3- OSI MODELİ KATMANLAR-AÇIKLAR-SALDIRILAR-ÖNLEMLER

Fiziksel + Veri Bağı Katmanı

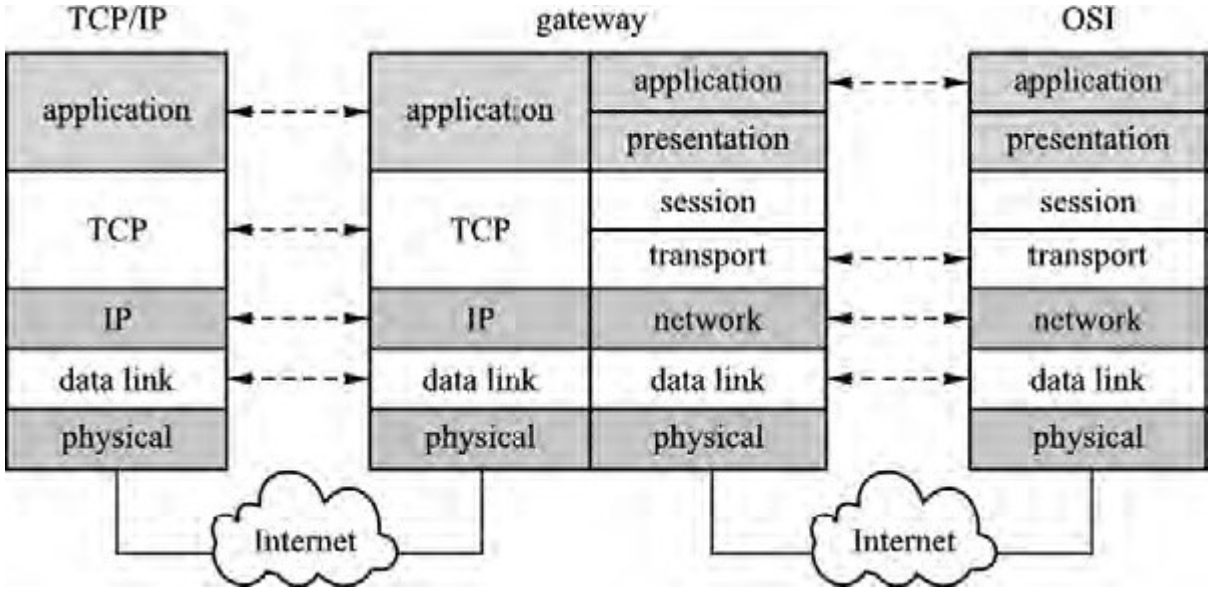
Açıklar-Saldırılar-Önlemler

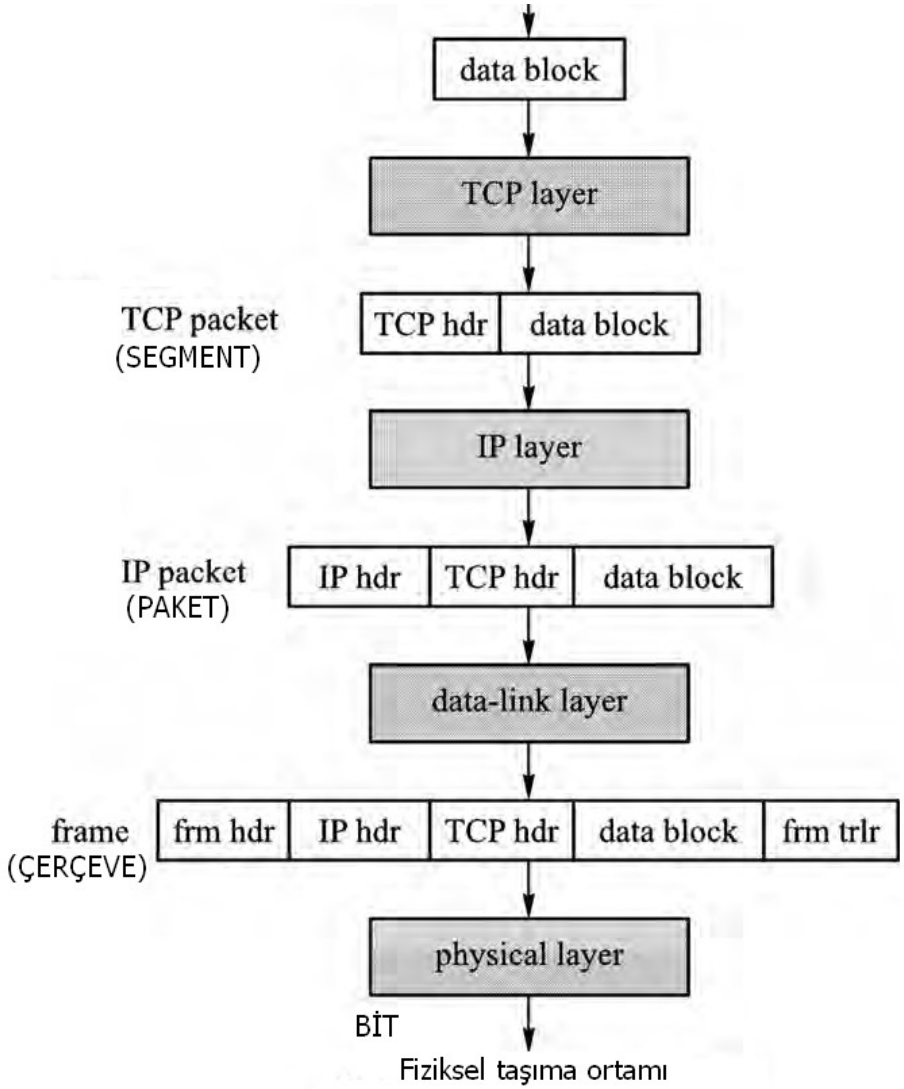
TCP/IP ve OSI Modeli

TCP/IP beş katmanlı bir mimariye sahiptir. TCP/IP protokol teknolojisinden farklı çalışan ağlar içinde modelleme yapabilmek için OSI modeli kullanılır.OSI modeli 7 katmanlı bir modeldir.

OSI mimarisi TCP/IP mimarisine oldukça benzer. OSI'nin uygulama ve sunum katmanı TCP/IP 'nin Uygulama katmanına denk düşer. OSI'nın sunum ve Transport katmanı TCP/IP'nin Transport katmanına denk düşer. Diğer katmanlar aynıdır. Her iki modelin yapısı ve özeti aşağıda verilmektedir.

Farklı iletişim protokollu ağlar arası geçiş için GATEWAY'lar kullanılır.




data block
TCP layer
TCP packet
(SEGMENT)
TCP hdr
data block
IP layer
IP packet
(PAKET)
IP hdr
TCP hdr
data block
data-link layer
frame
(ÇERÇEVE)
frm hdr
IP hdr
TCP hdr
data block
frm trlr
physical layer
BİT
Fiziksel taşıma ortamı

Katman	Tarif ve Anahtar Kelime	Protokol	Ağ elemanı	Kapsülasyon
Uygulama Application	* Kullanıcının ağdan istediği hizmetlerin tarif edilmesi için yazılım arayüzleri. * İletişim partnerinin tanımı	• HTTP • Telnet • FTP • TFTP • SNMP		Kullanıcı bilgisi ve DATA
Sunum Presentation	*Veri formatlama (dosya formatları) *Şifreleme, Deşifreleme, dönüştürme, sıkıştırma ve açma *Veri formatı değiştirme * İleteşecek düğümler arasındaki format ve işlem dönüşümleri yaparak gönderici ve alıcı uygulama katmanlarının kendi bildiği dili ve formatı kullanmasını sağlar.	• JPEG, BMP, TIFF, PICT • MPEG WMV, AVI • ASCII, EBCDIC • MIDI, WAV		DATA
Oturum Session	* Farklı hizmet istekleri için oturum tanımları yapılarak veri akışlarının biribirine karışmamasını sağlar. * İletişim oturumlarının bakımını ve kontrolunu yapar	• SQL • NFS • ASP • RPC • X window		DATA

Taşıma **Transport**		*Güvenilir (bağlantı yönlü) ve güvenilmez (bağlantısız) iletişim *Uçtan uca akış kontrolü *Bağlantı noktası ve soket numaraları *Segmentasyon, sıralama ve kombinasyon	• TCP (Bağlantılı) • UDP (Bağlantısız)		**SEGMENT**
Ağ Network		*Mantıksal adresler (IP v.b) *Yol (Rota) belirleme ve seçme * Ağlar arası Paket gönderme	• IP • IPX • AppleTalk • DECNET	• Routers • Layer 3 switches	PACKET
Veri Bağı Data Link	LLC MAC	*Bitleri bayt'a baytları Çerçeveye çevirir. *MAC adresi, fiziksel adresi kullanır. * LAN teknolojilerini tarif eder * Ortama erişimi kotarır * Akış kontrolunu yapar Flow control * ACK/Buffer * Pencereleme * Parity ve CRC kontrol işlemeleri	• LAN protocols 802.2 (LLC), 802.3 (Ethernet), 802.5(Token Ring), 802.11(Wireless) • WAN protocols HDLC,PPP, Frame Relay, ISDN	• (NIC) transceivers • Switch • Bridge	FRAME
Fiziksel Physical		* Bit düzeyinde medyada hareket * Kablo,konnektör,pin bağlantı pozisyonları * Sinyal senkronizasyonu, bit düzeyinde * Fiziksel ağ topolojisi	• EIA/TIA 232 (serial signaling) • V.35 (modem signaling) • Cat5 • RJ45	• Transmission media (cable and wires) • Mediaconnectors • Transceivers built into NICs) • Modems • Repeaters • Hubs • Multiplexers • CSUs/DSUs • Wireless Access P	BİT

Bilgisayar Ağlarında Katmanlı Modelleme açısından Güvenlik

- Bilgisayar ağlarında güvenlik konusu, ağ bilgisayarlarındaki ve iletişim halindeki verinin *Gizlilik, Bütünlük, İnkar edememe ve kullanılabilme* özelliklerini bozmak için yapılan (illegal olarak) saldırıları önlemektir.
- Bu saldırılar, **ağ iletişim protokollarının açıklarından, ağ cihazları ve iç/dış ağ erişiminin tam olarak denetlenememesinden, güvenlik politikalarının iyi oluşturulamamasından** kaynaklanmaktadır.
- Özellikle TCP/IP iletişim protokol kümesiyle çalışan internet gibi ağ yapılarında seyahat eden verilerin her türlü saldırıya açık olduğu bilinmektedir.
- Ağ güvenliği konusu üç farklı segment'te incelenecektir.

  1- İletişim protokolları açıklarından yararlanarak yapılan saldırılar ve tedbirler.

  2- İlgili Güvenlik protokollarının uygulanması

  3- Sistematik güvenlik (İç ağ/Dış Ağ koruma)
- Bu derste TCP/IP ve OSI katmanlı ağ modeli ve ilgili katman protokolları ve bunların zayıflıkları üzerinde durulacaktır. Bu zayıflıklardan yararlanılarak yapılacak saldırılar ve tedbirleri nelerdir?
- İlgili ağ cihazlarının korunması ve cihazların uygun konfigürasyonları ile ağ güvenlik açıklarının azaltılması üzerinde durulacaktır.

Fiziksel Katmanda Gizlilik/Bütünlük

Fiziksel Çevreden kaynaklanabilen sorunlar (Açıklar)

- Ağ ortamının çok katlı binalarda oluşturulması veya herkesin ulaşabileceği yerlerden geçmesi.
- Ağ cihazlarının konulduğu oda veya kabinlerin güvenlik altına alınmaması.
- Herkesin erişebileceği bir ağ altyapısı veya elektrifikasyon altyapısı.
- Elektromanyetik ortam
- Elektrik Kesintilerine karşı önlemlerin alınmayışı (KGK'lar)
- Tehdit: Ağ hizmetlerinin verilememesi, verilerin dinlenmesi, değiştirilmesi yok edilmesi ihtimalinin varlığı.

THİN ETHERNET (çok az kullanılmaktadır)

- Tek bir kablo ile iletişimin sağlanması

  Güvenlik Açığı: Tüm cihazlar için bilgi yayını.

  Tehdit: Bilgi Sızıntı, Yanlış Kullanım

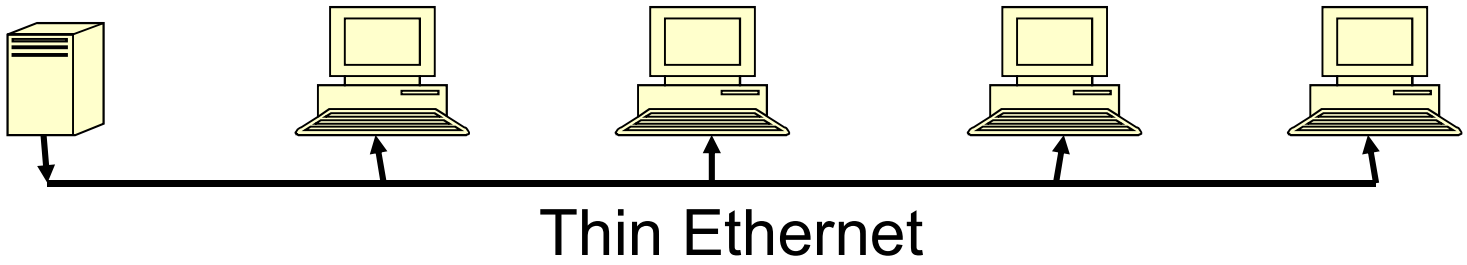
  Güvenlik Açığı: Bir kablo arızası ağı devre dışı bırakır.

  Tehdit: Denial of Service

- Kolay yükleme ve ek aygıtlar takabilme

  Güvenlik Açığı: Herkes ağa dahil olabilir.

  Tehdit: Yanlış kullanım.



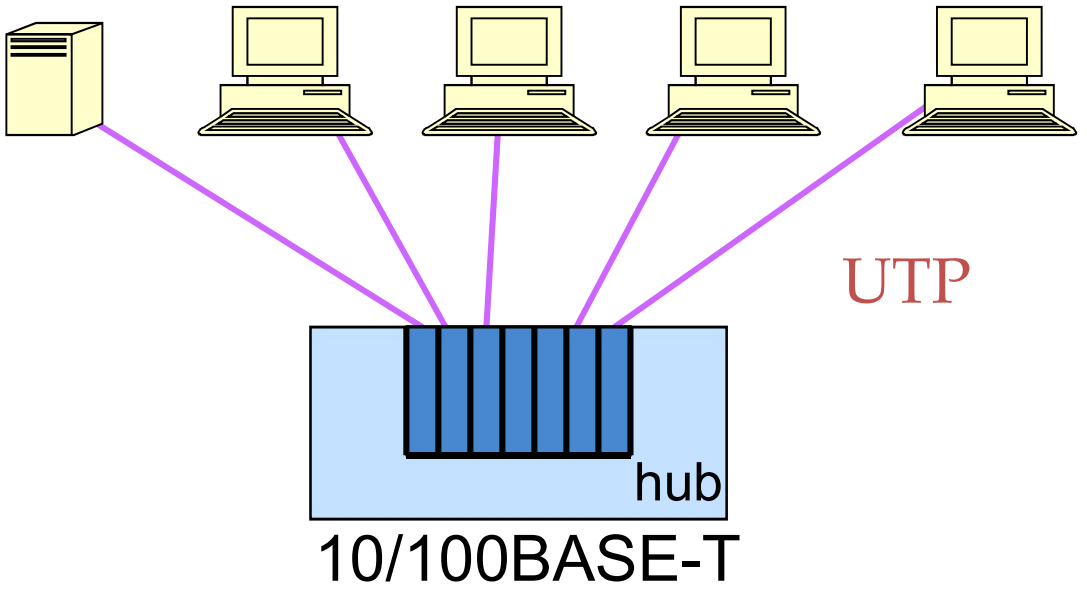
UTP ve Hub

- **Hub ve cihaz arasındaki ortam tek bir kablodur.**
- **Ek cihazlar sadece hub'a eklenebilir.**
- **Ayırma / kablo kopması nadiren diğer aygıtları etkiler**
- **Kolay kurulum**

– ***Kablonun indüktansından dolayı veri işaretleri etkilenebilir.***

– ***Ethernet kablosuna, herhangi bir yerden girilerek bilgiler dinlenebilir.***

– ***Uygun kablo kullanılmamışsa, Kablo bir manyetik alandan geçiyorsa veri işaretlerinde bozulmalar olabilir.***



HUB

- HUB’da veri herkese (Broadcast) yayınlanır.

Güvenlik Açığı: tüm cihazlar için bilgi yayını.
Tehdit: Bilgi kaçağı, Yanlış Kullanım

Güvenlik Açığı: Herkes hub'a takabilirsiniz.
Tehdit: Yanlış kullanın.

Fiziksel Katmandaki diğer medya

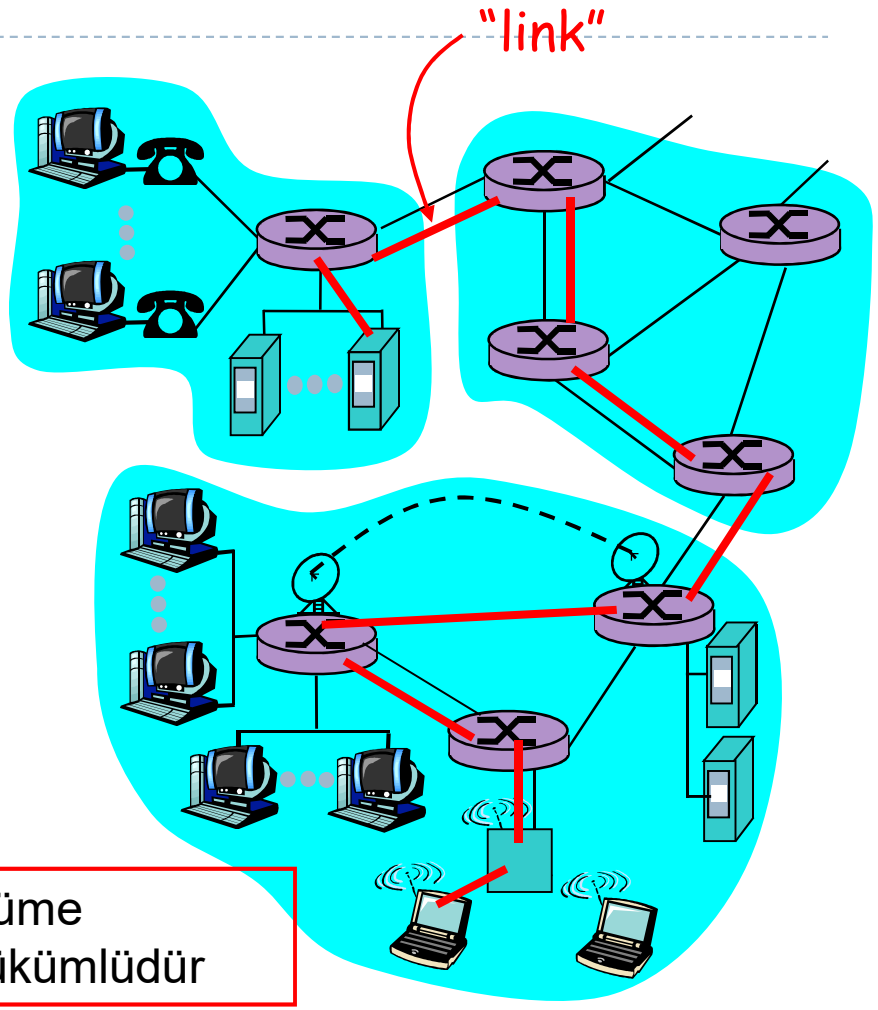
- **Radyo frekanslı dalgalar (Wireless LAN)**
  - Ağ iletişimi kullanılan radyo dalgaları 1-20GHz arasındaki mikrodalgalardır. Bu işaretler taşıyıcı işaretlerdir .
  - Radyo sinyalleri, girişime, tahribata, dinlenmeye uygundurlar.
  - Bulunduğu yayın alanında izinsiz dinlemelerin **(Jamming)** engellenmesi çok zordur.
  - Eğer taşıyıcının frekansı aralıklı olarak değiştirilirse, bilginin başkası tarafından dinlenmesi engellenmiş olabilir.
- **Fiber Optik**

  Hub ve cihaz arasındaki kablo tek ortamdır.
  - Kablo kurulumu ve çekilmesi zordur. Ek yapılması zordur.
  -Çok yüksek hızlarda çalışır.
  - Dinlenmesi zordur.
  - Magnetik ortamdan etkilenmez.

Veri bağı (Data Link Layer) Katmanı
Protokollar – açıklar- Saldırılar-Savunmalar

- Hostlar ve routerlara **node** diyeceğiz.
- Komşu düğümler arasındaki fiziksel iletişim ortamlarına (yollarına - kanallarına) LİNK diyeceğiz.
- Telli linkler
- Telsiz Linkler
- LAN'lar

DLL katmanı PDU = **frame** (Çerçeve)



Veri bağı katmanı, bir düğümden bitişik düğüme bir LİNK üzerinden datagram aktarmakla yükümlüdür

DATA LİNK LAYER (DLL)'in önemi

Veri bağı katmanı (DLL) ağdan, ağ cihazına (Switch, router, host, sunucu v.b) gelen çerçevelerin; kimlik filtreleme, erişim kontrol listeleri, kimlik doğrulama, çerçevenin hatalı gelip gelmediği v.b uygulamaların ilk yapıldığı katmandır. Çerçevenin üst katmanlara erişimini filtreleyen katmandır.

Ağ cihazındaki veya ağa bağlı hostların ağa göndereceği verilerin en son olarak kontrol edilip kapsüllendiği (çerçeve haline getirmek) yerdir.

Ağ katmanına ara servisi sağlanması

Çerçeveleme işlemi

İletim hatalarının sezilmesi ve kontrolu

Veri akışının düzenlenmesi

Yavaş Alıcılar hızlı göndericiler tarafından sıkıştırılmaz.

Ortama erişimin kotarılması (fiziksel adresleme),

Fiziksel katmandaki bit dizisi akışını anlamlı bit guruplarına (Çerçeve-Frame) dönüştürme

Veri bağı katmanı Protokolları

Veri Bağı katmanı protokoları, LAN ve WAN ağ yapıları için farklı farklıdır. Saldırı ve açıklar ve güvenlik protokollarının'da LAN veya WAN DLL protokollarına göre incelenmesi uygundur.

En çok kullanılan Veri bağı LAN protokolları

- Ethernet
- Token Ring
- FDDI

Sık kullanılan WAN veri bağı protokolları

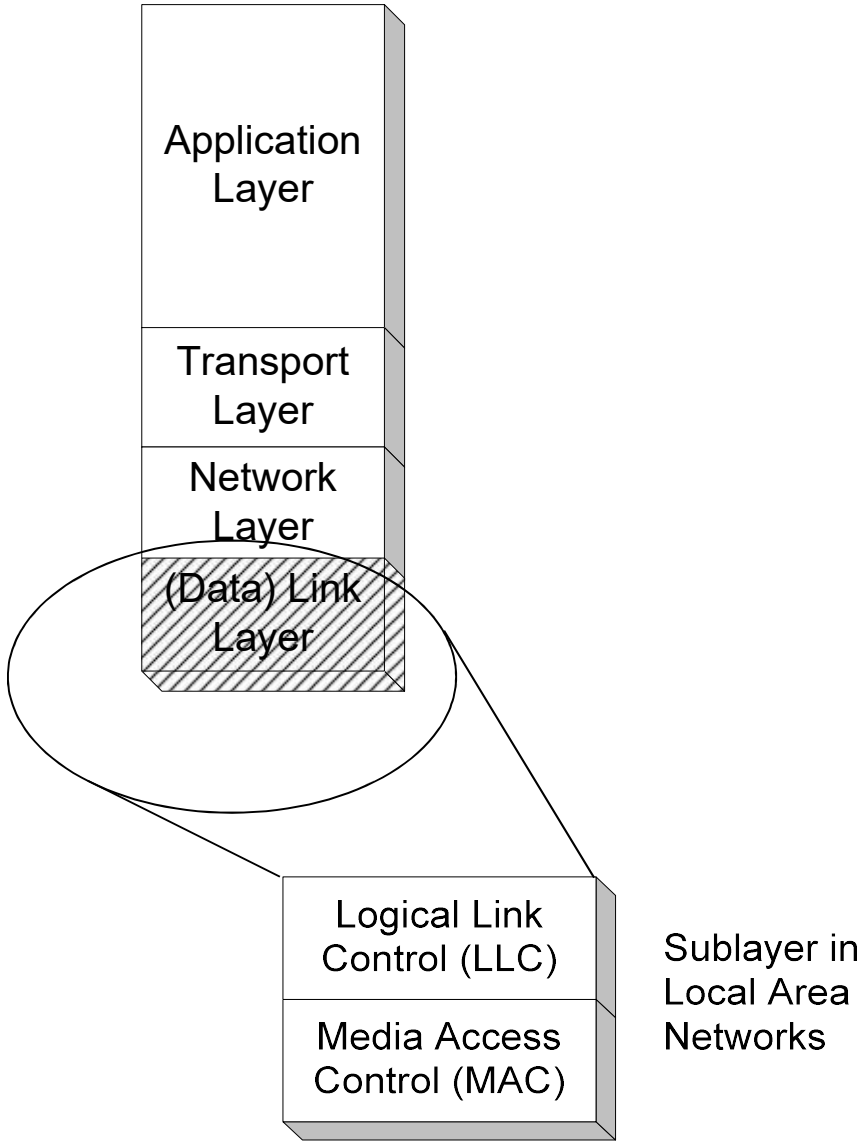
- PPP (point to point protocol)
- HDLC (High Level Data Link Control)
- Frame Relay
- ATM (Asychronus Transmısion Mode)

TCP/IP açısından Veri bağı katmanına bakış (LAN)

•Aslında OSI başvuru modelindeki Fiziksel katman ve Veri bağı katmanı, bir yerel ağdaki süreci tanımlamaya yeterlidir.

Network katmanından aldığı veri paketlerine hata kontrol bitlerini ekleyerek çerçevelere (frame) bölünmüş halde fiziksel katmana iletme işinden sorumludur.

Yani iletim ortamına erişim Veri bağı katmanının görevidir.



- Veri bağı katmanı ağ üzerindeki diğer bilgisayarları tanımlamasını, kablonun o anda kimin tarafından kullanıldığının tespitini yapabilir.
- Ayrıca iletilen çerçevenin doğru mu yoksa yanlış mı iletildiğini kontrol eder, eğer çerçeve hatalı iletilmişse çerçevenin yeniden gönderilmesini sağlar. Yani hat üzerinde oluşan hata bu katmanda sezilir **(ARQ).**
- Bu katmanda iletilen çerçevenin hatalı olup olmadığını anlamak için **CRC (Cyclic Redundancy Check yöntemi kullanılır.**
- Veri bağı katmanı iki alt bölüme ayrılır:

  Media Access Control (MAC)

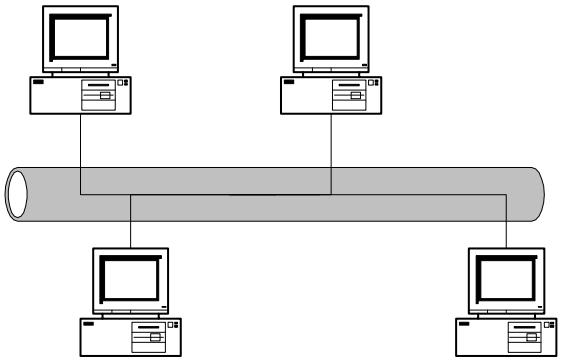
  MAC alt katmanı veriyi hata kontrol kodu(CRC), alıcı ve gönderenin MAC adresleri ile beraber oluşturup, fiziksel katmana aktarır. Alıcı tarafta da bu işlemleri tersine yapıp veriyi veri bağlantısı içindeki ikinci alt katman olan LLC'ye aktarmak görevi yine MAC alt katmanına aittir. MAC katmanı, aynı zamanda fiziksel adresleme bazında, verinin çoklu ortam üzerinden alıcısına ulaşmasından da sorumludur.

  Logical Link Control (LLC)

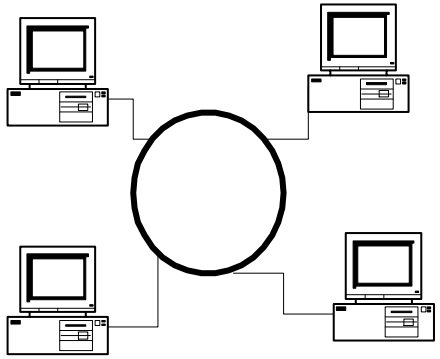
  LLC alt katmanı bir üst katman olan ağ katmanı için geçiş görevi görür. Protokole özel mantıksal portlar oluştururarak (Service Access Points, SAPs) gönderici ve alıcı tarafın aynı protokoller iletişime geçebilmesin sağlar(örneğin TCP/IP<-->TCP/IP). LLC ayrıca veri paketlerinden bozuk gidenlerin(veya karşı taraf için alınanların) tekrar gönderilmesinden sorumludur. Flow Control yani alıcının işleyebileğinden fazla veri paketi gönderilerek boğulmasının engellenmesi de LLC'nin görevidir.

Local Area Networks

- LAN’larda ortama erişim paylaşımlı kullanım şeklidir. Birçok ortama erişim yöntemi (Ethernet, Token Ring, ATM v.b) mevcuttur.



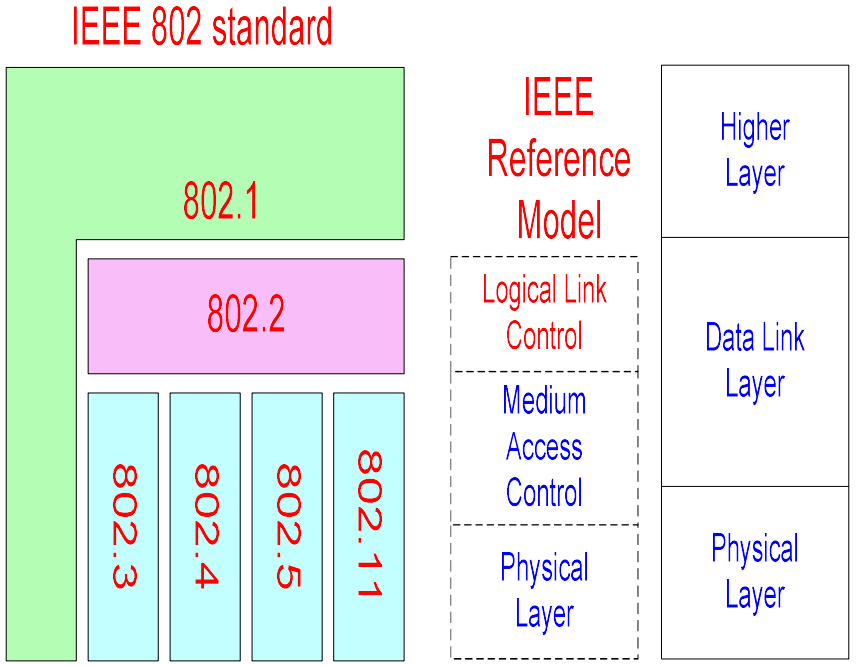
Bus LAN



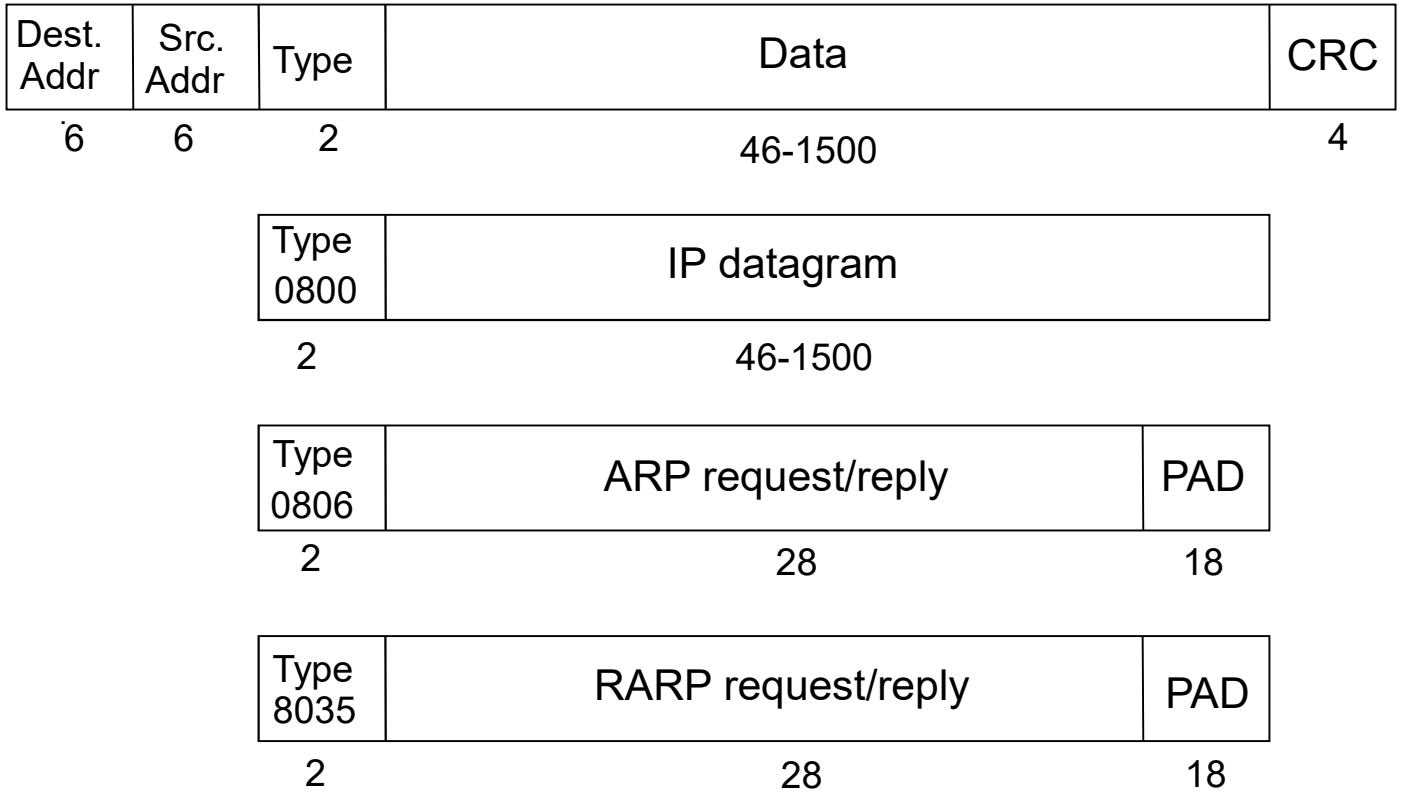
Ring LAN

IEEE 802 Standartları

- IEEE 802 bir LAN standartıdır. Bu standartta LLC katmanı ve değişik MAC alt katmanlar tanımlanır.
- 802.3 Ethernet
- 802.4 Token Bus
- 802.5 Token Ring
- 902.11 Wireless LAN



Ethernet Çerçeve Formatı



LANLAR'DA Adresleme

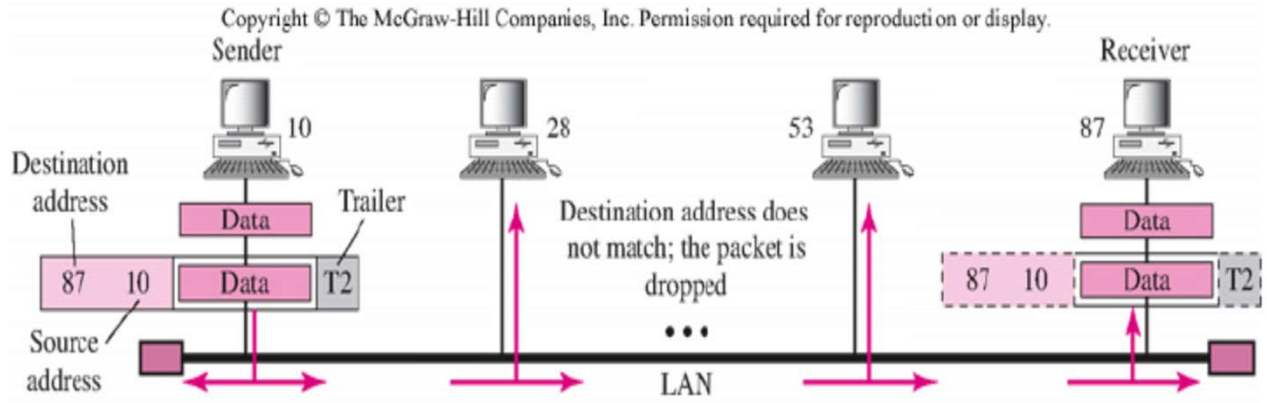
- Bir Ağ içerisindeki iki bilgisayarın biribirleriyle haberleşebilmesi için Fiziksel Adreslerinin bilinmesi gerekir.

Fiziksel Adresleme

- Ağdaki cihazların değişmez gerçek adresleri olarak tarif edebiliriz. NIC kartlarının belleklerinde yazılırlar. Ethernet teknolojisinde 48 bit uzunluğunda MAC (Media Acces Control)dır.
- Veri bağı katmanında adresleme sağlanır.
- Aynı ağ içerisinde bu adreslemeye göre çerçeveler yerine ulaşır.

Fiziksel adresleme

- Data link layer'da frame içinde bulunur. Ağ yapısına göre farklı uzunluktadır. (Ethernet için 6 byte NIC, LocalTalk Apple için 1 byte)



İkinci Katman Saldırıları

•Ağ saldırıları denince öncelikle OSI'nin üçüncü (Ağ Katmanı) ve daha yukarı katmanlarıyla ilgili ataklar akla gelmektedir. Fakat ikinci katman atakları da en az üst katmanlara yönelik yapılan ataklar kadar etkili olabilmektedir.

• İkinci katman atakları yerel alan ağlarının içinden (LAN) yapıldığı için güvenlik duvarı ya da saldırı engelleme / tespit etme sistemleri tarafından engellenememektedir / tespit edilememektedir. Çünkü bu sistemler genellikle üçüncü ve daha üst katmanların güvenliği için tasarlanmıştır.

• Ayrıca saldırı tespit veya engelleme sistemleri genellikle dış ağdan iç ağa gelebilecek saldırıları tespit ya da engellemek için kullanılmaktadır. Bu sistemlerin iç ağda yer alan bir saldırganın, yine iç ağda yer alan anahtarlara yapılacak saldırıları tespit edebilme / engelleme gibi bir şansı yoktur.

•Ağ güvenliği tüm OSI katmanlarının güvenliğinin ele alınmasıyla asıl amacına ulaşacaktır. Üst katmanların güvenliğinin alınıp, ikinci katman güvenliğinin ele alınmaması ağ güvenliğinin tam anlamıyla anlaşılamadığını gösterir.

- Veri bağı katmanı saldırılarının büyük bir kısmı; iletişim sırasında doğru kimlik doğrulama eksikliğine dayanır.

Bir LAN'da (İkinci katman) en yaygın saldırılar;

- Switch MAC tablosu tablosu taşması,
- VLAN hoping,
- Spanning Tree Protokolü (STP) manipülasyonu,
- ARP önbellek zehirlenmesi,
- DHCP Starvation,
- Cisco Keşif Protokolü (CDP) saldırıları olarak sayılabilir..

SWİTCH'ler

- Veri bağı katmanının en önemli görevlerinden birisi de lokal adresleme yapmaktır. Bu katmanda bu işi Switch'ler yapar.
- Fiziksel Adreslere (MAC v.b) göre.
- Ethernet, paketleri herkese yayınlar.

  2. katmanda paket süzme işlemi;

  – Hangi MAC adresi switc'hin hangi portunun arkasında olduğunun öğrenilmesi.
  – Paketi sadece uygun porta geçirme işlemi.

Switch işlemleri

- Bir çerçeve Switc'he geldiğinde
  - Switch, tablosundan bu çerçevenin gideceği hedef adresin hangi portta olduğuna bakar. İlgili porta çerçeveyi gönderir.

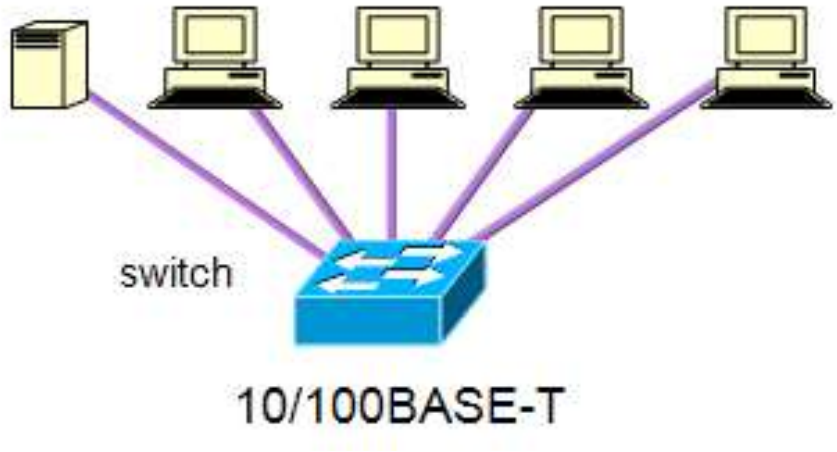
- Switch'lerin (Transparent v.b) MAC tablolarının nasıl doldurduklarının hatırlayınız????????

- SwitcH'ler akıllı cihazlardır.
  - Traffik izleme, fiziksel adres bazında yönlendirme ve uzaktan konfigüre edilebilme özelliğine sahiptir.
- Switch 2.katman cihazıdır.

Switch'ler

•Switch'ler veriyi sadece hedef alıcıya (Fiziksel adrese) gönderir. Switch'in üzerinde bir adres-port tablosu tutulur. Buna CAM (Content Addressable Memory) de denir. *Örnek: Cisco 3550 serisi switch MAC adres tablosunda 8192 tane MAC adresi bulundurabilmektedir.*

• MAC adresleri MAC adres tablosunda belirli bir süre (Örneğin 300 saniye) tutulur sonra silinir.



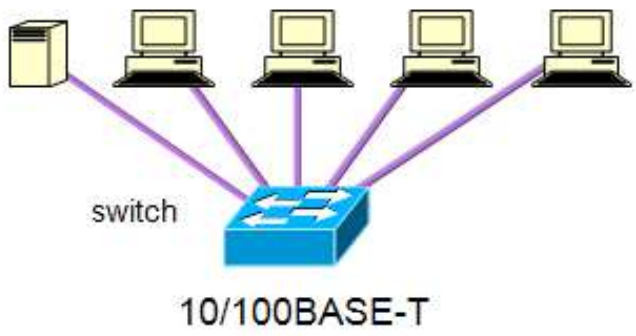
Device	MAC address
1	00:0e:81:10:19:FC
2	00:0e:81:32:96:af
3	00:0e:81:31:2f:d7
4	00:0e:81:97:03:05
8	00:0e:81:10:17:d1

Switch'lerde güvenlik Açıkları

Switchlerin önemli bir zafiyeti, MAC adres tablosunun dolması durumunda ortaya çıkmaktadır.

Gelen çerçevenin (frame) hedef MAC adresi, anahtarın MAC adres tablosunda bulunduğu takdirde anahtar bu çerçeveyi ilgili porta gönderecektir. Fakat anahtara gelen çerçevenin hedef MAC adresi, anahtarın MAC adres tablosunda bulunmadığı durumlarda, anahtar çerçeveyi tüm portlarına yollayacaktır.

Bu da saldırganın, anahtar üzerinde herhangi bir port yönlendirmesi yapmadan, *sadece anahtarın MAC adres tablosunu sahte MAC adresleriyle doldurmak suretiyle*, anahtar üzerindeki tüm trafiği dinleyebilmesine yol açacaktır. Bu durum ayrıca anahtarın performansına da olumsuz etki edecektir.



	Device	MAC address
1	1	00:0e:81:10:19:FC
2	4	00:0e:81:32:96:af
3	4	00:0e:81:32:96:b0
4	4	00:0e:81:32:96:b1
	...	...
9999	4	00:0e:81:32:97:a4

1. MAC Adres Atağı

- Anahtara gelen çerçevenin hedef MAC adresi, anahtarın MAC adres tablosunda bulunmadığı durumlarda, anahtar çerçeveyi (frame) tüm portlarına yollayacaktır. Peki bu nasıl gerçekleşir?

- Anahtarın MAC adres tablosunun tamamen dolu olduğunu düşünelim ve anahtarın, beşinci portuna bağlı bir bilgisayardan gönderilen çerçevenin (frame) hedef MAC adresinin, anahtarın MAC adres tablosunda bulunmadığını düşünelim. Bu durumda anahtar, beşinci portundan gelen çerçeveyi (frame) diğer tüm portlarına yollayacaktır. Bu da ilgili beşinci porttan çıkan tüm bilginin diğer portlara da gönderilmesi sonucunu doğuracaktır.

- Bu durum saldırganın, anahtar üzerinde herhangi bir port yönlendirmesi yapmadan, sadece anahtarın MAC adres tablosunu sahte MAC adresleriyle doldurmak suretiyle, anahtar üzerindeki tüm trafiği dinleyebilmesine yol açacaktır. Ayrıca anahtarın performansı da düşecektir.

2. Sahte MAC (MAC Spoofing) Atağı

- Bu atak türünde saldırgan, anahtara gönderdiği çerçevelerin (frame) içerisindeki “kaynak MAC adres” kısmına, dinlemek istediği bilgisayarın MAC adresini yazar.
- Anahtar MAC adres tablosunu bu duruma göre günceller. Böylece anahtarın MAC adres tablosunda, saldırganın bağlanmış olduğu anahtarın portu için iki adet MAC adresi yer almış olur. (Saldırganın MAC adresi ve hedef bilgisayarın MAC adresi) Hedef bilgisayara gönderilen çerçeveler de (frame) de böylece saldırganın bilgisayarına gönderilmiş olur.
- Hedef bilgisayar ağa paket gönderene kadar bu durum devam edecektir.

Switch tablolarını sahte MAC adresleriyle doldurmak (MAC FLOODİNG)

Buna MAC flooding (MAC taşması) atağı'da denir. Aşağıda normal bir switching tablosu verilmiştir.

vlan	mac address	type	protocols	port
20	000a.2281.61e4	dynamic	ip	GigabitEthernet1/1
20	000a.2201.9079	dynamic	ip	GigabitEthernet1/1
20	000a.22c0.ddf9	dynamic	ip	GigabitEthernet1/1
61	001b.2461.09f6	dynamic	ip	GigabitEthernet1/2
61	0040.ca79.8821	dynamic	ip	GigabitEthernet1/15
61	00d0.b7bc.3d2c	dynamic	ip	GigabitEthernet3/34
61	0800.8e05.1bbc	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.39b7	dynamic	ip	GigabitEthernet3/35

Anahtarın MAC adres tablosunu sahte MAC adresleriyle doldurabilecek yazılımlar mevcuttur. Anahtara bu yazılımlar ile saldırılıp MAC adres tablosu sahte adreslerle doldurulabilir. Bu saldırıdan sonra anahtarın MAC adres tablosu aşağıdakine benzer bir durumda olacaktır. Saldırganın portunun GigabitEthernet3/33 olduğunu düşünüyoruz.

vlan	mac address	type	protocols	destination port
20	000a.2281.61e4	dynamic	ip	GigabitEthernet1/1
20	000a.2201.9079	dynamic	ip	GigabitEthernet1/1
20	000a.22c0.ddf9	dynamic	ip	GigabitEthernet1/1
61	001b.2461.09f6	dynamic	ip	GigabitEthernet1/2
61	0040.ca79.8821	dynamic	ip	GigabitEthernet1/15
61	00d0.b7bc.3d2c	dynamic	ip	GigabitEthernet3/34
61	0800.8e05.1bbc	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1aaa	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1aab	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1aac	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1aad	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1aae	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1aaf	dynamic	ip	GigabitEthernet3/33
61	0800.8e05.1ab0	dynamic	ip	GigabitEthernet3/33
…….				
…….				
61	0800.8e05.39b7	dynamic	ip	GigabitEthernet3/35

ÇÖZÜM:

- Bu saldırıdan korunmanın yolu çok basittir: MAC adresi kilitlemesi (belirli bir MAC adresini kayıtlı bir IP adrsine eşleştirme). Ancak bunun için elimizdeki anahtarın MAC adres kilitlemesi özeliğinin olması gerekmektedir.
- Anahtarlarımızın portlarına MAC adresi kilitlemesi uygularsak bu olası saldırıdan kurtulmuş oluruz. Aşağıda Cisco anahtarlar için MAC adresi kilitlemesi örnek konfigürasyon satırları bulunmaktadır:
- (Aşağıdaki konfigürasyonlar sizin sistemlerinize uygun olmayabilir.)
- **CISCO konfigürasyonu**
- Anahtar(config)#interface range GigabitEthernet 3/2 – 48
- Anahtar(config-range)# switchport mode access
- Anahtar(config-range)# switchport port-security
- Anahtar(config-range)# switchport port-security maximum 3
- Anahtar(config-range)# switchport port-security violation restrict
- Anahtar(config-range)#switchport port-security mac-address sticky

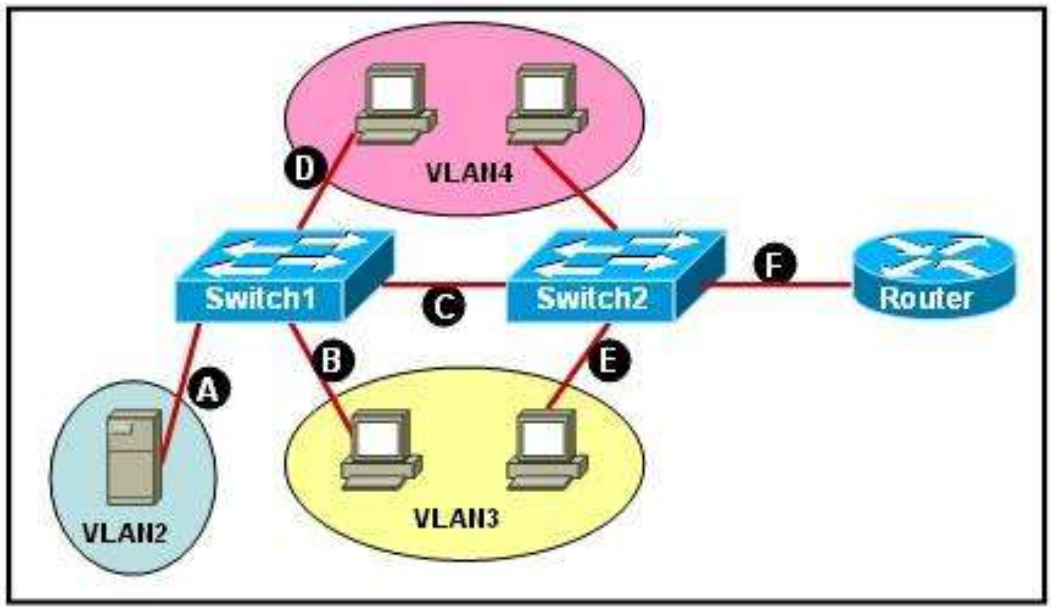
Koruma?

- Switchlerde fiziksel güvenlik
- Switchler çok sayıda gelen çerçeve süresince (su baskını) hata yapabilirler.
  - Tehdit: Denial of Service

  Önlem:

  1. Switch Tablosuna sadece statik olarak MAC adresleri ekleyebiliriz.
  2. MAC adres tablosunda bir port karsisina gelebilecek maksimum MAC adres sayisini belirli bir sayida sinirlayabiliriz.
  3. Belirledigimiz kurallarin disina çikildiginda switchin önlem almasini saglayabiliriz.
- Not: Bunun için Switch'in Acces (erişim) portu olmalı ve yönetilebilir Switch olmalıdır.

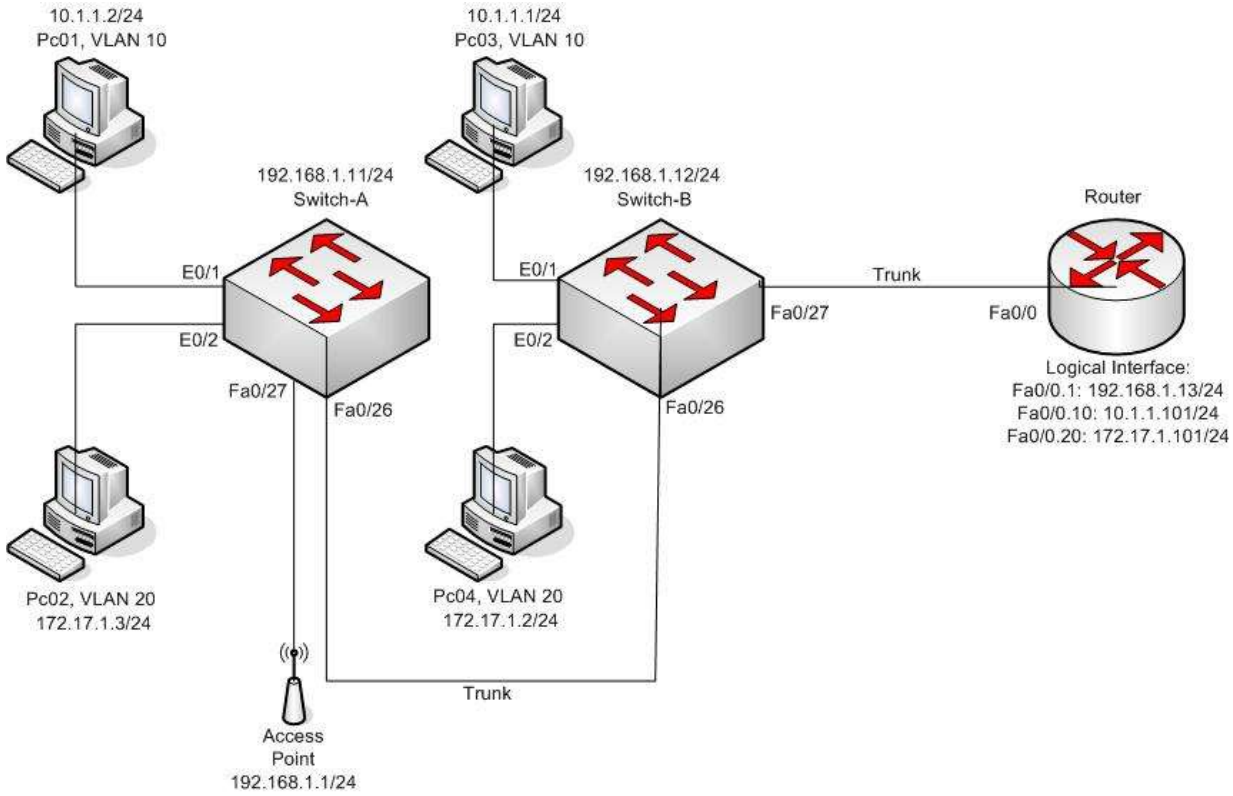
VLAN (Virtual LAN)



VLAN'lar Farklı veya aynı swithclerin (2.Katman) farklı portlarına bağlı hostlar ile bir broadcast domaini (farklı Subnet'te denebilir) oluşturmasına izin verir.

Farklı VLAN'lere üye olan bilgisayarlar ağ üzerinden birbirlerine erişemezler. Bir VLAN'in ARP isteği diğer VLAN'lere normalde hiçbir şekilde ulaşamaz. Çünkü herbir VLAN farklı bir "broadcast domain"idir.

- VLAN’lerin birbirlerine erişebilmeleri için, VLAN arayüzleri oluşturmak, bu arayüzlere birer IP numarası vermek ve sonrasında da “Inter-VLAN routing (VLAN’ler arası yönlendirme)” yapmak gerekir.
- Bunun için de ya bir yönlendiriciye ya da yönlendirici özelliği bulunan bir anahtarlama cihazına ihtiyaç vardır.



VLAN atlama (Hopping) atağı

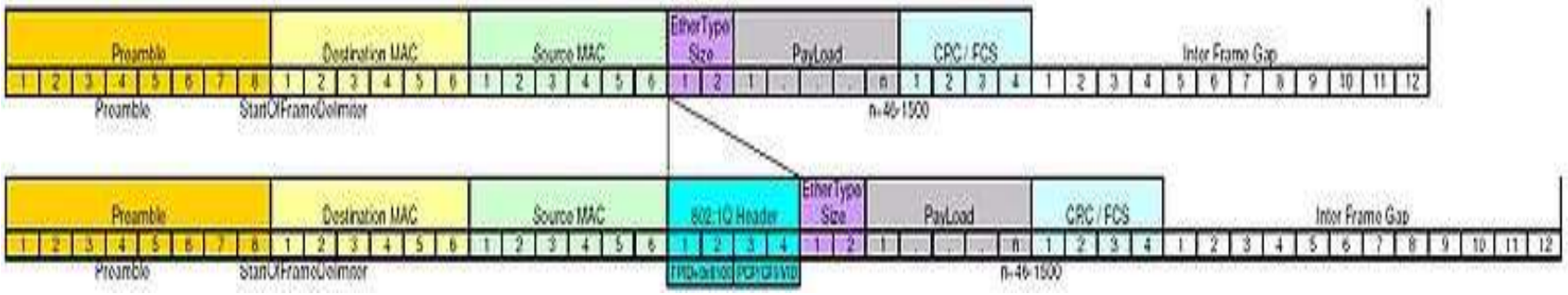
- Fakat anahtarlar üzerinde bazı güvenlik önlemleri alınmadığı takdirde VLAN'ler arası geçiş sağlanıp, bir VLAN'e bağlı bir bilgisayar, kendi VLAN'inin haricinde farklı bir VLAN'de yer alan başka bir bilgisayara erişebilmektedir.
-
- Saldırganın, bağlı bulunduğu anahtardan farklı bir anahtar üzerinde kendi VLAN'i haricindeki, normalde erişememesi gereken bir VLAN'e erişmesine *VLAN atlama atağı* denmektedir.

- VLAN atlama atakları ikinci katmanda (Layer 2) gerçekleştirildiği için IP tabanlı (Layer 3) saldırı tespit ya da engelleme sistemleri tarafından yakalanmaları mümkün değildir.

2. VLAN Hopping Atakları

a) Anahtar Sahtekarlığı (Switch Spoofing)

- Bu atak türü, Cisco marka anahtarlara yönelik bir ataktır. Cisco anahtarlarının portları ya “access port” ya da “trunk port” olarak tanımlanabilirler. “access port”, bir adet VLAN’e atanmış port olarak bilinir. “access port”ların, bağlı bulundukları VLAN haricindeki diğer VLAN portlarına erişimi yoktur. “trunk port” ise anahtar üzerinde yer alan tüm VLAN’lere üyedir ve farklı anahtarlar üzerinde tanımlı olan farklı VLAN’lere üye portların birbirleriyle iletişimini sağlar.
- Anahtarlar arasındaki trafiğin ayırt edilebilmesi için “trunk port”, üzerinden geçen çerçevelere (frame) bir etiket ekler. Bu etiketleme mekanizması iki türlü yapılır. Bunlardan birisi IEEE 802.1q ve diğeri de sadece Cisco anahtarlarda çalışabilen ISL (InterSwitch Link) etiketlemesidir.
- Anahtarlar arası VLAN erişiminin sağlanması için anahtarları birbirine bağlayan “trunk port”ların aynı etiketleme türüne sahip olması gereklidir. (Karşılıklı bağlanmış olan “trunk port”ların ya IEEE 802.1q ya da ISL etiketli olması gereklidir.)



- Bu ön bilgilendirmeden sonra şimdi de anahtar kandırma atağının nasıl yapıldığını inceleyelim:
- Cisco anahtarların portları beş modda çalışırlar: “on”, “off”, “desirable”, auto” ve nonegotiate”. Cisco anahtarların portları ön tanımlı (default) olarak “dynamic desirable” modundadırlar. Bu da şu anlama gelmektedir: Bu portun karşısındaki port “access port” ise port kendisini otomatik olarak “access port” olarak tanımlayacaktır. Karşısındaki portun modu “on”, “auto” ya da “dynamic desirable” ise port kendisini “trunk port” olarak tanımlayacaktır.
- Şimdi; bir saldırgan “dynamic desirable” modundaki bir porta kendisini “trunk port”muş gibi gösteren bir bilgisayar bağlandığı takdirde anahtarın ilgili portu “trunk port” olacaktır. Böylece saldırganın bilgisayarı tüm VLAN’lere erişebilecek duruma gelecektir. Çünkü bütün VLAN’lere gidecek olan çerçeveler (frame) saldırganın portuna da gelecektir. Saldırgan, bu sayede bütün VLAN’lere giden trafiği dinleme imkanına sahip olacaktır.

b) Çift Etiketleme (Double Tagging)

- Bu saldırının anlaşılabilmesi için “native(yerel) VLAN” ve IEEE 802.1q kavramlarının iyi bilinmesi gereklidir. Bu kavramları biraz açıklamaya çalışalım:

- Normalde anahtar üzerindeki her bir port sadece bir VLAN’e üye yapılabilir. Bir porttan birden fazla VLAN’e iletilm için ilgili porta IEEE 802.1q tanımlamasının yapılması gereklidir. IEEE 802.1q tanımı yapılmış olan port, kendisine gelen çerçevenin “MAC adresi” ve “EtherType” alanlarının arasına 32-bitlik bir başka alan ekler. Bundan da anlaşılabileceği üzere, IEEE 802.1q tanımı, aslında bir etiketlemeden (tagging) ibarettir. IEEE.802.1q portu, sadece etiketlenmiş (tagged) çerçeveleri iletir. Etiketlenmemiş (untagged) çerçeveler IEEE 802.1q portundan geçemezler.

- Bunun istisnası “native VLAN”e üye olan çerçevelerdir. IEEE 802.1q portuna gelen ve “native VLAN”e üye olan çerçeveler, herhangi bir etiketlenme yapılmaksızın IEEE 802.1q portu üzerinden karşıdaki anahtara iletilirler.

- Karşılıklı bağlanmış olan anahtarlar arasında VLAN iletişiminin yapılabilmesi için karşılıklı olarak bağlanmış bu anahtarların IEEE 802.1q portlarının “native VLAN” numaralarının aynı olması gereklidir.

- IEEE 802.1q portuna etiketlenmemiş çerçeve gelirse bu çerçeveler “native VLAN”e üye kabul edilirler. Özetle, IEEE 802.1q tanımı yapılmış olan portlar “native VLAN” için normal bir port gibi davranır.

“native VLAN” özelliği çift etiketlenmiş VLAN atlama saldırılarına açıktır. Şimdi çift etiketleme saldırısının nasıl yapıldığına bakalım:

Herhangi bir tanımlama yapılmadığı takdirde, bir IEEE 802.1q portunun “native VLAN” numarası “1”dir (VLAN 1). Saldırgan, oluşturmuş olduğu çift VLAN etiketli çerçevenin, dış VLAN etiket numarasına “native VLAN”in numarasını verir. İç VLAN etiket numarası olarak da hedef anahtarda yer alan hedef VLAN’in numarasını verir.
örnekle açıklayalım:

Saldırgan, kendisini “native VLAN”e üyeymiş gibi gösteren bir çerçeve oluşturur. Tabii ki bu saldırıyı yapabilmesi için saldırganın, bağlı olduğu anahtarın “native VLAN” numarasını bilmesi gereklidir. Yukarıda da belirtildiği gibi “native VLAN” için herhangi bir tanım yapılmamışsa, VLAN 1 “native VLAN”dir ki “native VLAN” numarası da anahtarlarda genellikle değiştirilmemektedir.

Bu durumda saldırgan kendisinin VLAN 1’de olduğunu belirten bir çerçeve oluşturur. Bu çerçeveye 32-bitlik bir etiket ekler (IEEE 802.1q etiketi). Bu ilk etiketin içindeki VLAN değerine de (VID) “1” verir.

Bundan sonra saldırgan, çerçeveye ikinci bir 32-bitlik etiket daha ekler. Bu etiketin içine de saldırıyı yapacağı VLAN’in numarasını yazar. Bu şekilde saldırgan çift etiketli bir çerçeve oluşturmuş olur. (Bu şekilde özel çerçevelerin (frame) oluşturulabildiği programlara internet üzerinden ulaşmak zor değildir.)

Önlem

- Anahtar kandırma (switch spoofing) atağını engellemek için anahtarın portlarından DTP (DynamicTrunking Port) özelliğini kaldırmak gerekir.
- IEEE 802.1q portuna ihtiyacımız olduğu takdirde bunun manuel olarak yapılması tavsiye edilir. Aşağıdaki komut satırı girilmek suretiyle anahtarın portlarından DTP kaldırılmış olur:

ANAHTAR(config)# interface range FastEthernet 0/1 – 24
ANAHTAR(config-if)# switchport mode access

- Çift etiketleme atağından korunmak için de aşağıdaki maddeler tavsiye edilir:

1. “native VLAN”i kullanıcılar için kullanmayın,
2. “default VLAN” numarasına “1”den farklı bir değer verin ve bu VLAN’i kullanıcılar için kullanmayın,
3. Kullanılmayan portları kapatın ve bu portları “default VLAN” haricinde başka bir VLAN’e dahil edin.

IP Adresleme

- IP adresleri 32 bit uzunluğundadır. (IPV4)
- Örnek.
    - 62.49.67.170
- RFC 1918'e göre aşağıdaki ağ adresleri özel ağlarda kullanılmak için ayrılmışlardır.
    - 10.0.0.0 to 10.255.255.255
    - 172.16.0.0 to 172.31.255.255
    - 192.168.0.0 to 192.168.255.255

IP Adresten Ethernet Adresine dönüş

- Address Resolution Protocolü (ARP)
  - 3.katman protokolüdür.
  - IP adreslerin MAC karşılıklarını haritalar.
  - Ağ katmanı, bir çerçeve hazırlanırken ARP'yi kullanır.
- ARP Sorgusu
  - 192.168.0.40 kimdir? 192.168.0.20 cevap verir.
- ARP Cevabı
  - 192.168.0.40 'nin MAC'ı 00:0e:81:10:19:FC
- ARP cache'ları hızlı çalışma için gereklidir.
- Önceki ARP cevaplarını kayıt eder.
- En eski sorgular silinir.

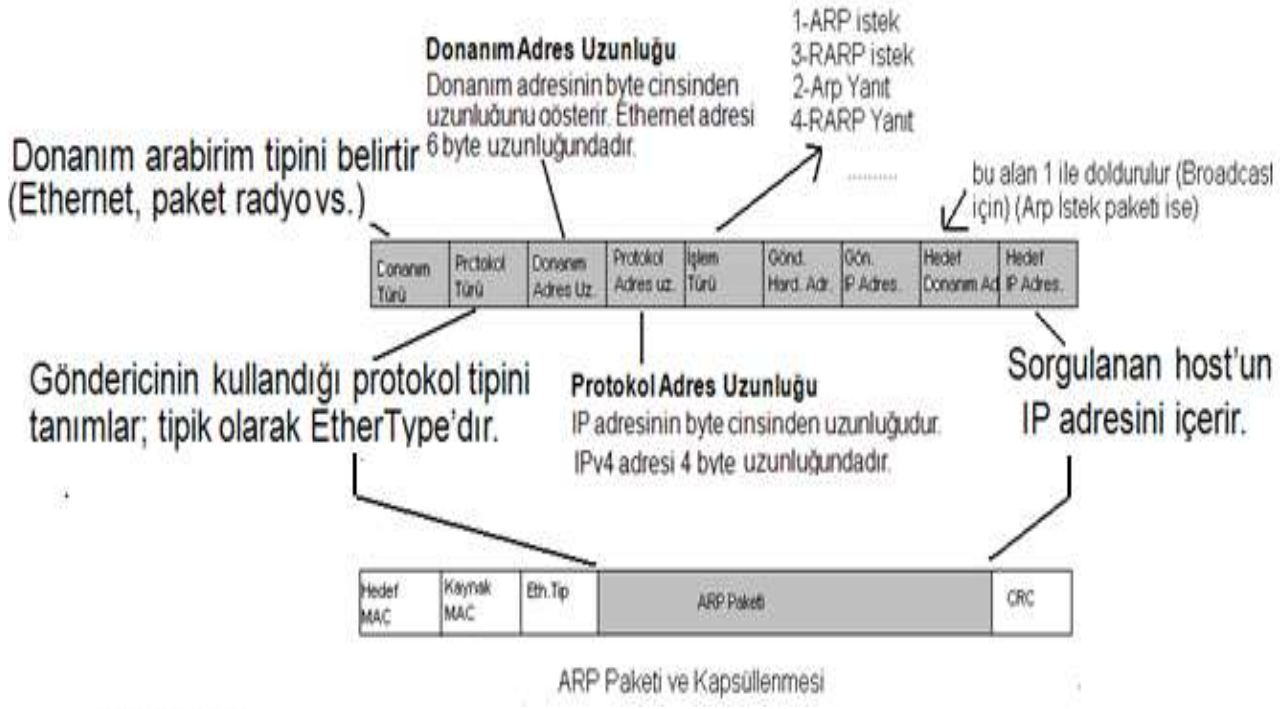
4. Sahte ARP (ARP Spoofing, ARP Poisoning) Atağı

- Normalde ağdaki bir bilgisayar, paket göndereceği başka bir bilgisayarın MAC adresini öğrenmek için anahtara ARP isteği (ARP request) paketi gönderir ve anahtar bu paketi tüm portlarına gönderir. Sadece paketin gönderileceği hedef bilgisayar bu ARP isteğine cevap verir. Paketi gönderen bilgisayar da bu IP – MAC eşleşmesini kendi ARP tablosunda tutar.
- Sahte ARP ataklarında saldırgan, paketin gönderileceği bilgisayarın yerine ARP isteğine cevap verir. Böylece paketi gönderen bilgisayarın ARP tablosunda (IP – MAC eşleşmesi tablosu) saldırgan bilgisayarının IP ve MAC adresleri bulunacaktır. Böylece hedefteki bilgisayar gönderilecek olan paketler saldırganın bilgisayarına gönderilir.
- Saldırgan varsayılan ağ geçidinin (default gateway) yerine ARP isteklerine cevap verecek olursa da, ağdan dışarı çıkacak olan tüm paketler, varsayılan ağ geçidi (default gateway) yerine saldırganın bilgisayarı üzerinden dışarı çıkacaktır. Böylece saldırgan hem ağdan çıkan tüm paketleri dinleyebilecektir hem de bilgisayarının donanım özelliklerine bağlı olarak ağda performans düşüklüğüne sebep olacaktır.

PROTOKOLLAR VE BUNLARA YAPILAN SALDIRILAR

ARP PROTOKOLU VE YÖNELİK SALDIRILAR:

- Adres Çözümleme Protokolü (ARP) Fiziksel (Ethernet MAC) arayüz adresi ile ağ IP adreslerini eşleştirme için kullanılır.
- Veri bağı katmanında Broadcast yayın yoluyla işlem yapar.
- Bu protokolda ençok kullanılan ARP istek (Request) ve ARP Cevap (reply) paketleri'dir.
- Bilinen MAC adresine karşılık gelen IP adresi ise RARP protokolu ile gerçekleşir.
- RARP protokolu daha çok ağa bağlı fakat HARD Diskİ olmayan bilgisayarların ağa dahil olduktan sonra kendi IP No'larnı bulmak için kullanılan protokoldur. (HD'si olan bilgisayarlar kendi IP adreslerini kendi HD'leri üzerinde barındırılar))
- Bunun için ortamda RARP veritabanı tutucu bilgisayarlar olmalıdır.
- RARP protokolu sunucu-istemci etkileşimi ile çalışırlar.



ARP Paketi ve Kapsüllenmesi

ARP İstek ve anıt paketleri

- ARP protokolu IP protokolu altında çalışır. ARP paketleri sadece bulundukları ağ içerisinde yayın yapabilir.
- ARP isteğinden önce, bilgisayarlar kendi ARP tablolarına bakarlar.

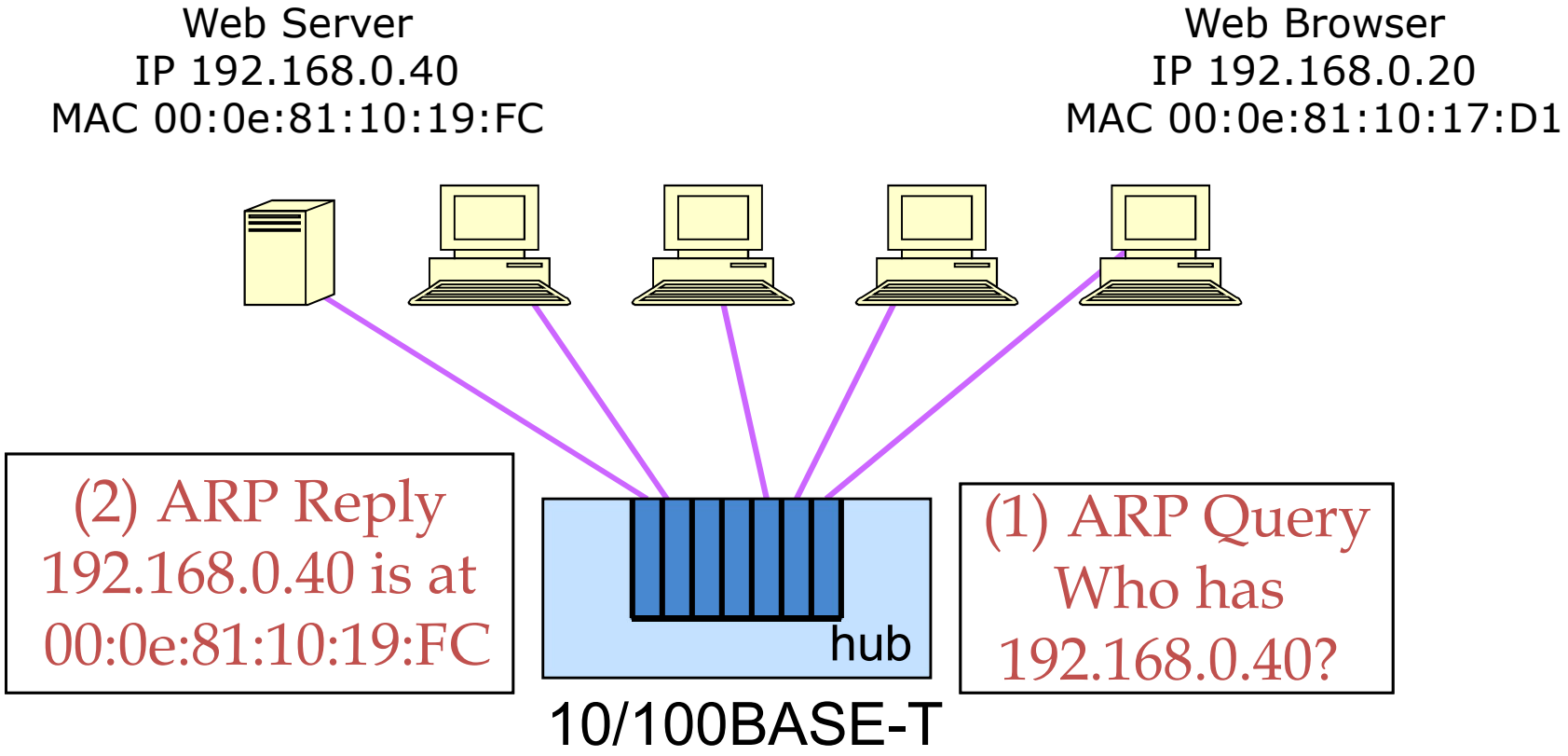
•Bilgisayarlar genellikle ilk açıldıklarında ağa dahil olduktan sonra ARP Broadcast paketi yayınlarlar: Niçin?

-Aynı ağ içerisindeki IPV4 IP çakışmalarını belirlemek için.
-Başka bilgisayarlardaki ARP tablolarının güncellenmesi için

ARP Sorgusu & ARP Cevabı

ARP tablosunu görmek için bilgisayarınızda "arp –a" komutu kullanılabilirsiniz.

```
C:\> arp -a
Arabirim: 192.168.1.70 --- 0x4
Internet Adresi      Fiziksel Adres          Tipi
192.168.1.1          00-02-xx-yy-ad-15       dinamik
192.168.1.253        00-0c-tt-zz-6b-5d       dinamik
```



ARP Güvenlik kusurları

ARP protokolunun işleyişi ve tasarım mekanizmasından dolayı önemli kusurlardan bazıları;

- ARP önbellekleri kapasitesinin sınırlı oluşu.
  ARP önbellekleri bir şekilde lüzumsuz olarak doldurulabilir.
- ARP Kimlik Doğrulama eksikliği
  - ARP cevapları, genellikle kabul edilen ve alınanın kim olduğu fazla önemsenmeden önbelleğe alınır.
  - Meşru ve gayri meşru mesajları ayırt etmek için hiçbir yöntem yoktur.

Kimlik doğrulama eksikliğinden dolayı;

- Geçersiz ARP cevapları: Bir ARP sorgusuna ki bu bir broadcast yayındır. Alakasız kimseler cevap verebilir. Bu durumda sorgulanan IP'ye ilgisiz kişiler kendisini eşleştirebilir.
- Karşılıksız - Sebepsiz (Gratuitous) ARP cevapları:
  Sorgu olmadan, saldırganın yönlendireceği ağın eşleştirilmesini sağlayan ARP cevaplarının ön belleğe yazılabilir olması.

ARP Güvenlik Açıkları

- ARP spoofing (ARP Kimlik Sahtekarlığı- ARP taklidi)
  - Sebepsiz, nedensiz ARP işlemleri.
  - Orijini doğrulanmayan ARP yanıtları.
  - Kötü niyetli bir cihaz herhangi bir MAC adresini talep edebilir.

ARP Saldırıları

- ARP önbelleklerindeki mevcut adreslerin değiştirilmesi (ARP tablosunda IP-MAC eşleşmesinin değiştirilmesiyle)

ARP sahtekarlığı (ARP spoofing, ARP flooding, ARP poisoning) saldırısı lokal ağlarda gerçekleştirilebilen bir saldırıdır.Bu saldırı, üç şekilde gerçekleştirilmektedir:

–Birincisi; hedef bilgisayarın ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilgisayarın göndereceği paketlerin saldırganın istediği adreslere gitmesini sağlamak.

–İkincisi; hedef bilgisayarın göndereceği tüm paketlerin, saldırganın bilgisayarı üzerinden geçmesini sağlamak **(Man in the Middle).**

–Üçüncüsü de; hedef bilgisayarın, paketlerini bir başka bilgisayara göndermesini sağlayarak bu bilgisayara servis dışı bırakma **(Denial of Service)** saldırısı yapmak şeklindedir.

ARP Saldırıları

- ARP Önbelleğinin aşırı kalabalık olması
  - Bazı uygulamalardaki hedef, çok sayıda gereksiz ARP yanıtları gönderilerek ARP belleğinin doldurulmasıdır.
    - Bu durumda önbellek maksimuma erişir. Switchler ya HUB gibi çalışır. Veya tekrardan öğrenme moduna girer.

Paketlerin Monitor edilmesi (Sniffing)

- HUB'lar bir portundan gelen paketleri diğer paketlere broadcast yaparlar. Bunun anlamı aynı Hub'ı paylaşan bilgisayarların paketleri monitor etmesine sebep olur.
- Switch'ler ise gelen paketin ***"Hedef MAC adresini"*** inceleyerek o paketi yalnızca ilgili porta yönlendirirler. Bu iş için oluşturdukları ***"MAC Adresi-Port no***' tablolarını kullanırlar.
- Switch kullanılan ağlarda, bu sayede bilgisayarların biribirlerine giden paketleri monitor etme olasılığı bir ölçüde önlenebilir.
- Switchler her ne kadar dinlenmemek üzere tasarlansa da değişik yöntemlerle bu durum aşılabilir.
- Gelişmiş switchler'de (kontrol edilebilir SWitch'ler) bu dinlenme problemi aşılabilir.

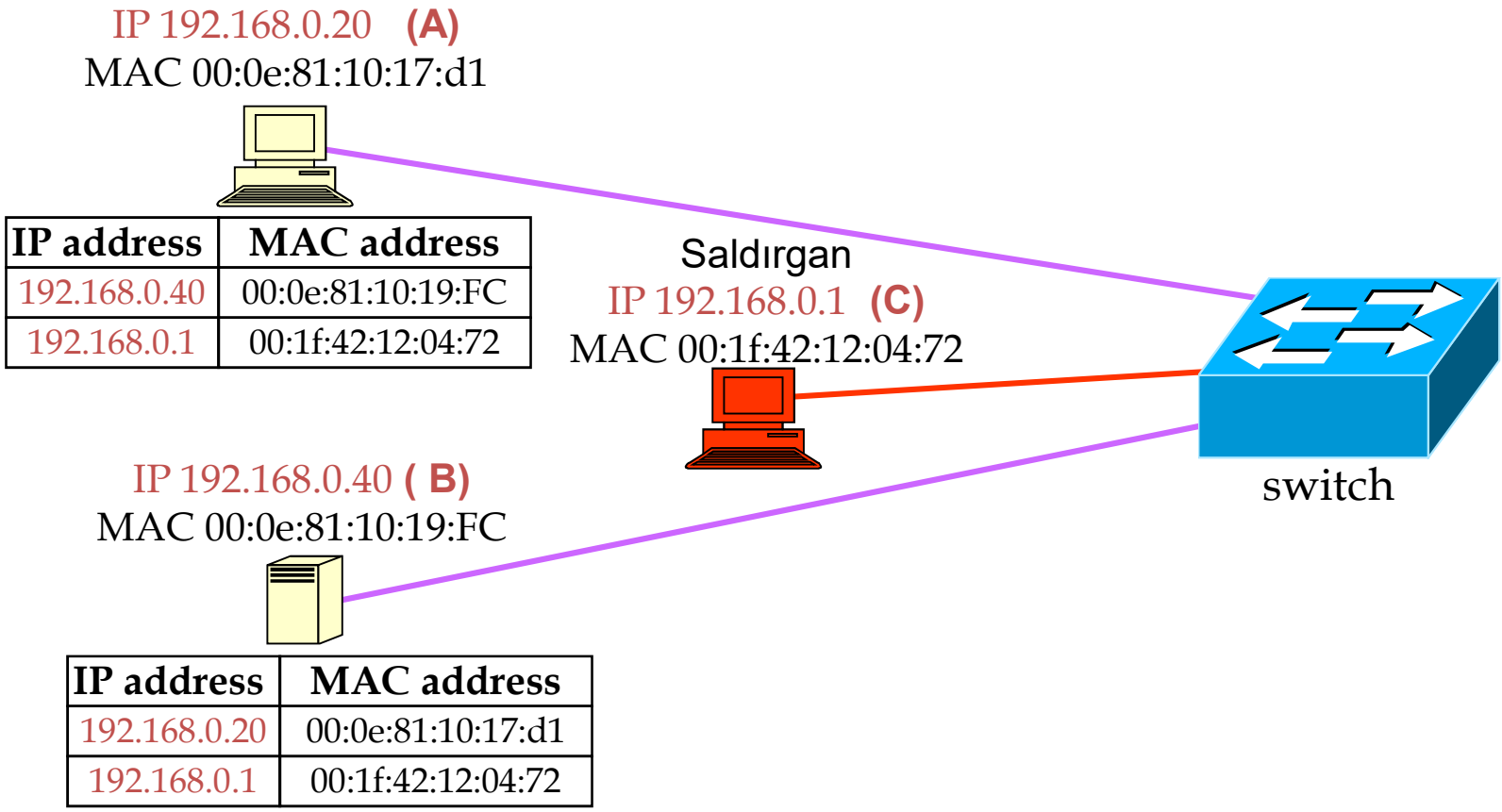
Paketlerin Monitor edilmesi (Sniffing)-II

- Gelişmiş olmayan switchler'in dinlenmesi için değişik yöntemler uygulanır. Bunlardan en önemlisi ARP Tablo(önbellek) zehirlenmesidir.
- ARP Tablo Zehirlenmesi (ARP SPOOFİNG – Cache Poisoning) : Bu yöntem, Ortadaki Sessiz Adam - Man in the Middle- saldırısı şeklinde etkisini gösterir.
- Saldıgan haberleşen iki bilgisayar arasına kendisini yerleştirerek bir köprü gibi veri akışının kendisi üzerinden sağlanmasını sağlar. Böylece gelen paketleri okuyan saldırgan paketleri iki makine arasında yönlendirir. Ortadaki adam ile DNS zehirlenmesi de yapılır.

- **Man-in-the-Middle Saldırıları:** Bu tür saldırılarda saldırgan kurban ile kurbanın gitmek istediği hedef noktası arasına girerek bütün iletişimi istediği gibi kontrol eder. Bu saldırılar birçok değişik şekilde karşımıza çıkabilir.(ARP Zehirlenmesi, DNS Ön Bellek Zehirlenmesi vb.)

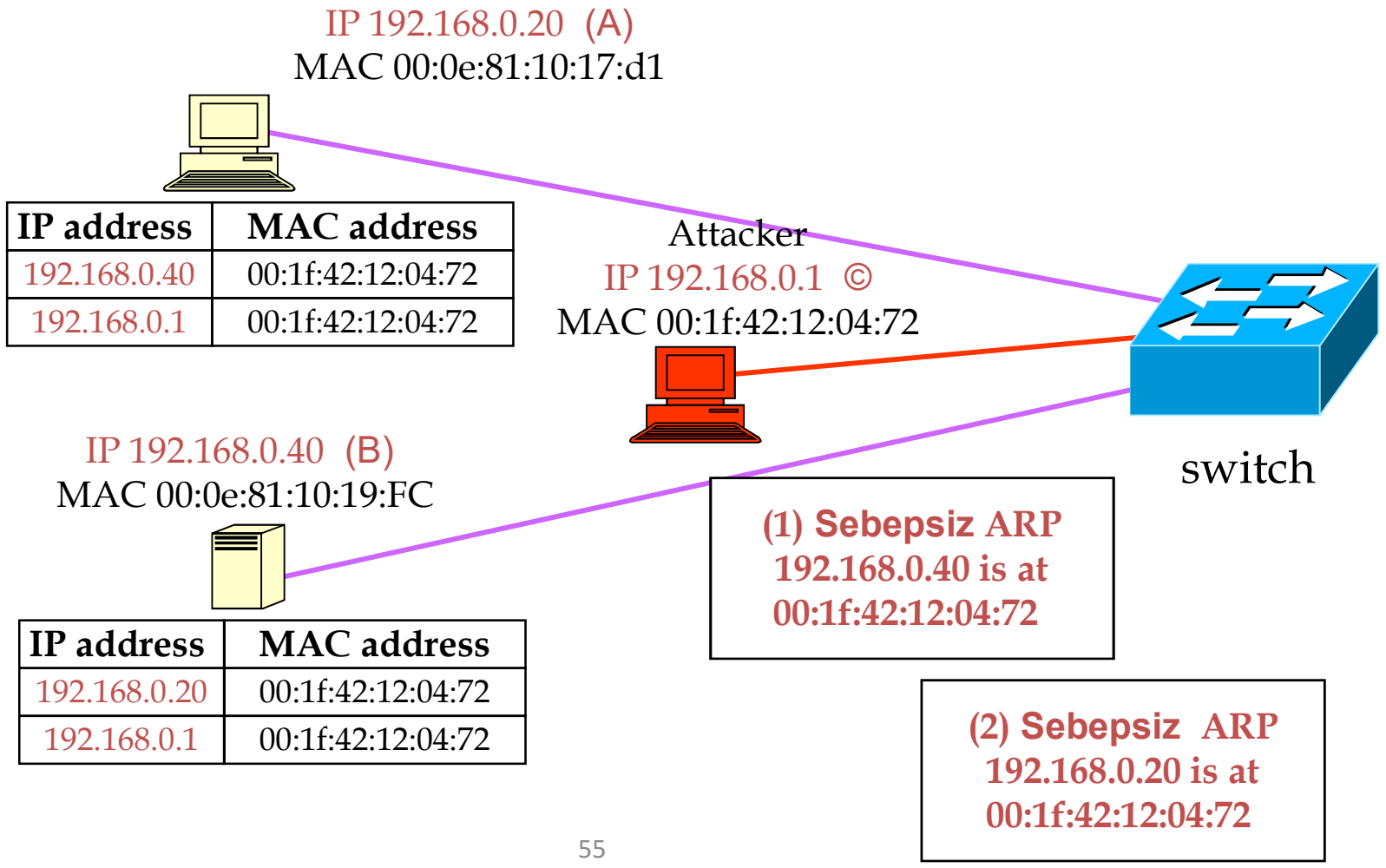
ARP Tablo Zehirlenmesinden (ARP Spoofing) önce

Bağlantı yapan iki makine A, B olsun. C Saldırgan olsun. Makinaların IP-MAC adres ikililerini değiştirmek amacıyla C Taklit edilmiş ARP Yanıt paketi gönderir.



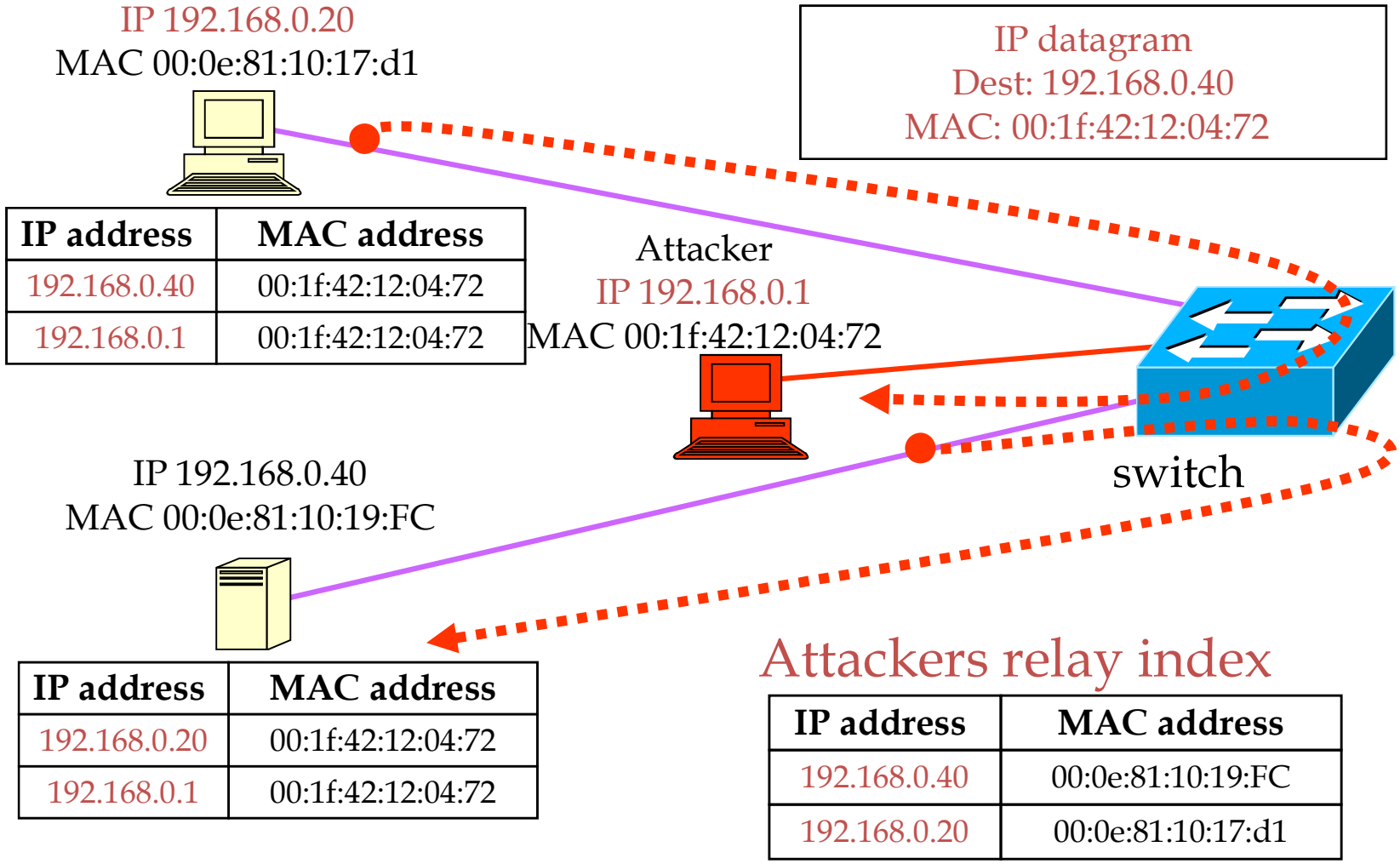
ARP Spoofing'den sonra

Bağlantı yapan iki makine A, B olsun. C Saldırgan olsun. Makinaların IP-MAC adres ikililerini değiştirmek amacıyla C Taklit edilmiş ARP Yanıt paketi gönderir (Sebepsiz ARP).



ARP Spoofing'in Etkisi (Ortadaki Adam etkisi)

Her iki bilgisayar arasındaki veriler, artık saldırgan üzerinden olacağından, saldırgan veriler üzerinde oynayabilir. Hatta haberleşen iki bilgisayar



IP address	MAC address
192.168.0.40	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

IP address	MAC address
192.168.0.20	00:1f:42:12:04:72
192.168.0.1	00:1f:42:12:04:72

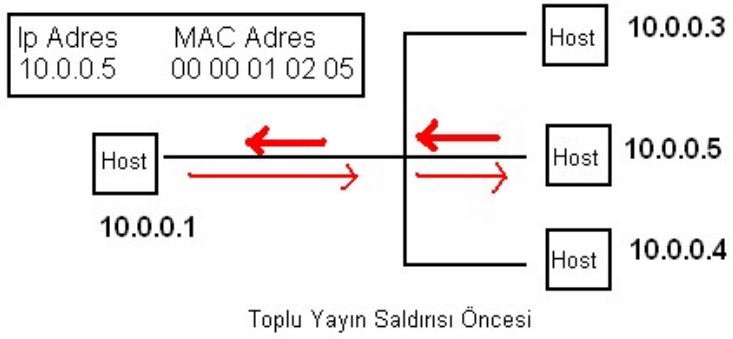
Attackers relay index

IP address	MAC address
192.168.0.40	00:0e:81:10:19:FC
192.168.0.20	00:0e:81:10:17:d1

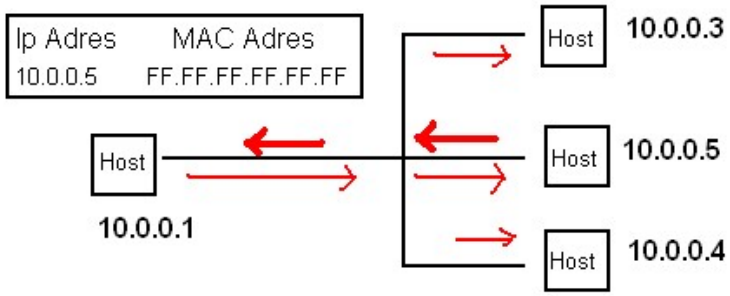
- Ortadaki adam etkisi ile iki bilgisayarın biribirleriyle haberleşmesi sürecinin saldırganın bilgisayarından geçmesi durumunda, bu iki bilgisayar arasındaki kurulacak üst seviye işlemlerinin de , örneğin *“Bağlantıya yönelik saldırı*” ele geçirilmesi söz konusudur. Bu işlem iki makine arasındaki iletişimde TCP katmanında bağlantı sıra numarasını kullanarak bağlantı içerisine veri gönderebilir.

Toplu yayın (Broadcast) Saldırısı

- Eğer ARP tablosu içerisindeki belirli bir IP adresine karşılık gelen MAC adresi, ARP spoofing (taklit ARP yanıtı) mesajı yoluyla değiştirilip FF.FF.FF.FF.FF.FF ile değiştirilirse, bu bilgisayara gönderilecek paketler tüm noktalar tarafından monitör edilebilir okunabilir.
- Eğer bir bilgisayarın ARP tablosunun içindeki ağ geçidinin IP'sine karşıkıl gelen MAC adresi toplu yayın adresi olarak değiştirilirse, **bu bilgisayarın dış dünya ile olan bağlantısı** rahatlıkla izlenebilir.

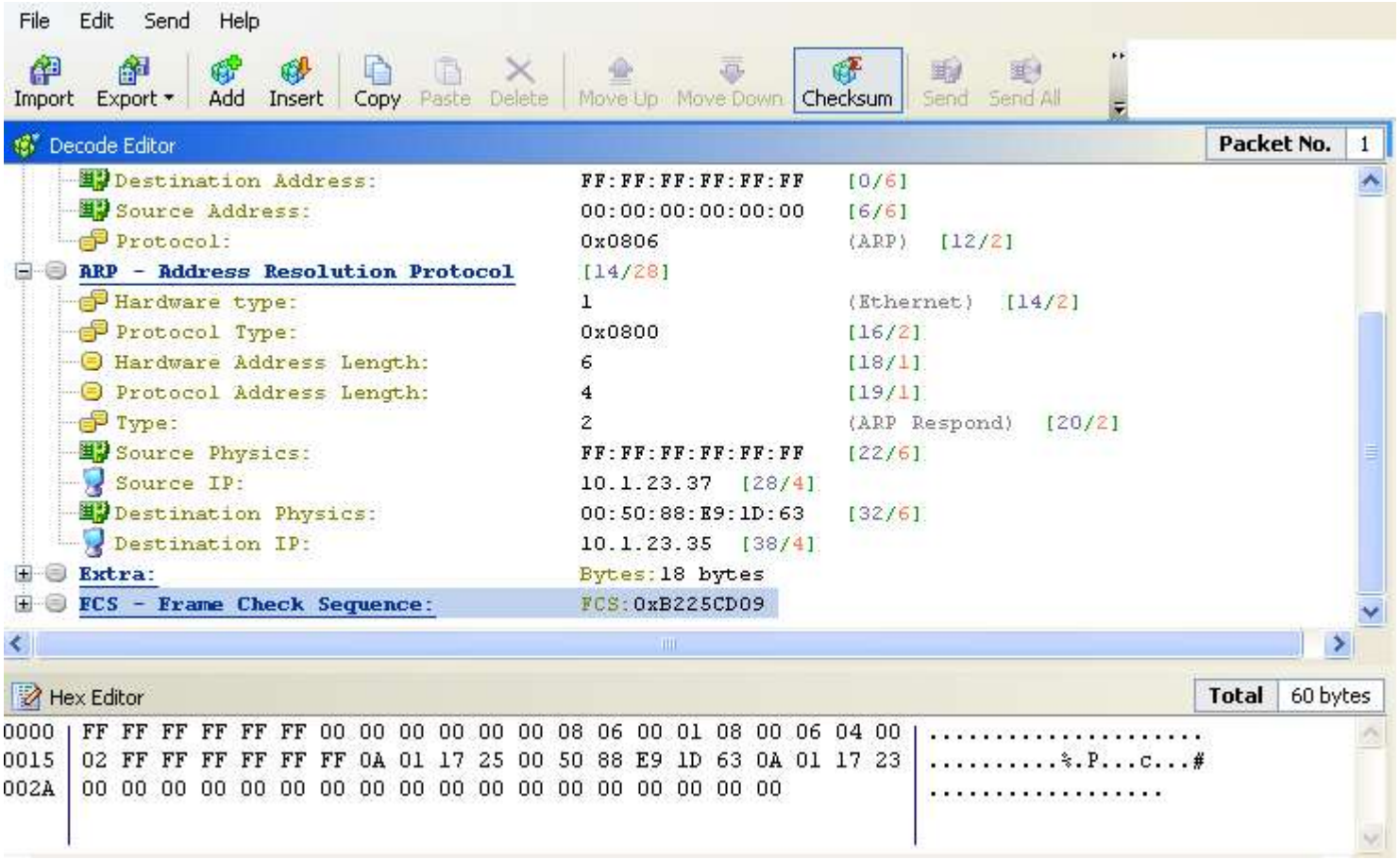


Toplu Yayın Saldırısı Öncesi



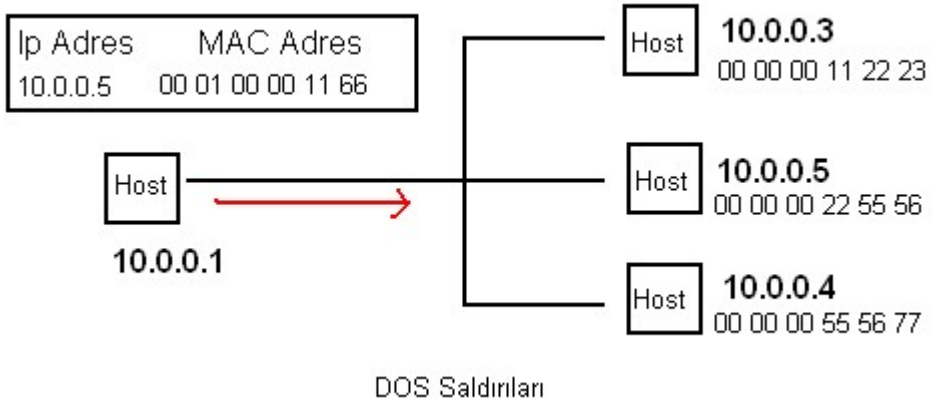
Toplu Yayın Saldırısı Sonrası

TAKLİT ARP REPLY PAKETİ OLUŞTURMAK



ARP PROTOKOLU İLE DOS Saldırıları

- Taklit edilmiş “ARP yanıt Paketi” kullanarak tablo içerisinde varolmayan MAC adresi değerlerine karşılık gelen IP adrteslerine sahip olan girdiler yapılır. Böylelikle tablo içerisinde yer alan IP adresine gönderilecek datagramlar hedeflerine varamaz. Bu durum ağı meşgul eder hem de MAC adresi değiştirilmiş bilgisayarla olan iletişim sonlandırılmış olur.



DOS Saldırıları

ARP SALDIRILARINA KARŞI ÖNLEMLER

Eski bir protokol olan ARP'ın çalışma yapısından *(Tablosunun düşük kapasiteli olması, ARP mesajları için herhangi bir durum tablosunun tutulmaması, ARP'ta herhangi bir kimlik doğrulama mekanizması olmadığı için, bilgisayar gelen ARP mesajlarının doğru bilgisayardan gelip-gelmediği kontrol edemeyecektir. Tüm bilgisayarlar kendisine gelen ARP mesajlarıyla ARP tablosunu herhangi bir kontrole tabi tutmadan güncellemek durumundadır v.b)* kaynaklanan bu sorunların protokol bazında bir çözümü bulunmamaktadır.

- Alınacak tedbirlerden ilki ARP tabloları içerisine statik girdiler yaratmaktır. Bu statik değerler saldırı sonucunda değişmeyeceği için belirli bir düzeyde güvenlik sağlanmış olur. Ancak bu yöntem ağdaki tüm bilgisayarların ARP tablolarına manuel olarak " IP-MAC adresi" tanımlaması yapmaktır. Mantıklı değildir. Kaldı ki Windows işletim sistemi, ARP tablosu içerisindeki statik eşleşmeleri kabul etmeyebilir. Aldığı Yanıt paketleri ile tabloyu değiştirebilir.

ARP SALDIRILARINA KARŞI ÖNLEMLER-2

- ARP' nin açıklarından yararlanılarak yapılan saldırıları SWİTCH cihazları üzerinde alınacak bazı önlemlerle kapatmak mümkündür.

Çözüm -1

- Switch'lerin IP adresi – MAC adresi eşleşmelerini (ARP tablosu) port bazında tutmalarıdır. (Bu işlem gelişmiş yapıda switch'ler üzerinde gerçekleştirilebilir (VLAN özellikli switchler v.b) . Bu durumda SWİTCH, üzerinden akan ARP paketlerini sürekli olarak denetler. Geçerli veya taklit paketleri bulur. Buna "Dynamic ARP Inspection **(DAI) –Değişken ARP denetimi-**, Dynamic ARP Protection"denir. CİSCO Catalyst 4500 serisi Switch'de bu özellik vardır.
- Switch üzerinde port bazındaki IP adresi – MAC adresi eşleştirmesi yapıldığından, saldırgan bağlı olduğu switch portundan farklı IP adresi – MAC adresi eşleşmelerine sahip olan ARP mesajları gönderemez.
- Bu yöntem DHCP sunuculu sistemlerde uygulanır.
- DAI MAC adresi-IP adresi eşleşmelerini sürekli takip ederek *"Ortadaki Adam"* saldırılarının önlenmesine yardım eder.

Çözüm – 2:

- Bir DHCP sunucusunun bulunmadığı bir ortamda (IP adreslerinin statik olduğu) IP adresi – MAC adresi eşleşmelerinin anahtarlama cihazları üzerinde el ile birer birer yapılması gerekmektedir. Yani DHCP sunucusundan hazır olarak alınan IP adresi – MAC adresi eşleştirmelerinin switch'e el ile girilmesi gerekmektedir. Bunun için anahtarlama cihazları üzerinde ARP erişim kontrol listeleri (ARP access control lists - ARP ACLs) tanımlanır.

Çözüm – 3:

- Saldırı için bir başka çözüm de, anahtarlama cihazının portlarına birim zamanda gelen ARP mesajlarını sınırlamaktır. Bu şekilde, ARP servis dışı bırakma saldırılarının da (ARP DoS) önüne geçilmiş olunur. Bu özellik, sadece Cisco marka anahtarların bazı modellerinde aktif hale getirilebilmektedir.