Network Katmanı (3.Katman) Atakları - Güvenliği - 1

Ağ katmanı - IP

- Farklı Fiziksel segmentlerdeki (LAN- veya farklı ağ) bilgisayarlar arasındaki paketleri taşımak için yapılması gerekenleri tarif eder.
- Bunun için kullanılan temel işlemler;
  - Routing (Yönlendirme): Rota keşfi ve mantıksal adreslemeye göre ağlar arası seyahat.
  - Düşük katmanlardaki adres keşfi işlemi : (Alt katman adresleri arama)
  - Error Messages (ICMP) (Hata mesajlaşma)

TCP/IP protokol yapısı

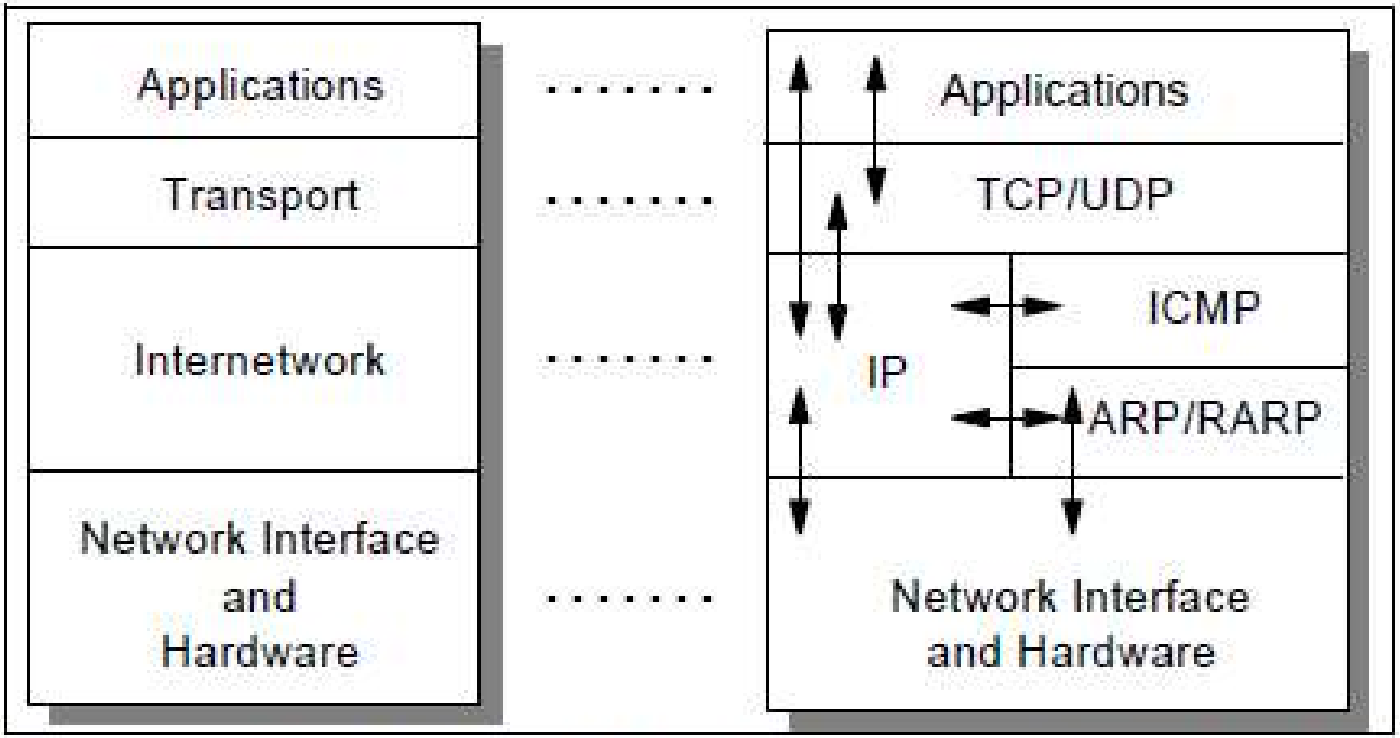
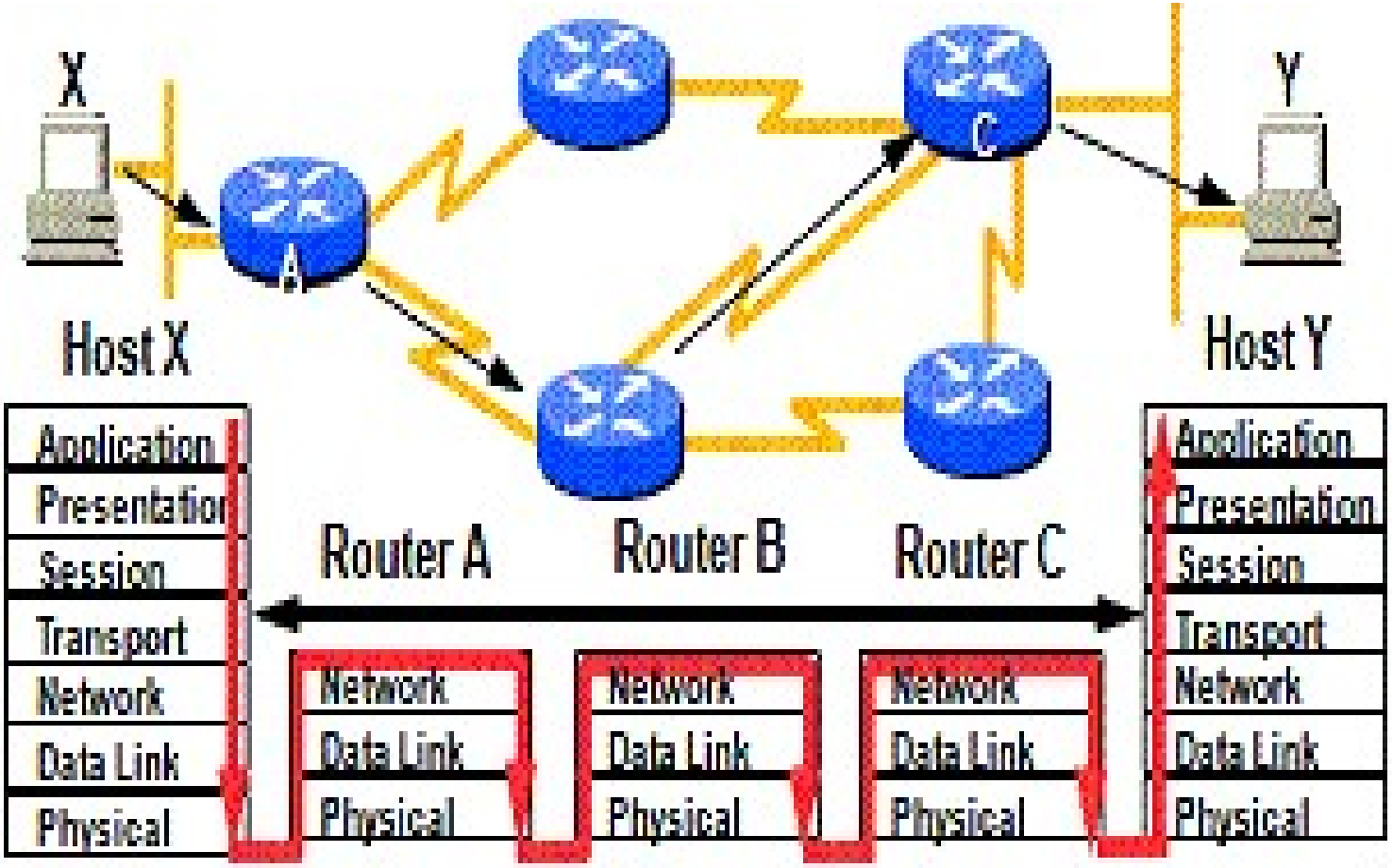
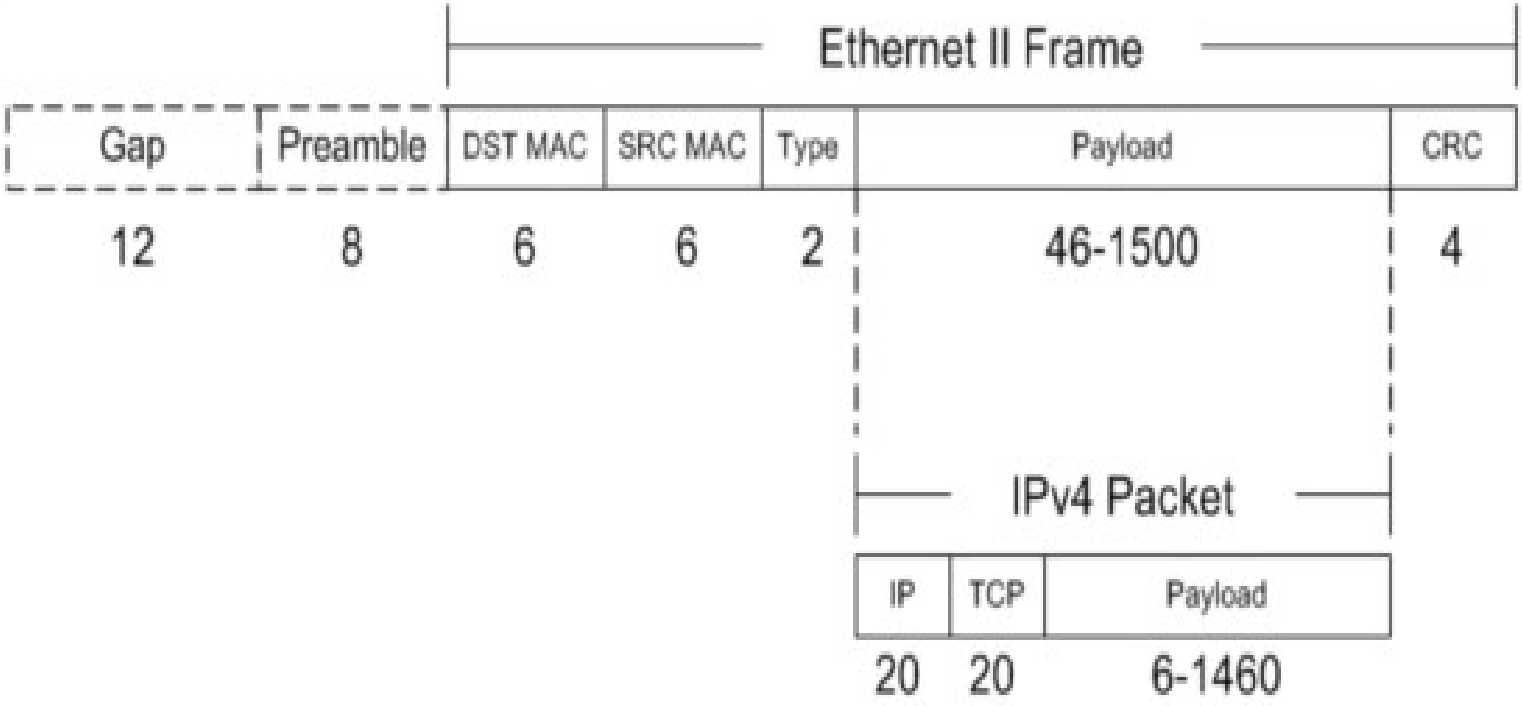


Figure 1-2 The TCP/IP protocol stack: Each layer represents a package of functions

Ağ katmanı- data seyahatı



-


Ethernet II Frame
Gap
Preamble
DST MAC
SRC MAC
Type
Payload
CRC
12
8
6
6
2
46-1500
4
IPv4 Packet
IP
TCP
Payload
20
20
6-1460

IP Paket yapısı

Başlık uzunluğu *satır cinsinden (32bit) verilir. En kısa başlık 5 satır (20 oktet) uzunluğundadır.*

Servis tipi (TOS) Paketin servis sınıfını belirtir.

Toplam Uzunluk *başlık ve verinin toplam uzunluğunu byte* cinsinden verir.

Tanıtıcı ;*parçalanmış IP datagramlarının birleştirilmesinde yardımcı olur.*

DF (Don't Fragment) *biti datagramın parçalanmaması gerektiğini gösterir.*

***MF (More*Fragments)** biti arkadan aynı datagrama ait başka bir parça gelip gelmediğini gösterir.
Son parça dışındaki tüm parçalarda 1 değerine sahiptir.

Parça No *(Fragment kayıklığı* olarak da adlandırılır) ilgili parçanın bütündeki yerini gösterir.

Yaşam Süresi : *Bu* değer her sekmede bi
Değer sıfıra eriştiğinde paket hala varış
ulaşmadıysa yok edilir.

Protokol :*hangi ulaşım protokolünün ku
gösterir.*

Başlık Sınaması *başlıktaki hataları fark
kullanılır..*

Seçenekler :*protokolün daha sonraki sür*

Protokol(8bit): Bir üst düzeyd
popülerleri;

- 1: Internet Control Message P
- 2: Internet Group Managemer
- 6: Transmission Control Proto
- 17: User Datagram Protocol (
- 89: Open Shortest Path First
- 132: Stream Control Transmis

Version (Sürüm- 4 bit)

Decimal	Keyword	Version
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol
5	ST	ST Datagram Mode
6	IPv6	Internet Protocol version 6
7	TP/IX	TP/IX: The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10-14		Unassigned
15		Reserved

0	1	2	3
öncelik			Gecikme

Öncelik Alan Kod

Değer	Öncelik
000	Rutin
001	Öncelikli
010	Acil
011	Flash
100	İvedi
101	Kritik
110	İnter. Kont.
111	Ağ Kont.

Bu alandaki ilk üc bit iletisim öncelikleri yanımlanması içindir. IP katmanı bu alandan aldığı bilgileri iletim katmanına bildirmek zorundadır.

Flash
En büyük öncelik.
Acil (Immediate)
Dört saat içinde.
Öncelikli (Priority)
Aynı gün içinde.
Rutin (Routine)
Bir gün içinde

Servis Alan Kodları ve Anlamları

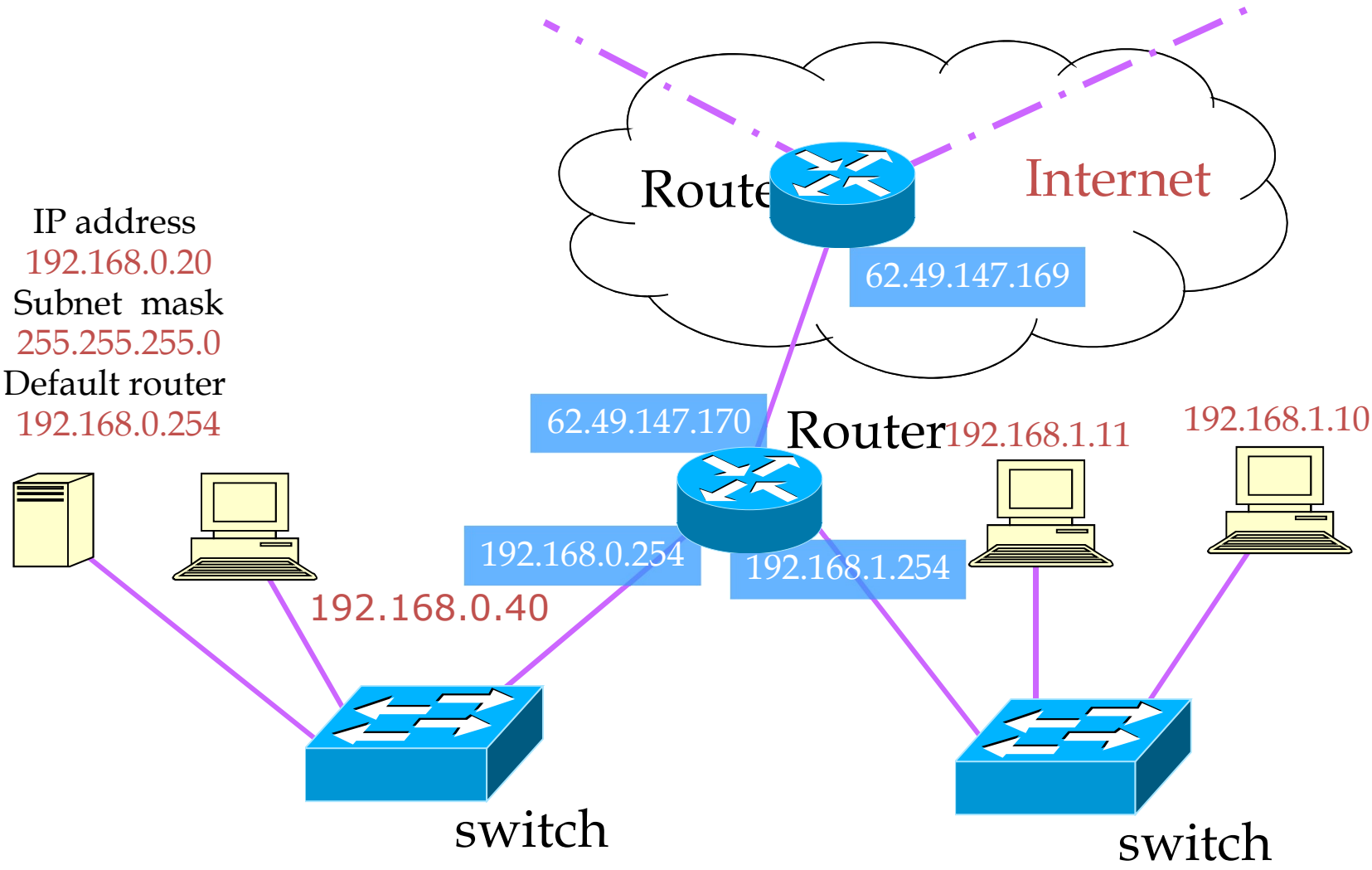
İlk 3 bitin ardından gelen 4 bit ..

Değer	Anlam
1000	Gecikmeleri Azalt
0100	Akış Hızını Arttır
0010	Güvenilirliği Arttır
0001	Etkinliği Arttır
0000	Normal İşlev

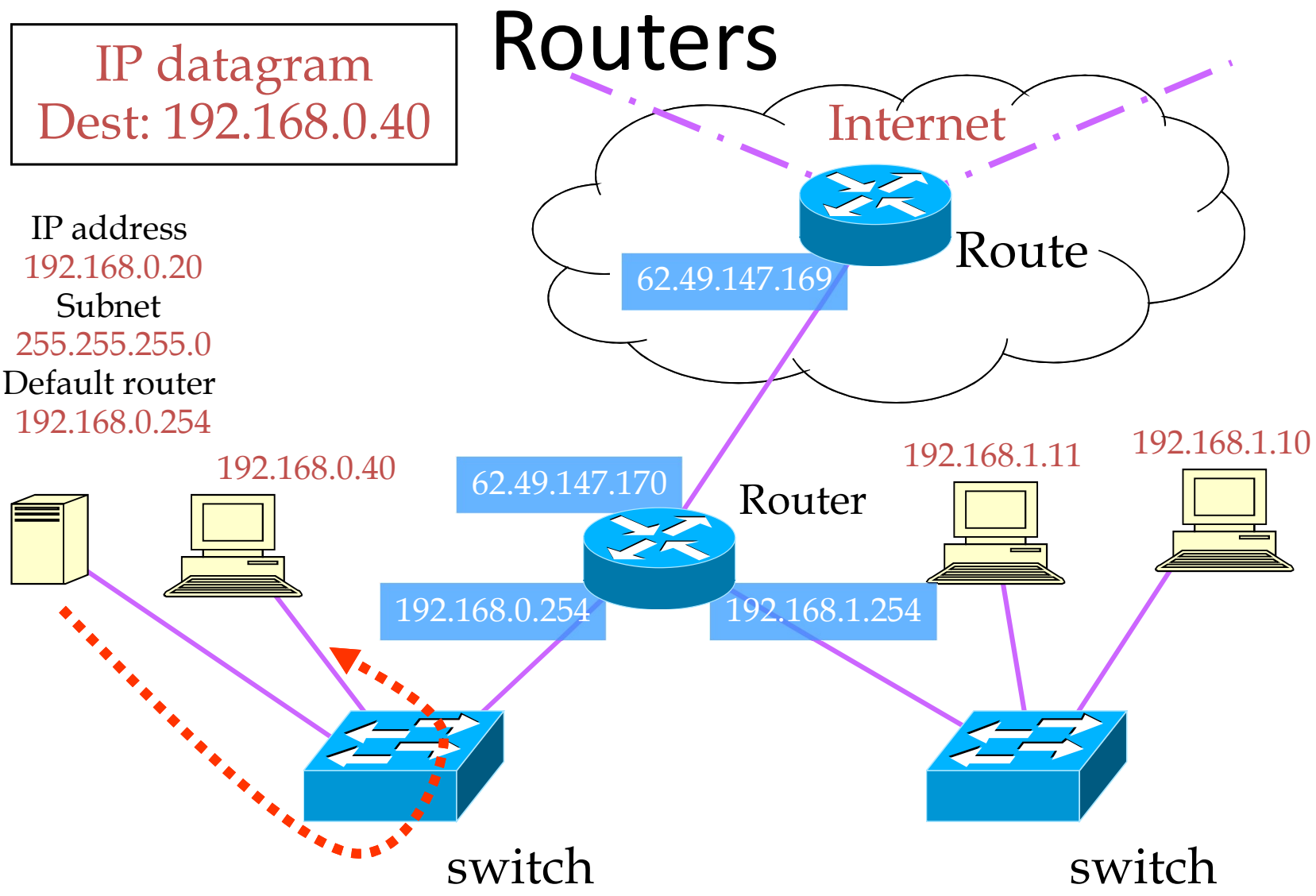
IP Router'lar

- Router'lar ağ katmanında çalışırlar ve ağ adreslerine göre ağdaki paketleri yönlendirirler.
- Router'lar IP datagramlarının yerine teslimini direkt veya dolaylı olarak desteklerler.
- Hedefe varabilecek olası yolları kullanmak için Yönlendirme tablolarını kullanırlar.
- Bir datagram için 3 olası durum sözkonusudur.
  - Doğrudan hedef Host'a gönderilme.
  - Bilinen hedef yolundaki bir sonraki router'a gönderilme.
  - Default Router'a gönderilme.
- IP Routerlar, katman 3'te çalışırlar.

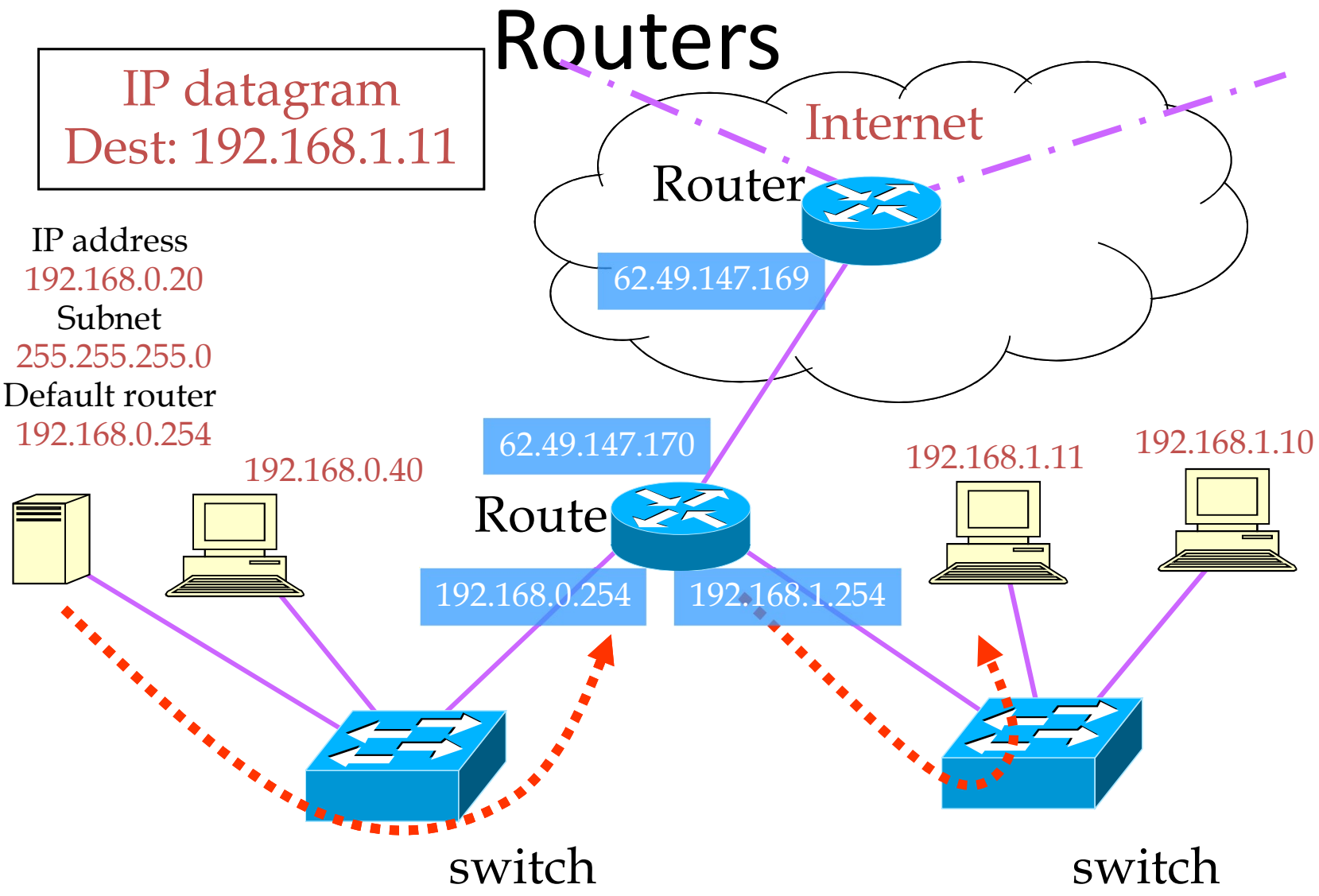
Router'lar


Route
Internet
62.49.147.169
IP address
192.168.0.20
Subnet mask
255.255.255.0
Default router
192.168.0.254
62.49.147.170
Router
192.168.1.11
192.168.1.10
192.168.0.254
192.168.1.254
192.168.0.40
switch
switch

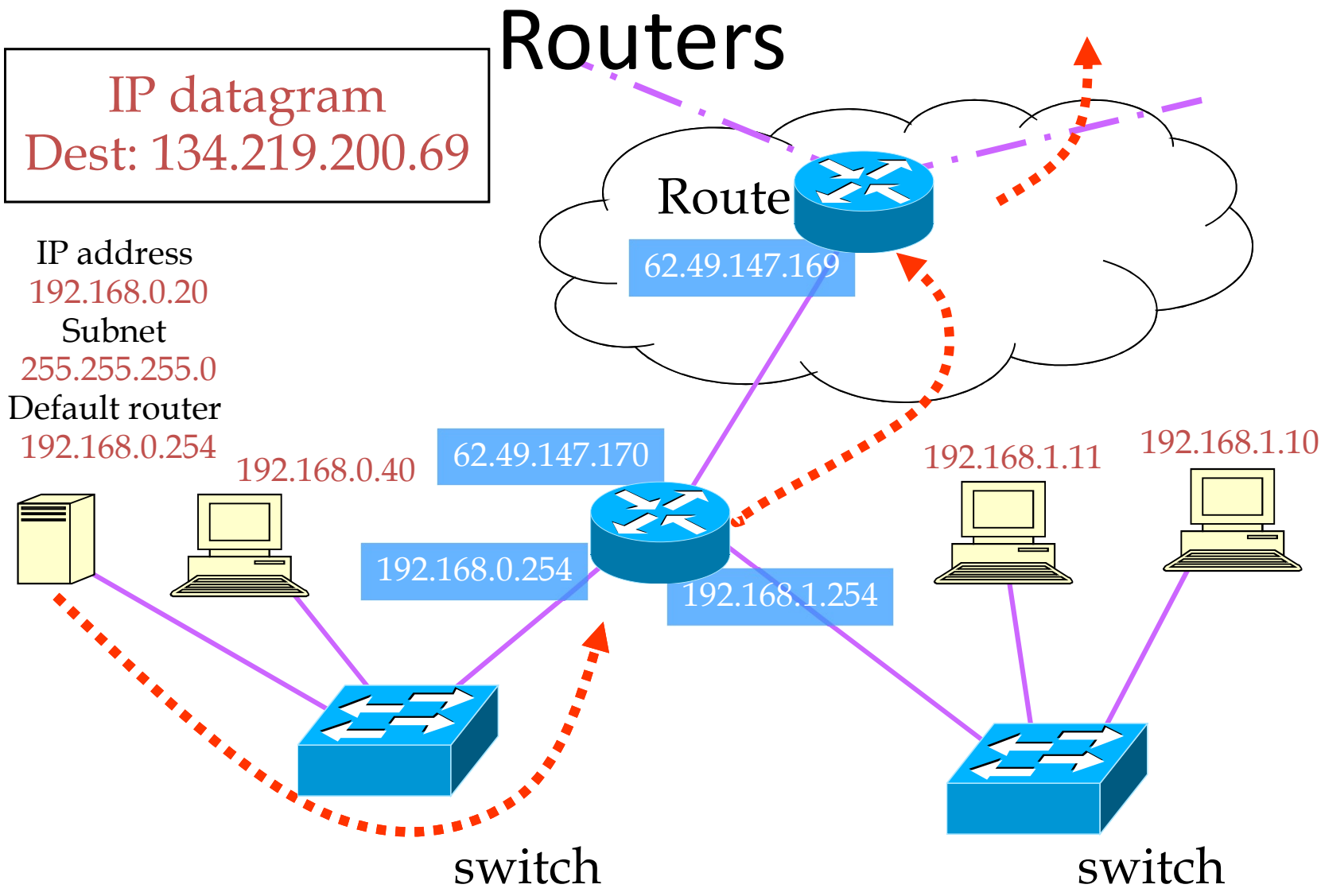
Routers


IP datagram
Dest: 192.168.0.40
IP address
192.168.0.20
Subnet
255.255.255.0
Default router
192.168.0.254
Internet
Route
62.49.147.169
62.49.147.170
Router
192.168.0.40
192.168.1.11
192.168.1.10
192.168.0.254
192.168.1.254
switch
switch

Routers


IP datagram
Dest: 192.168.1.11
Internet
Router
62.49.147.169
IP address
192.168.0.20
Subnet
255.255.255.0
Default router
192.168.0.254
192.168.0.40
62.49.147.170
Route
192.168.1.11
192.168.1.10
192.168.0.254
192.168.1.254
switch
switch

Routers


IP datagram
Dest: 134.219.200.69
IP address
192.168.0.20
Subnet
255.255.255.0
Default router
192.168.0.254
Route
62.49.147.169
192.168.0.40
62.49.147.170
192.168.1.11
192.168.1.10
192.168.0.254
192.168.1.254
switch
switch

ROUTER (YÖNLENDİRİCİ)

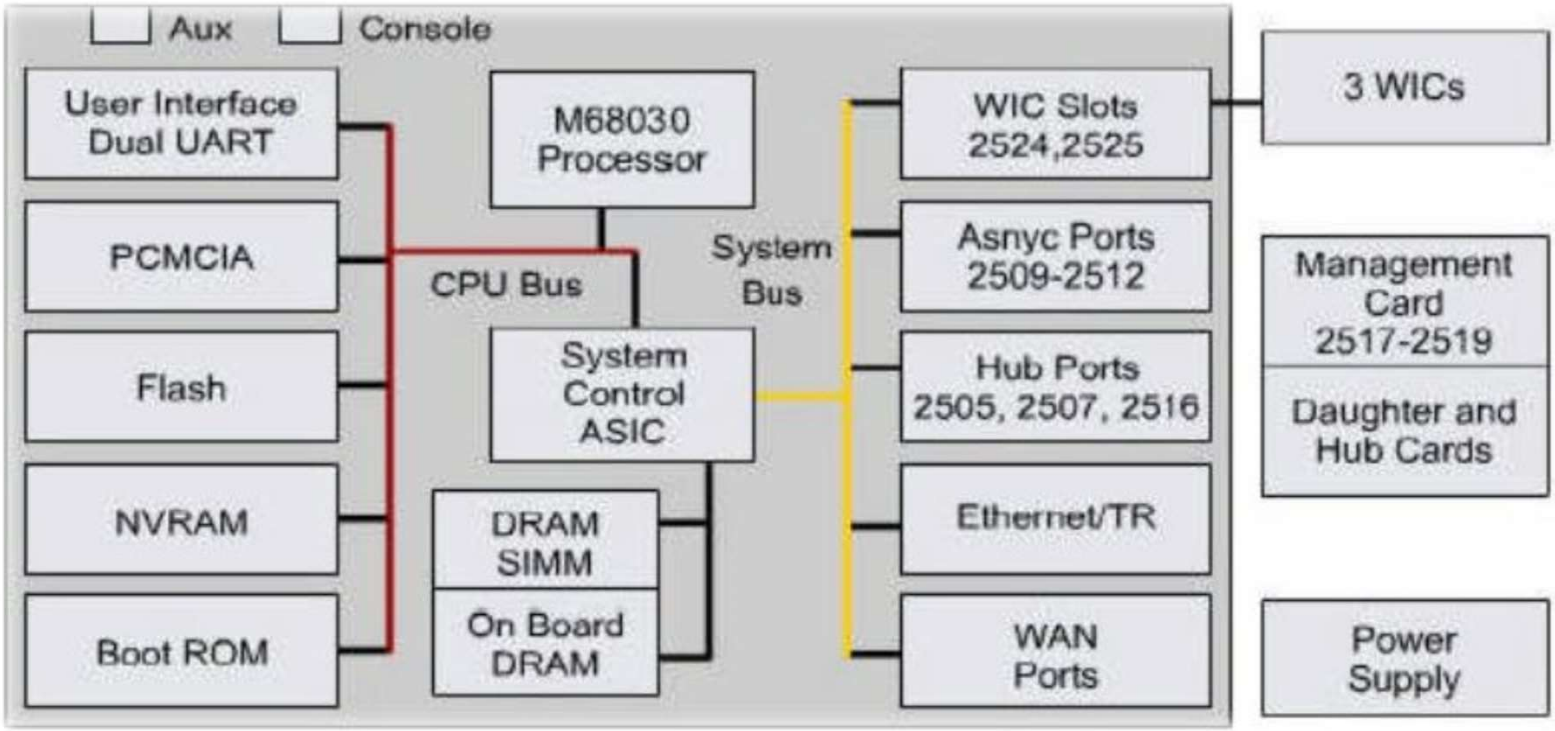
Resim 1.5: Yönlendirici arka paneli

Arka panelde;

1. Güç girişi,
2. Açma/Kapama düğmesi,
3. HWIC/WIC/VIC slot 0 (Genişleme Yuvası 1 – Resimde, 4 arayüzlü Ethernet kartı takılıdır.),
4. Konsol Arayüzü,
5. AuxiliaryArayüzü,
6. FastEthernetArayüzleri,
7. HWIC/WIC/VIC slot 1 (Genişleme Yuvası 2 – Resimde, WAN için seri arayüz kartı takılıdır.),
8. CF Kart Yuvası bulunur.

Router (Yönlendirici) yapısı

Temel donanımsal elemanları, donanımsal arayüzler (WAN,LAN), CPU, Flash, RAM, NVRAM, ROM'dur.



Yönlendirici iç yapısı blok şeması

CPU: Bu işlemci yönlendirme parametrelerini ve ağ arayüzlerini kontrol eder.

FLASH: Kalıcı hafıza birimidir. Her yönlendirici belirli bir işletim sistemine ihtiyaç duyar. İşletim sistemi imajı **(IOS-ROS)** ise "flash"da tutulur.

ROM: Fiziksel olarak sinyal yollayıp, donanımları test eden ve yönlendiriciyi başlatmaya yarayan program olan **"Bootstrap – Mini IOS"ı** içerir. Boostrap: Yönlendiricinin çalışmasını sağlayan bir yazılımdır.

RAM: Yönlendiricinin aktif bilgilerinin bulunduğu geçici hafıza birimidir. Yönlendirici açılırken bootstrap, flash'tan işletim sistemi imajını ve NVRAM'den başlangıç konfigirasyonunu RAM bölgesine yükler. Çalışan yapılandırma (running -config) bu alanda tutulur. Ayrıca RAM'de yönlendirme tabloları ve gelen fakat iletilmemiş verilerde tutulmaktadır. Yapılan konfigirasyon, running-config dosyası olarak kayıt edilir ve RAM'de tutulur. RAM'deki running-config dosyası NVRAM'e kaydedilmezse yönlendiricinin kapatılması durumunda, çalışan yapılandırma bilgileri kaybolur.

NVRAM: Kalıcı hafıza birimidir. Burada başlangıç (startup) ve yedek (backup) konfigirasyon dosyaları tutulur. Enerji kesilse bile bu bilgiler bellekte kalmaktadır. Router'ın konfigirasyon bilgilerinin kalıcı olarak tutulduğu hafızadır.

Interfaces: Her yönlendiricinin kendisine gelen bilgileri alması, göndermesi ve yapılandırmasının yapılması için kullanılan bağlantı noktalarına arayüz (interface) denir (Örneğin ethernet 0, consol gibi). Arayüz her zaman fiziksel bir olgu değildir

ROS Yazılımı

Bir yönlendirici, donanımı ve yazılım olmak üzere iki ana parçadan oluşur. **Yönlendirici işletim sistemi** (ROS: Router Operating System) yazılımı oldukça önemlidir. ROS'un işlevi, desteklediği 3. katman protokolları ve kullandığı yönlendirme algoritması için gerekli fonksiyonları sağlamaktır. Ayrıca ağ yöneticisine, yapılandırılmasını sağlamak için bir ara yüz sunar.

Cisco yönlendiriciler, **IOS (Internetwork Operating System)** kullanırlar. Aşağıda Cisco IOS yazılımının görevleri bulunmaktadır:

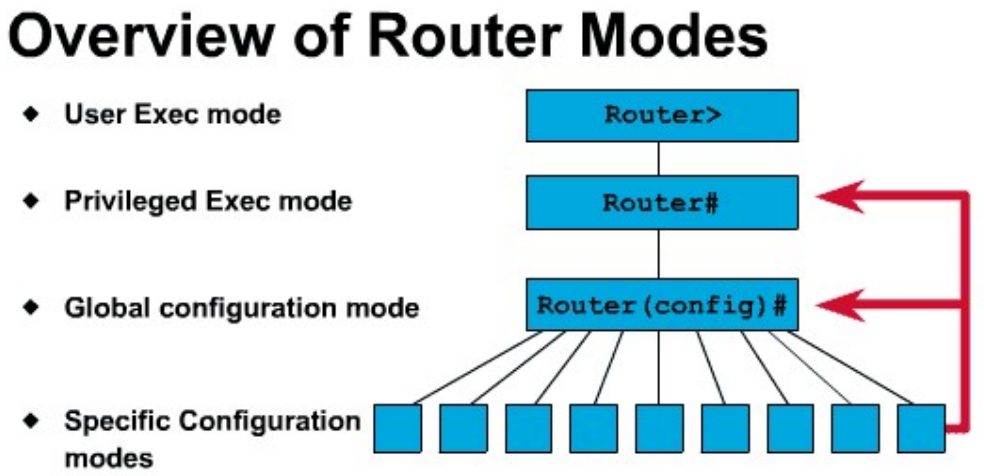
- Network protokol ve fonksiyonlarını taşımak
- Cihazlar arasındaki yüksek hızda trafiği bağlamak
- Erişimi kontrol etmek için güvenlik sağlamak ve izinsiz network kullanımını engellemek
- Ağın büyümesini ve kullanılabilirliğini kolaylaştırmak için ölçeklenebilirlik sağlamak.
- Network kaynaklarına bağlanmak için güvenliği sağlamak

Routerların konfügirasyon (yapılandırma) ayarlarını görmek ve değiştirmek için farklı kullanıcı seviyeleri (mod'ları) bulunmaktadır

User EXEC Mod: Yönlendirici açılıp arayüze erişildiği anda karşınıza çıkan moddur. Burada yönetimsel işlemler yapılamaz, bir sonraki modlara geçiş için kullanılır.

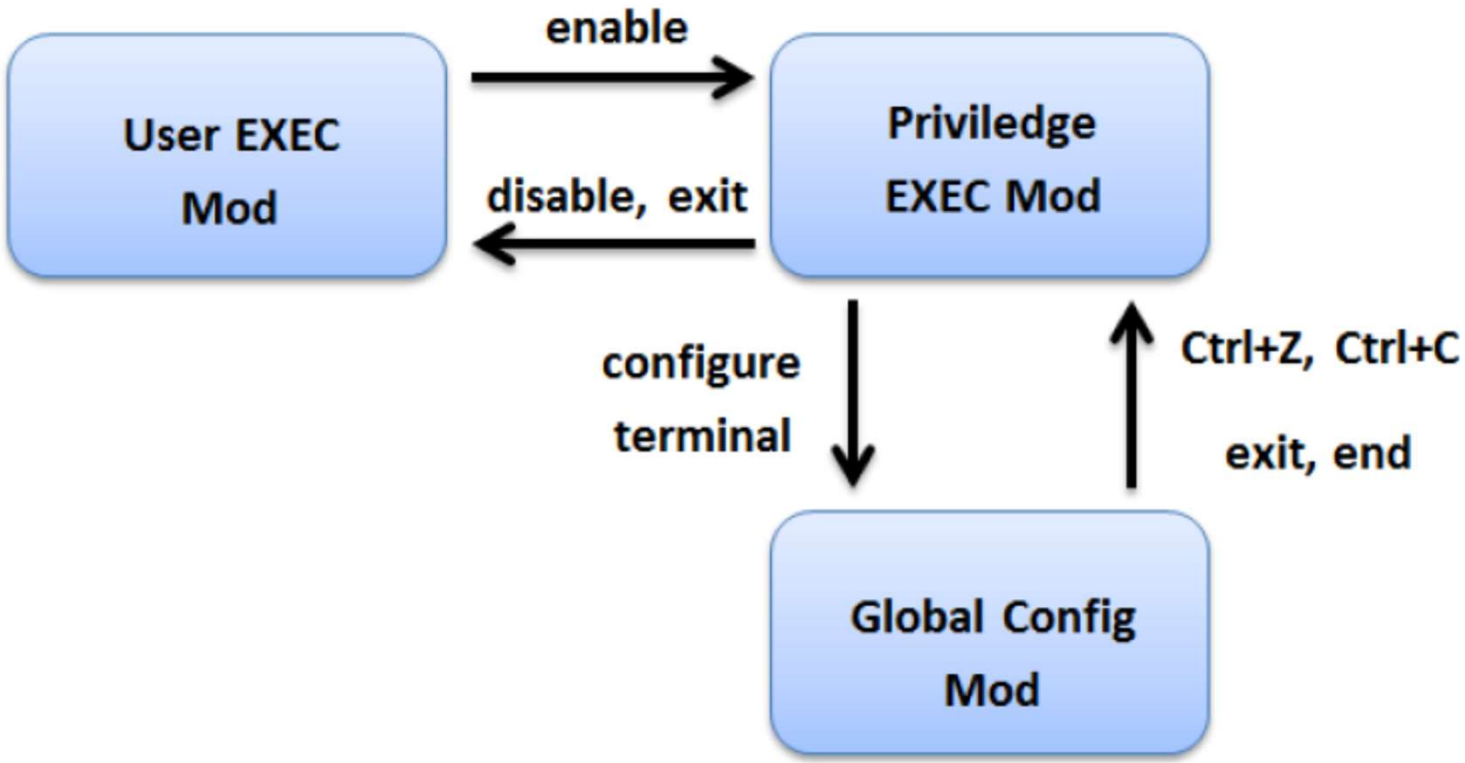
Privileged EXEC Mod: User EXEC modda iken **"enable"** yazıp "Enter"a basıldığında bu moda geçilir. Bu moda enable mod da denir ve önerilen davranış bu moda geçerken şifre konulmasıdır. Zira bir kullanıcı bu moda geçtikten sonra yönlendiriciye tamamen hâkim olur. Priviledge mod işaret **"#"** şeklindedir.

Global Configuration Mod: Config Mod diye de anılan bu moda geçmek için enable modda iken **"configure terminal"** yazılır ve "Enter"a basılır. Bu modda yapılan değişiklikler bütün yönlendiriciyi etkiler. Bu modayken işaretçi **"(config)#"**şeklinde gözükür.



Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

Yönlendirici çalışma modları arası geçiş



Resim 3.5: Modlar arası geçiş işlemleri

Router'ların GÜVENLİĞİ

1-Fiziksel Güvenlik:

Yönlendiriciler için ayrı bir oda ayırılamıyorsa en azından kilitli dolaplar (kabinet) içine koyulmalıdır. Bu odanın enerjisi hiç kesilmemelidir . Bu UPS (Uninterupted power supply) kullanarak sağlabilmektedir. Yönlendirici yakınlarına şifre veya ip bilgileri gibi bilgileri yazmaktan kaçınmaktır.

2.Yönlendiriciye Erişim Hakları

Yönlendiriciye kimlerin erişeceğinin bir politikayla belirlenmesi ve erişimlerin loglanması gerekmektedir. Bu politikada; kimin konfigürasyon yedeklerini alacağının, kimin yeni bir parça alımında yönlendiriciye yerleştireceğinin, kimin logları düzenli takip edileceğinin açık bir şekilde belirtilmesi gerekmektedir. Temelde yönlendiricilere, **kullanıcı (user)** ve **yönetici (enable)** olarak iki çeşit erişim hakkı vardır. Kullanıcı modunda sadece kontroller yapılabilirken, yönetici modda ek olarak cihaz konfigürasyonu da yapılabilmektedir.

Router güvenliği-2

3.Şifrelerin Güvenliği

Günümüzde büyük oranda kırma (hacking) işlemi “password quessing” (parola tahmin etme) yöntemiyle yapılmaktadır bu sebepten şifre seçimine gerektiği önem verilmelidir.

Cisco yönlendiricilerde kullanıcı adı ve parolasının konfigürasyon dosyasında gözükmemesi için *“service password-encription” komutu kullanılmalı.*

Zayıf şifreleme algoritması kullanan “enable password” kaldırılmalı, MD5-tabanlı algoritmayla şifreyi koruyan “enable secret” komutu kullanılmalıdır. *“no enable password” komutu kullanılarak enable password’ler* silinmeli yerine *“enable secret yeni_şifreniz” ile yeniden şifreler girilmelidir*

Router güvenliği-3

4.Erişim Protokollerinin Güvenliği

Routerlara fiziksel erişim konsol portundan yapılmaktadır. Bunun için fizikselgüvenliğin sağlanması gerekmektedir.

Diğer erişim yöntemleri olan HTTP, Telnet, SSH,TFTP, ve FTP kullanıldığında TCP/IP protokolünün zayıflıklarına karşı önlem alınması gerekmektedir. Alınması gereken önlemler aşağıdaki gibidir.

a) Belirli IP'lerin Cihaza Erişimine İzin Vermek:

Cihazlara sadece belirli IP adreslerinin ulaşmasına izin verilmelidir. Bu da erişim listesi (access-list) yazılarak sağlanır. Örneğin Cisco IOS'de sadece 200.100.17.2 ve 200.100.17.3 IP'lerin erişimine izin verilmesi ve diğer ip'lerin engellenmesi ve bu erişimlerin kaydının tutulması aşağıdaki erişim listesi ile sağlanmaktadır.

access-list 7 permit 200.100.17.2
access-list 7 permit 200.100.17.3
access-list 7 deny any log

R.Güvenliği -4

HTTP Erişimi:
HTTP protokolü ile web arayüzünden erişim, cihaza interaktif bağlantı demektir. Yönetilebilir cihazlarının birçoğunun üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir.

HTTP servisi verilecekse bu ağ yönetimini sağlayan belirli IP'lere kısıtlı olarak verilmelidir. Cihaz güvenliği nedeniyle mümkün olduğunca bu tür web üzerinden yönetimin kullanılmaması gerektiği önerilmektedir.

Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bileceği başka bir port üzerinden, örneğin *"ip http server port 500"* komutuyla 500 nolu portta çalıştırılabilecek şekilde ayarlanmalıdır.

R.güvenliği-5

Telnet, SNMP protokolleri ile cihaza erişimde, doğrulama mekanizması ağda şifrenin düz metin (clear text) şeklinde gönderimi ile sağlandığı için güvenlik açığı oluşmaktadır. Özellikle hub bulunan ortamlarda saldırganın ağ üzerinden dinleme (sniff) yoluyla iletilen bilgiyi elde etmesi mümkün olabilmektedir. Bunu engellemek için aşağıdaki önlemler alınabilir :

- - **Telnet yerine Secure Shell (SSH) Erişimi Vermek:** İletilen veriyi şifreleyen SSH protokolü mümkün olduğunca kullanılmalıdır.
- **Güncel SNMP Versiyonlarını Kullanmak:** SNMP Versiyon 1, düz metin doğrulama dizileri (string) kullandığından bu doğrulama dizilerinin spoof edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz (*digest) doğrulama şeması kullanan,* yönetim verilerine kısıtlı erişim sağlayan SNMP Versiyon 2 veya 3'ün kullanılması gerekmektedir.
- **Doğrulama Mekanizmaları Sağlamak:** Doğrulama mekanizması, onay sunucuları(Tacacs+, Radius …vb) kullanılarak yapılabilir. Cisco IOS'de doğrulama mekanizması ***"ip http authentication"*** *komutuyla sağlanmaktadır.*

R.Güvenliği-6

5.Gereksiz Servisleri Kapatmak

Yönlendiricide kullanılmayan servisler kapatılmalıdır. Örneğin kullanılmayan ve güvenlik açığı oluşturabilecek TCP/UDP services echo, chargen ve discard kapatılmalıdır:

no service tcp-small-servers
no service udp-small-servers

Bu cihaza bağlı kişiler hakkında saldırgana bilgiler sağlayabilecek "finger" servisi de kapatılmalıdır:

no service finger

Daha önceden de belirtildiği üzere yönlendiricide web sunucusu da çalıştırılmamalıdır:

no ip http server

R.Güvenliği-7

6.İşletim Sistemi

Yönlendirici için işletim sistemi (Operating System) seçilirken ağın ihtiyaclarına uygun ve aynı zamanda donanımın desteklediği bir versiyon olmasına dikkat edilmelidir. Her ne kadar işletim sistemleri güvenlik testlerine tabi tutulup daha sonra piyasaya sürülüyorsa da daha sonradan güvenlik açıkları bulunabilmektedir. Bu nedenden dolayı çıkan yamaları takip edip upgrade yapmak gerekebilmektedir.

AĞI ROUTER ile Korumak

Yönlendirici, bazı ağlarda yönlendirici görevinin yanı sıra güvenlik duvarı gibi çalışacak şekilde de ayarlanabilmektedir. güvenlik duvarı işlevi, basit bir paket filtreleme fonksiyonundan oluşmaktadır ve günümüzdeki güvenlik duvarlarına oranla oldukça ilkel kalmaktadır.

Yönlendiricinin temel görevinin yönlendirme (routing) olduğu unutulmamalı, bu tür bir güvenlik duvarı işlevinin cihazın performansını düşüreceği dikkate alınmalıdır.
Yönlendiriciyi aynı zamanda detaylı paket filtreleme özellikleri ile kullanmak, sadece küçük ağlarda veya güçlü omurga cihazlarının bulunduğu kampüs ağlarındaki iç yönlendiricilerde tercih edilmelidir.

Ağı R ile korumak-2

Bu bölümde yönlendirici ile ağdaki bilgisayarlara gelebilecek saldırıların engellenmesi için bazı ipuçları verilecektir.

1. Riskli portları kapatmak:

İnternet üzerindeki servisler, kullanıcılara hizmet götürebilmek için bazı sanal port numaraları kullanırlar (örn: http için 80 numaralı port kullanılmaktadır). Saldırganlar veya kötü yazılımlar servislerin açıklarını kullanarak hizmet verilen port numarası üzerinden bilgisayar ağına sızabilirler.

Bunu önlemenin bir yolu riskli portları yönlendirici ile kısıtlamaktır. Riskli portların listesi [http://www.nsa.gov/snac/cisco/guides/cis-2.pdf] adresteki referansının 38 ve 39 sayfalarında listelenmiştir. Aşağıdaki örnekte 445 nolu UDP portu ile finger servisi bloklanmaktadır:

access-list 101 deny udp any any eq 445
access-list 101 deny tcp any any eq finger
access-list 101 permit ip any any

Tanımlı mail ve web sunucularını belirlemek ve bu sunucular dışında bu tür protokolleri engellemek de mümkündür. Erişim listesi ne kadar kapsamlı olursa o kadar fazla işlemci gücü gerektirecek ve performans azalacaktır. O yüzden sık gelen paket türlerini erişim listesinde daha önde tutmak performansı arttıracaktır

Ağı R ile korumak-3

2.Bazı saldırı tekniklerine karşı önlemler

IP spoofing : Kötü niyeli kişi hattı dinler giden paketlerin kaynak ve hedef adresini alır. Hedef adresini kendi ip'si yaparak kaynak adrese cevap verir. Böylece erişim listesine takılmadan bilgisayar ağına sızmış olur.

Bunu önlemenin yolu, yönlendiricinin kaynak adresi hedef makinaya varmadan kimseye göstermemesidir. Bu işlem Cisco cihazlarda "*no ip source-route" komutuyla yapılabilmektedir* .

Routing Protokole olan saldırılar: Saldırgan yönlendiricinin routingprotokolünü bozmadan yollanan paketlerin bir kopyasının kendine de yollanmasını sağlayabilir veya protokolleri kaldırarak yönlendiricinin diğer yönlendiricilerle haberleşmesini kesebilir. Haberleşmenin yok olması, yönlendiricinin aldığı paketleri nereye göndereceğini bilmemesi ve servis dışı kalması(DoS) saldırısıdır. Bunu önlemenin yolu ise gönderilen ve alınan routing protokolu paketlerini filitrelemektir. Örneğin IGRP routing protokolünü filtrelemek için yazılmış ACL aşağıda verilmiştir.

router eigrp
network 200.100.17.0
distribute list 20 out ethernet 0
distance 255
distance 90 200.100.17.0 0.0.0.255
access-list 20 permit 200.100.17.0 0.0.0.255

Ağı R ile korumak-4

Çıkış (Egress) ve Giriş (Ingress) Erişim Listeleri

Bu erişim listeleriyle yönlendiriciye gelen paketlerdeki kaynak IP adresleri kontrol edilmektedir.

Dış ağdan iç ağa gelen paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne *giriş (ingress) filtreleme denmektedir. Bu kontrolde gelen paketlerdeki ip'lerde internet ortamında* kullanılmayan (rezerve edilmiş) adresler bulunduğunda bu paketler kabul edilmeyecektir. Ağ adresimiz 200.100.17.0/24 ise, dış dünyadan böyle bir IP aralığına ait bir paket gelmemesi gerekmektedir. O zaman ingress kısıtlamaları aşagıdaki gibi olacaktır:

access-list 101 deny ip 10.0.0.0 0.255.255.255 any
access-list 101 deny ip 172.16.0.0 0.15.255.255 any
access-list 101 deny ip 192.168.0.0 0.0.255.255 any
access-list 102 deny ip 200.100.17.0 0.0.0.255 any
access-list 101 permit ip any an

Ağı R ile korumak-5

Ağdan dış ağa giden paketlerde, gelen paketlerdeki kaynak ip'lerin kontrolüne *çıkış (egress) filtreleme denmektedir. Kendi ağ ip adresi aralığında olmayıp da internete çıkmak isteyen* ip'ler kısıtlanmalıdır. Böylece kurumun ağı kullanılarak başka kurumlara yapılabilecek kaynak IP adresi değiştirme tabanlı saldırılar engellenecektir. Bazı reserve edilmiş IP lerin kısıtlanması aşağıdaki gibidir:

access-list 102 permit ip 200.100.17.0 0.0.0.255 any
access-list 102 deny ip any any

Örnekte dışardan gelen trafik ingress erişim listesi ile seri arayüzde, içeriden gelen trafik de egress erişim listesi ile ethernet arayüzünde tanımlanmıştır.

interface serial 0
ip access-group 101 in
interface ethernet 0
ip access-group 102 in

Ağı R ile korumak-6

Reverse Path" Kontrolü: Gönderdiğimiz paket "ethernet 0" arayüzünden gönderiliyor fakat cevabı "ethernet 1" arayüzünden geliyorsa bu işte bir yanlışlık var demektir. Bunu önlemek için geliş gidiş istatiğini tutan CEF routing tablolarından yararlanmak gerekmektedir. Bunu sağlamak için de seri arayüzde bu komutun uygulanması gerekmektedir.

İp cef disributed
!
interface serial 0
ip verify unicast reverse-path

Ağı R ile lorumak-7

Smurf attack: IP adresi kandırmacası ve broadcast (aynı subnetteki herkese yollama) ilkelerine dayanır. Saldırgan, saldırmayı hedeflediği bilgisayarın IP'sinden paket geldiğinin sanılması için, kaynak adresi bu IP olan "broadcast ping" paketleri oluşturur ve gönderir.

Gönderilen ping paketlerinin cevabı gerçekte bu IP'ye sahip olan bilgisayara gider ve orada gereksiz trafik yaratarak bilgisayarın ağa ulaşması engellenir. Bu olayı yönlendiriciden önlemenin bir yolu da yönlendiricideki arayüzlere

"***no ip directed-broadcast***" *komutunu* girmektir.