

IP Spoofing (Yanıltma-Aldatma)

- Internet veya ağa bağlı sisteminizle başka bir sisteme bağlanacaksınız, fakat bu bağlantı sizin tarafınızdan yapıldığını gizlemek istiyorsunuz. Bunun için bağlantı sırasında kimliğinizi (ki TCP/IP protokollerinde kimliğiniz IP adresinizdir), yanlış gösteriyorsunuz. Bu IP spoofing işlemidir.
- Bu saldırının amacı bir makinenin IP adresini ele geçirmektir. Saldırıgan bu iş için genelde iki bilgisayar arasındaki güvenilir ilişkiden yararlanır.
- Bu saldırıyla, saldırıgan, kendi IP paketlerinin sahtekarlığını yaparak (nemesis v.b gibi programlar ile) diğer paketlerin arasınaki kendi paketinin kaynak IP alanını değiştirir.
- Kaynak değiştirildiğinden, sahte pakete karşılık gelen cevaplar saldırının makinesine gidemez. Spoof edilen makinaya gider.
- **Saldırıganın bu cevabı kendi makinasına alabilmesi için kullandığı önemli teknik "Kaynak yönlendirme-Source routing" dir.**

Spoofing (cont.)

- **Yerel spoofing:** Saldırgan(attacker) ve mağdur (victim-kurban) aynı alt ağdadır.
- Saldırgan, bir saldırısı başlatmak için gerekli temel bilgi parçalarını bulmak amacıyla trafik koğlama (sniffing - izleyici) ile işe başlar.
- **Blind spoofing:** Saldırgan ile mağdur aynı altağ'da değildir.
- Daha karmaşık ve gelişmiş saldırıdır. Saldırının başarılması için gerekli bilgi miktarı mevcut değildir. Anahtar parametreleri tahmin edilmelidir.
- Modern işletim sistemleri bu şekildeki saldırıları başlatmayı zor hale getirmek için, oldukça rastgele sıra numaraları kullanır.

Paketlerin Parçalanması (IP fragmentation)

- Veri bağı katmanı kullanılarak gönderilecek en büyük datagramın boyutuna **MTU (Maximum Transmission Unit)** denir. Değişik ağ teknolojilerindeki MTU'lar farklıdır.
- Paketlerin MTU'yu geçmeyecek şekilde ağlar arasında iletimin sağlamak için boyutlandırılması işlemine parçalama (fragmentation).
- IP başlığı, parçalanan bu paketin tekrar birleştirilmesi için gerekli bilgileri parçaların her birine aktarır.
- Paketlerin birleştirilme işlemi (reassembly) a ra yönlendiricilerde yapılmaz. Son noktalar tarafından yapılır.

Ağ Türü	MTU(Oktet)
Ethernet	1500
IEEE 802.3	1492
Token Ring	4440-17940
FDDI	4352
x.25	100

IP Datagram Parçalama/Birleştirme

- Ağdaki hatların taşıma kapasitesi MTU ile sınırlıdır (max.transfer size) - en büyük olası bağlantı katmanı çerçevesi.
 - Farklı hat tipleri, farklı MTU'lar
 - büyük IP datagram ağda bölünür ("fragmented" - "parçalanır")
 - Bir datagram pek çok datagram haline gelir
 - Sadece son hedefte "reassembled" - "birleştirilir"
 - IP başlık bitleri ilgili fragment-veri parçalarını tanımlama ve sıralamada kullanılır
-
- Fragmentation (parçalama):
girişte: bir büyük datagram
çıkışta: 3 daha küçük datagram
- Reassembly (birleştirme)

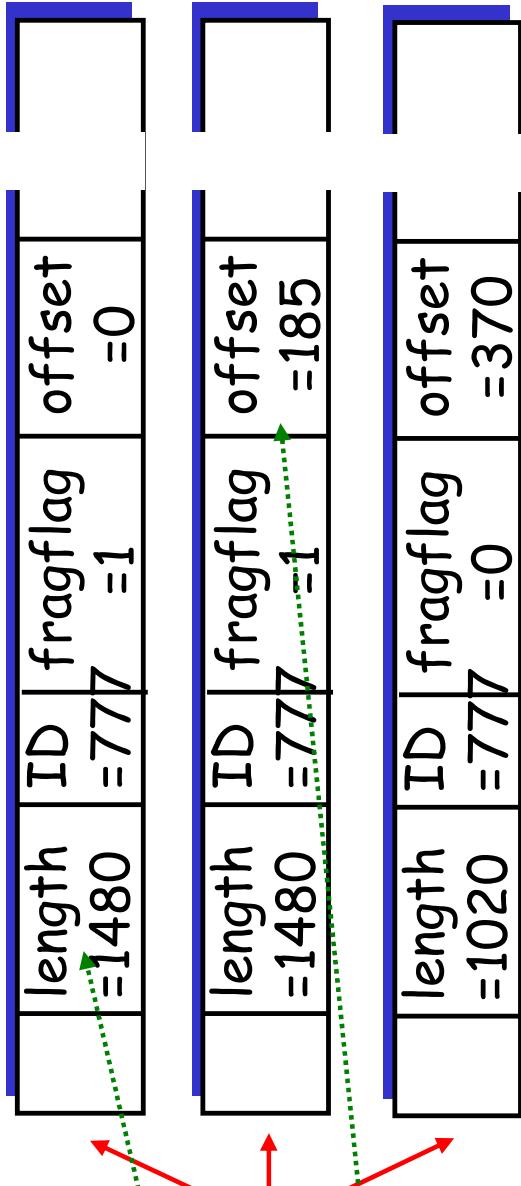
IP Datagram Parçalama/Birleştirme

Örnek

- 4000 byte
datagram
- MTU = 1500 bytes

Bir büyük datagram pek çok
daha küçük datagrama dönüşür

uzunluk =4000	ID =777	bayrak =0	öteleme =0
------------------	------------	--------------	---------------



Veri alanında 1480 bytes
offset
(öteleme)=
 $1480/8$

IP Datagram Parçalama/Birleştirme

Örnek

- 4000 byte
datagram
- MTU = 1500 bytes

Büyük bir datagram birkaç
küçük datagrama dönüşür

uzunluk =4000	ID =777	bayrak =0	öteleme =0
------------------	------------	--------------	---------------

length =1500	ID =777	fragflag =1	offset =0
length =1500	ID =777	fragflag =1	offset =1480
length =1040	ID =777	fragflag =0	offset =2960

Veri alanında 1480 bytes

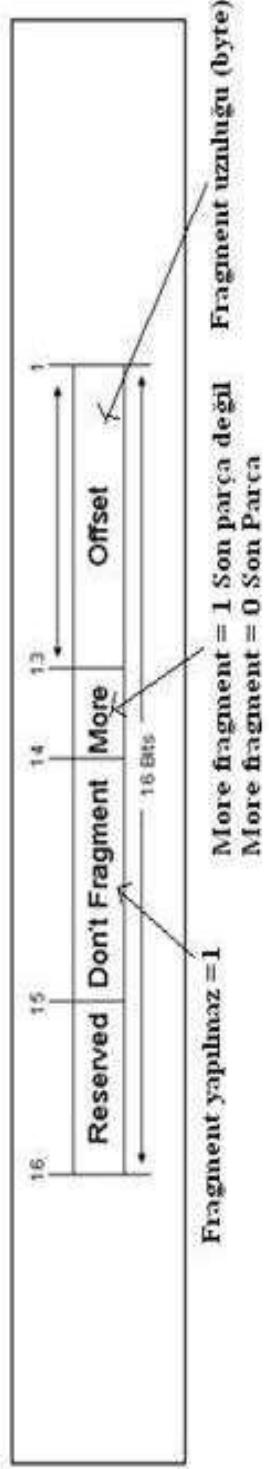
ICMP ?

Her IP paketi ?

Parçalama (Fragmentation)

- Paketlerin, farklı MTU değerleri olan farklı ağlarda iletilirken Parçalanması gerekebilir. Her bir fragment kendi IP başlığını alır ve farklı bir yol üzerinden seyahat edebilir.
- Parçalanan paketlerin hedefe ulaştığında doğru sırada birleştirilmesi gereklidir. Paketler hedefe ulaştığında tekrar birleştirilip orjinalinin elde edilmesi için her pakette bulunması gereken bazı alanlar vardır. Bunlar

IP DATAGRAM Başlığındaki Fragment ilgili (FLAG+FRAGMENT Offset - 16 bit) kısım



Fragmented Data

Internet Protocol.

version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00)
Total Length: 1500
Identification: 0xdca (3530)
Flags: 0x02 (More Fragments)
0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.1. = More fragments: Set
Fragment offset: 0
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0xb1eb [correct]
Source: 192.168.123.101 (192.168.123.101)
Destination: 192.168.123.180 (192.168.123.180)

0... = Reserved bit: Not set
.0.. = Don't fragment: Not set
.1. = More fragments: Not set
Fragment offset: 1480
Time to live: 128
Protocol: ICMP (0x01)
Header checksum: 0xb1eb [correct]
Source: 192.168.123.101 (192.168.123.101)
Destination: 192.168.123.180 (192.168.123.180)

- Parçalanmış her paket datagramın hangi kısmını taşıdığını (Offset değeri) ve sırasını bilmelidir. Kendisinden sonra ek parça paket varsa bu alan flags[1], paketin kendisi son paket ise değer flags [none] olur.

```

Identification: 0x5199 (20889)
└ Flags: 0x02 (More Fragments)
  0... = Reserved bit: Not set
  .0.. = Don't fragment: Not set
  ..1. = More fragments: Set
Fragment offset: 0

```

Parçalanmış her paket taşıdığı veri boyutunu ve hangi byte'dan itibaren taşıdığını bilmeli.
Ne kadarlık bir veri taşıdığı Total Length ile belirtilir.

```

└ Differentiated Services Field: 0x00 (DSGP 0x00: default; ECN: 0x00)
  Total Length: 1500
Identification: 0x517f (20863)

```

Hangi Byte'dan itibaren bu verinin ekleneceği de “Fragment Offset” değeri ile belirtilir. Yani önceki paket 2960 byte tasımıştır, biz de buna ek 1500 byte yapıp göndereceğiz, bir sonraki pakette offset değeri 2960+1500 olacaktır(asında 2960+1480)

```

Identification: 0x517f (20863)
└ Flags: 0x02 (More Fragments)
  0... = Reserved bit: Not set
  .0.. = Don't fragment: Not set
  ..1. = More fragments: Set
  Fragment offset: 2960
  Time to live: 128
  Protocol: ICMP (0x01)

```

Dikkat !!!!!

- Parçallanmış paketlerde sadece ilk paket protokol başlıklı bilgisini(TCP, UDP, ICMP vs) taşıır.

- **Reassembly** (**Tekrar Birleştirilme İşlemleri**): IP protokolu belirtimindeki bazı belirsizlikler nedeniyle, özel durumlarda farklı parçalama işlemleri meydana gelebilir ve bu parçaların yeniden birleştirilmesi gereklidir. Bu özel parçalama işlemlerini;
 - **Fragment retransmission** (*parçaların yeniden iletilmesi*),
 - **Fragment overlays** (parçaların üstüste gelmesi - bindirmeler)
 - **Fragments with non-neighbouring offsets.** (Komşu olmayan ofsetli parçalar.)
 - Eğer ağı koruyan cihazlardaki parçalar ile hedef host takiler farklılıklar gösterir ise; bu durum tutarsızlıklara yola açabilir.
 - Dolayısıyla **insertion** ve **evasion** atakları yapılabılır.

- **Bu bireleşme sürecindeki olabilecek atakları:**
- **Time out (Zaman aşımı)**: Parçalanmış paket; yalnızca tüm parçalarının parçalanma zaman aşımı süresi içinde alınmış ise yeniden birleştirilir.
- Hedef host ve IDS'de farklı zaman aşımı uzunluklarının kullanımı, saldırgan evasion atak gerçekleştirmesine izin verebilir.
- **TCP header division**: TCP oturumunu izleyip ve parçalanmış paketleri yeniden birleştirmeyi başaramayan IDS'ler, saldırgan tarafından oluşturulmuş daha küçük fragmentleri atlayabilirler. Bunlar TCP başlıklarını ikiye bölmüş fragmentler olabilir.
- Bu şekilde oluşmuş her bir bağımsız fragment, imzaya uyusmaz dolayısıyla atak sayılmaz.

Fragmentation Atakları

- Parçalanmış paketlerin üst üste çakışması (Overlay),
saldırganlara IDS, Firewall ve Routerlarda eski
paketlerin kaydırılması imkanını sunar.
- Bir routerden, windows temelli bir sisteme paket
gönderildiğinde;
- Eğer alınan paket duplike bir paket ise;
 - Router (veya IDS veya Firewall) en son gönderilen
fragmenti tercih eder.
 - Windows orijinal (ilk gönderileni) tercih eder.

- Parçalanmış paketler konusunda en sıkıntılı sistemler IDS/IPS'lerdir. Bunun nedeni bu sistemlerin temel işinin ağ trafiği incelemesi olmasıdır. Saldırı tespit sistemleri gelen bir paketin/paket grubunun saldırıcı içeriği olup olmadığını anlamak için çeşitli kontrollerden geçirir. Eğer bu kontrollere geçmeden önce paketleri birleştirmeye çok rahatlıkla kandırılabilir.
- Mesela HTTP trafiği içerisinde “/bin/bash” stringi arayan bir saldırımızı olsun. IDS sistemi 80.porta gelen giden her trafiği inceleyerek içerisinde /bin/bash geçen paketleri arar ve bu tanıma uyan paketleri bloklar. Eğer IDS sistemimiz paket birleştirme işlemini uygun bir şekilde yapamıyorsa, saldırgan paket bölmeye araçlarından birini kullanarak /bin/sh stringini birden fazla paket olacak şekilde (1. Paket /bin, 2.paket /bash) gönderip IDS sistemini atlatabilir.

Fragmentation Attacks (cont.)



Attacker modifies #2
And transmits #2 and #3



Windows keeps



Windows keeps



Router keeps

Same size, same offset

Fragmentation Attacks (cont.)

- Saldırgan mesajını 3 parçaaya böler.
- O hem yönlendiriciye hemde windows tabanlı sisteme 1. ve 2. parçayı gönderir. Her ikisi de parçaları kabul eder.
- Saldırgan 2 . Ve 3. parçaları gönderir. Yeniden gönderilen 2.parça ilki ile aynı boyut ve offsettedir. Fakat payload'ı farklıdır (Saldırı imzası taşımaz).
- Windows 2. parçanın orijinalini (saldırı mesajı bundadır) kabul ettiği halde router (veya IDS) yeniden (Son) gönderileni kabul eder. Dolayısıyla birleştiğinde bu mesajların saldırısı olmadığına karar verir.

Parçalanmış Paket Oluşturma Araçları

- Paket parçalama işlemi normalde bizim (kullanıcıları) tarafımızdan yapılmaz. Ağlar arası geçişleri sağlayan yönlendirici sistemler (router) gerektiğinde bu işlemi gerçekleştirir.
- Fakat internette bulunan çeşitli araçlar kullanılarak kendi isteğiimize göre paketleri parçalayıp gönderebiliriz.
- Bunları Öğreniniz!!!!!!!
- **Dikkat !!!** Parçalanmış paket saldırılarına sebep olan güvenlik açıklıkları uzun zaman önce işletim sistemi firmalar tarafından kapatılmıştır fakat paket parçalama ile yapılan Firewall/IDS/IPS atlatma yöntemleri hala bazı sistemler üzerinde çalışabilmektedir.

Source Routing (Kaynak Rotalama) atakları:

- Source routing, TCP/IP suitinde paket göndericisine, netwokte paketi rotaya göre ilerletmek için imkan veren bir seçenekir.
- Saldırırganlar bu Özelliği , belirli bir alt ağ ele geçirmek için yapacakları saldırısı için kullanabilirler.
- Şöyleki; saldırın, gönderici adresini aldatarak, o paketi bir alt ağdan geliyormuş gibi set edebilirler.
- Bunu önlemenin yolu, router'ın kaynak adresi hedef makinaya varmadan kimseye göstermemesidir.
- **Bu işlem Cisco cihazlarda “no ip source-route” komutıyla yapılabilmektedir.**

Teardrop Saldırıları

- Teardrop, targa, NewTear, Nestea Bonk, Boink, TearDrop2, ve SynDrop gibi bazı saldırı araçları, IP atakları için açıklara sahip makinaları çökertebilirler.
- Teardrop atağı IP paketlerinin tekrar birleştirilmesinden kaynaklanır. Mesaj, ağlar arasında iletildikten genellikle daha küçük parçalar ayrılr. Herbir parça orjinal paket gibi görünür. Fakat offset alanları farklıdır. Teardrop programı bir dizi IP paket parçaları oluşturur. Bu parçalar örtüşen offset alanlarına sahiptir. Bu parçacıklar varış noktasında tekrar birleştirildiklerinde bazı sistemler çökebilir, durabilir veya kapanıp açılabilir. Teardrop saldırısı bir DOS saldırısıdır.
- Overlapping, over-sized, payload paketler gönderilererek sistem bozulur.

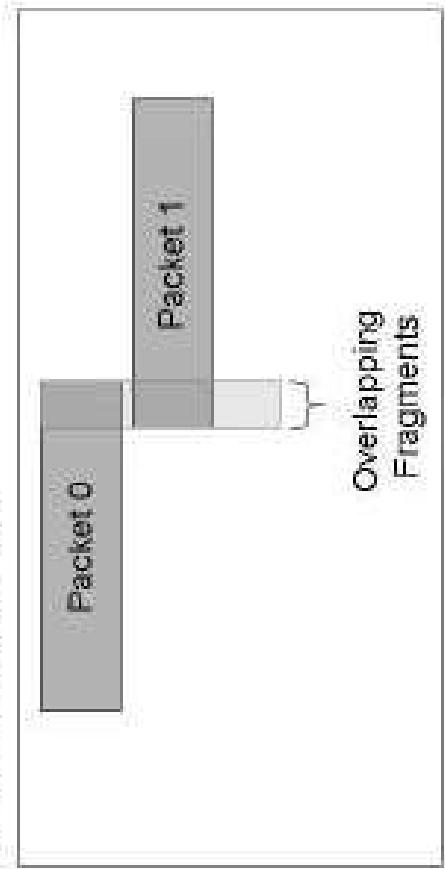


Figure 4.14 The Teardrop Attack

Ping of Death Atağı

- Ping of Death, IP paketlerine gömülü olarak ICMP ile gönderilen “echo request” mesajları ile yapılır. Bu mesajlar 65.535 bayt’tan daha büyük mesajlar halinde sürekli olarak gönderilirse Buffer kapasitesi küçük olan makinalarda buffer taşmasına sebep olarak makinanın çökmesine sebep olur. Ping of death bir DoS atağı çeşididir.

IP Katmanı genel Atak Tipleri

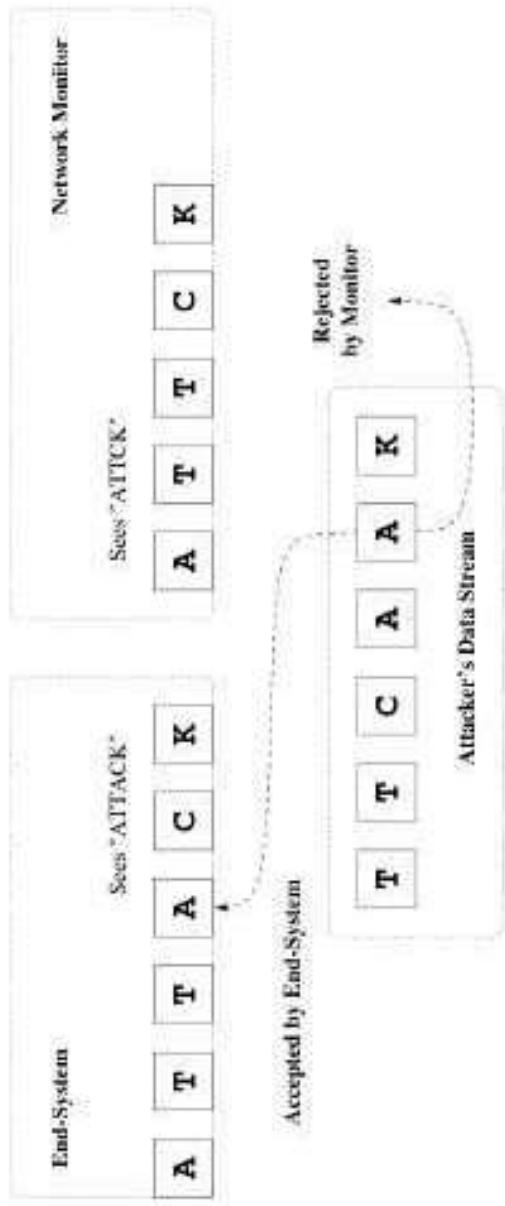
Paket bazlı ağ katmanındaki savunma sistemleri genelde IDS'lerledir._Saldırıyanlar ise bu yapıyı 3 tip genel atakla geçmek isterler.

1- *Evasion attack (Atlatma Atakları):*

Bu ataklarda paketler hem IDS'ye hem de hedefe gönderilir. IDS bu paketleri reddeder (dikkat atak olduğu için değil !!!!) , hedef host kabul eder.

- IDS reddettiği, düşürdüğü bu paketlerin payload'ını kontrol etmediği için atak olup olmadığına karar vermez.

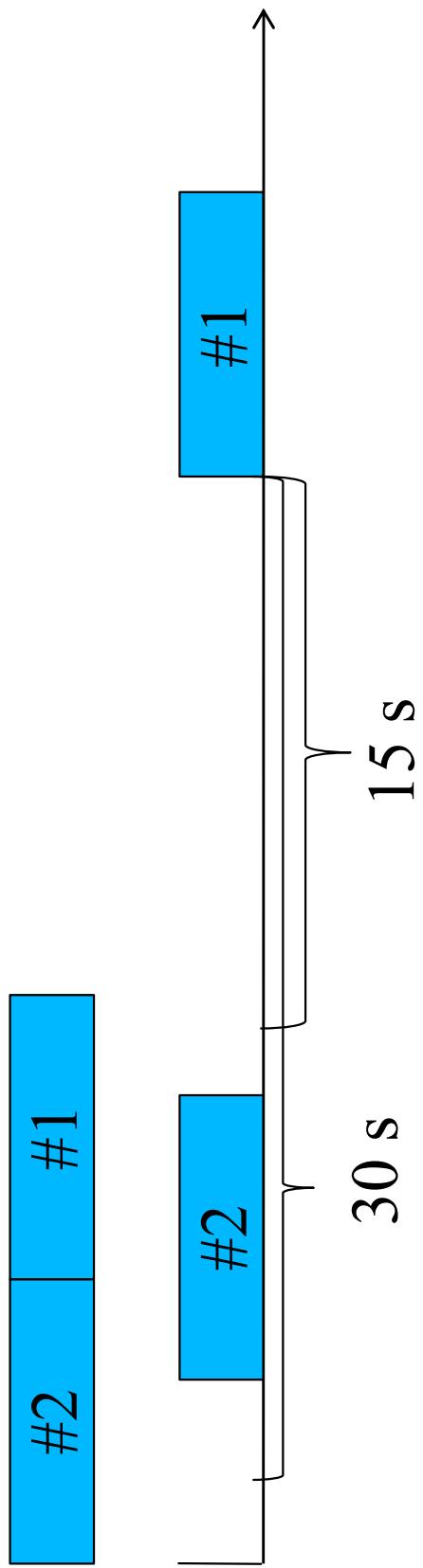
- Böylece saldırgan, kötü niyetli trafiğin bir kısmını veya tamamını IDS'nin denetiminden kaçırarak ağa göndererek ağa göndermiştir.



IDS evasion Attack [PN98]

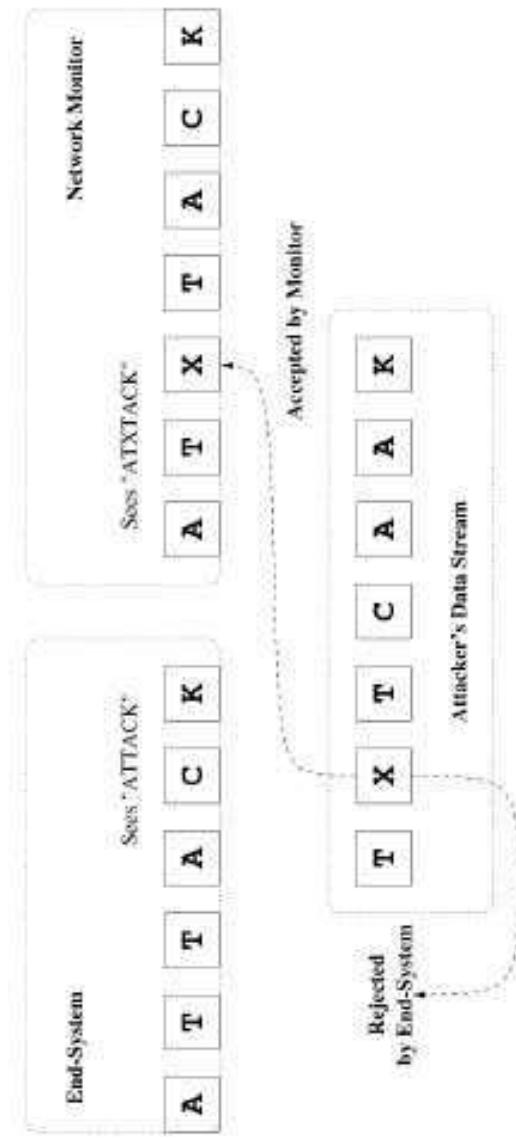
Evasion Attack (Atlatma Atakları)

- Bir saldırgan ilk fragmenti, timeout'u 15s olan IDS'ye ve timeout'u 30s olan hedef sisteme gönderir.
- Saldırgan 15s ile 30 s arasında bir zamanda ikinci fragmenti gönderir.
- IDS 2.fragmenti iptal eder. Çünkü timeout'u 15 s'den büyuktur. Fakat hedef sistem bu fragmenti kabul eder. Oysa bunun içinde bir atak olma ihtimali vardır.
- Böylece IDS atağı kayıt edemez. IDS atlatalmış olur.



2- Insertion attack (Araya koyma, Ekleme Atakları) :

- Bu ataklarda; hem son kullanıcıya hem IDS'ye gönderieln paketlerden, Son kullanıcının kabul etmediği, IDS tarafından kabul edilenler olabilir.
- Paket sadece IDS'de geçerlidir. Bu durumu uygun kullanabilen saldırgan; uygun bir paket trafigi ekleyerek imza analizi呸itindeki analizi önleyebilir (Son kullanıcı tarafından kabul edilmeyen paket ile, o paket gurubunun saldırısı olmadığı IDS'ye inandırılır.)



IDS insertion attack [PN98]

3- DOS(Denial of Service) Atakları

- IDS veya sistem kaynaklarını tüketmek için veya tamamen devreden çıkarmak için yapılan saldırılardır. Bu şekilde IDS gelen trafiğin hepsini analiz edemez hale gelir.
- DoS saldırısının en yaygın türü veya özelliği, istekleri ile mağduru bunalmasıdır.
- Bu istekler bir seferde birden fazla kaynaktan gönderiliriyse, buna dağıtık DoS (DDoS) saldırısı denir.

Cok bilinen ataklardan baziları

Time to live field attacks : IP başlığının TTL alanı bir paketin düşürülmeden önce,

yönlendirildiği rota üzerinde kaç atlama yapabileceğini ifade ediyordu. Her yönlendirici kendisine gelen paketi yönlendirdiğinde TTL alanındaki değeri bir eksiltiyordu.

- Buna göre ,ağ yapısı (topolojisi) hakkında önceden bilgi sahibi olan saldırınlar, paketleri öyle ustalıkla düzenleyebilir ki paketler, ağdaki IDS'ler tarafından düşürülmeden önce (IDS tarafından TTL'den dolayı) hedef hosta normal (TTL değeri 0'lanmadan) gibi ulaşır.

Maximum transmission unit (MTU) : Saldırıgan hedef host ile kendisinin kullandığı en düşük MTU değerini, "yol MTU Keşfi" olarak adlandırılan bir teknik ile öğrenebilir.

- Eğer bu minimum MTU değeri IDS ile hedef host arasındaki [bağlantıda geçerli](#) ise; saldırın **b u minimum MTU** değerinden daha büyük bir boyutlu paket yaratıp "Dont Fragment " bayrağını 1 yapar. Böylece bu paketler IDS tarafından kabul edilir. Fakat daha düşük MTU'lu ağın后面的 router TARAFLANDAN (hedef bilgisayar bu Router'ın arkasındaki ağdadır) tarafından reddedilir.

- Bu bir "[IDS insertion](#)" atağıdır. Böylece, IDS bu paket gurubu için imza analizi yapamaz.

IP checksum verification : IP checksum doğrulaması yapmayan bir IDS sistemi (performans kaybı olmasın diye genlede yapmazlar), insertion ataklarına karşı duyarlıdır. Çünkü bu sistemler hedef host'un reddettiği paketleri kabul edip işleyebilirler.

- IP checksum doğrulama, parçalanma (fragmentasyon) veya taşıma katmanı saldıruları ile birlikte kullanılır.

Ağ katmanı Saldırıları ve Koruma

2

YÖNLENDİRME Protokollarına VE Routerlara

ATAKLAR

- Routerların (Yönlendiricilerin) görevlerini tekrar hatırlarsak;
- **Yerel ağdan gelen paketleri filtrelemek :** Paket filtreleme, network adresi (IP), servisi ve protokolüne göre bilgi transferini kontrol etmetir. Yönlendirici bu kontrolleri ACL'ler (Access-Control List –Erişim Listesi) yardımı ile sağlar. ACL'ler kendisine gelen verinin kaynak, hedef ip adreslerine, bilgisinin gideceği port adresine veya kullanılmak istenen protokole göre kısıtlamalar yapabilmektedir.
- **Paketlerin nereye gideceğine karar vermek:** Yönlendirici, kendine bağlı olan bilgisayarların network adreslerini tuttuğu gibi, kendisine bağlı veya kullanılan protokole göre bağımsız yönlendiricilerin network adreslerini de routing tablolarında tutmaktadır. Yönlendirici kendisine gelen paketlerin nereye gideceğini öğrendikten sonra bu adresi routing tablolarıyla karşılaşarak hangi port'undan yollayacağına karar vermektedir.
- Böylece ROUTER ,yerel ağları birbirine bağladığı gibi kurumun WAN'a bağlantı noktasını da oluşturmakta ve internet erişimini de sağlamaktadır.

IP Datagramların Yönlendirilmesi

- Farklı ağlar üzerindeki bilgisayarların haberleşmesi için ağlar arasında datagramların yönlendirilmesi gereklidir.
- Router'larda en az iki adet farklı ağa bağlanmak için iki ağ donanım arabirimini bulunmalıdır.
- Routerlar datagramları yönlendirebilmek için hafızalarında IP Datagram yönlendirme tabloları bulundurmalıdır. Bu tablolarda hedef ağa ulaşabilmek için uygun yönlendiricilerin bilgileri bulunur

Statik ve dinamik yönlendirme tabloları

İki şekilde yönlendirme tablosu oluşturulur.

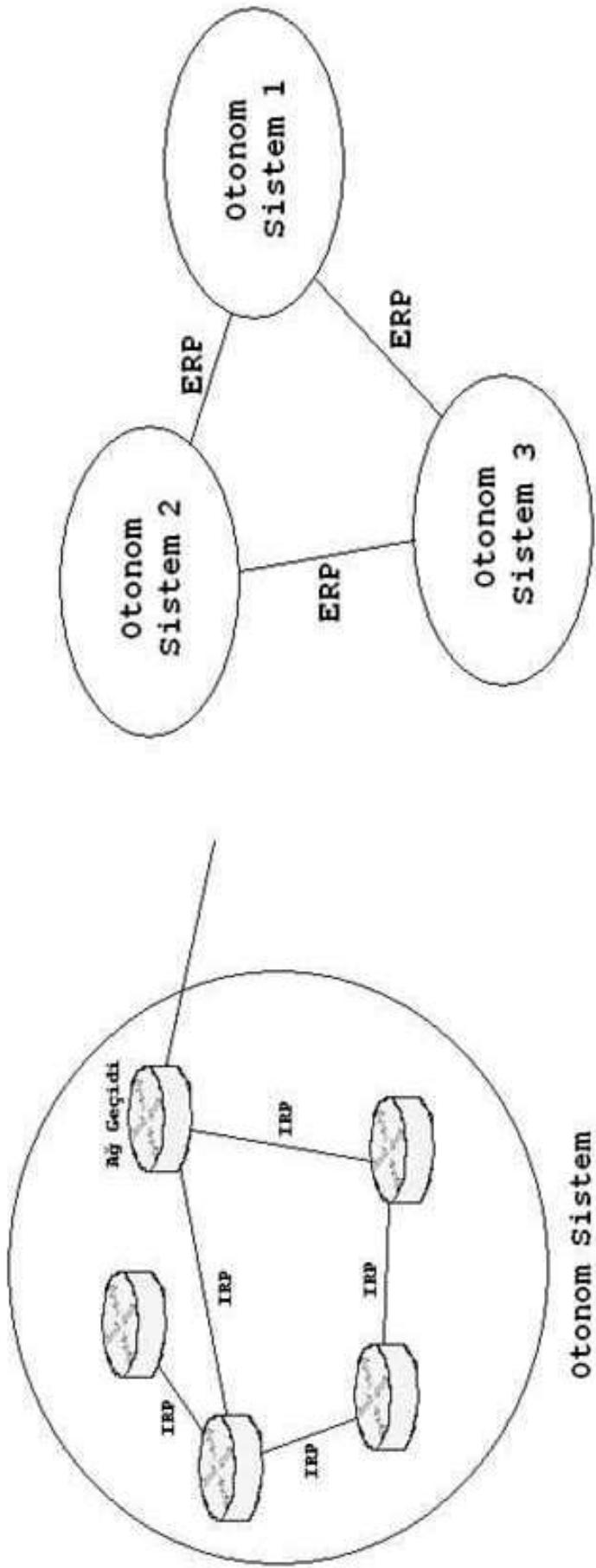
1-Dinamik yapılandırma: Routharlar bünyelerindeki yönlendirme tablo algoritmalarını çalıştırarak, komşularının durumuna göre en uygun ve hızlı yolları belirleyip tablolarını oluşturur ve güncellerler.

2- Statik yapılandırma: Hedef bilgisayar ağına bağlantı kurulabilmesi için tablo el ile doldurulur. Küçük ve yapısı değişmeyen ağlarda bu yöntem kullanılabilir.

IP datagram yönlendirme bilgilerinin routerlar arasında değişiminin etkin bir şekilde gerçekleşmesi için yönlendirme protokolları tanımlanmıştır. Bu protokolların devamlılığını sürdürmesi için mesaj değişiminin sürekli olması gereklidir.

DATAGRAM Yönlendirme protokolları

- Otonom sistemlerin kendi içindeki, temel yönlendirme değişim bilgisi için kullandıkları protokolleri IGP(Interior Gateway Protokolu) denir.
- Otonom sistemler arasındaki haberleşme için kullanılan routerların temel yönlendirme değişim bilgisi için kullandıkları protokolleri EGP(Exterior Gateway Protokolu) denir.



Yönlendirme Protokolleri

Protokollarından en çok bilinenleri

-RIP (*Routing Information Protocol - Yönlendirme Bilgi Değişim Protokolu*): Tablolarnı güncellemek için Uzaklık Vektör (Distance Vector) Algoritması kullanır.

-OSPF (*Open Shortest Path First- İlk önce en kısa yolunu seç*): Tablolarnı güncellemek için Link State algoritmasını kullanırlar.

EGP Protokollarından en fazla bilineni;

-BGP (*Border Gateway protocol – Sınır geçit protokolu*)

- Yönlendiriciler arasında, yönlendirme bilgileri IP datagramları aracılığı ile taşınır. Yönlendirme protokolları IP, TCP, UDP protokollarını kullanarak mesaj alış-verişini gerçekleştirir.
- *OSPF Protokolu* : IP datagramlarını kullanarak
- *RIP Protokolu* : UDP protokolunu kullanarak;
- *BGP protokolu*: TCP protokolunu kullanarak

Yönlendirme bilgisi mesaj alış-verişini sağlarlar.

RIP Versiyon 1 Mesaj Yapısı

IP V4 ağları içerisindeki Routerların diğer routerlara erişimi için en iyi rotayı sağlayan tablo bilgilerinin değişimi için kullanılan RIP mesajları UDP protokolunu kullanan RIP'ı kullanan Routrelar, yönlendirme bilgilerini güncellemek ve yönlendiricilerden yönlendirme bilgilerini istemek için 520 nolu UDP portunu kullanırlar.

2 tip RIP protokol mesajı vardır.

1-Yönlendirme bilgi yanıt mesajı

2-Yönlendirme bilgi isteği mesajı

Komut	Versiyon	Sıfır Alan	Komut Türü	Tanımı
Adres Belirteci	Sıfır Alan		1 (RIP İstek)	Yönlendirme yablosu gödeilmesi isteği.
IP adres	Sıfır Alan		2 (RIP Yanıt)	Yönlendirme tablo bilgilerinin gönderimi.
Sıfır Alan	Sıfır Alan		3	Bu komutun alındığı mesaj işleme konulmaz.
Sıfır Alanı	Sıfır Alanı		4	Bu komutun alındığı mesaj işleme konulmaz.
Metrik			5(Ayrılmış)	Sun Microsystem Taraflardan kullanılır.
Adres Belirteci	Sıfır Alanı			
IP adres	Sıfır Alanı			
Sıfır Alanı	Sıfır Alanı			
Metrik				
Düzenleme Bilgisi				

OSPF Genel Mesaj Başlığı

Versiyon	Tür	Paket Uzunluğu	Tür
0	Yönlendirici ID	16	1 Merhaba (Hello)
	Alan ID	8	2 Veritabanı (Database) tanımlaması
Kontrol Toplamı	Güvenlik Türü	32	3 Link Bağlantı n Durumu isteği
	Güvenlik Alanı		4 Link Bağlantı Durumu Güncellemesi
	Güvenlik Alanı		5 Link bağlantısı Durumu Bilgilendirmesi
			Güvenlik Türü
			0- Herhangibir şifreleme yok.

Genel OSPF Mesaj Başlığı yapısı

Versiyon: OSPF protokolünün versiyonu bildirir. Günlümüzde OSPF Version 2 kullanılır.
Yönlendirici ID:Mesajı gönderen Router'ın tanım alanı
Alan ID: Aynı alana ait routerların malan ID'si ayndır.

- 1 Merhaba (Hello)
- 2 Veritabanı (Database) tanımlaması
- 3 Link Bağlantı n Durumu isteği
- 4 Link Bağlantı Durumu Güncellemesi
- 5 Link bağlantısı Durumu Bilgilendirmesi

Güvenlik Türü

- 0- Herhangibir şifreleme yok.

- 1- Basit şifreleme metodu geçerli : Güvenlik alanı ile 64 bitlik şifreleme kullanımına imkan verer

Routing Protokollarına ataklar

- Distance-vector ve link-state routing protokolları özellikle DOS saldırılara çok uğrarlar.
- **RIP bir doğrulanmaz servis hizmeti olduğuundan DoS saldırılara karşı korumasızdır.**
- Sahte RIP paketleri göndерmek , ağ geçitleri ve hostların rotalarını değiştirmek ve onlardan bilgi sızdırma^k için yapıllır.
- Saldırganlar, yönlendirme bilgisini, networkte yeniden yönlendirmek için (onun şifrelerini analiz etmek için veya yolunu değiştirmek için veya zamanının değiştirmek için) değiştirebilir.

- Saldırgan yönlendiricinin routing protokolünü bozmadan
yollandan paketlerin bir kopyasının kendine de yollanmasını
sağlayabilir (kredi kart numaraları gibi verileri almak için) veya
protokollerini kaldırarak yönlendiricinin diğer yönlendiricilerle
haberleşmesini kesebilir.
- Haberleşmenin yok olması, yönlendiricinin aldığı paketleri
nereye göndereceğini bilmemesi ve servis dışı kalması(DoS)
anlamını taşımaktadır.

ROUTER



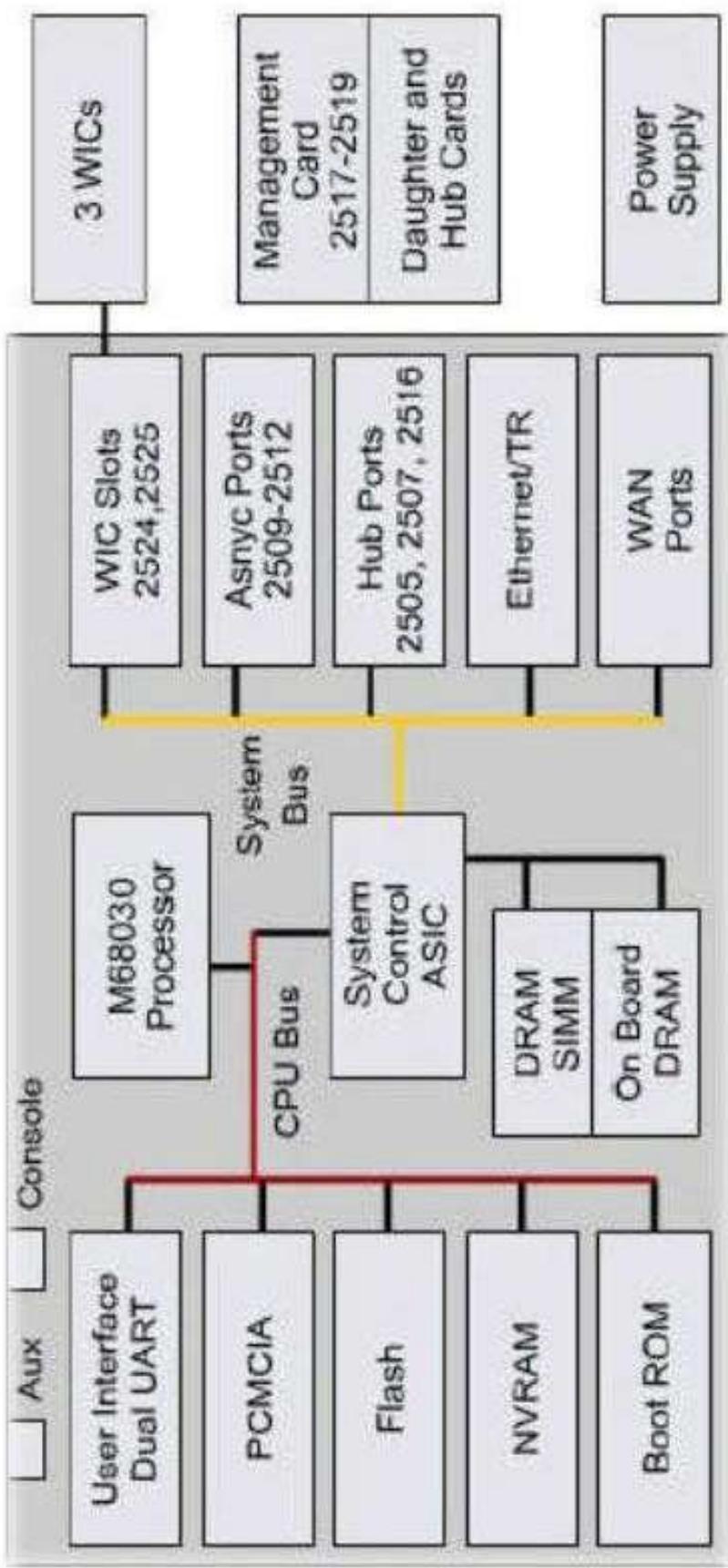
Resim 1.5: Yönlendirici arka paneli

Arka panelde;

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

Router (Yönlendirici) yapısı

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



Yönlendirici iç yapısı blok şeması

CPU: Bu işlemci yönlendirme parametrelerini ve ağ arayuzlerini 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. Yönünlendirici açılırken bootstrap, flash’tan işletim sistemi imajını ve NVRAM’den başlangıç konfigurasyonunu RAM bölgesine yükler. Çalışan yapılandırma (running -config) bu alanda tutulur. Ayrıca RAM’de yönlendirme tabloları ve gelen fakat iletilmemiş verilerde tutulmaktadır. Yapılan konfigürasyon, running-config dosyası olarak kayıt edilir ve RAM’de tutulur. RAM’deki running-config dosyası NVRAM’e kaydedilmemezse yönlendiricinin kapatılması durumunda, çalışan yapılandırma bilgileri kaybolur.

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

Interfaces: Her yönlendiricinin kendisine gelen bilgileri alması, gönderilmesi 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 gereklili fonksiyonları sağlamaktır. Bunun yanı sıra ağ yöneticisine, yapılandırılmışsa sağlama için bir ara yüz sunar.

Cisco yönlendiriciler, **IOS (Internetwork Operating System)** kullanırlar. Aşağıda Cisco IOS yazılıminin 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

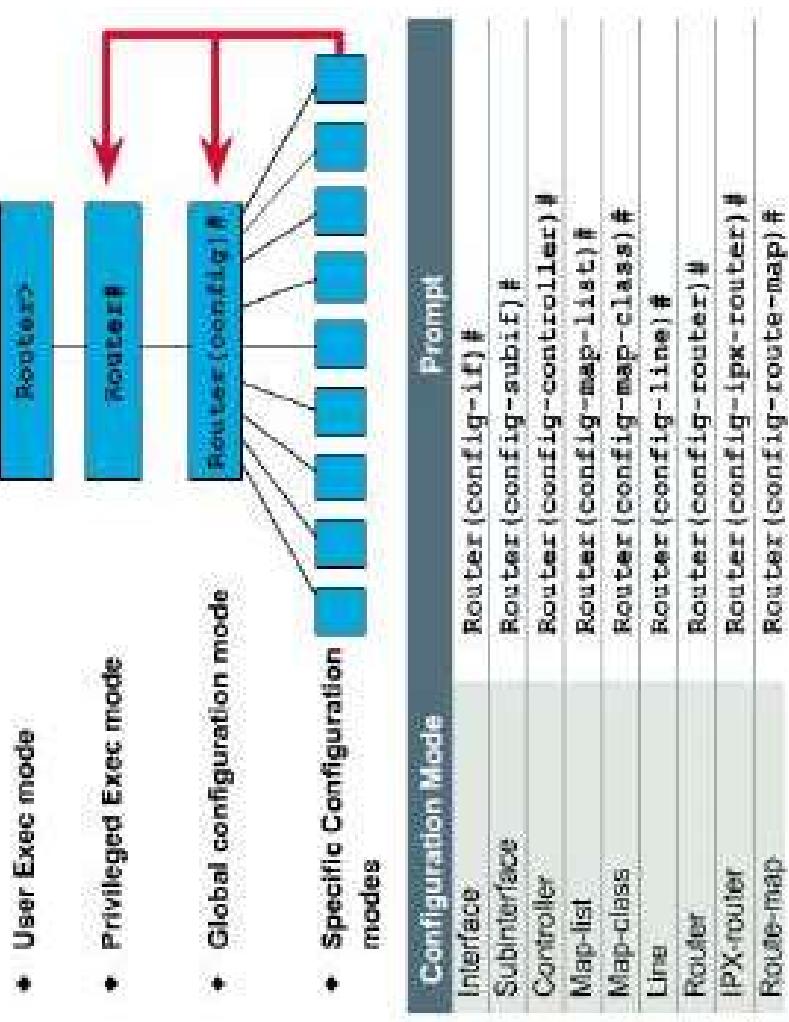
Routerların konfigürasyon (yapıllandırma) ayarlarını görmek ve değiştirmek için farklı kullanıcı seviyeleri (mod'ları) bulunmaktadır

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 geçiktikten sonra yönlendiriciye tamamen hâkim olur. Privilege 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 moda yapılan değişiklikler bütün yönlendiriciyi etkiler. Bu moddayken “**(config)#**” şeklinde gözükmür.

Overview of Router Modes



Configuration Mode

Interface

Subinterface

Controller

Map-list

Map-class

Line

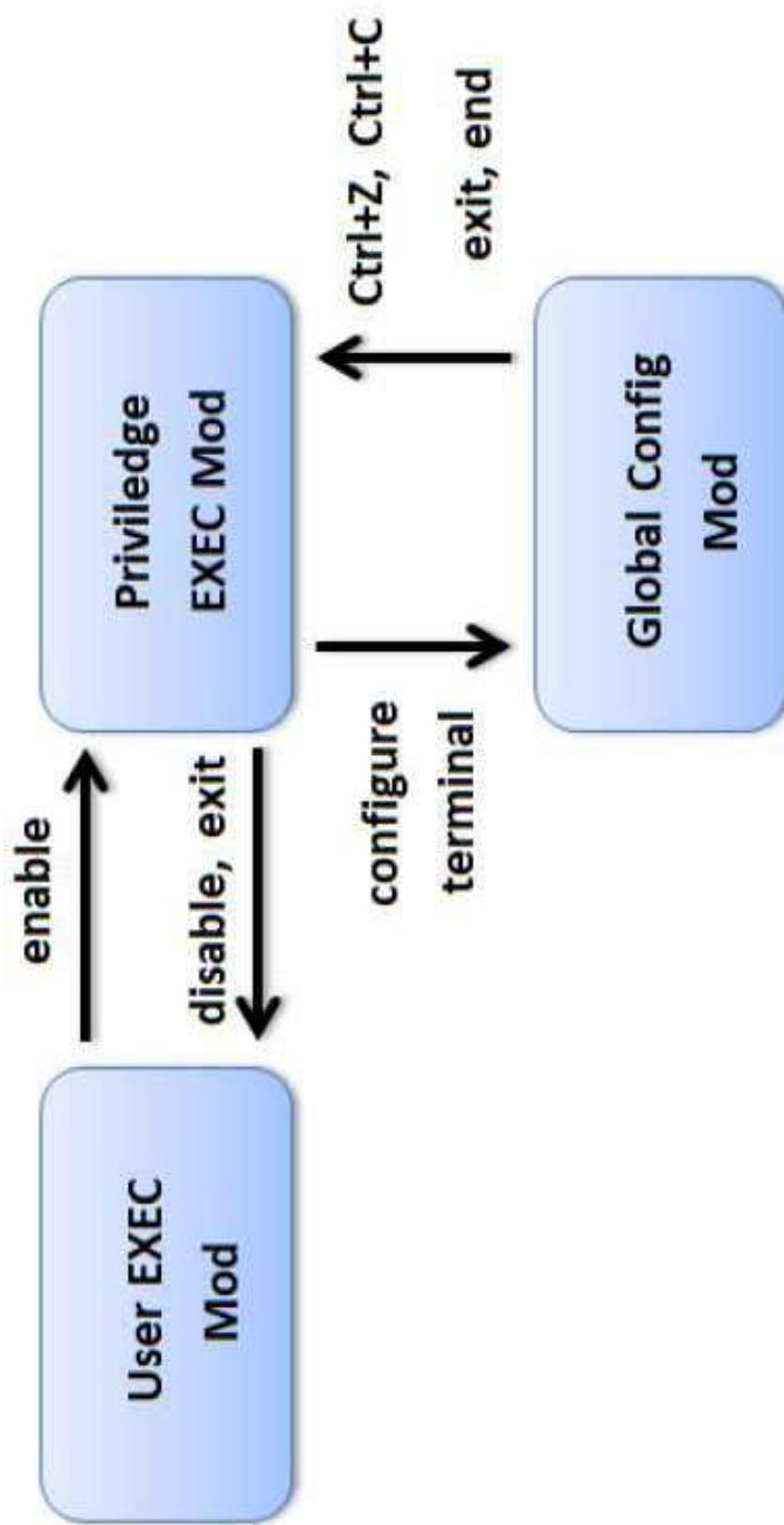
Router

IPX-router

Route-map

Prompt

Yönlendirici Çalışma modları arası geçiş



Resim 3.5: Modlar arası geçiş işlemleri

Router'ların GÜVENLİĞİ

Fiziksel Güvenlik:

Yönlendiriciler için ayrı bir oda ayıramamıysa en azından kilitli dolaplar (kabinet) içine koyulmalıdır. Bu odanın enerjisi hiç kesilmemelidir . Bu UPS (Uninterrupted power supply) kullanarak sağlanabilmektedir. Yönünlendirici yakınlarına şifre veya ip bilgileri gibi bilgileri yazmaktan kaçınmaktr.

2.Yönlendiriciye Erişim Hakkları

Yönlendiriciye kimlerin erişeceğini bir politikayla belirlenmesi ve erişimlerin loglanması gerekmektedir. Bu politikada; kimin konfigürasyon yedeklerini alacağıının, kimin yeni bir parça alımında yönlendiriciye yerlestireceğinin, kimin logları takip edileceğinin açık 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-encryption” komutu kullanılmalıdır.

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

Router güvenliği-3

4.Erişim Protokollerinin Güvenliği

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

Düzenler erişim yöntemleri olan HTTP, Telnet, SSH, TFTP, ve FTP kullanıldığından 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) yazarak 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 cihazların birçoğunu üzerinde web sunucusu çalışır. Bu da 80 nolu portta bir web sunucunun kurulu beklediğini gösterir.

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

Ama web üzerinden yönetim gerekiyorsa web sunucusu sadece sistem yöneticisinin bacağı bir port üzerinden, örneğin “*ip http server port 500*”, komutıyla 500 nolu portta çalıştırılacak 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 oluşturmaktadır. Özellikle hub bulunan ortamlarda saldırganın ağ üzerinden dinleme (sniff) yoluya 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) kullanıldığından bu doğrulama dizilerinin spoof edilmesi söz konusu olabilmektedir. Bu yüzden MD5'a dayanan öz (*digest*) doğrulama şeması kullanın, yönetim verilerine kısıtlı erişim sağlayan SNMP Versiyon 2 veya 3'ün kullanılması gerekmektedir.
- **Doğrulama Mekanizmaları Sağlamak:** Doğrulama mekanizması, onay sunucuları(Tacacs+, Radius ...vb) kullanılarak yapılabılır. Cisco IOS'de doğrulama mekanizması “*ip http authentication*” komutıyla 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 ağır ihtiyaçlarına uygun ve aynı zamanda donanımın desteklediği bir versiyon olmasına dikkat edilmeliidir. Her ne kadar işletim sistemleri güvenlik testlerine tabi tutulup daha sonra piyasaya sürülüğeyorsa da daha sonradan güvenlik açıkları bulunabilmektedir. Bu nedenden dolayı çıkan yamaları takip edip upgrade yapmak gerekebilir.

AĞI ROUTER İLE KORUMAK

Yönlendirici, bazı ağlarda yönlendirici görevinin yanı sıra güvenlik duvari gibi çalışacak şekilde de ayarlanabilmektedir. güvenlik duvari 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 özelliklerini ile kullanmak, sadece küçük ağlarda veya güçlü omurga cihazlarının bulunduğu kampüs ağlarındaki iç yönlendiricilerde tercih edilmelidir.

Ağlı R ile korumak-2

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

1. Riskli portları kapatmak:

İnternet üzerindeki servisler, kullanıcılar 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 önlemeyi bir yolu riskli portları kısıtlamaktır. Riskli portların listesi [<http://www.nsa.gov/snac/cisco/guides/cis-2.pdf>] adresındaki 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
```

Ağlı R ile korumak-3

2.Bazi 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 adresine cevap verir. Böylece erişim listesine takılmadan bilgisayar ağına sızmış olur.

Bunu önlemenin yolu, yönlendiricinin kaynak adresi hedef makinaya varmadan kimseye göstirmemesidir. Bu işlem Cisco cihazlarda “*no ip source-route*” komutıyla yapılabilir.

Routing Protokole olan saldırlılar: SalDIRGan yönlendiricinin routing protokolünü bozmadan yollanan paketlerin bir kopyasının kendine de yollandanmasını sağlayabilir veya protokollerı 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 filtrelemektir. Örneğin IGRP routing protokolünüfiltrelemek 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
```

Ağ İle korumak-4

Çıktı (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*) filtrelene *dennektedir*. Bu kontrolden gelen paketlerdeki ip 'lerde internet ortamında kullanılmayan (rezerve edilmiş) adresler bulunduğuunda 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 aşağıdaki gibi olacaktır:

```
access-list 101 deny ip 10.0.0.0.255.255.255 any  
access-list 101 deny ip 172.16.0.0.15.255.255 any  
access-list 101 deny ip 192.168.0.0.0.255.255 any  
access-list 102 deny ip 200.100.17.0.0.0.255 any  
access-list 101 permit ip any an
```

Ağlı 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 çıkışmak isteyen ip'ler kısıtlanmalıdır.* Böylece kurumun ağı kullanılarak başka kurumlara yapabilecek kaynak IP adresi değiştirme tabanlı saldirılar 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
```

Ağlı R ile korumak-6

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

```
ip cef distributed  
!  
interface serial 0  
ip verify unicast reverse-path
```

Ağlı R ile lorumak-7

Smurf attack: IP adresi kandırmacısı 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 bilgisayarin ağa ulaşması engellenir. Bu olayı yönlendiriciden önlemin bir yolu da yönlendiricideki arayüzlere

“*no ip directed-broadcast*” komutunu girmektir.

ICMP (Internet Control Message protocol) Protokolu

- IP protokolu bağlantısız bir protokol olduğundan, ağda seyahat eden datagramların iletim ve teslimat sürecinde meydana gelen hataları, uyarı ve kontrol bilgilerinin alışverişi için ICMP protokolu kullanılır. Bu mesajlar ağ yöneticileri tarafından değerlendirilerek ağ içerisindeki aksaklılıklar belirlenir.
- ICMP iletilleri IP datagramları içerisinde Kapsüllenenek seyahat eder.

- ICMP mesajları aşağıdaki fonksiyonlar içindir:

- **İstekler (Request)**
- **Yanıtlar (Responses)**
 - **Hata nesajları** : ICMP hata mesajı; başlık ve soruna neden olan IP datagram payload'ının bir kısmını içerir (ilk 8 byte).

ICMP Hata mesajları aşağıdaki durumlarda üretilir.

- IP datagramlarının hedefe ulaşamaması durumunda
- Ağ geçitlerinin, datagramları hedefe yönlendiremeyecek kadar yoğun olmaları durumunda
- Datagramların hedeflerine gidebileceği daha uygun bir yol olması durumunda.

- Routerlar, datagramları yönlendirirken oluşabilecek problemleri bildirmek için ICMP mesajı üretebilirler.
- Bilgisayarlar; protokol ve servis problemleri yaşadıkları zaman ICMP mesajı üretirler.
 - Bilgisayar veya ağ testleri için veya ağdan bilgi elde etmek içinde ICMP mesajları kullanılır. (Request ve Response)
 - **Sadece IP datagramlarıyla ilgili olaylarda ICMP mesajı üretilir.**
- Parçalanmış IP datagramlarda oluşacak hatalarda sadece ilki için ICMP mesajı iletilir.
- ICMP mesajlarının seyahat ile ilgili problemler için ICMP mesajı üretilmez.

ICMP Mesaj Formatı

MAC header	IP header	ICMP header	Data
------------	-----------	-------------	------

ICMP header:

Type	Code	ICMP header checksum	Data
------	------	----------------------	------

Type. 8 bits.

Specifies the format of the ICMP message.

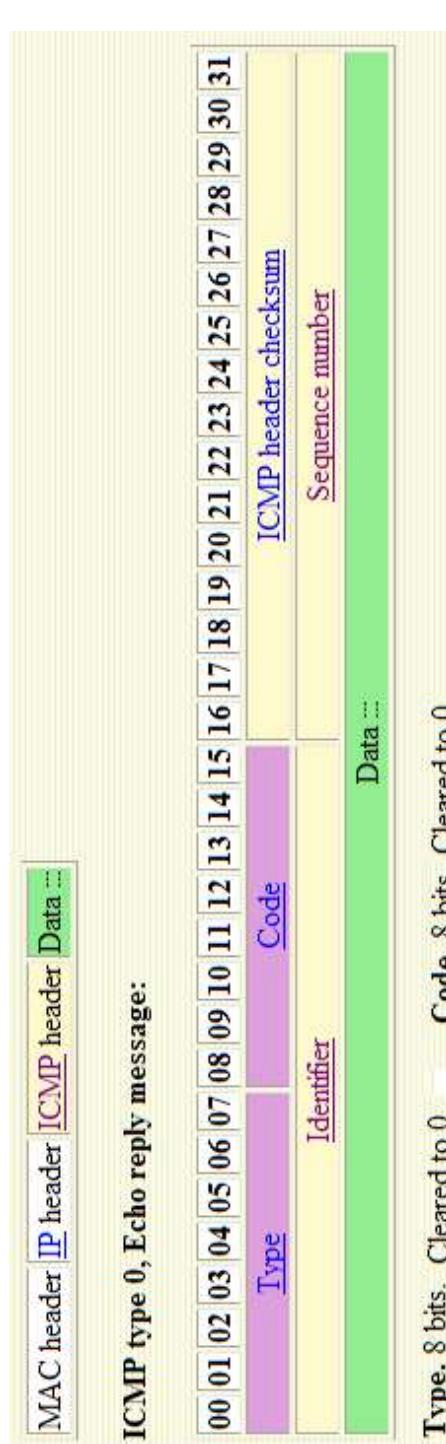
Type	Description		
0	Echo reply.	11	Time exceeded.
1		12	Parameter problem.
2		13	Timestamp request.
3	Destination unreachable.	14	Timestamp reply.
4	Source quench.	15	Information request. Obsolete.
5	Redirect.	16	Information reply. Obsolete.
6	Alternate host address.	17	Address mask request.
7		18	Address mask reply.
8	Echo request.	19	reserved (for security).
9	Router advertisement.	20	- reserved (for robustness exp
10	Router solicitation.	21	-
		22	Reserved
		23	255
		24	
		25	
		26	
		27	
		28	
		29	
		30	Traceroute.
		31	Conversion error.

Çok kullanılan ICMP Mesajları

Type	
0	Echo Reply (Yankı): hedefin ulaşılabilir olduğu denetimi için.
3	Destination Unreachable: hedefin erişilemez olduğunu belirler
4	Source Quench: Rotadaki router'ın çok yoğun olduğunu belirtir.
5	Redirect: Routerlar rota belirlemek için kullanır.
8	Echo Request
11	Time Exceeded : Zaman aşımı- TTL'in 0'landığı bilgisi
12	Parameter Problem : IP datagramda oluşan problemleri bildirir.
13	Timestamp : Paketlerin iki nokta arasındaki gidiş süreleri için.
14	Timestamp Reply:
15	Information Request
16	Information Reply

En çok kullanılan mesaj türüdür (Echo 0 - 8) . “Yanıt-istek-yanıt” mesajları olarak bilinir. Ping komutunun kullandığı mesaj’dır.

Ping ile sorgulanın bilgisayara echo istek (8) ile bir miktar bilgi gönderilir. Hedef bilgisayardan ise kendisinin gönderdiği verinin aynılığını yanıt (echo reply 0) ICMP mesajını göndermesini ister. Bu bildirim yapılmış ise iki nokta arasında iletişimimin yapılabılır olduğu anlaşılmır.



MAC header		IP header		ICMP header	Data
Type	Code				
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31					ICMP header checksum
	Identifier				Sequence number
		Originate timestamp			
		Receive timestamp			
		Transmit timestamp			

Type. 8 bits. Code. 8 bits.
Set to 13. Always cleared to 0.

MAC header		IP header		ICMP message 14	Data
Type	Code				
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31					ICMP header checksum
	Identifier				Sequence number
		Originate timestamp			
		Receive timestamp			
		Transmit timestamp			

Message format:

Type. 8 bits. Set to 14. Code. 8 bits. Always cleared to 0.

ICMP type 4, Source quench message:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Type. 8 bits. IP header + the first 64 bits of the original datagram's data.

Type. 8 bits. Set to 4. Code. 8 bits. Always cleared to 0. unused. 32 bits. Cleared to 0.

- **Parametre sorunu:** Bilgisayar veya router, başlık üzerinde IP datagramın iletilmesine mani bir durum olduğunu tespit ederse, datagramı yo edip karşıya bildirmesi içinir.

ICMP type 12, Parameter problem message:

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Type. 8 bits. Pointer. IP header + the first 8 bytes of the original datagram's data.

Code	Description
0	Invalid IP header.
1	A required option is missing.

ICMP mesajlarını kullanan programlar

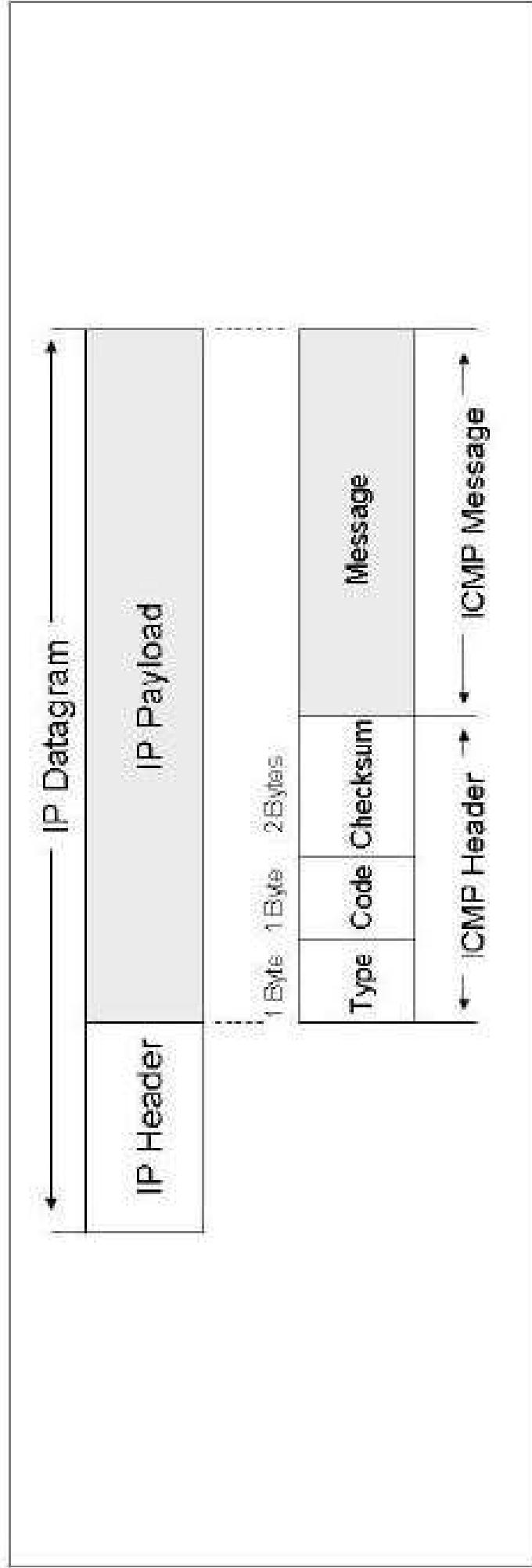
- **Ping** ve **traceroute** uygulamaları ICMP protokolunu kullanır.
- **Ping**: en çok kullanılan ağ analiz programlarından birisidir.
- Ping, hedef bilgisayara “yankı (echo) istek” mesajı gönderir. Eğer hedef bilgisayardan “yankı(echo)” yanıtı gelirse, Ağ üzerinde erişilebilir olduğu anlaşılır.
- Ping her gönderdiği mesaj üzerine gönderilme zamanını ekler. Alınan yanıtı kullanarak paket iletimi için geçen zamanı bulabilir.
- **Traceroute**: Datagramların hedeflerine ulaşıcaya kadar izledikleri rotanın belirlenmesi için kullanılan bir analiz programıdır.

ICMP ATAKLARI

- ICMP mantıksal hataları teşhis ve bildirim için kullanılır.
- ICMP kimlik doğrulaması sunmaz.
- Böylece ICMP, ağdaki cihazları tarama ve istismar etmek için kullanılabilir.
- ICMP kullanımı ile, backdoor, port scan, redirect trafik, echo gibi DoS atakları düzenlenebilir.

ICMP Format

Figure 4.12 The ICMP Format



ICMP Echo Atakları

- Ping (ICMP ile gerçekleşir) bombardımanı saldırının amacı, büyük miktarda ICMP yanıt istek paketlerini ağa yollayarak bant genişliğini kullanıp ağ kaynaklarını tüketmektedir.
- Alınan her ICMP yanıt istek (request) paketine karşılık, ICMP yanıt cevap paketininde yayındığına dikkat ediniz.
- Özellikle bant genişliği düşük olan ağlarda bu ataklar önemlidir.

Port Scanning

- ICMP, “hangi portların açık olduğunu keşfetmek için”, saldırganlar tarafından büyük oranda kullanılır.
- Çünkü TCP protokolu gibi bağlantılı bir protokol olmadığından saldırganlar için paha biçilmez bir araçtır.
- Bir bağlantı noktasına bir ICMP paket göndерilmesi ile portun açık olup olmadığını bildiren bir yanıt alırsınız.
 - Eğer port açık ise; bir cevap gelmeyecektir.
 - Eğer port kapalı ise; ICMP *tip3 code3* olan bir ICMP mesajı alınacaktır. (Hedef ulaşamaz, Port ulaşamaz).

Port Scanning (cont.)

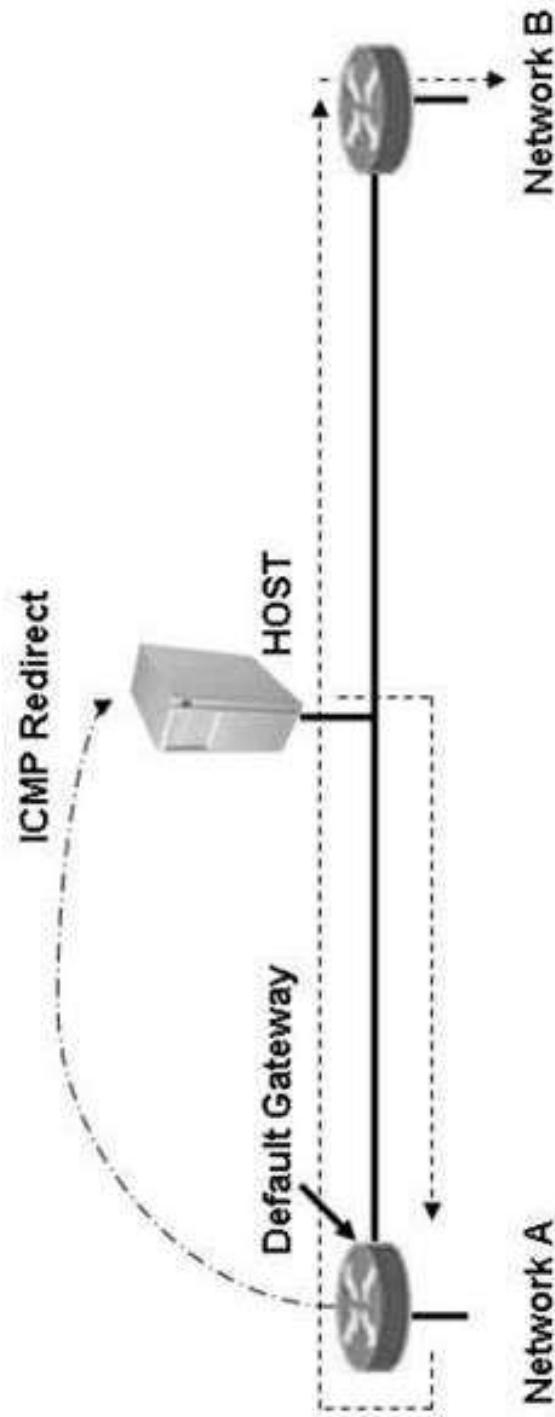
Figure 4.19 Port Scan

ICMP Nuke Atakları

- Bilgisayarlar çoğu zaman aralarındaki bağlantıının sağlamlığını birbirlerine ICMP paketleri göndererek anırlar.
- **ICMP Nuke Atağı;** Sahte adresler (spoof edilmiş) kullanarak, bir saldırgan; iki host arasındaki düzgün iletişim “Time Exceeded” (Type 11) veya “Destination Unreachable” (ICMP Type 3) mesajlarını her iki hosta’da göndererek, sanki hata varmış gibi gösterebilir, bozabilir.
- Bu bir DOS atağıdır. Eski bir atak türüdür.
- [ICMP Types and Codes](#) ‘lar konusuna bir gözat.

ICMP Redirect Attack (ICMP yeniden yönlendirme atağı)

- Bir saldırgan; ICMP “redirect” mesajlarını göndererek, bir hedef router'a yönlendirilmiş mesajları, IP adresi saldırganın adresi olan bir host'a forward eder.



ICMP Redirect Ataklarını Önleme

- Linux işletim sisteminde, kernel'de değişiklik yaparak redirect mesajlarının kabul edilmemesini sağlayabiliyoruz.

```
root@router# echo 0 >  
/proc/sys/net/ipv4/conf/eth0/accept_redirects
```

```
[root@localhost eth0]# pwd  
/proc/sys/net/ipv4/conf/eth0  
[root@localhost eth0]# ls  
accept_redirects [REDACTED] mc_forwarding  
accept_source_route disable_policy shared_media  
arp_accept disable_xfrm tag  
arp_announce force_igmp_version proxy_arp  
arp_filter forwarding rp_filter  
arp_ignore log_martians secure_redirects  
[root@localhost eth0]#
```

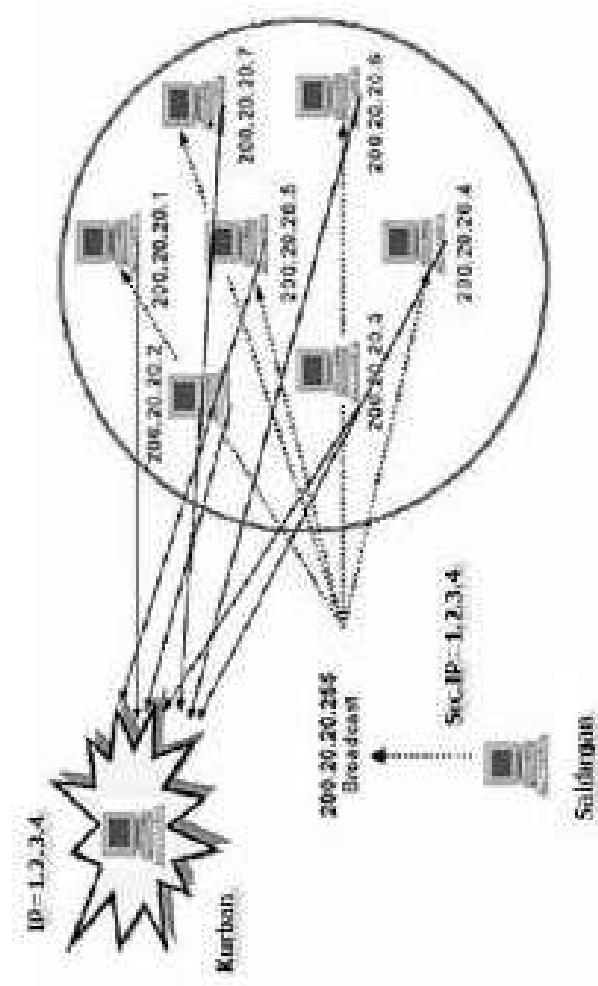
ICMP Flood (ICMP Taşkını-Sel basması Bombardımanı)

- Ping Flood, bir ping (ICMP üzerinden yapılır) broadcast firtinası yaratarak hedef sistemi buntaltabilir. Bu bir DoS saldırısıdır.
- Linux'ta, ping -f kullanılarak herhangibir host'a bir taşkin oluşturulabilir.

root@router# ping -f 10.10.10.12 -c 1000

ile 10.10.10.12 IP'li host'a 1,000 paket gönderilir.

IP ping paketinin işleyişinden yararlanan “Smurf saldırılı” da ICMP FLOOD'un özel bir halidir. Çok sayıda reply paketi ile hedefin gerçek trafiği alması engellenir. Smurf ataklarında; kurban bilgisayarın IP adresinden network'ün broadcast adresine Internet (ICMP) isteği (ping) gönderilerin ve network üzerindeki bütün bilgisayarlardan kurban bilgisayara yanıt göndermesi sağlanır.



Ping Flood'dan korunma

- Ping flood, IPTable 'in konfigürasyonu ile “ICMP echo-request messages” larının sayısını sınırlayarak durdurulabilir.

```
root@router# iptables -A FORWARD -p icmp -i cmp-  
type echo-request -m limit -limit 10/s -j  
ACCEPT
```

(sanıyede 10 tane gelen icmp echo request paketlerini kabul et)

```
root@router# iptables -A FORWARD -p icmp -i cmp-  
type echo-request -j DROP  
( ICMP echo-request paketlerini düşür )
```

Not:iptables, Linux veya Unix' te NAT' lama veya paket filtreleme için bir araçtır.

Ping of Death

- Ping of Death, IP paketlerine gömülü olarak ICMP ile gönderilen “echo request” mesajları ile yapılır. Bu mesajlar 65.535 bayt’tan daha büyük mesajlar halinde sürekli olarak gönderilirse Buffer kapasitesi küçük olan makinalarda buffer taşmasına sebep olarak makinanın çökmesine sebep olur. Ping of death bir DoS atağı çeşididir.

Windows komut satırından:

```
ping -1 65550 192.168.1.X
```

Linux komut satırından:

```
ping -s 65550 192.168.1.X
```

TCP/IP Zayıflıkları Ve Çözümleri

Hedefe ulaşan veri, IP paketlerinden olusmaktadır. Bu paketlerde:

- **Gizlilik (Confidentiality):** Paketin seyrettiği yol boyunca içeriği okunmamak olabilir.
Önlem: İçerigin sifrelenmesi.
- **Paket Doğrulama (Authentication):** Paketin kaynak adresi değiştirilebilir (Örn:spoof saldıruları).
Önlem: Daha kuvvetli doğrulama yöntemlerinin kullanılması.
- **İçerik bütünlüğü (integrity):** Paketin içeriği değiştirilmiş olabilir.
Önlem: Daha gelişmiş data bütünlüğü kontrolерinin yapılması.

- **YÖNLENDIRİCİ GÜVENLİĞİ**
- Sedat Kuldük, Enis Karaaslan,
- kulduk@bornova.ege.edu.tr,
enis@bornova.ege.edu.tr
- Ege Üniversitesi Network Güvenlik Grubu

OSI 4.katman (Transport - İletim layer) Güvenliği

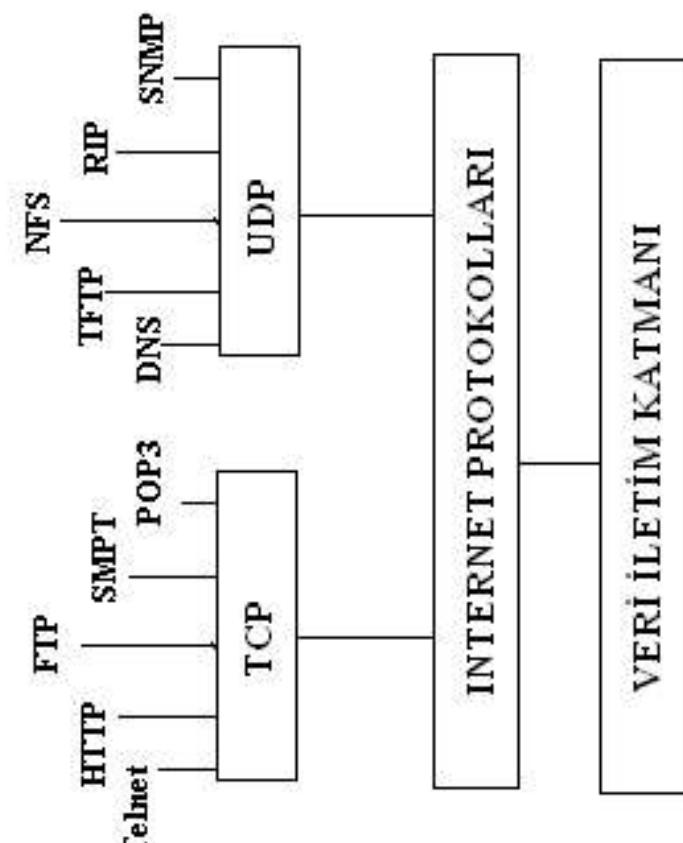
İletim katmanı protokolları

OSI modelinde, farklı ana sistemler üzerindeki uygulamalar arasında iletişimi sağlayan katman **transport katmanıdır**. Bu katman bünyesinde, TCP ve UDP gibi veri iletişiminin farklı şekillerde sağlamak üzere iki protokol barındırır.

- **TCP (Transmission Control Protocol)**; bağlantıda olan iki ucun senkonize olarak çalışmasını sağlar, hata denetimi yapar, güvenli veri akışını sağlar.

- **UDP (User datagram Protocol)** ise iletişim içinde olan iki nokta arasında senkronizasyon öngörmez, güvenilir olmayan veri akışı gerçekleştirir.

- Tek başına TCP ve UDP protokollerini kullanarak uzaktaki makinalara doğrudan veri iletimi yapılamaz. Fakat aynı bilgisayarda çalışan uygulamalar arasında veri iletişimi yapılabilir.



TCP protokolu, iki uç arasında bağlantıya dayalı güvenilir bir veri akışı sağlarken, UDP protokolunda gönderilen veri paketlerinin hedef bilgisayara ulaşacağı garanti edilemez. Akış kontrolü sağlanmaz. UDP genellikle, gönderilen paketlerin sadece belirli bir aktif cihazı hedef aldığı uygulamalarda kullanılır.

TCP Protokolu

- TCP protokolu; bilgisayarlarda çalışan uygulamalar arasında;
<istemci IP adresi, Port No>, <Sunucu IP adresi, Port no> ikililerini temel alan bağlantı kurar. Her TCP bağlantısı bu ikililerle ifade edilir.
- IP protokolu bağlantısızdır. Dolayısıyla gönderilen paketlerin yerlerine ulaşlığını garanti etmez. Bu açığı kapatmak için, bağlantılı ve güvenli veri akışını sağlayan TCP protokoluna ihtiyaç duyulur.
- TCP protokolunu kullanan uygulamalar veri göndermeden önce bağlantı kurmak zorundadırlar.
- TCP, bağlantıda olan bilgisayarlar arasındaki güvenli veri iletişimini sağlayan, sanal devre mantığıyla çalışan bir protokoldür.
- Hata denetimi yapar
- Güvenli veri iletimi sağlar.
- Bağlıktıda olan bilgisayarlar arasında akış, **tıkanıklık** kontrolu sağlar.
- Çoklama (Multiplexing) yöntemiyle birden fazla bağlantıya izin verir.
- Sadece bağlantı kurulduktan sonra veri iletimi sağlar.
- Gönderilen mesaj parçaları için, önceli, güvenlik tanımlamaları yapılabilir.

- Veriler, 8 bitlik guruplar halinde (bunlar 1 bayt olabileceği gibi binlerce bayt'lık guruplar şeklinde de olabilir) işaretlenerek (numaralanarak) gönderilir. Örneğin bir TCP uygulamasının 1024 oktetlik bir veri yollaması gerekiyorsa, bu bilgiler 1024 tane 1 oktetlik veya 256 tane 4 oktetlik parçalar halinde gönderebilir.
- İşaretlenerek gönderilen her parça için , alıcı uçtan cevap beklenir.
- TCP gönderdiği her parçayı numaralandırır. Bu no'lar kullanılarak, verilerin gönderildiği sıra ile alıcı tarafından alınması sağlanır.
- Gonderilen her veriye atanın dizi numarası sayesinde hangi verinin hedefe ulaşıp ulaşmadığı kontrol edilir. Dizi no TCP başlığı kismındadır.
- Alıcı ise TCP bağlantısı ile aldığı her pakete karşılık yeni bir mesaj parçasını göndericiye bildirir. Bu mesajın başlığındaki ACK no'su ise gönderilmesi beklenen bir sonraki parçanın sıra numarasını da barındırır.

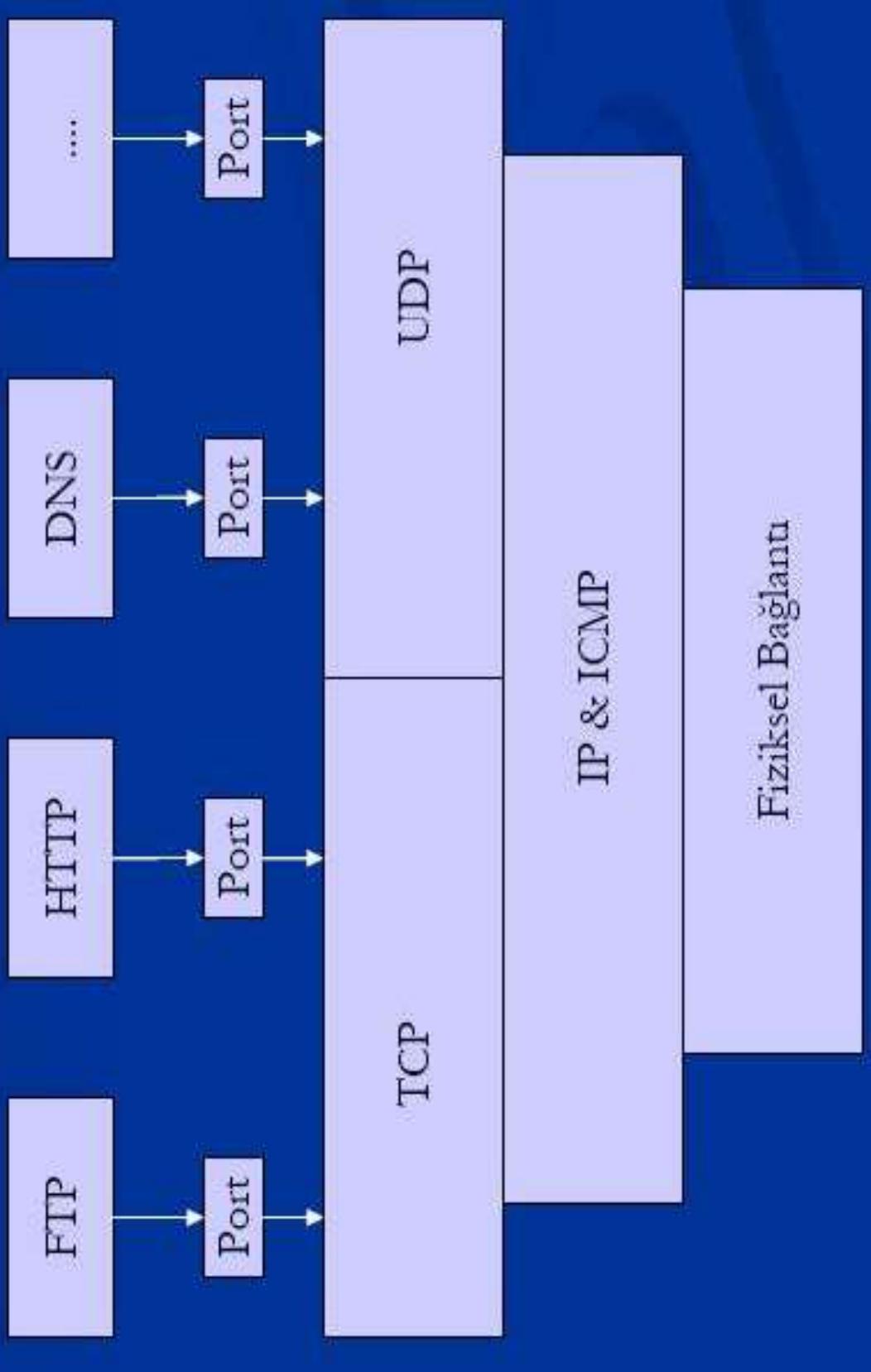
- TCP protokolu her iki yönde de veri akışına imkan sağlar (yani her iki trafta biribirlerine veri gönderebilirler. Gönderilen veriler byte(8 bitlik) grupları şeklinde değerlendirilir.
- Bağlantı kurulması $< IP\ adres1, port\ no\ 1, [IP\ adres2, portno2]>$ gibi iki noktası arasında gerçekleşir. Seçilen port no'lar uçlardaki uygulamalar tarafından farklı şekilde seçilmiş olabilir. Biribirleriyle aynı olma zorunluğu yoktur.
- Yukarıdaki parametreler sayesinde bilgisayarlar arasında birden fazla TCP bağlantısı sağlanabilir.

PORT KAVRAMI

- Bir Host'un diğer host üzerindeki değişik servisleri (hizmetleri) kullanabilmesi için veya değişik bilgisayarların aynı bilgisayardaki bir servisi kullanılabilmesi için bu servisi tanımlayan adreslemeler vardır.
- TCP protokolunda her ucta 2^{16} tane farklı TSAP adresi tanımlıdır. Bu adreslere PORT denir.
- Uç düşüğünün 32 bitlik IP adresi ve 16 bitlik port adresinin beraber kullanılmasına **soket no** denir. Bir soketin blok seması aşağıda verilmektedir.

Port no (TSAP Adresi)	IP Adresi
--------------------------	-----------

Port Kavramı

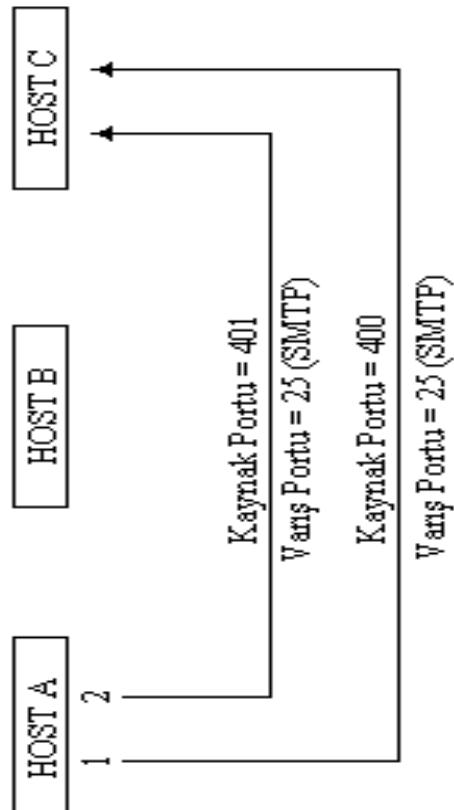


Transport (Ulaşım)Katmanı

Numarası	İsim	Tanımı
5	RJE	Uzaktan iş yürütme
7	ECHO	Eko
11	USERS	Aktif kullanıcılar
13	DAYTIME	Gündüz
20	FTP-DATA	Dosya transferi (veri)
21	FTP	Dosya transferi (kontrol)
23	TELNET	TELNET
25	SMTP	Basit mail transferi
37	TIME	Zaman
42	NAMESERV	Host isim sunucusu
43	NICKNAME	Takma-ad
53	DOMAIN	Domain name server
67	BOOTPS	Bootstrap protokol sunucusu
68	BOOTPC	Bootstrap protokol istekçisi
69	TFTP	Onemlisiz dosya transferi
79	FINGER	Finger
101	HOSTNAME	NIC host ismi sunucusu
102	ISO-TSAP	ISO TSAP
103	X400	X 400
104	X400SND	X 400 SND
105	CSNET-NS	CSNET posta-kutusu sunucusu
109	POP2	Posta ofisi protokolü 2
111	RPC	SUN RPC portmap
137	NETBIOS-NS	NETBIOS isim servisi
138	NETBIOS-DG	NETBIOS datagram servisi
139	NETBIOS-SS	NETBIOS oturum servisi

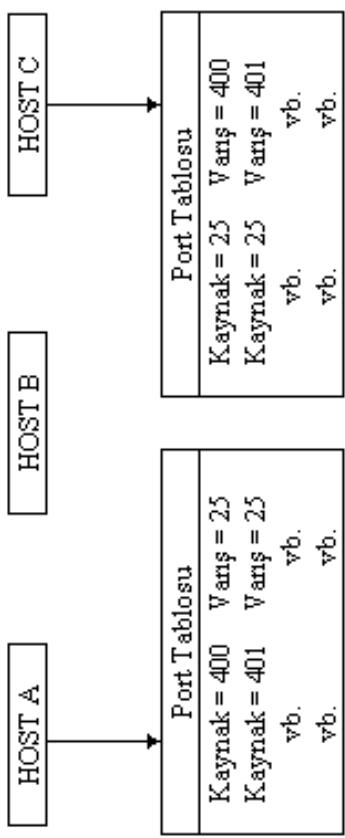
Port atama (Multiplexing-Çoklama)

- Aşağıdaki şenlik'te, Birinci olayda, A host'u, C host'una bir TCP segmenti gönderir. Bu segment bir yüksek-seviye prosesi ile haberleşmek için bir TCP bağlantısı istegidir. Burada SMTP'ye atanmış port 25 istenmemektedir. Varış port değeri 25 olarak sabitlenmiştir. Ancak, kaynak port tanımlayıcısı bölgесel bir sorundur. Bir host cihazı iç işlemleri için herhangi bir uygun numara seçebilir.
- İkinci bağlantı ise, (Şenlikde 2 rakamı ile gösterildi) SMTP'yi kullanmak üzere C host'una yapılmıştır. Neticede, varış portu 25 aynıdır. Kaynak port tanımlayıcısı farklıdır; bu durumda 401'e set edilmiştir. SMTP erişimi için iki farklı numaraların kullanılması A host'u ve C host'undaki iki oturum arasında bir karışıklık olmasını engeller.



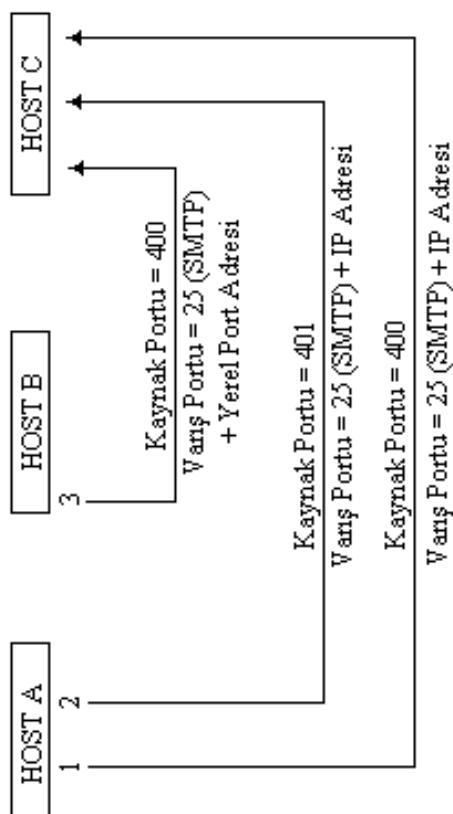
Port atama-2

- Şekil de, bir önceki iki segmentin nasıl bağlantı kurduğu gösterilmektedir. A ve C host'ları tipik olarak TCP bağlantıları ile ilgili bilgileri port tablolardında saklarlar.
- Dikkat edilirse bu tabloların kaynak ve varış değerleri arasında ters bir ilişki vardır. A host'unun port tablosunda, kaynaklar 400 ve 401, ve iki varış da 25`dir. C host`unda ise iki kaynak da 25, ve varışlar 400 ve 401`dir. Bu suretle, TCP modülleri ileri ve geri haberleşebilmek için kaynak ve varış port numaralarını terslerler.



Port atama -3

- Başka bir host`un C host`una aynı kaynak ve varış port değerleri ile bir bağlantı isteği göndermesi olasıdır. Varış port değerlerinin aynı olması olağanlığı değildir. Çünkü iyi-bilinen portlara sıkılıkla ulaşım isteği vardır. Bu durumda, varış portu 25 SMTP`yi tanımlayacaktır. Kaynak port tanımlayıcıları bölgeler bir olay olduğundan Şekil`de gördüğümüz gibi B host`uda kaynak portunu 400 olarak seçmiştir.
- **Ek bir tanımlayıcı olmaksızın, A ve C host`ları arasındaki ve B ve C host`ları arasında bağlantıda çakışma olacaktır** çünkü her iki bağlantı da aynı varış ve kaynak port numaralarını kullanmaktadır. Bu gibi durumlarda, C host`u datagramların IP başlıklarındaki IP adreslerini kullanarak ayırmayı kolayca başarır. Bu durumda kaynak portları ikilenir ancak internet adresleri oturumları farklılaştırır.



TCP Protokolu Mesaj Yapısı

Kaynak ve hedef portlar, servis noktalarının sağlanması içindir. İlk 1023 port no'su IANA tarafından kullanılan standart port nolarıdır. Uygulamalar diğer port nolarını diledikleri gibi seçerler.

Sıra (dizi) no ve onay (Ack-Bilgi) no kısımları bağlantı güvenliği için kullanılan parça sıra no ve alıcı tarafından bekendiği bildirilen (alıcı tarafında) parça no kümşüslərdir.

Bayrak alanı

ACK =1 bilgi numarasının geçerli olduğunu belirtir.

SYN =1 Bu durum TCP bağlantısının kurulacağını belirtir.

FIN =1 Bağlantının sonlanacağını bildirir.

RST = 1 bağlantının fazla hatalı olduğu, sonlandırılacağı anlamındadır.

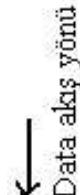
PSH =1 TCP modülü aldığı veriyi acilen üst katmanına gönderir.

URG =1 alıcıya, aldığıdataları işlemeden band dışı veri gönderilmesine izin verir.

0	16	31	TCP bağlantıları, "Üç adımda uzlaşma" Three Way handshaking yöntemiyle kurulur.
Kaynak Portu	Varış Portu	Sıra numarası	SYN=1 ve ACK=0 bağlantı açma isteği
Onay (Acknowledgment)			SYN=1 ve SYN=1 bağlantı açma onayı
Data Offset Reserve	Urgent Pointer	Window	SYN=0 ve ACK=1 Veri Paketi veya ACK paketi
Kontrol Toplamı	Açılı işareteti (Urgent Pointer)	Dolgu alanı	
Tercih Alanı			
Bilgi diğer 500 octet			

Pencere (Window) Alanı:

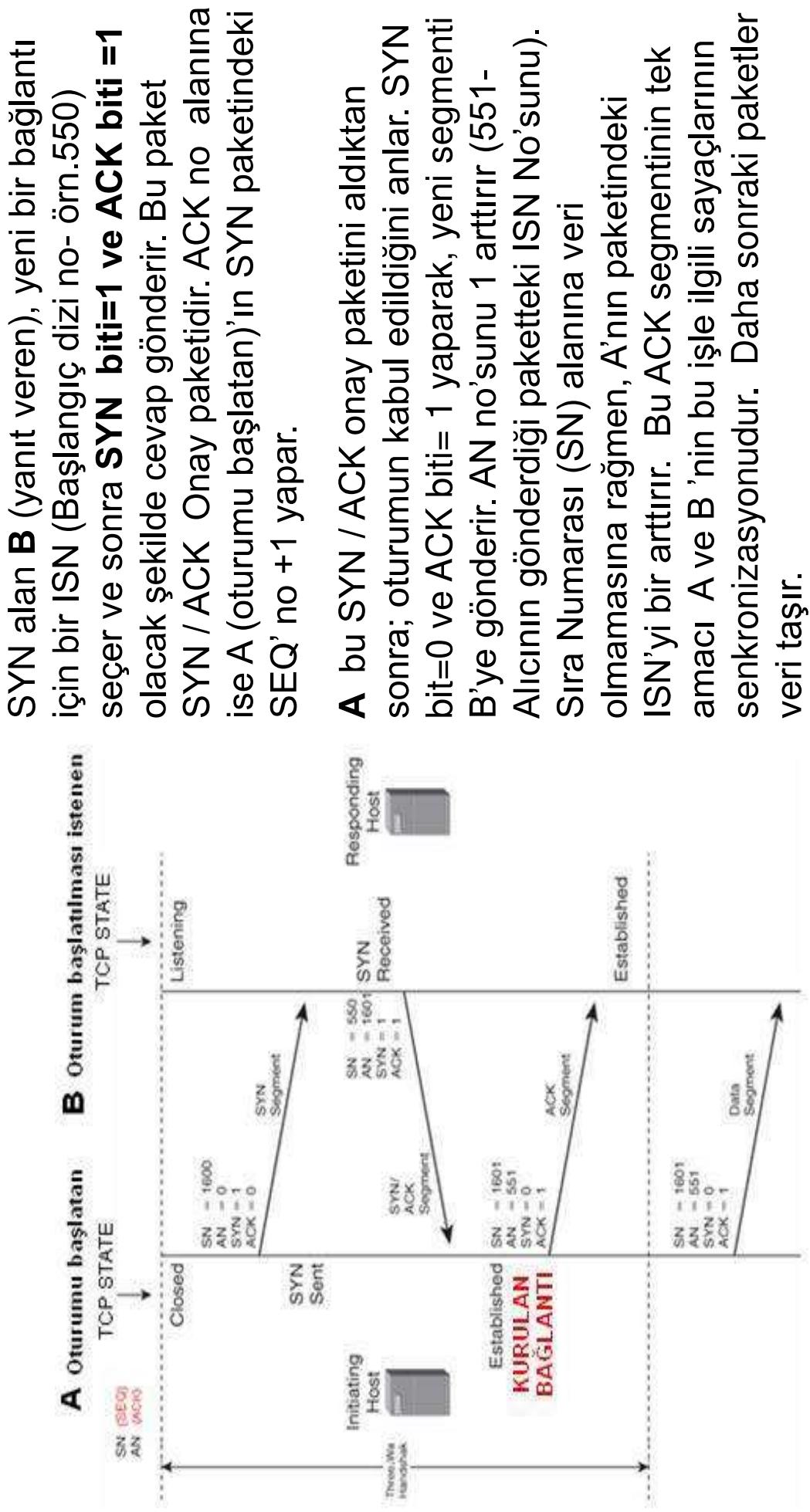
- Bu alan alıcı tarafından kullanılır ve *veri akışını kontrol* eder. Bu alan gönderilmesi gereken oktet miktarını belirler. Pencere alanı kullanılarak alınan paketler için tekbir bilgi paketi gönderilmesi sağlanır. Bu durum veri akışını hızlandırır.
- Alıcı gelen verileri aldıktan sonra, karşı tarafa bilgi paketi ile beraber, kabul edebileceği büyüğülükteki dizi numarasının da gönderilir. Kabul edilebilir dizi numarası aralığına pencere denir. Pencere, alıcı tarafının onayı ile, göndericinin iletebileceği oktet sayısını belirler.
- Böylece, gönderici verilerin alındığına dair bilgi mesajı almadan belirtilen miktarda veri transferi yapabilir. Bu da protokolün veri iletim hızını arttırmır.



D1-D2-D3-D4-D5-D6-	D7-D8-D9-D10-D11-	D12-D13-D14-	D15-D16-D17-D18
Gönderilen ve cevabı alınan veriler	Gönderilmek üzere sıralanmış veriler	Gönderilmek üzere sıralanmış veriler	Pencere içerişine dahil olduktan sonra gönderilecek veriler

TCP protokolündə bağlantı açma (Three way handshake)

TCP bağlantı başlatma yordamı iletişim noktaları arasında üç paket iletim gerektirdiğinden genellikle üç-yolu el sıkışma denir. Başlatan bilgisayar (**A**), yeni bağlantı için bir rastgele başlangıç sıra numarası (ISN –İnital service-sıra no) seçer ve daha sonra SYN biti=1 ve ACK biti =0 olarak ayarlanmış ilk paket gönderir. Bu pakete SYN denir



Bağlantının koparılması

- Gönderilen herbir veri parçasının (segmentin) ağ üzerinde kalabileceği bir belirli yaşam süresi vardır. Buna MSL (maximum Segment Life) denir.
- TCP segmentleri alıcısına iletildiği zaman , datagramları gönderen bilgisayar pencere alanını ilerletebilmek için , karşı tarafın bilgi paketi (ACK) göndermesini bekler. Bu bekleme süresine “zaman aşımı” (time –out interval)denir.
- TCP bağlantısının sonlanması isteği için FIN bayrağı =1 olan bir segmentler oluşturulup gönderilir.
- Bağlantının koparılması için her ,ki uç noktanın da FIN bayrağını kullanması gereklidir.
- Her iki ucun birlikte karar vererk bağlantının kesilmesi işlemine; zarif kapanış (graceful close) denir.
- Eğer taraflardan birisi diğerine haber vermeden bağlantıyı sonlandırırsa veri kaybı olabilir.

Kısa Özeti

Hizmet veren bir TCP portu açıksa kendisine gelen SYN paketine karşılık olarak ACK+SYN paketi döner. Dönен paketlerden ACK (onay paketi), SYN ise hizmet veren tarafın istek başlatma paketidir.

Port kapalıysa RST döner, SYNflood saldırısının başarılı olabilmesi için portun açık ve dinlemede (LISTEN mod) olması gereklidir.

UDP (User Datagram Protocol)

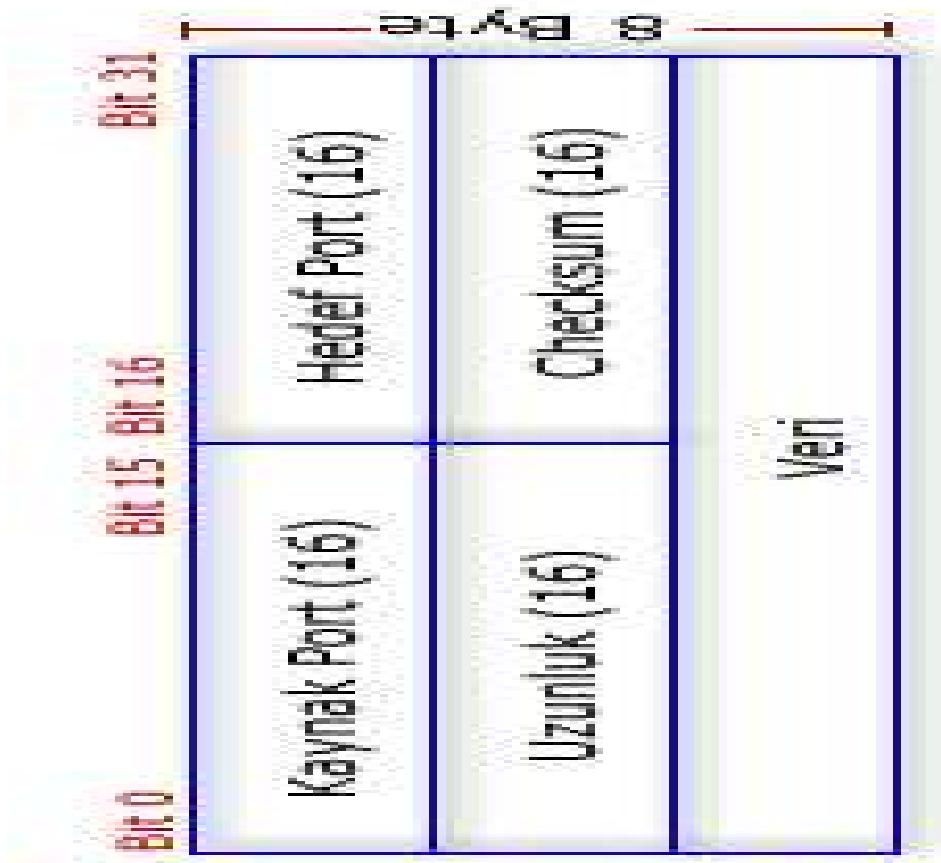
Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde bir datagram modu oluşturabilmek için UDP protokoli yazılmıştır. Bu protokol minimum protokol mekanizmasıyla bir uygulama programından diğerine mesaj göndermek için bir prosedür içerir.

UDP güvenilir olmayan bir aktarım protokolüdür. UDP protokolü ağ üzerinden paketi gönderir ve gidip gitmediğini takip etmez ve paketin yerine ulaşıp ulaşmayacağına onay verme yetkisi yoktur.

- Geniş alan ağlarında (WAN) ses ve görüntü aktarımı gibi gerçek zamanlı veri aktarımlarında UDP kullanılır.
- UDP bağlantı kurulum işlemlerini,akis kontrolü ve tekrar iletim işlemlerini yapmayaarak veri iletim süresini en aza indirir.
- UDP ve TCP aynı iletişim yolunu kullanıklarında UDP ile yapılan geçek zamanlı veri transferinin servis kalitesi TCP'nin oluşturduğu yüksek veri trafiği nedeniyle azalır.

UDP paket formatı

- **kaynak port:** Opsiyonel bir alandır. Gonderilen işlemin portunu gösterir. Eğer gönderen host bir kaynak numarasına sahip değilse bu alan “0” ile doludur
- **hedef port:** Hedef host içerisinde, işlemlere uygun ayrımları yapmak için kullanılır. Hedef port internet adresleri parçalarının genel durumunu içerir.
- **Uzunluk:** UDP veri ve UDP başlığının bayt cinsinden toplam uzunluğudur. minimum 8 bayttır
- **Checksum:** IP ve UDP başlığı ve verinin bilgisini içeren yalancı başlığın toplamı olan birbirinin tamamlayıcısı 16 bitten oluşur. Opsiyonel bir alandır. Hata kontrol mekanizması sağlar. Eğer hata kontrolü yapılmayacaksızı bu alan “0” ile doludur.
- **Veri:** Opsiyonel



UDP ile TCP 'nin farkları

Servis	TCP	UDP
Bağlantı kurulumu	Zaman alır ancak TCP bunu güvenli şekilde yapar.	Bağlantıya gerek yoktur.
Teslim garantisı	Gönderildiğini onaylar.	UDP onay mesajı göndermeden, alıcı paketin alındığına dair sinyal göndermez. Kaybolan paketler tekrar iletilmez.
Paket ardisıklığı (paketterin doğru sırası hakkında bilgi)	Ardışık numaralandırmış paketter	UDP ardisıklık numarası vermez. Paketterin sürekli ulaştığı veya kaybolduğu düşümlür.
Akış kontrolü	Alicı göndericiye yavaşlaması için sinyal gönderebilir.	Paket akış kontrolü için TCP' de kullanılan onay UDP' de geri dönmez.
Tıkanıklık kontrolü	Network cihazları TCP onayları sayesinde göndericilerin tavrını kontrol edebilir.	Onay olmadan network tıkanıklık sinyali gönderemez.

TCP protokolüne yönelik saldırılar

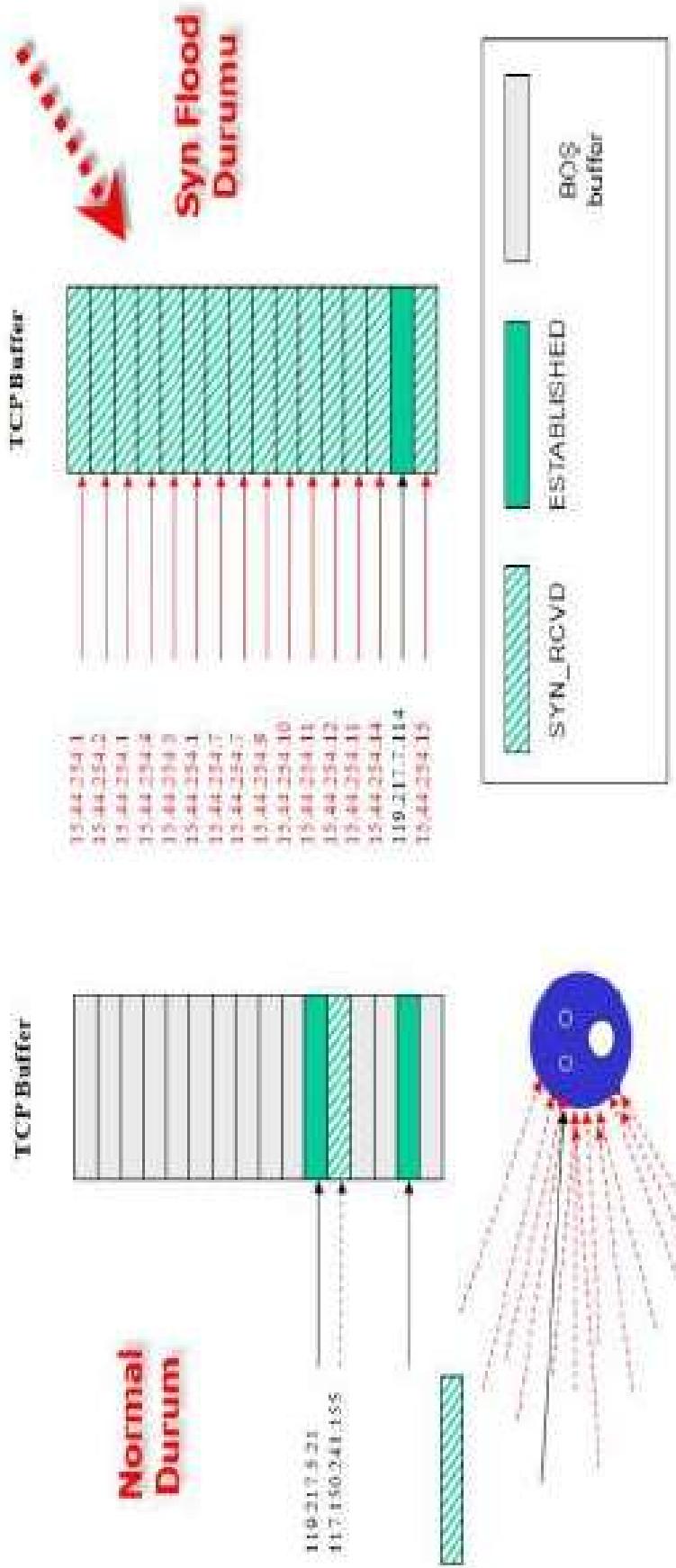
- TCP protokolünün tasarım özelliklerinden dolayı iki önemli zayıf noktası vardır.
 - Protokol, TCP bağlantısı kurma isteği “**SYN Bombardımanı-SYN Flooding**” sırasında zayıf kalır : SYN flooding genellikle serverlara yapılan bir saldırısı türüdür. Amacı çok sayıda “Bağlantı istek Paketi” hazırlayıp sunucuya göndererek hizmetleri aksatmaktır .
 - Protokol “**TCP oturumu ele geçirme**” saldırıları karşısında zayıf kalır. “TCP oturumunu ele geçirme”; iki bilgisayar arasında üç adımda sağlanan TCP bağlantısının birtakım yöntemlerle ele geçirilmesi veya veri akışına ; bağlantı içerisinde yer almaması gereken verileri eklemektir.

SYN FLOOD atakları

- SYN Flooding (SYN Bombardımanı) sunucunun başedemiyeceği kadar fazla “bağlantı kurma isteği” paketlerinin ağ üzerine bırakılması ile gerçekleştilir.
- Saldırganlar, sunucuya sadece **1. syn paketini** gondererek gelen **2. pakete** karsılık **3. syn onay mesajını** gondermeden araliksiz olarak **1. syn paketi (oturum açma isteği)** gonderebilir.
- Sunucunun kapasitesinde acilabilecek oturum sayısı rakamlarla ifade edilmiş ise kısa süre içerisinde bu syn paketleri ile oturum açma istekleri tamamen rezerve hale getirilir.
- Sunucu **3. syn paketini** almadığı sürece belirtilen zaman kadar bekleyerek oturum işlemini rezerve eder ve belirtilen sure dolmadan bu oturum isteğini kapatamaz.
- Yuzlerce hatta binlerce oturum açma isteği karsısında sunucu kısa süre sonra yanıt veremez hale gelir ve artık islevini yerine getiremez.
- Bu saldırısı türü, sunucunun mümkün olduğu kadar pasif çalışmasını hatta bağlantılı isteklerine hiçbir şekilde cevap vermemesini amaçlar.
- Bu bir DOS saldırısıdır.

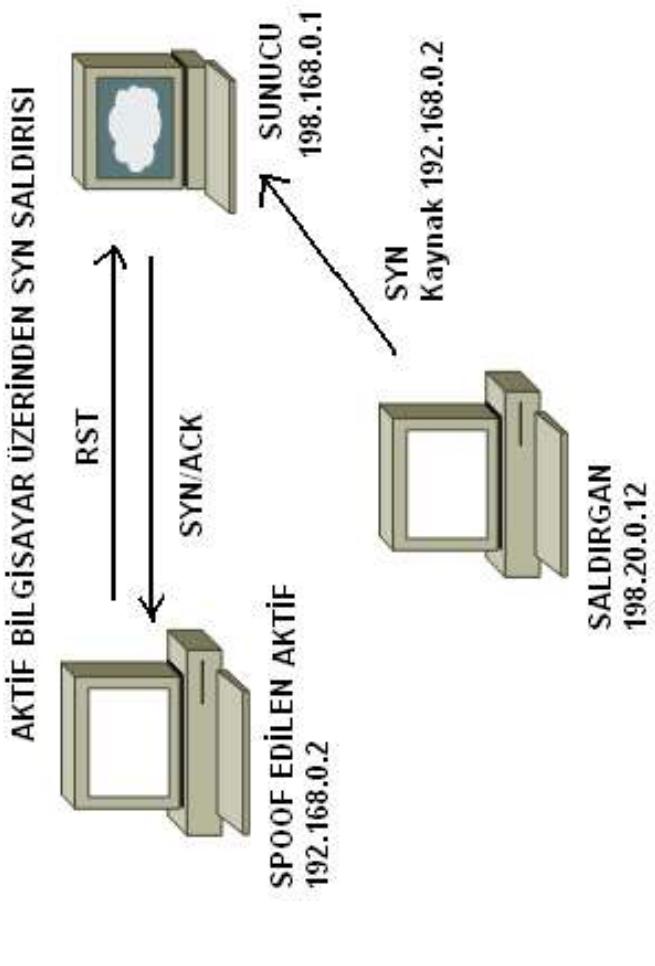
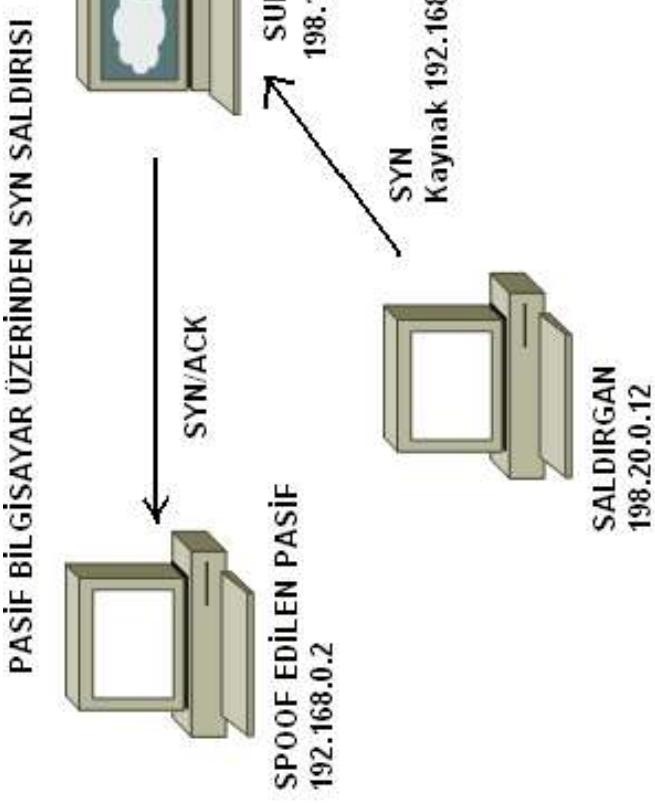
Syn Flood saldırısı, açık bir porta (dinlemeye olan port), sistemin kapasitesinden fazla gönderilecek SYN paketleriyle gerçekleştirilir. Bu kapasiteye **Backlog Queue** denilmektedir. İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar bellekten bir alan kullanırlar, bu alan **TCB (Transmission Control Block)** olarak adlandırılır. Bu alanların toplamı **Backlog queue (Bırıkım kuyruğu)** olarak adlandırılır. Başka bir ifadeyle işletim sisteminin half-open olarak ne kadar bağlantı tutabileceğini backlog queue veriyapısı belirler. Bu değer her işletim sisteminde vardır ve ön tanımlı olarak düşük bir değerdir(256 gibi).

Synflood saldırısında tüm mesele backlog queue'nın dolması ve yeni gelen bağlantıların reddedilmesidir. Backlog queue değerinin büyük olması demek daha fazla half-open(SYN paketi) bağlantı kabul edebilmek demektir. SYNFlood saldırılarda backlog değeri artırılarak saldırıya karşı ek önlem alınabilir. Backlog queue dolmasıyla birlikte işletim sistemi yeni bağlantı kabul edemez ve bu esnada sunucuya bağlanmaya çalışanlar bağlanamazlar ki bu da SYN Flood saldırısına denk gelir.



- SYN flood saldırısı için spoof edilmiş (taklit edilmiş) IP datagramlar kullanılır. Yani bağlantı kurma istek segmentini taşıyan paketlerin gönderici IP'sine spoof edilmiş veya yapay olarak yaratılmış adresler atanır.
- Taklit edilmiş paketler ile pasif bilgisayar saldırısı için, seçilen IP adresine, IP datagramlarının yönlendirilebilir olması fakat , bilgisayarın erişilebilir olmaması gereklidir (Sunucu Onay segmentini gönderip oturumun senkronizasyonunu sağlayan üçüncü paketi bekleyecektir.)

- Taklit edilmiş paketler için aktif bilgisayar saldırısında; Sunucunun gönderdiği SYN/ACK paketlerine, aktif bilgisayar, RST =1 olan datagramlar gönderir. Bu paketi alan sunucu bağlantı isteğini sonlandırır. Hafızadaki temizler.



Synflood Önleme Yöntem ve Çeşitleri

SynFlood saldırılara karşı çeşitli önlemler geliştirilmiştir. Bunlar arasında önemlileri;

- Syncookie
- Syncache(FreeBSD default)
- SynProxy
- TCP Authentication

SynCookie

Normal TCP bağlantılarında gelen SYN bayraklı pakete karşılık ACK paketi ve SYN paketi gönderilir. Gönderilen ikinci (sunucunun gönderdiği) SYN paketinde ISN (Sıra no) değeri random olarak atanır ve son gelecek ACK paketindeki sıra numarasının bizim gönderdiğimizden bir fazla olması beklenir, son paket gelene kadar da sistemden bu bağlantı için bir kaynak ayrırlar (backlog queue). Eğer bizim gönderdiğimiz SYN paketine dönen ACK cevabı bizim ISN+1 değilse paket kabul edilmez.

Syncookie aktif edilmiş bir sistemde gelen SYN paketi için sistemden bir kaynak ayrılmaz, bunun aksine SYN paketine dönecek cevaptaki ISN numarası Özel olarak hesaplanır (kaynak.ip + kaynak.port + hedef.ip + hedef.port + x değeri) ve hedefe gönderilir, hedef son paket olan ACK'i gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı kurulur, değilse bağlantı kurulmaz.

Böylece spoof edilmiş binlerce ip adresinden gelen SYN paketleri için sistemde bellek tüketilmemiş olacaktır ki bu da sistemin SYNflood saldırıları esnasında daha dayanıklı olmasını sağlar.