# Routers (Yönlendiriciler)

BİLİŞİM SİSTEMLERİ VE AĞ TEKNOLOJİLERİ EĞİTİMİ

ÜNSAL GÜNAL
İSTANBUL - 2019

# Router (Yönlendirici)

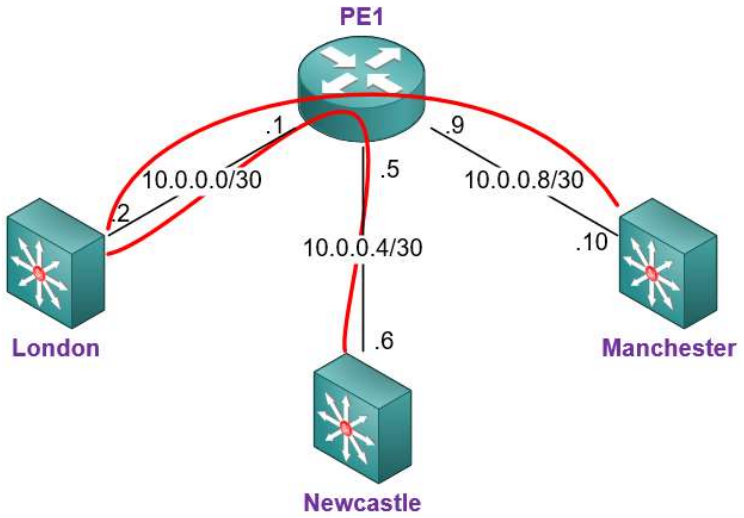
Router'lar, varsayılan olarak, broadcast domain'lerini ayıran cihazlar olarak bilindiği halde, collision domain'lerini de birbirlerinden ayırırlar. Router OSI yedi katman modelinin üçüncüsü olan ağ katmanını (Network) kullanır.

Ağınızda router kullanmanın iki avantajı vardır:

- Varsayılan olarak, broadcast'leri yönlendirmezler.
- IP adresi gibi 3. katman (ağ katmanı) bilgilerinin olduğu paketleri filtreleyebilirler.

Ağınızdaki dört router fonksiyonu aşağıdaki gibidir:

- Paket switching
- Paket filtreleme
- Ağlar arası iletişim
- Yol seçimi




# Router (Yönlendirici)

Routerların bulunduğu network katmanında iki paket türü bulunmaktadır:

**Veri paketleri:** Ağ topluluğu boyunca kullanıcı verisini aktarmak için kullanılır. Veri trafiğini desteklemek için kullanılan protokoller, routed protokoller (IP ve IPv6) olarak belirtilir.

**Route güncelleme paketleri:** Ağ topluluğundaki tüm router'lara bağlı ağlar hakkında komşu router'ları güncellemek için kullanılır. Route güncelleme paketi gönderen protokoller, routing protokolleri olarak belirtilir; RIP, RIPv2, EIGRP ve OSPF yaygın olarak kullanılan routing protokollerdir.

# Router (Yönlendirici)

Eğer bir network yönlendiriciye doğrudan bağlı ise router o networke nasıl ulaşacağını bilir. Eğer bir network doğrudan bağlı değilse, yönlendiricinin ağa ulaşmak için iki yolu vardır :

- Static Routing: Network Yöneticisi manuel olarak tüm networklerin tanımını routing tablosuna girer,
- Dynamic Routing: Router üzerinde çalıştırılan bir protokol aynı protokol ile çalışan diğer Router'lar ile belirli tanımlamalar ve kısıtlar çerçevesinde kalmak şartıyla haberleşerek yönlendirme tablosunu kendisi oluşturur/doldurur (populating routing table).

Static Routing (Statik Yönlendirme), «IP Route» komutu ile gerçekleşirken Dynamic Routing (Dinamik Yönlendirme), çeşitli routing protokolleri ile gerçekleşmektedir.

# Router (Yönlendirici)

Routing tablolarında şu bilgiler bulunur:

Network adresleri: Protokole özgü network adresleridir. Her routing protokolü, ağı farklı adresleme tasarımı (örneğin IP, IPv6 ve IPX) ile izlediğinden, bir router, ayrı routing protokolleri için bir routing tablosu oluşturmalıdır.

Interface: Belirli bir ağı hedeflediğinde, bir paketin bulunacağı çıkış ara yüzüdür.

Metrik: Uzak ağ mesafesidir. Farklı routing protokolleri bu mesafenin hesaplanmasında farklı yollar kullanırlar. Bazı protokoller bant genişliği, hattın gecikmesi ve hatta tick count (saniyenin 1/18'i) bile kullanırken, bazı routing protokolleri ise (RIP) hop count (bir paketin, bir route boyunca uzak bir ağa giderken uğradığı router sayısı) olarak belirtilen bir mekanizma kullanır.

# Statik Yönlendirme

Static Routing (Statik Yönlendirme) : Statik Yol aşağıdaki IOS komutlarıyla yapılandırılabilir.

*Router(config)# ip route destination_network subnet_mask default_gateway [administrative_distance] [permanent]*

*Router(config)# ip route destination_network subnet_mask interface_to_exit [administrative_distance] [permanent]*

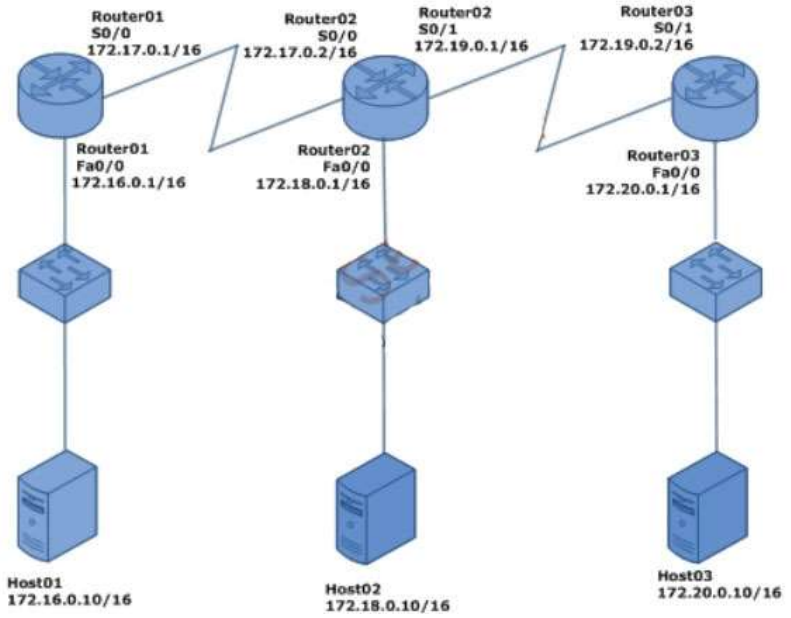
Burada, yönlendiricinin statik yol için kullandığı arabirim başarısız olsa bile, yönlendirme tablosundaki statik yolu koruyacaktır. İlgili show komutları şöyledir:

*Router# sh ip route*

*Router# sh running-config*

# Statik Yönlendirme

ÖRNEK : Aşağıdaki gibi bağlı üç yönlendiricimiz, üç anahtarımız ve üç ana makinemiz için **statik routing** ayarlarını yapalım.



# Dinamik Yönlendirme

**Dynamic Routing (Dinamik Yönlendirme) Protokolleri :**

- Distance Vector Protokoller : Bu türden protokoller routing tablosunu güncelleme mantığı ile çalışırlar. Yani belirli zaman aralıklarında sahip oldukları ağ bilgilerini komşu yönlendiricilere gönderirler ve aynı zamanda da komşu yönlendiricilerde bulunan bilgileri alırlar. Bu döngü sonucunda sistem üzerindeki tüm yönlendiriciler ağı öğrenmiş olurlar ve dolayısıyla en uygun yol seçimini yapabilirler.

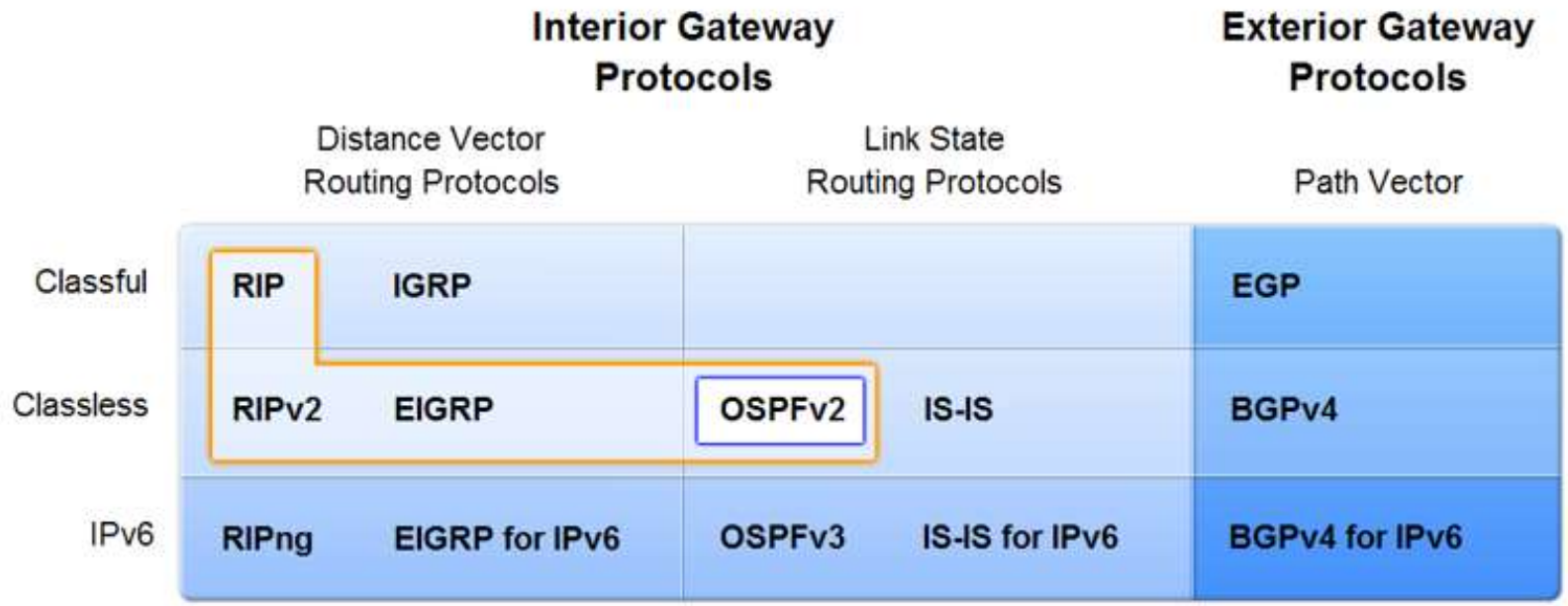
  Sistemdeki routerların tüm networkden haberdar olması durumuna “convergence” (yakınsama) denir. Distance Vector Protokolleri şunlardır :

  - RIP (Router Information Protocol) Verson 1 & Verson 2
  - IGRP (Interior Gateway Routing Protocol)

# Dinamik Yönlendirme

- Link State Protokoller : Bu tür protokoller sürekli güncelleme yapmak yerine komşu yönlendiricilere «up» olup olmadıklarını anlamak için küçük «Hello» paketçikleri gönderirler. Sadece gerektiği zamanlarda ya da sisteme yeni bir yönlendirici eklendiğinde veya bir yönlendirici kapatıldığında sadece o bilgileri güncellerler. Link State Protokolü :
  - OSPF (Open Shortest Path First)
  - ISIS (Intermediate System to Intermediate System)
- Hybrid Protokoller : Hem Distance Vektor ve hem de Link State protokollerinin bazı özelliklerini bir arada bulundururlar. Routing güncellemesi olarak komşularına yönlendirme tablolarını yollarlar. Fakat routing tablolarını yollarken sadece değişen kısımları günceller (differencial). Bunun yanında metric değerler de hedef networklere giden yol seçiminde kullanılırlar. Bu grupta bulunan EIGRP (Enhanced Interior Gateway Routing Protocol) protokolü Cisco tarafından geliştirilmiştir ve sadece Cisco yönlendiricilerde çalışmaktadır.

# Dinamik Yönlendirme



# AS (Autonomous System)

AS (Autonomous System):

- AS, benzer yönlendirme politikalarını paylaşan ve tek bir yönetim alanı içinde çalışan bir yönlendiriciler grubudur.
- Bir AS, tek bir IGP'yi çalıştıran yönlendiriciler topluluğu da olabilir ya da hepsi bir kuruma ait olan farklı protokolleri çalıştıran yönlendiriciler topluluğu da olabilir. Her iki durumda da, dış dünya tüm Özerk Sistemi tek bir varlık olarak görülür.
- Her AS, bir İnternet kaydı veya servis sağlayıcısı tarafından atanan bir tanım numarasına sahiptir. Bu numara 1 ile 65,535 arasındadır (16 bit).
- 64,512 - 65,535 aralığındaki AS numaraları özel kullanım için ayrılmıştır. Bu durum, IP adreslerine (RFC 1918) benzer.
- Sınırlı sayıda mevcut AS numaralarından dolayı, bir kuruluş AS numarasına atanmadan önce ihtiyacının gerekçesini sunmalıdır.

| Number | Bits | Description | Reference |
|---|---|---|---|
| 0 | 16 | Reserved | RFC1930 |
| 1 - 23455 | 16 | Public ASN's | |
| 23456 | 16 | Reserved for AS Pool Transition | RFC6793 |
| 23457 - 64534 | 16 | Public ASN's | |
| 64000 - 64495 | 16 | Reserved by IANA | |
| 64496 - 64511 | 16 | Reserved for use in documentation/sample code | RFC5398 |
| 64512 - 65534 | 16 | Reserved for private use | |
| 65535 | 16 | Reserved | |
| 65536 - 65551 | 32 | Reserved for use in documentation and sample code | RFC4893, RFC5398 |
| 65552 - 131071 | 32 | Reserved | |
| 131072 - 4199999999 | 32 | Public 32-bit ASN's | |
| 4200000000 - 4294967294 | 32 | Reserved for private use | RFC6996 |
| 4294967295 | 32 | Reserved | |

# AS (Autonomous System)

Orijinal 16-bit tam sayıların (0 ve 65,535) ve 32-bit tam sayıların (4.294.967.295) ilk ve son ASN'leri saklıdır ve operatörler tarafından kullanılmaz. Ayrıca 16-bit aralığın 64.496 ile 64.511'i ve 32-bit aralığın 65.536 ila 65.551'i RFC 5398'e ait belgelerde kullanılmak üzere ayrılmıştır. 32 bitlik seri, RFC 6996 tarafından Özel Kullanım için ayrılmıştır. Bu, dahili olarak kullanılabilecekleri ancak küresel İnternet'e duyurulmaması gerektiği anlamına gelir. Diğer tüm ASN'ler IANA tarafından atanır.

# RIP Protokolü

Dinamik Yönlendirme Protokolü komutları :

- **RIPv1 (Router Information Protocol):** Aşağıdaki komutlar, belirtilen ağa ait arabirimler için RIP güncellemelerinin gönderilmesini ve alınmasını sağlar.

  *Router (config)# router rip*

  *Router (config-router)# network <directly-connected-classful-network-address>*

ÖRNEK :

```
Router(config)#router rip
Router(config-router)#
```

```
Router(config-router)#network 192.168.0.0
```

# RIP Protokolü

- **RIPv2:** Belirtilen ağa ait arabirimler için RIPv2 güncellemelerinin gönderilmesini ve alınmasını sağlar. Otomatik özetleme devre dışı bırakıldığında, RIPv2, sınır yönlendiricilerdeki ağları, artık, sınıflarına göre özetleyemeyecektir.

*Router (config)# router rip*

*Router (config)# version 2*

*Router (config)# no auto-summary*

*Router (config-router)# network <directly-connected-classful-network-address>*

İlgili Show komutları şöyledir:

*Router# sh ip route*

*Router# sh running-config*

# RIP Protokolü

Genel olarak aşağıdaki show (sh) komutu kullanılarak dinamik protokol ile yapılan yönlendirme bilgilerine ulaşılabilir:

*Router02# sh ip route ?*

| | |
|---|---|
| *WORD* | *Network to display information about or hostname* |
| *bgp* | *Border Gateway Protocol (BGP)* |
| *connected* | *Connected* |
| *eigrp* | *Enhanced Interior Routing Protocol (EIGRP)* |
| *ospf* | *Open Shortest Path First (OSPF)* |
| *rip* | *Routing Information Protocol (RIP)* |
| *static* | *Static routes* |
| *summary* | *Summary of all routes* |
| *\|* | *Output Modifiers* |

# RIP Protokolü

RIPv1 ile RIPv2 karşılaştırması:

RIPv1

- Yalnızca sınıfsal (classful) yönlendirmeyi destekler (VLSM'yi desteklemez).
- Kimlik doğrulama yapmaz.
- RIPv1 broadcat kullanır.

RIPv2

- Sınıfsız  (VLSM) yönlendirmeyi destekler. RIPv2, sınıfsız yönlendirme yayınlarına izin vermek için ağ maskesini kullanır.
- Kimlik doğrulama yapılabilir.
- RIPv2 broadcat yerine multicast yayın kullanır. Çok noktaya yayın iletimi, RIP güncelleştirmelerini dinlemesi gerekmeyen ağ aygıtlarında, yükü azaltacaktır.

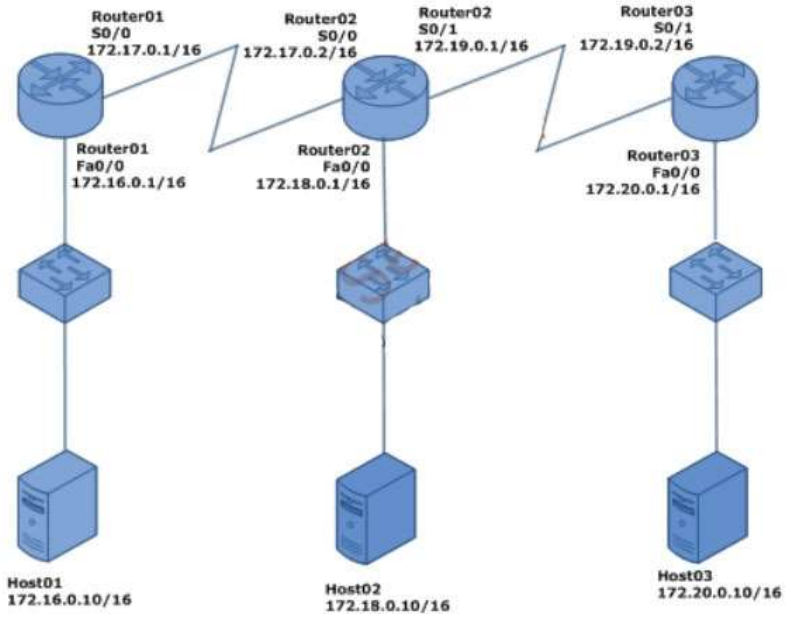
# RIP Protokolü

RIP Protokolünün avantajları ve dezavantajları:

- RIP, RFC 1388, 1723 ve 2453'e dayanan, mesafe-vektör yönlendirme protokolüdür.
- Küçük ağlar için ideal bir protokoldür. Öncelikli olarak sınırlaması, 15'ten fazla sekmesi olan bir ağı destekleyememesidir. RIP, 15 atlamadan (hop) fazla olan her şeyin sonsuz olduğunu varsayar ve bu nedenle de rotayı geçersiz kılar.
- Bununla birlikte RIP, çok yaygın olarak kullanılmaktadır. Birçok yönlendirici varsayılan olarak RIP protokolü ile gelir.
- Ayrıca, birçok güvenlik duvarı standart olarak RIP'i destekler, ancak OSPF veya EIGRP'i desteklemez.

# RIP Protokolü

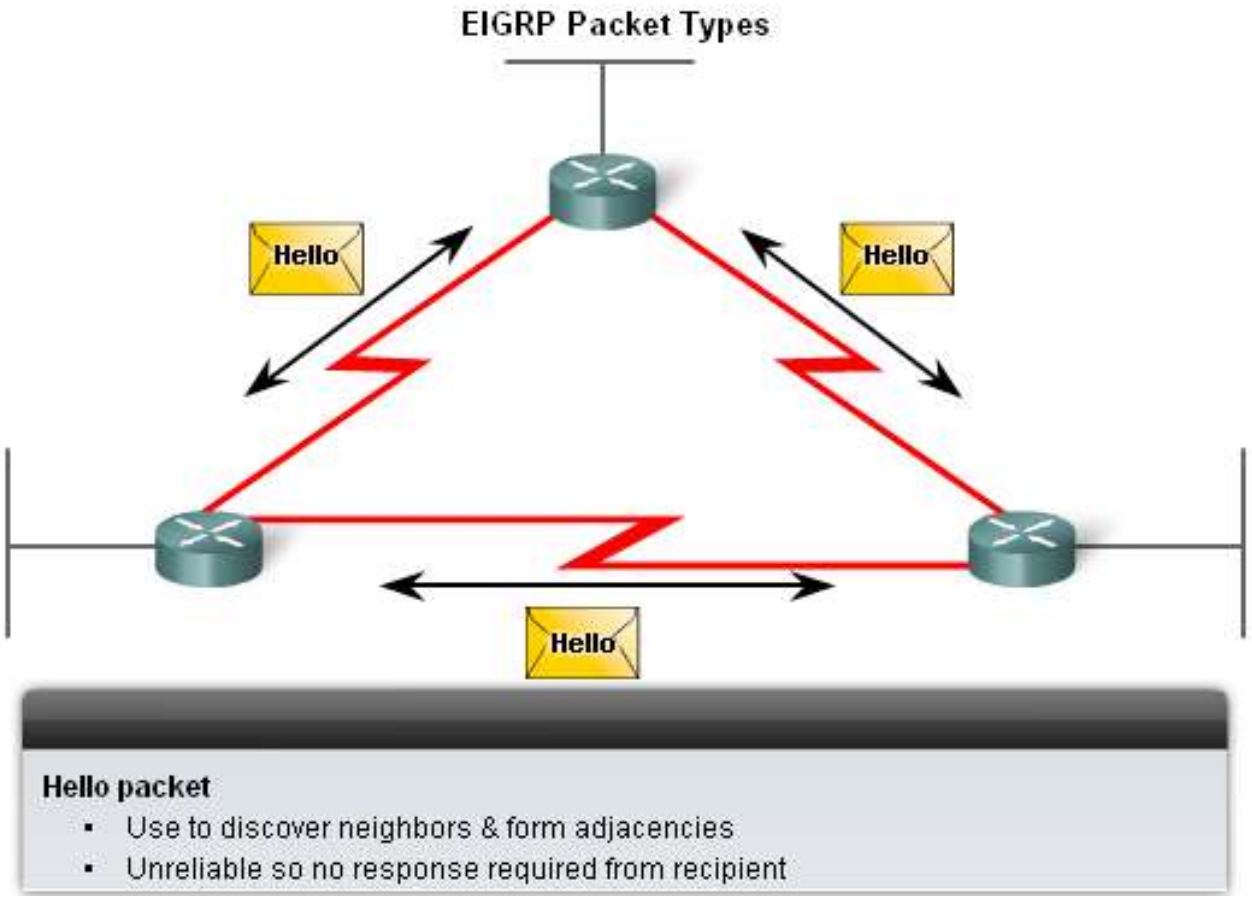
ÖRNEK : Aşağıdaki gibi bağlı üç yönlendiricimiz, üç anahtarımız ve üç ana makinemiz için **RIP routing** ayarlarını yapalım.



# EIGRP Protokolü

**EIGRP - Enhanced Interior Gateway Routing Protocol**

- Geliştirilmiş İç Ağ Geçidi Yönlendirme Protokolü (EIGRP - Enhanced Interior Gateway Routing Protocol), Cisco'nun tescilli gelişmiş Mesafe Vektör yönlendirme protokolüdür. EIGRP, IGRP'ye dayanmaktadır, bu nedenle konfigürasyonlar da birbirlerine benzerdir.
- EIGRP, bir Hibrit Yönlendirme Protokolü olarak kabul edilir, çünkü EIGRP Distance Vector Protokolü ve Link State Protokolünün her ikisinin de karakteristik özelliklerine sahiptir.
- EIGRP, IGRP'den daha hızlı yakınsamaya sahiptir ve sadece güncellemeleri kullandığından daha az ağ ile uğraşır.
- EIGRP'nin diğer bir önemli özellikleri ise, yönlendirme döngüsüz topoloji (routing loop-free topology), VLSM ve rota özetlemesi, çok noktaya yayın ve artımlı güncellemeler (multicast and incremental updates) ve çoklu yönlendirilmiş protokollerdir (IP, IPX ve AppleTalk).
- Geliştirilmiş İç Ağ Geçidi Yönlendirme Protokolü (EIGRP) En kısa yolu hesaplamak için Dağınık Güncelleme Algoritmasını (DUAL - Diffusing Update Algorithm) kullanır.




# EIGRP Protokolü

- «Hello» Paketleri

  Komşuları keşfetmek/bulmak için küçük «Hello» paketleri kullanılmaktadır.

- Update (Güncelleme) Paketleri

  Yönlendirme (routing) bilgilerini yaymak için kullanılır.

- Acknowledgement (Onay) Paketleri

  Güncelleme, sorgu ve cevap paketlerinin alındığını bildirmek için kullanılır.

- Query & Reply Paketleri

  Ağları aramak için DUAL tarafından kullanılır.

# EIGRP Protokolü (terimler)

- Neighbor table: Komşu tablo, EIGRP komşularının bir listesini içerir. EIGRP için yönlendirilen her protokolün kendi komşu tablosu vardır.
- Topology table: Topoloji tablosu, EIGRP yönlendiricisinin öğrendiği tüm hedeflerin ve yolların bir listesini içerir. Her bir yönlendirilmiş protokol için ayrı bir topoloji tablosu vardır.
- Successor: Bu, topoloji tablosu içinde bir hedefe ulaşmak için seçilen en iyi yoldur.
- Feasible successor: Bir hedefe ulaşmak için en iyi yedekleme yoludur.
- Routing table: Yönlendirme tablosu, topoloji tablosundaki tüm successor olan yolları içerir. Her yönlendirilen protokol için ayrı bir yönlendirme tablosu bulunur.
- Advertised distance: Komşu bir yönlendiricinin belirli bir rota için yayınladığı mesafedir (metrik).
- Feasible distance: Uygun mesafe, yönlendiricinizin belirli bir rotaya ulaşmak için kullanacağı mesafedir (metrik).

# EIGRP Protokolü

- EIGRP: İlk komut, kullanıcıyı, listelenen ASN için EIGRP yapılandırma moduna taşımaktır. Autonomous System (AS) numarası benzersizdir ve iletişim için çok önemlidir.

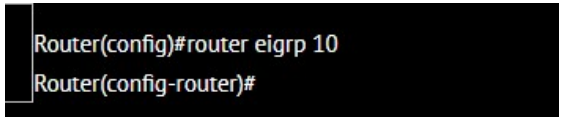
*Router (config) # router eigrp <AS number>*

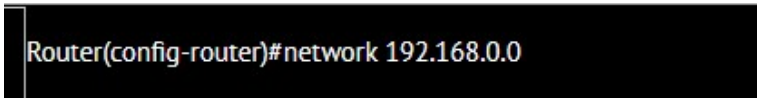
*Router (config) # network <network address>*

*Router (config) # network <network address> <wild-card mask>*

ÖRNEK :

EIGRP globaly 'i, «router eigrp as-number global» komutlarını kullanarak etkinleştirin. Bu komut sizi aşağıda gösterildiği gibi yönlendirme konfigürasyon moduna getirecektir:



# EIGRP Protokolü

- EIGRP protokolü için show komutunun seçenekleri aşağıdaki gibidir :

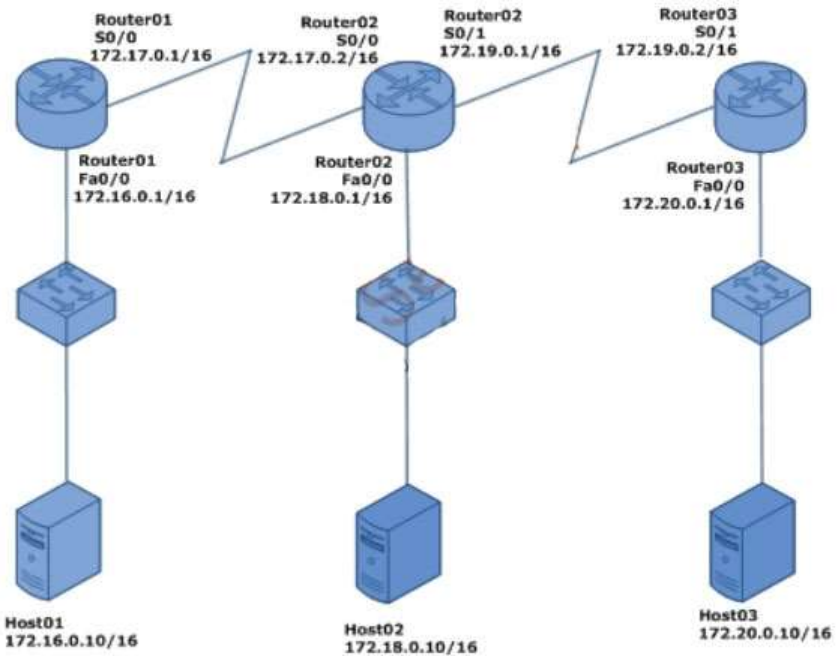
*Router#sh ip eigrp ?*

| | |
|---|---|
| *interfaces* | *IP-EIGRP interfaces* |
| *neighbors* | *IP-EIGRP neighbors* |
| *topology* | *IP-EIGRP Topology Table* |
| *traffic* | *IP-EIGRP Traffic Statistics* |

*Router#sh ip route*

*Router#sh running-config*

- Wild-card mask: subnet mask değerinin 1 ve 0 anlamında ters yazılmış halidir. Örneğin 255.255.255.0 subnet için wild-card mask değeri, 0.0.0.255 olacaktır. Yazılışı daha kolay ve hataya daha az açık bir yazım biçimidir.




# EIGRP Protokolü

Aşağıdaki formül, Gelişmiş İç Ağ Geçidi Yönlendirme Protokolü'nün (EIGRP) metrikini hesaplamak için kullanılır.

*Metric = [K1*Bandwidth + (K2*Bandwidth)/ (256 - Load) + K3*Delay] * [K5/(Reliability + K4)]*

K için varsayılan değerler K1 = 1, K2 = 0, K3 = 1, K4 = 0, K5 = 0'dır. Varsayılan davranış için formül metrik = bant genişliği + gecikme olarak basitleştirilebilir.

ÖRNEK : Yandaki gibi bağlı üç yönlendiricimiz, üç anahtarımız ve üç ana makinemiz için **EIGRP routing** ayarlarını yapalım.

# OSPF Protokolü

**OSPF (Open Shortest Path First)**

OSPF IETF (Internet Engineering Task Force) tarafıdan açık kaynak olarak geliştirilen Link state routing protokolüdür. Cisco nun EIGRP karşılık olarak geliştirilmiştir. Cisco'ya özel bir protokol değildir. Yani farklı marka routerlarda ortak olarak çalıştırılabilir. Tüm topolojinin haritasını çıkarır. ve SPF (Shortest Path First) algoritmasını kullanarak en iyi rotayı seçer.

- OSPF protokolünde, netwokteki yönlendirme bilgilerini kendisinde toparlayıp diğerlerine dağıtan yönlendiriciye, Designated router (DR) denir.  DR aktif olmadığı durumlarda Backup designated router (BDR) devreye girer.
- Administrative distance varsayılan değeri 110 dur.
- Network convergence olduktan sonra  tam güncelleme yapmaz. Bunun yerine değişiklikleri update (Triggered Update) yapar.
- EIGRP eşit olmayan cost değerli linklerde yük dengelemesi yapabilir. OSPF ise sadece eşit cost değerli linklerde yük dengelemesi yapabilir.

# OSPF Protokolü

QSPF avantajları ve dezavantajları :

- OSPF en büyük dezavantajı bitişikliği tutmak (OSPF komşularının listesi), topoloji (tüm yönlendiricileri ve rotalarını içeren bağlantı durumu veritabanı) ve yönlendirme tablolarını tutmak için çok fazla belleğe gereksinim duymasıdır.
- Ayrıca OSPF, SPF algoritmasını çalıştırmak ve OSPF nin karmaşık olan yönlendirme protokolü için de ek CPU işlemine ihtiyaç duyar.
- OSPF söz konusu olduğunda Özerk Sistemler (Autonomous Systems) ve Alanlar (Areas) olmak üzere iki önemli kavram ortaya çıkar. Alanlar, Özerk Bir Sistem içerisinde hiyerarşik yönlendirme sağlamak için kullanılır. Alanlar, ağınızdaki yönlendirme bilgilerinin ne zaman ve ne kadar paylaşılacağını kontrol etmek için kullanılır.
- OSPF iki katmanlı bir hiyerarşi uygular: Omurga (Alan-Area 0) ve omurga dışındaki alanlar (AS, 1–65,535). Bu iki farklı alan tipi, aralarındaki yönlendirme bilgisini birbirlerine özetlerler. Rota yazımı, yönlendirme tablolarını sıkıştırmaya yardımcı olur. Tüm alanlar Alan 0'a (örnek) bağlanmalıdır ve böylece bir Alandaki tüm yönlendiriciler de aynı topoloji tablosuna sahip olacaktır.
- Her Alan 50 tane yönlendiriciyi destekler. Bununla birlikte sınırsız Alan oluşturulabilir.

# OSPF Protokolü

| Protocol Feature | OSPFv2 | OSPFv3 |
|---|---|---|
| Distance Vector / Link State | Link State | Link State |
| Routed Protocol Supported | IPv4 | IPv6 |
| VLSM Support | Yes | Yes |
| Router ID | 32 bit Binary ID | 32 bit Binary ID |
| Metric Value | Cost (Based on Bandwidth) | Cost (Based on Bandwidth) |
| How DR and BDR are elected | Based on highest priority value and then highest RID | Based on highest priority value and then highest RID |
| OSPF multicast all routers IP address | 224.0.0.5 | FF02::5 |
| OSPF DR and BDR multicast IP address | 224.0.0.6 | FF02::6 |
| Support for multiple OSPF instances per interface | Not available | Available |

# OSPF Protokolü (terimler)

- Loopback Interface (Lo0): Geridöngü arabirimi, yönlendiricideki mantıksal ve sanal bir arabirimdir. Yöneltici, varsayılan olarak herhangi bir geridöngü arabirimine sahip değildir, ancak kolayca oluşturulabilir. Genel olarak teşhis ve sorun giderme için ve yerel makinede çalışan sunuculara bağlanmak için kullanılır. Bu arayüzler yönlendiricideki fiziksel arayüzler olarak değerlendirilir ve onlara ip adresleri atayabiliriz.

  *Yönlendirici (Config) #int loopback 2*

  *Yönlendirici (Config-if) #ip adresi 200.0.0.10 255.255.255.0*

- Area border router (ABR): Alan sınırı yönlendiricisi (ABR), bir veya daha fazla OSPF alanını ana omurga ağına bağlayan bir yönlendiricidir. Bağlı olduğu tüm alanların bir üyesi olarak kabul edilir.
- Internal router: Dahili Yönlendirici, aynı bölgedeki yönlendiricilerle yalnızca OSPF komşu ilişkileri olan bir yönlendiricidir.

# OSPF Protokolü (terimler)

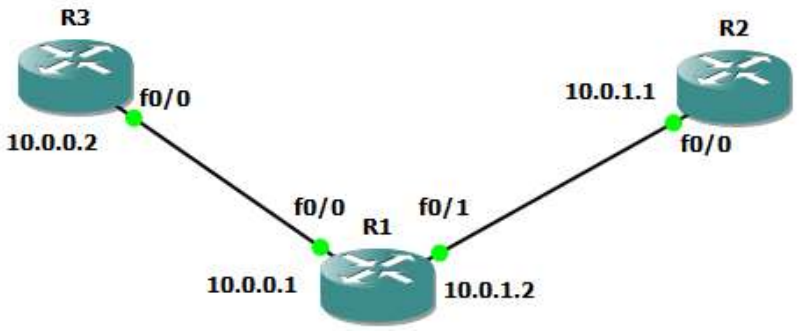
- Backbone router: Omurga Yönlendiricileri OSPF omurgasının bir parçasıdır. Bu, tüm alan sınır yönlendiricilerini ve ayrıca farklı alanları bağlayan yönlendiricileri de içerir.
- Designated Router (DR) and Backup Designated Router (BDR): Özel Yönlendirici (DR), bir ağ bölümündeki tüm yönlendiriciler arasında seçilen yönlendirici arabirimidir ve Atanmış Yedekleme Yönlendiricisi (BDR), Atanmış Yönlendirici (DR) için yedekleme yapar. Özel Yönlendiriciler (DR), yönlendirme güncellemeleri için bir kaynak sağlayarak ağ trafiğini azaltmak için kullanılırlar. Özel Router (DR) ağın tam bir topoloji tablosunu tutar ve güncellemeleri diğer yönlendiricilere,  multicast yayın yoluyla gönderir. Bir bölgedeki tüm yönlendiriciler, Belirlenmiş Yönlendirici (DR) ile bir slave/master ilişkisi oluşturacaktır.
- The link-state advertisement (LSA): İnternet Protokolü (IP) için OSPF yönlendirme protokolünün temel bir iletişim aracıdır. Yönelticinin yerel yönlendirme topolojisini, aynı OSPF alanındaki diğer tüm yerel yönlendiricilere iletir.

# OSPF Protokolü

- OSPF: (1 - 65535) aralığında, yereldeki process-id ile birlikte listelenen işlemler için OSPF yapılandırma moduna girer. Joker maskesi ile birlikte ağ adresi, bu ağ komutunu kullanılarak OSPF için etkinleştirilecek arabirim veya arabirim aralığını belirtmek için kullanılır.

*Router (config) # router ospf <process-id>*

*Router (config) # network <network address> <wild-card mask>  area <area number>*



# OSPF Protokolü

- OSPF protokolü için show komutunun seçenekleri aşağıdaki gibidir :

*Router02#sh ip ospf ?*

| | |
|---|---|
| *<1-65535>* | *Process ID number* |
| *border-routers* | *Border and Boundary Router Information* |
| *database* | *Database summary* |
| *interface* | *Interface information* |
| *neighbor* | *Neighbor list* |
| *virtual-links* | *Virtual link information* |

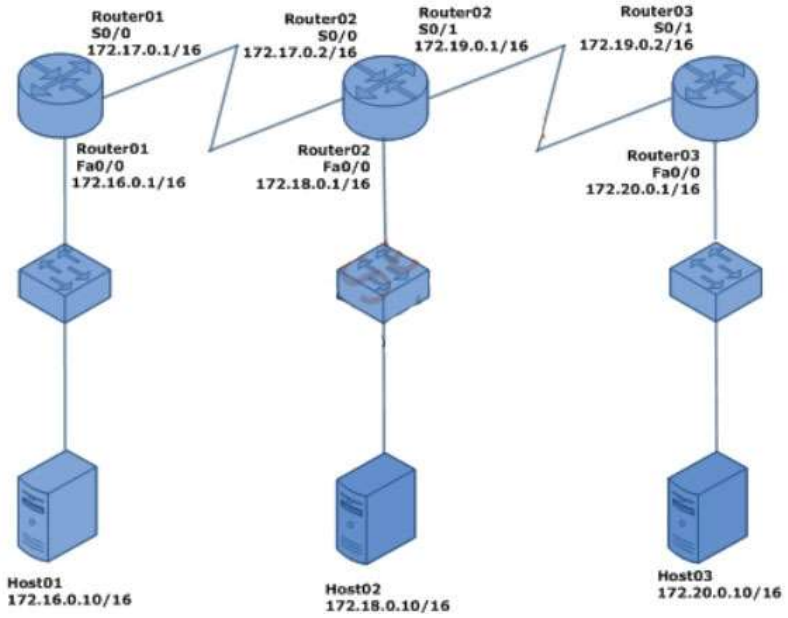
*Router#sh ip route*

*Router#sh ip protocols*

*Router#sh running-config*

# OSPF Protokolü

ÖRNEK : Aşağıdaki gibi bağlı üç yönlendiricimiz, üç anahtarımız ve üç ana makinemiz için **OSPF routing** ayarlarını yapalım.

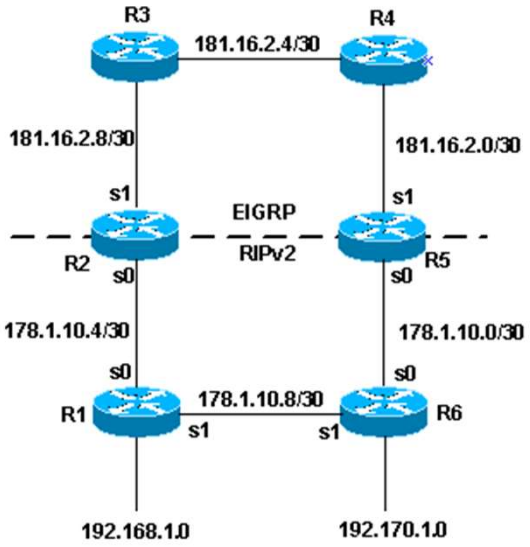


# Varsayılan Yönetimsel Uzaklık Değerleri

**Default Administrative Distances**

| Route Source | Administrative Distance |
|---|---|
| Connected | 0 |
| Static | 1 |
| EIGRP summary route | 5 |
| External BGP | 20 |
| Internal EIGRP | 90 |
| IGRP | 100 |
| OSPF | 110 |
| IS-IS | 115 |
| RIP | 120 |
| External EIGRP | 170 |
| Internal BGP | 200 |

# Redistribute



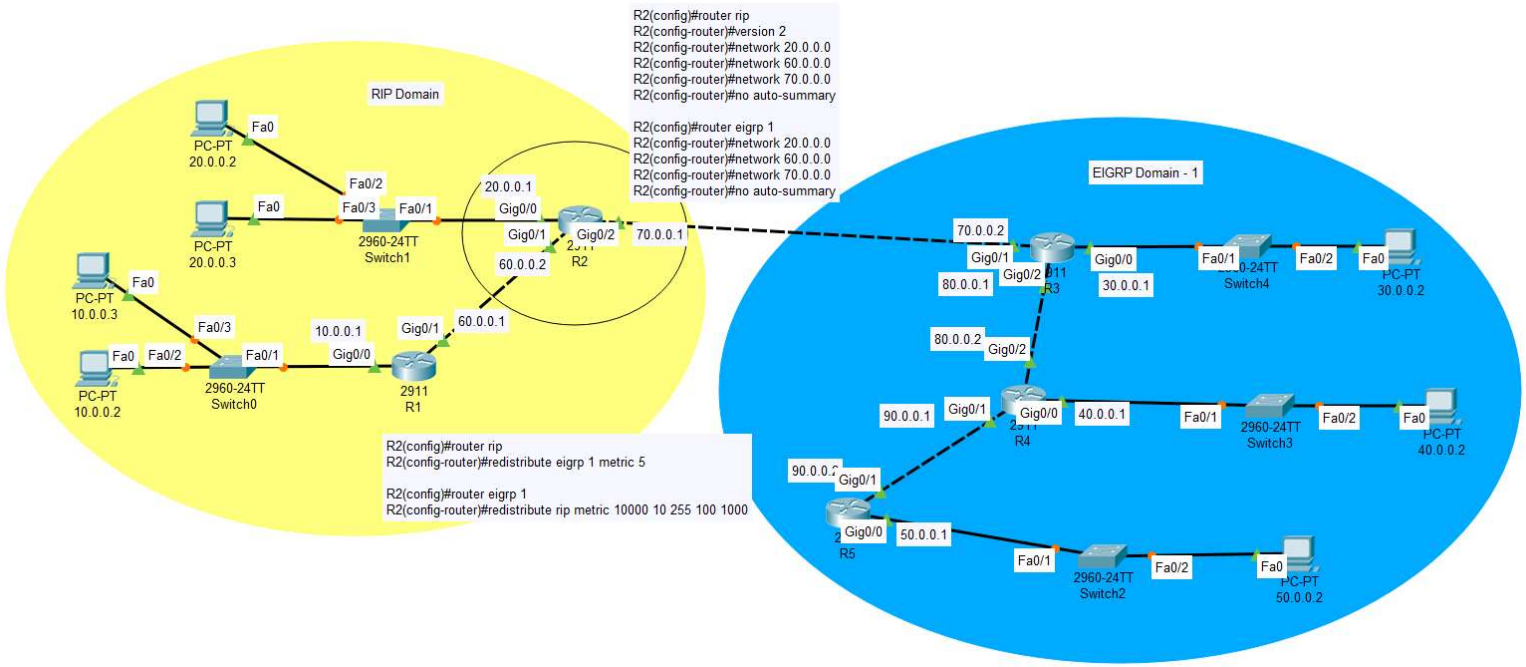

*redistribute protocol metric {metric info}*

Bu komut, OSPF içine RIP veya RIP içine statik gibi yönlendirme işlemini farklı bir kaynaktan yapılandırılmış yönlendirmeyi yeniden dağıtacak şekilde yapılandırmak için RIP, EIGRP veya OSPF yönlendirici yapılandırma modu içerisinde yürütülür.

Bir rotanın kullanılması için bir buna ilişkin metrik belirlenir. Örneğin, RIP atlama sayıları kullanır, OSPF maliyeti kullanır ve EIGRP K Değerlerini kullanır (bant genişliği, yük, gecikme, güvenilirlik, mtu)

# Redistribute

ÖRNEK : EIGRP, RIP, OSPF, Static yönlendirmelerinin kendi aralarında redistribution yapılması çalışmaları gerçekleştirilecek.

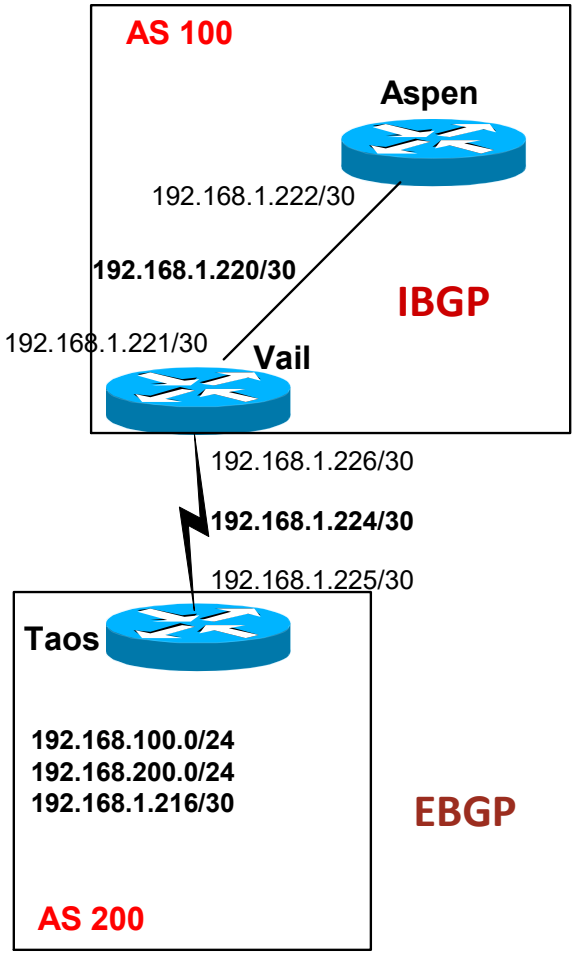


# BGP Protokolü

**Border Gateway Protocol (BGP)**

Routing Protokoller IGP ve EGP olarak ikiye ayrılır. IGP protokolleri aynı AS (Autonomous System) leri haberleştirirken, EGP'ler ise farklı AS leri haberleştirir.

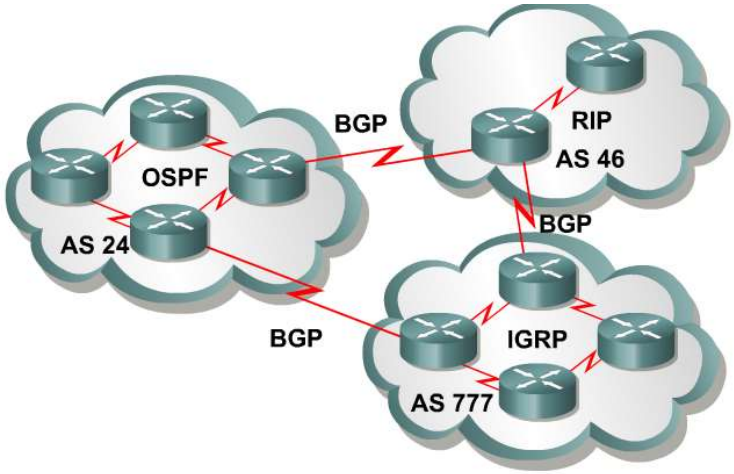
- IGP (İç Ağ Geçidi Protokolü) - RIP, IGRP, EIGRP, OSPF = Özerk bir sistem içinde yönlendirme bilgilerini değiştirmek için kullanılan yönlendirme protokolleridir.
- EGP (Dış Ağ Geçidi Protokolü) - BGP = Özerk sistemler arasında yönlendirme bilgisi alışverişinde kullanılan yönlendirme protokolleridir.
- AS (Autonomous System) içindeki paketleri yönlendirmek için bir IGP ve ortak ölçütler kullanarak paketleri diğer AS'lere yönlendirmek için bir EGP kullanılır.
- BGP protokolü bir yol vektörü (path vector) veya bir ileri mesafe vektörü yönlendirme (advanced distance vector routing) protokolü olarak adlandırılabilir.

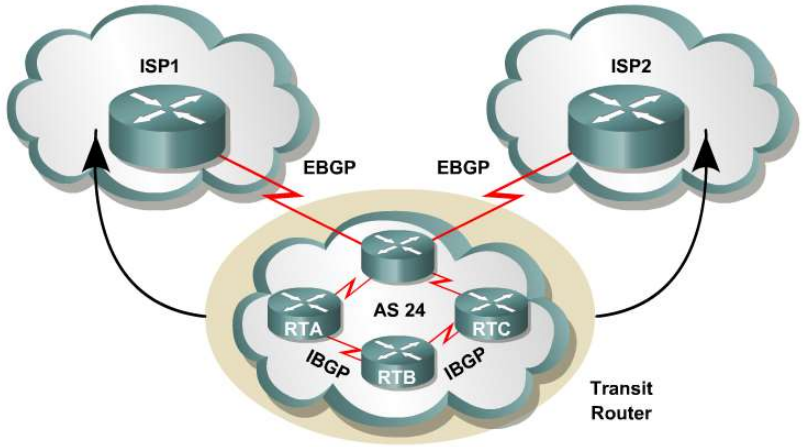



# BGP Protokolü

- BGP, RFC 1772 ile tanımlanmıştır.
- BGP aslında bir mesafe vektörü yönlendirme protokolüdür, çünkü yönlendirme tablosundan güzergahlar boyunca geçiş yapmak için akış aşağı komşulara dayanır.
- BGP, bir paketin hedefe ulaşmak için geçmesi gereken AS numaraları listesini kullanır.
- BGP bir AS içerisinde çalışırken, Dahili BGP (IBGP) olarak adlandırılır. Bir BGP yönlendiricisinin rolü IBGP trafiğini yönlendirmekse, buna transit yönlendirici adı verilir.
- BGP özerk sistemler arasında çalıştığında, Harici BGP (EBGP) olarak adlandırılır. Bir AS'nin sınırına oturan ve ISS ile bilgi alışverişinde EBGP'yi kullanan yönlendiricilere sınır yönlendiricileri denir.

# BGP Protokolü

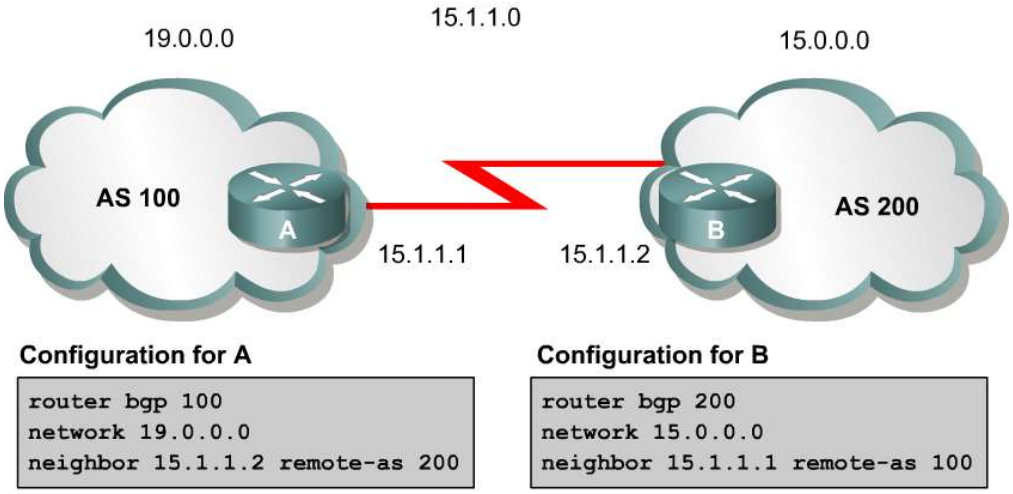



Aşağıdaki koşullardan biri mevcutsa, BGP kullanılır:

- AS, paketlerin bir başka AS'ye (transit AS) ulaşmak için içinden geçmesine izin vermesi gerekiyorsa,
- AS (Autonomous System)'nin diğer AS'lerle birden fazla bağlantısı varsa,
- AS'ye giren veya çıkan trafik akışı yönlendirilmek isteniyorsa.

# BGP Protokolü



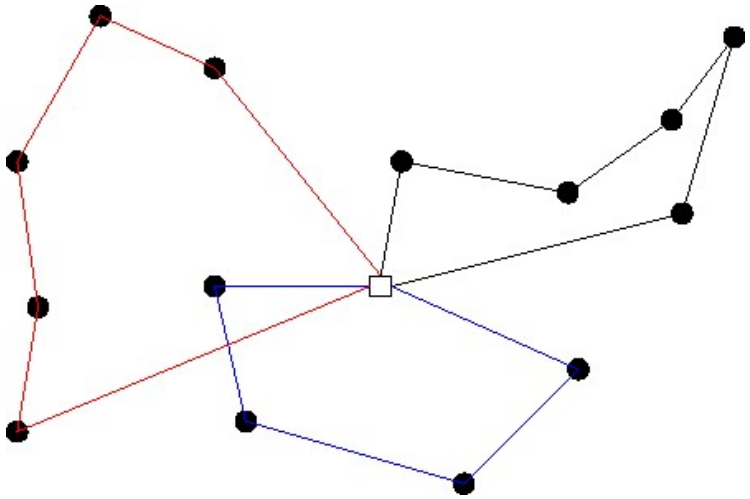

NEXT HOP: Bu özellik, RIP gibi bir IGP açısından, rotayı açıklayan yönlendiricinin (router) IP adresidir. Bir sonraki sıçrama (next-hop), farklı AS'ler arasında rotanın öğrenildiği EBGP komşusunun IP adresidir.

BGP işlemini yapılandırmaya başlamak için aşağıdaki komut dizini kullanılır:

*Router(config)#router bgp AS-number*

BGP yapılandırma komutları, tanıdık IGP (örneğin, RIP, OSPF) komutlarının sözdizimi ile benzerdir.

Not: Cisco IOS, bir seferde yalnızca bir BGP işleminin çalışmasına izin verir, bu nedenle bir yönlendirici birden fazla AS'ye ait olamaz.

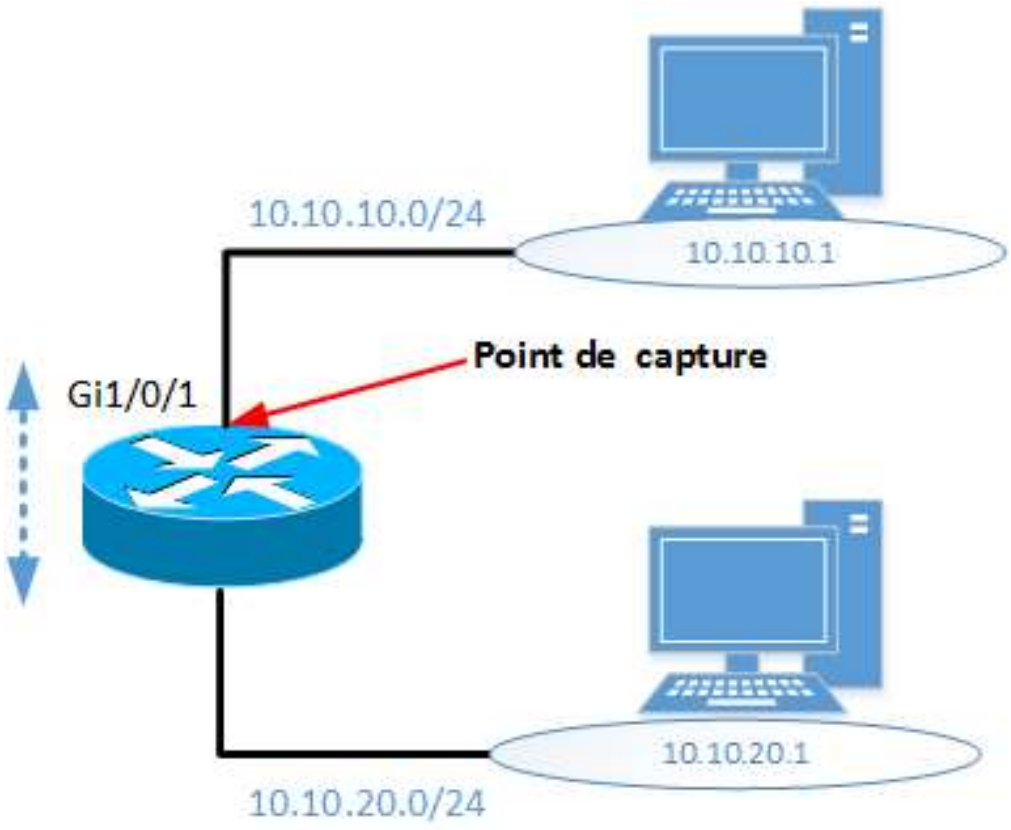


# Dinamik Yönlendirme

Dinamik yönlendirme Sorunları :

Bütün bunlarla birlikte, dinamik yönlendirme protokollerinin mükemmel olduğu düşünülmemelidir. Aşağıdaki durumlar olası karşılaşılabilecek sorunlardandır :

- Yönlendiriciler, yönlendirme tablolarını tutmak ve dinamik rotaları hesaplamak için daha fazla CPU ve RAM'e ihtiyaç duyabilirler.
- Dinamik yönlendirme protokolleri mükemmel değildir ve bazı durumlarda yönlendirme döngüleri (loop) içine girebilirler.
- Dinamik yönlendirme protokolleri ağınıza karmaşıklık getirecektir. Yeni dinamik yönlendirme protokollerini nasıl yapılandıracağınızı ve sorunları nasıl gidereceğinizi anlamanız gerekecektir.




# ACL (cisco)

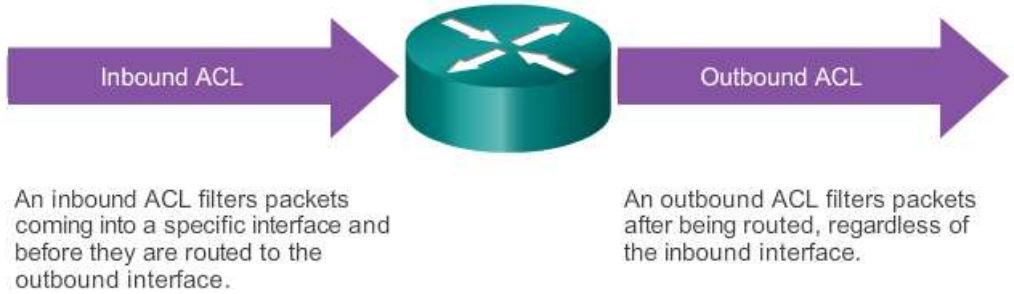
Erişim Denetim Liste (Access Control List) özelliği cisco yönlendiricilerde bulunmaktadır ve spesifik bir IP, subnet ya da tüm networkün başka bir IP, subnet veya  belli bir IP ye erişimini kontrol ederler.

Bunun yanı sıra ftp, http, smtp gibi network hizmetlerine erişimini de denetleyebilirler. Aslında ACL'ler bir çeşit güvenlik duvarıdır.

# ACL (cisco)

ACL'ler Standart ve Extended olmak üzere iki ana başlıkta incelenebilir:

- Standard ACL, sınırlı seviyede denetim sağlama izni verir. Standard ACL'ler bir IP adresi, bir IP bloğu ya da bir alt ağın hangi IP'lere veya alt ağlara erişebileceğinin denetimini yaparlar. Clasful veya clasless IP ağları için standart ACL'ler kullanılabilirler.
- Extended ACL ise standard ACL in yapabildiği şeylere ek olarak, kullanacağınız ya da yasaklayacağınız protokolleri de belirlemenize olanak tanır. Örneğin, 80 numaralı portu tanımlayarak http hizmeti için gerekli tanımlara yapılabilir.



# ACL (cisco)

**Standart Access List**

Router üzerine gelen paketlerin kaynak ip adresine bakılarak engelleme işleminin yapılmasıdır. İzin verme ya da yasaklama aksiyonu tüm protokol kümesini kapsar. Standart ACL, lokasyon olarak, filtrelenen ağda mümkün olduğunca hedefe yakın biçimde oluşturulmalıdır.

*Router(config)# access-list {access list number} {deny – permit} {source ip adress} {wildcard mask}*

- Access list numarası : 1 – 99 veya 1300 – 1999 arasında bir numara seçilmelidir.
- Deny: Yasaklamak için kullanılması gereken aksiyonu belirtmektedir.
- Permit: İzin vermek için kullanılması gereken aksiyonu belirtmektedir.
- Source ip: Belirlenen aksiyonun uygulanacağı kaynak ip adresidir.
- Wildcard Mask: Kaynak IP adresine ait subnet maskesinin tam tersi olarak yazılması gereken değerdir.

# ACL (cisco)

Standart ACL örnekler:

- 192.168.1.10 ipsine sahip bilgisayarın dışarıya çıkışı yasaklansın.

*Router(config)# access-list 1 deny 192.168.1.10 0.0.0.0*

- 192.168.1.20 ipsine sahip bilgisayarın dışarıya çıkışı yasaklansın.

*Router(config)# access-list 1 deny 192.168.1.20 0.0.0.0*

- Bu kriterlerin dışında kalan trafik devam etsin.

*Router(config)# access-list 1 permit any*

# ACL (cisco)

**Extended Access List**

Router üzerine gelen ip paketlerinin hem kaynak hemde hedef ip adresleri kontrol edilir. Extended ACL, lokasyon olarak, filtrelenen ağda mümkün olduğunca kaynağa yakın biçimde oluşturulmalıdır.

*Router(config)# access-list {Access List Number} {Deny – Permit} {Protocol} {Source IP Address} {Destination IP Adress} {Wildcard Mask} {eq – lt – gt – neq} Port Number*

- Access list numarası : 100 – 199 ve 2000 – 2699 arasında bir numara seçilmelidir.
- Deny: Yasaklamak için kullanılması gereken aksiyonu belirtmektedir.
- Permit: İzin vermek için kullanılması gereken aksiyonu belirtmektedir.
- Source IP: Kaynak IP adresi.
- Destination IP: Hedef IP adresi

# ACL (cisco)

Wildcard Mask anahtar terimler :

Example 1:

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

Example 2:

```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

- Wildcard Mask: Kaynak IP adresine ait subnet maskesinin tam tersi olarak yazılması gereken değerdir.

| | | |
|---|---|---|
| **0.0.0.0** | **Keeps all bits** | **Keyword is: Host** |
| **255.255.255.255** | **Eliminates all bits** | **Keyword is : ANY** |

- Port Number: Port Numarası için aşağıdaki saçenekler kullanılabilir.
  - eq (equal): Eşittir.
  - lt (less than): Küçüktür.
  - gt (greater than): Büyüktür.
  - neq (not equal): Eşit degildir.

# ACL (cisco)

Extended ACL için örnekler:

- 172.168.1.222 ip'sine sahip bilgisayarın 192.168.1.53 ip adresini kullanmakta olan bilgisayara 23 (telnet) numaralı porttan erişimi yasaklansın.

*Router(config)# access-list 110 deny tcp 172.16.1.222 0.0.0.0 host 192.168.1.53 eq 23*

- 172.16.1.11 ipsini kullanmakta olan bilgisayar ise 192.168.1.0 /24 networküne erişim gerçekleştiremesin.

*Router(config)# access-list 110 deny tcp host 172.16.1.11 192.168.1.0 0.0.0.255*

- 172.16.1.34 ipsini kullanmakta olan bilgisayar 192.168.1.46 ipsini kullanan bilgisayara 25 numaralı portu kullanan SMTP protokolü üzerinden erişemesin.

*Router(config)# access-list 110 deny tcp host 172.16.1.34 host 192.168.1.46 eq 25*

- Yukarıdaki kısıtlamaların dışında kalan trafik devam etsin.

*Router(config)# access-list 110 permit ip any any*

# ACL (cisco)

*Standard ACLs*

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

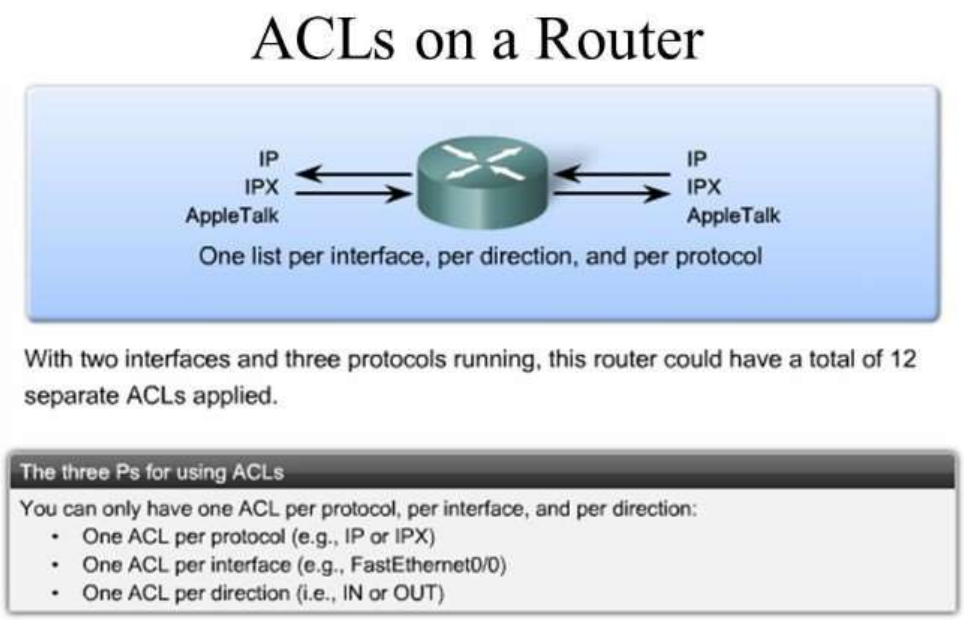
Standard ACLs filter IP packets based on the source address only.

*Extended ACLs*

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Extended ACLs filter IP packets based on several attributes, including the following:

- Source and destination IP addresses
- Source and destination TCP and UDP ports
- Protocol type/ Protocol number (example: IP, ICP, UDP, TCP, etc.)




# ACL (cisco)

ACL oluşturma yönergeleri (üç ps kuralı):

- Protokol başına bir ACL - Bir arabirimdeki trafik akışını kontrol etmek için, arabirimde etkin olan her protokol için bir ACL tanımlanması gerekir.
- Yön başına bir ACL - ACL'ler bir arabirimde bir seferde bir yönde trafiği kontrol eder. Gelen ve giden trafiği kontrol etmek için iki ayrı ACL oluşturulmalıdır.
- Arabirim başına bir ACL - ACL'ler, bir arabirim için trafiği denetler; örneğin, GigabitEthernet 0/0.

# ACL (cisco)

Access List Yazarken dikkat edilecekler :

- ACL yazarken her satırın bir kriteri belirlediğine dolayısı ile satır sıralamalarına dikkat edilmelidir.
- ACL'nin değişmesi gerektiğinde bir text editör kullanılarak düzenlendikten sonra yeninden uygulanması gerekir.
- ACL uygulandıktan sonra "implicit all deny" kuralı bütün trafiği yok edecektir. Yani her ACL ifadesinin sonunda aslın gizli bir «deny» bulunur. Bu kural göz önünde bulundurulmazsa erişim sorunlarına yol açacaktır.
- ACL oluşturulduktan sonra ilgili ara yüze uygulanmalıdır; aksi takdirde çalışmayacaktır.
- Her ara yüz için inbound veya outbound yönüne sadece bir tane ACL uygulanabilir. Aksi takdirde ACL çalışmayacaktır.

# ACL (cisco)

Gelişmiş ACL yöntemleri aşağıdaki gibidir:

- Named ACL: Standart ve extended access list oluşturmanın farklı bir yoludur.
- Switch Port ACL: Port ACL'ler, IP Access list'ler üzerinden IP trafiğini kontrol eder. IP olmayan bir trafik, MAC adresi kullanılarak filtrelenir.
- Lock and Key: Dinamik ACL yöntemidir.
- Reflexive ACL: Bu ACL tipi, üst katman oturum bilgilerine bağlı olarak IP paketlerini filtreler ve genelde dışarı giden trafiğin geçmesine izin verir, fakat gelen trafiği sınırlandırır. Dinamik ACL olarak da bilinir.
- Time-based ACL: Zaman-bağımlı ACL'ler, daha çok extended ACL'ler gibi çalışır. Fakat ACL türü, tamamıyla zaman yönelimlidir.
- Remark: ACL'lerde yaptığınız kayıtlarla ilgili yorum veya çok sayıda açıklama kabiliyeti sağlar.
- Context-based Access Control: Cisco IOS Firewall olarak çalışma özelliğidir.
- Authentication Proxy: Gelen kullanıcılar, giden kullanıcıları veya her ikisine de kimlik doğrulaması yapar. Bu özellik için Cisco IOS firewall özelliği kurulumuna sahip olunmalıdır.

```
Router(config)#ip access-list [standard | extended ] name
```

Alphanumeric name string must be unique and cannot begin with a number.

```
Router(config-std-nacl)#[permit | deny | remark] {source
[source- wildcard]} [log]
```

```
Router(config-if)#ip access-group name [in | out]
```

Activates the named IP ACL on an inteface.

# ACL (cisco)

**Named ACL**

Named ACL kullanarak access-list numarası yerine daha kolay akılda kalacak şekilde isimler belirlenerek listeler yaratılabilir.

Named ACL'yi diğerlerinden ayıran önemli bir özelliği, içerisinde yazılan ve kriterleri belirleyen satırların  ayrı ayrı olarak silinerek ACL'yi tamamen silmeden içeriğini değiştirebilmemizi sağlamasıdır.

Standart veya Extended olarak konfigüre edilebilirler.

# ACL (cisco)

Named ACL için örnekler:

- Named, Standart ACL:

  *Router(config)# ip access-list standard Wissen*

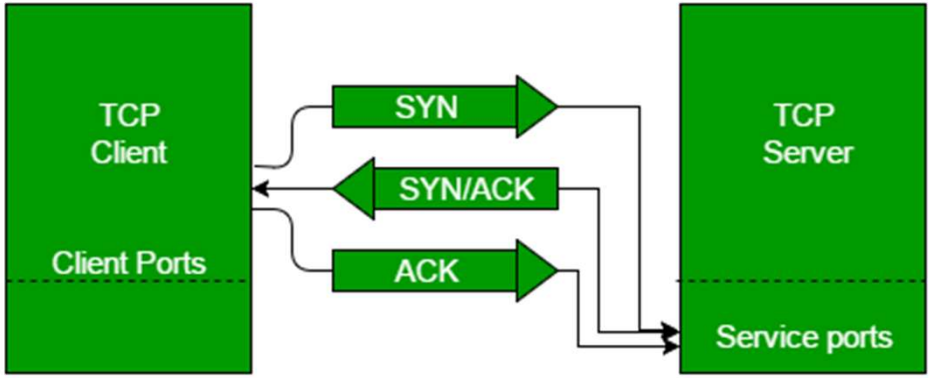
  *Router(config-ext-nacl)# deny tcp host 192.168.1.10 66.249.91.99 0.0.0.0 eq 80*

- Named, Extended ACL:

  *Router(config)# ip access-list extended Cisco*

  *Router(config-ext-nacl)# deny tcp host 192.168.1.10*

# ACL (cisco)




**TCP iletişimi**

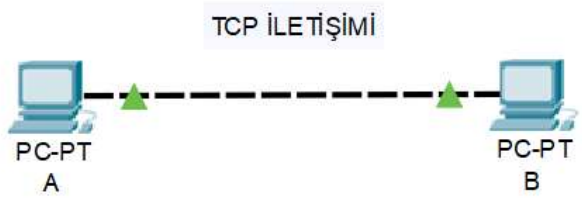
TCP'nin çalışma esası üç faz altında incelenebilir:

1. Öncelikle hedefle bir bağlantı gerçekleşir.
2. Bağlantı gerçekleştikten sonra veri transferi yapılır.
3. Veri transferi yapıldıktan sonra da bağlantı sona erdirilir.

# ACL (cisco)

**TCP bağlantısı nasıl kurulur?**
A bilgisayarı B bilgisayarına TCP yoluyla bağlanmak istediğinde şu yol izlenir:

- A bilgisayarı B bilgisayarına TCP SYNchronize mesajı yollar
- B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP SYN+ACKnowledgement mesajı yollar
- A bilgisayarı B bilgisayarına TCP ACK mesajı yollar
- B bilgisayarı bir ACK "TCP connection is ESTABLISHED" mesajı alır




Üç zamanlı el sıkışma (three-way handshake) adı verilen bu yöntem sonucunda TCP bağlantısı açılmış olur.

# ACL (cisco)

**Veri iletimi**

Bağlantı oluşturulduktan sonra, B bilgisayarı A bilgisayarından paketler almaya başlar. B, her aldığı paketten sonra bir süre bekledikten sonra en son düzgün olarak aldığı paket grubunu A'ya bildirir. Gelen bildirimlere göre A, daha sonra hangi paketleri yollaması gerektiğine karar verir ve yollar. Arada kaybolan paketler (veya paket alındı bilgileri) tekrar tekrar gönderir.

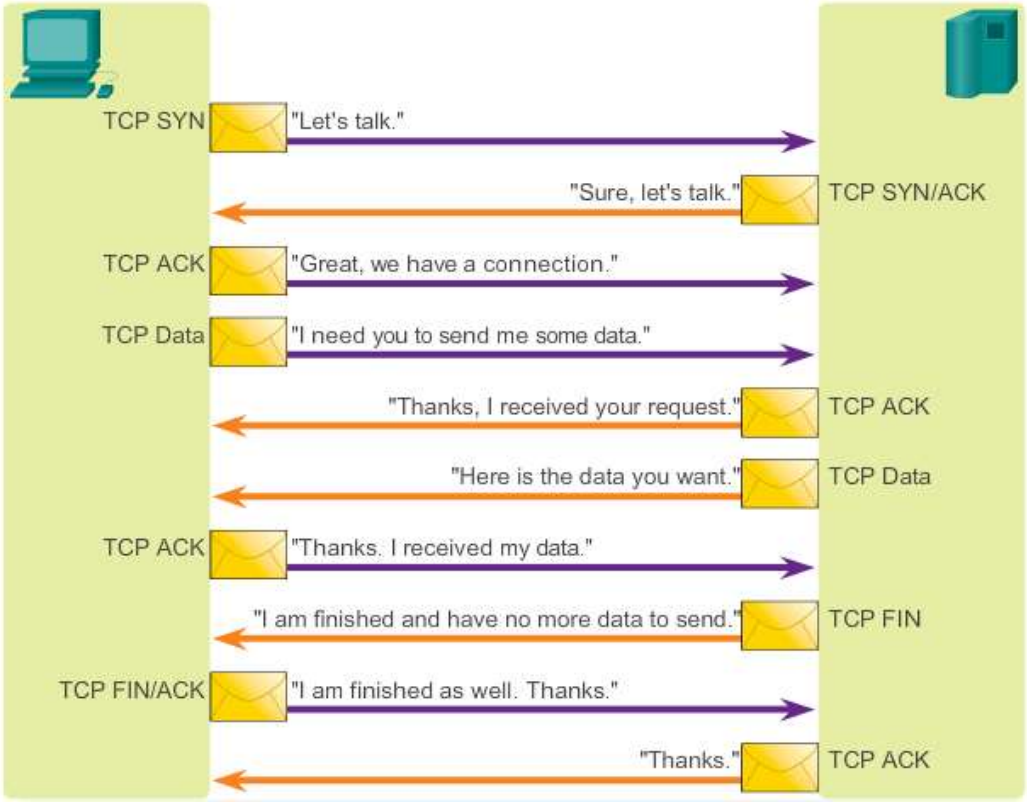
**TCP bağlantısının sona erdirilmesi**

Veri iletişimi bitince bilgisayarlardan herhangi biri diğerine TCP kapatma mesajı yollar. Diğer bilgisayar, kapatmayı teyid etme paketi ve kapatma isteği yollar. Son olarak, diğer bilgisayar da kapatma teyidini yollar ve bağlantı kapatılmış olur.  Bu işlemin adımları tam olarak şöyledir:

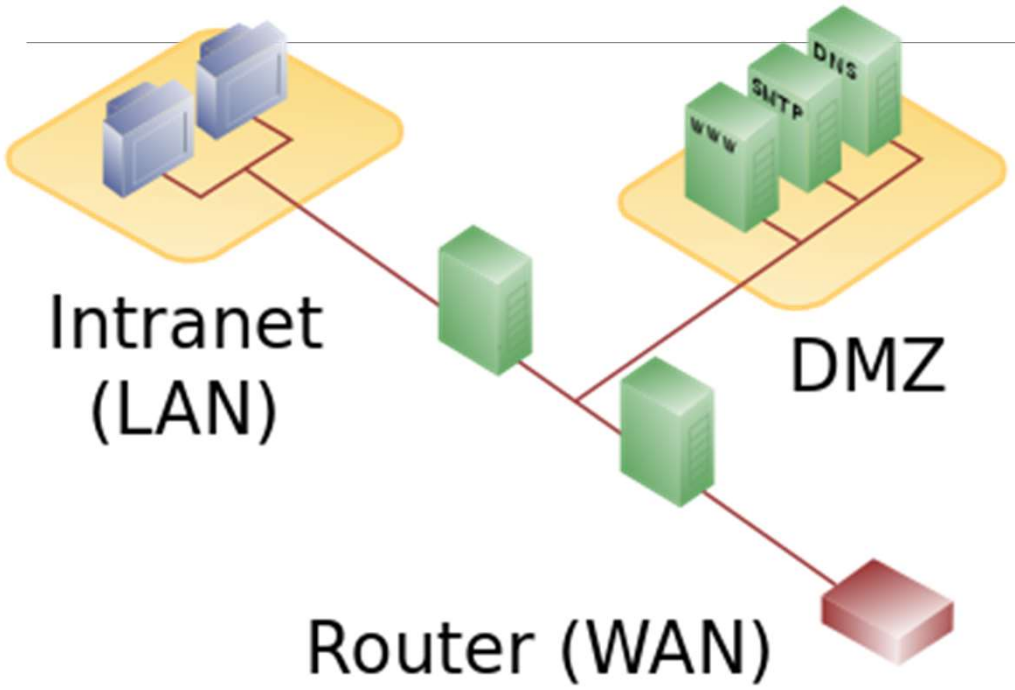
- A bilgisayarı B bilgisayarına bağlantıyı sonlandırmak istediğine dair TCP FIN mesajı yollar.
- B bilgisayarı A bilgisayarına bağlantı sonlandırma isteğini aldığına dair TCP ACK mesajı yollar.
- B bilgisayarı A bilgisayarına bağlantıyı sonlandırmak istediğine dair TCP FIN mesajı yollar.
- A bilgisayarı B bilgisayarına bağlantı sonlandırma isteğini aldığına dair TCP ACK mesajı yollar.

# ACL (cisco)

**TCP iletişimi**

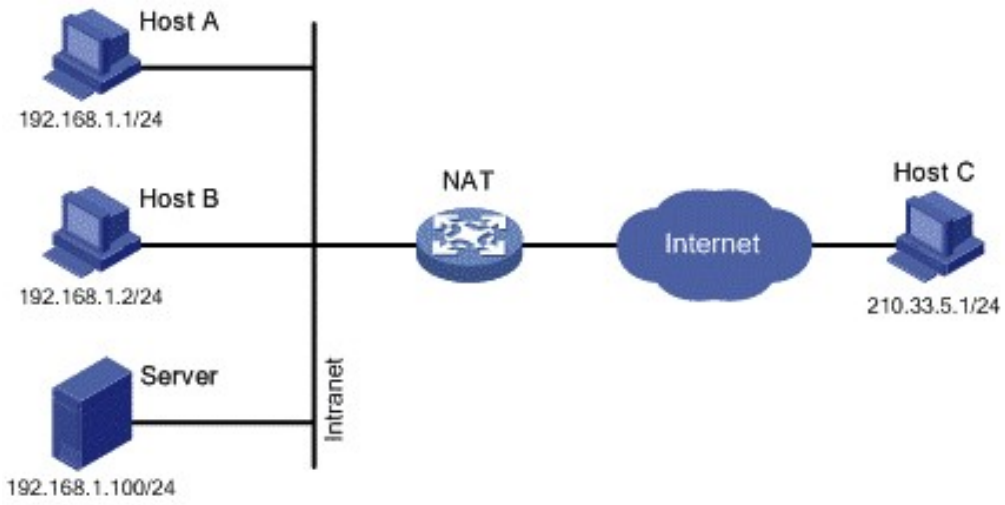


# DMZ (DeMilitarized Zone)




Bilgisayar güvenliğinde DMZ, bir kuruluşun dış servislerini içeren ve bu servisleri daha büyük güvensiz bir ağa (genellikle internet) bağlayan fiziksel veya mantıksal bir alt ağdır.

DMZ'nin amacı bir kuruluşun Yerel Alan Ağı (LAN)'na ek bir güvenlik katmanı eklemektir. Dışarıdaki bir saldırganın ağın herhangi başka bir bölümünden ziyade yalnızca DMZ içindeki ekipmana erişimi vardır.




# NAT (Network Address Translator)

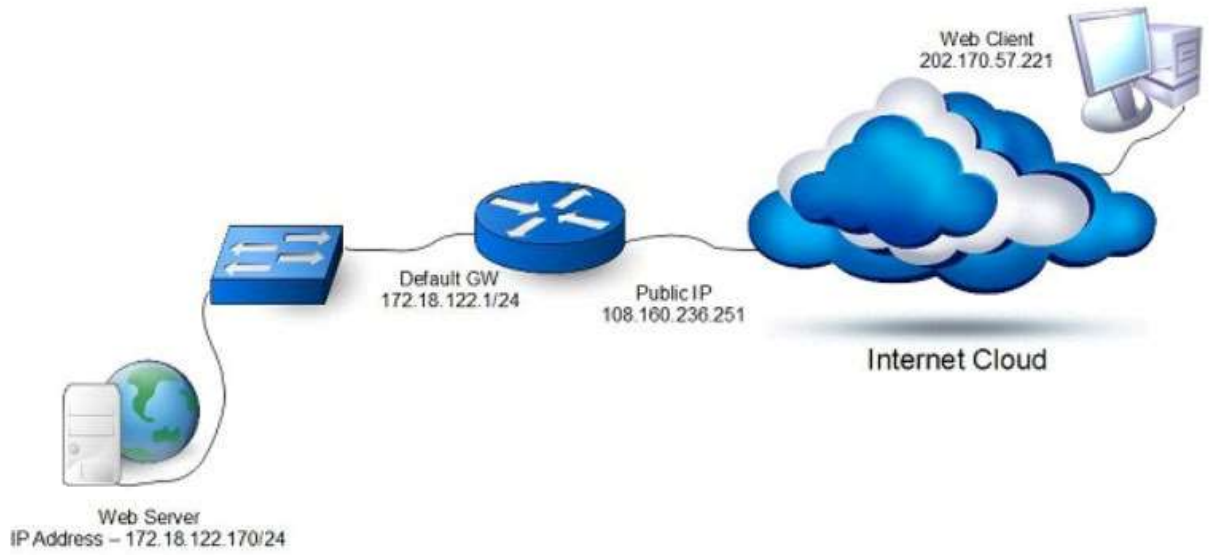
Ağ adresi çeviricisi (NAT), ağ adresi dönüştürme uygulayan ağ geçitleri arasında Internet protokolü bağlantılarının kurulması ve sürdürülmesi için kullanılan bir bilgisayar ağı tekniğidir.

NAT, yerel bir ağdaki (private network) bilgisayarların IP adreslerini tek bir IP adresine (public network) çevirir. Üç çeşit NAT vardır:

1. Statik NAT
2. Dinamik NAT
3. Overload NAT (PAT)

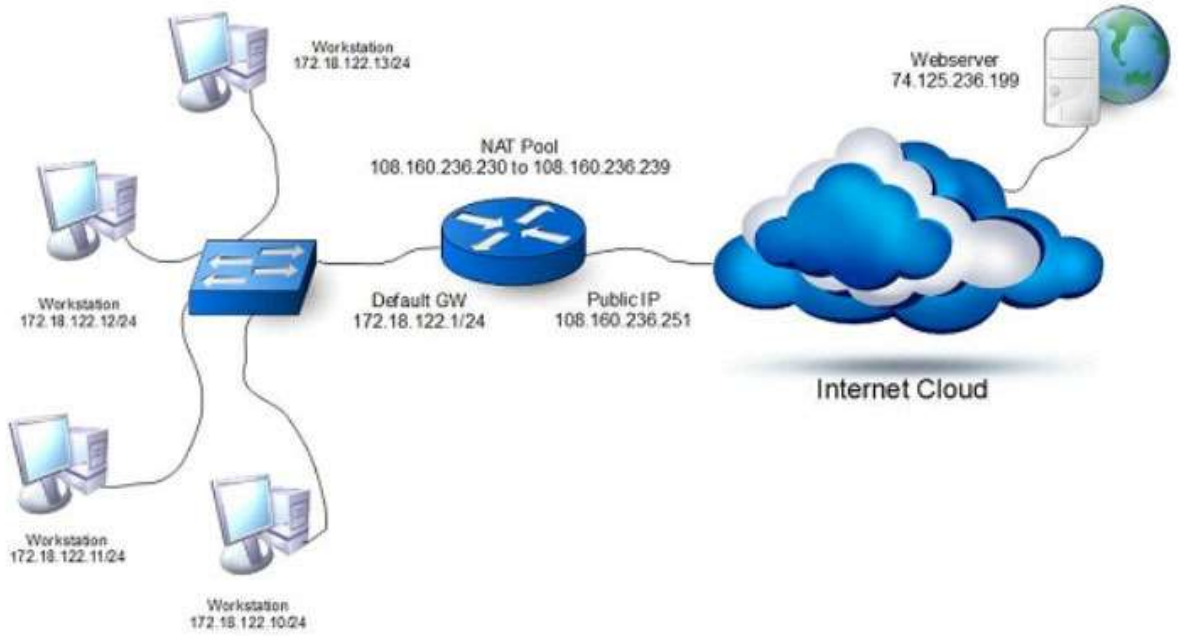
# NAT (Network Address Translator)

1. Static NAT (Network Address Translation) : Statik Ağ Adresi Çevirisi özel bir IP adresinin halka açık bir IP adresine birebir eşlenmesidir.



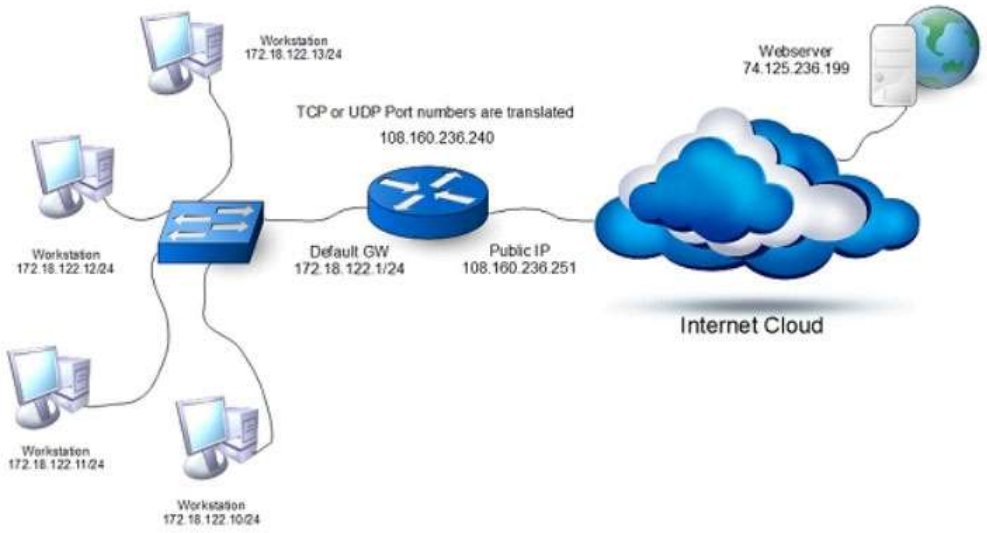
# NAT (Network Address Translator)

2. Dynamic NAT (Network Address Translation) : Dinamik Ağ Adresi Çevirisi, özel bir IP adresinin NAT havuzu olarak adlandırılan bir grup IP adresinden genel IP adresine eşlenmesi olarak tanımlanabilir.



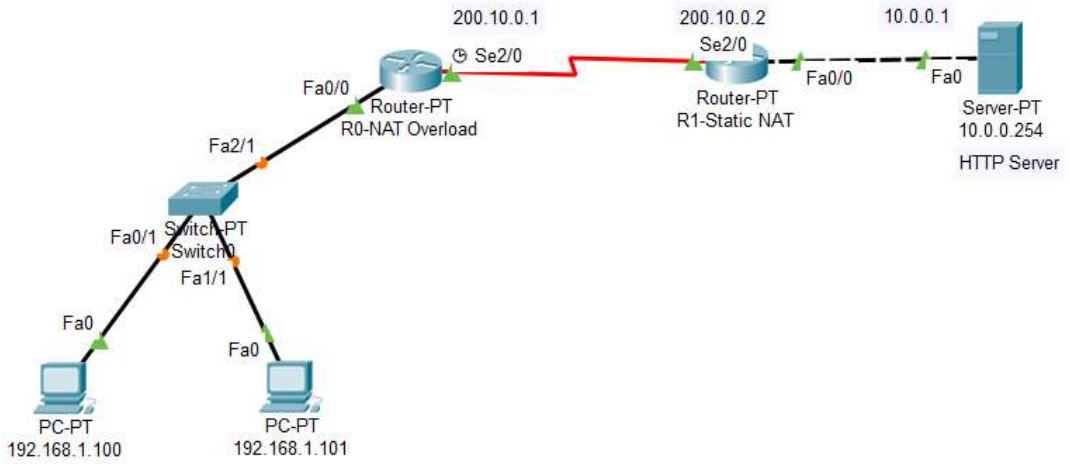
# NAT (Network Address Translator)

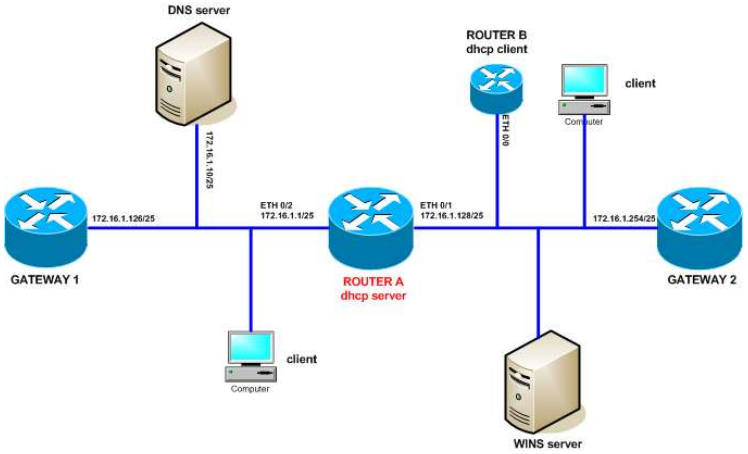
3. PAT (Port Address Translation) : Port Adres Çevirisi, «Port Address Translation» adıyla bilinen bir teknolojiyi kullanarak birden fazla özel IP adresini tek bir genel IP adresine eşleyebilen başka bir dinamik NAT türüdür. Burada, ağ içerisindeki bir istemci İnternet'teki bir ana bilgisayarla iletişim kurduğunda, yönlendirici kaynak bağlantı noktası (TCP veya UDP) port numarasını başka bir bağlantı noktası numarasıyla değiştirir.



# NAT (Network Address Translator)

ÖRNEK: Packet Tracer üzerinde NAT ve PAT uygulama örnekleri.






# DHCP (cisco)

Cisco yönlendiricilerde DHCP servisi :

Dynamic Host Configuration Protocol (DHCP), bir TCP/IP ağındaki cihazlara IP adresleri, alt ağ maskeleri, varsayılan ağ geçitleri vb. ağ yapılandırma parametrelerini dağıtmak için kullanılan bir uygulama katmanı protokolüdür.

DHCP, bir istemci-sunucu mimarisi kullanır. DHCP istemcisi, DHCP sunucusundan ağ parametreleri istemek üzere yapılandırılmıştır. Bir DHCP sunucusu, kullanılabilir bir IP adresleri havuzu ile yapılandırılır ve bu IP adreslerinden birisini DHCP istemcisine atar.

# DHCP (cisco)

Bir Cisco yönlendirici DHCP sunucusu olarak yapılandırılabilir. İşte bunu nasıl yapabilirsiniz:

1. *«ip dhcp excluded-address FIRST_IP LAST_IP»* komutunu kullanarak hariç tutulacak IP adreslerini belirtin,
2. *«ip dhcp pool NAME»* komutunu kullanarak yeni bir DHCP havuzu oluşturun,
3. *«network SUBNET SUBNET_MASK»* komutunu kullanarak ana bilgisayarlara IP adresleri atamak için kullanılacak bir alt ağ tanımlayın.
4. *«default-router IP»* komutunu kullanarak varsayılan ağ geçidini tanımlayın.
5. *«dns-server IP address»* komutunu kullanarak DNS sunucusunu tanımlayın.
6. (İsteğe bağlı, tüm yönlendiricilerde kullanılamaz) «*ip domain-name NAME»* komutunu kullanarak DNS etki alanı adını tanımlayın.
7. (İsteğe bağlı) Kiralama süresini «*lease DAYS HOURS MINUTES»* komutunu kullanarak tanımlayın. Bu parametreyi belirtmezseniz, 24 saatlik varsayılan kiralama süresi kullanılacaktır.

# DHCP (cisco)

ÖRNEK: Aşağıdaki örnekte bir router için DHCP konfigürasyonu verilmiştir.

- 192.168.5.0 - 192.168.5.25 aralığındaki IP adresleri ana makinelere atanmayacak
- DHCP havuzu oluşturuldu ve HQ_DHCP_SERVER olarak adlandırıldı
- Ana makinelere atanan IP adresleri 192.168.5.0/24 aralığında olacaktır.
- Varsayılan ağ geçidinin IP adresi 192.168.5.1
- DNS sunucusunun IP adresi 192.168.5.1'dir.

```
HQ_Router(config)#ip dhcp excluded-address 192.168.5.0 192.168.5.25
HQ_Router(config)#ip dhcp pool HQ_DHCP_SERVER
HQ_Router(dhcp-config)#network 192.168.5.0 255.255.255.0
HQ_Router(dhcp-config)#default-router 192.168.5.1
HQ_Router(dhcp-config)#dns-server 192.168.5.1
```