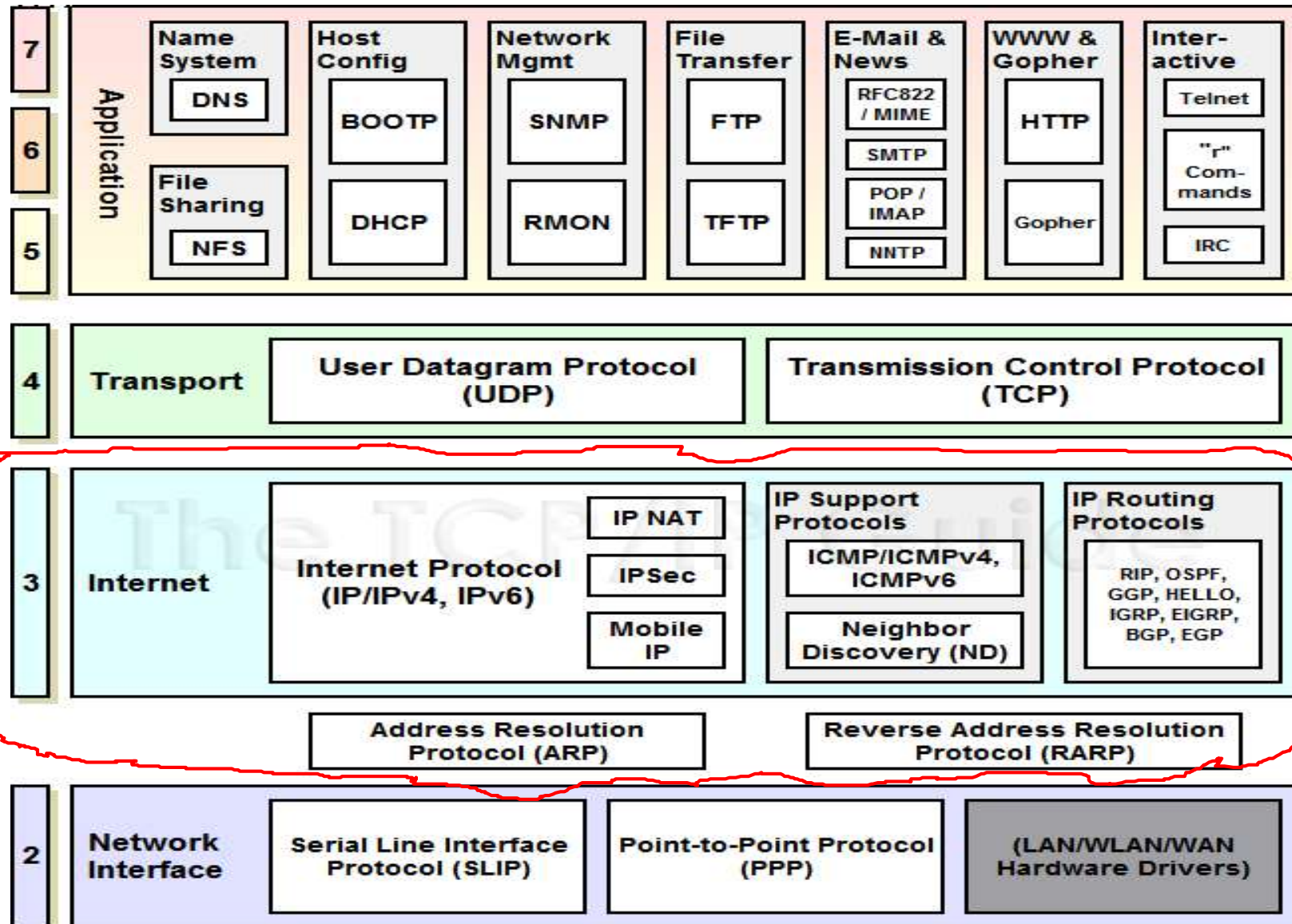
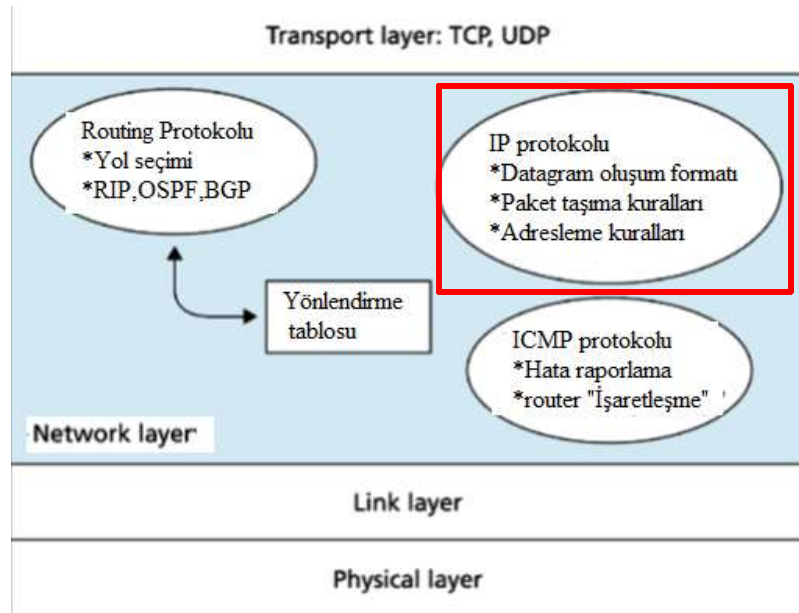


# Network Katmanı (3.Katman)

## Atakları - Güvenliği -2

# TCP/IP protokol kümesi





### IP protokolu Saldırıları

\* **IP spoofing:** Paketin kaynak adres kısmının olması gerekenden farklı bir IP adresi ile değiştirilmesidir.

1-ARP spoofing (Paketin kaynak adres kısmındaki sahte IP )

2-Source Routing (Kaynak Rotalama, kaynak adres kısmı sahte IP)

\* **IP Fragmentasyon Atağı:**

\* **Trafik arttırma atağı:** IP broadcast hedef'e müsaade eder. DOS..

### IP Protokolu zayıflıkları

**1.Gizlilik:** Bir paketin bir noktadan çıkıp karşı noktaya iletiildiği yol boyunca gizlenmemesi sebebi ile paketin içeriği yol boyunca, izlenebilir ve okunabilir.

**2.Paket doğrulama yoktur:** Bir paketin kaynak adresi değiştirilmiş olabilir. Ipv4 paketinde bunun doğru bir kaynak adresi olup olmadığının doğrulaması yoktur. Genelde Spoof (Hırsızlık) ismi verilen saldırıların temeli bu zayıflıktır.

**3.İçerik bütünlüğü korunmaz:** Paketin başlığının ve içeriğinin yolda değiştirilmediğini garanti eden bir tedbir yoktur.

**4.Paketlerin parçalanması ve birleştirilmesi süreci:** Bu süreçte bir doğrulama ve kontrol mekanizması yoktur

# IP Spoofing (Yanıltma-Aldatma)


- Internet veya ağa bağlı sisteminizle başka bir sisteme bağlanacaksınız, fakat bu bağlantının sizin tarafınızdan yapıldığını gizlemek istiyorsunuz. Bunun için bağlantı sırasında kimliğinizi (ki TCP/IP protokollerinde kimliğiniz IP adresinizdir), yanlış gösteriyorsunuz. Bu IP spoofing işlemidir.
- Bu saldırıyla, saldırgan, kendi IP paketlerinin sahtekarlığını yaparak (nemesis v.b gibi programlar ile) diğer paketlerin arasındaki kendi paketinin kaynak IP alanını değiştirir.
- Saldırgan, paketin kaynak adresi olarak dahili veya güvenilir bir IP adresi koyar. Böylelikle Erişim kontrol cihazının, IP adresini güvenilir olarak görmesini ve paketi geçirmesini sağlayabilir..
- Kaynak değiştirildiğinden, sahte pakete karşılık gelen cevaplar saldırganın makinesine gidemez. Spoof edilen makinaya gider.
- Saldırganın bu cevabı kendi makinasına alabilmesi için kullandığı önemli teknik "Kaynak yönlendirme-Source routing" dir.

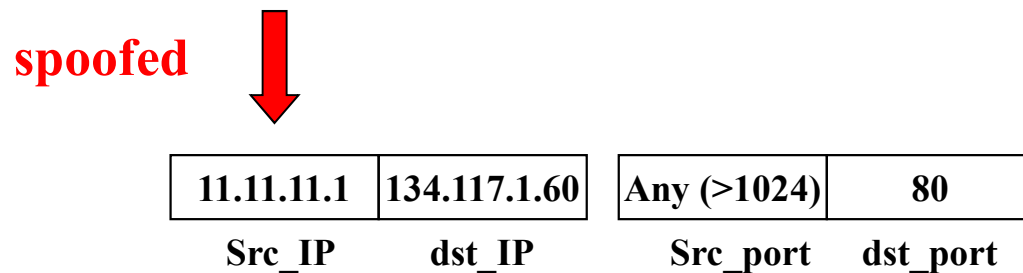
- IP spoofing (sahtekarlığı) için iki genel teknik kullanılır:
  - \* Güvenilir IP adresleri aralığında olan bir IP adresi kullanır.
  - \* Güvenilen yetkili bir dış IP adresi kullanır.

IP spoofing kolay başarılabacak bir saldırıdır. Çünkü;

- \*Yönlendiriciler yalnızca Hedef adreslerine bakar.
- \* Yalnızca Kaynak adreslerine göre kimlik doğrulama.
- \*IP başlık alanındaki kaynak adres alanını değiştirmek kolaydır.

  
 10.10.10.1  
 http://www.carleton.ca

  
 134.117.1.60



# Spooftng Atakları

**1- Yerel spoofing (Non blind spoofing):** Saldırgan ve mağdur (victim-kurban) aynı alt ağdadır.

Saldırgan, bir saldırı başlatmak için gerekli temel bilgi parçalarını bulmak amacıyla trafik koklama (sniffing - izleyici) ile işe başlar. Alt ağdaki bir normal kullanıcının gönderilerine müdahale etmek için kullanılır. Bu tür bir sahtekarlık tehdidi oturumun ele geçirilmesi ve bir saldırı bağlantısını kurmak için tüm kimlik doğrulama önlemlerini atlayabilir. Bu, kurulan bir bağlantının DataStream'ini bozarak, ardından doğru sıraya ve saldırı numaralarıyla onay numaralarına dayanarak yeniden kurarak gerçekleştirilir, normal bir TCP oturumunu resetleyebilir.

**2- Blind spoofing:** Saldırgan ile mağdur aynı altag'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.

**3- Man in the Middle:** Ortadaki adam saldırısı. Buna bağlantı hırsızlığı da denir. Bu saldırılarda, kötü niyetli bir taraf, iletişim akışını kontrol etmek ve asıl katılımcılardan birinin gönderdiği bilgileri bilgisi olmadan elemek veya değiştirmek için iki ev sahibi arasında meşru bir iletişim kurar.

**4. DOS Saldırısı:** Saldırıyı gerçekleştiren saldırganlar, DoS'un izlenmesini ve durdurulmasını mümkün olduğunca zorlaştırmak için kaynak IP adreslerini taklit eder. Birden fazla tehlike altındaki ana bilgisayar saldırıya katılırken, tüm gönderilen sahtekarlık trafiği, trafiği hızla engellemek için çok zordur.

IP sahtekarlığı ayrıca, IP adreslerine dayalı kimlik doğrulama gibi ağ güvenlik önlemlerini yenmek için kullanılan bir saldırı yöntemi olabilir. Bu tür bir saldırı, makineler arasında güven ilişkilerinin olduğu yerlerde en etkilidir. Örneğin, bazı şirket ağlarında,, iç ağdaki başka bir makineden bağlanması şartıyla kullanıcı adı veya şifre olmadan giriş yapılabilir (ve çoktan oturum açmış olması gerekir). . Bir saldırgan, güvenilir bir makineden yapılan bir sahtekarlığa sahte olarak, hedef makineye kimlik doğrulaması yapmadan erişebilir.

# IP spoofing'in anlaşılması ve önleme

Paketleri wireshark v.b gibi ağ izleme yazılımı kullanarak izlerseniz;

- hem kaynak hem de hedef IP adresinin lokal IP olduğu bir dış ağdan gelen paket, IP sahtekarlığının bir göstergesidir.
- Kullanılan bilgisayardaki trafik loglarının incelenmesiyle d tespit mümkün.
- IP sahtekarlığı sorununu önlemenin en iyi yöntemi, dış ağdan (giriş filtresi olarak da bilinir) gelen paketlerin, iç ağınızdaki bir kaynak adrese sahipse filitrelenmesidir (Router veya Gateway tarafından). Aynı şekilde; iç ağdankaynaklanan bir kaynak IP sahtekarlığı saldırısını önlemek için iç ağınızdan farklı bir kaynak adresine sahip giden paketleri filtrelemelisiniz. Dikkat!!! Bu işlemlerin yapılabileceği bir router veya firewall'a sahip olmalısınız.
- Ağınızda IP sahtekarlığının ortaya çıkmasını önlemek için, bazı yaygın uygulamalar şunlardır:
  - 1- Kaynak adres onayını kullanmaktan kaçının. Sistem genelinde kriptografik kimlik doğrulama uygulayın.
  - 2- Ağınızı, yerel bir adresten kaynaklandığı iddia edilen ağdan gelen paketleri reddetmek üzere yapılandırın.
  - 3- Kenar yönlendiricilere giriş ve çıkış filtreleme uygulamak ve i özel IP adreslerini engelleyen bir ACL (erişim kontrol listesi) uygulayın. Güvenilir ana bilgisayarlardan dış bağlantılara izin veriyorsanız, yönlendiricideki şifreleme oturumlarını etkinleştirin.

# Paketlerin Parçalanması (IP fragmentation)

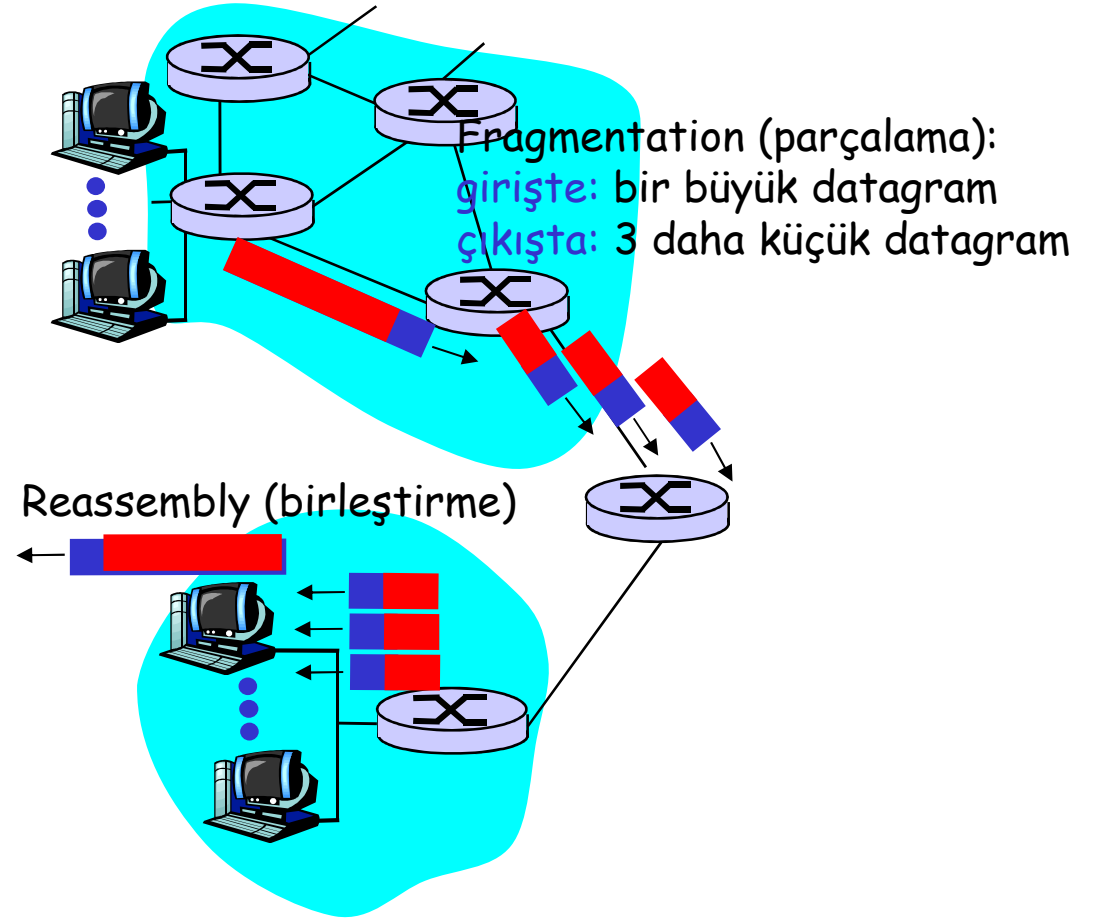
- Veri bağı katmanı kullanılarak gönderilebilecek en büyük datagramın boyutuna **MTU ( Maximum Transmission Unit)** denir. Değişik ağ teknolojilerindeki MTU'lar farklıdır.
- Paketlerin MTU'yu geçmeyecek şekilde ağlar arasında iletimin sağlamak için boyutlandırılması işlemine parçalama (fragmentation).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

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 MTUlar
- ❑ 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



# IP Datagram Parçalama/Birleştirme

## Örnek

- ❑ 4000 byte datagram
- ❑ MTU = 1500 bytes

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

Bir büyük datagram pek çok daha küçük datagrama dönüşür

Veri alanında 1480 bytes

offset  
(öteleme)=  
 $1480/8$

	length	ID	fragflag	offset
	=1480	=777	=1	=0

	length	ID	fragflag	offset
	=1480	=777	=1	=185

	length	ID	fragflag	offset
	=1020	=777	=0	=370

# IP Datagram Parçalama/Birleştirme

## Örnek

- ❑ 4000 byte datagram
- ❑ MTU = 1500 bytes

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

Büyük bir datagram birkaç küçük datagrama dönüşür

Veri alanında 1480 bytes

	length	ID	fragflag	offset	
	=1500	=777	=1	=0	

	length	ID	fragflag	offset	
	=1500	=777	=1	=1480	

	length	ID	fragflag	offset	
	=1040	=777	=0	=2960	

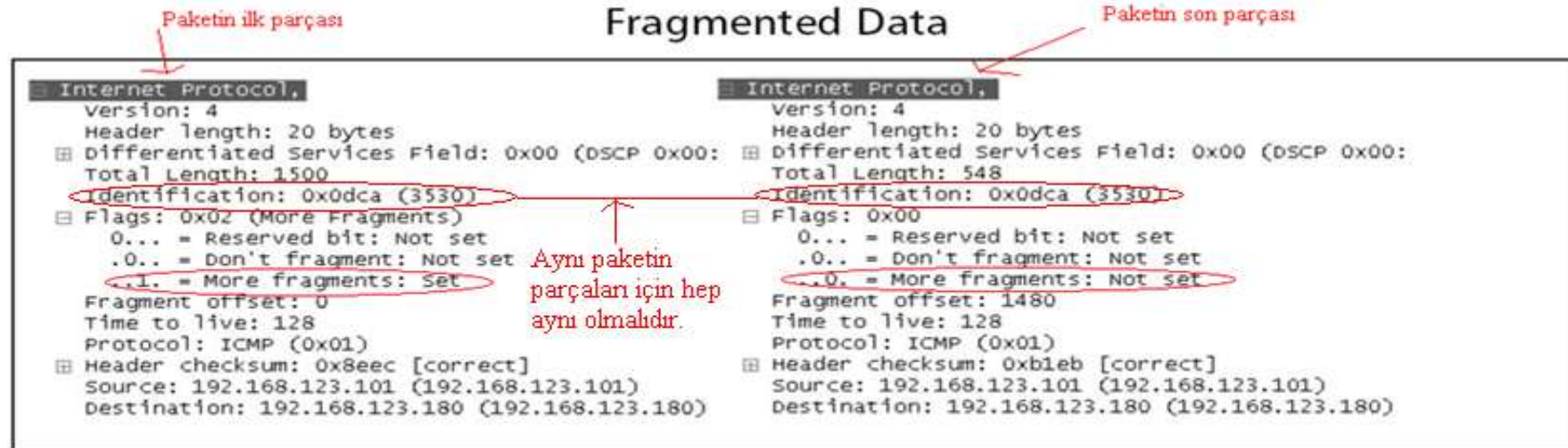
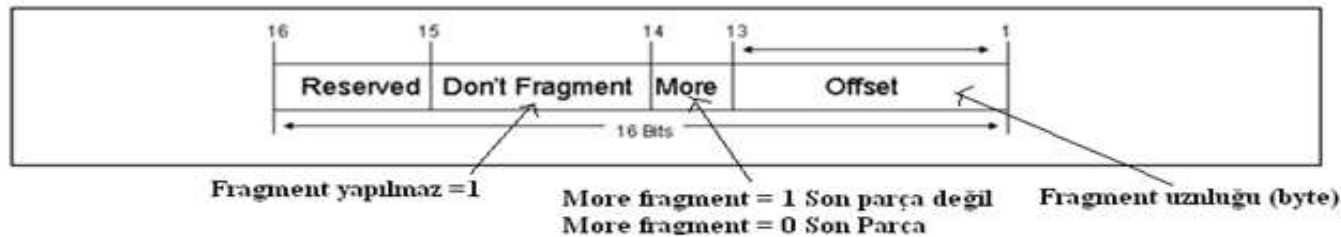
ICMP ?

Her IP paketi ?

# Parçalama (Fragmentation)

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

IP DATAGRAM Başlığındaki Fregmantla ilgili ( FLAG+FRAGmant Offset - 16 bit) kısım



- 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 bilmelidir. Ne kadarlık bir veri taşıdığı Total Length ile belirtilir.

```
⊕ Differentiated Services Field: 0x00 (DSCP 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 tasımadır, biz de buna ek 1500 byte yapıp göndereceğiz, bir sonraki pakette offset değeri 2960+1500 olacaktır(aslında 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 !!!!!

- Parçalanmış paketlerde sadece ilk paket protokol başlık bilgisini(TCP, UDP, ICMP vs) taşır.

- **Reassembly** ( Tekrar Birleştirilme İşlemleri): IP protokolü belirtimindeki bazı belirsizlikler nedeniyle, özel durumlarda farklı parçalama işlemleri meydana gelebilir ve bu parçaların yeniden birleştirilmesi gerekir. Bu özel parçalama işlemleri;
- ***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 hosttakiler farklılıklar gösterir ise; bu durum tutarsızlıklara yola açabilir.
- Dolayısıyla ***insertion*** ve ***evasion*** atakaları yapılabilir.

- **Bu birleştirme sürecindeki olabilecek ataklar;**
- **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 kullanılması, saldırgana 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 başlıkları ikiye üçe bölünmüş fragmentler olabilir.
- *Bu şekilde oluşmuş her bir bağımsız fragment, imzayla uyuşmaz dolayısıyla atak sayılmaz.*



# Fragmentation Atakları

- Parçalanmış paketlerin üst üste çakışması (Overlay), saldırganlara IDS, Firewall ve Routerlarda eski paketlerin kaydırılması imkanını sunar.
- Bir routerdan, 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 inceleme olmasıdır. Saldırı tespit sistemleri gelen bir paketin/paket grubunun saldırı içerikli olup olmadığını anlamak için çeşitli kontrollerden geçirir. Eğer bu kontrollere geçmeden önce paketleri birleştirmezse çok rahatlıkla kandırılabilir.
- Mesela HTTP trafiği içerisinde “/bin/bash” stringi arayan bir saldırı imzası 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 bölme araçlarından birini kullanarak /bin/sh stringini birden fazla paket olacak şekilde (1. Paket /bin, 2.paket /bash) gönderip IDS sistemini atlatabilir.

# Fragmentation Attacks (cont.)



Windows and router  
accepts #1 and #2

Attacker modifies #2  
And transmits #2 and #3



Windows keeps



Router keeps



Same size, same offset

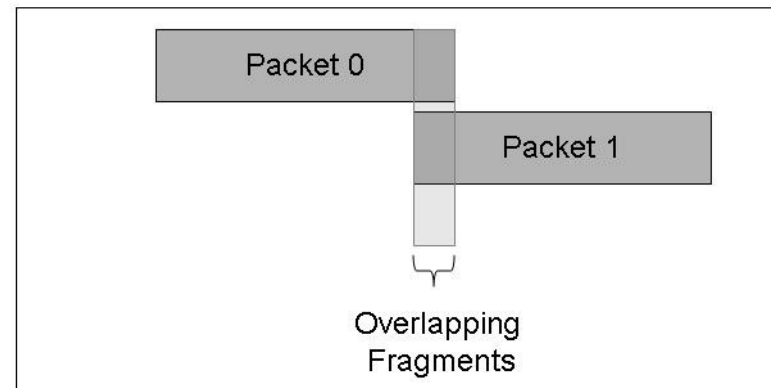
# Fragmentation Attacks (cont.)

- Saldırgan mesajını 3 parçaya 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 birleştirdiğinde bu mesajların saldırı olmadığına karar verir.

# 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 birleştirilmesindeki zayıflıktan yararlanır. Mesaj, ağlar arasında iletilirken genellikle daha küçük parçalar ayrılır. 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 gönderilerek sistem bozulur.

**Figure 4.14** The Teardrop Attack



# Parçalanmış Paket Oluşturma Araçları

- Paket parçalama işlemi normalde bizim (kullanıcılar) tarafımızdan yapılmaz. Ağlar arası geçişleri sağlayan yönlendirici sistemler (router) gerektiğinde bu işlemi gerçekleştirir.
- Fakat internette bulunan çeşitli araçlar kullanılarak kendi isteğimize göre paketleri parçalayıp gönderebiliriz.
- Bunları öğreniniz!!!!!!!!!!!!!!
- Dikkat !!!!Parçalanmış paket saldırılarına sebep olan güvenlik açıklıkları uzun zaman önce işletim sistemi geliştirici 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 suiteinde paket göndericisine, networkte paketi rotaya göre ilerletmek için imkan veren bir seçenektir.
- Saldırganlar bu özelliği , belirli bir alt ağı ele geçirmek için yapacakları saldırı için kullanabilirler.
- Şöyleki; saldırgan, gönderici adresini aldatarak, o paketi bir alt ağdan geliyormuş gibi set edebilirler.
- Bunu önlemenin yolu, router'ın kaynak adresi hedef makineye varmadan kimseye göstermemesidir.
- Bu işlem Cisco cihazlarda *“no ip source-route”* komutuyla yapılabilmektedir.

# 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.



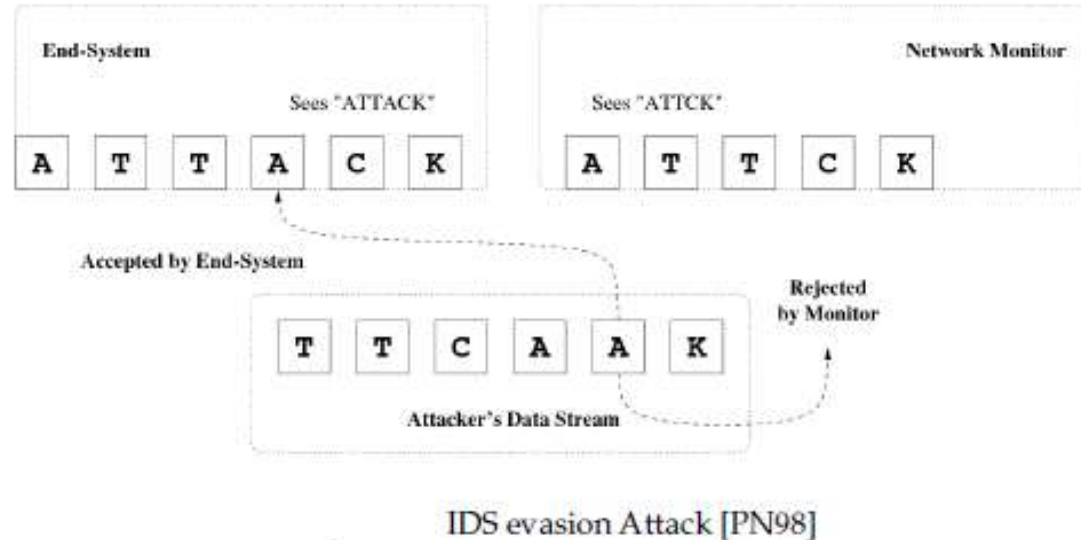
# IP Katmanı genel Atak Tipleri

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

## 1- Evasion attack (Atlatma Atakları):

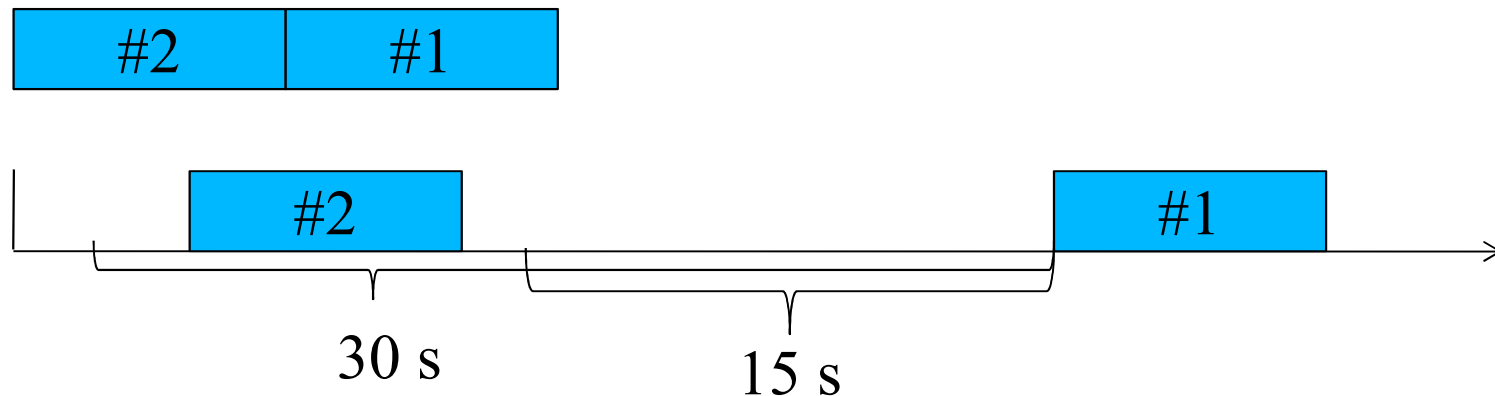
Bu ataklarda paketler hem IDS'ye hem de hedefe gönderilir. IDS bu paketleri reddeder (dikkat atak olduğu için değil..Kurala uymayabilir !!!!!) , hedef host kabul eder.

- IDS reddetiği, 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 göndermiş olur.



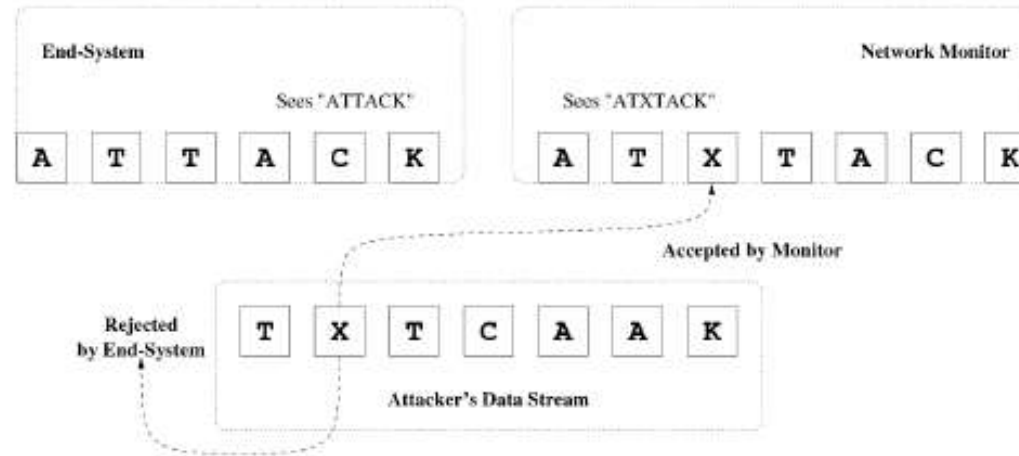
# Evasion Attack (Atlatma Atakları)

- 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 büyüktür. Fakat hedef sistem bu fragmenti kabul eder. Oysa bunun içinde bir atak olma ihtimali vardır.
- Böylece IDS atağı kayıt edemez. IDS atlatılmış olur.



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

- Bu ataklarda; hem son kullanıcıya hem IDS'ye gönderilen paketlerden, Son kullanıcının kabul etmediği, IDS tarafından kabul edilenler olabilir.
- Paket sadece IDS'de geçerlidir. Bu durumu uygun kullanabilen saldırgan; uygun bir paket trafiği ekleyerek imza analizi ile saldırı tespitindeki analizi önleyebilir (Son kullanıcı tarafından kabul edilmeyen paket ile, o paket grubunun saldırı olmadığı IDS'ye inandırılır.)



IDS insertion attack [PN98]

# Çok bilinen ataklardan bazıları

**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 saldırganlar, 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)** : Saldırgan 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; saldırgan bu 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 başındaki router TARAFINDAN (hedef bilgisayar bu Router'ın arkasındaki ağdadır) tarafından reddedilir.

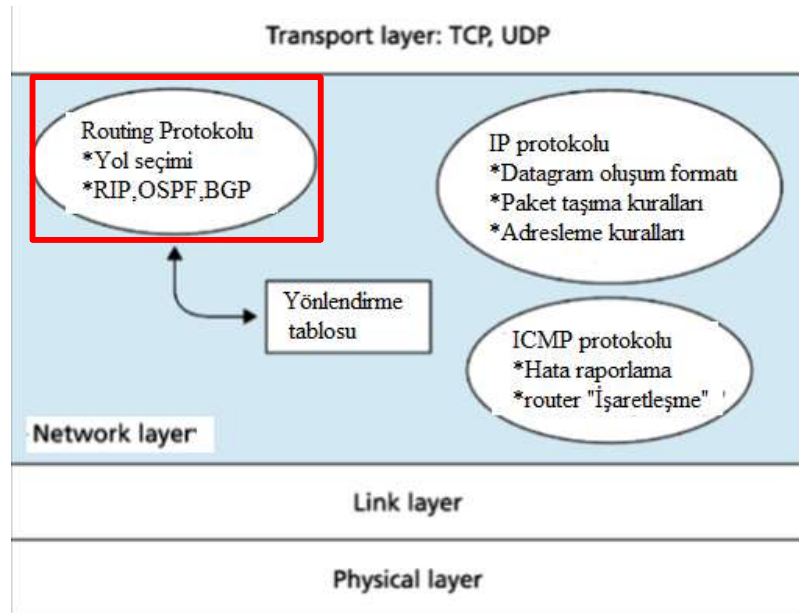
- Bu bir “**IDS insertion**” atağıdır. Böylece, IDS bu paket gurubu için imza analizi yapamaz.

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

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

# 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 etmektir. Yönlendirici bu kontrolleri ACL'ler (Access-Control List –Erişim Listesi) yardımı ile sağlar. ACL'ler kendisine gelen verinin kaynak, hedef ip adreslerine, bilginin 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 karşılaştırarak 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.



### ROUTING Protokolu Saldırıları

\* RIP spoofing ile rotadaki veya hosttaki rota tabloları değiştirilebilir. İstek mesajı ile rota tabloları kolaylıkla ele geçirilebilir.

### ROUTING Protokolu zayıflıkları

Routing protokolu seçenekleri RIP, IGRP, EIGRP, OSPF, BGP'dir. BGP, otonom ağlar içi ve ağlar arası iletişim için defacto yönlendirme standardıdır. RIP, IGP, OSPF, otonom ağlardaki iç yönlendirmede kullanılan protokollerdir.

- \* RIP Protokolu : UDP protokolunu kullanarak;
- \* BGP protokolu: TCP protokolunu kullanarak
- \* OSPF Protokolu: IP datagramlarını kullanarak yönlendirme bilgisi mesaj alış-verişini sağlarlar
  - \* RIP datagramları dahili sıra nosu içermez ve kimlik doğrulaması yoktur. Datagram gizliliği yoktur. UDP tabanlıdır (genellikle 520 portunu kullanır) ve durumsuzdur, yani, talep edilmemiş olsa da sahte cevap paketleri kabul edilir ve işlenir.
  - \* IP sahtekarlığı saldırısını kullanan herhangi bir saldırgan, yetkili bir BGP istemcisi olarak maskelenen yarı çift yönlü bir BGP oturumu üretebilir.
  - \* OSPF sadece kimlik doğrulama sağlar, gizlilik sağlamaz.

# IP Datagramların Yönlendirilmesi

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

# Statik ve dinamik yönlendirme tabloları

İki şekilde yönlendirme tablosu oluşturulur.

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

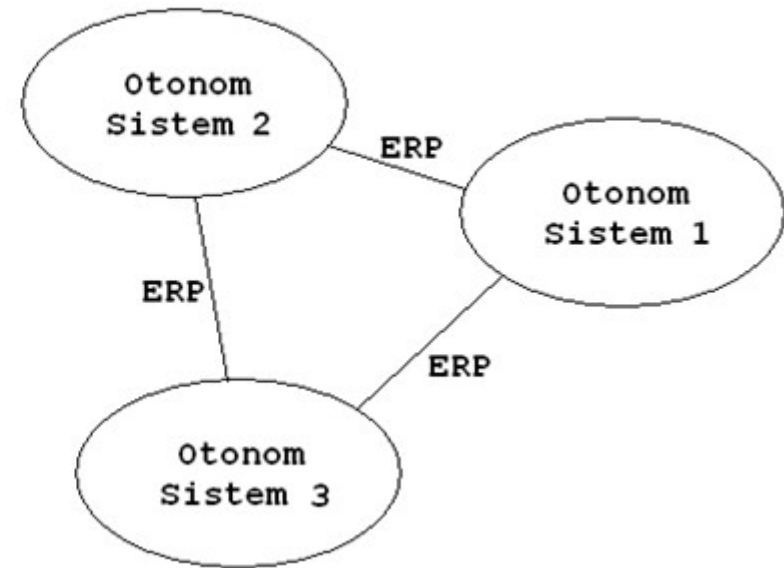
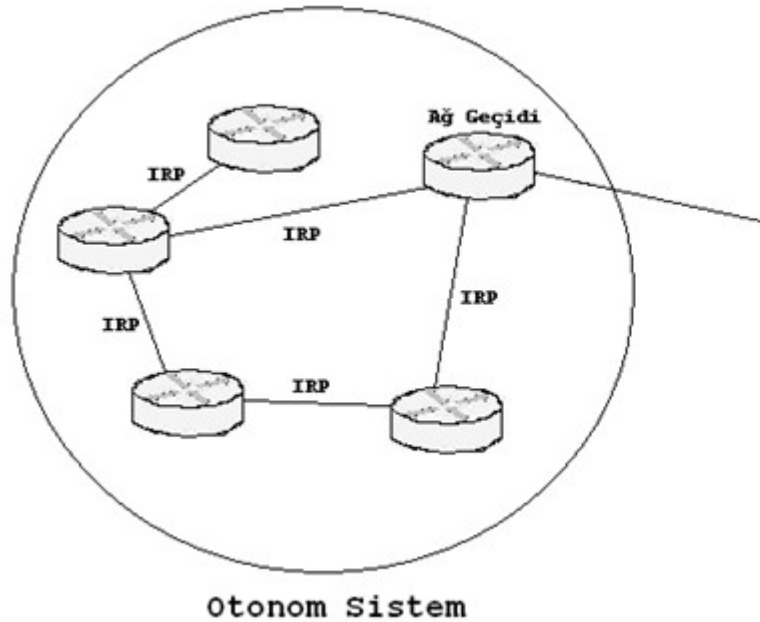
2- Statik yapılandırma : Hedef bilgisayar ağına bağlantı kurulabilmesi için tablo el ile doldurulur. Küçük ve yapısı değişmeyen ağlarda bu yöntem kullanılabilir.

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



# DATAGRAM Yönlendirme protokolları

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



# Yönlendirme Protokolleri

Protokollarından en çok bilinenleri

-RIP (*Routing Information Protocol - Yönlendirme Bilgi değişimi protokolu*) : Tablolarını güncellemek için Uzaklık Vektör (Distance Vector) Algoritması kullanır.

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

EGP Protokollarından en fazla bilineni;

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

- Yönlendiriciler arasında, yönlendirme bilgileri IP datagramlar aracılığı ile taşınır. Yönlendirme protokolları IP, TCP,UDP protokollarını kullanarak mesaj alış-verişini gerçekleştirir.
- **OSPF Protokolü** : IP datagramalarını kullanarak
- **RIP Protokolü** : UDP protokolunu kullanarak;
- **BGP protokolü**: 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 kullanır. RIP'ı kullanan Routerlar, 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**

0	8	16	32
<b>Komut</b>	<b>Versiyon</b>	<b>Sıfır Alanı</b>	
<b>Adres Belirteci</b>		<b>Sıfır Alanı</b>	
<b>IP adres</b>			
<b>Sıfır Alanı</b>			
<b>Sıfır Alanı</b>			
<b>Metrik</b>			
<b>Adres Belirteci</b>		<b>Sıfır Alanı</b>	
<b>IP adres</b>			
<b>Sıfır Alanı</b>			
<b>Sıfır Alanı</b>			
<b>Metrik</b>			
<b>Diğer yönlendirme Bilgileri</b>			

Komut Türü

Tanımı

- |               |  |
|---------------|--|
| 1 (RIP İstek) | Yönlendirme yablosu gödeilmesi isteği      |
| 2 (RIP Yanıt) | Yönlendirme tablo bilgilerinin gönderimi.  |
| 3             | Bu komutun alındığı mesj işleme konulmaz.  |
| 4             | Bu komutun alındığı mesaj işleme konulmaz. |
| 5(Ayrılmış)   | Sun Microsystem Tarafından kullanılır.     |

RIP Versiyon 1 Mesaj Yapısı

# OSPF Genel Mesaj Başlığı

0	8	16	32
Versiyon	Tür	Paket Uzunluğu	
Yönlendirici ID			
Alan ID			
Kontrol Toplamı		Güvenlik Türü	
Güvenlik Alanı			
Güvenlik Alanı			

Genel OSPF Mesaj Başlığı yapısı

## Tür

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

## Güvenlik Türü

- 0- Herhangibir şifreleme yok.
- 1- Basit şifreleme metodu geçerli : Güvenlik alanı ile 64 bitlik şifreleme kullanımına imkan vereri

**Versiyon:** OSPFprotokolunun versiyonu bildiriri. Günümüzde OSPF Version 2 kullanılır.

**Yönlendirici ID:**Mesajı gönderen Router'ın tanım alanıdır.

**Alan ID:** Aynı alana ait routerların malan ID'si aynıdır.

# Routing Protokollarına ataklar

- Distance-vector ve link-state routing protokolları özellikle DOS saldırılarına çok uğrarlar.
- **RIP bir doğrulanmaz servis hizmeti olduğundan DoS saldırılarına karşı korumasızdır.**
- Sahte RIP paketleri göndermek , ağ geçitleri ve hostların rotalarını değiştirmek ve onlardan bilgi sızdırmak için yapılır.
- 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 yollanan paketlerin bir kopyasının kendine de yollanmasını sağlayabilir (kredi kart numaraları gibi verileri almak için) veya protokolleri kaldırarak yönlendiricinin diğer yönlendiricilerle haberleşmesini kesebilir.
- Haberleşmenin yok olması, yönlendiricinin aldığı paketleri nereye göndereceğini bilmemesi ve servis dışı kalması(DoS) anlamını taşımaktadır.

# 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)