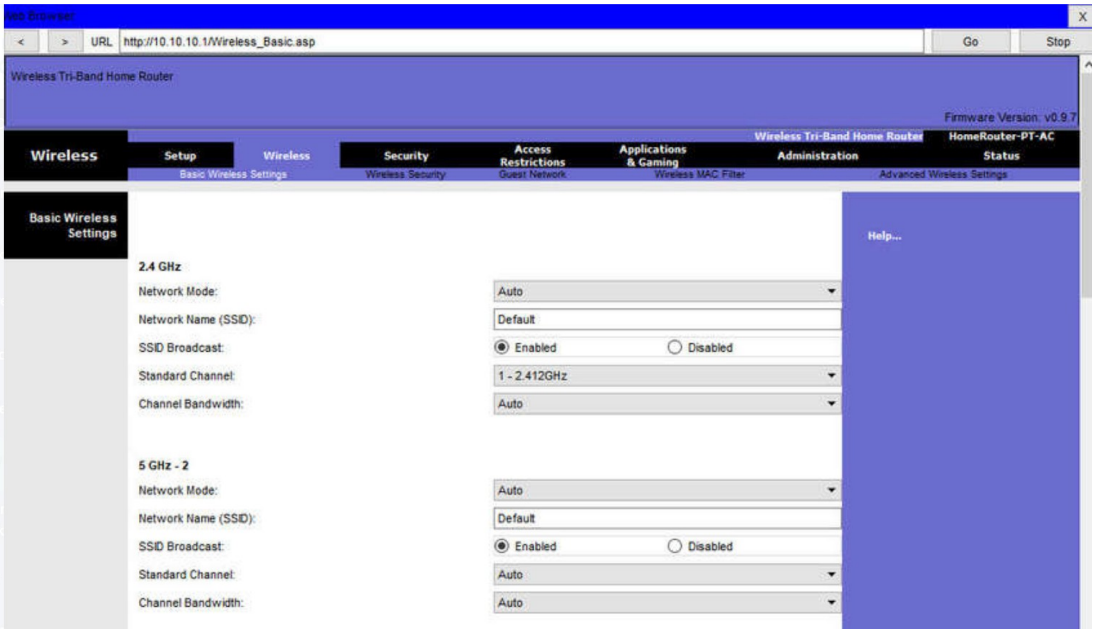
Temel kablosuz kurulum aşağıdaki adımları içerir:

1. WLAN varsayılanlarını görüntüleyin.
2. Ağ modunu değiştirin.
3. SSID'yi yapılandırın.
4. Kanalı yapılandırın.
5. Güvenlik modunu yapılandırın.
6. Parolayı yapılandırın.

**1 . WLAN varsayılanlarını görüntüleyin.**

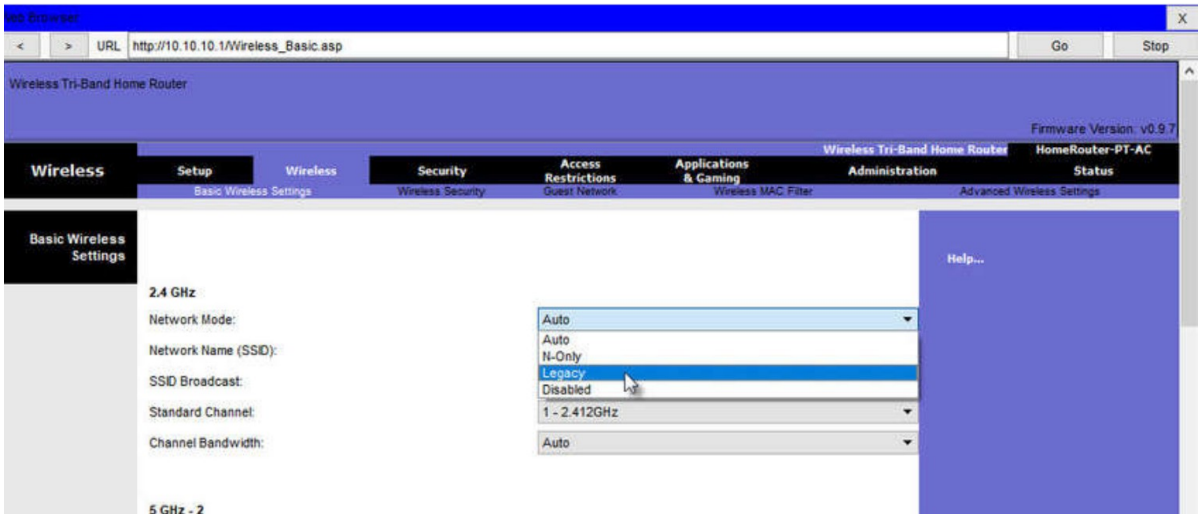
Kutudan çıkar çıkmaz bir kablosuz yönlendirici, varsayılan bir kablosuz ağ adı ve parolası kullanarak aygıtlara kablosuz erişim sağlar. Ağ adı, Hizmet Kümesi- Service Set Identified (SSID) olarak adlandırılır. Örnekte gösterildiği gibi, bu varsayılanları değiştirmek için yönlendiricinizin temel kablosuz ayarlarını bulun.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 2 . Ağ modunu değiştirin.

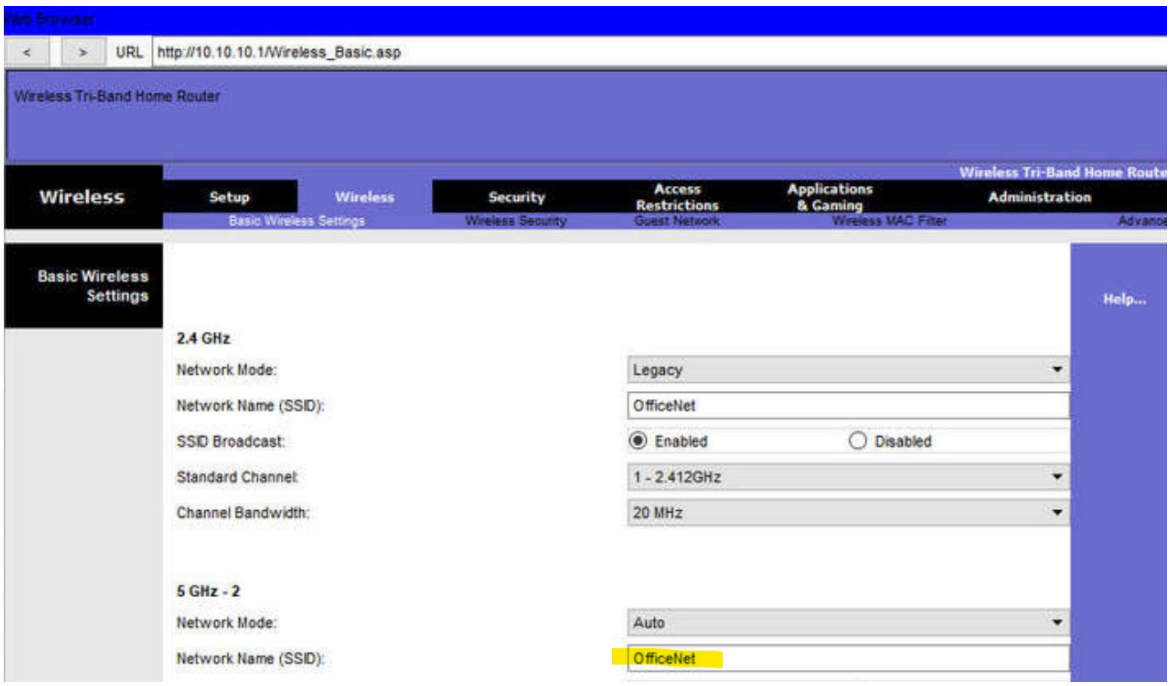
Bazı kablosuz yönlendiriciler, hangi 802.11 standardının uygulanacağını seçmenize izin verir. Örnek, "Eski"-Legacy nin seçildiğini göstermektedir. Bu, kablosuz yönlendiriciye bağlanan kablosuz cihazlarda çeşitli kablosuz NIC'lerin yüklü olabileceği anlamına gelir. Günümüzün eski veya karma mod için yapılandırılmış kablosuz yönlendiricileri, büyük olasılıkla 802.11a, 802.11n ve 802.11ac NIC'leri desteklemektedir.




## 3 . SSID'yi yapılandırın.

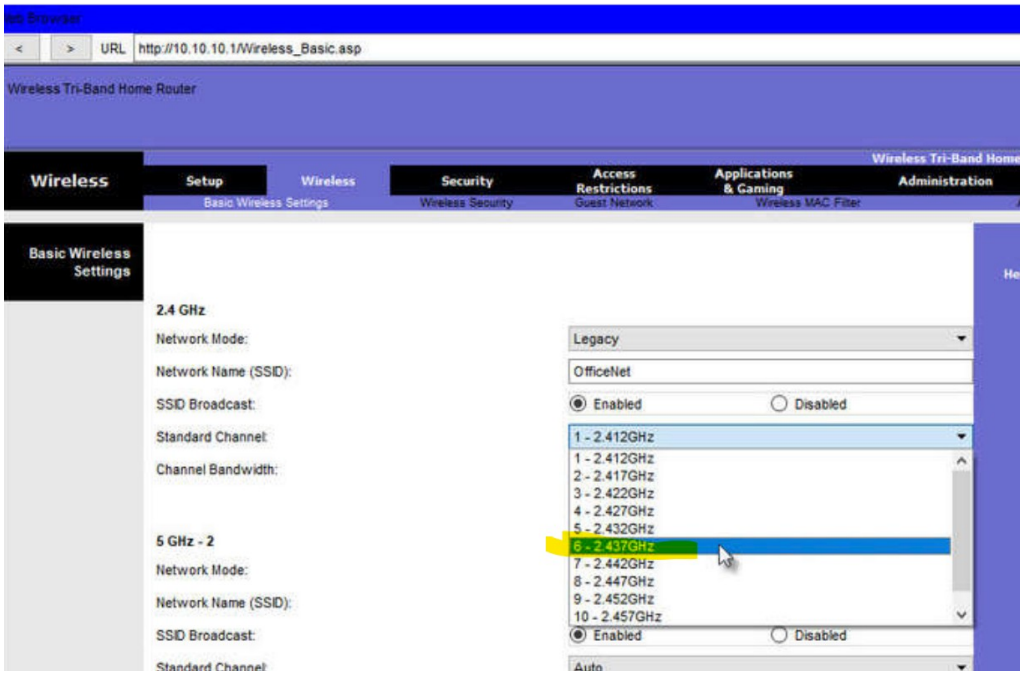
WLAN'lara bir SSID atayın. OfficeNet, örnekte üç WLAN için de kullanılmıştır (üçüncü WLAN gösterilmemiştir). Kablosuz yönlendirici, SSID'sini tanıtan yayınlar göndererek varlığını duyurur. Bu, kablosuz ana bilgisayarların kablosuz ağın adını otomatik olarak bulmasını sağlar. SSID yayını devre dışı bırakılırsa, WLAN'a bağlanan her kablosuz cihazda SSID'yi manuel olarak girmeniz gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




**4 . Kanalı yapılandırın.**

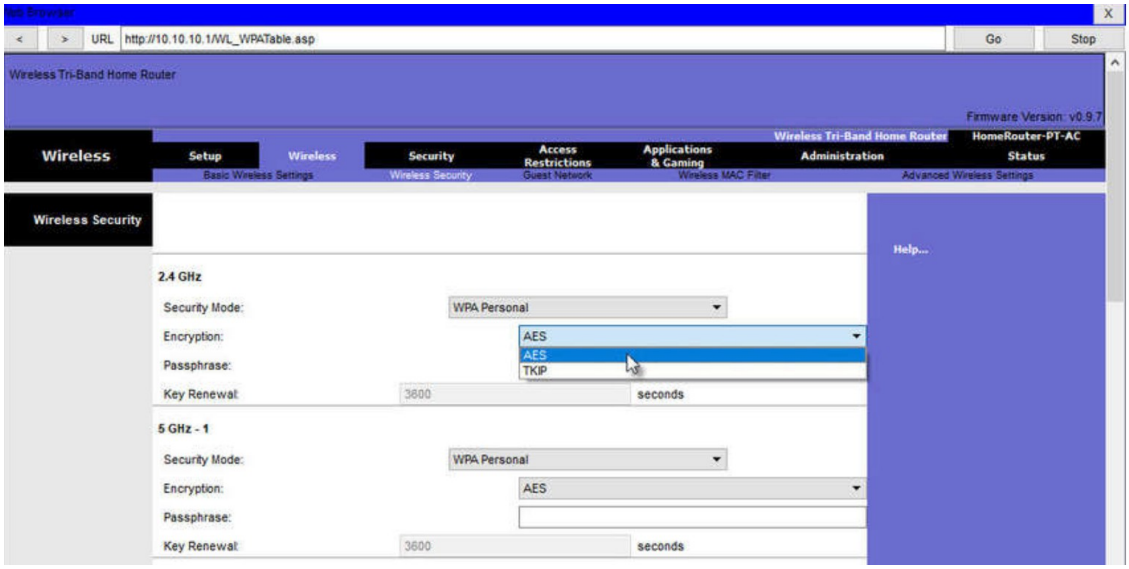
2.4GHz bandında aynı kanal ile yapılandırılan cihazlar üst üste gelebilir ve bozulmaya neden olabilir, kablosuz performansını yavaşlatabilir ve potansiyel olarak ağ bağlantılarını kesebilir. Paraziti önlemenin çözümü, kablosuz yönlendiricilerdeki çakışmayan kanalları ve birbirine yakın erişim noktaları yapılandırmaktır. Spesifik olarak, 1, 6 ve 11 numaralı kanallar çakışmamaktadır. Örnekte, kablosuz yönlendirici 6. kanalı kullanacak şekilde yapılandırılmıştır.




**5 . Güvenlik modunu yapılandırın.**

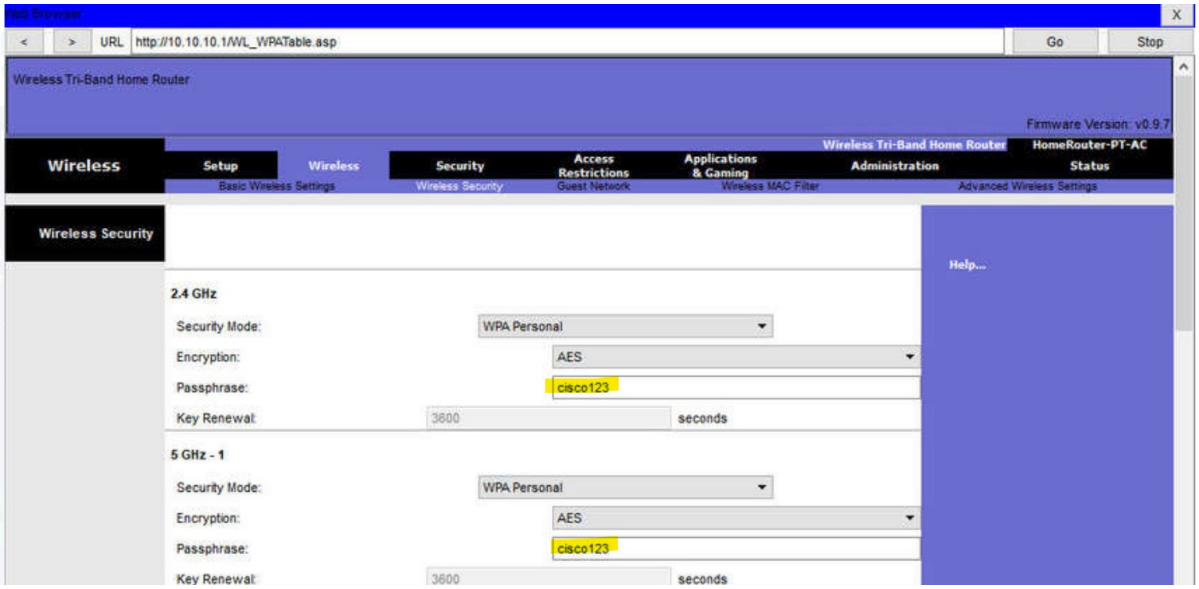
Licensed to yetkin karasungur, yetkinkrengr@gmail.com

Kutudan çıkar çıkmaz bir kablosuz yönlendiricide yapılandırılmış WLAN güvenliği olmayabilir. Örnekte, Wi-Fi Korumalı Erişim sürüm 2'nin (WPA2 Kişisel) kişisel sürümü üç WLAN'ın tümü için seçilmiştir. Gelişmiş Şifreleme Standardı (AES) şifrelemeli WPA2 şu anda en güçlü güvenlik modudur.




**6.Parolayı yapılandırın.**

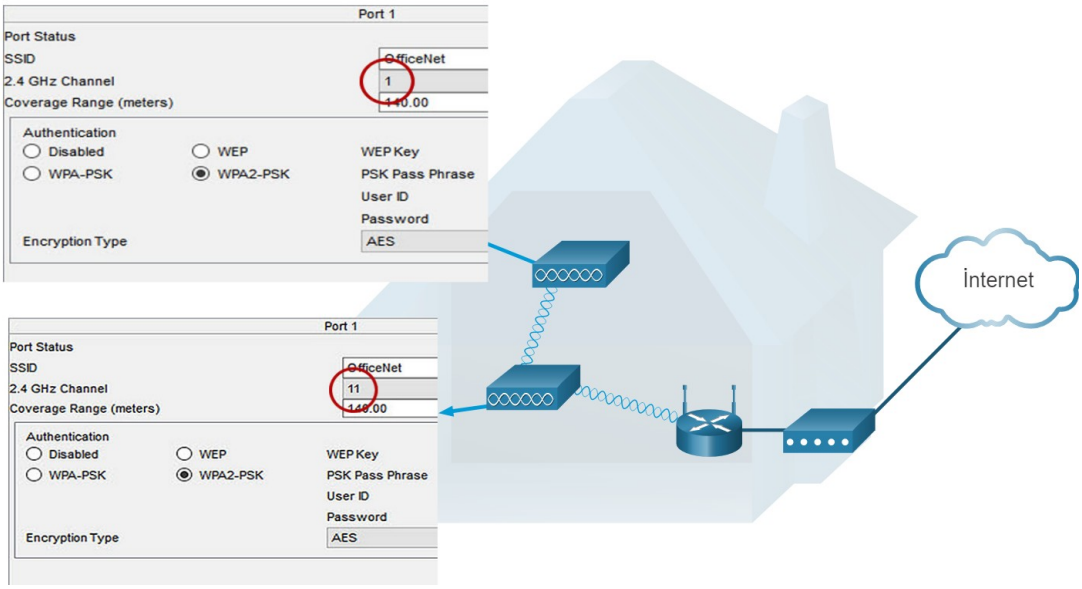
WPA2 personal, kablosuz istemcilerin kimliğini doğrulamak için bir parola kullanır. WPA2 kişisel, bir kimlik doğrulama sunucusu gerektirmediği için küçük bir ofis veya ev ortamında kullanımı daha kolaydır. Daha büyük kuruluşlar WPA2 kurumsal uygular ve kablosuz istemcilerin bir kullanıcı adı ve parola ile kimlik doğrulaması yapmasını gerektirir.




## 29.1.4.Kablosuz Ağı Yapılandırın

Küçük bir ofis veya ev ağında, bir kablosuz yönlendirici tüm istemcilere kablosuz erişim sağlamak için yeterli olabilir. Bununla birlikte, kapsama alanını iç mekanlarda yaklaşık 45 metre ve dış mekanlarda 90 metrenin ötesine genişletmek isterseniz, kablosuz erişim noktaları ekleyebilirsiniz. Şekilde kablosuz ağda gösterildiği gibi, iki erişim noktası önceki örneğimizdeki aynı WLAN ayarlarıyla yapılandırılmıştır. Erişim noktalarının kablosuz yönlendiricide daha önce yapılandırılan kanal 6 ile çakışmaması için seçilen kanalların 1 ve 11 olduğuna dikkat edin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

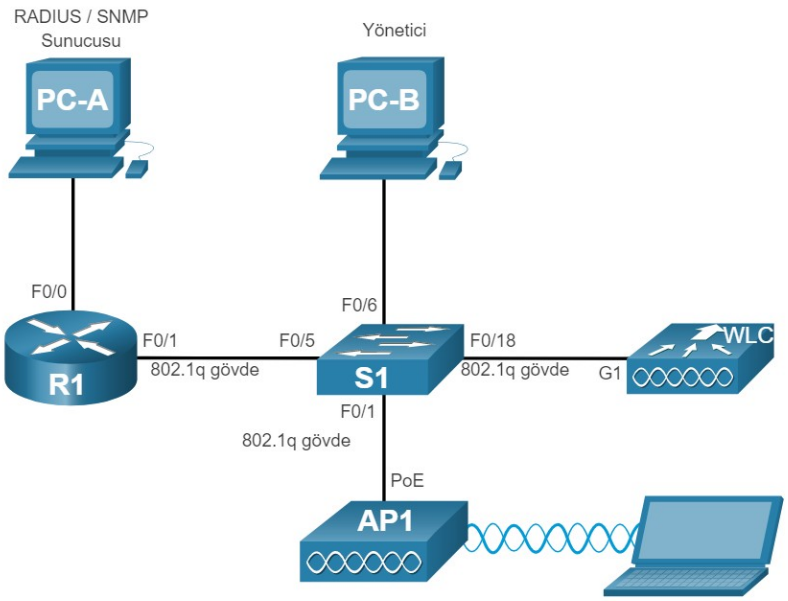



## 29.2.WLC'de WLAN Yapılandırma

### 29.2.1.WLC Topolojisi

Bu konu için kullanılan topoloji ve adresleme şeması şekilde ve tabloda gösterilmektedir. Erişim noktası (AP), özerk bir AP'nin aksine denetleyici tabanlı bir AP'dir. Denetleyici tabanlı AP'lerin ilk yapılandırma gerektirmediğini ve genellikle hafif AP'ler (LAP'ler) olarak adlandırıldığını hatırlayın. LAP'ler, bir WLAN denetleyicisi (WLC) ile iletişim kurmak için Hafif Erişim Noktası Protokolünü (LWAPP) kullanır. Denetleyici tabanlı AP'ler, ağda birçok AP'nin gerekli olduğu durumlarda kullanışlıdır. Daha fazla AP eklendikçe, her AP otomatik olarak yapılandırılır ve WLC tarafından yönetilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




AP, PoE'dir, yani anahtara bağlı Ethernet kablosundan güç alır.

| cihaz | Arayüz | IP adresi | Alt Ağ Maskesi |
|---|---|---|---|
| R1 | F0 / 0 | 172.16.1.1 | 255.255.255.0 |
| R1 | F0 / 1.1 | 192.168.200.1 | 255.255.255.0 |
| S1 | VLAN 1 | DHCP | |
| WLC | Yönetim | 192.168.200.254 | 255.255.255.0 |
| AP1 | Kablolu 0 | 192.168.200.3 | 255.255.255.0 |
| PC-A | NIC | 172.16.1.254 | 255.255.255.0 |
| PC-B | NIC | DHCP | |
| Kablosuz Dizüstü Bilgisayar | NIC | DHCP | |

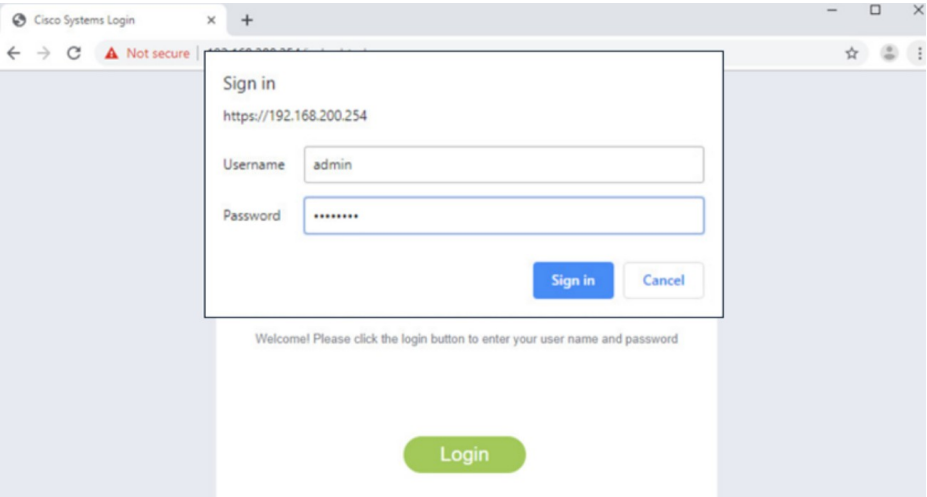
## 29.2.2.WLC'de Oturum Açma

Bir kablosuz LAN denetleyicisini (WLC) yapılandırmak, bir kablosuz yönlendiriciyi yapılandırmaktan çok da farklı değildir. En büyük fark, WLC'nin AP'leri kontrol etmesi ve çoğu bu kitabın kapsamı dışında kalan daha fazla hizmet ve yönetim yeteneği sağlamasıdır.

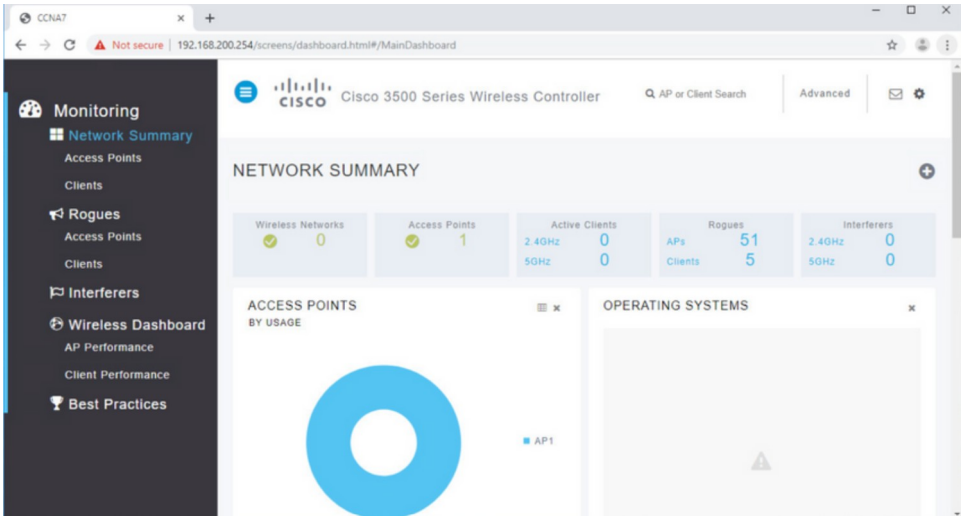
Not : Grafik kullanıcı arayüzünü (GUI) ve menüleri gösteren bu konudaki şekiller bir Cisco 3504 Kablosuz Denetleyiciden alınmıştır. Ancak, diğer WLC modelleri benzer menülere ve özelliklere sahip olacaktır.

Şekil, kullanıcının ilk kurulum sırasında yapılandırılan kimlik bilgileriyle WLC'de oturum açtığını gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

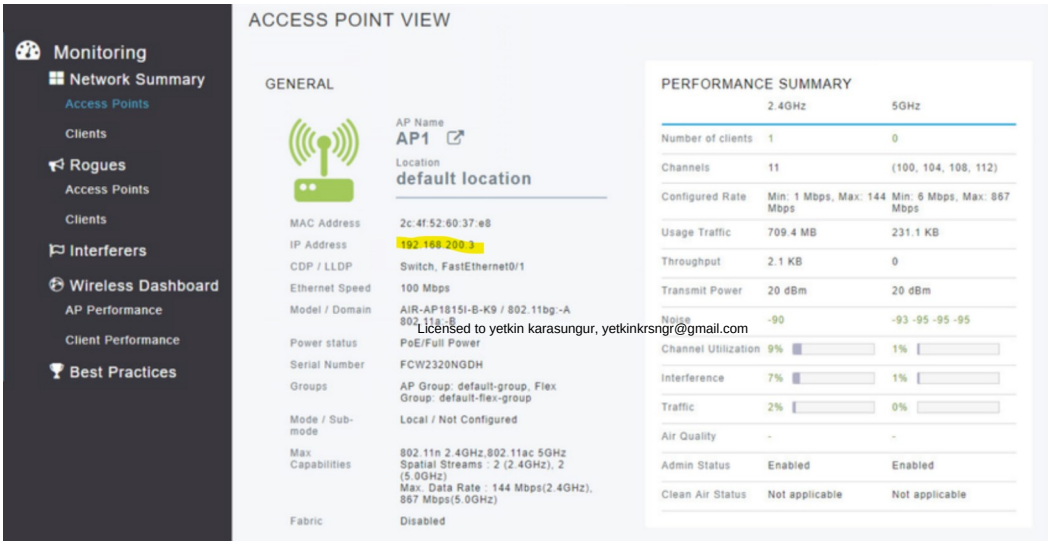



Ağ Özeti-Network Summary sayfası yapılandırılan kablosuz ağların sayısı, ilişkili erişim noktaları (AP) ve aktif istemcilere hızlı bir genel bakış sağlayan bir gösterge tablosudur. Ayrıca şekilde gösterildiği gibi, yetkisiz erişim noktalarının ve istemcilerin sayısını da görebilirsiniz.




## 29.2.3.AP Bilgilerini Görüntülemee

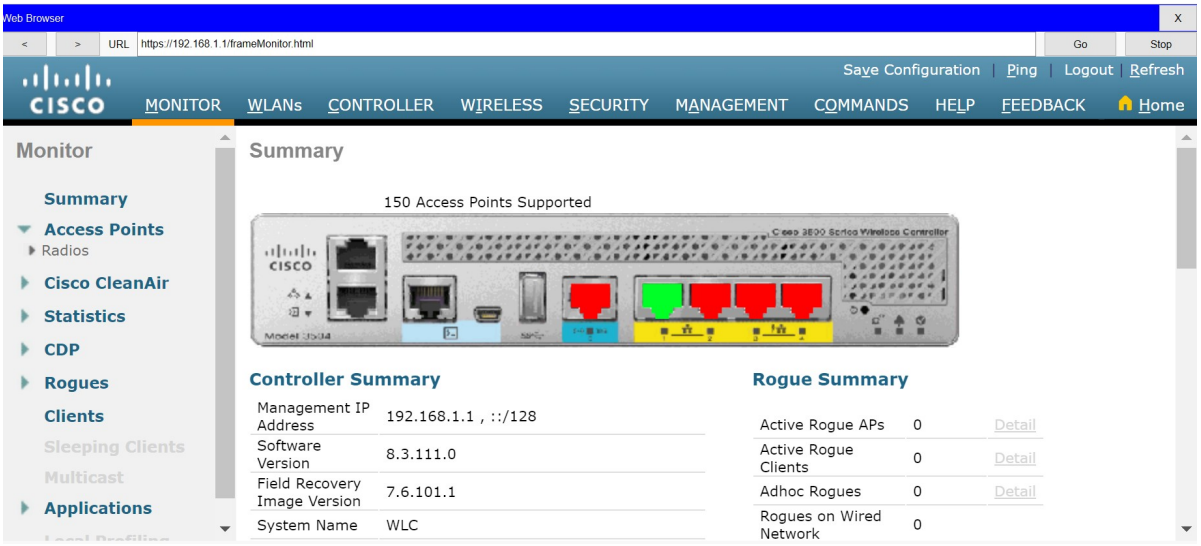
Sonraki şekilde gösterildiği gibi AP'nin sistem bilgilerinin ve performansının genel bir resmini görüntülemek için sol menüden Erişim Noktaları'na-Acess Points tıklayın . AP, 192.168.200.3 IP adresini kullanıyor. Cisco Keşif Protokolü (CDP) bu ağda etkin olduğu için, WLC, AP'nin anahtardaki FastEthernet 0/1 bağlantı noktasına bağlı olduğunu bilir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 29.2.4.Gelişmiş Ayarlar

Çoğu WLC, kullanıcıların çeşitli genel yapılandırmaları uygulamak için hızla erişebilecekleri bazı temel ayarlar ve menülerle birlikte gelir. Ancak, bir ağ yöneticisi olarak, genellikle gelişmiş ayarlara erişeceksiniz. Cisco 3504 Kablosuz Denetleyici için , şekilde gösterildiği gibi gelişmiş Özet-Summary sayfasına erişmek için sağ üst köşedeki Gelişmiş'e-Adavanced tıklayın . Buradan WLC'nin tüm özelliklerine erişebilirsiniz.




## 29.2.5.WLAN Yapılandırma

Kablosuz LAN Denetleyicilerinin bağlantı noktaları ve arabirimleri vardır. Bağlantı noktaları, kablolu ağa fiziksel bağlantılar için soketlerdir. Anahtar bağlantı noktalarına benzerler. Arayüzler sanaldır. Yazılım içinde oluşturulurlar ve VLAN arayüzlerine çok benzerler. Aslında, bir WLAN'dan gelen trafiği taşıyacak her arayüz, WLC üzerinde farklı bir VLAN olarak yapılandırılır. Cisco 3504 WLC, 150 erişim noktasını ve 4096 VLAN'ı destekleyebilir, ancak şekilde gösterildiği gibi yalnızca beş fiziksel bağlantı noktasına sahiptir. Bu, her fiziksel bağlantı noktasının birçok AP'yi ve WLAN'ı destekleyebileceği anlamına gelir. WLC'deki bağlantı noktaları, temelde, birden çok VLAN'dan birden çok AP'ye dağıtım için bir anahtara trafiği taşıyabilen ana bağlantı noktalarıdır. Her AP, birden çok WLAN'ı destekleyebilir.

**WLC'deki temel WLAN yapılandırması aşağıdaki adımları içerir:**

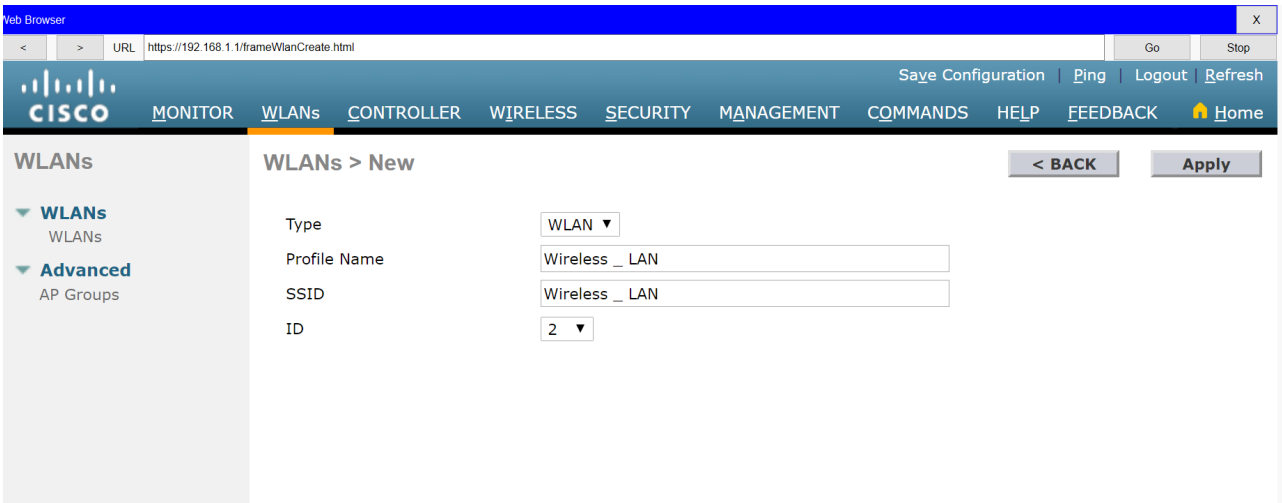
1. WLAN oluşturun
2. WLAN'ı uygulayın ve etkinleştirin
3. Arayüzü seçin
4. WLAN'ın güvenliğini sağlayın

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

5. WLAN'ın Çalışır durumda olduğunu doğrulayın
6. WLAN'ı izleyin
7. Kablosuz İstemci Bilgilerini Görüntüleyin

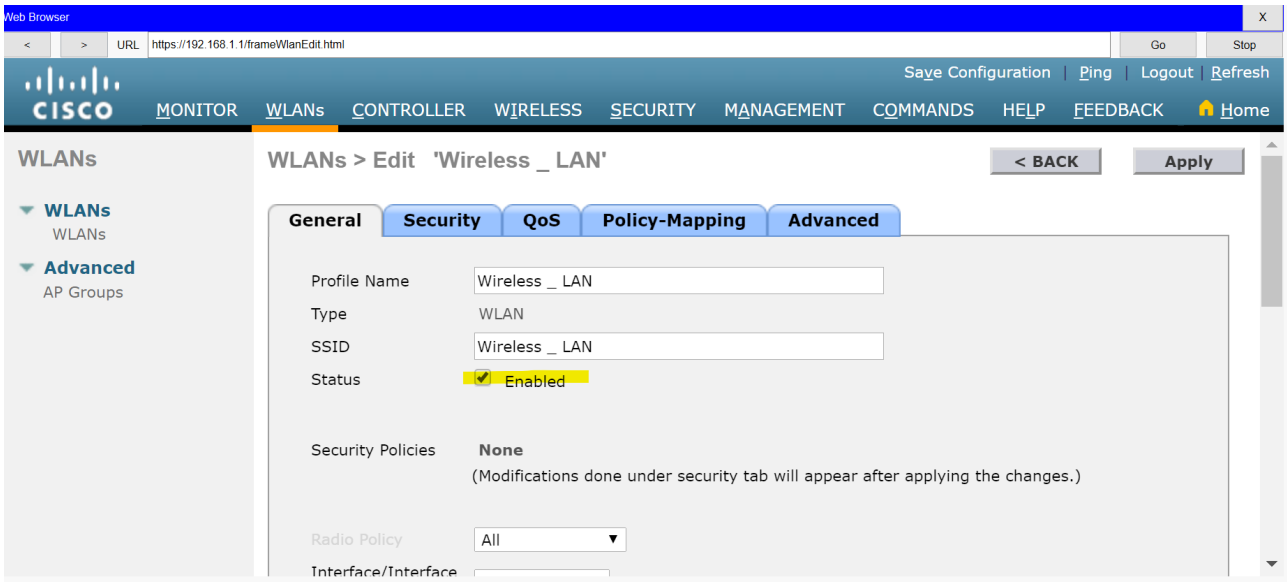
## 1 . WLAN oluşturun

Şekilde, yönetici, ad ve hizmet seti tanımlayıcısı (SSID) olarak Wireless _ LAN'ı kullanacak yeni bir WLAN oluşturuyor . Kimlik-ID, WLC'deki görüntü çıkışındaki WLAN'ı tanımlamak için kullanılan rastgele bir değerdir.




## 2.WLAN'ı uygulayın ve etkinleştirin

Uygula'ya-Apply tıkladıktan sonra , ağ yöneticisinin WLAN'ı, şekilde gösterildiği gibi kullanıcılar tarafından erişilebilmesi için etkinleştirmesi gerekir. Etkinleştir-Enabled onay kutusu, ağ yöneticisinin, kablosuz istemci erişimi için etkinleştirmeden önce WLAN için çeşitli özellikleri ve ek WLAN'ları yapılandırmasına olanak tanır. Buradan ağ yöneticisi, güvenlik, QoS, ilkeler ve diğer gelişmiş ayarlar dahil olmak üzere WLAN için çeşitli ayarları yapılandırabilir.



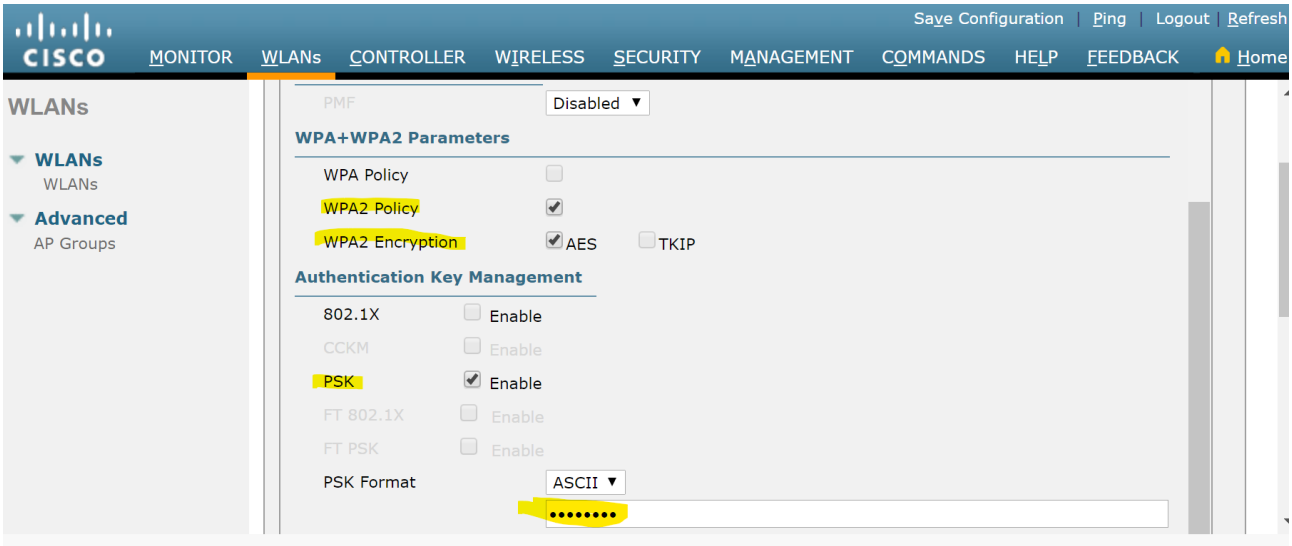

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 3 . Arayüzü seçin

Bir WLAN oluşturduğunuzda, WLAN trafiğini taşıyacak arayüzü seçmelisiniz. Sonraki şekil, WLC'de önceden oluşturulmuş bir arayüzün seçimini gösterir. Arayüzlerin nasıl oluşturulacağını daha sonra öğreneceğiz.

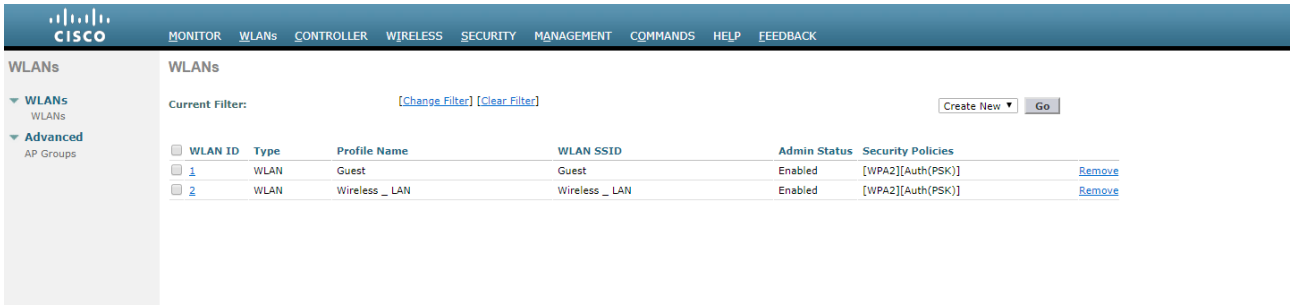
## 4 . WLAN'ın güvenliğini sağlayın

LAN güvenliğini sağlamak için mevcut tüm seçeneklere erişmek için Güvenlik-Security sekmesine tıklayın. Ağ yöneticisi, Katman 2'yi WPA2-PSK ile güvenli hale getirmek istiyor. WPA2 ve 802.1X varsayılan olarak ayarlanmıştır. Katman 2 Güvenliği-Layer 2 Security açılır kutusunda, WPA + WPA2'nin seçildiğini (gösterilmemiştir) doğrulayın . PSK'ya tıklayın ve şekilde gösterildiği gibi önceden paylaşılan anahtarı girin. Ardından Uygula'yı-Apply tıklayın . Bu, WPA2-PSK kimlik doğrulamalı WLAN'ı etkinleştirecektir. Önceden paylaşılan anahtarı bilen kablosuz istemciler artık AP ile ilişkilendirilebilir ve kimlik doğrulaması yapabilir.




## 5 . WLAN'ın Çalışır durumda olduğunu doğrulayın

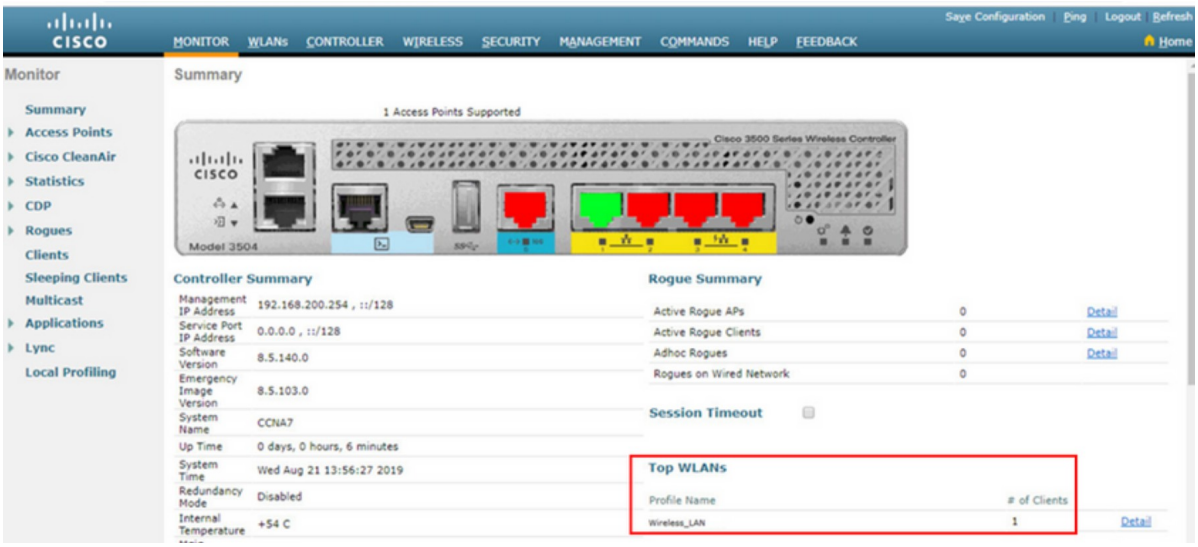
Yeni yapılandırılmış WLAN'ı görüntülemek için soldaki menüde WLAN'lara tıklayın . Şekilde, WLAN ID 1'in ad ve SSID olarak Wireless _ LAN ile yapılandırıldığını , etkinleştirildiğini ve WPA2 PSK güvenliğini kullandığını doğrulayabilirsiniz .




## 6 . WLAN'ı izleyin

Gelişmiş Özet sayfasına tekrar erişmek için üstteki Monitör sekmesine tıklayın . Burada , şekilde gösterildiği gibi , Wireless _ LAN'ın artık hizmetlerini kullanan bir istemciye sahip olduğunu görebilirsiniz .

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




**7 . Kablosuz İstemci Ayrıntılarını Görüntüleyin**

Şekilde gösterildiği gibi, WLAN'a bağlı istemciler hakkında daha fazla bilgi görüntülemek için sol menüdeki İstemciler'i-Clients tıklayın . Bir istemci AP1 aracılığıyla Wireless _ LAN'a bağlandı ve ona 192.168.5.2 IP adresi verildi. Bu topolojideki DHCP hizmetleri yönlendirici tarafından sağlanır.

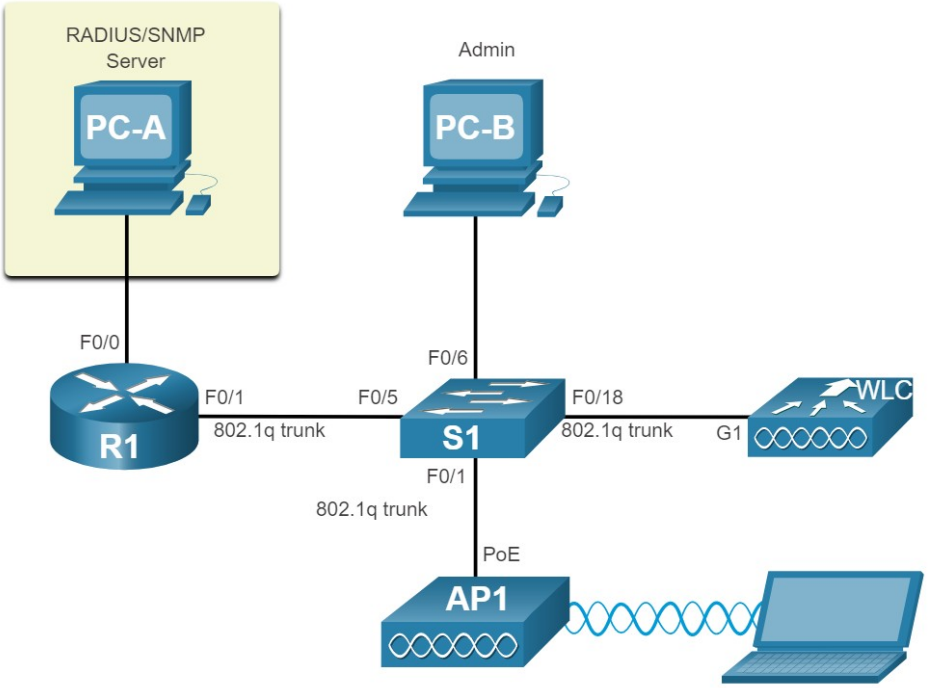
## 29.3.WLC'de WPA2 Kurumsal WLAN Yapılandırma

### 29.3.1.SNMP ve RADIUS

Şekilde, PC-A, Basit Ağ Yönetim Protokolü -Simple Network Management Protocol (SNMP) ve Uzaktan Kimlik Doğrulama Çevirmeli Kullanıcı Hizmeti- Remote Authentication Dial-In User Service(RADIUS) sunucu yazılımını çalıştırmaktadır. SNMP, ağı izlemek için kullanılır. Ağ yöneticisi, WLC'nin tuzaklar-traps adı verilen tüm SNMP günlük mesajlarını SNMP sunucusuna iletmesini ister.

Ayrıca, WLAN kullanıcı kimlik doğrulaması için, ağ yöneticisi kimlik doğrulama, yetkilendirme ve hesap oluşturma (AAA) hizmetleri için bir RADIUS sunucusu kullanmak ister. Kullanıcılar, WPA2-PSK'da olduğu gibi, kimlik doğrulaması için genel olarak bilinen önceden paylaşılan bir anahtar girmek yerine, kendi kullanıcı adlarını ve parola kimlik bilgilerini gireceklerdir. Kimlik bilgileri RADIUS sunucusu tarafından doğrulanacaktır. Bu şekilde, gerektiğinde bireysel kullanıcı erişimi izlenebilir ve denetlenebilir ve kullanıcı hesapları merkezi bir konumdan eklenebilir veya değiştirilebilir. RADIUS sunucusu, WPA2 Kurumsal kimlik doğrulaması kullanan WLAN'lar için gereklidir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

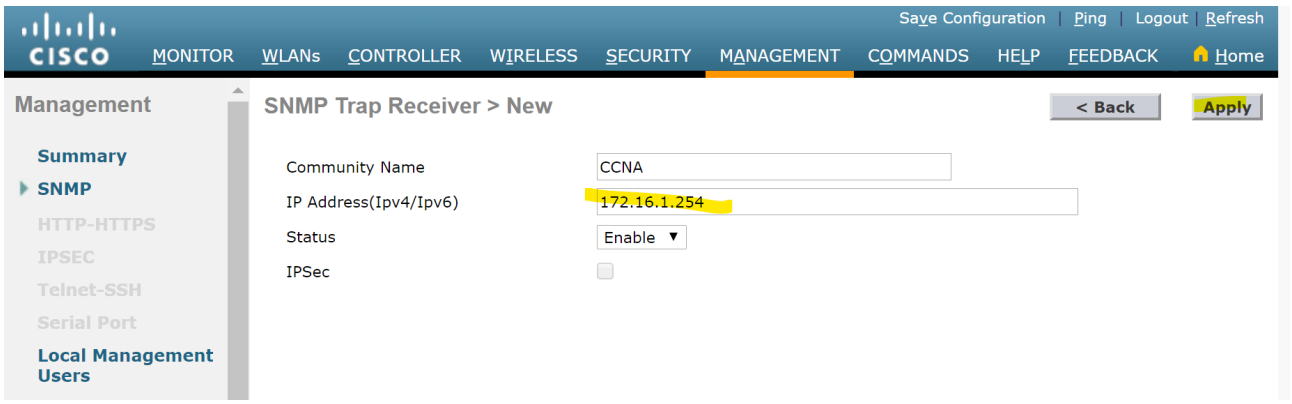



## 29.3.2.SNMP Sunucu Bilgilerini Yapılandırma

Çeşitli yönetim özelliklerine erişmek için YÖNETİM-Management sekmesine tıklayın . SNMP, sol taraftaki menünün üst kısmında listelenir. SNMP alt menüleri genişletin ve Tuzak Alıcılar-Trap receviers tıklayın . Şekilde gösterildiği gibi yeni bir SNMP tuzak alıcısı konfigüre etmek için Yeni-New ... öğesine tıklayın .

SNMP sunucusu için SNMP Topluluğu adını (Community name) ve IP adresini (IPv4 veya IPv6) girin. Uygula seçeneğine tıklayın . WLC şimdi SNMP günlük mesajlarını SNMP sunucusuna iletecektir.

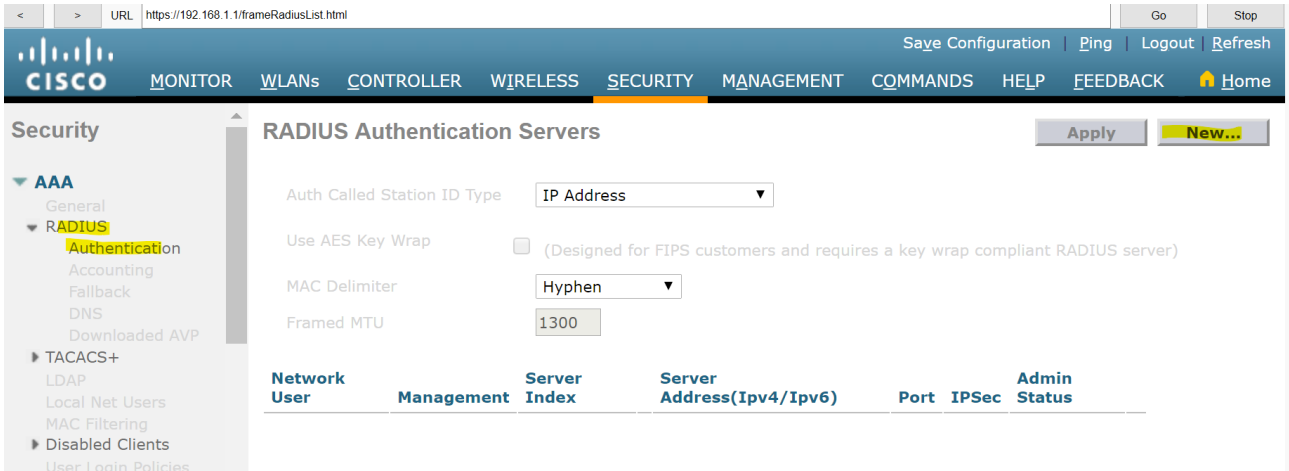
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 29.3.3.RADIUS Sunucu Bilgilerini Yapılandırma

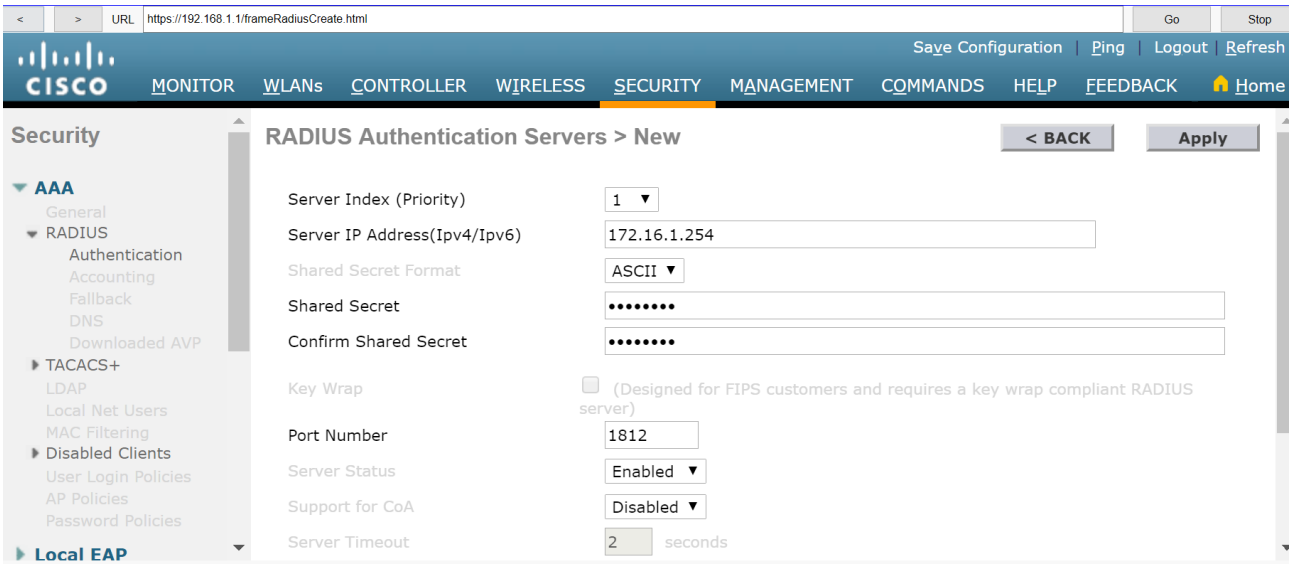
Örnek yapılandırmamızda, ağ yöneticisi WPA2 Personal veya WPA2 PSK yerine WPA2 Enterprise kullanarak bir WLAN yapılandırmak ister. Kimlik doğrulama, PC-A üzerinde çalışan RADIUS sunucusu tarafından yapılacaktır.

WLC'yi RADIUS sunucu bilgileriyle yapılandırmak için GÜVENLİK-Security sekmesi> RADIUS > Kimlik Doğrulama'ya- Authentication tıklayın . Şu anda yapılandırılmış RADIUS sunucusu yok. PC-A'yı RADIUS sunucusu olarak eklemek için Yeni-New ... öğesini tıklayın .

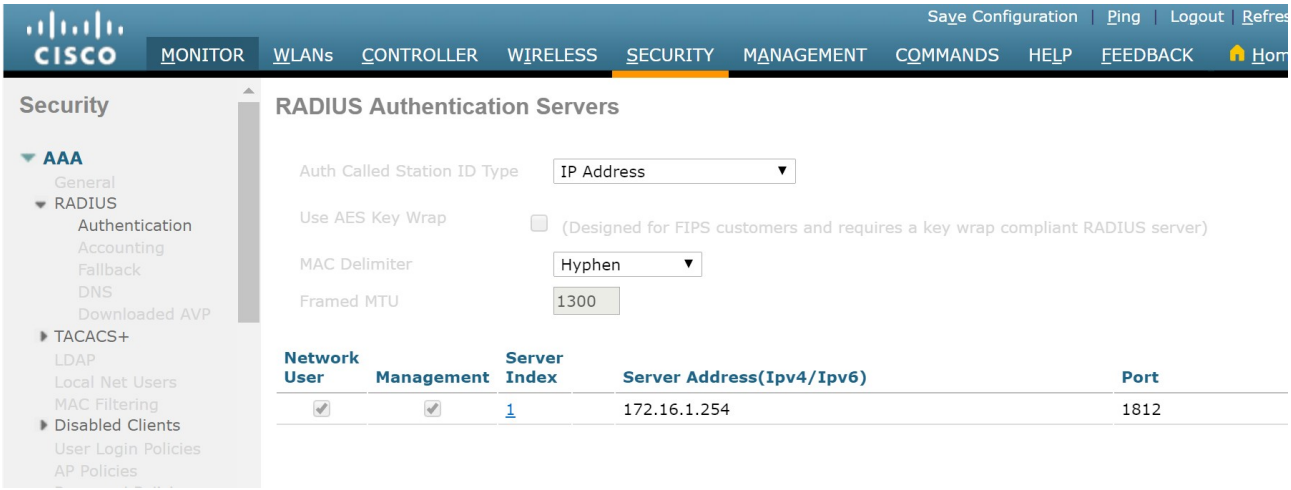



PC-A için IPv4 adresini ve paylaşılan secret key girin. Bu, WLC ve RADIUS sunucusu arasında kullanılan paroladır. Kullanıcılar için değildir. Şekilde gösterildiği gibi Uygula'yı tıklayın .

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Uygula'ya tıkladıktan sonra , yapılandırılmış RADIUS Kimlik Doğrulama Sunucuları listesi, şekilde gösterildiği gibi listelenen yeni sunucuyla yenilenir.

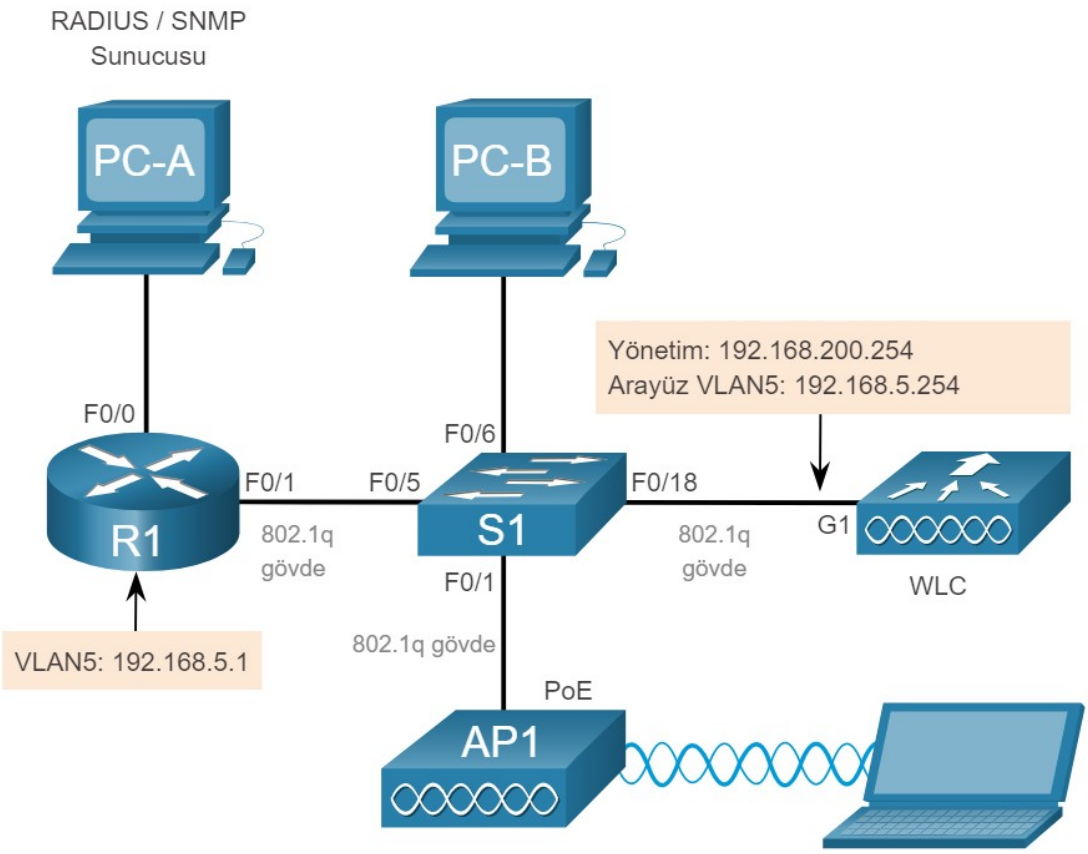



## 29.3.4.VLAN için WLC Yapılandırması

WLC'de yapılandırılan her WLAN'ın kendi sanal arayüzüne ihtiyacı vardır. WLC, veri trafiği için beş fiziksel bağlantı noktasına sahiptir. Her fiziksel bağlantı noktası, her biri kendi sanal arabiriminde bulunan birden çok WLAN'ı destekleyecek şekilde yapılandırılabilir. Yüksek bant genişliğine sahip bağlantılar oluşturmak için fiziksel bağlantı noktaları da toplanabilir.

Ağ yöneticisi, yeni WLAN'ın VLAN 5 arabirimini ve 192.168.5.0/24 ağını kullanacağına karar verdi. R1, topolojide gösterildiği gibi VLAN 5 için yapılandırılmış ve etkin bir alt arayüze sahiptir ve ip arayüzü kısa çıktısını gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            172.16.1.1      YES manual up                    up
FastEthernet0/1            unassigned      YES unset  up                    up
FastEthernet0/1.1          192.168.200.1   YES manual up                    up
FastEthernet0/1.5          192.168.5.254   YES manual up                    up
(output omitted)
R1#
```

## 29.3.5.Yeni Bir Arayüz Yapılandırma

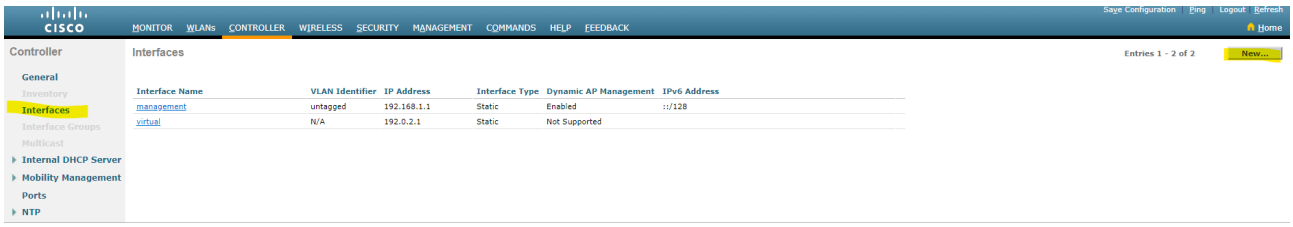
WLC'deki VLAN arayüz yapılandırması aşağıdaki adımları içerir:

1. Yeni bir arayüz oluşturun.
2. VLAN adını ve kimliğini yapılandırın.
3. Bağlantı noktasını ve arayüz adresini yapılandırın.
4. DHCP sunucusu adresini yapılandırın.
5. Uygula ve Onayla.
6. Arayüzleri Doğrulayın.

### 1 . Yeni bir arayüz oluşturun.

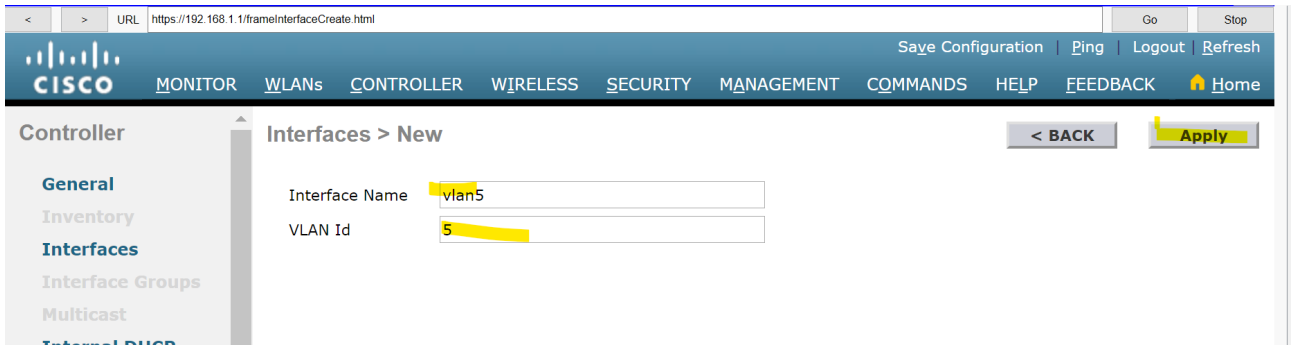
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yeni bir arayüz eklemek için , şekilde gösterildiği gibi DENETLEYİCİ-Controller> Arayüzler-Interfaces> Yeni-New ... öğesine tıklayın .



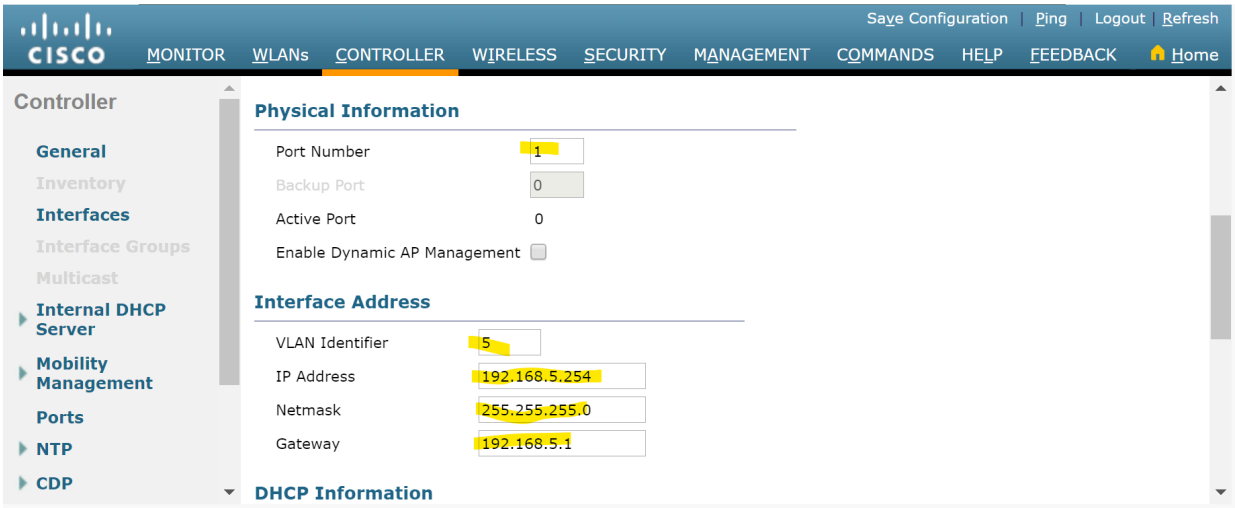

## 2 . VLAN adını ve kimliğini yapılandırın.

Şekilde, ağ yöneticisi arayüz adını vlan5 ve VLAN kimliğini 5 olarak yapılandırır . Uygula'ya tıklamak yeni arayüzü oluşturacaktır.




## 3 . Bağlantı noktasını ve arayüz adresini yapılandırın.

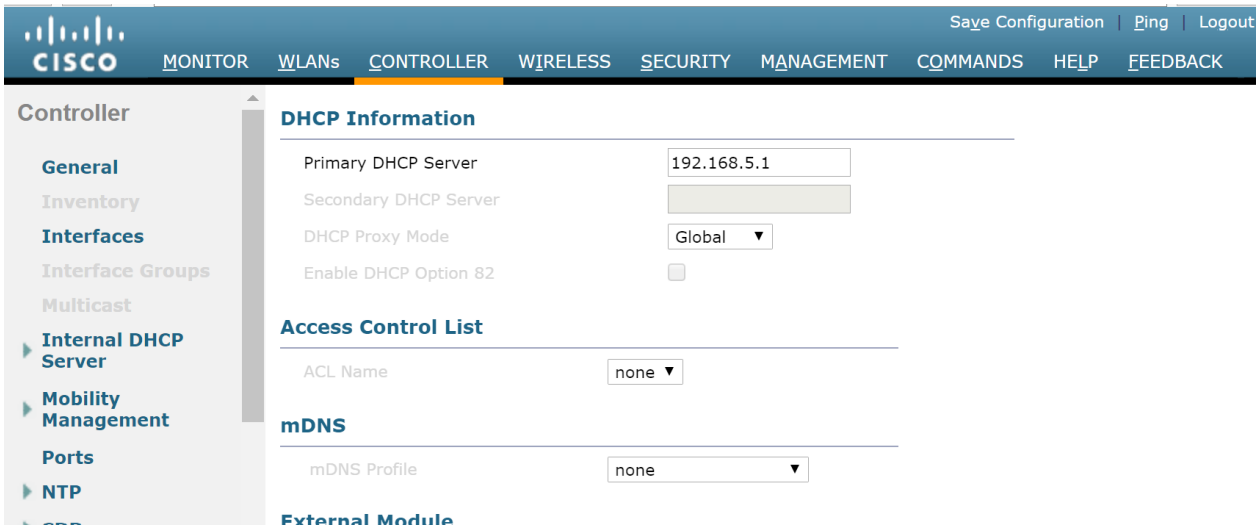
Düzenleme-Edit ile arayüzün fiziksel port numarasını yapılandırın. Topolojideki G1, WLC'deki Bağlantı Noktası Numarası 1'dir. Ardından VLAN 5 arayüz adreslemesini yapılandırın. Şekilde, VLAN 5'e 192.168.5.254/24 IPv4 adresi atanmıştır. R1, IPv4 adres 192.168.5.1'deki varsayılan ağ geçididir.




## 4. DHCP sunucu adresini yapılandırın.

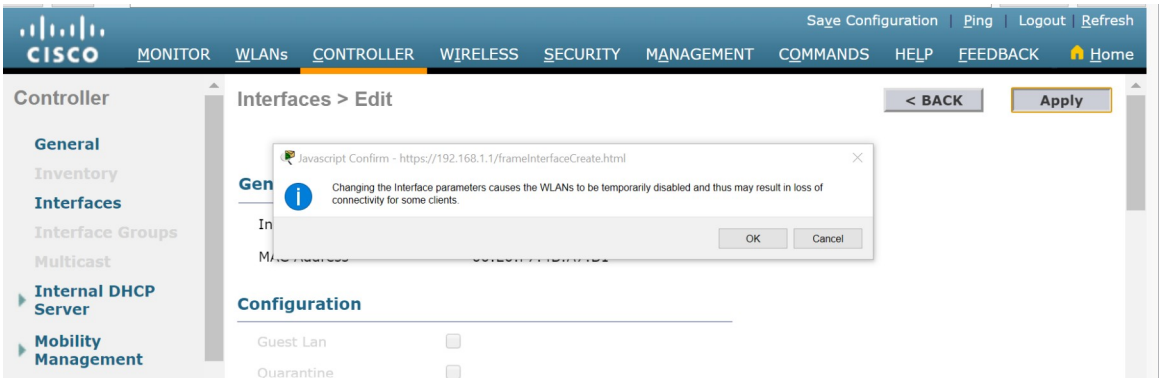
Daha büyük kuruluşlarda, WLC'ler DHCP mesajlarını özel bir DHCP sunucusuna iletecek şekilde yapılandırılacaktır. Birincil DHCP sunucusunu şekilde gösterildiği gibi IPv4 adresi 192.168.5.1 olarak yapılandırmak için sayfayı aşağı kaydırın. Bu, varsayılan ağ geçidi yönlendirici adresidir. Yönlendirici, WLAN ağı için bir DHCP havuzuyla yapılandırılmıştır. Ana bilgisayarlar, VLAN 5 arayüzüyle ilişkili WLAN'a katılırken, bu havuzdan adresleme bilgilerini alacaklar.

Licensed to yetkin karasunğur, yetkinkrsngr@gmail.com




## 5 . Uygula ve Onayla.

Sayfayı yukarı kaydırın ve şekilde gösterildiği gibi Uygula'yı tıklayın . Uyarı mesajı için Tamam'a tıklayın .




## 6 . Arayüzleri Doğrulayın.

Arayüzler'i (Interfaces) tıklayın . Yeni vlan5 arayüzü, şekilde gösterildiği gibi artık IPv4 adresiyle birlikte arayüzler listesinde gösterilmektedir.

## 29.3.6.DHCP Kapsamı (Scope) Yapılandırma

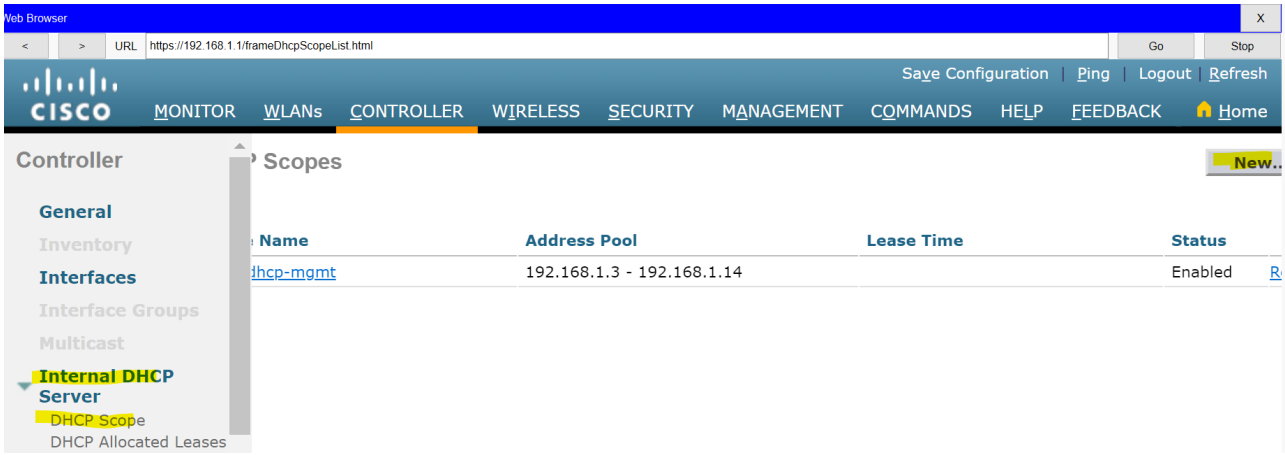
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

DHCP kapsam yapılandırması aşağıdaki adımları içerir:

1. Yeni bir DHCP kapsamı oluşturun.
2. DHCP kapsamını adlandırın.
3. Yeni DHCP kapsamını doğrulayın.
4. Yeni DHCP kapsamını yapılandırın ve etkinleştirin.
5. Etkin DHCP kapsamını doğrulayın

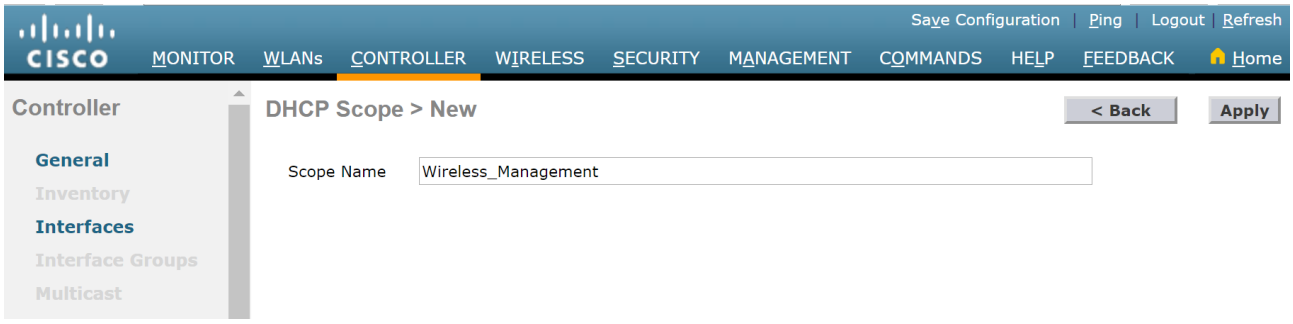
**1 . Yeni bir DHCP kapsamı oluşturun.**

Bir DHCP kapsamı, yönlendiricideki DHCP havuzuna çok benzer. DHCP istemcilerine atanacak bir adres havuzu, DNS sunucusu bilgileri, kiralama süreleri ve daha fazlasını içeren çeşitli bilgileri içerebilir. Yeni bir DHCP kapsamını yapılandırmak için , şekilde gösterildiği gibi Dahili DHCP Sunucusu> DHCP Kapsamı> Yeni ... (Internal DHCP Server > DHCP Scope > New... )öğesine tıklayın .




**2 . DHCP kapsamını adlandırın.**

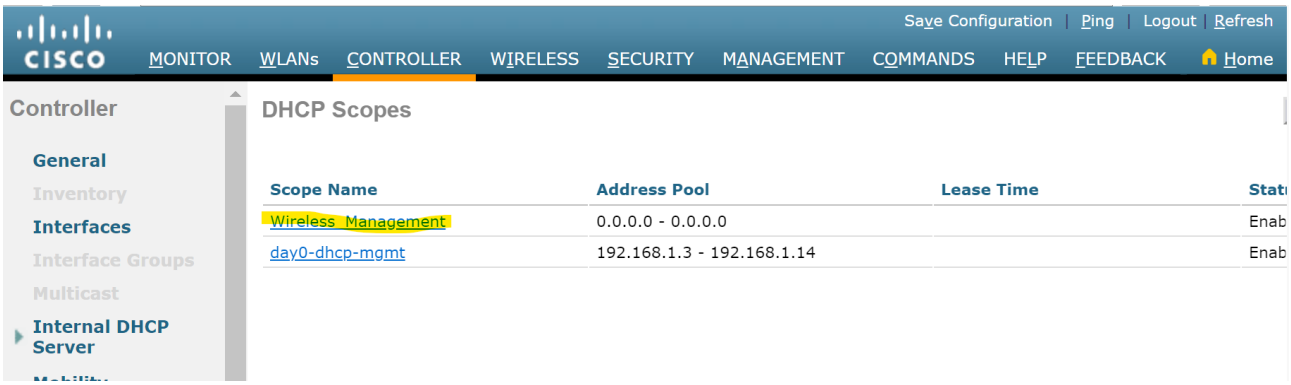
Sonraki ekranda kapsamı adlandırın. Bu kapsam kablosuz yönetim ağına uygulanacağından, ağ yöneticisi Kapsam Adı olarak Kablosuz _ Yönetimini (Wireless_Management) kullanır ve Uygula'yı tıklatır .




**3 . Yeni DHCP kapsamını doğrulayın.**

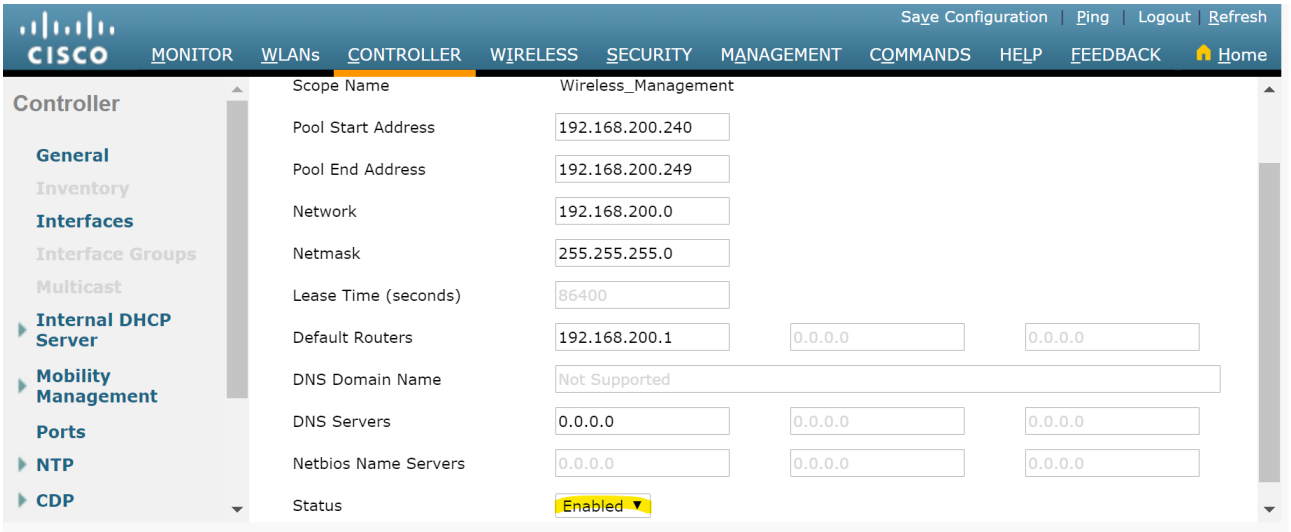
DHCP Kapsamları sayfasına dönersiniz ve kapsamın yapılandırılmaya hazır olduğunu doğrulayabilirsiniz. DHCP kapsamını yapılandırmak için yeni Kapsam Adına tıklayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 4 . Yeni DHCP kapsamını yapılandırın ve etkinleştirin.

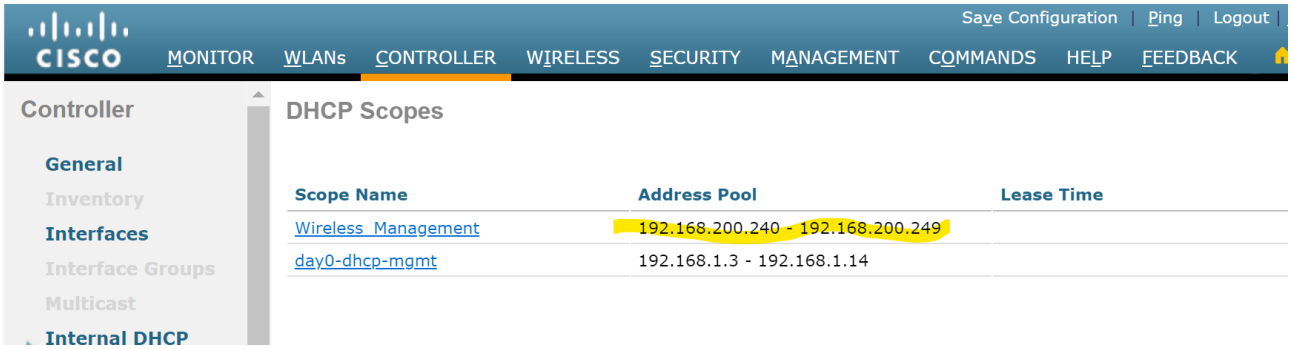
Kablosuz _ Yönetim (Wireless_Management) kapsamının Düzenle ekranında , 192.168.200.0/24 ağı için .240 ile başlayan ve .249 ile biten bir adres havuzu yapılandırın. Ağ adresi ve alt ağ maskesi yapılandırılmıştır. Varsayılan yönlendirici IPv4 adresi, 192.168.200.1'deki R1 için alt arabirim olan yapılandırılmıştır. Bu örnek için, kapsamın geri kalanı değişmeden bırakılmıştır. Ağ yöneticisi , Durum (Status) açılır listesinden Etkin'i (Enable) seçer ve Uygula'yı tıklar .




## 5 . DHCP etkinleştirme kapsamını doğrulayın

Ağ yöneticisi, DHCP Kapsamları sayfasına döndürülür ve kapsamın yeni bir WLAN'a tahsis edilmeye hazır olduğunu doğrulayabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 29.3.7.WPA2 Kurumsal WLAN'ı Yapılandırma

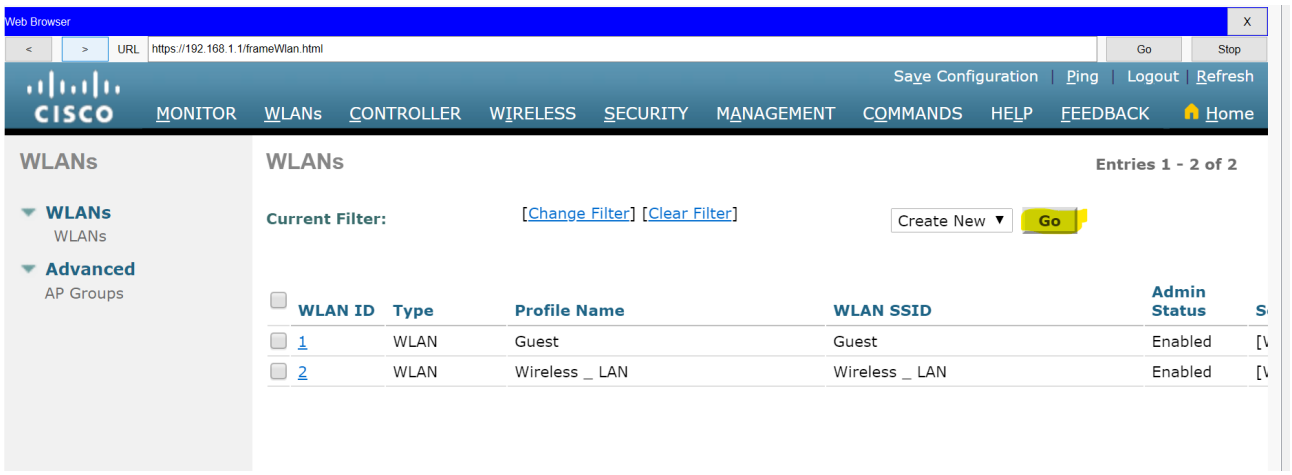
Varsayılan olarak, WLC'de yeni oluşturulan tüm WLAN'lar Gelişmiş Şifreleme Sistemi (AES) ile WPA2 kullanacaktır. 802.1X, RADIUS sunucusuyla iletişim kurmak için kullanılan varsayılan anahtar yönetimi protokolüdür. Ağ yöneticisi, WLC'yi PC-A üzerinde çalışan RADIUS sunucusunun IPv4 adresiyle zaten yapılandırdığından, yapılması gereken tek yapılandırma, arayüz vlan5'i kullanmak için yeni bir WLAN oluşturmaktır .

WLC'de yeni bir WLAN'ın yapılandırılması aşağıdaki adımları içerir:

1. Yeni bir WLAN oluşturun.
2. WLAN adını ve SSID'yi yapılandırın.
3. VLAN5 için WLAN'ı etkinleştirin.
4. AES ve 802.1X varsayılanlarını doğrulayın.
5. RADIUS sunucusunu kullanmak için WLAN güvenliğini yapılandırın.
6. Yeni WLAN'ın kullanılabilir olduğunu doğrulayın.

### 1 . Yeni bir WLAN oluşturun.

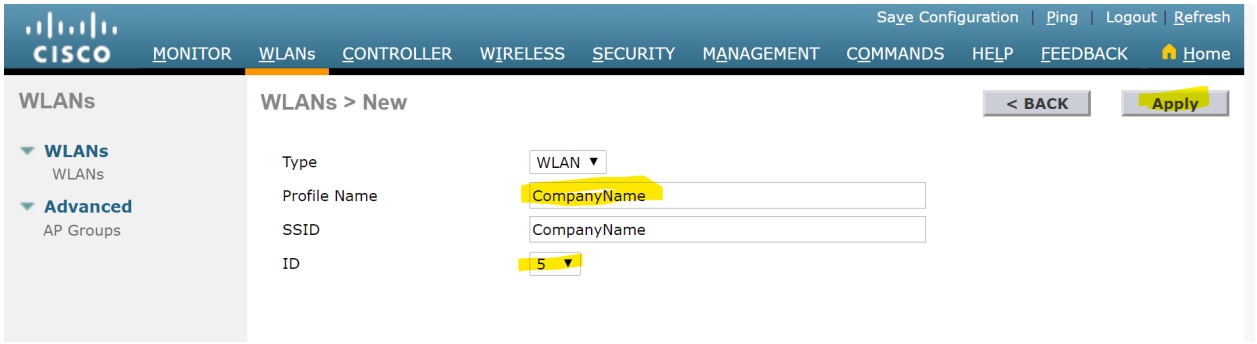
Şekilde gösterildiği gibi , WLAN'lar sekmesine ve ardından yeni bir WLAN oluşturmak için Git'e (Go) tıklayın .




### 2 . WLAN adını ve SSID'yi yapılandırın.

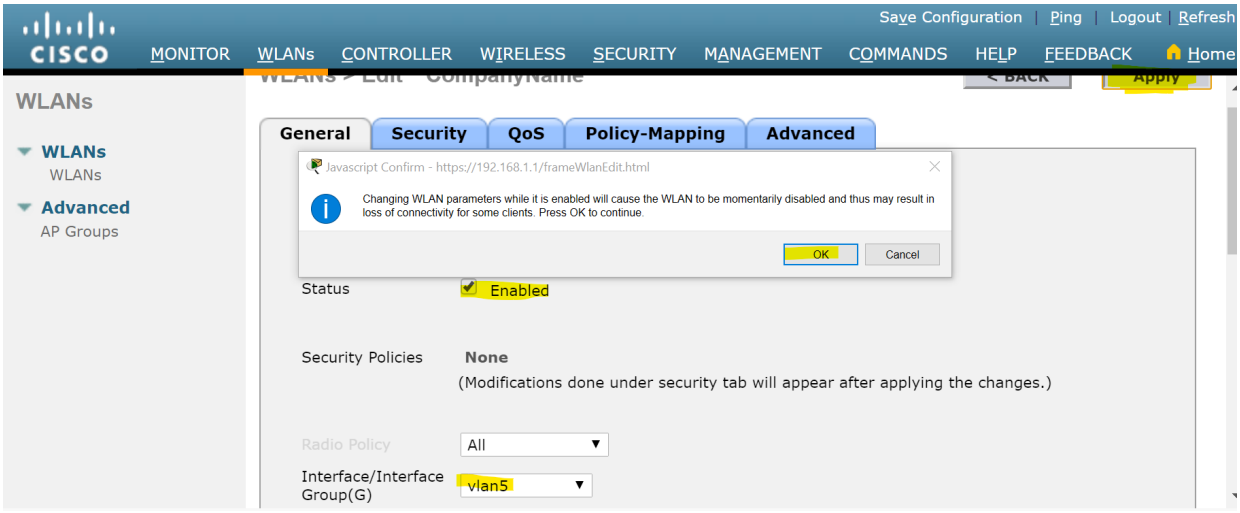
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Profil adını ve SSID'yi girin. Önceden yapılandırılmış olan VLAN ile tutarlı olmak için 5'i kimlik olarak seçin . Bununla birlikte, mevcut herhangi bir değer kullanılabilir. Yeni WLAN'ı şekilde gösterildiği gibi oluşturmak için Uygula'ya tıklayın .




### 3 . VLAN5 için WLAN'ı etkinleştirin .

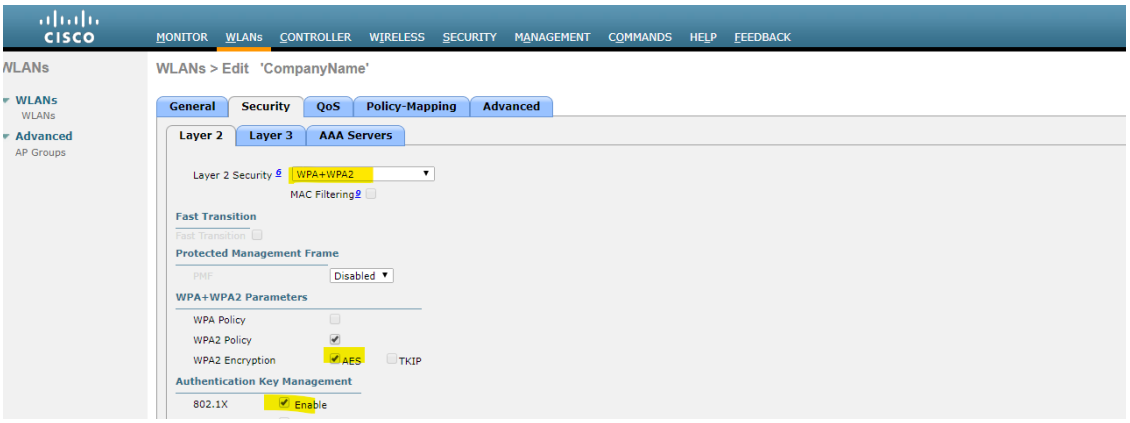
WLAN oluşturulur, ancak yine de etkinleştirilmesi ve doğru VLAN arayüzüyle ilişkilendirilmesi gerekir. Durumu Etkin olarak değiştirin ve Arayüz / Arayüz Grubu (G) açılır listesinden vlan5'i seçin. Şekilde gösterildiği gibi açılan mesajı kabul etmek için Uygula'ya tıklayın ve Tamam'a tıklayın.




### 4 . AES ve 802.1X varsayılanlarını doğrulayın.

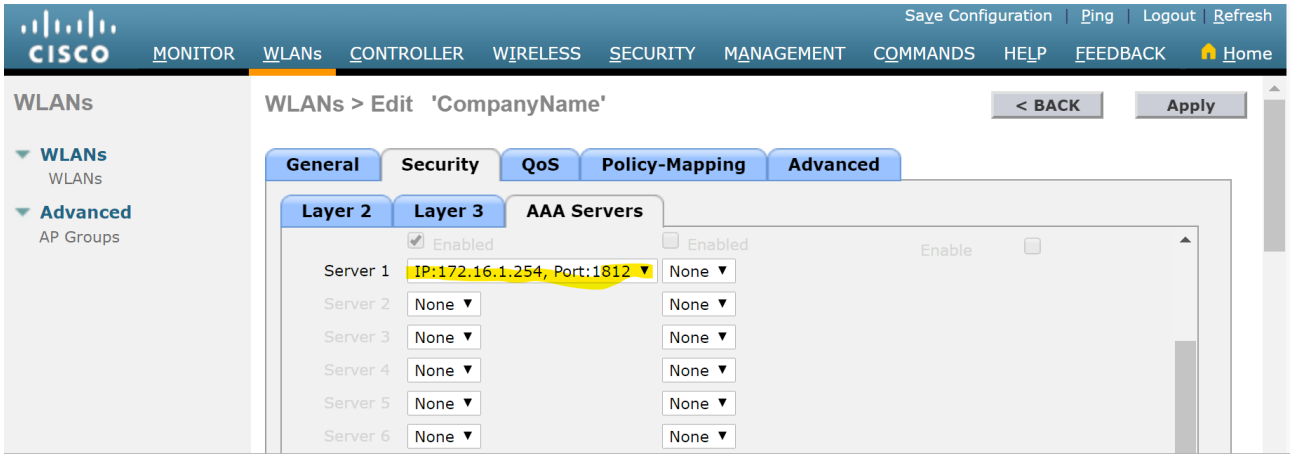
Yeni WLAN için varsayılan güvenlik yapılandırmasını görüntülemek için Güvenlik sekmesine tıklayın . WLAN, AES şifrelemeli WPA2 güvenliğini kullanacaktır. Kimlik doğrulama trafiği, WLC ve RADIUS sunucusu arasında 802.1X tarafından işlenir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



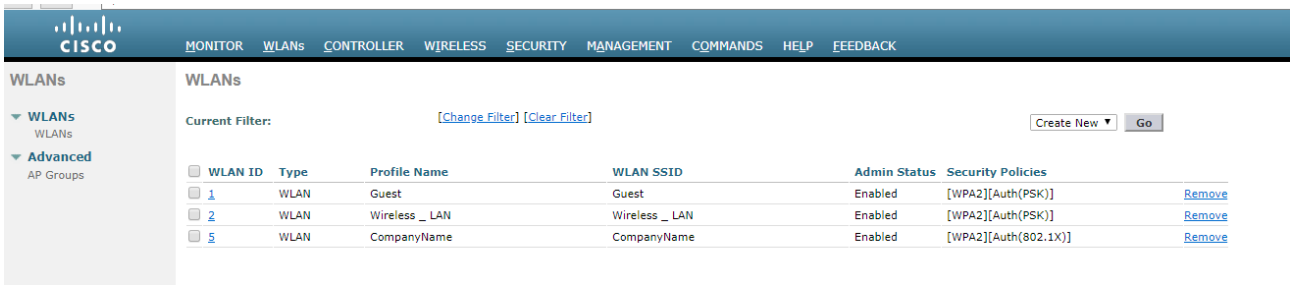

## 5 . RADIUS sunucusunu yapılandırın.

Şimdi, bu WLAN için kullanıcıların kimliklerini doğrulamak için kullanılacak RADIUS sunucusunu seçmemiz gerekiyor. AAA Sunucular sekmesine tıklayın. Açılır kutuda, daha önce WLC'de yapılandırılmış olan RADIUS sunucusunu seçin. Değişikliklerinizi uygulayın.




## 6 . Yeni WLAN'ın mevcut olduğunu doğrulayın.

Yeni WLAN'ın listelendiğini ve etkinleştirildiğini doğrulamak için, Geri'ye veya soldaki WLAN'lar alt menüsüne tıklayın . Hem Wireless _ LAN WLAN hem de CompanyName WLAN listelenir. Şekilde, her ikisinin de etkinleştirildiğine dikkat edin. Kablosuz _ LAN , PSK kimlik doğrulamalı WPA2 kullanıyor. CompanyNam e, 802.1X kimlik doğrulaması ile WPA2 güvenliğini kullanıyor.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 30.Bölüm: Yönlendirme Prensipleri

## 30.1.Yol Belirleme (Path Determination)

### 30.1.1.Yönlendiricinin İki Fonksiyonu

Bir yönlendirici paketi herhangi bir yere iletmeden önce, paketin alacağı en iyi yolu belirlemesi gerekir. Bu konu, yönlendiricilerin bu belirlemeyi nasıl yaptığını açıklamaktadır.

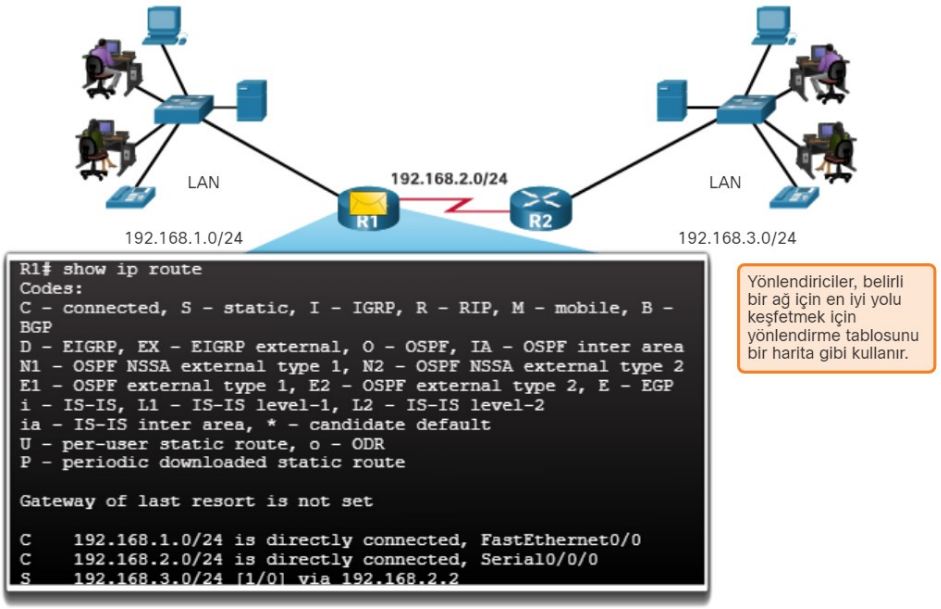
Ethernet anahtarları, uç cihazları ve diğer Ethernet anahtarları gibi diğer aracı cihazları aynı ağa bağlamak için kullanılır. Bir yönlendirici birden çok ağı birbirine bağlar, bu da her biri farklı bir IP ağına ait olan birden çok arabirime sahip olduğu anlamına gelir.

Bir yönlendirici, bir arabirimde bir IP paketi aldığında, paketi hedefe iletmek için hangi arabirimin kullanılacağını belirler. Bu, yönlendirme olarak bilinir. Yönlendiricinin paketi iletmek için kullandığı arabirim nihai hedef olabilir veya hedef ağa ulaşmak için kullanılan başka bir yönlendiriciye bağlı bir ağ olabilir. Bir yönlendiricinin bağlandığı her ağ, tipik olarak ayrı bir arayüz gerektirir, ancak bu her zaman geçerli olmayabilir.

Bir yönlendiricinin birincil işlevleri, yönlendirme tablosundaki bilgilere göre paketleri iletmek için en iyi yolu belirlemek ve paketleri hedeflerine iletmektir.

### 30.1.2.Yönlendirici İşlevleri Örneği

Yönlendirici, bir paketi iletmek için hangi yolun (yolun) kullanılacağını belirlemek için kendi IP yönlendirme tablosunu kullanır. Kaynak PC'den hedef PC'ye bir paketi takip etmek için şekilde bakınız. Hem R1 hem de R2'nin önce en iyi yolu belirlemek ve ardından paketi iletmek için ilgili IP yönlendirme tablolarını nasıl kullandığını görebilirsiniz.




### 30.1.3.En İyi Yol En Uzun Eşleşmeye (Prefix Match) Eşittir

**Yönlendirici, yönlendirme tablosundaki en iyi yolu belirlemeli derken ne kastedilmektedir? Yönlendirme tablosundaki en iyi yol, en uzun eşleşme olarak da bilinir. En uzun eşleşme, yönlendiricinin, paketin hedef IP adresi ile yönlendirme tablosundaki bir yönlendirme girişi arasında bir eşleşme bulmak için kullandığı bir işlemdir.**

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yönlendirme tablosu, bir ön ek (ağ adresi) ve önek uzunluğundan oluşan yol girişlerini içerir. Bir paketin hedef IP adresi ile yönlendirme tablosundaki bir yol arasında bir eşleşme olması için, paketin IP adresi ile yönlendirme tablosundaki yol arasında minimum sayıda en sol bit eşleşmelidir. Yönlendirme tablosundaki yolun önek uzunluğu, eşleşmesi gereken minimum uzak-sol bit sayısını belirlemek için kullanılır. Bir IP paketinin önek uzunluğunu değil, yalnızca hedef IP adresini içerdiğini unutmayın.

En uzun eşleşme, yönlendirme tablosundaki, paketin hedef IP adresi ile en fazla sayıda en çok sol eşleşen biti içeren yoldur. En fazla eşdeğer uzak-sol bit sayısına sahip rota veya en uzun eşleşme her zaman tercih edilen rotadır.

Not : Önek uzunluğu terimi, hem IPv4 hem de IPv6 adreslerinin ağ bölümünü ifade etmek için kullanılacaktır.

**IPv4 Adresi En Uzun Eşleşme Örneği**

Tabloda, bir IPv4 paketi 172.16.0.10 hedef IPv4 adresine sahiptir. Yönlendiricinin IPv4 yönlendirme tablosunda bu paketle eşleşen üç yol girişi vardır: 172.16.0.0/12, 172.16.0.0/18 ve 172.16.0.0/26. Üç yoldan 172.16.0.0/26 en uzun eşleşmeye sahiptir ve paketi iletmek için seçilir. Unutmayın, bu yollardan herhangi birinin bir eşleşme olarak kabul edilmesi için en azından yolun alt ağ maskesi tarafından belirtilen eşleşen bit sayısı olması gerekir.

| Hedef IPv4 Adresi | | İkili Adres |
|---|---|---|
| 172.16.0.10 | | **10101100.00010000.00000000.00** 001010 |
| **Rota Girişi** | **Önek / Önek Uzunluğu** | **İkili Adres** |
| 1 | 172.16.0.0 **/ 12** | **10101100.0001** 0000.00000000.00001010 |
| 2 | 172.16.0.0 **/ 18** | **10101100.00010000.00** 000000.00001010 |
| 3 | 172.16.0.0 **/ 26** | **10101100.00010000.00000000.00** 001010 |

**IPv6 Adresi En Uzun Eşleşme Örneği**

Tabloda, bir IPv6 paketinin hedef IPv6 adresi 2001: db8: c000 :: 99 vardır. Bu örnek, üç yol girişini gösterir, ancak bunlardan yalnızca ikisi geçerli bir eşleşmedir ve bunlardan biri en uzun eşleşmedir. İlk iki yol girişi, önek uzunluğu ile belirtildiği gibi gerekli sayıda eşleşen bitlere sahip ön ek uzunluklarına sahiptir. Önek uzunluğu / 40 olan ilk yol girişi, IPv6 adresindeki 40 en soldaki bit ile eşleşir. İkinci yol girişinin önek uzunluğu / 48'dir ve 48 bitin tümü hedef IPv6 adresiyle eşleşir ve en uzun eşleşmedir. Üçüncü yol girişi, / 64 öneki 64 eşleşen bit gerektirdiğinden bir eşleşme değildir. 2001: db8: c000: 5555 :: / 64 ön ekinin eşleşmesi için, ilk 64 bit paketin hedef IPv6 adresi olmalıdır. Yalnızca ilk 48 bit eşleşir, bu nedenle bu yol girişi bir eşleşme olarak kabul edilmez.

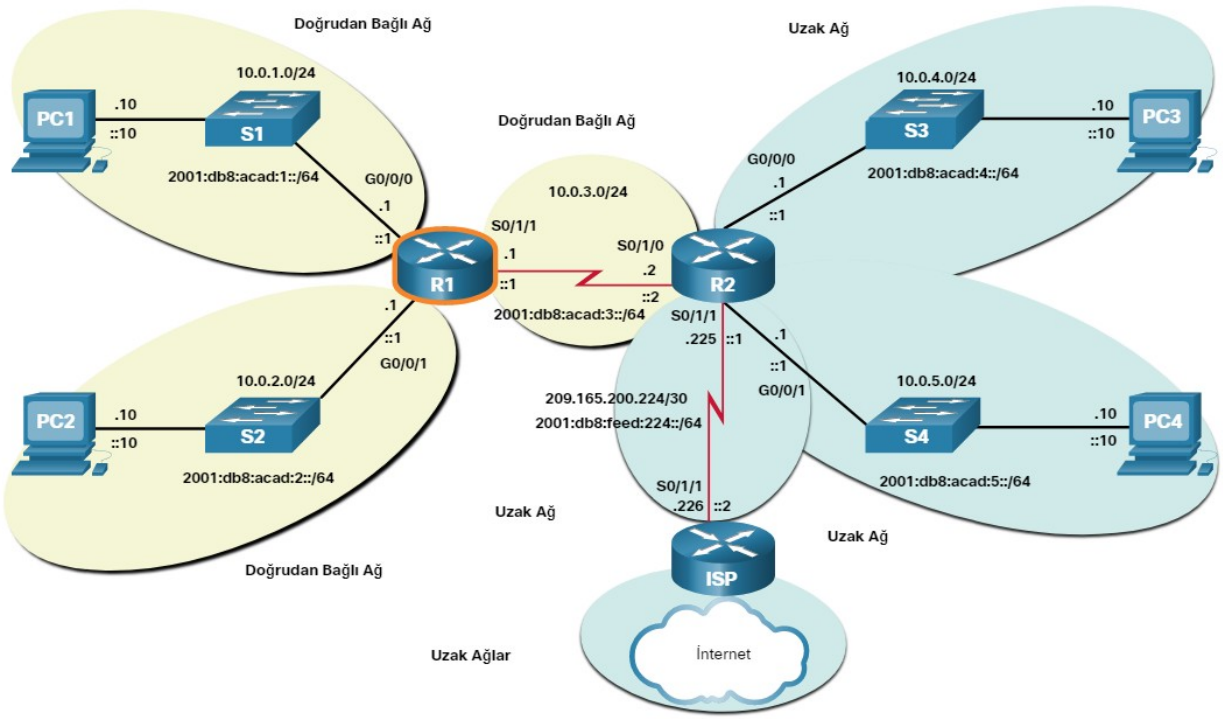
2001: db8: c000 :: 99 adresli hedef IPv6 paketi için aşağıdaki üç yol girişini göz önünde bulundurun:

| Rota Girişi | Önek / Önek Uzunluğu | Uyuyor mu? |
|---|---|---|
| 1 | **2001: db8: c0** 00 :: **/ 40** | 40 bitlik maç |
| 2 | **2001: db8: c000** :: **/ 48** | 48 bitlik maç (en uzun eşleşme) |
| 3 | **2001: db8: c000** : 5555 :: **/ 64** | 64 bit ile eşleşmiyor |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 30.1.4.Yönlendirme Tablosunu Oluşturma

Bir yönlendirme tablosu, öneklerden ve bunların önek uzunluklarından oluşur. Ancak yönlendirici bu ağları nasıl öğrenir? Şekildeki R1 yönlendirme tablosunu nasıl dolduruyor?




Topolojideki ağlar vurgulanır ve R1 perspektifinden etiketlenir. Sarı ile vurgulanan tüm IPv4 ve IPv6 ağları doğrudan bağlı ağlardır. Mavi ile vurgulanan tüm IPv4 ve IPv6 ağları uzak ağlardır.

### Doğrudan Bağlı Ağlar

Doğrudan bağlı ağlar, bir yönlendiricinin aktif arayüzlerinde yapılandırılan ağlardır. Bir arabirim bir IP adresi ve alt ağ maskesi (önek uzunluğu) ile yapılandırıldığında ve etkin olduğunda (yukarı ve yukarı) doğrudan bağlı bir ağ yönlendirme tablosuna eklenir.

### Uzak Ağlar

Uzak ağlar, yönlendiriciye doğrudan bağlı olmayan ağlardır. Yönlendiriciler uzak ağları iki şekilde öğrenir:

- Statik yollar - Bir yol manuel olarak yapılandırıldığında yönlendirme tablosuna eklenir.
- Dinamik yönlendirme protokolleri - Yönlendirme tablosuna eklenirken protokoller dinamik olarak uzak ağ hakkında bilgi alır. Dinamik yönlendirme protokolleri, Geliştirilmiş İç Ağ Geçidi Yönlendirme Protokolü (Enhanced Interior Gateway Routing Protocol-EIGRP), Önce En Kısa Yolu Aç (Open Shortest Path First -OSPF) ve diğerlerini içerir.

### Varsayılan rota

Varsayılan bir yol, yönlendirme tablosu hedef IP adresiyle eşleşen belirli bir yol içermediğinde kullanılacak bir sonraki atlama yönlendiricisini belirtir. Varsayılan yol, statik bir yol olarak manuel olarak girilebilir veya dinamik bir yönlendirme protokolünden otomatik olarak öğrenilebilir.

Licensed to yetkin karasundur yetkinkrsngr@gmail.com

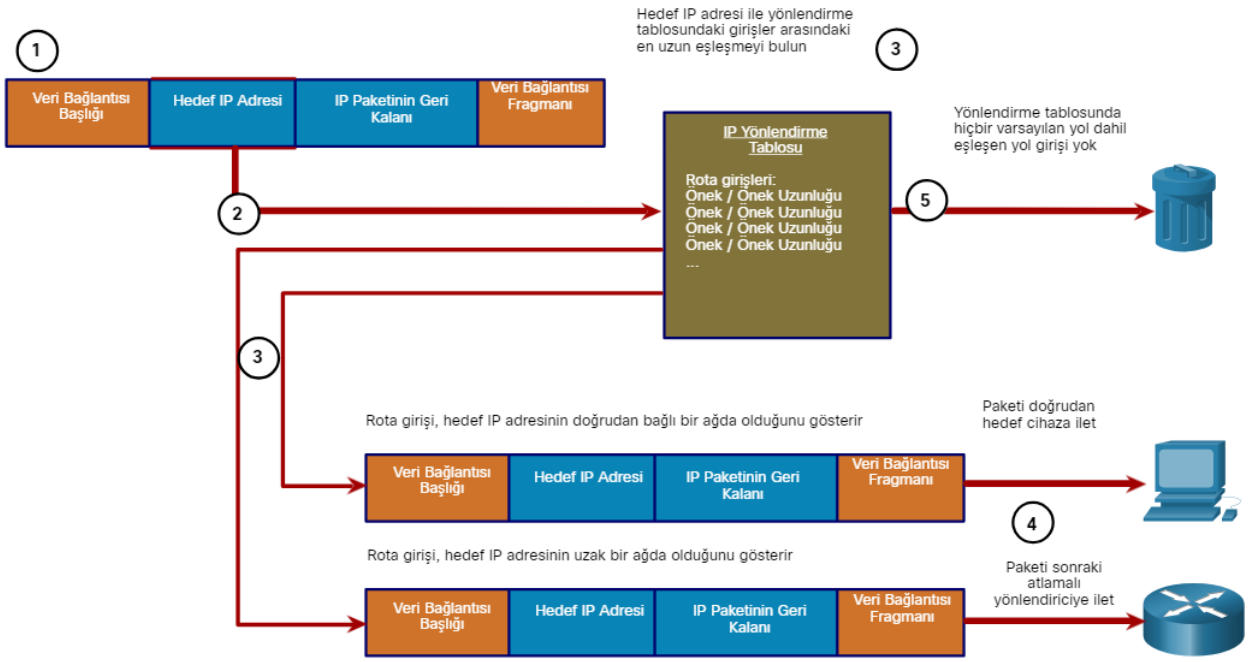
IPv4 üzerinden varsayılan bir yol 0.0.0.0/0 yol girişine ve IPv6 üzerinden varsayılan bir yol :: / 0 yol girişine sahiptir. / 0 önek uzunluğu, bu yol girişinin kullanılması için hedef IP adresiyle sıfır bitin veya hiçbir bitin eşleşmesi gerektiğini belirtir. Daha uzun eşleşmeli, 0 bitten fazla yol yoksa, paketi iletmek için varsayılan yol kullanılır. Varsayılan yol bazen son çare olarak bir ağ geçidi (gateway of last resort ) olarak anılır.

## 30.2.Paket Yönlendirme

### 30.2.1.Paket Yönlendirme Karar Süreci

Yönlendirici, en uzun eşleşmeye dayalı olarak bir paket için en iyi yolu belirlediğine göre sonrasında paketi nasıl kapsülleyeceğini ve doğru çıkış arayüzüne nasıl ileteceğini belirlemelidir.

Şekil, bir yönlendiricinin ilk olarak en iyi yolu nasıl belirlediğini ve ardından paketi nasıl ilettiğini gösterir.




Aşağıdaki adımlar, şekilde gösterilen paket yönlendirme sürecini açıklamaktadır:

1. Kapsüllenmiş bir IP paketine sahip veri bağlantı çerçevesi giriş arayüzüne ulaşır.
2. Yönlendirici, paket başlığındaki hedef IP adresini inceler ve IP yönlendirme tablosuna başvurur.
3. Yönlendirici, yönlendirme tablosunda en uzun eşleşen öneki bulur.
4. Yönlendirici, paketi bir veri bağlantı çerçevesinde sarmalar ve onu ağ çıkışı arayüzünden dışarı iletir. Hedef, ağa bağlı bir cihaz veya bir sonraki atlama yönlendiricisi olabilir.
5. Bununla birlikte, eşleşen yol girişi yoksa, paket bırakılır.

#### Paketi Doğrudan Bağlı Bir Ağ Üzerindeki Bir Aygıta İletir

Yol girişi çıkış arayüzünün doğrudan bağlı bir ağ olduğunu gösteriyorsa, bu, paketin hedef IP adresinin doğrudan bağlı ağdaki bir cihaza ait olduğu anlamına gelir. Bu nedenle, paket doğrudan hedef cihaza iletilebilir. Hedef cihaz tipik olarak bir Ethernet LAN üzerindeki bir uç cihazdır, bu da paketin bir Ethernet çerçevesi içinde kapsüllenmesi gerektiği anlamına gelir.

Paketi Ethernet çerçevesinde kapsüllemek için, yönlendiricinin, paketin hedef IP adresi ile ilişkili hedef MAC adresini belirlemesi gerekir. İşlem, paketin bir IPv4 veya IPv6 paketi olmasına bağlı olarak değişir:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

IPv4 paketi - Yönlendirici, hedef IPv4 adresi ve ilişkili bir Ethernet MAC adresi için ARP tablosunu kontrol eder. Eşleşme yoksa yönlendirici bir ARP İsteği gönderir. Hedef cihaz, MAC adresini içeren bir ARP Yanıtı döndürecektir. Yönlendirici artık IPv4 paketini uygun hedef MAC adresiyle bir Ethernet çerçevesinde iletebilir.
IPv6 paketi - Yönlendirici, hedef IPv6 adresi ve ilişkili bir Ethernet MAC adresi için komşu önbelleğini kontrol eder. Eşleşme yoksa, yönlendirici bir ICMPv6 Komşu Talep (NS) mesajı gönderir. Hedef cihaz, MAC adresiyle birlikte bir ICMPv6 Komşu Bildirisi (NA) mesajı döndürecektir. Yönlendirici artık IPv6 paketini uygun hedef MAC adresi ile bir Ethernet çerçevesinde iletebilir.

**Paketi Next-Hop Yönlendiriciye iletir**

Yol girişi, hedef IP adresinin uzak bir ağda olduğunu gösteriyorsa, bu, paketin hedef IP adresinin doğrudan bağlı olmayan ağdaki bir cihaza ait olduğu anlamına gelir. Bu nedenle, paketin başka bir yönlendiriciye, özellikle bir sonraki atlama yönlendiricisine iletilmesi gerekir. Sonraki atlama adresi yol girişinde belirtilir.

Yönlendirme yönlendiricisi ve sonraki atlama yönlendiricisi bir Ethernet ağı üzerindeyse, daha önce açıklandığı gibi paketin hedef MAC adresini belirlemek için benzer bir işlem (ARP ve ICMPv6 Komşu Keşfi) gerçekleşir. Aradaki fark, yönlendiricinin, paketin hedef IP adresi yerine ARP tablosunda veya komşu önbelleğinde sonraki atlama yönlendiricisinin IP adresini arayacak olmasıdır.

Not : Bu işlem, diğer Katman 2 ağ türleri için değişiklik gösterecektir.

**Paketi Düşürür - Yönlendirme Tablosunda Eşleşme Yok**

Hedef IP adresi ile yönlendirme tablosundaki bir önek arasında bir eşleşme yoksa ve varsayılan yol yoksa, paket bırakılacaktır.

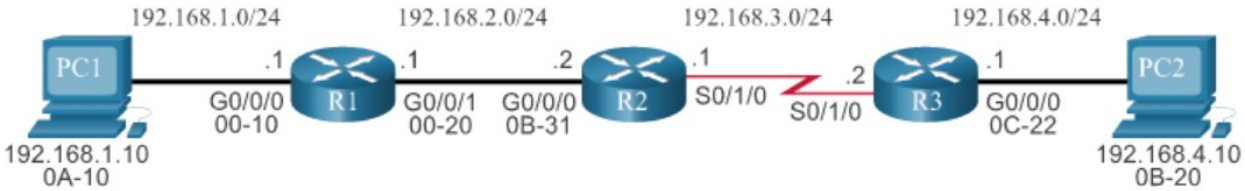
## 30.2.2.Uçtan Uca Paket Yönlendirme

Paket iletme fonksiyonunun birincil sorumluluğu, giden arayüz için uygun veri bağlantı çerçeve tipinde paketleri kapsüllemektir. Örneğin, bir seri bağlantı için veri bağlantı çerçeve formatı Noktadan Noktaya (Point-to-Point PPP) protokolü, Yüksek Seviye Veri Bağlantısı Kontrolü (High-Level Data Link Control -HDLC) protokolü veya başka bir Katman 2 protokolü olabilir.

**PC1, PC2'ye Paket Gönderir**

İlk şekilde, PC1, PC2'ye bir paket gönderir. PC2 farklı bir ağda olduğundan, PC1 paketi varsayılan ağ geçidine iletecektir. PC1, varsayılan ağ geçidinin MAC adresi için ARP önbelleğine bakacak ve belirtilen çerçeve bilgilerini ekleyecektir.

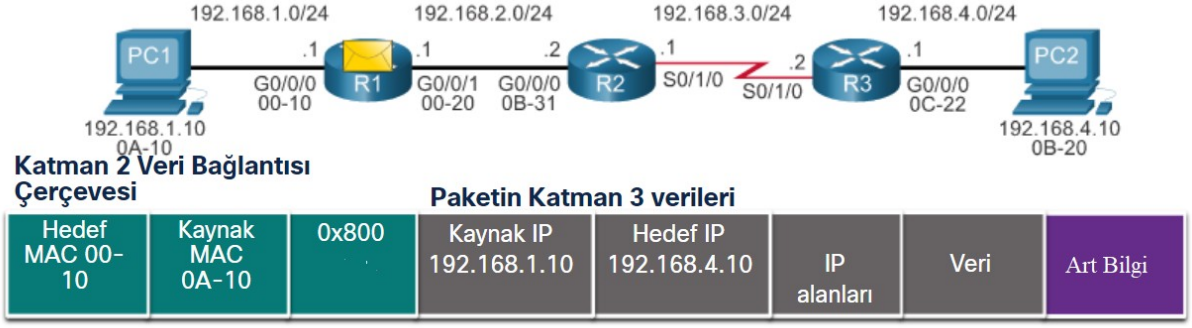
Not : 192.168.1.1 varsayılan ağ geçidi için ARP tablosunda bir ARP girişi yoksa, PC1 bir ARP isteği gönderir. Yönlendirici R1 daha sonra MAC adresiyle bir ARP yanıtı döndürecektir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### R1 Paketi PC2'ye İletir

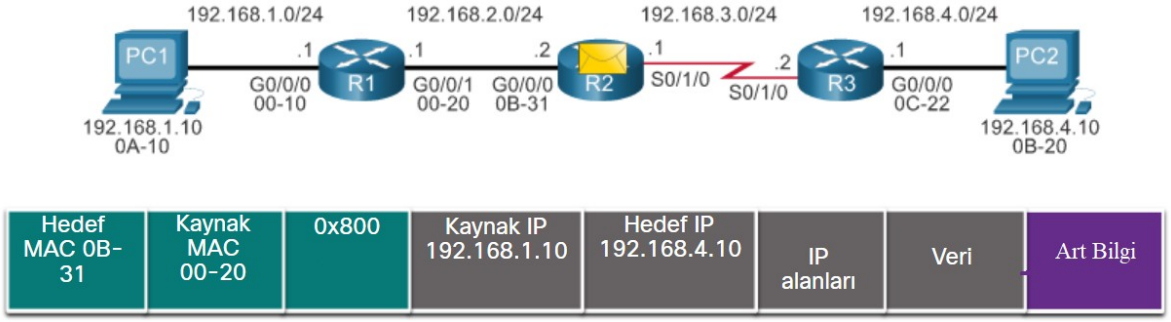
R1 şimdi paketi PC2'ye iletir. Çıkış arabirimi bir Ethernet ağında olduğundan, R1'in ARP tablosunu kullanarak bir hedef MAC adresiyle sonraki atlama IPv4 adresini çözmesi gerekir. 192.168.2.2'nin sonraki atlama arabirimi için ARP tablosunda bir ARP girişi yoksa, R1 bir ARP isteği gönderir. R2 daha sonra bir ARP Yanıtı döndürecektir.




R2

### Paketi R3'e İletir

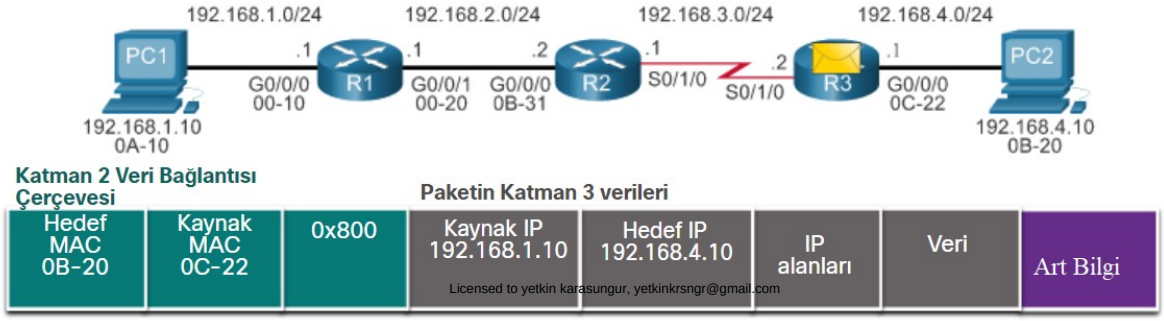
R2 şimdi paketi R3'e iletir. Çıkış arabirimi bir Ethernet ağı olmadığından, R2'nin sonraki atlama IPv4 adresini bir hedef MAC adresi ile çözmesi gerekmez. Arabirim noktadan noktaya (P2P) seri bağlantı olduğunda, yönlendirici IPv4 paketini çıkış arabirimi (HDLC, PPP, vb.) Tarafından kullanılan uygun veri bağlantısı çerçeve biçimine ekler. Seri arayüzlerde MAC adresi olmadığından, R2 veri bağlantısı hedef adresini bir yayına eşdeğer olarak ayarlar.




R3

### Paketi PC2'ye Yönlendirir

R3 şimdi paketi PC2'ye iletir. Hedef IPv4 adresi doğrudan bağlı bir Ethernet ağında olduğundan, R3, paketin hedef IPv4 adresini ilişkili MAC adresiyle çözmelidir. Giriş ARP tablosunda değilse, R3, FastEthernet 0/0 arayüzünden bir ARP isteği gönderir. PC2 daha sonra MAC adresiyle bir ARP yanıtı döndürecektir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 30.3.IP Yönlendirme Tablosu

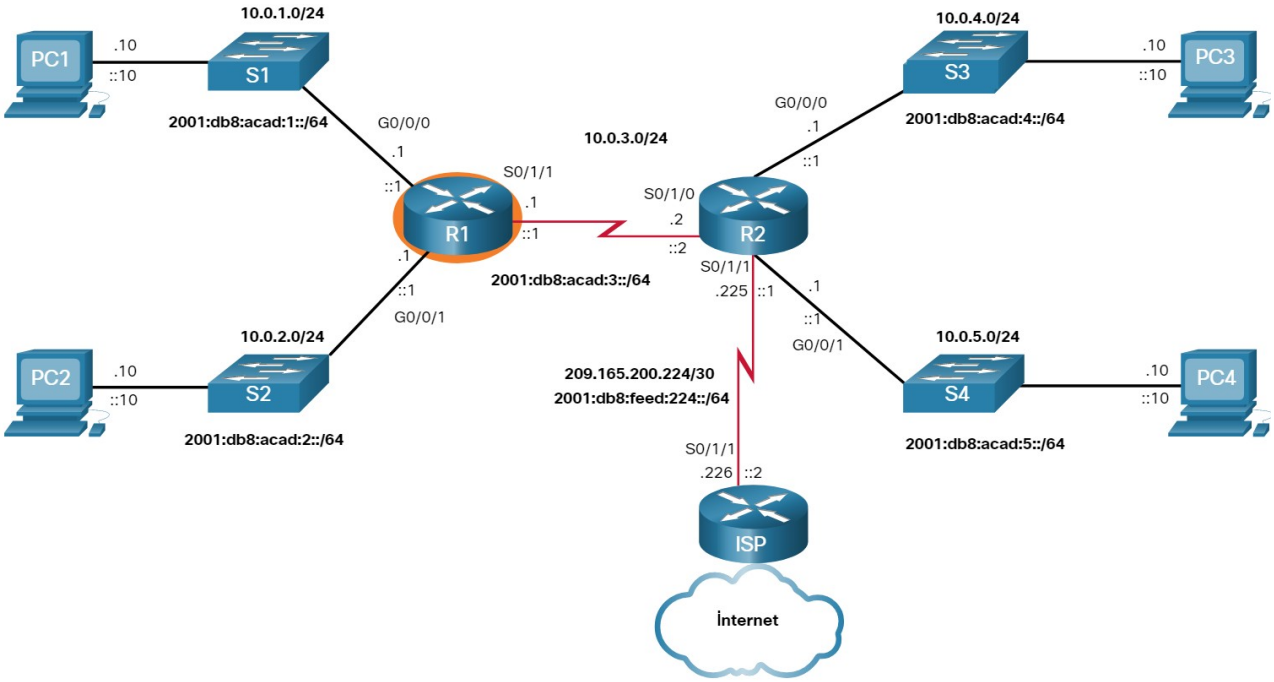
### 30.3.1.Rota Kaynakları

Bir yönlendirici, paketleri nereye gönderebileceğini nasıl bilir? İçinde bulunduğu ağa dayalı bir yönlendirme tablosu oluşturur.

Yönlendirme tablosu, bilinen ağlara giden yolların bir listesini içerir (önekler ve önek uzunlukları). Bu bilgilerin kaynağı aşağıdakilerden türetilmiştir:

- Doğrudan bağlı ağlar
- Statik yollar
- Dinamik yönlendirme protokolleri

Şekilde, R1 ve R2, yönlendirme bilgilerini paylaşmak için dinamik yönlendirme protokolü OSPF'yi kullanıyor. Ek olarak, R2, ISP'ye varsayılan bir statik yol ile yapılandırılır.




```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 10.0.3.2 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
C        10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
L        10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
C        10.0.3.0/24 is directly connected, Serial0/1/1
L        10.0.3.1/32 is directly connected, Serial0/1/1
O        10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O        10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1#
```

Lisansınız Yetkinkrsngr@gmail.com

```
R2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
Gateway of last resort is 209.165.200.226 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 209.165.200.226
     10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
O       10.0.1.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
O       10.0.2.0/24 [110/65] via 10.0.3.1, 00:31:38, Serial0/1/0
C       10.0.3.0/24 is directly connected, Serial0/1/0
L       10.0.3.2/32 is directly connected, Serial0/1/0
C       10.0.4.0/24 is directly connected, GigabitEthernet0/0/0
L       10.0.4.1/32 is directly connected, GigabitEthernet0/0/0
C       10.0.5.0/24 is directly connected, GigabitEthernet0/0/1
L       10.0.5.1/32 is directly connected, GigabitEthernet0/0/1
     209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C       209.165.200.224/30 is directly connected, Serial0/1/1
L       209.165.200.225/32 is directly connected, Serial0/1/1
```

R1 ve R2 için yönlendirme tablolarında, her yol için kaynakların bir kodla tanımlandığına dikkat edin. Kod, rotanın nasıl öğrenildiğini tanımlar. Örneğin, yaygın kodlar şunları içerir:

L - Bir yönlendirici arayüzüne atanan adresi tanımlar. Bu, yönlendiricinin, iletilmek yerine arabirim için bir paket aldığını etkin bir şekilde belirlemesini sağlar.
C - Doğrudan bağlı bir ağı tanımlar.
S - Belirli bir ağa ulaşmak için oluşturulmuş statik bir yolu tanımlar.
O - OSPF yönlendirme protokolünü kullanarak başka bir yönlendiriciden dinamik olarak öğrenilen bir ağı tanımlar.
* - Bu rota, varsayılan bir rota için adaydır.

## 30.3.2. Yönlendirme Tablosu Prensipleri

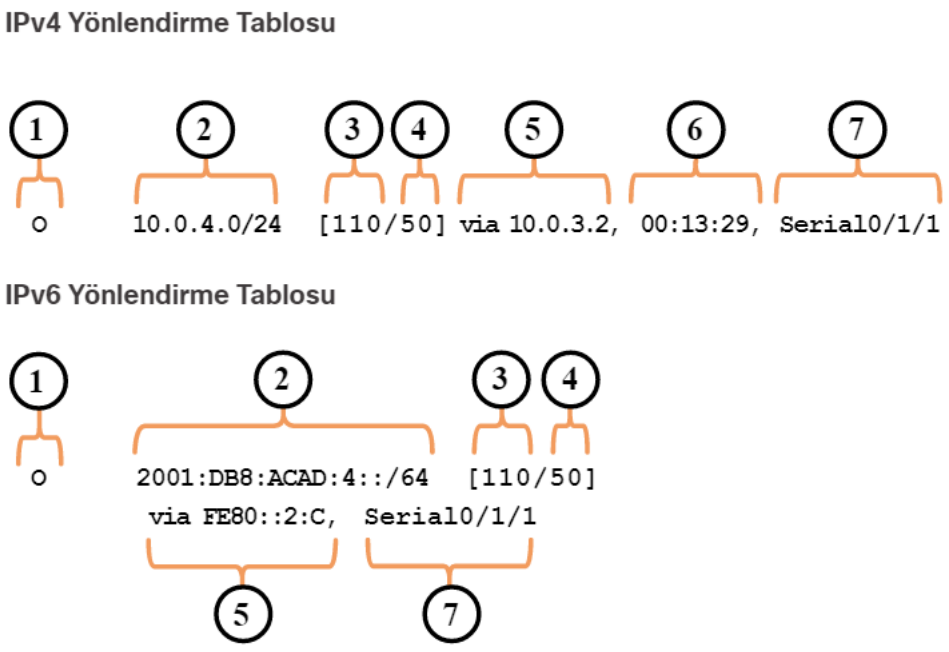
Tabloda açıklandığı gibi üç yönlendirme tablosu ilkesi vardır. Bunlar, dinamik yönlendirme protokollerinin veya kaynak ve hedef aygıtlar arasındaki tüm yönlendiricilerdeki statik yolların uygun şekilde yapılandırılmasıyla ele alınan sorunlardır.

| Yönlendirme Tablosu Prensibi | Misal |
|---|---|
| Her yönlendirici, kendi yönlendirme tablosundaki bilgilere dayanarak kararını tek başına verir. | • R1, paketleri yalnızca kendi yönlendirme tablosunu kullanarak iletebilir.<br>• R1, diğer yönlendiricilerin (örneğin R2) yönlendirme tablolarında hangi yolların olduğunu bilmez. |
| Bir yönlendiricinin yönlendirme tablosundaki bilgiler, başka bir yönlendiricinin yönlendirme tablosuyla mutlaka eşleşmez. | R1'in yönlendirme tablosunda R2 üzerinden internetteki bir ağa rota olması, R2'nin aynı ağı bildiği anlamına gelmez. |
| Bir yol hakkında yönlendirme bilgisi, dönüş yönlendirme bilgisi sağlamaz. | R1, PC1'in hedef IP adresi ve PC3'ün kaynak IP adresi ile bir paket alır. Sırf R1, paketi G0 / 0/0 arayüzünden dışarı iletmeyi bildiği için, PC1'den gelen paketleri PC3'ün uzak ağına nasıl ileteceğini bildiği anlamına gelmez. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 30.3.3.Yönlendirme Tablosu Girişleri

Bir ağ yöneticisi olarak, IPv4 ve IPv6 yönlendirme tablolarının içeriğinin nasıl yorumlanacağını bilmek zorunludur. Şekil, 10.0.4.0/24 ve 2001: db8: acad: 4 :: / 64 uzak ağına giden yol için R1'deki IPv4 ve IPv6 yönlendirme tablosu girişlerini gösterir. Bu yolların her ikisi de, OSPF yönlendirme protokolünden dinamik olarak öğrenildi.




Şekilde, sayılar aşağıdaki bilgileri tanımlar:

1. **Rota kaynağı** - Bu, rotanın nasıl öğrenildiğini tanımlar.
2. **Hedef ağ (önek ve önek uzunluğu)** - Bu, uzak ağın adresini tanımlar.
3. **İdari mesafe** - Bu, rota kaynağının güvenilirliğini tanımlar. Daha düşük değerler, tercih edilen yol kaynağını gösterir.
4. **Metrik** - Bu, uzak ağa ulaşmak için atanan değeri tanımlar. Daha düşük değerler tercih edilen yolları gösterir.
5. **Sonraki atlama** - Bu, paketin iletileceği sonraki yönlendiricinin IP adresini

#### 30.3.3.1.Doğrudan Bağlı Ağlar

Bir yönlendiricinin herhangi bir uzak ağ hakkında bilgi alabilmesi için, bir IP adresi ve alt ağ maskesi (önek uzunluğu) ile yapılandırılmış en az bir aktif arayüze sahip olması gerekir. Bu, doğrudan bağlı bir ağ veya doğrudan bağlı bir yol olarak bilinir. Yönlendiriciler, bir arabirim bir IP adresiyle yapılandırıldığında ve etkinleştirildiğinde yönlendirme tablosuna doğrudan bağlı bir yol ekler.

Doğrudan bağlı bir ağ, yönlendirme tablosunda C'nin bir durum kodu ile gösterilir . Yol, bir ağ öneki ve önek uzunluğu içerir.

Yönlendirme tablosu ayrıca, L' nin durum kodu ile gösterilen, doğrudan bağlı ağlarının her biri için yerel bir yol içerir . Bu, doğrudan bağlı ağdaki arabirime atanan IP adresidir. IPv4 yerel yolları için ön ek uzunluğu / 32'dir ve IPv6 yerel yolları için önek uzunluğu / 128'dir. Bu, paketin hedef IP adresinin, bu rotanın bir eşleşme olması için yerel yoldaki tüm bitlerle eşleşmesi gerektiği anlamına gelir. Yerel yolun amacı, iletilmesi gereken bir paket yerine arabirim için bir paket aldığında verimli bir şekilde belirlemektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Doğrudan bağlı ağlar ve yerel yollar aşağıdaki çıktıda gösterilmektedir.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(Output omitted)
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
R1#
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(Output omitted)

C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
R1#
```

### 30.3.3.2.Statik Yollar

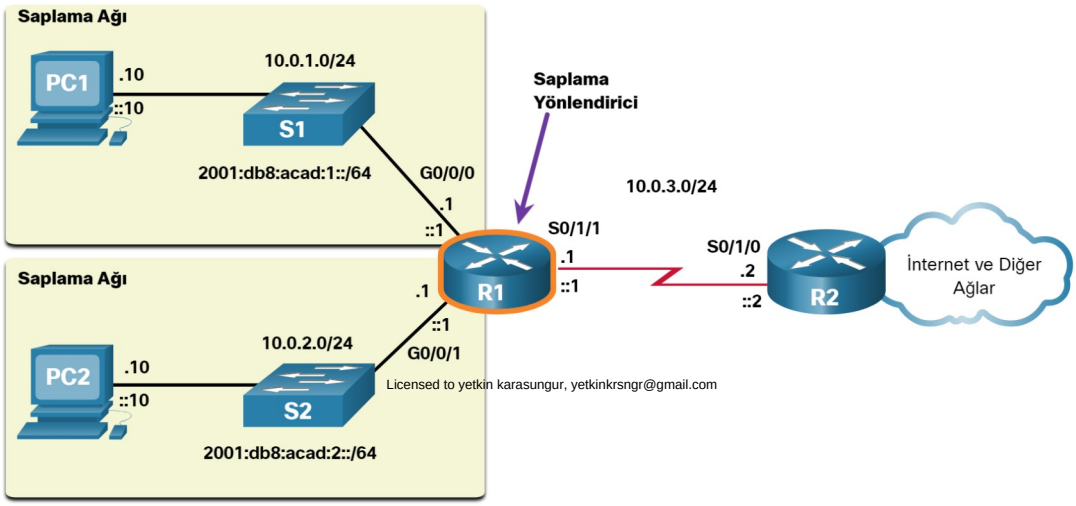
Doğrudan bağlanan arayüzler yapılandırıldıktan ve yönlendirme tablosuna eklendikten sonra, uzak ağlara erişim için statik veya dinamik yönlendirme uygulanabilir.

Statik yollar manuel olarak yapılandırılır. İki ağ cihazı arasında açık bir yol tanımlarlar. Dinamik bir yönlendirme protokolünün aksine, statik yollar otomatik olarak güncellenmez ve ağ topolojisi değişirse manuel olarak yeniden yapılandırılmalıdır. Statik yolları kullanmanın faydaları, gelişmiş güvenlik ve kaynak verimliliğini içerir. Statik yollar, dinamik yönlendirme protokollerinden daha az bant genişliği kullanır ve yolları hesaplamak ve iletmek için hiçbir CPU döngüsü kullanılmaz. Statik yolları kullanmanın ana dezavantajı, ağ topolojisi değişirse otomatik yeniden yapılandırmanın olmamasıdır.

Statik yönlendirmenin üç birincil kullanımı vardır:

- Önemli ölçüde büyümesi beklenmeyen küçük ağlarda yönlendirme tablosu bakımı kolaylığı sağlar.
- Yönlendirme tablosundaki başka bir yolla daha belirli bir eşleşmesi olmayan herhangi bir ağa giden yolu temsil etmek için tek bir varsayılan yol kullanır. Varsayılan yollar, bir sonraki yukarı akış yönlendiricisinin dışındaki herhangi bir hedefe trafik göndermek için kullanılır.
- Saplama (Stub) ağlarına yönlendirir. Saplama ağı, tek bir yolla erişilen bir ağdır ve yönlendiricinin yalnızca bir komşusu vardır.

Şekil, saplama ağlarının bir örneğini göstermektedir. R1'e bağlı herhangi bir ağın, ister R2'ye bağlı ağlara, ister R2'nin dışındaki hedeflere, diğer hedeflere ulaşmak için yalnızca bir yolu olacağına dikkat edin. Bu, 10.0.1.0/24 ve 10.0.2.0/24 ağlarının saplama ağları olduğu ve R1'in bir saplama yönlendiricisi olduğu anlamına gelir.

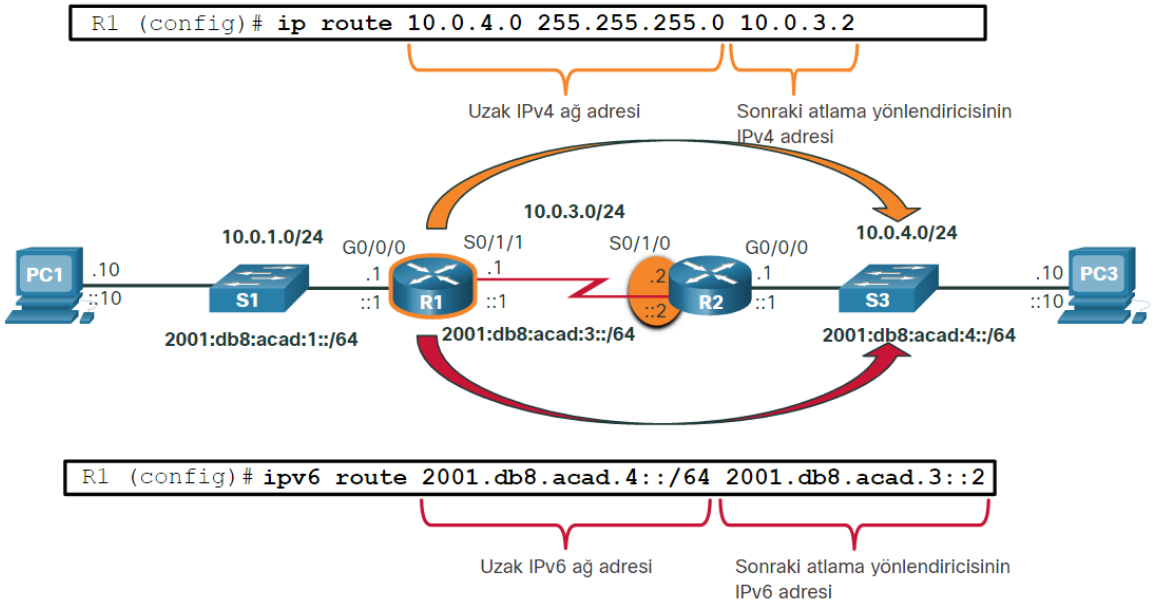


Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bu örnekte, R1 ağlarına ulaşmak için R2 üzerinde statik bir yol yapılandırılabilir. Ek olarak, R1'in yerel olmayan trafiği göndermek için tek bir yolu olduğundan, diğer tüm ağlar için bir sonraki sıçrama olarak R2'yi işaret etmek için R1'de varsayılan bir statik yol yapılandırılabilir.

### 30.3.3.3.IP Yönlendirme Tablosundaki Statik Yollar

Statik yönlendirmeyi göstermek için, şekildeki topoloji, her yönlendiriciye bağlı yalnızca bir LAN'ı gösterecek şekilde basitleştirilmiştir. Şekil, R2 üzerinde 10.0.4.0/24 ve 2001: db8: acad: 4 :: / 64 ağlarına ulaşmak için R1 üzerinde yapılandırılmış IPv4 ve IPv6 statik yollarını gösterir. Yapılandırma komutları yalnızca gösterim amaçlıdır ve başka bir bölümde ele alınmıştır.




Çıktı, R2 üzerindeki 10.0.4.0/24 ve 2001: db8: acad: 4 :: / 64 ağlarına erişebilen R1 üzerindeki IPv4 ve IPv6 statik yönlendirme girdilerini gösterir. Her iki yönlendirme girdisinin de, rotanın statik bir yolla öğrenildiğini belirten S durum kodunu kullandığına dikkat edin . Her iki giriş de ip adresi aracılığıyla bir sonraki atlama yönlendiricisinin IP adresini içerir . Static parametresi sadece statik rotaları görüntüler.

```
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
(output omitted)

      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
S        10.0.4.0/24 [1/0] via 10.0.3.2
R1# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
(output omitted)

S   2001:DB8:ACAD:4::/64 [1/0]
     via 2001:DB8:ACAD:3::2
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

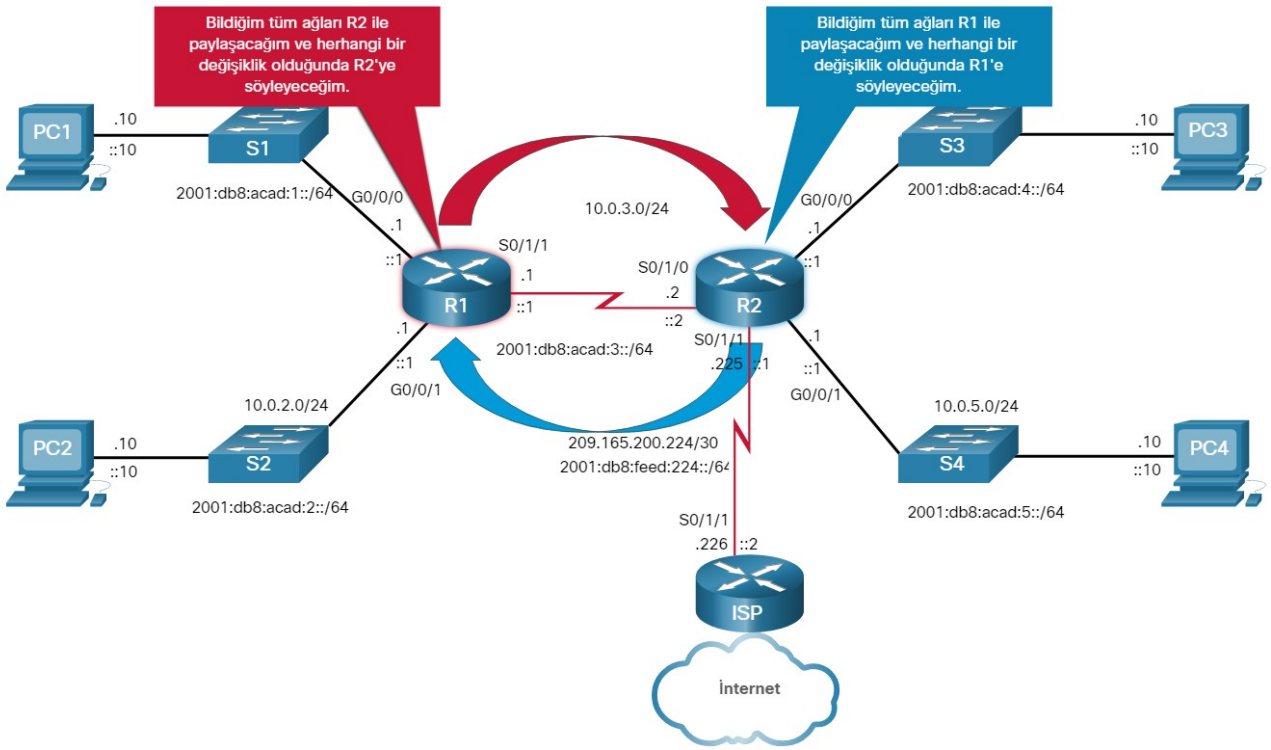
## 30.3.4.Dinamik Yönlendirme Protokolleri

Dinamik yönlendirme protokolleri, uzak ağların erişilebilirliği ve durumu hakkındaki bilgileri otomatik olarak paylaşmak için yönlendiriciler tarafından kullanılır. Dinamik yönlendirme protokolleri, ağ keşfi ve yönlendirme tablolarının bakımı dahil olmak üzere çeşitli aktiviteler gerçekleştirir.

Dinamik yönlendirme protokollerinin önemli avantajları, en iyi yolu seçme yeteneği ve topolojide bir değişiklik olduğunda yeni bir en iyi yolu otomatik olarak keşfetme yeteneğidir.

Ağ keşfi, bir yönlendirme protokolünün, hakkında bildiği ağlar hakkındaki bilgileri, aynı yönlendirme protokolünü kullanan diğer yönlendiricilerle paylaşma yeteneğidir. Her yönlendiricideki uzak ağlara manuel olarak yapılandırılmış statik yollara bağlı olmak yerine, dinamik bir yönlendirme protokolü, yönlendiricilerin bu ağları diğer yönlendiricilerden otomatik olarak öğrenmesine olanak tanır. Bu ağlar ve her birine giden en iyi yol yönlendiricinin yönlendirme tablosuna eklenir ve belirli bir dinamik yönlendirme protokolü tarafından öğrenilen bir ağ olarak tanımlanır.

Şekilde, ağ bilgilerini paylaşmak için ortak bir yönlendirme protokolü kullanan R1 ve R2 yönlendiricileri gösterilmektedir.




### 30.3.4.1.IP Yönlendirme Tablosundaki Dinamik Yollar

Önceki bir örnek 10.0.4.0/24 ve 2001: db8: acad: 4 :: / 64 ağlarına statik yollar kullanmıştır. Bu statik yollar artık yapılandırılmamaktadır ve OSPF artık R1 ve R2'ye bağlı tüm ağları dinamik olarak öğrenmek için kullanılmaktadır. Aşağıdaki örnekler, R2'de bu ağlara erişebilen R1 üzerindeki IPv4 ve IPv6 OSPF yönlendirme girişlerini gösterir. Her iki yönlendirme girişinin , yolun OSPF yönlendirme protokolü tarafından öğrenildiğini belirtmek için O durum kodunu kullandığına dikkat edin . Her iki giriş de ip adresi aracılığıyla sonraki atlama yönlendiricisinin IP adresini içerir .

Not : IPv6 yönlendirme protokolleri, sonraki atlama yönlendiricisinin yerel bağlantı adresini kullanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not : IPv4 ve IPv6 için OSPF yönlendirme yapılandırması bu kitabın kapsamı dışındadır.

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
(output omitted for brevity)
O        10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O        10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1# show ipv6 route
IPv6 Routing Table - default - 10 entries
(Output omitted)
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
O   2001:DB8:ACAD:4::/64 [110/50]
     via FE80::2:C, Serial0/1/1
O   2001:DB8:ACAD:5::/64 [110/50]
     via FE80::2:C, Serial0/1/1
```

## 30.3.5.Varsayılan Rota (Default Route)

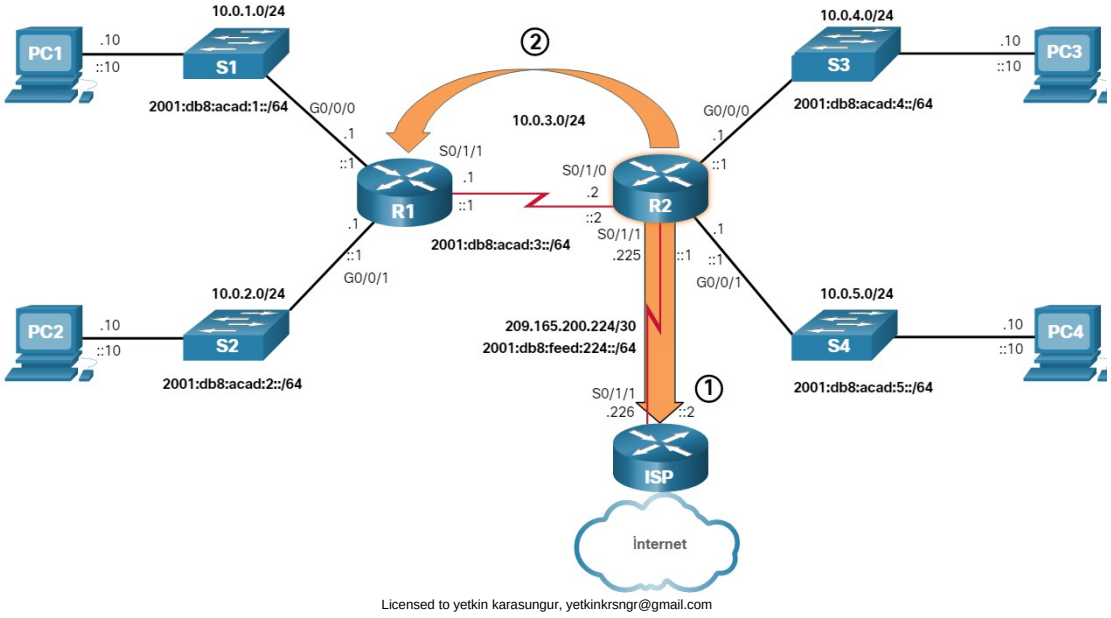
Varsayılan yol, ana bilgisayardaki varsayılan ağ geçidine benzer. Varsayılan yol, yönlendirme tablosu hedef IP adresiyle eşleşen belirli bir yol içermediğinde kullanılacak bir sonraki atlama yönlendiricisini belirtir.

Varsayılan bir yol, statik bir yol olabilir veya dinamik bir yönlendirme protokolünden otomatik olarak öğrenilebilir. Varsayılan bir yol, 0.0.0.0/0 IPv4 yol girişine veya :: / 0 IPv6 yol girişine sahiptir. Bu, hedef IP adresi ile varsayılan yol arasında sıfır veya sıfır bitin eşleşmesi gerektiği anlamına gelir.

Çoğu kurumsal yönlendiricinin yönlendirme tablolarında varsayılan bir yol vardır. Bu, bir yönlendirme tablosundaki yolların sayısını azaltmak içindir.

Yalnızca bir LAN'a sahip bir ev veya küçük ofis yönlendiricisi gibi bir yönlendirici, tüm uzak ağlarına varsayılan bir yol üzerinden erişebilir. Bu, yönlendiricinin yalnızca doğrudan bağlı ağlara ve bir servis sağlayıcı yönlendiricisine bir çıkış noktasına sahip olması durumunda yararlıdır.

Şekilde, R1 ve R2 yönlendiricileri, kendi ağları hakkında yönlendirme bilgilerini paylaşmak için OSPF kullanıyor (10.0.xx / 24 ve 2001: db8: acad: x :: / 64 ağları). R2, ISP yönlendiricisine giden statik bir varsayılan yola sahiptir. R2, yönlendirme tablosundaki ağlardan biriyle özel olarak eşleşmeyen bir hedef IP adresine sahip paketleri ISP yönlendiricisine iletecektir. Bu, internete yönelik tüm paketleri içerir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

1. R2, ISP yönlendiricisine giden statik bir varsayılan yola sahiptir.
2. Varsayılan yol, dinamik yönlendirme protokolü OSPF kullanılarak R2'den R1'e kadar bildirilir.

R2, varsayılan rotasını OSPF kullanarak R1 ile paylaştı. R1 artık yönlendirme tablosunda OSPF'den dinamik olarak öğrendiği bir varsayılan yola sahip olacaktır. R1 ayrıca, yönlendirme tablosundaki ağlardan biriyle özellikle eşleşmeyen bir hedef IP adresine sahip tüm paketleri R2'ye iletecektir.

Aşağıdaki örnekler, R2'de yapılandırılan statik varsayılan yollar için IPv4 ve IPv6 yönlendirme tablosu girdilerini gösterir.

```
R2# show ip route
(Output omitted)
S*    0.0.0.0/0 [1/0] via 209.165.200.226
R2#
R2# show ipv6 route
(Output omitted)
S   ::/0 [1/0]
     via 2001:DB8:FEED:224::2
R2#
```

## 30.3.6.IPv4 Yönlendirme Tablosunun Yapısı

IPv4, artık kullanılmayan sınıflandırılmış adresleme mimarisi kullanılarak 1980'lerin başında standartlaştırıldı. IPv4 yönlendirme tablosu, bu aynı sınıf yapısı kullanılarak düzenlenmiştir. **Show ip route** çıktısında, bazı rota girişlerinin sola yaslanmışken diğerlerinin girintili olduğuna dikkat edin. Bu, yönlendirme işleminin en uzun eşleşme için IPv4 yönlendirme tablosunda nasıl arama yaptığına bağlıdır. Bunların hepsi sınıflı (classfull) kullanımdan kaynaklanıyordu. Arama işlemi artık sınıfları kullanmasa da, IPv4 yönlendirme tablosunun yapısı yine de bu biçimde korunur.

```
Router# show ip route
(Output omitted)
     192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
O    192.168.2.0/24 [110/65] via 192.168.12.2, 00:32:33, Serial0/0/0
O    192.168.3.0/24 [110/65] via 192.168.13.2, 00:31:48, Serial0/0/1
     192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.12.0/30 is directly connected, Serial0/0/0
L       192.168.12.1/32 is directly connected, Serial0/0/0
     192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.13.0/30 is directly connected, Serial0/0/1
L       192.168.13.1/32 is directly connected, Serial0/0/1
     192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0/30 [110/128] via 192.168.12.2, 00:31:38, Serial0/0/0
Router#
```

Not : Örnekteki IPv4 yönlendirme tablosu, bu bölümde kullanılan topolojideki herhangi bir yönlendiriciye ait değildir.

Yapının detayları bu modülün kapsamı dışında olsa da, tablonun yapısını tanımakta fayda var. Girintili giriş, alt rota olarak bilinir. Sınıflı bir adresin alt ağıysa (A, B veya C sınıfı ağ) bir yol girişi girintilidir. Arayüzün yerel adresi her zaman yönlendirme tablosuna / 32 olarak girildiğinden, doğrudan bağlı ağlar her zaman girintilenir (alt yollar). Alt yol, yol kaynağını ve sonraki atlama adresi gibi tüm yönlendirme bilgilerini içerecektir. Bu alt ağın klas ağ adresi, yol girişinin üzerinde, daha az girintili ve kaynak kodu olmadan gösterilecektir. Bu rota, ana rota olarak bilinir.

Not : Bu, bir IPv4 yönlendirme tablosunun yapısına kısa bir giriş niteliğindedir ve bu mimarinin ayrıntılarını veya özelliklerini kapsamaz.

Licensed to yetkin karasungur, yetinkrshgr@gmail.com

Sonraki örnek, topolojide R1'in IPv4 yönlendirme tablosunu gösterir. Topolojideki tüm ağların, A sınıfı ağın alt yolları olan alt ağlar ve ana yol10.0.0.0 / 8 olduğuna dikkat edin.

```
R1# show ip route
(output omitted for brevity)
O*E2  0.0.0.0/0 [110/1] via 10.0.3.2, 00:51:34, Serial0/1/1
      10.0.0.0/8 is variably subnetted, 8 subnets, 2 masks
C        10.0.1.0/24 is directly connected, GigabitEthernet0/0/0
L        10.0.1.1/32 is directly connected, GigabitEthernet0/0/0
C        10.0.2.0/24 is directly connected, GigabitEthernet0/0/1
L        10.0.2.1/32 is directly connected, GigabitEthernet0/0/1
C        10.0.3.0/24 is directly connected, Serial0/1/1
L        10.0.3.1/32 is directly connected, Serial0/1/1
O        10.0.4.0/24 [110/50] via 10.0.3.2, 00:24:22, Serial0/1/1
O        10.0.5.0/24 [110/50] via 10.0.3.2, 00:24:15, Serial0/1/1
R1#
```

## 30.3.7.IPv6 Yönlendirme Tablosunun Yapısı

Klasik adresleme kavramı hiçbir zaman IPv6'nın bir parçası olmamıştır, bu nedenle bir IPv6 yönlendirme tablosunun yapısı çok basittir. Her IPv6 yol girişi aynı şekilde biçimlendirilir ve hizalanır.

```
R1# show ipv6 route
(output omitted for brevity)
OE2 ::/0 [110/1], tag 2
     via FE80::2:C, Serial0/0/1
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via GigabitEthernet0/0/1, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via GigabitEthernet0/0/1, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via Serial0/1/1, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via Serial0/1/1, receive
O   2001:DB8:ACAD:4::/64 [110/50]
     via FE80::2:C, Serial0/1/1
O   2001:DB8:ACAD:5::/64 [110/50]
     via FE80::2:C, Serial0/1/1
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

## 30.3.8.İdari,Yönetimsel Mesafe (Administrative Distance)

Belirli bir ağ adresi için bir yol girişi (önek ve önek uzunluğu) yönlendirme tablosunda yalnızca bir kez görünebilir. Bununla birlikte, yönlendirme tablosunun aynı ağ adresini birden fazla yönlendirme kaynağından öğrenmesi mümkündür.

Çok özel durumlar haricinde, bir yönlendiricide yalnızca bir dinamik yönlendirme protokolü uygulanmalıdır. Ancak, bir yönlendiricide hem OSPF hem de EIGRP'yi yapılandırmak mümkündür ve her iki yönlendirme protokolü de aynı hedef ağı öğrenebilir. Her yönlendirme protokolü, o yönlendirme protokolünün ölçüsüne bağlı olarak hedefe ulaşmak için farklı bir yola karar verebilir.

Lisanslı bir kullanıcıya ait [illegible]@gmail.com

Bu, aşağıdaki gibi birkaç soruyu gündeme getirir:

- Yönlendirici hangi kaynağı kullanacağını nasıl biliyor?
- Yönlendirme tablosuna hangi yolu yüklemelidir? OSPF'den öğrenilen rota veya EIGRP'den öğrenilen rota?

Cisco IOS, IP yönlendirme tablosuna kurulacak yolu belirlemek için yönetim mesafesi (AD) olarak bilinen şeyi kullanır. AD, rotanın "güvenilirliğini" temsil eder. AD ne kadar düşükse, rota kaynağı o kadar güvenilirdir. EIGRP'nin AD değeri 90 ve OSPF'nin AD'si 110 olduğundan, EIGRP yol girişi yönlendirme tablosuna yüklenecektir.

Not : AD, hangi dinamik yönlendirme protokolünün en iyi olduğunu göstermez.

Daha yaygın bir örnek, aynı ağ adresini statik bir yoldan ve OSPF gibi dinamik bir yönlendirme protokolünden öğrenen bir yönlendiricidir. Statik bir yolun AD'si 1 iken, OSPF tarafından keşfedilen bir yolun AD'si 110'dur. Aynı hedefe giden iki ayrı yol kaynağı verildiğinde, yönlendirici en düşük AD'ye sahip yolu yüklemeyi seçer. Bir yönlendirici bir statik yol ve bir OSPF yol seçeneğine sahip olduğunda, statik yol öncelikli olur.

Not : Doğrudan bağlı ağların en düşük AD'si 0'dır. Yalnızca doğrudan bağlanan bir ağın AD'si 0 olabilir.

Tablo, çeşitli yönlendirme protokollerini ve bunlarla ilişkili AD'leri listeler.

| Rota Kaynağı | İdari mesafe |
|---|---|
| Doğrudan bağlı | 0 |
| Statik yol | 1 |
| EIGRP özet rotası | 5 |
| Harici BGP | 20 |
| Dahili EIGRP | 90 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| Harici EIGRP | 170 |
| Dahili BGP | 200 |

## 30.4.Statik ve Dinamik Yönlendirme

### 30.4.1.Statik mi Dinamik mi?

Önceki konu, bir yönlendiricinin yönlendirme tablosunu oluşturma yollarını tartıştı. Böylece, IP adresleme gibi yönlendirmenin statik veya dinamik olabileceğini artık biliyorsunuz. Statik mi yoksa dinamik yönlendirme mi kullanmalısınız? Cevap ikisi de! Statik ve dinamik yönlendirme birbirini dışlamaz. Bunun yerine çoğu ağ, dinamik yönlendirme protokolleri ve statik rotaların bir kombinasyonunu kullanır.

**Statik Yollar**

Statik yollar genellikle aşağıdaki senaryolarda kullanılır:

Paketleri bir servis sağlayıcıya yönlendiren varsayılan bir yol olarak
Yönlendirme etki alanının dışındaki ve dinamik yönlendirme protokolü tarafından öğrenilmeyen yollar için
Ağ yöneticisi, belirli bir ağın yolunu açıkça tanımlamak istediğinde
Saplama ağları arasında yönlendirme için
Statik yollar, bir dış ağa yalnızca bir yolu olan küçük ağlar için kullanışlıdır. Ayrıca, belirli trafik türleri için daha büyük bir ağda güvenlik veya daha fazla kontrole ihtiyaç duyan diğer ağlara bağlantılar sağlarlar.

Licensed to yetkin.karasungur, yetkinkrsngr@gmail.com

**Dinamik Yönlendirme Protokolleri**

Dinamik yönlendirme protokolleri, ağ yöneticisinin zaman alıcı ve titiz bir statik yolları yapılandırma ve bakım sürecini yönetmesine yardımcı olur. Dinamik yönlendirme protokolleri, birkaç yönlendiriciden daha fazlasını içeren herhangi bir ağ türünde uygulanır. Dinamik yönlendirme protokolleri ölçeklenebilirdir ve topolojide bir değişiklik olması durumunda otomatik olarak daha iyi rotaları belirler.

Dinamik yönlendirme protokolleri, aşağıdaki senaryolarda yaygın olarak kullanılır:

Birkaç yönlendiriciden daha fazlasını içeren ağlarda
Ağ topolojisindeki bir değişiklik, ağın otomatik olarak başka bir yol belirlemesini gerektirdiğinde
Ölçeklenebilirlik için. Ağ büyüdükçe, dinamik yönlendirme protokolü herhangi bir yeni ağ hakkında otomatik olarak bilgi edinir.
Tablo, dinamik ve statik yönlendirme arasındaki bazı farklılıkların bir karşılaştırmasını gösterir.

| Özellik | Dinamik Yönlendirme | Statik yönlendirme |
|---|---|---|
| Yapılandırma karmaşıklığı | Ağ boyutundan bağımsız | Ağ boyutuyla birlikte artar |
| Topoloji değişiklikleri | Topoloji değişikliklerine otomatik olarak uyum sağlar | Yönetici müdahalesi gerekli |
| Ölçeklenebilirlik | Basitten karmaşık ağ topolojilerine uygun | Basit topolojiler için uygundur |
| Güvenlik | Güvenlik yapılandırılmalıdır | Güvenlik doğasında var |
| Kaynak kullanımı | CPU, bellek ve bağlantı bant genişliğini kullanır | Ek kaynak gerekmez |
| Yol Tahmin Edilebilirliği | Rota, kullanılan topolojiye ve yönlendirme protokolüne bağlıdır | Yönetici tarafından açıkça tanımlanmıştır |

## 30.4.2.Dinamik Yönlendirme Protokolü Kavramları

Yönlendirme protokolü, yönlendirme bilgilerini değiştirmek ve yönlendirme tablosunu en iyi yol seçenekleriyle doldurmak için kullanılan bir dizi işlem, algoritma ve mesajdır. Dinamik yönlendirme protokollerinin amacı aşağıdakileri içerir:

- 
- Uzak ağların keşfi
- Güncel yönlendirme bilgilerinin korunması
- Hedef ağlara giden en iyi yolu seçme
- Mevcut yol artık mevcut değilse yeni bir en iyi yol bulma yeteneği

Dinamik yönlendirme protokollerinin ana bileşenleri şunları içerir:

Veri yapıları - Yönlendirme protokolleri, işlemleri için tipik olarak tablolar veya veritabanları kullanır. Bu bilgiler RAM'de tutulur.
Yönlendirme protokol mesajları - Yönlendirme protokolleri, ağ hakkında doğru bilgileri öğrenmek ve korumak için komşu yönlendiricileri keşfetmek, yönlendirme bilgilerini değiştirmek ve diğer görevleri gerçekleştirmek için çeşitli mesaj türlerini kullanır.
Algoritma - Algoritma, bir görevi gerçekleştirmek için kullanılan sonlu bir adım listesidir. Yönlendirme protokolleri, yönlendirme bilgilerini kolaylaştırmak ve en iyi yol belirleme için algoritmalar kullanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yönlendirme protokolleri, her ağ için en iyi yolu veya rotayı belirler. Bu yol daha sonra yönlendirme tablosuna sunulur. Daha düşük AD'ye sahip başka bir yönlendirme kaynağı yoksa yol yönlendirme tablosuna yüklenecektir. Dinamik yönlendirme protokollerinin birincil yararı, yönlendiricilerin bir topoloji değişikliği olduğunda

yönlendirme bilgilerini değiştirmesidir. Bu değişim, yönlendiricilerin yeni ağları otomatik olarak öğrenmesine ve mevcut bir ağa bağlantı hatası olduğunda alternatif yollar bulmasına olanak tanır.

### 30.4.3.En İyi Yol

Yönlendirme tablosuna uzak bir ağa giden bir yol sunulmadan önce, dinamik yönlendirme protokolü o ağa giden en iyi yolu belirlemelidir. En iyi yolun belirlenmesi, aynı hedef ağa giden birden çok yolun değerlendirilmesini ve bu ağa ulaşmak için optimum veya en kısa yolun seçilmesini içerebilir. Aynı ağa giden birden fazla yol olduğunda, her yol, o ağa ulaşmak için yönlendiricide farklı bir çıkış arabirimi kullanır.

En iyi yol, bir ağa ulaşmak için mesafeyi belirlemek için kullandığı değer veya ölçüye dayalı bir yönlendirme protokolü tarafından seçilir. Bir metrik, belirli bir ağa olan mesafeyi ölçmek için kullanılan nicel değerdir. Bir ağa giden en iyi yol, en düşük ölçüye sahip yoldur.

Dinamik yönlendirme protokolleri, yönlendirme tablolarını oluşturmak ve güncellemek için genellikle kendi kurallarını ve ölçümlerini kullanır. Yönlendirme algoritması, ağdaki her yol için bir değer veya bir ölçü oluşturur. Metrikler, bir yolun tek bir özelliğine veya birkaç özelliğine dayalı olabilir. Bazı yönlendirme protokolleri, rota seçimini birden çok metriğe dayandırabilir ve bunları tek bir metrikte birleştirebilir.

Aşağıdaki tablo, yaygın dinamik protokolleri ve bunların ölçümlerini listeler.

| Yönlendirme Protokolü | Metrik |
|---|---|
| **Yönlendirme Bilgi Protokolü (RIP)** | • Metrik, "atlama sayısı" dır.<br>• Bir yol üzerindeki her yönlendirici, atlama sayısına bir atlama ekler.<br>• Maksimum 15 atlamaya izin verilir. |
| **Önce En Kısa Yolu Aç (OSPF)** | • Metrik, kaynaktan hedefe kümülatif bant genişliğine dayanan "maliyettir".<br>• Daha hızlı bağlantılara, daha yavaş (daha yüksek maliyetli) bağlantılara kıyasla daha düşük maliyetler atanır. |
| **Gelişmiş İç Ağ Geçidi Yönlendirme Protokolü (EIGRP)** | • En yavaş bant genişliği ve gecikme değerlerine göre bir metrik hesaplar.<br>• Metrik hesaplamaya yük ve güvenilirliği de dahil edebilir. |

### 30.4.4.Yük Dengeleme

Yönlendirme tablosunun aynı hedef ağa aynı ölçümlere sahip iki veya daha fazla yolu varsa ne olur?

Bir yönlendirici, eşit maliyet ölçülerine sahip bir hedefe giden iki veya daha fazla yola sahip olduğunda, yönlendirici paketleri her iki yolu da eşit olarak kullanarak iletir. Buna eşit maliyetli yük dengeleme denir. Yönlendirme tablosu tek hedef ağı içerir, ancak her eşit maliyet yolu için bir tane olmak üzere birden çok çıkış arayüzüne sahiptir. Yönlendirici, yönlendirme tablosunda listelenen çoklu çıkış arayüzlerini kullanarak paketleri iletir.

Doğru yapılandırılırsa, yük dengeleme ağın etkinliğini ve performansını artırabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Eşit maliyetli yük dengeleme, dinamik yönlendirme protokolleri tarafından otomatik olarak uygulanır. Farklı sonraki atlama yönlendiricileri kullanan aynı hedef ağa giden birden çok statik yol olduğunda, statik yollarla etkinleştirilir.

Not : Yalnızca EIGRP, eşit olmayan maliyet yükü dengelemesini destekler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 31.Bölüm: Statik Yönlendirme

## 31.1.Statik Rotalar

### 31.1.1.Statik Yol Türleri

Statik yollar genellikle bir ağ üzerinde uygulanır. Bu, yapılandırılmış bir dinamik yönlendirme protokolü olduğunda bile geçerlidir. Örneğin, bir kuruluş hizmet sağlayıcıya varsayılan bir statik yol yapılandırabilir ve bu yolu dinamik yönlendirme protokolünü kullanarak diğer kurumsal yönlendiricilere duyurabilir.

Statik yollar IPv4 ve IPv6 için yapılandırılabilir. Her iki protokol de aşağıdaki statik yol türlerini destekler:

- Standart statik yol
- Varsayılan (Default) statik yol
- Kayan (Floating) statik rota
- Özet (Summary) statik yol

Statik yollar, **ip route** ve **ipv6 route** genel yapılandırma komutları kullanılarak yapılandırılır.

### 31.1.2.Next-Hop Seçenekleri

Statik bir yol yapılandırırken, sonraki atlama bir IP adresi, çıkış arabirimi veya her ikisi ile tanımlanabilir. Hedefin nasıl belirtildiği aşağıdaki üç statik rota türünden birini oluşturur:

Sonraki atlama yolu - Yalnızca sonraki atlama IP adresi belirtilir
Doğrudan bağlı statik yol - Yalnızca yönlendirici çıkış arayüzü belirtilir
Tam olarak belirtilmiş statik yol - Sonraki atlama IP adresi ve çıkış arayüzü belirtilir

### 31.1.3.IPv4 Statik Route Komutu

IPv4 statik yolları, aşağıdaki genel yapılandırma komutu kullanılarak yapılandırılır:

```
Router(config)# ip route network-address subnet-mask { ip-address | exit-intf [ip-address]} [distance]
```

Not: Ya ip adresi , exit-intf veya ip adresi ve exit-intf parametreleri yapılandırılmalıdır.

Tabloda **ip route** komutu parametreleri açıklanmaktadır.

| Parametre | Açıklama |
|---|---|
| *network-address ağ adresi* | Yönlendirme tablosuna eklenecek uzak ağın hedef IPv4 ağ adresini tanımlar. |
| *subnet-mask*<br><br>*alt ağ maskesi* | Uzak ağın alt ağ maskesini tanımlar.<br><br>Alt ağ maskesi, bir ağ grubunu özetlemek ve özet bir statik yol oluşturmak için değiştirilebilir. |
| *IP adresi* | Sonraki atlama yönlendirici IPv4 adresini tanımlar.<br><br>Tipik olarak yayın ağları (yani Ethernet) ile kullanılır.<br><br>Yönlendiricinin çıkış arayüzünü bulmak için ek bir arama gerçekleştirdiği yinelemeli bir |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Parametre | Açıklama |
|---|---|
| | statik yol oluşturabilir. |
| *exit-intf* | Paketleri iletmek için çıkış arayüzünü tanımlar.<br><br>Doğrudan bağlı bir statik yol oluşturur.<br><br>Tipik olarak noktadan noktaya konfigürasyonda kullanılır. |
| *çıkış intf ip adresi* | Çıkış arabirimini ve sonraki atlama IPv4 adresini belirttiğinden tam olarak belirtilmiş bir statik yol oluşturur. |
| *distance*<br><br>*mesafe* | 1 ile 255 arasında bir idari mesafe değeri atamak için kullanılabilen isteğe bağlı komut.<br><br>Genellikle dinamik olarak öğrenilen bir rotadan daha yüksek bir yönetim mesafesi ayarlayarak kayan bir statik rota yapılandırmak için kullanılır. |

### 31.1.4.IPv6 Statik Route Komutu

IPv6 statik yolları, aşağıdaki genel yapılandırma komutu kullanılarak yapılandırılır:

```
Router(config)# ipv6 route ipv6-prefix/prefix-length {ipv6-address | exit-intf [ipv6-address]}
[distance]
```

Parametrelerin çoğu, komutun IPv4 sürümüyle aynıdır.

Tablo, çeşitli **ipv6 route** komutu parametrelerini ve açıklamalarını gösterir.

| Parametre | Açıklama |
|---|---|
| *ipv6 öneki* | Yönlendirme tablosuna eklenecek uzak ağın hedef IPv6 ağ adresini tanımlar. |
| */ önek uzunluğu* | Uzak ağın önek uzunluğunu tanımlar. |
| *ipv6 adresi* | Sonraki atlama yönlendirici IPv6 adresini tanımlar.<br><br>Tipik olarak yayın ağlarıyla (yani Ethernet) kullanılır<br><br>Yönlendiricinin çıkış arayüzünü bulmak için ek bir arama gerçekleştirdiği yinelemeli bir statik yol oluşturabilir. |
| *exit-intf* | Paketleri iletmek için çıkış arayüzünü tanımlar.<br><br>Doğrudan bağlı bir statik yol oluşturur.<br><br>Tipik olarak noktadan noktaya konfigürasyonda kullanılır. |
| *exit-intf ipv6-adresi* | Çıkış arabirimini ve sonraki atlama IPv6 adresini belirttiğinden tam olarak belirtilmiş bir statik yol oluşturur. |
| *mesafe* | 1 ile 255 arasında bir idari mesafe değeri atamak için kullanılabilen isteğe bağlı komut. |

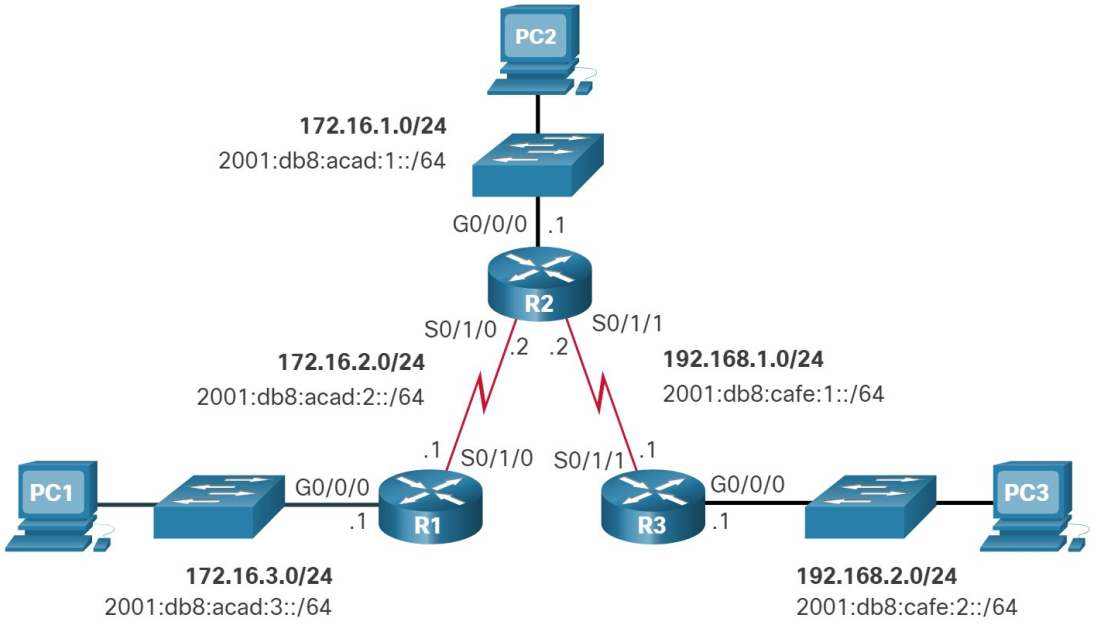
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Parametre | Açıklama |
|---|---|
| | Genellikle dinamik olarak öğrenilen bir rotadan daha yüksek bir yönetim mesafesi ayarlayarak kayan bir statik rota yapılandırmak için kullanılır. |

**Not : ipv6 unicast-routing genel yapılandırma komutu, yönlendiricinin IPv6 paketlerini iletmesini sağlamak için MUTLAKA yapılandırılmalıdır.**

## 31.1.5.Çift Yığın (Dual Stack) Topolojisi

Şekil, çift yığınlı bir ağ topolojisini göstermektedir. Şu anda IPv4 veya IPv6 için hiçbir statik yol yapılandırılmamıştır. Bundan sonra göreceğiniz bütün yapılandırmalar bu topoloji üzerinde gerçekleşir.




R1 yönlendiricisine ait yönlendirme tablosu çıktısı şekilde gösterilmiştir. Diğerleri de benzerdir. Bilgisayarlar birbirine ping atamamaktadır.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.1/32 is directly connected, Serial0/1/0
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
R1#
```

R1 yönlendiricisine ait IPv6 yönlendirme tablosu çıktısı şekilde gösterilmiştir. Diğerleri de benzerdir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# show ipv6 route | begin C
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/1/0, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

Show çıktılarından anlaşılacağı üzere her yönlendiricide sadece direkt (C) bağlı rotalar bulunmaktadır.

## 31.2.Statik Rotaları Yapılandırma

### 31.2.1.IPv4 Sonraki Atlamalı (Next-Hop ) Statik Yol

Standart statik yolları yapılandırma komutları, IPv4 ve IPv6 arasında biraz farklılık gösterir. Bu konu, hem IPv4 hem de Ipv6 için standart sonraki atlama, doğrudan bağlı ve tam olarak belirtilen statik yolları nasıl yapılandıracağınızı gösterir.

Sonraki atlama statik rotasında, yalnızca sonraki atlama IP adresi belirtilir. Çıkış arayüzü, bir sonraki atlamadan türetilir. Örneğin, sonraki atlama olan R2 IP adresi kullanılarak R1'de sonraki atlama IPv4 statik yolu yapılandırılır.

R1 yönlendiricisinden üç uzak ağa IPv4 statik yollarıyla yapılandırma komutları aşağıdaki gibidir:

```
R1(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 172.16.2.2
```

R1 için yönlendirme tablosunda artık üç uzak IPv4 ağına giden yollar vardır.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.1/32 is directly connected, Serial0/1/0
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 [1/0] via 172.16.2.2
S     192.168.2.0/24 [1/0] via 172.16.2.2

R1#
```

### 31.2.2.IPv6 Sonraki Atlamalı Statik Yol

R1 yönlendiricisinden üç uzak ağa IPv6 statik yollarıyla yapılandırma komutları aşağıdaki gibidir:

```
R1(config)# ipv6 unicast-routing
R1(config)# ipv6 route 2001:db8:acad:1::/64 2001:db8:acad:2::2
R1(config)# ipv6 route 2001:db8:cafe:1::/64 2001:db8:acad:2::2
R1(config)# ipv6 route 2001:db8:cafe:2::/64 2001:db8:acad:2::2
```

R1 için yönlendirme tablosunda artık üç uzak IPv6 ağına giden yollar vardır.

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S   2001:DB8:ACAD:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/1/0, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
S   2001:DB8:CAFE:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
S   2001:DB8:CAFE:2::/64 [1/0]
     via 2001:DB8:ACAD:2::2
L   FF00::/8 [0/0]
     via Null0, receive
```

## 31.2.3.IPv4 Doğrudan Bağlı Statik Yol

Çıkış arabirimi kullanılarak R1 üzerinde doğrudan bağlı üç IPv4 statik yol yapılandırılır.

```
R1(config)# ip route 172.16.1.0 255.255.255.0 s0/1/0
R1(config)# ip route 192.168.1.0 255.255.255.0 s0/1/0
R1(config)# ip route 192.168.2.0 255.255.255.0 s0/1/0
```

R1 için IPv4 yönlendirme tablosu, bir paket 192.168.2.0/24 ağı için hedeflendiğinde, R1'in yönlendirme tablosunda bir eşleşme aradığını ve paketi Seri 0/1/0 arayüzünden iletebileceğini bulduğunu gösterir. .

Not : Bir sonraki atlama adresinin kullanılması genellikle önerilir. Doğrudan bağlı statik yollar, bu örnekte olduğu gibi yalnızca noktadan noktaya seri arabirimlerle kullanılmalıdır.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 is directly connected, Serial0/1/0
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.1/32 is directly connected, Serial0/1/0
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 is directly connected, Serial0/1/0
S     192.168.2.0/24 is directly connected, Serial0/1/0
```

## 31.2.4.IPv6 Doğrudan Bağlı Statik Yol

Örnekte, çıkış arabirimi kullanılarak R1'de doğrudan bağlı üç IPv6 statik yolu yapılandırılmıştır.

```
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0
R1(config)# ipv6 route 2001:db8:cafe:1::/64 s0/1/0
R1(config)# ipv6 route 2001:db8:cafe:2::/64 s0/1/0
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Örnek çıktıdaki R1 için IPv6 yönlendirme tablosu, 2001: db8: cafe: 2 :: / 64 ağı için bir paket hedeflendiğinde, R1'in yönlendirme tablosunda bir eşleşme aradığını ve paketi Seri 0/1/0 arayüzünden dışarı iletebileceğini bulur.

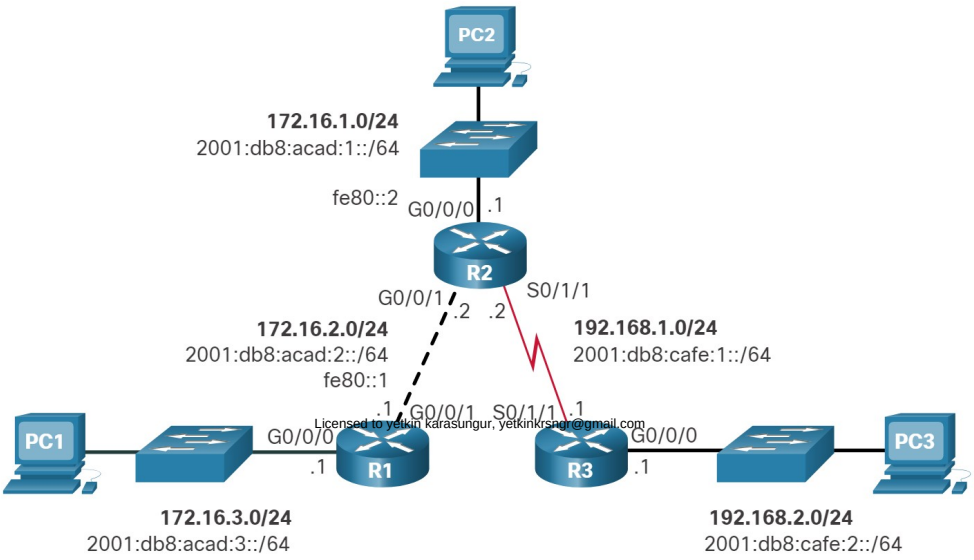
Not : Bir sonraki atlama adresinin kullanılması genellikle önerilir. Doğrudan bağlı statik yollar, bu örnekte olduğu gibi yalnızca noktadan noktaya seri arabirimlerle kullanılmalıdır.

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S   2001:DB8:ACAD:1::/64 [1/0]
     via Serial0/1/0, directly connected
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/1/0, receive
C   2001:DB8:ACAD:3::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:3::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
S   2001:DB8:CAFE:1::/64 [1/0]
     via Serial0/1/0, directly connected
S   2001:DB8:CAFE:2::/64 [1/0]
     via Serial0/1/0, directly connected
L   FF00::/8 [0/0]
     via Null0, receiveIPv6 Routing Table - default - 8 entries
R1#
```

## 31.2.5.IPv4 Tam Belirtilmiş (Fully Specified) Statik Yönlendirme

Tam olarak belirtilmiş bir statik yolda, hem çıkış arayüzü hem de sonraki atlama IP adresi belirtilir. Bu statik yol biçimi, çıkış arabirimi bir çoklu erişim arabirimi olduğunda ve bir sonraki sıçramayı açıkça tanımlamak gerektiğinde kullanılır. Bir sonraki atlama, belirtilen çıkış arayüzüne doğrudan bağlanmalıdır. Bir çıkış arabirimi kullanmak isteğe bağlıdır, ancak bir sonraki atlama adresi kullanmak gerekir.

R1 ve R2 arasındaki ağ bağlantısının bir Ethernet bağlantısı olduğunu ve R1'in GigabitEthernet 0/0/1 arayüzünün şekilde gösterildiği gibi bu ağa bağlı olduğunu varsayalım.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Ethernet çoklu erişim ağı ile noktadan noktaya seri ağ arasındaki fark, bir noktadan noktaya seri ağın o ağda yalnızca bir başka aygıta sahip olmasıdır; yönlendirici, bağlantının diğer ucundadır. Ethernet ağları ile, ana bilgisayarlar ve hatta birden çok yönlendirici dahil olmak üzere aynı çoklu erişim ağını paylaşan birçok farklı cihaz olabilir.

Çıkış arabirimi bir Ethernet ağı olduğunda, statik yolun bir sonraki atlama adresi içermesi önerilir. Hem çıkış arabirimini hem de sonraki atlama adresini içeren tam olarak belirtilmiş bir statik yol da kullanabilirsiniz.

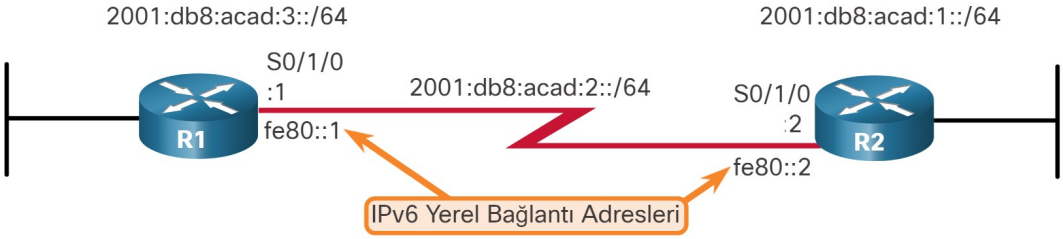
```
R1(config)# ip route 172.16.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
R1(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 0/0/1 172.16.2.2
```

Paketleri R2'ye iletirken, çıkış arabirimi GigabitEthernet 0/0/1 ve sonraki atlama IPv4 adresi, R1'den **show ip route** gösterme çıktısında gösterildiği gibi 172.16.2.2'dir .

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
C        172.16.2.0/24 is directly connected, GigabitEthernet0/0/1
L        172.16.2.1/32 is directly connected, GigabitEthernet0/0/1
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
S     192.168.2.0/24 [1/0] via 172.16.2.2, GigabitEthernet0/0/1
```

## 31.2.6.IPv6 Tam Olarak Belirtilmiş Statik Yol

Tam olarak belirtilmiş bir IPv6 statik yolunda, hem çıkış arabirimi hem de sonraki atlama IPv6 adresi belirtilir. IPv6'da tam olarak belirtilmiş bir statik yolun kullanılması gereken bir durum vardır. IPv6 statik yolu, sonraki atlama adresi olarak bir IPv6 bağlantı yerel adresi kullanıyorsa, tam olarak belirtilmiş bir statik yol kullanın. Şekil, sonraki atlama adresi olarak bir IPv6 bağlantı yerel adresini kullanan tam olarak belirtilmiş bir IPv6 statik yolunun bir örneğini gösterir.




```
R1(config)# ipv6 route 2001:db8:acad:1::/64 fe80::2
%Interface has to be specified for a link-local nexthop
R1(config)# ipv6 route 2001:db8:acad:1::/64 s0/1/0 fe80::2
```

Örnekte, tam olarak belirtilmiş bir statik yol, sonraki atlama adresi olarak R2'nin bağlantı yerel adresi kullanılarak yapılandırılır. IOS'un bir çıkış arayüzünün belirtilmesini gerektirdiğine dikkat edin.

Tam olarak belirtilmiş bir statik yolun kullanılması gerekmesinin nedeni, IPv6 bağlantı yerel adreslerinin IPv6 yönlendirme tablosunda yer almamasıdır. Yerel bağlantı adresleri yalnızca belirli bir bağlantı veya ağda

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

benzersizdir. Sonraki atlama yerel bağlantı adresi, yönlendiriciye bağlı birden çok ağda geçerli bir adres olabilir. Bu nedenle, çıkış arayüzünün dahil edilmesi gerekir.

Aşağıdaki örnek, bu yol için IPv6 yönlendirme tablosu girişini gösterir. Hem sonraki atlama yerel bağlantı adresinin hem de çıkış arayüzünün dahil edildiğine dikkat edin.

```
R1# show ipv6 route static | begin 2001:db8:acad:1::/64
S   2001:DB8:ACAD:1::/64 [1/0]
    via FE80::2, Seria0/1/0
```

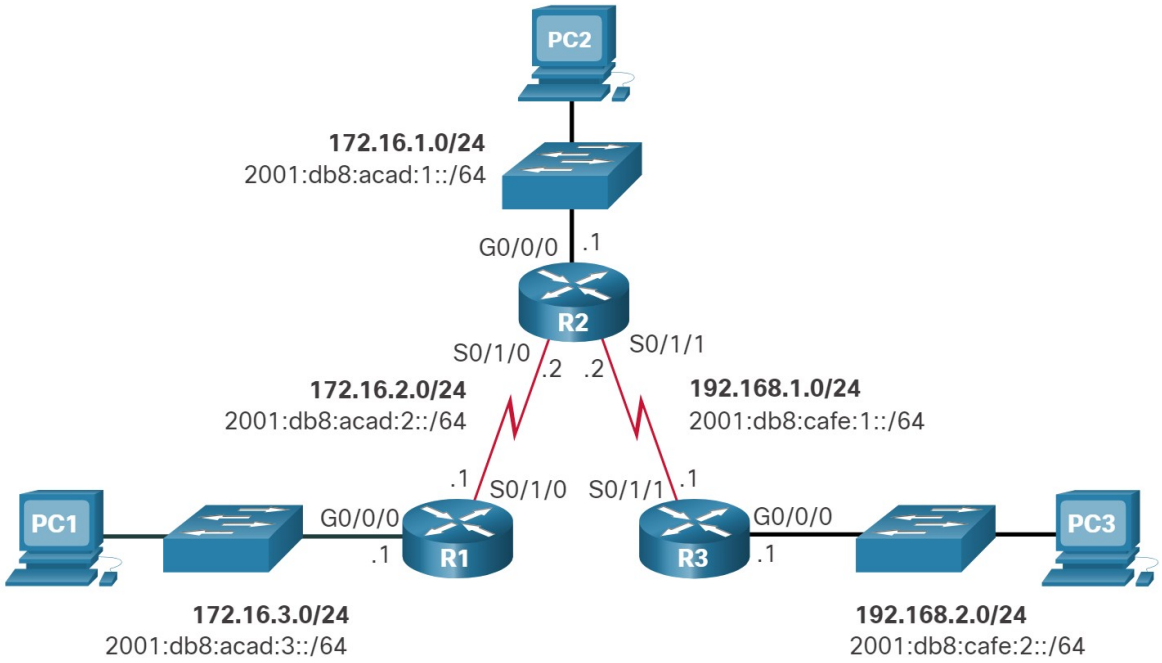
## 31.2.7.Yapılandırmaların Doğrulanması

Statik rota yapılandırmlarını doğrulamak için aşağıdaki komutlar kullanılır.

- **show ip route static**
- **show ip route** *network*
- **show running-config | section ip route**

**IPv6 statik rota yapılandırmalarını doğrulamak için komutlara v6 eklenmelidir.**

Komut örneklerini incelerken aşağıdaki şekle bakın.




### Yalnızca IPv4 Statik Yollarını Görüntüleme

Bu çıktı, yönlendirme tablosunda yalnızca IPv4 statik yollarını gösterir. Ayrıca, tüm kodlar hariç filtrenin çıktıyı nerede başlattığını da not edin.

```
R1# show ip route static | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2
S     192.168.1.0/24 [1/0] via 172.16.2.2
S     192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Belirli Bir IPv4 Ağını Görüntüleme

Bu komut, yönlendirme tablosunda yalnızca belirtilen ağ için çıktıyı gösterecektir.

```
R1# show ip route 192.168.2.1
Routing entry for 192.168.2.0/24
  Known via "static", distance 1, metric 0
  Routing Descriptor Blocks:
  * 172.16.2.2
      Route metric is 0, traffic share count is 1
R1#
```

### IPv4 Statik Yol Yapılandırmasını Görüntüleme

Bu komut, çalışan yapılandırmayı yalnızca IPv4 statik yolları için filtreler.

```
R1# show running-config | section ip route
ip route 172.16.1.0 255.255.255.0 172.16.2.2
ip route 192.168.1.0 255.255.255.0 172.16.2.2
ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1#
```

### Yalnızca IPv6 Statik Yollarını Görüntüleme

Bu çıktı, yönlendirme tablosunda yalnızca IPv6 statik yollarını gösterir. Ayrıca, tüm kodlar hariç filtrenin çıktıyı nerede başlattığını da not edin.

```
R1# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S   2001:DB8:ACAD:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
S   2001:DB8:CAFE:1::/64 [1/0]
     via 2001:DB8:ACAD:2::2
S   2001:DB8:CAFE:2::/64 [1/0]
     via 2001:DB8:ACAD:2::2
R1#
```

### Belirli Bir IPv6 Ağını Görüntüleme

Bu komut, yönlendirme tablosunda yalnızca belirtilen ağ için çıktıyı gösterecektir.

```
R1# show ipv6 route 2001:db8:cafe:2::
Routing entry for 2001:DB8:CAFE:2::/64
  Known via "static", distance 1, metric 0
  Route count is 1/1, share count 0
  Routing paths:
    2001:DB8:ACAD:2::2
      Last updated 00:23:55 ago

R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### IPv6 Statik Yol Yapılandırmasını Görüntüleme

Bu komut, çalışan yapılandırmayı yalnızca IPv6 statik yolları için filtreler.

```
R1# show running-config | section ipv6 route
ipv6 route 2001:DB8:ACAD:1::/64 2001:DB8:ACAD:2::2
ipv6 route 2001:DB8:CAFE:1::/64 2001:DB8:ACAD:2::2
ipv6 route 2001:DB8:CAFE:2::/64 2001:DB8:ACAD:2::2
R1#
```

## 31.3.IP Varsayılan Statik Yollarını Yapılandırma

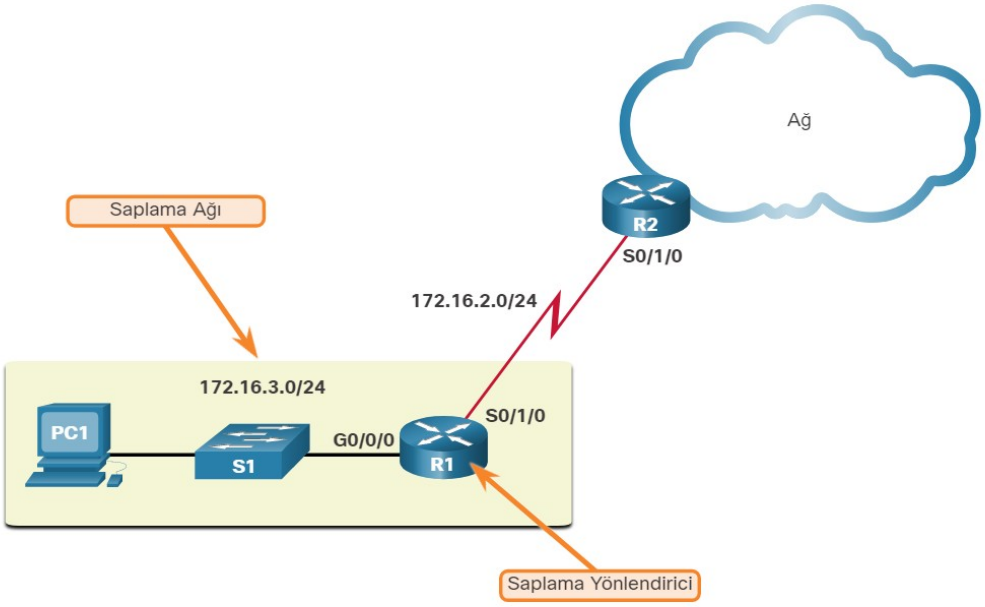
### 31.3.1.Varsayılan Statik Yol (Default Route)

Bu konu, IPv4 ve IPv6 için varsayılan bir yolu nasıl yapılandıracağınızı gösterir. Ayrıca varsayılan bir rotanın iyi bir seçim olduğu durumları da açıklar. Varsayılan bir yol, tüm paketlerle eşleşen statik bir yoldur. Yönlendiriciler, internetteki tüm ağlar için yolları depolamak yerine, yönlendirme tablosunda olmayan herhangi bir ağı temsil etmek için tek bir varsayılan yol depolayabilirler.

Yönlendiriciler genellikle yerel olarak yapılandırılan veya dinamik bir yönlendirme protokolü kullanarak başka bir yönlendiriciden öğrenilen varsayılan yolları kullanır. Varsayılan bir yol, varsayılan yol ile hedef IP adresi arasında herhangi bir en sol bitin eşleşmesini gerektirmez. Yönlendirme tablosundaki başka hiçbir yol, paketin hedef IP adresi ile eşleşmediğinde varsayılan bir yol kullanılır. Diğer bir deyişle, daha spesifik bir eşleşme yoksa, o zaman varsayılan yol Son Çare Ağ Geçidi olarak kullanılır.

Varsayılan statik yollar, bir uç yönlendiriciyi bir servis sağlayıcı ağına veya bir saplama (Stub) yönlendiricisine (yalnızca bir yukarı akış komşu yönlendiriciye sahip bir yönlendirici) bağlarken yaygın olarak kullanılır.

Şekilde tipik bir varsayılan statik yol senaryosu gösterilmektedir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

R1'in yalnızca doğrudan bağlı ağları bilmesi gerekir. Diğer tüm ağlar için R2'ye işaret eden varsayılan bir statik yol kullanabilir.

### IPv4 Varsayılan Statik Yol

IPv4 Varsayılan statik yol için komut sözdizimi ağ adresi olması dışında, başka herhangi bir IPv4 statik yol benzerdir 0.0.0.0 ve alt ağ maskesi 0.0.0.0 . Rotadaki 0.0.0.0 0.0.0.0, herhangi bir ağ adresiyle eşleşecektir.

Not : Bir IPv4 varsayılan statik yol, genellikle dört sıfırlı yol olarak adlandırılır.

Bir IPv4 varsayılan statik yolu için temel komut sözdizimi aşağıdaki gibidir:

```
Router(config)# ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

### IPv6 Varsayılan Statik Yol

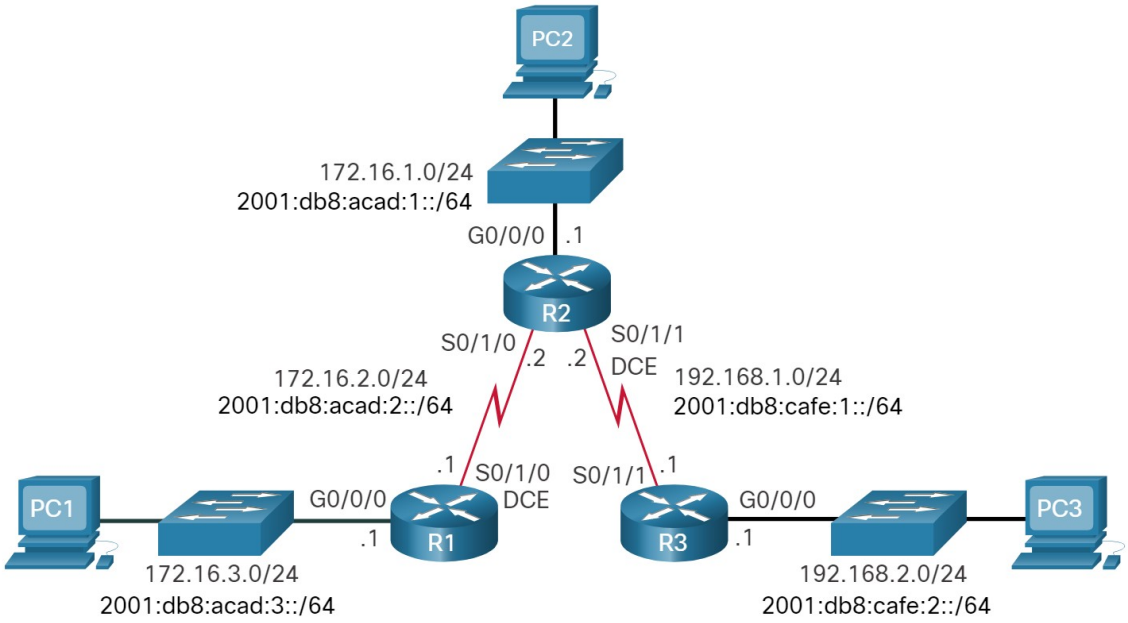
Bir IPv6 varsayılan statik yolunun komut sözdizimi , tüm yollarla eşleşen ipv6 önek / önek uzunluğunun :: / 0 olması dışında diğer herhangi bir IPv6 statik yoluna benzer .

Bir IPv6 varsayılan statik yolu için temel komut sözdizimi aşağıdaki gibidir:

```
Router(config)# ipv6 route ::/0 {ipv6-address | exit-intf}
```

## 31.3.2.Varsayılan Statik Yönlendirme Yapılandırma

Şekilde, R1, örnek topolojideki uzak ağların her birine ulaşmak için üç statik yol ile yapılandırılabilir. Ancak, R1 bir saplama yönlendiricidir çünkü yalnızca R2'ye bağlıdır. Bu nedenle, tek bir varsayılan statik yol yapılandırmak daha verimli olacaktır.




Örnek, R1'de yapılandırılmış bir IPv4 varsayılan statik yolunu gösterir. Örnekte gösterilen konfigürasyonla, daha spesifik yol girişleriyle eşleşmeyen herhangi bir paket, 172.16.2.2'de R2'ye iletilir.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bir IPv6 varsayılan statik yolu, benzer şekilde yapılandırılır. Bu yapılandırmayla, daha spesifik IPv6 yol girişleriyle eşleşmeyen paketler, 2001: db8: acad: 2 :: 2'de R2'ye iletilir.

```
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
```

## 31.3.3. Varsayılan Statik Yolu Doğrulama

### IPv4 Varsayılan Statik Yolunu Doğrulama

**show ip route static** komut çıktısı R1 den yönlendirme tablosundaki statik yolları içeriğini görüntüler. Rotanın yanındaki 'S' kodlu yıldız işaretine ( * ) dikkat edin. Show ip route çıktısındaki kodlar tablosunda gösterildiği gibi yıldız işareti, bu statik rotanın aday bir varsayılan rota olduğunu belirtir ve bu nedenle, Gateway of Last Resort olarak seçilmiştir.

```
R1# show ip route static
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 172.16.2.2

R1#
```

### IPv6 Varsayılan Statik Yolunu Doğrulayın

Bu örnek, yönlendirme tablosunun içeriğini görüntülemek için **show ipv6 route static** komut çıktısını gösterir.

```
R1# show ipv6 route static
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       a - Application
S   ::/0 [1/0]
     via 2001:DB8:ACAD:2::2

R1#
```

Statik varsayılan yol yapılandırmasının IPv4 varsayılan yolları için / 0 maskesini ve IPv6 varsayılan yolları için :: / 0 önekini kullandığına dikkat edin. Bir yönlendirme tablosundaki IPv4 alt ağ maskesinin ve IPv6 önek uzunluğunun, paketin hedef IP adresi ile yönlendirme tablosundaki yol arasında kaç bit eşleşmesi gerektiğini belirlediğini unutmayın. A / 0 maskesi veya :: / 0 öneki, bitlerin hiçbirinin eşleşmesi için gerekli olmadığını gösterir. Daha spesifik bir eşleşme olmadığı sürece, varsayılan statik yol tüm paketlerle eşleşir.

## 31.4.Kayan Statik Yolları Yapılandırma (Floating Static Routes)

### 31.4.1.Kayan Statik Yollar

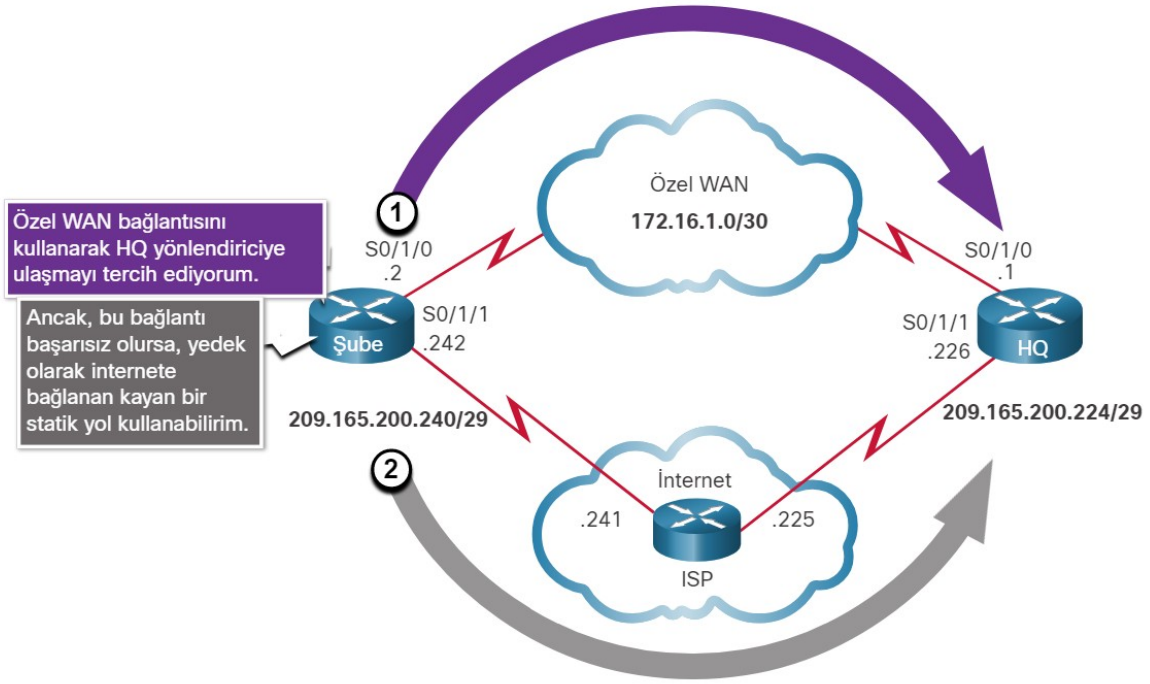
Bu bölümdeki diğer konularda olduğu gibi, IPv4 ve IPv6 kayan statik yolları nasıl yapılandıracağınızı ve bunları ne zaman kullanacağınızı öğreneceksiniz.

Diğer bir statik rota türü, kayan statik rotadır. Kayan statik yollar, bir bağlantı hatası durumunda birincil statik veya dinamik yola yedek yol sağlamak için kullanılan statik rotalardır. Kayan statik rota, yalnızca birincil rota mevcut olmadığında kullanılır.

Bunu başarmak için, kayan statik yol, birincil yoldan daha yüksek bir idari mesafe ile yapılandırılır. İdari mesafe, bir rotanın güvenilirliğini temsil eder. Hedefe giden birden fazla yol varsa, yönlendirici en düşük yönetim mesafesine sahip yolu seçecektir.

Örneğin, bir yöneticinin EIGRP ile öğrenilen bir yola yedek olarak kayan bir statik yol oluşturmak istediğini varsayalım. Kayan statik yol, EIGRP'den daha yüksek bir yönetim mesafesi ile yapılandırılmalıdır. EIGRP, 90'lık bir idari mesafeye sahiptir. Kayan statik yol, 95'lik bir idari mesafe ile konfigüre edilirse, EIGRP aracılığıyla öğrenilen dinamik yol, kayan statik yola tercih edilir. EIGRP ile öğrenilen rota kaybolursa, onun yerine kayan statik rota kullanılır.

Şekilde, şube yönlendiricisi tipik olarak tüm trafiği özel WAN bağlantısı üzerinden HQ yönlendiricisine iletir. Bu örnekte, yönlendiriciler EIGRP kullanarak yol bilgisini değiştirirler. Yönetim mesafesi 91 veya daha yüksek olan bir kayan statik yol, bir yedek yol olarak hizmet verecek şekilde yapılandırılabilir. Özel WAN bağlantısı başarısız olursa ve EIGRP yolu yönlendirme tablosundan kaybolursa, yönlendirici kayan statik yolu HQ LAN'a ulaşmak için en iyi yol olarak seçer.




1. Dinamik yönlendirme yoluyla öğrenilen bir rota tercih edilir.
2. Dinamik bir rota kaybedilirse, kayan statik rota kullanılacaktır.

Varsayılan olarak, statik rotaların yönetim mesafesi 1'dir, bu da onları dinamik yönlendirme protokollerinden öğrenilen rotalara göre tercih edilebilir kılar. Örneğin, bazı yaygın iç ağ geçidi dinamik yönlendirme protokollerinin idari mesafeleri şunlardır:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

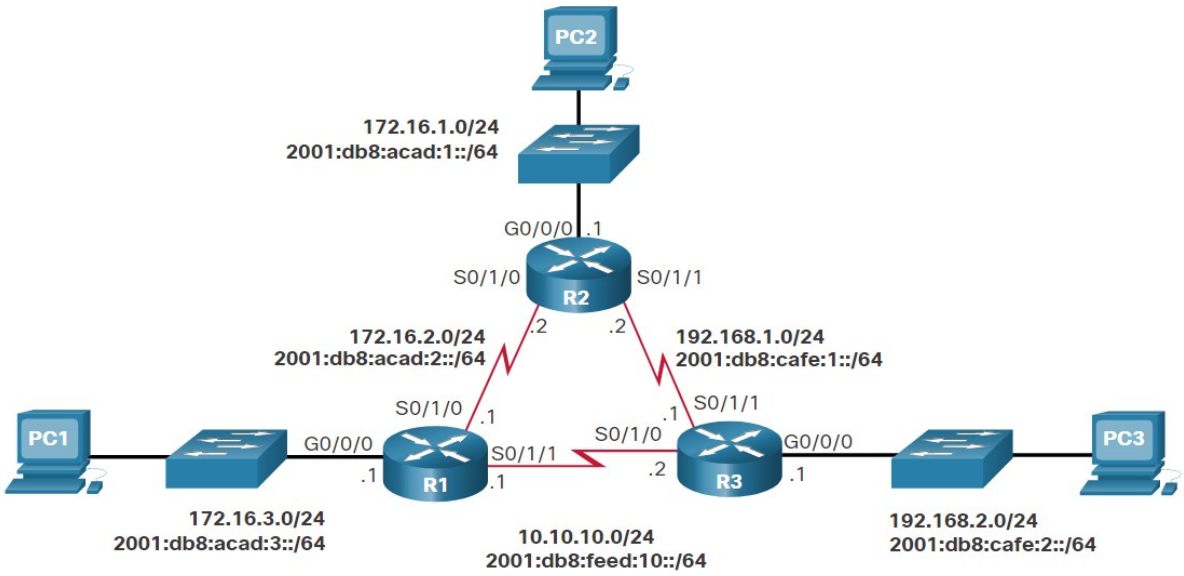
- EIGRP = 90
- OSPF = 110
- IS-IS = 115

Statik bir rotanın idari mesafesi, rotayı başka bir statik rotadan veya dinamik bir yönlendirme protokolü aracılığıyla öğrenilen bir rotadan daha az arzu edilir kılmak için artırılabilir. Bu şekilde, statik rota "kayar" ve daha iyi idari mesafeye sahip rota etkin olduğunda kullanılmaz. Bununla birlikte, tercih edilen rota kaybedilirse, kayan statik rota devralabilir ve trafik bu alternatif rota üzerinden gönderilebilir.

## 31.4.2.IPv4 ve IPv6 Kayan Statik Yollarını Yapılandırma

IP kayan statik yollar, bir yönetim mesafesi belirtmek için **distance** bağımsız değişkeni kullanılarak yapılandırılır . Yönetim mesafesi yapılandırılmamışsa, varsayılan değer (1) kullanılır.

Şekildeki topolojiye ve R1'de verilen **ip route** ve **ipv6 route** komutlarına bakın. Bu senaryoda, R1'den tercih edilen varsayılan yol R2'dir. R3 bağlantısı yalnızca yedekleme için kullanılmalıdır.




```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)# ipv6 route ::/0 2001:db8:acad:2::2
R1(config)# ipv6 route ::/0 2001:db8:feed:10::2 5
```

R1, R2'yi işaret eden IPv4 ve IPv6 varsayılan statik yollarla yapılandırılmıştır. Hiçbir yönetim mesafesi yapılandırılmadığından, bu statik yollar için varsayılan değer (1) kullanılır. R1 ayrıca, yönetim mesafesi 5 olan R3'e işaret eden IPv4 ve IPv6 kayan statik varsayılan yollarla yapılandırılmıştır. Bu değer, varsayılan değer olan 1'den daha büyüktür ve bu nedenle; bu yol yüzer ve tercih edilen yol başarısız olmadıkça yönlendirme tablosunda mevcut değildir.

**show ip route** ve **show ipv6 route** komutları R2 için varsayılan yollar yönlendirme tablosunu doğrular. R3'e giden IPv4 kayan statik yolunun yönlendirme tablosunda bulunmadığını unutmayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# show ip route static | begin Gateway
Gateway of last resort is 172.16.2.2 to network 0.0.0.0

S*   0.0.0.0/0 [1/0] via 172.16.2.2
R1# show ipv6 route static | begin S :
S   ::/0 [1/0]
     via 2001:DB8:ACAD:2::2
R1#
```

Kayan statik yolların yapılandırmada olduğunu doğrulamak için **show run** komutunu kullanın. Örneğin, aşağıdaki komut çıktısı, her iki IPv6 statik varsayılan yolunun da çalışan yapılandırmada olduğunu doğrular.

```
R1# show run | include ipv6 route
ipv6 route ::/0 2001:db8:feed:10::2 5
ipv6 route ::/0 2001:db8:acad:2::2
R1#
```

### 31.4.3.Kayan Statik Rotayı Test Etme

Topolojiye göre  R2 başarısız olursa yani o yolda bir arıza gerçekleşirse ne olur?

Bu arızayı simüle etmek için, konfigürasyonda gösterildiği gibi R2'nin her iki seri arayüzü de kapatılır.

```
R2(config)# interface s0/1/0
R2(config-if)# shut
*Sep 18 23:36:27.000: %LINK-5-CHANGED: Interface Serial0/1/0, changed state to administratively down
*Sep 18 23:36:28.000: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
R2(config-if)# interface s0/1/1
R2(config-if)# shut
*Sep 18 23:36:41.598: %LINK-5-CHANGED: Interface Serial0/1/1, changed state to administratively down
*Sep 18 23:36:42.598: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/1, changed state to down
```

R1'in otomatik olarak R2'ye giden seri arayüzün çalışmadığını belirten mesajlar oluşturduğuna dikkat edin.

```
R1#
*Sep 18 23:35:48.810: %LINK-3-UPDOWN: Interface Serial0/1/0, changed state to down
R1#
*Sep 18 23:35:49.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down
R1#
```

R1'in IP yönlendirme tablolarına bir bakış, kayan statik varsayılan yolların artık varsayılan yollar olarak kurulduğunu ve sonraki atlama yönlendiricisi olarak R3'ü işaret ettiğini doğrular.

```
R1# show ip route static | begin Gateway
Gateway of last resort is 10.10.10.2 to network 0.0.0.0
S*    0.0.0.0/0 [5/0] via 10.10.10.2
R1# show ipv6 route static | begin ::
S   ::/0 [5/0]
     via 2001:DB8:FEED:10::2
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 31.5.Statik Host Rotalarını Yapılandırma

### 31.5.1.Host Rotaları

Ana bilgisayar yolu (Host Route), 32 bit maskeli bir IPv4 adresidir veya 128 bit maskeli bir IPv6 adresidir. Aşağıda, yönlendirme tablosuna bir ana makine yolunun eklenmesinin üç yolu gösterilmektedir:

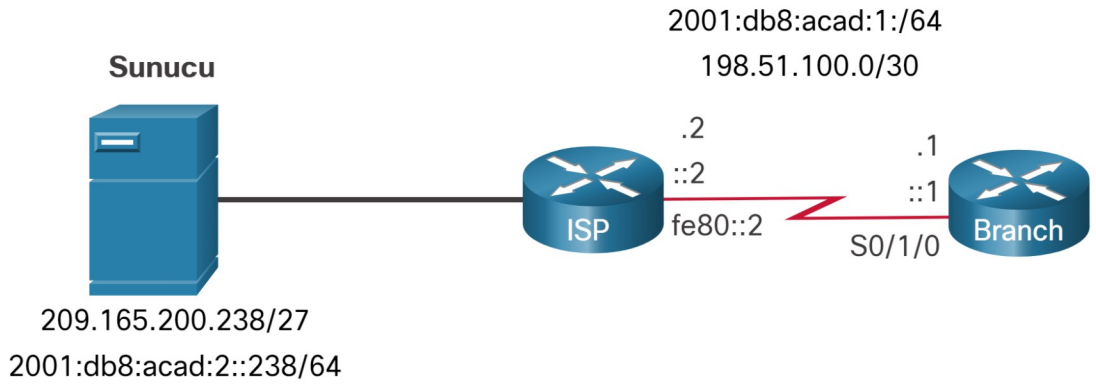
- Yönlendiricide bir IP adresi yapılandırıldığında otomatik olarak kurulur (şekillerde gösterildiği gibi)
- Statik ana bilgisayar yolu olarak yapılandırılır
- Diğer yöntemlerle otomatik olarak elde edilen ana bilgisayar yolu (sonraki bölümlerde açıklanmıştır)

### 31.5.2.Otomatik Olarak Yüklenen Ana Makine Yolları

Cisco IOS, yönlendiricide bir arabirim adresi yapılandırıldığında, yerel ana makine yolu olarak da bilinen bir ana bilgisayar yolunu otomatik olarak yükler. Bir ana bilgisayar yolu, paket iletme yerine yönlendiricinin kendisine yönlendirilen paketler için daha verimli bir işlem sağlar. Bu, arabirimin ağ adresi için yönlendirme tablosunda bir **C** ile gösterilen bağlı yola ilavedir .

Bir yönlendiricideki aktif bir arabirim bir IP adresiyle yapılandırıldığında, yönlendirme tablosuna otomatik olarak yerel bir ana bilgisayar yolu eklenir. Yerel yollar , yönlendirme tablosunun çıktısında **L** ile işaretlenir .

Örneğin, şekildeki topolojiye bakın.



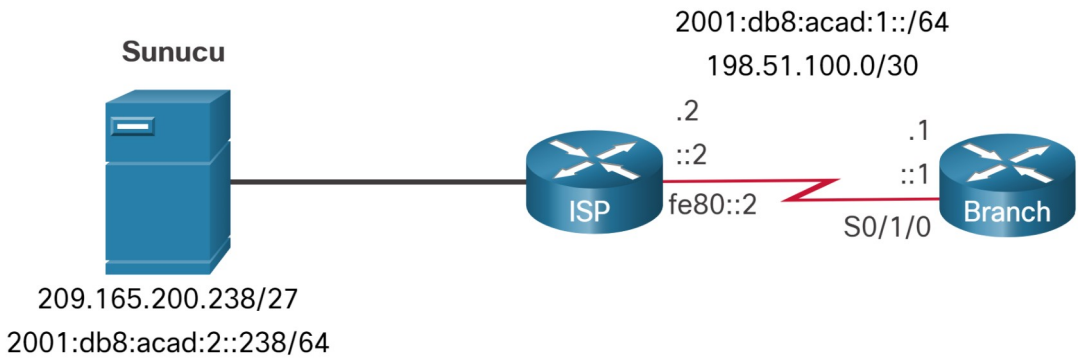

Branch Seri0 / 1/0 arayüzüne atanan IP adresleri 198.51.100.1/30 ve 2001: db8: acad: 1 :: 1/64'tür. Arayüz için yerel yollar, örnekte gösterildiği gibi IPv4 ve IPv6 yönlendirme tablolarında IOS tarafından kurulur.

```
Branch# show ip route | begin Gateway
Gateway of last resort is not set
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, Serial0/1/0
L        198.51.100.1/32 is directly connected, Serial0/1/0
Branch# show ipv6 route | begin ::
C   2001:DB8:ACAD:1::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via Serial0/1/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 31.5.3.Statik Ana Bilgisayar Yolları

Ana makine yolu (host route), trafiği şekilde gösterilen sunucu gibi belirli bir hedef cihaza yönlendirmek için manuel olarak yapılandırılmış bir statik yol olabilir. Statik yol, bir hedef IP adresi ve IPv4 ana makine yolları için 255.255.255.255 (/ 32) maske ve IPv6 ana bilgisayar yolları için bir / 128 ön ek uzunluğu kullanır.




### Statik Ana Bilgisayar Yönlendirmelerini Yapılandırma

Örnek, sunucuya erişmek için Branch yönlendiricisindeki IPv4 ve IPv6 statik ana bilgisayar yolu yapılandırmasını gösterir.

```
Branch(config)# ip route 209.165.200.238 255.255.255.255 198.51.100.2
Branch(config)# ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2
Branch(config)# exit
Branch#
```

### Statik Ana Bilgisayar Yönlendirmelerini Doğrulama

Hem IPv4 hem de IPv6 yönlendirme tablolarının incelenmesi, rotaların etkin olduğunu doğrular.

```
Branch# show ip route | begin Gateway
Gateway of last resort is not set
      198.51.100.0/24 is variably subnetted, 2 subnets, 2 masks
C        198.51.100.0/30 is directly connected, Serial0/1/0
L        198.51.100.1/32 is directly connected, Serial0/1/0
      209.165.200.0/32 is subnetted, 1 subnets
S        209.165.200.238 [1/0] via 198.51.100.2
Branch# show ipv6 route
(Output omitted)
C   2001:DB8:ACAD:1::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via Serial0/1/0, receive
S   2001:DB8:ACAD:2::238/128 [1/0]
     via 2001:DB8:ACAD:1::2
Branch#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 31.5.4.Link-Local Next-Hop ile IPv6 Statik Ana Bilgisayar Rotasını Yapılandırma

IPv6 statik yolları için sonraki atlama adresi, bitişik yönlendiricinin bağlantı yerel adresi olabilir. Bununla birlikte, örnekte gösterildiği gibi, bir sonraki atlama olarak bir yerel bağlantı adresi kullanırken bir arabirim türü ve bir arabirim numarası belirtmelisiniz. İlk olarak, orijinal IPv6 statik ana makine yolu kaldırılır, ardından sunucunun IPv6 adresi ve ISP yönlendiricisinin IPv6 bağlantı-yerel adresi ile yapılandırılmış tam olarak belirlenmiş bir yol.

```
Branch(config)# no ipv6 route 2001:db8:acad:2::238/128 2001:db8:acad:1::2
Branch(config)# ipv6 route 2001:db8:acad:2::238/128 serial 0/1/0 fe80::2
Branch# show ipv6 route | begin ::
C   2001:DB8:ACAD:1::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via Serial0/1/0, receive
S   2001:DB8:ACAD:2::238/128 [1/0]
     via FE80::2, Serial0/1/0
Branch#
```

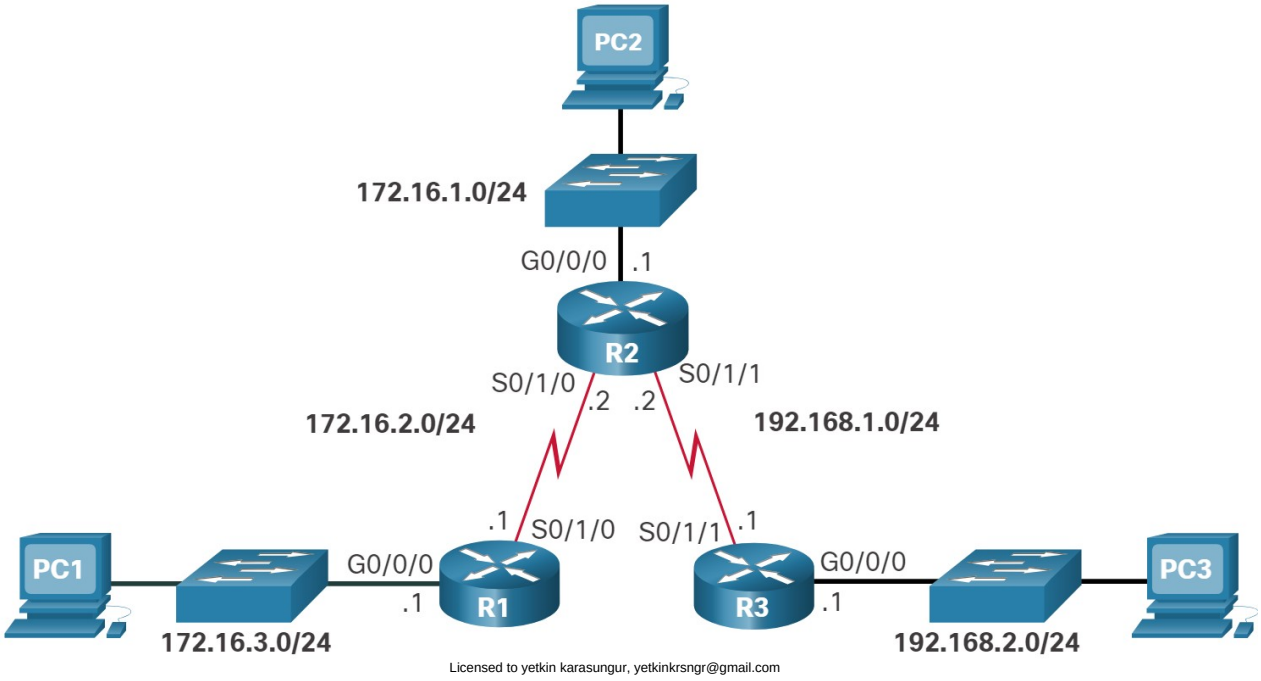
## 31.6.Statik Rota Yapılandırmasında Sorun Giderme

### 31.6.1.Yaygın Sorun Giderme Komutları

Yaygın IOS sorun giderme komutları şunları içerir:

- ping
- traceroute
- show ip route
- show ip interface brief
- show cdp neighbors detail

Şekil, bu komutları göstermek için kullanılan topolojiyi göstermektedir.



### ping

Örnek, R1'in kaynak arayüzünden R3'ün LAN arayüzüne genişletilmiş bir pingin sonucunu gösterir. Genişletilmiş ping, ping yardımcı programının geliştirilmiş bir sürümüdür. Genişletilmiş ping, ping paketleri için kaynak IP adresini belirlemenizi sağlar.

```
R1# ping 192.168.2.1 source 172.16.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/5 ms
R1#
```

### Traceroute

Bu örnek, R1'den R3 LAN'a bir izleme yolunun sonucunu gösterir. Her atlama yolunun bir ICMP yanıtı döndürdüğünü unutmayın.

```
R1# traceroute 192.168.2.1
Type escape sequence to abort.
Tracing the route to 192.168.2.1
VRF info: (vrf in name/id, vrf out name/id)
  1 172.16.2.2 1 msec 2 msec 1 msec
  2 192.168.1.1 2 msec 3 msec *
R1#
```

### show ip route

**show ip route komutu** bu örnekte R1 yönlendirme tablosunu görüntüler.

```
R1# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S        172.16.1.0/24 [1/0] via 172.16.2.2
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.1/32 is directly connected, Serial0/1/0
C        172.16.3.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.3.1/32 is directly connected, GigabitEthernet0/0/0
S     192.168.1.0/24 [1/0] via 172.16.2.2
S     192.168.2.0/24 [1/0] via 172.16.2.2
R1#
```

### show ip interface brief

Yönlendiricideki tüm arabirimlerin hızlı durumu, bu örnekte **show ip interface brief** komutu kullanılarak gösterilmektedir .

```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   172.16.3.1      YES manual up                    up
GigabitEthernet0/0/1   unassigned      YES unset  up                    up
Serial0/1/0            172.16.2.1      YES manual up                    up
Serial0/1/1            unassigned      YES unset  up                    up
R1#
```

Licensed to yetkin kerem gunduz yetkinkrsngr@gmail.com

**show cdp neighbors**

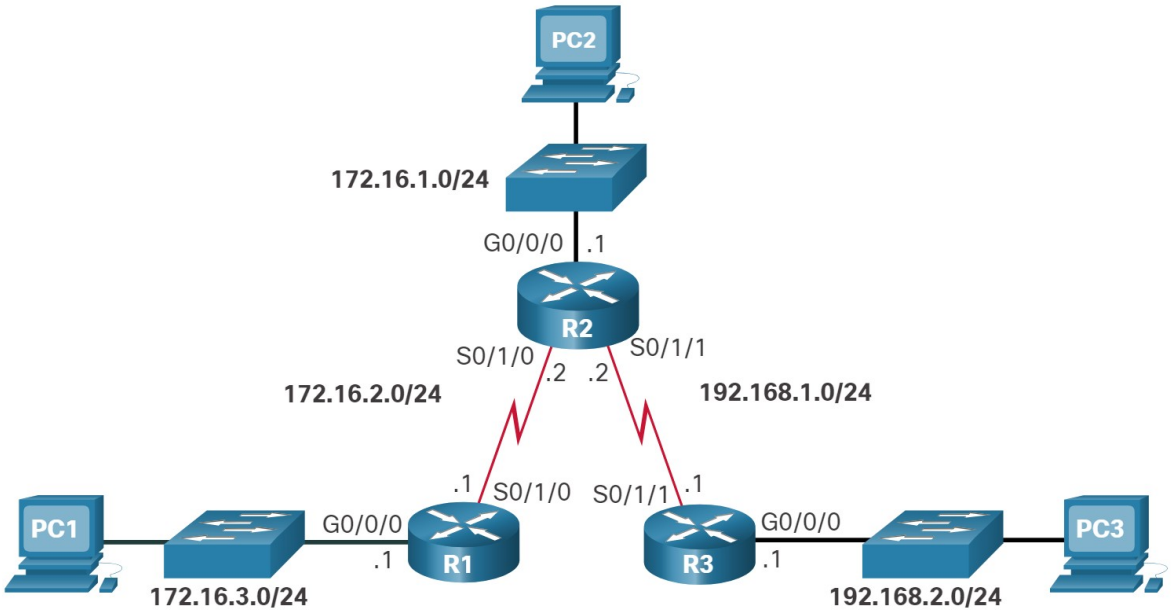
**show cdp neighbors** komutu doğrudan bağlı Cisco cihazlarının listesini sağlar. Bu komut Katman 2 (ve dolayısıyla Katman 1) bağlantısını doğrular. Örneğin, bir komşu cihaz komut çıktısında listelenmişse ancak pinglenemiyorsa, Katman 3 adresleme araştırılmalıdır.

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
Switch           Gig 0/0/1         129              S I   WS-C3560- Fas 0/5
R2               Ser 0/1/0         156            R S I  ISR4221/K Ser 0/1/0
Total cdp entries displayed : 3
R1#
```

## 31.6.2.Bağlantı Sorununu Çözme

Eksik (veya yanlış yapılandırılmış) bir rotayı bulmak, doğru araçlar metodik bir şekilde kullanılırsa nispeten basit bir süreçtir.

Örneğin, PC1'deki kullanıcı, R3 LAN'daki kaynaklara erişemediğini bildirir. Bu, kaynak olarak R1'in LAN arayüzünü kullanarak R3'ün LAN arayüzüne ping atılarak doğrulanabilir. Yine, bu bağlantı sorununun nasıl giderileceğini göstermek için şekildeki topolojiyi kullanacağız.




### Uzak LAN'a Ping Gönderme

Ağ yöneticisi, iki LAN arasındaki bağlantıyı PC1 yerine R1'den test edebilir. Bu, örnekte gösterildiği gibi, R1 üzerindeki G0 / 0/0 arayüzünden R3 üzerindeki G0 / 0/0 arayüzüne ping atılarak yapılabilir. Ping sonuçları, bu LAN'lar arasında bağlantı olmadığını gösterir.

```
R1# ping 192.168.2.1 source g0/0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
.....
Success rate is 0 percent (0/5)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Next-Hop Yönlendiriciye Ping Gönderme

Ardından, R2 üzerindeki S0 / 1/0 arayüzüne bir ping başarılı olur. Bu ping, R1'in S0 / 1/0 arayüzünden kaynaklanır. Bu nedenle, sorun R1 ve R2 arasındaki bağlantı kaybı değildir.

```
R1# ping 172.16.2.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
```

### R3 LAN'a S0 / 1 / 0'dan Ping

R1'den R3 arayüz 192.168.2.1'e bir ping de başarılıdır. Bu ping, R1 üzerindeki S0 / 1/0 arayüzünden kaynaklanır. R3, R1 ve R2, 172.16.2.0/24 arasında ağa geri giden bir rotaya sahiptir. Bu, R1'in R3 üzerindeki uzak LAN'a erişebileceğini doğrular. Ancak, R1 üzerindeki LAN'dan kaynaklanan paketler olamaz. Bu, R2 veya R3'ün R1'de LAN'a giden yanlış veya eksik bir rotaya sahip olabileceğini gösterir.

```
R1# ping 192.168.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/3/4 ms
```

### R2 Yönlendirme Tablosunu Doğrulayın

Bir sonraki adım, R2 ve R3'ün yönlendirme tablolarını incelemektir. R2 için yönlendirme tablosu örnekte gösterilmektedir. 172.16.3.0/24 ağının yanlış yapılandırıldığına dikkat edin. 172.16.3.0/24 ağına yönelik statik yol, sonraki atlama adresi 192.168.1.1 kullanılarak yapılandırılmıştır. Bu nedenle, 172.16.3.0/24 ağı için hedeflenen paketler, R1 yerine R3'e geri gönderilir.

```
R2# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.2/32 is directly connected, Serial0/1/0
S        172.16.3.0/24 [1/0] via 192.168.1.1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial0/1/1
L        192.168.1.2/32 is directly connected, Serial0/1/1
S     192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```

### R2 Statik Yol Yapılandırmasını Düzeltin

Çalışan yapılandırma aslında yanlış **ip route** ifadesini ortaya çıkarır . Yanlış rota kaldırılır ve ardından doğru rota girilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R2# show running-config | include ip route
ip route 172.16.3.0 255.255.255.0 192.168.1.1
ip route 192.168.2.0 255.255.255.0 192.168.1.1
R2#
R2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)# no ip route 172.16.3.0 255.255.255.0 192.168.1.1
R2(config)# ip route 172.16.3.0 255.255.255.0 172.16.2.1
R2(config)#
```

### Yeni Statik Yolu Doğrulayın

R2'deki yönlendirme tablosu, R1, 172.16.3.0'daki LAN'a yol girişinin doğru olduğunu ve R1'i işaret ettiğini onaylamak için bir kez daha kontrol edilir.

```
R2(config) # exit
R2#
*Sep 20 02:21:51.812: %SYS-5-CONFIG_I: Configured from console by console
R2# show ip route | begin Gateway
Gateway of last resort is not set
      172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
C        172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L        172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
C        172.16.2.0/24 is directly connected, Serial0/1/0
L        172.16.2.2/32 is directly connected, Serial0/1/0
S        172.16.3.0/24 [1/0] via 172.16.2.1
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial0/1/1
L        192.168.1.2/32 is directly connected, Serial0/1/1
S     192.168.2.0/24 [1/0] via 192.168.1.1
R2#
```

### Uzak LAN'a Tekrar Ping Gönderme

Daha sonra, G0 / 0/0 kaynaklı R1'den gelen bir ping, R1'in artık R3'ün LAN arayüzüne erişebildiğini doğrulamak için kullanılır. Onaylamanın son adımı olarak, PC1'deki kullanıcı ayrıca 192.168.2.0/24 LAN'a olan bağlantıyı da test etmelidir.

```
R1# ping 192.168.2.1 source g0/0/0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 172.16.3.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 32.Bölüm:OSPFv2 ve Yapılandırması

## 32.1.OSPF Özellikleri ve Karakteristikleri

### 32.1.1.OSPF'e Giriş

Bu konu, tek alan ve çoklu alan içeren Önce En Kısa Yolu Aç'a (Open Shortest Path First- OSPF) kısa bir genel bakış niteliğindedir. OSPFv2, IPv4 ağları için kullanılır. OSPFv3, IPv6 ağları için kullanılır. Bu kitabın tamamının birincil odak noktası tek alanlı OSPFv2'dir.

OSPF, mesafe vektörü Yönlendirme Bilgi Protokolü (Routing Information Protocol-RIP) için bir alternatif olarak geliştirilmiş bir bağlantı durumu yönlendirme protokolüdür. RIP, ağ ve internetin ilk günlerinde kabul edilebilir bir yönlendirme protokolüydü. Bununla birlikte, en iyi rotayı belirlemek için tek ölçü olarak RIP sekme sayımına bağlılığı hızla sorunlu hale geldi. Atlama sayısını kullanmak, farklı hızlarda birden çok yol içeren daha büyük ağlarda iyi ölçeklenmez. OSPF, RIP'e göre önemli avantajlara sahiptir, çünkü daha hızlı yakınsama sunar ve çok daha büyük ağ uygulamalarına ölçeklenir.

OSPF, alan kavramını kullanan bir bağlantı durumu yönlendirme protokolüdür. Bir ağ yöneticisi, yönlendirme etki alanını, yönlendirme güncelleme trafiğini kontrol etmeye yardımcı olan farklı alanlara bölebilir. Bağlantı, yönlendirici üzerindeki bir arayüzdür. Bir bağlantı aynı zamanda iki yönlendiriciyi bağlayan bir ağ kesimi veya tek bir yönlendiriciye bağlı bir Ethernet LAN gibi bir saplama ağıdır. Bir bağlantının durumu hakkındaki bilgiler, bağlantı durumu olarak bilinir. Tüm bağlantı durumu bilgileri ağ önekini, önek uzunluğunu ve maliyeti içerir.

### 32.1.2.OSPF Bileşenleri

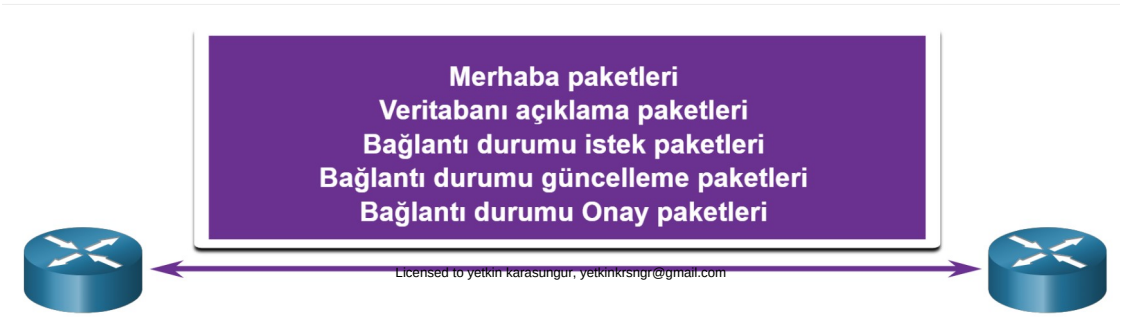
Tüm yönlendirme protokolleri benzer bileşenleri paylaşır. Bunların tümü, yol bilgilerini değiş tokuş etmek için yönlendirme protokolü mesajlarını kullanır. Mesajlar, daha sonra bir yönlendirme algoritması kullanılarak işlenen veri yapılarının oluşturulmasına yardımcı olur.

**Yönlendirme Protokolü Mesajları**

OSPF çalıştıran yönlendiriciler, beş tür paket kullanarak yönlendirme bilgilerini iletmek için mesaj alışverişi yapar. Bu paketler şekilde gösterildiği gibi aşağıdaki gibidir:

- Merhaba (Hello) paketi
- Veritabanı açıklama paketi
- Bağlantı durumu istek paketi
- Bağlantı durumu güncelleme paketi
- Bağlantı durumu onay paketi

Bu paketler, komşu yönlendiricileri keşfetmek ve ayrıca ağ hakkında doğru bilgileri korumak için yönlendirme bilgilerini değiştirmek için kullanılır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Veri Yapıları**

OSPF mesajları, aşağıdaki gibi üç OSPF veritabanı oluşturmak ve sürdürmek için kullanılır:

- Bitişiklik veritabanı - Bu, komşu tabloyu oluşturur.
- Bağlantı durumu veritabanı (LSDB-Link State Database) - Bu, topoloji tablosunu oluşturur.
- Yönlendirme veritabanı - Bu, yönlendirme tablosunu oluşturur.

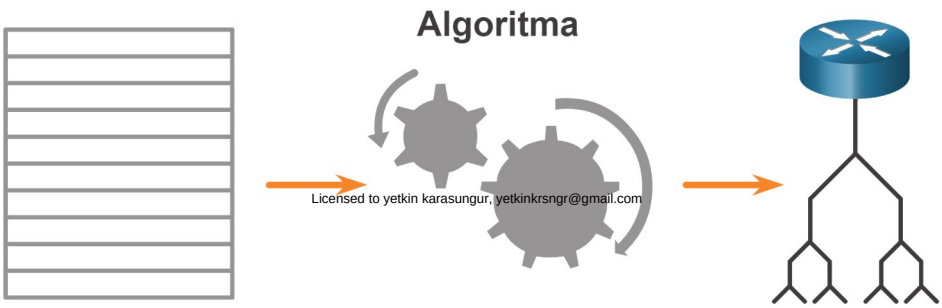
Bu tablolar, yönlendirme bilgilerinin değiş tokuşu için komşu yönlendiricilerin bir listesini içerir. Tablolar RAM'de tutulur ve saklanır. Aşağıdaki tabloda, her veri tablosunu görüntülemek için kullanılan komutu bulabilirisiniz.

| Veri tabanı | Tablo | Açıklama |
|---|---|---|
| Bitişiklik Veritabanı | Komşu Tablosu | Bir yönlendiricinin çift yönlü iletişim kurduğu tüm komşu yönlendiricilerin listesi.<br><br>Bu tablo her yönlendirici için benzersizdir.<br><br>show ip ospf neighbor komutu kullanılarak izlenebilir. |
| Bağlantı durumu Veritabanı | Topoloji Tablosu | Ağdaki diğer tüm yönlendiriciler hakkındaki bilgileri listeler.<br><br>Bu veritabanı ağ topolojisini temsil eder.<br><br>Bir alandaki tüm yönlendiriciler aynı LSDB'ye sahiptir.<br><br>show ip ospf database komutu kullanılarak izlenebilir. |
| Yönlendirme Veritabanı | Yönlendirme Tablosu | Bağlantı durumu veritabanında bir algoritma çalıştırıldığında oluşturulan yolların listesi.<br><br>Her yönlendiricinin yönlendirme tablosu benzersizdir ve paketlerin diğer yönlendiricilere nasıl ve nerede gönderileceği hakkında bilgi içerir.<br><br>show ip route komutu kullanılarak izlenebilir. |

**Algoritma**

Yönlendirici, Dijkstra en kısa yol ilk (shortest-path first- SPF) algoritmasına dayalı hesaplamaların sonuçlarını kullanarak topoloji tablosunu oluşturur. SPF algoritması, bir hedefe ulaşmak için kümülatif maliyete dayanır.

SPF algoritması, her yönlendiriciyi ağacın köküne yerleştirerek ve her düğüme giden en kısa yolu hesaplayarak bir SPF ağacı oluşturur. SPF ağacı daha sonra en iyi rotaları hesaplamak için kullanılır. OSPF, yönlendirme tablosunu yapmak için kullanılan yönlendirme veritabanına en iyi rotaları yerleştirir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

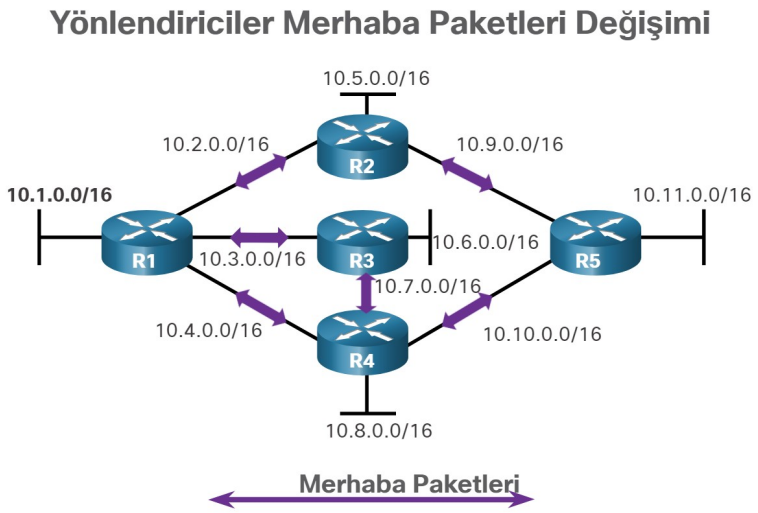
## 32.1.3.Bağlantı Durumu (Link State) İşlemi

Yönlendirme bilgilerini korumak için, OSPF yönlendiricileri bir yakınsama (convergence ) durumuna ulaşmak için genel bir bağlantı durumu yönlendirme işlemini tamamlar. Şekilde beş yönlendirici topolojisi gösterilmektedir. Yönlendiriciler arasındaki her bağlantı bir maliyet değeri ile etiketlenir. OSPF'de, hedefe giden en iyi yolu belirlemek için maliyet kullanılır. Aşağıda, bir yönlendirici tarafından tamamlanan bağlantı durumu yönlendirme adımları verilmiştir:

1. Komşu Bitişikliğinin Kurulması
2. Bağlantı Durumu Tanıtımlarının Değişimi
3. Bağlantı Durumu Veritabanını Oluşturma
4. SPF Algoritmasını Çalıştırma
5. En İyi Rotayı Seçme

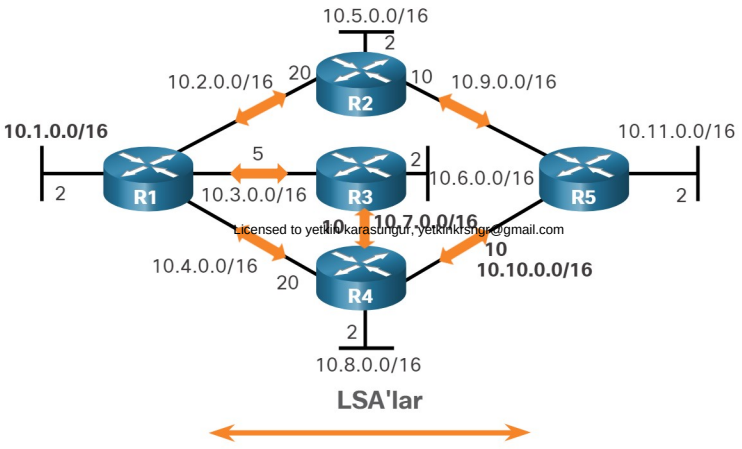
### 1 . Komşu Bitişikliğinin Kurulması

OSPF etkin yönlendiriciler, bilgi paylaşmadan önce ağ üzerinde birbirlerini tanımalıdır. OSPF etkin bir yönlendirici, bu bağlantılarda komşuların olup olmadığını belirlemek için tüm OSPF etkin arabirimlere Merhaba (Hello) paketleri gönderir. Bir komşu varsa, OSPF'nin etkin olduğu yönlendirici, bu komşuyla bir komşu bitişikliği oluşturmaya çalışır.




### 2. Bağlantı Durumu Tanıtımlarının Değişimi

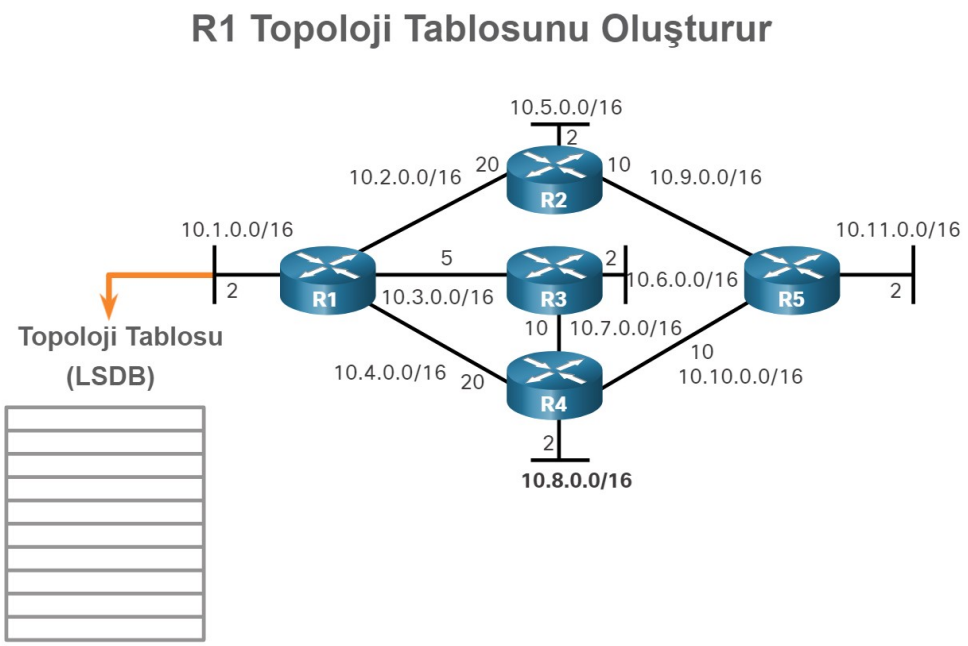
Bitişiklikler oluşturulduktan sonra, yönlendiriciler bağlantı durumu reklamlarını (Link State Advertisements LSA'lar) değiştirir. LSA'lar, doğrudan bağlanan her bağlantının durumunu ve maliyetini içerir. Yönlendiriciler, LSA'larını bitişik komşulara taşıyor. LSA'yı alan bitişik komşular, bölgedeki tüm yönlendiriciler tüm LSA'lara sahip olana kadar, doğrudan LSA'yı diğer doğrudan bağlı komşulara taşır.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

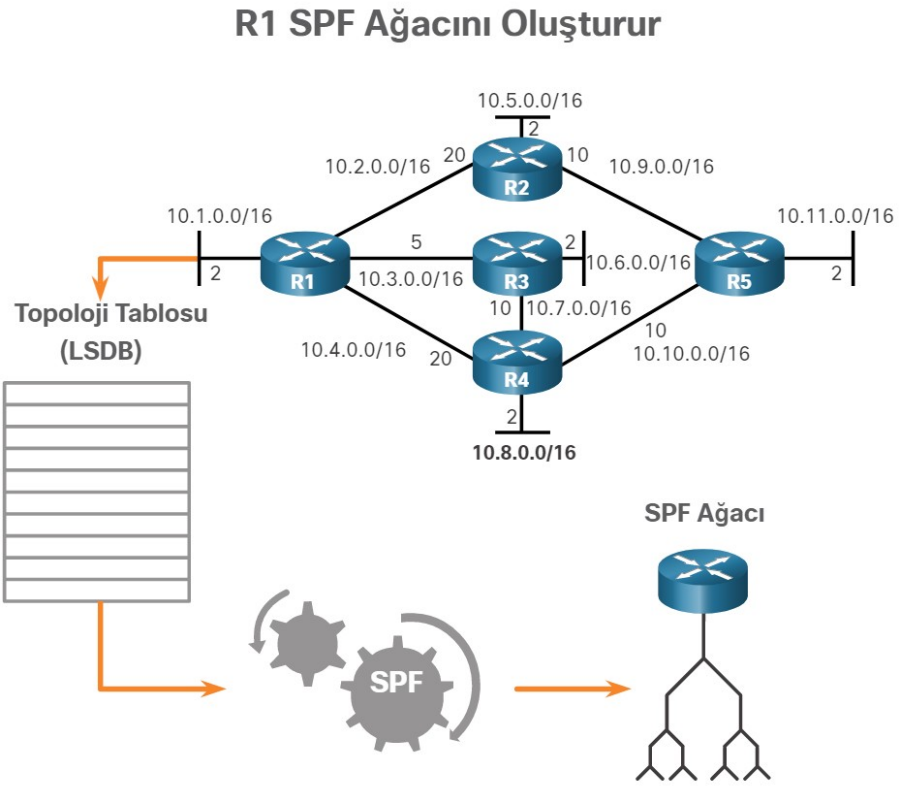
### 3. Bağlantı Durumu Veritabanını Oluşturma

LSA'lar alındıktan sonra, OSPF etkin yönlendiriciler alınan LSA'ları temel alarak topoloji tablosunu (LSDB) oluşturur. Bu veritabanı nihayetinde alanın topolojisi hakkındaki tüm bilgileri tutar.




### 4 . SPF Algoritmasını Çalıştırma

Yönlendiriciler daha sonra SPF algoritmasını yürütür. Bu adım için şekildeki dişliler, SPF algoritmasının yürütülmesini belirtmek için kullanılmıştır. SPF algoritması, SPF ağacını oluşturur.

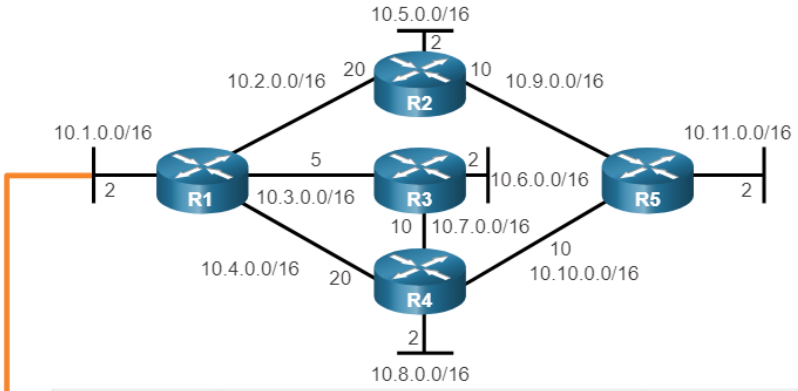



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 5 . En İyi Rotayı Seçme

SPF ağacı oluşturulduktan sonra, her ağa giden en iyi yollar IP yönlendirme tablosuna sunulur. Statik yol gibi daha düşük bir yönetim mesafesine sahip aynı ağa bir rota kaynağı olmadığı sürece rota, yönlendirme tablosuna eklenecektir. Yönlendirme kararları, yönlendirme tablosundaki girişlere göre verilir.

**R1 SPF Ağacının İçeriği**




| Hedef | En kısa yol | Maliyet |
|---|---|---|
| 10.5.0.0/16 | R1 → R2 | 22 |
| 10.6.0.0/16 | R1 → R3 | 7 |
| 10.7.0.0/16 | R1 → R3 | 15 |
| 10.8.0.0/16 | R1 → R3 → R4 | 17 |
| 10.9.0.0/16 | R1 → R2 | 30 |
| 10.10.0.0/16 | R1 → R3 → R4 | 25 |
| 10.11.0.0/16 | R1 → R3 → R4 → R5 | 27 |

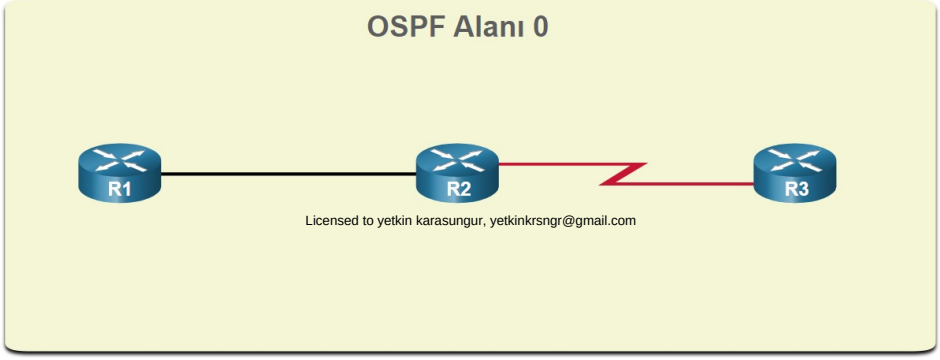
## 32.1.4.Tek Alanlı ve Çok Alanlı OSPF

OSPF'yi daha verimli ve ölçeklenebilir hale getirmek için OSPF, alanları kullanarak hiyerarşik yönlendirmeyi destekler. Bir OSPF alanı, LSDB'lerinde aynı bağlantı durumu bilgisini paylaşan bir yönlendiriciler grubudur. OSPF, aşağıdaki gibi iki yoldan biriyle uygulanabilir:

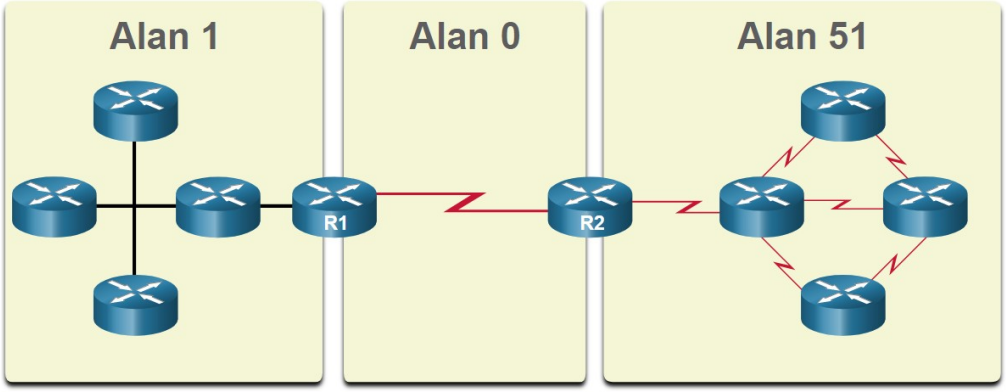
- Tek Alanlı (Single Area) OSPF - Tüm yönlendiriciler tek bir alandadır. En iyi uygulama alanı 0 kullanmaktır.
- Çok Alanlı (Multiarea OSPF) - OSPF, hiyerarşik bir tarzda birden çok alan kullanılarak uygulanır. Tüm alanlar omurga alanına (alan 0) bağlanmalıdır. Alanları birbirine bağlayan yönlendiriciler Alan Sınırı Yönlendiricileri (ABR'ler) olarak adlandırılır.

Bu kitabın odak noktası, tek alanlı OSPFv2 üzerinedir.

### Tek Alanlı OSPF



## Çok Alanlı OSPF




## Neden Çok Alanlı OSPF?

Çok alanlı OSPF ile, hiyerarşik yönlendirmeyi desteklemek için büyük bir yönlendirme alanı daha küçük alanlara bölünebilir. Yönlendirme hala alanlar arasında (alan arası yönlendirme) gerçekleşirken, veritabanının yeniden hesaplanması gibi işlemci yoğun yönlendirme işlemlerinin çoğu bir alan içinde tutulur.

Örneğin, bir yönlendirici alan içindeki bir topoloji değişikliği hakkında yeni bilgi aldığında (bir bağlantının eklenmesi, silinmesi veya değiştirilmesi dahil) yönlendirici, SPF algoritmasını yeniden çalıştırmalı, yeni bir SPF ağacı oluşturmalı ve yönlendirme tablosunu güncellemelidir. SPF algoritması yoğun CPU kullanır ve hesaplama için geçen süre, alanın boyutuna bağlıdır.

Not : Diğer alanlardaki yönlendiriciler, topoloji değişiklikleriyle ilgili güncellemeleri alır ancak bu yönlendiriciler, SPF algoritmasını yeniden çalıştırmaz, yalnızca yönlendirme tablosunu günceller.

Bir alanda çok fazla yönlendirici olması LSDB'leri çok büyük yapar ve CPU üzerindeki yükü artırır. Bu nedenle, yönlendiricileri alanlara göre düzenlemek, potansiyel olarak büyük bir veritabanını daha küçük ve daha yönetilebilir veritabanlarına etkili bir şekilde bölümler.

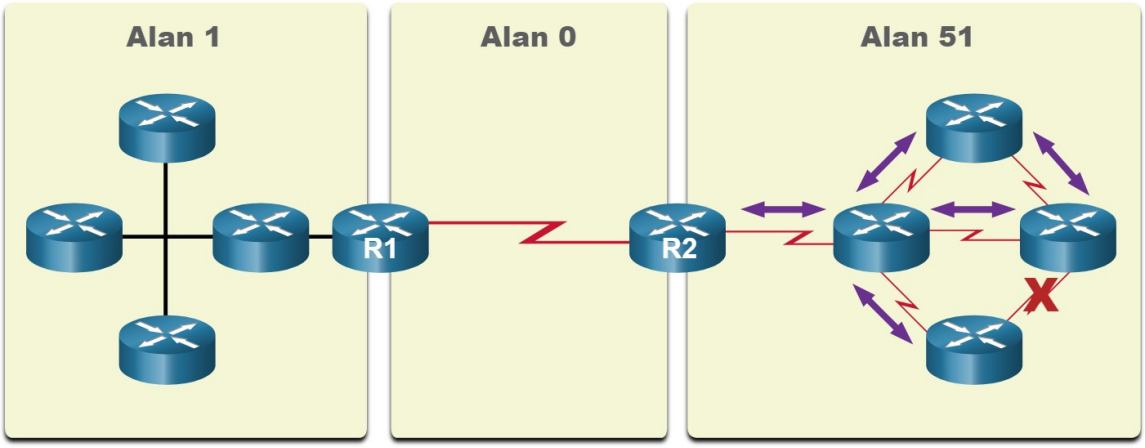
Çoklu alan OSPF ile hiyerarşik-topoloji tasarım seçenekleri aşağıdaki avantajları sağlayabilir.

- Daha küçük yönlendirme tabloları - Daha az yönlendirme tablosu girişi olduğundan tablolar daha küçüktür. Bunun nedeni, ağ adreslerinin alanlar arasında özetlenebilmesidir. Rota özetleme varsayılan olarak etkin değildir.
- Azaltılmış bağlantı durumu güncelleme yükü - Daha küçük alanlara sahip çok alanlı OSPF tasarlamak, işlem ve bellek gereksinimlerini en aza indirir.
- SPF hesaplamalarının azaltılmış sıklığı - Multiarea OSPF, bir alandaki topoloji değişikliğinin etkisini yerelleştirir. Örneğin, LSA taşması alan sınırında durduğu için yönlendirme güncelleme etkisini en aza indirir.

Örneğin, şekilde R2, alan 51 için bir ABR*'dir. Alan 51'deki bir topoloji değişikliği, tüm alan 51 yönlendiricilerinin SPF algoritmasını yeniden çalıştırmasına, yeni bir SPF ağacı oluşturmasına ve IP yönlendirme tablolarını güncellemesine neden olacaktır. ABR, R2, 0 alanındaki yönlendiricilere bir LSA gönderir ve bu da sonunda OSPF yönlendirme alanındaki tüm yönlendiricilere taşınır. Bu tür LSA, diğer alanlardaki yönlendiricilerin SPF algoritmasını yeniden çalıştırmasına neden olmaz. Yalnızca LSDB ve yönlendirme tablolarını güncellemeleri gerekir.

* ABR: Area Border Router

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




- Bağlantı hatası yalnızca yerel alanı etkiler (alan 51).
- ABR (R2), belirli bir LSA'nın taşmasını 51. alana izole eder.
- 0 ve 1 alanlarındaki yönlendiricilerin SPF algoritmasını çalıştırmasına gerek yoktur.

### 32.1.5.OSPFv3

OSPFv3, IPv6 öneklerinin değiş tokuşu için OSPFv2 eşdeğeridir. IPv6'da ağ adresine önek (prefix) ve alt ağ maskesine önek uzunluğu (prefix-length denildiğini hatırlayın.

IPv4 muadiline benzer şekilde, OSPFv3, IPv6 yönlendirme tablosunu uzak öneklerle doldurmak için yönlendirme bilgilerini değiştirir.

OSPFv2, IPv4 ağ katmanı üzerinden çalışır, diğer OSPF IPv4 eşleriyle iletişim kurar ve yalnızca IPv4 yollarının tanıtımını yapar.

OSPFv3, OSPFv2 ile aynı işlevselliğe sahiptir, ancak ağ katmanı aktarımı olarak IPv6'yı kullanır, OSPFv3 eşleriyle iletişim kurar ve IPv6 yollarını reklamı yapar. OSPFv3 ayrıca, yönlendirme etki alanı boyunca en iyi yolları belirlemek için hesaplama motoru olarak SPF algoritmasını kullanır.

OSPFv3, IPv4 muadilinden ayrı işlemlere sahiptir. Süreçler ve işlemler temelde IPv4 yönlendirme protokolündeki ile aynıdır, ancak bağımsız olarak çalışır. OSPFv2 ve OSPFv3'ün her biri, şekilde gösterildiği gibi ayrı bitişik tablolara, OSPF topoloji tablolarına ve IP yönlendirme tablolarına sahiptir.

OSPFv3 yapılandırma ve doğrulama komutları, OSPFv2'de kullanılanlara benzer.

## 32.2.OSPF Paketleri

### 32.2.1.OSPF Paket Türleri

Bağlantı durumu paketleri, bir paket için mevcut en hızlı yolu belirlemeye yardımcı olmak için OSPF tarafından kullanılan araçlardır. OSPF, komşu bitişiklikleri kurmak ve sürdürmek ve yönlendirme güncellemelerini değiştirmek için aşağıdaki bağlantı durumu paketlerini (LSP'ler) kullanır. Her paket, aşağıdaki gibi OSPF yönlendirme sürecinde belirli bir amaca hizmet eder:

Tip 1: Merhaba (Hello) paketi - Bu, diğer OSPF yönlendiricileriyle bitişiklik kurmak ve sürdürmek için kullanılır.
Tip 2: Veritabanı Açıklama (Database Desctription-DBD) paketi - Bu, gönderen yönlendiricinin LSDB'sinin kısaltılmış bir listesini içerir ve alıcı yönlendiriciler tarafından yerel LSDB'yi kontrol etmek için kullanılır. LSDB, doğru bir SPF ağacı oluşturmak için bir alandaki tüm bağlantı durumu yönlendiricilerinde aynı olmalıdır.
Tip 3: Bağlantı Durumu İsteği (Link State Request-LSR) paketi - Alıcı yönlendiriciler daha sonra bir LSR göndererek DBD'deki herhangi bir giriş hakkında daha fazla bilgi talep edebilir.

Licensed to yetkin karasungur yetkinkrsngr@gmail.com

Tip 4: Bağlantı Durumu Güncelleme (Link State Update-LSU) paketi - Bu, LSR'lere yanıt vermek ve yeni bilgileri duyurmak için kullanılır. LSU'lar birkaç farklı LSA türü içerir.
Tip 5: Bağlantı Durumu Onay (Link State Acknowledgment-LSAck) paketi - Bir LSU alındığında, yönlendirici LSU'nun alındığını onaylamak için bir LSAck gönderir. LSAck veri alanı boştur.

Tablo, OSPFv2 tarafından kullanılan beş farklı LSP türünü özetler. OSPFv3 benzer paket türlerine sahiptir.

| Tür | Paket Adı | Açıklama |
|---|---|---|
| 1 | Merhaba | Komşuları keşfeder ve aralarında komşular oluşturur |
| 2 | Veritabanı Açıklaması (DBD) | Yönlendiriciler arasında veritabanı senkronizasyonunu denetler |
| 3 | Bağlantı Durumu İsteği (LSR) | Yönlendiriciden yönlendiriciye belirli bağlantı durumu kayıtları ister |
| 4 | Bağlantı Durumu Güncellemesi (LSU) | Özel olarak istenen bağlantı durumu kayıtlarını gönderir |
| 5 | Bağlantı Durumu Bildirimi (LSAck) | Diğer paket türlerini onaylar |

## 32.2.2.Bağlantı Durumu Güncellemeleri

Yönlendiriciler başlangıçta, gönderen yönlendiricinin LSDB'sinin kısaltılmış bir listesi olan Tip 2 DBD paketlerini değiştirirler. Yerel LSDB'yi kontrol etmek için alıcı yönlendiriciler tarafından kullanılır.

Bir Tip 3 LSR paketi, alıcı yönlendiriciler tarafından DBD'deki bir giriş hakkında daha fazla bilgi talep etmek için kullanılır.

Tip 4 LSU paketi, bir LSR paketine yanıt vermek için kullanılır.

Bir Tip 4 LSU'nun alındığını onaylamak için bir Tip 5 paketi kullanılır.

LSU'lar, bağlantı değişiklikleri gibi OSPF yönlendirme güncellemelerini iletmek için de kullanılır. Spesifik olarak, bir LSU paketi, 11 farklı OSPFv2 LSA türü içerebilir ve bunlardan bazıları şekilde gösterilmektedir. OSPFv3, bu LSA'lardan birkaçını yeniden adlandırdı ve ayrıca iki ek LSA içerir.

Not : LSU ve LSA terimleri arasındaki fark bazen kafa karıştırıcı olabilir çünkü bu terimler genellikle birbirinin yerine kullanılır. Bununla birlikte, bir LSU bir veya daha fazla LSA içerir.

**LSU'lar**

| Tür | Paket Adı | Açıklama |
|---|---|---|
| 1 | Merhaba | Komşuları keşfeder ve aralarında komşular oluşturur |
| 2 | DBD | Yönlendiriciler arasında veritabanı senkronizasyonunu denetler |
| 3 | LSR | Yönlendiriciden yönlendiriciye belirli bağlantı durumu kayıtları ister |
| 4 | LSU | Özel olarak istenen bağlantı durumu kayıtlarını gönderir |
| 5 | LSAck | Diğer paket türlerini onaylar |

**LSA'lar**

| LSA Türü | Açıklama |
|---|---|
| 1 | Yönlendirici LSA'lar |
| 2 | Ağ LSA'ları |
| 3 veya 4 | Özet LSA'lar |
| 5 | Otonom Sistem Harici LSA'lar |
| 6 | Çok noktaya yayın OSPF LSA'ları |
| 7 | Çok Kısa Olmayan Alanlar için Tanımlandı |
| 8 | Sınır Ağ Geçidi Devriyesi (BGP'ler) için Harici Nitelikler LSA |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

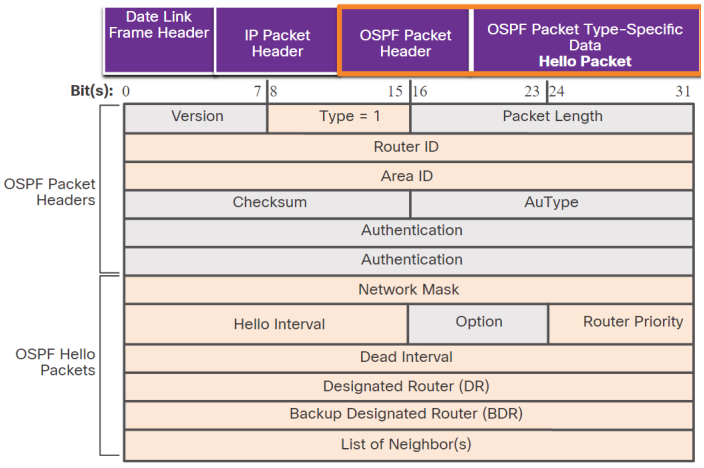
- Bir LSU, bir veya daha fazla LSA içerir.
- LSA'lar, hedef ağlar için rota bilgilerini içerir.

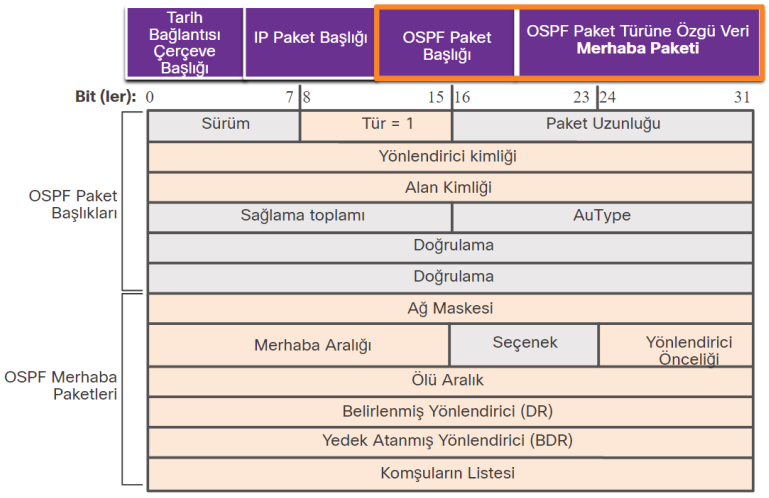
## 32.2.3.Merhaba (Hello) Paketi

OSPF Tip 1 paketi Merhaba paketidir. Merhaba paketleri aşağıdakileri yapmak için kullanılır:

OSPF komşularını keşfetme ve komşu bitişikliği oluşturma.
İki yönlendiricinin komşu olmayı kabul etmesi gereken parametreleri tanıtma.
Ethernet gibi çok erişimli ağlarda Atanmış Yönlendiriciyi (Designated Router-DR) ve Atanmış Yedek Yönlendiriciyi (Backup Designated RoutBDR) seçin. Noktadan noktaya bağlantılar DR veya BDR gerektirmez.

Şekil, OSPFv2 Tip 1 Merhaba paketinin içerdiği alanları gösterir.




Şekilde gösterilen önemli alanlar şunları içerir:

- **Tür** - Bu, paketin türünü tanımlar. 1 değeri, Merhaba paketini belirtir. 2 değeri bir DBD paketini, 3 bir LSR paketini, 4 bir LSU paketini ve 5 bir LSAck paketini tanımlar.
- **Yönlendirici Kimliği** - Noktalı ondalık gösterimle ifade edilen 32 bitlik bir değer (bir IPv4 adresi gibi), başlangıçtaki yönlendiriciyi benzersiz şekilde tanımlamak için kullanılır.
- **Alan Kimliği** - Bu, paketin çıktığı alanın numarasıdır.
- **Ağ Maskesi** - Bu, gönderen arayüzle ilişkili alt ağ maskesidir.
- **Merhaba Aralığı** - Bu, bir yönlendiricinin Merhaba paketleri gönderdiği saniye cinsinden frekansı belirtir. Çoklu erişim ağlarında varsayılan Merhaba aralığı 10 saniyedir. Bu zamanlayıcı, komşu yönlendiricilerde aynı olmalıdır; aksi takdirde bitişiklik kurulmaz.
- **Yönlendirici Önceliği** - Bu, DR / BDR seçiminde kullanılır. Tüm OSPF yönlendiricileri için varsayılan öncelik 1'dir, ancak 0'dan 255'e manuel olarak değiştirilebilir. Değer ne kadar yüksekse, yönlendiricinin bağlantıdaki DR olma olasılığı o kadar artar.
- **Ölü Aralık** - Bu, bir yönlendiricinin komşu yönlendiriciyi hizmet dışı ilan etmeden önce bir komşudan haber almayı beklediği saniye cinsinden süredir. Varsayılan olarak, yönlendirici Ölü Aralığı, Merhaba aralığının dört katıdır. Bu zamanlayıcı, komşu yönlendiricilerde aynı olmalıdır; aksi takdirde bitişiklik kurulmaz.
- **Belirlenmiş Yönlendirici (DR)** - Bu, DR'nin yönlendirici kimliğidir.
- **Yedek Atanmış Yönlendirici (BDR)** - Bu, BDR'nin yönlendirici kimliğidir.
- **Komşuların Listesi** - Bu liste, tüm bitişik yönlendiricilerin yönlendirici kimliklerini tanımlar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 32.3.OSPF Operasyonu

### 32.3.1.OSPF Operasyonel Durumları

Artık OSPF bağlantı durumu paketlerini bildiğinize göre, bu konu OSPF etkin yönlendiricilerle nasıl çalıştıklarını açıklamaktadır. Bir OSPF yönlendiricisi başlangıçta bir ağa bağlandığında, şunları yapmaya çalışır:

- Komşularla bitişiklikler oluşturma
- Yönlendirme bilgilerini değiştirme
- En iyi rotaları hesaplama
- Yakınsamaya ulaşma

Tablo, OSPF'nin yakınsamaya ulaşmaya çalışırken ilerlediği durumların ayrıntılarını verir:

| Durum | Açıklama |
|---|---|
| Down State<br>Aşağı Durumu | Merhaba paketi alınmadı = Aşağı.<br><br>Yönlendirici Merhaba paketleri gönderir.<br><br>Başlatma durumuna geçiş. |
| Init State<br>Başlangıç Durumu | Komşudan merhaba paketleri alınır.<br><br>Gönderen yönlendiricinin Yönlendirici Kimliğini içerirler.<br><br>İki Yönlü duruma geçiş. |
| Two-Way State<br>İki Yönlü Durum | Bu durumda, iki yönlendirici arasındaki iletişim çift yönlüdür.<br><br>Çoklu erişim bağlantılarında, yönlendiriciler bir DR ve bir BDR seçerler.<br><br>ExStart durumuna geçiş. |
| ExStart Durumu | Noktadan noktaya ağlarda, iki yönlendirici hangi yönlendiricinin DBD paket alışverişini başlatacağına ve ilk DBD paket sıra numarasına karar verir. |
| Exchange State<br>Değişim Durumu | Yönlendiriciler, DBD paketlerini değiştirir.<br><br>Ek yönlendirici bilgisi gerekiyorsa, Yükleniyor'a (Loading) geçer;aksi takdirde Tam (Full) duruma geçiş yapar. |
| Loading State<br>Yükleme Durumu | LSR'ler ve LSU'lar, ek rota bilgileri elde etmek için kullanılır.<br><br>Rotalar, SPF algoritması kullanılarak işlenir.<br><br>Tam duruma geçiş. |
| Full State<br>Tam Durum | Yönlendiricinin bağlantı durumu veritabanı tamamen senkronize edilmiştir. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

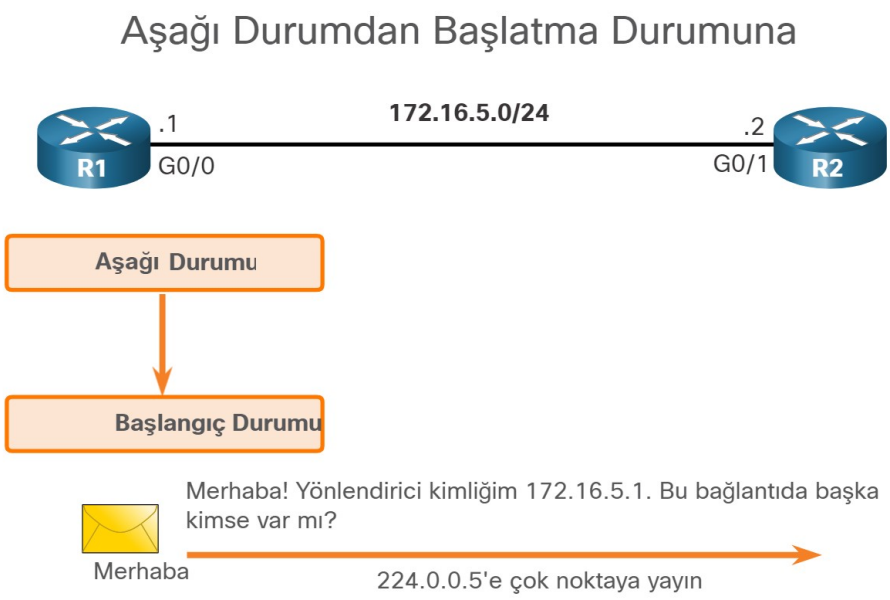
## 32.3.2.Komşu Bitişikliği Kurma

Bir arayüzde OSPF etkinleştirildiğinde, yönlendirici bağlantıda başka bir OSPF komşusu olup olmadığını belirlemelidir. Bunu başarmak için yönlendirici, tüm OSPF etkin arabirimlere kendi yönlendirici kimliğini içeren bir Merhaba paketi gönderir. Merhaba paketi, ayrılmış Tüm OSPF Yönlendiricileri IPv4 çok noktaya yayın adresine 224.0.0.5 gönderilir. Bu paketleri yalnızca OSPFv2 yönlendiricileri işleyecektir. OSPF yönlendirici kimliği (Router ID), OSPF işlemi tarafından OSPF alanındaki her yönlendiriciyi benzersiz şekilde tanımlamak için kullanılır. Yönlendirici kimliği, IPv4 adresi gibi biçimlendirilmiş ve OSPF eşleri arasında bir yönlendiriciyi benzersiz şekilde tanımlamak için atanan 32 bitlik bir sayıdır.

OSPF'nin etkin olduğu komşu bir yönlendirici, komşu listesinde olmayan bir yönlendirici kimliğine sahip bir Merhaba paketi aldığında, alıcı yönlendirici, başlatan yönlendiriciyle bir bitişiklik oluşturmaya çalışır.

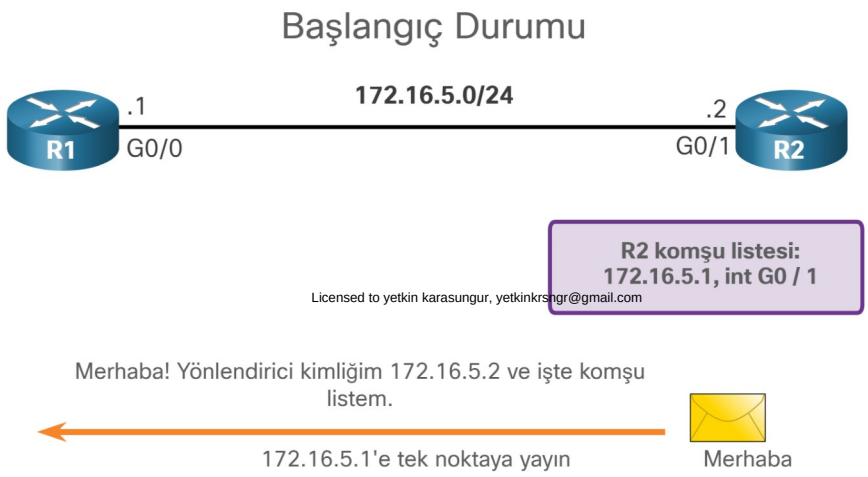
### 1.Aşağı Durumundan Başlatma Durumuna

OSPFv2 etkinleştirildiğinde, etkinleştirilen Gigabit Ethernet 0/0 arayüzü Aşağı durumdan Başlatma durumuna geçiş yapar. R1, OSPF komşularını keşfetmek için OSPF'nin etkin olduğu tüm arabirimlere Merhaba paketleri göndermeye başlar.




### 2.Başlangıç Durumu

R2, Merhaba paketini R1'den alır ve R1 yönlendirici kimliğini komşu listesine ekler. R2 daha sonra R1'e bir Merhaba paketi gönderir. Paket, aynı arayüz üzerindeki komşu listesinde R2 Yönlendirici Kimliği ve R1 Yönlendirici Kimliği'ni (Router ID )içerir.



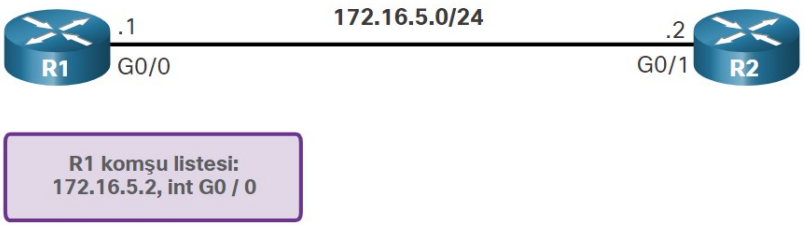

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 3.İki Yönlü Durum

R1, Merhaba'yı alır ve R2 Yönlendirici Kimliğini OSPF komşuları listesine ekler. Ayrıca Merhaba paketinin komşular listesinde kendi Yönlendirici Kimliğini de görür. Bir yönlendirici, Komşular listesinde listelenen Yönlendirici Kimliği ile bir Merhaba paketi aldığında, yönlendirici Başlatma durumundan İki Yönlü durumuna geçiş yapar.

İki Yönlü durumda gerçekleştirilen eylem, aşağıdaki gibi bitişik yönlendiriciler arasındaki ara bağlantı türüne bağlıdır:

- İki komşu komşu, noktadan noktaya bir bağlantı üzerinden birbirine bağlanırsa, hemen İki Yönlü durumdan ExStart durumuna geçerler.
- Yönlendiriciler ortak bir Ethernet ağı üzerinden birbirine bağlıysa, atanmış bir yönlendirici DR ve bir BDR seçilmelidir.




### 4.DR ve BDR Seçimi

R1 ve R2 bir Ethernet ağı üzerinden birbirine bağlı olduğundan, bir DR ve BDR seçimi gerçekleşir. Şekilde gösterildiği gibi, R2 DR olur ve R1 BDR olur. Bu işlem yalnızca Ethernet LAN'lar gibi çok erişimli ağlarda gerçekleşir.

Merhaba paketleri, yönlendirici bilgilerini korumak için sürekli olarak değiştirilir.

## 32.3.4.OSPF Veritabanlarını Senkronize Etme

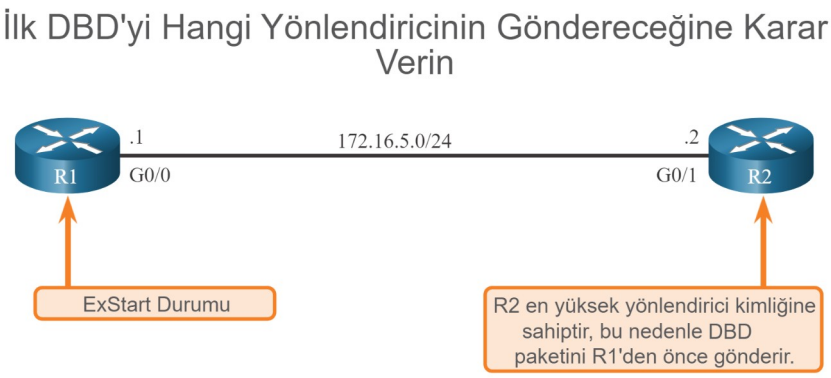
İki Yönlü durumdan sonra, yönlendiriciler veritabanı senkronizasyon durumlarına geçiş yapar. Merhaba paketi komşu bitişikliği oluşturmak için kullanılırken, LSDB'lerin değiş tokuşu ve senkronizasyonu sürecinde diğer dört OSPF paketi türü kullanılır. Bu, aşağıdaki gibi üç aşamalı bir işlemdir:

- İlk yönlendiriciye karar verme
- DBD'leri Değiştirme
- LSR gönderme

### 1 . İlk Yönlendiriciye Karar Verme

ExStart durumunda, iki yönlendirici, ilk olarak DBD paketlerini hangi yönlendiricinin göndereceğine karar verir. Daha yüksek yönlendirici kimliğine sahip yönlendirici, Exchange durumu sırasında DBD paketlerini gönderen ilk yönlendirici olacaktır. Şekilde, R2 daha yüksek yönlendirici kimliğine sahiptir ve önce DBD paketlerini gönderir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

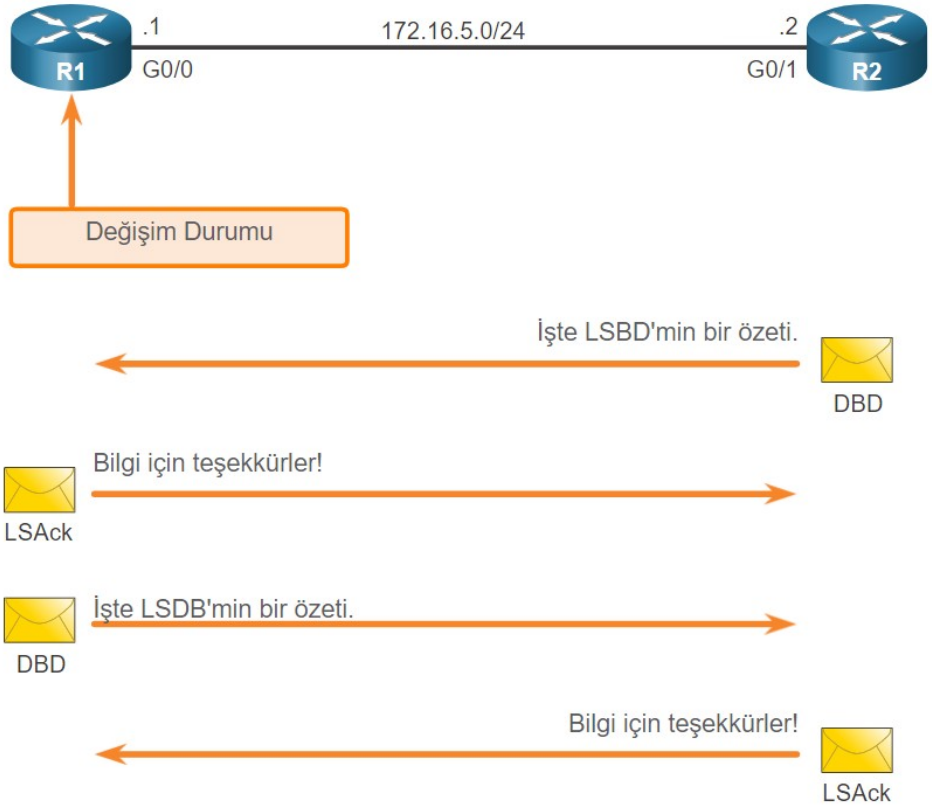



**2.DBD'leri Değiştirme**

Exchange durumunda, iki yönlendirici bir veya daha fazla DBD paketini değiştirir. Bir DBD paketi, yönlendiricinin LSDB'sinde görünen LSA giriş başlığı hakkındaki bilgileri içerir. Girişler bir bağlantı veya bir ağ hakkında olabilir. Her LSA giriş başlığı, bağlantı durumu türü, tanıtım yönlendiricisinin adresi, bağlantının maliyeti ve sıra numarası ile ilgili bilgileri içerir. Yönlendirici, sıra numarasını, alınan bağlantı durumu bilgilerinin yeniliğini belirlemek için kullanır.

Şekilde R2, R1'e bir DBD paketi gönderir. R1, DBD'yi aldığında, aşağıdaki eylemleri gerçekleştirir:

1. LSAck paketini kullanarak DBD'nin alındığını onaylar.
2. R1 daha sonra DBD paketlerini R2'ye gönderir.
3. R2, R1'i onaylar.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

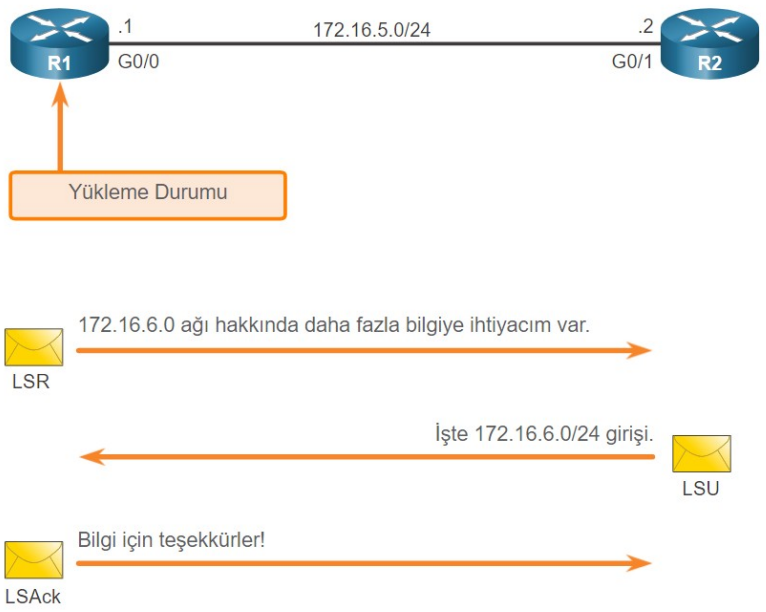
### 3.LSR gönderme

R1, aldığı bilgileri kendi LSDB'sinde bulunan bilgilerle karşılaştırır. DBD paketinin daha güncel bir bağlantı durumu girişi varsa, yönlendirici Yükleme durumuna geçer.

Örneğin, şekilde R1, ağ 172.16.6.0 ile ilgili olarak R2'ye bir LSR gönderir. R2, bir LSU paketindeki 172.16.6.0 hakkında tam bilgi ile yanıt verir. Yine, R1 bir LSU aldığında, bir LSAck gönderir. R1 daha sonra yeni bağlantı durumu girdilerini LSDB'sine ekler.

Belirli bir yönlendirici için tüm LSR'ler karşılandıktan sonra, bitişik yönlendiriciler senkronize edilmiş ve tam durumda kabul edilir. Güncellemeler (LSU'lar) aşağıdaki koşullarda yalnızca komşulara gönderilir:

- Bir değişiklik algılandığında (artımlı güncellemeler)
- 30 dakikada bir




## 32.3.5.DR İhtiyacı

DR ve BDR seçimi neden gereklidir?

Çoklu erişim ağları, LSA'ların taşması ile ilgili olarak OSPF için aşağıdaki gibi iki zorluk oluşturabilir:

Birden çok bitişikliğin oluşturulması - Ethernet ağları, birçok OSPF yönlendiricisini ortak bir bağlantı üzerinden potansiyel olarak birbirine bağlayabilir. Her yönlendiriciyle bitişik alanlar oluşturmak gereksiz ve istenmeyen bir durumdur. Aynı ağdaki yönlendiriciler arasında aşırı sayıda LSA alışverişine yol açar.
LSA'ların kapsamlı taşması - Bağlantı durumu yönlendiricileri, OSPF başlatıldığında veya topolojide bir değişiklik olduğunda LSA'larını taşırır. Bu aşırı bir yük oluşturabilir.
Birden çok bitişikteki sorunu anlamak için bir formülü incelemeliyiz:

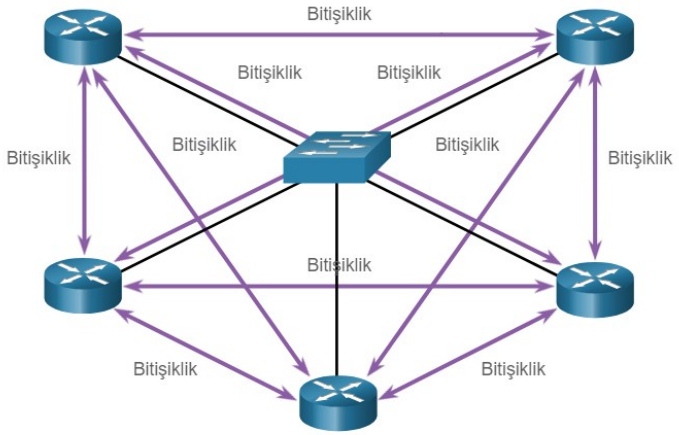
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Çok erişimli bir ağdaki herhangi bir sayıda yönlendirici ( n olarak belirtilir ) için n (n - 1) / 2 bitişik vardır.

Örneğin, şekil, tümü aynı çok erişimli Ethernet ağına bağlı olan beş yönlendiriciden oluşan basit bir topolojiyi göstermektedir. Bitişiklerin sayısını azaltmak için bir tür mekanizma olmadan, toplu olarak bu yönlendiriciler 10 bitişik oluşturur:

5 (5-1) / 2 = 10

Bu çok fazla görünmeyebilir, ancak ağa yönlendiriciler eklendikçe, bitişiklerin sayısı önemli ölçüde artar. Örneğin, 20 yönlendiriciye sahip çok erişimli bir ağ, 190 bitişik oluşturacaktır.



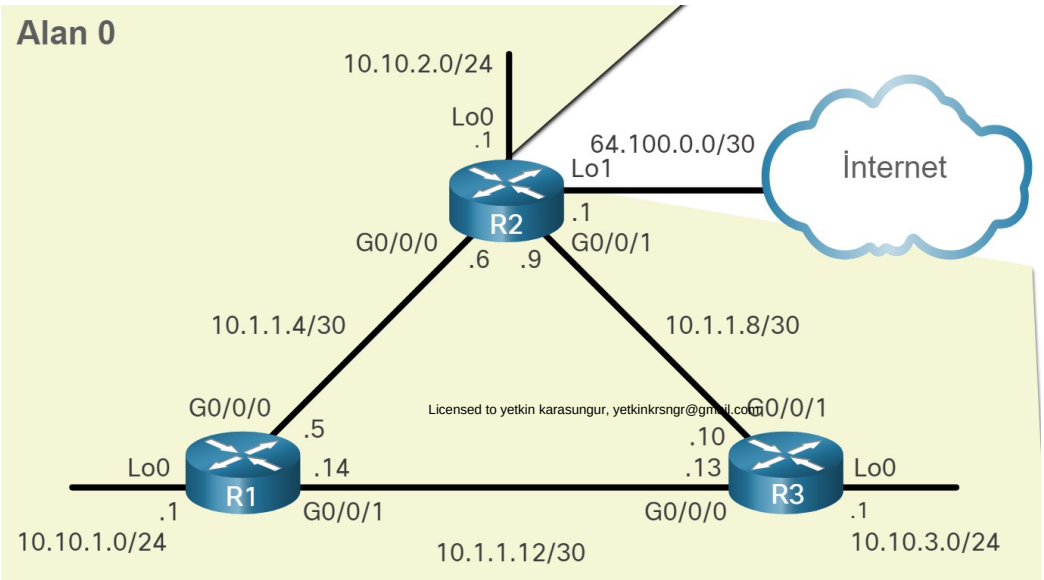

- Bitişik Alan Sayısı = n (n - 1) / 2
- n = yönlendirici sayısı
- Örnek: 5 (5 - 1) / 2 = 10 bitişik

## 32.4.OSPF Yapılandırması

### 32.4.1.OSPF Referans Topolojisi

Şekil, bu modülde OSPFv2'yi yapılandırmak için kullanılan topolojiyi gösterir. Topolojideki yönlendiriciler, arayüz adresleri dahil olmak üzere bir başlangıç konfigürasyonuna sahiptir. Şu anda hiçbir yönlendiricide yapılandırılmış statik yönlendirme veya dinamik yönlendirme yoktur. R1, R2 ve R3'teki tüm arabirimler (R2'deki geri döngü (loopback)1 hariç) OSPF omurga alanı içindedir. ISP yönlendiricisi, yönlendirme etki alanının internetine ağ geçidi olarak kullanılır.

Not : Bu topolojide, geridöngü arabirimi, İnternet'e WAN bağlantısını ve her yönlendiriciye bağlı bir LAN'ı simüle etmek için kullanılır. Bu, bu topolojinin yalnızca iki Gigabit Ethernet arabirimine sahip yönlendiricilerde gösterim amacıyla çoğaltılmasına izin vermek için yapılır.



## OSPF için Yönlendirici Yapılandırma Modu

OSPFv2, R1 için komut penceresinde gösterildiği gibi **router ospf** *process-id* genel yapılandırma modu komutu kullanılarak etkinleştirilir . İşlem kimliği (process-id) değeri 1 ile 65.535 arasında bir sayıyı temsil eder ve ağ yöneticisi tarafından seçilir. İşlem kimliği değeri yerel olarak önemlidir, yani bu komşularla bitişiklik kurmak için diğer OSPF yönlendiricilerinde aynı değerde olması gerekmez. Tüm OSPF yönlendiricilerinde aynı işlem kimliğinin kullanılması en iyi uygulama olarak kabul edilir.

**outer ospf** *process-id* komutunu girdikten sonra, yönlendirici , **R1(config-router)#** isteminde belirtildiği gibi yönlendirici yapılandırma moduna girer . Bu modda bulunan tüm komutları görüntülemek için bir soru işareti ( ? ) girin .

```
R1(config)# router ospf 10
R1(config-router)# ?
  area                    OSPF area parameters
  auto-cost               Calculate OSPF interface cost according to bandwidth
  default-information     Control distribution of default information
  distance                Define an administrative distance
  exit                    Exit from routing protocol configuration mode
  log-adjacency-changes   Log changes in adjacency state
  neighbor                Specify a neighbor router
  network                 Enable routing on an IP network
  no                      Negate a command or set its defaults
  passive-interface       Suppress routing updates on an interface
  redistribute            Redistribute information from another routing protocol
  router-id               router-id for this OSPF process
R1(config-router)#
```

## Yönlendirici Kimliği (Router ID)

OSPF yönlendirici kimliği, IPv4 adresi olarak gösterilen 32 bitlik bir değerdir. Yönlendirici kimliği, bir OSPF yönlendiricisini benzersiz şekilde tanımlamak için kullanılır. Tüm OSPF paketleri, kaynak yönlendiricinin yönlendirici kimliğini içerir. Her yönlendirici, bir OSPF etki alanına katılmak için bir yönlendirici kimliği gerektirir. Yönlendirici kimliği bir yönetici tarafından tanımlanabilir veya yönlendirici tarafından otomatik olarak atanabilir. Yönlendirici kimliği, aşağıdakileri yapmak için OSPF etkin bir yönlendirici tarafından kullanılır:

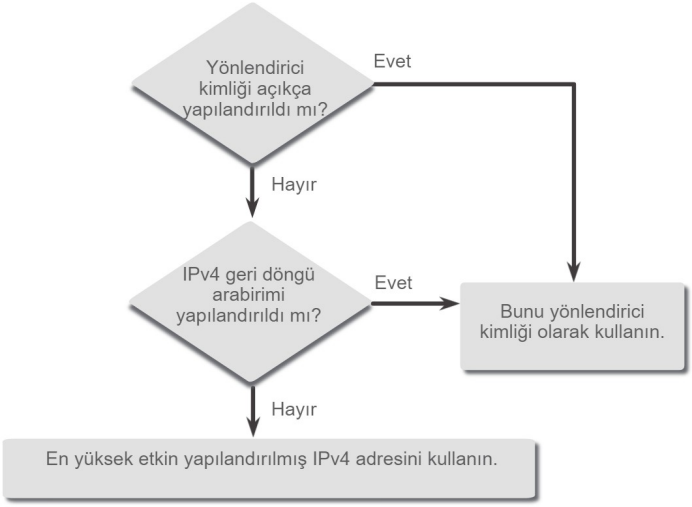
- OSPF veritabanlarının senkronizasyonuna katılım - Exchange Durumu sırasında, en yüksek yönlendirici kimliğine sahip yönlendirici önce veritabanı tanımlayıcı (DBD) paketlerini gönderir.
- Belirlenen yönlendiricinin (DR) seçimine katılım - Çok erişimli bir LAN ortamında, en yüksek yönlendirici kimliğine sahip yönlendirici DR olarak seçilir. İkinci en yüksek yönlendirici kimliğine sahip yönlendirme cihazı, yedek olarak belirlenmiş yönlendirici (BDR) olarak seçilir.

## Yönlendirici Kimliği Öncelik Sırası

Yönlendirici, yönlendirici kimliğini nasıl belirler? Şekilde gösterildiği gibi, Cisco yönlendiricileri yönlendirici kimliğini aşağıdaki tercih sırasına göre üç kriterden birine göre türetir:

1. Yönlendirici kimliği, OSPF **router-id** *rid* yönlendirici yapılandırma modu komutu kullanılarak yapılandırılır . *Rid* değeri IPv4 adres olarak ifade edilen herhangi bir 32-bit değeridir. Yönlendirici kimliği atamak için önerilen yöntem budur.
2. Yönlendirici kimliği açıkça yapılandırılmamışsa, yönlendirici, yapılandırılmış geri döngü (loopback) arabirimlerinden herhangi birinin en yüksek IPv4 adresini seçer. Bu, bir yönlendirici kimliği atamanın bir sonraki en iyi alternatifidir.
3. Geridöngü arabirimi yapılandırılmamışsa, yönlendirici fiziksel arabirimlerinden herhangi birinin en yüksek etkin IPv4 adresini seçer. Bu en az önerilen yöntemdir çünkü yöneticilerin belirli yönlendiricileri ayırt etmesini zorlaştırır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## Geri Döngü Arayüzünü Yönlendirici Kimliği Olarak Yapılandırma

Referans topolojide, yalnızca fiziksel arayüzler yapılandırılır ve etkindir. Geri döngü arabirimleri yapılandırılmamış. Yönlendiricide OSPF yönlendirmesi etkinleştirildiğinde, yönlendiriciler, yönlendirici kimliği olarak aşağıdaki en yüksek etkin yapılandırılmış IPv4 adresini seçecektir.

R1: 10.1.1.14 (G0 / 0/1)
R2: 10.1.1.9 (G0 / 0/1)
R3: 10.1.1.13 (G0 / 0/0)

Fiziksel arayüze güvenmek yerine, yönlendirici kimliği bir geri döngü arayüzüne atanabilir. Tipik olarak, bu tür bir geri döngü arabirimi için IPv4 adresi, 32 bitlik bir alt ağ maskesi (255.255.255.255) kullanılarak yapılandırılmalıdır. Bu etkili bir şekilde bir ana bilgisayar yolu oluşturur. 32 bitlik bir ana bilgisayar yolu, diğer OSPF yönlendiricilerine giden bir yol olarak bildirilmez.

Örnek, R1'de bir geri döngü arayüzünün nasıl yapılandırılacağını gösterir. Yönlendirici kimliğinin açıkça yapılandırılmadığını veya önceden öğrenilmediğini varsayarak, R1, yönlendirici kimliği olarak 1.1.1.1 IPv4 adresini kullanacaktır. R1'in henüz bir yönlendirici kimliği öğrenmediğini varsayın.

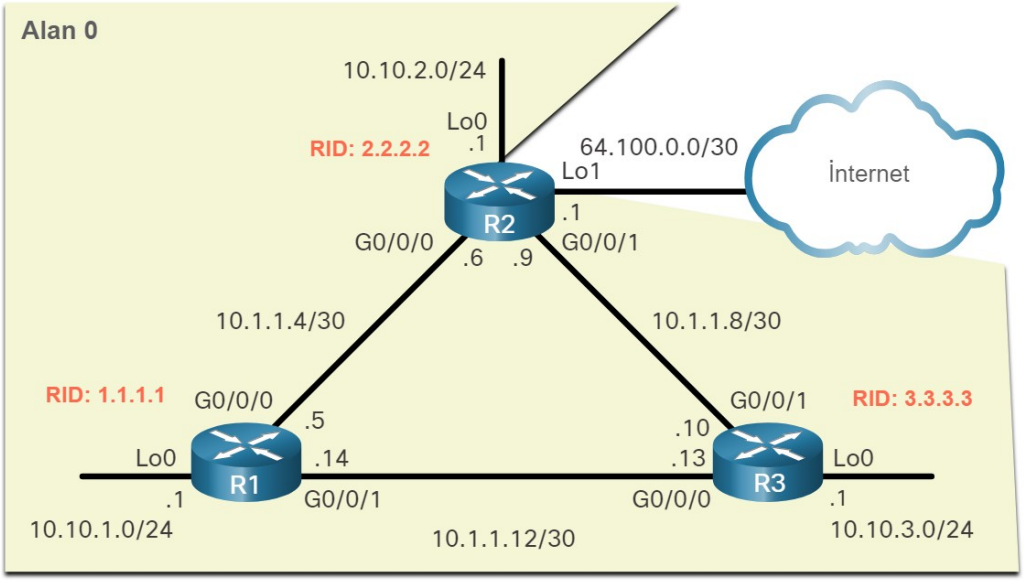
```
R1(config-if)# interface Loopback 1
R1(config-if)# ip address 1.1.1.1 255.255.255.255
R1(config-if)# end
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

## Yönlendirici Kimliğini Yapılandırma

Şekilde, topoloji her yönlendirici için yönlendirici kimliğini gösterecek şekilde güncellenmiştir:

- R1, yönlendirici kimliği 1.1.1.1'i kullanır
- R2, yönlendirici kimliği 2.2.2.2'i kullanır
- R3, yönlendirici kimliği 3.3.3.3'ü kullanır

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Yönlendirici kimliğini manuel olarak atamak için **router-id** *rid* yönlendirici yapılandırma modu komutunu kullanın. Örnekte, yönlendirici kimliği 1.1.1.1, R1'e atanmıştır. Yönlendirici kimliğini doğrulamak için **show ip protocols** komutunu kullanın.

```
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
R1(config-router)# end
*May 23 19:33:42.689: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

## Yönlendirici Kimliğini Değiştirme

Bir yönlendirici bir yönlendirici kimliği seçtikten sonra, etkin bir OSPF yönlendirici, yönlendirici yeniden yüklenene veya OSPF işlemi sıfırlanana kadar yönlendirici kimliğinin değiştirilmesine izin vermez.

Örneğin R1 için, yapılandırılmış yönlendirici kimliği kaldırıldı ve yönlendirici yeniden yüklendi. Geçerli yönlendirici kimliğinin 10.10.1.1 olduğuna ve bu da Loopback 0 IPv4 adresi olduğuna dikkat edin. Yönlendirici kimliği 1.1.1.1 olmalıdır. Bu nedenle, R1, r**outer-id 1.1.1.1** komutuyla yapılandırılır .

OSPF işleminin temizlenmesi veya yönlendiricinin yeniden yüklenmesi gerektiğini belirten bir bilgi mesajının nasıl göründüğüne dikkat edin. Bunun nedeni, R1'in 10.10.1.1 yönlendirici kimliğini kullanan diğer komşularla zaten bitişiklere sahip olmasıdır. Bu bitişiklikler, yeni yönlendirici kimliği 1.1.1.1 kullanılarak yeniden müzakere edilmelidir. Bitişiklikleri sıfırlamak için **clear ip ospf process** komutunu kullanın. Daha sonra, yalnızca yönlendirici kimliği bölümünü görüntülemek için R1'in **show ip protocols** komutuyla yeni yönlendirici kimliği komutunu kullandığını doğrulayabilirsiniz .

OSPF işleminin temizlenmesi, yönlendirici kimliğini sıfırlamak için tercih edilen yöntemdir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# show ip protocols | include Router ID
  Router ID 10.10.1.1
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router ospf 10
R1(config-router)# router-id 1.1.1.1
% OSPF: Reload or use "clear ip ospf process" command, for this to take effect
R1(config-router)# end
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
*Jun  6 01:09:46.975: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  6 01:09:46.975: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  6 01:09:46.981: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from LOADING to
FULL, Loading Done
*Jun  6 01:09:46.981: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from LOADING to
FULL, Loading Done
R1# show ip protocols | include Router ID
  Router ID 1.1.1.1
R1#
```

## 32.5.Noktadan Noktaya (Point to Point) OSPF Ağları

### 32.5.1.Network Komutu

OSPF tarafından sınıflandırılan bir ağ türü, noktadan noktaya ağdır. **Network** komutunu yapılandırarak, noktadan noktaya bir ağa ait olan arabirimleri belirtebilirsiniz . Ayrıca OSPF'yi daha sonra göreceğimiz gibi **ip ospf** komutu ile doğrudan arayüz üzerinden yapılandırabilirsiniz .

Her iki komut da bir OSPFv2 alanı için yönlendirme sürecine hangi arabirimlerin katıldığını belirlemek için kullanılır. **Network** komutunun temel sözdizimi aşağıdaki gibidir:

```
Router(config-router)# network network-address wildcard-mask area area-id
```

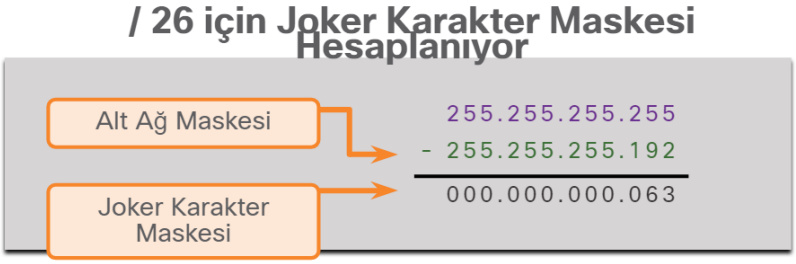
- **network-address** *wildcard-mask* sözdizimi arayüzlerde OSPF etkinleştirmek için kullanılır. **Network** komutundaki ağ adresiyle eşleşen bir yönlendirici üzerindeki tüm arabirimler, OSPF paketlerini göndermek ve almak için etkinleştirilir.
- **area** *area-id* sözdizimi OSPF alanı belirtir. Tek alanlı OSPFv2'yi yapılandırırken, ağ komutu tüm yönlendiricilerde aynı alan kimliği değeriyle yapılandırılmalıdır . Herhangi bir alan kimliği kullanılabilse de, tek alanlı OSPFv2 ile 0 alan kimliğini kullanmak iyi bir uygulamadır. Bu kural, ağın daha sonra çoklu alan OSPFv2'yi destekleyecek şekilde değiştirilmesini kolaylaştırır.

### 32.5.2.Wildcard Mask (Joker Karakter Maskesi)

Joker karakter maskesi, tipik olarak o arayüzde yapılandırılan alt ağ maskesinin tersidir. Bir alt ağ maskesinde, ikili 1 bir eşleşmeye eşittir ve ikili 0 bir eşleşme değildir. Joker karakter maskesinde, burada gösterildiği gibi bunun tersi doğrudur:

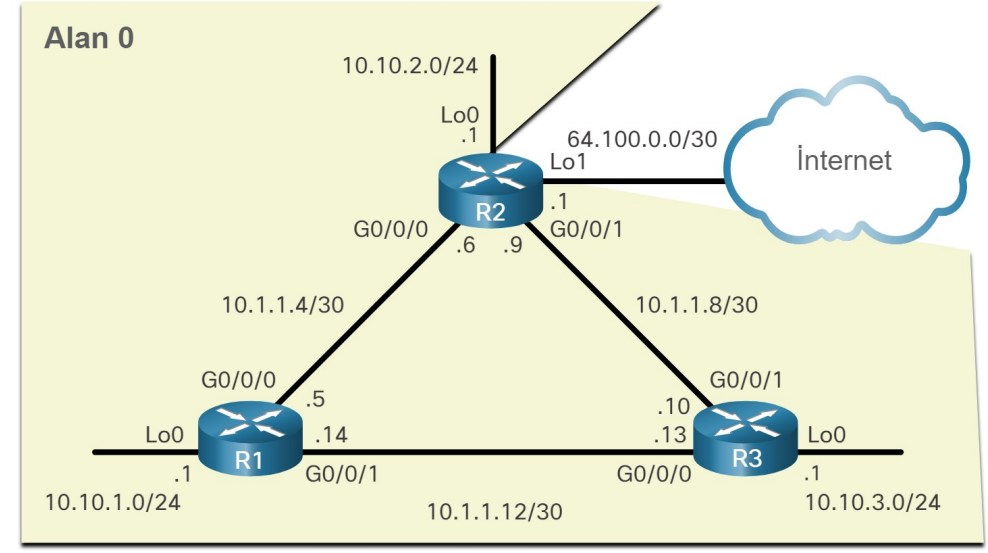
Joker karakter maskesi bit 0 - Adresteki ilgili bit değeriyle eşleşir.
Joker karakter maskesi bit 1 - Adresteki ilgili bit değerini yok sayar.
Joker karakter maskesini hesaplamanın en kolay yöntemi, şekilde / 24 ve / 26 alt ağ maskeleri için gösterildiği gibi, ağ alt ağ maskesini 255.255.255.255'ten çıkarmaktır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




### 32.5.3.Network Komutunu Kullanarak OSPF'yi Yapılandırma

Yönlendirme yapılandırma modunda, OSPFv2 yönlendirme sürecine katılacak arabirimleri belirlemenin iki yolu vardır. Şekilde referans topoloji gösterilmektedir.




İlk örnekte, joker karakter maskesi, arayüzü ağ adreslerine göre tanımlar. Bu ağa ait bir IPv4 adresiyle yapılandırılmış herhangi bir etkin arabirim, OSPFv2 yönlendirme sürecine katılacaktır.

```
R1(config)# router ospf 10
R1(config-router)# network 10.10.1.0 0.0.0.255 area 0
R1(config-router)# network 10.1.1.4 0.0.0.3 area 0
R1(config-router)# network 10.1.1.12 0.0.0.3 area 0
R1(config-router)#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not : Bazı IOS sürümleri, joker karakter maskesi yerine alt ağ maskesinin girilmesine izin verir. IOS daha sonra alt ağ maskesini joker karakter maskesi formatına dönüştürür.

Alternatif olarak, ikinci örnek OSPFv2'nin dörtlü sıfır joker karakter maskesi kullanarak tam arabirim IPv4 adresini belirleyerek nasıl etkinleştirilebileceğini gösterir. R1 üzerinde **network 10.1.1.5 0.0.0.0 area 0** girilmesi , yönlendiriciye yönlendirme işlemi için Gigabit Ethernet 0/0/0 arayüzünü etkinleştirmesini söyler. Sonuç olarak, OSPFv2 işlemi bu arayüzde (10.1.1.4/30) bulunan ağın reklamını yapacaktır.

```
R1(config)# router ospf 10
R1(config-router)# network 10.10.1.1 0.0.0.0 area 0
R1(config-router)# network 10.1.1.5 0.0.0.0 area 0
R1(config-router)# network 10.1.1.14 0.0.0.0 area 0
R1(config-router)#
```

Arayüzü belirlemenin avantajı, joker karakter maskesi hesaplamasının gerekli olmamasıdır. Her durumda, **area** bağımsız değişkeninin 0 alanını belirttiğine dikkat edin .

## 32.5.4.IP OSPF Komutunu Kullanarak OSPF'yi Yapılandırma

**Network** komutunu kullanmak yerine OSPF'yi doğrudan arayüzde de yapılandırabilirsiniz . OSPF'yi doğrudan arabirim üzerinde yapılandırmak için **ip ospf** arabirim yapılandırma modu komutunu kullanın. Sözdizimi aşağıdaki gibidir:

```
Router(config-if)# ip ospf process-id area area-id
```

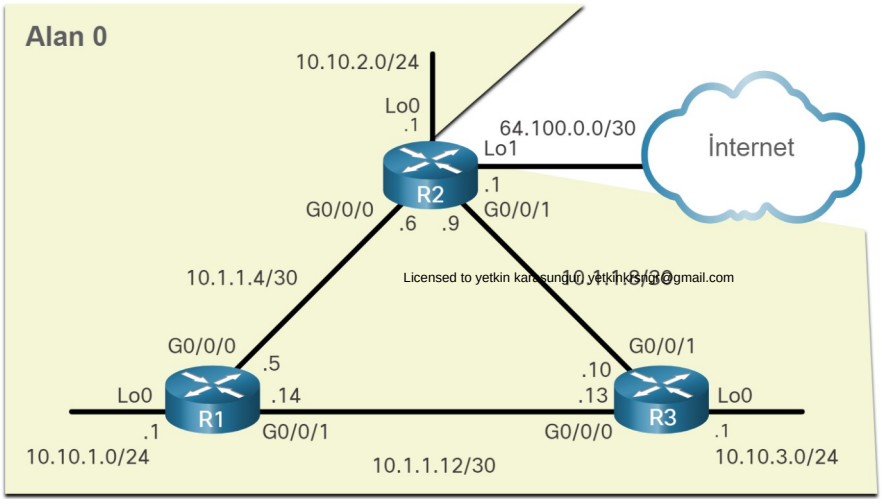
R1 için, network komutlarının no formunu kullanarak ağ komutlarını kaldırın. Ve sonra her bir arayüze gidin ve ip ospf komutunu şekilde gösterildiği gibi yapılandırın.

```
R1(config)# router ospf 10
R1(config-router)# no network 10.10.1.1 0.0.0.0 area 0
R1(config-router)# no network 10.1.1.5 0.0.0.0 area 0
R1(config-router)# no network 10.1.1.14 0.0.0.0 area 0
R1(config-router)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf 10 area 0
R1(config-if)# interface GigabitEthernet 0/0/1
R1(config-if)# ip ospf 10 area 0
R1(config-if)# interface Loopback 0
R1(config-if)# ip ospf 10 area 0
R1(config-if)#
```

## 32.5.5.Passive Interface

Varsayılan olarak, OSPF mesajları tüm OSPF etkin arabirimlere iletilir. Ancak, bu mesajların gerçekten yalnızca diğer OSPF etkin yönlendiricilere bağlanan arabirimlere gönderilmesi gerekir.

Şekildeki topolojiye bakın.



Licensed to yetkin karasungur yetkinkarasungur@gmail.com

Buradaki LAN'larda OSPFv2 komşusu olmamasına rağmen, OSPFv2 mesajları üç geri döngü arabiriminden dışarı iletilir. Bir üretim ağında, bu geri dönüşler, kullanıcılar ve trafik içeren ağlara fiziksel arayüzler olacaktır. Bir LAN üzerinden gereksiz mesajların gönderilmesi, ağı aşağıdaki gibi üç şekilde etkiler:

- Bant Genişliğinin Verimsiz Kullanımı - Kullanılabilir bant genişliği, gereksiz mesajları nakletmek için tüketilir.
- Kaynakların Verimsiz Kullanımı - LAN üzerindeki tüm cihazlar mesajı işlemeli ve sonunda atmalıdır.
- Artan Güvenlik Riski - Ek OSPF güvenlik yapılandırmaları olmadan, OSPF mesajları paket koklama yazılımı ile yakalanabilir. Yönlendirme güncellemeleri değiştirilebilir ve yönlendiriciye geri gönderilerek, yönlendirme tablosu trafiği yanlış yönlendiren yanlış ölçümlerle bozulur.

## Pasif Arayüzleri Yapılandırması

Yönlendirme mesajlarının bir yönlendirici arabirimi üzerinden iletilmesini önlemek için **passive-interface** yönlendirici yapılandırma modu komutunu kullanın, ancak yine de bu ağın diğer yönlendiricilere duyurulmasına izin verin. Yapılandırma örneği, R1 Loopback 0/0/0 arayüzünü pasif olarak tanımlar.

Not : Bu örnekteki geridöngü arabirimi bir Ethernet ağını temsil etmektedir. Üretim ağlarında, geridöngü arabirimlerinin pasif olması gerekmez.

**show ip protocols** komutu daha sonra geri döngü 0 arabirimin pasif olarak listelenen olduğunu doğrulamak için kullanılır. Arayüz hala “Routing on Interfaces Configured Explicitly (Area 0)” başlığı altında listelenmektedir; bu, bu ağın R2 ve R3'e gönderilen OSPFv2 güncellemelerine hala bir yol girişi olarak dahil edildiği anlamına gelir.

```
R1(config)# router ospf 10
R1(config-router)# passive-interface loopback 0
R1(config-router)# end
R1#
*May 23 20:24:39.309: %SYS-5-CONFIG_I: Configured from console by console
R1# show ip protocols
*** IP Routing is NSF aware ***
(output omitted)
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    GigabitEthernet0/0/1
    GigabitEthernet0/0/0
  Passive Interface(s):
    Loopback0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      01:01:48
    2.2.2.2              110      01:01:38
  Distance: (default is 110)
R1#
```

## 32.5.6.OSPF Noktadan Noktaya (Point to Point)Ağlar

Varsayılan olarak, Cisco yönlendiricileri, bağlantıda yalnızca bir başka cihaz olsa bile, Ethernet arayüzlerinde bir DR ve BDR seçer. Bunu, R1'in G0/0/0 örneğinde gösterildiği gibi **show ip ospf interface** komutuyla doğrulayabilirsiniz .

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 2.2.2.2, Interface address 10.1.1.6
  Backup Designated router (ID) 1.1.1.1, Interface address 10.1.1.5
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:08
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2  (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

R1, BDR'dir ve R2, DR'dir. DR / BDR seçim süreci, R1 ve R2 arasındaki noktadan noktaya ağda yalnızca iki yönlendirici olabileceğinden gereksizdir. Çıkışta yönlendiricinin ağ türünü BROADCAST-YAYIN olarak belirlediğine dikkat edin. Bunu noktadan noktaya bir ağa dönüştürmek için, DR / BDR seçim sürecini devre dışı bırakmak istediğiniz tüm arabirimlerde arabirim yapılandırma komutunu **ip ospf network point-to-point** kullanın . Aşağıdaki örnek, R1 için bu yapılandırmayı göstermektedir. OSPF komşu bitişiklik durumu birkaç milisaniye için azalacaktır.

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf network point-to-point
*Jun  6 00:44:05.208: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  6 00:44:05.211: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from LOADING to
FULL, Loading Done
R1(config-if)# interface GigabitEthernet 0/0/1
R1(config-if)# ip ospf network point-to-point
*Jun  6 00:44:45.532: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  6 00:44:45.535: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/1 from LOADING to
FULL, Loading Done
R1(config-if)# end
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:04
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
```

Gigabit Ethernet 0/0/0 arabiriminin artık ağ türünü POINT_TO_POINT olarak listelediğine ve bağlantıda DR veya BDR olmadığına dikkat edin.

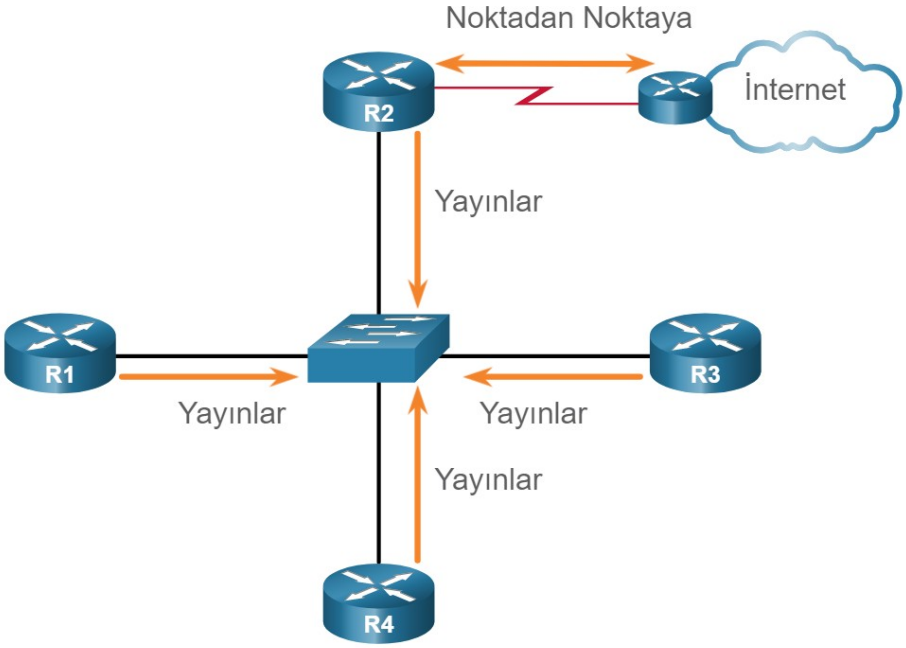
Licensed to yetkin karasungur, yetkinkrshgr@gmail.com

## 32.6.Çok Erişimli (Multiaccess) OSPF Ağları

### 32.6.1.OSPF Ağ Türleri

OSPF kullanan başka bir ağ türü, çoklu erişimli OSPF ağıdır. Çoklu erişim OSPF ağları, tek bir yönlendiricinin LSA'ların dağıtımını kontrol etmesi bakımından benzersizdir. Bu rol için seçilen yönlendirici, uygun yapılandırma ile ağ yöneticisi tarafından belirlenmelidir.

OSPF, ağın türüne bağlı olarak ek işlemler içerebilir. Önceki topoloji, yönlendiriciler arasında noktadan noktaya bağlantılar kullanıyordu. Bununla birlikte, yönlendiriciler, şekilde gösterildiği gibi, çoklu erişim ağı oluşturmak için aynı anahtara bağlanabilir. Ethernet LAN'lar, çok erişimli yayın ağlarının en yaygın örneğidir. Yayın (Broadcast) ağlarında, ağdaki tüm cihazlar tüm yayın ve çok noktaya yayın çerçevelerini görür.




### 32.6.2.OSPF Atanmış Yönlendirici (Designated Router)

Çoklu erişim ağlarında, OSPF'nin bitişiklerin sayısını ve bağlantı durumu tanıtımlarının (LSA'lar) taşmasını yönetmek için bir çözüm olarak bir DR ve BDR seçtiğini hatırlayın. DR, gönderilen ve alınan LSA'ları toplamaktan ve dağıtmaktan sorumludur. DR, tüm OSPF yönlendiricileri için tasarlanmış çok noktaya yayın IPv4 adresi 224.0.0.5'i kullanır.

DR'nin başarısız olması durumunda bir BDR de seçilir. BDR pasif olarak dinler ve tüm yönlendiricilerle bir ilişki kurar. DR, Hello paketlerini üretmeyi durdurursa, BDR kendisini destekler ve DR rolünü üstlenir.

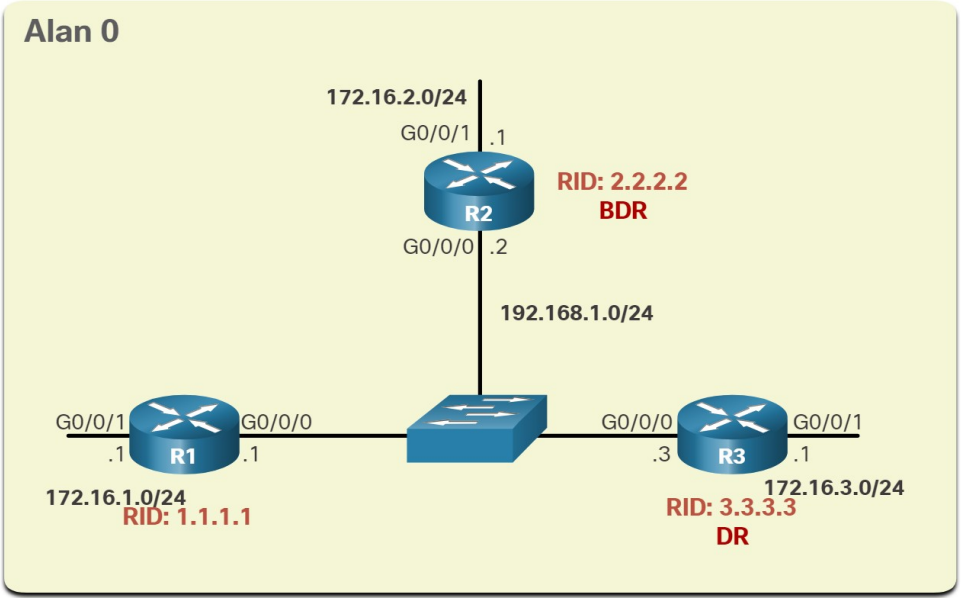
Diğer tüm yönlendiriciler DROTHER (ne DR ne de BDR olmayan bir yönlendirici) haline gelir. DROTHER'lar, OSPF paketlerini DR ve BDR'ye göndermek için çoklu erişim adresi 224.0.0.6'yı (tüm belirlenmiş yönlendiriciler) kullanır. Sadece DR ve BDR 224.0.0.6'yı dinler.

#### 32.6.3.OSPF Çoklu Erişim Referans Topolojisi

Şekilde gösterilen çoklu erişim topolojisinde, ortak bir Ethernet çoklu erişim ağı üzerinden birbirine bağlanmış üç yönlendirici vardır, 192.168.1.0/24. Her yönlendirici, Gigabit Ethernet 0/0/0 arayüzünde belirtilen IPv4 adresiyle yapılandırılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yönlendiriciler ortak bir çoklu erişim ağı üzerinden bağlandığından, OSPF otomatik olarak bir DR ve BDR seçmiştir. Bu örnekte, R3, yönlendirici kimliği bu ağdaki en yüksek değer olan 3.3.3.3 olduğu için DR olarak seçilmiştir. R2, BDR'dir çünkü ağdaki en yüksek ikinci yönlendirici kimliğine sahiptir.




## OSPF Yönlendirici Rollerini Doğrulama

OSPFv2 yönlendiricisinin rollerini doğrulamak için **show ip ospf interface** komutunu kullanın.

### R1 DROTHER

R1 tarafından üretilen çıktı, aşağıdakileri doğrular:

- R1 DR veya BDR değil, varsayılan önceliği 1 olan bir DROTHER'dır (Satır 7)
- DR, 192.168.1.3 IPv4 adresinde 3.3.3.3 yönlendirici kimliğine sahip R3 iken, BDR, 192.168.1.2 IPv4 adresinde 2.2.2.2 yönlendirici kimliğine sahip R2'dir. (8. ve 9. satırlar)
- R1'in iki bitişiği vardır: biri BDR ve diğeri DR ile. (20-22. Satırlar)

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:07
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 1
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
    Adjacent with neighbor 3.3.3.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## R2 BDR

R2 tarafından üretilen çıktı şunları doğrular:

- R2, varsayılan önceliği 1 olan BDR'dir. (Satır 7)
- DR, 192.168.1.3 IPv4 adresinde 3.3.3.3 yönlendirici kimliğine sahip R3 iken, BDR, 192.168.1.2 IPv4 adresinde 2.2.2.2 yönlendirici kimliğine sahip R2'dir. (8. ve 9. satırlar)
- R2'nin iki bitişiği vardır; biri yönlendirici kimliği 1.1.1.1 (R1) olan bir komşuyla ve diğeri DR ile. (20-22. Satırlar)

```
R2# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.2/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 1.1.1.1
    Adjacent with neighbor 3.3.3.3  (Designated Router)
  Suppress hello for 0 neighbor(s)
R2#
```

## R3 DR

R3 tarafından üretilen çıktı şunları doğrular:

- R3, varsayılan önceliği 1 olan DR'dir. (Satır 7)
- DR, 192.168.1.3 IPv4 adresinde 3.3.3.3 yönlendirici kimliğine sahip R3 iken, BDR, 192.168.1.2 IPv4 adresinde 2.2.2.2 yönlendirici kimliğine sahip R2'dir. (8. ve 9. satırlar)
- R3'ün iki bitişiği vardır: biri 1.1.1.1 (R1) yönlendirici kimliğine sahip bir komşu ve diğeri BDR ile. (20-22. Satırlar)

```
R3# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.3/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 3.3.3.3, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.1.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 1.1.1.1
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
R3#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**DR / BDR Bitişiklerini Doğrulama**

OSPFv2 bitişiklerini doğrulamak için, R1 örneğinde gösterildiği gibi **show ip ospf neighbor** komutunu kullanın. Çoklu erişim ağlarında komşuların durumu aşağıdaki gibi olabilir:

- FULL / DROTHER - Bu, DR olmayan veya BDR olmayan bir yönlendiriciye tamamen bitişik olan bir DR veya BDR yönlendiricidir. Bu iki komşu Merhaba paketlerini, güncellemeleri, sorguları, yanıtları ve onayları değiş tokuş edebilir.
- FULL / DR - Yönlendirici, belirtilen DR komşusuyla tamamen bitişiktir. Bu iki komşu, Merhaba paketlerini, güncellemeleri, sorguları, yanıtları ve onayları değiş tokuş edebilir.
- FULL / BDR - Yönlendirici, belirtilen BDR komşusuyla tamamen bitişiktir. Bu iki komşu Merhaba paketlerini, güncellemeleri, sorguları, yanıtları ve onayları değiş tokuş edebilir.
- 2-WAY/ DROTHER - DR olmayan veya BDR yönlendiricinin, DR olmayan veya BDR olmayan başka bir yönlendirici ile komşu ilişkisi vardır. Bu iki komşu, Merhaba paketlerini değiş tokuş eder.

  Bir OSPF yönlendiricisinin normal durumu genellikle FULL'dur. Bir yönlendirici başka bir durumda takılı kalırsa, bu, komşuları oluşturmada sorunlar olduğunun bir göstergesidir. Bunun tek istisnası, çok erişimli yayın ağında normal olan 2-WAY durumdur. Örnekler için DROTHER'lar, ağa katılan DROTHER'larla 2-WAY bir komşu bitişikliği oluşturacaktır. Bu olduğunda, komşu durumu 2 YOLLU / DROTHER olarak görüntülenir.

R1 tarafından üretilen çıktı, R1'in aşağıdaki yönlendiricilerle bitişiklere sahip olduğunu doğrular:

Yönlendirici kimliği 2.2.2.2 olan R2, Tam durumdadır ve R2'nin rolü BDR'dir.
3.3.3.3 yönlendirici kimliğine sahip R3, Tam durumdadır ve R3'ün rolü DR'dir.

```
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   FULL/BDR        00:00:31    192.168.1.2     GigabitEthernet0/0/0
3.3.3.3           1   FULL/DR         00:00:39    192.168.1.3     GigabitEthernet0/0/0
R1#
```

R2 tarafından üretilen çıktı, R2'nin aşağıdaki yönlendiricilerle bitişiklere sahip olduğunu doğrular:

Yönlendirici kimliği 1.1.1.1 olan R1 Tam durumdadır ve R1 ne DR ne de BDR'dir.
3.3.3.3 yönlendirici kimliğine sahip R3, Tam durumdadır ve R3'ün rolü DR'dir.

```
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DROTHER    00:00:31    192.168.1.1     GigabitEthernet0/0/0
3.3.3.3           1   FULL/DR         00:00:34    192.168.1.3     GigabitEthernet0/0/0
R2#
```

R3 tarafından üretilen çıktı, R3'ün aşağıdaki yönlendiricilerle komşuları olduğunu doğrular:

Yönlendirici kimliği 1.1.1.1 olan R1 Tam durumdadır ve R1 ne DR ne de BDR'dir.
Yönlendirici kimliği 2.2.2.2 olan R2, Tam durumdadır ve R2'nin rolü BDR'dir.

```
R3# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   FULL/DROTHER    00:00:37    192.168.1.1     GigabitEthernet0/0/0
2.2.2.2           1   FULL/BDR        00:00:33    192.168.1.2     GigabitEthernet0/0/0
R3#
```

Licensed to yetkin karasoftbil yetkinkarasoftbil@gmail.com

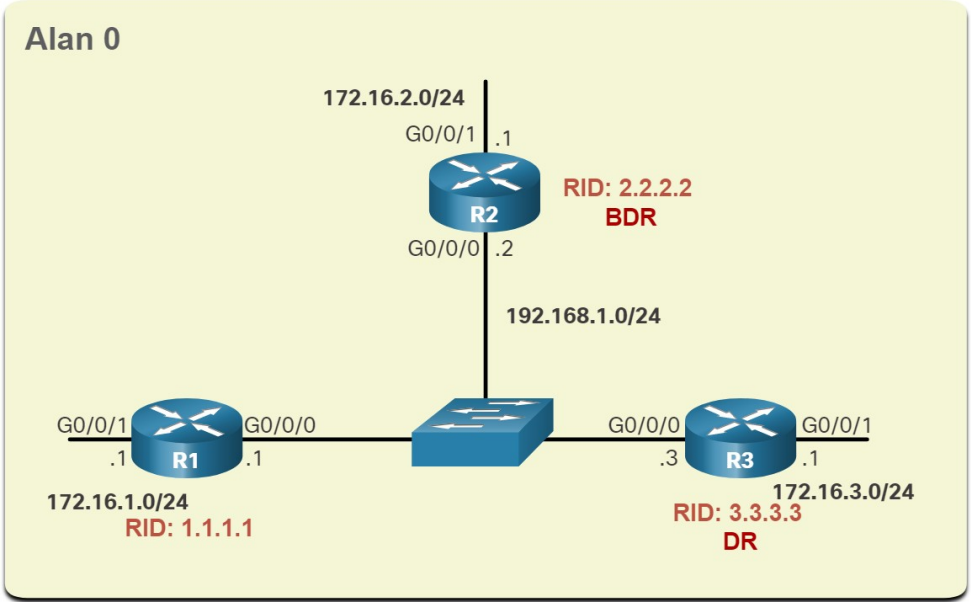
## 32.6.4.DR / BDR Seçim Süreci

DR ve BDR nasıl seçilir? OSPF DR ve BDR seçim kararı, sırayla aşağıdaki kriterlere dayanmaktadır:

1. Ağdaki yönlendiriciler, DR olarak en yüksek arayüz önceliğine (priority) sahip yönlendiriciyi seçer. İkinci en yüksek arayüz önceliğine sahip yönlendirici, BDR olarak seçilir. Öncelik, 0 - 255 arasında herhangi bir sayı olacak şekilde yapılandırılabilir. Arayüz öncelik değeri 0 olarak ayarlanırsa, bu arayüz DR veya BDR olarak seçilemez. Çoklu erişimli yayın arayüzlerinin varsayılan önceliği 1'dir. Bu nedenle, aksi yapılandırılmadıkça, tüm yönlendiriciler eşit bir öncelik değerine sahiptir ve DR / BDR seçimi sırasında başka bir bağlantı kesme yöntemine güvenmek zorundadır.
2. Arayüz öncelikleri eşitse, en yüksek yönlendirici kimliğine sahip yönlendirici DR olarak seçilir. İkinci en yüksek yönlendirici kimliğine sahip yönlendirici BDR'dir.

Yönlendirici kimliğinin aşağıdaki üç yoldan biriyle belirlendiğini hatırlayın:

1. Yönlendirici kimliği manuel olarak yapılandırılabilir.
2. Yönlendirici kimliği yapılandırılmamışsa, yönlendirici kimliği en yüksek geri döngü IPv4 adresi tarafından belirlenir.
3. Geridöngü arabirimi yapılandırılmamışsa, yönlendirici kimliği en yüksek etkin IPv4 adresi tarafından belirlenir.




Şekilde, tüm Ethernet yönlendirici arabirimlerinin varsayılan önceliği 1'dir. Sonuç olarak, yukarıda listelenen seçim kriterlerine dayalı olarak, OSPF yönlendirici kimliği DR ve BDR'yi seçmek için kullanılır. En yüksek yönlendirici kimliğine sahip R3, DR olur; ve ikinci en yüksek yönlendirici kimliğine sahip R2, BDR olur.

DR ve BDR seçim süreci, çoklu erişim ağında OSPF özellikli bir arayüze sahip ilk yönlendirici etkin olur olmaz gerçekleşir. Bu, önceden yapılandırılmış OSPF yönlendiricileri açıldığında veya arayüzde OSPF etkinleştirildiğinde meydana gelebilir. Seçim süreci yalnızca birkaç saniye sürer. Çoklu erişim ağındaki tüm yönlendiriciler önyüklemeyi bitirmediyse, daha düşük bir yönlendirici kimliğine sahip bir yönlendiricinin DR olması mümkündür.

OSPF DR ve BDR seçimleri önleyici değildir. DR ve BDR seçiminden sonra ağa daha yüksek önceliğe veya daha yüksek yönlendirici kimliğine sahip yeni bir yönlendirici eklenirse, yeni eklenen yönlendirici DR veya BDR rolünü devralmaz. Bunun nedeni, bu rollerin zaten atanmış olmasıdır. Yeni bir yönlendiricinin eklenmesi, yeni bir seçim sürecini başlatmaz.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

DR seçildikten sonra, aşağıdaki olaylardan biri gerçekleşene kadar DR olarak kalır:

- DR başarısız.
- DR üzerindeki OSPF işlemi başarısız oluyor veya durduruldu.
- DR üzerindeki çoklu erişim arabirimi başarısız oluyor veya kapanıyor.

DR başarısız olursa, BDR otomatik olarak DR'ye yükseltilir. İlk DR / BDR seçiminden sonra ağa daha yüksek önceliğe veya yönlendirici kimliğine sahip başka bir DROTHER eklense bile bu durum geçerlidir. Bununla birlikte, bir BDR DR'ye yükseltildikten sonra, yeni bir BDR seçimi gerçekleşir ve en yüksek önceliğe veya yönlendirici kimliğine sahip DROTHER, yeni BDR olarak seçilir.

## 32.6.5.Ip Ospf Priority Komutu

Arabirim öncelikleri tüm yönlendiricilerde eşitse, en yüksek yönlendirici kimliğine sahip yönlendirici DR olarak seçilir. Yönlendirici kimliğini DR / BDR seçimini işleyecek şekilde yapılandırmak mümkündür. Bununla birlikte, bu işlem yalnızca tüm yönlendiricilerde yönlendirici kimliğini ayarlamak için sıkı bir plan varsa çalışır. Yönlendirici kimliğini yapılandırmak bunu kontrol etmeye yardımcı olabilir. Ancak, büyük ağlarda bu külfetli olabilir.

Yönlendirici kimliğine güvenmek yerine, arabirim önceliklerini belirleyerek seçimi kontrol etmek daha iyidir. Bu aynı zamanda bir yönlendiricinin bir ağda DR ve diğerinde DROTHER olmasına izin verir. Bir arabirimin önceliğini ayarlamak için **ip ospf priority** *value* komutunu kullanın; burada değer 0 ila 255 arasındadır. 0 değeri, DR veya BDR olmaz. Arayüzde 1 ila 255 arasında bir değer, yönlendiricinin DR veya BDR olma olasılığını artırır.

### OSPF Önceliğini Yapılandırma

Topolojide, ip ospf priority komutu DR ve BDR'yi aşağıdaki gibi değiştirmek için kullanılacaktır:

- R1, DR olmalıdır ve 255 önceliği ile yapılandırılacaktır.
- R2, BDR olmalıdır ve varsayılan öncelik 1 olarak bırakılacaktır.
- R3 asla bir DR veya BDR olmamalıdır ve 0 önceliğiyle yapılandırılacaktır.

R1 G0 / 0/0 arayüz önceliğini 1'den 255'e değiştirin.

```
R1(config)# interface GigabitEthernet 0/0/0
R1(config-if)# ip ospf priority 255
R1(config-if)# end
R1#
```

R3 G0 / 0/0 arayüz önceliğini 1'den 0'a değiştirin.

```
R3(config)# interface GigabitEthernet 0/0/0
R3(config-if)# ip ospf priority 0
R3(config-if)# end
R3#
```

Aşağıdaki örnek, R1'de OSPF işleminin nasıl temizleneceğini gösterir. clear ip ospf process komutu R2 ve R3'de girilmelidir . Oluşturulan OSPF durum bilgisine dikkat edin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# clear ip ospf process
Reset ALL OSPF processes? [no]: y
R1#
*Jun  5 03:47:41.563: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  5 03:47:41.563: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  5 03:47:41.569: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from LOADING to
FULL, Loading Done
*Jun  5 03:47:41.569: %OSPF-5-ADJCHG: Process 10, Nbr 3.3.3.3 on GigabitEthernet0/0/0 from LOADING to
FULL, Loading Done
```

R1 üzerindeki **show in ospf interface g0/0/0** komutunun çıktısı, R1'in şimdi 255 önceliğe sahip DR olduğunu doğrular ve R1'in yeni komşu bitişiklerini tanımlar.

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 192.168.1.1/24, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1         no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State DR, Priority 255
  Designated Router (ID) 1.1.1.1, Interface address 192.168.1.1
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.1.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:00
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 2
  Last flood scan time is 0 msec, maximum is 1 msec
  Neighbor Count is 2, Adjacent neighbor count is 2
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
    Adjacent with neighbor 3.3.3.3
  Suppress hello for 0 neighbor(s)
```

## 32.7. Tek Alanlı OSPFv2 Yapılandırmasında Değişiklik Yapma

### 32.7.1.Cisco OSPF Maliyet (Cost) Metriği

Bir yönlendirme protokolünün, bir ağ üzerindeki bir paketin en iyi yolunu belirlemek için bir ölçü kullandığını hatırlayın. Bir metrik, paketleri belirli bir arayüz üzerinden göndermek için gerekli ek yükün göstergesini verir. OSPF, bir metrik olarak maliyeti kullanır. Daha düşük bir maliyet, daha yüksek bir maliyetten daha iyi bir yolu gösterir.

Bir arayüzün Cisco maliyeti, arayüzün bant genişliği ile ters orantılıdır. Bu nedenle, daha yüksek bir bant genişliği, daha düşük bir maliyeti gösterir. OSPF maliyetini hesaplamak için kullanılan formül:

Maliyet (Cost) = referans bant genişliği / arayüz bant genişliği

Varsayılan referans bant genişliği $10^8$'dir (100.000.000); bu nedenle formül şu şekildedir:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Maliyet = 100.000.000 bps / bps cinsinden arayüz bant genişliği

Maliyet hesaplamasının dökümü için tabloya bakın. OSPF maliyet değerinin bir tam sayı olması gerektiğinden, FastEthernet, Gigabit Ethernet ve 10 Gigabit Ethernet (10 GigE) arayüzleri aynı maliyeti paylaşır. Bu durumu düzeltmek için şunları yapabilirsiniz:

- Referans bant genişliğini , her OSPF yönlendiricisinde **auto-cost reference-bandwidth** komutuyla ayarlayın .
- OSPF maliyet değerini , gerekli arabirimlerde **ip ospf cost** komutuyla manuel olarak ayarlayın .

**Varsayılan Cisco OSPF Maliyetleri**

| arayüz türü | Bps cinsinden Referans Bant Genişliği | | Bps cinsinden varsayılan bant genişliği | Maliyet |
|---|---|---|---|---|
| **10 Gigabit Ethernet** 10 Gbps | 100.000.000 | ÷ | 10.000.000.000 | 0.01 = 1 |
| **Gigabit Ethernet** 1 Gbps | 100.000.000 | ÷ | 1.000.000.000 | 0.1 = 1 |
| **Hızlı Ethernet** 100 Mbps | 100.000.000 | ÷ | 100.000.000 | 1 |
| **Ethernet** 10 Mbps | 100.000.000 | ÷ | 10.000.000 | 10 |

Referans bant genişliği nedeniyle aynı maliyetler

## 32.7.2.Referans Bant Genişliğini Ayarlama

Maliyet değeri bir tam sayı olmalıdır. Tam sayıdan küçük bir şey hesaplanırsa, OSPF en yakın tam sayıya yuvarlar. Bu nedenle, varsayılan referans bant genişliği 100.000.000 bps olan bir Gigabit Ethernet arayüzüne atanan OSPF maliyeti 1'e eşit olacaktır, çünkü 0.1 için en yakın tam sayı 1 yerine 0'dır.

Maliyet = 100.000.000 bps / 1.000.000.000 = 1

Bu nedenle, Hızlı Ethernet'ten daha hızlı olan tüm arayüzler, Hızlı Ethernet arayüzüyle aynı maliyet değerine sahip olacaktır. OSPF'nin doğru yol belirlemesini yapmasına yardımcı olmak için, 100 Mbps'den daha hızlı bağlantılara sahip ağlara uyum sağlamak için referans bant genişliğinin daha yüksek bir değere değiştirilmesi gerekir.

Referans bant genişliğini değiştirmek aslında bağlantı üzerindeki bant genişliği kapasitesini etkilemez; daha ziyade, metriği belirlemek için kullanılan hesaplamayı etkiler. Referans bant genişliğini ayarlamak için, **auto-cost reference-bandwidth** *Mbps* yönlendirici yapılandırma komutunu kullanın.

```
Router(config-router)# auto-cost reference-bandwidth Mbps
```

Bu komut OSPF etki alanındaki her yönlendiricide yapılandırılmalıdır. Değerin Mbps olarak ifade edildiğine dikkat edin; bu nedenle, Gigabit Ethernet'in maliyetlerini ayarlamak için **auto-cost reference-bandwidth 1000** komutunu kullanın. 10 Gigabit Ethernet için, **auto-cost reference-bandwidth 10000** komutunu kullanın .

Varsayılan referans bant genişliğine dönmek için, **auto-cost reference-bandwidth 100** komutunu kullanın.

Hangi yöntem kullanılırsa kullanılsın, yapılandırmanın OSPF yönlendirme etki alanındaki tüm yönlendiricilere uygulanması önemlidir. Tablo, referans bant genişliği 10 Gigabit Ethernet bağlantısını barındıracak şekilde ayarlanmışsa OSPF maliyetini gösterir. Referans bant genişliği, FastEthernet'ten (100 Mbps) daha hızlı bağlantılar olduğu her zaman ayarlanmalıdır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| arayüz türü | Bps cinsinden Referans Bant Genişliği | | Bps cinsinden varsayılan bant genişliği | Maliyet |
|---|---|---|---|---|
| 10 Gigabit Ethernet 10 Gbps | 10.000.000.000 | ÷ | 10.000.000.000 | 1 |
| Gigabit Ethernet 1 Gbps | 10.000.000.000 | ÷ | 1.000.000.000 | 10 |
| Hızlı Ethernet 100 Mbps | 10.000.000.000 | ÷ | 100.000.000 | 100 |
| Ethernet 10 Mbps | 10.000.000.000 | ÷ | 10.000.000 | 1000 |

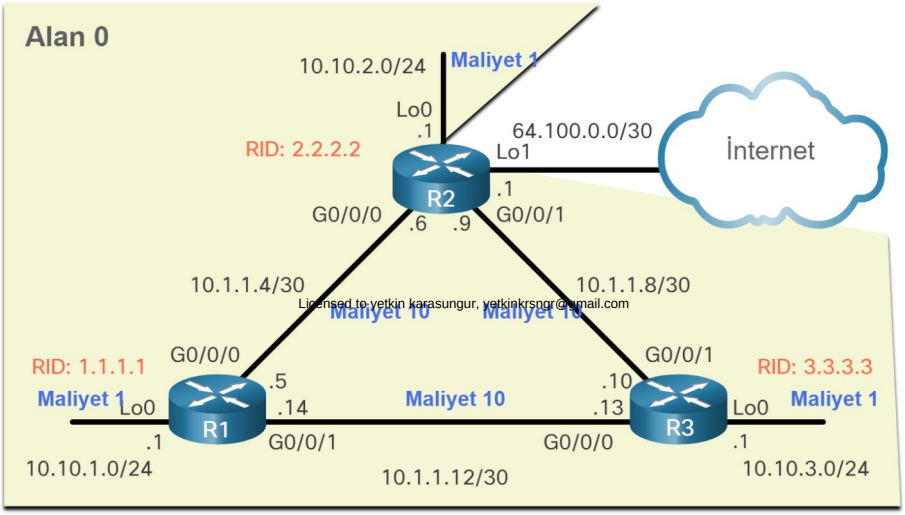
R1 GigabitEthernet 0/0/0 arayüzüne atanan geçerli OSPFv2 maliyetini doğrulamak için **show ip ospf interface g0/0/0** komutunu kullanın. 1 maliyetini nasıl gösterdiğine dikkat edin. O zaman, referans bant genişliğini ayarladıktan sonra maliyet şimdi 10'dur. Bu, gelecekte referans bant genişliğini yeniden ayarlamadan 10 Gigabit Ethernet arayüzüne ölçeklendirmeye izin verecektir.

Not : **auto-cost reference-bandwidth** komutu, doğru yol hesaplamalarını sağlamak için OSPF etki alanındaki tüm yönlendiricilerde tutarlı bir şekilde yapılandırılmalıdır.

```
R1# show ip ospf interface gigabitethernet0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 1
(output omitted)
R1# config t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# router ospf 10
R1(config-router)# auto-cost reference-bandwidth 10000
% OSPF: Reference bandwidth is changed.
        Please ensure reference bandwidth is consistent across all routers.
R1(config-router)# do show ip ospf interface gigabitethernet0/0/0
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 172.16.1.1/24, Area 0
  Process ID 10, Router ID 1.1.1.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
(output omitted)
```

## 32.7.3. OSPF Maliyet Değeri Değişimi

Bir OSPF yolunun maliyeti, bir yönlendiriciden hedef ağa biriken toplam maliyet değeridir. **auto-cost reference-bandwidth 10000** komutunun üç yönlendiricinin hepsinde yapılandırıldığı varsayılırsa, her yönlendirici arasındaki bağlantıların maliyeti artık 10'dur. Şekilde gösterildiği gibi geri döngü arabirimlerinin varsayılan maliyeti 1'dir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bu nedenle, her yönlendiricinin her ağa ulaşma maliyetini hesaplayabiliriz. Örneğin, R1'in 10.10.2.0/24 ağına ulaşmasının toplam maliyeti 11'dir. Bunun nedeni, R2'ye olan bağlantının maliyeti = 10 ve geri döngü varsayılan maliyetinin = 1. 10 + 1 = 11 olmasıdır.

Şekil 2'deki R1 yönlendirme tablosu, R2 LAN'a ulaşma ölçüsünün 11'lik bir maliyet olduğunu doğrular.

```
R1# show ip route | include 10.10.2.0
O        10.10.2.0/24 [110/11] via 10.1.1.6, 01:05:02, GigabitEthernet0/0/0
R1# show ip route 10.10.2.0
Routing entry for 10.10.2.0/24
  Known via "ospf 10", distance 110, metric 11, type intra area
  Last update from 10.1.1.6 on GigabitEthernet0/0/0, 01:05:13 ago
  Routing Descriptor Blocks:
  * 10.1.1.6, from 2.2.2.2, 01:05:13 ago, via GigabitEthernet0/0/0
      Route metric is 11, traffic share count is 1
R1#
```

### OSPF Maliyet Değerini Manuel Olarak Ayarlama

OSPF maliyet değerleri, OSPF tarafından seçilen rotayı etkilemek için değiştirilebilir. Örneğin, mevcut yapılandırmada, R1, 10.1.1.8/30 ağına yük dengeliyor. R2'ye biraz trafik ve R3'e biraz trafik gönderecek. Bunu yönlendirme tablosunda görebilirsiniz.

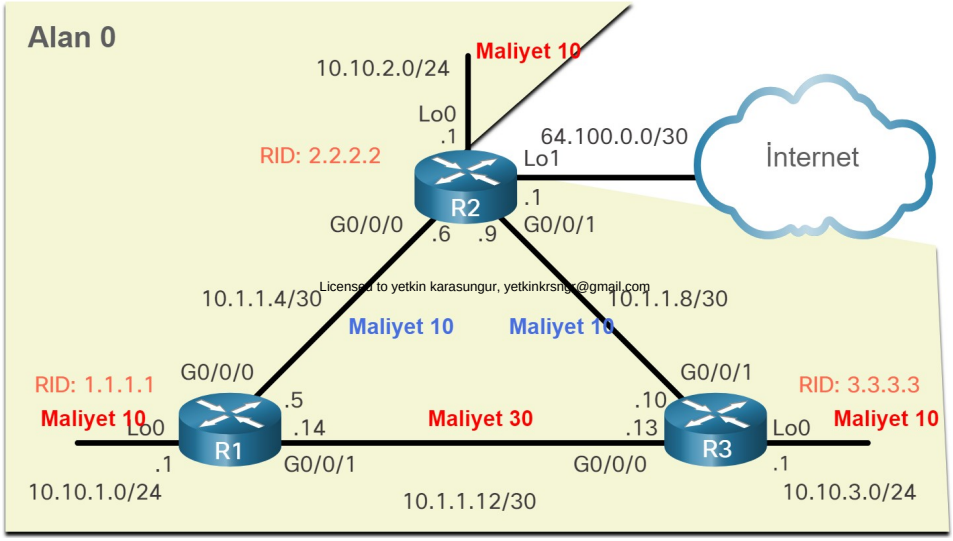
```
R1# show ip route ospf | begin 10
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
O        10.1.1.8/30 [110/20] via 10.1.1.13, 00:54:50, GigabitEthernet0/0/1
                     [110/20] via 10.1.1.6, 00:55:14, GigabitEthernet0/0/0
(output omitted)
R1#
```

Not : Bağlantının maliyetini değiştirmek istenmeyen sonuçlara yol açabilir. Bu nedenle, arayüz maliyet değerlerinin ayarlanması yalnızca sonuç tam olarak anlaşıldığında yapılandırılmalıdır.

Yönetici, R1 ile R2 arasındaki bağlantının kesilmesi durumunda trafiğin R2 üzerinden geçmesini ve R3'ü yedek yol olarak kullanmasını isteyebilir.

Maliyet değerini değiştirmenin bir başka nedeni, diğer satıcıların OSPF'yi farklı bir şekilde hesaplayabilmesidir. Maliyet değerini değiştirerek, yönetici OSPF çok satıcılı yönlendiriciler arasında paylaşılan yol maliyetlerinin yönlendirme tablolarına doğru bir şekilde yansıtıldığından emin olabilir.

Yerel OSPF yönlendiricisi tarafından bildirilen maliyet değerini diğer OSPF yönlendiricileriyle değiştirmek için, **ip ospf cost** *value* arabirim yapılandırma komutunu kullanın . Şekilde, Gigabit Ethernet hızlarını simüle etmek için geri döngü arayüzlerinin maliyetini 10 olarak değiştirmemiz gerekiyor. Ek olarak, R2 ve R3 arasındaki bağlantının maliyetini 30 olarak değiştireceğiz, böylece bu bağlantı bir yedek bağlantı olarak kullanılacak.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aşağıdaki örnek, R1 için yapılandırmadır.

```
R1(config)# interface g0/0/1
R1(config-if)# ip ospf cost 30
R1(config-if)# interface lo0
R1(config-if)# ip ospf cost 10
R1(config-if)# end
R1#
```

R2 ve R3 için OSPF maliyetlerinin yukarıdaki şekildeki topolojiyle eşleşecek şekilde yapılandırıldığı varsayıldığında, R1 için OSPF yolları aşağıdaki maliyet değerlerine sahip olacaktır. R1'in artık 10.1.1.8/30 ağına yük dengelemediğine dikkat edin. Aslında, tüm yollar, ağ yöneticisi tarafından istendiği gibi 10.1.1.6 aracılığıyla R2 üzerinden gider.

```
R1# show ip route ospf | begin 10
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
O        10.1.1.8/30 [110/20] via 10.1.1.6, 01:18:25, GigabitEthernet0/0/0
O        10.10.2.0/24 [110/20] via 10.1.1.6, 00:04:31, GigabitEthernet0/0/0
O        10.10.3.0/24 [110/30] via 10.1.1.6, 00:03:21, GigabitEthernet0/0/0
R1#
```

Not : **ip ospf cost** komutunun kullanılması, OSPF maliyet değerlerini değiştirmek için önerilen yöntem olsa da, bir yönetici bunu arabirim yapılandırma **bandwidth** *kbps* komutunu kullanarak da yapabilir . Ancak, bu yalnızca tüm yönlendiriciler Cisco ise işe yarar.

### Yedek Rotaya Yük Devretmeyi Test Edin

R1 ve R2 arasındaki bağlantı kesilirse ne olur? Gigabit Ethernet 0/0/0 arayüzünü kapatarak ve yönlendirme tablosunun sonraki atlama yönlendiricisi olarak R3'ü kullanacak şekilde güncellendiğini doğrulayarak bunu simüle edebiliriz. R1'in artık 10.1.1.4/30 ağına 10.1.1.13 ile R3 üzerinden 50 maliyet değeriyle ulaşabileceğine dikkat edin.

```
R1(config)# interface g0/0/0
R1(config-if)# shutdown
*Jun  7 03:41:34.866: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
*Jun  7 03:41:36.865: %LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively
down
*Jun  7 03:41:37.865: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed
state to down
R1(config-if)# end
R1# show ip route ospf | begin 10
      10.0.0.0/8 is variably subnetted, 8 subnets, 3 masks
O        10.1.1.4/30 [110/50] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
O        10.1.1.8/30 [110/40] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
O        10.10.2.0/24 [110/50] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
O        10.10.3.0/24 [110/40] via 10.1.1.13, 00:00:14, GigabitEthernet0/0/1
R1#
```

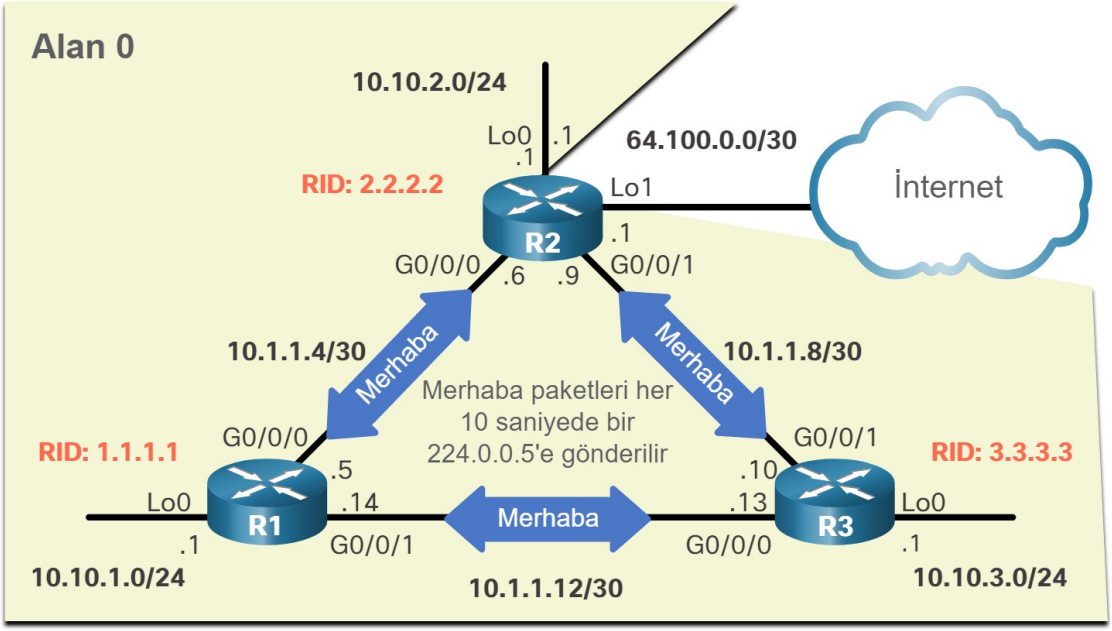
## 32.7.4.Merhaba Paketi Aralıkları (Hello Packet Intervals)

Şekilde gösterildiği gibi, OSPFv2 Merhaba paketleri, her 10 saniyede 224.0.0.5 çok noktaya yayın adresine (tüm OSPF yönlendiricileri) iletilir. Bu, çoklu erişim ve noktadan noktaya ağlarda varsayılan zamanlayıcı değeridir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not : Merhaba paketleri LAN arabirimlerinde gönderilmez çünkü bu arabirimler, yönlendirici yapılandırması passive-interface komutu kullanılarak pasif olarak ayarlanmıştır .

Ölü aralık (Dead İnterval), yönlendiricinin komşuyu aşağı-down bildirmeden önce bir Merhaba paketi almak için beklediği süredir. Dead aralığı, yönlendiriciler bir Merhaba paketi almadan önce sona ererse, OSPF bu komşuyu bağlantı durumu veritabanından (LSDB) kaldırır. Yönlendirici, LSDB'yi, OSPF'nin etkin olduğu tüm arabirimlerin dışında kalan komşu hakkında bilgi ile doldurur. Cisco, varsayılan olarak 4 kat Merhaba aralığı kullanır. Bu, çoklu erişim ve noktadan noktaya ağlarda 40 saniyedir.




## Merhaba ve Ölü Aralık Değerlerini (Hello&Dead Interval)Doğrulama

OSPF Hello ve Dead aralıkları, arabirim bazında yapılandırılabilir. OSPF aralıkları eşleşmelidir, aksi takdirde komşu bitişikliği oluşmaz. Mevcut yapılandırılmış OSPFv2 arabirim aralıklarını doğrulamak için , örnekte gösterildiği gibi **show ip ospf** arabirim komutunu kullanın. Gigabit Ethernet 0/0/0 Merhaba ve Ölü aralıkları, sırasıyla varsayılan 10 saniye ve 40 saniye olarak ayarlanmıştır.

```
R1# show ip ospf interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aşağıdaki örnekte gösterildiği gibi Ölü Zamanın 40 saniyeden geri sayımını görmek için **show ip ospf neighbor** komutunu kullanın. Varsayılan olarak, bu değer R1 komşudan bir Merhaba aldığında her 10 saniyede bir yenilenir.

```
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:35    10.1.1.13       GigabitEthernet0/0/1
2.2.2.2           0   FULL/  -        00:00:31    10.1.1.6        GigabitEthernet0/0/0
R1#
```

## Merhaba ve Ölü Aralık Değerlerini Değiştirme

Yönlendiricilerin ağ arızalarını daha kısa sürede algılaması için OSPF zamanlayıcılarının değiştirilmesi istenebilir. Bunu yapmak trafiği artırır, ancak bazen hızlı yakınsama ihtiyacı, oluşturduğu ekstra trafikten daha önemlidir.

Not : Varsayılan Merhaba ve Ölü aralıkları en iyi uygulamaları temel alır ve yalnızca nadir durumlarda değiştirilmelidir.

OSPFv2 Merhaba ve Ölü aralık, aşağıdaki arayüz yapılandırma modu komutları kullanılarak manuel olarak değiştirilebilir:

```
Router(config-if)# ip ospf hello-interval seconds
```

```
Router(config-if)# ip ospf dead-interval seconds
```

Aralıkları varsayılan değerlerine sıfırlamak için **no ip ospf hello-interval** ve **no ip ospf dead-interval** komutlarını kullanın.

Örnekte, R1 ve R2 arasındaki bağlantı için Merhaba aralığı 5 saniyeye değiştirilmiştir. Merhaba aralığını değiştirdikten hemen sonra Cisco IOS, Ölü aralığını otomatik olarak Merhaba aralığının dört katına değiştirir. Bununla birlikte, yapılandırmadaki yeni ölü aralığı gösterildiği gibi manuel olarak 20 saniyeye ayarlayarak belgeleyebilirsiniz.

Vurgulanan OSPFv2 bitiş mesajında gösterildiği gibi, R1'deki Ölü Zamanlayıcının süresi dolduğunda, R1 ve R2 bitişikliğini kaybeder. Bunun nedeni, R1 ve R2'nin aynı Merhaba aralığı ile yapılandırılması gerektiğidir. Komşuları doğrulamak için R1'de **show ip ospf neighbor** komutunu kullanın . Listelenen tek komşunun 3.3.3.3 (R3) yönlendirici olduğuna ve R1'in artık 2.2.2.2 (R2) komşusu ile bitişik olmadığına dikkat edin.

```
R1(config)# interface g0/0/0
R1(config-if)# ip ospf hello-interval 5
R1(config-if)# ip ospf dead-interval 20
R1(config-if)#
*Jun  7 04:56:07.571: %OSPF-5-ADJCHG: Process 10, Nbr 2.2.2.2 on GigabitEthernet0/0/0 from FULL to DOWN,
Neighbor Down: Dead timer expired
R1(config-if)# end
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:37    10.1.1.13       GigabitEthernet0/0/1
R1#
```

R1 ve R2 arasındaki yakınlığı geri yüklemek için, R2 Gigabit Ethernet 0/0/0 arayüzü Merhaba aralığı, aşağıdaki örnekte gösterildiği gibi 5 saniyeye ayarlanmıştır. Neredeyse hemen, IOS, bitişikliğin bir FULL durumuyla kurulduğunu belirten bir mesaj görüntüler. **Show ip ospf** arabirim komutunu kullanarak arabirim aralıklarını doğrulayın . Merhaba zamanının 5 saniye olduğuna ve Ölü Zamanın varsayılan 40 saniye yerine otomatik olarak 20 saniyeye ayarlandığına dikkat edin.

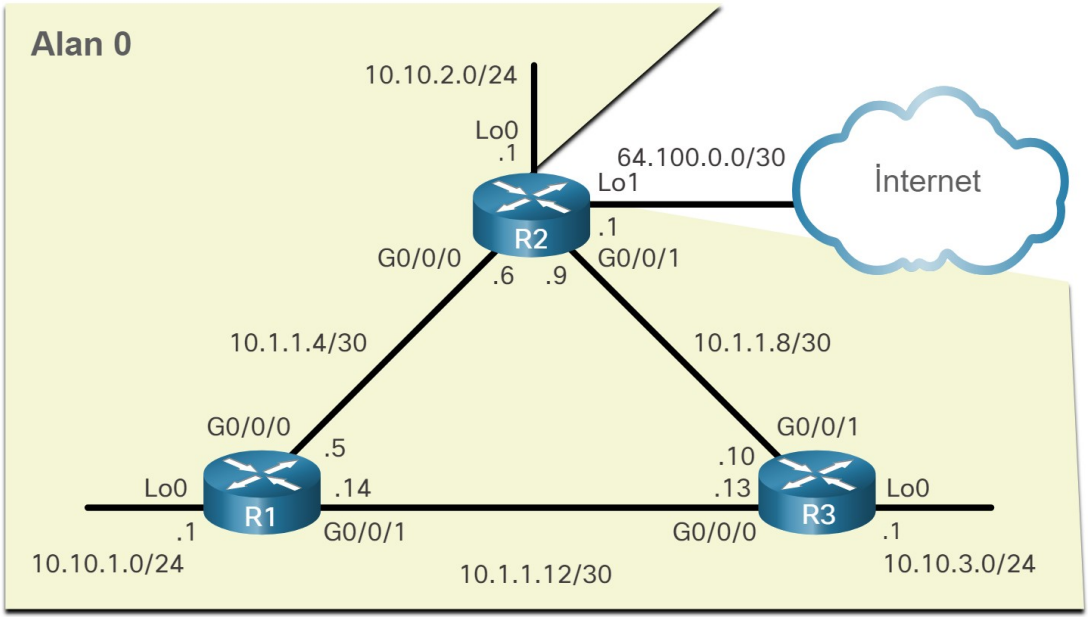
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R2(config)# interface g0/0/0
R2(config-if)# ip ospf hello-interval 5
*Jun  7 15:08:30.211: %OSPF-5-ADJCHG: Process 10, Nbr 1.1.1.1 on GigabitEthernet0/0/0 from LOADING to
FULL, Loading Done
R2(config-if)# end
R2# show ip ospf interface g0/0/0 | include Timer
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
R2# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:38    10.1.1.10       GigabitEthernet0/0/1
1.1.1.1           0   FULL/  -        00:00:17    10.1.1.5        GigabitEthernet0/0/0
R2#
```

## 32.8.Varsayılan Yol Yayılımı(Default Route Propagation)

### 32.8.1.OSPFv2'de Varsayılan Statik Yol Yayma

Ağ kullanıcılarınızın, ağınızdan İnternet gibi OSPF dışı ağlara paket göndermesi gerekecektir. Bu, kullanabilecekleri varsayılan bir statik yola sahip olmanız gereken yerdir. Şekildeki topolojide, R2 internete bağlıdır ve R1 ve R3'e varsayılan bir yol yaymalıdır. İnternete bağlı yönlendiriciye bazen kenar yönlendiricisi veya ağ geçidi yönlendiricisi denir. Bununla birlikte, OSPF terminolojisinde, bir OSPF yönlendirme etki alanı ile OSPF olmayan bir ağ arasında bulunan yönlendiriciye, otonom sistem sınır yönlendiricisi (autonomous system boundary router - ASBR) denir.




R2'nin internete ulaşması için gereken tek şey, servis sağlayıcıya giden varsayılan statik bir yoldur.

Not : Bu örnekte, servis sağlayıcıya olan bağlantıyı simüle etmek için IPv4 adresi 64.100.0.1 olan bir geridöngü arabirimi kullanılır.

Varsayılan bir yolu yaymak için, kenar yönlendiricisinin (R2) aşağıdaki şekilde yapılandırılması gerekir:

- **ip route 0.0.0.0 0.0.0.0 [next-hop-address | exit-intf]** komutu.
- **default-information originate** komutu yönlendirici R2'ye varsayılan yol bilgisinin kaynağı olmasını ve OSPF güncellemelerinde varsayılan statik yolu yaymasını söyler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aşağıdaki örnekte, R2, internet bağlantısını simüle etmek için bir geridöngü ile yapılandırılmıştır. Ardından, varsayılan bir yol yapılandırılır ve yönlendirme alanındaki diğer tüm OSPF yönlendiricilerine yayılır.

Not : Statik yolları yapılandırırken, en iyi uygulama sonraki atlama IP adresini kullanmaktır. Bununla birlikte, internete bir bağlantı simüle ederken, sonraki atlama IP adresi yoktur. Bu nedenle, exit-intf argümanını kullanıyoruz.

```
R2(config)# interface lo1
R2(config-if)# ip address 64.100.0.1 255.255.255.252
R2(config-if)# exit
R2(config)# ip route 0.0.0.0 0.0.0.0 loopback 1
%Default route without gateway, if not a point-to-point interface, may impact performance
R2(config)# router ospf 10
R2(config-router)# default-information originate
R2(config-router)# end
R2#
```

### Yayılmış Varsayılan Yolu Doğrulama

**Show ip route** komutunu kullanarak R2 üzerindeki varsayılan rota ayarlarını doğrulayabilirsiniz . Ayrıca R1 ve R3'ün varsayılan bir yol aldığını da doğrulayabilirsiniz.

R1 ve R3'teki yol kaynağının O * E2 olduğuna dikkat edin, bu da OSPFv2 kullanılarak öğrenildiğini gösterir. Yıldız işareti, bunu varsayılan yol için iyi bir aday olarak tanımlar. E2 ataması, bunun harici bir yol olduğunu tanımlar. E1 ve E2'nin anlamı bu kitabın kapsamı dışındadır.

```
R1# show ip route | begin Gateway
Gateway of last resort is 10.1.1.6 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 10.1.1.6, 00:11:08, GigabitEthernet0/0/0
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
C        10.1.1.4/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.5/32 is directly connected, GigabitEthernet0/0/0
O        10.1.1.8/30 [110/20] via 10.1.1.6, 00:58:59, GigabitEthernet0/0/0
C        10.1.1.12/30 is directly connected, GigabitEthernet0/0/1
L        10.1.1.14/32 is directly connected, GigabitEthernet0/0/1
C        10.10.1.0/24 is directly connected, Loopback0
L        10.10.1.1/32 is directly connected, Loopback0
O        10.10.2.0/24 [110/20] via 10.1.1.6, 00:58:59, GigabitEthernet0/0/0
O        10.10.3.0/24 [110/30] via 10.1.1.6, 00:48:11, GigabitEthernet0/0/0
R1#
```

```
R2# show ip route | begin Gateway
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
S*    0.0.0.0/0 is directly connected, Loopback1
      10.0.0.0/8 is variably subnetted, 9 subnets, 3 masks
C        10.1.1.4/30 is directly connected, GigabitEthernet0/0/0
L        10.1.1.6/32 is directly connected, GigabitEthernet0/0/0
C        10.1.1.8/30 is directly connected, GigabitEthernet0/0/1
L        10.1.1.9/32 is directly connected, GigabitEthernet0/0/1
O        10.1.1.12/30 [110/40] via 10.1.1.10, 00:48:42, GigabitEthernet0/0/1
                      [110/40] via 10.1.1.5, 00:59:30, GigabitEthernet0/0/0
O        10.10.1.0/24 [110/20] via 10.1.1.5, 00:59:30, GigabitEthernet0/0/0
C        10.10.2.0/24 is directly connected, Loopback0
L        10.10.2.1/32 is directly connected, Loopback0
O        10.10.3.0/24 [110/20] via 10.1.1.10, 00:48:42, GigabitEthernet0/0/1
      64.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        64.100.0.0/30 is directly connected, Loopback1
L        64.100.0.1/32 is directly connected, Loopback1
R2#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 32.9.Tek Alanlı OSPFv2 Yapılandırmasını Doğrulama

### 32.9.1.OSPF Komşularını Doğrulama

Tek alanlı OSPFv2'yi yapılandırdıysanız, yapılandırmalarınızı doğrulamanız gerekecektir. Bu konu, OSPF'yi doğrulamak için kullanabileceğiniz birçok komutun ayrıntılarını verir.

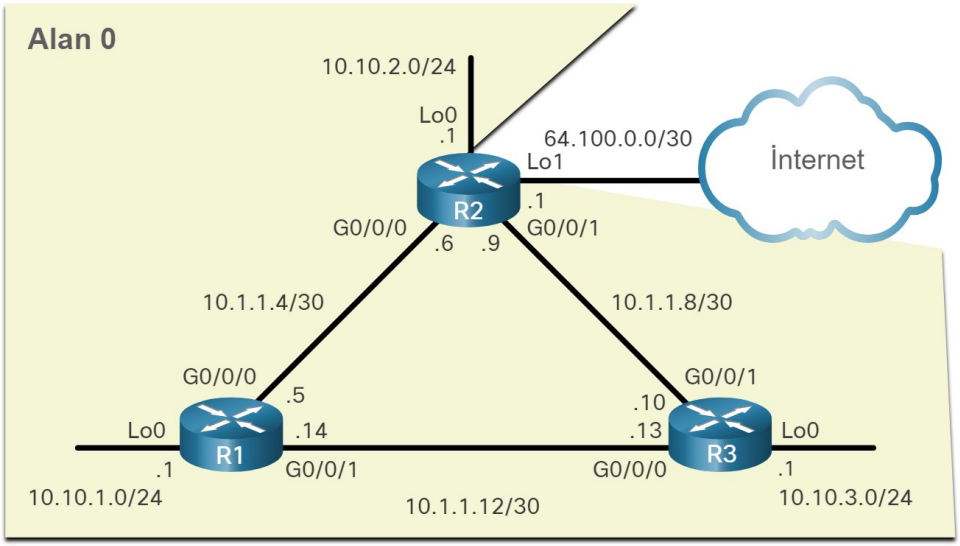
Bildiğiniz gibi, aşağıdaki iki komut özellikle yönlendirmeyi doğrulamak için kullanışlıdır:

- **show ip interface brief** - Bu, istenen arabirimlerin doğru IP adresiyle etkin olduğunu doğrular.
- **show ip route** - Bu, yönlendirme tablosunun beklenen tüm yolları içerdiğini doğrular.

OSPF'nin beklendiği gibi çalıştığını belirlemek için ek komutlar şunları içerir:

- **show ip ospf neighbor**
- **show ip protocols**
- **show ip ospf**
- **show ip ospf interface**

**OSPFv2 Referans Topolojisi**




Yönlendiricinin komşu yönlendiricileriyle bir bitişiklik oluşturduğunu doğrulamak için **show ip ospf neighbor** komutunu kullanın. Komşu yönlendiricinin yönlendirici kimliği görüntülenmiyorsa veya FULL durumunda görünmüyorsa, iki yönlendirici bir OSPFv2 bitişikliği oluşturmamış demektir.

İki yönlendirici bitişiklik oluşturmazsa, bağlantı durumu bilgisi değiş tokuş edilmez. Eksik LSDB'ler, hatalı SPF ağaçlarına ve yönlendirme tablolarına neden olabilir. Hedef ağlara giden yollar mevcut olmayabilir veya en uygun yol olmayabilir.

Not : DR olmayan veya BDR olmayan başka bir yönlendiriciyle komşu ilişkisi olan DR olmayan veya BDR olmayan bir yönlendirici, tam yerine iki yönlü bir bitişik görüntüleyecektir.

Aşağıdaki komut çıktısı R1'in komşu tablosunu görüntüler.

```
R1# show ip ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
3.3.3.3           0   FULL/  -        00:00:19    10.1.1.13       GigabitEthernet0/0/1
2.2.2.2           0   FULL/  -        00:00:18    10.1.1.6        GigabitEthernet0/0/0
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Her komşu için bu komut aşağıdakileri görüntüler:

- Komşu Kimliği - Bu, komşu yönlendiricinin yönlendirici kimliğidir.
- Pri - Bu, arabirimin OSPFv2 önceliğidir. Bu değer DR ve BDR seçimlerinde kullanılır.
- Durum - Bu, arayüzün OSPFv2 durumudur. FULL durumu, yönlendirici ve komşusunun aynı OSPFv2 LSDB'lerine sahip olduğu anlamına gelir. Ethernet gibi çok erişimli ağlarda, bitişik iki yönlendiricinin durumları 2- WAY olarak görüntülenebilir. Çizgi, ağ türü nedeniyle DR veya BDR gerekmediğini gösterir.
- Ölü Zaman - Bu, yönlendiricinin komşuyu devre dışı bırakmadan önce komşudan bir OSPFv2 Merhaba paketi almak için beklediği süredir. Arayüz bir Merhaba paketi aldığında bu değer sıfırlanır.
- Adres - Bu, yönlendiricinin doğrudan bağlı olduğu komşunun arayüzünün IPv4 adresidir.
- Arayüz - Bu, yönlendiricinin komşuyla bitişik oluşturduğu arayüzdür.
-

Aşağıdakiler meydana gelirse iki yönlendirici bir OSPFv2 bitişikliği oluşturmayabilir:

- Alt ağ maskeleri eşleşmiyor ve yönlendiricilerin ayrı ağlarda olmasına neden oluyor.
- OSPFv2 Merhaba veya Ölü Zamanlayıcılar eşleşmiyor.
- OSPFv2 Ağ Türleri eşleşmiyor.
- Eksik veya yanlış bir OSPFv2 network komutu var.

## 32.9.2.OSPF Protokol Ayarlarını Doğrulama

**Show ip protocols** aşağıdaki komut çıktısında görüldüğü gibi bu komut, hayati OSPF yapılandırma bilgilerini doğrulamak için hızlı bir yoldur. Bu, OSPFv2 işlem kimliğini, yönlendirici kimliğini, OSPF yollarının tanıtımını yapmak için açıkça yapılandırılmış arabirimleri, yönlendiricinin güncellemeleri aldığı komşuları ve OSPF için 110 olan varsayılan yönetim mesafesini içerir.

```
R1# show ip protocols
*** IP Routing is NSF aware ***
(output omitted)
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 1.1.1.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    Loopback0
    GigabitEthernet0/0/1
    GigabitEthernet0/0/0
  Routing Information Sources:
    Gateway         Distance      Last Update
    3.3.3.3              110      00:09:30
    2.2.2.2              110      00:09:58
  Distance: (default is 110)
R1#
```

## 32.9.3.OSPF İşlem Bilgilerini Doğrulama

**show ip ospf** aşağıdaki komut çıkışında gösterilen komut aynı zamanda, OSPFv2 işlem kimliği ve yönlendirici kimliğini incelemek için kullanılabilir. Bu komut OSPFv2 alan bilgilerini ve SPF algoritmasının en son çalıştırıldığı zamanı görüntüler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# show ip ospf
  Routing Process "ospf 10" with ID 1.1.1.1
  Start time: 00:01:47.390, Time elapsed: 00:12:32.320
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Supports area transit capability
  Supports NSSA (compatible with RFC 3101)
  Supports Database Exchange Summary List Optimization (RFC 5243)
  Event-log enabled, Maximum number of events: 1000, Mode: cyclic
  Router is not originating router-LSAs with maximum metric
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPFs 10000 msecs
External flood list length 0
IETF NSF helper support enabled
Cisco NSF helper support enabled
Reference bandwidth unit is 10000 mbps
   Area BACKBONE(0)
       Number of interfaces in this area is 3
       Area has no authentication
       SPF algorithm last executed 00:11:31.231 ago
       SPF algorithm executed 4 times
       Area ranges are
       Number of LSA 3. Checksum Sum 0x00E77E
       Number of opaque link LSA 0. Checksum Sum 0x000000
       Number of DCbitless LSA 0
       Number of indication LSA 0
       Number of DoNotAge LSA 0
       Flood list length 0
```

## 32.9.4.OSPF Arayüz Ayarlarını Doğrulama

**show ip ospf interfaces** komutu her OSPFv2 özellikli arayüz için ayrıntılı bir listesini sağlar. Gigabit Ethernet 0/0/0 için aşağıdaki çıktıda gösterildiği gibi, sadece o arayüzün ayarlarını görüntülemek için bir arayüz belirtin. Bu komut, işlem kimliğini, yerel yönlendirici kimliğini, ağ türünü, OSPF maliyetini, çoklu erişim bağlantıları (gösterilmemiştir) ve bitişik komşuları hakkında DR ve BDR bilgilerini gösterir.

```
R1# show ip ospf interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  Internet Address 10.1.1.5/30, Area 0, Attached via Interface Enable
  Process ID 10, Router ID 1.1.1.1, Network Type POINT_TO_POINT, Cost: 10
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           10        no          no            Base
  Enabled by interface config, including secondary ip addresses
  Transmit Delay is 1 sec, State POINT_TO_POINT
  Timer intervals configured, Hello 5, Dead 20, Wait 20, Retransmit 5
    oob-resync timeout 40
    Hello due in 00:00:01
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2
  Suppress hello for 0 neighbor(s)
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

OSPFv2'nin etkin olduğu arabirimlerin hızlı bir özetini almak için , aşağıdaki komut çıktısında gösterildiği gibi **show ip ospf interface brief** komutunu kullanın. Bu komut, aşağıdakiler dahil önemli bilgileri görmek için kullanışlıdır:

- Hangi arayüzler OSPF'ye katılıyor
- Tanıtımı yapılan ağlar (IP Adresi / Maske)
- Her bağlantının maliyeti
- Ağ durumu
- Her bağlantıdaki komşuların sayısı

```
R1# show ip ospf interface brief
Interface     PID   Area            IP Address/Mask    Cost  State Nbrs F/C
Lo0           10    0               10.10.1.1/24       10    P2P   0/0
Gi0/0/1       10    0               10.1.1.14/30       30    P2P   1/1
Gi0/0/0       10    0               10.1.1.5/30        10    P2P   1/1
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 33.Bölüm: Ağ Güvenliği

## 33.1.Günümüzde Siber Güvenlik

### 33.1.1.Mevcut Durum

Siber suçlular artık kritik altyapı ve sistemleri ortadan kaldırmak için gerekli uzmanlığa ve araçlara sahip. Araçları ve teknikleri gelişmeye devam ediyor.

Siber suçlular, kötü amaçlı yazılımları benzeri görülmemiş karmaşıklık ve etki düzeylerine taşıyor. Faaliyetlerini gizlemek için gizlilik ve kaçınma tekniklerini kullanma konusunda daha usta hale geliyorlar. Son olarak, siber suçlular güvenlikteki savunmasız boşlukları kullanıyor.

Ağ güvenliği ihlalleri e-ticareti bozabilir, iş verilerinin kaybına neden olabilir, kişilerin mahremiyetini tehdit edebilir ve bilgilerin bütünlüğünü tehlikeye atabilir. Bu ihlaller, şirketler için gelir kaybına, fikri mülkiyet hırsızlığına, davalara neden olabilir ve hatta kamu güvenliğini tehdit edebilir.

Güvenli bir ağın sürdürülmesi, ağ kullanıcılarının güvenliğini sağlar ve ticari çıkarları korur. Organizasyonların, düşmanların siber silahlarını bir araya getirme ve iyileştirme hızını ve ölçeğini fark edebilecek bireylere ihtiyacı var. Tüm kullanıcılar tablodaki güvenlik koşullarından haberdar olmalıdır.

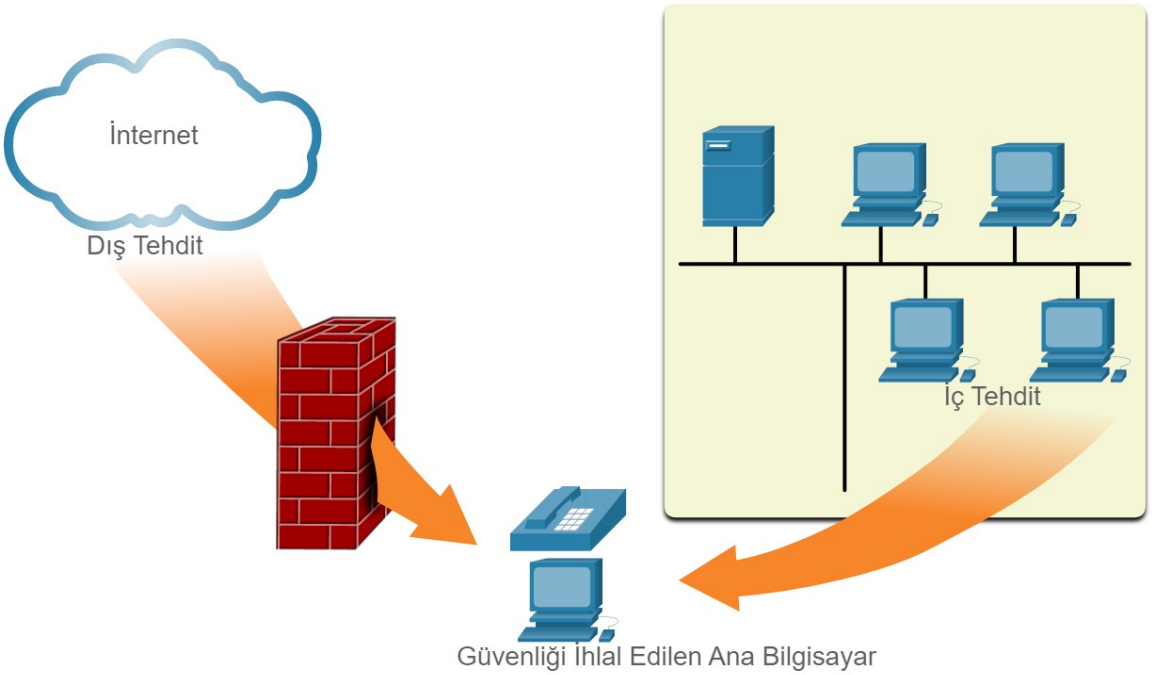
| Güvenlik Terimleri | Açıklama |
|---|---|
| Varlıklar-Assets | Bir varlık, kuruluş için değerli olan herhangi bir şeydir. İnsanları, ekipmanları, kaynakları ve verileri içerir. |
| Güvenlik Açığı-Vulnerability | Güvenlik açığı, bir sistemdeki veya tasarımındaki, bir tehdit tarafından kötüye kullanılabilecek bir zayıflıktır. |
| Tehdit-Threat | Tehdit, bir şirketin varlıkları, verileri veya ağ işlevselliği için potansiyel bir tehlikedir. |
| İstismar-Expolit | İstismar, bir güvenlik açığından yararlanan bir mekanizmadır. |
| Azaltma-Mitigation | Azaltma, potansiyel bir tehdit veya riskin olasılığını veya ciddiyetini azaltan karşı önlemdir. Ağ güvenliği, birden çok azaltma tekniği içerir. |
| Risk | Risk, bir organizasyonu olumsuz yönde etkilemek amacıyla, bir varlığın güvenlik açığından yararlanma tehdididir. Risk, bir olayın meydana gelme olasılığı ve sonuçları kullanılarak ölçülür. |

Varlıklar tanımlanmalı ve korunmalıdır. Güvenlik açıkları, bir tehdit haline gelmeden ve istismar edilmeden önce ele alınmalıdır. Saldırı öncesinde, sırasında ve sonrasında azaltma teknikleri gereklidir.

### 33.1.2.Ağ Saldırı Vektörleri

Saldırı vektörü, tehdit aktörünün bir sunucuya, ana bilgisayara veya ağa erişim sağlayabileceği bir yoldur. Saldırı vektörleri, şekilde gösterildiği gibi kurumsal ağın içinden veya dışından kaynaklanır. Örneğin, tehdit aktörleri, ağ işlemlerini kesintiye uğratmak ve bir hizmet reddi (DoS) saldırısı oluşturmak için internet üzerinden bir ağı hedefleyebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Not : Bir DoS saldırısı, bir ağ cihazı veya uygulaması yetersiz kaldığında ve artık yasal kullanıcılardan gelen istekleri destekleyemediğinde gerçekleşir.

Dahili bir kullanıcı, yanlışlıkla veya kasıtlı olarak şunları yapabilir:

- Gizli verileri çalıp ve çıkarılabilir medyaya, e-postaya, mesajlaşma yazılımına ve diğer medyaya kopyalama.
- Dahili sunuculardan veya ağ altyapısı cihazlarından ödün verme.
- Kritik bir ağ bağlantısını kesen ve bir ağ kesintisine neden olma.
- Virüs bulaşmış bir USB sürücüsünü kurumsal bir bilgisayar sistemine bağlama.

İç tehditler, dış tehditlere göre daha büyük hasara neden olma potansiyeline sahiptir çünkü dahili kullanıcılar binaya ve altyapı cihazlarına doğrudan erişime sahiptir. Çalışanlar ayrıca kurumsal ağ, kaynakları ve gizli verileri hakkında bilgi sahibi olabilir.

Ağ güvenliği uzmanları, hem harici hem de dahili tehditleri azaltmak için araçlar ve teknikler uygulamalıdır.

### 33.1.3.Veri Kaybı (Data Loss)

Veriler, muhtemelen bir kuruluşun en değerli varlığıdır. Organizasyonel veriler, araştırma ve geliştirme verilerini, satış verilerini, finansal verileri, insan kaynakları ve yasal verileri, çalışan verilerini, yüklenici verilerini ve müşteri verilerini içerebilir.

Veri kaybı veya veri hırsızlığı, verilerin kasıtlı veya kasıtsız olarak kaybolması, çalınması veya dış dünyaya sızdırılmasıdır. Veri kaybı şunlara neden olabilir:

- Marka hasarı ve itibar kaybı
- Rekabet avantajı kaybı
- Müşteri kaybı
- Gelir kaybı
- Para cezaları ve para cezaları ile sonuçlanan dava / yasal işlemler
- Etkilenen tarafları bilgilendirmek ve ihlalden kurtulmak için önemli maliyet ve çaba

Licensed to tekin kamsungur, yetkinkrsgor@gmail.com

Yaygın veri kaybı vektörleri tabloda gösterilmektedir.

| Veri Kaybı Vektörleri | Açıklama |
|---|---|
| E-posta / Sosyal Ağ | Ele geçirilen e-posta veya anlık mesajlar yakalanabilir ve gizli bilgileri açığa çıkarabilir. |
| Şifrelenmemiş Cihazlar | Veriler bir şifreleme algoritması kullanılarak depolanmazsa, hırsız değerli gizli verileri alabilir. |
| Bulut Depolama Cihazları | Zayıf güvenlik ayarları nedeniyle buluta erişim tehlikeye atılırsa hassas veriler kaybolabilir. |
| Çıkarılabilir Medya | Risklerden biri, bir çalışanın bir USB sürücüsüne yetkisiz veri aktarımı yapabilmesidir. Diğer bir risk de, değerli kurumsal veriler içeren bir USB sürücüsünün kaybolabilmesidir. |
| Basılı kopya | Gizli veriler artık gerekmediğinde parçalanmalıdır. |
| Uygun Olmayan Erişim Kontrolü | Güvenliği ihlal edilmiş parolalar veya zayıf parolalar, bir tehdit aktörünün kurumsal verilere kolay erişimini sağlayabilir. |

Ağ güvenliği uzmanları, kuruluşun verilerini korumalıdır. Stratejik, operasyonel ve taktik önlemleri birleştiren çeşitli Veri Kaybı Önleme-Data Loss Prevention (DLP) kontrolleri uygulanmalıdır.

## 33.2.Tehdit Aktörleri

### 33.2.1.Bilgisayar Korsanları (Hackerlar)

Hacker, bir tehdit aktörünü tanımlamak için kullanılan yaygın bir terimdir. Başlangıçta terim, bir programcı ve bilgisayar korsanlığı gibi yetenekli bir bilgisayar uzmanı olan birini ifade ediyordu ve akıllıca bir çözümdü. Terim daha sonra bugün bildiğimiz şeye dönüştü.

Tabloda gösterildiği gibi, beyaz şapkalı hacker, siyah şapkalı hacker ve gri şapkalı hacker terimleri genellikle bir hacker türünü tanımlamak için kullanılır.

| Hacker Türü | Açıklama |
|---|---|
| Beyaz Şapkalı Hackerlar | Bunlar, programlama becerilerini iyi, etik ve yasal amaçlar için kullanan etik bilgisayar korsanlarıdır. Beyaz şapkalı korsanlar, ağ güvenlik açıklarını keşfetmek için bilgisayar güvenlik sistemleri bilgilerini kullanarak ağları ve sistemleri tehlikeye atmak amacıyla ağ penetrasyon testleri gerçekleştirebilir. Güvenlik açıkları, güvenlik açıklarından yararlanılmadan önce düzeltmeleri için geliştiricilere bildirilir. |
| Gri Şapkalı Hackerlar | Bunlar, suç işleyen ve muhtemelen etik olmayan şeyler yapan kişilerdir, ancak kişisel kazanç veya zarar vermek için değil. Gri şapkalı bilgisayar korsanları, ağlarının güvenliğini ihlal ettikten sonra etkilenen kuruluşa bir güvenlik açığını ifşa edebilir. |
| Siyah Şapkalı Hackerlar | Bunlar, kişisel kazanç için veya ağlara saldırmak gibi kötü niyetli nedenlerle bilgisayar ve ağ güvenliğini tehlikeye atan etik olmayan suçlulardır. |

Not : Bu kitapta hacker terimini bu bölüm dışında kullanmayacağız. Tehdit aktörü terimini kullanacağız. Tehdit aktörü terimi, bilgisayar korsanlarını içerir. Ancak tehdit aktörü, kasıtlı veya kasıtsız olarak bir saldırının kaynağı olan herhangi bir cihazı, kişiyi, grubu veya ulus devleti de içerir.

### 33.2.2.Siber Suçlular

Siber suçluların tüketicilerden ve işletmelerden milyarlarca dolar çaldıkları tahmin ediliyor. Siber suçlular, saldırı araç kitleri, sıfır gün istismar kodu, botnet hizmetleri, bankacılık Truva atları, tuş kaydediciler ve çok daha fazlasını satın aldıkları, sattıkları ve ticaretini yaptıkları bir yeraltı ekonomisinde faaliyet gösterirler. Ayrıca çaldıkları özel bilgileri ve fikri mülkiyeti alıp satarlar. Siber suçlular küçük işletmeleri ve tüketicileri olduğu kadar büyük işletmeleri ve tüm endüstrileri hedef alır.

Lisans bir kişiye aittir. Kurumsal dağıtım yapılamaz.

### 33.2.3.Hacktivistler

Hacktivist grupların iki örneği Anonymous ve WikiLeaks'dir. Çoğu bilgisayar korsanlığı grubu iyi organize edilmemiş olsa da, hükümetler ve işletmeler için önemli sorunlara neden olabilirler. Hacktivistler, oldukça basit, ücretsiz olarak bulunabilen araçlara güvenme eğilimindedir.

### 33.2.4.Devlet Destekli Hackerlar

Devlet destekli bilgisayar korsanları, genellikle sıfırıncı gün (zero day) güvenlik açıkları adı verilen daha önce keşfedilmemiş yazılım güvenlik açıklarını kullanarak gelişmiş, özelleştirilmiş saldırı kodu oluşturur. Devlet destekli saldırıya bir örnek, İran'ın nükleer zenginleştirme yeteneklerine zarar vermek için oluşturulan Stuxnet kötü amaçlı yazılımıdır.

## 33.3.Tehdit Aktörü Araçları

### 33.3.1.Saldırı Araçlarına Giriş

Bir güvenlik açığından yararlanmak için, tehdit aktörünün bir tekniği veya araca sahip olması gerekir. Yıllar geçtikçe, saldırı araçları daha sofistike ve son derece otomatik hale geldi. Bu yeni araçların uygulanması için daha az teknik bilgi gerekir.

### 33.3.2.Güvenlik Araçlarının Gelişimi

Etik hackleme, ağı test etmek ve verilerini güvende tutmak için kullanılan birçok farklı araç türünü içerir. Bir ağın ve sistemlerinin güvenliğini doğrulamak için birçok ağ sızma testi aracı geliştirilmiştir. Bu araçların çoğunun siyah şapkalı korsanlar tarafından sömürü amacıyla kullanılabilmesi talihsiz bir durumdur.

Siyah şapka korsanları da birçok bilgisayar korsanlığı aracı oluşturdu. Bu araçlar, kötü amaçla yapılmıştır. Beyaz şapkalı bilgisayar korsanları, ağ sızma testleri gerçekleştirirken bu araçları nasıl kullanacaklarını da bilmelidir.

Tablo, yaygın sızma testi araçlarının kategorilerini vurgular. Beyaz şapkalılar ve siyah şapkalılar tarafından bazı aletlerin nasıl kullanıldığına dikkat edin. Her zaman yeni araçlar geliştirildiği için listenin kapsamlı olmadığını unutmayın.

| Penetrasyon Test Aracı | Açıklama |
|---|---|
| Parola Kırıcılar | Parola kırma araçları genellikle parola kurtarma araçları olarak adlandırılır ve bir parolayı kırmak veya kurtarmak için kullanılabilir. Bu, ya veri şifrelemesini atladıktan sonra orijinal parolayı kaldırarak ya da parolayı doğrudan keşfederek gerçekleştirilir. Parola kırıcılar, parola kırmak için tekrar tekrar tahminler yapar. Parola kırma araçlarına örnek olarak John the Ripper, Ophcrack, L0phtCrack, THC Hydra, RainbowCrack ve Medusa verilebilir. |
| Kablosuz Hacking Araçları | Kablosuz bilgisayar korsanlığı araçları, güvenlik açıklarını tespit etmek için bir kablosuz ağa kasıtlı olarak girmek için kullanılır. Kablosuz bilgisayar korsanlığı araçlarına örnek olarak Aircrack-ng, Kismet, InSSIDer, KisMAC, Firesheep ve NetStumbler verilebilir. |
| Ağ Tarama ve Bilgisayar Korsanlığı Araçları | Ağ tarama araçları, açık TCP veya UDP bağlantı noktaları için ağ cihazlarını, sunucuları ve ana bilgisayarları araştırmak için kullanılır. Tarama araçlarına örnek olarak Nmap, SuperScan, Angry IP Scanner ve NetScanTools verilebilir. |
| Paket Oluşturma Araçları | Bu araçlar, özel olarak hazırlanmış sahte paketleri kullanarak bir güvenlik duvarının sağlamlığını araştırmak ve test etmek için kullanılır. Örnekler Hping, Scapy, Socat, Yersinia, Netcat, Nping ve Nemesis verilebilir. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Penetrasyon Test Aracı | Açıklama |
|---|---|
| Paket Koklayıcılar | Bu araçlar, geleneksel Ethernet LAN'lar veya WLAN'lar içindeki paketleri yakalamak ve analiz etmek için kullanılır. Araçlar arasında Wireshark, Tcpdump, Ettercap, Dsniff, EtherApe, Paros, Fiddler, Ratproxy ve SSLstrip bulunur. |
| Rootkit Dedektörleri | Bu, beyaz şapkalılar tarafından kurulu rootkitleri tespit etmek için kullanılan bir dizin ve dosya bütünlüğü denetleyicisidir. Örnek araçlar arasında AIDE, Netfilter ve PF: OpenBSD Packet Filter bulunur. |
| Fuzzers Güvenlik Açıklarını Aramak İçin | Fuzzers, tehdit aktörleri tarafından bir bilgisayarın güvenlik açıklarını keşfetmek için kullanılan araçlardır. Örnekleri arasında Skipfish, Wapiti ve W3af bulunur. |
| Adli Bilişim Araçları | Bu araçlar, beyaz şapkalı bilgisayar korsanları tarafından bir bilgisayarda var olan herhangi bir kanıtı bulmak için kullanılır. Araçlara örnek olarak Sleuth Kit, Helix, Maltego ve Encase verilebilir. |
| Hata ayıklayıcılar | Bu araçlar, açıklardan yararlanmaya yararayan program yazarken ikili dosyaları tersine çevirmek için siyah şapkalılar tarafından kullanılır. Kötü amaçlı yazılımları analiz ederken beyaz şapkalar tarafından da kullanılırlar. Hata ayıklama araçları GDB, WinDbg, IDA Pro ve Immunity Debugger'ı içerir. |
| Bilgisayar Korsanlığı İşletim Sistemleri | Bunlar, bilgisayar korsanlığı için optimize edilmiş araçlarla önceden yüklenmiş özel olarak tasarlanmış işletim sistemleridir. Özel olarak tasarlanmış bilgisayar korsanlığı işletim sistemlerine örnek olarak Kali Linux, Knoppix, BackBox Linux verilebilir. |
| Şifreleme Araçları | Şifreleme araçları, şifrelenmiş verilere yetkisiz erişimi önlemek için verileri kodlamak için algoritma şemaları kullanır. Bu araçlara örnek olarak VeraCrypt, CipherShed, OpenSSH, OpenSSL, Tor, OpenVPN ve Stunnel verilebilir. |
| Güvenlik Açığı Sömürü Araçları | Bu araçlar, uzaktaki bir ana bilgisayarın bir güvenlik saldırısına açık olup olmadığını belirler. Güvenlik açığı istismar araçlarına örnek olarak Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit verilebilir. |
| Güvenlik Açığı Tarayıcıları | Bu araçlar, açık bağlantı noktalarını belirlemek için bir ağı veya sistemi tarar. Ayrıca bilinen güvenlik açıklarını taramak ve VM'leri, BYOD cihazlarını ve istemci veritabanlarını taramak için de kullanılabilirler.Araç örnekleri arasında Nipper, Secunia PSI, Core Impact, Nessus v6, SAINT, Netsparker ve Open VAS bulunur. |

Not : Bu araçların çoğu UNIX veya Linux tabanlıdır; bu nedenle, bir güvenlik uzmanının güçlü bir UNIX ve Linux geçmişi olmalıdır.

### 33.3.3.Saldırı Türleri

Tehdit aktörleri, saldırılar oluşturmak için daha önce bahsedilen saldırı araçlarını veya araçların bir kombinasyonunu kullanabilir. Tabloda yaygın saldırı türleri gösterilmektedir. Ancak, yeni saldırı güvenlik açıkları sürekli keşfedildiği için saldırı listesi kapsamlı değildir.

| Saldırı Tipi | Açıklama |
|---|---|
| Gizlice Dinleme Saldırısı | Bu, bir tehdit aktörünün ağ trafiğini yakalayıp "dinlediği" zamandır. Bu saldırı aynı zamanda koklama veya gözetleme olarak da adlandırılır. |
| Veri Değiştirme Saldırısı | Tehdit aktörleri kurumsal trafiği yakaladıysa, gönderenin veya alıcının bilgisi olmadan paketteki verileri değiştirebilirler. |
| IP Adresi Sahtekarlığı Saldırısı | Bir tehdit aktörü, kurumsal intranet içindeki geçerli bir adresten geliyormuş gibi görünen bir IP paketi oluşturur. |
| Parola Tabanlı Saldırılar | Tehdit aktörleri geçerli bir kullanıcı hesabı bulursa, tehdit aktörleri gerçek kullanıcı ile aynı haklara sahip olur. Tehdit aktörleri, diğer kullanıcıların listelerini, ağ bilgilerini almak, sunucu ve ağ yapılandırmalarını değiştirmek ve verileri değiştirmek, yeniden yönlendirmek veya silmek için bu geçerli hesabı kullanabilir. |
| Hizmeti engelleme saldırısı | DoS saldırısı, bilgisayarın veya ağın geçerli kullanıcılar tarafından normal şekilde kullanılmasını engeller. Bir DoS saldırısı, aşırı yük nedeniyle kapanma gerçekleşene kadar bir bilgisayarı veya tüm ağı trafiğe boğabilir. DoS saldırısı, trafiği de engelleyebilir ve bu da yetkili kullanıcıların ağ kaynaklarına erişimini kaybetmesine |

icerik@bilgisayarkursanyo.com yetkinbilgi@gmail.com

| Saldırı Tipi | Açıklama |
|---|---|
| | neden olabilir. |
| Ortadaki Adam Saldırısı | Bu saldırı, tehdit aktörleri kendilerini bir kaynak ile hedef arasında konumlandırdığında gerçekleşir. Artık iletişimi şeffaf bir şekilde izleyebilir, yakalayabilir ve kontrol edebilirler. |
| Güvenliği İhlal Edilmiş Anahtar Saldırısı | Bir tehdit aktörü gizli bir anahtar alırsa, bu anahtara güvenliği ihlal edilmiş anahtar adı verilir. Gönderen veya alıcı saldırıdan haberdar olmadan güvenli bir iletişime erişim sağlamak için güvenliği ihlal edilmiş bir anahtar kullanılabilir. |
| Sniffer Saldırısı | Sniffer, ağ veri alışverişini okuyabilen, izleyebilen ve yakalayabilen ve ağ paketlerini okuyabilen bir uygulama veya cihazdır. Paketler şifrelenmemişse, bir dinleyici paket içindeki verilerin tam bir görünümünü sağlar. |

## 33.4.Zararlı Yazılım (Malware)

### 33.4.1.Kötü Amaçlı Yazılımlara Genel Bakış

Son cihazlar özellikle kötü amaçlı yazılım saldırılarına eğilimlidir. Kötü amaçlı yazılım hakkında bilgi sahibi olmak önemlidir çünkü tehdit aktörleri, kullanıcıların güvenlik açıklarından yararlanmaya yardımcı olması için kötü amaçlı yazılım yüklemesine güvenir.

### 33.4.2.Virüsler ve Truva Atları (Trojans)

Kötü amaçlı yazılımın ilk ve en yaygın türü bir virüstür. Virüslerin yayılması ve diğer bilgisayarlara bulaşması için insan eylemi gerekir. Örneğin, bir kurban bir e-posta ekini açtığında, USB sürücüdeki bir dosyayı açtığında veya bir dosya indirdiğinde bir virüs bilgisayara bulaşabilir.

Virüs kendisini bilgisayar koduna, yazılıma veya bilgisayardaki belgelere ekleyerek gizlenir. Açıldığında, virüs bilgisayarı çalıştırır ve enfekte eder.

Virüsler şunları yapabilir:

- Dosyaları değiştirir, bozar, siler veya tüm sürücüleri siler.
- Bilgisayar önyükleme sorunlarına ve bozuk uygulamalara neden olabilir.
- Hassas bilgileri yakalayıp tehdit aktörlerine gönderir.
- Yaymak için e-posta hesaplarına erişir ve kullanır.
- Tehdit aktörü tarafından çağrılıncaya kadar uykuda kalır.

Modern virüsler, tabloda listelenenler gibi belirli amaçlar için geliştirilmiştir.

| Virüs Türleri | Açıklama |
|---|---|
| Önyükleme sektörü virüsü | Virüs, önyükleme sektörüne, dosya bölüm tablosuna veya dosya sistemine saldırır. |
| Firmware virüsü | Virüs, aygıtın aygıt yazılımına saldırır. |
| Makro virüsü | Virüs, MS Office veya diğer uygulamaların makro özelliğini kötü amaçla kullanır. |
| Program virüsü | Virüs kendisini başka bir çalıştırılabilir programa ekler. |
| Komut dosyası virüsü | Virüs, komut dosyalarını yürütmek için kullanılan işletim sistemi yorumlayıcısına saldırır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tehdit aktörleri, ana bilgisayarları tehlikeye atmak için Truva atlarını kullanır. Truva atı, yararlı görünen ancak aynı zamanda kötü amaçlı kod taşıyan bir programdır. Truva atları genellikle bilgisayar oyunları gibi ücretsiz çevrimiçi programlar ile sağlanır. Şüphelenmeyen kullanıcılar oyunu Truva atıyla birlikte indirip yükler.

Tabloda açıklandığı gibi birkaç tür Truva atı vardır.

| Truva Atı Türü | Açıklama |
|---|---|
| Uzaktan erişim | Truva atı, yetkisiz uzaktan erişim sağlar. |
| Veri gönderme | Truva atı, tehdit aktörüne parolalar gibi hassas veriler sağlar. |
| Yıkıcı | Truva atı dosyaları bozar veya siler. |
| Proxy | Truva atı, saldırılar başlatmak ve diğer yasadışı faaliyetleri gerçekleştirmek için kurbanın bilgisayarını kaynak cihaz olarak kullanacaktır. |
| FTP | Truva atı, uç cihazlarda yetkisiz dosya aktarım hizmetlerini etkinleştirir. |
| Güvenlik yazılımı devre dışı bırakıcı | Truva atı, virüsten koruma programlarının veya güvenlik duvarlarının çalışmasını durdurur. |
| Hizmet Reddi (DoS) | Truva atı, ağ etkinliğini yavaşlatır veya durdurur. |
| Keylogger | Truva atı, bir web formuna girilen tuş vuruşlarını kaydederek, kredi kartı numaraları gibi gizli bilgileri çalmaya çalışır. |

Virüsler ve Truva atları, tehdit aktörlerinin kullandığı yalnızca iki tür kötü amaçlı yazılımdır. Belirli amaçlar için tasarlanmış birçok başka kötü amaçlı yazılım türü vardır.

### 33.4.3.Diğer Kötü Amaçlı Yazılım Türleri

Tabloda birçok farklı kötü amaçlı yazılım türü hakkında ayrıntılar gösterilmektedir.

| Kötü Amaçlı Yazılım | Açıklama |
|---|---|
| Reklam yazılımı-Adware | Reklam yazılımı genellikle çevrimiçi yazılım indirilerek dağıtılır.<br><br>Reklam yazılımı, açılır web tarayıcı pencerelerini, yeni araç çubuklarını kullanarak istenmeyen reklamları görüntüleyebilir veya bir web sayfasını beklenmedik şekilde farklı bir web sitesine yönlendirebilir.<br><br>Yeni pencereler kullanıcının kapatabileceğinden daha hızlı açıldığından, açılır pencereleri kontrol etmek zor olabilir. |
| Fidye yazılımı-Ransomware | Fidye yazılımı, genellikle dosyaları şifreleyerek ve ardından şifre çözme anahtarı için fidye talep eden bir mesaj görüntüleyerek bir kullanıcının dosyalarına erişimini engeller.<br><br>Güncel yedeklemeleri olmayan kullanıcılar, dosyalarının şifresini çözmek için fidye ödemelidir.<br><br>Ödeme genellikle banka havalesi veya Bitcoin gibi kripto para birimleri kullanılarak yapılır. |
| Rootkit | Kök setleri, tehdit aktörleri tarafından bir bilgisayara yönetici hesabı düzeyinde erişim elde etmek için kullanılır.<br><br>Algılanmaları çok zordur çünkü güvenlik duvarını, antivirüs korumasını, sistem dosyalarını ve hatta işletim sistemi komutlarını değiştirerek varlıklarını |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Kötü Amaçlı Yazılım | Açıklama |
|---|---|
| | gizleyebilirler.<br><br>Tehdit aktörlerine PC'ye erişim sağlayan ve dosya yüklemelerine ve bir DDoS saldırısında kullanılmak üzere yeni yazılım yüklemelerine izin veren bir arka kapı sağlayabilir.<br><br>Bunları kaldırmak için özel rootkit kaldırma araçları kullanılmalıdır, aksi takdirde işletim sisteminin tamamen yeniden yüklenmesi gerekebilir. |
| Casus yazılım-SpyWare | Reklam yazılımına benzer, ancak kullanıcı hakkında bilgi toplamak ve kullanıcının izni olmadan tehdit aktörlerine göndermek için kullanılır.<br><br>Casus yazılım, göz atma verilerini toplayan düşük bir tehdit olabilir veya kişisel ve finansal bilgileri yakalayan yüksek bir tehdit olabilir. |
| Solucan-Worm | Solucan, yasal yazılımdaki güvenlik açıklarından yararlanarak kullanıcı eylemleri olmadan otomatik olarak yayılan, kendi kendini kopyalayan bir programdır.<br><br>Ağı, aynı güvenlik açığına sahip diğer kurbanları aramak için kullanır.<br><br>Bir solucanın amacı genellikle ağ işlemlerini yavaşlatmak veya bozmaktır. |

## 33.5.Yaygın Ağ Saldırıları

### 33.5.1.Ağ Saldırılarına Genel Bakış

Öğrendiğiniz gibi, bilgisayar korsanlarının kullanabileceği birçok kötü amaçlı yazılım türü vardır. Ancak bunlar bir ağa, hatta bir organizasyona saldırmanın tek yolu değildir.

Kötü amaçlı yazılım teslim edildiğinde ve yüklendiğinde, yük, ağla ilgili çeşitli saldırılara neden olmak için kullanılabilir.

Saldırıları azaltmak için saldırı türlerini anlamak yararlıdır. Ağ saldırılarını kategorize ederek, bireysel saldırılar yerine saldırı türlerini ele almak mümkündür.

Ağlar, aşağıdaki türden saldırılara karşı hassastır:

- Keşif Saldırıları
- Erişim Saldırıları
- DoS Saldırıları

### 33.5.2.Keşif Saldırıları

Keşif, bilgi toplamadır. Bu, bir mahalleye bir şey satıyormuş gibi kapı kapı dolaşıp dolaşan hırsızlara benzer. Hırsızın aslında yaptığı şey, kullanılmayan konutlar, kolay açılan kapıları veya pencereleri olan konutlar ve güvenlik sistemi veya güvenlik kamerası olmayan konutlar gibi kırılabilecek savunmasız evler aramaktır.

Tehdit aktörleri, sistemlerin, hizmetlerin veya güvenlik açıklarının yetkisiz keşfi ve haritalanması için keşif saldırılarını kullanır. Keşif saldırıları, erişim saldırıları veya DoS saldırılarından önce gelir.

Licensed to yetkin.karasinour, yetkinkrsnr@gmail.com

Kötü niyetli tehdit aktörlerinin keşif saldırılarını gerçekleştirmek için kullandıkları tekniklerden bazıları tabloda açıklanmıştır.

| Teknik | Açıklama |
|---|---|
| Bir hedefin bilgi sorgusunu gerçekleştirme | Tehdit aktörü, bir hedefle ilgili ilk bilgileri arıyor. Google arama, kuruluşların web sitesi, whois ve daha fazlası dahil olmak üzere çeşitli araçlar kullanılabilir. |
| Hedef ağda bir ping taraması başlatma | Bilgi sorgusu genellikle hedefin ağ adresini ortaya çıkarır. Tehdit aktörü artık hangi IP adreslerinin etkin olduğunu belirlemek için bir ping taraması başlatabilir. |
| Etkin IP adresleri için bir bağlantı noktası taraması başlatma | Bu, hangi bağlantı noktalarının veya hizmetlerin mevcut olduğunu belirlemek için kullanılır. Bağlantı noktası tarayıcı örnekleri arasında Nmap, SuperScan, Angry IP Scanner ve NetScanTools bulunur. |
| Güvenlik açığı tarayıcıları çalıştırma | Bu, ana bilgisayarda çalışan uygulama ve işletim sisteminin türünü ve sürümünü belirlemek için tanımlanan bağlantı noktalarını sorgulamak içindir. Araç örnekleri arasında Nipper, Secuna PSI, Core Impact, Nessus v6, SAINT ve Open VAS bulunur. |
| Sömürü araçlarını çalıştırma | Tehdit aktörü, artık kötüye kullanılabilecek savunmasız hizmetleri keşfetmeye çalışıyor. Metasploit, Core Impact, Sqlmap, Social Engineer Toolkit ve Netsparker dahil olmak üzere çeşitli güvenlik açığı istismar araçları mevcuttur. |

### 33.5.3.Erişim Saldırıları

Erişim saldırıları, kimlik doğrulama hizmetleri, FTP hizmetleri ve web hizmetlerindeki bilinen güvenlik açıklarından yararlanır. Bu tür saldırıların amacı, web hesaplarına, gizli veritabanlarına ve diğer hassas bilgilere giriş sağlamaktır.

Tehdit aktörleri, verileri almak, erişim elde etmek veya erişim ayrıcalıklarını yönetici durumuna yükseltmek için ağ aygıtlarına ve bilgisayarlara erişim saldırılarını kullanır.

**Şifre Saldırıları**

Bir parola saldırısında, tehdit aktörü çeşitli yöntemler kullanarak kritik sistem parolalarını keşfetmeye çalışır. Parola saldırıları çok yaygındır ve çeşitli parola kırma araçları kullanılarak başlatılabilir.

**Sahte Saldırılar**

Sahte saldırılarda, tehdit aktörü cihazı, verileri tahrif ederek başka bir cihaz gibi davranmaya çalışır. Yaygın sahtekarlık saldırıları arasında IP sahtekarlığı, MAC sahtekarlığı ve DHCP sahtekarlığı bulunur. Bu sahtekarlık saldırıları, bu modülün ilerleyen kısımlarında daha ayrıntılı olarak tartışılacaktır.

Diğer Erişim saldırıları şunları içerir:

- İstismar etme
- Bağlantı noktası yönlendirmeleri
- Ortadaki adam saldırıları
- Arabellek taşması saldırıları

### 33.5.4.Sosyal Mühendislik Saldırıları

Sosyal mühendislik, bireyleri eylemleri gerçekleştirmeye veya gizli bilgileri ifşa etmeye yönlendirmeye çalışan bir erişim saldırısıdır. Bazı sosyal mühendislik teknikleri şahsen yapılırken, diğerleri telefon veya interneti kullanabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Sosyal mühendisler genellikle insanların yardımcı olma istekliliğine güvenirler. Ayrıca insanların zayıflıklarından da beslenirler. Örneğin, bir tehdit aktörü, anında ağ erişimi gerektiren acil bir sorunla yetkili bir çalışanı arayabilir.

Tehdit aktörü, çalışanın gösterişine itiraz edebilir, isim bırakma teknikleri kullanarak otoriteyi çağırabilir veya çalışanın açgözlülüğüne başvurabilir.

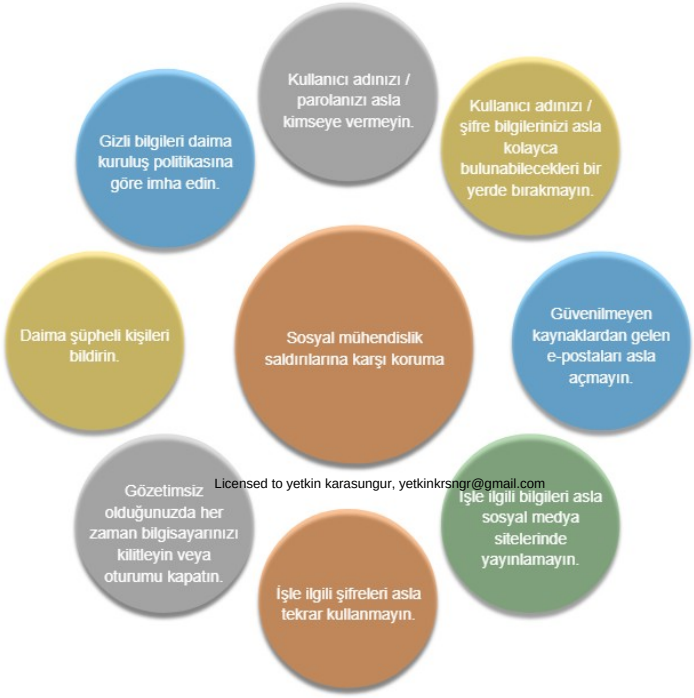
Sosyal mühendislik teknikleriyle ilgili bilgiler tabloda gösterilmektedir.

| Sosyal Mühendislik Saldırısı | Açıklama |
|---|---|
| Bahane Uydurma | Bir tehdit aktörü, alıcının kimliğini doğrulamak için kişisel veya finansal verilere ihtiyaç duyduğunu söyler. |
| E-dolandırıcılık | Bir tehdit aktörü, alıcıyı cihazına kötü amaçlı yazılım yüklemesi için kandırmak veya kişisel veya finansal bilgilerini paylaşmak için meşru, güvenilir bir kaynaktan geliyormuş gibi görünen sahtekarlık amaçlı e-posta gönderir. |
| Oltalama | Bir tehdit aktörü, belirli bir kişi veya kuruluş için özel olarak tasarlanmış hedefli bir kimlik avı saldırısı oluşturur. |
| İstenmeyen E-Posta (Spam) | İstenmeyen posta olarak da bilinen bu, genellikle zararlı bağlantılar, kötü amaçlı yazılımlar veya aldatıcı içerik içeren istenmeyen e-postadır. |
| Bir şey için bir şey | Bazen "Quid pro quo" olarak adlandırılan bu saldırı, bir tehdit aktörünün hediye gibi bir şey karşılığında bir taraftan kişisel bilgi talep etmesidir. |
| Canını sıkma | Bir tehdit aktörü, kötü amaçlı yazılım bulaşmış bir flash sürücüyü halka açık bir yerde bırakır. Bir kurban sürücüyü bulur ve istemeden kötü amaçlı yazılım yükleyerek dizüstü bilgisayarına yerleştirir. |
| Kimliğe bürünme | Bu tür bir saldırı, bir tehdit aktörünün mağdurun güvenini kazanmak için olmadığı biri gibi davranmasıdır. |
| Arkadan Takip | Bir tehdit aktörünün, güvenli bir alana erişim sağlamak için yetkili bir kişiyi hızlı bir şekilde güvenli bir konuma takip etmesidir. |
| Omuz Sörfü | Bir tehdit aktörünün, şifrelerini veya diğer bilgileri çalmak için göze çarpmadan omzunun üzerinden bakması veya cep telefonuyla kayıt etmesidir. |
| Çöplüğe Dalış | Bir tehdit aktörünün gizli belgeleri keşfetmek için çöp kutularını karıştırmasıdır. |

Sosyal Mühendislik Araç Seti (SET), beyaz şapkalı bilgisayar korsanlarının ve diğer ağ güvenliği uzmanlarının kendi ağlarını test etmek için sosyal mühendislik saldırıları oluşturmalarına yardımcı olmak için tasarlanmıştır.

İşletmeler, kullanıcılarını sosyal mühendisliğin riskleri hakkında eğitmeli ve kimlikleri telefonla, e-posta yoluyla veya şahsen doğrulamak için stratejiler geliştirmelidir.

Şekil, tüm kullanıcılar tarafından izlenmesi gereken önerilen uygulamaları göstermektedir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 33.5.5.DoS ve DDoS Saldırıları

Hizmet Reddi- Denial of Service (DoS) saldırısı, kullanıcılara, cihazlara veya uygulamalara yönelik ağ hizmetlerinde bir tür kesintiye neden olur. İki ana DoS saldırısı türü vardır:

Aşırı Trafik Miktarı - Tehdit unsuru, ağın, ana bilgisayarın veya uygulamanın başa çıkamayacağı bir hızda çok büyük miktarda veri gönderir. Bu, iletim ve yanıt sürelerinin yavaşlamasına neden olur. Ayrıca bir cihazı veya hizmeti çökertebilir.
Kötü Amaçlı Biçimlendirilmiş Paketler - Tehdit aktörü, kötü niyetli olarak biçimlendirilmiş bir paketi bir ana bilgisayara veya uygulamaya gönderir ve alıcı bunu işleyemez. Bu, alıcı cihazın çok yavaş çalışmasına veya çökmesine neden olur.

DoS saldırıları, iletişimi kesintiye uğrattığı ve önemli zaman ve para kaybına neden olduğu için büyük bir risktir. Bu saldırıların, vasıfsız bir tehdit aktörü tarafından bile yürütülmesi nispeten kolaydır.

Dağıtılmış DoS Saldırısı-Distributed DoS Attack (DDoS), DoS saldırısına benzer, ancak birden çok, koordineli kaynaklardan kaynaklanır. Örneğin, bir tehdit aktörü, zombiler olarak bilinen virüslü ana bilgisayarlardan oluşan bir ağ oluşturur. Tehdit aktörü, zombilere kontrol mesajları göndermek için bir komut ve kontrol (CnC) sistemi kullanır. Zombiler sürekli olarak daha fazla ana bilgisayarı bot zararlı yazılımıyla tarar ve bulaştırır. Bot kötü amaçlı yazılımı, bir ana bilgisayarı enfekte edecek şekilde tasarlanmıştır ve bu, onu CnC sistemiyle iletişim kurabilen bir zombi haline getirir. Zombilerin koleksiyonuna botnet denir. Tehdit aktörü hazır olduğunda, CnC sistemine zombilerin botnetini bir DDoS saldırısı gerçekleştirmesi talimatını verir.

## 33.6.IP Güvenlik Açıkları ve Tehditleri

### 33.6.1.IPv4 ve IPv6 saldırı Teknikleri

IP, bir pakette bulunan kaynak IP adresinin gerçekten bu kaynaktan gelip gelmediğini doğrulamaz. Bu nedenle, tehdit aktörleri sahte bir kaynak IP adresi kullanarak paket gönderebilir. Tehdit aktörleri, saldırılarını gerçekleştirmek için IP başlığındaki diğer alanlara da müdahale edebilir. Güvenlik analistleri, hem IPv4 hem de IPv6 üstbilgilerindeki farklı alanları anlamalıdır.

IP ile ilgili daha yaygın saldırılardan bazıları tabloda gösterilmektedir.

| IP Saldırı Teknikleri | Açıklama |
|---|---|
| ICMP saldırıları | Tehdit aktörleri, korumalı bir ağdaki alt ağları ve ana bilgisayarları keşfetmek, DoS taşkın saldırıları oluşturmak ve ana bilgisayar yönlendirme tablolarını değiştirmek için İnternet Kontrol Mesajı Protokolü (ICMP) yankı paketlerini (pingler) kullanır. |
| Amplifikasyon ve yansıtma saldırıları | Tehdit aktörleri, meşru kullanıcıların DoS ve DDoS saldırılarını kullanarak bilgilere veya hizmetlere erişmesini engellemeye çalışır. |
| Adres sahteciliği saldırıları | Tehdit aktörleri, sahtekarlık yapmak için bir IP paketindeki kaynak IP adresini aldatır. |
| Ortadaki adam saldırısı (MITM) | Tehdit aktörleri, iletişimi şeffaf bir şekilde izlemek, yakalamak ve kontrol etmek için kendilerini bir kaynak ile hedef arasında konumlandırır. Yakalanan paketleri inceleyerek kulak misafiri olabilir veya paketleri değiştirip orijinal hedeflerine iletebilirler. |
| Oturum çalma | Tehdit aktörleri fiziksel ağa erişim sağlar ve ardından bir oturumu ele geçirmek için bir MITM saldırısı kullanır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 33.6.2.ICMP Saldırıları

Tehdit aktörleri keşif ve tarama saldırıları için ICMP kullanır. Bir ağ topolojisini haritalamak, hangi ana bilgisayarların etkin (erişilebilir) olduğunu keşfetmek, ana bilgisayar işletim sistemini (işletim sistemi parmak izi) belirlemek ve bir güvenlik duvarının durumunu belirlemek için bilgi toplama saldırıları başlatabilirler. Tehdit aktörleri ayrıca DoS saldırıları için ICMP kullanır.

Not : IPv4 için ICMP (ICMPv4) ve IPv6 için ICMP (ICMPv6) benzer saldırı türlerine karşı hassastır.

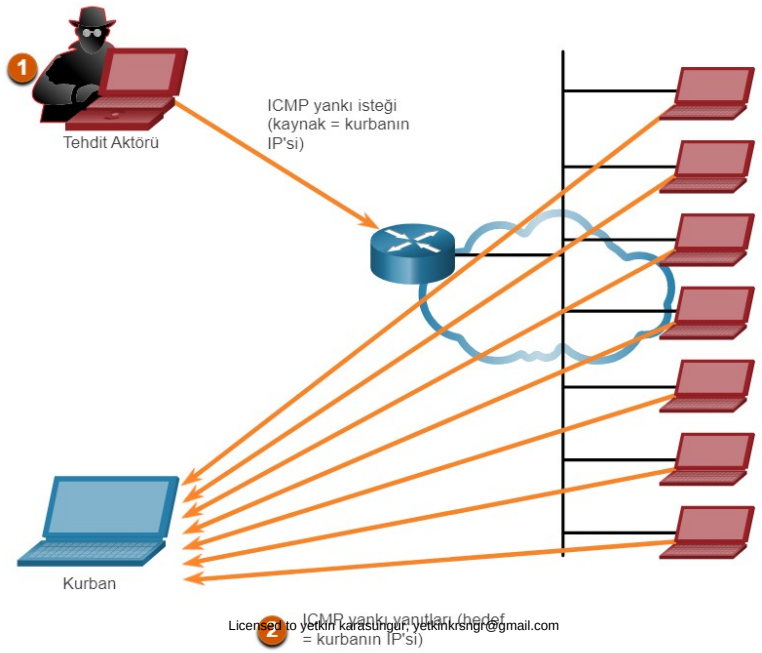
İnternetten ICMP incelemesini önlemek için ağlar, ağ kenarında sıkı ICMP erişim kontrol listesi (ACL) filtrelemesine sahip olmalıdır. Güvenlik analistleri, yakalanan trafiğe ve günlük dosyalarına bakarak ICMP ile ilgili saldırıları tespit edebilmelidir. Büyük ağlar söz konusu olduğunda, güvenlik duvarları ve saldırı tespit sistemleri (IDS) gibi güvenlik cihazları bu tür saldırıları tespit eder ve güvenlik analistlerine uyarılar üretir.

Tehdit aktörlerini ilgilendiren ortak ICMP mesajları tabloda listelenmiştir.

| Hackerlar tarafından kullanılan ICMP Mesajları | Açıklama |
|---|---|
| ICMP yankı isteği ve yankı yanıtı | Bu, ana bilgisayar doğrulaması ve DoS saldırıları gerçekleştirmek için kullanılır. |
| ICMP erişilemez | Bu, ağ keşfi ve tarama saldırıları gerçekleştirmek için kullanılır. |
| ICMP maskesi yanıtı | Bu, dahili bir IP ağını eşlemek için kullanılır. |
| ICMP yönlendirmeleri | Bu, hedef ana bilgisayarı tehlikeye atılmış bir cihaz üzerinden tüm trafiği göndermeye ve bir MITM saldırısı oluşturmaya ikna etmek için kullanılır. |
| ICMP yönlendirici keşfi | Bu, bir hedef ana bilgisayarın yönlendirme tablosuna sahte yol girişlerini enjekte etmek için kullanılır. |

## 33.6.3.Amplifikasyon ve Yansıtma Saldırıları

Tehdit aktörleri, DoS saldırıları oluşturmak için genellikle büyütme ve yansıtma tekniklerini kullanır. Şekildeki örnek, Smurf saldırısı adı verilen bir büyütme ve yansıtma tekniğinin, hedef istemciyi alt etmek için nasıl kullanıldığını göstermektedir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

1. **Yükseltme** - Tehdit aktörü, ICMP yankı isteği mesajlarını birçok ana bilgisayara iletir. Bu mesajlar, kurbanın kaynak IP adresini içerir.
2. **Yansıma** - Bu ev sahiplerinin tümü mağdurun sahte IP adresine yanıt vererek onu alt eder.

Not : DNS tabanlı yansıtma ve büyütme saldırıları ve Ağ Zaman Protokolü (NTP) büyütme saldırıları gibi daha yeni büyütme ve yansıtma saldırıları sıklıkla kullanılmaktadır.

Tehdit aktörleri ayrıca kaynak tüketme saldırılarını kullanır. Bu saldırılar, bir hedef ana bilgisayarın kaynaklarını, onu çökertmek veya bir ağın kaynaklarını tüketmek için kullanılır.

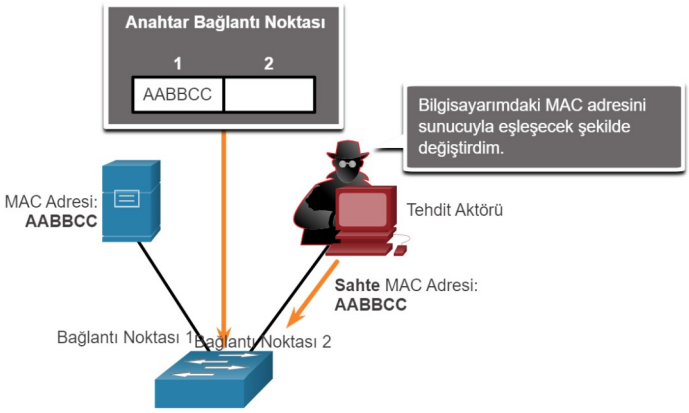
### 33.6.4.Adres Sahteciliği Saldırıları

IP adresi sahtekarlığı saldırıları, bir tehdit aktörü gönderenin kimliğini gizlemek veya başka bir meşru kullanıcı olarak görünmek için yanlış kaynak IP adresi bilgileriyle paketler oluşturduğunda meydana gelir. Tehdit aktörü daha sonra başka türlü erişilemeyen verilere erişim sağlayabilir veya güvenlik yapılandırmalarını atlatabilir. Adres sahteciliği genellikle Smurf saldırısı gibi başka bir saldırıya dahil edilir.

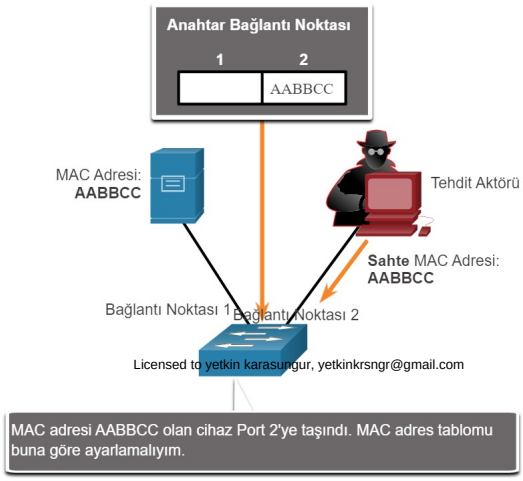
Adres sahteciliği saldırıları görünen veya görünmeyen olabilir:

Görünen sahtekarlık - Tehdit aktörü, ana bilgisayar ile hedef arasında gönderilen trafiği görebilir. Tehdit aktörü, hedef kurbandan gelen yanıt paketini incelemek için kör olmayan sahtekarlık kullanır. Görünen sahtekarlık, bir güvenlik duvarının durumunu ve sıra numarası tahminini belirler. Ayrıca yetkili bir oturumu ele geçirebilir.
Görünmeyen sahtekarlık - Tehdit aktörü, ana bilgisayar ile hedef arasında gönderilen trafiği göremez. DoS saldırılarında görünmeyen sahtekarlık kullanılır.

MAC adresi sahtekarlığı saldırıları, tehdit aktörlerinin dahili ağa erişimi olduğunda kullanılır. Tehdit aktörleri, ana bilgisayarlarının MAC adresini şekilde gösterildiği gibi, hedef ana bilgisayarın bilinen başka bir MAC adresiyle eşleşecek şekilde değiştirir. Saldıran ana bilgisayar daha sonra yeni yapılandırılmış MAC adresiyle ağ boyunca bir çerçeve gönderir. Anahtar çerçeveyi aldığında, kaynak MAC adresini inceler.




Anahtar, geçerli CAM tablosu girişinin üzerine yazar ve MAC adresini şekilde gösterildiği gibi yeni bağlantı noktasına atar. Daha sonra hedef ana bilgisayar için belirlenen çerçeveleri saldıran ana bilgisayara iletir.

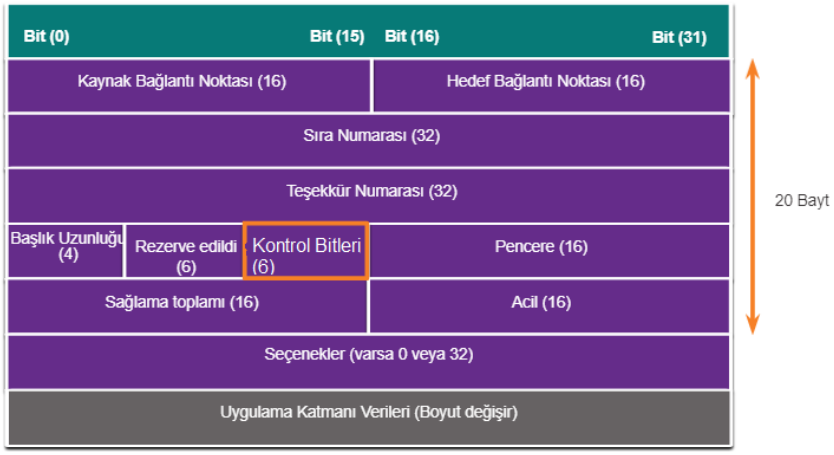


Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 33.7.TCP ve UDP Güvenlik Açıkları

### 33.7.1.TCP Segment Başlığı

TCP segment bilgisi, IP başlığından hemen sonra görünür. TCP segmentinin alanları ve Kontrol Bitleri alanı için bayraklar (flag) şekilde gösterilmektedir.




Aşağıdakiler, TCP segmentinin altı kontrol bitidir:

- **URG** - Acil işaretçi alanı önemli
- **ACK** - Önemli bilgi alanı
- **PSH** - İtme işlevi
- **RST** - Bağlantıyı sıfırlayın
- **SYN** - Sıra numaralarını senkronize et
- **FIN** - Gönderenden daha fazla veri yok

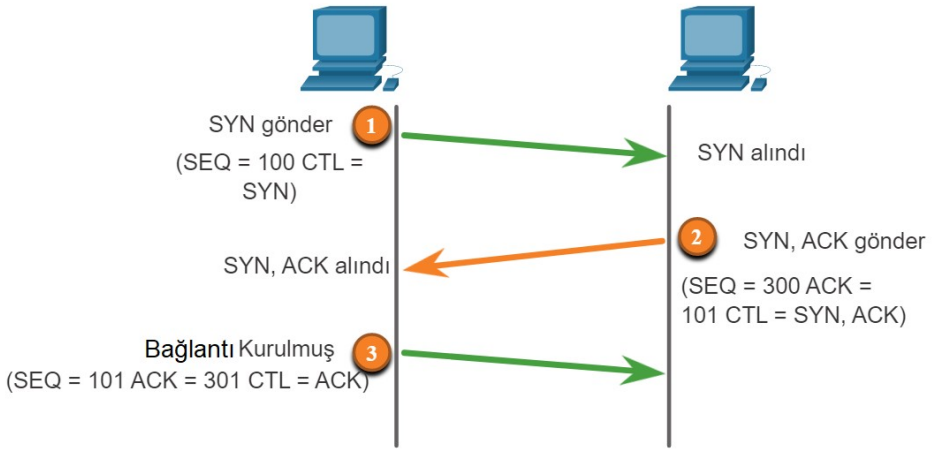
### 33.7.2.TCP Hizmetleri

TCP şu hizmetleri sağlar:

- Güvenilir teslimat - TCP, hataları algılamak ve çözmek için üst katman protokollerine güvenmek yerine teslimatı garanti etmek için onaylar içerir. Zamanında bir onay alınmazsa, gönderen verileri yeniden iletir. Alınan verilerin onaylanmasını zorunlu kılmak, önemli gecikmelere neden olabilir. TCP güvenilirliğinden yararlanan uygulama katmanı protokollerinin örnekleri arasında HTTP, SSL / TLS, FTP, DNS bölge aktarımları ve diğerleri bulunur.
- Akış denetimi - TCP, bu sorunu gidermek için akış denetimi uygular. Bir seferde bir segmenti onaylamak yerine, birden çok segment tek bir alındı segmenti ile onaylanabilir.
- Durum bilgisi olan iletişim - İki taraf arasındaki durum bilgisi olan TCP iletişimi, TCP'nin üç yönlü el sıkışması sırasında gerçekleşir. Veriler TCP kullanılarak aktarılmadan önce, üç yönlü bir el sıkışma, şekilde gösterildiği gibi TCP bağlantısını açar. Her iki taraf da TCP bağlantısını kabul ederse, veri TCP kullanılarak her iki tarafça gönderilebilir ve alınabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### TCP Üç Yönlü El Sıkışma




Üç adımda bir TCP bağlantısı kurulur:

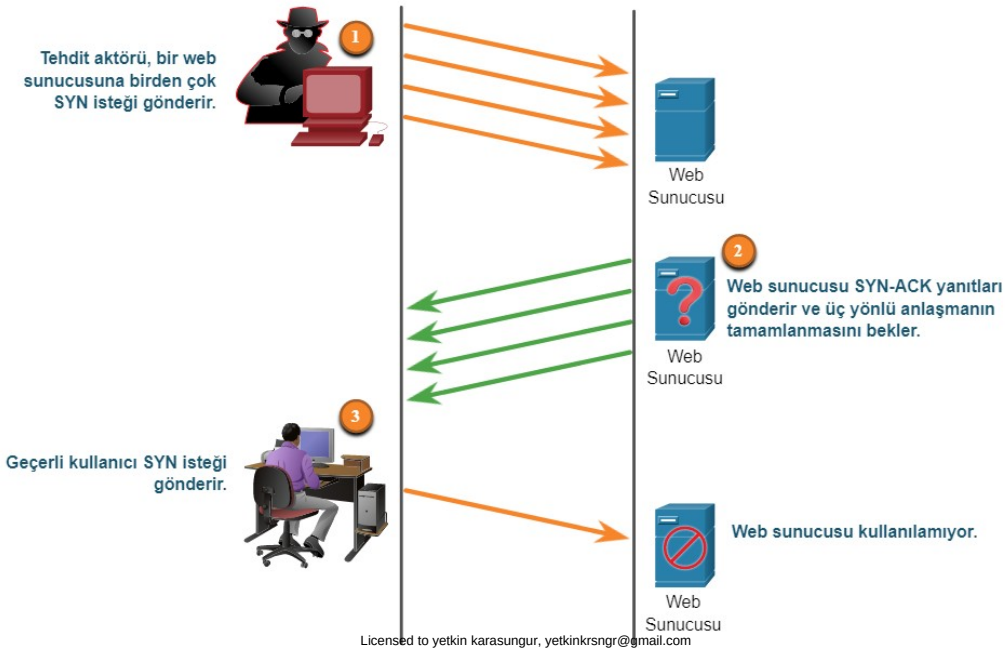
1. Başlatan istemci, sunucuyla istemciden sunucuya bir iletişim oturumu talep eder.
2. Sunucu, istemciden sunucuya iletişim oturumunu onaylar ve sunucudan istemciye bir iletişim oturumu talep eder.
3. Başlatan istemci, sunucudan istemciye iletişim oturumunu onaylar.

## 33.7.3.TCP Saldırıları

Ağ uygulamaları TCP veya UDP bağlantı noktalarını kullanır. Tehdit aktörleri, hangi hizmetleri sunduklarını keşfetmek için hedef cihazların bağlantı noktası taramalarını gerçekleştirir.

### TCP SYN Flood Saldırısı

TCP SYN Flood saldırısı, TCP'nin üç yönlü anlaşmasını kullanır. Şekil, bir tehdit aktörünün sürekli olarak rastgele sahte bir kaynak IP adresiyle bir hedefe TCP SYN oturum istek paketleri gönderdiğini göstermektedir. Hedef cihaz sahte IP adresine bir TCP SYN-ACK paketi ile yanıt verir ve bir TCP ACK paketini bekler. Bu yanıtlar asla gelmez. Sonunda, hedef ana bilgisayar yarı açık TCP bağlantılarıyla boğulur ve TCP hizmetleri yasal kullanıcılara hizmet veremez hale gelir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

1. Tehdit aktörü, bir web sunucusuna birden çok SYN isteği gönderir.
2. Web sunucusu, her SYN isteği için SYN-ACK'larla yanıt verir ve üç yönlü anlaşmanın tamamlanmasını bekler. Tehdit aktörü SYN-ACK'lara yanıt vermiyor.
3. Geçerli bir kullanıcı, web sunucusunda çok fazla yarı açık TCP bağlantısı olduğundan web sunucusuna erişemez.

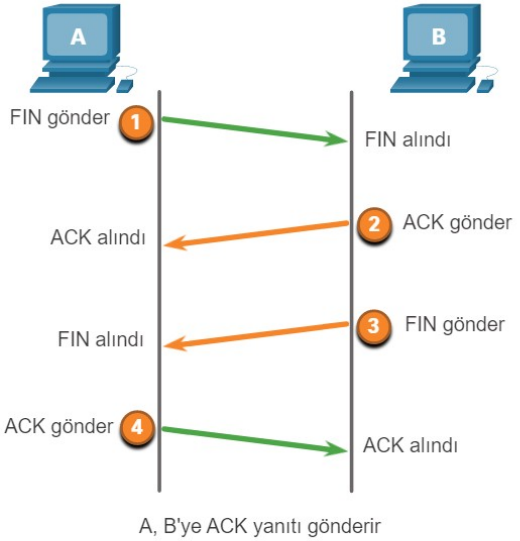
**TCP Sıfırlama Saldırısı**

İki ana bilgisayar arasındaki TCP iletişimini sonlandırmak için bir TCP sıfırlama saldırısı kullanılabilir. TCP, bir bağlantıyı normal ve normal olmayan yani ani bir şekilde sonlandırabilir.

Şekil, TCP bağlantısını kapatmak için her TCP uç noktasından gelen bir çift FIN ve ACK bölümünden oluşan dört yönlü bir değişim kullanan TCP'nin normal bir şeklini gösterir.

Normal olmayan yöntem, bir ana bilgisayarın RST bit kümesine sahip bir TCP segmenti almasıdır. Bu, TCP bağlantısını kesmenin ve alıcı ana bilgisayara TCP bağlantısını kullanmayı derhal durdurmasını bildirmenin ani bir yoludur.

Bir tehdit aktörü, bir TCP sıfırlama saldırısı gerçekleştirebilir ve bir TCP RST içeren sahte bir paketi bir veya iki uç noktaya gönderebilir.

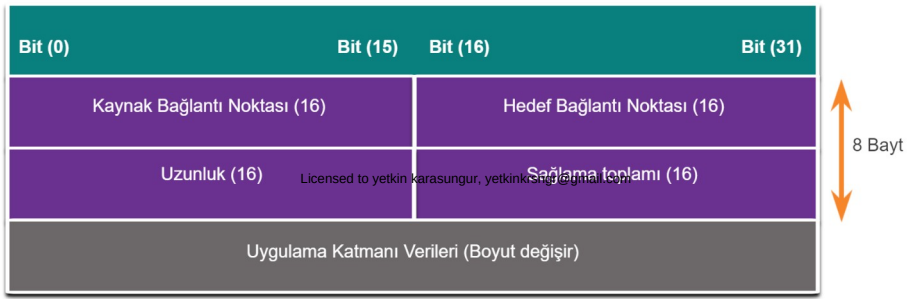



Bir TCP oturumunun sonlandırılması, aşağıdaki dört yönlü değişim sürecini kullanır:

1. İstemci akışta gönderilecek daha fazla veriye sahip olmadığında, FIN bayrağı ayarlanmış bir segment gönderir.
2. Sunucu, oturumu istemciden sunucuya sonlandırmak için FIN'in alındığını onaylamak için bir ACK gönderir.
3. Sunucu, sunucudan istemciye oturumu sonlandırmak için istemciye bir FIN gönderir.
4. İstemci, sunucudan FIN'i onaylamak için bir ACK ile yanıt verir.

## 33.7.4.UDP Segment Başlığı ve İşlemi

UDP, genellikle DNS, TFTP, NFS ve SNMP tarafından kullanılır. Aynı zamanda medya akışı veya VoIP gibi gerçek zamanlı uygulamalarla da kullanılır. UDP, bağlantısız bir aktarım katmanı protokolüdür. TCP'den çok daha düşük ek yüke sahiptir, çünkü bağlantı yönelimli değildir ve güvenilirlik sağlayan karmaşık yeniden iletim, sıralama ve akış kontrol mekanizmaları sunmaz. Şekilde gösterilen UDP segment yapısı, TCP'nin segment yapısından çok daha küçüktür.



Licensed to yetkin karasungur, yetkinkrsng@gmail.com

UPD normalde güvenilmez olarak adlandırılsa da, TCP'nin güvenilirliğinin aksine, bu, UDP kullanan uygulamaların her zaman güvenilmez olduğu veya UDP'nin daha düşük bir protokol olduğu anlamına gelmez. Bu, bu işlevlerin taşıma katmanı protokolü tarafından sağlanmadığı ve gerekirse başka bir yerde uygulanması gerektiği anlamına gelir.

UDP'nin düşük ek yükü, basit talep ve yanıt işlemleri yapan protokoller için onu çok arzu edilir kılar. Örneğin, DHCP için TCP kullanmak gereksiz ağ trafiğine neden olur. Yanıt alınmazsa, cihaz isteği yeniden gönderir.

### 33.7.5.UDP Saldırıları

UDP herhangi bir şifreleme ile korunmaz. UDP'ye şifreleme ekleyebilirsiniz, ancak varsayılan olarak kullanılamaz. Şifreleme eksikliği, herkesin trafiği görebileceği, değiştirebileceği ve hedefine gönderebileceği anlamına gelir. Trafikteki verileri değiştirmek 16 bitlik sağlama toplamını değiştirir, ancak sağlama toplamı isteğe bağlıdır ve her zaman kullanılmaz. Sağlama toplamı kullanıldığında, tehdit aktörü yeni veri yüküne göre yeni bir sağlama toplamı oluşturabilir ve ardından bunu başlığa yeni bir sağlama toplamı olarak kaydedebilir. Hedef cihaz, verilerin değiştirildiğini bilmeden sağlama toplamının verilerle eşleştiğini bulacaktır. Bu tür saldırılar yaygın olarak kullanılmamaktadır.

#### UDP Sel (Flooding) Saldırıları

Bir UDP sel saldırısı görme olasılığınız daha yüksektir. Bir UDP sel saldırısında, bir ağdaki tüm kaynaklar tüketilir. Tehdit aktörü, UDP Unicorn veya Low Orbit Ion Cannon gibi bir araç kullanır. Bu araçlar, genellikle sahte bir ana bilgisayardan alt ağdaki bir sunucuya bir dizi UDP paketi gönderir. Program, kapalı bağlantı noktalarını bulmaya çalışırken bilinen tüm bağlantı noktalarını tarayacaktır. Bu, sunucunun bir ICMP bağlantı noktasına erişilemez mesajıyla yanıt vermesine neden olur. Sunucuda çok sayıda kapalı bağlantı noktası olduğundan, bu, bant genişliğinin çoğunu kullanan segmentte çok fazla trafik oluşturur. Sonuç, DoS saldırısına çok benzer.

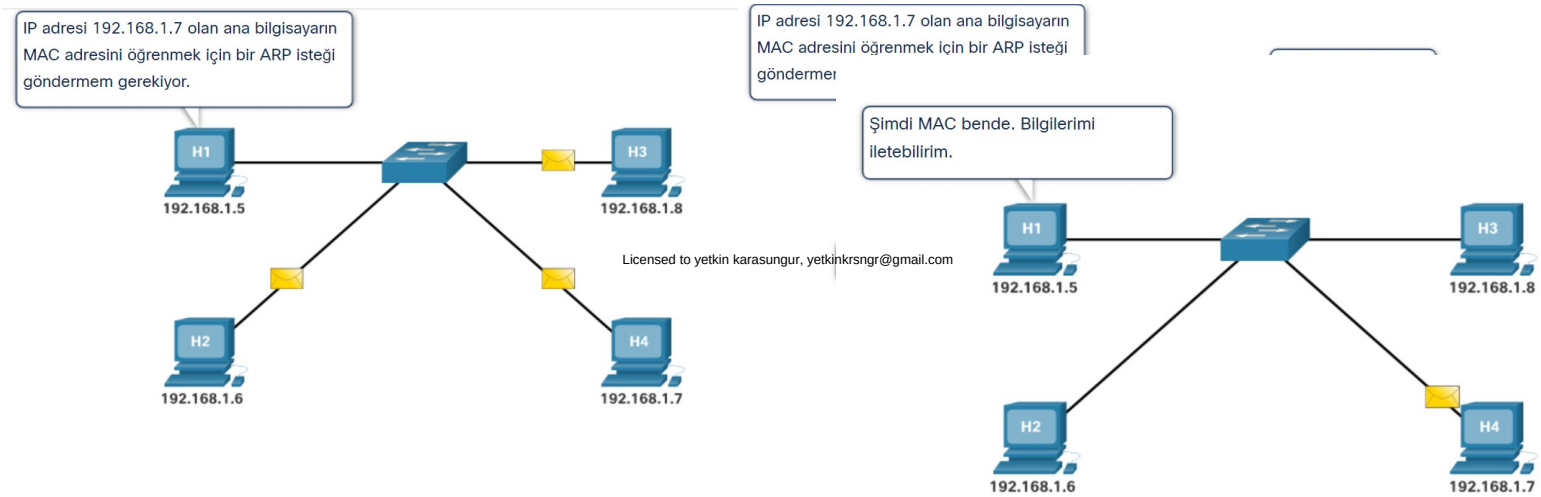
## 33.8.IP Servisleri

### 33.8.1.ARP Güvenlik Açıkları

TCP / IP protokol paketi hiçbir zaman güvenlik için oluşturulmadı. Bu nedenle, IP'nin ARP, DNS ve DHCP gibi adresleme işlevleri için kullandığı hizmetler de bu konuda öğreneceğiniz gibi güvenli değildir.

Ana bilgisayarlar, belirli bir IP adresine sahip bir ana bilgisayarın MAC adresini belirlemek için segmentteki diğer ana bilgisayarlara bir ARP İsteği yayınlar. Alt ağdaki tüm ana bilgisayarlar ARP İsteğini alır ve işler. ARP İsteğinde eşleşen IP adresine sahip ana bilgisayar bir ARP Yanıtı gönderir.

#### ARP Süreci




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

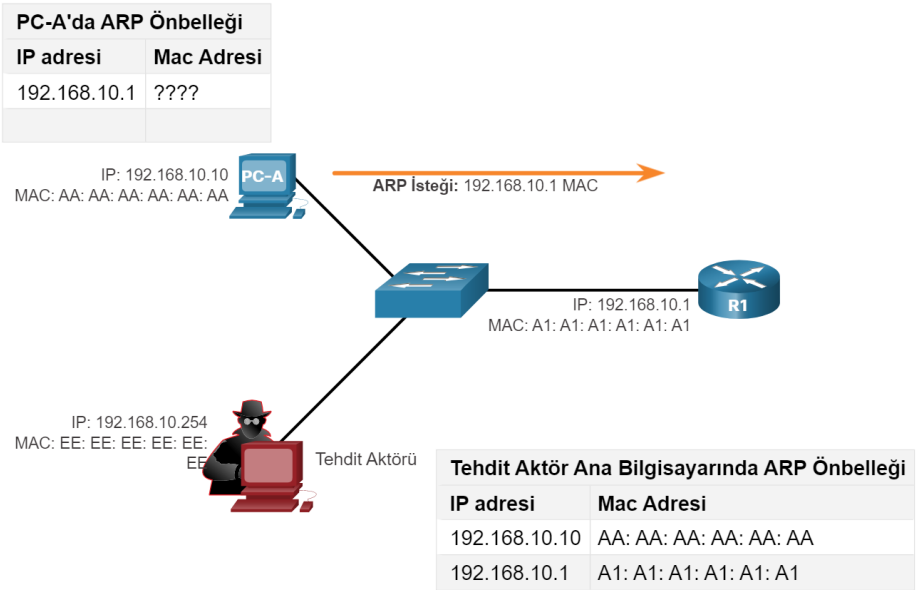
Herhangi bir istemci, "karşılıksız-nedensiz ( gratuitous arp) ARP" adı verilen, istenmeyen bir ARP Yanıtı gönderebilir. Bu genellikle bir cihaz ilk açıldığında yerel ağdaki diğer tüm cihazlara yeni cihazın MAC adresini bildirmek için yapılır. Bir ana bilgisayar karşılıksız bir ARP gönderdiğinde, alt ağdaki diğer ana bilgisayarlar, karşılıksız ARP'de bulunan MAC adresini ve IP adresini kendi ARP tablolarında saklar.

ARP'nin bu özelliği, herhangi bir ana bilgisayarın herhangi bir IP veya MAC'ın sahibi olduğunu iddia edebileceği anlamına da gelir. Bir tehdit aktörü, yerel ağdaki cihazların ARP önbelleğini zehirleyerek trafiği yeniden yönlendirmek için bir MITM saldırısı oluşturabilir. Amaç, bir kurban ana bilgisayarı hedeflemek ve varsayılan ağ geçidini tehdit aktörünün cihazıyla değiştirmesini sağlamaktır. Bu, tehdit aktörünü mağdur ile yerel alt ağın dışındaki diğer tüm sistemler arasında konumlandırır.

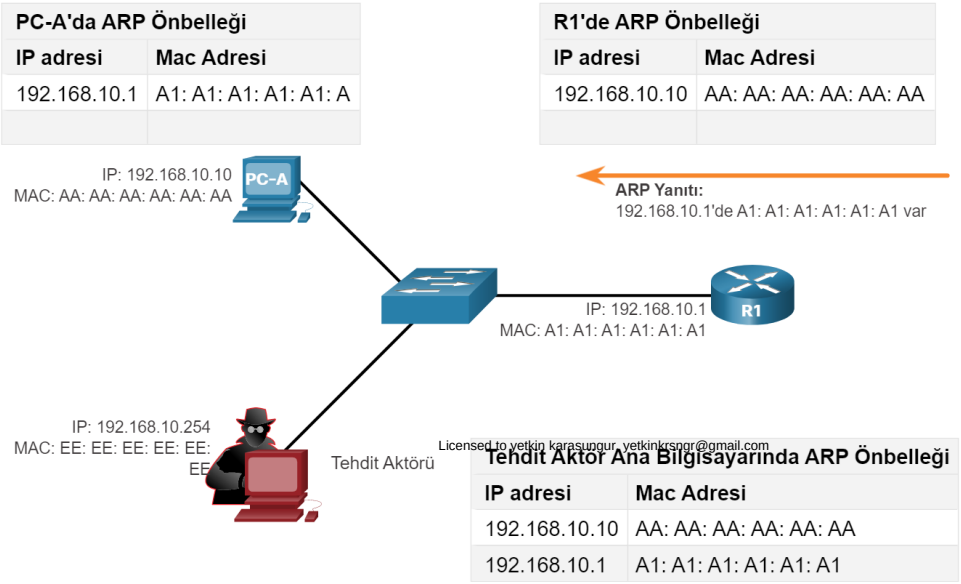
**ARP Önbellek Zehirlenmesi**

ARP önbellek zehirlenmesi, çeşitli ortadaki adam saldırıları başlatmak için kullanılabilir.

Şekil, ARP önbellek zehirlenmesinin nasıl çalıştığını göstermektedir. PC-A, varsayılan ağ geçidinin (R1) MAC adresini gerektirir; bu nedenle, 192.168.10.1 MAC adresi için bir ARP Talebi gönderir.



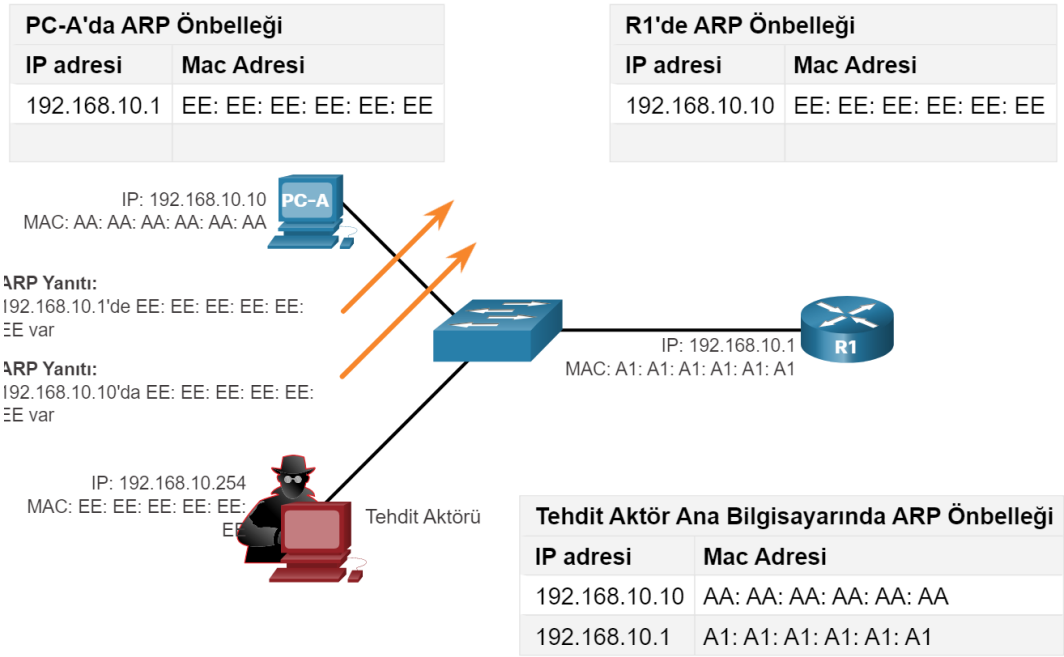

Bu şekilde R1, ARP önbelleğini PC-A'nın IP ve MAC adresleriyle günceller. R1, PC-A'ya bir ARP Yanıtı gönderir ve daha sonra ARP önbelleğini R1'in IP ve MAC adresleriyle günceller.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Şekilde, tehdit aktörü, belirtilen hedef IP adresleri için kendi MAC adresini kullanarak iki sahte nedensiz ARP Yanıtı gönderir. PC-A, artık tehdit aktörünün ana bilgisayar MAC adresini işaret eden varsayılan ağ geçidiyle ARP önbelleğini günceller. R1 ayrıca ARP önbelleğini tehdit aktörünün MAC adresini gösteren PC-A'nın IP adresiyle günceller.

Tehdit aktörünün sunucusu, bir ARP zehirlenmesi saldırısı gerçekleştiriyor. ARP zehirlenme saldırısı pasif veya aktif olabilir. Pasif ARP zehirlenmesi, tehdit aktörlerinin gizli bilgileri çaldığı yerdir. Aktif ARP zehirlenmesi, tehdit aktörlerinin aktarım sırasında verileri değiştirdiği veya kötü amaçlı verileri enjekte etmesidir.




İnternette, dsniff, Cain & Abel, ettercap, Yersinia gibi ARP MITM saldırıları oluşturmak için birçok araç bulunmaktadır.

## 33.8.2.DNS Saldırıları

Alanı Adı Hizmeti (DNS) protokolü, aşağıdakiler gibi kaynak adlarıyla eşleşen otomatik bir hizmeti tanımlar: www.cisco.com karşılık IPv4 veya IPv6 adresi gibi gerekli sayısal ağ adresiyle. Sorgular, yanıtlar ve veriler için biçim içerir ve DNS yanıtının türünü tanımlamak için kaynak kayıtlarını (RR) kullanır.

DNS'nin güvenliğini sağlamak genellikle göz ardı edilir. Bununla birlikte, bir ağın çalışması için çok önemlidir ve buna göre güvenlik altına alınmalıdır.

DNS saldırıları şunları içerir:

DNS açık çözümleyici saldırıları
DNS gizleme saldırıları
DNS etki alanı gölgeleme saldırıları
DNS tünelleme saldırıları

### DNS Açık Çözümleyici Saldırıları

Birçok kuruluş, sorgulara yanıt vermek için GoogleDNS (8.8.8.8) gibi herkese açık olan DNS sunucularının hizmetlerini kullanır. Bu tür DNS sunucusu, açık çözümleyici olarak adlandırılır. Bir DNS açık çözümleyicisi, yönetici etki alanının dışındaki istemcilerden gelen sorguları yanıtlar.

### DNS Gizleme Saldırıları

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tehdit aktörleri, kimliklerini gizlemek için, saldırılarını gerçekleştirmek için DNS gizlilik tekniklerini de kullanır.

**DNS Etki Alanı Gölgeleme Saldırıları**

Etki alanı gölgeleme, saldırılar sırasında kullanılacak birden çok alt etki alanını sessizce oluşturmak için etki alanı hesabı kimlik bilgilerini toplayan tehdit aktörünü içerir. Bu alt alanlar, genellikle ana etki alanının gerçek sahibini uyarmadan kötü amaçlı sunuculara işaret eder.

### 33.8.3.DNS Tünelleme

DNS tünellemesini kullanan tehdit aktörleri, DNS dışı trafiği DNS trafiği içine yerleştirir. Bu yöntem, bir tehdit aktörü korumalı bir ağ içindeki botlarla iletişim kurmak istediğinde veya kuruluştan parola veritabanı gibi verileri çalmak istediğinde genellikle güvenlik çözümlerini atlatır. Tehdit aktörü DNS tünellemesini kullandığında, farklı DNS kaydı türleri değiştirilir. Botnet'e gönderilen CnC komutları için DNS tünelleme şu şekilde çalışır:

1. Komut verileri birden çok kodlanmış parçaya bölünmüştür.
2. Her yığın, DNS sorgusunun daha düşük düzey bir etki alanı adı etiketine yerleştirilir.
3. Sorgu için yerel veya ağa bağlı DNS'den yanıt olmadığından, istek ISS'nin özyinelemeli DNS sunucularına gönderilir.
4. Özyinelemeli DNS hizmeti, sorguyu tehdit aktörünün yetkili ad sunucusuna iletir.
5. İşlem, parçalarını içeren tüm sorgular gönderilinceye kadar tekrarlanır.
6. Tehdit aktörünün yetkili ad sunucusu, virüslü cihazlardan DNS sorgularını aldığında, kapsüllenmiş, kodlanmış CnC komutlarını içeren her DNS sorgusu için yanıtlar gönderir.
7. Güvenliği ihlal edilen ana bilgisayardaki kötü amaçlı yazılım, yığınları yeniden birleştirir ve DNS kaydında gizlenen komutları yürütür.

DNS tünellemeyi durdurmak için, ağ yöneticisinin DNS trafiğini inceleyen bir filtre kullanması gerekir. Ortalamadan daha uzun olan veya alan adı şüpheli olan DNS sorgularına çok dikkat edin. Cisco OpenDNS gibi DNS çözümleri, şüpheli etki alanlarını belirleyerek DNS tünelleme trafiğinin çoğunu engeller.

## 33.9.En İyi Ağ Güvenliği Uygulamaları

### 33.9.1.Gizlilik, Bütünlük ve Kullanılabilirlik (Confidentiality, Integrity, and Availability)

Ağınızı savunmak için kullanabileceğiniz birçok en iyi uygulama var.

Ağ güvenliği, bilgi ve bilgi sistemlerini yetkisiz erişime, kullanıma, ifşa etmeye, kesintiye, değiştirmeye veya yok etmeye karşı korumayı içerir.

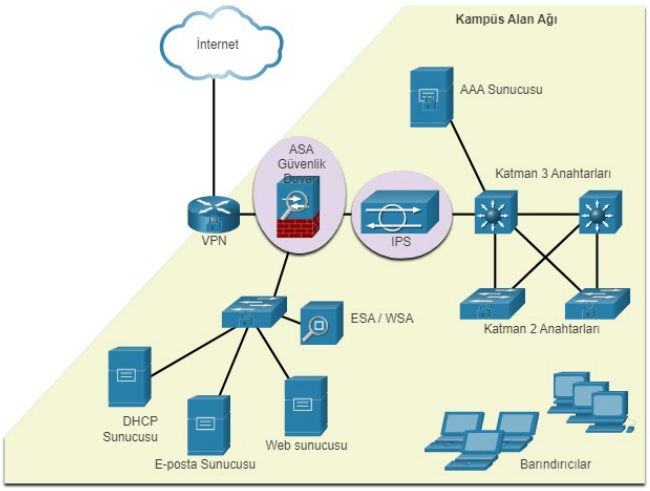
Çoğu kuruluş CIA bilgi güvenliği üçlüsünü takip eder:

**Gizlilik** - Yalnızca yetkili kişiler, kuruluşlar veya süreçler hassas bilgilere erişebilir. Verileri şifrelemek ve şifresini çözmek için AES gibi kriptografik şifreleme algoritmalarının kullanılmasını gerektirebilir.
**Bütünlük** - Verileri yetkisiz değişikliklere karşı korumayı ifade eder. SHA gibi kriptografik hash algoritmalarının kullanılmasını gerektirir.
**Kullanılabilirlik** - Yetkili kullanıcılar, önemli kaynaklara ve verilere kesintisiz erişime sahip olmalıdır. Yedekli hizmetler, ağ geçitleri ve bağlantıların uygulanmasını gerektirir.

### 33.9.2.Derinlemesine Savunma Yaklaşım

Hem genel hem de özel ağlar arasında güvenli iletişim sağlamak için yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar dahil olmak üzere cihazları güvenli hale getirmelisiniz. Çoğu kuruluş, güvenlik için derinlemesine bir savunma yaklaşımı kullanır. Bu aynı zamanda katmanlı bir yaklaşım olarak da bilinir. Birlikte çalışan ağ cihazları ve hizmetlerinin bir kombinasyonunu gerektirir. Şekildeki ağa bakınız.

Licensed to yetkin.karasangur.yetkinksg@gmail.com




Bir kuruluşun kullanıcılarını ve varlıklarını TCP / IP tehditlerine karşı korumak için çeşitli güvenlik cihazları ve hizmetleri uygulanmaktadır.

- **VPN** - Bir yönlendirici, kurumsal sitelerle güvenli VPN hizmetleri sağlamak ve güvenli şifrelenmiş tüneller kullanarak uzak kullanıcılar için uzaktan erişim desteği sağlamak için kullanılır.
- **ASA Güvenlik Duvarı** - Bu özel cihaz, durum bilgisi olan güvenlik duvarı hizmetleri sağlar. Dahili trafiğin dışarı çıkıp geri gelmesini sağlar, ancak dış trafik iç ana bilgisayarlara bağlantı başlatamaz.
- **IPS** - Bir Saldırı Önleme Sistemi (IPS), kötü amaçlı yazılım, ağ saldırısı imzaları ve daha fazlasını arayan gelen ve giden trafiği izler. Bir tehdidi fark ederse, hemen durdurabilir.
- **ESA / WSA** - E-posta güvenlik aracı (ESA), spam ve şüpheli e-postaları filtreler. Web güvenlik cihazı, bilinen ve şüpheli kötü amaçlı internet sitelerini filtreler.
- **AAA Sunucusu** - Bu sunucu, ağ cihazlarına erişme ve yönetme yetkisine sahip olan güvenli bir veritabanı içerir. Ağ cihazları, bu veritabanını kullanarak yönetici kullanıcıların kimliğini doğrular.

Yönlendirici ve anahtarlar da dahil olmak üzere tüm ağ aygıtları sağlamlaştırılmıştır; bu, tehdit aktörlerinin aygıtlara erişim sağlamasını ve bu aygıtlara müdahale etmesini önlemek için güvenli oldukları anlamına gelir.

Ardından, çeşitli bağlantılar arasında dolaşırken verileri güvenli hale getirmelisiniz. Bu, dahili trafiği içerebilir, ancak kuruluşun dışından şube sitelerine, uzaktan çalışma sitelerine ve ortak sitelere seyahat eden verileri korumak daha önemlidir.

## 33.9.3.Güvenlik Duvarları

Güvenlik duvarı, ağlar arasında bir erişim kontrol politikası uygulayan bir sistem veya sistemler grubudur.

Herhangi bir harici adresten web sunucusuna trafiğe **izin verin** .
FTP sunucusuna trafiğe **izin verin** .

SMTP sunucusuna trafiğe **izin verin** .

Dahili IMAP sunucusuna trafiğe **izin verin** .

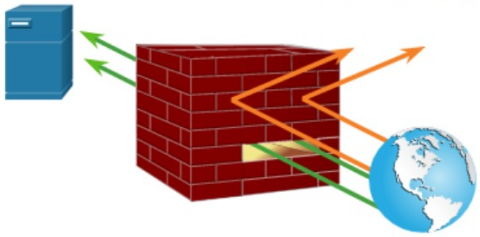
Dahili kayıtlı IP adresleriyle eşleşen ağ adreslerine sahip tüm gelen trafiği **reddedin** .
harici adreslerden sunucuya gelen tüm trafiği **reddedin** .

tüm gelen ICMP yankı isteği trafiğini **reddedin** .

tüm gelen MS Active Directory sorgularını **reddedin** .

MS SQL sunucusu sorguları tüm gelen trafiği **reddedin** .

tüm MS Domain Yerel yayınları **reddedin** .



Tüm güvenlik duvarları bazı ortak özellikleri paylaşır:

- Güvenlik duvarları ağ saldırılarına karşı dirençlidir.
- Güvenlik duvarları, dahili kurumsal ağlar ile harici ağlar arasındaki tek geçiş noktalarıdır çünkü tüm trafik güvenlik duvarından geçer.
- Güvenlik duvarları erişim kontrol politikasını uygular.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Bir ağda güvenlik duvarı kullanmanın çeşitli faydaları vardır:

- Hassas ana bilgisayarların, kaynakların ve uygulamaların güvenilmeyen kullanıcılara maruz kalmasını engeller.
- Protokol hatalarının kötüye kullanılmasını önleyen protokol akışını sterilize ederler.
- Kötü amaçlı verileri sunuculardan ve istemcilerden engellerler.
- Ağ erişim kontrolünün çoğunu ağdaki birkaç güvenlik duvarına yükleyerek güvenlik yönetimi karmaşıklığını azaltırlar.

Güvenlik duvarları da bazı sınırlamalara sahiptir:

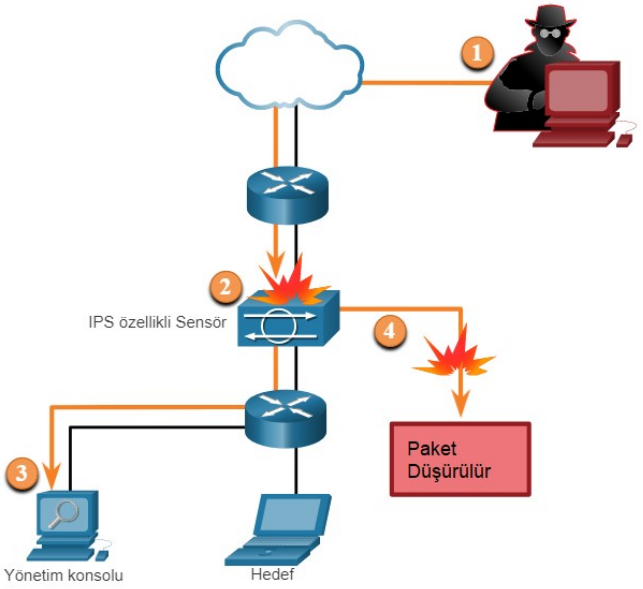
- Yanlış yapılandırılmış bir güvenlik duvarının, ağ üzerinde tek bir hata noktası haline gelmesi gibi ciddi sonuçları olabilir.
- Birçok uygulamadan gelen veriler güvenlik duvarlarından güvenli bir şekilde geçirilemez.
- Kullanıcılar, ağı olası saldırılara maruz bırakan engellenen materyali almak için proaktif olarak güvenlik duvarının çevresinde yollar arayabilir.
- Ağ performansı yavaşlayabilir.
- Yetkisiz trafik, güvenlik duvarı üzerinden yasal trafik olarak görünmesi için tünel haline getirilebilir veya gizlenebilir.

## 33.9.4.IPS

Hızlı hareket eden ve gelişen saldırılara karşı savunma yapmak için, saldırı tespit sistemleri-intrusion detection systems (IDS) veya daha ölçeklenebilir saldırı önleme sistemleri- intrusion prevention systems (IPS) gibi uygun maliyetli tespit ve önleme sistemlerine ihtiyacınız olabilir. Ağ mimarı, bu çözümleri ağın giriş ve çıkış noktalarına entegre eder.

IDS ve IPS teknolojileri, şekilde gösterildiği gibi birkaç özelliği paylaşır. IDS ve IPS teknolojilerinin her ikisi de sensörler olarak dağıtılır. Bir IDS veya IPS sensörü birkaç farklı cihaz biçiminde olabilir:

- Cisco IOS IPS yazılımıyla yapılandırılmış bir yönlendirici
- Özel IDS veya IPS hizmetleri sağlamak için özel olarak tasarlanmış bir cihaz
- Uyarlanabilir bir güvenlik cihazı (ASA), anahtar veya yönlendiriciye takılı bir ağ modülü




Şekil, bir IPS'nin reddedilen trafiği nasıl işlediğini gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

1. Tehdit aktörü, hedef dizüstü bilgisayara yönelik bir paket gönderir.
2. IPS trafiği keser ve onu bilinen tehditlere ve yapılandırılmış ilkelere göre değerlendirir.
3. IPS, yönetim konsoluna bir günlük mesajı gönderir.
4. IPS paketi düşürür.

IDS ve IPS teknolojileri, imzaları kullanarak ağ trafiğindeki kalıpları algılar. İmza, bir IDS veya IPS'nin kötü niyetli etkinliği tespit etmek için kullandığı bir dizi kuraldır. İmzalar, ciddi güvenlik ihlallerini tespit etmek, yaygın ağ saldırılarını tespit etmek ve bilgi toplamak için kullanılabilir. IDS ve IPS teknolojileri, atomik imza modellerini (tek paket) veya bileşik imza modellerini (çoklu paket) algılayabilir.

## 33.10.Kriptografi

### 33.10.1.İletişimin Güvenliğini Sağlama

Kuruluşlar, verileri bağlantılar arasında dolaşırken verilerin güvenliğini sağlamak için destek sağlamalıdır. Bu, dahili trafiği içerebilir, ancak kuruluşun dışından şube sitelerine, uzaktan çalışma sitelerine ve ortak sitelere giden verileri korumak daha da önemlidir.

Bunlar, güvenli iletişimin dört unsurudur:

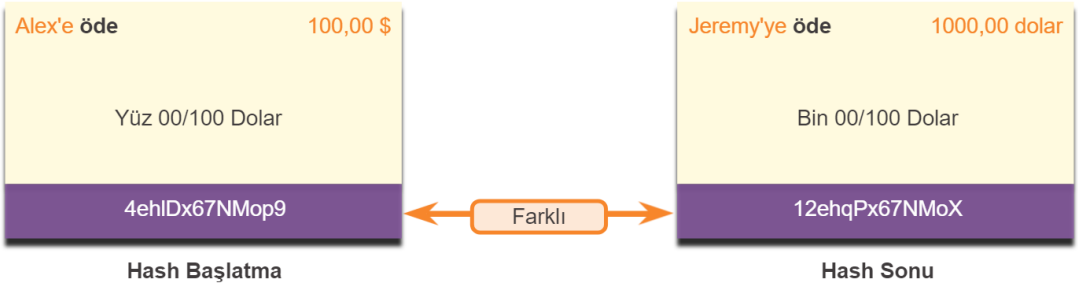
- Veri Bütünlüğü - Mesajın değiştirilmediğini garanti eder. Aktarım halindeki verilerde herhangi bir değişiklik tespit edilecektir. Bütünlük, Mesaj Özeti sürüm 5-Message Digest version 5 (MD5) veya Güvenli Karma Algoritma- Secure Hash Algorithm (SHA) karma oluşturma algoritmaları uygulanarak sağlanır.
- Kaynak Doğrulama - Mesajın sahte olmadığını ve aslında bildirdiği kişiden geldiğini garanti eder. Çoğu modern ağ, karma ileti kimlik doğrulama kodu- hash message authentication code (HMAC) gibi protokollerle kimlik doğrulaması sağlar.
- Veri Gizliliği - Yalnızca yetkili kullanıcıların mesajı okuyabileceğini garanti eder. Mesaj ele geçirilirse, makul bir süre içinde deşifre edilemez. Veri gizliliği simetrik ve asimetrik şifreleme algoritmaları kullanılarak gerçekleştirilir.
- Verilerin Reddedilmemesi - Gönderenin gönderilen bir mesajın geçerliliğini reddedemeyeceğini veya reddedemeyeceğini garanti eder. Reddetmeme, yalnızca gönderenin, bu mesajın nasıl ele alınacağına ilişkin benzersiz özelliklere veya imzaya sahip olmasına dayanır.

Kriptografi, veri iletişiminin olduğu hemen her yerde kullanılabilir. Aslında eğilim, tüm iletişimin şifrelenmesi yönündedir.

### 33.10.2.Veri Bütünlüğü

Bir mesajın bütünlüğünü sağlamak için karma (hash) işlevleri kullanılır. Mesaj verilerinin yanlışlıkla veya kasıtlı olarak değişmediğini garanti ederler.

Şekilde, gönderen Alex'e 100 dolarlık bir para transferi yapıyor.




Gönderen, alıcıya giden yolda mesajın değiştirilmediğinden emin olmak ister.

1. Gönderen cihaz, mesajı bir karma algoritmaya girer ve 4ehiDx67NMop9 sabit uzunluktaki karmasını hesaplar.
2. Bu karma daha sonra mesaja eklenir ve alıcıya gönderilir. Hem mesaj hem de karma düz metindir.
3. Alıcı cihaz, mesajı mesajdan çıkarır ve mesajı aynı karma algoritmaya girer. Hesaplanan hash, mesaja eklenmiş olana eşitse, mesaj iletim sırasında değiştirilmemiştir. Karmalar, şekilde gösterildiği gibi eşit değilse, mesajın bütünlüğüne artık güvenilemez.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Hash Fonksiyonları

Üç iyi bilinen hash işlevi vardır.

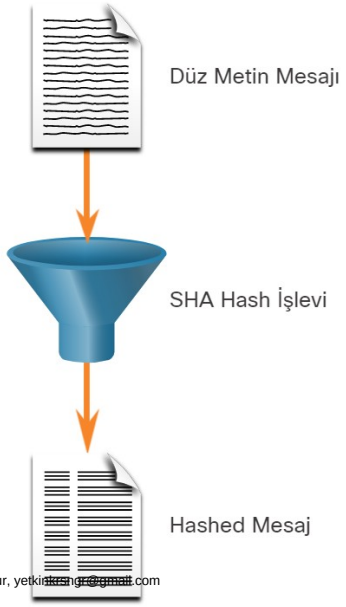
### 128-bit Özet ile MD5

MD5, şekilde gösterildiği gibi 128 bitlik bir karma mesaj üreten tek yönlü bir işlevdir. MD5, yalnızca daha iyi alternatifler olmadığında kullanılması gereken eski bir algoritmadır. Bunun yerine SHA-2 kullanın.

Şekilde, bir düz metin mesajı bir MD5 hash fonksiyonundan geçirilir. Sonuç, 128 bitlik bir karma mesajdır.

### SHA Hashing Algoritması

SHA-1, şekilde gösterildiği gibi MD5 hash işlevlerine çok benzer. Birkaç versiyon mevcuttur. SHA-1, 160 bitlik bir karma mesaj oluşturur ve MD5'ten biraz daha yavaştır. SHA-1'in bilinen kusurları vardır ve eski bir algoritmadır. Mümkünse SHA-2 kullanın.




Licensed to yetkin karasungur, yetkinkarsngr@gmail.com

Şekilde, bir düz metin mesajı bir SHA hash fonksiyonundan geçirilir. Sonuç, karma bir mesajdır.

## SHA-2

Buna SHA-224 (224 bit), SHA-256 (256 bit), SHA-384 (384 bit) ve SHA-512 (512 bit) dahildir. SHA-256, SHA-384 ve SHA-512, yeni nesil algoritmalardır ve mümkün olduğunda kullanılmalıdır.

Karma oluşturma, yanlışlıkla yapılan değişiklikleri tespit etmek için kullanılabilirken, kasıtlı değişikliklere karşı koruma sağlamak için kullanılamaz. Hashing prosedüründe göndericiden benzersiz bir tanımlama bilgisi yoktur. Bu, doğru hash işlevine sahip olan herkesin herhangi bir veri için bir hash hesaplayabileceği anlamına gelir.

Örneğin, mesaj ağ üzerinden geçtiğinde, potansiyel bir tehdit aktörü mesajı yakalayabilir, değiştirebilir, karmayı yeniden hesaplayabilir ve mesaja ekleyebilir. Alıcı cihaz, yalnızca eklenen karma değerlere göre doğrulama yapacaktır.

Bu nedenle, karma oluşturma ortadaki adam saldırılarına karşı savunmasızdır ve iletilen verilere güvenlik sağlamaz. Bütünlük ve kaynak kimlik doğrulaması sağlamak için daha fazlası gereklidir.

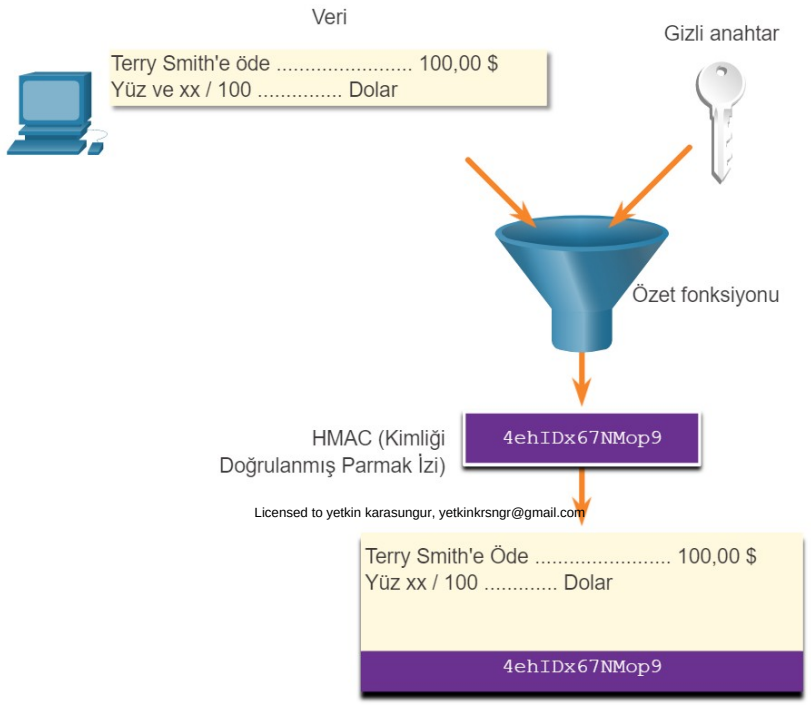
## Kaynak Kimlik Doğrulaması

Bütünlük güvencesine kimlik doğrulama eklemek için, bir anahtarlı karma ileti kimlik doğrulama kodu-keyed-hash message authentication code (HMAC) kullanın. HMAC, karma işlevine girdi olarak ek bir gizli anahtar kullanır.
Şekilde gösterildiği gibi, bir HMAC, bir şifreleme karma işlevini bir gizli anahtarla birleştiren herhangi bir kriptografik algoritma kullanılarak hesaplanır. Hash fonksiyonları, HMAC'lerin koruma mekanizmasının temelidir.

Yalnızca gönderen ve alıcı gizli anahtarı bilir ve karma işlevin çıktısı artık giriş verilerine ve gizli anahtara bağlıdır. Yalnızca bu gizli anahtara erişimi olan taraflar, bir HMAC işlevinin özetini hesaplayabilir. Bu, ortadaki adam saldırılarını yener ve veri kaynağının kimlik doğrulamasını sağlar.

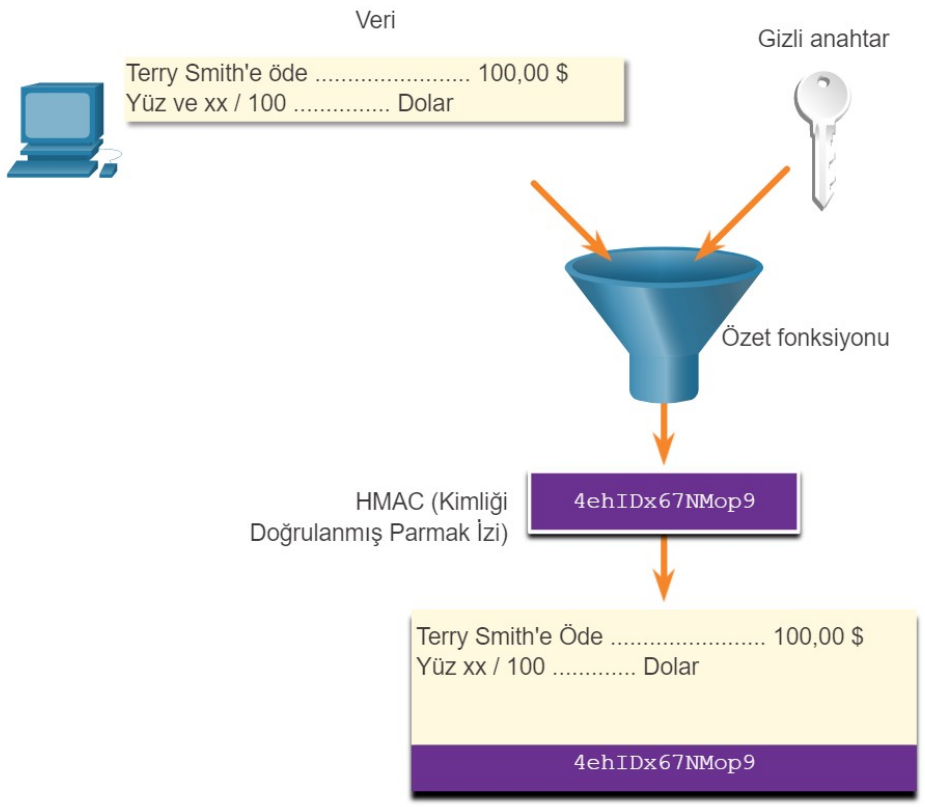
İki taraf bir gizli anahtarı paylaşırsa ve kimlik doğrulama için HMAC işlevlerini kullanırsa, bir tarafın aldığı bir mesajın uygun şekilde oluşturulmuş bir HMAC özeti, diğer tarafın mesajın kaynağı olduğunu gösterir. Bunun nedeni, diğer tarafın gizli anahtara sahip olmasıdır.

Şekilde gösterildiği gibi, gönderen cihaz verileri (Terry Smith'in 100 $ ödemesi ve gizli anahtar gibi) hash algoritmasına girer ve sabit uzunlukta HMAC özetini hesaplar. Bu doğrulanmış özet daha sonra iletiye eklenir ve alıcıya gönderilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Şekilde, alıcı cihaz, özeti mesajdan çıkarır ve düz metin mesajını gizli anahtarıyla aynı karma işlevine girdi olarak kullanır. Alıcı cihaz tarafından hesaplanan özet, gönderilen özete eşitse, mesaj değiştirilmemiştir. Ek olarak, yalnızca gönderen paylaşılan gizli anahtarın bir kopyasına sahip olduğu için mesajın kaynağı doğrulanır. HMAC işlevi, mesajın gerçekliğini sağlamıştır.

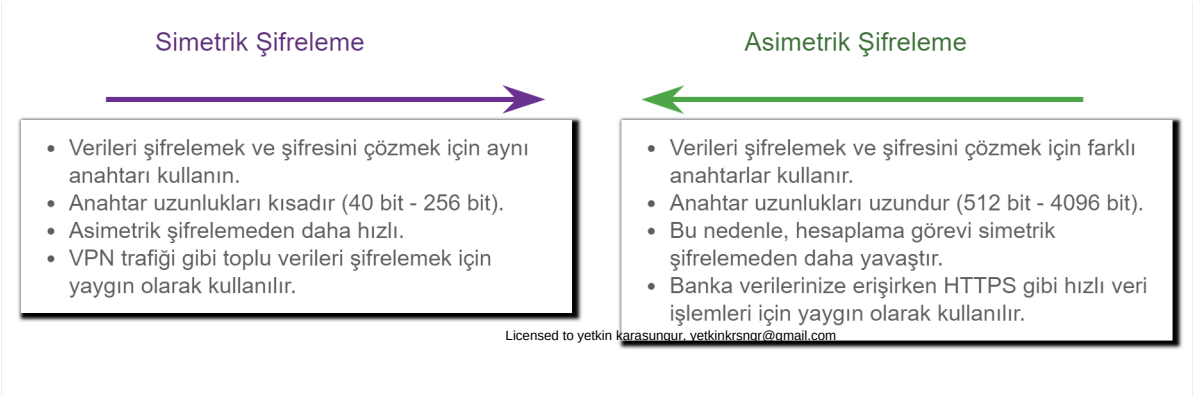



## 33.10.3.Veri Gizliliği

Veri gizliliğini sağlamak için kullanılan iki tür şifreleme vardır. Bu iki sınıf, anahtarları nasıl kullandıklarına göre farklılık gösterir.

(DES), 3DES ve Gelişmiş Şifreleme Standardı- Advanced Encryption Standard (AES) gibi simetrik şifreleme algoritmaları, iletişim kuran her bir tarafın önceden paylaşılan anahtarı bildiğine dayanır. Veri gizliliği, Rivest, Shamir ve Adleman (RSA) ve açık anahtar altyapısı- public key infrastructure ( (PKI) dahil asimetrik algoritmalar kullanılarak da sağlanabilir.

Şekil, her bir şifreleme algoritması yöntemi arasındaki bazı farklılıkları vurgulamaktadır.



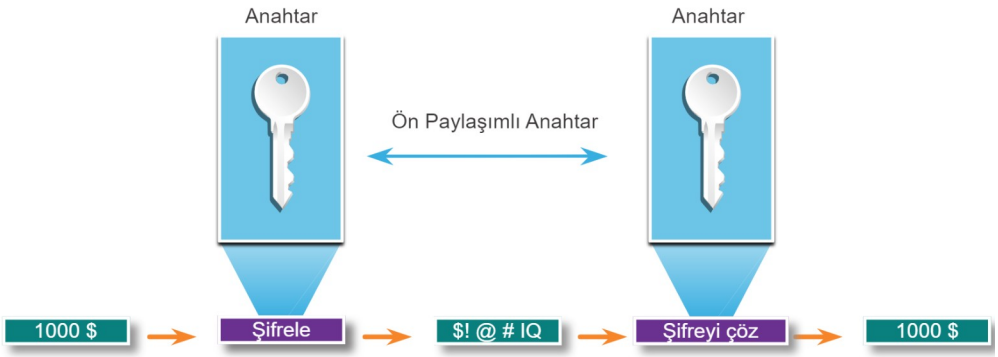

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Simetrik Şifreleme

Simetrik algoritmalar, verileri şifrelemek ve şifresini çözmek için aynı önceden paylaşılan anahtarı kullanır. Gizli anahtar olarak da adlandırılan önceden paylaşılan bir anahtar, herhangi bir şifreli iletişim gerçekleşmeden önce gönderen ve alıcı tarafından bilinir.

Simetrik şifrelemenin nasıl çalıştığını göstermeye yardımcı olması için, Alice ve Bob'un farklı yerlerde yaşadıkları ve posta sistemi aracılığıyla birbirleriyle gizli mesaj alışverişi yapmak istedikleri bir örneği düşünün. Bu örnekte Alice, Bob'a gizli bir mesaj göndermek istiyor.

Şekilde, Alice ve Bob, tek bir asma kilit için aynı anahtarlara sahiptir. Bu anahtarlar, herhangi bir gizli mesaj gönderilmeden önce değiştirildi. Alice gizli bir mesaj yazar ve anahtarıyla asma kilidi kullanarak kilitlediği küçük bir kutuya koyar. Kutuyu Bob'a postalar. Kutu postane sisteminden geçerken mesaj kutunun içinde güvenli bir şekilde kilitlenir. Bob kutuyu aldığında, asma kilidin kilidini açmak ve mesajı almak için anahtarını kullanır. Bob, Alice'e gizli bir cevap göndermek için aynı kutuyu ve asma kilidi kullanabilir.




Günümüzde simetrik şifreleme algoritmaları, VPN trafiğiyle yaygın olarak kullanılmaktadır. Bunun nedeni, simetrik algoritmaların asimetrik şifreleme algoritmalarından daha az CPU kaynağı kullanmasıdır. VPN kullanırken verilerin şifrelenmesi ve şifresinin çözülmesi hızlıdır. Diğer şifreleme türleri gibi simetrik şifreleme algoritmalarını kullanırken, anahtar ne kadar uzun olursa, birinin anahtarı keşfetmesi o kadar uzun sürer. Şifreleme anahtarlarının çoğu 112 ile 256 bit arasındadır. Şifrelemenin güvenli olduğundan emin olmak için minimum 128 bit anahtar uzunluğu kullanın. Daha güvenli iletişim için daha uzun bir anahtar kullanın.

İyi bilinen simetrik şifreleme algoritmaları tabloda açıklanmaktadır.

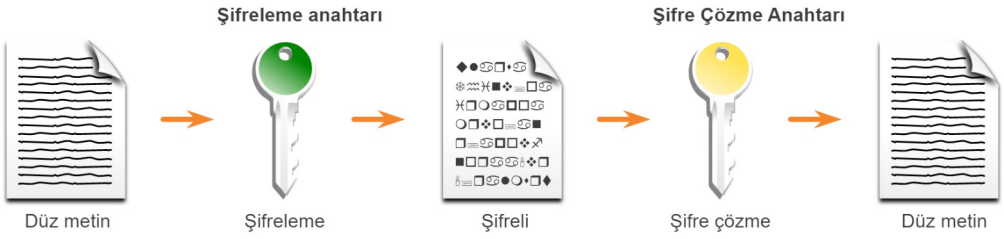
| Simetrik Şifreleme Algoritmaları | Açıklama |
|---|---|
| Veri Şifreleme Standardı-Data Encryption Standard (DES) | Bu, eski bir simetrik şifreleme algoritmasıdır.vAkış şifreleme modunda kullanılabilir, ancak genellikle verileri 64 bitlik blok boyutunda şifreleyerek blok modunda çalışır. Bir akış şifresi, her seferinde bir baytı veya bir biti şifreler. |
| 3DES (Üçlü DES) | Bu, daha yeni bir DES sürümüdür, ancak DES algoritma sürecini üç kez tekrarlar. Temel algoritma sahada 35 yıldan uzun süredir iyi bir şekilde test edilmiştir. Çok kısa anahtar ömürleri kullanılarak uygulandığında çok güvenilir kabul edilir. |
| Gelişmiş Şifreleme Standardı (AES) | AES, 3DES'ten daha güvenli ve daha verimli bir algoritmadır. Popüler ve önerilen bir simetrik şifreleme algoritmasıdır. 128, 192 veya 256 bit uzunluğundaki veri bloklarını şifrelemek için değişken anahtar uzunluğu 128, 192 veya 256 bit kullanarak dokuz anahtar ve blok uzunluğu kombinasyonu sunar. |
| Yazılım İçin Optimize Edilmiş Şifreleme Algoritması-Software-Optimized Encryption Algorithm (SEAL) | SEAL; DES, 3DES ve AES'e göre daha hızlı bir alternatif simetrik şifreleme algoritmasıdır. 160 bitlik bir şifreleme anahtarı kullanır ve diğer yazılım tabanlı algoritmalara kıyasla CPU üzerinde daha az etkiye sahiptir. |
| Rivest ciphers (RC) serisi algoritmaları | Bu algoritma Ron Rivest tarafından geliştirilmiştir. Çeşitli varyasyonlar geliştirilmiştir, ancak RC4 kullanımda en yaygın olanıdır. RC4 bir akış şifresidir ve SSL ve TLS'de web trafiğini güvence altına almak için kullanılır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Asimetrik Şifreleme

Açık anahtar algoritmaları olarak da adlandırılan asimetrik algoritmalar, şekilde gösterildiği gibi, şifreleme için kullanılan anahtarın, şifre çözme için kullanılan anahtardan farklı olacağı şekilde tasarlanmıştır. Şifre çözme anahtarı, makul bir süre içinde şifreleme anahtarından hesaplanamaz ve bunun tersi de geçerlidir.

Asimetrik algoritmalar bir ortak anahtar ve bir özel anahtar kullanır. Her iki anahtar da şifreleme işlemi yapabilir, ancak şifre çözme için tamamlayıcı eşleştirilmiş anahtar gereklidir. İşlem ayrıca tersine çevrilebilir. Genel anahtarla şifrelenen verilerin şifresinin çözülmesi için özel anahtar gerekir. Asimetrik algoritmalar, bu süreci kullanarak gizlilik, kimlik doğrulama ve bütünlük sağlar.




Hiçbir tarafın paylaşılan bir parola olmadığı için, çok uzun anahtar uzunlukları kullanılmalıdır. Asimetrik şifreleme, 512 ile 4.096 bit arasındaki anahtar uzunluklarını kullanabilir. 1.024 bit veya daha büyük anahtar uzunluklarına güvenilebilirken, daha kısa anahtar uzunlukları güvenilmez olarak kabul edilir.

Asimetrik anahtar algoritmaları kullanan protokol örnekleri şunları içerir:

- İnternet Anahtar Değişimi- Internet Key Exchange (IKE) - Bu, IPsec VPN'lerin temel bir bileşenidir.
- Güvenli Yuva Katmanı - Secure Socket Layer (SSL) - Bu, artık IETF standart Taşıma Katmanı Güvenliği (TLS) olarak uygulanmaktadır.
- Güvenli Kabuk-Secure Shell (SSH) - Bu protokol, ağ cihazlarına güvenli bir uzaktan erişim bağlantısı sağlar.
- Pretty Good Privacy (PGP) - Bu bilgisayar programı, kriptografik gizlilik ve kimlik doğrulama sağlar. Genellikle e-posta iletişimlerinin güvenliğini artırmak için kullanılır.

Asimetrik algoritmalar, simetrik algoritmalardan önemli ölçüde daha yavaştır. Tasarımları, son derece büyük sayıları çarpanlarına ayırmak veya çok büyük sayıların ayrık logaritmalarını hesaplamak gibi hesaplama problemlerine dayanmaktadır.

Yavaş oldukları için, asimetrik algoritmalar genellikle dijital imzalar ve anahtar değişimi gibi düşük hacimli kriptografik mekanizmalarda kullanılır. Bununla birlikte, asimetrik algoritmaların anahtar yönetimi, simetrik algoritmalardan daha basit olma eğilimindedir, çünkü genellikle iki şifreleme veya şifre çözme anahtarından biri halka açık hale getirilebilir.

Asimetrik şifreleme algoritmalarının yaygın örnekleri tabloda açıklanmaktadır.

| Asimetrik Şifreleme Algoritması | Anahtar Uzunluğu | Açıklama |
|---|---|---|
| Diffie-Hellman (DH) | 512, 1024, 2048, 3072, 4096 | Diffie-Hellman algoritması, iki tarafın birbirlerine göndermek istedikleri mesajları şifrelemek için kullanabilecekleri bir anahtar üzerinde anlaşmalarına izin verir.Bu algoritmanın güvenliği, bir sayıyı belirli bir güce yükseltmenin kolay olduğu, ancak sayı ve sonuç verildiğinde hangi gücün kullanıldığını hesaplamanın zor olduğu varsayımına bağlıdır. |
| Dijital İmza Standardı-Digital Signature Standard (DSS) | 512 - 1024 | DSS, DSA'yı dijital imzalar için algoritma olarak belirtir. DSA, ElGamal imza şemasına dayalı bir genel anahtar algoritmasıdır. İmza oluşturma hızı RSA'ya benzer, ancak doğrulama için 10 ila 40 kat daha yavaştır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Asimetrik Şifreleme Algoritması | Anahtar Uzunluğu | Açıklama |
|---|---|---|
| ve Dijital İmza Algoritması- Digital Signature Algorithm (DSA) | | |
| Rivest, Shamir ve Adleman şifreleme algoritmaları (RSA) | 512 ila 2048 | RSA, çok büyük sayıları çarpanlara ayırmanın mevcut zorluğuna dayanan açık anahtarlı kriptografi içindir. İmzalamaya olduğu kadar şifrelemeye de uygun olduğu bilinen ilk algoritmadır. Elektronik ticaret protokollerinde yaygın olarak kullanılmaktadır ve yeterince uzun anahtarlar ve güncel uygulamaların kullanımı verildiğinde güvenli olduğuna inanılmaktadır. |
| EIGamal | 512 - 1024 | Diffie-Hellman anahtar anlaşmasına dayanan, açık anahtarlı kriptografi için asimetrik bir anahtar şifreleme algoritması. ElGamal sisteminin bir dezavantajı, şifrelenmiş mesajın çok büyük olması, orijinal mesajın yaklaşık iki katı büyüklüğünde olması ve bu nedenle yalnızca gizli anahtarlar gibi küçük mesajlar için kullanılmasıdır. |
| Eliptik eğri teknikleri- Elliptical curve techniques | 160 | Eliptik eğri şifreleme, Diffie-Hellman veya ElGamal gibi birçok kriptografik algoritmayı uyarlamak için kullanılabilir. Eliptik eğri kriptografisinin temel avantajı, anahtarların çok daha küçük olabilmesidir. |

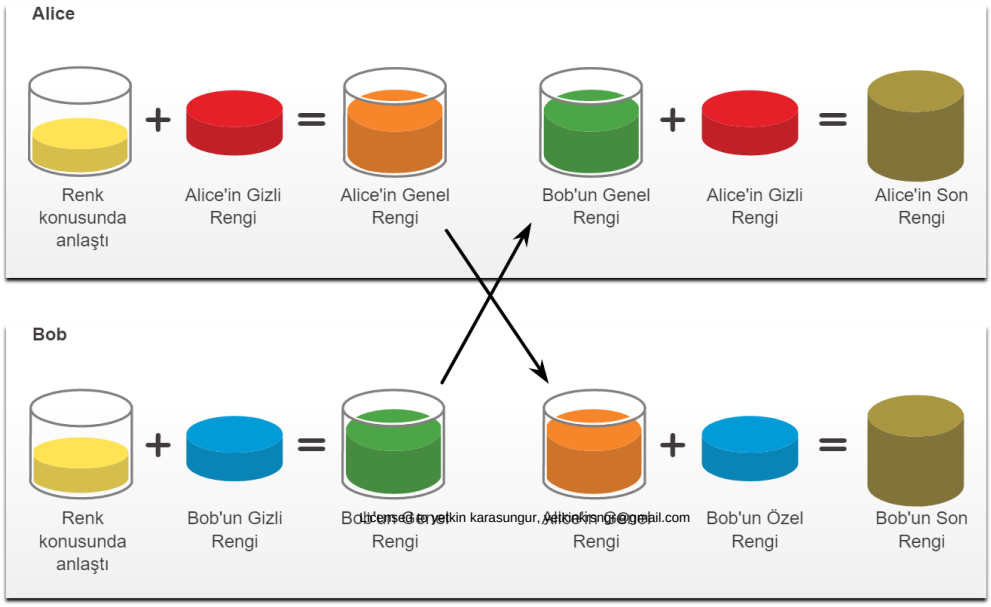
**Diffie-Hellman**

Diffie-Hellman (DH), iki bilgisayarın daha önce iletişim kurmadan aynı paylaşılan gizli anahtarı oluşturduğu asimetrik bir matematiksel algoritmadır. Yeni paylaşılan anahtar aslında gönderen ve alıcı arasında asla değiştirilmez. Bununla birlikte, her iki taraf da bildiği için, anahtar, iki sistem arasındaki trafiği şifrelemek için bir şifreleme algoritması tarafından kullanılabilir.

DH'nin yaygın olarak kullanıldığı üç örnek örneği aşağıda bulabilirsiniz:

- Veriler, bir IPsec VPN kullanılarak değiştirilir.
- Veriler internette SSL veya TLS kullanılarak şifrelenir.
- SSH verileri değiş tokuş edilir.

DH'nin nasıl çalıştığını göstermeye yardımcı olması için şekle bakın.



Licensed to yetkin karasungur, yetkinsungur@gmail.com

DH anahtarı anlaşması sürecini basitleştirmek için karmaşık uzun sayılar yerine şekildeki renkler kullanılacaktır. DH anahtar değişimi, Alice ve Bob'un gizli tutulması gerekmeyen rastgele bir ortak renk üzerinde anlaşmasıyla başlar. Örneğimizde üzerinde anlaşmaya varılan renk sarıdır.

Sonra, Alice ve Bob gizli bir renk seçecek. Bob maviyi seçerken Alice kırmızıyı seçti. Bu gizli renkler asla kimseyle paylaşılmayacak. Gizli renk, her bir tarafın seçilen gizli özel anahtarını temsil eder.

Alice ve Bob artık ortak bir renk oluşturmak için paylaşılan ortak rengi (sarı) ilgili gizli rengiyle karıştırıyor. Bu nedenle Alice, genel bir turuncu renk üretmek için sarıyı kırmızı rengiyle karıştıracaktır. Bob, genel bir yeşil renk oluşturmak için sarı ve maviyi karıştıracak.

Alice genel rengini (turuncu) Bob'a gönderir ve Bob genel rengini (yeşil) Alice'e gönderir.

Alice ve Bob, aldıkları rengi kendi orijinal gizli renkleriyle karıştırır (Alice için Kırmızı ve Bob için mavi.). Sonuç, ortağın son renk karışımıyla aynı olan son bir kahverengi renk karışımıdır. Kahverengi renk, Bob ve Alice arasında ortaya çıkan paylaşılan gizli anahtarı temsil eder.

DH'nin güvenliği, hesaplamalarında çok büyük sayılar kullanmasına dayanmaktadır. Örneğin, bir DH 1024 bitlik sayı kabaca 309 basamaklı ondalık bir sayıya eşittir. Bir milyarın 10 ondalık basamak (1.000.000.000) olduğu düşünüldüğünde, bir değil birden çok 309 basamaklı ondalık sayı ile çalışmanın karmaşıklığı kolayca hayal edilebilir.

Ne yazık ki, asimetrik anahtar sistemleri her tür toplu şifreleme için son derece yavaştır. Bu nedenle, trafiğin büyük kısmını 3DES veya AES gibi simetrik bir algoritma kullanarak şifrelemek ve şifreleme algoritması tarafından kullanılacak anahtarlar oluşturmak için DH algoritmasını kullanmak yaygındır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 34.Bölüm: ACL (Access Control List) Erişim Denetim Listeleri

## 34.1.ACL'lerin Amacı

### 34.1.1.ACL Nedir?

Yönlendiriciler, paket başlığındaki bilgilere göre yönlendirme kararları verir. Bir yönlendirici arayüzüne giren trafik, yalnızca yönlendirme tablosundaki bilgilere göre yönlendirilir. Yönlendirici, en iyi eşleşmeyi bulmak için hedef IP adresini yönlendirme tablosundaki yollarla karşılaştırır ve ardından paketi en iyi eşleşme yoluna göre iletir. Aynı işlem, bir erişim kontrol listesi (ACL) kullanarak trafiği filtrelemek için kullanılabilir.

ACL, paket başlığında bulunan bilgilere göre paketleri filtrelemek için kullanılan bir dizi IOS komutudur. Varsayılan olarak, bir yönlendiricinin yapılandırılmış herhangi bir ACL'si yoktur. Bununla birlikte, bir arayüze ACL uygulandığında, yönlendirici, paketin iletilip iletilemeyeceğini belirlemek için arayüzden geçerken tüm ağ paketlerini değerlendirme ek görevini gerçekleştirir.

ACL, erişim denetimi girdileri (Access Control Entries-ACE'ler) olarak bilinen sıralı bir izin verme veya reddetme deyimleri listesi kullanır.

Not: ACE'ler, genellikle ACL ifadeleri olarak da adlandırılır.

Ağ trafiği bir ACL ile yapılandırılmış bir arabirimden geçtiğinde, yönlendirici, paketin ACE'lerden biriyle eşleşip eşleşmediğini belirlemek için paket içindeki bilgileri her ACE ile sırayla karşılaştırır. Bu işleme paket filtreleme adı verilir.

Yönlendiriciler tarafından gerçekleştirilen çeşitli görevler, trafiği tanımlamak için ACL'lerin kullanılmasını gerektirir. Tablo, bu görevlerden bazılarını örneklerle listeler.

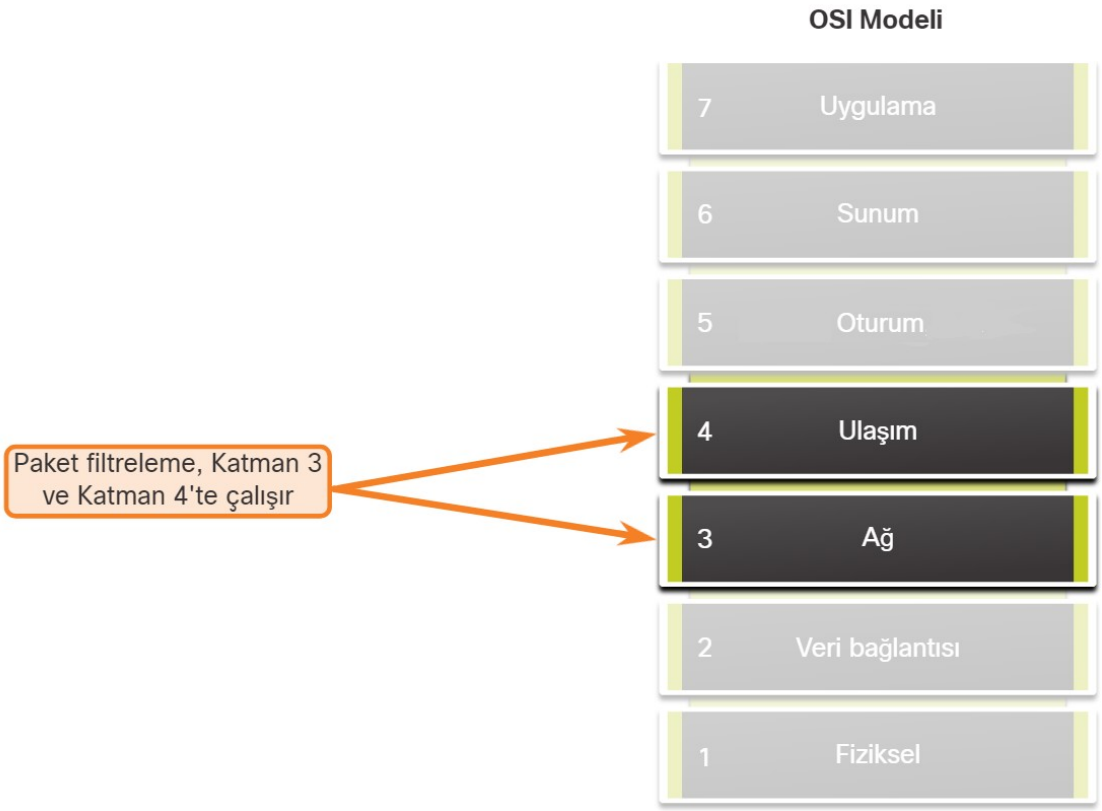
| Görev | Örnek |
|---|---|
| Ağ performansını artırmak için ağ trafiğini sınırlama | Kurumsal bir politika, ağ yükünü azaltmak için ağdaki video trafiğini yasaklar.<br><br>Video trafiğini engellemek için ACL'ler kullanılarak bir politika uygulanabilir. |
| Trafik akış kontrolü sağlama | Kurumsal bir politika, yönlendirme protokolü trafiğinin yalnızca belirli bağlantılarla sınırlandırılmasını gerektirir.<br><br>Yönlendirme güncellemelerinin dağıtımını yalnızca bilinen bir kaynaktan gelenlerle sınırlamak için ACL'ler kullanılarak bir politika uygulanabilir. |
| Ağ erişimi için temel düzeyde güvenlik sağlama | Kurumsal politika, İnsan Kaynakları ağına erişimin yalnızca yetkili kullanıcılarla sınırlandırılmasını gerektirir.<br><br>Belirtilen ağlara erişimi sınırlandırmak için ACL'ler kullanılarak bir politika zorlanabilir. |
| Trafik türüne göre trafiği filtreleme | Kurumsal politika, e-posta trafiğinin bir ağa girmesine izin verilmesini, ancak Telnet erişiminin reddedilmesini gerektirir.<br><br>Türe göre trafiği filtrelemek için EKL'ler kullanılarak bir politika uygulanabilir. |

Licensed to: ozgur@ozgurcelik.com

| Görev | Örnek |
|---|---|
| Ağ hizmetlerine erişime izin vermek veya erişimi engellemek için ana bilgisayarları tarama | Kurumsal politika, bazı dosya türlerine (örneğin, FTP veya HTTP) erişimin kullanıcı gruplarıyla sınırlı olmasını gerektirir.<br><br>Kullanıcıların hizmetlere erişimini filtrelemek için ACL'ler kullanılarak bir politika uygulanabilir. |
| Belirli ağ trafiği sınıflarına öncelik sağlama | Kurumsal trafik, herhangi bir kesintiyi önlemek için ses trafiğinin olabildiğince hızlı iletilmesini belirtir.<br><br>Ses trafiğini tanımlamak ve hemen işlemek için ACL'ler ve QoS hizmetleri kullanılarak bir politika uygulanabilir. |

### 34.1.2.Paket Filtreleme

Paket filtreleme, gelen ve / veya giden paketleri analiz ederek ve bunları ileterek veya verilen kriterlere göre bakarak bir ağa erişimi kontrol eder. Paket filtreleme, şekilde gösterildiği gibi Katman 3 veya Katman 4'te gerçekleşebilir.




Cisco yönlendiricileri iki tür ACL'yi destekler:

**Standart ACL'ler** - ACL'ler yalnızca kaynak IPv4 adresini kullanarak yalnızca Katman 3'te filtre uygular.
**Genişletilmiş ACL'ler** - ACL'ler, kaynak ve / veya hedef IPv4 adresini kullanarak Katman 3'te filtreler. Ayrıca, daha hassas kontrol için TCP, UDP bağlantı noktaları ve isteğe bağlı protokol türü bilgilerini kullanarak Katman 4'te filtreleme yapabilirler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 34.1.3.ACL İşlemi

ACL'ler, gelen arabirimlere giren paketler, yönlendirici aracılığıyla geçiş yapan paketler ve yönlendiricinin giden arabirimlerinden çıkan paketler için ek denetim sağlayan kurallar kümesini tanımlar.

ACL'ler, şekilde gösterildiği gibi gelen trafiğe (Inbound) ve giden trafiğe (Outbound) uygulanacak şekilde yapılandırılabilir.

Not : ACL'ler, yönlendiricinin kendisinden kaynaklanan paketler üzerinde etki etmez.

Bir gelen ACL, giden arayüze yönlendirilmeden önce paketleri filtreler. Gelen ACL etkilidir çünkü paket atılırsa yönlendirme aramalarının ek yükünü azaltır. Pakete ACL tarafından izin veriliyorsa, daha sonra yönlendirme için işlenir. Gelen ACL'ler, incelenmesi gereken tek paket kaynağı bir gelen arayüze bağlı ağ olduğunda paketleri filtrelemek için en iyi şekilde kullanılır.

Giden ACL, gelen arabirimden bağımsız olarak, yönlendirildikten sonra paketleri filtreler. Gelen paketler giden arayüze yönlendirilir ve ardından giden ACL üzerinden işlenir. Giden ACL'ler en iyi şekilde, aynı giden arabirimden çıkmadan önce birden çok gelen arabirimden gelen paketlere aynı filtre uygulandığında kullanılır.

Bir ACL bir arayüze uygulandığında, belirli bir işletim prosedürünü izler. Örneğin, trafik gelen standart IPv4 ACL yapılandırılmış bir yönlendirici arayüzüne girdiğinde kullanılan operasyonel adımlar burada verilmiştir.

1. Yönlendirici, kaynak IPv4 adresini paket başlığından çıkarır.
2. Yönlendirici ACL'nin üstünden başlar ve kaynak IPv4 adresini her ACE ile sıralı bir şekilde karşılaştırır.
3. Bir eşleşme yapıldığında, yönlendirici pakete izin vererek (permit) veya reddederek (deny) talimatı yerine getirir ve varsa ACL'de kalan ACE'ler analiz edilmez.
4. Kaynak IPv4 adresi ACL'deki herhangi bir ACE ile eşleşmiyorsa, tüm ACL'lere otomatik olarak uygulanan örtük bir reddetme (implicit deny) ACE'si olduğundan paket iptal edilir.

Bir ACL'nin son ACE ifadesi her zaman tüm trafiği engelleyen örtük bir reddetmedir (implicit deny). Varsayılan olarak, bu ifade, gizli olmasına ve yapılandırmada görüntülenmemesine rağmen, ACL'nin sonunda otomatik olarak bulunur.

Not : Bir ACL, en az bir izin ifadesine sahip olmalıdır, aksi takdirde tüm trafik, örtülü reddet ACE ifadesi nedeniyle reddedilecektir.

## 34.2.ACL'lerde Joker Karakter Maskeleri (Wildcard Masks)

### 34.2.1.Joker Karakter Maskesine Genel Bakış

IPv4 ACE, bir eşleşme için hangi adres bitlerinin inceleneceğini belirlemek için 32 bitlik bir joker karakter maskesi kullanır. Joker karakter maskeleri, OSPF yönlendirme protokolü tarafından da kullanılır.

Joker karakter maskesi, bir IPv4 adresindeki hangi bitlerin eşleşeceğini belirlemek için ANDing işlemini kullandığından, alt ağ maskesine benzer. Ancak, ikili 1'ler ve 0'larla eşleşme şekillerinde farklılık gösterirler. İkili 1'in eşleşmeye eşit olduğu ve ikili 0'ın eşleşme olmadığı bir alt ağ maskesinin aksine, joker karakter maskesinde bunun tersi doğrudur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Joker karakter maskeleri, ikili 1'ler ve 0'ları eşleştirmek için aşağıdaki kuralları kullanır:

Joker karakter maskesi bit 0 - Adresteki ilgili bit değerini eşleştirin
Joker karakter maskesi bit 1 - Adresteki ilgili bit değerini yoksay

Tablo, bazı joker karakter maskeleri örneklerini ve neyi tanımlayacaklarını listeler.

| Joker Karakter Maskesi | Son Sekizli (İkili) | Anlamı (0 - eşleşme, 1 - yok sayma) |
|---|---|---|
| 0.0.0.0 | 00000000 | Tüm sekizlileri eşleştir. |
| 0.0.0.63 | 00111111 | İlk üç sekizliyi eşleştirin<br><br>Son sekizlinin en soldaki iki bitini eşleştir<br><br>Son 6 biti yoksay |
| 0.0.0.15 | 00001111 | İlk üç sekizliyi eşleştirin<br><br>Son sekizlinin en soldaki dört bitini eşleştir<br><br>Son sekizlinin son 4 bitini yoksay |
| 0.0.0.252 | 11111100 | İlk üç sekizliyi eşleştirin<br><br>Son sekizlinin en fazla kalan altı bitini yoksay<br><br>Son iki biti eşleştir |
| 0.0.0.255 | 11111111 | İlk üç sekizliyi eşleştir<br><br>Son sekizliyi yok say |

**Joker Karakter Maske Türleri**

Joker karakter maskeleri kullanmak biraz pratik gerektirir. Joker karakter maskesinin bir ana bilgisayar, bir alt ağ ve bir IPv4 adres aralığı için trafiği filtrelemek üzere nasıl kullanıldığını öğrenmek için örneklere bakın.

Bir Ana Bilgisayarla Eşleşecek Joker Karakter

Bu örnekte, joker karakter maskesi belirli bir ana bilgisayar IPv4 adresiyle eşleşmek için kullanılır. ACL 10'un yalnızca IPv4 adresi 192.168.1.1 olan ana bilgisayara izin veren bir ACE'ye ihtiyacı olduğunu varsayın. "0" bir eşleşmeye eşittir ve "1" eşittir yoksay. Belirli bir ana bilgisayar IPv4 adresini eşleştirmek için, tüm sıfırlardan (yani 0.0.0.0) oluşan bir joker karakter maskesi gereklidir.

Tablo ikili olarak, ana bilgisayar IPv4 adresini, joker karakter maskesini ve izin verilen IPv4 adresini listeler.

0.0.0.0 joker maskesi, her bitin tam olarak eşleşmesi gerektiğini belirtir. Bu nedenle, ACE işlendiğinde, joker karakter maskesi yalnızca 192.168.1.1 adresine izin verecektir. ACL 10'da ortaya çıkan ACE, **access-list 10 permit 192.168.1.1** olacaktır.

| | Ondalık | İkili |
|---|---|---|
| IPv4 adresi | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Joker Karakter Maskesi | 0.0.0.0 | 00000000.00000000.00000000.00000000 |
| **İzin Verilen IPv4 Adresi** | **192.168.1.1** | 11000000.10101000.00000001.00000001 |

Licensed to yetkin karasungur ( yetkinsing@gmail.com )

IPv4 Alt Ağıyla Eşleşen Joker Karakter Maskesi

Bu örnekte, ACL 10'un 192.168.1.0/24 ağındaki tüm ana bilgisayarlara izin veren bir ACE'ye ihtiyacı vardır. Joker karakter maskesi 0.0.0.255, ilk üç sekizlinin tam olarak eşleşmesi gerektiğini, ancak dördüncü sekizlinin eşleşmediğini belirtir.

Tablo ikili olarak, ana bilgisayar IPv4 adresini, joker karakter maskesini ve izin verilen IPv4 adreslerini listeler.

İşlendiğinde, 0.0.0.255 joker maskesi, 192.168.1.0/24 ağındaki tüm ana bilgisayarlara izin verir. ACL 10'da ortaya çıkan ACE, **access-list 10 permit 192.168.1.0 0.0.0.255** olacaktır.

| | Ondalık | İkili |
|---|---|---|
| IPv4 adresi | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Joker Karakter Maskesi | 0.0.0.255 | 00000000.00000000.00000000.11111111 |
| **İzin Verilen IPv4 Adresi** | **192.168.1.0/24** | 11000000.10101000.00000001.00000000 |

IPv4 Adres Aralığı ile Eşleşen Joker Karakter Maskesi

Bu örnekte ACL 10, 192.168.16.0/24, 192.168.17.0/24,…, 192.168.31.0/24 ağlarındaki tüm ana bilgisayarlara izin veren bir ACE'ye ihtiyaç duyar. Joker karakter maskesi 0.0.15.255, bu adres aralığını doğru şekilde filtreleyecektir.

Tablo ikili olarak ana bilgisayar IPv4 adresini, joker karakter maskesini ve izin verilen IPv4 adreslerini listeler.

Vurgulanan joker karakter maskesi bitleri, IPv4 adresinin hangi bitlerinin eşleşmesi gerektiğini tanımlar. İşlendiğinde, joker karakter maskesi 0.0.15.255, 192.168.16.0/24 ile 192.168.31.0/24 ağlarındaki tüm ana bilgisayarlara izin verir. ACL 10'da ortaya çıkan ACE, **access-list 10 permit 192.168.16.0 0.0.15.255** olacaktır.

| | Ondalık | İkili |
|---|---|---|
| IPv4 adresi | 192.168.16.0 | 11000000.10101000.00010000.00000000 |
| Joker Karakter Maskesi | 0.0.15.255 | 00000000.00000000.00001111.11111111 |
| **İzin Verilen IPv4 Adresi** | **192.168.16.0/24 - 192.168.31.0/24** | 11000000.10101000.00010000.00000000<br>11000000.10101000.00011111.00000000 |

**Joker Karakter Maskesi Hesaplaması**

Joker karakter maskelerini hesaplamak zor olabilir. Bir kısayol yöntemi, alt ağ maskesini 255.255.255.255'ten çıkarmaktır. Alt ağ maskesini kullanarak joker karakter maskesinin nasıl hesaplanacağını öğrenmek için örneklere bakın.

Örnek 1

ACL 10'da 192.168.3.0/24 ağındaki tüm kullanıcılara erişime izin vermek için bir ACE istediğinizi varsayalım. Joker karakter maskesini hesaplamak için, tabloda gösterildiği gibi 255.255.255.255'ten alt ağ maskesini (yani 255.255.255.0) çıkarın.

Çözüm, 0.0.0.255 joker karakter maskesini üretir. Bu nedenle, ACE **access-list 10 permit 192.168.3.0 0.0.0.255** olacaktır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| | |
|---|---|
| Başlangıç değeri | 255.255.255.255 |
| Alt ağ maskesini çıkarın | - 255.255.255. 0 |
| **Ortaya çıkan joker karakter maskesi** | 0. 0. 0.255 |

Örnek 2

Bu örnekte, ACL 10'daki bir ACE'nin 192.168.3.32/28 alt ağındaki 14 kullanıcı için ağ erişimine izin vermesini istediğinizi varsayalım. Tabloda gösterildiği gibi 255.255.255.255'ten alt ağı (yani 255.255.255.240) çıkarın.

Bu çözüm, 0.0.0.15 joker karakter maskesini üretir. Bu nedenle, ACE **access-list 10 permit 192.168.3.32 0.0.0.15** olacaktır.

| | |
|---|---|
| Başlangıç değeri | 255.255.255.255 |
| Alt ağ maskesini çıkarın | - 255.255.255.240 |
| **Ortaya çıkan joker karakter maskesi** | 0. 0. 0. 15 |

Örnek 3

Bu örnekte, yalnızca 192.168.10.0 ve 192.168.11.0 ağlarına izin vermek için ACL 10'da bir ACE'ye ihtiyacınız olduğunu varsayın. Bu iki ağ, 255.255.254.0 alt ağ maskesi olan 192.168.10.0/23 olarak özetlenebilir. Yine, tabloda gösterildiği gibi 255.255.254.0 alt ağ maskesini 255.255.255.255'ten çıkardınız.

Bu çözüm, 0.0.1.255 joker maskesini üretir. Bu nedenle, ACE **access-list 10 permit 192.168.10.0 0.0.1.255** olacaktır.

| | |
|---|---|
| Başlangıç değeri | 255.255.255.255 |
| Alt ağ maskesini çıkarın | - 255.255.254. 0 |
| **Ortaya çıkan joker karakter maskesi** | 0. 0. 1.255 |

Örnek 4

192.168.16.0/24 ile 192.168.31.0/24 arasındaki ağları eşleştirmek için ACL numarası 10'a ihtiyacınız olan bir örneği düşünün. Bu ağ aralığı, 255.255.240.0'ın bir alt ağ maskesi olan 192.168.16.0/20 olarak özetlenebilir. Bu nedenle, tabloda gösterildiği gibi 255.255.240.0 alt ağ maskesini 255.255.255.255'ten çıkarın.

Bu çözüm, 0.0.15.255 joker maskesini üretir. Bu nedenle, ACE **access-list 10 permit 192.168.16.0 0.0.15.255** olacaktır.

| | |
|---|---|
| Başlangıç değeri | 255.255.255.255 |
| Alt ağ maskesini çıkarın | - 255.255.240. 0 |
| **Ortaya çıkan joker karakter maskesi** | 0. 0. 15.255 |

**Joker Karakter Maskesi Anahtar Kelimeleri**

İkili joker karakter maskesi bitlerinin ondalık gösterimiyle çalışmak sıkıcı olabilir. Bu görevi basitleştirmek için Cisco IOS, joker karakter maskelemesinin en yaygın kullanımlarını tanımlamak için iki anahtar sözcük sağlar. Anahtar sözcükler ACL tuş vuruşlarını azaltır ve ACE'yi okumayı kolaylaştırır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

İki anahtar kelime şunlardır:

- **host** - Bu anahtar kelime 0.0.0.0 maskesinin yerini alır. Bu maske, yalnızca bir ana bilgisayar adresini filtrelemek için tüm IPv4 adres bitlerinin eşleşmesi gerektiğini belirtir.
- **any** - Bu anahtar sözcük 255.255.255.255 maskesinin yerini alır. Bu maske, tüm IPv4 adresini yok saymayı veya herhangi bir adresi kabul etmeyi söyler.

Örneğin, komut çıkışında iki ACL yapılandırılır. ACL 10 ACE yalnızca 192.168.10.10 ana bilgisayarına izin verir ve ACL 11 ACE tüm ana bilgisayarlara izin verir.

```
R1(config)# access-list 10 permit 192.168.10.10  0.0.0.0
R1(config)# access-list 11 permit  0.0.0.0 255.255.255.255
R1(config)#
```

Alternatif olarak, host ve any  anahtar sözcükleri vurgulanan çıktının yerini almak için kullanılabilirdi.

Aşağıdaki komutlar, önceki komutlarla aynı görevi gerçekleştirir.

```
R1(config)# access-list 10 permit  host  192.168.10.10
R1(config)# access-list 11 permit  any
R1(config)#
```

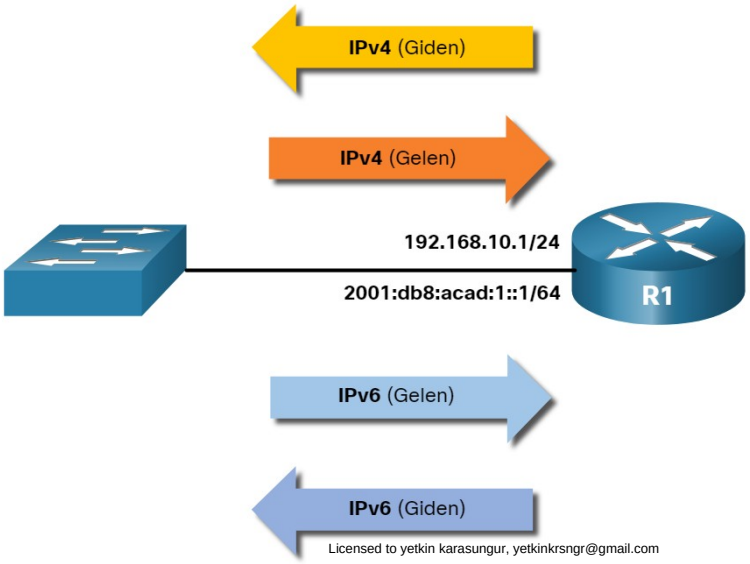
## 34.3.ACL Oluşturma Yönergeleri

### 34.3.1.Arayüz Başına Sınırlı ACL Sayısı

Bir yönlendirici arayüzüne uygulanabilecek ACL sayısında bir sınır vardır. Örneğin, çift yığınlı (yani IPv4 ve IPv6) bir yönlendirici arabiriminde, şekilde gösterildiği gibi dört adede kadar ACL uygulanabilir.

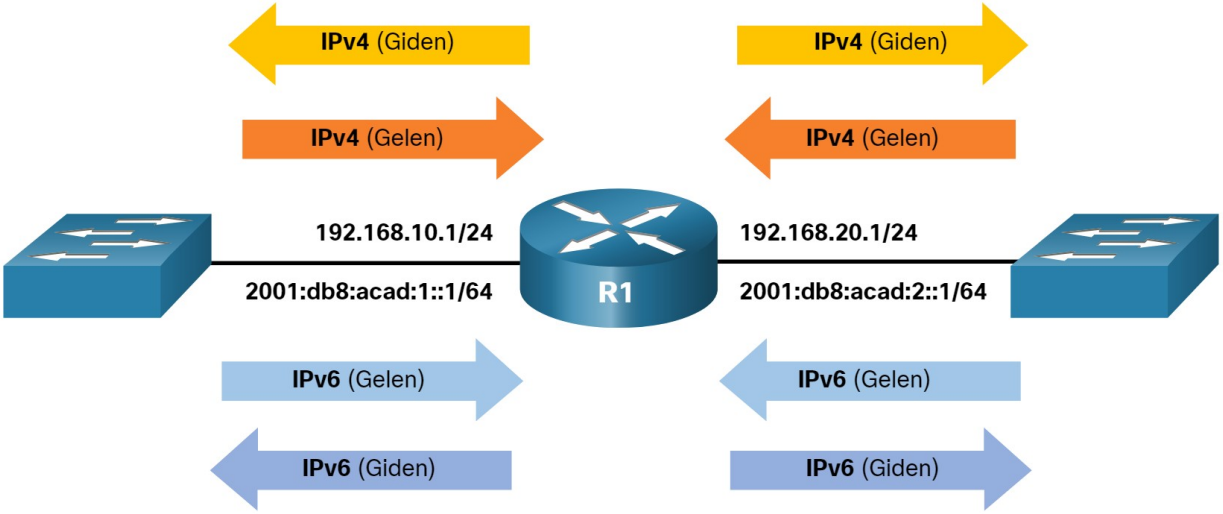
Özellikle, bir yönlendirici arayüzünde şunlar olabilir:

- bir giden IPv4 ACL
- bir gelen IPv4 ACL
- bir gelen IPv6 ACL
- bir giden IPv6 ACL



R1'in gelen ve giden IPv4 ve IPv6 ACL'leri uygulanmasını gerektiren iki çift yığınlı arabirime sahip olduğunu varsayın. Şekilde gösterildiği gibi, R1 arabirimlere yapılandırılmış ve uygulanmış en fazla 8 ACL'ye sahip olabilir. Her arayüzün dört ACL'si olacaktır; IPv4 için iki ACL ve IPv6 için iki ACL. Her protokol için, bir ACL gelen trafik ve diğeri giden trafik içindir.

Not : ACL'lerin her iki yönde de yapılandırılması gerekmez. ACL'lerin sayısı ve arayüze uygulanan yönü, kuruluşun güvenlik politikasına bağlı olacaktır.




## 34.3.2.En İyi ACL Uygulamaları

ACL'leri kullanmak, ayrıntılara dikkat ve büyük özen gerektirir. Hatalar kesinti süresi, sorun giderme çabaları ve zayıf ağ hizmeti açısından maliyetli olabilir. ACL'yi yapılandırmadan önce temel planlama gereklidir.

Tablo, ACL en iyi uygulamalar listesinin temelini oluşturan yönergeleri sunar.

| Yönerge | Yarar |
|---|---|
| ACL'leri kurumsal güvenlik politikalarına dayandırın. | Bu, kurumsal güvenlik yönergelerini uygulamanızı sağlayacaktır. |
| ACL'nin ne yapmasını istediğinizi yazın. | Bu, yanlışlıkla potansiyel erişim sorunları oluşturmaktan kaçınmanıza yardımcı olacaktır. |
| Tüm ACL'lerinizi oluşturmak, düzenlemek ve kaydetmek için bir metin düzenleyici kullanın. | Bu, yeniden kullanılabilir ACL'lerden oluşan bir kitaplık oluşturmanıza yardımcı olacaktır. |
| Remark komutunu kullanarak ACL'leri belgeleyin. | Bu sizin (ve diğerlerinin) bir ACE'nin amacını anlamanıza yardımcı olacaktır. |
| ACL'leri bir üretim ağında uygulamadan önce bir geliştirme ağında test edin. | Bu, maliyetli hatalardan kaçınmanıza yardımcı olacaktır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 34.4.IPv4 ACL Türleri

### 34.4.1.Standart ve Genişletilmiş ACL'ler

İki tür IPv4 ACL vardır:

- Standart ACL'ler - Bunlar paketlere yalnızca kaynak IPv4 adresini temel alarak izin verir veya reddeder.
- Genişletilmiş ACL'ler - Bunlar, kaynak IPv4 adresi ve hedef IPv4 adresi, protokol türü, kaynak ve hedef TCP veya UDP bağlantı noktaları ve daha fazlasına dayalı olarak paketlere izin verir veya reddeder.

Örneğin, aşağıdaki standart ALC komutuna bakın.

```
R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255
R1(config)#
```

ACL 10, 192.168.10.0/24 kaynak ağındaki ana bilgisayarlara izin verir. Sonunda "herhangi birini reddet" ifadesi nedeniyle, 192.168.10.0/24 ağından gelen trafik dışındaki tüm trafik bu ACL ile engellenir.

Sonraki örnekte, genişletilmiş ACL 100, hedef ana bilgisayar bağlantı noktası 80 (HTTP) ise, 192.168.10.0/24 ağındaki herhangi bir ana bilgisayardan herhangi bir IPv4 ağına giden trafiğe izin verir.

```
R1(config)# access-list 100 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)#
```

Standart ACL 10'un, genişletilmiş ACL 100 kaynağı ve hedef Katman 3 ve Katman 4 protokolü (yani, TCP) bilgilerini filtrelerken yalnızca kaynak adresine göre nasıl filtreleme yapabildiğine dikkat edin.

### 34.4.2.Numaralı ve Adlandırılmış ACL'ler

#### Numaralı ACL'ler

Resimde gösterildiği gibi, 1 ila 99 veya 1300 ila 1999 numaralı ACL'ler standart ACL'lerdir; 100 ila 199 veya 2000 ila 2699 numaralı ACL'ler, genişletilmiş ACL'lerdir.

```
R1(config)# access-list ?
  <1-99>       IP standard access list
  <100-199>    IP extended access list
  <1100-1199>  Extended 48-bit MAC address access list
  <1300-1999>  IP standard access list (expanded range)
  <200-299>    Protocol type-code access list
  <2000-2699>  IP extended access list (expanded range)
  <700-799>    48-bit MAC address access list
  rate-limit   Simple rate-limit specific access list
  template     Enable IP template acls
Router(config)# access-list
```

#### Adlandırılmış ACL'ler

ACL'leri yapılandırırken kullanmak için tercih edilen bir başka yöntem, adlandırılmış ACL'lerdir. Özellikle, standart ve genişletilmiş ACL'ler, ACL'nin amacı hakkında bilgi sağlamak için adlandırılabilir. Örneğin, genişletilmiş bir ACL FTP-FILTER adını vermek, numaralandırılmış bir ACL 100'e sahip olmaktan çok daha iyidir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aşağıdaki örnekte gösterildiği gibi **ip access-list** küresel yapılandırma komutu, adlandırılmış ACL oluşturmak için kullanılır.

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

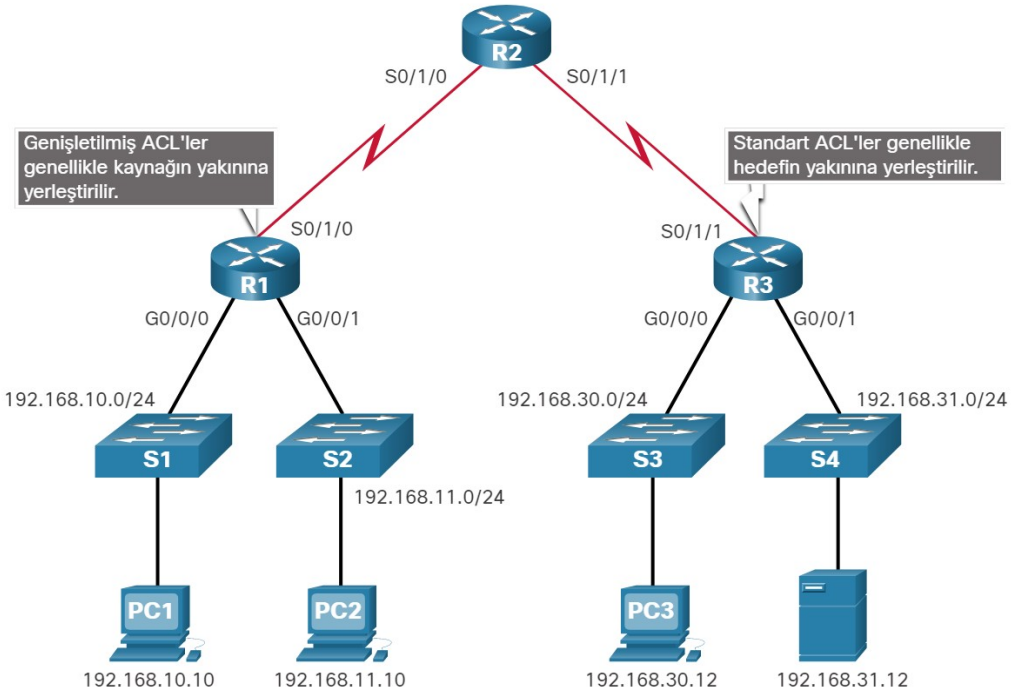
Aşağıda, adlandırılmış ACL'ler için izlenecek kurallar özetlenmektedir.

- ACL'nin amacını tanımlamak için bir ad atayın.
- İsimler alfanümerik karakterler içerebilir.
- İsimler boşluk veya noktalama işareti içeremez.
- İsmin BÜYÜK HARFLERLE yazılması önerilir.
- Girişler ACL içinde eklenebilir veya silinebilir.

## 34.4.3.ACL'leri Nereye Yerleştirmelisiniz?

Her ACL, verimlilik üzerinde en büyük etkiye sahip olduğu yere yerleştirilmelidir.

Şekil, standart ve genişletilmiş ACL'lerin bir kurumsal ağda nerede konumlandırılması gerektiğini göstermektedir. 192.168.10.0/24 ağından kaynaklanan trafiğin 192.168.30.0/24 ağına ulaşmasını engellemeyi hedefleyin.




Genişletilmiş ACL'ler, filtrelenecek trafiğin kaynağına mümkün olduğunca yakın yerleştirilmelidir. Bu şekilde, istenmeyen trafik, ağ altyapısını geçmeden kaynak ağın yakınında reddedilir.

Standart ACL'ler hedefe mümkün olduğunca yakın yerleştirilmelidir. Trafiğin kaynağına standart bir ACL yerleştirildiyse, trafiğin nereye gittiğine bakılmaksızın verilen kaynak adresine göre "izin verme-permit" veya "reddetme-deny" gerçekleşecektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

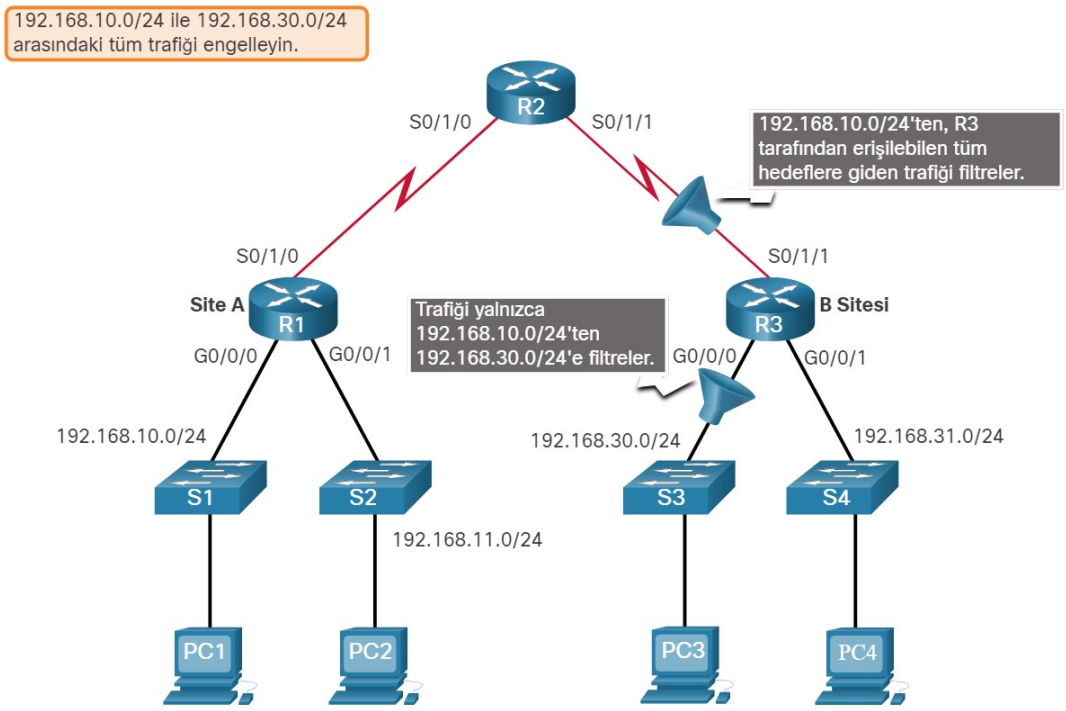
ACL'nin yerleştirilmesi ve dolayısıyla kullanılan ACL'nin türü de tabloda listelendiği gibi çeşitli faktörlere bağlı olabilir.

| ACL Yerleşimini Etkileyen Faktörler | Açıklama |
|---|---|
| Organizasyonel kontrolün kapsamı | ACL'nin yerleştirilmesi, kuruluşun hem kaynak hem de hedef ağları kontrol edip etmediğine bağlı olabilir. |
| İlgili ağların bant genişliği | Bant genişliği tüketen trafiğin iletimini önlemek için kaynaktaki istenmeyen trafiği filtrelemek istenebilir. |
| Yapılandırma kolaylığı | Hedefte bir ACL uygulamak daha kolay olabilir, ancak trafik bant genişliğini gereksiz yere kullanacaktır.<br><br>Trafiğin kaynaklandığı her yönlendiricide genişletilmiş bir ACL kullanılabilir. Bu, kaynaktaki trafiği filtreleyerek bant genişliğinden tasarruf sağlar, ancak birden çok yönlendiricide genişletilmiş ACL'ler oluşturmayı gerektirir. |

**Standart ACL Yerleştirme Örneği**

ACL yerleştirme yönergelerini izleyerek, standart ACL'ler hedefe mümkün olduğunca yakın yerleştirilmelidir.

Şekilde yönetici, 192.168.10.0/24 ağından kaynaklanan trafiğin 192.168.30.0/24 ağına ulaşmasını engellemek istemektedir.




Temel yerleştirme yönergelerini izleyerek, yönetici, yönlendirici R3'e standart bir ACL yerleştirir. Standart ACL'yi uygulamak için R3'te iki olası arayüz vardır:

- R3 S0/1/1 arayüzü (gelen) - Standart ACL, .10 ağından gelen trafiği reddetmek için R3 S0 / 1/1 arayüzünde gelen olarak uygulanabilir. Ancak, 192.168.31.0/24 (bu örnekte .31) ağına .10 trafiğini de filtreleyecektir. Bu nedenle, standart ACL bu arayüze uygulanmamalıdır.
- R3 G0 / 0 arayüzü (giden) - Standart ACL, R3 G0 / 0/0 arayüzünde giden olarak uygulanabilir. Bu, R3 tarafından erişilebilen diğer ağları etkilemeyecektir. .10 ağından gelen paketler hala .31 ağına erişebilecektir. Bu, standart ACL'yi trafik gereksinimlerini karşılayacak şekilde yerleştirmek için en iyi arabirimdir.

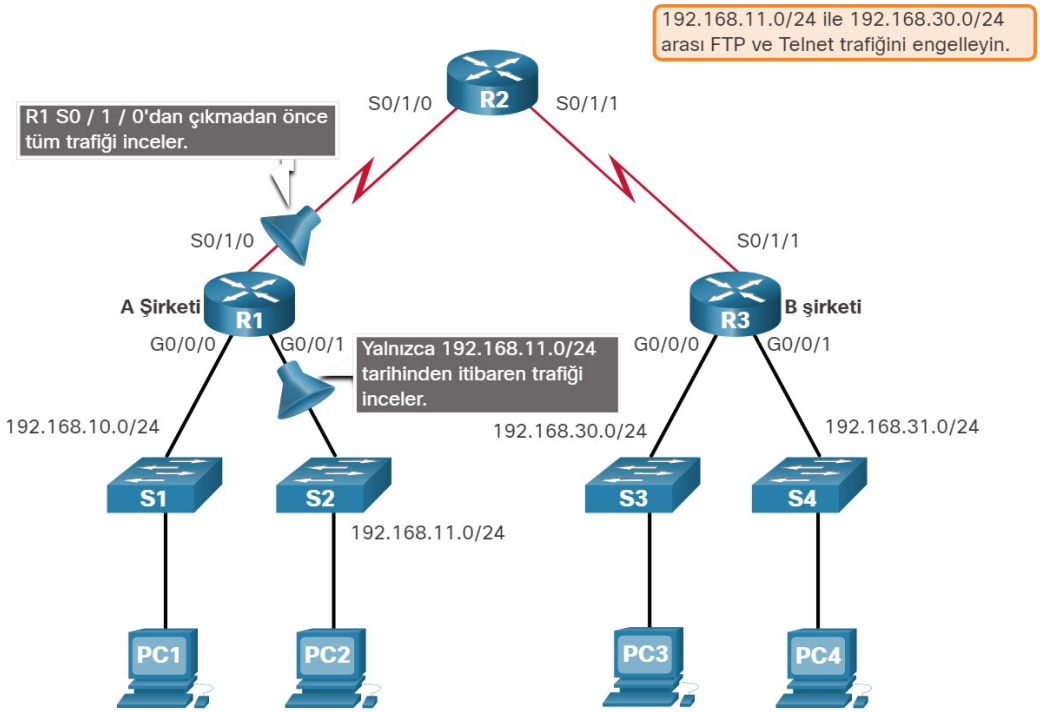
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Genişletilmiş ACL Yerleştirme Örneği**

Genişletilmiş ACL, kaynağa mümkün olduğunca yakın yerleştirilmelidir. Bu, istenmeyen trafiğin birden çok ağ üzerinden gönderilmesini, yalnızca hedefine ulaştığında reddedilmesini önler.

Ancak, kuruluş ACL'leri yalnızca kontrol ettikleri cihazlara yerleştirebilir. Bu nedenle, genişletilmiş EKL yerleşimi, organizasyonel kontrolün nereye yayıldığı bağlamında belirlenmelidir.

Şekilde, örneğin, Şirket A, diğer tüm trafiğe izin verirken, B Şirketinin 192.168.30.0/24 ağından 192.168.11.0/24 ağına Telnet ve FTP trafiğini reddetmek istemektedir.




Bu hedeflere ulaşmanın birkaç yolu vardır. R3 üzerinde genişletilmiş bir ACL görevi yerine getirir, ancak yönetici R3'ü kontrol etmez. Ayrıca bu çözüm, istenmeyen trafiğin tüm ağı geçmesine ve yalnızca hedefte engellenmesine izin verir. Bu, genel ağ verimliliğini etkiler.

Çözüm, hem kaynak hem de hedef adresleri belirten genişletilmiş bir ACL'yi R1'e yerleştirmektir.

Genişletilmiş ACL'yi uygulamak için R1'de iki olası arabirim vardır:

- R1 S0/1/0 arayüzü (giden) - Genişletilmiş ACL, S0 / 1/0 arayüzünde giden uygulanabilir. Ancak bu çözüm, 192.168.10.0/24 tarihli paketler de dahil olmak üzere R1'den çıkan tüm paketleri işleyecektir.
- R1 G0/0/1 arabirimi (gelen) - Genişletilmiş ACL, G0 / 0 / 1'de gelen olarak uygulanabilir ve yalnızca 192.168.11.0/24 ağından gelen paketler, R1'de ACL işlemeye tabidir. Filtrenin yalnızca 192.168.11.0/24 ağını terk eden paketlerle sınırlı olması gerektiğinden, genişletilmiş ACL'yi G0 / 1'e uygulamak en iyi çözümdür.

## 34.5.Standart IPv4 ACL'leri Yapılandırma

### 34.5.1.ACL Oluşturma

Tüm erişim kontrol listeleri (ACL'ler) planlanmalıdır. Ancak, bu özellikle birden çok erişim denetimi girişi (ACE) gerektiren ACL'ler için geçerlidir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Karmaşık bir ACL'yi yapılandırırken şunları yapmanız önerilir:

- Bir metin düzenleyici kullanın ve uygulanacak politikanın özelliklerini yazın.
- Bu görevleri gerçekleştirmek için IOS yapılandırma komutlarını ekleyin.
- ACL'yi belgelemek için açıklamalar (remark) ekleyin.
- Komutları kopyalayıp cihaza yapıştırın.
- İstenen politikayı doğru şekilde uyguladığından emin olmak için her zaman bir ACL'yi iyice test edin.

Bu öneriler, ağdaki trafiği etkilemeden ACL'yi dikkatlice oluşturmanıza olanak sağlar.

### 34.5.2.Numaralandırılmış Standart IPv4 ACL Sözdizimi

Numaralandırılmış bir standart ACL oluşturmak için aşağıdaki genel yapılandırma komutunu kullanın:

```
Router(config)# access-list access-list-number {deny | permit | remark text} source [source-wildcard]
[log]
```

Numaralandırılmış standart ACL'yi kaldırmak için **no access-list** *access-list-number* global genel yapılandırma komutunu kullanın.

Tablo, standart bir ACL için söz diziminin ayrıntılı bir açıklamasını sağlar.

| Parametre | Açıklama |
|---|---|
| *access-list-number*<br><br>*erişim listesi numarası* | Bu, ACL'nin ondalık sayısıdır.<br><br>Standart ACL numarası aralığı 1 ila 99 veya 1300 ila 1999'dur. |
| deny-reddetmek | Bu, koşul eşleşirse erişimi reddeder. |
| permit-izin | Bu, koşul eşleşirse erişime izin verir. |
| remark *text*<br><br>Açıklama *metin* | (İsteğe bağlı) Bu, dokümantasyon amaçlı bir metin girişi ekler.<br><br>Her açıklama 100 karakterle sınırlıdır. |
| *source*<br>*kaynak* | Bu, filtrelenecek kaynak ağı veya ana bilgisayar adresini tanımlar.<br><br>Tüm ağları belirtmek için herhangi bir anahtar sözcüğü kullanın.<br><br>Host *ip-address* anahtar sözcüğünü kullanın veya belirli bir IP adresini tanımlamak için bir *ip-adresi* (host anahtar sözcüğü olmadan)girin. |
| *source-wildcard*<br><br>*kaynak-joker karakter* | (İsteğe bağlı) Bu, *kaynağa* uygulanan 32 bitlik bir joker karakter maskesidir . Atlanırsa, varsayılan bir 0.0.0.0 maskesi varsayılır. |
| log<br>günlük | (İsteğe bağlı) Bu anahtar kelime, ACE eşleştiğinde bir bilgi mesajı oluşturur ve gönderir.<br><br>Mesaj ACL numarasını, eşleşen koşulu (yani, izin verildi veya reddedildi), kaynak adresini ve paket sayısını içerir.<br><br>Bu mesaj ilk eşleşen paket için oluşturulur.<br><br>Bu anahtar kelime yalnızca sorun giderme veya güvenlik nedenleriyle uygulanmalıdır. |

### 34.5.3.Adlandırılmış Standart IPv4 ACL Sözdizimi

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

ACL'yi adlandırmak, işlevini anlamayı kolaylaştırır. Adlandırılmış bir standart ACL oluşturmak için aşağıdaki genel yapılandırma komutunu kullanın:

```
Router(config)# ip access-list standard access-list-name
```

Bu komut, ACL ACE'lerini yapılandırdığınız adlandırılmış standart yapılandırma moduna girer.

ACL adları alfasayısaldır, büyük / küçük harfe duyarlıdır ve benzersiz olmalıdır. ACL adlarının büyük harfle yazılması gerekli değildir, ancak çalışan yapılandırma çıktısını görüntülerken bunların öne çıkmasını sağlar. Ayrıca, yanlışlıkla aynı ada sahip ancak farklı büyük harf kullanımlarıyla iki farklı ACL oluşturma olasılığınızı azaltır.

Not : Adlandırılmış bir standart IPv4 ACL'yi kaldırmak için **no ip access-list standard** genel yapılandırma komutunu kullanın.

Örnekte, NO-ACCESS adlı standart bir IPv4 ACL oluşturulmuştur. İstemin adlandırılmış standart ACL yapılandırma moduna değiştiğine dikkat edin. ACE ifadeleri, adlandırılmış standart ACL alt yapılandırma modunda girilir. Adlandırılmış tüm standart ACL ACE seçeneklerini görüntülemek için yardım özelliğini kullanın.

Vurgulanan üç seçenek, numaralandırılmış standart ACL'ye benzer şekilde yapılandırılır. Numaralandırılmış ACL yönteminden farklı olarak, her ACE için ilk **ip access-list** komutunu tekrar etmeye gerek yoktur .

```
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# ?
Standard Access List configuration commands:
  <1-2147483647>  Sequence Number
  default         Set a command to its defaults
  deny            Specify packets to reject
  exit            Exit from access-list configuration mode
  no              Negate a command or set its defaults
  permit          Specify packets to forward
  remark          Access list entry comment
R1(config-std-nacl)#
```

### Standart IPv4 ACL'nin Uygulanması

Standart bir IPv4 ACL yapılandırıldıktan sonra, bir arayüze veya özelliğe bağlanması gerekir. Aşağıdaki komut, numaralandırılmış veya adlandırılmış bir standart IPv4 ACL'yi bir arabirime bağlamak için kullanılabilir:

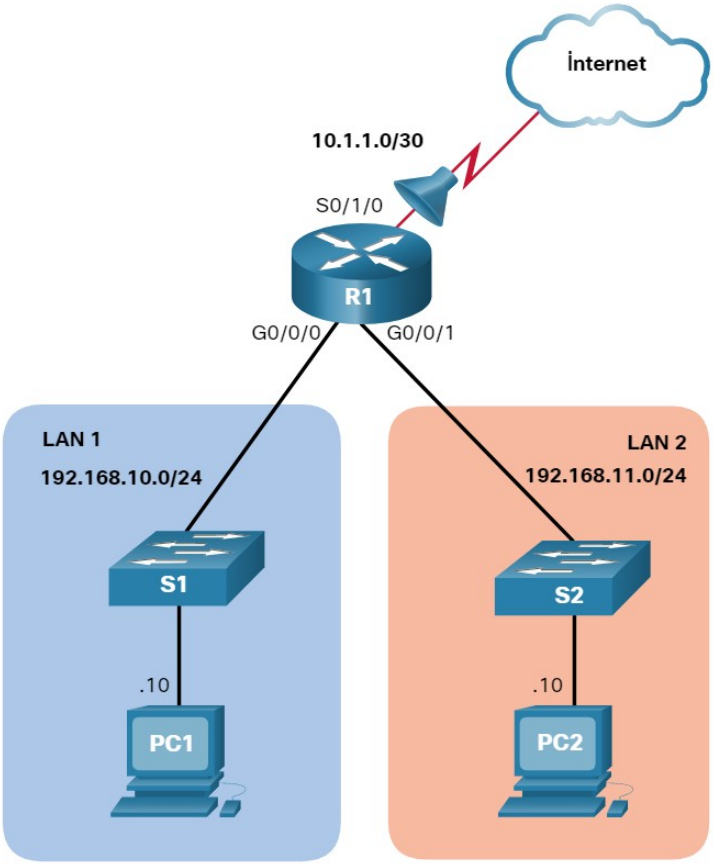
```
Router(config-if) # ip access-group {access-list-number | access-list-name} {in | out}
```

Bir ACL'yi arabirimden kaldırmak için, önce **no ip access-group** yapılandırma komutunu girin. Ancak, ACL yine de yönlendiricide yapılandırılacaktır. ACL'yi yönlendiriciden kaldırmak için **no access-list** genel yapılandırma komutunu kullanın.

### Numaralandırılmış Standart IPv4 ACL Örneği

Şekildeki topoloji, numaralandırılmış ve adlandırılmış standart IPv4 ACL'leri bir arabirime yapılandırmayı ve uygulamayı göstermek için kullanılacaktır. Bu ilk örnek, numaralandırılmış bir standart IPv4 ACL uygulamasını gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Yalnızca PC1'in internete çıkmasına izin verildiğini varsayın. Bu politikayı etkinleştirmek için, şekilde gösterildiği gibi S0/1 0'a standart bir ACL ACE uygulanabilir.

```
R1(config)# access-list 10 remark ACE permits ONLY host 192.168.10.10 to the internet
R1(config)# access-list 10 permit host 192.168.10.10
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
R1(config)#
```

Show access-list komutunun çıktısının remark-açıklama ifadelerini göstermediğine dikkat edin . ACL açıklamaları, çalışan yapılandırma dosyasında görüntülenir. ACL'yi etkinleştirmek için açıklama komutu gerekmese de, dokümantasyon amacıyla şiddetle tavsiye edilir.

Şimdi yeni bir ağ politikasının LAN 2'deki ana bilgisayarlara internete de izin verilmesi gerektiğini belirttiğini varsayalım. Bu politikayı etkinleştirmek için, çıktıda gösterildiği gibi ACL 10'a ikinci bir standart ACL ACE eklenebilir.

```
R1(config)# access-list 10 remark ACE permits all host in LAN 2
R1(config)# access-list 10 permit 192.168.20.0 0.0.0.255
R1(config)# do show access-lists
Standard IP access list 10
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1(config)#
```

ACL 10  Seri 0/1/0 arayüzüne gide yönde (outbound) uygulayın.

Mustafa Duyduk Kadıköy Bilgisayar Mühendisi mustafaduyduk@gmail.com

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group 10 out
R1(config-if)# end
R1#
```

Sonuçta ortaya çıkan ACL 10 politikası, yalnızca 192.168.10.10 ana bilgisayarına ve LAN 2'den gelen tüm ana makinelerin Seri 0/1/0 arayüzünden çıkmasına izin verecektir. 192.168.10.0 ağındaki diğer tüm ana bilgisayarların internete girmesine izin verilmeyecektir.

Çıktıda gösterildiği gibi yapılandırmadaki ACL'yi incelemek için show running-config komutunu kullanın.

```
R1# show run | section access-list
access-list 10 remark ACE permits host 192.168.10.10
access-list 10 permit 192.168.10.10
access-list 10 remark ACE permits all host in LAN 2
access-list 10 permit 192.168.20.0 0.0.0.255
R1#
```

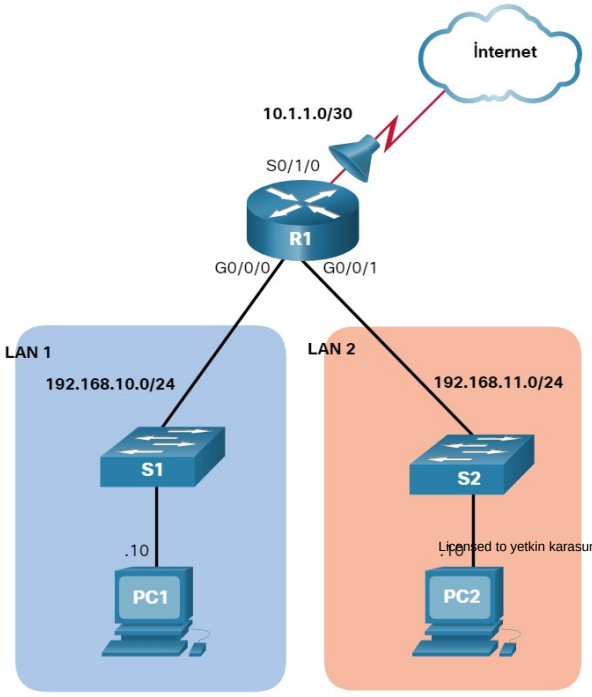
Remark-Açıklama ifadelerinin de nasıl görüntülendiğine dikkat edin .

Son olarak, bir arabirime ACL uygulanmış olup olmadığını doğrulamak için **show ip interface** komutunu kullanın. Örnek çıktıda, çıktı özellikle "erişim listesi" metnini içeren satırlar için Seri 0/1/0 arayüzüne bakmaktadır.

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is 10
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

## Adlandırılmış Standart IPv4 ACL Örneği

Bu ikinci örnek, adlandırılmış bir standart IPv4 ACL uygulamasını gösterir. Size kolaylık sağlamak için şekilde topoloji tekrar edilmiştir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yalnızca PC1'in internete çıkmasına izin verildiğini varsayın. Bu politikayı etkinleştirmek için, S0/1/0'da giden için PERMIT-ACCESS adlı bir adlandırılmış standart ACL uygulanabilir.

Önceden yapılandırılmış ACL 10'u kaldırın ve burada gösterildiği gibi PERMIT-ACCESS adlı bir adlandırılmış standart ACL oluşturun.

```
R1(config)# no access-list 10
R1(config)# ip access-list standard PERMIT-ACCESS
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)#
```

Şimdi yalnızca 192.168.10.10 ana bilgisayarına izin veren bir ACE ve tüm LAN 2 ana bilgisayarlarının internete girmesine izin veren başka bir ACE ekleyin.

```
R1(config-std-nacl)# remark ACE permits host 192.168.10.10
R1(config-std-nacl)# permit host 192.168.10.10
R1(config-std-nacl)# remark ACE permits all hosts in LAN 2
R1(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
```

Yeni adlandırılmış ACL giden bağlantısını Seri 0/1/0 arayüzüne uygulayın.

```
R1(config)# interface Serial 0/1/0
R1(config-if)# ip access-group PERMIT-ACCESS out
R1(config-if)# end
R1#
```

Çıktıda gösterildiği gibi yapılandırmadaki ACL'yi gözden geçirmek için **show access-list** ve **show running-config** komutunu kullanın.

```
R1# show access-lists
Standard IP access list PERMIT-ACCESS
    10 permit 192.168.10.10
    20 permit 192.168.20.0, wildcard bits 0.0.0.255
R1# show run | section ip access-list
ip access-list standard PERMIT-ACCESS
 remark ACE permits host 192.168.10.10
 permit 192.168.10.10
 remark ACE permits all hosts in LAN 2
 permit 192.168.20.0 0.0.0.255
R1#
```

Son olarak, bir arabirime ACL uygulanmış olup olmadığını doğrulamak için show ip interface komutunu kullanın. Örnek çıktıda, çıktı özellikle "erişim listesi" metnini içeren satırlar için Seri 0/1/0 arayüzüne bakmaktadır.

```
R1# show ip int Serial 0/1/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is PERMIT-ACCESS
  Inbound Common access list is not set
  Inbound  access list is not set
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 34.6.IPv4 ACL'leri Düzenleme

### 34.6.1.ACL'yi Değiştirmek için İki Yöntem

Bir ACL yapılandırıldıktan sonra değiştirilmesi gerekebilir. Birden çok ACE'ye sahip ACL'lerin yapılandırılması karmaşık olabilir. Bazen yapılandırılmış ACE beklenen davranışları vermez. Bu nedenlerle, ACL'ler istenen filtreleme sonucunu elde etmek için başlangıçta biraz deneme yanılma gerektirebilir.

Bu bölümde, bir ACL'yi değiştirirken kullanılacak iki yöntem açıklanacaktır:

- Bir Metin Düzenleyici Kullanın
- Sıra Numaralarını Kullanın

**Metin Düzenleyici Yöntemi**

Birden çok ACE'ye sahip ACL'ler bir metin düzenleyicide oluşturulmalıdır. Bu, gerekli ACE'leri planlamanıza, ACL'yi oluşturmanıza ve ardından bunu yönlendirici arayüzüne yapıştırmanıza olanak tanır. Ayrıca bir ACL'yi düzenleme ve düzeltme görevlerini de basitleştirir.

Örneğin , çalışan yapılandırmada gösterildiği gibi, ACL 1'in ilk sekizli için 192 yerine 19 kullanılarak yanlış girildiğini varsayın .

```
R1# show run | section access-list access-list 1 deny 192.168.10.10 access-list 1 permit 192.168.10.0
0.0.0.255
R1#
```

Örnekte, ilk ACE'nin 192.168.10.10'da ana bilgisayarı reddetmesi gerekirdi. Ancak, ACE yanlış girildi.

Hatayı düzeltmek için:

- ACL'yi çalışan yapılandırmadan kopyalayın ve metin düzenleyiciye yapıştırın.
- Gerekli değişiklikleri yapın.
- Yönlendiricideki önceden yapılandırılmış ACL'yi kaldırın, aksi takdirde, düzenlenen ACL komutlarının yapıştırılması yalnızca yönlendiricideki mevcut ACL ACE'lere eklenir (yani eklenir).
- Düzenlenen ACL'yi kopyalayıp yönlendiriciye geri yapıştırın.

ACL 1'in şimdi düzeltildiğini varsayın. Bu nedenle, hatalı ACL silinmeli ve düzeltilmiş ACL 1 ifadeleri çıktıda gösterildiği gibi genel yapılandırma modunda yapıştırılmalıdır.

```
R1(config)# no access-list 1
R1(config)#
R1(config)# access-list 1 deny 192.168.10.10
R1(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R1(config)#
```

**Sıra Numaraları Yöntemi**

ACL ACE, ACL sıra numaraları kullanılarak da silinebilir veya eklenebilir. Bir ACE girildiğinde sıra numaraları otomatik olarak atanır. Bu numaralar, **show access-list** komutunda listelenir . **show running-config** komutu sıra numaralarını göstermiyor.

Önceki örnekte, ACL 1 için yanlış ACE, örnekte gösterildiği gibi sıra numarası 10'u kullanıyor.

Metin Düzenleyici Yöntemi Kullanın

```
R1# show access-lists Standard IP access list 1
    10 deny 192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

ACL'yi düzenlemek için **ip access-list standard** komutunu kullanın. Mevcut bir ifadeyle aynı sıra numarası kullanılarak ifadelerin üzerine yazılamaz. Bu nedenle, önce **no 10** komutuyla mevcut deyimin silinmesi gerekir . Daha sonra sıra numarası 10 yapılandırılarak doğru ACE eklenebilir. Örnekte gösterildiği gibi **show access-list** komutunu kullanarak değişiklikleri doğrulayın .

```
R1# conf t
R1(config)# ip access-list standard 1
R1(config-std-nacl)# no 10
R1(config-std-nacl)# 10 deny host 192.168.10.10
R1(config-std-nacl)# end
R1# show access-lists
Standard IP access list 1
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

## Adlandırılmış ACL Düzenleme Örneği

Adlandırılmış ACL'ler, ACE'leri silmek ve eklemek için sıra numaralarını da kullanabilir. ACL NO-ACCESS örneğine bakın .

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
```

192.168.10.0/24 ağından 192.168.10.5 ana bilgisayarının da reddedilmiş olması gerektiğini varsayalım. Yeni bir ACE girdiyseniz, ACL'nin sonuna eklenir. Bu nedenle, ACE 20 bu ağdaki tüm ana bilgisayarlara izin verdiği için ana bilgisayar asla reddedilmeyecektir.

Çözüm, örnekte gösterildiği gibi ACE 10 ile ACE 20 arasına, örnekte gösterildiği gibi ACE 15 gibi bir ACE reddeden ana bilgisayar 192.168.10.5 eklemektir. Ayrıca, yeni ACE'nin host anahtar sözcüğü kullanılmadan girildiğine dikkat edin . Anahtar kelime, bir hedef ana bilgisayar belirlenirken isteğe bağlıdır.

ACL'nin artık **permit** ifadesinden önce uygun şekilde eklenen yeni bir ACE 15'e sahip olduğunu doğrulamak için **show access-list** komutunu kullanın.

Sıra numarası 15'in sıra numarası 10'dan önce görüntülendiğine dikkat edin. Çıktıdaki ifadelerin sırasının, girildikleri sırayı yansıtmasını bekleyebiliriz. Bununla birlikte, IOS, özel bir karma işlevi kullanarak ana bilgisayar deyimlerini sıraya koyar. Ortaya çıkan sıra, ACL'yi önce ana bilgisayar girişlerine ve ardından ağ girişlerine göre arama yapacak şekilde optimize eder.

```
R1# configure terminal
R1(config)# ip access-list standard NO-ACCESS
R1(config-std-nacl)# 15 deny 192.168.10.5
R1(config-std-nacl)# end
R1#
R1# show access-lists
Standard IP access list NO-ACCESS
    15 deny   192.168.10.5
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

karasungur, yetkinkrsngr@gmail.com

### 34.6.2.ACL İstatistikleri

Örnekteki **show access-list** komutunun, eşleşen her deyim için istatistikleri gösterdiğine dikkat edin . NO-ACCESS ACL'deki ACE reddi 20 kez eşleştirildi ve ACE izni 64 kez eşleştirildi.

Son ifadenin örtük reddetme ifadesinin herhangi bir istatistik göstermediğini unutmayın. Kaç tane örtük reddedilen paketin eşleştirildiğini izlemek için , ACL'nin sonundaki herhangi bir reddet komutunu manuel olarak yapılandırmanız gerekir .

ACL istatistiklerini temizlemek için **clear access-list counters** komutunu kullanın. Bu komut tek başına veya belirli bir ACL'nin numarası veya adıyla kullanılabilir.

```
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10  (20 matches)
    20 permit 192.168.10.0, wildcard bits 0.0.0.255  (64 matches)
R1# clear access-list counters NO-ACCESS
R1# show access-lists
Standard IP access list NO-ACCESS
    10 deny   192.168.10.10
    20 permit 192.168.10.0, wildcard bits 0.0.0.255
R1#
```

## 34.7.Standart IPv4 ACL ile VTY Bağlantı Noktalarını Güvenli Hale Getirme

### 34.7.1.Access-class Komutu

ACL'ler tipik olarak bir arabirimdeki gelen veya giden trafiği filtreler. Ancak, bir ACL, VTY hatlarını kullanarak bir aygıta uzaktan yönetim erişimini güvence altına almak için de kullanılabilir.

VTY hatlarına uzaktan yönetici erişimi sağlamak için aşağıdaki iki adımı kullanın:

- Hangi yönetici ana bilgisayarlara uzaktan erişime izin verileceğini belirlemek için bir ACL oluşturun.
- ACL'yi vty hatlarında gelen trafiğe uygulayın.

VTY satırlarına ACL uygulamak için aşağıdaki komutu kullanın:

```
R1(config-line)# access-class {access-list-number | access-list-name} { in | out }
```

**in** anahtar kelimesi gelen telnet trafiğini filtrelemek için en yaygın olarak kullanılan bir seçenektir. **Out** parametresi giden telnet trafiğini filtreler ve nadiren uygulanır.

Erişim listeleri vty hatlarında yapılandırılırken aşağıdakiler dikkate alınmalıdır:

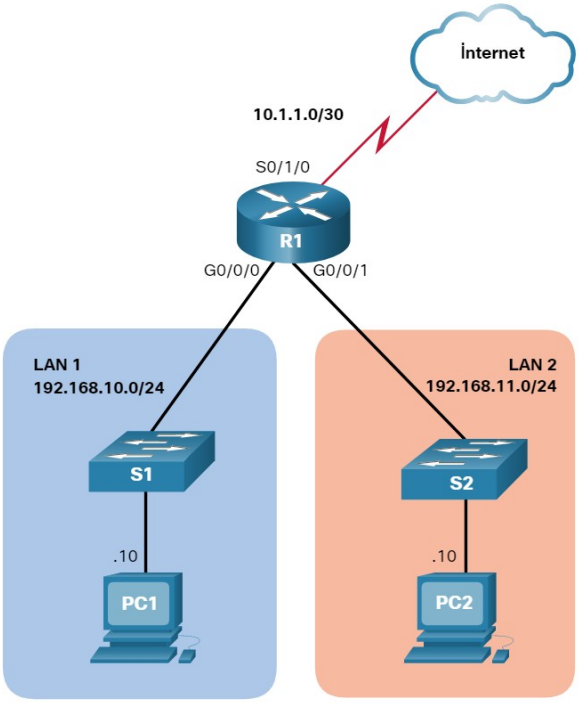
- Hem adlandırılmış hem de numaralandırılmış erişim listeleri vty hatlarına uygulanabilir.
- Bir kullanıcı bunlardan herhangi birine bağlanmayı deneyebileceğinden, tüm vty hatlarında aynı kısıtlamalar ayarlanmalıdır.

**Güvenli VTY Erişim Örneği**

Şekildeki topoloji, bir ACL'nin vty trafiğini filtrelemek için nasıl yapılandırılacağını göstermek için kullanılır. Bu örnekte, yalnızca PC1'in R1'e Telnet'e girmesine izin verilecektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Not : Telnet burada yalnızca gösterim amacıyla kullanılır. SSH, tercih edilmelidir.




Güvenli erişimi artırmak için bir kullanıcı adı ve parola oluşturulacak ve vty hatlarında oturum açma yerel kimlik doğrulama yöntemi kullanılacaktır. Örnekteki komut, bir kullanıcı ADMIN ve parola class olarak yerel bir veritabanı girişi oluşturur .

ADMIN-HOST adında bir adlandırılmış standart ACL oluşturulur ve PC1'i tanımlar. **deny any** bildirimi herhangi engellenen hostların erişim sayısını izlemek için yapılandırılmıştır.

Vty hatları, kimlik doğrulama için yerel veritabanını kullanacak, Telnet trafiğine izin verecek ve trafiği kısıtlamak için ADMIN-HOST ACL'yi kullanacak şekilde yapılandırılmıştır.

```
R1(config)# username ADMIN secret class
R1(config)# ip access-list standard ADMIN-HOST
R1(config-std-nacl)# remark This ACL secures incoming vty lines
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

Bir üretim ortamında, örnekte gösterildiği gibi vty satırlarını yalnızca SSH'ye izin verecek şekilde ayarlarsınız.

```
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# access-class ADMIN-HOST in
R1(config-line)# end
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 34.8.Genişletilmiş IPv4 ACL'leri Yapılandırma

### 34.8.1.Genişletilmiş ACL'ler

Standart ACL'ler yalnızca kaynak adresine filtre uygular. Daha hassas trafik filtreleme kontrolü gerektiğinde, genişletilmiş IPv4 ACL'leri oluşturulabilir.

Genişletilmiş ACL'ler, daha yüksek derecede kontrol sağladıkları için standart ACL'lerden daha sık kullanılır. Kaynak adresi, hedef adresi, protokol (yani, IP, TCP, UDP, ICMP) ve bağlantı noktası numarasına göre filtre uygulayabilirler. Bu, ACL'nin dayandırılacağı daha geniş bir kriter aralığı sağlar. Örneğin, genişletilmiş bir ACL, dosya aktarımlarını ve web taramasını reddederken bir ağdan belirli bir hedefe e-posta trafiğine izin verebilir.

Standart ACL'ler gibi, genişletilmiş ACL'ler şu şekilde oluşturulabilir:

Numaralı Genişletilmiş ACL - **access-list** *access-list-number* genel yapılandırma komutu kullanılarak oluşturulur.
Adlandırılmış Genişletilmiş ACL - **ip access-list extended** *access-list-name* komutu kullanılarak oluşturulur .

### 34.8.2.Numaralı Genişletilmiş IPv4 ACL Sözdizimi

Genişletilmiş ACL'leri yapılandırmak için prosedür adımları, standart ACL'lerle aynıdır. Genişletilmiş ACL önce yapılandırılır ve ardından bir arayüzde etkinleştirilir. Ancak, komut sözdizimi ve parametreleri, genişletilmiş ACL'ler tarafından sağlanan ek özellikleri desteklemek için daha karmaşıktır.

Numaralı bir genişletilmiş ACL oluşturmak için aşağıdaki genel yapılandırma komutunu kullanın:

```
Router(config)# access-list access-list-number {deny | permit | remark text} protocol source source-
wildcard [operator {port}] destination destination-wildcard [operator {port}] [established] [log]
```

Genişletilmiş bir ACL'yi kaldırmak için **no access-list** *access-list-number* genel yapılandırma komutunu kullanın.

Genişletilmiş ACL'ler için birçok anahtar sözcük ve parametre olmasına rağmen, genişletilmiş bir ACL'yi yapılandırırken bunların tümünü kullanmak gerekli değildir. Tablo, genişletilmiş bir ACL için söz diziminin ayrıntılı bir açıklamasını sağlar.

| Parametre | Açıklama |
|---|---|
| *access-list-number*<br>*erişim listesi numarası* | • Bu, ACL'nin ondalık sayısıdır.<br>• Genişletilmiş ACL numarası aralığı 100 ila 199 ve 2000 ila 2699'dur. |
| Deny<br>reddetme | Bu, koşul eşleşirse erişimi reddeder. |
| Permit<br>İzin verme | Bu, koşul eşleşirse erişime izin verir. |
| Remark *text*<br>açıklama *metin* | • (İsteğe bağlı) Belgeleme amacıyla bir metin girişi ekler.<br>• Her açıklama 100 karakterle sınırlıdır. |
| *protocol*<br>*protokol* | • İnternet protokolünün adı veya numarası.<br>• Yaygın anahtar kelimeler arasında ip , tcp , udp ve icmp bulunur.<br>• İp anahtar kelimesi tüm IP protokolleriyle eşleşir. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Parametre | Açıklama |
| --- | --- |
| *source*<br>*kaynak* | • Bu, filtrelenecek kaynak ağı veya ana bilgisayar adresini tanımlar.<br>• Tüm ağları belirtmek için herhangi bir anahtar sözcüğü kullanın.<br>• **Host** *ip-address* anahtar sözcüğünü kullanın veya belirli bir IP adresini tanımlamak için bir *ip-adresi* (host anahtar sözcüğü olmadan ) girin. |
| *source-wildcard*<br>*kaynak-joker karakter* | (İsteğe bağlı) Kaynağa uygulanan 32 bitlik bir joker karakter maskesi. |
| *destination*<br>*hedef* | • Bu, filtrelenecek hedef ağı veya ana bilgisayar adresini tanımlar.<br>• Tüm ağları belirtmek için herhangi bir anahtar sözcüğü kullanın.<br>• Kullanımı: **host** *ip-adres* anahtar sözcük veya *ip adresi.* |
| *destination-wildcard*<br>*hedef-joker karakter* | (İsteğe bağlı) Bu, hedefe uygulanan 32 bitlik bir joker karakter maskesidir. |
| *operator* | • (İsteğe bağlı) Bu, kaynak veya hedef bağlantı noktalarını karşılaştırır.<br>• Bazı operatörler arasında lt (küçüktür), gt (büyüktür), eq (eşittir) ve neq (eşit değildir) bulunur. |
| *port* | (İsteğe bağlı) Bir TCP veya UDP bağlantı noktasının ondalık sayısı veya adı. |
| **Established** | • (İsteğe bağlı) Yalnızca TCP protokolü için.<br>• Bu yeni nesil güvenlik duvarı özelliği. |
| log<br>günlük | • (İsteğe bağlı) Bu anahtar kelime, ACE eşleştiğinde bir bilgi mesajı oluşturur ve gönderir.<br>• Bu mesaj ACL numarasını, eşleşen koşulu (yani izin verilen veya reddedilen), kaynak adresini ve paket sayısını içerir.<br>• Bu mesaj ilk eşleşen paket için oluşturulur.<br>• Bu anahtar kelime yalnızca sorun giderme veya güvenlik nedenleriyle uygulanmalıdır. |

Bir arabirime genişletilmiş IPv4 ACL uygulama komutu, standart IPv4 ACL'ler için kullanılan komutla aynıdır.

```
Router(config-if)# ip access-group {access-list-number | access-list-name} {in | out}
```

Bir ACL'yi arabirimden kaldırmak için, önce **no ip access-group** arabirimi yapılandırma komutunu girin. ACL'yi yönlendiriciden kaldırmak için **no access-list** genel yapılandırma komutunu kullanın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 34.8.3.Protokoller ve Bağlantı Noktaları

Genişletilmiş ACL'ler, birçok farklı internet protokolü ve bağlantı noktası türüne filtre uygulayabilir.

### Protokol Seçenekleri

Vurgulanan dört protokol en popüler seçeneklerdir.

Not : ? karmaşık bir ACE girerken yardım almak için kullanılır.

Not: Bir internet protokolü listelenmemişse, IP protokol numarası belirtilebilir. Örneğin, ICMP protokol numarası 1, TCP 6 ve UDP 17'dir.

```
R1(config)# access-list 100 permit ?
  <0-255>       An IP protocol number
  ahp           Authentication Header Protocol
  dvmrp         dvmrp
  eigrp         Cisco's EIGRP routing protocol
  esp           Encapsulation Security Payload
  gre           Cisco's GRE tunneling
  icmp          Internet Control Message Protocol
  igmp          Internet Gateway Message Protocol
  ip            Any Internet Protocol
  ipinip        IP in IP tunneling
  nos           KA9Q NOS compatible IP over IP tunneling
  object-group  Service object group
  ospf          OSPF routing protocol
  pcp           Payload Compression Protocol
  pim           Protocol Independent Multicast
  tcp           Transmission Control Protocol
  udp           User Datagram Protocol
R1(config)# access-list 100 permit
```

### Anahtar Kelime Seçenekleri

Bir protokol seçmek, port seçeneklerini etkiler . Örneğin, şunları seçmek:

- tcp protokolü, TCP ile ilgili bağlantı noktası seçenekleri sağlar
- udp protokolü, UDP'ye özgü bağlantı noktası seçenekleri sağlar
- icmp protokolü, ICMP ile ilgili bağlantı noktaları (yani, mesaj) seçenekleri sağlar

Yine, kaç tane TCP bağlantı noktası seçeneğinin mevcut olduğuna dikkat edin. Vurgulanan bağlantı noktaları popüler seçeneklerdir.

Bağlantı noktası adları veya numarası belirtilebilir. Bununla birlikte, bağlantı noktası adları bir ACE'nin amacını anlamayı kolaylaştırır.
Bazı yaygın bağlantı noktası adlarının (örneğin, SSH ve HTTPS) listelenmediğine dikkat edin. Bu protokoller için port numaralarının belirtilmesi gerekecektir.

Licensed to yetkin karasu

```
R1(config)# access-list 100 permit tcp any any eq ?
  <0-65535>     Port number
  bgp           Border Gateway Protocol (179)
  chargen       Character generator (19)
  cmd           Remote commands (rcmd, 514)
  daytime       Daytime (13)
  discard       Discard (9)
  domain        Domain Name Service (53)
  echo          Echo (7)
  exec          Exec (rsh, 512)
  finger        Finger (79)
  ftp           File Transfer Protocol (21)
  ftp-data      FTP data connections (20)
  gopher        Gopher (70)
  hostname      NIC hostname server (101)
  ident         Ident Protocol (113)
  irc           Internet Relay Chat (194)
  klogin        Kerberos login (543)
  kshell        Kerberos shell (544)
  login         Login (rlogin, 513)
  lpd           Printer service (515)
  msrpc         MS Remote Procedure Call (135)
  nntp          Network News Transport Protocol (119)
  onep-plain    Onep Cleartext (15001)
  onep-tls      Onep TLS (15002)
  pim-auto-rp   PIM Auto-RP (496)
  pop2          Post Office Protocol v2 (109)
  pop3          Post Office Protocol v3 (110)
  smtp          Simple Mail Transport Protocol (25)
```

**Protokoller ve Bağlantı Noktası Numaraları Yapılandırma Örnekleri**

Genişletilmiş ACL'ler, farklı bağlantı noktası numarası ve bağlantı noktası adı seçeneklerine göre filtre uygulayabilir. Bu örnek, HTTP trafiğini filtrelemek için genişletilmiş bir ACL 100 yapılandırır. İlk ACE, www bağlantı noktası adını kullanır . İkinci ACE, 80 numaralı bağlantı noktasını kullanır . Her iki ACE de tam olarak aynı sonucu elde eder.

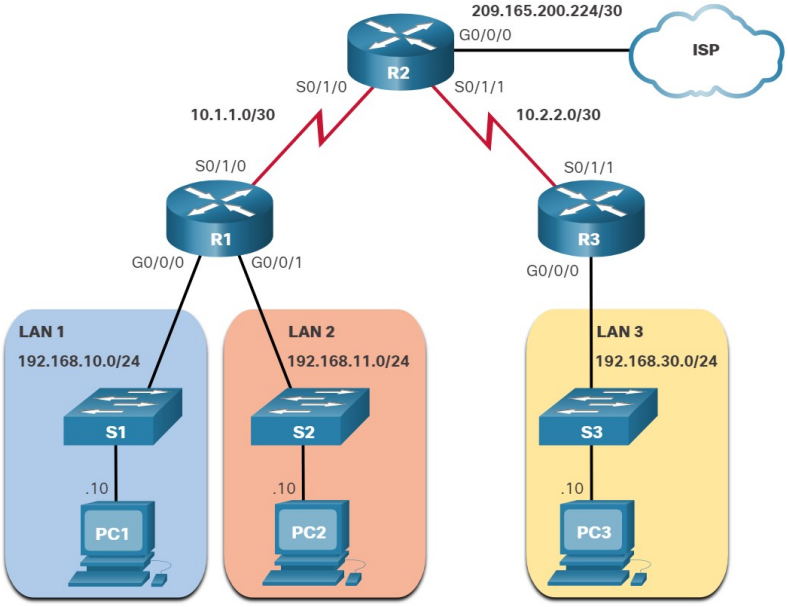
```
R1(config)# access-list 100 permit tcp any any eq www !or...
R1(config)# access-list 100 permit tcp any any eq 80
```

Sonraki örnekte gösterildiği gibi, SSH (bağlantı noktası numarası 22) veya HTTPS (bağlantı noktası numarası 443) gibi belirli bir protokol adı listelenmediğinde bağlantı noktası numarasının yapılandırılması gerekir.

```
R1(config)# access-list 100 permit tcp any any eq 22 R1(config)# access-list 100 permit tcp any any eq
443
R1(config)#
```

## 34.8.4.Numaralı Genişletilmiş IPv4 ACL Uygulaması

Şekildeki topoloji, numaralandırılmış ve adlandırılmış genişletilmiş IPv4 ACL'leri bir arabirime yapılandırmayı ve uygulamayı göstermek için kullanılacaktır. Bu ilk örnek, numaralandırılmış bir genişletilmiş IPv4 ACL uygulamasını gösterir.




Bu örnekte ACL, 192.168.10.0 ağından hem HTTP hem de HTTPS trafiğinin herhangi bir hedefe gitmesine izin verir.

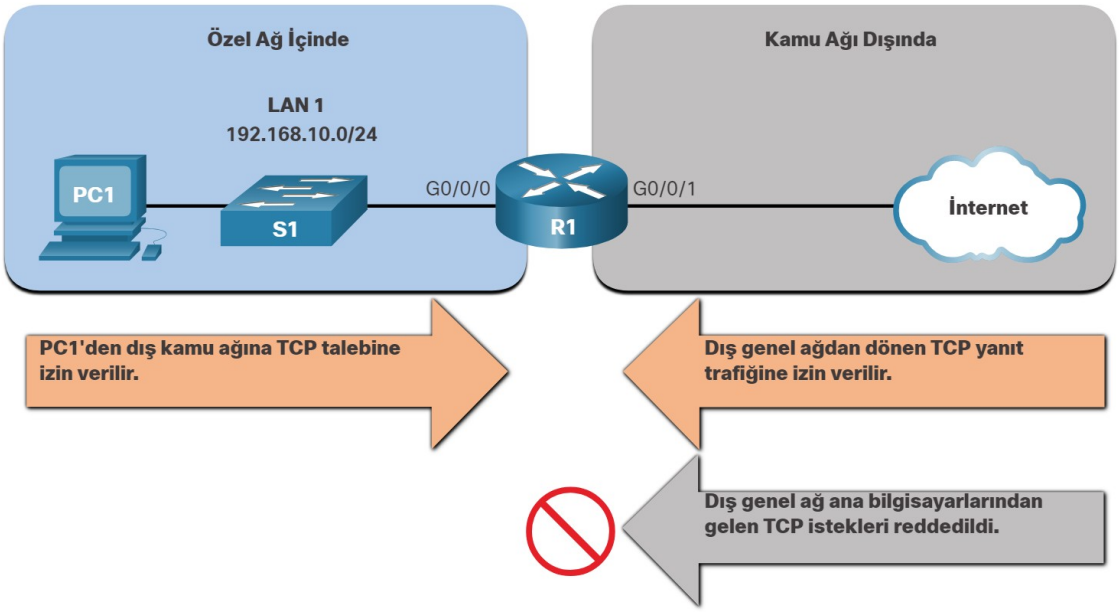
Genişletilmiş ACL'ler çeşitli yerlerde uygulanabilir. Ancak, genellikle kaynağa yakın uygulanırlar. Bu nedenle, ACL 110, R1 G0 / 0/0 arayüzünde gelen olarak uygulandı.

```
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config)# access-list 110 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 110 in
R1(config-if)# exit
R1(config)#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## TCP Established Genişletilmiş ACL

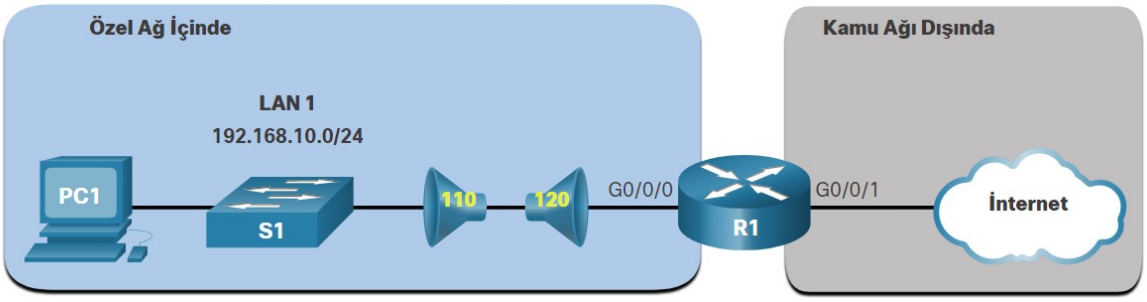
TCP, TCP **established** anahtar sözcüğünü kullanarak temel durum bilgisi olan güvenlik duvarı hizmetlerini de gerçekleştirebilir . Anahtar sözcük, iç trafiğin iç özel ağdan çıkmasını sağlar ve geri dönen yanıt trafiğinin şekilde gösterildiği gibi iç özel ağa girmesine izin verir.




Ancak, bir dış ana bilgisayar tarafından oluşturulan ve içerideki bir ana bilgisayarla iletişim kurmaya çalışan TCP trafiği reddedilir.

**Established** kelimesi kalan trafiği reddederken, istenen web sitelerinden sadece dönüş HTTP trafiğini izin vermek için kullanılabilir.

Topolojide, bu örneğin tasarımı, önceden yapılandırılmış olan ACL 110'un özel ağın içindeki trafiği filtreleyeceğini göstermektedir. ACL 120, **established** anahtar sözcüğü kullanarak , dış kamu ağından içerideki özel ağa gelen trafiği filtreleyecektir.




Örnekte, ACL 120 yalnızca web trafiğinin iç ana bilgisayarlara geri dönmesine izin verecek şekilde yapılandırılmıştır. Yeni ACL daha sonra R1 G0 / 0/0 arayüzünde giden uygulanır. **Show access-list** komutu her iki ACL'yi de görüntüler. Eşleşme istatistiklerinden, içerideki ev sahiplerinin internetten güvenli web kaynaklarına eriştiğine dikkat edin.

```
R1(config)# access-list 120 permit tcp any 192.168.10.0 0.0.0.255 established
R1(config)# interface g0/0/0
R1(config-if)# ip access-group 120 out
R1(config-if)# end R1# show access-lists
Extended IP access list 110
     10 permit tcp 192.168.10.0 0.0.0.255 any eq www
     20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (657 matches)
Extended IP access list 120     10 permit tcp any 192.168.10.0 0.0.0.255 established (1166 matches)
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

ACL 110'daki güvenli izinli HTTPS sayaçlarının (yani, eq 443) ve ACL 120'de geri dönen sayaçların arttığına dikkat edin.

Established parametresi 192.168.10.0/24 ağdan kaynaklanır bu ağa dönmek için bu trafiğin tek yanıtları verir. Spesifik olarak, geri dönen TCP kesimi ACK veya sıfırlama (RST) bayrak bitlerine sahipse bir eşleşme gerçekleşir. Bu, paketin mevcut bir bağlantıya ait olduğunu gösterir. ACL deyiminde belirlenen parametre olmadan , istemciler bir web sunucusuna trafik gönderebilir ve web sunucusundan dönen trafiği alabilir. Tüm trafiğe izin verilecek.

### 34.8.5.Adlandırılmış Genişletilmiş IPv4 ACL Sözdizimi

ACL'yi adlandırmak, işlevini anlamayı kolaylaştırır. Adlandırılmış bir genişletilmiş ACL oluşturmak için aşağıdaki genel yapılandırma komutunu kullanın:

```
Router(config)# ip access-list extended access-list-name
```

Bu komut, adlandırılmış genişletilmiş yapılandırma moduna girer. ACL adlarının alfasayısal, büyük / küçük harfe duyarlı olduğunu ve benzersiz olması gerektiğini hatırlayın.

Örnekte, NO-FTP-ACCESS adlı adlandırılmış bir genişletilmiş ACL oluşturulur ve komut istemi, adlandırılmış genişletilmiş ACL yapılandırma moduna değiştirilir. ACE ifadeleri, adlandırılmış genişletilmiş ACL alt yapılandırma modunda girilir.

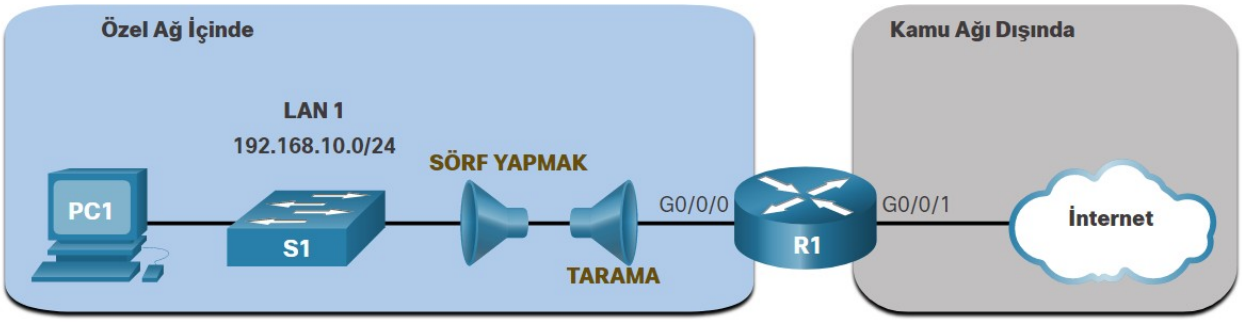
```
R1(config)# ip access-list extended NO-FTP-ACCESS
R1(config-ext-nacl)#
```

## 34.8.6.Adlandırılmış Genişletilmiş IPv4 ACL Örneği

Adlandırılmış genişletilmiş ACL'ler, esasen adlandırılmış standart ACL'lerin oluşturulduğu şekilde oluşturulur.

Şekildeki topoloji, adlandırılmış iki genişletilmiş IPv4 ACL'nin bir arabirime yapılandırılmasını ve uygulanmasını göstermek için kullanılır:

SURFING - Bu, HTTP ve HTTPS trafiğinin internete çıkmasına izin verecektir.
BROWSING - Bu, R1 G0 / 0/0 arayüzünden çıkan diğer tüm trafik örtük olarak reddedilirken yalnızca web trafiğinin içerideki ana bilgisayarlara geri dönmesine izin verir.




Örnek, gelen SURFING ACL ve outbound BROWSING ACL için yapılandırmayı gösterir.

SURFING ACL, içerideki kullanıcıların HTTP ve HTTPS trafiğinin internete bağlı G0 / 0/1 arayüzünden çıkmasına izin verir. İnternetten dönen web trafiğinin, BROWSING ACL tarafından iç özel ağa geri girmesine izin verilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Çıktıda gösterildiği gibi, SURFING ACL gelen ve R1 G0 / 0/0 arayüzünde giden BROWSING ACL uygulanır.

Inside hostlar internetten güvenli web kaynaklarına erişiyorlar. Show access-list komutu, ACL istatistiklerini doğrulamak için kullanılır. SURFING ACL'deki izin güvenli HTTPS sayaçlarının (yani, eq 443) ve BROWSING ACL'deki dönüş kurulu sayaçlarının arttığına dikkat edin.

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# Remark Permits inside HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)#
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# Remark Only permit returning HTTP and HTTPS traffic
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
R1(config-if)# end
R1# show access-lists
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443 (124 matches)
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established (369 matches)
R1#
```

## 34.8.7.Genişletilmiş ACL'leri Düzenleme

Standart ACL'ler gibi, genişletilmiş bir ACL, birçok değişiklik gerektiğinde bir metin düzenleyici kullanılarak düzenlenebilir. Aksi takdirde, düzenleme bir veya iki ACE için geçerliyse, sıra numaraları kullanılabilir.

Örneğin, SURFING ve BROWSING ACL'lerini yeni girdiğinizi ve **show access-list** komutunu kullanarak yapılandırmalarını doğrulamak istediğinizi varsayalım .

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 19.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

SURFING ACL'deki ACE sıra numarası 10'un yanlış bir kaynak IP ağ adresine sahip olduğunu fark ettiniz.

Sıra numaralarını kullanarak bu hatayı düzeltmek için, orijinal deyim no sıra _ # komutuyla kaldırılır ve orijinal deyimin yerine düzeltilmiş ifade eklenir.

```
R1# configure terminal
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# no 10
R1(config-ext-nacl)# 10 permit tcp 192.168.10.0 0.0.0.255 any eq www
R1(config-ext-nacl)# end
```

Çıktı, show access-list komutunu kullanarak yapılandırma değişikliğini doğrular .

```
R1# show access-lists
Extended IP access list BROWSING
    10 permit tcp any 192.168.10.0 0.0.0.255 established
Extended IP access list SURFING
    10 permit tcp 192.168.10.0 0.0.0.255 any eq www
    20 permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1#
```

Licensed to yetkin karamagur, yetkinkrsngr@gmail.com

## 34.8.8.Genişletilmiş ACL'leri Doğrulama

Bir ACL yapılandırıldıktan ve bir arabirime uygulandıktan sonra , yapılandırmayı doğrulamak için Cisco IOS show komutlarını kullanın.

### show ip interface

**show ip interface** komutu arayüzü ve çıkış gösterildiği gibi, uygulanan yöne ACL'i doğrulamak için kullanılır.

Komut oldukça fazla çıktı üretir, ancak büyük harfle yazılmış ACL adlarının çıktıda nasıl öne çıktığına dikkat edin.

Komut çıktısını azaltmak için, ikinci komutta gösterildiği gibi filtreleme tekniklerini kullanın.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Internet address is 192.168.10.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is REPLY-PC1
  Inbound  access list is PERMIT-PC1
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
```

### show access-lists

**show access-lists** komutu beklendiği gibi ACL çalışmasını onaylamak için kullanılabilir. Komut, bir ACE eşleştiğinde artan istatistik sayaçlarını görüntüler.

Not : ACL'nin işleyişini doğrulamak için trafik oluşturulmalıdır.

En üstteki örnekte, Cisco IOS komutu, tüm ACL'lerin içeriğini görüntülemek için kullanılır.

Bağlantı noktası numaraları yapılandırılmış olmasına rağmen IOS'nin anahtar kelimeyi nasıl görüntülediğine dikkat edin.

Ayrıca, genişletilmiş ACL'lerin standart ACL'lerle aynı dahili mantığı ve karma işlevi uygulamadığına dikkat edin. show access-lists komut çıktısında görüntülenen çıktı ve sıra numaraları , ifadelerin girildiği sıradır. Ana bilgisayar girişleri, aralık girişlerinden önce otomatik olarak listelenmez.

```
R1# show access-lists
Extended IP access list PERMIT-PC1
    10 permit tcp host 192.168.10.10 any eq ftp-data
    20 permit tcp host 192.168.10.10 any eq ftp
    30 permit tcp host 192.168.10.10 any eq 22
    40 permit tcp host 192.168.10.10 any eq telnet
    50 permit udp host 192.168.10.10 any eq domain
    60 permit tcp host 192.168.10.10 any eq domain
    70 permit tcp host 192.168.10.10 any eq www
    80 permit tcp host 192.168.10.10 any eq 443
    90 deny ip 192.168.10.0 0.0.0.255 any
Extended IP access list REPLY-PC1
    10 permit tcp any host 192.168.10.10 established
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**show running-config**

**show running-config** komutu yapılandırmayı doğrulamak için kullanılabilir. Komut ayrıca yapılandırılmış açıklamaları da görüntüler.

Komut, aşağıda gösterildiği gibi yalnızca ilgili bilgileri görüntülemek için filtrelenebilir.

```
R1# show running-config | begin ip access-list
ip access-list extended PERMIT-PC1
 remark Permit PC1 TCP access to internet
 permit tcp host 192.168.10.10 any eq ftp-data
 permit tcp host 192.168.10.10 any eq ftp
 permit tcp host 192.168.10.10 any eq 22
 permit tcp host 192.168.10.10 any eq telnet
 permit udp host 192.168.10.10 any eq domain
 permit tcp host 192.168.10.10 any eq domain
 permit tcp host 192.168.10.10 any eq www
 permit tcp host 192.168.10.10 any eq 443
 deny   ip 192.168.10.0 0.0.0.255 any
ip access-list extended REPLY-PC1
 remark Only permit returning traffic to PC1
 permit tcp any host 192.168.10.10 established
!
(output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 35.Bölüm: NAT(Network Address Translation)-Ağ Adres Çevirisi

## 35.1.NAT Özellikleri

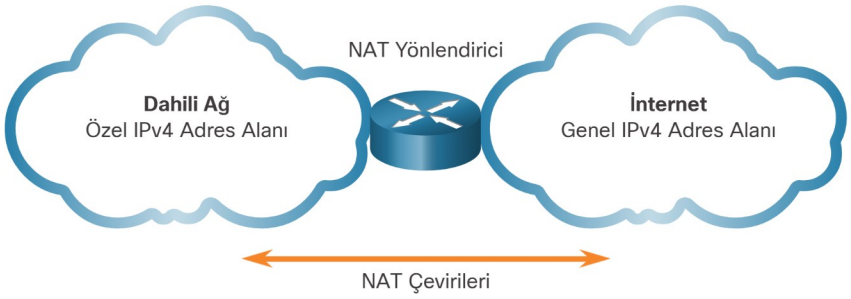
### 35.1.1.IPv4 Özel Adres Alanı

Bildiğiniz gibi, internete bağlı her cihaza benzersiz bir adres atamak için yeterli genel IPv4 adresi yoktur. Ağlar genellikle RFC 1918'de tanımlandığı gibi özel IPv4 adresleri kullanılarak uygulanır. RFC 1918'de bulunan adres aralığı aşağıdaki tabloda gösterilmiştir. Bu kitabı görüntülemek için kullandığınız bilgisayara büyük olasılıkla 192.168.1.121 gibi özel bir adres atanmıştır.

| Sınıf | RFC 1918 Dahili Adres Aralığı | Önek |
|---|---|---|
| A | 10.0.0.0 - 10.255.255.255 | 10.0.0.0/8 |
| B | 172.16.0.0 - 172.31.255.255 | 172.16.0.0/12 |
| C | 192.168.0.0 - 192.168.255.255 | 192.168.0.0/16 |

Bu özel adresler, cihazların yerel olarak iletişim kurmasına izin vermek için bir kuruluş veya site içinde kullanılır. Ancak, bu adresler tek bir şirketi veya kuruluşu tanımlamadığından, özel IPv4 adresleri internet üzerinden yönlendirilemez. Özel IPv4 adresine sahip bir aygıtın yerel ağ dışındaki aygıtlara ve kaynaklara erişmesine izin vermek için, özel adresin önce bir genel adrese çevrilmesi gerekir.

NAT, şekilde gösterildiği gibi özel adreslerin genel adreslere çevrilmesini sağlar. Bu, özel IPv4 adresine sahip bir cihazın, internette bulunanlar gibi kendi özel ağlarının dışındaki kaynaklara erişmesine izin verir. NAT, özel IPv4 adresleriyle birleştirildiğinde, genel IPv4 adreslerini korumanın birincil yöntemi olmuştur. Tek bir genel IPv4 adresi, her biri benzersiz bir özel IPv4 adresiyle yapılandırılmış yüzlerce, hatta binlerce cihaz tarafından paylaşılabilir.




NAT olmasaydı, IPv4 adres alanının tükenmesi 2000 yılından çok önce meydana gelirdi. Ancak NAT'ın sınırlamaları ve dezavantajları vardır ve bunlar bu bölümde daha sonraanlatılacaktır. IPv4 adres alanının tükenmesine ve NAT sınırlamalarına yönelik çözüm, nihai olarak IPv6'ya geçiştir.

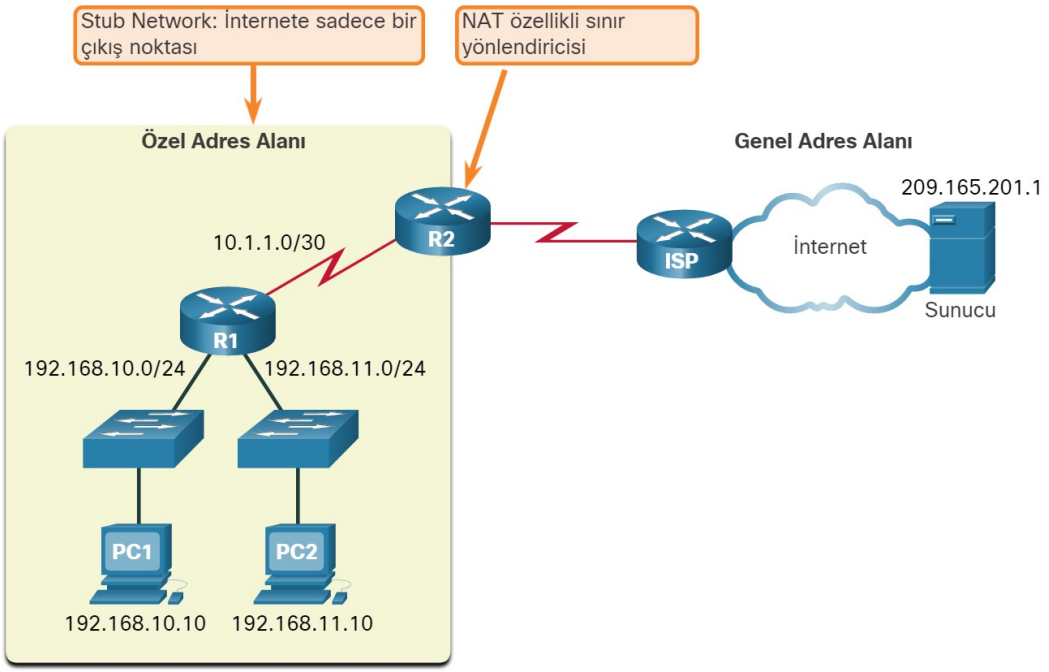
### 35.1.2.NAT Nedir?

NAT'ın birçok kullanımı vardır, ancak birincil kullanımı genel IPv4 adreslerini korumaktır. Bunu, ağların dahili olarak özel IPv4 adreslerini kullanmasına izin vererek ve yalnızca gerektiğinde bir genel adrese çeviri sağlayarak yapar. NAT, dahili IPv4 adreslerini dış ağlardan gizlediği için bir ağa bir derece gizlilik ve güvenlik eklemenin algılanan bir faydasına sahiptir.

NAT özellikli yönlendiriciler, bir veya daha fazla geçerli genel IPv4 adresiyle yapılandırılabilir. Bu genel adresler NAT havuzu olarak bilinir. Dahili bir aygıt ağın dışına trafik gönderdiğinde, NAT etkin yönlendirici, aygıtın dahili IPv4 adresini NAT havuzundan bir genel adrese çevirir. Dış cihazlara ağa giren ve çıkan tüm trafiğin sağlanan adres havuzundan genel bir IPv4 adresi olduğu görülür.

Cisco Networking Academy Mindshare | Yetkisiz kullanım yasaktır.

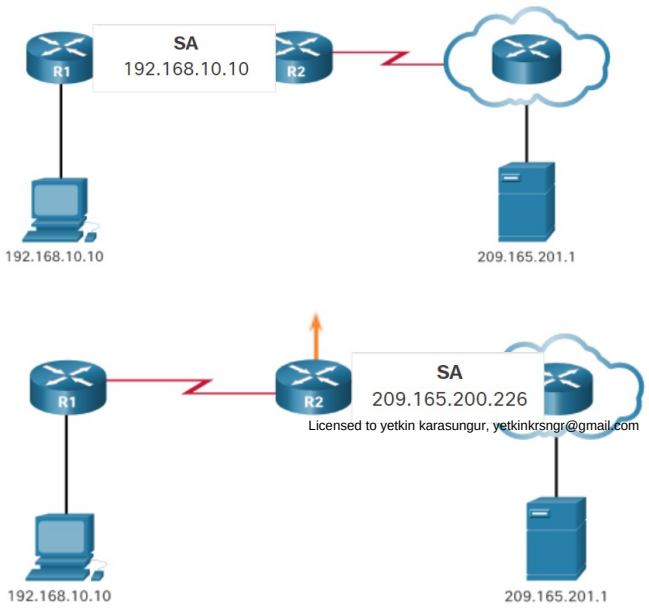
Bir NAT yönlendiricisi tipik olarak bir saplama ağının sınırında çalışır. Saplama ağı, komşu ağa tek bir bağlantıya sahip, ağa bir giriş ve bir çıkış yolu olan bir veya daha fazla ağdır. Şekildeki örnekte, R2 bir sınır yönlendiricisidir. ISP'den görüldüğü gibi, R2 bir saplama ağı oluşturur.




Saplama ağı içindeki bir cihaz, ağının dışındaki bir cihazla iletişim kurmak istediğinde, paket sınır yönlendiricisine iletilir. Sınır yönlendiricisi, aygıtın dahili özel adresini genel, dışarıdan yönlendirilebilir bir adrese çevirerek NAT işlemini gerçekleştirir.

## 35.1.3.NAT Nasıl Çalışır?

Bu örnekte, 192.168.10.10 özel adresli PC1, 209.165.201.1 genel adresli bir dış web sunucusuyla iletişim kurmak istiyor.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 35.1.4.NAT Terminolojisi

NAT terminolojisinde, iç ağ, çeviriye tabi olan ağlar kümesidir. Dış ağ, diğer tüm ağları ifade eder.

NAT kullanılırken, IPv4 adreslerinin özel ağda mı yoksa genel ağda (internet) mı olduklarına ve trafiğin gelen mi yoksa giden mi olduğuna bağlı olarak farklı atamaları vardır.

NAT dört tür adres içerir:

- Inside local address- İç yerel adres
- Inside global address-İç genel adres
- Outside local address-Dış yerel adres
- Outside global address-Dış genel adres

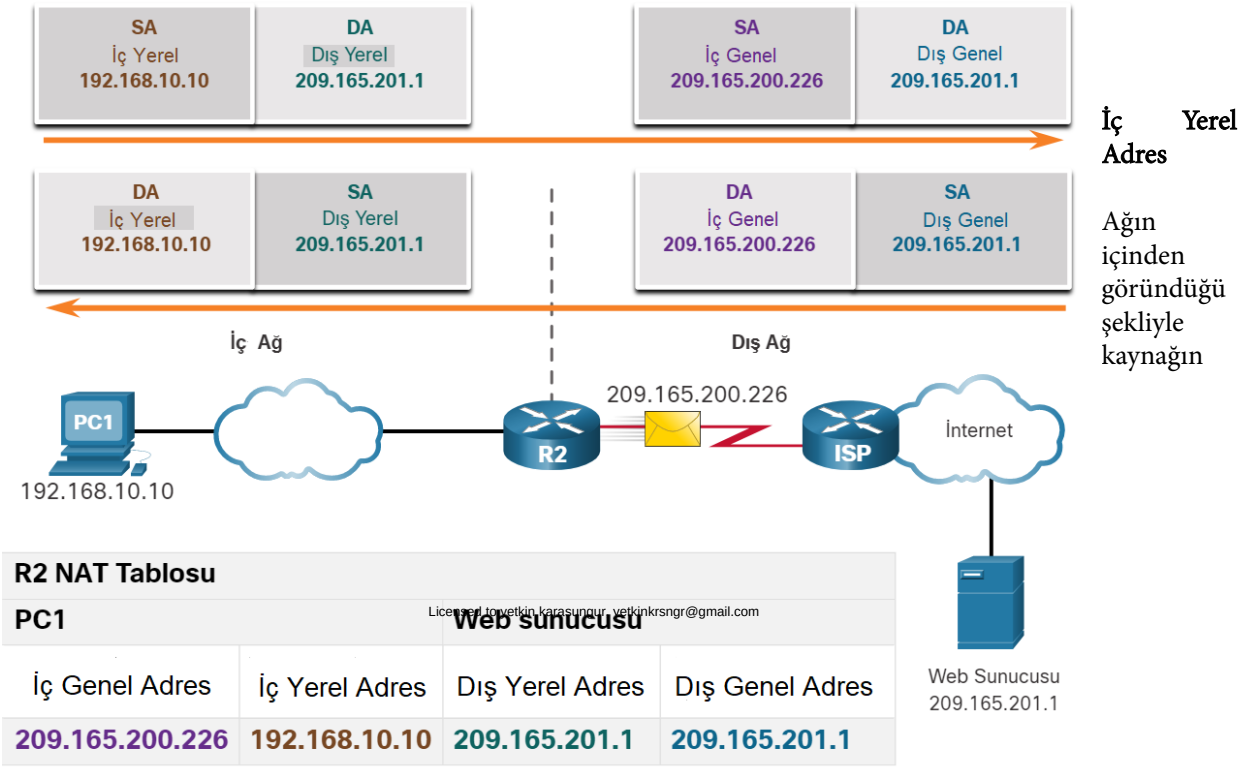
Hangi tür adresin kullanıldığını belirlerken, NAT terminolojisinin her zaman çevrilmiş adrese sahip cihaz perspektifinden uygulandığını unutmamak önemlidir:

İç adres - NAT tarafından çevrilen aygıtın adresi.
Dış adres - Hedef aygıtın adresi.

NAT ayrıca adreslerle ilgili olarak yerel veya genel (global) kavramını kullanır:

Yerel adres - Yerel adres , ağın iç kısmında görünen herhangi bir adrestir.
Genel adres - Genel adres , ağın dış kısmında görünen herhangi bir adrestir.

İç ve dış terimleri, belirli adreslere atıfta bulunmak için yerel ve genel terimlerle birleştirilmiştir. Şekildeki R2 NAT yönlendiricisi, iç ve dış ağlar arasındaki sınır noktasıdır. R2, içerideki ana bilgisayarlara atanacak bir genel adres havuzuyla yapılandırılmıştır. NAT adres türlerinin her birinin aşağıdaki açıklaması için şekildeki ağ ve NAT tablosuna bakın.




**İç Yerel Adres**

Ağın içinden göründüğü şekliyle kaynağın

**R2 NAT Tablosu**

| PC1 | | Web sunucusu | |
|---|---|---|---|
| İç Genel Adres | İç Yerel Adres | Dış Yerel Adres | Dış Genel Adres |
| 209.165.200.226 | 192.168.10.10 | 209.165.201.1 | 209.165.201.1 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

adresi. Bu genellikle özel bir IPv4 adresidir. Şekilde, IPv4 adresi 192.168.10.10 PC1'e atanmıştır. Bu, PC1'in iç yerel adresidir.

**İç Genel Adres**

Dış ağdan görüldüğü şekliyle kaynağın adresi. Bu genellikle genel olarak yönlendirilebilir bir IPv4 adresidir. Şekilde, 209.165.201.1'de PC1'den gelen trafik web sunucusuna gönderildiğinde, R2 dahili yerel adresi bir iç global adrese çevirir. Bu durumda R2, IPv4 kaynak adresini 192.168.10.10'dan 209.165.200.226'ya değiştirir. NAT terminolojisinde, 192.168.10.10 iç yerel adresi, 209.165.200.226 iç global adresine çevrilmiştir.

**Dış Genel (Küresel) Adres**

Dış ağdan görüldüğü şekliyle hedefin adresi. İnternetteki bir ana bilgisayara atanan, küresel olarak yönlendirilebilir bir IPv4 adresidir. Örneğin, web sunucusuna 209.165.201.1 IPv4 adresinden ulaşılabilir. Çoğu zaman dış yerel ve dış küresel adresler aynıdır.

**Dış Yerel Adres**

İç ağdan görüldüğü şekliyle hedefin adresi. Bu örnekte, PC1, 209.165.201.1 IPv4 adresindeki web sunucusuna trafik gönderir. Yaygın olmamakla birlikte, bu adres, hedefin global olarak yönlendirilebilir adresinden farklı olabilir.

PC1, 192.168.10.10 dahili yerel adresine sahiptir. PC1 perspektifinden, web sunucusunun 209.165.201.1 dış adresi vardır. Paketler PC1'den web sunucusunun global adresine gönderildiğinde, PC1'in iç yerel adresi 209.165.200.226'ya çevrilir (iç genel adres). Dış aygıtın adresi genellikle çevrilmez çünkü bu adres genellikle genel bir IPv4 adresidir.

PC1'in farklı yerel ve genel adreslere sahip olduğuna, oysa web sunucusunun her ikisi için de aynı genel IPv4 adresine sahip olduğuna dikkat edin. Web sunucusu açısından bakıldığında, PC1'den kaynaklanan trafiğin, iç global adres olan 209.165.200.226'dan geldiği görülmektedir.

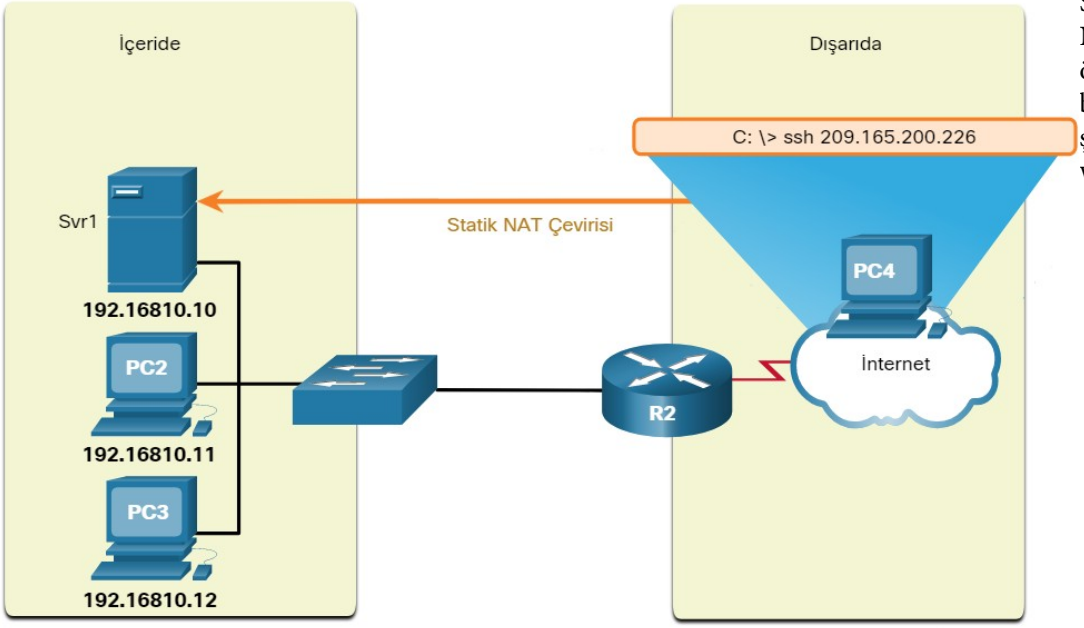
## 35.2.NAT Türleri

### 35.2.1.Statik NAT

Statik NAT, yerel ve global adreslerin bire bir eşlemesini kullanır. Bu eşlemeler ağ yöneticisi tarafından yapılandırılır ve sabit kalır.

Şekilde R2, Svr1, PC2 ve PC3'ün dahili yerel adresleri için statik eşlemeler ile yapılandırılmıştır. Bu cihazlar internete trafik gönderdiğinde, iç yerel adresleri, yapılandırılmış global adreslere çevrilir. Dış ağlara, bu cihazların genel IPv4 adresleri olduğu görülüyor.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Statik NAT, özellikle bir şirket web

**Statik NAT Tablosu**

| İç Yerel Adres | İç Genel Adres - R2 aracılığıyla ulaşılabilen adresler |
|---|---|
| 192.168.10.10 | 209.165.200.226 |
| 192.168.10.11 | 209.165.200.227 |
| 192.168.10.12 | 209.165.200.228 |

sunucusu gibi internetten erişilebilen tutarlı bir adrese sahip olması gereken web sunucuları veya cihazlar için kullanışlıdır. Ayrıca, site dışındayken yetkili personel tarafından erişilebilir olması gereken, ancak internetteki genel halk tarafından erişilemeyen cihazlar için de yararlıdır. Örneğin, PC4'ten bir ağ yöneticisi, Svr1'in dahili global adresine (209.165.200.226) erişmek için SSH'yi kullanabilir. R2 bunu dahili global adresi 192.168.10.10 iç yerel adrese çevirir ve oturumu Svr1'e bağlar.

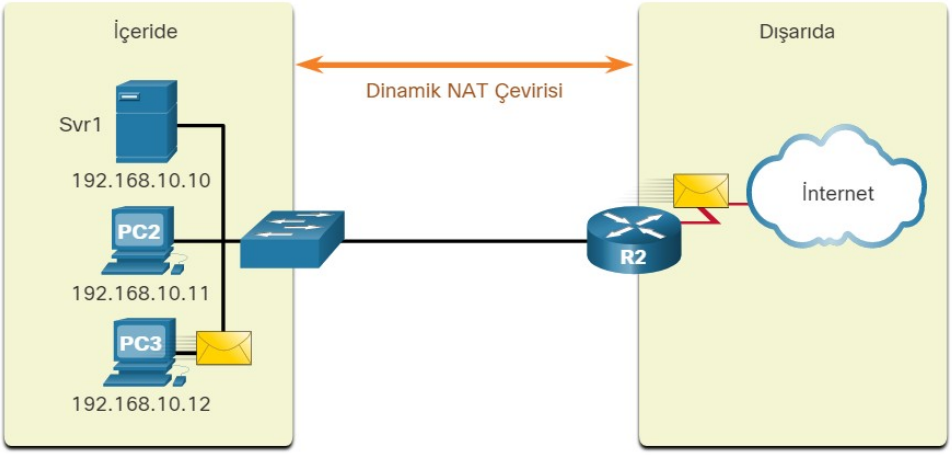
Statik NAT, eşzamanlı kullanıcı oturumlarının toplam sayısını karşılamak için yeterli genel adresin mevcut olmasını gerektirir.

## 35.2.2.Dinamik NAT

Dinamik NAT, bir genel adres havuzu kullanır ve bunları ilk gelene ilk hizmet esasına göre atar. Dahili bir cihaz bir dış ağa erişim istediğinde, dinamik NAT havuzdan kullanılabilir bir genel IPv4 adresi atar.

Şekilde, PC3, dinamik NAT havuzundaki ilk kullanılabilir adresi kullanarak internete erişmiştir. Diğer adresler hala kullanılabilir. Statik NAT'a benzer şekilde, dinamik NAT, eşzamanlı kullanıcı oturumlarının toplam sayısını karşılamak için yeterli genel adresin mevcut olmasını gerektirir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



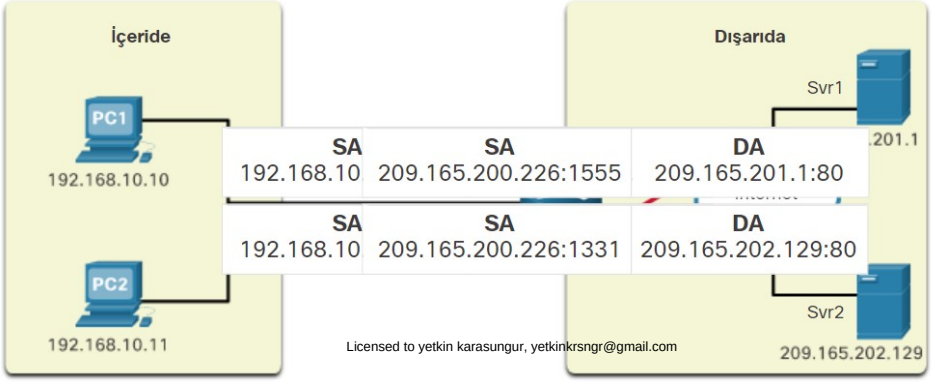

| IPv4 NAT Havuzu | | |
|---|---|---|
| İç Yerel Adres | İç Genel Adres Havuzu adresler | - R2 aracılığıyla ulaşılabilen |
| 192.168.10.12 | 209.165.200.226 | |
| Mevcut | 209.165.200.227 | |
| Mevcut | 209.165.200.228 | |
| Mevcut | 209.165.200.229 | |
| Mevcut | 209.165.200.230 | |

## 35.2.3.Port Adres Çevirisi (PAT-Port Address Translation)

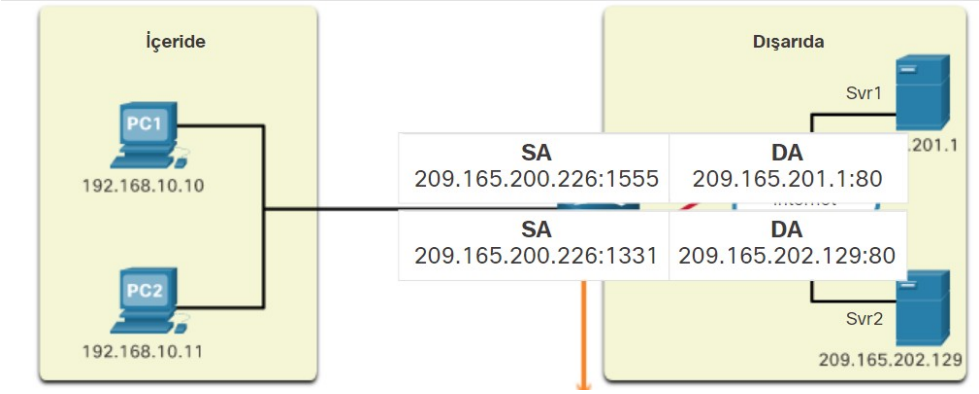
NAT aşırı yükü (NAT taşması) olarak da bilinen Bağlantı Noktası Adres Çevirisi (PAT), birden çok özel IPv4 adresini tek bir genel IPv4 adresine veya birkaç adrese eşler. Bu, çoğu ev yönlendiricisinin yaptığı şeydir. ISP, yönlendiriciye bir adres atar, ancak evin birkaç üyesi aynı anda internete erişebilir. Bu, hem ev hem de işletme için en yaygın NAT biçimidir.

PAT ile, her bir özel adres aynı zamanda bir port numarası ile izlendiğinden, birden çok adres bir veya birkaç adrese eşlenebilir. Bir cihaz bir TCP / IP oturumu başlattığında, oturumu benzersiz bir şekilde tanımlamak için bir TCP veya UDP kaynak bağlantı noktası değeri veya ICMP için özel olarak atanmış bir sorgu kimliği oluşturur. NAT yönlendiricisi istemciden bir paket aldığında, belirli NAT çevirisini benzersiz bir şekilde tanımlamak için kaynak bağlantı noktası numarasını kullanır.

PAT, cihazların internetteki bir sunucuyla her oturum için farklı bir TCP bağlantı noktası numarası kullanmasını sağlar. Sunucudan bir yanıt geldiğinde, dönüş yolculuğunda hedef bağlantı noktası numarası haline gelen kaynak bağlantı noktası numarası, yönlendiricinin paketleri hangi cihaza ilettiğini belirler. PAT işlemi ayrıca gelen paketlerin talep edildiğini doğrular ve böylece oturuma bir derece güvenlik ekler.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




R2 her paketi işlerken, paketin kaynaklandığı aygıtı tanımlamak için bir bağlantı noktası numarası (bu örnekte 1331 ve 1555) kullanır. Kaynak adresi (SA), eklenen TCP / UDP'ye atanan bağlantı noktası numarasıyla dahili yerel adrestir. Hedef adres (DA), servis port numarası eklenen dış global adrestir. Bu örnekte, hizmet bağlantı noktası HTTP olan 80'dir.

Kaynak adresi için R2, dahili yerel adresi, eklenen bağlantı noktası numarasıyla birlikte bir dahili global adrese çevirir. Hedef adres değiştirilmez, ancak artık dış küresel IPv4 adresi olarak anılmaktadır. Web sunucusu yanıt verdiğinde, yol tersine çevrilir.

### Sonraki Kullanılabilir Bağlantı Noktası

Önceki örnekte, istemci bağlantı noktası numaraları olan 1331 ve 1555 NAT etkin yönlendiricide değişmedi. Bu çok olası bir senaryo değildir, çünkü bu bağlantı noktası numaralarının zaten diğer aktif oturumlara eklenmiş olma ihtimali yüksektir.

PAT, orijinal kaynak bağlantı noktasını korumaya çalışır. Bununla birlikte, orijinal kaynak bağlantı noktası zaten kullanılıyorsa, PAT, uygun bağlantı noktası grubu 0-511, 512-1,023 veya 1,024-65,535'in başından başlayarak ilk kullanılabilir bağlantı noktası numarasını atar. Daha fazla bağlantı noktası olmadığında ve adres havuzunda birden fazla harici adres olduğunda, PAT, orijinal kaynak bağlantı noktasını tahsis etmeye çalışmak için sonraki adrese geçer. Bu işlem, başka kullanılabilir bağlantı noktası veya harici IPv4 adresi kalmayana kadar devam eder.

## 35.2.4.NAT ve PAT Karşılaştırması

Tablo, NAT ve PAT arasındaki farkların bir özetini sunar.

| NAT | PAT |
|---|---|
| Inside Local ve Inside Global adresleri arasında bire bir eşleştirme. | Bir Global Inside adresi birçok Inside Local adrese eşlenebilir. |
| Çeviri işleminde yalnızca IPv4 adreslerini kullanır. | Çeviri işleminde IPv4 adreslerini ve TCP veya UDP kaynak bağlantı noktası numaralarını kullanır. |
| Dış ağa erişen her bir dahili ana bilgisayar için benzersiz bir Inside Global adresi gereklidir. | Tek bir benzersiz Inside Global adresi, dış ağa erişen birçok dahili ana bilgisayar tarafından paylaşılabilir. |

Licensed to yetkin karasuugur, yetkinkrsngr@gmail.com

Şekil, bir NAT tablosunun basit bir örneğini göstermektedir. Bu örnekte, iç ağdaki dört ana bilgisayar dış ağla iletişim kuruyor. Soldaki sütun, genel adres havuzundaki NAT tarafından her ana bilgisayarın Dahili Yerel adresini çevirmek için kullanılan adresleri listeler. Dış ağa erişen dört ana bilgisayarın her biri için Inside Global

adreslerinin Inside Local adresleriyle bire bir ilişkisine dikkat edin. NAT ile, dış ağa bağlanması gereken her ana bilgisayar için bir Inside Global adresi gereklidir.

Not : NAT, tabloya başvurarak ve Inside Global adresini ana bilgisayarın ilgili Inside Local adresine geri çevirerek gelen dönüş paketlerini orijinal içindeki ana bilgisayara iletir.

| İç Global Adres | İç Yerel Adres |
|---|---|
| 209.165.200.226 | 192.168.10.10 |
| 209.165.200.227 | 192.168.10.11 |
| 209.165.200.228 | 192.168.10.12 |
| 209.165.200.229 | 192.168.10.13 |

NAT yalnızca IPv4 adreslerini değiştirirken, PAT hem IPv4 adresini hem de bağlantı noktası numarasını değiştirir. PAT ile, genellikle yalnızca bir veya çok az, herkese açık IPv4 adresi vardır. Örnek NAT tablosu, içteki dört ana bilgisayarın Inside Local adreslerini çevirmek için kullanılan bir Inside Global adresini gösterir. PAT, dört ana bilgisayarın görüşmelerini izlemek için Katman 4 bağlantı noktası numarasını kullanır.

| İç Global Adres | İç Yerel Adres |
|---|---|
| 209.165.200.226:2031 | 192.168.10.10:2031 |
| 209.165.200.226:1506 | 192.168.10.11:1506 |
| 209.165.200.226:1131 | 192.168.10.12:1131 |
| 209.165.200.226:1718 | 192.168.10.13:1718 |

**Katman 4 Segmenti Olmayan Paketler**

TCP veya UDP segmenti dışında veri taşıyan IPv4 paketleri ne olacak? Bu paketler Katman 4 bağlantı noktası numarası içermez. PAT, taşıma katmanı protokolü olarak TCP veya UDP kullanmayan, IPv4 tarafından taşınan en yaygın protokolleri çevirir. Bunlardan en yaygın olanı ICMPv4'tür. Bu tür protokollerin her biri PAT tarafından farklı şekilde ele alınır. Örneğin, ICMPv4 sorgu iletileri, yankı istekleri ve yankı yanıtları bir Sorgu Kimliği içerir. ICMPv4, bir yankı isteğini karşılık gelen yankı yanıtıyla tanımlamak için Sorgu Kimliğini kullanır. Sorgu Kimliği gönderilen her yankı isteği ile artırılır. PAT, Katman 4 port numarası yerine Sorgu Kimliğini kullanır.

Not : Diğer ICMPv4 mesajları Sorgu Kimliğini kullanmaz. TCP veya UDP bağlantı noktası numaralarını kullanmayan bu mesajlar ve diğer protokoller değişiklik gösterir ve bu müfredatın kapsamı dışındadır.

## 35.3.NAT Avantajları ve Dezavantajları

### 35.3.1.NAT'ın Avantajları

NAT, yeterli IPv4 adresine sahip olmama sorunumuzu çözer, ancak başka sorunlar oluşturabilir. Bu konu, NAT'ın avantajlarını ve dezavantajlarını ele almaktadır.

NAT, aşağıdakiler dahil birçok avantaj sağlar:

- NAT, intranetlerin özelleştirilmesine izin vererek yasal olarak kayıtlı adresleme şemasını korur. NAT, adresleri uygulama bağlantı noktası düzeyinde çoklama yoluyla korur. NAT aşırı yüklemesi (PAT) ile dahili ana bilgisayarlar, tüm harici iletişimler için tek bir genel IPv4 adresini paylaşabilir. Bu tür bir yapılandırmada, birçok dahili ana bilgisayarı desteklemek için çok az sayıda harici adres gerekir.
- NAT, genel ağa bağlantıların esnekliğini artırır. Güvenilir genel ağ bağlantıları sağlamak için birden çok havuz, yedekleme havuzu ve yük dengeleme havuzları uygulanabilir.

Lisansınız İsteyelin karadurgut,yedirinirsiz@gmail.com

- NAT, dahili ağ adresleme şemaları için tutarlılık sağlar. Özel IPv4 adresleri ve NAT kullanmayan bir ağda, genel IPv4 adres şemasını değiştirmek, mevcut ağdaki tüm ana bilgisayarların yeniden adreslenmesini gerektirir. Ana bilgisayarları yeniden adreslemenin maliyetleri önemli olabilir. NAT, mevcut özel IPv4 adres şemasının kalmasına izin verirken yeni bir genel adresleme şemasına kolay geçişe izin verir. Bu, bir kuruluşun ISS'leri değiştirebileceği ve içindeki istemcilerinden herhangi birini değiştirmesine gerek olmadığı anlamına gelir.
- RFC 1918 IPv4 adreslerini kullanan NAT, kullanıcıların ve diğer cihazların IPv4 adreslerini gizler. Bazı insanlar bunu bir güvenlik özelliği olarak kabul eder; ancak çoğu uzman NAT'ın güvenlik sağlamadığı konusunda hemfikirdir. Ağın kenarında güvenliği sağlayan şey, durum bilgisi olan bir güvenlik duvarıdır.

### 35.3.2.NAT'ın Dezavantajları

NAT'ın dezavantajları vardır. İnternetteki ana bilgisayarların, özel ağ içindeki gerçek ana bilgisayarla değil, doğrudan NAT özellikli aygıtla iletişim kuruyor gibi görünmesi, bir dizi sorun oluşturur.

NAT kullanmanın bir dezavantajı, özellikle VoIP gibi gerçek zamanlı protokoller için ağ performansıyla ilgilidir. Paket başlıkları içindeki her IPv4 adresinin çevrilmesi zaman aldığı için NAT, iletim gecikmelerini artırır. İlk paket her zaman daha yavaş bir yoldan geçerek süreç değiştirilir. Yönlendirici, çeviriye ihtiyacı olup olmadığına karar vermek için her pakete bakmalıdır. Yönlendirici IPv4 başlığını değiştirmeli ve muhtemelen TCP veya UDP başlığını değiştirmelidir. IPv4 üstbilgi sağlama toplamı, TCP veya UDP sağlama toplamı ile birlikte, her çeviri yapıldığında yeniden hesaplanmalıdır. Bir önbellek girişi varsa, kalan paketler hızlı geçişli yoldan geçer; aksi takdirde onlar da gecikir.

NAT işleminin neden olduğu iletme gecikmeleri, ISP'ler için genel IPv4 adres havuzları tükendikçe daha fazla sorun haline gelir. Birçok ISS, müşterilere genel bir IPv4 adresi yerine özel bir IPv4 adresi atamak zorunda kalıyor. Bu, müşterinin yönlendiricisinin paketi kendi özel IPv4 adresinden ISP'nin özel IPv4 adresine çevirdiği anlamına gelir. Paketi başka bir sağlayıcıya iletmeden önce, ISS, özel IPv4 adreslerini sınırlı sayıdaki genel IPv4 adreslerinden birine çevirerek tekrar NAT gerçekleştirecektir. Bu iki katmanlı NAT tercümesi süreci, Carrier Grade NAT (CGN) olarak bilinir.

NAT kullanmanın diğer bir dezavantajı, uçtan-uca adreslemenin kaybolmasıdır. Bu, uçtan uca ilke olarak bilinir. Birçok internet protokolü ve uygulaması, kaynaktan hedefe uçtan uca adreslemeye bağlıdır. Bazı uygulamalar NAT ile çalışmaz. Örneğin, dijital imzalar gibi bazı güvenlik uygulamaları, hedefe ulaşmadan önce kaynak IPv4 adresi değiştiğinden başarısız olur. Nitelikli bir etki alanı adı yerine fiziksel adresler kullanan uygulamalar, NAT yönlendiricisi üzerinden çevrilen hedeflere ulaşmaz. Bazen bu sorun, statik NAT eşlemeleri uygulanarak önlenebilir.

Uçtan uca IPv4 izlenebilirliği de kaybolur. Birden çok NAT atlamasında çok sayıda paket adresi değişikliğine uğrayan paketleri izlemek çok daha zor hale gelir ve sorun gidermeyi zorlaştırır.

NAT kullanımı ayrıca IPsec gibi tünel oluşturma protokollerinin kullanımını karmaşıklaştırır, çünkü NAT başlıklardaki değerleri değiştirerek bütünlük kontrollerinin başarısız olmasına neden olur.

Dış ağdan TCP bağlantılarının başlatılmasını gerektiren hizmetler veya UDP kullananlar gibi durum bilgisi olmayan protokoller bozulabilir. NAT yönlendirici bu tür protokolleri destekleyecek şekilde yapılandırılmadıkça, gelen paketler hedeflerine ulaşamaz. Bazı protokoller, katılan ana bilgisayarlar arasında bir NAT örneğini barındırabilir (örneğin, pasif mod FTP), ancak her iki sistem de NAT ile internetten ayrıldığında başarısız olur.

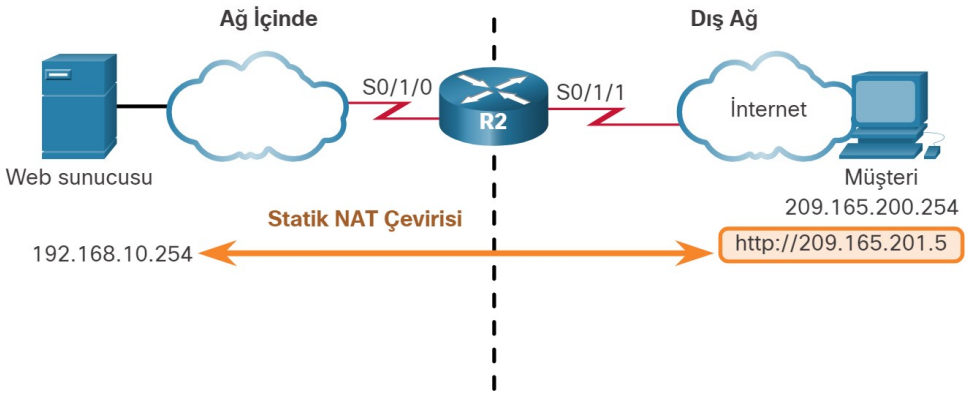
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 35.4.Statik NAT

### 35.4.1.Statik NAT Senaryosu

Bu konuda, statik NAT'ı nasıl yapılandıracağınızı ve doğrulayacağınızı öğreneceksiniz. Statik NAT, bir iç adres ile bir dış adres arasında bire bir eşleşmedir. Statik NAT, harici cihazların statik olarak atanmış genel adresi kullanarak dahili cihazlara bağlantı başlatmasına izin verir. Örneğin, bir dahili web sunucusu, dış ağlardan erişilebilmesi için belirli bir dahili global adrese eşlenebilir.

Şekil, özel bir IPv4 adresine sahip bir web sunucusu içeren bir iç ağı göstermektedir. Router R2, dış ağdaki (internet) cihazların web sunucusuna erişmesine izin vermek için statik NAT ile yapılandırılmıştır. Dış ağdaki istemci, genel bir IPv4 adresi kullanarak web sunucusuna erişir. Statik NAT, genel IPv4 adresini özel IPv4 adresine çevirir.




### 35.4.2.Statik NAT'ı Yapılandırma

Statik NAT çevirilerini yapılandırırken iki temel görev vardır:

1. Adım . İlk görev, iç yerel adres ile iç genel adresler arasında bir eşleme oluşturmaktır. Örneğin, şekildeki 192.168.10.254 dahili yerel adres ve 209.165.201.5 dahili genel adres, statik bir NAT çevirisi olarak yapılandırılmıştır.

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
```

2. Adım . Eşleme yapılandırıldıktan sonra, çeviriye katılan arayüzler NAT'a göre içeride veya dışarıda yapılandırılır. Örnekte, R2 Seri 0/1/0 arayüzü bir iç arayüz ve Seri 0/1/1 bir dış arayüzdür.

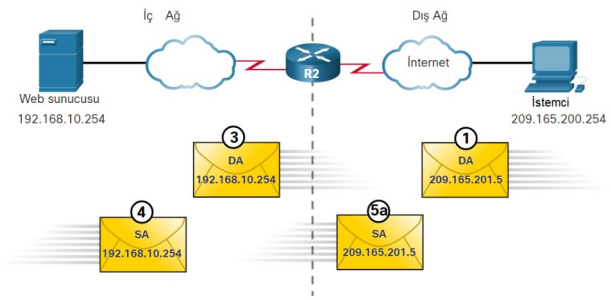
```
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Bu yapılandırmayla, yapılandırılmış yerel IPv4 adresinden (192.168.10.254) R2'nin iç arayüzüne (Seri 0/1/0) gelen paketler çevrilir ve ardından dış ağa iletilir. Küresel IPv4 adresi (209.165.201.5) içinde yapılandırılan R2'nin (Seri 0/1/1) dış arayüzüne gelen paketler, iç yerel adrese (192.168.10.254) çevrilir ve ardından ağ içinde iletilir.

Licensed to yetkin karasungur yetkinkrsnr@gmail.com

### Statik NAT'ı Analiz Etme

Önceki yapılandırmayı kullanan şekil, istemci ile web sunucusu arasındaki statik NAT çeviri sürecini gösterir. Genellikle statik çeviriler, dış ağdaki (internet) istemcilerin iç ağdaki sunuculara erişmesi gerektiğinde kullanılır.




1. İstemci, web sunucusuna bir bağlantı açmak istiyor. İstemci, 209.165.201.5 genel IPv4 hedef adresini kullanarak web sunucusuna bir paket gönderir. Bu, web sunucusunun iç genel adresidir.
2. R2'nin NAT dış arayüzünde istemciden aldığı ilk paket, R2'nin NAT tablosunu kontrol etmesine neden olur. 209.165.201.5 hedef IPv4 adresi NAT tablosunda bulunur ve 192.168.10.254'e çevrilir.
3. R2, 209.165.201.5 iç global adresini 192.168.10.254 iç yerel adresle değiştirir. R2 daha sonra paketi web sunucusuna iletir.
4. Web sunucusu paketi alır ve istemciye, yanıt paketinin kaynak adresi olarak içerideki yerel adresi 192.168.10.254 kullanarak yanıt verir.
5. (a) R2, paketi web sunucusundan, web sunucusunun dahili yerel adresinin kaynak adresi olan 192.168.10.254 ile NAT iç arayüzünde alır.
   (b) R2, NAT tablosunda yerel adresin tercümesini kontrol eder. Adres NAT tablosunda bulunur. R2, 192.168.10.254 kaynak adresini 209.165.201.5 dahili genel adresine çevirir ve paketi istemciye iletir.
6. (Gösterilmiyor) İstemci paketi alır ve konuşmaya devam eder. NAT yönlendiricisi, her paket için Adım 2 ila 5b'yi gerçekleştirir.

## 35.4.3.Statik NAT'ı Doğrulama

NAT işlemini doğrulamak için **show ip nat translation** komutunu çalıştırın. Bu komut aktif NAT çevirilerini gösterir. Örnek, statik bir NAT yapılandırması olduğundan, çeviri, herhangi bir etkin iletişimden bağımsız olarak her zaman NAT tablosunda mevcuttur.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local     Outside global
---  209.165.201.5       192.168.10.254     ---               ---
Total number of translations: 1
```

Komut etkin bir oturum sırasında verilirse, çıktı ayrıca aşağıdaki örnekte gösterildiği gibi dış aygıtın adresini de gösterir.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local        Outside global
tcp  209.165.201.5       192.168.10.254     209.165.200.254      209.165.200.254
---  209.165.201.5       192.168.10.254       ---                  ---
Total number of translations: 2
```

Diğer bir yararlı komut, toplam etkin çevirilerin sayısı, NAT yapılandırma parametreleri, havuzdaki adreslerin sayısı ve ayrılan adreslerin sayısı hakkındaki bilgileri görüntüleyen **show ip nat statistics** komutudur.

NAT çevirisinin çalıştığını doğrulamak için, test etmeden önce **clear ip nat statistics** komutunu kullanarak geçmiş çevirilerden istatistikleri temizlemek en iyisidir .

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 0  Misses: 0
(output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

İstemci web sunucusuyla bir oturum kurduktan sonra, **show ip nat statistics** , iç (Seri0/1/0) arayüzde dört kayıt (hit) artışını gösterir. Bu, statik NAT çevirisinin R2'de gerçekleştiğini doğrular.

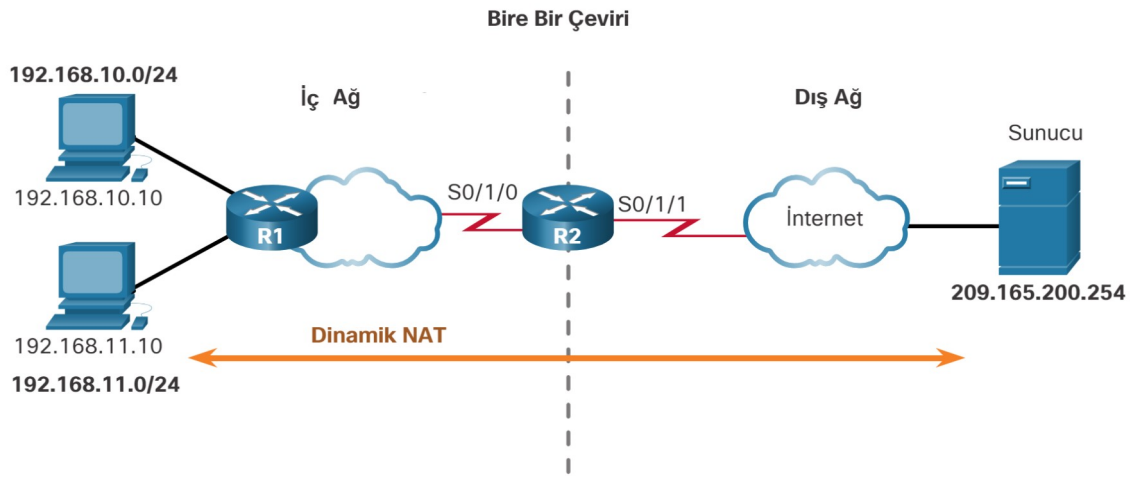
```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 1
(output omitted)
```

## 35.5.Dynamic NAT

### 35.5.1.Dinamik NAT Senaryosu

Bu konuda, dinamik NAT'ı nasıl yapılandıracağınızı ve doğrulayacağınızı öğreneceksiniz. Statik NAT, bir dahili yerel adres ile bir dahili global adres arasında kalıcı bir eşleme sağlasa da, dinamik NAT otomatik olarak iç yerel adresleri global adreslere eşler. Genel adresler içindeki bunlar tipik olarak genel IPv4 adresleridir. Dinamik NAT, statik NAT gibi, NAT'a katılan iç ve dış arabirimlerin **ip nat inside** ve **ip nat outside** arabirim yapılandırma komutlarıyla yapılandırılmasını gerektirir. Ancak, statik NAT tek bir adrese kalıcı bir eşleme oluşturduğunda, dinamik NAT bir adres havuzu kullanır.

Şekilde gösterilen örnek topoloji, RFC 1918 özel adres alanından adresleri kullanan bir iç ağa sahiptir. Yönlendirici R1'e bağlı iki LAN vardır: 192.168.10.0/24 ve 192.168.11.0/24. Sınır yönlendiricisi olan Router R2, 209.165.200.226 ile 209.165.200.240 arasındaki genel IPv4 adreslerinden oluşan bir havuz kullanılarak dinamik NAT için yapılandırılmıştır.



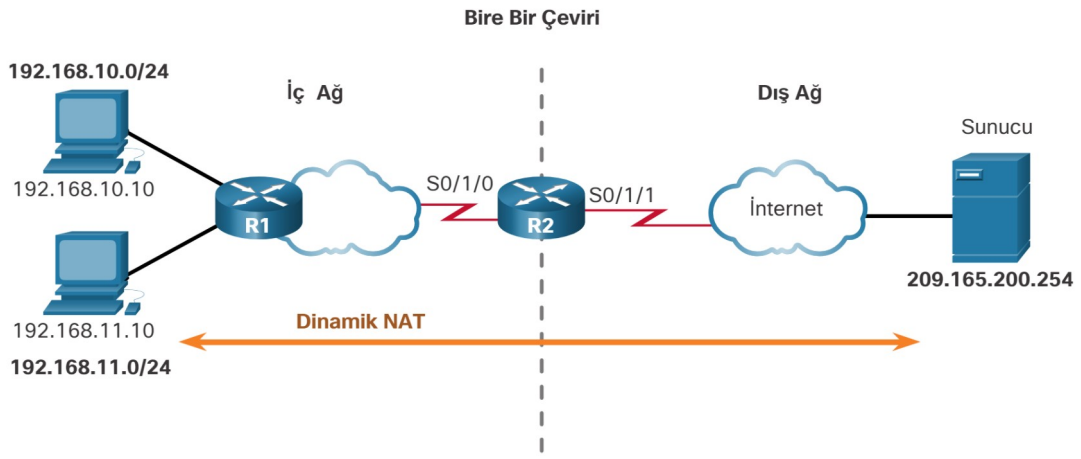

Genel IPv4 adresleri havuzu (iç global adres havuzu ), ilk gelene ilk hizmet esasına göre iç ağdaki herhangi bir cihaz tarafından kullanılabilir. Dinamik NAT ile tek bir iç adres, tek bir dış adrese çevrilir. Bu tür bir çeviri ile, havuzda, dış ağa eşzamanlı erişime ihtiyaç duyan tüm dahili cihazları barındıracak yeterli adres bulunmalıdır. Havuzdaki tüm adresler kullanımdaysa, bir aygıtın dış ağa erişmeden önce uygun bir adres beklemesi gerekir.

Not : Genel ve özel IPv4 adresleri arasında çeviri yapmak, NAT'ın açık arayla en yaygın kullanımıdır. Ancak, IPv4 adres çifti arasında NAT çevirileri gerçekleşebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 35.5.2.Dinamik NAT'ı Yapılandırma

Şekilde, NAT yapılandırmasının 192.168.0.0/16 ağındaki tüm ana bilgisayarlar için çeviriye izin verdiği örnek bir topoloji gösterilmektedir. Bu, ana bilgisayarlar S0/1/0 arayüzüne giren ve S0/1 /1'den çıkan trafik oluşturduğunda, 192.168.10.0 ve 192.168.11.0 LAN'ları içerir. Yerel adreslerin içindeki ana bilgisayar, 209.165.200.226 ile209.165.200.240 aralığında kullanılabilir bir havuz adresine çevrilir.




1.Adım

**ip nat pool** komutunu kullanarak çeviri için kullanılacak adres havuzunu tanımlayın . Bu adres havuzu tipik olarak bir genel adresler grubudur. Adresler, havuzun başlangıç IPv4 adresi ve bitiş IPv4 adresi belirtilerek tanımlanır. Ağ maskesi veya önek uzunluğu anahtar sözcüğü, hangi adres bitlerinin ağa ait olduğunu ve bu adres aralığı için hangi bitlerin ana bilgisayara ait olduğunu belirtir.

Senaryoda, NAT-POOL1 havuz adı altında genel IPv4 adreslerinden oluşan bir havuz tanımlayın.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
```

2.Adım

Yalnızca çevrilecek adresleri tanımlamak (izin vermek) için standart bir ACL yapılandırın. Fazla izin veren bir ACL, öngörülemeyen sonuçlara yol açabilir. Her ACL'nin sonunda örtük **deny all** ifadesi olduğunu unutmayın .

Senaryoda, hangi adreslerin çevrilmeye uygun olduğunu tanımlayın.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

3.Adım

Aşağıdaki komut sözdizimini kullanarak ACL'yi havuza bağlayın:

Router(config)# **ip nat inside source list** *{access-list-number | access-list-name}* **pool** *pool-name*

Bu yapılandırma, yönlendirici tarafından hangi cihazların ( listenin ) hangi adresleri ( havuz ) aldığını belirlemek için kullanılır . Senaryoda NAT-POOL1'i ACL 1 ile bağlayın.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

4.Adım

NAT ile ilgili olarak hangi arayüzlerin içeride olduğunu belirleyin; bu, iç ağa bağlanan herhangi bir arayüz olacaktır.

Senaryoda, 0/1/0 seri arayüzünü bir NAT arayüzü olarak tanımlayın.

```
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
```

5.Adım

NAT ile ilgili olarak hangi arayüzlerin dışarıda olduğunu belirleyin; bu, dış ağa bağlanan herhangi bir arayüz olacaktır.

Senaryoda, 0/1/1 seri numaralı arabirimi dış NAT arabirimi olarak tanımlayın.

```
R2(config)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

## 35.5.3.Dinamik NAT'ı Doğrulama

**show ip nat translations** komutunun çıktısı, yapılandırılmış olan tüm statik çevirileri ve trafik tarafından oluşturulan dinamik çevirileri görüntüler.

```
R2# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 209.165.200.228    192.168.10.10      ---                ---
--- 209.165.200.229    192.168.11.10      ---                ---
R2#
```

**verbose** anahtar sözcüğün eklenmesi, girdinin ne kadar süre önce oluşturulduğu ve kullanıldığı dahil olmak üzere her çeviri hakkında ek bilgi görüntüler.

```
R2# show ip nat translation verbose
Pro Inside global      Inside local       Outside local      Outside global
tcp 209.165.200.228    192.168.10.10      ---                ---
    create 00:02:11, use 00:02:11 timeout:86400000, left 23:57:48, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 10, lc_entries: 0
tcp 209.165.200.229    192.168.11.10      ---                ---
    create 00:02:10, use 00:02:10 timeout:86400000, left 23:57:49, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 12, lc_entries: 0
R2#
```

Varsayılan olarak, zamanlayıcılar genel yapılandırma modunda **ip nat translation timeout** *timeout-seconds* komutuyla yeniden yapılandırılmadıkça, çeviri girişleri 24 saat sonra zaman aşımına uğrar .

Zaman aşımı süresi dolmadan dinamik girdileri temizlemek için, **clear ip nat translation** ayrıcalıklı EXEC modu komutunu şekilde gösterildiği gibi kullanın. (sonuna * işareti ekleyerek)

```
R2# clear ip nat translation *
R2# show ip nat translation
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Diğer bir kullanışlı komut, **show ip nat statistics** komutudur , toplam aktif çevirilerin sayısı, NAT yapılandırma parametreleri, havuzdaki adres sayısı ve kaç adresin tahsis edildiği hakkında bilgi görüntüler.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 0 extended)
Peak translations: 4, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 47  Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 4
 pool NAT-POOL1: netmask 255.255.255.224
        start 209.165.200.226 end 209.165.200.240
        type generic, total addresses 15, allocated 2 (13%), misses 0
(output omitted)
R2#
```

Alternatif olarak, **show running-config** komutunu kullanabilir ve gerekli değerlerle NAT, ACL, arabirim veya havuz komutlarını arayabilirsiniz . Bunları dikkatlice inceleyin ve keşfedilen hataları düzeltin. Örnek, NAT havuzu yapılandırmasını gösterir.

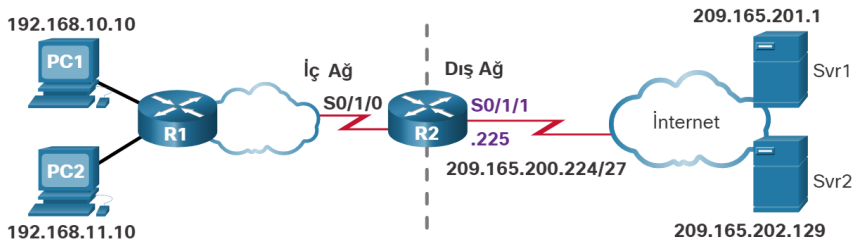
```
R2# show running-config | include NAT
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
ip nat inside source list 1 pool NAT-POOL1
```

## 35.6.PAT

### 35.6.1.PAT Senaryosu

Bu konuda, PAT'i nasıl yapılandıracağınızı ve doğrulayacağınızı öğreneceksiniz. ISS'nin genel IPv4 adreslerini nasıl tahsis ettiğine bağlı olarak PAT'ı yapılandırmanın iki yolu vardır. İlk durumda ISP, kuruluşun ISP'ye bağlanması için gerekli olan tek bir genel IPv4 adresini tahsis eder ve diğerinde kuruluşa birden fazla genel IPv4 adresi tahsis eder.

Her iki yöntem de şekilde gösterilen senaryo kullanılarak gösterilecektir.




| NAT Tablosu | | | |
|---|---|---|---|
| **İç Yerel Adres** | **İç Global Adres** | **Dış Global Adres** | **Dış Yerel Adres** |
| 192.168.10.10:1444 | 209.165.200.225:1444 | 209.165.201.1:80 | 209.165.201.1:80 |
| 192.168.11.10:1444 | 209.165.200.225:1445 | 209.165.202.129:80 | 209.165.202.129:80 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**PAT'ı Tek Bir IPv4 Adresi Kullanacak Şekilde Yapılandırma**

PAT'i tek bir IPv4 adresi kullanacak şekilde yapılandırmak için, **overload** anahtar kelimesini **ip nat inside source** komutuna eklemeniz yeterlidir. Yapılandırmanın geri kalanı, PAT ile birden çok ana bilgisayarın internete erişmek için aynı genel IPv4 adresini kullanabilmesi dışında statik ve dinamik NAT yapılandırmasına benzerdir.

Örnekte, yönlendirici R2 üzerinden internete trafik gönderen 192.168.0.0/16 (ACL 1 ile eşleşen) ağındaki tüm ana bilgisayarlar, 209.165.200.225 IPv4 adresine (S0 / 1/1 arabiriminin IPv4 adresi) çevrilecektir. **overload** anahtar sözcüğü yapılandırıldığı için trafik akışları NAT tablosundaki bağlantı noktası numaralarıyla tanımlanacaktır.

```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/1
R2(config-if)# ip nat outside
```

**PAT'ı Adres Havuzunu Kullanacak Şekilde Yapılandırma**

Bir ISS, bir kuruluşa birden fazla genel IPv4 adresi tahsis edebilir. Bu senaryoda, kuruluş PAT'i çeviri için IPv4 genel adres havuzunu kullanacak şekilde yapılandırabilir.

Bir siteye birden fazla genel IPv4 adresi verildiyse, bu adresler PAT tarafından kullanılan bir havuzun parçası olabilir. Küçük adres havuzu, internete erişmek için aynı genel IPv4 adresini kullanan birden çok ana bilgisayarla çok sayıda cihaz arasında paylaşılır. PAT için dinamik bir NAT adres havuzu için yapılandırmak, **overload** anahtar kelimesiyle ve **ip nat inside source** komutlarıyla gerçekleştirilir.

Bu yapılandırma için bir önceki topoloji kullanılmıştır.

Örnekte, NAT-POOL2, 192.168.0.0/16'nın çevrilmesine izin vermek için bir ACL'ye bağlıdır. Bu ana bilgisayarlar havuzdan bir IPv4 adresini paylaşabilir çünkü PAT **overload** anahtar kelimesiyle etkinleştirilir .

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)#
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial0/1/1
R2(config-if)# ip nat outside
R2(config-if)# end
R2#
```

## 35.6.2.PAT Yapılandırmasını Doğrulama

Yönlendirici R2, 192.168.0.0/16 istemcilere PAT sağlamak üzere yapılandırılmıştır. Dahili ana bilgisayarlar yönlendirici R2'den internete çıktığında, benzersiz bir kaynak bağlantı noktası numarasıyla PAT havuzundan bir IPv4 adresine çevrilirler.

Statik ve dinamik NAT'ı doğrulamak için kullanılan komutların aynısı, örnek çıktıda gösterildiği gibi PAT'ı doğrulamak için kullanılır. show ip nat translations komutu farklı web sunucularına iki farklı ana çevirileri görüntüler. İki farklı iç ana bilgisayara 209.165.200.226 ile aynı IPv4 adresinin tahsis edildiğine dikkat edin ( içi genel adresde). NAT tablosundaki kaynak port numaraları iki işlemi birbirinden ayırır.

Licensed to yetkin karaşungur, yetkinkrsngr@gmail.com

```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local      Outside global
tcp 209.165.200.225:1444  192.168.10.10:1444  209.165.201.1:80   209.165.201.1:80
tcp 209.165.200.225:1445  192.168.11.10:1444  209.165.202.129:80 209.165.202.129:80
R2#
```

Bir sonraki örnekte, **show ip nat statistics** komutu NAT-POOL2'nin her iki çeviri için tek bir adres ayırdığını doğrular. Çıktıda, etkin çevirilerin sayısı ve türü, NAT yapılandırma parametreleri, havuzdaki adres sayısı ve kaçının tahsis edildiği hakkında bilgiler yer alır.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
 pool NAT-POOL2: netmask 255.255.255.224
        start 209.165.200.225 end 209.165.200.240
        type generic, total addresses 15, allocated 1 (6%), misses 0
(output omitted)
R2#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 36.Bölüm:WAN Teknolojileri

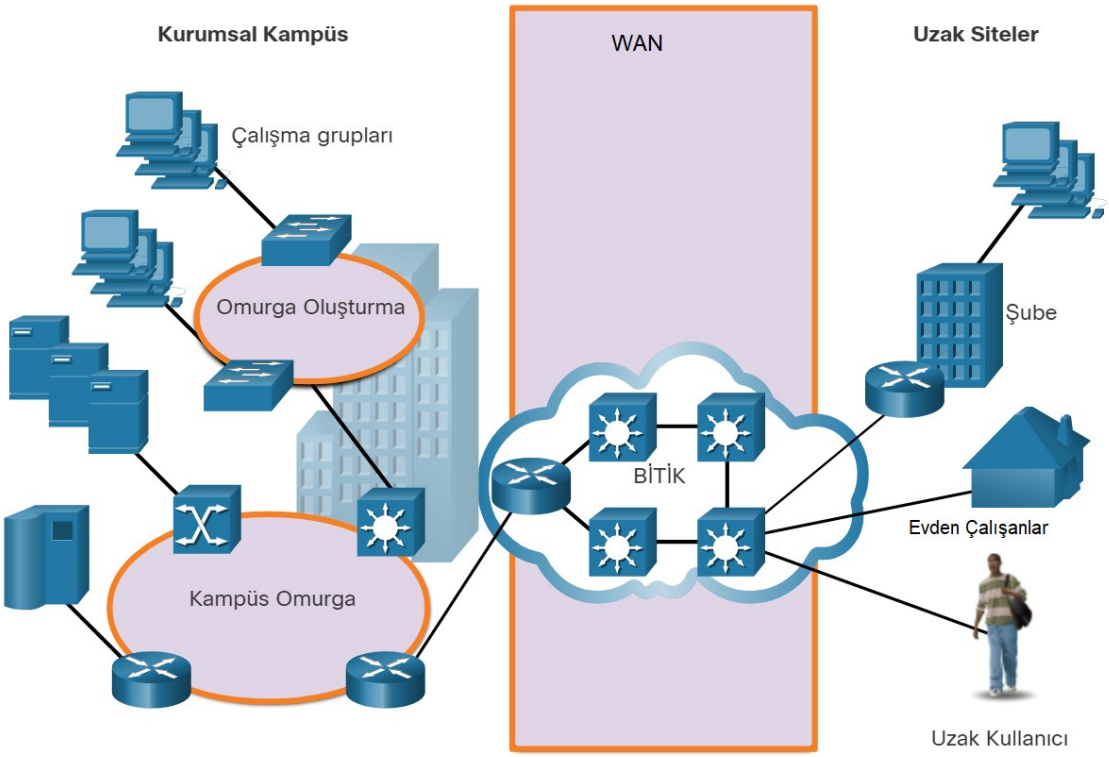
## 36.1.WAN'ların Kullanım Amacı

### 36.1.1.LAN'lar ve WAN'lar

İster işte ister evde, hepimiz Yerel Alan Ağlarını-Local Area Network (LAN) kullanıyoruz. Ancak, LAN'lar küçük bir coğrafi alanla sınırlıdır.

LAN sınırlarının ötesine bağlanmak için bir Geniş Alan Ağı-Wide Area Network (WAN) gereklidir. WAN, nispeten büyük bir coğrafi alana yayılan bir telekomünikasyon ağıdır. Bir WAN, bir LAN'ın coğrafi kapsamının ötesinde çalışır.

Şekilde, WAN hizmetlerinin bir kurumsal kampüs ağını şube sitelerindeki, evden çalışanlar ve uzaktaki kullanıcıların uzak LAN'lara bağlanması gerekir.




Tablo,

LAN'lar ve WAN'lar arasındaki farkları vurgular.

| Yerel Alan Ağları (LAN'lar) | Geniş Alan Ağları (WAN'lar) |
|---|---|
| LAN'lar, küçük bir coğrafi alan (yani, ev ağı, ofis ağı, bina ağı veya kampüs ağı) içinde ağ hizmetleri sağlar. | WAN'lar, geniş coğrafi alanlarda (yani şehirler, ülkeler ve kıtalar içinde ve arasında) ağ hizmetleri sağlar. |
| LAN'lar, yerel bilgisayarları, çevre birimlerini ve diğer cihazları birbirine bağlamak için kullanılır. | WAN'lar uzak kullanıcıları, ağları ve siteleri birbirine bağlamak için kullanılır. |
| LAN, bir kuruluşa veya ev kullanıcısına aittir ve bu kuruluş tarafından yönetilir. | WAN'lar internet hizmeti, telefon, kablo ve uydu sağlayıcılarına aittir ve bunlar tarafından yönetilir. |
| Ağ altyapısı maliyetleri dışında, LAN kullanmak için herhangi bir ücret alınmaz. | WAN hizmetleri ücret karşılığında verilmektedir. |
| LAN'lar, kablolu Ethernet ve Wi-Fi hizmetlerini kullanarak yüksek bant genişliği hızları sağlar. | WAN sağlayıcıları, karmaşık fiziksel ağları kullanarak uzun mesafelerde düşük ila yüksek bant genişliği hızları sunar. |

* Licensed to yetkin karasungur, yetkinksnq@gmail.com

## 36.1.2.Özel ve Genel WAN'lar

WAN'lar, aşağıdaki gibi çeşitli farklı kuruluş türleri tarafından oluşturulabilir:

- Farklı konumlardaki kullanıcıları birbirine bağlamak isteyen bir kuruluş
- Müşterileri internete bağlamak isteyen bir İSS (İnternet Servis Sağlayıcı)
- İSS'leri birbirine bağlamak isteyen bir İSS veya telekomünikasyon şirketi

Özel WAN, tek bir müşteriye ayrılmış bir bağlantıdır. Bu, aşağıdakileri sağlar:

- Garantili hizmet seviyesi
- Tutarlı bant genişliği
- Güvenlik

Genel bir WAN bağlantısı tipik olarak internet kullanan bir ISS veya telekomünikasyon servis sağlayıcısı tarafından sağlanır. Bu durumda, hizmet seviyeleri ve bant genişliği değişebilir ve paylaşılan bağlantılar güvenliği garanti etmez.

## 36.1.3.WAN Topolojileri

Fiziksel topolojiler, veriler bir kaynaktan bir hedefe giderken kullanılan fiziksel ağ altyapısını tanımlar. WAN'larda kullanılan fiziksel WAN topolojisi karmaşıktır ve çoğunlukla kullanıcılar tarafından bilinmemektedir. New York'taki bir kullanıcının Tokyo, Japonya'daki bir kullanıcıyla bir video konferans görüşmesi düzenlediğini düşünün. Kullanıcının New York'taki internet bağlantısı dışında, video görüşmesini desteklemek için gereken tüm gerçek fiziksel bağlantıları belirlemek mümkün olmayacaktır.

Bunun yerine, WAN topolojileri mantıksal bir topoloji kullanılarak tanımlanmıştır. Mantıksal topolojiler, kaynak ve hedef arasındaki sanal bağlantıyı tanımlar. Örneğin, New York ve Japonya'daki kullanıcı arasındaki video konferans görüşmesi mantıklı bir noktadan noktaya bağlantı olacaktır.

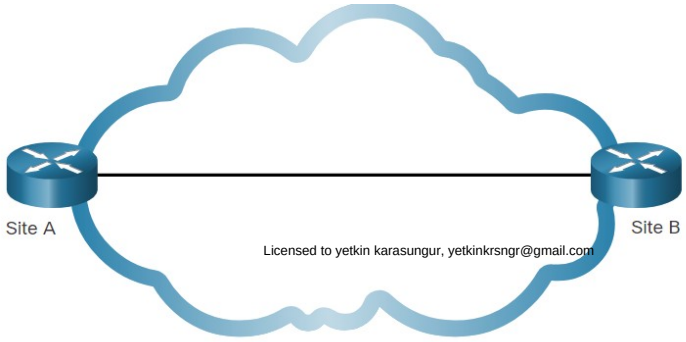
WAN'lar aşağıdaki mantıksal topoloji tasarımları kullanılarak uygulanır:

- Noktadan Noktaya (Point to Point)Topoloji
- Hub-and-Spoke Topolojisi
- Çift bağlantılı (Dual Homed)Topoloji
- Tam Örgü (Full Meshed)Topoloji
- Kısmen Mesh Topoloji

Not : Büyük ağlar genellikle bu topolojilerin bir kombinasyonunu kullanır.

**Noktadan Noktaya Topoloji**

Şekilde gösterildiği gibi bir noktadan noktaya topoloji, iki uç nokta arasında noktadan noktaya bir devre kullanır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

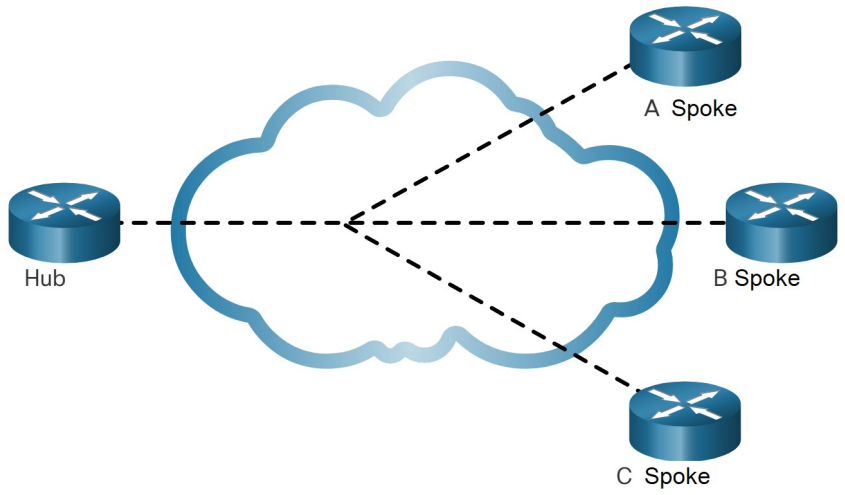
Noktadan noktaya bağlantılar genellikle kurumsal uç noktadan sağlayıcı ağlarına özel, kiralık hat bağlantılarını içerir. Noktadan noktaya bağlantı, servis sağlayıcı ağı üzerinden bir Katman 2 taşıma hizmetini içerir. Bir siteden gönderilen paketler diğer siteye teslim edilir ve bunun tersi de geçerlidir. Noktadan noktaya bağlantı, müşteri ağına şeffaftır. İki uç nokta arasında doğrudan fiziksel bir bağlantı varmış gibi görünüyor.

Çok sayıda noktadan noktaya bağlantı gerekliyse pahalı hale gelebilir.

**Hub-and-Spoke Topolojisi**

Bir hub ve bağlı bileşen topolojisi, hub yönlendiricideki tek bir arabirimin tüm bağlı devre devreleri tarafından paylaşılmasını sağlar. Spoke yönlendiriciler, sanal devreler ve yönlendirilmiş alt arabirimler kullanılarak hub yönlendirici aracılığıyla birbirine bağlanabilir. Şekilde, bir WAN bulutu üzerinden bir hub yönlendiricisine bağlanan üç kollu yönlendiriciden oluşan örnek bir hub ve bağlı bileşen topolojisi gösterilmektedir.

Bir hub ve bağlı bileşen topolojisi, tek bağlantılı bir topolojidir. Yalnızca bir hub yönlendirici vardır ve tüm iletişim bunun üzerinden geçmelidir. Bu nedenle, bağlı yönlendiriciler birbirleriyle yalnızca hub yönlendirici aracılığıyla iletişim kurabilir. Sonuç olarak, hub yönlendirici tek bir hata noktasını temsil eder. Başarısız olursa, spokelar arası iletişim de başarısız olur.

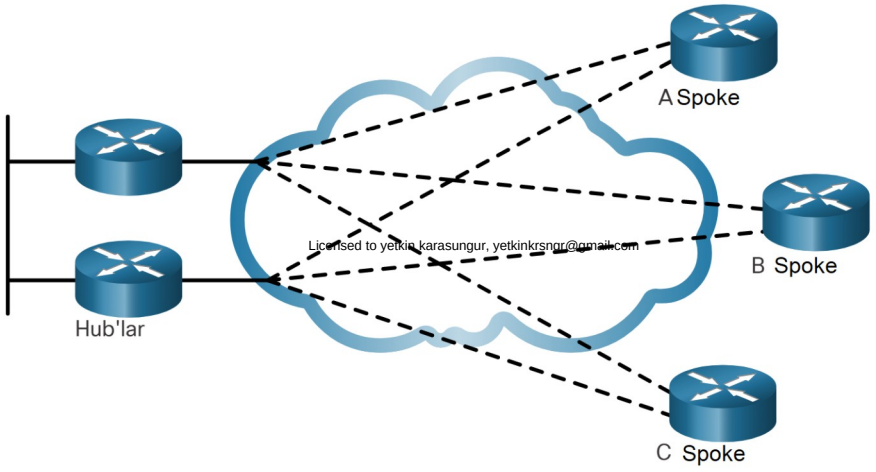



**Çift Bağlantılı Topoloji**

Çift bağlantılı bir topoloji artıklık sağlar. Şekilde gösterildiği gibi, iki hub yönlendiricisi çift bağlantılıdır ve bir WAN bulutu üzerindeki üç kollu yönlendiriciye yedek olarak bağlıdır.

Çift bağlantılı topolojilerin avantajı, gelişmiş ağ yedekliliği, yük dengeleme, dağıtılmış bilgi işlem ve işleme ve yedekleme hizmeti sağlayıcı bağlantılarını uygulama becerisi sunmalarıdır.

Dezavantajı, tek bağlantılı topolojilere göre uygulanmasının daha pahalı olmasıdır. Bunun nedeni, ek yönlendiriciler ve anahtarlar gibi ek ağ donanımı gerektirmeleridir. Çift bağlantılı topolojilerin uygulanması da daha zordur çünkü ek ve daha karmaşık yapılandırmalar gerektirirler.

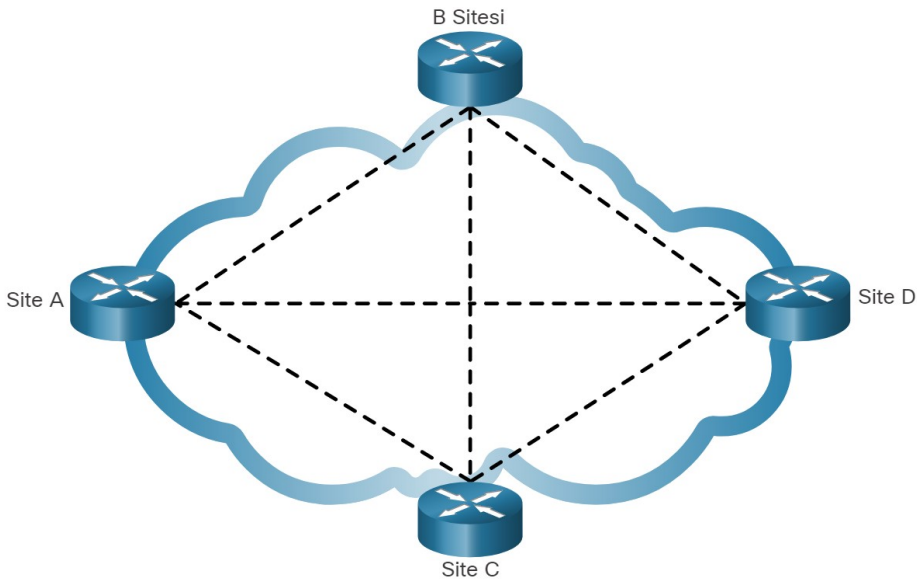


Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Tam Örgülü Topoloji

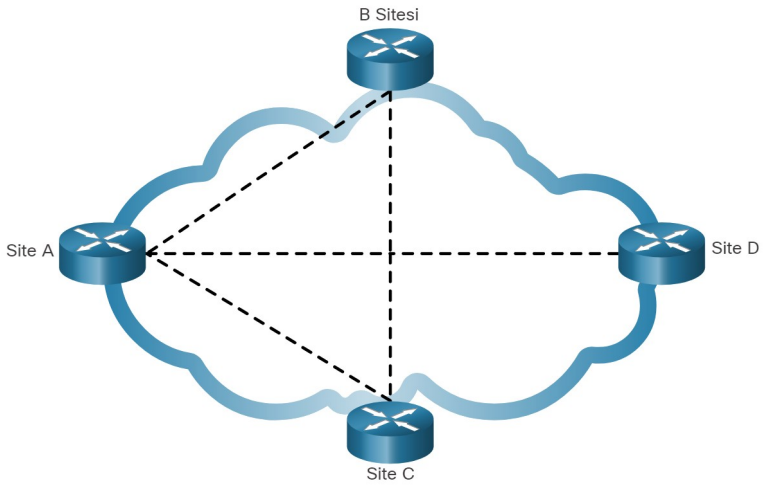
Tamamen örgülü bir topoloji, şekilde gösterildiği gibi, tüm siteleri bağlamak için birden çok sanal devre kullanır.

Bu, gösterilen en hataya dayanıklı topolojidir. Örneğin, B sitesi A sitesine olan bağlantıyı kaybederse, verileri site C veya site D üzerinden gönderebilir.




### Kısmen Mesh Topoloji

Kısmen örgülü bir topoloji birçok siteyi birbirine bağlar, ancak tüm siteleri birbirine bağlamaz. Örneğin, şekil sitelerinde A, B, C hala tamamen iç içe geçmiş durumdadır. Site D, B ve C sitelerine ulaşmak için A sitesine bağlanmalıdır.



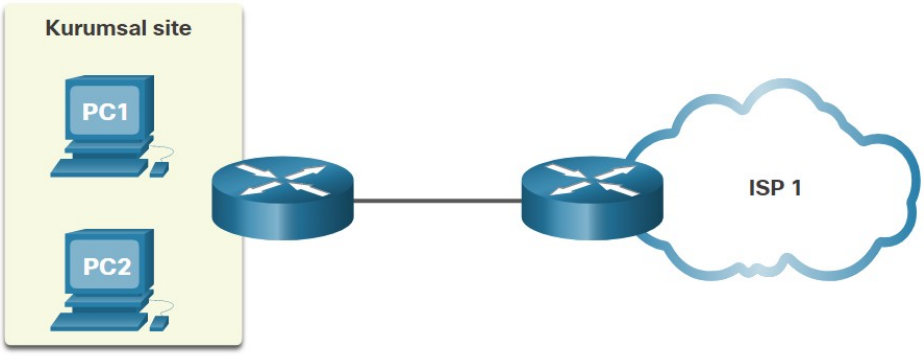

## 36.1.4.Taşıyıcı Bağlantıları

WAN tasarımının bir başka yönü, bir kuruluşun internete nasıl bağlandığıdır. Bir kuruluş genellikle bir hizmet sağlayıcıyla bir hizmet seviyesi anlaşması-Service Level Agreement (SLA) imzalar. SLA, bağlantının güvenilirliği ve kullanılabilirliği ile ilgili beklenen hizmetleri ana hatlarıyla belirtir. Servis sağlayıcı, gerçek taşıyıcı olabilir veya olmayabilir. Bir taşıyıcı, sağlayıcı ile müşteri arasındaki fiziksel bağlantı ve ekipmanın sahibidir ve bu bağlantıyı sürdürür. Tipik olarak, bir kuruluş tek veya çift taşıyıcılı bir WAN bağlantısını seçecektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

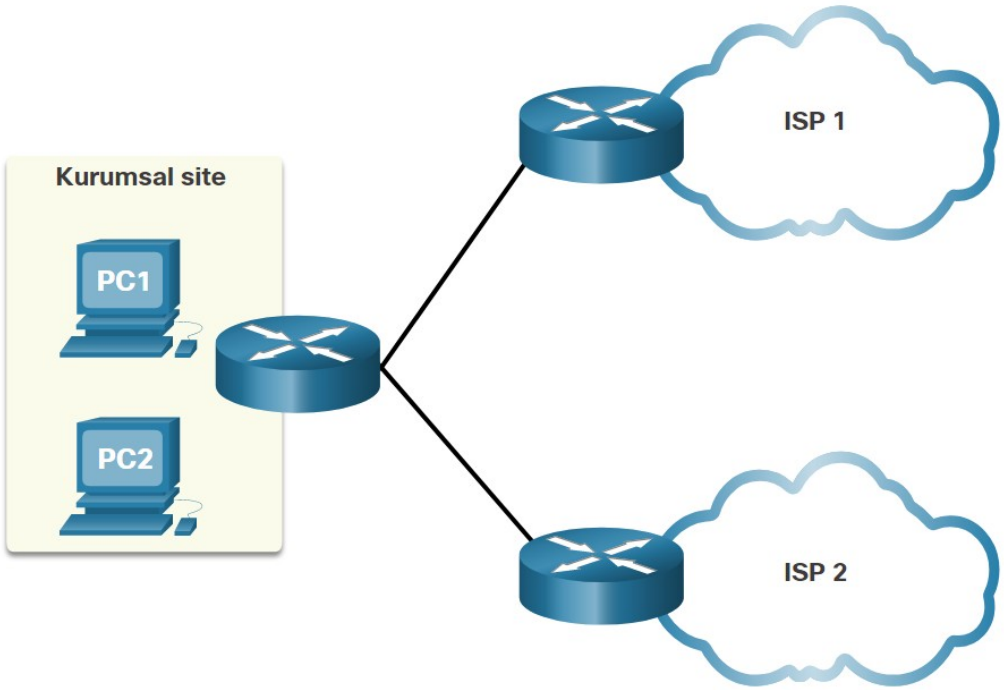
### Tek Taşıyıcı WAN Bağlantısı

Tek taşıyıcılı bağlantı, şekilde gösterildiği gibi bir kuruluşun yalnızca bir hizmet sağlayıcıya bağlanmasıdır. Kuruluş ve hizmet sağlayıcı arasında bir SLA müzakere edilir. Bu tasarımın dezavantajı, taşıyıcı bağlantısı ve servis sağlayıcının her ikisinin de tek başarısızlık noktaları olmasıdır. Taşıyıcı bağlantısı veya sağlayıcı yönlendiricisi başarısız olursa internet bağlantısı kesilir.




### Çift Taşıyıcılı WAN Bağlantısı

Çift taşıyıcılı bağlantı, şekilde gösterildiği gibi yedeklilik sağlar ve ağ kullanılabilirliğini artırır. Kuruluş, iki farklı hizmet sağlayıcıyla ayrı SLA'ları müzakere eder. Kuruluş, iki sağlayıcının her birinin farklı bir taşıyıcı kullandığından emin olmalıdır. Uygulanması daha pahalı olmasına rağmen, ikinci bağlantı yedek bağlantı olarak yedeklilik için kullanılabilir. Ağ performansını iyileştirmek ve internet trafiğini dengelemek için de kullanılabilir.




## 36.1.5.Gelişen Ağlar

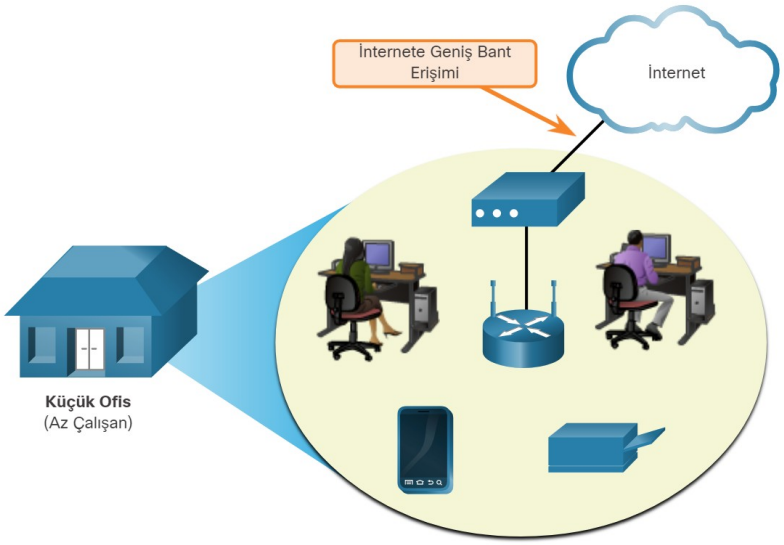
Bir şirketin ağ gereksinimleri, şirket zaman içinde büyüdükçe önemli ölçüde değişebilir. Çalışanların dağıtılması, birçok yönden maliyet tasarrufu sağlar, ancak ağa olan talepleri artırır. Bir ağ sadece işletmenin günlük operasyonel ihtiyaçlarını karşılamakla kalmaz, aynı zamanda şirket değiştikçe uyum sağlayabilmeli ve büyüyebilmelidir. Ağ tasarımcıları ve yöneticileri, ağ teknolojilerini, protokolleri ve hizmet sağlayıcılarını dikkatlice seçerek bu zorlukların üstesinden gelir. Ayrıca, çeşitli ağ tasarım teknikleri ve mimarileri kullanarak ağlarını optimize etmeleri gerekir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Ağ boyutu arasındaki farklılıkları göstermek için, küçük, yerel bir işletmeden küresel bir işletmeye doğru büyüyen Yeşil Mühendislik adlı hayali bir şirket kullanacağız. Bir çevre danışmanlık firması olan SPAN Engineering, evsel atıkları elektriğe dönüştürmek için özel bir süreç geliştirdi ve bölgesindeki yerel bir belediye yönetimi için küçük bir pilot proje geliştiriyor.

## Küçük Ağ

Şirket, şekilde gösterildiği gibi başlangıçta küçük bir ofiste çalışan 15 çalışandan oluşuyordu. Veri ve çevre birimlerini paylaşmak için kablosuz bir yönlendiriciye bağlı tek bir LAN kullandılar. İnternet bağlantısı, yerel telefon hizmeti sağlayıcıları tarafından sağlanan Dijital Abone Hattı-Digital Subscriber Line (DSL) adı verilen yaygın bir geniş bant hizmeti üzerinden yapılır. BT gereksinimlerini desteklemek için DSL sağlayıcısından hizmet sözleşmesi imzaladılar.

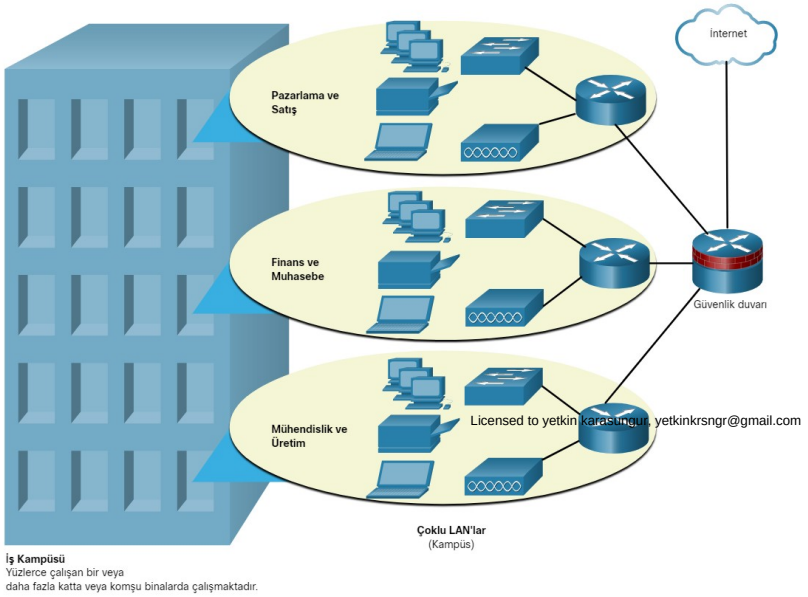



## Kampüs Ağı

Şirket, şekilde gösterildiği gibi birkaç yıl içinde büyüdü ve bir binanın birkaç katına ihtiyaç duydu.

Şirket artık bir Kampüs Alan Ağına-Campus Area Network (CAN) ihtiyaç duyuyordu. Bir CAN, sınırlı bir coğrafi alan içindeki birkaç LAN'ı birbirine bağlar. Bir kampüs ağ ortamında birden çok anahtara bağlanan çeşitli departmanları bölümlere ayırmak için birden çok LAN gereklidir.

Ağ, e-posta, veri aktarımı ve dosya depolama için özel sunucular ve web tabanlı üretkenlik araçları ve uygulamaları içerir. Güvenlik duvarı, kurumsal kullanıcılara internet erişimini güvence altına alır. İşletme artık ağı desteklemek ve sürdürmek için şirket içi BT personeline ihtiyaç duyuyor.

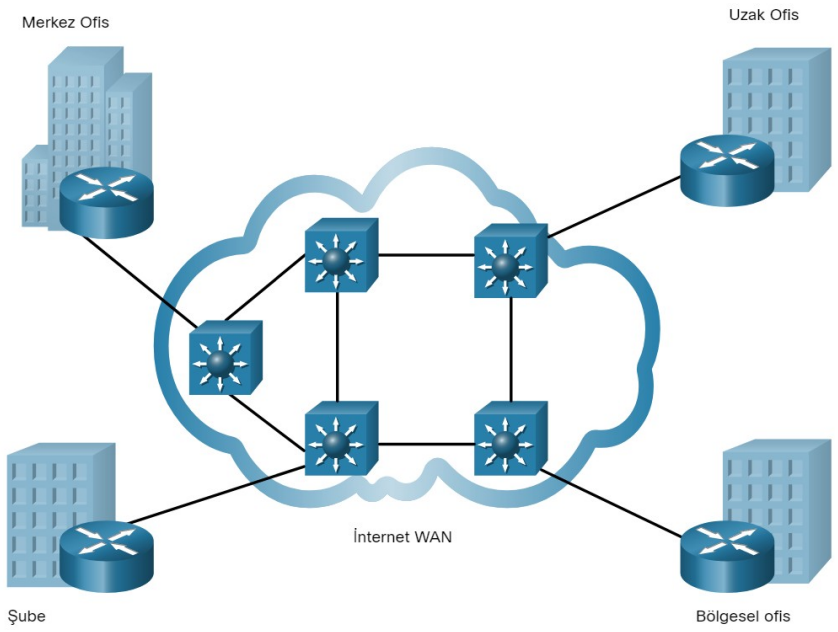


## Şube Ağı

Birkaç yıl sonra, şirket genişledi ve şehirde bir şube sitesi ve şekilde gösterildiği gibi diğer şehirlerde uzak ve bölgesel siteler ekledi.

Şirket artık şehir içindeki siteleri birbirine bağlamak için bir metropolitan alan ağına (MAN) ihtiyaç duyuyordu. MAN, LAN'dan daha büyük, ancak WAN'dan daha küçüktür.

Merkez ofise bağlanmak için, yakındaki şehirlerdeki şubeler yerel servis sağlayıcıları aracılığıyla özel ayrılmış hatlar kullandı. Diğer şehirlerdeki ve ülkelerdeki ofisler bir WAN hizmetlerini gerektirir veya uzak konumlara bağlanmak için internet hizmetlerini kullanabilir. Ancak internet, BT ekibinin ele alması gereken güvenlik ve gizlilik sorunlarını ortaya çıkarır.




## Dağıtılmış Ağ

Yeşil Mühendislik şu anda 20 yıldır faaliyet gösteriyor ve şekilde gösterildiği gibi dünya çapında ofislerde dağıtılan binlerce çalışana ulaştı.

Ağ maliyetlerini azaltmak, üretkenliği artırmak ve maliyetleri düşürmek için web-konferans, e-öğrenme ve çevrimiçi işbirliği araçları dahil olmak üzere web tabanlı uygulamaları kullanan uzaktan çalışmayı ve sanal ekipleri teşvik etti. Siteden siteye ve uzaktan erişim Sanal Özel Ağlar (VPN'ler), şirketin interneti dünyanın her yerindeki çalışanlar ve tesislerle kolay ve güvenli bir şekilde bağlanmasını sağlar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 36.2.WAN İşlemleri

### 36.2.1.WAN Standartları

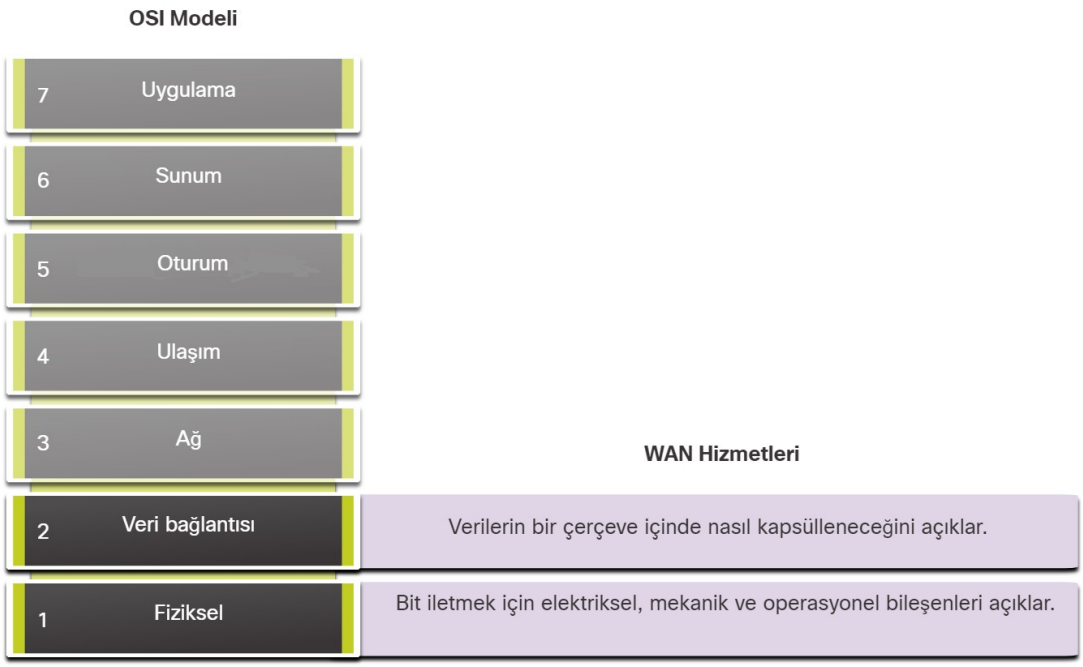
WAN kavramı uzun yıllardır piyasada. Telgraf sisteminin ilk büyük ölçekli WAN olduğunu, ardından radyo, telefon sistemi, televizyon ve şimdi de veri ağlarının geldiğini düşünün. Bu WAN'lar için geliştirilen teknolojilerin ve standartların çoğu, ağ WAN'larının temeli olarak kullanılmıştır.

Modern WAN standartları, aşağıdakiler dahil olmak üzere bir dizi tanınmış yetkili tarafından tanımlanır ve yönetilir:

- TIA/EIA - Telecommunications Industry Association and Electronic Industries Alliance
- ISO - International Organization for Standardization
- IEEE - Institute of Electrical and Electronics Engineers

### 36.2.2.OSI Modelinde WAN'lar

Çoğu WAN standardı, şekilde gösterildiği gibi fiziksel katmana (OSI Katman 1) ve veri bağlantı katmanına (OSI Katman 2) odaklanır.




Katman 1 Protokolleri

Katman 1 protokolleri, bitleri bir WAN üzerinden iletmek için gereken elektriksel, mekanik ve operasyonel bileşenleri tanımlar. Örneğin, hizmet sağlayıcılar aşağıdaki Katman 1 optik fiber protokol standartlarını kullanarak uzun mesafeleri (yani uzun mesafeyi) kapsamak için genellikle yüksek bant genişliğine sahip optik fiber ortamı kullanır:

- Synchronous Digital Hierarchy (SDH)
- Synchronous Optical Networking (SONET)
- Dense Wavelength Division Multiplexing (DWDM)

Licensed to Yetkin karasungur, yetkinkrsngr@gmail.com

SDH ve SONET temelde aynı hizmetleri sağlar ve DWDM teknolojisi kullanılarak iletim kapasiteleri artırılabilir.

Katman 2 Protokolleri

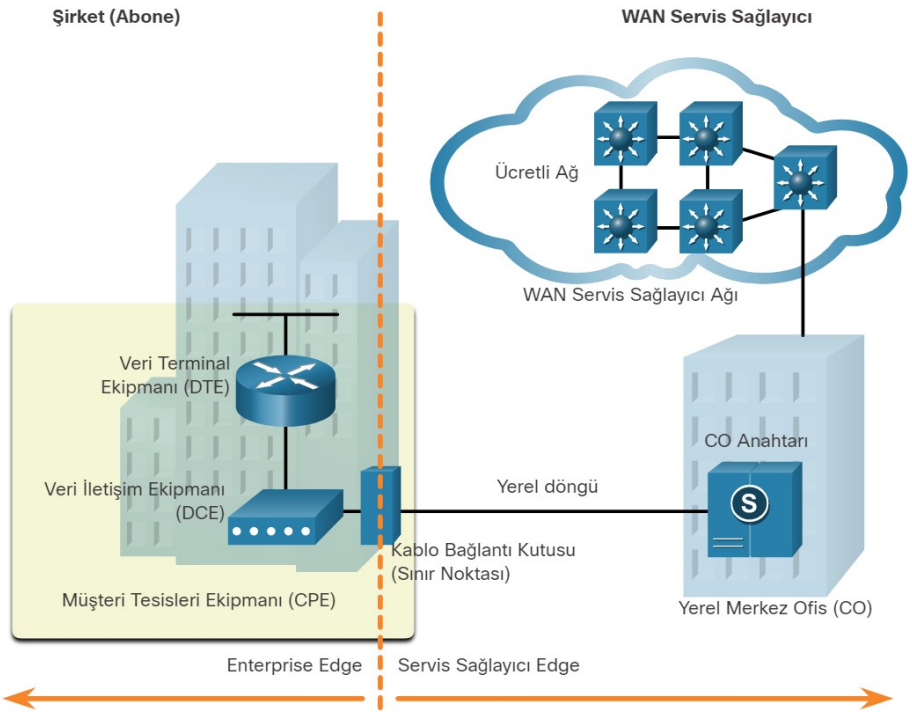
Katman 2 protokolleri, verilerin bir çerçeve içinde nasıl kapsülleneceğini tanımlar.
Yıllar içinde aşağıdakileri içeren birkaç Katman 2 protokolü geliştirilmiştir:

- Broadband (DSL ve Kablo)
- Wireless
- Ethernet WAN (Metro Ethernet)
- Multiprotocol Label Switching (MPLS)
- Point-to-Point Protocol (PPP) (daha az kullanılır)
- High-Level Data Link Control (HDLC) (daha az kullanılır)
- Frame Relay (legacy)
- Asynchronous Transfer Mode (ATM) (eski)

## 36.2.3.WAN Terimleri

WAN fiziksel katmanı, şirket ağı ile servis sağlayıcı ağı arasındaki fiziksel bağlantıları tanımlar.

Abone (yani şirket / müşteri) ile WAN hizmet sağlayıcısı arasındaki WAN bağlantılarını şekilde gösterildiği gibi tarif etmek için kullanılan belirli terimler vardır.




Şekilde gösterilen terimlerin açıklaması ve WAN ile ilgili bazı ek terimler için tabloya bakın.

| WAN Terimi | Açıklama |
|---|---|
| Data Terminal Equipment | Bu, abone LAN'larını WAN iletişim cihazına (yani DCE) bağlayan cihazdır. |
| Veri Terminal Ekipmanı (DTE) | İçerideki ana bilgisayarlar trafiğini DTE cihazına gönderir.<br>DTE, DCE aracılığıyla yerel döngüye bağlanır. |

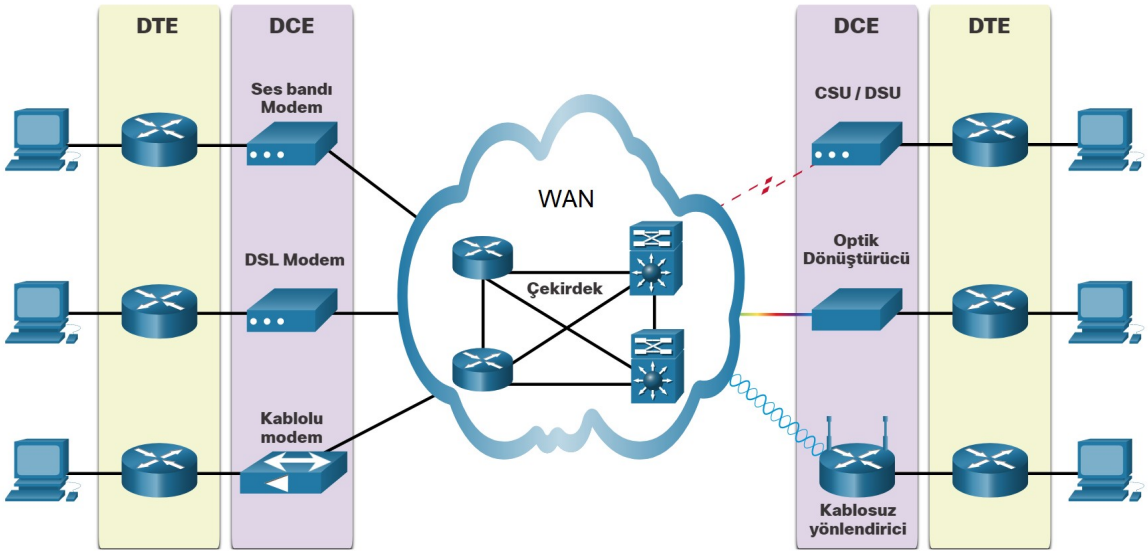
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| WAN Terimi | Açıklama |
|---|---|
| | DTE cihazı genellikle bir yönlendiricidir ancak bir ana bilgisayar veya sunucu olabilir. |
| Data Communications Equipment<br>Veri İletişim Ekipmanı (DCE) | Veri devresi sonlandırma ekipmanı olarak da adlandırılan bu, sağlayıcıyla iletişim kurmak için kullanılan cihazdır.<br><br>DCE, öncelikle aboneleri WAN bulutundaki bir iletişim bağlantısına bağlamak için bir arayüz sağlar. |
| Customer Premises Equipment<br>Müşteri Tesisleri Ekipmanı (CPE) | Bu, kurumsal uçta bulunan DTE ve DCE cihazlarıdır (yani yönlendirici, modem, optik dönüştürücü).<br><br>Abone, CPE'nin sahibidir veya CPE'yi hizmet sağlayıcıdan kiralar. |
| Point-of-Presence<br>Varlık Noktası (POP) | Bu, abonenin servis sağlayıcı şebekesine bağlandığı noktadır. |
| Demarcation Point<br>Sınır noktası | Bu, CPE'yi hizmet sağlayıcı ekipmanından resmi olarak ayıran bir bina veya kompleks içindeki fiziksel bir konumdur.<br><br>Sınır belirleme noktası, tipik olarak, CPE kablolamasını yerel döngüye bağlayan, müşteri tesislerinde bulunan bir kablo bağlantı kutusudur.<br><br>Ağ işletim sorumluluğunun aboneden servis sağlayıcıya değiştiği yeri tanımlar.<br><br>Sorunlar ortaya çıktığında, kullanıcının veya servis sağlayıcının sorun giderme veya onarımdan sorumlu olup olmadığını belirlemek gerekir. |
| Local Loop<br>Yerel Döngü (veya son mil) | Bu, CPE'yi servis sağlayıcının CO'suna bağlayan bakır veya fiber kablodur. |
| Central Office<br>Merkez Ofis (CO) | Bu, CPE'yi sağlayıcı ağına bağlayan yerel hizmet sağlayıcı tesisi veya binasıdır. |
| Toll network<br>Ücretli ağ | Buna ana taşıyıcı, uzun mesafeli, tamamen dijital, fiber optik iletişim hatları, anahtarlar, yönlendiriciler ve WAN sağlayıcı ağı içindeki diğer ekipmanlar dahildir. |
| Backhaul network<br>Ana taşıyıcı ağı | (Gösterilmiyor) Backhaul ağları, servis sağlayıcı ağının birden çok erişim düğümünü bağlar.<br><br>Ana taşıyıcı ağları belediyeler, ülkeler ve bölgelere yayılabilir.<br><br>Ana taşıyıcı ağları ayrıca internet servis sağlayıcılarına ve omurga ağına bağlıdır. |
| Backbone network<br>Omurga ağı | (Gösterilmiyor) Bunlar, servis sağlayıcı ağlarını birbirine bağlamak ve yedek bir ağ oluşturmak için kullanılan büyük, yüksek kapasiteli ağlardır.<br><br>Diğer hizmet sağlayıcılar omurgaya doğrudan veya başka bir hizmet sağlayıcı aracılığıyla bağlanabilir.<br><br>Omurga ağı servis sağlayıcılarına Katman-1 sağlayıcıları da denir. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 36.2.4.WAN Cihazları

WAN ortamlarına özgü birçok cihaz türü vardır. Bununla birlikte, bir WAN üzerinden uçtan uca veri yolu, şekilde gösterildiği gibi, genellikle kaynak DTE'den DCE'ye, ardından WAN bulutuna, ardından DCE'ye ve son olarak da hedef DTE'ye kadardır.




Şekilde gösterilen WAN cihazlarının açıklaması için tabloya bakın.

| WAN Cihazı | Açıklama |
|---|---|
| Voiceband Modem<br>Ses bandı Modem | Çevirmeli modem olarak da bilinir.<br><br>Bir bilgisayar tarafından üretilen dijital sinyalleri analog ses frekanslarına dönüştüren (yani modüle eden) eski cihaz.<br><br>Veri iletmek için telefon hatlarını kullanır. |
| DSL Modem ve Kablo Modem | Toplu olarak geniş bant modemler olarak bilinen bu yüksek hızlı dijital modemler, Ethernet kullanarak DTE yönlendiriciye bağlanır.<br><br>DSL modemler, telefon hatlarını kullanarak WAN'a bağlanır.<br><br>Kablo modemleri, koaksiyel hatlar kullanarak WAN'a bağlanır.<br><br>Her ikisi de ses bandı modeme benzer şekilde çalışır ancak daha yüksek geniş bant frekansları ve iletim hızları kullanır. |
| CSU / DSU | Dijital kiralanan hatlar için bir CSU ve bir DSU gerekir.<br><br>Dijital bir cihazı dijital bir hatta bağlar.<br><br>Bir CSU / DSU, modem gibi ayrı bir cihaz olabilir veya bir yönlendirici üzerindeki bir arayüz olabilir.<br><br>CSU, dijital sinyal için sonlandırma sağlar ve hata düzeltme ve hat izleme yoluyla bağlantı bütünlüğünü sağlar. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| WAN Cihazı | Açıklama |
|---|---|
| | DSU, hat çerçevelerini LAN'ın yorumlayabileceği çerçevelere dönüştürür ve bunun tersi de geçerlidir. |
| Optik Dönüştürücü | Optik fiber dönüştürücü olarak da bilinir.<br><br>Bu cihazlar fiber optik ortamı bakır ortama bağlar ve optik sinyalleri elektronik darbelere dönüştürür. |
| Kablosuz Yönlendirici veya Erişim Noktası | Cihazlar, bir WAN sağlayıcısına kablosuz olarak bağlanmak için kullanılır.<br><br>Yönlendiriciler ayrıca hücresel kablosuz bağlantı kullanabilir. |
| WAN Core cihazları | WAN omurgası, birden fazla yüksek hızlı yönlendirici ve Katman 3 anahtarından oluşur.<br><br>Bir yönlendirici veya çok katmanlı anahtar, WAN çekirdeğinde kullanılan en yüksek hızda birden çok telekomünikasyon arayüzünü destekleyebilmelidir.<br><br>Ayrıca tüm bu arabirimlerde IP paketlerini tam hızda iletebilmelidir.<br><br>Yönlendirici veya çok katmanlı anahtar, çekirdekte kullanılan yönlendirme protokollerini de desteklemelidir. |

## 36.2.5.Devre Anahtarlamalı (Circuit-Switched) İletişim

Ağ iletişimi, devre anahtarlamalı iletişim kullanılarak gerçekleştirilebilir. Devre anahtarlamalı bir ağ, kullanıcılar iletişim kurmadan önce uç noktalar arasında özel bir devre (veya kanal) kurar.

Spesifik olarak, devre anahtarlama, ses veya veri iletişimi başlamadan önce hizmet sağlayıcı ağı aracılığıyla dinamik olarak özel bir sanal bağlantı kurar.

Örneğin, bir kullanıcı bir sabit hat kullanarak bir telefon görüşmesi yaptığında, aranan numara sağlayıcı ekipman tarafından arayandan aranan tarafa özel bir devre oluşturmak için kullanılır.

Not : Sabit hat, sağlayıcıya bakır veya fiber optik medya kullanılarak bağlanan sabit bir konumda bulunan bir telefonu tanımlar.

Devre anahtarlamalı bir ağ üzerinden iletim sırasında, tüm iletişim aynı yolu kullanır. Devreye tahsis edilen sabit kapasitenin tamamı, aktarılacak bilgi olup olmadığına bakılmaksızın bağlantı süresi boyunca kullanılabilir. Bu, devre kullanımında verimsizliklere yol açabilir. Bu nedenle, devre anahtarlama genellikle veri iletişimi için uygun değildir.

Devre anahtarlamalı WAN teknolojilerinin en yaygın iki türü, genel anahtarlamalı telefon ağı-public switched telephone network (PSTN) ve eski Tümleşik Hizmetler Dijital Ağıdır- Integrated Services Digital Network (ISDN)

## 36.2.6.Paket Anahtarlamalı (Packet Switched) İletişim

Ağ iletişimi en yaygın olarak paket anahtarlamalı iletişim kullanılarak gerçekleştirilir. Devre anahtarlamanın tersine, paket anahtarlama, verileri paylaşılan bir ağ üzerinden yönlendirilen paketlere ayırır. Paket anahtarlamalı ağlar bir devre kurulmasını gerektirmez ve birçok düğüm çiftinin aynı kanal üzerinden iletişim kurmasına izin verir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Paket anahtarlama, devre anahtarlamadan çok daha ucuz ve daha esnektir. Gecikmelere ve gecikme değişkenliğine (titreme) duyarlı olmasına rağmen, modern teknoloji, bu ağlar üzerinde ses ve video iletişiminin tatmin edici bir şekilde taşınmasına izin verir.

Yaygın paket anahtarlamalı WAN teknolojileri türleri Ethernet WAN (Metro Ethernet), Çok Protokollü Etiket Anahtarlama- Multiprotocol Label Switching(MPLS) ve ayrıca eski Çerçeve Aktarma-Frame Relay ve eski Eşzamansız Aktarım Modu'dur -Asynchronous Transfer Mode (ATM).

## 36.2.7.SDH, SONET ve DWDM

Servis sağlayıcı ağları, kullanıcı verilerini hedefler arasında taşımak için fiber optik altyapıları kullanır. Fiber optik kablo, çok daha düşük zayıflaması ve paraziti nedeniyle uzun mesafeli iletimlerde bakır kablodan çok daha üstündür.

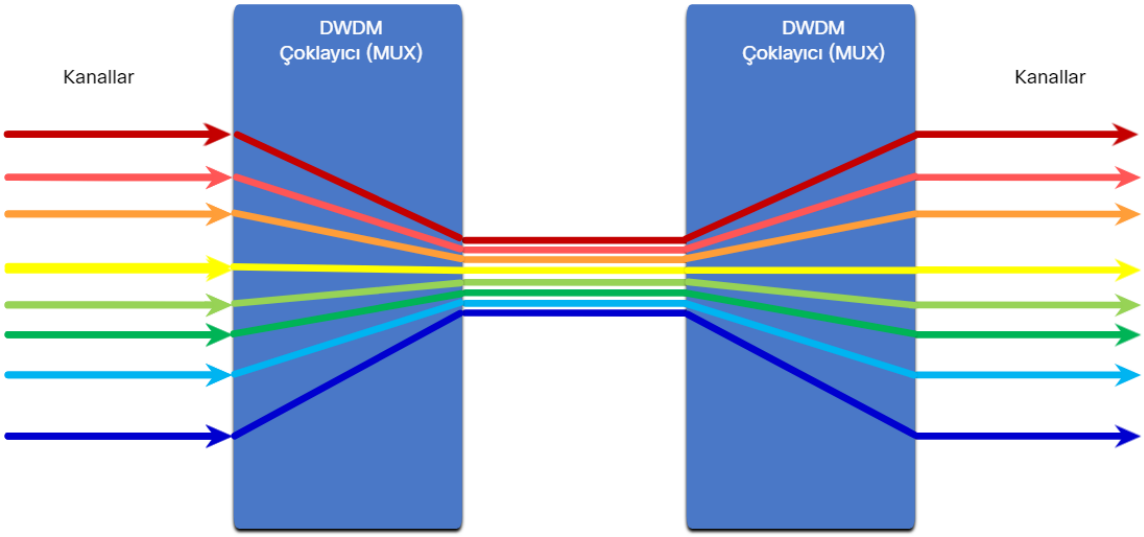
Hizmet sağlayıcıların kullanabileceği iki optik fiber OSI katman 1 standardı vardır:

- SDH - Senkron Dijital Hiyerarşi-Synchronous Digital Hierarchy (SDH), fiber optik kablo üzerinden veri aktarımı için global bir standarttır.
- SONET - Senkron Optik Ağ Oluşturma-Synchronous Optical Networking (SONET), SDH ile aynı hizmetleri sağlayan Kuzey Amerika standardıdır.

Her iki standart da temelde aynıdır ve bu nedenle genellikle SONET / SDH olarak listelenirler.

SDH / SONET lazerleri veya ışık yayan diyotları (LED'ler) kullanarak optik fiber üzerinden çok sayıda veri, ses ve video iletişiminin büyük mesafelerde nasıl aktarılacağını tanımlar. Her iki standart da, trafiğin her iki yönde akmasına izin veren yedekli fiber yollarını içeren halka ağ topolojisinde kullanılır.

Yoğun Dalgaboyu Bölmeli Çoğullama- Dense Wavelength Division Multiplexing(DWDM), şekilde gösterildiği gibi farklı ışık dalga boylarını kullanarak aynı anda birden fazla veri akışı göndererek (çoğullama) SDH ve SONET'in veri taşıma kapasitesini artıran daha yeni bir teknolojidir.




DWDM aşağıdaki özelliklere sahiptir:

- SONET ve SDH standartlarını destekler.
- Tek bir fibere 80'den fazla farklı veri kanalını (yani dalga boylarını) çoklayabilir.
- Her kanal, 10 Gbps çoğullamalı sinyal taşıma kapasitesine sahiptir.
- Gelen optik sinyalleri belirli ışık dalga boylarına (yani frekanslara) atar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

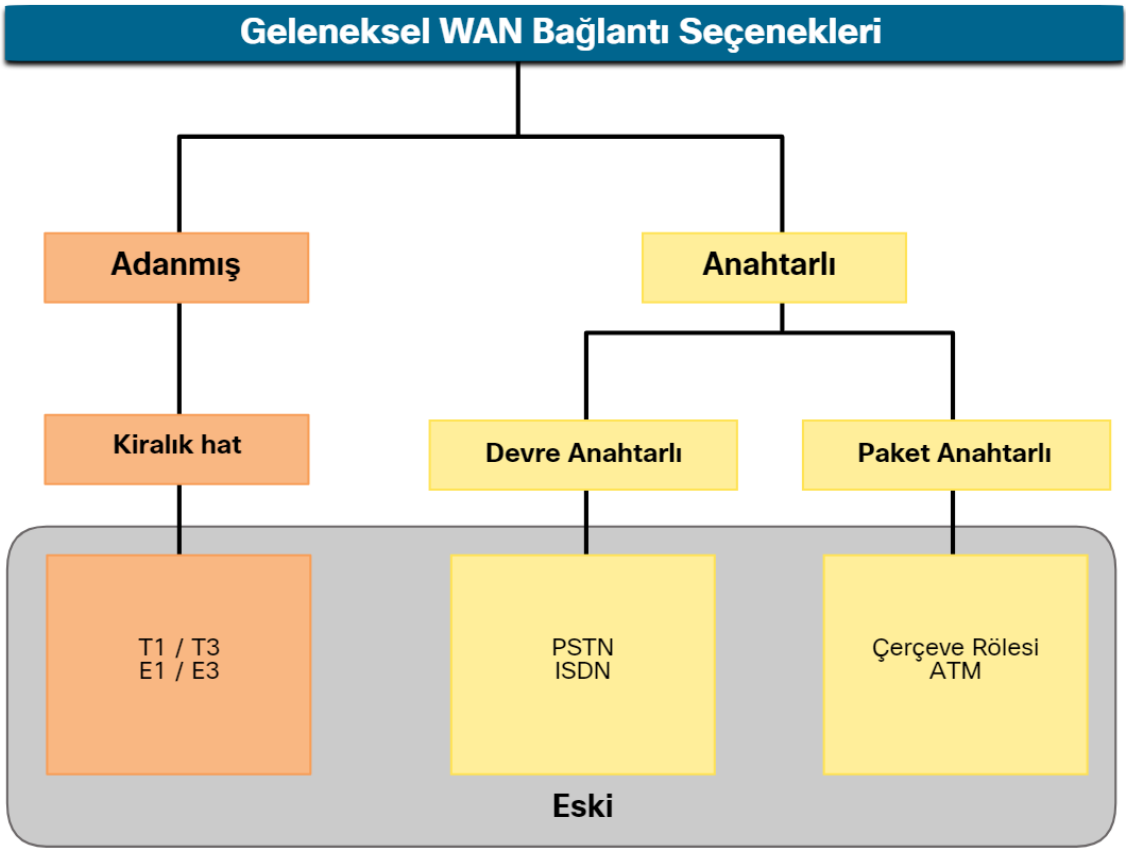
**Not:** DWDM devreleri, uzun mesafeli sistemlerde ve modern denizaltı iletişim kablo sistemlerinde kullanılır.

## 36.3.Geleneksel WAN Bağlantısı

### 36.3.1.Geleneksel WAN Bağlantı Seçenekleri

Bugünün WAN'larını anlamak için nereden başladıklarını bilmek yardımcı olur. Bu konu, WAN bağlantı seçeneklerini en başından açıklar. LAN'lar 1980'lerde ortaya çıktığında, kuruluşlar diğer lokasyonlarla bağlantı kurma ihtiyacını görmeye başladı. Bunu yapmak için, ağlarının bir servis sağlayıcının yerel döngüsüne bağlanmasına ihtiyaçları vardı. Bu, özel hatlar kullanılarak veya bir servis sağlayıcıdan anahtarlamalı hizmetler kullanılarak gerçekleştirildi.

Şekil, geleneksel WAN bağlantı seçeneklerini özetlemektedir.




### 36.3.2.Ortak WAN Terminolojisi

Kalıcı adanmış bağlantılar gerekli olduğunda, müşteri tesislerinden sağlayıcı ağına önceden kurulmuş bir WAN iletişim yolu sağlamak için bakır ortam kullanan noktadan noktaya bir bağlantı kullanıldı. Noktadan noktaya hatlar bir hizmet sağlayıcıdan kiralanabilir ve "kiralık hatlar" olarak adlandırılırdı. Bu terim, kuruluşun hattı kullanmak için bir hizmet sağlayıcıya aylık kira ücreti ödemesi anlamına gelir.

Kiralık hatlar 1950'lerin başından beri mevcuttur ve bu nedenle kiralık devreler, seri bağlantı, seri hat, noktadan noktaya bağlantı ve T1 / E1 veya T3 / E3 hatları gibi farklı isimlerle anılır.

Kiralık hatlar farklı sabit kapasitelerde mevcuttur ve genellikle gereken bant genişliği ve iki bağlantılı nokta arasındaki mesafeye göre fiyatlandırılır.

Bir bakır ortam seri bağlantısının dijital kapasitesini tanımlamak için kullanılan iki sistem vardır:

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

T taşıyıcı - Kuzey Amerika'da kullanılan T taşıyıcı, 1.544 Mbps'ye kadar bant genişliğini destekleyen T1 bağlantıları ve 43.7 Mbps'ye kadar bant genişliğini destekleyen T3 bağlantıları sağlar.

E-taşıyıcı - Avrupa'da kullanılan E-taşıyıcı, 2.048 Mbps'ye kadar bant genişliğini destekleyen E1 bağlantıları ve 34.368 Mbps'ye kadar bant genişliğini destekleyen E3 bağlantıları sağlar.
Not: Bakır kablo fiziksel altyapısının yerini büyük ölçüde fiber optik ağ almıştır. Optik fiber ağdaki iletim hızları, bir fiber optik ağın dijital iletim kapasitesini tanımlayan Optik Taşıyıcı (OC) iletim hızları cinsinden verilmiştir.

Tablo, kiralık hatların avantaj ve dezavantajlarını özetlemektedir.

| | |
|---|---|
| Avantajları | |
| Basitlik | Noktadan noktaya iletişim bağlantılarının kurulumu ve bakımı minimum düzeyde uzmanlık gerektirir. |
| Kalite | Noktadan noktaya iletişim bağlantıları, yeterli bant genişliğine sahiplerse, genellikle yüksek kaliteli hizmet sunar. Ayrılan kapasite, uç noktalar arasındaki gecikmeyi veya titreşimi ortadan kaldırır. |
| Kullanılabilirlik | E-ticaret gibi bazı uygulamalar için sürekli kullanılabilirlik önemlidir. Noktadan noktaya iletişim bağlantıları, VoIP veya IP üzerinden Video için gerekli olan kalıcı, özel kapasite sağlar. |
| Dezavantajları | |
| Maliyet | Noktadan noktaya bağlantılar genellikle en pahalı WAN erişim türüdür. Kiralanan hat çözümlerinin maliyeti, birçok siteyi artan mesafelerde birbirine bağlamak için kullanıldığında önemli hale gelebilir. Ek olarak, her uç nokta, yönlendirici üzerinde ekipman maliyetlerini artıran bir arayüz gerektirir. |
| Sınırlı esneklik | WAN trafiği genellikle değişkendir ve kiralık hatların sabit kapasiteleri vardır, böylece hattın bant genişliği nadiren tam olarak ihtiyaca cevap verir. Kiralanan hattaki herhangi bir değişiklik, genellikle kapasiteyi ayarlamak için ISP personelinin saha ziyaretini gerektirir. |

## 36.3.3.Devre Anahtarlamalı Seçenekler

Devre anahtarlamalı bağlantılar Genel Hizmet Telefon Ağı (PSTN) taşıyıcıları tarafından sağlanır. CPE'yi CO'ya bağlayan yerel döngü bakır ortamdır. İki geleneksel devre anahtarlamalı seçenek vardır.

### Kamu Hizmeti Telefon Ağı (PSTN)

Çevirmeli WAN erişimi, WAN bağlantısı olarak PSTN'yi kullanır. Geleneksel yerel döngüler, ikili bilgisayar verilerini bir ses bandı modem kullanarak sesli telefon ağı üzerinden taşıyabilir. Modem, dijital verileri kaynakta bir analog sinyale dönüştürür ve hedefte analog sinyali dijital veriye demodüle eder. Yerel döngünün fiziksel özellikleri ve bunun PSTN'ye bağlantısı, sinyal hızını 56 kbps'nin altında sınırlar.

Çevirmeli erişim, eski bir WAN teknolojisi olarak kabul edilir. Ancak, başka bir WAN teknolojisi mevcut olmadığında yine de uygulanabilir bir çözüm olabilir.

### Tümleşik Hizmetler Dijital Ağı (ISDN)

ISDN, PSTN yerel döngüsünün dijital sinyalleri taşımasını sağlayan bir devre anahtarlama teknolojisidir. Bu, çevirmeli erişimden daha yüksek kapasiteli anahtarlamalı bağlantılar sağladı. ISDN, 45 Kbps ile 2.048 Mbps arasında veri hızları sağlar.

ISDN, yüksek hızlı DSL ve diğer geniş bant hizmetleri nedeniyle popüleritesini büyük ölçüde düşürmüştür. ISDN, çoğu büyük sağlayıcının bu hizmeti durdurduğu eski bir teknoloji olarak kabul edilir.

## 36.3.4.Paket Anahtarlamalı Seçenekler

Paket anahtarlama, verileri paylaşılan bir ağ üzerinden yönlendirilen paketlere böler. Devre anahtarlamalı ağlar, özel bir devrenin kurulmasını gerektirir. Buna karşılık, paket anahtarlama ağları, birçok düğüm çiftinin aynı kanal üzerinden iletişim kurmasına izin verir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

İki adet geleneksel (eski) paket anahtarlamalı bağlantı seçeneği vardır.

**Çerçeve Rölesi-Aktarımı (Frame Relay)**

Frame Relay, kurumsal LAN'ları birbirine bağlamak için kullanılan basit bir Katman 2 yayın dışı çoklu erişim (NBMA) WAN teknolojisidir. Farklı PVC'ler kullanarak birden çok siteye bağlanmak için tek bir yönlendirici arabirimi kullanılabilir. PVC'ler, bir kaynak ve hedef arasında hem ses hem de veri trafiğini taşımak için kullanılır ve 4 Mbps'ye kadar veri hızlarını destekler; bazı sağlayıcılar daha da yüksek oranlar sunar.

Çerçeve Geçişi, bir veri bağlantısı bağlantı tanımlayıcısı (DLCI) ile benzersiz şekilde tanımlanan PVC'ler oluşturur. PVC'ler ve DLCI'ler, bir DTE cihazından diğerine çift yönlü iletişim sağlar.

Frame Relay ağlarının yerini büyük ölçüde daha hızlı Metro Ethernet ve internet tabanlı çözümler almıştır.

**Eşzamansız Aktarım Modu (ATM)**

Eşzamansız Aktarım Modu (ATM) teknolojisi, özel ve genel ağlar üzerinden ses, video ve verileri aktarabilir. Çerçeve tabanlı bir mimari yerine hücre tabanlı bir mimari üzerine inşa edilmiştir. ATM hücreleri her zaman 53 baytlık sabit uzunluktadır. ATM hücresi, 5 baytlık bir ATM başlığı ve ardından 48 bayt ATM yükü içerir. Küçük, sabit uzunluktaki hücreler ses ve video trafiğini taşımak için çok uygundur çünkü bu trafik gecikmeye tahammül etmez. Video ve ses trafiğinin daha büyük veri paketlerinin iletilmesini beklemesi gerekmez.

53 baytlık ATM hücresi, Frame Relay'in daha büyük çerçeve ve paketlerinden daha az verimlidir. Ayrıca, ATM hücresinin her 48 baytlık yük için en az beş bayt ek yükü vardır. Hücre, bölümlere ayrılmış ağ katmanı paketleri taşıdığında, ek yük daha yüksektir, çünkü ATM anahtarının paketleri hedefte yeniden birleştirebilmesi gerekir. Tipik bir ATM hattı, aynı hacimde ağ katmanı verilerini taşımak için Frame Relay'den neredeyse yüzde 20 daha fazla bant genişliğine ihtiyaç duyar.

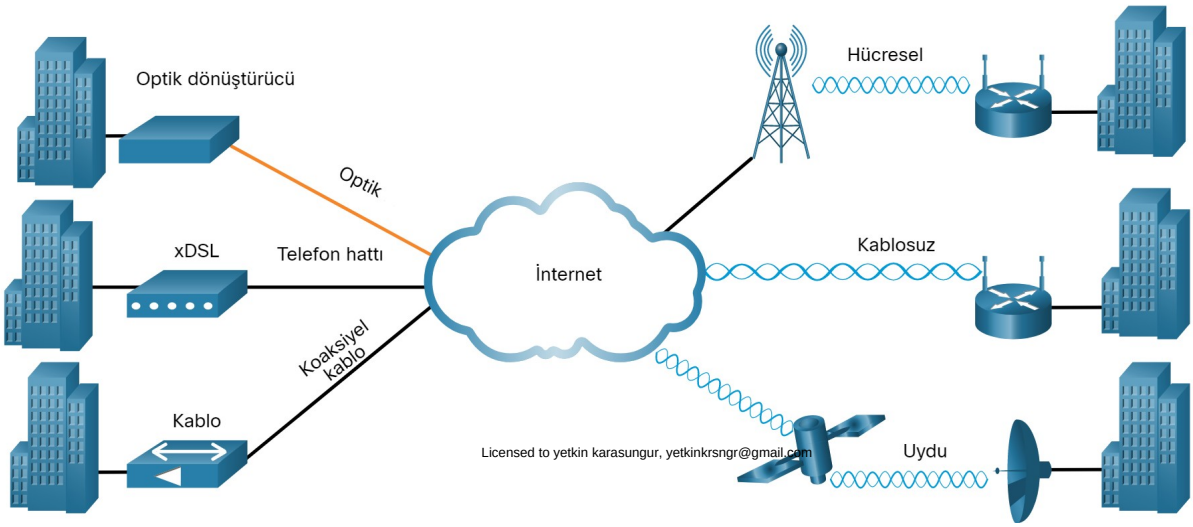
ATM ağlarının yerini büyük ölçüde daha hızlı Metro Ethernet ve internet tabanlı çözümler almıştır.

## 36.4.Modern WAN Bağlantısı

### 36.4.1.Modern WAN'lar

Modern WAN'lar, geleneksel WAN'lardan daha fazla bağlantı seçeneğine sahiptir. İşletmeler artık daha hızlı ve daha esnek WAN bağlantı seçeneklerine ihtiyaç duyuyor. Geleneksel WAN bağlantı seçenekleri, artık mevcut olmadıklarından, çok pahalı olduklarından veya sınırlı bant genişliğine sahip olduklarından kullanımda hızla azalmıştır.

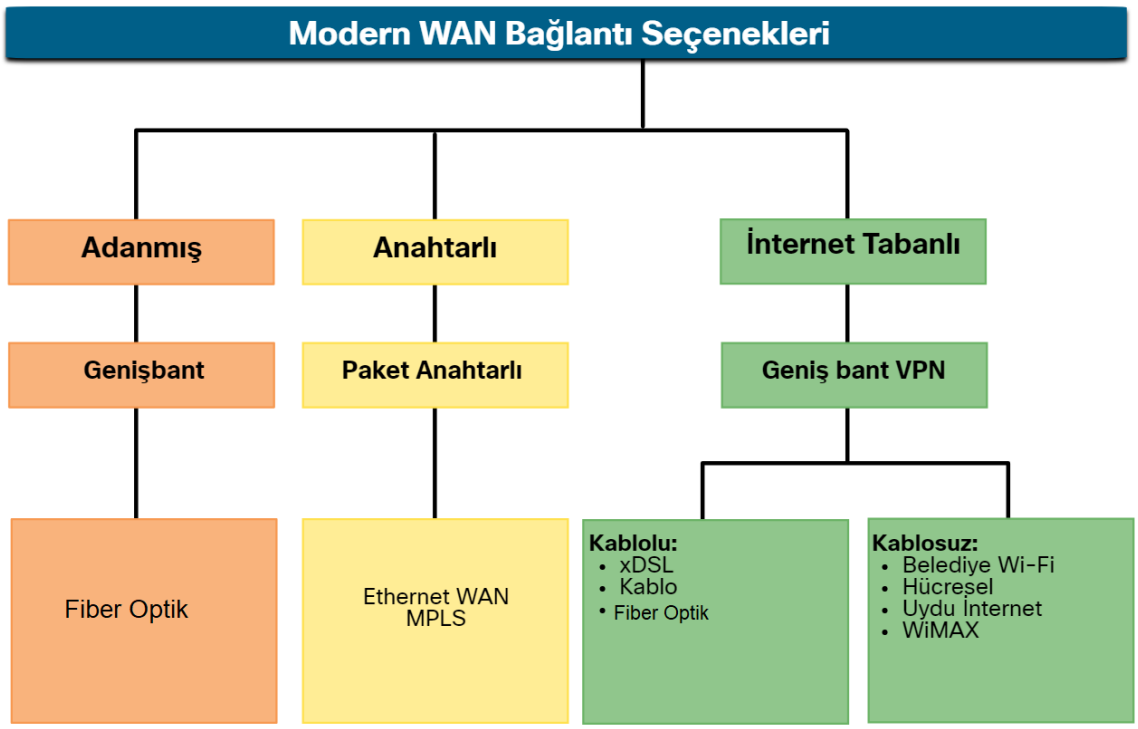
Şekil, bugün karşılaşılan yerel döngü bağlantılarını göstermektedir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 36.4.2.Modern WAN Bağlantı Seçenekleri

Sürekli olarak yeni teknolojiler ortaya çıkıyor. Şekil, modern WAN bağlantı seçeneklerini özetlemektedir.




### Ayrılmış Geniş Bant

1990'ların sonlarında, birçok telekomünikasyon şirketi, öngörülen yeni nesil ihtiyaçları karşılamak için yeterli fibere sahip fiber optik ağlar inşa etti. Bununla birlikte, dalga boyu bölmeli çoğullama- wavelength division multiplexing(WDM) gibi optik teknolojiler geliştirildi ve tek bir optik fiber telinin iletim kabiliyetini önemli ölçüde artırdı. Sonuç olarak, birçok fiber optik kablo hattı kullanımda değildir. Kullanımda olmayan ve bu nedenle "yanmayan" (yani karanlık) fiber optik kablo, koyu fiber (dark fiber) olarak adlandırılır.

Fiber, uzak konumları doğrudan birbirine bağlamak için bir kuruluş tarafından bağımsız olarak kurulabilir. Bununla birlikte, koyu fiber de bir tedarikçiden kiralanabilir veya satın alınabilir. Koyu fiberi kiralamak genellikle günümüzde mevcut olan diğer WAN seçeneklerinden daha pahalıdır. Bununla birlikte, en büyük esnekliği, kontrolü, hızı ve güvenliği sağlar

### Paket Anahtarlı

İki paket anahtarlamalı WAN ağ seçeneği mevcuttur.

Ethernet LAN teknolojisindeki gelişmeler, bunun MAN ve WAN alanlarına genişlemesini sağladı. Metro Ethernet, hızlı bant genişliği bağlantıları sağlar ve birçok geleneksel WAN bağlantı seçeneğinin değiştirilmesinden sorumludur.

Çok protokollü Etiket Anahtarlama-Multi-protocol Label Switching (MPLS), WAN sağlayıcı ağının yük verileri olarak herhangi bir protokolü (örneğin, IPv4 paketleri, IPv6 paketleri, Ethernet, DSL) taşımasını sağlar. Bu, farklı konumların (site) erişim teknolojilerinden bağımsız olarak sağlayıcı ağına bağlanmasını sağlar.

### İnternet Tabanlı Geniş Bant

Kuruluşlar artık WAN bağlantısı için genel olarak küresel internet altyapısını kullanıyor. Güvenlik endişelerini gidermek için, bağlantı seçenekleri genellikle VPN teknolojileriyle birleştirilir.

Geçerli WAN ağ seçenekleri arasında Dijital Abone Hattı (DSL), kablo, kablosuz ve fiber bulunur

## 36.4.3.Ethernet WAN

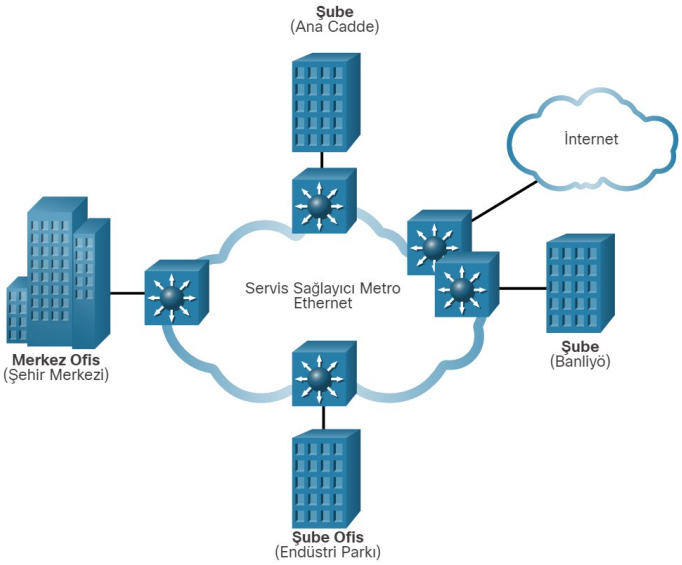
Ethernet başlangıçta bir LAN erişim teknolojisi olarak geliştirildi ve öncelikle bakır ortamın sağladığı sınırlı mesafe nedeniyle bir WAN erişim teknolojisi olarak uygun değildi.

Ancak, fiber optik kablolar kullanan daha yeni Ethernet standartları, Ethernet'i makul bir WAN erişim seçeneği haline getirdi. Örneğin, IEEE 1000BASE-LX standardı 5 km'lik fiber optik kablo uzunluklarını desteklerken, IEEE 1000BASE-ZX standardı 70 km'ye kadar kablo uzunluklarını destekler.

Servis sağlayıcılar artık fiber optik kablolama kullanarak Ethernet WAN hizmeti sunuyor. Ethernet WAN hizmeti, aşağıdakiler de dahil olmak üzere birçok adla görülebilir:

Metropolitan Ethernet (Metro E)
MPLS üzerinden Ethernet (EoMPLS)
Sanal Özel LAN Hizmeti (VPLS)

Şekilde basit bir Metro Ethernet topolojisi örneği gösterilmektedir.




Aşağıdakiler, bir Ethernet WAN'ın birkaç avantajıdır:

- Daha az masraf ve yönetim - Ethernet WAN, aynı altyapı üzerinde veri, ses ve videoyu yönetebilen anahtarlı, yüksek bant genişliğine sahip bir Katman 2 ağı sağlar. Bu, bant genişliğini artırır ve diğer WAN teknolojilerine pahalı dönüşümleri ortadan kaldırır. Teknoloji, işletmelerin bir metropol alanında çok sayıda siteyi birbirine ve internete ucuz bir şekilde bağlamasını sağlar.
- Mevcut ağlarla kolay entegrasyon - Ethernet WAN, mevcut Ethernet LAN'larına kolayca bağlanarak kurulum maliyetlerini ve süresini azaltır.
- Gelişmiş iş üretkenliği - Ethernet WAN, işletmelerin barındırılan IP iletişimleri, VoIP ve akış ve yayın videosu gibi TDM veya Frame Relay ağlarında uygulanması zor olan üretkenliği artıran IP uygulamalarından yararlanmalarını sağlar.

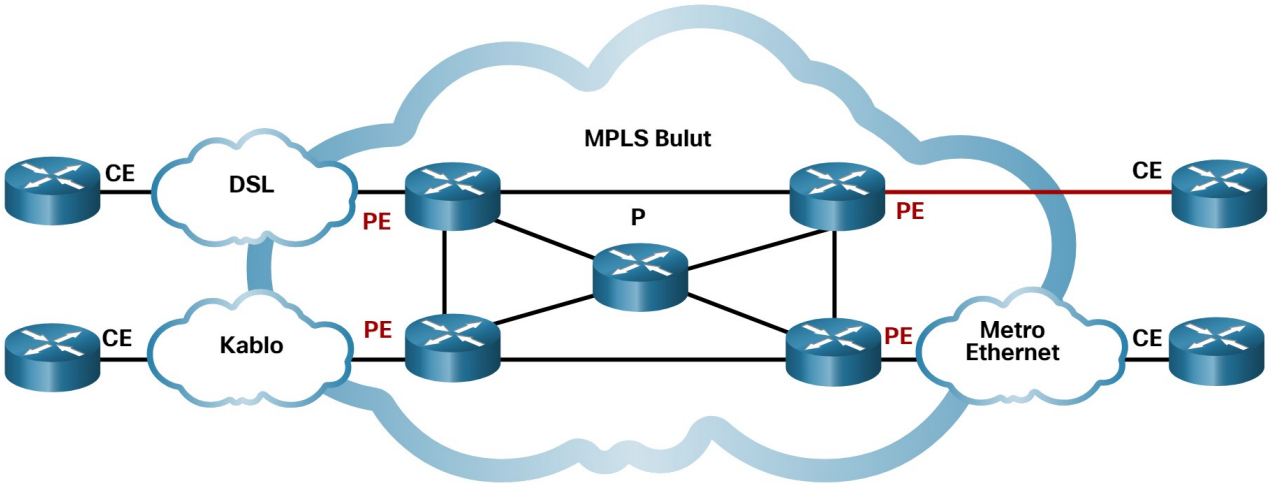
Not : Ethernet WAN'lar popülerlik kazanmıştır ve artık geleneksel seri noktadan noktaya, Çerçeve Aktarımı ve ATM WAN bağlantılarının yerini almak için yaygın olarak kullanılmaktadır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 36.4.4.MPLS

Multiprotocol Label Switching (MPLS), erişim yöntemine veya yüke bakılmaksızın istemcileri birbirine bağlamak için yüksek performanslı bir servis sağlayıcı WAN yönlendirme teknolojisidir. MPLS, çeşitli istemci erişim yöntemlerini destekler (örneğin, Ethernet, DSL, Kablo, Çerçeve Geçişi). MPLS, IPv4 ve IPv6 trafiği de dahil olmak üzere her tür protokolü kapsayabilir.

Basit bir MPLS etkin ağın örnek topolojisine bakın.




Bir MPLS yönlendiricisi, bir müşteri kenar-customer edge (CE) yönlendiricisi, bir sağlayıcı kenar- provider edge (PE) yönlendiricisi veya bir dahili sağlayıcı-provider (P) yönlendiricisi olabilir. MPLS'nin çeşitli istemci erişim bağlantılarını (kablo, DSL vb.) desteklediğine dikkat edin.

MPLS yönlendiricileri, etiket anahtarlamalı yönlendiricilerdir- label switched routers(LSRs). Bu, daha sonra diğer MPLS yönlendiricileri tarafından trafiği iletmek için kullanılan paketlere etiket ekledikleri anlamına gelir. Trafik CE'den ayrılırken, MPLS PE yönlendiricisi çerçeve başlığı ile paket başlığı arasına kısa bir sabit uzunlukta etiket ekler. MPLS P yönlendiricileri, paketin bir sonraki sıçramasını belirlemek için etiketi kullanır. Paket MPLS ağını terk ettiğinde etiket çıkış PE yönlendiricisi tarafından kaldırılır.

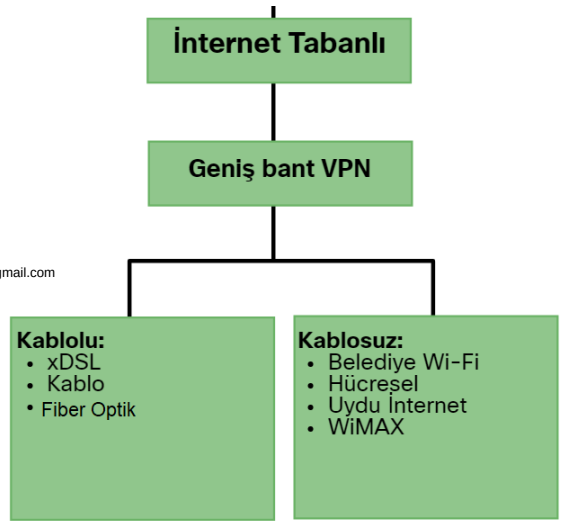
MPLS ayrıca QoS desteği, trafik mühendisliği, artıklık ve VPN'ler için hizmetler sağlar.

## 36.5.İnternet Tabanlı Bağlantı

### 36.5.1.İnternet Tabanlı Bağlantı Seçenekleri

Modern WAN bağlantı seçenekleri Ethernet WAN ve MPLS ile bitmez. Bugün, aralarından seçim yapabileceğiniz bir dizi internet tabanlı kablolu ve kablosuz seçenek var. İnternet tabanlı geniş bant bağlantısı, özel WAN seçeneklerini kullanmaya bir alternatiftir.

Şekilde internet tabanlı bağlantı seçenekleri listelenmektedir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

İnternet tabanlı bağlantı, kablolu ve kablosuz seçeneklere ayrılabilir.

Kablolu seçenekler

Kablolu seçenekler, tutarlı bant genişliği sağlamak ve hata oranlarını ve gecikmeyi azaltmak için kalıcı kablolama (örneğin, bakır veya fiber) kullanır. Kablolu geniş bant bağlantı örnekleri, Dijital Abone Hattı-Digital Subscriber Line (DSL), kablo bağlantıları ve fiber optik ağlardır.

Kablosuz seçenekleri

Veri iletmek için kablolu medya yerine radyo dalgalarını kullandıklarından, kablosuz seçenekleri diğer WAN bağlantı seçeneklerine kıyasla uygulamak daha ucuzdur. Ancak, kablosuz sinyaller, radyo kulelerine olan uzaklık, diğer kaynaklardan gelen parazit, hava durumu ve paylaşılan alana erişen kullanıcı sayısı gibi faktörlerden olumsuz etkilenebilir. Kablosuz geniş bant örnekleri, hücresel 3G / 4G / 5G veya uydu internet hizmetlerini içerir. Kablosuz operatör seçenekleri konuma göre değişiklik gösterir.

## 36.5.2.DSL Teknolojisi

Dijital Abone Hattı (DSL), kullanıcılara IP hizmetleri sağlamak için mevcut çift bükümlü telefon hatlarını kullanan, yüksek hızlı, her zaman açık bir bağlantı teknolojisidir. DSL, ev kullanıcıları için ve kurumsal BT departmanlarının tele-çalışanları desteklemek için popüler bir seçimdir.

POTS (Düz Eski Telefon Sistemi) etiketli alan, ses dereceli telefon hizmeti tarafından kullanılan frekans aralığını tanımlar. ADSL etiketli alan, yukarı akış ve aşağı akış DSL sinyalleri tarafından kullanılan frekans alanını temsil eder. Hem POTS alanını hem de ADSL alanını kapsayan alan, bakır tel çifti tarafından desteklenen tüm frekans aralığını temsil eder.

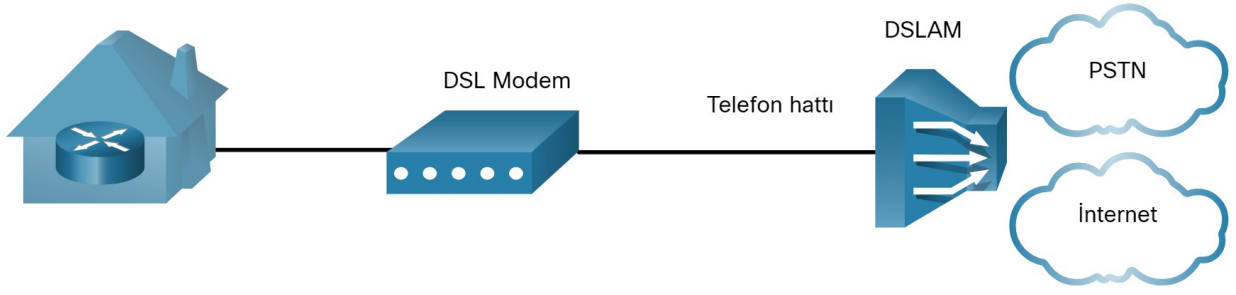
Farklı yükleme ve indirme aktarım hızları sunan birkaç xDSL çeşidi vardır. Ancak, tüm DSL biçimleri Asimetrik DSL (ADSL) veya Simetrik DSL (SDSL) olarak kategorize edilir. ADSL ve ADSL2 +, kullanıcıya yükleme bant genişliğinden daha yüksek aşağı akış bant genişliği sağlar. SDSL her iki yönde de aynı kapasiteyi sağlar.

Aktarım hızları ayrıca yerel döngünün gerçek uzunluğuna ve kablolamanın türüne ve durumuna bağlıdır. Örneğin, garantili sinyal kalitesi için bir ADSL döngüsü 5,46 km'den (3,39 mil) az olmalıdır.

Bu süreçte güvenlik riskleri oluşur, ancak VPN'ler gibi güvenlik önlemleriyle aracılık edilebilir.

### DSL Bağlantıları

Servis sağlayıcılar, yerel döngüde DSL bağlantılarını dağıtır. Şekilde gösterildiği gibi, bağlantı DSL modem ile DSL erişim çoklayıcı-DSL access multiplexer (DSLAM) arasında kurulur.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

DSL modem, teleworker (ev içindek router) cihazından gelen Ethernet sinyallerini, sağlayıcı konumundaki bir DSL erişim çoklayıcıya (DSLAM) iletilen bir DSL sinyaline dönüştürür.

DSLAM, sağlayıcının Merkez Ofisinde (CO) bulunan cihazdır ve birden çok DSL abonesinin bağlantılarını yoğunlaştırır. DSLAM, genellikle bir toplama yönlendiricisinde yerleşik olarak bulunur.
DSL'in kablo teknolojisine göre avantajı, DSL'nin paylaşılan bir ortam olmamasıdır. Her kullanıcının DSLAM'a ayrı bir doğrudan bağlantısı vardır. Kullanıcıların eklenmesi, ISP'ye veya internete DSLAM internet bağlantısı doygun hale gelmedikçe performansı engellemez.

## 36.5.3.DSL ve PPP

Noktadan Noktaya protokolü (Point to Point) (PPP), telefon servis sağlayıcıları tarafından, çevirmeli ve ISDN erişim ağları üzerinden yönlendiriciden yönlendiriciye ve ana bilgisayardan ağa bağlantılar kurmak için yaygın olarak kullanılan bir Katman 2 protokolüdür.

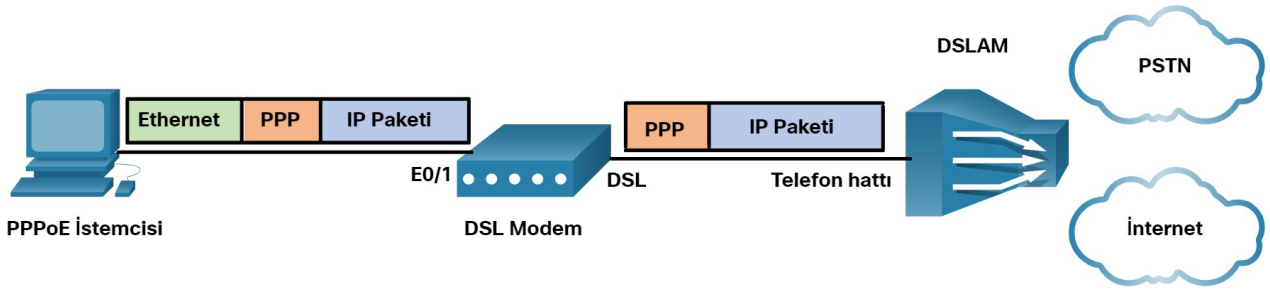
ISP'ler, aşağıdaki faktörler nedeniyle geniş bant DSL bağlantıları için Katman 2 protokolü olarak PPP'yi kullanmaya devam eder:

- Abonenin kimliğini doğrulamak için PPP kullanılabilir.
- PPP, aboneye genel bir IPv4 adresi atayabilir.
- PPP, bağlantı kalitesi yönetimi özellikleri sağlar.

Bir DSL modem, DSL ağına bağlanmak için bir DSL arayüzüne ve istemci cihaza bağlanmak için bir Ethernet arayüzüne sahiptir. Ancak, Ethernet bağlantıları PPP'yi yerel olarak desteklemez.

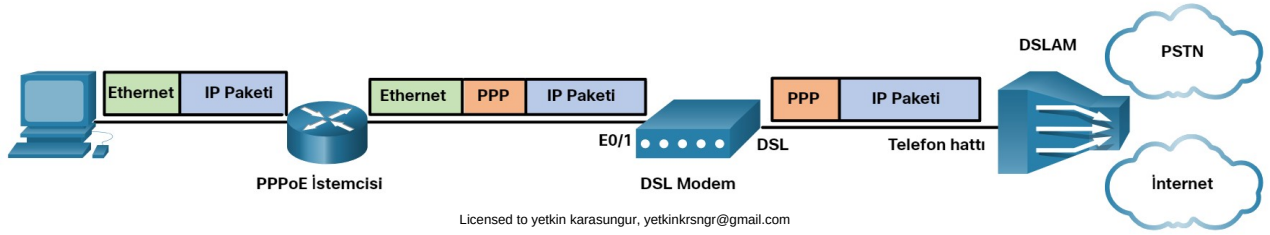
### PPPoE İstemcisi

Şekilde gösterildiği gibi, ana bilgisayar, sağlayıcı sitesinde bulunan bir PPPoE sunucusundan bir genel IP adresi almak için bir PPPoE istemcisi çalıştırır. PPPoE istemci yazılımı, PPPoE kullanarak DSL modem ile iletişim kurar ve modem, PPP kullanarak ISP ile iletişim kurar. Bu topolojide, yalnızca bir istemci bağlantıyı kullanabilir. Ayrıca, iç ağı koruyacak bir yönlendirici olmadığına dikkat edin.




### Yönlendirici PPPoE

Diğer bir çözüm de, şekilde gösterildiği gibi, bir yönlendiriciyi PPPoE istemcisi olacak şekilde yapılandırmaktır. Yönlendirici, PPPoE istemcisidir ve yapılandırmasını sağlayıcıdan alır. İstemciler, yönlendiriciyle yalnızca Ethernet kullanarak iletişim kurar ve DSL bağlantısından habersizdir. Bu topolojide, birden çok istemci DSL bağlantısını paylaşabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 36.5.4.Kablo Teknolojisi

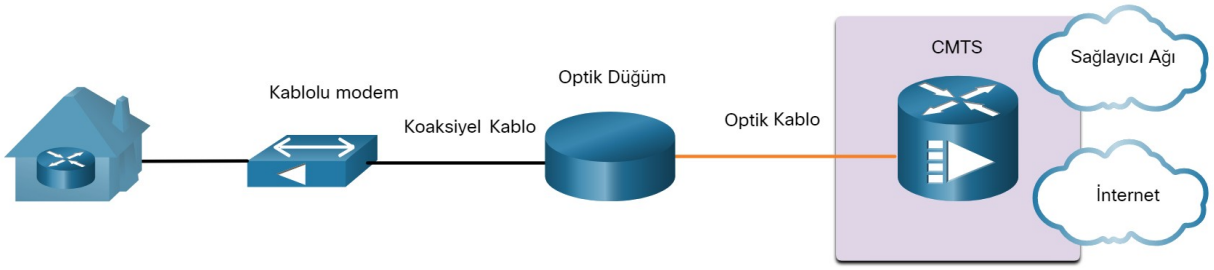
Kablo teknolojisi, kullanıcılara IP hizmetleri sağlamak için kablo şirketinden bir koaksiyel kablo kullanan yüksek hızlı, her zaman açık bağlantı teknolojisidir. DSL gibi, kablo teknolojisi de ev kullanıcıları ve kurumsal BT departmanları için uzaktan çalışanları desteklemek için popüler bir seçimdir.

Modern kablo sistemleri, müşterilere yüksek hızlı internet erişimi, dijital kablolu televizyon ve evlerde telefon hizmeti dahil olmak üzere gelişmiş telekomünikasyon hizmetleri sunar.

Kablo Üzerinden Veri Servis Arayüzü Spesifikasyonu-Data over Cable Service Interface Specification (DOCSIS), mevcut bir kablo sistemine yüksek bant genişliğinde veri eklemek için uluslararası standarttır.

Kablo operatörleri, verilerin kablo modemlere yüksek hızda iletilmesini sağlamak için hibrit fiber koaksiyel-hybrid fiber-coaxial (HFC) ağlar kullanır. Kablo sistemi, radyo frekansı (RF) sinyallerini son kullanıcıya taşımak için bir koaksiyel kablo kullanır.

HFC, ağın farklı bölümlerinde fiber optik ve koaksiyel kablo kullanır. Örneğin, kablo modem ile optik düğüm arasındaki bağlantı, şekilde gösterildiği gibi koaksiyel kablodur.




Optik düğüm, optikten RF sinyaline dönüşüm gerçekleştirir. Spesifik olarak, RF sinyallerini fiber optik kablo üzerinden ışık darbelerine dönüştürür. Fiber medya, sinyallerin, bir Kablo Modem Sonlandırma Sisteminin-Cable Modem Termination System (CMTS) bulunduğu sağlayıcı merkez ucuna uzun mesafeler boyunca gitmesini sağlar. Tüm yerel aboneler aynı kablo bant genişliğini paylaşır. Hizmete daha fazla kullanıcı katıldıkça, mevcut bant genişliği beklenen oranın altına düşebilir.

## 36.5.5.Fiber Optik

Birçok belediye, şehir ve sağlayıcı, kullanıcının bulunduğu yere fiber optik kablo kurar. Bu genellikle x'e Fiber (FTTx) olarak adlandırılır ve aşağıdakileri içerir:

- Eve Kadar Fiber- Fiber to the Home(FTTH) - Fiber, ikamet sınırına ulaşır. Pasif optik ağlar ve noktadan noktaya Ethernet, doğrudan bir servis sağlayıcı merkez ofisinden FTTH ağları üzerinden kablo TV, internet ve telefon hizmetleri sağlayabilen mimarilerdir.
- Binaya kadar Fiber-Fiber to the Building (FTTB) - Fiber, çok konutlu bir birimdeki bodrum gibi binanın sınırına ulaşır ve bireysel yaşam alanına son bağlantı kaldırım veya direk teknolojileri gibi alternatif yollarla yapılır.
- Düğüme / Mahalleye Fiber- Fiber to the Node/Neighborhood(FTTN) - Optik kablolama, optik sinyalleri bükümlü çift veya koaksiyel kablo için kabul edilebilir bir biçime dönüştüren bir optik düğüme ulaşır.

FTTx, tüm geniş bant seçenekleri arasında en yüksek bant genişliğini sağlayabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 36.5.6.Kablosuz İnternet

Kablosuz teknoloji, veri göndermek ve almak için lisanssız radyo spektrumunu kullanır. Lisanssız spektruma, kullandıkları cihazda kablosuz yönlendirici ve kablosuz teknolojisi olan herkes erişebilir.

Yakın zamana kadar, kablosuz erişimin bir sınırlaması, kablosuz bir yönlendiricinin veya internete kablolu bağlantısı olan bir kablosuz modemin yerel iletim aralığında (tipik olarak 100 fitten daha az) olması gerekliliğiydi.

### Belediye Wi-Fi

Birçok şehir belediye kablosuz ağlarını kurmaya başladı. Bu ağlardan bazıları, yüksek hızlı internet erişimini ücretsiz olarak veya diğer geniş bant hizmetlerinin fiyatından önemli ölçüde daha düşük bir fiyata sağlar. Diğerleri yalnızca şehir kullanımı içindir ve polis, itfaiye ve diğer şehir çalışanlarının işlerinin belirli yönlerini uzaktan yapmalarına izin verir. Bir belediye Wi-Fi ağına bağlanmak için, bir abonenin tipik olarak, geleneksel kablosuz adaptörlerden daha güçlü bir radyo ve yönlü anten sağlayan bir kablosuz modeme ihtiyacı vardır. Çoğu servis sağlayıcı, DSL veya kablo modemlerde olduğu gibi, gerekli ekipmanı ücretsiz veya bir ücret karşılığında sağlar.

### Hücresel

Giderek artan bir şekilde, hücresel hizmet, kullanıcıları ve başka hiçbir WAN erişim teknolojisinin mevcut olmadığı uzak konumları bağlamak için kullanılan başka bir kablosuz WAN teknolojisidir. Akıllı telefonları ve tabletleri olan birçok kullanıcı, e-posta göndermek, web'de gezinmek, uygulamaları indirmek ve video izlemek için hücresel verileri kullanabilir.

Telefonlar, tablet bilgisayarlar, dizüstü bilgisayarlar ve hatta bazı yönlendiriciler hücresel teknolojiyi kullanarak internet üzerinden iletişim kurabilir. Bu cihazlar, yakındaki bir cep telefonu kulesi aracılığıyla iletişim kurmak için radyo dalgalarını kullanır. Cihazın küçük bir radyo anteni vardır ve sağlayıcının, telefonun kilometrelerce yakınında bir kulenin tepesinde oturan çok daha büyük bir anteni vardır.

Aşağıda iki yaygın hücresel endüstri terimi bulunmaktadır:

3G / 4G / 5G Kablosuz - Bunlar 3. nesil, 4. nesil ve gelişmekte olan 5. nesil mobil kablosuz teknolojilerin kısaltmalarıdır. Bu teknolojiler kablosuz internet erişimini destekler. 4G standartları, 450 Mbps'ye kadar indirme ve 100 Mbps'ye kadar olan bant genişliklerini destekler. Ortaya çıkan 5G standardı, 100 Mbps ila 10 Gbps ve ötesini desteklemelidir.
(LTE) - Bu, daha yeni ve daha hızlı bir teknolojiyi ifade eder ve dördüncü nesil (4G) teknolojisinin bir parçasıdır.

### Uydu İnternet

Tipik olarak kırsal kesimdeki kullanıcılar tarafından veya kablo ve DSL'nin mevcut olmadığı uzak yerlerde kullanılır. Uydu internet hizmetlerine erişmek için abonelerin bir uydu çanağına, iki modeme (yukarı bağlantı ve aşağı bağlantı) ve çanak ile modem arasında koaksiyel kablolara ihtiyacı vardır.

Spesifik olarak, bir yönlendirici, bir servis sağlayıcı uydusunu işaret eden bir uydu çanağına bağlanır. Bu uydu uzayda eşzamanlı yörüngede. Sinyaller, uyduya ve geri yaklaşık 35,786 kilometre (22,236 mil) gitmelidir.

Birincil kurulum gereksinimi, antenin yörüngedeki uydunun çoğunun yerleştirildiği ekvatora doğru net bir görüşe sahip olmasıdır. Ağaçlar ve şiddetli yağmurlar sinyal alımını etkileyebilir.

Uydu internet, iki yönlü (yükleme ve indirme) veri iletişimi sağlar. Yükleme hızları, indirme hızının yaklaşık onda biridir. İndirme hızları 5 Mbps ile 25 Mbps arasındadır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 36.5.7.VPN Teknolojisi

Bir evden çalışan veya uzaktaki bir ofis çalışanı, internet üzerinden kurumsal WAN'a erişmek için bir geniş bant hizmeti kullandığında güvenlik riskleri ortaya çıkar.

Güvenlik endişelerini gidermek için geniş bant hizmetleri, VPN bağlantılarını kabul eden bir ağ cihazına Sanal Özel Ağlar-Virtual Private Network (VPN) bağlantıları sağlar. Ağ cihazı tipik olarak kurumsal komunda bulunur.

VPN, internet gibi genel bir ağ üzerinden özel ağlar arasında şifrelenmiş bir bağlantıdır. Kiralık bir hat gibi özel bir Katman 2 bağlantısı kullanmak yerine VPN, VPN tünelleri adı verilen sanal bağlantıları kullanır. VPN tünelleri, internet üzerinden şirketin özel ağından uzak siteye veya çalışan ana bilgisayarına yönlendirilir.

Aşağıdakiler, VPN kullanmanın birkaç avantajıdır:

- Maliyet tasarrufu - VPN'ler, kuruluşların uzak ofisleri bağlamak ve uzak kullanıcıları ana kurumsal siteye bağlamak için küresel interneti kullanmalarını sağlar. Bu pahalı, özel WAN bağlantılarını ve modem bankalarını ortadan kaldırır.
- Güvenlik - VPN'ler, verileri yetkisiz erişime karşı koruyan gelişmiş şifreleme ve kimlik doğrulama protokolleri kullanarak en yüksek düzeyde güvenlik sağlar.
- Ölçeklenebilirlik - VPN'ler ISS'ler ve cihazlar içindeki internet altyapısını kullandığından, yeni kullanıcılar eklemek kolaydır. Kurumlar, önemli bir altyapı eklemeden büyük miktarlarda kapasite ekleyebilir.
- Geniş bant teknolojisi ile uyumluluk - VPN teknolojisi, DSL ve kablo gibi geniş bant servis sağlayıcıları tarafından desteklenir. VPN'ler, mobil çalışanların ve telekomünikasyon çalışanlarının kurumsal ağlarına erişmek için evlerinin yüksek hızlı internet hizmetinden yararlanmalarına olanak tanır. İşletme sınıfı, yüksek hızlı geniş bant bağlantıları, uzak ofisleri bağlamak için uygun maliyetli bir çözüm de sağlayabilir.

VPN'ler genellikle şu şekilde uygulanır:

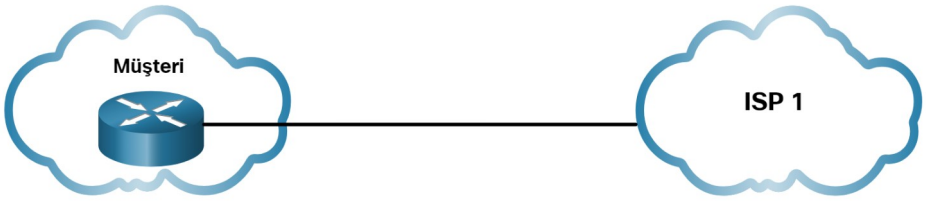
Siteden siteye VPN - VPN ayarları yönlendiricilerde yapılandırılır. Müşteriler verilerinin şifrelendiğinin farkında değiller.
Uzaktan Erişim - Kullanıcı farkındadır ve uzaktan erişim bağlantısını başlatır. Örneğin, bankanıza bağlanmak için bir tarayıcıda HTTPS kullanmak. Alternatif olarak, kullanıcı hedef cihaza bağlanmak ve kimlik doğrulaması yapmak için ana bilgisayarında VPN istemci yazılımını çalıştırabilir.

Not : VPN'ler bu kitabın ilerleyen kısımlarında daha ayrıntılı olarak anlatılacaktır.

## 36.5.8.ISP Bağlantı Seçenekleri

### Tek bağlantılı

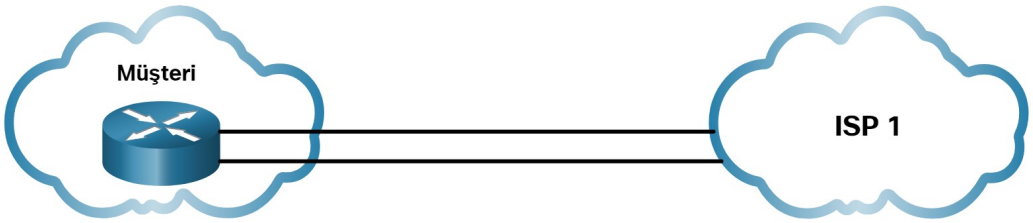
Tek bağlantılı ISP bağlantısı, internet erişiminin operasyon için çok önemli olmadığı durumlarda kuruluş tarafından kullanılır. Şekilde gösterildiği gibi, istemci bir bağlantı kullanarak ISP'ye bağlanır. Topoloji artıklık sağlamaz. Bu, gösterilen dört çözüm arasında en ucuz çözümdür.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

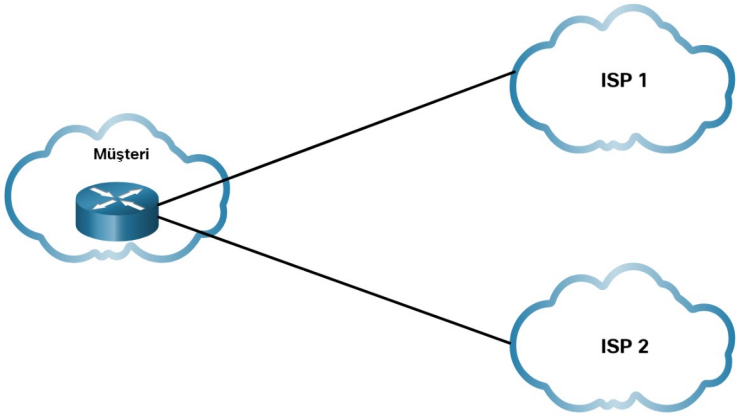
### Çift bağlantılı

Çift bağlantılı ISP bağlantısı, internet erişiminin operasyon için biraz önemli olduğu durumlarda bir kuruluş tarafından kullanılır. Şekilde gösterildiği gibi, istemci aynı ISP'ye iki bağlantı kullanarak bağlanır. Topoloji hem artıklık hem de yük dengeleme sağlar. Bir bağlantı başarısız olursa, diğer bağlantı trafiği taşıyabilir. Her iki bağlantı da çalışıyorsa, trafik bunlar üzerinden yük dengelenebilir. Ancak, ISP bir kesinti yaşarsa kuruluş internet bağlantısını kaybeder.



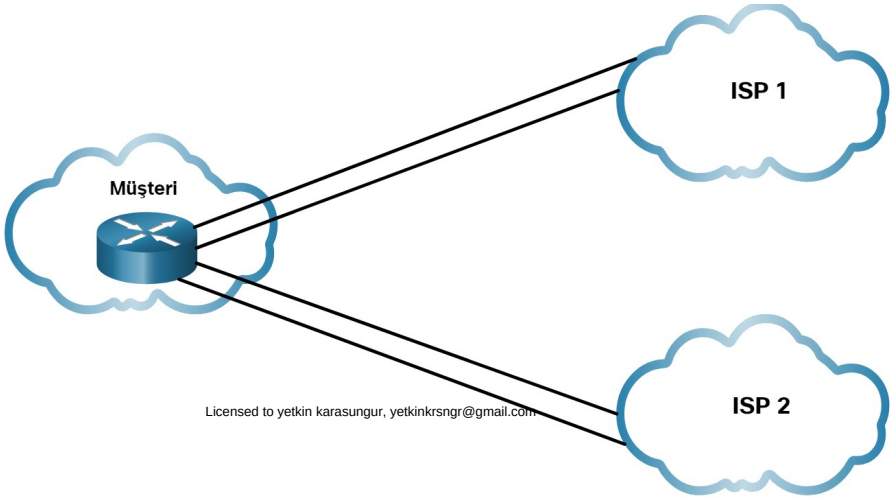

### Birden çok ağ bağlantılı

Çok ana bilgisayarlı ISP bağlantısı, internet erişiminin operasyon için çok önemli olduğu durumlarda bir kuruluş tarafından kullanılır. İstemci, şekilde gösterildiği gibi iki farklı ISP'ye bağlanır. Bu tasarım, daha fazla yedeklilik sağlar ve yük dengelemeye olanak tanır, ancak pahalı olabilir.




### Çift ağ bağlantılı

Dual-multihomed, gösterilen dördü arasında en esnek topolojidir. Müşteri, şekilde gösterildiği gibi, birden çok ISS'ye yedek bağlantılarla bağlanır. Bu topoloji, mümkün olan en fazla yedekliliği sağlar. Dördü arasında en pahalı seçenektir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

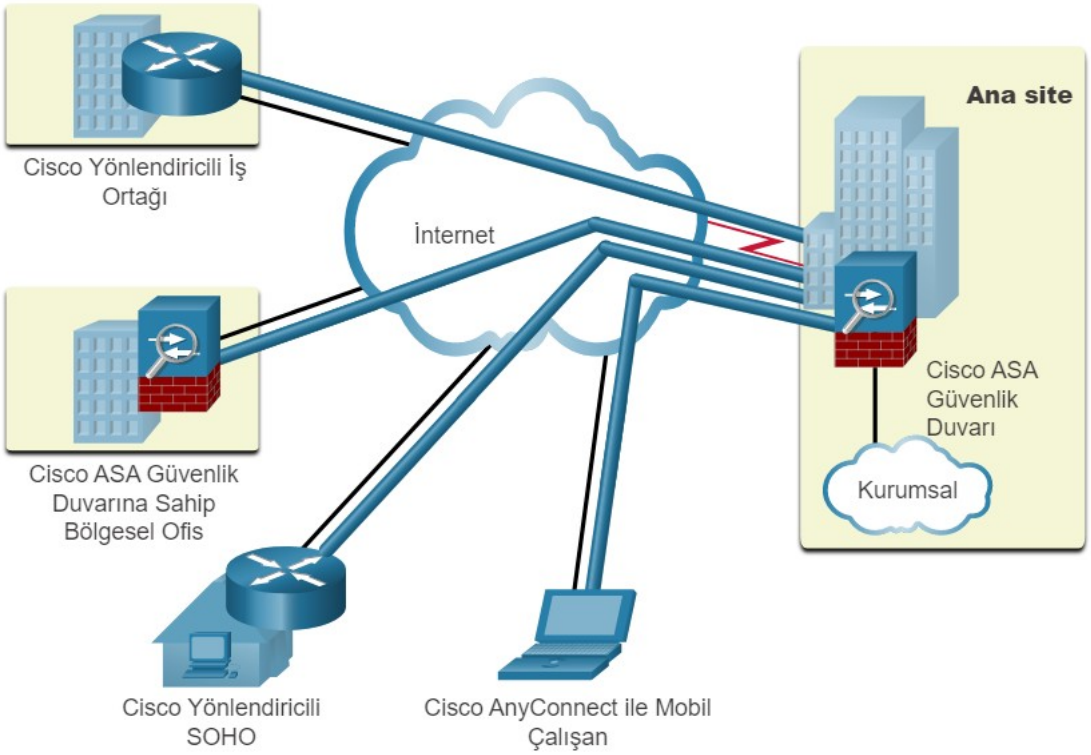
# 37.Bölüm: VPN ve IPsec

## 37.1.VPN (Virtual Private Network) Teknolojisi

### 37.1.1. VPN (Sanal Özel Ağlar)

Kuruluşlar, siteler (konumlar) ve kullanıcılar arasındaki ağ trafiğini güvence altına almak için uçtan uca özel ağ bağlantıları oluşturmak için sanal özel ağları (VPN'ler) kullanır. Bir VPN, bilgileri özel bir ağ içinde taşıdığı için sanaldır, ancak bu bilgi aslında genel bir ağ üzerinden taşınır. Bir VPN, genel ağ üzerinden taşınırken verileri gizli tutmak için trafiğin şifrelenmesi açısından özeldir.

Şekilde, bir işletmenin ana sitesi tarafından yönetilen çeşitli VPN türlerinin bir koleksiyonu gösterilmektedir. Tünel, uzak sitelerin ve kullanıcıların ana sitenin ağ kaynaklarına güvenli bir şekilde erişmesini sağlar.




- Cisco Adaptive Security Appliance (ASA) güvenlik duvarı, kuruluşların VPN'ler dahil güvenli, yüksek performanslı bağlantı ve uzak şubeler ve mobil kullanıcılar için her zaman açık erişim sağlamasına yardımcı olur.
- SOHO, VPN etkin yönlendiricinin kurumsal ana siteye tekrar VPN bağlantısı sağlayabildiği küçük ofis ev ofisi anlamına gelir.
- Cisco AnyConnect, uzaktaki çalışanların ana site ile istemci tabanlı VPN bağlantısı kurmak için kullanabilecekleri bir yazılımdır.

İlk VPN türleri, verilerin kimlik doğrulamasını veya şifrelenmesini içermeyen kesinlikle IP tünelleriydi. Örneğin, Generic Routing Encapsulation (GRE), Cisco tarafından geliştirilen ve şifreleme hizmetlerini içermeyen bir tünel protokolüdür. Sanal bir noktadan noktaya bağlantı oluşturmak için bir IP tüneli içinde IPv4 ve IPv6 trafiğini kapsüllemek için kullanılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 37.1.2.VPN Avantajları

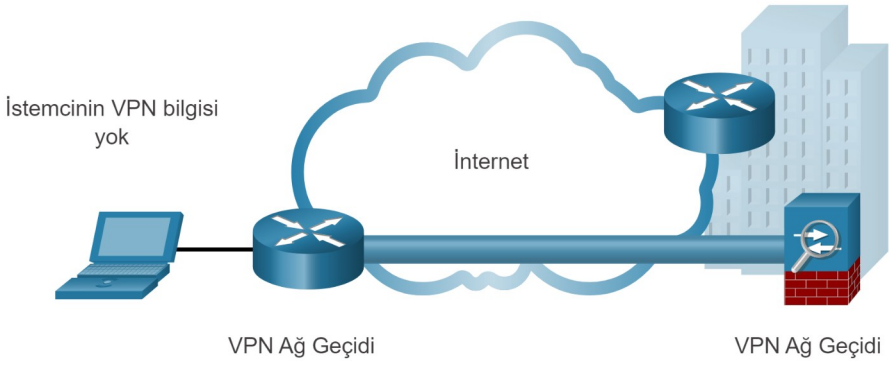
Modern VPN'ler siteler arasındaki ağ trafiğinin güvenliğini sağlamak için İnternet Protokolü Güvenliği-Internet Protocol Security (IPsec) ve Güvenli Yuva Katmanı-Secure Sockets Layer (SSL) VPN'ler gibi şifreleme özelliklerini desteklemektedir.

VPN'lerin başlıca faydaları tabloda gösterilmektedir.

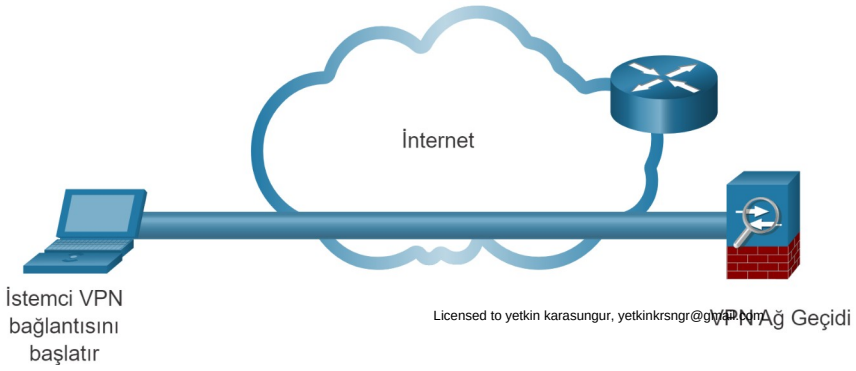
| Avantaj | Açıklama |
|---|---|
| Tasarruf | Uygun maliyetli, yüksek bant genişliğine sahip teknolojilerin ortaya çıkmasıyla, kuruluşlar bağlantı maliyetlerini düşürmek ve aynı zamanda uzak bağlantı bant genişliğini artırmak için VPN'leri kullanabilir. |
| Güvenlik | VPN'ler, verileri yetkisiz erişime karşı koruyan gelişmiş şifreleme ve kimlik doğrulama protokollerini kullanarak mümkün olan en yüksek güvenlik düzeyini sağlar. |
| Ölçeklenebilirlik | VPN'ler, kuruluşların interneti kullanmasına izin vererek önemli bir altyapı eklemeden yeni kullanıcılar eklemeyi kolaylaştırır. |
| Uyumluluk | VPN'ler, tüm popüler geniş bant teknolojileri dahil olmak üzere çok çeşitli WAN bağlantı seçeneklerine uygulanabilir. Uzaktaki çalışanlar, kurumsal ağlarına güvenli erişim sağlamak için bu yüksek hızlı bağlantılardan yararlanabilir. |

## 37.1.3.Siteden Siteye ve Uzaktan Erişim (Site to Site-Remote Access) VPN'leri

Siteden siteye VPN, VPN ağ geçitleri olarak da adlandırılan VPN sonlandırma cihazları, güvenli bir tünel oluşturmak için bilgilerle önceden yapılandırıldığında oluşturulur. VPN trafiği yalnızca bu cihazlar arasında şifrelenir. Dahili ana bilgisayarlar, bir VPN'in kullanıldığına dair hiçbir bilgiye sahip değildir.




Bir uzaktan erişim VPN, bir istemci ile VPN sonlandırma cihazı arasında güvenli bir bağlantı kurmak için dinamik olarak oluşturulur. Örneğin, bankacılık bilgilerinizi çevrimiçi olarak kontrol ettiğinizde uzaktan erişim SSL VPN kullanılır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

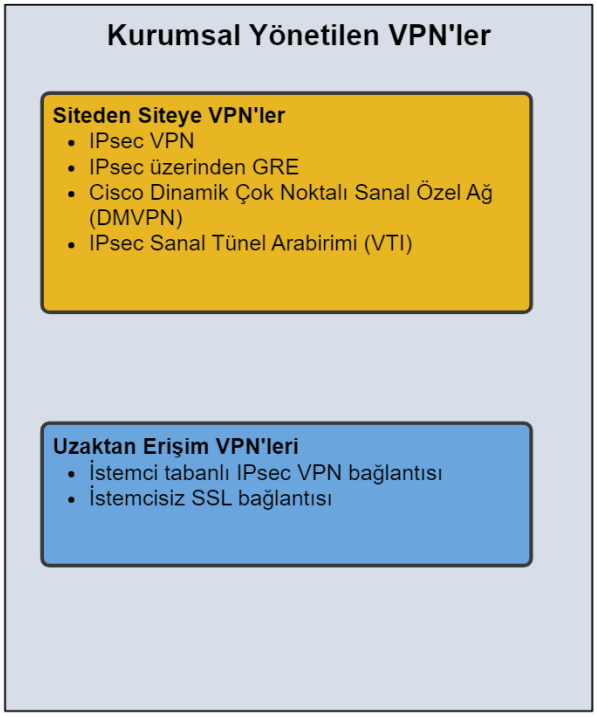
### 37.1.4.Kurumsal ve Servis Sağlayıcı VPN'leri

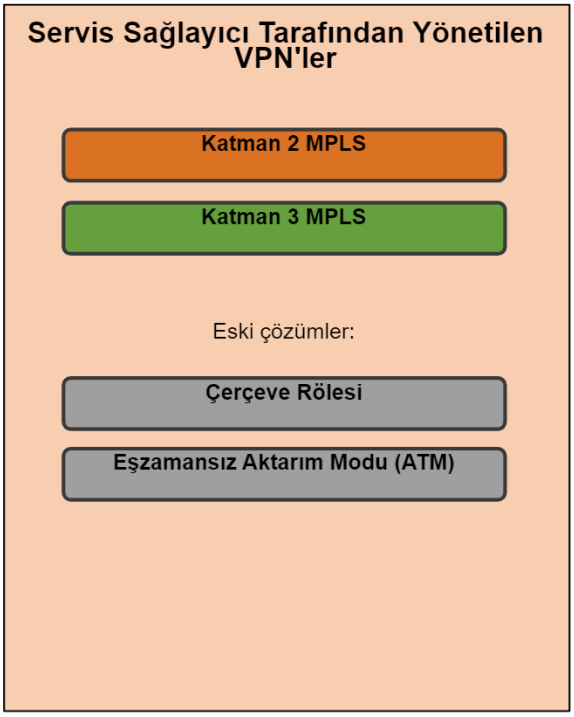
Kurumsal trafiği güvence altına almak için birçok seçenek mevcuttur. Bu çözümler, VPN'i kimin yönettiğine bağlı olarak değişir.

VPN'ler şu şekilde yönetilebilir ve dağıtılabilir:

- Kurumsal VPN'ler - Kurumsal yönetilen VPN'ler, internet üzerinden kurumsal trafiği güvence altına almak için yaygın bir çözümdür. Siteden siteye ve uzaktan erişim VPN'leri, kuruluş tarafından hem IPsec hem de SSL VPN'ler kullanılarak oluşturulur ve yönetilir.
- Servis Sağlayıcı VPN'leri - Servis sağlayıcı tarafından yönetilen VPN'ler, sağlayıcı ağı üzerinden oluşturulur ve yönetilir. Sağlayıcı, bir kuruluşun siteleri arasında güvenli kanallar oluşturmak için Katman 2 veya Katman 3'te Çok Protokollü Etiket Değiştirme'yi (MPLS) kullanır. MPLS, sağlayıcının siteler arasında sanal yollar oluşturmak için kullandığı bir yönlendirme teknolojisidir. Bu, trafiği diğer müşteri trafiğinden etkili bir şekilde ayırır. Diğer eski çözümler arasında Frame Relay ve Asynchronous Transfer Mode (ATM) VPN'ler bulunur.

Şekilde, bu modülde daha ayrıntılı olarak ele alınacak olan, işletme tarafından yönetilen ve servis sağlayıcı tarafından yönetilen farklı VPN dağıtım türleri listelenmektedir.




## 37.2.VPN Türleri

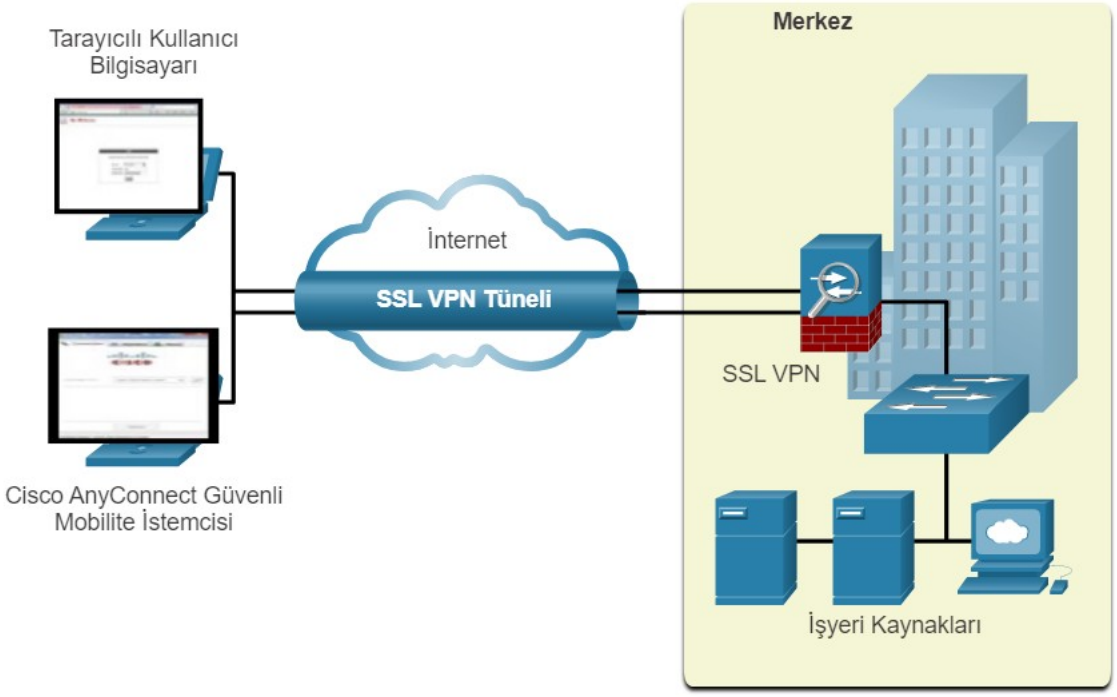
### 37.2.1.Uzaktan Erişim VPN'leri

VPN'ler, birçok nedenden ötürü uzaktan erişim bağlantısı için mantıksal çözüm haline gelmiştir. Şekilde gösterildiği gibi, uzaktan erişim VPN'leri, uzak ve mobil kullanıcıların şifreli bir tünel oluşturarak kuruma güvenli bir şekilde bağlanmasına izin verir. Uzak kullanıcılar, e-posta ve ağ uygulamaları dahil olmak üzere kurumsal güvenlik erişimlerini güvenli bir şekilde çoğaltabilir. Uzaktan erişim VPN'leri ayrıca yüklenicilerin ve ortakların gerektiğinde belirli sunuculara, web sayfalarına veya dosyalara sınırlı erişime sahip olmasına izin verir. Bu, bu kullanıcıların ağ güvenliğinden ödün vermeden iş verimliliğine katkıda bulunabileceği anlamına gelir.

Licensed to yetkin karasungur,yetkinkrsngr@gmail.com

Uzaktan erişim VPN'leri, genellikle gerektiğinde kullanıcı tarafından dinamik olarak etkinleştirilir. Uzaktan erişim VPN'leri, IPsec veya SSL kullanılarak oluşturulabilir. Şekilde gösterildiği gibi, bir uzak kullanıcı bir uzaktan erişim VPN bağlantısı başlatmalıdır.

Şekil, bir uzak kullanıcının bir uzaktan erişim VPN bağlantısı başlatabileceği iki yolu göstermektedir: istemcisiz VPN ve istemci tabanlı VPN.




- **İstemcisiz VPN bağlantısı** - Bağlantı, bir web tarayıcısı SSL bağlantısı kullanılarak güvence altına alınır. SSL, çoğunlukla HTTP trafiğini (HTTPS) ve IMAP ve POP3 gibi e-posta protokollerini korumak için kullanılır. Örneğin, HTTPS aslında bir SSL tüneli kullanan HTTP'dir. İlk olarak SSL bağlantısı kurulur ve ardından bağlantı üzerinden HTTP verileri değiş tokuş edilir.
- **İstemci tabanlı VPN bağlantısı** - Cisco AnyConnect Secure Mobility Client gibi VPN istemci yazılımı uzak kullanıcının uç cihazına yüklenmelidir. Kullanıcılar VPN istemcisini kullanarak VPN bağlantısını başlatmalı ve ardından hedef VPN ağ geçidinde kimlik doğrulamalıdır. Uzak kullanıcıların kimliği doğrulandığında, kurumsal dosyalara ve uygulamalara erişimleri olur. VPN istemci yazılımı, IPsec veya SSL kullanarak trafiği şifreler ve bunu internet üzerinden hedef VPN ağ geçidine iletir.

## 37.2.2.SSL VPN'ler

Bir istemci VPN ağ geçidi ile bir SSL VPN bağlantısı üzerinde anlaştığında, aslında Taşıma Katmanı Güvenliği-Transport Layer Security (TLS) kullanarak bağlanır. TLS, SSL'nin yeni sürümüdür ve bazen SSL / TLS olarak ifade edilir. Bununla birlikte, her iki terim de genellikle birbirinin yerine kullanılır.

SSL, eşlerin kimliğini doğrulamak için ortak anahtar altyapısını ve dijital sertifikaları kullanır. Hem IPsec hem de SSL VPN teknolojileri, neredeyse tüm ağ uygulamalarına veya kaynaklarına erişim sağlar. Bununla birlikte, güvenlik bir sorun olduğunda, IPsec üstün bir seçimdir. Destek ve dağıtım kolaylığı birincil sorunlarsa, SSL'yi düşünün. Uygulanan VPN yönteminin türü, kullanıcıların erişim gereksinimlerine ve kuruluşun BT süreçlerine bağlıdır.

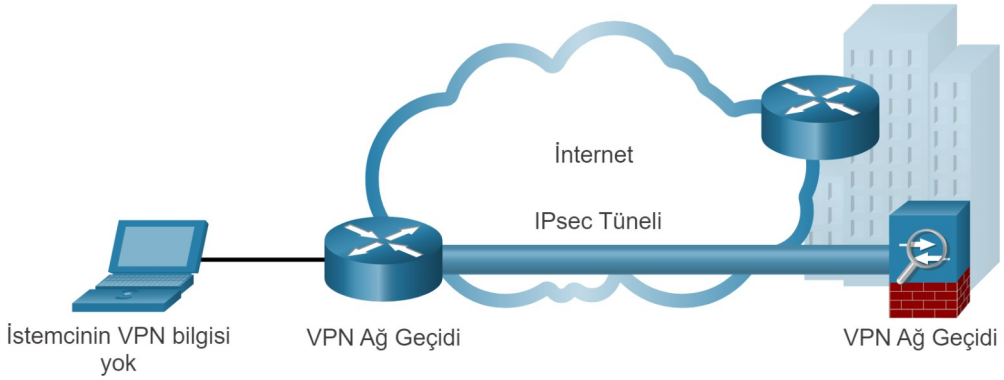
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tablo, IPsec ve SSL uzaktan erişim dağıtımlarını karşılaştırmaktadır.

| Özellik | IPsec | SSL |
|---|---|---|
| Desteklenen uygulamalar | Kapsamlı- Tüm IP tabanlı uygulamalar desteklenir. | Sınırlı- Yalnızca web tabanlı uygulamalar ve dosya paylaşımı desteklenir. |
| Kimlik doğrulama gücü | Güçlü- Paylaşılan anahtarlar veya dijital sertifikalarla iki yönlü kimlik doğrulaması kullanır. | Orta- Tek yönlü veya iki yönlü kimlik doğrulama kullanma. |
| Şifreleme Gücü | Güçlü- 56 bit ile 256 bit arasında anahtar uzunlukları kullanır. | Orta ila güçlü- 40 bit ile 256 bit arası anahtar uzunlukları. |
| Bağlantı karmaşıklığı | Orta- Çünkü bir ana bilgisayara önceden yüklenmiş bir VPN istemcisi gerektirir. | Düşük- Yalnızca bir ana bilgisayarda web tarayıcısı gerektirir. |
| Bağlantı seçeneği | Sınırlı- Yalnızca belirli yapılandırmalara sahip belirli cihazlar bağlanabilir. | Kapsamlı- Web tarayıcısı olan herhangi bir cihaz bağlanabilir. |

## 37.2.3.Siteden Siteye IPsec VPN'ler

Siteden siteye VPN'ler, ağları internet gibi başka bir güvenilmeyen ağa bağlamak için kullanılır. Siteden siteye VPN'de, son ana bilgisayarlar bir VPN sonlandırma cihazı aracılığıyla normal şifrelenmemiş TCP / IP trafiği gönderir ve alır. VPN sonlandırmasına genellikle VPN ağ geçidi denir. Bir VPN ağ geçidi cihazı, şekilde gösterildiği gibi bir yönlendirici veya bir güvenlik duvarı olabilir. Örneğin, şeklin sağ tarafında gösterilen Cisco Adaptive Security Appliance (ASA), güvenlik duvarı, VPN yoğunlaştırıcı ve izinsiz giriş önleme işlevini tek bir yazılım görüntüsünde birleştiren bağımsız bir güvenlik duvarı cihazıdır.




VPN ağ geçidi, giden trafiği kapsüller ve şifreler. Ardından trafiği bir VPN tüneli üzerinden internet üzerinden hedef sitedeki bir VPN ağ geçidine gönderir. Trafik alındıktan sonra, alıcı VPN ağ geçidi başlıkları çıkarır, içeriğin şifresini çözer ve paketi kendi özel ağı içindeki hedef ana bilgisayara iletir.

Siteden siteye VPN'ler genellikle IP güvenliği (IPsec) kullanılarak oluşturulur ve güvence altına alınır.

## 37.2.4.IPsec üzerinden GRE

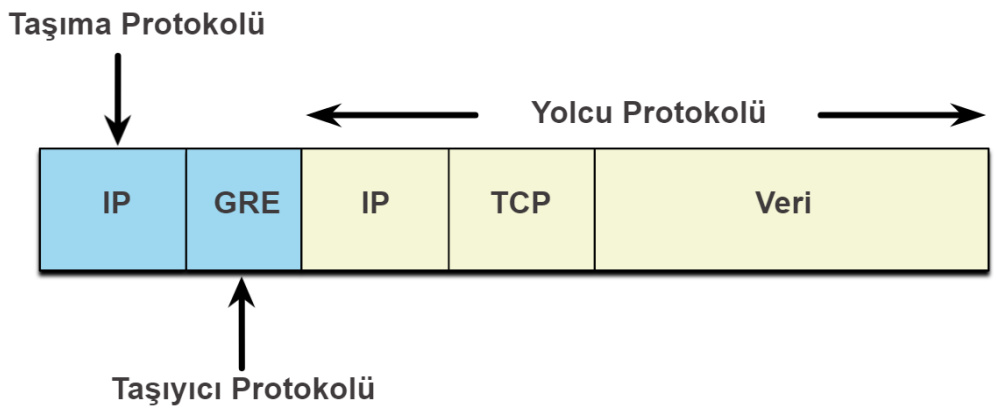
Generic Routing Encapsulation (GRE), güvenli olmayan bir siteden siteye VPN tünelleme protokolüdür. Çeşitli ağ katmanı protokollerini kapsayabilir. Ayrıca, kuruluşun bir VPN üzerinden çalışmak için yönlendirme protokollerine ihtiyaç duyması durumunda gerekli olabilecek çoklu yayın ve yayın trafiğini de destekler. Ancak, GRE varsayılan olarak şifrelemeyi desteklemez; ve bu nedenle, güvenli bir VPN tüneli sağlamaz.

Standart bir IPsec VPN (GRE olmayan) yalnızca tek noktaya yayın trafiği için güvenli tüneller oluşturabilir. Bu nedenle, yönlendirme protokolleri, bir IPsec VPN üzerinden yönlendirme bilgisi alışverişi yapmaz.

Bu sorunu çözmek için, bir GRE paketi kullanarak yönlendirme protokolü trafiğini kapsülleyebilir ve ardından GRE paketini, hedef VPN ağ geçidine güvenli bir şekilde iletmek için bir IPsec paketine kapsülleyebiliriz.

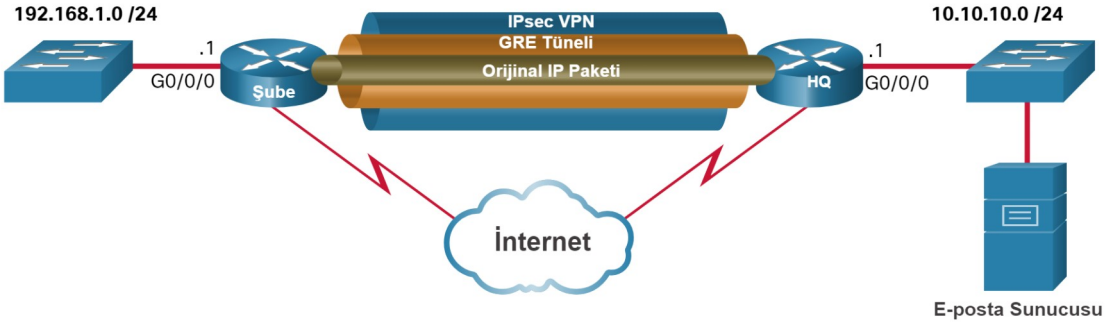
Kadersiz Ayşe'nin Kayıtlarıdır, yetkili olmadan çoğaltılamaz

GRE'nin IPsec tüneli üzerinden kapsüllenmesini açıklamak için kullanılan terimler, şekilde gösterildiği gibi yolcu protokolü, taşıyıcı protokolü ve taşıma protokolüdür.

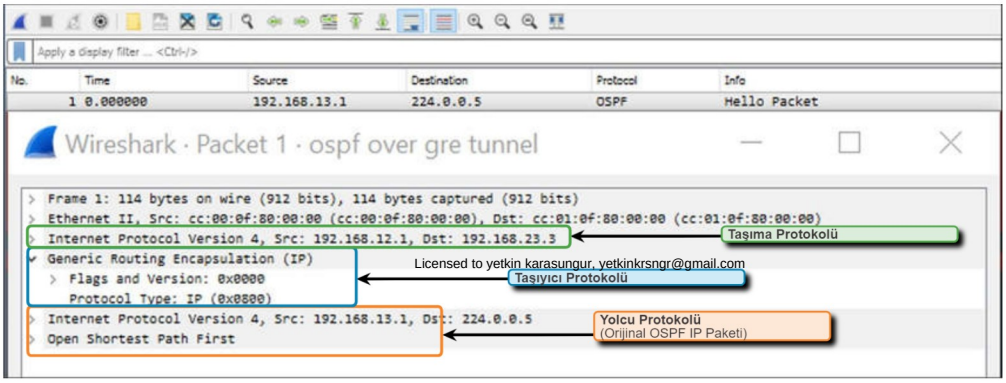



- **Yolcu protokolü** – Bu, GRE tarafından kapsüllenecek orijinal pakettir. Bir IPv4 veya IPv6 paketi, bir yönlendirme güncellemesi ve daha fazlası olabilir.
- **Taşıyıcı protokolü** – GRE, orijinal yolcu paketini kapsayan taşıyıcı protokolüdür.
- **Taşıma protokolü** – Bu, aslında paketi iletmek için kullanılacak protokoldür. Bu IPv4 veya IPv6 olabilir.

Örneğin, bir topolojiyi görüntüleyen şekilde, Branch ve HQ, bir IPsec VPN üzerinden OSPF yönlendirme bilgilerini değiş tokuş etmek ister. Ancak IPsec, çok noktaya yayın trafiğini desteklemez. Bu nedenle, IPsec üzerinden GRE, IPsec VPN üzerinden yönlendirme protokolü trafiğini desteklemek için kullanılır. Spesifik olarak, OSPF paketleri (yani, yolcu-passenger protokolü) GRE (yani, taşıyıcı protokolü) tarafından kapsüllenecek ve ardından bir IPsec VPN tünelinde kapsüllenecektir.




Şekildeki Wireshark ekran görüntüsü, GRE kullanılarak IPsec üzerinden gönderilen bir OSPF Merhaba paketini gösterir. Örnekte, orijinal OSPF Hello çok noktaya yayın paketi (yani, yolcu (passenger) protokolü), daha sonra başka bir IP başlığı (yani, taşıma protokolü) tarafından kapsüllenen bir GRE başlığı (yani, taşıyıcı protokolü) ile kapsüllenmiştir. Bu IP başlığı daha sonra bir IPsec tüneli üzerinden iletilecektir.



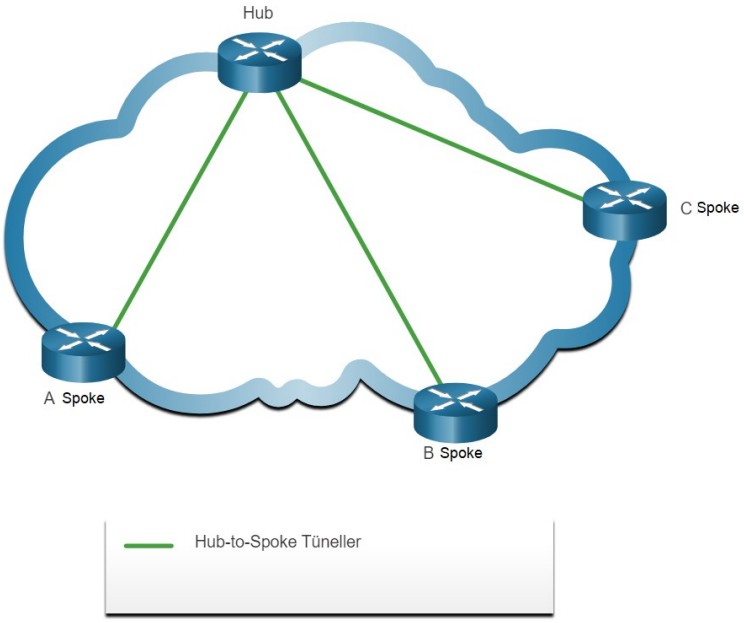
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 37.2.5.Dinamik Çok Noktalı VPN'ler (Dynamic Multipoint VPNs)

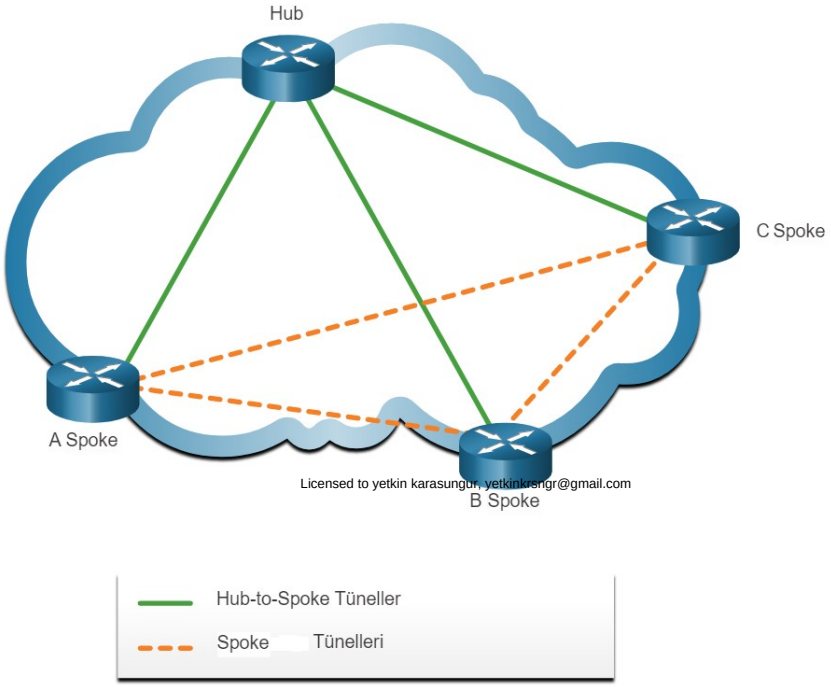
Siteden siteye IPsec VPN'ler ve IPsec üzerinden GRE, güvenli bir şekilde bağlantı için yalnızca birkaç site olduğunda kullanım için yeterlidir. Ancak, işletme çok daha fazla site eklediğinde bunlar yeterli değildir. Bunun nedeni, her sitenin diğer tüm sitelere veya merkezi bir siteye statik yapılandırmalar gerektirmesidir.

Dinamik Çok Noktalı VPN (Dynamic Multipoint VPN-DMVPN), kolay, dinamik ve ölçeklenebilir bir şekilde birden fazla VPN oluşturmak için bir Cisco yazılım çözümüdür. Diğer VPN türleri gibi, DMVPN internet gibi halka açık ağlar üzerinden güvenli aktarım sağlamak için IPsec'e güvenir.

DMVPN, VPN tüneli yapılandırmasını basitleştirir ve merkezi bir siteyi şube sitelerine bağlamak için esnek bir seçenek sunar. Tam bir ağ topolojisi oluşturmak için bir hub ve bağlı bileşen yapılandırması kullanır. Sözlü siteler, şekilde gösterildiği gibi, hub sitesi ile güvenli VPN tünelleri oluşturur.




Her site, Multipoint Generic Routing Encapsulation (mGRE) kullanılarak yapılandırılır . MGRE tünel arabirimi, tek bir GRE arabiriminin birden çok IPsec tünelini dinamik olarak desteklemesini sağlar. Bu nedenle, yeni bir site güvenli bir bağlantı gerektirdiğinde, hub sitesindeki aynı yapılandırma tüneli destekleyecektir. Ek bir yapılandırma gerekmeyecektir.
Spoke siteler ayrıca merkezi siteden diğer konuşulan siteler hakkında bilgi edinebilir ve şekilde gösterildiği gibi sanal spoke-spoke tünelleri oluşturabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 37.2.6.IPsec Sanal Tünel Arayüzü(IPsec Virtual Tunnel Interface)

DMVPN'ler gibi, IPsec Sanal Tünel Arabirimi (VTI), birden çok siteyi ve uzaktan erişimi desteklemek için gereken yapılandırma sürecini basitleştirir. IPsec VTI yapılandırmaları, IPsec oturumlarını fiziksel bir arabirimle statik eşlemek yerine sanal bir arabirime uygulanır.

IPsec VTI, hem IP tek noktaya yayın hem de çok noktaya yayın şifreli trafiği gönderip alabilir. Bu nedenle, yönlendirme protokolleri GRE tünellerini yapılandırmaya gerek kalmadan otomatik olarak desteklenir.

IPsec VTI, siteler arasında veya bir hub ve bağlı bileşen topolojisinde yapılandırılabilir.

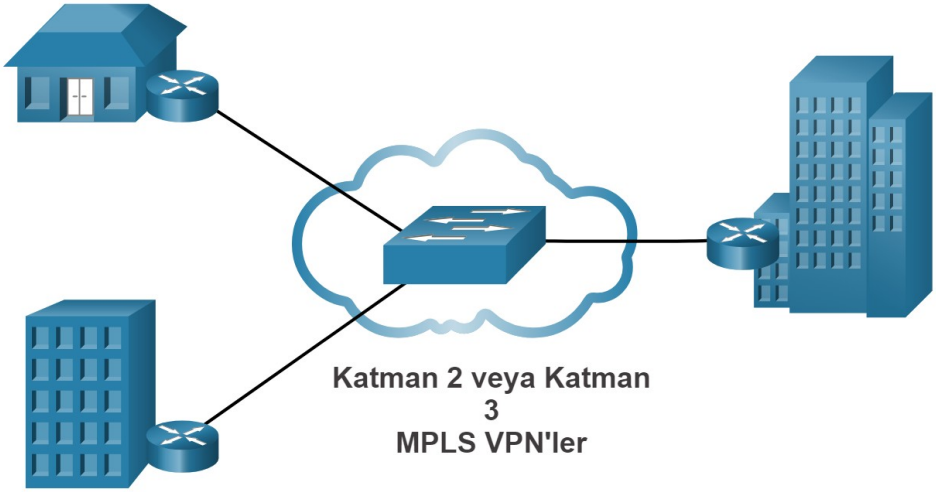
## 37.2.7.Servis Sağlayıcı MPLS VPN'leri

Kiralık hatlar, Frame Relay ve ATM bağlantıları gibi geleneksel hizmet sağlayıcı WAN çözümleri, tasarımlarında doğal olarak güvenliydi. Günümüzde servis sağlayıcılar, çekirdek ağlarında MPLS kullanıyor. Trafik, daha önce çekirdek yönlendiriciler arasında dağıtılan etiketler kullanılarak MPLS omurgası üzerinden iletilir. Eski WAN bağlantıları gibi, trafik güvenlidir çünkü servis sağlayıcı müşteriler birbirlerinin trafiğini göremezler.

MPLS, müşterilere yönetilen VPN çözümleri sağlayabilir; bu nedenle, müşteri siteleri arasındaki trafiğin güvenliğini sağlamak hizmet sağlayıcının sorumluluğundadır. Servis sağlayıcılar tarafından desteklenen iki tür MPLS VPN çözümü vardır:

- Katman 3 MPLS VPN - Hizmet sağlayıcı, müşterinin yönlendiricileri ile sağlayıcının yönlendiricileri arasında bir eşleme kurarak müşteri yönlendirmesine katılır. Ardından sağlayıcının yönlendiricisi tarafından alınan müşteri yolları, MPLS ağı üzerinden müşterinin uzak konumlarına yeniden dağıtılır.
- Layer 2 MPLS VPN - Servis sağlayıcı, müşteri yönlendirmesine dahil değildir. Bunun yerine sağlayıcı, MPLS ağı üzerinden bir Ethernet çoklu erişimli LAN kesimini taklit etmek için bir Sanal Özel LAN Hizmeti-Private LAN Service (VPLS) dağıtır. Yönlendirme dahil değildir. Müşterinin yönlendiricileri etkin bir şekilde aynı çoklu erişim ağına aittir.

Şekil, hem Katman 2 hem de Katman 3 MPLS VPN'leri sunan bir hizmet sağlayıcıyı göstermektedir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 37.3.IPsec

### 37.3.1.IPsec Teknolojileri

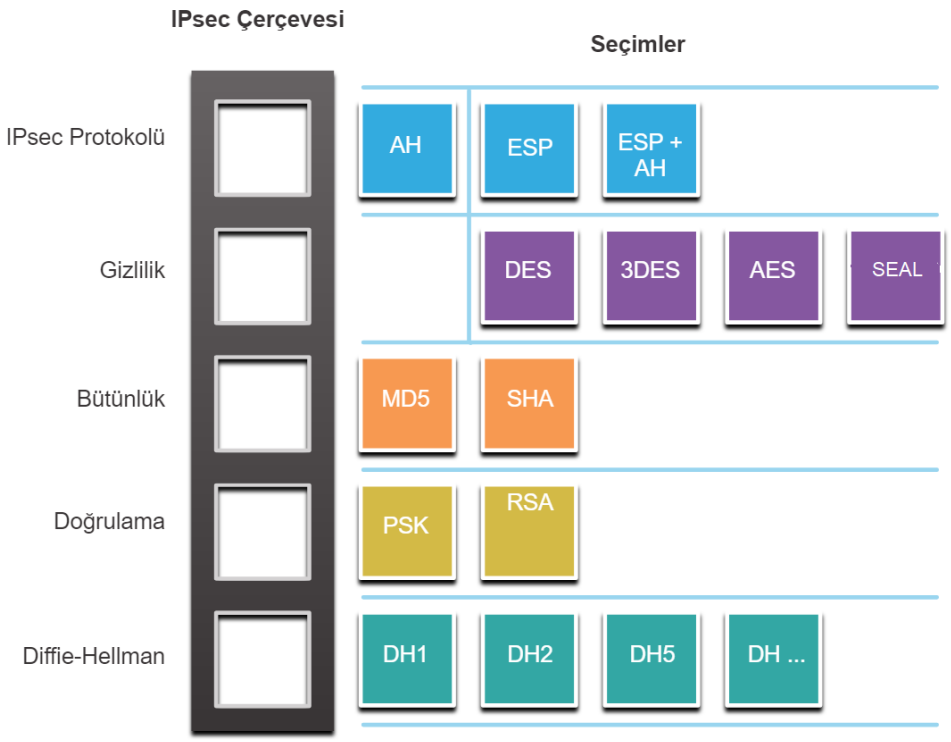
IPsec, bir VPN'in IP ağları arasında nasıl güvenli hale getirilebileceğini tanımlayan bir IETF standardıdır (RFC 2401-2412). IPsec, kaynak ve hedef arasındaki IP paketlerini korur ve doğrular. IPsec, Katman 4'ten Katman 7'ye kadar olan trafiği koruyabilir.

IPsec çerçevesini kullanarak IPsec şu temel güvenlik işlevlerini sağlar:

- Gizlilik - IPsec, siber suçluların paket içeriğini okumasını önlemek için şifreleme algoritmaları kullanır.
- Bütünlük - IPsec, kaynak ve hedef arasında paketlerin değiştirilmediğinden emin olmak için karma algoritmalar kullanır.
- Kaynak kimlik doğrulaması - IPsec, kaynak ve hedefin kimliğini doğrulamak için İnternet Anahtar Değişimi-Internet Key Exchange (IKE) protokolünü kullanır. Önceden paylaşılan anahtarlar (şifreler), dijital sertifikalar veya RSA sertifikaları dahil olmak üzere kimlik doğrulama yöntemleri.
- Diffie-Hellman - Genellikle DH algoritmasının çeşitli gruplarını kullanarak güvenli anahtar değişimi.

IPsec, güvenli iletişim için herhangi bir özel kurala bağlı değildir. Çerçevenin bu esnekliği, IPsec'in mevcut IPsec standartlarını güncellemeden yeni güvenlik teknolojilerini kolayca entegre etmesini sağlar. Şu anda mevcut teknolojiler, kendi özel güvenlik işlevleriyle uyumludur. Şekilde IPsec çerçevesinde gösterilen açık yuvalar, benzersiz bir güvenlik ilişkisi (SA) oluşturmak için bu IPsec işlevi için mevcut olan seçeneklerden herhangi biriyle doldurulabilir.

Şekilde IPsec çerçevesi için seçenekler gösterilmektedir. Beş IPsec işlevi vardır: IPsec Protokolü, Gizlilik, Bütünlük, Kimlik Doğrulama ve Diffie-Hellman. Her işlevin mevcut seçenekleri vardır. IPsec Protokolü için seçenekler şunlardır: AH, ESP veya ESP + AH. Gizlilik için seçenekler şunlardır: DES, 3DES, AES veya SEAL. Integrity için seçenekler MD5 veya SHA'dır. Kimlik Doğrulama seçenekleri şunlardır: PSK veya RSA. Diffie-Hellman için seçenekler DH1, DH2, DH5 vb .'dir.

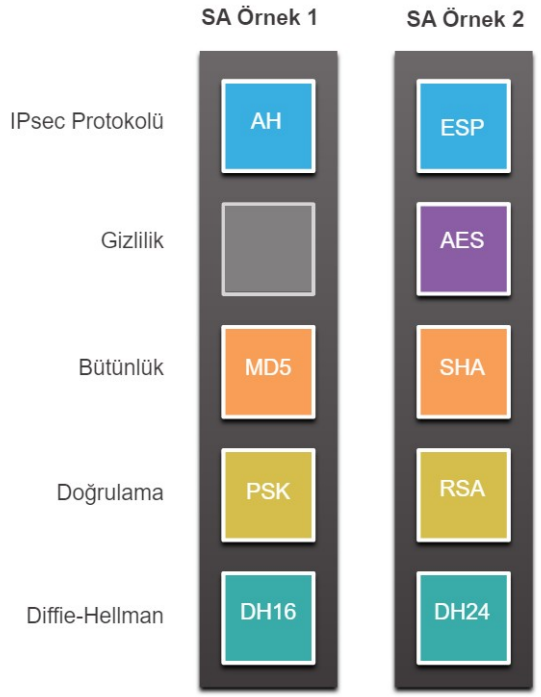



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Güvenlik işlevleri tabloda listelenmiştir.

| IPsec İşlevi | Açıklama |
|---|---|
| IPsec Protokolü | IPsec Protokolü seçenekleri arasında Kimlik Doğrulama Başlığı- Authentication Header(AH) veya Kapsülleme Güvenlik Protokolü-Encapsulation Security Protocol (ESP) bulunur. AH, Katman 3 paketinin kimliğini doğrular. ESP, Katman 3 paketini şifreler.Not: ESP + AH nadiren kullanılır çünkü bu kombinasyon bir NAT cihazını başarılı bir şekilde geçemeyecektir. |
| Gizlilik | Şifreleme, Katman 3 paketinin gizliliğini sağlar. Seçenekler arasında Veri Şifreleme Standardı-Data Encryption Standard(DES), Üçlü DES (3DES), Gelişmiş Şifreleme Standardı-Advanced Encryption Standard (AES) veya Yazılım İçin Optimize Edilmiş Şifreleme Algoritması-Software-Optimized Encryption Algorithm (SEAL) bulunur. Şifreleme de bir seçenektir. |
| Bütünlük | Mesaj özeti 5- message-digest 5(MD5) veya Güvenli Karma Algoritma-Secure Hash Algorithm (SHA) gibi bir karma algoritma kullanarak verilerin hedefe değişmeden ulaşmasını sağlar. |
| Doğrulama | IPsec, iletişimi bağımsız olarak gerçekleştirebilen kullanıcıların ve cihazların kimliğini doğrulamak için İnternet Anahtar Değişimi-Internet Key Exchange (IKE) kullanır. IKE, kullanıcı adı ve parola, tek seferlik parola, biyometri, önceden paylaşılan anahtarlar-pre-shared keys (PSK'lar) ve Rivest, Shamir ve Adleman (RSA) algoritmasını kullanan dijital sertifikalar dahil olmak üzere çeşitli kimlik doğrulama türleri kullanır. |
| Diffie-Hellman | IPsec, iki eşin paylaşılan bir gizli anahtar oluşturması için ortak bir anahtar değişim yöntemi sağlamak üzere DH algoritmasını kullanır. DH14, 15, 16 ve DH 19, 20, 21 ve 24 dahil seçilebilecek birkaç farklı grup vardır. DH1, 2 ve 5 artık önerilmemektedir. |

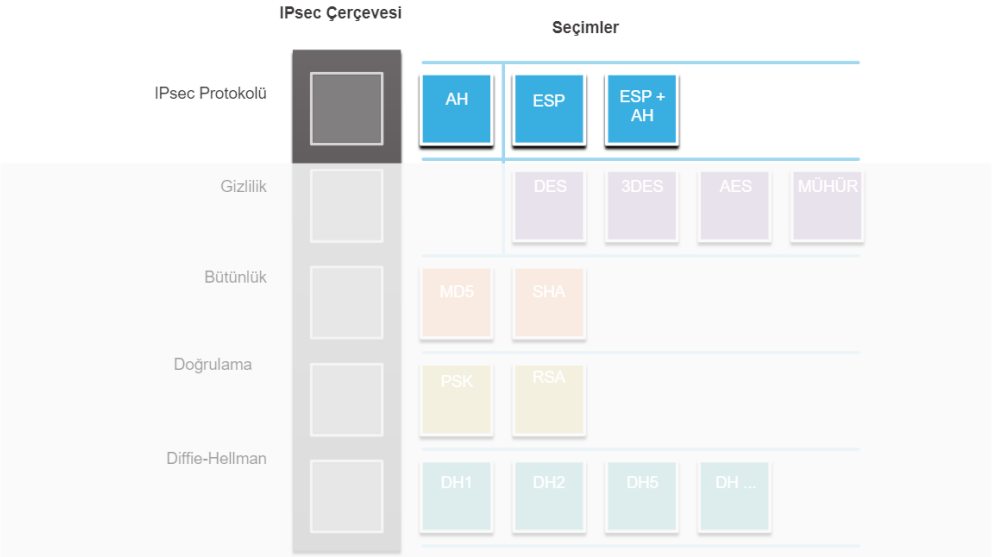
Şekilde, iki farklı uygulama için SA (Security Association) örnekleri gösterilmektedir. SA, IPsec'in temel yapı taşıdır. Bir VPN bağlantısı kurarken, eşler, anahtar değişim parametrelerini görüşmek, paylaşılan bir anahtar oluşturmak, birbirlerinin kimliğini doğrulamak ve şifreleme parametrelerini görüşmek için aynı SA'yı paylaşmalıdır. SA Örneği 1'in şifreleme kullanmadığına dikkat edin.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## IPsec Protokol Kapsüllemesi

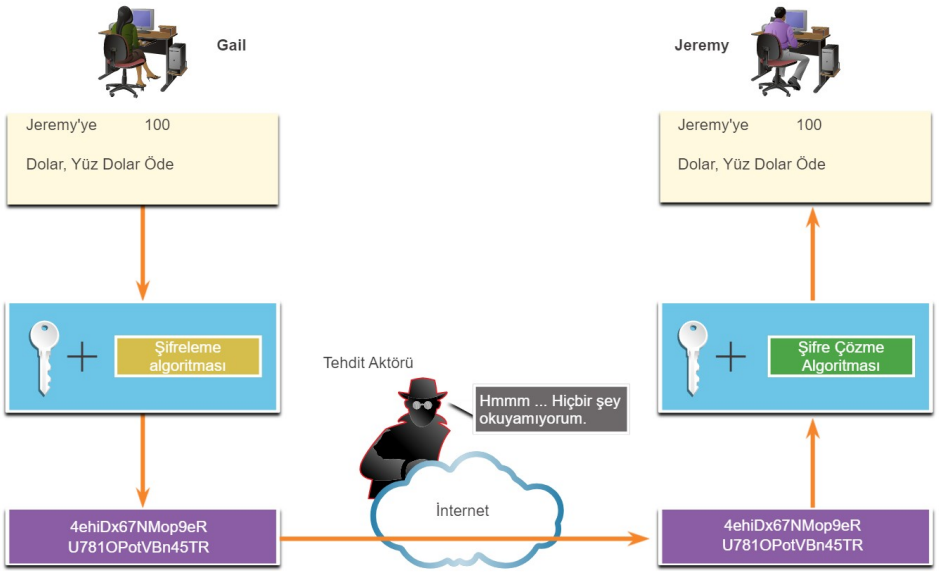
IPsec protokol kapsüllemesini seçmek, çerçevenin ilk yapı taşıdır. IPsec, Paketleri Kimlik Doğrulama Başlığı (AH) veya Kapsülleme Güvenlik Protokolü (ESP) kullanarak kapsüller. AH veya ESP seçimi, diğer hangi yapı taşlarının mevcut olduğunu belirler.




- AH, yalnızca gizlilik gerekli olmadığında veya buna izin verilmediğinde uygundur. Veri kimlik doğrulaması ve bütünlüğü sağlar, ancak veri gizliliği (şifreleme) sağlamaz. Tüm metin şifrelenmemiş olarak taşınır.
- ESP hem gizlilik hem de kimlik doğrulama sağlar. IP paketi üzerinde şifreleme yaparak gizlilik sağlar. ESP, iç IP paketi ve ESP başlığı için kimlik doğrulama sağlar. Kimlik doğrulama, veri kaynağı kimlik doğrulaması ve veri bütünlüğü sağlar. ESP'de hem şifreleme hem de kimlik doğrulama isteğe bağlı olsa da, en azından birinin seçilmesi gerekir.

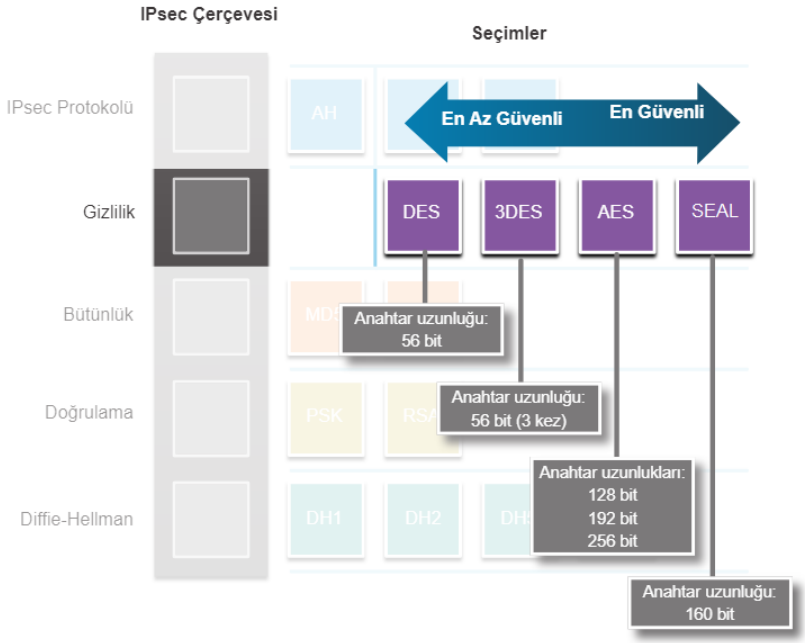
## Gizlilik

Gizlilik, şekilde gösterildiği gibi verilerin şifrelenmesiyle sağlanır. Gizlilik derecesi, şifreleme algoritmasına ve şifreleme algoritmasında kullanılan anahtarın uzunluğuna bağlıdır. Birisi bir kaba kuvvet saldırısı yoluyla anahtarı kırmaya çalışırsa, denenebilecek olasılıkların sayısı anahtarın uzunluğunun bir fonksiyonudur. Tüm olasılıkları işleme zamanı, saldıran aygıtın bilgisayar gücünün bir işlevidir. Anahtar ne kadar kısa olursa kırılması o kadar kolay olur. 64 bitlik bir anahtarın görece karmaşık bir bilgisayarla kırılması yaklaşık bir yıl alabilir. Aynı makineye sahip 128 bitlik bir anahtarın şifresinin çözülmesi kabaca 10 19 veya 10 kentilyon yıl sürebilir .




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

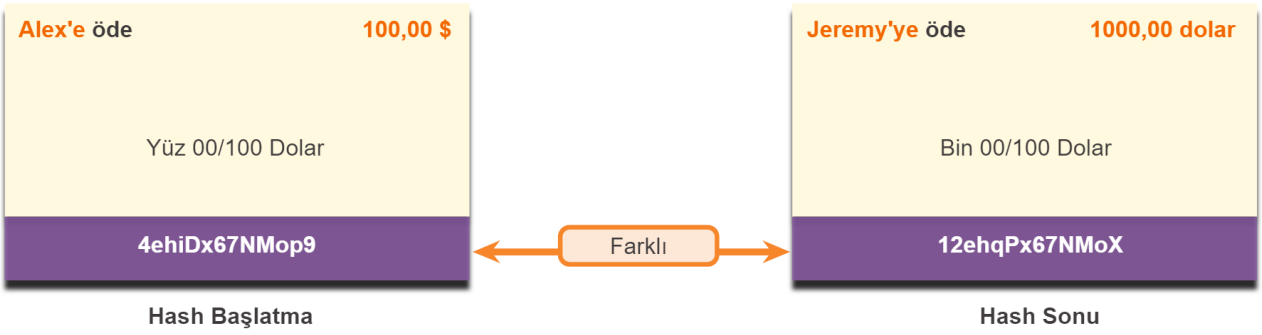
Şekilde vurgulanan şifreleme algoritmalarının tamamı simetrik anahtar şifreleme sistemleridir.




- DES, 56 bitlik bir anahtar kullanır.
- 3DES, 56 bit DES'in bir çeşididir. 64 bitlik blok başına üç bağımsız 56 bit şifreleme anahtarı kullanır ve DES'e göre önemli ölçüde daha güçlü şifreleme gücü sağlar.
- AES, DES'ten daha güçlü güvenlik sağlar ve sayısal olarak 3DES'ten daha verimlidir. AES, üç farklı anahtar uzunluğu sunar: 128 bit, 192 bit ve 256 bit.
- SEAL bir akış şifresidir, yani veri bloklarını şifrelemek yerine verileri sürekli olarak şifreler. SEAL, 160 bitlik bir anahtar kullanır.

**Bütünlük**

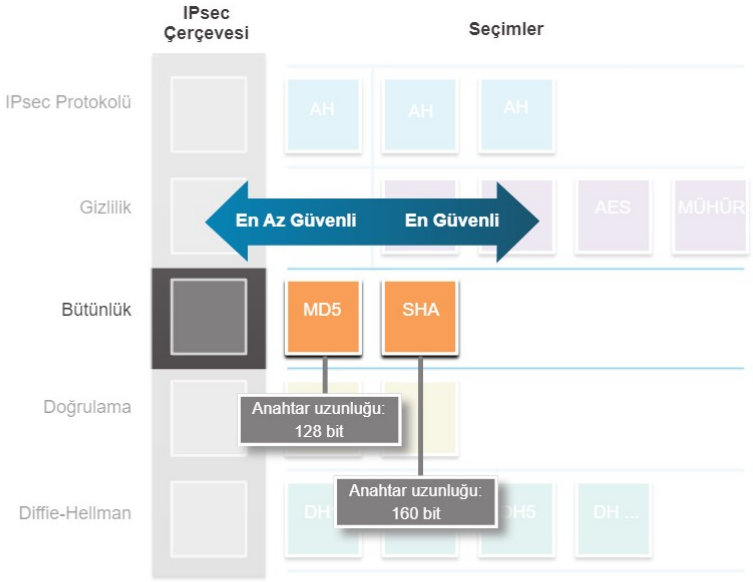
Veri bütünlüğü, alınan verilerin, gönderilen verilerle tamamen aynı olduğu anlamına gelir. Potansiyel olarak, veriler yakalanabilir ve değiştirilebilir. Örneğin, şekilde Alex'e 100 dolarlık bir çek yazıldığını varsayalım. Çek daha sonra Alex'e postalanır, ancak bir tehdit aktörü tarafından yakalanır. Tehdit aktörü, çekin üzerindeki adı Jeremy ve çek üzerindeki tutarı 1.000 $ 'a değiştirir ve paraya çevirmeye çalışır. Değiştirilen kontroldeki sahteciliğin kalitesine bağlı olarak saldırgan başarılı olabilir.




VPN verileri genel internet üzerinden taşındığından, içeriğin değiştirilmediğini garanti etmek için veri bütünlüğünü kanıtlama yöntemi gereklidir. Karma Mesaj Kimlik Doğrulama Kodu-Hashed Message Authentication Code (HMAC), bir karma değer kullanarak mesajın bütünlüğünü garanti eden bir veri bütünlüğü algoritmasıdır. Şekil, en yaygın iki HMAC algoritmasını vurgulamaktadır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

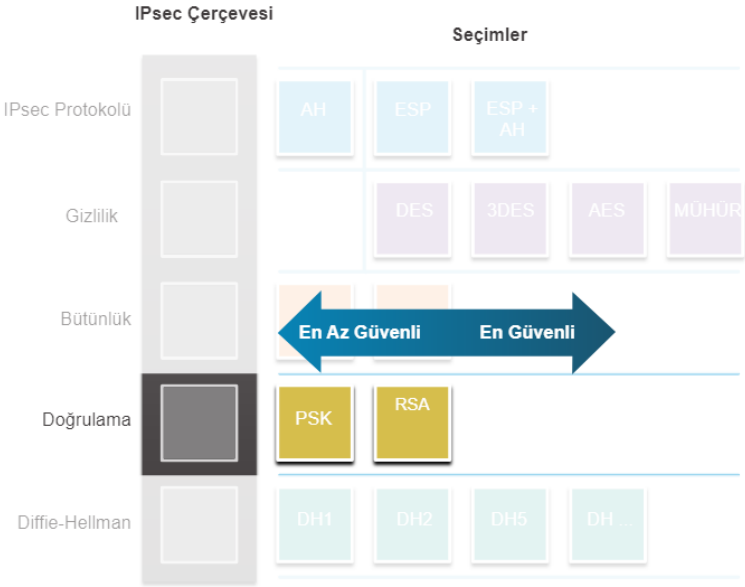
Not: Cisco artık SHA-1'i eski olarak derecelendiriyor ve bütünlük için en az SHA-256'yı öneriyor.




- Message Digest 5 (MD5), 128 bitlik paylaşılan gizli bir anahtar kullanır. Değişken uzunluklu mesaj ve 128 bitlik paylaşılan gizli anahtar birleştirilir ve HMAC-MD5 karma algoritmasıyla çalıştırılır. Çıktı, 128 bitlik bir karmadır.
- Güvenli Karma Algoritma (SHA), 160 bitlik bir gizli anahtar kullanır. Değişken uzunluklu mesaj ve 160 bitlik paylaşılan gizli anahtar birleştirilir ve HMAC-SHA-1 algoritmasıyla çalıştırılır. Çıktı 160 bitlik bir karmadır.

## Doğrulama

Uzun mesafe iş yaparken, telefonun, e-postanın veya faksın diğer ucunda kimin olduğunu bilmelisiniz. Aynısı VPN ağları için de geçerlidir. VPN tünelinin diğer ucundaki aygıt, iletişim yolu güvenli kabul edilmeden önce doğrulanmalıdır. Şekil, iki eş kimlik doğrulama yöntemini vurgulamaktadır.

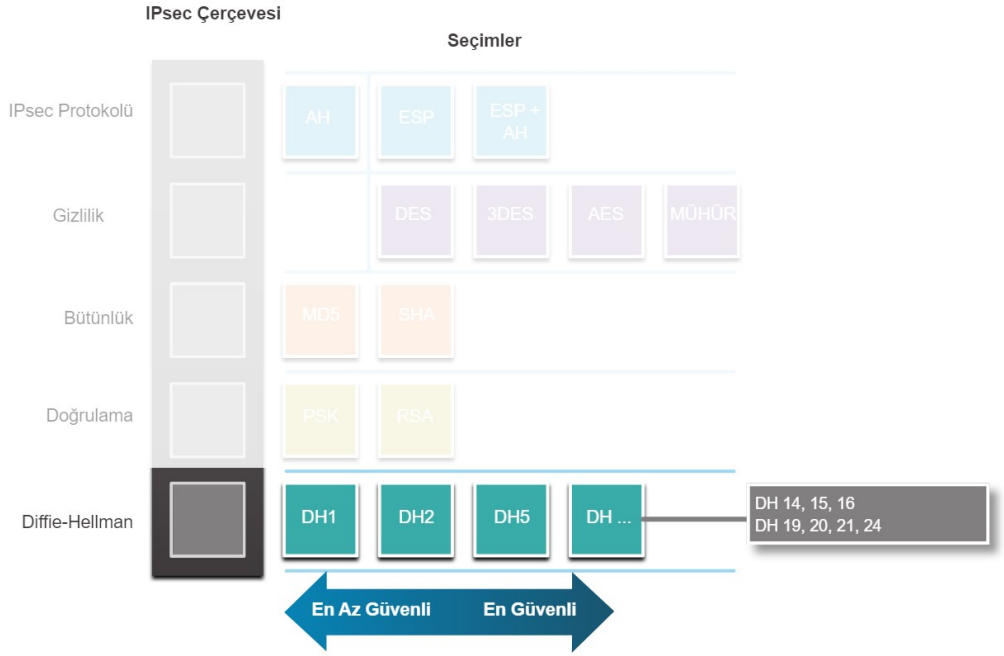



- Önceden paylaşılan bir gizli anahtar (PSK) değeri her bir eşe manuel olarak girilir. PSK, kimlik doğrulama anahtarını oluşturmak için diğer bilgilerle birleştirilir. PSK'ların manuel olarak yapılandırılması kolaydır, ancak iyi ölçeklenemezler çünkü her IPsec eşi, iletişim kurduğu diğer tüm eşlerin PSK'ları ile yapılandırılmalıdır.
- Rivest, Shamir ve Adleman (RSA) kimlik doğrulaması, eşlerin kimliğini doğrulamak için dijital sertifikalar kullanır. Yerel cihaz bir karma türetir ve bunu özel anahtarıyla şifreler. Şifrelenmiş karma mesaja eklenir ve uzak uca iletilir ve bir imza gibi davranır. Uzak uçta, şifrelenmiş karmanın şifresi, yerel ucun genel anahtarı kullanılarak çözülür. Şifresi çözülen hash, yeniden hesaplanan hash ile eşleşiyorsa, imza gerçektir. Tünelin güvenli olduğu kabul edilmeden önce her bir eş, diğer eşinin kimliğini doğrulamalıdır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Diffie-Hellman ile Güvenli Anahtar Değişimi

Şifreleme algoritmaları, şifreleme ve şifre çözme gerçekleştirmek için simetrik, paylaşılan bir gizli anahtar gerektirir. Şifreleme ve şifre çözme cihazları paylaşılan gizli anahtarı nasıl alır? En kolay anahtar değişim yöntemi, şekilde gösterildiği gibi Diffie-Hellman (DH) gibi bir genel anahtar değişim yöntemi kullanmaktır.




DH, iki eşin, güvenli olmayan bir kanal üzerinden iletişim kuruyor olsalar bile yalnızca kendilerinin bildiği bir paylaşılan gizli anahtar oluşturmaları için bir yol sağlar. DH anahtar değişiminin varyasyonları DH grupları olarak belirtilir:

- DH grupları 1, 2 ve 5 artık kullanılmamalıdır. Bu gruplar sırasıyla 768 bit, 1024 bit ve 1536 bitlik bir anahtar boyutunu destekler.
- DH grupları 14, 15 ve 16, sırasıyla 2048 bit, 3072 bit ve 4096 bit ile daha büyük anahtar boyutları kullanır ve 2030'a kadar kullanılması önerilir.
- İlgili anahtar boyutları 256 bit, 384 bit, 521 bit ve 2048 bit olan DH grupları 19, 20, 21 ve 24, anahtarları oluşturmak için gereken süreyi azaltan Eliptik Eğri Şifrelemesini (ECC) destekler. DH grup 24, tercih edilen yeni nesil şifrelemedir.

Seçtiğiniz DH grubu, anlaşma sırasında IPsec anahtarlarını korumak için yeterince güçlü veya yeterli bitlere sahip olmalıdır. Örneğin, DH grubu 1 DES ve 3DES şifrelemesini destekleyecek kadar güçlüdür, ancak AES'yi desteklemez. Örneğin, şifreleme veya kimlik doğrulama algoritmaları 128 bitlik bir anahtar kullanıyorsa, grup 14, 19, 20 veya 24'ü kullanın. Ancak, şifreleme veya kimlik doğrulama algoritmaları 256 bit veya daha yüksek bir anahtar kullanıyorsa, grup 21 veya 24'ü kullanın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 38.Bölüm: QoS

## 38.1.Ağ İletim Kalitesi

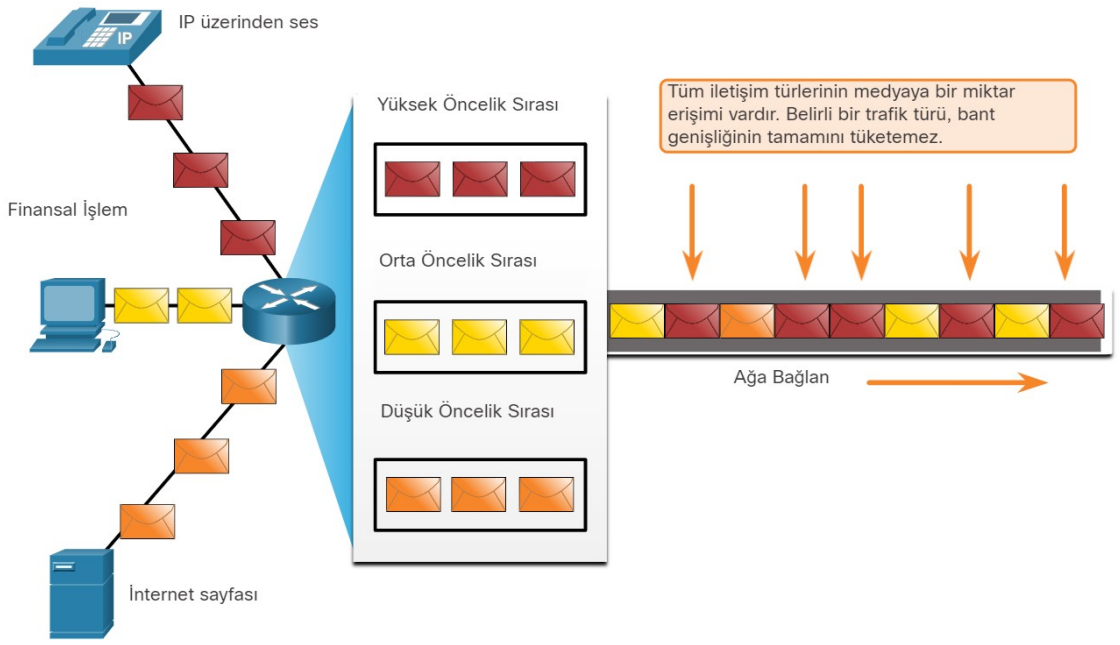
### 38.1.1.Trafiğe Öncelik Verme

QoS ((Quality of Service), günümüzde ağların giderek artan bir gereksinimidir. Ses ve canlı video aktarımı gibi yeni uygulamalar, kullanıcılar arasında kaliteli teslimat için daha yüksek beklentiler oluşturur.

Tıkanıklık, birden fazla iletişim hattı yönlendirici gibi tek bir cihazda toplandığında ve ardından bu verilerin çoğu yalnızca birkaç giden arayüze veya daha yavaş bir arayüze yerleştirildiğinde oluşur. Tıkanıklık, büyük veri paketleri daha küçük paketlerin zamanında iletilmesini engellediğinde de meydana gelebilir.

Trafik hacmi, ağ üzerinden taşınabilecek olandan daha büyük olduğunda, cihazlar, paketleri iletmek için kaynaklar mevcut olana kadar bellekte sıraya alır (tutar). Paketlerin sıraya alınması gecikmeye neden olur çünkü yeni paketler önceki paketler işlenene kadar iletilemez. Sıraya alınacak paket sayısı artmaya devam ederse, cihaz içindeki bellek dolar ve paketler atılır. Bu soruna yardımcı olabilecek bir QoS tekniği, şekilde gösterildiği gibi verileri birden çok kuyruğa sınıflandırmaktır.

Not : Bir cihaz, QoS'yi yalnızca bir tür tıkanıklık yaşadığında uygular.

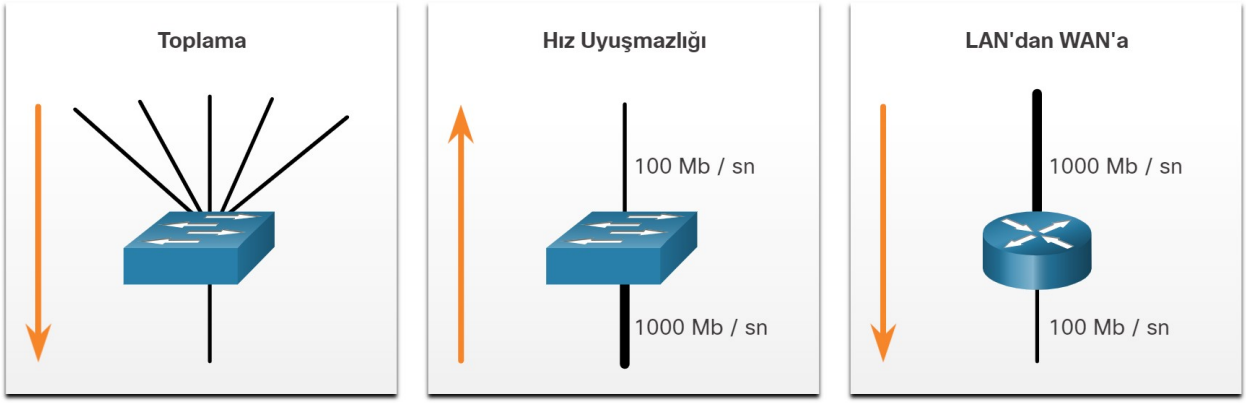



### 38.1.2.Bant Genişliği, Tıkanıklık, Gecikme ve Değişme (Bandwidth, Congestion, Delay, and Jitter)

Ağ bant genişliği, tek bir saniyede iletilebilen bit sayısı (bps) ile ölçülür. Örneğin, bir ağ cihazının saniyede 10 gigabit (Gbps) performans gösterme kabiliyetine sahip olduğu açıklanabilir.

Ağ tıkanıklığı gecikmeye neden olur. Bir arayüz, başa çıkabileceğinden daha fazla trafikle sunulduğunda tıkanıklık yaşar. Ağ tıkanıklığı noktaları, QoS mekanizmaları için ideal adaylardır. Şekil, tipik tıkanıklık noktalarının üç örneğini göstermektedir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Gecikme, bir paketin kaynaktan hedefe gitmesi için geçen süreyi ifade eder. İki tür gecikme vardır: sabit ve değişken. Sabit bir gecikme, iletim ortamına bir bitin ne kadar sürede yer alması gibi, belirli bir işlemin aldığı belirli bir süredir. Değişken bir gecikme, belirsiz bir süre alır ve trafiğin ne kadar işlendiği gibi faktörlerden etkilenir.

Gecikme kaynakları tabloda özetlenmiştir.

| Gecikme | Açıklama |
|---|---|
| Kod gecikmesi | İlk ağlar arası çalışma cihazına, genellikle bir anahtara aktarılmadan önce verilerin kaynakta sıkıştırılması için gereken sabit süre. |
| Paketleme gecikmesi | Bir paketi gerekli tüm başlık bilgileriyle kapsüllemek için gereken sabit süre. |
| Kuyruk gecikmesi | Bir çerçevenin veya paketin bağlantıda iletilmek için beklediği değişken zaman miktarı. |
| Serileştirme gecikmesi | Bir çerçeveyi tele iletmek için gereken sabit süre. |
| Yayılma gecikmesi | Çerçevenin kaynak ile hedef arasında gidip gelmesi için geçen değişken zaman miktarı. |
| De-jitter gecikmesi | Paket akışını tamponlamak ve ardından bunları eşit aralıklarla göndermek için gereken sabit süre. |

Jitter, alınan paketlerin gecikmesindeki değişimdir. Gönderen tarafta, paketler eşit aralıklarla aralıklı olarak sürekli bir akış halinde gönderilir. Ağ tıkanıklığı, yanlış kuyruklama veya yapılandırma hataları nedeniyle, her paket arasındaki gecikme sabit kalmak yerine değişebilir. Gerçek zamanlı ve etkileşimli trafiği desteklemek için hem gecikmenin hem de titreşimin kontrol edilmesi ve en aza indirilmesi gerekir.

### 38.1.3.Paket Kaybı

Herhangi bir QoS mekanizması olmadan, paketler alındıkları sıraya göre işlenir. Tıkanıklık meydana geldiğinde, yönlendiriciler ve anahtarlar gibi ağ cihazları paketleri bırakabilir. Bu, gerçek zamanlı video ve ses gibi zamana duyarlı paketlerin, e-posta ve web'de gezinme gibi zamana duyarlı olmayan verilerle aynı frekansta bırakılacağı anlamına gelir.

Bir yönlendirici, IP üzerinden Ses (VoIP) için bir Gerçek Zamanlı Protokol-Real-Time Protocol (RTP) dijital ses akışı aldığında, karşılaşılan titreşimi telafi etmelidir. Bu işlevi yerine getiren mekanizma, oynatma gecikme arabelleğidir(playout delay buffer). Oynatma gecikme tamponu, bu paketleri arabelleğe almalı ve ardından sabit bir akışta oynatmalıdır. Dijital paketler daha sonra tekrar analog ses akışına dönüştürülür.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Paket kaybı, bir IP ağındaki ses kalitesi sorunlarının çok yaygın bir nedenidir. Düzgün tasarlanmış bir ağda, paket kaybı sıfıra yakın olmalıdır. DSP tarafından kullanılan ses kodekleri, ses kalitesi üzerinde dramatik bir etki

olmaksızın bir dereceye kadar paket kaybını tolere edebilir. Ağ mühendisleri, ses paketlerini sıfır paket kaybı için sınıflandırmak üzere QoS mekanizmalarını kullanır. Gecikmelere duyarlı olmayan trafik üzerinden ses trafiğine öncelik verilerek sesli aramalarda bant genişliği garanti edilmektedir.

## 38.2.Trafik Özellikleri

### 38.2.1.Ağ Trafiği Eğilimleri

2000'lerin başlarında, baskın IP trafiği türleri ses ve veri idi. Ses trafiğinin tahmin edilebilir bir bant genişliği ihtiyacı ve bilinen paket varış süreleri vardır. Veri trafiği gerçek zamanlı değildir ve öngörülemeyen bant genişliği ihtiyacı vardır. Veri trafiği, büyük bir dosya indirilirken olduğu gibi geçici olarak patlayabilir. Bu patlama, bir bağlantının tüm bant genişliğini tüketebilir.

Daha yakın zamanlarda, video trafiği, ticari iletişim ve operasyonlar için giderek daha önemli hale geldi. Kuruluşların artık kullanıcılar ve müşterilerle buluşmak için video konferans, tesisleri ve ekipmanları uzaktan izlemek için yüksek tanımlı video gözetimi ve eğitim dahil çeşitli amaçlar için video akışını kullandığını düşünün. Cisco Görsel Ağ İndeksine (VNI) göre, 2022 yılına kadar video tüm internet trafiğinin% 82'sini temsil edecek. Ayrıca, mobil video trafiği 2022'ye kadar ayda 60,9 eksabayta ulaşacak. "

### 38.2.2.Ses

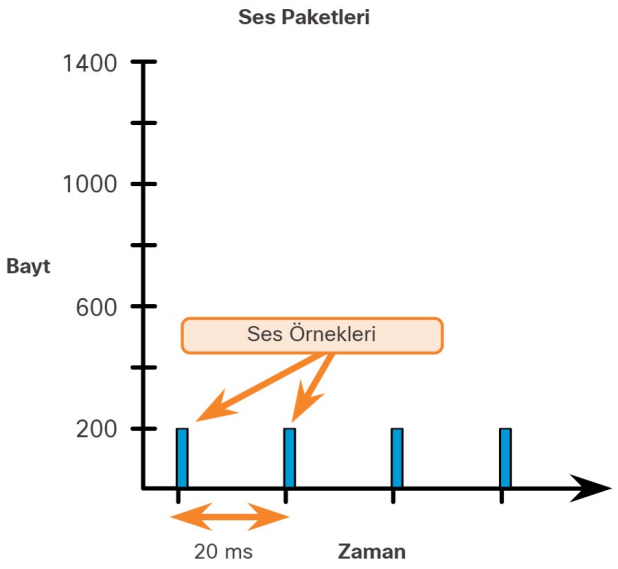
Tabloda gösterildiği gibi, ses trafiği tahmin edilebilir ve düzgündür. Ancak, ses gecikmelere ve düşen paketlere karşı çok hassastır. Paketler kaybolursa sesi yeniden iletmenin bir anlamı yoktur; bu nedenle, ses paketleri diğer trafik türlerinden daha yüksek bir öncelik almalıdır. Örneğin, Cisco ürünleri, ses trafiğine öncelik vermek için 16384 ila 32767 RTP bağlantı noktası aralığını kullanır. Ses, gözle görülür bir etki olmaksızın belirli bir miktarda gecikme, titreme ve kaybı tolere edebilir. Gecikme 150 milisaniyeden (ms) fazla olmamalıdır. Jitter, 30 ms'den fazla olmamalı ve ses paketi kaybı% 1'den fazla olmamalıdır. Ses trafiği en az 30 Kbps bant genişliği gerektirir. Tablo, ses trafiği özelliklerinin ve gereksinimlerinin bir özetini verir.

| Ses Trafik Özellikleri | Tek Yönlü Gereksinimler |
|---|---|
| Düzgün | |
| Uyumlu | Gecikme ≤ 150ms |
| Düşmeye hassas | Titreşim ≤ 30 ms |
| Gecikmeye duyarlı | Kayıp ≤% 1 Bant Genişliği (30-128 Kbps) |
| UDP önceliği | |

### 38.2.3.Video

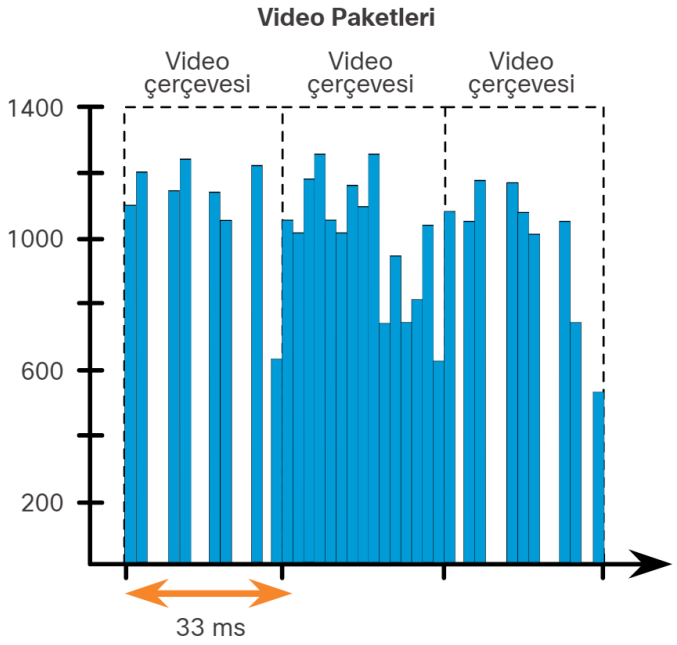
QoS ve önemli miktarda ekstra bant genişliği kapasitesi olmadan, video kalitesi tipik olarak düşer. Resim bulanık, pürüzlü veya ağır çekimde görünür. Beslemenin ses kısmı, videoyla senkronize edilmeyebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Video trafiği, ses trafiğine kıyasla tahmin edilemez, tutarsız ve patlamalı olma eğilimindedir. Sese kıyasla video, kayba karşı daha az dirençlidir ve paket başına daha yüksek veri hacmine sahiptir. Şekilde, ses paketlerinin her 20 ms'de bir nasıl ulaştığına ve her birinin öngörülebilir 200 bayt olduğuna dikkat edin.

Buna karşılık, video paketlerinin sayısı ve boyutu, şekilde gösterildiği gibi videonun içeriğine bağlı olarak her 33 ms'de bir değişir. Örneğin, video akışı çerçeveden çerçeveye pek değişmeyen içerikten oluşuyorsa, video paketleri küçük olacaktır ve kabul edilebilir kullanıcı deneyimini sürdürmek için daha azına ihtiyaç duyulacaktır. Bununla birlikte, video buharı, bir filmdeki bir eylem sekansı gibi hızla değişen içerikten oluşuyorsa, video paketleri daha büyük olacaktır. Kabul edilebilir bir kullanıcı deneyimini sürdürmek için 33 ms'lik zaman aralığı başına daha fazlası gerekir.




554 gibi UDP bağlantı noktaları, Gerçek Zamanlı Akış Protokolü (RSTP) için kullanılır ve diğer, daha az gecikmeye duyarlı ağ trafiğine göre öncelik verilmelidir. Sese benzer şekilde video, herhangi bir gözle görülür etki olmaksızın belirli bir miktarda gecikme, titreme ve kaybı tolere edebilir. Gecikme 400 milisaniyeden (ms) fazla olmamalıdır. Jitter 50 ms'den fazla olmamalı ve video paket kaybı% 1'den fazla olmamalıdır. Video trafiği en az 384 Kbps bant genişliği gerektirir. Tablo, video trafiği özelliklerinin ve gereksinimlerinin bir özetini verir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Video Trafik Özellikleri | Tek Yönlü Gereksinimler |
|---|---|
| Patlamalı<br>Doyumsuz<br>Düşmeye hassas<br>Gecikmeye duyarlı<br>UDP önceliği | Gecikme ≤ 200-400 ms<br>Titreşim ≤ 30-50 ms<br>Kayıp ≤% 0.1-1<br>Bant genişliği (384 Kbps -> 20 Mbps |

### 38.2.4.Veri

Çoğu uygulama TCP veya UDP kullanır. UDP'nin aksine, TCP hata kurtarma işlemi gerçekleştirir. E-posta ve web sayfaları gibi veri kaybına toleransı olmayan veri uygulamaları, paketler aktarılırken kaybolursa yeniden gönderileceklerinden emin olmak için TCP kullanır. Veri trafiği sorunsuz veya patlamalı olabilir. Ağ kontrol trafiği genellikle pürüzsüz ve tahmin edilebilirdir. Bir topoloji değişikliği olduğunda, ağ kontrol trafiği birkaç saniyeliğine patlayabilir. Ancak günümüz ağlarının kapasitesi, ağ yakınlaştıkça ağ kontrol trafiğindeki artışı kolayca idare edebilir.

Ancak, bazı TCP uygulamaları ağ kapasitesinin büyük bir bölümünü tüketebilir. FTP, bir film veya oyun gibi büyük bir dosya indirdiğinizde alabileceği kadar bant genişliği tüketecektir.

## 38.3.Kuyruk Algoritmaları

### 38.3.1.Kuyruklamaya (Queuing) Ön Bakış

Bu konu, QoS'yi uygulamak için kullanılan kuyruk algoritmalarını açıklayacaktır. Ağ yöneticisi tarafından uygulanan QoS politikası, bağlantıda tıkanıklık oluştuğunda etkin hale gelir. Kuyrupa alma, hedefe iletilmeden önce paketleri arabelleğe alabilen, önceliklendirebilen ve gerekirse yeniden sıralayabilen bir tıkanıklık yönetimi aracıdır.

Bir dizi kuyruk algoritması mevcuttur :

- İlk Giren İlk Çıkar- First-In, First-Out(FIFO)
- Ağırlıklı Adil Kuyruklama-Weighted Fair Queuing (WFQ)
- Sınıf Bazında Ağırlıklı Adil Sıraya Alma-Class-Based Weighted Fair Queuing (CBWFQ)
- Düşük Gecikmeli Kuyruklama- Low Latency Queuing(LLQ)

### 38.3.2.İlk Giren İlk Çıkar

En basit şekliyle İlk Giren İlk Çıkar (FIFO) kuyruğu, ilk gelen, ilk servis kuyruğu olarak da bilinir, paketleri varış sırasına göre arabelleğe alır ve iletir.

FIFO'nun öncelik kavramı veya trafik sınıfı yoktur ve sonuç olarak paket önceliği hakkında karar vermez. Yalnızca bir kuyruk vardır ve tüm paketler eşit olarak ele alınır. Paketler, şekilde gösterildiği gibi ulaştıkları sırayla bir arabirim gönderir. Öncelik sınıflandırmasına göre bazı trafik daha önemli veya zamana duyarlı olsa da, trafiğin alındığı sırayla gönderildiğine dikkat edin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

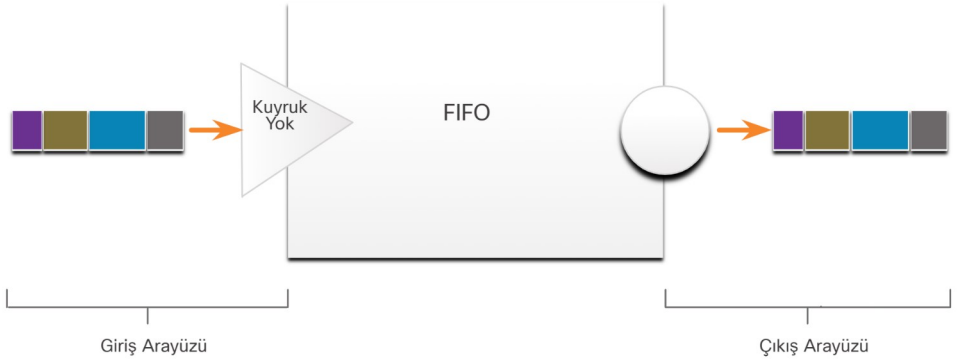
FIFO kullanıldığında, yönlendirici veya anahtar arayüzünde tıkanıklık olduğunda önemli veya zamana duyarlı trafik bırakılabilir. Başka kuyruklama stratejileri yapılandırılmadığında, E1 (2.048 Mbps) ve altındaki seri

arabirimler dışındaki tüm arabirimler varsayılan olarak FIFO kullanır. (E1 ve altındaki seri arayüzler varsayılan olarak WFQ kullanır.)

En hızlı kuyruğa alma yöntemi olan FIFO, çok az gecikme ve minimum tıkanıklık içeren büyük bağlantılar için etkilidir. Bağlantınız çok az tıkanıklığa sahipse, kullanmanız gereken tek kuyruk FIFO kuyruğu olabilir.

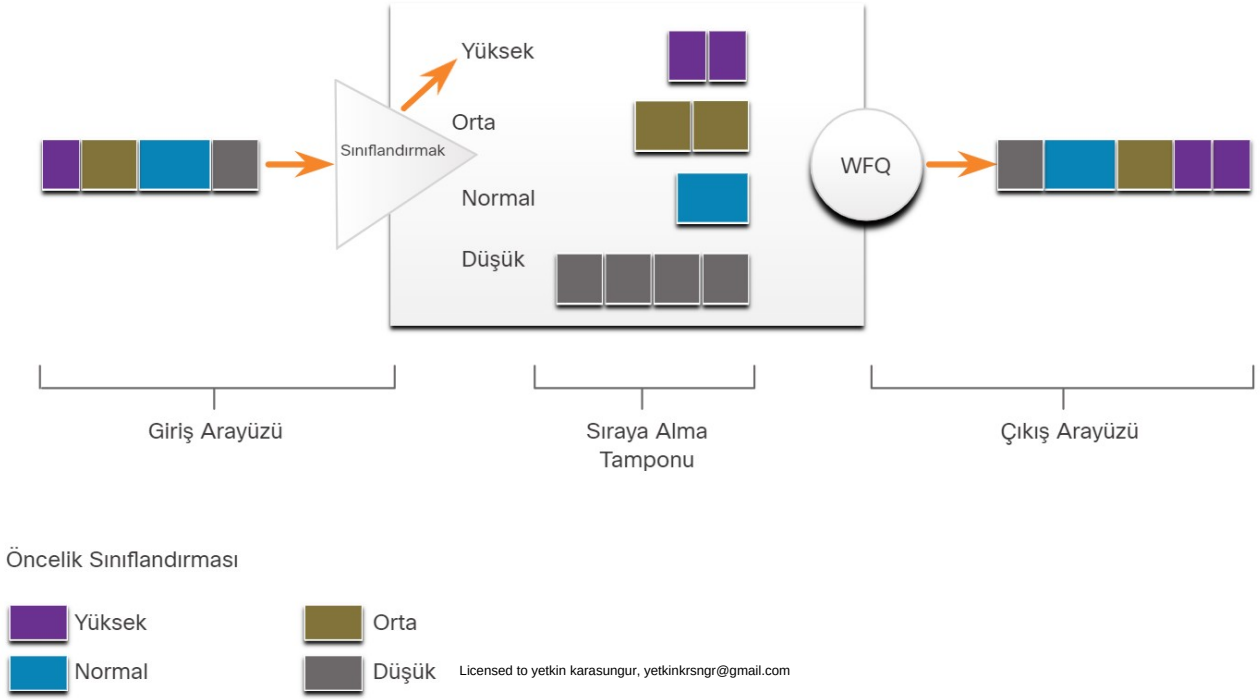
Şekilde İlk Giren İlk Çıkar (FIFO) kuyruğu örneği gösterilmektedir. Giriş arayüzüne dört farklı trafik türü ulaşmaktadır. Sıra yoktur ve tüm paketler eşit olarak işlenir. Çıkış arayüzünden alındıkları sırayla iletilirler.

**FIFO Kuyruk Örneği**




## 38.3.4.Ağırlıklı Adil Kuyruklama (WFQ)

Ağırlıklı Adil Kuyruklama (WFQ), tüm ağ trafiğine adil bant genişliği tahsisi sağlayan otomatik bir zamanlama yöntemidir. WFQ, sınıflandırma seçeneklerinin yapılandırılmasına izin vermez. WFQ, tanımlanan trafiğe öncelik veya ağırlıklar uygular ve bunu şekilde gösterildiği gibi konuşmalar veya akışlar olarak sınıflandırır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Daha sonra WFQ, diğer akışlara göre her akışa ne kadar bant genişliğine izin verildiğini belirler. WFQ tarafından kullanılan akış tabanlı algoritma, yanıt süresini azaltmak için eşzamanlı olarak etkileşimli trafiği bir kuyruğun önüne planlar. Daha sonra, kalan bant genişliğini yüksek bant genişliğine sahip akışlar arasında oldukça paylaşır. WFQ, Telnet oturumları ve ses gibi düşük hacimli, etkileşimli trafiğe, FTP oturumları gibi yüksek hacimli trafiğe göre öncelik vermenize olanak tanır. Birden çok dosya aktarımı akışı aynı anda gerçekleştiğinde, aktarımlara karşılaştırılabilir bant genişliği verilir.

WFQ, kaynak ve hedef IP adresleri, MAC adresleri, bağlantı noktası numaraları, protokol ve Hizmet Türü-Type of Service (ToS) değeri gibi özellikler dahil olmak üzere, paket başlığı adreslemesine dayalı olarak trafiği farklı akışlar halinde sınıflandırır. IP başlığındaki ToS değeri trafiği sınıflandırmak için kullanılabilir.

Trafiğin çoğunluğunu oluşturan düşük bant genişliğine sahip trafik akışları, sunulan tüm yüklerinin zamanında gönderilmesine olanak tanıyan tercihli hizmet alır. Yüksek hacimli trafik akışları, kalan kapasiteyi kendi aralarında orantılı olarak paylaşır.

**Sınırlamalar**

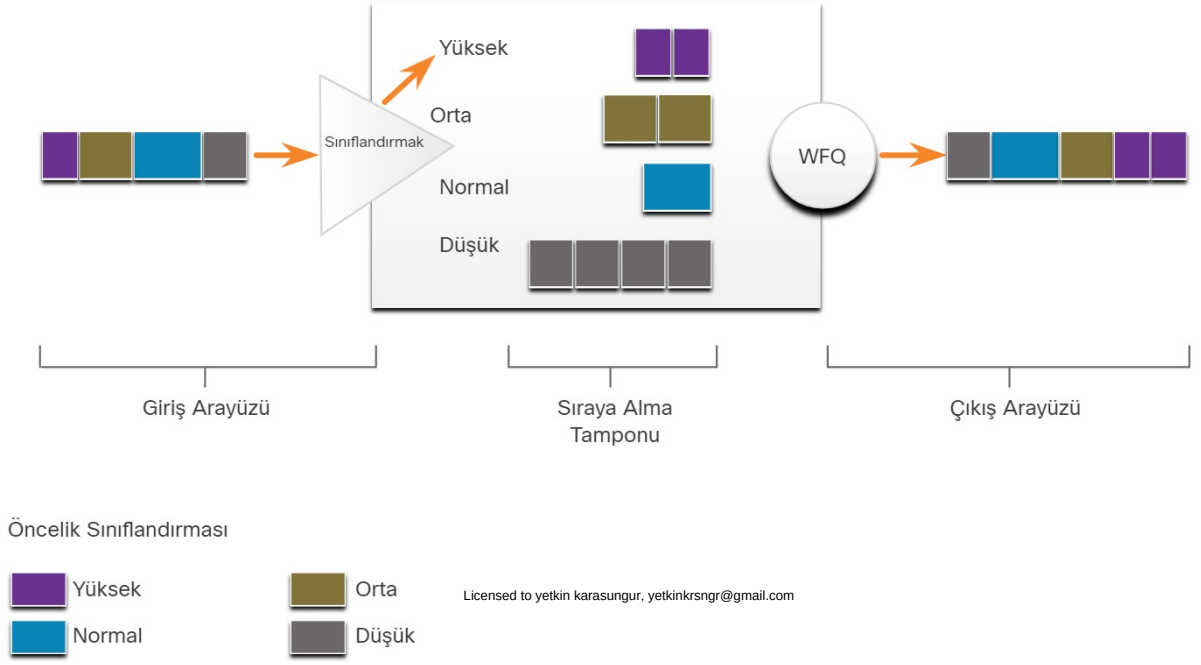
WFQ, tünelleme ve şifreleme ile desteklenmez çünkü bu özellikler, sınıflandırma için WFQ'nun gerektirdiği paket içeriği bilgilerini değiştirir.

WFQ, değişen ağ trafiği koşullarına otomatik olarak uyum sağlasa da, CBWFQ'nun sunduğu bant genişliği tahsisi üzerinde kesin kontrol derecesi sunmaz.

## 38.3.5.Sınıf Bazında Ağırlıklı Adil Sıraya Alma (CBWFQ)

Ağırlıklı Adil Kuyruklama (WFQ), tüm ağ trafiğine adil bant genişliği tahsisi sağlayan otomatik bir zamanlama yöntemidir. WFQ, sınıflandırma seçeneklerinin yapılandırılmasına izin vermez. WFQ, tanımlanan trafiğe öncelik veya ağırlıklar uygular ve bunu şekilde gösterildiği gibi konuşmalar veya akışlar olarak sınıflandırır.

Şekil, Ağırlıklı Adil Kuyruklama (WFQ) örneğini göstermektedir. Giriş arayüzüne dört farklı trafik türü ulaşmaktadır. Trafik, sınıflandırmalarına göre düzenlenir: yüksek, orta, normal veya düşük. Sınıflandırmalarına göre sırayla çıkış arabirimine iletilirler. Önce yüksek trafik ayrılır, sonra orta, normal ve son olarak düşüktür.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Daha sonra WFQ, diğer akışlara göre her akışa ne kadar bant genişliğine izin verildiğini belirler. WFQ tarafından kullanılan akış tabanlı algoritma, yanıt süresini azaltmak için eşzamanlı olarak etkileşimli trafiği bir kuyruğun önüne planlar. Daha sonra, kalan bant genişliğini yüksek bant genişliğine sahip akışlar arasında oldukça paylaşır. WFQ, Telnet oturumları ve ses gibi düşük hacimli, etkileşimli trafiğe, FTP oturumları gibi yüksek hacimli trafiğe göre öncelik vermenize olanak tanır. Birden çok dosya aktarımı akışı aynı anda gerçekleştiğinde, aktarımlara karşılaştırılabilir bant genişliği verilir.

WFQ, kaynak ve hedef IP adresleri, MAC adresleri, bağlantı noktası numaraları, protokol ve Hizmet Türü (ToS) değeri gibi özellikler dahil olmak üzere, paket başlığı adreslemesine dayalı olarak trafiği farklı akışlar halinde sınıflandırır. IP başlığındaki ToS değeri trafiği sınıflandırmak için kullanılabilir.

Trafiğin çoğunluğunu oluşturan düşük bant genişliğine sahip trafik akışları, sunulan tüm yüklerinin zamanında gönderilmesine olanak tanıyan tercihli hizmet alır. Yüksek hacimli trafik akışları, kalan kapasiteyi kendi aralarında orantılı olarak paylaşır.

**Sınırlamalar**

WFQ, tünelleme ve şifreleme ile desteklenmez çünkü bu özellikler, sınıflandırma için WFQ'nun gerektirdiği paket içeriği bilgilerini değiştirir.

WFQ, değişen ağ trafiği koşullarına otomatik olarak uyum sağlasa da, CBWFQ'nun sunduğu bant genişliği tahsisi üzerinde kesin kontrol derecesi sunmaz.

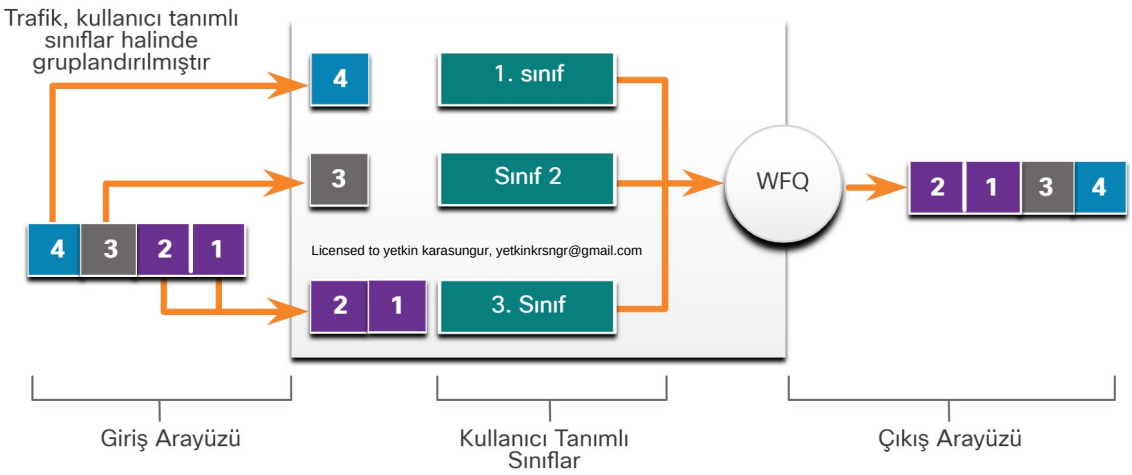
## 38.3.6.Sınıf Bazında Ağırlıklı Adil Sıraya Alma (CBWFQ)

Sınıf Tabanlı Ağırlıklı Adil Kuyruklama (CBWFQ), kullanıcı tanımlı trafik sınıfları için destek sağlamak üzere standart WFQ işlevselliğini genişletir. CBWFQ ile protokoller, erişim kontrol listeleri (ACL'ler) ve giriş arayüzleri dahil olmak üzere eşleşme kriterlerine göre trafik sınıfları tanımlarsınız. Bir sınıf için eşleşme ölçütlerini karşılayan paketler, o sınıfın trafiğini oluşturur. Her sınıf için bir FIFO kuyruğu ayrılır ve bir sınıfa ait trafik, şekilde gösterildiği gibi o sınıfın kuyruğuna yönlendirilir.

Bir sınıf, eşleşme kriterlerine göre tanımlandığında, ona karakteristikler atayabilirsiniz. Bir sınıfı karakterize etmek için, ona bant genişliği, ağırlık ve maksimum paket limiti atarsınız. Bir sınıfa atanan bant genişliği, tıkanıklık sırasında sınıfa sağlanan garantili bant genişliğidir.

Bir sınıfı karakterize etmek için, sınıfın kuyruğunda birikmesine izin verilen maksimum paket sayısı olan o sınıf için sıra sınırını da belirtirsiniz. Bir sınıfa ait paketler, sınıfı karakterize eden bant genişliği ve kuyruk sınırlamalarına tabidir.

Şekil, Sınıfa Dayalı Ağırlıklı Adil Kuyruklama (CBWFQ) örneğini göstermektedir. Giriş arayüzüne dört farklı trafik türü ulaşmaktadır. Trafik, kullanıcı tanımlı sınıflar halinde gruplandırılır. Ardından trafik, kullanıcı tanımlı sınıflara dayalı olarak çıkış arabiriminden dışarı iletilir. Örnek cihaza giren 1, 2, 3 ve 4 etiketli paketleri gösterir. Paket 4 Sınıf 1, paket 3 Sınıf 2 olarak tanımlanır ve paket 1 ve 2 Sınıf 3 olarak tanımlanır. Paketler sınıflarına göre düzenlenir, Sınıf 1 yüksek öncelik ve Sınıf 3 düşük öncelikli olmak. Paketlerin çıkış arayüzüne gönderilme sırası: 4, 3, 1 ve 2.



Bir kuyruk, yapılandırılmış kuyruk sınırına ulaştıktan sonra, sınıfa daha fazla paket eklemek, sınıf ilkesinin nasıl yapılandırıldığına bağlı olarak kuyruk bırakma veya paket bırakmanın etkili olmasına neden olur. Kuyruk bırakma, bir yönlendiricinin, paket tutma kaynaklarını tamamen kullanan bir kuyruğun son ucuna gelen herhangi bir paketi atması anlamına gelir. Bu, tıkanıklığa karşı varsayılan kuyruklama yanıtıdır. Kuyruk bırakma, tüm trafiği eşit olarak ele alır ve hizmet sınıfları arasında ayrım yapmaz.

## 38.3.7.Düşük Gecikmeli Kuyruklama (LLQ)

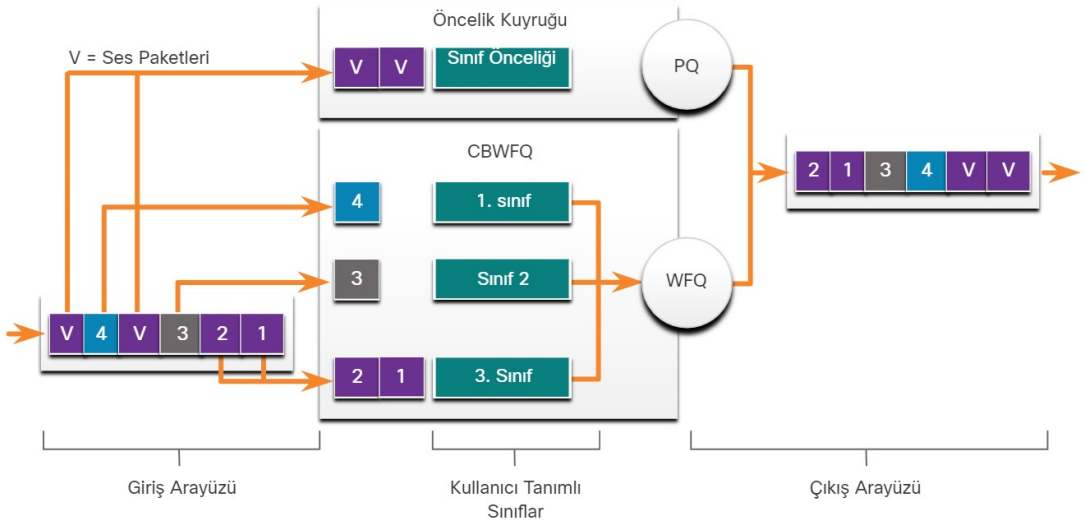
Düşük Gecikmeli Kuyruklama (LLQ) özelliği, CBWFQ'ya katı öncelik kuyruğunu (PQ) getirir. Katı PQ, ses gibi gecikmeye duyarlı paketlerin diğer kuyruklardaki paketlerden önce gönderilmesine izin verir. LLQ, şekilde gösterildiği gibi CBWFQ için kesin öncelikli kuyruğa alma sağlar ve sesli konuşmalardaki titreşimi azaltır.

LLQ olmadan CBWFQ, gerçek zamanlı trafik için kesin bir öncelik sırası olmaksızın tanımlanmış sınıflara dayalı WFQ sağlar. Belirli bir sınıfa ait bir paketin ağırlığı, onu yapılandırırken sınıfa atadığınız bant genişliğinden türetilir. Bu nedenle, bir sınıfın paketlerine atanan bant genişliği, paketlerin gönderilme sırasını belirler. Tüm paketler, ağırlık bazında makul bir şekilde servis edilir; hiçbir paket sınıfına kesin öncelik verilemez. Bu şema, büyük ölçüde gecikmeye tahammülü olmayan ses trafiği için, özellikle de gecikmedeki değişkenlik için sorunlar ortaya çıkarmaktadır. Ses trafiği için, gecikmedeki farklılıklar, duyulan konuşmada titreme olarak tezahür eden iletim düzensizliklerine neden olur.

LLQ, ilk olarak ses gibi gecikmeye duyarlı paketlerin (diğer kuyruklardaki paketlerden önce) gönderilmesine izin vererek gecikmeye duyarlı paketlere diğer trafiğe göre öncelikli muamele sağlar. Çeşitli gerçek zamanlı trafik türlerini katı öncelik kuyruğuna göre sınıflandırmak mümkün olsa da, Cisco yalnızca ses trafiğinin öncelik kuyruğuna yönlendirilmesini önerir.

Şekilde, Düşük Gecikmeli Kuyruklama (LLQ) örneği gösterilmektedir. Giriş arayüzünde altı paket alınır. Paketler 1, 2, 3, V (Ses), 4 ve V (Ses) olarak etiketlenmiştir. Trafik, bir öncelik kuyruğu ve bir CBWFQ, kullanıcı tanımlı sınıflar halinde gruplandırılır. Ses paketleri öncelik kuyruğunda tanımlanır. Paket 4, CBWFQ'da Sınıf 1 olarak tanımlanır, paket 3 Sınıf 2 olarak tanımlanır ve paket 1 ve 2 Sınıf 3'te olarak tanımlanır. Paketlerin sırası, çıkış arabirimine gönderilir: V ( Ses), V (Ses), 4, 3, 1 ve 2.

### LLQ Örneği




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 38.9.QoS Modelleri

### 38.9.1.QoS Politika Modeli Seçme

QoS uygulamak için üç model vardır:

- En iyi çaba-best effort modeli
- Entegre hizmetler-Integrated services (IntServ)
- Farklılaştırılmış hizmetler-Differentiated services (DiffServ)
-

Tablo bu üç modeli özetlemektedir. QoS, IntServ veya DiffServ kullanılarak bir ağda uygulanır. IntServ en yüksek QoS garantisini sağlarken, çok yoğun kaynak gerektirir ve bu nedenle kolayca ölçeklendirilemez. Buna karşılık, DiffServ daha az kaynak yoğun ve daha ölçeklenebilir. İkisi bazen ağ QoS uygulamalarında birlikte konuşlandırılır.

| Model | Açıklama |
|---|---|
| En iyi çaba modeli | QoS açıkça yapılandırılmadığından bu gerçek bir uygulama değildir.<br><br>Bunu QoS gerekli olmadığında kullanın. |
| Entegre hizmetler (IntServ) | IntServ, garantili teslimat ile IP paketlerine çok yüksek QoS sağlar.<br><br>Uygulamaların bir süre için özel QoS gerektirdiklerini ve bu bant genişliğinin ayrılması gerektiğini ağa bildirmeleri için bir sinyalleşme sürecini tanımlar.<br><br>IntServ, bir ağın ölçeklenebilirliğini ciddi şekilde sınırlayabilir. |
| Farklılaştırılmış hizmetler (DiffServ) | DiffServ, QoS uygulamasında yüksek ölçeklenebilirlik ve esneklik sağlar.<br><br>Ağ cihazları trafik sınıflarını tanır ve farklı trafik sınıflarına farklı QoS seviyeleri sağlar. |

### 38.9.2.En İyi Çaba Modeli

İnternetin temel tasarımı en iyi şekilde paket teslimatıdır ve hiçbir garanti vermez. Bu yaklaşım günümüzde hala internette baskındır ve çoğu amaç için uygun olmaya devam etmektedir. En iyi çalışma modeli, tüm ağ paketlerine aynı şekilde davranır, bu nedenle acil durum sesli mesajı, bir e-postaya eklenen dijital fotoğrafla aynı şekilde ele alınır. QoS olmadan ağ, paketler arasındaki farkı anlayamaz ve sonuç olarak paketleri tercihli olarak ele alamaz.

En iyi çaba modeli, konsept olarak standart posta kullanarak bir mektup göndermeye benzer. Mektubunuz diğer tüm mektuplarla aynı şekilde ele alınır. En iyi çaba modeliyle, mektup asla gelmeyebilir ve mektubu alıcısıyla ayrı bir bildirim düzenlemeniz olmadıkça, mektubun ulaşmadığını asla bilemezsiniz.

Tablo, en iyi çaba modelinin faydalarını ve dezavantajlarını listeler.

| Faydaları | Dezavantajlar |
|---|---|
| Model en ölçeklenebilir olanıdır. | Teslimat garantisi yoktur. |
| Ölçeklenebilirlik yalnızca mevcut bant genişliğiyle sınırlıdır ve bu durumda tüm trafik eşit şekilde etkilenir. | Paketler, ulaşabildikleri her zaman ve mümkün olan herhangi bir sırayla ulaşırlarsa, ulaşırlar. |
| Özel bir QoS mekanizmasına gerek yoktur. | Hiçbir paketin tercihli muamelesi yoktur. |
| Dağıtımı en kolay ve en hızlı modeldir. | Kritik veriler, sıradan e-postaların işlendiği şekilde ele alınır. |

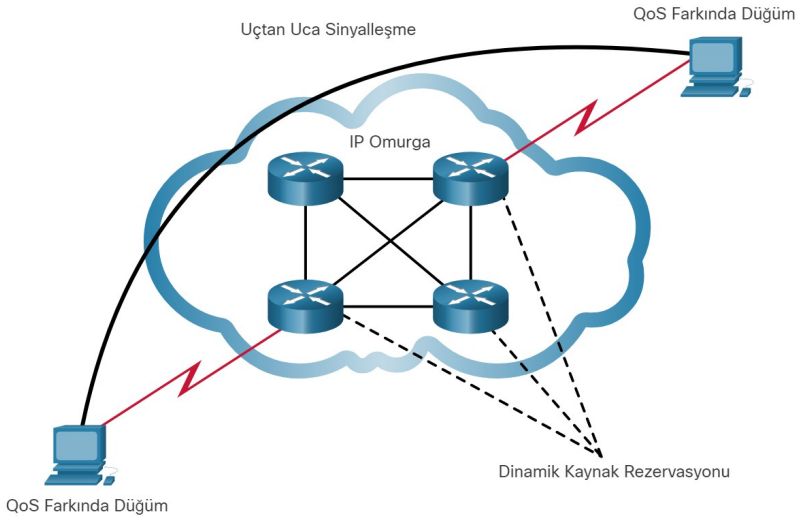
Licensed to yetkin karasungur, yetkin.karasungur@gmail.com

## 38.9.3.Entegre Servisler

IntServ mimari modeli (RFC 1633, 2211 ve 2212), uzak video, multimedya konferansı, veri görselleştirme uygulamaları ve sanal gerçeklik gibi gerçek zamanlı uygulamaların ihtiyaçlarını karşılamak için 1994 yılında geliştirilmiştir. IntServ, birçok QoS gereksinimini karşılayabilen çoklu hizmet modelidir.

IntServ, gerçek zamanlı uygulamaların gerektirdiği uçtan uca QoS'yi sunar. IntServ, bazen mikro akışlar olarak adlandırılan bireysel akışlara veya akışlara QoS sağlamak için ağ kaynaklarını açıkça yönetir. QoS'yi kurmak ve sürdürmek için yapı taşları olarak kaynak ayırma ve kabul kontrol mekanizmalarını kullanır. Bu, "katı QoS" olarak bilinen bir kavrama benzer. Hard QoS, uçtan uca bant genişliği, gecikme ve paket kaybı oranları gibi trafik özelliklerini garanti eder. Hard QoS, kritik görev uygulamaları için hem öngörülebilir hem de garantili hizmet seviyeleri sağlar.

Şekil, IntServ modelinin basit bir resmini gösterir.




IntServ, telefon ağı tasarımından miras alınan bağlantı odaklı bir yaklaşım kullanır. Her bir iletişim, kendi trafik tanımlayıcısını ve ağ için istenen kaynakları açıkça belirtmelidir. Uç yönlendirici, ağda mevcut kaynakların yeterli olduğundan emin olmak için kabul denetimi gerçekleştirir. IntServ standardı, bir yol boyunca yönlendiricilerin her bir iletişim için durumu ayarladığını ve durumunu koruduğunu varsayar.

IntServ modelinde, uygulama veri göndermeden önce ağdan belirli bir hizmet türü talep eder. Uygulama, ağa trafik profili hakkında bilgi verir ve bant genişliği ve gecikme gereksinimlerini kapsayabilen belirli bir hizmet türü talep eder. IntServ, ağ üzerinden uçtan uca yoldaki cihazlar boyunca bir uygulamanın trafiğinin QoS ihtiyaçlarını işaret etmek için Kaynak Rezervasyon Protokolünü (RSVP) kullanır. Yol üzerindeki ağ cihazları gerekli bant genişliğini ayırabilirse, başlatan uygulama iletime başlayabilir. Talep edilen rezervasyon yol boyunca başarısız olursa, başlatan uygulama herhangi bir veri göndermez.

Uç yönlendirici, uygulamadan gelen bilgilere ve mevcut ağ kaynaklarına dayalı olarak kabul denetimi gerçekleştirir. Ağ, trafik profil özellikleri dahilinde kaldığı sürece uygulamanın QoS gereksinimlerini karşılamayı taahhüt eder. Ağ, akış başına durumu koruyarak ve ardından bu duruma göre paket sınıflandırması, denetleme ve akıllı kuyruklama gerçekleştirerek taahhüdünü yerine getirir.

Tablo, IntServ modelinin avantajlarını ve dezavantajlarını listeler.

| Faydaları | Dezavantajlar |
|---|---|
| • Açık uçtan uca kaynak kabul denetimi<br>• İstek başına politika kabul denetimi<br>• Dinamik bağlantı noktası numaralarının sinyalizasyonu | • Sürekli sinyalleşme için durum bilgisi olan mimari gereksinimi nedeniyle kaynak yoğun.<br>• Akış tabanlı yaklaşım, internet gibi büyük uygulamalara ölçeklenemez. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 38.9.4.Farklılaştırılmış Hizmetler

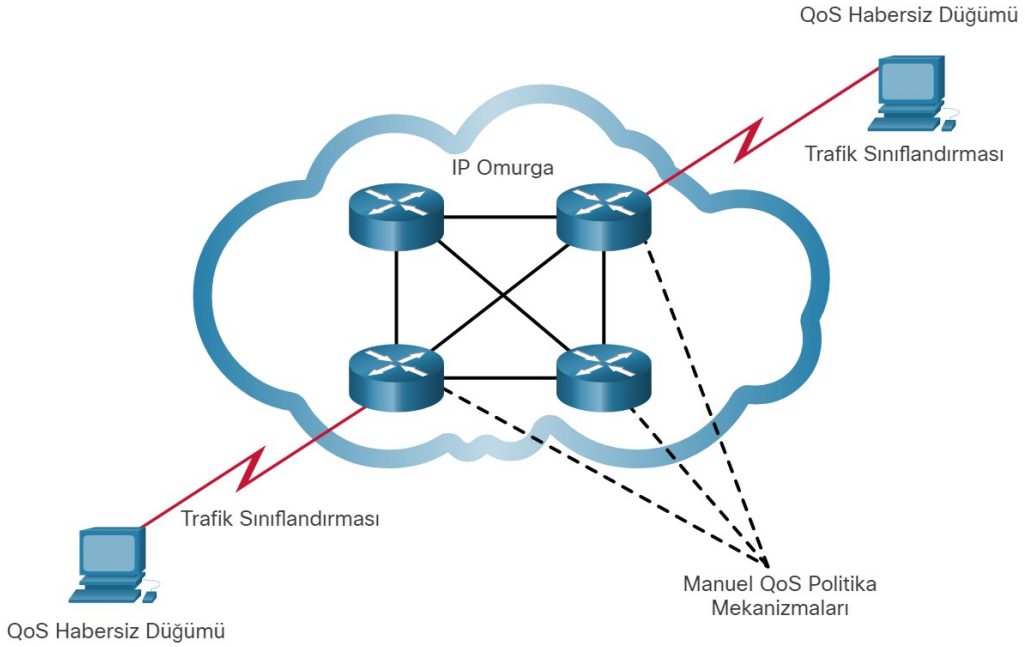
Farklılaştırılmış hizmetler (DiffServ) QoS modeli, ağ trafiğini sınıflandırmak ve yönetmek için basit ve ölçeklenebilir bir mekanizma belirtir. Örneğin, DiffServ, ses veya video gibi kritik ağ trafiğine düşük gecikmeli garantili hizmet sunarken, web trafiği veya dosya aktarımları gibi kritik olmayan hizmetlere basit ve en iyi şekilde trafik garantileri sağlar.

DiffServ tasarımı, hem en iyi çaba hem de IntServ modellerinin sınırlamalarının üstesinden gelir. DiffServ modeli, RFC'ler 2474, 2597, 2598, 3246, 4594'te açıklanmıştır. DiffServ, maliyet etkin ve ölçeklenebilir olmasına rağmen "neredeyse garantili" bir QoS sağlayabilir.

DiffServ modeli konsept olarak bir teslimat hizmeti kullanarak paket göndermeye benzer. Bir paket gönderirken bir hizmet düzeyi talep edersiniz (ve bunun için ödeme yaparsınız). Paket ağı boyunca, ödediğiniz hizmet seviyesi tanınır ve paketinize, ne istediğinize bağlı olarak tercihli veya normal hizmet verilir.

DiffServ uçtan uca bir QoS stratejisi değildir çünkü uçtan uca garantileri uygulayamaz. Bununla birlikte, DiffServ QoS, QoS'yi uygulamaya yönelik daha ölçeklenebilir bir yaklaşımdır. IntServ ve son ana bilgisayarların QoS ihtiyaçlarını ağa bildirdiği sabit QoS'nin aksine, DiffServ sinyalleme kullanmaz. Bunun yerine, DiffServ bir "yumuşak QoS" yaklaşımı kullanır. Ağ öğelerinin, her biri farklı QoS gereksinimlerine sahip birden çok trafik sınıfına hizmet verecek şekilde ayarlandığı, sağlanan QoS modelinde çalışır.

Şekil, DiffServ modelinin basit bir resmini gösterir.




Bir ana bilgisayar trafiği bir yönlendiriciye iletirken, yönlendirici akışları kümeler (sınıflar) halinde sınıflandırır ve sınıflar için uygun QoS ilkesini sağlar. DiffServ, hem esneklik hem de ölçeklenebilirlik sağlamak için her trafik sınıfına tek tip olarak küresel anlam uygulayarak, QoS mekanizmalarını atlamalı olarak uygular ve uygular. Örneğin, DiffServ, tüm TCP akışlarını tek bir sınıf olarak gruplayacak ve IntServ'in yapacağı gibi tek tek akışlar yerine bu sınıf için bant genişliği tahsis edecek şekilde yapılandırılabilir. DiffServ, trafiği sınıflandırmaya ek olarak, her ağ düğümündeki sinyal ve durum bakım gereksinimlerini en aza indirir.

Özellikle, DiffServ, ağ trafiğini iş gereksinimlerine göre sınıflara ayırır. Sınıfların her birine farklı bir hizmet düzeyi atanabilir. Paketler bir ağdan geçerken, ağ aygıtlarının her biri paket sınıfını tanımlar ve paketi bu sınıfa göre hizmet verir. DiffServ ile birçok servis seviyesi seçmek mümkündür. Örneğin, IP telefonlarından gelen ses trafiğine

Licensed to yetkin karasingir, yetkinksingir@gmail.com

genellikle diğer tüm uygulama trafiğine göre öncelikli muamele yapılır, e-postaya genellikle en iyi şekilde hizmet verilir ve ticari olmayan trafiğe çok kötü hizmet verilebilir veya tamamen engellenebilir.
Şekil, DiffServ modelinin faydalarını ve dezavantajlarını listeler.

| Faydaları | Dezavantajlar |
|---|---|
| • Son derece ölçeklenebilir<br>• Birçok farklı kalite seviyesi sağlar | • Hizmet kalitesinin mutlak garantisi yok<br>• Ağda uyum içinde çalışmak için bir dizi karmaşık mekanizma gerektirir |

## 38.10.QoS Uygulama Teknikleri

### 38.10.1.Paket Kaybını Önleme

Paket kaybı genellikle bir arayüzdeki tıkanıklığın sonucudur. TCP kullanan çoğu uygulama yavaşlama yaşar çünkü TCP otomatik olarak ağ tıkanıklığına göre ayarlanır. Düşen TCP kesimleri, TCP oturumlarının pencere boyutlarını küçültmesine neden olur. Bazı uygulamalar TCP kullanmaz ve düşmeleri (hassas akışlar) işleyemez.

Aşağıdaki yaklaşımlar, hassas uygulamalarda düşüşleri önleyebilir:

- Tıkanıklığı önlemek için bağlantı kapasitesini artırın.
- Yeterli bant genişliğini garanti edin ve kırılgan akışlardan gelen trafik patlamalarına uyum sağlamak için arabellek alanını artırın. Daha önce bahsettiğimiz WFQ, CBWFQ ve LLQ, bant genişliğini garanti edebilir ve düşmeye duyarlı uygulamalara öncelikli yönlendirme sağlayabilir.
- Daha düşük öncelikli paketleri tıkanıklık oluşmadan bırakın. Cisco IOS QoS, tıkanıklık oluşmadan önce düşük öncelikli paketleri bırakmaya başlayan ağırlıklı rastgele erken algılama- weighted random early detection ((WRED) gibi kuyruk oluşturma mekanizmaları sağlar.

### 38.10.2.QoS Araçları

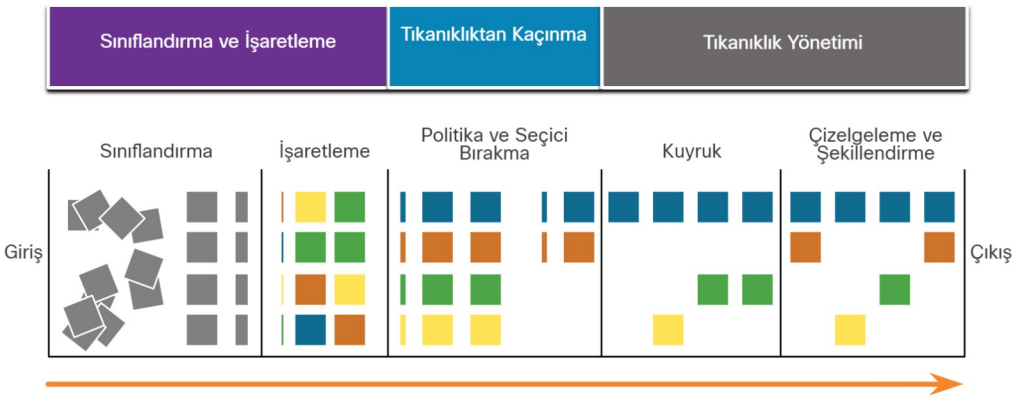
QoS araçlarının üç kategorisi vardır:

- Sınıflandırma ve işaretleme araçları
- Tıkanıklık önleme araçları
- Tıkanıklık yönetimi araçları

| QoS Araçları | Açıklama |
|---|---|
| Sınıflandırma ve işaretleme araçları | • Oturumlar veya akışlar, hangi trafik sınıfına ait olduklarını belirlemek için analiz edilir.<br>• Trafik sınıfı belirlendiğinde paketler işaretlenir. |
| Tıkanıklık önleme araçları | • Trafik sınıfları, QoS politikası tarafından tanımlandığı gibi, ağ kaynaklarının ayrılan kısımlarıdır.<br>• QoS politikası, tıkanıklığı önlemek için bazı trafiğin nasıl seçici olarak bırakılabileceğini, geciktirilebileceğini veya yeniden işaretlenebileceğini de tanımlar.<br>• Birincil tıkanıklıktan kaçınma aracı WRED'dir ve TCP veri trafiğini, kuyruk taşmalarının neden olduğu kuyruk düşüşleri meydana gelmeden önce bant genişliği açısından verimli bir şekilde düzenlemek için kullanılır. |
| Tıkanıklık yönetimi araçları | • Trafik mevcut ağ kaynaklarını aştığında, kaynakların kullanılabilirliğini beklemek için trafik kuyruğa alınır.<br>• Yaygın Cisco IOS tabanlı tıkanıklık yönetimi araçları, CBWFQ ve LLQ algoritmalarını içerir. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 38.10.3.QoS Sırası




Şekilde gösterildiği gibi, giriş paketleri (gri kareler) sınıflandırılır ve ilgili IP başlıkları işaretlenir (renkli kareler). Tıkanıklığı önlemek için, paketler daha sonra tanımlanmış ilkelere göre kaynaklar tahsis edilir. Paketler daha sonra sıraya alınır ve tanımlanmış QoS şekillendirme ve denetleme politikalarına göre çıkış arabiriminden dışarı iletilir.

Not : Sınıflandırma ve işaretleme giriş veya çıkışta yapılabilirken, kuyruklama ve şekillendirme gibi diğer QoS eylemleri genellikle çıkışta yapılır.

## 38.10.4.Sınıflandırma ve İşaretleme(Classification and Marking)

Bir pakete bir QoS politikası uygulanmadan önce, paketin sınıflandırılması gerekir. Sınıflandırma ve işaretleme, paket türlerini tanımlamamıza veya "işaretlememize" olanak tanır. Sınıflandırma, paketlerin veya çerçevelerin ait olduğu trafik sınıfını belirler. Yalnızca trafik işaretlendikten sonra ona politikalar uygulanabilir.

Bir paketin nasıl sınıflandırılacağı QoS uygulamasına bağlıdır. Katman 2 ve 3'teki trafik akışlarını sınıflandırma yöntemleri arasında arayüzler, ACL'ler ve sınıf haritaları kullanımı bulunur. Trafik, Ağ Tabanlı Uygulama Tanıma-Network Based Application Recognition(NBAR) kullanılarak Katman 4 ila 7 arasında da sınıflandırılabilir.

İşaretleme, paket başlığına bir değer eklediğimiz anlamına gelir. Paketi alan cihazlar, tanımlı bir ilkeyle eşleşip eşleşmediğini görmek için işaretli alana bakar. İşaretleme, kaynak cihaza mümkün olduğunca yakın yapılmalıdır. Bu güven sınırını oluşturur.
Trafiğin nasıl işaretlendiği genellikle teknolojiye bağlıdır. Şekildeki tablo, çeşitli teknolojilerde kullanılan bazı markalama alanlarını açıklamaktadır. Katman 2 veya 3'te (veya her ikisinde) trafiği işaretleyip işaretlememe kararı önemsiz değildir ve aşağıdaki noktalar dikkate alındıktan sonra verilmelidir:

- IP dışı trafik için katman 2 katman işaretlemesi gerçekleştirilebilir.
- Katman 2 çerçevelerin işaretlenmesi, "IP duyarlı" olmayan anahtarlar için kullanılabilen tek QoS seçeneğidir.
- Katman 3 işareti, QoS bilgilerini uçtan uca taşıyacaktır.

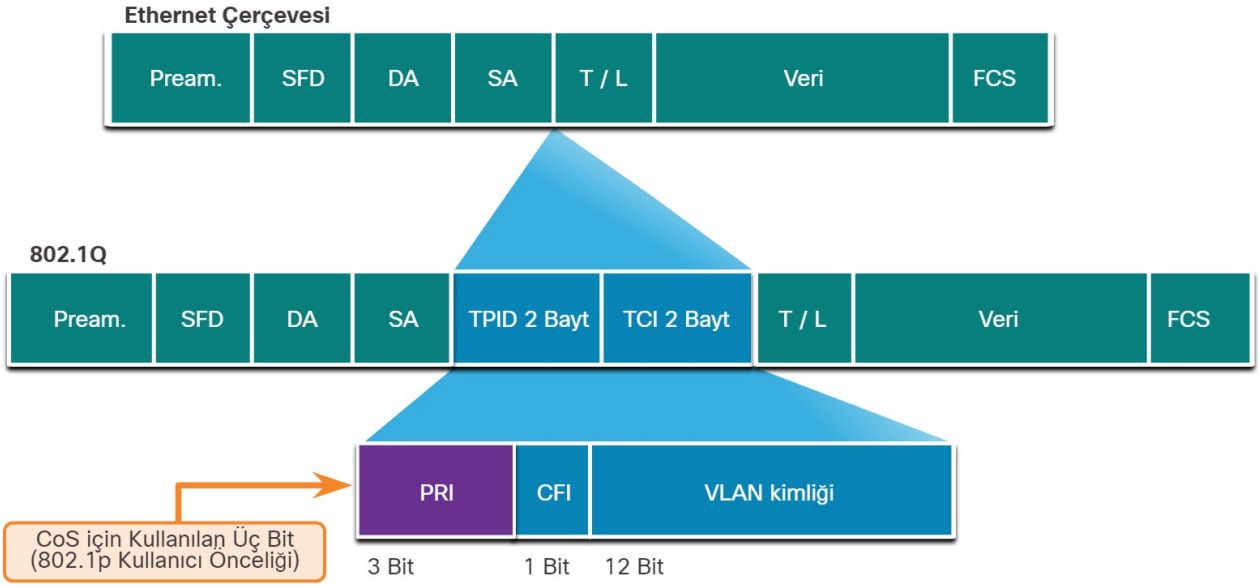
**QoS için Trafik İşaretlemesi**

| QoS Araçları | Katman | İşaretleme Alanı | Bit cinsinden genişlik |
|---|---|---|---|
| Ethernet (802.1Q, 802.1p) | 2 | Hizmet Sınıfı-Class of Service (CoS) | 3 |
| 802.11 (Kablosuz) | 2 | Wi-Fi Trafik Tanımlayıcı-Wi-Fi Traffic Identifier (TID) | 3 |
| MPLS | 2 | Deneysel-Experimental (EXP) | 3 |
| IPv4 ve IPv6 | 3 | IP Önceliği-IP Precedence (IPP) | 3 |
| IPv4 ve IPv6 | 3 | Farklılaştırılmış Hizmetler Kod Noktası- Differentiated Services Code Point (DSCP) | 6 |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 38.10.5.Katman 2'de İşaretleme

802.1Q, Ethernet ağlarında Katman 2'de VLAN etiketlemeyi destekleyen IEEE standardıdır. 802.1Q uygulandığında, Ethernet Çerçevesine iki alan eklenir. Şekilde gösterildiği gibi, bu iki alan, kaynak MAC adres alanını takiben Ethernet çerçevesine eklenir.




802.1Q standardı, IEEE 802.1p olarak bilinen QoS önceliklendirme şemasını da içerir. 802.1p standardı, Etiket Kontrol Bilgileri- Tag Control Information(TCI) alanındaki ilk üç biti kullanır. Öncelik (PRI) alanı olarak bilinen bu 3 bitlik alan, Hizmet Sınıfı (CoS) işaretlerini tanımlar. Üç bit, Katman 2 Ethernet çerçevesinin şekilde gösterildiği gibi sekiz öncelik seviyesinden biriyle (0-7 değerleri) işaretlenebileceği anlamına gelir.

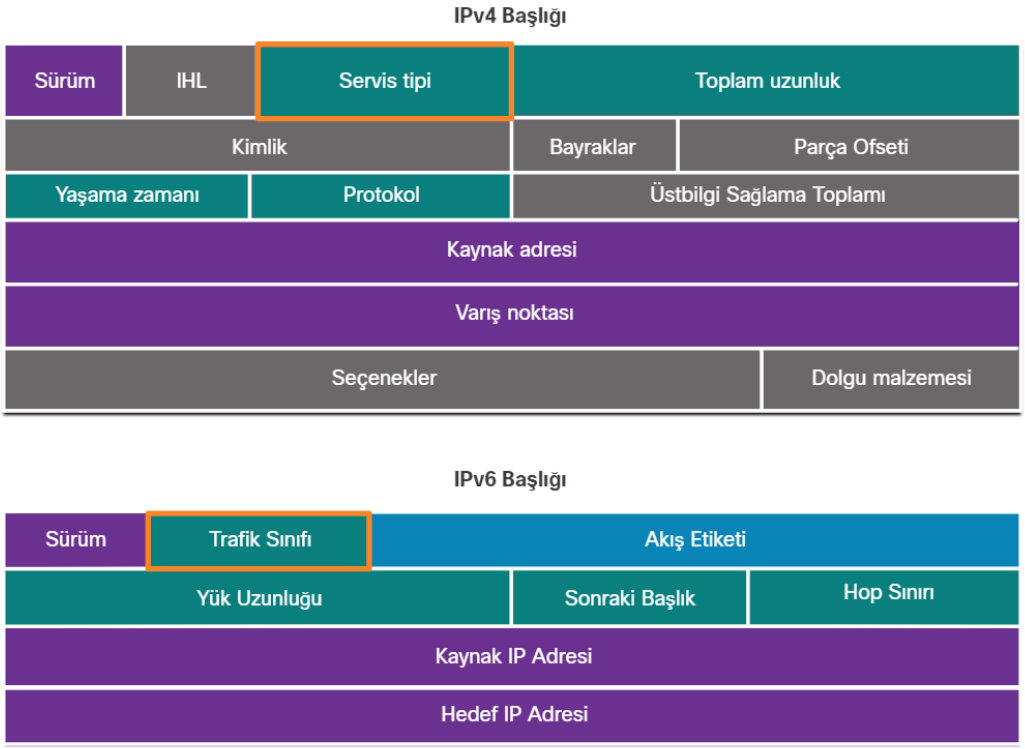
### Ethernet Hizmet Sınıfı-Class of Service (CoS) Değerleri

| CoS Değeri | CoS İkili Değeri | Açıklama |
|---|---|---|
| 0 | 000 | En İyi Çaba Verileri |
| 1 | 001 | Orta Öncelikli Veriler |
| 2 | 010 | Yüksek Öncelikli Veriler |
| 3 | 011 | Çağrı Sinyali |
| 4 | 100 | Video konferans |
| 5 | 101 | Ses taşıyıcı (ses trafiği) |
| 6 | 110 | Ayrılmış |
| 7 | 111 | Ayrılmış |

## 38.10.6.Katman 3'te İşaretleme

IPv4 ve IPv6, paketleri işaretlemek için paket başlıklarında 8 bitlik bir alan belirtir. Şekilde gösterildiği gibi, hem IPv4 hem de IPv6, işaretleme için 8 bitlik bir alanı destekler: IPv4 için Hizmet Türü- Type of Service (ToS) alanı ve IPv6 için Trafik Sınıfı- Traffic Class alanı.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

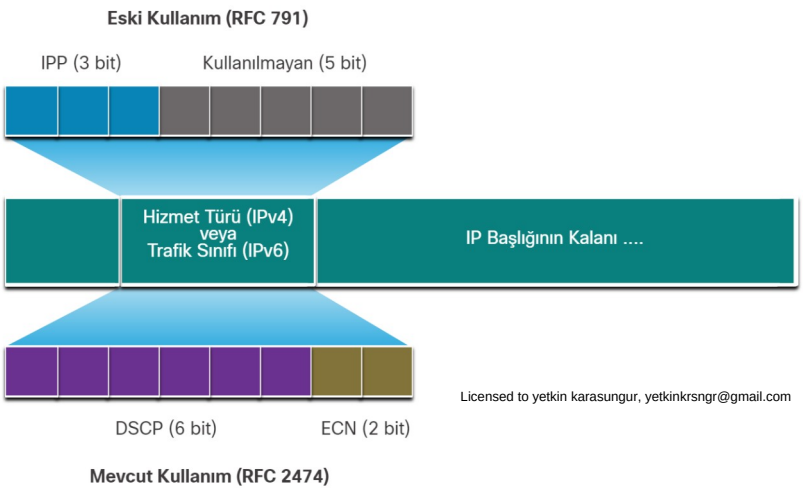



## 38.10.7.Hizmet Türü ve Trafik Sınıfı Alanı(Type of Service and Traffic Class Field)

Hizmet Türü (IPv4) ve Trafik Sınıfı (IPv6), QoS sınıflandırma araçları tarafından atanan paket işaretini taşır. Alan daha sonra uygun atanmış QoS politikasına göre paketleri ileten alıcı cihazlar tarafından belirtilir.

Şekil, 8 bitlik alanın içeriğini gösterir. RFC 791'de, orijinal IP standardı, QoS işaretlemeleri için kullanılacak IP Önceliği (IPP) alanını belirledi.

RFC 2474, RFC 791'in yerini alır ve IPP alanını yeniden adlandırıp genişleterek ToS alanını yeniden tanımlar. Şekilde gösterildiği gibi yeni alan, QoS için ayrılmış 6 bittir. Farklılaştırılmış Hizmetler Kod Noktası (DSCP) alanı olarak adlandırılan bu altı bit, maksimum 64 olası hizmet sınıfı sunar. Kalan iki IP Açık Tıkanıklık Bildirimi-Explicit Congestion Notification (ECN) biti, ECN tanıyan yönlendiriciler tarafından paketleri düşürmek yerine işaretlemek için kullanılabilir. ECN işareti, aşağı yöndeki yönlendiricilere paket akışında tıkanıklık olduğunu bildirir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 38.10.8.DSCP Değerleri

64 DSCP değeri üç kategoride düzenlenmiştir:

- En İyi Çaba-Best-Effort (BE) - Bu, tüm IP paketleri için varsayılandır. DSCP değeri 0'dır. Atlama başına davranış, normal yönlendirmedir. Bir yönlendirici tıkanıklık yaşadığında bu paketler atılır. QoS planı uygulanmaz.
- Hızlandırılmış İletim-Expedited Forwarding (EF) - RFC 3246 tanımlar EF DSCP ondalık değer 46 (ikili olarak 101 110). İlk 3 bit (101), ses trafiği için kullanılan Katman 2 CoS değeri 5 ile doğrudan eşleşir. Katman 3'te Cisco, EF'in yalnızca ses paketlerini işaretlemek için kullanılmasını önerir.
- Garantili Yönlendirme-Assured Forwarding (AF) - RFC 2597, AF'yi kuyrukları ve bırakma tercihini belirtmek için en önemli 5 DSCP bitini kullanacak şekilde tanımlar. AF'nin tanımı şekilde gösterilmektedir.

| Garantili Yönlendirme Değerleri | | | |
|---|---|---|---|
| | **Düşük Düşüş** | **Orta Düşüş** | **Yüksek Düşüş** |
| **4. Sınıf** | AF41 (34) | AF42 (36) | AF43 (38) |
| **3. Sınıf** | AF31 (26) | AF32 (28) | AF33 (30) |
| **Sınıf 2** | AF21 (18) | AF22 (20) | AF23 (22) |
| **1. sınıf** | AF11 (10) | AF12 (12) | AF13 (14) |

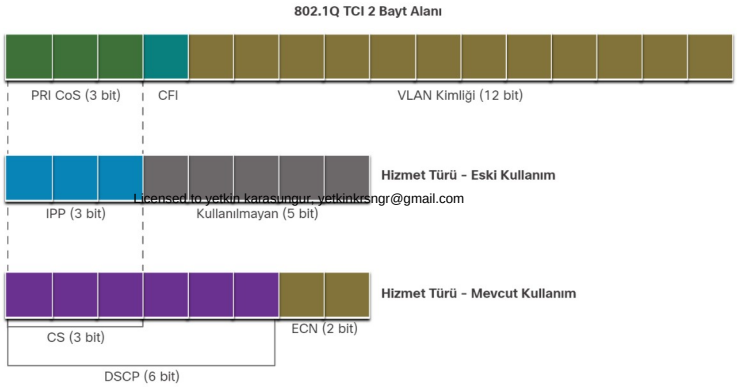
**AFxy** aşağıdaki şekilde formül belirtilir:

- Sınıfı belirlemek için en önemli ilk 3 bit kullanılır. Sınıf 4 en iyi kuyruktur ve Sınıf 1 en kötü kuyruktur.
- 4. ve 5. en önemli bitler, bırakma tercihini belirtmek için kullanılır.
- 6. en önemli bit sıfıra ayarlanmıştır.

Örneğin, AF32, 3. sınıfa (ikili 011) aittir ve orta bir düşme tercihine sahiptir (ikili 10). 6. 0 biti (ikili 011100) dahil ettiğiniz için tam DSCP değeri 28'dir.

## 38.10.9.Sınıf Seçici Bitler (Class Selector Bits)

DSCP alanının ilk 3 en önemli biti sınıfı gösterdiğinden, bu bitlere Sınıf Seçici (CS) bitleri de denir. Bu 3 bit, şekilde gösterildiği gibi 802.1p ve RFC 791 ile uyumluluğu korumak için CoS alanının 3 bitiyle ve IPP alanıyla doğrudan eşleşir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

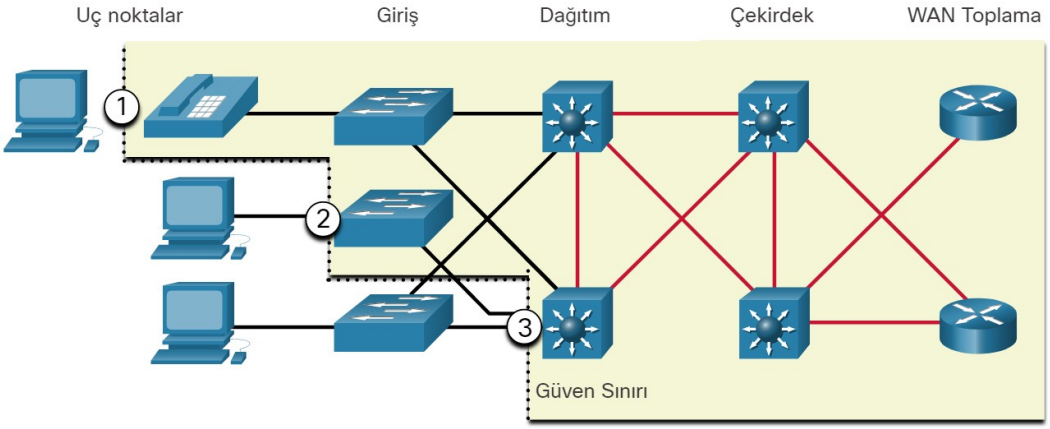
## 38.10.10.Güven Sınırları(Trust Boundaries)

İşaretler nerede oluşmalıdır? Trafik, teknik ve idari olarak uygun olduğu için kaynağına yakın olarak sınıflandırılmalı ve işaretlenmelidir. Bu, şekilde gösterildiği gibi güven sınırını tanımlar.

1. Güvenilir uç noktalar, uygulama trafiğini uygun Katman 2 CoS ve / veya Katman 3 DSCP değerlerine işaretlemek için yeteneklere ve zekaya sahiptir. Güvenilir uç noktaların örnekleri arasında IP telefonları, kablosuz erişim noktaları, video konferans ağ geçitleri ve sistemleri, IP konferans istasyonları ve daha fazlası bulunur.
2. Güvenli uç noktalarda, Katman 2 anahtarında trafik işaretli olabilir.
3. Trafik, Katman 3 anahtarlarında / yönlendiricilerinde de işaretlenebilir.

Trafiğin yeniden işaretlenmesi, örneğin, CoS değerlerinin IP Emsali veya DSCP değerlerine yeniden işaretlenmesi tipik olarak gereklidir.

**Çeşitli Güven Sınırları**




## 38.10.11.Tıkanıklıktan Kaçınma

Tıkanıklık yönetimi, bir çıkış arabiriminin gönderilmesini beklerken fazla trafiğin arabelleğe alındığı veya kuyruğa alındığı (ve bazen bırakıldığı) sıraya koyma ve zamanlama yöntemlerini içerir. Tıkanıklığı önleme araçları daha basittir. Sıkışıklık bir sorun haline gelmeden önce ortak ağdaki tıkanıklığı ve ağlar arası darboğazları tahmin etmek ve önlemek amacıyla ağ trafiği yüklerini izlerler. Bu araçlar, şekilde gösterildiği gibi kuyruğun ortalama derinliğini izleyebilir. Sıra minimum eşiğin altında olduğunda, düşüş olmaz. Kuyruk maksimum eşiğe kadar dolduğunda, küçük bir paket yüzdesi bırakılır. Maksimum eşik aşıldığında tüm paketler düşer.

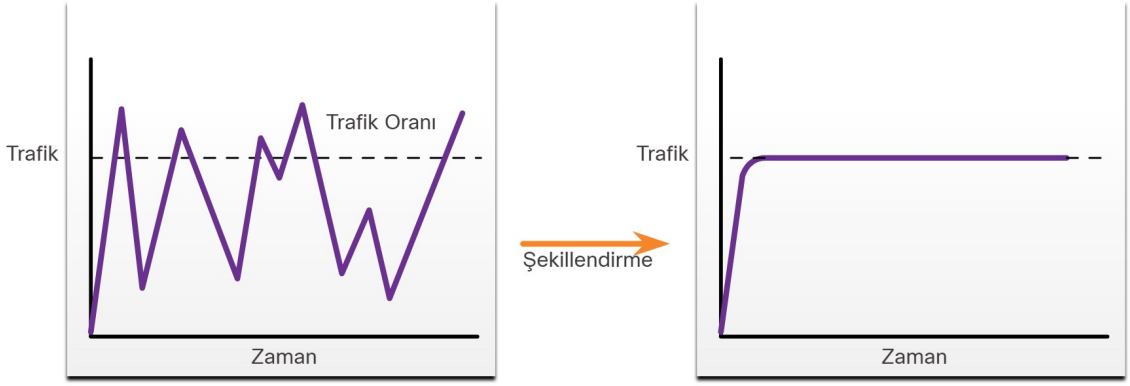
## 38.10.12.Şekillendirme ve Denetleme (Shaping and Policing)

Trafik şekillendirme ve trafik denetimi, tıkanıklığı önlemek için Cisco IOS QoS yazılımı tarafından sağlanan iki mekanizmadır.

Trafik şekillendirme, bir kuyruktaki fazla paketleri tutar ve ardından fazlalığı daha sonraki zaman aralıklarıyla iletmek üzere planlar. Trafik şekillendirmenin sonucu, şekilde gösterildiği gibi düzleştirilmiş bir paket çıktı hızıdır.

Şekil, trafiği şekillendirmenin bir örneğini göstermektedir. Şekilde iki grafik gösterilmektedir. İlk grafik, belirli bir süre boyunca maksimum trafik oranının üzerine çıkan trafiği gösterir. İkinci grafik, şekillendirmeden sonraki trafiği gösterir. Trafik, düzgün bir paket çıktı hızına sahip olacak şekilde şekillendirilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

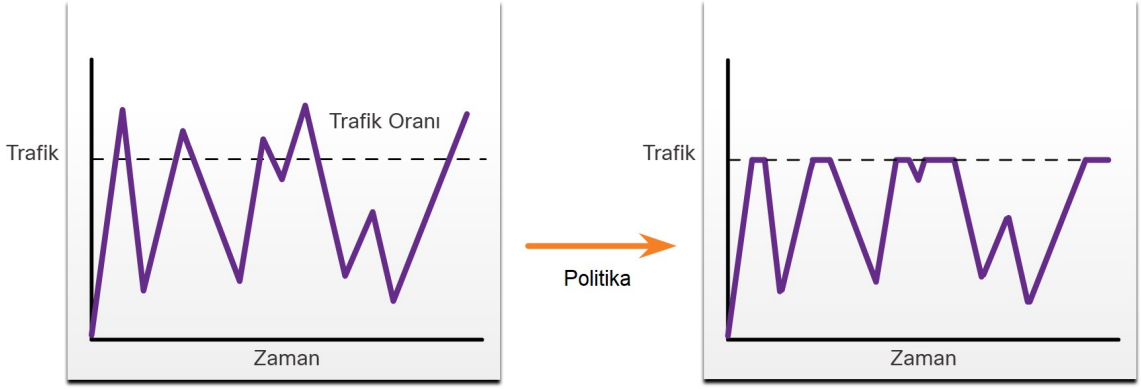



Biçimlendirme, bir kuyruğun ve gecikmeli paketleri arabelleğe almak için yeterli belleğin varlığını kabul ederken, denetim yapmaz.

Şekillendirmeyi etkinleştirirken yeterli belleğe sahip olduğunuzdan emin olun. Ek olarak, şekillendirme herhangi bir gecikmiş paketin daha sonraki iletimi için bir programlama işlevi gerektirir. Bu programlama işlevi, şekillendirme kuyruğunu farklı kuyruklar halinde düzenlemenizi sağlar. Zamanlama fonksiyonlarının örnekleri CBWFQ ve LLQ'dur.

Şekillendirme, giden bir kavramdır; bir arayüzden çıkan paketler sıraya alınır ve şekillendirilebilir. Bunun aksine, politika bir arayüzdeki gelen trafiğe uygulanır. Trafik hızı yapılandırılmış maksimum hıza ulaştığında, fazla trafik atılır veya yeniden işaretlenir.

Politika, sözleşmeli bir müşteri bilgi oranını- customer information rate (CIR) uygulamak için hizmet sağlayıcılar tarafından yaygın olarak uygulanır. Bununla birlikte, hizmet sağlayıcının ağı şu anda tıkanıklık yaşamıyorsa, hizmet sağlayıcı CIR üzerinden patlamaya-bursting da izin verebilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 39.Bölüm: Ağ Yönetimi

## 39.1.CDP ile Cihaz Keşfi

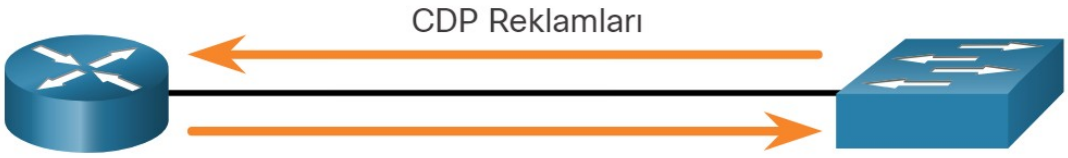
### 39.1.1.CDP'ye Genel Bakış

Ağınız hakkında bilmek istediğiniz ilk şey, içinde hangi cihazların olduğu? Bu bileşenler nerede? Nasıl bağlanırlar? Temel olarak, bir haritaya ihtiyacınız var. Bu konu, ağınızın bir haritasını oluşturmak için Cisco Keşif Protokolünü-Cisco Discovery Protocol (CDP) nasıl kullanabileceğinizi açıklamaktadır.

CDP, aynı veri bağlantısını paylaşan Cisco cihazları hakkında bilgi toplamak için kullanılan Cisco'ya özel bir Katman 2 protokolüdür. CDP, medyadan ve protokolden bağımsızdır ve yönlendiriciler, anahtarlar ve erişim sunucuları gibi tüm Cisco cihazlarında çalışır.

Cihaz, şekilde gösterildiği gibi bağlı cihazlara periyodik CDP reklamları-tanıtımları gönderir.

Şekilde, doğrudan bağlanan bir yönlendirici ve anahtar arasında gönderilen Cisco Keşif Protokolü (CDP) reklamları gösterilmektedir. CDP reklamları etiketli bir ok, anahtardan yönlendiriciye işaret ediyor ve başka bir ok, yönlendiriciden anahtara işaret ediyor. Oklar, iki cihaz arasında gönderilen periyodik CDP reklamlarını gösterir.




Bu reklamlar, keşfedilen cihazın türü, cihazların adı ve arayüzlerin sayısı ve türü hakkında bilgi paylaşır.

Çoğu ağ cihazı diğer cihazlara bağlı olduğundan, CDP ağ tasarımı kararlarında, sorun gidermede ve ekipmanda değişiklik yapmada yardımcı olabilir. CDP, komşu aygıtlar hakkındaki bilgileri belirlemek için bir ağ keşif aracı olarak da kullanılabilir. CDP'den toplanan bu bilgiler, dokümantasyon eksik veya ayrıntıda eksik olduğunda bir ağın mantıksal bir topolojisinin oluşturulmasına yardımcı olabilir.

### 39.1.2.CDP'yi Yapılandırma ve Doğrulama

Cisco cihazları için CDP varsayılan olarak etkindir. Güvenlik nedenleriyle, CDP'yi bir ağ cihazında global olarak veya arayüz başına devre dışı bırakmak istenebilir. CDP ile bir saldırgan, IP adresleri, IOS sürümleri ve cihaz türleri gibi ağ düzeni hakkında değerli bilgiler toplayabilir.

CDP'nin durumunu doğrulamak ve CDP hakkındaki bilgileri görüntülemek için, örnekte gösterildiği gibi **show cdp** komutunu girin .

```
Router# show cdp
Global CDP information:
      Sending CDP packets every 60 seconds
      Sending a holdtime value of 180 seconds
      Sending CDPv2 advertisements is enabled
```

Aygıtta desteklenen tüm arabirimler için CDP'yi global olarak etkinleştirmek için , global yapılandırma modunda **cdp run** yazın. CDP , global yapılandırma modunda **no cdp run** komutu ile aygıttaki tüm arabirimler için devre dışı bırakılabilir .

```
Router(config)# no cdp run
Router(config)# exit
Router# show cdp
CDP is not enabled
Router# configure terminal
Router(config)# cdp run
```

Bir ISP'ye bakan arabirim gibi belirli bir arabirimde CDP'yi devre dışı bırakmak için arabirim yapılandırma modunda **no cdp enable** komutunu girin . CDP, cihazda hala etkindir; ancak, bu arayüzden daha fazla CDP reklamı gönderilmeyecektir. CDP'yi belirli arayüzde tekrar etkinleştirmek için , örnekte gösterildiği gibi **cdp enable** yazın .

```
Switch(config)# interface gigabitethernet 0/0/1
Switch(config-if)# cdp enable
```

CDP'nin durumunu doğrulamak ve komşuların bir listesini görüntülemek için , ayrıcalıklı EXEC modunda **show cdp neighbors** komutunu kullanın. show cdp neighbors komutu CDP komşuları hakkında önemli bilgiler görüntüler. Örnekte görüntülenen **show cdp neighbours** komutunun sonuçlarında belirtildiği gibi, şu anda bu aygıtın herhangi bir komşusu yoktur, çünkü herhangi bir aygıta fiziksel olarak bağlı değildir .

```
Router# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID

Total cdp entries displayed : 0
```

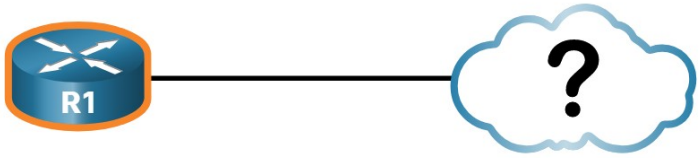
Bir aygıtta CDP etkin arabirimleri görüntülemek için **show cdp interface** komutunu kullanın. Her arayüzün durumu da görüntülenir. Şekil, başka bir cihaza yalnızca bir etkin bağlantıyla yönlendiricide beş arabirimin CDP etkin olduğunu göstermektedir.

```
Router# show cdp interface
GigabitEthernet0/0/0 is administratively down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0/1 is up, line protocol is up
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0/0/2 is down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/1/0 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
Serial0/1/1 is administratively down, line protocol is down
  Encapsulation HDLC
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
GigabitEthernet0 is down, line protocol is down
  Encapsulation ARPA
  Sending CDP packets every 60 seconds
  Holdtime is 180 seconds
 cdp enabled interfaces : 6
 interfaces up          : 1
 interfaces down        : 5
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 39.1.3.CDP Kullanarak Aygıtları Keşfedin

Şekilde gösterilen topolojideki dokümantasyon eksikliğini düşünün. Ağ yöneticisi yalnızca R1'in başka bir cihaza bağlı olduğunu bilir.

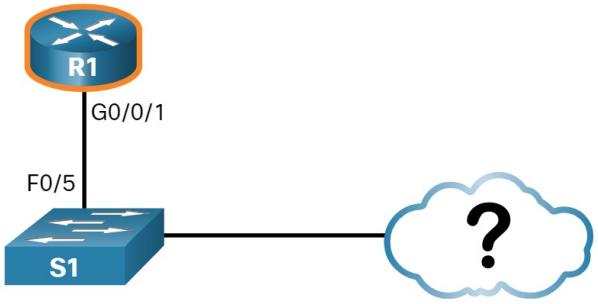



Ağda CDP etkinleştirildiğinde, **show cdp neighbours** komutu çıktıda gösterildiği gibi ağ düzenini belirlemek için kullanılabilir.

```
R1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Gig 0/0/1           179         S I      WS-C3560- Fas 0/5
```

Ağın geri kalanıyla ilgili hiçbir bilgi mevcut değildir. **show cdp neighbours** komutu aşağıdakilerden dahil olmak üzere her CDP komşu aygıt hakkında yararlı bilgiler sağlar:

Cihaz tanımlayıcıları - Bu, komşu cihazın (S1) ana bilgisayar adıdır.
Bağlantı noktası tanımlayıcı - Bu, yerel ve uzak bağlantı noktasının adıdır (sırasıyla G0 / 0/1 ve F0 / 5).
Yetenekler listesi - Bu, cihazın bir yönlendirici mi yoksa bir anahtar mı olduğunu gösterir (anahtar için S; IGMP için I)
Platform - Bu, cihazın donanım platformudur (Cisco 3560 anahtarı için WS-C3560).
Çıktı, R1 üzerindeki G0 / 0/1 arayüzüne bağlı başka bir Cisco cihazı S1 olduğunu gösterir. Ayrıca, güncellenmiş topolojide gösterildiği gibi S1, F0 / 5 aracılığıyla bağlanır.




Ağ yöneticisi, S1 için IP adresini keşfetmek için **show cdp neighbors detail** komutunu kullanır.. Çıkışta görüntülendiği gibi, S1 için adres 192.168.1.2'dir.

```
R1# show cdp neighbors detail
------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.2
Platform: cisco WS-C3560-24TS,  Capabilities: Switch IGMP
Interface: GigabitEthernet0/0/1,  Port ID (outgoing port): FastEthernet0/5
Holdtime : 136 sec

Version :
Cisco IOS Software, C3560 Software (C3560-LANBASEK9-M), Version 15.0(2)SE7, R
RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 23-Oct-14 14:49 by prod_rel_team
```

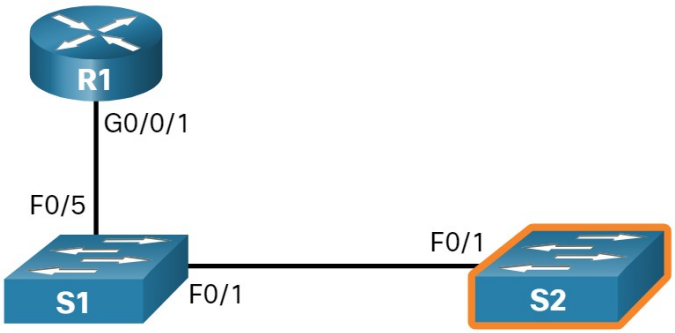
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
advertisement version: 2
Protocol Hello:  OUI=0x00000C, Protocol ID=0x0112; payload len=27,
value=00000000FFFFFFFF010221FF0000000000000002291210380FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 192.168.1.2

Total cdp entries displayed : 1
```

S1'e SSH aracılığıyla uzaktan veya konsol bağlantı noktası aracılığıyla fiziksel olarak erişerek, ağ yöneticisi, şekilde **show cdp neighbors** komutu çıktısında gösterildiği gibi, S1'e başka hangi cihazların bağlı olduğunu belirleyebilir .

```
S1# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S2               Fas 0/1           150             S I   WS-C2960- Fas 0/1
R1               Fas 0/5           179           R S I   ISR4331/K Gig 0/0/1
```

Çıktıda başka bir anahtar olan S2 ortaya çıkar. S2, şekilde gösterildiği gibi S1'deki F0 / 1 arayüzüne bağlanmak için F0 / 1 kullanıyor.




Yine, ağ yöneticisi S2 için IP adresini keşfetmek ve ardından ona uzaktan erişmek için **show cdp neighbors detail** özelliğini kullanabilir . Başarılı bir oturum açtıktan sonra, ağ yöneticisi daha fazla aygıt olup olmadığını keşfetmek için **show cdp neighbors** komutunu kullanır .

```
S2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Fas 0/1           141             S I   WS-C3560- Fas 0/1
```

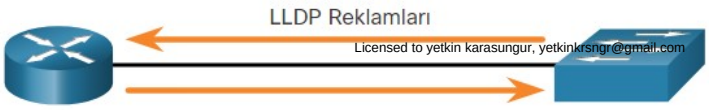
S2'ye bağlı tek cihaz S1'dir. Bu nedenle, topolojide keşfedilecek başka cihaz yoktur. Ağ yöneticisi artık keşfedilen cihazları yansıtacak şekilde belgeleri güncelleyebilir.

## 39.2.LLDP ile Cihaz Keşfi

### 39.2.1.LLDP'ye Genel Bakış

Bağlantı Katmanı Bulma Protokolü-Link Layer Discovery Protocol (LLDP), CDP ile aynı şeyi yapar, ancak Cisco cihazlarına özel değildir fakat  Cisco cihazlarınız varsa, yine de kullanabilirsiniz. Öyle ya da böyle, ağ haritanızı alacaksınız.

LLDP, CDP'ye benzer, satıcıdan bağımsız bir komşu keşif protokolüdür. LLDP, yönlendiriciler, anahtarlar ve kablosuz LAN erişim noktaları gibi ağ cihazlarıyla çalışır. Bu protokol, kimliğini ve yeteneklerini diğer cihazlara tanıtır ve bilgileri fiziksel olarak bağlı bir Katman 2 cihazından alır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 39.2.2.LLDP'yi Yapılandırma ve Doğrulama

Aygıta bağlı olarak, LLDP varsayılan olarak etkinleştirilebilir. LLDP'yi bir Cisco ağ cihazında global olarak etkinleştirmek için , global konfigürasyon modunda **run lldp** komutunu girin . LLDP'yi devre dışı bırakmak için , genel yapılandırma modunda **no lldp run** komutunu girin .

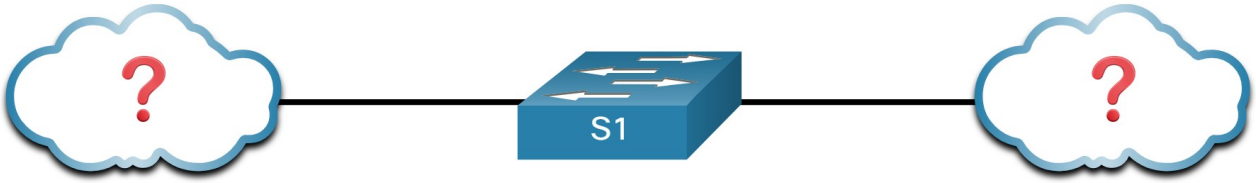
CDP'ye benzer şekilde, LLDP belirli arayüzlerde yapılandırılabilir. Ancak, LLDP, LLDP paketlerini iletmek ve almak için ayrı olarak yapılandırılmalıdır.

LLDP'nin cihazda etkinleştirildiğini doğrulamak için , ayrıcalıklı EXEC modunda **show lld**p komutunu girin .

```
Switch# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end
Switch# show lldp
Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds
```

## 39.2.3.LLDP Kullanarak Cihazları Keşfetme

Şekilde gösterilen topolojideki dokümantasyon eksikliğini düşünün. Ağ yöneticisi yalnızca S1'in iki cihaza bağlı olduğunu bilir.




LLDP etkinleştirildiğinde, aygıt komşuları çıktıda görüntülendiği gibi **show lldp neighbors** komutu kullanılarak keşfedilebilir .

```
S1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
Device ID           Local Intf     Hold-time  Capability      Port ID
R1                  Fa0/5          117        R               Gi0/0/1
S2                  Fa0/1          112        B               Fa0/1
Total entries displayed: 2
```

Ağ yöneticisi, S1'in komşu olarak bir yönlendiriciye ve bir anahtara sahip olduğunu keşfeder. Bu çıktı için, köprü için B harfi aynı zamanda anahtar anlamına gelir.

**show lldp neighbors** sonuçlarından, şekilde gösterildiği gibi S1'den bir topoloji oluşturulabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Komşular hakkında daha fazla ayrıntıya ihtiyaç duyulduğunda, **show lldp neighbors detail** komutu komşu IOS sürümü, IP adresi ve cihaz kapasitesi gibi bilgiler sağlayabilir.

```
S1# show lldp neighbors detail
------------------------------------------------
Chassis id: 848a.8d44.49b0
Port id: Gi0/0/1
Port Description: GigabitEthernet0/0/1
System Name: R1

System Description:
Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.9.4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre

Time remaining: 111 seconds
System Capabilities: B,R
Enabled Capabilities: R
Management Addresses - not advertised
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: - not advertised

------------------------------------------------
Chassis id: 0025.83e6.4b00
Port id: Fa0/1
Port Description: FastEthernet0/1
System Name: S2

System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE4, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2013 by Cisco Systems, Inc.
Compiled Wed 26-Jun-13 02:49 by prod_rel_team

Time remaining: 107 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses - not advertised
Auto Negotiation - supported, enabled
Physical media capabilities:
    100base-TX(FD)
    100base-TX(HD)
    10base-T(FD)
    10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: 1

Total entries displayed: 2
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 39.3.NTP (Network Time Protocol)

### 39.3.1.Zaman ve Takvim Hizmetleri

Ağ yönetimini gerçekten derinlemesine incelemeden önce, yolunuza devam etmenize yardımcı olacak tek şey, tüm bileşenlerinizin aynı saat ve tarihe ayarlandığından emin olmaktır.

Bir yönlendirici veya anahtardaki yazılım saati, sistem önyüklendiğinde başlar. Sistem için birincil zaman kaynağıdır. Ağdaki tüm cihazlarda zamanı senkronize etmek önemlidir, çünkü ağları yönetmenin, korumanın, sorun gidermenin ve planlamanın tüm yönleri doğru zaman damgası gerektirir. Cihazlar arasında zaman senkronize olmadığında, olayların sırasını ve bir olayın nedenini belirlemek imkansız olacaktır.

Tipik olarak, bir yönlendirici veya anahtardaki tarih ve saat ayarları iki yöntemden biri kullanılarak yapılabilir Örnekte gösterildiği gibi tarih ve saati manuel olarak yapılandırabilir veya Ağ Zaman Protokolünü (NTP) yapılandırabilirsiniz.

```
R1# clock set 16:01:00 sept 25 2020
*Sep 25 16:01:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 13:09:49 UTC Fri Sep 25
2020 to 16:01:00 UTC Fri Sep 25 2020, configured from console by console.
Sep 25 16:01:00.001: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been set.
R1#
```

Bir ağ büyüdükçe, tüm altyapı cihazlarının senkronize zamanla çalışmasını sağlamak zorlaşır. Daha küçük bir ağ ortamında bile, manuel yöntem ideal değildir. Bir yönlendirici yeniden başlatılırsa, nasıl doğru bir tarih ve zaman damgası alır?

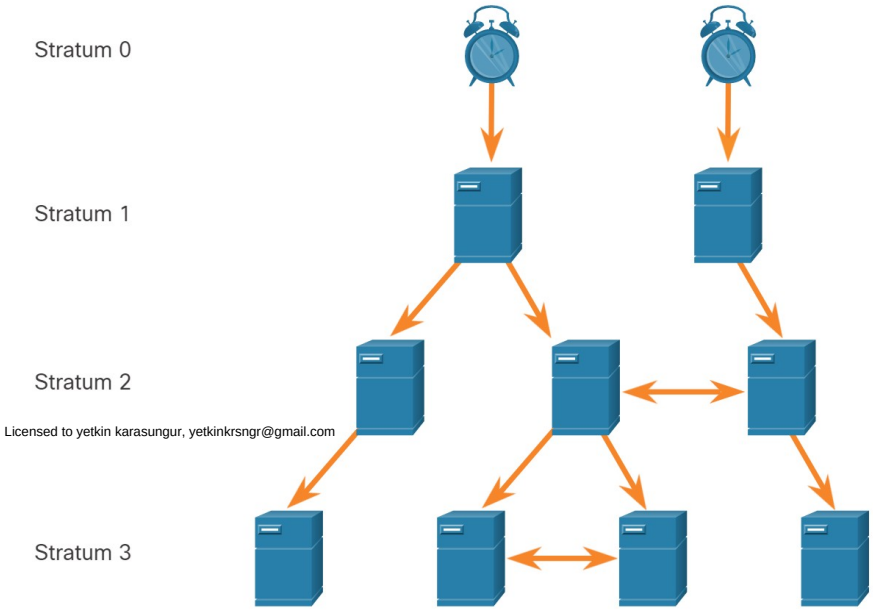
Ağda NTP'yi yapılandırmak daha iyi bir çözümdür. Bu protokol, ağdaki yönlendiricilerin zaman ayarlarını bir NTP sunucusuyla senkronize etmesine izin verir. Tek bir kaynaktan saat ve tarih bilgileri alan bir grup NTP istemcisi, daha tutarlı zaman ayarlarına sahiptir. Ağda NTP uygulandığında, özel bir ana saate senkronize olacak şekilde ayarlanabilir veya internette halka açık bir NTP sunucusuna senkronize edilebilir.

NTP, UDP bağlantı noktası 123'ü kullanır ve RFC 1305'te belgelenmiştir.

### 39.3.2.NTP Nasıl Çalışır?

NTP ağları, hiyerarşik bir zaman kaynakları sistemi kullanır. Bu hiyerarşik sistemdeki her seviyeye katman denir. Katman seviyesi, yetkili kaynaktan gelen atlama sayısı sayısı olarak tanımlanır. Senkronize zaman, NTP kullanılarak ağa dağıtılır. Şekilde örnek bir NTP ağı gösterilmektedir.

NTP sunucuları, üç tabakayı(Stratum) gösteren üç seviyede düzenlenmiştir. Tabaka- 1, Tabaka 0 saatlerine bağlıdır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tabaka 0

Bir NTP ağı, zamanı yetkili zaman kaynaklarından alır. Atomik ve GPS saatleri gibi Stratum 0 cihazları, en doğru yetkili zaman kaynaklarıdır. Spesifik olarak, katman 0 cihazları, doğru olduğu ve bunlarla ilişkili çok az veya hiç gecikme olmadığı varsayılan ağ dışı yüksek hassasiyetli zaman tutma cihazlarıdır. Şekilde, saat simgesiyle temsil edilirler.

Tabaka 1

Katman 1 cihazları, yetkili zaman kaynaklarına doğrudan bağlı ağ cihazlarıdır. NTP kullanan katman 2 cihazları için birincil ağ zaman standardı olarak işlev görürler.

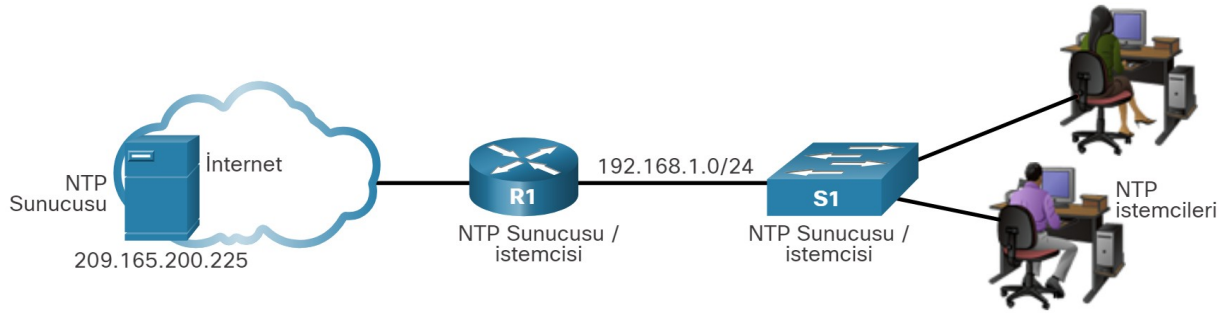
Tabaka 2 ve Altı

Katman 2 sunucular, ağ bağlantıları aracılığıyla katman 1 cihazlara bağlanır. NTP istemcileri gibi Stratum 2 cihazları, katman 1 sunucularından NTP paketlerini kullanarak zamanlarını senkronize eder. Ayrıca katman 3 cihazları için sunucu görevi görebilirler.

Daha küçük katman numaraları, sunucunun yetkili zaman kaynağına daha büyük katman sayılarından daha yakın olduğunu gösterir. Tabaka sayısı ne kadar büyükse, tabaka seviyesi o kadar düşüktür. En yüksek sekme sayısı 15'tir. En düşük tabaka seviyesi olan Tabaka 16, bir cihazın senkronize olmadığını gösterir. Aynı katman düzeyindeki zaman sunucuları, yedekleme veya zaman doğrulaması için aynı katman düzeyindeki diğer zaman sunucuları ile eş olarak hareket edecek şekilde yapılandırılabilir.

## 39.3.3.NTP'yi Yapılandırma ve Doğrulama

Şekil, NTP yapılandırmasını ve doğrulamasını göstermek için kullanılan topolojiyi göstermektedir.




NTP ağda yapılandırılmadan önce, **show clock** komutu, örnekte gösterildiği gibi yazılım saatindeki geçerli saati görüntüler. **Detail** seçeneğiyle, zaman kaynağının kullanıcı yapılandırması olduğuna dikkat edin. Bu, saatin clock komutuyla manuel olarak yapılandırıldığı anlamına gelir.

```
R1# show clock detail
20:55:10.207 UTC Fri Nov 15 2019
Time source is user configuration
```

**Ntp server** *ip address* komutu R1 için NTP sunucusu olarak yapılandırmak 209.165.200.225 için global konfigürasyon modunda verilir. Zaman kaynağının NTP olarak ayarlandığını doğrulamak için **show clock detail** komutunu kullanın. Şimdi zaman kaynağının NTP olduğuna dikkat edin.

```
R1(config)# ntp server 209.165.200.225
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Nov 15 2019
Time source is NTP
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Sonraki örnekte, **show ntp associations** ve **show ntp status** komutları, R1'in 209.165.200.225'te NTP sunucusuyla senkronize edildiğini doğrulamak için kullanılır. R1'in 209.165.200.225'te bir katman 1 NTP sunucusuyla senkronize edildiğine ve GPS saatiyle senkronize edildiğine dikkat edin. **show ntp status** komutu R1 şimdi 209.165.220.225 de NTP sunucusu ile senkronize olan bir tabaka 2 cihaz olduğunu gösterir.

```
R1# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~209.165.200.225 .GPS.           1     61     64   377  0.481   7.480  4.261
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Fri Nov 15 2019)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803 s/s
system poll interval is 64, last update was 169 sec ago.
```

Daha sonra, S1'deki saat, **ntp server** komutuyla R1'e senkronize olacak şekilde yapılandırılır ve ardından yapılandırma, görüntülendiği gibi **show ntp associations** komutuyla doğrulanır .

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
  address         ref clock       st   when   poll reach  delay  offset   disp
*~192.168.1.1     209.165.200.225  2     12     64   377  1.066  13.616  3.840
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured
```

**show ntp associations** komutunun çıkışı, S1'deki saatin artık NTP aracılığıyla 192.168.1.1'de R1 ile senkronize edildiğini doğrular. R1 bir tabaka 2 cihazı ve S1'e NTP sunucusudur. Artık S1, uç cihazlar gibi ağdaki diğer cihazlara NTP hizmeti sağlayabilen bir tabaka 3 cihazıdır.

```
S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Nov 15 2019)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925 s/s
system poll interval is 128, last update was 178 sec ago.
```

## 39.4.SNMP

### 39.4.1.SNMP'ye Giriş

SNMP (Simple Network Management Protocol), yöneticilerin bir IP ağı üzerindeki sunucular, iş istasyonları, yönlendiriciler, anahtarlar ve güvenlik araçları gibi düğümleri yönetmesine izin vermek için geliştirilmiştir. Ağ yöneticilerinin ağ performansını izlemesini ve yönetmesini, ağ sorunlarını bulup çözmesini ve ağ büyümesini planlamasını sağlar.

SNMP, yöneticiler ve aracılar arasındaki iletişim için bir mesaj formatı sağlayan bir uygulama katmanı protokolüdür. SNMP sistemi üç unsurdan oluşur:

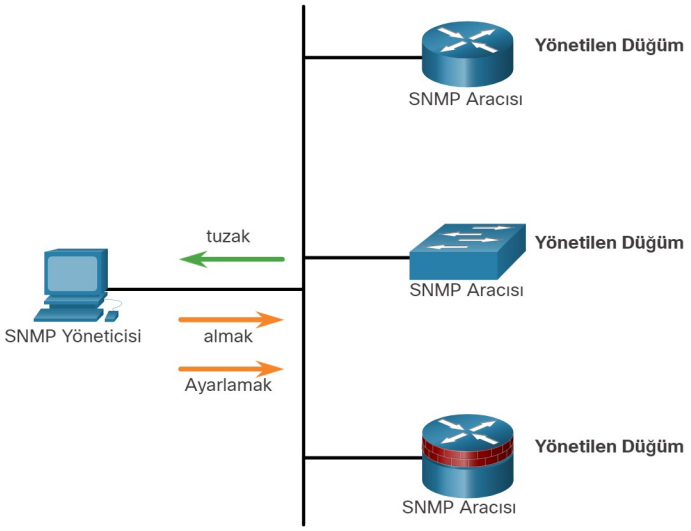
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

- SNMP yöneticisi (SNMP manager)
- SNMP aracıları (yönetilen düğüm) (SNMP agents (managed node))

- Yönetim Bilgi Tabanı (MIB) (Management Information Base)

SNMP'yi bir ağ aygıtında yapılandırmak için, önce yönetici ile aracı arasındaki ilişkiyi tanımlamak gerekir.

SNMP yöneticisi, bir ağ yönetim sisteminin-network management system (NMS) bir parçasıdır. SNMP yöneticisi, SNMP yönetim yazılımını çalıştırır. Şekilde gösterildiği gibi, SNMP yöneticisi "alma-get" eylemini kullanarak bir SNMP aracısından bilgi toplayabilir ve "ayarla-set" eylemini kullanarak bir aracıdaki yapılandırmaları değiştirebilir. Ek olarak, SNMP aracıları, "tuzakları-trap" kullanarak bilgileri doğrudan bir ağ yöneticisine iletebilir.




SNMP aracısı ve MIB, SNMP istemci cihazlarında bulunur. Anahtarlar, yönlendiriciler, sunucular, güvenlik duvarları ve iş istasyonları gibi yönetilmesi gereken ağ cihazları bir SNMP aracı yazılım modülüyle donatılmıştır. MIB'ler, cihaz ve operasyonel istatistikler hakkındaki verileri depolar ve kimliği doğrulanmış uzak kullanıcılar tarafından kullanılabilir olması amaçlanmıştır. SNMP aracısı, yerel MIB'ye erişim sağlamaktan sorumludur.

SNMP, ağ yönetimi uygulamaları ve yönetim aracıları arasında yönetim bilgilerinin nasıl değiş tokuş edildiğini tanımlar. SNMP yöneticisi, aracıları yoklar ve UDP bağlantı noktası 161'deki SNMP aracıları için MIB'yi sorgular. SNMP aracıları, her türlü SNMP tuzağını UDP bağlantı noktası 162 üzerindeki SNMP yöneticisine gönderir.

## 39.4.2.SNMP'nin Çalışması

Yönetilen cihazlarda bulunan SNMP aracıları, cihaz ve çalışması hakkında bilgi toplar ve depolar. Bu bilgiler, aracı tarafından MIB'de yerel olarak saklanır. SNMP yöneticisi daha sonra MIB içindeki bilgilere erişmek için SNMP aracısını kullanır.
İki birincil SNMP yöneticisi isteği vardır, alma ve ayarlama. Cihazı veri için sorgulamak için NMS tarafından bir alma isteği kullanılır. Aracı cihazdaki konfigürasyon değişkenlerini değiştirmek için NMS tarafından bir ayar talebi kullanılır. Bir set isteği, bir cihaz içindeki eylemleri de başlatabilir. Örneğin, bir küme yönlendiricinin yeniden başlamasına, bir yapılandırma dosyası göndermesine veya bir yapılandırma dosyası almasına neden olabilir. SNMP yöneticisi, tabloda açıklanan işlemleri gerçekleştirmek için alma ve ayarlama eylemlerini kullanır.

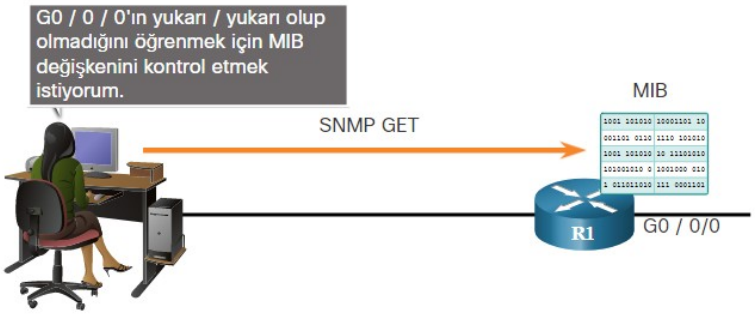
| Operasyon | Açıklama |
|---|---|
| get-request | Belirli bir değişkenden bir değer alır. |
| get-next-request | Bir tablodaki değişkenden bir değer alır; SNMP yöneticisinin değişken adını tam olarak bilmesine gerek yoktur. Bir tablo içinden gerekli değişkeni bulmak için sıralı bir arama yapılır. |
| get-bulk-request | Bir tablodaki birden çok satır gibi, aksi takdirde birçok küçük veri bloğunun iletimini gerektiren büyük veri bloklarını alır. (Yalnızca SNMPv2 veya üstü ile çalışır.) |
| get-response | Bir NMS tarafından gönderilen bir get-request, get-next-isteği ve set-isteğine yanıt verir. |
| set-request | Belirli bir değişkende bir değer depolar. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

SNMP aracısı, SNMP yöneticisi isteklerine aşağıdaki şekilde yanıt verir:

- **Bir MIB değişkeni alın** - SNMP aracısı, bu işlevi ağ yöneticisinden bir GetRequest-PDU'ya yanıt olarak gerçekleştirir. Aracı, talep edilen MIB değişkeninin değerini alır ve ağ yöneticisine bu değerle yanıt verir.
- **Bir MIB değişkeni ayarlayın** - SNMP aracısı, bu işlevi ağ yöneticisinden bir SetRequest-PDU'ya yanıt olarak gerçekleştirir. SNMP aracısı, MIB değişkeninin değerini ağ yöneticisi tarafından belirtilen değere değiştirir. Ayarlanan bir isteğe SNMP aracısı yanıtı, cihazdaki yeni ayarları içerir.

Şekil, G0 / 0/0 arayüzünün açık / yukarı olup olmadığını belirlemek için bir SNMP GetRequest kullanımını gösterir.




## 39.4.3.SNMP Ajan Tuzakları (Agent Traps)

Bir NMS, alma isteğini kullanarak yönetilen cihazlarda bulunan SNMP ajanlarını periyodik olarak sorgular. NMS cihazı veri için sorgular. Bu işlemi kullanarak, bir ağ yönetimi uygulaması, trafik yüklerini izlemek ve yönetilen cihazların cihaz yapılandırmalarını doğrulamak için bilgi toplayabilir. Bilgiler, NMS'de bir GUI aracılığıyla görüntülenebilir. Ortalamalar, minimumlar veya maksimumlar hesaplanabilir. Veriler grafikle gösterilebilir veya eşikler, eşikler aşıldığında bir bildirim sürecini tetikleyecek şekilde ayarlanabilir. Örneğin, bir NMS, bir Cisco yönlendiricinin CPU kullanımını izleyebilir. SNMP yöneticisi, değeri periyodik olarak örnekler ve bu bilgileri ağ yöneticisinin bir temel oluştururken, bir rapor oluştururken veya gerçek zamanlı bilgileri görüntülemede kullanması için bir grafikte sunar.

Periyodik SNMP sorgulamasının dezavantajları vardır. İlk olarak, bir olayın meydana geldiği zaman ile bunun NMS tarafından fark edildiği zaman (sorgulama yoluyla) arasında bir gecikme vardır. İkinci olarak, yoklama sıklığı ve bant genişliği kullanımı arasında bir denge vardır.

Bu dezavantajları azaltmak için, SNMP aracılarının NMS'yi belirli olaylardan hemen haberdar etmek için tuzaklar oluşturması ve göndermesi mümkündür. Tuzaklar, SNMP yöneticisini ağdaki bir durum veya olay hakkında uyaran istenmeyen mesajlardır. Tuzak koşullarının örnekleri arasında, bunlarla sınırlı olmamak üzere, uygunsuz kullanıcı kimlik doğrulaması, yeniden başlatmalar, bağlantı durumu (yukarı veya aşağı), MAC adresi izleme, bir TCP bağlantısının kapatılması, bir komşuyla bağlantı kaybı veya diğer önemli olaylar yer alır. Tuzağa yönelik bildirimler, bazı SNMP yoklama isteklerine olan ihtiyacı ortadan kaldırarak ağ ve aracı kaynaklarını azaltır.

Şekil, G0 / 0/0 arayüzünün başarısız olduğu konusunda ağ yöneticisini uyarmak için bir SNMP tuzağının kullanımını göstermektedir. NMS yazılımı ağ yöneticisine bir metin mesajı gönderebilir, NMS yazılımında bir pencere açabilir veya NMS GUI'de yönlendirici simgesini kırmızıya döndürebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 39.4.4.SNMP Sürümleri

SNMP'nin birkaç sürümü vardır:

- SNMPv1 - Bu, RFC 1157'de tanımlanan Tam İnternet Standardı olan Basit Ağ Yönetimi Protokolüdür.
- SNMPv2c - Bu, 1901 ile 1908 arasındaki RFC'lerde tanımlanmıştır. Topluluk dizesi tabanlı bir Yönetim Çerçevesi kullanır.
- SNMPv3 - Bu, orijinal olarak 2273 ila 2275 arasındaki RFC'lerde tanımlanan birlikte çalışabilir standartlara dayalı bir protokoldür. Ağ üzerinden paketleri doğrulayarak ve şifreleyerek cihazlara güvenli erişim sağlar. Şu güvenlik özelliklerini içerir: bir paketin geçiş sırasında tahrif edilmemesini sağlamak için mesaj bütünlüğü, mesajın geçerli bir kaynaktan olduğunu belirlemek için kimlik doğrulama ve bir mesajın içeriğinin yetkisiz bir kaynak tarafından okunmasını önlemek için şifreleme.

Tüm sürümler SNMP yöneticilerini, aracıları ve MIB'leri kullanır. Cisco IOS yazılımı yukarıdaki üç sürümü desteklemektedir. Sürüm 1 eski bir çözümdür ve günümüzde ağlarda pek rastlanmamaktadır; bu nedenle, bu kurs 2c ve 3 sürümlerine odaklanmaktadır.

Hem SNMPv1 hem de SNMPv2c, topluluk tabanlı bir güvenlik biçimi kullanır. Temsilcinin MIB'sine erişebilen yöneticiler topluluğu, bir topluluk dizesiyle (community string.) tanımlanır.

SNMPv1'den farklı olarak, SNMPv2c bir toplu geri alma mekanizması ve yönetim istasyonlarına daha ayrıntılı hata mesajı raporlama içerir. Toplu erişim mekanizması, gerekli gidiş dönüş sayısını en aza indirerek tabloları ve büyük miktarda bilgiyi alır. SNMPv2c iyileştirilmiş hata işleme, farklı türdeki hata durumlarını ayırt eden genişletilmiş hata kodlarını içerir. Bu koşullar SNMPv1'de tek bir hata kodu ile rapor edilir. SNMPv2c'deki hata dönüş kodları, hata türünü içerir.

Not : SNMPv1 ve SNMPv2c, minimum güvenlik özellikleri sunar. Özellikle, SNMPv1 ve SNMPv2c, bir yönetim mesajının kaynağını doğrulayamaz veya şifreleme sağlayamaz. SNMPv3 en güncel olarak RFC 3410 ila 3415'te açıklanmaktadır. Yönetilen cihazlar arasında kritik verilerin güvenli aktarımını sağlamak için yöntemler ekler.

SNMPv3, hem güvenlik modelleri hem de güvenlik seviyeleri sağlar. Bir güvenlik modeli, bir kullanıcı ve kullanıcının içinde bulunduğu grup için kurulan bir kimlik doğrulama stratejisidir. Güvenlik seviyesi, bir güvenlik modeli içinde izin verilen güvenlik seviyesidir. Güvenlik seviyesi ve güvenlik modelinin bir kombinasyonu, bir SNMP paketini işlerken hangi güvenlik mekanizmasının kullanılacağını belirler. Mevcut güvenlik modelleri SNMPv1, SNMPv2c ve SNMPv3'tür.

Tablo, farklı güvenlik modelleri ve düzeyleri kombinasyonlarının özelliklerini tanımlar.

| **SNMPv1** | |
|---|---|
| **Seviye** | noAuthNoPriv |
| **Doğrulama** | Topluluk dizesi |
| **Şifreleme** | Hayır |
| **Sonuç** | Kimlik doğrulama için bir topluluk dizesi eşleşmesi kullanır. |

| **SNMPv2c** | |
|---|---|
| **Seviye** | noAuthNoPriv |
| **Doğrulama** | Topluluk dizesi |
| **Şifreleme** | Hayır |
| **Sonuç** | Kimlik doğrulama için bir topluluk dizesi eşleşmesi kullanır. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| SNMPv3 noAuthNoPriv | |
|---|---|
| **Seviye** | noAuthNoPriv |
| **Doğrulama** | Kullanıcı adı |
| **Şifreleme** | Hayır |
| **Sonuç** | Kimlik doğrulama için bir kullanıcı adı eşleşmesi kullanır (SNMPv2c'ye göre bir iyileştirme). |

| SNMPv3 authNoPriv | |
|---|---|
| **Seviye** | authNoPriv |
| **Doğrulama** | Mesaj Özeti 5 (MD5) veya Güvenli Karma Algoritma (SHA) |
| **Şifreleme** | Hayır |
| **Sonuç** | HMAC-MD5 veya HMAC-SHA algoritmalarına dayalı kimlik doğrulama sağlar. |

| SNMPv3 authPriv | |
|---|---|
| **Seviye** | authPriv (kriptografik yazılım görüntüsünü gerektirir) |
| **Doğrulama** | MD5 veya SHA |
| **Şifreleme** | Veri Şifreleme Standardı (DES) veya Gelişmiş Şifreleme Standardı (AES) |
| **Sonuç** | HMAC-MD5 veya HMAC-SHA algoritmalarına dayalı kimlik doğrulama sağlar. Şu şifreleme algoritmalarıyla Kullanıcı Tabanlı Güvenlik Modelini (USM) belirlemeye izin verir:<br>• CBC-DES (DES-56) standardına dayalı kimlik doğrulamaya ek olarak DES 56-bit şifreleme<br>• 3DES 168 bit şifreleme<br>• AES 128-bit, 192-bit veya 256-bit şifreleme |

Bir ağ yöneticisi, yönetim istasyonu tarafından desteklenen SNMP sürümünü kullanmak için SNMP aracısını yapılandırmalıdır. Bir aracı birden fazla SNMP yöneticisi ile iletişim kurabildiğinden, yazılımı SNMPv1, SNMPv2c veya SNMPv3 kullanarak iletişimi destekleyecek şekilde yapılandırmak mümkündür.

## 39.4.5.Topluluk Dizeleri (Community Strings)

SNMP'nin çalışması için, NMS'nin MIB'ye erişimi olmalıdır. Erişim isteklerinin geçerli olduğundan emin olmak için bir tür kimlik doğrulama mevcut olmalıdır.

SNMPv1 ve SNMPv2c, MIB'ye erişimi kontrol eden topluluk dizelerini kullanır. Topluluk dizeleri düz metin parolalardır. SNMP topluluk dizeleri, MIB nesnelerine erişimi doğrular.

İki tür topluluk dizesi vardır:

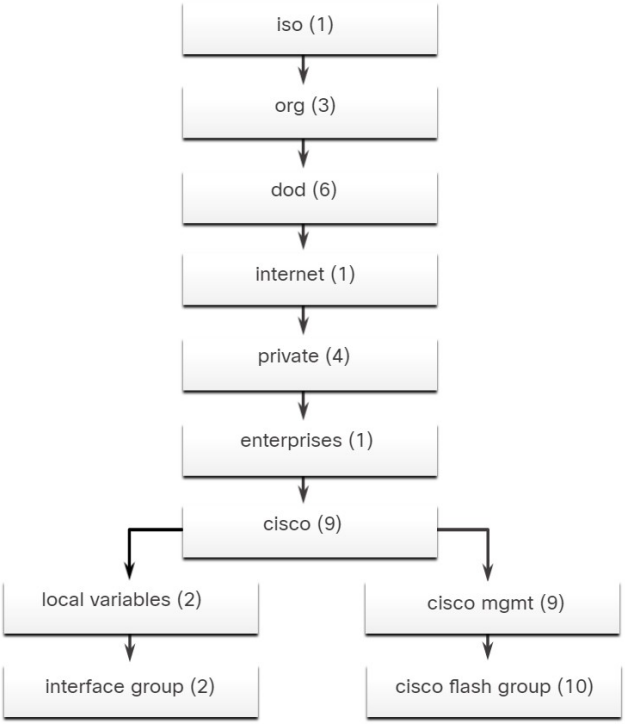
- Salt okunur-Read-only (ro) - Bu tür, MIB değişkenlerine erişim sağlar, ancak bu değişkenlerin değiştirilmesine izin vermez, yalnızca okunur. Sürüm 2c'de güvenlik minimum olduğundan, birçok kuruluş SNMPv2c'yi salt okunur modda kullanır.
- Okuma-yazma- Read-write (rw) - Bu tür, MIB'deki tüm nesnelere okuma ve yazma erişimi sağlar.

  MIB değişkenlerini görüntülemek veya ayarlamak için, kullanıcının okuma veya yazma erişimi için uygun topluluk dizesini belirtmesi gerekir.

Licensed to yetkin karasungur, yetkinksngr@gmail.com

## 39.4.6.MIB Nesne Kimliği (MIB Object ID)

MIB, değişkenleri hiyerarşik olarak düzenler. MIB değişkenleri, yönetim yazılımının ağ cihazını izlemesini ve kontrol etmesini sağlar. Resmi olarak, MIB her değişkeni bir nesne kimliği (OID) olarak tanımlar. OID'ler, MIB hiyerarşisindeki yönetilen nesneleri benzersiz şekilde tanımlar. MIB, OID'leri RFC standartlarına dayalı olarak, genellikle bir ağaç olarak gösterilen bir OID hiyerarşisi halinde düzenler.

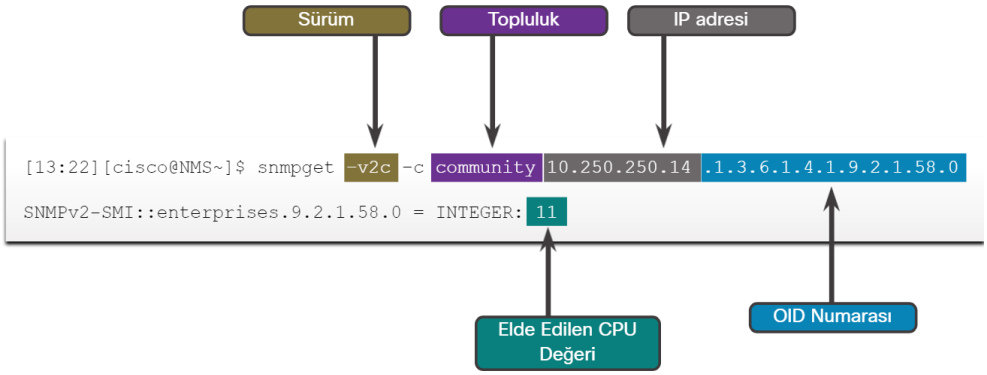



Herhangi bir cihaz için MIB ağacı, birçok ağ cihazında ortak olan değişkenlere sahip bazı dalları ve bu cihaza veya satıcıya özgü değişkenlere sahip bazı dalları içerir.

RFC'ler bazı ortak değişkenleri tanımlar. Çoğu cihaz bu MIB değişkenlerini uygular. Ek olarak, Cisco gibi ağ donanımı satıcıları, cihazlarına özgü yeni değişkenleri barındırmak için ağacın kendi özel dallarını tanımlayabilir.

Şekil, MIB yapısının Cisco tarafından tanımlanan kısımlarını göstermektedir. Ağaçta belirli bir değişkeni bulmaya yardımcı olmak için OID'nin kelimeler veya sayılarla nasıl tanımlanabileceğine dikkat edin. Cisco'ya ait OID'ler şu şekilde numaralandırılır: .iso (1) .org (3) .dod (6) .internet (1) .private (4) .enterprises (1) .cisco (9). Bu nedenle OID 1.3.6.1.4.1.9'dur.

Veriler, NMS'de yayınlanan snmpget yardımcı programı aracılığıyla alınır. Snmpget yardımcı programını kullanarak gerçek zamanlı verileri manuel olarak alabilir veya NMS'nin bir rapor çalıştırmasını sağlayabilirsiniz. Bu rapor, ortalamayı elde etmek için verileri kullanabileceğiniz bir süre verir. Snmpget yardımcı programı, SNMP sürümünün, doğru topluluğun, sorgulanacak ağ aygıtının IP adresinin ve OID numarasının ayarlanmasını gerektirir. Şekil, MIB'den bilgilerin hızlı bir şekilde alınmasını sağlayan ücretsiz snmpget yardımcı programının kullanımını göstermektedir.




Snmpget yardımcı program komutunun birkaç parametresi vardır:

- - v2c - Bu, SNMP'nin sürümüdür.
- - c topluluğu - Bu, topluluk dizesi adı verilen SNMP parolasıdır.
- 10.250.250.14 - Bu, izlenen cihazın IP adresidir.
- 1.3.6.1.4.1.9.2.1.58.0 - Bu, MIB değişkeninin OID'sidir.

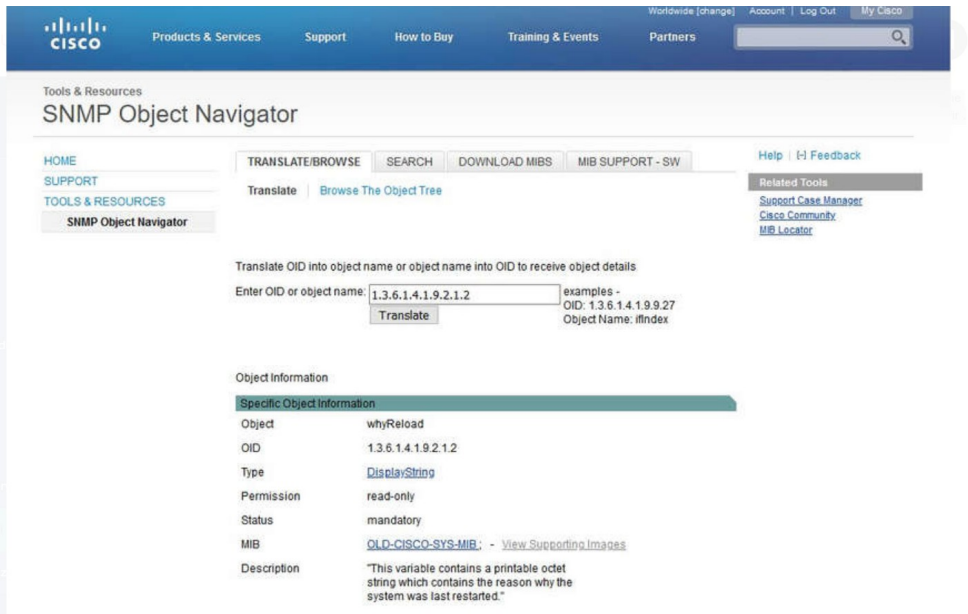
Son satır yanıtı gösterir. Çıktı, MIB değişkeninin kısaltılmış bir versiyonunu gösterir. Daha sonra MIB konumundaki gerçek değeri listeler. Bu durumda, CPU meşgul yüzdesinin 5 dakikalık hareketli ortalaması yüzde 11'dir.

## 39.4.7.SNMP Nesne Gezgini (SNMP Object Navigator)

Snmpget yardımcı programı, SNMP'nin nasıl çalıştığına dair temel mekanikler hakkında fikir verir. Bununla birlikte, 1.3.6.1.4.1.9.2.1.58.0 gibi uzun MIB değişken isimleriyle çalışmak, ortalama bir kullanıcı için sorunlu olabilir. Daha yaygın olarak, ağ operasyonları personeli, tüm MIB veri değişken isimlendirmesini kullanıcı için şeffaf hale getiren, kullanımı kolay bir GUI'ye sahip bir ağ yönetimi ürünü kullanır.

Licensed to yetkinkaraburgur, yetkinkrsngr@gmail.com

Bir ağ yöneticisinin belirli bir OID hakkında ayrıntıları araştırmasına olanak tanıyan Cisco aracını bulmak için "Cisco SNMP Nesne Gezgini aracı" nı arayın. Şekil, whyReload nesnesine ilişkin OID bilgilerini araştırmak için gezginin kullanımına bir örnek gösterir .



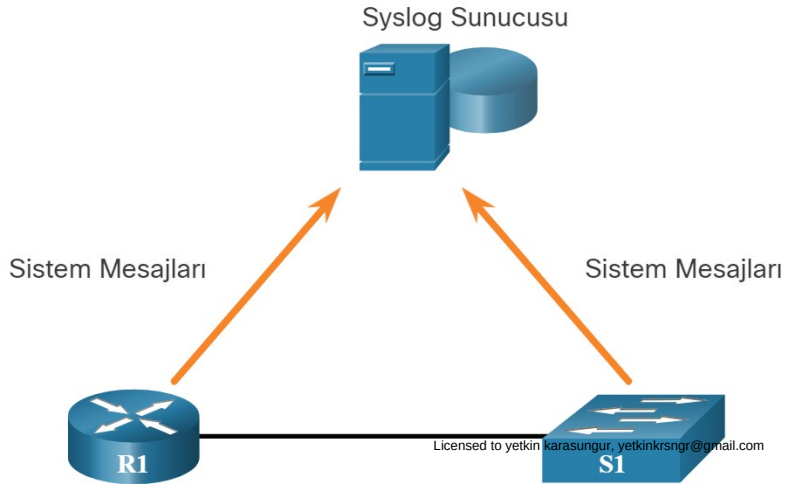

## 39.5.Sistem Günlüğü (Syslog)

### 39.5.1.Syslog'a Giriş

Sistem günlüğü protokolü, bu mesajları almanızı ve anlamanızı sağlamak için tasarlanmıştır. Bir ağda belirli olaylar meydana geldiğinde, ağ aygıtları, yöneticiyi ayrıntılı sistem mesajlarıyla bilgilendirmek için güvenilir mekanizmalara sahiptir. Bu mesajlar kritik olmayabilir veya önemli olabilir. Ağ yöneticilerinin bu mesajları saklamak, yorumlamak ve görüntülemek için çeşitli seçenekleri vardır. Ağ altyapısı üzerinde en büyük etkiye sahip olabilecek mesajlar konusunda da uyarılabilirler.

Sistem mesajlarına erişmenin en yaygın yöntemi syslog adı verilen bir protokol kullanmaktır.

Syslog, bir standardı tanımlamak için kullanılan bir terimdir. Ayrıca o standart için geliştirilen protokolü açıklamak için de kullanılır. Sistem günlüğü protokolü, 1980'lerde UNIX sistemleri için geliştirilmiştir, ancak ilk olarak 2001'de IETF tarafından RFC 3164 olarak belgelenmiştir. Syslog, şekilde gösterildiği gibi, IP ağları üzerinden olay mesajı toplayıcılarına olay bildirim mesajları göndermek için UDP bağlantı noktası 514'ü kullanır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yönlendiriciler, anahtarlar, uygulama sunucuları, güvenlik duvarları ve diğer ağ cihazları dahil olmak üzere birçok ağ cihazı syslog'u destekler. Syslog protokolü, ağ cihazlarının sistem mesajlarını ağ üzerinden syslog sunucularına göndermesine izin verir.

Windows ve UNIX için birkaç farklı syslog sunucusu yazılım paketi vardır. Birçoğu ücretsiz yazılımdır.

Syslog günlük kaydı hizmeti, aşağıdaki gibi üç temel işlev sağlar:

- İzleme ve sorun giderme için günlük bilgilerini toplama yeteneği
- Yakalanan günlük bilgilerinin türünü seçme yeteneği
- Yakalanan syslog mesajlarının hedeflerini belirleme yeteneği

## 39.5.2.Sistem Günlüğü İşlemi

Cisco ağ cihazlarında, syslog protokolü , cihaza dahil olan yerel bir günlük işlemine sistem mesajları ve hata ayıklama çıktısı göndererek başlar . Günlüğe kaydetme sürecinin bu mesajları ve çıktıları nasıl yönettiği, cihaz yapılandırmalarına bağlıdır. Örneğin, syslog mesajları ağ üzerinden harici bir syslog sunucusuna gönderilebilir. Bu mesajlar, gerçek cihaza erişmeye gerek kalmadan alınabilir. Harici sunucuda depolanan günlük mesajları ve çıktılar, daha kolay okunması için çeşitli raporlara çekilebilir.

Alternatif olarak, syslog mesajları bir dahili tampona gönderilebilir. Dahili arabelleğe gönderilen mesajlar yalnızca cihazın CLI'sinden görüntülenebilir.

Son olarak, ağ yöneticisi yalnızca belirli türdeki sistem mesajlarının çeşitli hedeflere gönderilmesini belirtebilir. Örneğin cihaz, tüm sistem mesajlarını harici bir syslog sunucusuna iletecek şekilde yapılandırılabilir. Bununla birlikte, hata ayıklama düzeyindeki mesajlar dahili arabelleğe iletilir ve yalnızca yönetici tarafından CLI'den erişilebilir.

Şekilde gösterildiği gibi, syslog mesajları için popüler hedefler şunları içerir:

- Günlük tamponu-Logging buffer (bir yönlendirici veya anahtar içindeki RAM)
- Konsol hattı
- Terminal hattı
- Syslog sunucusu

## 39.5.3.Sistem Günlüğü Mesaj Biçimi

Cisco cihazları, ağ olaylarının bir sonucu olarak syslog mesajları üretir. Her sistem günlüğü mesajı bir önem seviyesi ( severity level ) ve bir tesis (facility) içerir.

Daha küçük sayısal seviyeler, daha kritik syslog alarmlarıdır. Mesajların önem seviyesi, her mesaj tipinin nerede görüntülendiğini kontrol edecek şekilde ayarlanabilir (yani konsolda veya diğer hedeflerde). Sistem günlüğü düzeylerinin tam listesi tabloda gösterilmektedir.

| Önem Adı | Önem Düzeyi | Açıklama |
|---|---|---|
| Acil Durum-Emergency | Seviye 0 | Sistem Kullanılamaz |
| Alarm-Alert | Seviye 1 | Acil İşlem Gerekiyor |
| Kritik-Critical | Seviye 2 | Kritik durum |
| Hata-Error | Seviye 3 | Hata Durumu |
| Uyarı-Warning | Seviye 4 | Uyarı Durumu |
| Bildirim-Notification | Seviye 5 | Normal, ancak Önemli Durum |
| Bilgilendirici-Informational | Seviye 6 | Bilgilendirme Mesajı |
| Hata ayıklama-Debugging | Seviye 7 | Hata Ayıklama Mesajı |

Licensed to [illegible]

Her sistem günlüğü düzeyinin kendi anlamı vardır:

- Uyarı Düzeyi 4 - Acil Durum Düzeyi 0 : Bu mesajlar, yazılım veya donanım arızalarıyla ilgili hata mesajlarıdır; bu tür mesajlar, cihazın işlevselliğinin etkilendiği anlamına gelir. Sorunun ciddiyeti, uygulanan gerçek syslog düzeyini belirler.
- Bildirim Düzeyi 5 : Bu bildirim düzeyi, normal ancak önemli olaylar içindir. Örneğin, arayüz yukarı veya aşağı geçişleri ve sistem yeniden başlatma mesajları, bildirim düzeyinde görüntülenir.
- Bilgi Düzeyi 6 : Bu, aygıt işlevselliğini etkilemeyen normal bir bilgi mesajıdır. Örneğin, bir Cisco cihazı önyüklenirken, aşağıdaki bilgi mesajını görebilirsiniz:% LICENSE-6-EULA _ ACCEPT _ ALL: Son Kullanıcı Lisans Sözleşmesi Kullanım Hakkı kabul edildi.
- Hata Ayıklama Seviyesi 7 : Bu seviye, mesajların çeşitli hata ayıklama-debug komutlarının verilmesinden üretildiğini gösterir .

## 39.5.4.Sistem Günlüğü Tesisleri

Önem düzeyini belirlemeye ek olarak, syslog iletileri tesisle ilgili bilgileri de içerir. Syslog tesisleri, hata ve olay mesajı raporlaması için sistem durumu verilerini tanımlayan ve kategorilere ayıran hizmet tanımlayıcılardır. Mevcut olan günlük kaydı olanağı seçenekleri ağ cihazına özeldir. Örneğin, Cisco IOS Sürüm 15.0 (2) çalıştıran Cisco 2960 Serisi anahtarlar ve Cisco IOS Sürüm 15.2 (4) çalıştıran Cisco 1941 yönlendiricileri, 12 tesis türüne ayrılan 24 tesis seçeneğini destekler.

Cisco IOS yönlendiricilerinde bildirilen bazı yaygın syslog mesaj tesisi kodları şunları içerir:

- IF - Sistem günlüğü mesajının bir arabirim tarafından oluşturulduğunu tanımlar.
- IP - Sistem günlüğü mesajının IP tarafından oluşturulduğunu belirtir.
- OSPF - Sistem günlüğü mesajının OSPF yönlendirme protokolü tarafından oluşturulduğunu tanımlar.
- SYS - Sistem günlüğü mesajının aygıt işletim sistemi tarafından oluşturulduğunu belirtir.
- IPSEC - syslog mesajının IP Güvenliği şifreleme protokolü tarafından oluşturulduğunu belirtir.

Varsayılan olarak, Cisco IOS Yazılımındaki syslog mesajlarının biçimi aşağıdaki gibidir:

```
%facility-severity-MNEMONIC: description
```

Örneğin, EtherChannel bağlantı durumunu yukarı değiştiren bir Cisco anahtarındaki örnek çıktı:

```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Burada tesis LINK'dir ve önem seviyesi 3'tür, MNEMONIC ise UPDOWN

En yaygın mesajlar, bağlantı yukarı ve aşağı mesajları ve bir cihazın yapılandırma modundan çıktığında ürettiği mesajlardır. ACL günlüğü yapılandırılırsa, paketler bir parametre koşuluyla eşleştiğinde cihaz syslog mesajları oluşturur.

## 39.5.5.Sistem Günlüğü Zaman Damgasını Yapılandırma

Varsayılan olarak, günlük mesajları zaman damgalı değildir. Örnekte, R1 GigabitEthernet 0/0/0 arayüzü kapatılmıştır. Konsola kaydedilen mesaj, arayüz durumunun ne zaman değiştirildiğini tanımlamaz. Günlük mesajları, bir Syslog sunucusu gibi başka bir hedefe gönderildiklerinde mesajın ne zaman oluşturulduğuna dair bir kayıt olacak şekilde zaman damgalı olmalıdır.

Günlüğe kaydedilen olayları tarih ve saati görüntülemeye zorlamak için komut hizmeti zaman damgalarını günlüğü tarih saatini kullanın. Komut çıktısında gösterildiği gibi, R1 GigabitEthernet 0/0/0 arayüzü yeniden etkinleştirildiğinde, günlük mesajları artık tarih ve saati içerir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*Mar  1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Mar  1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Mar  1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

Not : datetime anahtar sözcüğünü kullanırken, ağ aygıtındaki saat daha önce anlatıldığı gibi manuel olarak veya NTP aracılığıyla ayarlanmalıdır.

## 39.6.Yönlendirici ve Anahtar Dosya Bakımı

### 39.6.1.Yönlendirici Dosya Sistemi

Cisco IOS Dosya Sistemi (IFS), yöneticinin farklı dizinlere gitmesine ve dosyaları bir dizinde listelemesine izin verir. Yönetici ayrıca flash bellekte veya bir diskte alt dizinler oluşturabilir. Kullanılabilen dizinler cihaza bağlıdır.

Örnek , bir Cisco 4221 yönlendiricisindeki mevcut tüm dosya sistemlerini listeleyen **show file systems** komutunun çıktısını gösterir .

```
Router# show file systems
File Systems:
       Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
*   7194652672    6294822912      disk     rw   bootflash: flash:
     256589824     256573440      disk     rw   usb0:
    1804468224    1723789312      disk     ro   webui:
             -             -    opaque     rw   null:
             -             -    opaque     ro   tar:
             -             -   network     rw   tftp:
             -             -    opaque     wo   syslog:
      33554432      33539983     nvram     rw   nvram:
             -             -   network     rw   rcp:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -   network     rw   sftp:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
Router#
```

Bu komut, toplam ve boş bellek miktarı, dosya sistemi türü ve izinleri gibi yararlı bilgiler sağlar. İzinler, salt okunur (ro), yalnızca yazma (wo) ve okuma ve yazma (rw) içerir. İzinler, komut çıktısının Bayraklar sütununda gösterilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Listelenen birkaç dosya sistemi olmasına rağmen, bizi ilgilendiren tftp, flash ve nvram dosya sistemleri olacaktır.

Flash dosya sisteminin de önünde bir yıldız işareti olduğuna dikkat edin. Bu, flash'ın geçerli varsayılan dosya sistemi olduğunu gösterir. Önyüklenebilir IOS flash'ta bulunur; bu nedenle, pound simgesi (#) flash listesine eklenir ve bunun önyüklenebilir bir disk olduğunu belirtir.

### Flash Dosya Sistemi

Örnek, dir (dizin) komutunun çıktısını görüntüler .

Flash varsayılan dosya sistemi olduğundan, dir komutu flash içeriğini listeler. Flash'ta birkaç dosya bulunur, ancak özellikle ilgi çekici olan son listedir. Bu, RAM'de çalışan geçerli Cisco IOS dosya görüntüsünün adıdır.

```
Router# dir
Directory of bootflash:/
   11  drwx            16384   Aug 2 2019 04:15:13 +00:00  lost+found
370945  drwx             4096   Oct 3 2019 15:12:10 +00:00  .installer
338689  drwx             4096   Aug 2 2019 04:15:55 +00:00  .ssh
217729  drwx             4096   Aug 2 2019 04:17:59 +00:00  core
379009  drwx             4096  Sep 26 2019 15:54:10 +00:00  .prst_sync
80641  drwx             4096   Aug 2 2019 04:16:09 +00:00  .rollback_timer
161281  drwx             4096   Aug 2 2019 04:16:11 +00:00  gs_script
112897  drwx           102400   Oct 3 2019 15:23:07 +00:00  tracelogs
362881  drwx             4096  Aug 23 2019 17:19:54 +00:00  .dbpersist
298369  drwx             4096   Aug 2 2019 04:16:41 +00:00  virtual-instance
   12  -rw-               30   Oct 3 2019 15:14:11 +00:00  throughput_monitor_params
 8065  drwx             4096   Aug 2 2019 04:17:55 +00:00  onep
   13  -rw-               34   Oct 3 2019 15:19:30 +00:00  pnp-tech-time
249985  drwx             4096  Aug 20 2019 17:40:11 +00:00  Archives
   14  -rw-            65037   Oct 3 2019 15:19:42 +00:00  pnp-tech-discovery-summary
   17  -rw-          5032908  Sep 19 2019 14:16:23 +00:00  isr4200_4300_rommon_1612_1r_SPA.pkg
   18  -rw-        517153193  Sep 21 2019 04:24:04 +00:00  isr4200-universalk9_ias.16.09.04.SPA.bin
7194652672 bytes total (6294822912 bytes free)
Router#
```

### NVRAM Dosya Sistemi

NVRAM içeriğini görüntülemek için , örnekte gösterildiği gibi cd (dizini değiştir) komutunu kullanarak mevcut varsayılan dosya sistemini değiştirmelisiniz.

```
Router#
Router# cd nvram:
Router# pwd
nvram:/
Router# dir
Directory of nvram:/
32769  -rw-             1024                      startup-config
32770  ----               61                      private-config
32771  -rw-             1024                      underlying-config
    1  ----                4                      private-KS1
    2  -rw-             2945                      cwmp_inventory
    5  ----              447                      persistent-data
    6  -rw-             1237                      ISR4221-2x1GE_0_0_0
    8  -rw-               17                      ecfm_ieee_mib
    9  -rw-                0                      ifIndex-table
   10  -rw-             1431                      NIM-2T_0_1_0
   12  -rw-              820                      IOS-Self-Sig#1.cer
   13  -rw-              820                      IOS-Self-Sig#2.cer
33554432 bytes total (33539983 bytes free)
Router#
```

Mevcut çalışma dizinini gösteren komut pwd'dir . Bu komut NVRAM dizinini görüntülediğimizi doğrular. Son olarak, dir komutu NVRAM'in içeriğini listeler. Listelenen birkaç yapılandırma dosyası olmasına rağmen, özellikle ilgi çekici olan başlangıç yapılandırma dosyasıdır.

### Dosya Sistemlerini Değiştirme

Licensed to yetkin karaşungur, yetkinkrsngr@gmail.com

Cisco 2960 anahtar flash dosya sistemi ile, yapılandırma dosyalarını kopyalayabilir ve yazılım görüntülerini arşivleyebilirsiniz (karşıya yükleyebilir ve indirebilirsiniz).

Dosya sistemlerini bir Catalyst anahtarında görüntüleme komutu, Cisco yönlendiricideki ile aynıdır ,örnekte görüntülendiği gibi: **show file systems**

```
Switch# show file systems
File Systems:
       Size(b)     Free(b)      Type  Flags  Prefixes
*    32514048    20887552     flash     rw    flash:
           -           -    opaque     rw       vb:
           -           -    opaque     ro       bs:
           -           -    opaque     rw   system:
           -           -    opaque     rw   tmpsys:
       65536       48897     nvram     rw    nvram:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -    opaque     rw     null:
           -           -    opaque     ro      tar:
           -           -   network     rw     tftp:
           -           -   network     rw      rcp:
           -           -   network     rw     http:
           -           -   network     rw      ftp:
           -           -   network     rw      scp:
           -           -   network     rw    https:
           -           -   opaque      ro      cns:
Switch#
```

## 39.6.2.Yapılandırmayı Yedeklemek ve Geri Yüklemek için TFTP Kullanma

### Bir Yapılandırmayı Yedeklemek için TFTP Kullanın

Yapılandırma dosyalarının kopyaları, bir sorun olması durumunda yedek dosyalar olarak saklanmalıdır. Yapılandırma dosyaları, Önemsiz Dosya Aktarım Protokolü-Trivial File Transfer Protocol (TFTP) sunucusunda veya bir USB sürücüsünde saklanabilir. Ağ belgelerine bir yapılandırma dosyası da dahil edilmelidir.

Çalışan yapılandırmayı veya başlangıç yapılandırmasını bir TFTP sunucusuna kaydetmek için , örnekte gösterildiği gibi **copy running-config tftp** veya **copy startup-config tftp** komutunu kullanın.

```
R1# copy running-config tftp
Remote host []?192.168.10.254
Name of the configuration file to write[R1-config]? R1-Jan-2019
Write file R1-Jan-2019 to 192.168.10.254? [confirm]
Writing R1-Jan-2019 !!!!!! [OK]
```

Çalışan yapılandırmayı bir TFTP sunucusuna yedeklemek için şu adımları izleyin:

1. Adım . **copy running-config tftp** komutunu girin.
2. Adım . Yapılandırma dosyasının saklanacağı ana bilgisayarın IP adresini girin.
3. Adım . Yapılandırma dosyasına atanacak adı girin.
4. adım . Her seçeneği onaylamak için Enter tuşuna basın.

### Bir Yapılandırmayı Geri Yüklemek için TFTP Kullanın

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Çalışan yapılandırmayı veya başlangıç yapılandırmasını bir TFTP sunucusundan geri yüklemek için, **copy tftp running-config** veya **copy tftp startup-config** komutunu kullanın. Çalışan yapılandırmayı bir TFTP sunucusundan geri yüklemek için aşağıdaki adımları kullanın:

1. Adım . **copy tftp running-confi**g komutunu girin.
2. Adım . Yapılandırma dosyasının saklandığı ana bilgisayarın IP adresini girin.
3. Adım . Yapılandırma dosyasına atanacak adı girin.
4. adım . Her seçeneği onaylamak için Enter tuşuna basın .

## 39.6.3.Cisco Yönlendiricideki USB Bağlantı Noktaları

Evrensel Seri Veri Yolu (USB) depolama özelliği, belirli Cisco yönlendirici modellerinin USB flash sürücüleri desteklemesini sağlar. USB flash özelliği, isteğe bağlı bir ikincil depolama özelliği ve ek bir önyükleme aygıtı sağlar. İmageler, yapılandırmalar ve diğer dosyalar, Compact Flash kart kullanılarak dosyaların depolanması ve alınmasıyla aynı güvenilirlikle Cisco USB flash belleğe veya bu bellekten kopyalanabilir. Ek olarak, modüler entegre servis yönlendiricileri, USB flash belleğe kaydedilen herhangi bir Cisco IOS Yazılım görüntüsünü önyükleyebilir. İdeal olarak, USB flash, Cisco IOS'un birden çok kopyasını ve birden çok yönlendirici yapılandırmasını tutabilir. Konsol bağlantıları için kullanılabilen bir USB Tip B mini bağlantı noktası da vardır. Cisco 4321 Router'ın USB portları şekilde gösterilmiştir.

Örnekte gösterildiği gibi USB flash sürücünün içeriğini görüntülemek için **dir** komutunu kullanın .

```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

## 39.6.4.Yapılandırmayı Yedeklemek ve Geri Yüklemek için USB Kullanma

Bir USB bağlantı noktasına yedeklerken, örnekte gösterildiği gibi USB sürücüsünün orada olduğunu doğrulamak ve adı onaylamak için **show file systems** komutunu vermek iyi bir fikirdir .

```
R1# show file systems
File Systems:
                Size(b)       Free(b)      Type  Flags  Prefixes
              -             -    opaque     rw   archive:
              -             -    opaque     rw   system:
              -             -    opaque     rw   tmpsys:
              -             -    opaque     rw   null:
              -             -   network     rw   tftp:
*    256487424     184819712      disk     rw   flash0: flash:#
              -             -      disk     rw   flash1:
        262136        249270     nvram     rw   nvram:
              -             -    opaque     wo   syslog:
              -             -    opaque     rw   xmodem:
              -             -    opaque     rw   ymodem:
              -             -   network     rw   rcp:
              -             -   network     rw   http:
              -             -   network     rw   ftp:
              -             -   network     rw   scp:
              -             -    opaque     ro   tar:
              -             -   network     rw   https:
              -             -    opaque     ro   cns:
    4050042880    3774152704  usbflash     rw   usbflash0:
R1#
```

Licensed to yetkin tanrıöngür yetkinkrsnr@gmail.com

Son çıktı satırının USB bağlantı noktasını ve "usbflash0:" adını gösterdiğine dikkat edin.

Ardından, yapılandırma dosyasını USB flash sürücüye kopyalamak için **copy run usbflash0: /** komutunu kullanın. Dosya sisteminde belirtildiği gibi, flash sürücünün adını kullandığınızdan emin olun. Eğik çizgi isteğe bağlıdır ancak USB flash sürücünün kök dizinini gösterir.

IOS, dosya adını soracaktır. Dosya USB flash sürücüde zaten mevcutsa, yönlendirici, örneklerde gösterildiği gibi üzerine yazmak isteyecektir.

USB flash sürücüye kopyalarken, önceden dosya olmadan aşağıdaki çıktı görüntülenecektir.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
5024 bytes copied in 0.736 secs (6826 bytes/sec)
```

USB flash sürücüye kopyalarken, aynı yapılandırma dosyası zaten sürücüde ile aşağıdaki çıktıyı görüntüleyecektir.

```
R1# copy running-config usbflash0:
Destination filename [running-config]? R1-Config
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
5024 bytes copied in 1.796 secs (2797 bytes/sec)
R1#
```

USB sürücüsündeki dosyayı görmek için dir komutunu kullanın ve örnekte gösterildiği gibi içeriği görmek için more komutunu kullanın.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024   Jan 7 2013 20:26:50 +00:00  R1-Config
4050042880 bytes total (3774144512 bytes free)
R1#
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
no ipv6 cef
R1#
```

### Yapılandırmaları bir USB Flash Sürücü ile Geri Yükleme

Dosyayı geri kopyalamak için, USB R1-Config dosyasını bir metin düzenleyiciyle düzenlemek gerekecektir. Dosya adının R1-Config olduğunu varsayarak, çalışan bir yapılandırmayı geri yüklemek için **copy usbflash0:/R1-Config** *running-config* komutunu kullanın .

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 39.6.5.Parola-Şifre Kurtarma Prosedürleri

Cihazlardaki parolalar, yetkisiz erişimi önlemek için kullanılır. Gizli parolaları etkinleştirme gibi şifreli parolalar için, parolaların kurtarıldıktan sonra değiştirilmesi gerekir. Cihaza bağlı olarak, şifre kurtarma için ayrıntılı prosedür değişiklik gösterir. Ancak, tüm şifre kurtarma prosedürleri aynı prensibi izler:

1. Adım . ROMMON moduna girin.
2. Adım . Yapılandırma kaydını değiştirin.
3. Adım . Startup-config'i running-config'e kopyalayın.
4. adım . Şifreyi değiştirin.
5. Adım . Running-config'i yeni Startup-config olarak kaydedin.
6. adım . Cihazı yeniden yükleyin.

Parola kurtarma için bilgisayardaki bir terminal veya terminal emülatör yazılımı aracılığıyla aygıta konsol erişimi gerekir. Cihaza erişim için terminal ayarları şunlardır:

9600 baud rate
No parity
8 data bits
1 stop bit
No flow control

## 39.6.6.Parola-Şifre Kurtarma Örneği

**Adım 1. ROMMON moduna girin.**

Konsol erişimiyle, bir kullanıcı, önyükleme işlemi sırasında bir kesme dizisi kullanarak veya aygıt kapatıldığında harici flaş belleği çıkararak ROMMON moduna erişebilir. Başarılı olduğunda , örnekte gösterildiği gibi rommon 1> istemi görüntülenir.

Not : PuTTY için kesme dizisi Ctrl + Break şeklindedir. Diğer terminal öykünücüleri ve işletim sistemleri için standart kesme anahtarı dizilerinin bir listesi internette arama yapılarak bulunabilir.

```
Readonly ROMMON initialized

monitor: command "boot" aborted due to user interrupt
rommon 1 >
```

**Adım 2. Yapılandırma kaydını değiştirin.**

ROMMON yazılımı, confreg gibi bazı temel komutları destekler . Confreg 0x2142 komutu kullanıcı 0x2142 yapılandırma kayıt ayarlamanızı sağlar. 0x2142'deki yapılandırma kaydı ile aygıt, başlatma sırasında başlangıç yapılandırma dosyasını yoksayar. Başlangıç yapılandırma dosyası, unutulan parolaların saklandığı yerdir. Yapılandırma kaydını 0x2142 olarak ayarladıktan sonra , cihazı yeniden başlatmak için istemde reset yazın. Cihaz, IOS'yi yeniden başlatırken ve sıkıştırmayı açarken kesme sırasını girin. Örnek, önyükleme işlemi sırasında bir kesinti dizisi kullandıktan sonra ROMMON modunda bir 1941 yönlendiricinin terminal çıkışını görüntüler.

```
rommon 1 > confreg 0x2142
rommon 2 > reset

System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2010 by cisco Systems, Inc.
(output omitted)
```

Licensed to: ozan karasungur, yetkinkrsngr@gmail.com

**Adım 3. Start-config'i running-config'e kopyalayın.**

Aygıt yeniden yüklemeyi bitirdikten sonra, örnekte gösterildiği gibi copy startup-config running-config komutunu kullanarak başlangıç yapılandırmasını çalışan yapılandırmaya kopyalayın . Yönlendirici isteminin R1 # olarak değiştiğine dikkat edin, çünkü ana bilgisayar adı başlangıç yapılandırmasında R1 olarak ayarlanmıştır.

DİKKAT: copy running-config startup-config girmeyin . Bu komut, orijinal başlangıç yapılandırmanızı siler.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

**Adım 4. Parolayı değiştirin.**

Ayrıcalıklı EXEC modunda olduğunuz için, şimdi örnekte gösterildiği gibi gerekli tüm parolaları yapılandırabilirsiniz.

Not: **cisco** parolası güçlü bir parola değildir ve burada yalnızca örnek olarak kullanılmıştır.

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# enable secret cisco
```

**Adım 5. running-config'i yeni startup-config olarak kaydedin.**

Yeni parolalar yapılandırıldıktan sonra, genel yapılandırma modunda config-register 0x2102 komutunu kullanarak yapılandırma kaydını tekrar 0x2102 olarak değiştirin . Örnekte gösterildiği gibi, running-config'i startup-config'e kaydedin.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

**Adım 6. Cihazı yeniden yükleyin.**

Örnekte gösterildiği gibi cihazı yeniden yükleyin. Yeniden yüklemeyi onaylamanızın nasıl istendiğine dikkat edin. Devam etmek için Enter'a basın. Aksi takdirde , iptal etmek için Control-C'ye basın .

Cihaz artık kimlik doğrulama için yeni yapılandırılmış şifreleri kullanıyor. Tüm konfigürasyonların hala yerinde olduğunu doğrulamak için show komutlarını kullandığınızdan emin olun . Örneğin, parola kurtarma işleminden sonra uygun arabirimlerin kapatılmadığını doğrulayın.

Belirli bir cihaz için şifre kurtarma prosedürlerine yönelik ayrıntılı talimatları bulmak için internette arama yapın.

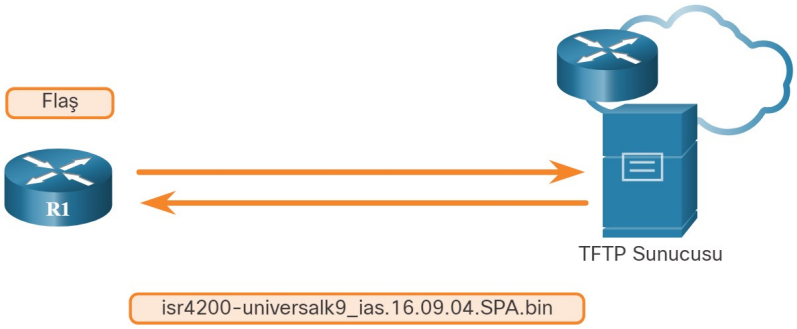
```
R1# reload
Proceed with reload? [confirm]

*Mar  1 13:04:53.009: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload Command.
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 39.7.IOS Görüntü (Image) Yönetimi

### 39.7.1.Yedek Konum Olarak TFTP Sunucuları

Bir ağ büyüdükçe, Cisco IOS Yazılımı görüntüleri ve yapılandırma dosyaları, şekilde gösterildiği gibi merkezi bir TFTP sunucusunda saklanabilir. Bu, IOS görüntülerinin sayısını ve bu IOS görüntülerinde yapılan revizyonların yanı sıra korunması gereken yapılandırma dosyalarının sayısını kontrol etmeye yardımcı olur.




Üretim ağları genellikle geniş alanlara yayılır ve birden çok yönlendirici içerir. Herhangi bir ağ için, yönlendiricideki sistem görüntüsünün bozulması veya yanlışlıkla silinmesi durumunda Cisco IOS Yazılım görüntüsünün yedek bir kopyasını saklamak iyi bir uygulamadır.

Yaygın olarak dağıtılan yönlendiriciler, Cisco IOS Yazılım görüntüleri için bir kaynak veya yedekleme konumuna ihtiyaç duyar. Bir ağ TFTP sunucusu kullanmak, ağ üzerinden görüntü ve konfigürasyon yüklemelerine ve indirmelerine izin verir. Ağ TFTP sunucusu başka bir yönlendirici, bir iş istasyonu veya bir ana bilgisayar sistemi olabilir.

### 39.7.2.IOS Görüntüsünü TFTP Sunucusuna Yedekleme Örneği

Ağ işlemlerini minimum kesinti süresiyle sürdürmek için, Cisco IOS görüntülerini yedeklemeye yönelik prosedürlere sahip olmak gerekir. Bu, ağ yöneticisinin görüntünün bozulması veya silinmesi durumunda bir görüntüyü hızla yönlendiriciye kopyalamasına olanak tanır.

Şekilde, ağ yöneticisi , 172.16.1.100'deki TFTP sunucusuna yönlendiricideki (isr4200-universalk9_ias.16.09.04.SPA.bin) mevcut imaj dosyasının bir yedeğini oluşturmak istiyor .

**Adım 1. TFTP sunucusuna ping atın.**

Ağ TFTP sunucusuna erişim olduğundan emin olun. Örnekte gösterildiği gibi, bağlantıyı test etmek için TFTP sunucusuna ping atın.

```
R1# ping 172.16.1.100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5),
round-trip min/avg/max = 56/56/56 ms
```

**Adım 2. Flash'ta görüntü boyutunu doğrulayın.**

TFTP sunucusunun Cisco IOS Yazılım görüntüsünü barındırmak için yeterli disk alanına sahip olduğunu doğrulayın. Cisco IOS görüntü dosyasının boyutunu belirlemek için yönlendiricide show flash0: komutunu kullanın . Örnekteki dosya 517153193 bayt uzunluğundadır.

```
R1# show flash0:
-# - --length-- -----date/time------ path
8   517153193   Apr 2 2019 21:29:58  +00:00
                        isr4200-universalk9_ias.16.09.04.SPA.bin
(output omitted)
```

Adım 3. IOS Görüntüsünü TFTP sunucusuna kopyalayın.

**copy** *source-url destination-url* komutunu kullanarak görüntüyü TFTP sunucusuna kopyalayın . Belirtilen kaynak ve hedef URL'leri kullanarak komutu verdikten sonra, kullanıcıdan kaynak dosya adı, uzak ana bilgisayarın IP adresi ve hedef dosya adı istenir. Tipik olarak, kaynak dosya adını hedef dosya adı olarak kabul etmek için Enter tuşuna basarsınız . Transfer daha sonra başlayacaktır.

```
R1# copy flash: tftp:
Source filename []? isr4200-universalk9_ias.16.09.04.SPA.bin
Address or name of remote host []? 172.16.1.100
Destination filename [isr4200-universalk9_ias.16.09.04.SPA.bin]?
Writing isr4200-universalk9_ias.16.09.04.SPA.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
(output omitted)
517153193 bytes copied in 863.468 secs (269058 bytes/sec)
```

## 39.7.3.Önyükleme Sistem (boot system) Komutu

Bu görüntü yönlendiricinin flash belleğine kaydedildikten sonra kopyalanan IOS görüntüsüne yükseltmek için, yönlendiriciyi örnekte gösterildiği gibi **boot system** komutunu kullanarak önyükleme sırasında yeni görüntüyü yükleyecek şekilde yapılandırın . Yapılandırmayı kaydedin. Yönlendiriciyi yeni görüntü ile başlatmak için yönlendiriciyi yeniden yükleyin.

```
R1# configure terminal
R1(config)# boot system flash0:isr4200-universalk9_ias.16.09.04.SPA.bin
R1(config)# exit
R1#
R1# copy running-config startup-config
R1#
R1# reload
Proceed with reload? [confirm]

*Mar  1 12:46:23.808: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.
```

Başlatma sırasında, önyükleme kodu , yüklenecek Cisco IOS Software görüntüsünün adını ve konumunu belirten boot system komutları için NVRAM'deki başlangıç yapılandırma dosyasını ayrıştırır . Hataya dayanıklı bir önyükleme planı sağlamak için birkaç boot systemkomutu sırayla girilebilir.

Yapılandırmada boot system komutu yoksa , yönlendirici varsayılan olarak ilk geçerli Cisco IOS görüntüsünü flash bellekte yükler ve çalıştırır.

Yönlendirici başlatıldıktan sonra, yeni görüntünün yüklendiğini doğrulamak için , örnekte gösterildiği gibi **show version** komutunu kullanın .

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
R1# show version
Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fuji], ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9_IAS-M), Version 16.9.4, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 18:09 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2019 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.

ROM: IOS-XE ROMMON
Router uptime is 2 hours, 19 minutes
Uptime for this control processor is 2 hours, 22 minutes
System returned to ROM by PowerOn
System image file is "flash:isr4200-universalk9_ias.16.09.04.SPA.bin"
(output omitted)
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 40.Bölüm: Network Tasarımı

## 40.1.Hiyerarşik Ağlar

### 40.1.1.Ağı Ölçeklendirme İhtiyacı

Dijital dünyamız değişiyor. İnternete ve kurumsal ağa erişim yeteneği artık fiziksel ofisler, coğrafi konumlar veya saat dilimleriyle sınırlı değil. Günümüzün küreselleşmiş işyerinde çalışanlar kaynaklara dünyanın her yerinden erişebilir ve bilgiler her zaman ve herhangi bir cihazda mevcut olmalıdır. Bu gereksinimler, güvenli, güvenilir ve yüksek düzeyde erişilebilir yeni nesil ağlar oluşturma ihtiyacını doğurur.

Bu yeni nesil ağlar, yalnızca mevcut beklentileri ve ekipmanları desteklemekle kalmamalı, aynı zamanda eski platformları entegre edebilmelidir. İşletmeler, kritik görev hizmetleri sağlamak için ağ altyapılarına giderek daha fazla güveniyor. İşletmeler büyüdükçe ve geliştikçe, daha fazla çalışan işe alır, şubeler açar ve küresel pazarlara açılırlar. Bu değişiklikler, işletmenin ihtiyaçlarını karşılamak için ölçeklendirilebilmesi gereken bir ağın gereksinimlerini doğrudan etkiler.

Bir ağ, veri dosyaları, e-posta, IP telefonu ve birden çok iş birimi için video uygulamaları dahil olmak üzere çeşitli ağ trafiği türlerinin değişimini desteklemelidir. Tüm kurumsal ağlar aşağıdakileri yapabilmelidir:

- Kritik uygulamaları destekleme
- Yakınsanmış ağ trafiğini destekleme
- Çeşitli iş ihtiyaçlarını destekleme
- Merkezi idari kontrol sağlama

LAN, son kullanıcılar ve cihazlar için ağ iletişim hizmetlerine ve kaynaklarına erişim sağlayan ağ altyapısıdır. Son kullanıcılar ve cihazlar tek bir kata veya binaya yayılmış olabilir. Küçük bir coğrafi alana yayılmış bir grup LAN'ı birbirine bağlayarak bir kampüs ağı oluşturursunuz. Kampüs ağ tasarımları, binlerce bağlantıya sahip çok büyük ağlara kadar tek bir LAN anahtarı kullanan küçük ağları içerir.

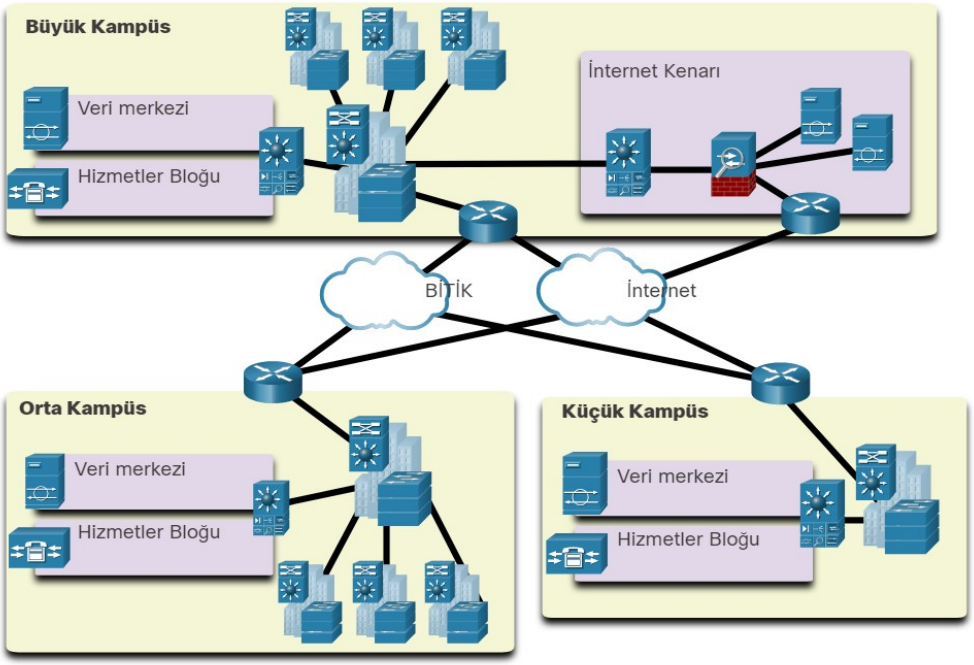
### 40.1.2.Sınırsız Anahtarlı Ağlar(Borderless Switched Networks)

Birleştirilmiş ağın artan talepleri ile birlikte ağ, zekayı içeren, işlemleri basitleştiren ve gelecekteki talepleri karşılamak için ölçeklenebilir bir mimari yaklaşımla geliştirilmelidir. Ağ tasarımındaki en yeni gelişmelerden biri Cisco Sınırsız Ağ'dır.

Cisco Sınırsız Ağ, yenilik ve tasarımı birleştiren bir ağ mimarisidir. Kuruluşların, herhangi birini, her yerde, her zaman, herhangi bir cihazda birbirine bağlayabilen sınırsız bir ağı desteklemesine olanak tanır; güvenli, güvenilir ve sorunsuz. Bu mimari, birleşik ağın desteklenmesi ve çalışma modellerinin değiştirilmesi gibi BT ve iş zorluklarını ele almak için tasarlanmıştır.

Cisco Sınırsız Ağ, birçok farklı cihaz türünde politika, erişim kontrolü ve performans yönetimi dahil olmak üzere kablolu ve kablosuz erişimi birleştirmek için bir çerçeve sağlar. Bu mimariyi kullanarak, şekilde gösterilen sınırsız ağ, ölçeklenebilir ve esnek olan hiyerarşik bir donanım altyapısı üzerine inşa edilmiştir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




Bu donanım altyapısını ilke tabanlı yazılım çözümleriyle birleştiren Cisco Sınırsız Ağ, iki ana hizmet kümesi sağlar: ağ hizmetleri ve entegre bir yönetim çözümü çatısı altında kullanıcı ve uç nokta hizmetleri. Optimizasyon, ölçeklenebilirlik ve güvenlik sağlarken, farklı ağ öğelerinin birlikte çalışmasını sağlar ve kullanıcıların herhangi bir yerden, herhangi bir zamanda kaynaklara erişmesine olanak tanır.

## 40.1.3.Sınırsız Anahtarlı Ağda Hiyerarşi

Sınırsız anahtarlı bir ağ oluşturmak, maksimum kullanılabilirlik, esneklik, güvenlik ve yönetilebilirlik sağlamak için sağlam ağ tasarımı ilkelerinin kullanılmasını gerektirir. Sınırsız anahtarlamalı ağ, mevcut gereksinimleri ve gelecekteki gerekli hizmetleri ve teknolojileri sağlamalıdır. Kenarlıksız anahtarlı ağ tasarımı yönergeleri aşağıdaki ilkeler üzerine inşa edilmiştir:

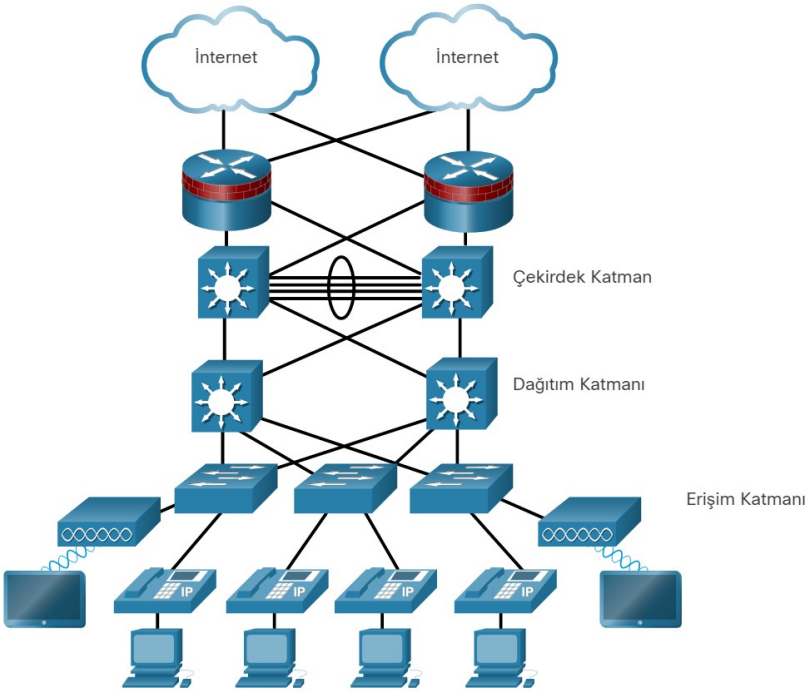
- Hiyerarşik - Tasarım, her bir katmanda her bir cihazın rolünün anlaşılmasını kolaylaştırır, dağıtımı, operasyonu ve yönetimi basitleştirir ve her katmanda hata etki alanlarını azaltır.
- Modülerlik - Tasarım, isteğe bağlı olarak sorunsuz ağ genişletmeye ve entegre hizmet etkinleştirmeye olanak tanır.
- Esneklik - Tasarım, ağı her zaman açık tutmak için kullanıcı beklentilerini karşılar.
- Esneklik - Tasarım, tüm ağ kaynaklarını kullanarak akıllı trafik yükü paylaşımına izin verir.

Bunlar bağımsız ilkeler değildir. Her bir ilkenin diğerlerinin bağlamına nasıl uyduğunu anlamak çok önemlidir. Hiyerarşik bir tarzda kenarlıksız anahtarlı bir ağ tasarlamak, ağ tasarımcılarının güvenlik, hareketlilik ve birleşik iletişim özelliklerini üst üste koymasına olanak tanıyan bir temel oluşturur. Kampüs ağları için zaman içinde test edilmiş ve kanıtlanmış iki hiyerarşik tasarım çerçevesi, üç katmanlı katman ve iki katmanlı katman modelleridir.

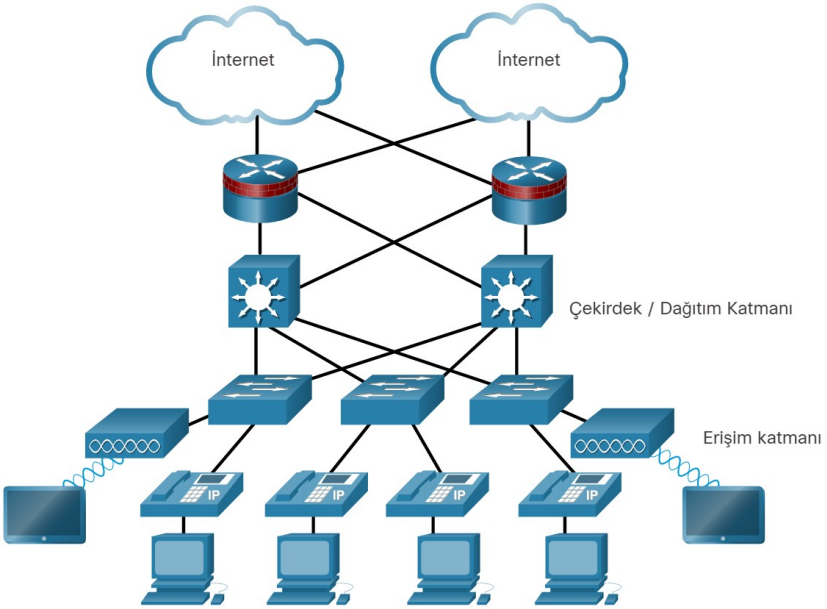
Bu katmanlı tasarımlardaki üç kritik katman erişim (access), dağıtım(distribution) ve çekirdek(core) katmanlardır. Her katman, kampüs ağında belirli rollere ve işlevlere sahip, iyi tanımlanmış, yapılandırılmış bir modül olarak görülebilir. Kampüs hiyerarşik tasarımına modülerliğin dahil edilmesi, kampüs ağının kritik ağ hizmetlerini sağlayacak kadar esnek ve esnek kalmasını sağlar. Modülerlik ayrıca, zaman içinde meydana gelen büyüme ve değişikliklere izin vermeye de yardımcı olur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Üç Katmanlı Model




### İki Katmanlı Model




## 40.1.4.Erişim, Dağıtım ve Çekirdek Katman İşlevleri

### Erişim Katmanı

Erişim katmanı, trafiğin kampüs ağına girip çıktığı ağ kenarını temsil eder. Geleneksel olarak, bir erişim katmanı anahtarının birincil işlevi, kullanıcıya ağ erişimi sağlamaktır. Erişim katmanı anahtarları, yönlendirme, hizmet kalitesi ve güvenlik gibi ağ temel teknolojilerini uygulayan dağıtım katmanı anahtarlarına bağlanır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Ağ uygulamasını ve son kullanıcı talebini karşılamak için, yeni nesil anahtarlama platformları artık ağ ucundaki çeşitli uç noktalara daha yakınsamalı, entegre ve akıllı hizmetler sağlıyor. Erişim katmanı anahtarlarında zeka uygulamaları oluşturmak, uygulamaların ağ üzerinde daha verimli ve güvenli bir şekilde çalışmasını sağlar.

**Dağıtım Katmanı**

Dağıtım katmanı, aşağıdakiler de dahil olmak üzere birçok önemli işlevi sağlamak için erişim katmanı ile çekirdek katman arasında arayüz oluşturur:

- Büyük ölçekli kablolama odası ağlarını bir araya getirmek
- Katman 2 yayın alanlarını ve Katman 3 yönlendirme sınırlarını birleştirme
- Ağın geri kalanına erişmek için akıllı anahtarlama, yönlendirme ve ağ erişim politikası işlevleri sağlama
- Son kullanıcıya yedek dağıtım katmanı anahtarları aracılığıyla yüksek kullanılabilirlik ve çekirdeğe eşit maliyet yolları sağlama
- Ağın ucunda çeşitli hizmet uygulamaları sınıflarına farklılaştırılmış hizmetler sunmak

**Çekirdek Katman**

Çekirdek katman, ağ omurgasıdır. Kampüs ağının birkaç katmanını birbirine bağlar. Çekirdek katman, tüm dağıtım katmanı aygıtları için toplayıcı görevi görür ve kampüsü ağın geri kalanıyla birbirine bağlar. Çekirdek katmanın birincil amacı, hata yalıtımı ve yüksek hızlı omurga bağlantısı sağlamaktır.

## 40.2.Ölçeklenebilir Ağlar

### 40.2.1.Ölçeklenebilirlik İçin Tasarım

Ağınızın değişeceğini anlıyorsunuz. Kullanıcı sayısı muhtemelen artacaktır, her yerde bulunabilirler ve çok çeşitli cihazlar kullanırlar. Ağınız, kullanıcılarıyla birlikte değişebilmelidir. Ölçeklenebilirlik, kullanılabilirliği ve güvenilirliği kaybetmeden büyüyebilen bir ağ için kullanılan terimdir.

Büyük, orta veya küçük bir ağı desteklemek için ağ tasarımcısı, ağın kullanılabilir olmasını ve etkili ve kolay bir şekilde ölçeklenmesini sağlamak için bir strateji geliştirmelidir. Temel bir ağ tasarım stratejisine aşağıdaki öneriler dahildir:

- Yetenekleri artırmak için kolayca yükseltilebilen genişletilebilir, modüler ekipman veya kümelenmiş cihazlar kullanın. Cihaz modülleri, büyük ekipman yükseltmelerine gerek kalmadan yeni özellikleri ve cihazları desteklemek için mevcut ekipmana eklenebilir. Bazı cihazlar, yönetimi ve yapılandırmayı basitleştirmek için tek bir cihaz olarak çalışmak üzere bir kümeye entegre edilebilir.
- Ağın diğer işlevsel alanlarının tasarımını etkilemeden, gerektiğinde eklenebilen, yükseltilebilen ve değiştirilebilen modülleri içerecek hiyerarşik bir ağ tasarlayın. Örneğin, kampüs ağının dağıtımını ve çekirdek katmanlarını etkilemeden genişletilebilen ayrı bir erişim katmanı oluşturmak.
- Hiyerarşik bir IPv4 ve IPv6 adres stratejisi oluşturun. Dikkatli adres planlaması, ek kullanıcıları ve hizmetleri desteklemek için ağı yeniden adresleme ihtiyacını ortadan kaldırır.
- Yayınları sınırlandırmak ve ağdan gelen diğer istenmeyen trafiği filtrelemek için yönlendiricileri veya çok katmanlı anahtarları seçin. Ağ çekirdeğine gelen trafiği filtrelemek ve azaltmak için Katman 3 cihazları kullanın.

### 40.2.2.Artıklık (Redundancy) Planı

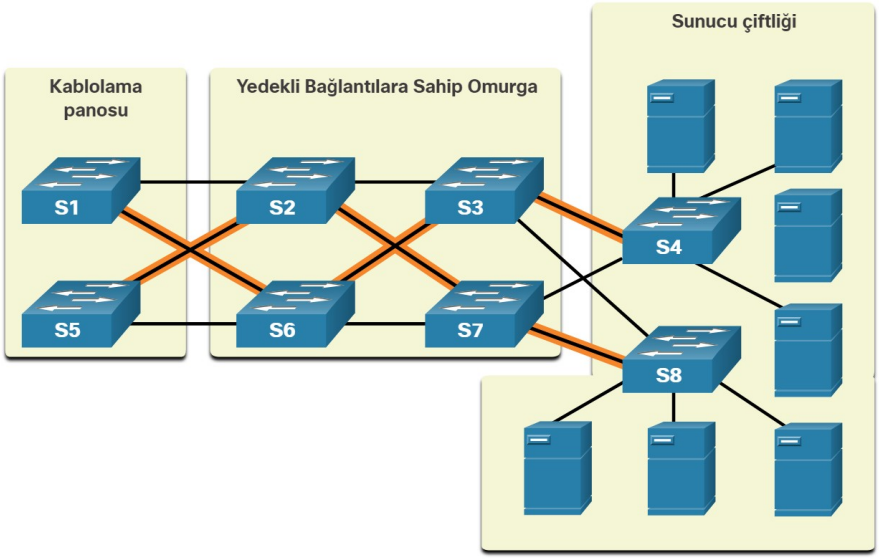
Birçok kuruluş için ağın kullanılabilirliği, iş ihtiyaçlarını desteklemek için çok önemlidir. Yedeklilik, ağ tasarımının önemli bir parçasıdır. Tek bir arıza noktası olasılığını en aza indirerek ağ hizmetlerinin kesintiye uğramasını önleyebilir. Yedekliliği uygulamanın bir yöntemi, yinelenen ekipmanı kurmak ve kritik cihazlar için yük devretme hizmetleri sağlamaktır.

Fazlalık uygulamanın başka bir yöntemi, şekilde gösterildiği gibi artık yollardır. Yedekli yollar, verilerin ağı geçmesi için alternatif fiziksel yollar sunar. Anahtarlamalı bir ağdaki yedekli yollar, yüksek kullanılabilirliği destekler. Bununla birlikte, anahtarların çalışması nedeniyle, anahtarlamalı bir Ethernet ağındaki yedek yollar mantıksal Katman 2 döngülerine neden olabilir. Bu nedenle, Yayılan Ağaç Protokolü (STP) gereklidir.

Lisansınızı yönetmek ve kullanmak yalnızca size aittir.

STP, anahtarlar arasında fazladan bağlantılar kullanıldığında Katman 2 döngülerini ortadan kaldırır. Bunu, anahtarlı bir ağdaki yedekli yolları, yol gerekli olana kadar devre dışı bırakmak için bir mekanizma sağlayarak yapar. STP, döngü içermeyen bir mantıksal topoloji oluşturmak için anahtarlı bir ortamda kullanılan açık standart bir protokoldür.

Ana iletişim hattında Katman 3'ü kullanmak, Katman 2'de STP'ye ihtiyaç duymadan artıklık gerçekleştirmenin başka bir yoludur. Katman 3 ayrıca en iyi yol seçimi ve yük devretme sırasında daha hızlı yakınsama sağlar.




## 40.2.3.Arıza Etki Alanı Boyutunu Azaltma

İyi tasarlanmış bir ağ yalnızca trafiği kontrol etmekle kalmaz, aynı zamanda hata etki alanlarının boyutunu da sınırlar. Hata etki alanı, kritik bir aygıt veya ağ hizmeti sorunlarla karşılaştığında etkilenen ağ alanıdır.

Başlangıçta başarısız olan cihazın işlevi, bir arıza alanının etkisini belirler. Örneğin, bir ağ segmentindeki arızalı bir anahtar normalde yalnızca o segmentteki ana bilgisayarları etkiler. Bununla birlikte, bu segmenti diğerlerine bağlayan yönlendirici başarısız olursa, etki çok daha büyük olur.

Yedek bağlantıların ve güvenilir kurumsal sınıf ekipmanların kullanılması, bir ağdaki kesinti olasılığını en aza indirir. Daha küçük hata alanları, bir arızanın şirket üretkenliği üzerindeki etkisini azaltır. Ayrıca sorun giderme sürecini basitleştirir, böylece tüm kullanıcılar için kesinti süresini kısaltırlar.

### Hata Etki Alanlarının Boyutunu Sınırlandırma

Bir ağın çekirdek katmanındaki bir arıza potansiyel olarak büyük bir etkiye sahip olabileceğinden, ağ tasarımcısı genellikle arızaları önleme çabalarına odaklanır. Bu çabalar, ağı uygulama maliyetini büyük ölçüde artırabilir. Hiyerarşik tasarım modelinde, dağıtım katmanındaki bir hata alanının boyutunu kontrol etmek en kolay ve genellikle en ucuzdur. Dağıtım katmanında, ağ hataları daha küçük bir alanda tutulabilir; bu nedenle, daha az kullanıcıyı etkiler. Dağıtım katmanında Katman 3 cihazları kullanılırken, her yönlendirici sınırlı sayıda erişim katmanı kullanıcısı için bir ağ geçidi işlevi görür.

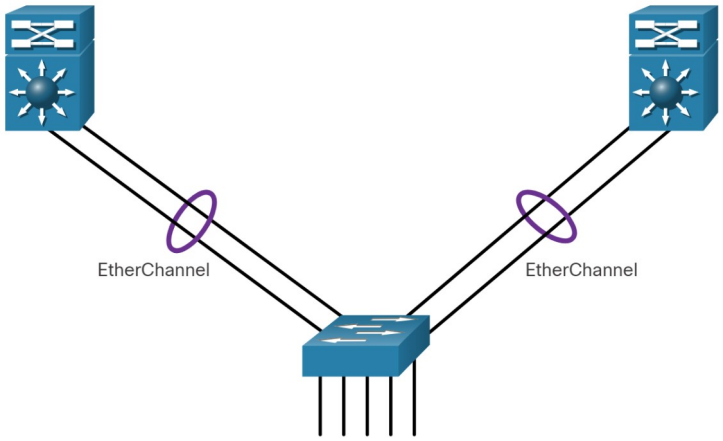
### Anahtar Bloğu Dağıtımı

Yönlendiriciler veya çok katmanlı anahtarlar genellikle, aralarında eşit olarak bölünmüş erişim katmanı anahtarları ile çiftler halinde dağıtılır. Bu yapılandırma, bir bina veya departmana ait anahtar bloğu olarak adlandırılır. Her bir anahtar bloğu diğerlerinden bağımsız olarak hareket eder. Sonuç olarak, tek bir cihazın arızalanması ağın kapanmasına neden olmaz. Anahtar bloğunun tamamının arızalanması bile önemli sayıda son kullanıcıyı etkilemez.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 40.2.4.Bant Genişliğini Arttırma

Hiyerarşik ağ tasarımında, erişim ve dağıtım anahtarları arasındaki bazı bağlantıların diğer bağlantılardan daha fazla miktarda trafiği işlemesi gerekebilir. Birden çok bağlantıdan gelen trafik tek, giden bir bağlantıda birleştiğinden, bu bağlantının bir darboğaz haline gelmesi mümkündür. EtherChannel gibi bağlantı toplama, bir yöneticinin birkaç fiziksel bağlantıdan oluşan tek bir mantıksal bağlantı oluşturarak cihazlar arasındaki bant genişliği miktarını artırmasına olanak tanır.

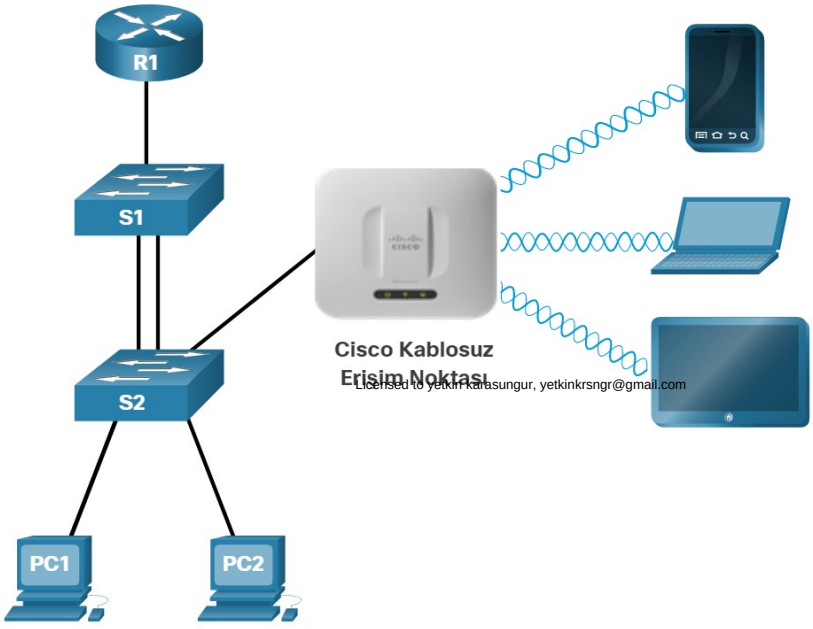



EtherChannel, mevcut anahtar bağlantı noktalarını kullanır. Bu nedenle, bağlantıyı daha hızlı ve daha pahalı bir bağlantıya yükseltmek için ek maliyetler gerekli değildir. EtherChannel, EtherChannel arayüzü kullanan tek bir mantıksal bağlantı olarak görülür. Çoğu yapılandırma görevi, her bir bağlantı noktası yerine EtherChannel arabiriminde yapılır ve bağlantılar boyunca yapılandırma tutarlılığı sağlanır. Son olarak, EtherChannel yapılandırması, aynı EtherChannel'in parçası olan bağlantılar arasındaki yük dengelemeden yararlanır ve donanım platformuna bağlı olarak bir veya daha fazla yük dengeleme yöntemi uygulanabilir.

## 40.2.5.Erişim Katmanını Genişletme

Ağ, gerektiğinde bireylere ve cihazlara ağ erişimini genişletebilecek şekilde tasarlanmalıdır. Erişim katmanı bağlantısını genişletmek için giderek daha önemli olan bir seçenek kablosuzdur. Kablosuz bağlantı sağlamak, artan esneklik, düşük maliyetler ve değişen ağ ve iş gereksinimlerine büyüme ve uyum sağlama yeteneği gibi birçok avantaj sunar.

Kablosuz iletişim kurmak için, uç cihazlar, bir radyo vericisi / alıcısı ve onu çalıştırmak için gerekli yazılım sürücüsünü içeren bir kablosuz NIC gerektirir. Ek olarak, kullanıcıların bağlanması için şekilde gösterildiği gibi bir kablosuz yönlendirici veya kablosuz erişim noktası (AP) gereklidir.

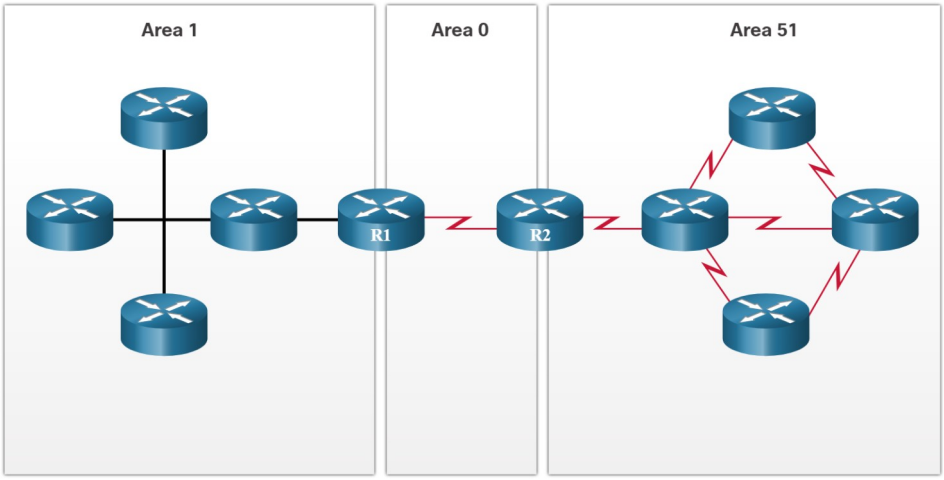


Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 40.2.6.Yönlendirme Protokollerini Ayarlama

Önce En Kısa Yolu Aç-Open Shortest Path First (OSPF) gibi gelişmiş yönlendirme protokolleri, büyük ağlarda kullanılır.

OSPF, bir bağlantı durumu yönlendirme protokolüdür. Şekilde gösterildiği gibi, OSPF, hızlı yakınsamanın önemli olduğu daha büyük hiyerarşik ağlarda iyi çalışır. OSPF yönlendiricileri, diğer bağlı OSPF yönlendiricileriyle komşu komşuları oluşturur ve korur. OSPF yönlendiricileri, bağlantı durumu veritabanlarını senkronize eder. Bir ağ değişikliği meydana geldiğinde, bağlantı durumu güncellemeleri gönderilir, bu da diğer OSPF yönlendiricilerini değişiklik hakkında bilgilendirir ve varsa yeni bir en iyi yol oluşturur.




## 40.3.Switch Donanımları

### 40.3.1.Switch Platformları

Hiyerarşik ve ölçeklenebilir ağlar oluşturmanın basit bir yolu, iş için doğru ekipmanı kullanmaktır. Bir anahtar seçmeden önce göz önünde bulundurmanız gereken çeşitli anahtar platformları, form faktörleri ve diğer özellikler vardır.

Bir ağ tasarlarken, ağın büyümesine izin vermenin yanı sıra mevcut ağ gereksinimlerini karşılayacak doğru donanımı seçmek önemlidir. Bir kurumsal ağ içinde, hem anahtarlar hem de yönlendiriciler, ağ iletişiminde kritik bir rol oynar.

**Kampüs LAN Anahtarları**

Bir kurumsal LAN'da ağ performansını ölçeklendirmek için çekirdek, dağıtım, erişim ve kompakt anahtarlar vardır. Bu anahtar platformları, sekiz sabit bağlantı noktasına sahip fansız anahtarlardan yüzlerce bağlantı noktasını destekleyen 13 blade anahtarlara kadar çeşitlilik gösterir. Kampüs LAN anahtar platformları arasında Cisco 2960, 3560, 3650, 3850, 4500, 6500 ve 6800 Serileri bulunur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Bulut Tarafından Yönetilen Anahtarlar**

Cisco Meraki bulut yönetimli erişim anahtarları, anahtarların sanal olarak yığınlanmasını sağlar. Yerinde BT personelinin müdahalesi olmadan web üzerinden binlerce anahtar bağlantı noktasını izler ve yapılandırırlar.

**Veri Merkezi Anahtarları**

Bir veri merkezi, altyapı ölçeklenebilirliğini, operasyonel sürekliliği ve taşıma esnekliğini destekleyen anahtarlara dayalı olarak oluşturulmalıdır. Veri merkezi anahtar platformları, Cisco Nexus Serisi anahtarları içerir.

**Servis Sağlayıcı Anahtarları**

Servis sağlayıcı anahtarları iki kategoriye ayrılır: toplama anahtarları ve Ethernet erişim anahtarları. Toplama anahtarları, bir ağın ucundaki trafiği toplayan taşıyıcı sınıfı Ethernet anahtarlarıdır. Servis sağlayıcı Ethernet erişim anahtarları, uygulama zekası, birleşik hizmetler, sanallaştırma, entegre güvenlik ve basitleştirilmiş yönetim özelliklerine sahiptir.

**Sanal Ağ**

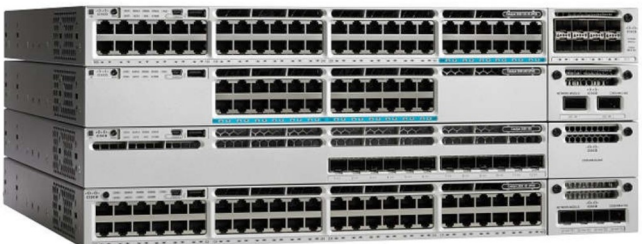
Ağlar giderek sanallaştırılıyor. Cisco Nexus sanal ağ anahtarı platformları, veri merkezi ağına sanallaştırma zeka teknolojisini ekleyerek güvenli çok kiracılı hizmetler sağlar.

Lisansınız yetkinkrsngr@gmail.com

## 40.3.2.Switch Form Faktörleri

### Sabit konfigürasyon anahtarları

Sabit konfigürasyon anahtarlarındaki özellikler ve seçenekler, orijinal olarak anahtarla birlikte gelenlerle sınırlıdır.



### Modüler konfigürasyon anahtarları

Modüler anahtarlardaki kasa, sahada değiştirilebilir hat kartlarını kabul eder.

### İstiflenebilir (Stackable) konfigürasyon anahtarları

Tek bir büyük anahtar olarak etkin bir şekilde çalışmasına izin veren istiflenebilir anahtarları bağlamak için özel kablolar kullanılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Kalınlık**

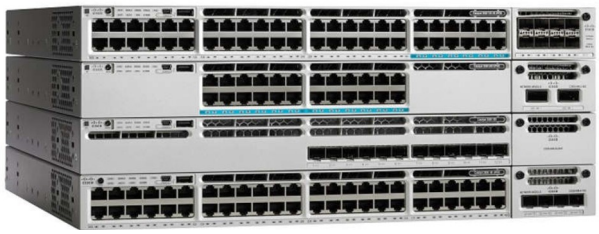
Raf birimlerinin sayısı ile ifade edilen anahtarın kalınlığı, rafa monte edilen anahtarlar için de önemlidir. Örneğin, şekilde gösterilen sabit yapılandırma anahtarlarının tümü bir raf birimidir (1U) veya 1,75 inç (44,45 mm) yüksekliğindedir.

## 40.3.3.Bağlantı Noktası Yoğunluğu

Bir anahtarın bağlantı noktası yoğunluğu, tek bir anahtarda bulunan bağlantı noktalarının sayısını ifade eder. Şekil, üç farklı anahtarın bağlantı noktası yoğunluğunu göstermektedir.

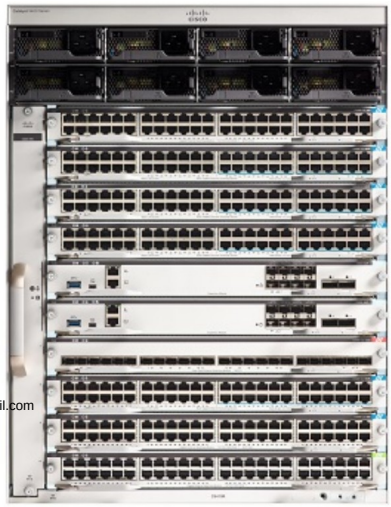
Sabit yapılandırma anahtarları, çeşitli bağlantı noktası yoğunluğu yapılandırmalarını destekler. Cisco Catalyst 3850, şekilde gösterildiği gibi 12, 24, 48 bağlantı noktası yapılandırmalarında gelir. 48 bağlantı noktalı anahtar, küçük form faktörlü takılabilir-small form-factor pluggable (SFP) aygıtlar için ek bağlantı noktaları seçeneğine sahiptir.

**Cisco Catalyst 3850 Switches**



Modüler anahtarlar, birden çok anahtar portu hat kartının eklenmesiyle çok yüksek bağlantı noktası yoğunluklarını destekleyebilir. Bir sonraki şekilde gösterilen modüler Catalyst 9400 anahtarı, 384 anahtar portu arayüzünü destekler.

**Catalyst 9400 Anahtarı**



Binlerce ağ cihazını destekleyen büyük ağlar, alanı ve gücü en iyi şekilde kullanmak için yüksek yoğunluklu, modüler anahtarlar gerektirir. Yüksek yoğunluklu modüler bir anahtar kullanmadan ağ, ağ erişimine ihtiyaç duyan cihazların sayısını barındırmak için birçok sabit yapılandırma anahtarına ihtiyaç duyar. Bu yaklaşım, birçok elektrik prizini ve çok fazla dolap alanını tüketebilir.

Ağ tasarımcısı ayrıca yukarı bağlantı darboğazları konusunu da dikkate almalıdır. Bir dizi sabit konfigürasyon anahtarı, hedef performansa ulaşmak amacıyla anahtarlar arasında bant genişliği toplama için birçok ek bağlantı noktası kullanabilir. Tek bir modüler anahtarla, bant genişliği toplama daha az sorun teşkil eder çünkü kasanın arka paneli, anahtar bağlantı noktası hat kartlarına bağlı aygıtları barındırmak için gerekli bant genişliğini sağlayabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

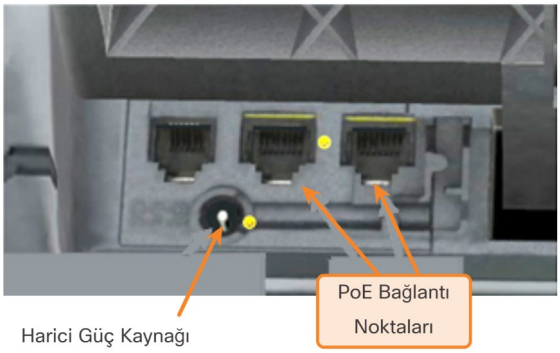
## 40.3.4.Ethernet Üzerinden Güç (Power over Ethernet)

Ethernet Üzerinden Güç (PoE), anahtarın mevcut Ethernet kabloları üzerinden bir cihaza güç sağlamasına izin verir. Bu özellik IP telefonlar ve bazı kablosuz erişim noktaları tarafından kullanılabilir ve bunların Ethernet kablosunun olduğu herhangi bir yere kurulmasına izin verir. Bir ağ yöneticisi, PoE özelliklerinin belirli bir kurulum için gerçekten gerekli olduğundan emin olmalıdır çünkü PoE'yi destekleyen anahtarlar pahalıdır.

### Switch

PoE bağlantı noktaları, diğer herhangi bir anahtar bağlantı noktasıyla aynı görünür. Bağlantı noktasının PoE'yi destekleyip desteklemediğini belirlemek için anahtarın modelini kontrol edin.

### IP Telefon




### WAP

Kablosuz erişim noktalarındaki PoE bağlantı noktaları, diğer anahtar bağlantı noktaları ile aynı görünür. Bağlantı noktasının PoE'yi destekleyip desteklemediğini belirlemek için kablosuz erişim noktasının modelini kontrol edin.

### Cisco Catalyst 2960-C

Cisco Catalyst 2960-C ve 3560-C Serisi kompakt anahtarlar, PoE geçişini destekler. PoE geçişi, bir ağ yöneticisinin belirli yukarı akış anahtarlarından güç çekerek anahtara bağlı PoE cihazlarının yanı sıra anahtarın kendisine güç sağlamasına olanak tanır.

## 40.3.5.Çok Katmanlı Anahtarlama (Multilayer Switching)

Çok katmanlı anahtarlar, genellikle bir kuruluşun anahtarlı ağının çekirdek ve dağıtım katmanlarında konuşlandırılır. Çok katmanlı anahtarlar, bir yönlendirme tablosu oluşturma, birkaç yönlendirme protokolünü destekleme ve IP paketlerini Katman 2 yönlendirmesine yakın bir hızda iletme yetenekleriyle karakterize edilir. Çok katmanlı anahtarlar genellikle uygulamaya özel entegre devreler- application-specific integrated circuits (ASIC'ler) gibi özel donanımları destekler. Özel yazılım veri yapılarıyla birlikte ASIC'ler, CPU'dan bağımsız olarak IP paketlerinin iletimini kolaylaştırabilir.

Licensed to Yalçın Karatunçur, yalcinkarat@gmail.com

Saf Katman 3 anahtarlamalı bir ortama doğru ağ oluşturmada bir eğilim var. Anahtarlar ağlarda ilk kez kullanıldığında, hiçbiri yönlendirmeyi desteklemiyordu. Artık neredeyse tüm anahtarlar yönlendirmeyi destekliyor. Yakında tüm anahtarların bir yönlendirme işlemcisini dahil etmesi muhtemeldir çünkü bunu yapmanın maliyeti diğer kısıtlamalara göre azalmaktadır.

Şekilde bir Catalyst 2960 gösterilmektedir. Catalyst 2960 anahtarları, saf bir Katman 3 ortamına geçişi göstermektedir. 15.x'ten önceki IOS sürümlerinde, bu anahtarlar yalnızca bir etkin anahtarlamalı sanal arabirimi (SVI) destekler. IOS 15.x ile bu anahtarlar artık birden çok etkin SVI'yı desteklemektedir. Bu, anahtara farklı ağlarda birden çok IP adresi aracılığıyla uzaktan erişilebileceği anlamına gelir.

## 40.4.Router Donanımı

### 40.4.1.Yönlendirici Gereksinimleri

Anahtarlar, çeşitli özelliklerle gelen bir ağın tek bileşeni değildir. Yönlendirici seçiminiz çok önemli bir karardır. Yönlendiriciler, evleri ve işletmeleri internete bağlayarak, bir kurumsal ağ içindeki birden çok siteyi birbirine bağlayarak, yedekli yollar sağlayarak ve internet üzerinden ISS'leri bağlayarak ağ oluşturmada kritik bir rol oynar. Yönlendiriciler ayrıca farklı ortam türleri ve protokoller arasında bir çevirmen görevi görebilir. Örneğin, bir yönlendirici, bir Ethernet ağından paketleri kabul edebilir ve bir seri ağ üzerinden aktarım için bunları yeniden kapsülleyebilir.

Yönlendiriciler, paketleri uygun hedefe yönlendirmek için hedef IP adresinin ağ bölümünü (önek) kullanır. Bir bağlantı koparsa alternatif bir yol seçerler. Yerel bir ağdaki tüm ana bilgisayarlar, IP yapılandırmalarında yerel yönlendirici arayüzünün IP adresini belirtir. Bu yönlendirici arayüzü varsayılan ağ geçididir. Verimli bir şekilde yönlendirme ve ağ bağlantısı hatalarından kurtarma yeteneği, paketleri hedeflerine teslim etmek için kritik öneme sahiptir.

Yönlendiriciler ayrıca aşağıdaki gibi diğer yararlı işlevlere de hizmet eder:

- Yayınları yerel ağ ile sınırlandırarak yayın kapsamı sağlarlar.
- Coğrafi olarak ayrılmış konumları birbirine bağlarlar.
- Kullanıcıları, ortak ihtiyaçlara veya aynı kaynaklara erişim gerektiren bir şirket içindeki uygulamaya veya departmana göre mantıksal olarak gruplandırırlar.
- Erişim kontrol listeleri aracılığıyla istenmeyen trafiği filtreleyerek gelişmiş güvenlik sağlarlar.

### 40.4.2.Cisco Yönlendiriciler

Ağ büyüdükçe, gereksinimlerini karşılayacak doğru yönlendiricileri seçmek önemlidir. Cisco yönlendiricilerinin farklı kategorileri vardır.

#### Şube Yönlendiriciler

Şekilde gösterilen şube yönlendiricileri, şube ve WAN altyapıları arasında optimum uygulama deneyimi sağlarken, şube hizmetlerini tek bir platformda optimize eder. Şubede hizmet kullanılabilirliğini en üst düzeye çıkarmak, 24x7x365 çalışma süresi için tasarlanmış ağlar gerektirir. Yüksek kullanılabilirliğe sahip şube ağları, hizmet üzerindeki etkiyi en aza indirirken veya ortadan kaldırırken tipik hatalardan hızlı kurtarma sağlamalı ve basit ağ yapılandırması ve yönetimi sağlamalıdır. Cisco Integrated Services Router (ISR) 4000 Serisi Yönlendiriciler gösterilmektedir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Ağ Uç Yönlendiricileri**

Şekilde gösterilen ağ ucu yönlendiricileri, ağ ucunun kampüs, veri merkezi ve şube ağlarını birleştiren yüksek performanslı, oldukça güvenli ve güvenilir hizmetler sunmasını sağlar. Müşteriler, yüksek kaliteli bir medya deneyimi ve her zamankinden daha fazla içerik türü bekliyor. Müşteriler tüm içerik için etkileşim, kişiselleştirme, hareketlilik ve kontrol istiyor. Müşteriler ayrıca içeriğe istedikleri zaman ve istedikleri yerden, herhangi bir cihaz üzerinden, evde, işte veya hareket halindeyken erişmek istiyor. Ağ uç yönlendiricileri, gelişmiş hizmet kalitesi ve kesintisiz video ve mobil yetenekler sunmalıdır. Cisco Toplama Hizmetleri Yönlendiricileri-Cisco Aggregation Services Routers ( (ASR) 9000 Serisi Yönlendiriciler gösterilmiştir.

**Servis Sağlayıcı Yönlendiricileri**

Şekilde gösterilen servis sağlayıcı yönlendiricileri, uçtan uca ölçeklenebilir çözümler ve abonelerin farkında olan hizmetler sunar. Operatörler, tüm cihazlarda ve konumlarda yeni nesil internet deneyimleri sunmak için işlemleri optimize etmeli, masrafları azaltmalı, ölçeklenebilirliği ve esnekliği geliştirmelidir. Bu sistemler, hizmet dağıtım ağlarının işletimini ve dağıtımını basitleştirmek ve geliştirmek için tasarlanmıştır. Şekilde gösterilenler, Cisco Network Convergence System (NCS) 6000 Serisi Yönlendiricilerdir.

Kapı Kapalı

Kapı açık

**Sanayi Tipi**

Şekilde gösterilenler gibi endüstriyel yönlendiriciler, zorlu ve zorlu ortamlarda kurumsal sınıf özellikler sağlamak üzere tasarlanmıştır. Kompakt, modüler, sağlamlaştırılmış tasarımları, kritik görev uygulamaları için mükemmeldir. Gösterilenler, Cisco 1100 Serisi Endüstriyel Tümleşik Servis Yönlendiricileridir.

## 40.4.3.Yönlendirici Form Faktörleri

Anahtarlar gibi, yönlendiriciler de birçok form faktöründe gelir. Kurumsal ortamdaki ağ yöneticileri, küçük bir masaüstü yönlendiriciden rafa monte edilmiş veya blade modele kadar çeşitli yönlendiricileri destekleyebilmelidir.

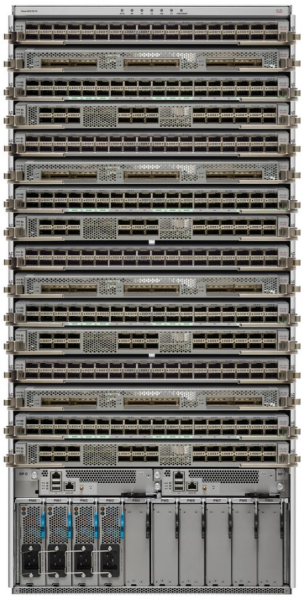
**Cisco 900 Serisi**

Bu, küçük bir şube ofisi yönlendiricisidir. Küçük ve orta ölçekli işletmeler için kompakt, fansız bir platformda WAN, anahtarlama, güvenlik ve gelişmiş bağlantı seçeneklerini bir araya getirir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Cisco ASR 9000 ve 1000 Serisi Toplama Hizmetleri Yönlendiricileri ( Aggregation Services Routers)**

Bu yönlendiriciler, ölçeklenebilir bir ağ sınırı için programlanabilirlik ile yoğunluk ve esneklik sağlar.



**Cisco Network Convergence System 5500 Serisi Yönlendiriciler**

Bu yönlendiriciler, büyük veri merkezleri ve büyük kurumsal ağlar, web ve servis sağlayıcı WAN ve toplama ağları arasında verimli bir şekilde ölçeklenecek şekilde tasarlanmıştır.

**Cisco 800 Endüstriyel Tümleşik Hizmetler Yönlendiricisi**

Bu yönlendirici kompakttır ve zorlu ortamlar için tasarlanmıştır.

Yönlendiriciler ayrıca sabit konfigürasyon veya modüler olarak kategorize edilebilir. Sabit konfigürasyonla, istenen yönlendirici arayüzleri yerleşiktir. Modüler yönlendiriciler, bir ağ yöneticisinin yönlendirici üzerindeki arabirimleri değiştirmesine olanak tanıyan birden çok yuvaya sahiptir. Yönlendiriciler, Hızlı Ethernet, Gigabit Ethernet, Seri ve Fiber Optik gibi çeşitli farklı arabirimlerle birlikte gelir.

Kapsamlı bir Cisco yönlendirici listesi, Cisco'nun web sitesinde arama yapılarak bulunabilir.
www.cisco.com
.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 41.Bölüm: Ağ Sorunlarını Giderme

## 41.1.Ağı Belgelendirme

### 41.1.1.Ağ Belgelendirmeye Genel Bakış

Ağ sorun giderme gibi karmaşık faaliyetlerde olduğu gibi, işe iyi belgelerle başlamanız gerekecektir. Ağları etkin bir şekilde izlemek ve gidermek için doğru ve eksiksiz ağ belgeleri gereklidir.

Ortak ağ belgeleri aşağıdakileri içerir:

- Fiziksel ve mantıksal ağ topolojisi diyagramları
- İlgili tüm cihaz bilgilerini kaydeden ağ cihazı belgeleri
- Ağ performansı temel belgeleri

Tüm ağ belgeleri, basılı kopya olarak veya korumalı bir sunucu üzerindeki ağda tek bir yerde tutulmalıdır. Yedek belgeler ayrı bir yerde tutulmalı ve saklanmalıdır.

### 41.1.2.Ağ Topolojisi Diyagramları

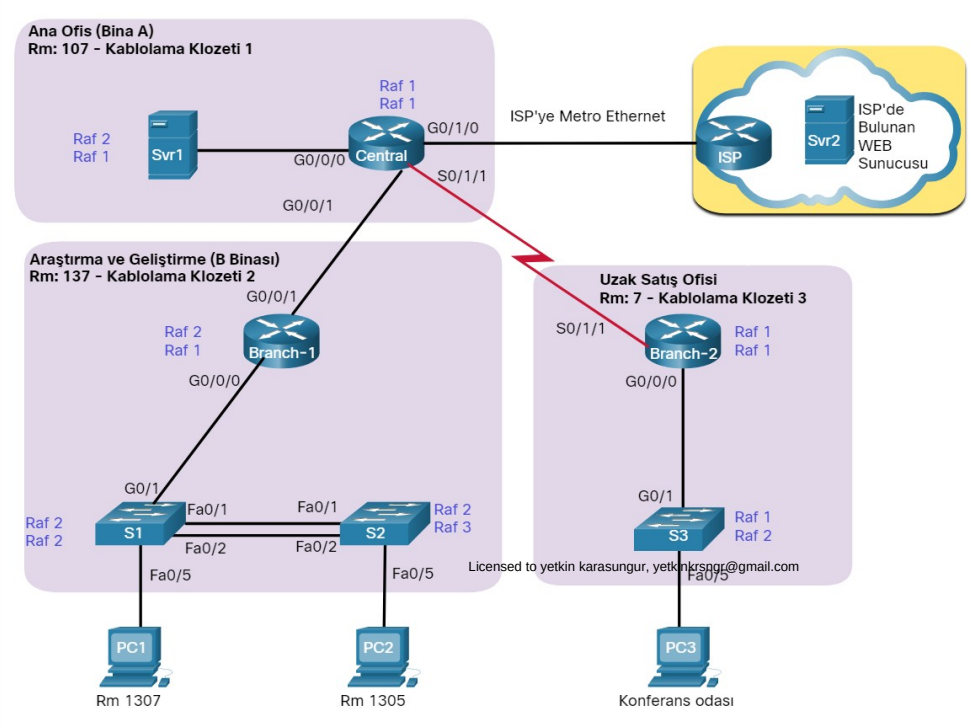
Ağ topolojisi diyagramları, ağdaki cihazların konumunu, işlevini ve durumunu takip eder. İki tür ağ topolojisi diyagramı vardır: fiziksel topoloji ve mantıksal topoloji.

#### Fiziksel Topoloji

Fiziksel bir ağ topolojisi, ağa bağlı cihazların fiziksel düzenini gösterir. Fiziksel katman sorunlarını gidermek için cihazların fiziksel olarak nasıl bağlandığını bilmeniz gerekir. Fiziksel topolojiye kaydedilen bilgiler tipik olarak şunları içerir:

- Cihaz adı
- Cihaz konumu (adres, oda numarası, raf konumu)
- Arayüz ve kullanılan bağlantı noktaları
- Kablo tipi

Şekil, örnek bir fiziksel ağ topolojisi diyagramını göstermektedir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

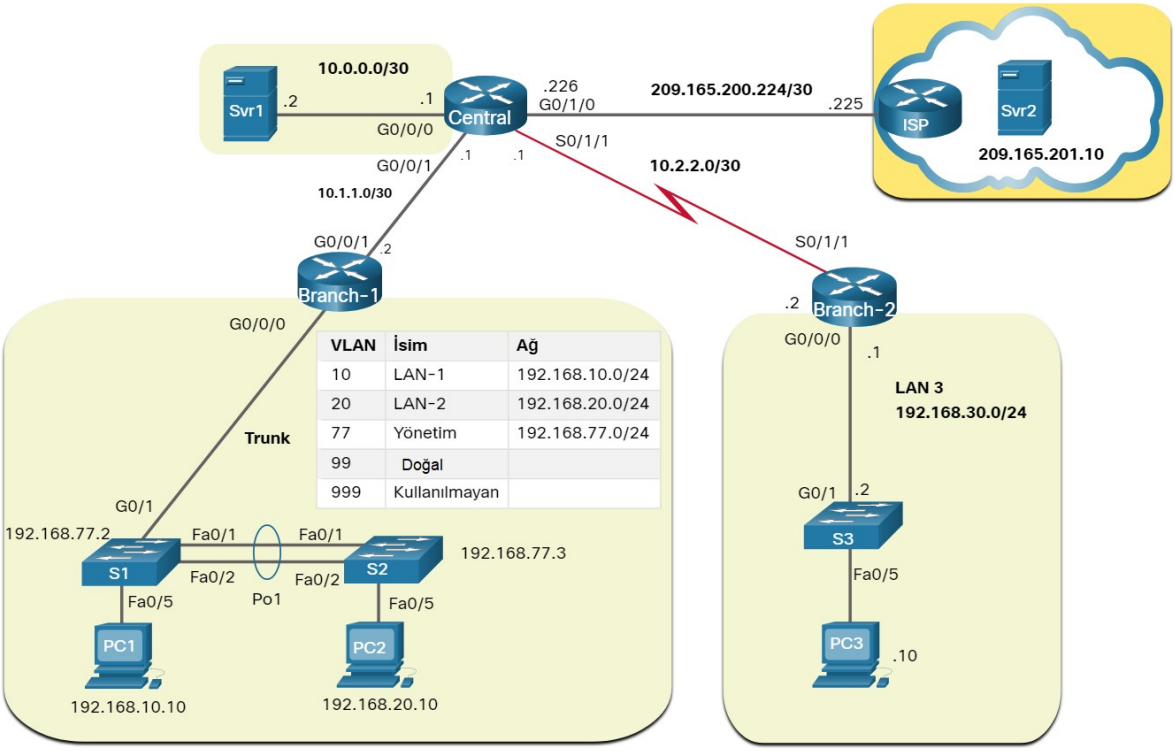
**Mantıksal Topoloji**

Mantıksal bir ağ topolojisi, cihazların mantıksal olarak ağa nasıl bağlandığını gösterir. Bu, cihazların diğer cihazlarla iletişim kurarken ağ üzerinden nasıl veri aktardığını ifade eder. Semboller, yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar gibi ağ bileşenlerini temsil etmek için kullanılır. Ek olarak, birden çok site arasındaki bağlantılar gösterilebilir, ancak gerçek fiziksel konumları temsil etmez.

Mantıksal bir ağ topolojisine kaydedilen bilgiler aşağıdakileri içerebilir:

- Cihaz tanımlayıcıları
- IP adresleri ve önek uzunlukları
- Arayüz tanımlayıcıları
- Yönlendirme protokolleri / statik yollar
- Katman 2 bilgileri (yani, VLAN'lar, ana hatlar, EtherChannels)

Şekilde örnek bir mantıksal IPv4 ağ topolojisi gösterilmektedir.




## 41.1.3.Ağ Cihazı Belgeleri

Ağ cihazı belgeleri, ağ donanımı ve yazılımının doğru, güncel kayıtlarını içermelidir. Dokümantasyon, ağ cihazları ile ilgili tüm bilgileri içermelidir.

Birçok kuruluş, ilgili cihaz bilgilerini yakalamak için tablolar veya elektronik tablolar içeren belgeler oluşturur.

**Yönlendirici Cihaz Belgeleri**

Tablo, birbirine bağlanan iki yönlendirici için örnek ağ cihazı belgelerini gösterir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| cihaz | Modeli | Açıklama | yer | IOS | Lisans |
|---|---|---|---|---|---|
| **Merkez** | ISR 4321 | Merkezi Kenar Yönlendirici | Bina A Rm: 137 | Cisco IOS XE Yazılımı, Sürüm 16.09.04 flash: isr4300-universalk9_ias.16.09.04.SPA.bin | ipbasek9 securityk9 |

| Arayüz | Açıklama | IPv4 Adresi | IPv6 Adresi | Mac Adresi | Yönlendirme |
|---|---|---|---|---|---|
| G0 / 0/0 | SVR-1'e bağlanır | 10.0.0.1/30 | 2001: db8: acad: 1 :: 1/64 | a03d.6fe1.e180 | OSPF |
| G0 / 0/1 | Branch-1'e bağlanır | 10.1.1.1/30 | 2001: db8: acad: a001 :: 1/64 | a03d.6fe1.e181 | OSPFv3 |
| G0 / 1/0 | ISP'ye bağlanır | 209.165.200.226/30 | 2001: db8: besleme: 1 :: 2/64 | a03d.6fc3.a132 | Varsayılan |
| S0 / 1/1 | Branch-2'ye bağlanır | 10.1.1.2/24 | 2001: db8: acad: 2 :: 1/64 | yok | OSPFv3 |

| cihaz | Modeli | Açıklama | Site | IOS | Lisans |
|---|---|---|---|---|---|
| **Şube-1** | ISR 4221 | Branch-2 Kenar Yönlendirici | Bina B Rm: 107 | Cisco IOS XE Yazılımı, Sürüm 16.09.04 flash: isr4200-universalk9.16.09.04.SPA.bin | ipbasek9 securityk9 |

| Arayüz | Açıklama | IPv4 Adresi | IPv6 Adresi | Mac Adresi | Yönlendirme |
|---|---|---|---|---|---|
| G0 / 0/0 | S1'e bağlanır | Çubuk üzerinde yönlendirici | Çubuk üzerinde yönlendirici | a03d.6fe1.9d90 | OSPF |
| G0 / 0/1 | Merkeze bağlanır | 10.1.1.2/30 | 2001: db8: acad: a001 :: 2/64 | a03d.6fe1.9d91 | OSPF |

## LAN Switch Cihaz Dokümantasyonu

Bu tablo, bir LAN anahtarı için örnek cihaz belgelerini gösterir.

| cihaz | Modeli | Açıklama | Mgt. IP adresi | IOS | VTP |
|---|---|---|---|---|---|
| **S1** | Cisco Catalyst WS-C2960-24TC-L | Branch-1 LAN1 anahtarı | 192.168.77.2/24 | IOS: 15,0 (2) SE7 Görüntü: C2960-LANBASEK9-M | Etki Alanı: CCNA Modu: Sunucu |

| Liman | Açıklama | Giriş | VLAN | Gövde | EtherChannel | Yerli | Etkin |
|---|---|---|---|---|---|---|---|
| Fa0 / 1 | Port Channel 1 trunk'dan S2 Fa0 / 1'e | - | - | Evet | Port-Kanal 1 | 99 | Evet |
| Fa0 / 2 | Port Channel 1 trunk'dan S2 Fa0 / 2'ye | - | - | Evet | Port-Kanal 1 | 99 | Evet |
| Fa0 / 3 | *** Kullanımda değil *** | Evet | 999 | - | - | | Kapamak |
| Fa0 / 4 | *** Kullanımda değil *** | Evet | 999 | - | - | | Kapamak |
| Fa0 / 5 | Kullanıcıya erişim portu | Evet | 10 | - | - | | Evet |
| ... | | | | - | - | | - |
| Fa0 / 24 | Kullanıcıya erişim portu | Evet | 20 | - | - | | Evet |
| Fa0 / 24 | *** Kullanımda değil *** | Evet | 999 | - | - | | Kapamak |
| G0 / 1 | Şube-1'e ana bağlantı | - | - | Evet | - | 99 | Evet |
| G0 / 2 | *** Kullanımda değil *** | Evet | 999 | | - | | |

## Son Sistem Dokümantasyon Dosyaları

Son sistem belgeleri sunucularda, ağ yönetim konsollarında ve kullanıcı iş istasyonlarında kullanılan donanım ve yazılıma odaklanır. Yanlış yapılandırılmış bir uç sistem, bir ağın genel performansı üzerinde olumsuz bir etkiye sahip olabilir. Bu nedenle, sorun giderme sırasında son sistem cihaz belgelerine erişim çok yararlı olabilir.

Licensed to yetkin karagunguz yetkinkrsngr@gmail.com

Bu tablo, bir son sistem cihaz belgesine kaydedilebilecek bilgilerin bir örneğini gösterir.

| cihaz | işletim sistemi | Hizmetler | Mac Adresi | IPv4 / IPv6 Adresleri | Varsayılan giriş | DNS |
|---|---|---|---|---|---|---|
| SRV1 | MS Sunucu 2016 | SMTP, POP3, Dosya hizmetleri, DHCP | 5475.d08e.9ad8 | 10.0.0.2/30 | 10.0.0.1 | 10.0.0.1 |
| | | | | 2001: db8: acad: 1 :: 2/64 | 2001: db8: acad: 1 :: 1 | 2001: db8: acad: 1 :: 1 |
| SRV2 | MS Sunucu 2016 | HTTP, HTTPS | 5475.d07a.5312 | 209.165.201.10 | 209.165.201.1 | 209.165.201.1 |
| | | | | 2001: db8: besleme: 1 :: 10/64 | 2001: db8: besleme: 1 :: 1 | 2001: db8: besleme: 1 :: 1 |
| PC1 | MS Windows 10 | HTTP, HTTPS | 5475.d017.3133 | 192.168.10.10/24 | 192.168.10.1 | 192.168.10.1 |
| | | | | 2001: db8: acad: 1 :: 251/64 | 2001: db8: acad: 1 :: 1 | 2001: db8: acad: 1 :: 1 |
| ... | | | | | | |

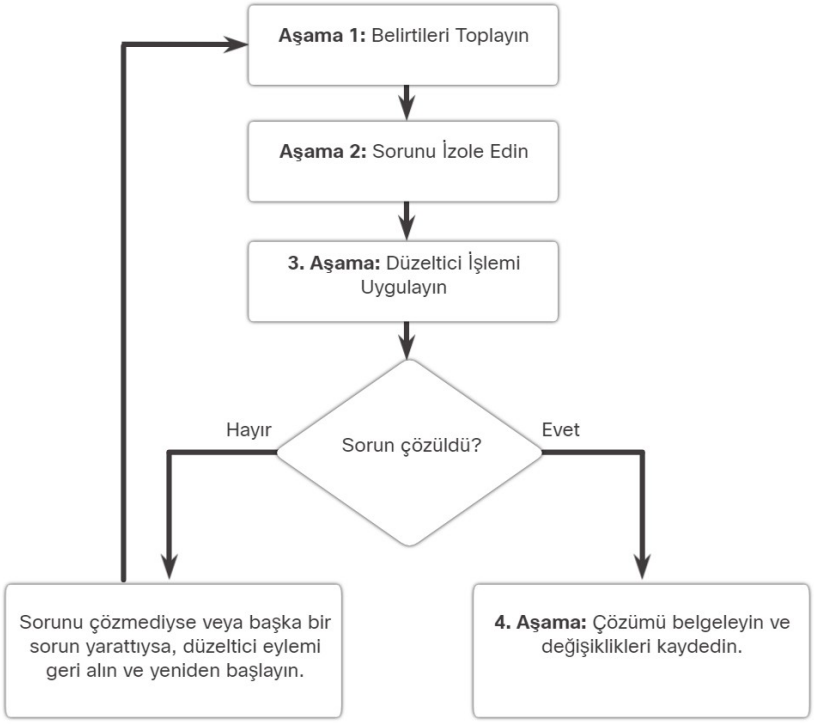
## 41.2.Sorun Giderme Süreci

### 41.2.1.Genel Sorun Giderme Prosedürleri

Ağlar farklı olduğundan, sorunlar farklı olduğundan ve sorun giderme deneyimi değişiklik gösterdiğinden sorun giderme zaman alıcı olabilir. Ancak deneyimli yöneticiler, yapılandırılmış bir sorun giderme yöntemi kullanmanın genel sorun giderme süresini kısaltacağını bilir.

Bu nedenle, sorun giderme süreci yapılandırılmış yöntemlerle yönlendirilmelidir. Bu, düzensiz hata giderme sorun giderme ile ilgili boşa harcanan zamanı en aza indirmek için iyi tanımlanmış ve belgelenmiş sorun giderme prosedürleri gerektirir. Ancak bu yöntemler statik değildir. Bir sorunu çözmek için atılan sorun giderme adımları her zaman aynı değildir veya tam olarak aynı sırayla yürütülmez.

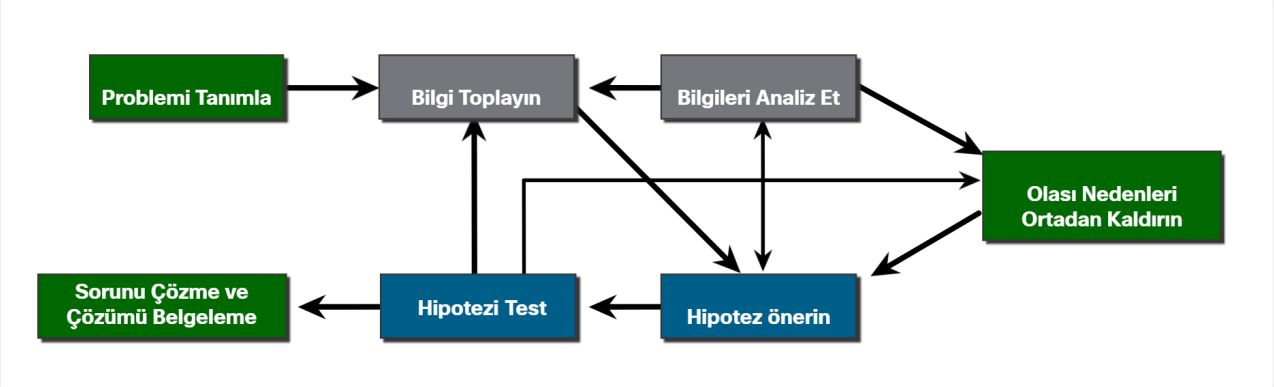
Bir sorunu çözmek için kullanılabilecek birkaç sorun giderme süreci vardır. Şekilde, basitleştirilmiş üç aşamalı sorun giderme sürecinin mantık akış şeması gösterilmektedir. Ancak, daha ayrıntılı bir işlem bir ağ sorununu çözmek için daha yararlı olabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 41.2.2.Yedi Adımda Sorun Giderme Süreci

Şekilde daha ayrıntılı yedi aşamalı bir sorun giderme süreci gösterilmektedir. Bazı adımların birbiriyle nasıl bağlantılı olduğuna dikkat edin. Bunun nedeni, bazı teknisyenlerin deneyim düzeylerine bağlı olarak adımlar arasında geçiş yapabilmeleridir.




### Problemi Tanımla

Bu aşamanın amacı, bir sorun olduğunu doğrulamak ve ardından sorunun ne olduğunu doğru bir şekilde tanımlamaktır. Sorunlar genellikle bir belirti ile tanımlanır (örneğin, ağ yavaş veya çalışmayı durdurdu). Ağ belirtileri, ağ yönetim sisteminden gelen uyarılar, konsol mesajları ve kullanıcı şikayetleri dahil olmak üzere birçok farklı biçimde görünebilir.

Semptomları toplarken, sorunu daha küçük olasılıklara göre yerelleştirmek için soru sormak ve konuyu araştırmak önemlidir. Örneğin, sorun tek bir aygıtla mı, bir aygıt grubuyla mı, yoksa tüm bir alt ağla mı veya aygıt ağıyla mı sınırlı?

Bir organizasyonda, sorunlar genellikle ağ teknisyenlerine sorun biletleri olarak atanır. Bu biletler, her bir biletin ilerlemesini izleyen sorun bildirme yazılımı kullanılarak oluşturulur. Sorun bildirme yazılımı ayrıca bilet göndermek için bir self servis kullanıcı portalı, aranabilir bir sorun biletleri bilgi tabanına erişim, son kullanıcı sorunlarını çözmek için uzaktan kumanda yetenekleri ve daha fazlasını içerebilir.

### Bilgi toplamak

Bu adımda, araştırılacak hedefler (yani ana bilgisayarlar, cihazlar) belirlenmeli, hedef cihazlara erişim sağlanmalı ve bilgi toplanmalıdır. Bu adım sırasında, teknisyen, tanımlanan özelliklere bağlı olarak daha fazla semptom toplayabilir ve belgeleyebilir.

Sorun kuruluşun kontrolünün sınırları dışındaysa (örneğin, otonom sistemin dışında internet bağlantısının kesilmesi), ek ağ belirtilerini toplamadan önce harici sistem için bir yönetici ile iletişime geçin.

### Bilgileri analiz edin

Olası nedenler belirlenmelidir. Toplanan bilgiler, ağ dokümantasyonu, ağ temelleri, organizasyonel bilgi tabanlarında arama, internette arama ve diğer teknisyenlerle konuşma kullanılarak yorumlanır ve analiz edilir.

### Olası Nedenleri Ortadan Kaldırın

Birden fazla neden belirlenirse, en olası nedeni sonunda belirlemek için olası nedenler aşamalı olarak ortadan kaldırılarak liste azaltılmalıdır. Sorun giderme deneyimi, nedenleri hızlı bir şekilde ortadan kaldırmak ve en olası nedeni belirlemek için son derece değerlidir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Hipotez önerin**

En olası neden belirlendiğinde, bir çözüm formüle edilmelidir. Bu aşamada, bir plan önerirken sorun giderme deneyimi çok değerlidir.

**Hipotezi Test**

Çözümü test etmeden önce, sorunun etkisini ve aciliyetini değerlendirmek önemlidir. Örneğin, çözümün diğer sistemler veya süreçler üzerinde olumsuz bir etkisi olabilir mi? Problemin ciddiyeti, çözümün etkisine karşı tartılmalıdır. Örneğin, kritik bir sunucu veya yönlendiricinin önemli bir süre çevrimdışı olması gerekiyorsa, düzeltmeyi uygulamak için iş gününün sonuna kadar beklemek daha iyi olabilir. Bazen asıl sorun çözülene kadar bir geçici çözüm oluşturulabilir.

Bir çözümün nasıl hızlı bir şekilde tersine çevrileceğini tanımlayan bir geri alma planı oluşturun. Çözüm başarısız olursa bu gerekli olabilir.

Çözümü uygulayın ve sorunu çözdüğünü doğrulayın. Bazen bir çözüm beklenmedik bir sorunu ortaya çıkarır. Bu nedenle, bir sonraki adıma geçmeden önce çözümün tamamen doğrulanması önemlidir.

Çözüm başarısız olursa, denenen çözüm belgelenir ve değişiklikler kaldırılır. Teknisyen şimdi Bilgi Toplama adımına geri dönmeli ve sorunu izole etmelidir.

**Problemi çözün**

Sorun çözüldüğünde, kullanıcıları ve sorun giderme sürecine dahil olan herkesi sorunun çözüldüğüne dair bilgilendirin. Diğer BT ekip üyeleri çözüm hakkında bilgilendirilmelidir. Nedenin ve düzeltmenin uygun şekilde belgelendirilmesi, diğer destek teknisyenlerine gelecekte benzer sorunları önleme ve çözme konusunda yardımcı olacaktır.

## 41.2.3.Son Kullanıcıların Soruları

Birçok ağ sorunu başlangıçta bir son kullanıcı tarafından rapor edilir. Bununla birlikte, sağlanan bilgiler genellikle belirsiz veya yanıltıcıdır. Örneğin, kullanıcılar genellikle "ağ kapalı", "e-postama erişemiyorum" veya "bilgisayarım yavaş" gibi sorunları bildiriyor.

Çoğu durumda, bir sorunu tam olarak anlamak için ek bilgi gerekir. Bu genellikle sorunun "kim", "ne" ve "ne zaman" olduğunu keşfetmek için etkilenen kullanıcıyla etkileşim kurmayı içerir.

Kullanıcıyla iletişim kurulurken aşağıdaki öneriler kullanılmalıdır:

- Karmaşık terminolojiyi kullanmaktan kaçınabilecekleri ve anlayabilecekleri teknik bir düzeyde konuşun.
- Her zaman kullanıcının ne söylediğini dikkatle dinleyin veya okuyun. Karmaşık bir sorunu belgelerken not almak yardımcı olabilir.
- Her zaman düşünceli olun ve kullanıcılara karşı empati kurun ve onlara problemlerini çözmelerine yardımcı olacağınızı bildirin. Bir sorunu bildiren kullanıcılar, sorunu olabildiğince çabuk çözmek için stres altında ve endişeli olabilirler.

Kullanıcıyla röportaj yaparken, sorunu hızla tespit etmek için konuşmayı yönlendirin ve etkili sorgulama tekniklerini kullanın. Örneğin, ağ sorunu hakkında önemli gerçekleri keşfetmek için açık sorular (yani, ayrıntılı yanıt gerektirir) ve kapalı sorular (yani, evet, hayır veya tek kelimelik yanıtlar) kullanın.

Tablo, bazı soru sorma yönergeleri ve örnek açık uçlu son kullanıcı soruları sağlar.

Kullanıcıyla görüşmeyi bitirdiğinizde, her ikinizin de bildirilen sorun üzerinde hemfikir olduğunuzdan emin olmak için kullanıcıya sorunu anladığınızı tekrarlayın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Yönergeler | Örnek Açık Uçlu Son Kullanıcı Soruları |
|---|---|
| İlgili sorular sorun. | • Ne çalışmıyor?<br>• Sorun tam olarak nedir?<br>• Neyi başarmaya çalışıyorsun? |
| Sorunun kapsamını belirleyin. | • Bu sorun kimi etkiliyor? Sadece sen mi yoksa diğerleri mi?<br>• Bu hangi cihazda oluyor? |
| Sorunun ne zaman ortaya çıktığını / oluştuğunu belirleyin. | • Sorun tam olarak ne zaman ortaya çıkıyor?<br>• Sorun ilk ne zaman fark edildi?<br>• Görüntülenen herhangi bir hata mesajı var mıydı? |
| Sorunun sürekli mi yoksa aralıklarla mı ortaya çıktığını belirleyin. | • Sorunu yeniden oluşturabilir misin?<br>• Bana sorunun ekran görüntüsünü veya videosunu gönderebilir misin? |
| Herhangi bir şeyin değişip değişmediğini belirleyin. | Son çalıştığından beri ne değişti? |
| Olası sorunları ortadan kaldırmak veya keşfetmek için sorular kullanın. | • Ne çalışıyor?<br>• Ne çalışmıyor? |

## 41.2.4.Bilgi Toplama

Şüpheli ağ cihazından semptomları toplamak için Cisco IOS komutlarını ve paket yakalama ve cihaz günlükleri gibi diğer araçları kullanın.

Tabloda, bir ağ sorununun belirtilerini toplamak için kullanılan yaygın Cisco IOS komutları açıklanmaktadır.

| Komut | Açıklama |
|---|---|
| ping { *ana bilgisayar* \| *ip-adresi* } | • Bir adrese yankı istek paketi gönderir ve ardından yanıt bekler<br>• Ana *bilgisayar* veya *ip adresi* değişkeni, hedef sistemin IP takma adı veya IP adresidir |
| traceroute *hedef* | • Bir paketin ağlar üzerinden geçtiği yolu tanımlar<br>• *Hedef* değişken hedef sistemin adı veya IP adresidir |
| telnet { *ana bilgisayar* \| *ip-adresi* } | • Telnet uygulamasını kullanarak bir IP adresine bağlanır<br>• Telnet yerine mümkün olduğunca SSH kullanın |
| ssh -l *kullanıcı kimliği ip adresi* | • SSH kullanarak bir IP adresine bağlanır<br>• SSH, Telnet'ten daha güvenlidir |
| show ip interface brief<br>show ipv6 interface brief | • Bir cihazdaki tüm arayüzlerin özet durumunu görüntüler<br>• Tüm arayüzlerde IP adreslemesini hızlı bir şekilde tanımlamak için kullanışlıdır. |
| show ip route<br>show ipv6 route | Bilinen tüm ağ hedeflerine giden yolları içeren geçerli IPv4 ve IPv6 yönlendirme tablolarını görüntüler |
| show protocols | Yapılandırılmış protokolleri görüntüler ve herhangi bir yapılandırılmış Katman 3 protokolünün global ve arayüze özgü durumunu gösterir |
| debug | Hata ayıklama olaylarını etkinleştirmek veya devre dışı bırakmak için seçeneklerin bir listesini görüntüler |

Licensed to yetkin karasungur,yetkinkrsngr@gmail.com

Not: Hata ayıklama-debug komutu semptomları toplamak için önemli bir araç olsa da, büyük miktarda konsol mesaj trafiği oluşturur ve bir ağ cihazının performansı önemli ölçüde etkilenebilir. Hata ayıklamanın normal çalışma saatlerinde gerçekleştirilmesi gerekiyorsa, ağ kullanıcılarını bir sorun giderme çabasının devam ettiği ve ağ performansının etkilenebileceği konusunda uyarın. İşiniz bittiğinde hata ayıklamayı devre dışı bırakmayı unutmayın.

## 41.2.5.Katmanlı Modellerle Sorun Giderme

OSI ve TCP / IP modelleri, sorun giderme sırasında ağ sorunlarını izole etmek için uygulanabilir. Örneğin, belirtiler fiziksel bir bağlantı sorunu gösteriyorsa, ağ teknisyeni fiziksel katmanda çalışan devrede sorun gidermeye odaklanabilir.

Şekil, bazı yaygın cihazları ve o cihaz için sorun giderme işlemi sırasında incelenmesi gereken OSI katmanlarını gösterir.

Şema, sorun giderme sırasında incelenmesi gereken OSI model katmanlarını ve ilişkili cihazları gösterir. En üstte, bir uç sistem Uygulama Katmanı 7, Sunum Katmanı 6 ve Oturum Katmanı 5 ile ilişkilendirilmiştir. Bir yönlendirici ve çok katmanlı anahtar, Taşıma Katmanı 4 ve Ağ Katmanı 3 ile ilişkilendirilmiştir. Veri Bağlantısı Katmanı 2. Bir hub Fiziksel Katman 1 ile ilişkilidir.

Yönlendiricilerin ve çok katmanlı anahtarların, taşıma katmanı olan Katman 4'te gösterildiğine dikkat edin. Yönlendiriciler ve çok katmanlı anahtarlar genellikle Katman 3'te yönlendirme kararları verse de, bu cihazlardaki ACL'ler Katman 4 bilgilerini kullanarak filtreleme kararları vermek için kullanılabilir.

## 41.2.6.Yapılandırılmış Sorun Giderme Yöntemleri

Kullanılabilecek birkaç yapılandırılmış sorun giderme yaklaşımı vardır. Hangisinin kullanılacağı duruma bağlı olacaktır. Her yaklaşımın avantajları ve dezavantajları vardır. Bu konu, yöntemleri açıklar ve belirli bir durum için en iyi yöntemi seçmek için yönergeler sağlar.

### Aşağıdan Yukarıya

Aşağıdan yukarıya sorun gidermede, ağın fiziksel katmanıyla ve fiziksel bileşenleriyle başlarsınız ve sorunun nedeni belirlenene kadar OSI modelinin katmanları arasında yukarı çıkarsınız.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Aşağıdan yukarıya sorun giderme, sorunun fiziksel olduğundan şüphelenildiğinde kullanmak için iyi bir yaklaşımdır. Ağ sorunlarının çoğu alt düzeylerde bulunur, bu nedenle aşağıdan yukarıya yaklaşımını uygulamak genellikle etkilidir.

Aşağıdan yukarıya sorun giderme yaklaşımının dezavantajı, sorunun olası nedeni bulunana kadar ağdaki her cihazı ve arabirimi kontrol etmenizi gerektirmesidir. Her bir sonucun ve olasılığın belgelenmesi gerektiğini unutmayın, böylece bu yaklaşımla ilişkili çok sayıda kağıt işi olabilir. Bir başka zorluk da, önce hangi cihazların incelemeye başlayacağını belirlemektir.

**Yukarıdan aşağıya**

Yukarıdan aşağıya sorun giderme, son kullanıcı uygulamalarıyla başlar ve sorunun nedeni belirlenene kadar OSI modelinin katmanlarında aşağı doğru ilerler.

Bir son sistemin son kullanıcı uygulamaları, daha spesifik ağ oluşturma parçalarının üstesinden gelmeden önce test edilir. Bu yaklaşımı daha basit sorunlar için veya sorunun bir yazılım parçasıyla ilgili olduğunu düşündüğünüzde kullanın.

Yukarıdan aşağıya yaklaşımın dezavantajı, sorunun olası nedeni bulunana kadar her ağ uygulamasının kontrol edilmesini gerektirmesidir. Her bir sonuç ve olasılık belgelenmelidir. Buradaki zorluk, hangi uygulamanın önce incelemeye başlayacağını belirlemektir.

**Böl ve keşfet**

Ağ yöneticisi bir katman seçer ve bu katmandan her iki yönde de test eder.

Böl ve yönet sorun gidermede, soruna ilişkin kullanıcı deneyimlerini toplayarak başlar, belirtileri belgelendirir ve ardından bu bilgileri kullanarak araştırmanıza hangi OSI katmanının başlayacağına dair bilinçli bir tahmin yürütürsünüz. Bir katmanın düzgün çalıştığı doğrulandığında, altındaki katmanların çalıştığı varsayılabilir. Yönetici OSI katmanlarını çalıştırabilir. Bir OSI katmanı düzgün çalışmıyorsa, yönetici OSI katman modelinde çalışabilir.

Örneğin, kullanıcılar web sunucusuna erişemiyorlar ancak sunucuya ping atabiliyorlarsa, sorun Katman 3'ün üzerindedir. Sunucuya ping işlemi başarısız olursa, sorun muhtemelen daha düşük bir OSI katmanındadır.

**Yolu takip et**

Bu, en temel sorun giderme tekniklerinden biridir. Yaklaşım ilk olarak kaynaktan hedefe kadar trafik yolunu keşfeder. Sorun giderme kapsamı, yalnızca yönlendirme yolunda bulunan bağlantılara ve cihazlara indirgenmiştir. Amaç, eldeki sorun giderme görevi ile ilgisi olmayan bağlantıları ve cihazları ortadan kaldırmaktır. Bu yaklaşım genellikle diğer yaklaşımlardan birini tamamlar.

**ikame**

Bu yaklaşıma bileşen değiştirme adı da verilir, çünkü sorunlu cihazı bilinen, çalışan bir cihazla fiziksel olarak değiştirirsiniz. Sorun çözülürse, sorun çıkarılan cihazdadır. Sorun devam ederse, neden başka bir yerde olabilir.

Belirli durumlarda, bu, kritik tek bir hata noktası gibi, hızlı problem çözümü için ideal bir yöntem olabilir. Örneğin, bir sınır yönlendiricisi kapanır. Sorunu gidermek yerine, yalnızca cihazı değiştirmek ve hizmeti geri yüklemek daha faydalı olabilir.

Sorun birden fazla cihazda bulunuyorsa, sorunu doğru şekilde izole etmek mümkün olmayabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Karşılaştırma**

Bu yaklaşım aynı zamanda farklılıkları tespit etme yaklaşımı olarak da adlandırılır ve çalışmayan unsurları çalışan unsurlarla tutarlı olacak şekilde değiştirerek sorunu çözmeye çalışır. Çalışan ve çalışmayan durumlar arasındaki yapılandırmaları, yazılım sürümlerini, donanımı veya diğer cihaz özelliklerini, bağlantıları veya işlemleri karşılaştırır ve bunlar arasındaki önemli farklılıkları tespit edersiniz.

Bu yöntemin zayıf yönü, sorunun temel nedenini açıkça ortaya koymadan çalışan bir çözüme yol açabilmesidir.

## 41.3.Sorun Giderme Araçları

### 41.3.1.Yazılım Sorun Giderme Araçları

Bildiğiniz gibi ağlar yazılım ve donanımdan oluşur. Bu nedenle, hem yazılım hem de donanım, sorun giderme için kendi araçlarına sahiptir. Bu konu, her ikisi için de kullanılabilen sorun giderme araçlarını tartışır.

Sorun gidermeyi kolaylaştırmak için çok çeşitli yazılım ve donanım araçları mevcuttur. Bu araçlar, ağ sorunlarının belirtilerini toplamak ve analiz etmek için kullanılabilir. Genellikle ağ temelini oluşturmak için kullanılabilecek izleme ve raporlama işlevleri sağlarlar.

**Ağ Yönetim Sistemi Araçları**

Ağ yönetim sistemi-Network management system (NMS) araçları, cihaz düzeyinde izleme, yapılandırma ve hata yönetimi araçlarını içerir. Bu araçlar, ağ sorunlarını araştırmak ve düzeltmek için kullanılabilir. Ağ izleme yazılımı, ağ cihazlarının fiziksel bir görünümünü grafik olarak görüntüleyerek ağ yöneticilerinin uzaktaki cihazları sürekli ve otomatik olarak izlemelerine olanak tanır. Cihaz yönetimi yazılımı, temel ağ cihazları için dinamik cihaz durumu, istatistikler ve yapılandırma bilgileri sağlar.

**Bilgi Veri Tabanları**

Çevrimiçi ağ cihazı satıcısı bilgi veri tabanları, vazgeçilmez bilgi kaynakları haline geldi. Satıcı tabanlı bilgi tabanları internet arama motorları ile birleştirildiğinde, bir ağ yöneticisinin geniş bir deneyime dayalı bilgi havuzuna erişimi olur.

Örneğin, Cisco Araçlar ve Kaynaklar sayfası şu adreste bulunabilir:
http://www.cisco.com Support menüsü altında . Bu sayfa, Cisco donanımı ve yazılımı için kullanılabilecek araçları sağlar.

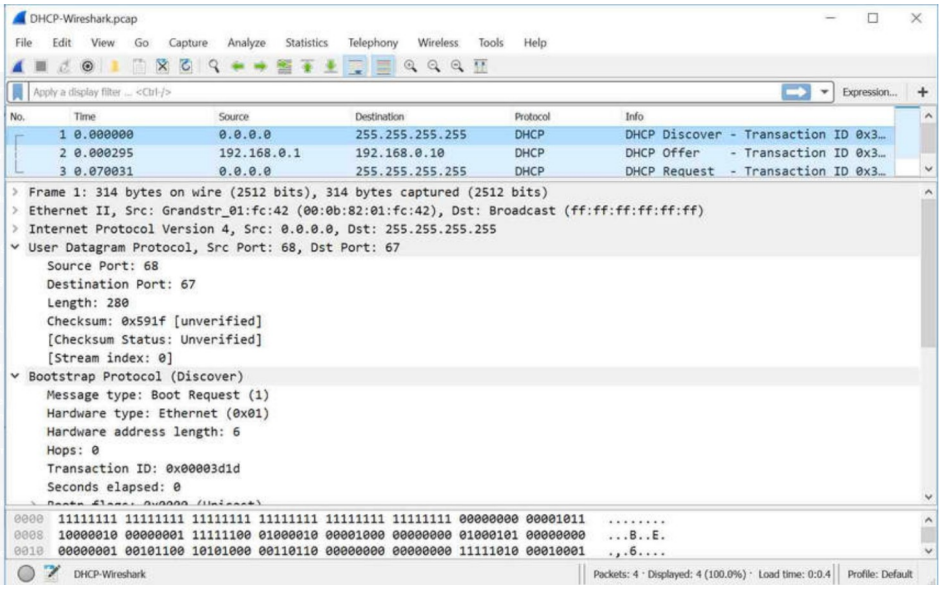
**Ağ Performans Araçları**

Ağ dokümantasyonunu ve temel oluşturma sürecini otomatikleştirmek için birçok araç mevcuttur. Bu araçlar, genel dokümantasyon görevlerine yardımcı olur. Örneğin, ağ diyagramları çizebilir, ağ yazılım ve donanım belgelerini güncel tutmaya yardımcı olabilir ve temel ağ bant genişliği kullanımını uygun maliyetli bir şekilde ölçmeye yardımcı olabilirler.

### 41.3.2.Protokol Analizörleri

Protokol çözümleyicileri, ağ üzerinden akarken paket içeriğini inceleyebilir. Bir protokol analizcisi, kaydedilmiş bir çerçevedeki çeşitli protokol katmanlarının kodunu çözer ve bu bilgileri kullanımı nispeten kolay bir formatta sunar. Şekilde, Wireshark protokol analizörünün ekran görüntüsü gösterilmektedir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com



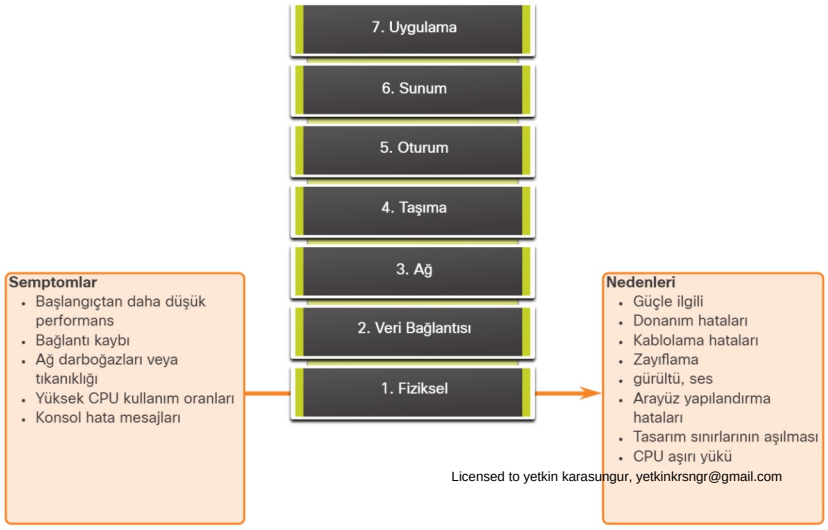

Bir protokol analizcisi tarafından görüntülenen bilgiler, fiziksel katman bit verilerini, veri bağlantı katmanı bilgilerini, protokolleri ve her çerçeve için açıklamaları içerir. Çoğu protokol çözümleyicisi, belirli kriterleri karşılayan trafiği filtreleyebilir, böylece bir cihaza gelen ve giden tüm trafik yakalanabilir. Wireshark gibi protokol çözümleyicileri, ağ performansı sorunlarını gidermeye yardımcı olabilir. Her bir TCP / IP katmanındaki bilgileri incelemek için hem TCP / IP'yi hem de bir protokol çözümleyicisinin nasıl kullanılacağını iyi anlamak önemlidir.

## 41.4.Ağ Sorunlarının Belirtileri ve Nedenleri

### 41.4.1.Fiziksel Katman Sorunlarını Giderme

Bir ağdaki sorunlar genellikle performans sorunları olarak ortaya çıkar. Performans sorunları, beklenen davranış ile gözlemlenen davranış arasında bir fark olduğu ve sistemin makul şekilde beklendiği gibi çalışmadığı anlamına gelir. Fiziksel katmandaki arızalar ve yetersiz koşullar, kullanıcıları rahatsız etmekle kalmaz, aynı zamanda tüm şirketin üretkenliğini de etkileyebilir. Bu tür koşullarla karşılaşan ağlar genellikle kapanır. OSI modelinin üst katmanlarının çalışması fiziksel katmana bağlı olduğundan, bir ağ yöneticisinin bu katmandaki sorunları etkili bir şekilde izole etme ve düzeltme becerisine sahip olması gerekir.

Şekil, fiziksel katman ağı sorunlarının semptomlarını ve nedenlerini özetlemektedir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Tablo, fiziksel katman ağı sorunlarının genel belirtilerini listeler.

| Semptom | Açıklama |
|---|---|
| **Başlangıçtan daha düşük performans** | • Karşılaştırma için önceki temelleri gerektirir.<br>• Yavaş veya zayıf performansın en yaygın nedenleri arasında aşırı yüklenmiş veya yetersiz güç verilen sunucular, uygun olmayan anahtar veya yönlendirici yapılandırmaları, düşük kapasiteli bir bağlantıda trafik sıkışıklığı ve kronik çerçeve kaybı yer alır. |
| **Bağlantı kaybı** | • Bağlantı kaybı, arızalı veya bağlantısı kesilmiş bir kablodan kaynaklanıyor olabilir.<br>• Basit bir ping testi kullanılarak doğrulanabilir.<br>• Kesintili bağlantı kaybı, gevşek veya oksitlenmiş bir bağlantı olduğunu gösterebilir. |
| **Ağ darboğazları veya tıkanıklığı** | • Bir yönlendirici, arabirim veya kablo arızalanırsa, yönlendirme protokolleri trafiği ekstra kapasiteyi taşımak üzere tasarlanmamış diğer yollara yönlendirebilir.<br>• Bu, ağın bazı bölümlerinde tıkanıklığa veya darboğazlara neden olabilir. |
| **Yüksek CPU kullanım oranları** | • Yüksek CPU kullanım oranları, yönlendirici, anahtar veya sunucu gibi bir aygıtın tasarım sınırlarında çalıştığının veya bunları aştığının bir belirtisidir.<br>• Hızlı bir şekilde ele alınmazsa, CPU aşırı yüklemesi bir aygıtın kapanmasına veya arızalanmasına neden olabilir. |
| **Konsol hata mesajları** | • Aygıt konsolunda bildirilen hata mesajları, fiziksel bir katman sorununu gösterebilir.<br>• Konsol mesajları, merkezi bir sistem günlüğü sunucusuna kaydedilmelidir. |

Tablo, fiziksel katmanda yaygın olarak ağ sorunlarına neden olan sorunları listelemektedir.

| Problem Nedeni | Açıklama |
|---|---|
| **Güçle ilgili** | • Bu, ağ arızasının en temel nedenidir.<br>• Fanların çalışmasını kontrol edin ve kasa girişi ve egzoz havalandırma deliklerinin açık olduğundan emin olun.<br>• Yakındaki diğer ünitelerin de gücü kesildiyse, ana güç kaynağında bir güç kesintisinden şüphelenin. |
| **Donanım hataları** | • Hatalı ağ arabirim kartları (NIC'ler), geç çakışmalar, kısa çerçeveler ve sarsıntı nedeniyle ağ aktarım hatalarının nedeni olabilir.<br>• Jabber, genellikle bir ağ cihazının sürekli olarak rastgele, anlamsız verileri ağa ilettiği durum olarak tanımlanır.<br>• Jabber'ın diğer olası nedenleri, hatalı veya bozuk NIC sürücü dosyaları, bozuk kablolama veya topraklama sorunlarıdır. |
| **Kablolama hataları** | • Çoğu sorun, kısmen bağlantısı kesilen kabloları yeniden yerleştirerek düzeltilebilir.<br>• Fiziksel bir inceleme gerçekleştirirken, hasarlı kablolar, uygun olmayan kablo türleri ve kötü kıvrılmış RJ-45 konektörleri arayın.<br>• Şüpheli kablolar test edilmeli veya çalıştığı bilinen bir kabloyla değiştirilmelidir. |
| **Zayıflama** | • Bir kablo uzunluğu ortam için tasarım sınırını aşarsa veya gevşek bir kablo veya kirli veya oksitlenmiş kontaklardan kaynaklanan zayıf bir bağlantı olduğunda zayıflamaya neden olabilir.<br>• Zayıflama şiddetli ise, alıcı cihaz her zaman veri akışındaki bir biti başka bir bitten başarılı bir şekilde ayırt edemez. |
| **gürültü, ses** | • Yerel elektromanyetik girişim (EMI) genellikle gürültü olarak bilinir.<br>• FM radyo istasyonları, polis telsizi, bina güvenliği ve otomatik iniş için aviyonikler, karışma (aynı yoldaki diğer kabloların veya bitişik kabloların neden olduğu gürültü), yakındaki elektrik kabloları, büyük elektrikli cihazlar gibi birçok kaynaktan gürültü üretilebilir. motorlar veya cep telefonundan daha güçlü bir verici içeren herhangi bir şey. |
| **Arayüz yapılandırma hataları** | • Hatalı saat hızı, yanlış saat kaynağı ve arayüzün açılmaması gibi birçok şey, arayüzde arızalanmasına neden olacak şekilde yanlış yapılandırılabilir.<br>• Bu, bağlı ağ segmentleriyle bağlantı kaybına neden olur. |
| **Tasarım sınırlarının aşılması** | • Bir bileşen, spesifikasyonların veya yapılandırılmış kapasitenin ötesinde kullanıldığı için fiziksel katmanda alt-optimal olarak çalışıyor olabilir.<br>• Bu tür bir problemi giderirken, cihaz için kaynakların maksimum kapasitede veya yakınında çalıştığı ve arayüz hatalarının sayısında bir artış olduğu ortaya çıkar. |
| **CPU aşırı yükü** | • Belirtiler arasında yüksek CPU kullanım yüzdelerine sahip işlemler, giriş sırası düşüşleri, yavaş performans, SNMP zaman aşımları, uzaktan erişim yok veya DHCP, Telnet ve ping gibi hizmetler yavaş veya yanıt vermiyor.<br>• Bir anahtarda şunlar meydana gelebilir: ağaç yeniden birleştirme, EtherChannel bağlantılarının geri dönmesi, UDLD dalgalanması, IP SLA hataları.<br>• Yönlendiriciler için, yönlendirme güncellemeleri, yol kanat çırpma veya HSRP kanat çırpma olamaz.<br>• Bir yönlendiricide veya anahtarda CPU aşırı yüklenmesinin nedenlerinden biri yüksek trafiktir.<br>• Bir veya daha fazla arabirim düzenli olarak trafikle aşırı yüklenmişse, ağdaki trafik akışını yeniden tasarlamayı veya donanımı yükseltmeyi düşünün. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 41.4.2.Veri Bağlantısı Katmanı Sorunlarını Giderme

Katman 2 sorunlarının giderilmesi zorlu bir süreç olabilir. Bu protokollerin yapılandırılması ve çalışması, işlevsel, iyi ayarlanmış bir ağ oluşturmak için kritik öneme sahiptir. 2. Katman sorunları, fark edildiğinde sorunun hızlı bir şekilde tanımlanmasına yardımcı olacak belirli semptomlara neden olur.

Şekil, veri bağlantı katmanı ağ sorunlarının semptomlarını ve nedenlerini özetlemektedir.

Tablo, veri bağlantı katmanı ağ sorunlarının genel belirtilerini listeler.

| Semptom | Açıklama |
|---|---|
| **Ağ katmanında veya üstünde işlevsellik veya bağlantı yok** | Bazı Katman 2 sorunları, bir bağlantı üzerinden çerçeve alışverişini durdurabilirken, diğerleri yalnızca ağ performansının düşmesine neden olabilir. |
| **Ağ, temel performans seviyelerinin altında çalışıyor** | • Bir ağda meydana gelebilecek iki farklı tipte uygun olmayan Katman 2 işlemi vardır.<br>• İlk olarak, çerçeveler hedeflerine ulaşmak için yetersiz bir yol alırlar ancak ulaşırlar ve bu da ağın bağlantılarda beklenmedik yüksek bant genişliği kullanımı yaşamasına neden olur.<br>• İkinci olarak, bazı çerçeveler, anahtar veya yönlendiricide görünen hata sayacı istatistikleri ve konsol hata iletileri aracılığıyla tanımlandığı gibi atılır.<br>• Genişletilmiş veya sürekli bir ping, çerçevelerin düşüp düşmediğini ortaya çıkarmaya yardımcı olabilir. |
| **Aşırı yayın** | • İşletim sistemleri, ağ hizmetlerini ve diğer ana bilgisayarları keşfetmek için yaygın olarak yayınları ve çok noktaya yayınları kullanır.<br>• Genel olarak, aşırı yayınlar, kötü programlanmış veya yapılandırılmış bir uygulamaların, büyük bir Katman 2 yayın alanının veya temelde yatan bir ağ sorununun (örneğin, STP döngüleri veya rota dalgalanması) sonucudur. |
| **Konsol mesajları** | • Bir yönlendirici, Katman 2 sorununun oluştuğunu anlar ve konsola uyarı mesajları gönderir.<br>• Tipik olarak, bir yönlendirici bunu gelen karelerin yorumlanmasında bir sorun algıladığında (kapsülleme veya çerçeveleme sorunları) veya bekletme beklendiğinde ancak ulaşmadığında yapar.<br>• Katman 2 sorununu gösteren en yaygın konsol mesajı, bir hat protokolü kapalı mesajıdır |

Tablo, veri bağlantı katmanında yaygın olarak ağ sorunlarına neden olan sorunları listeler.

| Problem Nedeni | Açıklama |
|---|---|
| **Kapsülleme hataları** | • Gönderici tarafından bir alana yerleştirilen bitler, alıcının görmeyi beklediği şeyler olmadığı için bir kapsülleme hatası oluşur.<br>• Bu durum, bir WAN bağlantısının bir ucundaki kapsülleme, diğer uçta kullanılan kapsüllemeden farklı şekilde yapılandırıldığında ortaya çıkar. |
| **Adres eşleme hataları** | • Noktadan çok noktaya veya yayın Ethernet gibi topolojilerde, çerçeveye uygun bir Katman 2 hedef adresinin verilmesi önemlidir. Bu, doğru varış noktasına varmasını sağlar.<br>• Bunu başarmak için, ağ cihazı bir hedef Katman 3 adresini statik veya dinamik haritalar kullanarak doğru Katman 2 adresiyle eşleştirmelidir.<br>• Dinamik bir ortamda, Katman 2 ve Katman 3 bilgilerinin eşlenmesi başarısız olabilir, çünkü cihazlar ARP isteklerine yanıt vermeyecek şekilde yapılandırılmış olabilir, önbelleğe alınan Katman 2 veya Katman 3 bilgileri fiziksel olarak değişmiş olabilir veya geçersiz ARP yanıtları yanlış yapılandırma veya güvenlik saldırısı nedeniyle alındı. |
| **Çerçeveleme hataları** | • Çerçeveler genellikle 8 bitlik bayt grupları halinde çalışır.<br>• Bir çerçeve 8 bitlik bir bayt sınırında bitmediğinde çerçeveleme hatası oluşur.<br>• Bu olduğunda, alıcı bir karenin nerede bittiğini ve başka bir karenin nerede başladığını belirlemekte sorun yaşayabilir.<br>• Çok fazla sayıda geçersiz çerçeve, geçerli tutma öğelerinin değiştirilmesini engelleyebilir.<br>• Çerçeveleme hatalarına, gürültülü bir seri hat, yanlış tasarlanmış bir kablo (çok uzun veya düzgün korumalı olmayan), hatalı NIC, çift yönlü uyumsuzluk veya yanlış yapılandırılmış kanal servis birimi (CSU) hat saati neden olabilir. |

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| | |
|---|---|
| **STP hataları veya döngüleri** | • Yayılan Ağaç Protokolünün (STP) amacı, yedekli bağlantı noktalarını bloke ederek yedekli bir fiziksel topolojiyi ağaç benzeri bir topolojiye dönüştürmektir.<br>• Çoğu STP sorunu, yedekli bir topolojide hiçbir bağlantı noktası engellenmediğinde ve trafik süresiz olarak daireler halinde iletildiğinde ortaya çıkan yönlendirme döngüleri ile ilgilidir. Bu, yüksek oranda STP topolojisi değişiklikleri nedeniyle aşırı taşmaya neden olur.<br>• İyi yapılandırılmış bir ağda topoloji değişikliği nadir bir olay olmalıdır.<br>• İki anahtar arasındaki bir bağlantı yukarı veya aşağı gittiğinde, bağlantı noktasının STP durumu yönlendirmeye veya yönlendirmeden değiştiğinde sonunda bir topoloji değişikliği olur.<br>• Bununla birlikte, bir bağlantı noktası kanat çırptığında (yukarı ve aşağı durumlar arasında salınım yaparken), bu, tekrarlayan topoloji değişikliklerine ve taşmasına veya yavaş STP yakınsamasına veya yeniden yakınsamaya neden olur.<br>• Bunun nedeni gerçek ve belgelenmiş topoloji arasındaki uyumsuzluk, STP zamanlayıcılarının tutarsız konfigürasyonu gibi bir konfigürasyon hatası, yakınsama sırasında aşırı yüklenmiş bir anahtar CPU'su veya bir yazılım hatası olabilir. |

## 41.4.3.Ağ Katmanı Sorunlarını Giderme

Ağ katmanı sorunları, IPv4, IPv6, EIGRP, OSPF vb. Gibi Katman 3 protokolü içeren herhangi bir sorunu içerir. Şekil, ağ katmanı ağ sorunlarının semptomlarını ve nedenlerini özetler.

Tablo, ağ katmanı ağ sorunlarının genel belirtilerini listeler.

| Semptom | Açıklama |
|---|---|
| **Ağ hatası** | • Ağ arızası, ağın neredeyse veya tamamen işlevsel olmaması ve ağdaki tüm kullanıcıları ve uygulamaları etkilemesidir.<br>• Bu arızalar genellikle kullanıcılar ve ağ yöneticileri tarafından hızlı bir şekilde fark edilir ve açıkça bir şirketin üretkenliği için kritiktir. |
| **Yetersiz performans** | • Ağ optimizasyonu sorunları genellikle bir kullanıcı, uygulama, hedef veya bir trafik türü alt kümesini içerir.<br>• Optimizasyon sorunlarını tespit etmek ve hatta izole etmek ve teşhis etmek daha zor olabilir.<br>• Bunun nedeni, genellikle birden çok katmanı veya hatta tek bir ana bilgisayarı içermesidir.<br>• Sorunun bir ağ katmanı sorunu olduğunu belirlemek zaman alabilir. |

Çoğu ağda, statik yollar dinamik yönlendirme protokolleri ile birlikte kullanılır. Statik yolların yanlış yapılandırılması, optimumun altında yönlendirmeye neden olabilir. Bazı durumlarda, yanlış yapılandırılmış statik yollar, ağın bazı bölümlerine erişilemez hale getiren yönlendirme döngüleri oluşturabilir.

Dinamik yönlendirme protokollerinde sorun giderme, belirli yönlendirme protokolünün nasıl çalıştığının tam olarak anlaşılmasını gerektirir. Bazı sorunlar tüm yönlendirme protokollerinde ortaktır, diğer sorunlar ise bireysel yönlendirme protokolüne özgüdür.

Katman 3 problemlerini çözmek için tek bir şablon yoktur. Yönlendirme sorunları, sorunu izole etmek ve teşhis etmek için bir dizi komut kullanılarak metodik bir süreçle çözülür.

Tablo, yönlendirme protokollerini içeren olası bir sorunu teşhis ederken keşfedilecek alanları listeler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Problem Nedeni | Açıklama |
|---|---|
| **Genel ağ sorunları** | • Genellikle topolojideki bir aşağı bağlantı gibi bir değişikliğin, ağın diğer alanları üzerinde o sırada açık olmayabilecek etkileri olabilir.<br>• Bu, statik veya dinamik yeni rotaların kurulumunu veya diğer rotaların kaldırılmasını içerebilir.<br>• Ağdaki herhangi bir şeyin yakın zamanda değişip değişmediğini ve şu anda ağ altyapısı üzerinde çalışan biri olup olmadığını belirleyin. |
| **Bağlantı sorunları** | • Kesintiler ve çevre sorunları (örneğin, aşırı ısınma) gibi güç sorunları dahil olmak üzere herhangi bir ekipman ve bağlantı sorununu kontrol edin.<br>• Kablolama sorunları, bozuk bağlantı noktaları ve ISP sorunları gibi Katman 1 sorunlarını da kontrol edin. |
| **Yönlendirme tablosu** | • Eksik yollar veya beklenmedik yollar gibi beklenmedik herhangi bir şey için yönlendirme tablosunu kontrol edin.<br>• Yönlendirme güncellemelerini ve yönlendirme tablosu bakımını görüntülemek için **hata ayıklama** komutlarını kullanın . |
| **Komşu sorunları** | Yönlendirme protokolü bir komşuyla bir bitişiklik kurarsa, komşu komşuları oluşturan yönlendiricilerde herhangi bir sorun olup olmadığını kontrol edin. |
| **Topoloji veritabanı** | Yönlendirme protokolü bir topoloji tablosu veya veritabanı kullanıyorsa, eksik girişler veya beklenmeyen girişler gibi beklenmedik herhangi bir şey için tabloyu kontrol edin. |

## 41.4.4.Taşıma Katmanı Sorunlarını Giderme - ACL'ler

Ağ sorunları, yönlendiricideki, özellikle trafiğin incelendiği ve değiştirildiği ağın ucundaki taşıma katmanı sorunlarından kaynaklanabilir. Örneğin, hem erişim kontrol listeleri (ACL'ler) hem de Ağ Adres Çevirisi (NAT), ağ katmanında çalışır ve şekilde gösterildiği gibi, taşıma katmanındaki işlemleri içerebilir.

ACL'lerle ilgili sorunlar, aksi takdirde çalışan sistemlerin başarısız olmasına neden olabilir. Tablo, yanlış yapılandırmaların sıklıkla meydana geldiği alanları listeler.

| Yanlış yapılandırmalar | Açıklama |
|---|---|
| **Trafik akışının seçimi** | • Trafik, hem trafiğin gittiği yönlendirici arayüzü hem de bu trafiğin gittiği yön tarafından tanımlanır.<br>• Doğru arayüze bir ACL uygulanmalı ve düzgün çalışması için doğru trafik yönü seçilmelidir. |
| **Erişim kontrol girişlerinin sırası** | • ACL'deki girişler özelden genele doğru olmalıdır.<br>• Bir ACL, bir tür trafik akışına özel olarak izin veren bir girdiye sahip olsa da, paketler listenin önceki başka bir girdisi tarafından reddediliyorsa, bu girdiyle asla eşleşmez.<br>• Yönlendirici hem ACL'leri hem de NAT'ı çalıştırıyorsa, bu teknolojilerin her birinin bir trafik akışına uygulanma sırası önemlidir.<br>• Gelen trafik, dışarıdan içeriye NAT tarafından işlenmeden önce gelen ACL tarafından işlenir.<br>• Giden trafik, içeriden dışarıya NAT tarafından işlendikten sonra giden ACL tarafından işlenir. |
| Örtük red | ACL'de yüksek güvenlik gerekli olmadığında, bu örtük erişim denetimi öğesi, ACL yanlış yapılandırmasının nedeni olabilir. |
| **Adresler ve IPv4 joker karakter maskeleri** | • Karmaşık IPv4 joker karakter maskeleri, verimlilikte önemli gelişmeler sağlar, ancak daha çok yapılandırma hatalarına tabidir.<br>• Karmaşık joker karakter maskesine bir örnek, 10.0.0.0 ağında veya 10.0.32.0 ağında ilk 15 ana bilgisayar adresini seçmek için IPv4 adresi 10.0.32.0 ve joker karakter maskesi 0.0.32.15 kullanmaktır. |
| **Taşıma katmanı protokolünün seçimi** | • ACL'leri yapılandırırken, yalnızca doğru taşıma katmanı protokollerinin belirtilmesi önemlidir.<br>• Çoğu ağ yöneticisi, bir trafik akışı türünün TCP bağlantı noktası mı yoksa UDP bağlantı noktası mı kullandığından emin olmadığında, her ikisini de yapılandırır.<br>• Her ikisinin de belirtilmesi, güvenlik duvarında bir delik açar ve muhtemelen davetsiz misafirlere ağda bir yol sağlar.<br>• Ayrıca ACL'ye fazladan bir öğe ekler, böylece ACL'nin işlenmesi daha uzun sürer ve ağ iletişimlerinde daha fazla gecikme sağlar. |

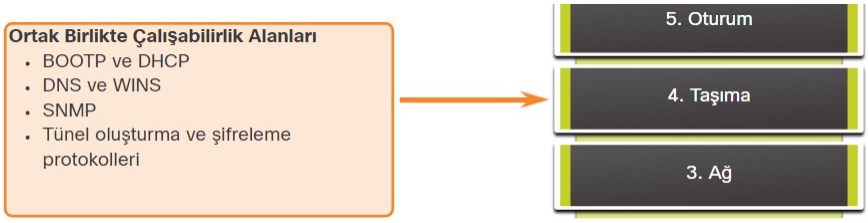
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| | |
|---|---|
| **Kaynak ve hedef bağlantı noktaları** | • İki ana bilgisayar arasındaki trafiğin düzgün şekilde kontrol edilmesi, gelen ve giden ACL'ler için simetrik erişim kontrol öğeleri gerektirir.<br>• Yanıt veren bir ana bilgisayar tarafından oluşturulan trafik için adres ve bağlantı noktası bilgileri, başlatan ana bilgisayar tarafından oluşturulan trafiğe yönelik adres ve bağlantı noktası bilgilerinin ayna görüntüsüdür. |
| **Yerleşik anahtar kelimenin kullanımı** | • **Kurulan** anahtar bir ACL tarafından sağlanan güvenliği artırır.<br>• Ancak, anahtar kelime yanlış uygulanırsa beklenmedik sonuçlar ortaya çıkabilir. |
| **Yaygın olmayan protokoller** | • Yanlış yapılandırılmış ACL'ler genellikle TCP ve UDP dışındaki protokollerde sorunlara neden olur.<br>• Popülerlik kazanan nadir protokoller, VPN ve şifreleme protokolleridir. |

## 41.4.5.Aktarım Katmanı Sorunlarını Giderme - IPv4 için NAT

NAT ile ilgili, DHCP ve tünelleme gibi hizmetlerle etkileşime girmeme gibi çeşitli sorunlar vardır. Bunlar, içinde yanlış yapılandırılmış NAT, dışarıda NAT veya ACL'leri içerebilir. Diğer sorunlar, diğer ağ teknolojileriyle, özellikle de paketteki ana bilgisayar ağ adreslemesinden bilgi içeren veya türetenler ile birlikte çalışabilirliği içerir.

Şekil, NAT ile ortak birlikte çalışabilirlik alanlarını özetler.




Tablo, NAT ile ortak çalışabilirlik alanlarını listeler.

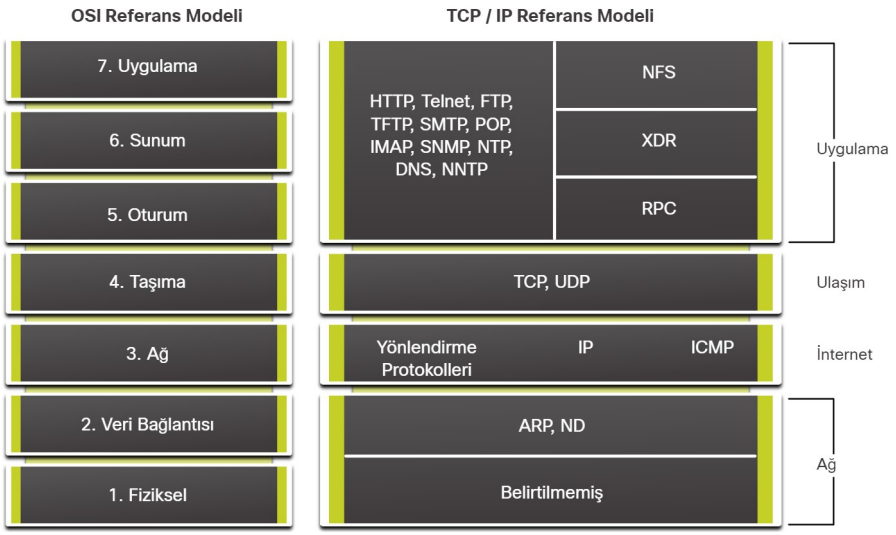
| Protokol | Açıklama |
|---|---|
| **BOOTP ve DHCP** | • Her iki protokol de IPv4 adreslerinin istemcilere otomatik olarak atanmasını yönetir.<br>• Yeni bir istemcinin gönderdiği ilk paketin bir DHCP-İstek yayın IPv4 paketi olduğunu hatırlayın.<br>• DHCP-İstek paketinin kaynak IPv4 adresi 0.0.0.0'dır.<br>• NAT hem geçerli bir hedef hem de kaynak IPv4 adresi gerektirdiğinden, BOOTP ve DHCP, statik veya dinamik NAT çalıştıran bir yönlendirici üzerinden çalışırken zorluk yaşayabilir.<br>• IPv4 yardımcı özelliğini yapılandırmak bu sorunu çözmeye yardımcı olabilir. |
| **DNS** | • Dinamik NAT çalıştıran bir yönlendirici, tablo girişlerinin süresi doldukça ve yeniden oluşturuldukça iç ve dış adresler arasındaki ilişkiyi düzenli olarak değiştirdiğinden, NAT yönlendiricisinin dışındaki bir DNS sunucusu, yönlendirici içindeki ağın doğru bir temsiline sahip değildir.<br>• IPv4 yardımcı özelliğini yapılandırmak bu sorunu çözmeye yardımcı olabilir. |
| **SNMP** | • DNS paketleri gibi NAT, paketin veri yükünde depolanan adresleme bilgilerini değiştiremez.<br>• Bu nedenle, bir NAT yönlendiricisinin bir tarafındaki bir SNMP yönetim istasyonu, NAT yönlendiricisinin diğer tarafındaki SNMP aracılarıyla iletişim kuramayabilir.<br>• IPv4 yardımcı özelliğini yapılandırmak bu sorunu çözmeye yardımcı olabilir. |
| **Tünel oluşturma ve şifreleme protokolleri** | • Şifreleme ve tünel oluşturma protokolleri genellikle trafiğin belirli bir UDP veya TCP bağlantı noktasından kaynaklanmasını veya taşıma katmanında NAT tarafından işlenemeyen bir protokol kullanılmasını gerektirir.<br>• Örneğin, IPsec tünel oluşturma protokolleri ve VPN uygulamaları tarafından kullanılan genel yönlendirme kapsülleme protokolleri NAT tarafından işlenemez. |

## 41.4.6.Uygulama Katmanı Sorunlarını Giderme

Uygulama katmanı protokollerinin çoğu kullanıcı hizmetleri sağlar. Uygulama katmanı protokolleri genellikle ağ yönetimi, dosya aktarımı, dağıtılmış dosya hizmetleri, terminal oturumu ve e-posta için kullanılır. Genellikle VPN'ler ve VoIP gibi yeni kullanıcı hizmetleri eklenir.

Licensed to yasin karasungur, yasinkarsungur@yahoo.com

Şekil, en yaygın olarak bilinen ve uygulanan TCP / IP uygulama katmanı protokollerini göstermektedir.




Tablo, bu uygulama katmanı protokollerinin kısa bir açıklamasını sağlar.

| Uygulamalar | Açıklama |
|---|---|
| **SSH / Telnet** | Kullanıcıların uzak ana bilgisayarlarla terminal oturumu bağlantıları kurmasını sağlar. |
| **HTTP** | Web üzerinde metin, grafik görüntü, ses, video ve diğer multimedya dosyalarının alışverişini destekler. |
| **FTP** | Ana bilgisayarlar arasında etkileşimli dosya aktarımları gerçekleştirir. |
| **TFTP** | Genellikle ana bilgisayarlar ve ağ aygıtları arasında temel etkileşimli dosya aktarımlarını gerçekleştirir. |
| **SMTP** | Temel mesaj teslim hizmetlerini destekler. |
| **POP** | Posta sunucularına bağlanır ve e-postayı indirir. |
| **SNMP** | Ağ cihazlarından yönetim bilgilerini toplar. |
| **DNS** | IP adreslerini ağ cihazlarına atanan adlarla eşler. |
| **Ağ Dosya Sistemi (NFS)** | Bilgisayarların sürücüleri uzak ana bilgisayarlara takmasına ve bunları yerel sürücülermiş gibi çalıştırmasına olanak tanır. Başlangıçta Sun Microsystems tarafından geliştirilmiş, uzak ağ kaynaklarına şeffaf erişim sağlamak için diğer iki uygulama katmanı protokolünü, harici veri gösterimini (XDR) ve uzaktan yordam çağrısını (RPC) birleştirir. |

Semptom türleri ve nedenleri gerçek uygulamanın kendisine bağlıdır.

Uygulama katmanı sorunları, hizmetlerin uygulama programlarına sağlanmasını engeller. Uygulama katmanındaki bir sorun, fiziksel, veri bağlantısı, ağ ve taşıma katmanları işlevsel olduğunda erişilemez veya kullanılamaz kaynaklara neden olabilir. Tam ağ bağlantısına sahip olmak mümkündür, ancak uygulama basitçe veri sağlayamaz.

Uygulama katmanındaki başka bir problem türü, fiziksel, veri bağlantısı, ağ ve taşıma katmanları işlevsel olduğunda, ancak tek bir ağ hizmetinden veya uygulamasından ağ hizmetlerine yönelik veri aktarımı ve talepleri kullanıcının normal beklentilerini karşılamadığında ortaya çıkar.

Uygulama katmanındaki bir sorun, kullanıcıların veri aktarırken veya ağ hizmetleri talep ederken ağın veya birlikte çalıştıkları bir uygulamanın yavaş veya normalden daha yavaş olduğundan şikayet etmelerine neden olabilir.

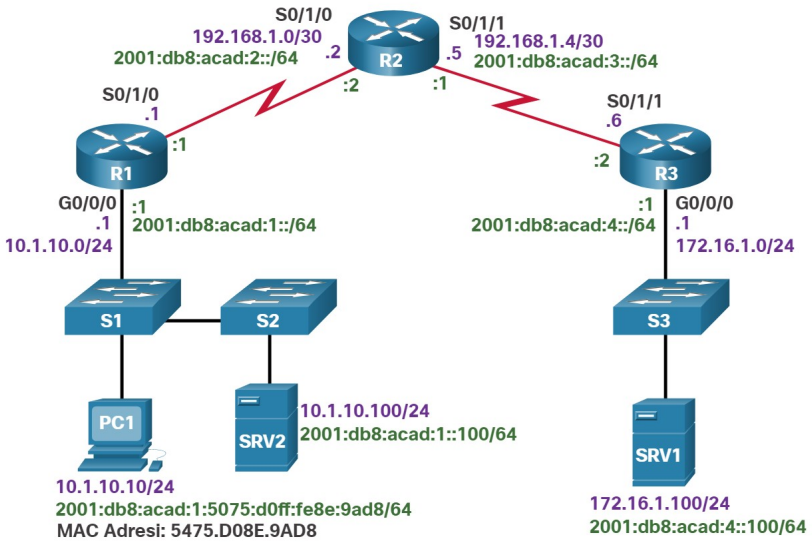
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 41.5.IP Bağlantısı Sorunlarını Giderme

### 41.5.1.Uçtan Uca Bağlantı Sorunlarını Giderme Bileşenleri

Bu konu, tek bir topoloji ve uçtan uca bir bağlantı sorununu teşhis etmek ve bazı durumlarda çözmek için araçlar sunar. Sorunları teşhis etmek ve çözmek, ağ yöneticileri için önemli bir beceridir. Sorun giderme için tek bir tarif yoktur ve bir sorun birçok şekilde teşhis edilebilir. Bununla birlikte, sorun giderme sürecine yapılandırılmış bir yaklaşım uygulayarak, bir yönetici bir sorunu teşhis etmek ve çözmek için gereken süreyi azaltabilir.

Bu konu boyunca aşağıdaki senaryo kullanılmaktadır. İstemci ana bilgisayarı PC1, Sunucu SRV1 veya Sunucu SRV2 üzerindeki uygulamalara erişemez. Şekil bu ağın topolojisini göstermektedir. PC1, IPv6 global tek noktaya yayın adresini oluşturmak için EUI-64 ile SLAAC kullanır. EUI-64, Ethernet MAC adresini kullanarak, ortasına FFFE ekleyerek ve yedinci biti çevirerek Arayüz Kimliği oluşturur




Uçtan uca bağlantı olmadığında ve yönetici aşağıdan yukarıya bir yaklaşımla sorun gidermeyi seçtiğinde, yöneticinin alabileceği genel adımlar şunlardır:

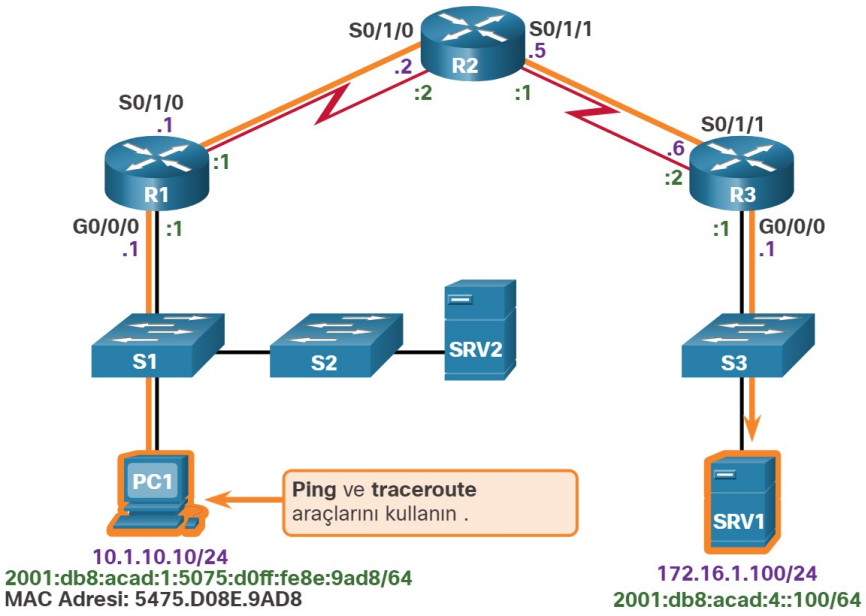
Adım 1. Ağ iletişiminin durduğu noktada fiziksel bağlantıyı kontrol edin. Buna kablolar ve donanım da dahildir. Sorun, hatalı bir kablo veya arabirimde olabilir veya yanlış yapılandırılmış veya hatalı donanımla ilgili olabilir.
Adım 2. Dubleks uyumsuzluklarını kontrol edin.
Adım 3. Yerel ağdaki veri bağlantısını ve ağ katmanı adreslemesini kontrol edin. Bu, IPv4 ARP tablolarını, IPv6 komşu tablolarını, MAC adres tablolarını ve VLAN atamalarını içerir.
Adım 4. Varsayılan ağ geçidinin doğru olduğunu doğrulayın.
Adım 5. Cihazların kaynaktan hedefe doğru yolu belirlediğinden emin olun. Gerekirse yönlendirme bilgilerini değiştirin.
Adım 6.Taşıma katmanının düzgün çalıştığını doğrulayın. Telnet, komut satırından aktarım katmanı bağlantılarını test etmek için de kullanılabilir.
Adım 7. Trafiği engelleyen ACL'lerin olmadığını doğrulayın.
Adım 8. DNS ayarlarının doğru olduğundan emin olun. Erişilebilir bir DNS sunucusu olmalıdır.

Bu sürecin sonucu operasyonel, uçtan-uca bağlantıdır. Tüm adımlar herhangi bir çözüm olmadan gerçekleştirildiyse, ağ yöneticisi ya önceki adımları tekrarlamak ya da sorunu kıdemli bir yöneticiye iletmek isteyebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 41.5.2.Uçtan Uca Bağlantı Sorunu Sorun Giderme Başlangıcı

Genellikle bir sorun giderme çabasını başlatan şey, uçtan uca bağlantıyla ilgili bir sorun olduğunu keşfetmektir. Uçtan uca bağlantıyla ilgili bir sorunu doğrulamak için kullanılan en yaygın yardımcı programlardan ikisi , şekilde gösterildiği gibi ping ve traceroute'dur .




### IPv4 ping

Ping, muhtemelen ağ oluşturmada en çok bilinen bağlantı testi aracıdır ve her zaman Cisco IOS Yazılımının bir parçası olmuştur. Belirtilen bir ana bilgisayar adresinden yanıt istekleri gönderir. Ping komutu ICMP denilen TCP / IP paketinin bir parçası olan bir Layer 3 protokolünü kullanır. Ping, ICMP yankı isteğini ve ICMP yankı yanıt paketlerini kullanır. Belirtilen adresteki ana bilgisayar ICMP yankı talebini alırsa, bir ICMP yankı yanıt paketi ile yanıt verir. Ping, hem IPv4 hem de IPv6 için uçtan uca bağlantıyı doğrulamak için kullanılabilir. Komut çıkışı, 172.16.1.100 adresinde PC1'den SRV1'e başarılı bir ping gösterir.

```
C:\> ping 172.16.1.100
Pinging 172.16.1.100 with 32 bytes of data:
Reply from 172.16.1.100: bytes=32 time=199ms TTL=128
Reply from 172.16.1.100: bytes=32 time=193ms TTL=128
Reply from 172.16.1.100: bytes=32 time=194ms TTL=128
Reply from 172.16.1.100: bytes=32 time=196ms TTL=128
Ping statistics for 172.16.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 193ms, Maximum = 199ms, Average = 195ms
C:\>
```

### IPv4 Traceroute

Gibi ping komutu, Cisco IOS traceroute komutu IPv4 ve IPv6 ikisi için de kullanılabilir. Tracert komutu, Windows işletim sistemleri kullanılır. İzleme, yol boyunca başarıyla ulaşılan atlamaların, yönlendirici IP adreslerinin ve hedef IP adresinin bir listesini oluşturur. Bu liste, önemli doğrulama ve sorun giderme bilgileri sağlar. Veriler hedefe ulaşırsa, iz, yoldaki her yönlendiricideki arabirimi listeler. Veriler yol boyunca bir sıçramada başarısız olursa, izlemeye yanıt veren son yönlendiricinin adresi bilinir. Bu adres, sorunun veya güvenlik kısıtlamalarının nerede bulunduğunun bir göstergesidir.

Tracert çıktısı IPv4 paketler hedeflerine geçtikleri yolu göstermektedir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```
C:\> tracert 172.16.1.100
Tracing route to 172.16.1.100 over a maximum of 30 hops:
  1     1 ms    <1 ms    <1 ms  10.1.10.1
  2     2 ms     2 ms     1 ms  192.168.1.2
  3     2 ms     2 ms     1 ms  192.168.1.6
  4     2 ms     2 ms     1 ms  172.16.1.100
Trace complete.
C:\>
```

### IPv6 ping ve traceroute

Bu yardımcı programları kullanırken, Cisco IOS yardımcı programı, adresin bir IPv4 veya IPv6 adresi olup olmadığını algılar ve bağlantıyı test etmek için uygun protokolü kullanır. Komut çıktısı, IPv6 bağlantısını test etmek için kullanılan yönlendirici R1 üzerindeki ping ve traceroute komutlarını gösterir .

```
R1# ping 2001:db8:acad:4::100
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:4::100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/56 ms
R1#
R1# traceroute 2001:db8:acad:4::100
Type escape sequence to abort.
Tracing the route to 2001:DB8:ACAD:4::100
1.   2001:DB8:ACAD:2::2 20 msec 20 msec 20 msec
2.   2001:DB8:ACAD:3::2 44 msec 40 msec 40 msec
R1#
```

### Adım 1 - Fiziksel Katmanı Doğrulayın

Tüm ağ cihazları özel bilgisayar sistemleridir. En azından, bu cihazlar bir CPU, RAM ve depolama alanından oluşur ve cihazın işletim sistemini ve arayüzleri önyüklemesine ve çalıştırmasına izin verir. Bu, ağ trafiğinin alınmasına ve iletilmesine izin verir. Bir ağ yöneticisi, belirli bir aygıtta bir sorun olduğunu ve bu sorunun donanımla ilgili olabileceğini belirlediğinde, bu genel bileşenlerin işleyişini doğrulamak faydalı olacaktır. Bu amaçla en sık kullanılan Cisco IOS komutları, show processes cpu, show memory, and show interfaces.

Performansla ilgili sorunların giderilmesi ve donanımın hatalı olduğundan şüphelenildiğinde , trafiğin geçtiği arayüzleri doğrulamak için show interfaces komutu kullanılabilir.

**Show interfaces** komutunun komut çıktısına bakın .

```
R1# show interfaces GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c0(bia d48c.b5ce.a0c0)
Internet address is 10.1.10.1/24
(Output omitted)
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
 Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
85 packets input, 7711 bytes, 0 no buffer
Received 25 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 5 multicast, 0 pause input
10112 packets output, 922864 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
11 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 pause output
0 output buffer failures, 0 output buffers swapped out
R1#
```

Input queue drops

Giriş kuyruğu düşüşleri (ve ilgili göz ardı edilen ve kısma sayaçları), bir noktada yönlendiriciye işleyebileceğinden daha fazla trafiğin teslim edildiğini gösterir. Bu mutlaka bir sorun olduğu anlamına gelmez. Bu, yoğun dönemlerde normal trafik olabilir. Bununla birlikte, CPU'nun paketleri zamanında işleyemediğinin bir göstergesi olabilir, bu nedenle bu sayı sürekli olarak yüksekse, bu sayaçların hangi anlarda arttığını ve bunun CPU kullanımıyla nasıl ilişkili olduğunu bulmaya çalışmak faydalı olacaktır.

Output queue drops

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Çıkış kuyruğu düşüşleri, arayüzdeki tıkanıklık nedeniyle paketlerin düştüğünü gösterir. Toplam girdi trafiğinin çıktı trafiğinden daha yüksek olduğu herhangi bir noktada çıktı düşüşlerini görmek normaldir. Yoğun trafik

dönemlerinde, trafik arayüze gönderilebileceğinden daha hızlı teslim edilirse paketler atılır. Ancak, bu normal bir davranış olarak kabul edilse bile, paket düşüşlerine ve kuyruğa alma gecikmelerine yol açar, bu nedenle, VoIP gibi bunlara duyarlı uygulamalar performans sorunlarından muzdarip olabilir. Sürekli olarak çıktı kuyruğu düşüşlerini görmek, QoS'yi uygulamak veya değiştirmek için gelişmiş bir kuyruk mekanizması uygulamanız gerektiğinin bir göstergesi olabilir.

Input Errors

Giriş hataları, CRC hataları gibi çerçevenin alınması sırasında yaşanan hataları gösterir. Çok sayıda CRC hatası, kablolama sorunlarını, arabirim donanım sorunlarını veya Ethernet tabanlı bir ağda çift yönlü uyumsuzlukları gösterebilir.

Output Errors

Çıktı hataları, bir çerçevenin iletimi sırasında çarpışmalar gibi hataları gösterir. Günümüzde çoğu Ethernet tabanlı ağda, tam çift yönlü iletim normdur ve yarı çift yönlü iletim istisnadır. Tam çift yönlü iletimde, işlem çakışmaları meydana gelemez; bu nedenle, çarpışmalar (özellikle geç çarpışmalar) genellikle çift yönlü uyumsuzlukları gösterir.

**Adım 2 - Dubleks Uyumsuzluklarını Kontrol Edin**

Arabirim hatalarının diğer bir yaygın nedeni, bir Ethernet bağlantısının iki ucu arasındaki uyumsuz çift yönlü moddur. Pek çok Ethernet tabanlı ağda, noktadan noktaya bağlantılar artık norm haline geldi ve hub'ların kullanımı ve ilişkili yarı çift yönlü operasyon daha az yaygın hale geliyor. Bu, günümüzde çoğu Ethernet bağlantısının tam çift yönlü modda çalıştığı anlamına gelir ve bir Ethernet bağlantısı için çarpışmalar normal iken, günümüzde çarpışmalar genellikle çift yönlü anlaşmanın başarısız olduğunu veya bağlantının doğru çift yönlü modda çalışmadığını gösterir.

IEEE 802.3ab Gigabit Ethernet standardı, hız ve çift yönlü için otomatik anlaşmanın kullanılmasını zorunlu kılar. Ek olarak, kesinlikle zorunlu olmasa da, pratik olarak tüm Hızlı Ethernet NIC'leri de varsayılan olarak otomatik anlaşmayı kullanır. Hız ve çift yönlü için otomatik anlaşmanın kullanılması şu anda önerilen uygulamadır.

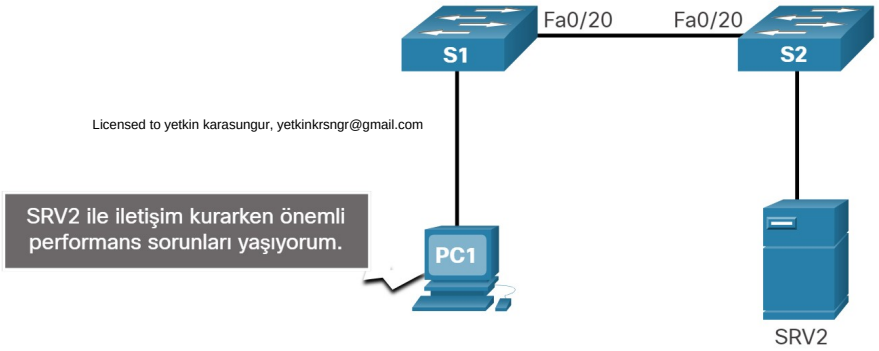
Bununla birlikte, herhangi bir nedenle çift yönlü görüşme başarısız olursa, hızı ve çift yönlü ayarı her iki uçta da manuel olarak ayarlamak gerekebilir. Tipik olarak bu, çift yönlü modun bağlantının her iki ucunda da tam çift yönlü olarak ayarlanması anlamına gelir. Bu işe yaramazsa, her iki uçta yarı çift yönlü çalıştırmak, çift yönlü uyumsuzluğa tercih edilir.

Çift yönlü yapılandırma yönergeleri şunları içerir:

- 
- Hız ve çift yönlü otomatik anlaşma önerilir.
- Otomatik anlaşma başarısız olursa, birbirine bağlanan uçlarda hızı ve çift yönlü ayarı manuel olarak ayarlayın.
- Noktadan noktaya Ethernet bağlantıları her zaman tam çift yönlü modda çalışmalıdır.
- Yarı çift yönlü yaygın değildir ve genellikle yalnızca eski hublar kullanıldığında karşılaşılır.

**Sorun Giderme Örneği**

Önceki senaryoda, ağ yöneticisinin ağa ek kullanıcılar eklemesi gerekiyordu. Bu yeni kullanıcıları dahil etmek için, ağ yöneticisi ikinci bir anahtar kurdu ve bunu ilkine bağladı. Ağa S2 eklendikten kısa bir süre sonra, her iki anahtardaki kullanıcılar, şekilde gösterildiği gibi diğer anahtardaki cihazlara bağlanırken önemli performans sorunları yaşamaya başladı.



Ağ yöneticisi, S2 anahtarında bir konsol mesajı fark eder:

```
*Mar 1 00:45:08.756: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on FastEthernet0/20 (not half
duplex), with Switch FastEthernet0/20 (half duplex).
```

**show interfaces fa 0/20** komutunu kullanarak, ağ yöneticisi S2'ye bağlanmak için kullanılan S1 üzerindeki arayüzü inceler ve komut çıktısında gösterildiği gibi tam çift yönlü olarak ayarlandığını fark eder.

```
S1# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Full-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S1#
```

Ağ yöneticisi şimdi bağlantının diğer tarafını, S2'deki bağlantı noktasını inceler. Komut çıkışı, bağlantının bu tarafının yarı çift yönlü olarak yapılandırıldığını gösterir.

```
S2# show interface fa 0/20
FastEthernet0/20 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96d2.4001 (bia 0cd9.96d2.4001)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set Keepalive set (10 sec)
Half-duplex, Auto-speed, media type is 10/100BaseTX

(Output omitted)

S2(config)# interface fa 0/20
S2(config-if)# duplex auto
S2(config-if)#
```

Ağ yöneticisi , otomatik olarak çift yönlü görüşme yapmak için ayarı **duplex auto** olarak düzeltir . S1 üzerindeki bağlantı noktası tam çift yönlü olarak ayarlandığından, S2 de tam çift yönlü kullanır.

Kullanıcılar artık herhangi bir performans sorunu olmadığını bildiriyor.

### Adım 3 - Yerel Ağda Adreslemeyi Doğrulayın

Uçtan uca bağlantı sorunlarını giderirken, hedef IP adresleri ile ayrı segmentlerdeki Katman 2 Ethernet adresleri arasındaki eşlemeleri doğrulamak yararlıdır. IPv4'te bu işlevsellik ARP tarafından sağlanır. IPv6'da, ARP işlevselliği, komşu keşif süreci ve ICMPv6 ile değiştirilir. Komşu tablo, IPv6 adreslerini ve bunların çözümlenmiş Ethernet fiziksel (MAC) adreslerini önbelleğe alır.

### Windows IPv4 ARP Tablosu

Arp IPv4 adresleri ve onların çözümlenmiş Ethernet fiziksel (MAC) adreslerini saklamak için kullanılan ARP önbelleğinde Windows komut görüntüler ve değiştirir girişleri. Komut çıktısında gösterildiği gibi, arp Windows komutu şu anda ARP önbelleğinde bulunan tüm aygıtları listeler.

Her cihaz için görüntülenen bilgiler, IPv4 adresini, fiziksel (MAC) adresini ve adresleme türünü (statik veya dinamik) içerir.

Ağ yöneticisi önbelleği güncellenmiş bilgilerle yeniden doldurmak isterse , arp -d Windows komutu kullanılarak önbellek temizlenebilir .

Licensed to yetkin karasungur, yetkinkrshgr@gmail.com

Not : Linux ve MAC OS X'teki arp komutları benzer bir sözdizimine sahiptir.

```
C:\> arp -a
Interface: 10.1.10.100 --- 0xd
  Internet Address      Physical Address      Type
  10.1.10.1             d4-8c-b5-ce-a0-c0     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\>
```

### Windows IPv6 Komşu Tablosu

Netsh interface ipv6 show neighbor Windows komut çıktısı, şu anda komşu tablosunda bulunan tüm aygıtları listeler.

Her cihaz için görüntülenen bilgiler, IPv6 adresini, fiziksel (MAC) adresini ve adresleme türünü içerir. Ağ yöneticisi, komşu tabloyu inceleyerek hedef IPv6 adreslerinin doğru Ethernet adresleriyle eşleştiğini doğrulayabilir. R1'in tüm arabirimlerindeki IPv6 bağlantı yerel adresleri manuel olarak FE80 :: 1'e yapılandırılmıştır. Benzer şekilde R2, arabirimlerinde FE80 :: 2'nin bağlantı yerel adresi ile yapılandırılmış ve R3, arabirimlerinde FE80 :: 3'ün bağlantı yerel adresi ile yapılandırılmıştır. Unutmayın, yerel bağlantı adresleri bağlantı veya ağ üzerinde benzersiz olmalıdır.

Not : Linux ve MAC OS X için komşu tablo **ip neigh show** komutu kullanılarak görüntülenebilir .

```
C:\> netsh interface ipv6 show neighbor
Internet Address                            Physical Address   Type
------------------------------------------  -----------------  -----------
fe80::9657:a5ff:fe0c:5b02                   94-57-a5-0c-5b-02  Stale
fe80::1                                     d4-8c-b5-ce-a0-c0  Reachable (Router)
ff02::1                                     33-33-00-00-00-01  Permanent
ff02::2                                     33-33-00-00-00-02  Permanent
ff02::16                                    33-33-00-00-00-16  Permanent
ff02::1:2                                   33-33-00-01-00-02  Permanent
ff02::1:3                                   33-33-00-01-00-03  Permanent
ff02::1:ff0c:5b02                           33-33-ff-0c-5b-02  Permanent
ff02::1:ff2d:a75e                           33-33-ff-2d-a7-5e  Permanent
```

### IOS IPv6 Komşu Tablosu

**Show ipv6 neighbors** komut çıktısı, Cisco IOS yönlendiricisindeki komşu tablosunun bir örneğini görüntüler.

Not : IPv6 için komşu durumlar, IPv4'teki ARP tablosu durumlarından daha karmaşıktır. Ek bilgiler RFC 4861'de bulunur.

```
R1# show ipv6 neighbors
IPv6 Address                          Age  Link-layer Addr   State  Interface
FE80::21E:7AFF:FE79:7A81                8  001e.7a79.7a81    STALE  Gi0/0
2001:DB8:ACAD:1:5075:D0FF:FE8E:9AD8     0  5475.d08e.9ad8    REACH  Gi0/0
```

### Anahtar MAC Adres Tablosu

Anahtar MAC adres tablosunda bir hedef MAC adresi bulunduğunda, anahtar çerçeveyi yalnızca bu MAC adresine sahip aygıtın bağlantı noktasına iletir. Bunu yapmak için, anahtar kendi MAC adres tablosuna başvurur. MAC adres tablosu, her bağlantı noktasına bağlı MAC adresini listeler. Kullanım gösteri mac adresi masa anahtarı MAC adresi tablosunu görüntülemek için komut. Komut çıkışında bir anahtar MAC adresi tablosu örneği gösterilmektedir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

VLAN 10'daki bir aygıt olan PC1 için MAC adresinin, PC1'in bağlandığı S1 anahtar bağlantı noktasıyla birlikte nasıl keşfedildiğine dikkat edin. Anahtarın MAC adres tablosunun, Ethernet MAC adresi ve bağlantı noktası

numarası dahil olmak üzere yalnızca Katman 2 bilgilerini içerdiğini unutmayın. IP adresi bilgileri dahil edilmemiştir.

```
S1# show mac address-table
              Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type      Ports
All       0100.0ccc.cccc      STATIC    CPU
All       0100.0ccc.cccd      STATIC    CPU
10        d48c.b5ce.a0c0      DYNAMIC   Fa0/4
10        000f.34f9.9201      DYNAMIC   Fa0/5
10        5475.d08e.9ad8      DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 5
```

## VLAN Atama Örneğinde Sorun Giderme

Uçtan uca bağlantı sorunlarını giderirken göz önünde bulundurulması gereken bir diğer konu da VLAN atamasıdır. Anahtarlamalı ağda, bir anahtardaki her bağlantı noktası bir VLAN'a aittir. Her VLAN ayrı bir mantıksal ağ olarak kabul edilir ve VLAN'a ait olmayan istasyonlara yönelik paketler, yönlendirmeyi destekleyen bir cihaz aracılığıyla iletilmelidir. Bir VLAN'daki bir ana bilgisayar, bir ARP isteği gibi bir yayın Ethernet çerçevesi gönderirse, aynı VLAN'daki tüm ana bilgisayarlar çerçeveyi alır; diğer VLAN'lardaki ana bilgisayarlar bunu yapmaz. İki ana bilgisayar aynı IP ağında olsa bile, iki ayrı VLAN'a atanmış bağlantı noktalarına bağlanırlarsa iletişim kuramazlar. Ek olarak, bağlantı noktasının ait olduğu VLAN silinirse, bağlantı noktası devre dışı kalır. Silinen VLAN'a ait bağlantı noktalarına bağlı tüm ana bilgisayarlar, ağın geri kalanıyla iletişim kuramaz.show vlan , bir anahtardaki VLAN atamalarını doğrulamak için kullanılabilir.

Örneğin, kablolama dolabındaki kablo yönetimini iyileştirmek için şirketinizin S1 anahtarına bağlanan kabloları yeniden düzenlediğini varsayalım. Neredeyse hemen sonra, kullanıcılar artık kendi ağları dışındaki cihazlara erişemeyeceklerini belirterek destek masasını aramaya başladılar.

### ARP Tablosunu Kontrol Edin

Arp Windows komutu kullanılarak PC1 ARP tablosunun incelenmesi, ARP tablosunun komut çıktısında gösterildiği gibi, varsayılan ağ geçidi 10.1.10.1 için artık bir girdi içermediğini gösterir.

```
C:\> arp -a
Interface: 10.1.10.100 --- 0xd
  Internet Address      Physical Address      Type
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\>
```

### Anahtar MAC  Tablosunu Kontrol Edin

Yönlendiricide herhangi bir yapılandırma değişikliği olmadığı için sorun gidermenin odak noktası S1'dir.

Komut çıkışında gösterildiği gibi S1 için MAC adres tablosu, R1 için MAC adresinin PC1 dahil 10.1.10.0/24 cihazlarının geri kalanından farklı bir VLAN'da olduğunu gösterir.

```
S1# show mac address-table
              Mac Address Table
-------------------------------------------
Vlan      Mac Address         Type      Ports
All       0100.0ccc.cccc      STATIC    CPU
All       0100.0ccc.cccd      STATIC    CPU
 1        d48c.b5ce.a0c0      DYNAMIC   Fa0/1
10        000f.34f9.9201      DYNAMIC   Fa0/5
10        5475.d08e.9ad8      DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

Licensed to: yetkin karasungur, yetkinkrsngr@gmail.com

### VLAN Atamasını Düzeltin

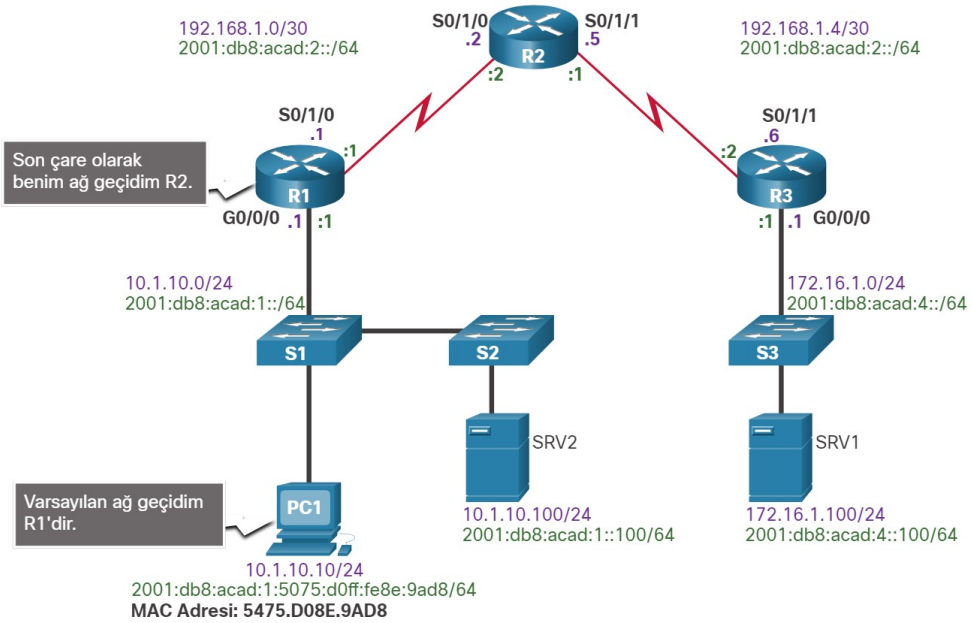
Yeniden kablolama sırasında, R1 için yama kablosu, VLAN 10'daki Fa 0/4'ten VLAN 1'deki Fa 0 / 1'e taşındı. Ağ yöneticisi, S1'in Fa 0/1 bağlantı noktasını VLAN 10'da olacak şekilde yapılandırdıktan sonra, komut çıktısında gösterilen sorun çözüldü. MAC adres tablosu artık Fa 0/1 portunda R1'in MAC adresi için VLAN 10'u göstermektedir.

```
S1(config)# interface fa0/1
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 10
S1(config-if)# exit
S1#
S1# show mac address-table
              Mac Address Table
-------------------------------------------
Vlan       Mac Address         Type      Ports
All        0100.0ccc.cccc      STATIC    CPU
All        0100.0ccc.cccd      STATIC    CPU
10         d48c.b5ce.a0c0      DYNAMIC   Fa0/1
10         000f.34f9.9201      DYNAMIC   Fa0/5
10         5475.d08e.9ad8      DYNAMIC   Fa0/13
Total Mac Addresses for this criterion: 5
S1#
```

### Adım 4 - Varsayılan Ağ Geçidini Doğrulayın

Yönlendiricide ayrıntılı bir yol yoksa veya ana bilgisayar yanlış varsayılan ağ geçidi ile yapılandırılmışsa, farklı ağlardaki iki uç nokta arasındaki iletişim çalışmaz.

Şekil, PC1'in varsayılan ağ geçidi olarak R1'i nasıl kullandığını göstermektedir. Benzer şekilde, R1, R2'yi varsayılan ağ geçidi veya son çare olarak ağ geçidi olarak kullanır. Bir ana bilgisayarın yerel ağ dışındaki kaynaklara erişmesi gerekiyorsa, varsayılan ağ geçidi yapılandırılmalıdır. Varsayılan ağ geçidi, yerel ağın ötesindeki hedeflere giden yoldaki ilk yönlendiricidir.




IPv4 Varsayılan Ağ Geçidi İle İlgili Sorunları Giderme Örneği

Bu örnekte, R1, R2'nin IPv4 adresi olan doğru varsayılan ağ geçidine sahiptir. Ancak, PC1 yanlış varsayılan ağ geçidine sahiptir. PC1, R1 10.1.10.1 varsayılan ağ geçidine sahip olmalıdır. IPv4 adresleme bilgileri PC1'de manuel olarak yapılandırıldıysa, bu manuel olarak yapılandırılmalıdır. IPv4 adresleme bilgisi bir DHCPv4 sunucusundan otomatik olarak alınmışsa, DHCP sunucusundaki konfigürasyon incelenmelidir. DHCP sunucusundaki bir yapılandırma sorunu genellikle birden çok istemciyi etkiler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

R1 Yönlendirme Tablosu

Show ip route Cisco IOS komutunun komut çıktısı , R1'in varsayılan ağ geçidini doğrulamak için kullanılır.

```
R1# show ip route | include Gateway|0.0.0.0

Gateway of last resort is 192.168.1.2 to network 0.0.0.0
S* 0.0.0.0/0 [1/0] via 192.168.1.2

R1#
```

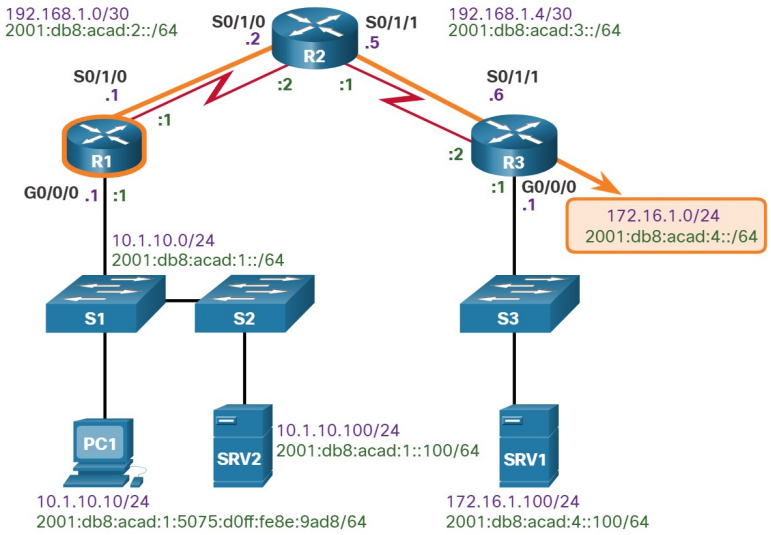
PC1 Yönlendirme Tablosu

Bir Windows ana bilgisayarında, Windows **route print** komutu, komut çıktısında gösterildiği gibi IPv4 varsayılan ağ geçidinin varlığını doğrulamak için kullanılır.

```
C:\> route print
(Output omitted)

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0        10.1.10.1      10.1.10.10      11
(Output omitted)
```

## Adım 5 - Hedef Yolu Doğrulayın

Sorun giderme sırasında, genellikle hedef ağın yolunu doğrulamak gerekir. Şekil, PC1'den SRV1'e paketler için amaçlanan yolu gösteren referans topolojisini gösterir.




R1 IPv4 Yönlendirme Tablosu

```
R1# show ip route | begin Gateway
Gateway of last resort is 192.168.1.2 to network 0.0.0.0
O*E2  0.0.0.0/0 [110/1] via 192.168.1.2, 00:00:13, Serial0/1/0
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.1.10.0/24 is directly connected, GigabitEthernet0/0/0
L        10.1.10.1/32 is directly connected, GigabitEthernet0/0/0
      172.16.0.0/24 is subnetted, 1 subnets
O        172.16.1.0 [110/100] via 192.168.1.2, 00:01:59, Serial0/1/0
      192.168.1.0/24 is variably subnetted, 3 subnets, 2 masks
C        192.168.1.0/30 is directly connected, Serial0/1/0
L        192.168.1.1/32 is directly connected, Serial0/1/0
O        192.168.1.4/30 [110/99] via 192.168.1.2, 00:06:25, Serial0/1/0
R1#
```

yetkin karasungur, yetkinkrsngr@gmail.com

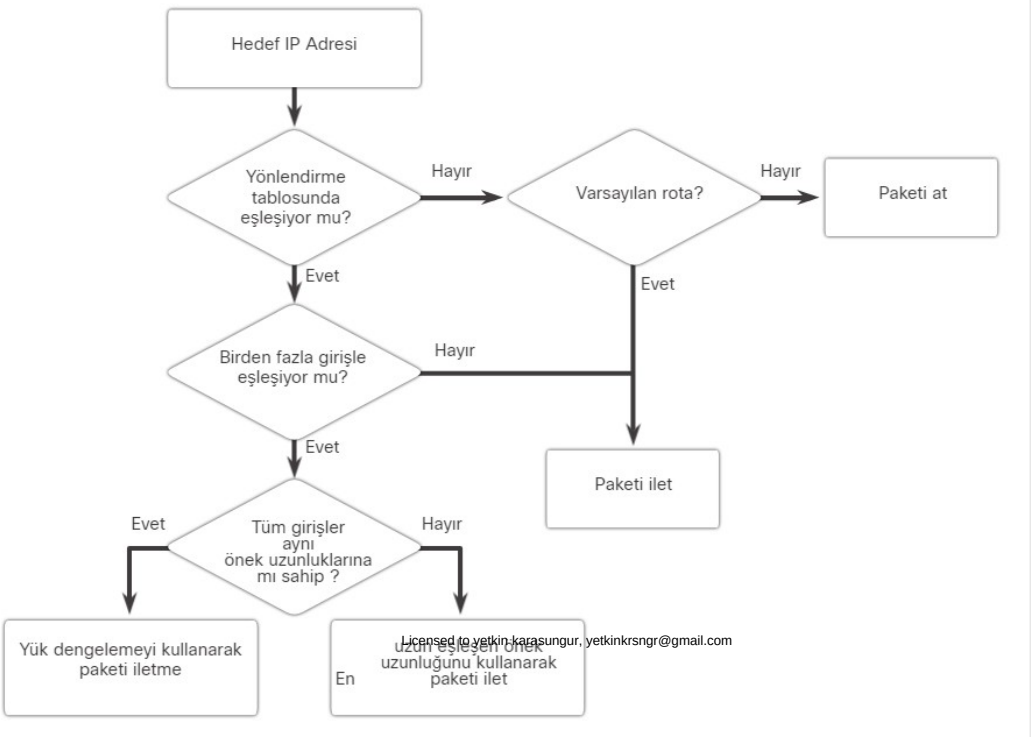
R1 IPv6 Yönlendirme Tablosu

```
R1# show ipv6 route
IPv6 Routing Table - default - 8 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1
       OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
       a - Application
OE2 ::/0 [110/1], tag 1
     via FE80::2, Serial0/1/0
C   2001:DB8:ACAD:1::/64 [0/0]
     via GigabitEthernet0/0/0, directly connected
L   2001:DB8:ACAD:1::1/128 [0/0]
     via GigabitEthernet0/0/0, receive
C   2001:DB8:ACAD:2::/64 [0/0]
     via Serial0/1/0, directly connected
L   2001:DB8:ACAD:2::1/128 [0/0]
     via Serial0/1/0, receive
O   2001:DB8:ACAD:3::/64 [110/99]
     via FE80::2, Serial0/1/0
O   2001:DB8:ACAD:4::/64 [110/100]
     via FE80::2, Serial0/1/0
L   FF00::/8 [0/0]
     via Null0, receive
R1#
```

IPv4 ve IPv6 yönlendirme tabloları aşağıdaki yöntemlerle doldurulabilir:

- Doğrudan bağlı ağlar
- Yerel ana bilgisayar veya yerel yollar
- Statik yollar
- Dinamik rotalar
- Varsayılan rotalar

IPv4 ve IPv6 paketlerini iletme işlemi, en uzun bit eşleşmesine veya en uzun önek eşleşmesine dayanır. Yönlendirme tablosu işlemi, en soldaki en çok eşleşen bit sayısına sahip yönlendirme tablosundaki bir girişi kullanarak paketi iletmeye çalışacaktır. Eşleşen bitlerin sayısı, rotanın ön ek uzunluğu ile belirtilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yukarıdaki akış şemasına göre aşağıdaki senaryoları inceleyin. Bir paketteki hedef adres:

- Yönlendirme tablosundaki bir girişle eşleşmezse, varsayılan yol kullanılır. Yapılandırılmış varsayılan bir yol yoksa, paket atılır.
- Yönlendirme tablosundaki tek bir girişle eşleşir, ardından paket bu rotada tanımlanan arayüz üzerinden iletilir.
- Yönlendirme tablosunda birden fazla girdiyle eşleşir ve yönlendirme girdileri aynı önek uzunluğuna sahiptir, ardından bu hedef için paketler yönlendirme tablosunda tanımlanan yollar arasında dağıtılabilir.
- Yönlendirme tablosundaki birden fazla girdiyle eşleşir ve yönlendirme girdilerinin farklı önek uzunlukları vardır, ardından bu hedefe yönelik paketler, daha uzun önek eşleşmesine sahip yol ile ilişkili arabirimden dışarı iletilir.

Sorun Giderme Örneği

Aygıtlar, 172.16.1.100'de SRV1 sunucusuna bağlanamıyor. **Show ip route** komutunu kullanarak, yönetici, 172.16.1.0/24 ağına bir yönlendirme girişi olup olmadığını kontrol etmelidir. Yönlendirme tablosunun SRV1 ağına belirli bir yolu yoksa, ağ yöneticisi daha sonra 172.16.1.0/24 ağı yönünde varsayılan veya özet bir yol girişinin varlığını kontrol etmelidir. Hiçbiri yoksa, sorun yönlendirmeyle ilgili olabilir ve yönetici ağın dinamik yönlendirme protokolü yapılandırmasına dahil olduğunu doğrulamalı veya statik bir yol eklemelidir.

### Adım 6 - Taşıma Katmanını Doğrulayın

Ağ katmanı beklendiği gibi çalışıyorsa, ancak kullanıcılar yine de kaynaklara erişemiyorsa, ağ yöneticisinin üst katmanlarda sorun gidermeye başlaması gerekir. Taşıma katmanı bağlantısını etkileyen en yaygın iki sorun, ACL yapılandırmalarını ve NAT yapılandırmalarını içerir. Aktarım katmanı işlevselliğini test etmek için yaygın bir araç, Telnet yardımcı programıdır.

Dikkat : Telnet, aktarım katmanını test etmek için kullanılabilirken, güvenlik nedenleriyle cihazları uzaktan yönetmek ve yapılandırmak için SSH kullanılmalıdır.

### Sorun Giderme Örneği

Bir ağ yöneticisi, HTTP kullanarak bir yönlendiriciye bağlanamadığı bir sorunu gideriyor. Yönetici, komut çıktısında gösterildiği gibi R2'ye ping gönderir.

```
R1# ping 2001:db8:acad:2::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:2::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/2/3 ms
R1#
```

R2 yanıt verir ve ağ katmanının ve ağ katmanının altındaki tüm katmanların çalıştığını onaylar. Yönetici, sorunun Katman 4 veya üzeri olduğunu bilir ve bu katmanlarda sorun gidermeye başlamalıdır.

Ardından yönetici, komut çıktısında gösterildiği gibi R2'ye Telnet yapabileceklerini doğrular.

```
R1# telnet 2001:db8:acad:2::2
Trying 2001:DB8:ACAD:2::2 ... Open
User Access Verification
Password:
R2> exit
[Connection to 2001:db8:acad:2::2 closed by foreign host]
R1#
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Yönetici, Telnet hizmetlerinin R2 üzerinde çalıştığını onayladı. Telnet sunucu uygulaması, iyi bilinen 23 numaralı bağlantı noktasında çalışmasına ve Telnet istemcilerinin varsayılan olarak bu bağlantı noktasına bağlanmasına rağmen, test edilmesi gereken herhangi bir TCP bağlantı noktasına bağlanmak için istemcide farklı bir bağlantı noktası numarası belirtilebilir. 23 numaralı TCP bağlantı noktasından farklı bir bağlantı noktasının kullanılması, bağlantının kabul edilip edilmediğini (çıkışta "Aç" kelimesiyle belirtildiği gibi), reddedildiğini veya zaman aşımına uğradığını gösterir. Bu yanıtların herhangi birinden, bağlantıyla ilgili daha fazla sonuç çıkarılabilir. Bazı uygulamalar, ASCII tabanlı bir oturum protokolü kullanıyorlarsa, bir uygulama başlığı bile görüntüleyebilir, SMTP, FTP ve HTTP gibi belirli anahtar sözcükleri yazarak sunucudan bazı yanıtları tetiklemek mümkün olabilir.

Örneğin, yönetici 80 numaralı bağlantı noktasını kullanarak R2'ye Telnet sağlamaya çalışır.

```
R1# telnet 2001:db8:acad:2::2 80
Trying 2001:DB8:ACAD:2::2, 80 ... Open
^C
HTTP/1.1 400 Bad Request
Date: Mon, 04 Nov 2019 12:34:23 GMT
Server: cisco-IOS
Accept-Ranges: none
400 Bad Request
[Connection to 2001:db8:acad:2::2 closed by foreign host]
R1#
```

Çıktı, başarılı bir aktarım katmanı bağlantısını doğrular, ancak R2, 80 numaralı bağlantı noktasını kullanarak bağlantıyı reddediyor.

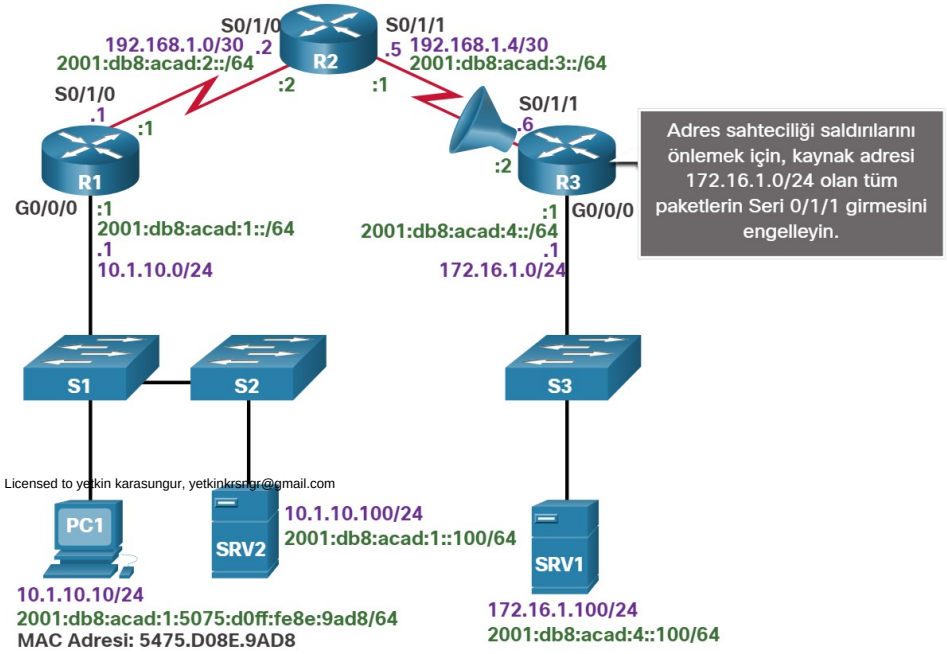
### 7. Adım - ACL'leri Doğrulayın

Yönlendiricilerde, protokollerin gelen veya giden yönde arayüzden geçmesini engelleyen ACL'ler olabilir.

Tüm IPv4 ACL'lerin içeriğini görüntülemek için **show ip access- list** komutunu ve bir yönlendiricide yapılandırılan tüm IPv6 ACL'lerin içeriğini görüntülemek için **show ipv6 access- list** komutunu kullanın. Belirli ACL, bu komut için bir seçenek olarak ACL adı veya numarası girilerek görüntülenebilir. **show ip interfaces** ve **show ipv6 interfaces** komutları arabirimde herhangi bir IP ACL'nin ayarlanıp ayarlanmadığını gösteren IPv4 ve IPv6 arabirim bilgilerini görüntüler.

### Sorun Giderme Örneği

Adres sahteciliği saldırılarını önlemek için ağ yöneticisi, şekilde gösterildiği gibi, kaynak ağ adresi 172.16.1.0/24 olan cihazların R3 üzerinde gelen S0/0/1 arayüzüne girmesini engelleyen bir ACL uygulamaya karar verdi. Diğer tüm IP trafiğine izin verilmelidir.



Ancak, ACL'yi uyguladıktan kısa bir süre sonra, 10.1.10.0/24 ağındaki kullanıcılar, SRV1 dahil 172.16.1.0/24 ağındaki cihazlara bağlanamadı.

### show ip access-lists

Show ip access-list komutu, komut çıktısında gösterildiği gibi ACL'nin doğru şekilde yapılandırıldığını gösterir.

```
R3# show ip access-lists
Extended IP access list 100
    10 deny ip 172.16.1.0 0.0.0.255 any (108 matches)
    20 permit ip any any (28 matches)
R3#
```

### Show ip interfaces

**Show ip interfaces serial 0/1/1** komutu ve **show ip interfaces serial 0/0/0** komutunu kullanarak ACL'nin hangi arabirime uygulandığını doğrulayabiliriz . Çıktı, ACL'nin Seri 0/0/1 üzerinde gelen arayüze hiçbir zaman uygulanmadığını, ancak yanlışlıkla G0 / 0/0 arayüzüne uygulandığını ve 172.16.1.0/24 ağından tüm giden trafiği engellediğini ortaya koymaktadır.

```
R3# show ip interface serial 0/1/1 | include access list
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is not set
R3#
R3# show ip interface gig 0/0/0 | include access list
  Outgoing Common access list is not set
  Outgoing access list is not set
  Inbound Common access list is not set
  Inbound  access list is 100
R3#
```

### Sorunu Düzeltin

IPv4 ACL'yi, komut çıktısında gösterildiği gibi Seri 0/0/1 gelen arabirimine doğru şekilde yerleştirdikten sonra, aygıtlar sunucuya başarıyla bağlanabilir.

```
R3(config)# interface GigabitEthernet 0/0/0
R3(config-if)# no ip access-group 100 in
R3(config-if)# exit
R3(config)#
R3(config)# interface serial 0/1/1
R3(config-if)# ip access-group 100 in
R3(config-if)# end
R3#
```

### Adım 8 - DNS'i Doğrulayın

DNS protokolü, ana bilgisayar adlarını IP adresleriyle eşleştirebileceğiniz dağıtılmış bir veritabanı olan DNS'yi kontrol eder. Cihazda DNS'yi yapılandırdığınızda, IP adresi için ana bilgisayar adını ping veya telnet gibi tüm IP komutlarıyla değiştirebilirsiniz .

Anahtar veya yönlendiricide DNS yapılandırma bilgilerini görüntülemek için **show running-config** komutunu kullanın. Herhangi bir DNS sunucusu kurulu olmadığında, IP eşlemelerine doğrudan anahtar veya yönlendirici yapılandırmasına adlar girmek mümkündür. Komut çıkışında gösterildiği gibi, anahtarın veya yönlendiricinin IPv4 adresi yerine kullanılacak bir ad girmek için **ip host** komutunu kullanın .

Kadir Has Üniversitesi Bilgisayar Ağ Güvenliği Dersi

```
R1(config)# ip host ipv4-server 172.16.1.100
R1(config)# exit
R1#
```

Komut çıktısında gösterildiği gibi, artık IP adresi yerine atanan ad kullanılabilir.

```
R1# ping ipv4-server
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.100, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/7 ms
R1#
```

Windows tabanlı bir bilgisayarda ad-IP adresi eşleme bilgilerini görüntülemek için **nslookup** komutunu kullanın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 42.Bölüm: Ağ Sanallaştırma

## 42.1.Bulut Bilişim (Cloud Computing)

### 42.1.1.Buluta Genel Bakış

Bulut bilgi işlem, fiziksel olarak herhangi bir yere yerleştirilebilen bir ağ üzerinden bağlanan çok sayıda bilgisayarı içerir. Sağlayıcılar, bulut bilişim hizmetlerini sunmak için büyük ölçüde sanallaştırmaya güveniyor. Bulut bilgi işlem, kaynakları daha verimli kullanarak operasyonel maliyetleri azaltabilir. Bulut bilgi işlem, çeşitli veri yönetimi sorunlarını ele alır:

- Kurumsal verilere her yerde ve her zaman erişim sağlar
- Yalnızca gerekli hizmetlere abone olarak kuruluşun BT işlemlerini kolaylaştırır
- Yerinde BT ekipmanı, bakım ve yönetim ihtiyacını ortadan kaldırır veya azaltır
- Ekipman, enerji, fiziksel tesis gereksinimleri ve personel eğitimi ihtiyaçlarını azaltır
- Artan veri hacmi gereksinimlerine hızlı yanıtlar sağlar

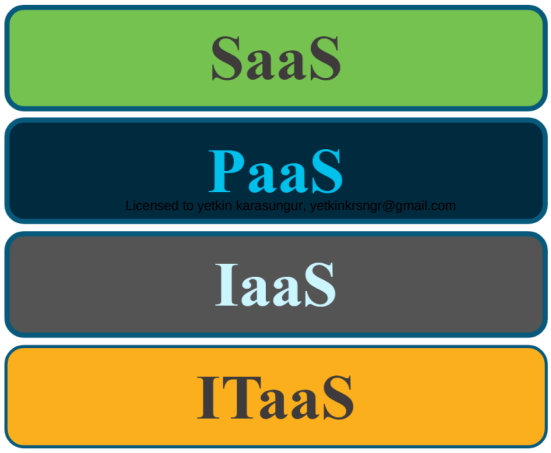
Bulut bilişim, "kullandıkça öde" modeliyle, kuruluşların bilgi işlem ve depolama masraflarını altyapıya yatırım yapmak yerine bir yardımcı program olarak ele almasına olanak tanır. Sermaye harcamaları işletme harcamalarına dönüştürülür.

### 42.1.2.Bulut Hizmetleri

Bulut hizmetleri, müşteri gereksinimlerini karşılayacak şekilde uyarlanmış çeşitli seçeneklerde mevcuttur. National Institute of Standards and Technology (NIST) tarafından Özel Yayınları 800-145'te tanımlanan üç ana bulut bilişim hizmeti aşağıdaki gibidir:

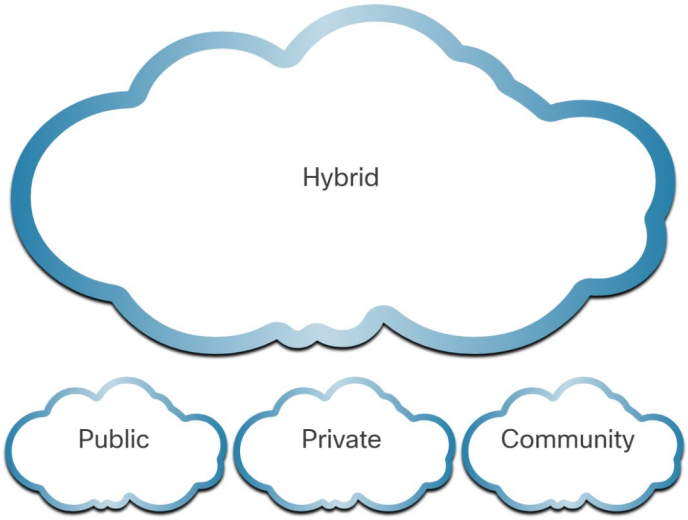
- Hizmet Olarak Yazılım- Software as a Service (SaaS) - Bulut sağlayıcısı, internet üzerinden sağlanan e-posta, iletişim ve Office 365 gibi uygulama ve hizmetlere erişimden sorumludur. Kullanıcı, kullanıcıya özgü sınırlı uygulama ayarları dışında bulut hizmetlerinin hiçbir yönünü yönetmez. Kullanıcının yalnızca verilerini sağlaması gerekir.
- Hizmet Olarak Platform- Platform as a Service (PaaS) - Bulut sağlayıcısı, kullanıcıların uygulamaları sunmak için kullanılan geliştirme araçlarına ve hizmetlere erişimini sağlamaktan sorumludur. Bu kullanıcılar genellikle programcılardır ve bulut sağlayıcısının uygulama barındırma ortamının yapılandırma ayarları üzerinde kontrole sahip olabilirler.
- Hizmet Olarak Altyapı-Infrastructure as a Service (IaaS) - Bulut sağlayıcısı, BT yöneticilerine ağ ekipmanına, sanallaştırılmış ağ hizmetlerine ve destek ağ altyapısına erişim sağlamaktan sorumludur. Bu bulut hizmetini kullanmak, BT yöneticilerinin işletim sistemlerini ve uygulamaları içerebilen yazılım kodunu dağıtmasına ve çalıştırmasına olanak tanır.

Bulut hizmeti sağlayıcıları, şekilde gösterildiği gibi, bulut bilişim hizmetlerinin (ITaaS) her biri için BT desteği sağlamak için bu modeli genişletti. İşletmeler için ITaaS, yeni altyapıya yatırım, yeni personel eğitimi veya yeni yazılım lisansı almadan ağın kapasitesini genişletebilir. Bu hizmetler talep üzerine sunulur ve güvenlik veya işlevden ödün vermeden dünyanın herhangi bir yerindeki herhangi bir cihaza ekonomik olarak sunulur.



### 42.1.3.Bulut Modelleri

Şekilde gösterildiği gibi dört ana bulut modeli vardır.




- Genel bulutlar - Genel bir bulutta sunulan bulut tabanlı uygulamalar ve hizmetler genel nüfusun kullanımına sunulur. Hizmetler ücretsiz olabilir veya çevrimiçi depolama için ödeme yapma gibi kullanım başına ödeme modelinde sunulabilir. Genel bulut, hizmet sağlamak için interneti kullanır.
- Özel bulutlar - Özel bir bulutta sunulan bulut tabanlı uygulamalar ve hizmetler, devlet gibi belirli bir kuruluş veya varlığa yöneliktir. Özel bir bulut, kuruluşun özel ağı kullanılarak kurulabilir, ancak bunun oluşturulması ve bakımı pahalı olabilir. Özel bir bulut, sıkı erişim güvenliğine sahip bir dış kuruluş tarafından da yönetilebilir.
- Karma bulutlar - Karma bulut, her bir parçanın ayrı bir nesne olarak kaldığı, ancak her ikisinin de tek bir mimari kullanılarak birbirine bağlandığı iki veya daha fazla buluttan oluşur (örnek: kısmen özel, kısmen genel). Bir hibrit bulut üzerindeki bireyler, kullanıcı erişim haklarına bağlı olarak çeşitli hizmetlere erişim derecelerine sahip olabilir.
- Topluluk bulutları - Belirli bir topluluk tarafından özel kullanım için bir topluluk bulutu oluşturulur. Genel bulutlar ve topluluk bulutları arasındaki farklar, topluluk için özelleştirilmiş işlevsel ihtiyaçlardır. Örneğin, sağlık kuruluşları, özel kimlik doğrulama ve gizlilik gerektir.

### 42.1.4.Bulut Bilişim ve Veri Merkezi Karşılaştırması

Veri merkezi ve bulut bilişim terimleri genellikle yanlış kullanılır. Veri merkezi ve bulut bilişimin doğru tanımları şunlardır:

- 
- Veri merkezi : Tipik olarak, şirket içi bir BT departmanı tarafından çalıştırılan veya iş yeri dışında kiralanan bir veri depolama ve işleme tesisi.
- Bulut bilişim : Tipik olarak, yapılandırılabilir bilgi işlem kaynaklarının paylaşılan havuzuna isteğe bağlı erişim sunan şirket dışı bir hizmet. Bu kaynaklar, minimum yönetim çabasıyla hızla tedarik edilebilir ve serbest bırakılabilir.

Veri merkezleri, bulut bilişim hizmetlerinin bilgi işlem, ağ ve depolama ihtiyaçlarını sağlayan fiziksel tesislerdir. Bulut hizmeti sağlayıcıları, bulut hizmetlerini ve bulut tabanlı kaynaklarını barındırmak için veri merkezlerini kullanır.

Bir veri merkezi, bir binanın bir odasını, bir veya daha fazla katı veya bir binanın tamamını işgal edebilir. Veri merkezlerinin kurulması ve bakımı genellikle çok pahalıdır. Bu nedenle, yalnızca büyük kuruluşlar verilerini barındırmak ve kullanıcılara hizmet sağlamak için özel olarak oluşturulmuş veri merkezlerini kullanır. Kendi özel veri merkezlerini koruyamayan daha küçük kuruluşlar, buluttaki daha büyük bir veri merkezi kuruluşundan sunucu ve depolama hizmetlerini kiralayarak toplam sahip olma maliyetini düşürebilir.

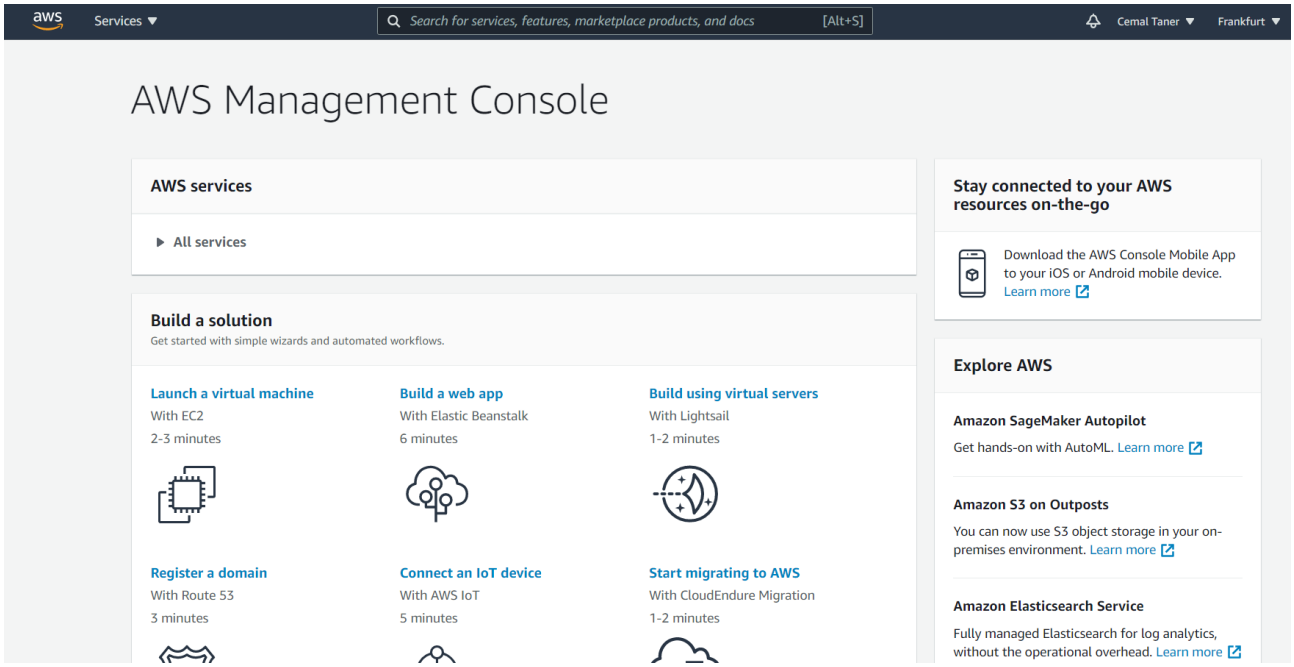
## 42.2.Sanallaştırma

### 42.2.1.Bulut Bilişim ve Sanallaştırma

"Bulut bilişim" ve "sanallaştırma" terimleri genellikle birbirinin yerine kullanılır; ancak farklı şeyler ifade ediyorlar. Sanallaştırma, bulut bilişimin temelidir. Bu olmadan, en yaygın şekilde uygulandığı şekliyle bulut bilişim mümkün olmazdı.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

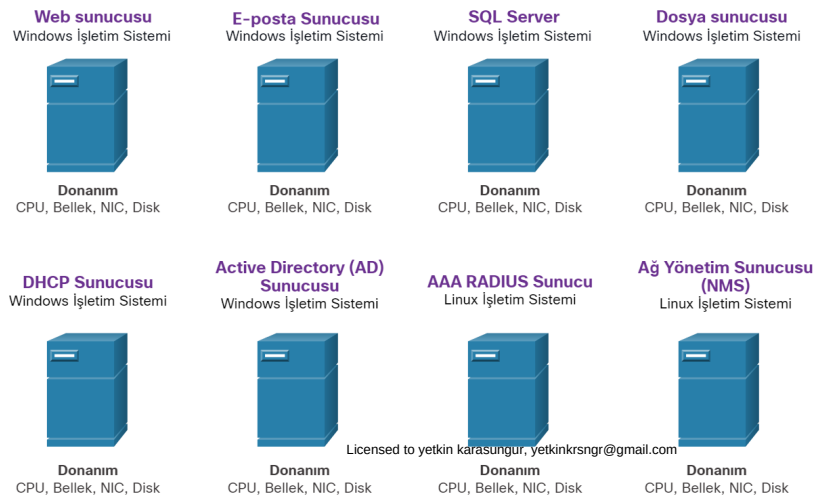
Sanallaştırma, işletim sistemini (OS) donanımdan ayırır. Çeşitli sağlayıcılar, gerektiğinde sunucuları dinamik olarak hazırlayabilen sanal bulut hizmetleri sunar. Örneğin, Amazon Web Services (AWS), müşterilerin ihtiyaç duydukları bilgi işlem kaynaklarını dinamik olarak tedarik etmeleri için basit bir yol sağlar. Bu sanallaştırılmış sunucu örnekleri, talep üzerine oluşturulur. Şekilde gösterildiği gibi, ağ yöneticisi AWS Management Console'dan sanal makineler, web uygulamaları, sanal sunucular ve IoT cihazlarına bağlantılar dahil olmak üzere çeşitli hizmetleri dağıtabilir.




## 42.2.2.Özel Sunucular

Sanallaştırmayı tam olarak değerlendirmek için, önce sunucu teknolojisinin geçmişinin bir kısmını anlamak gerekir. Tarihsel olarak, kurumsal sunucular, şekilde gösterildiği gibi, belirli bir donanıma kurulan Windows Server veya Linux Server gibi bir sunucu işletim sisteminden oluşuyordu. Bir sunucunun tüm RAM'i, işlem gücü ve sabit disk alanı, sağlanan hizmete (örneğin, Web, e-posta hizmetleri, vb.) ayrılmıştır.

Bu yapılandırmadaki en büyük sorun, bir bileşen başarısız olduğunda, bu sunucu tarafından sağlanan hizmetin kullanılamaz hale gelmesidir. Bu, tek bir başarısızlık noktası olarak bilinir. Diğer bir sorun, adanmış sunucuların yetersiz kullanılmasıydı. Tahsis edilmiş sunucular genellikle uzun süre boşta kalır ve sağladıkları belirli hizmeti sunma ihtiyacı doğana kadar beklerler. Bu sunucular enerji israf etti ve sağlanan hizmet miktarının garanti ettiğinden daha fazla yer kapladı. Bu, sunucu yayılması olarak bilinir.



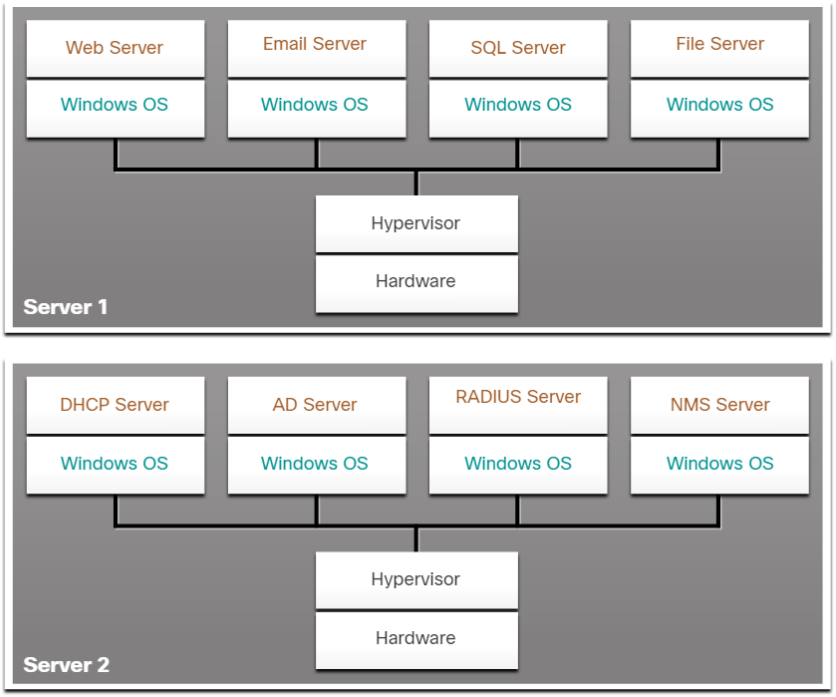

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 42.2.3.Sunucu Sanallaştırma

Sunucu sanallaştırma, boştaki kaynaklardan yararlanır ve gerekli sunucuların sayısını birleştirir. Bu aynı zamanda birden fazla işletim sisteminin tek bir donanım platformunda var olmasına izin verir.

Örneğin, şekilde, önceki sekiz adanmış sunucu, işletim sistemlerinin birden çok sanal örneğini desteklemek için hipervizörler kullanılarak iki sunucuda konsolide edilmiştir.

**Hipervizör İşletim Sistemi Kurulumu**




Sanallaştırmanın kullanımı, normalde tek bir hata noktasından korunmak için fazlalık içerir. Yedeklilik farklı şekillerde uygulanabilir. Hipervizör başarısız olursa, VM başka bir hipervizör üzerinde yeniden başlatılabilir. Ayrıca, aynı VM aynı anda iki hipervizör üzerinde çalışabilir, RAM ve CPU talimatlarını aralarında kopyalayabilir. Bir hipervizör başarısız olursa, VM diğer hipervizör üzerinde çalışmaya devam eder. Sanal makineler üzerinde çalışan hizmetler de sanaldır ve gerektiğinde dinamik olarak kurulabilir veya kaldırılabilir.

Hipervizör, fiziksel donanımın üstüne bir soyutlama katmanı ekleyen bir program, bellenim veya donanımdır. Soyutlama katmanı, fiziksel makinenin CPU'lar, bellek, disk denetleyicileri ve NIC'ler gibi tüm donanımlarına erişimi olan sanal makineler oluşturmak için kullanılır. Bu sanal makinelerin her biri eksiksiz ve ayrı bir işletim sistemi çalıştırır. Sanallaştırmayla, işletmeler artık ihtiyaç duydukları sunucu sayısını birleştirebilirler. Örneğin, 100 fiziksel sunucunun hipervizör kullanan 10 fiziksel sunucu üzerinde sanal makineler olarak konsolide edilmesi alışılmadık bir durum değildir.

## 42.2.4.Sanallaştırmanın Avantajları

Sanallaştırmanın önemli bir avantajı, genel olarak daha düşük maliyettir:

- Daha az ekipman gerekir - Sanallaştırma, daha az fiziksel sunucu, daha az ağ aygıtı ve daha az destekleyici altyapı gerektiren sunucu birleştirme sağlar. Aynı zamanda daha düşük bakım maliyetleri anlamına gelir.
- Daha az enerji tüketilir - Sunucuları birleştirmek, aylık güç ve soğutma maliyetlerini düşürür. Daha az tüketim, işletmelerin daha küçük bir karbon ayak izi elde etmesine yardımcı olur.
- Daha az alan gerekir - Sanallaştırma ile sunucu konsolidasyonu, veri merkezinin genel ayak izini azaltır. Daha az sayıda sunucu, ağ cihazı ve raf, gerekli zemin alanı miktarını azaltır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

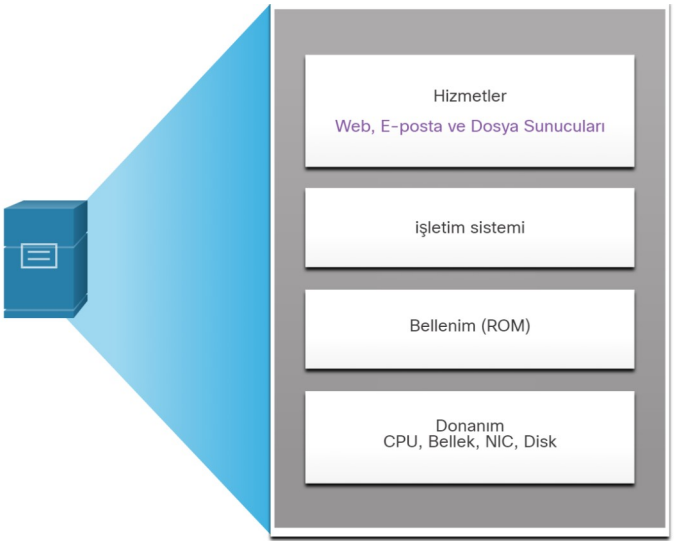
Sanallaştırmanın ek avantajları şunlardır:

- Daha kolay prototip oluşturma - İzole ağlarda çalışan bağımsız laboratuvarlar, ağ dağıtımlarını test etmek ve prototiplemek için hızla oluşturulabilir. Bir hata yapılırsa, bir yönetici basitçe önceki bir sürüme dönebilir. Test ortamları çevrimiçi olabilir, ancak son kullanıcılardan izole edilebilir. Test tamamlandığında, sunucular ve sistemler son kullanıcılara dağıtılabilir.
- Daha hızlı sunucu sağlama - Bir sanal sunucu oluşturmak, fiziksel bir sunucu sağlamaktan çok daha hızlıdır.
- Artan sunucu çalışma süresi - Çoğu sunucu sanallaştırma platformu artık canlı geçiş, depolama geçişi, yüksek kullanılabilirlik ve dağıtılmış kaynak zamanlaması gibi gelişmiş yedekli hata toleransı özellikleri sunuyor.
- İyileştirilmiş olağanüstü durum kurtarma - Sanallaştırma, gelişmiş iş sürekliliği çözümleri sunar. Kurtarma sitesinin artık üretim ortamındaki donanımla aynı donanıma sahip olmasına gerek kalmaması için donanım soyutlama yeteneği sağlar. Çoğu kurumsal sunucu sanallaştırma platformunda, bir felaket meydana gelmeden önce yük devretmenin test edilmesine ve otomatikleştirilmesine yardımcı olabilecek yazılımlar da vardır.
- Eski destek - Sanallaştırma, işletim sistemlerinin ve uygulamaların ömrünü uzatabilir ve kuruluşların daha yeni çözümlere geçmesi için daha fazla zaman sağlayabilir.

## 42.2.5.Soyutlama Katmanları

Sanallaştırmanın nasıl çalıştığını açıklamaya yardımcı olmak için, bilgisayar mimarilerinde soyutlama katmanlarının kullanılmasına yardımcı olur. Bir bilgisayar sistemi, şekilde gösterildiği gibi aşağıdaki soyutlama katmanlarından oluşur:

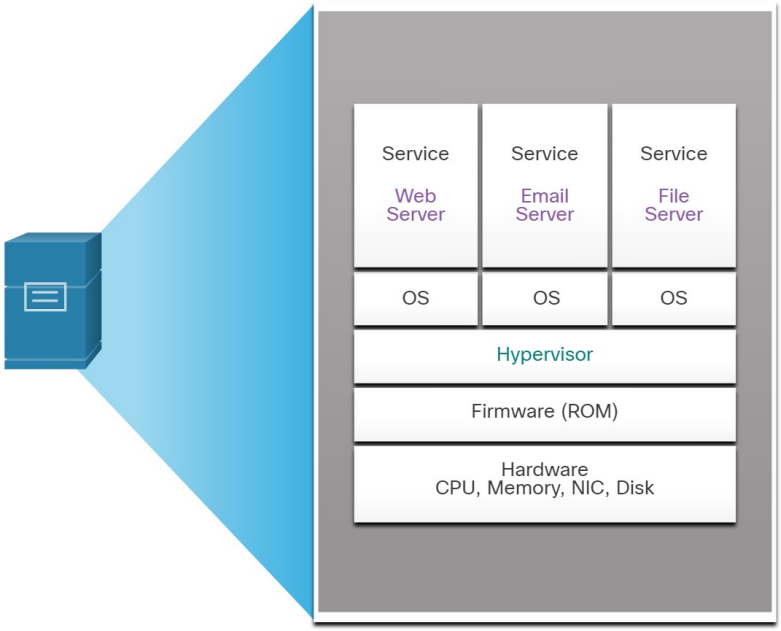
- Hizmetler
- işletim sistemi
- Firmware
- Donanım




Bu soyutlama katmanlarının her birinde, aşağıdaki katman ile yukarıdaki katman arasında bir arayüz olarak bir tür programlama kodu kullanılır. Örneğin, donanıma erişen aygıt yazılımını programlamak için genellikle C programlama dili kullanılır.

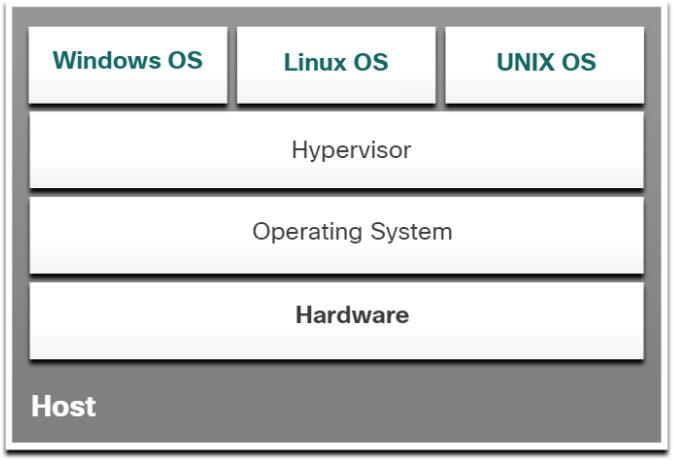
Şekilde bir sanallaştırma örneği gösterilmektedir. Donanım yazılımı ile işletim sistemi arasına bir hipervizör kurulur. Hipervizör, birden çok işletim sistemi örneğini destekleyebilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com




## 42.2.6.Tip 2 Hipervizör

Tip 2 hipervizör, sanal makine örnekleri oluşturan ve çalıştıran bir yazılımdır. Bir hipervizörün bir veya daha fazla VM'yi desteklediği bilgisayar, bir ana makinedir. Tip 2 hipervizörler, barındırılan hipervizörler olarak da adlandırılır. Bunun nedeni, hipervizörün macOS, Windows veya Linux gibi mevcut işletim sisteminin üzerine yüklenmesidir. Ardından, şekilde gösterildiği gibi hipervizörün üstüne bir veya daha fazla ek işletim sistemi örneği yüklenir.




Tip 2 hipervizörlerin büyük bir avantajı, yönetim konsolu yazılımına gerek olmamasıdır.

Tip 2 hipervizörler, tüketiciler ve sanallaştırmayı deneyen kuruluşlar arasında çok popülerdir. Ortak Tip 2 hipervizörler şunları içerir:

- Virtual PC
- VMware Workstation
- Oracle VM VirtualBox
- VMware Fusion
- Mac OS X Parallels

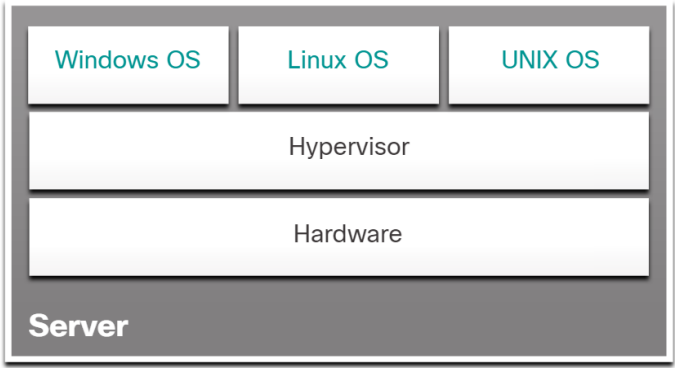
Bu Tip 2 hipervizörlerin çoğu ücretsizdir. Ancak, bazı hipervizörler bir ücret karşılığında daha gelişmiş özellikler sunar.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 42.3.Sanal Ağ Altyapısı

### 42.3.1.Tip 1 Hipervizörler

Tip 1 hipervizörlere "çıplak metal-bare metal" yaklaşımı da denir çünkü hiper yönetici doğrudan donanıma kurulur. Tip 1 hipervizörler genellikle kurumsal sunucularda ve veri merkezi ağ cihazlarında kullanılır.

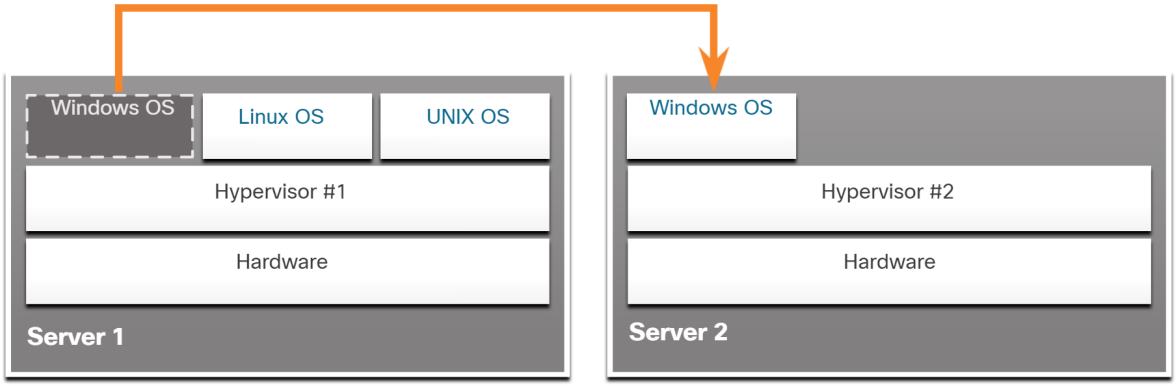



Tip 1 hipervizörlerle, hipervizör doğrudan sunucuya veya ağ donanımına kurulur. Ardından, şekilde gösterildiği gibi bir işletim sisteminin örnekleri hiper denetleyiciye yüklenir. Tip 1 hipervizörlerin donanım kaynaklarına doğrudan erişimi vardır. Bu nedenle, barındırılan mimarilerden daha verimlidirler. Tip 1 hipervizörler ölçeklenebilirliği, performansı ve sağlamlığı iyileştirir.

### 42.3.2.Hipervizör Üzerine Sanal Makine Kurmak

Bir Tip 1 hipervizör kurulduğunda ve sunucu yeniden başlatıldığında, işletim sistemi sürümü, RAM miktarı ve IP adresi gibi yalnızca temel bilgiler görüntülenir. Bu ekrandan bir işletim sistemi örneği oluşturulamaz. Tip 1 hipervizörler, hipervizörü yönetmek için bir "yönetim konsolu" gerektirir. Yönetim yazılımı, aynı hipervizör kullanarak birden çok sunucuyu yönetmek için kullanılır. Yönetim konsolu, sunucuları otomatik olarak birleştirebilir ve gerektiğinde sunucuları açıp kapatabilir.

Örneğin, şekildeki Sunucu1'in kaynakların azaldığını varsayın. Daha fazla kaynağı kullanılabilir kılmak için ağ yöneticisi, Windows örneğini Sunucu2'deki hipervizöre taşımak için yönetim konsolunu kullanır. Yönetim konsolu, hareketi otomatik olarak tetikleyecek eşiklerle de programlanabilir.




Yönetim konsolu, donanım arızasından kurtarma sağlar. Bir sunucu bileşeni başarısız olursa, yönetim konsolu sanal makineyi otomatik olarak başka bir sunucuya taşır. Cisco UCS Manager, birden çok sunucuyu kontrol eder ve binlerce VM için kaynakları yönetir.

Bazı yönetim konsolları ayrıca sunucunun fazla tahsis edilmesine izin verir. Fazla ayırma, birden çok işletim sistemi örneğinin kurulduğu, ancak bellek ayırmalarının bir sunucunun sahip olduğu toplam bellek miktarını aştığı zamandır. Örneğin, bir sunucuda 16 GB RAM bulunur, ancak yönetici, her birine 10 GB RAM ayrılmış dört işletim sistemi örneği oluşturur. Bu tür aşırı tahsis, yaygın bir uygulamadır çünkü dört işletim sistemi örneğinin tümü, herhangi bir anda 10 GB RAM'in tamamını nadiren gerektirir.

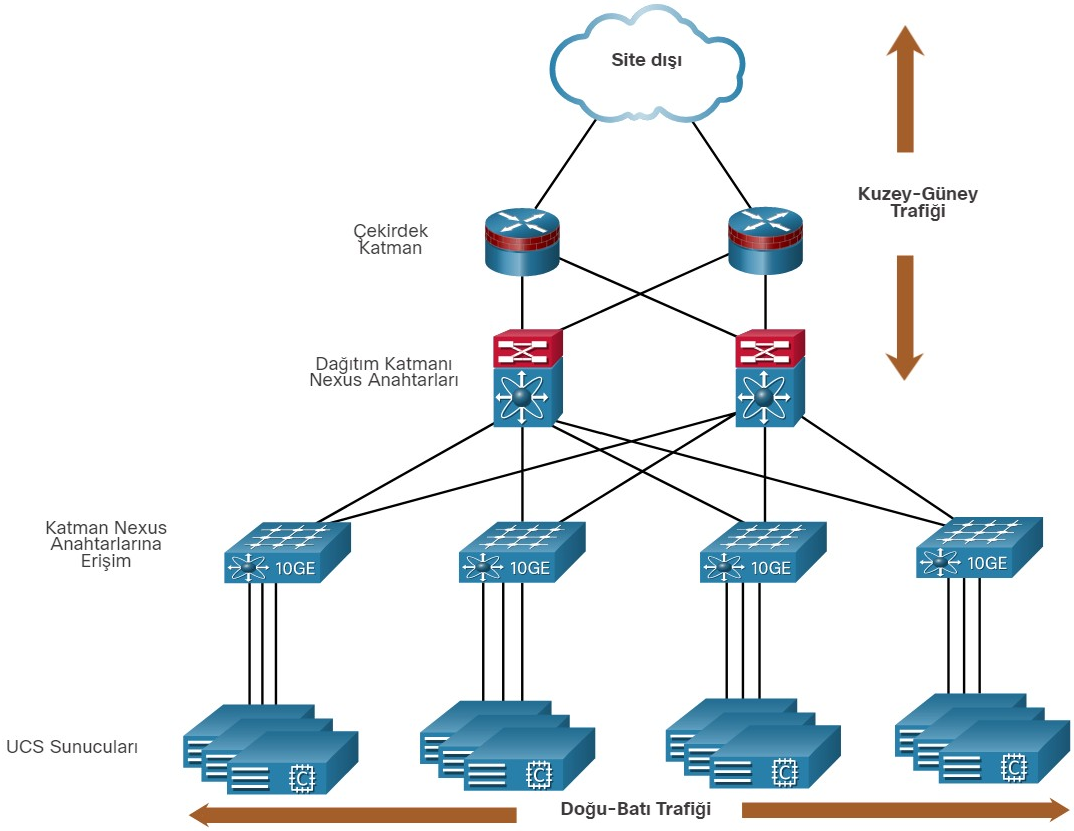
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 42.3.3.Ağ Sanallaştırmanın Karmaşıklığı

Sunucu sanallaştırma, fiziksel sunucuların, işlemcilerin ve işletim sistemlerinin sayısı ve kimliği gibi sunucu kaynaklarını sunucu kullanıcılarından gizler. Veri merkezi geleneksel ağ mimarilerini kullanıyorsa, bu uygulama sorun yaratabilir.

Örneğin, VM'ler tarafından kullanılan Sanal LAN'lar (VLAN'lar), hiper yönetici çalıştıran fiziksel sunucu ile aynı anahtar bağlantı noktasına atanmalıdır. Ancak, VM'ler taşınabilirdir ve ağ yöneticisinin ağ kaynaklarını ve profillerini ekleyebilmesi, çıkarabilmesi ve değiştirebilmesi gerekir. Bu işlem, geleneksel ağ anahtarları ile manuel ve zaman alıcı olacaktır.

Diğer bir sorun, trafik akışlarının geleneksel istemci-sunucu modelinden önemli ölçüde farklı olmasıdır. Tipik olarak, bir veri merkezi, şekilde gösterilen UCS sunucuları gibi sanal sunucular arasında önemli miktarda trafiğe sahiptir. Bu akışlara Doğu-Batı trafiği denir ve zaman içinde konum ve yoğunlukta değişiklik gösterebilir. Kuzey-Güney trafiği, dağıtım ve çekirdek katmanları arasında gerçekleşir ve genellikle başka bir veri merkezi, diğer bulut sağlayıcıları veya internet gibi site dışı konumlara yönelik trafiktir.




Dinamik sürekli değişen trafik, ağ kaynak yönetimine esnek bir yaklaşım gerektirir. Mevcut ağ altyapıları, bireysel akışlar için Hizmet Kalitesi (QoS) ve güvenlik düzeyi yapılandırmalarını kullanarak trafik akışlarının yönetimi ile ilgili değişen gereksinimlere yanıt verebilir. Ancak, çok tedarikçili ekipman kullanan büyük kuruluşlarda, yeni bir VM her etkinleştirildiğinde, gerekli yeniden yapılandırma çok zaman alabilir.

Ağ altyapısı da sanallaştırmadan yararlanabilir. Ağ işlevleri sanallaştırılabilir. Her ağ cihazı, bağımsız cihazlar olarak çalışan birden çok sanal cihaza bölünebilir. Örnekler arasında alt arayüzler, sanal arayüzler, VLAN'lar ve yönlendirme tabloları bulunur. Sanallaştırılmış yönlendirme, sanal yönlendirme ve yönlendirme (VRF-virtual routing and forwarding ) olarak adlandırılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 42.4.Yazılım Tanımlı Ağ( Software-Defined Networking)-SDN

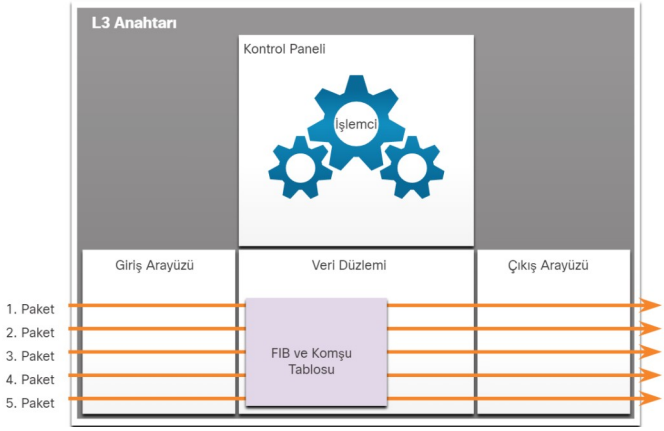
### 42.4.1.Kontrol Düzlemi ve Veri Düzlemi(Control Plane and Data Plane)

Bir ağ cihazı aşağıdaki düzlemleri içerir:

- 
- Kontrol düzlemi - Bu genellikle bir cihazın beyni olarak kabul edilir. Yönlendirme kararları vermek için kullanılır. Kontrol düzlemi, yönlendirme protokolü komşu tabloları ve topoloji tabloları, IPv4 ve IPv6 yönlendirme tabloları, STP ve ARP tablosu gibi Katman 2 ve Katman 3 yol yönlendirme mekanizmalarını içerir. Kontrol düzlemine gönderilen bilgiler CPU tarafından işlenir.
- Veri düzlemi - Yönlendirme düzlemi olarak da adlandırılan bu düzlem, tipik olarak bir cihazdaki çeşitli ağ bağlantı noktalarını bağlayan anahtar yapısıdır. Her cihazın veri düzlemi, trafik akışlarını iletmek için kullanılır.

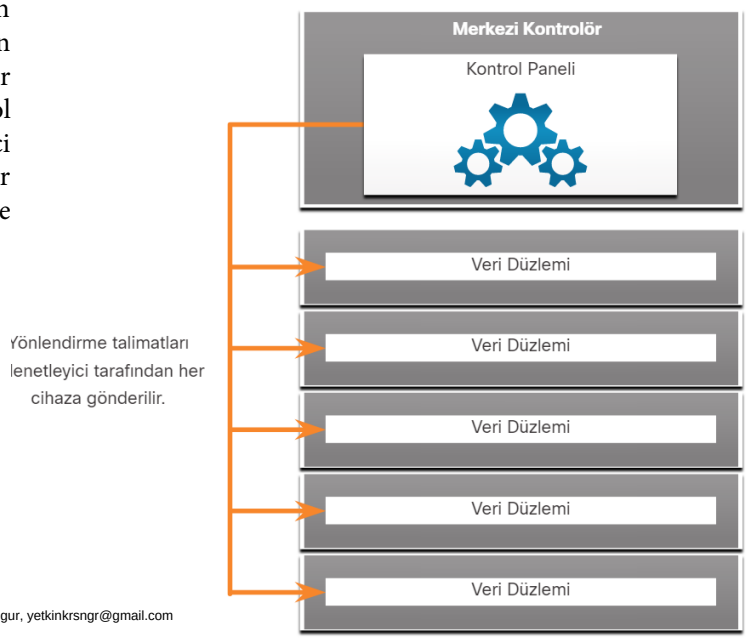
Yönlendiriciler ve anahtarlar, gelen trafiği uygun çıkış arayüzünden yönlendirmek için kontrol düzleminden gelen bilgileri kullanır. Veri düzlemindeki bilgiler tipik olarak, CPU dahil olmadan özel bir veri düzlemi işlemcisi tarafından işlenir.

Şekil, Cisco Express Forwarding'in (CEF) paketleri işlemek için kontrol düzlemini ve veri düzlemini nasıl kullandığını göstermektedir.




CEF, paketlerin kontrol düzlemine danışmadan veri düzleminde iletilmesini sağlayan gelişmiş bir Katman 3 IP anahtarlama teknolojisidir. CEF'de, kontrol düzleminin yönlendirme tablosu, veri düzlemindeki CEF Yönlendirme Bilgi Tabanı (FIB) tablosunu önceden doldurur. Kontrol düzleminin ARP tablosu bitişiklik tablosunu önceden doldurur. Paketler daha sonra, kontrol düzlemindeki bilgilere başvurmaya gerek kalmadan, FIB ve bitişik tablodaki bilgilere dayalı olarak veri düzlemi tarafından doğrudan iletilir.

SDN temelde kontrol düzlemi ile veri düzleminin ayrılmasıdır. Kontrol düzlemi işlevi her cihazdan kaldırılır ve şekilde gösterildiği gibi merkezi bir kontrolör tarafından gerçekleştirilir. Merkezi kontrolör, kontrol düzlemi işlevlerini her cihaza iletir. Merkezi denetleyici veri akışını yönetirken, güvenliği artırır ve diğer hizmetleri sağlarken artık her cihaz veri iletmeye odaklanabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

**Yönetim Düzlemi**

Şekillerde gösterilmeyen, bir cihazı ağa bağlantısı yoluyla yönetmekten sorumlu olan yönetim düzlemidir. Ağ yöneticileri, yönetim düzlemine erişmek ve bir cihazı yapılandırmak için Güvenli Kabuk (SSH), Önemsiz Dosya Aktarım Protokolü (TFTP), Güvenli FTP ve Güvenli Köprü Metni Aktarım Protokolü (HTTPS) gibi uygulamaları kullanır. Yönetim düzlemi, ağ çalışmalarınızda cihazlara nasıl eriştiğiniz ve bunları nasıl yapılandırdığınızdır. Ek olarak, Basit Ağ Yönetimi Protokolü (SNMP) gibi protokoller yönetim düzlemini kullanır.

## 42.4.2.Ağ Sanallaştırma Teknolojileri

On yıldan fazla bir süre önce, VMware bir ana işletim sisteminin bir veya daha fazla istemci işletim sistemini desteklemesini sağlayan bir sanallaştırma teknolojisi geliştirdi. Çoğu sanallaştırma teknolojisi artık bu teknolojiye dayanmaktadır. Adanmış sunucuların sanallaştırılmış sunuculara dönüşümü benimsenmiş ve veri merkezi ve kurumsal ağlarda hızla uygulanmaktadır.

Ağ sanallaştırmayı desteklemek için iki büyük ağ mimarisi geliştirilmiştir:

Yazılım Tanımlı Ağ Oluşturma (SDN) - Ağı sanallaştıran, ağ yönetimi ve yönetimine yönetim sürecini basitleştirmeyi ve kolaylaştırmayı amaçlayan yeni bir yaklaşım sunan bir ağ mimarisi.
Cisco Uygulama Merkezli Altyapısı-Cisco Application Centric Infrastructure (ACI) - Bulut bilişim ve veri merkezi yönetimini entegre etmek için amaca yönelik tasarlanmış bir donanım çözümü.

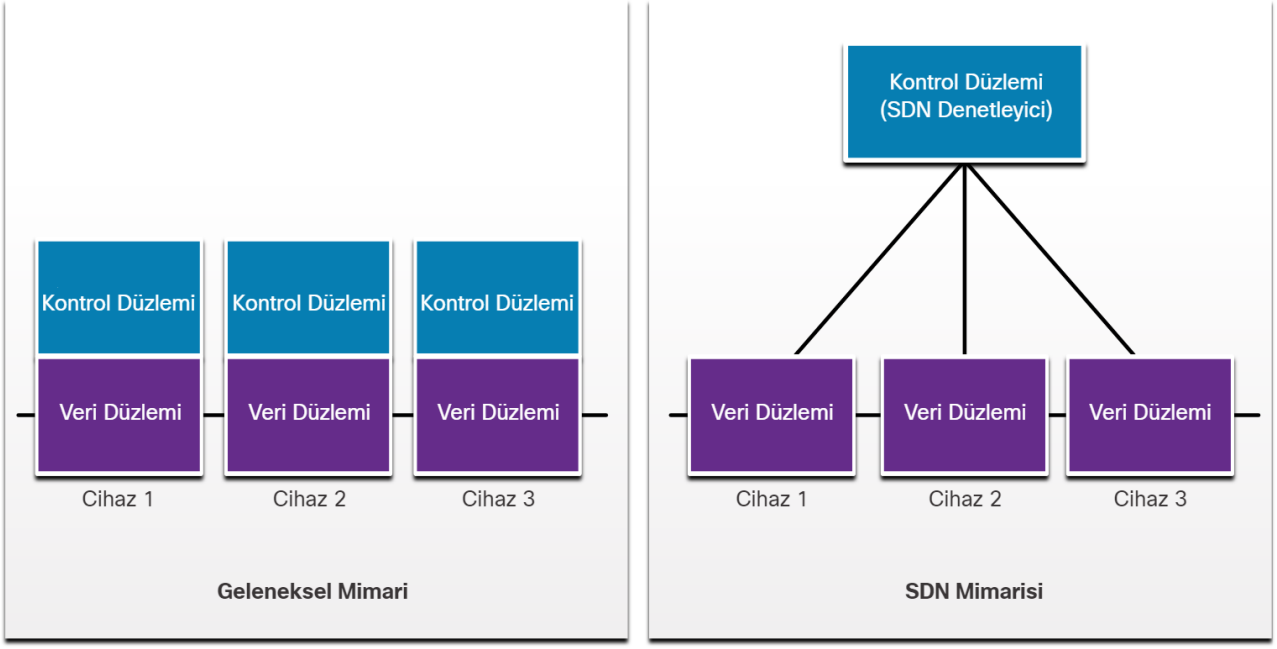
SDN'nin bileşenleri aşağıdakileri içerebilir:

- OpenFlow - Bu yaklaşım, yönlendiriciler, anahtarlar, kablosuz erişim noktaları ve bir denetleyici arasındaki trafiği yönetmek için Stanford Üniversitesi'nde geliştirilmiştir. OpenFlow protokolü, SDN çözümlerinin oluşturulmasında temel bir unsurdur. Daha fazla bilgi için OpenFlow ve Open Networking Foundation'ı arayın.
- OpenStack - Bu yaklaşım, ölçeklenebilir bulut ortamları oluşturmak ve bir IaaS çözümü sağlamak için tasarlanmış bir sanallaştırma ve düzenleme platformudur. OpenStack, genellikle Cisco ACI ile birlikte kullanılır. Ağ iletişiminde düzenleme, sunucular, depolama, anahtarlar, yönlendiriciler ve uygulamalar gibi ağ bileşenlerinin provizyonunu otomatikleştirme sürecidir. Daha fazla bilgi için OpenStack'i arayın.
- Diğer bileşenler - Diğer bileşenler arasında Yönlendirme Sistemine Arayüz- Interface to the Routing System(I2RS), Çok Sayıda Bağlantının Şeffaf Ara Bağlantısı-Transparent Interconnection of Lots of Links (TRILL), Cisco FabricPath (FP) ve IEEE 802.1aq En Kısa Yol Köprüleme-Shortest Path Bridging (SPB) bulunur.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

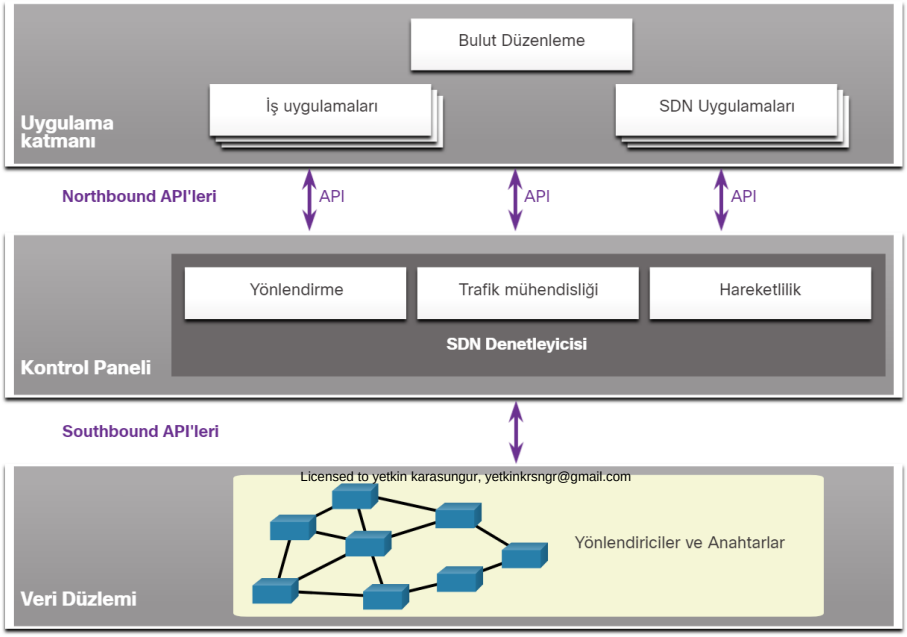
## 42.4.3.Geleneksel ve SDN Mimarileri

Geleneksel bir yönlendirici veya anahtar mimarisinde, kontrol düzlemi ve veri düzlemi işlevleri aynı cihazda gerçekleşir. Yönlendirme kararları ve paket iletme, aygıt işletim sisteminin sorumluluğundadır. SDN'de, kontrol düzleminin yönetimi merkezi bir SDN denetleyicisine taşınır. Şekil, geleneksel ve SDN mimarilerini karşılaştırmaktadır.




SDN denetleyicisi, ağ yöneticilerinin anahtarların ve yönlendiricilerin veri düzleminin ağ trafiğini nasıl yönetmesi gerektiğini yönetmesini ve dikte etmesini sağlayan mantıksal bir varlıktır. Uygulamalar ve ağ öğeleri arasındaki iletişimi düzenler, aracılık eder ve kolaylaştırır.

Tam SDN çerçevesi şekilde gösterilmiştir. SDN çerçevesi içinde Uygulama Programlama Arayüzlerinin-Application Programming Interfaces (API'ler) kullanımına dikkat edin. API, bir uygulamanın başka bir uygulamadan hizmet talep etmesi için doğru yolu tanımlayan standartlaştırılmış istekler kümesidir. SDN denetleyicisi, yukarı akış uygulamalarıyla iletişim kurmak için kuzeye giden API'leri kullanır. Bu API'ler, ağ yöneticilerinin trafiği şekillendirmesine ve hizmetleri dağıtmasına yardımcı olur. SDN denetleyicisi ayrıca, veri düzlemlerinin aşağı akış anahtarları ve yönlendiricilerdeki davranışını tanımlamak için güneye bağlı API'leri kullanır. OpenFlow, orijinal ve yaygın olarak uygulanan güneye bağlı API'dir.



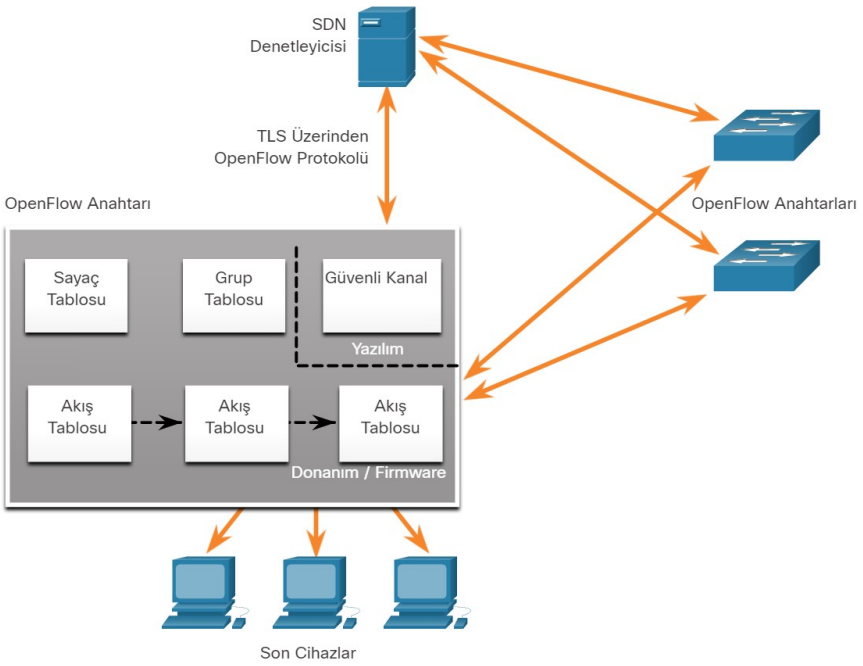
## 42.5.Kontrolörler- SDN Denetleyicileri

### 42.5.1.SDN Denetleyici ve İşlemleri

SDN denetleyici, merkezi kontrol düzlemi ile ayrı yönlendiriciler ve anahtarlar üzerindeki veri düzlemleri arasındaki veri akışlarını tanımlar.

Ağ üzerinden hareket eden her akış, önce, ağ politikasına göre iletişime izin verildiğini doğrulayan SDN denetleyicisinden izin almalıdır. Denetleyici bir akışa izin verirse, akışın alması için bir yol hesaplar ve yol üzerindeki anahtarların her birine bu akış için bir giriş ekler.

Tüm karmaşık işlevler kontrolör tarafından gerçekleştirilir. Denetleyici akış tablolarını doldurur. Anahtarlar akış tablolarını yönetir. Şekilde, bir SDN denetleyicisi OpenFlow protokolünü kullanarak OpenFlow uyumlu anahtarlarla iletişim kurar. Bu protokol, ağ üzerinden kontrol düzlemi iletişimlerini güvenli bir şekilde göndermek için Taşıma Katmanı Güvenliği'ni-Transport Layer Security (TLS) kullanır. Her bir OpenFlow anahtarı diğer OpenFlow anahtarlarına bağlanır. Ayrıca, bir paket akışının parçası olan son kullanıcı cihazlarına da bağlanabilirler.




Her anahtarda, anahtar aracılığıyla paket akışlarını yönetmek için donanımda veya bellenimde uygulanan bir dizi tablo kullanılır. Anahtar için akış, akış tablosundaki belirli bir girişle eşleşen paket dizisidir.

Önceki şekilde gösterilen üç tablo türü aşağıdaki gibidir:

- Akış Tablosu - Bu tablo, gelen paketleri belirli bir akışla eşleştirir ve paketler üzerinde gerçekleştirilecek işlevleri belirtir. Bir boru hattı tarzında çalışan birden çok akış tablosu olabilir.
- Grup Tablosu - Bir akış tablosu, bir akışı Grup Tablosuna yönlendirebilir ve bu da bir veya daha fazla akışı etkileyen çeşitli eylemleri tetikleyebilir.
- Sayaç Tablosu - Bu tablo, trafiği hız sınırlama yeteneği de dahil olmak üzere bir akışta performansla ilgili çeşitli eylemleri tetikler.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 42.5.2.Cisco ACI (Application Centric Infrastructure)

Gerçekten çok az sayıda kuruluş, ağı SDN araçlarını kullanarak programlama arzusuna veya becerisine sahiptir. Ancak, kuruluşların çoğu ağı otomatikleştirmek, uygulama dağıtımlarını hızlandırmak ve BT altyapılarını iş gereksinimlerini daha iyi karşılayacak şekilde uyumlu hale getirmek istiyor. Cisco, bu hedefleri daha önceki SDN yaklaşımlarından daha gelişmiş ve yenilikçi yollarla karşılamak için Uygulama Merkezli Altyapıyı (ACI) geliştirdi.

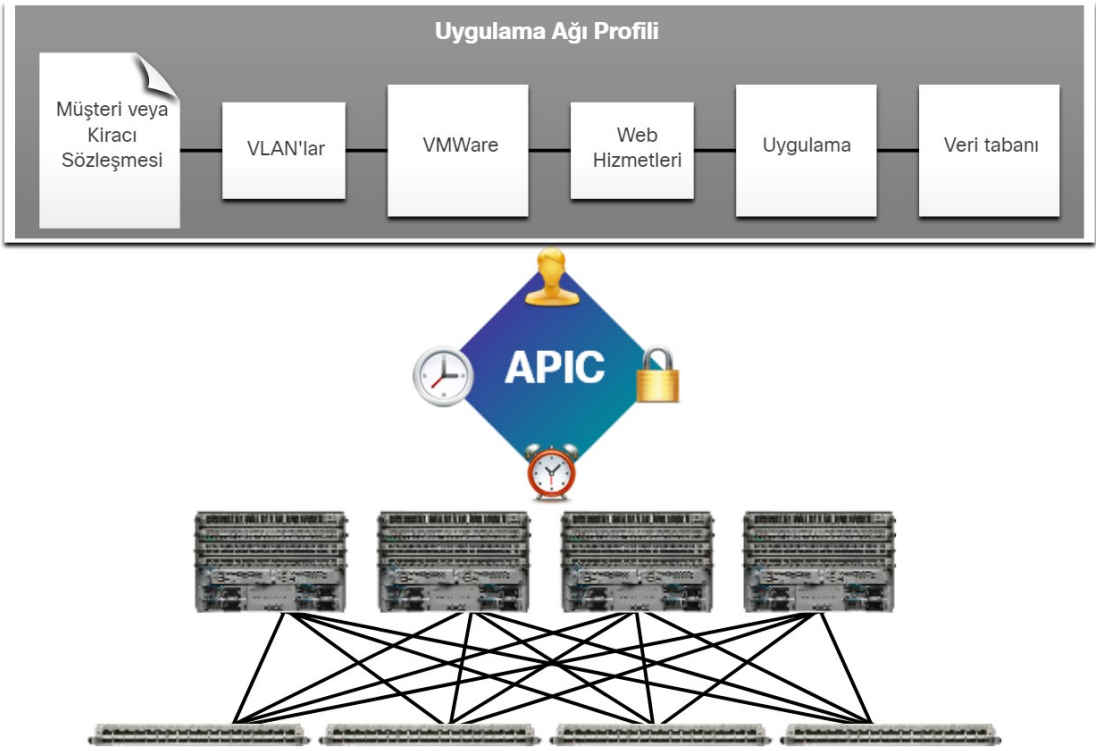
Cisco ACI, bulut bilişim ve veri merkezi yönetimini entegre etmek için bir donanım çözümüdür. Yüksek düzeyde, ağın politika öğesi veri düzleminden kaldırılır. Bu, veri merkezi ağlarının oluşturulma şeklini basitleştirir.

## 42.5.3.ACI'nin Temel Bileşenleri

ACI mimarisinin üç temel bileşeni şunlardır:

- Uygulama Ağı Profili-Application Network Profile (ANP) - Bir ANP, uç nokta gruplarının (EPG), bağlantılarının ve bu bağlantıları tanımlayan politikaların bir koleksiyonudur. Şekilde gösterilen VLAN'lar, web servisleri ve uygulamalar gibi EPG'ler sadece örnektir. Bir ANP genellikle çok daha karmaşıktır.
- Uygulama Politikası Altyapı Denetleyicisi-Application Policy Infrastructure Controller (APIC) - APIC, ACI mimarisinin beyni olarak kabul edilir. APIC, ölçeklenebilir bir ACI kümelenmiş yapısını yöneten ve çalıştıran merkezi bir yazılım denetleyicisidir. Programlanabilirlik ve merkezi yönetim için tasarlanmıştır. Uygulama politikalarını ağ programlamasına çevirir.
- Cisco Nexus 9000 Serisi anahtarlar- Cisco Nexus 9000 Series switches- Bu anahtarlar, uygulamaya duyarlı bir anahtarlama yapısı sağlar ve sanal ve fiziksel ağ altyapısını yönetmek için bir APIC ile çalışır.

APIC, APN ile ACI özellikli ağ altyapısı arasında konumlandırılır. APIC, şekilde gösterildiği gibi, uygulama gereksinimlerini bu ihtiyaçları karşılamak için bir ağ yapılandırmasına çevirir.



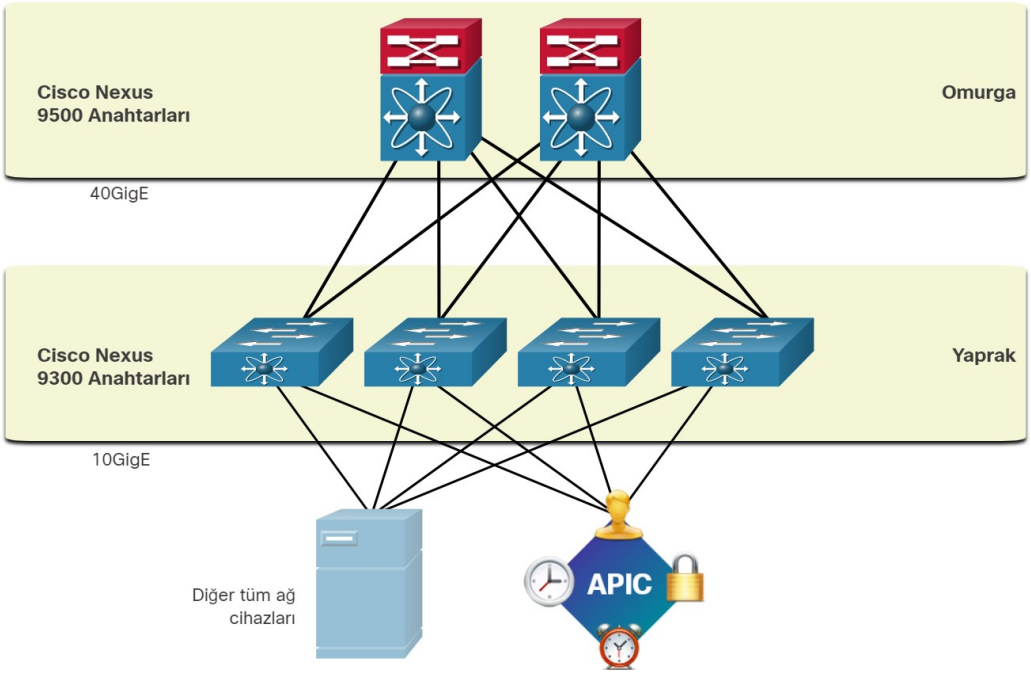

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 42.5.4.Omurga-Yaprak Topolojisi (Spine-Leaf Topology)

Cisco ACI yapısı, şekilde gösterildiği gibi, iki katmanlı omurga-yaprak topolojisi kullanan APIC ve Cisco Nexus 9000 serisi anahtarlardan oluşur. Yaprak anahtarlar her zaman omurgaya tutturulur, ancak asla birbirine yapışmazlar. Benzer şekilde, omurga anahtarları yalnızca kanat ve çekirdek anahtarlara (gösterilmemiştir) takılır. Bu iki katmanlı topolojide, her şey diğer her şeyden bir atlama şeklindedir.

Cisco APIC'leri ve ağdaki diğer tüm cihazlar, yaprak anahtarlara fiziksel olarak bağlanır.

SDN ile karşılaştırıldığında, APIC denetleyicisi veri yolunu doğrudan değiştirmez. Bunun yerine APIC, politika tanımını merkezileştirir ve yaprak anahtarlarını, tanımlanan politikalara göre trafiği yönlendirecek şekilde programlar.

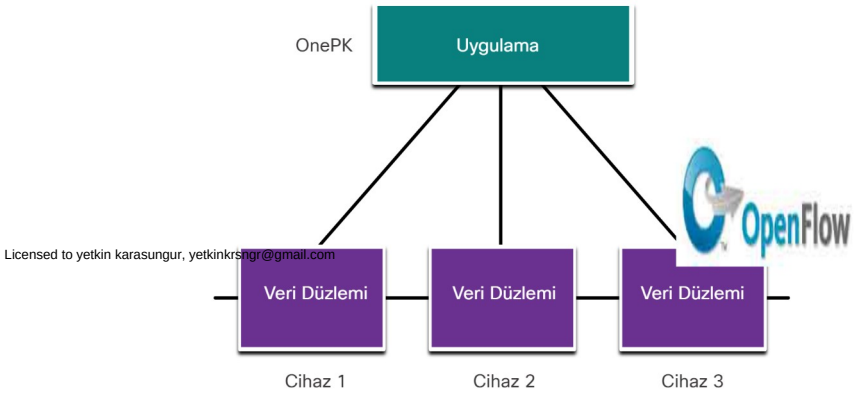



## 42.5.5.SDN Tipleri

Cisco Uygulama Politikası Altyapı Denetleyicisi - Kurumsal Modül-Cisco Application Policy Infrastructure Controller - Enterprise Module (APIC-EM), kuruluş ve kampüs dağıtımlarına yönelik ACI'yı genişletir. APIC-EM'yi daha iyi anlamak için, üç SDN türüne daha geniş bir göz atmak faydalı olacaktır.

### Cihaz Tabanlı SDN

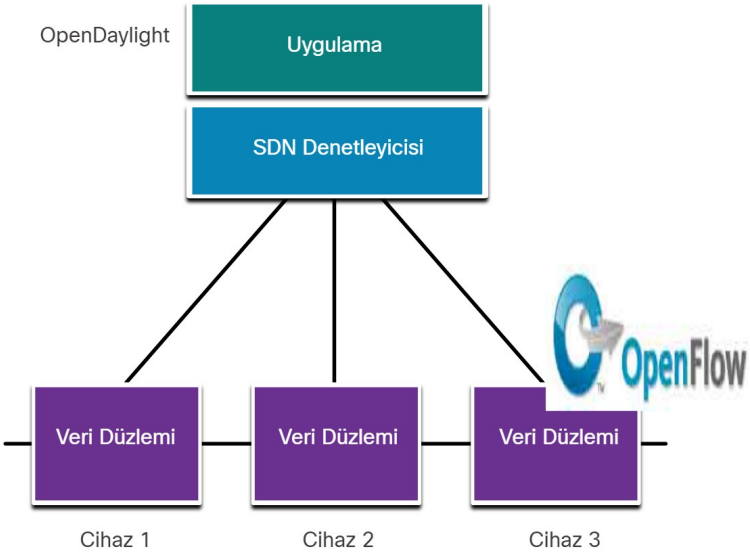
Bu tür SDN'de, cihazlar, şekilde gösterildiği gibi, cihazın kendisinde veya ağdaki bir sunucuda çalışan uygulamalar tarafından programlanabilir. Cisco OnePK, cihaz tabanlı bir SDN örneğidir. Programcıların Cisco cihazlarını entegre etmek ve bunlarla etkileşim kurmak için C ve Python ile Java kullanarak uygulamalar oluşturmasına olanak tanır.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

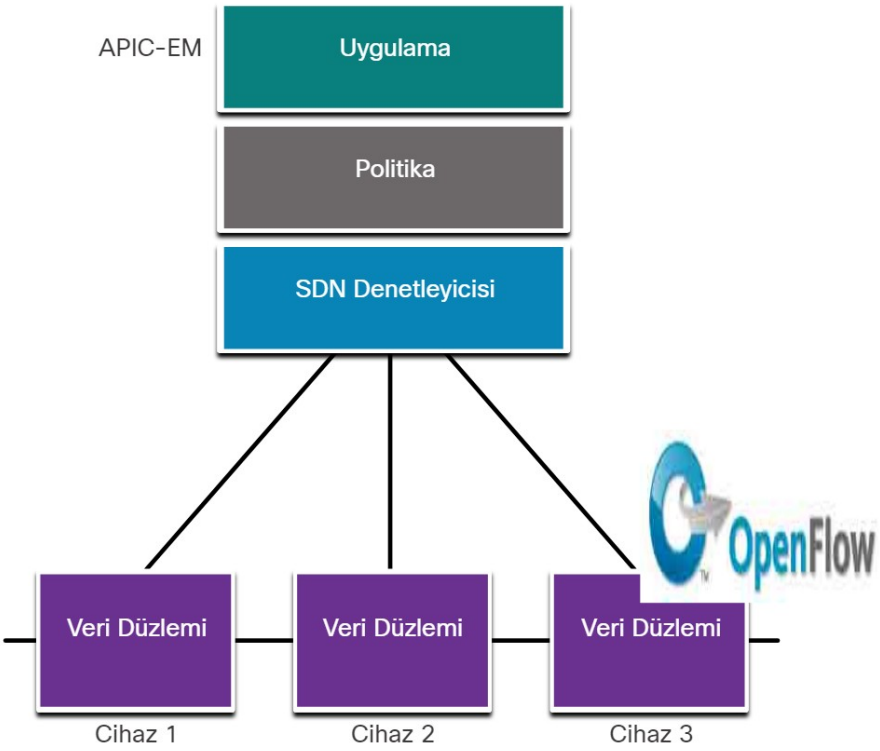
## Denetleyici Tabanlı SDN

Bu tür SDN, şekilde gösterildiği gibi ağdaki tüm cihazların bilgisine sahip merkezi bir kontrolör kullanır. Uygulamalar, cihazların yönetilmesinden ve ağdaki trafik akışlarının yönetilmesinden sorumlu kontrolör ile arayüz oluşturabilir. Cisco Open SDN Denetleyicisi, OpenDaylight'ın ticari bir dağıtımıdır.




## Politika Tabanlı SDN

Bu tür SDN, şekilde gösterildiği gibi, merkezi bir denetleyicinin ağdaki tüm cihazların bir görünümüne sahip olduğu denetleyici tabanlı SDN'ye benzer. Politika tabanlı SDN, daha yüksek bir soyutlama düzeyinde çalışan ek bir Politika katmanı içerir. Kılavuzlu bir iş akışı ve kullanıcı dostu GUI aracılığıyla gelişmiş yapılandırma görevlerini otomatikleştiren yerleşik uygulamaları kullanır. Hiçbir programlama becerisi gerekmez. Cisco APIC-EM, bu tür SDN'nin bir örneğidir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

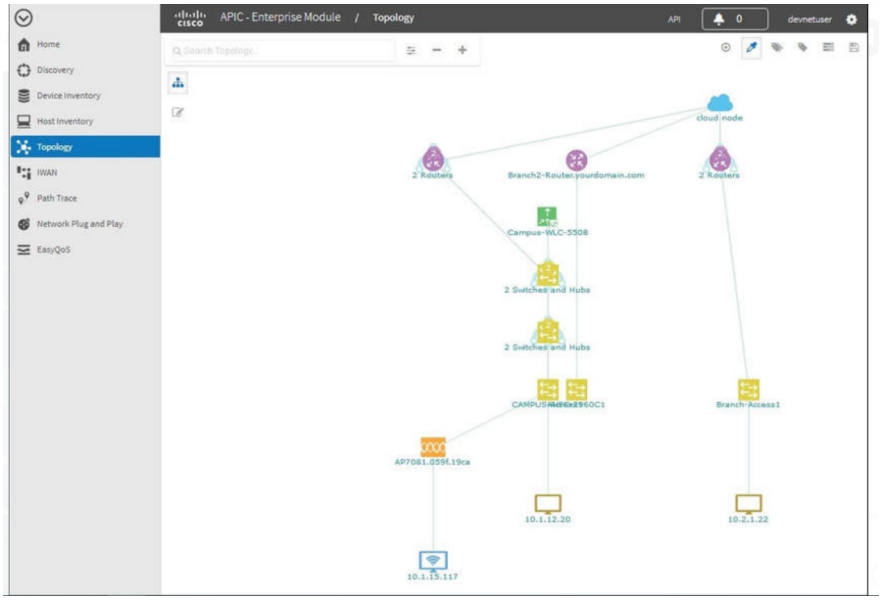
## 42.5.6.APIC-EM Özellikleri

Her tür SDN'nin kendine has özellikleri ve avantajları vardır. Politika tabanlı SDN en sağlam olanıdır ve ağın tamamındaki politikaları kontrol etmek ve yönetmek için basit bir mekanizma sağlar.

Cisco APIC-EM, politika tabanlı SDN'nin bir örneğidir. Cisco APIC-EM, aşağıdakileri içeren ağ yönetimi için tek bir arayüz sağlar:

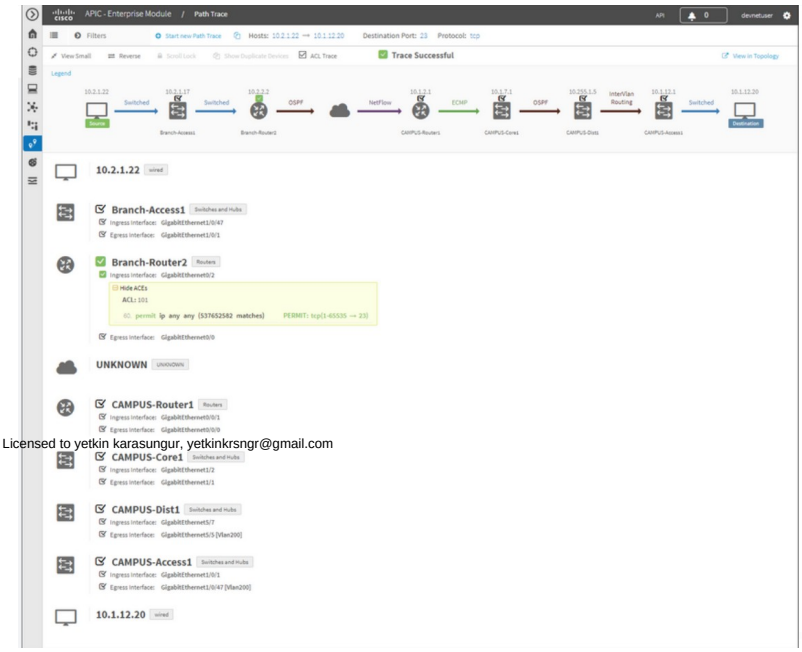
- cihaz ve ana bilgisayar envanterlerini keşfetmek ve bunlara erişmek,
- topolojiyi görüntüleme (şekilde gösterildiği gibi),
- uç noktalar arasında bir yol izlemek ve
- politikaları belirleme.

APIC-EM Demosuna https://sandboxapic.cisco.com adresinden
Kullanıcı Adı: devnetuser
Parola: Cisco123!
İle giriş yapabilirsiniz.




## 42.5.7.APIC-EM Yol İzleme (Path Trace)

APIC-EM Yol İzleme aracı, yöneticinin trafik akışlarını kolayca görselleştirmesine ve çakışan, yinelenen veya gölgeli ACL girişlerini keşfetmesine olanak tanır. Bu araç, iki uç düğüm arasındaki yoldaki belirli ACL'leri inceler ve olası sorunları görüntüler. Şekilde gösterildiği gibi, yol boyunca ACL'lerin trafiğinize nerede izin verdiğini veya engellediğini görebilirsiniz. Branch-Router2'nin tüm trafiğe nasıl izin verdiğine dikkat edin. Ağ yöneticisi artık trafiği daha iyi filtrelemek için gerekirse ayarlamalar yapabilir.




Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

# 43.Bölüm: Ağ Otomasyonu

## 43.1.Otomasyona Genel Bakış

### 43.1.1.Otomasyondaki Artış

Otomasyon, kendi kendine çalışan, insan müdahalesi ihtiyacını azaltan ve potansiyel olarak ortadan kaldıran herhangi bir süreçtir.

Otomasyon bir zamanlar imalat endüstrisiyle sınırlıydı. Otomobil montajı gibi oldukça tekrarlayan işler makinelere devredildi ve modern montaj hattı doğdu. Makineler, aynı görevi yorulmadan ve insanların bu tür işlerde yapmaya meyilli olduğu hatalar olmadan tekrarlama konusunda mükemmeldir.

Otomasyonun faydalarından bazıları şunlardır:

- Makineler günde 24 saat kesintisiz çalışabilir, bu da daha fazla çıktı sağlar.
- Makineler daha düzgün bir ürün sağlar.
- Otomasyon, bir olayı veya süreci yönlendirmeye yardımcı olabilecek bilgiler sağlamak için hızla analiz edilebilen büyük miktarda verinin toplanmasına izin verir.
- Robotlar, madencilik, yangınla mücadele ve endüstriyel kazaların temizlenmesi gibi tehlikeli koşullarda kullanılmaktadır. Bu, insanlara yönelik riski azaltır.
- Belirli koşullar altında akıllı cihazlar, enerji kullanımını azaltmak, tıbbi bir teşhis koymak ve otomobil sürüş güvenliğini artırmak için davranışlarını değiştirebilir.

### 43.1.2.Düşünen Cihazlar

Cihazlar düşünebilir mi? Çevrelerinden öğrenebilirler mi? Bu bağlamda “düşünmek” kelimesinin birçok tanımı vardır. Olası bir tanım, bir dizi ilgili bilgi parçasını birbirine bağlama ve ardından bunları bir eylem planını değiştirmek için kullanma becerisidir.

Artık birçok cihaz, davranışlarını yönetmeye yardımcı olmak için akıllı teknolojiyi kullanıyor. Bu, en yoğun talep dönemlerinde güç tüketimini azaltan akıllı bir cihaz kadar basit veya sürücüsüz bir araba kadar karmaşık olabilir.

Bir cihaz, dışarıdaki bir bilgi parçasına dayalı bir hareket tarzı gerçekleştirdiğinde, o cihaza akıllı cihaz adı verilir. Etkileşimde bulunduğumuz birçok cihazın adlarında artık akıllı kelimesi var. Bu, aygıtın ortamına bağlı olarak davranışını değiştirme yeteneğine sahip olduğunu gösterir.

Cihazların "düşünebilmesi" için ağ otomasyon araçları kullanılarak programlanmaları gerekir.

## 43.2.Veri Biçimleri

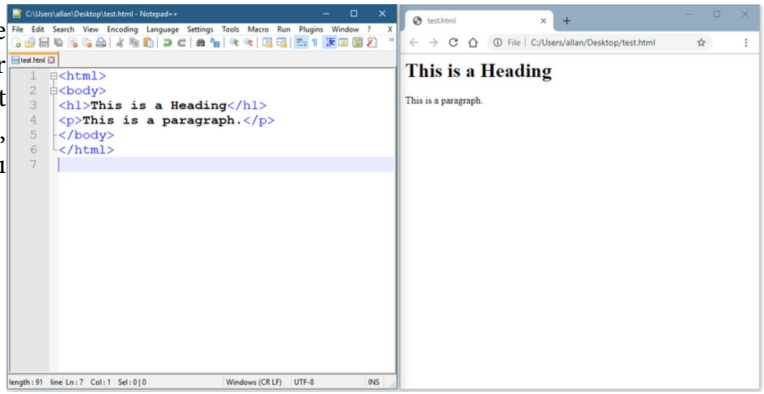
### 43.2.1.Veri Biçimleri Kavramı

Akıllı cihazlar aslında küçük bilgisayarlardır. Mantıksal sürücü gibi bir akıllı cihazın değişen koşullara tepki verebilmesi için, sensör gibi başka bir akıllı cihaz tarafından kendisine gönderilen bilgileri alabilmesi ve yorumlayabilmesi gerekir. Bu iki akıllı cihaz, veri formatı adı verilen ortak bir 'dili' paylaşmalıdır. Paylaşılan veri formatları, ağdaki diğer cihazlar tarafından da kullanılır.

Verileri insanlarla paylaşırken, bu bilgilerin nasıl gösterileceğine dair olasılıklar neredeyse sonsuzdur. Örneğin, bir restoranın menüyü nasıl biçimlendirebileceğini düşünün. Yalnızca metin, madde işaretli bir liste veya başlık içeren fotoğraflar veya yalnızca fotoğraflar olabilir. Bunların hepsi, restoranın menüyü oluşturan verileri biçimlendirebileceği farklı yollardır. İyi tasarlanmış bir form, bilgileri hedef kitlenin anlaması için en kolay hale getiren şey tarafından belirlenir. Aynı ilke, bilgisayarlar arasında paylaşılan veriler için de geçerlidir. Bir bilgisayar, verileri başka bir bilgisayarın anlayabileceği bir biçime koymalıdır.

Licensed to yetkin karasunger, yetkinkrsnan@gmail.com

Veri biçimleri, verileri yapılandırılmış bir biçimde depolamanın ve değiştirmenin bir yoludur. Böyle bir biçim, Köprü Metni Biçimlendirme Dili-Hypertext Markup Language (HTML) olarak adlandırılır. HTML, şekilde gösterildiği gibi web sayfalarının yapısını açıklamak için standart bir biçimlendirme dilidir.




Bunlar, ağ otomasyonu ve programlanabilirlik dahil olmak üzere birçok uygulamada kullanılan bazı yaygın veri biçimleridir:

- 
- JavaScript Nesne Gösterimi-JavaScript Object Notation (JSON)
- eXtensible Markup Language (XML)
- YAML, Biçimlendirme Dili Değildir-Ain't Markup Language (YAML)

Seçilen veri formatı, kullandığınız uygulama, araç veya komut dosyası tarafından kullanılan formata bağlı olacaktır. Birçok sistem birden fazla veri formatını destekleyebilir ve bu da kullanıcının tercih ettiği formatı seçmesine olanak tanır.

### 43.2.2.Veri Biçimi Kuralları

Veri formatlarının, programlama ve yazı dillerinde sahip olduğumuza benzer kuralları ve yapısı vardır. Her veri formatının belirli özellikleri olacaktır:

- [ ] , (), {}, Beyaz boşluk kullanımı veya girinti, tırnak işaretleri, virgül ve daha fazlası gibi kullanılan parantez türlerini içeren sözdizimi .
- Karakterler, dizeler, listeler ve diziler gibi nesnelerin nasıl temsil edildiği.
- Anahtar / değer çiftlerinin nasıl temsil edildiği. Anahtar genellikle sol taraftadır ve verileri tanımlar veya açıklar. Sağdaki değer verinin kendisidir ve bir karakter, dize, sayı, liste veya başka bir veri türü olabilir.

Uluslararası Uzay İstasyonunun mevcut konumunu izleyen bir web sitesi bulmak için internette "ISS konumunu şimdi bildir" için arama yapın. Bu web sitesinde veri formatlarının nasıl kullanıldığını ve aralarındaki bazı benzerlikleri görebilirsiniz. Bu web sitesi, bir sunucuya basit bir Uygulama Programlama Arayüzü (API) çağrısı için bir bağlantı içerir; bu, uzay istasyonunun geçerli enlem ve boylamını bir UNIX zaman damgasıyla birlikte döndürür. Aşağıdaki örnek, sunucu tarafından JavaScript Nesne Gösterimi (JSON) kullanılarak döndürülen bilgileri gösterir. Bilgi ham formatta görüntülenir. Bu, verilerin yapısını anlamayı zorlaştırabilir.

```
{"message": "success", "timestamp": 1560789216, "iss_position": {"latitude": "25.9990", "longitude":
"-132.6992"}}
```

"JSONView" tarayıcı uzantısını veya JSON'u daha okunabilir bir biçimde görüntülemenize olanak tanıyan herhangi bir uzantıyı bulmak için internette arama yapın. Veri nesneleri anahtar / değer çiftlerinde görüntülenir. Aşağıdaki çıktı, JSONView kullanılarak bu aynı çıktıyı gösterir. Anahtar / değer çiftlerinin yorumlanması çok daha kolaydır. Aşağıdaki örnekte, anahtar enlemini ve 25.9990 değerini görebilirsiniz .

```
{
        "message": "success",
        "timestamp": 1560789260,
        "iss_position": {
                "latitude": "25.9990",
                "longitude": "-132.6992"
        }
}
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 43.2.3.Veri Biçimlerinin Karşılaştırması

Aynı verileri XML veya YAML olarak biçimlendirilmiş görmek için internette bir JSON dönüştürme aracı arayın. Bu noktada, her veri formatının ayrıntılarını anlamak önemli değildir, ancak her veri formatının sözdizimini nasıl kullandığına ve anahtar / değer çiftlerinin nasıl temsil edildiğine dikkat edin.

JSON Biçimi

```
{
        "message": "success",
        "timestamp": 1560789260,
        "iss_position": {
                "latitude": "25.9990",
                "longitude": "-132.6992"
        }
}
```

YAML Biçimi

```
message: success
timestamp: 1560789260
iss_position:
    latitude: '25.9990'
    longitude: '-132.6992'
```

XML Biçimi

```
<?xml version="1.0" encoding="UTF-8" ?>
<root>
  <message>success</message>
  <timestamp>1560789260</timestamp>
  <iss_position>
    <latitude>25.9990</latitude>
    <longitude>-132.6992</longitude>
  </iss_position>
</root>
```

### 43.2.4.JSON Veri Biçimi

JSON, uygulamalar tarafından verileri depolamak, aktarmak ve okumak için kullanılan, okunabilir bir veri formatıdır. JSON, herkese açık veriler sağlamak için web hizmetleri ve API'ler tarafından kullanılan çok popüler bir formattır. Bunun nedeni, ayrıştırılması kolay olması ve Python da dahil olmak üzere çoğu modern programlama diliyle kullanılabilmesidir.

Aşağıdaki çıktı, bir yönlendiricideki **show interface GigabitEthernet0/0/0** komutundan kısmi IOS çıkışı örneğini gösterir .

```
GigabitEthernet0/0/0 is up, line protocol is up (connected)
  Description: Wide Area Network
  Internet address is 172.16.0.2/24
```

Aynı bilgiler JSON formatında gösterilebilir. Her nesnenin (her anahtar / değer çifti), adı, açıklaması ve arabirimin etkinleştirilip etkinleştirilmediğini içeren arabirim hakkında farklı bir veri parçası olduğuna dikkat edin.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

JSON Çıkışı

```
{
    "ietf-interfaces:interface": {
        "name": "GigabitEthernet0/0/0",
        "description": "Wide Area Network",
        "enabled": true,
        "ietf-ip:ipv4": {
            "address": [
                {
                    "ip": "172.16.0.2",
                    "netmask": "255.255.255.0"
                }
            ]
        }
    }
}
```

### 43.2.5.JSON Sözdizimi Kuralları

JSON'un özelliklerinden bazıları şunlardır:

- Hiyerarşik bir yapı kullanır ve iç içe geçmiş değerler içerir.
- Nesneleri ve köşeli parantezleri [ ] dizileri tutmak için parantez {} kullanır .
- Verileri anahtar / değer çiftleri olarak yazılır.
- JSON'da, nesne olarak bilinen veriler, süslü ayraçlar {} içine alınmış bir veya daha fazla anahtar / değer çiftidir.

JSON nesnesinin sözdizimi şunları içerir:

- Anahtarlar çift tırnak işareti "" içinde dizeler olmalıdır.
- Değerler, geçerli bir JSON veri türü (dize, sayı, dizi, Boolean, null veya başka bir nesne) olmalıdır.
- Anahtarlar ve değerler iki nokta üst üste ile ayrılır.
- Bir nesne içindeki birden çok anahtar / değer çifti virgülle ayrılır.
- Boşluk önemli değil.

Bazen bir anahtar birden fazla değer içerebilir. Bu dizi olarak bilinir. JSON'daki bir dizi, sıralı bir değerler listesidir. JSON'daki dizilerin özellikleri şunları içerir:

- Anahtar ve ardından iki nokta üst üste işareti ve köşeli parantez [ ] içinde değerlerin listesi .
- Dizi, sıralı bir değerler listesidir.
- Dizi, dizi içinde bir dizi, sayı, Boole, nesne veya başka bir dizi dahil olmak üzere birden çok değer türü içerebilir.
- Dizideki her bir değer virgülle ayrılır.

Örneğin, IPv4 adreslerinin bir listesi aşağıdaki çıktı gibi görünebilir. Anahtar "adresler" dir. Listedeki her öğe, süslü ayraçlar {} ile ayrılmış ayrı bir nesnedir. Nesneler iki anahtar / değer çiftidir: bir IPv4 adresi ("ip") ve virgülle ayrılmış bir alt ağ maskesi ("ağ maskesi"). Listedeki nesneler dizisi, her nesne için kapatma ayracının ardından virgülle ayrılır.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

JSON IPv4 Adresleri Listesi

```
{
  "addresses": [
    {
      "ip": "172.16.0.2",
      "netmask": "255.255.255.0"
    },
    {
      "ip": "172.16.0.3",
      "netmask": "255.255.255.0"
    },
    {
      "ip": "172.16.0.4",
      "netmask": "255.255.255.0"
    }
  ]
}
```

### 43.2.6.YAML Veri Formatı

YAML, uygulamalar tarafından verileri depolamak, aktarmak ve okumak için kullanılan başka bir insan tarafından okunabilir veri formatı türüdür. YAML'nin bazı özelliklerinden bazıları şunlardır:

- JSON gibidir ve JSON'un bir üst kümesi olarak kabul edilir.
- Hem okumayı hem de yazmayı kolaylaştıran minimalist bir formatı vardır.
- Köşeli parantez veya virgül kullanmadan yapısını tanımlamak için girintiyi kullanır.

Örneğin, bir Gigabit Ethernet 2 arayüzü için bu JSON çıkışına bakın.

```
{
   "ietf-interfaces:interface": {
      "name": "GigabitEthernet2",
      "description": "Wide Area Network",
      "enabled": true,
      "ietf-ip:ipv4": {
         "address": [
            {
               "ip": "172.16.0.2",
               "netmask": "255.255.255.0"
            },
            {
               "ip": "172.16.0.3",
               "netmask": "255.255.255.0"
            },
            {
               "ip": "172.16.0.4",
               "netmask": "255.255.255.0"
            }
         ]
      }
   }
}
```

YAML formatındaki aynı verilerin okunması daha kolaydır. JSON'a benzer şekilde, bir YAML nesnesi bir veya daha fazla anahtar-değer çiftidir. Anahtar değer çiftleri, tırnak işaretleri kullanılmadan iki nokta üst üste ile ayrılır. YAML'de, bir listedeki her bir öğeyi ayırmak için bir kısa çizgi kullanılır. Bu, aşağıdaki çıktıdaki üç IPv4 adresi için gösterilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

```yaml
ietf-interfaces:interface:
  name: GigabitEthernet2
  description: Wide Area Network
  enabled: true
  ietf-ip:ipv4:
    address:
    - ip: 172.16.0.2
      netmask: 255.255.255.0
    - ip: 172.16.0.3
      netmask: 255.255.255.0
    - ip: 172.16.0.4
      netmask: 255.255.255.0
```

### 43.2.7.XML Veri Biçimi

XML, uygulamalar tarafından verileri depolamak, aktarmak ve okumak için kullanılan bir başka insan tarafından okunabilir veri formatı türüdür. XML'in bazı özellikleri şunları içerir:

Web sayfaları ve web uygulamaları oluşturmak için standartlaştırılmış biçimlendirme dili olan HTML gibidir.
Kendini tanımlayıcıdır. Verileri ilgili bir etiket kümesi içinde barındırır: < etiket > veri < / etiket >
HTML'den farklı olarak, XML önceden tanımlanmış etiket veya belge yapısı kullanmaz.
XML nesneleri, başlangıç etiketi anahtarın adı olarak kullanılan bir veya daha fazla anahtar / değer çiftidir: < anahtar > değer < / anahtar >

Aşağıdaki çıktı, XML veri yapısı olarak biçimlendirilmiş GigabitEthernet2 için aynı verileri gösterir. Değerlerin nesne etiketlerinin içine nasıl yerleştirildiğine dikkat edin. Bu örnekte, her anahtar / değer çifti ayrı bir satırdadır ve bazı satırlar girintilidir. Bu gerekli değildir ancak okunabilirlik için yapılır. Liste, listedeki her öğe için tekrarlanan < etiket > < / etiket > örneklerini kullanır . Bu tekrarlanan örneklerdeki öğeler, bir veya daha fazla anahtar / değer çiftini temsil eder.

```xml
<?xml version="1.0" encoding="UTF-8" ?>
<ietf-interfaces:interface>
  <name>GigabitEthernet2</name>
  <description>Wide Area Network</description>
  <enabled>true</enabled>
  <ietf-ip:ipv4>
    <address>
      <ip>172.16.0.2</ip>
      <netmask>255.255.255.0</netmask>
    </address>
    <address>
      <ip>172.16.0.3</ip>
      <netmask>255.255.255.0</netmask>
    </address>
    <address>
      <ip>172.16.0.4</ip>
      <netmask>255.255.255.0</netmask>
    </address>
  </ietf-ip:ipv4>
</ietf-interfaces:interface>
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

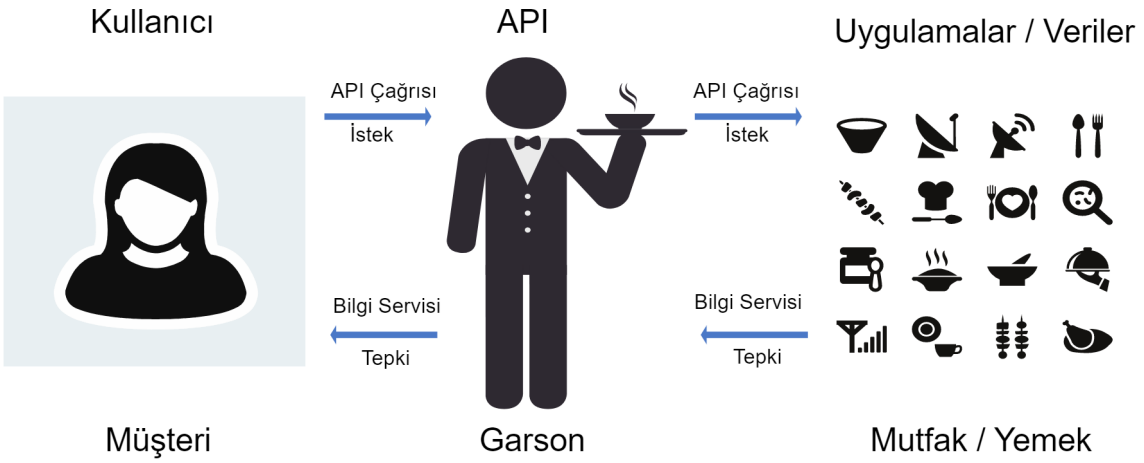
## 43.3.API'ler

### 43.3.1.API Kavramı

API'ler hemen hemen her yerde bulunur. Amazon Web Services, Facebook ve termostatlar, buzdolapları ve kablosuz aydınlatma sistemleri gibi ev otomasyon cihazlarının tümü API kullanır. Programlanabilir ağ otomasyonu oluşturmak için de kullanılırlar.

API, diğer uygulamaların verilerine veya hizmetlerine erişmesine izin veren bir yazılımdır. Bir uygulamanın diğeriyle nasıl etkileşime girebileceğini ve etkileşimin gerçekleşmesine izin veren talimatları açıklayan bir dizi kuraldır. Kullanıcı, belirli bilgileri isteyen bir sunucuya bir API isteği gönderir ve istenen bilgilerle birlikte sunucudan karşılığında bir API yanıtı alır.

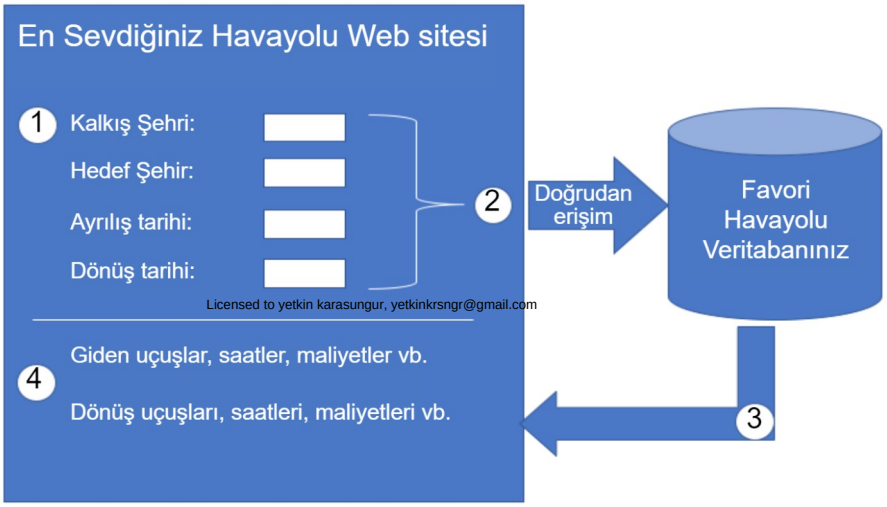
Bir API, aşağıdaki şekilde gösterildiği gibi bir restorandaki garsona benzer. Bir restorandaki bir müşteri, masaya yemek getirilmesini istiyor. Yemekler pişirildiği ve hazırlandığı mutfakta. Garson, API'ye benzer bir haberci. Garson (API), müşterinin siparişini (talebi) alan ve mutfağa ne yapması gerektiğini söyleyen kişidir. Yemek hazır olduğunda, garson yemeği (yanıt) müşteriye geri gönderir.



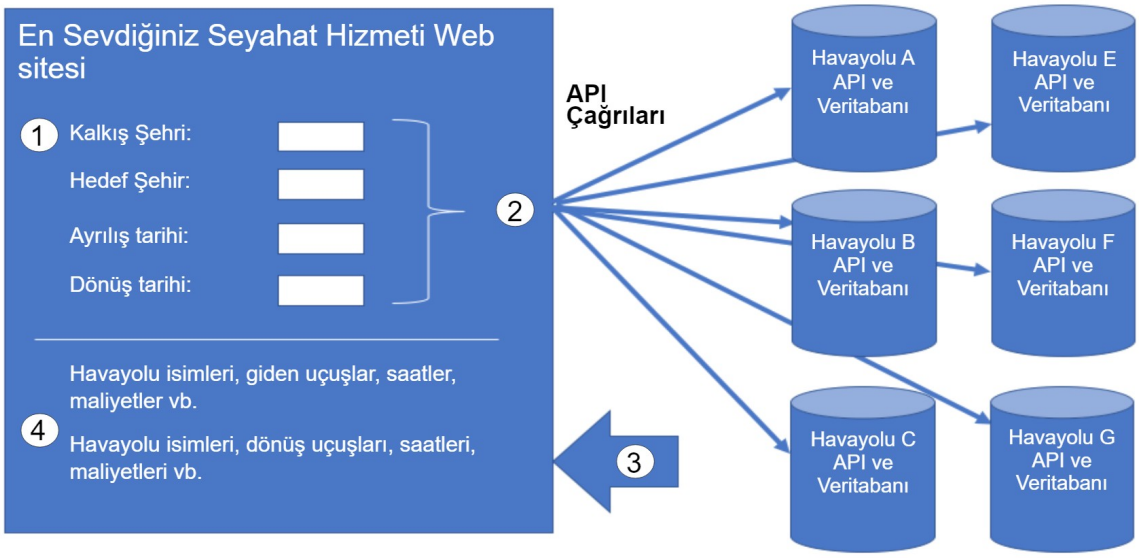

Daha önce, Uluslararası Uzay İstasyonu'nun geçerli enlem ve boylamını döndüren bir sunucuya bir API isteği gördünüz. Bu, Open Notify'ın Ulusal Havacılık ve Uzay Dairesi'ndeki (NASA) bir web tarayıcısından verilere erişmeyi sağlayan bir API idi.

### 43.3.2.Bir API Örneği

API'lerin veri ve hizmet sağlamak için nasıl kullanılabileceğini gerçekten anlamak için, havayolu rezervasyonları için iki seçeneğe bakacağız. İlk seçenek, şekilde gösterildiği gibi belirli bir havayolunun web sitesini kullanır. Kullanıcı, havayolunun web sitesini kullanarak rezervasyon talebinde bulunmak için bilgileri girer. Web sitesi, doğrudan havayolunun kendi veri tabanı ile etkileşime girer ve kullanıcıya, kullanıcının talebiyle eşleşen bilgileri sağlar.



Kendi bilgilerine doğrudan erişimi olan tek bir havayolu web sitesini kullanmak yerine ikinci bir seçenek vardır. Kullanıcılar, yalnızca belirli bir havayolundan değil, çeşitli havayollarından bu aynı bilgilere erişmek için bir seyahat sitesini kullanabilir. Bu durumda kullanıcı, benzer rezervasyon bilgilerini girer. Seyahat hizmeti web sitesi, her bir havayolu tarafından sağlanan API'leri kullanarak çeşitli havayolu veritabanları ile etkileşim kurar. Seyahat hizmeti, söz konusu havayolundan bilgi istemek için her bir havayolu API'sini kullanır ve ardından şekilde gösterildiği gibi, tüm havayollarının bilgilerini kendi web sayfasında görüntüler.




API, talep eden uygulama ile veriyi veya hizmeti sağlayan sunucudaki uygulama arasında bir tür haberci görevi görür. İstekte bulunan uygulamadan verilerin bulunduğu sunucuya gönderilen mesaj, API çağrısı olarak bilinir.

### 43.3.3.Açık, Dahili ve İş Ortağı API'leri

Bir API geliştirirken dikkat edilmesi gereken önemli bir nokta, açık, dahili ve iş ortağı API'leri arasındaki ayrımdır:

- 
- Açık API'ler veya Genel API'ler - Bu API'ler herkese açıktır ve herhangi bir kısıtlama olmaksızın kullanılabilir. International Space Station API, Public API'nin bir örneğidir. Bu API'ler herkese açık olduğundan, Google Haritalar gibi birçok API sağlayıcısı, API'yi kullanmadan önce kullanıcının ücretsiz bir anahtar veya jeton almasını ister. Bu, aldıkları ve işledikleri API isteklerinin sayısını kontrol etmeye yardımcı olmak içindir. Genel API'lerin bir listesini internette arayın.
- Dahili veya Özel API'ler - Bunlar, bir kuruluş veya şirket tarafından yalnızca dahili kullanım için verilere ve hizmetlere erişmek için kullanılan API'lerdir. Dahili API'ye bir örnek, yetkili satış görevlilerinin mobil cihazlarındaki dahili satış verilerine erişmesine izin vermektir.
- İş Ortağı API'leri - Bunlar, bir şirket ile iş ortakları veya yüklenicileri arasında aralarındaki işi kolaylaştırmak için kullanılan API'lerdir. Muhatap, API'yi kullanmak için bir lisansa veya başka bir izne sahip olmalıdır. Bir havayolunun API'sini kullanan bir seyahat hizmeti, iş ortağı API'sine bir örnektir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 43.3.4.Web Hizmeti API Türleri

Web hizmeti, İnternet üzerinden World Wide Web kullanılarak sunulan bir hizmettir. Dört tür web hizmeti API'si vardır:

- Basit Nesne Erişim Protokolü- Simple Object Access Protocol(SOAP)
- Temsili Durum Transferi-Representational State Transfer (REST)
- Genişletilebilir İşaretleme Dili-Uzaktan Prosedür Çağrısı-eXtensible Markup Language-Remote Procedure Call (XML-RPC)
- JavaScript Nesne Gösterimi-Uzaktan Prosedür Çağrısı-JavaScript Object Notation-Remote Procedure Call (JSON-RPC)

| Karakteristik | SOAP | REST | XML-RPC | JSON-RPC |
|---|---|---|---|---|
| Veri formatı | XML | JSON, XML, YAML ve diğerleri | XML | JSON |
| İlk yayınlanma | 1998 | 2000 | 1998 | 2005 |
| Güç | Köklü | Esnek biçimlendirme ve en yaygın olarak kullanılan | Köklü, basitlik | Basitlik |

SOAP, XML yapılı bilgi alışverişi için, çoğunlukla HTTP veya Basit Posta Aktarım Protokolü (SMTP) üzerinden bir mesajlaşma protokolüdür. 1998'de Microsoft tarafından tasarlanan SOAP API'leri, ayrıştırmada yavaş, karmaşık ve katı kabul edilir.

Bu, XML gerektirmeyen daha basit bir REST API çerçevesinin geliştirilmesine yol açtı. REST, HTTP kullanır, daha az ayrıntılıdır ve kullanımı SOAP'tan daha kolaydır. REST, yazılım mimarisi tarzını ifade eder ve performansı, ölçeklenebilirliği, basitliği ve güvenilirliği nedeniyle popüler hale gelmiştir.

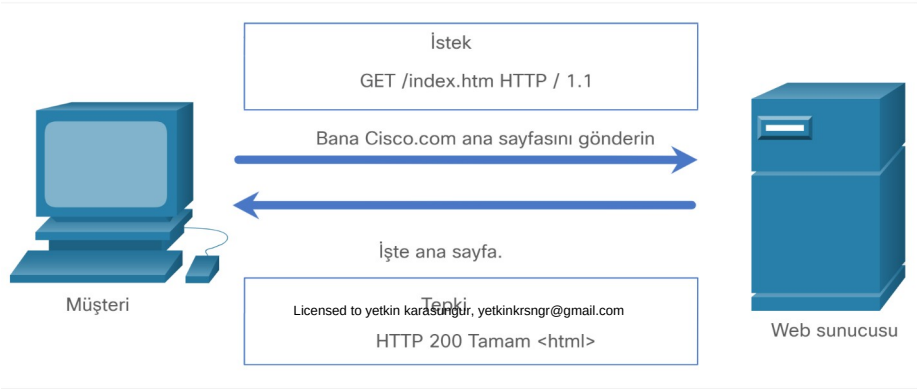
REST, en yaygın kullanılan web hizmeti API'sidir ve kullanılan tüm API türlerinin% 80'inden fazlasını oluşturur. REST, bu modülde daha ayrıntılı olarak ele alınacaktır.

RPC, bir sistemin başka bir sistemin bazı kodları yürütmesini istemesi ve bilgileri döndürmesidir. Bu, ağın ayrıntılarını anlamak zorunda kalmadan yapılır. Bu, REST API'ye çok benzer şekilde çalışır, ancak biçimlendirme ve esneklikle ilgili farklılıklar vardır. XML-RPC, SOAP'tan önce geliştirilen ve daha sonra SOAP haline gelen bir protokoldür. JSON-RPC çok basit bir protokoldür ve XML-RPC'ye benzer.

## 43.4.REST

### 43.4.1.REST ve RESTful API

Web tarayıcıları, bir web sayfası istemek (GET) için HTTP veya HTTPS kullanır. Başarılı bir şekilde istenirse (HTTP durum kodu 200), web sunucuları GET isteklerine şekilde gösterildiği gibi HTML kodlu bir web sayfası ile yanıt verir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

REST, web servis uygulamalarını tasarlamak için bir mimari stildir. Birçok temel özelliğe sahip olan ve istemcilerin ve sunucuların davranışını yöneten bir web mimarisi tarzını ifade eder. Basitçe ifade etmek gerekirse, bir REST API, HTTP protokolünün üzerinde çalışan bir API'dir. Geliştiricilerin istekleri gerçekleştirmek ve GET ve POST gibi HTTP protokolü aracılığıyla yanıt almak için kullanabilecekleri bir dizi işlevi tanımlar.

REST mimarisinin kısıtlamalarına uygunluk genellikle "RESTful" olarak adlandırılır. Bir API, aşağıdaki özelliklere sahipse "RESTful" olarak kabul edilebilir:

- İstemci-Sunucu - İstemci ön ucu ve sunucu arka ucu yönetir. İkisi de birbirinden bağımsız olarak değiştirilebilir.
- Durumsuz - İstekler arasında sunucuda hiçbir istemci verisi depolanmaz. Oturum durumu istemcide saklanır.
- Önbelleğe alınabilir - İstemciler performansı artırmak için yanıtları önbelleğe alabilir.

## 43.4.2.RESTful Uygulama

RESTful web hizmeti HTTP kullanılarak uygulanır. Dört tanımlanmış yönü olan bir kaynaklar koleksiyonudur:

- Web hizmeti için temel Tekdüzen Kaynak Tanımlayıcısı (URI), örneğin http://example.com/resources
- Web servisi tarafından desteklenen veri formatı. Bu genellikle JSON, YAML veya XML'dir, ancak geçerli bir köprü metni standardı olan herhangi bir başka veri biçimi de olabilir.
- HTTP yöntemlerini kullanan web hizmeti tarafından desteklenen işlemler kümesi.
- API, hiper metne dayalı olmalıdır.

RESTful API'ler, POST, GET, PUT, PATCH ve DELETE gibi yaygın HTTP yöntemlerini kullanır. Aşağıdaki tabloda gösterildiği gibi, bunlar RESTful işlemlerine karşılık gelir: Oluşturma, Okuma, Güncelleme ve Silme- Create, Read, Update, and Delete(veya kısaca CRUD).

| HTTP Method | RESTful Operation |
|---|---|
| POST | Create |
| GET | Read |
| PUT/PATCH | Update |
| DELETE | Delete |

Şekilde, HTTP isteği JSON biçimli verileri ister. İstek API belgelerine göre başarıyla oluşturulmuşsa, sunucu JSON verileriyle yanıt verecektir. Bu JSON verileri, verileri görüntülemek için bir müşterinin web uygulaması tarafından kullanılabilir. Örneğin, bir akıllı telefon haritalama uygulaması San Jose, California'nın konumunu gösterir.


```
{
  - route: {
        hasTollRoad: false,
        hasBridge: true,
      - boundingBox: {
          - lr: {
                lng: -121.667061,
                lat: 36.596809
            },
          - ul: {
                lng: -121.897125,
                lat: 37.335358
            }
        },
        distance: 71.712,
        hasTimedRestriction: false,
        hasTunnel: false,
        hasHighway: true,
        computedWaypoints: [ ],
      - routeError: {
            errorCode: -400,
            message: ""
        },
        formattedTime: "01:12:59",
        sessionId: "5ce1ebf7-017f-5f21-02b4-1a7b-06b08100f026",
        hasAccessRestriction: false,
        realTime: 4378,
        hasSeasonalClosure: false,
        hasCountryCross: false,
        fuelUsed: 3.29,
      - legs: [
          - {
                hasTollRoad: false,
                hasBridge: true,
                destNarrative: "Proceed to MONTEREY, CA.",
                distance: 71.712,
```

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### 43.4.3.URI, URN ve URL

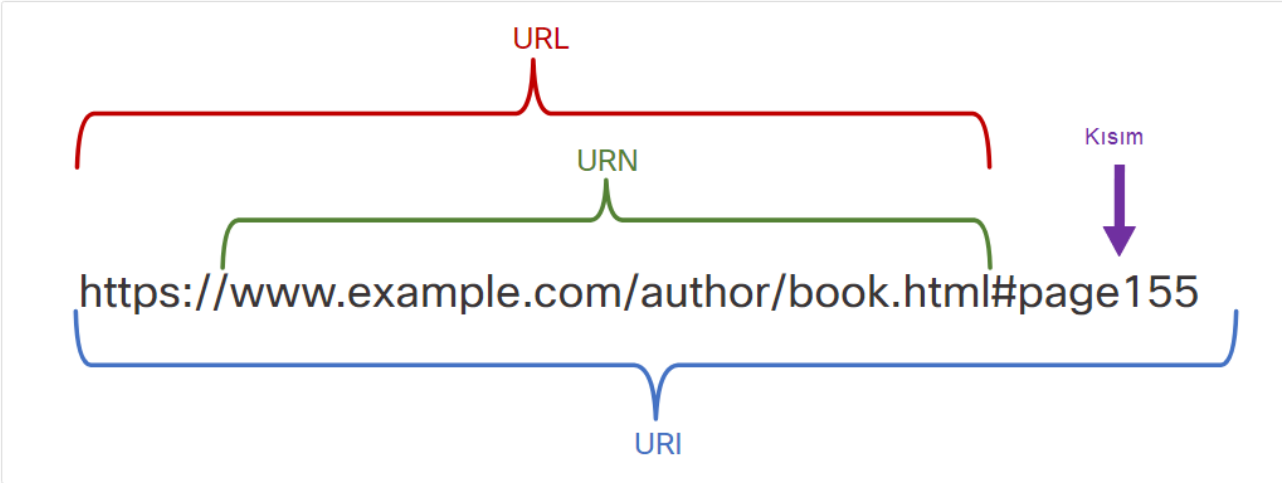
RESTful API'ler gibi web kaynakları ve web hizmetleri bir URI kullanılarak tanımlanır. URI, belirli bir ağ kaynağını tanımlayan bir karakter dizisidir. Şekilde gösterildiği gibi, bir URI'nin iki özelliği vardır:

- Tekdüzen Kaynak Adı-Uniform Resource Name (URN) - protokole başvurmadan yalnızca kaynağın ad alanını (web sayfası, belge, resim, vb.) tanımlar.
- Tekdüzen Kaynak Konum Belirleyicisi-Uniform Resource Locator (URL) - ağdaki belirli bir kaynağın ağ konumunu tanımlar. HTTP veya HTTPS URL'leri genellikle web tarayıcıları ile kullanılır. FTP, SFTP, SSH ve diğerleri gibi diğer protokoller bir URL kullanabilir. SFTP kullanan bir URL şöyle görünebilir: sftp: //sftp.example.com.

Şekilde gösterildiği gibi, bunlar bir URI'nin parçalarıdır:

- Protokol / şema - HTTPS veya FTP, SFTP, mailto ve NNTP gibi diğer protokoller
- Ana bilgisayar adı -
- www.example.com
- Yol ve dosya adı - /author/book.html
- Kısım - # page155

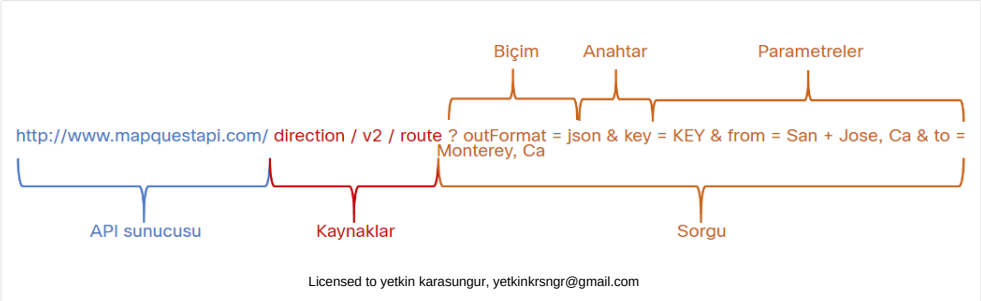
Bir URI'nin bölümleri




### 43.4.4.RESTful Bir İsteğin Anatomisi

Bir RESTful Web hizmetinde, bir kaynağın URI'sine yapılan bir istek bir yanıt ortaya çıkaracaktır. Yanıt, genellikle JSON biçiminde biçimlendirilmiş bir yük olacaktır, ancak HTML, XML veya başka bir biçim de olabilir. Şekil, MapQuest yönler API'sinin URI'sini gösterir. API isteği, San Jose, California'dan Monterey, California'ya yol tarifi içindir.

API İsteğinin Bölümleri




Şekil, API yanıtının bir bölümünü göstermektedir. Bu örnekte, JSON formatında San Jose'den Monterey'e MapQuest yönleridir.

API isteğinin farklı bölümleri şunlardır:

- API Sunucusu - Bu, REST isteklerini yanıtlayan sunucunun URL'sidir. Bu örnekte, MapQuest API sunucusudur.
- Kaynaklar - İstenen API'yi belirtir. Bu örnekte, MapQuest yönler API'sidir.
- Sorgu - İstemcinin API hizmetinden istediği veri biçimini ve bilgileri belirtir. Sorgular şunları içerebilir:
- Biçim - Bu genellikle JSON'dur ancak YAML veya XML olabilir. Bu örnekte JSON istenmektedir.
- Anahtar - Gerekirse anahtar yetkilendirme içindir. MapQuest, yol tarifleri API'si için bir anahtar gerektirir. Yukarıdaki URI'de, geçerli bir istek göndermek için "KEY" i geçerli bir anahtarla değiştirmeniz gerekir.
- Parametreler - Parametreler, isteğe ilişkin bilgileri göndermek için kullanılır. Bu örnekte, sorgu parametreleri, API'nin ihtiyaç duyduğu yönler hakkında bilgi içerir, böylece hangi yönlerin döneceğini bilir: "from = San + Jose, Ca" ve "to = Monterey, Ca".

Genel API'ler dahil birçok RESTful API, bir anahtar gerektirir. Anahtar, talebin kaynağını belirlemek için kullanılır. Bir API sağlayıcısının bir anahtara ihtiyaç duymasının bazı nedenleri şunlardır:

- API'yi kullanma yetkisine sahip olduklarından emin olmak için kaynağın kimliğini doğrulamak için.
- API kullanan kişi sayısını sınırlandırmak için.
- Kullanıcı başına istek sayısını sınırlamak için.
- Kullanıcılar tarafından talep edilen verileri daha iyi yakalamak ve izlemek için.
- API kullanan kişiler hakkında bilgi toplamak.

Not : MapQuest API'yi kullanmak isterseniz, API bir anahtar gerektirir. Bir MapQuest anahtarı almak için URL'yi internette arayın. Arama parametrelerini kullanın: developer.mapquest. Ayrıca, MapQuest gizlilik politikasını özetleyen mevcut URL'yi internette de arayabilirsiniz.

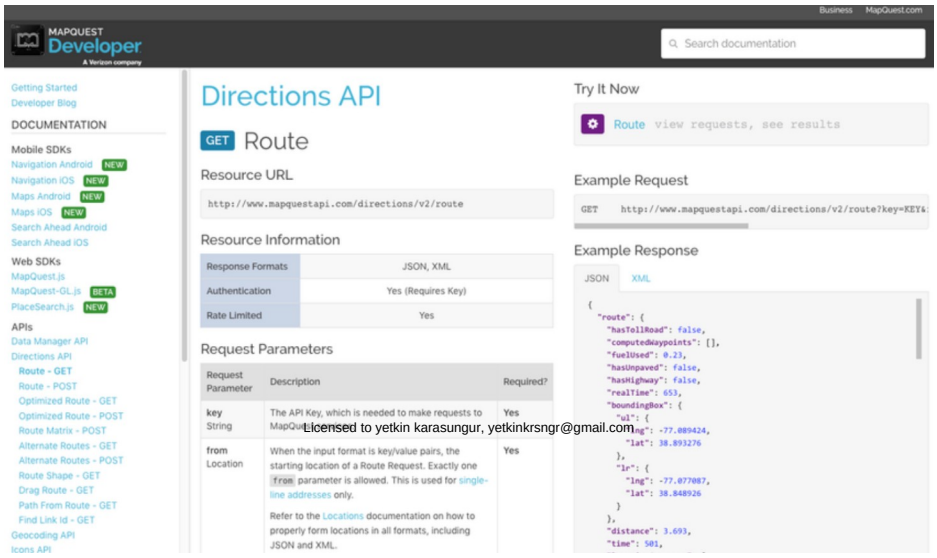
## 43.4.5.RESTful API Uygulamaları

Birçok web sitesi ve uygulama, bilgilere erişmek ve müşterilerine hizmet sunmak için API'leri kullanır. Örneğin, bir seyahat hizmeti web sitesini kullanırken, seyahat hizmeti, kullanıcıya havayolu, otel ve diğer bilgileri sağlamak için çeşitli havayollarının API'sini kullanır.

Bazı RESTful API talepleri, bir web tarayıcısı içinden URI yazılarak yapılabilir. MapQuest yönler API'si buna bir örnektir. RESTful API talebi başka şekillerde de yapılabilir.

### Geliştirici Web Sitesi

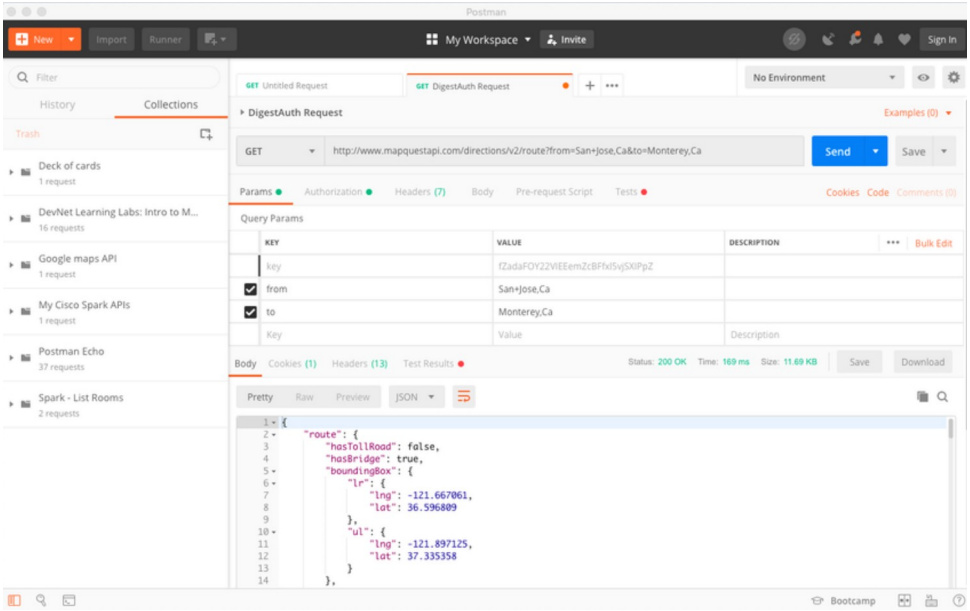
Geliştiriciler genellikle API ile ilgili bilgiler, parametre bilgileri ve kullanım örnekleri içeren web siteleri bulundururlar. Bu siteler, kullanıcının parametreleri ve diğer bilgileri girerek geliştirici web sayfası içinde API talebini gerçekleştirmesine de izin verebilir. Aşağıdaki şekil, MapQuest Directions API web sayfasının bir örneğini gösterir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## Postman

Postman, REST API'lerini test etmek ve kullanmak için bir uygulamadır. Bir tarayıcı uygulaması veya bağımsız bir kurulum olarak mevcuttur. Sorgu parametrelerinin ve anahtarlarının girilmesi dahil REST API isteklerini oluşturmak ve göndermek için gereken her şeyi içerir. Postman, sık kullanılan API çağrılarını geçmişte veya koleksiyonlar olarak toplamanıza ve kaydetmenize olanak tanır. Postman, API taleplerinin nasıl oluşturulacağını öğrenmek ve bir API'den döndürülen verileri analiz etmek için mükemmel bir araçtır. Aşağıdaki şekil, MapQuest API'sini Postman ile kullanma örneğini gösterir.




## Python

API'ler ayrıca bir Python programı içinden çağrılabilir. Bu, API'nin olası otomasyonuna, özelleştirmesine ve Uygulama entegrasyonuna izin verir. Aşağıdaki şekil, istekleri MapQuest API'ye göndermek için kullanılan bir Python programının bir parçası örneğini göstermektedir.

```
#Replace "your_api_key" with your MapQuest API key

import urllib.parse
import requests

main_api = "https://www.mapquestapi.com/directions/v2/route?"
key = "your_api_key"

while True:
    orig = input("Starting Location: ")
    if orig == "quit" or orig == "q":
        break

    dest = input("Destination: ")
    if dest == "quit" or dest == "q":
        break

    url = main_api + urllib.parse.urlencode({"key": key, "from":orig, "to":
    dest})
    print("URL: " + (url))

    json_data = requests.get(url).json()
    json_status = json_data["info"]["statuscode"]

    if json_status == 0:
        print("API Status: " + str(json_status) + " = A successful route
        call.\n")
        print("Directions from " + (orig) + " to " + (dest))
        print("Trip Duration:   " + (json_data["route"]["formattedTime"]))
        print("Kilometers:      " + str("{:.2f}".format((json_data["route"][
        "distance"])*1.61)))
        print("Fuel Used (Ltr): " + str("{:.2f}".format((json_data["route"][
        "fuelUsed"])*3.78)))
```

## Ağ İşletim Sistemleri

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

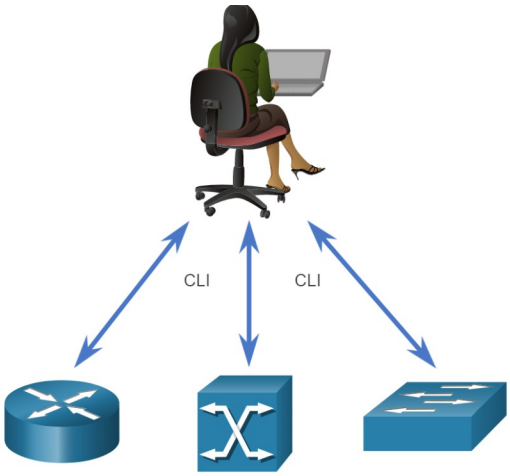
NETCONF (NET CONFiguration) ve RESTCONF gibi protokolleri kullanan ağ işletim sistemleri, yapılandırma, izleme ve yönetim için alternatif bir yöntem sağlamaya başlıyor. Örneğin, aşağıdaki çıktı, kullanıcı komut satırında

bir NETCONF oturumu kurduktan sonra bir yönlendiriciden gelen açılış yanıtı olabilir. Ancak, komut satırında çalışmak ağı otomatikleştirmez. Bunun yerine, bir ağ yöneticisi yönlendiriciyle programlı olarak etkileşimde bulunmak için Python komut dosyalarını veya Cisco DNA Center gibi diğer otomasyon araçlarını kullanabilir.

```
$ ssh admin@192.168.0.1 -p 830 -s netconf
admin@192.168.0.1's password:
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<capabilities>
  <capability>urn:ietf:params:netconf:base:1.1</capability>
  <capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
  <capability>urn:ietf:params:xml:ns:yang:ietf-netconf-monitoring</capability>
  <capability>urn:ietf:params:xml:ns:yang:ietf-interfaces</capability>
  [output omitted and edited for clarity]
</capabilities>
<session-id>19150</session-id></hello>
```

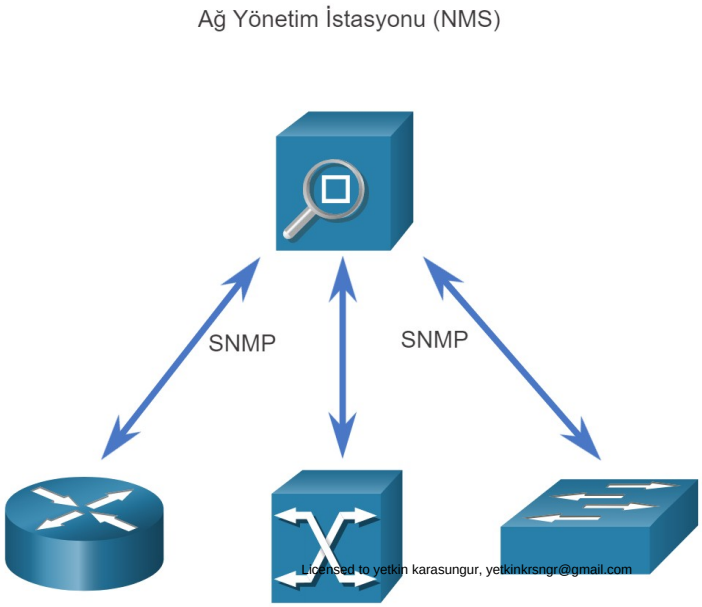
## 43.4.Yapılandırma ve Yönetim Araçları

### 43.4.1.Geleneksel Ağ Yapılandırması




Yönlendirici, anahtarlar ve güvenlik duvarları gibi ağ aygıtları, geleneksel olarak şekilde gösterildiği gibi CLI kullanılarak bir ağ yöneticisi tarafından yapılandırılır. Bir değişiklik veya yeni özellik olduğunda, gerekli yapılandırma komutlarının tüm uygun cihazlara manuel olarak girilmesi gerekir. Çoğu durumda, bu yalnızca zaman alıcı olmakla kalmaz, aynı zamanda hatalara da açık olabilir. Bu, daha büyük ağlarda veya daha karmaşık yapılandırmalarda büyük bir sorun haline gelir.

Basit Ağ Yönetim Protokolü (SNMP), yöneticilerin bir IP ağındaki sunucular, iş istasyonları, yönlendiriciler, anahtarlar ve güvenlik araçları gibi düğümleri yönetmesine olanak sağlamak için geliştirilmiştir. Aşağıdaki şekilde gösterilen bir ağ yönetim istasyonu (NMS) kullanan SNMP, ağ yöneticilerinin ağ performansını izlemesine ve yönetmesine, ağ sorunlarını bulmasına ve çözmesine ve istatistikler için sorgular gerçekleştirmesine olanak tanır. SNMP, cihaz izleme için oldukça iyi çalışır. Bununla birlikte, güvenlik endişeleri ve uygulama güçlüğü nedeniyle tipik olarak konfigürasyon için kullanılmaz. SNMP yaygın olarak bulunmasına rağmen, günümüz ağları için bir otomasyon aracı olarak hizmet edemez.

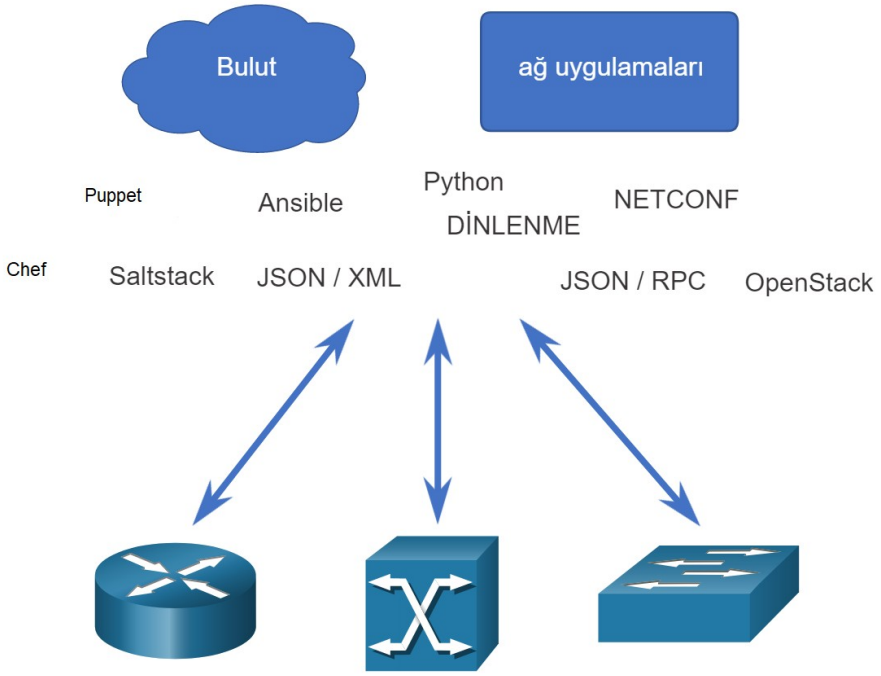



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Ağ kaynaklarının dağıtımını ve yönetimini otomatikleştirmek için API'leri de kullanabilirsiniz. Ağ yöneticisi bağlantı noktalarını, erişim listelerini, hizmet kalitesini (QoS) ve yük dengeleme politikalarını manuel olarak yapılandırmak yerine, yapılandırmaları otomatikleştirmek için araçlar kullanabilir. Bu araçlar, rutin ağ sağlama görevlerini otomatikleştirmek için ağ API'lerine bağlanarak yöneticinin ihtiyaç duyduğu ağ hizmetlerini seçmesine ve dağıtmasına olanak tanır. Bu, ağ yöneticilerinin daha önemli şeyler üzerinde çalışması için zaman kazanmak amacıyla birçok tekrarlayan ve sıradan görevi önemli ölçüde azaltabilir.

### 43.4.2.Ağ Otomasyonu

Bir ağ yöneticisinin birkaç düzine ağ cihazını yönettiği, yüzlerce, binlerce ve hatta on binlerce karmaşık ağ cihazını (hem fiziksel hem de sanal) dağıttığı ve yönettiği bir dünyadan hızla uzaklaşıyoruz. yazılım. Bu dönüşüm, veri merkezindeki başlangıcından ağın tüm yerlerine hızla yayılıyor. Ağ operatörlerinin ağı otomatik olarak izlemesi, yönetmesi ve yapılandırması için yeni ve farklı yöntemler vardır. Şekilde gösterildiği gibi, bunlar REST, Ansible, Puppet, Chef, Python, JSON, XML ve daha fazlası gibi protokolleri ve teknolojileri içerir.




### 43.4.3.Yapılandırma Yönetim Araçları

Yapılandırma yönetimi araçları, görevleri otomatikleştirmek için RESTful API isteklerinden yararlanır ve binlerce cihaz arasında ölçeklenebilir. Yapılandırma yönetimi araçları, tutarlılık için bir sistemin veya ağın özelliklerini korur. Yöneticilerin otomatikleştirmeden yararlandığı ağın bazı özellikleri şunlardır:

- Yazılım ve sürüm kontrolü
- Adlar, adresler ve güvenlik gibi cihaz özellikleri
- Protokol yapılandırmaları
- ACL yapılandırmaları

Yapılandırma yönetimi araçları tipik olarak otomasyon ve orkestrasyonu içerir. Otomasyon, bir aracın bir sistemde otomatik olarak bir görevi gerçekleştirmesidir. Bu, bir arabirimi yapılandırmak veya bir VLAN dağıtmak olabilir. Düzenleme, yapılması gereken sıra, başka bir görev başlamadan önce tamamlanması gerektiği vb. Gibi tüm bu otomatik faaliyetlerin nasıl olması gerektiğine ilişkin süreçtir. Düzenleme, bir koordinatla sonuçlanan otomatik görevlerin düzenlenmesidir. süreç veya iş akışı.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Konfigürasyon yönetimini kolaylaştırmak için birkaç araç mevcuttur:

- Ansible
- Chef
- Puppet
- SaltStack

Tüm bu araçların amacı, yüzlerce, hatta binlerce cihazla büyük ölçekli bir ağ altyapısının yapılandırılması ve sürdürülmesi için gereken karmaşıklığı ve zamanı azaltmaktır. Aynı araçlar daha küçük ağlara da fayda sağlayabilir.

### 43.4.4.Ansible, Chef, Puppet ve SaltStack'i Karşılaştırın

Ansible, Chef, Puppet ve SaltStack, RESTful API isteklerini yapılandırmak için API belgeleriyle birlikte gelir. Hepsi JSON ve YAML ile diğer veri formatlarını destekler. Aşağıdaki tablo Ansible, Puppet, Chef ve SaltStack yapılandırma yönetim araçlarının temel özelliklerinin karşılaştırmasının bir özetini gösterir.

| Karakteristik | Ansible | Chef | Puppet | SaltStack |
|---|---|---|---|---|
| Hangi programlama dili? | Python + YAML | Ruby | Ruby | Python |
| Aracı (agent) tabanlı mı yoksa aracısız mı? | Aracısız | Aracılı | İkisini de destekler | İkisini de destekler |
| Cihazlar nasıl yönetilir? | Herhangi bir cihaz "kontrolör" olabilir | Chef Master | Puppet Master | Salt Master |
| Araç tarafından ne oluşturulur? | Playbook | Cookbook | Manifest | Pillar |

- Hangi programlama dili? - Ansible ve SaltStack Python üzerine inşa edilmiştir, Puppet ve Chef ise Ruby üzerine inşa edilmiştir. Python'a benzer şekilde Ruby, çapraz platform olan açık kaynaklı bir programlama dilidir. Bununla birlikte, Ruby tipik olarak Python'dan öğrenmesi daha zor bir dil olarak kabul edilir.
- Aracı tabanlı mı yoksa aracısız mı? - Yapılandırma yönetimi aracı tabanlı veya aracısızdır. Ajan tabanlı konfigürasyon yönetimi "çekme tabanlıdır", yani yönetilen cihazdaki ajanın, konfigürasyon bilgileri için periyodik olarak ana bilgisayara bağlanması anlamına gelir. Master üzerinde değişiklikler yapılır ve cihaz tarafından aşağı çekilir ve yürütülür. Aracısız yapılandırma yönetimi "push tabanlıdır." Ana birimde bir yapılandırma betiği çalıştırılır. Master, cihaza bağlanır ve komut dizisindeki görevleri yürütür. Tablodaki dört yapılandırma aracından yalnızca Ansible aracısızdır.
- Cihazlar nasıl yönetilir? - Master, Puppet, Chef ve SaltStack Master adlı bir cihazda bulunur. Bununla birlikte, Ansible aracısız olduğundan, herhangi bir bilgisayar denetleyici olabilir.
- Araç tarafından ne oluşturulur? - Ağ yöneticileri, yürütülecek bir dizi talimat oluşturmak için konfigürasyon yönetimi araçlarını kullanır. Her aracın şu talimatlar için kendi adı vardır: Playbook, cookbook, Manifest ve Pilar. Bunların her biri için ortak olan, cihazlara uygulanacak bir ilke veya yapılandırmanın belirtimidir. Her cihaz türünün kendi politikası olabilir. Örneğin, tüm Linux sunucuları aynı temel yapılandırma ve güvenlik politikasına sahip olabilir.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

## 43.5.IBN ve Cisco DNA Merkezi

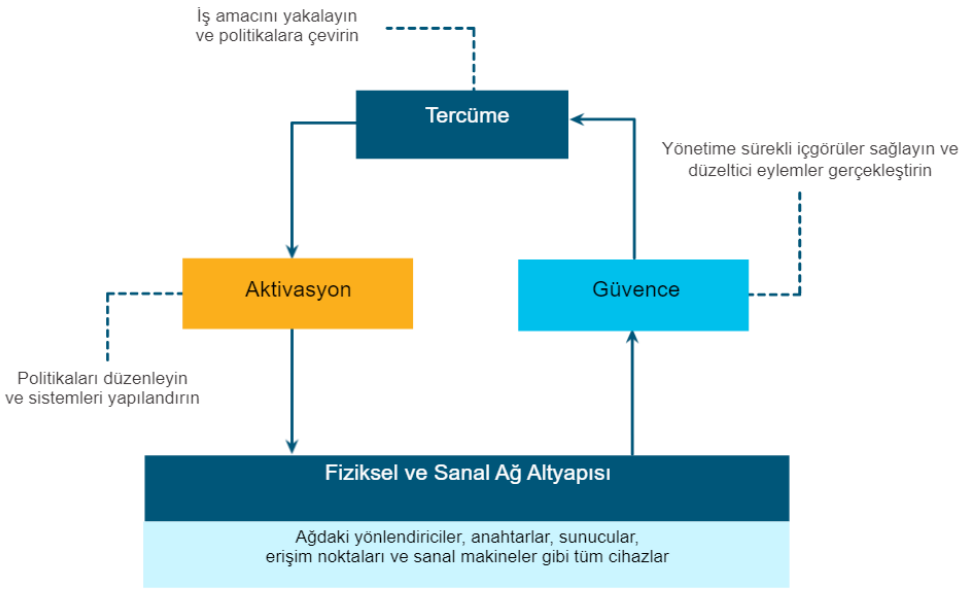
### 43.5.1.Amaca Dayalı Ağa (Intent-Based Networking) Genel Bakış

IBN, yeni nesil ağ iletişimi için gelişmekte olan endüstri modelidir. IBN, Yazılım Tanımlı Ağ Oluşturma (SDN) üzerine kuruludur ve ağları tasarlamak ve çalıştırmak için donanım merkezli ve manuel bir yaklaşımı yazılım merkezli ve tamamen otomatik olana dönüştürür.

Ağ için iş hedefleri, niyet olarak ifade edilir. IBN, işin amacını yakalar ve iş ihtiyaçları değiştikçe ağı sürekli ve dinamik bir şekilde hizalamak için analitik, makine öğrenimi ve otomasyon kullanır.

IBN, iş amacını yakalar ve ağda tutarlı bir şekilde otomatikleştirilebilen ve uygulanabilen ağ politikalarına dönüştürür.

Cisco, IBN'yi üç temel işleve sahip olarak görüyor: çeviri, etkinleştirme ve güvence. Bu işlevler, şekilde gösterildiği gibi altta yatan fiziksel ve sanal altyapı ile etkileşim halindedir.



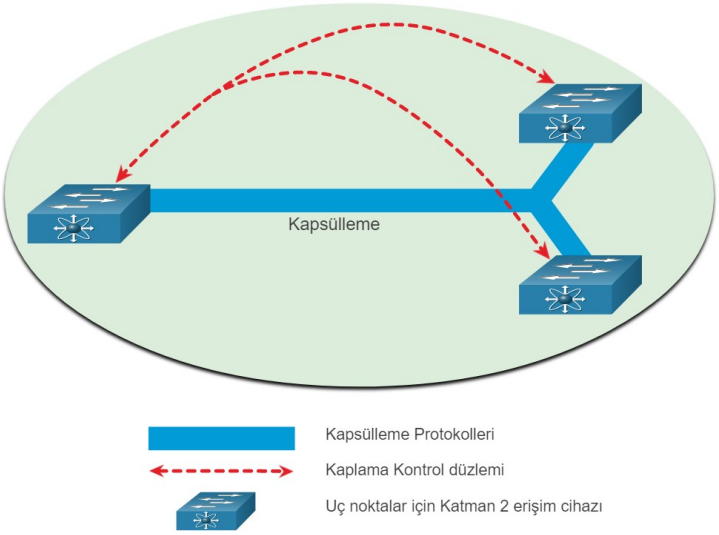

- **Çeviri** - Çeviri işlevi, ağ yöneticisinin iş amacını en iyi şekilde destekleyecek beklenen ağ oluşturma davranışını ifade etmesini sağlar.
- **Etkinleştirme** - Yakalanan amacın daha sonra ağ üzerinde uygulanabilecek ilkeler olarak yorumlanması gerekir. Aktivasyon işlevi, bu ilkeleri ağ çapında otomasyonu kullanarak fiziksel ve sanal ağ altyapısına yükler.
- **Güvence** - **İfade** edilen amacın herhangi bir zamanda ağ tarafından yerine getirildiğini sürekli olarak kontrol etmek için, güvence işlevi sürekli bir doğrulama ve doğrulama döngüsü sürdürür.

### 43.5.2.Yapı Olarak Ağ Altyapısı

IBN açısından fiziksel ve sanal ağ altyapısı bir yapıdır. Yapı, şekilde gösterildiği gibi aygıtlara sanal olarak bağlanmak için kullanılan mantıksal topolojiyi temsil eden bir kaplamayı tanımlamak için kullanılan bir terimdir. Yer paylaşımı, ağ yöneticisinin programlaması gereken cihaz sayısını sınırlar. Ayrıca, temeldeki fiziksel aygıtlar tarafından kontrol edilmeyen hizmetler ve alternatif yönlendirme yöntemleri sağlar. Örneğin, yer paylaşımı IP güvenliği (IPsec) ve Kablosuz Erişim Noktalarının Kontrolü ve Sağlanması (CAPWAP) gibi kapsülleme protokollerinin gerçekleştiği yerdir. Bir IBN çözümü kullanarak, ağ yöneticisi ilkeler aracılığıyla bindirme kontrol düzleminde tam olarak ne olacağını belirleyebilir. Anahtarların fiziksel olarak nasıl bağlandığının kaplamayla ilgili olmadığına dikkat edin.

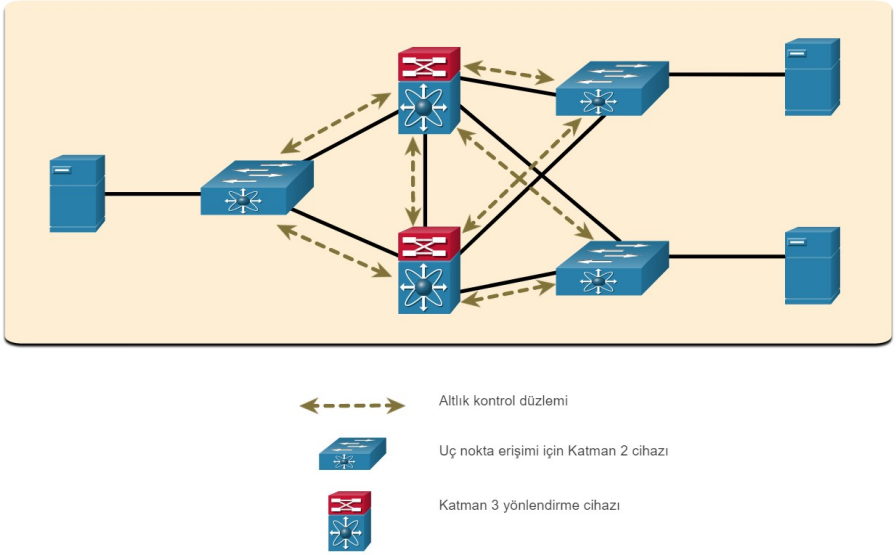
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

### Örnek Yer Paylaşımlı Ağ




Alt katman (underlay) ağı, iş hedeflerini karşılamak için gereken tüm donanımı içeren fiziksel topolojidir. Altlık, ek cihazları ortaya çıkarır ve şekilde gösterildiği gibi bu cihazların nasıl bağlandığını belirtir. Şekildeki sunucular gibi uç noktalar, ağa Katman 2 cihazları aracılığıyla erişir. Döşeme altı kontrol düzlemi, basit yönlendirme görevlerinden sorumludur.

### Örnek Underlay Network




### 43.5.3.Cisco Dijital Ağ Mimarisi (DNA)

Cisco, IBN yapısını Cisco DNA kullanarak uygular. Şekilde gösterildiği gibi, iş amacı ağ altyapısına (yapıya) güvenli bir şekilde yerleştirilir. Cisco DNA, daha sonra zengin bir bilgi bağlamı sağlamak için sürekli olarak çok sayıda kaynaktan (cihazlar ve uygulamalar) veri toplar. Bu bilgiler daha sonra, ağın optimum düzeyde ve iş amacı ve ağ politikalarına uygun olarak güvenli bir şekilde çalıştığından emin olmak için analiz edilebilir.

Cisco DNA, sürekli öğrenen, iş ihtiyaçlarını desteklemek için uyarlanan bir sistemdir. Tablo, bazı Cisco DNA ürünlerini ve çözümlerini listeler.

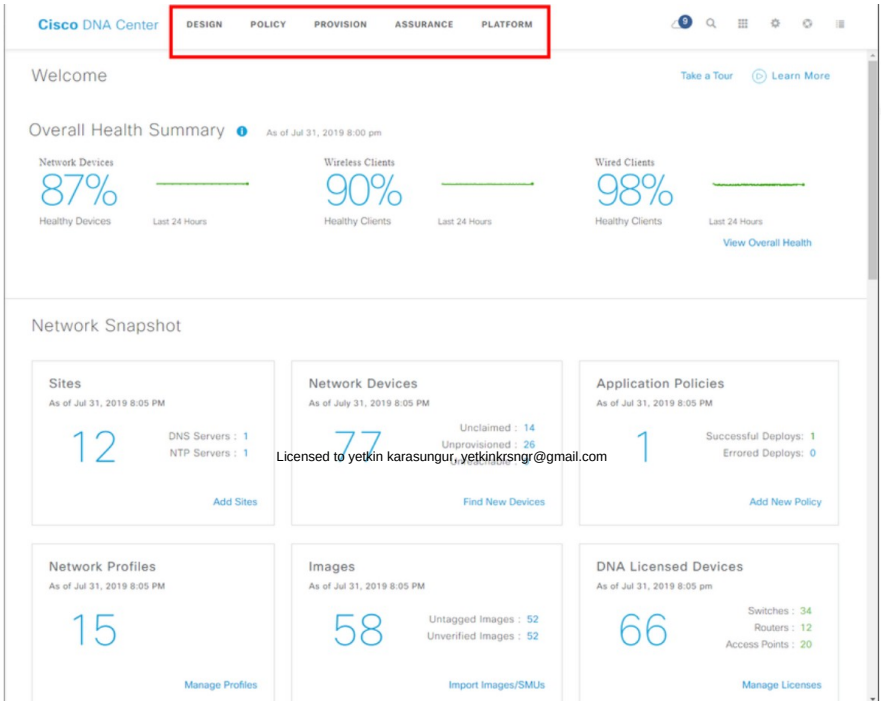
Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

| Cisco DNA Çözümü | Açıklama | Faydaları |
|---|---|---|
| **SD Erişimi** | • Cisco DNA kullanılarak oluşturulmuş ilk amaca dayalı kurumsal ağ çözümü.<br>• Tutarlı, son derece güvenli bir kullanıcı deneyimi oluşturmak için LAN ve WLAN üzerinden tek bir ağ yapısı kullanır.<br>• Kullanıcı, cihaz ve uygulama trafiğini bölümlere ayırır ve bir ağ üzerinden herhangi bir uygulama ile herhangi bir kullanıcı veya cihaz için doğru politikayı oluşturmak üzere kullanıcı erişim politikalarını otomatikleştirir. | Güvenlikten ödün vermeden herhangi bir kullanıcı veya cihaz için herhangi bir uygulamaya dakikalar içinde ağ erişimini sağlar. |
| **SD-WAN** | • WAN bağlantılarını merkezi olarak yönetmek için güvenli bir bulut tabanlı mimari kullanır.<br>• Veri merkezlerini, şubeleri, kampüsleri ve ortak yerleşim tesislerini bağlamak için güvenli, esnek ve zengin WAN hizmetlerinin sunumunu basitleştirir ve hızlandırır. | • Şirket içinde veya bulutta bulunan uygulamalar için daha iyi kullanıcı deneyimleri sunar.<br>• Daha kolay dağıtım ve taşıma bağımsızlığı sayesinde daha fazla çeviklik ve maliyet tasarrufu elde edin. |
| **Cisco DNA Güvencesi** | • BT üretkenliğini gidermek ve artırmak için kullanılır.<br>• Performansı ve sorun çözümünü iyileştirmek için gelişmiş analitik ve makine öğrenimi uygular ve ağ performansını garanti altına almayı öngörür.<br>• Dikkat gerektiren ağ koşulları için gerçek zamanlı bildirim sağlar. | • Temel nedenleri belirlemenize olanak tanır ve daha hızlı sorun giderme için önerilen çözüm sağlar.<br>• Cisco DNA Merkezi, içgörüler ve ayrıntıya inme yetenekleri ile kullanımı kolay tek bir gösterge panosu sağlar.<br>• Makine öğrenimi, sorunları ortaya çıkmadan önce tahmin etmek için ağ zekasını sürekli olarak geliştirir. |
| **Cisco DNA Güvenliği** | • Ağı gerçek zamanlı analiz ve zeka için bir sensör olarak kullanarak görünürlük sağlamak için kullanılır.<br>• Politikayı uygulamak ve ağdaki tehditleri kontrol altına almak için daha fazla granüler kontrol sağlar. | • Riski azaltın ve kuruluşunuzu, şifreli trafikte bile tehditlere karşı koruyun.<br>• Ağ genelinde derin zeka için gerçek zamanlı analitik aracılığıyla 360 derece görünürlük elde edin.<br>• Uçtan uca güvenlik ile daha düşük karmaşıklık. |

## 43.5.4.Cisco DNA Merkezi

Cisco DNA Center, Cisco DNA'nın kalbindeki temel denetleyici ve analiz platformudur. Kurumsal ağda temel otomasyon yetenekleri, yapı sağlama ve ilke tabanlı bölümleme dahil olmak üzere çoklu kullanım durumları için niyet ifadesini destekler. Cisco DNA Center, ağ cihazlarının sağlanması ve yapılandırılması için bir ağ yönetimi ve komuta merkezidir. Güvence, analitik ve otomasyona odaklanan bir 'tek bölme' (tek arabirim) sağlayan bir donanım ve yazılım platformudur.

DNA Merkezi arayüzü başlatma sayfası, şekilde gösterildiği gibi size genel bir sağlık özeti ve ağ anlık görüntüsü verir. Buradan, ağ yöneticisi ilgi alanlarını hızla inceleyebilir.



Licensed to yetkin karasungur, yetkinkrsngr@gmail.com

Üst kısımdaki menüler, DNA Merkezinin beş ana alanına erişim sağlar. Şekilde görüldüğü gibi bunlar

Tasarım - Kampüs, şube, WAN ve bulut genelinde siteler ve binalardan cihazlara ve hem fiziksel hem de sanal bağlantılara kadar tüm ağınızı modelleyin.
İlke - Ağ yönetimini otomatikleştirmek ve basitleştirmek için politikaları kullanın, yeni ve geliştirilmiş hizmetlerin sunumunu hızlandırırken maliyeti ve riski azaltır.
Sağlama - Ağ boyutundan ve karmaşıklığından bağımsız olarak, kurumsal ağınızda kullanıcılara kolay, hızlı ve güvenli yeni hizmetler sağlayın.
Güvence - Sorunları daha hızlı tahmin etmek ve ilke ve yapılandırma değişikliklerinin istediğiniz iş amacına ve kullanıcı deneyimine ulaşmasını sağlamak için ağdan, cihazlardan ve uygulamalardan proaktif izleme ve öngörüler kullanın.
Platform - Uçtan uca çözümler oluşturmak ve çok satıcılı cihazlar için destek eklemek üzere tercih ettiğiniz BT sistemleriyle entegre etmek için API'leri kullanın.

Licensed to yetkin karasungur, yetkinkrsngr@gmail.com