

Celal Çeken

Ağ Programlama

OSI ve TCP/IP Protokol Mimarileri

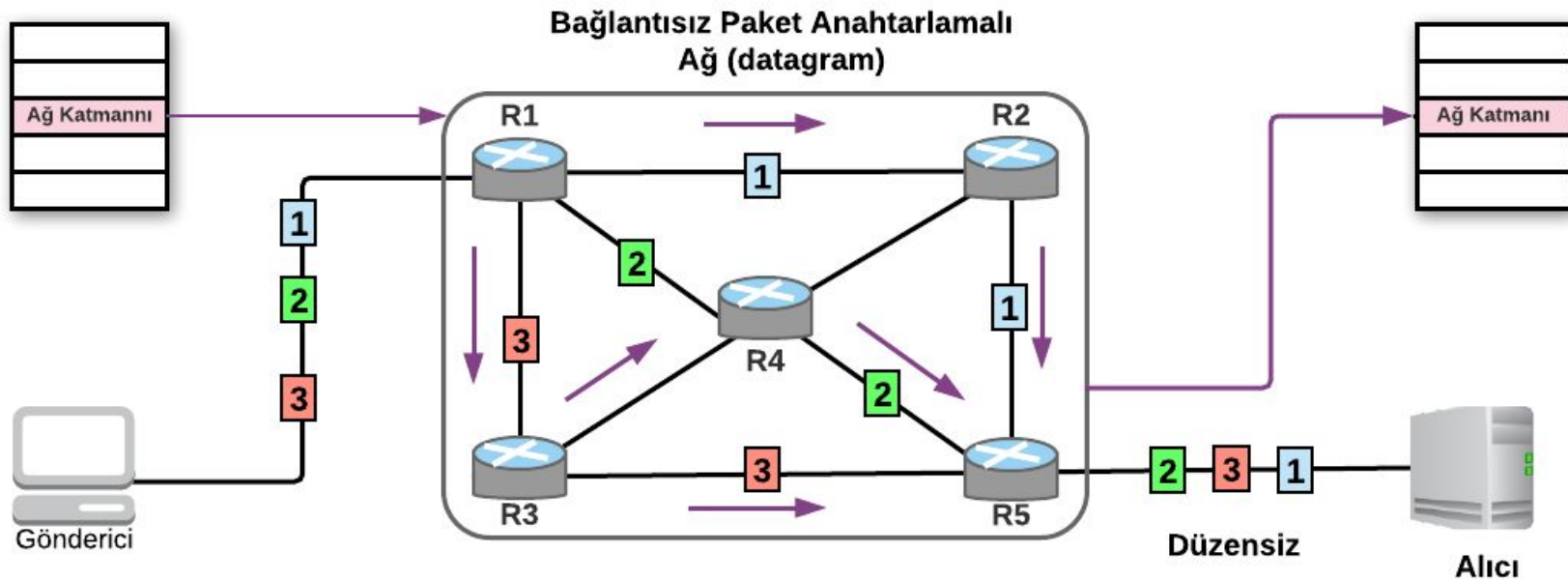


Konular

- ✓ Haberleşme Ağları, Devre Anahtarlama / Paket Anahtarlama
- ✓ Protokol
- ✓ OSI Referans Modeli
- ✓ Paketleme (Encapsulation)
- ✓ Protokol Veri Birimleri PVB (PDU)
- ✓ TCP/IP
- ✓ TCP/IP Protokolleri
- ✓ IP Başlığı
- ✓ Anahtar & Yönlendirici
- ✓ Taşıma Katmanı : Port Adresi
- ✓ TCP Bağlantı Kurulumu / Bağlantı Sonlandırma
- ✓ Traceroute ile Topoloji Keşfi
- ✓ Ağ Geçidi(Gateway) & Firewall
- ✓ Vekil Sunucu (Proxy Server)
- ✓ Kaynaklar

Haberleşme Ağları

- ✓ Ağ kurulumunun amacı kaynak ve bilgi paylaşımı yapabilmektir.
- ✓ Açık sistemler farklı platformlar arasında da paylaşımın yapılabilmesine olanak sağlar.
- ✓ Döğüm ve aralarındaki bağlantılardan oluşan yapıya haberleşme ağı denir
- ✓ Döğümler arası bağlantılar genellikle çoklanır (FDM, TDM) .
- ✓ Herhangi iki uç döğüm arasında doğrudan bir hat yoktur.
- ✓ Döğümler arasında alternatif yolların çok olması istenir.
- ✓ İki farklı anahtarlama teknolojisi kullanılır.
 - ✓ Devre Anahtarlama
 - ✓ Paket Anahtarlama



Devre Anahtarlama

- ✓ Haberleşen istasyonlar arasında, ağ bağlantı noktaları üzerinden geçen, görüşme boyunca o görüşmeye özel haberleşme yollarının kurulmasını sağlar.
- ✓ Ağın düğümleri içerisindeki iki nokta arasında bir ayrılmış haberleşme yolu oluşturulur.
- ✓ Bu yol, düğümler arasında sıra ile fiziksel bağlantıların oluşturulması ile kurulur.
- ✓ Bir kaynaktan üretilen veri, özel ayrılmış bir yol üzerinden mümkün olduğunca hızlı çıkış kanalına gecikmeden yönlendirilir veya anahtarlanır.

Örnek: telefon şebekesi (PSTN)

Üstünlükleri

- Veri akış hızı sabittir.
- Bağlantı sağlandıktan sonra gecikmeler küçük ve kestirilebilirdir.

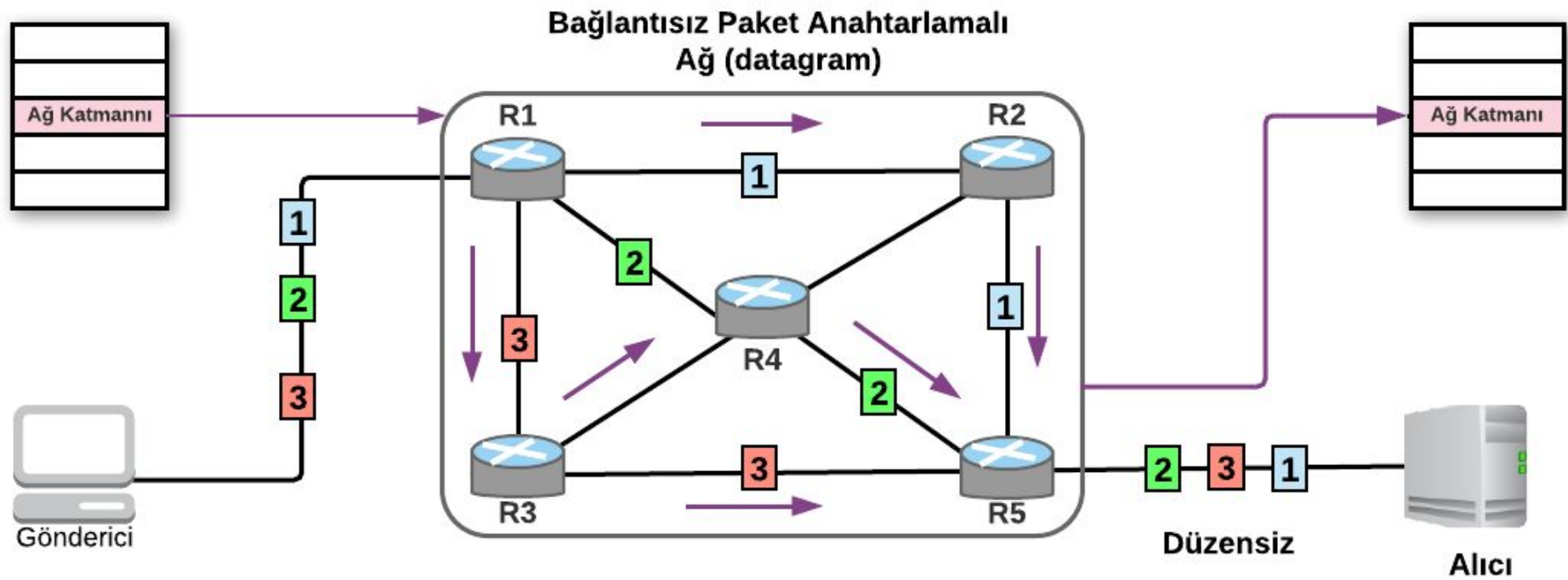
Zayıf Yönleri

- Bağlantı kurulum gecikmesi
- Patlama türündeki veri akışlarında verimsiz (Bağlantı sonucu fiziksel bir hat tahsis edildikten sonra iki uç nokta haberleşmeyi devam ettirmese bile, bu hat başka bir uygulama tarafından kullanılamaz)

Paket Anahtarlama

- ✓ Veri, paketler olarak adlandırılan küçük parçalardan oluşan bir dizi olarak hedefe gönderilir.
- ✓ İletim kanalı herhangi bir uygulama trafiği için tahsis edilmez.
- ✓ Bir paket kaynaktan hedefe doğru giderken düğümden düğüme aktarılır.
- ✓ Her düğümde bütün paket alınır, kısa bir süre saklanır ve daha sonra bir sonraki düğüme iletilir.
- ✓ İnternet'in alt yapısında paket anahtarlama teknolojisi vardır.

Paket Anahtarlama

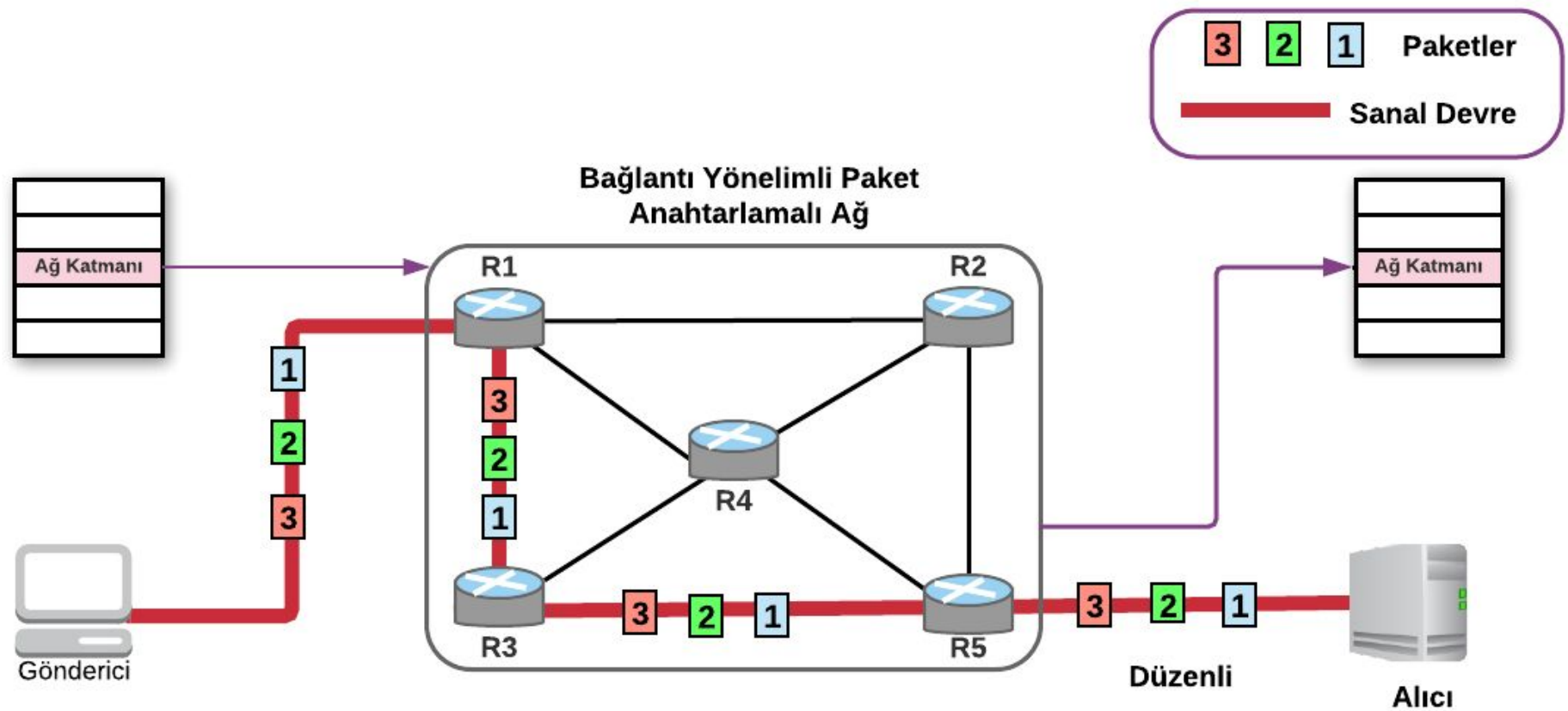


Paket Anahtarlamanın Avantajları ve Dezavantajları

- ✓ Aynı hat farklı uygulamalar tarafından kullanılabilir- kanal kullanım verimliliği
- ✓ Patlamalı trafikler için daha uygundur.
- ✓ Öncelik mekanizması kullanılabilir.

- ✓ Gecikmeler fazla olabilir (yönlendirme algoritmaları)
- ✓ Gecikme değişimi (jitter) fazla olabilir.
- ✓ Başlık bilgisi fazladır.

Paket Anahtarlama



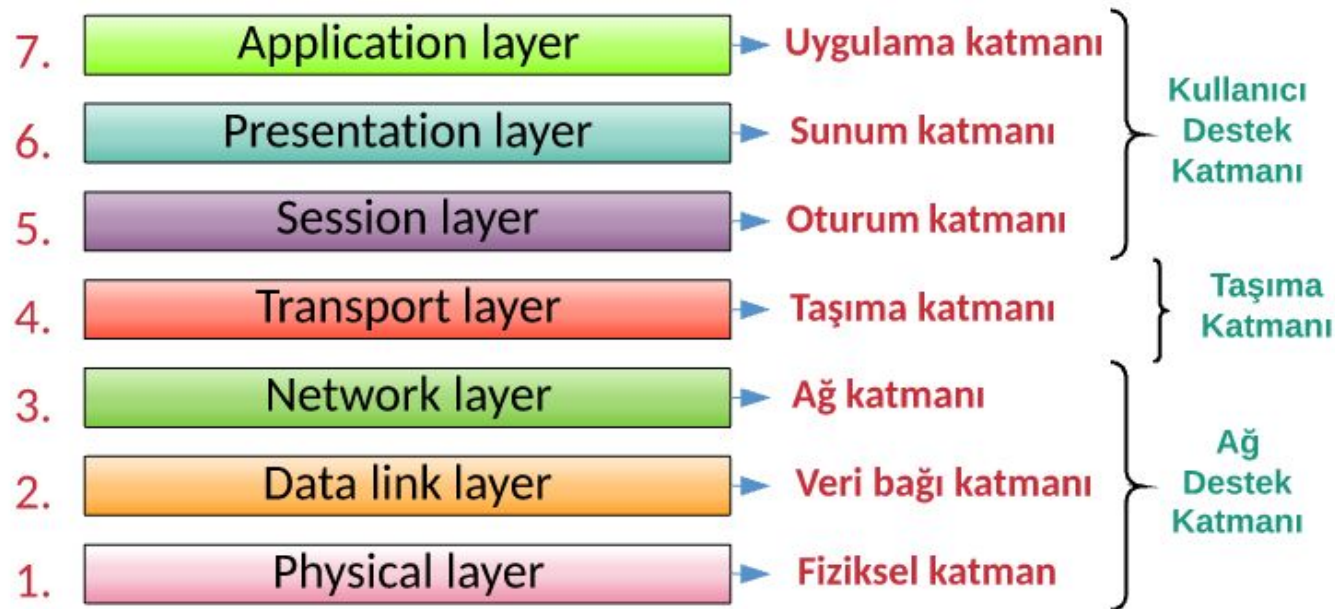
Protokol

- ✓ Veri haberleşmesinde protokol, verilerin ağ üzerinde taşınması için belirlenen kurallar dizisi olarak tanımlanabilir.
- ✓ Bir protokol neyin, ne zaman ve nasıl iletileceğini tanımlar.
- ✓ Veriler birimler arasında taşınırken yapılması gerekenler oldukça karmaşıktır. (oturum oluşturulması, hata kontrol, yönlendirme, senkronizasyon v.s.)
- ✓ Tek bir modül kullanmak yerine görevleri birbirinden bağımsız alt modüllere ayırmak daha mantıklıdır. (Yazılım geliştirmede olduğu gibi)
- ✓ Bir protokol mimarisi dikey yığın şeklinde düzenlenir ve her bir modüle katman adı verilir.
- ✓ Alt katman bir üst katmana servis sağlar.
- ✓ Alıcı ve vericide eş katmanlar ortak bir protokol ile haberleşirler.

OSI (Open Systems Interconnection) Referans Modeli

Açık sistemin amacı üreticiye özel çözümleri azaltarak standartlaştırmayı sağlamak. TCP/IP açık sisteme güzel bir örnektir. Piyasalarda çok sayıda ürün bulunabilir.

- Açık sistem (open system), iki sistemin altyapılarına bağlı kalmaksızın iletişimini sağlayan protokoller kümesidir.
- OSI bir ağ mimarisinin tasarlanması ve anlaşılmasında kullanılan kavramsal (gerçeklenmemiş) bir modeldir.
- OSI birbirinden ayrı ancak ilişkide olan 7 katmandan oluşur.
- Her katman iletişim için kendisine atanmış bazı işlemleri yapar.
- Gönderici ve alıcıdaki eş katmanlar aynı protokolü kullanır



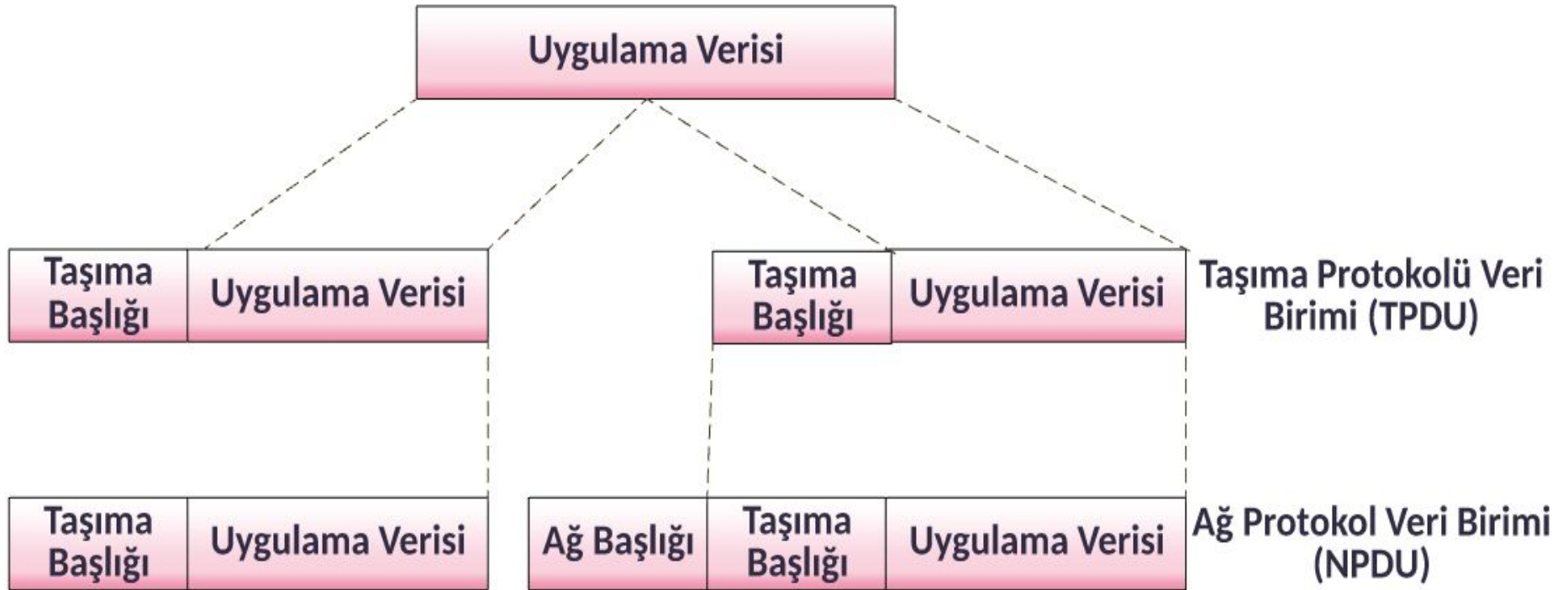
Katmanlı mimarinin tercih edilme nedenleri:

- ✓ Karmaşıklık azaltılır (böl ve yönet)
- ✓ Gelişimi hızlandırır
- ✓ Öğrenme ve öğretmeyi basitleştirir

Protokol Veri Birimleri PVB (PDU)

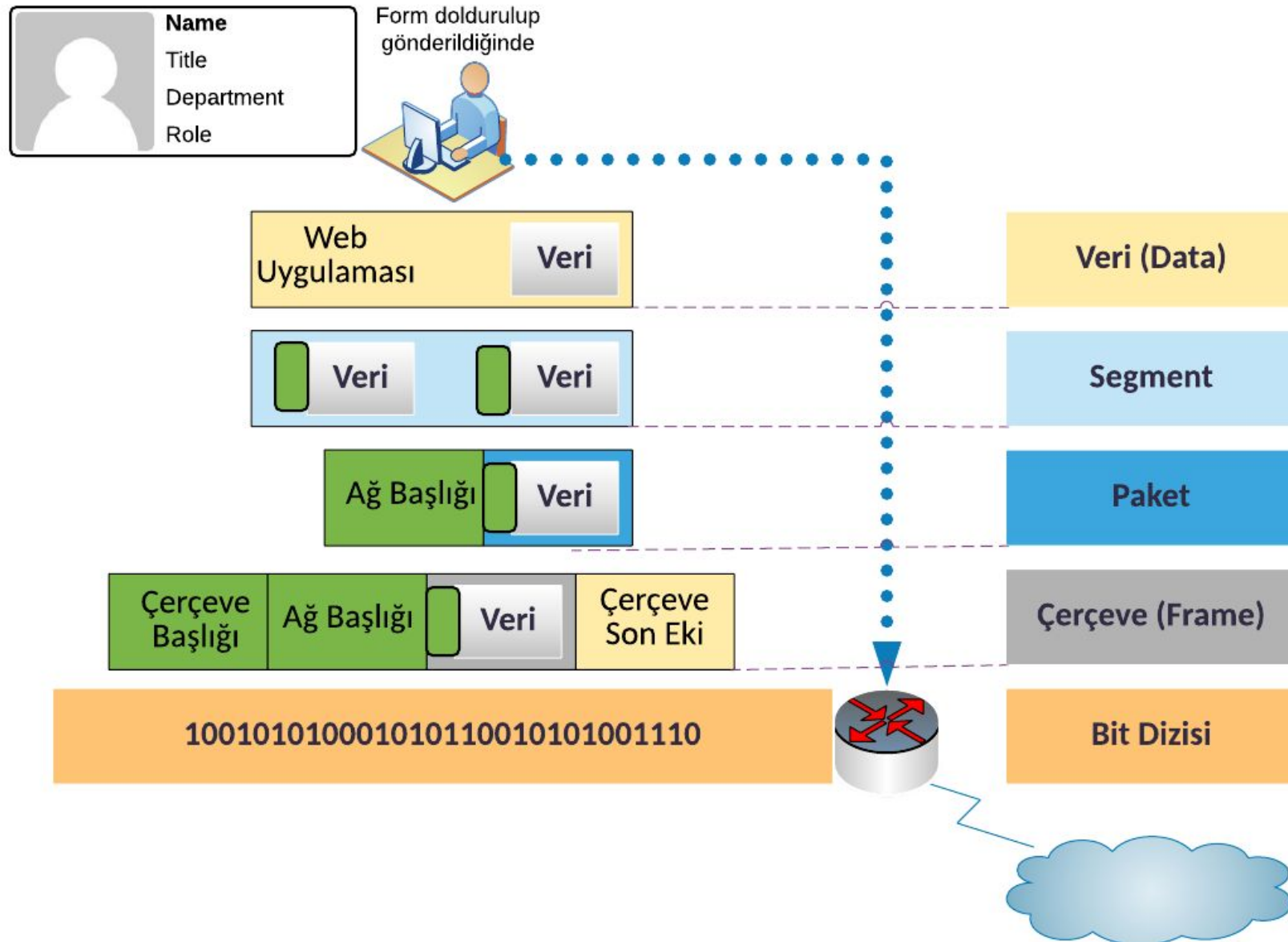
- ✓ Her bir katmanda haberleşme için protokoller kullanılır.
- ✓ Her bir katmandaki kullanıcı verisine kontrol bilgisi eklenir.
 - Adres bilgisi
 - Hata algılama kodu
 - Protokol kontrol
 - Protokol fonksiyonlarını uygulamak için eklenmesi gereken bilgiler.
- ✓ Bu işleme Zarflama (Encapsulation) denir.
- ✓ Zarflama işlemi sonucunda PVB oluşur.

PROTOKOL VERİ BİRİMİ



Protokol Data Birimi (PDU) = Kontrol Bilgisi + Her Katmandaki Veriler

TCP/IP de PVB



TCP/IP Mimarisi

OSI Referans Modeli TCP/IP Modeli

| | |
|---------------|-----------|
| Uygulama | Uygulama |
| Sunum | |
| Oturum | |
| Taşıma | Taşıma |
| Ağ | İnternet |
| Veri Bağlantı | Ağ Erişim |
| Fiziksel | |

Uygulama Katmanı

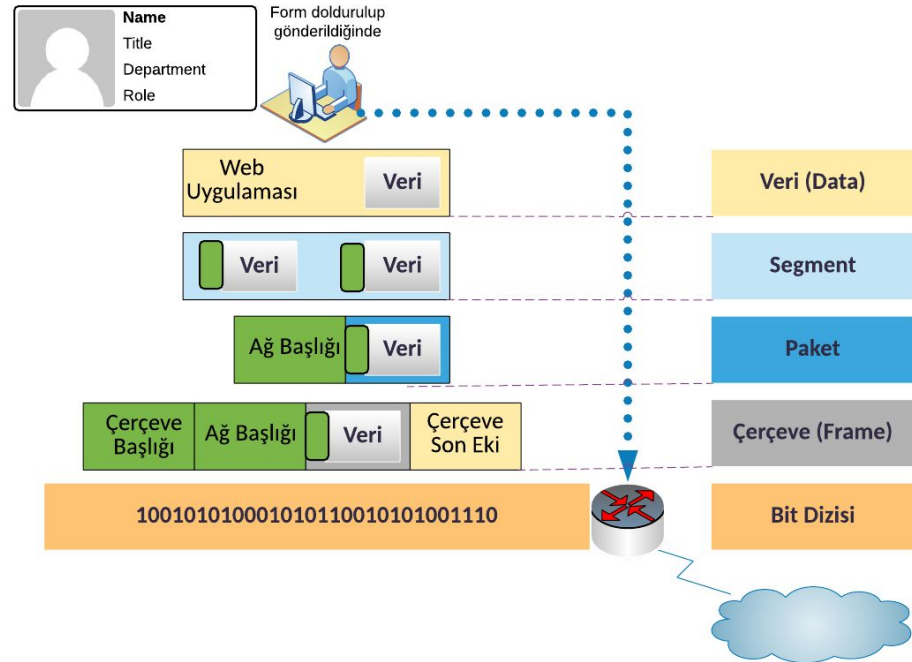
- GÜygulamaların ağa erişimini sağlayan protokollerdir.
- Uygulamanın kendisi değildir.
- Örneğin; bir web tarayıcısının kullandığı http gibi.
- HTTP, FTP, SMTP, Telnet, DHCP, SIP vs. protokoller uygulama katmanında çalışır.

Oturum Katmanı

- Gönderilecek veriye check point eklenmesi (senkronizasyon): 2000 sayfa gönderilecek, her 100 sayfadan sonra check point eklenir. 523. sayfada sorun olduğunda önceki 500 sayfanın gönderilmesi önlenir.
- İki sistemin dialog kurmasına imkan verir (dialog control).

Sunum Katmanı

- Format/kod dönüşümleri
- Şifreleme/şifre çözme
- Sıkıştırma/Açma



Taşıma Katmanı

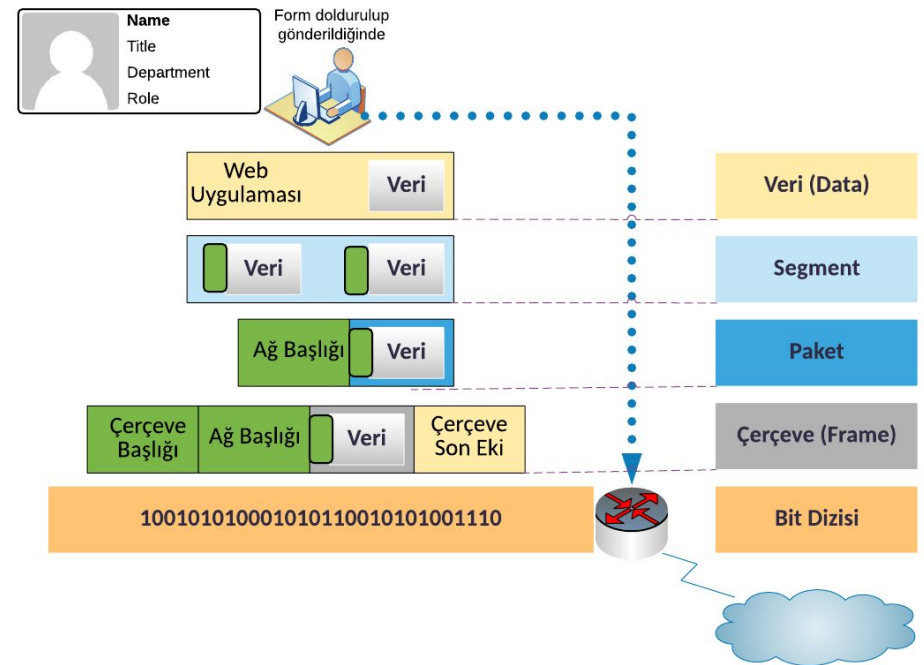
Uygulamaların adreslenmesi sağlanır. Port adresi burada belirlenir.

Ağ katmanı paketler arasında ilişki oluşturmaz. Bu katmanda oluşturulur; sıralama, akış denetimi, hata denetimi.

Mesajlar segmentlere bölünerek sıra numarası eklenir. Sıralama işlemi yapılır.

Uçtan uca akış denetimi ve hata denetimi yapılır. Veri Bağlantı katmanı iki komşu düğüm arasında yapar.

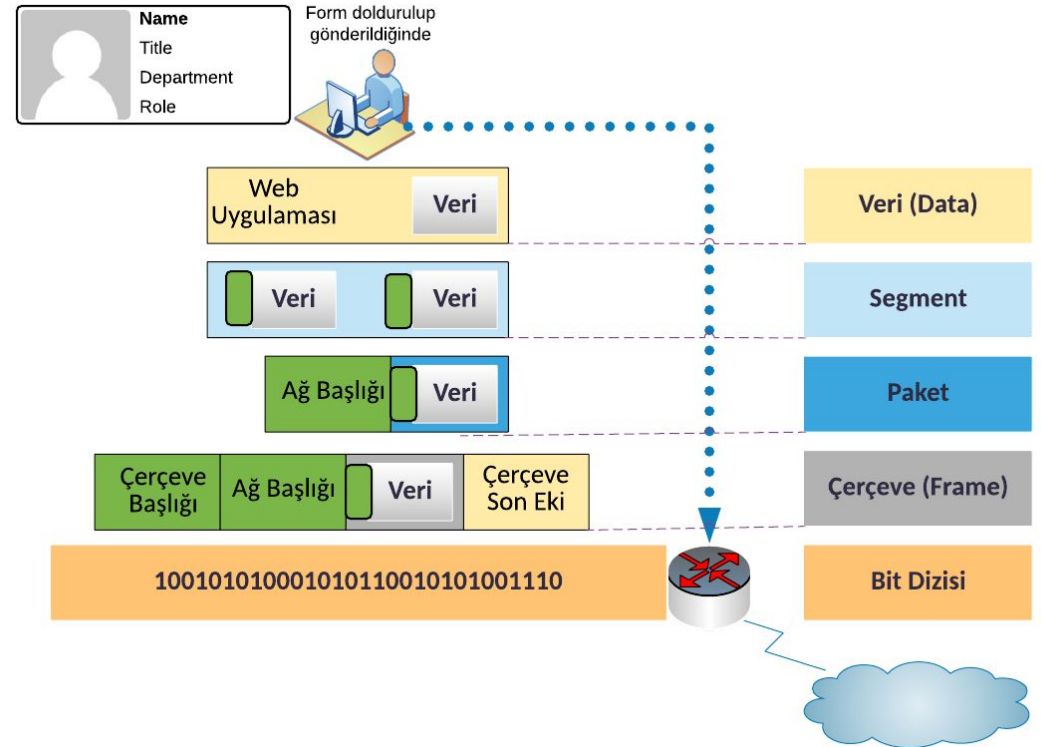
TCP ve UDP burada çalışır.



Ağ Katmanı

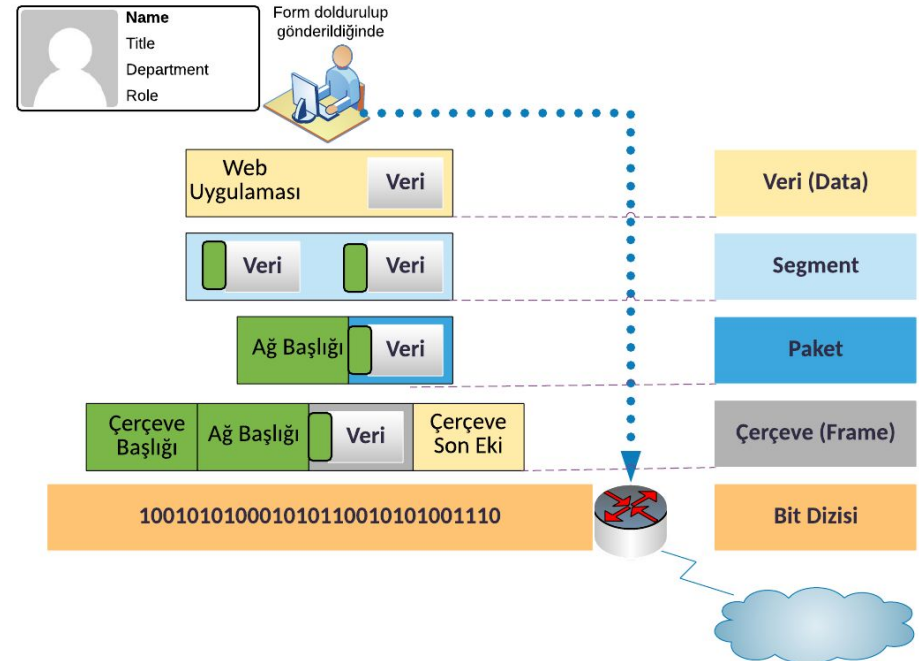
Mantıksal adresleme yapılır. Alıcı ve göndericinin mantıksal adresleri pakete eklenir.

Yönlendirme işlemi bu katmanın görevidir. Paketlerin nereye yönlendirileceğine karar verilir.



Veri Bağlantı Katmanı

- Fiziksel katmandaki basit veri iletimini güvenilir bağlantıya çevirir.
- Ağ katmanından gelen verileri çerçeve(frame)'lere böler.
- **Fiziksel adresleme yapılır.** Çerçevevelere header (alıcı ve verici adresleri) ve trailer (hata denetim bilgisi) ekler.
- Çerçeve bazında akış denetimi yapar.
- Hata denetimi yapar. Kaybolan ve bozulan çerçeveler yeniden gönderilir (retransmit).
- Erişim denetimi yapar. İletim ortamının cihazlar arasında nasıl paylaşılacağı belirlenir.



Fiziksel Katman

Fiziksel ortamda bitlerin taşınması için gerekli işlemler gerçekleştirilir.

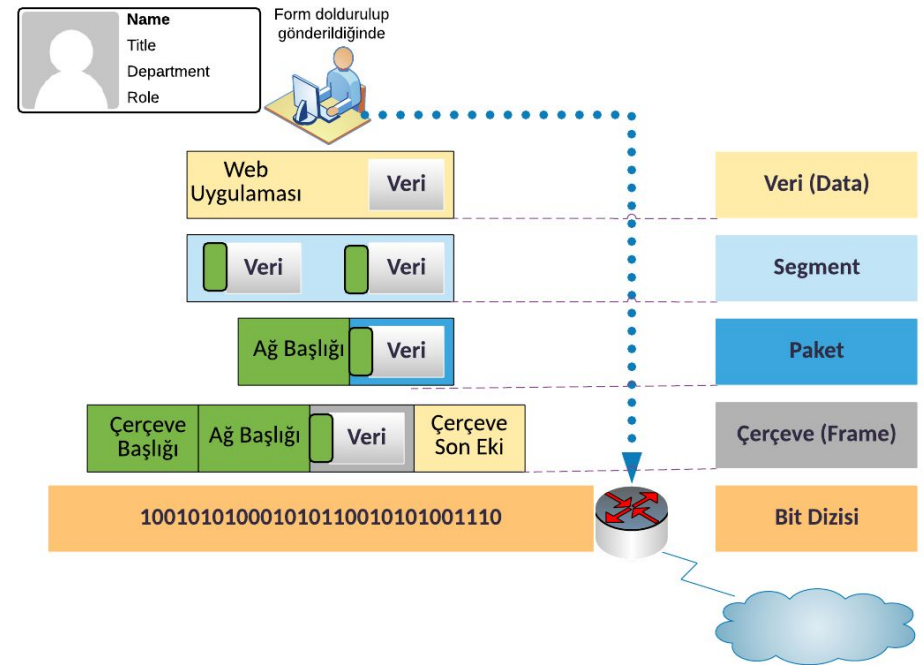
Bitlerin gösterimi tanımlanır (modülasyon, kanal kodlama v.s.)

Veri iletim hızı belirlenir. (bps)

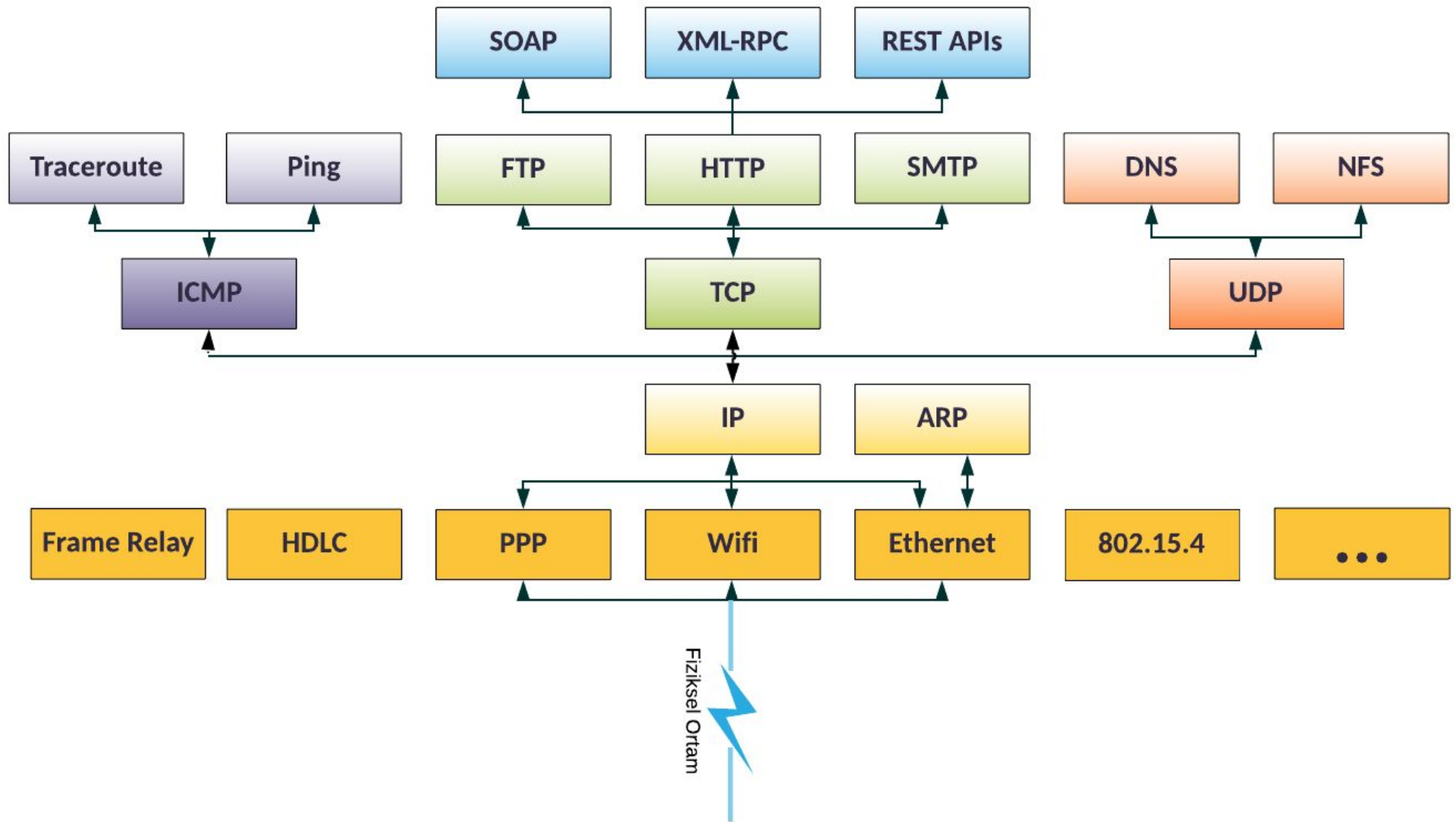
Alıcı ve gönderici arasında bit seviyesinde senkronizasyon yapılır.

Ağ topoloji tanımlanır.(mesh, star, bus, ring)

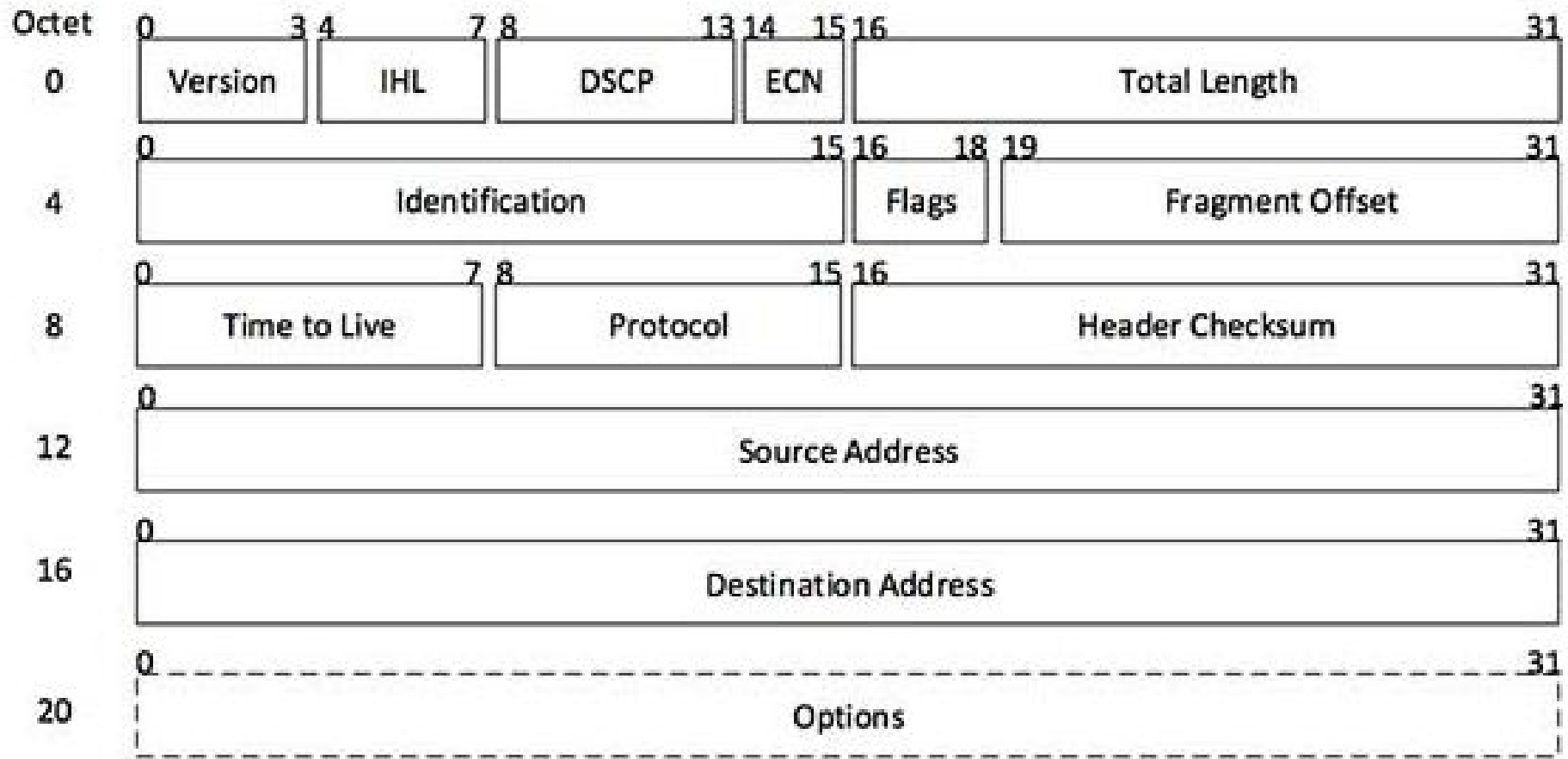
İletim modu tanımlanır. (simplex, half-duplex, full-duplex)



TCP/IP Protokolleri



Ağ Katmanı - IP Başlığı



http://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm

Anahtar

Learning

Flooding

Filtering

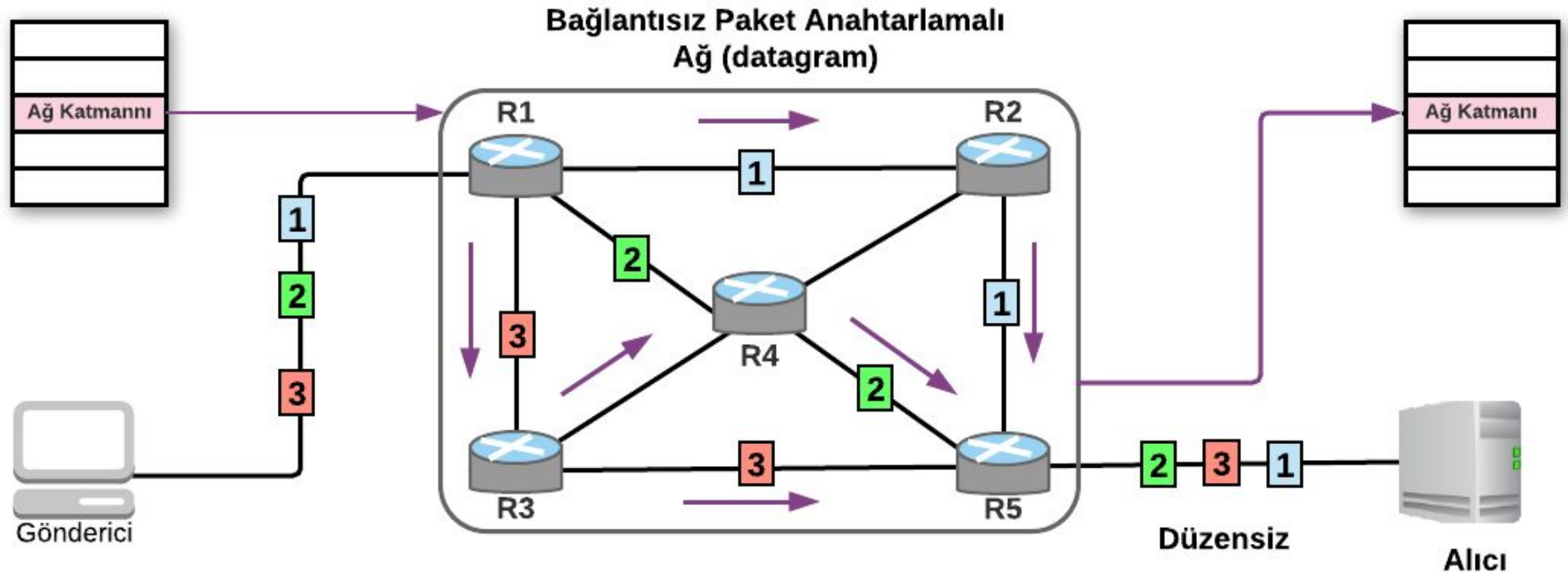
Forwarding

Aging

(<https://computer.howstuffworks.com/lan-switch11.htm>)

AgProgramlama1Anahtar.swf

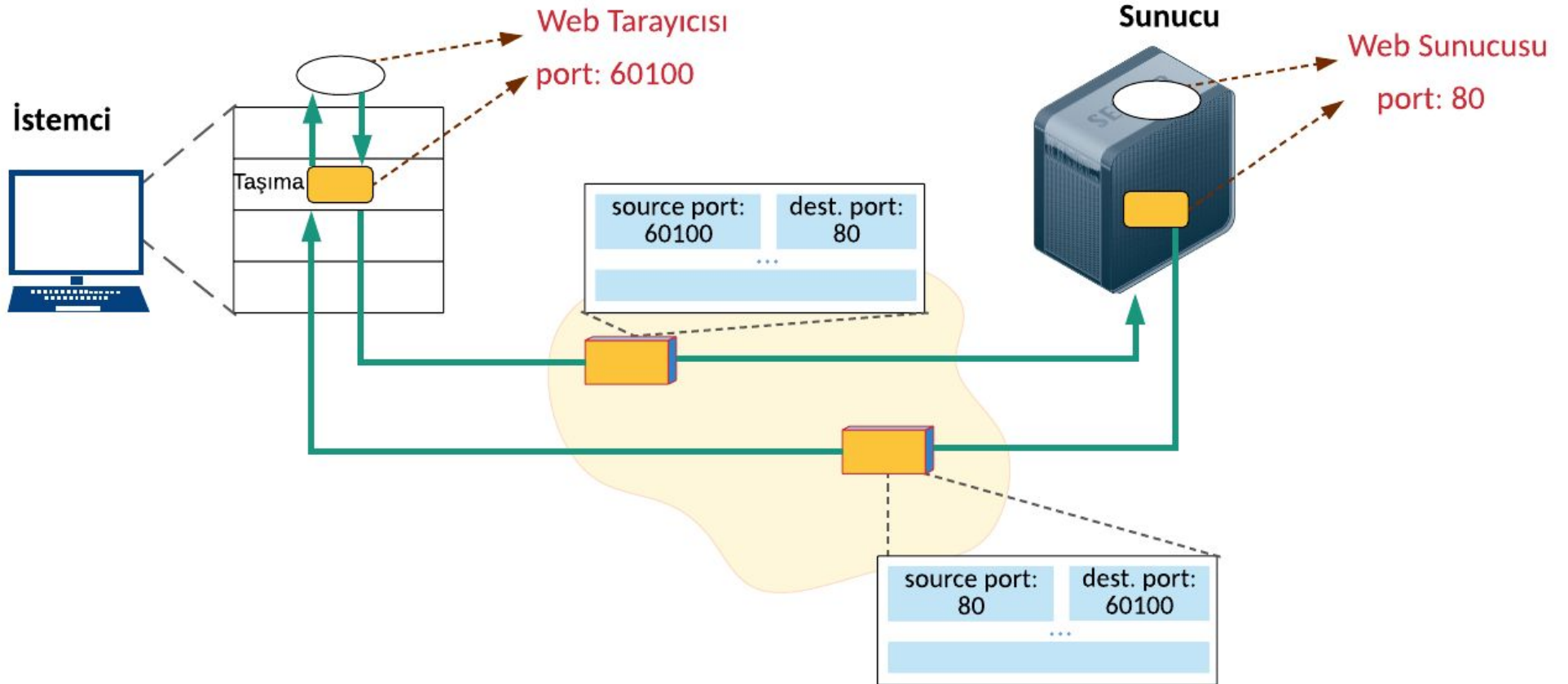
Yönlendirici



AgProgramlama1Yonlendirici.swf

Taşıma Katmanı : Port Adresi

Uygulamaların adreslenmesi sağlanır. Port adresi burada belirlenir.



Taşıma Katmanı : Port Adresi

- ✓ Bilgisayarlar IP ile adreslenir.
- ✓ Bilgisayarda çalışan uygulamaları adreslemek için, taşıma katmanında, port numaraları kullanılır.
- ✓ 0-65535 arası değerler alır. (2 byte)
- ✓ 0-1024 bilinen protokollere tahsis edilmiştir.
- ✓ 1,024 to 49,151 RFC lerde tanımlı değildir, IANA organize eder.
- ✓ 49,152 to 65,535 genel amaçlı

Port Adresi

GNU nano 2.2.6

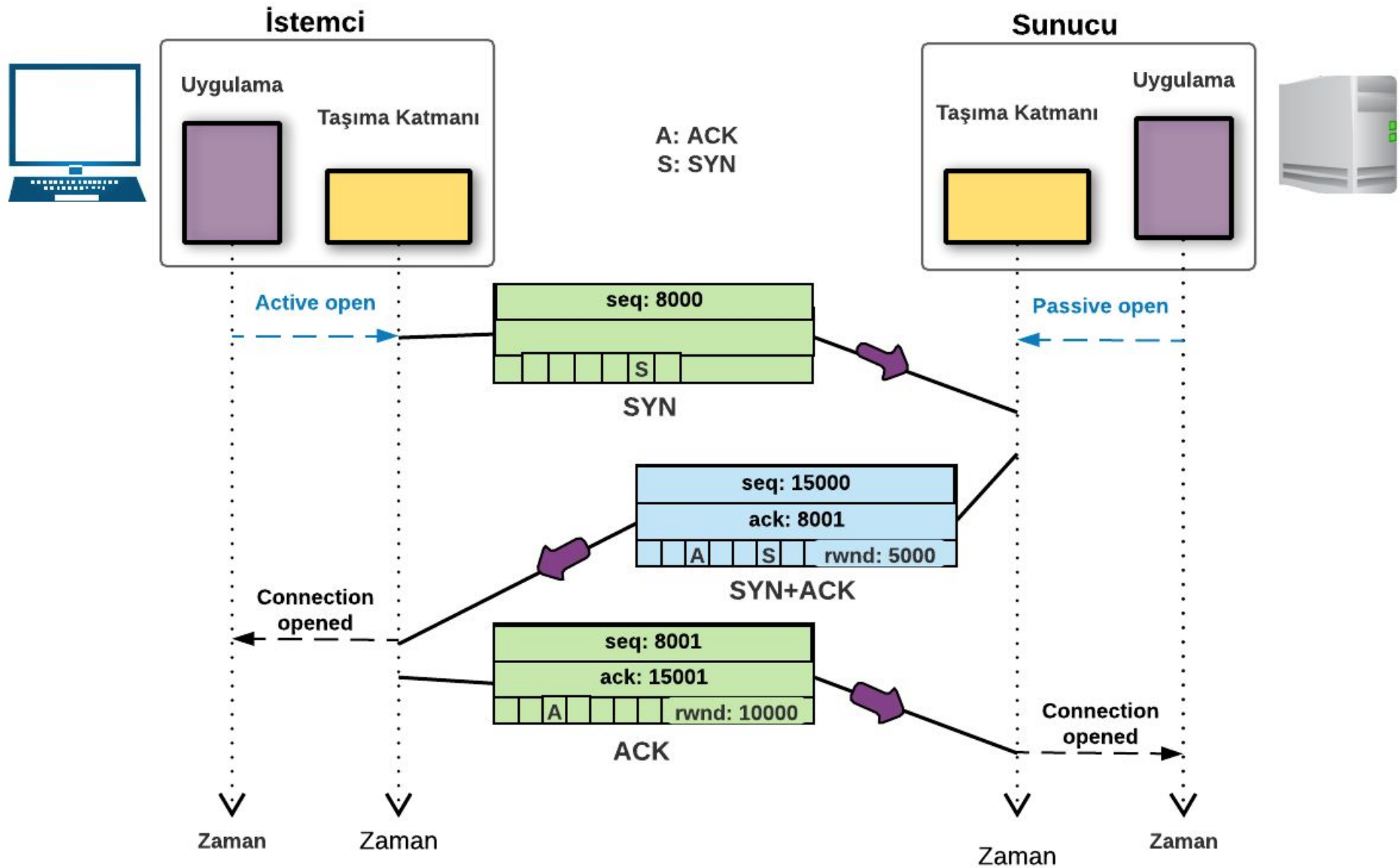
File: /etc/services

```
discard      9/udp      sink null
systat       11/tcp     users
daytime      13/tcp
daytime      13/udp
netstat      15/tcp
qotd         17/tcp     quote
msp          18/tcp     # message send protocol
msp          18/udp
chargen      19/tcp     ttytst source
chargen      19/udp     ttytst source
ftp-data     20/tcp
ftp          21/tcp
fsp          21/udp     fspd
ssh          22/tcp     # SSH Remote Login Protocol
ssh          22/udp
telnet       23/tcp
smtp         25/tcp     mail
time         37/tcp     timserver
time         37/udp     timserver
rlp          39/udp     resource    # resource location
nameserver   42/tcp     name        # IEN 116
whois        43/tcp     nickname
tacacs       49/tcp     # Login Host Protocol (TACACS)
tacacs       49/udp
re-mail-ck   50/tcp     # Remote Mail Checking Protocol
re-mail-ck   50/udp
domain       53/tcp     # Domain Name Server
domain       53/udp
mtp          57/tcp     # deprecated
```

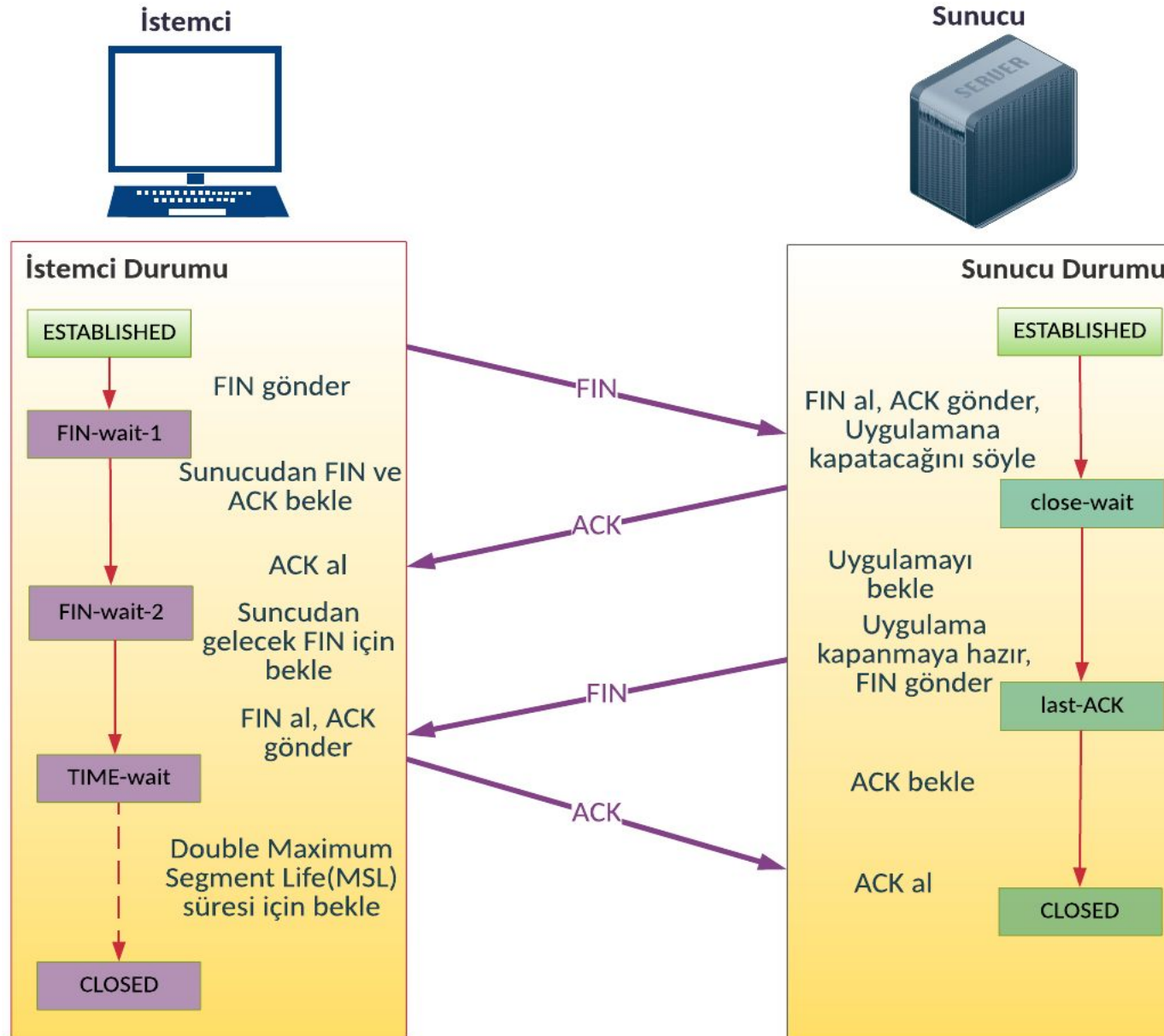
Port Adresi

| | | | |
|-----------|---------|-----------------------------|--------------------------------|
| tacacs-ds | 65/tcp | | # TACACS-Database Service |
| tacacs-ds | 65/udp | | |
| bootps | 67/tcp | | # BOOTP server |
| bootps | 67/udp | | |
| bootpc | 68/tcp | | # BOOTP client |
| bootpc | 68/udp | | |
| tftp | 69/udp | | |
| gopher | 70/tcp | | # Internet Gopher |
| gopher | 70/udp | | |
| rje | 77/tcp | netrjs | |
| finger | 79/tcp | | |
| http | 80/tcp | www | # WorldWideWeb HTTP |
| http | 80/udp | | # HyperText Transfer Protocol |
| link | 87/tcp | ttylink | |
| kerberos | 88/tcp | kerberos5 krb5 kerberos-sec | # Kerberos v5 |
| kerberos | 88/udp | kerberos5 krb5 kerberos-sec | # Kerberos v5 |
| supdup | 95/tcp | | |
| hostnames | 101/tcp | hostname | # usually from sri-nic |
| iso-tsap | 102/tcp | tsap | # part of ISODE |
| acr-nema | 104/tcp | dicom | # Digital Imag. & Comm. 300 |
| acr-nema | 104/udp | dicom | |
| csnet-ns | 105/tcp | cso-ns | # also used by CS0 name server |
| csnet-ns | 105/udp | cso-ns | |
| rtelnet | 107/tcp | | # Remote Telnet |
| rtelnet | 107/udp | | |
| pop2 | 109/tcp | postoffice pop-2 | # POP version 2 |
| pop2 | 109/udp | pop-2 | |
| pop3 | 110/tcp | pop-3 | # POP version 3 |
| pop3 | 110/udp | pop-3 | |

TCP Bağlantı Kurulumu



TCP Bağlantı Sonlandırma



Traceroute ile Topoloji Keşfi

> traceroute google.com

```
wsans-MacBook-Pro:~ wsan$ traceroute google.com
traceroute to google.com (216.58.206.174), 64 hops max, 52 byte packets
 1  mitrastar.home (192.168.1.1)  1.381 ms  1.383 ms  1.951 ms
 2
 3
 4
 5                                     .834 ms  7.235 ms  7.139 ms
 6  * * 212.156.104.84 307-sof-col-2.34-acibadem-xrs-t2-2.statik.turktelekom.com.tr (212.156.104.84)  44.028 ms
 7  74.125.51.92 (74.125.51.92)  38.954 ms  38.680 ms  37.397 ms
 8  108.170.250.177 (108.170.250.177)  38.605 ms  42.566 ms
   108.170.250.161 (108.170.250.161)  39.071 ms
 9  108.170.238.171 (108.170.238.171)  38.385 ms
   209.85.142.55 (209.85.142.55)  73.846 ms  73.531 ms
10  sof02s27-in-f14.1e100.net (216.58.206.174)  41.664 ms  46.516 ms  41.453 ms
wsans-MacBook-Pro:~ wsan$
```

> sudo tcpdump -i en0

```
12:22:18.723264 IP 108.170.250.177 > 192.168.1.9: ICMP time exceeded in-transit, length 60
12:22:18.724076 IP 192.168.1.9.55833 > mitrastar.home.domain: 57859+ PTR? 177.250.170.108.in-addr.arpa. (46)
12:22:18.809983 IP mitrastar.home.domain > 192.168.1.9.55833: 57859 NXDomain 0/1/0 (106)
12:22:18.810369 IP 192.168.1.9.33599 > sof02s17-in-f14.1e100.net.33457: UDP, length 24
12:22:18.852771 IP 108.170.250.161 > 192.168.1.9: ICMP time exceeded in-transit, length 60
12:22:18.853414 IP 192.168.1.9.54593 > mitrastar.home.domain: 65251+ PTR? 161.250.170.108.in-addr.arpa. (46)
12:22:18.922493 IP mitrastar.home.domain > 192.168.1.9.54593: 65251 NXDomain 0/1/0 (106)
12:22:18.922864 IP 192.168.1.9.33599 > sof02s17-in-f14.1e100.net.33458: UDP, length 24
12:22:18.967380 IP 108.170.250.161 > 192.168.1.9: ICMP time exceeded in-transit, length 60
12:22:18.967494 IP 192.168.1.9.33599 > sof02s17-in-f14.1e100.net.33459: UDP, length 24
12:22:19.008830 IP 216.239.54.3 > 192.168.1.9: ICMP time exceeded in-transit, length 60
12:22:19.009518 IP 192.168.1.9.53033 > mitrastar.home.domain: 44208+ PTR? 3.54.239.216.in-addr.arpa. (43)
12:22:19.151670 IP mitrastar.home.domain > 192.168.1.9.53033: 44208 NXDomain 0/1/0 (103)
12:22:19.152189 IP 192.168.1.9.33599 > sof02s17-in-f14.1e100.net.33460: UDP, length 24
12:22:19.195195 IP 216.239.54.1 > 192.168.1.9: ICMP time exceeded in-transit, length 60
12:22:19.195789 IP 192.168.1.9.62902 > mitrastar.home.domain: 11391+ PTR? 1.54.239.216.in-addr.arpa. (43)
12:22:19.323266 IP mitrastar.home.domain > 192.168.1.9.62902: 11391 NXDomain 0/1/0 (103)
12:22:19.323752 IP 192.168.1.9.33599 > sof02s17-in-f14.1e100.net.33461: UDP, length 24
12:22:19.365684 IP 216.239.54.1 > 192.168.1.9: ICMP time exceeded in-transit, length 60
12:22:19.365804 IP 192.168.1.9.33599 > sof02s17-in-f14.1e100.net.33462: UDP, length 24
12:22:19.404143 IP sof02s17-in-f14.1e100.net > 192.168.1.9: ICMP sof02s17-in-f14.1e100.net udp port 33462 unreachable
```

Ağ Geçidi (Gateway) & Firewall

- ✓ İç ağ dışarıya bağlayan düğümlere ağ geçidi denir. Yönlendirici, ADSL Modem, ya da bir bilgisayar olabilir. Üzerinde iki ağ arayüz kartı bulunur.
- ✓ İç ağ ile dış ağ arasındaki trafiği (gelen/giden) denetleyen ve uygun olmayanları (uygun olmayan port, ya da IP bloğu) filtreleyen donanımsal/yazılımsal düğümlere ateş duvarı (firewall) denir.

Vekil Sunucu (Proxy Server)

- ✓ İç düğümler için vekil sunucu tanımlandığında dışarıya çıkış vekil sunucu üzerinden olur. (Ateş duvarı sadece vekil sunucuya izin verir.) Böylece içerik filtreleme ve loglama yapılabilir. Dışarıdan sadece proxy görülür. Proxy dışarıdan gelen trafiği ilgili istemciye iletir. İç düğümlere erişim daha güvenlidir.
- ✓ Vekil sunucular genellikle uygulama katmanında (http, ftp, smtp) çalışırlar (SOCKS vekil sunucular taşıma katmanında çalışır).
- ✓ Ön bellekleme yapmak için de kullanılırlar. Bir istemci dışarıdan bir dosya istediğinde proxy ilk olarak kendi ön belleğine bakar ve dosya var ise dışarıdan getirmez kendisinde bulunanı gönderir.

Kaynaklar

- ✓ Behrouz A. Forouzan, Firouz Mosharraf, Computer Networks: A Top Down Approach
- ✓ http://www.tcpipguide.com/free/t_TCPConnectionTermination-2.htm
- ✓ http://www.tutorialspoint.com/ipv4/ipv4_packet_structure.htm
- ✓ Kurose J., Ross K., “Computer Networking: A Top Down Approach”, Pearson, 2013