

ICMP hangi protokolu
ping ne isi yara

google'e ping atmak için " ping 8.8.8.8" yapılıyor ve hangi protokol ICMP ve hangi katman? ağ katman

internet'e çekiyorsun ve switch'a kadar gidebiliyorsun ama internet'e gidemiyorsan ping ile hata nerede olduğunu tespit edebiliriz

TCP/IP Protokol Kümesi

Temel Kavramlar

Portokol acikla:
port
cat-r25

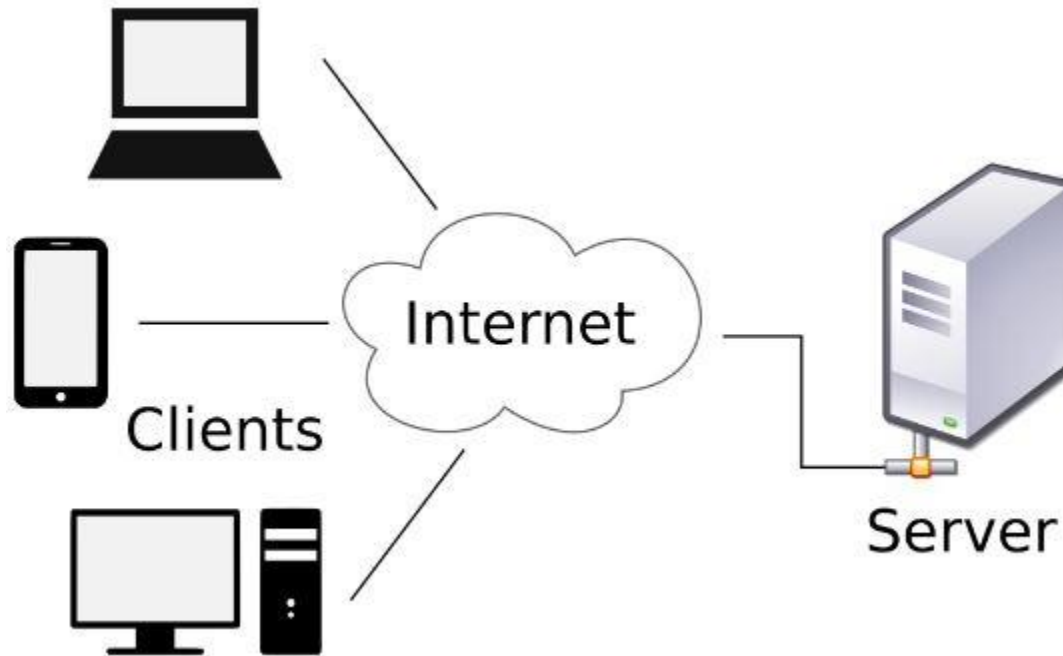
protokol:ortak kabullar

Protokol: Bir ağ üzerindeki bilgisayarlar arasındaki iletişimi yöneten kurallar kümesidir.

İstemci/Sunucu Mimarisi:

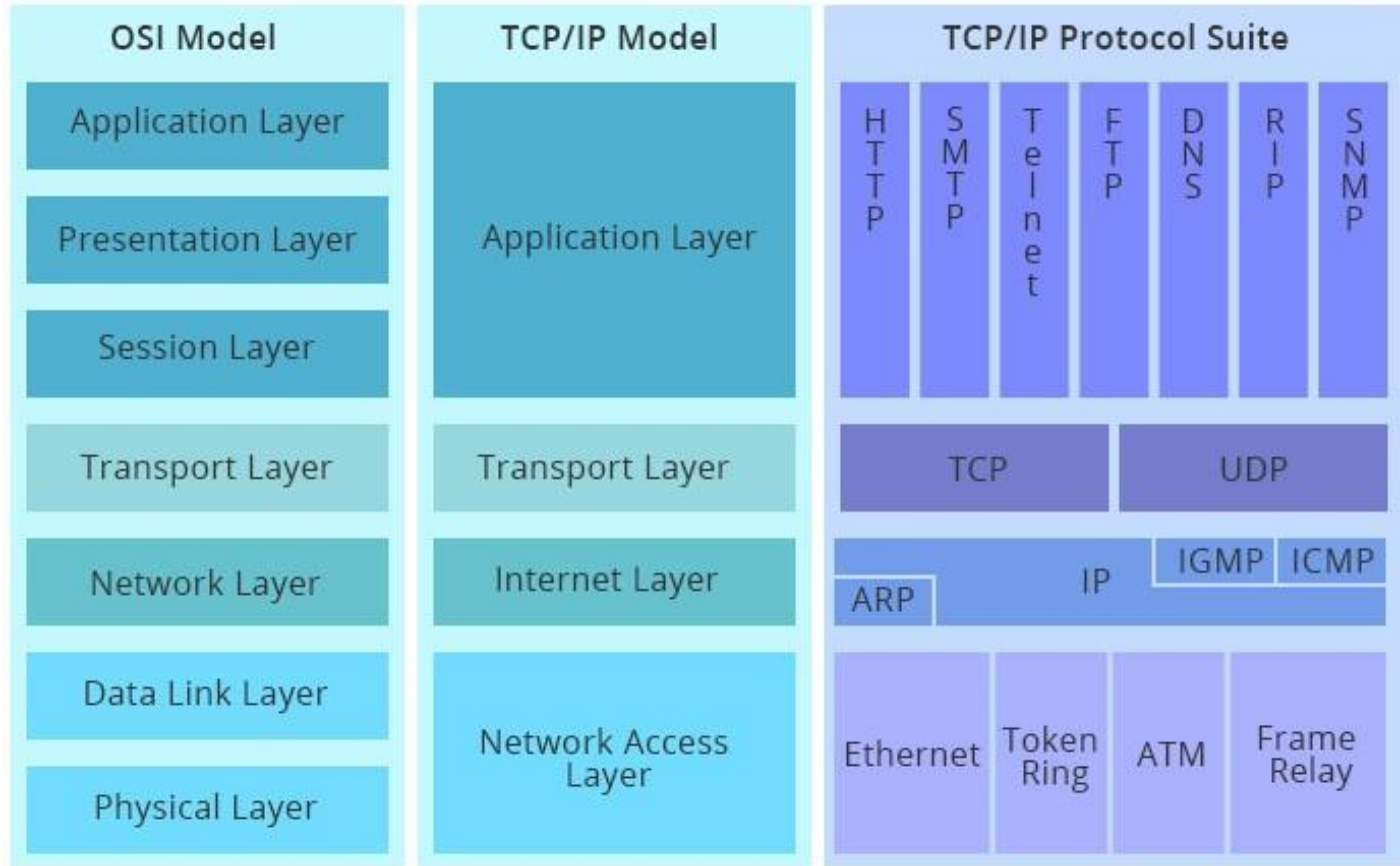
Port: İstemcilerin birbirleriyle iletişimde kullandığı sanal bağlantı noktalarıdır.

65353bin portvar



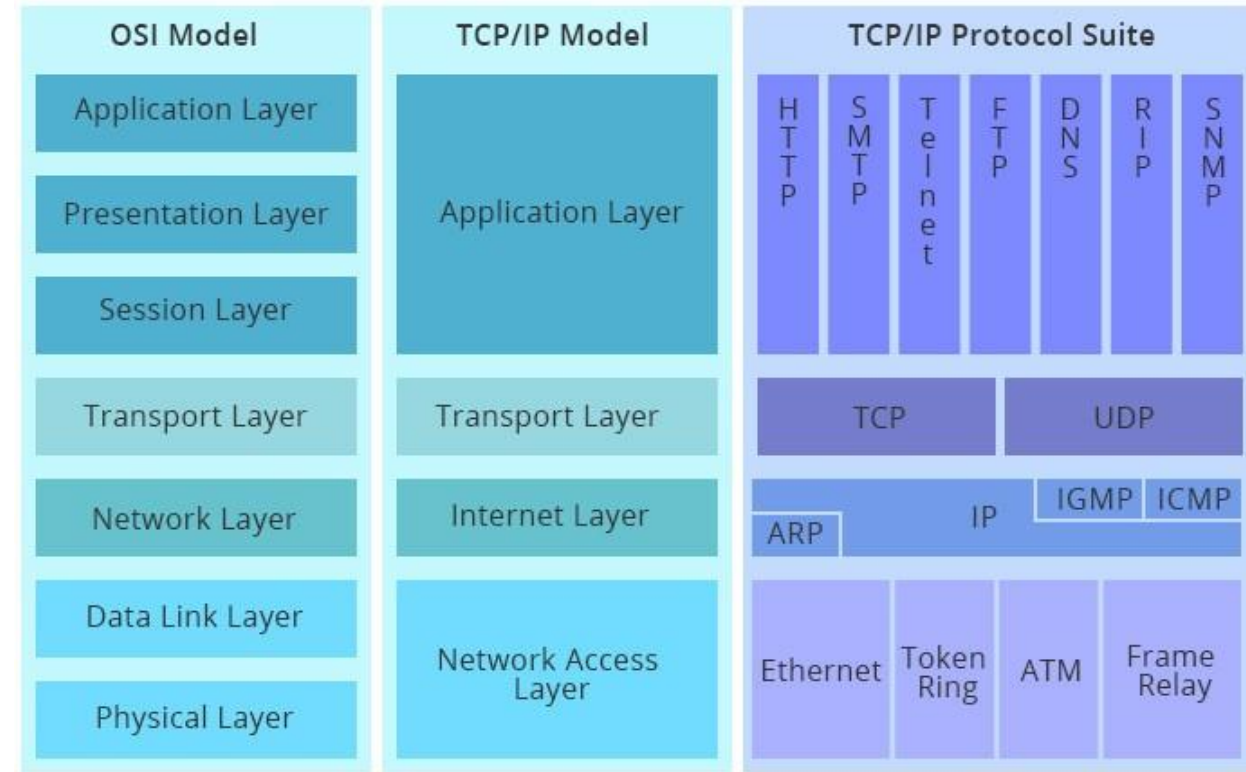
Giriş

- TCP/IP ağiletişimi için tanımlanmış bir protokol kümesidir.
- İnternet ağında TCP/IP protokol kümesi kullanılmaktadır.
- Bu model ABD Savunma Bakanlığı tarafından geliştirilmiş bir modeldir.
- Tasarlanışının nedeni ise nükleer savaş dâhil her türlü şartta sürekli ayakta durabilen bir ağ yapısının istenmesiydi.
- TCP/IP (Transmission Control Protocol / Internet Protocol) modeli OSI standartlarına uygun düzenlenmiş 4 katmandan oluşmaktadır. orada 7 ama burada 4 cunku bazi katmanlar zip yaptilar
- TCP ve IP isimleri bu küme içerisinde birer protokol adı iken "TCP/IP" şeklinde kullanılması protokol kümesine işaret eder.



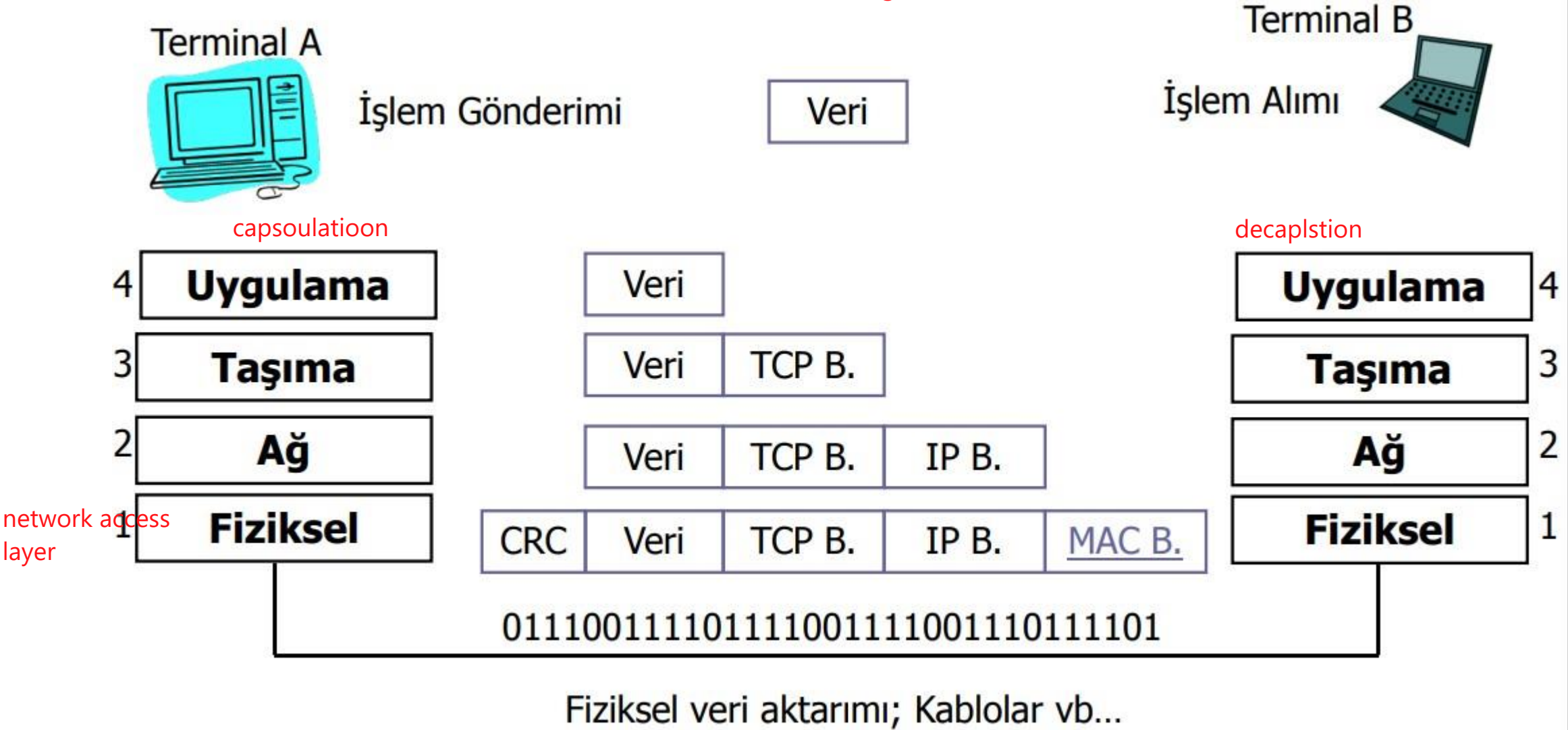
TCP/IP Katmanları

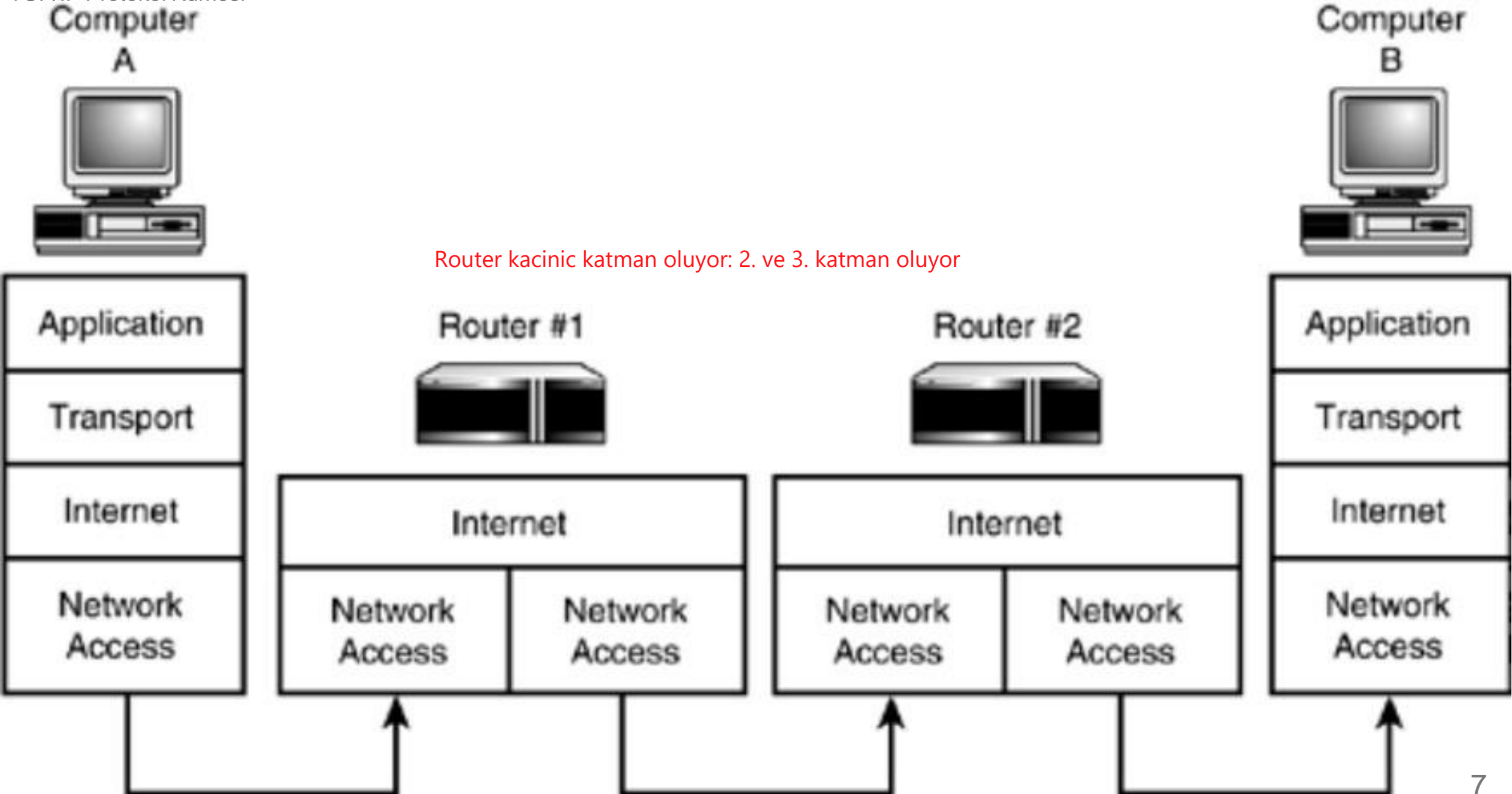
1. Fiziksel Katman - Ağ Erişim Katmanı
2. İnternet Katmanı - Ağ Katmanı
3. Taşıma Katmanı
4. Uygulama Katmanı

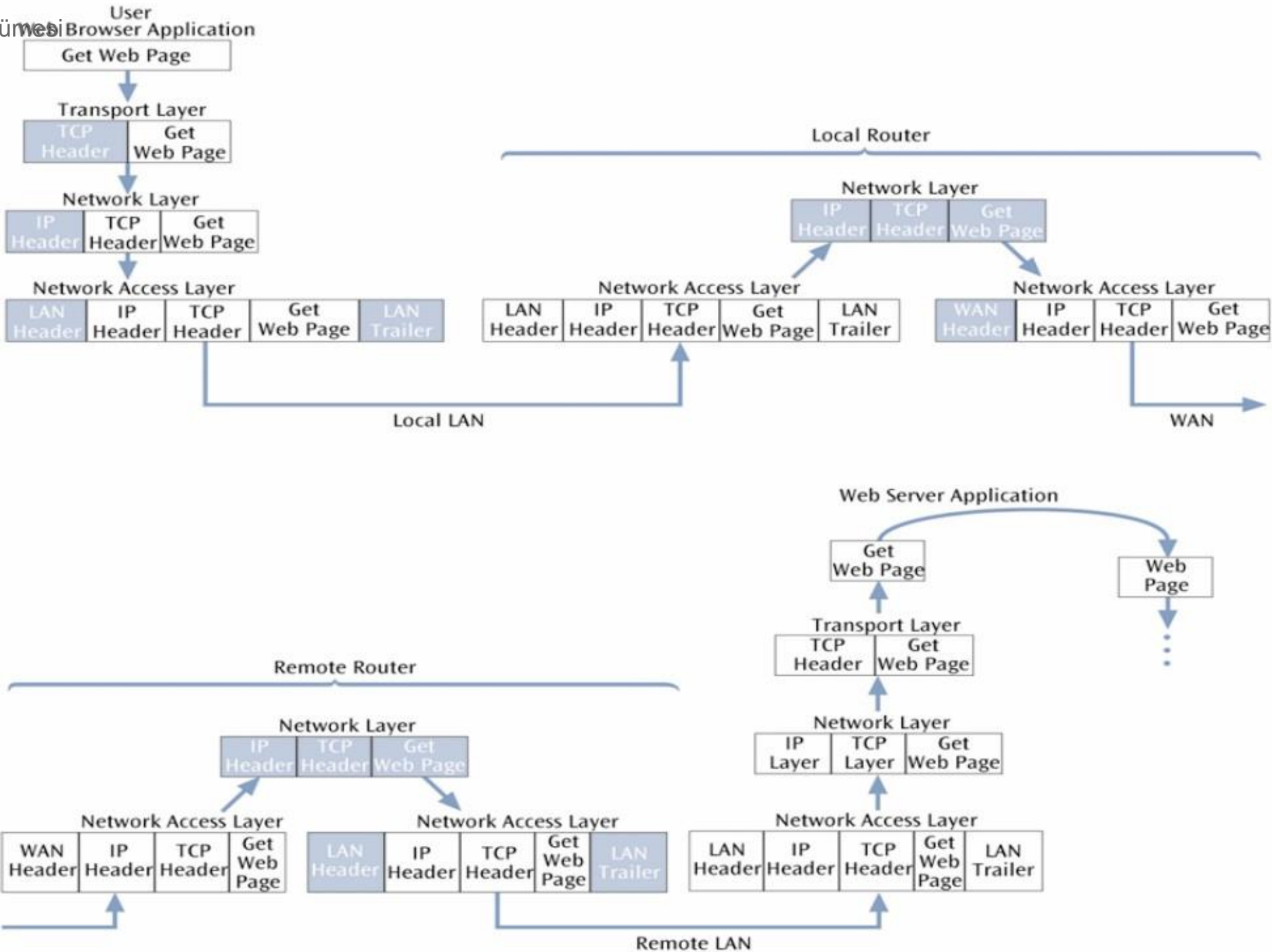


Veri Aktarımı

buradan bir soru gelecek







Protokoller

adin gibi ezberle
çok önemli

TCP/IP Layers

Application Layer
Transport Layer
Network Layer
Network Interface Layer

TCP/IP Prototocols

HTTP	FTP	Telnet	SMTP	DNS <small>SSH</small>
TCP			UDP	
IP		ARP	ICMP	IGMP
Ethernet	Token Ring		Other Link-Layer Protocols	

önemli

Uygulama Katmanı

- OSI modelindeki üst katmanlardan Uygulama, Sunum ve Oturum katmanlarının birleşiminden oluşan TCP/IP katmanıdır.
- Uygulamaların çalışması, iletim için hazırlık ve ortak bir formatta haberleşme bu katmanda gerçekleşir.
- Son kullanıcının etkileşime girdiği katman.

oturum

sunum

Uygulama Katmanı Protokolleri

Uygulama katmanında tanımlı olan protokoller web tarayıcı, e-posta, dosya aktarımı gibi uygulamalara hizmet verirler.

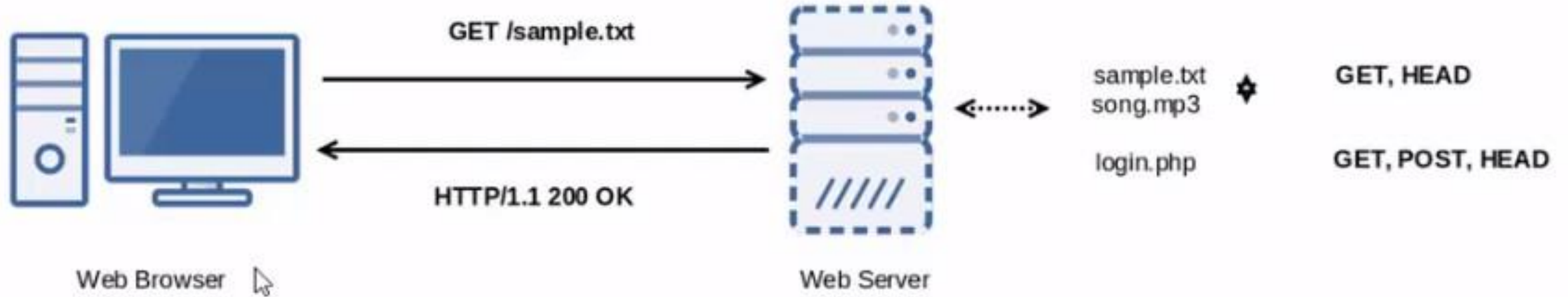
Uygulama katmanı protokollerinden bazıları şunlardır:

HTTP (HyperText Transfer Protocol)

- Web sayfalarının aktarımı için kullanılır. sinavda
- Kullanıcı istekte bulunur, sunucu web sayfa içeriğini gönderir.
- Öntanımlı port numarası 80.

HTTPS (Secure HTTP)

- HTTP isteklerini ve yanıtlarını şifrelenmiş biçimde iletir.
- SSL. S temesil eder
- Öntanımlı port numarası 443. güvenli



bilgisayarlarda: 65535: port var

FTP (File Transfer Protocol)

- Dosya aktarım protokolüdür.
- FTP hizmeti öntanımlı 21. porttan yapılır.

SNMP (Simple Network Management Protocol)

- Ağ içerisinde bulunan router, switch gibi cihazların merkezi bir yerden gözlenmesi ve yönetilmesi için kullanılan protokoldür.

Hala uygulama katmandayız

SMTP (Simple Mail Transfer Protocol)

- E-posta gönderimi için kullanılır.
- Güvensiz bağlantılar için 25.
- Güvenli bağlantılar için 465. veya 587. portlar kullanılır.
- Mümkünse 587. port tercih edilir.

mail'ler için

IMAP (Internet Access Message Protocol)

- Sunucudaki mailleri istemci tarafına alabilen ve yönetebilen protokol.
- Mail gönderemez.
- Güvensiz bağlantı için 143. güvenli bağlantı için 993. port kullanılır.

POP3 (Post Office Protocol v3)

- Sunucudan mailleri **çekip okumaya imkan sağlayan** protokol.
- **Güvensiz** bağlantı için **110. portu**, güvenli bağlantı için **995.** portu kullanır.

IMAP vs POP3

POP3:

- Bağlantı kurulduktan sonra mesajlar tamamen istemciye **taşınır** ve bağlantı kapatılır.
- Tüm e-postalar ilk bağlanan istemciye indiğinden başka istemciler indiremez.

IMAP:

- E-posta okunacağı zaman bağlantı kurulur, e-postanın kopyası istemciye indirilip bağlantı kapatılır.
- E-postaların kopyası sunucuda bırakıldığından başka istemciler de o e-postalara erişebilir.

ip dagitier

DHCP (Dynamic Host Configuration Protocol)

gorevi nedir:
ip dagitiyor

- İstemcilere otomatik ip adresi dağıtır.
- 67 ve 68. portları kullanır.

DNS (Domain Name System)

bu linkeri donustorleri ip'ye

- Alan adları ile IP adreslerini birbirine bağlayan sistemdir.
- Paylaşılmış bir veritabanı olarak çalışır.
- **53** numaralı portu kullanır.

Ör: Alan adı: ecylmz.com, IP adresi: 185.199.111.153

biligisayr ip anlar ama bix .com anlyoruz

ip'ler static ve sabit olabilir(dinamik)
ama MAC dagisiyor

Telnet

- En eski bağlantı şekillerinden biridir.
- Uzaktaki bilgisayarlara bağlanmak için kullanılır.
- **23** numaralı port kullanılır.

giris yapabiliriz

Ping

banlnti salnıp saglanmadini kontrol eder

- Ping, bir IP adresinin veya bir bilgisayarın erişilebilirliğini test etmek için kullanılan bir yardımcı programıdır.

ping 8.8.8.8
google dns

burad 22 port

hangi portokol 32 port kulanir

SSH (Secure Shell)

- SSH, telnet gibi uzaktaki sunuculara bağlanmak için kullanılır.
- istemci ve sunucu arasında bağlantı şifrelidir. Bundan dolayı adı güvenli kabuktur.
- Öntanımlı olarak 22. portu kullanır.
- Uzaktaki sunucuya SSH ile bağlanabilmeniz için, uzaktaki sunucunun IP'sini, sunucudaki kullanıcı adını ve bu kullanıcının parolasını bilmeniz gerekmekte veya bu kullanıcının SSH anahtarına sahip olmanız gerekmekte.

Taşıma Katmanı Protokolleri

- Taşıma katmanında **TCP** ve **UDP** olmak üzere iki farklı protokol tanımlanmıştır.
- **TCP**: Transmission Control Protocol, **UDP**: User Datagram Protocol

hata denetimi yapar ve bu UDP'le bir farktır

TCP

burada iki duplex olur çünkü iki yönlü

- TCP bağlantıya yönelik çalışır, yani iki istemci arasında sanal bir oturum kurulur. İki yönlü iletim yapılır.
- Veri aktarımı bu katmanda denetim altında gerçekleşir.
- Akış denetimi, tıkanma, veriyi parçalama ve birleştirme özellikleri vardır.
- Hata denetimi yapar. Paketler gitmediyse bir daha gönderir.
- Taşıma katmanında TCP ile bir kerede gönderilebilen veri parçasına **bölüm (segment)** denilir.
- HTTP, FTP, SMTP, SSH protokolleri TCP'i kullanır.

frame sora paket sonra segment : önemli

TCP Başlığı (TCP Header)

başlık'te kaynak ve hedef portu bilimamez gerekir

<u>Kaynak portu</u> (16 bit)		Hedef portu (16 bit)	
Hedef portu bilimamez gerekir			
<u>Sıra numarası</u> (32 bit)			
<u>Alındı bilgisi numarası</u> (32 bit)			
Veri ofseti (4 bit)	Ayrılmış (6 bit)	Bayraklar (6 bit)	<u>Pencere</u> (16 bit)
<u>Checksum</u> (Kontrol Toplamı – 16 bit)		Acil İşaretçiler (16 bit)	
Opsiyonlar – Değişkenler			
Veri			

UDP

güvensiz ve taşıma katmanında çalışır

ve TCP ile karşılaştırın

- UDP bağlantısız çalışır, yani gönderilecek veri karşıdaki istemcinin adresine gönderilir.
- UDP paketlerin karşı tarafa ulaşp ulaşmadığını kontrol etmez.
- Genellikle küçük boyuttaki verileri gönderir. Parçalama ve birleştirme özelliği yoktur.
- **DNS, DHCP** gibi protokoller oturum kurmadan çalışır.

UDP Başlığı (UDP Header)

ounu baslik daha bsit

<u>Kaynak portu</u> (16 bit)	Hedef portu (16 bit)
Uzunluk	<u>Checksum</u> (Kontrol Toplamı – 16 bit)
Veri	

Ağ Katmanı Protokolleri

- Ağkatmanı TCP/IP protokol kümesinin en önemli katmanıdır denebilir.
- Internet IP yönlendirme protokolü üzerine kurulmuştur.
- Bu katmanda tanımlanan protokoller, binlerce hatta milyonlarca yönlendiricinin birbirine bağlanmasıyla, paketlerin alıcısına en uygun yol üzerinden optimum maliyetle aktarılma işini yapmaktalar.
- Bu katmandaki protokoller: IP, ICMP, ARP, IGMP

IP : nedir ve versionleri nelerdir?
ip 4. sinirli bu yuzden daha az olur
ama ip 6 daha ock kulanilir

IP Protokolü (İnternet Protocol)

IP adresi bir ağbağlı istemcilerin ağüzerinden birbirlerine veri yollamak için kullandıkları adrestir. **Ör:** 192.168.2.10

Bu katmanda taşıma katmanından gelen segmentlere özel bir **IP başlık bilgisi** eklenir.

Bu katmanda, veri parçasına artık **IP paketi** denmektedir.

segment ve paketler aralarında fark

IP Başlığı (IP Header)

IP versiyon	IP başlık uzunluğu	Hizmet türü	Toplam uzunluk
Kimlik		Parçalanma durumu	Parçalanma Ofseti
TTL	Protokol	Başlık kontrol toplamı (Checksum)	
Kaynak Adresi			
Hedef Adresi			
Opsiyonlar			
Veri			

ICMP (Internet Control Message Protocol)

- Kontrol amaçlı bir protokoldür.
- Genel olarak sistemler arası kontrol mesajları ICMP üzerinden aktarılır.
- **Ping komutu.**

IGMP (Internet Group Management Protocol)

- IGMP, TCP/IP'de çoklu dağıtım (**multicast**) üyelerini yönetmek için kullanılan bir iletişim protokolüdür.
- IGMP **online streaming videolarda** ve oyunlarda kullanılabilir. Bu tip uygulamaları desteklerken kaynaklarının daha verimli şekilde kullanılmasını sağlar.

br switch gonderdiginiz messaj hem ip hme de mac aliyor arp cunku coklu veri gonderiri

ARP (Address Resolution Protocol)

- Adres çözümleme protokolüdür..
- Yerel ağda iletişim MAC adresleri aracılığıyla yapıldığı için, IP adreslerine karşılık gelen MAC adreslerinin bilinmesi gerekmektedir.
- Bu protokol, IP adreslerine karşılık gelen yerel alan ağ adreslerini(MAC adreslerini) belirlemekte, dönüş tablolarında bu değerleri tutmaktadır.

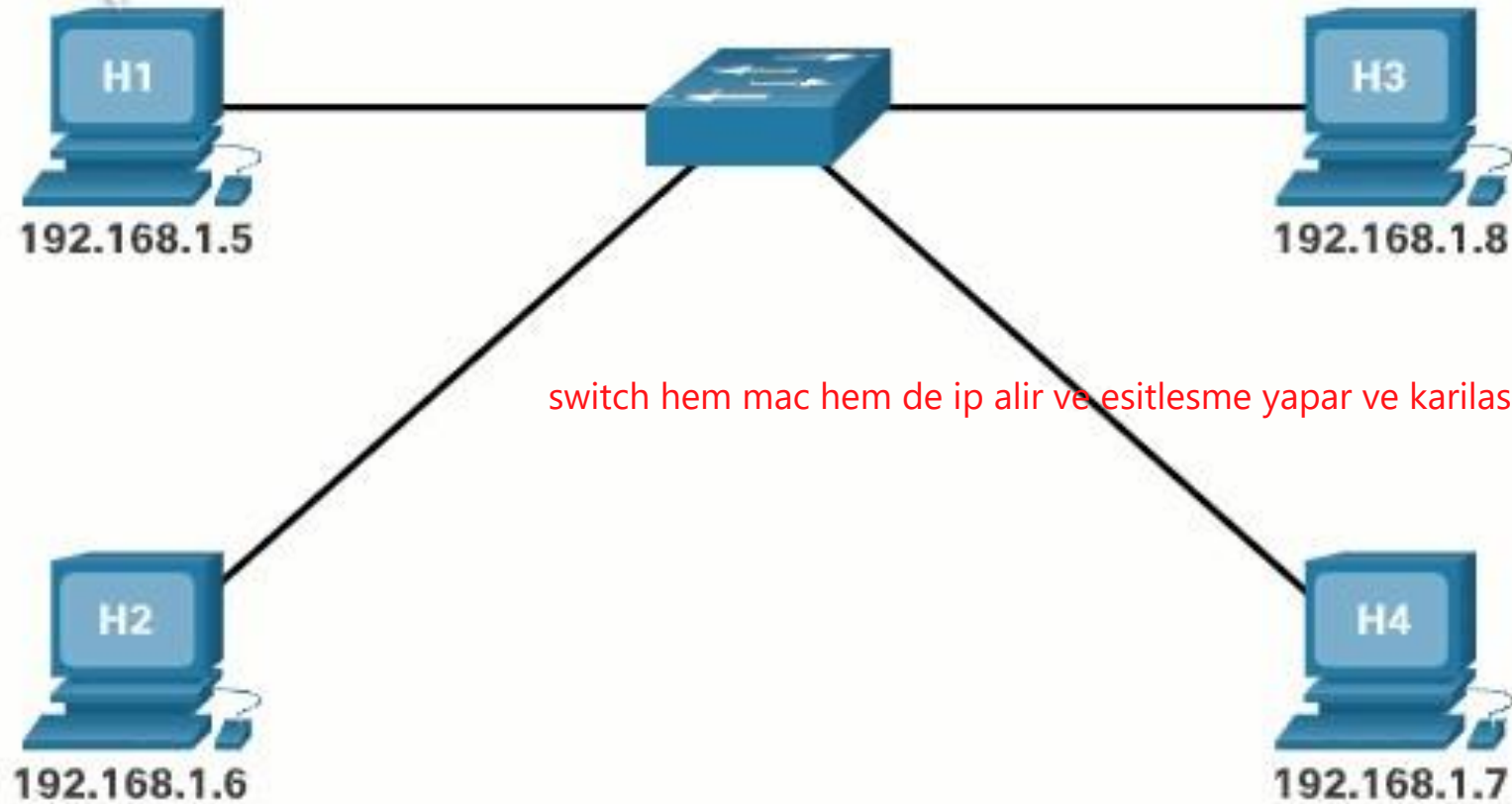
bulmak için

ARP İşleyişi

- Bir istemciye IP adresi geldiğinde onun MAC adresi karşılığını ARP dönüşüm tablosunda arar.
- Eğer dönüşüm tablosunda MAC adresi yoksa tüm ağa ARP isteği gönderir.
- Ağdaki diğer bilgisayarlar bu IP'nin MAC adresini biliyorlarsa isteği yapan bilgisayara yanıtı gönderir.
- İstekte bulunan bilgisayar kendi ARP dönüşüm tablosunu da günceller.

mac adressin bulmak için ve switchler de

I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.



switch hem mac hem de ip alır ve eşitleme yapar ve karılama yapar

RARP (Reverse ARP)

- Ters adres çözümleme protokolüdür.
- RARP, ARP'ın tersi işlem yapar, yani fiziksel adresten IP adresine ulaşmayı hedefler.
- İki ARP'ınkiyle aynıdır. Tüm ağa RARP isteği gönderilir.
- Bilgisayar ağa kendi mac adresini gönderir benim IP nedir diye sorar. Günümüzde bunun yerine DHCP kullanılmaktadır.

bu soru sorulur

3 Yollu El Sıkışma (3-Way Handshake)

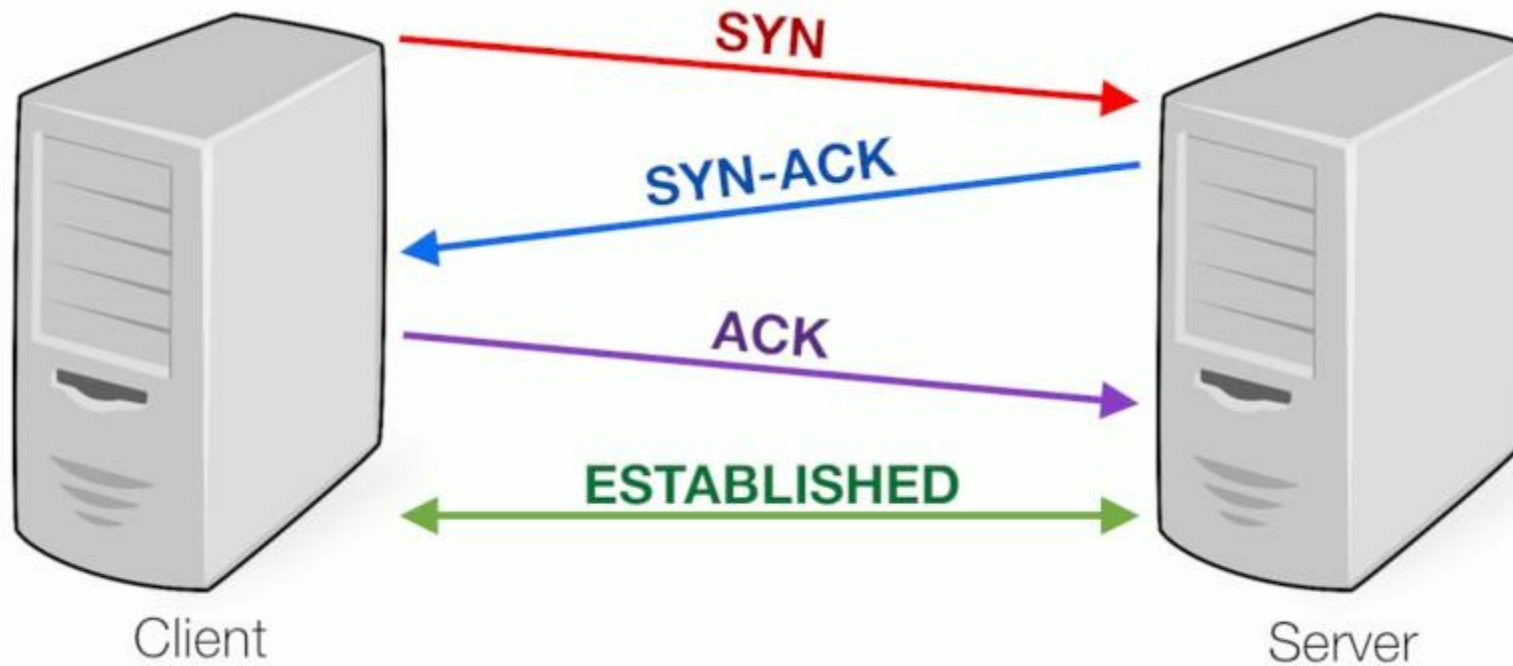
- İki bilgisayar arasında bir TCP bağlantısı kurulmak istendiğinde işleyiş şu şekilde olur.

1. A bilgisayarı B bilgisayarına TCP **SYN**chronize mesajı yollar.
2. B bilgisayarı A bilgisayarının isteğini aldığına dair bir TCP **SYN+ACK**nowledgement mesajı yollar
3. A bilgisayarı B bilgisayarına TCP **ACK** mesajı yollar
4. B bilgisayarı bir **ACK** "TCP connection is **ESTABLISHED**" mesajı alır

Üç yollu el sıkışma adı verilen bu yöntem sonucunda TCP bağlantısı açılmış olur.

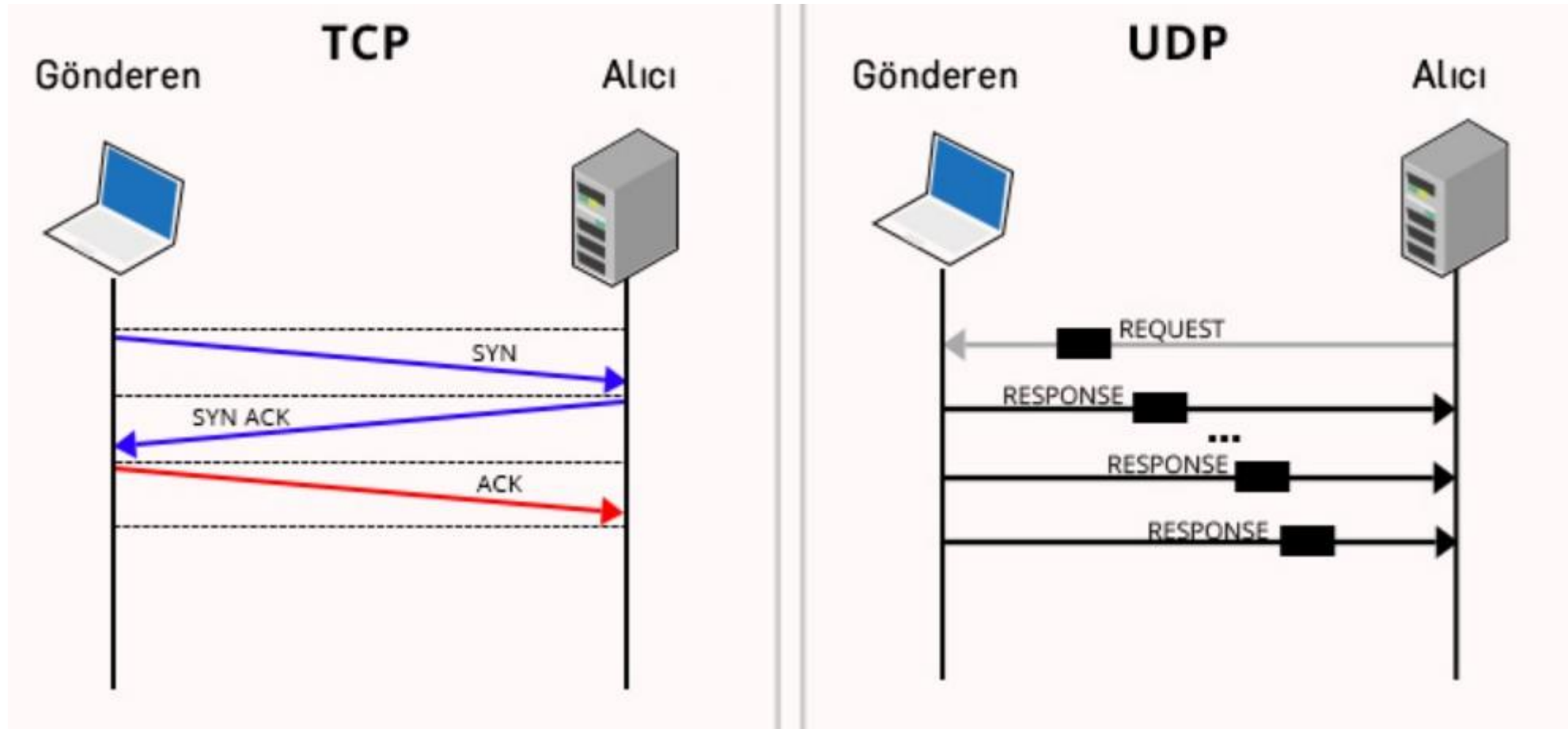
3 Yollu El Sıkışma

3 yolu deme syn,syn-ac,ack demek



TCP vs UDP

udp kontrol eder



osi
tcp/ip gorduk

Kaynaklar

- Bilgisayar Ağları ve İnternet Mühendisliği / Toros Rifat Çölkesen / Papatya Yayınları / 2019