

Bilgisayar Ağları Ders Notları

Bilecik Şeyh Edebali Üniversitesi

Murat Özalp

Kaynak belirtmek kaydıyla istenildiği gibi kullanılabilir (Murat Özalp)

İÇİNDEKİLER

1. Giriş ve Teşekkür	5
2. PDF biçiminde indirmek için	5
3. Daha fazla bilgi	5
4. Ağ Topolojileri	6
4.1 Doğrusal (Bus) Topoloji	6
4.2 Halka (Ring) Topoloji	7
4.3 Yıldız (Star) Topoloji	7
4.4 Örgü (Mesh) Topoloji	8
5. OSI Modeli	10
5.1 İnternet'in Kısa Tarihçesi	10
5.2 OSI ve TCP/IP modelleri	10
5.3 OSI MODELİ KATMANLARI	12
5.4 OSI modelini anlamak için kullanılabilecek uygulamalar	25
5.5 Wireshark ile trafik analizi	26
5.6 OSI modeli ve güvenlik	26
6. Temel Kavramlar	29
6.1 Aktarım Verimliliği	29
6.2 MTU	29
6.3 RTT	30
6.4 TTL	30
6.5 Bant Genişliği (Bandwidth)	30
6.6 Gecikme kaynakları	32
6.7 Jitter	33
6.8 QoS - hizmet önceliklendirme	33
6.9 Temel Bant ve Geniş Bant	34
6.10 Paralel ve Seri İletişim	35
6.11 Haberleşme Kanalı Modları	35
7. İletim Ortamları	37
7.1 İki Telli Bakır Telefon Hattı	37
7.2 Koaksiyel (Coaxial) Kablo	38
7.3 Bükümlü Çift Kablo (Twisted Pair Cable)	39
7.4 Fiberoptik Kablolar	44
8. Yerel Ağlar - LAN/VLAN	53
8.1 Ethernet Protokolü	53
8.2 MAC Adresi	53

8.3	ARP	54
8.4	Yayın Adresi (Broadcast Address)	55
8.5	Yayın Alanı	55
8.6	Çarpışma (çakışma) Alanı	55
8.7	Anahtarların Kapasitesi	56
8.8	Ağ Geçidi (gateway)	56
8.9	Ağları bölmenin faydaları	57
8.10	Alt Ağ Bölme Yöntemleri	57
8.11	VLAN Anahtarlar	58
8.12	IEEE 8021.Q VLAN protokolü	61
8.13	Anahtar Kullanım Mimarisi	63
9.	İnternet'in Protokolü: IP	66
9.1	Genel Bilgiler	66
9.2	Rezerve IP Adresleri	68
9.3	IP Adresi ve Hesaplamaları	70
9.4	Alt Ağlara Bölme	79
9.5	Ağ Geçidi IP Adresleri	86
9.6	İki Bilgisayar Aynı Ağda Mı?	89
10.	IP Yönlendirme	90
10.1	STATİK YÖNLENDİRME	90
10.2	DİNAMİK YÖNLENDİRME	91
11.	Bilgisayar Ağları Modelleme	92
11.1	Simülatör & Emülatör	92
11.2	Ağ Modelleme Platformları (Ücretsiz Olanlar)	92
11.3	CORE ile Uygulama	93
12.	Kaynaklar	94
13.	Yerel Ağlarda Güvenlik	95
13.1	Fiziksel Güvenlik	95
13.2	Erişim Kontrolü	95
13.3	Trafik Güvenliği	95
13.4	VLAN Kullanımı ve Segmentasyon	95
13.5	Port Güvenliği	95
13.6	Loglama ve Denetim	96
13.7	Yazılım ve Donanım Güncellemeleri	96
14.	Ağ İzleme ve Yönetimi	97
14.1	Temel Protokoller	97
14.2	Ağ İzleme Araçları	97
14.3	Log işlemleri	97

14.4	Performans İzleme	97
14.5	Ağ Haritalama ve Topoloji Görselleştirme	97
14.6	Güvenlik Olaylarının İzlenmesi	97
14.7	Otomasyon ve Betikleme	98
15.	Deneme Tahtası	99
15.1	Material for MkDocs	99
15.2	Callouts eklentisi	99
15.3	PlantUML Grafiği	99
15.4	Mermaid Grafiği	99
15.5	Formül denemesi	100
15.6	Dipnot ve sözlük kullanımı	100
15.7	Görsel kullanımı	100
16.	Son başlık.	101

1. Giriş ve Teşekkür

Bu çalışma, 2022 yılında BŞEÜ Bilgisayar Mühendisliği 4. sınıf öğrencilerinin önerisi üzerine başlatılmıştır. El yazısı ile yazılmış ve eski kalmış olan ders notlarının kolay güncellenmesi ve güncel tutulması amacını taşımaktadır.

Katkıda bulunanlar

-   Ibrahim Khalil Atteib Yacoub
-   Aleyna Çelik
-   Burhan Hoşlan
-   Mahamat kabir Souleymane

2. PDF biçiminde indirmek için



Web içerikleri her güncellendiğinde, PDF sürümü de otomatik olarak oluşturulmaktadır. PDF biçiminde isterseniz, şuradan indirebilirsiniz:

<https://ozalpmurat.github.io/BilgisayarAglari-Kitap/BilgisayarAglari-Murat%C3%96zalp.pdf>

3. Daha fazla bilgi

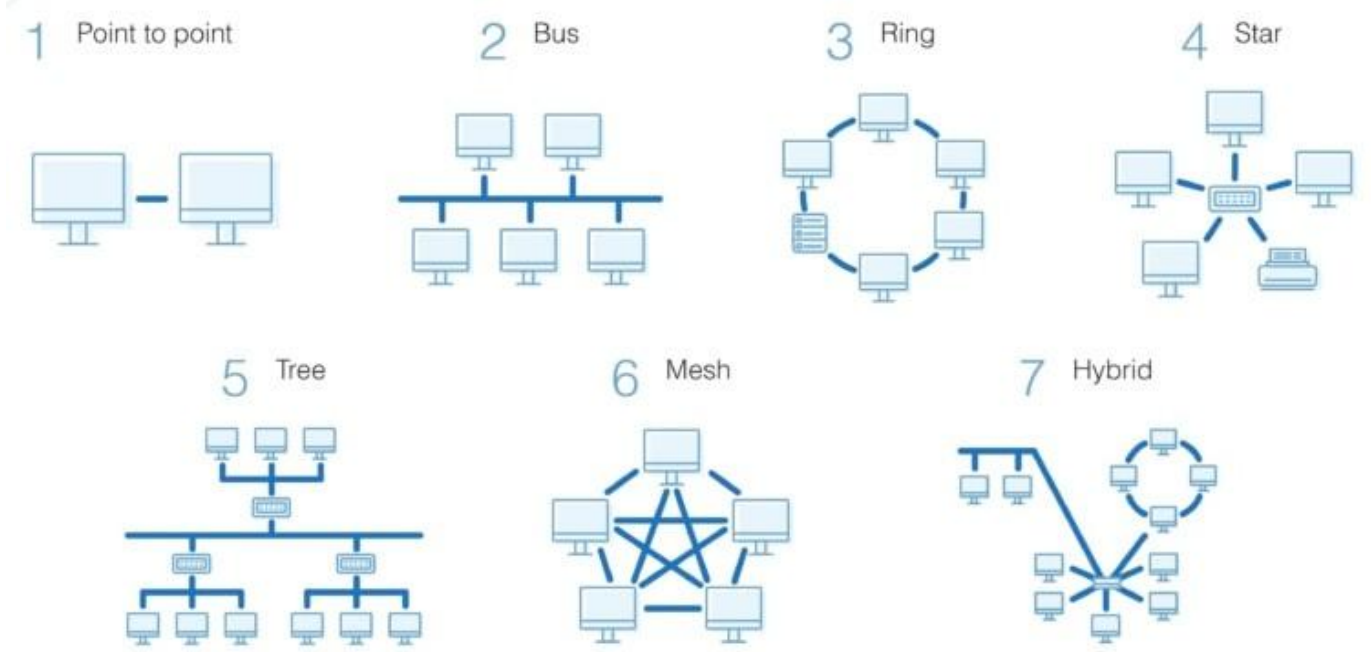
Siteyi yaparken şuradaki dokümanı uyguladım: <https://github.com/ldelugi/markdown-docs> **mkdocs** kullanılarak oluşturulmuştur.

Projenin github adresi

<https://github.com/ozalpmurat/BilgisayarAglari-Kitap>

4. Ağ Topolojileri

Ağ topolojisi, bir ağı oluşturan cihazların fiziksel ve mantıksal yerleşim biçimidir. Bu bölümde çokça bilinen fiziksel ağ topolojilerini inceleyeceğiz.



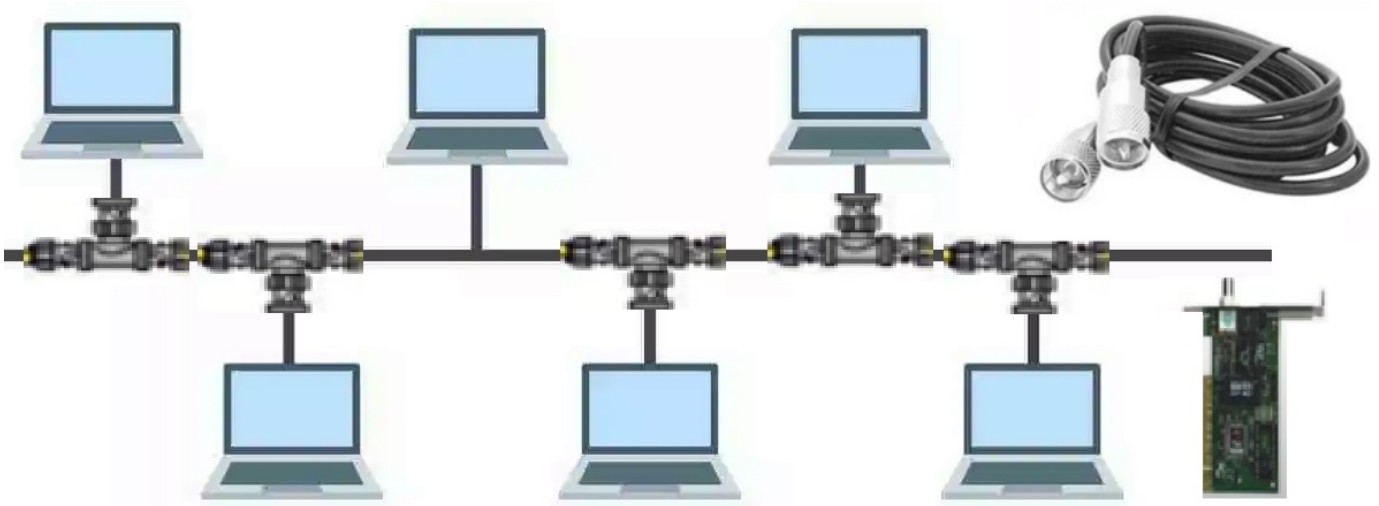
Görsel kaynağı: <https://www.dnsstuff.com/what-is-network-topology>

Note

"Ağ topolojisi" kavramını her kullandığımızda, bilgisayar ağlarından bahsettiğimizi unutmayalım. Bilgisayar ağlarının dışında da ağ sistemleri bulunmaktadır ve bunlar farklı topolojiler kullanıyor olabilirler.

4.1 Doğrusal (Bus) Topoloji

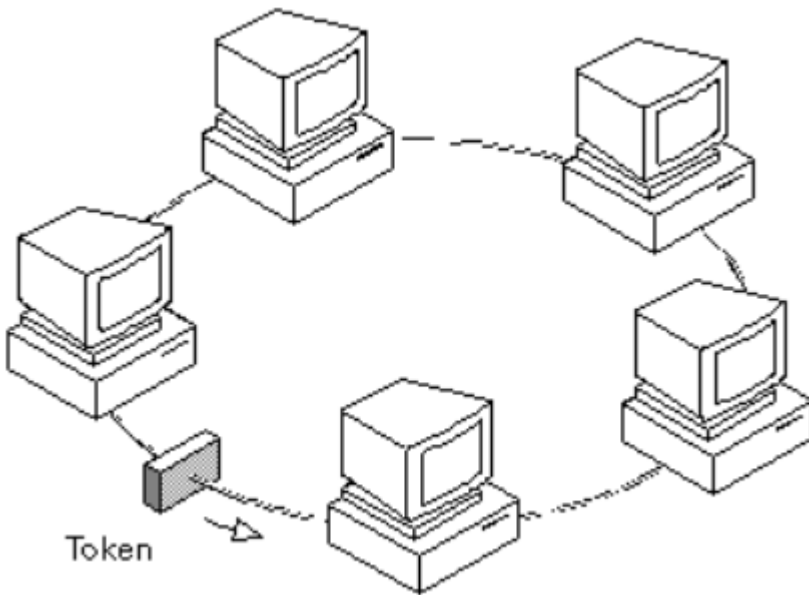
Doğrusal bir hat üzerinde bilgisayarların T konnektörlerle bağlanması şeklinde kurulur. Hattın her iki ucunda sonlandırıcı kullanmak zorunludur. Koaksiyel kablo kullanılır. Ağın herhangi bir noktasında arıza olması durumunda ağın tamamı çöker. Ağdaki veri trafiği tüm uçlara gider. Herkes herkesin trafiğini görebilir. Bu yüzden çok fazla **çakışma (collision)** olur.



Görsel kaynağı: <https://www.lunarcomputercollege.com/computer-network-topologies/>

4.2 Halka (Ring) Topoloji

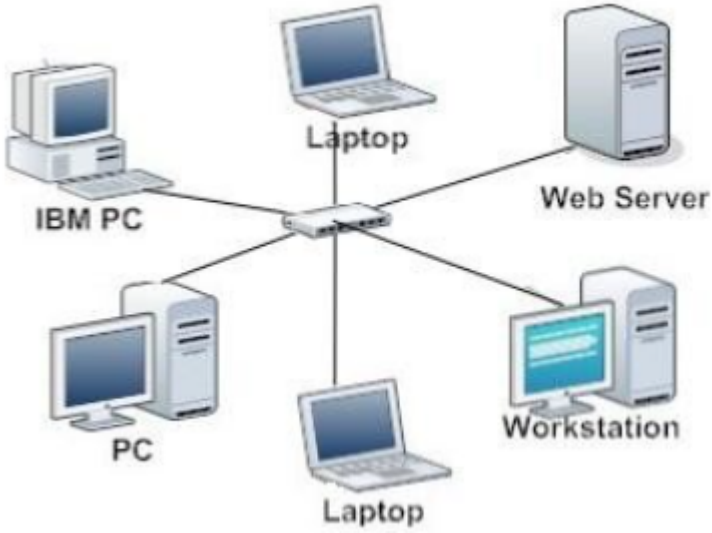
Doğrusal topolojiye benzer. Sonlandırıcı kullanılmaz. Hattın iki ucu birleşiktir. Hatta sanal bir jeton dolaşır(token). Jeton sırası gelen bilgisayar, jeton boş ise göndereceği veriyi hatta yerleştirir. Bilgisayarlar sırayla veri gönderdiklerinden çakışma daha azdır. Günümüzde hiç kullanılmamaktadır. Herkes herkesin verisini kullanabilmektedir.



Görsel kaynağı: <https://www.cse.iitk.ac.in/users/dheeraj/cs425/lec07.html>

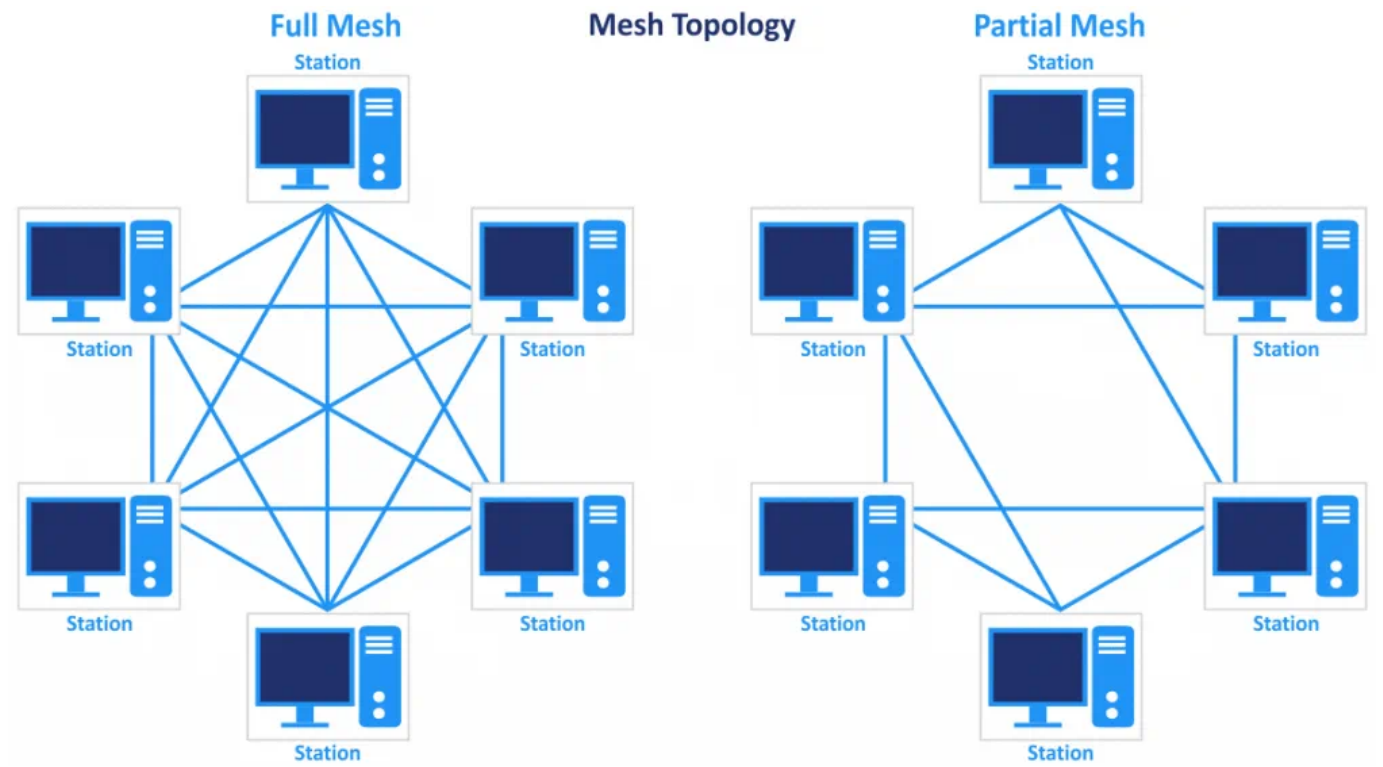
4.3 Yıldız (Star) Topoloji

Merkezde dağıtıcı bir cihaz olur. Buradan tüm bilgisayarlara birer kablo gider. Ağın bir noktasındaki arıza sadece ilgili bilgisayarın ağ bağlantısına zarar verir. Genellikle (bükümlü çift (twisted pair,xtp)) kullanılır. Trafığın herkese mi gönderileceği ya da sadece ilgili uca mı gideceği dağıtıcıya bağlıdır. Dağıtıcının performansı ve kabiliyeti ağı doğrudan etkiler. Günümüzde en yaygın topolojidir.



Görsel kaynağı: https://www.researchgate.net/publication/327897159_Hotel_Reservation_System_Based_Local_Area_Network_at_Samarinda

4.4 Örgü (Mesh) Topoloji



Görsel kaynağı: <https://www.nakivo.com/blog/types-of-network-topology-explained/>

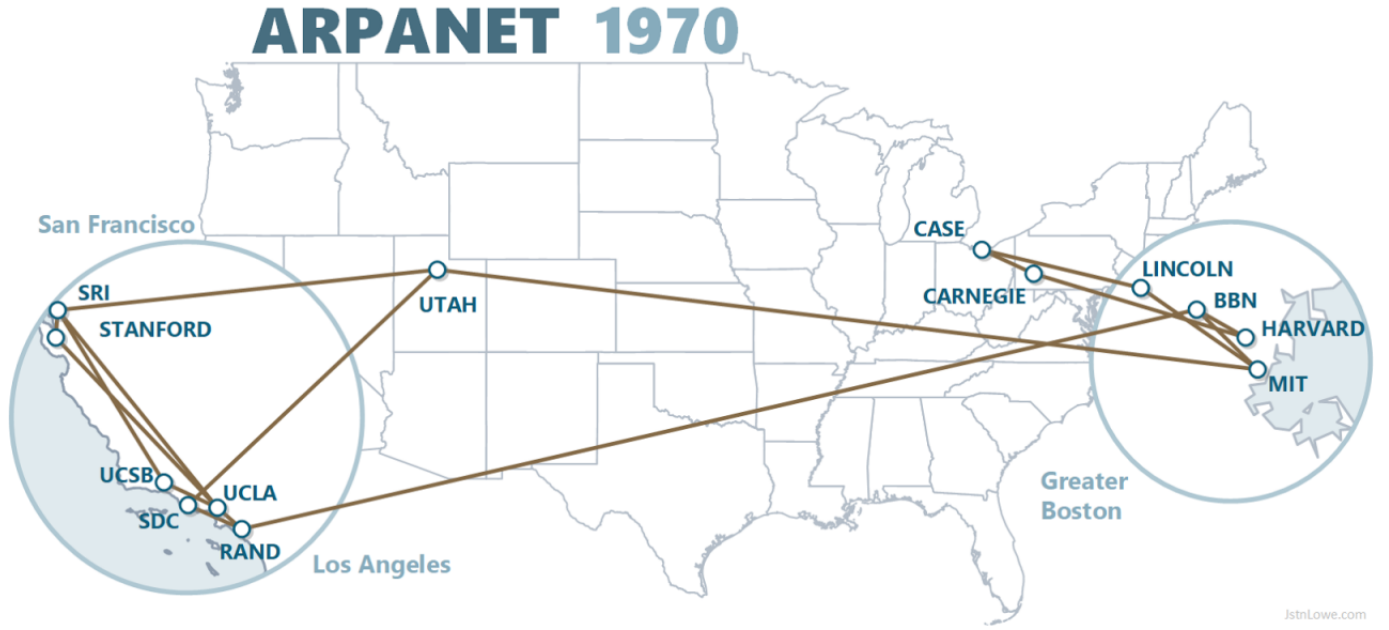
Uçları arasında birden fazla rota üzerinde haberleşme imkanı olan yapılardır. Günümüzde genellikle farklı yıldız ağlar arasında yedekleme amacı olarak kullanılır. Bunun dışında kablosuz ağlarda da yaygın olarak kullanılmaktadır.



Görsel kaynağı: https://www.researchgate.net/publication/234015211_FastM_Design_and_Evaluation_of_a_Fast_Mobility_Mechanism_for_Wireless_Mesh_Networks

5. OSI Modeli

5.1 İnternet'in Kısa Tarihçesi



ARPA NET 1970

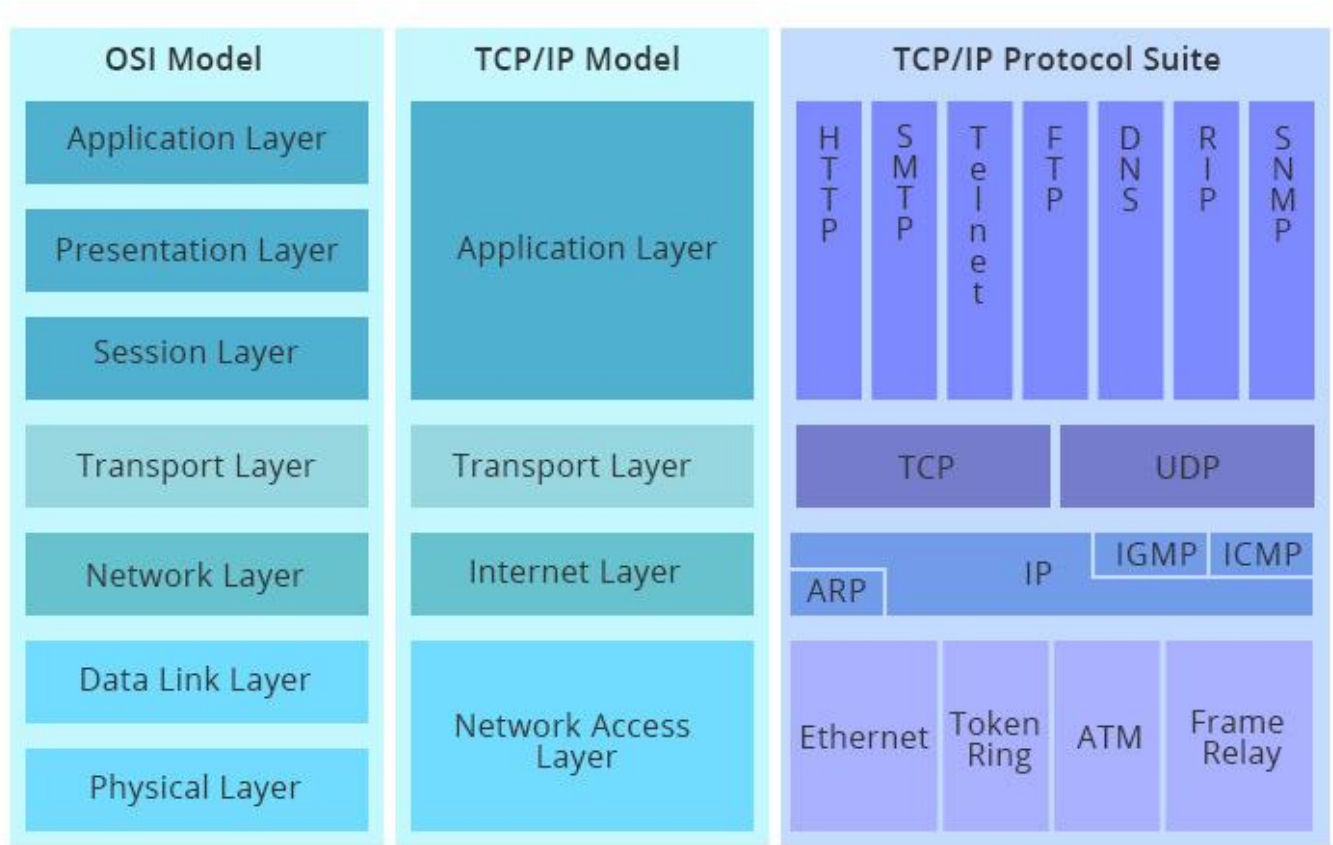
ARPA NET, "Advanced Research Projects Agency Network" (Gelişmiş Araştırma Projeleri Ajansı Ağı) kısaltmasıdır. ARPA NET, ABD Savunma Bakanlığı'nın (DARPA) finanse ettiği ve 1960'ların sonlarında ve 1970'lerin başlarında geliştirildi. İnternet'in dedesidir.

TCP/IP modeli 1989'da 1122 ve 1123 numaralı RFC'ler ile yayınlanmıştır. OSI modeli ise 1978'de taslak olarak yayınlanmış, 1984'te ise standart halini almıştır.

1980'lerin sonlarında bu teknolojiler, sivil ve ticari kullanıma açılarak İnternet'i başlattı.

5.2 OSI ve TCP/IP modelleri

Bilgisayar ağlarının nasıl çalıştığını anlamak için kullanılır. Geliştirilen donanımlar ve yazılımlar bu modellere uygun olursa İnternet üzerinde sorunsuzca iletişim kurabilirler.



Görsel kaynağı: <https://community.fs.com/article/tcpip-vs-osi-whats-the-difference-between-the-two-models.html>

TCP/IP	OSI
Implementation of OSI model	Reference model
Model around which Internet is developed	This is a theoretical model
Has only 4 layers	Has 7 layers
Considered more reliable	Considered a reference tool
Protocols are not strictly defined	Stricter boundaries for the protocols
Horizontal approach	Vertical approach
Combines the session and presentation layer in the application layer	Has separate session and presentation layer
Protocols were developed first and then the model was developed	Model was developed before the development of protocols
Supports only connectionless communication in the network layer	Supports connectionless and connection-oriented communication in the network layer
Protocol dependent standard	Protocol independent standard InstrumentationTools.com

Görsel kaynağı: <https://instrumentationtools.com/difference-tcpip-model-osi-model/>

5.3 OSI MODELİ KATMANLARI

Bir bilgisayardan gönderilen bir bilginin diğer bilgisayara nasıl ulaştığını anlatmak için tasarlanmıştır. İletişimi 7 katmanlı mimarı ile tanımlar. Ağ elemanlarının nasıl çalıştığını ve verinin iletimi sırasında hangi işlemlerden geçtiğini kavramak için kullanılan rehberdir. OSI Katmanlarının mantığını anlamak ağları planlamak, ağ üzerinden çalışan program yazmak ve ağ sorunlarını çözmek için önemlidir.

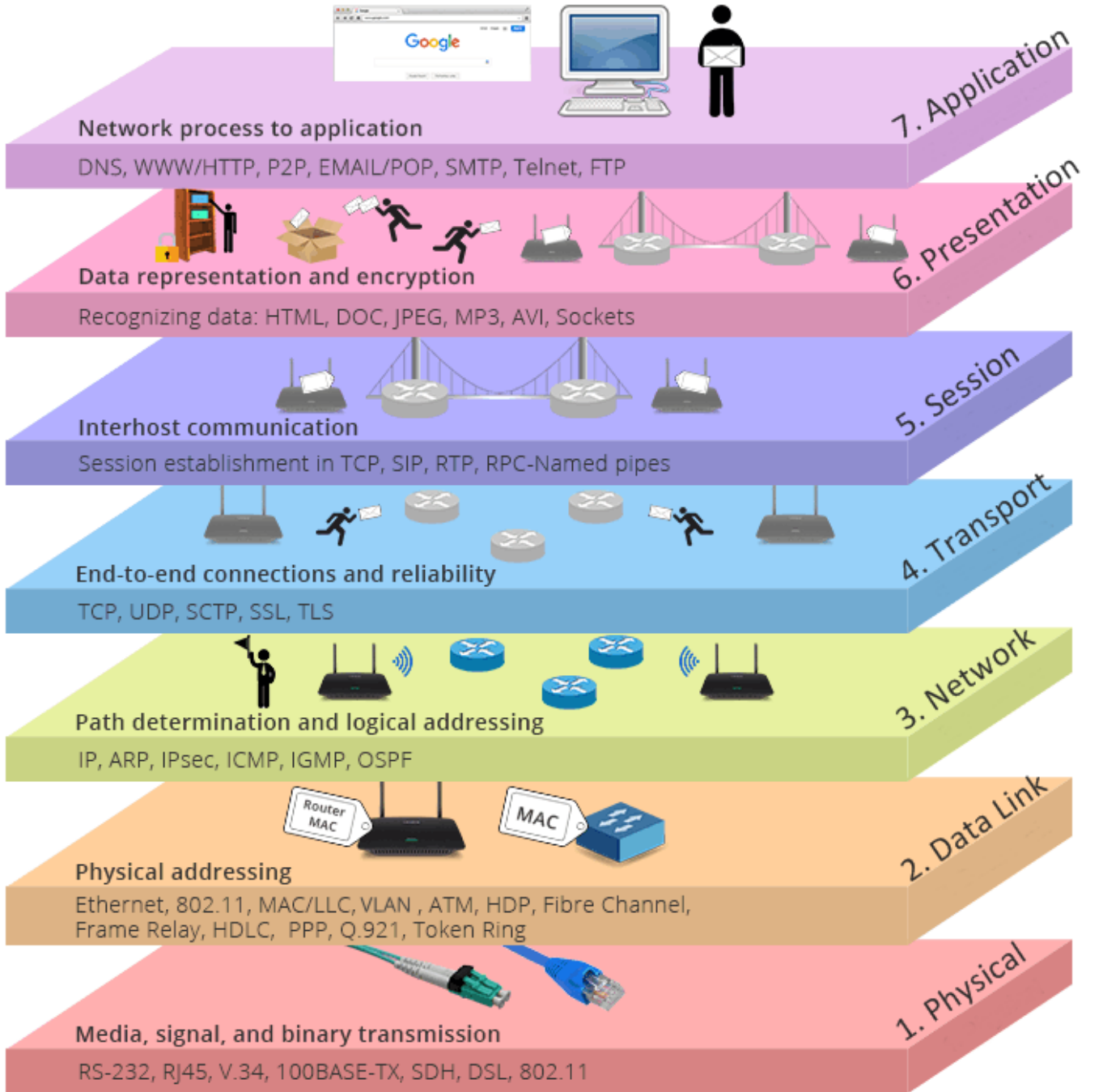
- 7-Uygulama (Application)
- 6-Sunum (Presentation)
- 5-Oturum (Session)
- 4-Taşıma (Transport)
- 3-Ağ (IP)
- 2-Veri Bağlantı (Data link)
- 1-Fiziksel (Physical)



Görsel kaynağı: <https://www.practicalnetworking.net/series/packet-traveling/osi-model/>

OSI Model	Function	TCP/IP Layers
7 APPLICATION	» End user layer » HTTP, FTP, IRC, SSH, DNS	APPLICATION
6 PRESENTATION	» Syntax layer » SSL, SSH, IMAP, FTP, MPEG, JPEG	
5 SESSION	» Synch & sent to port » API's, Sockets, WinSock	
4 TRANSPORT	» End-to-end connections » TCP, UDP	TRANSPORT
3 NETWORK	» Packets » IP, ICMP, IPSec, IGMP	NETWORK
2 DATA LINK	» Frames » Ethernet, PPP, Switch, Bridge	NETWORK INTERFACE
1 PHYSICAL	» Physical structure » Coax, Fiber, Wireless, Hubs, Repeaters	

Görsel kaynağı: <https://planetechusa.com/layer-2-vs-layer-3-switches/>



Görsel kaynağı: <https://community.fs.com/article/tcpip-vs-osi-whats-the-difference-between-the-two-models.html>

5.3.1 1: Fiziksel Katman

Haberleşme kanalının elektriksel ve mekanik olarak tanımlandığı katmandır. Bir uçtan gönderilen sinyalin karşı uca iletilmesinden sorumludur. Sayısal haberleşmede en küçük birim bit olduğundan bu katmanın hızı **bps, b/s (bit/saniye)** cinsindendir. Birinci katman donanımları:

1. Bakır ve fiber optik kablolar
2. RF (Antenler)
3. Sinyali (işareti) elektrik olarak yükselten ve çoklayan HUB cihazları
4. Tekrarlayıcılar (repeater)
5. Kablosuz iletişimde kullanılan hava

5.3.2 2: Veri Bağlantı Katmanı

Verinin fiziksel ortamdan güvenli bir şekilde taşınmasından sorumlu olan katmandır. Kaynaktan çıkan verilerin(bitler) hedefe ulaşan verilerle aynı olup olmadığını sıyanan sistemler kullanılır. En çok kullanılan hata bulma algoritmaları **eşlik biti (parity check)** ve **CRC algoritmasıdır**.



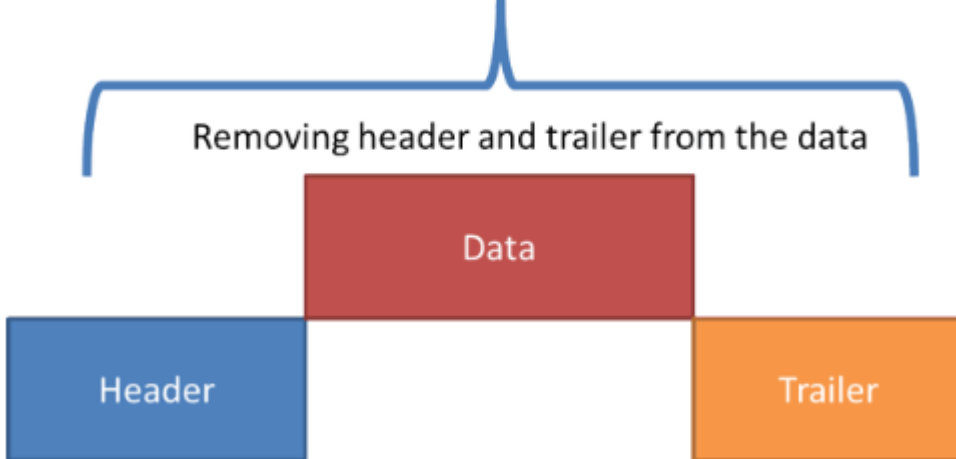
Görsel kaynağı: <https://www.hbmacit.com/2020/06/12/c-ile-parite-biti-hesaplama/>

Verinin doğru olup olmadığına bakmaz, sadece sağlamlığını kontrol eder. Bu katmanda üst katmandan gelen veriler çerçeve (frame) adı verilen paketleme işlemini tabi tutulur. Kapsülleme de denir. Birbirine doğrudan bağlı ağ cihazlarının aynı kapsülleme yöntemini (ikinci katman protokolünü) kullanması gerekir.

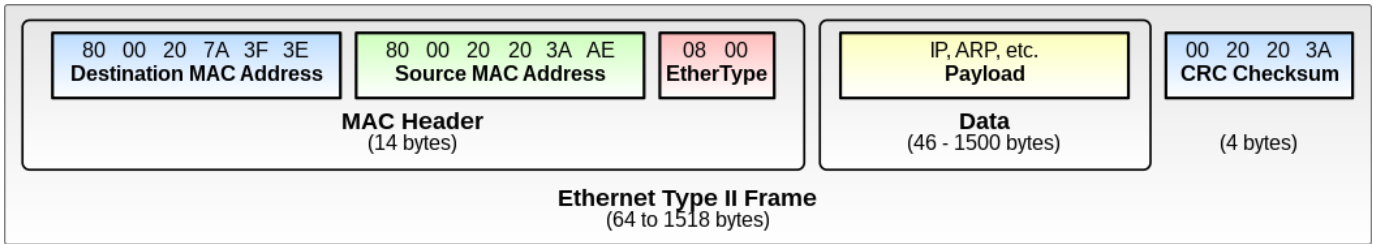
Encapsulation



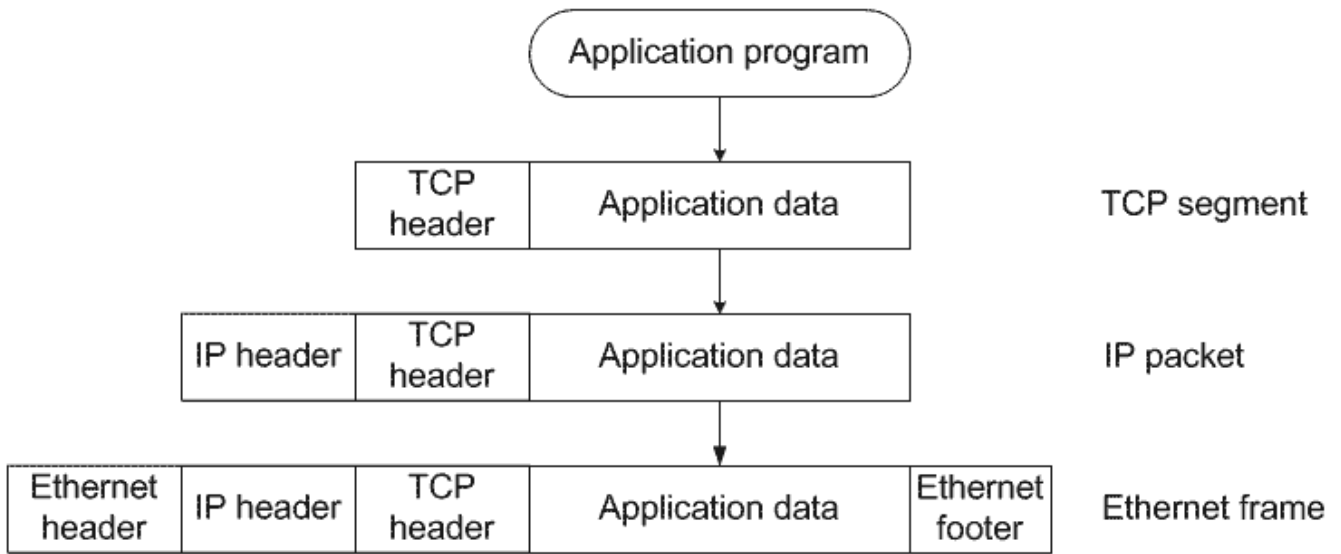
De-encapsulation



Görsel kaynağı: <https://www.computernetworkingnotes.com/ccna-study-guide/data-encapsulation-and-de-encapsulation-explained.html>



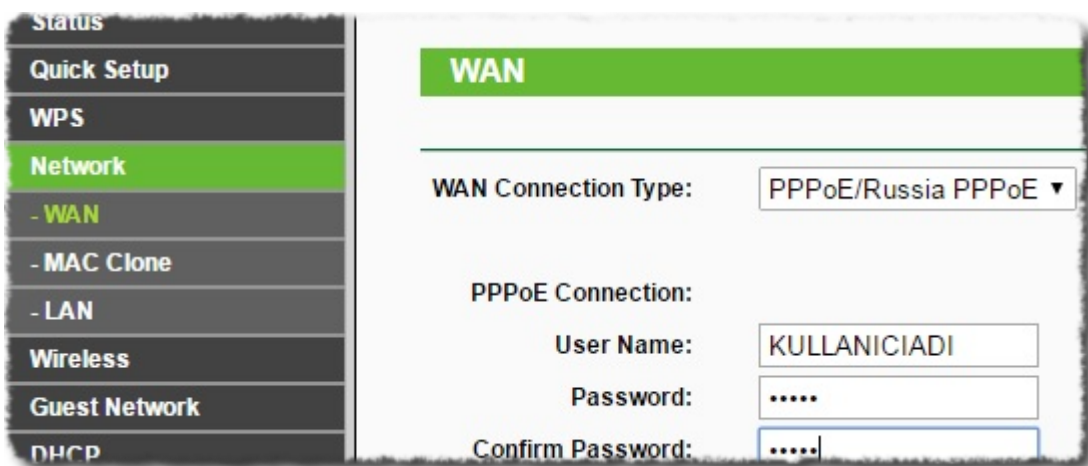
Görsel kaynağı: https://en.wikipedia.org/wiki/Ethernet_frame



Görsel kaynağı: <http://som.csudh.edu/cis/471/hout/netech/encapsulation.htm>

Günümüzde en yaygın ikinci katman protokolleri

- Yerel ağda (LAN): **Ethernet**
- Uzak ağlarda (WAN) : **Metroethernet**. Eskiden ATM, PPP, Frame-Relay gibi protokoller vardı ama günümüzde kullanımı azaldı. Eskiden çevirmeli ağlarda kullanılan PPP yerine günümüzde PPPoE kullanılıyor artık.



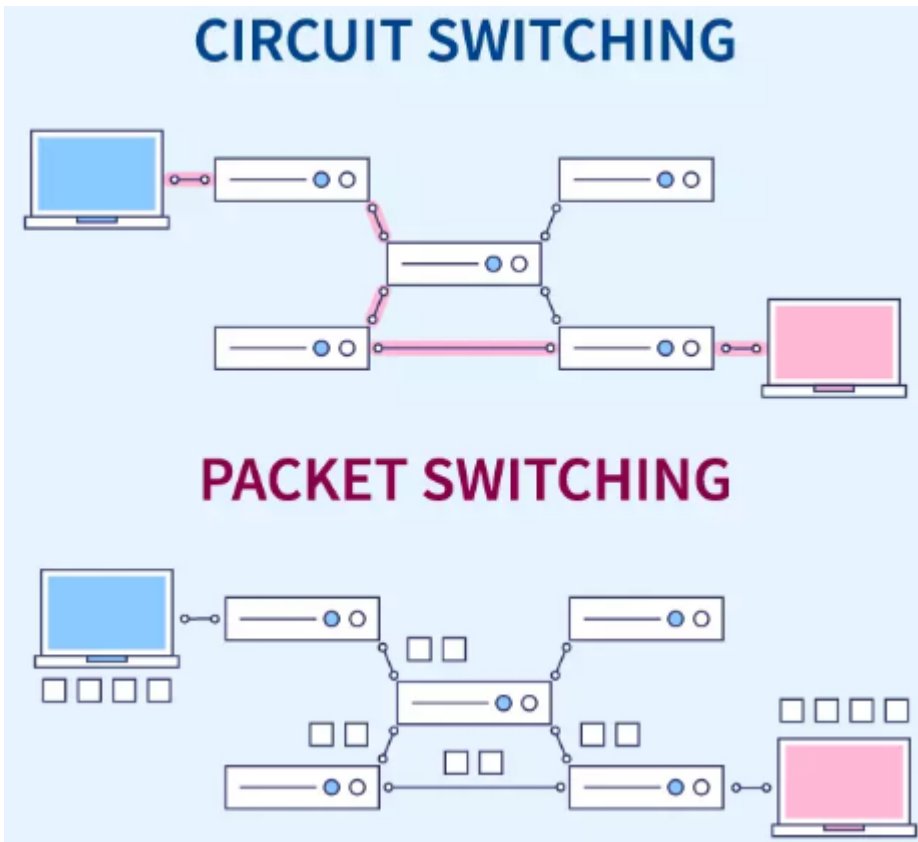
Görsel kaynağı: <https://www.alfanett.com.tr/modem.html>

5.3.3 LAN ve WAN nedir?

- **LAN:** Local Area Network (yerel alan ağı). Kendi arazisi (binası) içerisinde, kimseden izin almaya gerek kalmadan kablolu yapılan ağlara LAN denir. Örneğin üniversite kampüsü ya da aynı binanın birkaç katını kullanan şirketler gibi.
- **WAN:** Wide Area Network (geniş alan ağı). Kurumların kendi arazisinin (binasının) dışında olan bir yer ile kurulan ağlardır. Sokağın karşısındaki binaya kablo çekemeyiz. Eğer karşılıklı iki binada iletişim kurulması gerekiyorsa, ISP (Internet Service Provider ~ internet servis sağlayıcı) firmadan hizmet satın almak gerekir.
- **Fark ne?:** LAN'da istediğimiz kablolu türü ve istediğimiz protokolü kullanabiliriz. Hiç bir kısıtlama olmadan ağa bağlanabiliriz. WAN'da ise servis sağlayıcının sunduğu hizmetlerden ve onun kurallarına uyarak bağlanabiliriz.

5.3.4 Anahtarlama Türleri

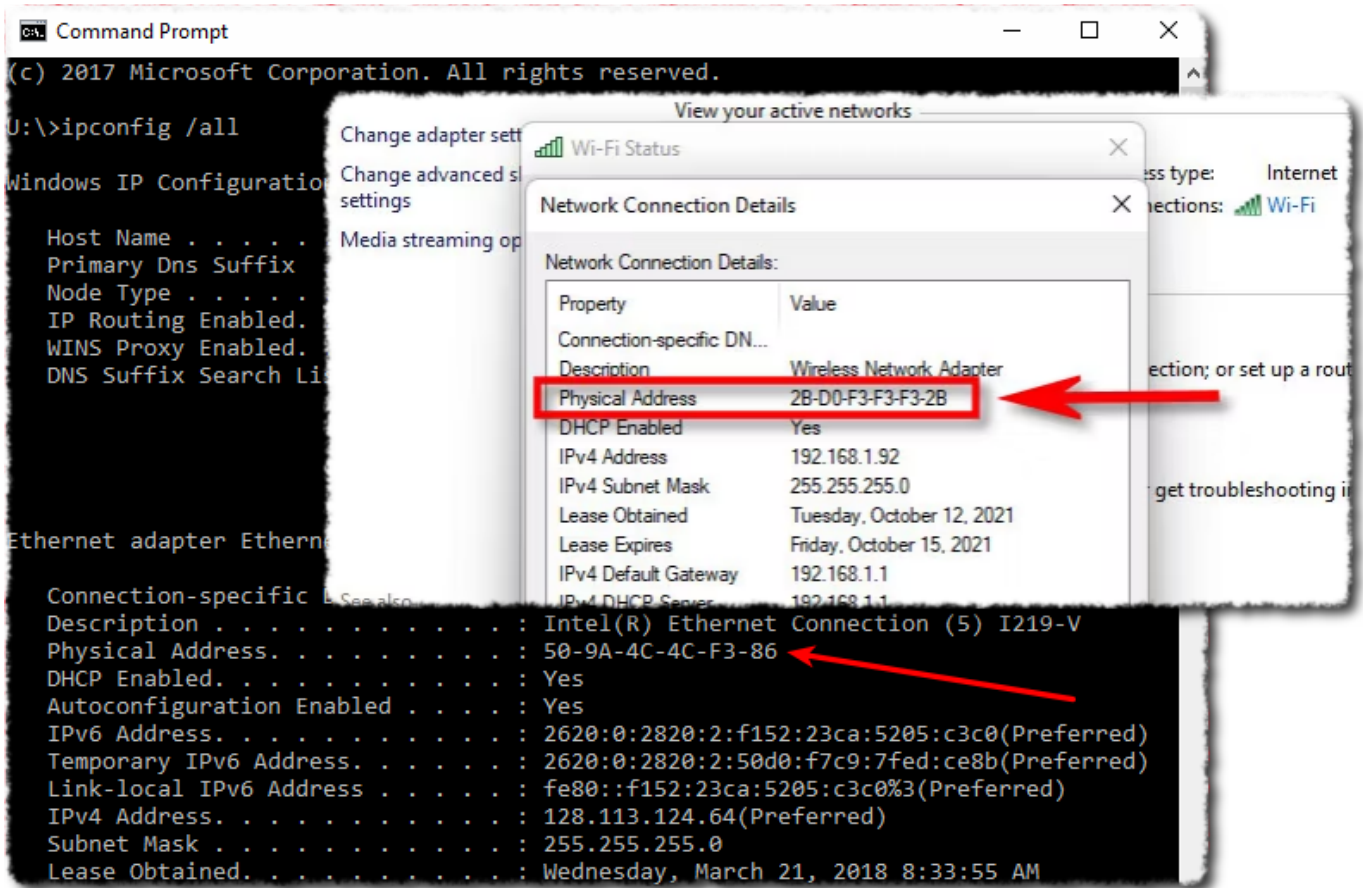
- **Devre Anahtarlama:** Veri aktarımı, fiziksel değişikliklerle yapılır.
- **Paket Anahtarlama:** Veri aktarımı, her bir veri paketi için hesaplanarak, yazılımsal olarak yapılır.



Görsel kaynağı: <https://www.scaler.com/topics/computer-network/circuit-switching-and-packet-switching/>

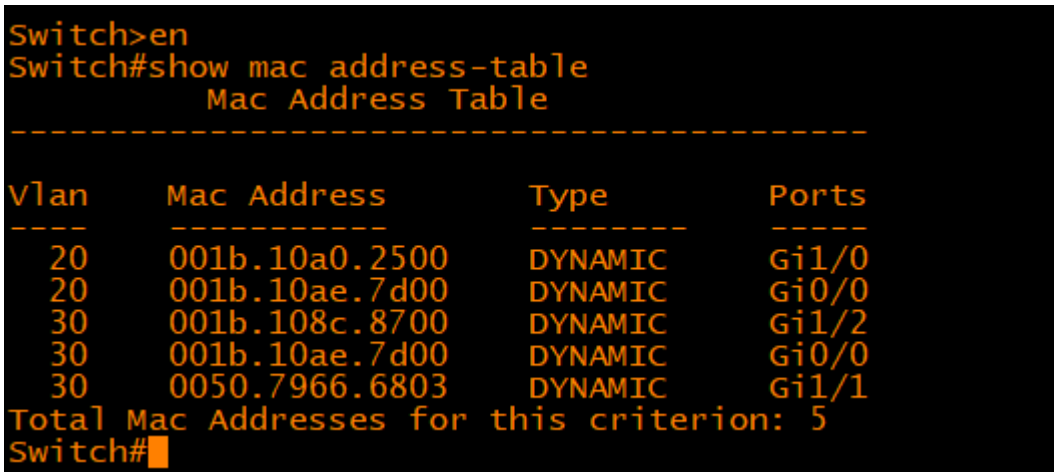
5.3.5 Ethernet Protokolünde Anahtarlama

Ethernet protokolünde kaynak ve hedef adresleri olarak **MAC** adresi (fiziksel adres) kullanılır. Çakışmaları engellemek için aynı ağda iki MAC adresi olmamalıdır.



Windows'ta MAC adresi (fiziksel adres)

5.3.6 MAC Adres Tablosu



Görsel kaynağı: <https://community.spiceworks.com/t/how-to-find-ip-mac-addresses-on-cisco-ios-devices/1012165>

```

C:\> Command Prompt

Microsoft Windows [Version 10.0.22610.1]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sharm>arp -a

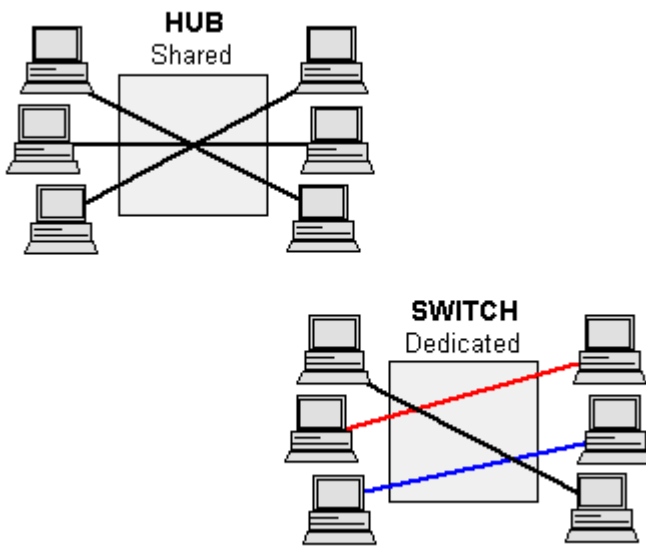
Interface: 192.168.1.33 --- 0xa
Internet Address      Physical Address      Type
192.168.1.1           54-47-e8-17-9d-a0     dynamic
192.168.1.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.251          01-00-5e-00-00-fb     static
224.0.0.252          01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static
255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\sharm>

```

Görsel kaynağı: <https://www.geeksforgeeks.org/what-is-mac-address-table/>

Anahtarlar (switch) ikinci katmanda çalışır. Anahtarlar portlarına bağlı olan cihazların MAC adreslerini bilmek zorundadır (otomatik öğrenir). Bu şekilde iki farklı portu arasındaki trafiği, diğer cihazlar görmeden aktarabilirler. **HUB'lardan en önemli farkı budur.**



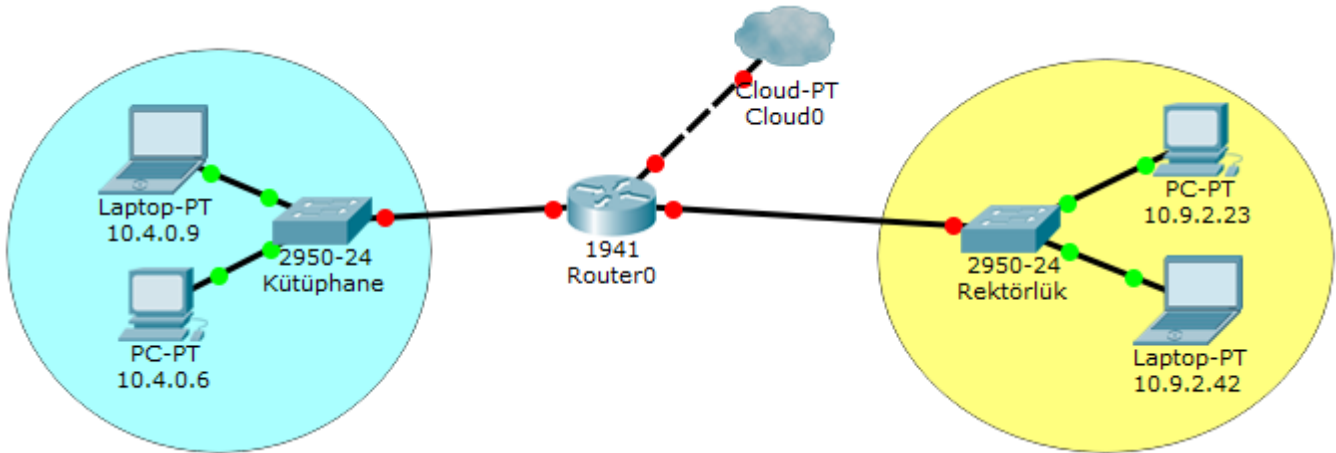
Görsel kaynağı: <https://www.pcmag.com/encyclopedia/term/ethernet-hub>

5.3.7 3: Ağ Katmanı (IP)

İnternet'i dünyanın farklı yerlerindeki ağlar üzerinden erişilebilir kılan katman budur. Kaynak ve hedef olarak IP adresi kullanılır. IP yönlendirilebilir bir protokol olduğundan her türlü veri ağı üzerinden haberleşmeye olarak sağlanır. Bu katman en önemli görevi yönlendirme işlemidir. Yönlendirme işlemi birden fazla ağ arayüzüne (network interface) sahip olan yönlendirici(router) adı verilen cihazlar tarafından yapılır. IP internetin temel protokolüdür. Yani bir PC internete bağlanacaksa IP'yi mutlaka biliyor olmalıdır.

Note

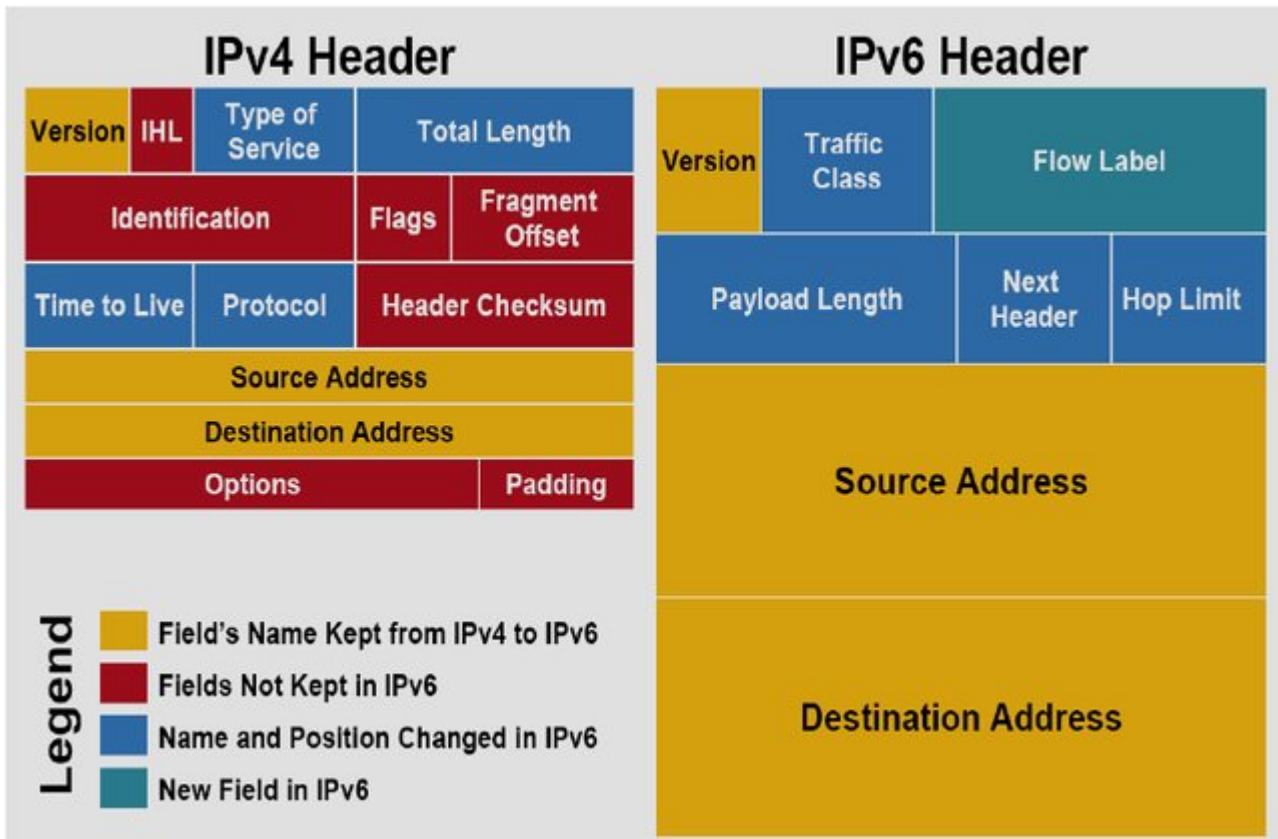
3. katmanda aktarılan verinin en küçük anlamlı birimine **paket** denir.



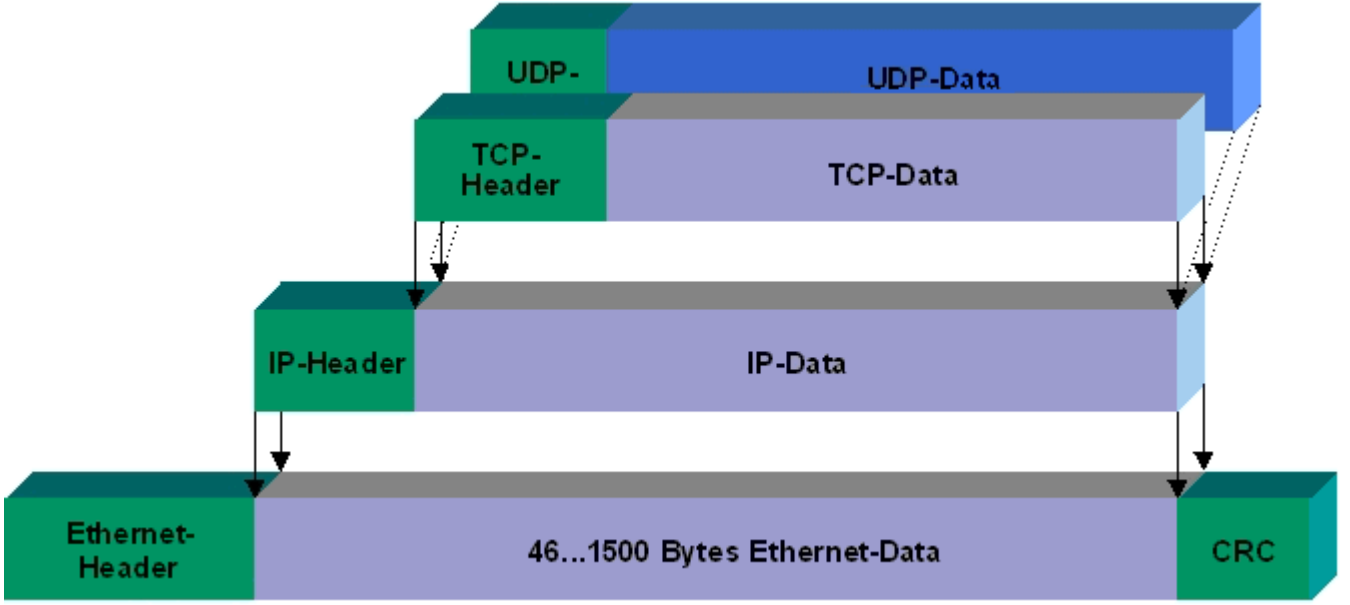
Ağlar arası bağlantı

Farklı ağların birbiri ile görüşmesi için mutlaka yönlendirme yapılması gerekir. Yukarıdaki şekilde iki farklı ağ yönlendirme yapılarak bağlanmıştır.

- **Kütüphane** tarafındaki bilgisayarlar aynı ağdadır. Birbirleriyle MAC adresleriyle haberleşir (2. katman).
- **Rektörlük** tarafındaki bilgisayarlar aynı ağdadır. Birbirleriyle MAC adresleriyle haberleşir (2. katman).
- **Kütüphane** ve **Rektörlük** bilgisayarları farklı ağlarda olduklarından birbirleriyle MAC adresleriyle haberleşemez, IP adresi ile yönlendirme yapılarak haberleşebilirler. (3. katman).



Görsel Kaynağı: https://www.researchgate.net/publication/269810379_IPv4IPv6_Transition

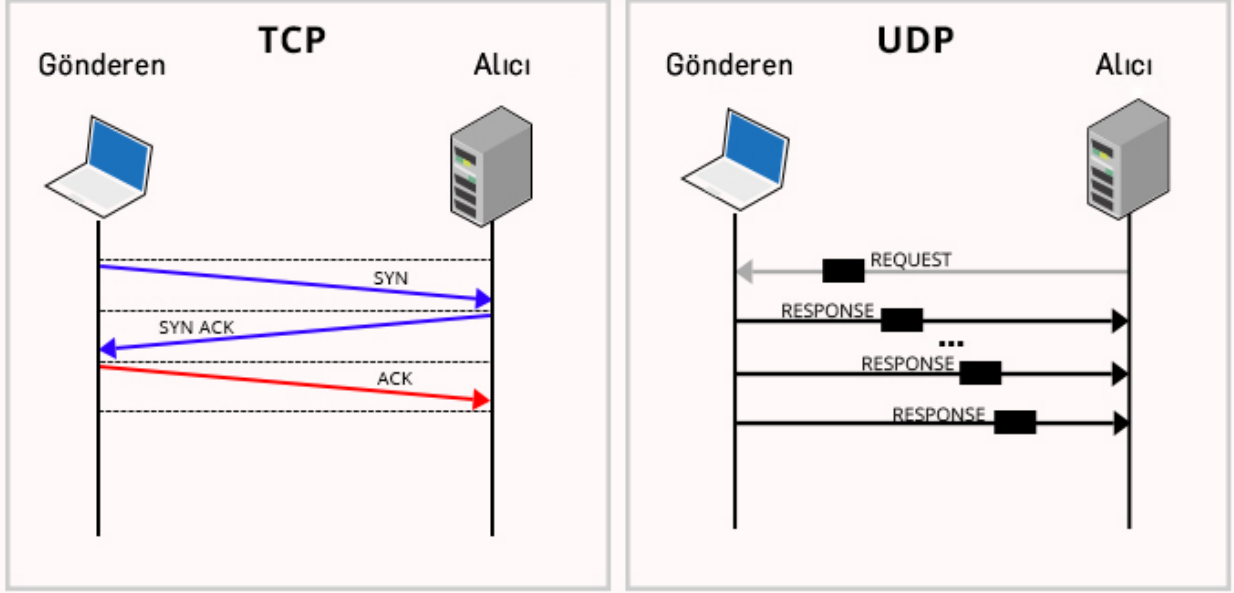


Görsel Kaynağı: <https://infosys.beckhoff.com/english.php?content=../content/1033/bc9191/2792604555.html&id=>

5.3.8 4: Taşıma Katmanı

İnternette IP üzerinde kullanılan 2 tane 4. katman protokolü vardır. Bunlar TCP ve UDP'dir. Bu katman uygulama programları için seri iletişim kanalları kuran katmandır. Bu kanallar port adı verilen servis numaralarıyla kurulur.

TCP ve UDP İletişim



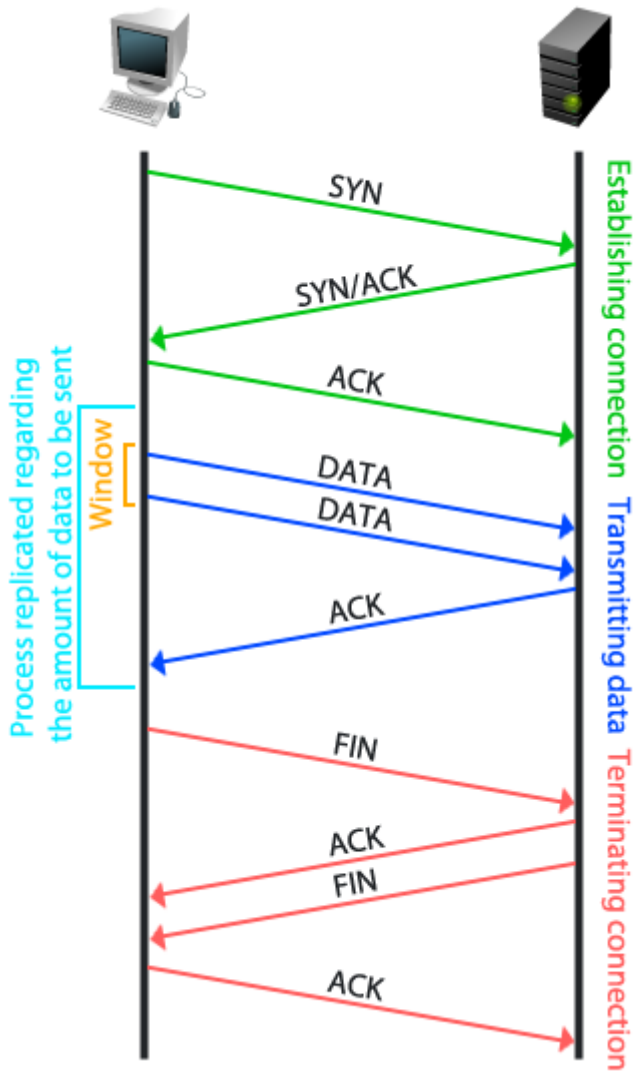
Görsel Kaynağı: <https://www.karel.com.tr/bilgi/tcp-ve-udp-arasindaki-farklar-nedir>

- **TCP:** Bağlantı temelli bir protokoldür. Trafik başlamadan önce karşıdaki uca müsait olup olmadığı sorulur. Bu yönüyle telefon görüşmesine benzer.
- **UDP:** Bağlantı temelli değildir. Trafik doğrudan başlatıldığı için paketlerin iletimi garanti edilmez. SMS gönderimine benzetilebilir. Özellikle gerçek zamanlı görüntü ve ses taşıma uygulamalarında elverişlidir. TCP'ye göre daha hızlıdır.

	TCP	UDP
Bağlantı Kurulumu	Güvenli Bağlantı Kurulur	Bağlantısız Çalışır
İletim Yönetimi	Paketi sırasıyla gönderilir	Paket akış şeklinde gönderilir
Hata Tespit ve düzeltilmesi	Mevcuttur	Mevcut değildir
Teslim Garantisi	Gönderdiğini onaylar	Onay mekanizması yoktur.
Hız	Yavaş	Hızlı
Tıkanıklık Kontrolü	Tıkanıklık kontrolü vardır.	Tıkanıklık kontrolü yoktur.
Bağlantı Koparma	Bağlantı koparma sürecine sahiptir.	Bağlantı koparma süreci yoktur.

Görsel Kaynağı: <https://medium.com/@mehmet.topac/tcp-nedi%CC%87r-udp-nedi%CC%87r-farklari-nelerdi%CC%87r-6ff6a29573b7>

3 way handshaking - 3 aşamalı el sıkışma



Görsel Kaynağı: <https://toschprod.wordpress.com/2012/01/30/osi-model-layer-4-transport/>



Görsel Kaynağı: <https://www.reddit.com/r/ProgrammerHumor/comments/18hkwj0/acknowledge/>

Note

Dördüncü katmanın bir başka görevi de üst katmanlardan gelen veriyi bölümleyerek daha küçük parçalara ayırmaktır. Bu parçalara *segment* denir.

TCP'de el sıkışmadan sonra, ilk olarak veri boyutu ve toplam kaç parçada gönderileceği karşı tarafa söylenir. Sonra segmentler halinde veri gönderilir.

Örnek senaryolar

- HTTP üzerinden 1GB'lık program indireceksek ve 80 segment halinde karşıya gönderilecekse, `1/80, 2/80, ..., 80/80` şeklinde parçalanarak ve her bir segmente numara eklenerek karşıya iletilir.
- İnternette radyo dinleyeceksek genelde **UDP** ile dinleriz. Çünkü gelecek olan verinin boyutu (kaç GB?) belli değil. Segmentasyon yapma şansı yok.



TCP



UDP

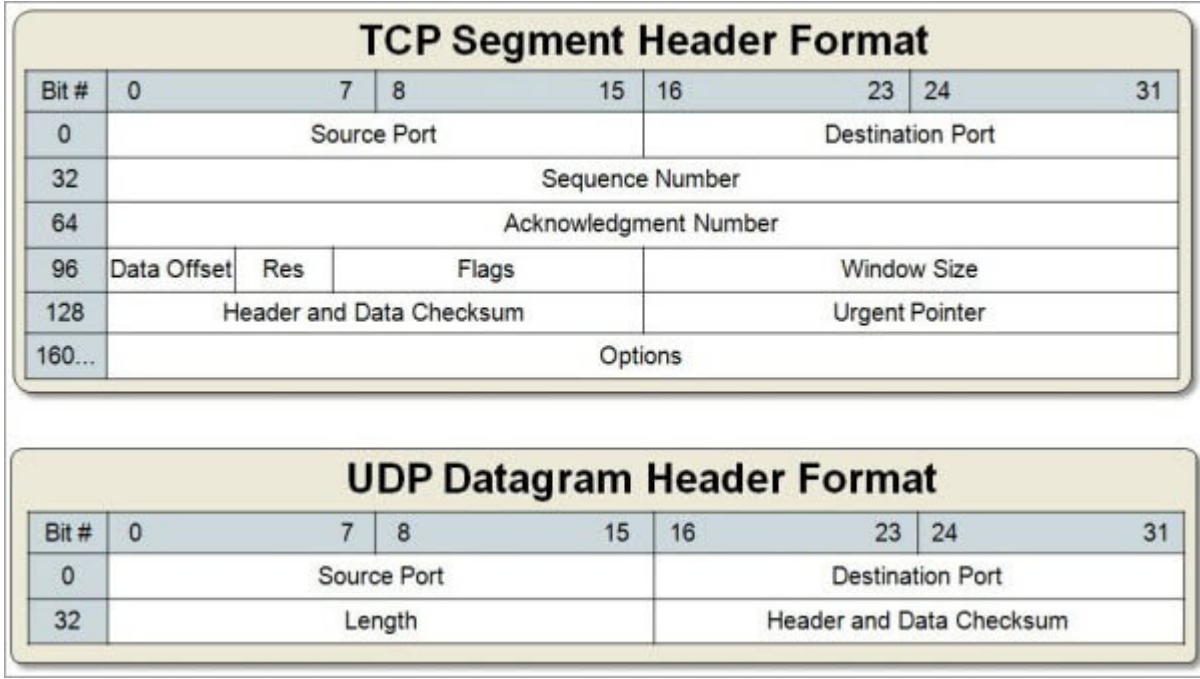


MULTICAST



BROADCAST

Görsel kaynağı: <https://www.pinterest.com/pin/808536939357862630/>



Görsel kaynağı: <https://www.softwaretestinghelp.com/tcp-vs-udp/>

5.3.9 5-7: Uygulama Seviyesi Katmanları

Aslında uygulama seviyesi sadece 7. katmandır. Ancak 5 ve 6 yaygın kullanılmadığından ve farklı uygulamalar arasında standart olmadığından bu derste üçünü tek başlıkta inceliyoruz.

Uygulama programları genellikle 7. katmanda çalışmakta ve genellikle doğrudan 4. katman ile iletişime geçmektedir. Oturum ve sunum gibi işlemler yapılacaksa da genellikle uygulama içerisinde yapıp 4. katmana aktarılmaktadır.

Yaygın kullanılan bazı servisler

Bilgisayar ağları kapsamında **Servis** (hizmet) kavramı, ağ üzerinde belirli bir portu dinleyen uygulama anlamındadır. Örneğin, WEB portunu (TCP 80) web sunucusu dinler. Web sunucusu uygulamasına servis denir bu durumda.

- DHCP (UDP 67 & 68)
- DNS (UDP 53)
- HTTP (TCP 80)
- HTTPS (TCP 443)
- SMTP (TCP 25)
- SSH (TCP 22)
- RDP (TCP 3389)
- MS-SQL (TCP 1433)
- MySQL (TCP 3306)

5.4 OSI modelini anlamak için kullanılabilecek uygulamalar

- **ping** (hping): Karşı uç ile aramızda 3. katmanda bağlantı var mı? Paketler kaç milisaniyede gidip geliyor? Büyük paketler ve küçük paketler ağdan aynı şekilde gidebiliyor mu?
- **tracert** (tracert): Uzaktaki bir sisteme IP üzerinden hangi rotadan gittiğimizi gösterir. ICMP kapalı olan sistemlerde TCP Trace denenebilir.

- **Telnet:** Ağlarda yönetim ve kontrol amaçlı kullanılır. Ağ cihazlarının genellikle tamamı telnet ile yönetimi destekler. Bunun dışında, 2 cihaz arasında 4. katmanda bağlantı (erişebilirlik) kontrolü yapmak için de kullanılır. Örneğin SMTP veya HTTP gibi protokoller, Telnet ile çalıştırılabilir.
- **netstat** Bilgisayarımızda açık olan portları ve aktif ağ bağlantılarımızı gösterir. Linux'ta `sudo netstat -antulp` şeklinde en güzel çıktıyı verir.
- **nmap** (zenmap): TCP ve UDP port taraması yapar. 0-65536 arası tüm portlar ya da belirli portlar taranabilir. Script taraması sayesinde zafiyet taraması bile yapabilir. Çok güçlü bir araçtır.
- **wireshark (tcpdump):** Ethernet kartını izler, tüm trafikleri kaydeder. İstenirse filtre girilerek kayıt yapması da sağlanabilir.
- **TCPView (Microsoft)** Windows'ta aktif ağ bağlantılarını gösterir. Hangi uygulama nereye bağlantı yapıyor?

5.5 Wireshark ile trafik analizi

Örnek uygulamalar:

- DHCP trafiği
- TCP 3-way handshake
- HTTP/Telnet vb. parola görüntüleme
- DNS ve HTTP trafikleri arka arkaya

!!! Ubuntu'da basit parola web sayfası yapma:

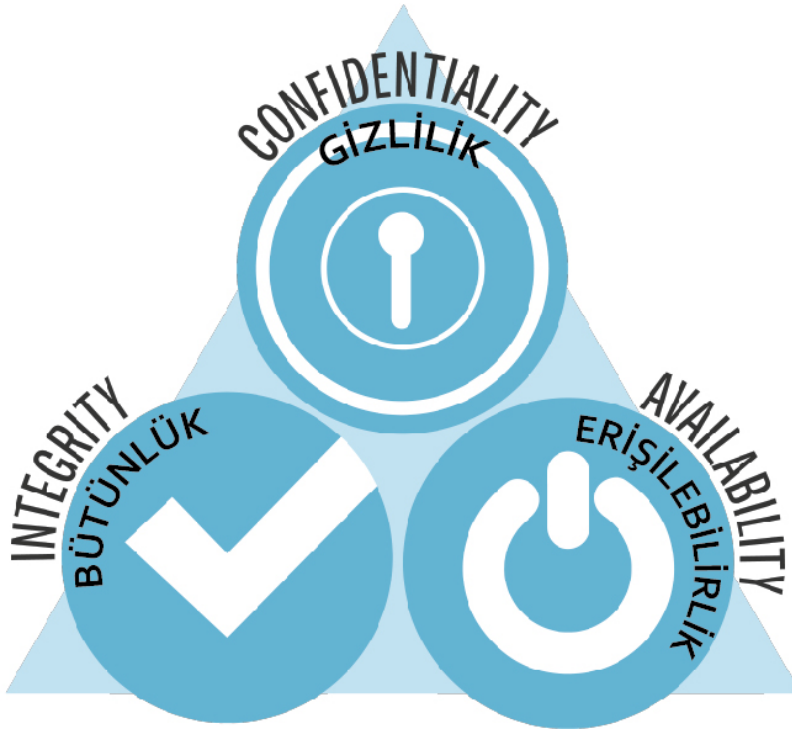
```
sudo apt install python3-venv
python3 -m venv venv-sauth
source venv-sauth/bin/activate
pip install sauth
sauth abc 123
```

5.6 OSI modeli ve güvenlik

Layer	Device / Protocols	Function	Cyberattack / Threat Examples
7. Application	FTP, HTTP, IMAP, SMTP	User interface	Ransomware, Viruses, Worms, Malware, Botnets, Keyloggers, Rootkits, ARP Spoofing, Man-in-the-Middle attack, Spyware, Cache Poisoning, DNS-redirecting
6. Presentation	JPG, MPEG, PNG	Data format; encryption	
5. Session	SQL, RPC, NFS	Process to process communication	
4. Transport	TCP, UDP	End-to-end communication maintenance	RIP Attacks, SYN Flooding
3. Network	L3 Switches, Routers	Routing data, logical addressing, WAN delivery	IP Smurfing, Address spoofing, Misconfigured devices, Vulnerable old firmwares, Default passwords
2. Data Link	L2 Switches, Bridges	Physical addressing, LAN delivery	
1. Physical	Physical cabling	Transmitting bits	Environmental and physical threats: Dust, Water, Rodents

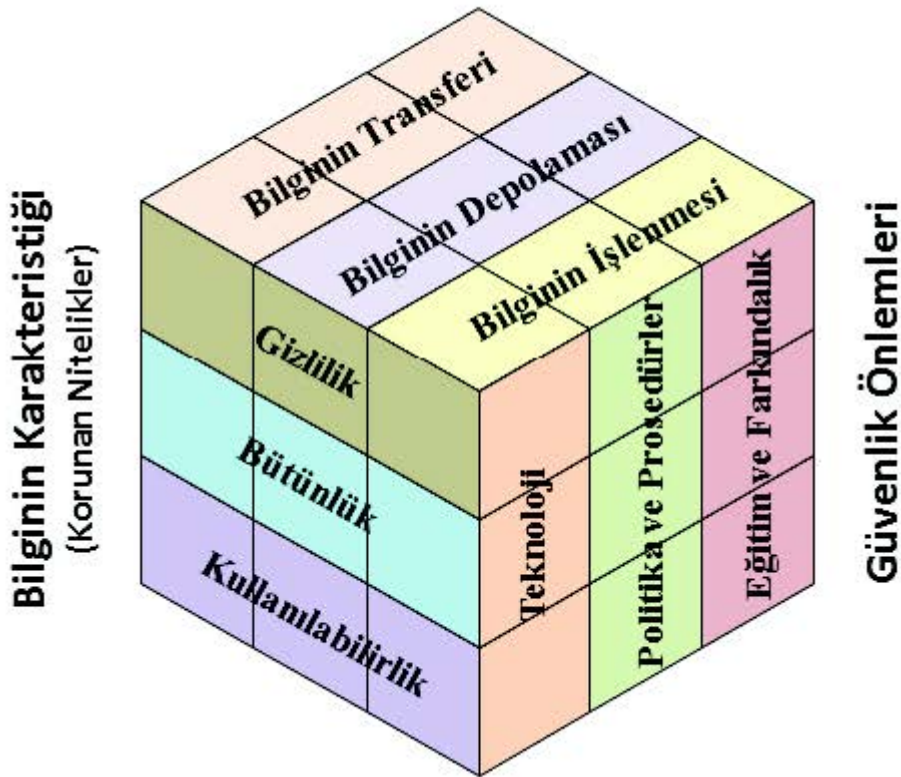
Görsel kaynağı: https://www.researchgate.net/publication/346192126_Requirements_for_cybersecurity_in_agricultural_communication_networks/

5.6.1 Bilgi güvenliđinin temel unsurları



CIA üçgeni. Görsel kaynađı: <https://fikirjeneratoru.com/bilgi-guvenligi-ve-bilgi-guvenligi-unsurlari/>

Bilginin Durumu



McCumber Küpü. Görsel kaynađı: <https://fikirjeneratoru.com/bilgi-guvenligi-ve-bilgi-guvenligi-unsurlari/>



Geniřletilmiş *CIA* üçgeni

6. Temel Kavramlar

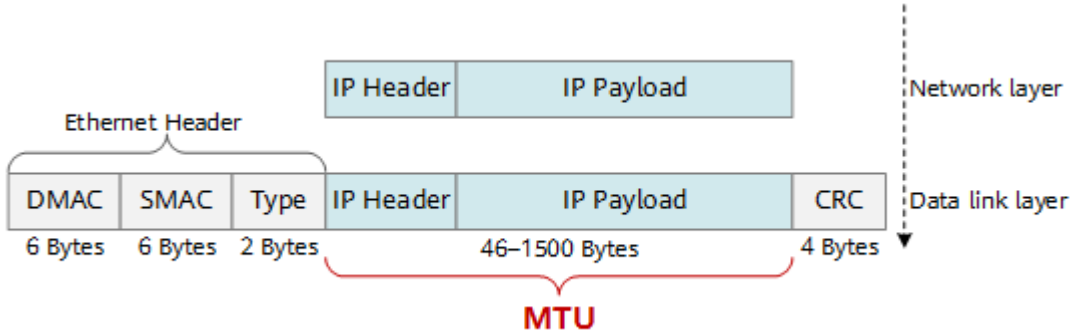
6.1 Aktarım Verimliliği

$$\text{Verimlilik} = \frac{\text{Veri}}{\text{Veri} + \text{TCP/UDP başlığı} + \text{IP başlığı} + \text{Ethernet başlığı}}$$

Bu denkleme göre; bir seferde gönderilen veri bloğu ne kadar büyürse, verim o kadar artar.

6.2 MTU

Maximum Transmission Unit. Bir seferde gönderilebilecek maksimum veri miktarını belirler. Ethernet ağlarında MTU değeri varsayılan olarak **1500 bayt/kapsül**



Görsel Kaynağı: <https://info.support.huawei.com/info-finder/encyclopedia/en/MTU.html/>

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.407]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>netsh interface ipv4 show subinterfaces

MTU  MediaSenseState  Bytes In  Bytes Out  Interface
-----
1500  1  1861275532  785975034  Ethernet
1500  1  0  37634053  VMware Network Adapter VMnet1
4294967295  1  0  33993823  Loopback Pseudo-Interface 1
1500  1  37537940  VMware Network Adapter VMnet8
1500  1  5132745  2202382  Ethernet 2

C:\WINDOWS\system32>netsh interface ipv4 set subinterface "Ethernet" mtu=1518 store=persistent
Ok.

C:\WINDOWS\system32>netsh interface ipv4 show subinterfaces

MTU  MediaSenseState  Bytes In  Bytes Out  Interface
-----
1518  1  1861993800  786529873  Ethernet
1500  1  0  37713641  VMware Network Adapter VMnet1
4294967295  1  0  34065789  Loopback Pseudo-Interface 1
1500  1  37617324  VMware Network Adapter VMnet8
1500  1  5540555  2505417  Ethernet 2

C:\WINDOWS\system32>
```

Görsel Kaynağı: <https://softkeys.uk/blogs/blog/how-to-check-mtu-size-in-windows-10/>

6.3 RTT

Round Trip Time. Paketlerin karşı tarafa gidip geri gelmesi için geçen süre.

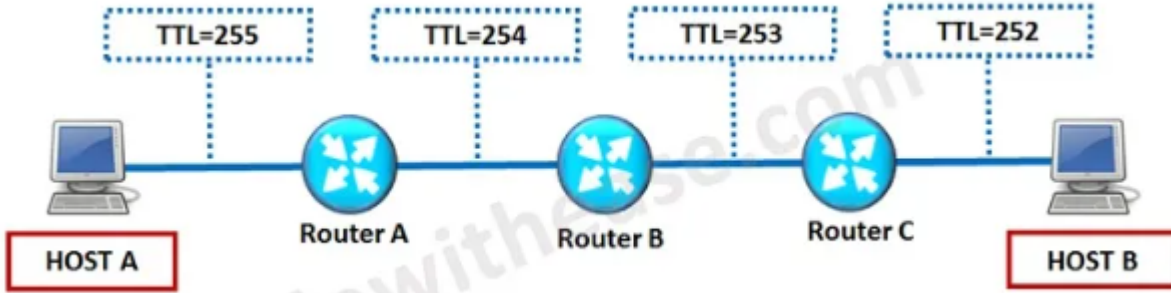
```
murat@BSEU0793:~$ ping -c3 bilecik.edu.tr
PING bilecik.edu.tr (79.123.224.15) 56(84) bytes of data.
64 bytes from www.bilecik.edu.tr (79.123.224.15): icmp_seq=1 ttl=126 time=1.75 ms
64 bytes from www.bilecik.edu.tr (79.123.224.15): icmp_seq=2 ttl=126 time=2.13 ms
64 bytes from www.bilecik.edu.tr (79.123.224.15): icmp_seq=3 ttl=126 time=2.61 ms

--- bilecik.edu.tr ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.753/2.165/2.613/0.352 ms
murat@BSEU0793:~$
```

Linux'ta ping çıktısı

6.4 TTL

Time to Live. Paketlerin ağda sonsuza kadar dolaşmaması için kullanılan **yaşam süresidir**. Başlangıç TTL değeri sistemden sisteme değişir. 256, 128 veya 64 olabilmektedir. Bir paket, **hop noktaları** arasında her aktarıldığında **TTL değeri 1 azalır**.



Görsel kaynağı: <https://ipwithease.com/what-is-time-to-live-ttl-in-networking/>



Zamana Karşı filmindeki insanların TTL değeri

6.5 Bant Genişliği (Bandwidth)

Haberleşme kanalının veya iletim ortamının kapasitesini ifade etmek için kullanılır. Analog sinyallerde birini **Hertz (hz)** iken, dijital sistemlerde **bps (b/s)** şeklindedir.

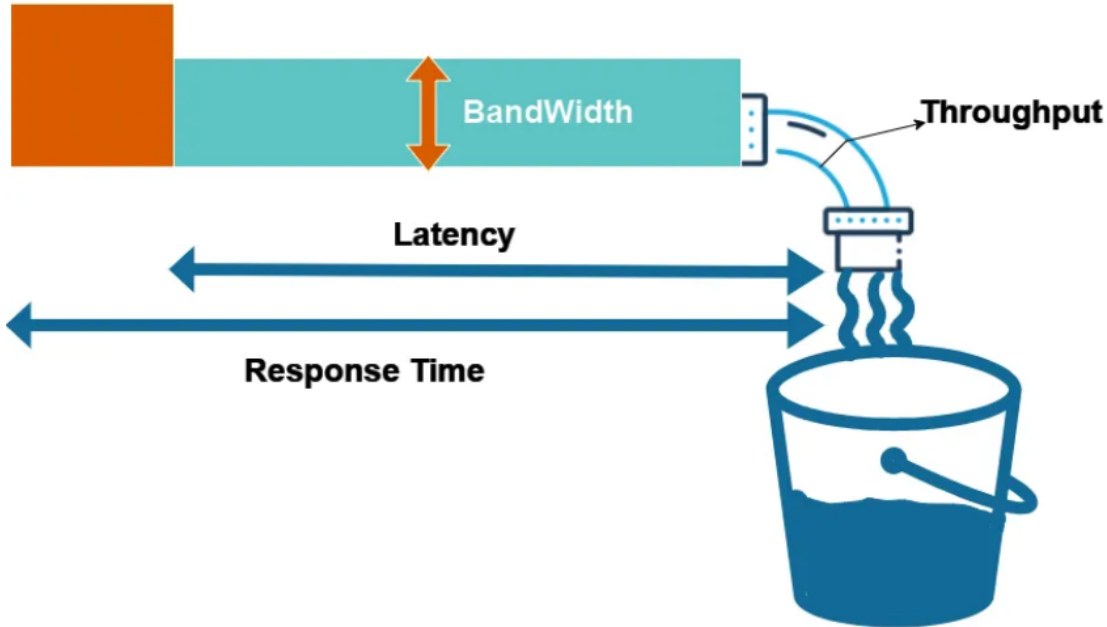
Note

"Bant geniřlięi" kavramını otoban yolda řerit sayısı gibi dūřünebiliriz. Trafik ne kadar fazla olursa olsun, řerit sayısı arttıkça trafik sorunsuz ilerleyebilir. Bu kavram doęrudan iletimin hızını ifade etmemekte ama dolaylı olarak iletim süresinin kısalmasını saęlamaktadır.

Bir haberleřme sistemi, gönderici, alıcı ve iletim ortamından oluşur. İletim kapasitesi en küçük olan, bütün sistemin bant geniřlięi belirler.

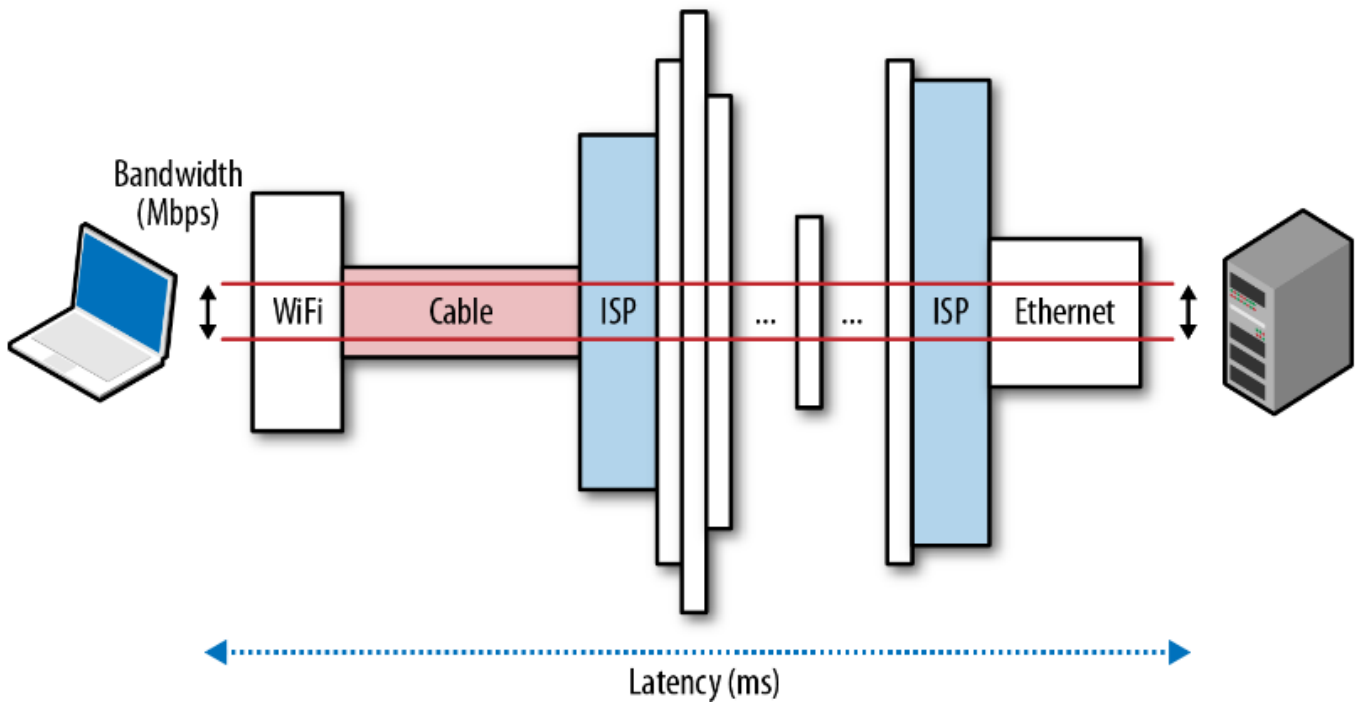
Bant geniřlięi ile ilgili dięer kavramlar:

1. Latency (gecikme süresi): Verinin aę üzerinde aktarımı sırasında geęen süre.
2. Response time (cevap süresi): Bilgisayarların performansı da dahil edilerek cevap almak için geęen toplam süre.
3. Throughput (işlem hacmi): Bant geniřlięi teorik bir kavram iken, işlem hacmi uygulamada görülen geręek kapasiteyi ifade eder. Anahtar (switch) cihazlarının da işlem kapasitesi bu kavram ile ifade edilir.

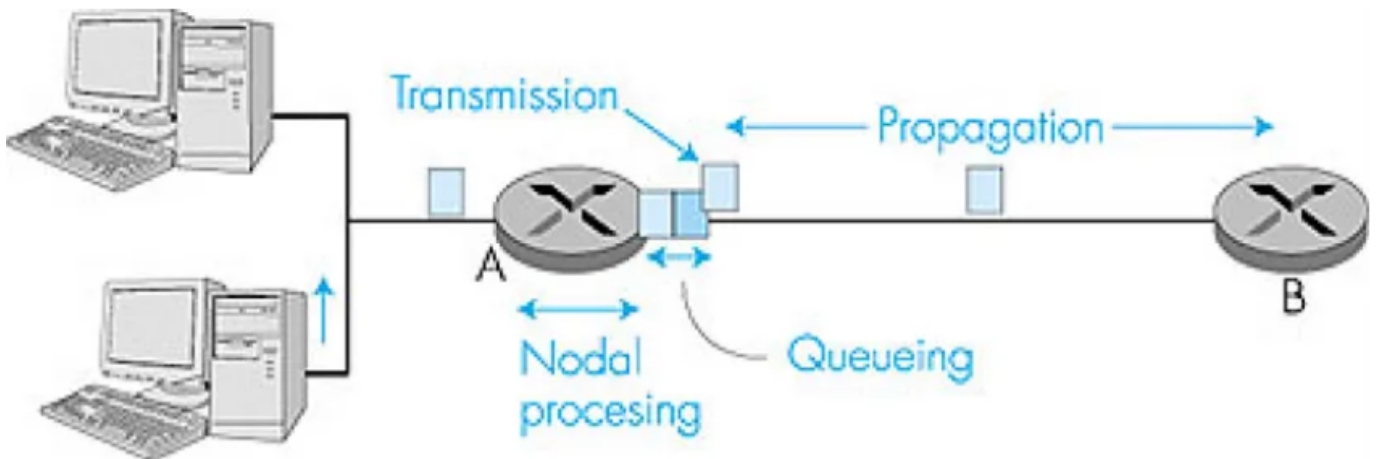


Görsel kaynaęı: <https://medium.com/@sandeep15mca/latency-bandwidth-throughput-and-response-time-0ee4d9028277>

6.6 Gecikme kaynakları



Görsel kaynağı: <https://www.oreilly.com/content/primer-on-latency-and-bandwidth/>

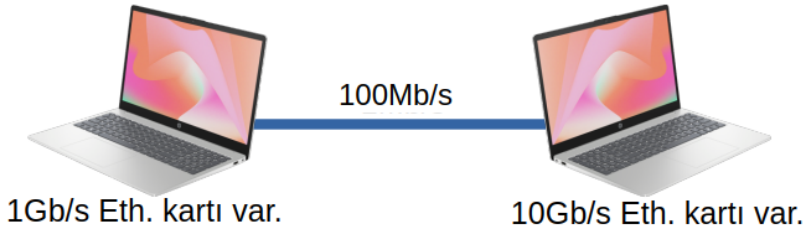


Gecikme Kaynakları. Görsel kaynağı: <https://medium.com/@ComNetworks2014/computer-networks-traffic-delay-and-throughput-97c1c2820466/>

Örnek Soru

240 MB büyüklüğündeki bir MP3 dosyası, görseldeki sistemde 4 dakikada aktarılıyor.

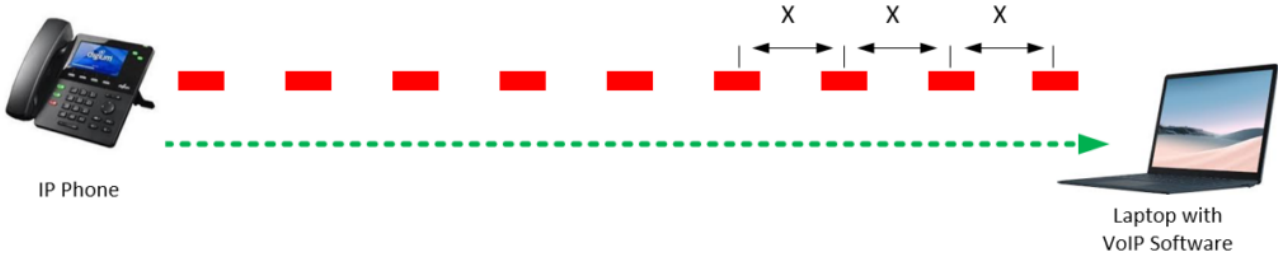
1. Bu sistemin aktarım kapasitesi (bant genişliği) ne kadardır?
2. Dosya aktarım hızı b/s cinsinden ne olmuştur?
3. Aktarılan dosya, MP3 yerine MPG olsaydı ne olurdu?



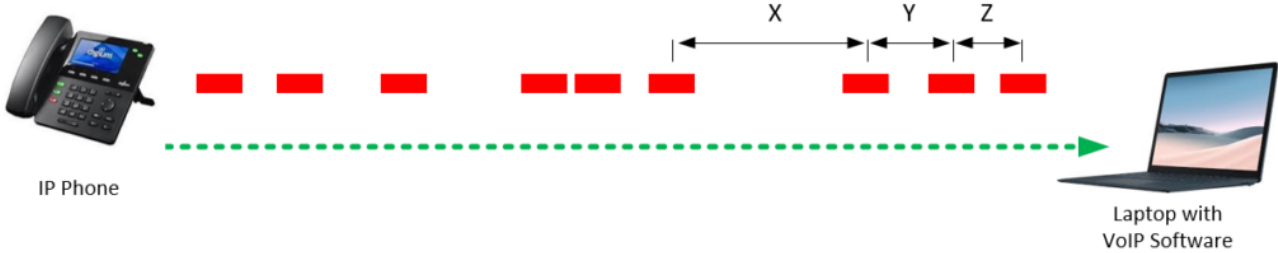
6.7 Jitter

Dilimize *seğirme*, *sapma* şeklinde çevrilebilir. Giden veri paketlerinin gecikme sürelerinde farklılık olması durumu. Özellikle canlı anlık iletişimin sağlıklı olmasına sebep olabilir.

No Jitter



Jitter

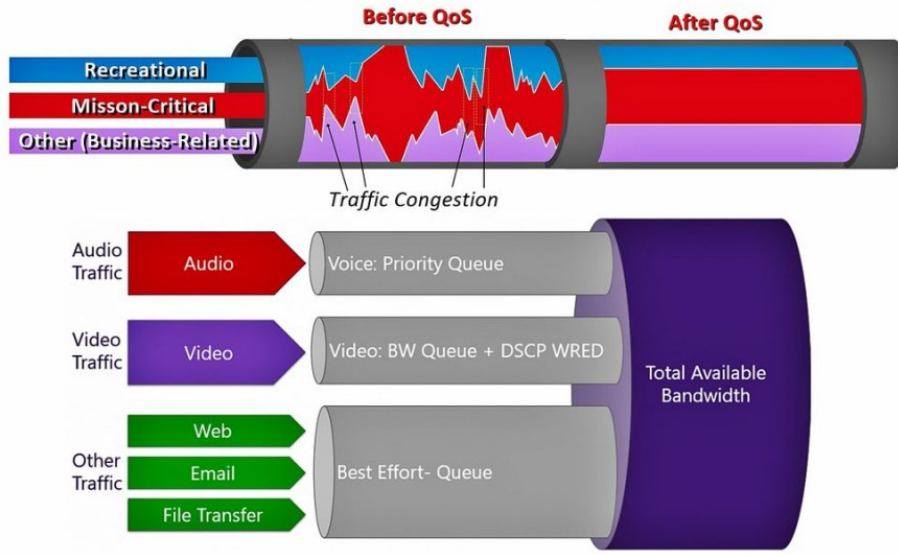


Görsel kaynağı: <https://sonary.com/content/jitter-what-it-is-and-how-to-deal-with-it/>

6.8 QoS - hizmet önceliklendirme

Quality of Service. Bant genişliğinin verimli kullanılması için bazı trafik verilerine öncelik vermek için kullanılır. Ambulans önceliği gibi düşünebilirsiniz. Belirli IP adreslerine ya da belirli uygulamalara öncelik verilebilir. Özellikle canlı anlık iletişim sağlayan telefon görüşme uygulamaları gibi durumları önceliklendirmek için kullanılır.

What is QoS?

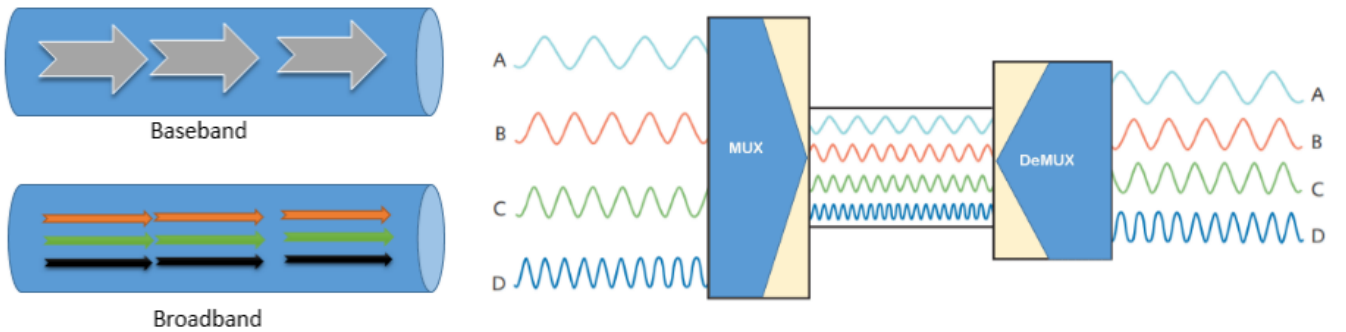


How Does QoS Work In The Networks?

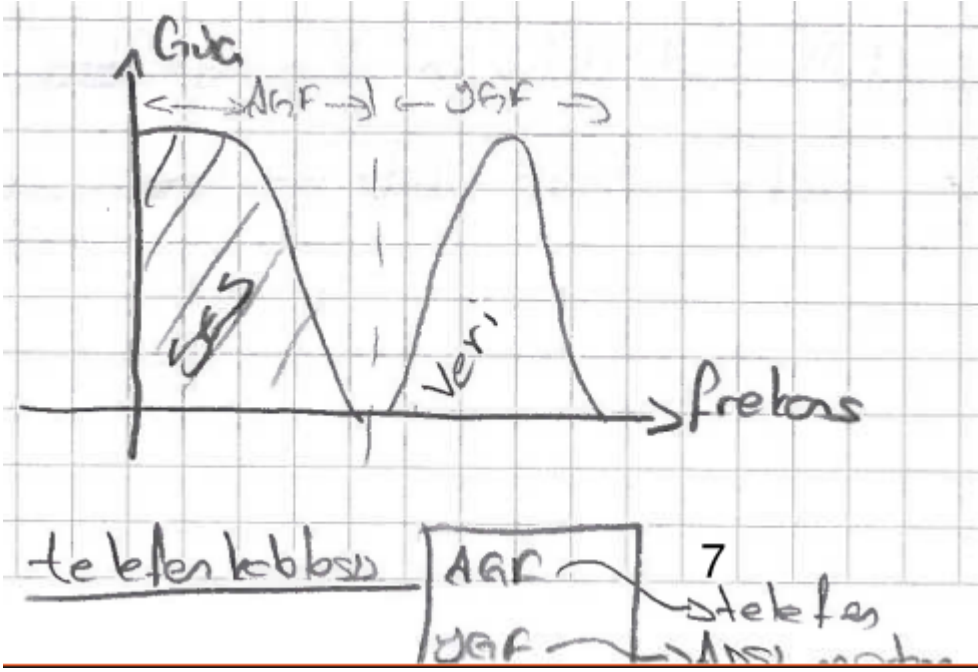
QoS. Görsel kaynağı: <https://www.linkedin.com/pulse/what-qos-saravind-rajan/>

6.9 Temel Bant ve Geniş Bant

- **Temel bant** (*Base Band*). İletim ortamında tek bir frekans bandı kullanılır. Böylece teorik olarak iletim ortamının tüm kapasitesi tek bir kanal için kullanılır. Ethernet'te temel bant kullanılır.
- **Geniş Bant** (*Broad band*). İletim ortamında birden fazla frekans bandı kullanılır. bulunur. Basit bir frekans band filtresi sayesinde kanallar ayrıştırılabilir. Telefon hattından aynı anda ses verinin taşınması buna örnektir.



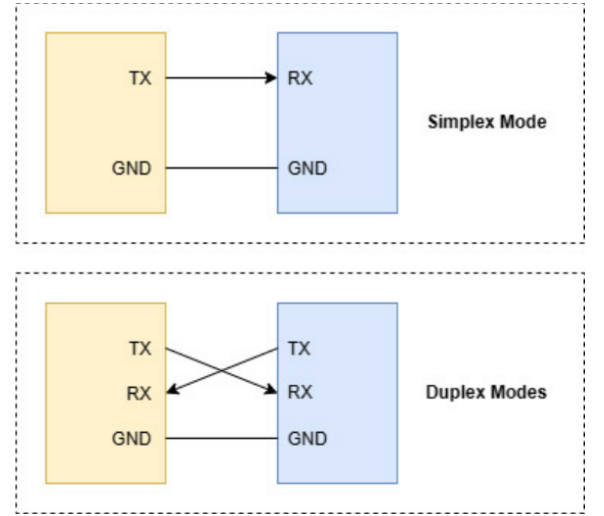
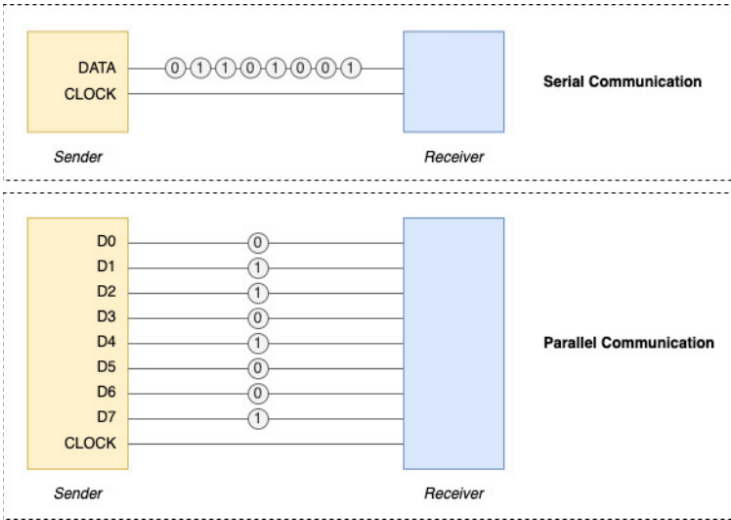
Görsel Kaynağı: <https://www.computernetworkingnotes.com/networking-tutorials/differences-between-baseband-and-broadband-explained.html/>



Geniş bant içindeki farklı verileri ayırıştırma

6.10 Paralel ve Seri İletişim

Paralel iletişimde byte düzeyinde iletişim sağlanır. İki uç arasında en az 8 tane fiziksel iletim ortamı olmalıdır. Band genişliği teorik olarak 8 hat daha fazla olduğu düşünülebilir. Ancak hem maliyet hem protokol tercihi hem de kullanılan topoloji gibi etkenler bu konuda etkilidir.



Görsel kaynağı: <https://www.digikey.com/en/maker/tutorials/2023/what-is-serial-communication-and-how-does-it-compare-to-parallel>

Araştırma sorusu

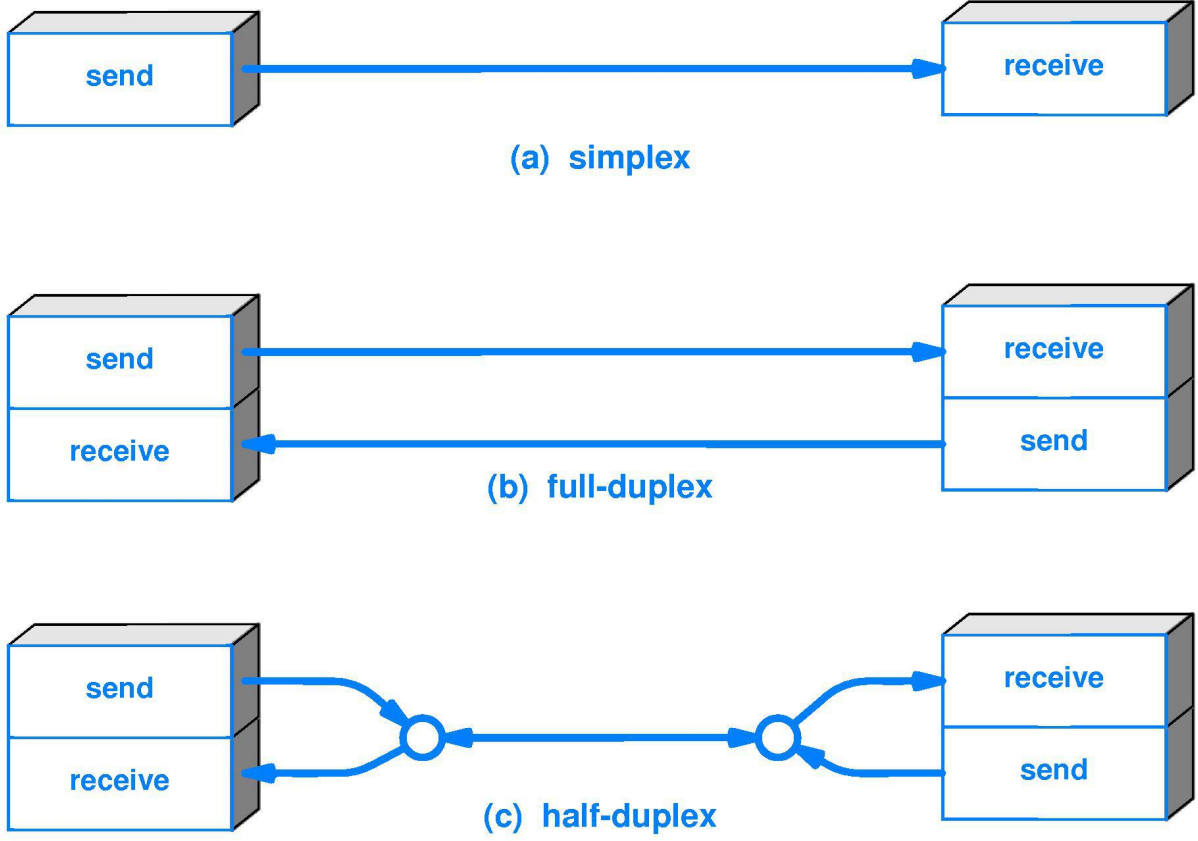
Paralel iletişim daha hızlı olmasına rağmen neden günümüzde hala bazı yerlerde seri iletişim kullanılıyor? Gündelik hayatımızda bilgisayar kullanırken nerelerde seri iletişim kuruyoruz?

6.11 Haberleşme Kanalı Modları

1. **Simplex Kanal:** Televizyon ve radyo gibi yayının tek tarafı olarak yapıldığı kanallardır.

2. **Half-dupleks Kanal:** Çift yönlü iletişim vardır. Ancak aynı anda sadece bir taraf veri gönderebilir. **telsiz** gibi.
3. **Full-dupleks Kanal:** İki uç arasında iki tane simplex kanal vardır. Böylece aynı anda iki taraf veri gönderebilir ve alabilir. Örnek **telefon görüşmeleri**.

Günümüzde tüm bilgisayar ağları **full-dupleks**'tir.



Görsel kaynağı: <https://www.blackbox.co.uk/gb-gb/page/25069/Resources/Technical-Resources/Black-Box-Explains/Fibre-Optic-Cable/Simplex-vs-duplex-fiber-patch-cable/>

7. İletim Ortamları

Temelde **atmosfer** ve **kablo** olmak üzere iki farklı iletim ortamı mevcuttur. Atmosferde **RF** (radyo frekans) dalgalarını kullanarak iletişim gerçekleşir. Kablolarda ise genellikle **fiberoptik** ve **bakır** kablo kullanılmaktadır.

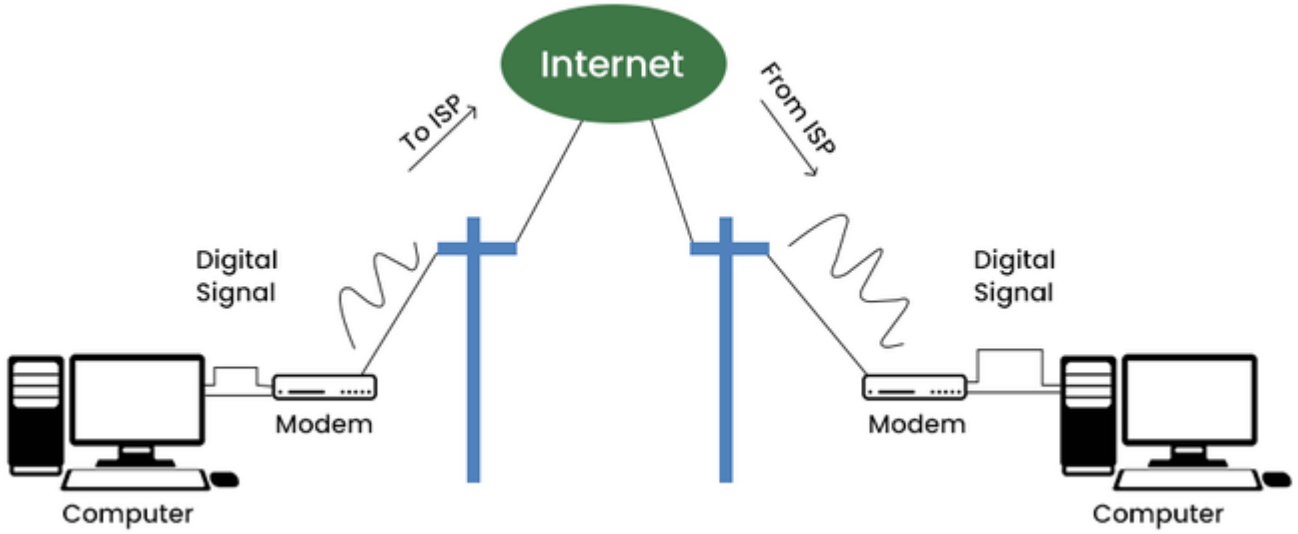
İnternet yaygınlaşmaya başladığında, dünyadaki her eve kablo çekmek mümkün olmadığından, mevcut altyapılardan nasıl yararlanılacağına çalışıldı. Her eve gidebilecek en kolay yöntem telefon hattı olduğundan ilk İnternet bağlantıları telefon hattı üzerinden sağlandı. Eskiden telefon hattı üzerinden internet hizmeti de kullanmaya çalışırken, şimdi internet altyapısı üzerinden *-ihtiyaç olursa-* telefon hizmeti de kullanabiliyoruz.



Görsel: https://www.instagram.com/memeforprogrammer/p/DEkZzG6Kd2_/

7.1 İki Telli Bakır Telefon Hattı

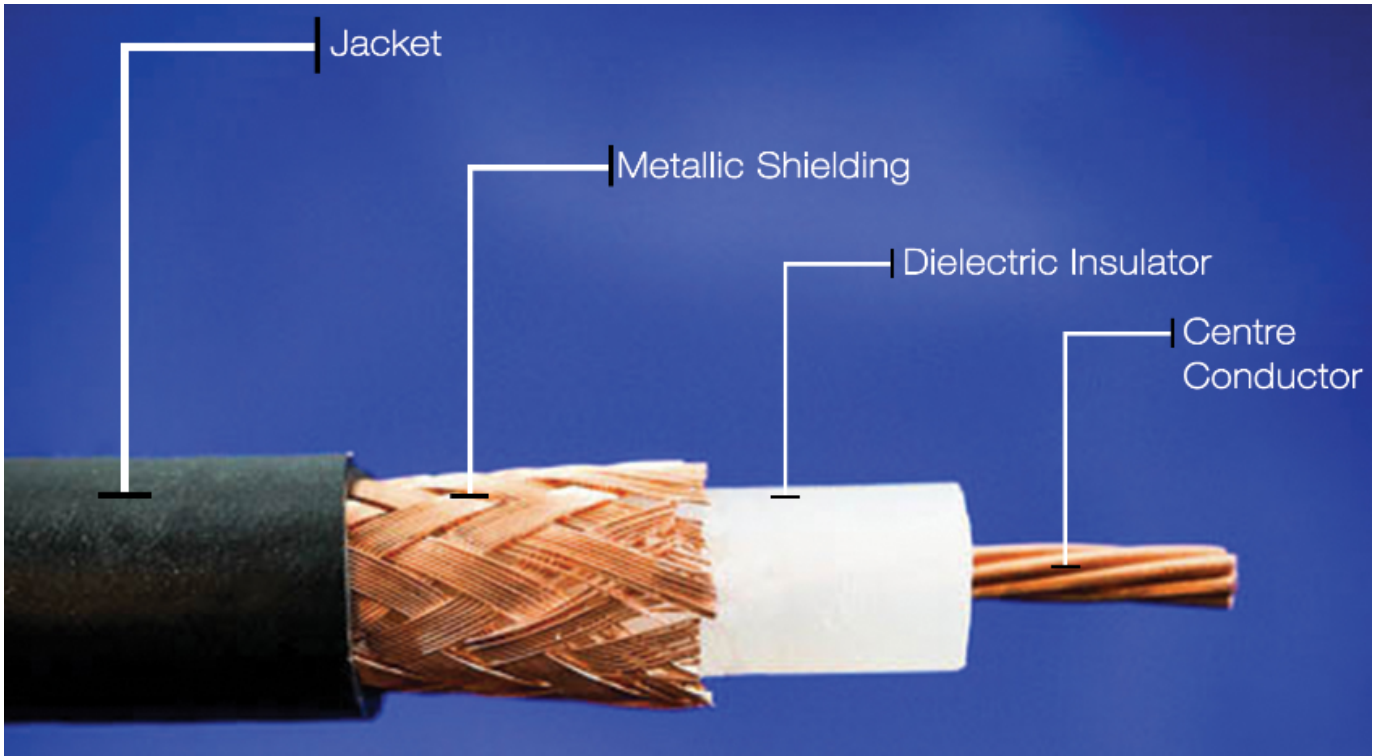
Telefon iletişimini sağlamak için tasarlanmıştır. İnternet'te yaygın kullanılan ilk kablo türüdür. Temel bant ve geniş bant internet hizmeti verilmektedir. Analog modülasyon teknikleriyle en fazla 56 Kb/s'lik band genişliği sağlar. xDSL teknolojileriyle teorik olarak 400 Mb/s'lik bant genişliğine ulaşılmaktadır.



Görsel kaynağı: <https://www.geeksforgeeks.org/types-of-internet-connection/>

7.2 Koaksiyel (Coaxial) Kablo

Genellikle elektriksel gürültünün yoğun olduğu şartlarda kullanılırdı. Yalıtkan bir tüpün içerisinde giden bir tel ve tüpün dışına sarılmış kafes şeklinde teller vardır. Yerel ağlarda (LAN) 180m'de(max) 10M b/s bant genişliği sağlar. Bu kullanımı 10 Base 2 olarak bilinir. Daha sonra 500 m mesafede çalıştırılacak hale getirilir. 10 Base 2 ismiyle standartlaştırılmıştır. 50 ohm'luk direnç değeri vardır. BNC tarzında konnektörler kullanılır. Günümüzde LAN'da hiç kullanılmamaktadır. Sebebi hem 10 Mb/s hızının çok düşük olması, hem de UTP kablolar kadar ekonomik ve işlevsel olmamasıdır. Bilgisayar ağlarında doğrusal (bus) topolojilerde kullanılmıştır.



Görsel kaynağı: <https://www.wiremasters.com/newshub/news/the-ins-and-outs-of-coaxial-cable>



BNC Konnektörler

7.3 Bükümlü Çift Kablo (Twisted Pair Cable)

İçerisinde bükülmüş çiftler halinde bakır tel bulunur. Kabloların birbirleri üzerindeki direnç elektromanyetik etkisini azaltmak için ikiyeşerli olarak sarılı durumundadırlar.



Bükümlü çift kablo

UTP**FTP****STP****SFTP**

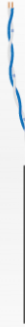
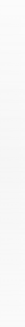
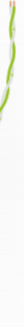
Görsel kaynağı: <https://www.linx-com.com/copper-construction/>

- U: Unshielded (Korumasız)
- F: Foiled (Folyolu)
- S: Shielded (Korumalı)

7.3.1 Frekanslarına Göre xTP kablolar

Category	Maximum Speed	Max. Length	Frequency	SHIELDING	Application
CAT 1	Up to 1Mbps(Carry only Voice)	--	1MHz	Unshielded	Old telephone cabling
CAT 2	Up to 4Mbps	--	4MHz	Unshielded	Token Ring Network
CAT 3	Up to 10Mbps	100m	16MHz	Unshielded	Token Ring & 10BASE-T Network
CAT 4	Up to 16Mbps	100m	20MHz	Unshielded	Token Ring Network
CAT 5	Up to 100Mbps	100m	100MHz	Unshielded	Ethernet, Fast ethernet and Token Ring
CAT 5e	Up to 1Gbps	100m	100MHz	Unshielded or Shielded	Ethernet, Fast ethernet & Gigabit ethernet
CAT 6	Up to 10Gbps	100m	250MHz	Unshielded or Shielded	Ethernet, Fast ethernet, Gigabit ethernet & 10G Ethernet(37 - 55 meter)
CAT 6a	Up to 10Gbps	100m	500MHz	Shielded	Ethernet, Fast ethernet, Gigabit ethernet & 10G Ethernet(37 - 55 meter)
CAT 7	Up to 10Gbps	100m	600MHz	Shielded	Ethernet, Fast ethernet, Gigabit ethernet & 10G Ethernet(100 meter)
CAT 8	Up to 40Gbps	100m	2000MHz	Shielded	Ethernet, Fast ethernet, Gigabit ethernet & 25G-40G Ethernet(30 meter)

Görsel kaynağı: <https://dc.mynetworkinsights.com/categories-of-copper-twisted-pair-cables/>

											
CAT 1	CAT 2	CAT 3	CAT 4	CAT 5	CAT 5e	CAT 6	CAT 6A	CAT 7	CAT 7A	CAT 8.1	CAT 8.2
1 Mbps	4 Mbps	10 Mbps	16 Mbps	100 Mbps	1 Gbps	1 Gbps	10 Gbps	10 Gbps	10 Gbps	25 Gbps	40 Gbps
400 KHz	4 MHz	16 MHz	20 MHz	100 MHz	100 MHz	250 MHz	500 MHz	600 MHz	1000 MHz	2000 MHz	2000 MHz
1983	1987	1991	1993	1995	2001	2002	2008	2010	2013	2016	2018

All Rights Reserved, Samm Teknoloji / telecom.samm.com / telecom@samm.com

Görsel kaynağı: <https://telecom.samm.com/history-of-ethernet-lan-cables-categories>

CAT-1, CAT-2, CAT-3

Telefon hatlarında kullanılır, ağlarda kullanılmaz.

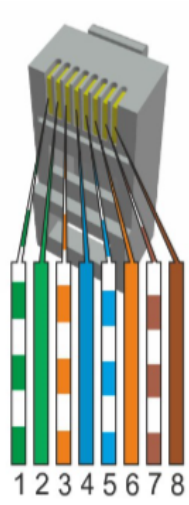


Görsel kaynağı: <https://www.electricalvolt.com/how-to-crimp-rj45-connector/>

Bükümlü çift CAT5 VE CAT6 Kabloları sonlandırmak için RJ-45 adı verilen konnektörler kullanılır. Bu kablolar iki farklı iki şekilde sonlandırılabilir: **568-A, 568-B**

Kablonun iki ucunun aynı standartlarla sonlandırılmasına **düz (Straight kablo)** denir. İki ucunda iki farklı standartta sonlandırılma yapılırsa **çapraz(cross-over)kablo** adı verilir.

7.3.2 Ethernet Kablosunda Pin Dizilimi

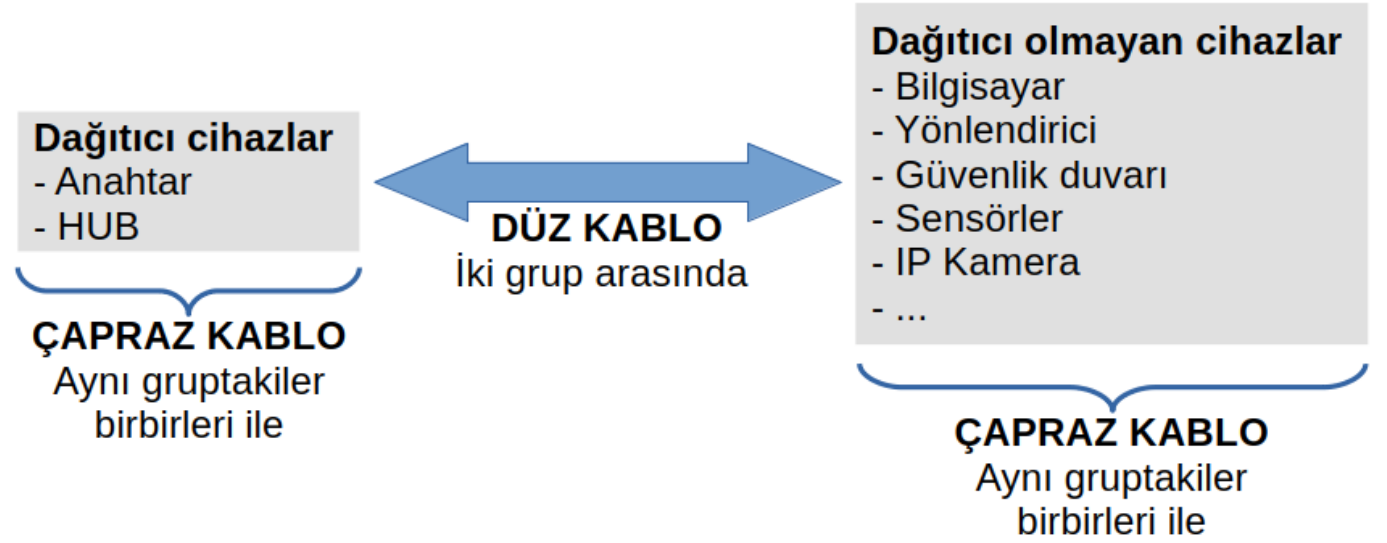


RJ45 Pin #	Wire Color (T568A)	Wire Diagram (T568A)	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	White/Green		Transmit+	BI_DA+
2	Green		Transmit-	BI_DA-
3	White/Orange		Receive+	BI_DB+
4	Blue		Unused	BI_DC+
5	White/Blue		Unused	BI_DC-
6	Orange		Receive-	BI_DB-
7	White/Brown		Unused	BI_DD+
8	Brown		Unused	BI_DD-

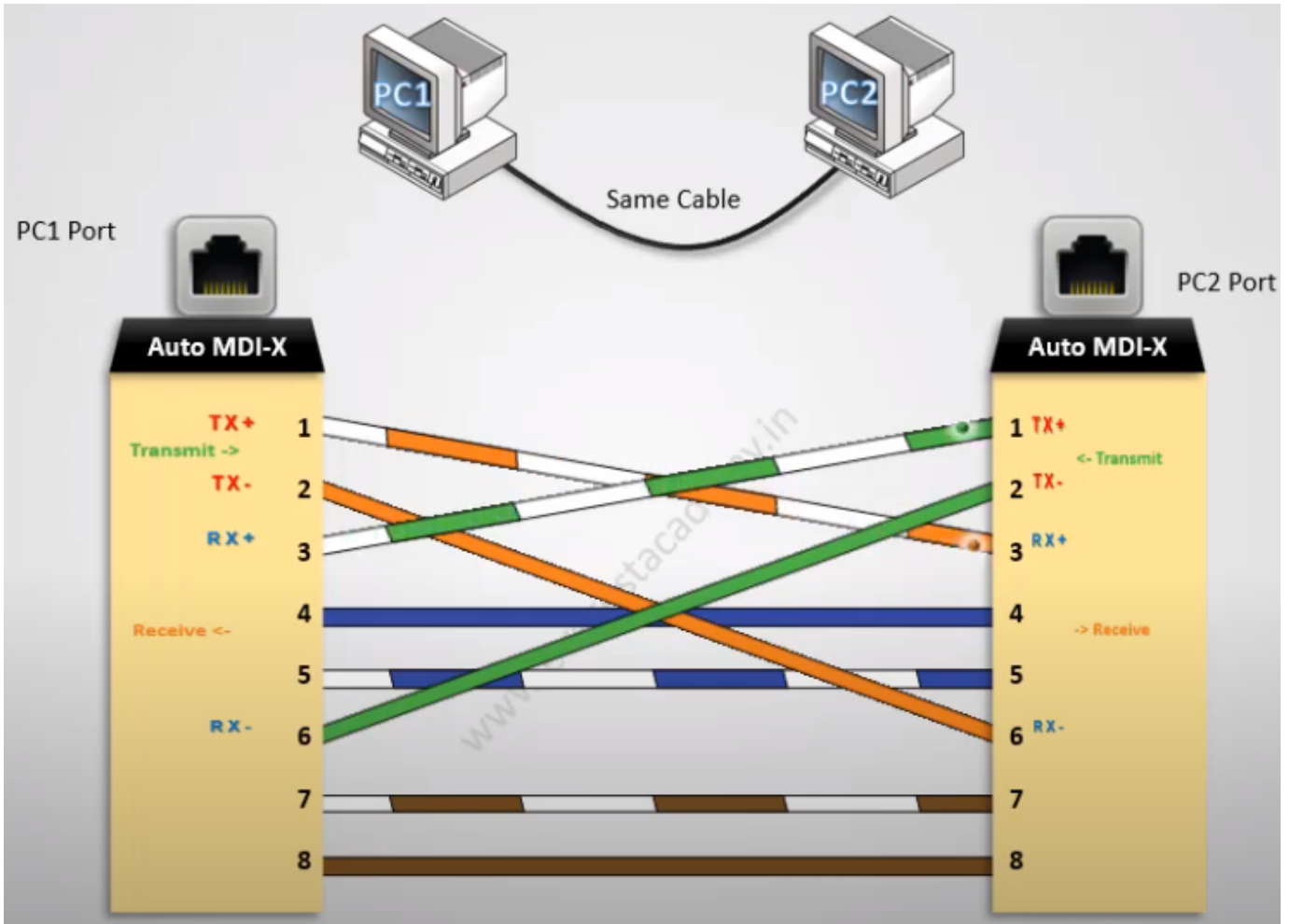
Görsel kaynağı: <https://resources.altium.com/p/gigabit-ethernet-101-basics-implementation/>

7.3.3 Çapraz ve Düz Kablo

Bilgisayar ile dağıtıcı cihazların (anahtar, hub) iletişim kurabilmesi için; Bilgisayarın TX (Transmit) hattına karşılık anahtarın RX (Receive) hattı denk gelmelidir. Dağıtıcı olan ve olmayan cihazların pinleri karşılıklı denk gelecek şekilde (TX <-> RX) tasarlanmıştır. Ancak aynı türde iki cihaz birbirine bağlanırsa o zaman TX-TX ve RX-RX portlar karşılıklı gelmiş olur. Bu durumda çapraz (Crossover) kablo kullanılır.



Çapraz kablo ne zaman kullanılır?



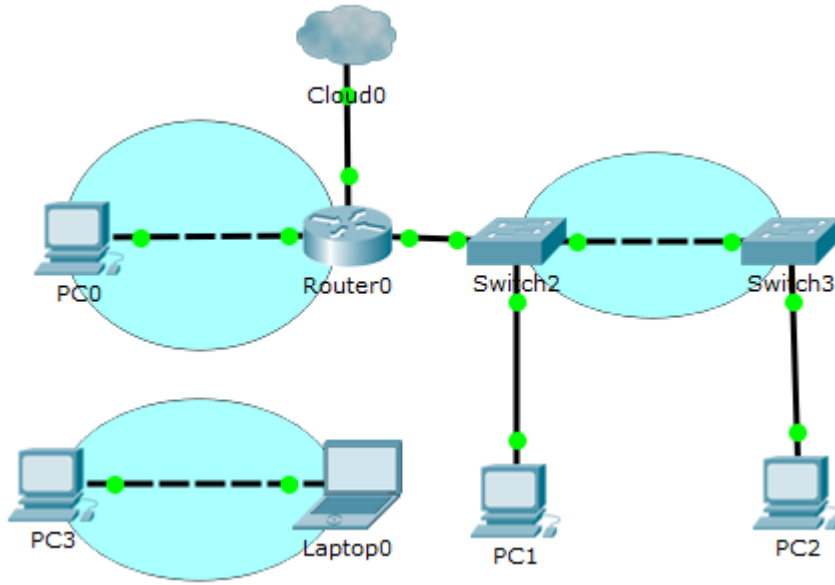
FastEthernet çapraz kablosu. Görsel kaynağı: <https://www.youtube.com/watch?v=WSIuPM4q5Tw/>

Auto-MDI-X

Yeni ağ cihazlarının tamamı Auto-MDI-X adı verilen teknoloji sayesinde karşıdaki cihazın ne tarz bir cihaz olduğunu anlar ve hangi pin'in ne amaçla kullanılacağını buna göre düzenler.

Örnek

Görsel, Cisco Packet Tracer uygulamasında oluşturulmuştur. Kesikli çizgiler çapraz kabloyu temsil eder. Düz çizgi de düz kabloyu temsil eder.



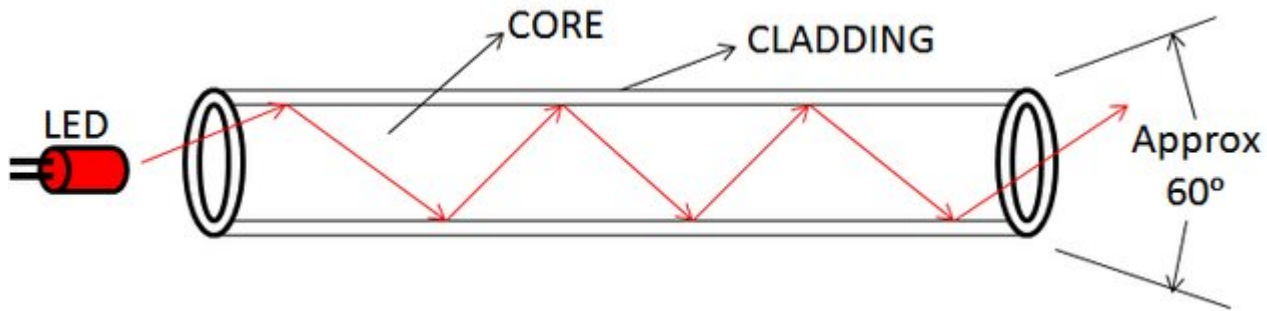
Çapraz kablo kullanım yerleri (örnek)

7.4 Fiberoptik Kablolar

Işığın cam bir tüp içinde iletilmesi şeklinde çalışır. Veri optik dalgalar arıcılığı ile ışığın yansıma kurallarına göre iletilir. Elektriksel sinyallere kıyasla, sinyalin mesafeye bağlı zayıflama ve kayıpları çok azdır. Bakır kablolarla zorunlu olan *gerilim farkından kaynaklanan topraklama ihtiyacı* yoktur.

Verici tarafından ışık kaynağı olarak lazer diyot(led), alıcı tarafında ise fotodiyot ya da foto transistör gibi elektronik elemanlar kullanılır.

Uzak mesafelerde veri iletişimi konusunda fiberoptik kablo dışında Wifi ve uydu iletişimi gibi seçenekler de bulunmaktadır. Ancak en sağlam ve ucuz seçenek fiberoptik kablolardır.

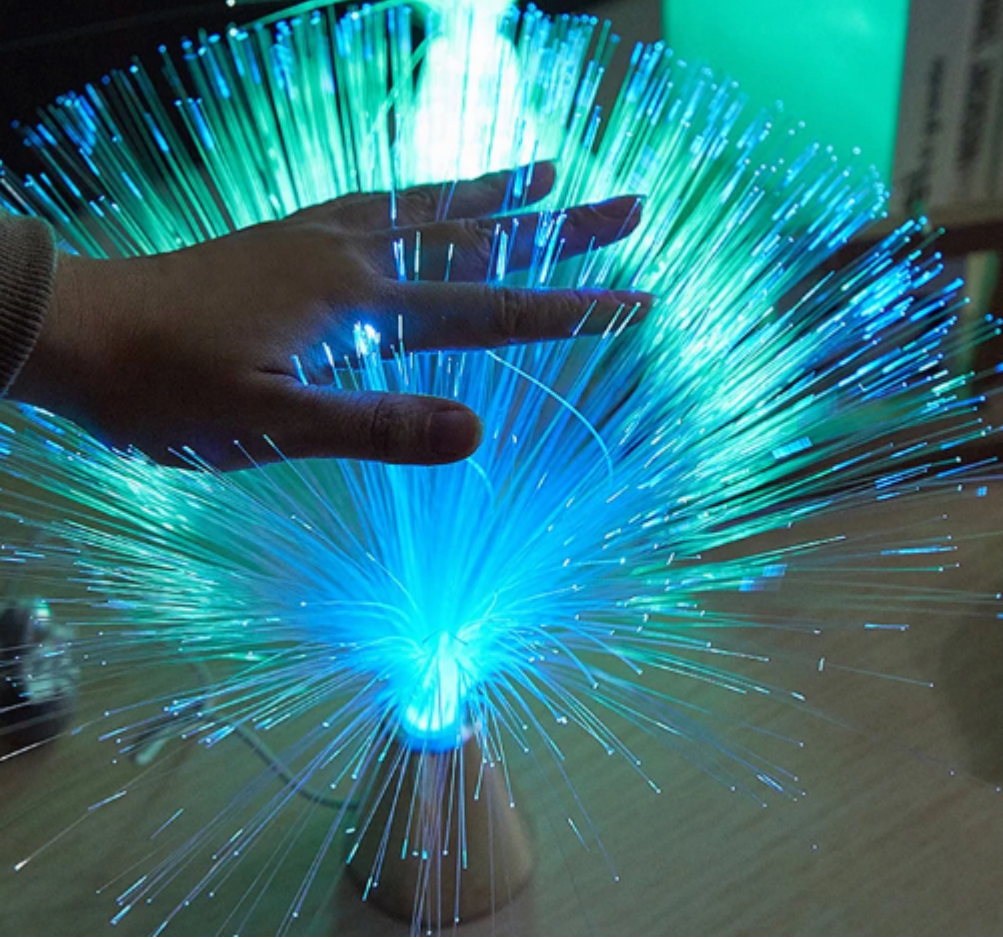


Görsel kaynağı: https://www.researchgate.net/publication/325386764_Optical_Fiber_Sensor_Review_and_Applications/

7.4.1 Fiberoptik kablo avantajları

1. **Yüksek hız ve bant genişliği:** Fiber optik kablolar, geleneksel metal iletişim hatlarına göre daha yüksek bant genişliği sağlar. Bu sayede hızlı ve verimli veri aktarımı mümkün olur.
2. **Daha az sinyal zayıflaması:** Optik fiberdeki sinyal kaybı bakır tellere göre daha azdır. Bu nedenle daha uzun mesafelerde veri iletişimi sağlanabilir.
3. **Daha az elektromanyetik girişim (EMI):** Fiber optik kablolar, elektromanyetik girişime karşı daha az duyarlıdır ve daha güvenilirdir.

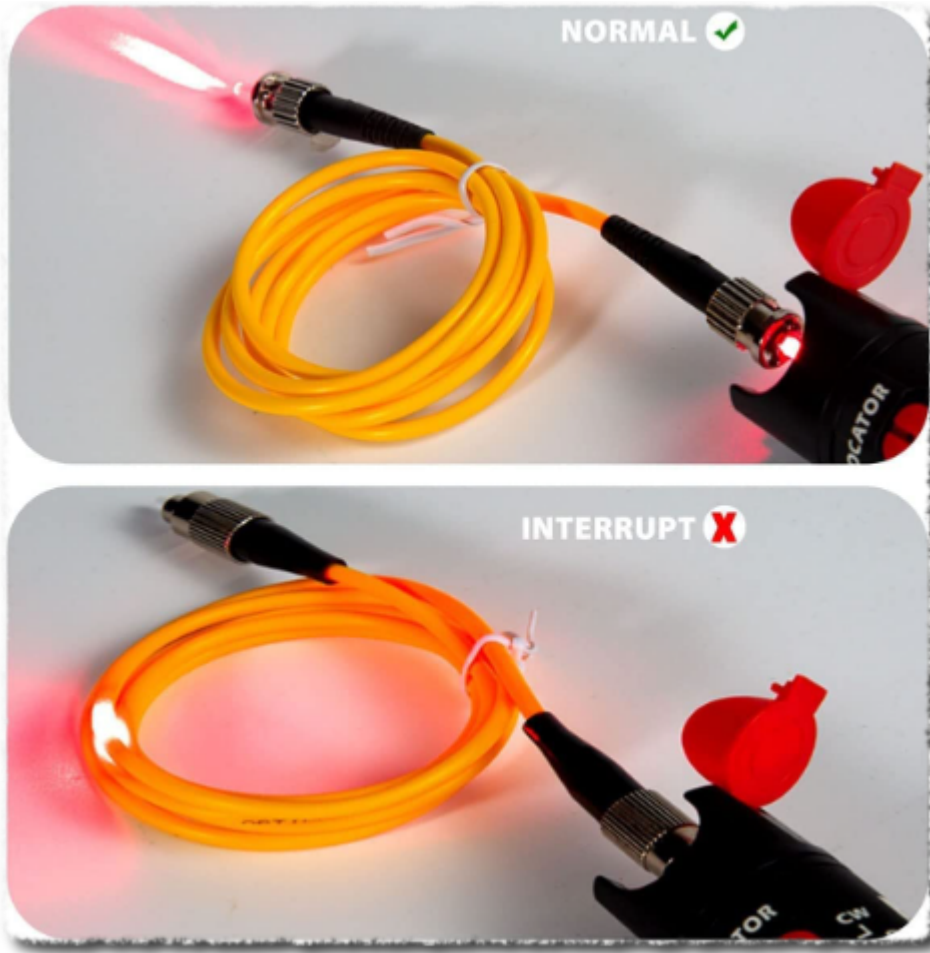
4. **İnce ve hafif:** Fiber optik kablolar, bakır kablolar gibi kalın ve ağır değildir. Bu özellikleri sayesinde kurulum ve bakım işlemleri daha kolaydır.
5. **Dış ortam koşullarına dayanıklı:** Sıcaklık değişimleri, su baskınları, şiddetli hava ve nem gibi çevresel parametrelere karşı dayanıklıdır.
6. **Güvenli:** Elektromanyetik enerji sızması meydana gelmediği için bilgi güvenliği de sağlanmış olur. Kötü kişilerin araya girmesi, bakırdaki kadar kolay değildir.



Görsel kaynağı: <https://he.aliexpress.com/item/1005005348057886.html/>

7.4.2 Fiberoptik kablo dezavantajları

1. **Kırılganlık** - Fiber optik, bakır tellere kıyasla daha kırılgandır ve hasara karşı daha hassastır. Fiber optik kabloları bükmemeli veya bükmemelisiniz.
2. **Pahalı.** Yerel ağlarda, bakır kablolar ve ekipmanlarına göre maliyetli olmaktadır.

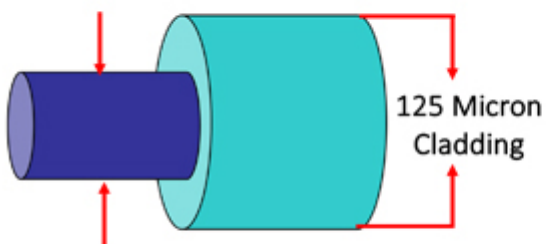


Görsel kaynağı: <https://www.amazon.in/3D-Cloud-Plastic-Connector-Equipment/dp/B07SZFLHB1/>

7.4.3 Fiberoptik kablo türleri

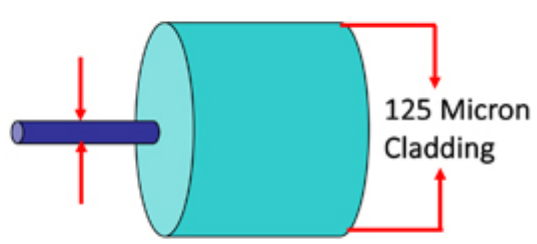
Işık ileten tüpün çapına göre; Single Mod(SM) ve Multi Mod(MM) olmak üzere ikiye ayrılır:

62.5 or 50 Micron Core



Multimode Fiber

8.3 Micron Core

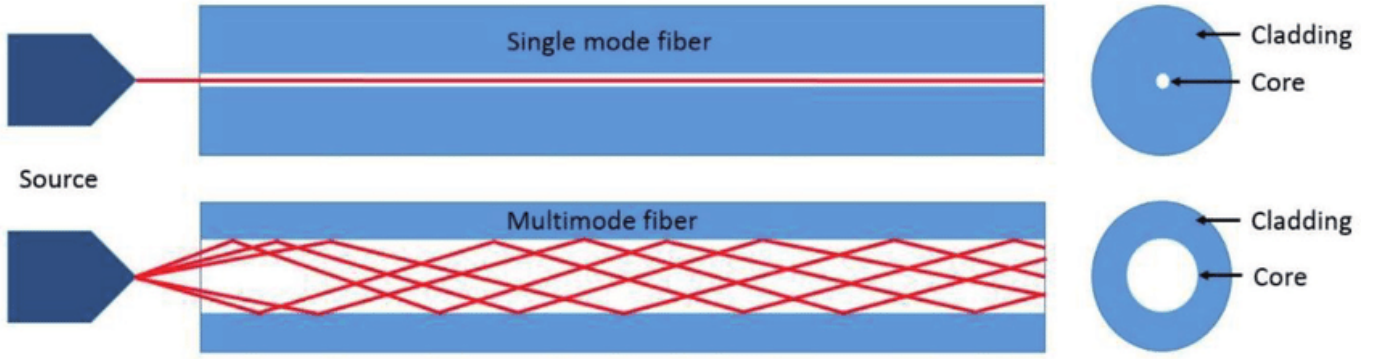


Single-mode Fiber

Görsel kaynağı: <https://learn.aflglobal.com/enterprise/single-mode-vs-multimode/>

Multi-Mode: Bina ya da kampüs içi kısa mesafelerde tercih edilir. Verici ve alıcı maliyetleri single moda göre yarı yarıya azdır.

Single-Mode: Daha uzun mesafelerde daha yüksek bant genişliğine imkan sağlar. Verici ve alıcı donanım maliyetleri daha fazladır.



Görsel kaynağı: <https://fukuoka-ken-ken.co.jp/multi-mode-optical-fiber-k.html>

7.4.4 Fiberoptik çeviriciler

Fiberoptik kablodan gelen ışık sinyallerinin bakır yerel ağlarda kullanılabilmesi için elektriksel sinyallere dönüştürülmesini sağlar. Günümüzde, SFP adı verilen küçük tipte çeviriciler kullanılmaktadır.



Görsel kaynağı: https://salepubsm.live/product_details/37305281.html/

SFP'ler, switch'lere takılarak kullanılır. Kullanılan çeviriciye göre bağlantının bant genişliği belirlenir. Fiberoptik çeviriciler için kullanılan diğer isimler şöyle sıralanabilir:

- F/O converter
- F/O transceiver (transmitter & receiver)
- GBIC. *Gigabit Interface Connector*. Switch modülü halinde olur.
- SFP. *Small Form-factor Pluggable Module*. Switch modülü halinde olur. Bakır ve fiber için SFP'ler bulunmaktadır.



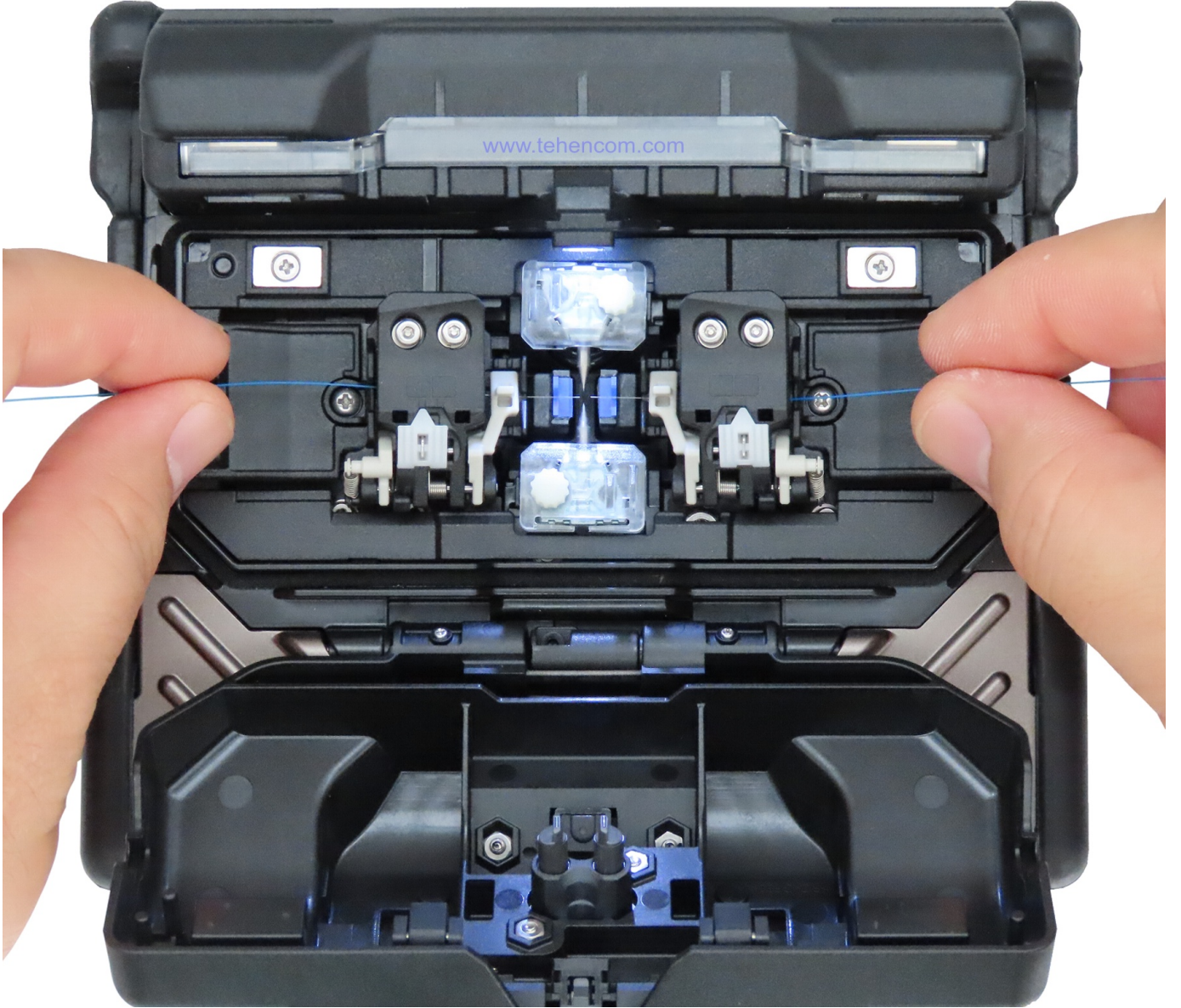
Fiber SFP Module



Copper SFP Module

Görsel kaynağı: <https://www.qsfptek.com/qt-news/sfp-module-introduction-sfp-meaning-fiber-sfp-and-copper-sfp/>

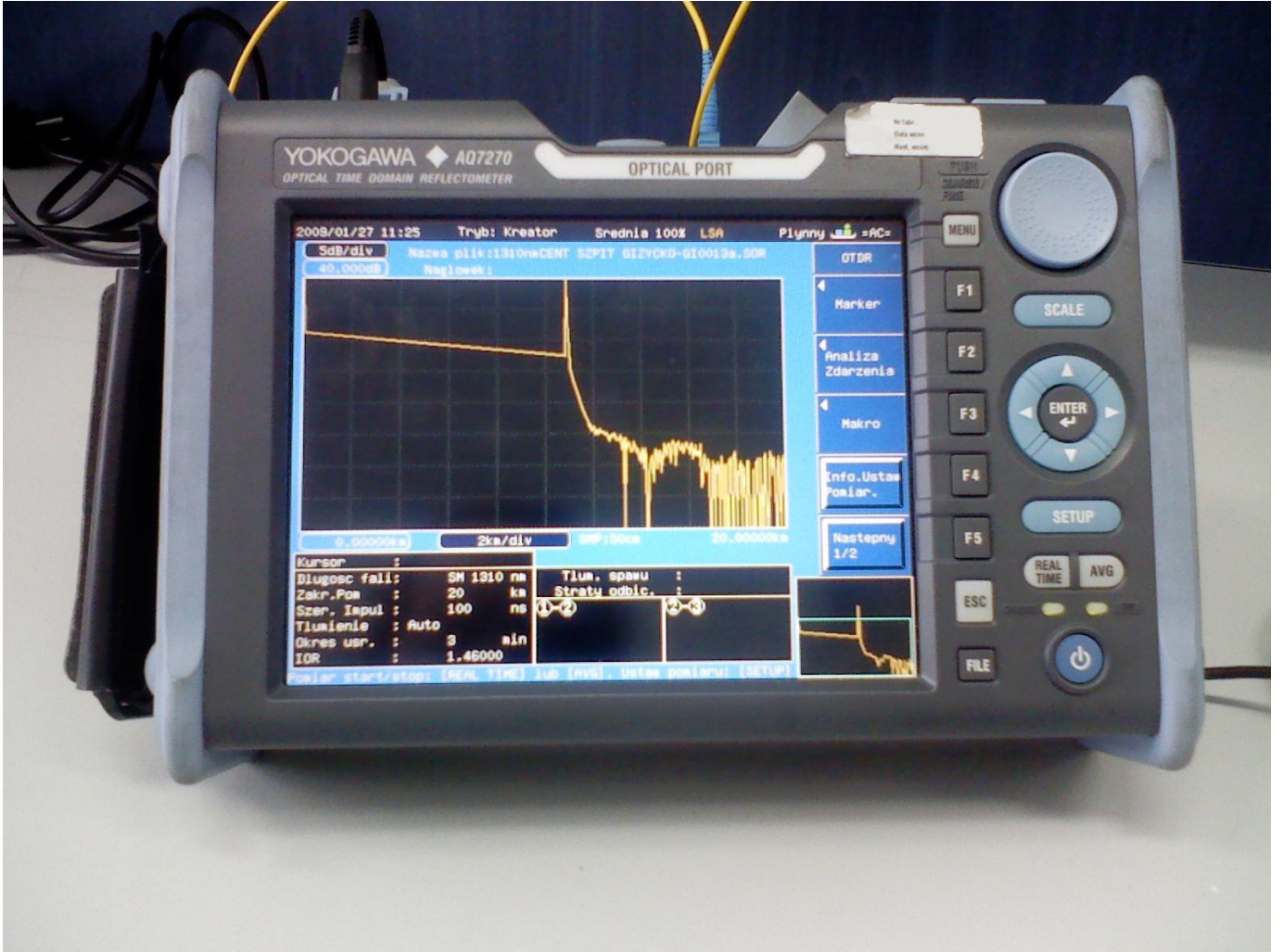
7.4.5 Ekleme ve test işlemleri



Fiberoptik kablo ek (füzyon) işlemi. Görsel kaynağı: <https://www.tehencom.com/fiber-optic-fusion-splicers/fujikura-42s-standard>

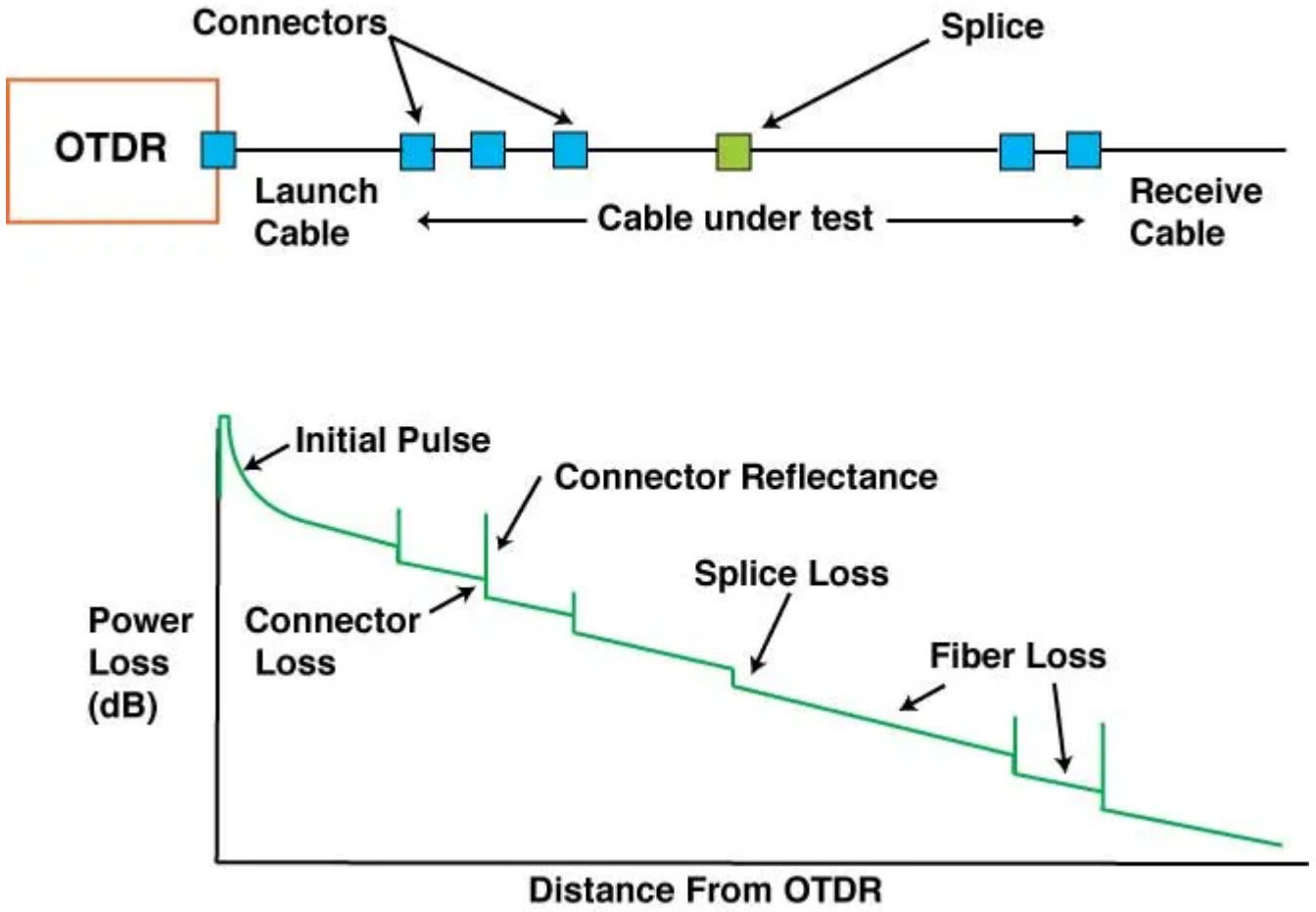


Fiberoptik kablo ek (füzyon) işlemi. Görsel kaynağı: <https://www.tehencom.com/fiber-optic-fusion-splicers/fujikura-42s-standard>



F/O kablo testleri "OTDR" isimli cihaz ile yapılır. Görsel: https://en.wikipedia.org/wiki/Optical_time-domain_reflectometer

OTDR Trace Information



OTDR sonuçları. Görsel: <https://www.baudcom.com.cn/blog/what-is-otdr>

8. Yerel Ağlar - LAN/VLAN

8.1 Ethernet Protokolü

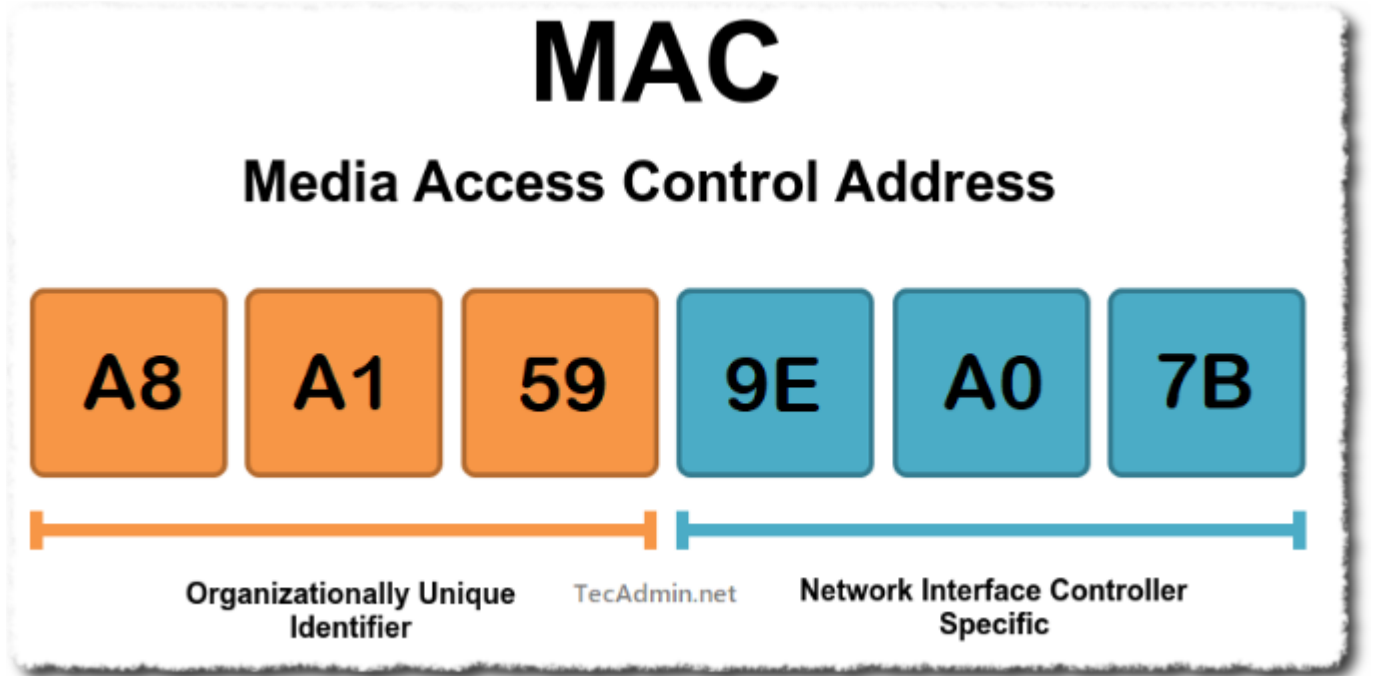
İlk kez Intel ve Xerox firmaları tarafından geliştirilmiştir. Daha sonra IEEE (Institute of Electrical and Electronical Engineering) tarafından 802.3 ismi ile standartlaştırılmıştır.

İsimlendirmeler

- 10 Base 2: 10 sayısı 10 Mb/s'yi ifade eder. "Base" sözcüğü temel bandı ifade eder. En sondaki kablo türüdür. 2 olduğunda ince (thin) koaksiyel kablo ile ~200 metre sınırını belirtir.
- 10 Base 5: Sondaki 5 Kalın(thick) koaksiyel kablo olduğunu belirtir.
- 10 Base T: "T" harfi, bükümlü çift kablo olduğunu ifade eder.
- 100 Base TX: Fast Ethernet Cat-5 kablo kullanılır.
- 100 Base FX: F harfi Fiberoptik Kablo kullanıldığını belirtir.
- 1000 Base T: Gigabit bükümlü çift kablo.
- 1000 Base LX: L long kısaltmasıdır. SM FO kablolar kullanılır. Uzak mesafelerde tercih edilir. En önemli dezavantajı maliyetlerin SX'e göre fazla olmasıdır.
- 1000 Base SX: MM FO kablolar kullanılır. Kısa mesafeleri destekler. Ekipmanları daha ucuzdur.

8.2 MAC Adresi

Yerel ağlarda haberleşmeyi sağlayan ethernet çerçevesinde(frame) 48 bitlik adres kullanılır. MAC adresi 16'lık sayı sisteminde 12 tane karakter ile gösterilir.



Görsel kaynağı: <https://tecadmin.net/media-access-control-address/>

İlk 6 karakter (ilk 24 bit) üretici kodunu (OUI), son 6 karakter ise seri numarasını belirtir. Bir üretici aynı MAC adresini birden fazla karta veremez. Dolayısıyla -teorik olarak- MAC adresleri dünyada tektir (uniq).

GSM ile benzerlik

Telefon sistemindeki IMEI numarası ile GSM numarası arasındaki ilişkinin benzeri, MAC adresi ile IP adresi arasında da vardır.

Dikkat

Birden fazla aynı MAC adresi aynı ağ üzerinde (LAN / VLAN) olmamalıdır.

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\>ipconfig /all

Windows IP Configuration

Host Name . . . . . : GB211341
Primary Dns Suffix . . . . . : uwgb.edu
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : uwgb.edu
System Quarantine State . . . . . : Not Restricted

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : uwgb.edu
Description . . . . . : Intel(R) 82579LM Gigabit
Physical Address. . . . . : 24-BE-05-0F-A7-A0
Dhcp Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
IPv4 Address. . . . . : 143.200.145.52(Preferred)
Subnet Mask . . . . . : 255.255.192.0
Lease Obtained. . . . . : Saturday, February 16, 2013
```

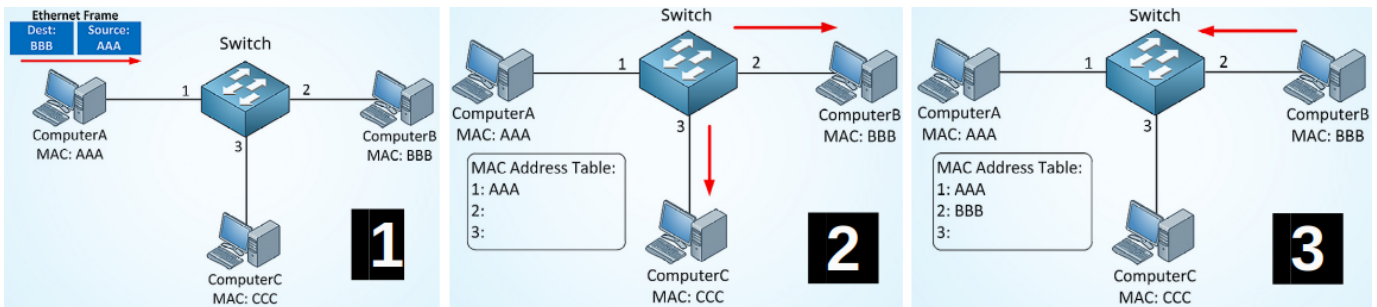
*Görsel kaynağı: <https://uknowit.uwgb.edu/page.php?id=28810/>

8.3 ARP

"Adres Çözümleme Protokolü" anlamındadır. İkinci katmanda çalışır. Ağdaki Bilgisayarların MAC adreslerini öğrenmek ve bu cihazdaki ARP tablosunu güncellemek en temel görevidir.

Ağa yeni bağlanan cihaz IP adresi henüz olmadığından yayın mesajı göndererek IP adresi ister. Anahtarlarda tutulan IP ve MAC adreslerinin tablosuna "ARP tablosu" denir. ARP Tablosu dinamik olarak güncellenir ancak istenirse elle düzenleme ya da statik kayıt işlemi yapılabilir.

Anahtarların MAC tablosu ve ARP tablosunu nasıl güncellediği aşağıdaki görselde görülmektedir.



Görsel kaynağı: <https://community.fs.com/article/switch-mac-address-whats-it-and-how-does-it-work.html>

Soru

ARP tablosunda "statik kayıt ekleme özelliği" ne işe yarar?

8.4 Yayın Adresi (Broadcast Address)

Tüm yerel ağı temsil eden adrese **yayın adresi** denir. Bu adrese gönderilen veri, ağdaki tüm cihazlara aynı anda ulaştırılır. İkinci veya üçüncü katmanda yayın mesajı gönderilebilir.

İkinci katmanda yayın adresi göndermek için çerçevedeki hedef MAC adresi kısmında tüm bitler 1 yapılır. Dolayısıyla hedef adresi FF:FF:FF:FF:FF:FF olmuş olur.

Üçüncü katmanda yayın mesajı gönderebilmek için, hedef IP adresi kısmına o ağın son (en büyük) IP adresi yazılmalıdır. Üçüncü katmandaki yayın mesajları, sonraki bölümde detaylı incelenecektir.

8.5 Yayın Alanı

Bir yayın paketi gönderildiğinde, bunu alabilen tüm cihazlar aynı yayın alanındadır. Yayın alanı içindeki bilgisayarlar ikinci katmanda MAC adresleriyle haberleşebilirler. **Bu bilgisayarlar aynı ağıdadır.**

Yayın alanı, ağ geçidinde biter

Bir bilgisayar kendi yayın alanında olmayan başka bir bilgisayarla haberleşmek için "ağ geçidinden" geçmek zorundadır.

8.6 Çarpışma (çakışma) Alanı

Aynı çarpışma alanındaki bilgisayarlar birbirine gelen her paketi görürler, ancak sadece kendi MAC adreslerine gelen her paketi işleme alırlar. Bir yayın alanı içerisinde bir veya birden fazla çarpışma alanı bulunabilir. Çarpışma alanı aynı anda sadece bir PC tarafından kullanılabilir. İki PC aynı anda veri göndermek isterse çarpışma(collision) oluşur. Adını buradan alır.

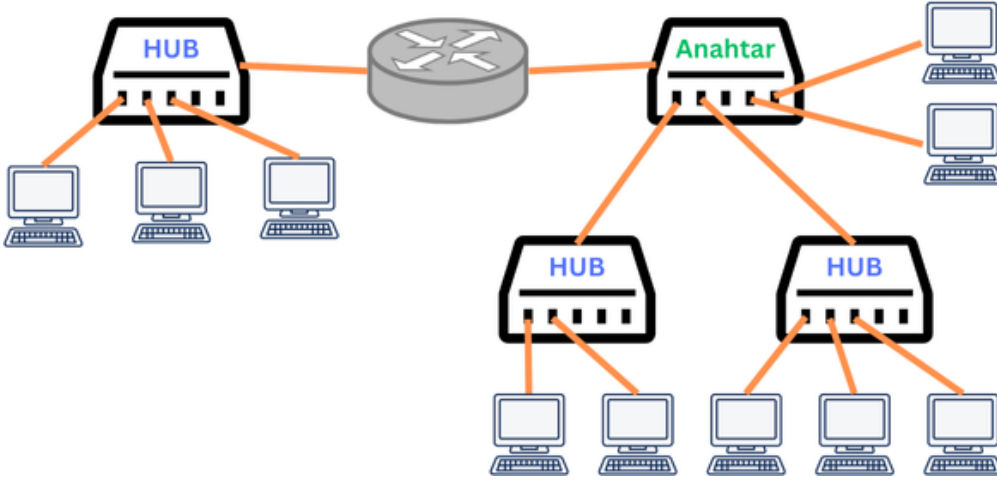
Çarpışma alanı

Çarpışma alanı istenmeyen bir durumdur. HUB'lar çarpışma alanına sebep olur.

8.6.1 Örnek 1

Aşağıdaki soruları görsele göre cevaplayın:

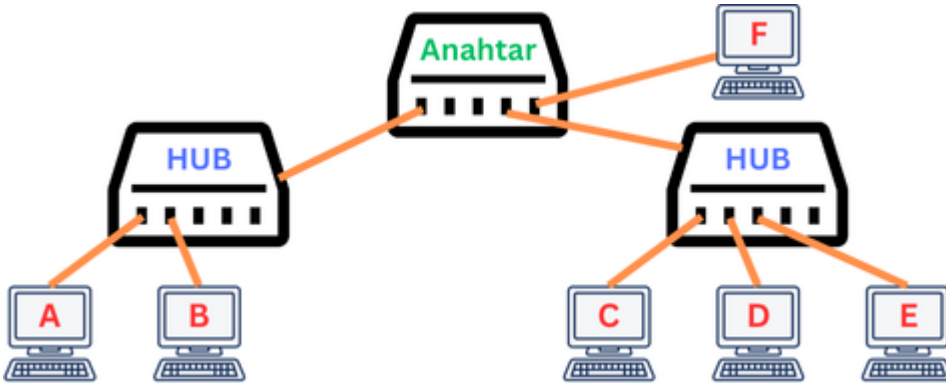
1. Kaç tane yayın alanı vardır?
2. Kaç tane çarpışma alanı vardır?
3. Her çarpışma alanında kaç tane bilgisayar vardır?
4. Her yayın alanında kaç tane bilgisayar vardır?



8.6.2 Örnek 2

Aşağıdaki soruları görsele göre cevaplayın:

1. A ile B aynı anda veri gönderebilir mi?
2. B ile C aynı anda veri gönderebilir mi?
3. C yayın mesajı gönderdiğinde tüm PC'lere gider mi?
4. B ile C aynı arasındaki trafiği E görür mü?
5. B ile C aynı arasındaki trafiği F görür mü?



8.7 Anahtarların Kapasitesi

Anahtar üzerinde pc'lerin haricinde dış dünya ile iletişim kurmak için bağlantı yapılan porta "**uplink**" portu denir. Anahtarın bilgisayara bağlanan normal portlarına "**access port**" denir. Bazı anahtarların tüm portları aynı kapasitede iken, bazı anahtarlarda ise uplink portları daha yüksek kapasiteli olur.

Anahtarın aynı anda çevirebileceği trafik miktarına "**backplane kapasitesi**" ya da "**anahtarlama kapasitesi** (switching capacity)" denir.

Bir anahtarın veri iletim performansını belirleyen en önemli faktörlerden biri de "**throughput**" olup, anahtarın belirli bir süre içinde iletebileceği maksimum veri miktarını ifade eder.

8.8 Ağ Geçidi (gateway)

Bir ağdaki bilgisayarlar, kendi ağı dışındaki ağlara gidebilmek için ağ geçidinden geçmek zorundadır. Başka bir deyişle; "ağ geçidi, bir ağın dışarı açılan kapısıdır". Sıradan bir PC, 3.katman(L3) anahtar, yönlendirici veya özel üretilmiş donanımlar ağ

geçidi görevi yapabilir. Hatta cep telefonumuzun internet bağlantısını bilgisayarımıza paylaştığımızda, cep telefonumuz, bilgisayar için bir "ağ geçidi" olmaktadır.

Bazı ağ geçitleri, üzerindeki ağ arayüzüne(interface) bağlı olarak ethernet, Frame Relay, ATM, PPPoE gibi protokolleri kullanılabilmek üzere özelliğine sahip olduğundan bazı kaynaklarda *protokol çevirici* olarak adlandırılır.

Önceden bahsedildiği gibi, anahtarlar çarpışma alanını geçirmezler ancak yayın trafiğini geçirirler. İçerisinde çok fazla bilgisayar bulunan yerel ağlarda yayın paketlerin çokluğu, ağı hantallaştırabilir. Bu nedenle LAN'ları birden fazla alt ağlara bölmek performansı arttıracaktır.

Örnek yayın mesajları:

- IPV4 - IPV6 keşif mesajları
- Komşuluk mesajları
- Donanım keşif mesajları
- IP alma (DHCP) mesajları
- Virüs (solucan) gibi kötü yazılımlar

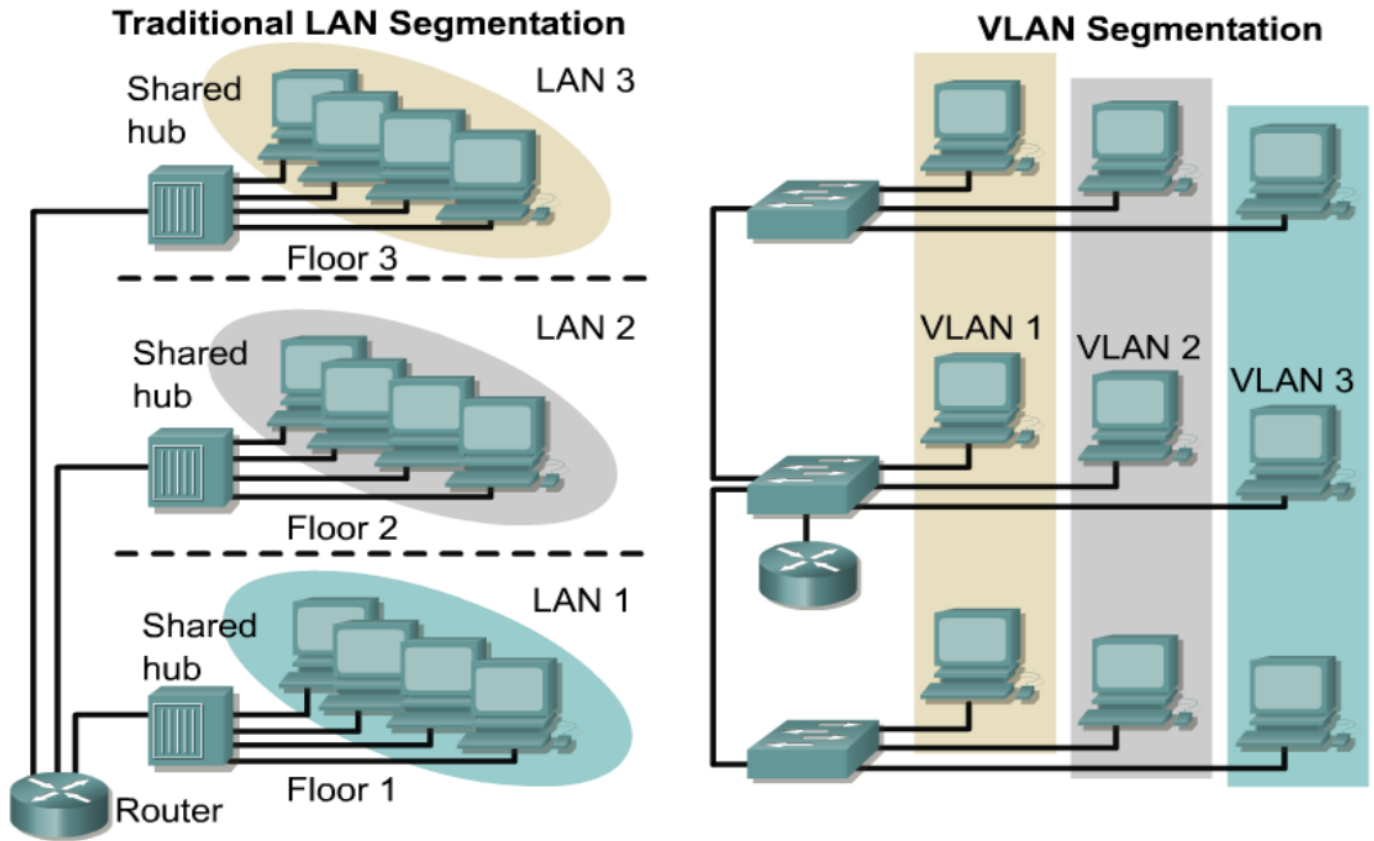
8.9 Ağları bölmenin faydaları

1. **İşletme Kolaylığı:** Ağlar küçük olduğunda sorunu çözmek kolaylaşır. Ağ isimleri, IP grupları ve kullanım yerleri eşleştirilerek hiyerarşik sistemler oluşturulabilir.
2. **PC sayısını azaltmak:** Her bir ağdaki PC sayısını azaltarak yayın alanını daraltmak, fazlalık yayın mesajlarını azaltmak ve performansı arttırmak
3. **Güvenlik:** Birbirine erişimi kısıtlanması gereken ağlar arasında erişim denetim listeleri (Access Control List ~ ACL) oluşturularak erişim kısıtlanabilir.

8.10 Alt Ağa Bölme Yöntemleri

Klasik yöntemde her bir ağ için bir fiziksel bir ağ geçidi kullanılması zorunludur. Dolayısıyla cihazların ve iletim ortamlarının sınırları en önemli kısıtlardır.

Bir **VLAN yapısında** ise fiziksel bir müdahale olmadan, hatta uzaktan bağlanarak ağ istenilen şekilde özelleştirilebilir.



Görsel kaynağı: <https://www.ws.afnog.org/afnog2011/sie/250-vlans/vlans.pdf>

VLAN (Sanal ağ) kullanmanın avantajları

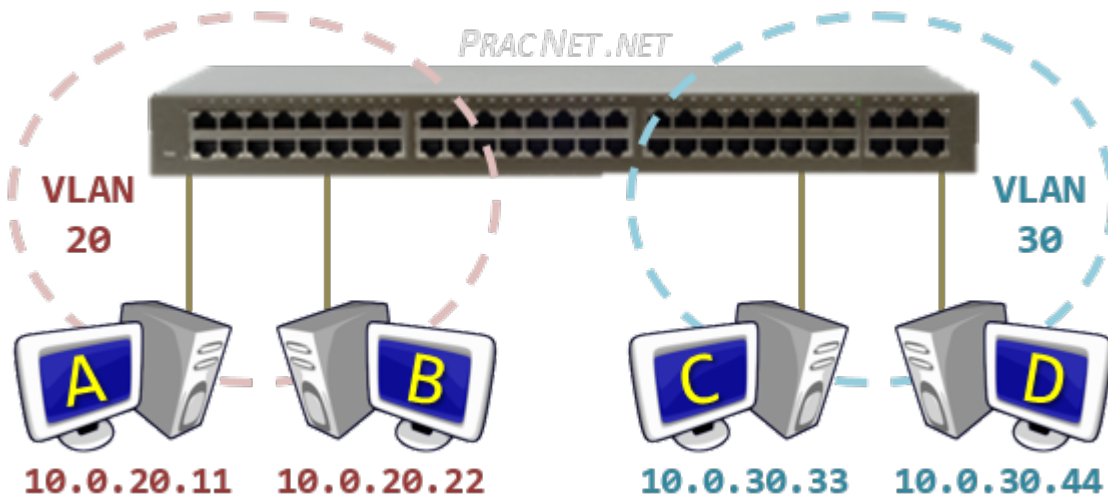
- Farklı anahtarlar üzerindeki bilgisayarlar aynı ağda olabilir.
- Aynı anahtarda birden fazla farklı ağ (VLAN) olabilir.
- Ağlarda değişiklik yapmak için fiziksel değişiklik yapmaya gerek yoktur. Uzaktan dahi kolayca yapılabilir.

VLAN'lar ve yönlendirme

Görsel kaynağı: <https://www.ws.afnog.org/afnog2011/sie/250-vlans/vlans.pdf>

8.11 VLAN Anahtarlar

Üzerinde sanal ağlar tanımlanabilen anahtarlardır. Aynı zamanda ayarlanabilir anahtarlardır. Bu nedenle yönetilebilir anahtarlar da denmektedir. VLAN anahtarın üzerindeki portlar gruplandırılarak birden çok sanal ağ oluşturulabilir.



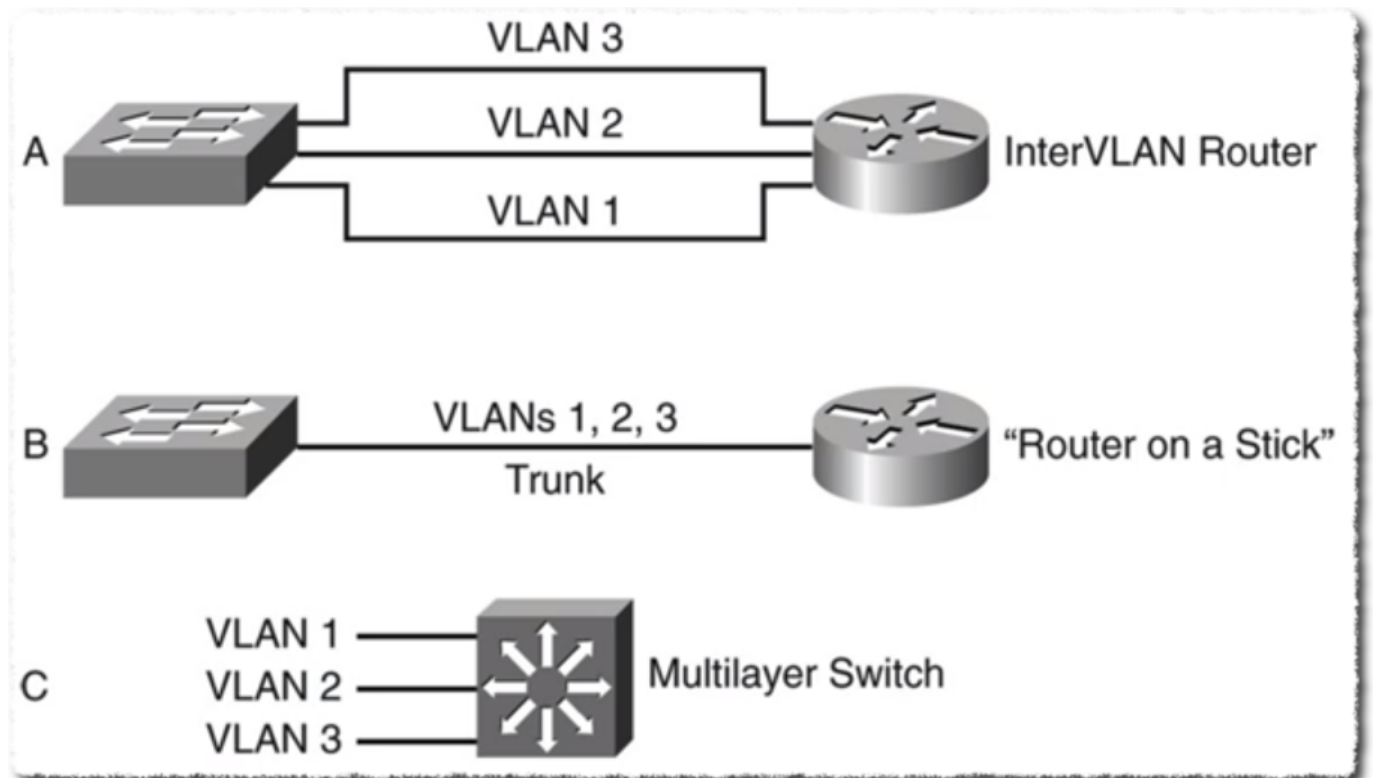
Görsel kaynağı: <https://www.practicalnetworking.net/stand-alone/routing-between-vlans/>

Her bir sanal anahtar, ayrı bir ağ gibi çalıştırılabilir. Bu sanal ağlara "VLAN" (Virtual LAN ~ Sanal Ağ) denir. Her bir VLAN'ın kendine özel VLAN-ID isminde bir tanımlayıcı numarası olur. Anahtarların fiziksel portları, VLAN ID'ler ile eşleştirilerek ağlar düzenlenir.

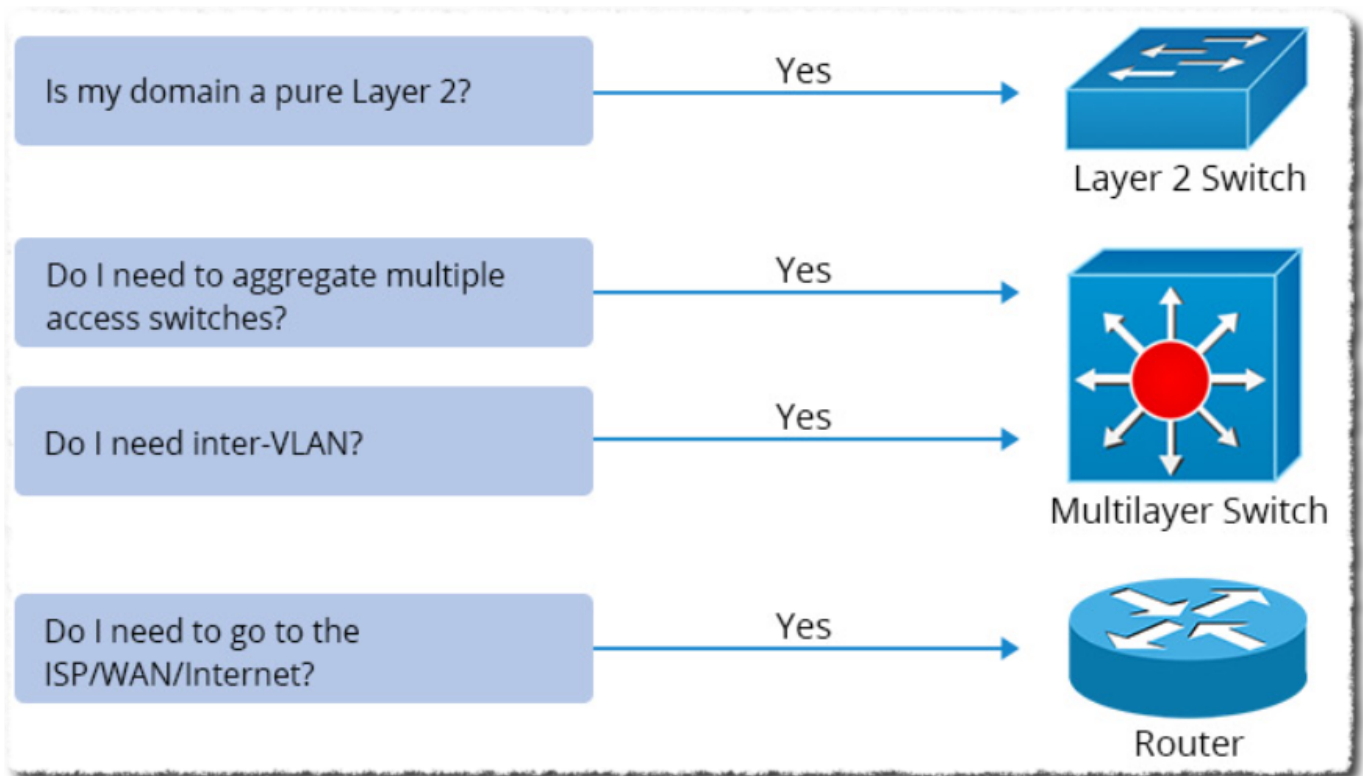
Info

Aynı VLAN numarasına sahip portlar aynı sanal ağa aittir.

Bazı durumlarda VLAN yapılandırılması portlardan ve fiziksel bağlantılardan bağımsız olarak yapılabilir. Örneğin PC'nin MAC adreslerine göre, protokole göre (IP telefon gibi), kullanıcı kimlik doğrulama yöntemine göre (parola, parmak izi, vb.) VLAN ataması yapılabilir. VLAN anahtarlar üzerinde birden fazla sanal ağ oluşturulursa bu alt ağlar arasında trafiğin yönlendirilmesi gerekmektedir. Bu yönlendirme işlemi anahtarın kendi üzerinde veya ayrı bir yönlendirici cihazla yapmak mümkündür.

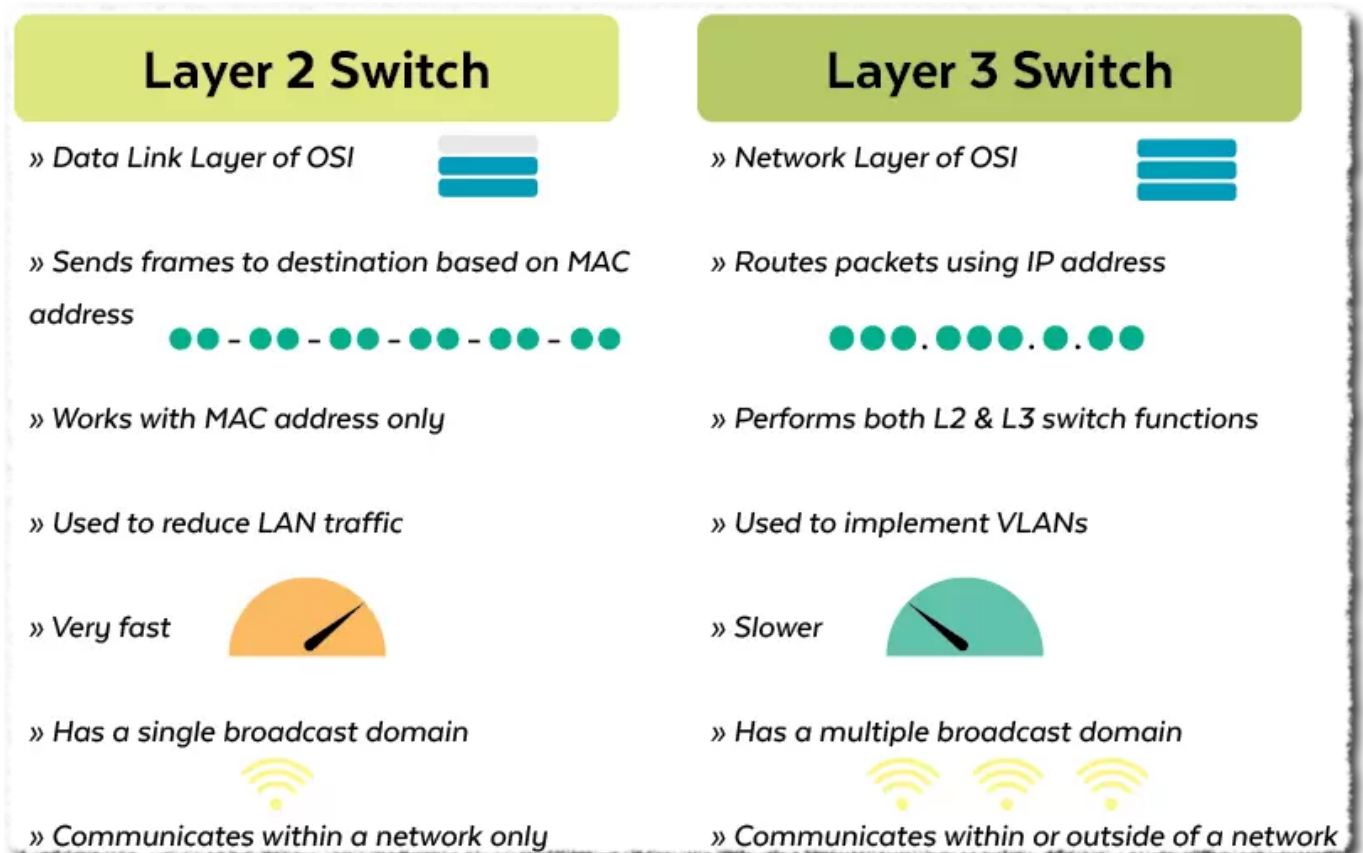


Görsel kaynağı: <https://www.youtube.com/watch?v=SPloasxkMQ>



Görsel kaynağı: <https://www.qsfptek.com/qt-news/how-to-choose-best-aggregation-switch.html>

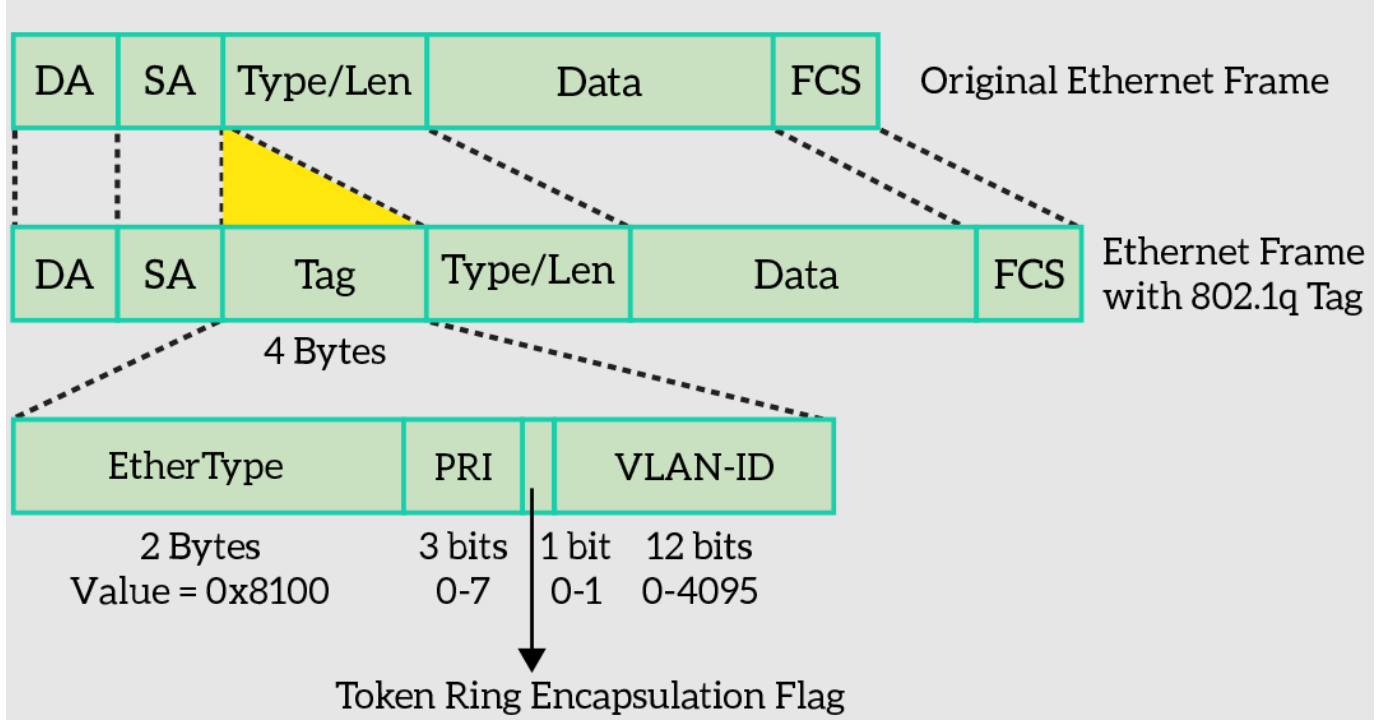
Anahtar üzerinde yönlendirme yapılacaksa 3 katmanda(L3) çakıştırılacak bir anahtar kullanılmalıdır.



*Görsel kaynağı: <https://planetechusa.com/layer-2-vs-layer-3-switches>

8.12 IEEE 802.1Q VLAN protokolü

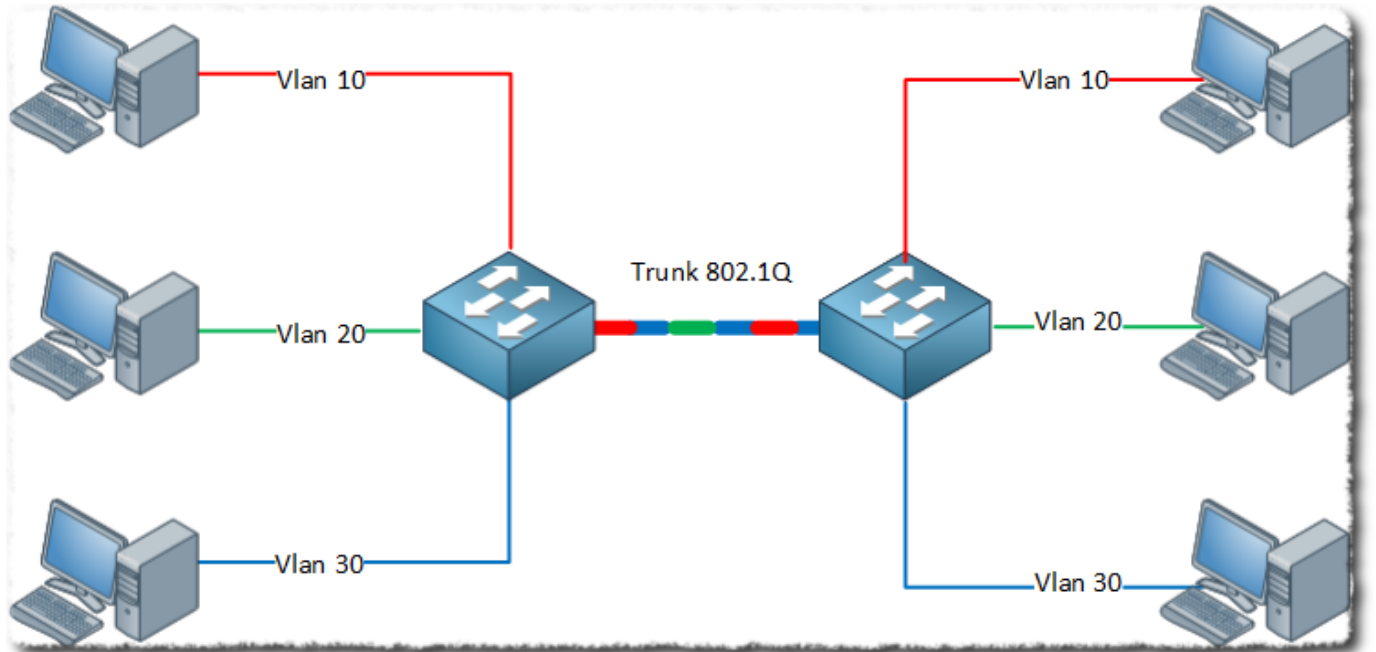
Dot1q olarak ta bilinir. Ethernet protokolü ilk tasarlandığında VLAN ihtiyacı yoktu. 1998 yılında yayınlanan 802.1q protokolü ile Ethernet protokolü VLAN farkındalığı kazandı.



Görsel kaynağı: <https://www.ictshore.com/free-ccna-course/vlans-configuration-cisco-switch/>

trunk (tagged) port: Anahtarın herhangi bir portundan birden fazla VLAN taşınması gerekiyorsa o port trunk olarak yapılandırılmalıdır. Aynı zamanda bu bağlantıya da "trunk" denir. Genellikle iki anahtar arasında kullanılır ancak ihtiyaca göre 1 bilgisayara bile trunk bağlantı verilebilir. Anahtarlar, bu portta gelen-giden trafiklere bakarak başlık bilgisindeki trafiğin ilgili VLAN'a gitmesini sağlar.

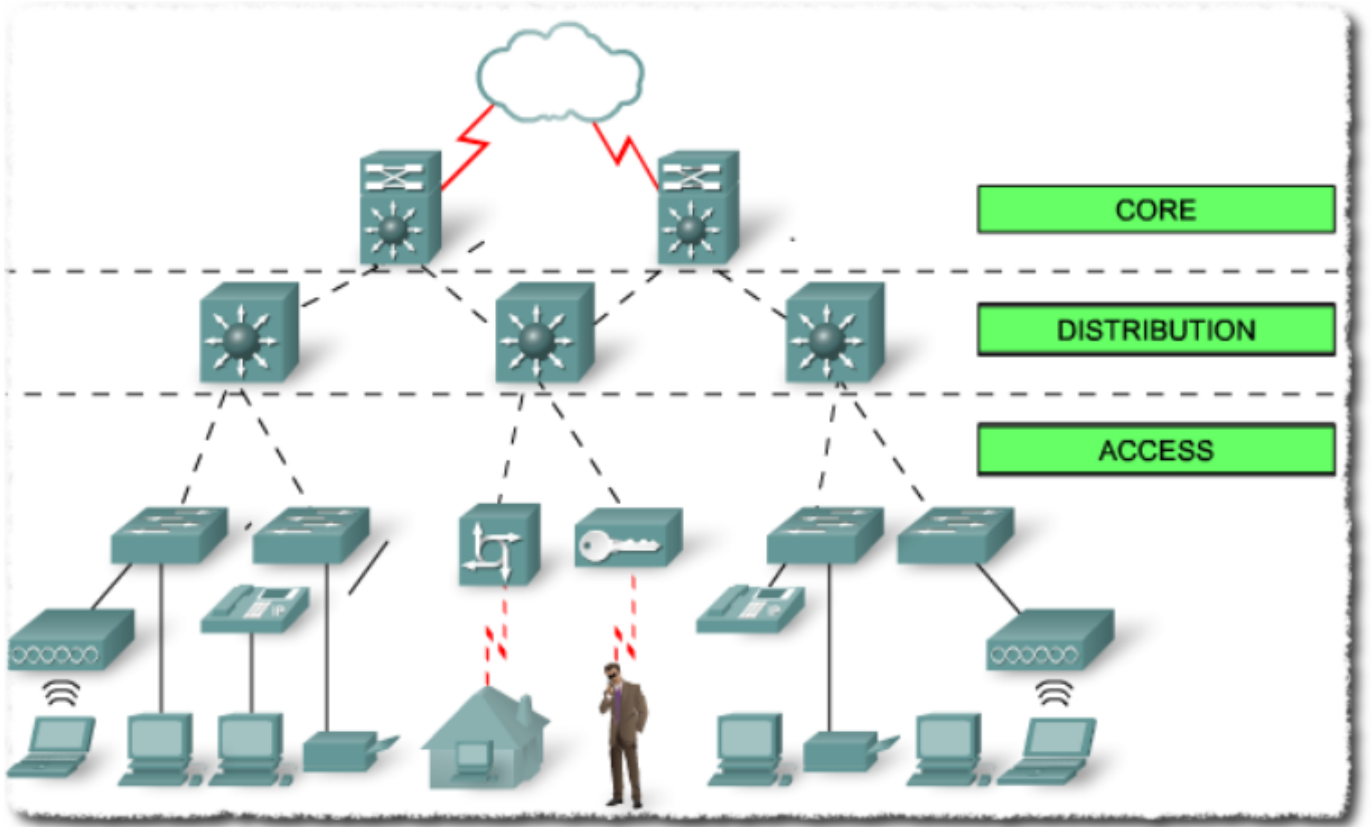
access (untagged) port: Bu portta VLAN etiketleri olmaz. Anahtar üzerinde config yapılarak, bu porttan gelen-giden tüm trafiğin belirli bir VLAN'a gitmesi sağlanır.



Görsel kaynağı: <https://networklessons.com/switching/802-1q-encapsulation-explained>

Cisco firması `trunk/access` sözcüklerini kullanırken diğer üreticiler genellikle `tagged/untagged` sözcüklerini tercih etmektedir.

8.13 Anahtar Kullanım Mimarisi



Görsel kaynağı: <https://blog.router-switch.com/2014/04/network-design-with-examples-core-and-distribution/>

1. OMURGA(CORE)

Üçüncü katman veya daha üstü anahtar kullanılır.Genellikle tüm VLANlar burada oluşturulur.Ağın tüm yönlendirme yükü bunun üzerindedir.Bu nedenle genellikle yedekli kullanılır.Performansı çok fazladır.Binalar arası bağlantıyı sağlamak için kullanılır.Bu nedenle çok sayıda fiberoptik port sergilerler.Modüler yapıdadırlar,yani port sayıları ve türleri modüler halinde takılıp çıkartılabilir. Modüllerin takıldığı yere "şase" denir.Fiziksel olarak çok yer kaplarlar ve pahalıdırlar.



Görsel kaynağı: <https://thenetworkinstallers.com/blog/fiber-optic-installation-process/>

2. Dağıtım(Distribution)Katmanı

Omurga anahtarında bağlı olan ve binaların içerisinde küçük bir omurga gibi düşünebileceğimiz anahtarlardır. Omurga anahtarına göre daha ucuzdur.L2 veya L3 olabilir.

3. KENAR

Son kullanıcı cihazlarının bağlandığı anahtarlardır. Bu nedenle özel görevleri olabilir. İhtiyaca göre:

4. 802.1x(Kimlik Doğrulama)
5. PoE(802.3aaf) Enerji göndermek için kullanılır.
6. Güvenlik (port-security, DHCP koruması, vb.)

	Access	Distribution	Core
Bandwidth aggregation	✓	✓	✓
Fast Ethernet/Gigabit Ethernet	✓		
Gigabit Ethernet/10 Gigabit Ethernet		✓	✓
High forwarding rate		✓	✓
Layer-3 Support		✓	✓
Port security	✓		
Power over Ethernet (PoE)	✓		
Quality of Service (QoS)	✓	✓	✓
Redundant components		✓	✓
Security Policies/Access Control Lists		✓	
Very High forwarding rate			✓
VLANs	✓		

Görsel kaynağı: <https://blog.router-switch.com/2014/04/network-design-with-examples-core-and-distribution/>

8.13.1 Örnek 3

20 portlu bir VLAN anahtar, 4 portlu bir ağ geçidine bağlanıyor. Aşağıdaki durumları yorumlayınız.

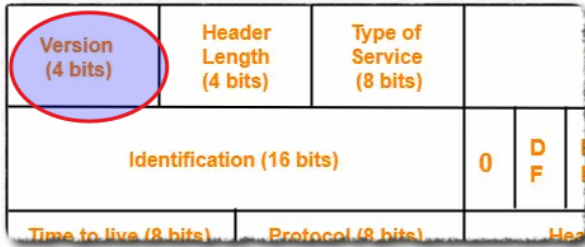
1. Her VLAN'daki port sayısı 5'er tanedir.
2. Bu VLAN anahtar üzerine doğrudan bağlanacak PC sayısı 16'dır.
3. Her VLAN'a atanmış portlar ardışık olmak zorundadır.

9. İnternet'in Protokolü: IP

Bu bölümdeki içeriği anlattığım bir video var. Alt ağlara bölme konusuna kadar anlatmıştım. İsteyenler videodan da faydalanabilir: <https://www.youtube.com/embed/e9-1U0aXz1g>

I

9.1 Genel Bilgiler



IPv4 adresleri tükendiği için, artık IPv6 adresleri dağıtılmaktadır. Uzunca bir süre daha ikisini birlikte kullanmak zorundayız.

IPv4 adresleme sisteminde (2^{32}) IP adresi kullanılabilirken, IPv6 adreslemesinde (2^{128}) adet IP adresi kullanılabilir. Aşağıda bu iki sayı açık olarak yazılmıştır:

- **IPv4 adres sayısı:** $(4.294.967.296)$ (yaklaşık 4,3 milyar)
- **IPv6 adres sayısı:** $(340.282.366.920.938.463.463.374.607.431.768.211.456)$

Bu ders içerisinde IP ifadesi her kullanıldığında, IPv4 anlaşılmalıdır. Bu ders açısından ikisi arasındaki en önemli fark; birisinin 32, diğerinin ise 128 bit olmasıdır. IP hesaplamaları tamamen aynıdır. Hesap mantığını anlamak için v4 hesapları -kısa olduğu için- daha iyi olacaktır. Sonrasında aynı hesapları v6'da da yapabilirsiniz.

9.1.1 IANA: IP Dağıtan Kuruluş

<https://www.iana.org/> web sitesinde faaliyetleri hakkında bilgi alınabilir.



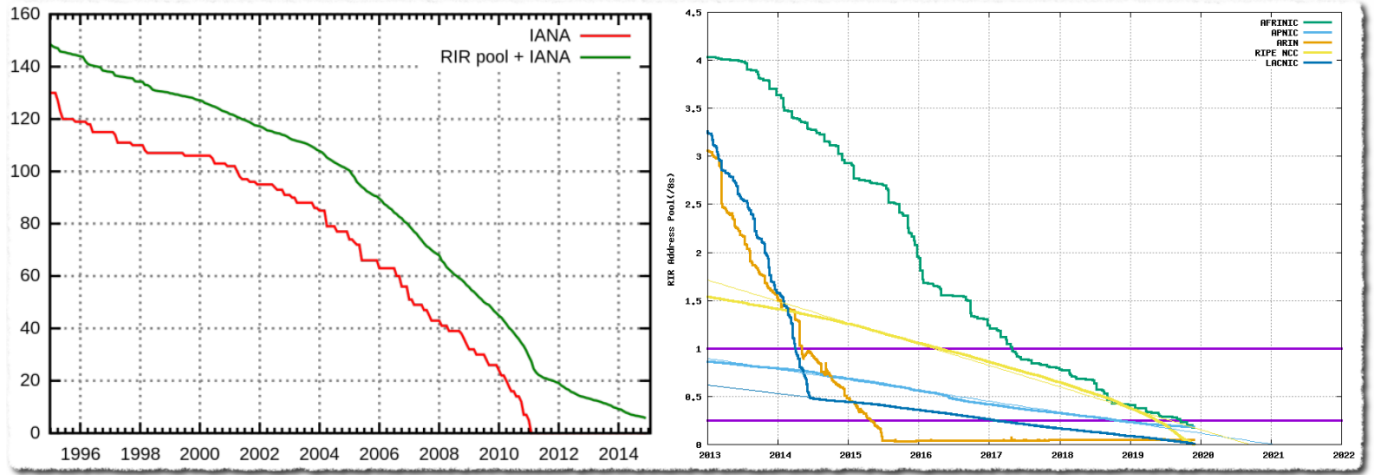
IANA tarafından yetkilendirilen bölgesel internet kayıtçıları (RIR)

IANA, IP adreslerini /8 şeklinde RIR'lara dağıttı.

Prefix	Designation	Date	WHOIS
000/8	IANA - Local Identification	1981-09	
001/8	APNIC	2010-01	whois.apnic.net
002/8	RIPE NCC	2009-09	whois.ripe.net
003/8	Administered by ARIN	1994-05	whois.arin.net
004/8	Administered by ARIN	1992-12	whois.arin.net

Görsel kaynağı: <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>

IANA elindeki tüm IPv4 adresleri 2011'de bitti.



Görsel kaynağı: https://en.wikipedia.org/wiki/IPv4_address_exhaustion

9.1.2 IP Sınıfları

IP'nin ilk tasarlandığı sıralarda ortaya çıkmış bir kavramdır. Kurumlarda IP adresleri tahsis edilirken ihtiyaca göre optimal sayıda IP adresi verebilmek için tasarlanmıştır. En büyük IP sınıfı A sınıfı olanlar, en küçük IP sınıfı da C sınıfı olanlardır.

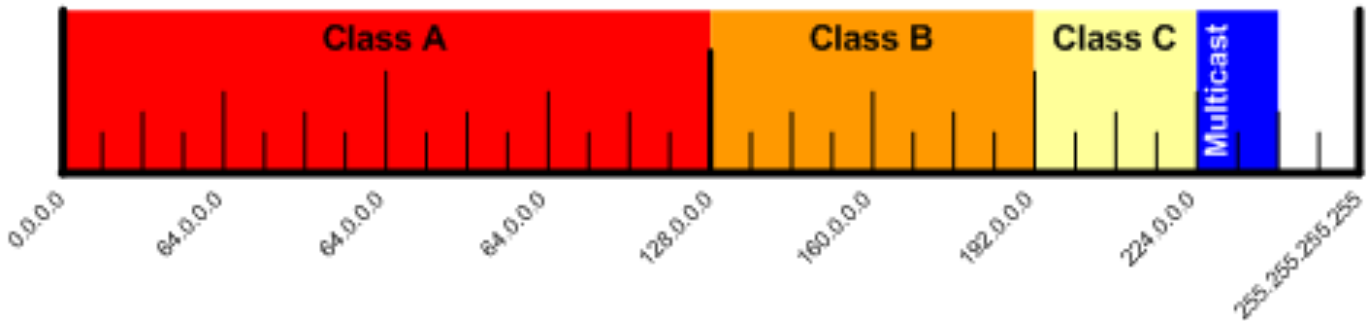
Cancel bilgi

Günümüzde IP sınıfları bu anlamın yanında, ağın büyüklüğünü ifade etmek için kullanılmaktadır.

Five Different Classes of IPv4 Addresses

Class	First Octet decimal (range)	First Octet binary (range)	IP range	Subnet Mask	Hosts per Network ID	# of networks
Class A	0 – 127	0XXXXXXXX	0.0.0.0-127.255.255.255	255.0.0.0	$2^{24}-2$	2^7
Class B	128 – 191	10XXXXXXXX	128.0.0.0-191.255.255.255	255.255.0.0	$2^{16}-2$	2^{14}
Class C	192 – 223	110XXXXXX	192.0.0.0-223.255.255.255	255.255.255.0	2^8-2	2^{21}
Class D (Multicast)	224 – 239	1110XXXX	224.0.0.0-239.255.255.255			
Class E (Experimental)	240 – 255	1111XXXX	240.0.0.0-255.255.255.255			

Görsel kaynağı: <https://medium.com/networks-security/tricks-to-remember-five-classes-of-ipv4-484c191678fb>



Görsel kaynağı: <https://www.routerfreak.com/definitive-guide-ip-address-classes/>

Örnekler:

- **BŞEÜ:** 79.123.224.15 A sınıfı olduğu için, bu IP'nin dahil olduğu ağda (2^{24}) (~16M) tane IP olabilir.
- **ODTÜ:** 144.122.145.153 IP adresi B sınıfıdır. Bu IP'nin dahil olduğu ağda, (2^{16}) (~65K) tane IP olabilir.
- **SAÜ:** 193.140.253.240 IP adresi C sınıfıdır. Bu IP'nin dahil olduğu ağda (2^8) (256) tane IP olabilir.

IP sınıflarının günümüzdeki anlamı

İlk başta IP adresleri dağıtılırken kolaylık olsun diye tasarlanmış olan IP sınıfları günümüzde bu anlamda kullanılmamaktadır. BŞEÜ'de 16M IP adresi yoktur. SAÜ'de de C sınıfından (256) daha fazla IP adresi vardır. Örneklerden sadece ODTÜ'nünki gerçekten B sınıfı olarak (~65K) tahsis edilmiştir.

9.2 Rezerve IP Adresleri

IETF ve IANA tarafından, özel amaçlar için kullanılmak üzere farklı adres blokları ayrılmıştır. En temel olarak; **özel** ve **genel** IP adresleri şeklinde bir ayrım yapılmıştır. İç ağda özel IP adresine sahip olan bilgisayarlar, İnternet'e çıkarken genel IP adresi kullanırlar.

Bunların dışında da farklı amaçlarla ayrılmış adres aralıkları bulunmaktadır. Aşağıda ayrılmış olan bu adresler kısaca açıklanmıştır.

9.2.1 Özel ve genel IP Adresleri (Private & public IP Blocks)

Özel (private) IP adresleri, İnternet'te kullanılmayan IP adresleridir. Bu nedenle *sanal IP adresi* de denir. İnternet üzerinde hiçbir yönlendirici tarafından iletilmezler. Bu adreslerin kullanım amacı, test uygulamaları ve NAT uygulamaları gibi durumlardır. Aşağıdaki tabloda özel IP adres aralıkları verilmiştir. Bunların dışındaki adresler, genel (public) IP adresidir.

CIDR gösterimi	Adres aralığı	IP sayısı
/8	10.0.0.0 - 10.255.255.255	16.777.216
/12	172.16.0.0 - 172.31.255.255	1.048.576
/16	192.168.0.0 - 192.168.255.255	65.536

9.2.2 Diğer ayrılmış IP adres aralıkları

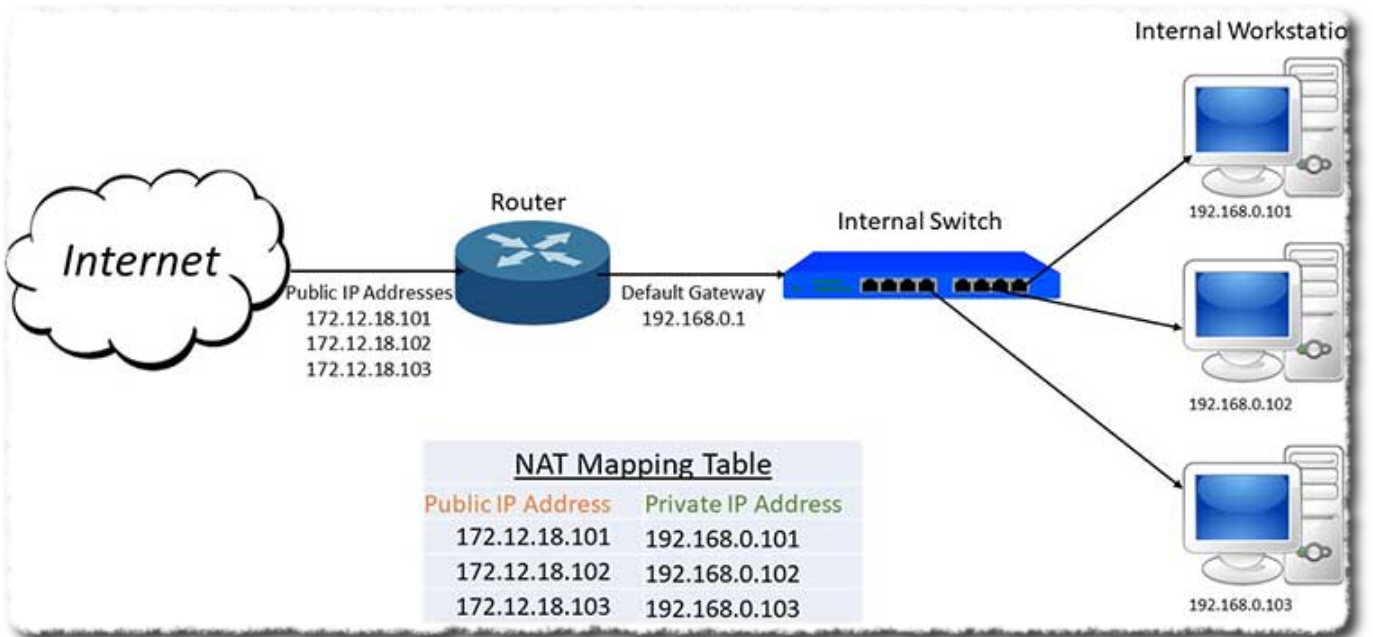
Adres bloğu	Adres aralığı	Adres sayısı	Açıklama
0.0.0.0/8	0.0.0.0 - 0.255.255.255	16.777.216	Ağın kendisi ("Bu" ağ)
127.0.0.0/8	127.0.0.0 - 127.255.255.255	16.777.216	Loopback (localhost)
169.254.0.0/16	169.254.0.0 - 169.254.255.255	65.536	Link-local

Loopback adresi: Bilgisayarın kendisini temsil eder. Paketler bilgisayardan cihazdan asla ayrılmazlar. Bilgisayarın kendi üzerinde çalıştırılan uygulamalar için kullanılır. Test amacıyla da kullanılabilir.

IPv4 için, 127.0.0.0/8 A sınıfı adres bloğunun tamamı loopback için ayrılmıştır. IPv6'da ise bu amaçla sadece ::1 adresi kullanılır.

Link-local adresler: DHCP vasıtasıyla otomatik IP almak üzere yapılandırılmış ağlarda, bir IP adresi alamayan bilgisayarlar bu bloktan kendi kendine bir IP adresi verirler. Eğer bir bilgisayarda 169.254.x.x şeklinde bir IP adresi görürseniz, "bu bilgisayar IP alamamış" denir. Eğer DHCP sisteminde bir sorun olursa, link-local adresler sayesinde aynı ağdaki (LAN) bilgisayarlar kendileri arasında haberleşebilirler.

9.2.3 NAT (Network Address Translation)



Görsel kaynağı: <https://onlinecomputertips.com/support-categories/networking/601-network-address-translation-nat/>

Bir IP adresinin, diğer ağlara giderken farklı bir adrese dönüştürülmesi işlemidir. Genellikle, kurumlarda tahsis edilen az sayıda - *hatta tek*- public IP adresini, çok sayıda bilgisayarda kullanabilmek için uygulanır. IPv4'ün beklenenden erken bitmesine karşılık çözüm olarak kullanılmaktadır. IPv6'ya geçildiğinde bu işlemlere gerek kalmayacaktır.

NAT Tablosu: NAT işlemi yapılırken hangi IP adresini kimin ne zaman kullandığını tutar. Bu sayede ilgili IP'nin yaptığı isteklere gelen cevaplar doğru şekilde iletilebilir.

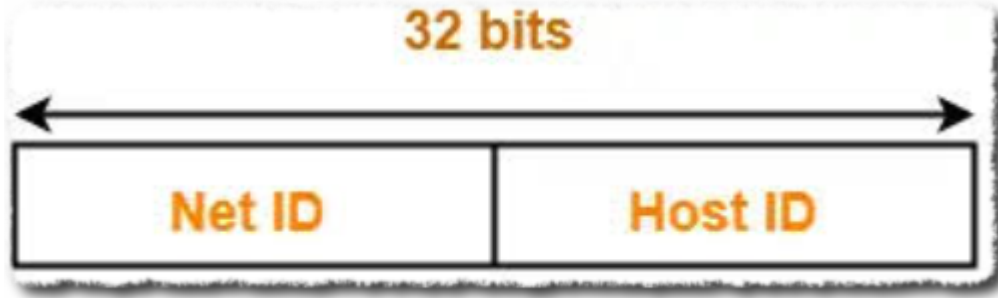
Bahçe terliği benzetmesi

Yalnızca 1 public IP adresi olan bir kurumun ağında çok sayıda bilgisayar internet'e çıkıyor olsun. Bu örneği, evin arka bahçe kapısında tek terlik bulunmasına benzetebiliriz. Bahçede işi olan kişi terliği giyer, işini halledince terliği çıkarıp eve girer. Sonra başkası aynı terliği kullanır. Bahçeyi gören komşular hep aynı terlikleri görürler ama o terlikleri kullanan kişi değişmiş olur.

9.3 IP Adresi ve Hesaplamaları

32 bit uzunluğa sahip olan IP adresi 2 temel bileşene sahiptir:

1. Ağ tanımlayıcı
2. Host tanımlayıcı

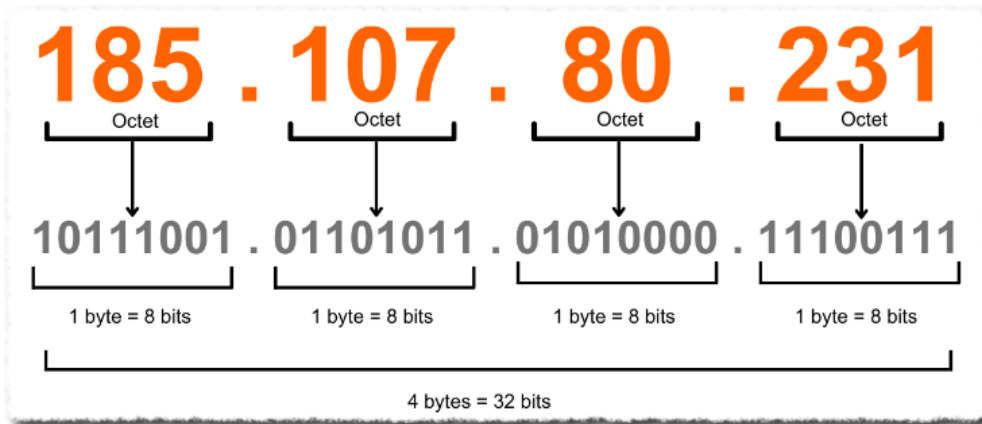


IP bileşenleri

Host

Bir ağ içerisinde IP atanabilen ve kendisinin ağa bağlanma ihtiyacı olan cihazların tümüne **host** denir. Örneğin; bilgisayar, yönlendirici, güvenlik duvarı, akıllı saat, cep telefonu, IoT cihazları, vb.

IP adresleri 32 bitin sekizerli olarak gruplandırılması ve onluk (decimal) olarak gösterilmesi şeklindedir. Bu 8 bitlik grupların her birine **oktet** denir. Her oktet birbirinden nokta ile ayrılır.



Görsel kaynağı: <https://www.cloudns.net/blog/what-is-ipv4-everything-you-need-to-know/>

Kaç bitle kaç adres?

$\backslash(N)$ tane bit kullanılarak yapılacak bir adresleme sisteminde, $\backslash(2^N)$ tane adres kullanılabilir.

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

4 bit ile $2^4=16$ tane farklı adres kullanılabilir

9.3.1 Host ve Network Kısımlarının Ayrıştırılması

Bir IP adresinde soldan itibaren ilk X tane bit ağ tanımlayıcısıdır. Geri kalan Y tane bit te host tanımlayıcısıdır. Bu durumda $\backslash(X+Y=32)$ olur.

IP address class	Address format	Address range	Network ID	Subnet mask
Class A	N H H H	0.0.0.0- 127.255.255.255	0.0.0.0- 127.0.0.0	255.0.0.0
Class B	N N H H	128.0.0.0- 191.255.255.255	128.0.0.0- 192.255.0.0	255.255.0.0
Class C	N N N H	192.0.0.0- 223.255.255.255	192.0.0.0- 223.255.255.0	255.255.255.0

Görsel kaynağı: <https://sherihansliit.blogspot.com/2012/12/understanding-ip-address-configuration.html/>

Müteahhit problemi

Metin adında bir müteahhit, bir arazi üzerinde konut projesi yapacak. Metin'e şu şartlarla izin veriliyor:

1. Toplam 16 tane adres numarası kullanabilir. Bu numaraları bina numarası veya daire numarası olarak kullanabilir.
2. Her binada zemin kat ve çatı katında kimse oturamaz.

Metin, kaç daireli kaç bina yapmalı ki; hem kârı çok azalmasın hem de müşteriler mutsuz olmasın?



Müteahhit problemi. 16 daireli tek bina mı, 8 daireli 2 bina mı, ya da?

Note

Ağlardaki bilgisayar sayıları (kullanılabilecek IP sayıları) belirlenirken maksimum kapasite 2'nin kuvveti 2^n alınarak belirlenir.

ÖRNEK : Bir şirketin iki farklı şubesinde 120 ve 280 adet bilgisayar kullanılmaktadır. Bu şirketler için optimal ağ büyüklüklerini hesaplayınız.

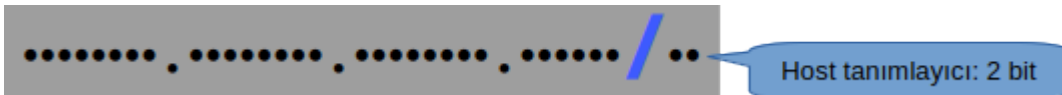
$2^0 = 1$	
$2^1 = 2$	
$2^2 = 4$	
$2^3 = 8$	
$2^4 = 16$	
$2^5 = 32$	
$2^6 = 64$	
$2^7 = 128$	120
$2^8 = 256$	
$2^9 = 512$	280
$2^{10} = 1024$	

IP sayısı ve host sayısı

Host tanımlayıcısı kısmındaki bit sayısı ile elde edilebilecek adres sayısı, o ağda kullanılabilecek IP adresi sayısıdır. Her ağın ilk IP adresi **ağ adresi** ve son IP adresi de **yayın adresi** olarak kullanıldığından, her ağda kullanılabilecek **host sayısı IP sayısından 2 eksiktir**.

- Host bitleri : (N) tane
- Ağdaki IP adresi : (2^N) tane
- Ağda kullanılabilecek host sayısı $(2^N - 2)$

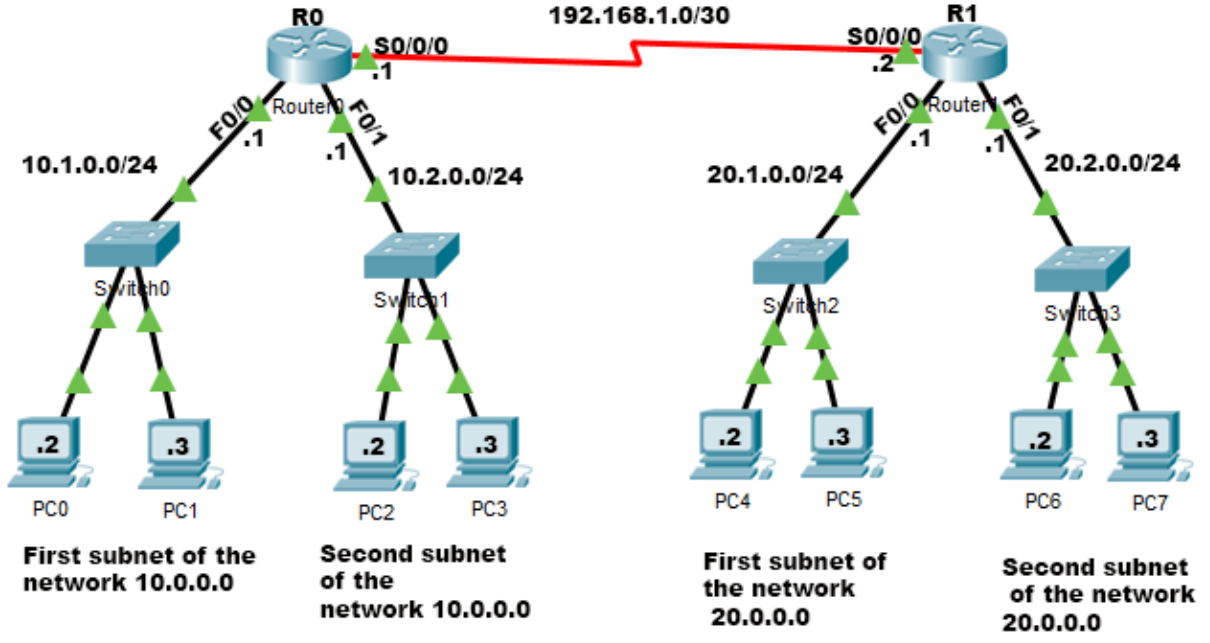
ÖRNEK : 10.9.8.0 IP adresinin 30. bitten sonra bölündüğünü varsayalım. Bu ağda kullanılabilecek bütün IP adreslerini, kullanım amacına göre yazalım.



IP sayısı = $(2^2 = 4)$ tane

Host sayısı = $(2^2 - 2 = 2)$ tane

1. IP adresi 10.9.8.0 : Ağ adresi
2. IP adresi 10.9.8.1 : Hostlar için kullanılabilir
3. IP adresi 10.9.8.2 : Hostlar için kullanılabilir
4. IP adresi 10.9.8.3 : Yayın adresi

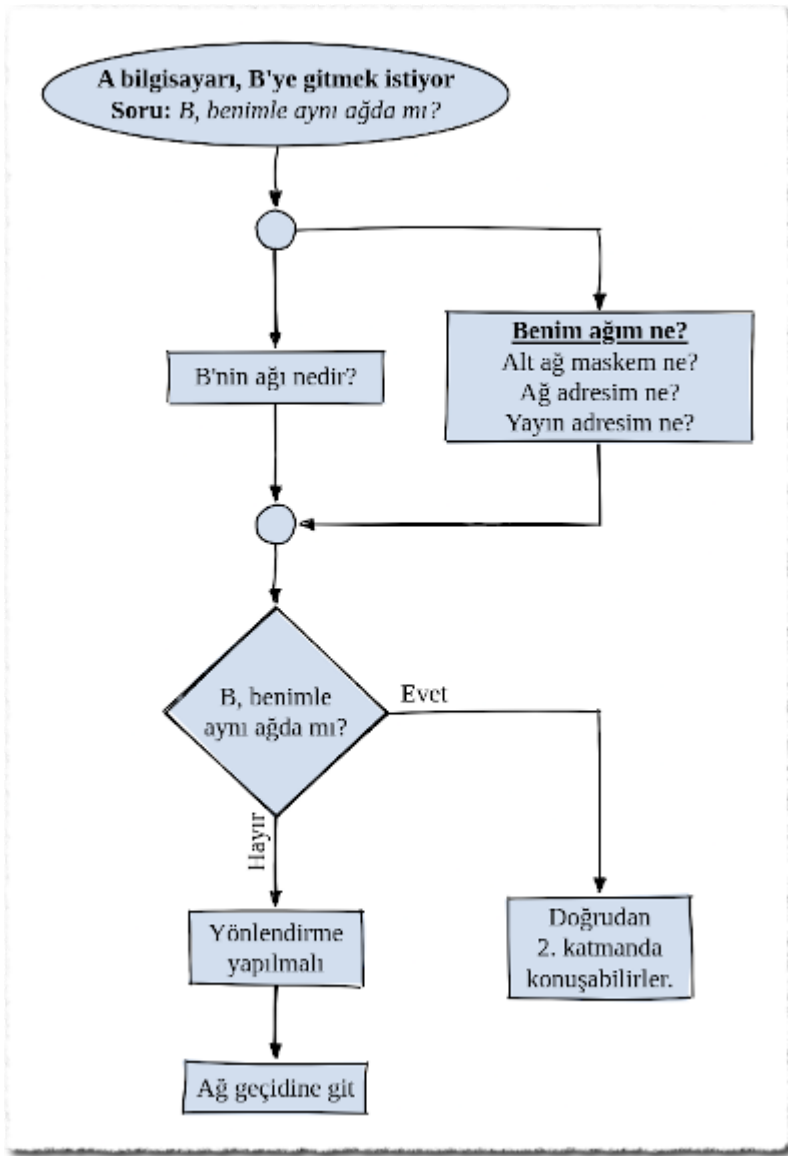


Örnek /30 ağ kullanım şekli: Dummy Network

Görsel kaynağı: <https://www.computernetworkingnotes.com/ccna-study-guide/contiguous-and-discontiguous-networks-explained.html>

9.3.2 Ağ hesapları neden yapılıyor?

Eğer iki bilgisayar aynı ağda ise doğrudan 2. katmanda (MAC adresleri ile) haberleşebilirler. Farklı ağlarda iseler mutlaka kendi ağ geçitlerine gitmeleri gerekir.



A ile B aynı ağda mı? Sorusunun cevabını arıyoruz

9.3.3 Ağ Maskesi (Netmask)

"Alt ağ maskesi" de denir Ağın kaçınıcı bitten bölündüğü belirtir. IP adresi gibi 32 bitten oluşur. İkilik sistemde soldan itibaren 1'lerle başlar, sonra 0'larla devam eder. 1'den 0'a geçilen nokta, ağın bölündüğü kısımdır. Gündelik hayatta kolay olması için, onluk sistemde kullanılır.

Ağ maskesinin temel görevleri:

1. IP adresinde, network ID ile host ID kısımlarının hangi bitlerden ayrıldığını belirlemek.
2. Ağın büyüklüğünü belirtmek
3. Ağın nerede başladığı (ağ adresi) hesabında kullanmak

Örnek bazı maskeler:

255.255.255.0	11111111.11111111.11111111.00000000
255.0.0.0	11111111.00000000.00000000.00000000



Görsel kaynağı: <https://www.bestpickreports.com/blog/post/6-painting-hacks-with-tape/>

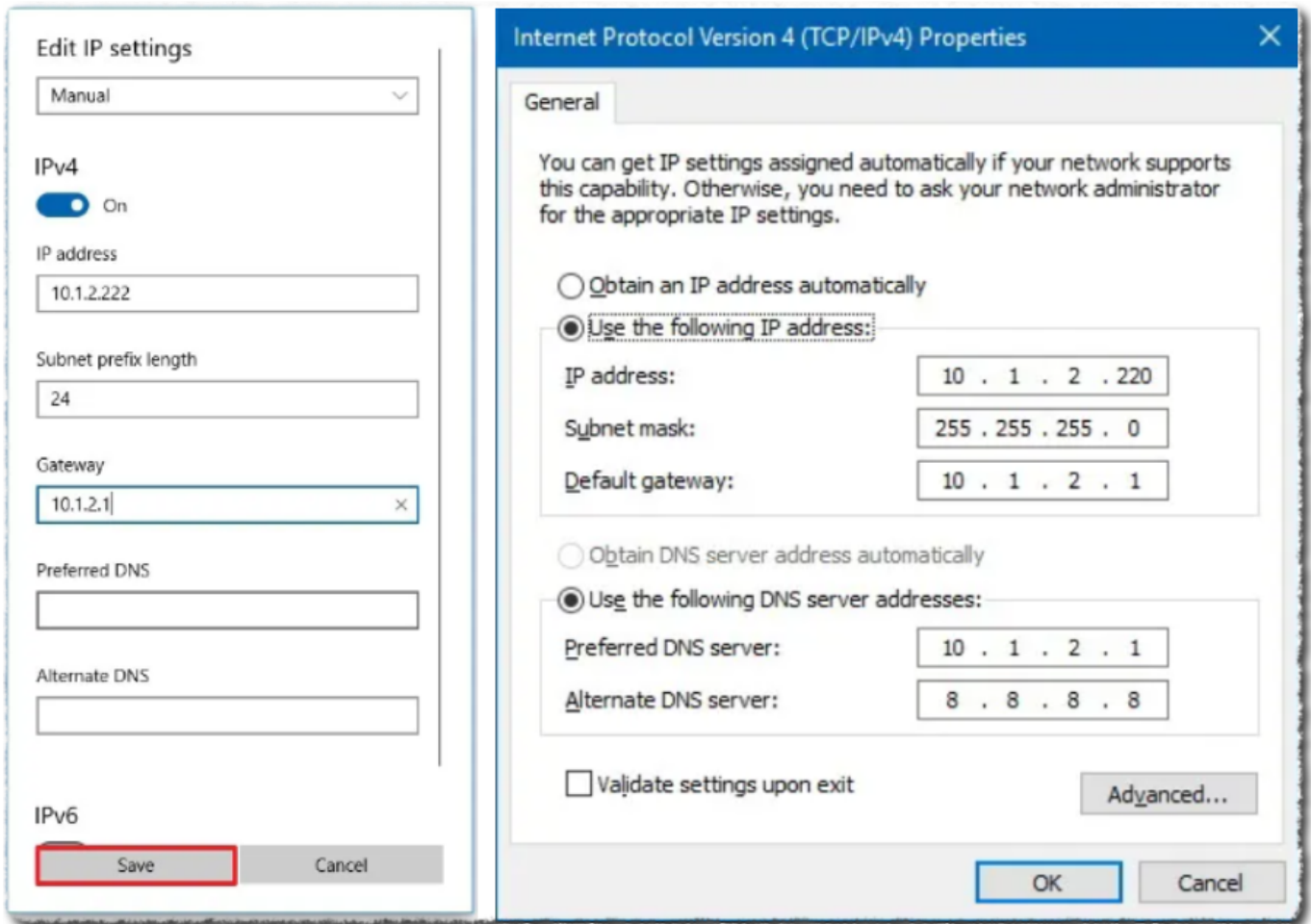
Note

IP adresi ile beraber, ağ maskesinin kullanılması zorunludur.

Netwok	Host	Host	Host
255	0	0	0

Netwok	Network	Host	Host
255	255	0	0

Netwok	Network	Network	Host
255	255	255	0



Windows'ta iki farklı yerden IP yapılandırması yapılabilir. Görsel kaynağı: <https://pureinfotech.com/set-static-ip-address-windows-10/>

Suffix	Hosts	32-Borrowed=CIDR	2^Borrowed = Hosts	Binary=> dec = Suffix
.255	1	/32	0	11111111
.254	2	/31	1	11111110
.252	4	/30	2	11111100
.248	8	/29	3	11111000
.240	16	/28	4	11110000
.224	32	/27	5	11100000
.192	64	/26	6	11000000
.128	128	/25	7	10000000

Görsel kaynağı: <https://www.trance-cat.com/electrical-circuit-calculators/en/subnet-mask-calculator.php>

9.3.4 CIDR Notasyonu

Ağ maskesine alternatif olarak CIDR Notasyonu kullanılmaktadır. Bu gösterim şeklinde, IP adresinin sağına / işareti konulup kaçınıcı bittten sonra bölündüğü bilgisi yazılır.

Örnekler:

- 192.168.1.75 IP adresli ve 255.255.255.0 ağ maskesine sahip bir cihazın CIDR notasyonu 192.168.1.75/24 şeklindedir.
- 10.1.0.0 ve 255.0.0.0 ise 10.1.0.0/8 olarak gösterilir.
- 10.9.8.0 ve 255.255.255.128 ise 10.9.8.0/25 şeklinde gösterilir. (128 ikilik tabanda 10000000 şeklinde gösterildiğinden soldan itibaren 25 tane 1, 7 tane de 0 vardır.)

9.3.5 Ağ adresi

Ağ maskesi herhangi bir IP adresi ile ikilik sistemde çarpılırsa (mantıksal VE işlemi) çıkan sonuç **ağın adresini** verir. Bu sayede, ağın nerede başladığı bulunmuş olur.



Görsel kaynağı: https://en.wikipedia.org/wiki/Mask_%28computing%29

Örnek: IP adresi 192.168.1.75 olsun. Alt ağ maskesi de 255.255.255.0 olsun. Bu ağın ağ adresini bulalım.

192.168. 1.75
X 255.255.255. 0

Onluk sistemde çarpma işlemi yapamayız

İkili sistemde yazıp çarpalım:

11000000.10101000.00000001.01001011
X 11111111.11111111.11111111.00000000

11000000.10101000.00000001.00000000

Sonucu onluk sistemde yazalım: 192.168.1.0

9.3.6 Ağ adresi ve yayın adresinin pratik hesabı

IP adresinin nereden bölündüğünü biliyorsak; **IP adresinde** bu bittten sonrası 1 yapılırsa, **yayın adresi** ni buluruz. Aynı bitleri 0 yaptığımızda ise **ağ adresi** ni buluruz.

IP adresi: 192.168.1.75
 Ağ maskesi: 255.255.255.0

24. bitten bölünmüş

IP adresini ikilik sistemde yazalım:
 11000000.10101000.00000001.01001011

24. bitten sonrasını 0 yaparsak:
 11000000.10101000.00000001.00000000
 Ağ adresi: 192.168.1.0

24. bitten sonrasını 1 yaparsak:
 11000000.10101000.00000001.11111111
 Yayın adresi: 192.168.1.255

9.3.7 IP hesaplarında formüller ve özet

- IP (v4) adresleri \ (32\ bitten oluşur.** Bu bitler sekizer gruplu (oktet) olarak yazılır ve okunur. Örnek: 10.170.265.44 . IP adresinin her oktetinde 8 bit bulunduğundan, hiç bir oktet 255'ten büyük olamaz. Yani az önce verdiğim IP adresi, bozuk bir IP adresidir.
- IP adresindeki \ (32\ bitin soldan itibaren \ (M\ tanesi ağı tanımlar. geri kalan \ (N\ tanesi de \ (N=32-M\)) hostları tanımlar. Bu iki bileşeni birbirinden ayırmanın iki yolu vardır:
 - CIDR** gösteriminde bölü işareti ("/") kullanılır. örnek: 10.5.0.100/16
 - Maske** ile gösteriminde M tane 1, N tane 0 olacak şekilde bitler ifade edilir. Sonra 10'luk sisteme çevrilerek IP adresinin yanına yazılır. Örnek: 10.5.0.100 - 255.255.0.0
- Bir **ağda kaç IP** olduğunu bulmak için, bölü işaretinden sonraki bitlerin sayısına bakılır. \ (N\ tane bit varsa, \ (2^N\ formülü ile ağdaki IP sayısı hesaplanır.
- Ağları alt ağlara bölmeye başlamadan önce mutlaka mevcut ağı tanımla. Nerede başlar? Nerede biter? Maskesi nedir? CIDR gösterimi nedir? Bu ağda kaç IP vardır?
- Bir ağın **alt ağ maskesini** bulmak için;
 - IP adresinde, bölü'den önceki bitlerin tamamı 1 yapılır.
 - IP adresinde, bölü'den sonraki bitlerin tamamı 0 yapılır.
 - Sonra 10'luk sisteme çevrilir.
- Bir ağın **ağ adresini** bulmak için;
 - IP adresinde bölü'den sonraki bitlerin tamamı 0 yapılır. Sonra 10'luk sisteme çevrilir.
- Bir ağın **yayın adresini** bulmak için;
 - IP adresinde bölü'den sonraki bitlerin tamamı 1 yapılır. Sonra 10'luk sisteme çevrilir.
- \ (N\ şeklinde verilen bir ağı 2 alt ağa bölersek, yeni ağlar \ ((N-1)\) olmuş olur. Yani bölü işareti 1 bit sağa kaymış olur. Örneğin, /20 şeklinde bir ağı ikiye bölersek iki tane /21 ağ oluşur. Benzer şekilde, \ (N\ şeklindeki bir ağı dörde bölersek, 2 bit kaydırmalıyız. Yani /20 şeklindeki ağ dörde bölünürse elimizde 4 tane /22 ağ oluşur.

9.4 Alt Ağlara Bölme

IP adresi ve ağı temsil eden bit sayısı belirli olan bir ağ, birden fazla küçük ağlara bölünebilir. Alt ağa bölme işlemi alt ağ maskesinde bit kaydırılarak yapılır. /N şeklindeki bir ağ için; /(N+1) şeklinde 1 bitlik kaydırma yapılırsa, önceki ağ ikiye bölünmüş olur. 2 bit kaydırılırsa, 4'e bölünmüş olur. Bu şekilde \ (2^n\ tane alt ağ bölme işlemi yapılabilir.

Not:

Çözüme geçmeden önce mutlaka bölünmemiş ağın analiz edilmesi gerekir. Başlangıç-bitiş adreslerini ve kaç IP adresi olduğunu belirlemeliyiz.

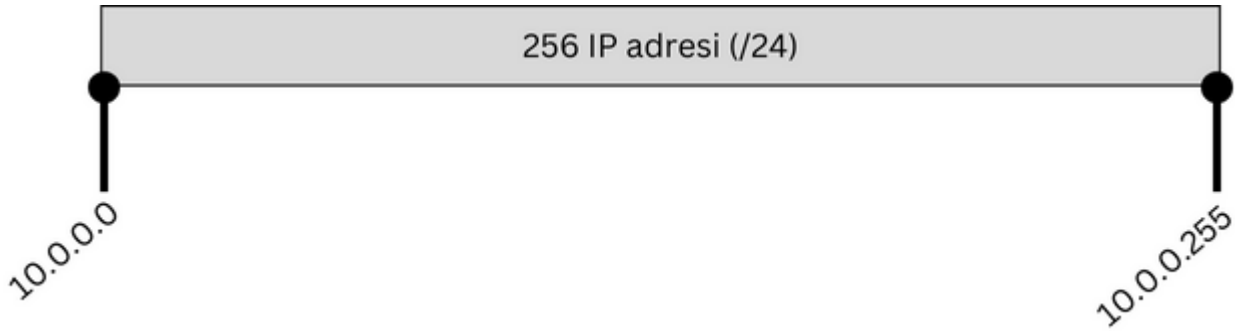
9.4.1 Örnek-1: İkiye bölme

İkiye bölme

10.0.0.0/24 ağını iki ayrı ağa bölünüz.

ANALİZ

- Verilen ağ /24 şeklindedir. Bunu ağ maskesi cinsinden yazmak istersek; 24 tane 1, 8 tane 0 olur. Yani alt ağ maskesi 255.255.255.0 şeklindedir.
- Bu ağda hostları tanımlamak için 8 bit kullanılmıştır. Demek ki ağda $(2^8) = 256$ tane IP adresi vardır. İkiye böldüğümüzde 128 IP'lik iki ayrı ağ oluşacaktır.
- Ana ağın başlangıç noktasını belirlemek için ağ adresini bulmalıyız. Bu ağda ağ adresi 10.0.0.0 IP adresidir.
- Ana ağın son IP adresi ise yayın adresidir. Bunu hesaplarsak, 10.0.0.255 buluruz.

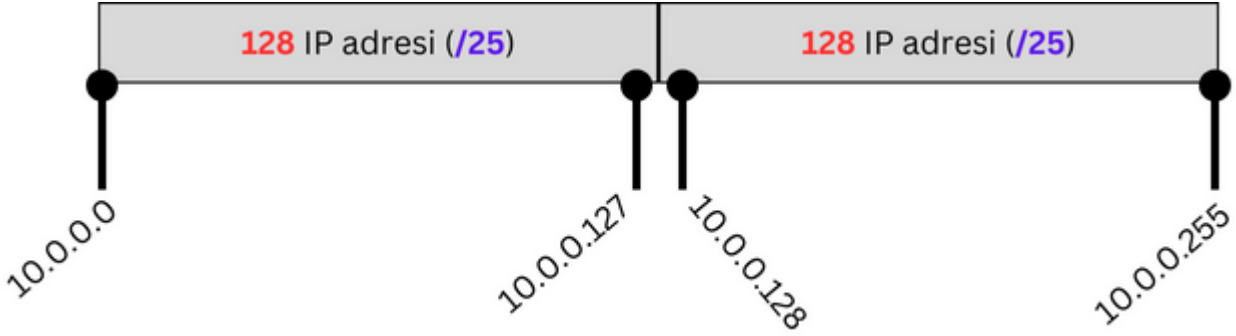


Görsel: IP adres aralığı. Bölünmeden önceki hali

ÇÖZÜM

- Ana ağın maskesini ikilik sistemde `11111111.11111111.11111111.00000000` şeklinde yazabiliriz.
- 24. bitten bölünmüş olan ağda 1 bit kaydırma yaparsak; 25 tane 1, 7 tane 0 olacaktır. Bu durumda ana ağı ikiye bölmüş oluruz. Her bir alt ağda $(2^7)=128$ tane IP adresi olur.
- Ağ bölündükten sonra 1. alt ağın başlangıç adresi (ağ adresi), ana ağın ağ adresi ile aynı olacaktır. Buna göre tabloyu oluşturabiliriz.

	Ağ adresi	Yayın adresi	Ağ maskesi	IP sayısı	Host sayısı
1. ağ	10.0.0.0/25	10.0.0.127	255.255.255.128	128	126
2. ağ	10.0.0.128/25	10.0.0.255	255.255.255.128	128	126



Görsel: IP adres aralığı. İkiye bölünmüş hali

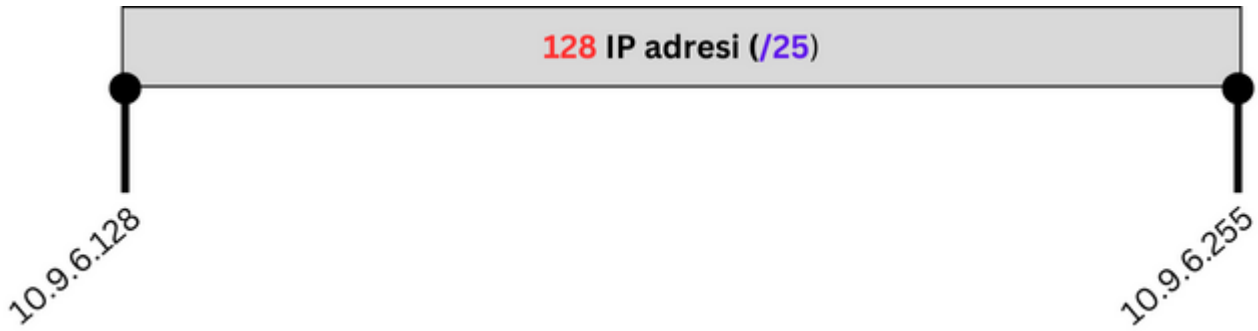
9.4.2 Örnek-2: Dörde bölme

Dörde bölme

10.9.6.200/25 şeklinde verilen bir IP adresi var. Bu IP adresinin bulunduğu ağı, 4 ayrı alt ağa bölünüz.

ANALİZ

- Alt ağ maskesi:** Verilen ağ /25 şeklindedir. Bunu ağ maskesi cinsinden yazmak istersek; 25 tane 1, 7 tane 0 olur. Yani alt ağ maskesi 255.255.255.128 şeklindedir. Bunu dörde böldüğümüzde, /27 şeklinde 4 tane alt ağ oluşacaktır.
- Ağıdaki IP sayısı:** Bu ağda hostları tanımlamak için 7 bit kullanılmıştır. Demek ki ağda $(2^7)=128$ tane IP adresi vardır. Dörde böldüğümüzde 32 IP'lik dört ayrı ağ oluşacaktır.
- Ağ adresi:** Ana ağın başlangıç noktasını belirlemek için, IP adresindeki 25. bitten sonrasını 0 yaparsak "10.9.6.(10000000)₂" olur. Bunu onluk olarak yazarsak, ağ adresini 10.9.6.128 şeklinde buluruz.
- Yayın adresi:** Ana ağın son IP adresini hesaplamak için 25. bitten sonrasını 1 yaparsak "10.9.6.(11111111)₂" olur. Bunu onluk olarak yazarsak, 10.9.6.255 buluruz.

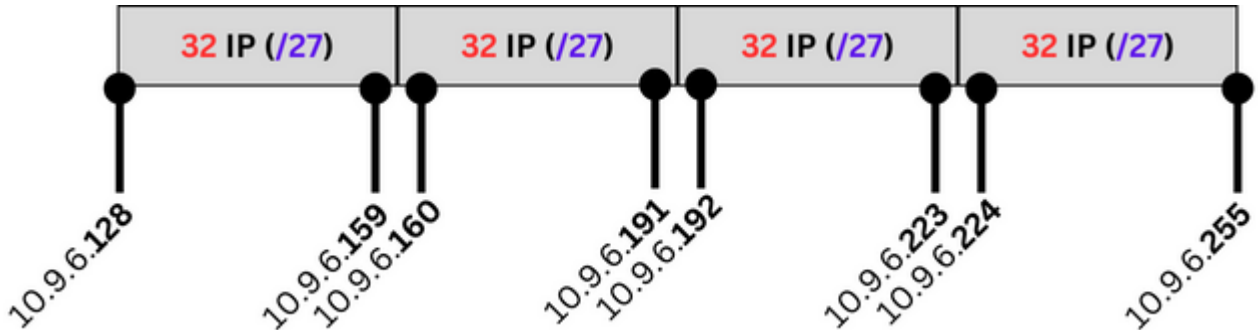


Görsel: IP adres aralığı. Bölünmeden önceki hali

ÇÖZÜM

- 25 . bitten bölünmüş olan ağda 2 bit kaydırma yaparsak; ağı dörde bölmüş oluruz ($2^2=4$). Alt ağların maskesinde; 27 tane 1, 5 tane 0 olacaktır. Bu durumda ana ağı dörde bölmüş oluruz. Her bir alt ağda 32 tane IP adresi olur.
- Ağ bölündükten sonra 1. alt ağın başlangıç adresi (ağ adresi), ana ağın ağ adresi ile aynı olacaktır. Buna göre tabloyu oluşturabiliriz.
- İlk ağın ilk IP adresinden itibaren, 32 ekleyerek devam edersek, bütün alt ağların ağ adreslerini bulabiliriz.

	Ağ adresi	Yayın adresi	Ağ maskesi	IP sayısı	Host sayısı
1. ağ	10.9.6.128/27	10.9.6.159	255.255.255.224	32	30
2. ağ	10.9.6.160/27	10.9.6.191	255.255.255.224	32	30
3. ağ	10.9.6.192/27	10.9.6.223	255.255.255.224	32	30
4. ağ	10.9.6.224/27	10.9.6.255	255.255.255.224	32	30



Görsel: IP adres aralığı. Bölündükten sonra

9.4.3 Örnek-3: Büyük ağları bölme

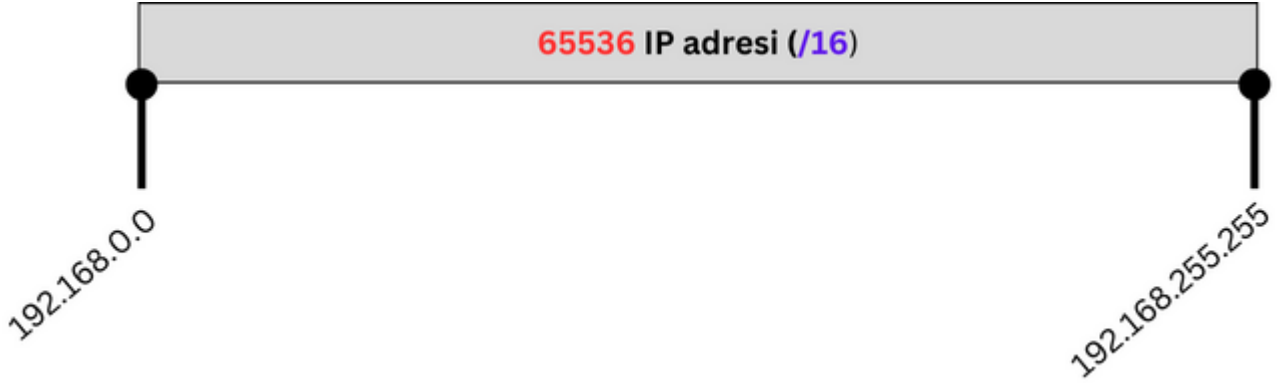
Büyük ağları bölme

192.168.1.100/16 ağını 8 alt ağa bölün. İlk ve son alt ağlar için şunları hesaplayın:

- Ağ adresi
- Yayın adresi - Alt ağ maskesi

ANALİZ

- **Alt ağ maskesi:** Verilen ağ /16 şeklindedir. Bunu ağ maskesi cinsinden yazmak istersek; 16 tane 1, 16 tane 0 olur. Yani alt ağ maskesi 255.255.0.0 şeklindedir. Bunu sekize böldüğümüzde, /19 şeklinde 8 tane alt ağ oluşacaktır.
- **Ağdaki IP sayısı:** Bu ağda hostları tanımlamak için 16 bit kullanılmıştır. Demek ki ağda $(2^{16}) = 65536$ tane IP adresi vardır. Sekize böldüğümüzde 8192 IP'lik sekiz ayrı ağ oluşacaktır.
- **Ağ adresi:** Ana ağın başlangıç noktasını belirlemek için, IP adresindeki 16. bitten sonrasını 0 yaparsak 192.168.0.0 olur.
- **Yayın adresi:** Ana ağın son IP adresini hesaplamak için 16. bitten sonrasını 1 yaparsak 192.168.255.255 olur.



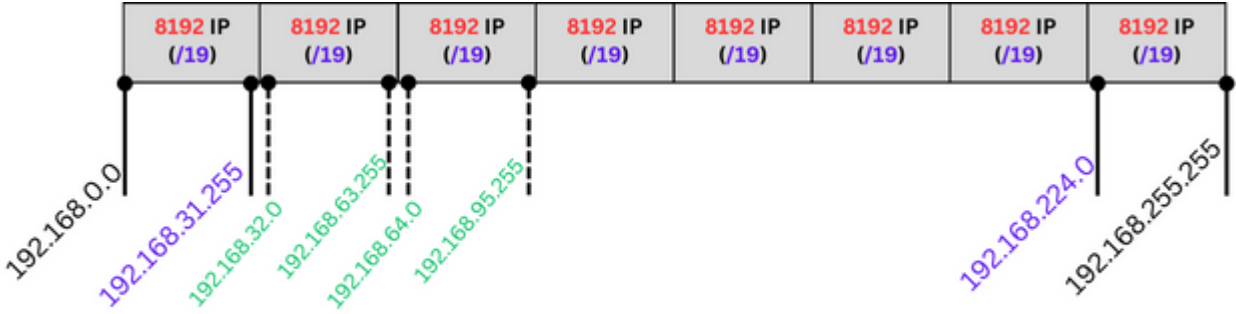
Görsel: IP adres aralığı. Bölünmeden önceki hali

Not:

Küçük ağlarda alt ağları hesaplamak için, örneğin 32'şer ilerleyerek kolayca hesaplayabiliyoruz. Ancak büyük ağlarda 8192 ekleyerek gitmek çok kolay olmayacak. Bu örneğin öncekilerden farklı yanı budur. Aşağıdaki çözüme dikkat ediniz.

ÇÖZÜM

- 16 . bitten bölünmüş olan ağda 3 bit kaydırma yaparsak; ağı sekize bölmüş oluruz ($2^3=8$). Alt ağların maskesinde; 19 tane 1, 13 tane 0 olacaktır. Bu durumda ana ağı sekize bölmüş oluruz. Her bir alt ağda 8192 tane (2^{13}) IP adresi olur.
- Ağ bölündükten sonra **1. alt ağın başlangıç adresi** (ağ adresi), ana ağın ağ adresi ile aynı olacaktır: **192.168.0.0**
- **Son alt ağın yayın adresi** de ana ağın yayın adresi ile aynı olacaktır: **192.168.255.255**
- Birinci alt ağın yayın adresini bulmak için, bu alt ağ içindeki herhangi bir IP adresini örnek olarak alıp, 19. bitten sonrasını 1 yapabiliriz. Elimizde zaten bu alt ağdan bir IP adresi var. 192.168.0.0 IP adresi hem bölünmemiş ana ağın, hem de bölündükten sonraki ilk alt ağın bir parçasıdır. Eğer /16 olarak düşünülürse, ana ağın bir parçası olarak hesaplanabilir. /19 olarak düşündüğümüzde ise 8192 IP adresine sahip olan 1. alt ağa ait bir IP adresidir. 192.168.0.0 IP adresinin 19. bitten sonrasını 1 yaparsak **birinci alt ağın yayın adresini** buluruz:
 $192.168.(00011111.11111111)_2 = 192.168.31.255$
- Üstteki maddeye benzer şekilde; son alt ağdan 1 IP adresini alıp bunun ağ adresini (/19 olarak) hesaplırsak, son alt ağın ağ adresini bulmuş oluruz. Bu nedenle son alt ağa ait olan 192.168.255.255 IP adresinin 19. bitten sonrasını 0 yaparsak **son alt ağın ağ adresini** buluruz:
 $192.168.(11100000.00000000)_2 = 192.168.224.0$
- Yeni oluşan küçük ağların alt ağ maskesini hesaplamak için /19 olan ifadeyi ikilik sistemde yazmalıyız:
 $(11111111.11111111.11100000.00000000)_2 = 255.255.224.0$



Görsel: IP adres aralığı. Bölündükten sonra

Görsel üzerinde siyah ile işaretlenen IP adresleri zaten ilk analizde bulunmuştu. Mavi ile işaretlenenler, soruda istenen ve çözümde bulduğumuz IP adresleri. Yeşil ile işaretlenenler soruda istenmiyordu ama birkaç tanesini göstermek istedim şekil üzerinde de. Soruda istenen verileri yeniden tablo halinde yazalım:

	Ağ adresi	Yayın adresi	Ağ maskesi
1. ağ	192.168.0.0/19	192.168.31.255	255.255.224.0
8. ağ	192.168.224.0/19	192.168.255.255	255.255.224.0

9.4.4 Örnek-4: Farklı büyüklüklerde alt ağlar

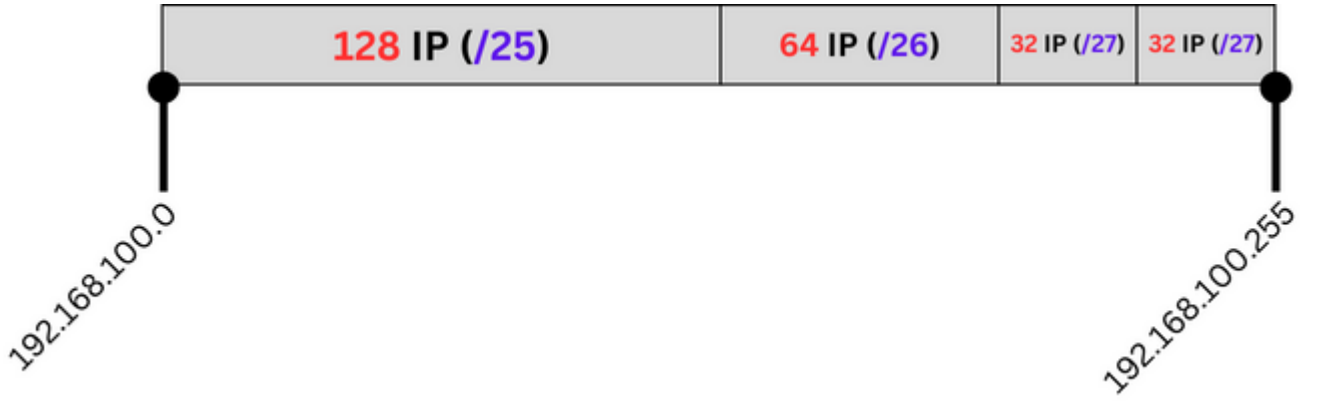
Farklı büyüklüklerde alt ağlar

Bir şirkete 192.168.100.0/24 şeklinde IP aralığı tahsis edilmiştir. Şekilde sistem yöneticisi ağdaki aşırı yayın trafiğinin sorun çıkardığını düşünerek alt ağlara bölmek istiyor. Birimlerin PC sayısı aşağıdaki gibidir.

Teknik birim=70, Pazarlama=40, Muhasebe=20, İdari birim=25

ANALİZ

- **Alt ağ maskesi:** Verilen ağ /14 şeklindedir. Bunu ağ maskesi cinsinden yazmak istersek; 255.255.0.0 şeklindedir.
- **Ağdaki IP sayısı:** Ağda $(2^8) = 256$ tane IP adresi vardır.
- **Ağ adresi:** IP adresindeki 24. bitten sonrasını 0 yaparsak 192.168.100.0/24 olur.
- **Yayın adresi:** Ana ağın son IP adresini hesaplamak için 16. bitten sonrasını 1 yaparsak 192.168.100.255 olur.
- Her birim için 2^n formülüne göre optimum ağ büyüklüklerini yazalım:
 Teknik: $2^7 = 128$
 Pazarlama : $2^6 = 64$
 Muhasebe: $2^5 = 32$
 İdari: $2^5 = 32$
- Ağları alt ağlara bölerken iki eşit parçaya bölündüğünü biliyoruz. Burada ise farklı boyutlarda ağ ihtiyacı var. Normalde bu tarz bir uygulama pek olmamaktadır. Ancak verilen soru özellikle hazırlanmıştır. Önce ağı ikiye bölerek 2x128 ağ yapılabilir. Sonra bu alt ağlardan birisi yeniden ikiye bölünerek 128+64+64 şeklinde 3 ağ yapılabilir. BU 64'lerden birisi bir daha ikiye bölünürse 128+64+32+32 şeklinde 4 tane alt ağ elde edebiliriz. Bu da tam örneğe uygun hale gelmektedir.



Görsel: bölünme sonrası durum

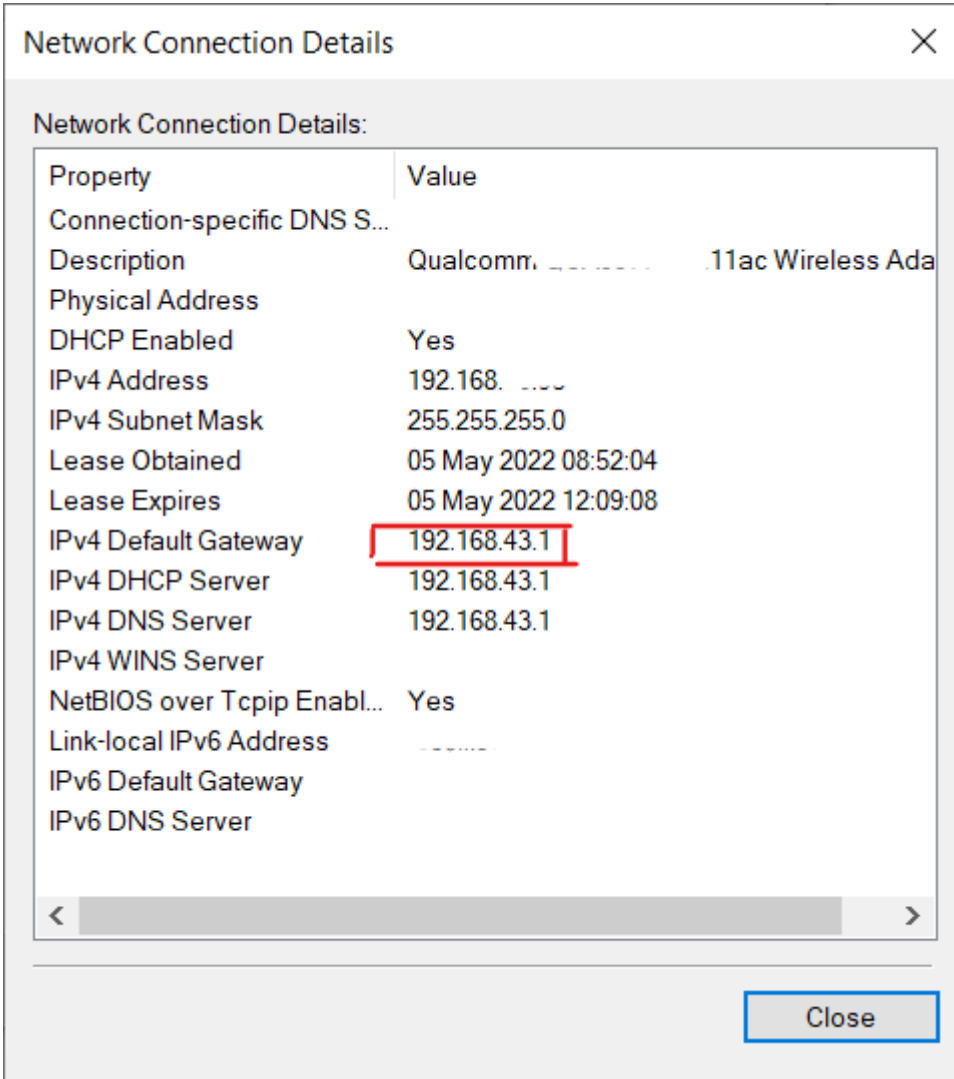
ÇÖZÜM

Çözümü size bırakıyorum.

9.4.5 Çalışma soruları

1. /17 şeklinde gösterilen ağın maskesi nedir?
2. IP adresi 10.10.0.0 ve alt ağ maskesi 255.255.0.0 olan bir bilgisayarın bulunduğu ağda kaç IP olabilir?
3. 255.255.255.224 şeklindeki alt ağ maskesi olan bir ağda kaç host olabilir?
4. 192.168.1.0/8 ağını ikiye bölün.
5. 172.16.172.220/26 ağını ikiye bölün.
6. 10.0.0.0/8 ağını 16'ya bölün. Sadece ilk alt ağ için ağ adresi, yayın adresi, alt ağ maskesi değerlerini hesaplayın.
7. 10.0.0.0/29 ağını ikiye bölün.
8. 10.50.100.200/25 şeklinde IP adresi tahsis edilmiş bir bilgisayarın ağ adresi ve yayın adresi nedir?

9.5 Ağ Geçidi IP Adresleri



Görsel: Windows bilgisayarda ağ geçidi IP adresi

Aynı ağdaki bilgisayarlar, kendi aralarında 2. katmanda MAC adresleri ile haberleşirler. Farklı bir ağdaki IP adresi ile iletişim kurmak istediklerinde, ilk gitmeleri gereken yer, kendi ağ geçidi olarak bildikleri IP adresidir. Ağ geçidi, bir ağdaki bilgisayarların diğer ağlara gidebilmesi için geçmeleri gereken kapıya denir.

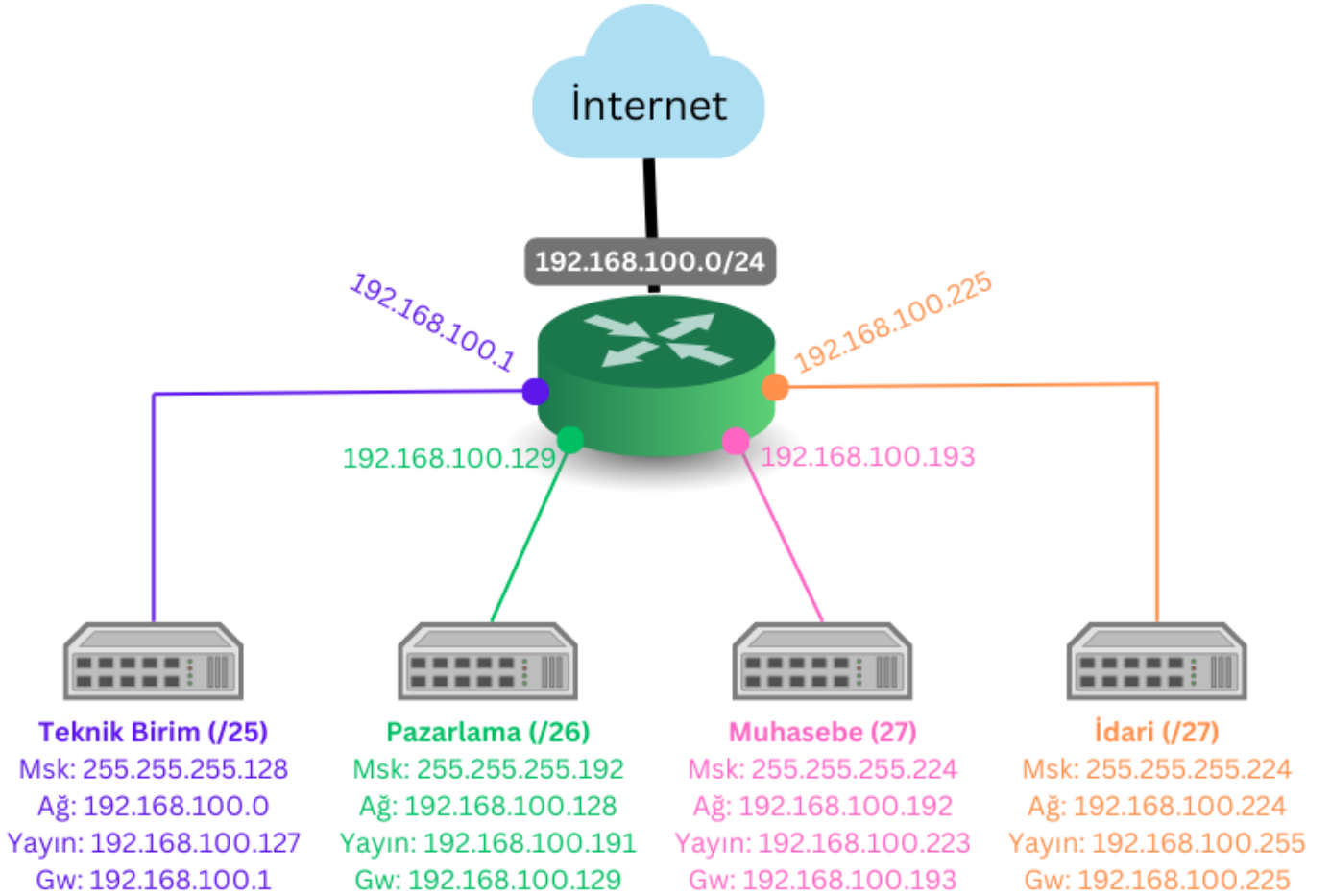
Genellikle her ağda yalnızca 1 tane ağ geçidi olur. Bu da IP adresleri ile beraber bilgisayarlara otomatik olarak gönderilir. Özel durumlarda ağlarda birden fazla ağ geçidi olabilir. Bu tarz durumlarda hangi hedeflere giderken hangi ağ geçidinden geçmesi gerektiğini belirten "yönlendirme tablosu" kullanılır.

Her ağ için; ilk IP adresinin ağ adresi, son IP adresinin yayın adresi olduğunu biliyoruz. Kural olmamakla birlikte, genel teamüllere göre, ağ adresinden sonraki ilk IP adresi (kullanılabilecek ilk host adresi) ağ geçidi olarak belirlenir.

Ağ geçidi IP adresi

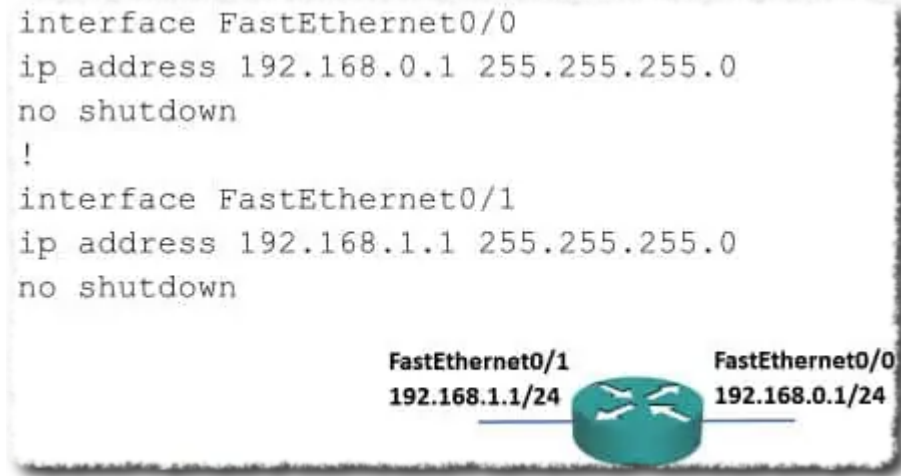
Ağ geçidi IP adresi, her bir ağın doğrudan bağlı olduğu yönlendirici arayüzünde (interface, ağ arabirimi, port, ethernet kartı, NIC[Network Interface Card]) tanımlı olan IP adresi olmak zorundadır.

Yukarıdaki örnek için ağ geçidi bilgileri aşağıdaki görselde verilmiştir. Her ağın kullanılabilecek ilk host adresi "ağ geçidi" IP adresi olarak yönlendiricinin ilgili bacağına (NIC) verilmiştir. Yönlendiricinin WAN bacağı ise internet bağlantısı olarak kullanılmaktadır. Bu bacadaki 256 IP adresi tanımlıdır.



Görsel: Önceki örneğin ağ bilgileri

Aşağıdaki görselde, Cisco yönlendiricilerde bir bacağa (NIC, Ethernet kartı, port) IP adresinin nasıl verildiği görülmektedir. Görselde verilen yönlendiricide iki NIC vardır: FastEthernet 0/1 ve FastEthernet 1/1 şeklinde. Bu iki interface'e IP adresi verilebilmesi için yapılması gereken konfig te aynı görselin üst kısmındaki metinlerde verilmiştir.

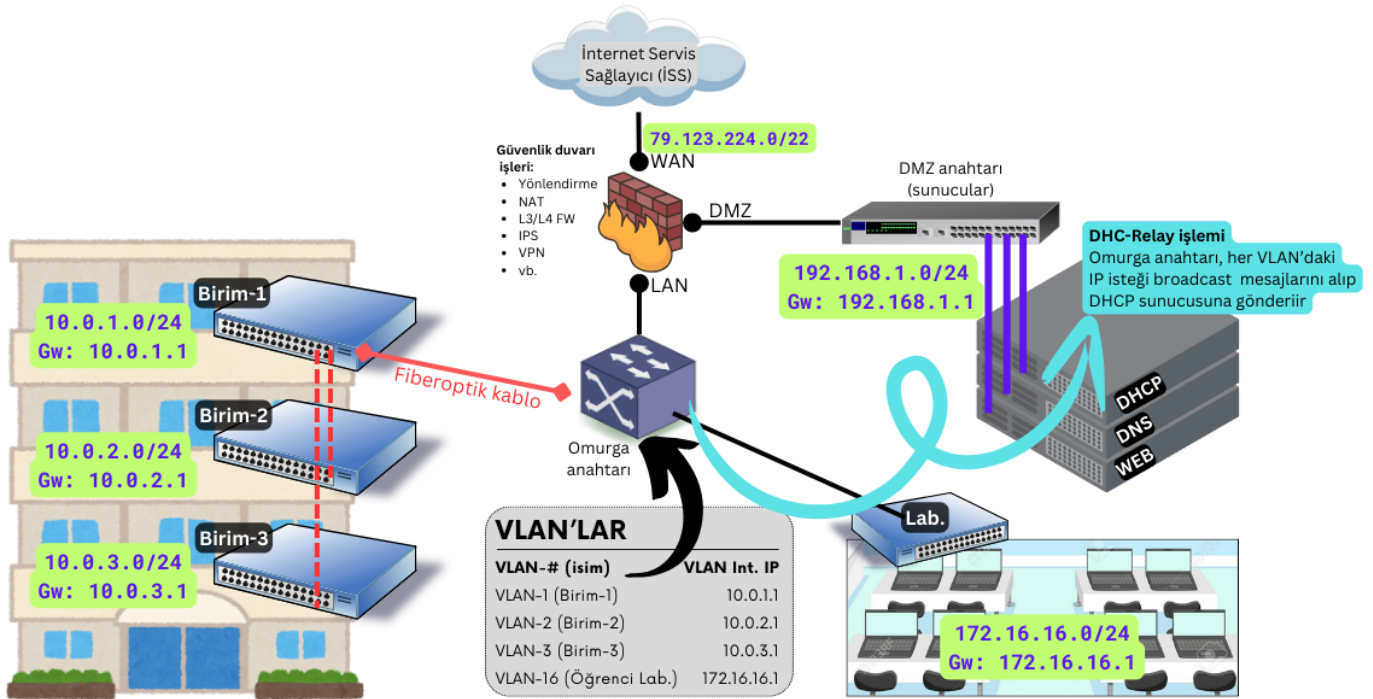


Görsel kaynağı: <https://www.flackbox.com/cisco-basic-router-switch-configuration>

Aşağıdaki görselde kurumlarda güncel durumda kullanılan standart bir topoloji verilmiştir. Artık bulut tabanlı çözümlere geçilmeye başlandığı için birçok kurumda fiziksel sunucu bile bulunmamaktadır. Ancak kendi veri merkezi olan ve sunucusu olan

kurumlar bu tarz bir yapı kullanmaktadır. Bu görsele ilaveten istenirse; IPS, WAF, traffic shaper, NAC, vb. birçok sistem eklenebilir. Ancak sade olması için minimal çizim yapılmıştır. Görselde birkaç noktayı vurgulayabiliriz:

1. Güvenlik duvarının 3 bacağı (*interface, NIC, port, Ethernet kartı. Hepsi aynı anlamda.*) var: LAN, WAN ve DMZ. İstenirse bu bölgelerin sayısı artırılabilir.
2. Hem LAN'lar hem de VLAN'lar kullanılıyor.
3. VLAN'lar omurga anahtarında oluşturulmuş. Her VLAN'ın bir interface'i (sanal NIC) var. Bu interface'lere IP adresi verilmiş. Her VLAN'daki her bilgisayarın da ağ geçidi bu IP adresleri olarak kullanılıyor.
4. Herhangi bir VLAN veya LAN'da bir PC IP almak istediğinde, "Ortamda DHCP sunucusu var mı?" (*discovery*) diye bir broadcast mesajı gönderiyor. Bu mesaj sadece kendi ağındaki IP'lere gidiyor. Bu IP'lere kendi ağ geçidi de dahil. Ağ geçidi olan cihaz da (*bu topoloji için omurga anahtarı*) bu mesajı alıp DHCP sunucuya aktarıyor. Gelen cevabı (*offer*) ilgili PC'ye geri gönderiyor. Bir IP alma isteğinin, başka bir ağıdaki sunucuya iletilmesi işlemine **DHCP relay** denir. DHCP relay işlemini; anahtar, yönlendirici ya da ağıdaki herhangi bir PC yapabilir.
5. Sunucu bölgesinde otomatik IP kullanılmayabilir. Elle yönetmek çok zor olmaz, hatta "elle IP vermek" hataları da azaltabilir. Ancak kullanıcı bilgisayarlarında her zaman otomatik IP kullanırız.
6. DHCP sunucusuna bir "IP isteği" mesajı geldiğinde, sunucu bu mesaja 4 temel veri içeren bir cevap döndürür: IP adresi, alt ağ maskesi, ağ geçidi, DNS sunucu IP adresi. İstenirse bunlara ilave başka veriler de gönderilebilir: NTP server, TFTP server, vb.
7. Evlerde kullandığımız xDSL modemler buradaki bir çok işi tek başına yapıyor: Protokol çevirme, yönlendirme, NAT, güvenlik duvarı, switching, Wifi Access point, traffic shaping, vb.



Kurumlarda kullanılan güncel topoloji

Aşağıdaki görsele Cisco cihazlarda yapılan bir DHCP-relay işlemi gösterilmiştir. Görseldeki 50.0.0.10 IP adresi, o network'ün DHCP server IP adresidir.

```
Router(config)#interface fastethernet 0/1
Router(config-if)#ip helper-address 50.0.0.10
Router(config-if)#exit
```

Görsel: Cisco DHCP relay işlemi

9.6 İki Bilgisayar Aynı Ağda Mı?

İki bilgisayar aynı ağda mı?

A bilgisayarı; iletişim kurmak istediği B bilgisayarı ile aynı ağda olup olmadığını anlamak için, B'nin IP adresiyle kendi ağ maskesini çarpar. Çıkan sonucu kendi ağ adresiyle karşılaştırır.

9.6.1 Örnek-5

Örnek-5

10.0.0.127/24 ve 10.0.0.128/24 IP adreslerinin, birbirleri ile haberleşebilmek için ağ geçidine ihtiyaçları var mıdır?

A'nın B ile haberleşmesi :

B'nin IP adresi 10.0.0.128 A'nın ağ maskesi x 10.0.0.128 10.0.0.0

Çıkan sonuç A'nın ağ adresiyle aynı olduğundan haberleşirler.

A'nın C ile haberleşmesi :

C'nin IP adresi 10.0.0.254 A'nın ağ maskesi x 10.0.0.128 10.0.0.128

Çıkan sonuç A'nın ağ adresiyle aynı olmadığından haberleşemezler.

10. IP Yönlendirme

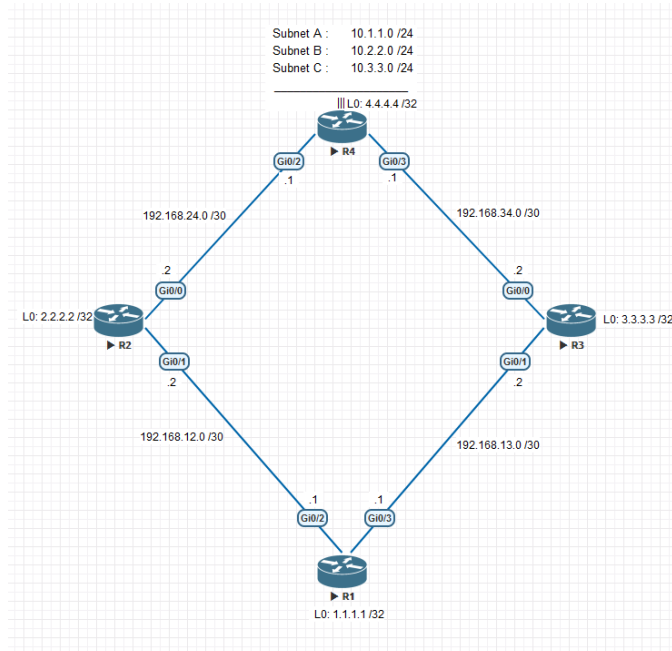
IP'nin yönlendirilebilir olması protokolün en güçlü özelliğidir. Çok sayıda iletişim protokolü mevcut olmasına rağmen IP'nin yönlendirilebilir esnek yapısı internetin temel dili olmasını sağlamıştır. Yönlendirme işlemini "Yönlendirici(Router)" yapar.

Yönlendirme Tablosunda

1. Kaynak
2. Hedef (IP ve Maske)
3. Ağ Geçidi
4. Ara Birim (Interface)
5. Ölçüt (Metrik)

```
murat@ozalp:~$ route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          10.9.222.1     0.0.0.0         UG        100    0      0 enp4s0
0.0.0.0          10.90.0.1      0.0.0.0         UG        600    0      0 wlp0s20f3
10.0.3.0         0.0.0.0        255.255.255.0   U         0      0      0 lxcbr0
10.9.222.0       0.0.0.0        255.255.255.0   U         100    0      0 enp4s0
10.90.0.0        0.0.0.0        255.255.240.0   U         600    0      0 wlp0s20f3
```

Linux'ta yönlendirme tablosu. Hem kablolu hem de kablosuz bağlantı aktif



```
R1#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       I - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, I - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PFR

Gateway of last resort is 192.168.13.2 to network 0.0.0.0

S* 0.0.0.0/0 [1/0] via 192.168.13.2
C 1.0.0.0/32 is subnetted, 1 subnets
   1.1.1.1 is directly connected, Loopback0
C 2.0.0.0/32 is subnetted, 1 subnets
   2.2.2.2 [90/130816] via 192.168.12.2, 01:29:21, GigabitEthernet0/2
C 3.0.0.0/32 is subnetted, 1 subnets
   3.3.3.3 [110/2] via 192.168.13.2, 01:29:29, GigabitEthernet0/3
D 4.0.0.0/32 is subnetted, 1 subnets
   4.4.4.4 [90/131072] via 192.168.12.2, 01:29:20, GigabitEthernet0/2
D 10.0.0.0/8 is variably subnetted, 7 subnets, 3 masks
   10.1.1.0/24
     [90/131072] via 192.168.12.2, 01:29:20, GigabitEthernet0/2
   10.1.1.0/30 [1/0] via 192.168.12.2
   10.1.1.1/32 [110/3] via 192.168.13.2, 01:29:29, GigabitEthernet0/3
D 10.2.2.0/24
     [90/131072] via 192.168.12.2, 01:29:20, GigabitEthernet0/2
   10.2.2.1/32 [110/3] via 192.168.13.2, 01:29:29, GigabitEthernet0/3
D 10.3.3.0/24
     [90/131072] via 192.168.12.2, 01:29:20, GigabitEthernet0/2
   10.3.3.1/32 [110/3] via 192.168.13.2, 01:29:29, GigabitEthernet0/3
O 192.168.12.0/24 is variably subnetted, 2 subnets, 2 masks
   192.168.12.0/30 is directly connected, GigabitEthernet0/2
   192.168.12.1/32 is directly connected, GigabitEthernet0/2
C 192.168.13.0/24 is variably subnetted, 2 subnets, 2 masks
   192.168.13.0/30 is directly connected, GigabitEthernet0/3
   192.168.13.1/32 is directly connected, GigabitEthernet0/3
D 192.168.24.0/30 is subnetted, 1 subnets
   192.168.24.0 [90/3072] via 192.168.12.2, 01:29:21, GigabitEthernet0/2
O 192.168.34.0/30 is subnetted, 1 subnets
   192.168.34.0 [110/2] via 192.168.13.2, 01:29:29, GigabitEthernet0/3
R1#
```

Görsel kaynağı: <https://willgrana.com/posts/reading-cisco-ios-routing-table/>

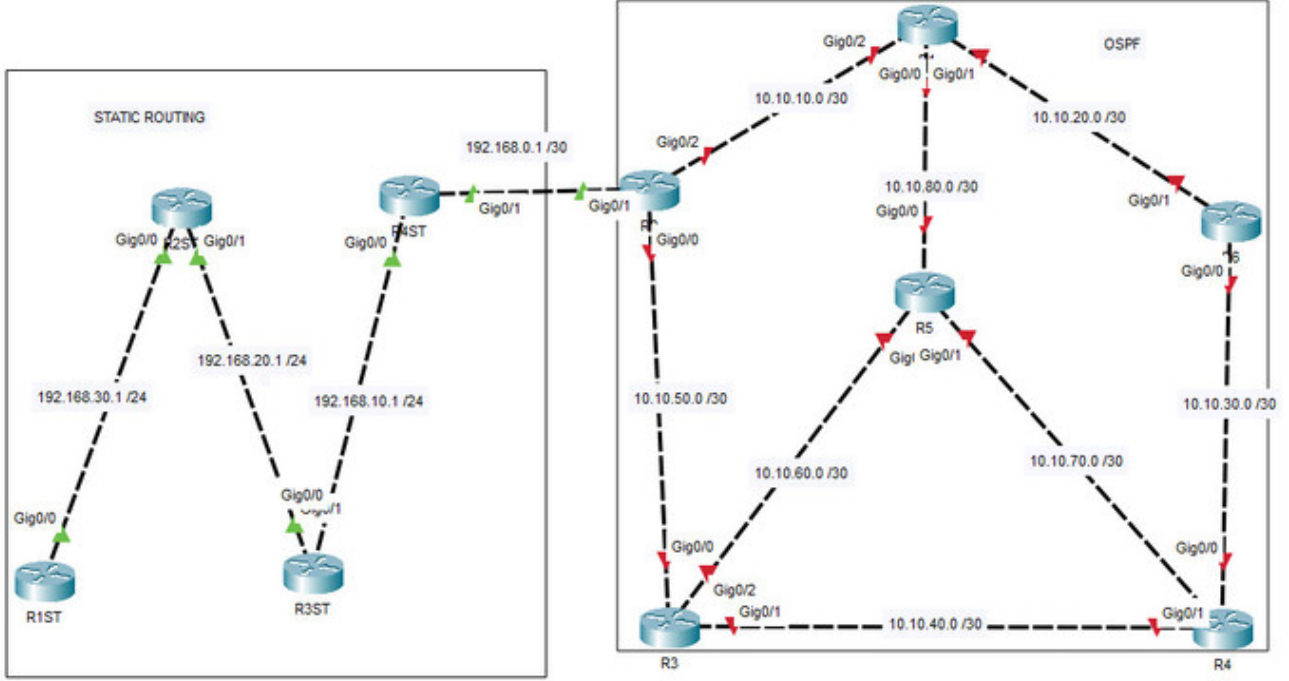
Yönlendirme tablosunda birbirini kapsayan kurallar var ise bunlar küçükten büyüğe sıra ile değerlendirilir.

10.1 STATİK YÖNLENDİRME

Ağ yöneticisi tarafından elle sabit olarak yazılır. Genellikle yönlendiricisi ve yönlendirme işlemi çok fazla olmayan ağlarda kullanılır. Yönlendirme tablolarının güncellemesi ağıdaki fiziksel değişikliklere göre yeniden elle yapılmalıdır.

10.2 DİNAMİK YÖNLENDİRME

Yönlendirme algoritmaları tarafından hesaplanarak bulunur. Ağ yöneticisi tarafından önceden bazı filtreler ve tanımlamalar yapılmalıdır. Ağda değişiklik olduğunda yollar otomatik olarak düzeltilir. En yaygın yönlendirme algoritmaları OSPF, BGP, RIP şeklindedir.



Görsel kaynağı: <https://learningnetwork.cisco.com/s/question/0D53i00000S8yMLCAZ/static-and-dynamic-routing>

11. Bilgisayar Ağları Modelleme

Bu başlıkta simülâtör ve emülâtör kavramları açıklanmaya çalışılıp örnek uygulamalar verilecektir.

11.1 Simülâtör & Emülâtör

Bilgisayar üzerinde bir ağı modellemek için; simülâtör ve emülâtör şeklinde iki tür program kullanılmaktadır:

Simülâtör: Gerçek ortamdaki sistemler ile (çok benzese de) birebir aynı şekilde çalışmaz. Uçuş simülâtörleri buna örnek gösterilebilir. Gerçek sistemlerde kullanılan donanımların üzerindeki yazılımlar bunda kullanılmaz, simülâtörlerde kullanılan sanal cihazlarda özel geliştirilmiş ve kısıtlı yazılımlar çalışır. Ayrık zamanda çalışır: gerçek hayatta binlerce saat sürececek bir işlem 1 saniyede yapılabilir; gerçek hayatta 1ms içerisinde biten bir eylem saniyelerce sürececek şekilde yavaşlatılabilir.

Emülâtör: Gerçek cihazlarda kullanılan yazılımlar doğrudan burada da çalıştırılır. Virtualbox üzerinde Windows çalıştırmak için, gerçek Windows kurulumu yaptığımızı hatırlayın. Donanımlar sanallaştırılır ama donanımlar üzerinde gerçek yazılımlar (işletim sistemleri) kullanılır. Gerçek zamanda çalışır.

Simülâtör ve emülâtör kavramlarını bilgisayar ağları konusu özelinde özetlemeye çalışalım.

İnternet'in ortak dilinin IP olması gibi, bilgisayar ağlarında ortak donanım da Cisco firmasının ürünleridir. Pazara erken girmiş olması, ürünlerinin kaliteli olması, geniş ürün yelpazesi olması, bol miktarda dokümanı olması, kullanıcı sayısının çok olması, vb. nedenlerle bilgisayar ağları çalışan hemen herkes Cisco cihazlara hakim olmaktadır. Bu nedenle, ağ modelleme programlarında öncelikle Cisco cihazlara (yönlendirici, anahtar, vb.) destek sağlanmaktadır.

Emülâtör uygulamalarında, *-simülâtörlerden farklı olarak-* gerçek Cisco işletim sistemi kullanılması gerekmektedir. Gerçek işletim sistemi kullanıldığı için, gerçek cihazlarla yapılan fiziksel ağ uygulamalarına çok yakın bir çalışma ortamı sağlamaktadır. Bunun en büyük dezavantajı ise Cisco işletim sistemleri ücretli olduğu için ilave maliyet çıkarmasıdır. Diğer taraftan; bu işletim sistemlerinin İnternet'in yeraltı dünyasında yaygınlaşması gibi illegal durumlara da sebebiyet vermektedir.

11.2 Ağ Modelleme Platformları (Ücretsiz Olanlar)

11.2.1 Cisco Packet Tracer

Cisco firması tarafından geliştirilmektedir. Cisco'nun Networking Academy adı altında vermiş olduğu eğitimlerde katılımcılara verilmektedir. Bunun haricinde satışı bulunmamaktadır. Simülâtör tarzında bir uygulamadır.

Cisco Packet Tracer arayüzü. Sol tarafta "mantıksal", sağ tarafta "fiziksel" görünüm

Cisco Packet Tracer arayüzü. Sol tarafta "mantıksal", sağ tarafta "fiziksel" görünüm

Katalogunda Sadece Cisco firmasına ait ürünler bulunmaktadır. Yönlendirici, anahtar, kablosuz erişim noktası, IP telefon sistemler, vb. farklı türde ürünler kullanılabilir. Linux ve Windows sürümleri bulunmaktadır. Program kurulduğunda, ilave bir işlem yapmaya gerek kalmadan tüm özellikleri ile aktif halde olmaktadır. Program içerisinde oluşturulan sanal cihazların gerçek hayat ile bağlantısı yapılamamaktadır. Sadece klasik bilgisayar ağları değil, üst katmanlarda da uygulama gerçekleştirilebilmektedir. Sanal sunucu cihazı üzerinden HTTP, DNS, e-posta sunucuları gibi servisler de simüle edilebilmektedir.

11.2.2 GNS3 (Graphical Network Simulator 3)

Cisco'nun kendi cihazları için tasarladığı IOS isimli işletim sistemlerini kullanır. Bu IOS'lerden GNS3 içerisine en az 1 tane dahil edilmelidir. Bu IOS'leri elde etmek için yasal bir yol malesef bulunmamaktadır. Cisco müşterisi olanlar WEB üzerinden indirebilmektedir. Bunun haricinde satışı bulunmamaktadır. VirtualBox PC'leri bunun içine dahil edilebilmektedir. Gerçek yönlendirici imajları ve gerçek sanal bilgisayarlar kullandığından oldukça gerçekçi bir çalışma ortamı sağlamaktadır. Cisco

sertifikasyon sınavlarına hazırlananlar için de kullanışlıdır. Programın önemli bir özelliği de sanal ağda kullanılan sanal makinaların Host-PC (fiziksel bilgisayar) üzerinden internet'e çıkabilmesidir.

GNS3 arayüzü içindeki yönlendiricinin konsolu

GNS3 arayüzü içindeki yönlendiricinin konsolu

11.2.3 CORE (Common Open Resource Emulator)

Linux ve BSD üzerinde çalışıyor. Windows üzerinde sanal bilgisayarda çalıştırılabilir. Hatta kendi sitesinde, VmWare Player için hazır imajları da var. CORE içindeki her bir sanal PC'de Linux çalışıyor. Sanal ağ üzerinde lazım olan tüm işlevleri bu Linux'lar vasıtasıyla gerçekleştirilebilir. DHCP sunucusu, yönlendirici hizmeti, WEB sunucusu, vb. tüm işlevler Linux platformları üzerinden sağlanabilir. Yönlendirici olarak Cisco kullanma alışkanlığı olanlar, bir sanal Linux üzerine Quagga kurarak, onu sahte Cisco yönlendiriciye çevirebilirler.

Sanal ağ, gerçek ağa bağlayarak internet'e çıkarma özelliği bulunmaktadır. Büyük projelerde kullanmak üzere dağıtık hesaplama desteği de bulunmaktadır. Örneğin; elinizde 3 tane fiziksel PC varsa ve 200 tane node'dan oluşan sanal bir ağ kullanmak istiyorsanız, node'ları iki fiziksel PC'ye paylaştırabilir, 1 PC'yi de GUI amacı ile kullanabilirsiniz. Python ile script yazılabildiğini de belirtelim.

CORE ekran görüntüsü

CORE ekran görüntüsü

11.2.4 Diğerleri

- **NS2:** <http://www.isi.edu/nsnam/ns/>
- **NS3:** <https://www.nsnam.org/> (NS2'nin devamı olarak yapılmasına rağmen geriye doğru uyumluluğu olmadığından ayrı bir yazılım olarak değerlendiriliyor)
- **Cloonix:** <http://clownix.net> Açık kaynaklı. KVM sanal makine desteği var.
- **IMUNES:** <http://www.imunes.net> Açık kaynaklı. FreeBSD üzerinde çalışıyor. Sanal makinede çalıştırılabilir.
- **OMNeT++:** <http://www.omnetpp.org/>
- **Marionnet:** <http://www.marionnet.org/EN/>
- **Mininet:** <http://www.mininet.org>
- **Netkit:** <http://wiki.netkit.org>
- **Psimulator2:** <http://code.google.com/p/psimulator/>
- **Virtualsquare:** http://wiki.virtualsquare.org/wiki/index.php/Main_Page
- **VNX and VNUML:** <http://www.dit.upm.es/vnx>
- **OPNET (Ücretli):** <http://www.riverbed.com/products/performance-management-control/opnet.html>

11.3 CORE ile Uygulama

11.3.1 Genel Bilgiler

1. Linux'ta çalışıyor. Konteyner kullanıyor.
2. As an emulator, CORE builds a representation of a real computer network that runs in real time, as opposed to simulation.
3. The live-running emulation can be connected to physical networks and routers.
4. It provides an environment for running real applications and protocols, taking advantage of tools provided by the Linux operating system.

Kullanım alanları: 1. network and protocol research 2. demonstrations 3. application and platform testing 4. evaluating networking scenarios 5. security studies 6. and increasing the size of physical test networks.

Mimari

Çok sayıda bileşenden oluşuyor. Hepsini ayrı ayrı kurmaya gerek yok, otomasyon betiği kendisi kuruyor.

11.3.2 Kurulum

1. <https://coreemu.github.io/core/install.html>
2. Emülasyonda kullanılacak cihaz sayısına göre CPU ve bellek ihtiyacı var.
3. Ubuntu ve Centos destekleniyor ama diğer Linux'lara da kurulabilir. Centos 8 üzerine kurdum. Ubuntuda hatırlamadığım sorunlar yaşadım. Çok ta uğraşmadım.

11.3.3 Arayüz tanıtımı

1. Save/open
2. Canvas size, Wallpaper
3. View/show

11.3.4 Uygulamalar

1. ping
2. ifconfig
3. traceroute
4. nmap
5. netstat
6. tcpdump
7. iperf3

12. Kaynaklar

1. <http://www.brianlinkletter.com/open-source-network-simulators/>
2. <http://www.finmars.co.uk/blog/4-evaluating-network-simulation-tools>
3. <http://nil.uniza.sk/network-simulation-and-modelling/network-simulators-list>

13. Yerel Ağlarda Güvenlik

LAN ortamlarında karşılaşılabilecek başlıca tehditler şunlardır:

- Yetkisiz erişim
- Veri dinleme (sniffing)
- Adres sahteciliği (ARP/DHCP spoofing)
- Zararlı yazılımlar (malware)
- İç tehditler (içeriden erişim yapan kötü niyetli kullanıcılar)

13.1 Fiziksel Güvenlik

Ağ güvenliğinin ilk adımı fiziksel güvenliktir. Anahtarlar (switch), yönlendiriciler (router) ve sunucular gibi aktif cihazlar kilitli dolaplarda veya sunucu odalarında saklanmalıdır. Ağ bağlantı noktalarına fiziksel erişim sadece yetkili personele verilmelidir.

13.2 Erişim Kontrolü

- MAC adresi filtreleme: Belirli cihazlara ağ erişimi sağlanır.
- 802.1X: Port tabanlı kimlik doğrulama protokolüdür. Erişim öncesi kullanıcı doğrulaması yapılır.
- NAC (Network Access Control): Ağa bağlanan cihazların sağlık durumu ve politikalarla uyumluluğu kontrol edilir.

13.3 Trafik Güvenliği

LAN'da veri trafiğinin güvenliğini sağlamak için aşağıdaki önlemler alınabilir:

- ARP spoofing: Saldırgan, sahte ARP mesajlarıyla ağdaki veri akışını üzerine çeker.
- Çözüm: Dynamic ARP Inspection, statik ARP tabloları.
- DHCP spoofing: Saldırgan sahte DHCP sunucusu gibi davranarak kullanıcıları yönlendirir.
- Çözüm: DHCP Snooping ile sadece yetkili portlardan DHCP yanıtı alınması sağlanır.

13.4 VLAN Kullanımı ve Segmentasyon

Ağ segmentasyonu ile farklı kullanıcı gruplarının trafiği ayrılır. VLAN'lar, bu segmentasyonu mantıksal olarak sağlar. VLAN hopping saldırılarına karşı:

- Etiketli/etiketsiz port ayarları doğru yapılmalı,
- Native VLAN yapılandırmasına dikkat edilmelidir.

13.5 Port Güvenliği

Switch portlarına yönelik güvenlik önlemleri şunlardır:

- Kullanılmayan portlar devre dışı bırakılmalı,
- Belirli MAC adreslerine izin verilerek sabitleme (Sticky MAC) yapılmalı,
- Port güvenliği ihlalinde port otomatik olarak kapanmalıdır (shutdown).

13.6 Loglama ve Denetim

Ağ olaylarının izlenmesi ve kaydedilmesi güvenliğin sürekliliği açısından önemlidir.

- SNMP ve Syslog gibi protokollerle loglar merkezi sistemlere yönlendirilir.
- SIEM sistemleri, logları analiz ederek anormal aktiviteleri tespit eder.

13.7 Yazılım ve Donanım Güncellemeleri

Ağ cihazlarında üretici güncellemeleri ve güvenlik yamaları zamanında uygulanmalıdır. Firmware güncellemeleri, yeni tehditlere karşı cihazları korur ve performansı artırır.

14. Ağ İzleme ve Yönetimi

- Ağ izleme kavramı
- Proaktif vs reaktif izleme
- Performans, güvenlik ve arıza tespiti neden önemlidir?
- ISO/OSI ve TCP/IP katmanlarına göre izleme
- FCAPS modeli (Fault, Configuration, Accounting, Performance, Security)

14.1 Temel Protokoller

- SNMP (Simple Network Management Protocol)
- Syslog protokolü
- NetFlow, sFlow, IPFIX

14.2 Ağ İzleme Araçları

- Open-source ve ticari araçlara genel bakış
- Wireshark, tcpdump, nmap
- Zabbix, Nagios, MRTG, PRTG, LibreNMS, NetDisco, Cacti
- Rsyslog, Graylog, vb.
- Wazuh
- Ntopng / Grafana / Prometheus

14.3 Log işlemleri

- Rsyslog
- SIEM, Graylog

14.4 Performans İzleme

- CPU, RAM, disk, ping, latency ölçümleri
- MRTG, PRTG, Cacti, SmokePing, vb.

14.5 Ağ Haritalama ve Topoloji Görselleştirme

- Network topology tools: Netdisco, OpenNMS, The Dude

14.6 Güvenlik Olaylarının İzlenmesi

- IDS/IPS sistemleri (Snort, Suricata)
- Port taramaları ve anormallik tespiti
- SIEM sistemlerine giriş
- CrowdSec

14.7 Otomasyon ve Betikleme

- Ağ izleme işlemleri için basit betikler (Bash, Python, Expect)
- API ile izleme sistemlerine entegrasyon (anahtarlar da API destekliyor artık). HP Aruba CX OS işletim sistemi VM.
- Webhook, alert script örnekleri
- DevOps araçları (Ansible gibi)

15. Deneme Tahtası

15.1 Material for MkDocs

<https://squidfunk.github.io/mkdocs-material/reference/>

15.2 Callouts eklentisi

<https://squidfunk.github.io/mkdocs-material/reference/admonitions/#classic-admonitions-docsstylesheetsextracss>

Writing custom titles

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla et euismod nulla. Curabitur feugiat, tortor non consequat finibus, justo purus auctor massa, nec semper lorem quam in massa.

Writing custom titles

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla et euismod nulla. Curabitur feugiat, tortor non consequat finibus, justo purus auctor massa, nec semper lorem quam in massa.

Note

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla et euismod nulla. Curabitur feugiat, tortor non consequat finibus, justo purus auctor massa, nec semper lorem quam in massa.

15.3 PlantUML Grafiği

Alice -> Bob

```
@startuml sign_in_sequence
title "Sign In Sequence Diagram"
actor User
participant "@action authenticate" as authenticate
entity User as UserModel
User -> authenticate: {"email": email, "password": password}
```

15.4 Mermaid Grafiği

```
graph LR
  hello --> world
  world --> again
  again --> hello
```

```
graph LR
  A[Start] --> B{Error?};
  B -->|Yes| C[Hmm...];
  C --> D[Debug];
  D --> B;
  B ---->|No| E[Yay!];
```

15.5 Formül denemesi

math kütüphanesi

15.5.1 Satır içi formül

When $(a \neq 0)$, there are two solutions to $((ax^2 + bx + c = 0))$ and they are

15.5.2 Satır arası formül

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

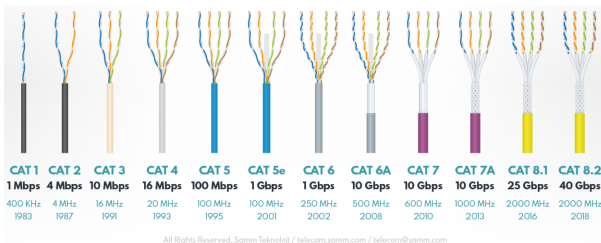
15.6 Dipnot ve sözlük kullanımı

IP, bps, RF ve OSI¹ gibi ifadeler sözlük şeklinde kullanılabilir. BSEU MF.

15.7 Görsel kullanımı

Boyut kullanılabiliyor. Başlık ta kullanılabiliyor ama VSCode'da görünmüyor, yazımı da pek güzel değil.

15.7.1 Görselde boyut kullanma



Görsel kaynağı: <https://telecom.samm.com/history-of-ethernet-lan-cables-categories>

15.7.2 Görselde başlık metni kullanımı



Görsel kaynağı: <https://www.electricalvolt.com/how-to-crimp-rj45-connector/>

16. Son başlık.

..

1. [OSI -Open Systems Interconnection-](#) modeli ISO tarafından geliştirilmiştir. ←