SAKARYA ÜNİVERSİTESİ

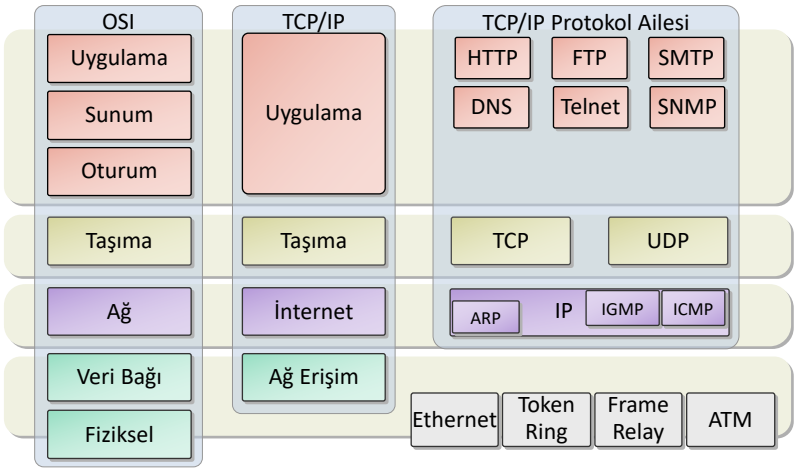
SİBER GÜVENLİĞE GİRİŞ

TCP/IP GÜVENLİĞİ

Prof. Dr. İbrahim ÖZÇELİK
Bilgisayar ve Bilişim Bilimleri Fakültesi

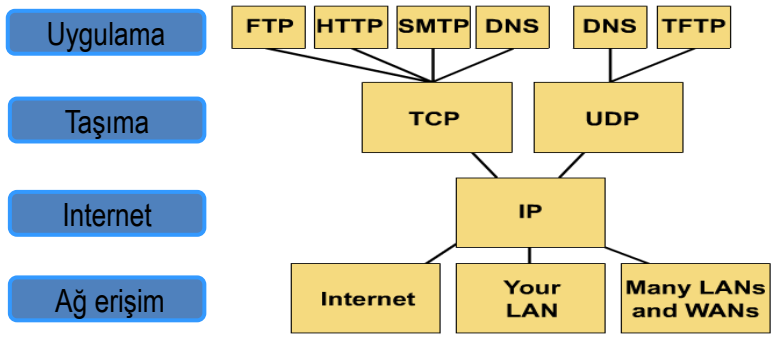
1

OSI ve TCP/IP Mimarisi



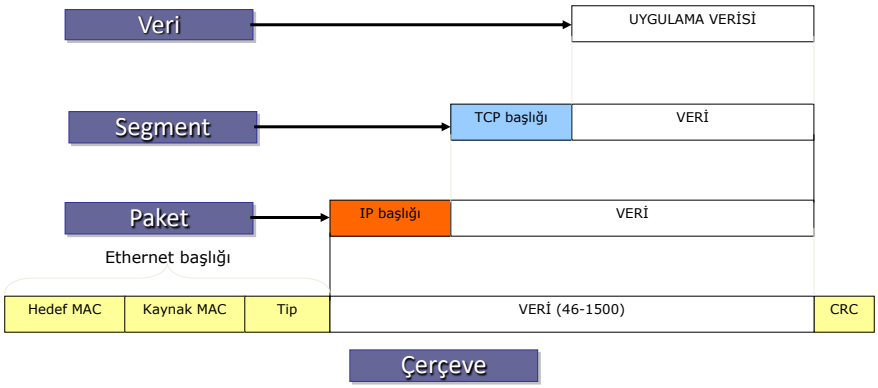
2

TCP/IP Protokol Mimarisi ve İşleyişi



3

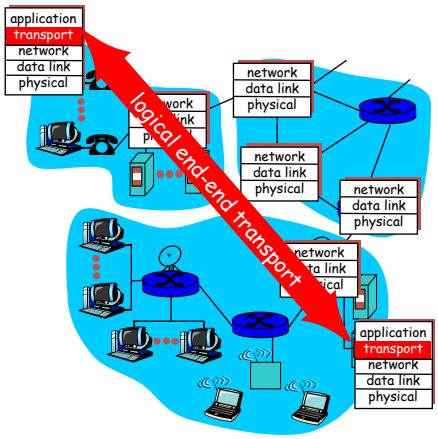
Katmanların Uygulama Verisiyle İlişkisi



4

Taşıma Katmanı Hizmetleri

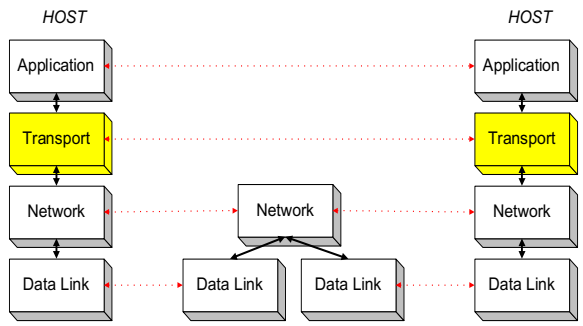
- Farklı düğümler üzerinde çalışan uygulama prosesleri arasında mantıksal bir iletişim destekler
- Taşıma protokolleri uç sistemler içerisinde çalışır
  - Gönderici tarafı: uygulama mesajlarını segmentler içerisine kapsüller ve ağ katmanına aktarır
  - Alıcı tarafı: segmentleri mesajlar haline dönüştürür ve uygulama katmanına aktarır

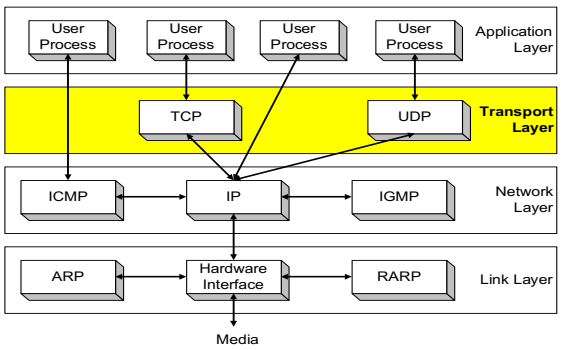


5

Taşıma Katman Protokolleri

- Uygulamalar için birden fazla taşıma katman protokolü mevcuttur. TCP ve UDP
- Taşıma katman protokolleri uçtan-uca çalışan protokollerdir
- Sadece düğümlerde gerçeklenir

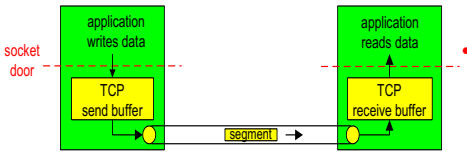




6

TCP Servisleri

- point-to-point:
  - Bir gönderici, bir alıcı
- reliable, in-order *byte stream:*
- pipelined:
  - Pencere açıklığı (windows size), TCP tıkanıklık ve akış kontrolü tarafından belirlenir
- *send & receive buffers*

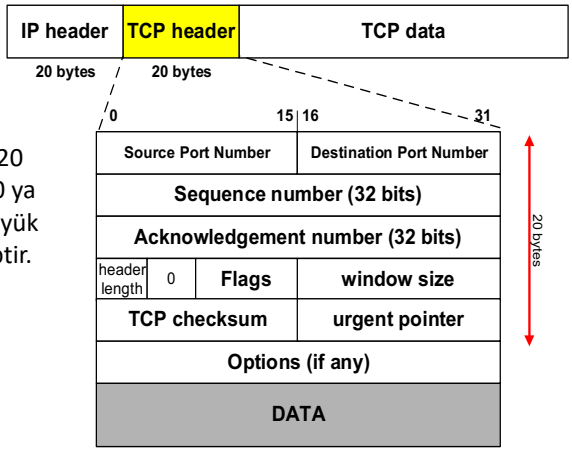


- full duplex data:
  - Aynı bağlantı üzerinden iki yönlü veri akışı
  - MSS: maximum segment size
- connection-oriented:
  - handshaking (kontrol mesajlarının alış verişi), veri değişiminden önce alıcı durumu
- flow controlled:
  - Gönderici alıcıya fazla yüklenmeyecektir

7

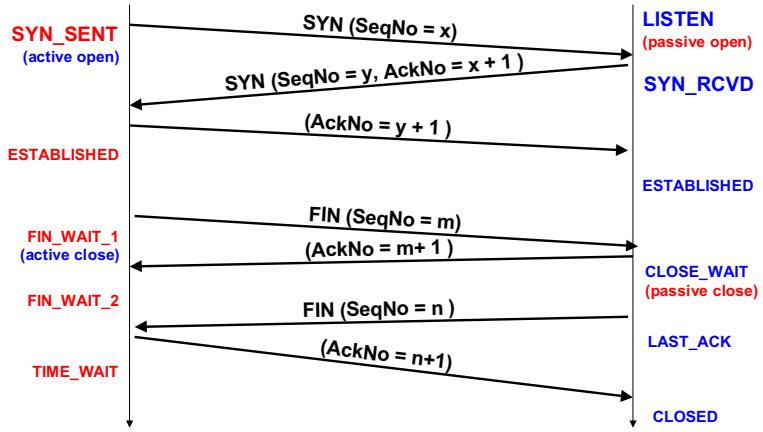
TCP Başlığı ve Segmenti

TCP segmentleri 20 baytlık başlık ve 0 ya da 0'dan daha büyük veri alanına sahiptir.



8

Bağlantı Süresince TCP Durumları



9

Akış/Tıkanıklık/Hata Kontrolü

- Akış (Flow) Control: Göndericinin alıcıyı fazla çalıştırmasını (overrun) önlemek için kullanılan kontroldür
- Error Control: Paket kayıplarından dolayı oluşan etkileri engellemek ya da düzeltmek için kullanılan kontroldür
- Tıkanıklık (Congestion) Control: Göndericinin ağı fazla yüklemesini önlemek için kullanılan kontroldür

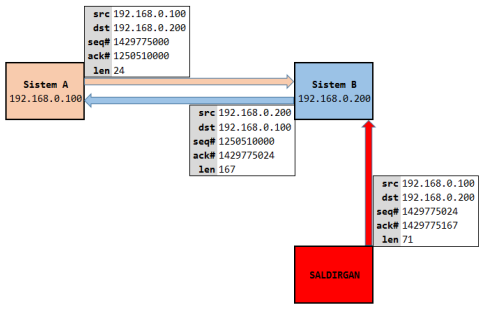
→ Her bir kontrol mekanizmasının amacı farklıdır.

→ Fakat gerçekleme birleştirilmiştir.

10

Katman4 – Sıra Tahmini ve Oturum Çalma

- Sahte IP adresi ile TCP üçlü el sıkışmasının tamamlanması için TCP başlığındaki 32 bit sıra numarası (ISN) tahmin edilebilir olmalı
  - Günümüz işletim sistemlerinin hemen hepsinde bu değer yeteri kadar rastgele olacak şekilde üretilmektedir.



11

Katman 4: Desenkronizasyon

- Geçerli bir bağlantıya RST ve FIN bayraklı paketler gönderilir ve oturum sonlandırılır.
- Eğer kaynak IP sahte ve ACK numarası doğru ise alıcı bunun doğru bir istek olduğunu düşünerek bağlantıyı yeniden başlatır

12

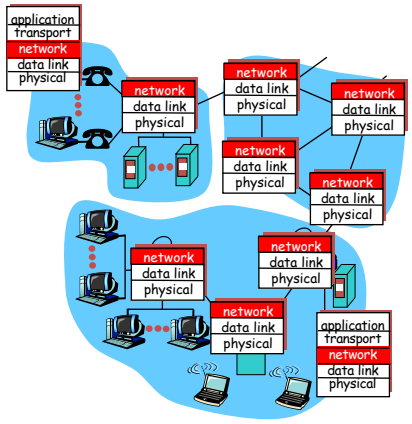
Katman 4: Flood Saldırıları

- SYN Flood / FIN Flood / TCP Connection Flood saldırıları gerçekleştirme
  - #hping3 –S –p 80 www.google.com –c 5
  - #hping3 –F –p 80 www.google.com –c 5

13

Ağ Katmanı

- Bir segmenti göndericiden alıcı düğüme taşır
- Gönderici tarafta segmentler datagramların içine yerleştirilir (kapsüllenir)
- Alıcı tarafta segmentler taşıma katmanına teslim edilir
- Her düğüm ve yönlendirici içerisinde ağ katman protokolleri mevcuttur
- Yönlendirici kendisine gelen tüm IP datagramların içerisindeki başlık alanlarını kontrol eder



14

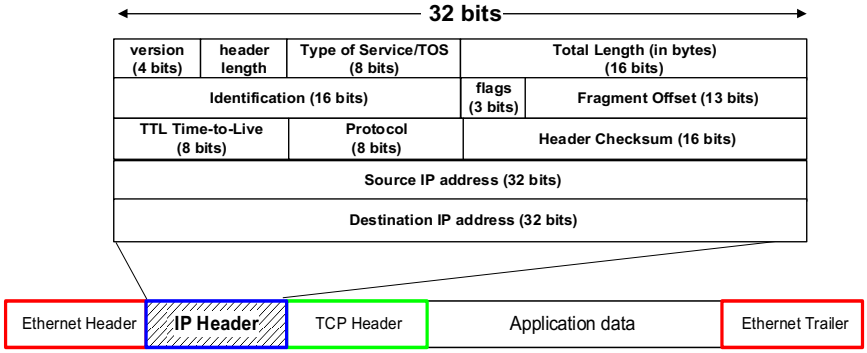
IP Hizmetleri

- IP'nin teslim hizmeti minimum özelliklere sahiptir
- IP *güvenilir olmayan bağlantısız en iyi eforlu* bir hizmet yapısını destekler (aynı zamanda datagram hizmeti olarak da isimlendirilir).
  - **Güvenilir olmayan (Unreliable):** IP kaybolan paketleri kurtarmak için bir teşebbüste bulunmaz
  - **Bağlantısız (Connectionless):** Her bir paket (datagram) bağımsız olarak ele alınır . IP düğümler arasındaki paketlerin mantıksal bir dizi içerisinde gönderildiğinden habersizdir
  - **En iyi eforlu (Best effort):** IP, bu hizmet üzerinde herhangi bir şeyi garanti etmez (verim, gecikme, vb) . Bundan dolayı IP tarafından gönderilen paketler kaybolabilir, sıradışı varabilir veya iki kez ulaşmış da olabilir.
- Sonuçlar:
  - Üst katman protokolleri, paketlerin kaybolması ve tekrar gönderilmesi ile ilgilenmek zorundadır
  - Paketler sıradışı bir şekilde teslim edilebilir

15

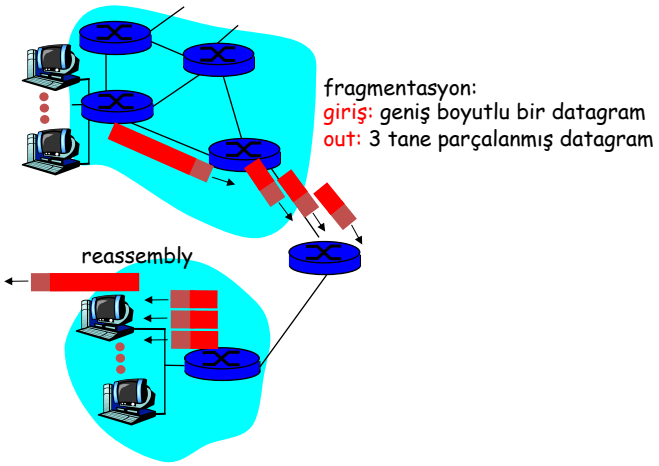
IP Datagram ve Başlığı

- Bir IP ağı içerisindeki transfer edilen birim = IP datagram.
- Bir IP başlığı ve verisi üst katman protokolleri ile ilgilidir
- IP datagram başlığı minimum 20 bayt uzunluğa sahiptir



16

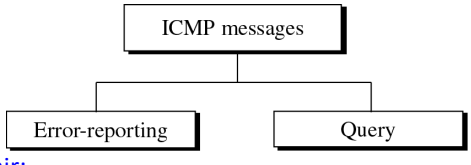
IP Fragmantasyon ve Birleştirme



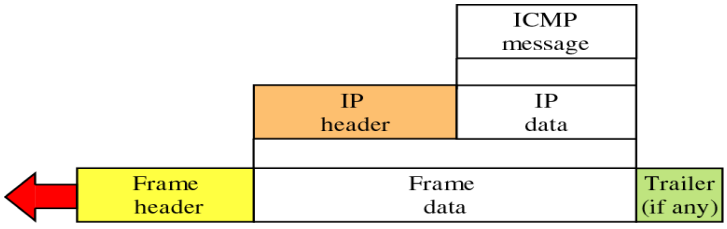
17

ICMP Mesajları

- **Internet Control Message Protocol (ICMP)**, IP protokolünü hata raporlama ve basit sorgular noktasında destekleyen yardımcı bir protokoldür.

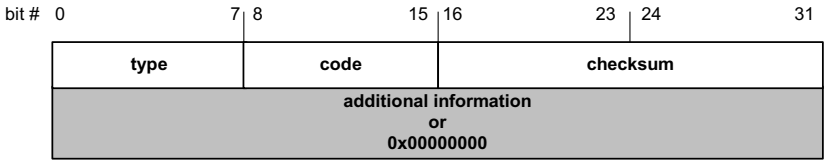


- ICMP mesajları IP datagramları olarak kapsüllenir:



18

ICMP Mesaj Formatı

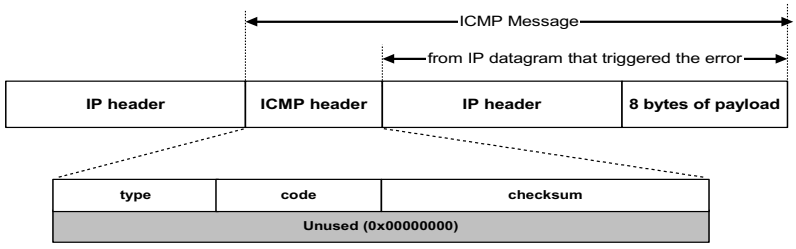


4 bayt başlık:

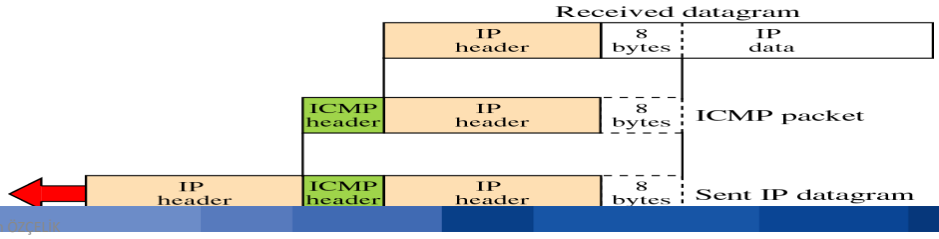
- Type (1 bayt): ICMP mesaj tipini tanımlar
- Code (1 byte): İlgili ICMP mesaj tipi tarafından rapor edilen datagram için hata kodunu içerir. Yorumlama mesaj tipine bağlı olarak değişebilir - ICMP mesajının alttipi de olabilir
- Kontrol Toplamı (Checksum - 2 bayt): IP başlığındaki kontrol toplamına benzerdir. Chechsum tüm ICMP mesajı üzerinden hesaplanır.
- Eğer ek bir veri yoksa, 4 bayt sıfır değerine sahiptir. ICMP mesajlarının her biri birbirinden bağımsız bir şekilde tanımlanır ve en az 8 bayt uzunluğundadır

19

ICMP Hata Mesajı



- ICMP hata mesajları IP başlığının tamamını ve veri alanının da (tipik olarak UDP, TCP) ilk 8 baytını içerir.



20

Örnek ICMP Hata Mesajları

Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
4	0	Source quench	Send many to an important host, and a sufficient slowdown may be close to a denial of service
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

21

Katman 3 – IP Spoofing

- İstenilen IP adresinden TCP/IP paketleri (TCP, UDP, IP, ICMP, HTTP, SMTP, DNS vb.) gönderebilme işlemi
- DDoS saldırılarında kullanılır
  - Syn ve Syn+Ack bayrağı set edilmiş paketler üretilecektir.
    - # hping3 -p 80 -S www.google.com
  - yahoo.com adresinden www.google.com adresine gidiyormuş gibi syn paketleri üretecektir. Syn+ack paketleri yahoo'ya gidecektir.
    - # hping3 -a www.yahoo.com -p 80 -S -c 4 www.google.com
  - Kendi ip adresinin de bulunduğu rasgele IP adreslerinden UDP paketleri gönderecektir.
    - # hping3 --udp 8.8.8.8 --rand-source –flood
- Port taramalarında da kullanılır
  - Nmap –D <IPadresi> www.google.com

22

Katman 3 – IP Fragmantasyon Saldırıları

- IDS/IPS ve WAF atlatmada kullanılabilir
  - #fragroute –f /etc/fragroute.conf <IPadresi>
  - /etc/passwd → fragroute → No1: /et, No2: c, No3: /pass No4: wd
- Port taramada kullanılabilir
  - #nmap –f <IPadresi>
  - #nmap --mtu 320 <IPadresi>

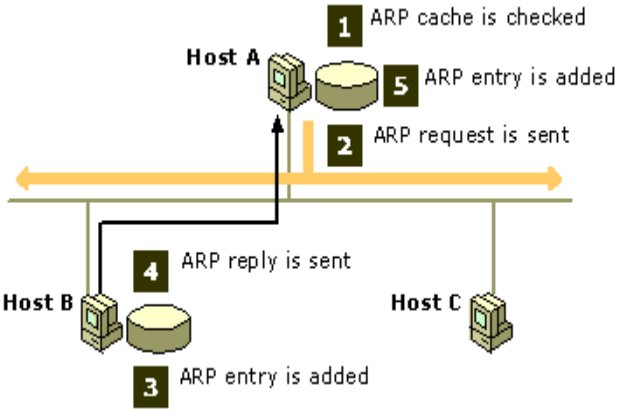
23

Katman 3 – ICMP Saldırıları

- ICMP Redirect mesajları ile MITM atakları (yönlendirme tablosu kaydı değiştirme)
  - Linux sistemlerde ICMP redirect mesajlarının kabul edilmemesi için /etc/sysctl.conf dosyası içerisine net.ipv4.conf.all.accept_redirects = 0
- ICMP mesajları ile işletim sistemi tespiti
  - Her işletim sistemi ICMP mesajlarına farklı cevaplar verir.
- Hedef ve kaynak bilgisayarlara ICMP time exceeded veya destination unreachable paketleri göndererek TCP bağlantısının koparılması
- Smurf Attack: Sahte kaynak adresine sahip ICMP 8-0 paketleri Broadcast adresine gönderilir. Cevaplar sahteIPadresine dönecektir.
  - #hping3 --icmp --flood –a <sahteIPadresi> <subnetbroadcastIPadresi-x.x.255.255>

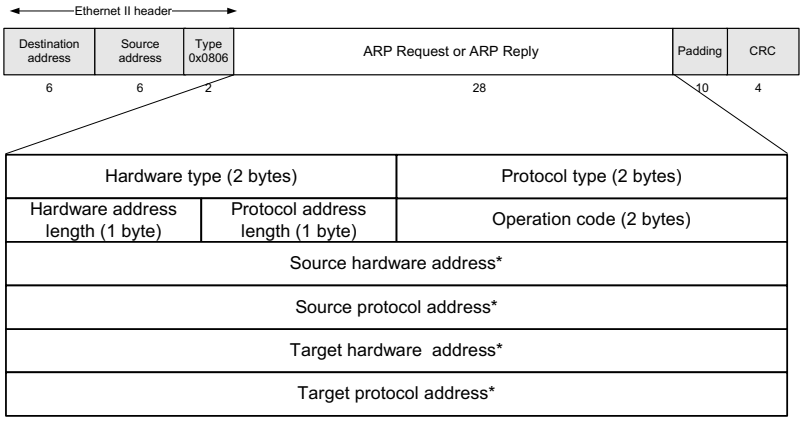
24

Yerel Trafik İçin ARP Çözümlemesi



25

ARP Paket Formatı



* Note: The length of the address fields is determined by the corresponding address length fields

26

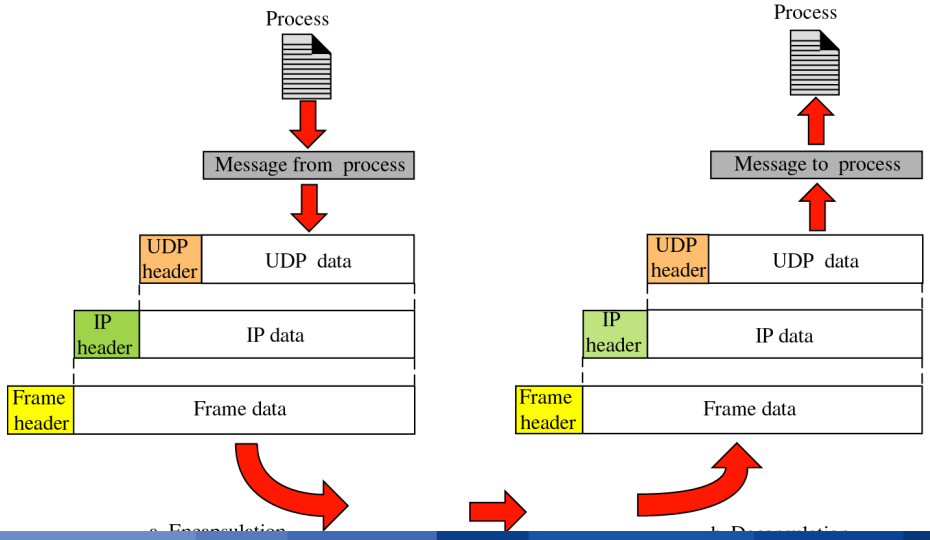
Ethernet II (DIX) ve IEEE 802.3 Çerçeveleri

IEEE 802.3						
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimeter	Destination Address	Source Address	Length Type	Data	Frame Check Sequence

Ethernet II					
8	6	6	2	46 to 1500	4
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

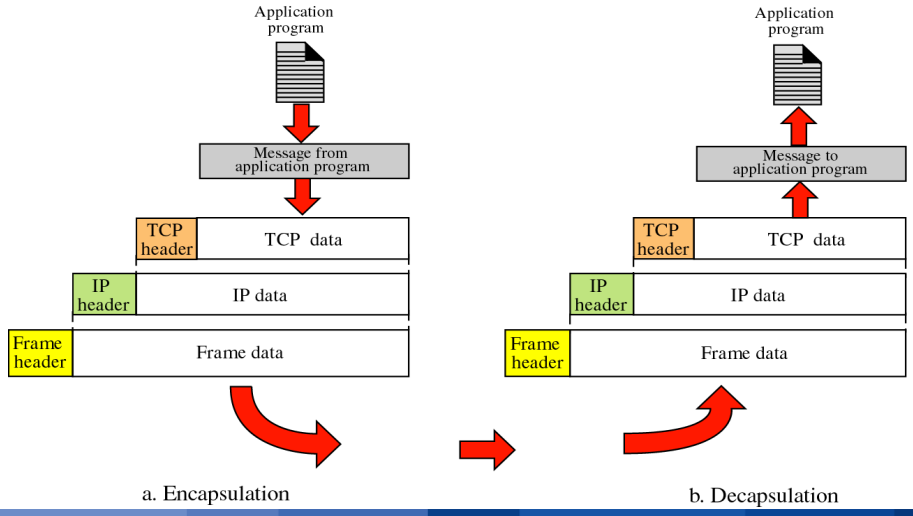
27

UDP Encapsulation / Decapsulation



28

TCP Encapsulation / Decapsulation



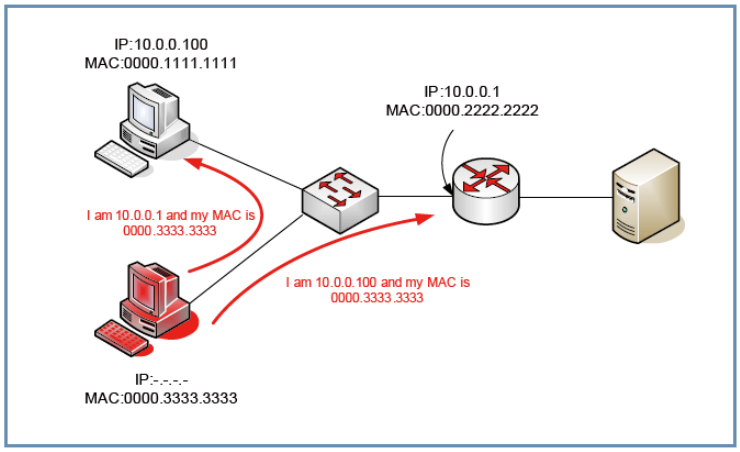
29

Katman2 Saldırı ve Güvenlik

1	ARP	Gratutious ARP ARP Atakları
2	VLAN	Anahtar Kandırma Çift Etiketleme VTP Atağı
3	Port Güvenliği	Çeşitli saldırılara karşı L2 önlemleri
4	MACSec	L2 şifreleme

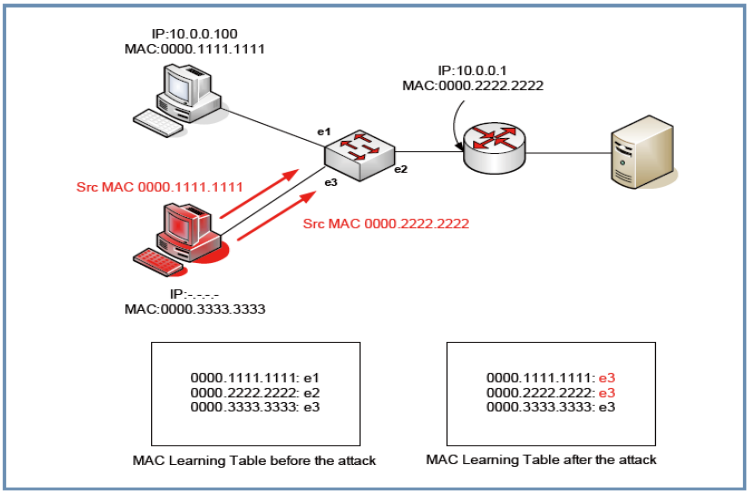
30

ARP Spoofing (ARP Cache Poisoning)



31

MAC Flooding



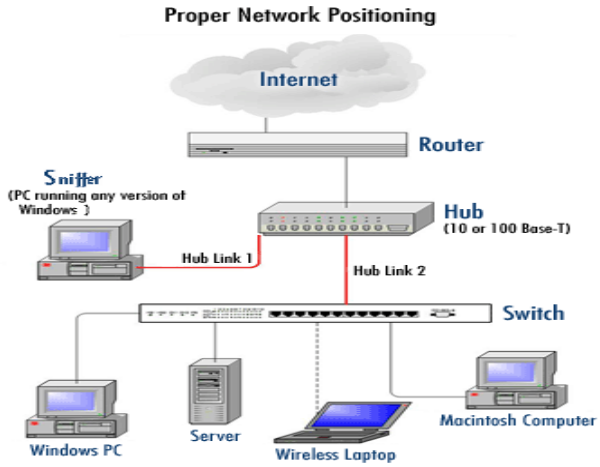
32

Fiziksel Katman Güvenliği - Kablo

- Fiziksel güvenlik sağlanmadan diğer katmanların güvenliği sağlanmaz.

33

Fiziksel Katman Güvenliği – Sistem Odası



34

Ağ Protokolü Analiz (Sniffer) Programları

- Ağ üzerindeki trafiği sezebilen, çözebilen ve değiştirebilen donanım ve yazılım araçlarının bir kombinasyonudur
  - Pasif izleme (sezme)
  - Aktif (atak yapma)
- Hem ticari hem de ücretsiz sürümleri bulunmaktadır
- Genelde yazılım tabanlıdır
- Sniffer olarak da bilinirler
  - Ağ üzerindeki veriyi pasif olarak izleyen bir programdır
  - Makineniz üzerinde çalışan uygulamalar ve protokoller tarafından gönderilen ya da alınan paketlerin bir kopyasını alır
- Yaygın kullanılan ağ protokolü analiz programları
  - **Wireshark ,** Ethereal , Windump ve diğerleri
- Sniffer programlarını efektif bir şekilde kullanmak için iyi bir ağ bilgisine sahip olmak gerekmektedir.

35

Wireshark

- Gerald Combs tarafından Ethereal ismi ile başlatılan bir projedir
- İlk versiyonu 1998 yılında yayınlanmıştır, Wireshark ismi haziran 2006'da verilmiştir
- Paket sniffer uygulamasıdır, dolayısıyla bir ağın haritasını çıkartmak için kullanılamaz
- Fonksiyonelliği tcpdump'a çok benzerdir ve diğer bir çok sniffer ile de uyumludur
- Birçok bilgiyi sıralayan ve filtreleyen özelliklere, komut satırına ve grafik arabirimine sahiptir
- 750'nin üzerinde protokol destekler ve bu protokollerin yapısını gösterir
- Kapsüllemeli bir yapıda görünüm sunar ve anlamlarını yorumlar
- Sadece pcap tarafından desteklenen ağlar üzerinde veri yakalama yapabilir
- Açık kaynak kodludur ve farklı işletim sistemleri üzerinde çalışabilir
- İnternet ortamında bir çok online kaynak mevcuttur
- Pasif bir izleme aracıdır, dolayısıyla ağ verisi üretmez

36

Wireshark ve WinPcap (libpcap: Linux:)

Wireshark – Paketleri Snif etmek için uygulama

WinPcap – Paket yakalamak için açık kaynak kütüphanesi

Operating System – Windows & Unix/Linux

Network Card Drivers – Ethernet/WiFi Kartı

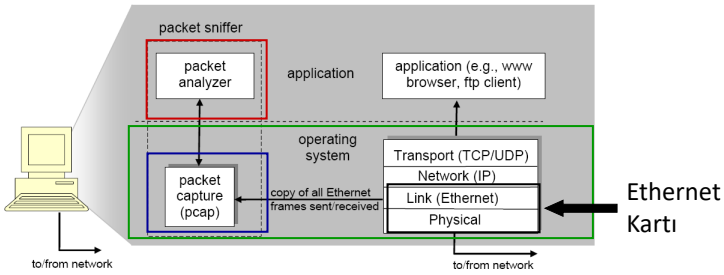
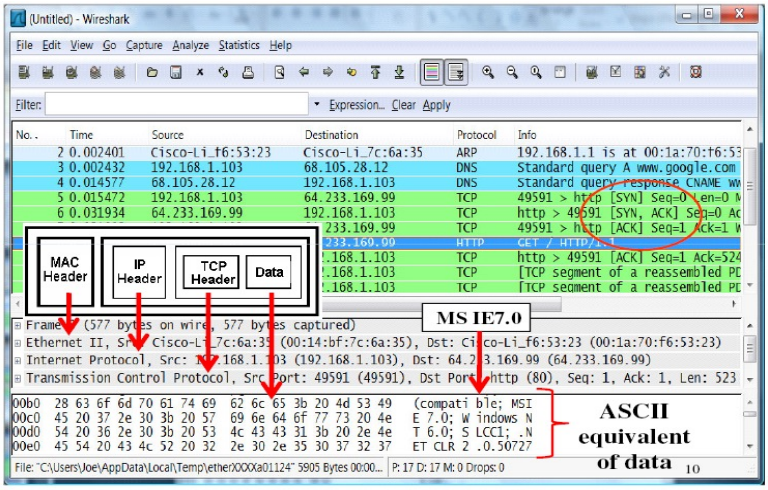


Figure 1: Packet sniffer structure

37

Wireshark Kullanıcı Arayüzünün Değerlendirimi



38