Bilgi Güvenliğine Giriş
TCP IP Ağ Güvenliği

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr bağlantısından erişebilirsiniz.

1. Bölüm

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr bağlantısından erişebilirsiniz.

Sunum İçeriği

- İnternet ve Tarihçesi
- OSI ve TCP/IP Referans Modelleri
- Tcpdump ve Wireshark ile Paket Analizi
- Fiziksel Katman
- Veri Bağı Katmanı
- Ağ Katmanı
- Taşıma Katmanı

İnternet ve Tarihçesi

TÜBİTAK
eğitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

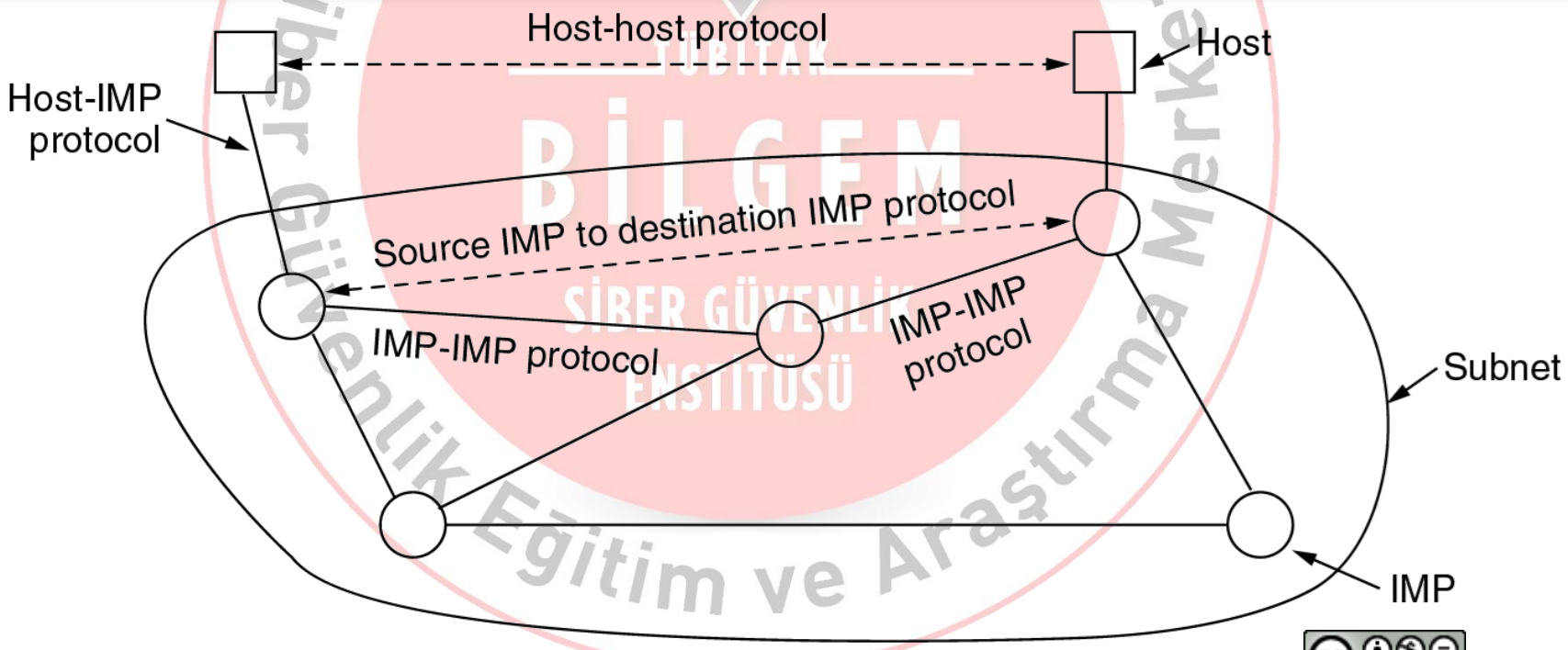
Internet ve Tarihi Gelişimi

İlk paket anahtarlamalı deneyim

1960 - Advanced Research Projects Agency (ARPA)

Amaç

Dağıtık, tek bir çöküş noktası yok.



* *Computer Networks, Fourth Edition, Andrew S. Tanenbaum*

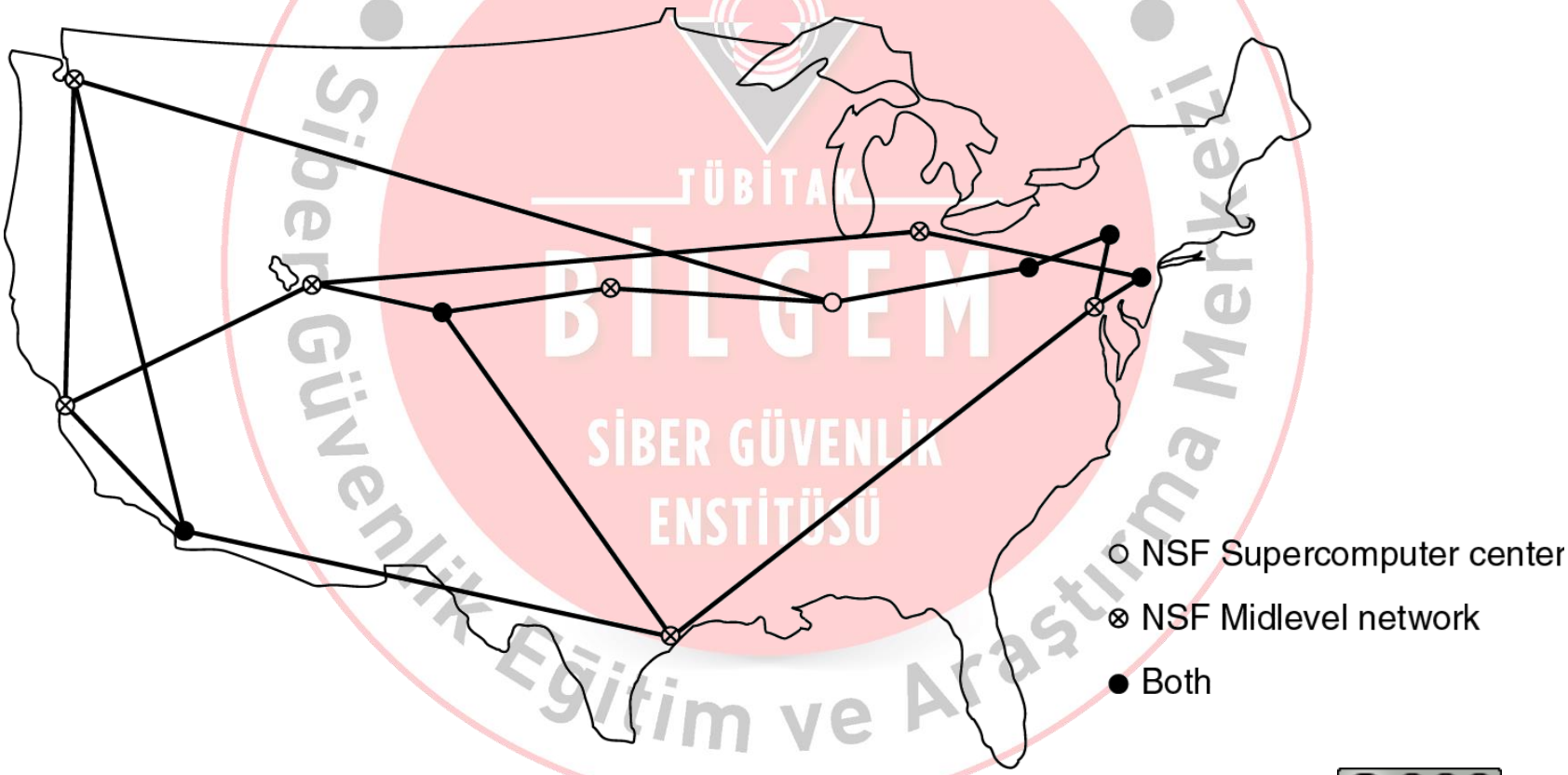
TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü Eğitim ve Araştırma Merkezi

Internet ve Tarihi Gelişimi

Unix işletim sistemine eklenmesi

1984 – Domain Name System

1988 – NFSNET Backbone



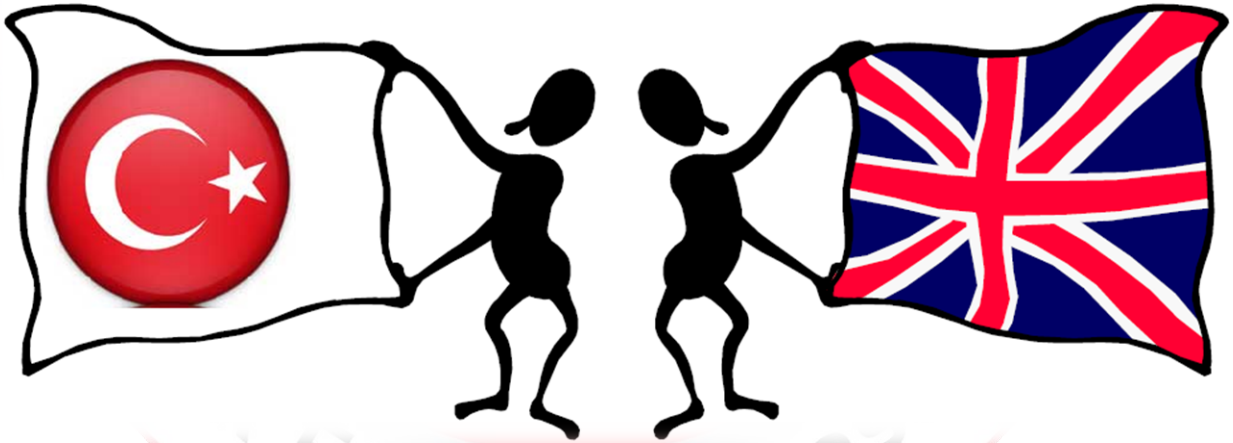
* *Computer Networks, Fourth Edition, Andrew S. Tanenbaum*

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma Merkezi

Protokol Kavramı

Protokol

- İletişimi yönetmek amacıyla konulmuş kurallar bütünü.
- Dillere benzerlik gösterir.
- Standart arayüzlerle ürünlerin birbiriyle uyumlu çalışması hedefi.



TÜBİTAK Eğitim ve Araş

cc BY NC ND

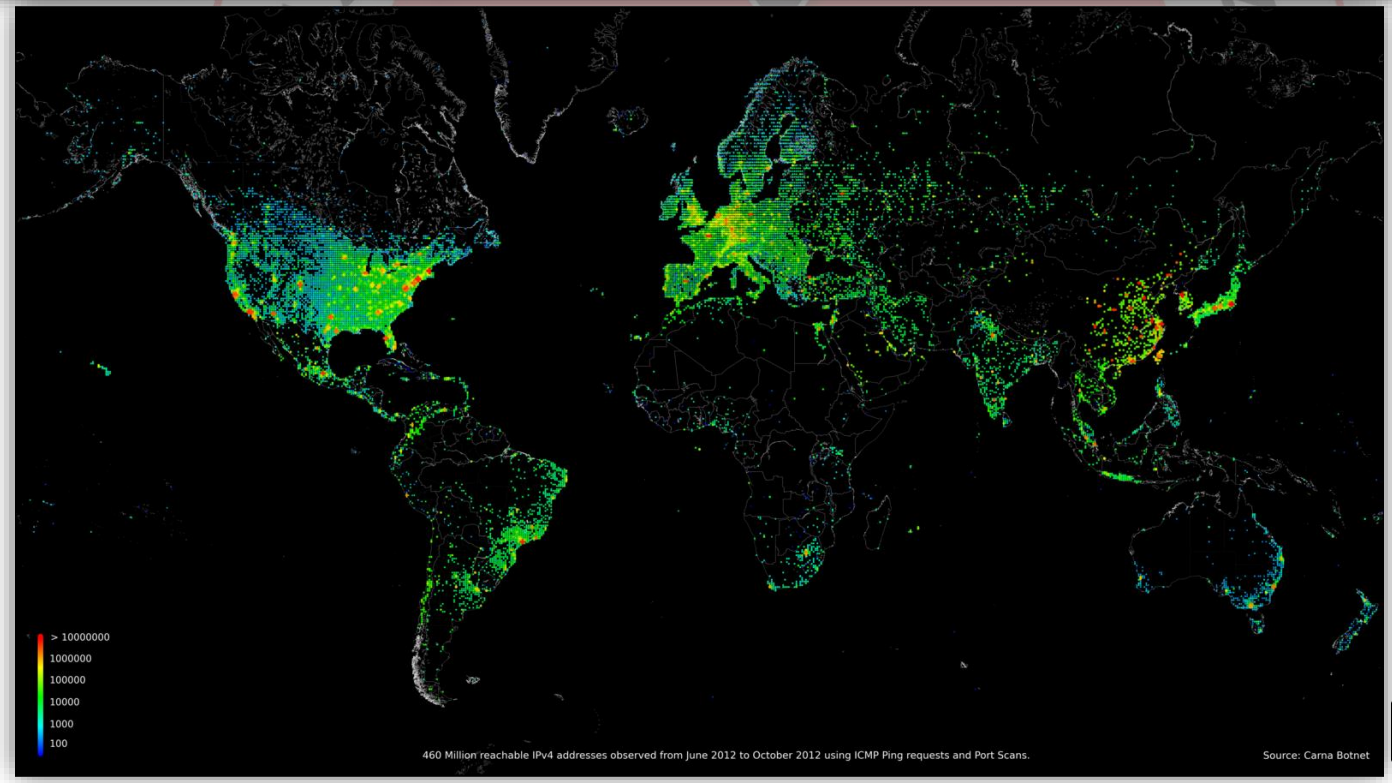
IP

İnternet Protokolü

IP: bilgisayar ve yönlendiricilerin iletişimi için ortak ağ protokolü

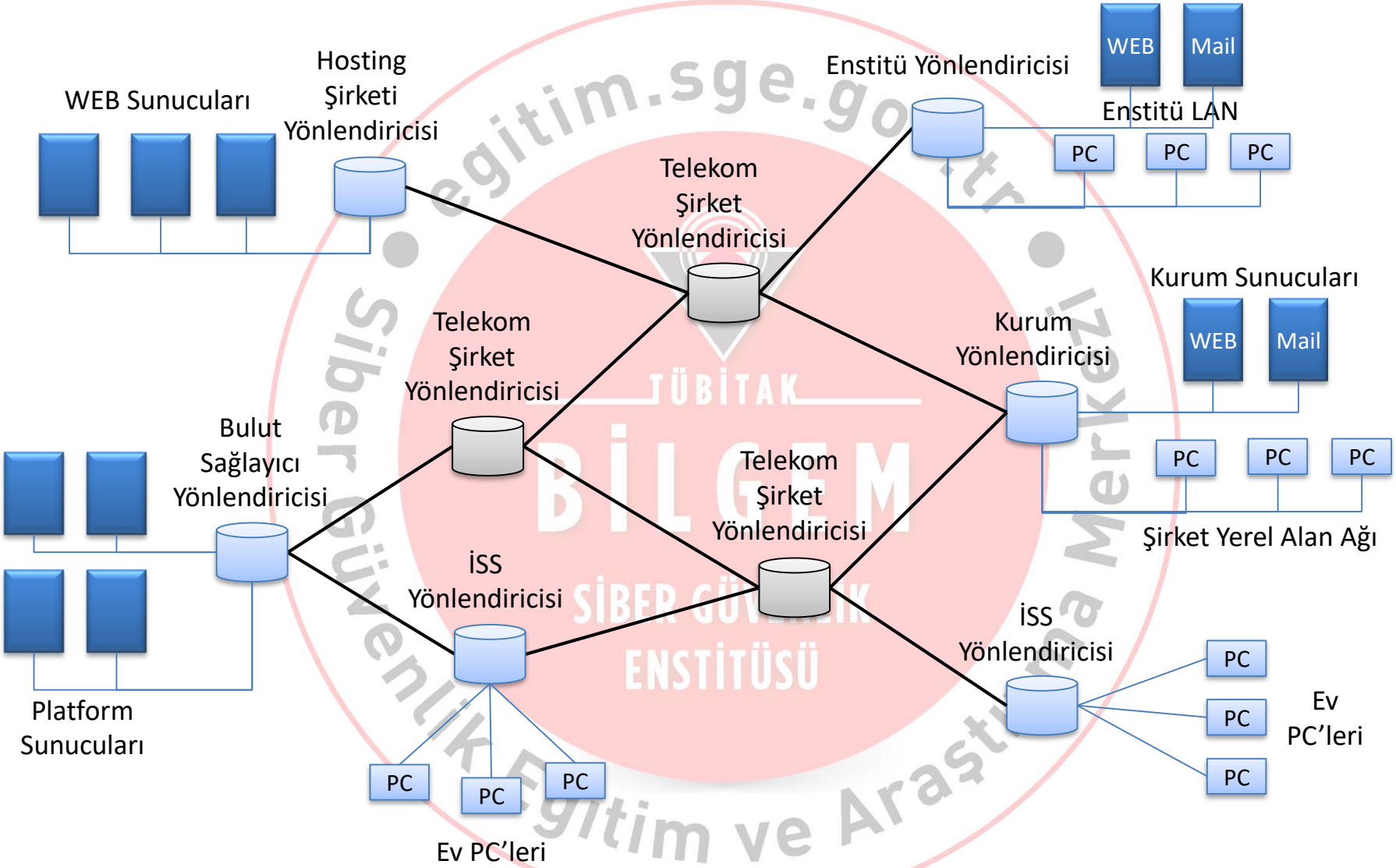
Basit yapısı nedeniyle beklenenden fazla talep

2018 itibarı ile 4 milyar insan internet servislerini kullanmakta



BY NC ND

Geniş Alan Ağı Örneği



egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

CC BY NC ND

OSI ve TCP/IP Referans Modelleri

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma Merkezi
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

OSI Referans Modeli

Kullanıcı etkileşimli uygulamalar: HTTP, SMTP

Veri formatlarının birbirine dönüşümü: ASCII, MP3, JPG

Soket açma, oturum kurma: SQL, RPC

Hata ve akış kontrolü: TCP, UDP

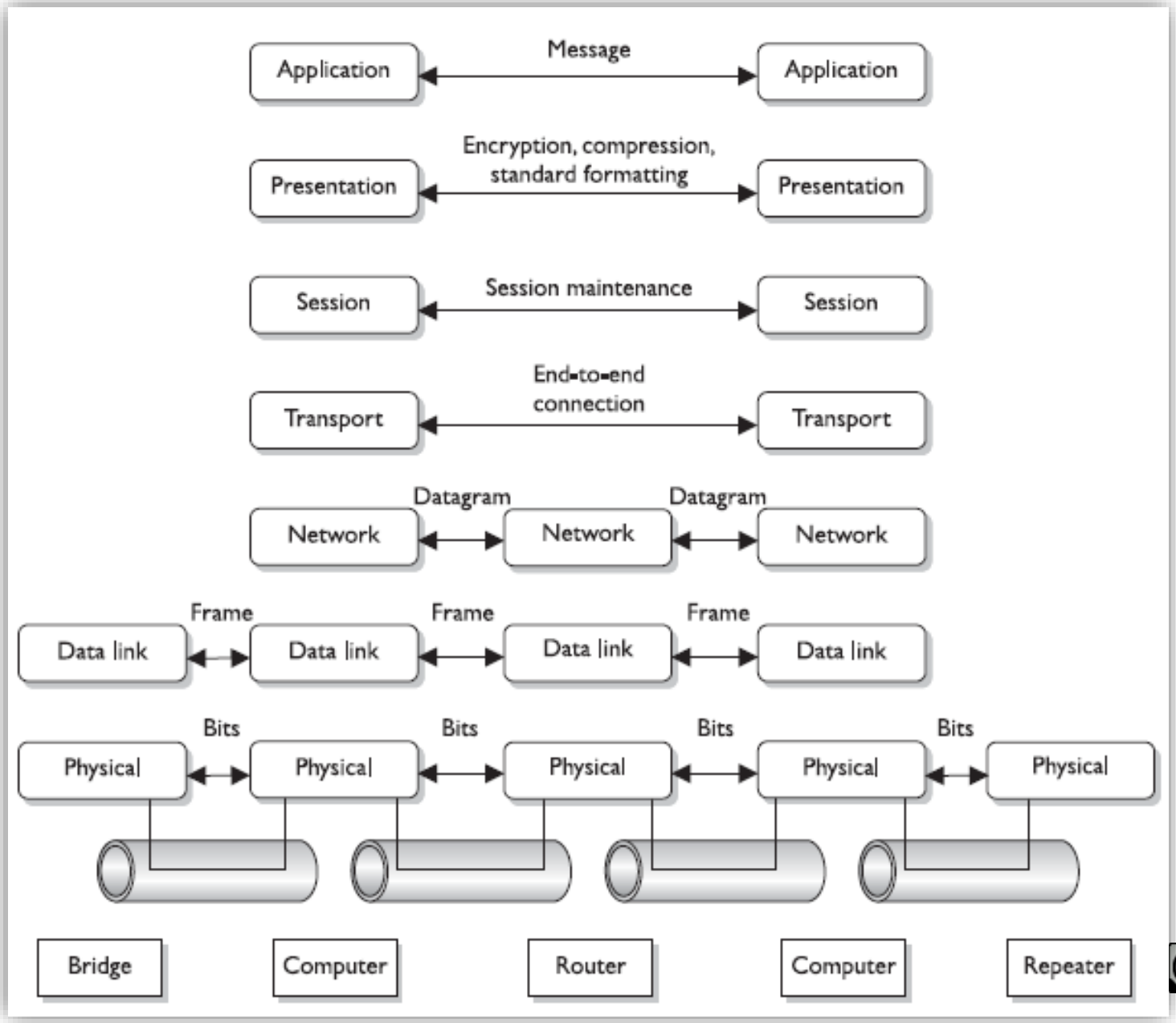
Uçtan uca iletişim, sanal adresleme: IP

Ortama Erişim: Ethernet, Wireless

İkili iletim: Koaksiyel, UTP, STP ve fiber kablolar

CC BY NC ND

Katmanlar Arası Haberleşme



BY NC ND

Katmanlar ve Protokoller

Application	HTTP Hyper Text Transport Protocol	Telnet Virtual Terminal	FTP File Transfer Protocol	SMTP Simple Mail Transfer Protocol	TFTP Trivial File Transfer Protocol	DNS Domain Name Server	SNMP Simple Network Mgmt Protocol
Presentation							
Session							
Transport	TCP (Reliable Datagram Service)				UDP (Unreliable Datagram Service)		
Network	IP Addressing, Routing, Fragmentation						
Data Link	802.3 CSMA/CD (Ethernet)	802.4 Token Bus			802.5 Token Ring		FDDI
Physical	Physical Medium (Token Ring, 10Base-T, 100BaseTx...)						

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

TCP/IP Standardı

TCP/IP

İnternetin temeli

4 katmandan oluşur.

- Uygulama
- Taşıma
- Ağ
- Ağ Erişimi

SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

CC BY NC ND

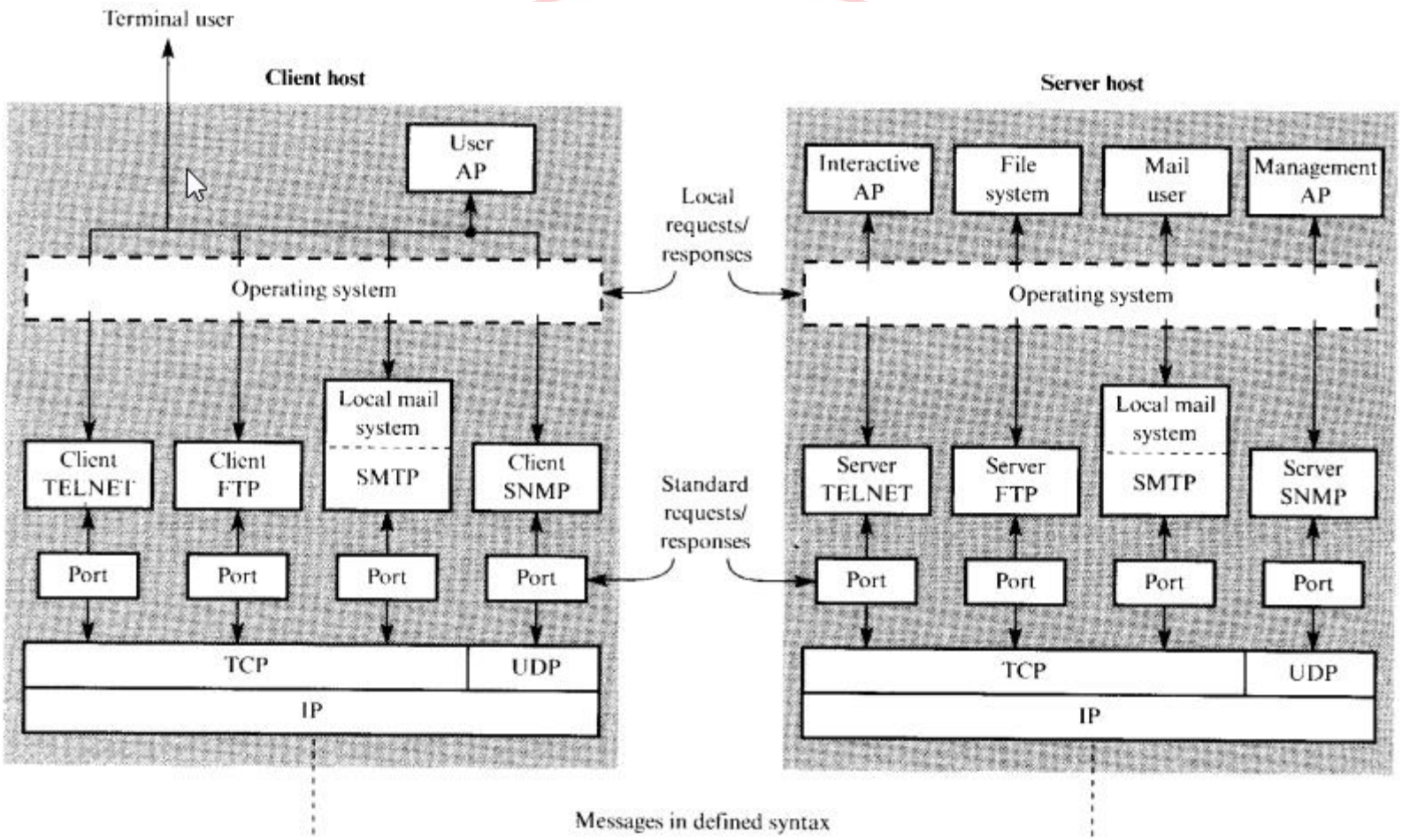
OSI ve TCP/IP

OSI	TCP/IP
Uygulama Katmanı (L5)	Uygulama Katmanı
Sunum Katmanı (L6)	
Oturum Katmanı (L5)	
Taşıma Katmanı (L4)	Taşıma Katmanı
Ağ Katmanı (L3)	Ağ Katmanı
Veri Bağı Katmanı (L2)	Ağ Erişim ve Fiziksel Katman
Fiziksel Katman (L1)	

Her katman çalışmak için bir alt katmanın servisine ihtiyaç duyar.

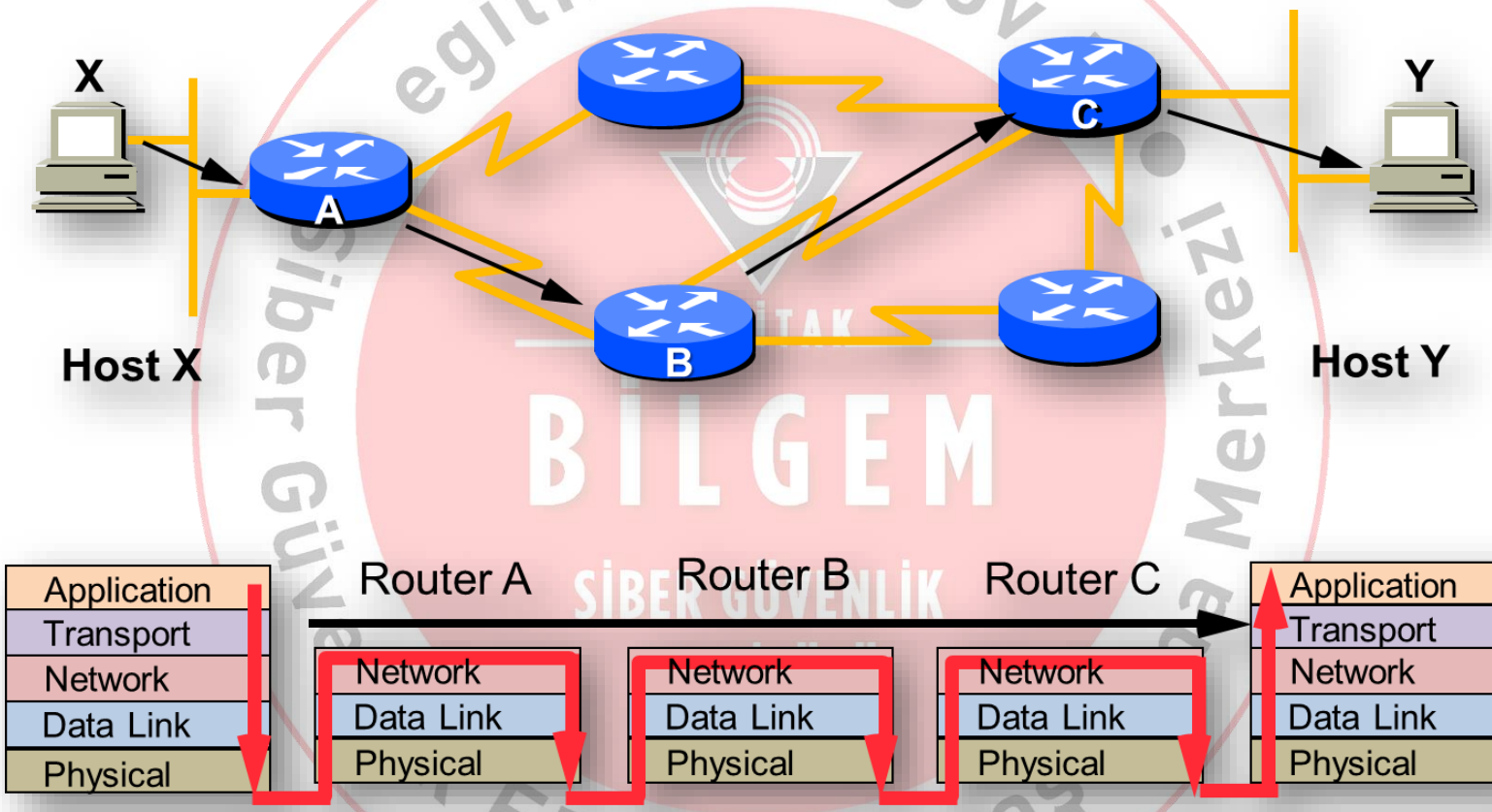
CC BY NC ND

OSI ve TCP/IP - İletişim



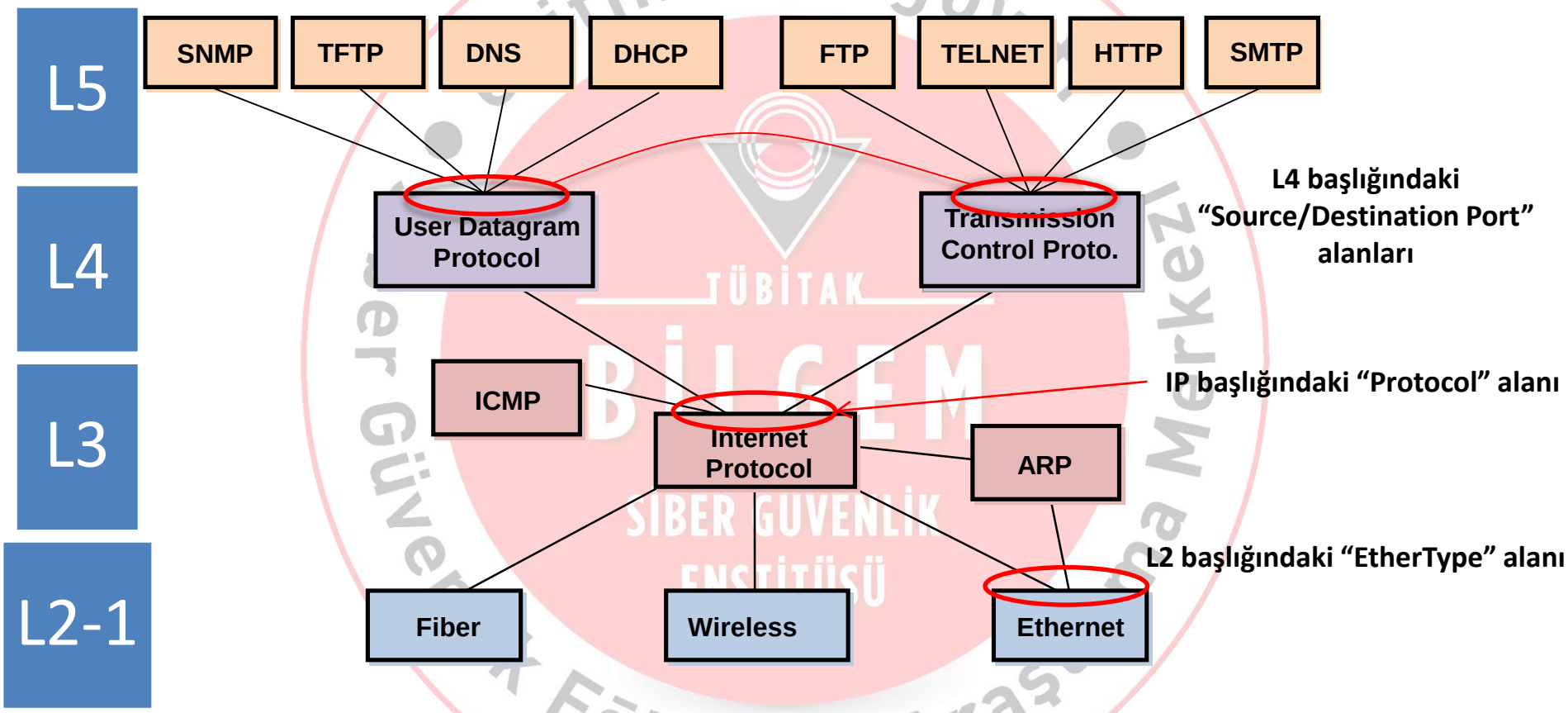
Eğitim ve Araş

TCP/IP ile İletişim



egitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
BİLGEM
SİBER GÜVENLİK
TÜBİTAK

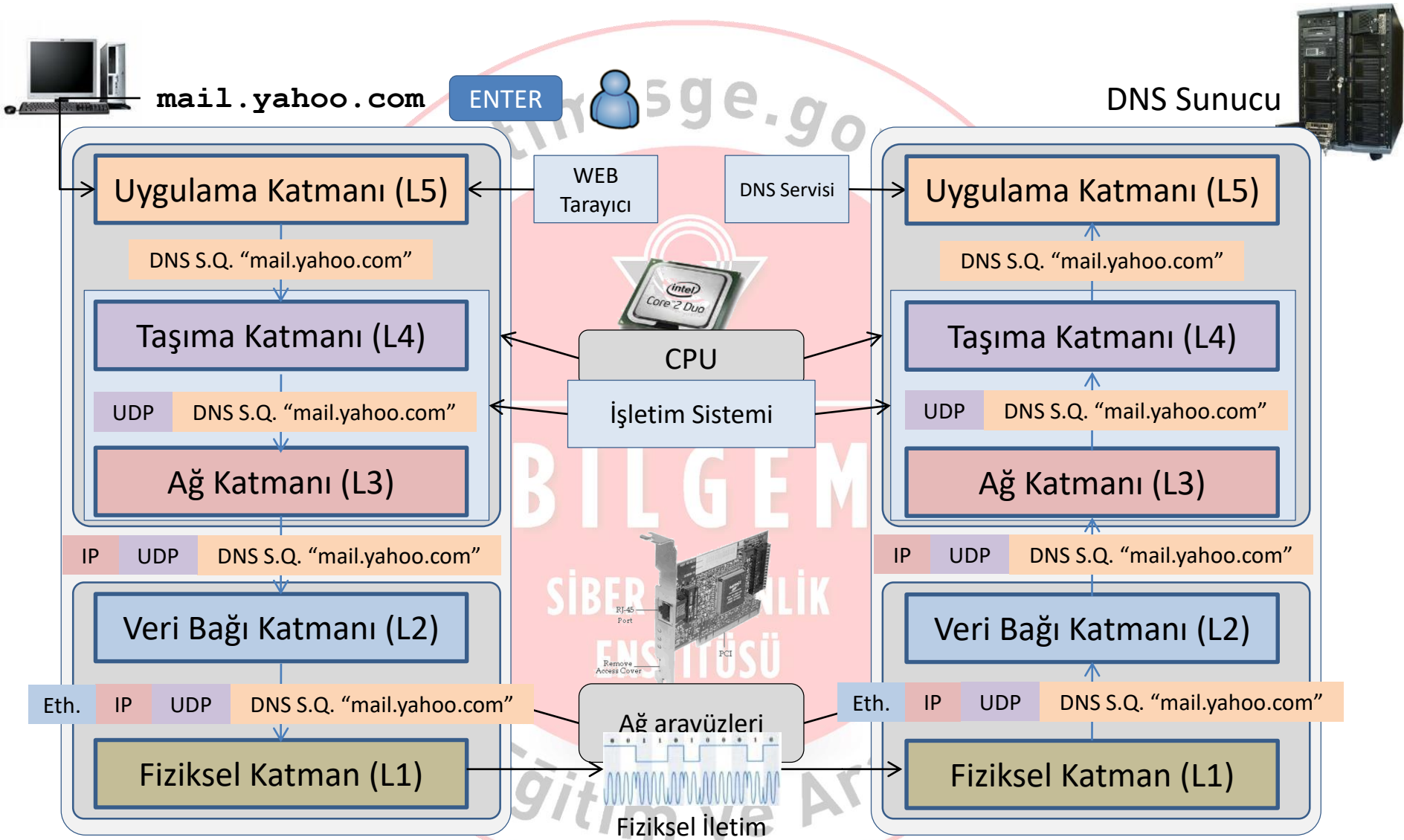
Protokoller ve Çoğullama



TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Eğitim ve Araştırma Merkezi

BY NC ND

Örnek: DNS Protokolü



BY NC ND

Tcpdump ve Wireshark ile Paket Analizi

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma Merkezi
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

Aktif-Pasif Paket Dinleme

Paket Dinleme (Sniffing)

İyi niyetli kullanım:

- Sistem problemlerini ve performansını anlama
- Uygulama operasyonlarının testi
- Saldırıların tespiti

Kötü niyetli kullanım:

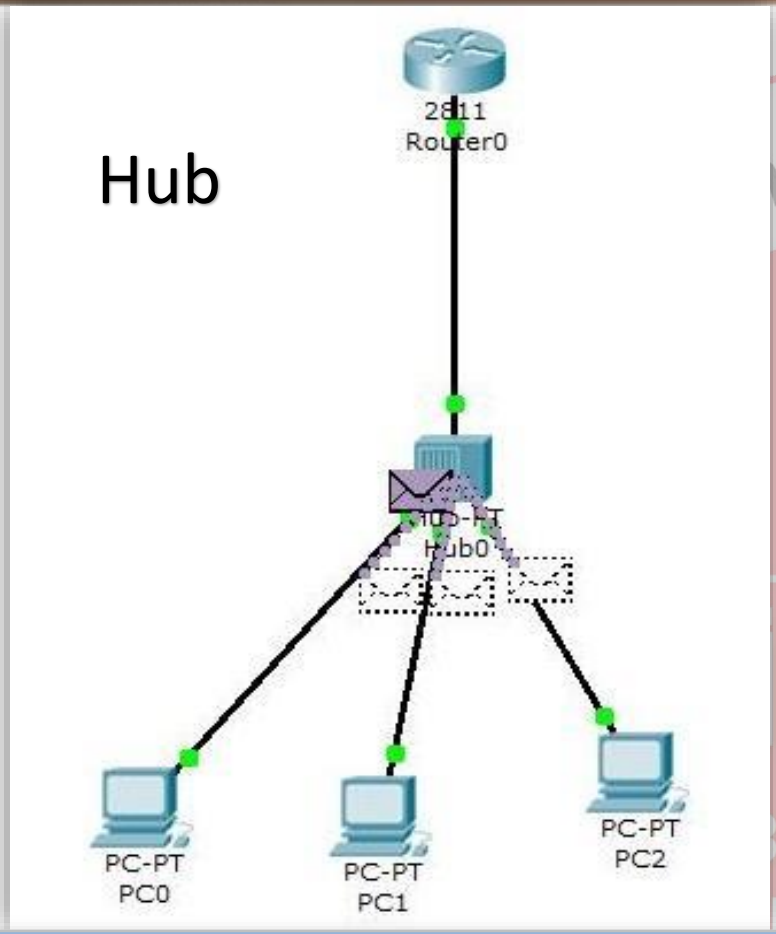
- Protokoller üzerinden pasif olarak veri toplama
- Hedef ağın trafiğini ve örüntüsünü keşif
- Ağ içerisine dâhil olarak arka kapı bırakma

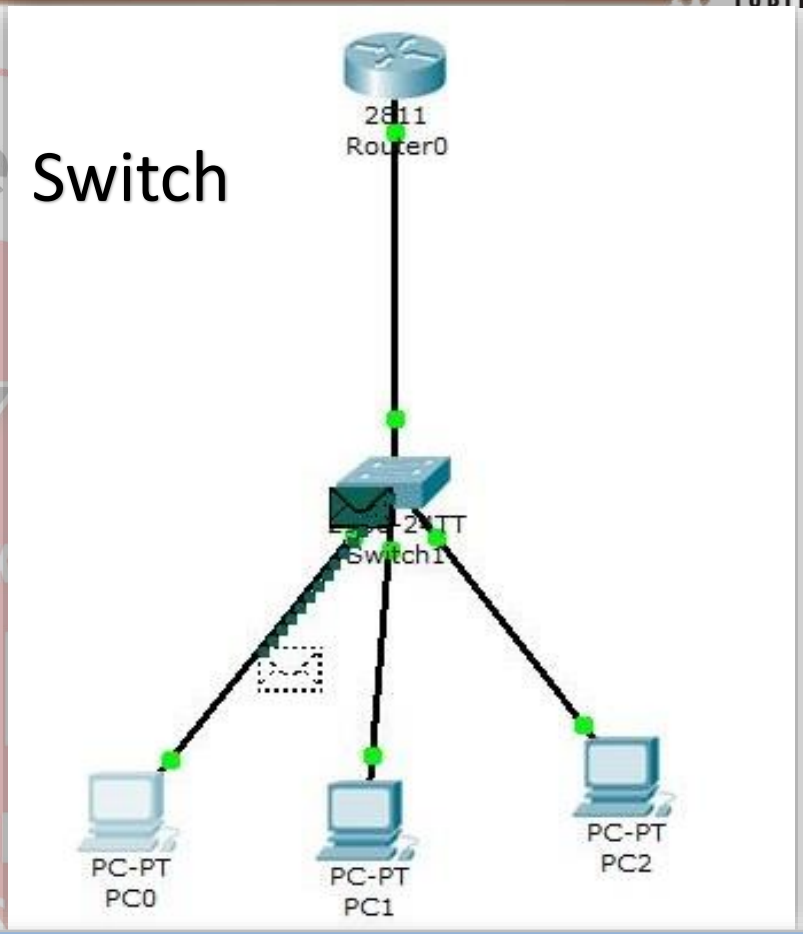
Paket Dinleyici (Sniffer)

- Farklı işlem modlarında (pasif ve aktif) kullanılabilir.
- Ticari ve ücretsiz sürümleri bulunabilmektedir.
- Genelde yazılım tabanlıdır.
- Bilgisayar veya sunucu sistemler üzerinde çalışan uygulamalar ve protokoller tarafından gönderilen/alınan paketlerin birer kopyasını alır.
- Yaygın kullanılan ağ protokolü analiz programları: Wireshark, Tcpdump

BY NC ND

Aktif-Pasif Paket Dinleme: Ortam





Promiscuous mod

Sistemlerin hedefi kendisi olmayan paketleri alabilmesi için gereklidir.

BY NC ND

Tcpdump – Komut Satırından Paket Analizi

- *Bir pcap dosyasını tcpdump ile açmak için **-r** parametresi kullanılır:*

tcpdump -r test.pcap

- ***-n** parametresi de kullanıldığında IP çözümlemesi yapmaz, bilinen protokollerin isimlerini yazar ve daha hızlı sonuç verir:*

tcpdump -r test.pcap -n

- ***-i** parametresi ile belirtilen arayüzde dinleme yapılabilir, **-w** parametresi ile de dinlenen arayüzdeki trafik bir pcap dosyasına kaydedilebilir:*

tcpdump -n -i eth0 -w sonuc.pcap

BY NC ND

Tcpdump ile Paket Analizi

- ***-t** parametresi ile sonuçlarda yer alan zaman damgası (timestamp) değerini gizlemesini,*
- ***-c** parametresi ile de pcap dosyasındaki istenen sayıdaki satırı görüntülemesini sağlayabilirsiniz:*

tcpdump -r test.pcap -ntc 2

- ***-x** parametresi ile **HEX** değerleri, **-X** parametresi ile de hem **HEX** hem de **ASCII** değerleri görüntülenebilir:*

tcpdump -r test.pcap -ntxc 1

- ***-v** parametresi ile ayrıntılı (**Verbose**) modda paket değerleri görüntülenebilir:*

tcpdump -r test.pcap -ntvc 1

- ***-e** parametresi ile **MAC**/Ethernet adreslerinin görüntülenmesi sağlanır:*

tcpdump -r test.pcap -ntec 1

BY NC ND

Tcpdump ile Paket Analizi

Örnek çıktı

16:21:24.174180 192.168.60.3.34720 > 10.10.10.3.3389: S 2354677536:2354677536(0) win 5840 <mss 1460,sackOK,timestamp 25027249 0,nop,wscale 0> (DF)

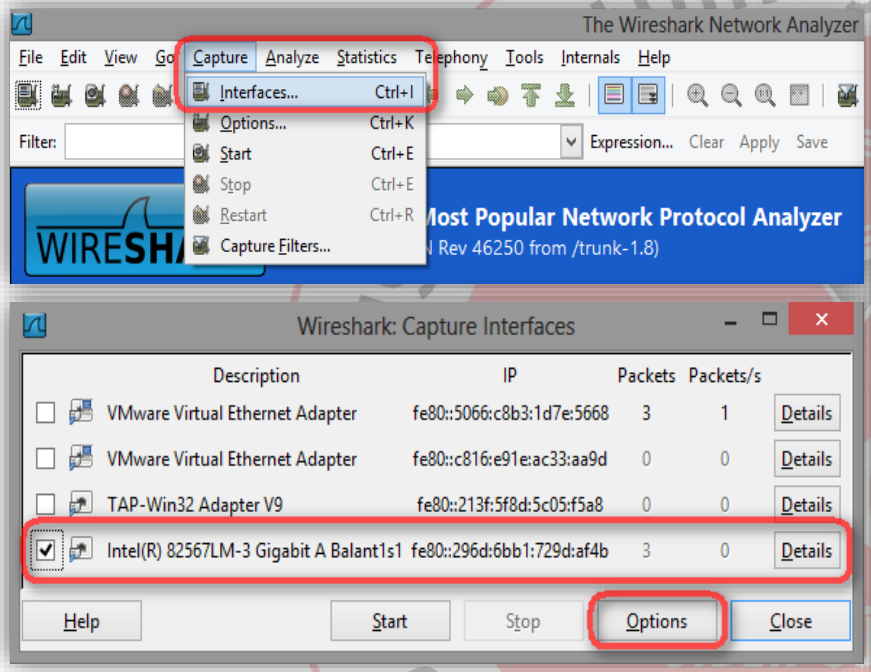
16:21:24.174180	Zaman Damgası
192.168.60.3	Kaynak IP Adresi
34720	Kaynak Port Numarası
>	Yön Belirteci
10.10.10.3	Hedef IP Adresi
3389	Hedef Port Numarası
S	TCP SYN Bayrağı Aktif Hale Getirilmiş
2354677536	TCP Başlangıç Seri Numarası (ISN)

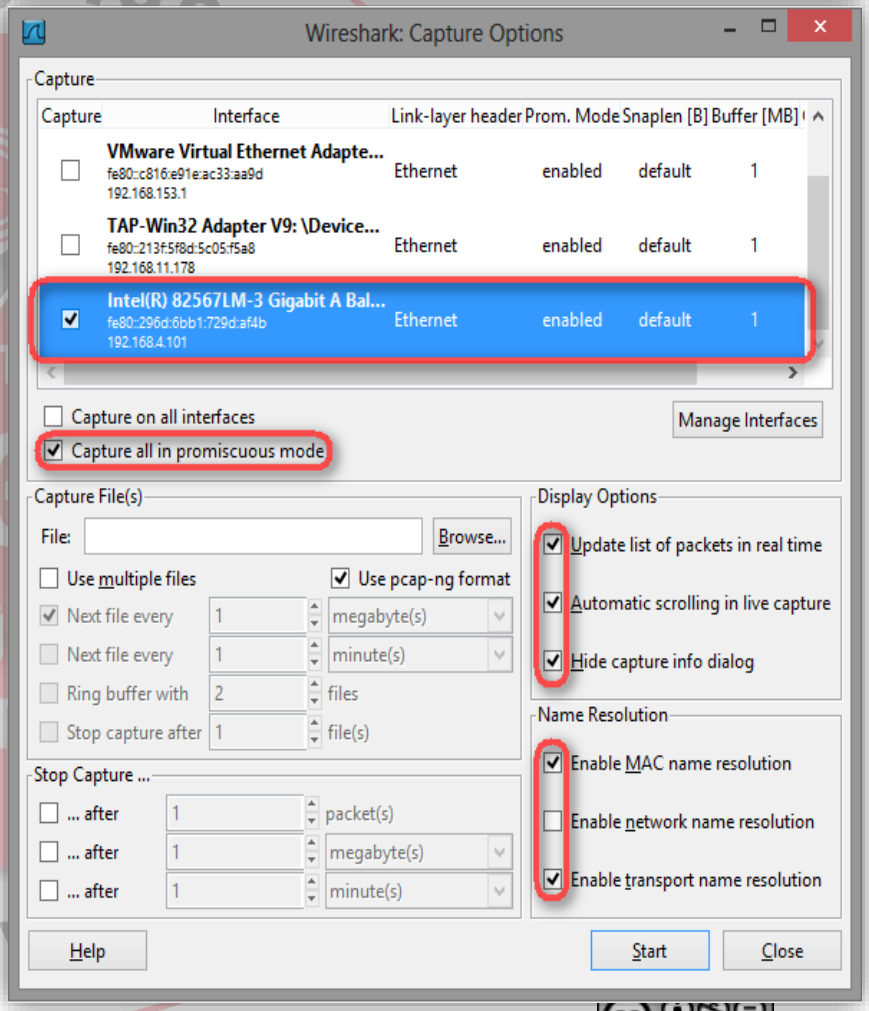
BY NC ND

Wireshark

İşlevsel olarak tcpdump'a benzer

Grafik arayüzü





BY NC ND

Wireshark

*WiFi [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.2.110	192.168.52.10	DNS	65	Standard query 0xb75b SOA local
2	1.70255900	SamsungE_d0:ad:a4	Broadcast	ARP	60	Who has 192.168.2.1? Tell 192.168.2.91
3	2.00025900	192.168.2.110	192.168.2.1	DNS	65	Standard query 0xb75b SOA local
4	2.03078700	192.168.2.1	192.168.2.110	DNS	140	Standard query response 0xb75b No such name
5	2.03357900	192.168.2.110	192.168.52.10	DNS	65	Standard query 0x2297 SOA local
6	2.32859000	192.168.2.110	192.168.2.1	DNS	70	Standard query 0x4285 A google.com
7	2.36095700	192.168.2.110	192.168.2.1	DNS	70	Standard query 0x4285 A google.com
8	2.36723400	192.168.2.1	192.168.2.110	DNS	382	Standard query response 0x4285 A 173.194.11
9	2.39011300	192.168.2.110	173.194.113.46	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, t

```
⊞ Frame 6: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
⊞ Ethernet II, Src: IntelCor_13:df:ee (c4:d9:87:13:df:ee), Dst: AirtiesW_39:c7:b7 (18:28:61:39:c7:b7)
⊞ Internet Protocol Version 4, Src: 192.168.2.110 (192.168.2.110), Dst: 192.168.2.1 (192.168.2.1)
⊞ User Datagram Protocol, Src Port: 53893 (53893), Dst Port: domain (53)
⊟ Domain Name System (query)
    [Response In: 8]
    Transaction ID: 0x4285
  ⊞ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ⊟ Queries
    ⊞ google.com: type A, class IN
```

```
0000  18 28 61 39 c7 b7 c4 d9  87 13 df ee 08 00 45 00   .(a9.... ......E.
0010  00 38 33 58 00 00 80 11  81 9d c0 a8 02 6e c0 a8   .83X.... .....n..
0020  02 01 d2 85 00 35 00 24  50 ed 42 85 01 00 00 01   .....5.$ P.B.....
0030  00 00 00 00 00 00 06 67  6f 6f 67 6c 65 03 63 6f   .......g oogle.co
0040  6d 00 00 01 00 01                                  m.....
```

Text item (text), 16 bytes | Packets: 25 · Displayed: 25 (100,0%) · Dropped: 0 (0,0%) | Profile: Default

Fiziksel Katman (L1)

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma M

Fiziksel Katman

Radikal 18 Mayıs 2011, Çarşamba
Son Güncelleme 13:49
ANTALYA 28°C / 18°C
Aranacak Metin

Ana Sayfa | Türkiye | Politika | Yaşam | Ekonomi | Dünya | Kültür | Tartışı-Yorum | Spor | Çevre | Eğitim | Sağ

Anasayfa > Dünya > 75 yaşındaki Gürcü kadın interneti çökertti

Yazdır | Arkadaşına Gönder | Yorum Yaz | Arşive Ekle

75 yaşındaki Gürcü kadın interneti çökertti

06/04/2011 16:46

Yazı Boyutu

75 yaşında Gürcü bir kadın, komşu Ermenistan'ın internet bağlantısını çökertmekle suçlanıyor.

< Önceki Haber | Sonraki Haber >

Tavsiye et | Bir kişi bunu tavsiye etti. Arkadaşların arasında tavsiye eden ilk sen ol

28 Mart tarihinde Gürcistan ile arasındaki kablolar hasar gördüğü için Ermenistan ülke çapında saatlerce internetsiz kalmıştı. Kesintinin gerekçesiyse bir kadının 'bakır hurda' araması. Gürcistan İçişleri Bakanlığı sözcüsü, yaşlı bir emekli kadının yerde bakır hurda ararken iki ülke arasındaki fiberoptik bağlantıya hasar verdiğini itiraf ettiğini açıkladı. Gürcistan'ın Ksani köyünde yaşayan kadının yaşından dolayı tutuksuz yargılanmasına karar verildi. Suçlu bulunması

Radikal

260 milyar dolarlık borsa bir kepçe darbesiyle çöktü

Yol çalışmasında bir kepçe veri kablolarını kopardı. Borsa idaresi hasardan işlem saati yaklaşırken haberdar oldu. Taşeron tamircileri grevdeki sendika durdurdu

cc BY NC ND

Neden Önemli?

www.businessinsider.com/heres-how-to-take-an-entire-continent-offline-2013-3

How To Take An Entire Continent Offline

Leo Mirani, Quartz | Mar. 28, 2013, 7:37 AM | 2,402 | 4

Recommend 25 Share 12 Tweet 98 +1 32 Email More

At its peak, Cyberbunker clogged up a mind-boggling 300 gigabits per second of the Internet in what's being called the biggest cyber-attack in history. But what if you could switch off 1.28 terabits—four times as much bandwidth—with nothing more high-tech than an axe?

That's what three men tried to do in an unsophisticated but effective form of sabotage in Egypt yesterday; their identities and motives are not yet known. Reuters reports the Egyptian coastguard intercepted a fishing boat off the coast of Alexandria and arrested three men trying to cut through the SEA-ME-WE 4 undersea cable. The cable is one of the main connections between Asia and Europe,

YouTube/antzoulis

QUARTZ

- S&P 500 hits all-time record—despite Apple
- The yen punishes Kuroda for pulling nothing new from his central banker bag of tricks
- Sorry everyone, but those ridiculously large phones are here to stay
- BlackBerry finally surprises market in a good way

cc BY NC ND

Veri Bağı Katmanı (L2)

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

L2 - Saldırı ve Güvenlik

1	ARP	Gratuitous (asılsız) ARP, ARP Atakları
2	VLAN	Anahtar Kandırma, Çift Etiketleme, VTP Atağı
3	Port Güvenliği	Çeşitli Saldırılara Karşı L2 Önlemleri
4	MACSec	L2 Şifreleme

BY NC ND

ARP

Address Resolution Protocol

- 48 bit gerçek donanım adresleri – MAC
- IP'nin fiziksel adresleri öğrenmesi için kullanılır.
- Broadcast Request, Unicast Reply
- Statik ve dinamik ARP belleği
  - ARPCacheLife

Statik kayıt eklemek için

```
# arp -s 10.0.0.200 00-10-54-CA-E1-40
```

ENSTİTÜSÜ
enlik Eğitim ve Araştırma

Gratuitous (asılsız/karşılıksız) ARP

FF:FF:FF:FF:FF:FF hedefli «X IP adresi bana ait» mesajları

- Yedekli yapılarda **failover** durumlarında kullanılmakta,
- Kötü niyetli kullanımda bütün ağ trafiği kesilebilir/üzerine alınabilir.

```
# arping -c 4 -A -I eth1 192.168.1.1
```

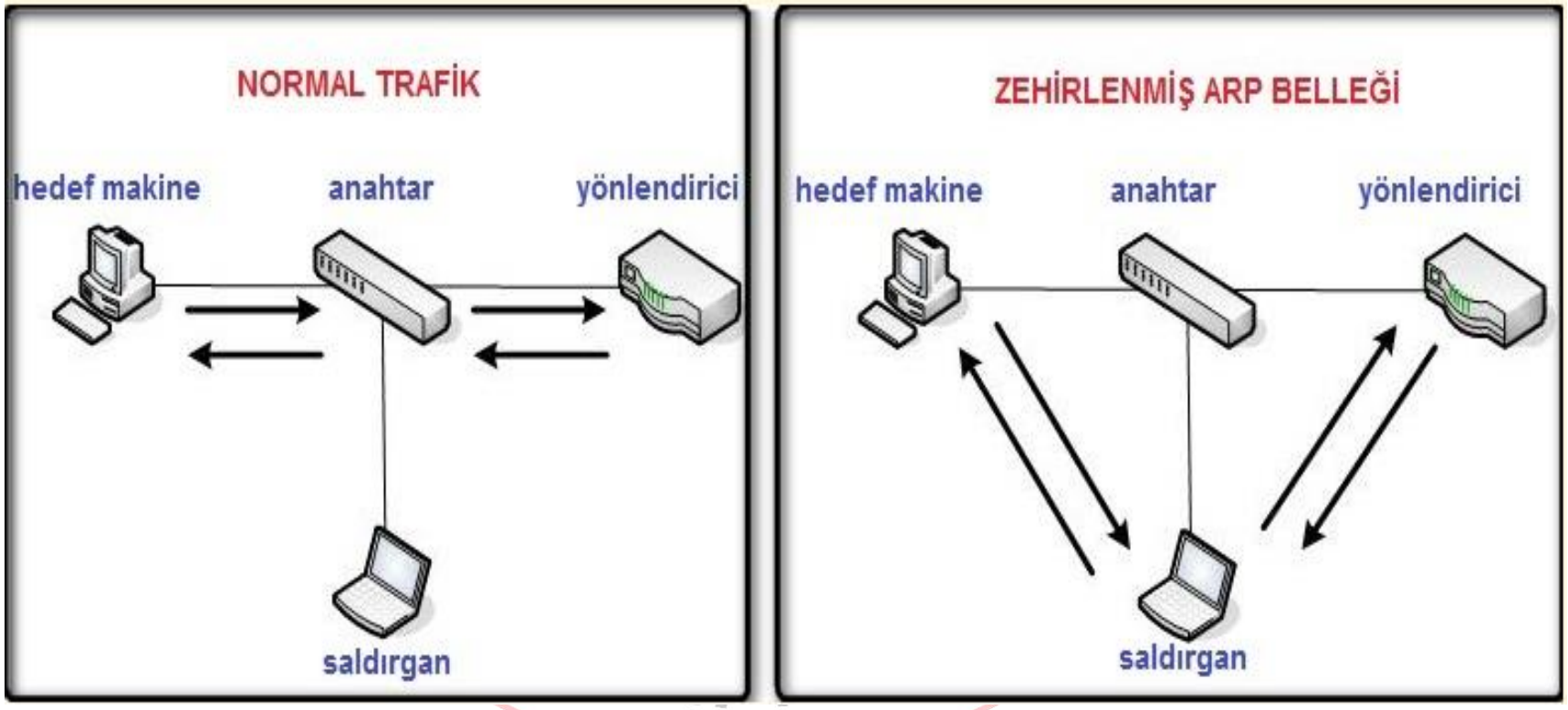
```
Ethernet II, Src: 02:02:02:02:02:02, Dst: ff:ff:ff:ff:ff:ff
    Destination: ff:ff:ff:ff:ff:ff (Broadcast)
    Source: 02:02:02:02:02:02 (02:02:02:02:02:02)
    Type: ARP (0x0806)
    Trailer: 000000000000000000000000000000000000
Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: 02:02:02:02:02:02 (02:02:02:02:02:02)
    Sender IP address: 192.168.1.1 (192.168.1.1)
    Target MAC address: ff:ff:ff:ff:ff:ff (Broadcast)
    Target IP address: 192.168.1.1 (192.168.1.1)
0000  ff ff ff ff ff ff 02 02 02 02 02 02 08 06 00 01   ................
0010  08 00 06 04 00 01 02 02 02 02 02 02 c0 a8 01 01   ................
0020  ff ff ff ff ff ff c0 a8 01 01 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

CC BY NC ND

L2 Saldırıları

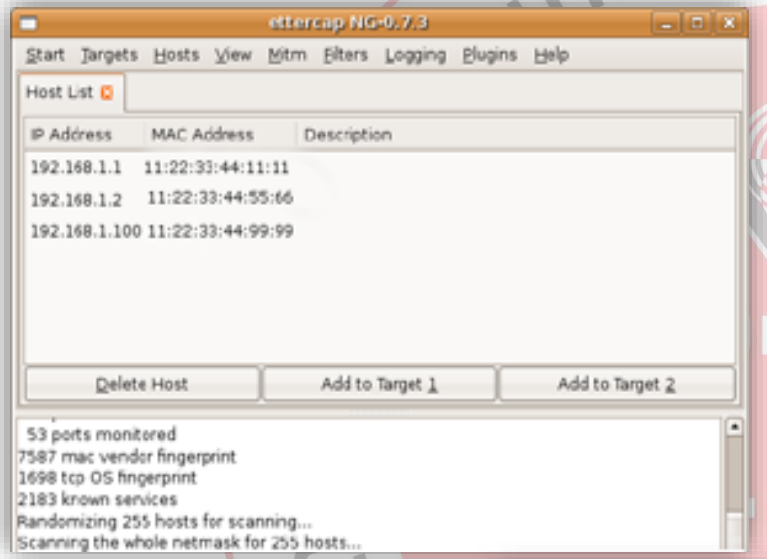
Sahte ARP Atağı (Spoofing, Cache Poisoning)

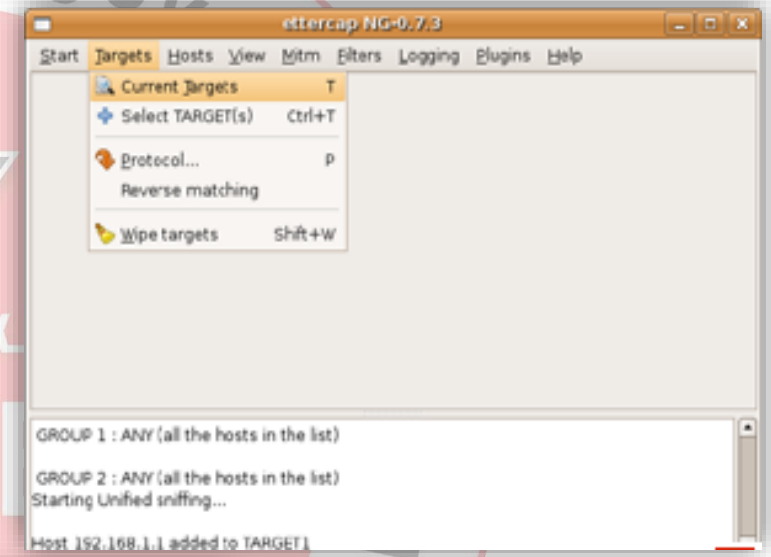
Yerel ağ içerisinde aynı alt ağ içerisinde bulunan istemcilerin MAC adres bilgisini değiştirerek kurban ile ön tanımlı ağ geçidi arasındaki iletişimin kendi üzerinden gerçekleştirilmesinin sağlanmasıdır.



BY NC ND

Ettercap ile ARP Zehirlemesi





cc BY NC ND

L2 Saldırıları

MAC Seli ve Servis Dışı Bırakma

Saldırgan anahtarın MAC tablosunu sahte MAC adresleriyle doldurmak suretiyle, anahtar üzerindeki tüm trafiği dinleyebilir duruma gelebilir.

Siber Güvenlik Eğitim ve Araştırma Merkezi

L2 Saldırıları

Macof ile MAC Seli

```
# while  true; do macof -d 192.168.1.1 -n 100000; sleep 30; done
```

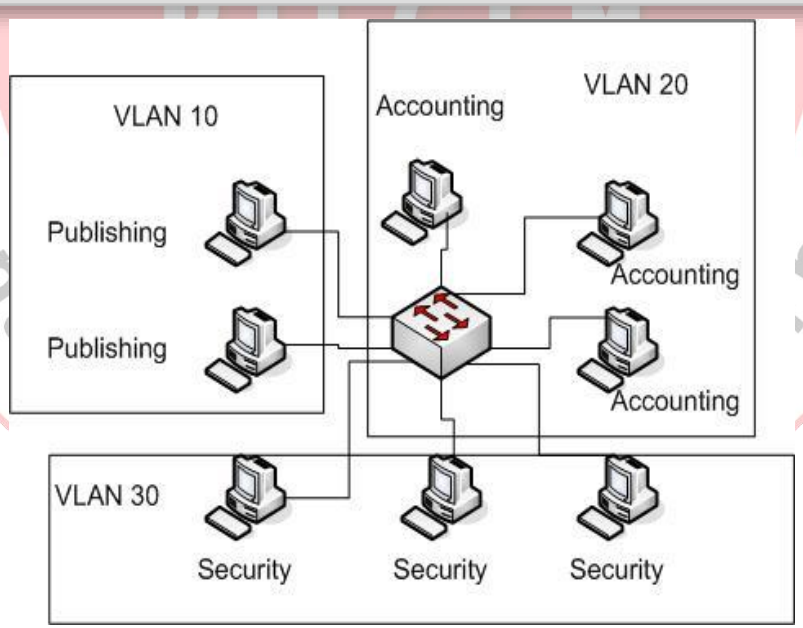
```
6509E#show mac address-table
Legend: * - primary entry
        age - seconds since last seen
        n/a - not available

  vlan   mac address     type    learn     age              ports
------+----------------+--------+-----+----------+--------------------
----
*    7  f27e.9679.038d  dynamic  Yes       1120   Gi1/2
*    7  b875.907c.4480  dynamic  Yes       1120   Gi1/2
*    7  b0fd.fb4a.c0ec  dynamic  Yes       1120   Gi1/2
*    7  fedc.8f6f.7888  dynamic  Yes       1120   Gi1/2
*    7  f271.1738.db59  dynamic  Yes       1115   Gi1/2
*    7  aa38.204c.d3f7  dynamic  Yes       1110   Gi1/2
*    7  c627.f87a.57d5  dynamic  Yes       1105   Gi1/2
*    7  4432.4415.293f  dynamic  Yes       1100   Gi1/2
*    7  d8b5.021c.bcda  dynamic  Yes       1095   Gi1/2
*    7  06d3.9265.aaca  dynamic  Yes       1095   Gi1/2
*    7  0480.8839.be1c  dynamic  Yes       1090   Gi1/2
*    7  c4b0.ec12.f1df  dynamic  Yes       1090   Gi1/2
*    7  c82f.237b.5933  dynamic  Yes       1085   Gi1/2
*    7  e4d6.8144.4921  dynamic  Yes       1085   Gi1/2
*    7  26a7.623b.8ff0  dynamic  Yes       1085   Gi1/2
*    7  2e1e.9314.5afd  dynamic  Yes       1085   Gi1/2
*    7  8a91.f242.da51  dynamic  Yes       1125   Gi1/2
*    7  0e9c.1a56.8f83  dynamic  Yes       1115   Gi1/2
*    7  1cbb.7004.1039  dynamic  Yes       1115   Gi1/2
```

BY NC ND

VLAN Kavramı

Sanal Yerel Alan Ağları

- Yerel alan ağı üzerindeki kullanıcıların mantıksal olarak gruplandırılmasıdır.
- Her VLAN, sadece kendi **broadcast** paketlerini alır.
- Daha verimli bant genişliği, daha fazla güvenlik
- 802.1q etiketleme (tagging)



BY NC ND

L2 Güvenliği

Port Güvenliği

- Porta varsayılan güvenlik politikası uygulanması
- Belirlenen sayıda MAC adresiyle iletişim
  - Aşımı halinde kapat
- MAC filtreleme

```
(config-if)# switchport mode access
(config-if)# switchport port-security
(config-if)# switchport port-security violation shutdown
(config-if)# switchport port-security maximum 3
(config-if)# switchport port-security mac-address mac-address sticky
(config-if)# switchport port-security aging time 10
(config-if)# switchport port-security aging type inactivity
```

BY NC ND

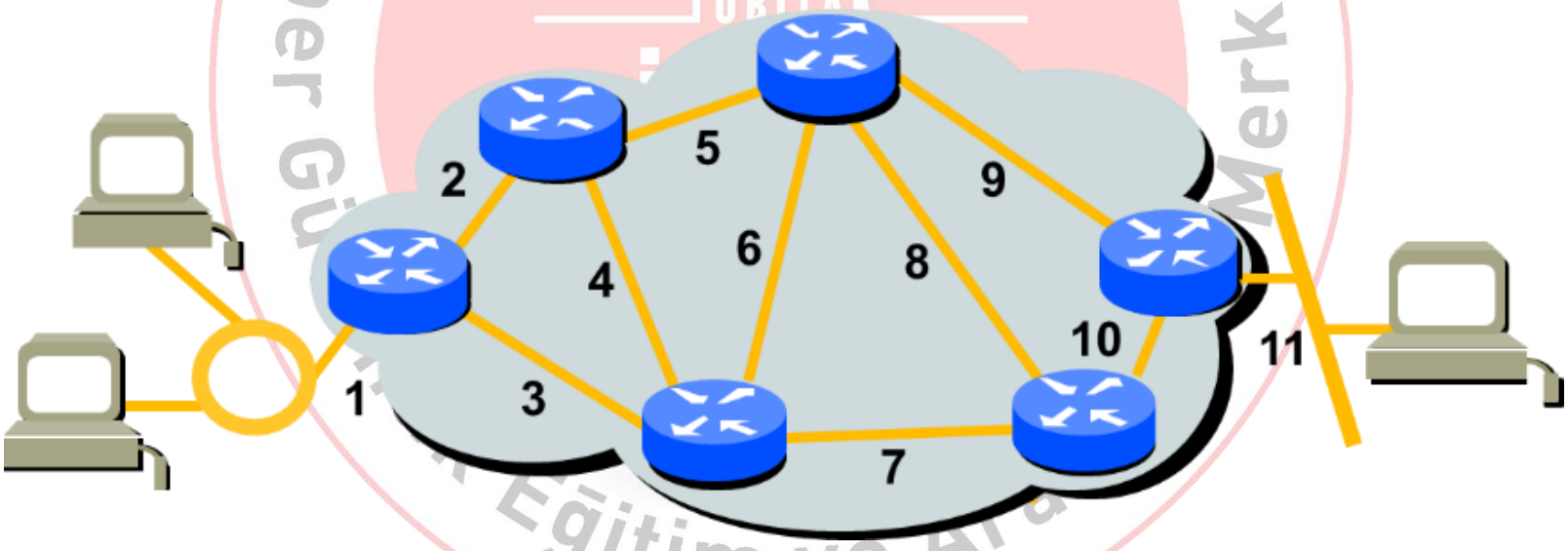
Ağ Katmanı (L3)

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

Ağ Katmanı (L3)

Uçtan uca veri yönlendirmesi için kullanılır.

- IP ve ICMP protokolleri, bir üst katmandan gelen segmentleri alıcıya uygun yoldan ulaştırmakla yükümlüdür.
- Segmentlere özel bir IP başlık bilgisi eklenir.



BY NC ND

IP

1982 – RFC 791

- Bağlantısız bir protokol
  - İletimin garantisi üst seviye protokollerle sağlanır.
- Yaygın olarak IPv4
  - 32 bitlik mantıksal adres
- IPv6 geçiş süreci

BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştı

IPv4

Onlu Düzendeki Noktalı Yazım

İlk oktet;

- 0-127 arasında ise A sınıfı,
- 128-191 arasında ise B sınıfı,
- 192-223 arasında ise C sınıfı olarak isimlendirilir

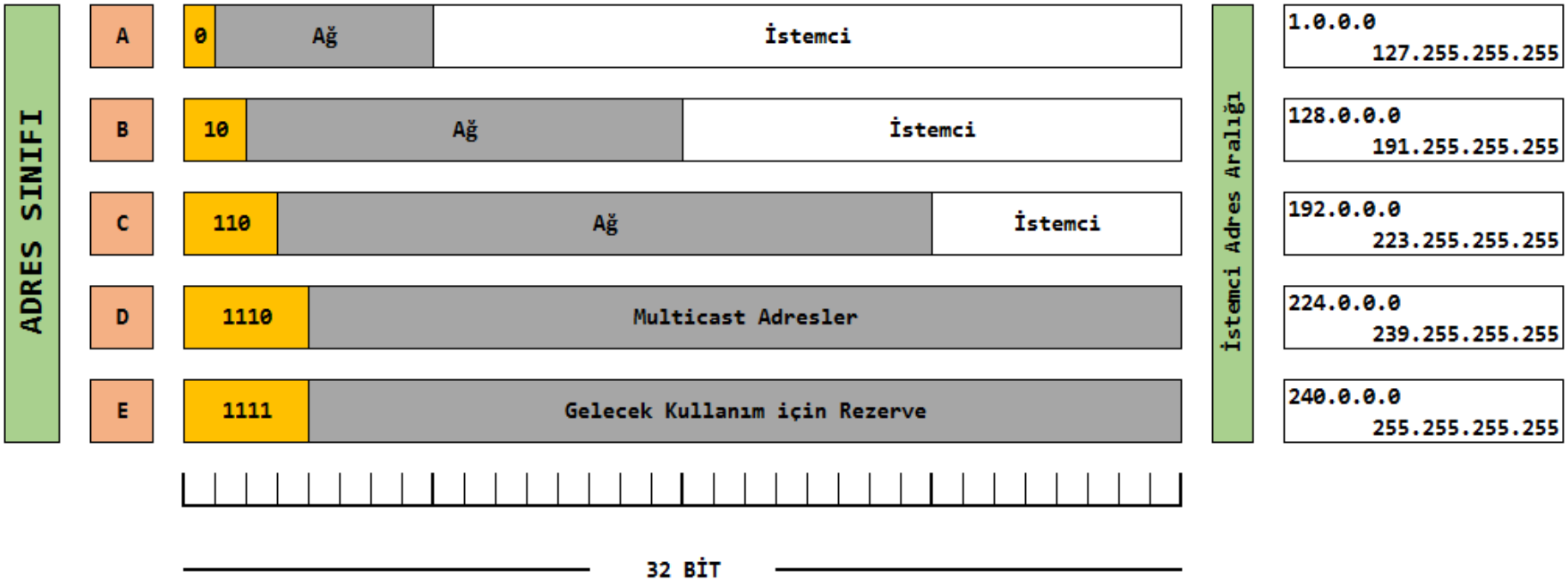
100000011 01101011 00000001 00001100

131 . 107 . 1 . 12

255 . 255 . 0 . 0

BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

IPv4 Adres Aralıkları



eğitim.sge.gov.tr
Eğitim ve Araştırma

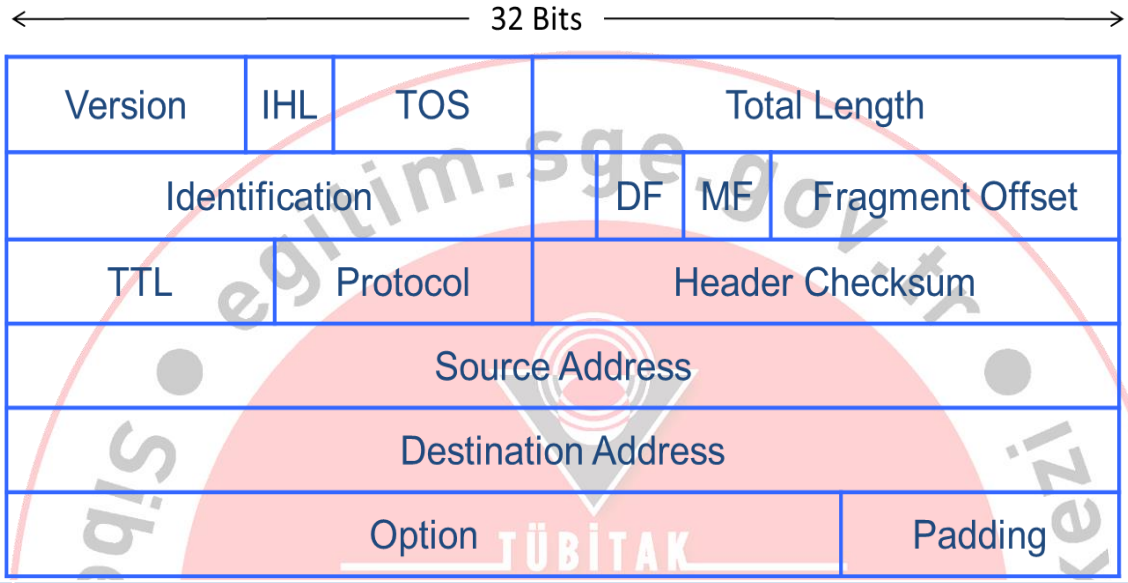
Özel Adres Blokları

İnternete direkt bağlanmayan, NAT veya vekil sunucusu aracılığı ile bağlanan cihazlarda kullanım için ayrılmıştır

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

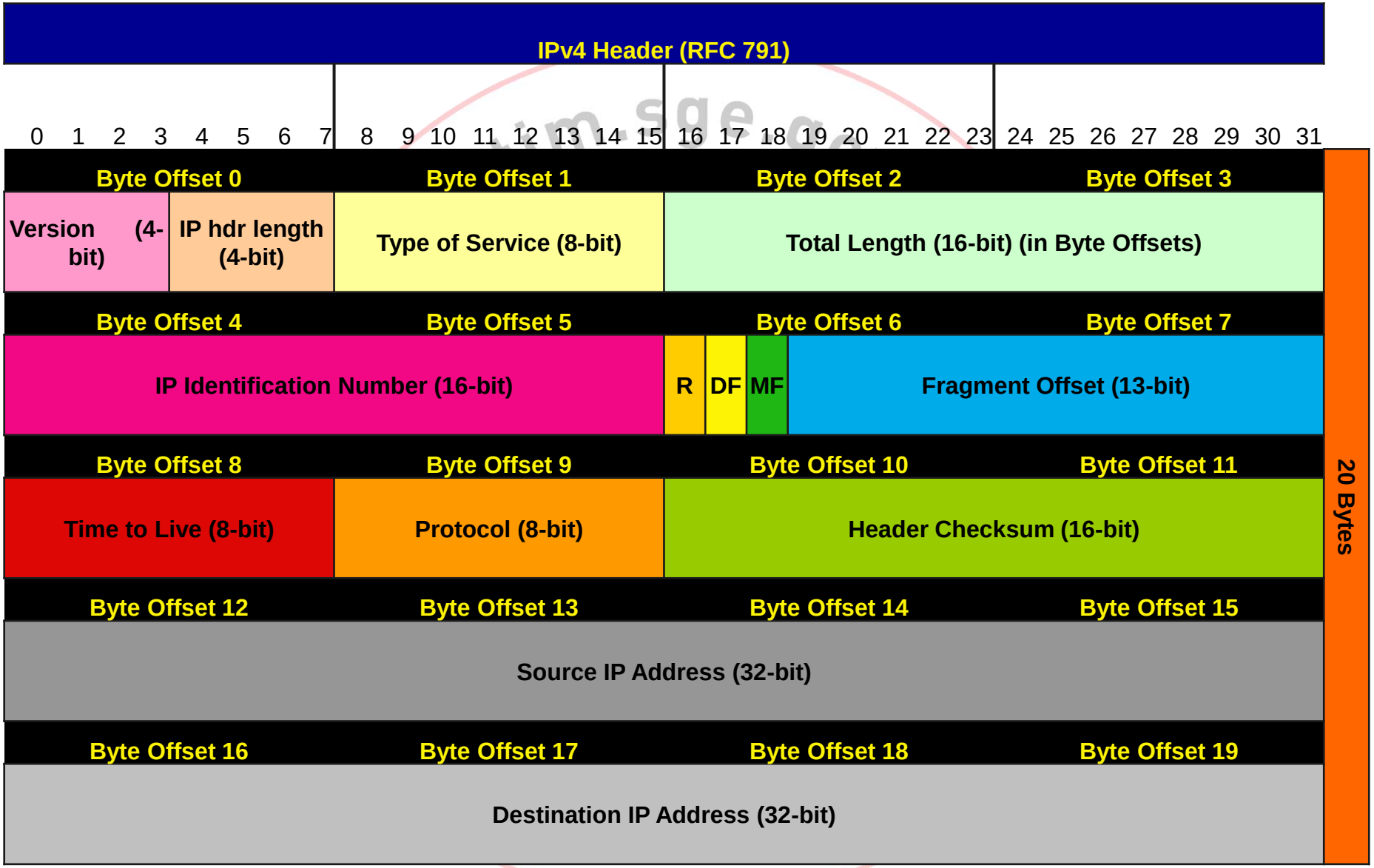
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

IPv4 Paket Başlığı



IP Başlık Alanı	İşlevi
Kaynak IP Adresi	Kaynak verinin IP adresi
Hedef IP Adresi	Gideceği yerin IP adresi
Tanımlama	Spesifik IP datagramını tanımlamak için kullanılır.
Protokol	Paketlerin TCP, UDP, ICMP ya da diğer protokollerle iletişimi ile ilgili
Checksum	IP başlığının bütünlüğünü kontrol etmek için kullanılan matematiksel hesaplama.
Time-to-Live (TTL)	Datagramın dolaşacağı ağ ucu sayısını belirler. Böylece paketlerin sürekli dolaşması (loop) engellenir.

IPv4 Paket Başlığı



BY NC ND

Uygulama - 1

Wireshark ile IP Paketi Analizi

No.	Time	Source	Destination	Protocol	Info
4	1.001207	172.16.1.10	172.16.1.5	ICMP	Echo (ping) request

```
▷ Frame 4 (74 bytes on wire, 74 bytes captured)
▽ Ethernet II, Src: 00:48:54:85:43:e3, Dst: 00:48:54:85:3d:05
    Destination: 00:48:54:85:3d:05 (DigitalS_85:3d:05)
    Source: 00:48:54:85:43:e3 (DigitalS_85:43:e3)
    Type: IP (0x0800)
▽ Internet Protocol, Src Addr: 172.16.1.10 (172.16.1.10), Dst Addr: 172.16.1.5 (172.16.1.5)
    Version: 4
    Header length: 20 bytes
  ▽ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..0. = ECN-Capable Transport (ECT): 0
      .... ...0 = ECN-CE: 0
    Total Length: 60
    Identification: 0x04f5 (1269)
  ▽ Flags: 0x00
      0... = Reserved bit: Not set
      .0.. = Don't fragment: Not set
      ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
    Header checksum: 0xdb9c (correct)
    Source: 172.16.1.10 (172.16.1.10)
    Destination: 172.16.1.5 (172.16.1.5)
```

```
0000  00 48 54 85 3d 05 00 48  54 85 43 e3 08 00 45 00   .HT.=..H T.C...E.
0010  00 3c 04 f5 00 00 80 01  db 9c ac 10 01 0a ac 10   .<...... ........
0020  01 05 08 00 da 5b 02 00  71 00 61 62 63 64 65 66   .....[.. q.abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Internet Protocol (ip), 20 by | P: 227 D: 227 M: 0

BY NC ND

IP Sahteciliği

İstenilen IP adresinden TCP/IP paketleri (TCP, UDP, IP, ICMP, HTTP, SMTP, DNS vb.) gönderebilme işlemi

DDoS saldırılarında önem kazanır.

stateful olmayan protokollerle gerçekleştirilenler için geçerlidir.

hping

```
# hping3 -a <sahte_ip_adresi> -p 80 -S -c 4 www.sirket.com.tr
```

Siber Güvenlik Eğitim ve Araştırma Merkezi
BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ

cc BY NC ND

Ağ Adres Dönüşümü

Adres dönüşümü kavramı

- Özel IP adresleri, gerçek IP adreslerine dönüştürülür.
- Dış dünyadaki bilgisayarlar iç ağdaki bilgisayarların orijinal IP adreslerini **kesinlikle** bilemez.
- 3 farklı adres dönüşümü vardır:
  - Statik Ağ Adres Dönüşümü
  - Dinamik Ağ Adres Dönüşümü
  - Port Yönlendirme

SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

CC BY NC ND

Statik Adres Dönüşümü

Statik Ağ Adres Dönüşümü

Her bir bilgisayarın IP'si ayrı bir IP adresine dönüştürülmektedir.

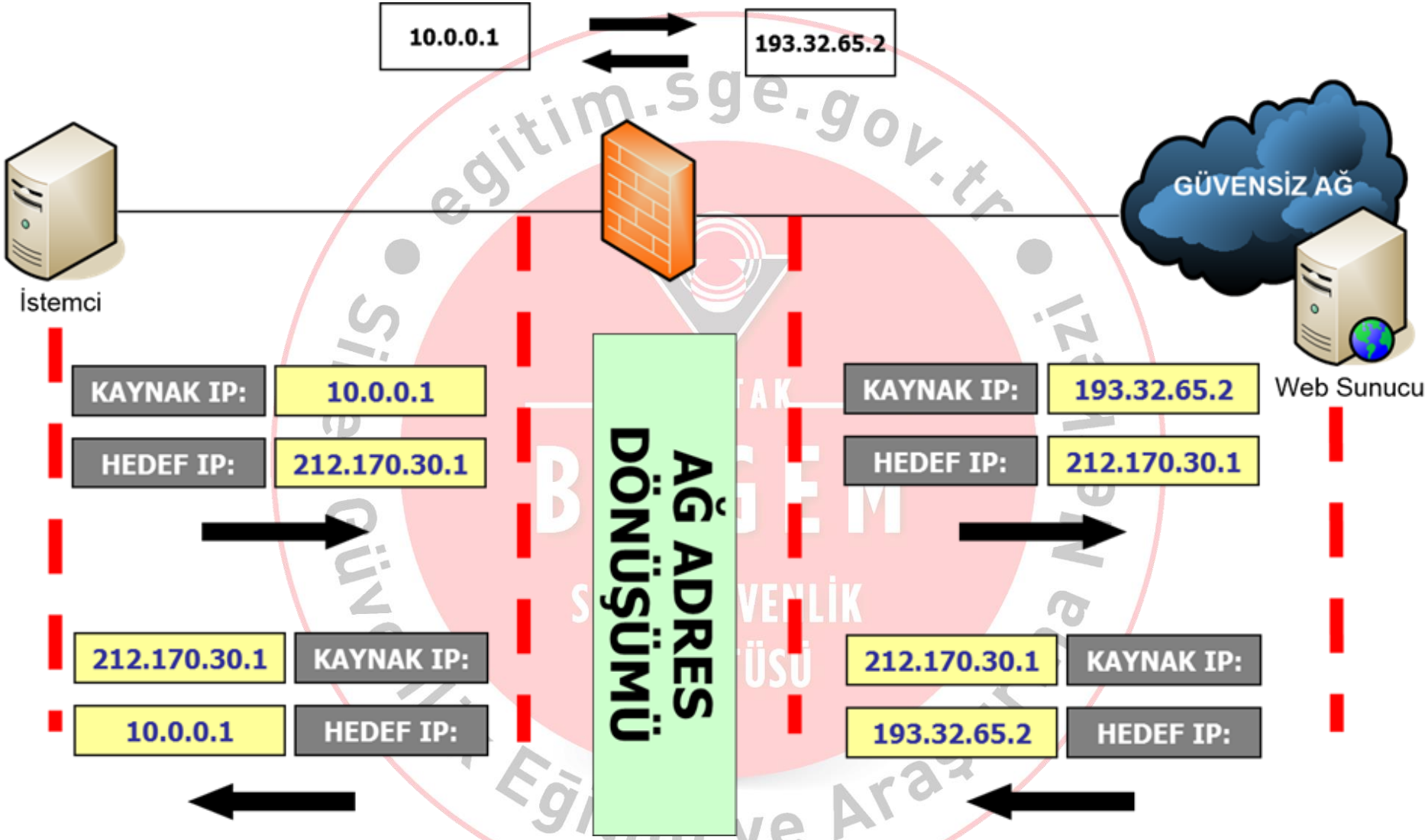
Statik ağ adres dönüşümü kuralları iki yönlü olarak tanımlanmalıdır.

10.0.0.1 ⇄ **193.32.65.2**

No	Kaynak IP	Hedef IP	Servis	Kaynak IP	Hedef IP	Servis
1	10.0.0.1	HERHANGİ	HERHANGİ	193.32.65.2	ORİJİNAL	ORİJİNAL
2	HERHANGİ	193.32.65.2	HERHANGİ	ORİJİNAL	10.0.0.1	ORİJİNAL

CC BY NC ND

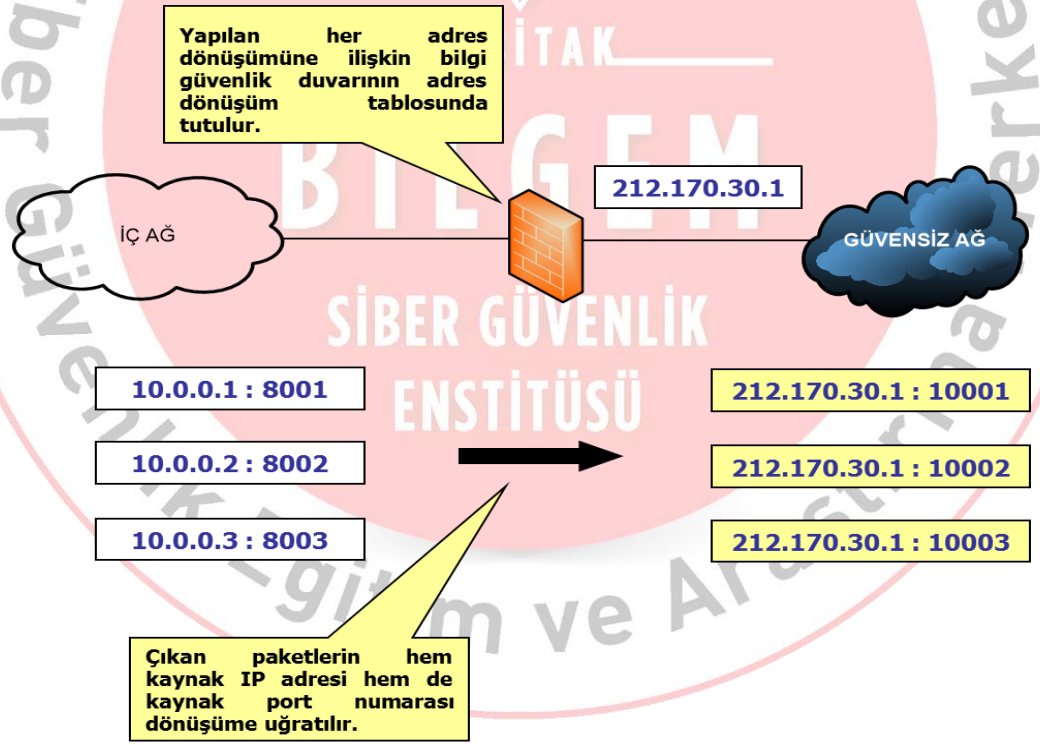
Statik Ağ Adres Dönüşümü - NAT



cc BY NC ND

Dinamik Ağ Adres Dönüşümü

- İç ağdaki IP adresleri tek bir gerçek IP adresine dönüştürülmektedir.
- Tek yönlü olarak çalışmaktadır.
  - Sadece iç ağdaki bilgisayarlar bağlantıyı başlatan taraf olabilir.



BY NC ND

Dinamik Ağ Adres Dönüşümü - PAT

IPtables kullanarak adres dönüşümü aşağıdaki gibi yapılabilir.

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
# iptables -A FORWARD -i eth0 -o eth1 -m state --state
RELATED,ESTABLISHED -j ACCEPT
# iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

IP yönlendirme etkin hale getirilmiş olmalıdır

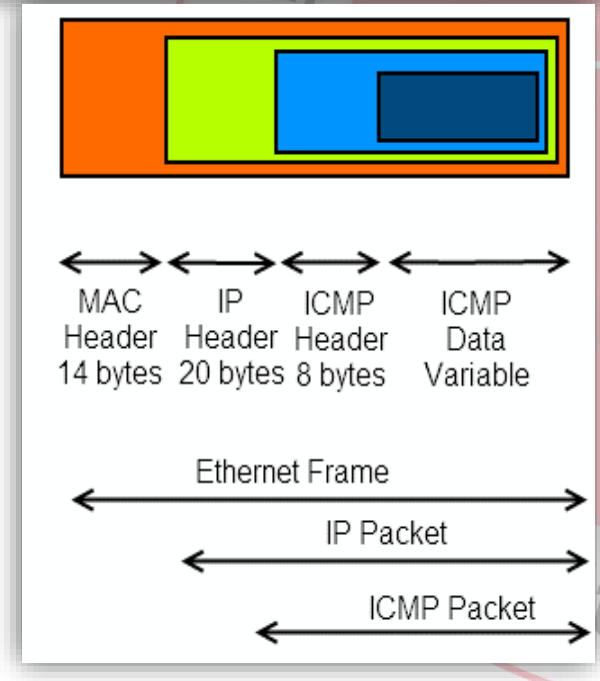
```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

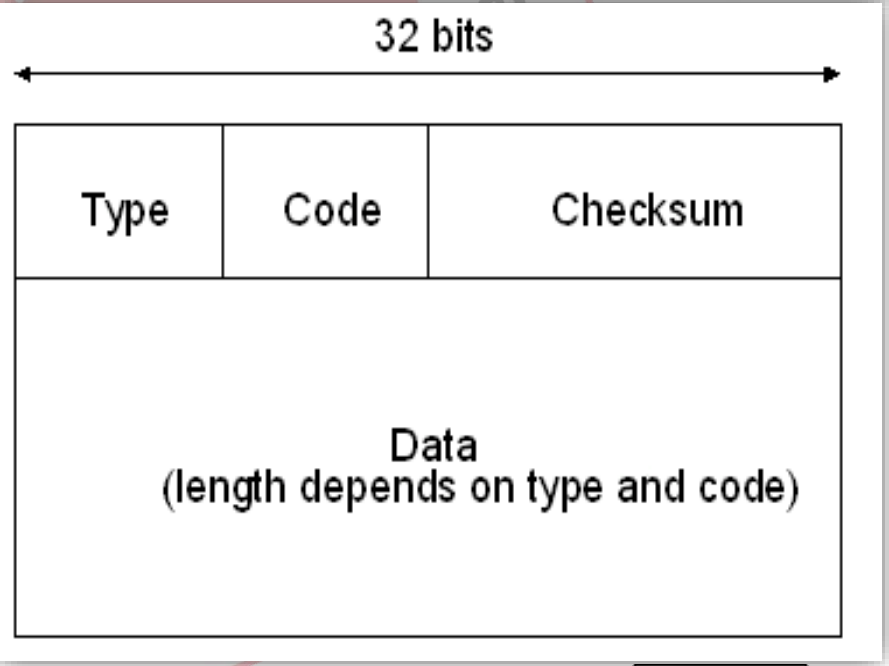
BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Güvenlik Eğitim ve Araştırma Merkezi

ICMP

Özellikler

- Kontrol amaçlı bir protokol
- Sistemler arası kontrol mesajları IP yerine ICMP üzerinden aktarılır
- Internet protokolünü daha güvenli hâle getirmez, sadece datagram iletimi sırasında meydana gelen hataların sebepleri ile ilgili bilgi sağlar.





cc BY NC ND

ICMP Paket Başlığı

ICMP Header (792)			
0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Byte Offset 0	Byte Offset 1	Byte Offset 2	Byte Offset 3
Message Type (8-bit)	Message Code (8-bit)	Checksum (16-bit)	
Byte Offset 4	Byte Offset 5	Byte Offset 6	Byte Offset 7
(contents depends on type and code)			

- 0 Echo reply
- 3 Destination Unreachable
  - 0 Net Unreachable
  - 1 Host Unreacheable
  - 2 Protocol Unreachable
  - 3 Port Unreachable
  - 4 Fragmentation Needed & Don't Fragment Flag Set
  - 5 Source Route Failed
  - 6 Destionation Network Unknown
  - 7 Destination Host Unknown
  - 8 Source Route Isolated
  - 9 Network Administratively Prohibited
  - 10 Host Administratively Prohibited
  - 11 Network Unreachable for TOS
  - 12 Host Unreachable for TOS
  - 13 Communication Administratively Prohibited
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 9 Router Advertisement
- 10 Router Selection
- 11 Time Exceeded
  - 0 Time to Live exceeded in transit
  - 1 Fragment Reassembly Time Exceeded
- 12 Parameter Problem
  - 0 Pointer indicates the error
  - 1 Missing a Required Option
  - 2 Bad Length
- 13 Timestamp Request
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply
- 17 Address Mask Request
- 18 Address Mask Reply
- 30 Traceroute

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

ICMP Mesaj Tipleri

Tip Kodu Değeri	ICMP Mesajın Tipi
0	Eko Yanıt - ping yanıtı (Echo Reply)
3	Hedefe Erişilemedi (Destination Not Reachable)
4	Kaynak Kapatma (Source Quench)
5	Yeniden Yönlendirme (Redirection Required)
8	Eko Yanıt - ping istemi (Echo Request)
9	Yönlendirici Tanıtımı
10	Yönlendirici İstemi
11	Zaman Aşımı - traceroute kullanır - (Time to Live Exceeded)
12	Parametre Problemi (Parameter Problem)
13	Timestamp İstemi (Timestamp Request)
14	Timestamp Yanıtı (Timestamp Reply)
15	Bilgi İstemi (Information Request)
16	Bilgi Yanıtı (Information Reply)
17	Adres Maskesi İstemi (Address Mask Request)
18	Adres Maskesi Yanıtı (Address Mask Reply)

BY NC ND

ICMP Saldırıları

DoS, ICMP Sweep ve Ping of Death

- **DoS:** hedef ve kaynak bilgisayarlara ICMP time exceeded veya destination unreachable paketleri göndererek TCP bağlantısının koparılması
- **ICMP Sweep:** Ağ taraması
- **Ping of Death:** 65535 bayttan büyük ping paketi oluşturularak çalışamaz hale getirmek hedeflenir (1997-98).

SİBER GÜVENLİK ENSTİTÜSÜ

BY NC ND

IPv6

Özellikler

- IPv4 adresleri 32 bit ve teorik olarak 4.294.967.296 adettir.
- IPv4 yetersiz kalınca 1998'de IPv6 geliştirildi.
  - 128 bit adres alanı

$$2^{32} = 4.294.967.296 \asymp 4,3 \cdot 10^{9}$$

IPv6

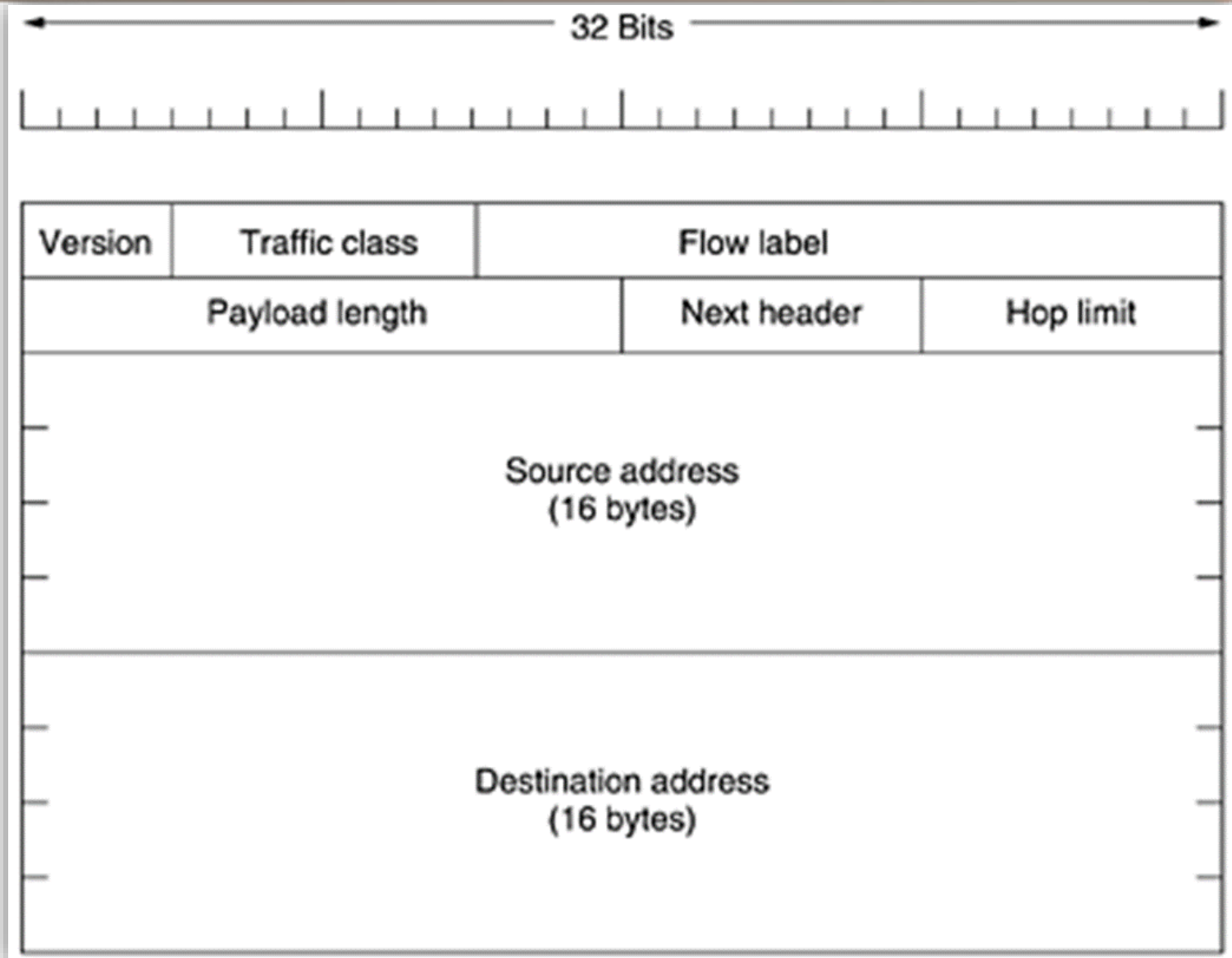
$$2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456 \asymp 3,4 \cdot 10^{38}$$

Örnek tarama süreleri karşılaştırması

- **IPv4 C sınıfı : 4,3 dk.**
- **IPv6 /64 : 585 yıl**

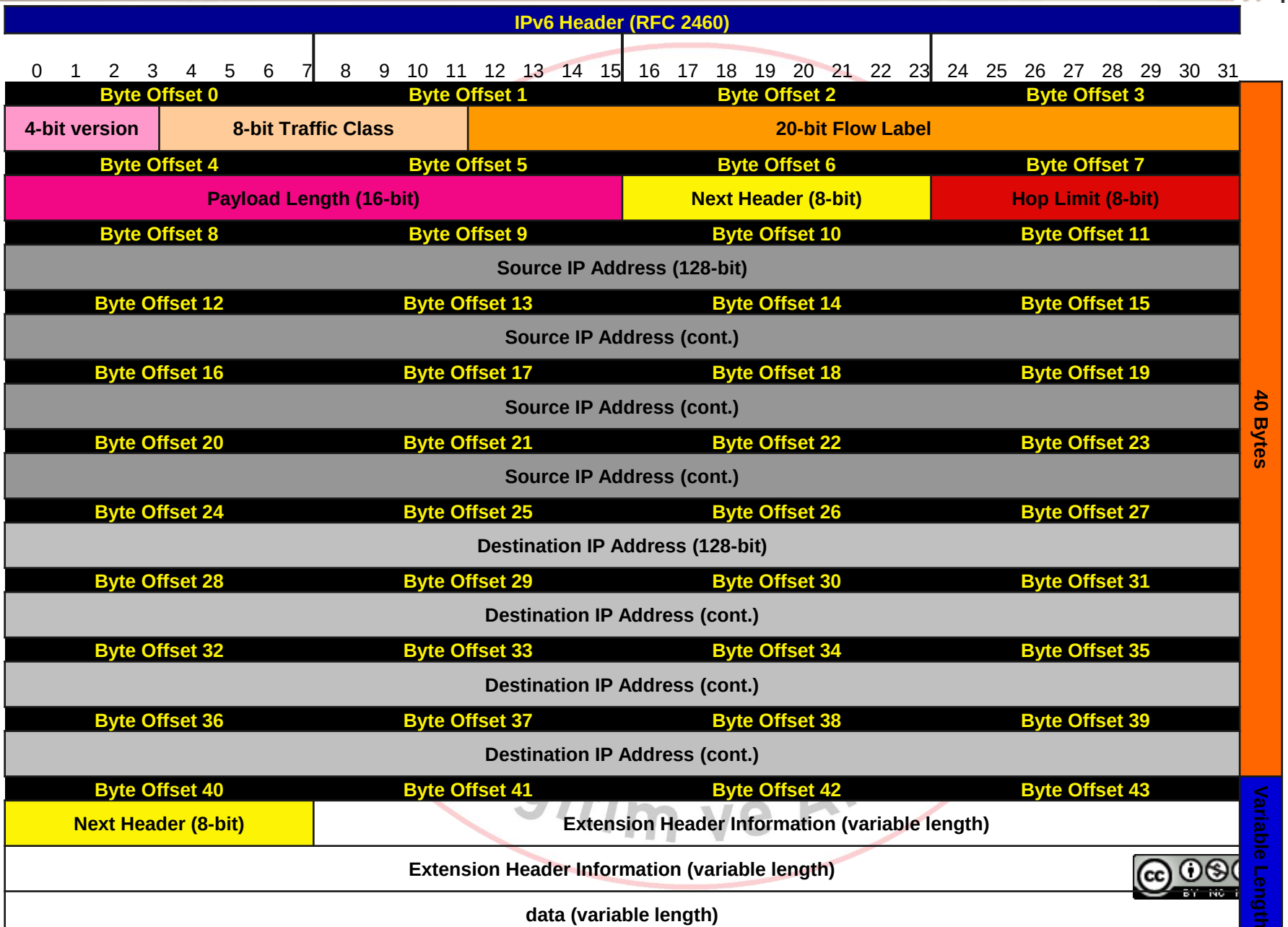
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Ortak Merkezi
CC BY NC ND

IPv6 Başlık Yapısı

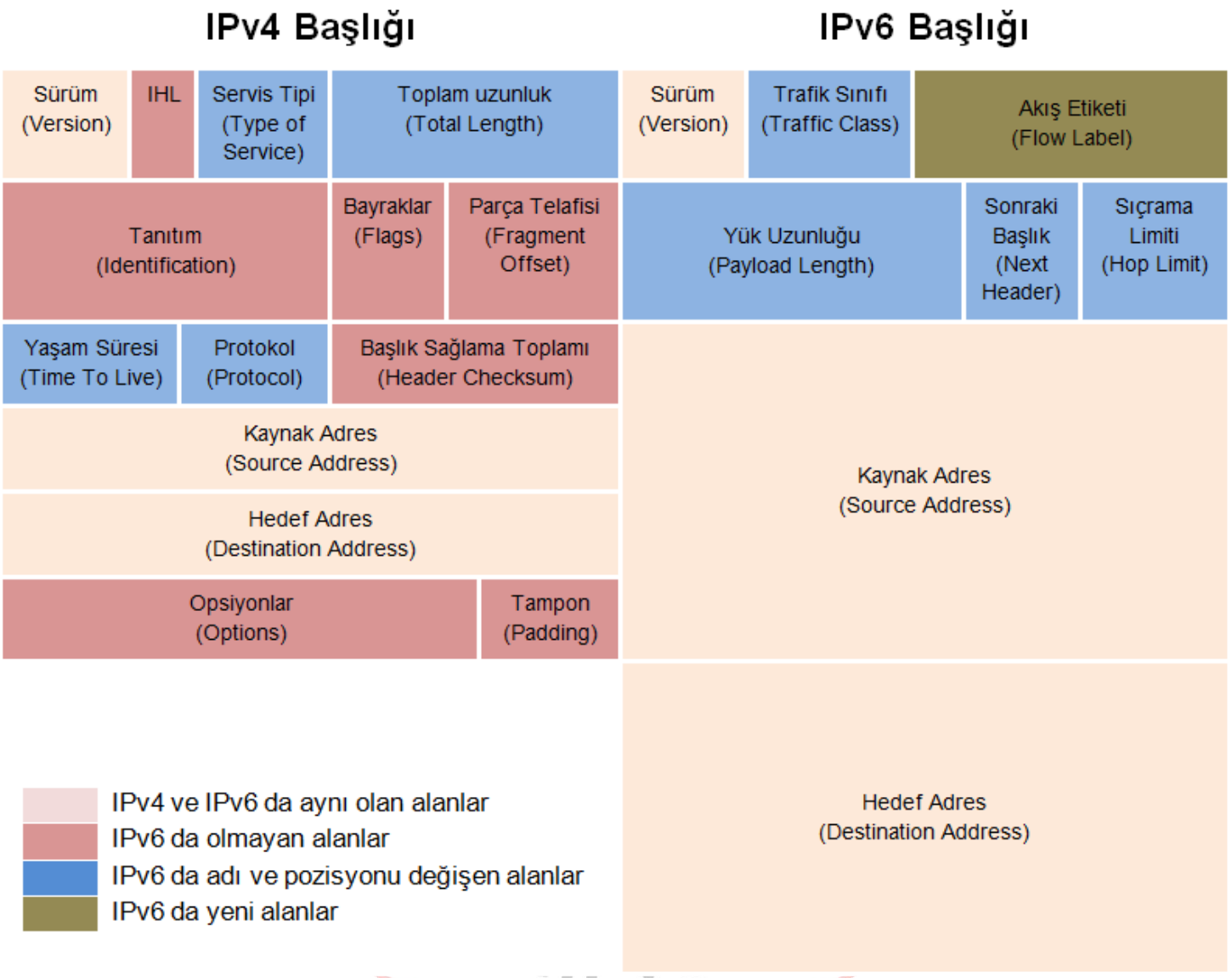


BY NC ND

IPv6 Başlık Yapısı



IPv4 vs IPv6



BY NC ND

IPv6 Adresleme

2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01:: Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi
eğitim.sge.gov.tr

IPv4 & IPv6

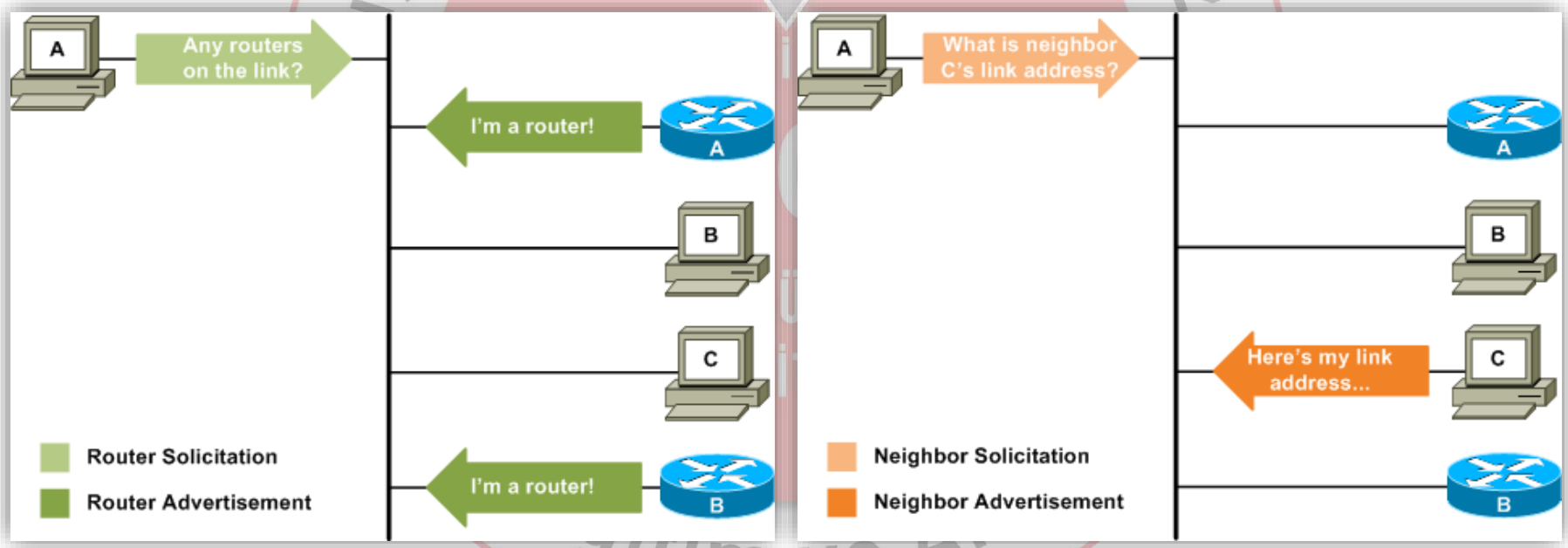
IPv4	192.168.0.5
HEX	C0A8:0005
IPv6	::ffff:C0A8:5

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
BİLEM

CC BY NC ND

Komşu Keşfi (Neighbor Discovery)

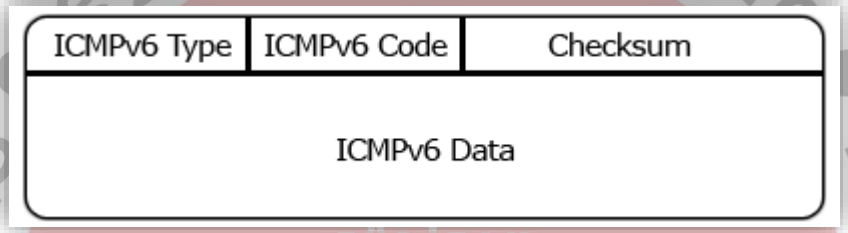
IPv4'te kullanılan yönlendirici keşfi (router discovery - RDISC), adres çözümleme protokolü (ARP) ve ICMP yeniden yönlendirme bileşenlerinin görevleri IPv6'da komşu keşfi tarafından yapılmaktadır.



CC BY NC ND

ICMPv6

ICMP Protokolünün IPv6 için uyarlanmış halidir.



Mesaj Tipi	Mesaj Adı
1	Hedef erişilemez
2	Paket çok büyük
3	Zaman Aşımı
4	Parametre Problemi
133	Yönlendirici Talebi
134	Yönlendirici İlanı
135	Komşu Talebi
136	Komşu İlanı

BY NC ND

IPv6'ya Yönelik Saldırılar

IPSec «desteğinin» zorunlu olması

Yönetilebilirlik ve cihazların işlem gücü açısından olası gözükmemektedir.

IPv6'ya Yönelik Saldırılar

- Paket Koklama
- Keşif Saldırıları
- ARP yerine Neighbor Discovery kullanılması
- Uzantı Başlıkları
- Ortadaki Adam Saldırısı (Man-in-the-Middle)
- Servis Dışı Bırakma

ENSTİTÜSÜ
nlik Eğitim ve Araştırm

IPv6 - Keşif

- IPv4 tarzı tarama çok zor
- IPv6 ile beraber DNS kullanımı, çok daha fazla önemli olacaktır.
- DNS üzerinden tarama - FQDN Enumeration

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

IPv6 - Servis Dışı Bırakma (DoS)

Broadcast adresi yok

Smurf/amplification tipi saldırılar mümkün değil

ICMPv6'nın hata mesajlarında, hedef adresinin çoklu gönderim adresi olarak tanımlanabilmesi

Tüm DHCPv6 adreslerini temsil eden FF05::1:3 ile DHCPv6 sunucuları

Adres uzayı çok büyük

NDP tablo boyutu sınırlı

TÜBİTAK
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

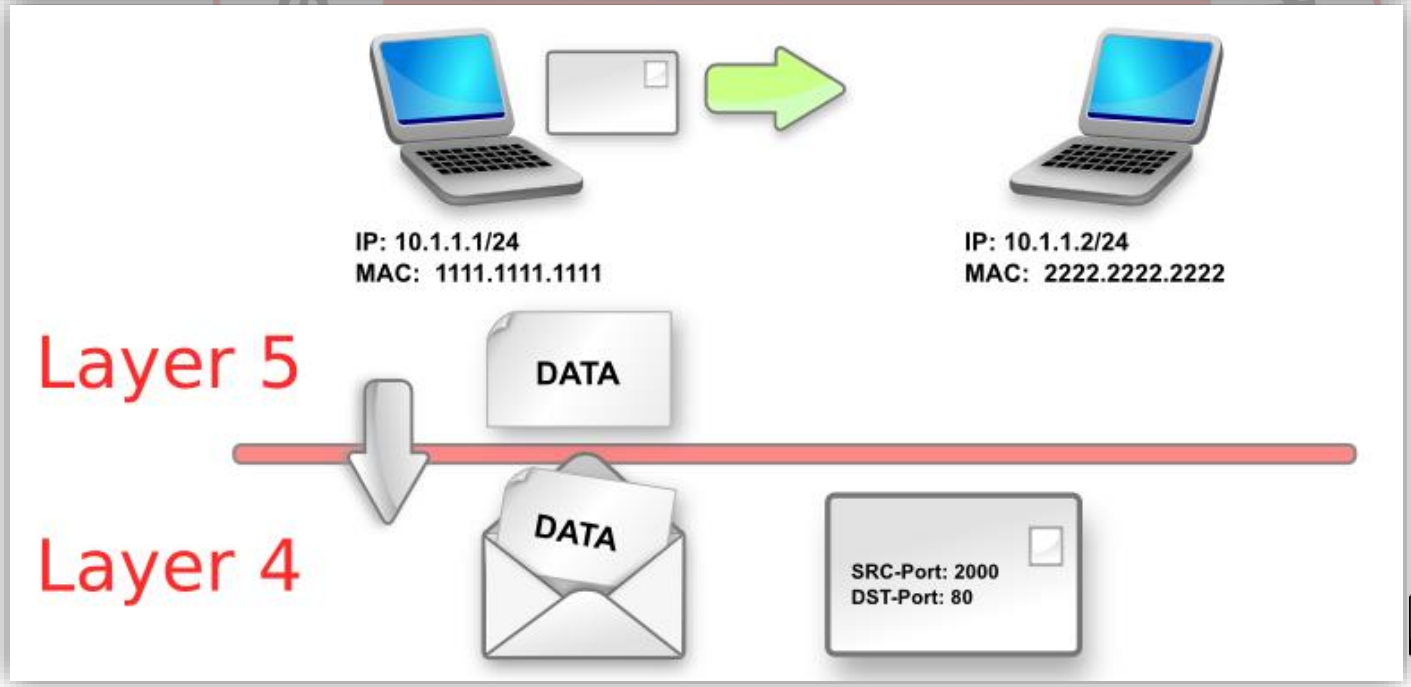
Taşıma Katmanı (L4)

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

Taşıma Katmanı (L4)

Özellikler

- Üst katmanlardan gelen veriyi ağ paketi boyutunda parçalara böler.
- Alt katmanlar ve üst katmanlar arasında geçit görevi görür.
- Alt katmanlar verinin ne olduğuna bakmadan karşı tarafa yollama işini yaparken, üst katmanlar da kullanılan donanım ile ilgilenmeden verinin kendisi ile uğraşabilirler.



BY NC ND

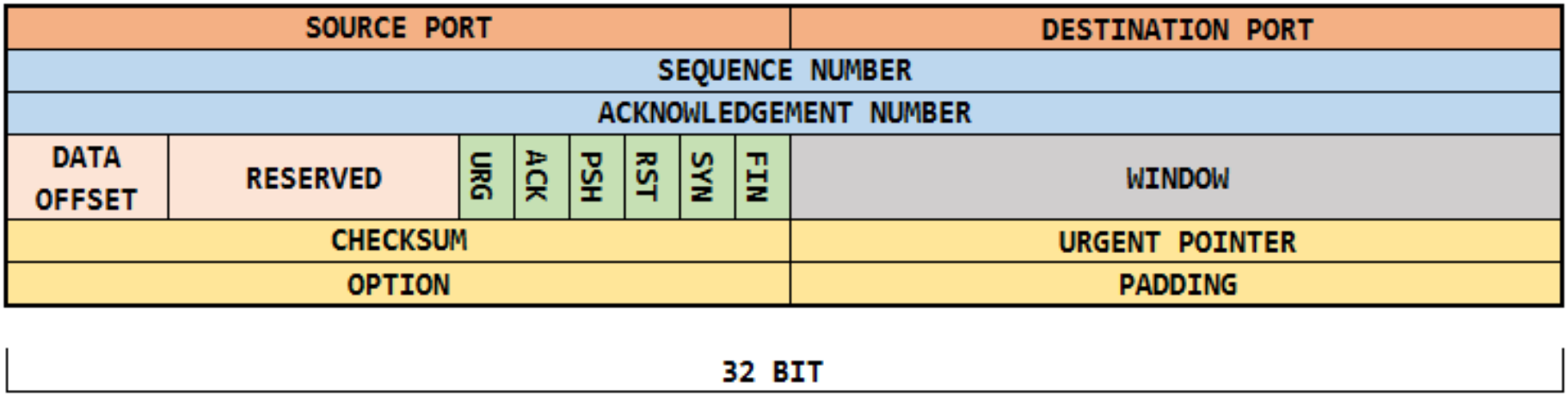
TCP

Özellikler

- Bağlantı yönelimli bir protokoldür (Connection-Oriented).
- Verilere sıra numarası ekler (Sequence Number).
- Veriler, parçalara bölünerek yollanabilir.
- Güvenilirdir. Kaybolan veri tekrar yollanır. Verinin hedefe gidip gitmediğini kontrol eder.
- Akış kontrolü vardır (Flow Control).
- Çift yönlüdür (Full Duplex).

SİBER GÜVENLİK ENSTİTÜSÜ
Ulusal Siber Güvenlik Eğitim ve Araştırma

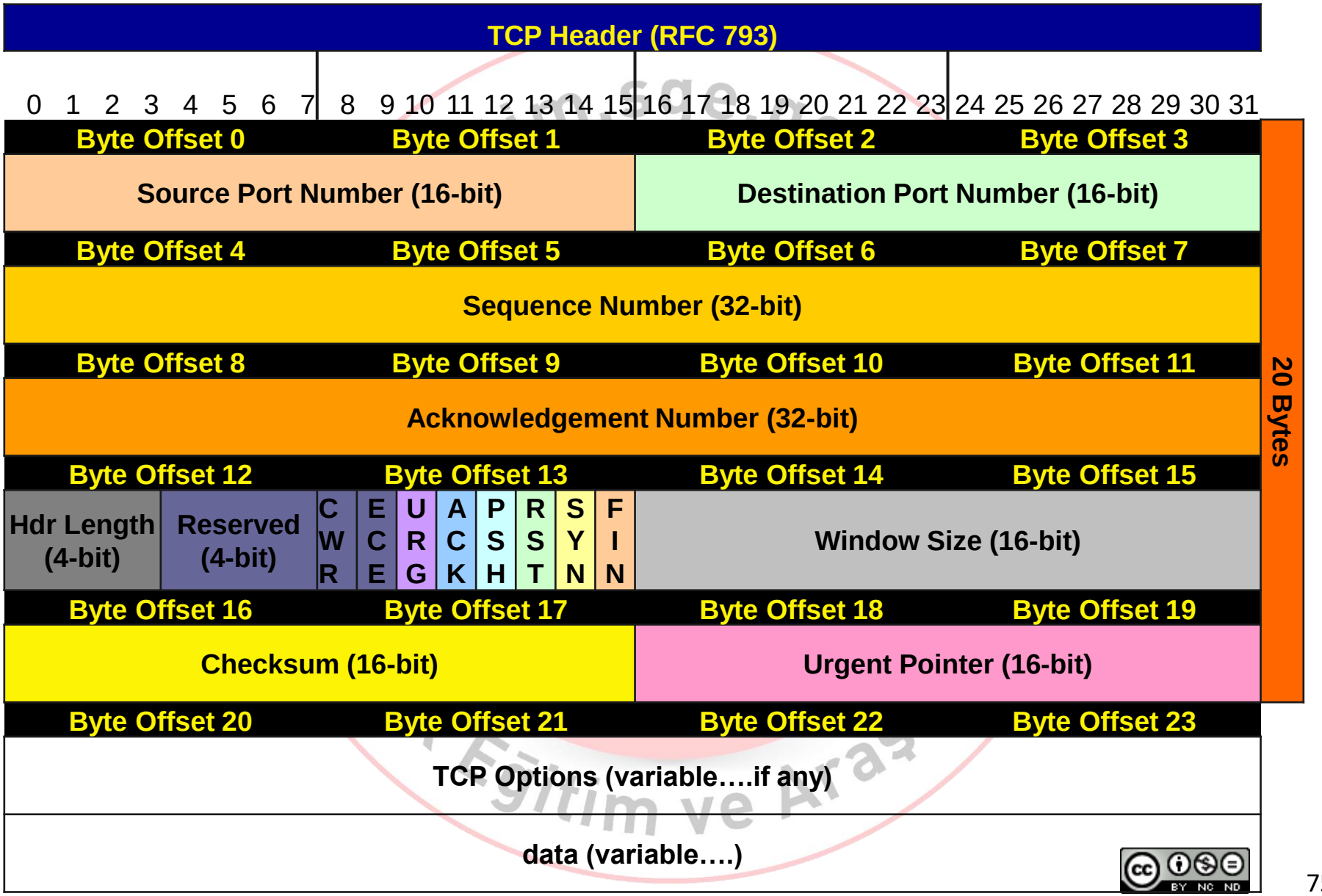
TCP Paket Başlığı



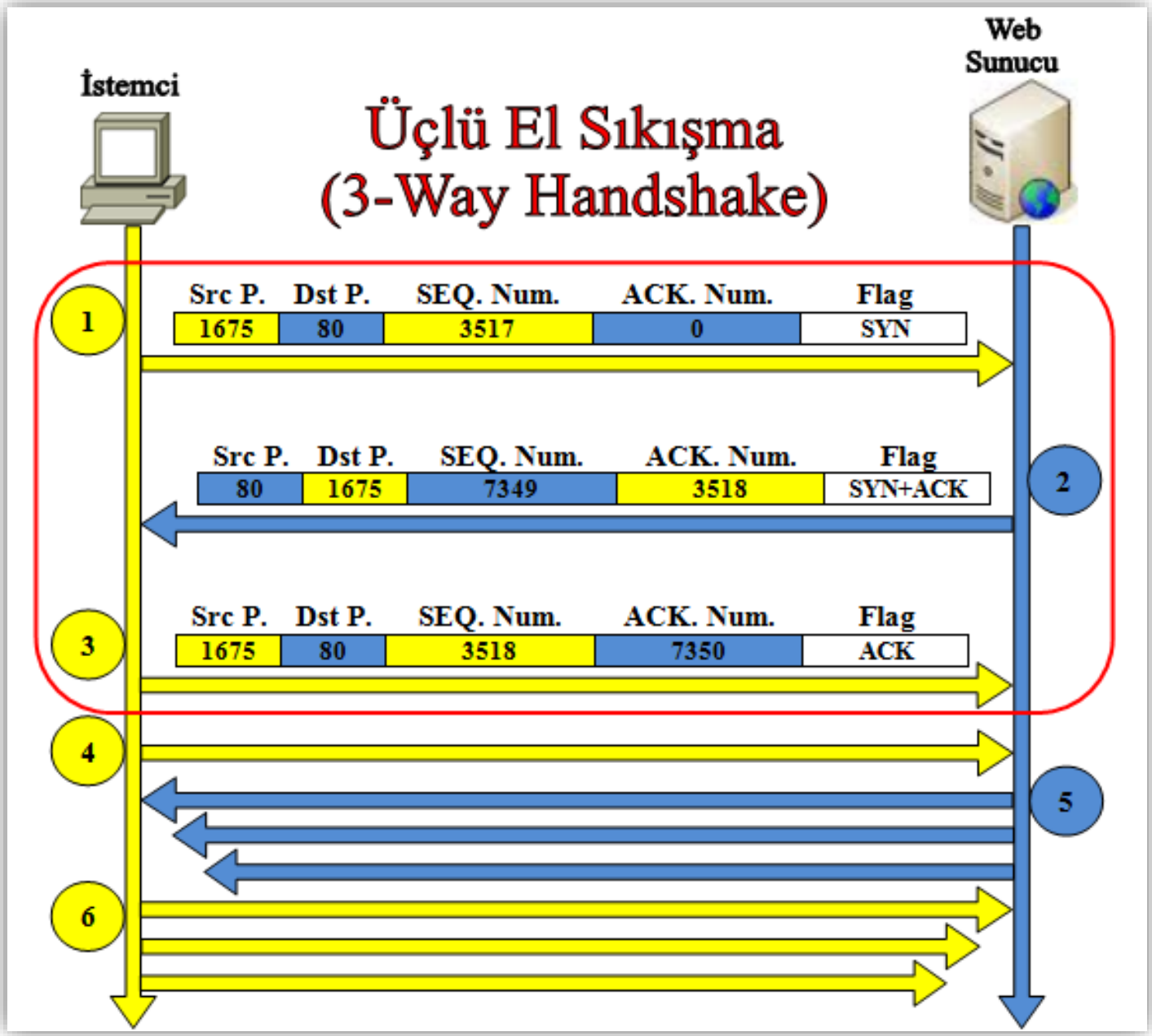
Alan	İşlevi
Source Port	Gönderenin TCP portu.
Destination Port	Alanın (hedefin) TCP portu.
Sequence Number	TCP segmenti içindeki birinci baytın sıra numarası.
Window	TCP ara bellek (buffer) alanının şu anki mevcut büyüklüğü.
TCP Checksum	TCP başlığı ve verisinin bütünlüğünü kontrol için kullanılır.

cc BY NC ND

TCP Paket Başlığı



TCP: Oturum Kurma



BY NC ND

Uygulama 2 – TCP 3'lü El Sıkışma Analizi

«_Uygulama 2 - TCP 3'lü El Sıkışma.pdf»

dosyasını açınız.

Lütfen uygulamayı tamamlayınız!

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

TCP: TCP 3'lü El Sıkışma Paket Analizi

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.104	216.18.166.136	TCP	74	49859 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
2	0.307187	216.18.166.136	192.168.1.104	TCP	74	http > 49859 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1440 TSval
3	0.307372	192.168.1.104	216.18.166.136	TCP	66	49859 > http [ACK] Seq=1 Ack=1 Win=17136 Len=0 TSval=305793 TSecr

```
⊞ Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: Tp-LinkT_38:f1:00 (74:ea:3a:38:f1:00), Dst: Intel_90:29:61 (00:19:d2:90:29:61)
⊞ Internet Protocol Version 4, Src: 216.18.166.136 (216.18.166.136), Dst: 192.168.1.104 (192.168.1.104)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 49859 (49859), Seq: 0, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 49859 (49859)
    [Stream index: 0]
    Sequence number: 0    (relative sequence number)
    Acknowledgment number: 1    (relative ack number)
    Header length: 40 bytes
  ⊟ Flags: 0x012 (SYN, ACK)
      000. .... .... = Reserved: Not set
      ...0 .... .... = Nonce: Not set
      .... 0... .... = Congestion Window Reduced (CWR): Not set
      .... .0.. .... = ECN-Echo: Not set
      .... ..0. .... = Urgent: Not set
      .... ...1 .... = Acknowledgment: Set
      .... .... 0... = Push: Not set
      .... .... .0.. = Reset: Not set
    ⊞ .... .... ..1. = Syn: Set
      .... .... ...0 = Fin: Not set
    Window size value: 5792
    [Calculated window size: 5792]
  ⊞ Checksum: 0xf8e7 [validation disabled]
  ⊞ Options: (20 bytes), Maximum segment size, No-Operation (NOP), No-Operation (NOP), Timestamps, No-Operation (NOP), Window scale
  ⊞ [SEQ/ACK analysis]

0010  00 3c 00 00 40 00 2d 06  0d 11 d8 12 a6 88 c0 a8   .<..@.-. ........
0020  01 68 00 50 c2 c3 29 91  a6 b8 d5 e2 df b5 a0 12   .h.P..). ........
0030  16 a0 f8 e7 00 00 02 04  05 a0 01 01 08 0a 4e 62   ........ ......Nb
0040  b9 10 00 04 aa 62 01 03  03 09                     .....b.. ..
```

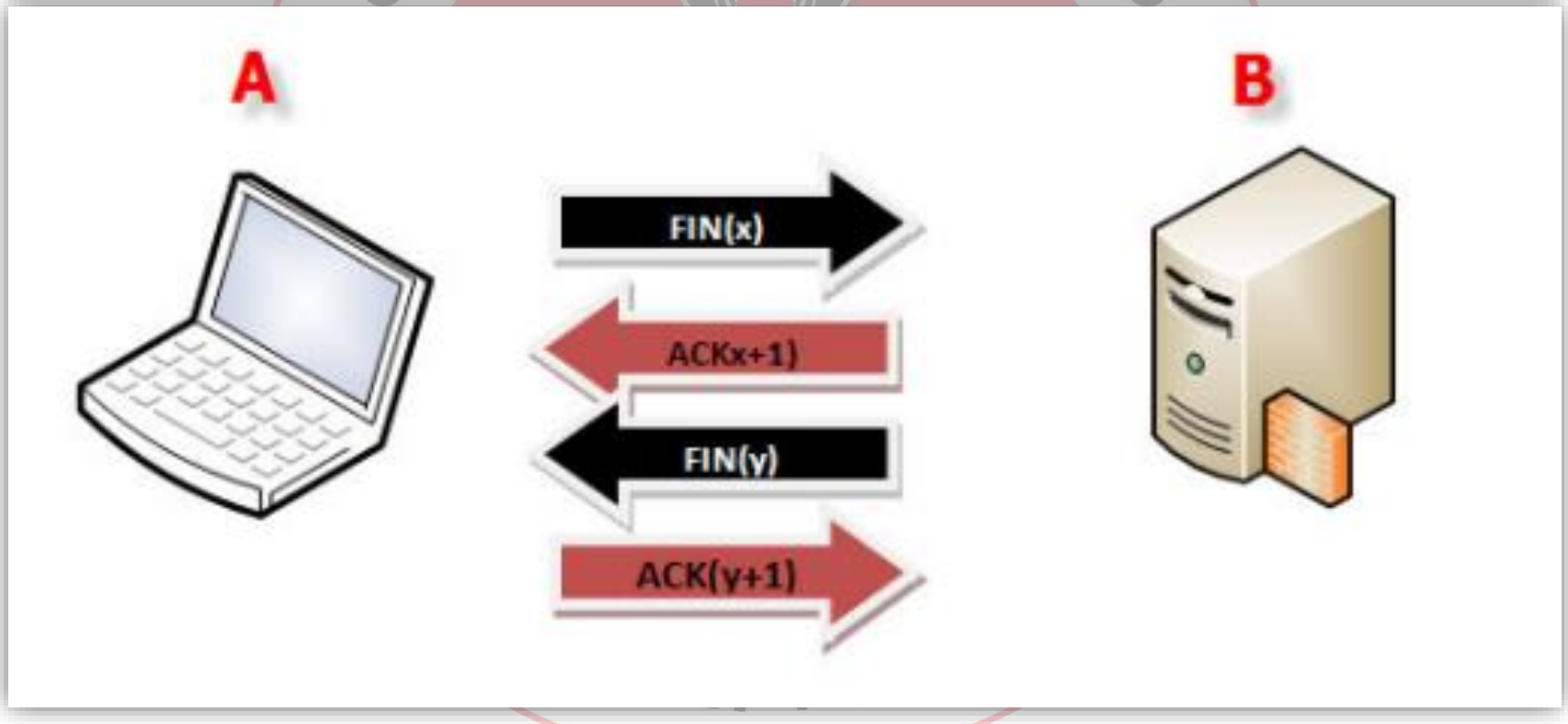
Tcpdump ile nasıl tespit edilir?

BY NC ND

TCP: Oturum Sonlandırma

Oturum sonlandırma, her iki tarafın da anlaşması ile tamamlanır.

Taraflardan birinin ilgili bayraklı paketi göndermemesi, geç göndermesi bağlantının sağlıklı olarak sonlanmasına engel olur.



BY NC ND

UDP

İletişim sırasında bağlantı oluşturmaz.

Hata denetimi yok.

Kaybolan paketin yeniden gönderilmesi söz konusu değildir.

Veri aktarımı daha hızlıdır.

Doğrulama mekanizması yok.

Sahteciliğe açık.

BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Güvenlik Eğitim ve Araştırma Me

CC BY NC ND

UDP Paket Başlığı

SOURCE PORT	DESTINATION PORT
LENGTH	CHECKSUM

32 BIT

Alan	İşlevi
Source Port	Gönderen bilgisayarın UDP portu.
Destination Port	Alıcı bilgisayarın UDP portu.
Checksum	UDP başlığı ve verisinin kontrolü için kullanılır.

TÜBİTAK ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma Merkezi

UDP Paket Başlığı

UDP Header (RFC 768)			
0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
Byte Offset 0	Byte Offset 1	Byte Offset 2	Byte Offset 3
Source Port Mumber (16-bit)		Destination Port Number (16-bit)	
Byte Offset 4	Byte Offset 5	Byte Offset 6	Byte Offset 7
Length (16-bit)		Checksum (16-bit)	
Byte Offset 8	Byte Offset 9	Byte Offset 10	Byte Offset 11
data (variable….)			

Siber Güvenlik Enstitüsü
Güvenlik Eğitim ve Araştırma

2. Bölüm

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Bu doküman, alıntı vererek kullanılabilir ya da paylaşılabilir ancak değiştirilemez ve ticari amaçla kullanılamaz.
Detaylı bilgiye https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.tr bağlantısından erişebilirsiniz.

Sunum İçeriği

- Paket Oluşturma
- TCP/IP ve Farklı Durumlar
- Uygulama Katmanı
- Ağ Güvenliği: Protokoller
- DOS/DDOS Saldırıları

Paket Oluşturma

TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

Paket Oluşturma

Neden paket oluşturulur?

- Normal ve normal olmayan paket izlerini gözlemlemek için (Fingerprinting)
- Saldırı tespit ve önleme sistemlerini atlatmak için
- Paketleri gizlemek ve iletilen mesajları saklamak için

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

Paket Oluşturma Araçları

Hangi araçlar kullanılır?

- hping3
- sendip
- nemesis
- scapy

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

CC BY NC ND

Hping3 ile Paket Oluşturma

TÜBİTAK

SYN paketlerinin oluşturulması

```
# hping3 -S www.sunucu.com -p 80 -c 3
```

UDP paketlerinin oluşturulması

```
# hping3 -U www.sunucu.com -p 53 -c 3
```

ICMP paketlerinin oluşturulması

```
# hping3 -1 www.sunucu.com -c 3
```

Port tarama işlemi

```
# hping3 -S www.sunucu.com -p  ++440
```

440.porttan itibaren tarama

SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

CC BY NC ND

Nmap ile İşletim Sistemi Tespiti

nmap –O 172.16.1.10

Starting Nmap

Nmap scan report for 172.16.1.10

Host is up (0.00015s latency).

Not shown: 992 filtered ports

PORT STATE SERVICE

53/tcp open domain

445/tcp open microsoft-ds

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port

Device type: general purpose

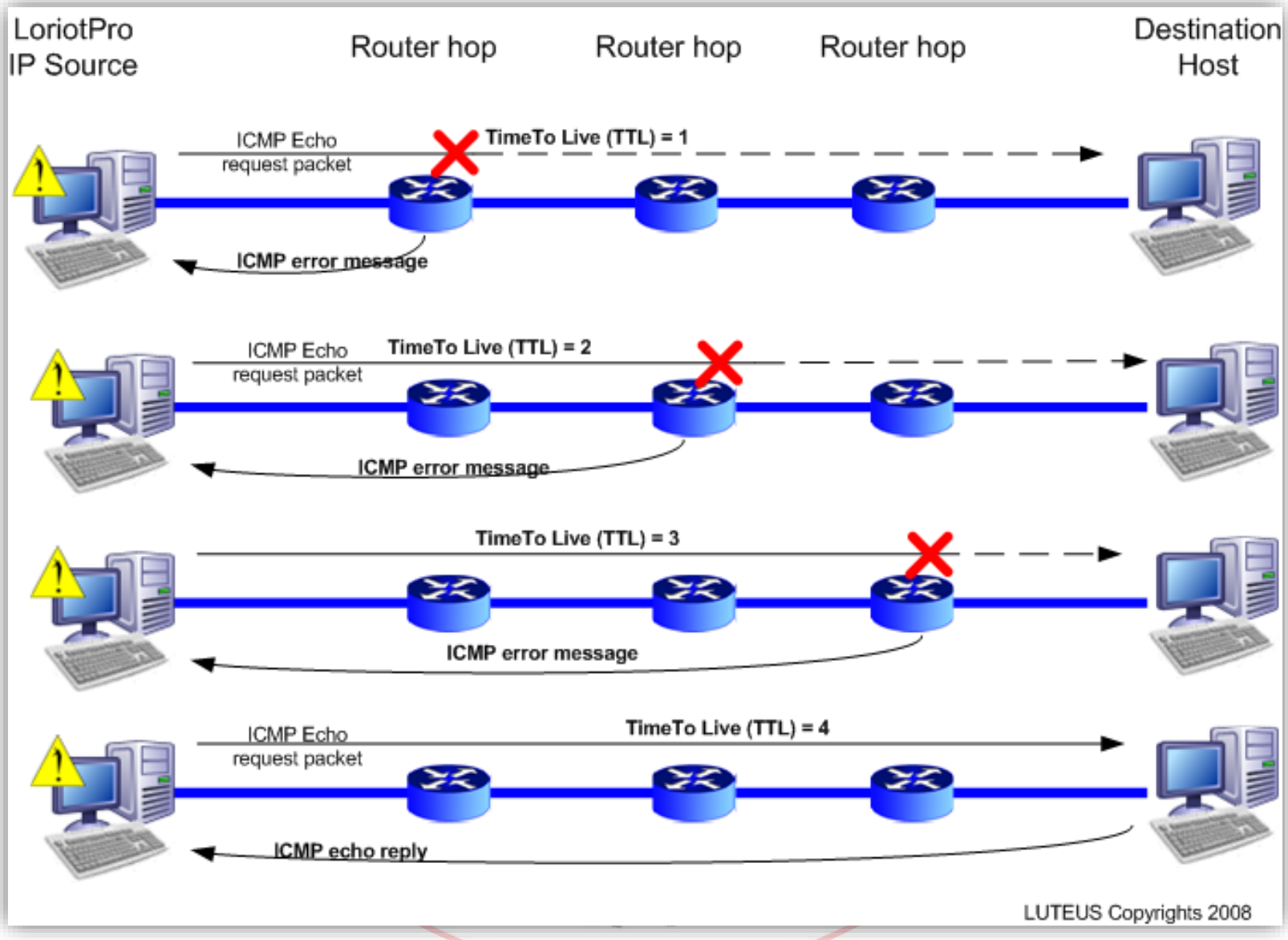
Running: Microsoft Windows 7|Vista|2008

BY NC ND

TCP/IP ve Farklı Durumlar

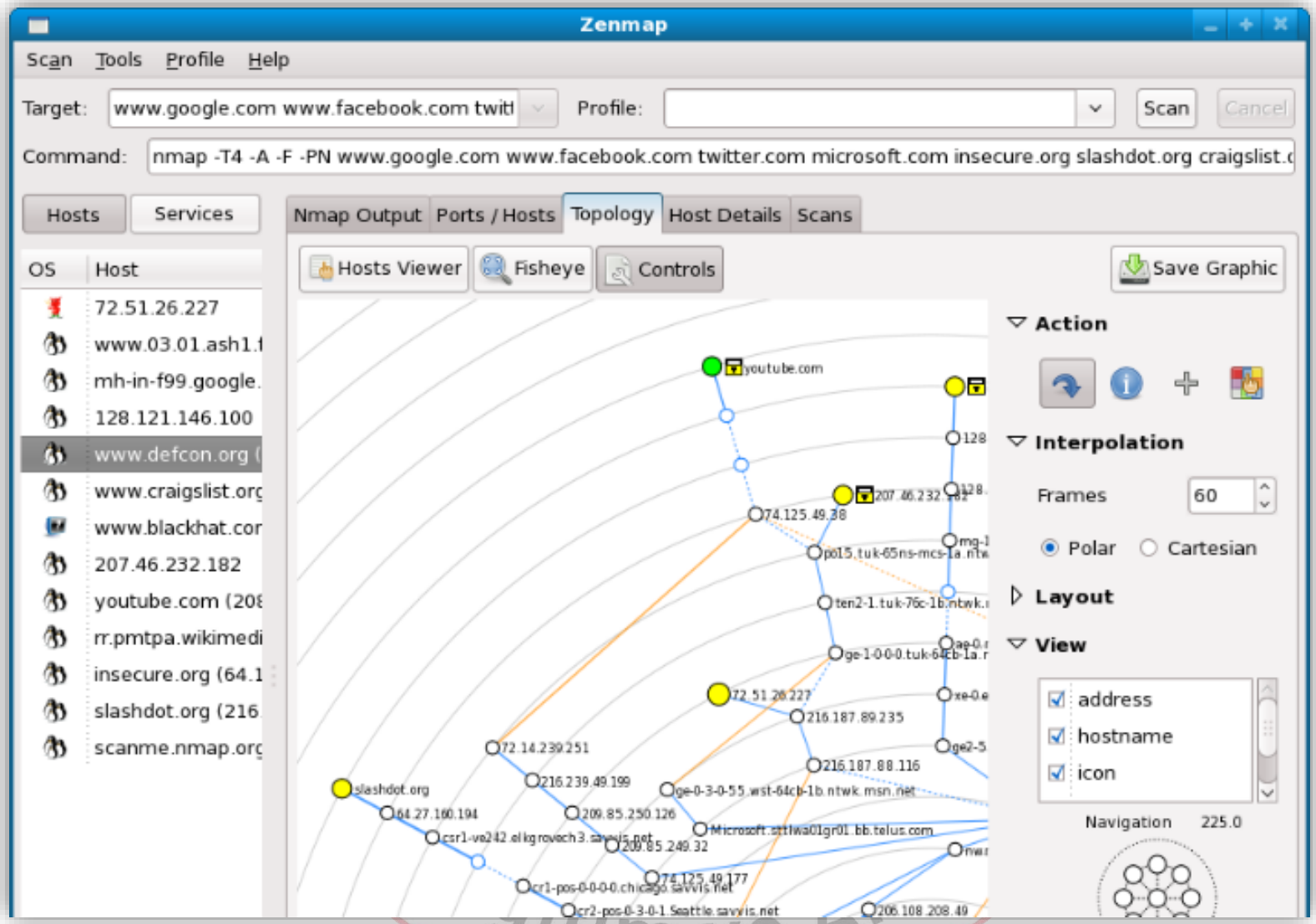
TÜBİTAK
egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

traceroute



BY NC ND

Tcptraceroute



nmap -Pn --traceroute -p 8000 www.sunucu.com

ICMP Üzerinden Veri Aktarımı

ICMP Echo Request paketlerinin içerisindeki padding için ayrılan bölümden faydalanılarak veri iletimi

```
# while read -n12 line;do ping 10.0.2.16 -p $(echo $line|xxd -p -u) -c 1;done < dosya.txt
```

Filter: icmp Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
12	3.28735700	192.168.4.187	192.168.4.101	ICMP	98	Echo (ping) reques
13	3.28748400	192.168.4.101	192.168.4.187	ICMP	98	Echo (ping) reply

```
Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Vmware_06:cd:4b (00:0c:29:06:cd:4b), Dst: Hewlett-_c2:96:df (78:e7:
Internet Protocol Version 4, Src: 192.168.4.187 (192.168.4.187), Dst: 192.168.4.101 (
Internet Control Message Protocol
```

```
0000  78 e7 d1 c2 96 df 00 0c  29 06 cd 4b 08 00 45 00   x....... )..K..E.
0010  00 54 00 00 40 00 40 01  b0 38 c0 a8 04 bb c0 a8   .T..@.@. .8......
0020  04 65 08 00 5a e7 69 42  00 01 85 9f 24 51 83 5a   .e..Z.iB ....$Q.Z
0030  02 00 69 6e 67 0a 50 6f  72 74 73 75 7a 50 69 6e   ..ing.Po rtsuzPin
0040  67 0a 50 6f 72 74 73 75  7a 50 69 6e 67 0a 50 6f   g.Portsu zPing.Po
0050  72 74 73 75 7a 50 69 6e  67 0a 50 6f 72 74 73 75   rtsuzPin g.Portsu
0060  7a 50                                              zP
```

CC BY NC ND

Uygulama 3 – ICMP ile Veri Aktarımı

«_Uygulama 3 - ICMP ile Veri Aktarımı.pdf»

dosyasını açınız.

Lütfen uygulamayı tamamlayınız!

eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

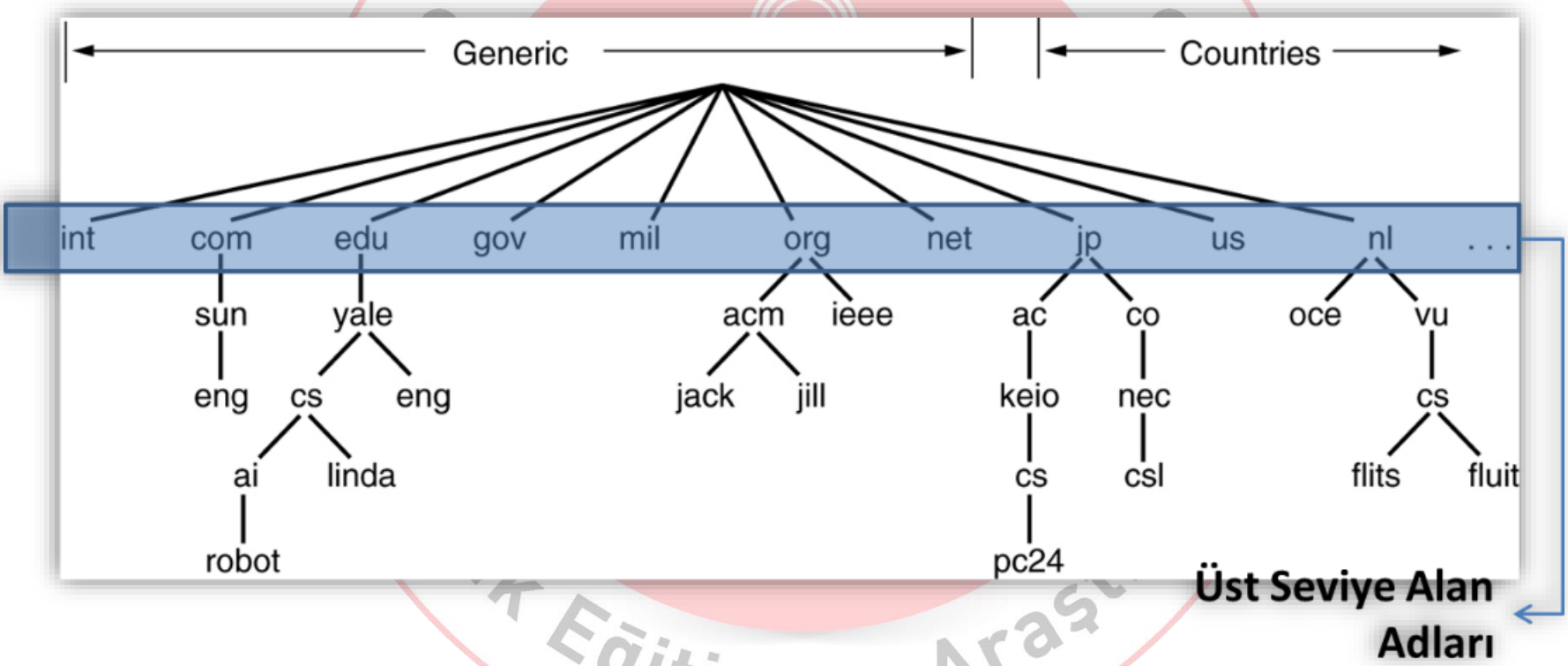
Uygulama Katmanı (L7)

egitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma

DNS

Alan adını (FQDN) IP adresine çevirmek için kullanılan sistemdir.

1984 – Hosts dosyası



Eğitim ve Araş

BY NC ND

Kök (Root) DNS Sunucuları

Güvenlik Eğ

BY NC ND

DNS: Kayıt Tipleri

Kayıt Tipi	Açıklama
A (Adress Record)	Adres kaydı olup host isimleri ile IPv4 eşleşmesi yapılır.
MX (Mail Exchanger)	Sistemde bulunan mail sunucuları tanımlamak için kullanılır.
PTR (Pointer Record)	IP adresinden isme eşleşme yapan kayıttır.
AAAA (Address Record)	Adres kaydı olup host isimleri ile IPv6 eşleşmesi yapılır.
SOA (Start Of Authority)	Bir DNS sunucunun o alandan (zone) sorumlu olduğunu belirler.
TXT (Text)	Belirli bir kaynak hakkında, nerede bulunduğu ve sahipliği gibi bilgiler
CNAME (Canonical Name)	Alias yani takma isim yoluyla başka bir kayda yönlendirir.
NS (Name Server)	Ağ üzerinde bulunan ve kullanımda olan DNS sunucuları tanımlar.

Eğitim ve Ara

DNS: Wireshark

Filter: udp | Expression... | Clear | Apply

No.	Time	Source	Destination	Protocol	Length	Info
30	27.785015	192.168.2.3	192.168.2.255	UDP	1328	Source port: 6646 Destination port: 6646
31	29.531792	192.168.2.3	google-public-dns-a.g	DNS	80	Standard query PTR 8.8.8.8.in-addr.arpa
32	29.553962	google-public-dns-a.g	192.168.2.3	DNS	124	Standard query response PTR google-public-dns-a.google.com
33	29.555056	192.168.2.3	google-public-dns-a.g	DNS	81	Standard query A mail.yahoo.com.Belkin
34	29.580244	google-public-dns-a.g	192.168.2.3	DNS	156	Standard query response, No such name
35	29.580855	192.168.2.3	google-public-dns-a.g	DNS	81	Standard query AAAA mail.yahoo.com.Belkin
36	29.604097	google-public-dns-a.g	192.168.2.3	DNS	156	Standard query response, No such name
37	29.604639	192.168.2.3	google-public-dns-a.g	DNS	74	Standard query A mail.yahoo.com
38	29.629549	google-public-dns-a.g	192.168.2.3	DNS	169	Standard query response CNAME login.yahoo.com CNAME login-global.lgg
39	29.630494	192.168.2.3	google-public-dns-a.g	DNS	74	Standard query AAAA mail.yahoo.com
40	29.654908	google-public-dns-a.g	192.168.2.3	DNS	214	Standard query response CNAME login.yahoo.com CNAME login-global.lgg

```
Frame 31: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
Ethernet II, Src: IntelCor_5f:e2:76 (00:1e:65:5f:e2:76), Dst: Belkin_53:95:77 (00:11:50:53:95:77)
Internet Protocol Version 4, Src: 192.168.2.3 (192.168.2.3), Dst: google-public-dns-a.google.com (8.8.8.8)
User Datagram Protocol, Src Port: 56301 (56301), Dst Port: domain (53)
Domain Name System (query)
```

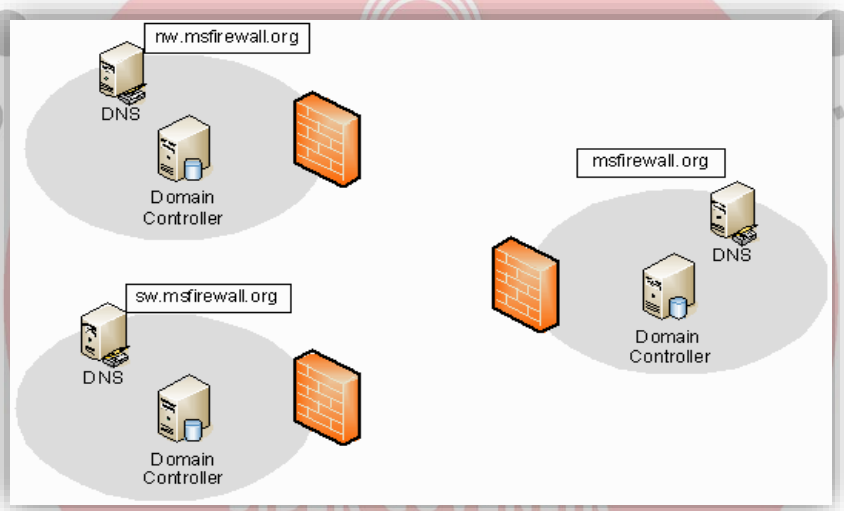
```
0000  00 11 50 53 95 77 00 1e  65 5f e2 76 08 00 45 00   ..PS.w.. e_.v..E.
0010  00 42 32 95 00 00 80 11  35 5b c0 a8 02 03 08 08   .B2..... 5[......
0020  08 08 db ed 00 35 00 2e  37 86 00 01 01 00 00 01   .....5.. 7.......
0030  00 00 00 00 00 00 01 38  01 38 01 38 01 38 07 69   .......8 .8.8.8.i
0040  6e 2d 61 64 64 72 04 61  72 70 61 00 00 0c 00 01   n-addr.a rpa.....
```

BY NC ND

Alan (Zone) Transferi

Birincil ve ikincil DNS sunucuların arasında kayıtları güncelleme

Yetkisiz kullanıcıların alan transferi yapmasına izin verilirse, DNS sunucuya girilmiş tüm adres kayıtlarına erişmek mümkün olacaktır.




```
# dig @ns.sirket.com sirket.com AXFR
```

```
# host -t ns sirket.com
# host -l sirket.com ns. sirket.com
```

BY NC ND

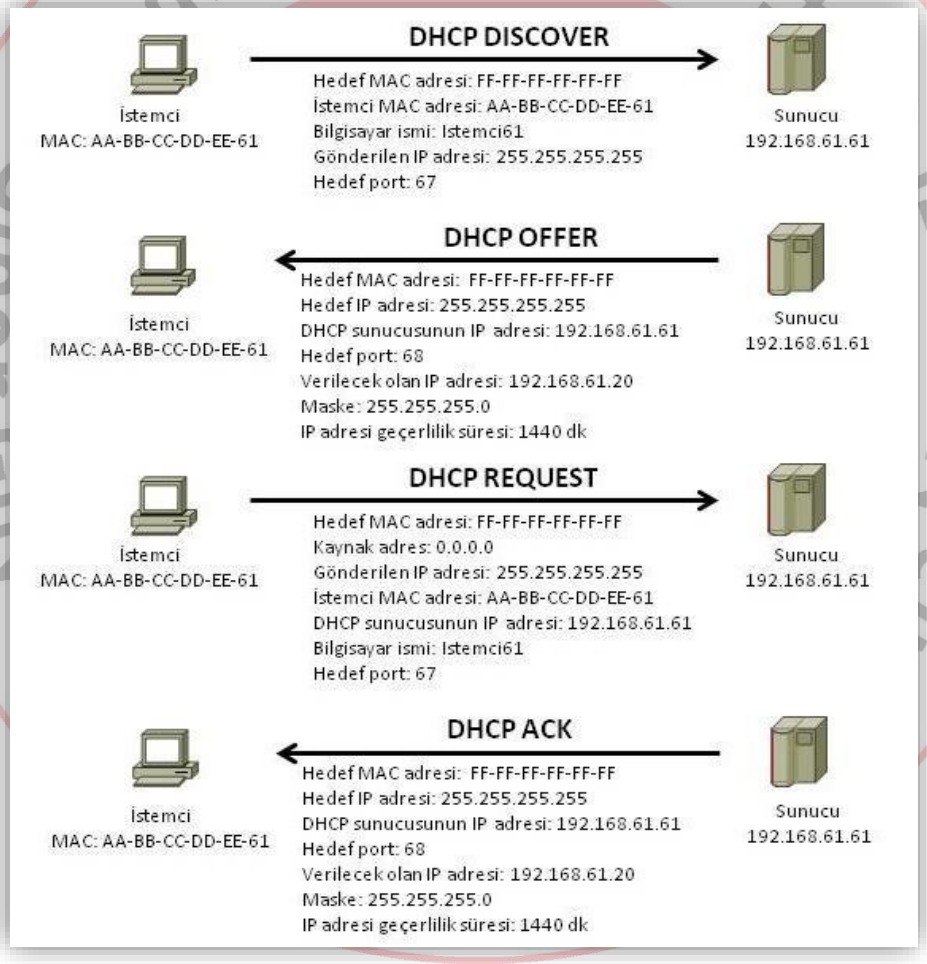
Alan (Zone) Transferi

```
root@SGE:~# host -t ns zonetransfer.me
zonetransfer.me name server ns16.zoneedit.com.
zonetransfer.me name server ns12.zoneedit.com.
root@SGE:~# host -l zonetransfer.me ns12.zoneedit.com
Using domain server:
Name: ns12.zoneedit.com
Address: 209.62.64.46#53
Aliases:

zonetransfer.me name server ns16.zoneedit.com.
zonetransfer.me name server ns12.zoneedit.com.
zonetransfer.me has address 217.147.180.162
164.180.147.217.in-addr.arpa.zonetransfer.me domain name pointer www.zonetransfe
r.me.
ipv6actnow.org.zonetransfer.me has IPv6 address 2001:67c:2e8:11::c100:1332
office.zonetransfer.me has address 4.23.39.254
owa.zonetransfer.me has address 207.46.197.32
asfdbbox.zonetransfer.me has address 127.0.0.1
canberra_office.zonetransfer.me has address 202.14.81.230
alltcpportsopen.firewall.test.zonetransfer.me has address 127.0.0.1
www.zonetransfer.me has address 217.147.180.162
deadbeef.zonetransfer.me has IPv6 address dead:beaf::
vpn.zonetransfer.me has address 174.36.59.154
dc_office.zonetransfer.me has address 143.228.181.132
```

BY NC ND

DHCP

IP adresi ve alt ağ maskesi başta olmak üzere, TCP/IP parametrelerini otomatik olarak dağıtan bir protokoldür.



cc BY NC ND

DHCP İstismarı: Adres Havuzunun Tüketilmesi

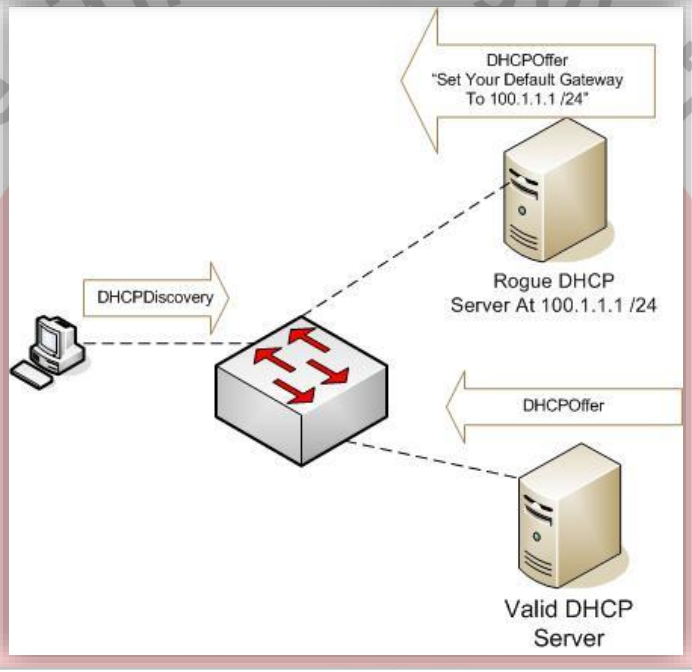
MAC adres bilgileri değiştirilerek sürekli olarak farklı IP adresleri alınmasıyla DHCP sunucu IP havuzunun tüketilmesi

```
#!/bin/bash
 while true; do
   killall dhclient3
   rm -f /var/run/dhclient3.pid
   ifconfig eth0 down
   macchanger -a eth0 2>&1 | grep Faked
   ifconfig eth0 up
   dhclient eth0 2>&1 | grep DHCPACK
 done
```

BY NC ND

DHCP İstismarı: Sahte DHCP Sunucu

Saldırgan sahte DHCP sunucusuyla istemcilere varsayılan ağ geçidi ve DNS sunucusu olarak kendi bilgisayarının adresini verebilir.



(config)# ip dhcp snooping vlan 20-61

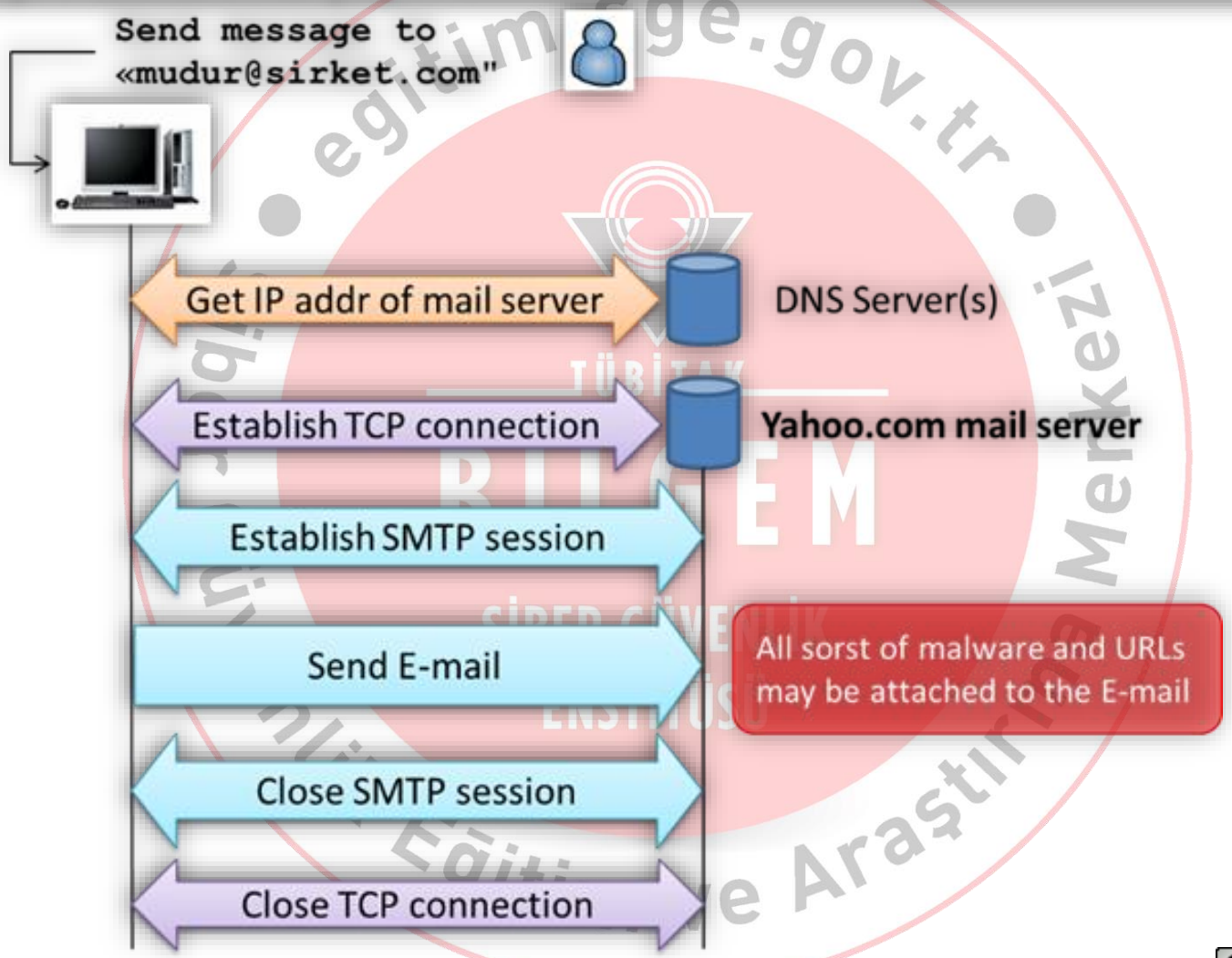
(config)# interface GigabitEthernet 6/17 (DHCP sunucusu portu)

(config-if)# ip dhcp snooping trust

BY NC ND

SMTP

Amaç: Postalama yapmaktır.



BY NC ND

E-posta Sahteciliği

```
S: 220 xyz.com SMTP service ready
C: HELO abcd.com
S: 250 xyz.com says hello to abcd.com
C: MAIL FROM: <elinor@abcd.com>
S: 250 sender ok
C: RCPT TO: <carolyn@xyz.com>
S: 250 recipient ok
C: DATA
S: 354 Send mail; end with "." on a line by itself
C: From: elinor@abcd.com
C: To: carolyn@xyz.com
C: MIME-Version: 1.0
C: Message-Id: <0704760941.AA00747@abcd.com>
C: Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
C: Subject: Earth orbits sun integral number of times
C:
C: This is the preamble. The user agent ignores it. Have a nice day.
C:
C: --qwertyuiopasdfghjklzxcvbnm
C: Content-Type: text/enriched
C:
C: Happy birthday to you
C: Happy birthday to you
C: Happy birthday dear <bold> Carolyn </bold>
C: Happy birthday to you
C:
C: --qwertyuiopasdfghjklzxcvbnm
C: Content-Type: message/external-body;
C:        access-type="anon-ftp";
C:        site="bicycle.abcd.com";
C:        directory="pub";
C:        name="birthday.snd"
C:
C: content-type: audio/basic
C: content-transfer-encoding: base64
C: --qwertyuiopasdfghjklzxcvbnm
C: .
S: 250 message accepted
C: QUIT
S: 221 xyz.com closing connection
```

Server message

Client message

Ulusal Siber Olay Müdahale Merkezi

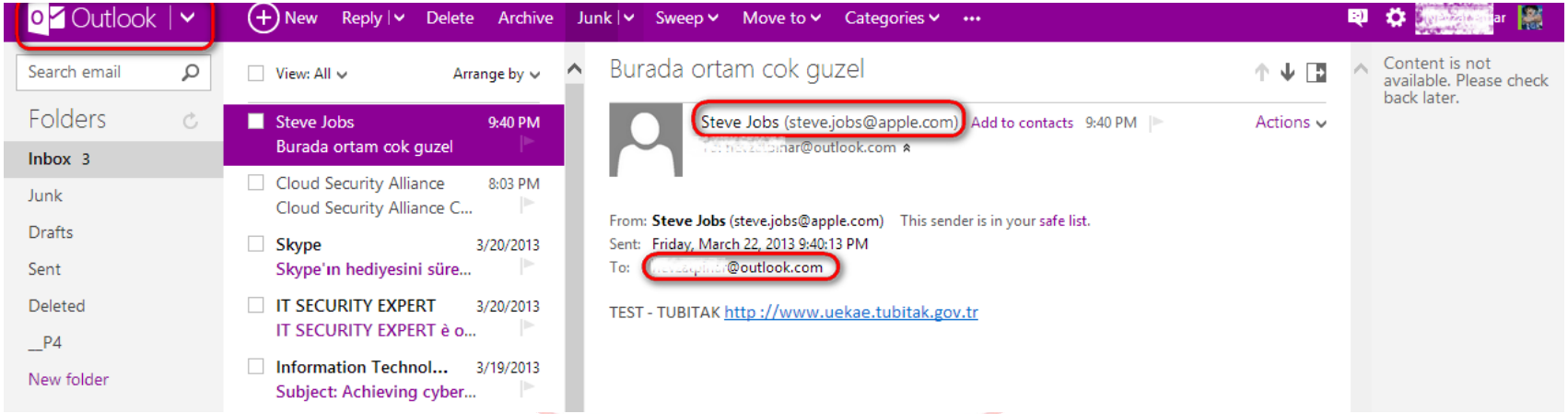
TÜBİTAK

CC BY NC ND

E-posta Sahteciliği

Microsoft Corporation [US] https://snt137.mail.live.com/mail/GetMessageSource.aspx?msgid=498f6e59-9328-11e2-8512-002264c1c798&folderid=(

```
x-store-info:4r51+eLowCe79NzwdU2kRwMf1FfZT+JrNNeZqyGSHNVQH/hWJAbEQGrC1H+C+zZxE17/pgn5GYWKjgwVuVmo83QEMT0iEO4oINmBiNzsFDVRoaCbcnR8sp98Fn8zoFv7YO1VqgtY1v8=
Authentication-Results: hotmail.com; spf=temperror (sender IP is 193.140.74.69) identity alignment result is fail and alignment mode is relaxed) smtp.mailfrom=galkan@uekae.tubitak.gov.tr;
X-SID-PRA: steve.jobs@apple.com
X-AUTH-Result: NONE
X-SID-Result: NONE
X-Message-Status: n:n
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MjtHRD0yO1NDTD02
X-Message-Info: 11chDOWgoTktmx98Ro6W2iU8v4T8G3MLbptg4aG2DECTyF3uTtd7XVLCmmZbcy3GcRkhhRxQrV1Jhf7uL05vauyjCCjh7pt4/S4ECDiz6isaplX1kvFFwXg9Z92nHg7bgZjtKC782yfw34UHVlMdeos/CWi4lj2K
Received: from pentest.uekae.tubitak.gov.tr ([193.140.74.69]) by SNT0-MC4-F5.Snt0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4900);
         Fri, 22 Mar 2013 12:40:11 -0700
Received: from pentest.uekae.tubitak.gov.tr (localhost [127.0.0.1])
        by pentest.uekae.tubitak.gov.tr (8.14.3/8.14.3/Debian-9.1ubuntu1) with ESMTP id r2MJlqNR027435
        for <nevzatpinar@outlook.com>; Fri, 22 Mar 2013 21:47:52 +0200
Date: Fri, 22 Mar 2013 21:47:52 +0200
Message-Id: <201303221947.r2MJlqNR027435@pentest.uekae.tubitak.gov.tr>
Content-Type: multipart/alternative;
   boundary="127.0.1.1.0.27434.1363981672.442.1"
From: Steve Jobs <steve.jobs@apple.com>
Subject: Burada ortam cok guzel
MIME-Version: 1.0
To: nevzatpinar@outlook.com
Return-Path: galkan@uekae.tubitak.gov.tr
X-OriginalArrivalTime: 22 Mar 2013 19:40:12.0242 (UTC) FILETIME=[119AA320:01CE2735]


--127.0.1.1.0.27434.1363981672.442.1
Content-Type: text/plain;
    charset="utf-8"
Content-Transfer-Encoding: quoted-printable

Burada ortam cok guzel
--127.0.1.1.0.27434.1363981672.442.1
```



BY NC ND

Uygulama 4 – Phishing (Oltalama) Saldırısı Analizi

«_Uygulama 4 - Phishing Saldırısı Analizi.pdf»

dosyasını açınız.

Lütfen uygulamayı tamamlayınız!

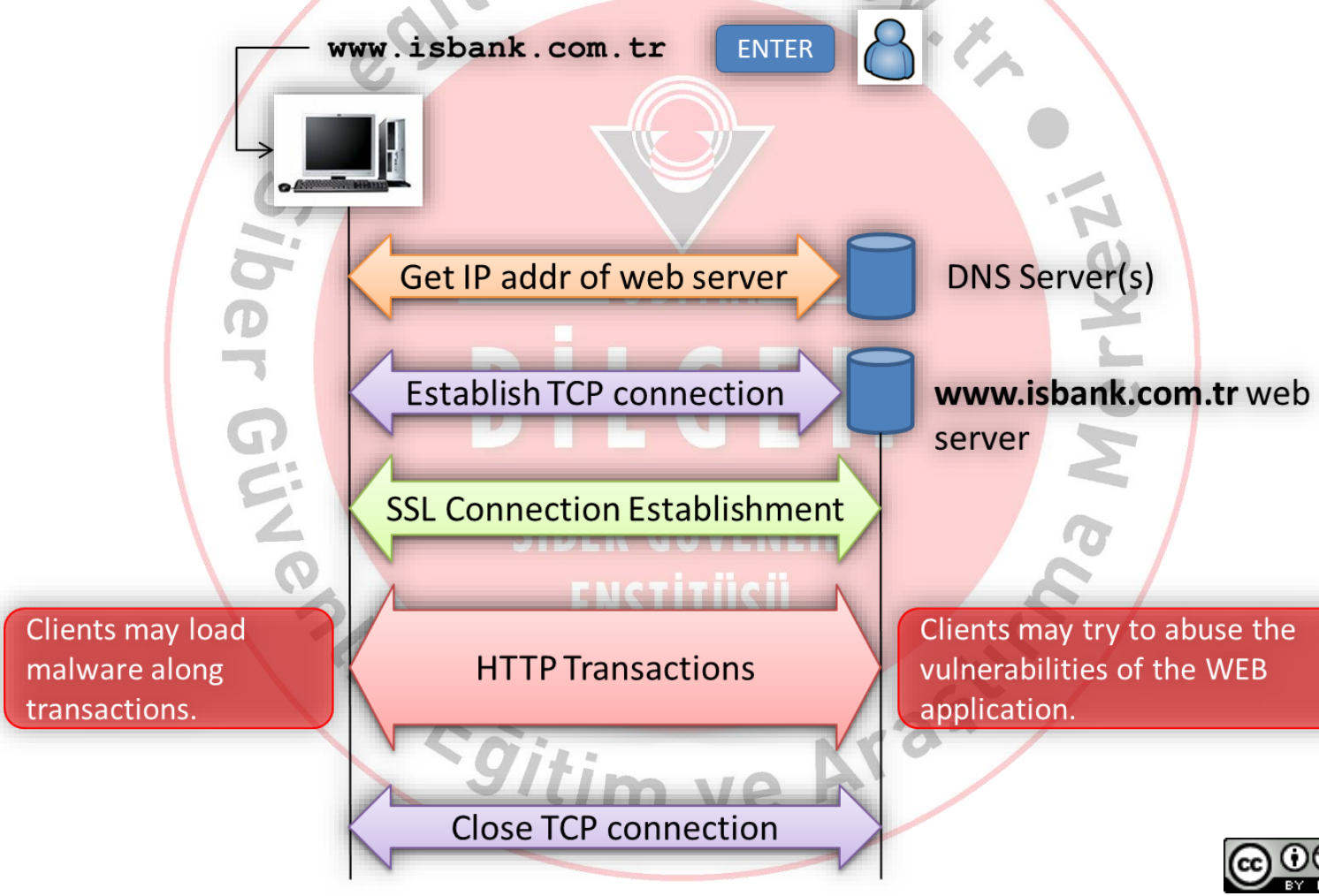
eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

FTP

- TCP ile bir uçtan diğer bir uca dosya transferi
- Kullanıcı adı ve parola, açık bir şekilde ağ üzerinden iletilmekte
- FTP over SSL, SFTP

TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

WEB üzerinde veri iletiminin kaynağı olan protokoldür



CC BY NC ND

HTTP: Metotlar

Vast majority of requests to Web servers from the clients.

Requests from the System Admin to modify the WEB content!

Method	Description
GET	Request to read a Web page
HEAD	Request to read a Web page's header
PUT	Request to store a Web page
POST	Append to a named resource (e.g., a Web page)
DELETE	Remove the Web page
TRACE	Echo the incoming request
CONNECT	Reserved for future use
OPTIONS	Query certain options

Submits data to be processed (e.g., from an HTML form).

egitim.sge.gov.tr
ENSTİTÜSÜ
Eğitim ve Araştırma

BY NC ND

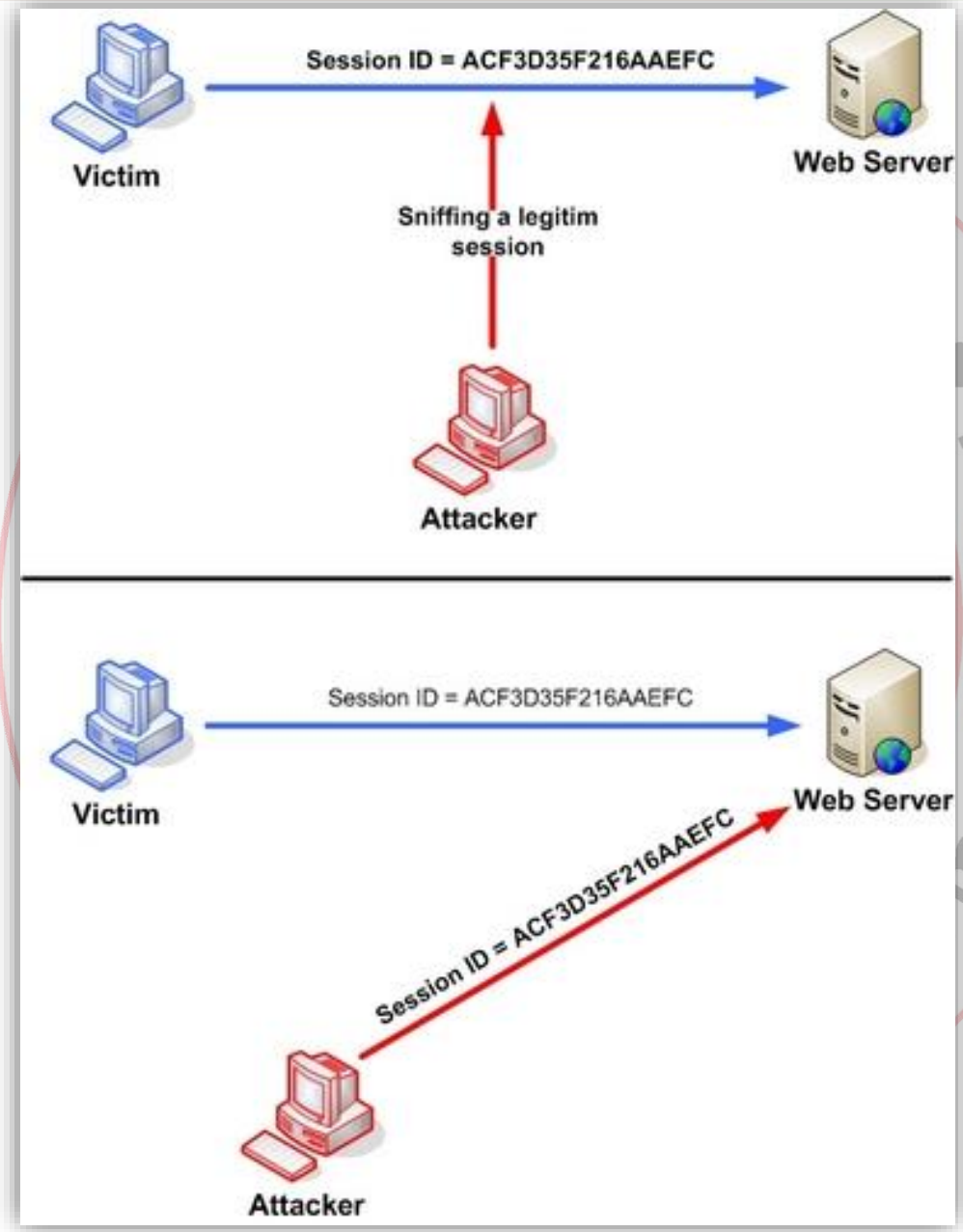
HTTP: Paket Analizi

No.	Time	Source	Destination	Protocol	Info
25	2.232123	192.168.1.165	192.168.1.178	HTTP	GET /hiding.php HTTP/1.0
26	2.233117	192.168.1.178	192.168.1.165	TCP	http > 63801 [ACK] Seq=1 Ack=404 Win=6432 Le
27	2.297124	192.168.1.178	192.168.1.165	HTTP	HTTP/1.1 200 OK (text/html)
28	2.297127	192.168.1.178	192.168.1.165	TCP	http > 63801 [FIN, ACK] Seq=377 Ack=404 Win=
29	2.298120	192.168.1.165	192.168.1.178	TCP	63801 > http [ACK] Seq=404 Ack=378 Win=63864

```
⊞ HTTP/1.1 200 OK\r\n
  Date: Mon, 18 May 2009 01:48:43 GMT\r\n
  Server: Apache/2.2.8 (Unix) mod_ssl/2.2.8 OpenSSL/0.9.8g DAV/2 PHP/5.2.6\r\n
  X-Powered-By: PHP/5.2.6\r\n
  Content-Encoding: gzip\r\n
  Vary: Accept-Encoding\r\n
  Content-Length: 109
  Connection: close\r\n
  Content-Type: text/html\r\n
  \r\n
  Content-encoded entity body (gzip): 109 bytes -> 100 bytes
⊟ Line-based text data: text/html
  <html>\n
  <body>\n
  <p>You can't read the content of this page while sniffing on wire.</p>\n
  </html>\n
  <body>\n
```

Eğitim ve Araş

HTTP: Oturum Çalma



TÜBİTAK

Ağ Güvenliği: Protokoller

TÜBİTAK
egitim.sge.gov.tr
Güvenlik Eğitim ve Araştırma
SİBER GÜVENLİK ENSTİTÜSÜ
CC BY NC ND

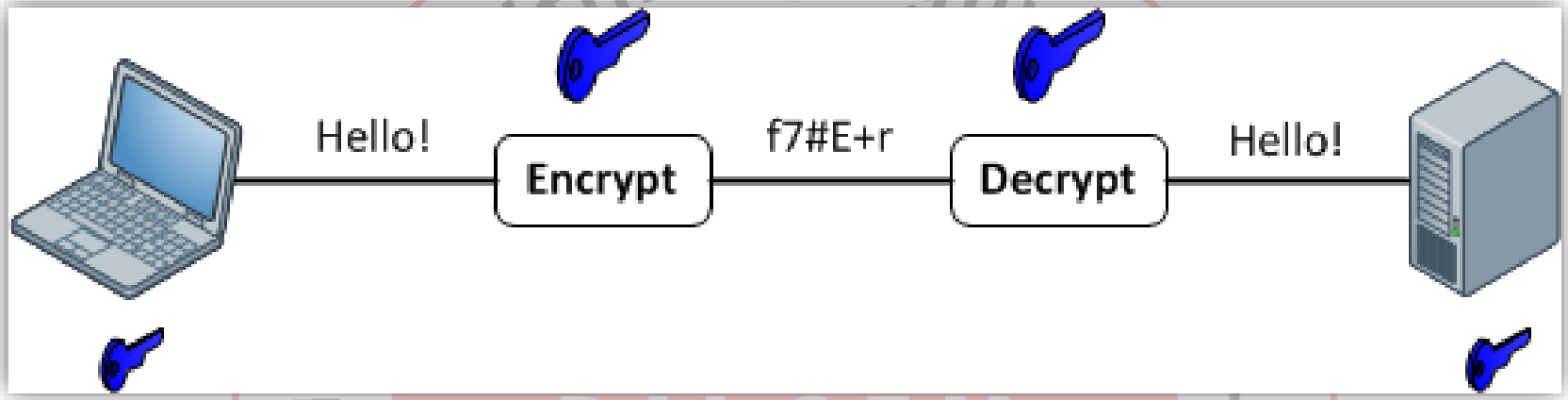
Gizlilik, bütünlük, kimlik doğrulama, veri asıllaması, anahtar paylaşımı ve imzalama

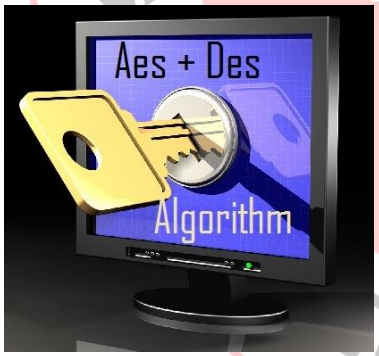
- Simetrik (Gizli Anahtar) Algoritmalar
- Asimetrik (Ortak Anahtar) Algoritmalar
- Özet (Hash) Fonksiyonları
- Sayısal Sertifikalar ve Sertifika Makamları

BİLGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma Me

CC BY NC ND

Simetrik Şifreleme

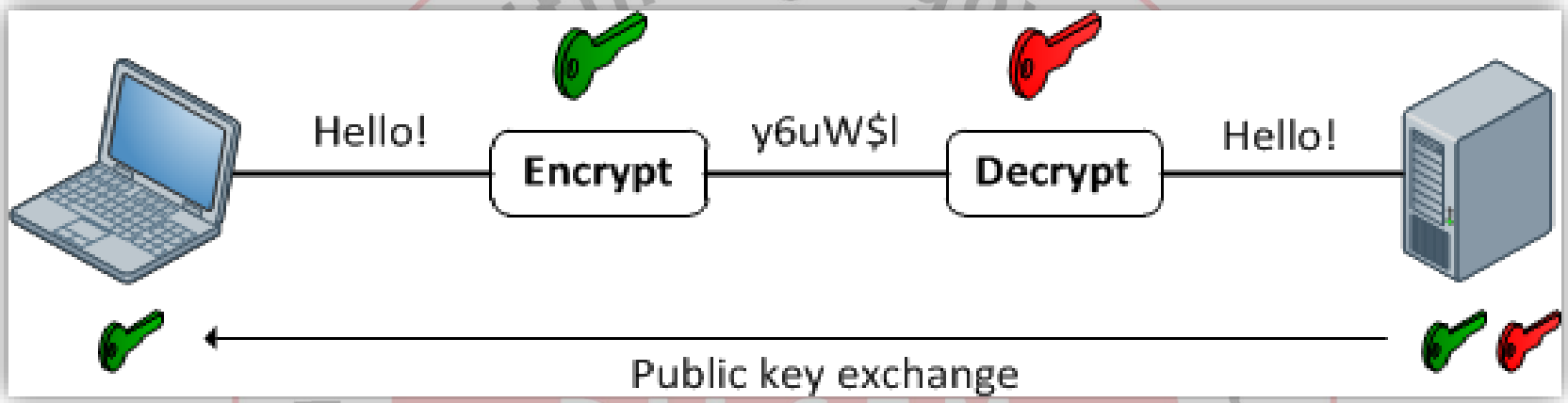




	Veri boyu	Anahtar boyu
AES	128 bit	128-192-256 bit
DES	64 bit	56 bit
3DES	64 bit	112 bit

BY NC ND

Asimetrik Şifreleme

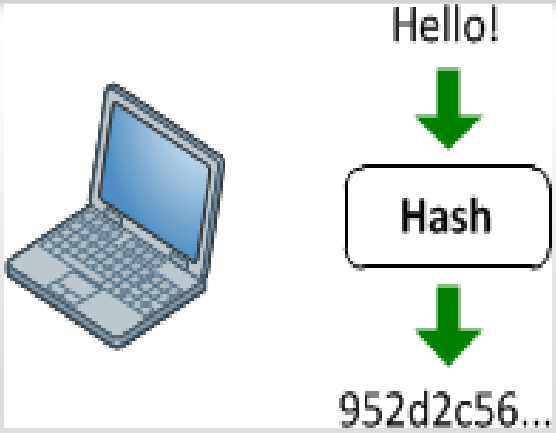


BILGEM
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma Mer
RSA

Özet (Hash) Fonksiyonları

Büyük boyutlardaki verinin daha küçük boyutlarda ifadesi

- Anahtarlı özet fonksiyonları
  - CBC-MAC
- Anahtarsız özet fonksiyonları
  - SHA-1
  - SHA-2




```
# echo -n "Şifrelenecek Metin" | md5sum
# echo -n "Şifrelenecek Metin" | sha512sum
```

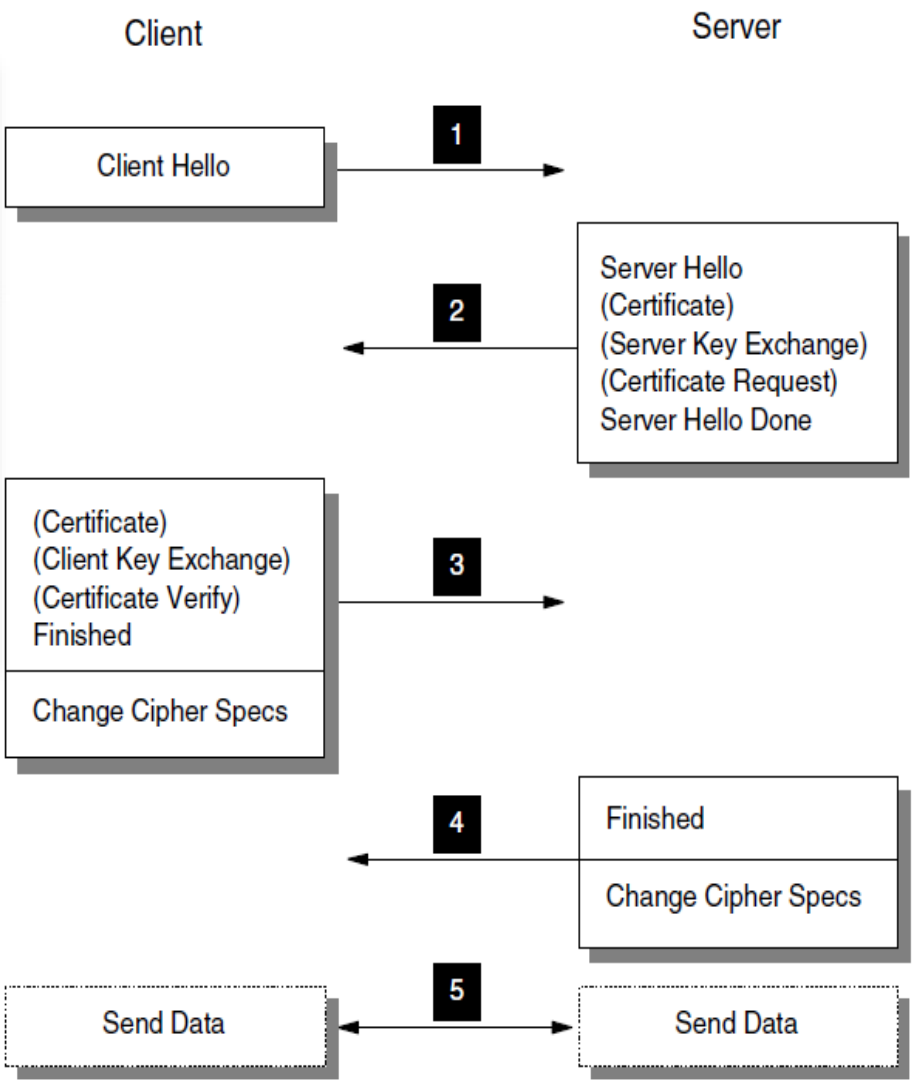
BİLGEM ENSTİTÜSÜ Siber Güvenlik Eğitim ve Araştırma

cc BY NC ND

Sayısal Sertifikalar ve Sertifika Makamları

Sertifika, en basit anlamda açık anahtarın bir otorite tarafından imzalanmış halidir.

Sertifika makamı üzerinde bir otorite olmadığından, kendi sertifikasını oluştururken kendi gizli anahtarı ile kendi açık anahtarını imzalamaktadır.



Güvenlik Eğitim
SİBER G
ENST

Sanal Özel Ağlar (VPN)

Güvensiz ağlar üzerinde güvenli olarak haberleşmek

- IPSEC, PPTP, L2TP
- DES, 3DES, IDEA, CAST128, Blowfish vs…
- MD-5, SHA-1

BİLGEM Bilgi Güvenlik Eğitim ve Araştırma Merkezi Enstitüsü

cc BY NC ND

IPSec

AH (Authentication Header): Kimlik Doğrulama

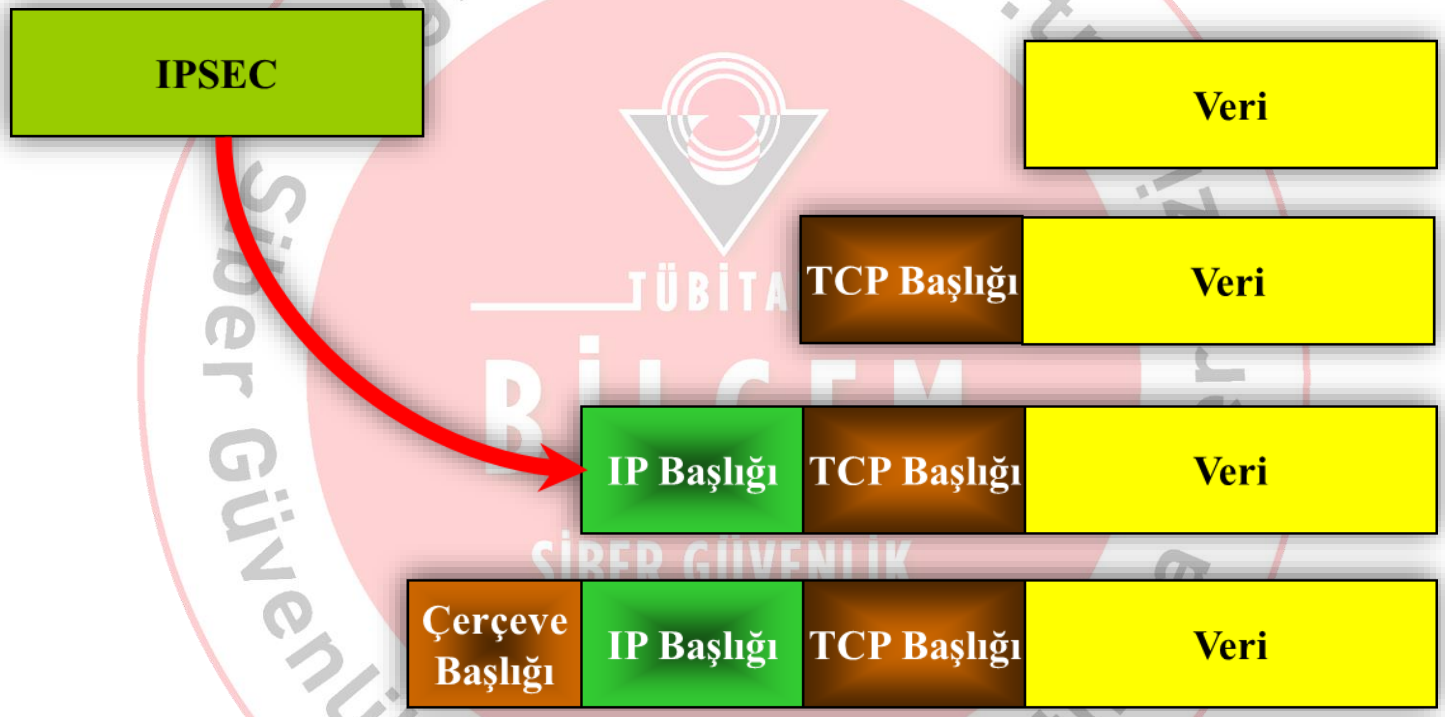
ESP (Encapsulating Security Payload): Gizlilik

IKE (Internet Key Exchange): Anahtar Değişimi

	AH	ESP
Erişim Denetimi	Var	Var
Bağlantısız Bütünlük	Var	-
Veri Kaynağı Doğrulama	Var	-
Tekrarlanan Paketlerin Reddedilmesi	Var	Var
Gizlilik	-	Var
Sınırlı Trafik Gizliliği	-	Var

BY NC ND

IPSec Paket Başlığı

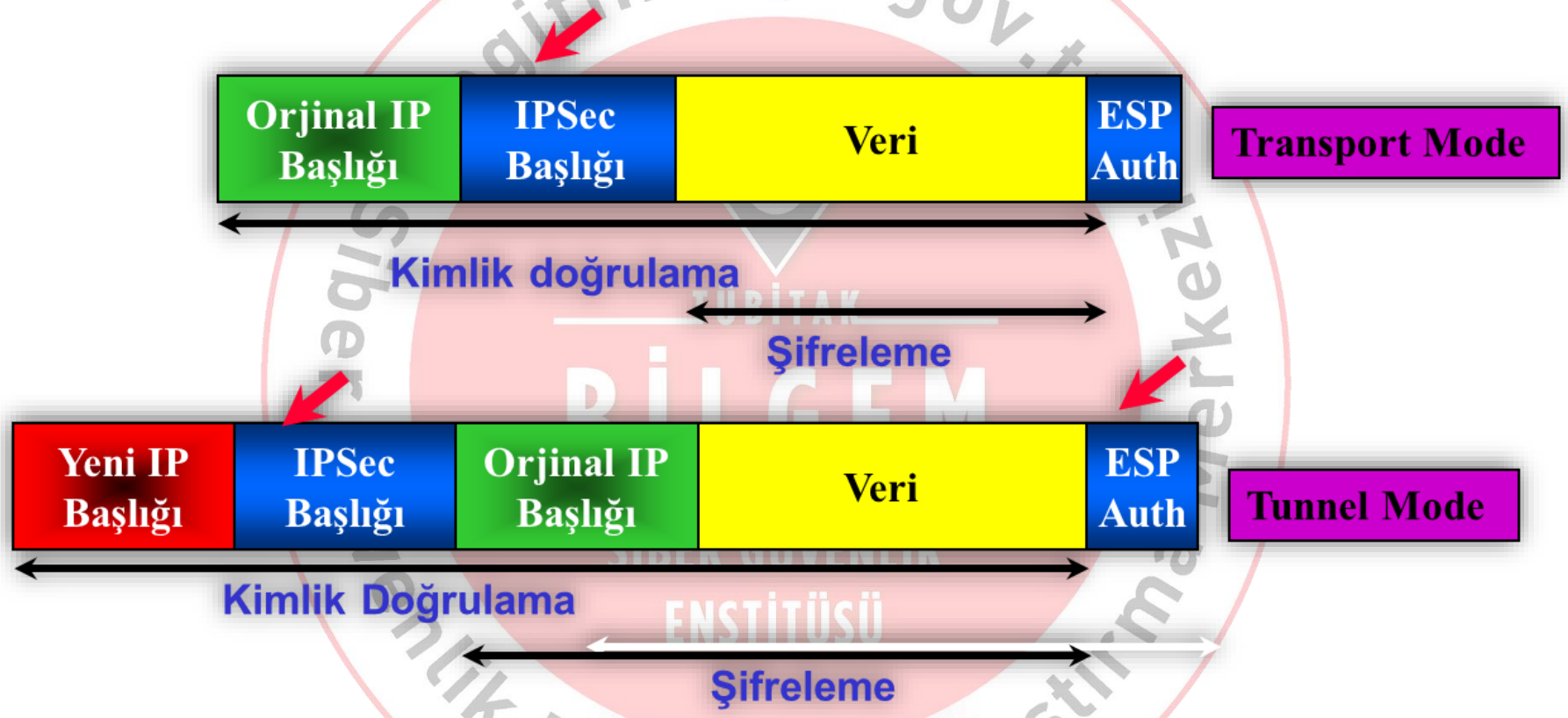


BY NC ND

Authentication Header (AH)

eğitim.sge.gov.tr
TÜBİTAK
SİBER GÜVENLİK ENSTİTÜSÜ
Siber Güvenlik Eğitim ve Araştırma Merkezi

Encapsulating Security Payload (ESP)

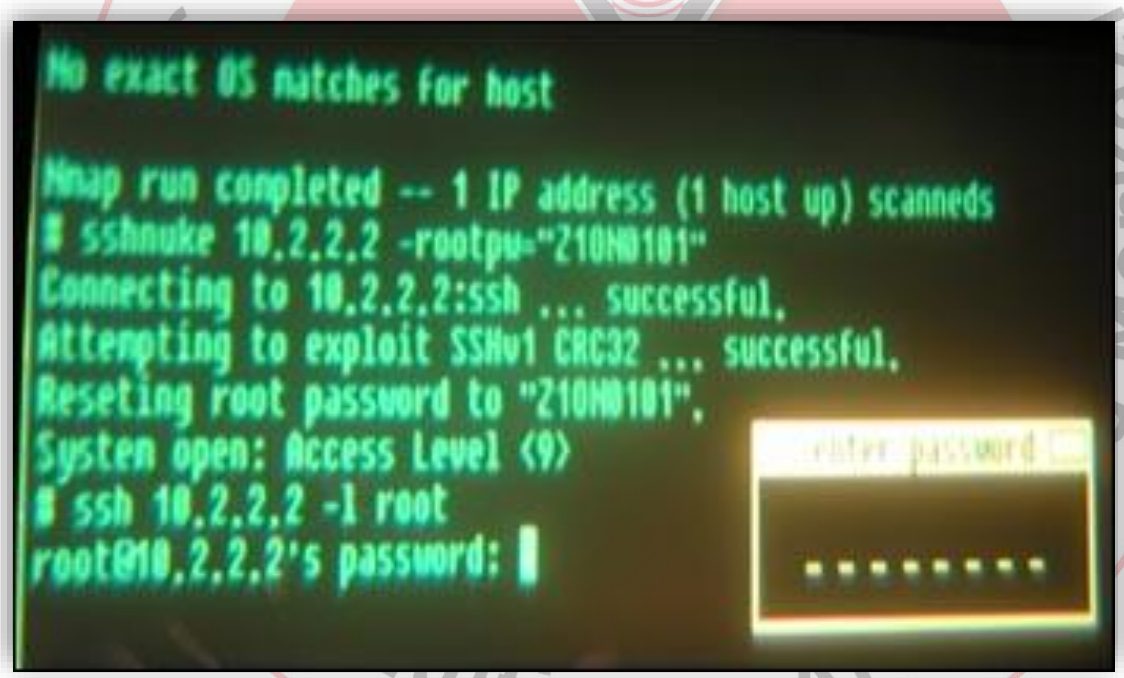


BY NC ND

Secure Shell (SSH)

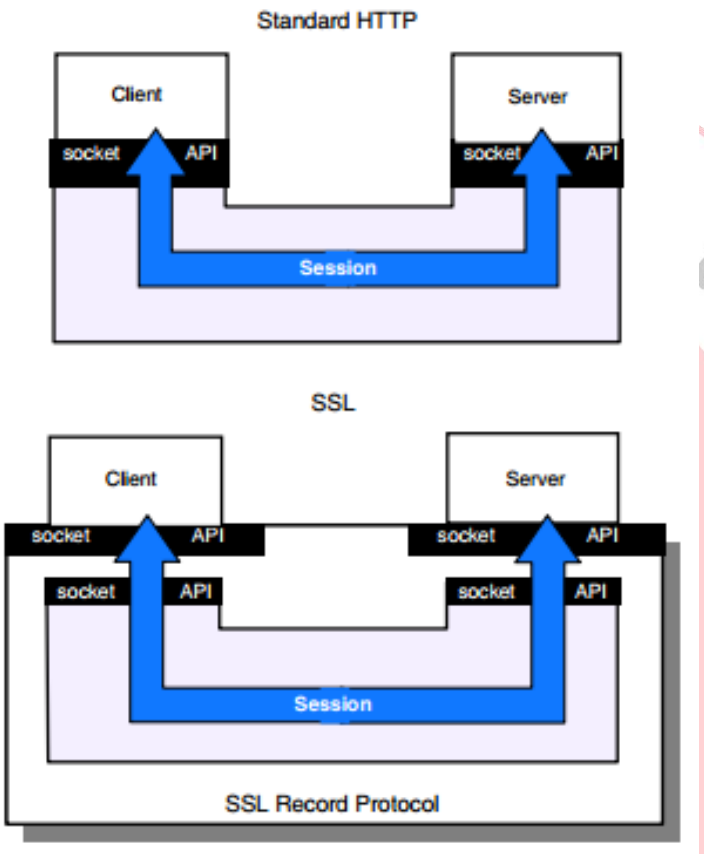
Verinin güvenli bir tünel içerisinden geçmesini sağlar.

Güvenli olmayan erişim protokollerinin yerine kullanılmalıdır.



BY NC ND

SSL & TLS



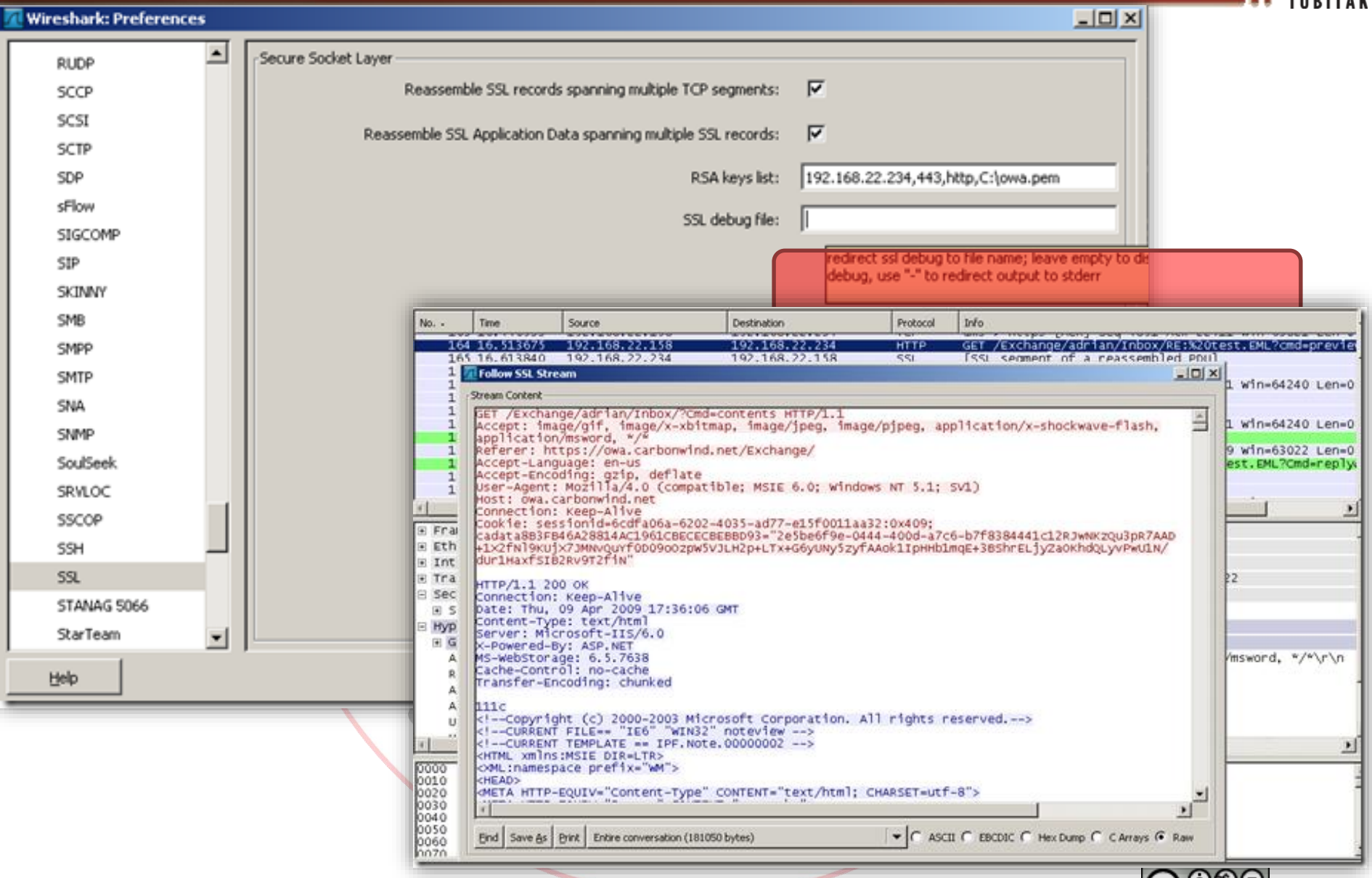
SSL: Bağlantının en başından sonuna kadar tüm iletişim şifreli

TLS: TCP üçlü el sıkışma işlemi düz ve şifresiz

```
# openssl s_client -connect bilgiguvenligi.gov.tr:443 -ssl3
```

cc BY NC ND

SSL: Wireshark ile Paket Analizi



BY NC ND

Uygulama 5 – Wireshark ile SSL Şifre Çözme

«_Uygulama 5 - Wireshark ile SSL Şifre Çözme.pdf»

dosyasını açınız.

Lütfen uygulamayı tamamlayınız!

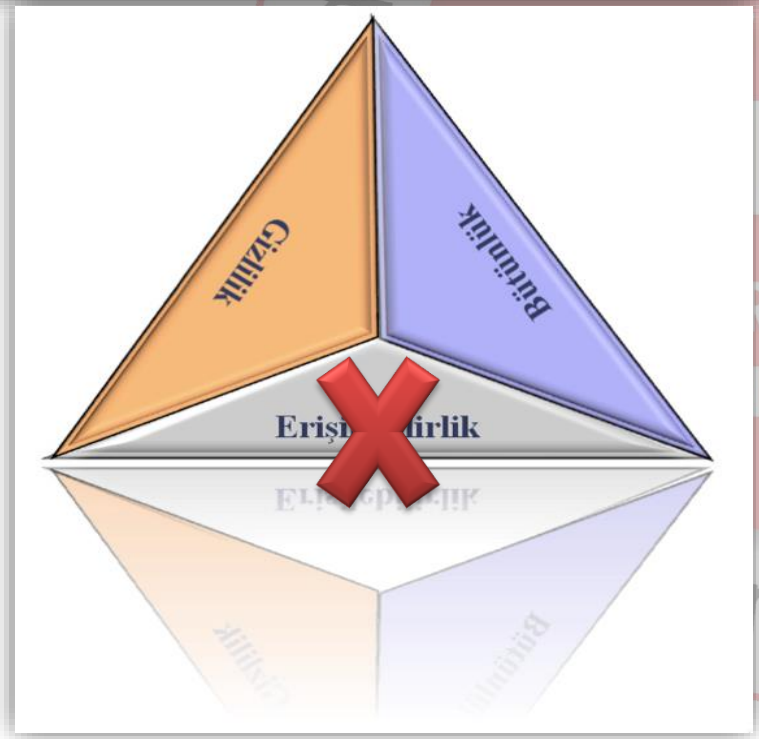
eğitim.sge.gov.tr
Siber Güvenlik Eğitim ve Araştırma Merkezi
TÜBİTAK BİLGEM SİBER GÜVENLİK ENSTİTÜSÜ

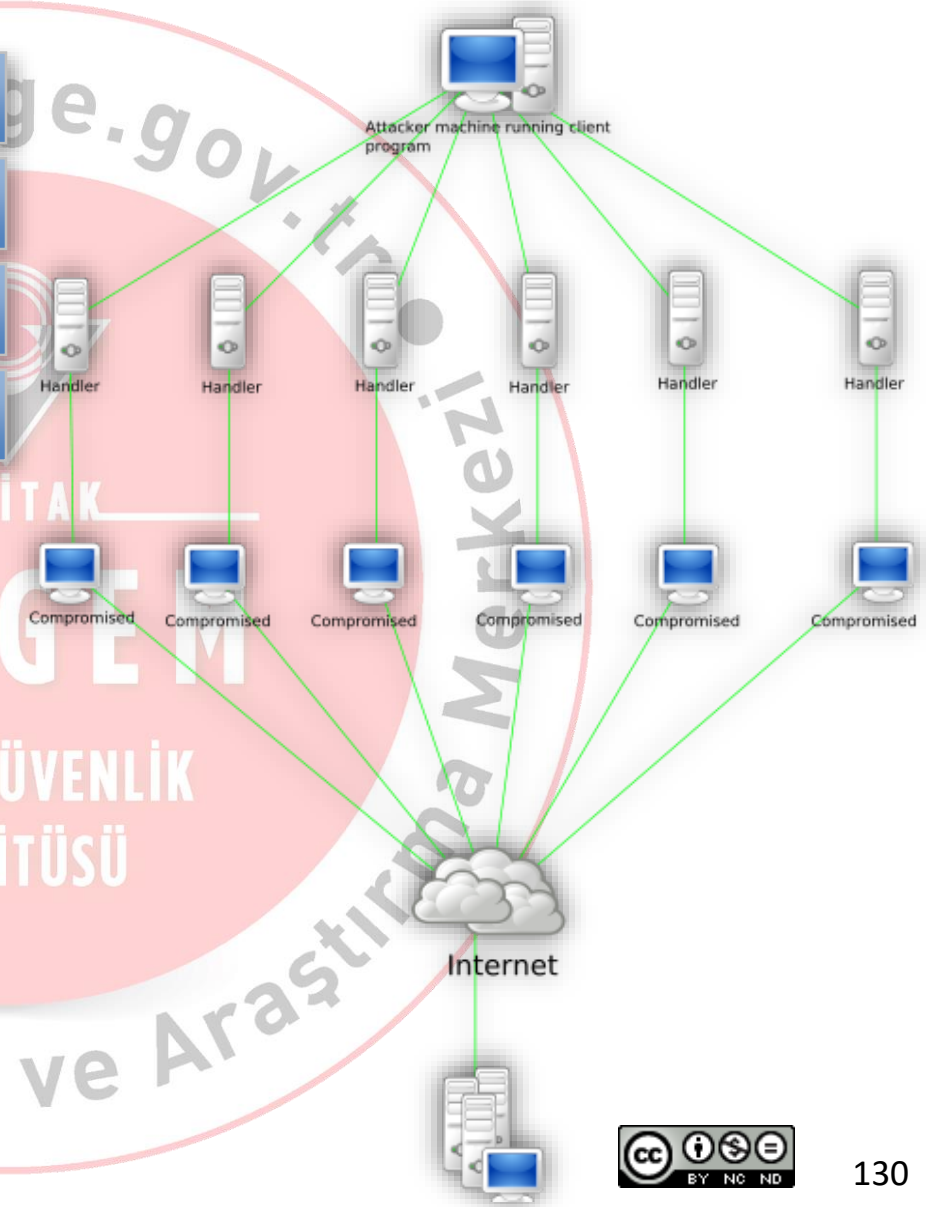
DoS/DDoS Saldırıları

TÜBİTAK
eğitim.sge.gov.tr
SİBER GÜVENLİK ENSTİTÜSÜ
Güvenlik Eğitim ve Araştırma
CC BY NC ND

Kavramlar

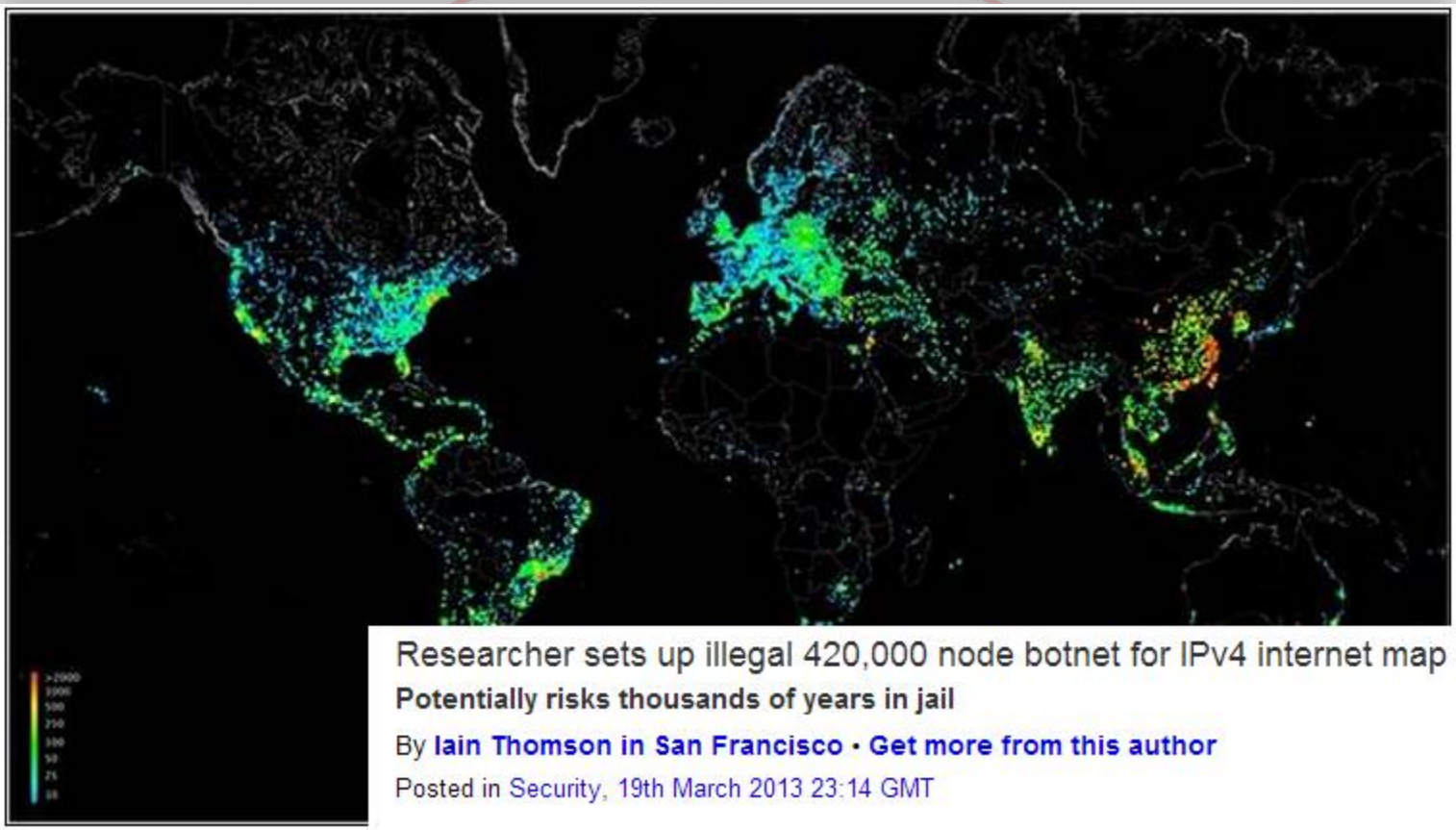
- DoS
- DDoS
- Hedef: Erişilebilirlik
- BotNet





BY NC ND

roBOTNETwork



The Carna IPv4 botnet

Eğitim ve Araş

BY NC ND

Yakın Tarihten Bazı Örnekler

- 2016 – BBC
- 2015 – PlayStation Network & Xbox Live
- 2013 – Çin: İnternet Arızası
- 2012 – Türk Hava Yolları: İş bırakma eylemi
- 2010 – Wikileaks, Mavi Marmara, TİB, BTK, TÜBİTAK
- 2009 – Twitter
- 2008 – Rusya-Gürcistan: Güney Osetya anlaşmazlığı
- 2007 – Rusya-Estonya: Savaş anıtı konusunda ihtilaf
- 2002 – Kök DNS sunucularını hedef alan DDoS saldırıları
- 1996 – Panix (Bilinen ilk DDoS atağı)

BY NC ND

Maliyeti Nedir?

Current prices on the Russian underground market:

Hacking corporate mailbox: $500

Winlocker ransomware: $10-$20

Unintelligent exploit bundle: $25

Intelligent exploit bundle: $10-$3,000

Basic crypter (for inserting rogue code into a benign file): $10-$30

SOCKS bot (to get around firewalls): $100

Hiring a DDoS attack: $30-$70/day, $1,200/month

Botnet: $200 for 2,000 bots

DDoS Botnet: $700

ZeuS source code: $200-250

Windows rootkit (for installing malicious drivers): $292

Hacking Facebook or Twitter account: $130

Hacking Gmail account: $162

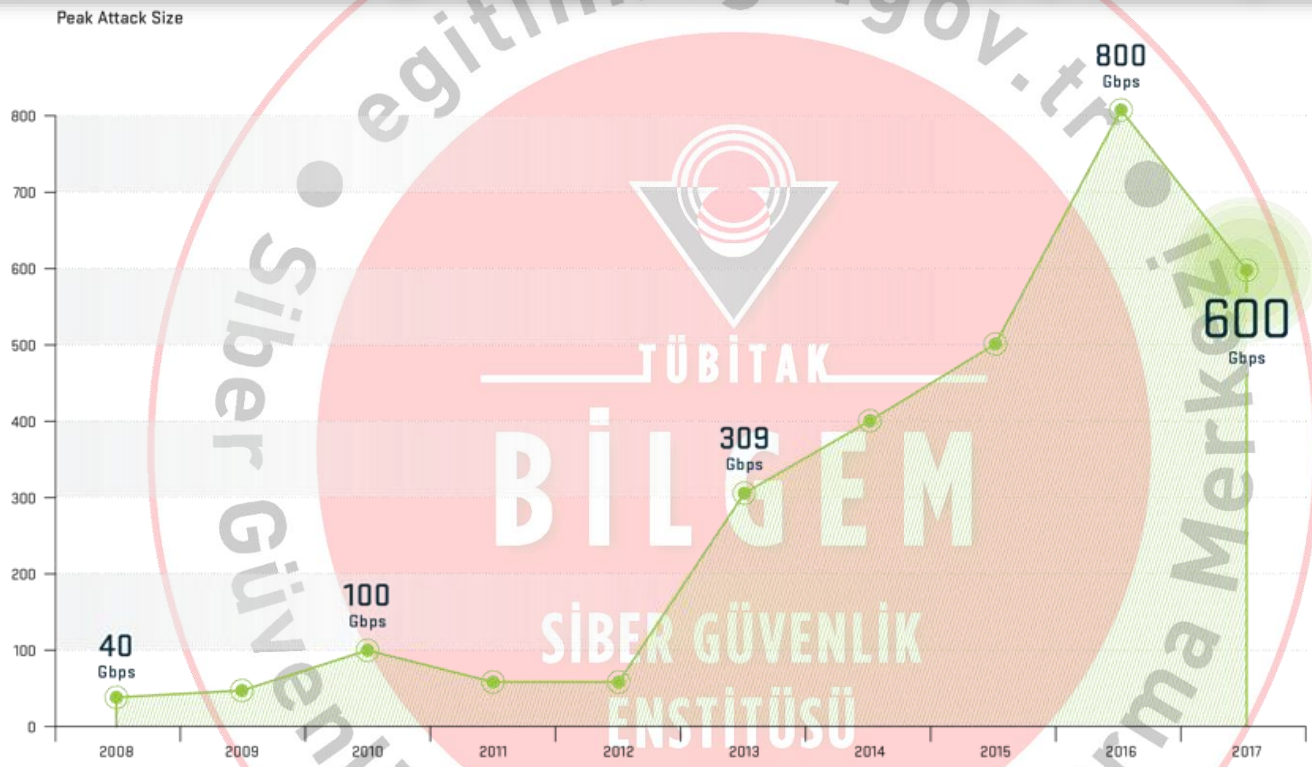
Email spam: $10 per one million emails

Email scam (using customer dtabase) $50-$500 per one million emails

BY NC ND

DDoS = Bant Genişliği?

Gelen saldırı bant genişliğinden fazlaysa yapılacak çok şey yok!



DDoS saldırılarının büyük çoğunluğu, bant genişliğini taşırma şeklinde gerçekleşmektedir.

CC BY NC ND

DDoS vs OSI

	OSI	TCP/IP
Uygulama hafıza ve CPU kullanımını arttırma	Layer 7 Application	Application Telnet, FTP, NFS, NIS
Anlaşılamayan veriler ile uygulamayı etkisiz bırakma	Layer 6 Presentation	Session e.g. RPC
Başka bir kullanıcıya ait oturumu sonlandırma	Layer 5 Session	Transport Sockets/Streams - TLI
TCP SYN seli, UDP seli	Layer 4 Transport	TCP / UDP
Parçalı IP paketi, büyük boyutlu ICMP paketi gönderme	Layer 3 Network	Network IP + ARP/RARP/ICMP
ARP Spoof, Wi-Fi De-Auth frameleri gönderme	Layer 2 Data Link	Physical Protocol Ethernet/TR/FDDI/PPP
Ağ kablosunun çekilmesi, kesilmesi	Layer 1 Physical	Transmission medium Coax, Fiber, 10baseT..

TÜBİTAK

Teşekkürler