

# Module 1: Günümüzde Ağ Yönetimi

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

**Modül Adı:** Günümüzde Ağ Yönetimi

**Modül Amacı:** Modern teknolojilerdeki gelişmeleri açıklayın.

Konu Başlığı	Konu Hedefi
Ağlar Hayatımızı Etkiliyor	Ağların günlük hayatımıza nasıl etkilediğini açıklayın.
Ağ Bileşenleri	Ana bilgisayar ve ağ aygıtlarının nasıl kullanıldığını açıklayın.
Ağ Gösterimleri ve Topolojiler	Ağ gösterimlerini ve ağ topolojilerinde nasıl kullanıldığını açıklayın.
Network Tipleri	Sık rastlanan ağ türlerinin özelliklerini karşılaştırın.
İnternet Bağlantıları	LAN'ların ve WAN'lerin internete nasıl bağlandığını açıklayın.
Güvenilir Ağlar	Güvenilir bir ağın dört temel gereksinimini açıklayın.
Ağ Trendleri	BYOD, çevrimiçi işbirliği, video ve bulut bilgi işlem gibi eğilimlerin etkileşim şeklimizi nasıl değiştirdiğini açıklayın.
Ağ Güvenliği	Tüm ağlar için bazı temel güvenlik tehditlerini ve çözümlerini belirleyin.
BT Uzmanı	Ağ alanındaki istihdam fırsatlarını açıklayın.

# 1.1 Networkler Hayatımızı Etkiler

## Ağlar Bizi Bağlar

- ❑ İletişim bizim için neredeyse hava, su, yiyecek ve barınak bağımlılığımız kadar önemlidir.
- ❑ Günümüz dünyasında, ağların kullanımı sayesinde, daha önce hiç olmadığı kadar bağlıyız.

# Video – Cisco Networking Academy Öğrenme Deneyimi

**Cisco Networking Academy:** Dünyayı daha iyi bir yer haline getirmek için teknolojiyi nasıl kullandığımızı öğrenin.



## Sınırları Olmayan

- Sınırları olmayan dünya
- Küresel topluluklar
- İnsan ağı



# 1.2 Ağ Bileşenleri

# Host Rolleri

Ağdaki her bilgisayara ana bilgisayar (host) veya son aygıt denir.

Sunucular (server), son aygıtlara bilgi sağlayan bilgisayarlardır:

- e-posta sunucuları
- web sunucuları
- dosya sunucusu

İstemciler (Clients), bilgi almak için sunuculara istek gönderen bilgisayarlardır:

- bir web sunucusundan web sayfası
- bir e-posta sunucusundan e-posta

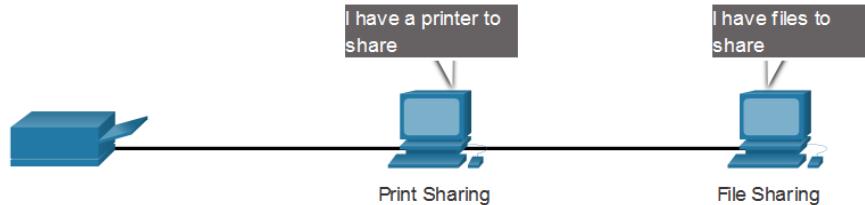


Sunucu Türü	Açıklama
E-posta	E-posta sunucusu e-posta sunucusu yazılımı çalıştırır. Clientlar e-postaya erişmek için istemci yazılımlarını kullanır.
Web	Web sunucusu web sunucusu yazılımı çalıştırır. Clientlar web sayfalarına erişmek için tarayıcı yazılımı kullanır.
File	Dosya sunucusu kurumsal ve kullanıcı dosyalarını depolar. İstemci aygıtları bu dosyalara erişir.

# Peer-to-Peer

**Eşler Arası Ağ'da (Peer to Peer) bir aygıtın istemci (client) ve sunucu (server) olması mümkündür.**

Bu tür ağ tasarıımı yalnızca çok küçük ağlar için önerilir.

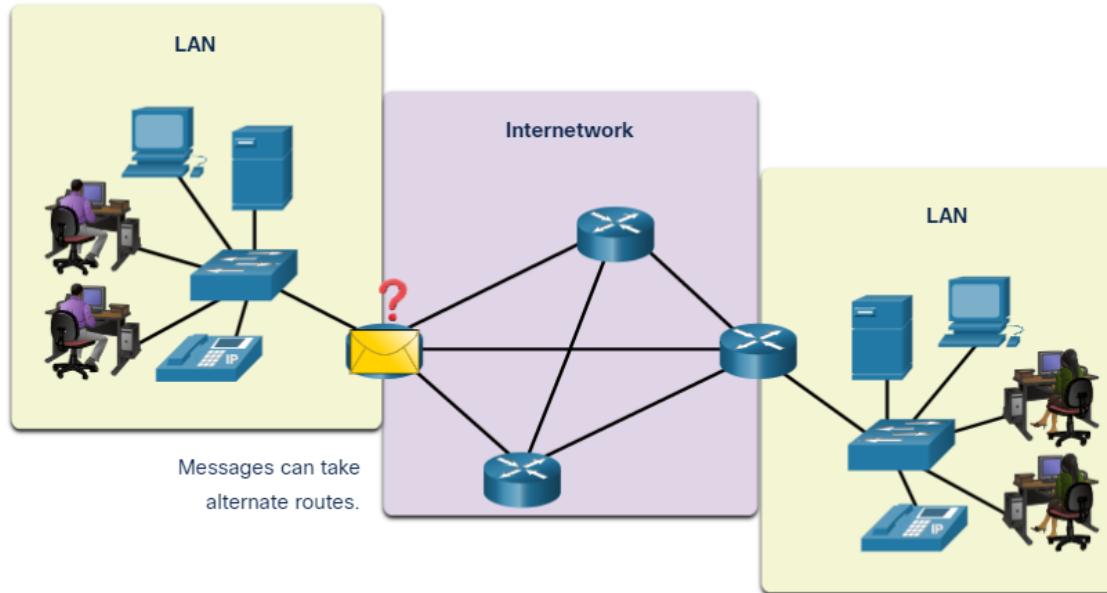


Avantajları	Dezavantajları
Kurulumu kolay	Merkezi yönetim yok
Daha az karmaşık	O kadar güvenli değil
Daha düşük maliyet	Ölçeklenebilir değil
<b>Basit görevler için kullanılır: dosya aktarma ve yazıcı paylaşımı</b>	Daha yavaş performans

# End Devices (Son Aygıtlar)

Son aygıt (end device), iletinin **ilk kaynağı** veya **iletinin ulaştığı** yerdir.

Veriler **bir son aygıtın kaynaklanır** (origin), ağ üzerinden akar ve **bir son aygıta varır**.



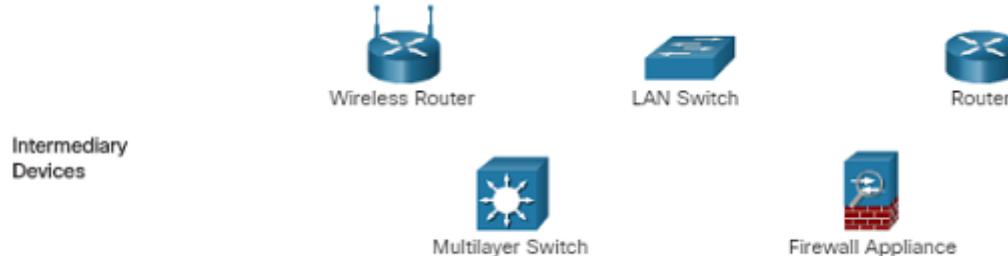
# Aracı Ağ Cihazları (Intermediary Network Device)

**Bir ara aygıt son aygıtları birbirine bağlar.**

Örnekler arasında **anahtarlar** (switch), **kablosuz erişim noktaları** (access point), **yönlendiriciler** (router) ve **güvenlik duvarları** (firewall) sayılabilir.

**Bir ağ üzerinden akarken verilerin yönetimi de aracı aygıtın rolüdür:**

- Data sinyallerini tekrar oluşturmak ve yeniden iletmek.
  - Ağda hangi yolların bulunduğu hakkında bilgiyi tutmak.
  - Diğer aygıtlara hataları ve iletişim hatalarının bildirimi.



# Network Bileşenleri

## Network Media

Ağ üzerinden iletişim, iletinin kaynaktan hedefe geçmesine olanak tanıyan bir ortam aracılığıyla gerçekleştirilir.

Medya Türleri	Açıklama	Copper	Fiber-optic	Wireless
Kablolar içindeki metal kablolar	Elektrik impulslarını kullanır.			
Glass or plastic fibers within cables (fiber-optic cable)	İşik darbeleri (pulses of light) kullanır.			
Kablosuz iletim (Wireless transmission)	Elektromanyetik dalgaların belirli frekanslarının modülasyonu kullanılır.			

# 1.3 Ağ Gösterimleri ve Topolojiler

# Network Representations and Topologies

## Ağ Gösterimleri

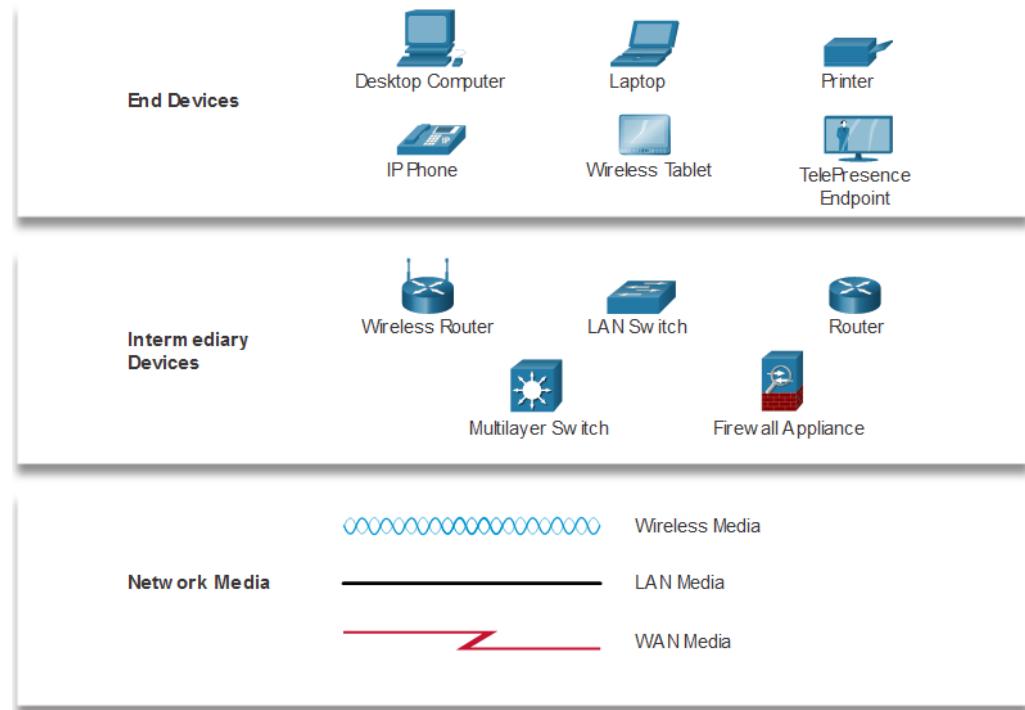
Genellikle topoloji diyagramları olarak adlandırılan ağ diyagramları, **ağ içindeki aygıtları temsil etmek için semboller kullanır.**

**Bilinmesi gereken önemli terimler sunlardır:**

- Network Interface Card – Ağ arabirim kartı (NIC)
- Fiziksel Port
- Interface (Arabirim)

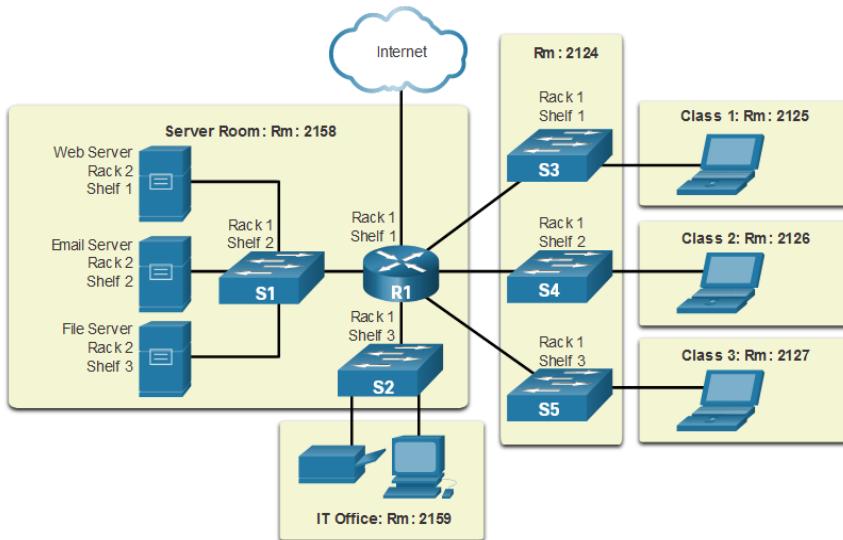
**Not:** Genellikle, bağlantı noktası ve arabirim terimleri birbirinin yerine kullanılır

**cisco**

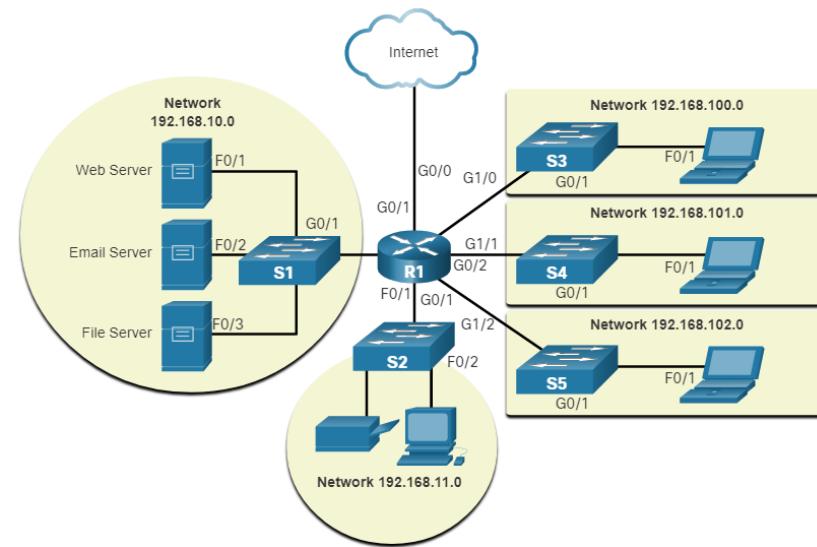


## Topoloji Diyagramları

Fiziksel topoloji diyagramları ara cihazların ve kablo kurulumunun fiziksel konumunu gösterir.



Mantıksal topoloji diyagramları aygıtları, bağlantı noktalarını ve ağın adresleme düzenini gösterir.



# 1.4 Sık Rastlanan Ağ Türleri

# Farklı Ölçeklerdeki Ağlar



Small Home



SOHO



Medium/Large



World Wide

- **Small Home Networks** – birkaç bilgisayarı birbirine ve Internet'e bağlar
- **Small Office/Home Office** – bir ev veya uzak ofis içindeki bilgisayarın bir şirket ağına bağlanması sağlar
- **Medium to Large Networks** – çok sayıda lokasyondaki bağlı yüzlerce, binlerce bilgisayar
- **World Wide Networks** – dünya çapında yüz milyonlarca bilgisayara bağlanır – internet gibi
-

## Common Types of Networks

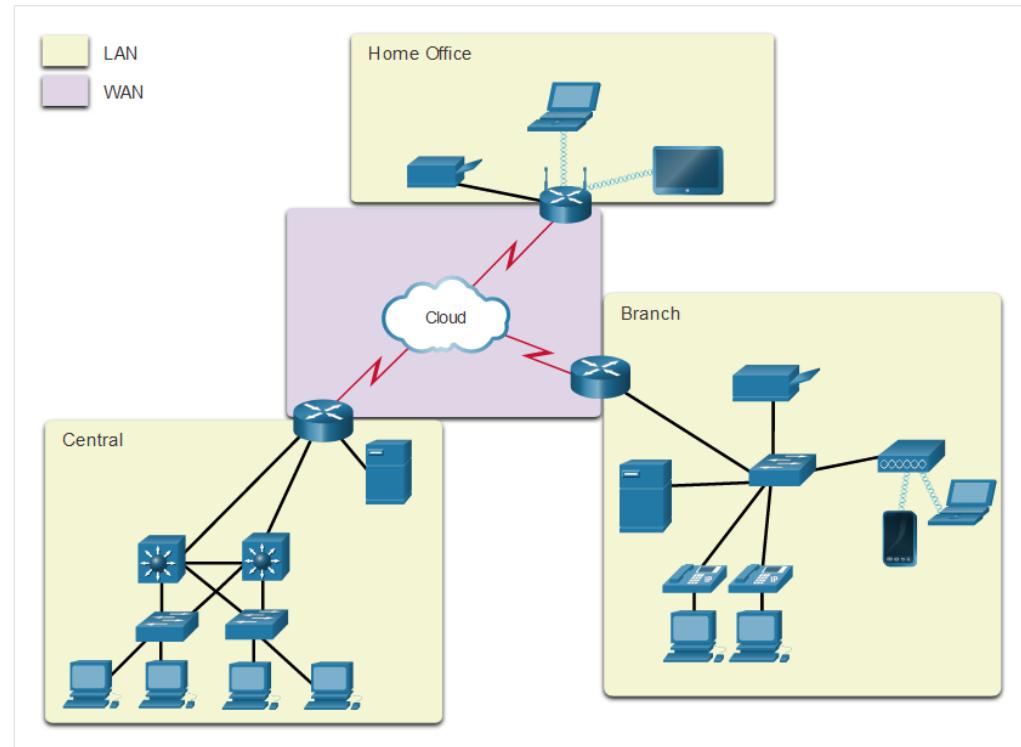
# LAN & WAN'lar

Ağ altyapıları alttaki kategorilerde farklılaşır:

- Kapsanan alanın boyutu
- Bağlı kullanıcı sayısı
- Kullanılabilir hizmet sayısı ve türleri
- Sorumluluk alanı

En yaygın iki ağ türü:

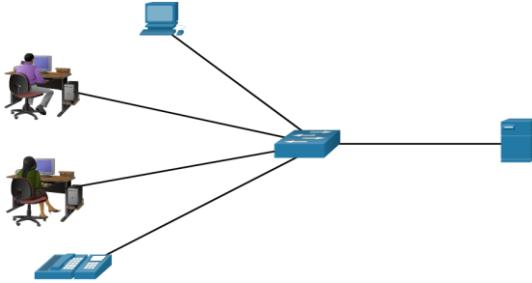
- Local Area Network (LAN)
- Wide Area Network (WAN).



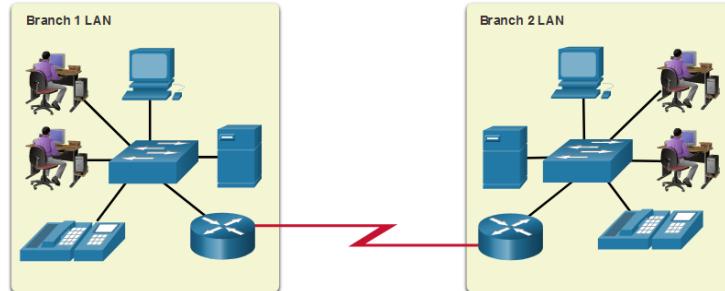
## Common Types of Networks

# LAN & WAN'lar (dvm)

LAN, küçük bir coğrafi alana yayılan bir ağ altyapısıdır.



WAN, geniş bir coğrafi alana yayılan bir ağ altyapısıdır.



LAN	WAN
Sınırlı bir alanda üç aygıtları bağlar.	Geniş coğrafi alanlar üzerinde LAN'leri birbirine bağlar.
Tek bir kuruluş veya birey tarafından yönetilir.	Genellikle bir veya daha fazla hizmet sağlayıcısı tarafından yönetilir.
Dahili aygıtlara yüksek hızlı bant genişliği sağlar.	Genellikle LAN'ler arasında daha yavaş hız bağlantıları sağlar.

## Common Types of Networks

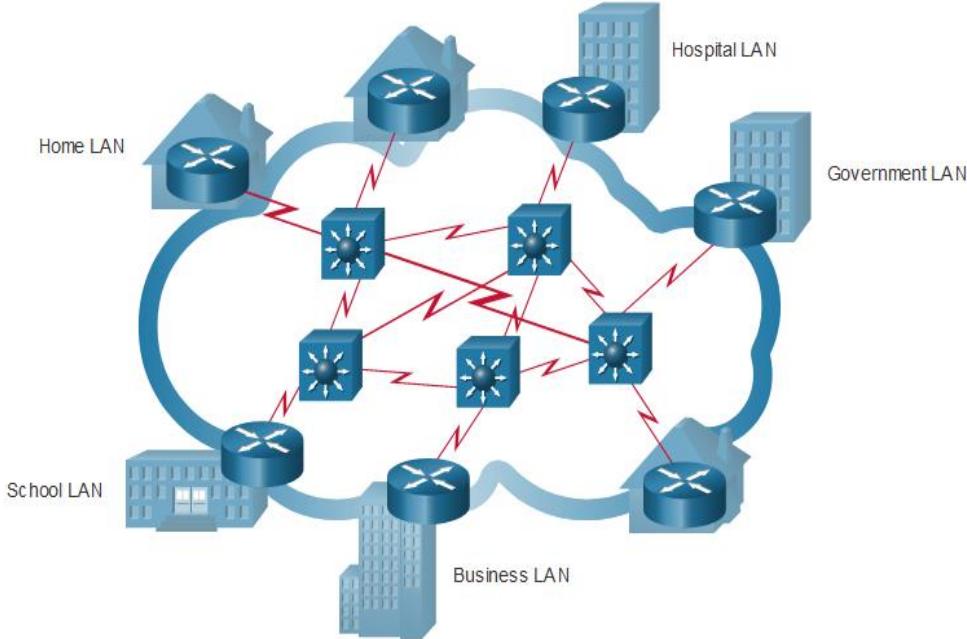
### Internet

Internet, küresel bir LAN ve WAN koleksiyonudur.

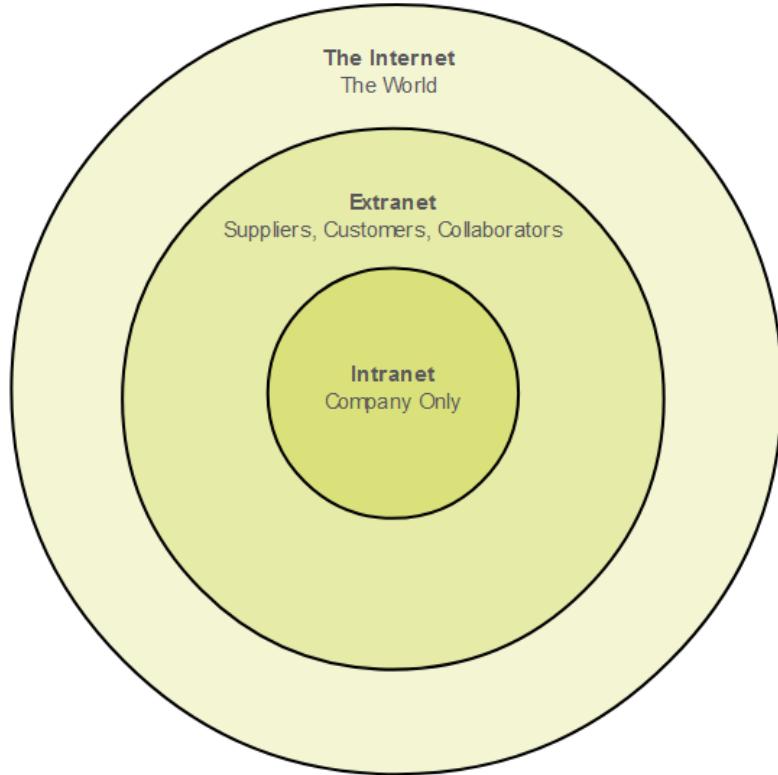
- LAN'ler, WAN'ler kullanılarak birbirine bağlanır.
- WAN'lar **bakır teller, fiber optik kablolar ve kablosuz transmission** kullanabilir.

Internet herhangi bir kişi veya gruba ait değildir. Aşağıdaki gruplar internet üzerindeki yapının korunmasına yardımcı olmak için geliştirilmiştir:

- IETF (Internet Engineering Task Force)
- ICANN (Internet Corporation for Assigned Names and Numbers)
- IAB (Internet Architecture Board)



# Intranet ve Extranet'ler



**Intranet, yalnızca kuruluş üyeleri veya yetkilendirmesi olan diğer kuruluşların üyeleri tarafından erişilebilir olması amaçlanan kuruluşa dahili, LAN'lar ve WAN'lerin özel bir koleksiyonudur.**

**Kuruluş farklı organizasyonlarda çalışan bireylere kendi ağına güvenli erişim sağlamak için extranet kullanabilir.**

# 1.5 Internet Bağlantıları

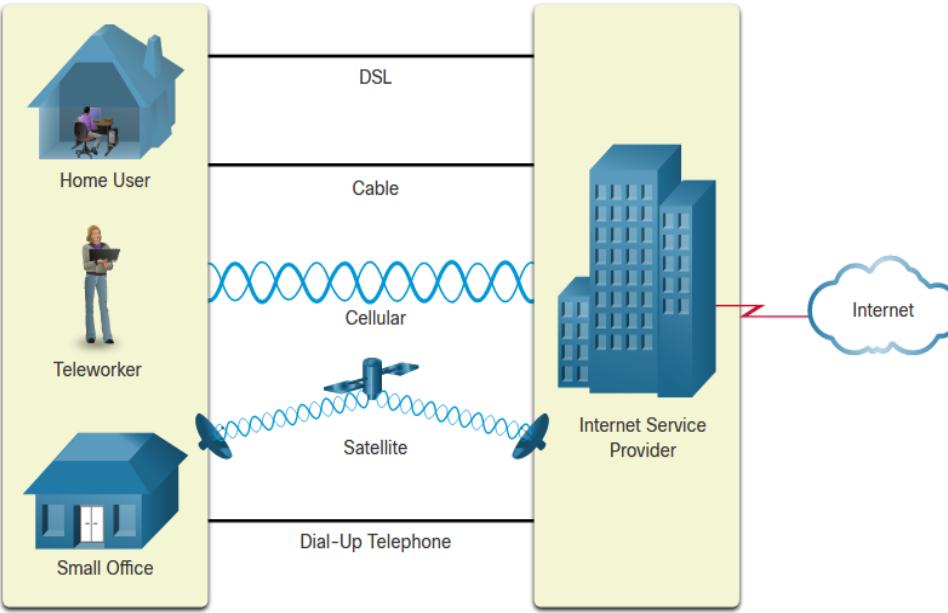
# Internet Erişim Teknolojileri



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 depolamayı desteklemek için daha hızlı bağlantılar**ına İhtiyacı vardır.
- İş sınıfı ara bağlantılar genellikle hizmet sağlayıcılar (SP) tarafından sağlanır ve sunları içerebilir: iş DSL, kiralık hatlar ve Metro Ethernet.

# Ev ve Küçük Ofis Internet Bağlantıları

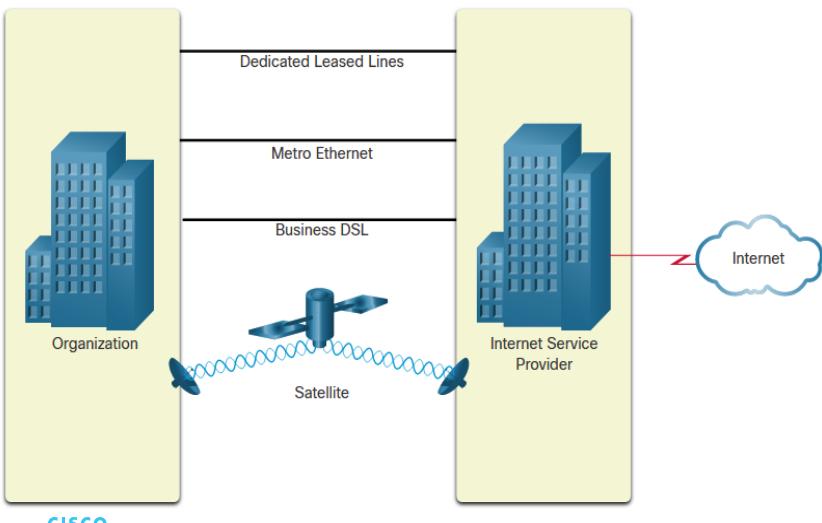


Connection	Description
Kablo	yüksek bant genişliği, her zaman açık, kablolu televizyon servis sağlayıcıları tarafından sunulan internet hizmetidir.
DSL	yüksek bant genişliği, her zaman açık, telefon hattı üzerinden çalışan internet bağlantısı sunar
Hücresel	internete bağlanmak için bir cep telefonu ağı kullanır.
Uydu	İnternet Servis Sağlayıcıları olmayan kırsal alanlara büyük fayda sağlar
Çevirmeli bağlantı	modem kullanan ucuz, düşük bant genişliği seçeneği sunar.

# Kurumsal İnternet Bağlantısı

Kurumsal iş bağlantıları gerektirebilir:

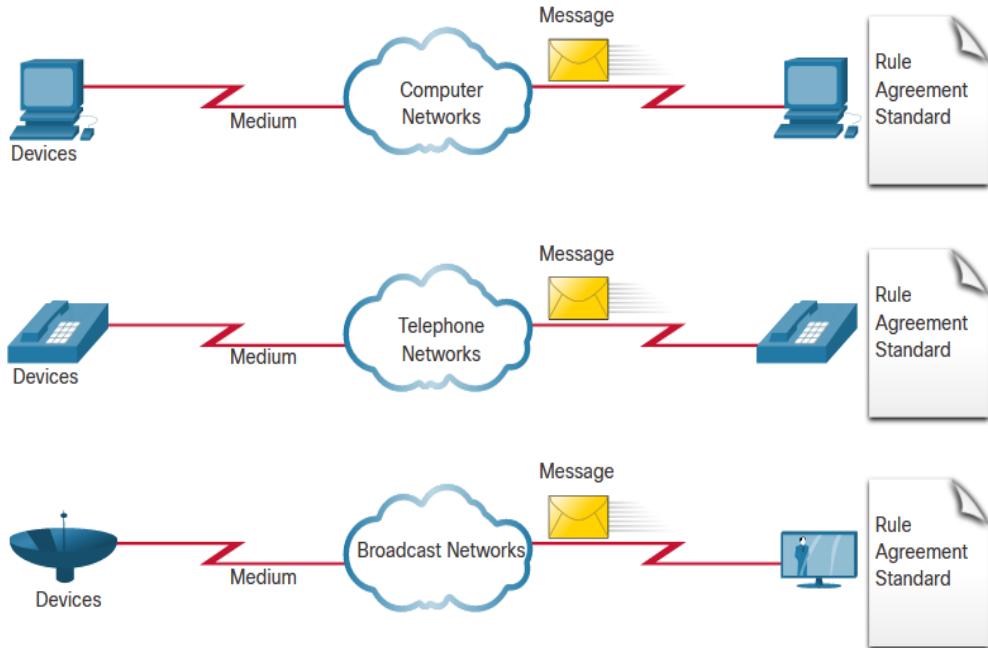
- daha yüksek bant genişliği
- özel bağlantılar
- yönetilen hizmetler



Bağlantı Türü	Açıklama
Özel Kiralık Hat	Bunlar, hizmet sağlayıcının ağındaki uzak ofisleri özel ses ve/veya veri ağıyla birbirine bağlayan ayrılmış devrelerdir.
Ethernet WAN	LAN erişim teknolojisini WAN'a genişletir.
DSL	İş DSL'si, Simetrik Dijital Abone Hatları (SDSL) dahil olmak üzere çeşitli formatlarda mevcuttur.
Uydu	Bu, kablolu bir çözüm olmadığından bağlantı sağlayabilir.

# Birleştirilmiş/yakınsanmış Ağ (The Converging Network)

- ❖ Yakınsanmış ağlardan önce, bir kuruluş **telefon**, **video** ve **veri** için ayrı ayrı kablolarırdı.
- ❖ **Bu ağların her biri, sinyali taşımak için farklı teknolojiler kullanır.**
- ❖ **Bu teknolojilerin her biri farklı bir dizi kural ve standart kullanır.**

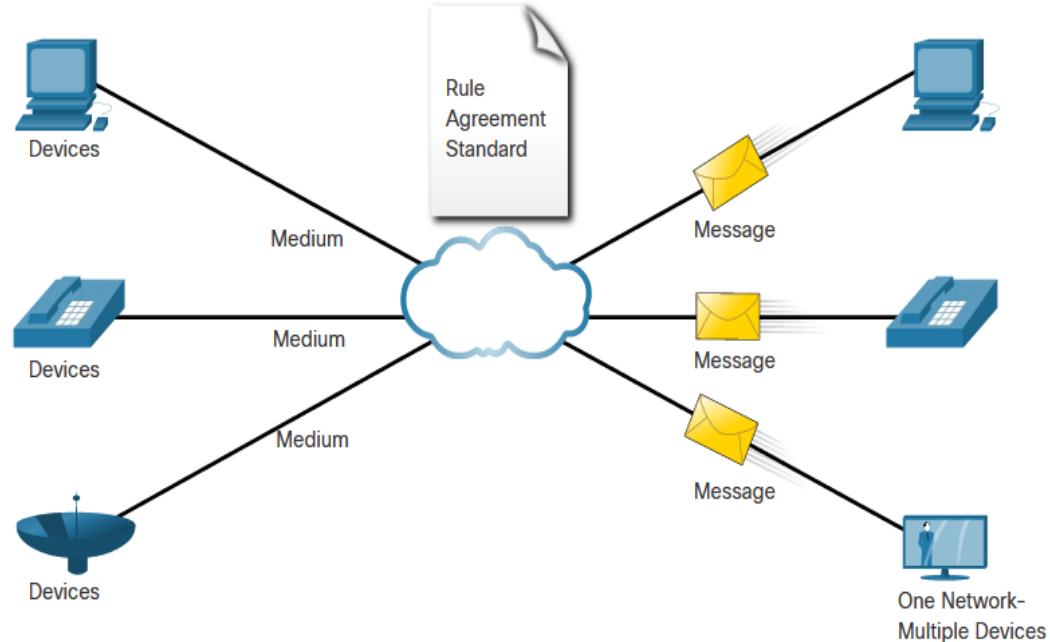


# Birleştirilmiş/yakınsanmış Ağ (The Converging Network)

Birleştirilmiş veri ağları, aşağıdakiler de dahil olmak üzere **tek bir bağlantı üzerinde birden fazla hizmet taşır**:

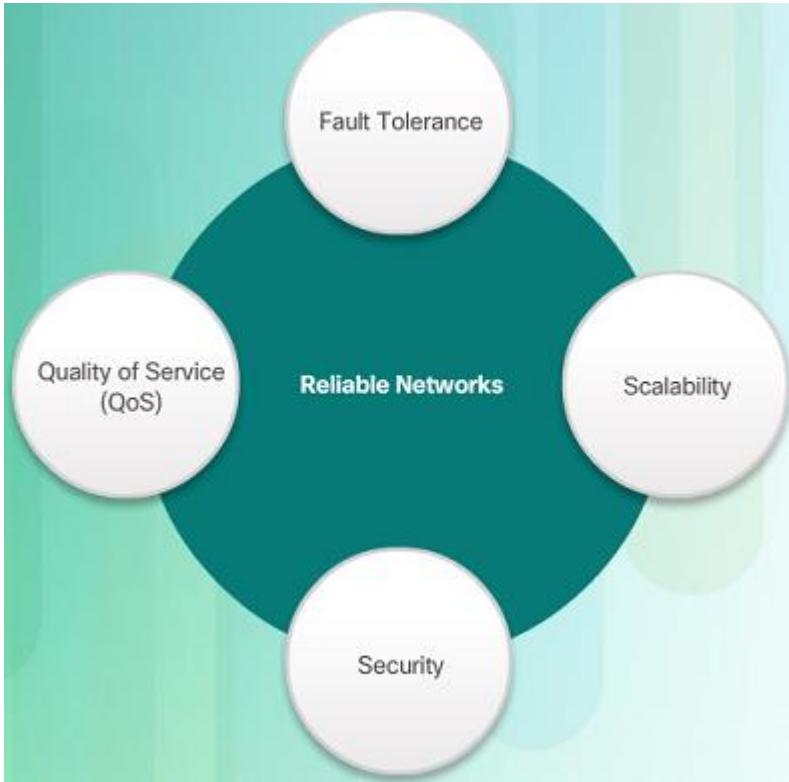
- veri
- Ses
- video

**Ağ altyapısı aynı kural ve standartları kullanır.**



# 1.6 Güvenilir Ağlar

# Reliable Network Ağ Mimarisi



Ağ Mimarisi (Network Architecture), verileri ağ üzerinde hareket ettiren altyapıyı (infrastructure) destekleyen teknolojileri ifade eder.

Temel mimarilerin kullanıcı bekłentilerini karşılamak için ele alması gereken dört temel özellik vardır:

- **Fault Tolerance (hataya dayanıklı)**
- **Scalability (ölçeklenebilir)**
- **Quality of Service (QoS) (hizmet kalitesi)**
- **Security (Güvenlik)**

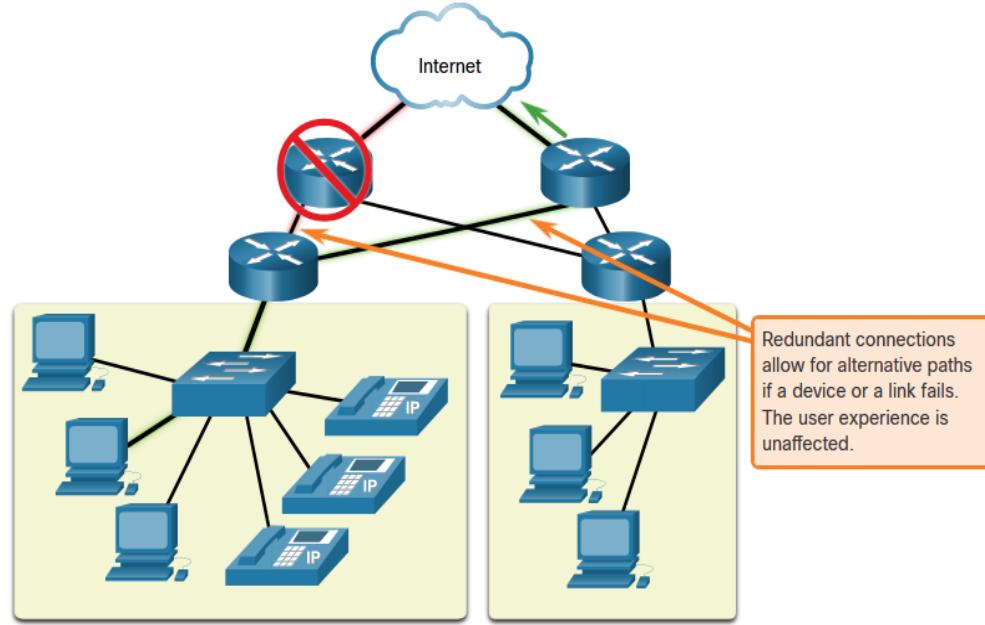
## Hata Toleransı

**Hataya dayanıklı ağ, etkilenen aygitların sayısını sınırlayarak bir hatanın etkisini sınırlar. Hata toleransı için birden çok yol gereklidir.**

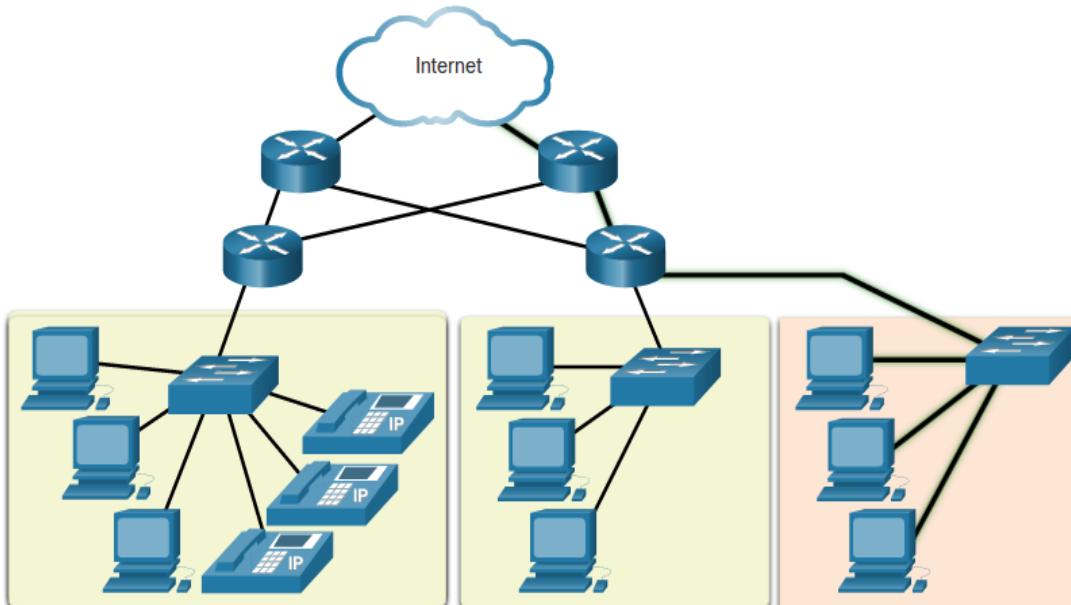
Güvenilir ağlar (reliable network), **paket anahtarlı (packet switched network)** ağ uygulayarak redundancy sağlar:

- Paket anahtarlama, **trafiği ağ üzerinden yönlendirilen paketlere böler.**
- Her paket teorik olarak **hedefe farklı bir yol alabilir.**

Dedike devreler kurulan devre anahtarlı (circuit-switched network) şebekeler ile bu mümkün değildir.



# Scalability (Ölçeklenebilirlik)



Additional users and whole networks can be connected to the Internet without degrading performance for existing users.

Ölçeklenebilir ağ, mevcut kullanıcılarla **hizmet performansını etkilemeden** yeni kullanıcıları ve uygulamaları desteklemek için **hızlı ve kolay** bir şekilde genişletilebilir.

Ağ tasarımcıları, ağları ölçeklenebilir hale getirmek için **kabul edilen standartları** ve **protokollerini** izler.

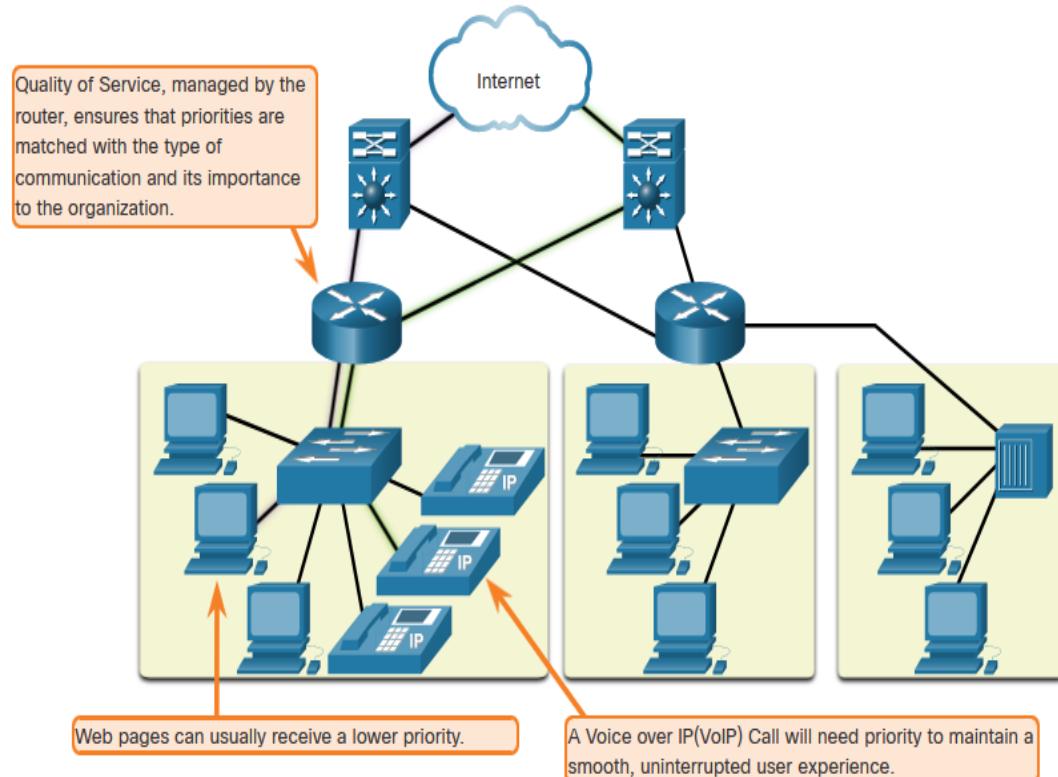
# Quality of Service (Hizmet kalitesi)

Ses ve canlı video iletimleri (transmissions), teslim edilen hizmetler için daha yüksek bekłentiler gerektir.

**Hiç sürekli molalar ve duraklamalar ile canlı bir video izledim mi? Bu, bant genişliği için mevcut olandan daha yüksek bir talep olduğunda ve QoS yapılandırılmamışsa olur.**

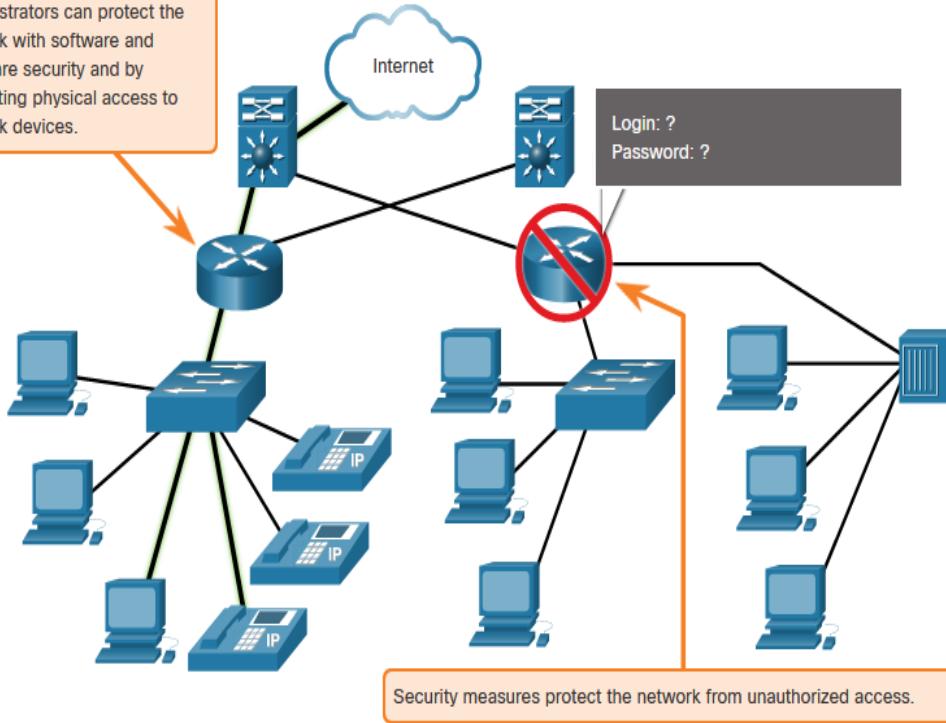
Hizmet Kalitesi (QoS), tüm kullanıcılar için içeriğin güvenilir bir şekilde sunulmasını sağlamak için kullanılan birincil mekanizmadır.

Bir QoS politikasının kullanımıyla, **yönlendirici veri akışını ve ses trafiğini** daha kolay yönetebilir.



# Reliable Network Network Güvenliği

Administrators can protect the network with software and hardware security and by preventing physical access to network devices.



Ele alınması gereken iki ana ağ güvenliği türü vardır:

## Network altyapı güvenliği

- Ağ aygıtlarının **fiziksel güvenliği**
- Aygıtlara **yetkisiz erişimi önleme**
- **Bilgi Güvenliği**
- Ağ üzerinden aktarılan **bilgi** veya **verilerin korunması**

## Ağ güvenliğinin üç hedefi:

- Confidentiality - **Gizlilik** – yalnızca amaçlanan alıcılar verileri okuyabilir
- Integrity - **Bütünlük** – iletim sırasında verilerin **değiştirilmemişinin güvencesi**
- Availability - **Kullanılabilirlik** – yetkili kullanıcılar için verilere zamanında ve güvenilir erişim güvencesi

# 1.7 Ağ Trendleri

# Son Trendler

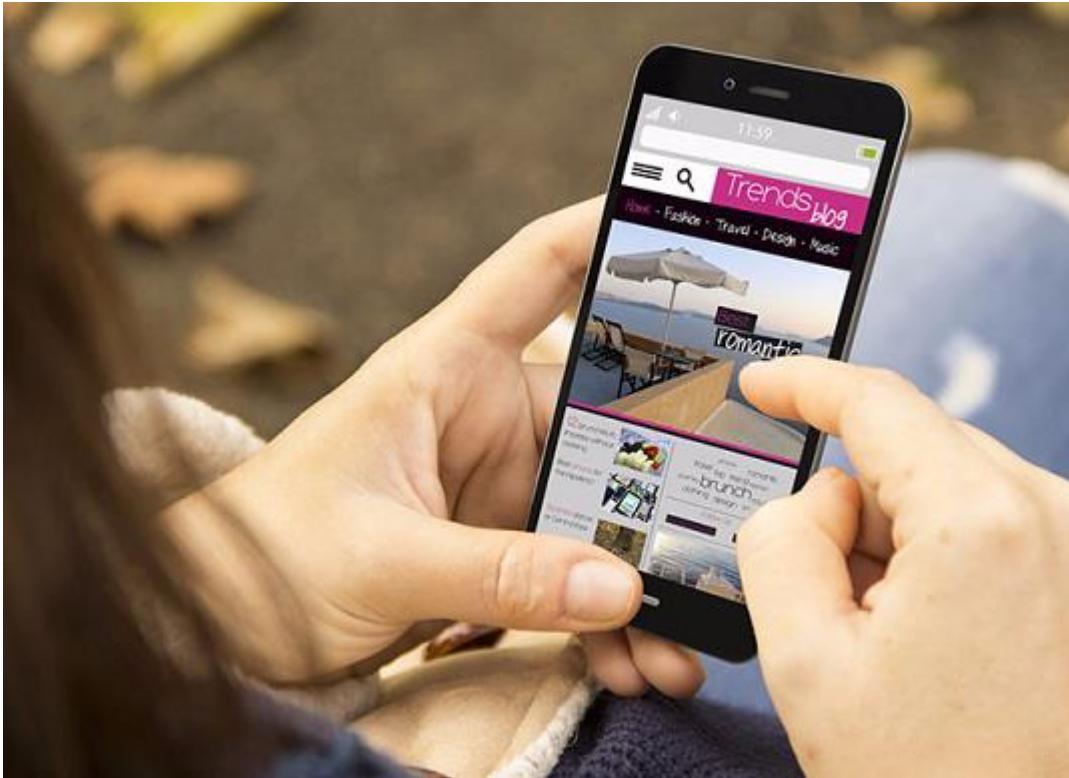


Pazardaki yeni teknolojiler ve gelişen son tüketici cihazlarına ayak uydurabilmek için networkün rolü sürekli uyumlanmalı ve değişimlidir.

Kuruluşları ve tüketicileri etkileyen birkaç yeni ağ trendi:

- Bring Your Own Device (BYOD) (kendi cihazını getir)
- Online collaboration (çevrimiçi işbirliği)
- Video bağlantıları
- Cloud computing (Bulut bilişim)

# Bring Your Own Device



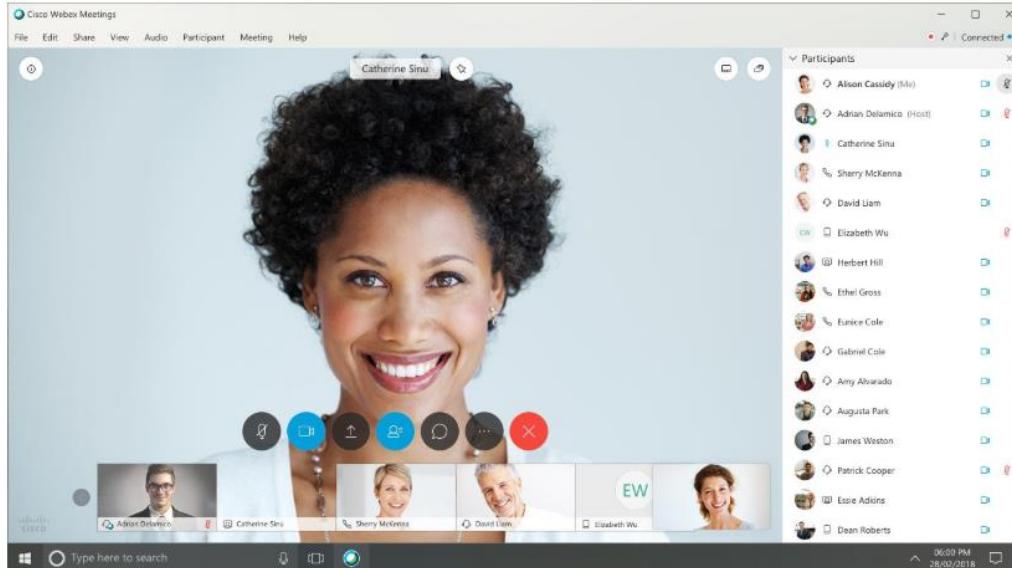
Kendi Cihazını Getir (BYOD), kullanıcıların kendi cihazlarını kullanmalarına olanak sağlayarak daha fazla fırsat ve daha fazla esneklik sağlar.

BYOD, son kullanıcıların bilgilere erişmek ve iletişim kurmak için kişisel araçları kullanma özgürlüğüne sahip olmasını sağlar:

- Laptoplar
- Netbooklar
- Tabletler
- Akıllı telefonlar
- E-okuyucular

BYOD cihazın sahibinin, cihazın tipinin, ve kullanıldığı yerin sınırsız olduğu senaryodur.

## Online Collaboration



- Ortak projelerde ağ üzerinden işbirliği yapın ve başkalarıyla birlikte çalışın.
- Cisco WebEx (şekilde gösterilmiştir) dahil olmak üzere işbirliği araçları (collab araçları), kullanıcılar arasında bağlanma ve etkileşim imkanı sağlar.
- İşbirliği işletmeler ve eğitim için çok yüksek bir önceliktir.
- Cisco Webex Teams çok fonksiyonlu bir işbirliği aracıdır.
  - anlık ileti gönderme
  - görüntüler gönder
  - video ve bağlantılar gönder

# Cloud Computing (Bulut Bilişim)

Cloud Computing, kişisel dosyaları depolamamıza veya verilerimizi internet üzerinden sunucularda yedeklememize olanak tanır.

- Uygulamalara Bulut'u kullanarak da erişilebilir.
- İşletmelerin dünyanın herhangi bir yerindeki herhangi bir cihaza servis etmesine olanak tanır.

Bulut bilişim veri merkezleri tarafından mümkün kılınır.

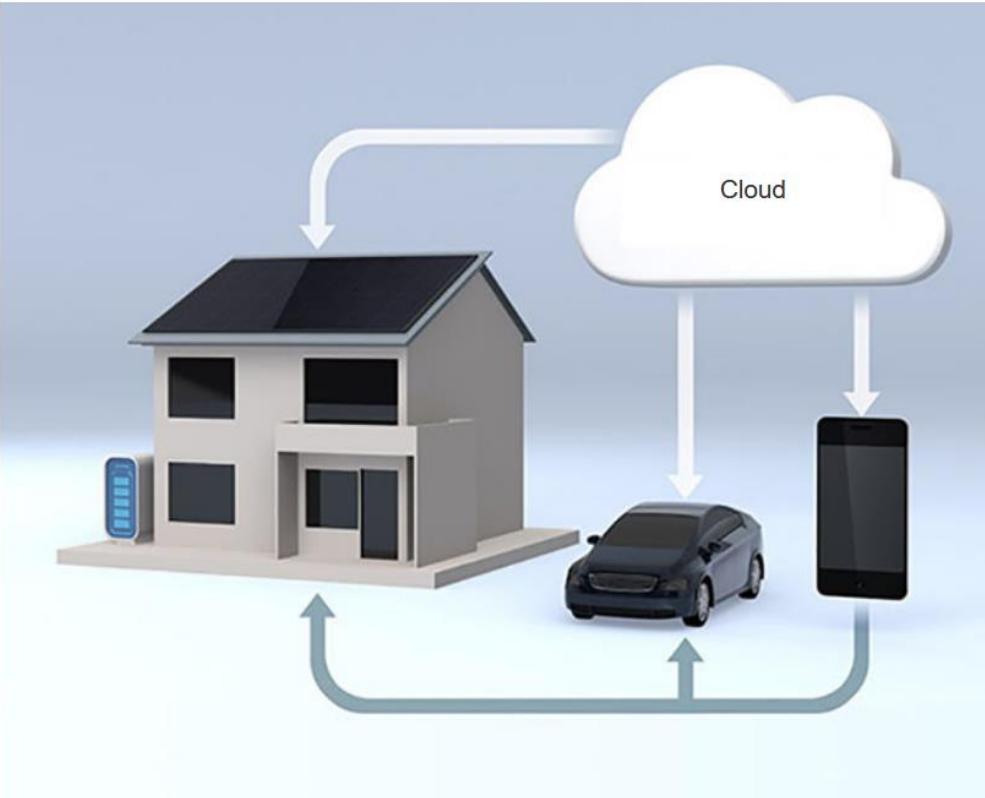
- Kendi veri merkezlerini karşılayamayan küçük şirketler,
- Bulut'taki daha büyük veri merkezi kuruluşlarından sunucu ve depolama hizmetleri kiralar.

# Cloud Computing (devamı)

Dört tür Bulut:

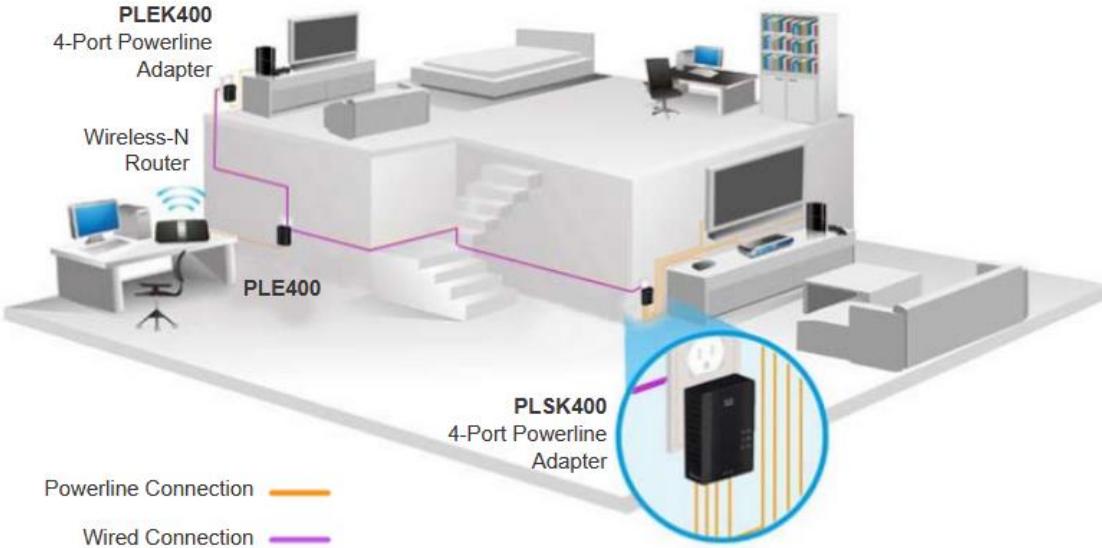
- Public Cloud
  - Kullanım başına ödeme modeli veya ücretsiz olarak genel kullanıma sunulan.
- Private Cloud
  - Hükümet gibi belirli bir kurum veya kuruluş için tasarlanmıştır.
- Hybrid Cloud
  - İki veya daha fazla Bulut türünden oluşur – örneğin, kısmen özel ve kısmen genel.
  - Her parça ayırt edici bir nesne olarak kalır, ancak her ikisi de aynı mimari kullanılarak bağlanır.
- Custom Cloud
  - Sağlık veya medya gibi belirli bir endüstrinin ihtiyaçlarını karşılamak için oluşturulmuştur.
  - Private veya Public olabilirler.

# Evde Teknoloji Trendleri



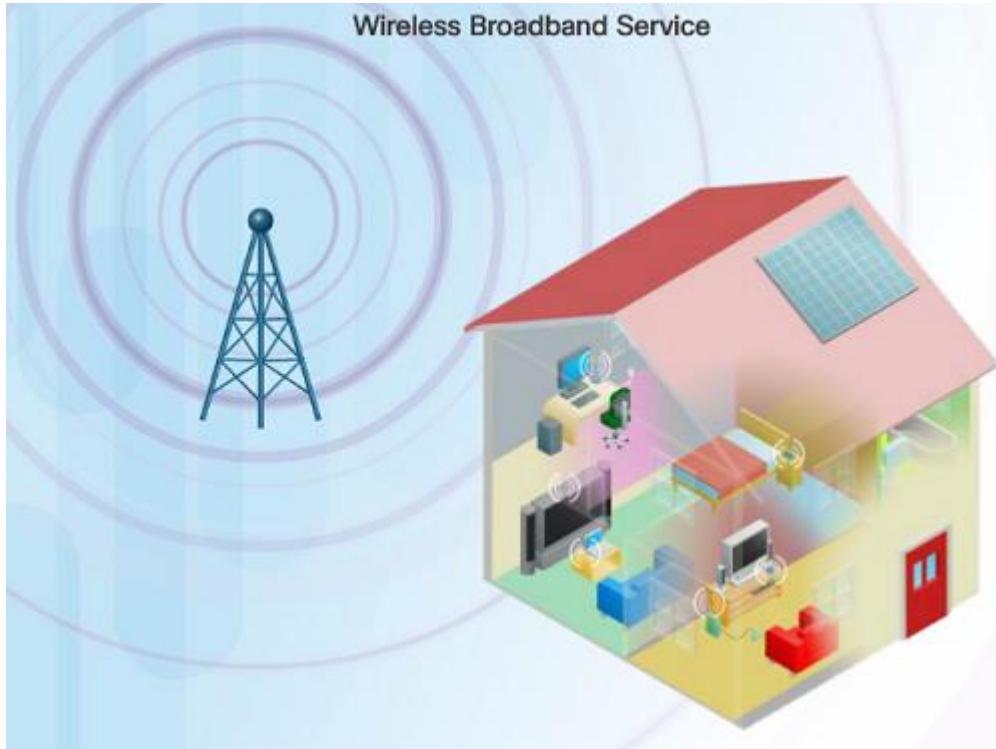
- Akıllı ev teknolojisi her gün kullanılan cihazların birbiriyle konuşmasını sağlayacak teknolojinin entegrasyonunu içeren giderek büyüyen bir teknoloji trendidir.
- **Fırınlar takvim uygulamanızla iletişime geçerek akşam kaçta evde olacağınızı ve yemeğin ne zaman pişirilmesi** gerekeceğini bilebilirler.
- Akıllı ev teknolojisi şu anda bir ev içindeki tüm odalar için geliştirilmektedir.

# Güç Hattı İletişimi (Powerline Networking)



- Powerline networkleri **data ağları** veya **mobil iletişim** geçerli bir seçenek olmadığından LAN'e **bağlanmayı sağlar**.
- Aygıtlar, standart bir powerline adapter kullanarak, belirli frekanslarda veri göndererek bir **elektrik prizi** olan **her yerde LAN'a bağlanabilir**.
- **Kablosuz** erişim noktaları evdeki tüm aygıtlara ulaşamıyorsa, **powerline ağ kullanımı** özellikle **kullanışlıdır**.

# Kablosuz geniş bant (Wireless Broadband)

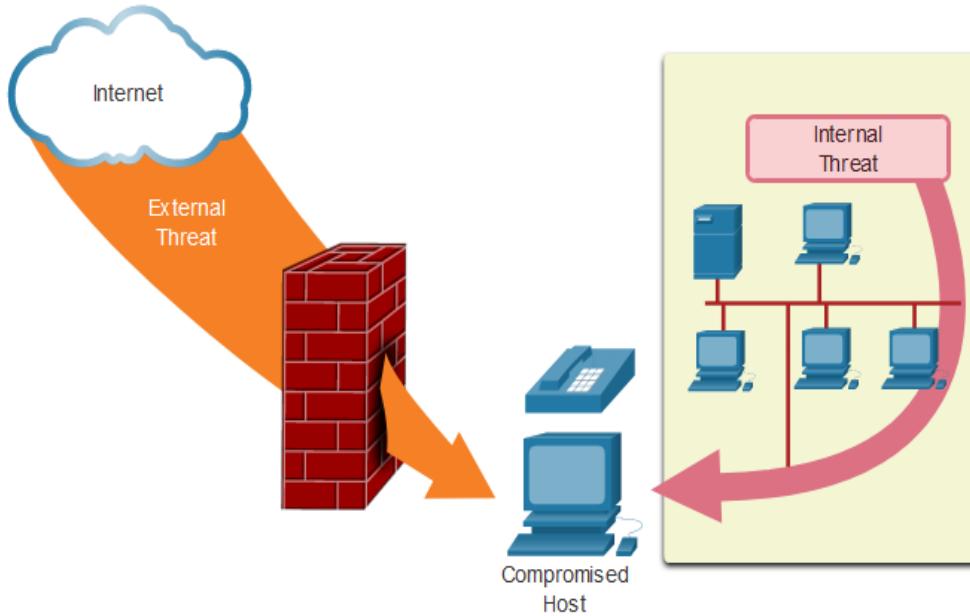


DSL ve kabloya ek olarak, **kablosuz evleri ve küçük işletmeleri internete bağlamak için kullanılan bir alternatif**tir.

- Daha yaygın olarak **kırsal ortamlarda bulunan Kablosuz İnternet Servis Sağlayıcısı (WISP)**, aboneleri belirlenmiş erişim noktalarına veya etkin noktalara bağlayan bir ISS'dir.
- **Kablosuz geniş bant ev ve küçük işletmeler için başka bir çözüm**dir.
- Akıllı telefon tarafından kullanılan hücresel teknolojisi kullanır.
- **Evdeki cihazlar için kablosuz veya kablolu bağlantı sağlayan bir anten** evin dışına kurulur.

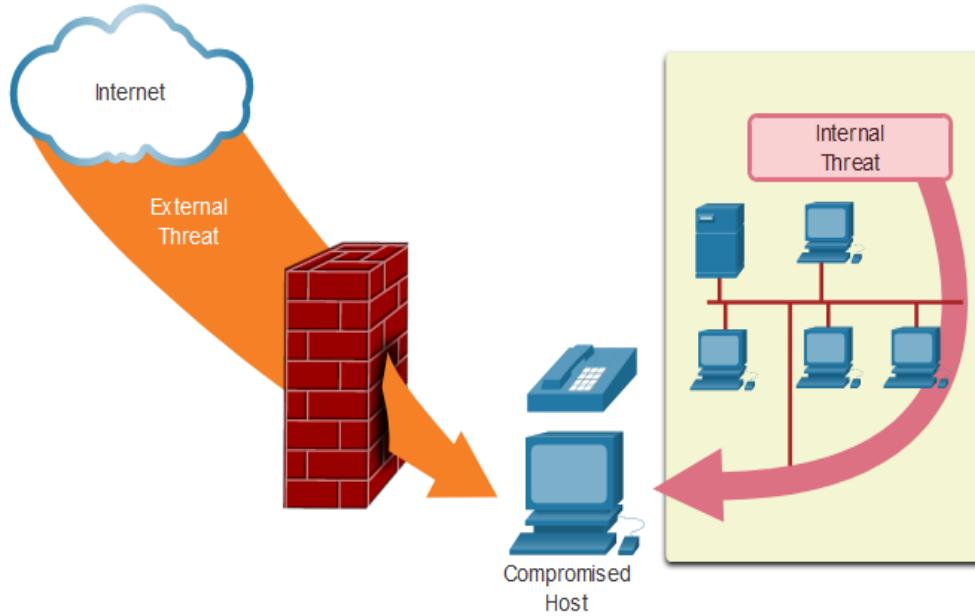
# 1.8 Network Güvenliği

# Güvenlik Tehditleri



- Ağ güvenliği, **ağın boyutundan bağımsız olarak**, **ağ yönetiminin ayrılmaz bir parçasıdır**.
- Uygulanan ağ güvenliği, verileri güvence altına alırken ağdan beklenen hizmet kalitesine izin verecek şekilde ortamı dikkate almalıdır.
- Bir ağın güvenliğini sağlamak, verileri güvence altına almak ve tehditleri azaltmak için **birçok protokol, teknoloji, araç, teknik ve teknoloji içerir**.
- **Tehdit vektörleri harici veya dahili olabilir**.

## Güvenlik Tehditleri (devamı)



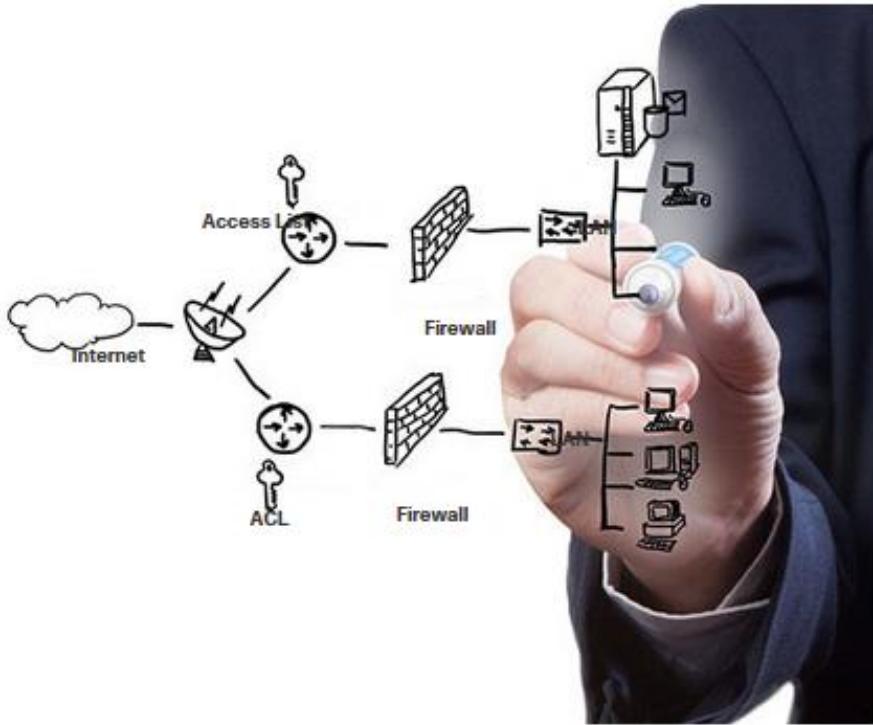
### Dış Tehditler:

- Virusler, worms (solucanlar), and Trojan horses (Truva atları)
- Casus yazılımları (Spyware) ve reklam yazılımları (adware)
- Sıfır gün saldıruları (Zero-day attacks)
- Threat Actor attacks
- Hizmet reddi saldıruları (Denial of service attacks)
- Veri önleme (Data interception) ve hırsızlık
- Kimlik çalma (Identity theft)

### İç Tehditler:

- kaybolan veya çalınan cihazlar
- çalışanlar tarafından kazara kötüye kullanım
- kötü niyetli çalışanlar

# Güvenlik Çözümleri

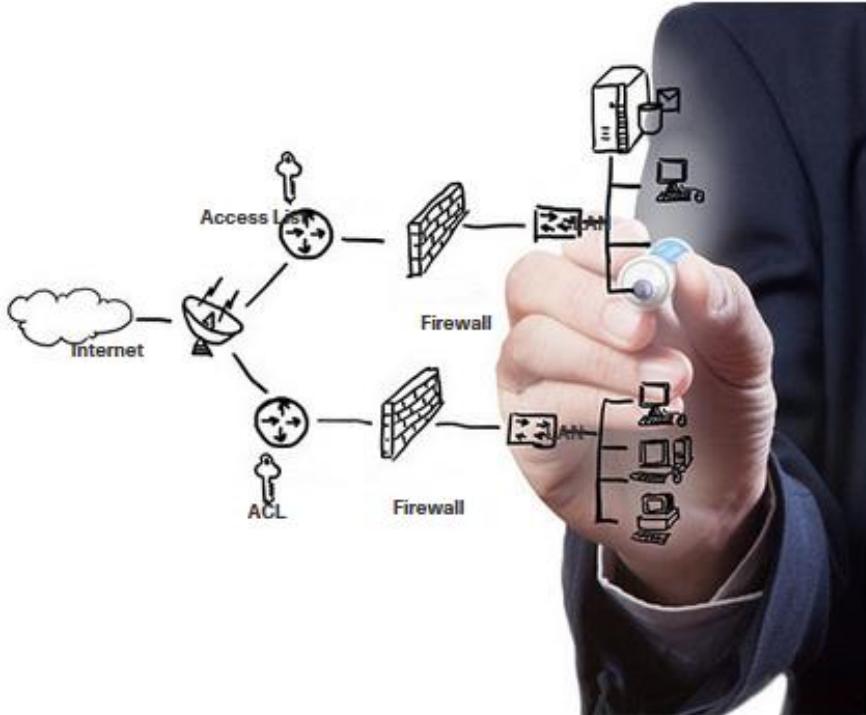


Güvenlik birden fazla güvenlik çözümü kullanılarak birden çok katmanda uygulanmalıdır.

**Ev veya küçük ofis ağları** için ağ güvenliği bileşenleri:

- Son cihazlara **virüsten koruma ve casus yazılım önleme yazılımı** yüklenmelidir.
- **Ağa yetkisiz erişimi engellemek** için kullanılan güvenlik duvarı滤resi (firewall).

# Security Solutions (Cont.)



Daha büyük ağların ek güvenlik gereksinimleri vardır:

- **Dedike firewall sistemleri**
- **Erişim denetim listeleri** (Access control lists ACL)
- **Saldırı önleme sistemi** (Intrusion prevention systems IPS)
- **Virtual private network** (VPN)

Ağ güvenliği çalışması, temel anahtarlama (switching) ve yönlendirme (routing) altyapısının net bir şekilde anlaşılması ile başlar.

# 1.9 BT Uzmanı

# The IT Professional CCNA



## Cisco Certified Network Associate (CCNA) sertifikasyon:

- temel teknolojiler hakkında bilgi sahibi olduğunuzu gösterir
- Yeni nesil teknolojilerin benimsenmesinde gerekli yetkinlikler için güncel kalmanızı sağlar.

## Yeni CCNA odak:

- **IP temeli ve güvenlik konuları**
- **Kablosuz, sanallaştırma, otomasyon ve ağ programlanabilirliği.**

Associate, specialist ve profesyonel seviyelerinde yeni DevNet sertifikasyonları da programlama yetkinliklerinizi valide eder.

Specialist sertifikasyonu **işinizdeki rol ve ilginize yönelik yetkinliklerinizi valide eder.**

# The IT Professional Networking İşleri

## Employment Opportunities

Discover career possibilities and options from our Talent Bridge employment program.



### Talent Bridge Matching Engine

Find employment opportunities where you live with the new pilot program, the Talent Bridge Matching Engine. Search for jobs with Cisco as well as Cisco partners and distributors seeking Cisco Networking Academy students and alumni. Register now to complete your profile. Must be 18 years of age or older to register and participate in the Matching Engine.



### Be Part of Our Dream Team

We offer opportunities to gain hands-on experiences throughout the year. These are specific projects that we invite students to participate in as a Dream Team member. Learn more about this experience and how you can participate.



### Your Career, our Talent Bridge Resources

Learn about the resources we have to offer that can help you on your journey to becoming gainfully employed.



[www.netacad.com](http://www.netacad.com)'da Kariyer menüsüne tıklayıp iş fırsatlarını seçebilirsiniz..

- Talent Bridge Eşleştirme Motoru'nu kullanarak iş fırsatları bulun.
- Cisco Networking Academy öğrencileri ve mezunları arayan Cisco, Cisco iş ortakları ve distribütörlerle iş arayın.

# 1.10 Modül Uygulama ve Sınav

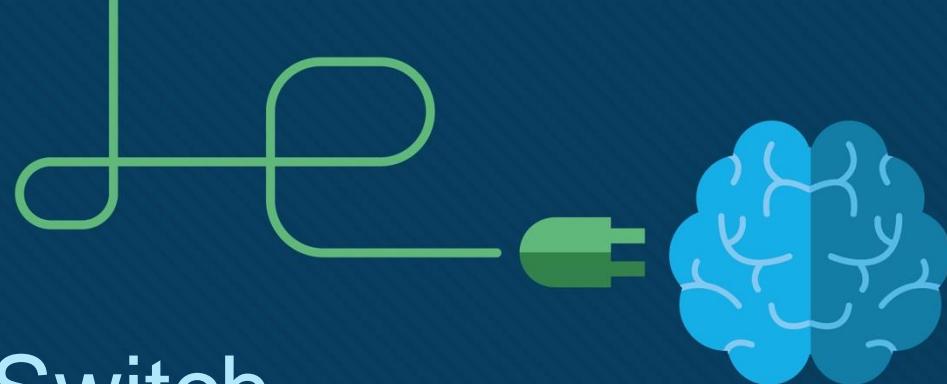
## Bu modülde ne öğrendim??

- Ağların kullanımı sayesinde, daha önce hiç olmadığı kadar birbirimize bağlıyız.
- Bir ağa bağlı olan ve doğrudan ağ iletişimine katılan tüm bilgisayarlar ana bilgisayar (host) olarak sınıflandırılır.
- Ağ diyagramları genellikle bir ağı oluşturan farklı aygıtları ve bağlantıları temsil etmek için semboller kullanır.
- Diyagram, aygıtların büyük bir ağıda nasıl bağlayacağını anlamanın kolay bir yolunu sağlar.
- İki tür ağ altyapısı Yerel Alan Ağları (LAN) ve Geniş Alan Ağlardır (WAN).
- SOHO internet bağlantıları kablo, DSL, Hücresel, Uydu ve Dial-up telefon içerir.
- İş internet bağlantıları özel Leased hat, Metro Ethernet, Business DSL ve Uydu içerir.

## Bu modülde ne öğrendim?? (devamı)

- Ağ mimarisi, verileri ağ üzerinde hareket ettiren altyapıyı ve programlanmış hizmetleri ve kuralları veya protokollerini destekleyen teknolojileri ifade eder.
- Ağ mimarisinin dört temel özelliği vardır: Hata Toleransı, Ölçeklenebilirlik, Hizmet Kalitesi (QoS) ve Güvenlik.
- Kuruluşları ve tüketicileri etkileyen en son ağ eğilimleri: Kendi Cihazınızı Getir (BYOD), çevrimiçi işbirliği (collaboration), video iletişim ve bulut bilişim.
- Ağlara yönelik çeşitli yaygın dış ve iç tehditler vardır.
- Daha büyük ağlar ve şirket ağları virüsten koruma, casus yazılım önleme ve güvenlik duvarı filtreleme kullanır, ancak farklı güvenlik gereksinimleri de vardır: Dedicated firewall sistemleri, Access control listeleri (ACL), Intrusion prevention systems (IPS), ve Virtual private networks (VPN)
- Cisco Certified Network Associate (CCNA) sertifikasyon, temel teknolojiler hakkındaki bilginizi gösterir.





# Modül 2: Temel Switch (Anahtar) ve End Device (Son Aygıt) Yapılandırması (Konfigürasyonu)

Introductions to Networks v7.0  
(ITN)



# Modül Hedefleri

## Modül Başlığı: Temel Switch ve End Device Konfigürasyon

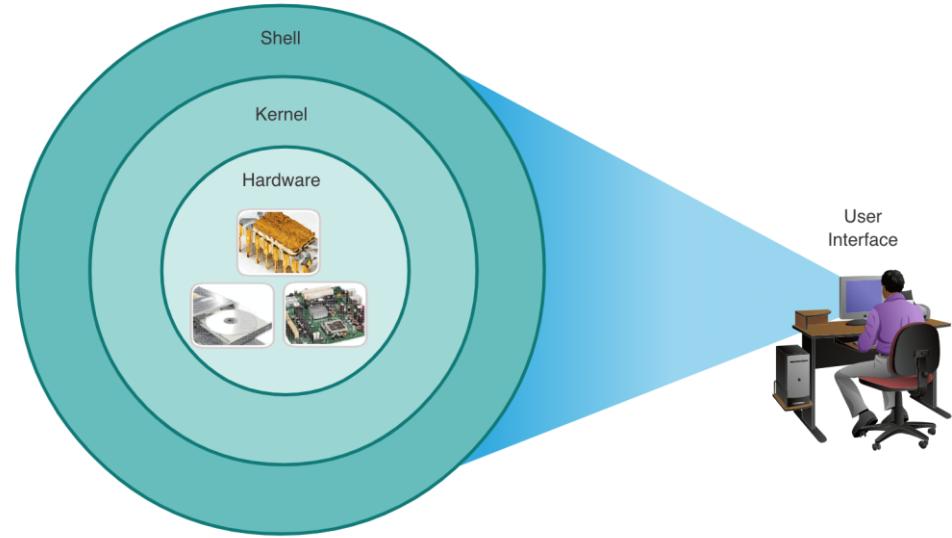
**Modül Hedefi:** Network switch ve son aygıtlarda parolalar, IP adresleme ve varsayılan ağ geçidi parametreleri dahil olmak üzere ilk ayarları uygulama.

Konu Başlığı	Konu Hedefi
Cisco IOS Erişimi	Yapilandırma amacıyla bir Cisco IOS cihazına nasıl erişileceğini açıklayın.
IOS Navigasyon	Ağ aygıtlarını yapılandırmak için Cisco IOS'u nasıl naviye edeceklerini açıklayın.
Komut Yapısı	Cisco IOS yazılımının komut yapısını açıklayın.
Temel Aygit Yapılandırması	CLI kullanarak bir Cisco IOS cihazını yapılandırın.
Yapılandırmaları Kaydet	Çalışan yapılandırmayı kaydetmek için IOS komutlarını kullanın.
Portlar ve Adresler	Aygıtların ağ ortamları arasında nasıl iletişim kurduğunu açıklayın.
IP Adresleme yapılandırma	IP adresi olan bir ana bilgisayar aygitini yapılandırın.
Bağlantı doğrula	İki son aygit arasındaki bağlantıyı doğrulayın.

# 2.1 Cisco IOS Erişimi

# İşletim Sistemleri (Operating Systems)

- **Shell** - (Kabuk) Kullanıcıların bilgisayardan belirli görevleri istemesine olanak tanıyan kullanıcı arabirimini. Bu istekler CLI veya GUI arabirimleri aracılığıyla yapılabilir.
- **Kernel** - (Çekirdek) Bilgisayarın donanımı ve yazılımı arasında iletişim kurar ve donanım kaynaklarının yazılım gereksinimlerini karşılamak için nasıl kullanıldığını yönetir.
- **Hardware** - (Donanım) Altta yatan elektronik de dahil olmak üzere bilgisayarın fiziksel parçası.



# Cisco IOS Access GUI

- GUI, kullanıcının grafik ikonları, menüleri ve pencerelerden oluşan bir ortamı kullanarak sistemle etkileşim kurmasını sağlar.
- GUI daha kullanıcı dostudur ve sistemi kontrol eden temel komut yapısı hakkında daha az bilgi gerektirir.
- Örnekleri: Windows, macOS, Linux KDE, Apple iOS and Android.
- GUIs fail, crash edebilir, veya istendiği gibi çalışmayabilir (operate). Bu nedenlerden dolayı, ağ aygıtlarına genellikle bir CLI üzerinden erişilir.



# İşletim Sistemi'nin (OS) Amacı

PC işletim sistemi, bir kullanıcının aşağıdakileri yapmasını sağlar:

- Seçimler yapmak ve programları çalıştırmak için fareyi kullanma
- Metin ve metin tabanlı komutları giriş
- Çıktıyı monitörde görüntüleme



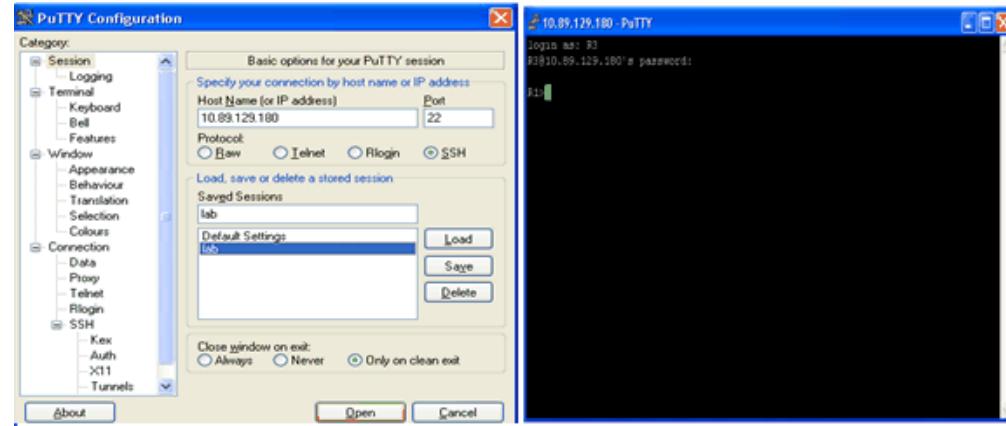
CLI tabanlı ağ işletim sistemi, bir ağ teknisyeninin aşağıdakileri yapabilmesini sağlar:

- CLI tabanlı ağ programlarını çalıştırmak için klavye kullanma
- Metin ve metin tabanlı komutları girmek için klavye kullanma
- Çıktıyı monitörde görüntüleme
- 

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

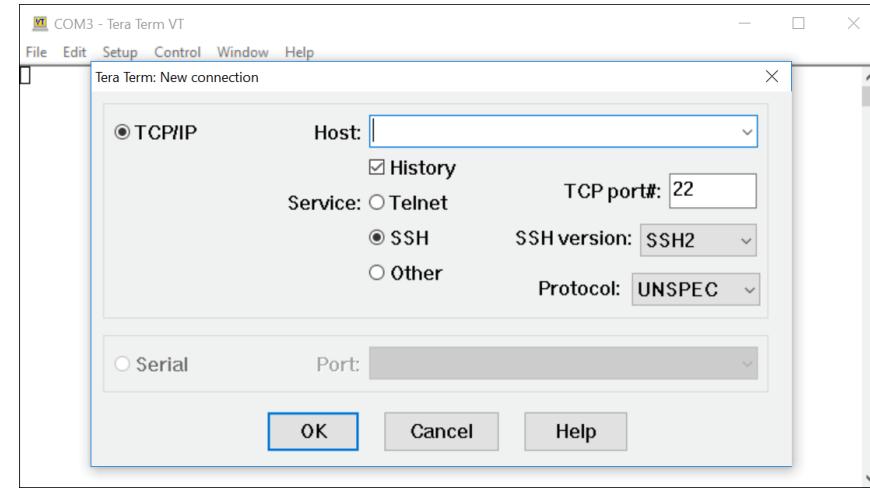
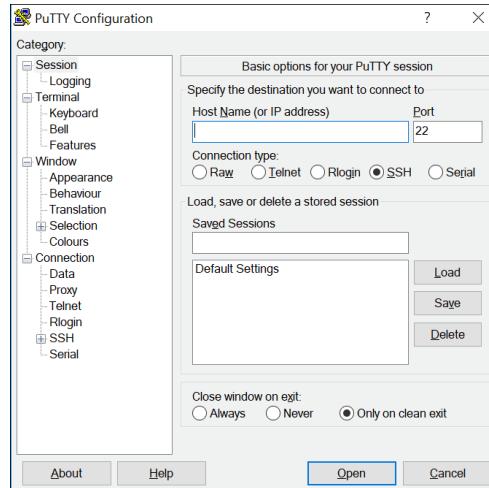
# Erişim Yöntemleri

- **Konsol (Console)** – İlk yapılandırmalar gibi bakım hizmeti sağlamak üzere **kullanılan fiziksel yönetim portu** (bağlantı noktası).
- **Güvenli Kabuk (Secure Shell SSH)** – Bir aygıta network üzerinden **bir sanal arabirim aracılığıyla güvenli bir uzaktan CLI bağlantısı kurar.** (Not: Bu, bir aygıta uzaktan bağlanmak için önerilen yöntemdir.)
- **Telnet** – Ağ üzerinden bir aygıta güvenli **olmayan uzaktan CLI bağlantısı kurar.** (Not: Kullanıcı kimlik doğrulaması, parolalar ve komutlar ağ üzerinden düz metin olarak gönderilir.)



# Terminal Emülatör Programları

- **Terminal emülatör programları**, bir ağ aygıtına **konsol bağlantı noktası** veya **SSH/Telnet bağlantısı** ile bağlanmak için kullanılır.
- **PuTTY**, **Tera Term** ve **SecureCRT** gibi çeşitli terminal emülatör programları vardır.



# 2.2 IOS Navigasyon

# Birincil Komut Modları

## User EXEC Mod:

- Yalnızca **sınırlı sayıda temel izleme komutuna** erişim sağlar
- > simgesi ile biten CLI komut istemi (prompt) ile tanımlanır
- 

```
Router>
```

```
Switch>
```

## Privileged EXEC Mod:

- **Tüm komutlara ve özelliklere erişim sağlar**
- # simgesi ile biten CLI komut istemi (prompt) ile tanımlanır

```
Router#
```

```
Switch#
```

# Konfigürasyon Modu ve Alt Yapılandırma (subconfig) Modları

## Global Configuration Mod:

- **Aygıttaki yapılandırma seçeneklerine erişmek için kullanılır**

```
Switch(config)#
```

## Line Configuration Mod:

- **Konsol, SSH, Telnet veya AUX erişimini yapılandırmak için kullanılır**

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

## Interface Configuration Mod:

- **Anahtar bağlantı noktası veya yönlendirici arabirimini yapılandırmak için kullanılır**

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

# Video – IOS CLI Birincil Komut Modları

Bu video aşağıdakileri kapsayacaktır:

- User EXEC mod
- Privilege EXEC mod
- Global Config mod

# IOS Modları Arasında Navigasyon

## ▪ Privileged EXEC Mod:

- Kullanıcı EXEC mod'undan privileged (ayraklı) EXEC moduna geçmek **enabled** komutunu kullanın.

```
Switch> enable  
Switch#
```

## ▪ Global Configuration Mod:

- Global Configuration moduna **geçiş** ve **çıkış** için **configure terminal** (command) komutunu kullanın.
- Privilege EXEC moduna dönmek için **exit** komutunu kullanın.

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

## ▪ Line Configuration Mod:

- Line configuration moduna geçiş ve çıkış için **line** command ve management line type kullanın. Genel yapılandırma moduna dönmek için, **exit** komutunu kullanın.

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

# IOS Modları Arasında Navigasyon (devamı)

## Alt Yapılandırma Modları (Subconfiguration Modes):

- Herhangi bir alt yapılandırma modundan çıkış global konfigürasyon moduna dönmek için **exit** komutunu kullanın.
- Privilige EXEC moduna dönüş için **end** komutunu veya **Ctrl +Z** tuş kombinasyonunu kullanın.
- Bir alt yapılandırma modundan diğerine doğrudan taşımak için, **istenilen alt yapılandırma modu komutunu** yazın.
- Örnekte komut istemi (**config-line**)# 'dan (**config-if**)#' e geçiyor.

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

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

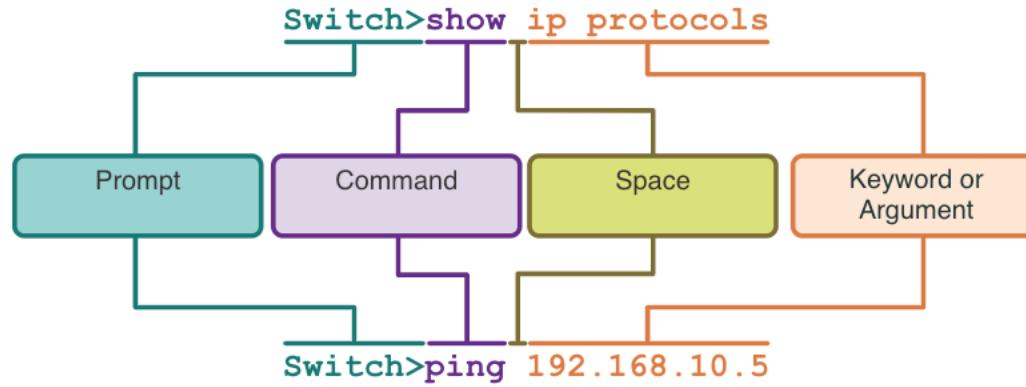
# Video – IOS Modları Arasında Navigasyon

Bu video aşağıdakileri kapsayacaktır:

- enable
- disable
- configure terminal
- exit
- end
- Klavyede Control + Z
- Alt yapılandırma modlarını girmek için diğer komutlar

# 2.3 The Komut Yapısı (Command Structure)

# Temel IOS Komut Yapısı



- **Keyword (Anahtar Kelime)** – Bu, işletim sisteminde tanımlanan belirli bir parametredir (şekilde, **ip protokol**).
- **Argument (Bağımsız Değişken)** - Önceden tanımlı olmayan; kullanıcı tarafından tanımlanan bir değer veya değişkendir (şekilde, **192.168.10.5**).

# IOS Komut Syntax Kontrol

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

- Boldface metni gösterildiği gibi girilen komutları ve anahtar kelimeleri gösterir.
- Italik metin, kullanıcının değer atayacağı bir bağımsız değişkeni gösterir.

Convention	Description
<b>boldface</b>	Boldface metinler aynen gördüğünüz gibi girdiğiniz komut ve anahtar kelimeleri gösterir.
<i>italics</i>	Italik metin, değer sağladığınız bağımsız değişkenleri gösterir.
[x]	Kare ayraçlar isteğe bağlı bir ögeyi (anahtar kelime veya bağımsız değişken) gösterir.
{x}	Ayraçlar <b>gerekli ögeyi</b> (anahtar kelime veya bağımsız değişken) gösterir.
[x {y   z}]	<b>Ayraçlar ve kare ayraçlar</b> içindeki <b>dikey çizgiler isteğe bağlı</b> bir öge içinde gerekli seçimi gösterir. Boşluklar, komutun bazı bölümlerini açıkça ifade etmek için kullanılır.

# IOS Komut Sözdizimi Kontrol (devamı)

- Komut sözdizimi, bir komut girerken kullanılması gereken desen veya biçimini sağlar.
- Komut **ping** ve kullanıcının tanımladığı argüman hedef cihazın *ip-adresi*. Örneğin, **ping 10.10.10.5**.
- Komut **traceroute** ve kullanıcının tanımladığı argüman hedef cihazın *ip-adres*. Örneğin, **traceroute 192.168.254.254**.
- Bir komut birden çok bağımsız değişkenli ise, **bu şekilde temsil edildiğini görebilirsiniz**:

```
ping ip-address
```

```
traceroute ip-address
```

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

# IOS Yardım Özellikleri

IOS'un iki yardım şekli vardır: **bağlam duyarlı** (context-sensitive help) ve **komut söz dizimi denetimi** (command syntax check).

- **İçeriğe duyarlı yardım**, bu soruların yanıtlarını hızla 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?
- **Komut sözdizimi denetimi**, kullanıcı tarafından **geçerli bir komut girişini doğrular**.
  - Interpreter eğer girilen komutu anlayamaz ise, **komutta neyin yanlış olduğunu açıklayıcı bir geri bidirim döner**.

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

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

# Video – Bağlam Duyarlı Yardım ve Komut Sözdizimi Denetleyicisi

Bu video aşağıdakileri kapsayacaktır:

- User EXEC, privileged EXEC, ve global config modlarında Yardım kullanımı
- Komutları ve bağımsız değişkenleri yardım komutuyla bitirme
- Sözdizimi hatalarını ve eksik komutları düzeltmek için komut sözdizimi denetleyicisinin kullanımı.

# Hot Keys ve Shortcuts (Kısa yollar)

- IOS CLI, **yapılardırmayı, izlemeyi** ve **sorun giderme işlemlerini** kolaylaştırın kısayollar sağlar.
- **Komutlar ve anahtar kelimeler**, benzersiz bir seçimi tanımlayan **en az karakter sayısına kısaltılabilir**. Örneğin, **configure** komutu **conf** olarak kısaltılabilir çünkü **configure conf** ile başlayan tek komuttur.

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

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

# Kısa Yollar (Hot Keys ve Shortcuts devamı)

- Alttaki tablo, komut satırı düzenlemelerini iyileştirmek için kullanılabilecek tuş vuruşlarının kısa bir listesidir.

Keystroke	Açıklama
Tab	Kısmi komut adı girişini tamamlar.
Backspace	İmlecin solundaki karakteri siler.
Left Arrow veya Ctrl+B	Kursörü (imleci) bir karakter sola taşır.
Right Arrow veya Ctrl+F	İmleci bir karakter sağa taşır.
Up Arrow veya Ctrl+P	En son komutlardan başlayarak geçmiş arabelleğindeki komutları geri çağırır.

# Kısa Yollar (Hot Keys ve Shortcuts devamı)

- Bir komut çıktısı terminal penceresinde görüntülenebilecektен daha fazla metin ürettiğinde, IOS bir "**--More-**" komut istemi görüntüler. Aşağıdaki tabloda, bu komut istemi görüntülendiğinde kullanılabilen tuş vuruşları görülmektedir.
- Aşağıdaki tabloda, bir işlemden çıkmak için kullanılabilecek komutlar listelenebilir.

Keystroke	Description
Enter	Sonraki satırı görüntüler.
Space Bar	Sonraki ekranı görüntüler.
Herhangi diğer tuş	Privileged EXEC moduna geri dönerek ekran dizesini sona erdirir.

Keystroke	Description
Ctrl-C	Herhangi bir yapılandırma modundayken, yapılandırma modu sona erer ve privileged EXEC moduna geri döner.
Ctrl-Z	Herhangi bir yapılandırma modundayken, yapılandırma modu sona erer ve privileged EXEC moduna geri döner.
Ctrl-Shift-6	DNS, aramalar, traceroutes, pingleri, vs iptal etmek için çok amaçlı kesme sırası.

Not: Daha fazla anahtar ve kısayol görmek için 2.3.5'e bakın.

# Video – Kısa Yollar

Bu video aşağıdakileri kapsayacaktır:

- Tab tuşu (tab completion)
- Komut kısaltma
- Yukarı ve aşağı ok tuşu
- CTRL + C
- CTRL + Z
- CTRL + Shift + 6
- CTRL + R

# Packet Tracer – IOS Navigasyon

Bu Packet Tracer'da, aşağıdakileri yapacaksınız:

- Temel Bağlantılar Kurun, CLI'ye Erişin ve Yardım Keşfedin
- EXEC Modlarını keşfedin
- Saati Ayarlayın
-

# Lab – Konsol Bağlantısı için Tera Terimini Kullanarak IOS'da Navigasyon

Bu laboratuvara, aşağıdaki hedefleri tamamlayacaksınız:

- Seri Konsol Bağlantı Noktasından Cisco Switch'e erişin
- Temel Aygit Ayarlarını Görüntüleme ve Yapılandırma
- (İsteğe bağlı) Mini USB Konsol Kablosu Kullanarak Cisco Router'a Erişin

# 2.4 Temel Aygıt Yapılandırması

# Cihaz Adları

- Herhangi bir cihazdaki ilk yapılandırma komutu, benzersiz bir hostname vermek olmalıdır.
- Varsayılan olarak, tüm aygıtlar bir fabrika varsayılan adı atanır. Örneğin, bir Cisco IOS switch "Switch" olarak adlandırılır.
- Cihazları adlandırma için kılavuz:
  - Bir harfle başla
  - Boşluk içermez
  - Harf veya rakamla sonlansın
  - Yalnızca harfleri, rakamları ve tire kullan
  - Uzunluğu 64 karakterden az olsun
  -

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

**Not:** Switch'i varsayılan prompta döndürmek için **no hostname** global config komutunu kullanın.

# Şifre Yönergeleri

- Zayıf veya kolayca tahmin edilen parolaların kullanımı bir güvenlik sorunudur.
- Tüm network cihazları, privileged EXEC, user EXEC ve uzaktan Telnet erişimi parola kullanarak yönetsel (administrative) erişimi sınırlırmalıdır. Buna ek olarak, tüm şifreler şifrelenmeli ve yasal bildirimler sağlanmalıdır.
- Şifre Yönergeleri:
  - Uzunluğu sekiz karakterden fazla olan parolaları kullanın.
  - Büyük ve küçük harfler, sayılar, özel karakterler ve/veya sayısal dizilerin birleşimini kullanın.
  - Tüm aygıtlar için aynı parolayı kullanmaktan kaçının.
  - Kolayca tahmin edildikleri için sık kullanılan kelimeleri kullanmayın.



**Not:** Bu kurstaki laboratuvarların çoğu, **cisco** veya **class** gibi basit parolalar kullanmaktadır. Bu parolalar zayıf ve kolayca tahmin edilebilir olarak kabul edilir ve production ortamlarında kullanılmamalıdır.

# Parolaları Yapılandırma

### User EXEC modu erişimini güvence altına alma

- Öncelikle, global configurasyon modunda **line console 0** komutunu kullanarak line console konfigürasyonuna geçin.
- Ardından, **password password** komutunu kullanarak user EXEC mode parolasını belirleyin.
- Son olarak, oturum açma komutunu kullanarak user EXEC erişimini etkinleştirin.

### Privileged EXEC modu erişimini güvence altına alma:

- Önce global yapılandırma moduna girin.
- Ardından **enable secret password** komutunu kullanın.

```
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#
```

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

# Parolaları Yapılandırma (devamı)

VTY line erişimini güvenceye alma:

- İlk olarak, global configuration modda, **line vty 0 15** komutunu kullanarak VTY configuration moduna geçin.
  - Ardından **password password** komutunu kullanarak VTY parolasını belirleyin.
  - Son olarak, **login** komutunu kullanarak VTY erişimini etkinleştirin.
- 
- Not: VTY hatları cihaza Telnet veya SSH kullanarak uzaktan erişim sağlar. Cisco cihazlarının pek çoğu 0 dan 15 numaralandırılan 16'ya kadar VTY line'ını destekler.

```
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#
```

# Parolaları Şifreleme (encrypt)

- Startup-config ve running-config dosyaları çoğu parolayı düz metin olarak görüntüler.
- Tüm düz metin paroları şifrelemek için **service password-encryption** global config komutunu kullanın.

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

- Cihazdaki paroların şifrelenmiş olduğunu teyit etmek 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
```

# Banner Mesajları

- Cihaza erişmeye çalışan yetkisi olmayan personeli uyarmak için banner mesajı önemlidir.
- Bir network cihazında günün banner mesajını oluşturmak için **banner motd** # *the message of the day* # global config komutunu kullanın.

Not: Komut sözdiziminde "#" adlı karakter delimiting - sınırlayıcı karakter olarak adlandırılır. İletiden önce ve sonra girilir.

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

Banner, aygıta erişme girişimlerinde görüntülenir.



```
Press RETURN to get started.
```

```
Authorized Access Only!
```

```
User Access Verification
```

```
Password:
```

# Video – Anahtara Güvenli Yönetim Erişimi

Bu video aşağıdakileri kapsayacaktır:

- Switch'i güvenli kılmak için komut satırına erişim
- Konsol bağlantı noktasına güvenli erişim
- Uzaktan erişim için güvenli sanal terminal erişimi
- Anahtardaki parolaları şifreleme
- Banner iletisini yapılandırma
- Güvenlik değişikliklerini doğrulama

# 2.5 Yapılandırmaları Kaydet

# Yapilandırma Dosyaları

- Aygıt yapılandırmasını depolayan iki sistem dosyası vardır:

- startup-config** - Bu, NVRAM'da depolanan kaydedilmiş yapılandırma dosyasıdır. Başlatılırken veya yeniden başlatılırken aygit tarafından kullanılacak tüm komutları içerir. Flash, aygit kapalıken içeriğini kaybetmez.
- running-config** - Bu Random Access Memory de (RAM) saklanır. Geçerli yapılandırmayı yansıtır. Çalışan bir yapılandırmayı değiştirmek, Cisco aygitinin çalışmasını hemen etkiler. RAM geçici bellektir. Aygit kapatıldığında veya yeniden başlatıldığından tüm içeriğini kaybeder.
- Running configurationda (çalışan yapılandırma) yapılan değişiklikleri startup config'e (başlangıç yapılandırması) kaydetmek için **copy running-config startup-config** privileged EXEC mode 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
```

```
Router#show running-config
Building configuration...

Current configuration : 624 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
```

# Çalışan Yapılandırmaları Değiştirme

Çalışan config'de yapılan değişiklikler istenen etkiyi yaratmazsa ve çalışan config henüz kaydedilmemişse, aygıtı önceki yapılandırmasına geri yükleyebilirsiniz. Bunu yapmak için şunları yapabilirsiniz:

- Değiştirilen komutları tek tek kaldırma.
- Privileged EXEC modunda **reload** komutunu kullanarak aygıtı yeniden yükleme. *Not: Bu, aygıtın kısa bir süre çevrimdışı geçmesine ve network downtime'na neden olur.*
- İstenmeyen değişiklikler, start-up config'e kaydedildi ise, privileged EXEC modunda, the **erase startup-config** komutunu kullanarak tüm yapılandırmaları temizlemek gerekebilir.
- Start-up config'i sildikten sonra, running-config dosyasını RAM'den temizlemek için aygıtı yeniden yükleyin.

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

```
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#
```

# Video –Running Configuration (çalışan yapılandırma)yi değiştirme

Bu video aşağıdakileri kapsayacaktır:

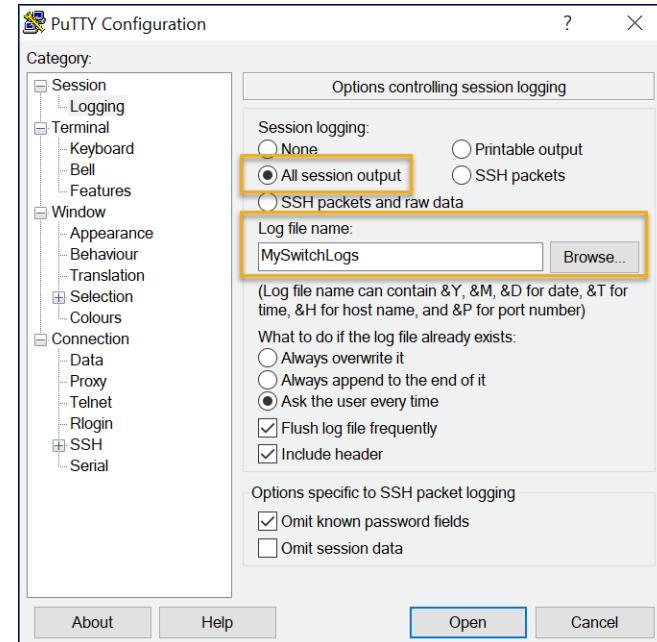
- Running-config dosyasını startup-config dosyasına kopyalama
- Dosyaların flash veya NVRAM dizininde gösterimi
- Komut kısaltmasını kullanma
- Başlangıç-config dosyasını silme
- Start-config dosyasını running-config dosyasına kopyalama

## Save Configurations

# Yapılardırımı Metin Dosyasında Saklama

Yapılardırma dosyaları da kaydedilebilir ve bir metin belgesine arşivlenebilir.

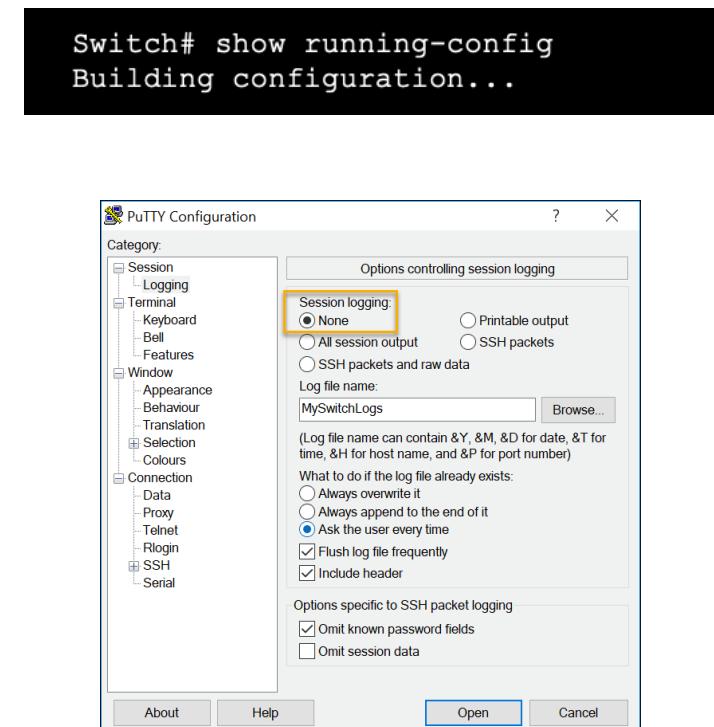
- **Adım 1.** PuTTY veya Tera Term gibi zaten bir anahtara bağlı olan bir emulator yazılımını aç.
- **Adım 2.** Terminal yazılımına oturum açmayı etkinleştirin ve günlük dosyasını kaydetmek için bir ad ve dosya konumu belirleyin. Şekil tüm oturum çıktısının (**All session output**) belirtilen dosyaya alınacağını göstermektedir (örn., MySwitchLogs).



# Yapilandırmayı Metin Dosyasında Saklama (devamı)

- Adım 3.** Privileged EXEC promptunda **show running-config** veya **show startup-config** komutunu yürüt. Terminal penceresinde görüntülenen metin seçilen dosyada görüntülenir.
- Adım 4.** Terminal yazılımında günlüğe kaydetmeyi devre dışı bırakın. Şekil, **None** session logging opsyonu seçilerek günlüğe kaydetmenin nasıl devre dışı bırakılacağını gösterir.

Not: Oluşturulan metin dosyası, aygıtın şu anda nasıl yapılandırıldığından kaydı olarak kullanılabilir. Dosya, kaydedilen yapılandırmayı aygıta geri yüklemek için kullanılmadan önce düzenleme gerektirebilir.



# Packet Tracer – İlk Anahtar Ayarlarını Yapılandırır

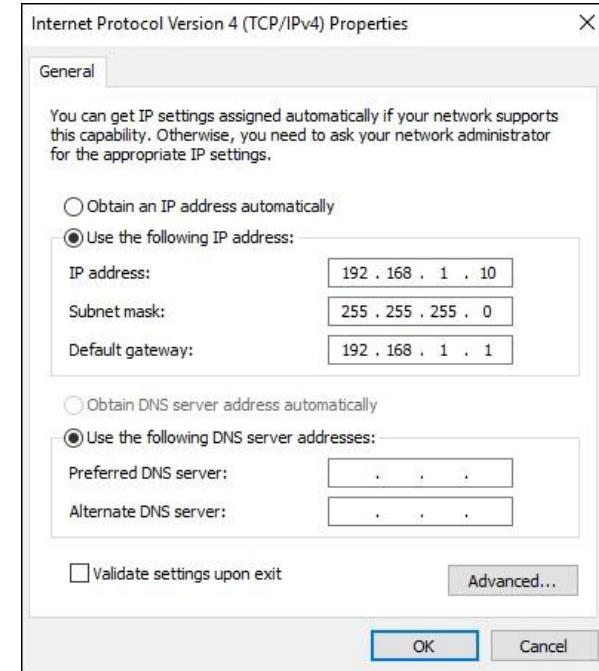
Bu Packet Tracer'da, aşağıdakileri yapacaksınız:

- Default Switch Configuration'ı doğrulayın
- Basit bir Switch Configuration tamamlayın
- MOTD Banner yapılandırın
- Yapılandırma Dosyalarını NVRAM'a Kaydedin
- İkinci bir Anahtarı yapılandırın

# 2.6 Port ve Adresler

# IP Adresleri

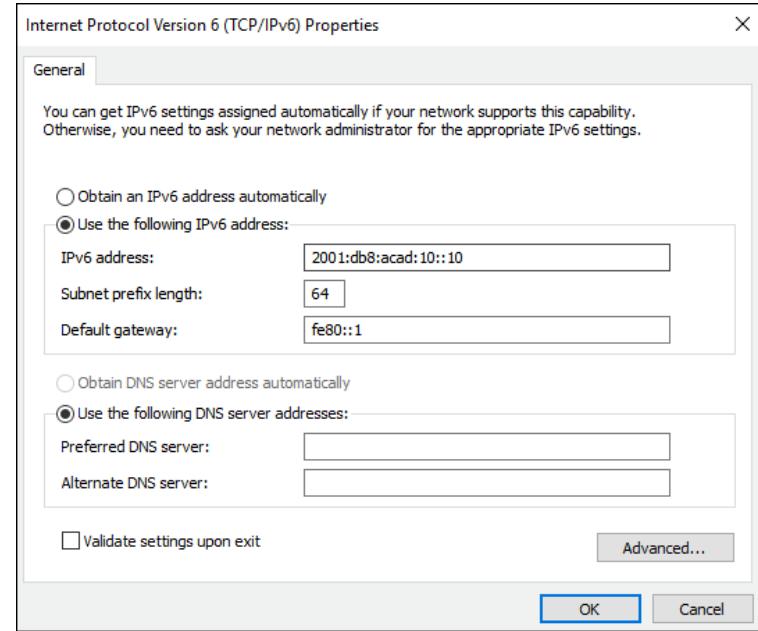
- IP adreslerinin kullanımı, cihazların birbirini bulmasını ve internet üzerinde uçtan uca iletişim kurmasını sağlayanın birincil yöntemdir.
- IPv4 adresinin yapısına noktalı ondalık gösterim denir ve 0 ile 255 arasında dört ondalık sayı ile gösterilir.
- IPv4 subnet mask, adresin network kısmını host kısmından ayıran 32 bitlik değerdir. IPv4 adresi ile birleştirildğinde, subnet mask (alt ağ maskesi) cihazın hangi subnetin üyeli olduğunu belirler.
- Varsayılan gateway adresi, host bilgisayarın internet de dahil olmak üzere uzak ağlara erişim için kullanacağı **router'ın IP adresidir**.



# IP Adresleri (devamı)

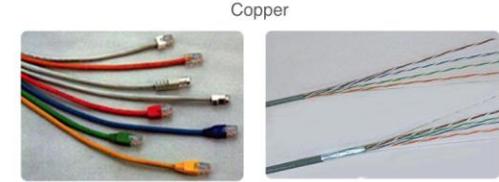
- IPv6 adresleri 128 bit uzunluğundadır ve hexadecimal değerler dizisi olarak yazılır. Toplam 32 hexadecimal değer için, her dört bit tek bir hexadecimal basamakla temsil edilir;. Dört hexadecimal basamak grupları bir kolon ":" ile ayrılır.
- IPv6 adresleri büyük/küçük harfduyarlı değildir ve küçük veya büyük harfle yazılabilir.

**Not:** Bu dersteki IP hem IPv4 hem de IPv6 protokollerini ifade eder. IPv6 IP en son sürümüdür ve daha yaygın olan IPv4'ün yerini alıyor.



# Arayüzler ve Bağlantı Noktaları

- Ağ iletişimini, son kullanıcı aygıtı arabirimlerine, ağ aygıtı arabirimlerine ve bunları bağlayan kablolarla bağlıdır.
- Ağ ortam türleri: bükümlü çift bakır kablolar, fiber optik kablolar, koaksiyel kablolar veya kablosuz.
- Farklı ağ ortam türleri farklı özelliklere ve avantajlara sahiptir. Çeşitli ortam türleri arasındaki farklardan bazıları şunlardır:
  - Medyanın sinyali taşıyabildiği mesafe
  - Medyanın kurulacağı ortam
  - Veri miktarı ve iletilmesi gereken hız
  - Ortam ve kurulum maliyeti



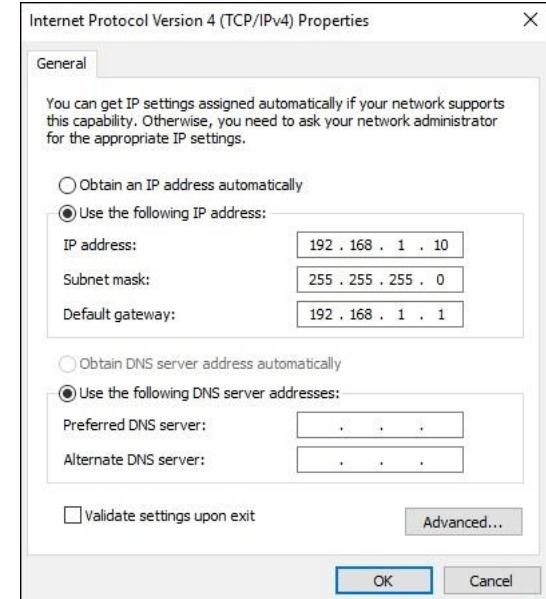
Wireless



# 2.7 IP Adresleme yapılandırması

# Son Aygıtlar için Manuel IP Adresi Yapılandırması

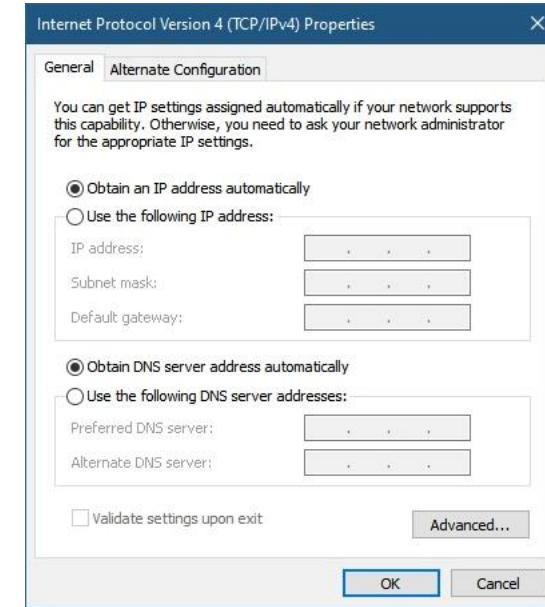
- Aşağıdaki son aygıtlar (end devices), aşağıdaki diğer aygıtlarla iletişim kurmak için bir IP adresine ihtiyaç duyar.
- IPv4 adres bilgileri son aygıtlara manuel olarak veya Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP) kullanılarak otomatik olarak girilebilir.
- Windows PC de bir IPv4 adresini yapılandırmak için kontrol panelden ağ paylaşım merkezini seçip **Control Panel > Network Sharing Center > Change adapter settings**, sonra da adapter ayarlarını seçin. Sonra, sağ tıklayıp özellikleri seçerek Yerel Alan Bağlantı Özelliklerini görüntüleyin; (**Local Area Connection Properties**).
  - Ardından, **Internet Protokolü Sürüm 4 (TCP/IPv4) Özellikleri** penceresini açmak için Özellikleri'ni tıklatın. Ardından IPv4 adresi ve alt ağ maskesi bilgilerini ve varsayılan ağ geçidini yapılandırın.



**Not:** IPv6 adresleme ve yapılandırma seçenekleri IPv4'e benzerdir.

# Son Aygıtlar için Otomatik IP Adresi Yapılandırması

- DHCP, DHCP özellikli her son aygit için otomatik IPv4 adres yapılandırmasını sağlar.
- Son aygıtlar, otomatik IPv4 adres konfigürasyonu için genellikle varsayılan olarak DHCP kullanır.
  - Windows PC'de DHCP yapılandırmak için kontrol panelde Ağ Paylaşım Merkezini açın ve bağıdaştırıcıyı seçin. (To configure DHCP on a Windows PC, open the **Control Panel > Network Sharing Center > Change adapter settings** and choose the adapter.) Sonraki sağ tıklatın ve Yerel Alan Bağlantı Özelliklerini (**Local Area Connection Properties**) görüntülemek için Özellikleri seçin.
  - Ardından, Internet Protokolü Sürüm 4 (TCP/IPv4) Özellikleri penceresini açmak için Özellikleri tıklatın, ardından otomatik olarak IP adresi edinin'i ve DNS sunucu adresini otomatik olarak edinin'i seçin. **Properties → Internet Protocol Version 4 (TCP/IPv4) Properties → Obtain an IP address automatically ve Obtain DNS server address automatically** seçin.



**Not:** IPv6 dinamik adres ayırma için DHCPv6 ve SLAAC (Stateless Address Autoconfiguration) kullanılır.

# Switch Sanal Arayüz Yapılandırması (Virtual Interface Configuration)

Anahtara uzaktan erişmek için, Bir IP adresi ve bir alt ağ maskesi SVI üzerinde yapılandırılmalıdır.

Switch üzerinde SVI yapılandırmak için:

- Global config modda **interface vlan 1** komutunu girin.
- Sonra **ip address ip-address subnet-mask** command kullanarak bir IPv4 adresi ata.
- Son olarak **no shutdown** command komutunu kullanarak sanal arabirimini (virtual interface) etkinleştir.

```
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
```

# Packet Tracer – Temel Bağlantı Uygulaması

Bu Packet Tracer'da, aşağıdakileri yapacaksınız:

- İki anahtarda Temel Yapılandırma gerçekleştirmeye
- PC'leri yapılandırma
- Anahtar Yönetimi Arabirimini Yapılandırma
-

# 2.8 Bağlantı doğrulama

# Video – Arayüz Atamasını Test Edin

Bu video aşağıdakileri kapsayacaktır:

- Bilgisayardan anahtara bir konsol kablosu bağlama
- Terminal emülatör programı kullanın ve sizi komut satırına getirecek varsayılanları kabul edin
- Privileged EXEC moduna girmek için etkinleştirme (enable)
- No shutdown komutunu girmek için global configuration modunu ve interface configuration modunu kullan

## Video – End-to-End Connectivity Test

Bu video, hem anahtarlarla hem de her iki bilgisayarda bağlantı test etmek için ping komutunun kullanımını kapsayacaktır.

# 2.9 Modül Uygulama ve Sınav

# Packet Tracer – Temel Anahtar ve Son Aygit Yapılandırması

Bu Packet Tracer'da, aşağıdakileri yapacaksınız:

- Ana bilgisayar adlarını ve IP adreslerini iki anahtarda yapılandırma
- Cihaz yapılandırmalarına erişimi belirtmek veya sınırlamak için Cisco IOS komutlarını kullanma
- Running configuration'ı kaydetmek için IOS komutlarını kullanın
- IP adresleriyle iki ana bilgisayar aygitını yapılandırın
- İki PC son aygıtı arasındaki bağlantıyı doğrulayın
-

# Lab – Temel Anahtar ve Son Aygıt Yapılandırması

Bu laboratuvara, aşağıdaki hedefleri tamamlayacaksınız:

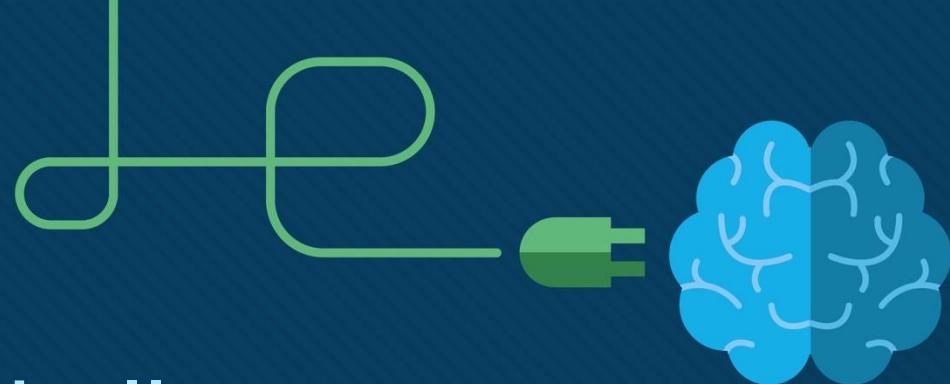
- Ağ Topolojisini Ayarlama
- PC Ana Bilgisayarlarını Yapılandırma
- Temel Anahtar Ayarlarını Yapılandır ve Doğrula
-

# Bu modülde ne öğrendim??

- Tüm son aygıtlar ve ağ aygıtları bir işletim sistemi gerektirir (OS).
- Cisco IOS yazılımı yönetim erişimini aşağıdaki iki komut moduna ayırır: User EXEC Mode ve Privileged EXEC Mode.
- Diğer özel yapılandırma modlarından önce küresel yapılandırma (global configuration) moduna erişilir. Genel config modundan, kullanıcı farklı alt yapılandırma modları girebilir.
- Her IOS komutu belirli bir biçimde veya sözdizimine sahiptir ve yalnızca uygun modda yürütülebilir.
- Temel aygit yapılandırmaları- hostname, password, şifreleri şifrelemek ve banner.
- Aygit yapılandırmasını depolayan iki sistem dosyası vardır: startup-config ve running-config.
- IP adresleri, cihazların birbirini bulmasını ve internet üzerinden ucldan uca iletişim kurmasını sağlar. Ağdaki her son aygit bir IP adresiyle yapılandırılmalıdır.







# Modül 3: Protokoller ve Modeller

Eğitmen Materyalleri

Ağlara Giriş v7.0 (ITN)



# Modül Hedefleri

**Modül Başlığı :** Protokoller ve Modeller

**Modülün Amacı :** Ağ protokollerinin, **cihazların yerel ve uzak ağ kaynaklarına erişmesini nasıl sağladığının açıklanması.**

Konu Başlıkları	Amaç
<b>Kurallar</b>	Başarılı bir şekilde iletişim kurmak için gerekli olan kural türlerini açıklayın.
<b>Protokoller</b>	Ağ iletişiminde protokollerin neden gerekli olduğunu açıklayın.
<b>Protokol Paketleri</b>	Bir protokol paketine bağlı kalmanın amacını açıklayın.
<b>Standart Kuruluşlar</b>	Ağ birlikte çalışabilirliği için protokoller oluşturmada standart kuruluşlarının rolünü açıklayın.
<b>Referans Modelleri</b>	İletişim sürecinde standardizasyonu kolaylaştırmak için TCP / IP modelinin ve OSI modelinin nasıl kullanıldığını açıklayın.
<b>Veri Kapsülleme</b>	Veri kapsüllemenin, verilerin ağ üzerinden taşınmasına nasıl izin verdiği açıklayın.
<b>Veri Erişimi</b>	Yerel ana bilgisayarların bir ağdaki yerel kaynaklara nasıl eriştiğini açıklayın.

# Sınıf Etkinliği– Bir İletişim Sistemi Tasarlayın

## Bir İletişim Sistemi Tasarlama

### Hedefler:

- Ağ iletişiminde birlikte çalışabilirliği kolaylaşdırınmada protokollerin ve standart organizasyonlarının rolünün açıklaması.

# 3.1 Kurallar

# Kurallar

## Video – Baloncuktaki Cihazlar

Bu video, cihazların ağdaki yerlerini görmek ve diğer cihazlarla iletişim kurmak için kullandıkları protokollerı açıklayacaktır.

## İletişimin Temelleri

❑ Ağların boyutu ve karmaşıklığı değişebilir.

Bağlantının olması yeterli değildir.

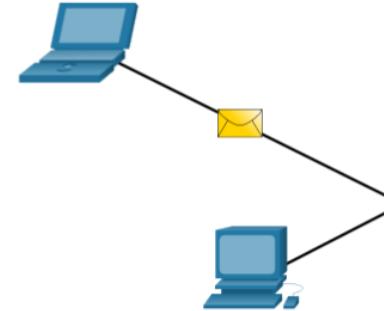
Cihazlar "nasıl" iletişim kuracakları konusunda anlaşmalıdır.

▪ Herhangi bir iletişimün üç unsuru vardır:

- **Bir kaynak (gönderen) olacak.**
- **Bir hedef (alıcı) olacaktır.**
- İletişim yolunun olmasını sağlayan **bir kanal (medya) olacaktır.**

# İletişim Protokollerı

- Tüm iletişim, protokoller tarafından yönetilir.
- Protokoller, iletişimimin izleyeceği kurallardır.
- Bu kurallar protokole bağlı olarak değişecektir.



# Kural Oluşumu

- Bireyler, görüşmeyi yönetmek için **yerleşik kuralları** veya **anlaşmaları** kullanmalıdır.
- İlk mesaj düzgün biçimlendirilmediğinden okunması zordur.
- İkincisi, mesajın doğru biçimlendirildiğini gösterir.

humans communication between govern rules. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. A estrutura da gramatica, da lingua, da pontuacao e do sentence faz a configuracao humana comprehensivel por muitos individuos diferentes.

Rules govern communication between humans. It is very difficult to understand messages that are not correctly formatted and do not follow the established rules and protocols. The structure of the grammar, the language, the punctuation and the sentence make the configuration humanly understandable for many different individuals.

## Kural Oluşumu (Devam)

Protokoller aşağıdaki gereksinimleri hesaba katmalıdır:

- **Tanımlanmış bir gönderen ve alıcı**
- **Ortak dil ve gramer**
- **Teslimatın hızı ve zamanlaması**
- **Onay veya kabul gereksinimleri**

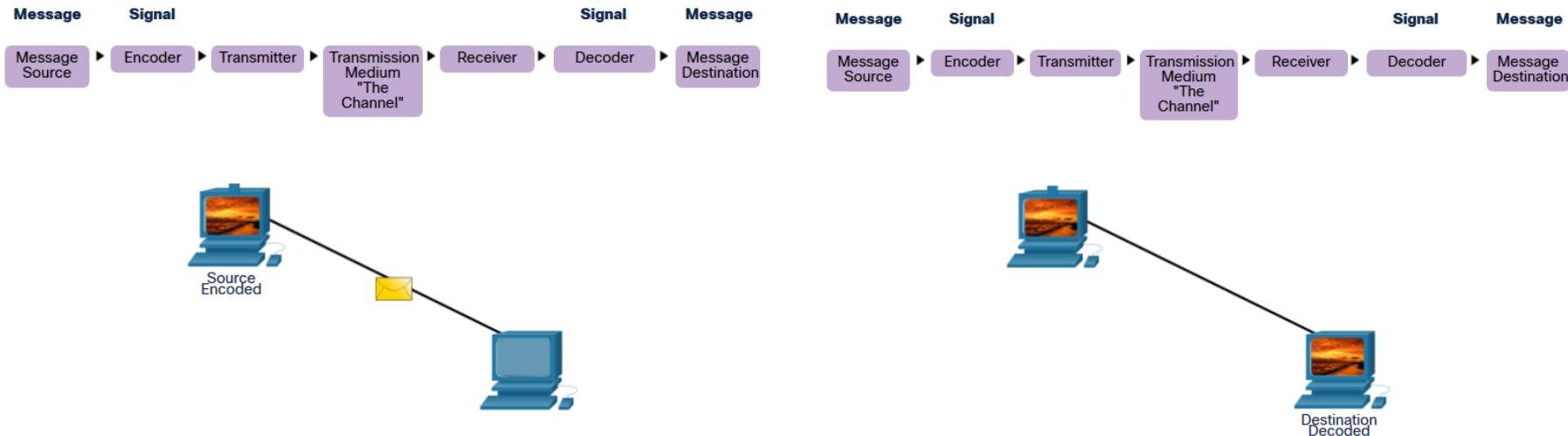
# Ağı Protokol Gereksinimleri

Ortak bilgisayar protokollerini, uyumlu olmalı ve aşağıdaki gereksinimleri içermelidir:

- ❖ Mesaj **kodlama**
- ❖ Mesaj **biçimlendirme** ve **kapsülleme**
- ❖ Mesaj **boyutu**
- ❖ Mesaj **zamanlaması**
- ❖ Mesaj **teslim seçenekleri**

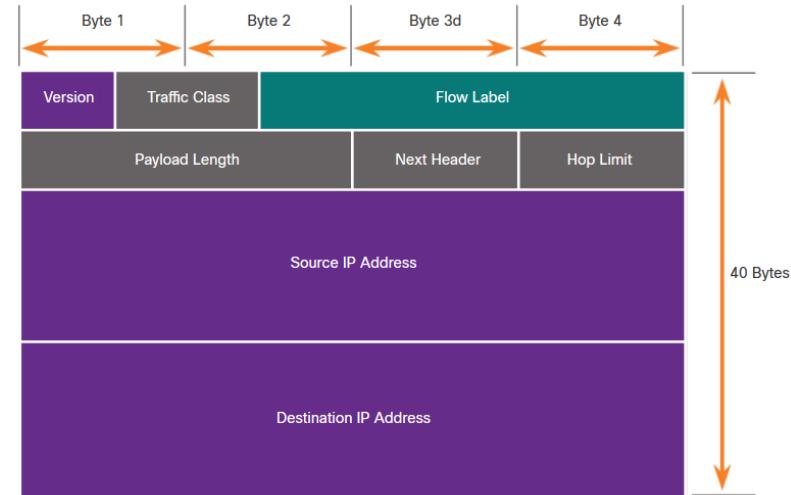
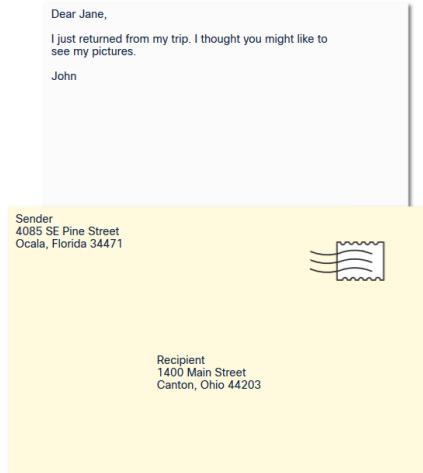
# Mesaj Kodlaması

- **Kodlama**, bilgiyi aktarım için kabul edilebilir başka bir biçimde dönüştürme işlemidir.
- **Kod çözme**, bilgiyi yorumlamak için bu işlemi tersine çevirir.



# Mesajı Biçimlendirme ve Kapsülleme

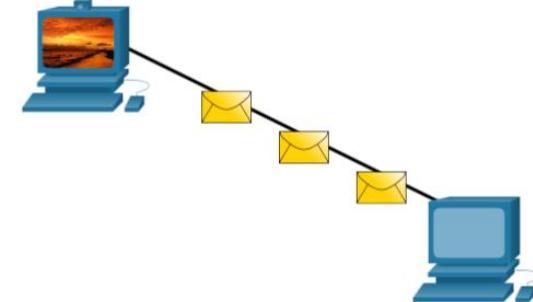
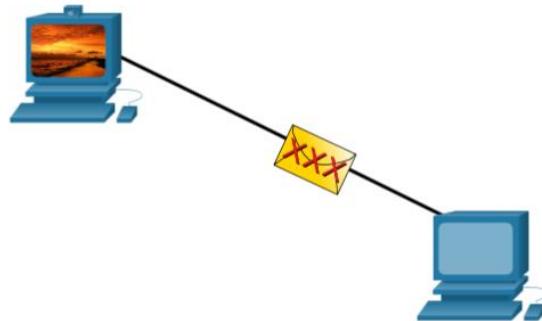
- Bir mesaj gönderildiğinde, belirli bir format veya yapı kullanması gereklidir.
- **Mesaj formatları, mesajın türüne ve mesajı iletmek için kullanılan kanala bağlıdır.**



# Mesaj Boyutu

Ana bilgisayarlar arasındaki kodlama, **ortama uygun bir formatta olmalıdır.**

- Ağ üzerinden gönderilen mesajlar bitlere dönüştürülür.
- Bitler bir ışık, ses veya elektriksel dürtü modeline kodlanır.
- Hedef ana bilgisayar, mesajı yorumlamak için sinyallerin kodunu çözmeli dir.



# Mesaj Zamanlaması

Mesaj zamanlaması şunları içerir:

**Akış Kontrolü** - Veri aktarım oranını yönetir ve ne kadar bilginin gönderilebileceğini ve iletilebileceği hızı tanımlar.

**Yanıt Zaman Aşımı** - Bir aygıtın hedeften bir yanıt almaması durumunda ne kadar bekleyeceğini yönetir.

**Erişim yöntemi** - Birinin ne zaman mesaj gönderebileceğini belirler.

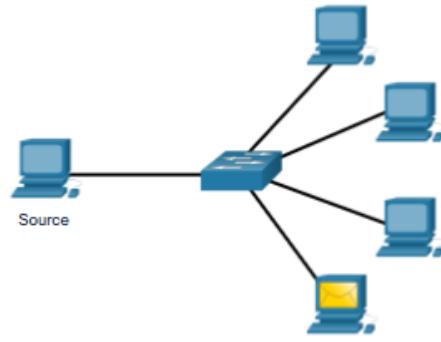
- "Çarpışmalar" gibi konuları yöneten çeşitli kurallar olabilir. Bu, birden fazla cihazın aynı anda trafik gönderdiği ve mesajların bozulduğu zamanıdır.
- Bazı protokoller **proaktiftir** ve çarşışmaları önlemeye çalışır.
- Diğer protokoller **reaktiftir** ve çarşışma meydana geldikten sonra bir kurtarma yöntemi oluşturur.

## Mesaj Gönderme Seçenekleri

İleti teslimi aşağıdaki yöntemlerden biri olabilir:

- **Unicast** - bire bir iletişim
  - **Mutlicast**- birden çoğa , genellikle hepsine değil
  - **Broadcast** - hepsine
- **Not: Yayınlar IPv4 ağlarında kullanılır**, ancak IPv6 için bir seçenek değildir. Daha sonra IPv6 için ek bir teslimat seçeneği olarak "**Anycast**" i de göreceğiz.

# Mesaj Gönderme Seçenekleri



Unicast

Multicast

Broadcast

Unicast

Source

Source



Multicast

Broadcast

Source

Unicast

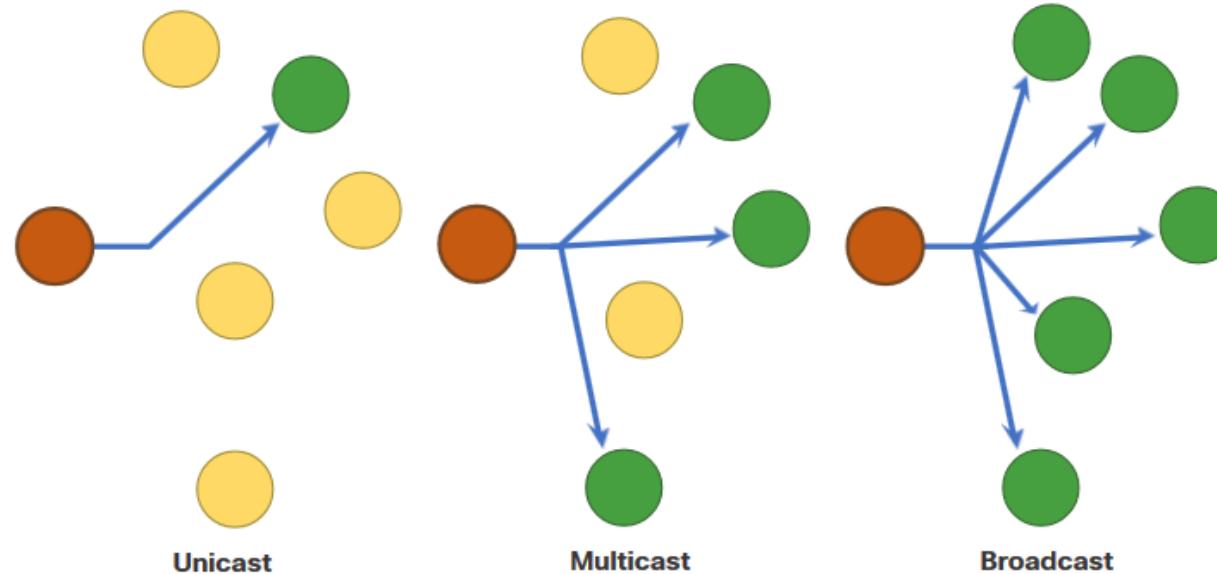
Multicast

Broadcast



# Düğüm Simgesi Hakkında Bir Not

- **Belgeler**, tüm aygıtları temsil etmek için **tipik olarak bir daire olan düğüm simgesini kullanabilir.**
- **Şekil**, dağıtım seçenekleri için düğüm simgesinin kullanımını göstermektedir.



# 3.2 Protokoller

# Ağ Protokollerine Genel Bakış

Ağ protokolleri, ortak bir kurallar kümesini tanımlar.

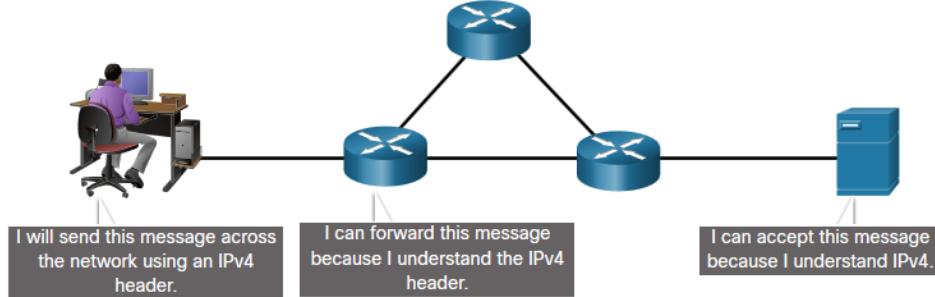
- Aşağıdaki cihazlarda uygulanabilir:
  - **Yazılım**
  - **Donanım**
  - **Her ikisi de**
- Protokollerin kendine ait:
  - **Fonksiyon**
  - **Biçim**
  - **Kurallar**

# Ağ Protokollerine Genel Bakış

Protokol Tipi	Açıklama
❖ Ağ İletişimi	<b>İki veya daha fazla cihazın bir veya daha fazla ağ üzerinden iletişim kurmasını sağlayın</b>
❖ Ağ güvenliği	<b>Kimlik doğrulama, veri bütünlüğü ve veri şifreleme sağlamak için verileri güvenli hale getirin</b>
❖ Yönlendirme	<b>Yönlendiricilerin rota bilgilerini değişim tokus etmesini, yol bilgilerini karşılaştırmasını ve en iyi yolu seçmesini sağlayın</b>
❖ Servis Keşfi	<b>Cihazların veya hizmetlerin otomatik olarak algılanması için kullanılır</b>

# Ağ Protokol İşlevleri

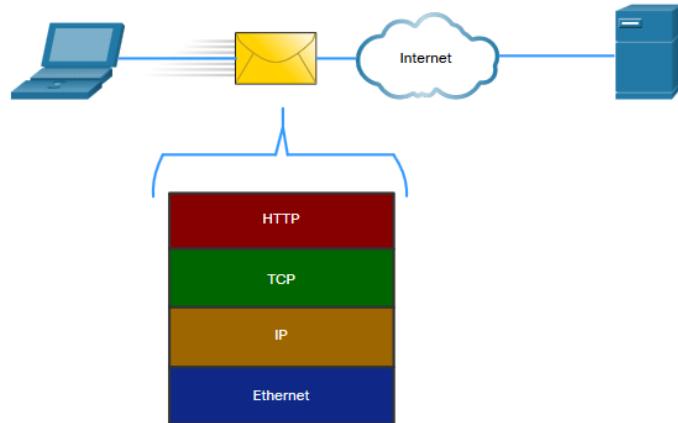
- Cihazlar, iletişim kurmak için üzerinde anlaşılan protokollerini kullanır.
- Protokollerin bir veya işlevleri olabilir.



Function	Description
Adresleme	Göndereni ve <b>alıcıyı tanımlar</b>
Güvenilirlik	<b>Garantili teslimat sağlar</b>
Akış kontrolü	Verimli bir hızda <b>veri akışını sağlar</b>
Sıralama	İletilen her veri segmentini <b>benzersiz şekilde etiketler</b>
Hata Tespiti	Verilerin <b>aktarım sırasında bozulup bozulmadığını</b> belirler

# Protokol Etkileşimi

- Ağlar birkaç protokolün kullanılmasını gerektirir.
- Her protokolün kendi işlevi ve biçimini vardır.



Protocol	Function
Hypertext Transfer Protocol (HTTP)	<ul style="list-style-type: none"> <li>Bir web sunucusu ile bir web istemcisinin etkileşim şeklini yönetir</li> <li>İçeriği ve biçimini tanımlar</li> </ul>
Transmission Control Protocol (TCP)	<ul style="list-style-type: none"> <li>Bireysel görüşmeleri yönetir</li> <li>Garantili teslimat sağlar</li> <li>Akiş kontrolünü yönetir</li> </ul>
Internet Protocol (IP)	Mesajları gönderenden alıcıya global olarak iletir
Ethernet	Aynı <b>Ethernet Yerel Alan Ağrı (LAN)</b> üzerindeki bir NIC (Network Interface Card) 'den başka bir NIC'ye mesajlar iletir

# 3.3 Protokol Paketleri

## Ağ Protokol Paketleri

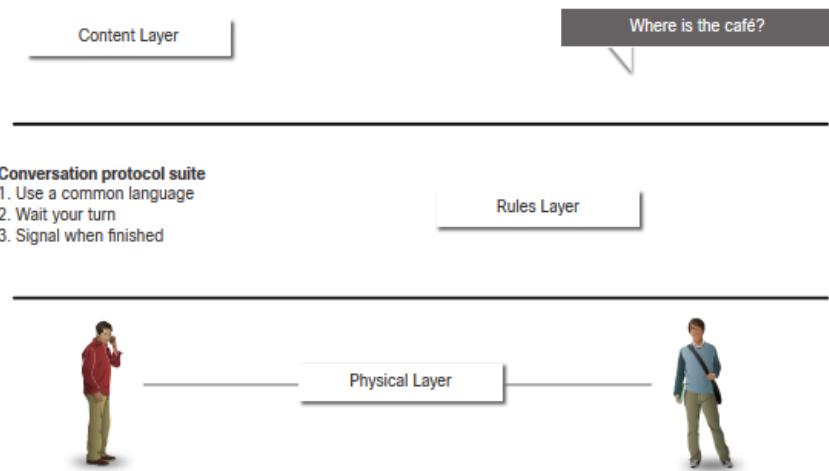
Protokoller diğer protokollerle çalışabilmelidir.

### Protokol Suiti:

- Bir iletişim işlevini gerçekleştirmek için gerekli olan birbiriyle ilişkili bir grup protokol
- Bir sorunu çözmeye yardımcı olmak için birlikte çalışan kurallar dizisidir.

### Protokoller, katmanlar açısından incelenir:

- Daha Yüksek Katmanlar
- Alt Katmanlar - verilerin taşınmasıyla ilgilidir ve üst katmanlara hizmet sağlar.



Protocol suites are sets of rules that work together to help solve a problem.

# Protokol Takımlarının Evrimi

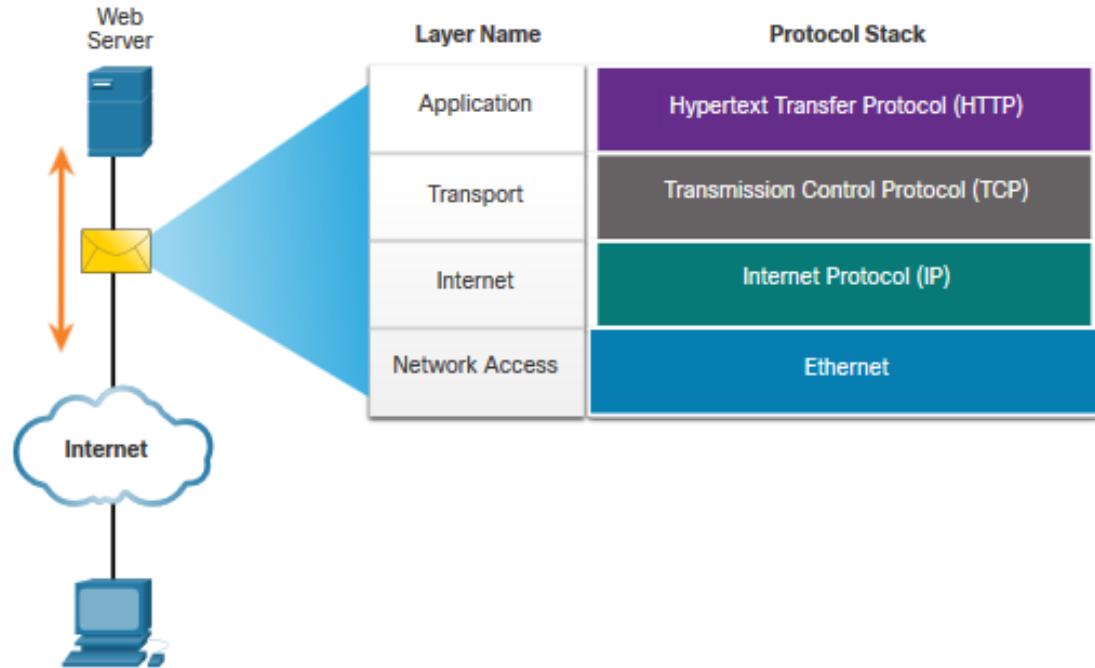
Birkaç protokol paketi vardır.

- Internet Protokol Paketi veya TCP / IP -** En yaygın protokol paketi ve İnternet Mühendisliği Görev Gücü (IETF) tarafından korunur
- Açık Sistemler Bağlantısı (OSI) protocols-** geliştirilen Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Telekomünikasyon Birliği (ITU) tarafından
- AppleTalk -** Apple Inc. tarafından tescilli paket sürümü
- Novell NetWare -** Novell Inc. tarafından geliştirilen tescilli paket.

TCP/IP Layer Name	TCP/IP	ISO	AppleTalk	Novell Netware
Application	HTTP DNS DHCP FTP	ACSE ROSE TRSE SESE	AFP	NDS
Transport	TCP UDP	TP0 TP1 TP2 TP3 TP4	ATP AEP NBP RTMP	SPX
Internet	IPv4 IPv6 ICMPv4 ICMPv6	CONP/CMNS CLNP/CLNS	AARP	IPX
Network Access		Ethernet ARP WLAN		

# TCP/IP Protokol Örnekleri

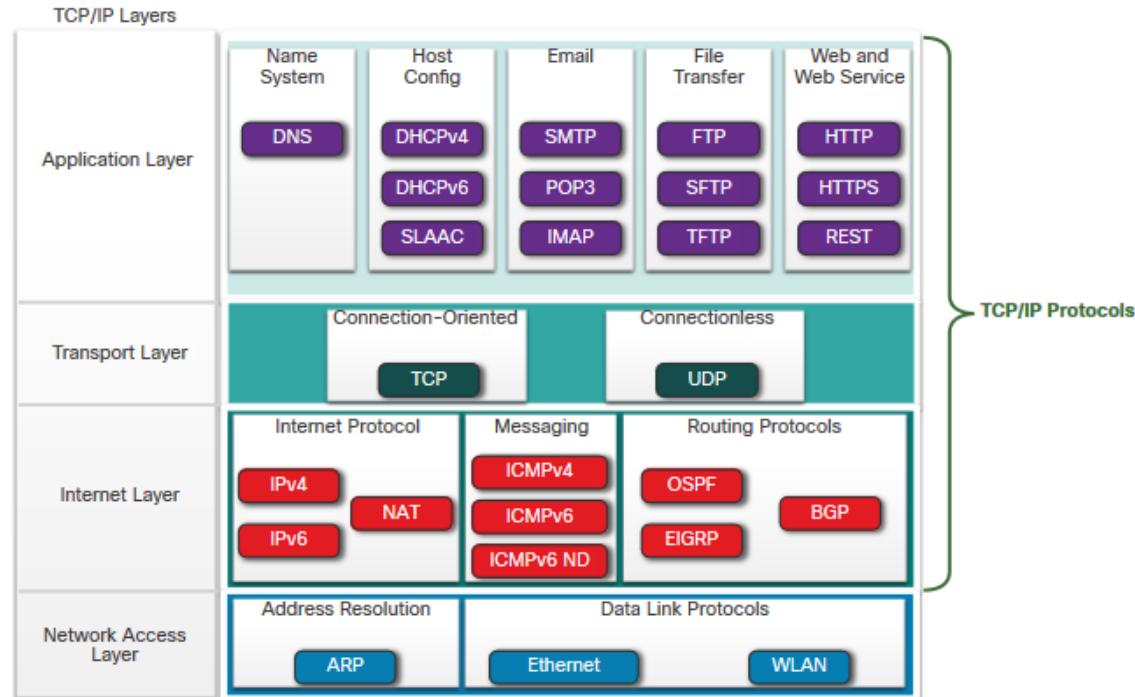
- TCP / IP protokollerinin **uygulama, aktarım ve internet katmanlarında** çalışır.
- En yaygın **ağ erişim katmanı LAN** protokollerini Ethernet ve **WLAN'dır** (kablosuz LAN).



# Protokol Paketleri

## TCP/IP Protokol Paketleri

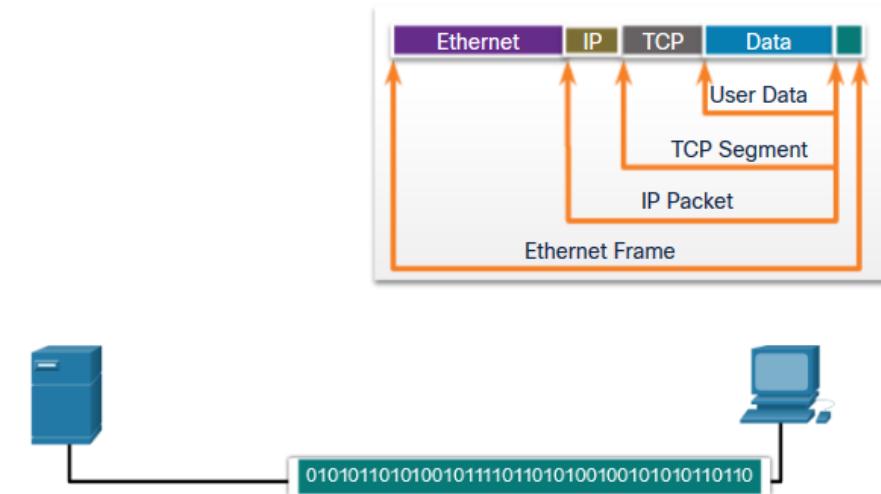
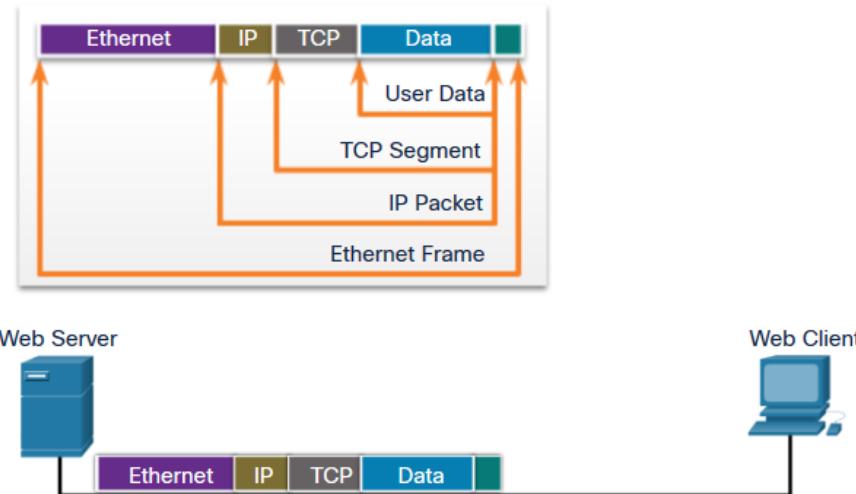
- TCP / IP, internet tarafından kullanılan protokol paketidir ve birçok protokol içerir.
- TCP / IP:
  - Herkese ücretsiz olarak sunulan ve herhangi bir satıcı tarafından kullanılabilen açık standart bir protokol paketi
  - Ağ endüstrisi tarafından onaylanan ve birlikte çalışabilirliği sağlamak için bir standart organizasyon tarafından onaylanan standartlara dayalı bir protokol paketi



## TCP/IP İletişim Süreci

❖ Bir web sayfasını **kapsülleyen** ve **istemciye** gönderen bir web sunucusu.

❖ Web tarayıcısı için web sayfasının **kapsülünü** **çözen** bir **istemci**



# 3.4 Standart Organizasyonları

# Standart Organizasyonları Açık Standartlar



## Açık standartlar şunları teşvik eder:

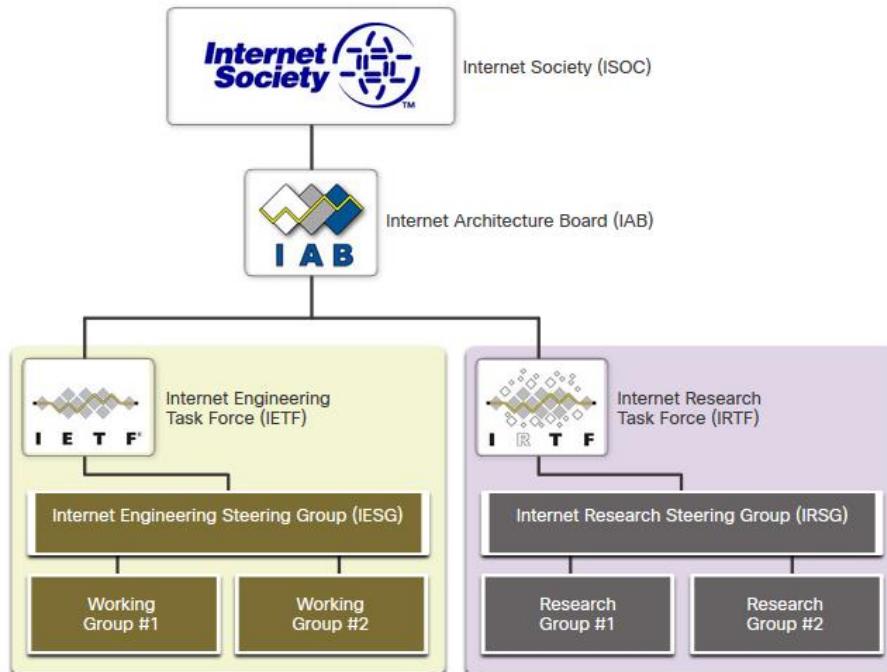
- Birlikte çalışabilirlik
- Rekabet
- Yenilik

## Standart organizasyonlar:

- Satıcıdan bağımsız
- Kar amacı gütmeyen kuruluşlar
- Açık standartlar kavramını geliştirmek ve desteklemek için kurulmuştur.

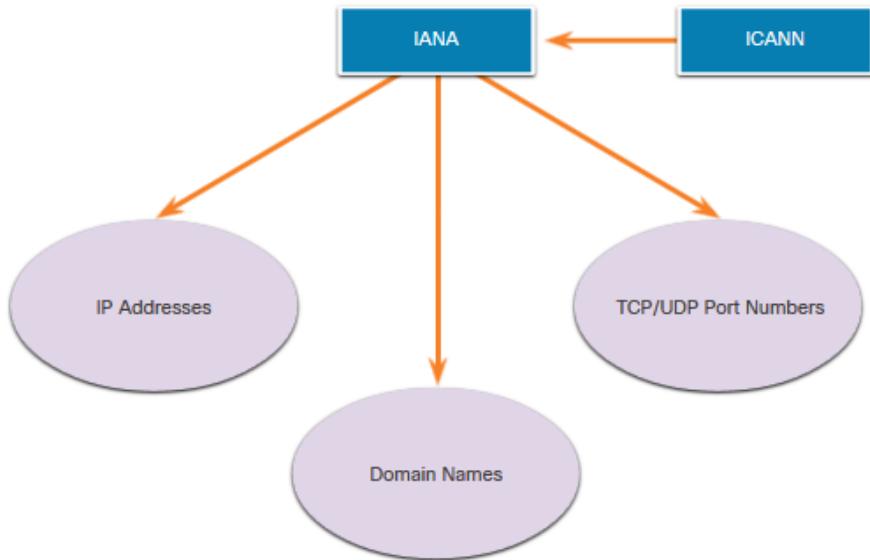
# Standart Organizasyonları

## Internet Standartları



- **Internet Society (ISOC)** İnternetin açık gelişimini ve evrimini destekler
- **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 protokollerini ile ilgili uzun vadeli araştırmalara odaklandır

# Internet Standardları (Cont.)



TCP / IP'nin geliştirilmesi ve desteklenmesiyle ilgili standart organizasyonlar

- **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

# Elektronik ve İletişim Standartları

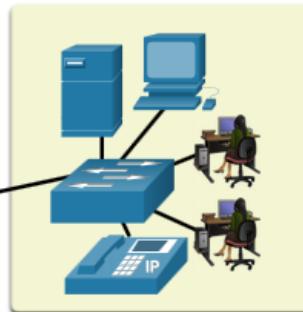
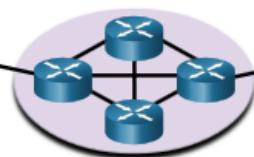
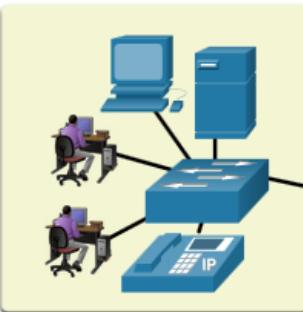
- **Institute of Electrical and Electronics Engineers (IEEE)** ( IEEE , "I-üçlü-E" olarak telaffuz edilir) - **güç ve enerji, sağlık hizmetleri, telekomünikasyon ve ağ oluşturma** konularında standartlar oluşturmaya adanmıştır
- **Electronic Industries Alliance (EIA)** - **elektrik kabloları, konektörler ve ağ ekipmanını monte etmek** için kullanılan 19 inçlik raflarla ilgili standartları geliştirir
- **Telecommunications Industry Association (TIA)** - **radyo ekipmanı, hücresel kuleler, IP üzerinden Ses (VoIP) cihazları, uydu iletişimleri 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

# Lab – Ağ Standartlarını Araştırma

- **Bu laboratuvara aşağıdakileri yapacaksınız:**
  - Bölüm 1: Araştırma Ağı Standartları Kuruluşları
  - Bölüm 2: İnternet ve Bilgisayar Ağı Deneyimi Üzerine Düşünme
-

# 3.5 Referans Modeller

# Katmanlı Model Kullanmanın Yararları



OSI Model	TCP/IP Protocol Suite	TCP/IP Model
Application		Application
Presentation	HTTP, DNS, DHCP, FTP	
Session		
Transport	TCP, UDP	Transport
Network	IPv4, IPv6, ICMPv4, ICMPv6	Internet
Data Link	Ethernet, WLAN, SONET, SDH	Network Access
Physical		

- ❖ Bir ağın nasıl çalıştığı gibi karmaşık kavramların açıklanması ve anlaşılması zor olabilir.
- ❖ Bu nedenle katmanlı bir model kullanılmaktadır.

İki katmanlı model, ağ işlemlerini tanımlar:

- Açık Sistem Ara Bağlantısı (OSI) Referans Modeli
- TCP / IP Referans Modeli

# Katmanlı Model Kullanmanın Yararları

**Katmanlı bir model kullanmanın avantajları şunlardır:**

- Protokol tasarımına yardımcı olur, çünkü belirli bir katmanda çalışan protokoller, etki ettiğleri tanımlanmış bilgilere ve üst ve alt katmanlara tanımlı bir arayüze sahiptir.
- Farklı tedarikçilerin ürünleri birlikte çalışabildiği için rekabeti teşvik edin
- Bir katmandaki teknoloji veya yetenek değişikliklerinin yukarıdaki ve alttaki diğer katmanları etkilemesini öner.
- Ağ işlevlerini ve yeteneklerini açıklamak için ortak bir dil sağlar.

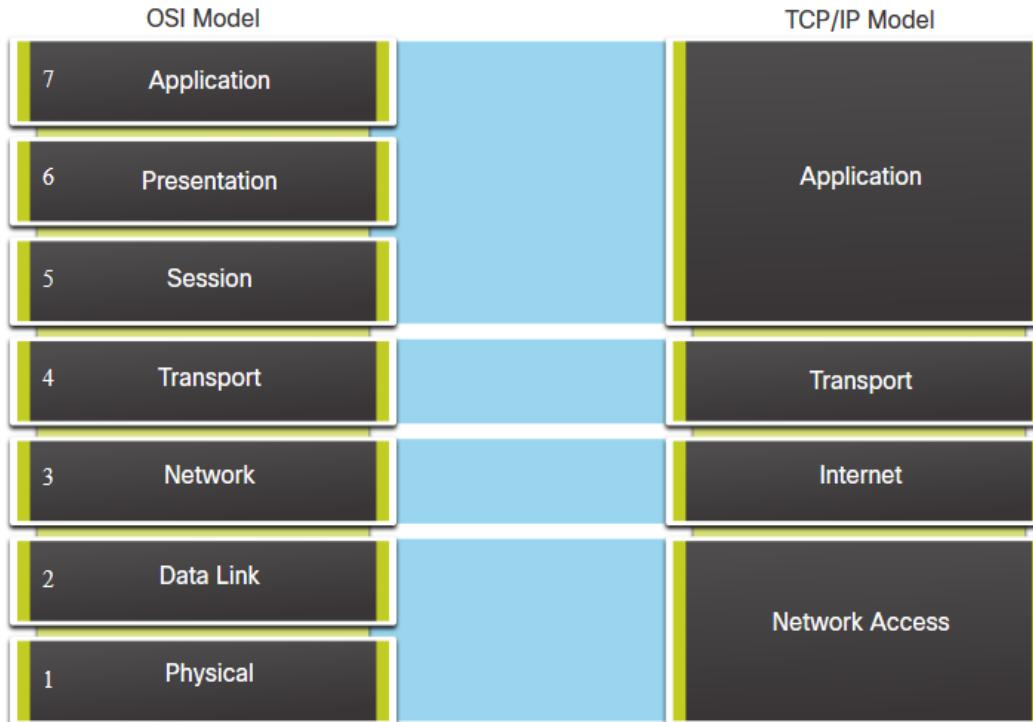
# OSI Referans Model

OSI Model Katmanları	Açıklama
<b>7 - Application</b>	Proses-proses iletişimleri için kullanılan protokollerini içerir.
<b>6 - Presentation</b>	Uygulama katmanı hizmetleri arasında aktarılan verilerin ortak temsiliğini sağlar.
<b>5 - Session</b>	Sunum katmanına ve veri alışverişini yönetmeye yönelik hizmetler sağlar.
<b>4 - Transport</b>	Bireysel iletişimler için verileri böümlere ayırmak, aktarmak ve yeniden birleştirmek için hizmetleri tanımlar.
<b>3 - Network</b>	Ağ üzerinden bireysel veri parçalarının alışverişi için hizmetler sağlar.
<b>2 - Data Link</b>	Veri çerçevelerini ortak bir ortam üzerinden değişim tokusu etme yöntemlerini açıklar.
<b>1 - Physical</b>	Fiziksel bağlantıları etkinleştirme, sürdürme ve devre dışı bırakma araçlarını açıklar.

# The TCP/IP Referans Model

TCP/IP Model Katmanları	Açıklama
<b>Application</b>	Kullanıcıya veriyi, ayrıca kodlamayı ve iletişim kutusu denetimini temsil eder.
<b>Transport</b>	Farklı ağlarda çeşitli cihazlar arasında iletişimini destekler.
<b>Internet</b>	Ağdaki en iyi yolu belirler.
<b>Network Access</b>	Ağı oluşturan donanım aygıtlarını ve medyayı kontrol eder.

# OSI ve TCP/IP Modellerinin Karşılaştırılması



- OSI modeli, TCP / IP modelinin **ağ erişim katmanını** ve **uygulama katmanını** birden çok katmana böler.
- TCP / IP protokol paketi, **fiziksel bir ortam** üzerinden iletim yaparken hangi protokollerin kullanılacağını belirlemeyez.
- OSI Katman **1 ve 2**, ortama erişmek için gerekli prosedürleri ve bir ağ üzerinden veri göndermek için fiziksel araçları tartışır.

## Packet Tracer –TCP/IP ve OSI Modellerini İnceleme

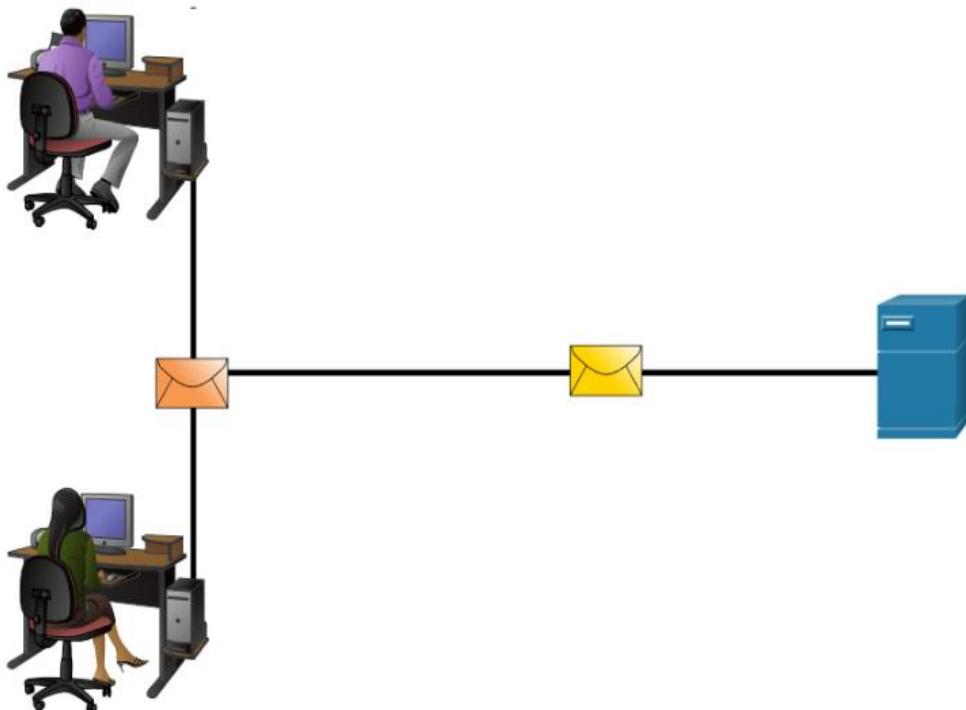
Bu simülasyon etkinliği, TCP / IP protokol paketini ve OSI modeliyle ilişkisiyi anlamak için bir temel sağlamayı amaçlamaktadır. Simülasyon modu, her katmanda ağ üzerinden gönderilen veri içeriklerini görüntülemenizi sağlar.

Bu Packet Tracer'da şunları yapacaksınız:

- Bölüm 1: HTTP Web Trafiğini İnceleyin
- Bölüm 2: TCP / IP Protokol Paketinin Görüntü Öğeleri

# 3.6 Veri Kapsülleme

# Bölümleme Mesajları

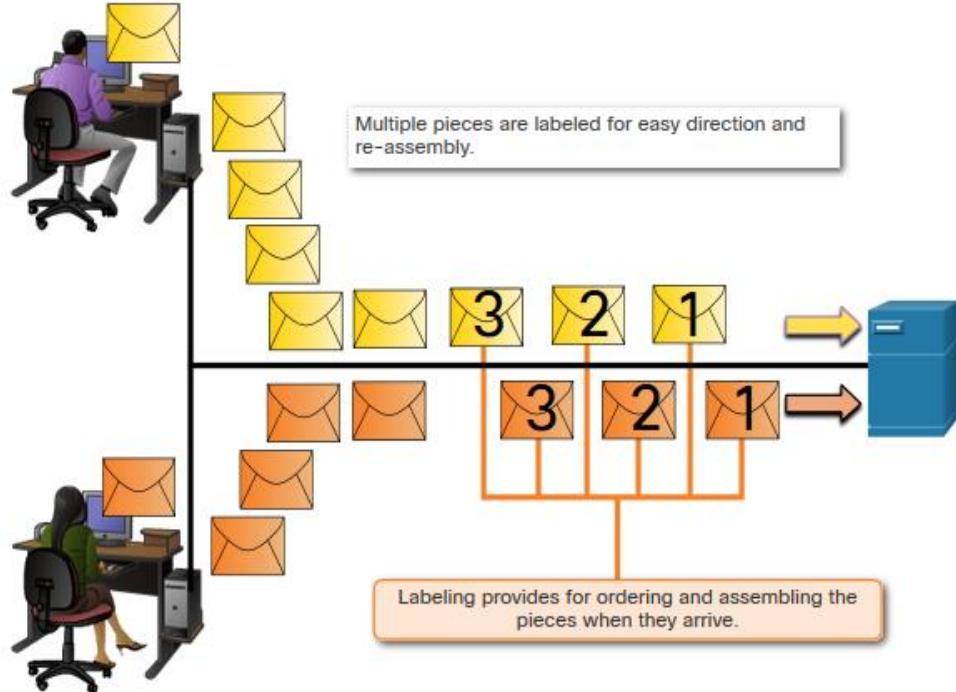


- ❖ **Bölümleme**, mesajları daha küçük birimlere ayırma işlemidir.
- ❖ **Çoklama**, birden fazla bölümlenmiş veri akışını alıp bunları bir araya getirme işlemidir.

Mesajları segmentlere ayırmadanın iki temel faydası vardır:

- **Hızı artırır** - Bir iletişim bağlantısı bağlamadan ağ üzerinden büyük miktarda veri gönderilebilir.
- **Verimliliği artırır** - Tüm veri akışının değil, yalnızca hedefe ulaşamayan segmentlerin yeniden iletilmesi gereklidir.

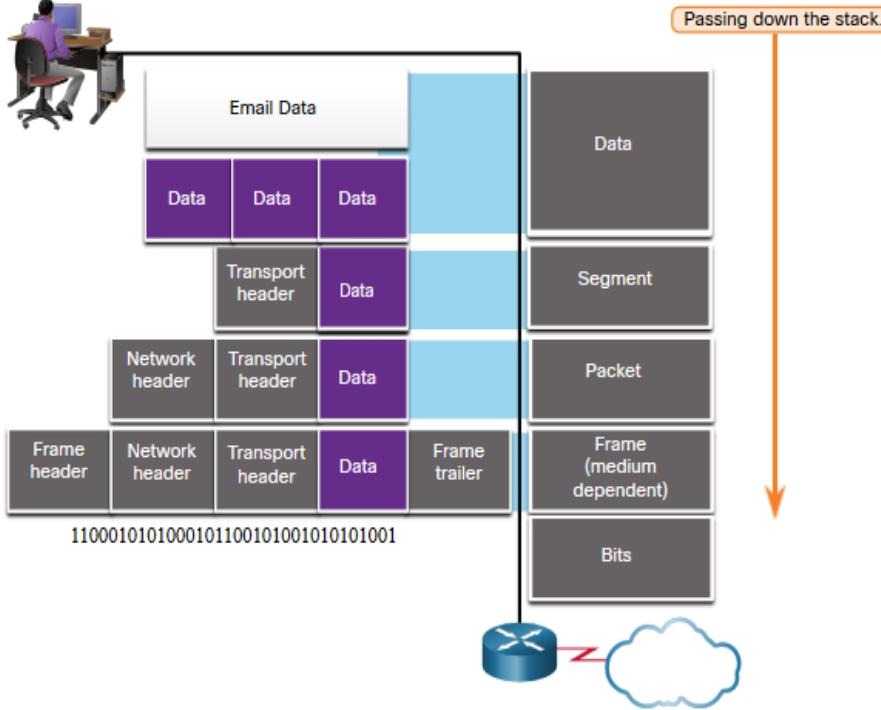
# Veri Kapsülleme Sıralaması



- ❖ Mesajların sıralanması, mesajın hedefte yeniden birleştirilebilmesi için segmentlerin **numaralandırılması işlemidir.**
- ❖ TCP, bireysel segmentlerin sıralanmasından sorumludur.

# Veri Kapsülleme

## Veri Birimleri Protokolü

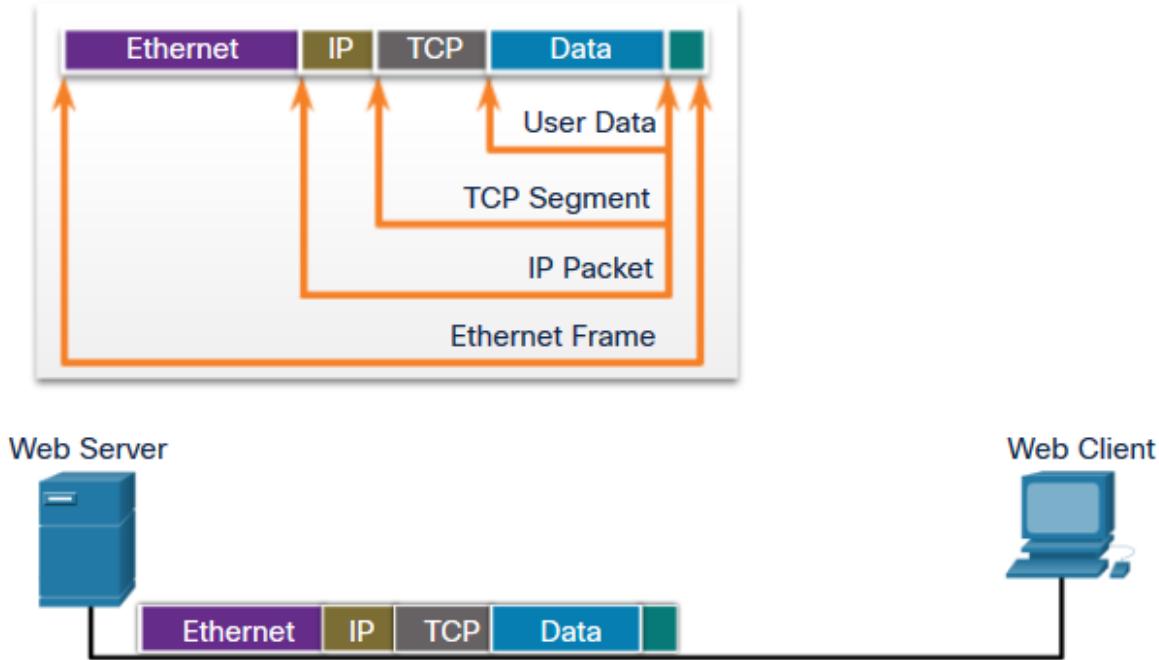


❖ **Kapsülleme**, protokollerin bilgilerini verilere eklediği süreçtir.

- Sürecin her aşamasında, bir **PDU (Protocol Data Unit)** 'nın yeni işlevlerini yansıması için farklı bir adı vardır.
- PDU'lar için evrensel bir adlandırma kuralı yoktur.
- Bu derste kursta PDU'lar TCP / IP paketinin protokollerine göre adlandırılır.
- Yiğindan geçen PDU'lar aşağıdaki gibidir:
  - Veri (Veri Akışı)
  - Bölüm
  - Paket
  - Çerçeve
  - Bitler (Bit Akışı)

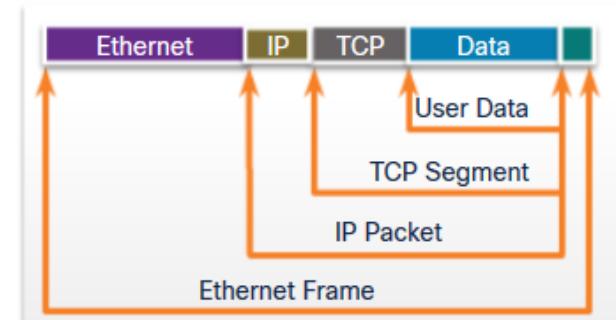
# Kapsülleme Örneği

- **Kapsülleme, yukarıdan aşağıya bir süreçtir.**
- **Yukarıdaki düzey, sürecini gerçekleştirir ve ardından onu modelin bir sonraki düzeyine geçirir.**
- Bu işlem, **bit akışı olarak gönderilene kadar her katman tarafından tekrarlanır.**



# Kapsülü Açıma Örneği

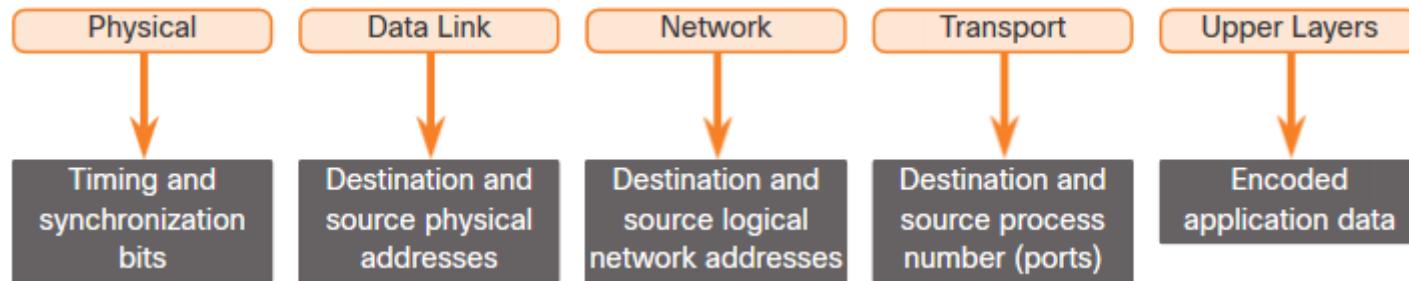
- Veri **yığında yukarı doğru, ilerlerken kapsüller kaldırılır.**
- Bir katman işlemini tamamladığında, bu katman başlığını çıkarır ve işlenmek üzere bir sonraki düzeye geçirir.
- Bu, uygulamanın işleyebileceği bir veri akışı olana kadar her katmanda tekrarlanır.
  - Bit Olarak Alındı (Bit Akışı)
  - Çerçeve
  - Paket
  - Bölüm
  -  Cisco
  - Veri (Veri Akışı)



# 3.7 Veri Erişimi

# Adresler

- ❖ Hem **veri bağlantısı** hem de **ağ katmanları**, kaynaktan hedefe veri iletmek için adreslemeyi kullanır.
- ❖ **Ağ katmanı kaynak ve hedef adresleri** - IP paketini orijinal kaynaktan nihai hedefe teslim etmekten sorumludur.
- ❖ **Veri bağlantı katmanı kaynağı ve hedef adresleri** - Veri bağlantı çerçevesini bir ağ arabirim kartından (NIC) aynı ağdaki başka bir NIC'ye iletmekten sorumludur.

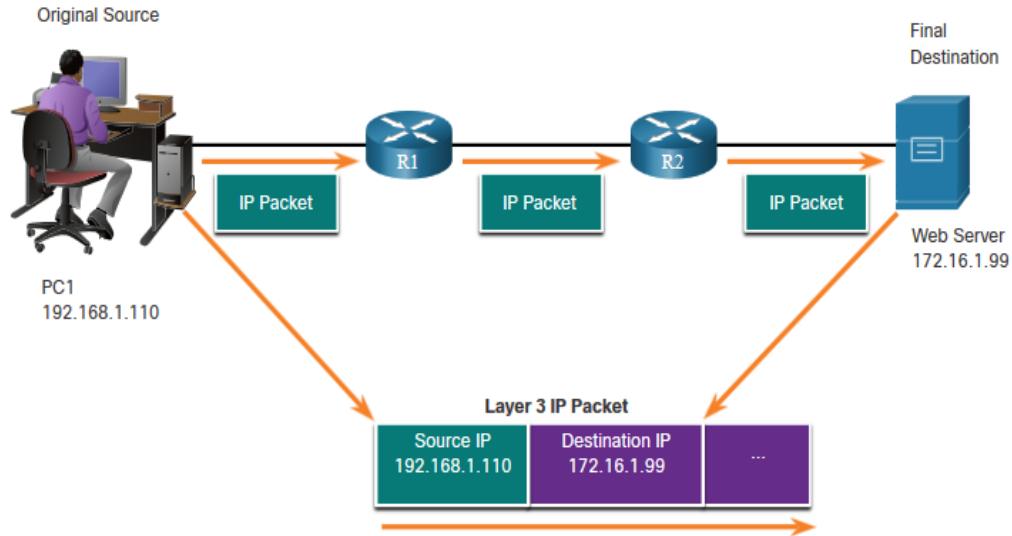


# Layer 3 Mantıksal Adresler

IP paketi iki IP adresi içerir:

- **Kaynak IP adresi** - Gönderen aygıtın IP adresi, paketin orijinal kaynağı.
- **Hedef IP adresi** - Alıcı cihazın IP adresi, paketin son hedefi.

Bu adresler aynı bağlantıda veya uzak olabilir.



# Layer 3 Mantıksal Adresler

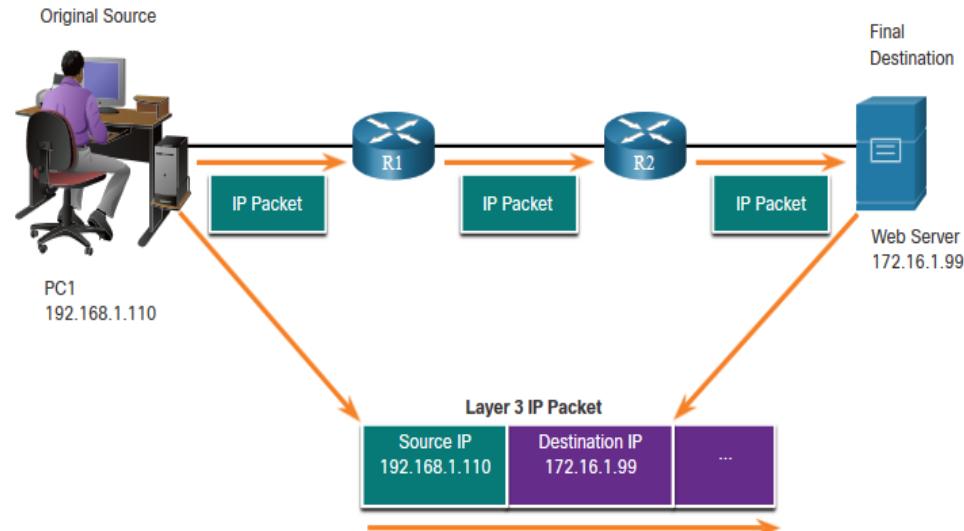
Bir IP adresi iki bölümden oluşur:

## Ağ bölümü (IPv4) veya Önek (IPv6)

- **Adresin en sol kısmı, IP adresinin üye olduğu ağ grubunu gösterir.**
- **Her LAN veya WAN aynı ağ kısmına sahip olacaktır.**

## Ana bilgisayar bölümü (IPv4) veya Arabirim Kimliği (IPv6)

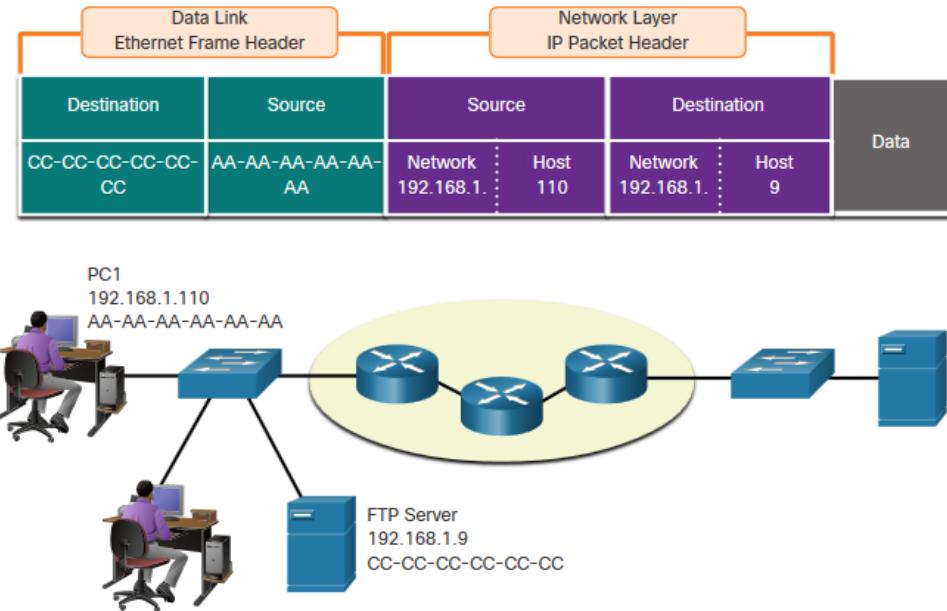
- **Adresin geri kalan kısmı, grup içindeki belirli bir cihazı tanımlar.**
- Bu bölüm, ağdaki her cihaz için benzersizdir.



# Aynı Ağdaki Cihazlar

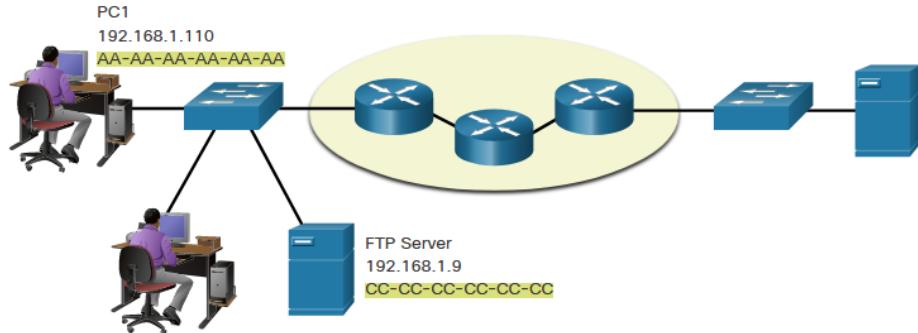
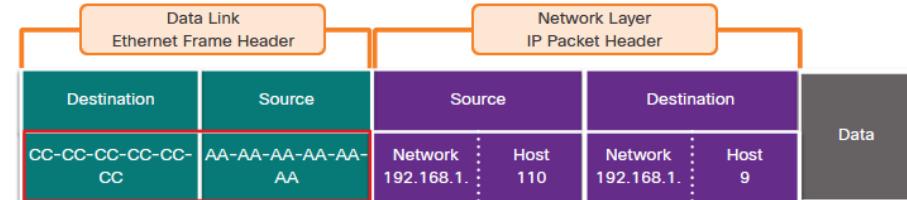
- Cihazlar aynı ağ üzerinde olduğunda, kaynak ve hedef, adresin ağ kısmında aynı numaraya sahip olacaktır.

- PC1 - 192.168.1.110
- FTP Sunucusu - 192.168.1.9



# Data Link Layer Adreslerinin Rolü : Aynı IP Ağı

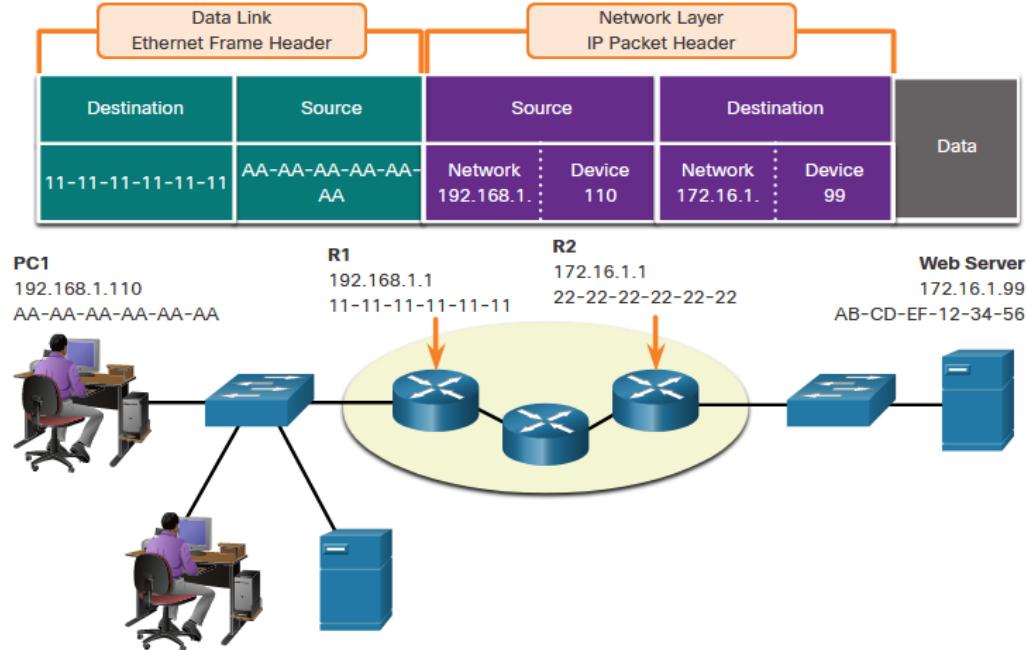
- ❖ Aygıtlar aynı Ethernet ağında olduğunda, veri bağlantı çerçevesi hedef NIC'nin gerçek MAC adresini kullanacaktır.
- ❖ MAC adresleri *fiziksel* olarak Ethernet NIC'ye gömülüdür ve yerel adreslemedir.
  - **Kaynak MAC adresi**, bağlantıdaki oluşturulanın adresi olacaktır.
  - **Hedef MAC adresi**, nihai hedef uzak olsa bile her zaman kaynakla aynı bağlantıda olacaktır.



## Veri Erişimi

# Uzak Ağlardaki Cihazlar

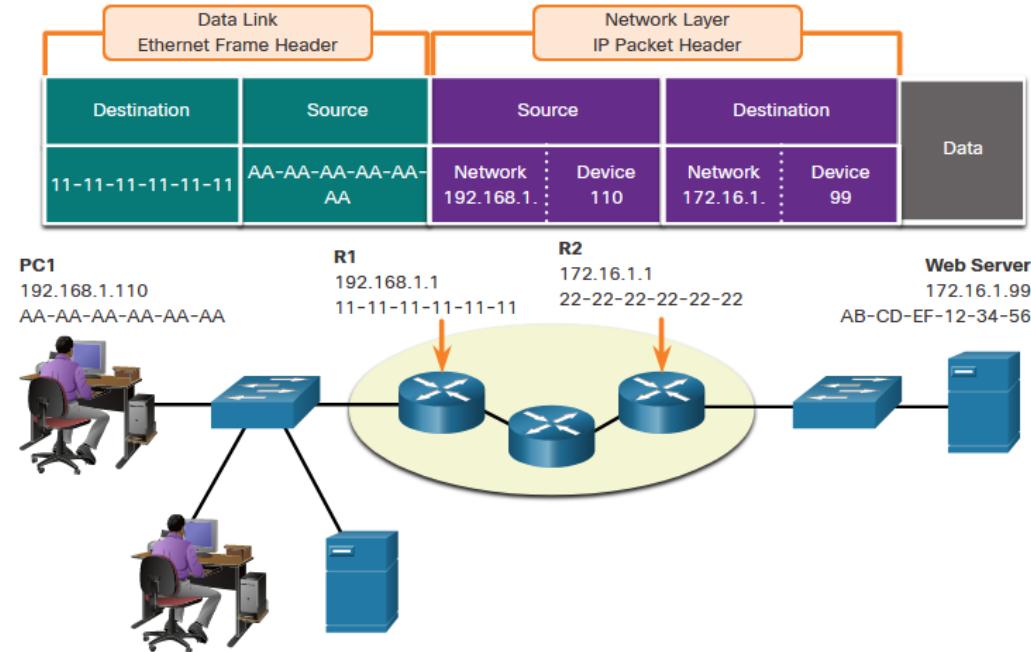
- Gerçek (nihai) hedef aynı LAN üzerinde olmadığında ve uzak olduğunda ne olur?
- PC1 Web Sunucusuna ulaşmaya çalıştığında ne olur?
- Bu, ağ ve veri bağlantısı katmanlarını etkiler mi?



# Ağ katmanı Adreslerinin Rolü

❖ **Kaynak** ve **hedef** farklı bir ağ kismına sahip olduğunda, **bu farklı ağlarda oldukları anlamına gelir.**

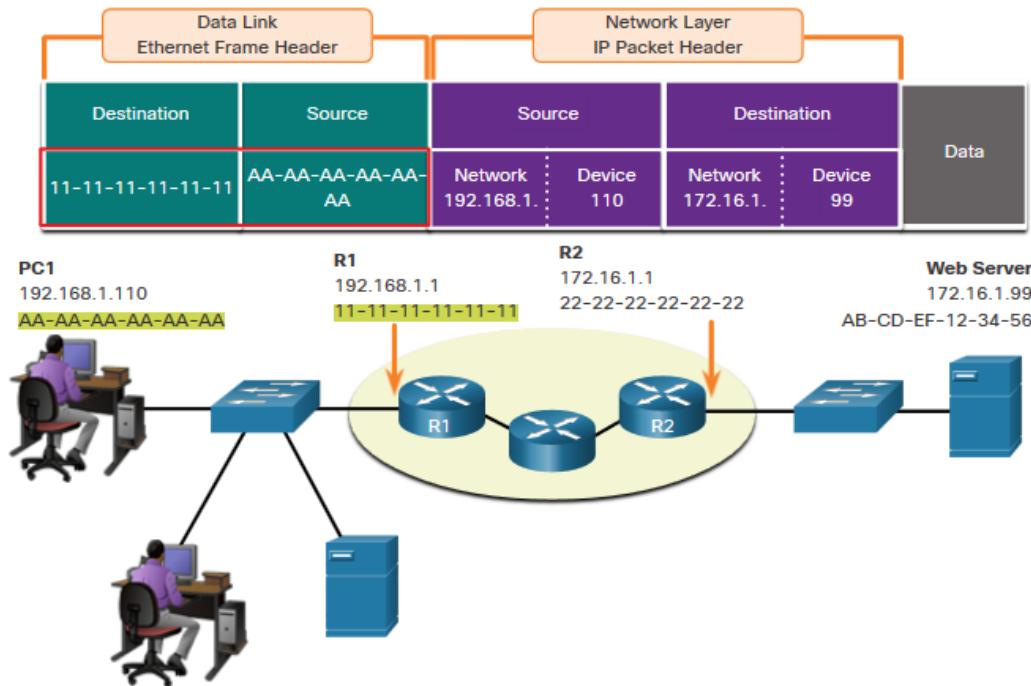
- PC1 - 192.168.1
- Web Sunucusu - 172.16.1



# Data Link Layer Adreslerinin Rolü : Farklı IP Ağları

❖ Nihai hedef uzak olduğunda, **Katman 3, Yönlendirici adresi olarak** da bilinen yerel varsayılan ağ geçidi IP adresini Katman 2'ye sağlayacaktır.

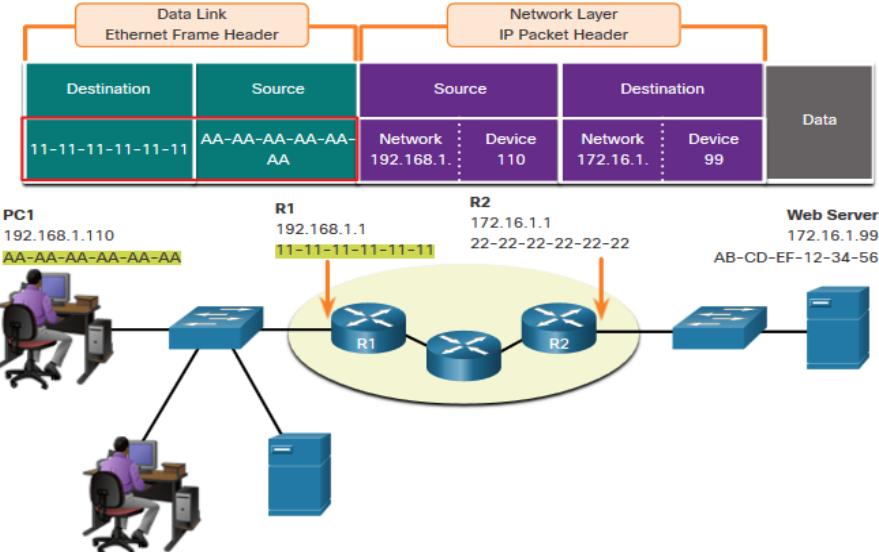
- Varsayılan ağ geçidi (DGW), bu LAN'ın bir parçası olan ve diğer tüm uzak konumlara "kapı" veya "ağ geçidi" olacak olan yönlendirici arayüzü IP adresidir.
- LAN üzerindeki tüm cihazlara bu adres hakkında bilgi verilmelidir, aksi takdirde trafiği yalnızca LAN ile sınırlanacaktır.
- PC1'deki Katman 2 varsayılan ağ geçidine (Yönlendirici) iletişiminde, yönlendirici bilgisi gerçek hedefe almak için yönlendirme sürecini başlatabilir.



# Data Link Layer Adreslerinin Rolü : Farklı IP Ağları

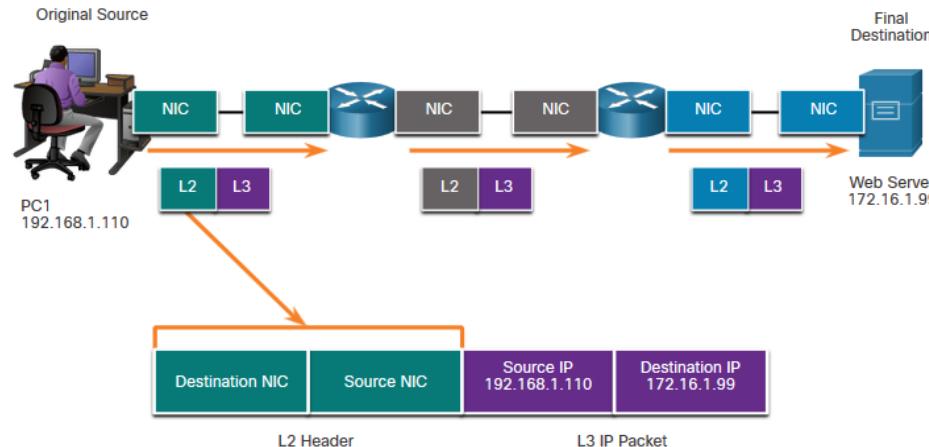
- Veri bağlantısı adreslemesi yerel adreslemedir, bu nedenle her bağlantı için bir kaynak ve hedefe sahip olacaktır.
- İlk segment için MAC adreslemesi şöyledir:
  - Kaynak - AA-AA-AA-AA-AA-AA (PC1) Çerçeveyi gönderir.
  - Hedef - 11-11-11-11-11-11 (R1-Varsayılan Ağ Geçidi MAC) Çerçeveyi alır.

**Not:** L2 yerel adresleme, bağlantıdan bağlantıya veya atlamaadan atlamaya değişse de, **L3** adreslemesi aynı kalır.



# Data Link Adresleri

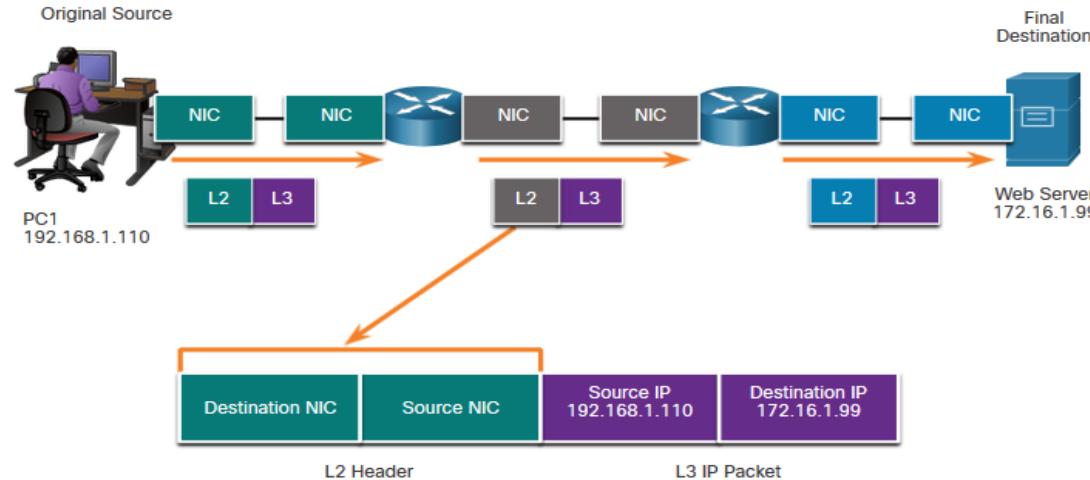
- Veri bağlantısı adresleme yerel adresleme olduğundan, hedefe giden yolculuğun her segmenti veya sekmesi için bir kaynağı ve hedefi olacaktır.
- İlk segment için MAC adreslemesi şöyledir:
  - Kaynak - (PC1 NIC) çerçeve gönderir
  - Hedef - (İlk Yönlendirici - DGW arayüzü) çerçeve alır



# Data Link Adresleri

İkinci atlama için MAC adreslemesi şöyledir:

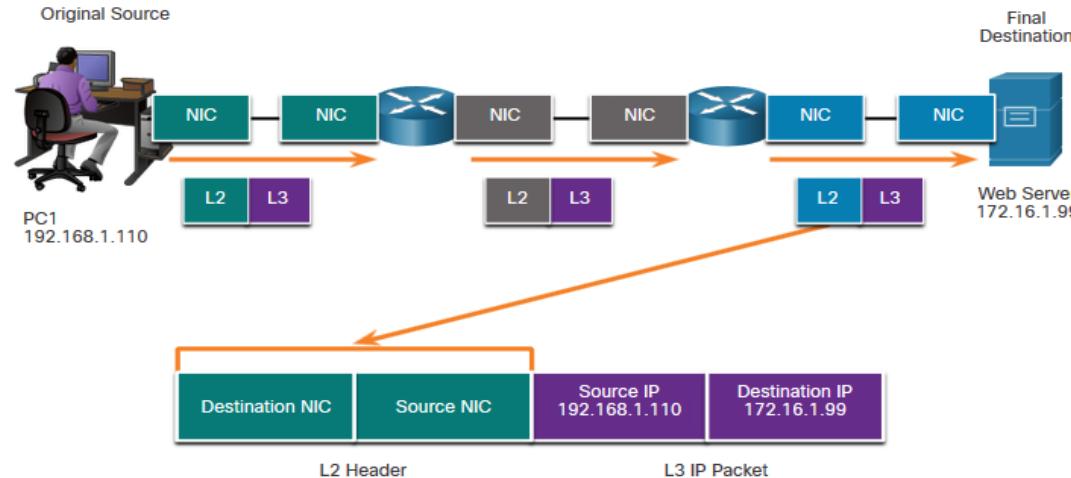
- Kaynak - (İlk Yönlendirici - çıkış arayüzü) çerçeve gönderir
- Hedef - (İkinci Yönlendirici) çerçeve alır



# Data Link Adresleri

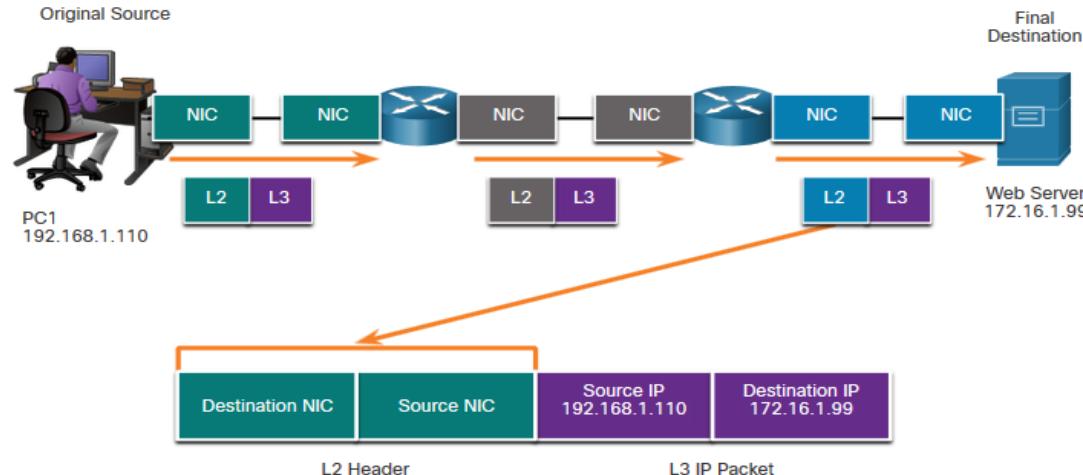
Son segment için MAC adreslemesi:

- Kaynak - (İkinci Yönlendirici-çıkış arayüzü) çerçeve gönderir
- Hedef - (Web Sunucusu NIC) çerçeve alır



# Data Link Adresleri

- Paketin değiştirilmediğine, ancak çerçevenin değiştiğine dikkat edin, bu nedenle L3 IP adreslemesi, L2 MAC adreslemesi gibi bölümden bölüme değişmez.
- L3 adresleme, global olduğu ve nihai hedef hala Web Sunucusu olduğu için aynı kalır.



# Lab –Wireshark Kurulumu

BU laboratuvara aşağıdakileri yapınız:

- Wireshark’I indirin ve kurun

## Lab – Ağ trafigini gözlemek için Wireshark kullanımı

Bu laboratuvara aşağıdakileri yapacaksınız:

- Bölüm 1: Wireshark'ta Yerel ICMP Verilerini Yakalayın ve Analiz Edin
- Bölüm 2: Wireshark'ta Uzaktan ICMP Verilerini Yakalayın ve Analiz Edin

■

# 3.8 Alıştırmalar ve Sınav

# Bu modülde ne öğrendim?

## Kurallar

- Protokollerin bir göndereni ve bir alıcısı olmalıdır.
- Yaygın bilgisayar protokolleri şu gereksinimleri içerir: mesaj kodlama, biçimlendirme ve kapsülleme, boyut, zamanlama ve teslim seçenekleri.

## Protokoller

- Ağ üzerinden bir mesaj göndermek için birkaç protokolün kullanılması gereklidir.
- Her ağ protokolünün kendi işlevi, biçimini ve iletişim kuralları vardır.

## Protokol Paketleri

- Bir protokol paketi, birbiriyle ilişkili bir protokoller grubudur.
- TCP / IP protokol paketi, günümüzde kullanılan protokollerdir.

## Standart Kuruluşlar

- Açık standartlar birlikte çalışabilirliği, rekabeti ve yeniliği teşvik eder.

# Bu modülde ne öğrendim?

## Referans Modelleri

- Ağ oluşturmada kullanılan iki model, TCP / IP ve OSI modelidir.
- TCP / IP modelinin 4 katmanı ve OSI modelinin 7 katmanı vardır.

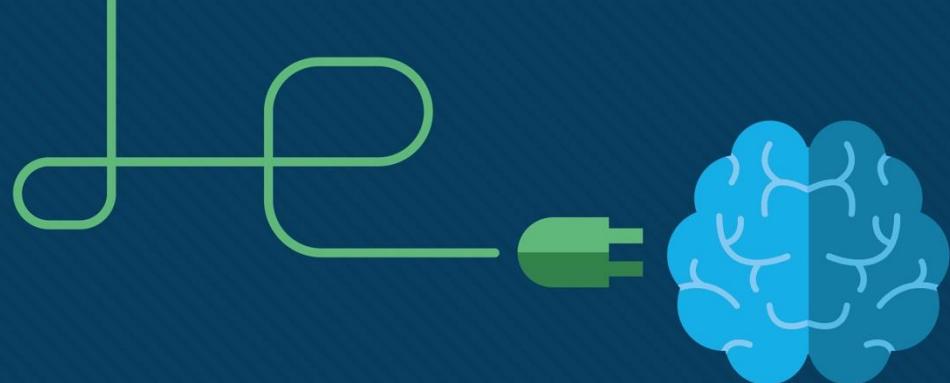
## Veri Kapsülleme

- Bir veri parçasının herhangi bir katmanda aldığı forma *protokol veri birimi (PDU)* denir .
- Veri kapsülleme sürecinde kullanılan beş farklı PDU vardır: veri, segment, paket, çerçeve ve bitler

## Veri Erişimi

- Ağ ve Veri Bağlantısı katmanları, verileri ağ üzerinden taşımak için adresleme sağlayacaktır.
- Katman 3, IP adresleme sağlayacak ve katman 2, MAC adresleme sağlayacaktır.
- Bu katmanların adreslemeyi işleme şekli, kaynağın ve hedefin aynı ağıda olup olmamasına veya hedefin kaynaktan farklı bir ağıda olmasına bağlı olacaktır.





# Modül 4: Fiziksel Katman

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

## Modül Başlığı: Fiziksel Katman

**Modül Hedefi:** Fiziksel katman protokollerinin, hizmetlerinin ve ağ ortamının veri ağları arasındaki iletişimini nasıl desteklediğini açıklayın.

Konu Başlığı	Konu Hedefi
Fiziksel Katmanın Amacı	Ağdaki fiziksel katmanın amacını ve işlevlerini açıklayın.
Fiziksel Katman Özellikleri	Fiziksel katmanın özelliklerini açıklayın.
Bakır Kablolama	Bakır kablolamanın temel özelliklerini belirleyin.
UTP Kablolama	Ethernet ağlarında UTP kablosunun nasıl kullanıldığını açıklayın.
Fiber Optik Kablolama	Fiber optik kablolama ve diğer medya üzerinde ana avantajları açıklayın.
Kablosuz Medya	Kablolu ve kablosuz ortam kullanarak cihazları bağlayın.

# 4.1 Fiziksel Katmanın Amacı

# Fiziksel Katmanın Amacı

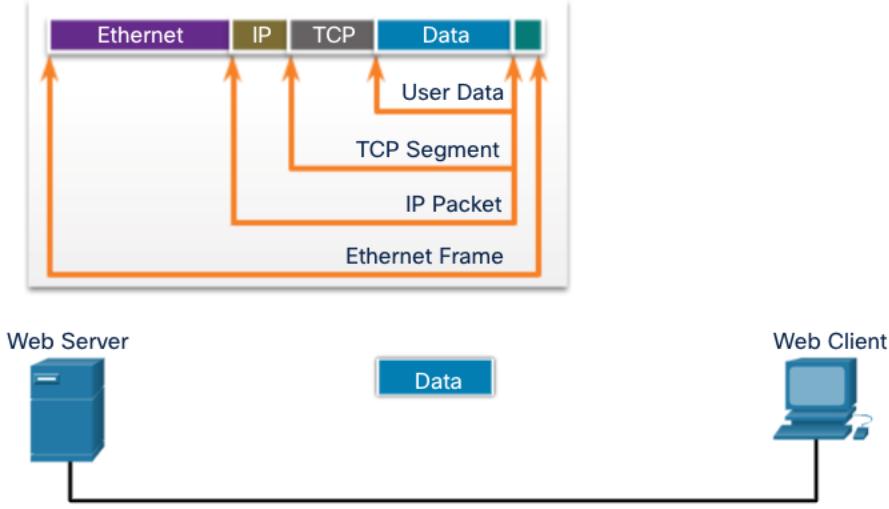
# Fiziksel Bağlantı

- Herhangi bir ağ iletişimini oluşmadan önce, yerel bir ağa fiziksel bir bağlantı kurulmalıdır.
- Bu bağlantı, ağın kurulumuna bağlı olarak **kablolu** veya **kablosuz** olabilir.
- Bu genellikle bir şirket ofisi veya bir ev için geçerlidir.
- **Ağ Arabirim Kartı** (NIC - Network Interface Card) **bir aygıtı ağa bağlar.**
- Bazı aygıtlarda yalnızca bir Ağ Arabirim Kartı NIC bulunurken, bazlarında birden çok NIC olabilir (örneğin **Kablolu** ve/veya **Kablosuz**).
- Tüm fiziksel bağlantılar aynı performans düzeyini sunmaz.

# Fiziksel Katmanın Amacı

# Fiziksel Katman

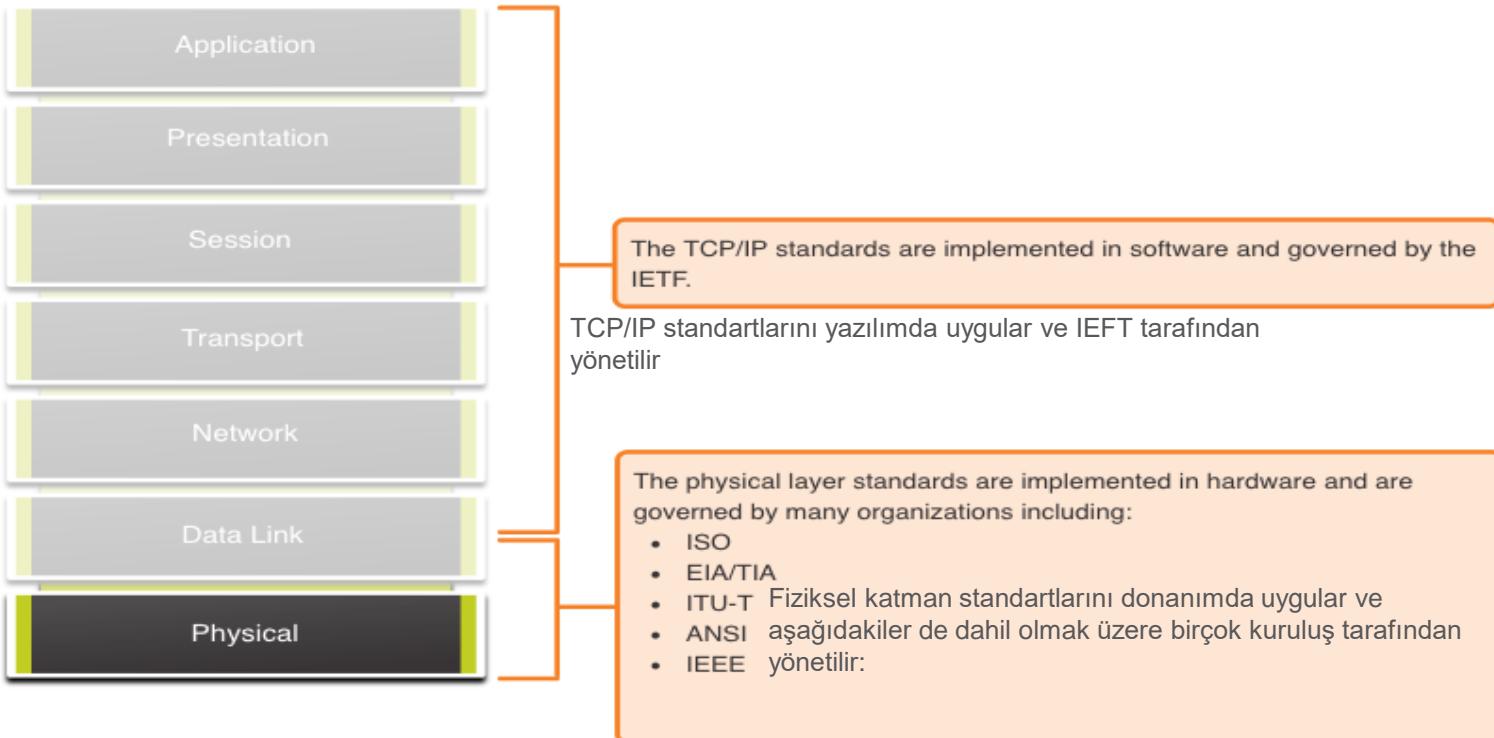
- Bitleri ağ ortamı üzerinden taşıır
- Veri Bağlantısı Katmanı'ndan tam bir çerçeve kabul eder ve yerel ortama iletilen bir dizi sinyal olarak kodlar
- **Bu kapsülleme işleminin son adımıdır.**
- Hedefe giden yolda bir sonraki aygit bitleri alır ve çerçeveyi yeniden kapsüller, sonra onunla ne yapacağına karar verir.



# 4.2 Fiziksel Katman Özellikleri

# Fiziksel Katman Karakteristiği

# Fiziksel Katman Standartları



## Fiziksel Katman Standartları üç işlevsel alanı:

- Fiziksel Bileşenler
- Kodlama
- Sinyal

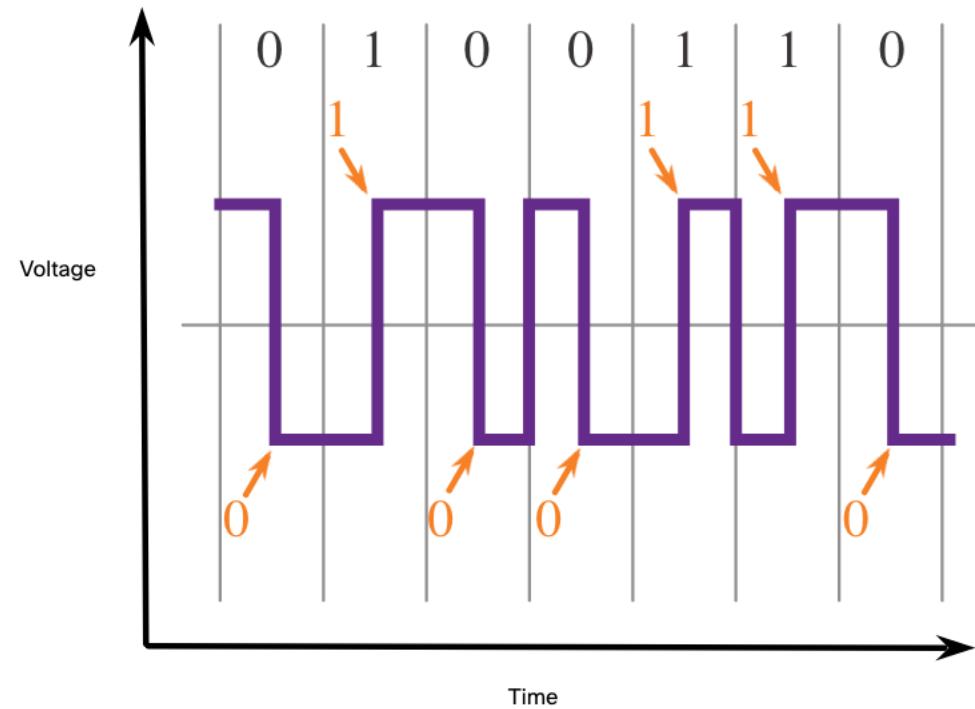
**Fiziksel Bileşenler**, bitleri temsil eden sinyalleri ileten donanım aygıtları, ortam ve diğer bağlayıcılardır.

- **Ağ Arabirim Kartları** (NIC - Network Interface Card), **arabirimler** ve **konektörler**, **kablo malzemeleri** ve **kablo tasarımları** gibi donanım bileşenlerinin tümü fiziksel katmanla ilişkili standartlarda belirtilir.

# Fiziksel Katman Özellikleri

## Kodlama

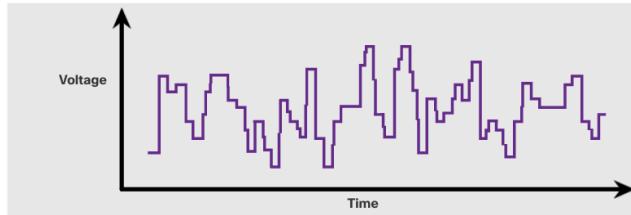
- Kodlama, bit akışını ağ yolundaki sonraki aygit tarafından tanımlayabilir bir biçimde dönüştürür.
- Bu 'kodlama' sonraki aygit tarafından tanımlayabilir öngörelebilir desenler sağlar.
- Kodlama yöntemlerine örnek olarak **Manchester** (şekilde gösterilmiştir), 4B/5B ve 8B/10B verilebilir.



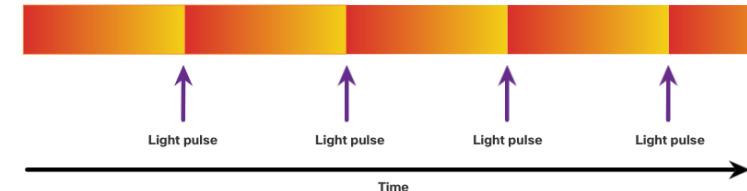
# Fiziksel Katman Özellikleri

## Sinyalleme

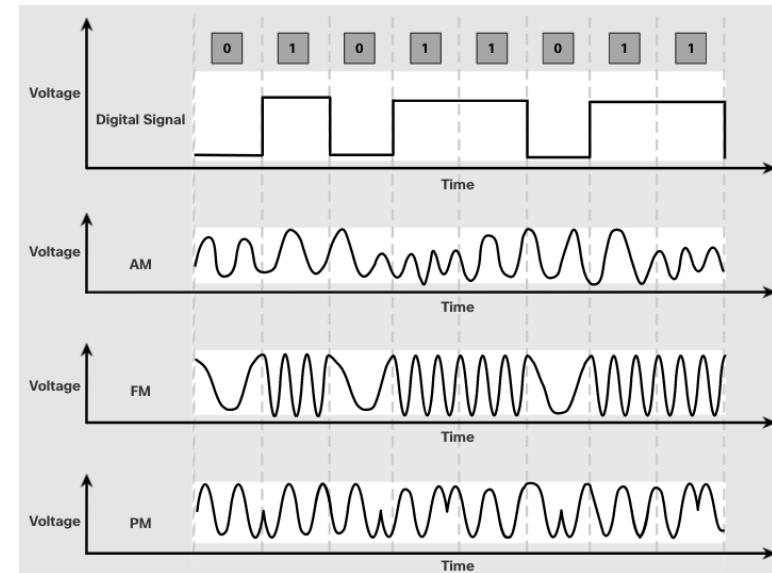
- Sinyalleme yöntemi, bit değerleri, "1" ve "0" fiziksel ortamda **nasıl temsil edildiği**dir.
- Sinyalleme yöntemi kullanılan ortamın türüne göre değişir.



Bakır Kablo Üzerindeki Elektrik Sinyalleri



Fiber Optik Kablo Üzerinde İşık Darbeleri



Kablosuz Üzerinden Mikrodalga Sinyalleri

# Fiziksel Katman Özellikleri

## Bant genişliği

- **Bant genişliği, bir ortamın veri taşıyabileceği kapasitedir.**
- **Dijital bant genişliği**, belirli bir süre içinde bir yerden diğerine akabilen veri miktarını ölçer; **saniyede kaç bit iletilebilir**.
- Fiziksel ortam özellikleri, **mevcut teknolojiler ve fizik yasaları mevcut bant genişliğinin belirlenmesinde rol oynar**.

Bant Genişliği Birimi	Kısaltma	Denklik
Saniyede bit	bps	1 bps = bant genişliğinin temel birimi
Saniyede kilobit	Kbps	1 Kbps = 1,000 bps = $10^3$ bps
Saniyede megabit	Mbps	1 Mbps = 1,000,000 bps = $10^6$ bps
Saniyede gigabit	Gbps	1 Gbps – 1,000,000,000 bps = $10^9$ bps
Saniyede terabit	Tbps	1 Tbps = 1,000,000,000,000 bps = $10^{12}$ bps

# Fiziksel Katman Özellikleri Bant Genişliği Terminolojisi

## Gecikme (Latency)

- Verilerin belirli bir noktadan diğerine geçmesi için gecikmeler de dahil olmak üzere süredir.

## Verim (Throughput)

- Belirli bir süre içinde medya üzerinden bit aktarımının ölçüsüdür.

## Goodput

- Belirli bir süre içinde aktarılan kullanılabilir verilerin ölçüsüdür.
- Goodput = Verim - trafik yükü

# 4.3 Bakır Kablolama

## Bakır Kablolamanın Özellikleri

- Bakır kablolama günümüzde ağlarda kullanılan en yaygın kablolama türündür.
- Ucuzdur, kurulumu kolaydır ve elektrik akımına karşı direnci düşüktür.

### Sınırlama:

**Zayıflama** – elektrik sinyalleri ne kadar uzun süre hareket etmek zorunda kalırsa, **o kadar zayıflar**.

- Elektrik sinyali, veri sinyallerini bozabilen ve bozabilen iki kaynaktan gelen parazite (**Elektromanyetik Girişim (EMI - Electromagnetic Interference)**) ve **Radyo Frekans Paraziti (RFI - Radio Frequency Interference)** ve **Crosstalk'a** (seste karışma) karşı hassastır.

## Azaltma:

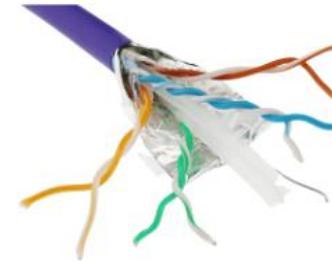
- Kablo uzunluğu sınırlarına sıkı sıkıya bağlı kalmak zayıflamayı azaltacaktır.
- **Bazı bakır kablo türleri metalik koruma ve topraklama kullanarak Elektromanyetik Girişim (EMI) ve Radyo Frekans Paraziti (RFI) azaltabilir.**
- Bazı bakır kablo türleri, karşıt devre çift kablolalarını birbirine bükererek çapraz konuşmayı (*sinyallerin birbirine tesir etmeleri*) hafifletir.

# Bakır Kablolama Çeşitleri



Unshielded Twisted-Pair (UTP) Cable

Korumasız Bükümlü Çift Kablo



Shielded Twisted-Pair (STP) Cable

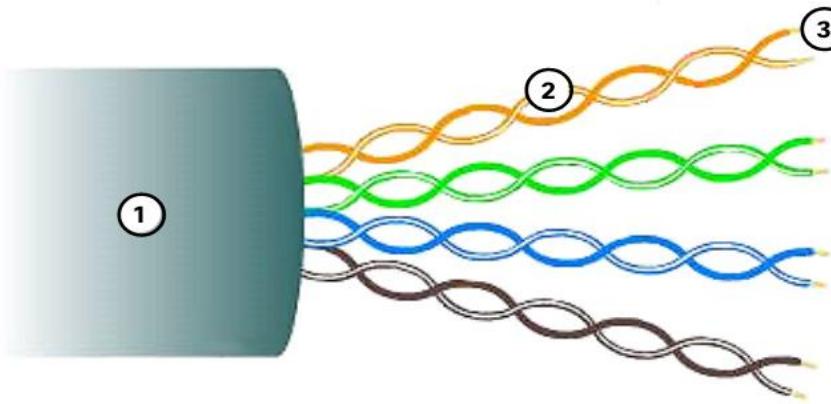
Korumalı Bükümlü Çift Kablo



Coaxial Cable

Koaksiyel Kablo

# Korumasız Bükümlü Çift

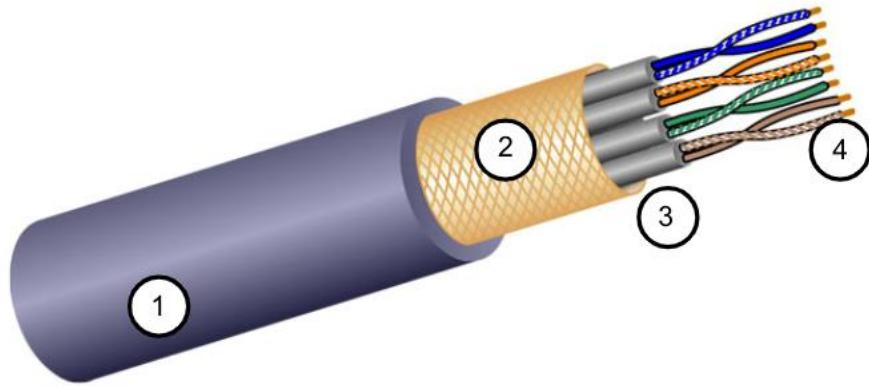


- Korumasız Bükümlü Çift en yaygın ağ ortamıdır.
- RJ-45 konektörleri ile sonlandırılır.
- **Ana bilgisayarları ara ağ aygıtlarıyla birbirine bağlar.**

#### Temel Özellikler:

- \* Dış ceket bakır telleri fiziksel hasardan korur.
- \* Bükümlü çiftler sinyali parazite karşı korur.
- \* Renk kodlu plastik yalıtmış elektriksel birbirinden teller izole ve her çifti tanımlar.

# Bakır Kablolama Korumalı Bükümlü Çift



- Korumasız Bükümlü Çift kablodan daha iyi gürültü koruması vardır.
- Korumasız Bükümlü Çift kablodan daha pahalıdır.
- Korumasız Bükümlü kablodan kurulumu daha zordur
- RJ-45 konektörleri ile sonlandırıldı
- **Ana bilgisayarları ara ağ aygıtlarıyla birbirine bağlar**

Temel Özellikle:

- \* Dış ceket bakır telleri fiziksel hasardan korur
- \* Örgülü veya folyo kalkan EMI/RFI koruması sağlar
- \* Her bir kablo çifti için folyo kalkan EMI/RFI koruması sağlar
- \* Renk kodlu plastik yalıtım elektriksel birbirinden teller izole ve her çifti tanımlar

# Bakır Kablolama Koaksiyel Kablo

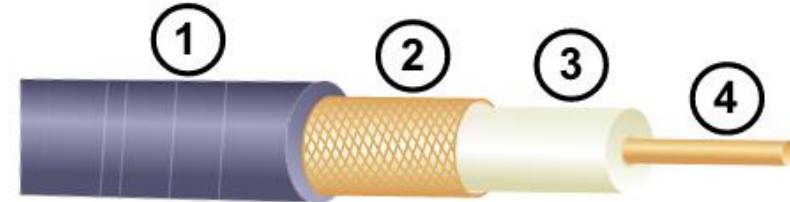
Aşağıdakilerden oluşur:

1. Küçük fiziksel hasarı önlemek için dış kablo ceketi
2. Dokuma bakır örgü veya metalik folyo, devredeki **ikinci tel ve iç iletken** için bir kalkan görevi görür.
3. Esnek plastik yalıtmış tabakası
4. Bakır iletken elektronik sinyalleri iletmek için kullanılır.

Koaksiyel kablo ile kullanılan konektörlerin farklı türleri vardır.

Yaygın olarak aşağıdaki durumlarda kullanılır:

- \* **Kablosuz kurulumlar** - antenleri kablosuz aygıtlara takın
- \* **Kablo internet kurulumları** - müşteri tesislerinde kablolama



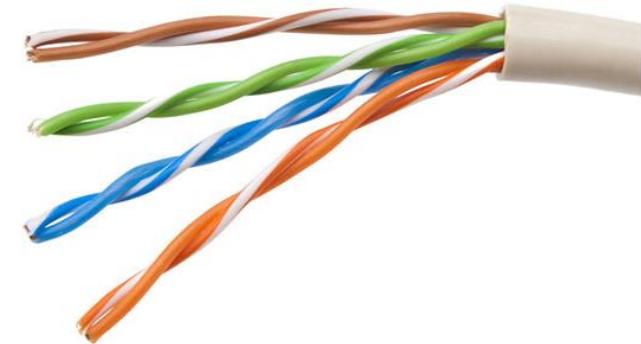
# 4.4 Korumasız Bükümlü Çift Kablolama

(Unshielded Twisted Pair (UTP))

# UTP Kablolamanın Özellikleri

UTP renk kodlu bakır teller dört çift birlikte bükülmüş ve esnek bir plastik kılıf kaplı vardır. Koruma kullanılmaz. UTP, çapraz konuşmayı sınırlamak için aşağıdaki özelliklere dayanır:

- \* İptal - Bir çift teldeki her tel zıt polarite kullanır. Bir tel negatif, diğer tel pozitif. Birlikte bükülürler ve manyetik alanlar birbirlerini ve EMI/RF dışında etkin bir şekilde iptal ederler.
- \* Her telde ayak başına büküm değişimi - Her tel farklı miktarda bükülür, bu da kablodaki teller arasında çapraz konuşmayı önlemeye yardımcı olur.



\* UTP: Unshielded Twisted-Pair Cable (Korumasız Bükümlü Çift Kablo)

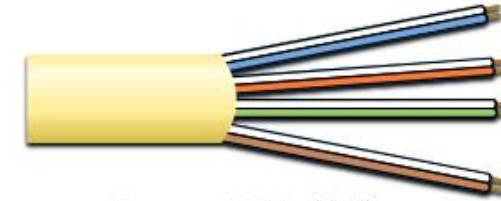
# UTP Kablolama Standartları ve Konektörler

UTP standartları TIA/EIA tarafından belirlenir. TIA/EIA-568 gibi unsurları standartlaştırmır:

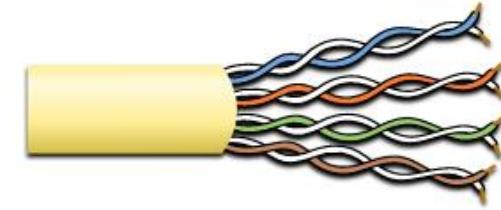
- \* Kablo Tipleri
- \* Kablo Uzunlukları
- \* Bağlayıcı
- \* Kablo Sonlandırma
- \* Test Yöntemleri

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

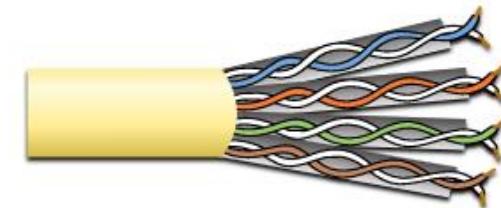
- Kategori 3
- Kategori 5 ve 5e
- Kategori 6



Category 3 Cable (UTP)



Category 5 and 5e Cable (UTP)



Category 6 Cable (UTP)

# UTP Kablolama Standartları ve Konektörler



RJ-45 Connector



RJ-45 Konektörü



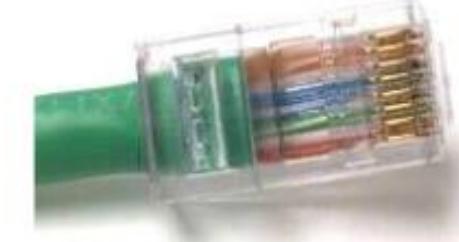
RJ-45 Socket

RJ-45 Soketi



Poorly terminated UTP cable

Kötü sonlandırılmış UTP kablosu

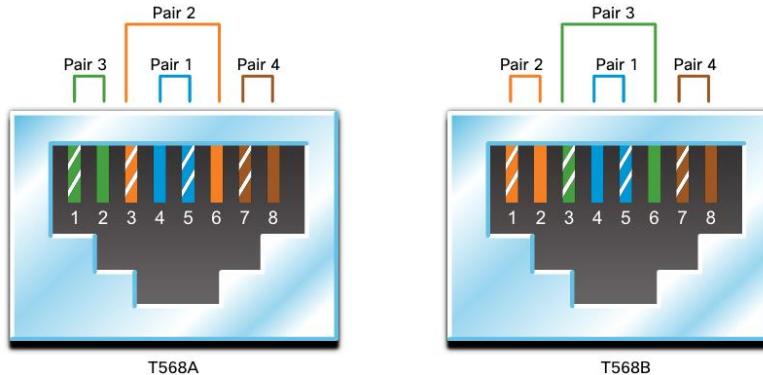


Properly terminated UTP cable

Düzgün bir şekilde sonlandırılan UTP kablosu

# UTP Kablolama

## Düz ve Crossover UTP Kabloları



Kablo Tipi	Standart	Uygulama
Ethernet Düz	Her iki uç T568A veya T568B	<b>Ağ Aygıtına Ana Bilgisayar</b>
Ethernet Çapraz *	Bir uç <b>T568A</b> , diğer uç <b>T568B</b>	Ana Bilgisayardan Ana Bilgisayara, <b>Anahtardan Anahtara, Yönlendiriciden Yönlendiriciye</b>
Rollover	Cisco Tescilli	<b>Bir bağdaştırıcı kullanarak seri bağlantı noktasını Yönlendirici veya Switch Console Port'a barındırma</b>

\* UTP: Unshielded Twisted-Pair Cable (Korumasız Bükümlü Çift Kablo)

# 4.5 Fiber Optik Kablolama

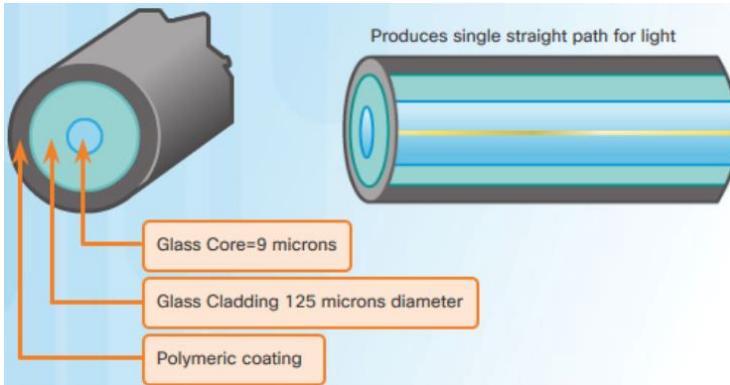
# Fiber Optik Kablolamanın Özellikleri

- Gider nedeniyle UTP kadar yaygın değil
- Bazı ağ senaryoları için idealdir.
- Verileri diğer ağ ortamlarından **daha yüksek bant genişliğinde** daha uzun mesafelerde iletir.
- **Zayıflamaya daha az duyarlıdır ve EMI/RFI'ye karşı tamamen bağışiktır**
- Çok saf cam esnek, son derece ince iplikçiklerden yapılmıştır
- Lig darbeleri olarak bit kodlamak için bir lazer veya LED kullanırıht
- Fiber optik kablo, en az sinyal kaybı ile **iki uç arasında ışık iletmek için bir dalga kılavuzu olarak hareket eder**

# Fiber Optik Kablolama

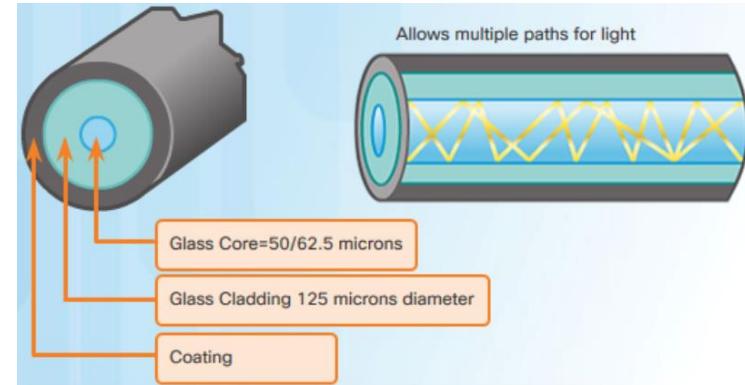
## Fiber Ortam Türleri

### Tek Modlu Fiber



- Çok küçük çekirdek
- Pahalı lazerler kullanır
- Uzun mesafe uygulamaları

### Çok Modlu Fiber



- Daha büyük çekirdek
- Daha ucuz LED kullanır
- LED'ler farklı açılarda iletir
- **550 metre üzerinde 10 Gbps'ye kadar**

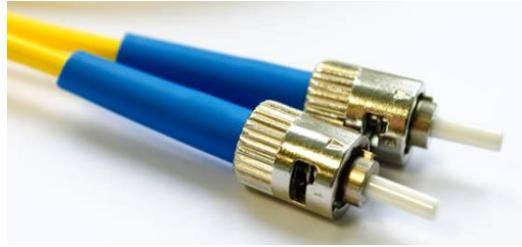
Dağılım, bir ışık darbesinin zaman içinde yayılması anlamına gelir. Artan dağılım, sinyal mukavemetinin artması anlamına gelir. Çok Modlu Fiber, **Tek Modlu Fiber'den daha fazla dağılıma sahiptir** ve **Çok Modlu Fiber için maksimum kablo mesafesi 550 metredir.**

# Fiber Optik Kablolama Kullanımı

**Fiber optik kablolama dört tip kullanılmaktadır:**

- 1. Kurumsal Ağlar** - Omurga kablolama uygulamaları ve birbirine bağlı altyapı aygıtları için kullanılır.
- 2. Eve Fiber (FTTH - Fiber-to-the-Home)** - Evlere ve küçük işletmelere **her zaman açık geniş bant hizmetleri sağlamak** için kullanılır.
- 3. Uzun Mesafe Ağları** - Ülke ve şehirleri birbirine **bağlamak** için hizmet sağlayıcılar tarafından kullanılır
- 4. Denizaltı Kablo Ağları** - **Okyanus ötesi mesafelere kadar zorlu sualtı ortamlarında** hayatta kabilme yeteneğine sahip güvenilir yüksek hızlı, yüksek kapasiteli çözümler sağlamak için kullanılır.

# Fiber Optik Konektörler



Straight-Tip (ST) Connectors

Düz Uçlu Konektörler



Subscriber Connector (SC) Connectors

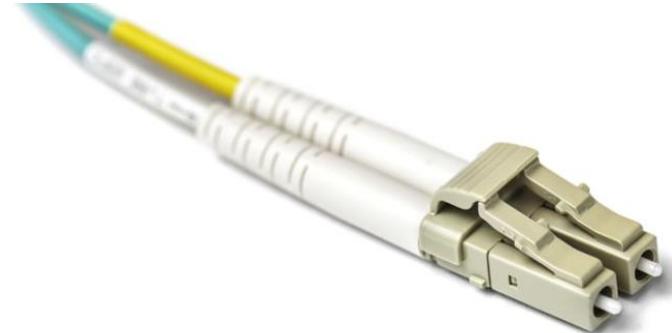


Abone Bağlayıcıları Konektörler



Lucent Connector (LC) Simplex Connectors

Lucent Konektörü Simplex Konektörleri



Duplex Multimode LC Connectors

Dubleks Çok Modlu LC Konektörleri

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

## Fiber Yama Kordonları



SC-SC MM Patch Cord  
SC-SC MM Patch Kablosu



LC-LC SM Patch Cord  
LC-LC SM Yama Kablosu



ST-LC MM Patch Cord  
ST-LC MM Yama Kablosu



ST-SC SM Patch Cord  
ST-SC SM Yama Kablosu

**Sarı olanlar tek modlu fiber kablolar ve turuncu olanlar çok modlu fiber kablolarıdır**

# Fiber - Bakır Karşılaştırması

Optik fiber öncelikle yüksek trafik, noktadan noktaya omurga kablolama olarak kullanılır, veri dağıtım tesisleri arasındaki bağlantılar ve binaların ara bağlantısı için çok binalı Kampüslerde kullanılır.

Uygulama Sorunları	UTP Kablolama	Fiber Optik Kablolama
Bant genişliği destekli	10 Mb/s - 10 Gb/s	10 Mb/s - 100 Gb/s
Mesafe	Nispeten kısa (1 - 100 metre)	Nispeten uzun ( 1 - 100.000 metre)
EMI ve RFI'ye dokunulmazlık	Düşük	Yüksek (Tamamen bağışık)
Elektriksel tehlikelere karşı bağışıklık	Düşük	Yüksek (Tamamen bağışık)
Medya ve konektör maliyetleri	En düşük	Yüksek
Kurulum becerileri	En düşük	Yüksek
Güvenlik önlemleri	En düşük	Yüksek

# 4.6 Kablosuz Medya

# Kablosuz Medyanın Özellikleri

**Radyo** veya **mikrodalga** frekansları kullanarak ikili basamakları temsil eden elektromanyetik sinyaller taşıır. Bu en büyük hareketlilik seçeneği sağlar. Kablosuz bağlantı numaraları artmaya devam ediyor.

## Kablosuz bağlantının bazı sınırlamaları:

- **Kapsama alanı** - Etkili kapsama alanı, dağıtım konumunun fiziksel özelliklerinden önemli ölçüde etkilenebilir.
- **Girişim** - Kablosuz girişime açıktır ve birçok yaygın aygit tarafından kesintiye uğrayabilir.
- **Güvenlik** - Kablosuz iletişim kapsama alanı, fiziksel bir ortam zincirine erişim gerektirmez, böylece herkes iletme erişebilir.
- **Paylaşılan ortam** - WLAN'lar yarı çift yönlü olarak çalışır, bu da aynı anda yalnızca bir aygıtın gonderip alabileceği anlamına gelir. WLAN'a aynı anda erişen birçok kullanıcı, her kullanıcı için bant genişliğinin azalmasına neden olabilir.

## Kablosuz Ortam Türleri

Kablosuz veri iletişimini için **IEEE** ve **telekomünikasyon endüstri standartları**

hem **veri bağlantısını** hem de **fiziksel katmanları** kapsar.

Bu standartların her birinde, **fiziksel katman özellikleri**:

- \* **Radyo sinyal kodlama yöntemlerine** veri
- \* **İletimin frekansı ve gücü**
- \* **Sinyal alımı ve kod çözme gereksinimleri**
- \* **Anten tasarıımı ve yapımı**

# Kablosuz Ortam Türleri

## Kablosuz Standartlar:

- **Wi-Fi (IEEE 802.11)** - Kablosuz LAN (WLAN) teknolojisi
- **Bluetooth (IEEE 802.15)** - Kablosuz Kişisel Alan ağı (WPAN) standarı
- **WiMAX (IEEE 802.16)** - Geniş bant kablosuz erişim sağlamak için noktadan çok noktaya topoloji kullanır
- **Zigbee (IEEE 802.15.4)** - Düşük veri hızı, düşük güç tüketimi iletişimini, öncelikle Nesnelerin İnterneti (IoT) uygulamaları için

**Genel olarak, Kablosuz LAN (WLAN) aşağıdaki aygıtları gerektirir:**

- **Kablosuz Erişim Noktası (AP - Access Point)** - *Kullanıcılarından gelen kablosuz sinyalleri yoğunlaştırır ve mevcut bakır tabanlı ağ altyapısına bağlanır*
- **Kablosuz NIC Adaptörleri** - **Ağ ana bilgisayarlarına kablosuz iletişim yeteneği sağlama**

**WLAN standartları vardır.** WLAN ekipmanı satın alırken, *uyumluluğu* ve *birlikte çalışabilirliği* sağlayın.

Ağ Yöneticileri, WLAN'ları yetkisiz erişim ve hasardan korumak için sıkı güvenlik ilkeleri ve süreçleri geliştirmeli ve uygulamalı.

# Paket Tracer – Kablolu ve Kablosuz LAN'ı Bağlayın

Bu Paket Tracer'da aşağıdakileri yapın:

- \* Buluta Bağlan
- \* Yönlendirici baglama(Router)
- \* Kalan Cihazları Bağla
- \* Bağlantıları Doğrula
- \* Fiziksel Topolojiyi İnceleyin

# Lab – Kablolu ve Kablosuz NIC Bilgilerini Görüntüle

Bu laboratuvara, aşağıdaki hedefleri tamamlanacaktır:

- PC NIC'leri tanımlama ve bunlarla çalışma
- Sistem Tepsisi Ağ Simgelerini Tanımla ve Kullan

# 4.7 Modül Uygulama ve Sınav

## Bu modülde ne öğrendim?

- Herhangi bir ağ iletişimini gerçekleştirmeden önce, kablolu veya kablosuz yerel bir ağa fiziksel bir bağlantı kurulmalıdır.
- Fiziksel tabaka, mühendisler tarafından geliştirilen elektronik devreler, ortam ve konektörlerden oluşur.
- Fiziksel katman standartları üç işlevsel alanı ele alır: fiziksel bileşenler, kodlama ve sinyalleme.
- Üç tür bakır kablolama vardır: UTP, STP ve koaksiyel kablo (koaksiyel kablo).
- UTP kablolama, TIA/EIA tarafından ortaklaşa belirlenen standartlara uygundur. Bakır kablolamanın elektriksel özellikleri Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) tarafından tanımlanır.
- Belirli kablolama kuralları kullanılarak elde edilen ana kablo tipleri Ethernet Straight-through ve Ethernet Crossover'dır.

## Bu modülde ne öğrendim?

- Optik fiber kablo, verileri diğer ağ ortamlarından daha uzun mesafelerde ve daha yüksek bant genişliklerinde iletir.
- Dört tür fiber optik konnektör vardır: ST, SC, LC ve çift yönlü çok modlu LC.
- Fiber optik yama kabloları SC-SC çok modlu, LC-LC tek modlu, ST-LC çok modlu ve SC-ST tek modlu içerir.
- Kablosuz ortam, radyo veya mikrodalga frekansları kullanarak veri iletişimiminin ikili basamaklarını temsil eden elektromanyetik sinyaller taşır. Kablosuz kapsama alanı, girişim, güvenlik ve paylaşılan herhangi bir ortamda oluşan sorunlar gibi bazı sınırlamalar vardır.
- Kablosuz standartlar şunlardır: Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), WiMAX (IEEE 802.16) ve Zigbee (IEEE 802.15.4).
- Kablosuz LAN (WLAN) kablosuz AP ve kablosuz NIC bağıdaştırıcıları gerektirir.

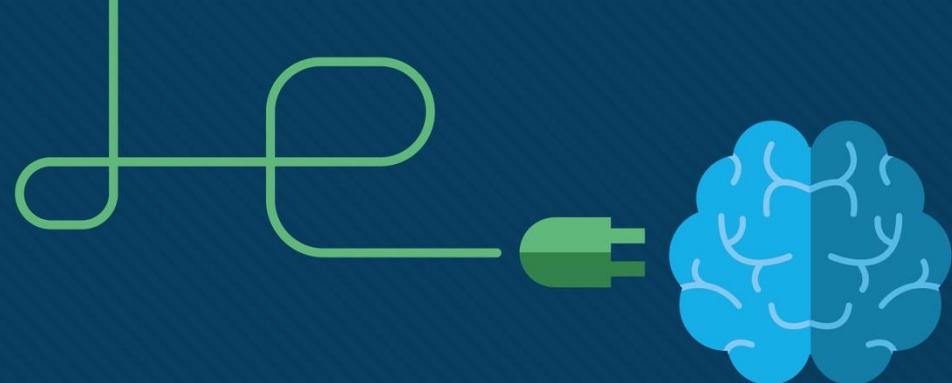
# 4.8 Özet

# Paket Tracer – Fiziksel Katmanı Bağla

Bu Paket Tracer'da aşağıdakileri yapacaksınız:

- \* Internet Çalışma Cihazlarının Fiziksel Özelliklerini Belirleme
- \* Bağlantı için Doğru Modülleri Seçin
- \* Cihazları Bağla
- \* Bağlantıyı Kontrol Et





# Modül 5: Sayı Sistemleri

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

**Modül Başlığı:** Sayı Sistemleri

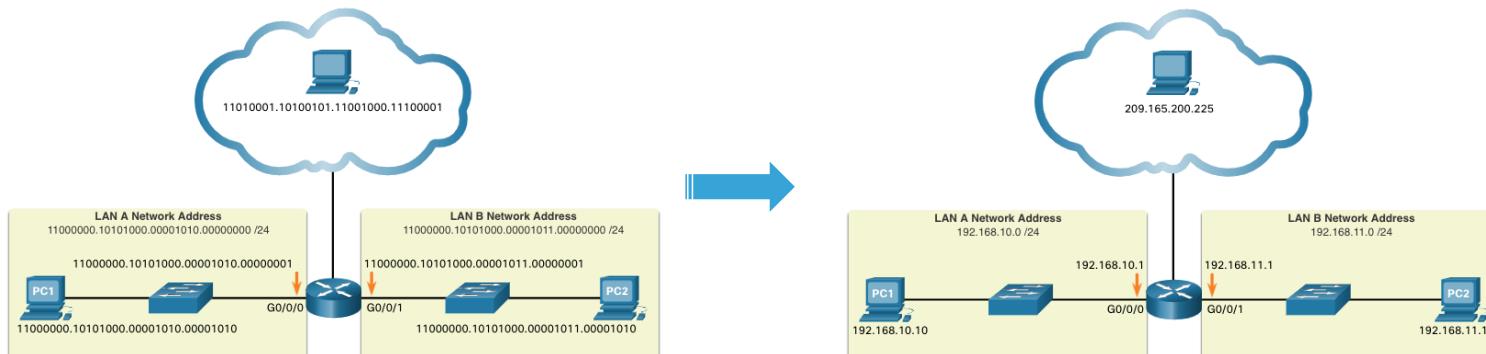
**Modül Hedefi:** Ondalık, ikili ve hexadecimal sistemler arasındaki sayıları hesaplayın.

Konu Başlığı	Konu Hedefi
<b>İkili Sayı Sistemi</b>	Ondalık ve ikili sistemler arasındaki sayıları hesaplayın.
<b>Heksadecimal Sayı Sistemi</b>	Ondalık ve heksadecimal sistemler arasındaki sayıları hesaplayın.

# 5.1 İkili Sayı Sistemi

# İkili Sayı Sistemi İkili ve IPv4 Adresleri

- İkili numaralandırma sistemi 1'ler ve 0'lardan oluşur, bit olarak adlandırılır
- Ondalık sayı sistemi 0 ile 9 arasında sayılarından oluşur
- Ana bilgisayarlar, sunucular ve ağ donanımları** birbirini tanımlamak için **ikili adresleme kullanırlar.**
- Her adres, sekizli adı verilen **dört bölüme bölünmüş 32 bitlik bir dizeden oluşur.**
- Her sekizli, **bir nokta ile ayrılmış 8 bit (veya 1 bayt) içerir.**
- Kişiler tarafından kullanım kolaylığı için, bu noktalı gösterim noktalı ondalığa dönüştürülür.



# Video – İkili ve Ondalık Numaralandırma Sistemleri Arasında Dönüşüm

Bu video aşağıdakileri kapsayacaktır:

- Konumsal gösterim incelemesi
- 10'un katları incelemesi
- Ondalık - taban 10 numaralandırma incelemesi
- İkili – baz 2 numaralandırma incelemesi
- İkili bir P adresini ondalık numaralandırmaya dönüştürme

# İkili Konumsal Gösterim

- Konumsal gösterim, bir basamağın sayı dizisinde bulunduğu "konuma" bağlı olarak farklı değerleri temsil etmesidir.
- Ondalık konumsal gösterim sistemi aşağıdaki tablolarda gösterildiği gibi çalışır.

Radix (Sayı Tabanı)	10	10	10	10
Sayıdaki Konum	3	2	1	0
Hesap	$(10^3)$	$(10^2)$	$(10^1)$	$(10^0)$
Konum Değeri	1000	100	10	1



	Binler	Yüzler	Onlar	Birler
Konumsal Değer	1000	100	10	1
Ondalık Sayı (1234)	1	2	3	4
Hesap	$1 \times 1000$	$2 \times 100$	$3 \times 10$	$4 \times 1$
ekleyin ...	1000	+ 200	+ 30	+ 4
Sonuç	<b>1,234</b>			

# İkili Konumsal Gösterim (devamı)

İkili konumsal gösterim sistemi aşağıdaki tablolarda gösterildiği gibi çalışır.

Radix	2	2	2	2	2	2	2	2
Sayıdaki Konum	7	6	5	4	3	2	1	0
Hesap	$(2^7)$	$(2^6)$	$(2^5)$	$(2^4)$	$(2^3)$	$(2^2)$	$(2^1)$	$(2^0)$
Konum Değeri	128	64	32	16	8	4	2	1



Konumsal Değer	128	64	32	16	8	4	2	1
Ondalık Sayı (1234)	1	1	0	0	0	0	0	0
Hesap	$1 \times 128$	$1 \times 64$	$0 \times 32$	$0 \times 16$	$0 \times 8$	$0 \times 4$	$0 \times 2$	$0 \times 1$
ekleyin ...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
Sonuç	192							

# İkili Sayıları Ondalık Sayılara Dönüştür

11000000.10101000.00001011.00001010 ondalık sayıya dönüştür.

Konumsal Değer	128	64	32	16	8	4	2	1
İkili Sayı (11000000)	1	1	0	0	0	0	0	0
Hesap	1x128	1x64	0x32	0x16	0x8	0x4	0x2	0x1
Ekleyin...	128	+ 64	+ 0	+ 0	+ 0	+ 0	+ 0	+ 0
İkili Sayı (10101000)	1	0	1	0	1	0	0	0
Hesap	1x128	0x64	1x32	0x16	1x8	0x4	0x2	0x1
Ekleyin...	128	+ 0	+ 32	+ 0	+ 8	+ 0	+ 0	+ 0
İkili Sayı (00001011)	0	0	0	0	1	0	1	1
Hesap	0x128	0x64	0x32	0x16	1x8	0x4	1x2	1x1
Ekleyin...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 1
İkili Sayı (00001010)	0	0	0	0	1	0	1	0
Hesap	0x128	0x64	0x32	0x16	1x8	0x4	1x2	0x1
Ekleyin...	0	+ 0	+ 0	+ 0	+ 8	+ 0	+ 2	+ 0

 192

 168

192.168.11.10

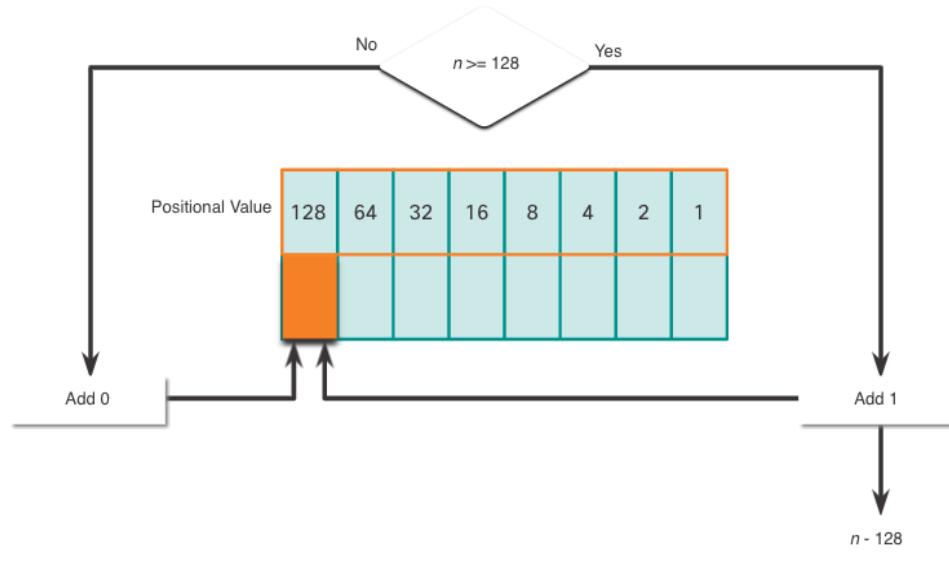
 11

 10

# Ondalık - İkili Dönüşümme

İkili konumsal değer tablosu, noktalı ondalık **IPv4** adresini ikili sisteme çevirmek için faydalıdır.

- 128 pozisyonunda başlayın (**en önemli bit**). Sekizlinin ondalık sayısı ( $n$ ) 128'e eşit mi ya da büyük mü?
- Hayır ise, **128 konumsal değere 0 kaydedin** ve **64 konumsal değere geçin**.
- Evet ise, **128 konumsal değere 1 kaydedin**, ondalık sayıdan **128'i çıkarın** ve **64 konumsal değere geçin**.
- Bu adımları **1 konumsal degree kadar yineleyin**.



# Ondalık - İkili Dönüşüm Örneği

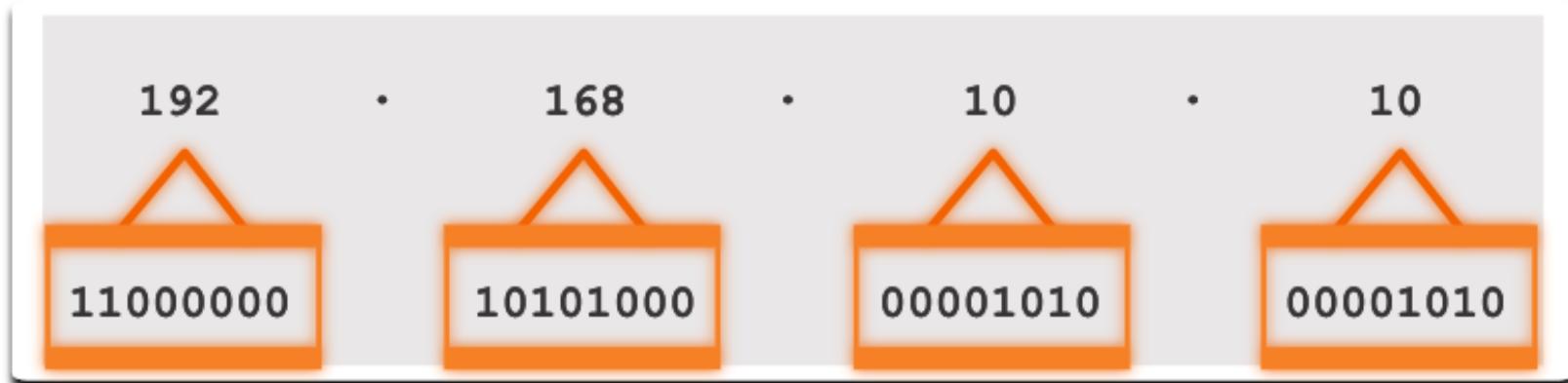
- Ondalık 168'i ikili sisteme dönüştürme
- $168 > 128$  mi?  
Evet, 128 pozisyonda 1 girin ve 128 çıkarın ( $168-128=40$ )  
 $40 > 64$  mü?  
Hayır, 64 pozisyonda 0 girin ve devam edin  
 $40 > 32$  mi?  
Evet, 32 pozisyonda 1 girin ve 32 çıkarın ( $40-32=8$ )  
 $8 > 16$  mi?  
Hayır, 16 pozisyonda 0 girin ve devam edin  
 $8 > 8$  mi?  
Equal. 8 pozisyonda 1 girin ve 8 çıkarın ( $8-8=0$ )  
Değer kalmadı. Kalan ikili pozisyonlara 0 girin

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

Ondalık 168 ikili sistemde 10101000 olarak yazılır

# İkili Sayı Sistemi IPv4 Adresleri

- Yönlendiriciler ve bilgisayarlar yalnızca ikili sistemi anlarken, insanlar ondalık sayılarla çalışır. Bu iki numaralandırma sistemini ve ağda nasıl kullanıldıklarını tam olarak anlamak önemlidir.



# 5.2 Hexadecimal Sayı Sistemi

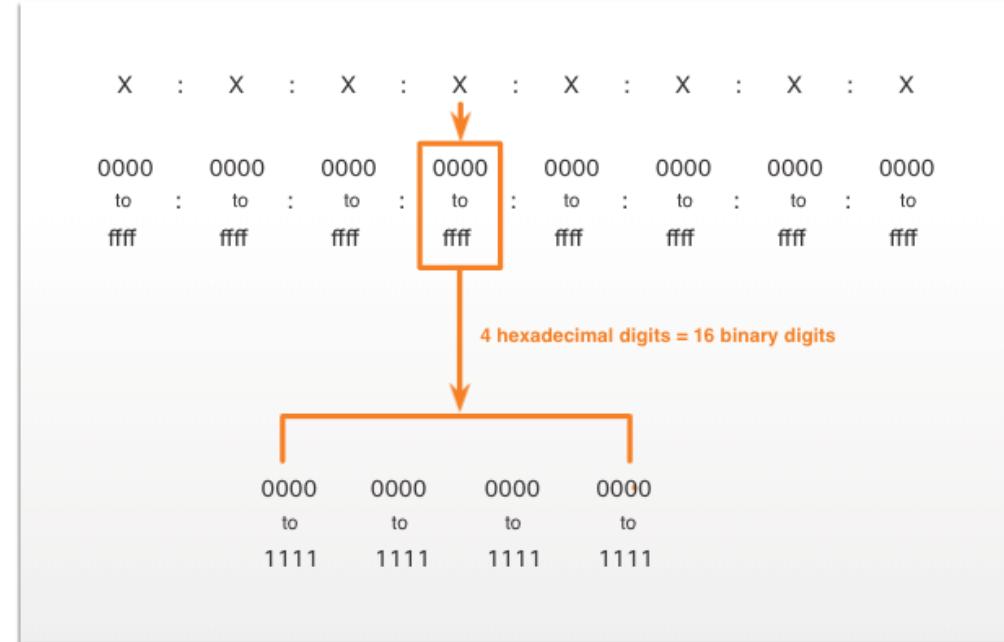
# Hexadecimal ve IPv6 Adresleri

- **IPv6** adreslerini anlamak için **hexadecimal**'ı ondalık sayıya veya ondalık sayıyı hexadecimal'a dönüştürebilmelisin.
- Hexadecimal, 0'dan 9'a ve A'dan F'ye doğru olan sayıları kullanan bir baz onaltı numaralandırma sistemidir.
- Bir değeri tek bir hexadecimal basamak olarak ifade etmek, dört ikili bit olarak ifade etmekten daha kolaydır.
- Hexadecimal, **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

# Hexadecimal ve IPv6 Adresleri (devamı)

- IPv6 adresleri 128 bit uzunluğundadır.
- **Her 4 bit tek bir hexadecimal basamak la temsil edilir.** Bu da IPv6 adresini toplam 32 hexadecimal değer yapar.
- Şekil, her X'in dört hexadecimal değeri temsil ettiği bir IPv6 adresi yazma yöntemi gösterir.
- Her dört hexadecimal karakter grubu hextet olarak adlandırılır.



# Video – Hexadecimal ve Ondalık Numaralandırma Sistemleri Arasında Dönüştürme

Bu video aşağıdakileri kapsayacaktır:

- Hexadecimal Sistemin Özellikleri
- Hexadecimal'dan Ondalık'a dönüştürme
- Ondalıktan Hexadecimal'a dönüştürme

# Ondalık - Hexadecimal Dönüşümler

Ondalık sayıları hexadecimal değerlere dönüştürmek için aşağıdaki adımları izleyin:  
Ondalık sayıyı 8 bitli ikili dizeleri dönüştürün.

- Divide the binary strings in groups of four starting from the rightmost position.
- Convert each four binary numbers into their equivalent hexadecimal digit.

Örneğin, 168'i üç adımlı işlemi kullanarak hex dönüştürme

- 168 ikili sistemde 10101000 olarak gösterilir
- 10101000 dört ikili basamak iki grupta 1010 ve 1000 olarak gösterilir
- 1010 hex A ve 1000 hex 8, bu yüzden 168 hexadecimal A8 olarak gösterilir.
-

## Hexadecimal - Ondalık Dönüşümler

Hexadecimal sayıları ondalık değerlere dönüştürmek için aşağıdaki adımları izleyin:  
Hexadecimal sayıyı 4-bit ikili dizeleri dönüştürün.

- En sağ konumdan başlayarak 8 bitlik ikili gruplandırma oluşturun.
- Her 8 bit ikili gruplandırmayı eşdeğer ondalık basamaklarına dönüştürün.

Örneğin, Üç adımlı işlemi kullanarak ondalık alana dönüştürülen D2 sayısı:

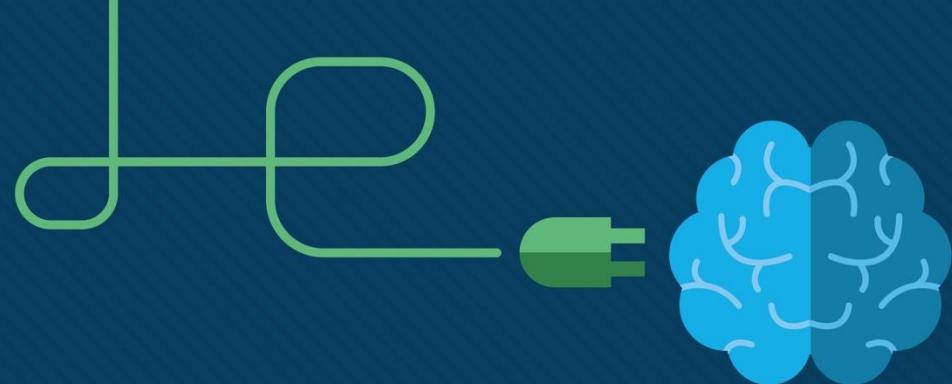
- D2 4-bit ikili dizeleri 1101 ve 0010 olarak gösterilir.
- 1101 ve 0010 8 bitlik bir grüplamada 11010010 olarak gösterilir.
- İkili sistemde 11010010 ondalık sistemde 210'a eşdeğerdir, bu nedenle D2, 210 olarak gösterilir.

# 5.3 Modül Uygulaması ve Sınav

# Bu modülde ne öğrendim?

- İkili, 0 ve 1 sayılarından oluşan ve bit adı verilen bir "taban iki" numaralandırma sistemidir.
- Ondalık, 0'dan 9'a kadar olan sayılarından oluşan bir "taban on" numaralandırma sistemidir.
- İkili, ana bilgisayarların, sunucuların ve ağ ekipmanlarının birbirini tanımlamak için kullandığı numaralandırma sistemidir.
- Hexadecimal, 0'dan 9'a kadar olan sayılar ve A'dan F'ye kadar olan harflerden oluşan "taban on altı" numaralandırma sistemidir.
- Hexadecimal IPv6 adreslerini ve MAC adreslerini temsil etmek için kullanılır.
- IPv6 adresleri 128 bit uzunluğundadır ve her 4 bit, toplam 32 hexadecimal basamak için bir hexadecimal basamakla temsil edilir.
- Hexadecimal'ı ondalık'a dönüştürmek için önce hexadecimal'ı ikiliye dönüştürmeniz, sonra ikiliyi ondalika dönüştürmeniz gereklidir.
- Ondalık sayıyı hexadecimal'a dönüştürmek için önce ondalık sayıyı ikiliye sonra da ikiliyi hexadecimal'a dönüştürmeniz gereklidir.





# Modül 6: Veri Bağlantısı Katmanı

Introduction to Networks v7.0  
(ITN)



# Modülün Amaçları

## Modül Başlığı: Veri Bağlantısı Katmanı

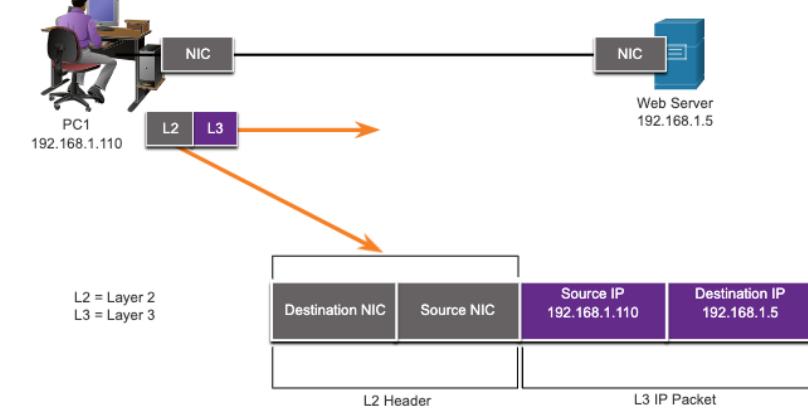
Modül Amacı: Veri bağlantısı katmanındaki **medya erişim kontrolünün ağlar arasında iletişimini nasıl desteklediğini** açıklabilmek.

Konu Başlığı	Konu Amacı
<b>Veri Bağlantısı Katmanının amacı</b>	Belirli ortamlarda iletim için iletişimini hazırlarken veri bağlantı katmanının amacını ve işlevini açıklamak.
<b>Topolojiler</b>	WAN ve LAN topolojilerindeki medya erişim kontrol yöntemlerinin özelliklerini karşılaştırmak.
<b>Veri Bağlantısı Çerçevesi</b>	Veri bağlantı çerçevesinin özelliklerini ve işlevlerini açıklamak.

# 6.1 Veri Bağlantısı Katmanının Amacı

# Veri Bağlantısı Katmanın Amacı Veri Bağlantısı Katmanı

- **Veri Bağlantısı katmanı, uç cihaz ağ arayüz kartları arasındaki iletişimden sorumludur.**
- **Üst katman protokollerinin fiziksel katman ortamına erişmesine izin verir ve Katman 3 paketlerini (IPv4 ve IPv6) Katman 2 Çerçeveveleri içine alır.**
- **Ayrıca hata tespiti yapar ve bozuk çerçeveleri reddeder.**



# IEEE 802 LAN/MAN Veri Bağlantısı Alt Katmanları

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

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

- **LLC alt katmanı**, üst katmanlardaki ağ yazılımı ile alt katmanlardaki cihaz donanımı arasında iletişim kurar.
- **MAC alt katmanı**, veri kapsüllemeden ve ortam erişim kontrolünden sorumludur.

		Network Layer Protocol		
Data Link	LLC Sublayer	LLC Sublayer - IEEE 802.2		
	MAC Sublayer	Ethernet IEEE 802.3	WLAN IEEE 802.11	WPAN IEEE 802.15
Physical		Various Ethernet standards for Fast Ethernet, Gigabit Ethernet, etc.	Various WLAN standards for different types of wireless communications	Various WPAN standards for Bluetooth, RFID, etc.

# Veri Bağlantısı Katmanın Amacı Medyaya Erişim Sağlama

Düğüm (Node) arasında **değiş tokuş edilen paketler, çok sayıda veri bağlantı katmanı ve ortam geçişleriyle** karşılaşabilir.

Yol boyunca her atlama, bir yönlendirici **dört temel Katman 2 işlevi** gerçekleştirir:

- Ağ ortamından bir çerçeveye kabul eder.
- Kapsullenmiş paketi açığa çıkarmak için çerçeveyi kapsülden çıkarır.
- **Paketi yeni bir çerçevede yeniden kapsüller.**
- Yeni çerçeveyi sonraki ağ segmentinin ortamında ileter.

# Veri Bağlantısı Katmanı Standartları

Veri bağlantı katmanı protokollerini 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

# Fiziksel ve Mantıksal Topolojiler

**Bir ağın topolojisi, ağ cihazlarının ve bunlar arasındaki ara bağlantıların düzenlenmesi ve ilişkisidir.**

Ağları tanımlarken kullanılan iki tür topoloji vardır:

- **Fiziksel topoloji** - fiziksel bağlantıları ve cihazların birbirine nasıl bağlandığını gösterir.
- **Mantıksal topoloji** - cihaz arayüzlerini ve IP adresleme şemalarını kullanan cihazlar arasındaki sanal bağlantıları tanımlar.

## Üç yaygın fiziksel WAN topolojisi vardır:

- **Noktadan noktaya** - en basit ve en yaygın WAN topolojisi. **İki uç nokta arasında kalıcı bir bağlantidan oluşur.**
- **Hub ve spoke** – merkezi bir sitenin *dal sitelerini noktadan noktaya bağlantılar aracılığıyla* birbirine bağladığı bir yıldız topolojisine benzer.
- **Mesh** – **yüksek kullanılabilirlik sağlar**, ancak her üç sistemin diğer tüm üç sistemlere bağlanması gerektirir.

# Noktadan Noktaya WAN Topolojisi

- Fiziksel noktadan noktaya topolojiler doğrudan iki nodu birbirine bağlar.
- Nodlar medyayı diğer hostlarla paylaşmayabilir.
- Medyadaki tüm çerçeveler yalnızca iki noda veya bu noddan gidebildiği için, Noktadan Noktaya WAN protokoller çok basit olabilir.



# Topolojiler LAN Topolojisi

LAN'lar üzerindeki **uç cihazlar tipik olarak bir yıldız veya genişletilmiş yıldız topolojisi kullanılarak birbirine bağlanır.**

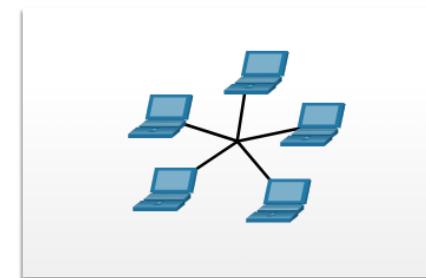
Yıldız ve genişletilmiş yıldız topolojilerinin **kurulumu kolaydır, çok ölçeklenebilir ve sorun giderilmesi kolaydır.**

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

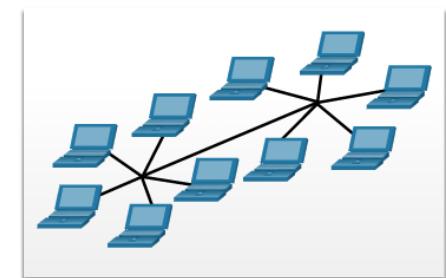
- **Bus (Veriyolu)** – Tüm uç sistemler birbirine zincirlenmiş ve **her bir uça sonlandırılmıştır.**
- **Ring (Halka)** – Her uç sistem, bir halka oluşturmak için ilgili **komşularına bağlanır.**



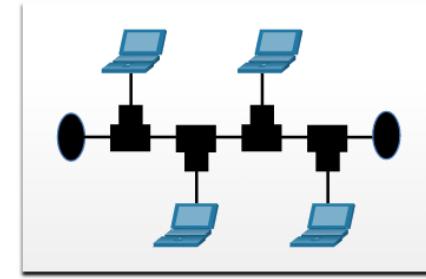
Physical Topologies



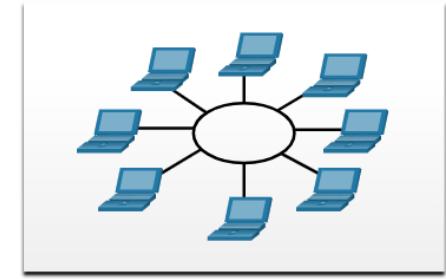
Star Topology



Extended Star Topology



Bus Topology



Ring Topology

## Yarı-çift yönlü iletişim

- Paylaşılan bir ortamda **aynı anda yalnızca bir aygıtın gönderip almasına izin verir.**
- WLAN'larda ve Ethernet hub'lı eski veri yolu topolojilerinde kullanılır.

## Tam-çift yönlü iletişim

- **Her iki cihazın da paylaşılan bir ortamda aynı anda iletim ve alım yapmasına izin verir.**
- **Ethernet switchleri tam çift yönlü modda çalışır.**

## Çekişmeli Erişim

Yarı çift yönlü çalışan tüm nodlar, ortamın kullanımı için rekabet eder.

Örnekler:

- Eski veri yolu topolojisi Ethernet'te kullanıldığı gibi, **çarpışma algılamalı** (collision detection - CSMA / CD) taşıyıcı algılama çoklu erişimi.
- Taşıyıcı, **Kablosuz LAN'larda** kullanıldığı gibi **çarpışma önleme (CSMA / CA)** ile çoklu erişimi algılar.

## Kontrollü Erişim

- Her nodun ortam üzerinde kendi zamanına sahip olduğu deterministik erişim.
- **Token Ring** ve **ARCNET** gibi eski ağlarda kullanılır.

# Çatışmaya Dayalı Erişim - Contention-Based Access – CSMA/CD

## CSMA/CD (Carrier Sense Multiple Access With Collision Detection)

- Eski Ethernet LAN'ları tarafından kullanılır.
- **Aynı anda yalnızca bir aygıtın gönderip aldığı yarı çift yönlü modda çalışır.**
- Bir cihazın **ne zaman gönderebileceğini ve aynı anda birden fazla cihaz gönderirse ne olacağını yönetmek için bir çarpışma algılama işlemi kullanır.**

### CSMA/CD çarpışma algılama süreci:

- Eşzamanlı iletişim yapan cihazlar, paylaşılan medyada bir sinyal çarşyasına neden olacaktır.
- **Cihazlar çarşmayı algılar.**
- Cihazlar rastgele bir süre bekler ve verileri yeniden iletir.

# Çatışmaya Dayalı Erişim - Contention-Based Access – CSMA/CA

## CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

- IEEE 802.11 WLAN'lar tarafından kullanılır.
- Aynı anda yalnızca bir aygıtın gönderip aldığı yarı çift yönlü modda çalışır.
- Bir cihazın ne zaman gönderebileceğini ve aynı anda birden fazla cihaz gönderirse ne olacağını yönetmek için bir çarpışmadan kaçınma süreci kullanır

### CSMA/CA çarpışma önleme süreci:

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

# 6.3 Veri Bağlantısı Çerçeveesi

## Çerçeve

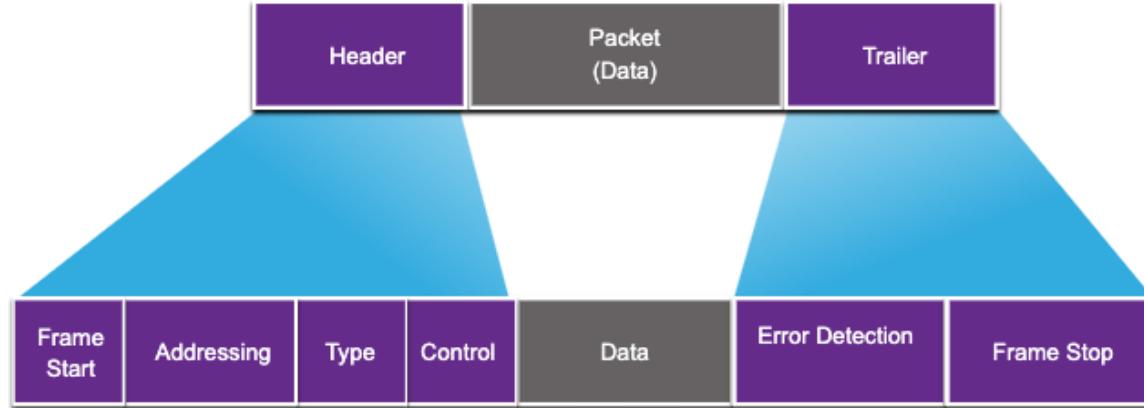
- Veriler, bir çerçeve oluşturmak için bir başlık ve bir trailer (sonlandırma bilgisi ) ile veri bağlantı katmanı tarafından kapsülle**nir.

**Bir veri bağlantısı çerçevesi üç bölümden oluşur:**

- Üstbilgi (Header)
- Data
- Trailer

- Başlık ve Trailer alanları, veri bağlantı katmanı protokolüne göre değişir.**
- Çerçvede taşınan kontrol bilgisi miktarı, erişim kontrol bilgisi ve mantıksal topolojiye göre değişir.**

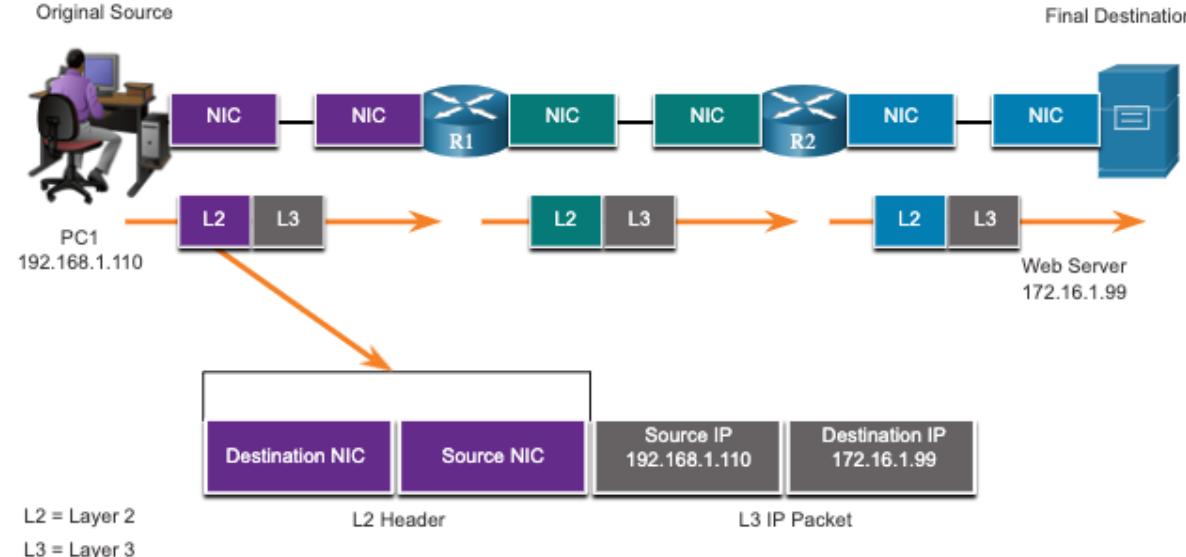
# Veri Bağlantısı Çerçevesi Çerçeve Alanları



Alan	Açıklama
Çerçeve Başlat ve Durdur	Çerçevenin başlangıcını ve sonunu tanımlar
Addresleme	Kaynak ve hedef nodlarını gösterir
Tip	Kapsüllenmiş Katman 3 protokolünü tanımlar
Kontrol	Akış kontrol hizmetlerini tanımlar
Data	Çerçeve yükünü içerir
Hata Tespitı	İletim hatalarını belirlemek için kullanılır

# Veri Bağlantısı Çerçevesi Katman 2 Adresleri

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



**Mantıksal topoloji ve fiziksel ortam, kullanılan veri bağlantı protokolünü belirler:**

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

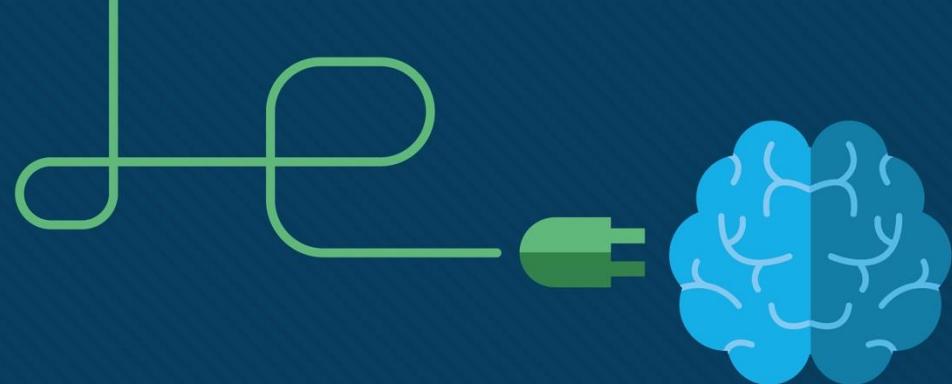
**Her protokol, belirli mantıksal topolojiler için ortam erişim denetimi gerçekleştirir.**

# 6.4 Modül Pratiği ve Quiz

## Bu modülde ne öğrendim?

- OSI modelinin veri bağlantı katmanı (Katman 2), fiziksel ağ için ağ verilerini hazırlar.
- Veri bağlantı katmanı, ağ arayüz kartından (Network Interface Card-NIC) ağ arayüz kartı iletişimine kadar sorumludur.
- IEEE 802 LAN / MAN veri bağlantı katmanı iki alt katmandan oluşur: LLC ve MAC.
- LAN ve WAN ağlarında kullanılan iki tür topoloji fiziksel ve mantıksaldır.
- Üç yaygın fiziksel WAN topolojisi türü şunlardır: noktadan noktaya, hub and spoke ve mesh.
- Yarı çift yönlü iletişim, her seferinde tek yönde veri alışverişesi yapar. Tam çift yönlü, verileri eşzamanlı olarak gönderir ve alır.
- Çekişme tabanlı çoklu erişim ağlarında, tüm düğümler yarı çift yönlü olarak çalışır.
- Çekişmeye dayalı erişim yöntemlerinin örnekleri şunları içerir: veri yolu topolojisi Ethernet LAN'ları için CSMA / CD ve WLAN'lar için CSMA / CA.
- Veri bağlantısı çerçevesinin üç temel bölümü vardır: başlık, data ve trailer.
- Çerçeve alanları şunları içerir: çerçeve başlatma ve durdurma göstergeleri bayrakları, adresleme, tür, kontrol, veri ve hata algılama.
- Veri bağlantı adresleri, fiziksel adresler olarak da bilinir.
- Veri bağlantı adresleri yalnızca çerçevelerin yerel bağlantı teslimi için kullanılır.





# Modül 7: Ethernet Anahtarlama

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

**Modül Başlığı:** Ethernet Anahtarlama

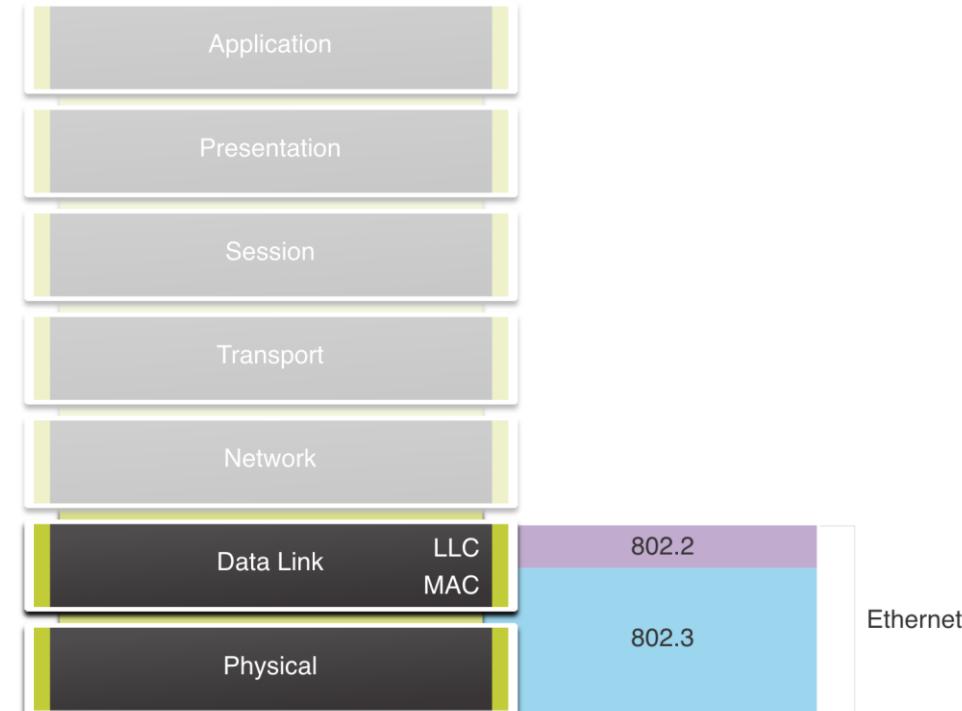
**Modül Hedefi:** Anahtarlı bir ağda Ethernet'in nasıl çalıştığını açıklamak.

Başlık	Hedef
Ethernet Frame	Ethernet alt katmanlarının çerçeve alanlarıyla nasıl ilişkili olduğunu açıklamak
Ethernet MAC Adresi	Ethernet MAC adresini tanımlamak
MAC Adres Tablosu	Bir anahtarın MAC adres tablosunu nasıl oluşturduğunu ve çerçeveleri nasıl ilettiğini açıklamak
Switch Speeds and Forwarding Methods	Katman 2 anahtar bağlantı noktalarında bulunan <u>anahtar yönlendirme yöntemlerini</u> ve <u>bağlantı noktası ayarlarını</u> açıklamak

# 7.1 Ethernet Çerçeveesi

# Ethernet Kapsülleme

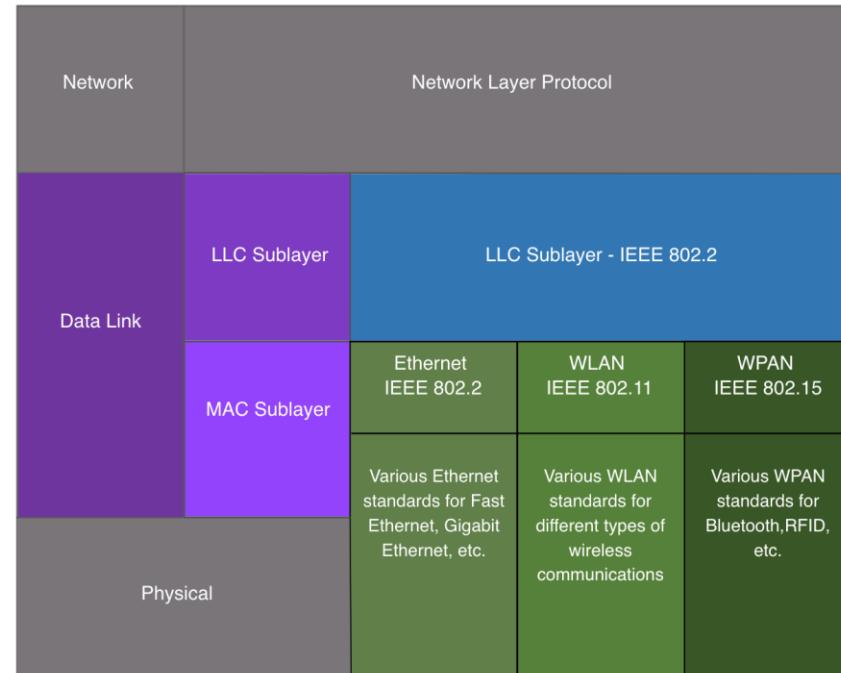
- **Ethernet, veri bağlantı katmanında ve fiziksel katmanda çalışır.**
- **IEEE 802.2 ve 802.3 standartlarında tanımlanan bir ağ teknolojileri ailesidir.**



# Veri Bağlantısı Alt Katmanları

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

- LLC Alt Katmanı:** (IEEE 802.2) Çerçeve için hangi ağ katmanı protokolünün kullanıldığını belirlemek amacıyla çerçeveeye bilgi yerleştirir.
- MAC Alt Katmanı:** (IEEE 802.3, 802.11, veya 802.15) **Veri kapsülleme ve medya erişim kontrolünden** sorumludur ve veri bağlantı katmanı adresleme sağlar.



**MAC alt katmanı, veri kapsüllemeden ve medyaya erişimden sorumludur.**

## **Veri Kapsülleme**

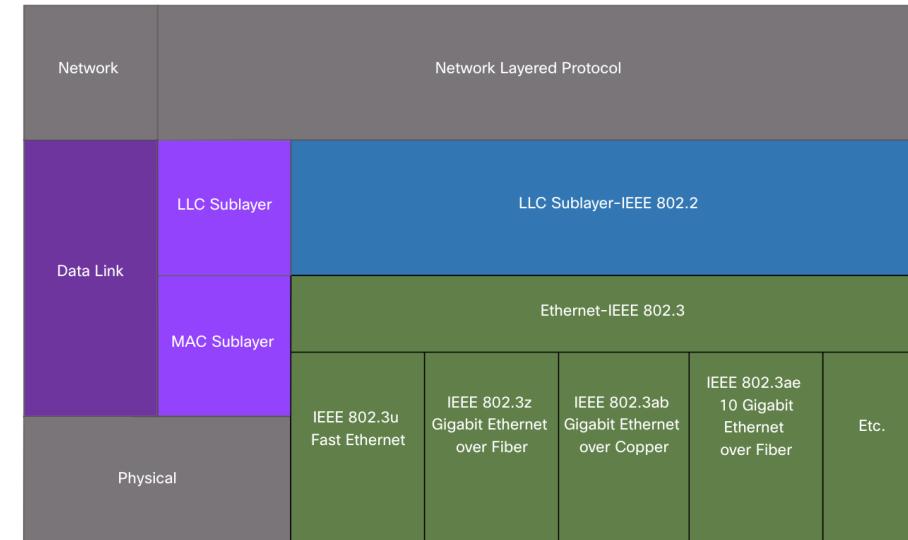
IEEE 802.3 veri kapsülleme şunları içerir:

- 1. Ethernet çerçevesi** - Bu, Ethernet çerçevesinin iç yapısıdır.
- 2. Ethernet Adresleme** - Ethernet çerçevesi, Ethernet çerçevesini Ethernet NIC'den Ethernet NIC'ye aynı LAN üzerinde iletmek için **hem bir kaynak hem de hedef MAC adresi içerir.**
- 3. Ethernet Hata Tespiti**- Ethernet çerçevesi, **hata tespiti için** kullanılan bir **çerçeve kontrol dizisi (FCS)** fragmanı içerir.

# Ethernet Çerçeveleri MAC Alt Katmanı

## Medya Erişimi

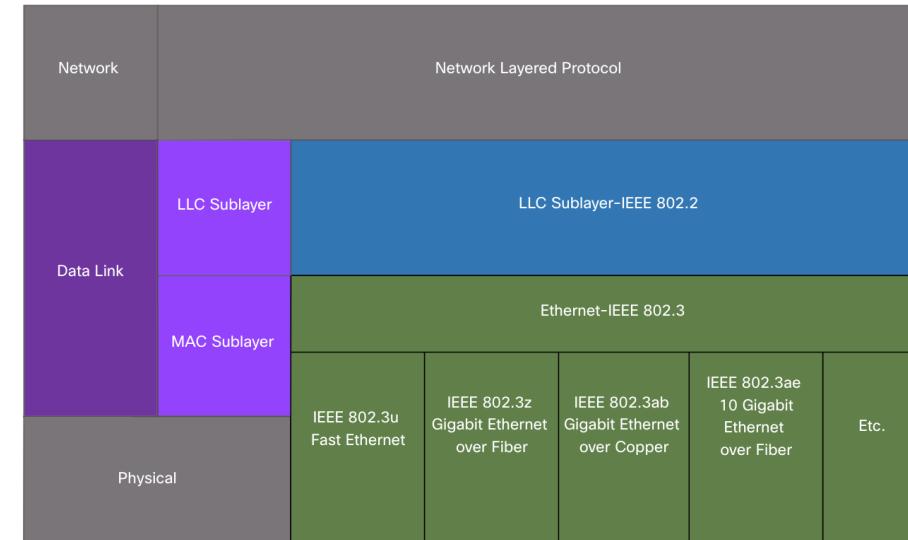
- IEEE 802.3 MAC alt katmanı, **bakır ve fiber** dahil olmak üzere **çeşitli ortam türleri** üzerinden farklı **Ethernet iletişim standartları** için spesifikasyonlar içerir.
- Bir veri yolu **topolojisi** veya hub kullanan eski Ethernet, paylaşılan, yarı çift yönlü bir ortamdır.
- **Yarı çift yönlü bir ortam üzerinden Ethernet, contention tabanlı** erişim yöntemi kullanır, taşıyıcı, çoklu erişim / **çakışma algılaması (CSMA / CD)** kullanır.
- 



# Ethernet Çerçeveleri MAC Alt Katmanı

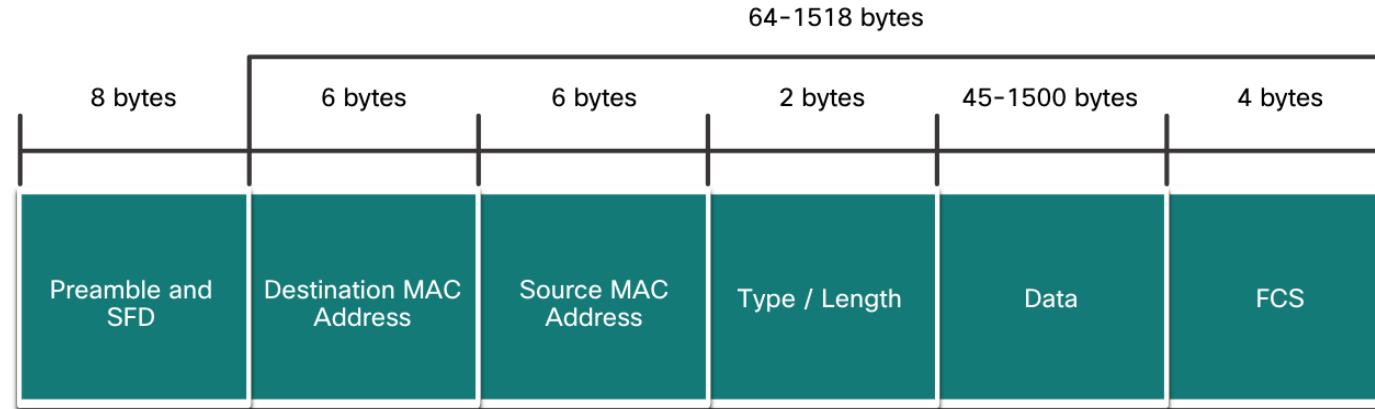
## Medya Erişimi

- Günümüzün **Ethernet LAN'ları tam çift yönlü çalışan anahtarlar kullanır.**
- Ethernet anahtarlarıyla tam çift yönlü iletişim, **CSMA / CD aracılığıyla erişim kontrolü gerektirmez.**



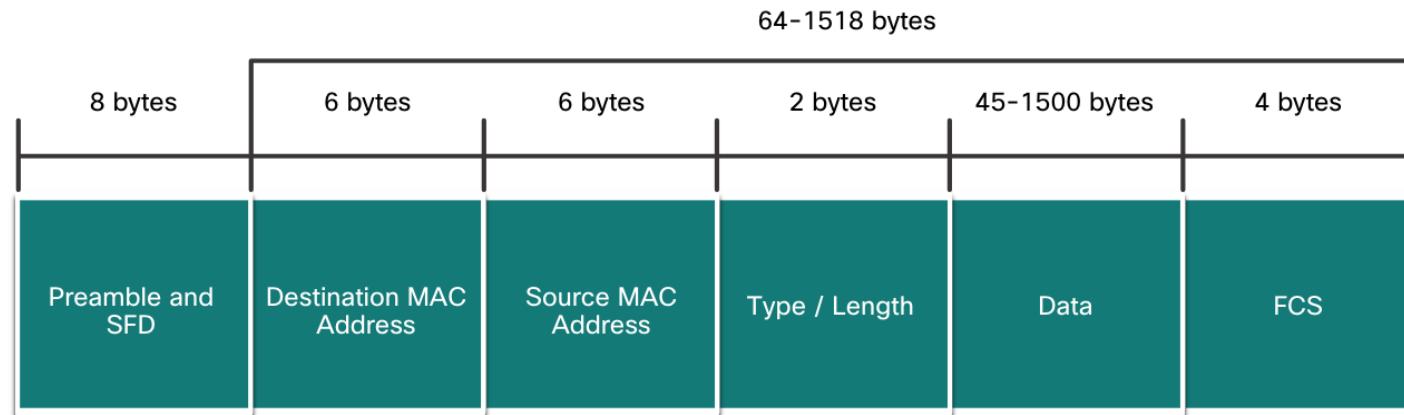
# Ethernet Çerçeve Alanları

- Minimum Ethernet çerçeve boyutu, **64 bayt** ve maksimum **1518 bayttır**.
- Giriş alanı, çerçevenin boyutunu açıklarken **dahil edilmez**.
- 64 bayttan daha kısa herhangi bir çerçeve**, bir "çarpışma parçası" veya "kısa çerçeve" ("collision fragment" or "runt frame") **olarak kabul edilir** ve **otomatik olarak atılır**.
- 1500 bayttan fazla veriye sahip çerçeveler "jumbo" veya "bebek dev çerçeveler" (baby giant frames) **olarak kabul edilir**.**



# Ethernet Çerçeve Alanları

- İletilen bir çerçevenin boyutu minimumdan küçükse veya maksimumdan büyüğe, aıcı cihaz çerçeveyi düşürür.
- Düşen kareler muhtemelen çarpışmaların veya diğer istenmeyen sinyallerin sonucu olacaktır.
- Bu durumda geçersiz sayılırlar.
- Jumbo çerçeveler genellikle çoğu Hızlı Ethernet ve Gigabit Ethernet anahtarı ve NIC tarafından desteklenir.



# Lab – Ethernet Çerçevelerini İncelemek için Wireshark'ı Kullanın

Bu laboratuvara aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Ethernet II Çerçeveşinde Başlık Alanlarını İnceleyin
- Bölüm 2: Ethernet Çerçevelerini Yakalamak ve Analiz Etmek için Wireshark'ı Kullanın

# 7.2 Ethernet MAC Adresleri

# MAC Adresi ve Heksadesimal

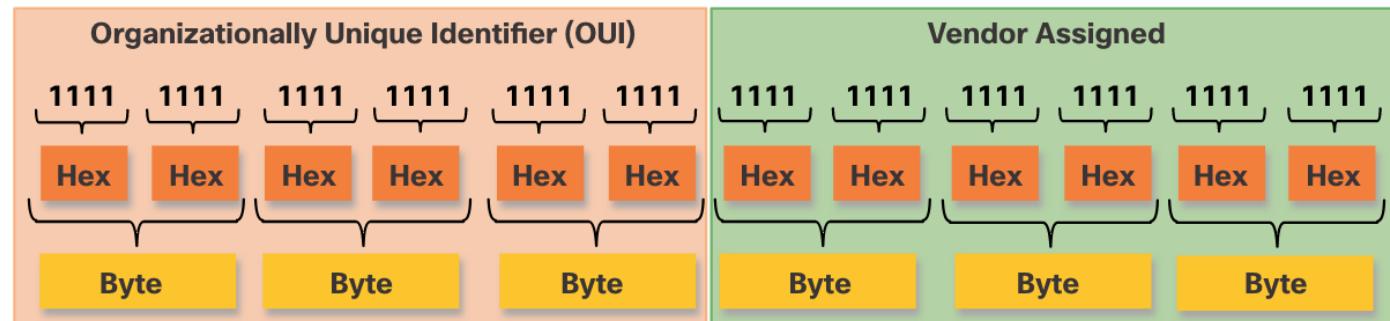
- Bir Ethernet MAC adresi, **12** onaltılık değer kullanılarak ifade edilen **48 bitlik bir ikili değerden oluşur.**
- 8 bitin (bir bayt) ortak bir ikili gruptama olduğu göz önüne alındığında, ikili 00000000 - 11111111, 00 - FF aralığı olarak onaltılık olarak temsil edilebilir,
- Heksadesimal kullanırken, 8 bit gösterimini tamamlamak için her zaman baştaki sıfırlar görüntülenir.
- Örneğin, 0000 1010 ikili değeri onaltılık olarak 0A olarak temsil edilir.

## MAC Adresi ve Heksadesimal

- **Onaltılık sayılar**, dokümantasyonda **ondalık** ve **onaltılık değerleri** **ayırt etmek için** genellikle **0x** (ör. **0x73**) önündeki değerle temsil edilir.
- **Onaltılık ayrıca** bir alt simge 16 veya onaltılık sayı ve ardından bir **H** (ör., **73H**) ile temsil edilebilir.

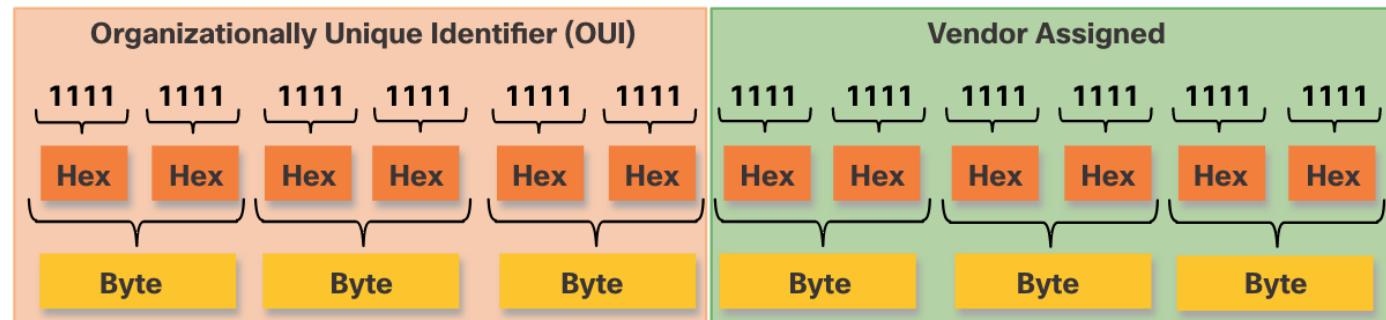
# Ethernet MAC Adresi

- 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 rakam kullanılarak ifade edilen 48 bitlik bir adresidir. Bir bayt 8 bite eşit olduğu için, **bir MAC adresinin 6 bayt uzunluğunda olduğu da söylenebilir.**



# Ethernet MAC Adresi

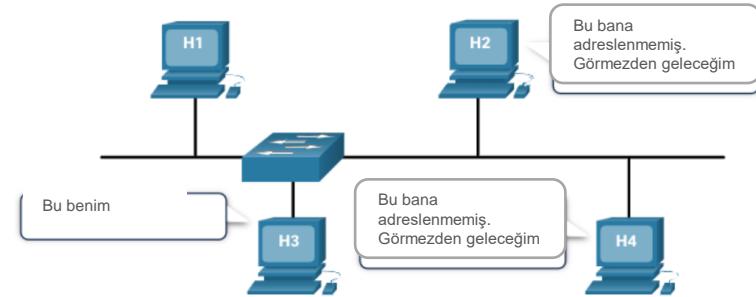
- **Tüm MAC adresleri** Ethernet cihazına veya Ethernet arayüzüne özel olmalıdır.
- Bunu sağlamak için, Ethernet cihazları satan tüm satıcıların, organizasyonel olarak **benzersiz tanımlayıcı (OUI)** adı verilen benzersiz bir 6 onaltılık (yani 24 bit veya 3 bayt) kod elde etmek için **IEEE'ye kaydolması gereklidir**.
- **Bir Ethernet MAC adresi**, 6 onaltılık satıcı OUI kodunun ardından **6 onaltılık satıcı tarafından atanmış değerden** oluşur.



# Ethernet MAC Adresleri Çerçeve İşleme

- Bir cihaz bir Ethernet ağına bir mesaj iletirken, Ethernet başlığı bir **Kaynak MAC adresi** ve bir **Hedef MAC adresi** içerir.
- Bir NIC bir Ethernet çerçevesi aldığında, RAM'de depolanan fiziksel MAC adresiyle eşleşip eşleşmediğini görmek için hedef MAC adresini inceler.
- Eşleşme yoksa cihaz çerçeveyi atar.
- Bir eşleşme varsa, çerçeveyi kapsülleme işleminin gerçekleştiği OSI katmanlarından geçirir.

Variş Adresi	Kaynak Adresi	Veri
Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		

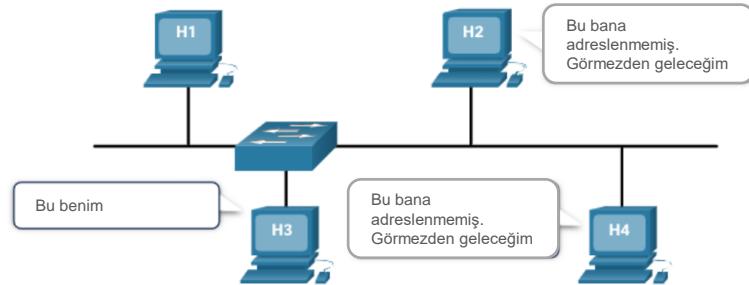


# Ethernet MAC Adresleri Çerçeve İşleme

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

- Bir Ethernet çerçevesinin kaynağı veya hedefi olan herhangi bir aygit, bir Ethernet NIC'ye ve dolayısıyla bir MAC adresine sahip olacaktır.
- Buna iş istasyonları, sunucular, yazıcılar, mobil cihazlar ve yönlendiriciler dahildir.

Varış Adresi	Kaynak Adresi	Veri
Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		

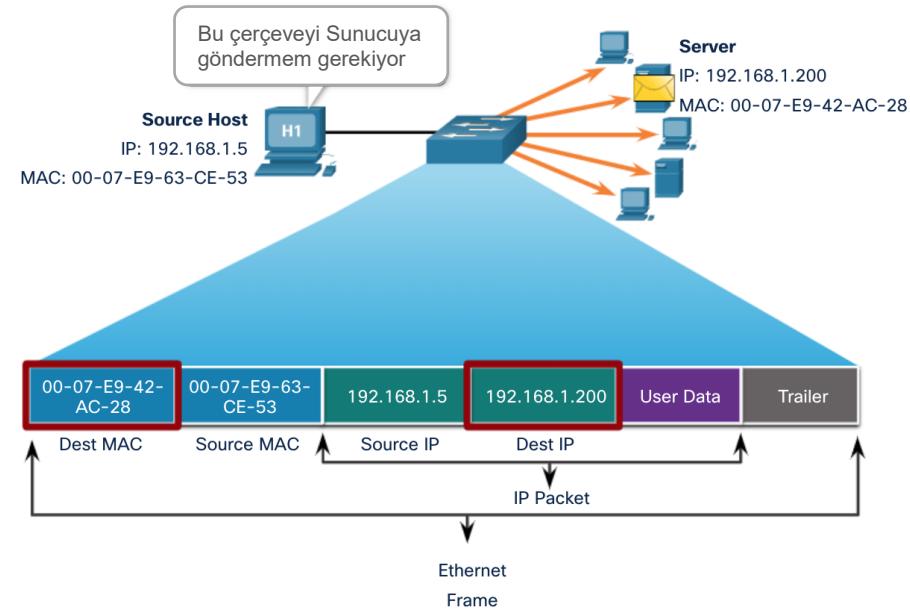


# Tek noktaya yayın (Unicast) MAC Adresi

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

- Tek noktaya yayın MAC adresi, **tek bir iletim cihazından tek bir hedef cihaza çerçeve gönderildiğinde kullanılan benzersiz adresdir.**

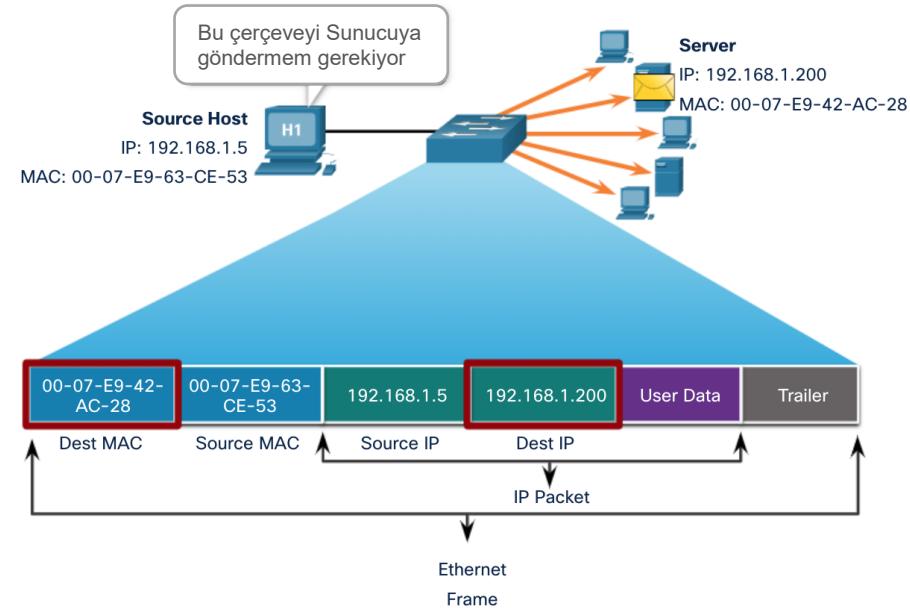
**Not:** Kaynak MAC adresi her zaman tek noktaya yayın olmalıdır (Unicast).



# Tek noktaya yayın (Unicast) MAC Adresi

- 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 Keşfi (Neighbor Discovery/ND)** olarak bilinir.

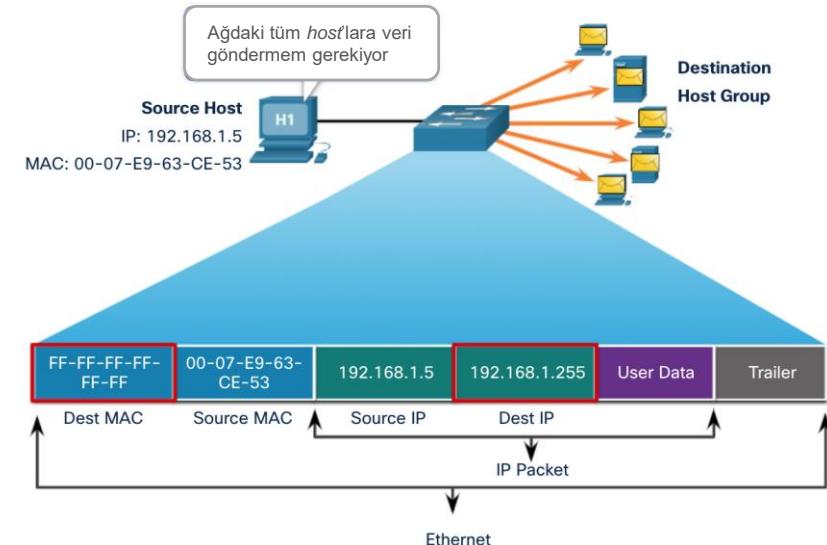
**Not:** Kaynak MAC adresi her zaman tek noktaya yayın olmalıdır (Unicast).



# Yayın MAC Adresi (*Broadcast MAC Address*)

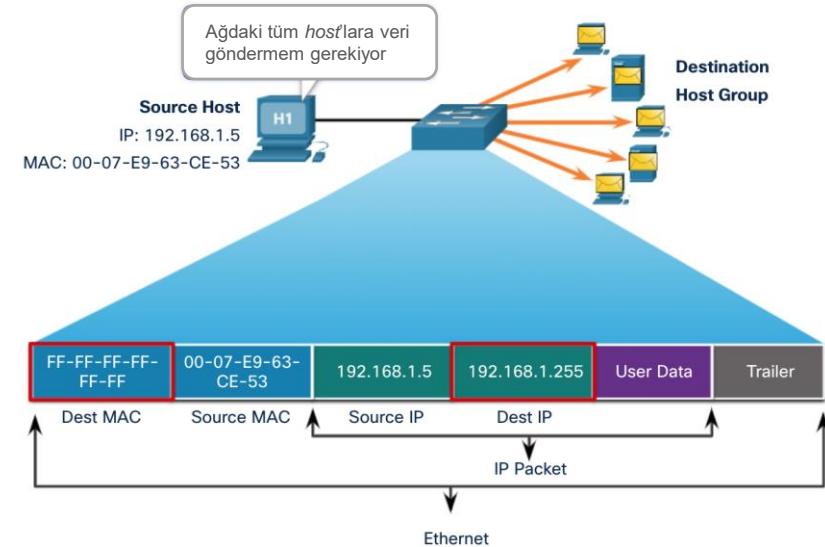
Ethernet LAN üzerindeki her cihaz tarafından bir Ethernet yayın çerçevesi alınır ve işlenir. Bir Ethernet yayınının özellikleri aşağıdaki gibidir:

- Onaltılık olarak **FF-FF-FF-FF-FF-FF**'nin **hedef MAC adresi vardır** (ikili olarak 48 tane).
- Gelen bağlantı noktası dışındaki tüm Ethernet anahtarı bağlantı noktalarının dışında su basmıştır.
- Bir yönlendirici tarafından iletilmez.



# Yayın MAC Adresi (*Broadcast MAC Address*)

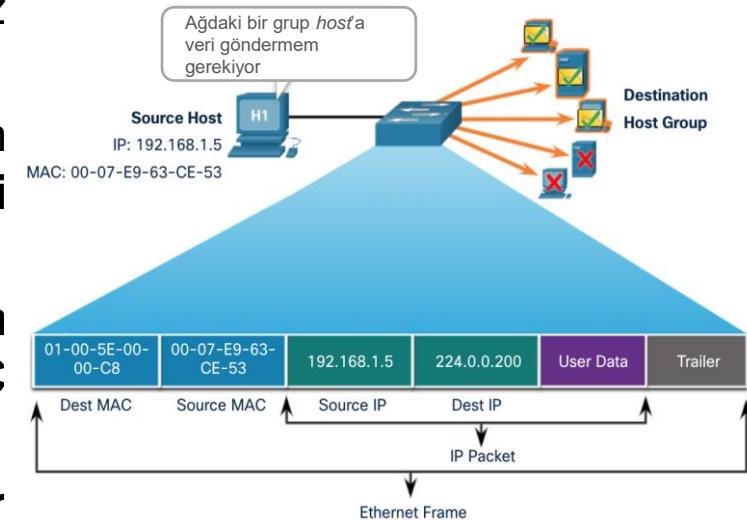
- Kapsüllenmiş veriler bir **IPv4 yayın paketi**yse, bu, paketin ana bilgisayar bölümünde tümü (1'ler) olan bir hedef IPv4 adresi içeriği anlamına gelir.
- Adreste bu numaralandırma, o yerel ağdaki (yayın etki alanı/ *broadcast domain*) **tüm ana bilgisayarların paketi alacağı ve işleyeceği anlamına gelir.**



# Çok noktaya yayın MAC Adresi (*Multicast MAC Address*)

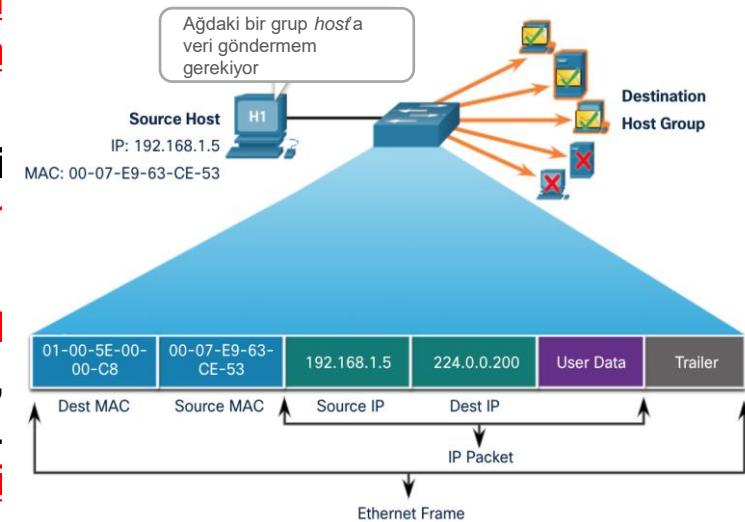
Bir Ethernet çok noktaya yayın çerçevesi, aynı çok noktaya yayın grubuna ait bir grup cihaz tarafından alınır ve işlenir.

- Kapsüllenmiş veri bir IPv4 çok noktaya yayın paketi olduğunda **01-00-5E hedef MAC adresi** vardır.
- Kapsüllenmiş veri bir IPv6 çok noktaya yayın paketi olduğunda **33-33 hedef MAC adresi** vardır.
- Kapsüllenmiş verilerin IP olmadığı zamanlar için **Spanning Tree Protocol (STP)** gibi başka ayrılmış çok noktaya yayın hedef MAC adresleri vardır.



# Çok noktaya yayın MAC Adresi (*Multicast MAC Address*)

- Anahtar çok noktaya yayın gözetleme için yapılandırılmadığı sürece, gelen bağlantı noktası dışındaki tüm Ethernet anahtarı bağlantı noktalarının dışında kalır.**
- Yönlendirici, çoklu yayın paketlerini yönlendirecek şekilde yapılandırılmadıkça, 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 gerektir.**



# Lab – Ağ Cihazı MAC Adreslerini Görüntüle

Bu laboratuvara aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Topolojiyi Kurun ve Cihazları Başlatın
- Bölüm 2: Cihazları Yapılandırın ve Bağlantıyı Doğrulayın
- Bölüm 3: Ethernet MAC Adreslerini Görüntüle, Tanımla ve Analiz Et

# 7.3 MAC Adres Tablosu

# MAC Adres Tablosu Anahtarlama Temel Bilgiler

- Bir Katman 2 Ethernet anahtarı, yönlendirme kararları vermek için **Katman 2 MAC adreslerini kullanır.**
- IPv4 paketi, ARP mesajı veya IPv6 ND paketi gibi çerçeveden veri bölümünde taşınan verilerin (protokol) tamamen farkında değildir.
- Anahtar, yönlendirme kararlarını yalnızca **Katman 2 Ethernet MAC adreslerine** göre verir.
- Bir Ethernet anahtarı, **gelen bağlantı noktası dışındaki tüm bağlantı noktalarını** bit tekrarlayan eski Ethernet hub'larından farklı olarak, her çerçeve için bir **yönlendirme kararı vermek üzere MAC adres tablosunu inceler.**
- Bir anahtar açıldığında, **MAC adres tablosu boştur.**

**Not:** MAC adres tablosu bazen bir içerik adreslenebilir bellek (content addressable memory / CAM) tablosu olarak adlandırılır.

# Anahtarlama Öğrenme ve Yönlendirme

## Kaynak MAC Adresini İnceleyin (Öğrenme / Learn)

- ❖ 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.

- ❖ **Kaynak MAC adresi yoksa**, **gelen bağlantı noktası numarasıyla birlikte tabloya eklenir.**
- ❖ **Kaynak MAC adresi mevcutsa**, anahtar bu giriş için **yenileme zamanlayıcısını günceller**. Varsayılan olarak, **çoğu Ethernet anahtarı tablodaki bir giriş 5 dakika tutar.**

**Not:** 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.**

# Anahtarlama Öğrenme ve Yönlendirme

## Hedef MAC Adresini Bulun (*İletme / Forward*)

- ❖ 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 noktasından dışarı ileticektir.
- ❖ **Hedef MAC adresi tabloda değilse**, anahtar, çerçeveyi gelen bağlantı noktası dışındaki tüm bağlantı noktalarını ileticektir.

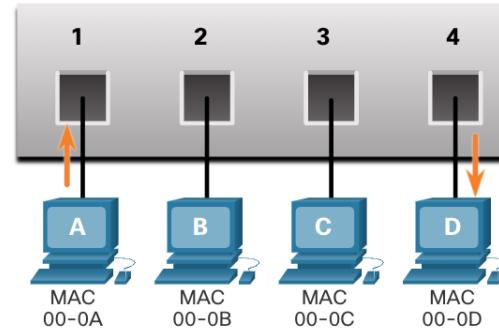
Buna bilinmeyen tek noktaya yayın denir.

**Not: Hedef MAC adresi bir yayın veya çok noktaya yayın ise, cerçeve de gelen bağlantı noktası dışındaki tüm bağlantı noktalarının dışına taşınır.**

# Filtering Frames (*Filtering Frames*)

- ❖ Bir anahtar farklı cihazlardan kareler aldığımda, her çerçevenin kaynak MAC adresini inceleyerek MAC adres tablosunu doldurabilir.
- ❖ Anahtarın MAC adres tablosu, hedef MAC adresini içerdiginde, çerçeveyi filtreleyebilir ve tek bir bağlantı noktasını iletebilir.

MAC Address Table	
Port	MAC Address
1	00-0A
4	00-0D



# Video – Bağlı Anahtarlardaki MAC Adresi Tabloları

Bu video aşağıdakileri kapsamaktadır:

- Anahtarlar MAC adres tablolarını nasıl oluşturur?
- İleri çerçeveleri MAC adres tablolarının içeriğine göre nasıl değiştirir?

# Video – Çerçeveyi Varsayılan Ağ Geçidine Gönderme

Bu video aşağıdakileri kapsamaktadır :

- Hedef AMC adresi anahtarın MAC adres tablosunda listelenmediğinde bir anahtar ne yapar.
- Kaynak AMC adresi anahtarın MAC adres tablosunda listelenmediğinde bir anahtar ne yapar?

# Lab – MAC Adresi Değiştirme Tablosunu Görüntüleme

Bu laboratuvara aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Ağ Oluşturma ve Yapılandırma
- Bölüm 2: Anahtar MAC Adres Tablosunu İnceleme

# 7.4 Anahtar Hızları ve Yönlendirme Yöntemleri

## Cisco Anahtarlarında Çerçeve Yönlendirme Yöntemleri

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

- ❖ **Depola ve ilet anahtarlama (*Store-and-forward switching*)** - Bu çerçeve yönlendirme yöntemi, **tüm çerçeveyi alır** ve Cyclic Redundancy Check (Döngüsel Artıklık Denetimi) hesaplar.
- **CRC geçerliyse**, anahtar, giden arabirimini belirleyen **hedef adresi** arar.
- Ardından çerçeve doğru bağlantı noktasından dışarı ilettilir.
- ❖ **Kesmeli geçiş (*Cut-through switching*)** - Bu çerçeve yönlendirme yöntemi, **çerçeveyi tamamen alınmadan önce iletir**.
- En azından **çerçevenin hedef adresi, çerçevenin iletilebilmesi için okunmalıdır**.

## Cisco Anahtarlarında Çerçeve Yönlendirme Yöntemleri

- **Depola ve ilet anahtarlamanın büyük bir avantajı**, çerçeveyi yaymadan önce bir çerçevede hata olup olmadığını belirlemesidir.
- Bir çerçevede bir hata algılandığında, anahtar çerçeveyi atar.
- Hatalı karelerin atılması, bozuk veriler tarafından tüketilen bant genişliğini miktaranı azaltır.
- **Depola ve ilet anahtarlama**, trafik önceliklendirmesi için çerçeve sınıflandırmasının gerekli olduğu birleşik ağlarda hizmet kalitesi (QoS) analizi için gereklidir.
- **Örneğin, IP üzerinden ses (VoIP) veri akışlarının web'de gezinme trafiğine göre önceliği olmalıdır.**

## Kesmeli geçiş (*Cut-through switching*)

**Kesmeli anahtarlamada (*Cut-through switching*), anahtar, aktarım tamamlanmasa bile, alınır alınmaz veriye etki eder.**

Anahtar, verileri hangi bağlantı noktasına iletmesi gerektiğini belirleyebilmesi için hedef MAC adresini okumaya yetecek kadar çerçeveyi arabelleğe alır.

**Anahtar, çerçeve üzerinde herhangi bir hata kontrolü gerçekleştirmez.**

**Geçiş anahtarlamanın iki çeşidi vardır:**

- **Fast-forward anahtarlama** - Hedef adresi okuduktan hemen sonra bir paketi ileterek en düşük gecikme seviyesini sunar.
- **Hızlı ileri anahtarlama**, *tüm paket alınmadan önce iletmeye başladığından*, paketlerin hatalarla iletildiği zamanlar olabilir.
- **Hedef NIC, hatalı paketi aldıktan sonra atar.**
- **Hızlı ileri anahtarlama**, tipik geçiş yöntemidir.

## Kesmeli geçiş (*Cut-through switching*)

- **Fragment-free anahtarlama** - Store-and-forward anahtarlamanın yüksek gecikmesi ve yüksek bütünlüğü ile hızlı ileri anahtarlamanın düşük gecikme süresi ve azaltılmış bütünlüğü arasında bir uzlaşma olan anahtar, iletmeden önce çerçevenin ilk 64 baytı üzerinde bir hata kontrolü gerçekleştirir ve depolar.
- Çoğu ağ hatası ve çakışması ilk 64 bayt sırasında meydana geldiğinden, bu, çerçeveyi iletmeden önce bir çakışmanın olmamasını sağlar.

# Anahtarlarda Hafıza Tamponlama (Memory Buffering)

Bir Ethernet anahtarı, çerçeveleri iletmenden önce veya **hedef bağlantı noktası tıkanıklık** nedeniyle meşgul olduğunda bir arabelleğe alma tekniği kullanabilir.

Method	Tanım
<b>Port bazlı hafıza (Port-based memory)</b>	<ul style="list-style-type: none"> <li>Çerçeve, belirli gelen ve giden bağlantı noktalarına bağlı kuyruklarda saklanır.</li> <li><b>Bir çerçeve, yalnızca kuyruktaki ilerideki tüm çerçeveler başarıyla iletildiğinde giden bağlantı noktasına iletilir.</b></li> <li>Meşgul bir hedef bağlantı noktası nedeniyle tek bir çerçevenin bellekteki tüm çerçevelerin iletimini geciktirmesi mümkündür.</li> <li>Bu gecikme, diğer çerçeveler açık hedef bağlantı noktalarına iletilse bile oluşur..</li> </ul>
<b>Paylaşılan hafıza (Shared memory)</b>	<ul style="list-style-type: none"> <li>Tüm çerçeveleri, tüm anahtar bağlantı noktaları tarafından paylaşılan <b>ortak bir bellek arabelleğine yatar</b> ve bir bağlantı noktasının gerektirdiği arabellek <b>belleği miktarı dinamik olarak tahsis edilir</b>.</li> <li>Arabellekteki çerçeveler, bir paketin bir bağlantı noktasında alınmasını ve daha sonra başka bir bağlantı noktasına taşınmadan <b>farklı bir kuyruğa iletilmesini sağlayan hedef bağlantı noktasına dinamik olarak bağlanır</b>.</li> </ul>

- Paylaşilan bellek arabelleği, daha az sayıda atlanan çerçeve ile iletilebilen daha büyük çerçevelerle de sonuçlanır.** Bu, farklı bağlantı noktalarında farklı veri hızlarına izin veren asimetrik anahtarlama önemlidir. **Bu nedenle, belirli bağlantı noktalarına (örneğin, sunucu bağlantı noktası) daha fazla bant genişliği tahsis edilebilir.**

## Çift Yönlü ve Hız Ayarları (*Duplex and Speed Settings*)

Bir anahtardaki en temel ayarlardan ikisi, **her bir anahtar bağlantı noktası** için **bant genişliği ("hız")** ve **çift yönlü ayarlarıdır.**

**Çift yönlü ve bant genişliği ayarlarının, anahtar bağlantı noktası ile bağlı cihazlar arasında eşleşmesi çok önemlidir.**

Bir Ethernet ağında iletişim için kullanılan **iki tür çift yönlü ayar vardır:**

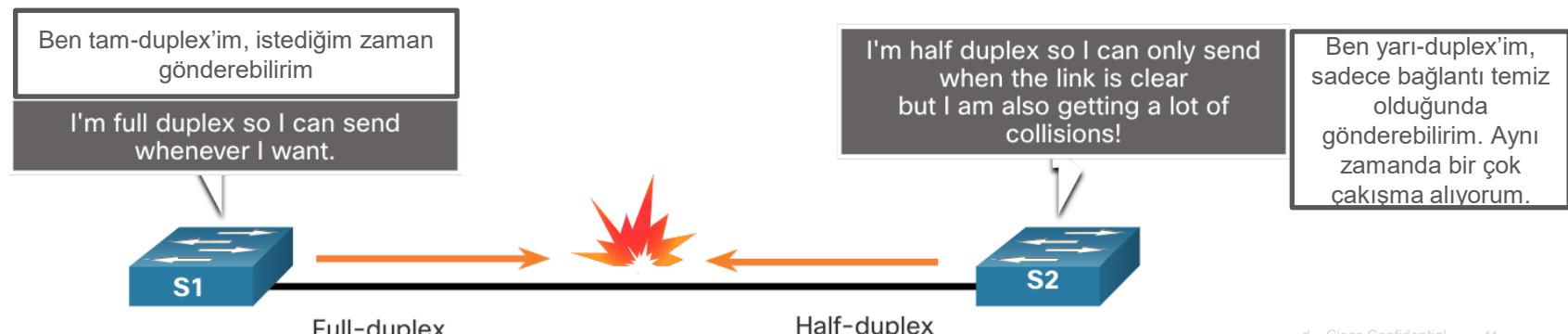
- **Tam-duplex** - Bağlantının her iki ucu aynı anda gönderip alabilir.
- **Yarı-duplex** - Tek seferde bağlantının yalnızca bir ucu gönderebilir.

*Autonegotiation*, çoğu Ethernet anahtarı ve NIC'de bulunan isteğe bağlı bir işlevdir. İki cihazın en iyi hız ve çift yönlü yetenekleri otomatik olarak ayarlamasını sağlar.

**Not:** Gigabit Ethernet bağlantı noktaları yalnızca tam çift yönlü çalışır.

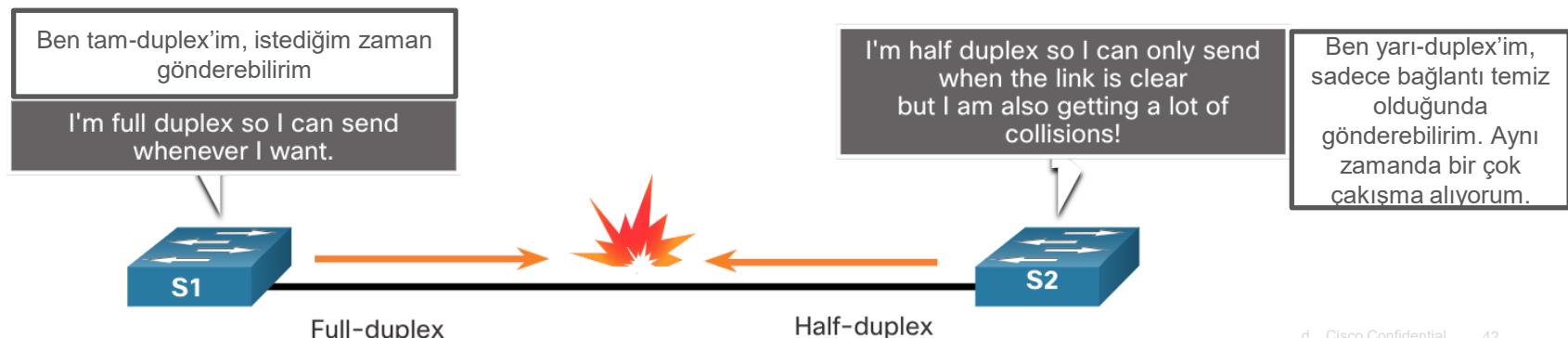
## Çift Yönlü ve Hız Ayarları (*Duplex and Speed Settings*)

- Çift yönlü uyumsuzluk (*Duplex mismatch*), 10/100 Mbps Ethernet bağlantılarındaki performans sorunlarının en yaygın nedenlerinden biridir.
- Bağlantı üzerindeki bir bağlantı noktası yarı çift yönlü çalışırken, diğer bağlantı noktası tam çift yönlü çalışırken oluşur.



## Çift Yönlü ve Hız Ayarları (*Duplex and Speed Settings*)

- Bu, bir bağlantıdaki bağlantı noktalarından biri veya her ikisi de sıfırlandığında meydana gelebilir ve otomatik anlaşma süreci, her iki bağlantı ortağının da aynı yapılandırmaya sahip olmasıyla sonuçlanmaz.
- Kullanıcılar bir bağlantının bir tarafını yeniden yapılandırip diğerini yeniden yapılandırmayı unuttuğunda da ortaya çıkabilir.
- **Bağlantının her iki tarafında da özerk pazarlık açık olmalı veya her iki tarafta da devre dışı bırakılmalıdır.**
- En iyi uygulama, her iki Ethernet anahtarı bağlantı noktasını **tam çift yönlü olarak yapılandırmaktır.**



### Auto-MDIX

Cihazlar arasındaki bağlantılar bir zamanlar ya **bir çapraz** ya da **düz kablo kullanımını gerektiriyordu**.

Gerekli kablo türü, birbirine bağlanan cihazların türüne bağlıdır.

**Not:** Yönlendirici ile ana bilgisayar **arasındaki doğrudan bağlantı**, yönlendiriciler arasında ise **çapraz bağlantı** gerektirir.

- Çoğu anahtar cihazı artık otomatik orta bağımlı arabirim geçisi (otomatik MDIX) özelliğini desteklemektedir.
- Etkinleştirildiğinde, anahtar bağlantı noktasına takılı kablo tipini otomatik olarak algılar ve arayüzleri buna göre yapılandırır.

# Auto-MDIX

- Otomatik MDIX (Ortam bağımlı arayüz geçişi) özelliği, Cisco IOS Sürüm 12.2 (18) SE veya üzerini çalıştırılan **anahtarlarda varsayılan olarak etkindir**.
- **Ancak özellik devre dışı bırakılabilir.**
- Bu nedenle, **her zaman doğru kablo tipini kullanmalı ve auto-MDIX özelliğine güvenmemelisiniz.**
- Auto-MDIX, **mdix auto interface configuration** komutu kullanılarak yeniden etkinleştirilebilir.

# 7.5 Modül Sınavı

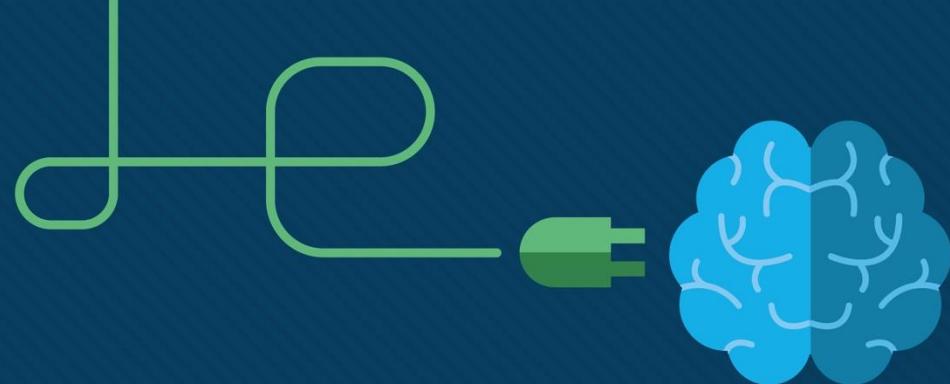
## Bu modülde ne öğrendim?

- Ethernet, veri bağlantı katmanında ve fiziksel katmanda çalışır. Ethernet standartları hem Katman 2 protokollerini hem de Katman 1 teknolojilerini tanımlar.
- Ethernet, çalışmak için veri bağlantı katmanının LLC ve MAC alt katmanlarını kullanır.
- Ethernet çerçeve alanları şunlardır: giriş ve başlangıç çerçeve sınırlayıcı, hedef MAC adresi, kaynak MAC adresi, EtherType, veri ve FCS.
- MAC adresleme, OSI modelinin veri bağlantı katmanında cihaz tanımlama için bir yöntem sağlar.
- Ethernet MAC adresi, 12 onaltılık rakam veya 6 bayt kullanılarak ifade edilen 48 bitlik bir adresdir.
- Bir cihaz bir Ethernet ağına bir mesaj iletirken, Ethernet başlığı kaynak ve hedef MAC adreslerini içerir. Ethernet'te, Katman 2 tek noktaya yayın, yayın ve çok noktaya yayın iletişimleri için farklı MAC adresleri kullanılır.

## Bu modülde ne öğrendim?

- Bir Katman 2 Ethernet anahtarı, yönlendirme kararlarını yalnızca Katman 2 Ethernet MAC adreslerine göre verir.
- Anahtar, bir bağlantı noktasından alınan çerçevelerin kaynak MAC adresini inceleyerek MAC adres tablosunu dinamik olarak oluşturur.
- Anahtar, çerçevedeki hedef MAC adresi ile MAC adres tablosundaki bir giriş arasında bir eşleşme arayarak çerçeveleri ileter.
- Anahtarlar, ağ bağlantı noktaları arasında veri geçisi yapmak için aşağıdaki yönlendirme yöntemlerinden birini kullanır: sakla ve ilet anahtarlama veya geçiş anahtarlama. Kesmeli anahtarlamanın iki çeşidi hızlı ileri ve parça içermez.
- İki bellek tamponlama yöntemi bağlantı noktası tabanlı bellek ve paylaşılan bellektir.
- Bir Ethernet ağında iletişim için kullanılan iki tür çift yönlü ayar vardır: tam çift yönlü ve yarı çift yönlü.





# Modül 8: Ağ Katmanı

Introduction to Networks v7.0  
(ITN)



# Modül 8: Konular

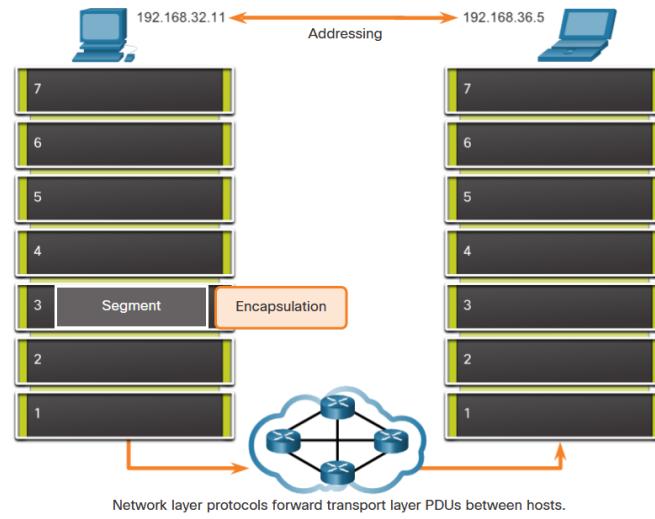
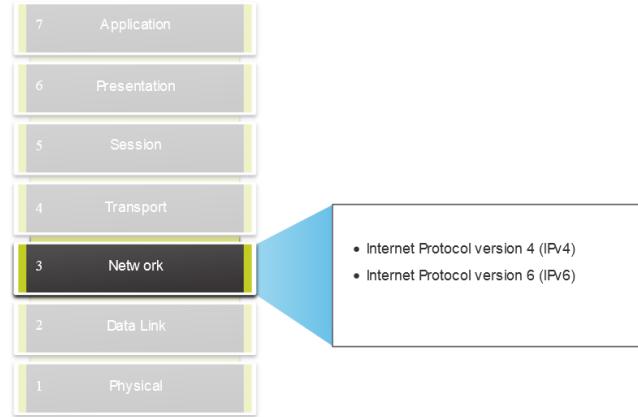
Bu modülde ne öğreneceğim?

Konu Başlığı	Konu Amacı
Ağ Katmanı Özellikleri	Ağ katmanının güvenilir iletişim için IP protokollerini nasıl kullandığını açıklayın.
IPv4 Paketi	IPv4 paketindeki ana başlık alanlarının rolünü açıklayın
IPv6 Paketi	IPv6 paketindeki ana başlık alanlarının rolünü açıklayın
Yönlendiriciler nasıl barındırılır?	Ağ cihazlarının paketleri bir hedef ağa yönlendirmek için yönlendirme tablolarını nasıl kullandığını açıklayın.
Router Yönlendirme Tabloları	Bir yönlendiricisinin yönlendirme tablosundaki alanların işlevini açıklayın.

# 8.1 Ağ Katmanları Özellikleri

## Ağ Katmanı

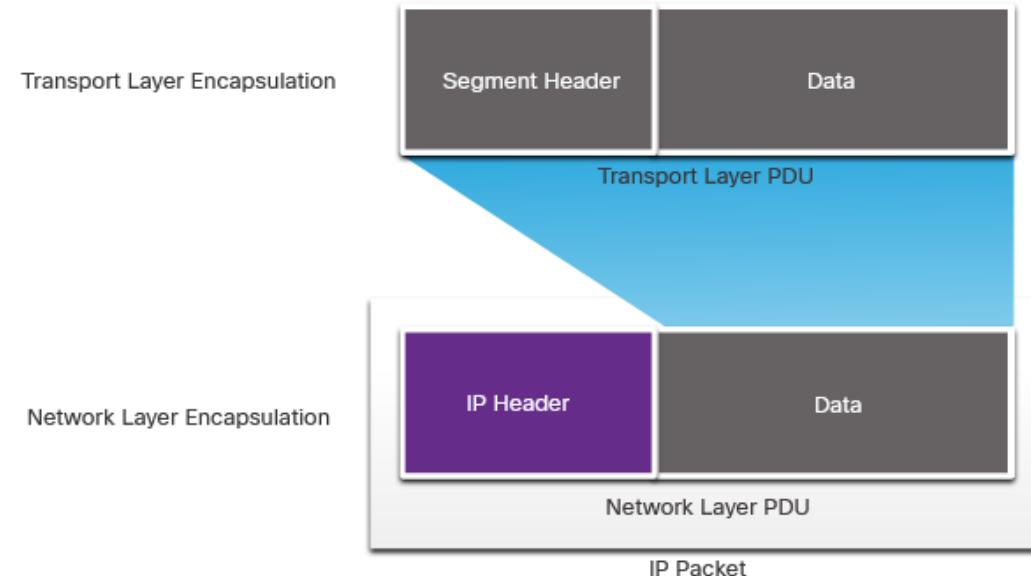
- Uç cihazların veri alışverişini yapmasına izin veren hizmetler sağlar.
- IP version 4 (IPv4) and IP version 6 (IPv6) temel ağ katmanı iletişim protokolleridir.
- Ağ katmanı dört temel işlemi gerçekleştirir:
  1. Uç cihazları adresleme
  2. Kapsülleme (Encapsulation)
  3. Yönlendirme (Routing)
  4. Kapsül açma (De-encapsulation)



## IP Kapsülleme

- IP, taşıma katmanı segmentini kapsüller.
- IP, IPv4 veya IPv6 paketini kullanabilir ve katman 4 segmentini etkilemez.
- IP paketi, ağı geçerken tüm 3. katman cihazları tarafından incelenir.
- IP adresleme kaynaktan hedefe değişmez.

**Not:** NAT adreslemeyi değiştirecektir, bu konu ileriki modülde anlatılacaktır.



# Ağ Katmanı Özellikleri

## IP'nin Özellikleri

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

- **Bağlantısız**
- **En iyi çaba**
- **Medyadan bağımsız**

# Bağlantısız

IP bağlantısızdır.

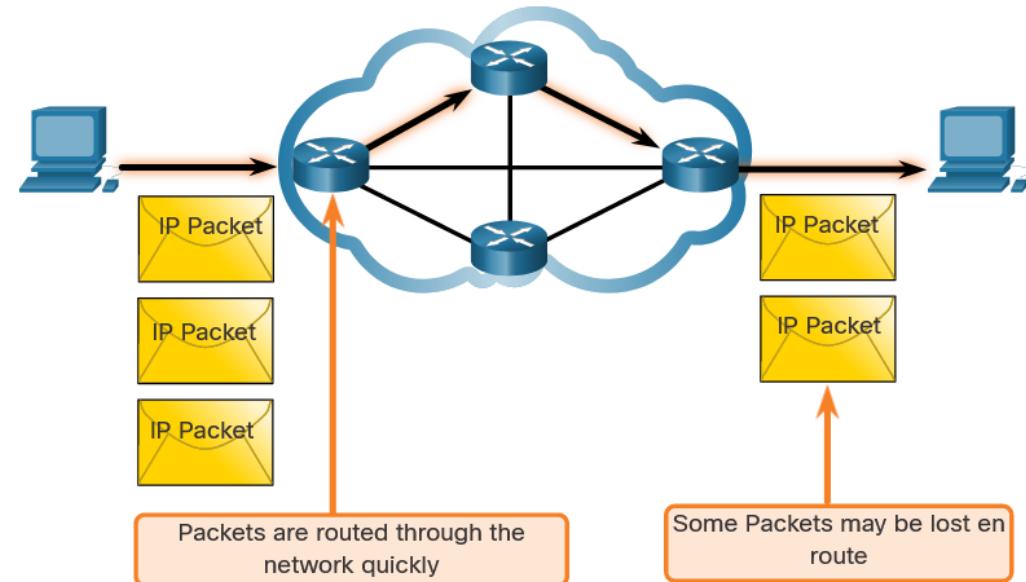
- IP, paketi göndermeden önce hedef ile bağlantı kurmaz.
- Gerekli kontrol bilgisi (senkronizasyonlar, onaylar, vb.) yoktur.
- Hedef ulaştığında paketi alacaktır, ancak **IP tarafından ön bildirim gönderilmez.**
- **Bağlantı yönelimli trafiğe ihtiyaç varsa**, bunu başka bir protokol gerçekleştirecektir (tipik olarak taşıma katmanındaki TCP).



## En iyi çaba

IP en iyi çabasıdır.

- IP, paketin teslimini garanti etmez.
- Alınmayan verileri yeniden gönderecek bir mekanizma olmadığı için IP ek yükü azaltır.
- IP onay beklemez.
- IP diğer cihazın çalışıp çalışmadığını veya paketi alıp almadığını bilmez.



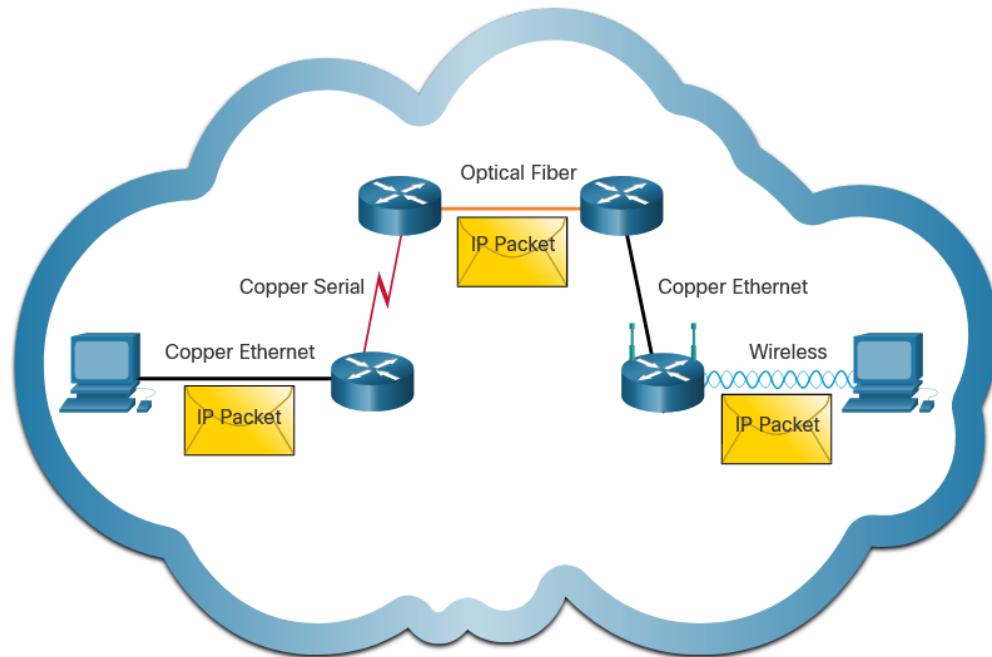
# Medyadan Bağımsız

IP güvenilmezdir:

- Teslim edilmeyen veya bozuk paketleri yönetemez veya düzeltmez.
- Bir hatadan sonra IP yeniden iletilemez.
- IP, sıradan çıkış paketleri yeniden düzenleyemez.
- IP, bu işlevler için diğer protokollere güvenmelidir

IP medyadan bağımsızdır:

- **IP**, veri bağlantı katmanında gereken çerçeve türü veya fiziksel katmandaki ortam türü ile ilgilenmez.
- IP, herhangi bir ortam türü üzerinden gönderilebilir: **bakır**, **fiber** veya **kablosuz**.



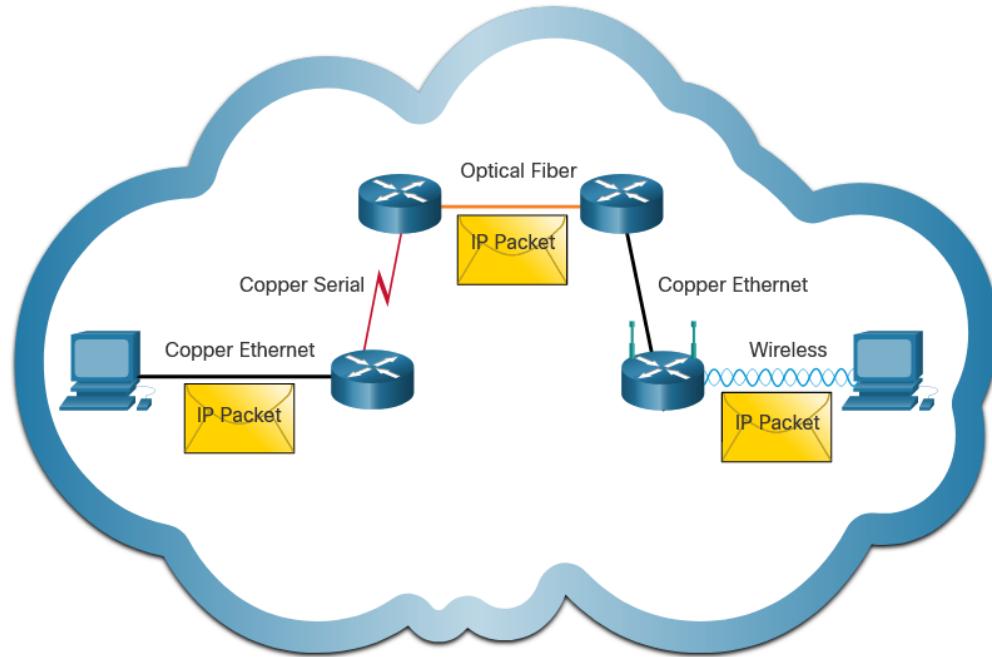
# Medyadan Bağımsız (devamı)

Ağ katmanı Maximum Transmission Unit (MTU)'i kurar.

- 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 ayırmasıdır.

- Parçalanma gecikmeye neden olur.
- IPv6 paketleri parçalamaz.
- Örnek: Yönlendirici, Ethernet'ten daha küçük MTU'ya sahip yavaş bir WAN'a geçer



# 8.2 IPv4 Paketi

## IPv4 Paket Başlığı

IPv4 ağ katmanı için birincil iletişim protokolüdür.

**Ağ başlığının bir çok amacı vardır:**

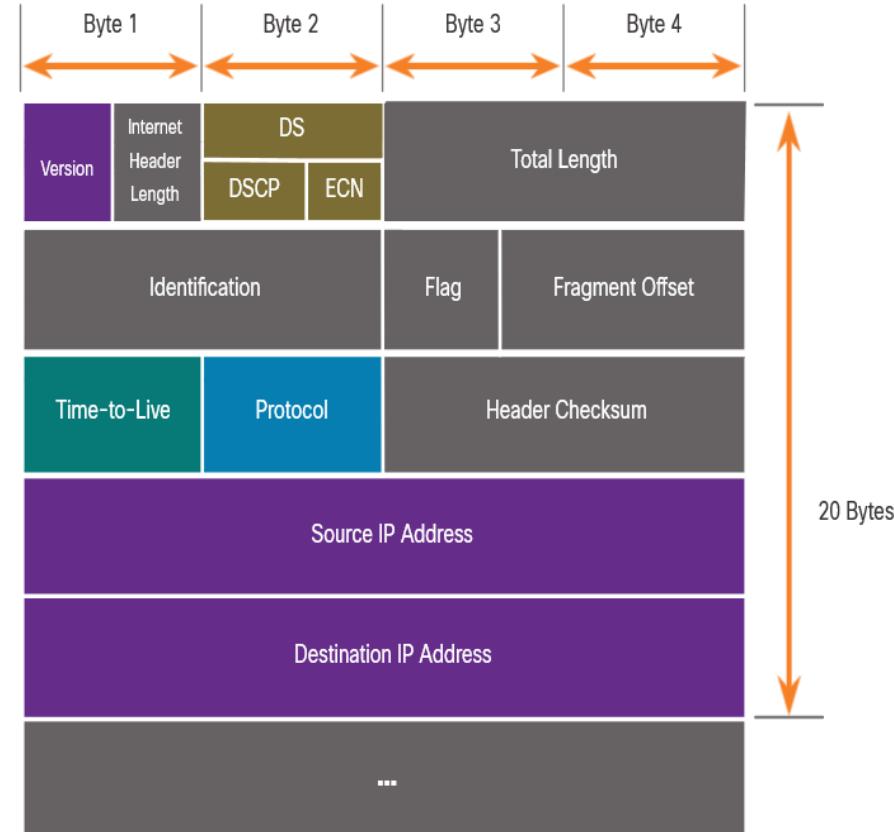
- Paketin doğru yönde (hedefe) gönderilmesini sağlar.
- Çeşitli alanlarda ağ katmanı işlemesi için bilgiler içerir.
- **Başlıktaki bilgiler**, paketi işleyen tüm katman 3 cihazları tarafından kullanılır.

# IPv4 Paket Başlık Alanları

IPv4 ağ başlığı özellikleri:

- İkili durumdadır.
- Birkaç bilgi alanı içerir.
- Diyagram soldan sağa, satır başına 4 bayt okunur.**
- En önemli iki alan kaynak ve hedeftir.

Protokollerin bir veya daha fazla işlevi olabilir.



# IPv4 Paket Başlık Alanları

IPv4 başlığındaki önemli alanlar:

Fonksiyon	Açıklama
Sürüm (Versiyon)	Bu, v6'nın aksine v4 için 4 bitlik bir alan = 0100 olacaktır
Farklılaştırılmış Hizmetler	QoS için kullanılır: DiffServ - DS alanı veya daha eski IntServ - ToS veya Hizmet Türü
Başlık Kontrolü (Header Checksum)	IPv4 başlığındaki bozulmayı tespit eder
Yaşam Süresi (Time to Live - TTL)	Katman 3 atlama sayısı. Sıfır olduğunda, yönlendirici paketi atar
Protokol	Bir sonraki seviye protokolü tanımlar: ICMP, TCP, UDP, vb.
Kaynak IPv4 Adresi	32-bit kaynak adresi
Hedef IPV4 Adresi	32-bit kaynak adresi

# Video – Wireshark'ta Örnek IPv4 Başlıklarları

Bu video aşağıdakileri kapsayacaktır:

- Wireshark'ta IPv4 Ethernet paketleri
- Kontrol bilgileri
- Paketler arasındaki fark

# 8.3 IPv6 Paketleri

## IPv4'ün Sınırlamaları

- ❑ **IPv4'ün üç ana sınırlaması vardır:**
- ❑ IPv4 adres tükenmesi – Temelde IPv4 adreslememiz bitmiştir.
  - **Uçtan uca bağlantı eksikliği** - IPv4'ün bu kadar uzun süre dayanmasını sağlamak için özel adresleme ve **NAT (Network Address Translation)** oluşturulmuştur.
  - **NAT, aynı ağ içerisinde bulunan birden fazla cihazın aynı IP'yi kullanarak internete erişebilmesini sağlayan yöntemdir.**
  - Bu, genel adresleme ile doğrudan iletişimleri sona erdirdi.
  - **Artan ağ karmaşıklığı** - NAT, geçici çözüm olarak oluşturulmuştu ve ağ üstbilgilerinin adreslemesini değiştirmenin bir yan etkisi olarak ağda sorunlar yaratmaktadır.
  - **NAT, gecikmeye ve sorun giderme sorunlarına neden olur.**

# IPv6'ya Genel Bakış

- **IPv6 Internet Engineering Task Force (IETF) tarafından geliştirilmiştir.**
- **IPv6, IPv4'ün sınırlamalarının üstesinden gelir.**
- IPv6'nın sağladığı iyileştirmeler:
  - **Artan adres alanı** - 32-bit yerine 128-bit adrese göre
  - **İyileştirilmiş paket işleme** - daha az alan içeren basitleştirilmiş başlık
  - **NAT ihtiyacını ortadan kaldırır** - çok fazla adresleme olduğundan, **dahili olarak özel adresleme kullanmaya ve paylaşılan bir genel adrese eşlenmeye 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	$10^{36}$	1,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000

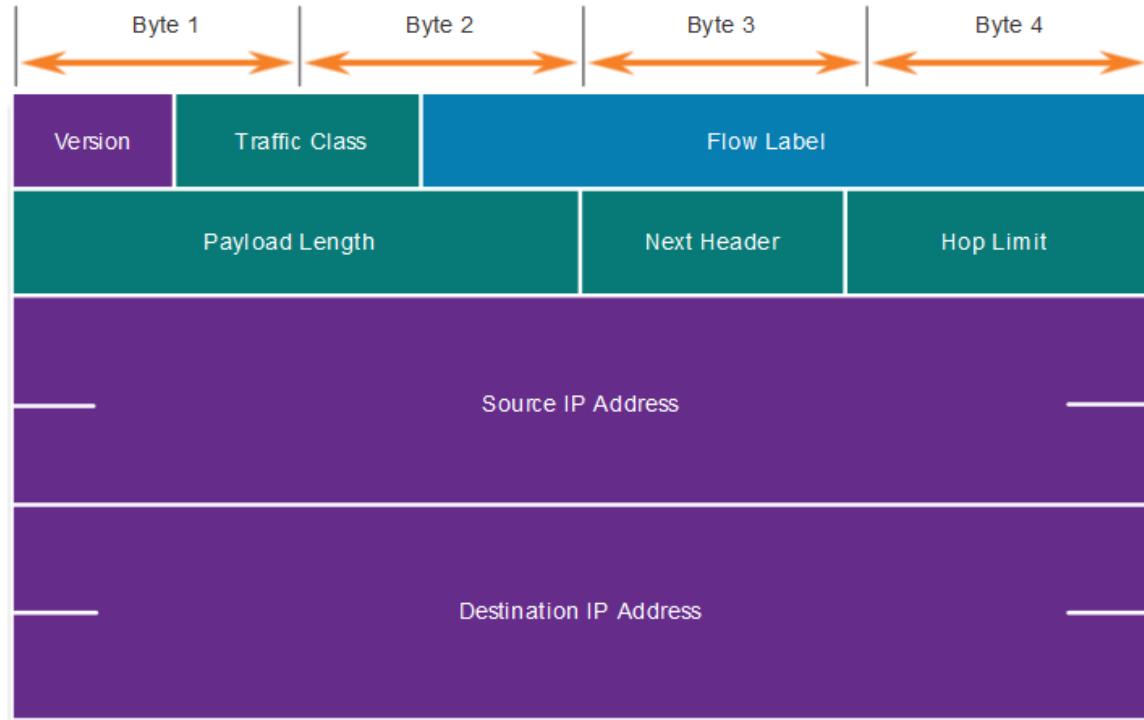
Legend

 There are 4 billion IPv4 addresses

 There are 340 undecillion IPv6 addresses

# IPv6 Paket BaşlığındaKİ IPv4 Paket Başlığı Alanları

- IPv6 başlığı basitleştirilmiştir, ancak daha küçük değildir.
- **Başlık, 40 Bayt veya sekizli uzunluğunda sabitlenmiştir.**
- Performansı artırmak için birkaç IPv4 alanı kaldırılmıştır.
- Performansı artırmak için bazı IPv4 alanları kaldırıldı::
  - **Bayrak (Flag)**
  - **Parça Numarası (Fragment Offset)**
  - **Başlık Kontrolü (Header Checksum)**



# IPv6 Paket Başlıklarısı

IPv6 başlığındaki önemli alanlar:

Fonksiyon	Açıklama
<b>Sürüm (Versiyon)</b>	Bu, v6'da v4'ün aksine, 4 bitlik bir alan = 0110 olacaktır.
<b>Trafik Sınıfı</b>	QoS için kullanılır: DiffServ'e eşdeğer - DS alanı
<b>Akiş Etiketi</b>	Aygıtta aynı akış etiketlerini aynı şekilde, 20 bitlik alanla işlemesini bildirir
<b>Yük Boyutu</b>	Bu 16 bitlik alan, IPv6 paketinin veri kısmının veya yükünün uzunluğunu gösterir
<b>Sonraki Başlık</b>	<b>Bir sonraki seviye protokolü tanımlar:</b> ICMP, TCP, UDP, vb.
<b>Sıçrama Limiti</b>	TTL alanı Katman 3 atlama sayısını değiştirir
<b>Kaynak IPv4 Adresi</b>	128-bit kaynak adresi
<b>Hedef IPV4 Adresi</b>	128-bit hedef adresi

## IPv6 Paket Başlığı (devamı)

IPv6 paketi ayrıca **uzantı başlıkları (EH)** içerebilir.

**EH başlıklarının özelliklerı:**

- istege bağlı ağ katmanı bilgisi sağlar
- istege bağlıdır
- IPv6 başlığı ile yük arasına yerleştirilir
- parçalanma, güvenlik, mobilite desteği vb. için kullanılabilir.

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

# Video – Wireshark'ta Örnek IPv6 Başlıklar

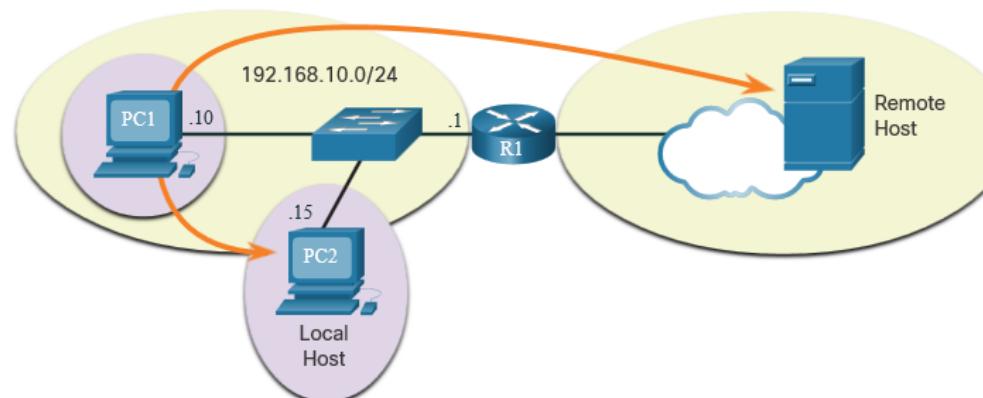
Bu video aşağıdakileri kapsayacaktır:

- Wireshark'ta IPv6 Ethernet paketleri
- Kontrol bilgileri
- Paketler arasındaki fark

# 8.4 Host Nasıl Yönetlendirilir

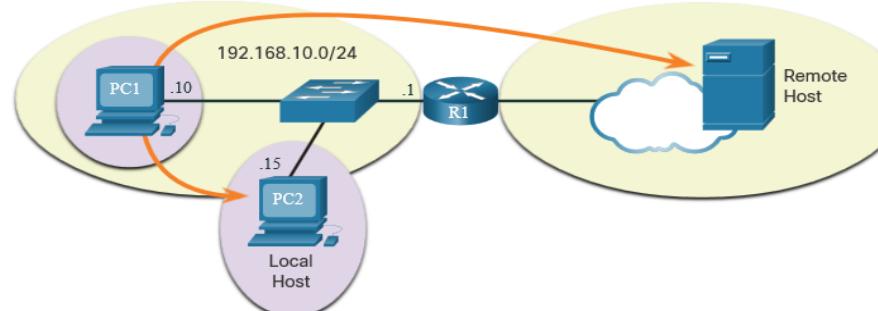
## Host Yönlendirme Kararı

- Paketler her zaman kaynakta oluşturulur.
- Her host kendi yönlendirme tablosunu oluşturur.
- Bir host aşağıdakilere paket gönderebilir:
  - **Kendisi** – 127.0.0.1 (IPv4), ::1 (IPv6)
  - **Yerel Hostlar** – hedef aynı LAN üzerindedir
  - **Uzak Hostlar** – cihazlar aynı LAN üzerinde değildir



## Host Yönlendirme Kararı (devamı)

- Kaynak cihaz 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 (*router*) tarafından tanıtılan **ağ adresini** ve **ön eki** kullanır
- Yerel trafik, bir aracı cihaz tarafından işlenmek üzere ana bilgisayar arayüzünden atılır.
- Uzak trafik doğrudan LAN üzerindeki varsayılan ağ geçidine iletılır.



## Varsayılan Ağ Geçidi

**Bir yönlendirici veya katman 3 switch, varsayılan bir ağ geçidi olabilir.**

Varsayılan bir ağ geçidinin (DGW) özellikleri:

**LAN'ın geri kalanıyla aynı aralıkta bir IP adresine sahip olmalıdır.**

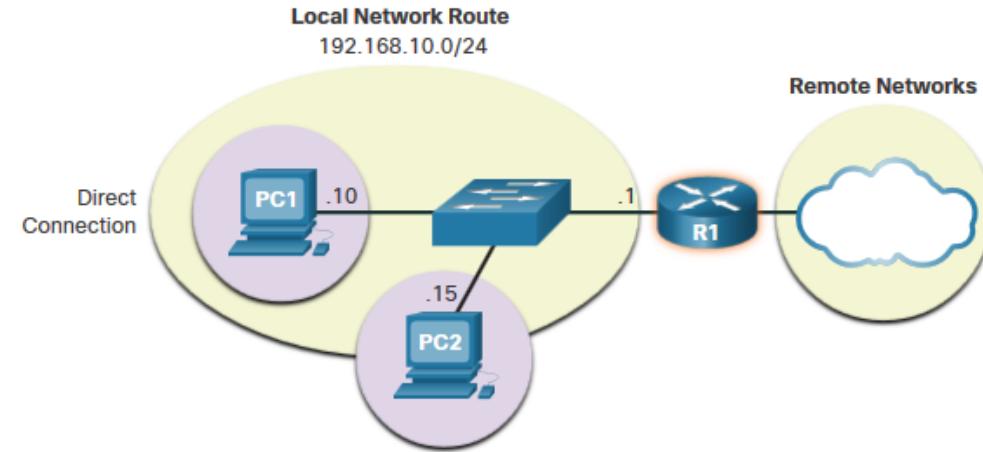
- LAN'dan veri kabul edebilir ve LAN üzerinden trafiği iletебilir.
- Diğer ağlara yönlendirilebilir.

Bir aygıtın varsayılan ağ geçidi yoksa veya kötü bir varsayılan ağ geçidi yoksa, trafiği LAN'ı terk edemez.

Host nasıl yönlendirilir

## Host Varsayılan Ağ Geçidine Yönlendirir

- Host **varsayılan ağ geçidini (DGW)** statik olarak veya IPv4'teki DHCP aracılığıyla bileyebilir.
- IPv6, DGW'yi bir yönlendirici talebi (router solicitation - RS) aracılığıyla gönderir veya manuel olarak yapılandırılabilir.
- **DGW**, yönlendirme tablosundaki son çare yolu olacak **statik yoldur**.
- LAN üzerindeki tüm aygıtlar, trafiği uzaktan göndermeyi planlıyorlarsa, router'ın DGW'sine ihtiyaç duyacaktır.



## Host Yönlendirme Tablosu

- Windows'ta, PC yönlendirme tablosunu görüntülemek için print veya **netstat -r**'yi yönlendirin
- Bu iki komutla görüntülenen üç bölüm:
  - **Arayüz Listesi** - tüm potansiyel arayüzler ve MAC adresleme
  - **IPv4 Yönlendirme Tablosu**
  - **IPv6 Yönlendirme Tablosu**



IPv4 Routing Table for PC1

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

IPv4 Route Table

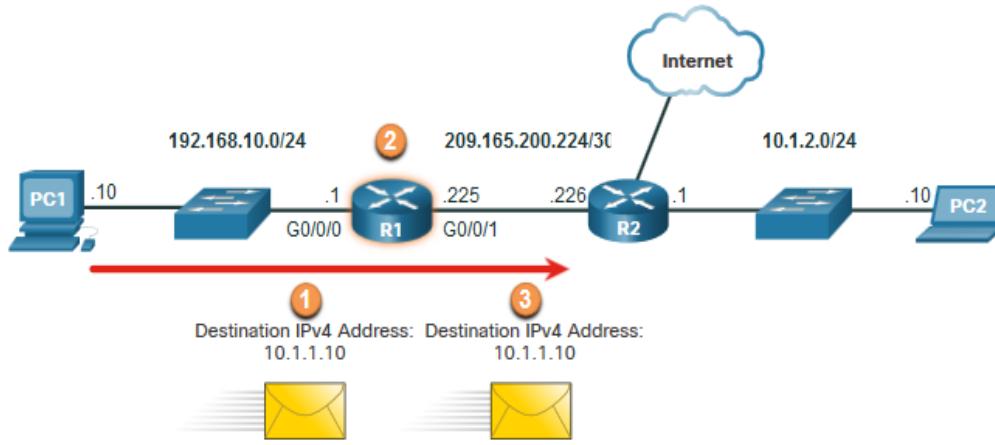
=====  
Active Routes:

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 (Routing) Giriş

# Router Paket Yönlendirme Kararı

- Router çerçeveyi ana cihazdan aldığında ne olur?



- Packet arrives on the Gigabit Ethernet 0/0/0 interface of router R1. R1 de-encapsulates the Layer 2 Ethernet header and trailer.
- Router R1 examines the destination IPv4 address of the packet and searches for the best match in its IPv4 routing table. The route entry indicates that this packet is to be forwarded to router R2.
- Router R1 encapsulates the packet into a new Ethernet header and trailer, and forwards the packet to the next hop router R2.

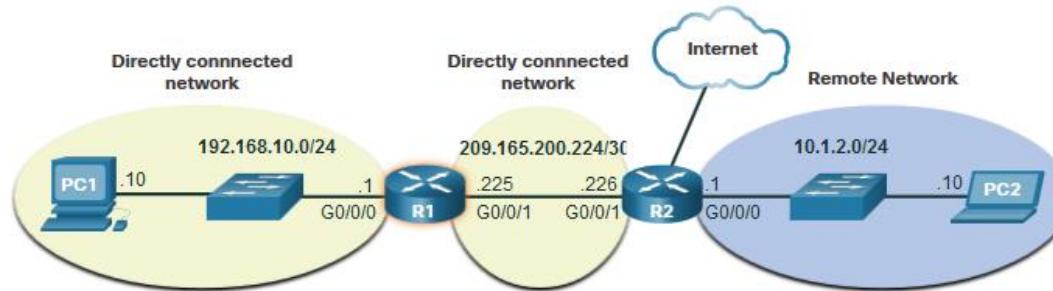
## R1 Routing Table

Route	Next Hop or Exit Interface
192.168.10.0 /24	G0/0/0
209.165.200.224/30	G0/0/1
<b>10.1.1.0/24</b>	<b>via R2</b>
Default Route 0.0.0.0/0	via R2

# IP Router Yönlendirme Tablosu

Bir router'ın yönlendirme tablosunda üç tür yol vardır:

- **Doğrudan Bağlı** - Arayüzün etkin olması ve adresleme içermesi şartıyla, bu rotalar router tarafından otomatik olarak eklenir.
- **Uzak** - Bunlar, **yönlendiricinin doğrudan bağlantıya sahip olmadığı** ve öğrenilebilen rotalardır:
  - **Manuel olarak** – statik bir rotayla
  - **Dinamik olarak** – routerların bilgilerini birbirleriyle paylaşmasını sağlamak için bir yönlendirme protokolü kullanarak
- **Varsayılan Rota** – bu, yönlendirme tablosunda bir eşleşme olmadığında **tüm trafiği belirli bir yöne yönlendirir.**

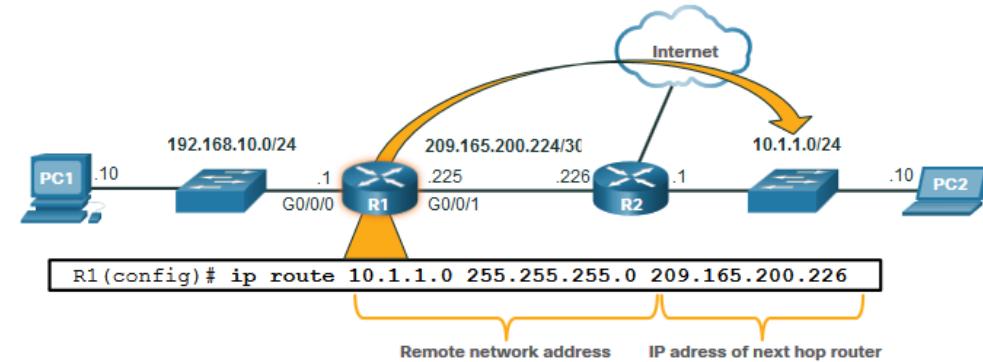


# Yönlendirmeye Giriş

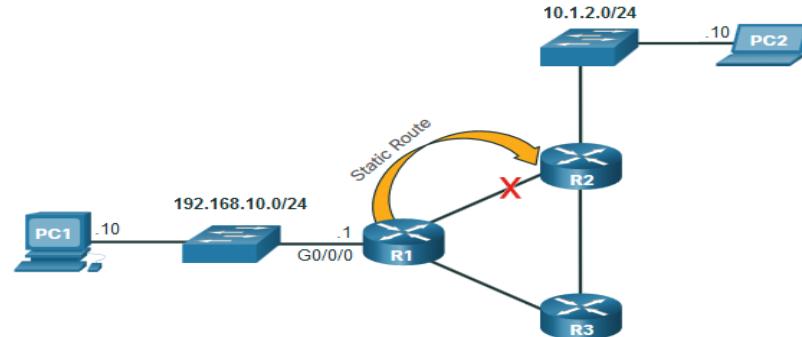
## Statik Yönlendirme

### Statik Yönlendirme Özellikleri:

- Manuel olarak yapılandırılmalıdır
- Topolojide bir değişiklik olduğunda yönetici tarafından manuel olarak ayarlanmalıdır
- Küçük yedekli olmayan ağlar için uygundur
- Genellikle bir varsayılan yolu yapılandırmak için dinamik bir yönlendirme protokolüyle birlikte kullanılır.



R1 is manually configured with a static route to reach the 10.1.1.0/24 network. If this path changes, R1 will require a new static route.



If the route from R1 via R2 is no longer available, a new static route via R3 would need to be configured. A static route does not automatically adjust for topology changes.

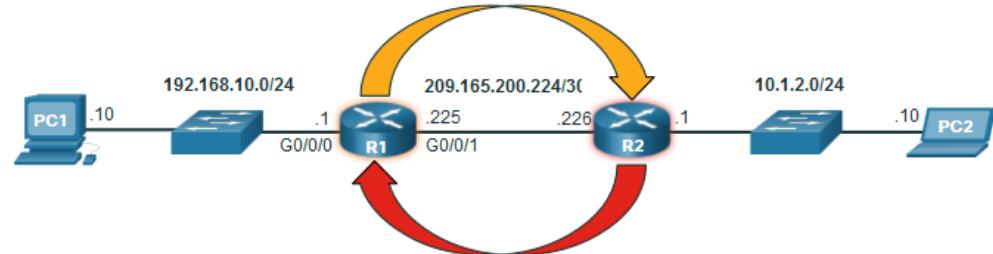
# Yönlendirmeye Giriş

## Dinamik Yönlendirme

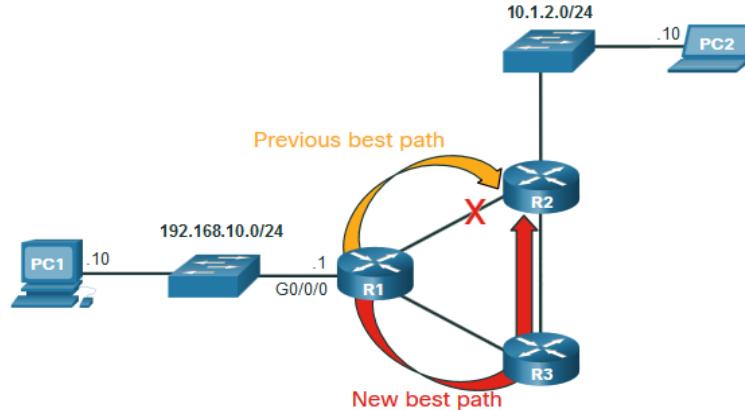
### Dinamik rotalar otomatik olarak:

- Uzak ağları keşfeder
- Güncel bilgileri korur
- **Hedefe giden en iyi yolu seçer**
- **Topoloji değişikliği** olduğunda en iyi yeni yolları bulur.

Dinamik yönlendirme, statik varsayılan yolları diğer yönlendiricilerle de paylaşabilir.



- R1 is using the routing protocol OSPF to let R2 know about the 192.168.10.0/24 network.
- R2 is using the routing protocol OSPF to let R1 know about the 10.1.1.0/24 network.



R1, R2, and R3 are using the dynamic routing protocol OSPF. If there is a network topology change, they can automatically adjust to find a new best path.

# Video – IPv4 Router Yönlendirme Tabloları

Bu video, IPv4 router yönlendirme tablosundaki bilgileri açıklayacaktır.

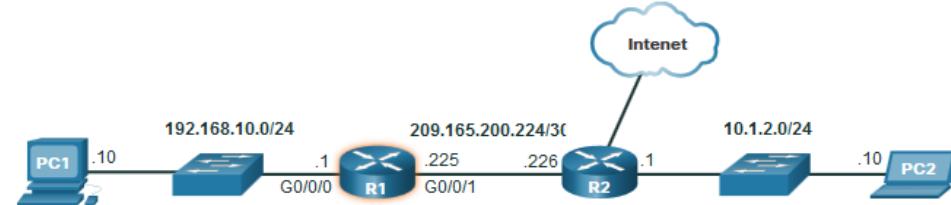
## IPv4 Yönlendirme Tablolarına Giriş

Show ip route komutu aşağıdaki yönlendirme 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

Bu komut rota türlerini gösterir:

- Doğrudan bağlantılı – C ve L
- Uzak Rotalar– O, D, vb.
- Varsayılan Rotalar– S\*



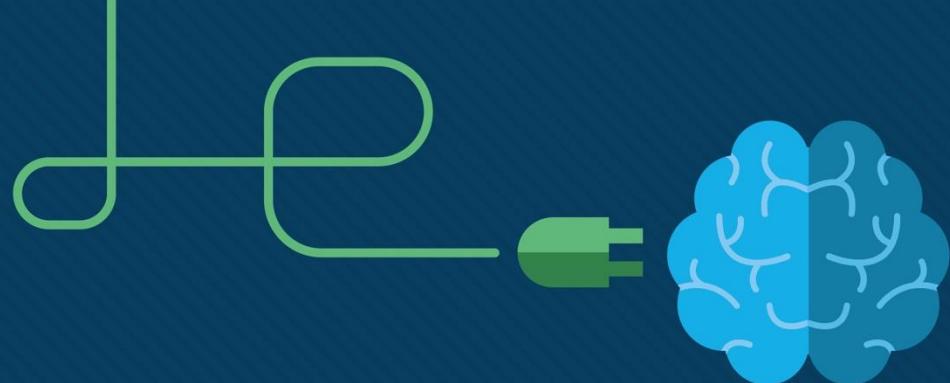
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
      D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
      N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1, E2 - OSPF external type 2
      i - 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, 1 - LIS
      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#
```

# 8.6 Modül Pratiği ve Quiz

## Bu modülde ne öğrendim?

- IP bağlantısızdır, en iyi çabasıdır ve medyadan bağımsızdır.
- IP, paket teslimini garanti etmez.
- IPv4 paket başlığı, paketle ilgili bilgileri içeren alanlardan oluşur.
- IPv6, IPv4'ün uçtan uca bağlantı eksikliğinin ve artan ağ karmaşıklığının üstesinden gelir.
- Bir cihaz, bir hedefin kendisi mi, başka bir yerel ana bilgisayar (local host) ve uzak bir ana bilgisayar (remote host) mı olduğunu belirleyecektir.
- Varsayılan bir ağ geçidi, LAN'ın bir parçası olan ve diğer ağlara açılan bir kapı olarak kullanılacak olan yönlendiricidir.
- Yönlendirme tablosu, bilinen tüm ağ adreslerinin (önekler) ve paketin nereye yönlendirileceğinin bir listesini içerir.
- Yönlendirici en uzun alt ağ maskesini veya önek eşleşmesini kullanır.
- Yönlendirme tablosunun üç tür yol girişi vardır: doğrudan bağlı ağlar, uzak ağlar ve varsayılan yol.





# Modül 9: Adres Çözümleme

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

## Modül Başlığı: Adres Çözümleme

**Modül Amacı:** Adres Çözümleme Protokolü ve Komşu Saptama'nın bir ağ üzerinde iletişimini nasıl etkinleştirdiğini açıklamak.

Konu Başlığı	Konu Amacı
<b>MAC ve IP</b>	MAC adresinin ve IP adresinin rollerini karşılaştırın.
<b>Adres Çözümleme Protokolü (Address Resolution Protocol - ARP)</b>	Adres Çözümleme Protokolü'nün amacını açıklayın.
<b>Komşu Saptama (Neighbor Discovery – ND)</b>	IPv6 komşu saptamanın işleyişini açıklayın.

# 9.1 MAC ve IP

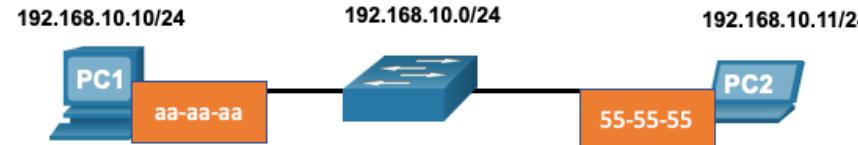
# Aynı Ağdaki Hedef

Bir Ethernet LAN üzerinde bir cihaza atanmış iki birincil adres vardır:

- Katman 2 fiziksel adresi (MAC adresi)** - Aynı Ethernet ağında NIC'ten NIC'e iletişimleri için kullanılır.
- Katman 3 mantıksal adresi (IP adresi)** - Paketi kaynak cihazdan hedef cihaza göndermek için kullanılır.

**Katman 2 adresleri**, çerçeveleri aynı ağ üzerindeki bir NIC'den başka bir NIC'ye göndermek için kullanılır.

**Bir hedef IP adresi aynı ağ üzerindeyse, hedef MAC adresi, hedef aygıtın adresi olacaktır.**

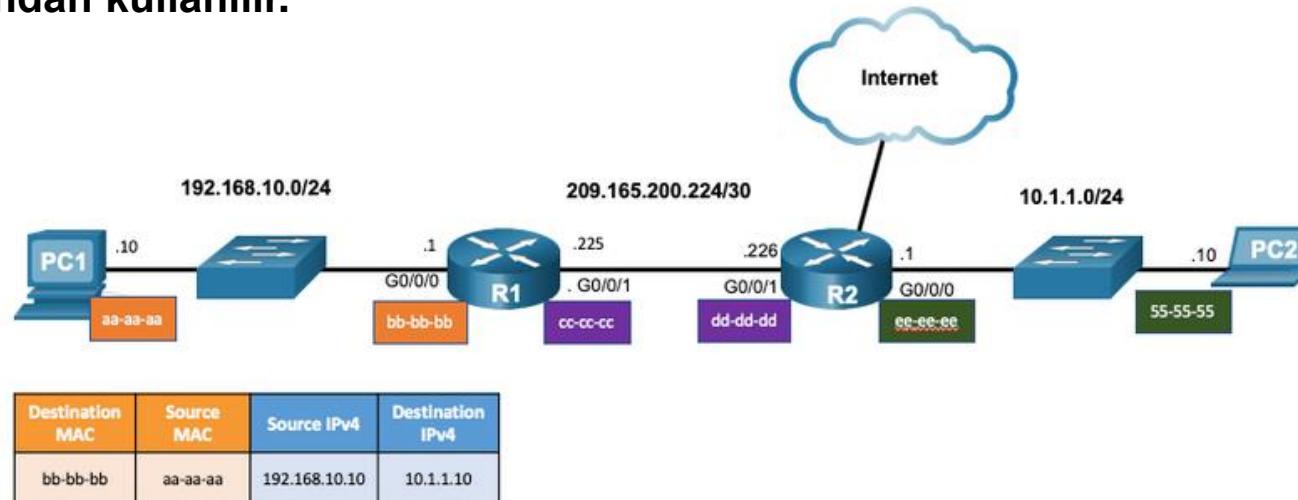


Destination MAC	Source MAC	Source IPv4	Destination IPv4
55-55-55	aa-aa-aa	192.168.10.10	192.168.10.11

# Uzak Ağdaki Hedef

Hedef IP adresi uzak bir ağ üzerindeyse, hedef MAC adresi varsayılan ağ geçidinininkidir.

- **Adres Çözümleme Protokolü**, bir aygıtın **IPv4** adresini aygit NIC'inin MAC adresiyle ilişkilendirmek için **IPv4** tarafından kullanılır.
- **ICMPv6**, bir aygıtın **IPv6** adresini aygit **NIC**'inin MAC adresiyle ilişkilendirmek için **IPv6** tarafından kullanılır.



# Paket İzleyici (Packet Tracer) –MAC ve IP Adreslerini Tanımlayın

Bu Paket İzleyicide aşağıdaki hedefleri tamamlayacaksınız:

- Yerel Ağ İletişimi için PDU Bilgilerini Toplayın
- Uzak Ağ İletişimi için PDU Bilgilerini Toplayın

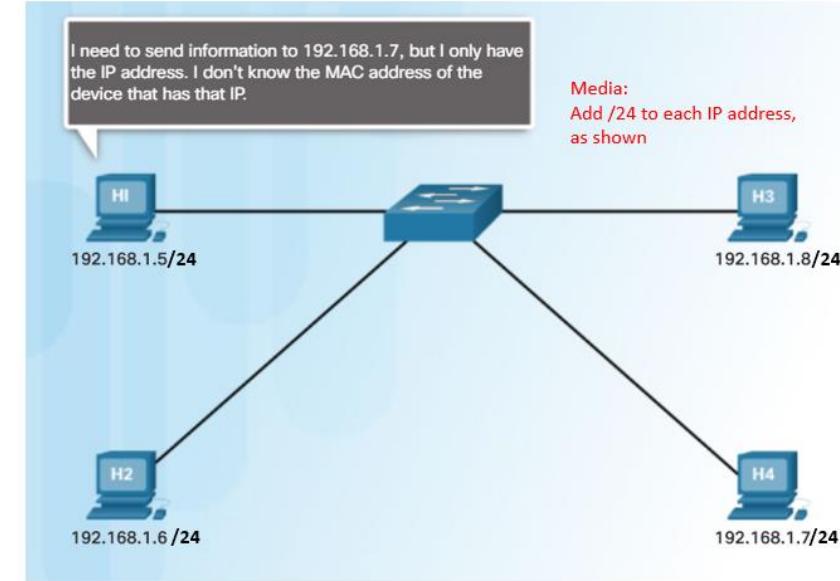
# 9.2 Adres Çözümleme Protokolü (ARP)

# Adres Çözümleme Protokolü (ARP) ARP'ye Genel Bakış

**Bir cihaz, IPv4 adresini bildiğiinde yerel bir cihazın hedef MAC adresini belirlemek için Adres Çözümleme Protokolünü (ARP) kullanır.**

**ARP iki temel işlev sağlar:**

- IPv4 adreslerini MAC adreslerine çözümleme
- IPv4 - MAC adresi eşleştirmelerinin ARP tablosunu koruma



# ARP Fonksiyonları

- ❑ Bir çerçeve göndermek için, cihaz ARP tablosunda bir hedef IPv4 adresi ve karşılık gelen bir MAC adresi arayacaktır.
  - Paketin hedef IPv4 adresi **aynı ağ üzerindeyse**, **cihaz hedef IPv4 adresini ARP tablosunda arayacaktır.**
  - Hedef IPv4 adresi **farklı bir ağdaysa**, cihaz **varsayılan ağ geçidinin IPv4 adresini ARP tablosunda arayacaktır.**
  - **Cihaz IPv4 adresini bulursa, ilgili MAC adresi çerçevedeki hedef MAC adresi olarak kullanılabilir.**
  - **ARP tablosu girişи bulunamazsa, cihaz bir ARP isteği gönderir.**

# Adres Çözümleme Protokolü Video - ARP İsteği

Bu video, bir MAC adresi için bir ARP talebini kapsayacaktır.

# Video – ARP Operasyonu - ARP Cevabı

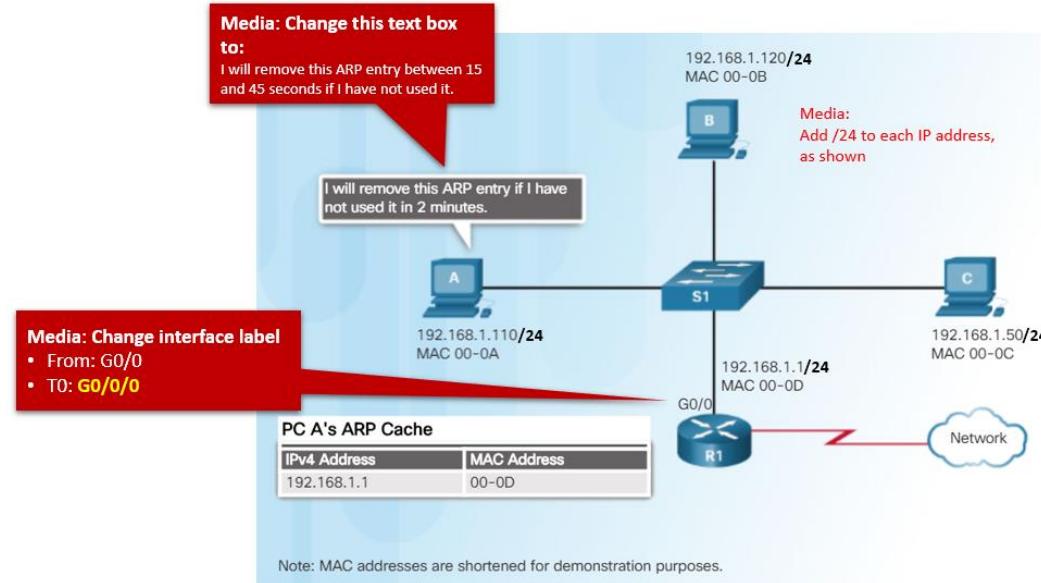
Bu video, bir ARP isteğine yanıt olarak bir ARP yanıtını kapsayacaktır.

# Video – Uzaktan İletişimde ARP'nin Rolü

Bu video, bir ARP isteğinin bir ana makineye varsayılan ağ geçidinin MAC adresini nasıl sağlayacağını ele alacaktır.

# Bir ARP Tablosundan Girişlerin Kaldırılması

- ARP tablosundaki girişler **kalıcı değildir** ve bir ARP önbellek zamanlayıcısının belirli bir süre sonra süresi dolduğunda kaldırılır.
- ARP önbellek zamanlayıcısının süresi, işletim sistemine bağlı olarak farklılık gösterir.
- ARP tablo girişleri yönetici tarafından manuel olarak da kaldırılabilir.



# Ağ Aygıtlarındaki ARP Tabloları

- **show ip arp** komutu Cisco router’ı üzerinde ARP tablosunu gösterir.
- **arp -a** komutu Windows 10 PC üzerinde ARP tablosunu gösterir.

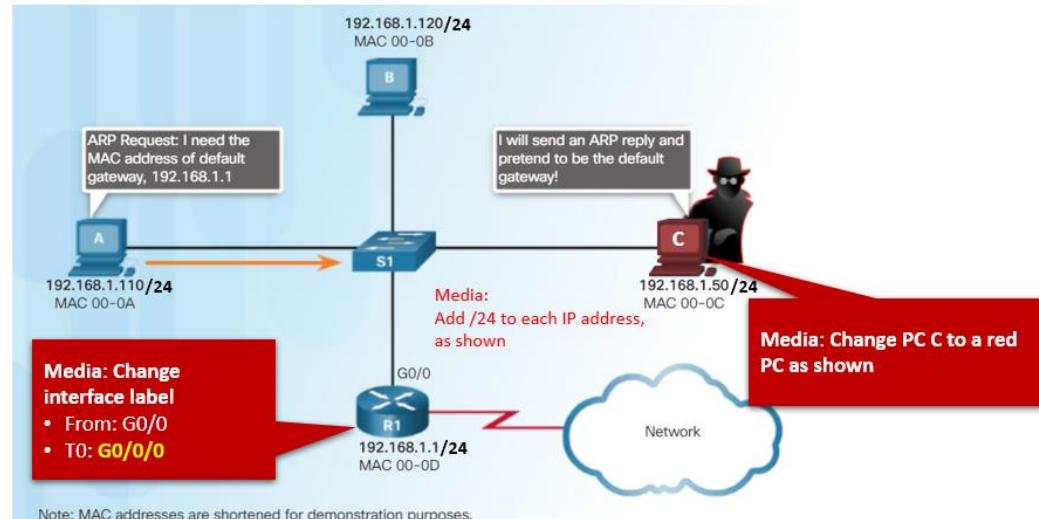
```
R1# show ip arp
Protocol Address          Age (min)  Hardware Addr      Type      Interface
Internet 192.168.10.1        -         a0e0.af0d.e140  ARPA     GigabitEthernet0/0/0
```

```
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
```

# ARP Sorunları – ARP Yayınları ve ARP Yanıltması

- ARP istekleri yerel ağdaki her cihaz tarafından alınır ve işlenir.
- Aşırı ARP yayınları performansta bir miktar düşüşe neden olabilir.
- ARP yanıtları, ARP poisoning saldırısı gerçekleştirmek için bir tehdit aktörü tarafından yanıltılabilir.
- Kurumsal düzeydeki switchler, ARP saldırılara karşı koruma sağlamak için azaltma tekniklerini içerir.



## Adres Çözümleme Protokolü (ARP)

# Paket İzleyici (Packet Tracer) – ARP Tablosunu İnceleyin

Bu Paket İzleyicide aşağıdaki hedefleri tamamlayacaksınız:

- ARP İsteğini İnceleme
- Switch MAC Adres Tablosunu inceleme
- Uzaktan İletişimde ARP Sürecini inceleme

# 9.3 Bakır Kablolama

# Video – IPv6 Komşu Saptama

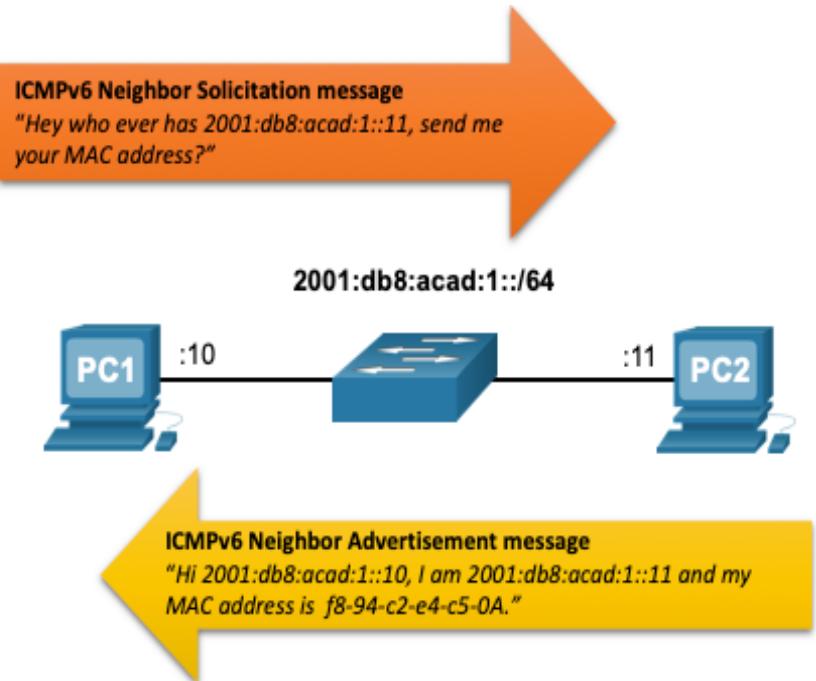
Bu video, IPv6'nın ICMPv6 komşu talep ve komşu reklam mesajlarını kullanarak adres çözümleme işlemini nasıl gerçekleştirdiğini açıklayacaktır.

# IPv6 Komşu Saptama Mesajları

IPv6 Komşu Saptama (Neighbor Discovery - ND) protokolü şunları sağlar:

- Adres Çözünürlüğü
- Router keşfi
- Yönlendirme hizmetleri
- ICMPv6 Komşu Talebi (Neighbor Solicitation - NS) ve Komşu Reklam (Neighbor Advertisement - NA) mesajları, adres çözümleme gibi cihazdan cihaza mesajlaşma için kullanılırlar.
- ICMPv6 Router Solicitation (RS) ve Router Advertisement (RA) mesajları, yönlendirici keşfi için cihazlar ve yönlendiriciler arasında mesajlaşma için kullanılır.
- ICMPv6 yeniden yönlendirme mesajları, daha iyi bir sonraki atlama seçimi için yönlendiriciler tarafından kullanılır.

# IPv6 Komşu Saptama – Adres Çözümlemesi



- IPv6 cihazları, bilinen bir IPv6 adresinin MAC adresini çözmek için **Komşu Saptama (ND)** kullanır.
- **ICMPv6 Komşu Talep (NS) mesajları**, özel Ethernet ve IPv6 çok noktaya yayın adresleri kullanılarak gönderilir.

# Paket İzleyici (Packet Tracer) – IPv6 Komşu Saptama

Bu Paket İzleyicide aşağıdaki hedefleri tamamlayacaksınız:

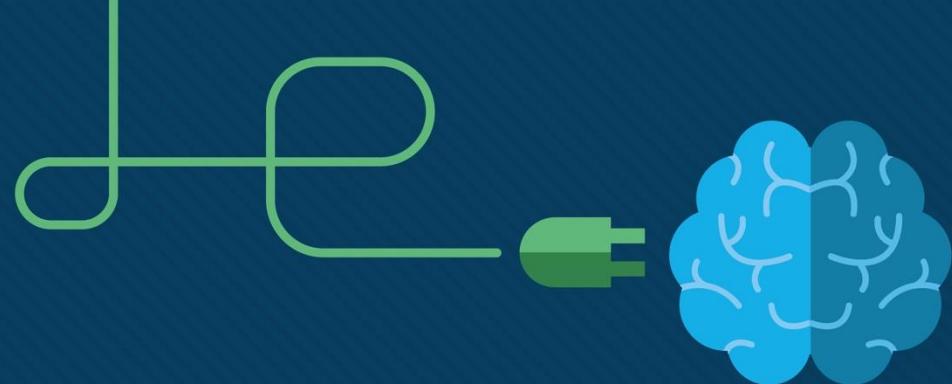
- Bölüm 1: IPv6 Komşu Keşfi Yerel Ağ
- Bölüm 2: IPv6 Komşu Keşfi Uzak Ağ

# 9.4 Modül Pratiği ve Quiz

# Bu modülde ne öğrendim?

- Katman 2 fiziksel adresleri (yani, Ethernet MAC adresleri), kapsüllenmiş IP paketi ile veri bağlantı çerçevesini aynı ağ üzerindeki bir NIC'den başka bir NIC'ye iletmek için kullanılır.
- Hedef IP adresi aynı ağ üzerindeyse, hedef MAC adresi, hedef aygıtın adresi olacaktır.
- Hedef IP adresi (IPv4 veya IPv6) uzak bir ağ üzerindeyse, hedef MAC adresi ana bilgisayarın varsayılan ağ geçidinin (yani yönlendirici arayüzü) adresi olacaktır.
- Bir IPv4 cihazı, IPv4 adresini bildiğinde yerel bir cihazın hedef MAC adresini belirlemek için ARP'yi kullanır.
- ARP iki temel işlev sağlar: IPv4 adreslerini MAC adreslerine çözümlemek ve IPv4 - MAC adresi eşlemeleri tablosunu sürdürmek.
- ARP yanıtı alındıktan sonra, cihaz IPv4 adresini ve ilgili MAC adresini ARP tablosuna ekleyecektir.
- Her cihaz için, bir ARP önbellek zamanlayıcısı, belirli bir süre kullanılmayan ARP girişlerini kaldırır.
- IPv6 ARP kullanmaz, MAC adreslerini çözmek için ND protokolünü kullanır.
- Bir IPv6 cihazı, IPv6 adresini bildiğinde yerel bir cihazın hedef MAC adresini belirlemek için ICMPv6 Komşu Keşfini kullanır.





# Modül 10: Temel Yönlendirici Yapılandırması

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

**Modül Başlığı:** Temel yönlendirici yapılandırması

**Modül Hedefi:** Yönlendirici ve son cihazlarda ilk ayarları uygulama

Konu Başlığı	Konu Hedefi
<b>Yönlendiricinin Başlangıç Yapılandırması</b>	İlk ayarları bir IOS Cisco yönlendiricide yapılandırın.
<b>Yapılandırma Arayüzleri</b>	Cisco IOS yönlendiricisi üzerinde iki etkin arayüz yapılandırın.
<b>Varsayılan Ağ Geçidi Yapılandırması</b>	Aygıtları varsayılan ağ geçidini kullanacak şekilde yapılandırın.

# 10.1 Yönlendirici İlk Ayarları Yapılandırma

# Temel Yönlendirici Yapılandırma Adımları

- Cihaz ismi yapılandırma
- Güvenli ayrıcalıklı (privileged) EXEC modu
- Kullanıcı EXEC modunu güvenli hale getirir.
- Güvenli uzaktan Telnet / SSH erişimi.
- Tüm metin parolalarını şifreleyin.
- Yasal bildirim sağlayın ve yapılandırmayı kaydedin.

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

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

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

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

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

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

# Temel Yönlendirici Yapılandırma Örneği

- R1'deki temel yönlendirici yapılandırması için komutlar.
- Yapılandırma NVRAM'a kaydedilir.

```
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
```

# Paket Tracer – İlk Yönlendirici Ayarlarını Yapılandırır

Bu Paker Tracer'da aşağıdakileri yapacaksınız:

- Varsayılan yönlendirici yapılandırmasını doğrulama.
- İlk yönlendirici yapılandırmasını yapılandırma ve doğrulama.
- Çalışan yapılandırma dosyasını kaydedin.

# 10.2 Arayüzleri Yapılandırma

# Yönlendirici Arayüzlerini Yapılandırma

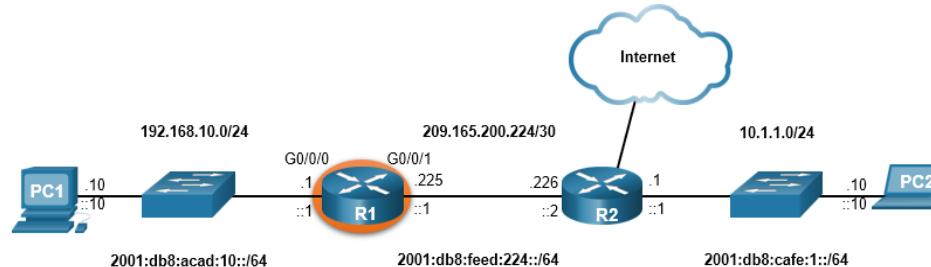
Yönlendirici arayüzlerini yapılandırmak aşağıdaki komut adımlarını içerir:

```
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
```

- **Description** (Açıklama) komutu arayüze bağlı ağ hakkında bilgi eklemek için iyi bir komuttur.
- **No shutdown** komutu arayüzü etkinleştirir.

# Yönlendirici Arayüzlerini Yapılandırma Örneği

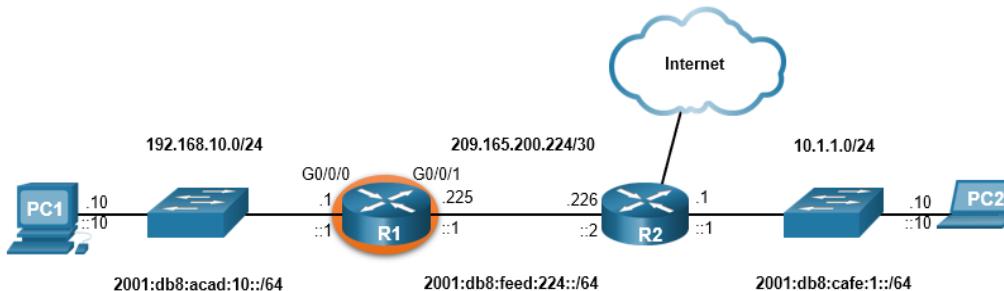
R1'de G0/0/0 arayüzüünü yapılandırmak için komutlar aşağıdadır:



```
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
```

# Yönlendirici Arayüzlerini Yapılandırma Örneği (Devamı)

R1'de G0/0/1 arayüzüünü yapılandırmak için komutlar aşağıdadır:



```
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
```

# Arayüz Yapılandırması'nı doğrula

Arayüz yapılandırmasını doğrulamak için **show ip interface brief** ve **show ipv6 interface brief** komutlarını kullanabilirsiniz:

```
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#
```

# Doğrulama Komutlarını Yapılandırma

Tablo, arayüz yapılandırmalarını doğrulamak için kullanılan komutlarının açıklamalarını gösterir.

Komut	Açıklama
<code>show ip interface brief</code> <code>show ipv6 interface brief</code>	Tüm arayüzler için, IP adreslerini ve geçerli durumlarını görüntüler.
<code>show ip route</code> <code>show ipv6 route</code>	RAM'de depolanan IP yönlendirme tablolarının içeriğini görüntüler.
<code>show interfaces</code>	Aygıttaki tüm arayüzlerinin istatistiklerini görüntüler. Yalnızca IPv4 adres bilgilerini görüntüler.
<code>show ip interfaces</code>	Bir yönlendiricideki tüm arayüzlerinin IPv4 istatistiklerini görüntüler.
<code>show ipv6 interfaces</code>	Bir yönlendiricideki tüm arayüzlerinin IPv6 istatistiklerini görüntüler.

# Doğrulama Komutlarını Yapılandırma (Devamı)

**show ip interface brief** ve **show ipv6 interface brief** komutları ile tüm arayüzlerin durumlarını görüntüleyin

```
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#
```

```
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#
```

# Doğrulama Komutlarını Yapılandırma (Devamı)

IP yönlendirme tablolarını **show ip route** ve **show ipv6 route** komutu ile görüntüleyebilirsiniz:

```
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#
```

# Doğrulama Komutlarını Yapılandırma (Devamı)

Burada gösterildiği gibi,  
**show interfaces** komutu  
ile tüm arayüzleri  
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#
```

# Doğrulama Komutlarını Yapılandırma (Devamı)

Burada gösterildiği gibi,  
**show ip interface** komutu  
ile yönlendirici arayüzleri  
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#
```

# Configure Verification Commands (Cont.)

Burada gösterilen **show ipv6 interface** komutu ile yönlendirici arayüzleri için IPv6 istatistiklerini görüntüleyin:

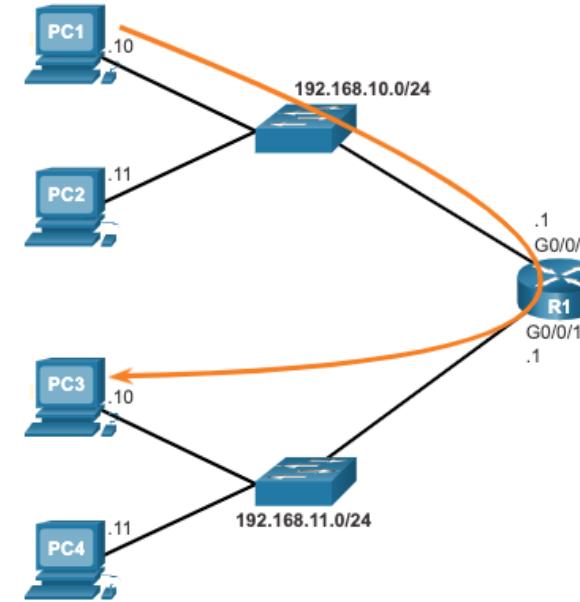
```
R1# show ipv6 interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
    FE80::868A:8DFF:FE44:49B0
      No Virtual link-local address(es) :
      Description: Link to LAN
      Global unicast address(es) :
        2001:DB8:ACAD:10::1, subnet is 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 Varsayılan Ağ Geçidini Yapılandırma

# Ana Bilgisayarda Varsayılan Ağ Geçidi

- **Varsayılan ağ geçidi, ana bilgisayar başka bir ağdaki bir aygıta paket gönderdiğinde kullanılır.**
- **Varsayılan ağ geçidi adresi** genellikle **ana bilgisayar yerel ağına bağlı yönlendirici arayüzünün adresi**dir.
- PC3'e ulaşmak için PC1, PC3'ün **IPv4 adresine sahip bir paket oluşturur**, ancak paketi varsayılan ağ geçidi olan R1'in G0/0/0 arabirimini **olan g1'e ileter**.

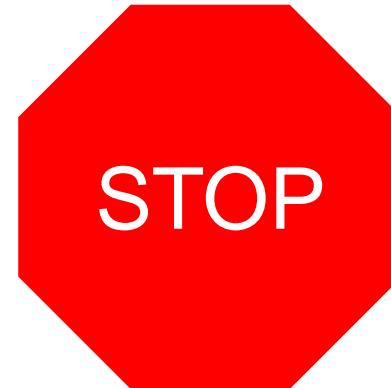


Not: Ana bilgisayar ve yönlendirici arayüzünün IP adresi aynı anda olmalıdır.

# Anahtarlayıcı da Varsayılan Ağ Geçidi

- Bir anahtarlayıcının varsayılan ağ geçidi adresi başka bir anahtarlayıcı tarafından uzaktan yapılandırılacak şekilde olmalıdır.
- Anahtarlayıcındaki varsayılan ağ geçidini yapılandırmak için **ip default-gateway ip-address** global komutunu kullanın.

MEDIA IS WORKING ON A CORRECTED VERSION OF THE GRAPHIC FROM 10.3.2.  
IT IS WRONG ON AR, AND ON THE GLOBAL BUG LIST



# Paket Tracer – Bir Yönlendirici’yi LAN'a bağlayın

Bu Paket Tracer'da, aşağıdakileri yapacaksınız::

- Yönlendirici bilgilerini görüntüleme.
- Yönlendirici arabirimlerini yapılandırma.
- Yapılandırmayı doğrulama.

# Packet Tracer – Varsayılan Ağ Geçidi Sorunlarında Çözüm Bulma

Bu Paket Tracer'da, aşağıdakileri yapacaksınız:

- Ağ belgelerini doğrulayın ve sorunları belirlemek için testleri kullanma.
- Belirli bir sorun için uygun bir çözüm belirleme.
- Çözümü uygulama.
- Belirlenen problem için çözümü test etme
- Çözümü belgele.

# 10.4 Modül Uygulama ve Sınav

# Video – Ağ Cihazı Farkları: Bölüm 1

Bu video aşağıdaki yönlendiricilerin farklı özelliklerini kapsayacaktır:

- Cisco 4000 Serisi Yönlendirici.
- Cisco 2900 Serisi Yönlendirici.
- Cisco 1900 Serisi Yönlendirici.

## Video – Ağ Cihazı Farkları: Bölüm 2

Bu video aşağıdaki yönlendiricilerin farklı yapılandırmalarını kapsayacaktır :

- Cisco 4000 Serisi Yönlendirici.
- Cisco 2900 Serisi Yönlendirici.
- Cisco 1900 Serisi Yönlendirici.

# Paket Tracer – Temel Aygıt Yapılandırması

Bu Paket Tracer'da, aşağıdakileri yapacaksınız::

- Ağ dökümanlarını tamamlama.
- Yönlendirici ve anahtarlayıcı üzerinde temel aygıt yapılandırmalarını gerçekleştirmeye.
- Bağlantıyı doğrulama ve sorunları giderme.

# Yönlendirici İlk Ayarlarını Yapılandırma Lab – Anahtarlayıcı ve Yönlendirici Ağı Oluştur

Bu Laboratuvara, aşağıdaki hedefler tamamlanacaktır:

- Topolojiyi hazırlama ve cihazları başlatma.
- Aygıtları yapılandırma ve bağlantıyı doğrulama.
- Cihaz bilgilerini görüntüleyin.

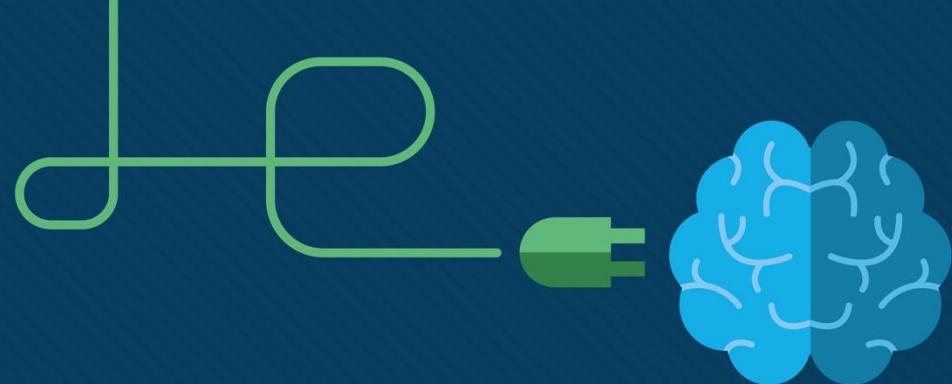
# Bu modülde ne öğrendim?

- Yönlendirici üzerinde ilk ayarları yapılandıırken tamamlanması gereken görevler.
  - Aygit adını yapılandırma.
  - Güvenli ayrıcalıklı (privileged) EXEC modu
  - Kullanıcı EXEC modunu güvenli hale getirme.
  - Güvenli uzaktan Telnet / SSH erişimi.
  - Yapılandırma dosyasındaki tüm parolaları güvenli hale getirme.
  - Yasal bildirim sağlama.
- Yönlendircilere ulaşılabilmesi için yönlendirici arayüzlerinin yapılandırılması gereklidir.
  - **No shutdown** komutunu kullanarak arayüzü etkinleştir. Fiziksel katmanın etkin olması için arayüz anahtarlayıcı veya yönlendirici gibi başka aygıtlara bağlanmalıdır. Arayüz yapılandırmasının durumunu sorgulamak için kullanılabilecek çeşitli komutlar vardır. **show ip interface brief** ve **show ipv6 interface brief**, **show ip route** ve **show ipv6 route**, **show interfaces**, **show ip interface** ve **show ipv6 interface**.

## Bu modülde ne öğrendim? (Devamı)

- Bir son aygıtın diğer ağlara erişmesi için varsayılan ağ geçidinin yapılandırılması gereklidir.
  - Ana bilgisayar aygıtının IP adresi ve yönlendirici arayüzünün adresi aynı ağa olmalıdır.
  - Bir anahtarlayıcının varsayılan ağ geçidi adresi başka bir anahtarlayıcı tarafından uzaktan yapılandırılacak şekilde olmalıdır.
  - Anahtarlayıcındaki varsayılan ağ geçidini yapılandırmak için **ip default-gateway ip-address** global komutunu kullanın.





# Modül 11: IPv4 Adreslesme

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

**Modül Adı:** IPv4 Adresleme

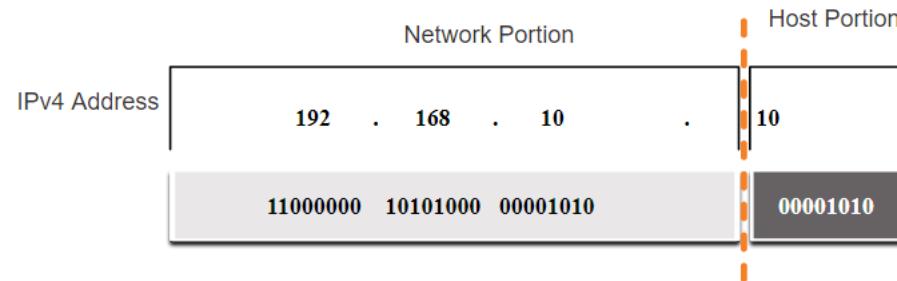
**Modül Hedefi:** Ağınızı verimli bir şekilde bölümlemek için IPv4 alt ağ maskesi ile hesaplama

Konu Başlığı	Konu Hedefi
<b>IPv4 Adres Yapısı</b>	Ağ bilgisi, ana bilgisayar bölümü ve alt ağ maskesini içeren bir IPv4 adresinin yapısını açıklama
<b>IPv4 ile Unicast, Broadcast, ve Multicast yayın yapmak</b>	IPv4 adreslerinin özelliklerini ve kullanımlarını tek noktaya yayın (Unicast), sınırlı yayın (broadcast) ve çok noktaya yayın (Multicast) bakımından karşılaştırma
<b>IPv4 Adres Türleri</b>	Herkese açık (public), özel (private) ve ayrılmış (reserved) IPv4 adres çeşitlerini açıklama
<b>Ağ Bölümleme</b>	Daha verimli iletişim için alt ağ maskeleri ile ağı böülümlendirme
<b>IPv4 Ağı İçin Alt Ağ Maskesi</b>	IPv4 alt ağ maskelerini /24 formatında hesaplama

# 11.1 IPv4 Adres Yapısı

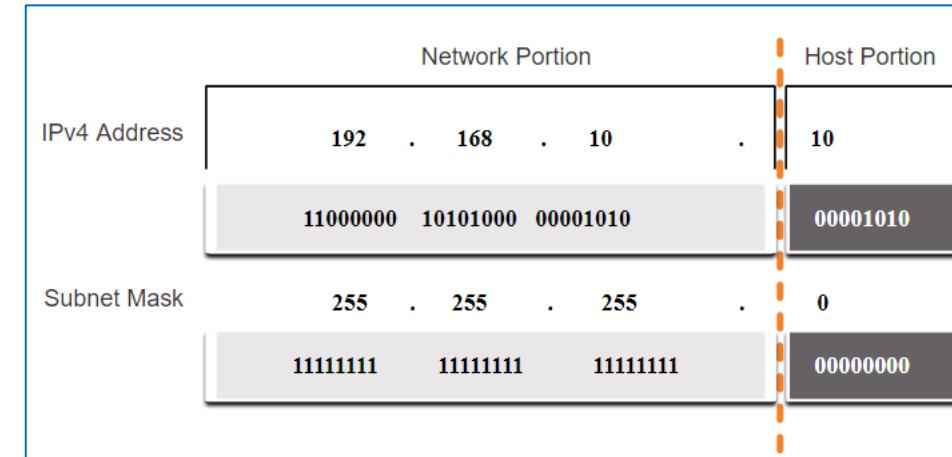
# Ağ ve Ana Bilgisayar Bölümleri

- IPv4 adresi, ağ bölümü ve ana bilgisayar kısmından oluşan 32 bitlik hiyerarşik bir adresstir.
- Ağ bölümünü ana bilgisayar kısmına göre belirlerken, 32 bit formatına bakmanız gereklidir.
- Ağ ve ana bilgisayar bölümlerini belirlemek için bir alt ağ maskesi kullanılır.



# IPv4 Adres Yapısı Alt Ağ Maskesi

- Bir IPv4 adresinin ağ ve ana bilgisayar bölgelerini tanımlamak için, soldan sağa her bir bit için IPv4 adresi ile alt ağ maskesi karşılaştırılır.
- Ağ ve ana bilgisayar bölgelerini tanımlamak için kullanılan bu işleme ANDing denir.



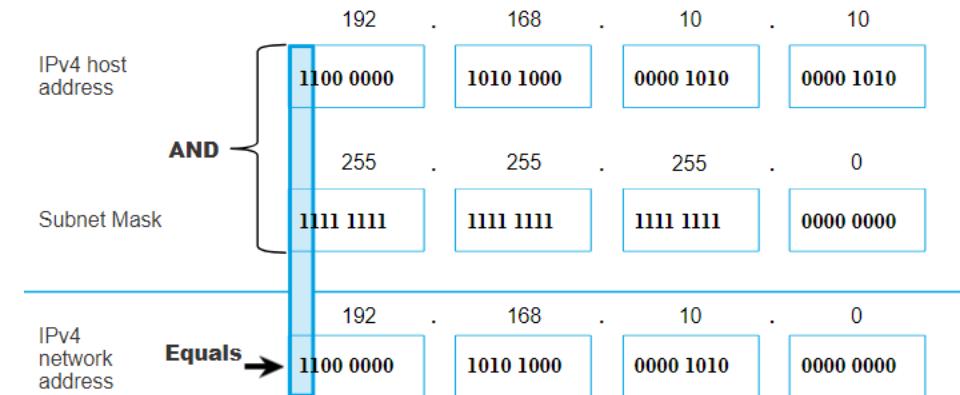
# Önek Uzunluğu (Prefix Length)

- Önek uzunluğu, alt ağ maskesi adresini tanımlamak için kullanılan daha pratik bir yöntemdir.
- Önek uzunluğu, alt ağ maskesinde bit sayısı olarak 1'e ayarlanır.
- "Eğik çizgi" şeklinde yazılmıştır, bu nedenle, alt ağ maskesindeki bit sayısını sayın ve başına bir bölümü çizgisi ekleyin.

Alt Ağ Maskesi	32-bit Adres	Önek Uzunluğu
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

# Ağı Belirleme: Mantıksal AND

- Mantıksal AND Boolean işlemi ağ adresi belirlemede kullanılır.
- Mantıksal AND iki bitin karşılaştırılması işlemidir. Sadece 1 AND 1 karşılaştırmasının sonucu 1'dir, diğer karşılaştırmaların sonucu 0'dır.
- $1 \text{ AND } 1 = 1$ ,  $0 \text{ AND } 1 = 0$ ,  $1 \text{ AND } 0 = 0$ ,  $0 \text{ AND } 0 = 0$
- $1 = \text{Dogru ve}$   $0 = \text{Yanlış}$
- Ağ adresini tanımlamak için, ana bilgisayar IPv4 adresi ile alt ağ maskesi mantıksal olarak teker teker AND edilir.



# Video – Ağ, Ana Bilgisayar ve Yayın Adresleri

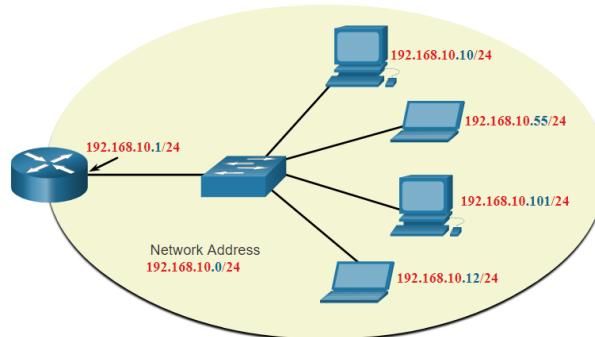
Bu video aşağıdakileri kapsayacaktır:

- Ağ adresleri
- Yayın Adresi
- İlk Kullanılabilir Adres
- Son Kullanılabilir Adres

# Ağ, Ana Bilgisayar ve Yayın Adresleri

- Her ağ içinde üç tür IP adresi vardır:

- Ağ adresi**
- Ana bilgisayar adresleri**
- Yayın adresi**



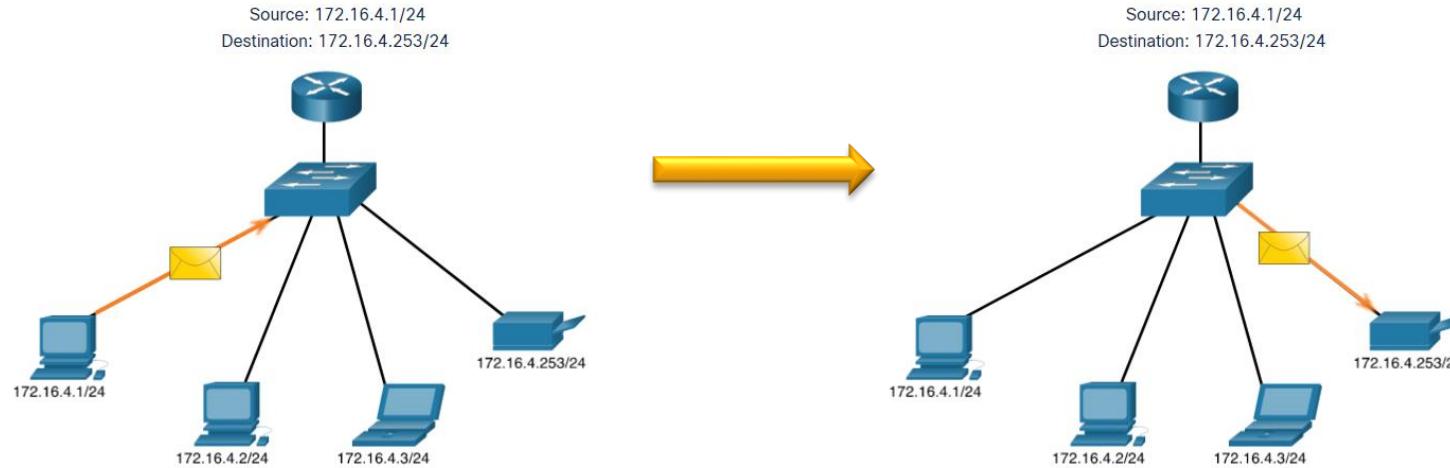
Ağ Bölümü	Ana Bilgisayar Bölümü	Ana Bilgisayar Bitleri
Alt ağ maskesi 255.255.255.0 or /24	255 255 255 11111111 11111111 11111111	0 00000000
Ağ adresi 192.168.10.0 or /24	192 168 10 11000000 10100000 00001010	0 00000000
İlk adres 192.168.10.1 or /24	192 168 10 11000000 10100000 00001010	1 00000001
Son adres 192.168.10.254 or /24	192 168 10 11000000 10100000 00001010	254 11111110
Yayın adresi 192.168.10.255 or /24	192 168 10 11000000 10100000 00001010	255 11111111

# 11.2 IPv4 Unicast, Broadcast ve Multicast Yayınları

# IPv4 Unicast, Broadcast, and Multicast Yayınları

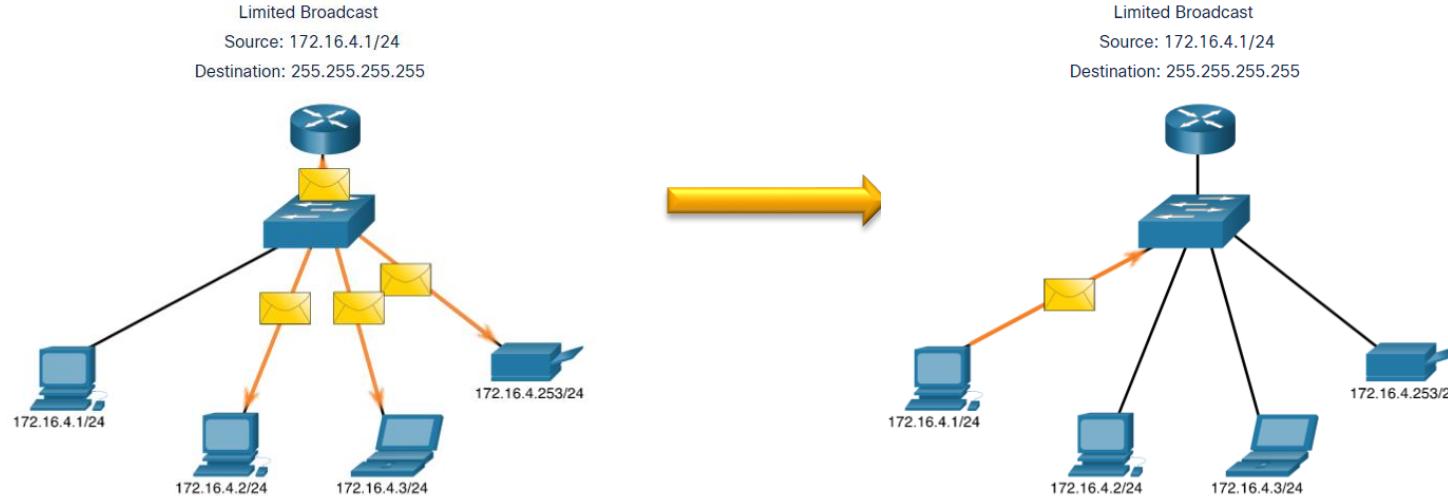
## Unicast Yayınları

- Unicast iletişimde bir hedef IP adresine paket gönderilir.
- Örneğin, **172.16.4.1**'deki bilgisayar **172.16.4.253** deki yazıcıya unicast bir paket gönderiyor.



# IPv4 Unicast, Broadcast, ve Multicast Yayın Broadcast Yayın

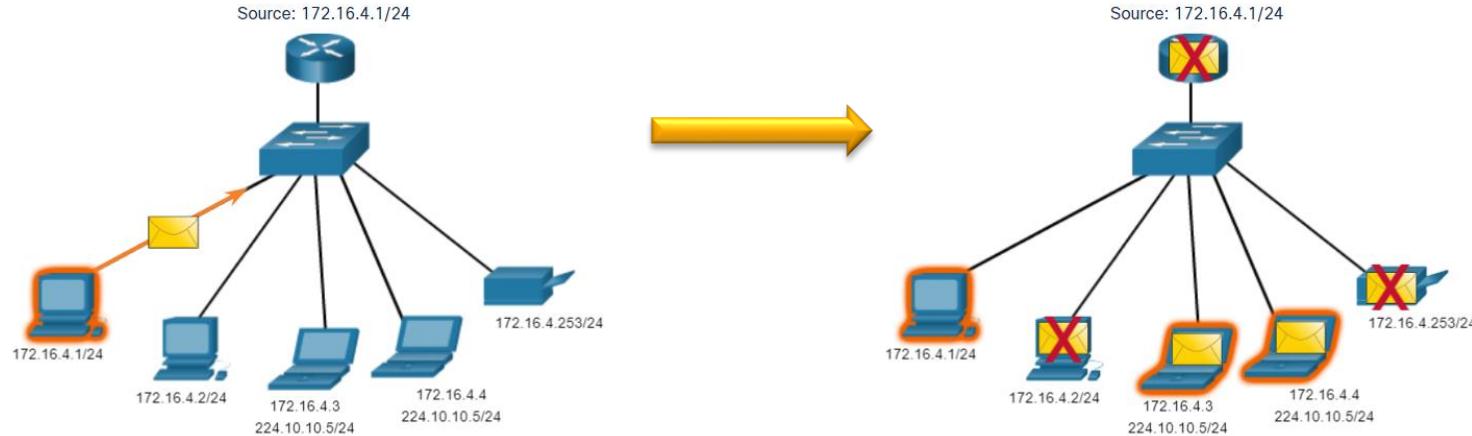
- **Broadcast iletimi**, diğer tüm hedef IP adreslerine bir paket gönderilir.
- Örneğin, **172.16.4.1**'deki bilgisayar kendisi hariç ağıdaki diğer tüm işlemcilere Broadcast paketi yolluyor.



# IPv4 Unicast, Broadcast, ve Multicast Yayını

## Multicast Yayını

- Multicast yayın ile, multicast adres yayın grubuna dahil olan işlemcilere paket gönderilir.
- Örneğin, 172.16.4.1'deki bilgisayar **multicast grup adresi** olan 224.10.10.5 adresine multicast paketi gönderiyor.



# 11.3 IPv4 Adres Türleri

# Genel ve Özel IPv4 Adresleri

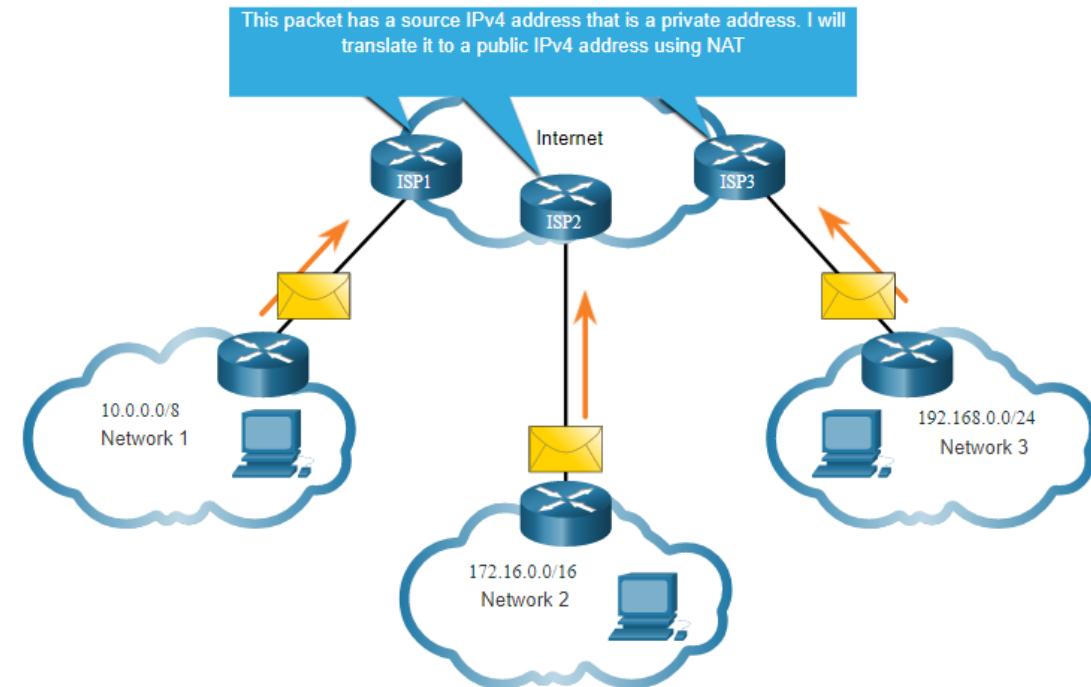
- RFC 1918'de tanımlandığı gibi, genel IPv4 adresleri internet servis sağlayıcısı (ISS) tarafından yönlendiriciler arasında genel olarak adreslenir.
- **Özel adresler, çoğu kuruluş tarafından IPv4 adreslerini dahili ana bilgisayarlaraya atamak için kullanılan ortak adres bloklarıdır.**
- **Özel IPv4 adresleri benzersiz değildir** ve herhangi bir ağ içinde dahili olarak kullanılabilir.
- **Ancak, özel adresler küresel olarak yönlendirilebilir değildir.**

Ağ Adresi ve Önek(Prefix)	RFC 1918 Özel Adres Aralığı
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

# IPv4 Adres Türleri Internet'e yönlendirme

- Ağ Adresi Çevirisi (NAT), **özel IPv4 adreslerini genel IPv4 adreslerine çevirir.**

- NAT genellikle interne bağlanan kenar (edge) yönlendiricide etkinleştirilir.
- Dahili özel adresi genel bir genel IP adresine çevirir.



# Özel Kullanım İçin Olan IPv4 Adresleri

## Loopback addresses

- 127.0.0.0 /8 (127.0.0.1 to 127.255.255.254)
- Yaygın olarak sadece 127.0.0.1 olarak tanımlanır
- TCP/IP'nin çalışır durumda olup olmadığını test etmek için ana bilgisayarda kullanılır.

```
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
```

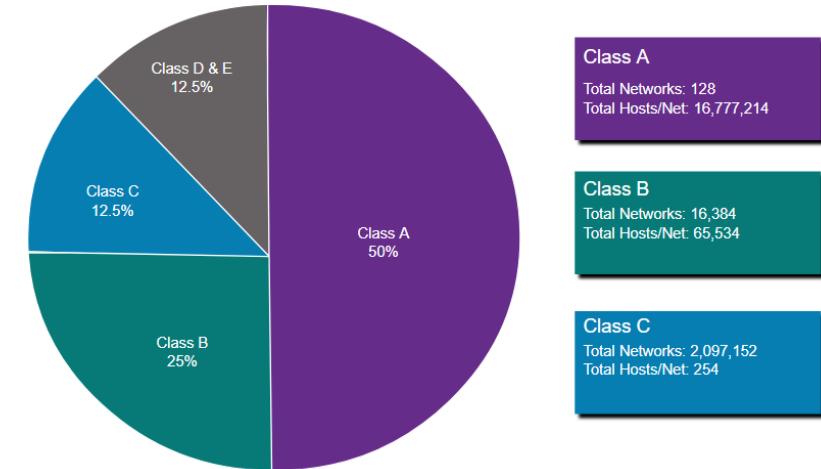
## Link-Local addresses

- 169.254.0.0 /16 (169.254.0.1 to 169.254.255.254)
- Genellikle Otomatik Özel IP Adresleme (APIPA) adresleri veya kendi kendine atanan adresler olarak bilinir.
- Ortamda hiçbir DHCP sunucusu olmadığından, Windows DHCP istemcileri tarafından kendi kendini yapılandırmak için kullanılır.

# Legacy Sınıflandırma Adresleri

RFC 790 (1981)'de ayrılan IPv4 adres sınıfları

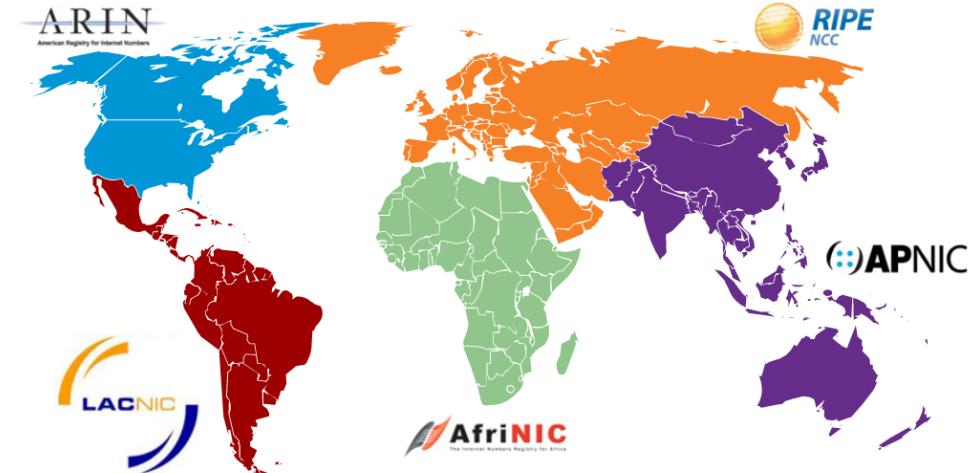
- Sınıf A (0.0.0.0/8 to 127.0.0.0/8)
- Sınıf B (128.0.0.0 /16 – 191.255.0.0 /16)
- Sınıf C (192.0.0.0 /24 – 223.255.255.0 /24)
- Sınıf D (224.0.0.0 to 239.0.0.0)
- Sınıf E (240.0.0.0 – 255.0.0.0)
- **Sınıflandırma adresleri ile birçok IPv4 adresi boş harcanmıştır.**



Sınıflı adres ayırma, sınıfların kurallarını (A, B, C) yok sayan sınıfsız adresleme ile değiştirildi.

# IP Adreslerinin Atanması

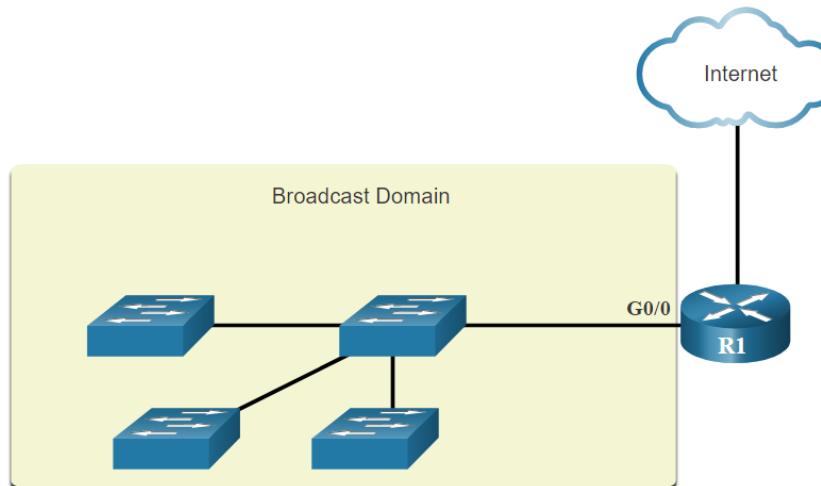
- **Internet Atanmış Sayılar Yetkilisi (IANA)**, IPv4 ve IPv6 adreslerinin bloklarını beş Bölgesel İnternet Kaydına (RI) göre yönetir ve ayırrır.
- 
- RI'ler, IP adreslerini daha küçük ISS'lere ve kuruluşlara IPv4 adres blokları sağlayan ISS'lere ayırmakla yükümlüdür.



# 11.4 Ağ Bölümleme

# Yayın Etki Alanları ve Segmentasyon

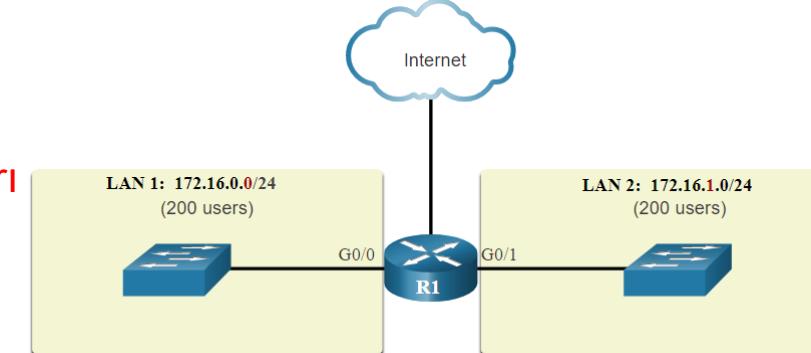
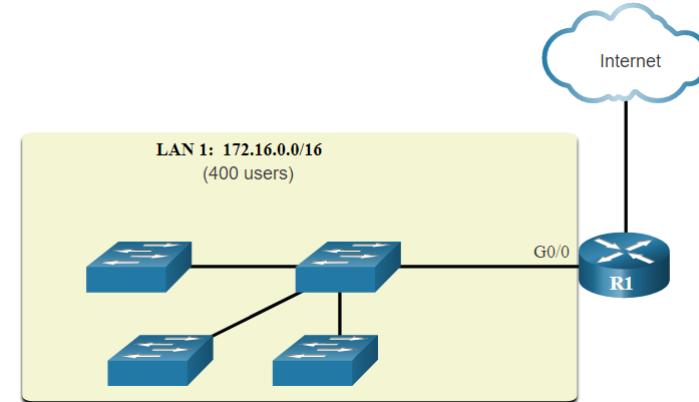
- Birçok protokol **broadcast** veya **multicast** yayını kullanılır (örneğin, ARP protokolü diğer cihazları bulmak için Broadcast yayını kullanır, ana bilgisayarlar bir DHCP sunucusu bulmak için DHCP discover yayınıları gönderir.)
- Anahtarlayıcılar tüm arayüzlerinden gelen broadcast yayınlarını alır ve yaymaya devam eder.



- Yayınları durduran tek cihaz yönlendiricidir.
- **Yönlendiriciler yayınıları yaymaz.**
- Her yönlendirici arayüzü bir **yayın etki alanına bağlanır** ve yayınlar yalnızca belirli bir yayın etki alanı içinde yayılır.

# Büyük Broadcast Etki Alanları Problemleri

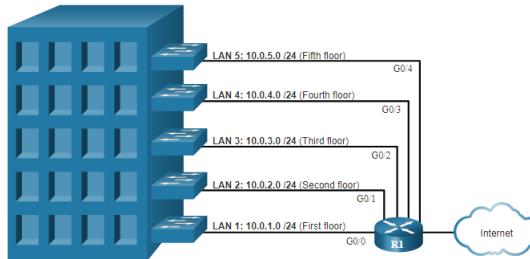
- Geniş bir yayın etki alanıyla ilgili bir sorun, bu ana bilgisayarların **aşırı yayın üretebilmesi** ve **ağı olumsuz etkileyebilmesidir.**
- Çözüm, **alt ağ oluşturma** adı verilen bir işlemde daha küçük yayın etki alanları **oluşturmak** için ağın boyutunu azaltmaktır.
- Ağ adresi **172.16.0.0 /16'yi** her biri 200 kullanıcından **iki alt ağına bölmek:** 172.16.0.0 /24 ve 172.16.1.0 /24.
- Yayınlar yalnızca daha küçük yayın etki alanları içinde yayılır.**



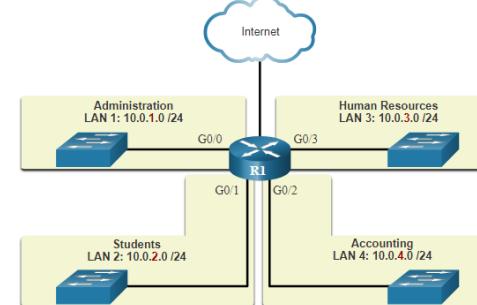
# Ağ Bölümleme Ağları Bölme Nedenleri

- Subnetting genel ağ trafiğini azaltır ve ağ performansını artırır.
- Subnetler arasında güvenlik ilkeleri uygulamak için kullanılabilir.
- Subnetting anomal yayın trafiği etkilenen aygıtların sayısını azaltır.
- Subnetler(Alt ağlar) dahil olmak üzere çeşitli nedenlerle kullanılır:

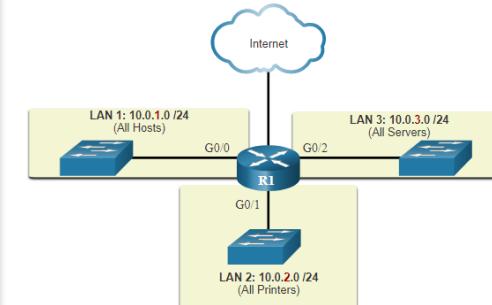
Location



Group or Function



Device Type



# 11.5 IPv4 Ağlarındaki Subnet

# Oktet Sistemindeki Subnetleme

- Ağlar en kolay /8, /16 ve /24 subnetlerinde kullanılır.
- Daha uzun **prefix uzunlukları kullanmanın ana bilgisayar sayısını azalttığını** dikkat edin.

Prefix Length	Subnet Mask	Subnet Mask in Binary (n = network, h = host)	# of hosts
/8	255.0.0.0	nnnnnnnn.hhhhhh.hhhhhh.hhhhhh 11111111.00000000.00000000.00000000	16,777,214
/16	255.255.0.0	nnnnnnnn.nnnnnnnn.hhhhhh.hhhhhh 11111111.11111111.00000000.00000000	65,534
/24	255.255.255.0	nnnnnnnn.nnnnnnnn.nnnnnnnn.hhhhhh 11111111.11111111.11111111.00000000	254

# Oktet sistemindeki Subnetleme(Devamı)

- İlk tabloda  $10.0.0.0/8$  /16 ve ikinci tabloda bir /24 subnetleme kullanılmıştır.

<b>Subnet Address (256 Possible Subnets)</b>	<b>Host Range (65,534 possible hosts per subnet)</b>	<b>Broadcast</b>
<b>10.0.0.0/16</b>	<b>10.0.0.1 - 10.0.255.254</b>	<b>10.0.255.255</b>
<b>10.1.0.0/16</b>	<b>10.1.0.1 - 10.1.255.254</b>	<b>10.1.255.255</b>
<b>10.2.0.0/16</b>	<b>10.2.0.1 - 10.2.255.254</b>	<b>10.2.255.255</b>
<b>10.3.0.0/16</b>	<b>10.3.0.1 - 10.3.255.254</b>	<b>10.3.255.255</b>
<b>10.4.0.0/16</b>	<b>10.4.0.1 - 10.4.255.254</b>	<b>10.4.255.255</b>
<b>10.5.0.0/16</b>	<b>10.5.0.1 - 10.5.255.254</b>	<b>10.5.255.255</b>
<b>10.6.0.0/16</b>	<b>10.6.0.1 - 10.6.255.254</b>	<b>10.6.255.255</b>
<b>10.7.0.0/16</b>	<b>10.7.0.1 - 10.7.255.254</b>	<b>10.7.255.255</b>
...	...	...
<b>10.255.0.0/16</b>	<b>10.255.0.1 - 10.255.255.254</b>	<b>10.255.255.255</b>

<b>Subnet Address (65,536 Possible Subnets)</b>	<b>Host Range (254 possible hosts per subnet)</b>	<b>Broadcast</b>
<b>10.0.0.0/24</b>	<b>10.0.0.1 - 10.0.0.254</b>	<b>10.0.0.255</b>
<b>10.0.1.0/24</b>	<b>10.0.1.1 - 10.0.1.254</b>	<b>10.0.1.255</b>
<b>10.0.2.0/24</b>	<b>10.0.2.1 - 10.0.2.254</b>	<b>10.0.2.255</b>
...	...	...
<b>10.0.255.0/24</b>	<b>10.0.255.1 - 10.0.255.254</b>	<b>10.0.255.255</b>
<b>10.1.0.0/24</b>	<b>10.1.0.1 - 10.1.0.254</b>	<b>10.1.0.255</b>
<b>10.1.1.0/24</b>	<b>10.1.1.1 - 10.1.1.254</b>	<b>10.1.1.255</b>
<b>10.1.2.0/24</b>	<b>10.1.2.1 - 10.1.2.254</b>	<b>10.1.2.255</b>
...	...	...
<b>10.100.0.0/24</b>	<b>10.100.0.1 - 10.100.0.254</b>	<b>10.100.0.255</b>
...	...	...
<b>10.255.255.0/24</b>	<b>10.255.255.1 - 10.255.255.254</b>	<b>10.255.255.255</b>

# Oktet Sistemindeki Subnetleme

- /24 şeklinde olan bir ağ 6 farklı yolla bölebiliriz.

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

# Video – Subnet Mask (Alt Ağ Maskesi)

- Bu video subnetting işlemlerini göstermektedir.

# Video – Sihirli Sayı ile Subnetleme

- Bu video sihirli numarası ile subnetting gösterecektir.

# Paket Tracer – IPv4 Ağındaki Subnetleme

Bu Paket Tracer'da, aşağıdakileri yapacaksınız::

- IPv4 Ağ Alt Ağ Şeması Tasarlama
- Cihazları Yapılandırma
- Ağ Test Etme ve Sorun Giderme

# 11.6 /16 ve /8 Subnetleme

# /16 ile Subnet Yaratma

- Tablo /16 ile yapılabilecek tüm muhtemel subnetleri gösterir.

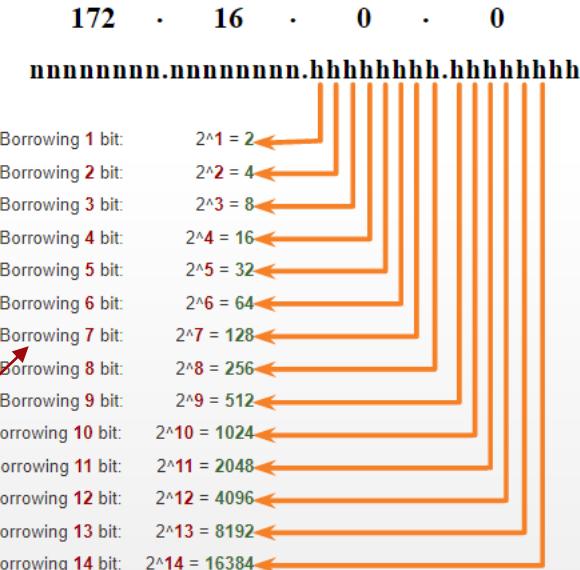
Prefix Length	Subnet Mask	Network Address (n = network, h = host)	# of subnets	# of hosts
/17	255.255.128.0	nnnnnnnn.nnnnnnnn. <b>n</b> hhhhh.hhhhhh 11111111.11111111. <b>1</b> 0000000.00000000	2	32766
/18	255.255.192.0	nnnnnnnn.nnnnnnnn. <b>nn</b> hhhhh.hhhhhh 11111111.11111111. <b>11</b> 000000.00000000	4	16382
/19	255.255.224.0	nnnnnnnn.nnnnnnnn. <b>nnn</b> hhhh.hhhhhh 11111111.11111111. <b>111</b> 00000.00000000	8	8190
/20	255.255.240.0	nnnnnnnn.nnnnnnnn. <b>nnnn</b> hhh.hhhhhh 11111111.11111111. <b>1111</b> 0000.00000000	16	4094
/21	255.255.248.0	nnnnnnnn.nnnnnnnn. <b>nnnnn</b> hh.hhhhhh 11111111.11111111. <b>11111</b> 000.00000000	32	2046
/22	255.255.252.0	nnnnnnnn.nnnnnnnn. <b>nnnnn</b> hh.hhhhhh 11111111.11111111. <b>111111</b> 00.00000000	64	1022
/23	255.255.254.0	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> h.hhhhhh 11111111.11111111. <b>11111110</b> .00000000	128	510
/24	255.255.255.0	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> hh.hhhhhh 11111111.11111111. <b>11111111</b> .00000000	256	254
/25	255.255.255.128	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> n.hhhhhh 11111111.11111111. <b>11111111</b> .10000000	512	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> n. <b>n</b> hhh 11111111.11111111. <b>11111111</b> .11000000	1024	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> n. <b>nn</b> hhh 11111111.11111111. <b>11111111</b> .11100000	2048	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> n. <b>nnn</b> hhh 11111111.11111111. <b>11111111</b> .11110000	4096	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> n. <b>nnnnn</b> hh 11111111.11111111. <b>11111111</b> .11111000	8192	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn. <b>nnnnnnn</b> n. <b>nnnnn</b> hh 11111111.11111111. <b>11111111</b> .11111100	16384	2

# /16 ile 100 Subnet oluşturma

**En az 100 Subnet (alt ağ) gerektiren ve dahili ağ adresi (Network Adresi) olarak 172.16.0.0/16 olan büyük bir kuruluş düşünün.**

- Şekil, üçüncü oktet ve dördüncü oktetten 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).

**Kuruluşa 100 alt ağ gereksinimini karşılamak için, 7 bitin** (yani,  $2^7 = 128$  alt ağ) ödünç alınması gereklidir (toplam 128 alt ağ için).



# /8 ile 1000 Subnet oluşturma

Ağ adresi 10.0.0.0/8 olan ve istemcileri için **1000** (subnet) alt ağ gerektiren küçük bir ISS düşünün, bu da ağ kısmında 8 bit ve alt ağ dan ödünç almak için kullanılabilir 24 ana bilgisayar biti olduğu anlamına gelir.

- Şekil, ikinci ve üçüncü bitlerden borçlandırılırken oluşturulabilecek alt ağ sayısını (Subnet) görüntüler.
- Şu anda ödünç alınabilecek en fazla 22 ana bilgisayar biti olduğuna dikkat edin (yani, son iki bit ödünç alınamaz).

Kuruluşa 1000 alt ağ gereksinimini karşılamak için, **10 bit** (yani,  $2^{10}=1024$  alt ağlar) ödünç alınması gereklidir (toplam 128 alt ağ için)



# Video – Birden Fazla Octetli Arası Subnetleme

Bu video birden fazla Octet arasında subnet oluşturma gösterecektir.

# Lab – IPv4 Alt Ağlarını Hesapla

Bu laboratuvara, aşağıdaki hedefler tamamlanacaktır:

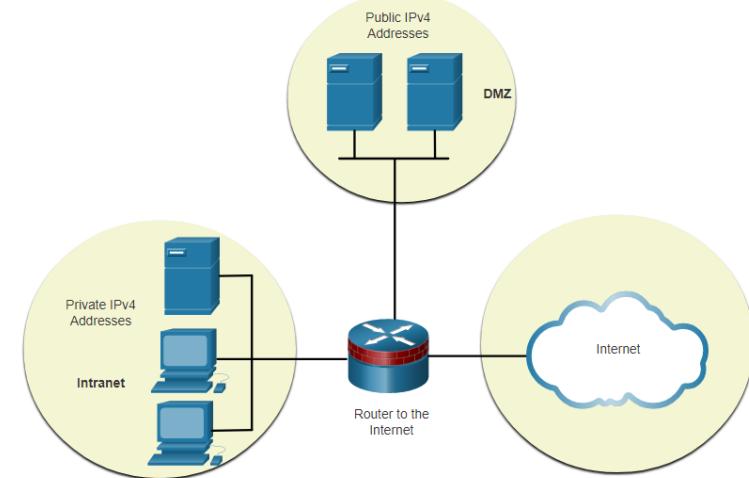
- Bölüm 1: IPv4 Adres Subnetleri Belirleme
- Part 2: IPv4 Adres Subnetleri Hesaplama

# 11.7 Gereksinimleri Karşılamak için Subnet

# Gereksinimleri Karşılamak İçin Subnet Subnet Private karşı Genel IPv4 Adres Alanı

Kurumsal ağlar şunlara sahiptir:

- **Intranet** - Bir şirketin dahili ağı genellikle özel IPv4 adreslerini kullanır.
- **DMZ** – **Karşılıklı olan şirket internet sunucular.** DMZ'deki aygıtlar genel IPv4 adreslerini kullanır.
- Bir şirket /16 veya /24 ağ sınırında 10.0.0.0/8 ve alt ağı kullanabilir.
- **DMZ aygıtlarının genel IP adresleriyle yapılandırılması** gereklidir.



# Gereksinimleri Karşılamak için Subnet Kullanılmayan Ana Bilgisayar IPv4 Adreslerini En Aza Indirin ve Alt Ağları En Üst Düzeye Çıkarın

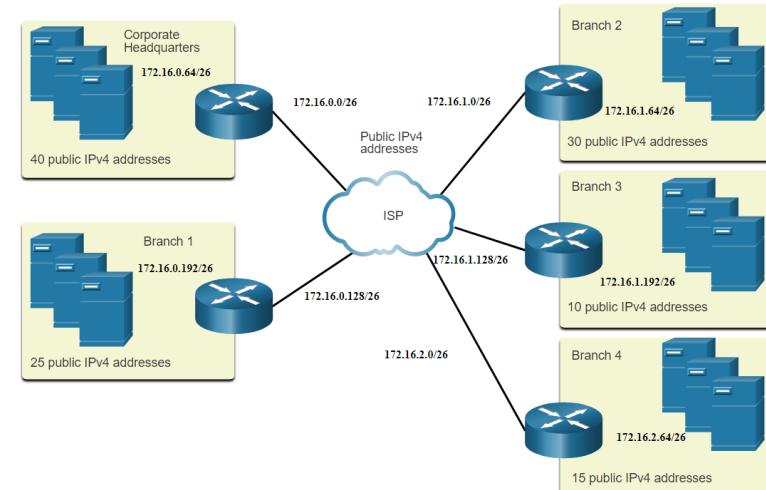
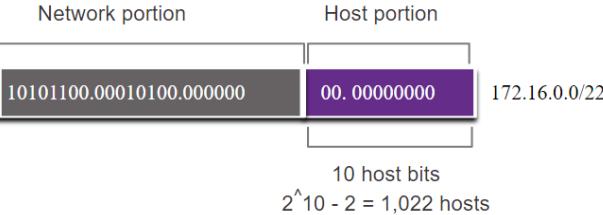
Alt ağları planlarken göz önünde bulundurulması gereken noktalar:

- Her ağ için gereken ana bilgisayar adreslerinin sayısı
- Gerekli tek tek alt ağ 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. <b>n</b> hhhhhhh 11111111.11111111.11111111. <b>1</b> 0000000	2	126
/26	255.255.255.192	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nn</b> hhhhhhh 11111111.11111111.11111111. <b>11</b> 000000	4	62
/27	255.255.255.224	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnn</b> hhhhhhh 11111111.11111111.11111111. <b>111</b> 00000	8	30
/28	255.255.255.240	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnn</b> hhh 11111111.11111111.11111111. <b>1111</b> 0000	16	14
/29	255.255.255.248	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnnn</b> hh 11111111.11111111.11111111. <b>11111</b> 000	32	6
/30	255.255.255.252	nnnnnnnn.nnnnnnnn.nnnnnnnn. <b>nnnnnn</b> hh 11111111.11111111.11111111. <b>111111</b> 00	64	2

# Gereksinimleri Karşılamak İçin Subnet Örnek: Verimli IPv4 Subnetleme

- Bu örnekte, şirket merkezi **1.022** ana bilgisayar adresi sağlayan ISS tarafından **172.16.0.0/22** (10 ana bilgisayar biti) ortak ağ adresi tahsis edilmiştir.
- Beş site** ve bu nedenle **beş internet bağlantısı**, yani kuruluşun en büyük alt ağa sahip 10 alt ağ için 40 adres gerektirdiği anlamına gelir.
- 
- Bir /26 (yani, 255.255.255.192) alt ağ maskesi ile 10 alt ağ tahsis edilir.



# Gereksinimleri Karşılamak İçin Subnet Paket Tracer - Subnetting Senaryo

Bu Paket Tracer'da, aşağıdakileri yapacaksınız::

- IP Adresleme Şeması Tasarlama
- IP Adreslerini Ağ Aygıtlarına Atama ve Bağlantıyı Doğrulama

# 11.8 VLSM (Değişken Uzunluklu Alt Ağ Maskeleri)

# Video – VLSM Temelleri

- Bu video VLSM temellerini açıklayacaktır.

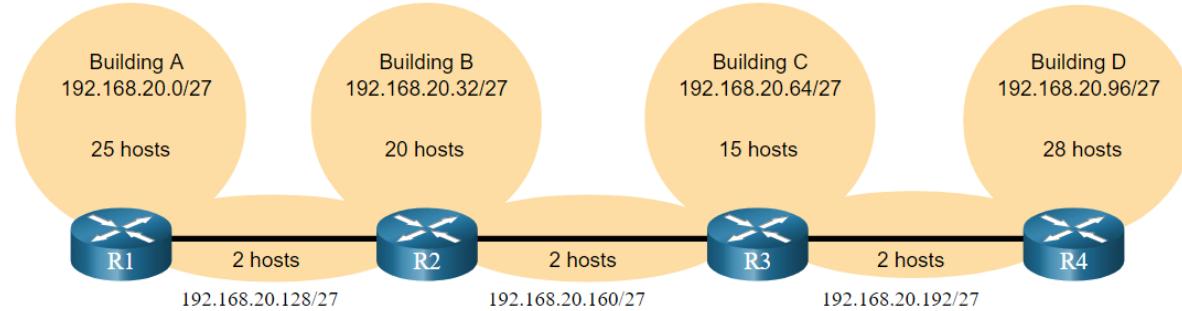
# Video – VLSM Örneği

- Bu video, ağın ihtiyaçlarına göre özel alt ağlar oluşturmayı gösterir.

# IPv4 Adres Koruma

Topoloji göz önüne alındığında, **7 alt ağ** (yani, *dört LAN ve üç WAN bağlantıları*) gereklidir ve **en fazla sayıda ana bilgisayar, 28 ana bilgisayarla D Binası'ndadır.**

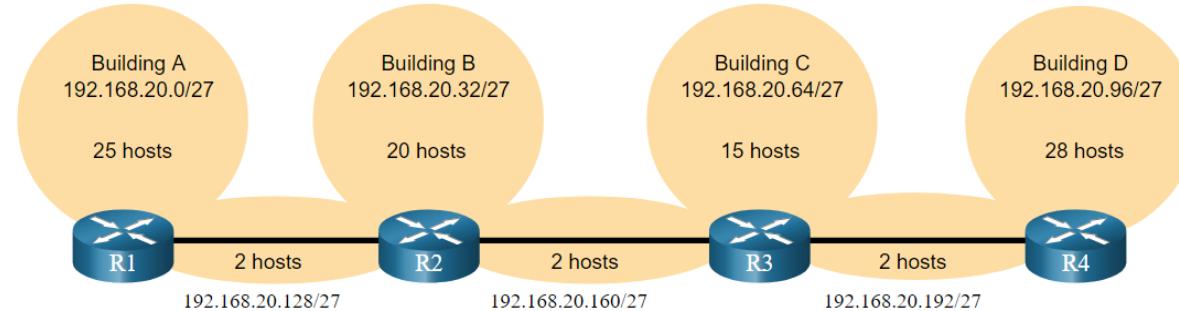
- Bir /27 maskesi **30 ana bilgisayar** IP adresinin **8 subneti sağlar** ve bu nedenle bu topolojiyi destekler.



# IPv4 Adres Koruma (Devamı)

Ancak, **noktadan noktaya WAN bağlantıları** yalnızca **iki adres gereklidir** ve bu nedenle **her biri toplam 84 kullanılmayan adres için 28 adresi boş harcar.**

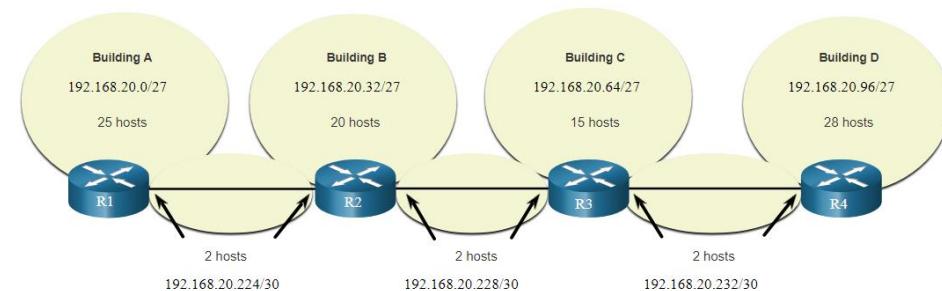
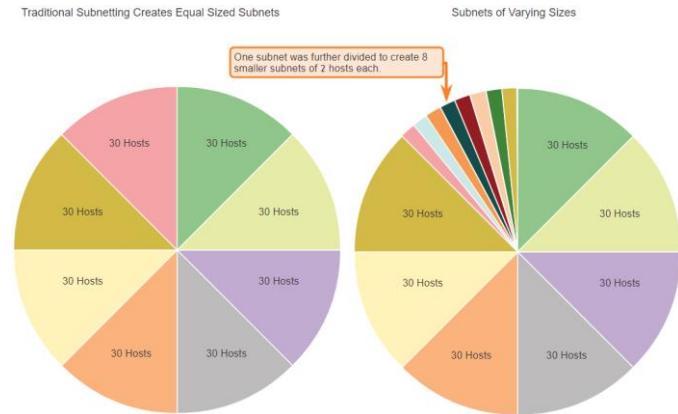
Host portion  
 $2^5 - 2 = 30$  host IP addresses per subnet  
30 – 2 = 28  
Each WAN subnet wastes 28 addresses  
 $28 \times 3 = 84$   
84 addresses are unused



- Bu senaryoya geleneksel bir alt ağ maskesi uygulamak çok verimli değildir ve boş IP adresi harcamak demektir.
- VLSM, bir alt ağ sağlamamızı sağlayarak adreslerin israf edilmesini önlemek için geliştirilmiştir.

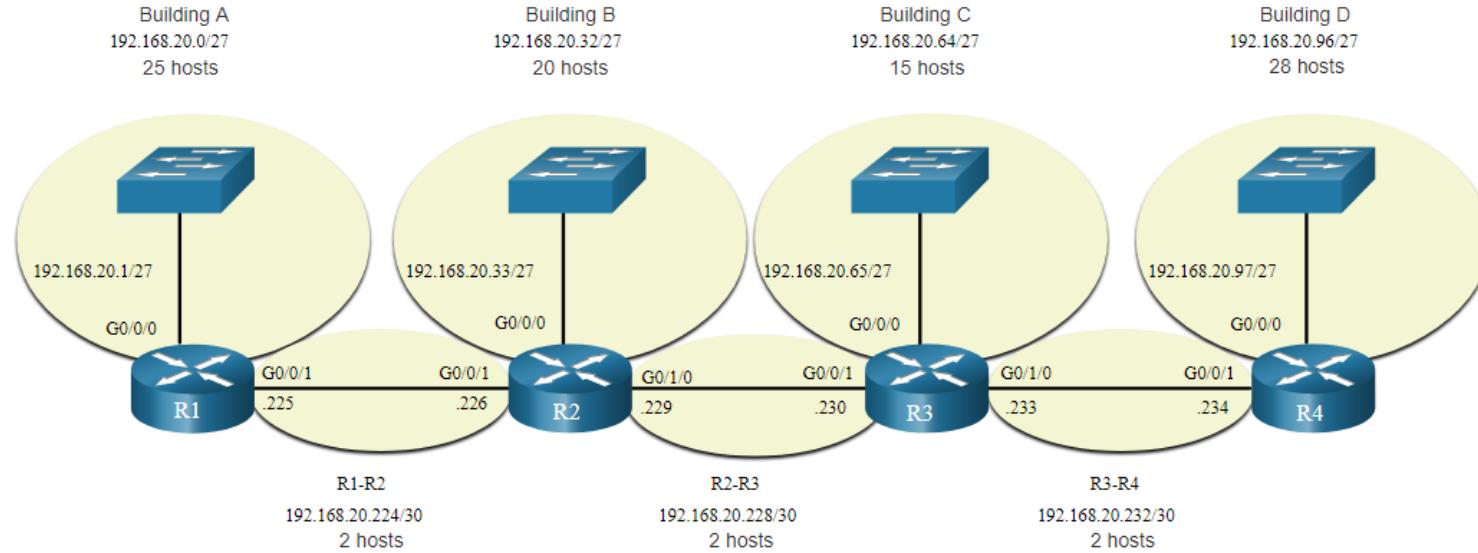
# VLSM

- Sol tarafta geleneksel alt ağ şeması (yani aynı alt ağ maskesi) görüntülenirken, sağ taraf VLSM'nin bir alt ağının alt ağda nasıl kullanabileceğini ve son alt ağın sekiz /30 alt ağa nasıl bölebileceğini gösterir.
- VLSM kullanırken, **her zaman en büyük alt ağın ana bilgisayar gereksinimlerini karşılayarak başlayın ve en küçük alt ağın ana bilgisayar gereksinimleri karşılanıncaya kadar alt ağlandırmaya devam edin.**
- Ortaya çıkan topolojiye VLSM uygulandı.



# VLSM Topoloji Adres Atama

- VLSM alt ağları kullanılarak, LAN ve yönlendirici ağları mantıksal topoloji diyagramında gösterildiği gibi gereksiz adresler olmadan ele alınabilir.



# 11.9 Yapılandırılmış Tasarım

IP ağ planlaması, kurumsal bir ağa ölçeklenebilir bir çözüm geliştirmek için çok önemlidir.

- Bir IPv4 ağ geniş adresleme şeması geliştirmek için
- kaç alt ağ gerektiğini,
- belirli bir alt ağ kaç ana bilgisayar gerektirdiğini,
- alt ağın hangi aygıtların alt ağın parçası olduğunu,
- ağınızın hangi bölümlerinin özel adresleri kullandığını
- hangilerinin genel adresleri kullandığını ve
- diğer birçok belirleyici etkeni bilmeniz gereklidir.

# Yapilandırılmış Tasarım IPv4 Ağ Adres Planlama

**Bir kuruluşun ağ kullanımının gereksinimlerini ve alt ağların nasıl yapılandırılacağını inceleyin.**

- Her alanın nasıl bölgelere alınacağını belirlemek için tüm ağa bakarak bir ağ gereksinimi çalışması gerçekleştirin.
- Kaç alt ağ gerektiğini ve alt ağ başına kaç ana bilgisayar gerektiğini belirleyin.
- DHCP adres havuzlarını ve Katman 2 VLAN havuzlarını belirlemeyin.

# Yapilandırılmış Tasarım Cihaz Adresi Atama

Bir ağ içinde, adres gerektiren farklı aygit türleri vardır:

- **Son kullanıcı istemcileri** – Coğu, ağ destek personeli üzerindeki hataları ve yükü azaltmak için DHCP kullanır. IPv6 istemcileri DHCPv6 veya SLAAC kullanarak adres bilgilerini edinebilirler
- **Sunucular ve çevre birimleri (Peripherals)**– Bunlar öngörelebilir statik bir IP adresine sahip olmalıdır.
- **Internet'ten erişilebilen sunucular** – Sunucuların genel bir IPv4 adresi olmalıdır ve en sık olarak NAT kullanılır.
- **Ara aygıtlar** – Aygıtlara ağ yönetimi, izleme ve güvenlik için adresler atanır.
- **Ağ Geçidi** – *Yönlendiriciler ve güvenlik duvarı aygıtları*, bu ağdaki ana bilgisayarlar için ağ geçididir.

Bir IP adresleme düzeni geliştirirken, genellikle adreslerin her aygit türüne nasıl ayrılacağına dair bir dizi desenin olması önerilir.

# Paket Tracer – VLSM Tasarım ve Uygulama Uygulaması

Bu Paket Tracer'da, aşağıdakileri yapacaksınız::

- Ağ Gereksinimlerini İnceleme
- VLSM Adresleme Şemasını Tasarlama
- Cihazlara IP Adresleri Atama ve Bağlantıyı Doğrulama

# 11.10 Modül Uygulama ve Sınav

# Packet Tracer – VLSM Adresleme Şeması Tasarla ve Uygula

Bu Paket Tracer'da, aşağıdakileri yapacaksınız::

- Gereksinimler verilen bir VLSM IP adresleme şeması tasarlama
- Ağ aygıtlarında ve ana bilgisayarlarda adres yapılandırma
- IP bağlantısını doğrulama
- Gerektiğinde bağlantı sorunlarını giderme.

# Laboratuvar - VLSM Adresleme Şeması Tasarla ve Uygula

Bu laboratuvara, aşağıdaki hedefleri tamamlayacaktır:

- Ağ Gereksinimlerini İncele
- VLSM Adres Şemasını Tasarla
- Kablo ve IPv4 Ağ Yapılandırılması
-

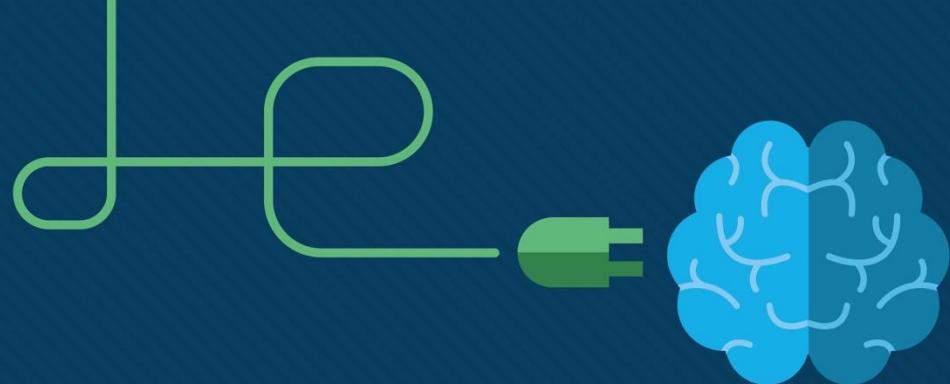
## Bu modülde ne öğrendim??

- IP adresleme yapısı, bir ağı ve ana bilgisayar bölümünü tanımlayan 32 bit hiyerarşik ağ adresinden oluşur. Ağ aygıtları, ağ ve ana bilgisayar bölgelerini tanımlamak için IP adresini ve ilişkili alt ağ maskesini kullanarak ANDing adı verilen bir işlem kullanır.
- Hedef IPv4 paketleri, unicast, broadcast, ve multicast olabilir.
- IANA tarafından küresel yönlendirilebilir IP adresleri vardır ve küresel olarak yönlendirilemez ancak tüm dahili özel ağlarda kullanılabilen üç farklı aralıkta özel IP ağ adresleri vardır.
- Daha küçük yayın etki alanları oluşturmak, genel ağ trafiğini azaltmak ve ağ performansını artırmak için alt ağları kullanarak büyük yayın etki alanlarını azaltılır.
- Ağ bitleri olarak bir veya daha fazla ana bilgisayar bitini kullanarak IPv4 alt ağları oluşturulabilir. Ancak, ağlar en kolay şekilde / 8, / 16 ve / 24 alt ağlarına bölünebilir.
- Kullanılmayan ana bilgisayar adreslerinin alt ağ başına sayısını azaltmak için VLSM'yi kullanın.

## Bu modülde ne öğrendim? (Devamı)

- VLSM, ağ alanının eşit olmayan parçalara bölünmesini sağlar. Her zaman en büyük alt ağın ana bilgisayar gereksinimlerini karşılayarak başlayın. En küçük alt ağın ana bilgisayar gereksinimleri karşılanındakialt ağlandırmaya devam edin.
- Ağ adresleme şeması tasarlarken; DMZ ,iç ve dış gereksinimleri göz önünde bulundurun. Adreslerin her aygit türüne nasıl tahsis edildiğini gösteren bir dizi şema içeren tutarlı bir IP adresleme şeması kullanın.





# Module 12: IPv6 Adresleme

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

**Modül Başlığı:** IPv6 Adresleme

**Modül Hedefi:** Bir IPv6 Adresleme şeması uygulayın.

Konu Başlığı	Konu Amaç
IPv4 Sorunları	IPv6 adresleme ihtiyacını açıklayın.
IPv6 Adres Gösterimi	IPv6 adreslerinin nasıl temsil edildiğini açıklayın.
IPv6 Adres Türleri	IPv6 ağ adresi türlerini karşılaştırın.
GUA ve LLA Statik Yapılandırma	Statik genel tek noktaya yayın ve bağlantı yerel IPv6 ağ adreslerinin nasıl yapılandırılacağını açıklayın.
IPv6 GUA'lar için Dinamik Adresleme	Global tek noktaya yayın adreslerinin dinamik olarak nasıl yapılandırılacağını açıklayın.

# Modül Hedefleri (Devam)

## Modül Başlığı: IPv6 Adresleme

**Modül Hedefi :** Bir IPv6 Adresleme şeması uygulayın.

Konu Başlığı	Konu Amaç
IPv6 LLA'lar için Dinamik Adresleme	Bağlantı yerel adresleri dinamik olarak yapılandırın.
IPv6 Çok Noktaya Yayın Adresleri	IPv6 adreslerini tanımlayın.
IPv6 Ağına Alt Ağ	Alt ağa sahip bir IPv6 adresleme şeması uygulayın.

# 12.1 IPv4 Sorunları

## IPv6 için Gereken IPv4 Sorunları

- ❖ IPv4 adresleri tükeniyor.
- ❖ IPv6, çok daha büyük 128 bit adres alanına sahiptir.
- ❖ IPv6'nın geliştirilmesi, IPv4 sınırlamaları ve diğer geliştirmeler için düzeltmeleri de içermektedir.
- ❖ Artan internet nüfusu, sınırlı bir IPv4 adres alanı, **NAT** ve **IoT** ile ilgili sorunlar ile IPv6'ya geçişe başlama zamanı gelmiştir.



## IPv4 Sorunları IPv4 ve IPv6 Bir Arada Var Olma

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

IETF, ağ yöneticilerinin ağlarını IPv6'ya taşımalarına yardımcı olmak için çeşitli protokoller ve araçlar oluşturmuştur.

Bu geçiş teknikleri üç kategoriye ayrılabilir:

- **Çift yığın** - Cihazlar hem IPv4 hem de IPv6 protokol yığınlarını aynı anda çalıştırır.
- **Tünelleme** - Bir IPv6 paketini bir IPv4 ağı üzerinden taşıma yöntemidir.
- **IPv6 paketi, bir IPv4 paketi içinde kapsülleñir.**
- **Çeviri** - Ağ Adresi Çevirisi 64 (NAT64), IPv6 etkin aygıtların IPv4 için NAT'a benzer bir çeviri teknigi kullanarak IPv4 etkin aygıtlarla iletişim kurmasını sağlar.



**Not:** Tünel oluþturma ve çeviri yerel IPv6'ya geçiş içindir ve yalnızca ihtiyaç duyulduğunda kullanılmalıdır. **Hedef, kaynaktan hedefe yerel IPv6 iletişim olmalıdır.**

# 12.2 IPv6 Adres Gösterimi

# IPv6 Adres Formatları

- **IPv6 adresleri** 128 bit uzunluğundadır ve onaltılık olarak yazılmıştır.
- **IPv6 adresleri büyük / küçük harfe duyarlı değildir ve küçük veya büyük harfle yazılabilir.**
- **Bir IPv6 adresi** yazmak için tercih edilen format x: x: x: x: x: x: x: x şeklindedir ve her "x" dört onaltılık değerden oluşur.
- IPv6'da, bir hekstet, 16 bitlik bir segmenti veya dört onaltılık değeri ifade etmek için kullanılan resmi olmayan bir terimdir.
- Tercih edilen formattaki IPv6 adreslerine örnekler:

2001: 0db8: 0000: 1111: 0000: 0000: 0000: 0200

2001: 0db8: 0000: 00a3: abcd: 0000: 0000: 1234

# Kural 1 - Baştaki Sıfırı Atla

IPv6 adreslerinin gösterimini azaltmaya yardımcı olacak ilk kural, baştaki 0'ları (sıfırları) atlamaktır.

## Örnekler:

- 01ab, 1ab olarak temsil edilebilir
- 09f0, 9f0 olarak temsil edilebilir
- 0a00, a00 olarak temsil edilebilir
- 00ab, ab olarak temsil edilebilir

**Not : Bu kural yalnızca baştaki 0'lar için geçerlidir, sondaki 0'lar için DEĞİL, aksi takdirde adres belirsiz olur.**

Tür	Birim
Tercihli	2001: 0 db8: 000 0: 1111: 000 0: 000 0: 000 0: 0 200
Önde sıfır yok	2001: db8: 0: 1111: 0: 0: 0: 200

# IPv6 Adres Gösterimi Kural 2 – Çift Kolon

**Çift iki nokta üst üste (::),** tümü sıfırlardan oluşan bir veya daha fazla 16-bit hextets herhangi bir tek, bitişik dizesinin yerini alabilir.

**Misal:**

- 2001: db8: cafe: 1: 0: 0: 0: 1 (baştaki 0'lar atlandı) 2001: db8: cafe: 1 :: 1 olarak gösterilebilir.

**Not : Çift iki nokta üst üste (::) bir adres içinde yalnızca bir kez kullanılabilir, aksi takdirde birden fazla sonuçta ortaya çıkan olası adres olabilir.**

Tür	Biçim
Tercihli	2001: 0 db8: 000 0: 1111: 0000 : 0000 : 0000 : 0 200
Sıkıştırılmış	2001: db8: 0: 1111 :: 200

# 12.3 IPv6 Adres Türleri

# Unicast, Multicast, Anycast

IPv6 adreslerinin üç geniş kategorisi vardır:

- **Unicast** - Unicast, IPv6 özellikli bir cihazdaki bir arabirimini benzersiz şekilde tanımlar.
- **Çoklu Yayın** - Çoklu yayın, tek bir IPv6 paketini birden çok hedefe göndermek için kullanılır.
- **Anycast** - Bu, birden çok aygıta atanabilen herhangi bir IPv6, tek noktaya yayın adresidir. **Her noktaya yayın adresine gönderilen bir paket, bu adrese sahip en yakın cihaza yönlendirilir**

Not : **IPv4'ün aksine, IPv6'nın yayın adresi yoktur.**

Ancak, temelde aynı sonucu veren bir IPv6, **tüm düğümlü çok noktaya yayın adresi vardır.**

# IPv6 Önek Uzunluğu

- Önek uzunluğu, eğik çizgi ile temsil edilir ve bir IPv6 adresinin ağ bölümünü belirtmek için kullanılır.
- IPv6 ön ek uzunluğu 0 ila 128 arasında değişebilir.
- LAN'lar ve diğer ağ türlerinin çoğu için önerilen IPv6 ön ek uzunluğu / 64'tür.

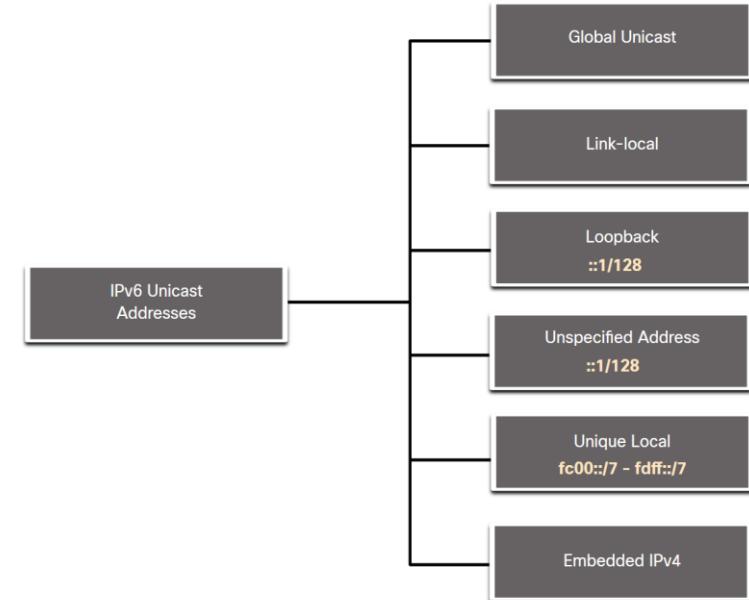


**Not :** Çoğu ağ için 64 bit Arabirim Kimliği kullanılması şiddetle önerilir. Bunun nedeni, durum bilgisi olmayan otomatik adres yapılandırmasının (SLAAC) Arabirim Kimliği için 64 bit kullanmasıdır. Ayrıca, alt ağ oluşturmanın oluşturulmasını ve yönetilmesini kolaylaştırır.

# IPv6 Tek Noktaya Yayın Adres Türleri

Yalnızca tek bir adrese sahip IPv4 cihazlarının aksine, **IPv6 adresleri genellikle iki tek noktaya yayın adresine sahiptir:**

- **Global Tek Noktaya Yayın Adresi (GUA)** - Bu, genel bir IPv4 adresine benzer. Bunlar küresel olarak benzersiz, internete yönlendirilebilir adreslerdir.
- **Yerel Bağlantı Adresi (LLA)** - Her IPv6 etkin aygıt için gereklidir ve aynı yerel bağlantıdaki diğer aygıtlarla iletişim kurmak için kullanılır. **LLA'lar yönlendirilemez** ve tek bir bağlantıyla sınırlıdır.



# Benzersiz Yerel Adres Hakkında Bir Not

IPv6 benzersiz yerel adresleri (fc00 :: / 7 - fdff :: / 7 aralığı), IPv4 için RFC 1918 özel adresleriyle bazı benzerliklere sahiptir, ancak önemli farklılıklar vardır:

- Benzersiz yerel adresler, *bir site içinde veya sınırlı sayıda site arasında yerel adresleme* için kullanılır.
- Hiçbir zaman başka bir ağa erişmesi gerekmeyen cihazlar için benzersiz yerel adresler kullanılabilir.
- Benzersiz yerel adresler genel olarak yönlendirilmez veya genel bir IPv6 adresine çevrilmez.

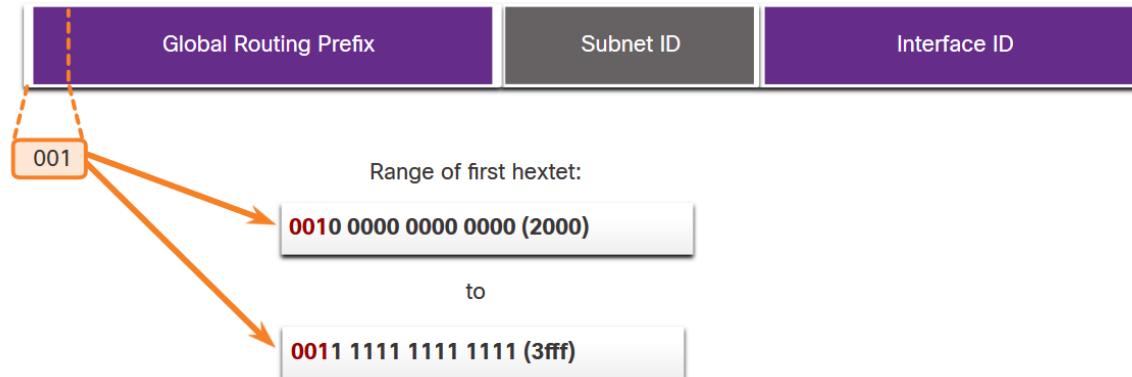
**Not :** Birçok site, ağlarını potansiyel güvenlik risklerinden korumak veya gizlemek için RFC 1918 adreslerinin özel doğasını kullanır. Bu asla ULA'ların amaçlanan kullanımı olmadı.

# IPv6 Adres Türleri

## IPv6 GUA

IPv6 global tek noktaya yayın adresleri (GUA'lar) küresel olarak benzersizdir ve IPv6 internet üzerinden yönlendirilebilir.

- Şu anda, yalnızca **001** veya **2000 :: / 3'ün ilk üç bitine sahip GUA'lar** atanmaktadır.
- Şu anda mevcut GUA'lar 2 veya 3 ondalık sayı ile başlar (**Bu, kullanılabilir toplam IPv6 adres alanının yalnızca 1 / 8'i**dir).



# IPv6 GUA Yapısı

## Global Yönlendirme Öneki:

- *Global yönlendirme öneki*, bir ISP gibi sağlayıcı tarafından bir müşteriye veya siteye atanın adresin öneki veya ağ kısmıdır. Global yönlendirme öneki, ISP politikalarına bağlı olarak değişecektir.

## Alt Ağ Kimliği:

- Alt Ağ Kimliği alanı, **Global Yönlendirme Öneki ile Arayüz Kimliği arasındaki alandır.**
- Alt Ağ Kimliği, bir kuruluş tarafından kendi sitesindeki alt ağları tanımlamak için kullanılır.

## Arayüz Kimliği:

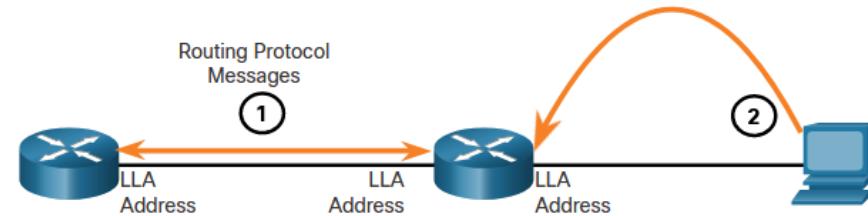
- *IPv6 arabirim kimliği*, bir IPv4 adresinin ana bilgisayar kısmına eşdeğerdir. Çoğu durumda 64 bit arabirim kimliği oluşturan 64 alt ağın kullanılması şiddetle önerilir.

**Not :** IPv6, all-0'ların ve all-1'lerin ana bilgisayar adreslerinin bir cihaza atanmasına izin verir. All-0s adresi bir Alt Ağ Yönlendirici her noktaya yayın adresi olarak ayrılmıştır ve yalnızca yönlendiricilere atanmalıdır.

# IPv6 LLA

Bir IPv6 bağlantı yerel adresi (LLA), bir aygıtın aynı bağlantı üzerindeki diğer IPv6 etkin aygıtlarla ve yalnızca bu bağlantı (alt ağ) üzerinden iletişim kurmasını sağlar.

- **Kaynak veya hedef LLA'ya sahip paketler yönlendirilemez.**
  - IPv6'nın etkin olduğu her ağ arayüzünde bir LLA olmalıdır.
  - Bir LLA, bir arayüzde manuel olarak yapılandırılmamışsa, cihaz otomatik olarak bir LLA oluşturacaktır.
  - IPv6 LLA'lar **fe80 :: / 10** aralığındadır.



1. Routers use the LLA of neighbor routers to send routing updates.
2. Hosts use the LLA of a local router as the default-gateway.

# 12.4 GUA ve LLA Statik Yapılandırma

# Bir Yönlendiricide Statik GUA Yapılandırması

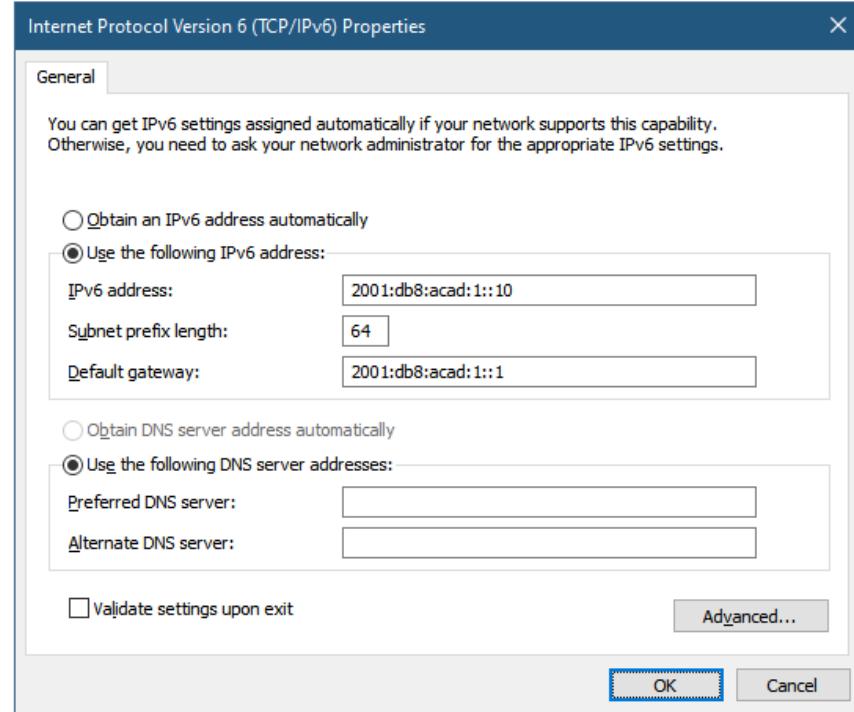
- Cisco IOS'taki çoğu IPv6 yapılandırma ve doğrulama komutları, IPv4 emsallerine benzer.
- Coğu durumda, tek fark, komutlar içinde **ip** yerine **ipv6** kullanılmasıdır .
- Bir arabirimde IPv6 GUA yapılandırma komutu şudur: *ipv6 adresi / önek uzunluğu*.
- Örnek, R1 üzerindeki G0 / 0/0 arayüzünde bir 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
```

# Windows Ana Bilgisayarında Statik GUA Yapılandırması

- IPv6 adresini bir ana bilgisayarda manuel olarak yapılandırmak, bir IPv4 adresini yapılandırmaya benzer.
- Yönlendirici arayüzünün GUA veya LLA'sı varsayılan ağ geçidi olarak kullanılabilir. En iyi uygulama, LLA'yı kullanmaktadır.**

**Not :** DHCPv6 veya SLAAC (otomatik adres yapılandırmasının) kullanıldığında, yönlendiricinin LLA'sı otomatik olarak varsayılan ağ geçidi adresi olarak belirtilecektir.



# Link-Local Unicast Adreslerinin GUA da Statik Yapılandırılması

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

- LLA'lar, **ipv6 adresi ipv6-bağlantı-yerel-adres bağlantı-yerel** komutu kullanılarak manuel olarak yapılandırılabilir .
- Örnek, R1 üzerindeki G0 / 0/0 arayüzünde bir LLA yapılandırmak için komutları 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 :** Aynı LLA, o bağlantıda benzersiz olduğu sürece her bağlantı için yapılandırılabilir.

Yayın uygulama, yönlendiriciyi ve belirli arabirimini tanımlamayı kolaylaştırmak için yönlendiricinin her arabiriminde farklı bir LLA oluşturmaktadır.

# 12.5 IPv6 GUA'lar için Dinamik Adresleme

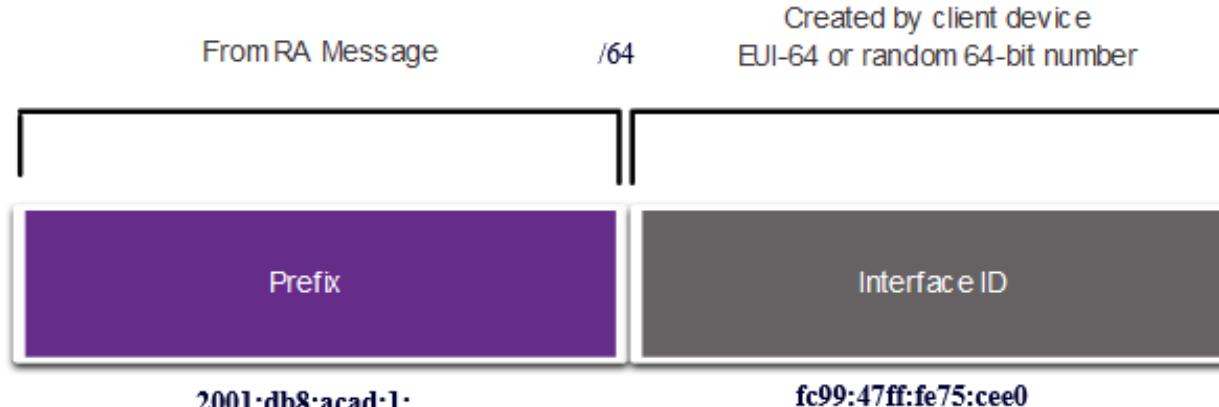
# RS and RA Mesajları için Dinamik Adresleme

Aygıtlar, GUA adreslerini Internet Denetim İletisi Protokolü sürüm 6 (ICMPv6) iletileri aracılığıyla dinamik olarak alır.

- Yönlendirici Talep (RS) mesajları, IPv6 yönlendiricilerini keşfetmek için ana cihazlar tarafından gönderilir
- Yönlendirici Tanıtımı (RA) mesajları, ana bilgisayarlara bir IPv6 GUA'nın nasıl alınacağı konusunda bilgi vermek ve aşağıdaki gibi yararlı ağ bilgileri sağlamak için yönlendiriciler tarafından gönderilir:
  - \* Ağ öneki ve önek uzunluğu
  - \* Varsayılan ağ geçidi adresi
  - \* DNS adresleri ve alan adı
  - \* RA, bir IPv6 GUA yapılandırması için üç yöntem sağlayabilir:
    - 1- SLAAC
    - 2- Durum bilgisi olmayan DHCPv6 sunuculu SLAAC
    - 3- Durum bilgili DHCPv6 (SLAAC yok)

# Yöntem 1: SLAAC (Otomatik Adres Yapılandırması )

- SLAAC, bir cihazın DHCPv6 hizmetleri olmadan bir GUA'yı yapılandırmamasına izin verir.
- **Aygıtlar, yerel yönlendiricinin ICMPv6 RA mesajlarından bir GUA yapılandırmak için gerekli bilgileri alır.**
- **Ön ek, RA (Yönlendirisi Tanıtım) tarafından sağlanır ve cihaz, bir arabirim kimliği oluşturmak için EUI-64 veya rastgele oluşturma yöntemini kullanır.**

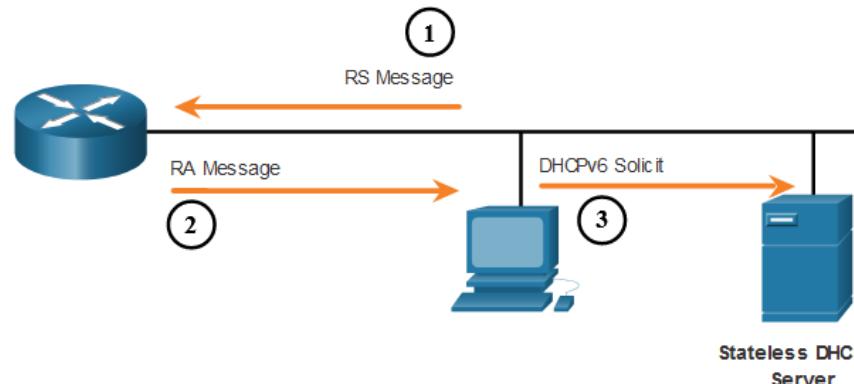


## Yöntem 2: SLAAC ve Durumsuz DHCP

Bir RA, bir aygıta hem SLAAC hem de durum bilgisiz DHCPv6'yi kullanma talimatı verebilir.

RA mesajı, cihazların aşağıdakileri kullandığını gösterir:

- SLAAC kendi IPv6 GUA'sını oluşturmak için
- Varsayılan ağ geçidi adresi olarak RA kaynağı, IPv6 adresi olan yönlendirici LLA'sını
- DNS sunucusu adresi ve etki alanı adı gibi düzen bilgileri almak için durum bilgisiz bir DHCPv6 sunucusunu



## Yöntem 3: Durum bilgili DHCPv6

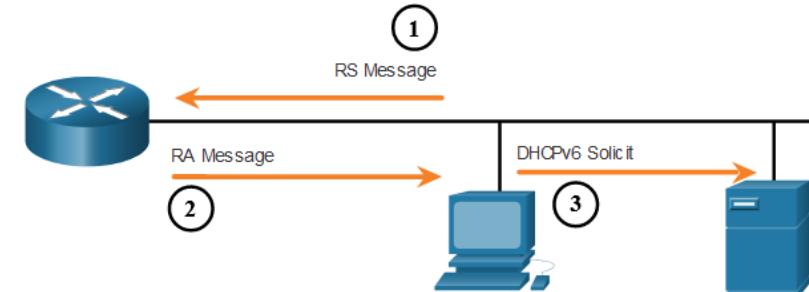
- RA, bir aygıta yalnızca durum bilgisi olan DHCPv6'yi kullanma talimatı verebilir.

Durum bilgisi olan DHCPv6, IPv4 için DHCP'ye benzer.

Bir cihaz, durum bilgisi olan bir DHCPv6 sunucusundan otomatik olarak bir GUA, önek uzunluğu ve DNS sunucularının adreslerini alabilir.

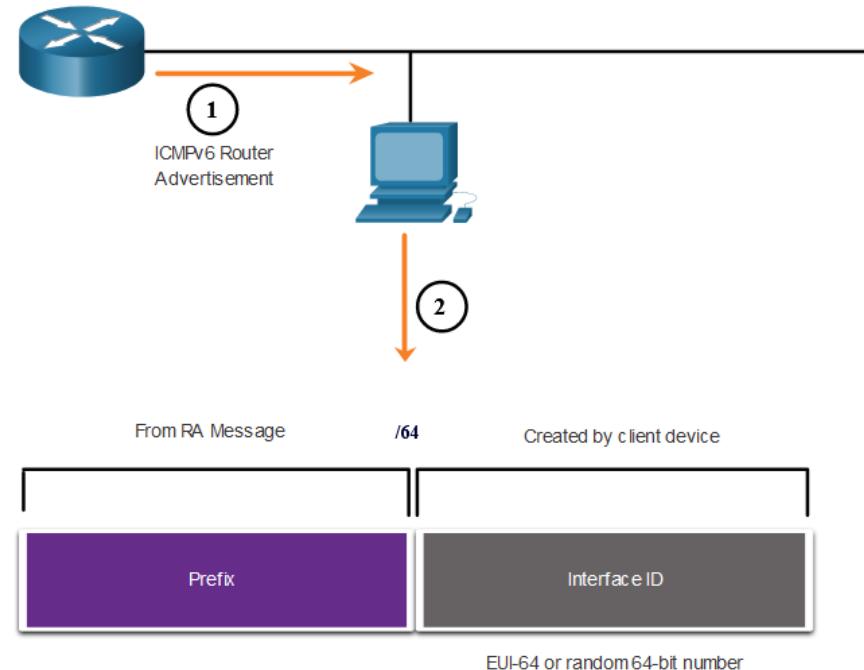
- RA mesajı, cihazların aşağıdakileri kullandığını gösterir:

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



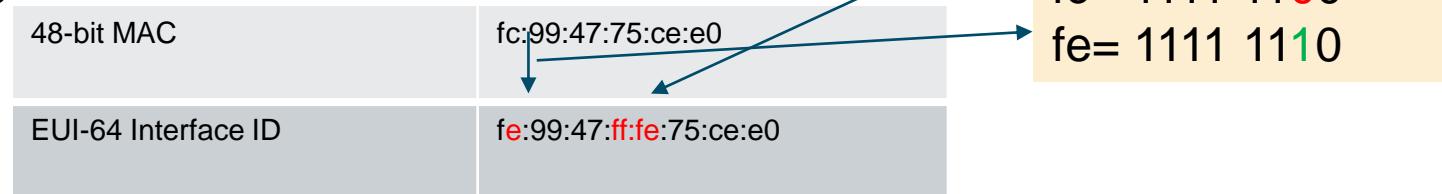
# EUI-64 Süreci ile Rastgele Oluşturulan Karşılaştırması

- ❑ RA mesajı, durum bilgisi olmayan DHCPv6 ile SLAAC veya **SLAAC** olduğunda, istemcinin kendi arayüz kimliğini oluşturması gereklidir.
- ❑ Arayüz kimliği, EUI-64 işlemi veya **rastgele oluşturulmuş 64 bitlik bir sayı** kullanılarak oluşturulabilir.



**IEEE**, aşağıdakileri gerçekleştiren **Genişletilmiş Benzersiz Tanımlayıcıyı** (EUI) veya değiştirilmiş EUI-64 sürecini tanımlamıştır:

- İstemcinin **48 bitlik Ethernet MAC adresinin ortasına 16 bitlik bir fffe değeri (onaltılık olarak) eklenir.**
- İstemci MAC adresinin 7. biti ikili 0'dan 1'e ters çevrilir.
- Örneğin:



# Rastgele Oluşturulan Arayüz Kimlikler

- **İşletim sistemine bağlı olarak, bir cihaz, MAC adresini ve EUI-64 işlemini kullanmak yerine rastgele oluşturulan bir arayüz kimliği kullanabilir.**
- Windows Vista'dan başlayarak, Windows, EUI-64 ile oluşturulan yerine rasgele oluşturulmuş bir arabirim 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:\>
```

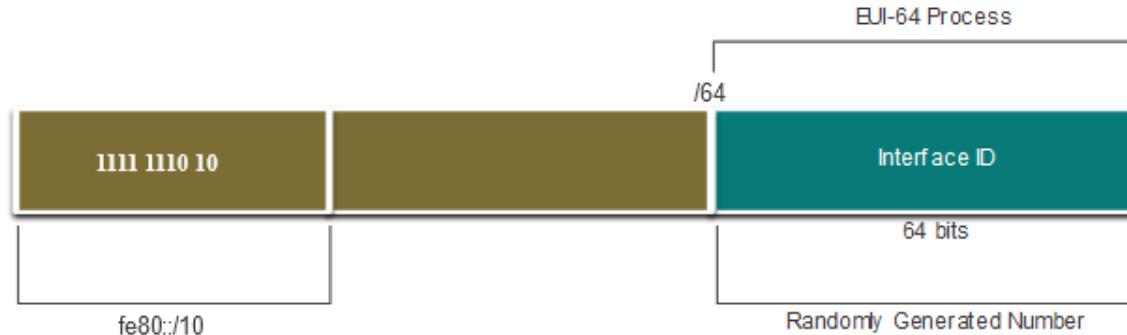
**Not :** Herhangi bir IPv6 tek noktaya yayın adresinin benzersizliğini sağlamak için istemci, **Yinelenen Adres Algılama (DAD)** olarak bilinen bir işlem kullanabilir. Bu, kendi adresi için yapılan ARP talebine benzer. Cevap yoksa adres benzersizdir.

# 12.6 IPv6 LLA'lar için Dinamik Adresleme

# IPv6 LLA'lar için Dinamik Adresleme

## Dinamik LLA'lar

- Tüm IPv6 arabirimlerinin bir IPv6 LLA'sı olmalıdır.
- IPv6 GUA'lar gibi, LLA'lar da **dinamik olarak yapılandırılabilir**.
- Şekil, LLA'nın **fe80 :: / 10 öneki ve EUI-64 işlemi** veya **rastgele oluşturulmuş 64 bitlik** bir sayı kullanılarak arabirim kimliği kullanılarak **dinamik olarak oluşturulduğunu göstermektedir**.



# IPv6 LLA'lar için Dinamik Adresleme Windows'ta Dinamik LLA'lar

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

EUI-64 Oluşturulan Arayüz Kimliği:

```
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:\>
```

# Cisco Yönlendiricilerde Dinamik LLA'lar

- Cisco yönlendiricileri, arayüze bir GUA atandığında otomatik olarak bir IPv6 LLA oluşturur.
- **Varsayılan olarak, Cisco IOS yönlendiricileri**, IPv6 arayüzlerindeki tüm LLA'lar için arayüz kimliği oluşturmak **için EUI-64'ü 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
```

# Packet Tracer –IPv6 Adreslemeyi Yapılandırma

- **Bu Paket İzleyicide aşağıdakileri yapacaksınız:**

- \* Yönlendiricide IPv6 Adreslemeyi yapılandırın
- \* Sunucularda IPv6 Adreslemeyi yapılandırın
- \* İstemcilerde IPv6 Adreslemeyi yapılandırın
- \* Ağ bağlantısını test edin ve doğrulayın

# 12.7 IPv6 Multicast Adresleri

# Atanan IPv6 Multicast Adresleri

IPv6 çok multicast yayın adresleri **ff00 :: / 8** önekine sahiptir.

İki tür IPv6 çok noktaya yayın adresi vardır:

1. Tanınmış çok noktaya yayın adresleri
2. İstenen düğüm çok noktaya yayın adresler

**Not : Çoklu yayın adresleri yalnızca hedef adresler olabilir, kaynak adresler olamaz.**

# İyi Bilinen IPv6 Multicast Adresleri

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

**İki yaygın IPv6 Atanmış çok noktaya yayın grubu vardır:**

**1- ff02 :: 1 Tüm düğümler çok noktaya yayın grubu –**

- Bu, tüm IPv6 etkin aygıtların katıldığı bir çok noktaya yayın grubudur.
- **Bu gruba gönderilen bir paket, bağlantı veya ağ üzerindeki tüm IPv6 arayüzleri tarafından alınır ve işlenir.**

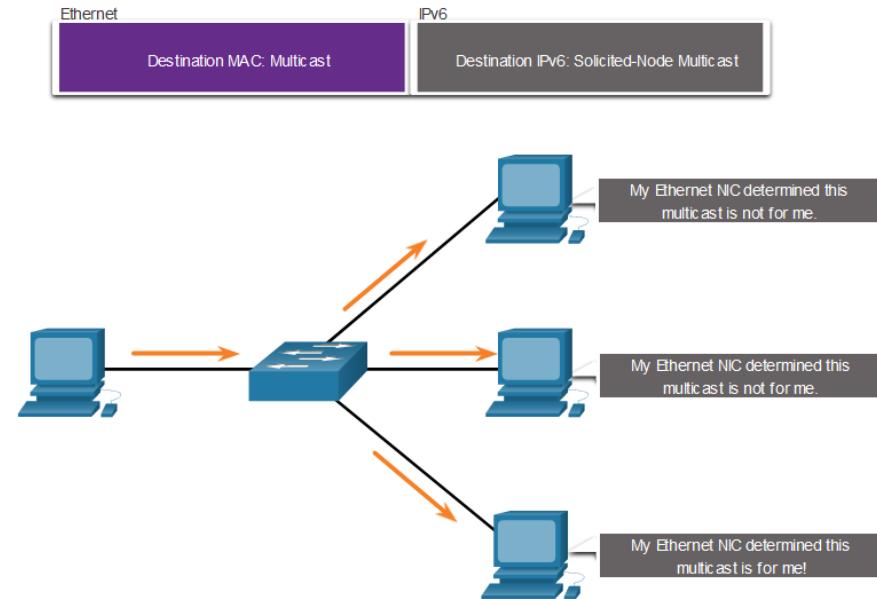
# İyi Bilinen IPv6 Multicast Adresleri

## 2- ff02 :: 2 Tüm yönlendiriciler çok noktaya yayın grubu –

- Bu, tüm IPv6 yönlendiricilerinin katıldığı bir çok noktaya yayın grubudur.
- Bir yönlendirici, ipv6 tek noktaya yayın yönlendirme genel yapılandırma komutuyla bir IPv6 yönlendiricisi olarak etkinleştirildiğinde bu grubun bir üyesi olur .

# İstenen Düğüm IPv6 Multicast

- İstenen düğümlü çok noktaya yayın adresi, tüm düğümler çok noktaya yayın adresine benzer.
- İstenen düğümlü 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.



# Lab –IPv6 Adreslerini Belirleyin

**Bu laboratuvara aşağıdaki hedefleri tamamlarsınız:**

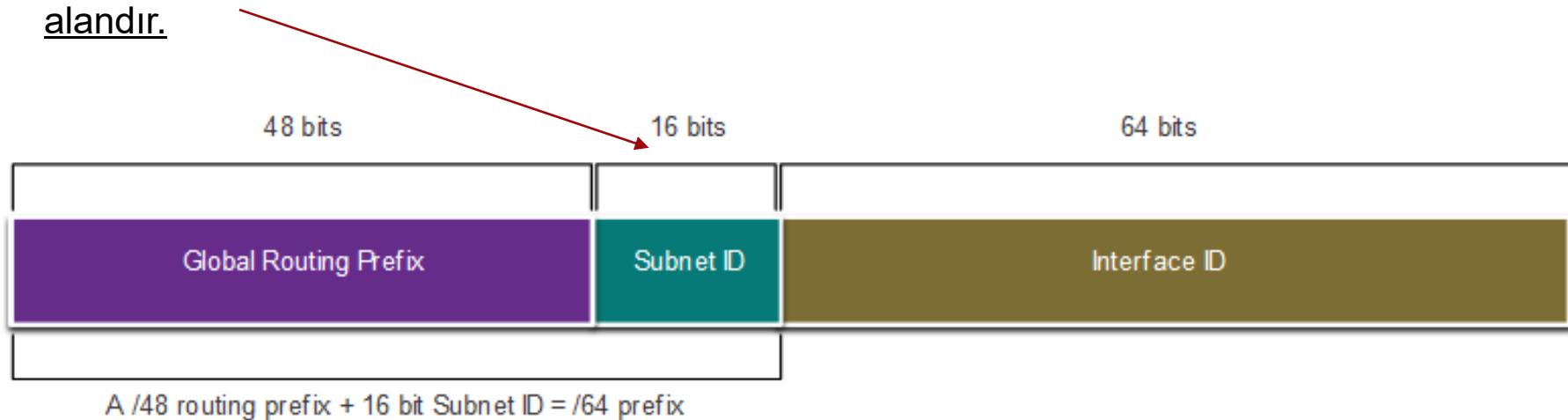
- Farklı IPv6 Adres Türlerini Belirleyin
- Bir Ana Bilgisayar IPv6 Ağ Arayüzü ve Adresini İnceleyin
- IPv6 Adres Kısaltmasını Uygulama

# 12.8 IPv6 Network Kullanarak Alt Ağa Bağlama

# Subnet Kullanarak Subnet ID Bağlama

IPv6, alt ağlar düşünülmüş olarak tasarlanmıştır.

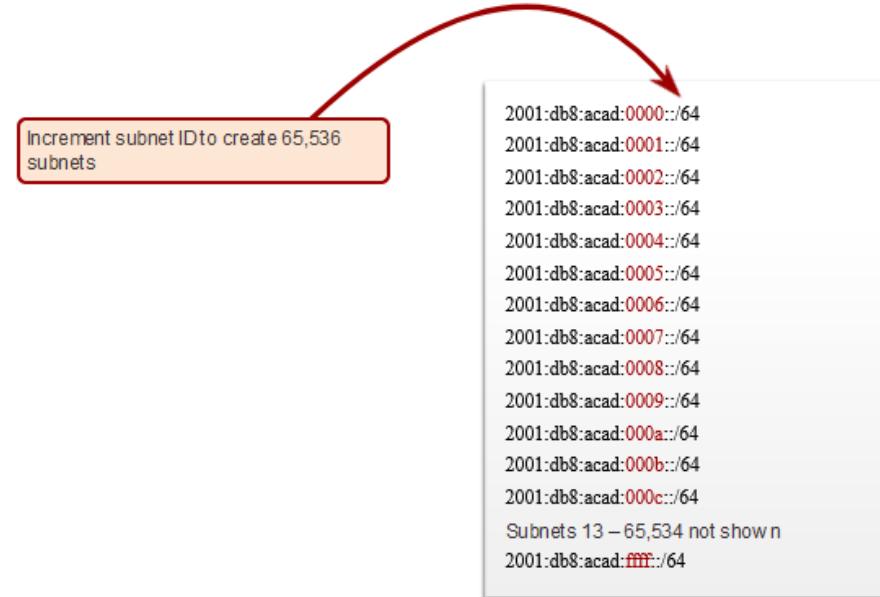
- IPv6 **GUA'daki ayrı bir alt ağ kimliği alanı**, alt ağlar oluşturmak için kullanılır.
- **Alt ağ kimliği alanı**, **Global Yönlendirme Öneki** ile arabirim kimliği arasındaki alandır.



# IPv6 Subnet Örnekleri

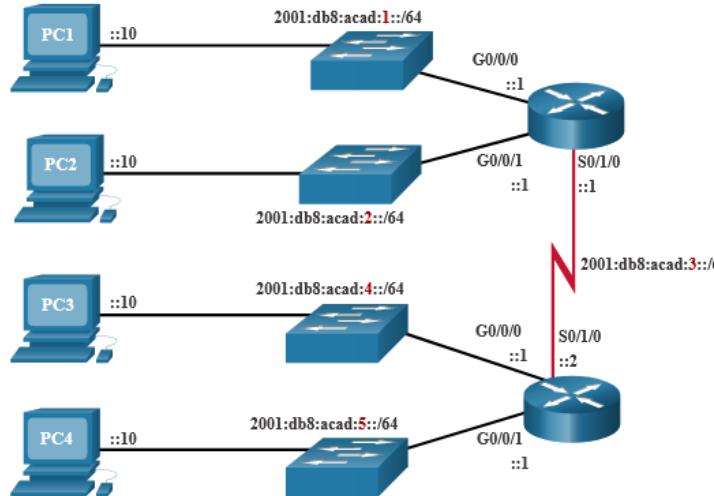
**2001: db8: acad :: / 48 genel yönlendirme öneki, 16 bitlik bir alt ağ kimliğiyle verildiğinde.**

- 65.536 / 64 alt ağa izin verir
- Global yönlendirme öneki tüm alt ağlar için aynıdır.



# Subnet an IPv6 Network IPv6 Subnet Tahsisi

- **Örnek topoloji, her LAN için bir tane ve ayrıca R1 ile R2 arasındaki seri bağlantı için olmak üzere beş alt ağ gerektirir.**
- **Beş IPv6 alt ağı, 0001'den 0005'e kadar olan alt ağ kimliği alanıyla tahsis edildi.**
- **Her / 64 alt ağ, gerekenden daha fazla adres sağlayacak.**



5 subnets allocated from 65,536 available subnets

Address Block
2001:db8:acad:0000::/64
2001:db8:acad:0001::/64
2001:db8:acad:0002::/64
2001:db8:acad:0003::/64
2001:db8:acad:0004::/64
2001:db8:acad:0005::/64
2001:db8:acad:0006::/64
2001:db8:acad:0007::/64
2001:db8:acad:0008::/64
2001:db8:acad:ffff::/64

# Router ile konfigüre edilmiş IPv6 Subnetler

Örnek, R1 üzerindeki yönlendirici arabirimlerinin her birinin farklı bir IPv6 subnetinde olacak şekilde yapılandırıldığını göstermektedir.

```
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
```

# 2.9 Modül Alıştırması ve Quiz

# Paket İzleyici–Subnetted IPv6 Adres Şemasının implementasyonu

- **Bu Paket İzleyicide aşağıdakileri yapacaksınız:**
- IPv6 alt ağlarını ve adresleme şemasını belirleyin
- Yönlendiriciler ve PC'lerde IPv6 adreslemesini yapılandırın
- IPv6 bağlantısını doğrulayın

# Lab – Ağ Aygıtlarında IPv6 Adreslerini Yapılandırma

**Bu laboratuvara aşağıdaki hedefleri tamamlarsınız:**

- Topolojiyi ayarlayın ve temel yönlendirici ve anahtar ayarlarını yapılandırın
- IPv6 adreslerini manuel olarak yapılandırın
- Uçtan uca bağlantıyı doğrulayın

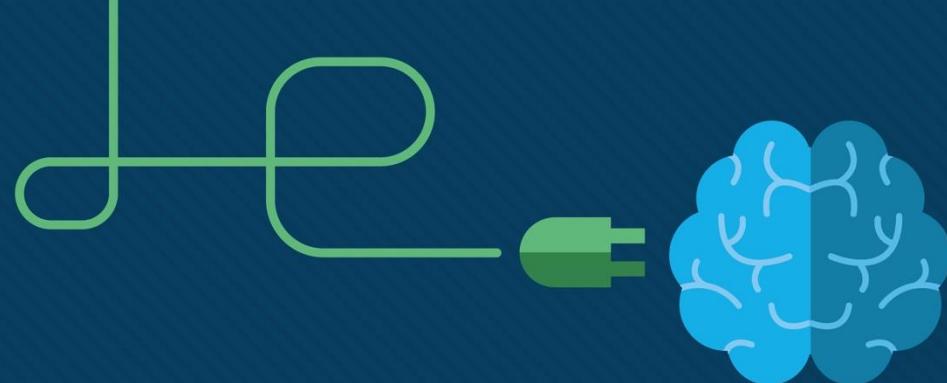
# Bu modülde ne öğrendim?

- IPv4 teorik olarak maksimum 4,3 milyar adrese sahiptir.
- IETF, ağ yöneticilerinin ağlarını IPv6'ya taşımalarına yardımcı olmak için çeşitli protokoller ve araçlar oluşturmuştur. Geçiş teknikleri üç kategoriye ayrılabilir: ikili yiğin, tünelleme ve çevirme.
- IPv6 adresleri 128 bit uzunluğundadır ve onaltılık değerler dizisi olarak yazılır.
- Bir IPv6 adresi yazmak için tercih edilen format x: x: x: x: x: x: x şeklindedir ve her "x" dört onaltılık değerden oluşur.
- Üç tür IPv6 adresi vardır: tek noktaya yayın, çok noktaya yayın ve her noktaya yayın.
- Bir IPv6 tek noktaya yayın adresi, IPv6 özellikli bir cihazdaki bir arabirimini benzersiz şekilde tanımlar.
- IPv6 global tek noktaya yayın adresleri (GUA'lar) küresel olarak benzersizdir ve IPv6 internet üzerinden yönlendirilebilir.
- Bir IPv6 bağlantı yerel adresi (LLA), bir aygıtın aynı bağlantı üzerindeki diğer IPv6 etkin aygıtlarla ve yalnızca bu bağlantı (alt ağ) üzerinden iletişim kurmasını sağlar.
- Bir arabirimde bir IPv6 GUA yapılandırma komutu **ipv6 adresi ipv6 adresi / önek uzunluğu**dur .
- Bir cihaz, bir GUA'yı ICMPv6 mesajları aracılığıyla dinamik olarak elde eder. IPv6 yönlendiricileri, ağdaki tüm IPv6 etkin aygıtlara her 200 saniyede bir ICMPv6 RA iletisileri gönderir.

## Bu modülde ne öğrendim? (Devam)

- RA mesajlarının üç yöntemi vardır: SLAAC, durum bilgisi olmayan DHCPv6 sunuculu SLAAC ve durum bilgisi olan DHCPv6 (SLAAC yok).
- Arayüz kimliği, EUI-64 işlemi veya rastgele oluşturulmuş 64 bitlik bir sayı kullanılarak oluşturulabilir.
- EUIs işlemi, istemcinin 48-bit Ethernet MAC adresini kullanır ve 64-bit arayüz kimliği oluşturmak için MAC adresinin ortasına 16 bit daha ekler.
- İşletim sistemine bağlı olarak, bir cihaz rastgele oluşturulmuş bir arayüz kimliği kullanabilir.
- Tüm IPv6 cihazlarının bir IPv6 LLA'sı olmalıdır. Bir LLA manuel olarak yapılandırılabilir veya dinamik olarak oluşturulabilir.
- Cisco yönlendiricileri, arayüze bir GUA atandığında otomatik olarak bir IPv6 LLA oluşturur.
- İki tür IPv6 çok noktaya yayın adresi vardır: iyi bilinen çok noktaya yayın adresleri ve istenen düğüm çok noktaya yayın adresleri.
- İki ortak IPv6 atanmış çok noktaya yayın grubu şunlardır: ff02 :: 1 Tüm düğümler çok noktaya yayın grubu ve ff02 :: 2 Tüm yönlendiriciler çok noktaya yayın grubu.
- İstenen düğümlü çok noktaya yayın adresi, tüm düğümler çok noktaya yayın adresine benzer. İstenen düğümlü çok noktaya yayın adresinin avantajı, özel bir Ethernet çok noktaya yayın adresine eşlenmesidir.
- IPv6, alt ağlar düşünülerek tasarlanmıştır. IPv6 GUA'daki ayrı bir alt ağ kimliği alanı, alt ağlar oluşturmak için kullanılır.





# Modül 13: ICMP

Ağlara Giriş v7.0 (ITN)



# Modül Hedefleri

## Modül Başlığı: ICMP

- Module Amacı: Ağ bağlantısını test etmek için çeşitli araçların kullanımı

Topic Title	Topic Objective
ICMP Mesajları	Ağ bağlantısını test etmek için ICMP'nin nasıl kullanıldığın açıklanması
Ping ve Traceroute Testleri	Ağ bağlantısını test etmek için <b>ping</b> ve <b>traceroute</b> yardımcı programlarının kullanımı

# 13.1 ICMP Mesajları

## ICMPv4 ve ICMPv6 Mesajları

- ❑ **Internet Kontrol Mesajı Protokolü (ICMP)**, belirli koşullar altında 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 olan ICMP mesajları şunları içerir:
  - Ana bilgisayar erişilebilirliği
  - **Hedef** veya **Hizmet Ulaşılamıyor**
  - Zaman aşımı yapıldı

**Not:** ICMPv4 mesajları gerekli değildir ve güvenlik nedenleriyle genellikle bir ağ içinde izin verilmez.



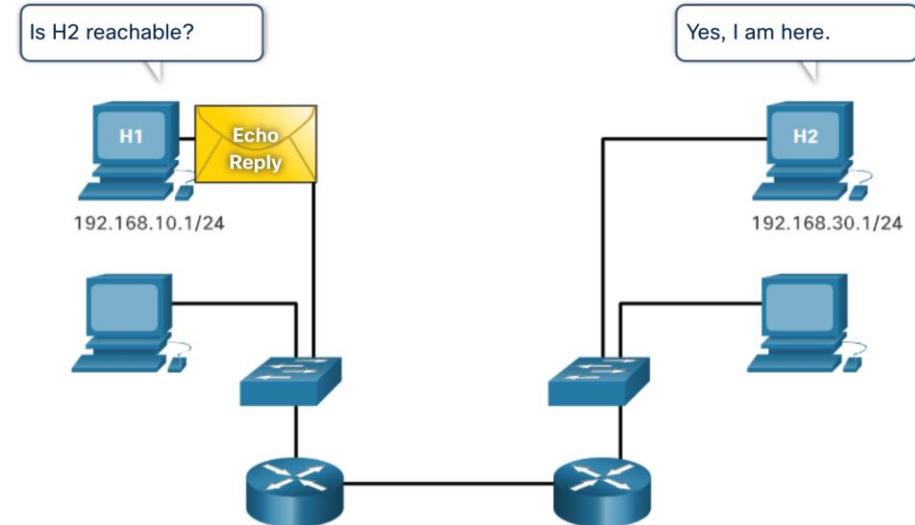
## ICMP Mesajları

# Ana Bilgisayar Erişilebilirliği

- ❑ **ICMP Yankı Mesajı**, bir IP ağındaki bir ana bilgisayarın erişilebilirliğini test etmek için kullanılabilir.

Örnek:

- Yerel ana bilgisayar, bir ana bilgisayara bir ICMP Yankı İsteği gönderir.
- Ana bilgisayar uygunsa, hedef ana bilgisayar bir Yankı Yanıtı ile yanıt verir.



# Hedef veya Servise Ulaşılamıyor

- Bir hedef veya hizmetin ulaşılamaz olduğunu kaynağına bildirmek için **bir ICMP Hedefe Ulaşılamıyor mesajı kullanılabilir.**
- ICMP mesajı, paketin neden teslim edilemediğini belirten bir kod içerecektir.
- **ICMPv4 için birkaç Hedef Ulaşılamaz kod aşağıdaki gibidir:**
  - 0 - Erişilemeyen ağ
  - 1 - Ana bilgisayara erişilemiyor
  - 2 - Protokole ulaşılamıyor
  - 3 - Bağlantı noktasına ulaşılamıyor
- **ICMPv6 için birkaç Hedef Ulaşılamaz kod aşağıdaki gibidir:**
  - 0 - Hedefe rota yok
  - 1 - Hedef ile iletişim yönetimsel olarak yasaklanmıştır (örneğin, güvenlik duvarı)
  - 2 - Kaynak adresin kapsamının ötesinde
  - 3 - Ulaşılamayan adres
  - 4 - Bağlantı noktasına ulaşılamıyor



Not: ICMPv6, Hedef Ulaşılamaz mesajlar için benzer ancak biraz farklı kodlara sahiptir.

# Mesaj Süresi Aşıldı

- Bir paketteki Yaşam Süresi (TTL) alanı 0'a düşürüldüğünde, kaynak ana bilgisayara bir ICMPv4 Süresi Aşıldı mesajı gönderilecektir.
- ICMPv6 ayrıca bir Süre Aşıldı mesajı gönderir.
- IPv4 TTL alanı yerine ICMPv6, paketin süresinin dolup dolmadığını belirlemek için IPv6 Atlama Sınırı 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 mesajlar tarafından kullanılan traceroute aracı.

## ICMPv6 Mesajları

- ICMPv6, Komşu Bulma Protokolünün (ND veya NDP) bir parçası olarak **dört yeni protokol dahil** olmak üzere, ICMPv4'te bulunmayan yeni özelliklere ve gelişmiş işlevsellige sahiptir.

- **Dinamik adres atama dahil** olmak üzere bir IPv6 yönlendiricisi ile IPv6 cihazı arasındaki mesajlaşma aşağıdaki gibidir:

- Yönلendirici Talep (RS) mesajı
- Yönlendirici Tanıtımı (RA) mesajı

- **Yinelenen adres algılama** ve **adres çözümleme** dahil olmak üzere IPv6 cihazları arasında mesajlaşma aşağıdaki gibidir:

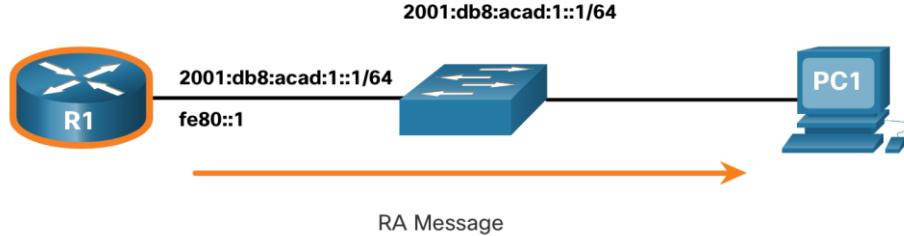
- Komşu Talep (NS) mesajı
- Komşu İlanı (NA) mesajı



Not : ICMPv6 ND, ICMPv4'te kullanılan yeniden yönlendirme mesajına benzer bir işlev sahip olan yeniden yönlendirme mesajını da içerir.

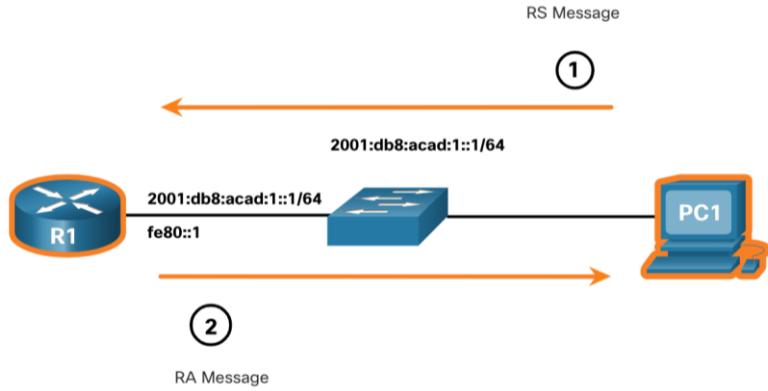
## ICMPv6 Mesajları (Devam)

- RA mesajları, IPv6 özellikli ana bilgisayarlara adres bilgileri sağlamak için IPv6 etkin yönlendiriciler tarafından her 200 saniyede gönderilir.
- RA mesajı, önek, önek uzunluğu, **DNS adresi ve alan adı** gibi ana bilgisayar için adresleme bilgilerini içerebilir.
- Durum Bilgisiz Adres Otomatik Yapılandırması (**SLAAC**) kullanan bir ana bilgisayar, varsayılan ağ geçidini RA'yı gönderen yönlendiricinin yerel bağlantı adresine ayarlayacaktır.



# ICMPv6 Mesajları (Devam)

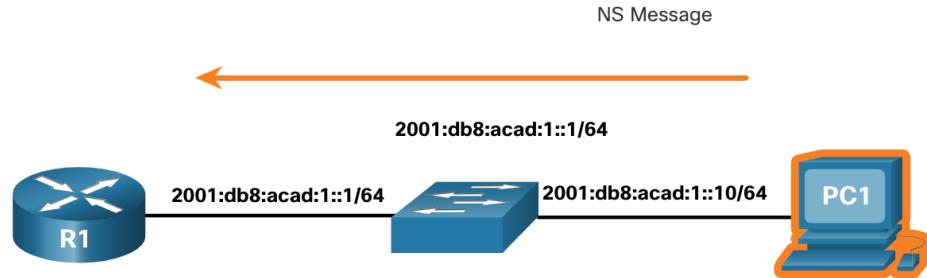
- ❑ IPv6 özellikle bir yönlendirici ayrıca bir RS mesajına yanıt olarak bir RA mesajı gönderir.
- ❑ Şekilde, PC1, IPv6 adres bilgisinin dinamik olarak nasıl alınacağını belirlemek için bir RS mesajı gönderir.



- R1, RS'ye RA mesajıyla yanıt verir.
- PC1 bir RS mesajı gönderir, "Merhaba, yeni başlattım."
- Ağda bir IPv6 yönlendirici var mı?
- IPv6 adres bilgilerimi dinamik olarak nasıl alacağımı bilmem gerekiyor."
- R1 bir RA mesajı ile yanıt verir.
- "Merhaba tüm IPv6 etkin cihazlar."
- Ben R1 ve bir IPv6 global tek noktaya yayın adresi oluşturmak için SLAAC kullanabilirsiniz.
- Ön ek `2001: db8: acad: 1 :: / 64` şeklindedir.
- Bu arada, bağlantı-yerel adresim `fe80 :: 1'i` varsayılan ağ geçidiniz olarak kullanın."

## ICMPv6 Mesajları (Devam)

- Global IPv6 tek noktaya yayın veya bağlantı yerel tek noktaya yayın adresi atanmış bir cihaz, IPv6 adresinin benzersiz olmasını sağlamak için yinelenen adres algılaması (DAD) gerçekleştirebilir.
- Bir adresin benzersizliğini kontrol etmek için cihaz, hedeflenen IPv6 adresi olarak kendi IPv6 adresini içeren bir **NS mesajı** gönderecektir.
- **Ağdaki başka bir cihaz bu adrese sahipse**, gönderen cihaza adresin kullanımında olduğunu bildiren **bir NA mesajı ile yanıt verecektir.**

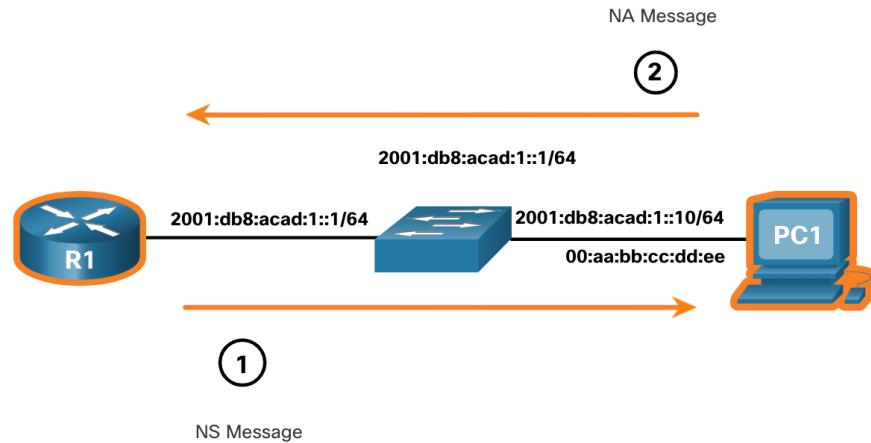


**Not :** DAD gerekli değildir, ancak RFC 4861, DAD'nın tek noktaya yayın adreslerinde gerçekleştirilmesini önerir.

## ICMP Mesajları

# ICMPv6 Mesajları (Devam)

- ❑ **Hedefin MAC adresini belirlemek** için, cihaz istenen **düğüm adresine** bir **NS mesajı gönderecektir.**
- ❑ Mesaj, bilinen (hedeflenen) IPv6 adresini içerecektir.
- ❑ Hedeflenen IPv6 adresine sahip cihaz, Ethernet MAC adresini içeren **bir NA mesajı ile yanıt verecektir.**
- ❑ Şekilde, R1 2001: db8: acad: 1 :: 10'a **MAC adresini soran** bir **NS mesajı** gönderir.



# 13.2 Ping ve Traceroute Testleri

# Ping – Test Bağlantısı

- ❑ Ping komutu ICMP yanıt isteği kullanır ve yanıt yanıt mesajlarını bağlantıyı sınamak için konaklar arasında ve hedefe başarı oranını ve ortalama geri dönüş süresini içeren bir özetini sağlar IPv4 ve IPv6 test aracıdır.
- ❑ Zaman aşımı süresi içinde bir yanıt alınmazsa, ping bir yanıtın alınmadığını belirten bir mesaj sağlar.
- ❑ ICMP Yanıtı isteği gönderilmeden önce adres çözümlemesinin (ARP veya ND) yapılması gerekiyorsa, ilk ping'in 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
```

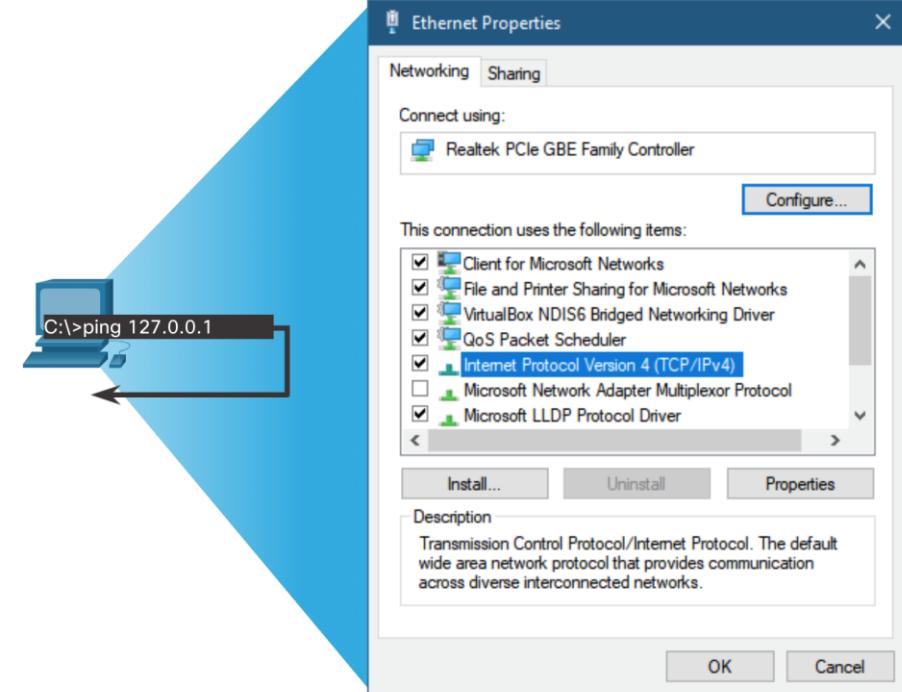
Type escape sequence to abort.

```
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

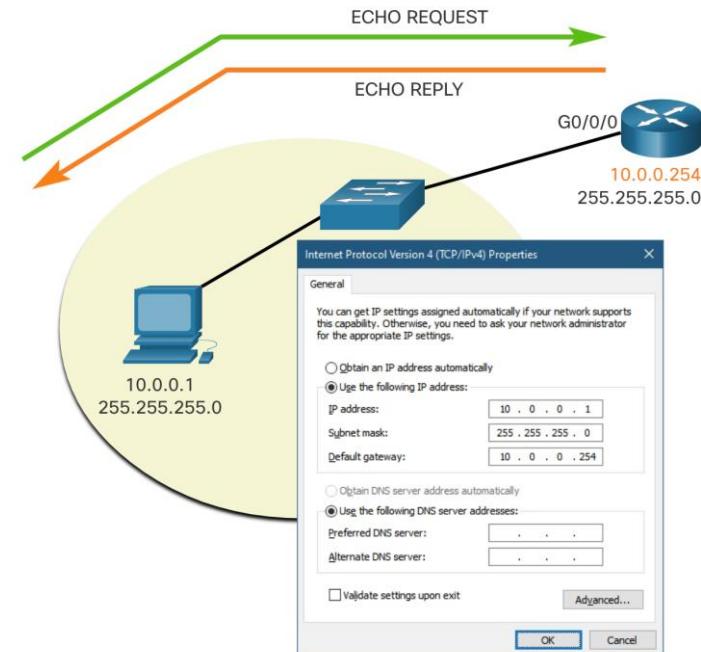
# Ping the Loopback

- Ping, yerel ana bilgisayarda IPv4 veya IPv6'nın dahili yapılandırmasını test etmek için kullanılabilir.
- Bunu yapmak için IPv4 için 127.0.0.1 (IPv6 için ::1) yerel geri döngü adresine ping atın.
- IPv4 için 127.0.0.1'den veya IPv6 için ::1'den gelen bir yanıt, IP'nin ana bilgisayara düzgün şekilde yüklediğini gösterir.
- Bir hata mesajı, TCP/IP'nin ana bilgisayarda çalışmadığını gösterir.



# Varsayılan Ağ Geçidine Ping Gönderme

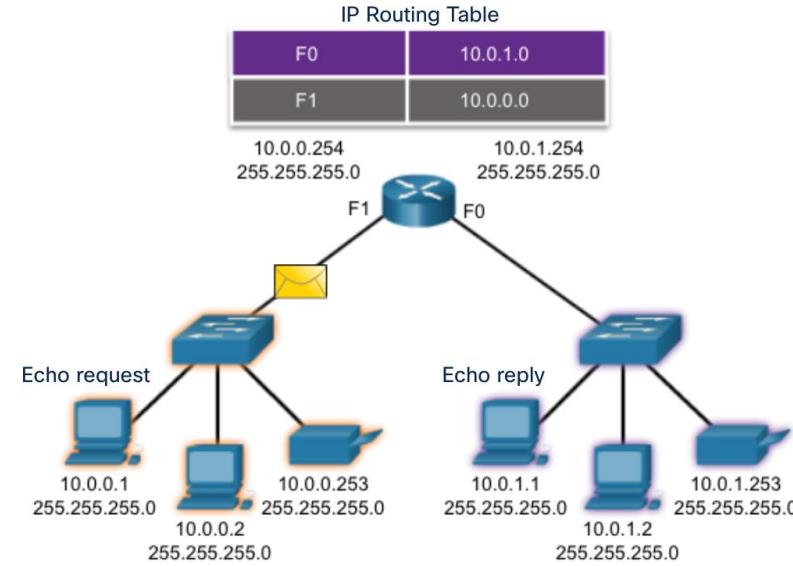
- ❑ **Ping** komutu yerel ağa iletişim kurmak için bir konağın kabiliyetini test etmek için kullanılabilir.
- ❑ **Varsayılan ağ geçidi adresi en sık kullanılır** çünkü yönlendirici normalde **her zaman çalışır** durumda.
  - **Varsayılan ağ geçidine başarılı bir ping işlemi**, ana bilgisayar ve **varsayılan ağ geçidi** olarak hizmet veren yönlendirici arayüzünün yerel ağa çalıştığını gösterir.
  - **Varsayılan ağ geçidi adresi yanıt vermezse**, yerel ağa çalıştığı bilinen başka bir ana bilgisayarın **IP adresine** bir ping gönderilebilir.



# Uzak Ana Bilgisayara Ping Gönderme

- **Ping** aynı zamanda yerel bir ana bilgisayarın bir ağlar arası iletişim kurma yeteneğini test etmek için de kullanılabilir.
- **Yerel bir ana bilgisayar**, uzak bir ağdaki bir ana bilgisayara ping atabilir.
- Internet ağında başarılı bir **ping** , **yerel ağdaki iletişimini doğrular**.

**Not:** Birçok ağ yönetici ICMP mesajlarının girişini sınırlar veya yasaklar, bu nedenle ping yanıtının olmaması güvenlik kısıtlamalarından kaynaklanıyor olabilir.



# Traceroute – Yolu Test Edin

- **Traceroute** ( **tracert** ), iki ana bilgisayar arasındaki yol test etmek ve bu yol boyunca başarıyla ulaşılan atlamaların bir listesini sağlamak için kullanılan bir yardımcı programdır.
- **Traceroute**, yol boyunca her atlama için gidiş-dönüş süresi sağlar ve bir sekmenin yanıt veremeyeceğini belirtir.
- **Kayıp veya yanıtlanmamış bir paketi** belirtmek için **yıldız işaretü (\*)** kullanılır.
- **Bu bilgi, yoldaki sorunlu bir yönlendiriciyi bulmak için kullanılabilir veya yönlendiricinin yanıt vermeyecek şekilde yapılandırıldığını gösterebilir.**

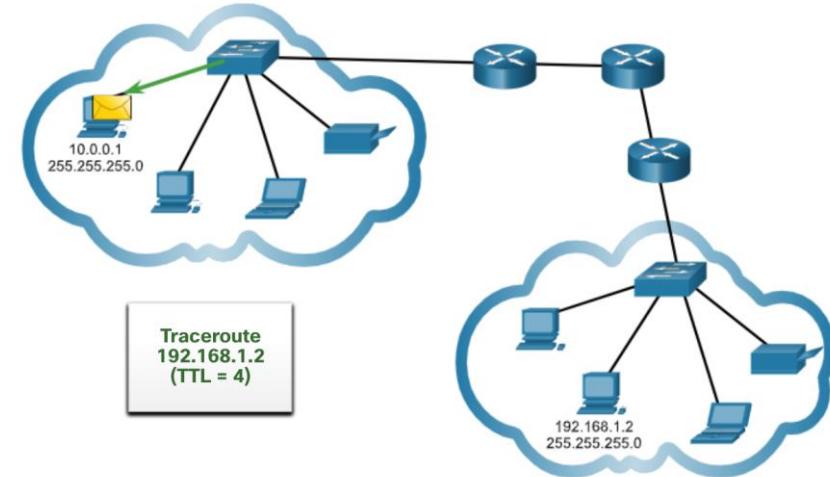
```
R1#traceroute 192.168.40.2  
Type escape sequence to abort.  
Tracing the route to 192.168.40.2
```

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:** İzleme Yolu, ICMP Süresi Aşıldı mesajıyla birlikte IPv4'teki TTL alanının ve IPv6'daki Atlama Sınırı alanının Katman 3 üstbilgilerindeki bir işlevini kullanır.

## Traceroute – Yolu Test Edin ( Devam )

- **Traceroute**'den gönderilen ilk mesajın TTL alan değeri 1 olacaktır.
- Bu, TTL'nin ilk yönlendiricide zaman aşımına uğramasına neden olur.
- **Bu yönlendirici** daha sonra bir ICMPv4 Süresi Aşıldı mesajıyla yanıt verir.
- **Traceroute** daha sonra her ileti dizisi için TTL alanını (2, 3, 4 ...) aşamalı olarak artırır.
- Bu, paketler yolun ilerleyen kısımlarında zaman aşımına uğradığında bize her bir sekmenin adresini sağlar.
- **TTL alanı**, hedefe ulaşılana kadar artırılmaya devam eder veya önceden tanımlanmış bir maksimuma yükseltilir.



# Paket Tracer – IPv4 ve IPv6 Adreslerini Doğrulayın

Bu Paket İzleyicide aşağıdakileri yapacaksınız:

- Adresleme Tablosu Dokümantasyonunu Doldurun
- Ping Kullanarak Bağlantıyı Test Edin
- Rotayı İzleyerek Yolu Keşfedin

# Paket Tracer – Ağ Bağlantısını Test Etmek için Ping ve Traceroute Kullanımı

Bu Paket İzleyicide aşağıdakileri yapacaksınız:

- IPv4 Bağlantısını Test Edin ve Geri Yükleyin
- IPv6 Bağlantısını Test Edin ve Geri Yükleyin

# 13.3 Modül Alıştırmaları ve Sınavı

# Paket Tracer – Ağ Bağlantısını Test Etmek ve Düzeltmek için ICMP Kullanın

Bu Paket İzleyicide aşağıdakileri yapacaksınız:

- Bağlantı sorunlarını bulmak için ICMP kullanın.
- Ağ cihazlarını bağlantı sorunlarını düzeltcecek şekilde yapılandırın.

# Lab – Ağ Bağlantısını Test Etmek İçin Ping ve İzleme Yolunun Kullanımı

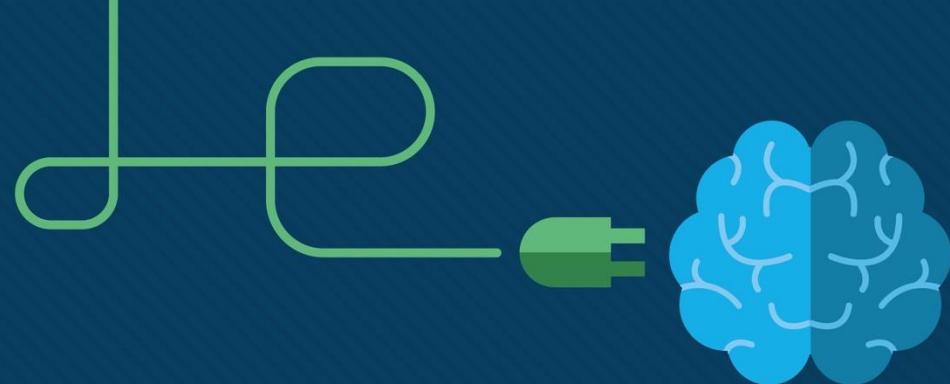
Bu laboratuvara aşağıdaki hedefleri tamamlarsınız:

- Ağı Oluşturun ve Yapılandırın
- Temel Ağ Testi için Ping Komutunu Kullanın
- Temel Ağ Testi için Tracert ve Traceroute Komutlarını Kullanın
- Topoloji sorunlarını giderin

## Bu modülde ne öğrendim?

- ICMP mesajlarının amacı, belirli koşullar altında IP paketlerinin işlenmesiyle ilgili sorunlar hakkında geri bildirim sağlamaktır.
- Hem ICMPv4 hem de ICMPv6 için ortak olan ICMP mesajları şunlardır: Ana bilgisayara erişilebilirlik, Hedef veya Hizmet Erişilemez ve Süre aşındırı.
- Dinamik adres tahsisi dahil olmak üzere bir IPv6 yönlendiricisi ile bir IPv6 cihazı arasındaki mesajlar RS ve RA'yı içerir. IPv6 cihazları arasındaki mesajlar, yeniden yönlendirme (IPv4'e benzer), NS ve NA'yı içerir.
- Ping (IPv4 ve IPv6 tarafından kullanılır), ana bilgisayarlar arasındaki bağlantıyı test etmek için ICMP yankı isteği ve yankı yanıt mesajlarını kullanır
- Ping, yerel ana bilgisayarda IPv4 veya IPv6'nın dahili yapılandırmasını test etmek için kullanılabilir.





# Modül 14: Taşınma Katmanı

Eğitmen Materyalleri

Ağlara Girişi v7.0 (ITN)



# Modül Hedefleri

## Modül Başlığı: Taşınma Katmanı

**Modülün Amacı:** Uçtan uca iletişim desteklemeye taşıma katmanı protokollerinin işlemlerini karşılaştırma

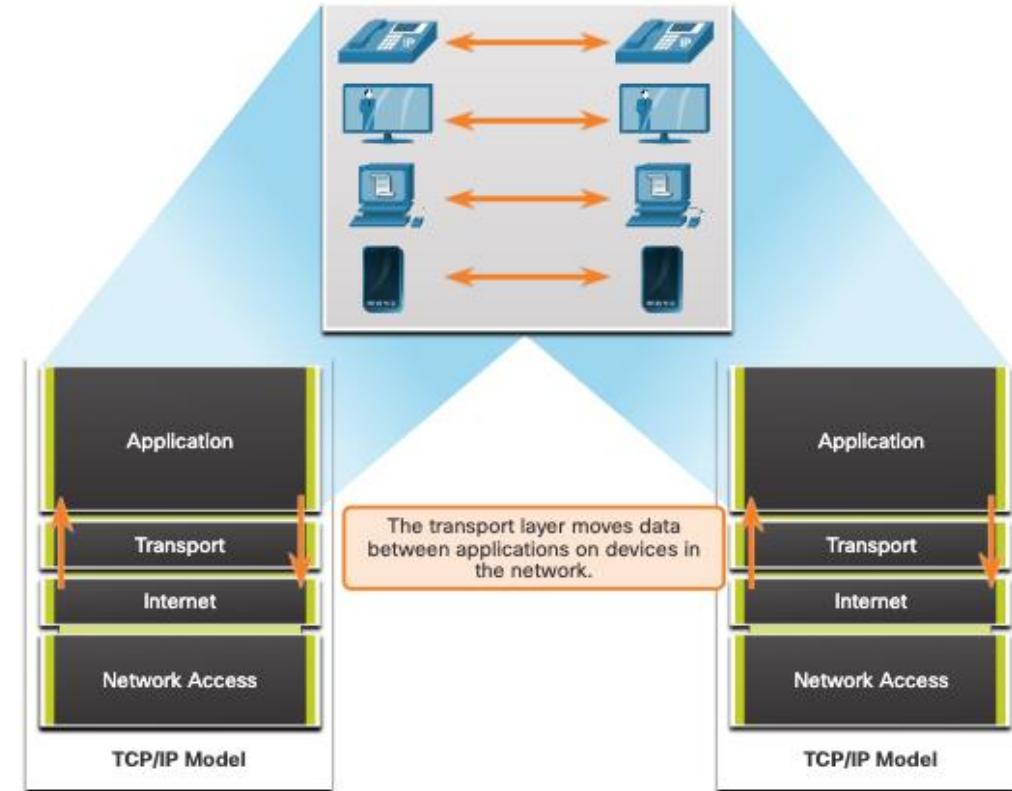
Konu Başlığı	Amaç
Verinin Taşınması	Uçtan uca iletişimde veri aktarımını yönetmede taşıma katmanın amacının açıklanması
TCP 'ye Genel Bakış	TCP özelliklerinin açıklanması
UDP 'ye Genel Bakış	UDP özelliklerinin açıklanması
Port Numaları	TCP ve UDP'nin bağlantı noktası numaralarını nasıl kullandığını açıklanması.
TCP İletişim Süreçleri	TCP oturumu kurma ve sonlandırma süreçlerinin güvenilir iletişimini nasıl kolaylaştırdığını açıklanması
Güvenilirlik ve Akış Kontrolü	CP protokolü veri birimlerinin nasıl iletildiğini ve teslimatı garanti etmek için kabul edildiğini açıklanması
UDP İletişimi	Uçtan uca iletişim desteklemek için taşıma katmanı protokollerinin işlemlerini karşılaştırılması

# 14.1 Verilerin Taşınması

# Taşınma Katmanının Rolü

## Taşıma katmanı:

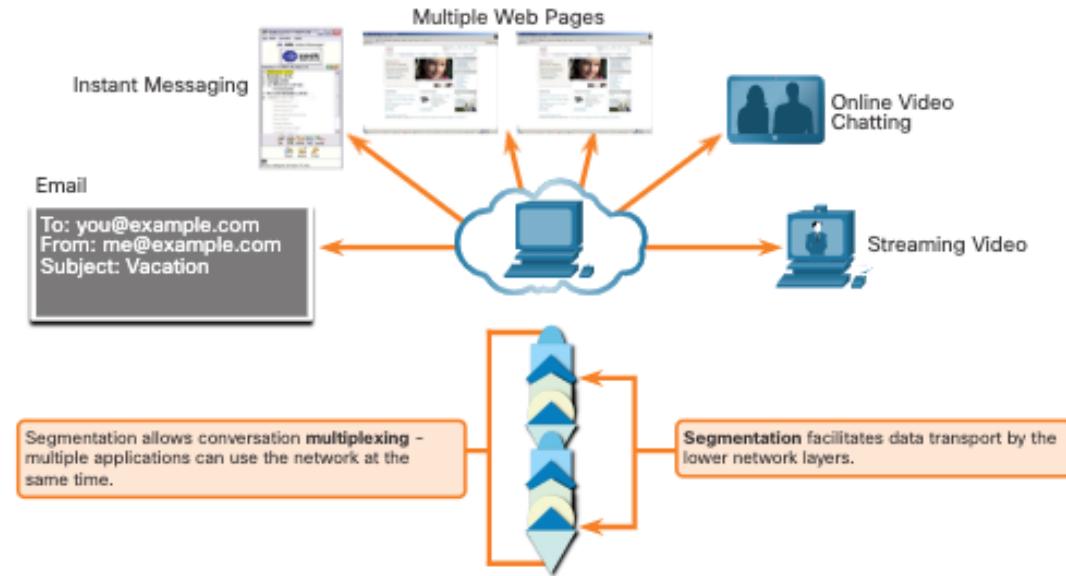
- Farklı ana bilgisayarlarda çalışan uygulamalar arasındaki mantıksal iletişimden sorumludur.
- Uygulama katmanı ile ağ iletişiminden sorumlu alt katmanlar arasındaki bağlantıdır.



# Taşıma Katmanının Sorumlulukları

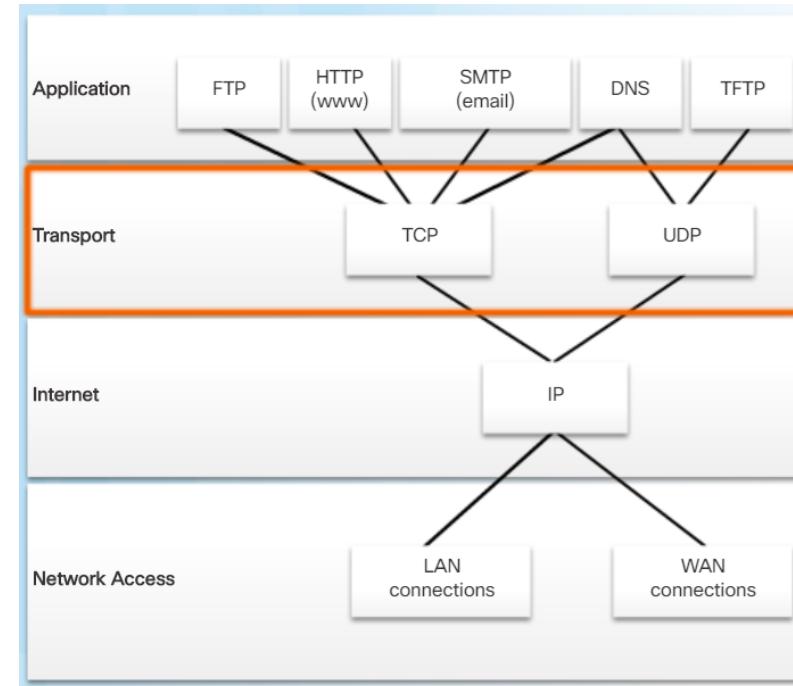
Taşınma katmanın sorumlulukları aşağıdaki gibidir :

- **Bireysel görüşmeleri izleme**
- **Verileri segmentlere ayırma ve segmentleri yeniden birleştirme**
- **Başlık bilgilerini ekleme**
- **Birden çok konuşmayı tanımlama, ayırma ve yönetme**
- **Farklı iletişim görüşmelerinin aynı ağ üzerinde araya eklenmesini sağlamak için bölümleme ve çoklama kullanır.**



# Taşınma Katmanı Protokolleri

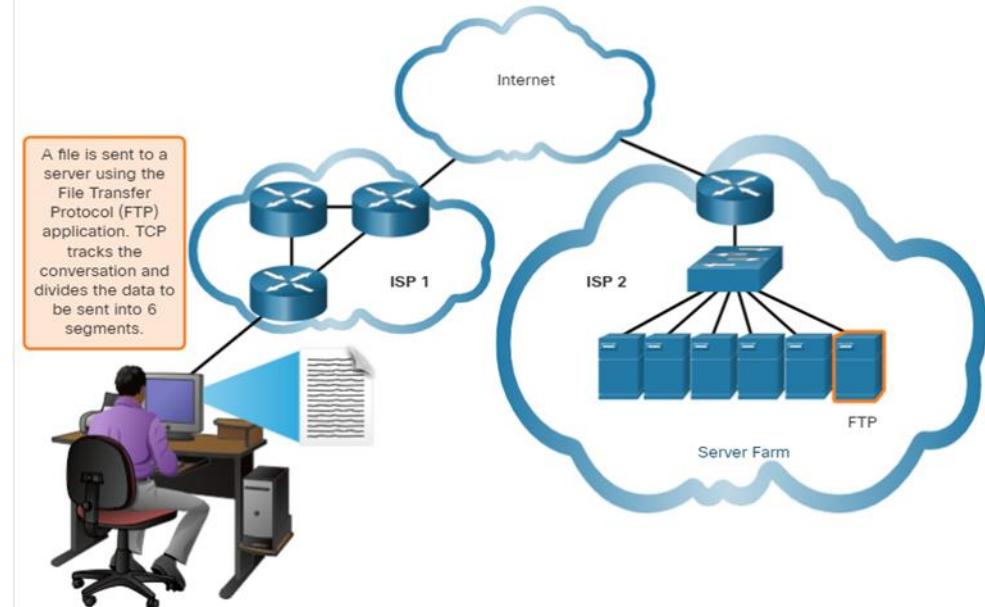
- IP, paketlerin **teslimatının veya nakliyesinin nasıl gerçekleştiğini belirtmez.**
- **Taşıma katmanı protokolleri**, mesajların ana bilgisayarlar arasında nasıl aktarılacağını belirler ve bir görüşmenin güvenilirlik gereksinimlerini yönetmekten sorumludur.
- **Taşıma katmanı**, TCP ve UDP protokollerini içerir.



# Veri İletim Kontrol Protokolü

TCP, güvenilirlik ve akış denetimi sağlar. TCP temel işlemleri:

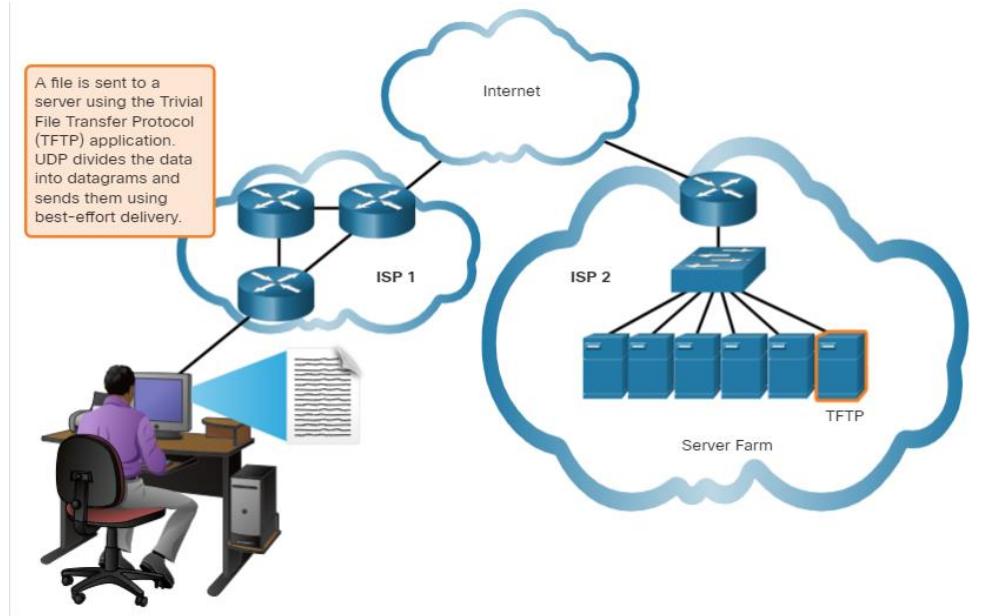
- Belirli bir uygulamadan belirli bir ana bilgisayara iletilen veri segmentlerini **numaralar** ve **takip eder**
- **Alınan verileri onaylar**
- **Onaylanmamış** verileri belirli bir süre sonra **yeniden iletir**
- Yanlış sırada ulaşabilecek verileri sıralar
- **Verileri, alıcı tarafından kabul edilebilir verimli bir hızda gönderir.**



# User Datagram Protocol (UDP)

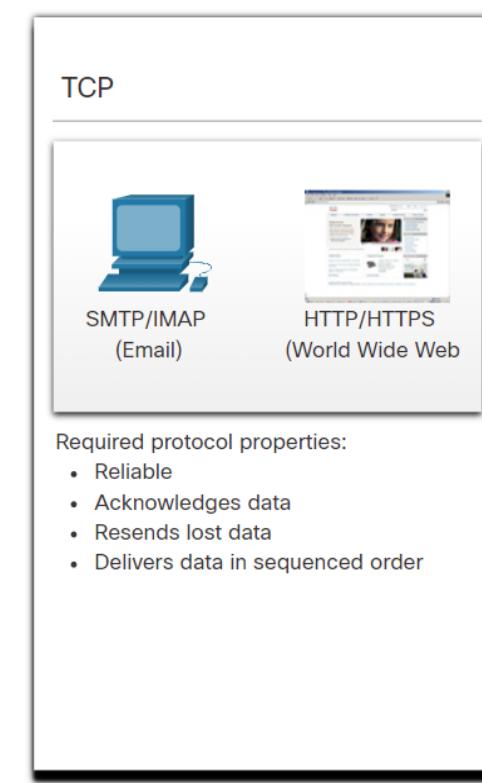
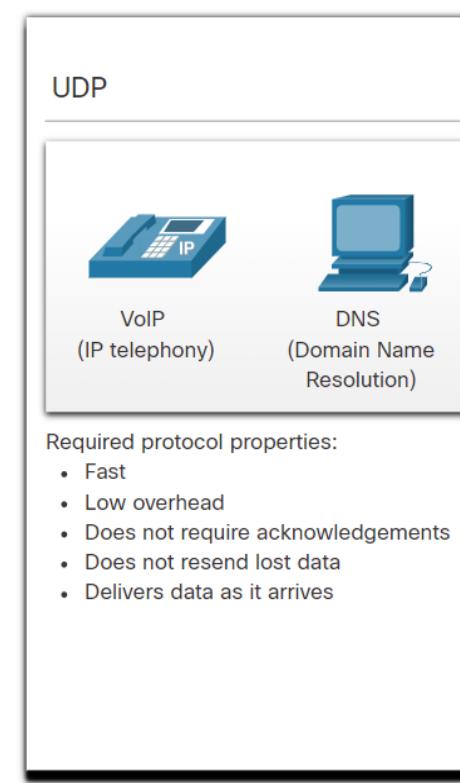
UDP, çok az ek yük ve veri denetimi ile uygun uygulamalar arasında veri birimi dağıtımını için temel işlevleri sağlar.

- **UDP**, bağlantısız bir protokoldür.
- **UDP**, verinin hedefte alındığına dair herhangi bir **onay olmadığından**, en iyi uygulama protokolü olarak bilinir.



# Doğru Uygulama için Doğru Taşınma Protokolü

- **UDP**, verilerin minimum düzeyde olduğu ve yeniden iletimin hızlı bir şekilde yapılabildiği istek ve yanıt uygulamaları tarafından da kullanılır.
- Tüm verilerin gelmesi ve uygun sırada işlenebilmesi önemliyse, taşıma protokolü olarak **TCP** kullanılır.



# 14.2 TCP 'ye Genel Bakış

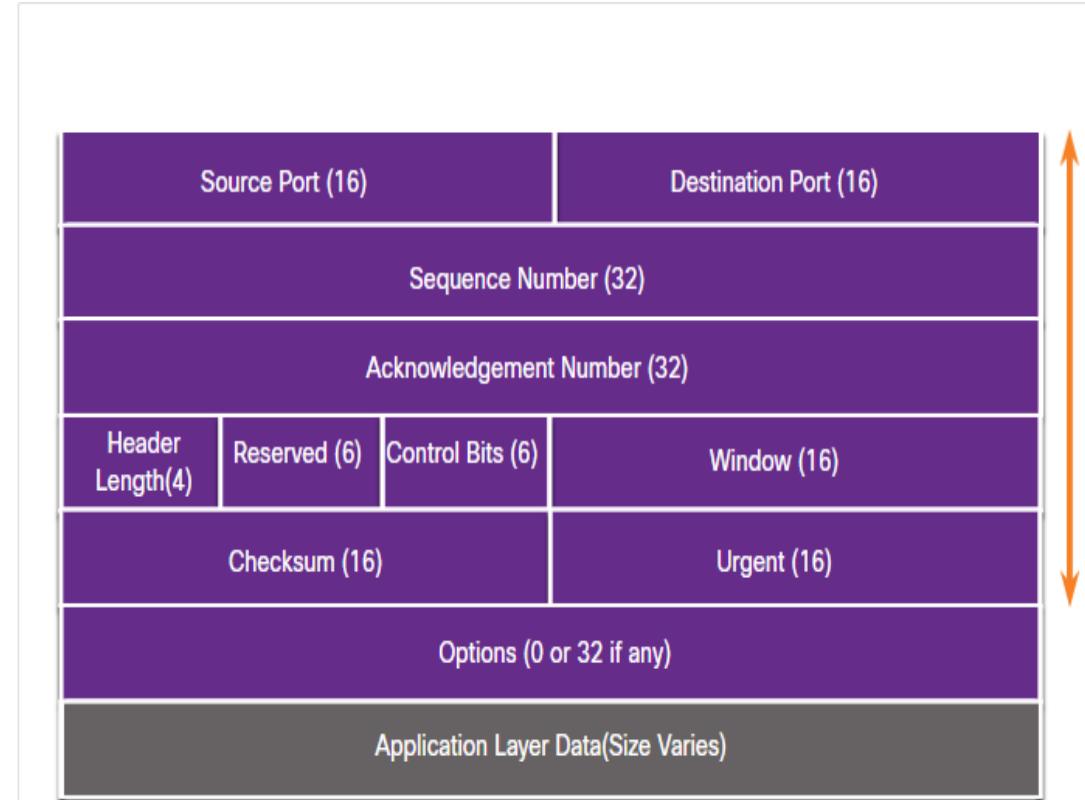
## TCP Özellikleri

- **Bir Oturum Kurar** - TCP, herhangi bir trafiği iletmenden önce **kaynak** ve **hedef cihazlar** arasında kalıcı bir bağlantı (veya oturum) müzakere eden ve kurulan **bağlantı odaklı bir protokoldür**.
- **Güvenilir Teslimat Sağlar** - Birçok nedenden dolayı, bir segmentin ağ üzerinden iletiliği için **bozulması** veya **tamamen kaybolması** mümkün değildir. TCP, kaynak tarafından gönderilen her kesimin **hedefe ulaşmasını sağlar**.
- **Aynı Sırayla Teslimat Sağlar** - Ağlar farklı aktarım hızlarına sahip olabilen **birden fazla yol sağlayabileceğinden**, veriler yanlış sırada gelebilir.
- **Akış Kontrolünü Destekler** - Ağ ana bilgisayarlarının **sınırlı kaynakları vardır** (yani, bellek ve işlem gücü). **TCP**, bu kaynakların **aşırı yüklediğinin farkında olduğunda**, gönderen uygulamanın **veri akış hızını düşürmesini isteyebilir**.

# TCP Genel Bakış

## TCP Başlığı

- **TCP, durum bilgisi olan bir protokoldür**, yani iletişim oturumunun durumunu takip eder.
- **TCP, hangi bilgileri gönderdiğini ve hangi bilgilerin onaylandığını kaydeder.**

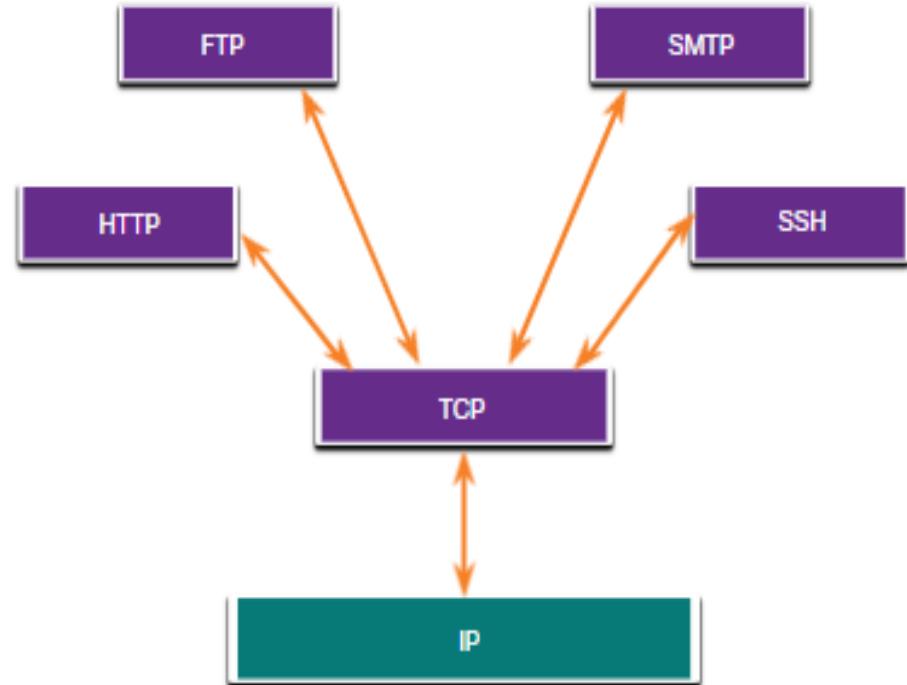


# TCP Başlık Alanları

TCP Başlık Alanları	Açıklama
Kaynak Port	Kaynak uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bitlik bir alanıdır.
Hedef Port	Hedef uygulamayı <b>bağlantı noktası numarasına</b> göre tanımlamak için kullanılan <b>16 bitlik bir alan</b> .
Sıra Numarası	Verileri yeniden birleştirme amacıyla kullanılan 32 bitlik bir alan.
Onay Numarası	Verinin alındığını ve bir sonraki baytin kaynaktan beklendiğini belirtmek için kullanılan 32 bitlik bir alan
Başlık Uzunluğu	TCP bölüm başlığının uzunlığını belirten ve "veri uzaklığı" olarak bilinen 4 bitlik bir alan
Rezerve Alan	<b>Gelecekte kullanılmak üzere ayrılmış 6 bitlik bir alan</b>
Kontrol Bitleri	<b>TCP</b> segmentinin amacını ve işlevini gösteren bit kodlarını veya bayrakları içeren 6 bitlik bir alan
Pencere Boyutu	<b>Bir seferde kabul edilebilecek bayt sayısını belirtmek</b> için kullanılan 16 bitlik bir alan
Sağlama	Segment <b>başlığının ve verilerinin hata kontrolü</b> için kullanılan 16 bitlik bir alan
Acil	İçerilen verilerin <b>acil olup olmadığını belirtmek</b> için kullanılan 16 bitlik bir alan

# TCP Kullanan Uygulamalar

- **TCP**, veri akışını **segmentlere bölmek**, **güvenilirlik sağlamak**, veri akışını **kontrol etmek** ve **segmentleri yeniden düzenlemekle** ilgili tüm görevleri yerine getirir.



# 14.3 UDP ‘ye Genel Bakış

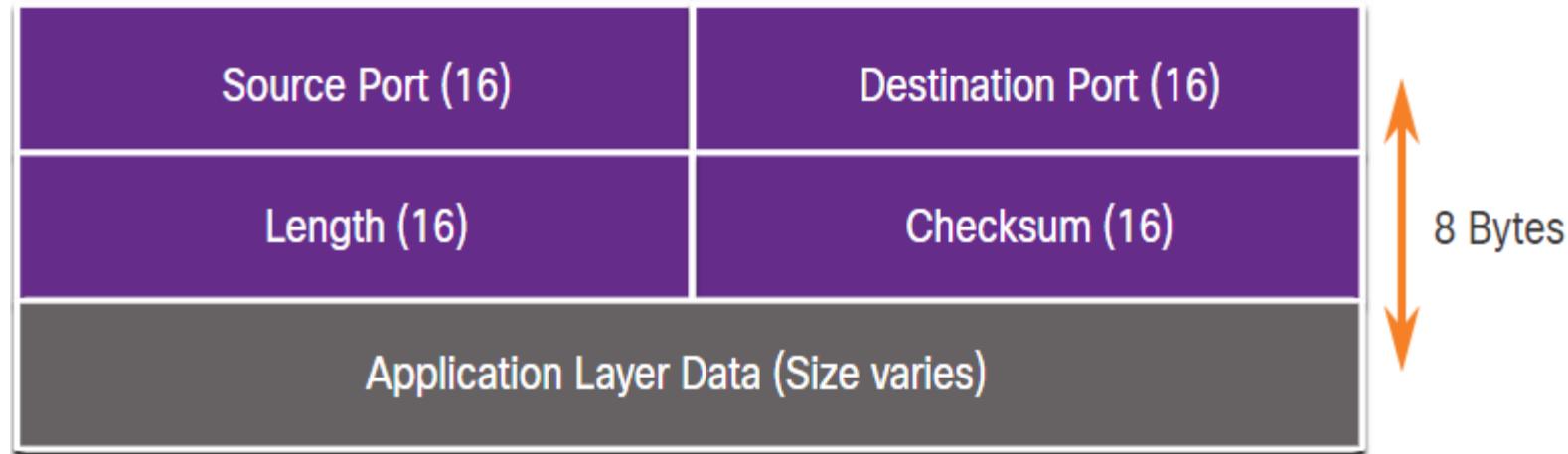
# UDP Özellikleri

UDP özellikleri şunları içerir:

- Veriler, alındıkları sırayla yeniden oluşturulur.
- Kaybolan herhangi bir segment yeniden gönderilmez.
- Oturum kurulması yoktur.
- Gönderme, kaynak kullanılabilirliği hakkında bilgilendirilmez.

# UDP Başlıkları

UDP başlığı TCP başlığından çok daha basittir çünkü yalnızca dört alanı vardır ve 8 bayt (yani 64 bit) gerektirir.



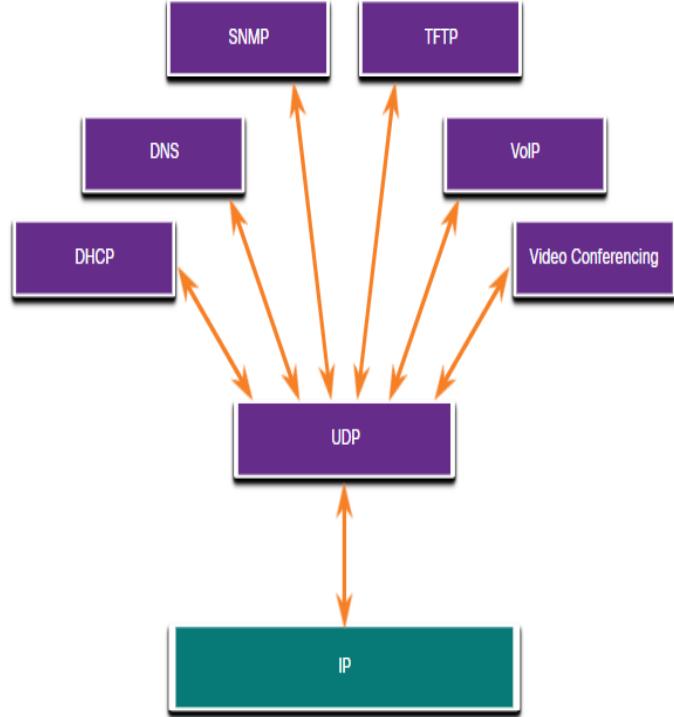
# UDP Başlık Alanları

Tablo, bir UDP başlığındaki dört alanı tanımlar ve açıklar.

UDP Başlık Alanları	Açıklama
Kaynak Port	Kaynak uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bitlik bir alan
Hedef Port	Hedef uygulamayı bağlantı noktası numarasına göre tanımlamak için kullanılan 16 bitlik bir alan
Uzunkuk	UDP datagram başlığının uzunluğunu gösteren 16 bitlik bir alan
Sağlama	Datagram başlığının ve verilerin hata kontrolü için kullanılan 16 bitlik bir alan

# UDP Kullanan Uygulamalar

- Canlı video ve multimedya uygulamaları** - Bu uygulamalar bazı veri kayıplarını toler 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.



# 14.4 Port Numaları

# Çoklu Ayrı İletişim

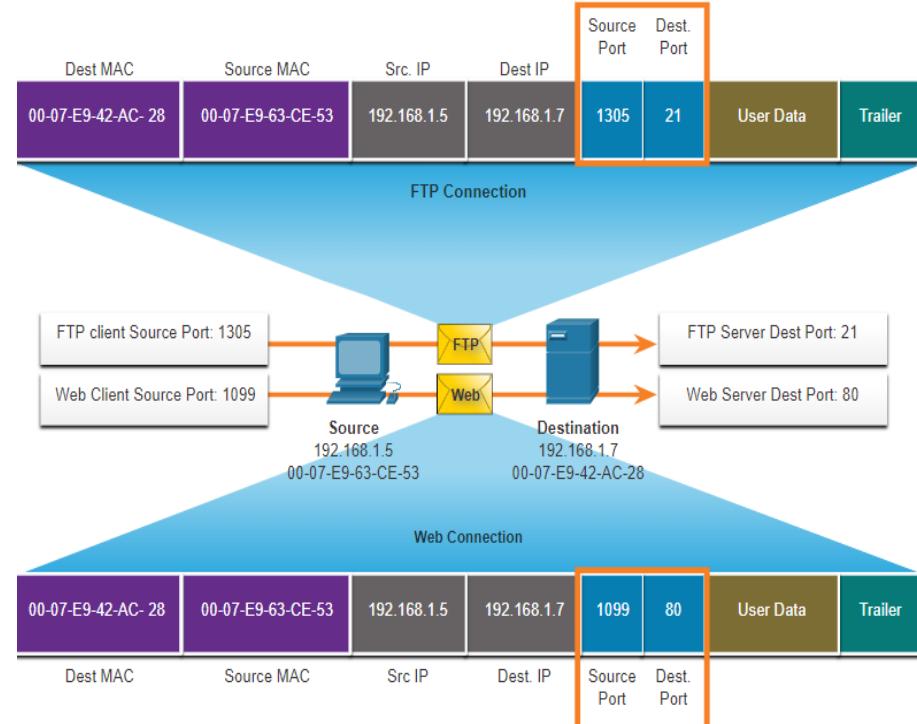
- ❖ **TCP** ve **UDP** aktarım katmanı protokolleri, **aynı anda birden çok konuşmayı yönetmek** için bağlantı noktası numaralarını kullanır.
- ❖ **Kaynak bağlantı noktası numarası**, yerel ana bilgisayardaki kaynak uygulama ile ilişkilendirilirken, hedef bağlantı noktası numarası uzak ana bilgisayardaki hedef uygulama ile ilişkilidir.

Source Port (16)

Destination Port (16)

# Port Numaları Soket Çiftleri

- **Kaynak ve hedef bağlantı noktaları, segmentin içine yerleştirilir.**
- **Segmentler** daha sonra bir **IP paketi** içinde kapsüllenir.
- **Kaynak IP adresi** ve **kaynak bağlantı noktası numarası** veya **hedef IP adresi** ile **hedef bağlantı noktası numarasının birleşimi soket olarak bilinir.**
- **Soketler**, bir istemcide çalışan birden çok işlemin kendilerini birbirinden ayırt etmesini ve bir sunucu işlemeye birden çok bağlantının birbirinden ayırt edilmesini sağlar.



# Port Numara Grupları

Port Grup	Numara Aralığı	Açıklama
Tanınmış Portlar	0 'dan 1,023	<ul style="list-style-type: none"> <li>Bu bağlantı noktası numaraları, <b>web tarayıcıları</b>, <b>e-posta istemcileri</b> ve <b>uzaktan erişim istemcileri</b> gibi <b>yaygın</b> veya <b>popüler</b> hizmetler ve uygulamalar için ayrılmıştır.</li> <li>Yaygın sunucu uygulamaları için tanımlanmış, iyi bilinen bağlantı noktaları, istemcilerin gereken ilişkili hizmeti kolayca tanımlamasını sağlar.</li> </ul>
Kayıtlı Portlar	1,024 'dan 49,151	<ul style="list-style-type: none"> <li>Bu bağlantı noktası numaraları, <b>IANA tarafından belirli süreçler</b> veya <b>uygulamalarla kullanmak üzere talepte bulunan bir varlığa atanır</b>.</li> <li>Bu işlemler, iyi bilinen bir bağlantı noktası numarası alacak genel uygulamalardan ziyade, <b>bir kullanıcının yüklemeyi seçtiği bireysel uygulamalardır</b>.</li> <li>Örneğin, <b>Cisco</b>, <b>RADIUS</b> sunucu kimlik doğrulama işlemi için <b>1812</b> numaralı bağlantı noktasını kaydetmiştir.</li> </ul>
Özel ve / veya Dinamik Portlar	49,152 'dan 65,535	<ul style="list-style-type: none"> <li>Bu bağlantı noktaları, <b>geçici bağlantı noktaları olarak da bilinir</b>.</li> <li><b>İstemcinin işletim sistemi</b>, bir hizmete bağlantı başlatıldığında genellikle bağlantı noktasını numaralarını <b>dinamik olarak atar</b>.</li> <li>Dinamik bağlantı noktası daha sonra <b>iletim sırasında istemci uygulamasını tanımlamak için kullanılır</b>.</li> </ul>

# Port Numara Grupları (Devam)

## Tanınmış Port Numaraları

Port Numarası	Protokol	Uygulama
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)

# “netstat” Komutu

Açıklanamayan TCP bağlantıları, büyük bir güvenlik tehdidi oluşturabilir.  
Netstat, bağlantıları doğrulamak için önemli bir araçtır.

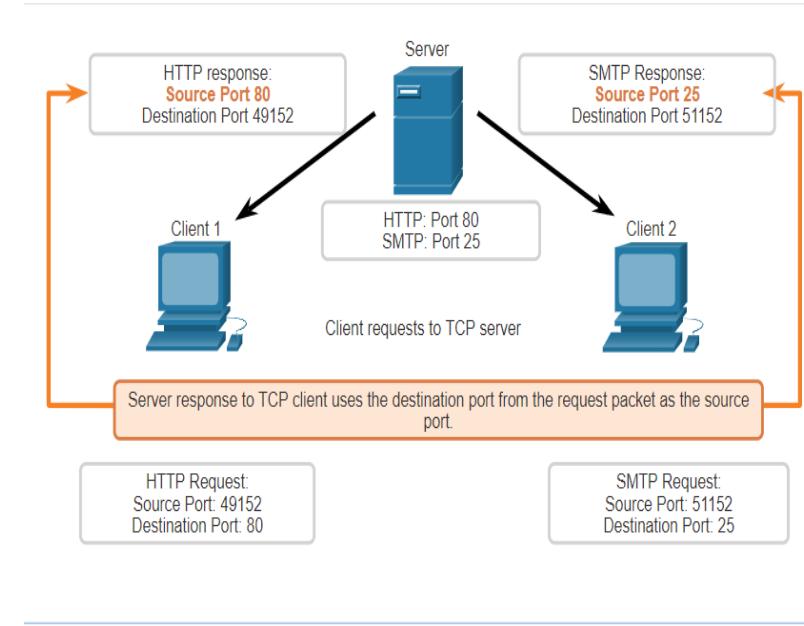
Active Connections			
Proto	Local Address	Foreign Address	State
TCP	192.168.1.124:3126	192.168.0.2:netbios-ssn	ESTABLISHED
TCP	192.168.1.124:3158	207.138.126.152:http	ESTABLISHED
TCP	192.168.1.124:3159	207.138.126.169:http	ESTABLISHED
TCP	192.168.1.124:3160	207.138.126.169:http	ESTABLISHED
TCP	192.168.1.124:3161	sc.msn.com:http	ESTABLISHED
TCP	192.168.1.124:3166	www.cisco.com:http	ESTABLISHED

# 14.5 TCP İletişim Süreci

# TCP Sunucu İşlemleri

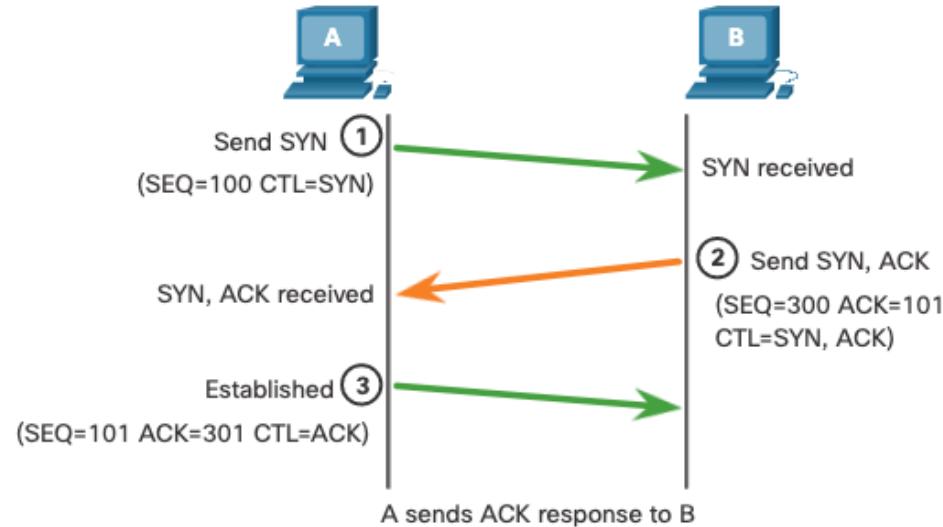
Bir sunucuda çalışan her uygulama işlemi, bir bağlantı noktası numarası kullanacak şekilde yapılandırılır.

- **Tek bir sunucu**, aynı taşıma katmanı hizmetleri içinde aynı bağlantı noktası numarasına atanmış iki hizmete sahip olamaz.
- Belirli bir bağlantı noktasına atanen etkin bir sunucu uygulaması öncelikle kabul edilir,
- Bu da taşıma katmanının o bağlantı noktasına adreslenen bölümleri kabul ettiği ve işlediği anlamına gelir.
- Doğru sokete gönderilen herhangi bir gelen istemci talebi kabul edilir ve veriler sunucu uygulamasına iletilir.



## TCP Bağlantı Kurulumu

- **Adım 1:** Başlatan istemci, sunucuya **istemciden sunucuya** bir iletişim oturumu talep eder.
- **Adım 2:** Sunucu, **istemciden sunucuya** iletişim oturumunu onaylar ve sunucudan istemciye bir iletişim oturumu talep eder.
- **Adım 3:** Başlatan istemci, sunucudan istemciye iletişim oturumunu onaylar.



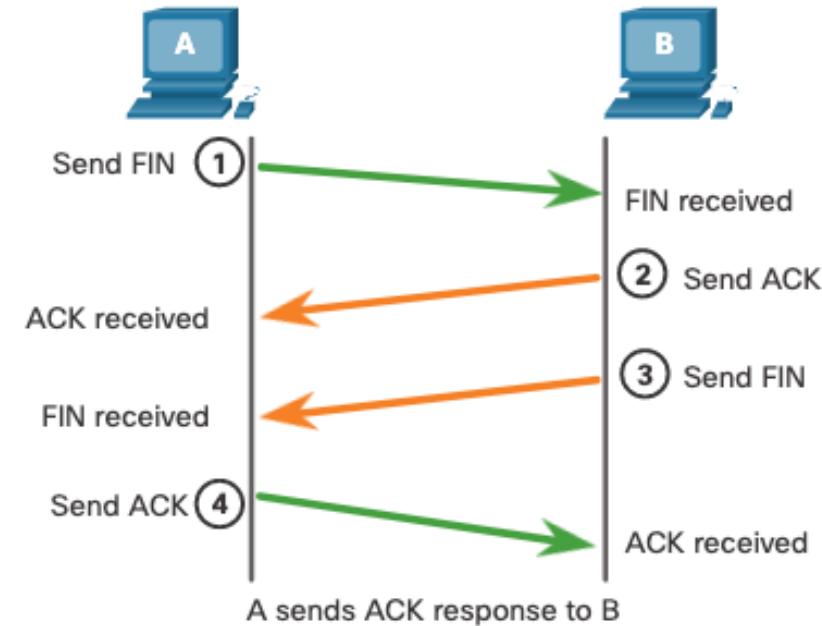
# TCP İletişim Süreci Oturum Sonlandırma

**Adım 1:** İstemcinin akışta gönderecek daha fazla verisi kalmadığında, **FIN bayrağı ayarlanmış bir segment gönderir.**

**Adım 2:** Sunucu, oturumu istemciden sunucuya sonlandırmak için FIN'in alındığını onaylamak için bir **ACK** gönderir.

**Adım 3:** Sunucu, sunucudan istemciye oturumu sonlandırmak için istemciye bir FIN gönderir.

**Adım 4:** İstemci, sunucudan FIN'i onaylamak için **bir ACK ile yanıt verir.**



## TCP 3 Aşamalı Uzlaşma Analizi

3 Aşamalı Uzlaşma İşlevi:

- Hedef aygıtın ağa 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.

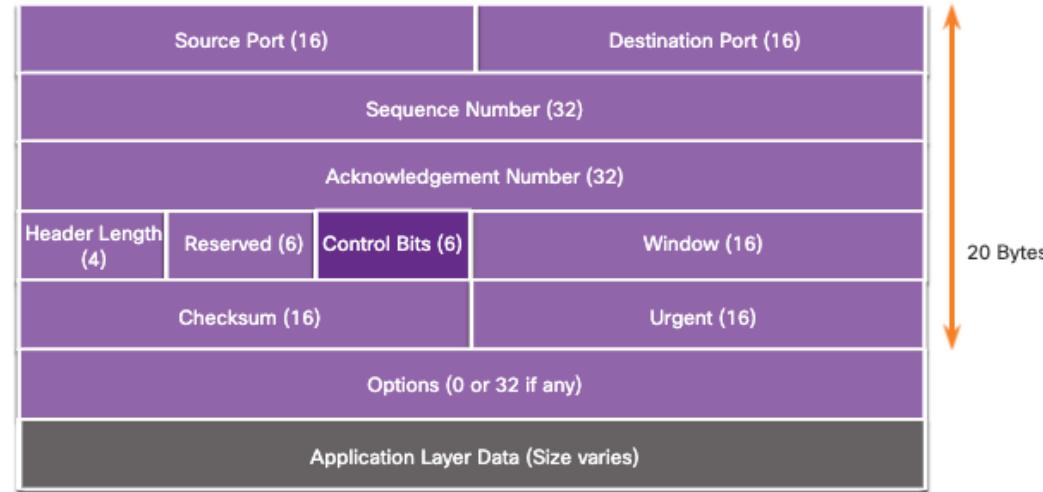
İletişim tamamlandıktan sonra oturumlar kapatılır ve bağlantı sonlandırılır.

Bağlantı ve oturum mekanizmaları, TCP güvenilirlik işlevini etkinleştirir.

# TCP 3 Aşamalı Uzlaşma Analizi (Devam)

Altı kontrol bit bayrağı aşağıdaki gibidir:

- **URG** - Acil işaretçi alanı önemli
- **ACK** - Bağlantı kurulumunda 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



# Video TCP Aşamalı Uzlaşma

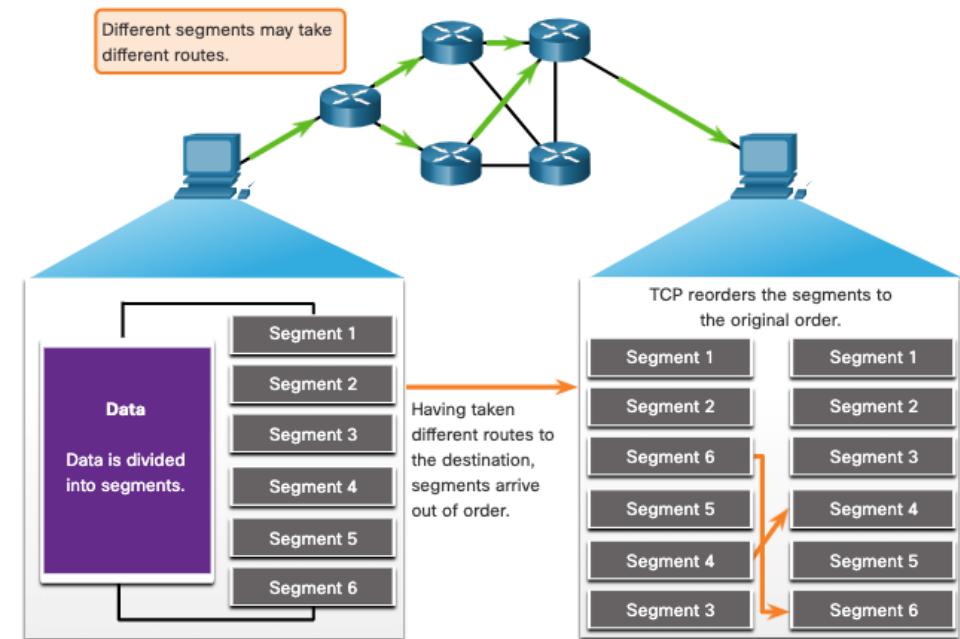
Bu video aşağıdakileri kapsar :

- TCP 3 Aşamalı Uzlaşma
- TCP Görüşmesinin Sonlandırılması

# 14.6 Güvenilirlik ve Akış Kontrolü

# TCP Güvenilirliği - Garantili ve Sipariş Edilen Teslimat

- **TCP**, paket akışının korunmasına da yardımcı olabilir, **böylece aygıtlar aşırı yüklenmez**.
- **TCP** kesimlerinin hedeflerine ulaşmadığı veya **sıra dışı** ulaştığı zamanlar olabilir.
- **Tüm veriler alınmalı** ve bu segmentlerdeki veriler **orijinal sıraya göre yeniden birleştirilmelidir**.
- **Bu hedefe ulaşmak için her paketin başlığında sıra numaraları atanır**.



# Video -TCP Güvenilirliği – Sıra Numaraları ve Onaylar

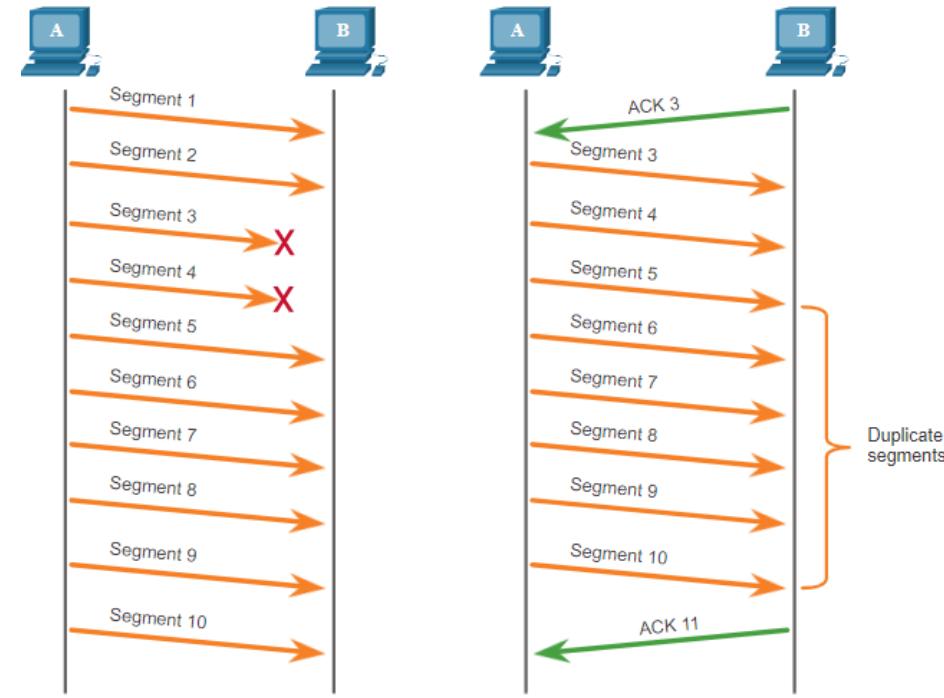
Bu video, başlangıçta hedef tarafından alınmayan segmentleri yeniden gönderme sürecini gösterir.

# TCP Güvenilirliği - Veri Kaybı ve Yeniden İletimi

❖ Bir ağ ne kadar iyi tasarlanırsa tasarlansın, zaman zaman veri kaybı meydana gelir.

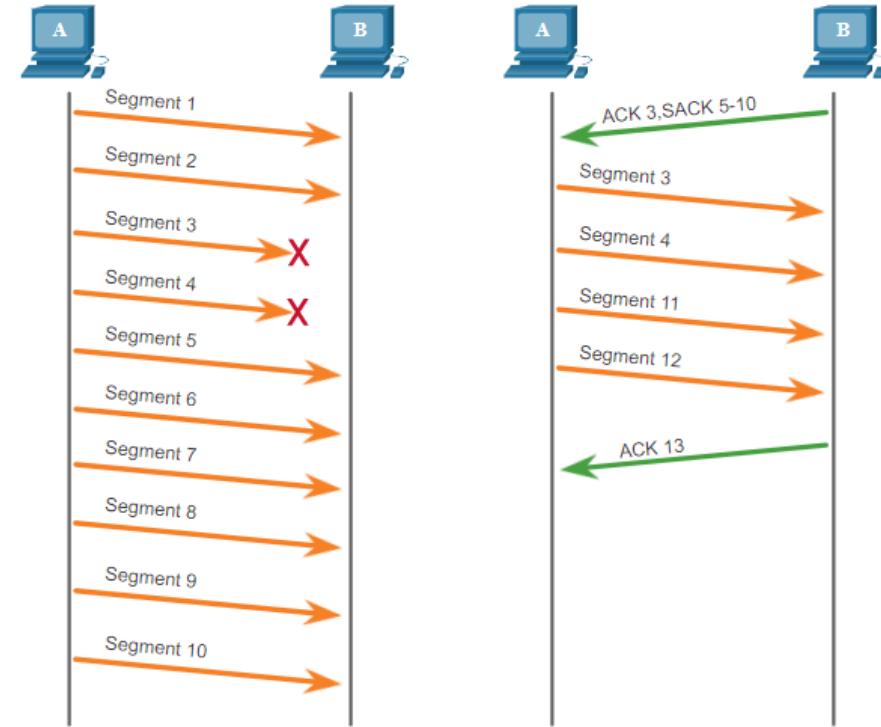
❖ TCP, bu segment kayıplarını yönetme yöntemleri sağlar.

❖ Bunların arasında, onaylanmamış veriler için segmentleri yeniden iletme mekanizması vardır.



# TCP Güvenilirliği - Veri Kaybı ve Yeniden İletimi (Devam)

- ❖ Bugün ana bilgisayar işletim sistemleri tipik olarak, **üç yönlü el sıkışma** sırasında görüşülen, seçici onay (SACK) adı verilen istege bağlı bir TCP özelliğini kullanır.
- ❖ **Her iki ana bilgisayar SACK'i** destekliyorsa, **alıcı, kesintili bölümler** de dahil olmak üzere hangi bölümlerin (baytların) alındığını açıkça onaylayabilir.



# Video - TCP Güvenilirliği - Veri Kaybı ve Yeniden İletimi

Bu video, başlangıçta hedef tarafından alınmayan segmentleri yeniden gönderme sürecini gösterir.

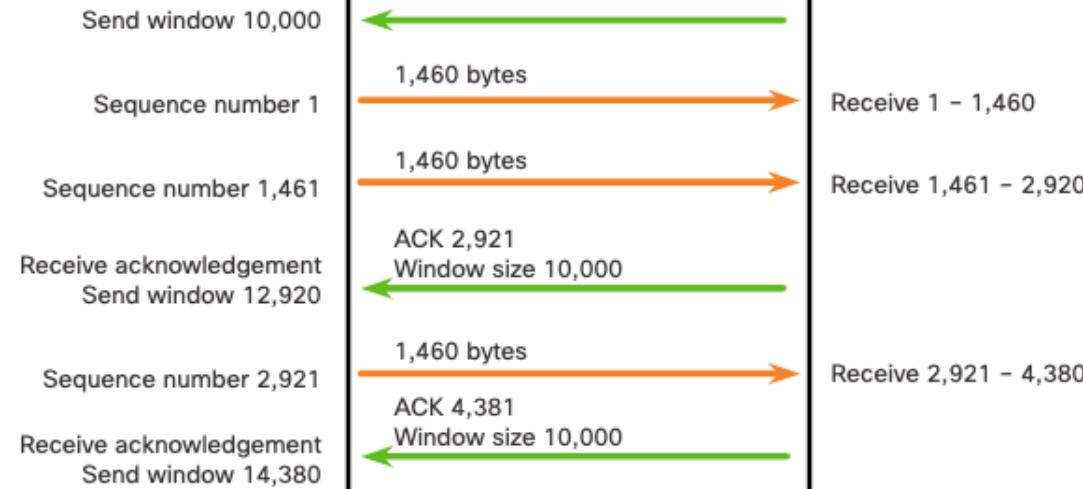
# TCP Akış Kontrolü - Pencere Boyutu ve Onaylar

CP ayrıca aşağıdaki gibi 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.**



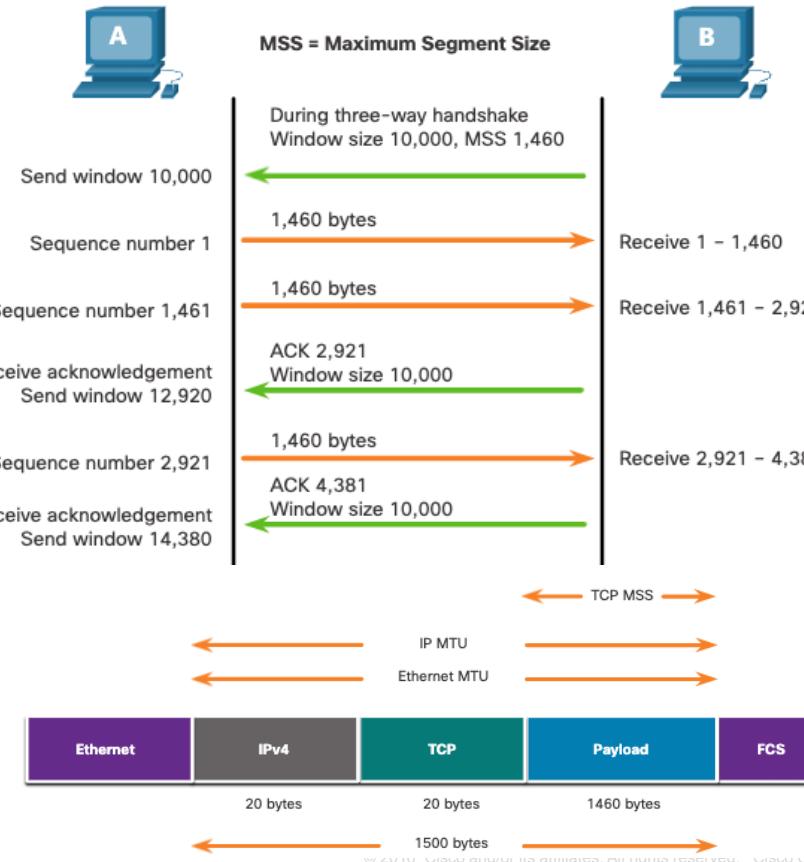
MSS = Maximum Segment Size



# TCP Akış Kontrolü - Maksimum Segment Boyutu

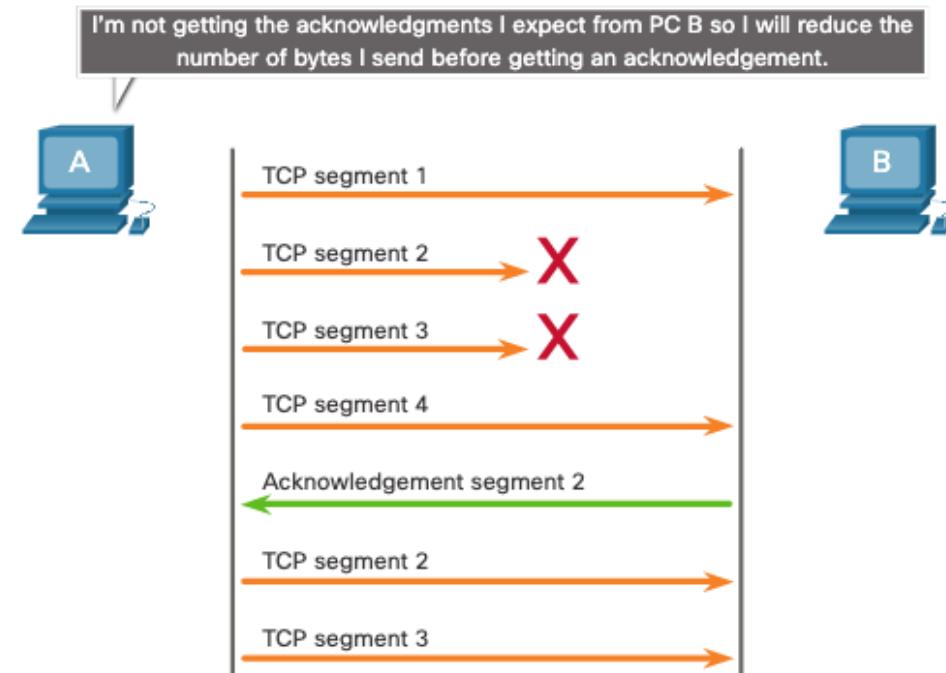
**Maksimum Segment Boyutu (MSS), hedef cihazın alabileceği maksimum veri miktarıdır.**

- IPv4 kullanılırken yaygın bir MSS **1.460 bayttır**.
- Bir ana bilgisayar, MSS alanının değerini, varsayılan olarak **1500 bayt olan Ethernet maksimum iletim biriminden (MTU)** IP ve TCP başlıklarını çıkararak belirler.
- 1500 eksi 40** (IPv4 üstbilgisi için 20 bayt ve TCP üstbilgisi için 20 bayt), 1460 bayt bırakır.



# TCP Akış Kontrolü - Tıkanıklıktan Kaçınma

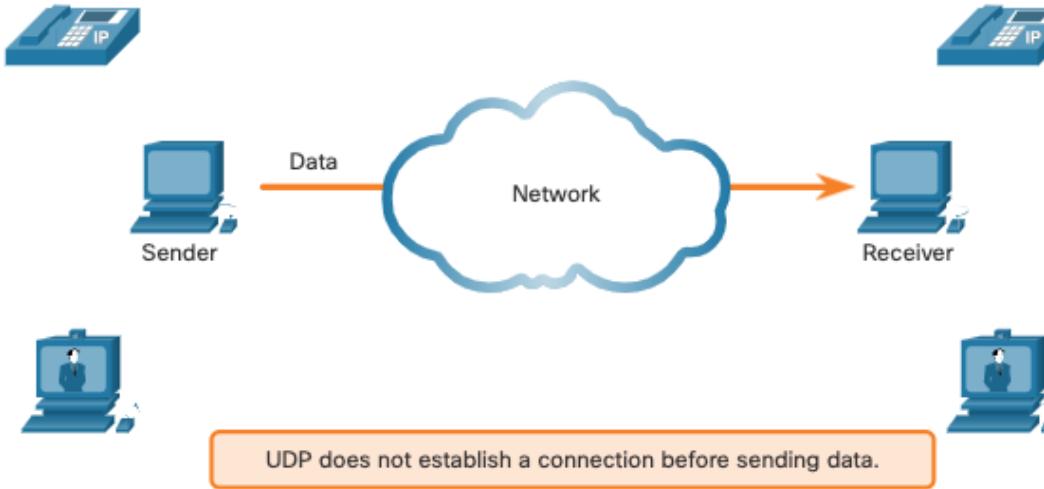
- Bir ağda tıkanıklık oluştuğunda, paketlerin aşırı yüklenmiş yönlendirici tarafından atılmasına neden olur.
- TCP, tıkanıklığı önlemek ve kontrol etmek için çeşitli tıkanıklık işleme mekanizmaları, zamanlayıcılar ve algoritmalar kullanır.



# 14.7 UDP İletişimi

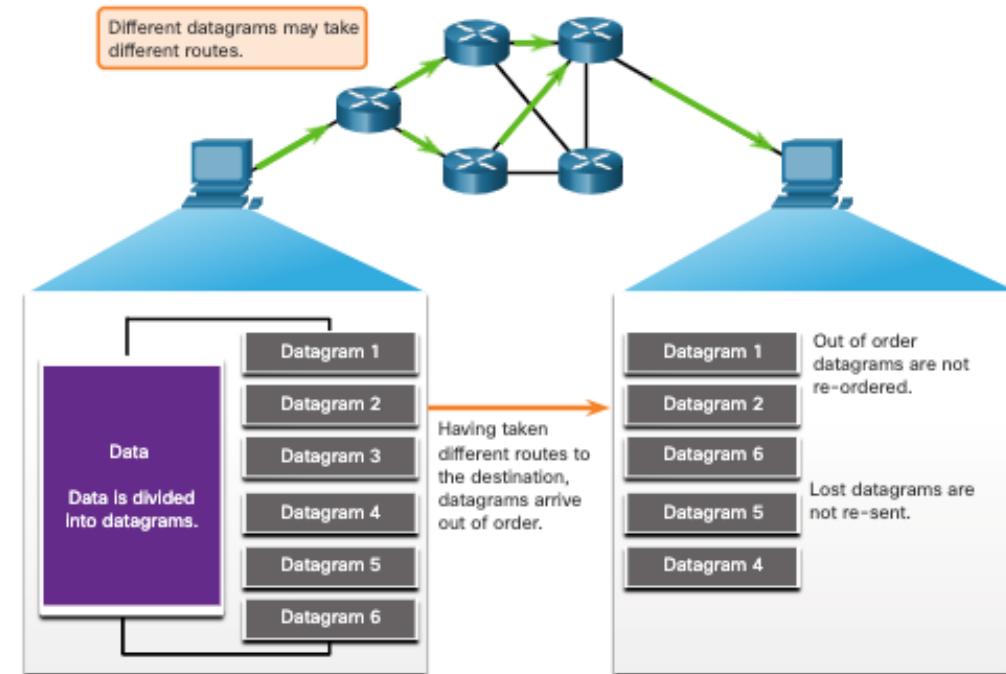
# UDP Düşük Ek Yük ve Güvenilirlik

- ❖ UDP bir bağlantı kurmaz.
- ❖ UDP, küçük bir veri birimi başlığına sahip olduğu ve ağ yönetimi trafiği olmadığı için düşük ek yük veri aktarımı sağlar.



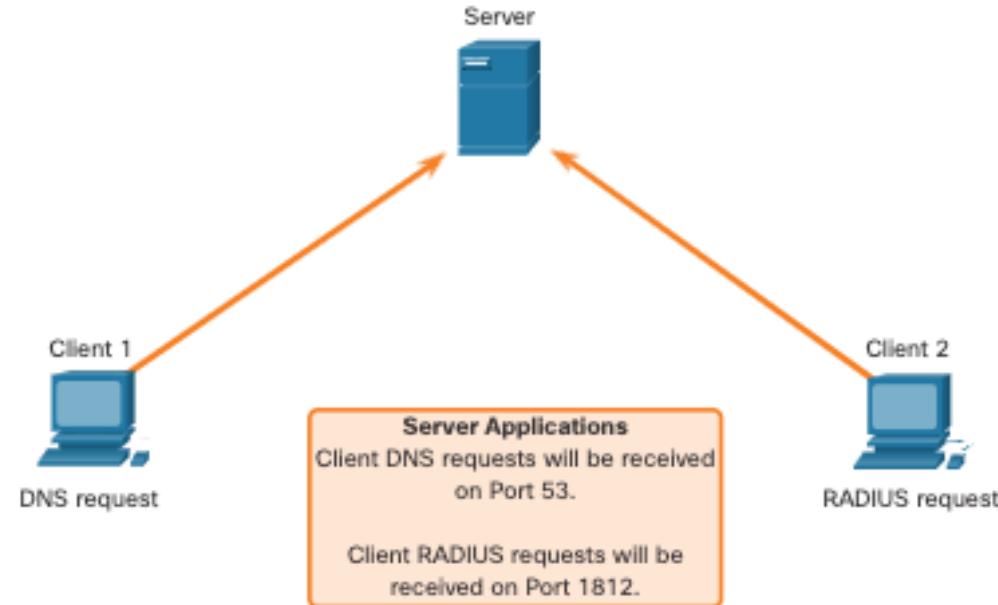
# UDP Datagram Yeniden Birleştirme

- UDP, TCP'nin yaptığı gibi sıra numaralarını izlemez.
- UDP, datagramları aktarım sıralarına göre yeniden sıralamanın bir yolu yoktur.
- UDP, verileri alındıkları sıraya göre yeniden birleştirir ve uygulamaya iletir.



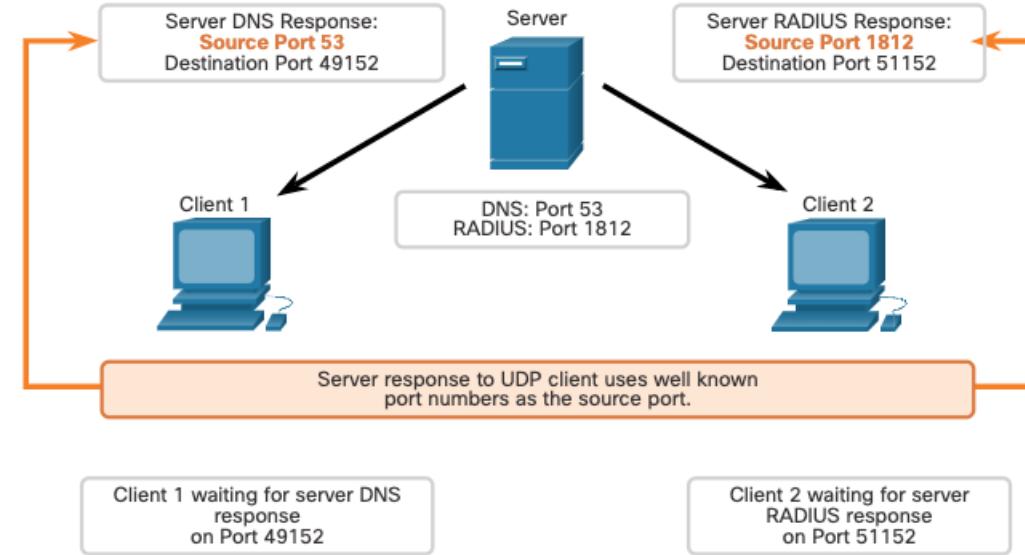
# UDP Sunucu İşlemleri ve Talepleri

- ❖ UDP tabanlı sunucu uygulamalarına iyi bilinen veya kayıtlı **bağlantı noktası numaraları atanır.**
- ❖ UDP, bu bağlantı noktalarından birine **yönelik bir veri birimi alır,** uygulama **bağlantı noktası numarasına** göre **uygun uygulamaya iletir.**



# 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**.
- Bir müşteri kaynak ve hedef bağlantı noktalarını **seçtiğinden sonra**, işlemdeki tüm **datagramların başlığında aynı bağlantı noktası çifti kullanılır**.



# 14.8 Alıştırmalar ve Sınav

# Packet Tracer - TCP ve UDP İletişimi

Packet Tracer ile , aşağıdakileri yapacaksınız :

- Simülasyon Modunda Ağ Trafiği Oluşturma.
- TCP ve UDP Protokollerinin İşlevselliğini inceleme

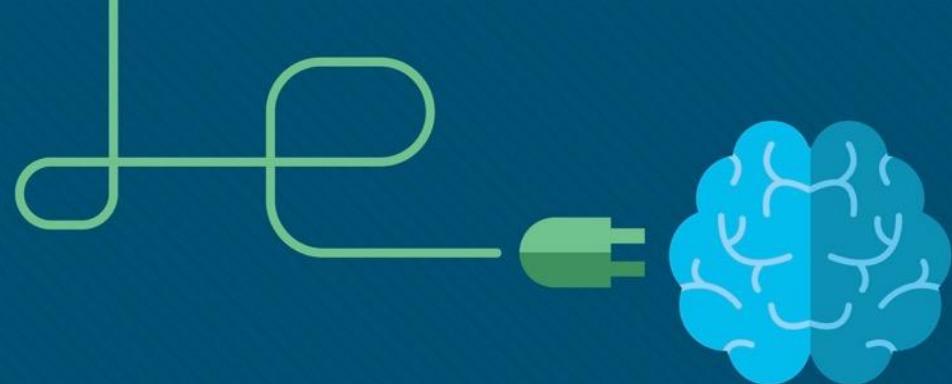
# BU modülde ne öğrendim?

- Taşıma katmanı, uygulama katmanı ile ağ iletiminden sorumlu olan alt katmanlar arasındaki bağlantıdır.
- Taşıma katmanı, TCP ve UDP'yi içerir.
- TCP, oturumlar kurar, güvenilirlik sağlar, aynı sipariş teslimatı sağlar ve akış kontrolünü destekler.
- UDP, temel taşıma katmanı işlevlerini sağlayan basit bir protokoldür.
- UDP, verileri alındıkları sırayla yeniden yapılandırır, kaybolan segmentler yeniden gönderilmez, oturum kurulmaz ve UDP, göndereni kaynak kullanılabilirliği konusunda bilgilendirmez.
- TCP ve UDP taşıma katmanı protokolleri, aynı anda birden çok konuşmayı yönetmek için bağlantı noktası numaralarını kullanır.
- Bir sunucuda çalışan her uygulama işlemi bir bağlantı noktası numarası kullanacak şekilde yapılandırılır.
- Bağlantı noktası numarası, bir sistem yönetici tarafından otomatik olarak atanır veya manuel olarak yapılandırılır.
- Orijinal mesajın alıcı tarafından anlaşılabilmesi için tüm verilerin alınması ve bu segmentlerdeki verilerin orijinal sıraya göre yeniden birleştirilmesi gereklidir.

# BU modülde ne öğrendim?

- Sıra numaraları, her paketin başlığında atanır.
- Akış kontrolü, kaynak ve hedef arasındaki veri akış hızını ayarlayarak TCP iletiminin güvenilirliğini korumaya yardımcı olur.
- Bir kaynak, her TCP segmenti içinde 1.460 bayt veri iletiyor olabilir. Bu, bir hedef aygıtın alabileceği tipik MSS'dir.
- Hedefin alınan baytları işlerken onay gönderme süreci ve kaynağın gönderme penceresinin sürekli ayarlanması, kayan pencereler olarak bilinir.
- TCP, tıkanıklığı önlemek ve kontrol etmek için çeşitli tıkanıklık işleme mekanizmaları kullanır.





# Modül 15: Uygulama Katmanı

Introduction to Networks v7.0  
(ITN)



# Modül Hedefleri

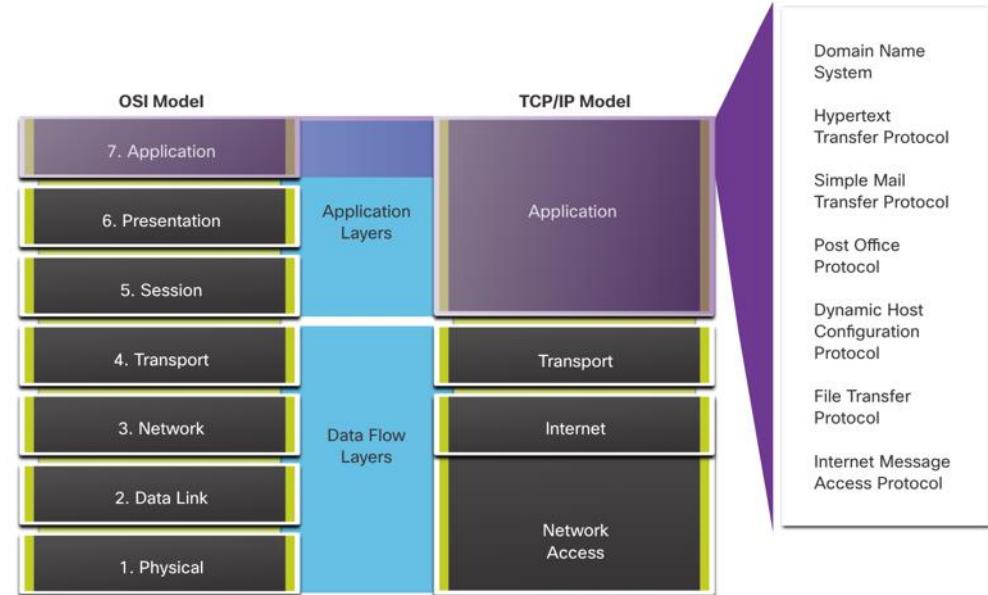
- **Modül Başlığı:** Uygulama Katmanı
- **Modül Amacı:** Son kullanıcı uygulamalarına destek sağlamaada uygulama katmanı protokollerinin işleyişinin açıklanması

Konu Başlığı	Amaç
Uygulama, Sunum, ve Oturum	Uygulama katmanının, sunum katmanının ve oturum katmanının işlevlerinin, son kullanıcı uygulamalarına ağ hizmetleri sağlamak için birlikte nasıl çalıştığını açıklaması
Eşler Arası (Peer-to-Peer)	Üç kullanıcı uygulamalarının eşler arası bir ağda nasıl çalıştığını açıklaması
Web ve E-Posta Protokolleri	Web ve Eposta protokollerinin nasıl çalıştığını açıklaması
IP Adres Servisleri	DNS ve DHCP 'nin nasıl çalıştığını açıklaması.
Dosya Paylaşım Servisleri	Dosya aktarım protokollerinin nasıl çalıştığını açıklaması

# 15.1 Uygulama , Sunum ve Oturum

## Uygulama Katmanı

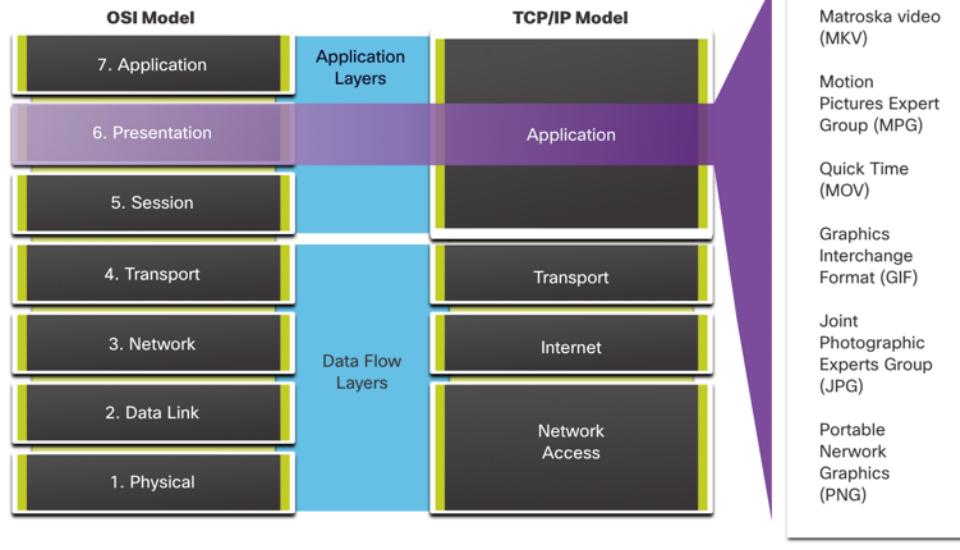
- **OSI** modelinin üstteki üç katmanı (uygulama, sunum ve oturum), **TCP / IP uygulama katmanının işlevlerini tanımlar.**
- **Uygulama katmanı**, iletişim için kullanılan uygulamalar ile mesajların iletiliği temel ağ arasındaki arayüzü **sağlar**.
- En yaygın olarak bilinen uygulama katmanı protokollerinden bazıları **HTTP, FTP, TFTP, IMAP** ve **DNS**'dir.



# Sunum ve Oturum Katmanları

## ❖ Sunum katmanının 3 temel işlevi vardır:

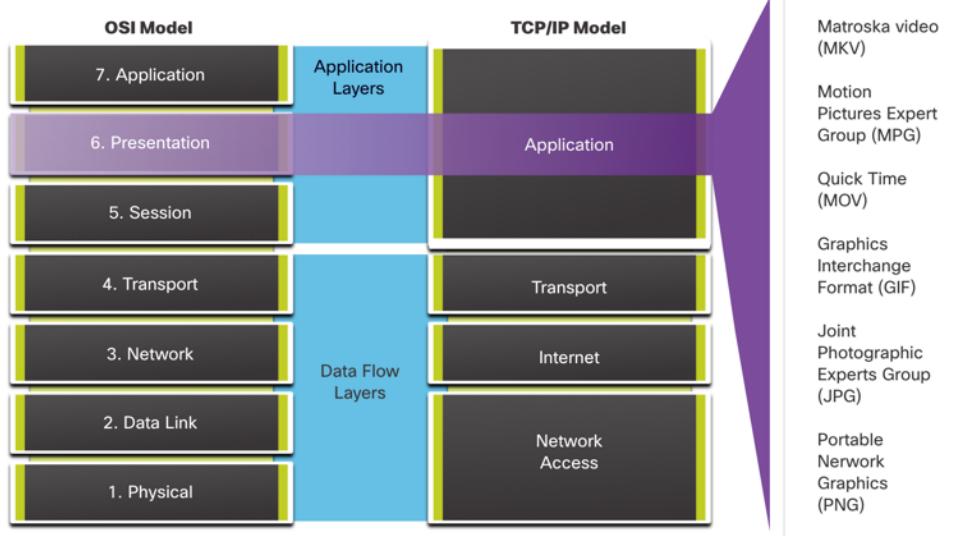
1. Hedef cihaz tarafından alınmak üzere kaynak cihazdaki **verileri uyumlu bir formatta formatlama veya sunma**
2. **Verilerin**, hedef cihaz tarafından açılabilen şekilde sıkıştırılması
3. İletim için verileri **şifreleme** ve alındıktan sonra **verilerin şifresini çözme.**



# Sunum ve Oturum Katmanları

## ❖ Oturum Katmanın İşlevleri:

1. Kaynak ve hedef uygulamalar arasında diyaloglar oluşturur ve sürdürürlük sağlar.
2. Diyalogları **başlatmak**, onları **aktif tutmak** ve **kesintiye uğramış** veya **uzun süre boşta kalan oturumları yeniden başlatmak** için bilgi alışverisini yönetir.



# TCP/IP Uygulama Katmanı Protokollerı

- **TCP / IP uygulama protokollerı**, birçok yaygın internet iletişim işlevi için **gerekli olan format** ve **kontrol bilgilerini belirtir.**
- **Uygulama katmanı protokollerı**, bir iletişim oturumu sırasında **hem kaynak** hem de **hedef cihazlar** tarafından kullanılır.
- İletişimin başarılı olması için, **kaynak** ve **hedef** ana bilgisayarda uygulanan **uygulama katmanı protokollerinin uyumlu olması** gereklidir.

## İsim Sistemi

### DNS – Alan Adı Sistemi (Servisi)

- TCP, UDP istemci 53
- Cisco.com gibi alan adlarını IP adreslerine çevirir.

## Ana Bilgisayar Yapılandırması

### DHCP – Dinamik Ana Bilgisayar Yapılandırma Protokolü

- UDP istemci 68, sunucu 67
- Artık ihtiyaç duyulmadığında yeniden kullanılacak IP adreslerini dinamik olarak atar

## Web

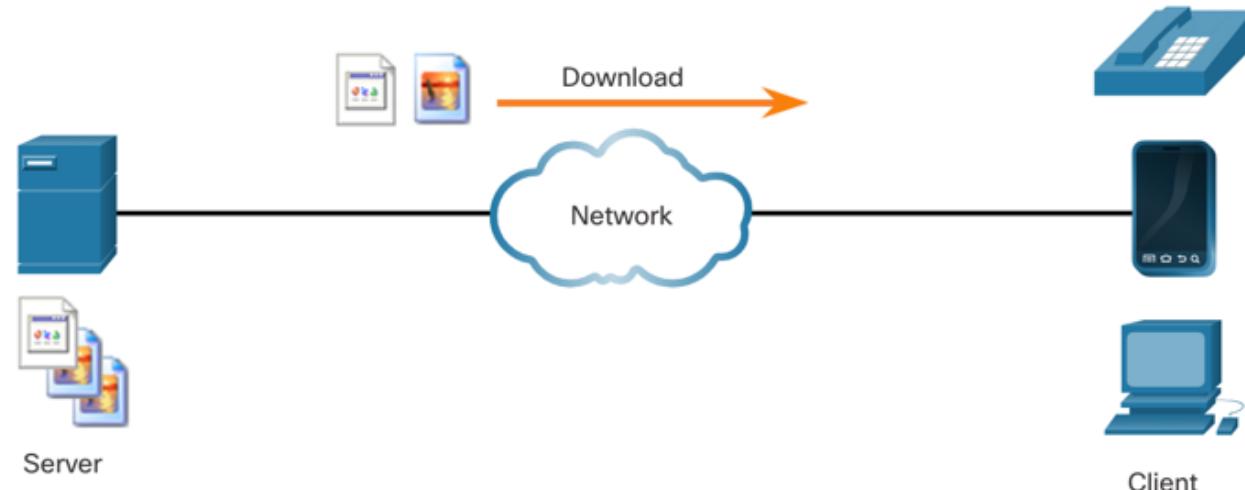
### HTTP - Hypertext Transfer Protokolü

- TCP 80, 8080
- World Wide Web'de metin, grafik görüntü, ses, video ve diğer multimedya dosyalarını değişim tokusu etmek için bir dizi kural

# 15.2 Eşler Arası (Peer-to-Peer)

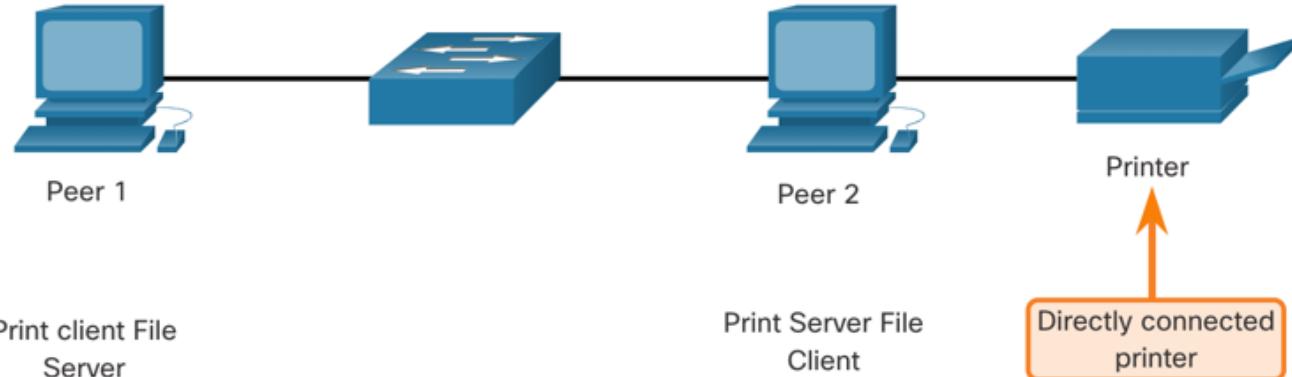
# İstemci Sunucu Modeli

- ❖ İstemci ve sunucu süreçleri uygulama katmanında kabul edilir.
- ❖ İstemci / sunucu modelinde **bilgi talep eden cihaza istemci, talebe cevap veren cihaza ise sunucu** adı verilir.
- ❖ Uygulama katmanı protokolleri, istemciler ve sunucular arasındaki **isteklerin ve yanıtlarının biçimini tanımlar**.



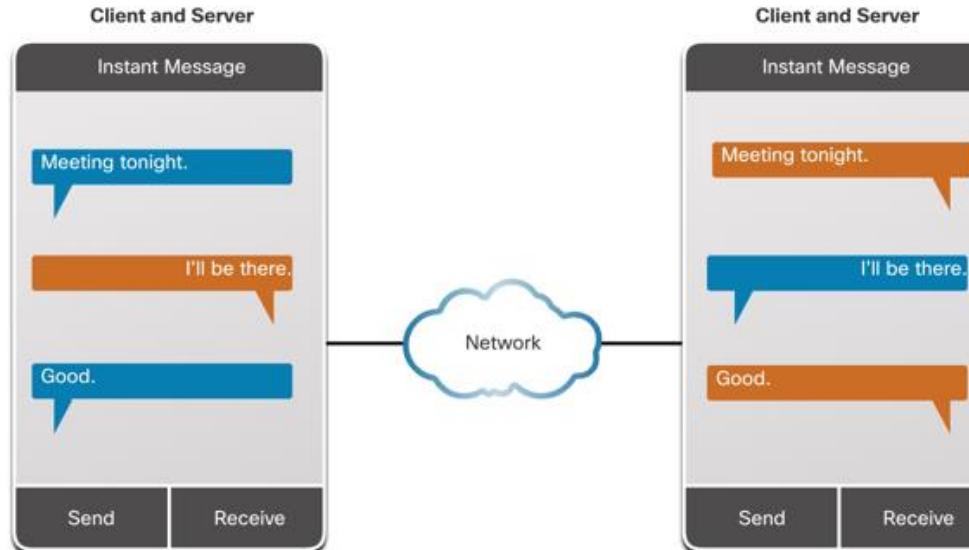
# Eşler Arası Ağlar

- ❖ Eşler arası (P2P) bir ağa, iki veya daha fazla bilgisayar bir ağ üzerinden 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, bir işlem için sunucu rolünü üstlenirken, aynı anda bir başkası için bir istemci olarak hizmet verebilir.
- ❖ İstemci ve sunucunun rolleri isteğe göre belirlenir.



# Eşler Arası Uygulamalar

- Bir P2P uygulaması, bir cihazın aynı iletişim içinde hem istemci hem de sunucu olarak hareket etmesine izin verir.
- Bazı P2P uygulamaları, her bir eşin başka bir eşte depolanan bir kaynağın konumunu almak için bir dizin sunucusuna eriştiği karma bir sistem kullanır.

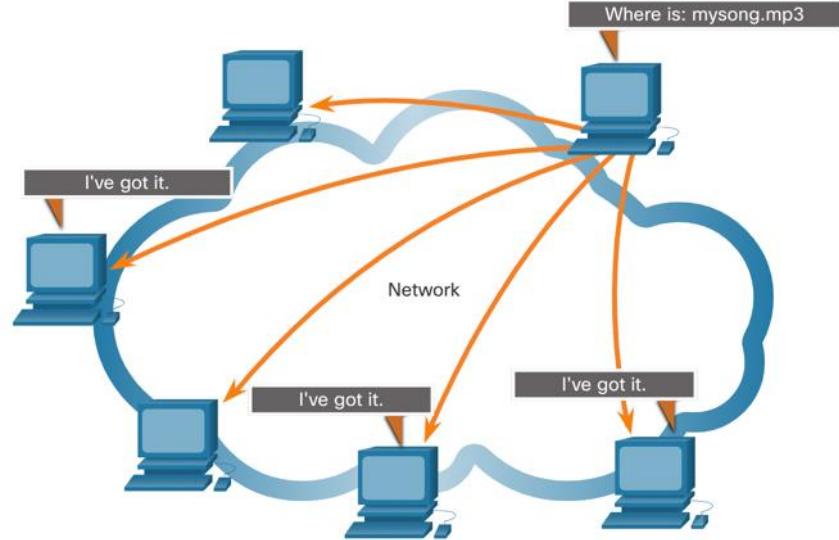


# Yaygın P2P Uygulamalar

**P2P uygulamalarıyla,** uygulamayı çalıştırılan ağdaki her bilgisayar, uygulamayı çalıştırılan ağdaki diğer bilgisayarlar için **bir istemci veya sunucu görevi görebilir.**

Yaygın P2P ağları :

- BitTorrent
- Direct Connect
- eDonkey
- Freenet



# 15.3 Web ve Eposta Protokollerı

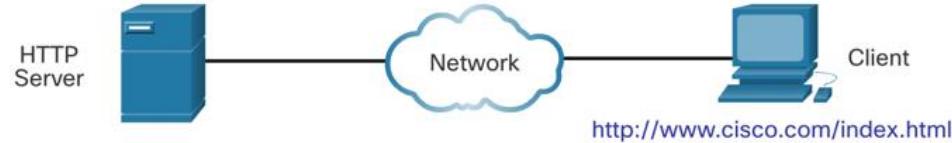
# Hypertext Transfer Protokolü ve Hypertext Biçimlendirme Dili

- Bir web adresi veya Tekdüzen Kaynak Konum Belirleyicisi (URL) **bir web tarayıcısına yazıldığında, web tarayıcısı web hizmetiyle bir bağlantı kurar.**
- **Web hizmeti**, HTTP protokolünü kullanan sunucuda çalışıyor.
- Web tarayıcısının ve web sunucusunun nasıl etkileşim kurduğunu daha iyi anlamak için, bir web sayfasının bir tarayıcıda nasıl açıldığını inceleyin.

## Adım 1

Tarayıcı, URL'nin üç bölümünü yorumlar:

- http (protokol veya şema)
- www.cisco.com (sunucu adı)
- index.html (istenen belirli dosya adı)



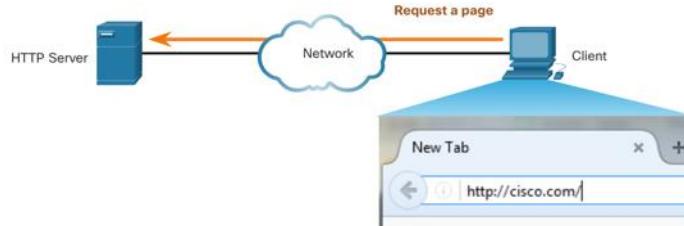
# Web ve Eposta Protokolü

## Hypertext Transfer Protokolü ve Hypertext Biçimlendirme Dili ( Devam )

### Adım 2

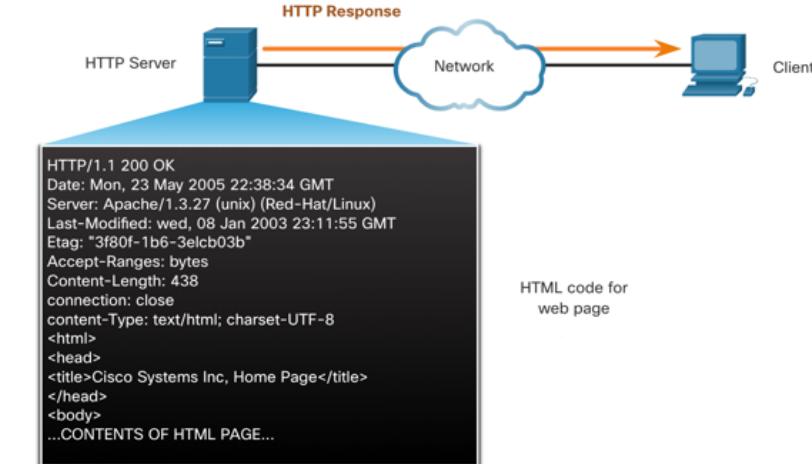
Tarayıcı daha sonra **www.cisco.com'u** sunucuya bağlanmak için kullandığı sayısal bir IP adresine dönüştürmek için bir ad sunucusuyla kontrol eder.

İstemci, sunucuya bir **GET** isteği göndererek bir sunucuya bir **HTTP** isteği başlatır ve **index.html** dosyasını ister.



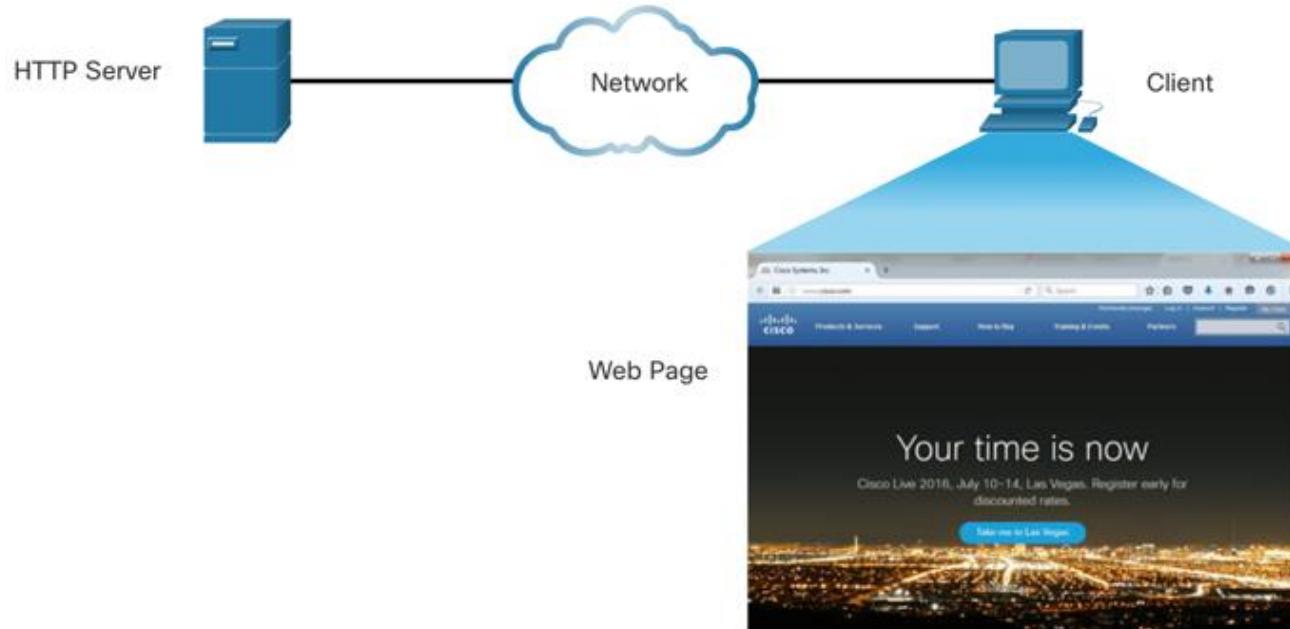
### Adım 3

İsteğe yanıt olarak, sunucu bu web sayfası için HTML kodunu tarayıcıya gönderir.



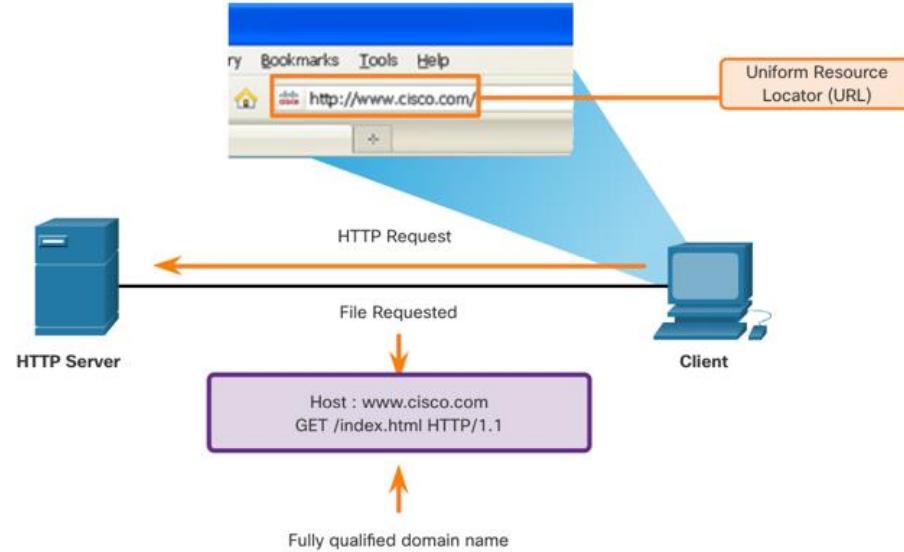
### Adım 4

Tarayıcı, HTML kodunu çözer ve tarayıcı penceresi için sayfayı biçimlendirir.



# HTTP ve HTTPS

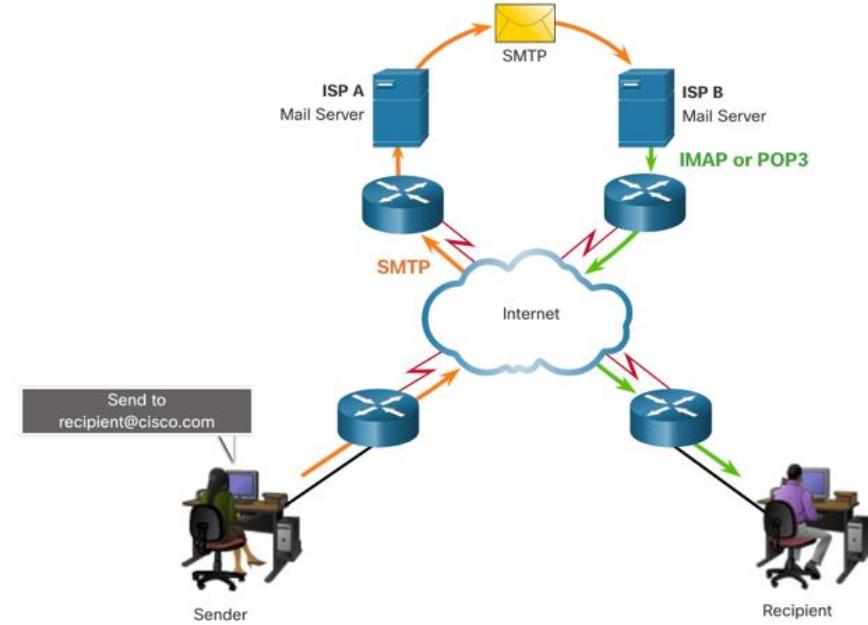
- **HTTP** HTTP, söz konusu iletişim için kullanılan mesaj türlerini belirten **bir istek / yanıt protokolü**dür.
- **Üç yaygın mesaj türü GET, POST ve PUT'** tur:
  - **GET** - Bu, veri için bir müşteri isteğidir. Bir istemci (web tarayıcısı), HTML sayfalarını talep etmek için GET mesajını web sunucusuna gönderir.
  - **POST** - Bu, form verileri gibi veri dosyalarını web sunucusuna yükler.
  - **PUT** - Bu, bir resim gibi kaynakları veya içeriği web sunucusuna yükler.



**Not:** **HTTP, güvenli bir protokol değildir.**  
İnternet üzerinden gönderilen güvenli iletişim için **HTTPS** kullanılmalıdır.

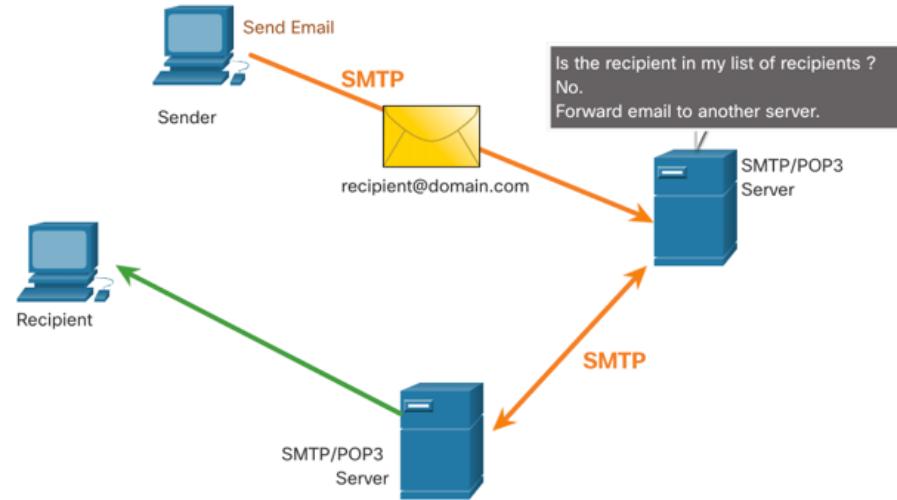
# Eposta Protokolü

- **E-posta, elektronik mesajları bir ağ üzerinden göndermenin, saklamanın ve geri almanın bir sakla ve ilet yöntemidir.**
- **E-posta mesajları, posta sunucularındaki veritabanlarında saklanır.**
- **E-posta istemcileri, e-posta göndermek ve almak için posta sunucusu ile iletişim kurar.**
- **İşlem için kullanılan e-posta protokolleri şunlardır:**
  - Basit Posta Aktarım Protokolü (SMTP) - **posta göndermek için kullanılır.**
  - Postane Protokolü (POP) ve IMAP - **istemcilerin posta alması için kullanılır.**



# SMTP, POP ve IMAP

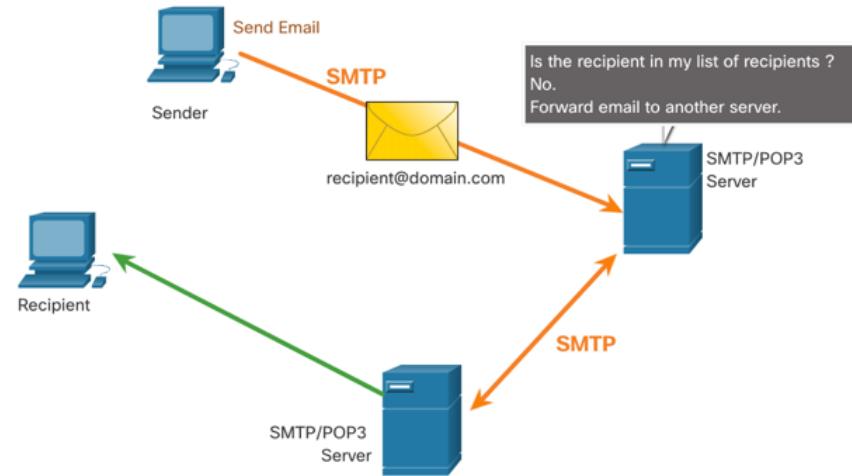
- Bir istemci e-posta gönderdiğinde, istemci SMTP işlemi, iyi bilinen 25 numaralı bağlantı noktasındaki bir sunucu SMTP işlemine bağlanır.
- Bağlantı kurulduktan sonra, istemci e-postayı bağlantı üzerinden sunucuya göndermeye çalışır.



**Not:** SMTP mesaj biçimleri bir mesaj başlığı (alıcı e-posta adresi ve gönderen e-posta adresi) ve bir mesaj gövdesi gerektirir.

# SMTP, POP ve IMAP

- Sunucu iletiyi aldığında, ya **alıcı yerelse** iletiyi yerel bir hesaba **yerleştirir** ya da **iletisi teslim edilmek üzere** başka **bir posta sunucusuna** iletir.
- **Hedef e-posta sunucusu, çevrimiçi olmayabilir** veya **meşgul olabilir**.
- Öyleyse, **SMTP, iletileri daha sonra gönderilmek üzere biriktirir.**



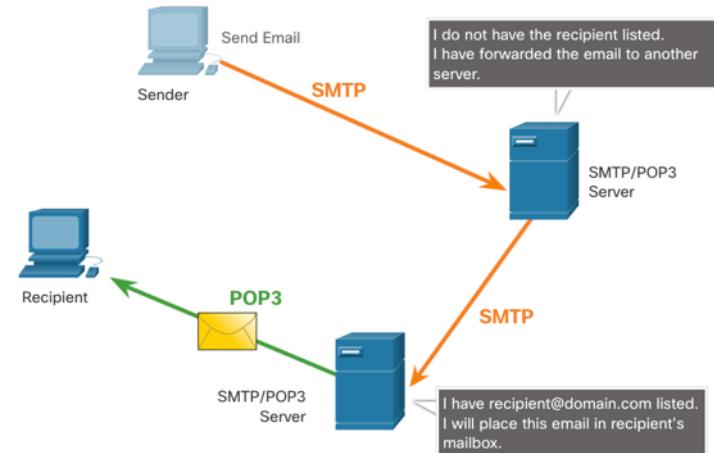
Not: SMTP mesaj biçimleri **bir mesaj başlığı** (alıcı e-posta adresi ve gönderen e-posta adresi) ve **bir mesaj gövdesi** gerektirir.

# SMTP, POP ve IMAP (Devam)

**POP, bir uygulama tarafından posta sunucusundan posta almak için kullanılır.**

**Posta, sunucudan istemciye POP kullanılarak indirildiğinde, mesajlar sunucudan silinir.**

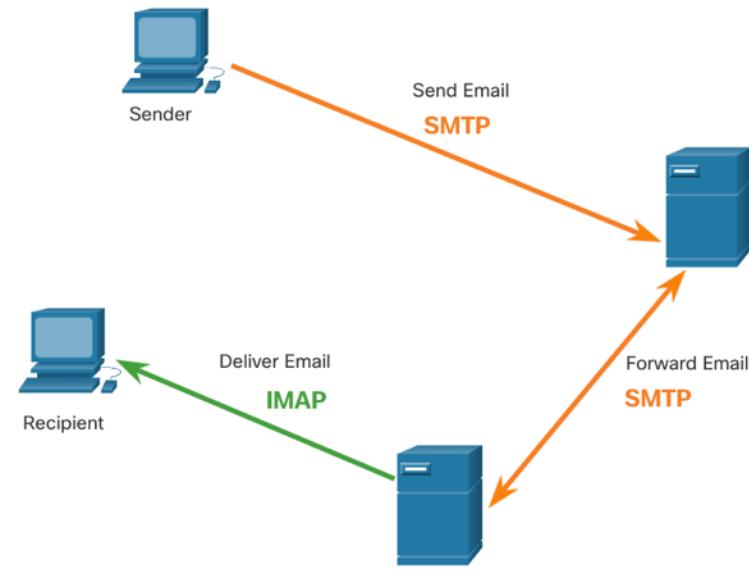
- Sunucu, istemci bağlantı istekleri için TCP bağlantı noktası 110'u pasif olarak dinleyerek **POP hizmetini başlatır.**
- Bir istemci hizmetten yararlanmak istediyinde, sunucuya bir **TCP bağlantısı kurmak için bir istek gönderir.**
- Bağlantı kurulduğunda, **POP sunucusu bir karşılama mesajı gönderir.**
- **İstemci ve POP sunucusu, bağlantı kapanana veya kesilene kadar komut ve yanıt alışverişinde bulunur.**



**Not: POP, iletileri depolamadığından, merkezi bir yedekleme çözümüne ihtiyaç duyan küçük işletmeler için önerilmez.**

# SMTP, POP ve IMAP (Devam)

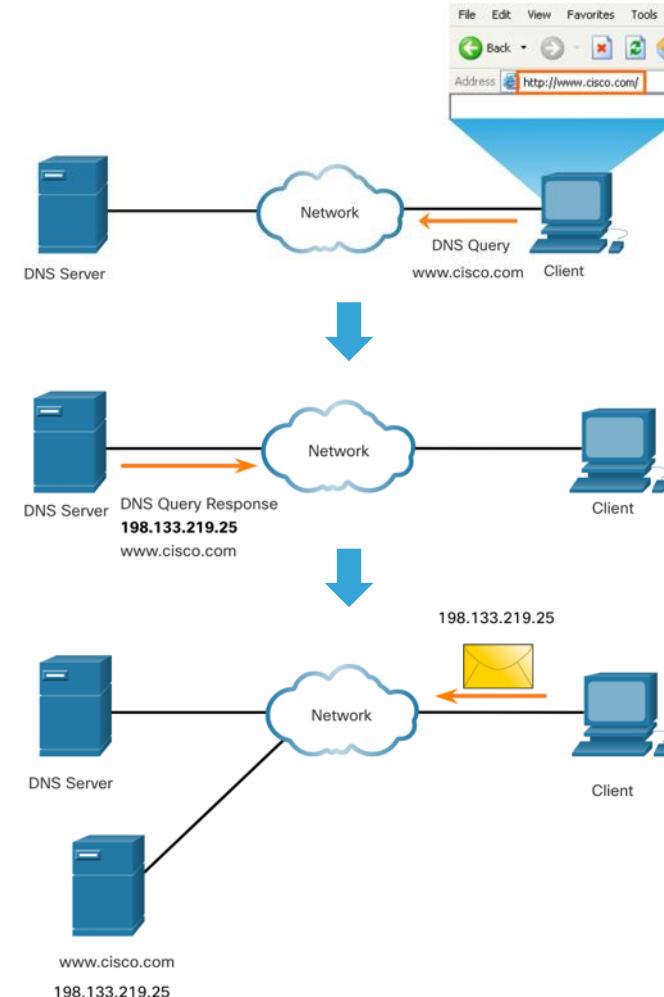
- **IMAP**, e-posta mesajlarını alma yöntemini tanımlayan başka bir protokoldür.
- **POP'un aksine**, bir kullanıcı bir IMAP sunucusuna bağlandığında, **mesajların kopyaları istemci uygulamasına indirilir.**
- Orijinal mesajlar, manuel olarak silinene kadar sunucuda tutulur.
- **Bir kullanıcı bir mesajı silmeye karar verdiğinde**, sunucu bu eylemi senkronize eder ve mesajı sunucudan siler.



# 15.4 IP Adres Servisleri

# Alan Adı Servisi

- **Alan adları**, sayısal IP adreslerini basit, tanımlayıcı bir ada dönüştürmek için oluşturulmuştur.
- **Http://www.cisco.com** gibi **tam nitelikli alan adları** (FQDN'ler), **198.133.219.25**'e göre insanların hatırlaması için çok daha kolaydır.
- **DNS protokolü**, kaynak adlarını gerekli sayısal ağ adresiyle eşleştiren otomatik bir hizmeti tanımlar.
- **Sorgular, yanıtlar ve veriler** için format **İçerir**.



## DNS Mesaj Formatı

- **DNS sunucusu**, adları çözümlemek için kullanılan **farklı kaynak kayıt türlerini depolar**.
- Bu kayıtlar, **kayıt adını**, **adresini** ve **türünü** içerir.
- **Bu kayıt türlerinden bazıları aşağıdaki gibidir:**
  - **A** - Bir son cihaz IPv4 adresi
  - **NS** - Yetkili bir ad sunucusu
  - **AAAA** - Bir uç cihaz IPv6 adresi (quad-A olarak okunur)
  - **MX** - Posta alışverişi kaydı

**Bir istemci bir soru yaptığından**, sunucu DNS işlemi adı çözümlemek için önce **kendi kayıtlarına bakar**.

Saklanan kayıtlarını kullanarak adı **çözümlenemezse**, adı **çözülemek için diğer sunucularla iletişim kurar**.

**Bir eşleşme bulunduktan ve orijinal istekte bulunan sunucuya geri döndükten sonra**, sunucu aynı adın tekrar istenmesi durumunda **numaralı adresi geçici olarak saklar**.

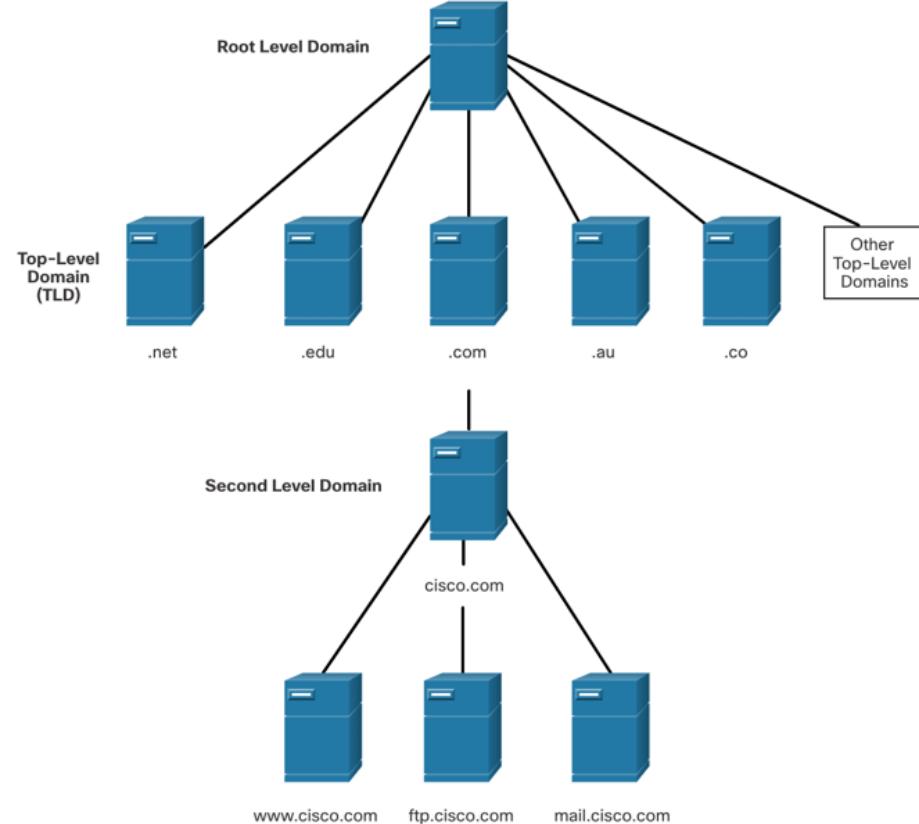
# DNS Mesaj Formatı (Devam)

❖ DNS, bir soru, yanıt, yetki ve tüm istemci sorguları ve sunucu yanıtları, hata iletileri ve kaynak kaydı bilgilerinin aktarımı için **ek bilgilerden oluşan sunucular arasında aynı ileti biçimini kullanır.**

DNS Mesaj Bölümü	Açıklama
Soru	İsim Sunucusu için Soru
Cevap	Soruyu yanıtlayan kaynak kayıtları
Yetki	Bir otoriteyi işaret eden kaynak kayıtları
Ekler	Ek bilgi içeren kaynak kayıtları

## DNS Hiyerarşisi

- DNS, ad çözümlemesi sağlamak üzere bir veritabanı oluşturmak için **hiyerarşik bir sistem kullanır.**
- Her DNS sunucusu belirli bir veritabanı dosyası tutar ve yalnızca tüm DNS yapısının bu küçük bölümü için addan **IP'ye eşleştirmelerin yönetilmesinden sorumludur.**
- Bir DNS sunucusu, **kendi DNS bölgesi içinde olmayan bir ad çevirisini için istek aldığımda, DNS sunucusu isteği çeviri için uygun bölge içindeki başka bir DNS sunucusuna iletir.**
- **Üst düzey alanlara örnekler:**
  - .com - bir işletme veya endüstri
  - .org - kar amacı gütmeyen bir kuruluş
  -  .au - Avustralya



# nslookup Komutu

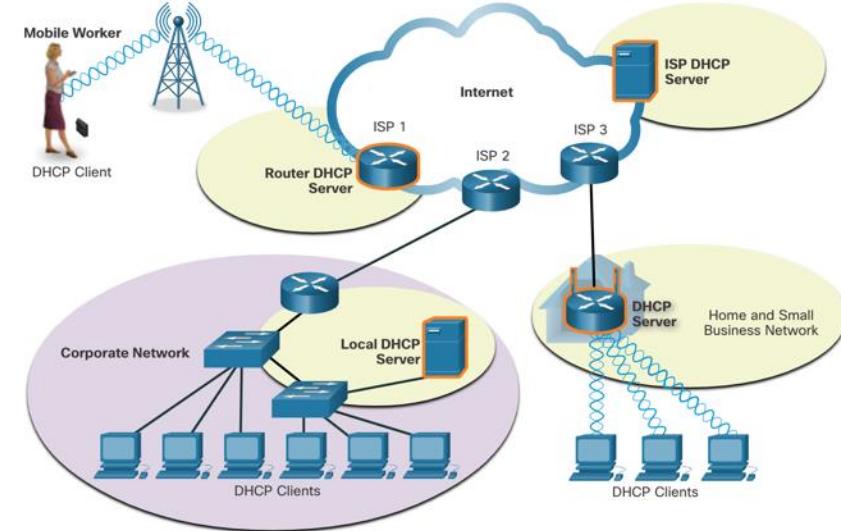
- **Nslookup**, bir kullanıcının belirli bir ana bilgisayar adını çözmek için cihazda yapılandırılmış DNS sunucularını manuel olarak sorgulamasına olanak tanıyan bir bilgisayar işletim sistemi yardımcı programıdır.
- **Bu yardımcı program**, ad çözümleme sorunlarını gidermek ve ad sunucularının mevcut durumunu doğrulamak için de kullanılabilir.
- Ne zaman **nslookup** komutu verilir, Barındırıcınıza yapılandırılmış varsayılan DNS sunucusu görüntülenir.
- Bir ana bilgisayarın veya etki alanının adı **nslookup** isteminde 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
>
```

# Dinamik Ana Bilgisayar Yapılandırma Protokolü

- IPv4 hizmeti için **Dinamik Ana Bilgisayar Yapılandırma Protokolü (DHCP)**, **IPv4 adreslerinin, alt ağ maskelerinin, ağ geçitlerinin ve diğer IPv4 ağ parametrelerinin atanmasını otomatikleştirir.**
- **DHCP**, statik adreslemeye kıyasla **dynamik adresleme olarak kabul edilir.**
- **Statik adresleme**, IP adresi bilgilerini **manuel olarak girmektir.**

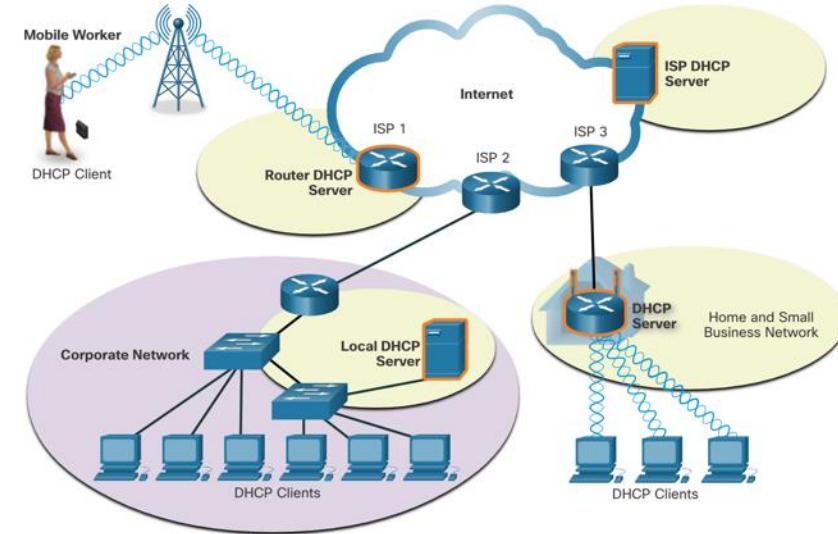


**Not:** IPv6 için DHCP (DHCPv6), IPv6 istemcileri için benzer hizmetler sağlar.

Ancak **DHCPv6**, varsayılan bir ağ geçidi adresi sağlanamaz. Bu, yalnızca yönlendiricinin **Yönlendirici Bildirisi** mesajından dinamik olarak elde edilebilir.

# Dinamik Ana Bilgisayar Yapılandırma Protokolü

- Bir ana bilgisayar ağa bağlandığında, DHCP sunucusuyla iletişim kurulur ve bir adres istenir.
- DHCP sunucusu, havuz adı verilen yapılandırılmış bir adres aralığından bir **adres seçer** ve bunu ana bilgisayara atar (**kiralas**).
- Birçok ağ hem **DHCP** hem de **statik adresleme** kullanır.
- **DHCP**, son kullanıcı cihazları gibi **genel amaçlı ana bilgisayarlar için kullanılır**.
- **Statik adresleme, ağ geçidi yönlendiricileri, anahtarlar, sunucular ve yazıcılar gibi ağ aygıtları için kullanılır**.

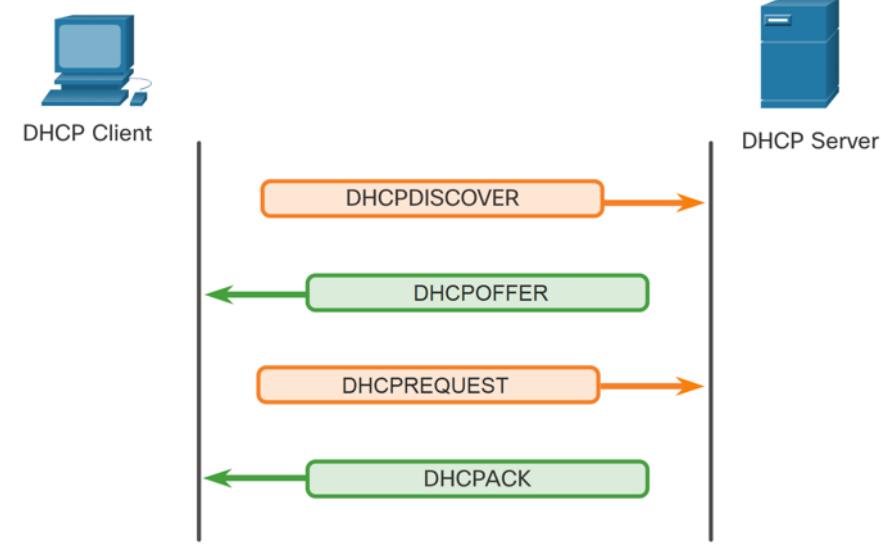


**Not:** IPv6 için DHCP (DHCPv6), IPv6 istemcileri için benzer hizmetler sağlar. Ancak DHCPv6, varsayılan bir ağ geçidi adresi sağlamaz. Bu, yalnızca yönlendiricinin Yönlendirici Bildirisi mesajından dinamik olarak elde edilebilir.

# DHCP İşlemleri

## DHCP Süreci:

- Bir IPv4, DHCP yapılandırmalı aygit başlatıldığında veya ağa bağlandığında, istemci ağdaki herhangi bir kullanılabilir.
- DHCP sunucusunu tanımlamak için bir **DHCP keşfetme** (DHCPDISCOVER) mesajı yayarlar.
- Bir **DHCP sunucusu**, istemciye kira sunan bir **DHCP teklifi** (DHCPOFFER) mesajıyla yanıt verir.
- (Bir istemci, ağdaki birden çok DHCP sunucusu nedeniyle **birden fazla teklif alırsa, birini seçmelidir.**)

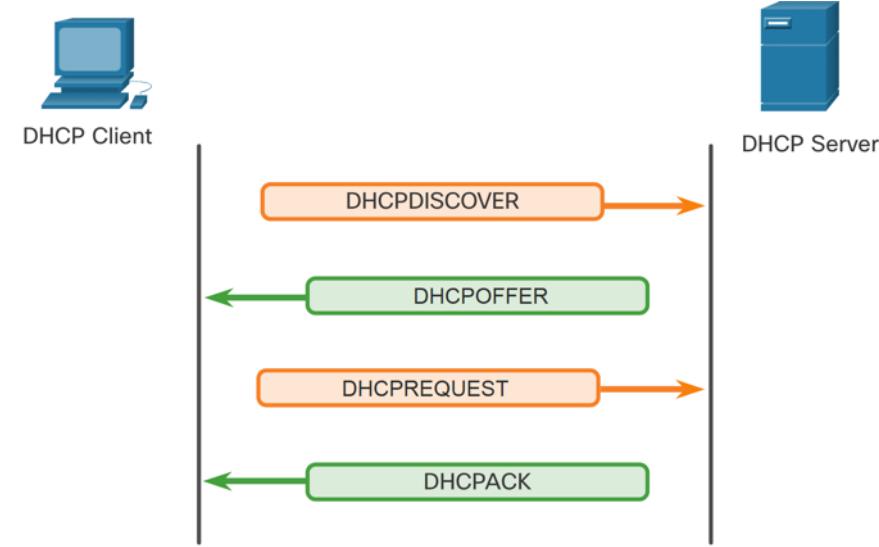


**Not:** DHCPv6, DHCPv4 için olanlara benzer bir dizi mesaja sahiptir. DHCPv6 mesajları SOLICIT, ADVERTISE, INFORMATION REQUEST ve REPLY şeklindedir.

# DHCP İşlemi

## DHCP Süreci:

- **İstemci**, açık sunucuyu ve istemcinin kabul ettiği kiralama teklifini tanımlayan bir **DHCP talebi** (DHCPREQUEST) mesajı gönderir.
- **Sunucu** daha sonra istemciye kiralama işleminin tamamlandığını bildiren bir **DHCP alındı bildirimi** (DHCPACK) mesajı döndürür.
- **Teklif artık geçerli değilse**, seçilen sunucu bir **DHCP negatif alındı** (DHCPNAK) mesajı ile **yanıt verir** ve **işlem** yeni bir **DHCPDISCOVER** mesajıyla başlamalıdır.



**Not:** DHCPv6, DHCPv4 için olanlara benzer bir dizi mesaja sahiptir. DHCPv6 mesajları SOLICIT, ADVERTISE, INFORMATION REQUEST ve REPLY şeklindedir.

# Lab –DNS Çözümlenmesi

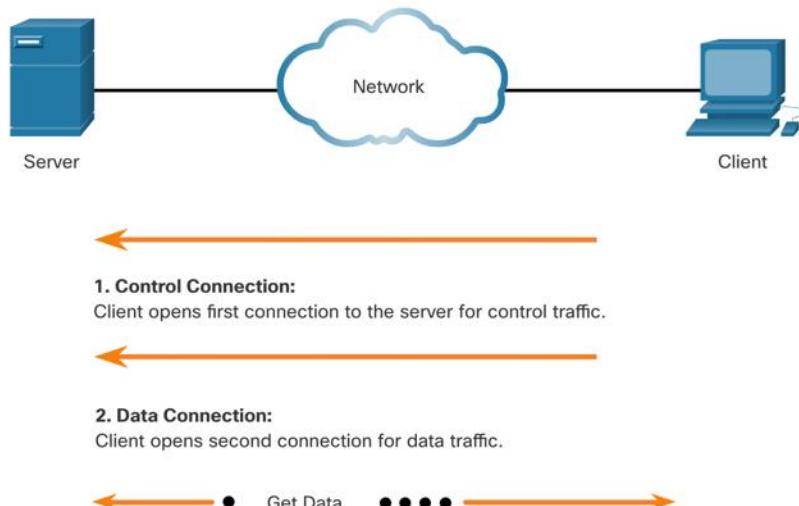
Bu laboratuvara aşağıdaki hedefleri tamamlarsınız:

- Bir URL'nin bir IP Adresine DNS Dönüşümünü Gözlemleyin
- Bir Web Sitesinde **nslookup** Komutunu Kullanarak DNS **Aramasını** Gözlemleyin
- Posta Sunucularında **nslookup** Komutunu Kullanarak DNS **Aramasını** Gözlemleyin

# 15.5 Dosya Paylaşım Servisleri

# Dosya Paylaşım Protokolü

- ❑ FTP, bir istemci ile bir sunucu arasında veri aktarımına izin vermek için geliştirilmiştir.
- ❑ Bir FTP istemcisi, bir FTP sunucusundan **veri çekmek** için kullanılan **bir bilgisayarda çalışan bir uygulamadır**.



**Adım 1 - İstemci, TCP bağlantı noktası 21'i kullanarak trafiği kontrol etmek için sunucuya ilk bağlantıyı kurar.**

Trafik, istemci komutlarından 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 olabilir.** İstemci sunucudan veri indirebilir (cekebilir) veya istemci verileri sunucuya yükleyebilir (itebilir).

## Sunucu Mesaj Bloğu

**Sunucu Mesaj Bloğu (SMB)** bir istemci / sunucu, istek-yanıt dosya paylaşım protokolüdür.

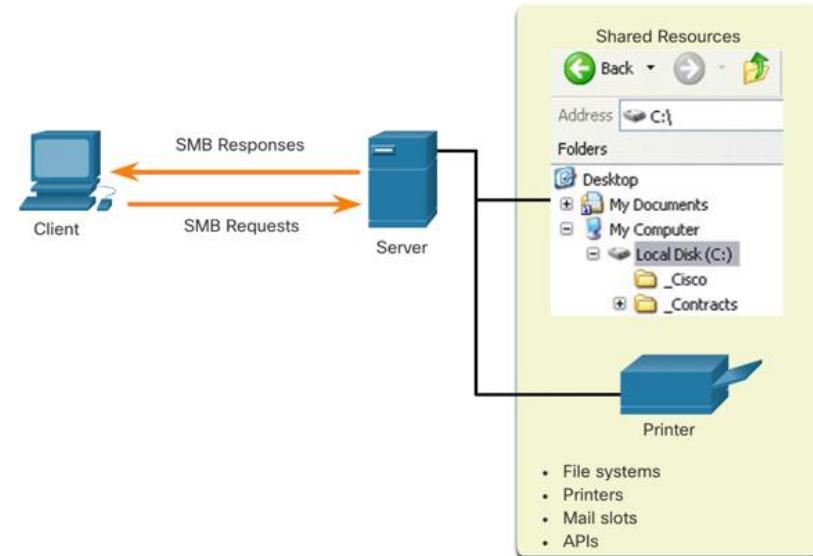
Sunucular, kendi kaynaklarını ağdaki istemcilerin kullanımına sunabilir.

- **SMB mesajlarının üç işlevi:**

- Oturumları başlatın, doğrulayın ve sonlandırın
- Dosya ve yazıcı erişimini kontrol edin
- Bir uygulamanın başka bir cihazdan mesaj gönderip almasına izin ver

- **FTP tarafından desteklenen dosya paylaşımının aksine**, istemciler sunuculara uzun vadeli bir bağlantı kurarlar.

- Bağlantı kurulduktan sonra, **istemcinin kullanıcısı**, sanki **kaynak istemci** ana bilgisayarına **yerelmiş gibidir** sunucudaki kaynaklara erişebilir.

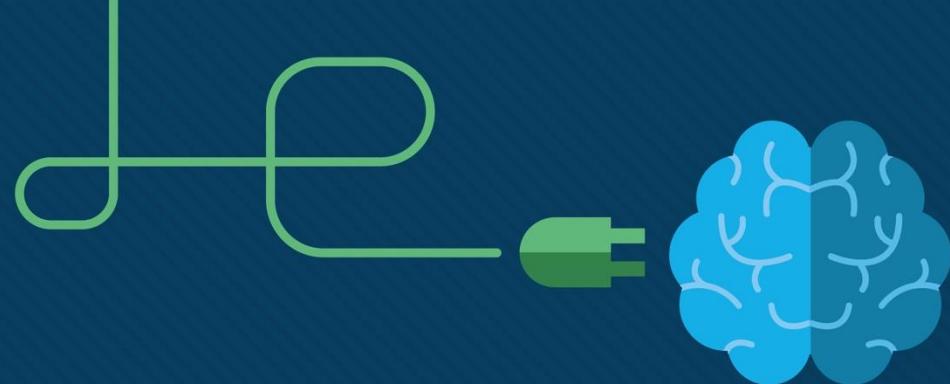


# 15.6 Modül Alıştırması ve Sınav

# Bu modülde ne öğrendim ?

- Uygulama katmanı protokollerini, kaynak ve hedef ana bilgisayarlarda çalışan programlar arasında veri alışverişini yapmak için kullanılır. Sunum katmanının üç temel işlevi vardır: verileri biçimlendirme veya sunma, verileri sıkıştırma ve aktarım için verileri şifreleme ve alındıktan sonra verilerin şifresini çözme. Oturum katmanı, kaynak ve hedef uygulamalar arasında diyaloglar oluşturur ve sürdürür.
- İstemci / sunucu modelinde bilgi talep eden cihaza istemci, talebe cevap veren cihaza ise sunucu adı verilir.
- Bir P2P ağında, iki veya daha fazla bilgisayar bir ağ üzerinden bağlanır ve özel bir sunucuya sahip olmadan kaynakları paylaşabilir.
- Üç yaygın HTTP mesaj türü GET, POST ve PUT'tur.
- E-posta, işlem için üç ayrı protokolü destekler: SMTP, POP ve IMAP.
- DNS protokolü, kaynak adlarını gerekli sayısal ağ adresiyle eşleştirir.
- IPv4 hizmeti için DHCP, IPv4 adreslerinin, alt ağ maskelerinin, ağ geçitlerinin ve diğer IPv4 ağ parametrelerinin atanmasını otomatikleştirir. DHCPv6 mesajları SOLICIT, ADVERTISE, INFORMATION REQUEST ve REPLY şeklindedir.
- Bir FTP istemcisi, bir FTP sunucusundan veri çekmek ve çekmek için kullanılan bir bilgisayarda çalışan bir uygulamadır.
- SMB mesajlarının üç işlevi: oturumları başlatma, doğrulama ve sonlandırma, dosya ve yazıcı erişimini kontrol etme ve bir uygulamanın başka bir cihaza veya cihazdan mesaj göndemesine veyamasına izin verme.





# Modül 16: Ağ Güvenliği Temelleri

Eğitmen Materyalleri

Ağlara Giriş v7.0 (ITN)



# Modül Hedefleri

**Modül Başlığı:** Ağ Güvenliği Temelleri

**Modül Amacı:** Güvenliği artırmak için aygit güçlendirme özellikleriyle anahtarları ve yönlendiricileri yapılandırma

Konu Başlığı	Amaç
Güvenlik Tehditleri ve Açıkları	Ağ cihazlarında neden temel güvenlik önlemlerinin gerekli olduğunu açıklama
Ağ Saldırıları	Güvenlik açıklarını belirleme
Ağ Saldırılarını Azaltma	Genel azaltma tekniklerini tanımlama
Cihaz Güvenliği	Güvenlik tehditlerini azaltmak için ağ aygitlarını aygit güçlendirme özellikleriyle yapılandırma

# 16.1 Güvenlik Tehditleri ve Açıkları

## Tehdit Türleri

- ❖ Bir ağa yapılan saldırılar yıkıcı olabilir ve önemli bilgi veya varlıkların hasar görmesi veya çalınması nedeniyle zaman ve para kaybına neden olabilir.
- ❖ İzinsiz girenler, yazılım güvenlik açıkları, donanım saldırıları veya birinin kullanıcı adı ve şifresini tahmin ederek bir ağa erişim sağlayabilir.
- ❖ Yazılımı değiştirerek veya yazılım güvenlik açıklarını kullanarak erişim elde eden davetsiz misafirlere tehdit aktörleri denir.

Tehdit aktörü ağa erişim kazandıktan sonra, dört tür tehdit ortaya çıkabilir:

- Bilgi Hırsızlığı
- Veri Kaybı ve manipülasyonu
- Kimlik Hırsızı
- Hizmet Kesintisi

## Açık Türleri

- Güvenlik açığı**, bir ağ veya cihazdaki zayıflık derecesidir.
- Yönlendiriciler, anahtarlar, masaüstleri, sunucular ve hatta **güvenlik cihazlarında** bir dereceye kadar **güvenlik açığı** vardır.
- Tipik olarak, saldırısı altındaki **ağ cihazları**, sunucular ve masaüstü **bilgisayarlar** gibi üç noktalardır.

**Üç temel güvenlik açığı veya zayıflık vardır:**

1. **Teknolojik Güvenlik Açıkları** arasında TCP / IP Protokolü zayıflıkları, İşletim Sistemi Zayıflıkları ve Ağ Ekipmanı zayıflıkları yer alabilir.

# Açık Türleri

**Üç temel güvenlik açığı veya zayıflık vardır:**

- 2. Yapılandırma Açıkları**, güvenli olmayan kullanıcı hesaplarını, kolayca tahmin edilebilen şifreli sistem hesaplarını, yanlış yapılandırılmış internet hizmetlerini, güvenli olmayan varsayılan ayarları ve yanlış yapılandırılmış ağ ekipmanını içerebilir.
- 3. Güvenlik Politikası Güvenlik Açıkları**, yazılı bir güvenlik politikasının eksikliğini, politikayı, kimlik doğrulama sürekliliğinin olmayışını, uygulanmayan mantıksal erişim kontrollerini, yazılım ve donanım kurulumunu ve politikayı takip etmeyen değişiklikleri ve var olmayan bir felaket kurtarma planını içerebilir.

Bu güvenlik açığı kaynaklarının üçü de bir ağı veya cihazı kötü niyetli kod saldıruları ve ağ saldıruları dahil olmak üzere çeşitli saldırılara açık bırakabilir.

# Fiziksel Güvenlik

**Ağ kaynakları fiziksel olarak tehlikeye atılabiliyorsa, bir tehdit aktörü ağ kaynaklarının kullanımını reddedebilir.**

**Dört fiziksel tehdit sınıfı aşağıdaki gibidir:**

- 1. Donanım tehditleri** - Bu, sunuculara, yönlendiricilere, anahtarlarla, kablolama tesisine ve iş istasyonlarına fiziksel hasarı içerir.
  - 2. Çevresel tehditler** - Bu, **aşırı sıcaklıklar** (çok sıcak veya çok soğuk) veya **aşırı nem** (çok ıslak veya çok kuru) içerir.
- ❖ Bu sorunları gidermek için **iyi bir fiziksel güvenlik planı oluşturulmalı ve uygulanmalıdır.**

## Fiziksel Güvenlik

Dört fiziksel tehdit sınıfı aşağıdaki gibidir:

3. **Elektriksel tehditler** - Buna **voltaj yükselmeleri**, **yetersiz besleme voltajı** (elektrik kesintileri), **koşulsuz güç** (gürültü) ve **toplam güç kaybı** dahildir.
4. **Bakım tehditleri** - Bu, temel elektrik bileşenlerinin kötü kullanımı (elektrostatik deşarj), **kritik yedek parça eksikliği**, **zayıf kablo bağlantısı** ve **kötü etiketlemeyi** içerir.

Bu sorunları gidermek için iyi bir fiziksel güvenlik planı oluşturulmalı ve uygulanmalıdır.

# 16.2 Ağ Saldırıları

# Keşif Saldırıları

❖ **Kötü amaçlı kod saldırılara ek olarak, ağların çeşitli ağ saldırılarına da kurban gitmesi mümkündür.**

❖ **Ağ saldırıları üç ana kategoriye ayrılabilir:**

- **Keşif saldırıları** - Sistemlerin, hizmetlerin veya güvenlik açıklarının keşfedilmesi ve haritalanması.
- **Erişim saldırıları** - Verilerin, sistem erişiminin veya kullanıcı ayrıcalıklarının yetkisiz manipülasyonu.
- **Hizmet reddi** - Ağların, sistemlerin veya hizmetlerin devre dışı bırakılması veya bozulması.

Keşif saldırıları için, dış tehdit aktörleri, belirli bir şirket veya varlığa atanan IP adres alanını kolayca belirlemek için **nslookup** ve **whois** yardımcı programları gibi internet araçlarını kullanabilir .

**IP adresi alanı belirlendikten sonra, bir tehdit aktörü, aktif olan adresleri belirlemek için herkese açık IP adreslerine ping atabilir.**



## Erişim Saldırıları

- ❖ **Erişim saldırıları**, web hesaplarına, gizli veritabanlarına ve diğer hassas bilgilere giriş sağlamak için kimlik doğrulama hizmetlerindeki,
- ❖ **FTP hizmetlerinde** ve **web hizmetlerindeki bilinen güvenlik açıklarından** yararlanır.

**Erişim saldırıları** dört türe ayrılabilir:

1. **Parola saldırıları** - Kaba kuvvet, truva atı ve paket algılayıcılar kullanılarak gerçekleştirilir
2. **Güven istismarı** - Bir tehdit aktörü, bir sisteme erişmek için yetkisiz ayrıcalıkları kullanır ve muhtemelen hedefi tehlikeye atar.

## Erişim Saldırıları

Erişim saldırıları dört türe ayrılabilir:

3. **Bağlantı noktası yeniden yönlendirme** : - Bir tehdit aktörü, diğer hedeflere yönelik saldırılar için **bir üs olarak güvenliği ihlal edilmiş bir sistemi kullanır.**

Örneğin, **güvenliği ihlal edilmiş** bir A ana bilgisayarına bağlanmak için **SSH**'yi (bağlantı noktası 22) kullanan **bir tehdit aktörü**, ana bilgisayar B'ye güvenir ve bu nedenle tehdit aktörü, ona erişmek için **Telnet (bağlantı noktası 23)** kullanabilir.

3. **Ortadaki Adam** - Tehdit aktörü, **iki taraf arasında geçen verileri okumak veya değiştirmek** için iki meşru varlık arasında konumlandırılır.

# Hizmet Reddi Saldırıları

**Hizmet reddi (DoS) saldırıları**, en çok duyurulan ve ortadan kaldırılması **en zor olan saldırı türüdür**.

Ancak, **uygulama kolaylıklarını** ve **potansiyel olarak önemli hasarları nedeniyle DoS saldırıları**, **güvenlik yöneticilerinin özel ilgisini hak eder**.

- **DoS saldırıları birçok biçimde olabilir.**
- Sonuçta yetkili kişilerin sistem kaynaklarını tüketerek bir hizmeti kullanmasını engellerler.
- DoS saldırılarını önlemeye yardımcı olmak için, **işletim sistemleri** ve uygulamalar için **en son güvenlik güncellemelerini takip etmek önemlidir.**

# Hizmet Reddi Saldırıları

- ❖ **DoS saldırısı**, 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.
- ❖ **DDoS**, DoS saldırısına benzer, ancak birden çok, koordineli kaynaklardan kaynaklanır.
- Örneğin, bir tehdit aktörü, **zombiler olarak bilinen virüslü ana bilgisayarlardan oluşan bir ağ oluşturur**.
- Bir zombi ağına botnet denir.
- **Tehdit aktörü**, zombilerin botnet'ine **DDoS saldırısı gerçekleştirmeye talimatı vermek** için bir komut ve kontrol (CnC) programı kullanır.

# Lab – Araştırma Ağı Güvenliği Tehditleri

Bu laboratuvara aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: SANS Web Sitesini Keşfedin
- Bölüm 2: Son Ağ Güvenliği Tehditlerini Belirleyin
- Bölüm 3: Belirli Bir Ağ Güvenlik Tehdidini Ayrıntılandırın

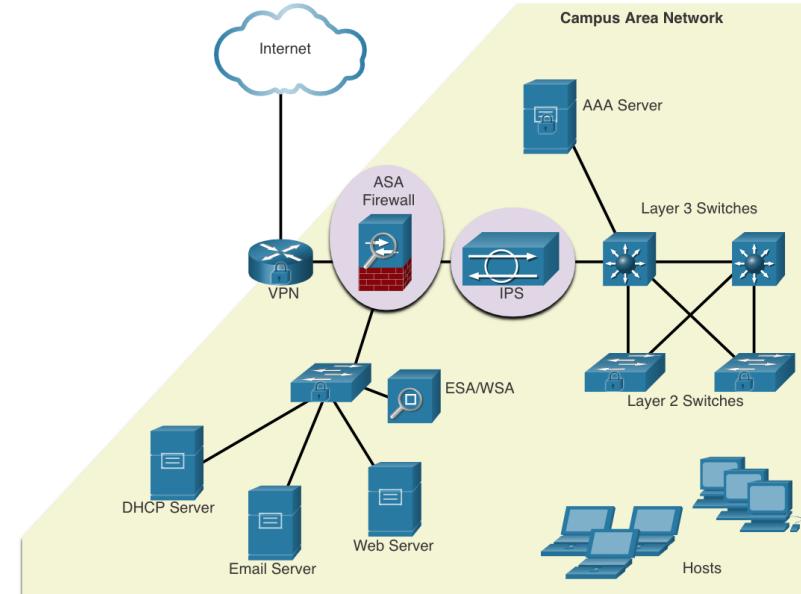
# 16.3 Ağ Saldırısının Azaltılması

# Derinlemesine Savunma Yaklaşımı

- ☐ Ağ saldırınızı azaltmak için önce yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar dahil cihazları **güvenli hale getirmelisiniz.**
- ☐ Çoğu kuruluş, güvenlik için derinlemesine savunma yaklaşımı (**katmanlı yaklaşım olarak da bilinir**) kullanır.
- ☐ Bu, birlikte çalışan ağ aygıtları ve hizmetlerinin bir kombinasyonunu gerektirir.

Bir kuruluşun kullanıcılarını ve varlıklarını TCP / IP tehditlerine karşı korumak için **çeşitli güvenlik cihazları ve hizmetleri uygulanır:**

- VPN
- ASA Güvenlik Duvarı
- IPS
- ESA / WSA
- AAA Sunucusu



# Ağ Saldırısı Azaltılması Yedek Tutma

- ❖ **Aygıt yapılandırmalarını ve verileri yedeklemek**, veri kaybına karşı korumanın en etkili yollarından biridir.
- ❖ **Yedeklemeler, güvenlik politikasında belirtildiği gibi düzenli olarak yapılmalıdır.**
- ❖ **Veri yedeklemeleri**, ana tesise herhangi bir şey olması durumunda **yedekleme ortamını korumak için genellikle iş yeri dışında depolanır**.

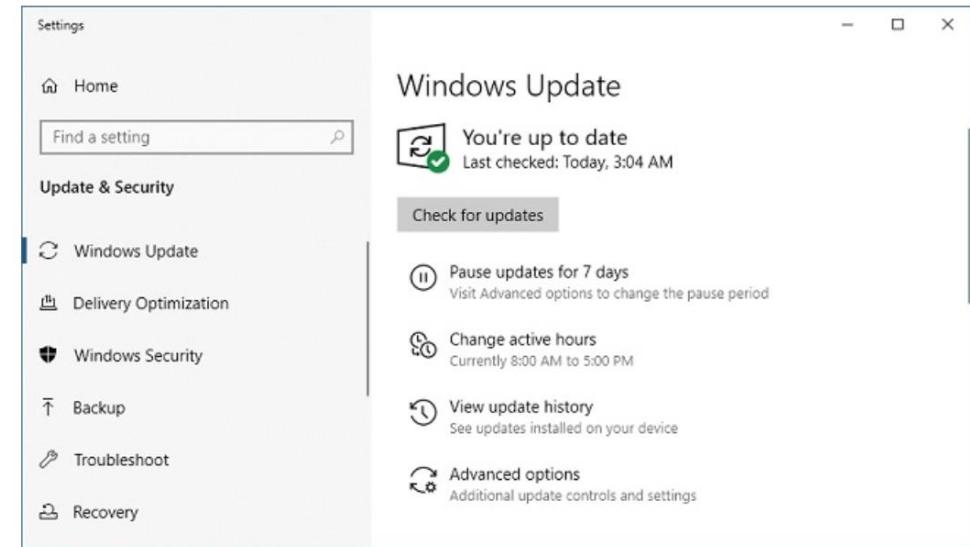
Tablo, yedeklemeyle ilgili konuları ve açıklamalarını gösterir.

Düşünce	Açıklama
Sıklık	<ul style="list-style-type: none"><li>Güvenlik politikasında belirtildiği gibi, düzenli olarak yedekleme yapın.</li><li>Tam yedeklemeler zaman alıcı olabilir, bu nedenle değiştirilen dosyaların sık sık kısmı yedeklenmesiyle aylık veya haftalık yedeklemeler gerçekleştirin.</li></ul>
Depolama	<ul style="list-style-type: none"><li>Verilerin bütünlüğünü sağlamak ve dosya geri yükleme prosedürlerini doğrulamak için her zaman yedekleri doğrulayın.</li></ul>
Güvenlik	<ul style="list-style-type: none"><li><b>Yedekler</b>, güvenlik politikasının gerektirdiği şekilde <b>günlük, haftalık veya aylık rotasyonla</b> onaylanmış bir saha dışı depolama konumuna taşınmalıdır.</li></ul>
Doğrulama	<ul style="list-style-type: none"><li>Yedeklemeler <b>güçlü parolalar kullanılarak korunmalıdır</b>. Verileri geri yüklemek için parola gereklidir.</li></ul>

# Yükseltme, Güncelleme ve Yama

Yeni kötü amaçlı yazılım piyasaya sürüldüğünde, işletmelerin antivirüs yazılımının en son sürümlerini güncel tutması gereklidir.

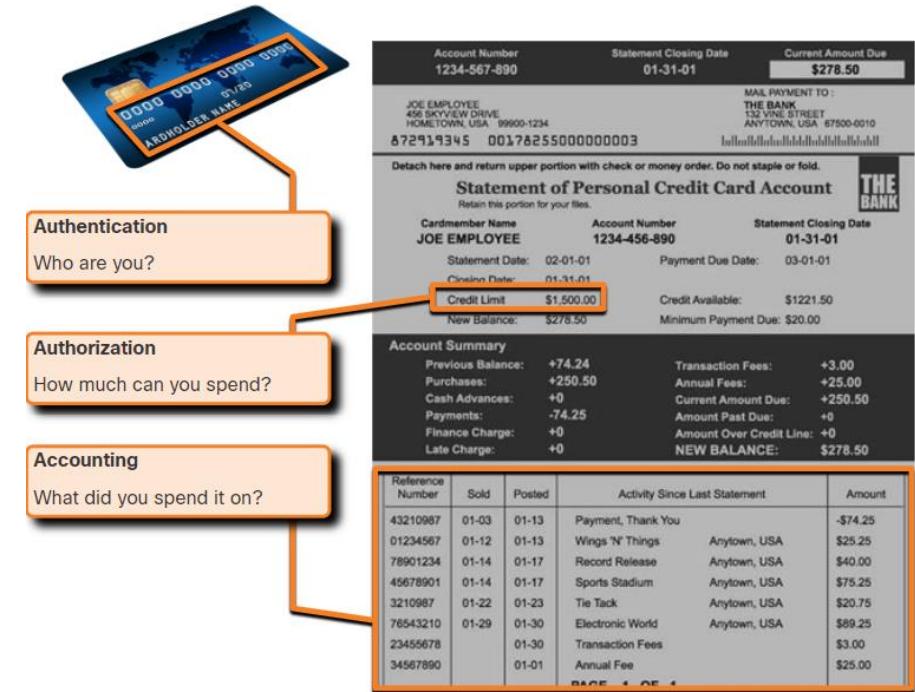
- Bir solucan saldırısını azaltmanın en etkili yolu, işletim sistemi satıcısından güvenlik güncellemelerini indirmek ve tüm savunmasız sistemleri yamamaktır.
- Kritik güvenlik yamalarının yönetimine yönelik bir çözüm, tüm üç sistemlerin güncellemeleri otomatik olarak indirmesini sağlamaktır.



## Kimlik Doğrulama, Yetkilendirme ve Hesap Oluşturma

**Kimlik doğrulama, yetkilendirme ve hesaplama (AAA veya "üçlü A") ağ güvenliği hizmetleri, ağ cihazlarında erişim denetimini kurmak için birincil çerçeveyi sağlar.**

- AAA, bir ağa kimlerin erişmesine izin verildiğini (kimlik doğrulama), ağa erişirken hangi eylemleri gerçekleştirdiklerini (yetkilendirme) ve oradayken yapılanların kaydını tutmanın (hesap oluşturma) bir yoludur.**
- AAA kavramı, kredi kartı kullanımına benzer.**
- Kredi kartı, onu kimin kullanabileceğini, bu kullanıcının ne kadar harcayabileceğini tanımlar ve kullanıcının para harcadığı kalemlerin hesabını tutar.



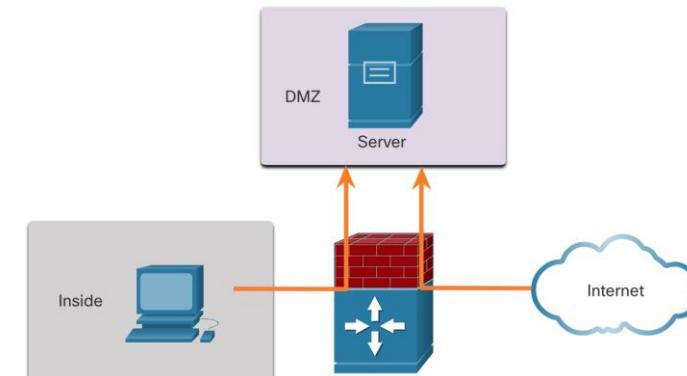
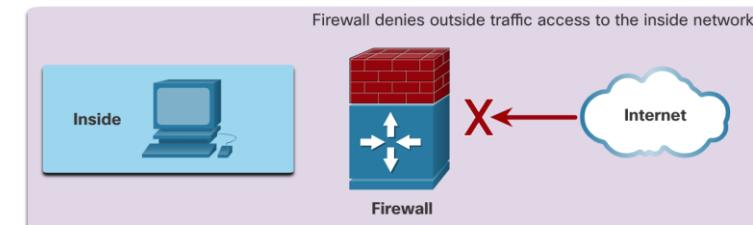
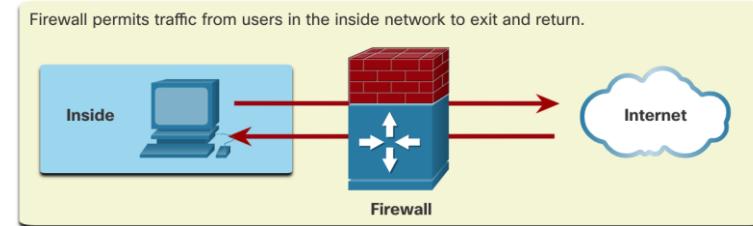
# Ağ Saldırısı Azaltılması Güvenlik Duvarı

- ☐ Ağ güvenlik duvarları iki veya daha fazla ağ arasında bulunur, aralarındaki trafiği kontrol eder ve yetkisiz erişimi önlemeye yardımcı olur.

Bir güvenlik duvari, dış kullanıcıların belirli hizmetlere kontrollü erişime izin verebilir.

Örneğin, dış kullanıcılar tarafından erişilebilen sunucular genellikle askerden arındırılmış bölge (DMZ) olarak adlandırılan özel bir ağa bulunur.

DMZ, bir ağ yöneticisinin o ağa bağlı ana bilgisayarlar için belirli ilkeler uygulamasını sağlar.



# Güvenlik Duvarı Türleri

Güvenlik duvari ürünleri çeşitli biçimlerde paketlenmiştir.

Bu ürünler, bir ağa neyin erişime izin verileceğini veya reddedileceğini belirlemek için farklı teknikler kullanır.

Aşağıdakileri içerir:

- **Paket filtreleme** - IP veya **MAC** adreslerine göre **erişimi engeller** veya **erişime izin verir**
- **Uygulama filtreleme** - Bağlantı noktası numaralarına göre belirli **uygulama türlerine** göre erişimi **engeller** veya buna izin verir
- **URL filtreleme** - Belirli URL'lere veya anahtar kelimelere göre **web sitelerine erişimi engeller** veya bunlara **izin verir**
- **Durum bilgili paket incelemesi (SPI)** - **Gelen paketler**, dahili ana bilgisayarlardan gelen isteklere verilen **meşru yanıtlar olmalıdır**. Özel olarak **izin verilmeyen**, **istenmeyen** paketler **engellenir**. SPI ayrıca hizmet redi (DoS) gibi belirli saldırı türlerini tanıma ve filtreleme yeteneğini de içerebilir.

# Ağ Saldırısı Azaltılması Uç Nokta Güvenliği

Bir uç nokta veya **ana bilgisayar**, bir ağ istemcisi olarak **işlev gören bağımsız bir bilgisayar sistemi** veya **cihazdır**.

Yaygın uç noktalar **dizüstü bilgisayarlar**, **masaüstü bilgisayarlar**, **sunucular**, **akıllı telefonlar** ve **tabletlerdir**.

**Uç nokta cihazlarının güvenliğini sağlamak**, insan doğasını içerdiği için bir **ağ yöneticisinin en zorlu görevlerinden biridir**.

Bir şirketin iyi belgelenmiş politikaları olmalıdır ve çalışanlar bu kuralların farkında olmalıdır.

**Çalışanların ağın doğru kullanımı konusunda eğitilmesi gereklidir**. Politikalar genellikle antivirüs yazılımının kullanımını ve ana bilgisayar izinsiz giriş önleme kullanımını içerir. Daha kapsamlı uç nokta güvenlik çözümleri, ağ erişim kontrolüne dayanır.

# 16.4 Cihaz Güvenliği

- ❖ Bir cihaza yeni bir işletim sistemi yüklendiğinde, **güvenlik ayarları varsayılan değerlere ayarlanır.**
- ❖ Çoğu durumda, bu güvenlik seviyesi yetersizdir. Cisco yönlendiricileri için, **Cisco AutoSecure** özelliği sistemin güvenliğini sağlamaya yardımcı olmak için kullanılabilir.

**Ek olarak, çoğu işletim sistemi için geçerli olan bazı basit adımlar vardır:**

- Varsayılan kullanıcı adları ve şifreler derhal değiştirilmelidir.
- Sistem kaynaklarına erişim, yalnızca bu kaynakları kullanmaya yetkili kişilerle sınırlanmalıdır.
- Gereksiz hizmetler ve uygulamalar mümkün olduğunda kapatılmalı ve kaldırılmalıdır.
- Genellikle, üretilen sevk edilen cihazlar bir süredir bir depoda durmaktadır ve en güncel yama

# Şifreler

Ağ cihazlarını korumak için güçlü şifreler kullanmak önemlidir. İşte uyulması gereken standart kurallar:

- En az sekiz karakter uzunluğunda, **tercihen 10** veya daha fazla karakter **uzunluğunda bir şifre kullanın.**
- **Parolaları karmaşık hale getirin.** İzin veriliyorsa, büyük ve küçük harflerin, sayıların, sembollerin ve boşlukların karışımını ekleyin.
- **Tekrarlara, yaygın sözlük kelimelerine,** harf veya sayı dizilerine, kullanıcı adlarına, akraba veya evcil hayvan00 adlarına, doğum tarihleri gibi biyografik bilgilere, kimlik numaralarına, ata adlarına veya diğer kolayca tanımlanabilen bilgilere dayanan şifrelerden kaçının.

# Şifreler

- Parolayı kasıtlı olarak yanlış yazın. Örneğin, Smith = Smyth = 5mYth veya Security = 5ecur1ty.
- **Parolaları sık sık değiştirin.** Bir parola bilinmeden tehlikeye atılırsa, tehdit aktörünün parolayı kullanması için fırsat penceresi sınırlanır.
- **Parolaları bir yere yazmayın ve masa veya monitör gibi görünür yerlerde bırakmayın.**

**Cisco yönlendiricilerinde**, parolalar için **baştaki boşluklar yok sayılır**, ancak **ilk karakterden sonraki boşluklar göz ardı edilir**.

Bu nedenle, güçlü bir parola oluşturmanın bir yolu, boşluk çubuğu kullanmak ve **birçok sözcükten oluşan bir ifade oluşturmaktır**. Buna parola denir.

Bir parolayı hatırlamak genellikle basit bir paroladan daha kolaydır. Aynı zamanda daha uzun ve tahmin edilmesi daha zor.

# Ek Şifre Güvenliği

Parolaların bir **Cisco yönlendirici** ve anahtar üzerinde gizli kalmasını sağlamak yardımcı olmak için atılabilecek birkaç adım vardır:

- Tüm düz metin parolalarını **hizmet parolası şifreleme** komutuyla **şifreleyin**.
- **Güvenlik parolaları minimum uzunluk** komutuyla kabul edilebilir bir minimum parola uzunluğu belirleyin.
- İle kaba kuvvet şifre tahmin saldıruları caydırırmak **giriş bloğu** için # girişimi # içinde # komutu.
- **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#
```

## SSH'i Etkinleştir

Aşağıdaki adımları kullanarak bir Cisco cihazını SSH'yi destekleyecek şekilde yapılandırmak mümkündür:

**Benzersiz bir cihaz ana bilgisayar adı yapılandırın**. Bir cihazın varsayıldan farklı bir benzersiz ana bilgisayar adı olmalıdır.

**IP alan adını yapılandırın**. Genel yapılandırma modu komutu **ip-etki alanı adını** kullanarak ağın IP etki alanı adını yapılandırın .

**SSH trafiğini şifrelemek için bir anahtar oluşturun** . **SSH, kaynak ve hedef arasındaki trafiği şifreler**. Bununla birlikte, bunu yapmak için, küresel yapılandırma komutu kullanılarak benzersiz bir kimlik doğrulama anahtarı, **rsa genel anahtar modülü bitleri oluşturan kripto anahtarı üretilmelidir** . Modül **bitleri** , anahtarın boyutunu belirler ve **360** bit ila **2048** bit arasında yapılandırılabilir. Bit değeri ne kadar büyükse, anahtar o kadar güvenli olur. **Ancak, daha büyük bit değerlerinin de bilgileri şifrelemesi ve şifresini çözmeye daha uzun süre**. **Önerilen minimum modül uzunluğu 1024** bittir.



## SSH'i Etkinleştir

Aşağıdaki adımları kullanarak bir Cisco cihazını SSH'yi destekleyecek şekilde yapılandırmak mümkündür:

**Yerel bir veritabanı girişini doğrulayın veya oluşturun .**

Kullanıcı **adı** genel yapılandırma komutunu kullanarak yerel bir veritabanı kullanıcı adı girişini oluşturun .

**Yerel veritabanına göre kimlik doğrulaması yapın .** Yerel veritabanına göre **vty** satırının kimliğini doğrulamak için **oturum açma yerel** hat yapılandırma komutunu kullanın.

**Vty gelen SSH oturumlarını etkinleştirin .** Varsayılan olarak, vty hatlarında hiçbir giriş oturumuna izin verilmez. **[Ssh | taşıma girdisini** kullanarak Telnet ve SSH dahil olmak üzere birden çok girdi protokolü belirtebilirsiniz. **telnet]** komutu.

## Kullanılmayan Hizmetleri Devre Dışı Bırak

**Cisco yönlendiricileri ve anahtarları, ağıınızda 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 istismar etmesini önleyin.**

Varsayılan olarak açık olan hizmetlerin türü, **IOS sürümüne bağlı olarak değişecektir**. Örneğin, IOS-XE'de tipik olarak yalnızca **HTTPS** ve **DHCP bağlantı noktaları açık olacaktır**.

Bunu **show ip ports all** komutu ile doğrulayabilirsiniz .

IOS-XE'den önceki IOS sürümleri **show control-plane host open-ports** komutunu kullanır.

# Paket Tracer –Güvenli Şifreleri ve SSH'yi Yapılandırın

Bu Paket İzleyicide, şifreleri ve SSH'yi yapılandıracaksınız:

- Ağ yöneticisi sizden RTA ve SW1'i dağıtım için hazırlamanızı istedİ. Ağa bağlanmadan önce güvenlik önlemlerinin etkinleştirilmesi gereklİ.

# Lab – Ağ Aygıtlarını SSH ile Yapılandırma

Bu laboratuvara aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Temel Aygit Ayarlarını Yapılandırma
- Bölüm 2: Yönlendiriciyi SSH Erişimi için Yapılandırma
- Bölüm 3: Anahtarı SSH Erişimi için Yapılandırma
- Bölüm 4: Anahtardaki CLI'den SSH

# 16.5 Alıştırmalar ve Sınav

# Paket Tracer – Güvenli Ağ Cihazları

Bu aktivitede, gereksinimler listesine göre bir yönlendirici ve bir anahtar yapılandıracaksınız.

# Lab – Güvenli Ağ Cihazları

- Bu laboratuvara aşağıdaki hedefleri tamamlayacaksınız:
- Temel Cihaz Ayarlarını Yapılandırın
- Yönlendiricide Temel Güvenlik Önlemlerini Yapılandırın
- Anahtarda Temel Güvenlik Önlemlerini Yapılandırın

# Bu modülde ne öğrendim ?

- Tehdit aktörü ağa erişim kazandıktan sonra dört tür tehdit ortaya çıkabilir: bilgi hırsızlığı, veri kaybı ve manipülasyon, kimlik hırsızlığı ve hizmet kesintisi.
- Üç temel güvenlik açığı veya zayıflık vardır: teknolojik, yapılandırma ve güvenlik politikası.
- Dört fiziksel tehdit sınıfı şunlardır: donanım, çevre, elektrik ve bakım.
- Kötü amaçlı yazılım, kötü amaçlı yazılımın kısaltmasıdır. Verilere, ana bilgisayarlara veya aklara zarar vermek, bozmak, çalmak veya "kötü" veya yasadışı eylemde bulunmak için özel olarak tasarlanmış kod veya yazılımdır. Virüsler, solucanlar ve Truva atları kötü amaçlı yazılım türleridir.
- Ağ saldırıları üç ana kategoriye ayrılabilir: keşif, erişim ve hizmet reddi.
- Ağ saldırılarını azaltmak için önce yönlendiriciler, anahtarlar, sunucular ve ana bilgisayarlar dahil cihazları güvenli hale getirmelisiniz. Çoğu kuruluş, güvenlik için derinlemesine bir savunma yaklaşımı kullanır. Bu, birlikte çalışan ağ aygıtları ve hizmetlerinin bir kombinasyonunu gerektirir.
- Bir kuruluşun kullanıcılarını ve varlıklarını TCP / IP tehditlerine karşı korumak için çeşitli güvenlik cihazları ve hizmetleri uygulanır: VPN, ASA güvenlik duvarı, IPS, ESA / WSA ve AAA sunucusu.

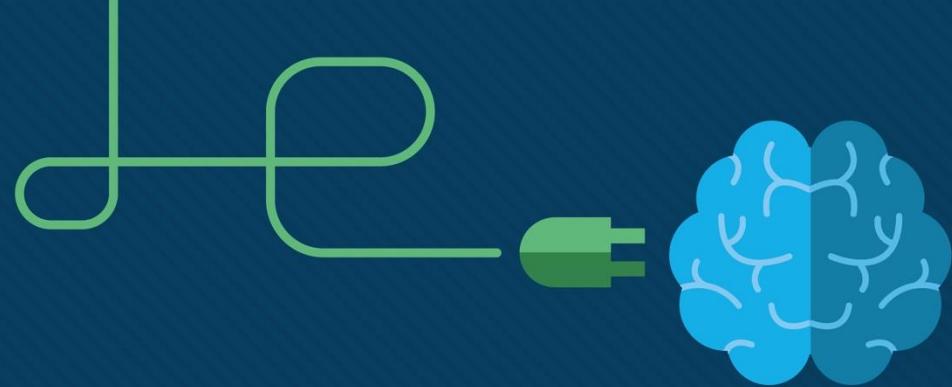
## Bu modülde ne öğrendim ?

- Altyapı cihazlarının, bir FTP veya benzer dosya sunucusunda yapılandırma dosyalarının ve IOS görüntülerinin yedekleri olmalıdır. Bilgisayar veya yönlendirici donanımı arızalanırsa, veriler veya yapılandırma yedek kopya kullanılarak geri yüklenebilir.
- Bir solucan saldırısını azaltmanın en etkili yolu, işletim sistemi satıcısından güvenlik güncellemelerini indirmek ve tüm savunmasız sistemleri yamamaktır. Kritik güvenlik yamalarını yönetmek, tüm uç sistemlerin güncellemeleri otomatik olarak indirdiğinden emin olmak için.
- AAA, bir ağa kimlerin erişmesine izin verildiğini (kimlik doğrulama), oradayken ne yapabileceklerini (yetkilendirme) ve ağa erişirken (hesaplama) hangi eylemleri gerçekleştirdiklerini kontrol etmenin bir yoludur.
- Ağ güvenlik duvarları iki veya daha fazla ağ arasında bulunur, aralarındaki trafiği kontrol eder ve yetkisiz erişimi önlemeye yardımcı olur.
- Uç nokta cihazlarının güvenliğini sağlamak, ağ güvenliği için çok önemlidir. Bir şirketin, antivirüs yazılımının kullanımı ve ana bilgisayar izinsiz giriş önleme gibi iyi belgelenmiş ilkeleri olmalıdır. Daha kapsamlı uç nokta güvenlik çözümleri, ağ erişim kontrolüne dayanır.

# Bu modülde ne öğrendim ?

- Cisco yönlendiricileri için, Cisco AutoSecure özelliği sistemin güvenliğini sağlamaya yardımcı olmak için kullanılabilir. Çoğu işletim sistemi için varsayılan kullanıcı adları ve parolalar derhal değiştirilmeli, sistem kaynaklarına erişim yalnızca bu kaynakları kullanma yetkisine sahip kişilerle sınırlanmalıdır ve mümkün olduğunda gereksiz hizmetler ve uygulamalar kapatılmalı ve kaldırılmalıdır.
- Ağ cihazlarını korumak için güçlü şifreler kullanmak önemlidir. Bir parolayı hatırlamak genellikle basit bir paroladan daha kolaydır. Aynı zamanda daha uzun ve tahmin edilmesi daha zor.
- Yönlendiriciler ve anahtarlar için, tüm düz metin parolalarını şifreleyin, minimum kabul edilebilir bir parola uzunluğu belirleyin, kaba kuvvet parola tahmin saldırılarını engelleyin ve belirli bir süre sonra etkin olmayan ayrıcalıklı bir EXEC modu erişimini devre dışı bırakın.
- SSH'yi desteklemek için uygun cihazları yapılandırın ve kullanılmayan hizmetleri devre dışı bırakın.





# Modül 17: Küçük Bir Ağ Oluşturun

Eğitmen Materyalleri

Ağlara Giriş v7.0 (ITN)



# Modül Hedefleri

**Modü Başlığı:** Küçük Bir Ağ Oluşturun

**Modül Amacı :** Küçük bir ağ için bir yönlendirici, bir anahtar ve üç cihazlar içeren bir ağ tasarımları uygulanması

Konu Başlığı	Amaç
<b>Küçük Bir Ağdaki Cihazlar</b>	Küçük bir ağda kullanılan cihazları tanımlama
<b>Küçük Ağ Uygulamaları ve Protokollerı</b>	Küçük bir ağda kullanılan uygulamaları ve protokollerini tanımlama
<b>Daha Büyük Ağlara Ölçeklendirme</b>	Küçük bir ağın daha büyük ağların temeli olarak nasıl hizmet ettiğinin açıklanması
<b>Bağlantıyı Doğrulama</b>	Bağlantıyı doğrulamak ve göreli ağ performansı oluşturmak için ping ve traceret komutlarının çıktısını kullanma
<b>Host ve IOS Komutları</b>	Bir ağdaki cihazlar hakkında bilgi almak için ana bilgisayar ve IOS komutlarını kullanın
<b>Sorun Giderme Metodojileri</b>	Yaygın sorun giderme metodojilerinin tanımlanması
<b>Sorun Giderme Senaryoları</b>	Ağdaki cihazlar ile ilgili sorunları giderme

# 17.1 Küçük Bir Ağdaki Cihazlar

## Küçük Ağ Topolojileri

- İşletmelerin çoğu küçüktür, iş ağlarının çoğu da küçüktür.
- Küçük bir ağ tasarımı genellikle basittir.
- Küçük ağlar tipik olarak DSL, kablo veya Ethernet bağlantısıyla sağlanan tek bir WAN bağlantısına sahiptir.
- **Büyük ağlar, ağ cihazlarının bakımı, güvenliği ve sorunlarını gidermek ve kurumsal verileri korumak** için bir BT departmanı gerektirir.
- **Küçük ağlar, yerel bir BT teknisyeni veya sözleşmeli bir profesyonel tarafından yönetilir.**

## Küçük Ağlar İçin Cihaz Seçimi

Büyük ağlar gibi, küçük ağlar da **kullanıcı gereksinimlerini karşılamak için planlama ve tasarım gerektirir.**

Planlama, tüm gereksinimlerin, **maliyet faktörlerinin** ve dağıtım seçeneklerinin gereken şekilde dikkate alınmasını sağlar.

İlk tasarım değerlendirmelerinden biri, **ağı desteklemek için kullanılacak ara cihazların türündür.**

Ağ cihazlarını seçerken dikkate alınması gereken faktörler şunları içerir:

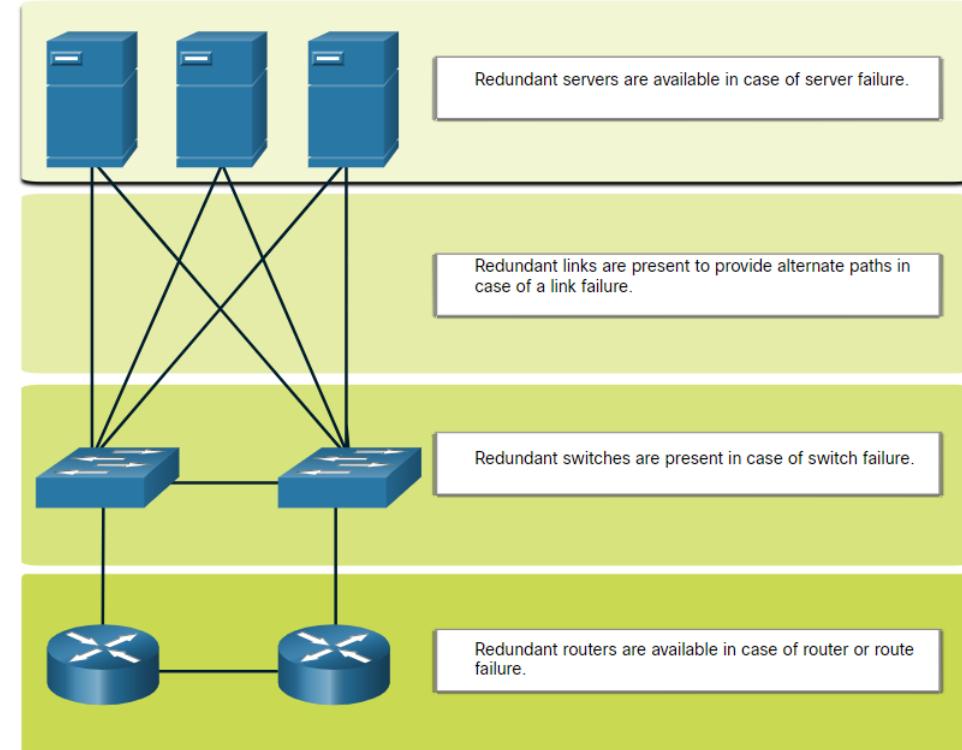
- **Maliyet**
- **Hız ve bağlantı noktası / arabirim türleri**
- **Genişletilebilirlik**
- **İşletim sistemi özellikleri ve hizmetleri**

# Küçük Ağlar İçin IP Adresleri

- ❖ Bir ağ uygularken, bir IP adresleme şeması oluşturun ve kullanın.
- ❖ Bir ağ ağı içindeki **tüm ana bilgisayarlar ve cihazlar benzersiz bir adrese sahip olmalıdır.**
- ❖ IP adresleme şemasını hesaba katacak cihazlar şunları içerir:
  - Son kullanıcı cihazları - Bağlantıların sayısı ve türü (ör. Kablolu, kablosuz, uzaktan erişim)
  - Sunucular ve çevre birimleri aygıtları (ör. Yazıcılar ve güvenlik kameraları)
  - Anahtarlar ve erişim noktaları dahil aracı cihazlar
- ❖ Cihaz türüne göre bir **IP adresleme şeması planlamamanız, belgelemeniz ve sürdürmeniz önerilir.**
- ❖ Planlanmış bir **IP adresleme şemasının kullanılması, bir cihaz türünü tanımlamayı ve sorunları gidermeyi kolaylaştırır.**

# Küçük Ağlarda Yedeklilik

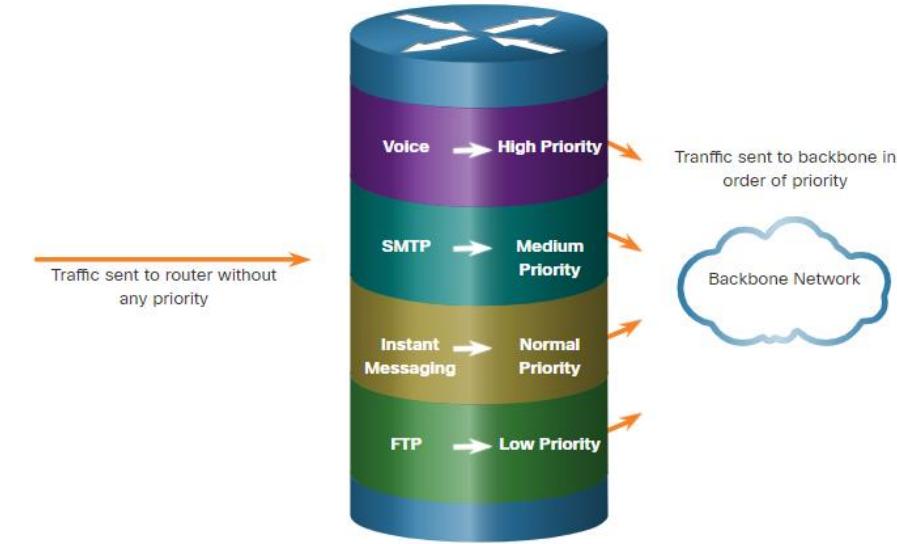
- Yüksek derecede güvenilirlik sağlamak için ağ tasarımında **yedeklilik** gereklidir.
- Yedeklilik, tek hata noktalarını ortadan kaldırılmaya yardımcı olur.
- **Yedekleme, yinelenen ekipmanı kurarak gerçekleştirilebilir.**
- Kritik alanlar için yinelenen ağ bağlantıları sağlayarak da gerçekleştirilebilir.



# Küçük Bir Ağdaki Cihazlar

## Trafik Yönetimi

- ❖ İyi bir ağ tasarımının amacı, çalışanların üretkenliğini 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 kuyruğunun dört kuyruğu vardır. Yüksek öncelikli kuyruk her zaman önce boşaltılır.



# 17.2 Küçük Ağ Uygulamalar ve Protokoller

# Küçük Ağ Uygulamalar ve Protokoller

## Genel Uygulamalar

- ❖ Kurulumunu yaptıktan sonra, ağınızın çalışması için hala belirli türden uygulamalara ve protokollere ihtiyacı vardır.
- ❖ Ağ, yalnızca üzerinde bulunan uygulamalar kadar kullanılmalıdır.

**Ağa erişim sağlayan iki tür yazılım programı veya işlemi vardır:**

- **Ağ Uygulamaları** : Uygulama katmanı protokollerini uygulayan ve protokol yığınının alt katmanlarıyla doğrudan iletişim kurabilen uygulamalar.
- **Uygulama Katmanı Hizmetleri** : Ağa duyarlı olmayan uygulamalar için, ağ ile arabirim oluşturan ve verileri aktarım için hazırlayan programlar.

## Genel Protokoller

**Ağ protokolleri**, çalışanlar tarafından **küçük bir ağda kullanılan uygulamaları ve hizmetleri destekler.**

- Ağ yöneticileri genellikle **ağ cihazlarına ve sunuculara erişim gerektirir**.
- En yaygın iki uzaktan erişim çözümü **Telnet** ve **Güvenli Kabuk**'tur (**SSH**).
- Hypertext Transfer Protocol (**HTTP**) ve Hypertext Transfer Protocol Secure (**HTTPS**), **web istemcileri** ve **web sunucuları** arasında kullanılır.
- Basit Posta Aktarım Protokolü (**SMTP**) e-posta göndermek için kullanılır, Postane Protokolü (**POP3**) veya İnternet Posta Erişim Protokolü (**IMAP**) istemciler tarafından e-posta almak için kullanılır.

# Küçük Ağ Uygulamalar ve Protokoller

## Genel Protokoller

Ağ protokolleri, çalışanlar tarafından küçük bir ağda kullanılan uygulamaları ve hizmetleri destekler.

- Dosya Aktarım Protokolü (**FTP**) ve Güvenlik Dosya Aktarım Protokolü (**SFTP**), bir istemci ile bir FTP sunucusu arasında dosya indirmek ve yüklemek için kullanılır.
- Dinamik Ana Bilgisayar Yapılandırma Protokolü (**DHCP**), istemciler tarafından bir DHCP Sunucusundan bir IP yapılandırması almak için kullanılır.
- Alan Adı Hizmeti (**DNS**), alan adlarını IP adreslerine çözümler.

**Not :** Bir sunucu birden çok ağ hizmeti sağlayabilir.

Örneğin, bir sunucu bir e-posta, **FTP** ve **SSH** sunucusu olabilir.

# Küçük Ağ Uygulamalar ve Protokoller

## Genel Protokoller (Devam.)

Bu ağ protokolleri, aşağıdakileri tanımlayan bir **ağ uzmanının temel araç setini içerir**:

- Bir iletişim oturumunun her iki ucundaki işlemler.
- Mesaj türleri.
- Mesajların sözdizimi.
- Bilgi alanlarının anlamı.
- Mesajların nasıl gönderildiği ve beklenen yanıt.
- Bir sonraki alt katmanla etkileşim.

Birçok şirket, mümkün olduğunda bu protokollerin güvenli sürümlerini (örneğin, **SSH**, **SFTP** ve **HTTPS**) kullanma politikası oluşturmuştur.

# Küçük Ağ Uygulamalar ve Protokoller

## Ses ve Video Uygulamaları

- **Günümüzde işletmeler**, müşteriler ve iş ortaklarıyla **iletişim kurmak ve çalışanlarının uzaktan çalışmasını sağlamak** için giderek daha fazla **IP telefonu ve akışlı ortam kullanıyor**.
- **Ağ yöneticisi**, ağa doğru ekipmanın takıldığından ve ağ cihazlarının öncelikli teslimatı **sağlayacak şekilde yapılandırıldığından emin olmalıdır**.
- Küçük bir ağ yöneticisinin **gerçek zamanlı uygulamaları** desteklerken **göz önünde bulundurması gereken faktörler**:
  - **Altyapı** - Gerçek zamanlı uygulamaları destekleme kapasitesi ve yeteneği var mı?
  - **VoIP** - VoIP tipik olarak IP Telefonundan daha ucuzdur, ancak kalite ve özellik pahasına.
  - **IP Telefonu** - Bu, arama kontrolü ve sinyallemeden özel sunucular kullanır.
  - **Gerçek Zamanlı Uygulamalar** - Ağ, gecikme sorunlarını en aza indirmek için **Hizmet Kalitesi (QoS)** mekanizmalarını desteklemelidir. **Gerçek Zamanlı Aktarım Protokolü (RTP)** ve **Gerçek Zamanlı Aktarım Kontrol Protokolü (RTCP)** ve **gerçek zamanlı uygulamaları destekleyen iki protokol**.

# 17.3 Daha Büyük Ağlara Ölçeklendirme

# Daha Büyük Ağlara Ölçeklendirme Küçük Ağları Büyütmeye

- ❖ **Büyüme**, birçok küçük işletme için **doğal bir süreçtir** ve ağları buna göre büyümelidir.
- ❖ İdeal olarak, ağ yöneticisinin, ağı şirketin büyümesine **paralel olarak büyütme konusunda akıllı kararlar vermek için yeterli ön zamanı vardır**.

Bir ağı ölçeklendirmek için birkaç öğe gereklidir:

- **Ağ dokümantasyonu** - Fiziksel ve mantıksal topoloji
- **Cihaz envanteri** - Ağ kullanan veya ağ oluştururan cihazların listesi
- **Bütçe** - Mali yıl ekipman satın alma bütçesi dahil olmak üzere ayrıntılı BT bütçesi
- **Trafik analizi** - Protokoller, uygulamalar ve hizmetler ve bunların ilgili trafik gereksinimleri belgelenmelidir

Bu öğeler, küçük bir ağın ölçeklendirilmesine eşlik eden karar verme sürecini bilgilendirmek için kullanılır.

# Daha Büyük Ağlara Ölçeklendirme Protokol Analizi

- ❖ Ağı geçen trafik türünü ve mevcut trafik akışını anlamak önemlidir.
- ❖ Bu amaçla kullanılabilecek **birkaç ağ yönetim aracı vardır.**

**Trafik akış modellerini belirlemek** için aşağıdakileri yapmak önemlidir:

- Farklı trafik türlerinin iyi bir temsilini elde etmek için yoğun kullanım zamanlarında **trafiği yakalayın.**
- **Yakalama işlemini farklı ağ segmentlerinde** ve cihazlarda gerçekleştirin çünkü **trafik belirli bir segment için yerel olacaktır.**
- **Protokol analizcisi** tarafından toplanan bilgiler, **trafiğin kaynağı** ve **hedefi** ile gönderilen **trafiğin türüne göre değerlendirilir.**
- Bu analiz, **trafiğin daha verimli bir şekilde nasıl yönetileceğine** dair kararlar **almak** için kullanılabilir.

## Daha Büyük Ağlara Ölçeklendirme Çalışan Ağ Kullanımı

- Çoğu işletim sistemi**, bu tür ağ kullanım bilgilerini görüntülemek için yerleşik araçlar sağlar.
- Bu araçlar, aşağıdaki gibi bilgilerin bir "**anlık görüntüsünü**" yakalamak için kullanılabilir:
  - İşletim Sistemi ve İşletim Sistemi Sürümü
  - CPU kullanımı
  - RAM kullanımı
  - Sürücü kullanımı
  - Ağ dışı uygulamalar
  - Ağ uygulamaları

**Küçük bir ağdaki çalışanlar** için belirli bir süre **anlık görüntülerin belgelenmesi**, gelişen protokol gereksinimlerini ve ilgili trafik akışlarını **belirlemek** için çok yararlıdır.



# 17.4 Bağlantıyı Doğrulama

# Ping ile Bağlantıyı Doğrulama

- ❑ Ağınız ister küçük ve yeni olsun, ister mevcut bir ağı ölçeklendiriyor olun, **bileşenlerinizin birbirine ve internete doğru şekilde bağlandığını her zaman doğrulayabilmek isteyeceksiniz.**
- Çoğu işletim sisteminde bulunan **ping** komutu, bir kaynak ve hedef IP adresi arasındaki **Katman 3 bağlantısını hızlı bir şekilde test etmenin en etkili yoludur.**
- Ping komutu **Internet Kontrol Mesajı Protokolü (ICMP)** yankısı (ICMP Tip 8) ve yanıt yanıtı (ICMP Tip 0) mesajlarını kullanır.



# Ping ile Bağlantıyı Doğrulayın (Devam)

Windows 10 ana bilgisayarında, **ping** komutu art arda dört ICMP yanıt mesajı gönderir ve hedeften **art arda dört ICMP yanıt mesajını bekler.**

IOS ping, **beş ICMP yanıt mesajı gönderir** ve alınan **her ICMP yanıt mesajını gösterge** göründürler.

## ▪ **IOS Ping Göstergeleri aşağıdaki gibidir:**

Element	Açıklama
!	<ul style="list-style-type: none"><li>Ünlem işaretti, bir yanıt mesajının başarıyla alındığını gösterir.</li><li><b>Kaynak ve hedef arasındaki Katman 3 bağlantısını doğrular.</b></li></ul>
.	<ul style="list-style-type: none"><li>Bir süre, <b>bir yanıt mesajını bekleyerek sürenin dolduğu anlamına gelir.</b></li><li>Bu, yol üzerinde <b>bir yerde bağlantı sorunu olduğunu gösterir.</b></li></ul>
U	<ul style="list-style-type: none"><li>Büyük "U" harfi , ICMP Tip 3 "hedef ulaşılamaz" hata mesajıyla yanıtlanan <b>yol üzerindeki bir yönlendiriciyi belirtir.</b></li><li>Olası nedenler arasında yönlendiricinin hedef ağın yönünü bilmemesi veya <b>hedef ağda ana bilgisayarı bulamaması</b> yer alır.</li></ul>

**Not:** Diğer olası ping yanıtları arasında **Q, M,?** Veya **&** bulunur. Ancak bunların anlamı bu modül için kapsam dışındadır.

# Bağlantıyı Doğrulama Genişletilmiş Ping

- ❖ **Cisco IOS**, ping komutunun "genişletilmiş" bir modunu sunar .

**Genişletilmiş ping, ayrıcalıklı EXEC modunda hedef IP adresi olmadan ping** yazılarak girilir .

Daha sonra genişletilmiş ping'i özelleştirmeniz için size birkaç komut verilecektir .

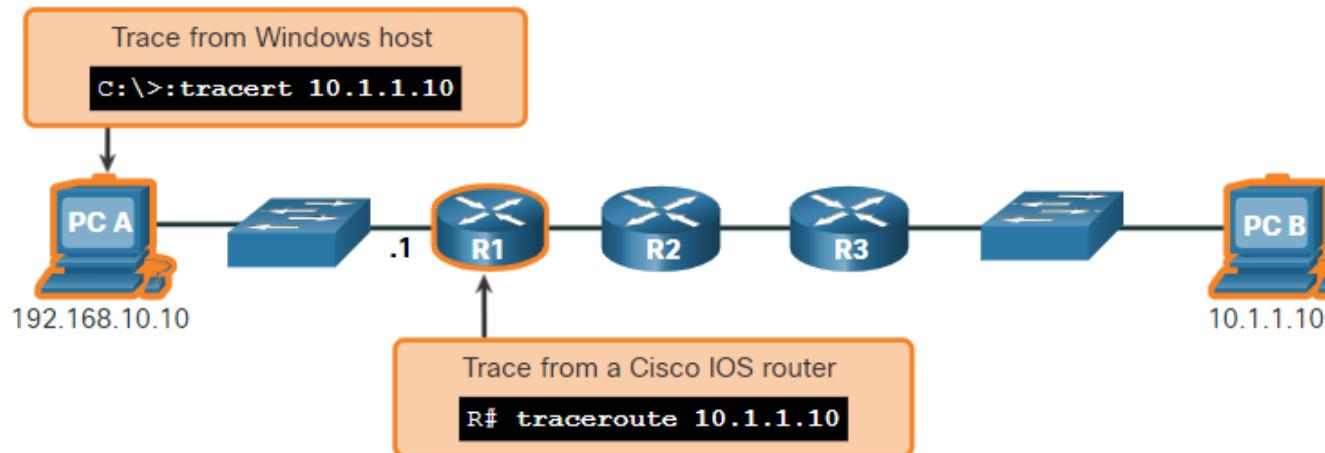
**Not:** Enter tuşuna basılması , **belirtilen varsayılan değerleri kabul eder.**

**Ping ipv6 IPv6** için kullanılan komut pingleri uzatıldı.

```
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#
```

# Traceroute ile Bağlantıyı Doğrulama

- ❑ **Ping komutu**, Katman 3 bağlantı sorunu olup olmadığını hızlı bir şekilde belirlemek için kullanışlıdır. Ancak, sorunun yol boyunca nerede olduğunu belirlemez.
- **İzleme yolu**, bir ağdaki **Katman 3** sorunlu alanların bulunmasına yardımcı olabilir.
- Bir izleme, bir paket ağ üzerinden yönlendirilirken bir atlama listesi döndürür.
- **Trace** komutunun sözdizimi işletim sistemleri arasında değişiklik gösterir.



# Traceroute ile Bağlantıyı Doğrulama (Devam)

Aşağıda, bir **Windows 10** ana bilgisayarında **tracert** komutunun örnek bir çıktısı verilmiştir .

**Not:** Windows'ta bir izlemeyi kesmek için **Ctrl-C** tuşlarını kullanın .

Tek başarılı yanıt, **R1**'deki ağ geçidinden geldi. Bir sonraki atlama için izleme istekleri **yıldız işaretiyile (\*)** gösterildiği gibi **zaman aşımına uğradı**, bu, sonraki atlama yönlendiricisinin **yanıt vermediği** veya **ağ yolunda bir arıza olduğu anlamına gelir**. Bu örnekte, **R1** ve **R2** arasında bir sorun var gibi görünüyor.

```
C:\Users\PC-A> tracert 10.1.1.10
Tracing route to 10.1.1.10 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>
```

# Traceroute ile Bağlantıyı Doğrulama (Devam)

- 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, "trace" PC B'ye başarıyla ulaşabileceğini doğruladı.  
Sağda, 10.1.1.10 ana bilgisayarı kullanılamıyordu ve çıktı, **yanıtların zaman aşımına uğradığı yıldız işaretlerini gösteriyor.**
- Zaman aşımları, olası bir ağ sorununu gösterir.  
Cisco IOS'ta traceroute kesmek için **Ctrl-Shift-6 tuşlarını kullanın** .

**Not :** Windows uygulaması traceroute (tracert), ICMP Yankı İstekleri gönderir. **Cisco IOS ve Linux**, geçersiz bir bağlantı noktası numarasıyla **UDP** kullanır.

- Son hedef, bir ICMP bağlantı noktasına erişilemez mesajı döndürecektr.



# Genişletilmiş Traceroute

Genişletilmiş ping komutu gibi, **genişletilmiş traceroute** komutu da vardır. Yöneticinin komut işlemiyle ilgili parametreleri ayarlamasına izin verir.

Windows **tracert** komutu, **komut satırındaki seçenekler aracılığıyla birkaç parametrenin girilmesine izin verir**. Ancak, genişletilmiş traceroute IOS komutu gibi yönlendirilmez. Aşağıdaki çıktı, Windows **tracert** komutu için mevcut seçenekleri görüntüler :

```
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>
```

# Genişletilmiş Traceroute (Devam)

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** modunda girilir .

IOS, tüm farklı parametrelerin ayarlanmasıyla ilgili **bir dizi bilgi istemi sunarak komut seçeneklerinde size rehberlik edecktir.**

**Not : Enter tuşuna basılması , belirtilen varsayılan değerleri kabul eder.**

```
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#
```

## Bağlantıyı Doğrulama Ağ Tabanı

- Ağ performansını izlemek ve sorun gidermek için en etkili araçlardan biri, bir ağ temeli oluşturmaktır.
- Bir temel başlatmanın bir yöntemi, yürütülen bir ping, izleme veya diğer ilgili komutlardan alınan sonuçları kopyalayıp bir metin dosyasına yapıştmaktır.
- Bu metin dosyalarına tarih eklenebilir ve daha sonra geri çağrıma ve karşılaştırma için bir arşive kaydedilebilir.
- Dikkate alınacak öğeler arasında hata mesajları ve ana bilgisayardan ana bilgisayara yanıt süreleri vardır.
- Temel bilgileri depolamak ve işlemek için profesyonel düzeyde yazılım araçları mevcuttur.

# Lab –Ping ve Traceroute ile Ağ Gecikme Testi

Bu laboratuvara , aşağıdaki hedefleri tamamlayacaksınız:

- Bölüm 1: Ping Göndererek Ağ Gecikmesisini belgeleme
- Bölüm 2: Ağ Gecikmesini Belgelemek İçin Traceroute Kullanma

# 17.5 Host ve IOS Komutları

# Windows Host üzerinde IP Konfigürasyonu

**Windows 10'da**, dört önemli ayarı hızlı bir şekilde görüntülemek için **Ağ ve Paylaşım Merkezi'nden** IP adresi ayrıntılarına erişebilirsiniz : **adres**, **maske**, **yönlendirici** ve **DNS**. Veya **ipconfig** komutunu bir Windows bilgisayarın komut satırından da verebilirsiniz .

- **MAC** adresini ve cihazın **L3** adreslemesine ilişkin bir dizi ayrıntıyı görüntülemek için **ipconfig / all** komutunu kullanın.
- Bir ana bilgisayar bir DHCP istemcisi olarak yapılandırılmışsa, IP adresi yapılandırması **ipconfig / release** ve **ipconfig / renew** komutları kullanılarak yenilenebilir .
- Windows PC'lerdeki DNS İstemci hizmeti, önceden çözümlenmiş adları bellekte depolayarak **DNS** adı çözümlemesinin performansını da optimize eder.
- **İpconfig / displaydns** tüm Windows bilgisayar sisteminde önbelleğe **DNS girdilerinin görüntüler komuta.**

```
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)
```

# Linux Host üzerinde IP Konfigürasyonu

- Bir Linux makinesinde **GUI** kullanılarak **IP ayarlarının doğrulanması**, Linux dağıtımına ve **masaüstü arayüzüne bağlı olarak farklılık gösterecektir.**
- Komut satırında, şu anda etkin olan arabirimlerin durumunu ve IP yapılandırmalarını görüntülemek için **ifconfig** komutunu kullanın.
- Linux **ip adresi** komutu, adresleri ve özelliklerini görüntülemek için kullanılır.
- IP adreslerini 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
```

# MacOS Host üzerinde IP Konfigürasyonu

- Bir Mac ana bilgisayarının GUI'sinde , IP adresleme bilgilerini almak için **Ağ Tercihleri> Gelişmiş'i açın** .
- İfconfig** komutu komut satırında arayüzü IP yapılandırmasını doğrulamak için kullanılabilir.
- Ana bilgisayar IP ayarlarını doğrulamak için diğer yararlı **macOS komutları arasında** **networksetup -listallnetworkservices** ve **networksetup -getinfo <network service>** .

```
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$ 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$
```

**Arp komutu Windows, Linux veya Mac komut isteminden çalıştırılır.**

Komut, şu anda ana bilgisayarın **ARP** önbelleğinde bulunan tüm cihazları listeler.

- **Arp -a** komut bilinen **IP adresi** ve **MAC** adresi bağlayıcı.
- **ARP önbelleği** yalnızca son erişilen cihazlardan gelen bilgileri görüntüler.
- **ARP önbelleğinin doldurulduğundan emin olmak için**, bir aygıta **ARP tablosunda** bir giriş olacak şekilde **ping** atın.
- **Önbellek , ağ yöneticisinin önbelleği güncellenmiş bilgilerle yeniden doldurmak istemesi** durumunda **netsh arabirimini ip delete arpcache** komutu kullanılarak temizlenebilir .

**Not : netsh interface ip delete arpcache** komutunu kullanabilmek için [ana bilgisayarda yönetici erişimine ihtiyacınız olabilir .](#)

# Yaygın “show” Komutları

Komut	Açıklama
show running-config	Mevcut <b>yapılandırmayı</b> ve <b>ayarları</b> doğrular
show interfaces	Arayüz <b>durumunu doğrular</b> ve tüm <b>hata mesajlarını</b> görüntüler
show ip interface	Bir arayüzün <b>Katman 3</b> bilgilerini <b>doğrular</b>
show arp	Yerel <b>Ethernet LAN'larındaki</b> bilinen <b>ana bilgisayarların listesini doğrular</b>
show ip route	<b>Katman 3</b> yönlendirme bilgilerini doğrular
show protocols	Hangi protokollerin <b>çalıştığını</b> doğrular
show version	Cihazın <b>hafızasını</b> , <b>arayüzlerini</b> ve <b>lisanslarını</b> doğrular

# “show cdp neighbors” Komutu

**CDP, her bir CDP komşu cihazı hakkında aşağıdaki bilgileri sağlar:**

- **Cihaz tanımlayıcıları** - Bir anahtarın, yönlendiricinin veya başka bir cihazın yapılandırılmış ana bilgisayar adı
- **Adres listesi** - Desteklenen her protokol için bir ağ katmanı adresine kadar
- **Port tanımlayıcısı** - FastEthernet 0/0 gibi bir ASCII karakter dizesi biçimindeki yerel ve uzak bağlantı noktasının adı
- **Yetenekler listesi** - Belirli bir cihazın Katman 2 anahtarı mı yoksa Katman 3 anahtarı mı olduğu
- **Platform** - Cihazın donanım platformu.

**show cdp neighbors detail** komutu bir komşu cihazın IP adresini ortaya koymaktadır.

```
R3# 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
S3              Gig 0/0/1          122        S I       WS-C2960+ Fas 0/5
Total cdp entries displayed : 1
R3#
```

# “show ip interface brief” Komutu

En sık kullanılan komutlardan biri **show ip interface brief** komutudur.

Bu komut **show ip interface** komutundan **daha kısaltılmış bir çıktı sağlar** . Bir yönlendiricideki tüm ağ arayüzleri için önemli bilgilerin bir özeti sağlar.

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
GigabitEthernet0/0/0 209.165.200.225 YES manual up
GigabitEthernet0/0/1 192.168.10.1   YES manual up
Serial0/1/0          unassigned     NO  unset  down
Serial0/1/1          unassigned     NO  unset  down
GigabitEthernet0      unassigned     YES unset administratively down down
R1#
```

```
S1# show ip interface brief
Interface          IP-Address      OK? Method Status        Protocol
Vlan1              192.168.254.250 YES manual up
FastEthernet0/1      unassigned     YES unset  down
FastEthernet0/2      unassigned     YES unset  up
FastEthernet0/3      unassigned     YES unset  up
```

## Video –"show version" Komutu

Bu video, yönlendiricilarındaki bilgileri görüntülemek için show version komutunu kullanmayı gösterecektir.

# Packet Tracer – “Interpret show” Komutu Çıktısı

Bu etkinlik, yönlendirici ”show” komutlarının kullanımını güçlendirmek için tasarlanmıştır . Yapılandırmanız gerekmek, bunun yerine birkaç show komutunun çıktısını analiz etmeniz gereklidir.

# 17.6 Sorun Giderme Metodolojileri

# Temel Sorun Giderme Yaklaşımları

Adım	Açıklama
Adım 1. Sorunu Belirleyin	<ul style="list-style-type: none"> <li>Bu, sorun giderme <b>sürecinin ilk adımıdır</b>.</li> <li>Bu adımda araçlar kullanılabilese de, <b>kullanıcıyla konuşmak genellikle çok faydalıdır</b>.</li> </ul>
Adım 2. Olası Nedenler Teorisi Oluşturun	<ul style="list-style-type: none"> <li>Sorun belirlendikten sonra, olası nedenlerle ilgili bir <b>teori oluşturmaya çalışın</b>.</li> <li>Bu adım genellikle soruna birkaç olası nedenden fazlasını verir.</li> </ul>
Adım 3. Nedeni Belirlemek için Teoriyi Test Edin	<ul style="list-style-type: none"> <li>Olası nedenlere bağlı olarak, sorunun nedeninin hangisi olduğunu belirlemek için <b>teorilerinizi test edin</b>.</li> <li>Bir teknisyen, test etmek ve sorunu çözüp çözmediğini görmek için <b>hızlı bir düzeltme uygulayabilir</b>.</li> <li>Hızlı bir düzeltme sorunu çözmezse, <b>kesin nedenini belirlemek için sorunu daha fazla araştırmanız gerekebilir</b>.</li> </ul>
Adım 4. Bir Eylem Planı Oluşturun ve Çözümü Uygulayın	Sorunun kesin nedenini belirledikten sonra, <b>sorunu çözmek ve çözümü uygulamak</b> için bir eylem planı oluşturun.
Adım 5. Çözümü Doğrulayın ve Önleyici Tedbirler Uygulayın	<ul style="list-style-type: none"> <li>Sorunu düzelttikten sonra <b>tam işlevselligi doğrulayın</b>.</li> <li>Mممكئنse, önleyici tedbirler uygulayın.</li> </ul>
Adım 6. Bulguları, Eylemleri ve Sonuçları Belgeleyin	<ul style="list-style-type: none"> <li>Sorun giderme sürecinin son adımda <b>bulgularınızı, eylemlerinizi ve sonuçlarınızı</b> belgeleyin.</li> <li>Bu ileride başvurmak için <b>çok önemlidir</b>.</li> </ul>

## Çözüm veya Yükseltme?

- ❖ Bazı durumlarda sorunu **hemen çözmek** mümkün olmayabilir.
- ❖ Bir yönetici kararı, belirli bir uzmanlık veya sorun giderme teknisyeninin erişemeyeceği ağ erişim düzeyi gerektirdiğinde bir sorun yükseltilmelidir.
- ❖ **Bir şirket politikası**, bir teknisyenin **bir sorunu ne zaman ve nasıl yükseltmesi gerektiğini** açıkça belirtmelidir.

## Sorun Giderme Metodolojileri “debug” Komutu

- IOS **debug** komutu, yöneticinin analiz için **işletim sistemi sürecini, protokolünü, mekanizmasını ve olay mesajlarını gerçek zamanlı olarak görüntülemesini sağlar.**
- Tüm **debug** komutları ayrıcalıklı **EXEC** modunda girilir.
- Cisco IOS, **debug** çıktısını yalnızca ilgili **özellik** veya **alt özellik** içerecek şekilde daraltmaya izin verir .
- **Debug** komutlarını yalnızca belirli sorunları gidermek için kullanın .
  - Tüm hata ayıklama komut seçeneklerinin kısa bir açıklamasını listelemek için “**debug ?**” komutu kullanılır .

# Sorun Giderme Metodolojileri

## “debug” Komutu

- Belirli bir hata ayıklama özelliğini kapatmak için **debug** komutunun önüne “**no**” ekleyin
- Alternatif olarak, ayrıcalıklı **EXEC** modunda komutun **debug** biçimini girebilirsiniz .
- Aynı anda tüm aktif ayıklama komutları kapatmak için, **undebug all** komutu.
- Bazı **debug** komutlarını kullanırken dikkatli olun , çünkü bunlar önemli miktarda **çıktı üretebilir** ve **sistem kaynaklarının büyük bir bölümünü kullanabilir**.
- Yönlendirici, **debug** mesajlarını görüntüleyerek o kadar meşgul olabilir ki, **ağ işlevlerini gerçekleştirmek** için **yeterli işlem gücüne sahip olmayabilir**, hatta **hata ayıklamayı kapatmak** için komutları bile dinleyebilir.

# Sorun Giderme Metodolojileri “terminal monitor” Komutu

- **debug** ve belirli diğer **IOS** mesaj çıktısı uzak bağlantıarda **otomatik olarak görüntülenmez.**
- Bunun nedeni, günlük mesajlarının **vty** satırlarında görüntülenmesinin engellenmesidir.
- Günlük mesajlarını bir terminalde (sanal konsol) görüntülemek için, **terminal monitor privileged EXEC** komutunu kullanın.
- Bir terminalde mesajların günlüğe kaydedilmesini durdurmak için **”no terminal monitor privileged EXEC”** komutunu kullanın.

```
R2# telnet 209.165.200.225
Trying 209.165.200.225 ... Open
Authorized access only!
User Access Verification
Password:
R1> enable
Password:
R1# debug ip icmp
ICMP packet debugging is on
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#
```

```
R1# terminal monitor
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 16:03:49.735: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.737: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.738: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.740: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
**Aug 20 16:03:49.741: ICMP: echo reply rcvd, src 10.1.1.1, dst 209.165.200.225,topology BASE, dscp 0
topoid 0
R1# no debug ip icmp
ICMP packet debugging is off
R1#
```

# 17.7 Sorun Giderme Senaryoları

## Çift Taraflı İşlem ve Uyumsuzluk Sorunları

- Birbirine bağlanan **Ethernet** arayüzleri, en iyi iletişim performansı için ve bağlantıda verimsizlik ve gecikmeyi önlemek için aynı çift yönlü modda çalışmalıdır.
- **Ethernet** otomatik anlaşma 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 tarafın da desteklediği en yüksek performans modunu seçer.

## Çift Taraflı İşlem ve Uyumsuzluk Sorunları

- Bağlı iki aygıtın biri tam çift yönlü, diğeri yarı çift yönlü çalışıyorsa, çift yönlü uyumsuzluk oluşur.
- Veri iletişimi, çift yönlü uyumsuzluğa sahip bir bağlantı yoluyla gerçekleşecek olsa da, bağlantı performansı çok zayıf olacaktır.
- Çift yönlü uyuşmazlıklar genellikle yanlış yapılandırılmış bir arabirimden veya nadir durumlarda **başarısız** bir otomatik anlaşmadan kaynaklanır.
- Cihazlar arasındaki iletişim devam ettiği için çift yönlü uyumsuzlukları gidermek zor olabilir.

# IOS Cihazlarında IP Adresleme Sorunları

- Yanlış IPv4 atamasının **iki yaygın nedeni**, manuel atama **hataları** veya **DHCP** ile ilgili sorunlardır.
- Ağ yöneticilerinin **genellikle sunucular ve yönlendiriciler** gibi cihazlara **manuel olarak IP adresi ataması** gereklidir.
- Atama sırasında bir hata yapılrsa, büyük olasılıkla cihazla iletişim sorunları yaşanır.
- Bir IOS aygıtından, ağ arabirimlerine hangi IPv4 adreslerinin atandığını doğrulamak için **show ip interface** veya **show ip interface brief** komutlarını kullanın.
- Örneğin, gösterildiği gibi **show ip interface brief** komutunun verilmesi, R1'deki arayüz 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#
```

## Son Kullanıcı Cihazlarında IP Adresleme Sorunları

- Windows tabanlı makinelerde, cihaz bir **DHCP sunucusuyla bağlantı kurmadığında, Windows otomatik olarak 169.254.0.0/16 aralığına ait bir adres atayacaktır.**
- Bu özelliğe **Otomatik Özel IP Adresleme (APIPA) denir.**
- **APIPA** adresine sahip bir bilgisayar, ağdaki diğer cihazlarla iletişim kuramaz çünkü bu cihazlar büyük olasılıkla **169.254.0.0/16** ağına ait olmayacağından emin olmayı tercih eder.
  - **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 atanmış IP adreslerini doğrulamak için **ipconfig** komutunu kullanın.

## Varsayılan Ağ Geçidi Sorunları

- Bir son cihaz için **varsayılan ağ geçidi**, trafiği diğer ağlara iletебilen son cihazla aynı ağa ait olan en yakın ağ cihazıdır.
- **Bir aygıt yanlış veya var olmayan bir varsayılan ağ geçidi adresine sahipse**, uzak ağlardaki aygıtlarla iletişim kuramayacaktır.
- IPv4 adresleme sorunlarına benzer şekilde, varsayılan ağ geçidi sorunları, yanlış yapılandırma (manuel atama durumunda) veya **DHCP** sorunları (otomatik atama kullanımdaysa) ile ilgili olabilir.

## Varsayılan Ağ Geçidi Sorunları

- Windows tabanlı bilgisayarlarda varsayılan ağ geçidini doğrulamak için **ipconfig** komutunu kullanın.
- Bir **yönlendiricide**, **yönlendirme tablosunu** listelemek ve **varsayılan yol olarak bilinen** varsayılan ağ geçidinin ayarlandığını doğrulamak için **show ip route** komutunu kullanın.
- Bu yol, **paketin hedef adresi yönlendirme tablosundaki diğer yollarla eşleşmediğinde kullanılır.**

## DNS Sorunları Giderme

- Kullanıcıların yanlışlıkla bir internet bağlantısının çalışmasını **DNS**'nin kullanılabilirliğiyle ilişkilendirmesi yaygındır.
- **DNS sunucusu adresleri** **manuel** veya **otomatik olarak DHCP** aracılığıyla atanabilir.
- **Şirketlerin** ve kuruluşların kendi **DNS sunucularını yönetmeleri** yaygın olsa da, herhangi bir erişilebilir **DNS sunucusu adları** çözümlemek için 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.

## DNS Sorunları Giderme

- 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 gösterildiği gibi kullanın.
- **Nslookup** komutu PC'ler için başka bir faydalı bir DNS sorun giderme aracıdır.
- **nslookup** bir kullanıcı manuel olarak **DNS** sorgularını yerleştirmek ve **DNS** tepkisini analiz edebilirsiniz.

# Lab – Bağlantı Sorunlarını Giderme

Bu laboratuvara , aşağıdaki hedefleri tamamlayacaksınız:

- Sorunu Tanımlayın
- Ağ Değişikliklerini Uygulayın
- Tam İşlevselliği Doğrulayın
- Belge Bulguları ve Yapılandırma Değişiklikleri

# Packet Tracer – Bağlantı Sorunlarını Giderme

Bu Packet Tracer etkinliğinin amacı, mümkünse bağlantı sorunlarını gidermek ve çözmektir. Aksi takdirde, sorunlar açıkça belgelendirilmeli ve böylece yükseltiler olmalıdır.

# 17.8 Alıştırmalar ve Sınav

# Lab – Bir Küçük İşletme Ağı Tasarlayın ve Oluşturun

Bu laboratuvara bir ağ tasarlayacak ve inşa edeceksiniz. Doğrudan bağlı segmentlerden oluşan küçük bir ağın nasıl oluşturulduğunu, yapılandırıldığını ve doğrulandığını açıklayacaksınız.

# Packet Tracer – Beceri Entegrasyon Zorluğu

Bu Packet Tracer etkinliğinde, bu kurs boyunca edindiğiniz tüm becerileri kullanacaksınız.

## Senaryo:

Yönlendirici Merkezi, ISP kümesi ve Web sunucusu tamamen yapılandırılmıştır. 192.168.0.0/24 ağını kullanarak 4 alt ağı barındıracak yeni bir IPv4 adresleme şeması oluşturmalısınız. BT departmanı 25 ana bilgisayara ihtiyaç duyar. Satış departmanının 50 ana bilgisayara ihtiyacı var. Personelin geri kalanı için alt ağ 100 ana bilgisayar gerektirir. Gelecekte 25 ana bilgisayarı barındıracak bir Konuk alt ağı eklenecektir. Ayrıca R1'de temel güvenlik ayarlarını ve arayüz yapılandırmalarını da bitirmelisiniz. Ardından, SVI arayüzü ve S1, S2 ve S3 anahtarlarındaki temel güvenlik ayarlarını yapılandıracaksınız

# Packet Tracer – “Sorun Giderme”

Bu Packet Tracer etkinliğinde, mevcut bir LAN'daki bir dizi sorunu giderecek ve çözeceksiniz.

# Bu modülde ne öğrendim ?

- Küçük bir ağ için ağ cihazlarını seçerken göz önünde bulundurulması gereken faktörler maliyet, hız ve bağlantı noktası / arayüz türleri, genişletilebilirlik ve işletim sistemi özellikleri ve hizmetleridir.
- Bir ağ uygularken, bir IP adresleme şeması oluşturun ve bunu üç cihazlarda, sunucularda ve çevre birimlerinde ve ara cihazlarda kullanın.
- Yedekleme, yinelenen ekipman kurarak gerçekleştirilebilir, ancak kritik alanlar için yinelenen ağ bağlantıları sağlayarak da gerçekleştirilebilir.
- Küçük bir ağdaki yönlendiriciler ve anahtarlar, ses ve video gibi gerçek zamanlı trafiği, diğer veri trafiğine göre uygun bir şekilde destekleyecek şekilde yapılandırılmalıdır.
- Ağa erişim sağlayan iki tür yazılım programı veya işlemi vardır: ağ uygulamaları ve uygulama katmanı hizmetleri.
- Bir ağı ölçeklendirmek için birkaç öğe gereklidir: ağ dokümantasyonu, cihaz envanteri, bütçe ve trafik analizi.
- Ping komutu, bir kaynak ve hedef IP adresi arasındaki Katman 3 bağlantısını hızlı bir şekilde test etmenin en etkili yoludur.
- Cisco IOS, kullanıcının komut işlemiyle ilgili parametreleri ayarlayarak özel ping türleri oluşturmasına izin veren "genişletilmiş" bir ping komutu modu sunar.

## Bu modülde ne öğrendim ?

- Bir izleme, bir paket ağ üzerinden yönlendirilirken bir atlama listesi döndürür.
- Ayrıca genişletilmiş bir iz yolu komutu da vardır. Yöneticinin komut işlemiyle ilgili parametreleri ayarlamasına izin verir.
- Ağ yöneticileri, ipconfig komutunu vererek bir Windows ana bilgisayarındaki IP adresleme bilgilerini (adres, maske, yönlendirici ve DNS) görüntüler. Diğer gerekli komutlar **ipconfig / all , ipconfig / release ve ipconfig / renew ve ipconfig / displaydns**'dir .
- Bir Linux makinesinde GUI kullanarak IP ayarlarının doğrulanması, Linux dağıtımına (dağıtım) ve masaüstü arayüzüne bağlı olarak farklılık gösterecektir. Gerekli komutlar ifconfig ve ip adresidir.
- Bir Mac host GUI'sinde, IP adresleme bilgilerini almak için Ağ Tercihleri> Gelişmiş'i açın. Mac için diğer IP adresleme komutları ifconfig ve networksetup -listallnetworkservices ve networksetup -getinfo <ağ hizmeti> dir.
- **Arp** komutu Windows, Linux veya Mac komut isteminden çalıştırılır. Komut, her cihaz için IPv4 adresini, fiziksel adresi ve adresleme türünü (statik / dinamik) içeren ana bilgisayarın ARP önbelleğinde bulunan tüm cihazları listeler.
- **Arp -a** komut bilinen IP adresi ve MAC adresi bağlayıcı.



## Bu modülde ne öğrendim ?

- Ortak “show komutları **show running-config**, **show interfaces**, **show ip address**, **show arp**, **show ip route**, **show protocols**, ve **show version** ‘ dır. **show cdp neighbor** komutu her CDP cihaz hakkında aşağıdaki bilgileri sağlar : Tanımlayıcılar , adres listesi, port tanımlayıcıları, kabiliyet listesi ve platform
- **“show cdp neighbors detail”** komutu CDP komşularından birinin bir IP yapılandırması hata varsa komut belirlemek yardımcı olacaktır.
- **“show ip interface brief”** komutu çıktısı , yönlendirici üzerindeki tüm bağlantı arabirimlerini , her bir arabirimde atanan IP adreslerini ve arabirimlerin operasyonel durumlarını gösterir.
- Sorun gidermeye yönelik altı temel adım : Adım 1. Sorunu belirleme Adım 2. Muhtemel nedenlerle ilgili bir teori oluşturun. Adım 3. Nedeni belirlemek için teoriyi test edin. Adım 4. Bir eylem planı oluşturun ve çözümü uygulayın. Adım 5. Çözümü doğrulayın ve önleyici tedbirleri uygulayın. Adım 6. Bulguları, eylemleri ve sonuçları belgeleyin.
- Bir yöneticinin kararını, belirli bir uzmanlığı veya sorun giderme teknisyeninin erişemeyeceği ağ erişim düzeyini gerektirdiğinde bir sorun yükseltilmelidir.
- İşletim sistemi süreçleri, protokoller, mekanizmaları ve olayları, durumlarını bildirmek için mesajlar üretir. IOS hata ayıklama komutu, yöneticinin bu mesajları analiz için gerçek zamanlı olarak görüntülemesini sağlar.
- Günlük mesajlarını bir terminalde (sanal konsol) görüntülemek için, terminal monitor privileged EXEC komutunu kullanın.

