# Data Communications and Computer Networks

## *"Network Technologies"*

Dr. Cahit Karakuş, 2020

# Switched Networks…

- Depending on the nature of the established connection, switched networks are divided into two categories: Circuit-Switched Networks and Packet-Switched Networks.
- A well-known example of switched networks is Wide Area Networks (WANs).
- The goal is to transport data between two points by relaying it from one node to the next until it reaches its destination.
- In Packet-Switched networks, data (bit:0/1 series) is transmitted between transceiver computers via a series of nodes (Gateway, Router, Ethernet Switch, etc.).
- Nodes typically have dedicated peer-to-peer connections.
- In Circuit Switching that inter-node connections are typically established through multiplexers (TDM, PDH and SDH).
- Nodes other than the transmitter and receiver are not concerned with the content of the data.

# Circuit Switched Networks

- In Circuit Switched  Networks, a dedicated communication path is established between two computers, used solely for the data sent through the nodes.
- This path connects a series of physical links between the nodes.
- A logical channel in each link is dedicated to the established connection.
- Data generated by the source computer is sent rapidly over this dedicated path.
- Incoming data is routed, or switched, to the appropriate channel at the nodes with minimal delay.
- Telephone networks, TDM-E1, PDH and SDH multiplexing systems are examples of circuit-switched networks.
- Circuit-switched networks are established in three stages:
  - Circuit installation
  - Transmission and transmitting of data
  - Removal of the circuit connection

# Packet Switched Networks

- In packet-switched networks, data is sent in the pieces called packets.
- The network's transmission capacity is sufficient for multiple computers sending simultaneously.
- Each packet is transferred from node to node until it reaches its destination.
- At each node, the entire packet is received, stored, and retransmitted.
- Packet switching operates on the same principle as sending letters from sender to receiver.

# Ağ Protokolleri

# Network Definitions

- What does "Frame" mean in networking? A "Window" refers to the number of segments of a data packet that can be sent from a source to a destination before an acknowledgment is received. A "Window" refers to the number of segments allowed to be sent from a source to a destination before an acknowledgment is returned.

- What is a MAC address? A MAC address stands for Media Access Control address. It is the address of a device defined as the Media Access Control Layer in network architecture. A MAC address is unique and is usually stored in ROM.

- A checksum is a simple error detection process in which the transmitted data (bit: 0/1) is accompanied by a numerical value based on the number of bits set. A checksum is created from the 1s and 0s in the data packet to be sent.

# Network Technologies

- Network technology: The technological infrastructure and backbone through which two or more computer systems, possessing specific hardware, software, and protocols, across different locations, communicate reliably without direct connection.
- A network is a communication infrastructure through which a group of computer systems with NIC interfaces share information and hardware.
- Data transmission in computer networks occurs in two ways: wired and wireless.
- Computers connect to each other via copper telephone cables, fiber optic cables, or wirelessly via electromagnetic waves.
- An interconnection of computers and other devices (machines containing computer systems), including:
  - Network Devices: Hubs and Switches (Data Packet Switching), Routers – Gateways (Data Packet Routing), Firewall (Security)
  - Client computers, Servers (Used for database creation, Terminal servers).

# Data Package

- In devices within the network infrastructure, data (binary numbering system) is represented by binary bits (1s and 0s). These bits form data packets. They have equal access rights across the communication medium (TCIP).
- What is a Data Packet? A Data Packet is the result of data encapsulation. These (data encapsulation) are packaged data (1/0). Data Packets are also called datagrams.
- What does a data packet consist of? A data packet consists of sender information (address), receiver information (address), and the data it contains. It also has a numerical identification number that defines the packet number and sequence type. When data is sent over the network, this information is divided into data packets. In short, data packets carry information messages (receiver and sender addresses, security), switching, and routing configuration for your transmitted message.

# Computer Network Technologies

- A computer network is a communication network where two or more computer systems are connected to each other for data communication.

- Computer systems within a computer network (computer + NIC – Network interface card: Interface circuit used to connect to the computer network) communicate with each other and share data.
- If a system will be connected to network for data communication, a system has a NIC card. Every NIC card has diferrent identificatioın number.
- Networks created by a limited number of computer systems within a specific area are called LANs (Local Area Networks).
- When networks are large in terms of geographic area and number of users, the concept of WANs (Wide Area Networks) emerges.

# Network Operating Systems

- Network Operating Systems (NOS) are the software that runs a LAN.
- They have two distinct implementations: Server (Computer system + Data storage: master data storage area) NOSs and Client (Client: end user computer) NOSs.
- Server NOSs allow the server to execute and respond to requests sent to them as web servers, print servers, file servers, etc. Client NOS functionality is typically found in most operating system packages.

# Ağ Oluşturmada Protokol

- Ağ oluşturmada protokol, Ağ iletişiminde bir protokol, iki aygıtın birbirine bağlanmasını ve birbirine veri iletmesini sağlayan bir dizi görünmez bilgisayar kuralıdır.

# Raid Nedir?

- RAID, Yedekli Bağımsız Diskler Dizisi anlamına gelir. RAID, hataya dayanıklı disk sistemlerini standartlaştırmak ve kategorize etmek için kullanılan bir yöntemdir. RAID seviyeleri performans, maliyet, güvenilirlik vb. gibi çeşitli olanaklar sağlar. Bu üçü en çok kullanılan RAID seviyeleridir:
- Seviye 0: (Çizgileme)
- Seviye 1: (Yansıtma)
- Seviye 5: (Çizgileme ve Parite)

# The differences between RIP and IGRP

| Basis of Comparison | RIP | IGRP |
|---|---|---|
| **Full form** | RIP stands for routing information protocol. | IGRP stands for interior gateway routing protocol. |
| **Description** | RIP is a distance vector-based routing protocol. | IGRP is a distance vector based interior gateway routing protocol. |
| **Determination of route** | RIP depends on the number of hops to determine the best route to the network. | IGRP considers many factors before decides the best route to take, i.e., bandwidth, reliability, MTU and hops count. |
| **Standard** | RIP is a industry standard dynamic protocol. | IGRP is a Cisco standard dynamic protocol. |
| **Organization used** | RIP is mainly used for smaller sized organizations. | IGRP is mainly used for medium to large-sized organizations. |
| **Maximum routers** | It supports maximum 15 routers. | It supports a maximum 255 routers. |
| **Symbol used** | RIP is denoted by 'R' in the routing table. | IGRP is denoted by 'I' in the routing table. |
| **Administrative distance** | The administrative distance of RIP is 120. | The administrative distance of IGRP is 100. |
| **Algorithm** | RIP works on Bellman ford Algorithm. | IGRP works on Bellman ford Algorithm. |

# RIP'in IGRP'den farkı nedir?

- RIP, bir ağa giden en iyi rotayı belirlemek için atlama sayısına dayanır. Öte yandan, IGRP bant genişliği, güvenilirlik, MTU ve atlama sayısı gibi izlenecek en iyi rotaya karar vermeden önce birçok faktörü dikkate alır.

# Network Architecture

- Refers to how the computer or devices are designed in a network
- Basic types:
  - Centralized – using mainframes
  - Peer-2-Peer: (2: to) (Computers connected end-to-end over a network technology)
    - Each computer (peer) has equal responsibilities, capacities, sharing hardware, data, with the other computers on the peer-to-peer network
    - Good for small businesses and home networks
    - Simple and inexpensive
  - Client/Server:
    - All clients must ***request*** service from the server (Client is a computer that connects to the server via a network technology)
    - The server is also called a ***host***
    - Different servers perform different tasks: *File server*, *network server*, web server, mail server, terminal server, etc.

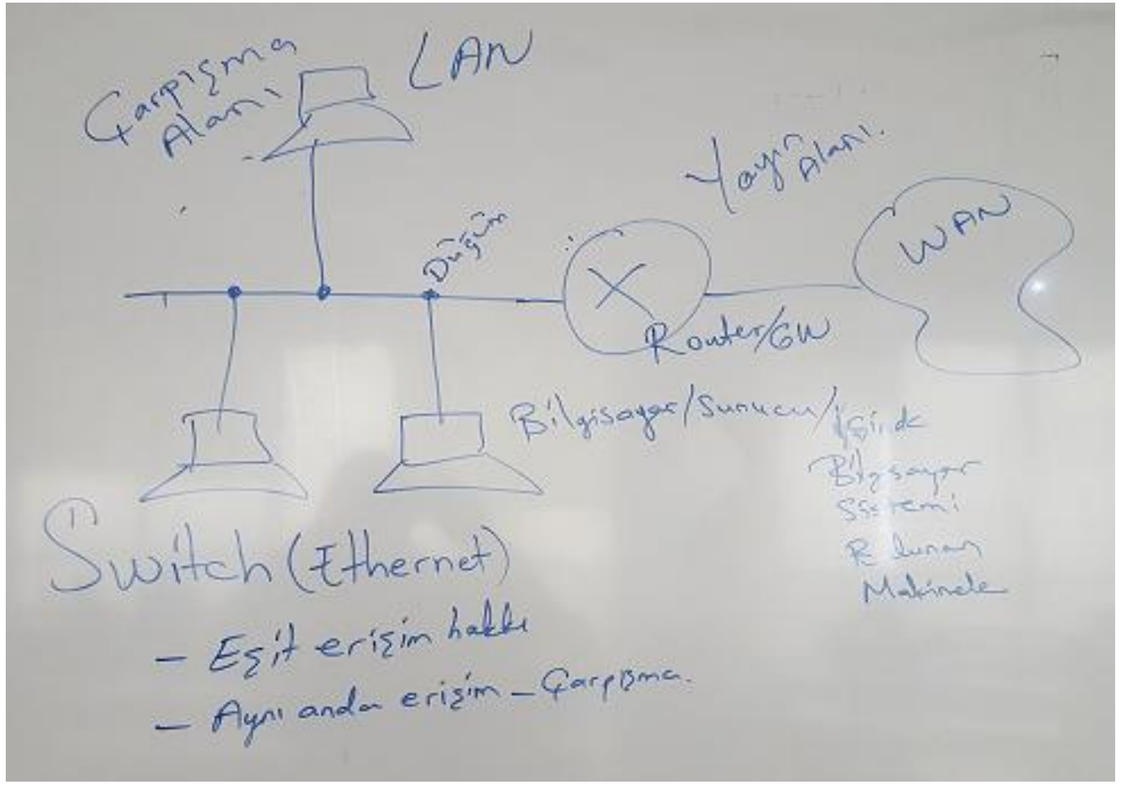
# MTU

- What is MTU? MTU stands for maximum transmission unit and is used to indicate the maximum packet size that can be sent on a data link without requiring fragmentation.

- What does MTU stand for? What is the default size? MTU stands for maximum transmission unit. The default MTU size is 1500 bytes.

# WAN:broadcast area" and LAN collision area

- Difference between "broadcast domain" and "collision domain": (Explain the difference between a 'broadcast domain' and a 'collision domain'?)
- A broadcast domain is a logical portion of a computer network where all nodes (NICs) can reach each other by broadcasting at the data link layer. Example: Router (WAN)
- A collision domain is a portion of a network where data packets can collide with each other while being sent across a shared medium or through repeaters. Example: Ethernet switch (LAN)
- Everyone has equal access to the Ethernet switch circuit. Simultaneous access is possible, and in this case, a conflict occurs. When a data conflict occurs, the conflicting systems generate random time. They dominate the path that produces the shortest time and send data packets.



# HTTP - URL - ISP

**HTTP (Hyper Text Transfer Protocol):**

- HTTP is the protocol that allows us to use the internet and defines web rules.
- Web browsers do not require the use of http://. They automatically add this address.

**URL (Uniform Resource Locators):**

- Web pages on the Internet have an address known as a URL.
- A URL is entered in the address bar of browser programs.
- A URL uses letters and punctuation marks.
- Örnek: http://ckk.com.tr

**ISS(Internet Service Provider):**

- This is the name given to institutions that provide services for connecting to the Internet.

# FTP (File Transfer Protocol)

- It's a protocol that enables file transfers and receipts over the Internet.
- Large companies often share their software installation files this way.
- There are many software programs available for using FTP addresses.
- SmartFTP, FileZilla, and CuteFTP are among the most commonly used.

# UDP - ICMP

- UDP: Another transport layer protocol. It's typically used to transfer small data for query and test purposes. Because the data is small, fragmentation isn't necessary. It's not a secure transmission method. TCP is more secure than UDP because TCP/IP has segments that check whether the packet is corrupted and whether it has arrived.
- ICMP: Sends control messages and provides notification of whether it arrived or not. The PING command uses this protocol to determine whether the receiving computer is up and running.
- IP: Addresses and routes packets.

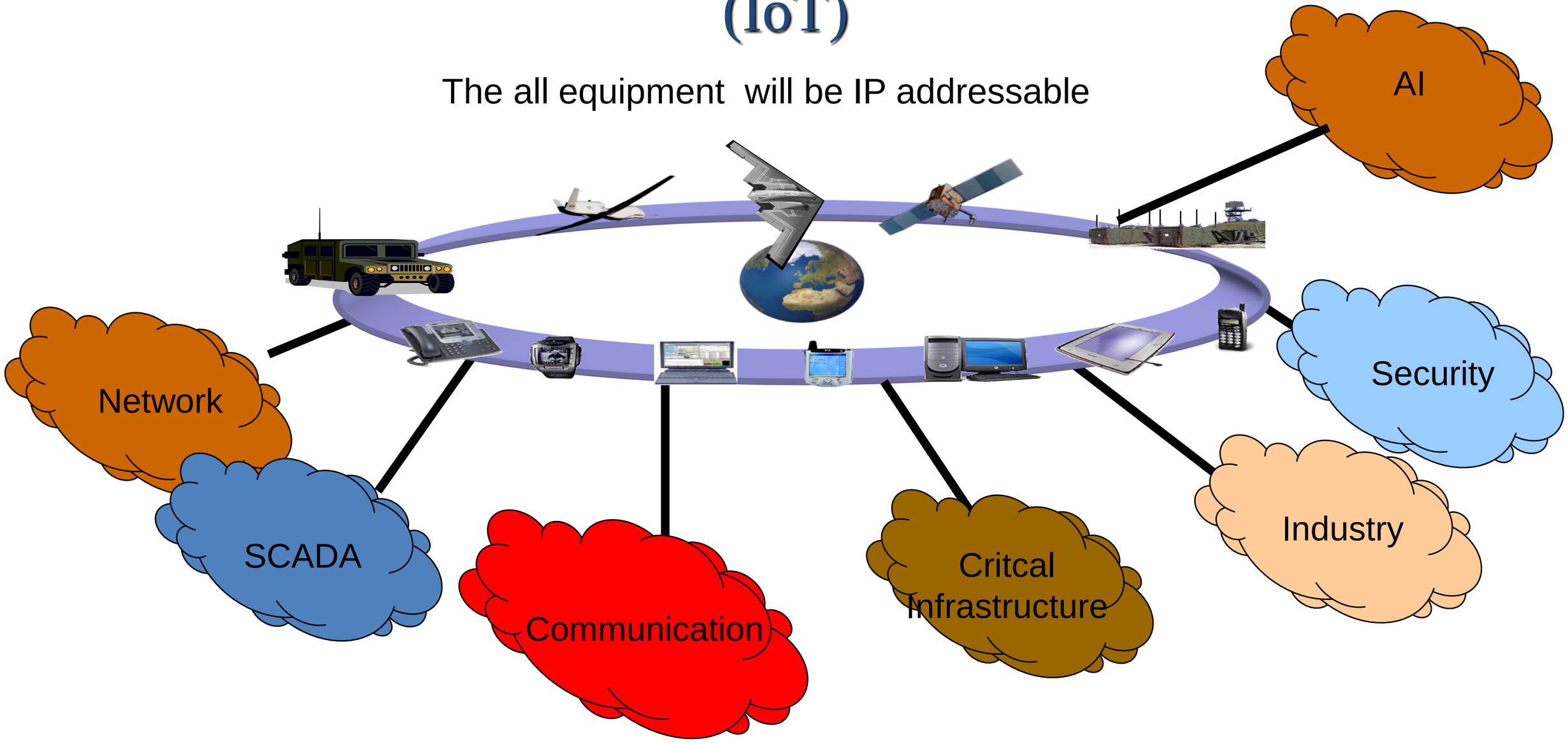
# Networking features

- Topology: This refers to how computers or nodes are arranged in a network. Computers are organized physically or logically.
- Protocols: This refers to how computers communicate with each other.
- Media: These are the systems and environments used by computers for communication.

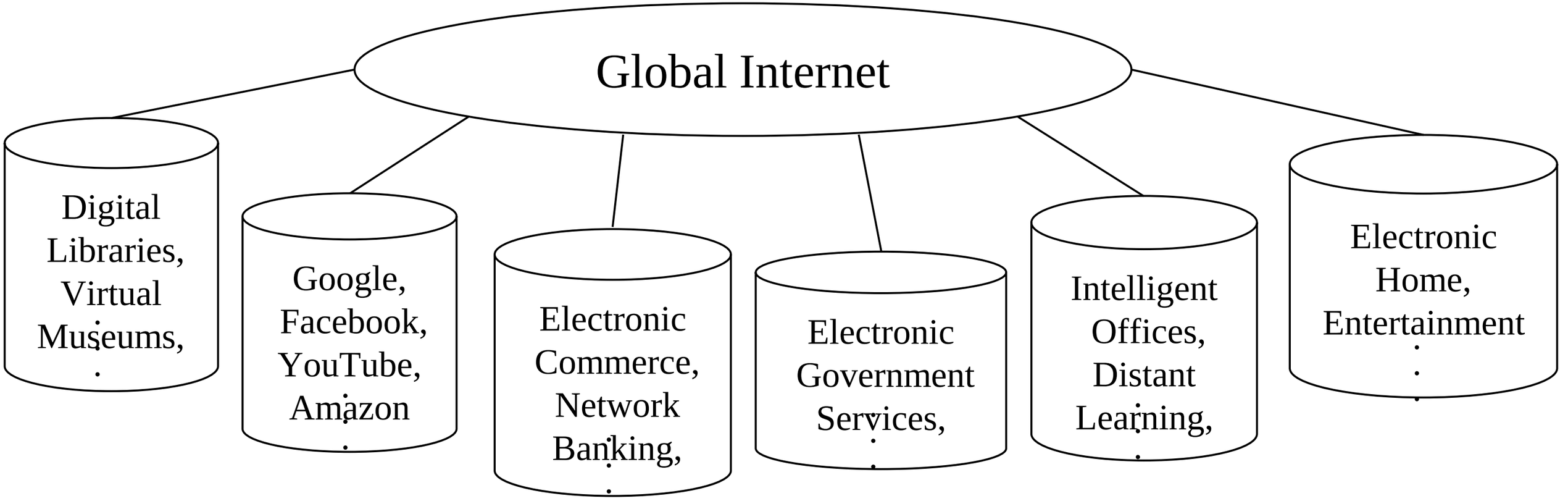
# *Internet*

# Internet: IP – ACCESS MEDIA (IoT)

The all equipment  will be IP addressable



# The Global Internet



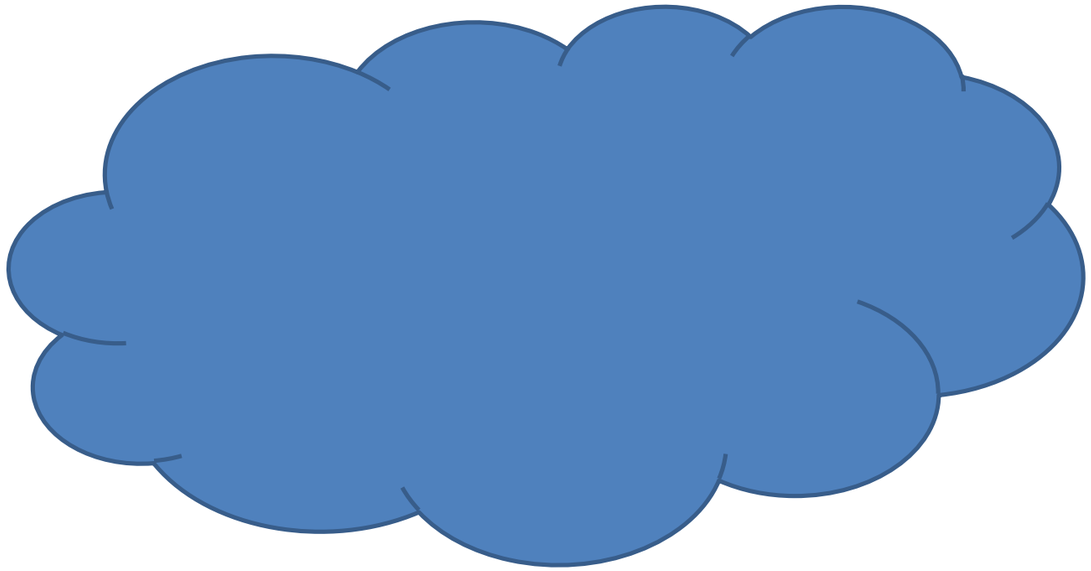
## The Global Internet

- Network technology connects everywhere globally
- Large volumes of information spread around the world in microseconds
- Multi-access environment, multilingual, multifunctional
- Cross-cultural, cross-domain, cross-regional
- Globally integrating all information systems and information-related activities

# Internet Terms

- **Data Packet** – data sent over the internet
- **Hub** – connects other devices to the network and sends packets to all devices connected to it.
- **Bridge –** It connects two network infrastructures. Filtering is applied; data packets are allowed to go to the other side. Not all data packets travel across the two network topologies. It combines two LANs. It creates a single LAN, but each LAN operates independently. Filtering allows data packets to be sent from one LAN to the other when needed.
- **Switches** – connects multiple devices and filters packets based upon destination.
- **Router** – receives and analyzes packets, then route and sends them to specific destinations.

# Cloud Computing

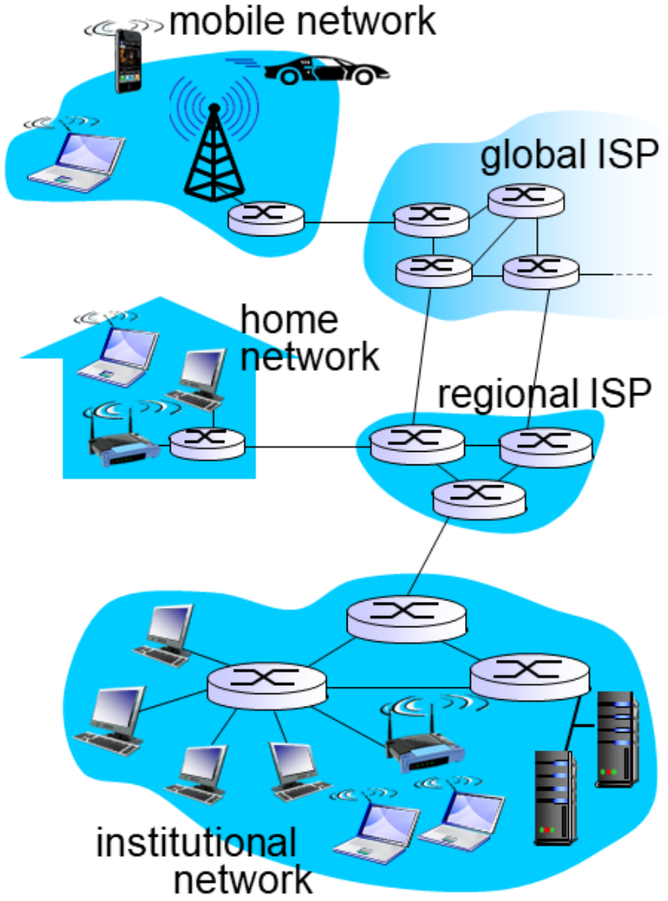


**= Internet**

Do not forget above network diagram.  The Internet is always represented by a cloud. Computing services over the internet.

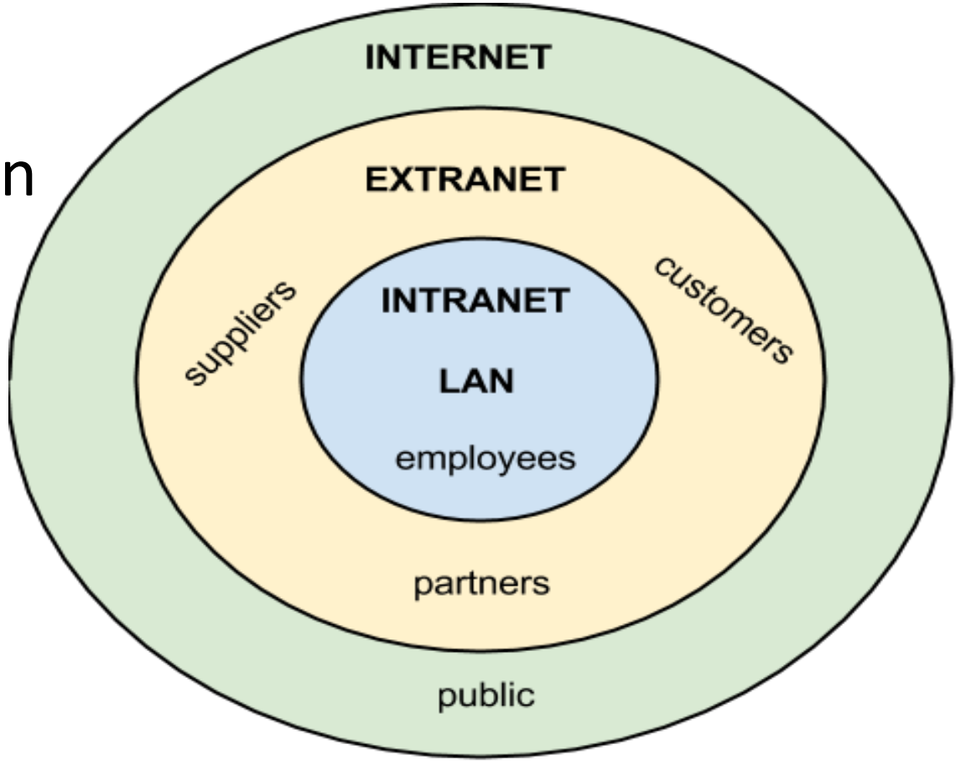
# The Internet

- millions of connected computing devices:
  - *hosts = end systems*
  - running *network apps*
- *communication links*
  - fiber, copper (2 wire or 4 wire), microwave, satellite
  - transmission rate: *bandwidth (B=maximum frequency – minumum frequency in a signal)*
- *Packet switches:* forward packets (chunks of data)
  - *routers* and *switches*
  - *All networks has GW, Router or Ethernet switch.*
- Home network: laptops, Computers, GSM phones, router/GW and switches.
- Mobile Network: GSM phone, laptops, router/GW
- Global or regional ISP: Router, GW, switches
- Institutional network: Computers, servers, laptops, Wireless networks, router, GW, Switches

# Organizational Networking

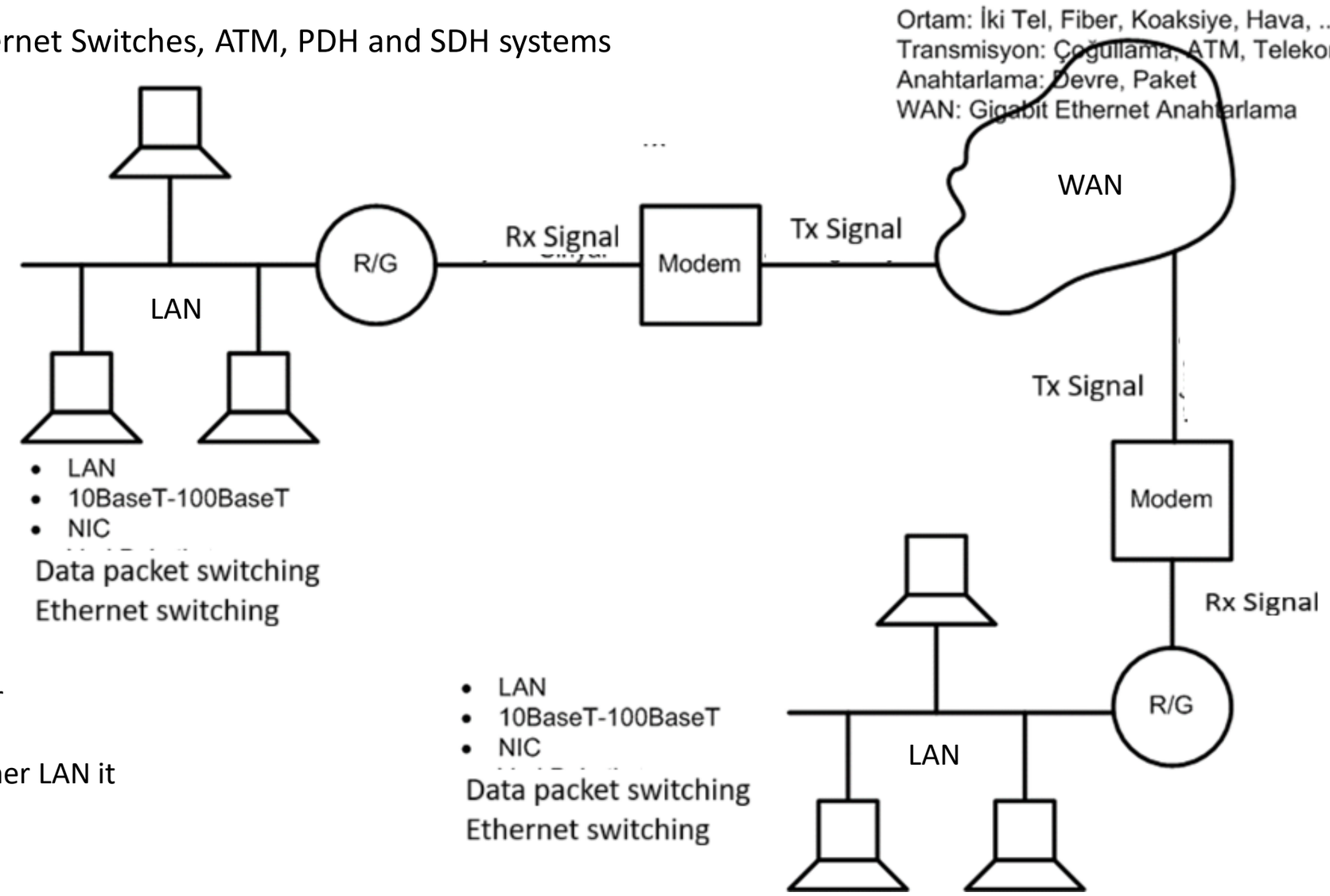
- Intranet – within the organization.
- Extranet – allowing partners into your network for specific things (eg. Supply Chain Management)
- Internet



# LAN - WAN

*communication links:* fiber, copper (2 wire or 4 wire), microwave, satellite. For connection LAN to WAN
WAN equipmet: Router, Gateway, Ethernet Switches, ATM, PDH and SDH systems

A **modem** (short for **mo**dulator–**dem**odulator) is a network device that allows digital devices (like computers, phones, or routers/GW) to communicate over analog communication lines (like telephone lines, cable systems, or fiber networks).
The modem adapts the signal so that it is not affected by the disruptive effects in the communication environment.

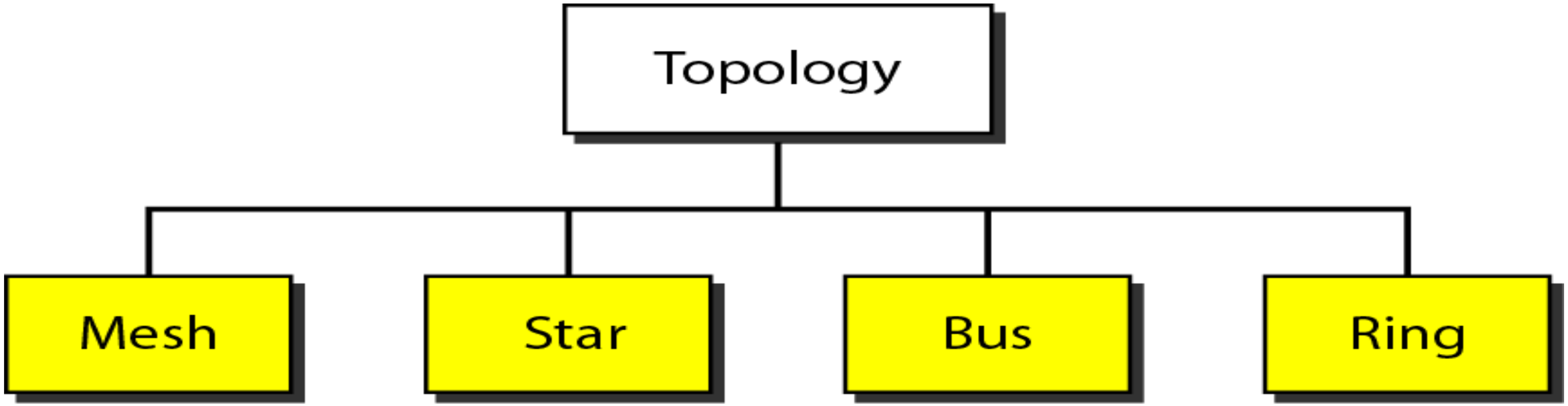



Ethernet switch is enough for computer communiation each other.
If a computer wants to send data to other LAN it is necessary Router or Gateway.

Router/Gateway: Cisco Huawei

# Ağ Topolojileri

*Categories of topology*



# Network Profiles

- Ağ profili, veri dosyaları, yazıcılar vb. Dahil olmak üzere, her bir sunucudaki diğer bilgisayarlar tarafından kullanılmak üzere ağda hangi kaynakların mevcut olduğunu belirtir.
- Ağ profilinde bulunmayan cihazlar ağ üzerinden kullanılamaz.
- Kullanıcı profilleri, bir LAN üzerindeki her bir kullanıcının neye erişimi olduğunu açıklar.
- Çoğu LAN, hangi kullanıcının hangi ağ kaynağına eriştiğini takip eden denetim yazılımı da kullanır.

# Ağ Topolojileri

- Ağ Topolojileri, bir bilgisayar ağının çeşitli öğelerinin (bağlantılar, düğümler vb.) belirli bir sırada düzenlenmesidir. Network'de kullanılan farklı topoloji türleri şunlardır: Bus, Star, Ring, Mesh, Tree, Hybrid
- Pasif topoloji,  ağdaki bilgisayarların yalnızca sinyalleri dinlemesine ve almasına izin verdiğinde, sinyalleri zaten yükseltmedikleri için pasif topoloji olarak bilinir.

# Ağ Yapılarına (Topoloji) göre Ağların Sınıflandırılması

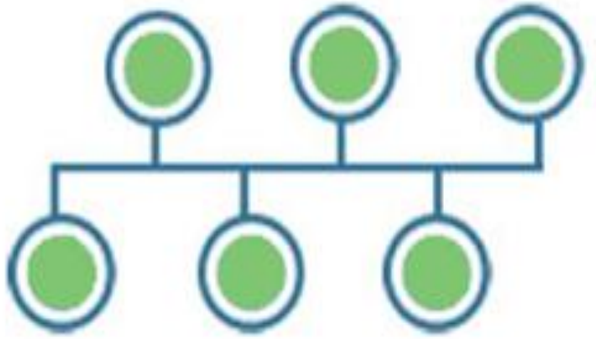
- Topoloji, bir ağdaki bilgisayarların nasıl yerleşeceğini, nasıl bağlanacağını, veri iletiminin nasıl olacağını belirleyen genel yapıdır.
- Topoloji iki temel gruba ayrılır.
  - Fiziksel topoloji: Ağın fiziksel olarak nasıl görüneceğini belirler (Fiziksel katman)
  - Mantıksal topoloji: Bir ağdaki veri akışının nasıl olacağını belirler (Veri iletim katmanı)
- Temel Topoloji Türleri
  - (Bus Topology)
  - (Ring Topology)
  - (Star Topology)
  - (Tree Topology)
  - (Mesh Topology)

LAN

WAN

# Bus Topolojisi

- Bus topolojisi, tüm düğümlerin merkezi kablo veya bus olarak bilinen tek bir haberleşme ortamına (kabloya) bağlandığı bir ağ topolojisidir.
- Haberleşme ortamı tekdir. Veri paketi göndermek isteyen bilgisayar sistemi ortamda paket yok ise veri paketini ortama bırakır. Herkesin eşit erişim hakkı var. Aynı anda veri paketi bırakma olduğunda çatışma olur. Bu durumda çatışmaya girmeyen bilgisayar sistemleri, sistem normale dönüşünceye kadar beklerler. Çatışmaya giren bilgisayar sistemleri rasgele zaman üretirler, en kısa zamanı üreten ortama veri paketini bırakır.
- Paylaşılan bir iletişim ortamı görevi görür, yani herhangi bir cihaz verileri diğer cihazlara göndermek isterse, verileri veri yolu üzerinden gönderir ve bu da verileri bağlı tüm cihazlara gönderir.
- Bus topolojisi, az sayıda cihaz için kullanışlıdır. Bus hasar görür ise tüm ağ başarısız olur.



Bus

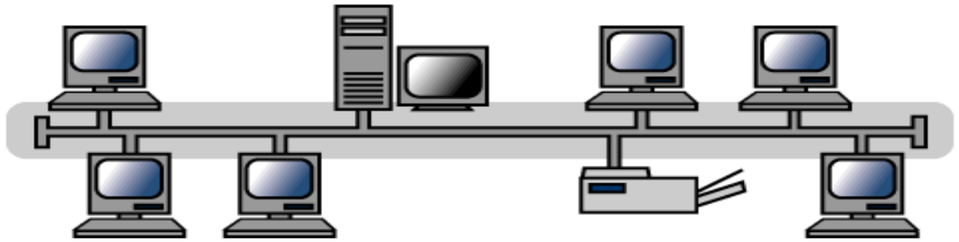
# Doğrusal (Bus) Topoloji

- Bu topoloji yayın (broadcast) felsefesi izler.
- Bus topolojisinde tek bir iletişim ortamı (örneğin bir kablo), düğümlerin birbirleriyle iletişimini sağlar.
- Bus topolojide genellikle Ethernet kartları kullanılmaktadır.
- İstasyonlar (düğümler) veri yoluna  tap adı verilen bir bağ ile bağlanmışlardır.
- İstasyonlar ve arabirimler ile iletişim ortamı arasında çift-yönlü bir iletişim (full-duplex) vardır.
- Veri yolunun başlangıç ve bitişi birbirine bağlı değildir.
- Bu topolojide her düğüme bir adres verilir ve bu yapıdaki bir ağda veri herhangi iki düğüm arasında iletilebilir.
- Ancak iletişim, bir zaman biriminde yalnızca bir çift düğüm arasında gerçekleşebilir.
- İletişimde bulunan düğümler veri yolunu iletim süresince işgal eder.
- Bundan dolayı her istasyon mesaj göndermeden önce veri yolunu kontrol ederek herhangi bir mesaj olup olmadığına bakar.
- Aynı iletişim ortamı tüm düğümlerce paylaşıldığı için, mesajlar gönderildiği düğümün adresiyle iletilir.

# Doğrusal Topolojinin Avantajları ve Dezavantajları

Avantajları:

- Ağa bir bilgisayarı bağlamak oldukça kolaydır
- Daha az uzunlukta kablo gerektirir.
- Bir bilgisayarda oluşacak hata tüm ağı etkilemez.
- Merkez birime ihtiyaç duyulmaz.



Dezavantajları:

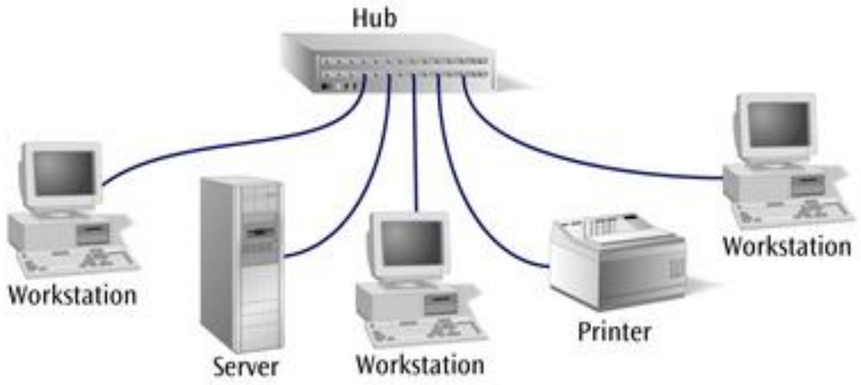
- LAN Omurga kabloda bir bozulma veya kesilme olursa tüm ağ bağlantısı kesilir.
- Kablonun sonunda sonlandırıcı (Terminator) olmalıdır.
- Ağda sorun olduğunda sorunun nerden kaynaklandığını bulmak zaman alıcı olabilir.
- Tek başına tüm bir binanın ağ çözümü için genellikle kullanılmamaktadır.
- Bilgisayar sayısı aşırı arttığında veri paketlerinde çarpışma sayısının artma olma olasılığı yüksektir.
- Maksimum sınırlı sayıda bilgisayar sistemi bağlanabilir.

# Star Topolojisi

- Yıldız topolojisi, tüm düğümlerin merkezi cihaz olarak bilinen tek bir cihaza bağlı olduğu bir ağ topolojisidir.
- Yıldız topolojisi, diğer topolojilere göre daha fazla kablo gerektirir. Bu nedenle, bir kablodaki arıza yalnızca bu kabloya bağlı belirli bir bilgisayarın bağlantısını keseceğinden daha sağlamdır.
- Merkezi cihaz hasar görürse, tüm ağ başarısız olur.
- Star topolojisinin kurulumu, yönetimi ve sorun gidermesi çok kolaydır.
- Yıldız topolojisi, ofis ve ev ağlarında yaygın olarak kullanılmaktadır.

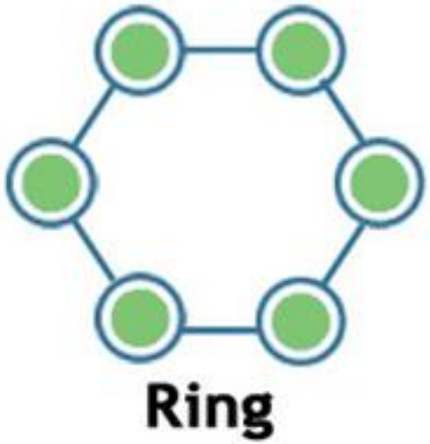
# Yıldız (Star Topology)

- Tüm düğümlerin ortak bir merkeze (örneğin, hub, switch) bağlanmasıdır.
- Ağa bağlanan her cihaz için bir kablo çekilmesi gereklidir.
- Switch ya da hub'a bir şey olduğunda tüm ağ çalışmaz hale gelir.
- Ağın genişletilmesi switch'ın yada hub'ın kapasitesine bağlıdır.
- Sistem performansı da switch ya da hub'ın veri yolu kapasitesine bağlıdır.



# Ring Topolojisi

- Halka topolojisi, düğümlerin tam olarak iki veya daha fazla düğüme bağlandığı ve böylece iletim için tek bir sürekli yol oluşturan bir ağ topolojisidir.
- Düğümler arasındaki bağlantıyı kontrol etmek için herhangi bir merkezi sunucuya ihtiyaç duymaz.
- Tek düğüm hasar görürse, tüm ağ başarısız olur.
- Ring topolojisi pahalı, kurulumu ve yönetimi zor olduğundan çok nadiren kullanılır.
- **Ring topolojisine örnek olarak SONET ağı, SDH ağı vb. verilebilir.**



# Halka (Ring Topology)

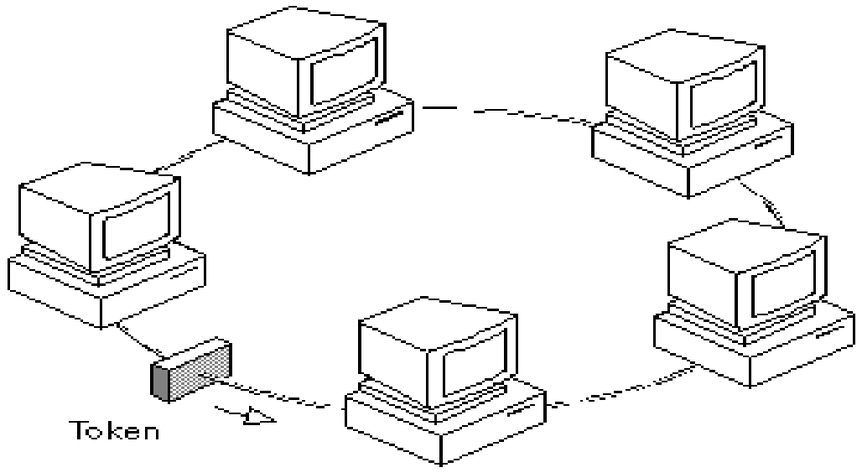
- Halka ağların düzgün çalışabilmesi için 3 fonksiyona ihtiyacı vardır.
  - Verinin gönderilmesi
  - Gönderilen verinin alınması
  - Verinin silinmesi
- Verinin gönderilmesi durumunda yineleyici, gönderilecek olan bitleri bilgisayardan alır, yeniden oluşturur ve bağlantıya yönlendirir.
- Gelen mesaj, alıcı adresi o düğüm ise saklanır.
- Veri halka boyunca taşınıp vericiye tekrar geldiğinde ise silinmelidir (halkadan atılmalıdır).
- Bu topolojide yineleyici gibi çalışan ağ düğümleri noktadan noktaya bağlantılarla ağa bağlanmışlardır.
- İletişim bağlantısının başlangıç ve bitişleri birbirlerine bağlanmıştır.
- Veriler paket halinde gönderilir ve halka boyunca tek yönde iletilir.
- Yineleyici hattın üzerindeki veriyi bit bit alarak, bekletmeden diğer tarafa iletir.
- Halkayı birçok bilgisayar paylaştığından hangi bilgisayarın paketinin halka üzerinde iletileceğinin kontrol etmek amacıyla mekanizmalar geliştirilmiştir.
- Buna örnek olarak jetonlu halka (token ring) verilebilir.

# Halka Topolojinin Avantaj ve Dezavantajları

- Bekleme süresi devredeki eleman sayısına bağlıdır.
- Sistemin hızı devreye eklenen her elemanla biraz daha azalır.
- Her PC bilgisayar ağının bir elemanı olduğu için PC'de bir aksaklık olması halinde network durur. Paralel bir ikinci hattın (by pass hattı) çekilmesiyle bu soruna çözüm bulmak mümkündür.
- Hem ağın yayıldığı tüm alan hem de bilgisayarlar arası mesafe sınırlıdır.
- Maliyet bakımından diğer ağlardan biraz daha pahallıdır.
- İletişim hızları kablolama sisteme bağlıdır.

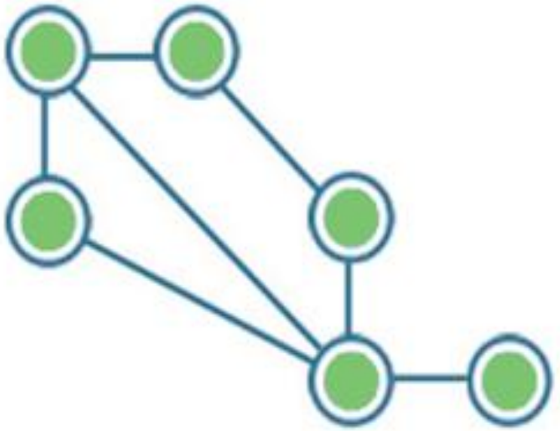
# Jetonlu Halka (Token Ring Topology)

- Bu tip topolojide iletişim ağ içerisinde sürekli dönen jeton (token) yardımıyla yapılır.
- Jeton özel iletişim kodu ile iletişimi düzenler.
- Token (Jeton) (3 byte'lık) düğümler arasında dolaşan bilgidir.
- İletişime başlamak isteyen düğüm öncelikle jeton'un kendisine ulaşmasını bekler ve ulaştığında jeton'u alır.
- Artık jeton serbest dolaşımdan kullanıma geçmiş olur. Bilgi gönderildikten sonra alıcıya gelene kadar halka etrafında dolaşır.
- Halka topoloji de genel yayın amaçlı (broadcast) uygulamalar için uygundur.



# Mesh Topolojisi

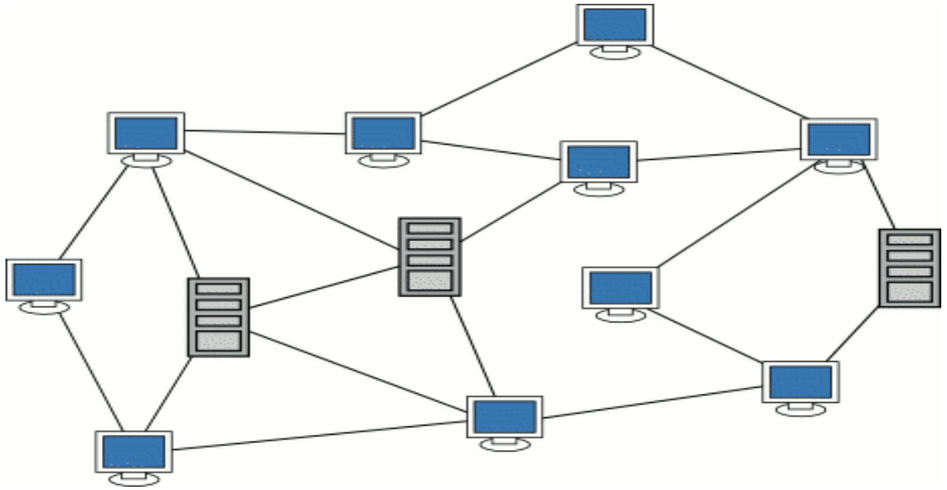
- Mesh topolojisi, tüm düğümlerin ayrı ayrı diğer düğümlere bağlandığı bir ağ topolojisidir.
- Düğümler arasındaki bağlantıyı kontrol etmek için herhangi bir merkezi anahtara veya hub'a ihtiyaç duymaz.
- Mesh topolojisi iki kısma ayrılır:
  - Tam bağlantılı ağ topolojisi: Bu topolojide tüm düğümler birbirine bağlıdır.
  - Kısmi bağlantılı ağ topolojisi: Bu topolojide tüm düğümler birbirine bağlı değildir.
- Sağlamdır, çünkü bir kablodaki bir arıza, yalnızca bu kabloya bağlı olan belirtilen bilgisayarın bağlantısını kesecektir.
- Ağ topolojisi, bağlantı arttığında kurulum ve konfigürasyon zor olduğu için nadiren kullanılır.
- Toplu kablolama gerektirdiğinden kablolama maliyeti yüksektir.



Mesh

# Örgü (Mesh Topology)

- Tipik olarak mesh topolojisi en geniş ya da en önemli yerlerin bağlandığı hibrid ağlarda kullanılır.
  - Örneğin bir kuruluşun 4 veya 5 ana merkezi ile çok sayıda uzak ofisi olduğunu varsayalım.
  - Her bir ana merkezde  birer mainframe ve bu mainframelerin dağıtık bir veritabanı idare etmek için iletişim kurmak zorunluluğu olsun.
  - Mainframeler arası iletişimden emin olabilmek için merkezler arasında artık hatlar içeren bir hybrid mesh topoloji kullanmak gerekir.



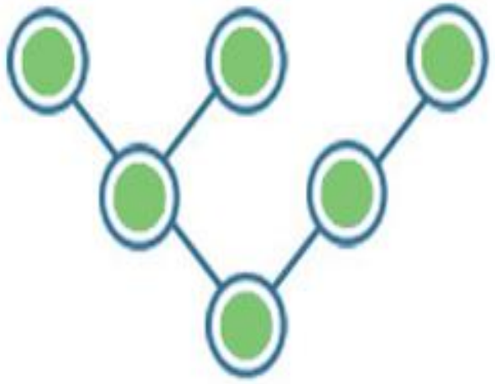
Gerçek Mesh Topoloji



Hibrid Mesh Topoloji

# Tree Topolojisi

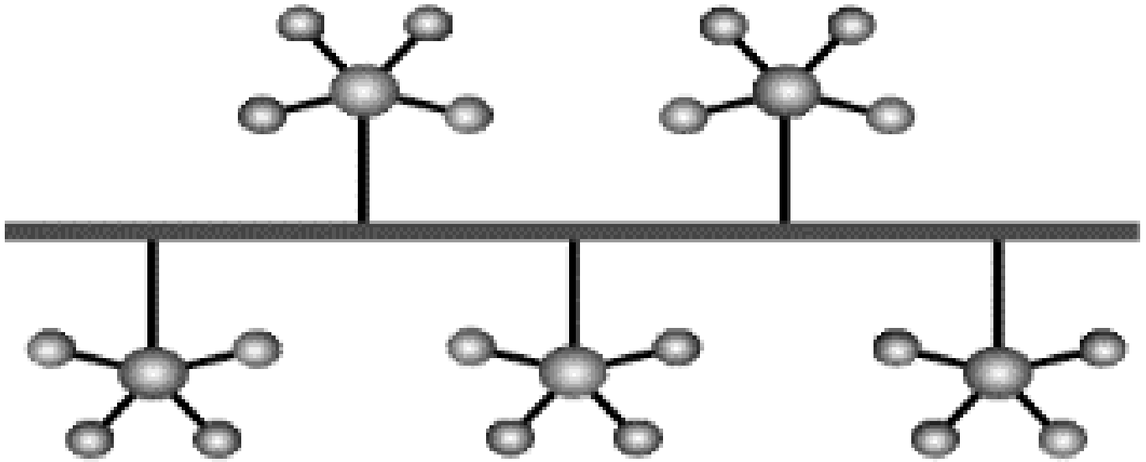
- Ağaç topolojisi, yıldız ve veri yolu topolojisinin bir birleşimidir. Genişletilmiş yıldız topolojisi olarak da bilinir.
- Ağaç topolojisinde tüm yıldız ağları tek bir veri yoluna bağlıdır.
- Bu topolojide Ethernet protokolü kullanılmaktadır.
- Bunda, tüm ağ, kolayca korunabilen yıldız ağları olarak bilinen bölümlere ayrılmıştır.
- Bir segment hasar görmüşse, ancak diğer segmentler üzerinde herhangi bir etkisi yoktur.
- Ağaç topolojisi "ana veri yoluna" bağlıdır ve bozulursa tüm ağ zarar görür.



Tree

# Ağaç (Tree Topology)

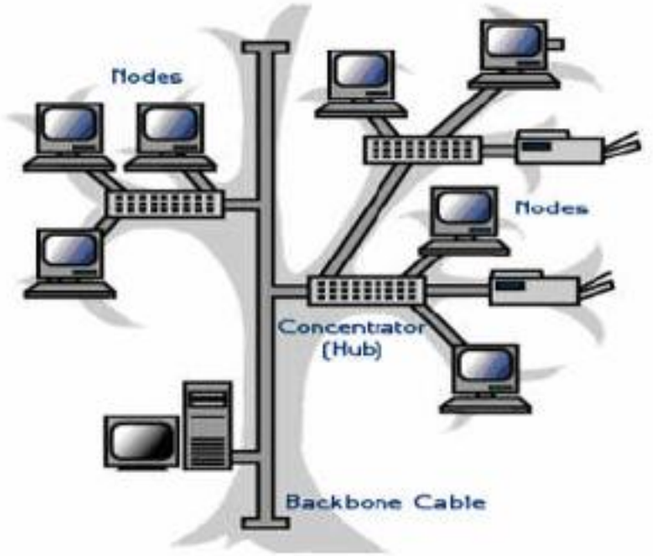
- Ağaç topolojisi Bus ve yıldız topolojilerinin karakteristiklerini birleştirir.
- Bus omurga üzerinde yıldız topolojide bilgisayarlardan oluşur.
- Böylece ağlar büyütülebilir.
- Bir ağacın dalları farklı topolojilerdeki ağları temsil eder, ağacın gövdesi ile de bunlar birbirine bağlanabilir.



Tree network

# Ağaç (Tree Topology)

- Ağaç topolojisinin diğer adı hiyerarşik topolojidir.
- Ağacın merkezinde sorumluluğu en fazla olan bilgisayar bulunur.
- Dallanma başladıkça sorumluluğu daha az olan  bilgisayarlara ulaşılır.
- Bu topoloji çok büyük ağların ana omurgalarını oluşturmakta kullanılır.
- Ağaç topolojisi de  yol topolojisine benzer İletim ortamı kapalı döngüsü olmayan ve dallanan bir kablodur.
- Ağaç düzeni kablo başı (headend) olarak bilinen bir noktadan başlar.
- Herhangi bir istasyondan gelen iletim, ortam boyunca yayılır, diğer tüm istasyonlar tarafından alınabilir ve uç noktalarda yok edilir.
- Halkada olduğu gibi iletim, adres ve kullanıcı bilgisini içeren paketler şeklindendir.
- Her istasyon ortamı izler ve kendisine adreslenen paketleri kopyalar.
- Tüm istasyonlar ortak bir iletim bağlantısını paylaştıklarından bir zaman diliminde yalnızca bir istasyon iletimde bulunabilir ve erişimi düzenlemek için ortama erişim kontrol tekniğine ihtiyaç vardır.



# Ağaç Topolojisinin Avantaj ve Dezavantajları

- Avantajları:
  - Her bir bölüme (segment) ulaşmak kolaydır
  - Bir çok çalışma grubu bir araya getirilebilir.
- Dezavantajları:
  - Her bir bölümün uzunluğu kullanılan kablo ile sınırlıdır.
  - Omurga kablosu bozulduğunda bölümlerdeki ağ trafiği etkilenir.
  - Kurulumu ve düzenlenmesi daha zordur.

# Hybrid Topolojisi

- Bir hibrit topoloji, ortaya çıkan bir topoloji oluşturmak için farklı topolojilerin bir kombinasyonudur.
- Yıldız topolojisi başka bir yıldız topolojisine bağlıysa, yıldız topolojisi olarak kalır.
- Yıldız topolojisi farklı topoloji ile bağlanırsa Hibrit topoloji olur.
- Farklı bir ağ ortamında uygulanabildiği için esneklik sağlar.
- Bir topolojinin zayıflığı göz ardı edilir ve yalnızca gücü dikkate alınır.

# Topolojilerin Karşılaştırılması

| Topoloji | Kurulum | Düzenleme | Sorun çözme | Veri aktarımında problem |
|---|---|---|---|---|
| Doğrusal | Çok kolay | Kısmen zor | Zor | Tek bir kablo, kabloda problem veri aktarımını etkiler |
| Halka | Kısmen Kolay | Kısmen zor | Kolay | Halkadaki bozukluk veri aktarımını etkiler |
| Yıldız | Kolay, ancak zaman alıcı | Kolay | Kolay | Tek bir kablodaki bozukluk bir pc'yi etkiler |
| Ağaç | Zor | Zor | Kolay | Oldukça az |
| Karmaşık | Zor | Zor | Kolay | Oldukça az |

# *Computer Networks*

# Computer network

- The Internet: A computer network that connects computers. Internet is a data communication medium.
- A computer network enables computer systems on the network to communicate with each other and share information.
- The Internet, which provides an international infrastructure and standard for information sharing, has also added new dimensions to communication.

# Network Concepts

- LAN (local area network): A local area network established for computers to communicate with each other within a specific region.
- WAN (wide area network): A network containing computers, etc., located in different regions.
- ROUTER (router): Devices that direct or route data packets according to their intended addresses.
- QOS (quality of service): A device that recognizes data packets and prioritizes voice or video calls by passing both voice and data.
- VOIP (voice over IP): Voice communication using the IP protocol.
- GATEWAY (gateway): Devices that provide routing with QoS services in an internet network.
- VPN (Virtual Private Network): A private, secure virtual network that connects institutions or locations, creating a local network.

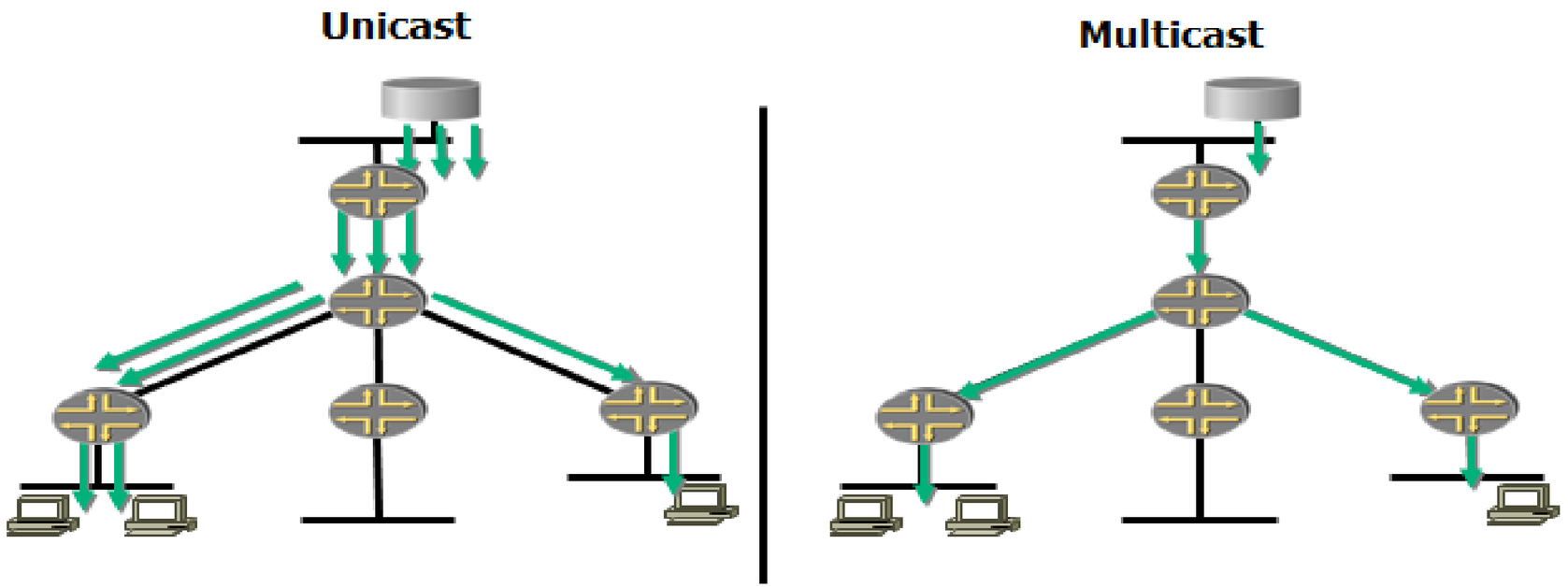
# Equipment by Network Classes

Computer networks are generally classified according to their distance from each other, service type, or density.

- Local Area Networks (LAN): Ethernet Switch
- Wide Area Networks (WAN):
  - Packet Switching:  Ethernet Switch, ATM
  - Routing: Router, GW
  - Circuit Switching: TDM (E1), SDH, PDH
  - Modems:
- Metropolitan Area Networks (MAN): Giga Switch, Router, GW, Modems
- Personal Area Networks (PAN/BAN): ADSL, FTTH, Switch, Bluetooth, Mobile Data
- ADSL: Modem, GW, Switch, Wireless LAN access, Firewall

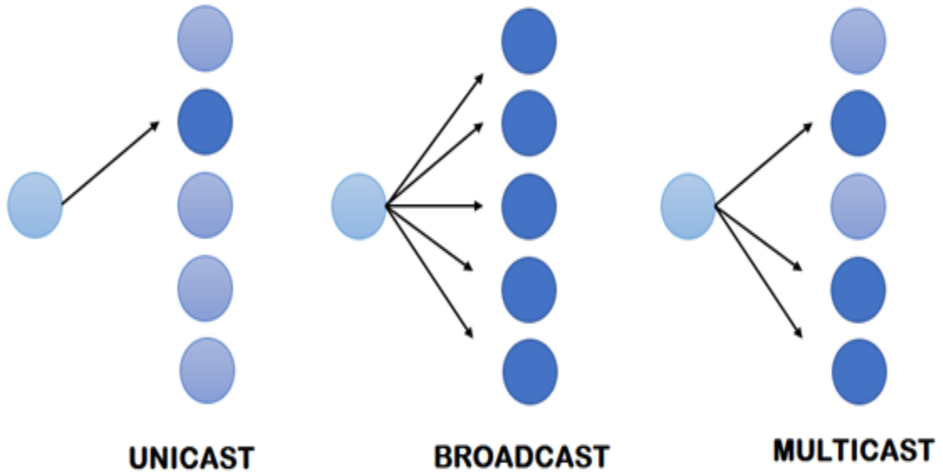
# Broadcast networks…

- If a packet is sent from a server (host)  to only one computer, it's called unicasting.
- If it's sent from a server (host) to more than one computer, it's called multicasting.
- If it's sent to all computers, it's called broadcasting.



# Tek noktaya yayın, çok noktaya yayın, yayın

- Tek noktaya yayın - Bire bir (Unicast),
- Çok noktaya yayın (Multicast),
- Yayın (Broadcast)
- Tüm bu üç terimde, 'cast', veri paketlerinin istemciden alıcıya iletişim kanalı üzerinden iletilmesini ifade eder.



# Tek noktaya yayın – Bire bir (Unicast)

- Ağdaki tek bir gönderici ile tek bir alıcı arasında veri iletişiminin gerçekleştiği bire bir iletişim tekniğidir.
- Bire bir iletişimi belirtir.
- Ağda bulunan iki cihaz arasında veri iletişiminin gerçekleştiği bir iletişim tekniğidir.
- İnternette gezinmeye bir örnek düşünün. Web sunucusuna bir sayfa için istek gönderdiğimizde, istek doğrudan istenen sayfanın adresini bulmak için web sunucusuna gider. Bu nedenle, bu istemci ve sunucu arasındaki bire bir iletişimdir.
- Dosyaları FTP sunucusundan indirmek de tek noktaya yayın iletişiminin en iyi örneğidir.
- Tek noktaya yayın örnekleri şunlardır:
  - Bir web sitesinde gezinme. Web sunucusu göndericidir ve bilgisayarınız alıcıdır.
  - FTP Sunucusundan dosya indirme. FTP Sunucusu göndericidir ve bilgisayarınız alıcıdır.

# Çok noktaya yayın - Birden Çoka  (Multicast)

- Çok noktaya yayın, birden çok gruba veya bire çok iletişimi belirtir. Çok noktaya yayında, bir veya daha fazla gönderici ve bir veya daha fazla alıcı veri aktarımına katılır. IP çok noktaya yayın trafiği bir gruba gönderilir ve çok noktaya yayın trafiğini yalnızca o grubun üyeleri alır. Grubu tanımlamak için IGMP (İnternet Grup Yönetim Protokolü) protokolünü kullanır.
- Çok Noktaya Yayın Örnekleri: Belirli bir posta grubuna e-posta gönderme.

- Bire bir iletişimi belirtir.
- Bir grup cihaz arasında veri iletişiminin gerçekleştiği bir iletişim tekniğidir.
- Multicast, grubu tanımlamak için IGMP(Internet Group Management Protocol) protokolünü kullanır.
- Bir video konferans örneğini düşünün. Belirli bir gruptaki herhangi bir kullanıcı aramayı başlatabilirse ve bu gruba ait kişiler bu aramaya katılabilir.
- Belirli bir posta grubuna e-posta göndermek de çok noktaya yayın iletişimi örneği olarak kabul edilebilir.

# Yayın - Bire Tüm (Broadcast)

- Bire bir iletişimi belirtir. Veri iletişimi, ağda bulunan tüm cihazlar arasında gerçekleşir. Veriler bir bilgisayardan bir kez gönderilir ve bu verilerin bir kopyası bağlı tüm cihazlara iletilir. İki tür Yayın vardır: Sınırlı Yayın ve Doğrudan Yayın.
- Yayın Örneği:  Video ve ses dağıtımı için televizyon ağları.
- Bire bir iletişimi belirtir.
- Ağda bulunan tüm cihazlar arasında veri iletişiminin gerçekleştiği bir iletişim tekniğidir.

**Yayın iki şekilde gerçekleştirilebilir:**

1. Üst düzey bir standart, yani Mesaj iletme arayüzü kullanarak. Birden fazla bilgisayar arasında mesaj alışverişi yapmak için kullanılan bir arayüzdür.
2. Düşük seviyeli bir standart kullanarak, yani bir ethernet üzerinden yayın yaparak.

Ağ, yayında güvenli değildir, çünkü davetsiz misafirlerin ağa saldırması durumunda veri kaybına neden olabilir.

**'Yarım çift yönlü' ve 'tam çift yönlü' sistem arasındaki fark nedir?** Yarım dupleks bir sistemde iletişim yalnızca bir yönde gerçekleşirken, tam çift yönlü bir sistemde iletişim her iki yönde de gerçekleşir.

# Major types of networks

- There are two major type of networks:
  - Server-based network and (Server: Verilerin depalandığı sunucu)
  - Peer-to-peer network.

# Host

- Host: A computer or other computer-controlled device connected to a network. A host computer can also function as a server that provides information resources, services, and applications to users or other hosts on the network. It is a participating computer. Participating computers are assigned at least one network address.
- A computer participating in networks that use the Internet protocol suite can also be called an IP host. Specifically, computers participating on the Internet are called Internet hosts.
- Internet hosts and other IP hosts have one or more IP addresses assigned to their network interfaces. Addresses are configured manually by an administrator, automatically at startup via Dynamic Host Configuration Protocol (DHCP), or through stateless address autoconfiguration methods.
- Network participating computers participating in applications that use the client-server computing model are classified as either server or client systems. Network hosts can also function as nodes in peer-to-peer applications, where all nodes share and consume resources in a coordinated manner.

# peer-to-peer communication

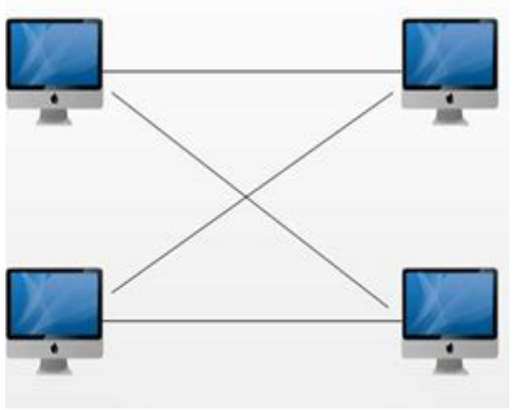
- Peer-to-peer communication eliminates the need for a central database by allowing each user to create their own database.
- In peer-to-peer communication, each participant (host) can share files with the other user outside of a server-client structure.
- Multiplayer games, internet telephony, video telephony, internet radio, and, by their very nature, email utilize peer-to-peer communication.

# Peer to Peer Communication Networks

- Peer-to-peer networks do not use dedicated servers.
- Any computer in a peer-to-peer network can act as a client, accessing resources or information on other computers in the network, or as a server, allowing access to additional information or resources.
- Peer-to-peer networks tend to be smaller networks.
- The main advantage of peer-to-peer networking is lower cost, as there is no dedicated server, which is typically the most expensive network component.
- The main disadvantage is that peer-to-peer networks are generally slower than dedicated server networks because each computer is less powerful and can be in use as both a client and a server simultaneously.

# Eşler Arası Ağ (Peer-to-Peer Network –P2P)

- Eşler arası bir ağda, 'eşler' bir internet bağlantısı aracılığıyla birbirine bağlanan bilgisayarlardır.
- Herhangi bir bilgisayar sunucusuna ihtiyaç duymadan ağ üzerindeki bilgisayar sistemleridir.
- Bu nedenle, P2P'deki bilgisayar bir "bilgisayar sunucusu" ve aynı zamanda bir "istemci"dir.
- Bir bilgisayarın eşler arası ağa sahip olması için gereksinimler, internet bağlantısı ve P2P yazılımıdır.
- Yaygın P2P yazılım eşlerinden bazıları Kazaa, Limewire, BearShare, Morpheus ve Acquisition'dır.
- P2P ağına bağlandıktan sonra, diğer insanların bilgisayarındaki dosyaları arayabiliriz.



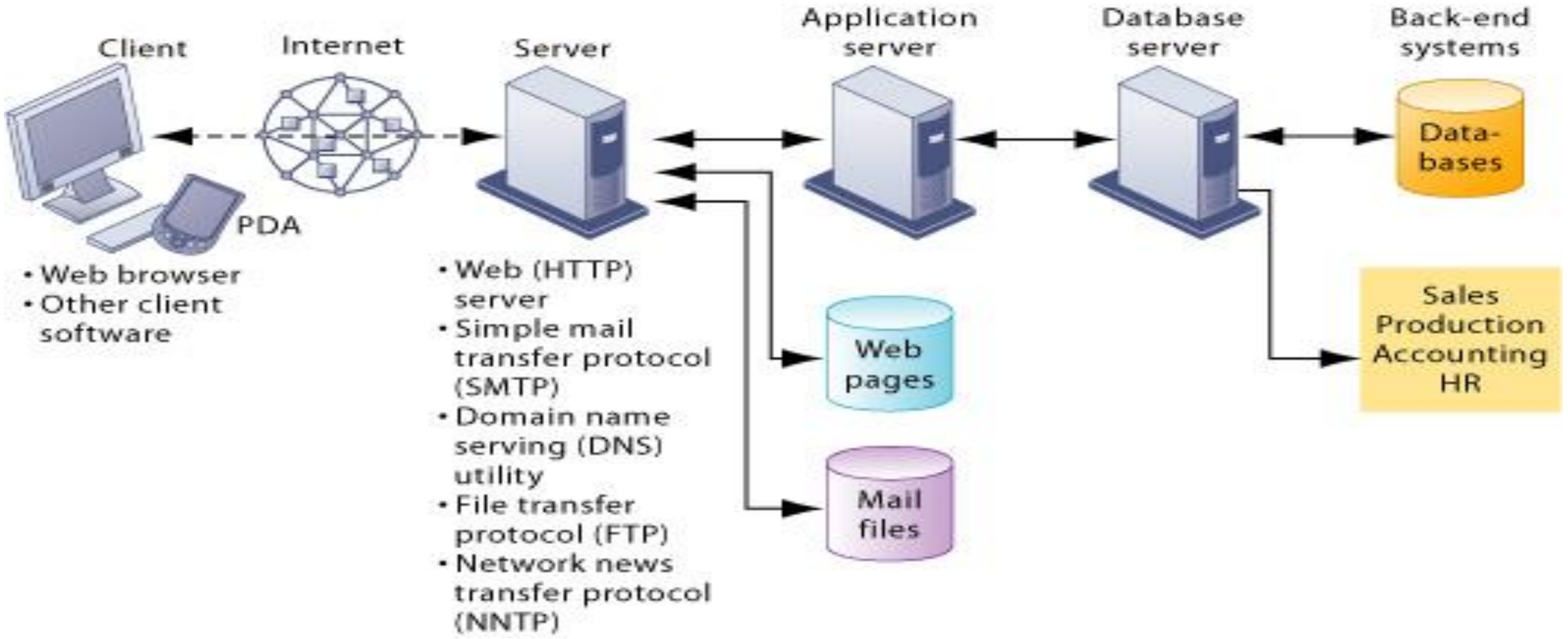
**Eşler arası ağ türleri:**

- Saf P2P: P2P'de eşler bir istemci ve sunucu görevi görür. Saf P2P'de merkezi sunucu ve merkezi yönlendirici yoktur.
- Hybrid P2P: Hybrid P2P, bilgileri depolayan ve bu bilgi talebine yanıt veren merkezi bir sunucuya sahiptir. Eşler, bilgileri merkezi bir sunucu olarak barındırmak için kullanılır, dosyaları saklamaz. Nasper, Hybrid P2P'nin bir örneğidir.
- Karışık P2P: Karışık P2P, saf P2P ve Hibrit P2P'nin bir kombinasyonudur.

# What are proxy servers and how do they protect computer networks?

- Proxy servers prevent external users from identifying the IP addresses of an internal network.
- They make a network virtually invisible to external users, who cannot identify the physical location of a network without knowledge of the correct IP address.

# Client/server Computing on the Internet

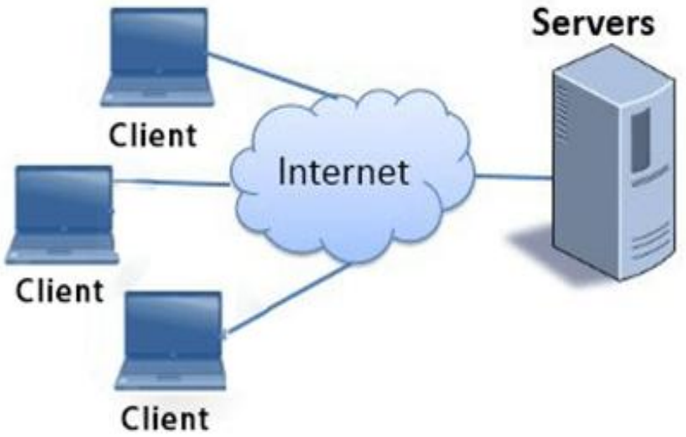


# What is a client-server model?

- The client-server model or architecture is a communication framework for network processes. This framework is distributed among service requesters, customers, and service providers, providing them with transparent access across multiple platforms to applications, data, computing services, or any other resource within the workgroup and/or organization.

# Sunucu Tabanlı Ağ  (Server-based Network)

- Sunucu tabanlı bir ağda, sunucu, merkezi sunucu olarak bilinen ağ için bir temel görevi görür.
- Merkezi sunucu, kullanıcıların kimliğini doğrulamak, dosyaları depolamak, yazıcıları yönetmek ve veritabanı ve e-posta programları gibi uygulamaları çalıştırmak gibi birden çok görevi yerine getirir.
- Sunucu tabanlı bir ağ olması durumunda, güvenlik, kullanıcının herhangi bir bilgisayar sisteminde oturum açmak için bir oturum açma kimliği ve şifresine sahip olmasına izin veren sistemde merkezileştirilir.
- Sunucu tabanlı ağlar daha karmaşık ve maliyetlidir ve genellikle yönetim için tam zamanlı hizmetler gerektirir.
- Sunucu tabanlı ağlarda, trafiğin çoğu sunucular arasında gerçekleşir.



# Client-Server Working Model

- Client computers: These are user computers on a network that receive services from server computers. Access to information is determined by the server.
- The client machine (or client process) requests a resource or service, and the server machine (server process) processes the request and returns the response (result) to the client.
- On a database server, the client queries the server for records from the database, and the server searches for the records and responds to the client.
- The user on the client machine may not even know which machine on the network owns the database.
- In fact, the database may be distributed across several machines on the network.
- The client must know the server's existence and address.
- However, the server does not need to know the client's existence or address before the connection.
- Once a connection is established, both parties can send and receive information.

# Client – Server Architecture

- Server (Server: workstation or computer):
  - Data storage unit.
  - Inactive.
  - Waits for requests.
  - When requested, prepares information and sends a response.
- Client (Client: computer or mobile device):
  - Active.
  - Sends requests.
  - Waits for a response. Multitasking allows the server to continue its other work.

# Client and Server in a network

- Clients and servers are separate logical devices that work together on a network to accomplish a task.
- A client application is a communication element that requests or requests a network service, such as accessing a web page, downloading a file, or sending an email.
- A server application is a communication element that responds to client requests and provides the required service, such as sending the web page, requested file, or email.
- The client-server model is used by computer applications such as email, the World Wide Web, and network printing.

# Client-Server Functions

- User interface management
- Management of shared peripherals
- Capture and validate input data
- Create queries and reports on databases
- Control concurrent access to shared databases
- Create communication links with other local or wide area networks

# Which are the most typical functional units of the client/server applications?

The most typical functional units of the client/server applications are

- Presentation logic or user interface (e.g., ATMs)
- Business logic (e.g., Account balance inquiry)
- Data (e.g., Bank account records)

# TCP/IP - Ethernet

# TCP/IP

- TCP/IP: Transmission Control Protocol / Internet Protocol
- TCP enables data transfer from one point to another by switching data packets.
- IP is the network layer. It provides a data packet distribution service (host-to-host). IP translates between different data connection protocols.

- IP provides connectionless, unreliable delivery of data packets.
  - Connectionless: Each data packet is independent of the others. Every data packet has a number. Because big data packet divides a lot small data packets. So data packets are numbered.
  - Unreliable: There is no guarantee that data packets are delivered correctly, or even that they are not delivered at all.

# Ethernet – TCP/IP

**TCP/IP:**

- Developed in 1973 for use on the ARPANET, which was a defense force research network.
- All hosts on the internet are required to use TCI/IP. They have equal access rights.
- TCP/IP allows data transfer using packet switching.
- The layers in the TCP/IP protocol do not exactly match those in the OSI model.
- The original TCP/IP protocol is defined as having four layers: host-to-network, internet, transport, and application.
- TCP/IP, Communications Control Protocol, and Internet Protocol, specify how data should be packaged, transmitted, and routed in end-to-end data communications.

**Ethernet Switch (LAN: Ethernet Network):**

- Carrier Sense Multiple Access/Collision Detection (CSMA/CD) standart.
- Most popular LAN protocol is used on bus and star
- Inexpensive

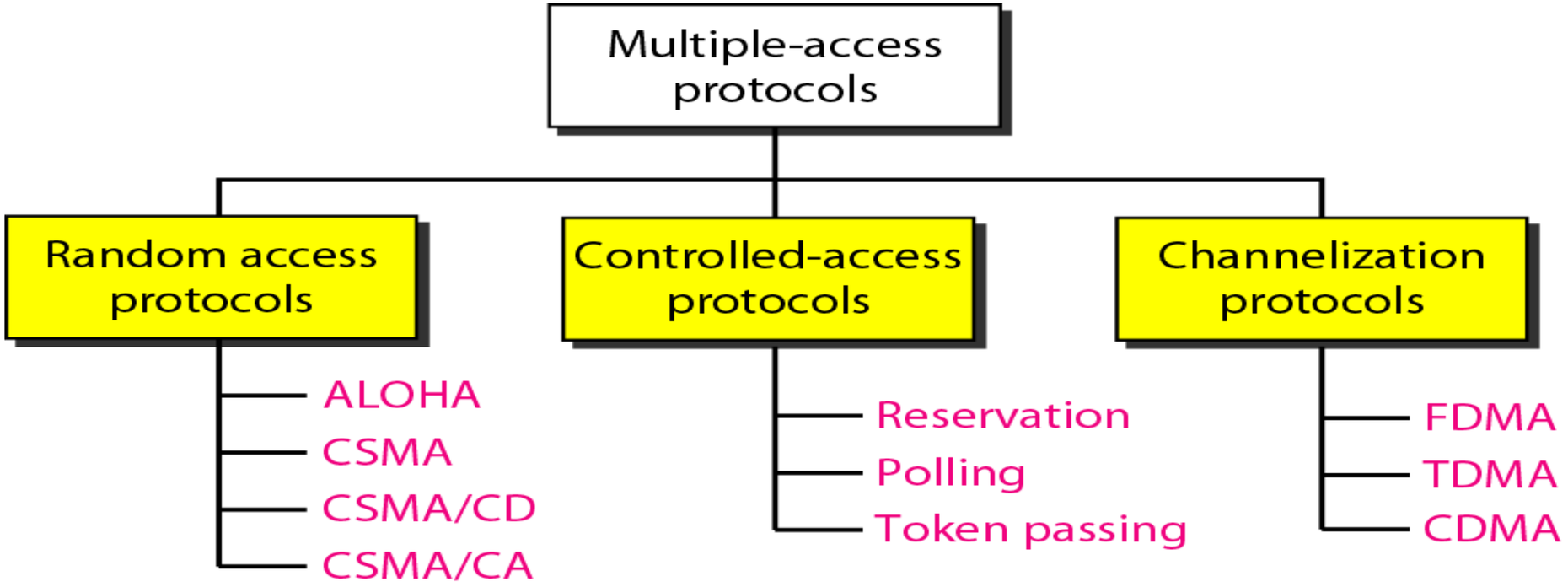
# TCP (Transmission Control Protocol)

- TCP is control protocol for packet data transmission.
- This involves a shared communication medium.
- It is a connection-oriented protocol.
- A connection must be established before data can be transmitted over the network.
- Delivery of data to the destination router (Router/Gateway) is guaranteed. If the connection is interrupted during file transfer, the server will claim the lost portion.
- Messages will be delivered in the order they were sent.
- Broadcasting is not supported.
- Data is read as a stream. When one packet ends, the next begins.
- The header size is 20 bytes.
- It is slower than UDP.
- This protocol is primarily used where secure communication is required. Examples: web browsing and email.

# Ethernet (IEEE 802.3)

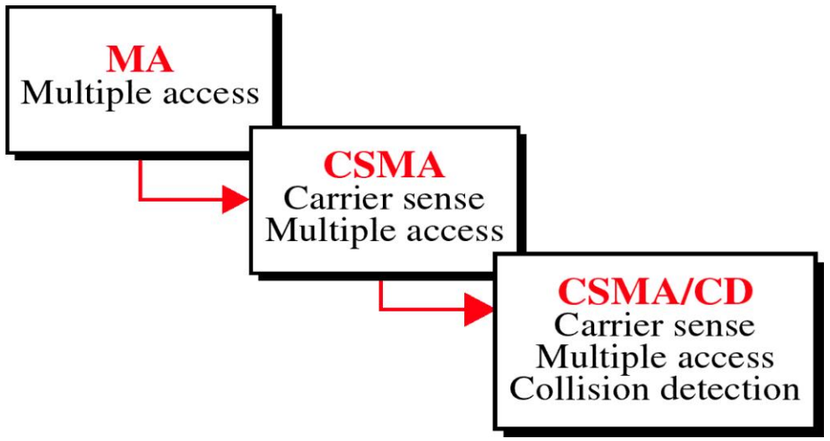
- Developed at Xerox in 1976. First  protocol approved as an industry standard protocol 1983.  LAN protocol uses on bus and star
- Almost all LANs today use Ethernet Switch
- Originally, Ethernet was jointly developed by a consortium of Digital Equipment Corp., Intel and Xerox and was standardized as **IEEE 802.3**.
- Ethernet LANs that use swithces and hubs
  - Ethernet (Ethernet Network) TCP/IPMost popular LAN protocol, Inexpensive
  - Carrier Sense Multiple Access/Collision Detection (CSMA/CD)
- The Ethernet port allows computer systems equipped with a NIC card to communicate with each other over an Ethernet network.
- The USB port connects devices to computer systems.

# Multiple-Access Protocols



# CSMA/CD

- Stands for: **C**arrier **S**ense **M**ultiple **A**ccess / **C**ollision **D**etect
- **Carrier Sense**: Before a computer wants to send data paketc, this computer listen, monitor or trace to the network (switch) to see if another computer is communicating before sending anything themselves.  If any computer does not communicate each oter, it sends the data packet.
- **Multiple Access**: all computers have access to the network medium. There are no master computers or slave computers. Every computer is equal.
- **Collision Detect**: **If two or more computers attempt to send data packets at the same time, the data packets will collide. I**f all computers detect a collision (CD), they then wait a random amount of time and resend the frame (It has to be random in order to avoid another collision). Those not in conflict wait. Those in conflict generate random timeouts. They send the data packet that produces the shortest timeout.



# Contention Protocols

- **CSMA** (Carrier Sense Multiple Access)
  - Improvement: Start transmission only if no transmission is ongoing
- **CSMA/CD** (CSMA with Collision Detection)
  - Improvement: Stop ongoing transmission if a collision is detected
- **CSMA/CA** (CSMA with Collision Avoidance)
  - Improvement: Wait a random time and try again when carrier is quiet. If still quiet, then transmit
- **CSMA/CA with ACK**
- **CSMA/CA with RTS/CTS**

# CSMA/CD Algorithm

- Sense for carrier.
- If carrier (computer sending data packets) present on the transmission media (Ethernet switch), wait until carrier ends.
  - Sending would force a collision and waste time
- Send packet and sense for collision.
- If no collision detected, consider packet delivered.
- Otherwise, abort immediately, perform “exponential back off” and send packet again.
  - Start to send at a random time picked from an interval
  - Length of the interval increases with every retransmission

# What is the difference between CSMA/CD and CSMA/CA?

- CSMA/CD stands for Carrier Sense Multiple Access with Collision Detection. It is a media access control method used in local area networking using early Ethernet technology to overcome the occurred collision.
- CSMA/CA stands for Carrier Sense Multiple Access with Collision Avoidance. It is used in the wireless network to avoid the collision.
- Following are the differences between CSMA/CD and CSMA/CA:

| CSMA/CD | CSMA/CA |
|---|---|
| Full form of CSMA/CD is carrier sense multiple access with collision detection. | Full form of CSMA/CA is carrier sense multiple access with carrier avoidance. |
| CSMA/CD detects the collision, and once the collision is detected, then it stops continuing the data transmission. | CSMA/CA does not deal with the recovery of the collision. |
| Wired installation is used in a CSMA/CD to detect the collision. | Wireless installation is used in a CSMA/CA as it avoids the collision. Therefore, it does not need a wired network. |
| An 802.3 Ethernet network uses CSMA/CD. | An 802.11 ethernet network uses CSMA/CA. |
| CSMA/CD takes effect after the occurrence of a collision. | CSMA/CA takes effect before the occurrence of a collision. |

# Types of Ethernet Cable

- mmmBaseT, mmm: Megabit/sec, T: twisted cable.
- Seven types of shared Ethernet have been in use:
- **10Base5** = thick Ethernet, uses thick coax. This is the original Ethernet specification. Now uncommon.
- **10Base2** = thin Ethernet, uses thin coax. Became popular in the early 1990s as a cheaper alternative to 10Base5. Now uncommon.
- **10BaseT cable** = twisted pair Ethernet, most common type of Ethernet. Uses Cat-5 or more UTP cable. Common but rapidly losing ground to 100BaseT.
- **100BaseT** = also called Fast Ethernet, has replaced 10BaseT in sales volume. Uses Cat-5 or more UTP cable: (Sometimes combined 10/100 Ethernet is found in which some segments run 10BaseT and some run 100BaseT is also used by some organizations).
- **1000BaseT** = Gigabit Ethernet. Maximum cable length is only 100 meters. Cat-6 or cat-7, fiber cables are used.
- **10GbE** = 10 Gbps Ethernet. Uses fiber and is typically full duplex.
- **40GbE** = 40 Gbps Ethernet. Uses fiber and is typically full duplex.

| Name | Maximum Data Rate | Cables |
|---|---|---|
| **10Base5** | 10 Mbps | Coaxial |
| 10Base2 | 10 Mbps | Coaxial |
| 10BaseT | 10 Mbps | UTP cat 3, UTP cat 5 |
| 100BaseT | 100 Mbps | UTP cat-5 or cat-6, fiber |
| 1000BaseX | 1 Gbps | UTP UTP cat-5e, UTP cat-6, fiber |
| 10 GbE | 10 Gbps | **fiber** |
| 40 GbE | 40 Gbps | fiber |

# Types of Ethernet Cable

# Network Equipments

# Ağlar

- **Kişisel Alan Ağı (PAN-Personal Area Network ):** Evde sıklıkla kullanılan en küçük ve temel ağ türüdür. Bilgisayar ile telefon, yazıcı, modem tabletleri gibi başka bir cihaz arasındaki bağlantıdır.
- Yerel Alan Ağı (LAN-Local Area Network ): LAN küçük ofisler ve internet kafelerde küçük bir bilgisayar grubunu birbirine bağlamak için kullanılır. Genellikle bir dosyayı aktarmak veya oyunu ağda oynamak için kullanılırlar.
- Büyükşehir Alan Ağı (MAN-Metropolitan Area Network): LAN'dan daha güçlü bir ağ türüdür. MAN tarafından kapsanan alan küçük bir kasaba, şehir vs.'dir. Bağlantı için bu kadar geniş bir alanı kapsayan büyük bir sunucu kullanılır.
- Geniş Alan Ağı (Wide Area Network-WAN): LAN'dan daha karmaşıktır ve tipik olarak geniş bir fiziksel mesafeyi kapsayan geniş bir alanı kapsar. İnternet, dünyaya yayılmış en büyük WAN'dır. WAN herhangi bir kuruluşa ait değildir ancak sahipliğini dağıtmıştır.

# Internet, Intranet ve Extranet arasındaki fark

Internet, Intranet ve Extranet terminolojileri ağdaki uygulamalara nasıl erişilebileceğini tanımlamak için kullanılır. Benzer TCP / IP teknolojisi kullanırlar, ancak ağ içindeki ve ağ dışındaki her kullanıcı için erişim düzeyleri bakımından farklılık gösterirler.

- Internet: Uygulamalara web'i kullanan herhangi bir konumdan herkes erişebilir.
- Intranet: Aynı kuruluştaki kullanıcılara sınırlı erişime izin verir.
- Extranet: Farklı konumlardaki  kullanıcıların tek kuruluşun ağ uygulamasını kullanmasına izin verilir veya erişim sağlanır.

# Intranet (Özel Ağ – İç Ağ)

- Belirli bir kuruluş içindeki TCP/IP tabanlı bir ağ sistemine verilen isimdir (şirket içi İnternet).
- Intranet'ler ağ geçitleri ile diğer ağlara veya İnternet'e bağlanabilir. İnternet çıkışı genellikle *Firewall* olarak bilinen her iki yönde de ileti trafiğini kontrol eden bir güvenlik sistemi üzerinden sağlanmaktadır.
- Intranet'te genellikle sanal IP kullanılır. Böylece sadece İnternet çıkışı için tek bir gerçek IP kullanılarak iç ağdaki tüm bilgisayarlara İnternet erişimi verilebilir.

# Summary

- Transmission Mediums: 2 or 4 twisted pair conductor wire, fiber optic cable, coaxial; wireless (air, space)
- In the transmission medium, the signal is only analog. In computer systems, the analog signal is converted to the digital signal (ADC). Conversion steps are discrete values, quantization, encoding to binary as bit: 0/1
- In the transmission medium, type of the analog signal is changed to prevent message in the signal from being not affected by noise, via modem devices.
- Wireless Communication Systems (Air/space):
  - Satellite PtP (SCPC), PtMP (VSAT)
  - Radiolink PtP, PtMP
  - Wireless internet access: Wi-Fi - Bluetooth, WiMax, 3G, 4G, 5G, 6G
- Terminal Server: Pre-storage and preparation of data on the local campus.
- Data Switching Systems:
  - Circuit switching: TDM (E1), SDH, PDH; ISDN, Leased Line
- Packet switching:
  - NIC, Ethernet switch, Router, GW, ATM, Frame Relay, ADSL

# Why is the analog signal converted to a digital signal in computer systems?

- Because computers can only process digital data. All operations inside a computer are based on binary values (0 and 1). Analog signals (sound, temperature, light, electrical signalsetc.) are continuous and cannot be directly understood by digital electronic circuits.
- 1. Computers are digital machines
  - They operate using binary logic. So analog signals must be converted to digital form using an ADC (Analog-to-Digital Converter).
- 2. Digital signals are more reliable
  - Analog signals easily get distorted by noise.
  - Digital signals are far more stable and can be transmitted or stored without losing quality.
- 3. Easy storage and processing
  - Digital data can be stored, copied, compressed, encrypted, and processed very fast.
- 4. Accuracy and flexibility
  - Digital formats allow precise mathematical processing and manipulation.
- 5. Standardization
  - Modern communication, storage, and computing systems all use digital formats.

# Network Equipments

- Network devices are interface devices that enable computer systems, which are NIC interface units, to communicate data with each other.
- The simplest network device is the Ethernet switch. This device performs the functions of the first two layers in the OSI model.
- Network cards (NICs), which are used to connect a computer to another computer or a network device, are also known as Ethernet cards because they generally use the Ethernet protocol.
- The following devices are used to enable and control data transmission in computer networks.
  - ❖ Modem (Modulator/Demodulator) provides local area network (LAN) connections over other WANs using a wide area network structure via communication mediums. It enables routers or gateway devices to connect to the communication medium and the WAN.
  - ❖ Switch (Network Switch) is LAN equipment. Switch equipment that can be used in WAN is available. It is used extensively in Gigabit Ethernet infrastructure.
  - ❖ Router (Router), Gateway (Network Gateway) connects the LAN infrastructure to wide area networks (WAN).
  - ❖ Bridge: Connects two LANs to each other (LAN to LAN)

# The Networking Devices(Nodes)

1. NIC Card
2. Repeater
3. Hub
4. Switch
5. Bridge
6. Router
7. Gateway
8. Firewall

# Computer Network Hardware Devices

- **Repeaters**
- **Bridges**
- **Routers**
- **Gateways**
- **Routing Algorithms**

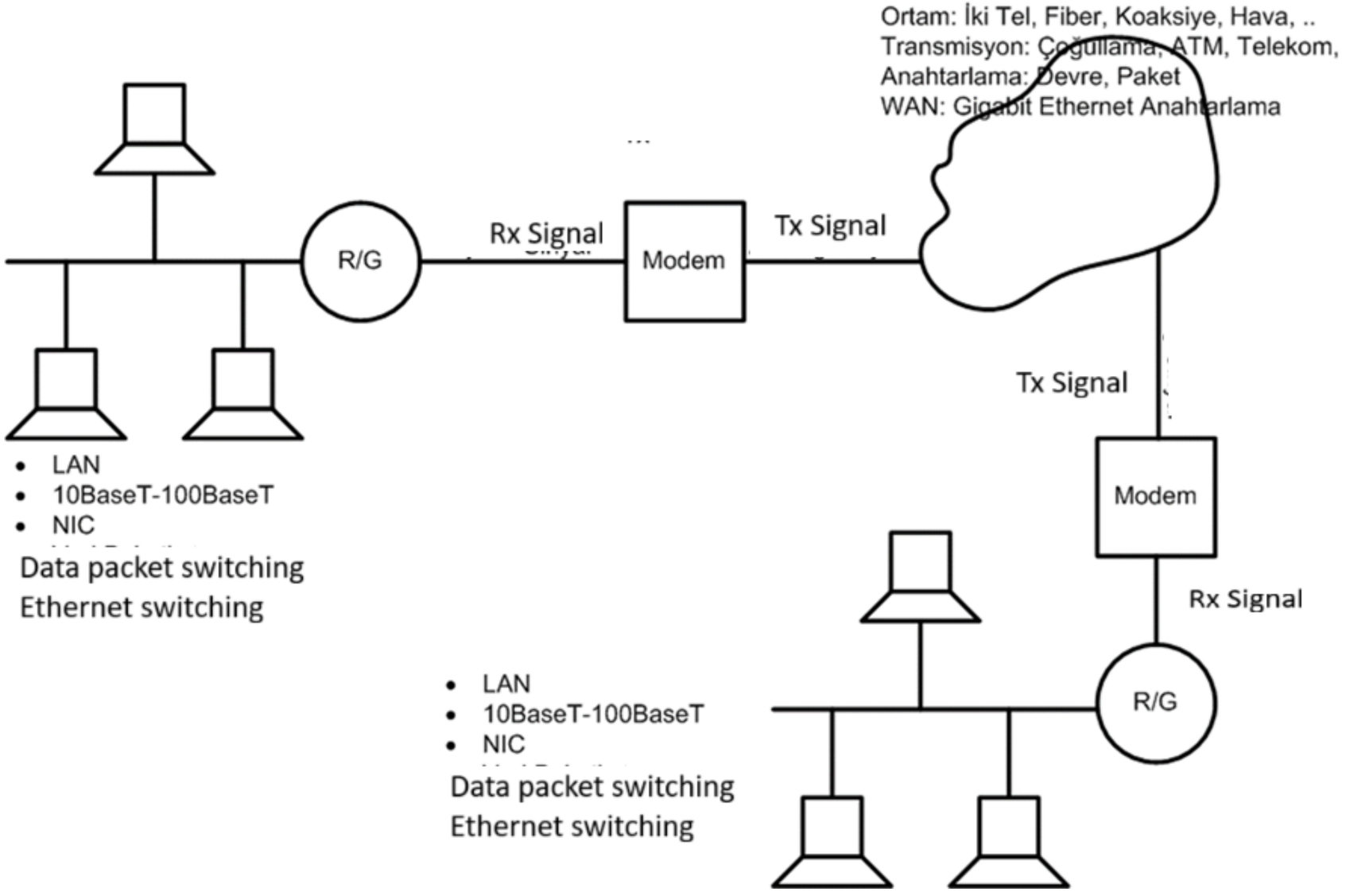
- Servers: Help manage the network and its resources. In larger networks, servers typically have specific tasks such as:
  - File Servers: store and manage files,
  - Printer Servers: manage printers and print jobs,
  - Mail Server: manages email,
  - Web Server: manages web access.
  - A terminal server is a network device or software system that allows multiple users or terminals to connect to a central computer or server. It is used at end points for clients.
- Routers: connect multiple networks together and are protocol-independent. They can be used instead of switches or bridges.
- Hubs: like dual adapters/power boards in a home, we plug computers in to allow them to communicate instead of plugging in extension cords.
- Switches: are intelligent devices that forward packets only to the destination port.

# Terminal server

- Terminal server is a network device or software system that allows multiple users or terminals to connect to a central computer or server. Two common meanings:
- 1. Hardware Terminal Server (Network Device)
  - A hardware terminal server connects multiple serial devices (like sensors, barcode scanners, old terminals) to a network.
  - It converts serial communication (RS-232/RS-485) to TCP/IP network traffic
  - Allows remote devices to communicate over Ethernets often used in industrial systems, data centers, and legacy equipment
- 2. Software Terminal Server (Remote Access Server)
- In modern computing, “terminal server” often refers to a server that hosts applications to be accessed remotely, especially in Windows environments.
  - Examples:Microsoft Remote Desktop Services (RDS)
- Citrix servers
  - It allows many users to:
  - Log in remotely
  - Run applications on the server
  - Use the server’s CPU, memory, and storage
- So instead of installing software on every computer, users access the server through:
  - Remote Desktop Protocol (RDP)
  - Thin clients
  - Terminals
- In simple terms: A terminal server allows many users or devices to connect to and use a central computer from remote locations.

# Data Packets

- Data packets are numbered.
- Packets do not travel sequentially from one endpoint (client, server) to another (client, server), but rather in a distibuted manner.
- They are sorted at the receiving point, and if a packet is missing or arrives incorrectly, it is requested again from the source using its number.
- Mapping: client to client, client to server, server to client, server to server.
- A packet contains the destination address, the packet's own address, the packet length, the packet number, and an acknowledgment statement.
- Routers or gateways route data packets to each other.
- Data packets are routed and switched in Ethernet switch equipment.
- For example, a computer sends data packets to another computer within its network only after switching.
- For example, a computer switches data packets to another computer in another network area via a router; this router then routes them to the other router over the WAN.


Ortam: İki Tel, Fiber, Koaksiye, Hava, ..
Transmisyon: Çoğullama, ATM, Telekom,
Anahtarlama: Devre, Paket
WAN: Gigabit Ethernet Anahtarlama
R/G
Rx Signal
Modem
Tx Signal
Tx Signal
Modem
Rx Signal
R/G
• LAN
• 10BaseT-100BaseT
• NIC
Data packet switching
Ethernet switching
• LAN
• 10BaseT-100BaseT
• NIC
Data packet switching
Ethernet switching

# Network Technology Concepts

- **Internet:** The name given to the computer network technology that connects computers to each other. It is the general name for the data communication medium.
- **Internet layer:** Data coming from the transmission layer becomes data packets here. The tasks related to routing the packets are also performed here.
- LAN (Local Area Network): A local communication network infrastructure established for computers to communicate with each other in a limited environment.
- LAN equipment is only ethernet switch, IP-based devices (Computers, Smartphones, sensors, IP phones, ...)
- WAN (Wide Area Network): The network infrastructure where computer systems located in different geographical areas communicate with each other.
- LAN to WAN connection equipments are Router, Gateway, Modem
- WAN to WAN connection equipments are Router, Gateway
- ROUTER: Devices that route data packets according to the addresses they need to be delivered to.
- GATEWAY: Devices that perform routing with QoS services in an internet network. VPN (Virtual Private Network): A private virtual network that connects organizations or locations to each other in a highly secure way over the internet, creating a local network. Backbone: Network backbone.
- QOS (Quality of Service): Prioritizing real-time image, video, voice, and data packets.
- VOIP (Voice over IP): Voice communication using the IP protocol.

# Network Technologies Critical Features

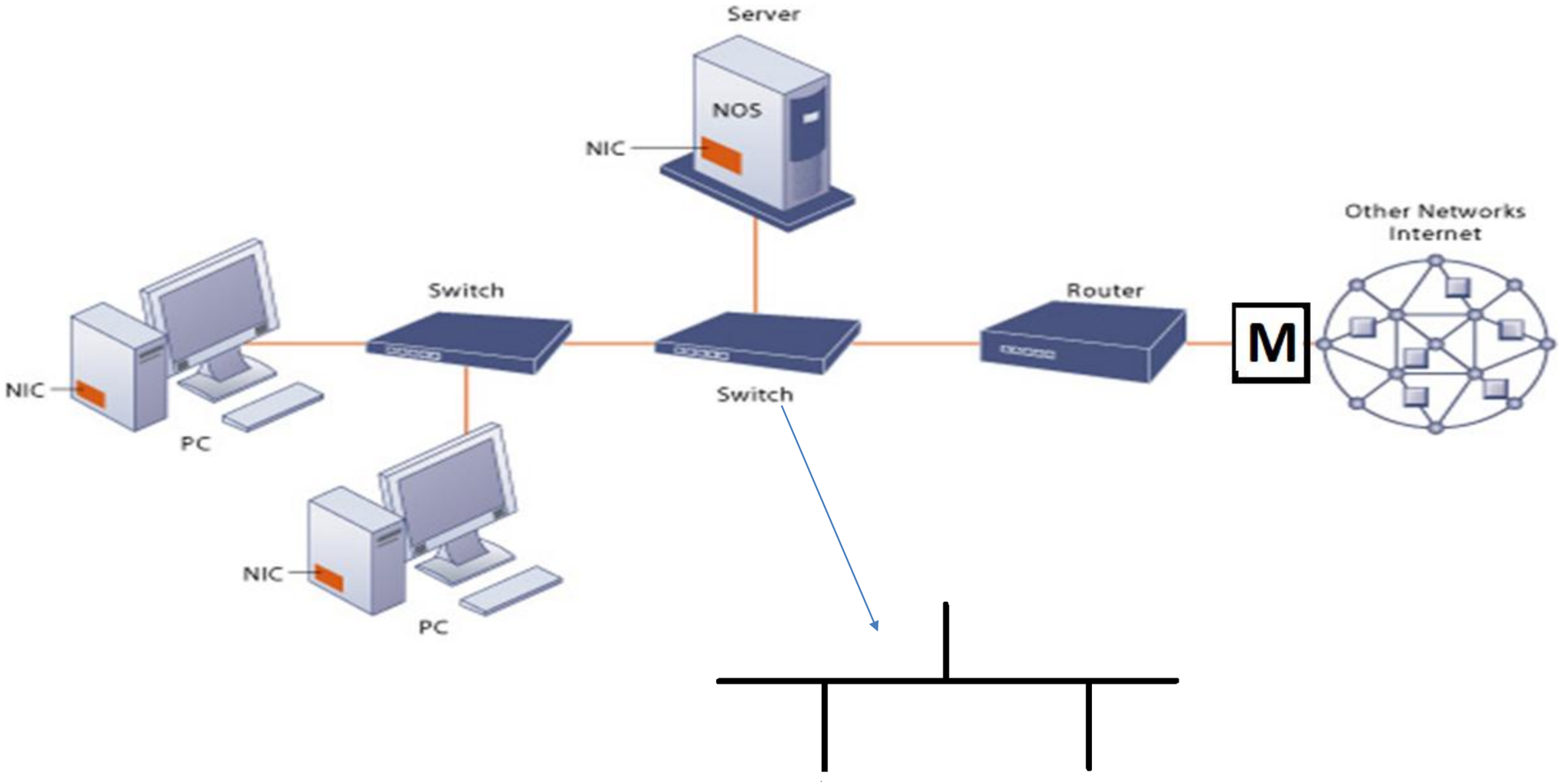
- **Round trip time**, is the time it takes for a packet to travel from a source destination to a other destination and back again. Data packet losses are tested.
- **Network congestion** occurs when network devices, such as routers and switches, send more data than they can handle. This is a common situation when many users try to use the same bandwidth. Network congestion results from a large number of users trying to use a bandwidth simultaneously. Congestion in a network most commonly occurs in larger networks that do not use network segmentation.
- **Latency** is the amount of time delay measured from the point a network device receives a data packet to the time it sends it again to another network segment. It is the expression of the time it takes for a data packet to travel from one specified point to another. Latency is the amount of time delay. It is measured as the time difference between the moment a network receives data and the time it is sent by another network.
- Bandwidth refers to the transmission range of a medium in terms of frequency (BW = fmax - fmin). It is a measure of how much volume a communication channel can handle and is specified in Hz. Digital channel capacity, on the other hand, is measured in bps. Here, bps indicates the number of bits that can be transferred per second.

# Example

Question: LANs have been set up in a workplace. What LAN equipments are used?

- Ethernet switch (10BaseT, 100BaseT, 1000BaseT; bandwidth increases as data speed increases, therefore the distance of 4-pair twisted UTP cable decreases. The highest quality UTP cable: S-FTP 1000BaseT (Data transfer speed, 1000Mbit/s = 1 Gigabit/s, T: 4-pair twisted S-FTP cable)
- If the distance is more than 100 meters, a fiber to 1000BaseT converter and fiber cable should be used
- Computer systems are connected to the ports of the Ethernet switch device in Ethernet environments.
- Ethernet port: NIC interface unit, the port type should be noted. The port type is determined according to the data speed. If a data speed of 100Mbit/s is mentioned, 100BaseT Ethernet cable is used.

# Components of a Simple Network



# NIC, Network Interface Card

- All equipmenta that use wtih computer systems use NICs to communicate over the internet. Each NIC has a unique identification information.
- NIC stands for Network Interface Card. No computer system can connect to a network without a NIC.
- It is also known as a Network Adapter or Ethernet Adapter Card.
- It is in the form of an add-on card and is plugged into a computer system so that the computer can connect to a network.
- Each NIC has a MAC address that helps identify the computer on a network.
- Each NIC has a different address. All computer systems have a unique NIC address. It contains identification information.
- NICs are part of both the physical and data link layer and contain a unique data link layer address (sometimes called a MAC address) placed on them by their manufacturers. Before sending data to the network, the network card also organizes the data into frames and then sends them over the network.
- Laptops typically use NICs that plug into a PCMCIA port.

# Firewall

- A firewall is a network security system used to protect computer networks from unauthorized access.
- Firewall prevents malicious access to the computer network from the outside. A firewall can also be created to provide limited access to external users.
- A firewall consists of a hardware device and a software or an only software system.
- All messages passing through the firewall are examined according to specific security criteria, and messages that meet the criteria are either successfully transmitted over the network or blocked.

# Wireless internet connections

1) Broadband Connection - This type of connection provides consistently high-speed internet. Examples include: cable modems, fiber optics, wireless connections, satellite connections, etc.

2) Wi-Fi - A wireless internet connection between devices. It uses radio waves to connect to devices or appliances.

3) WiMAX - The most advanced type of internet connection, more feature-rich than Wi-Fi. It is nothing more than a high-speed and advanced broadband connection.

# Example

Question: LANs have been created in a workplace. How are the connections to other LANs made?

- Repeater, Hub, Switch, Bridge, Wireless Bridge, Wireless Access units; Router and Gateway, Modem. All of them is not correct, you can select for your needs.

Question: LANs have been created in a workplace. How is communication with the LAN of the company in Paris made?

- Router/GW, Modem are used to route to the telecom switching and transmission service. After the modem, we need a communication medium.
- What is in the communication medium: Twisted pair wire, fiber, radio link, satellite
- French Telecom communication medium for our office in France: Twisted pair wire, fiber, radio link, satellite
- Office in France: Modem, Router/GW and LAN- switch
- The most decisive factor is data speed? It is the number of bits transferred from one point to another in one second.

- Thus, many companies provide voice, data and video services in a high-quality manner

# Network Equipment: Ethernet Switch

# The advantage of using an Ethernet Switch

- When a Ethernet switch receives a data packet from router/GW or computers, a data frame is created from the bits in that packet. This process allows it to gain access to the Ethernet medium, read the destination address, and then forward that frame to the appropriate port. This is a very efficient data transmission method instead of broadcasting on all ports.
- Switches are used to receive a data packet signal and create a frame from the bits in that data packet signal. Data packet allow to access and read the destination address, and after reading it, forward that frame to the appropriate frame. Therefore, switches are a vital part of transmission.
- It allows full duplex data transmission and reception. It performs media rate adaptation. It provides easy and efficient switching.
- In seamless LAN switching, in Cut-Through LAN switching, as soon as the router receives the data frame, it will forward it to the next network segment after reading the destination address. Voice and live video...

# Advantages of LAN switching

LAN switching is a form of packet switching used in Local Area Networks. It is a vital component of most networks and helps improve the overall efficiency of the LAN and address existing bandwidth issues. It allows multiple users to communicate directly with each other. LAN switching creates a synchronous, point-to-point connection system between pairs of devices. It provides a collision-free network and a network that transfers high-speed data packets. It consists of layers.

- Increased network scalability: LAN switching can handle increasing amounts of workload. Therefore, since performance decreases as capacity increases, if the ports are 100BaseT, then when using two switches, an additional 1000BaseT port should be used.
- Improved bandwidth performance: We need higher bandwidth performance when users run multimedia applications or some database interactions.
- Multiple simultaneous connections: LAN switching allows multiple simultaneous connections, meaning it can transmit multiple data at the same time. This is because it has a layered structure. This is not possible in a hub-based network.
- Reduced congestion and transmission latency: LAN switching improves the performance of a network because a segmented network consists of fewer hosts per subnet, thus minimizing local traffic.
- No single point of failure: LAN switching ensures proper network design. Therefore, there is a lower probability of network failure.
- Allows full-duplex data transfer: LAN switching allows full-duplex data transfer, meaning data can be transmitted simultaneously on a bidirectional line.
- Improved manageability and security.

# HUB: Shared Ethernet Topology

- Ethernet's logical topology is a bus topology. This means that all computers on the network receive messages from all other computers, whether or not the message is intended for them. When a frame is received by a computer, the first task is to read the frame's destination address to see if the message is intended for it.
- Today, almost all Ethernet network topologies use a physical star topology with computers connected to hubs. It is also common to connect multiple hubs to create more complex physical topologies.
- A hub doesn't just send data to the receiver; it sends it to all the computers connected to it. The computers detect whether the data has been sent to them. A hub can only transmit 1 message at a time. Other connected computers must wait for a transmission.

# Switched Ethernet Topology

- A modem is a communication medium device. Modems connect routers or gateway devices to WAN communication media. They convert digital data into analog signals. They ensure the transfer of data to communication media without corruption.
- An Ethernet switch is an advanced version of a hub. Ethernet switches connect to routers, gateways, computers, and computer systems. They connect via NIC cards. NIC addresses are unique.
- An Ethernet switch offers multiple switched paths to the devices connected to it, instead of a single common path. A hub device offers a single common path. Two systems can communicate simultaneously. However, in the Ethernet switch architecture, it is possible for multiple communications to occur simultaneously. In hub systems, as the number of computers increases, network traffic also increases, and the use of switches is preferred over hubs.

# What is the difference between a switch, a hub, and a router?

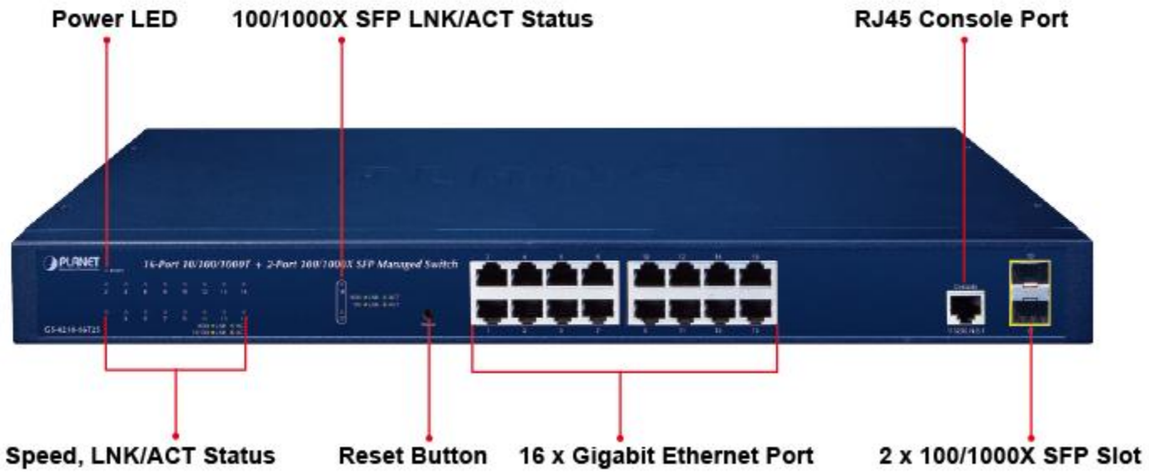
- A hub has a single broadcast domain and a collision domain. Everything coming from one port is sent to the others. It is a device that filters and forwards packets between LAN segments.
- Switches have a single broadcast domain and multiple collision domains. They support any packet protocol because they operate at both link layer 2 and layer 3.
- A router is a device that forwards data packets across networks.
- Switches are used at the link layer, hubs at the physical layer.
- A bridge does not divide the network into smaller segments. What a bridge actually does is take the large network and filter it without changing the size of the network.

| Basis of Comparison | Hub | Switch |
|---|---|---|
| **Description** | Hub is a networking device that connects the multiple devices to a single network. | A switch is a control unit that turns the flow of electricity on or off in a circuit. |
| **Layer** | Hubs are used at the physical layer. | Switches are used at the data link layer. |
| **Transmission type** | Transmission type can be unicast, broadcast or multicast. | Initially, the transmission type is broadcast and then is unicast. |
| **Ports** | Hub has 4/12 ports. | The switch has 24/48 ports. |
| **Transmission mode** | Half duplex | Half/Full duplex. |
| **Collisions** | Collisions occur commonly in a Hub. | No collisions occur in a full duplex switch. |
| **Address used for data transmission** | Hub uses MAC address for data transmission. | The switch uses a MAC address for data transmission. |
| **Data transmission form** | Electrical signal is a data transmission form of a hub. | A Frame is a data transmission form of a switch. |

# What is the difference between Switch and Router?

| Basis of Comparison | Router | Switch |
|---|---|---|
| **Description** | It is a layer 3 device that connects the two different networks and identifies the network devices based on their IP addresses. | It is a layer 2 device and determines the network devices based on their MAC addresses. |
| **Mode of transmission** | Router transmits the data in the form of packets. | Switch transmits the data in the form of frames. |
| **Address used** | It uses an IP address for the data transmission. | It uses a MAC address to transmit the data. |
| **Layer of OSI model** | It uses Layer 3 OSI model and layer is the network layer. | It uses layer 2 OSI model and layer is the data link layer. |
| **Table** | It uses a routing table for routes to move to the destination IP. | It uses a Content address memory table for MAC addresses. |
| **Network used** | It is used for WAN and LAN networks. | It is used only for LAN networks. |
| **Mode of transmission** | Router is used in a full-duplex mode. | A switch is used in half as well as in a full-duplex mode. |

# Managed Switch with Advanced L2/L4 Switching and Security



# Network Equipment: Router

# Network Equipment: Router

- A router, also known as a packet router, is a device that routes data packets within a network infrastructure.
- Routing is the process of finding the shortest and fastest path for data to travel from source to destination. Routing is done using router or gateway devices.
- What are routers?
  - Routers, also known as gateways, are network layer devices.
  - Routers use headers and a routing table to determine the best and fastest path to transmit packets.
  - The router analyzes data packets sent over the network, modifies how they are packaged, and sends them over the network.
- Routing uses a routing table that maintains routes to various destinations.
  - Static routing: Static routing is a routing technique where an administrator manually adds routes to a routing table. Static routes are used when route choices are limited. Static routes can also be used when there are fewer devices and no changes to route configuration are needed in the future.
  - Dynamic routing: Dynamic routing is a routing technique where protocols automatically update the information in a routing table

# Types of Routers

1. Brouter: Brouter stands for "Bridge Router". It acts as both a router and a bridge.
2. Core Router: A core router is a router that routes data within a network, not between networks.
3. End Router: An end router is a router located at the edge of a network.
4. Virtual Router: A virtual router is a software-based router. A virtual router performs packet routing functions through a software application. The Virtual Router Redundancy protocol implements the virtual router to increase network reliability.
5. Wireless Router: A wireless router is a router that connects local networks to another local network.

# Bir yönlendiricide kullanılan bellekler

- Router ya da GW içinde bilgisayar sistemleri bulunan bir haberleşme cihazıdır. Aşağıdakiler, bir yönlendiricinde kullanılan farklı belleklerdir:

1. NVRAM (Geçici Olmayan Rastgele Erişim Belleği): Geçici olmayan rastgele erişim belleği anlamına gelir. Başlangıç yapılandırma dosyasını saklamak için kullanılır. NVRAM, yönlendirici kapatılsa bile yapılandırma dosyasını korur.
2. DRAM (Dinamik Rastgele Erişim Belleği) : DRAM, dinamik rastgele erişim belleği anlamına gelir. Yürütülen konfigürasyon dosyasını saklar. DRAM, işlemci tarafından verilere sıfırdan erişmek yerine doğrudan erişmek için kullanılır. DRAM, verilere sabit disk gibi depolama ortamlarından daha hızlı erişim sağlayan işlemcinin yanında bulunur (cache bellek). Basit tasarım, düşük maliyet ve yüksek hız, DRAM belleğin ana özellikleridir. DRAM geçici bir bellektir.
3. ROM (Salt Okunur Bellek) – POST tanılama talimatlarını çalıştıran ve sürdüren önyükleme yazılımıdır.
4. Flash Bellek – Router IOS'u saklar. Sistem IOS'unu saklamak için kullanılır. IOS görüntülerini saklamak için flash bellek kullanılır. Flash bellek silinebilir ve yeniden programlanabilir ROM'dur. Flash belleğin kapasitesi, birçok farklı IOS sürümünü barındıracak kadar büyüktür.

# Configuring a router remotely

- The most popular and easiest way to configure a router remotely is to use the AutoInstall Procedure. However, you must ensure that the router is connected to either the WAN or LA

**Explain how to use the 'ping' command.**

- Ping (Packet Internet Groper) is a computer network tool used to test whether a particular host is accessible over an IP network. You can access the router in three ways:
  - Telnet (IP)
  - AUX (Telephone)
  - Console (Cable)

# OSI katmanlarında Router

- Yönlendirici, Katman 3 cihazıdır.
- İki veya daha fazla Katman 3 ağı arasındaki trafiği "yönlendirmek" için kullanılır.
- Yönlendiriciler, tek tek Katman 2 MAC adreslerinin aksine, ağ adresi gruplarına veya sınıflara göre kararlar verir.
- Yönlendiriciler, yerel arayüzlere doğrudan bağlı ağların 3. Katman adreslerini ve komşu yönlendiricilerden öğrenilen ağ yollarını kaydetmek için yönlendirme tablolarını kullanır.
- Yönlendiriciler yayınları iletmek zorunda değildir.

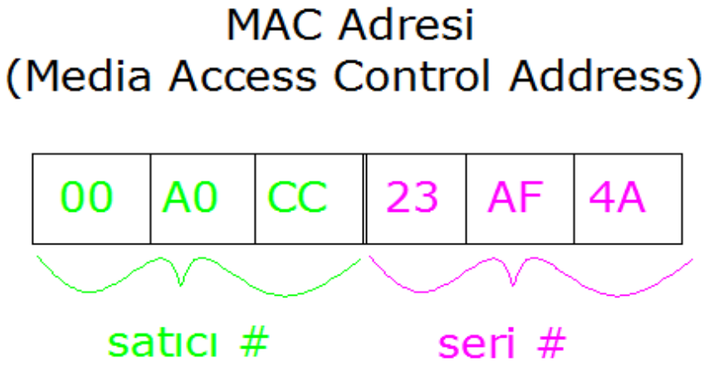
# IP address, Internet Control Protocol

# MAC: Media Access Control

- MAC addresses, or Media Access Control addresses, are used to identify network hardware in a computer network. For example, your computer's modem and network card each have their own unique MAC address.
- Since MAC is a 48-bit address,
- 2^48 = 281,474,976,710,656 different network cards can be identified.
- MAC addresses, also called physical addresses or hardware addresses, enable the identification of network hardware.
- MAC addresses are information encoded by the manufacturer into the computer's ethernet card.
- Each piece of hardware has a unique address. There is no such thing as more than one network device with the same MAC address.
- Communication between two network devices on the same network is possible via MAC addresses.
- MAC address is 48 bits, 6 octets: A MAC address consists of 6 octets (sections). The first 3 octets indicate the manufacturer of the hardware. The last 3 octets indicate the hardware.

In the binary system, a MAC address is as follows:: 000100100011010001010110 011110001001000010101011

- However, since it is quite difficult to say and write this number in binary system, it is written in hexadecimal system, that is;
- 12:34:56:78:90:AB. To reiterate; MAC addresses are written in hexadecimal with a colon (":") between them:
- Example: 01:23:45:67:89:AB.

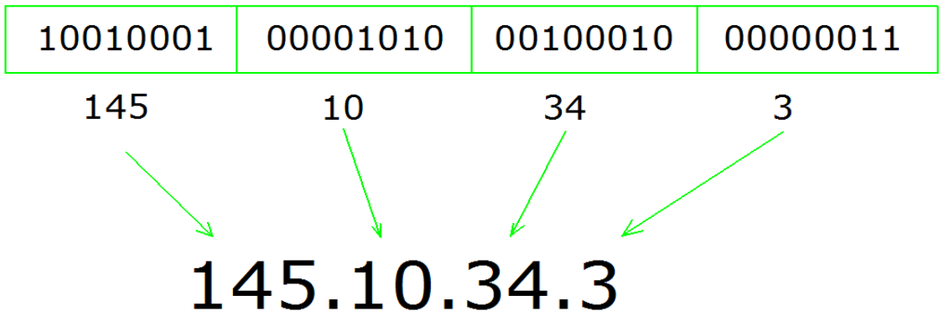


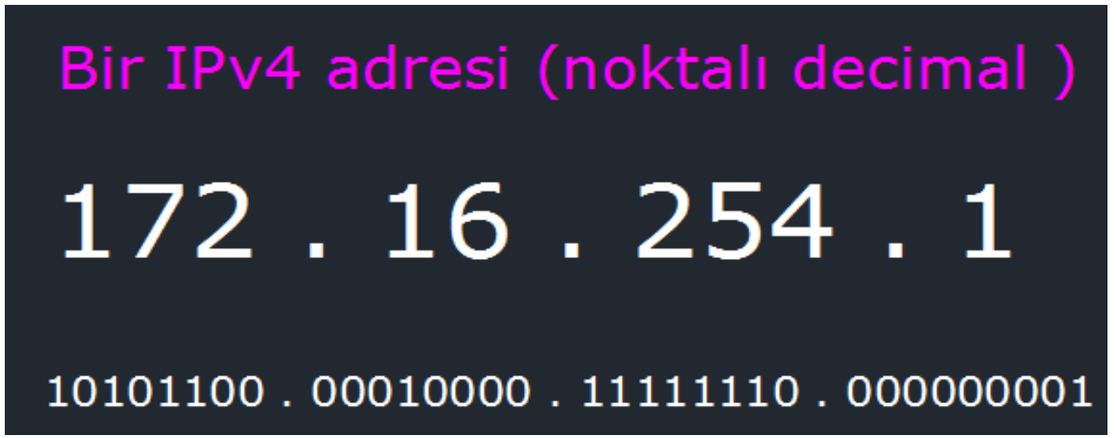
# IP address, Internet Control Protocol

- An IP address is a unique number that devices on a network use to recognize each other, communicate, and exchange data.
- Every device with an internet connection must have an IP address assigned to it.
- This IP address or number ensures that information is sent to the correct address and data is received from the correct address.
- There are currently two types of Internet Protocols in use and under testing: IPv4 and IPv6.

# IPv4 Protocol

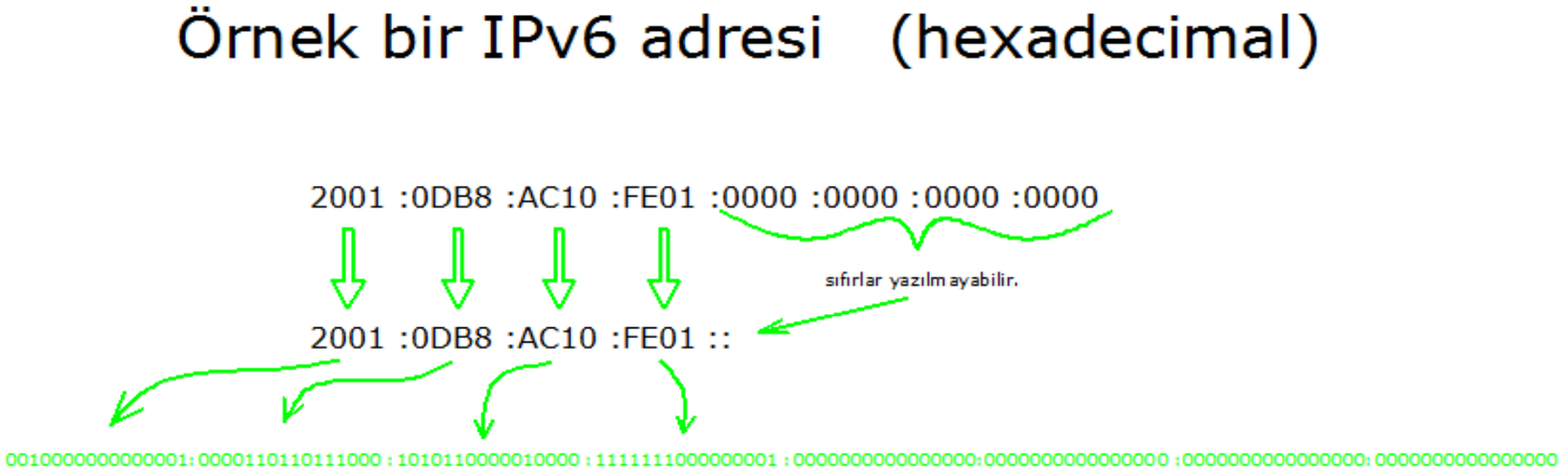
- IPv4 is the standard Internet protocol currently in use and consists of 32 bits, or 4 bytes. These numbers range from 0 to 255.
- An address in the IPv4 protocol can be any number between 1.0.0.0 and 255.255.255.255. More than 4 billion addresses can be generated using this protocol.
- An example IPv4 address: Dotted decimal notation, 4 bytes = 32 bits
- Example: Convert the IPv4 address 123.45.67.89 to binary.
- 01111011.00101101.01000011.01011001
- Example: Convert the IPv4 address given below to dotted decimal notation.01011110.01100010.10011011.00010000
- 94.98.155.16



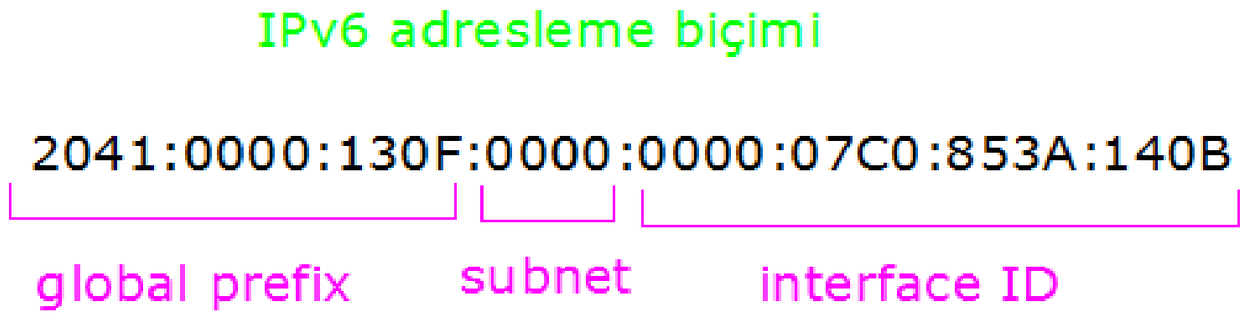



# IPv6

- Due to the increasing number of network users, a larger IP address is needed.
- IPv6 was born from this need.
- Unlike IPv4, IPv6 is 128 bits wide,
- which means 2128 unique addresses, or in other words, 3 x $10^{38}$ unique addresses.
- It consists of 8 four-digit hexadecimal numbers. (::) is used to shorten the address where there are 0s.



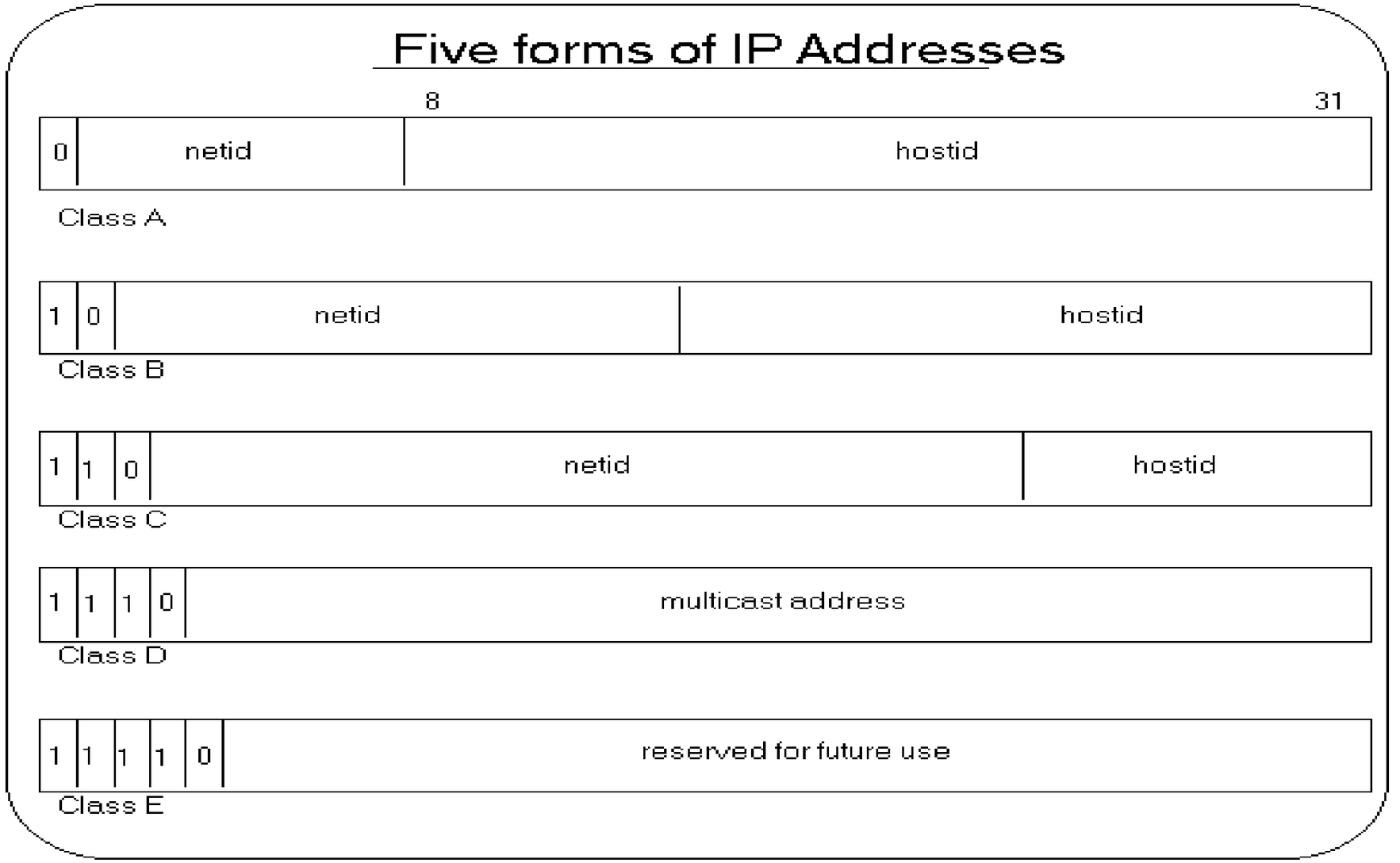
# Example of IPv6 addressing format:



# Classification of IP addresses

- 00
- Hostid: Defines the computer/server address. The address must be known by the computer systems (NICs) at the host point. The switch does not look at the address.
- Netid: Network, Router, Gateway: Routing exists. The network address must be known for routing to be possible.
- Addressing is done at two points: Netid, Hostid
- The first 8 bits are looked at:
  - If the first bit is 0, it is Class-A
  - If the first two bits are 10, it is Class-B
  - If the first three bits are 110, it is Class-C
  - If the first four bits are 1110, it is Class-D
  - If the first five bits are 11110, it is Class-E
- Example: Which IP class does 64.127.252.8 belong to? (64)d=(0100 0000)b; since the first bit is 0, it is Class-A
- Example: Which IP class does 164.127.252.8 belong to? (164)d=128+32+4=(1010 0100)b; since the first two bits are 10, it is Class-B

# IP address format




A-Class:
Netid: ilk 8 bit
Hostid: geriye kalan 24 bit

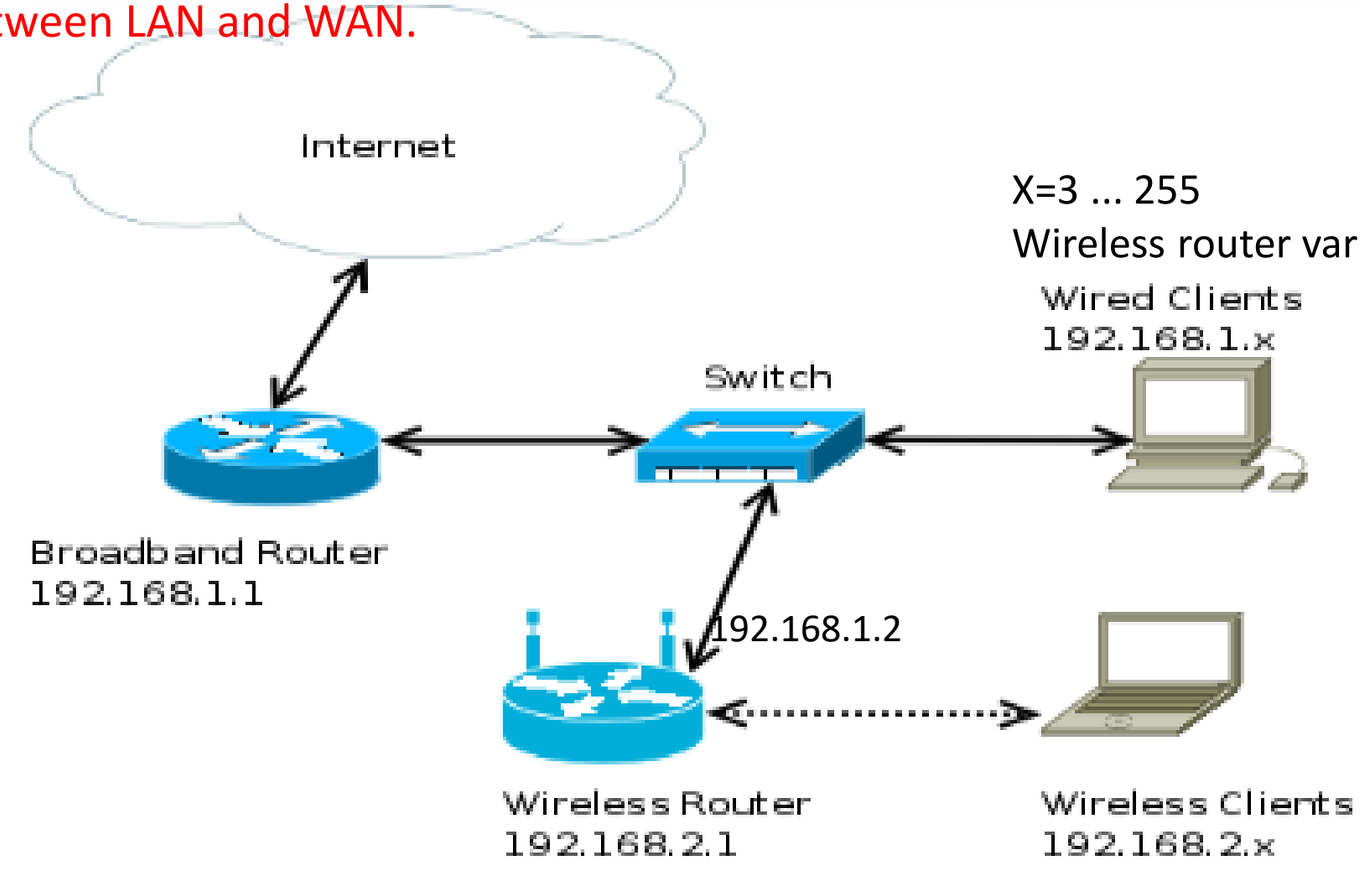
B-Class:
Netid: ilk16bit
Hostid: geriye kalan 16 bit

C-Class:
Netid: ilk 24 bit
Hostid: geriye kalan 8 bit

# Router IP Addressing

- Generally used in LAN-WAN and LAN-LAN connections. It has separate ports for LAN and WAN. It collects and routes data packets.
- The router or gateway connects to another WAN or LAN via a modem. Two connections are important here: the connection port to the communication medium (fiber, satellite, 2 or 4 wires). Ethernet port.
- A router is a network device that connects two or more network segments. Routers are used to transfer information (data packets) from source to destination.
- Routers send information in the form of data packets, and when these data packets are transmitted from one router to another, the router reads the network address in the packets and identifies the destination network.
- Modems are used in communication media between LAN and WAN.

IP addressing: X1.X2.X3.X4
X1, X2, X3, X4: 0,1, ..., 255
1- In X3, a different number is assigned to each LAN group. Since there are 2 different LAN groups in the view on the right, X3 becomes 1,2. 2- X4 is the numbering of computers with ethernet ports. In routers, X4 is always 1.



# LAN – Local Area Network

# Local Area Networks (LAN)

- Local area networks (LANs) are generally formed by combining personal computers to share resources over a communication medium. Hub-switch equipment is used. As the name suggests, the computers connected to these networks are located close to each other within a building.
- While these types of networks are easy to set up and modify, their speeds are lower and the distance between connected computers is shorter.

# Why use a LAN?

- There are two main benefits to using a local area network: information sharing and resource sharing.
- Examples of information sharing include file sharing, email exchange, and internet access.
- Examples of resource sharing include hardware and software sharing, such as sharing an expensive printer.
- Another important resource sharing technique is purchasing software on a per-user basis. For example, instead of buying 20 copies of the same program, purchasing only a 10-user license for a software program on a network with 20 clients.

# Basic LAN Components

- The 8 basic LAN components are:
  1. Clients
  2. Servers
  3. Network Interface Cards
  4. Network Cables: RJ45
  5. Hubs and Switches
  6. Router - Gateway
  7. Network Operating System
  8. QoS

# Local Area Networks

- **Introduction**
  - Why use a LAN? Dedicated servers vs. Peer-to-peer LANs
- **LAN Components**
  - NICs, Cables, Hubs and Network Operating Systems
- **Traditional Ethernet (IEEE 802.3)**
  - Topology, Media Access Control, Ethernet Types
- **Switched Ethernet**
  - Topology, Media Access Control, Performance Benefits
- **Wireless LANs (IEEE 802.11)**
  - Topology, Media Access Control, Wireless Ethernet Types
- **Other Wireless Technologies**
  - Infrared Wireless, Bluetooth
- **Improving LAN Performance**
  - Improving Server Performance, Improving Circuit Capacity, Reducing Network Demand

# LAN – Local Area Networks

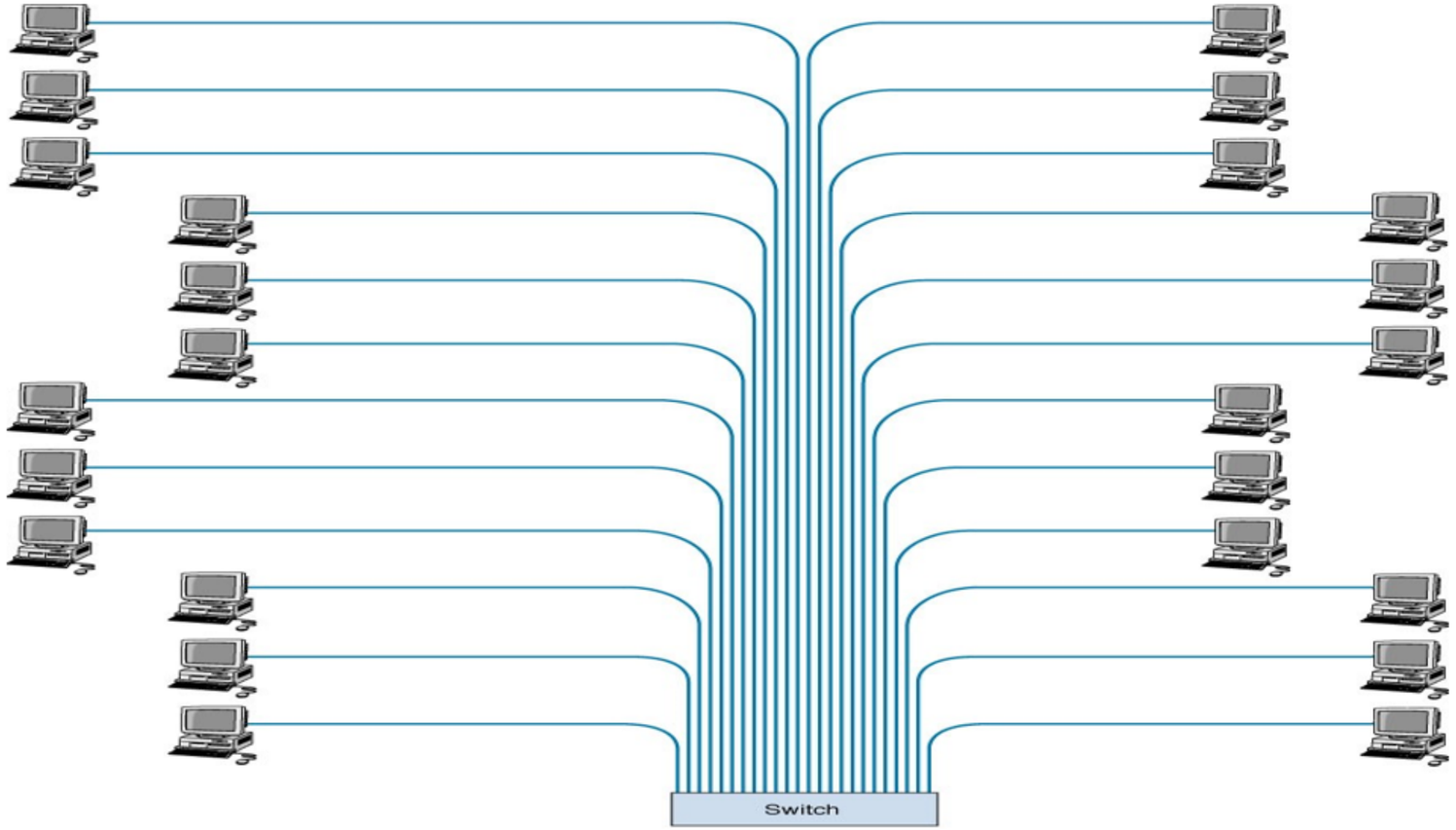
- Devices: LAN: Switch, Hub, Bridge, Repeater, Converter; LAN to WAN: Router, Gateway, Firewall; Modems
- TCP/IP protocol, Ethernet port, RJ45 connector
- Twisted 4-pair data cable; UTP cat5e, Cat6, STP, FTP, S-FTP
- Fiber Cable: Multimode, Single mode, shielded, indoor, outdoor, number of cores, Connector types; SC, ST, MTRJ, LC, Fiber termination, Fiber panel
- Modem interface connection cables: RS232, VGA, HDMI...
- Data socket, Keystone jack
- Patch Panel, Patch cord cable, Organizer, Label
- Edge switch, Backbone switch
- 10/100/1000Base-T
- System Room; Cabinet: Fan, wheels, rack, ducts, UPS, air conditioning, grounding, raised floor, lowered ceiling
- Energy distribution
- Cable routing
- Structural cabling, considerations in cable selection
- Cable tests

What is this system? LAN

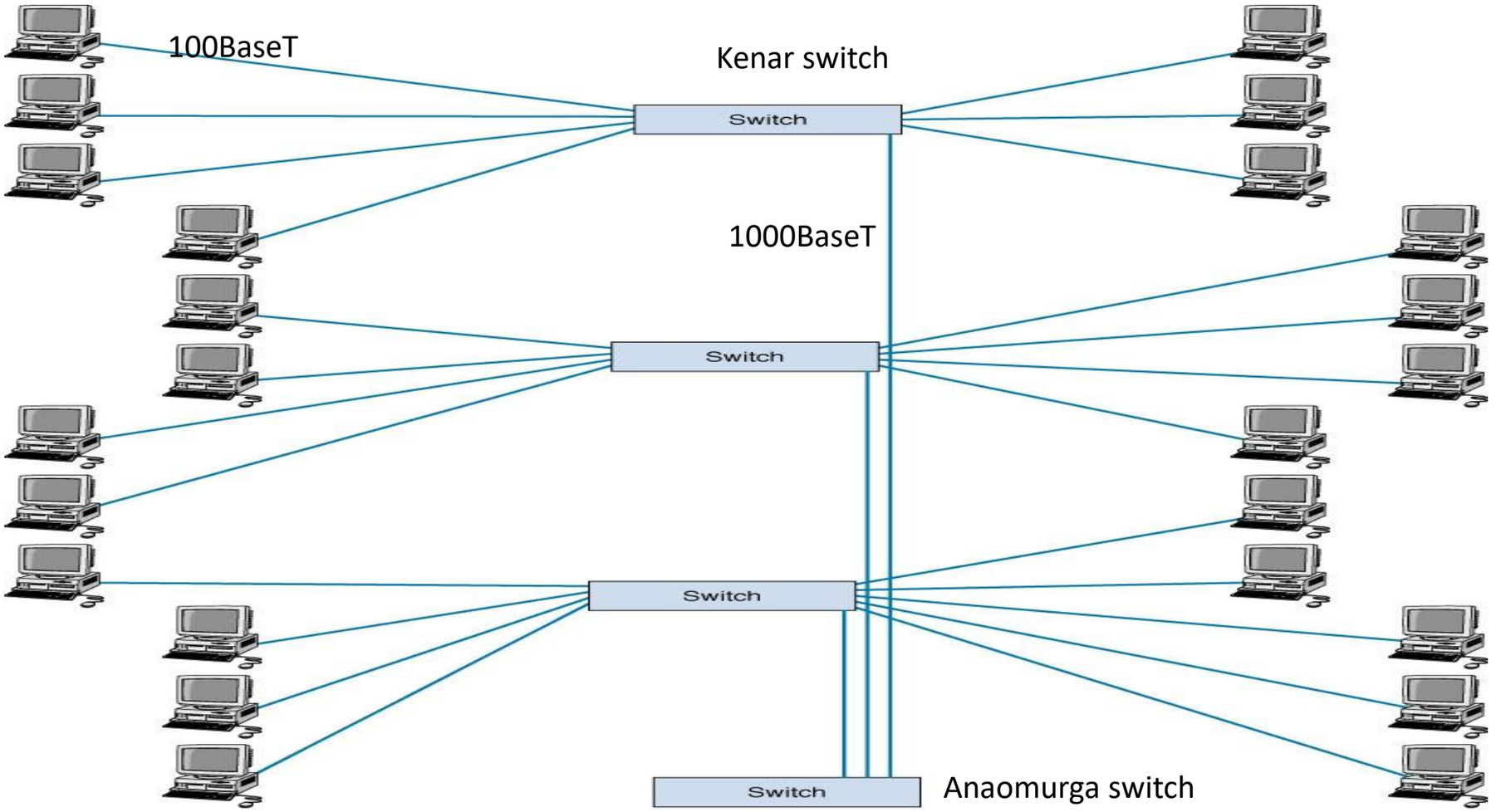
Do the computers connected to the Ethernet switch here communicate with each other? Yes

Can any computer in this system connect to the internet? No

Each one has a different IP address. What is the connection cable: 4 twisted pair, UTP



Fiber optic cable is used when connecting switches to the main backbone switch if the distance is more than 100m. If the distance between the endpoint computer and the edge switch is more than 100m, a Ethernet-to-fiber converter is used. S-FTP 4-pair twisted-pair cable is used in noisy environments.

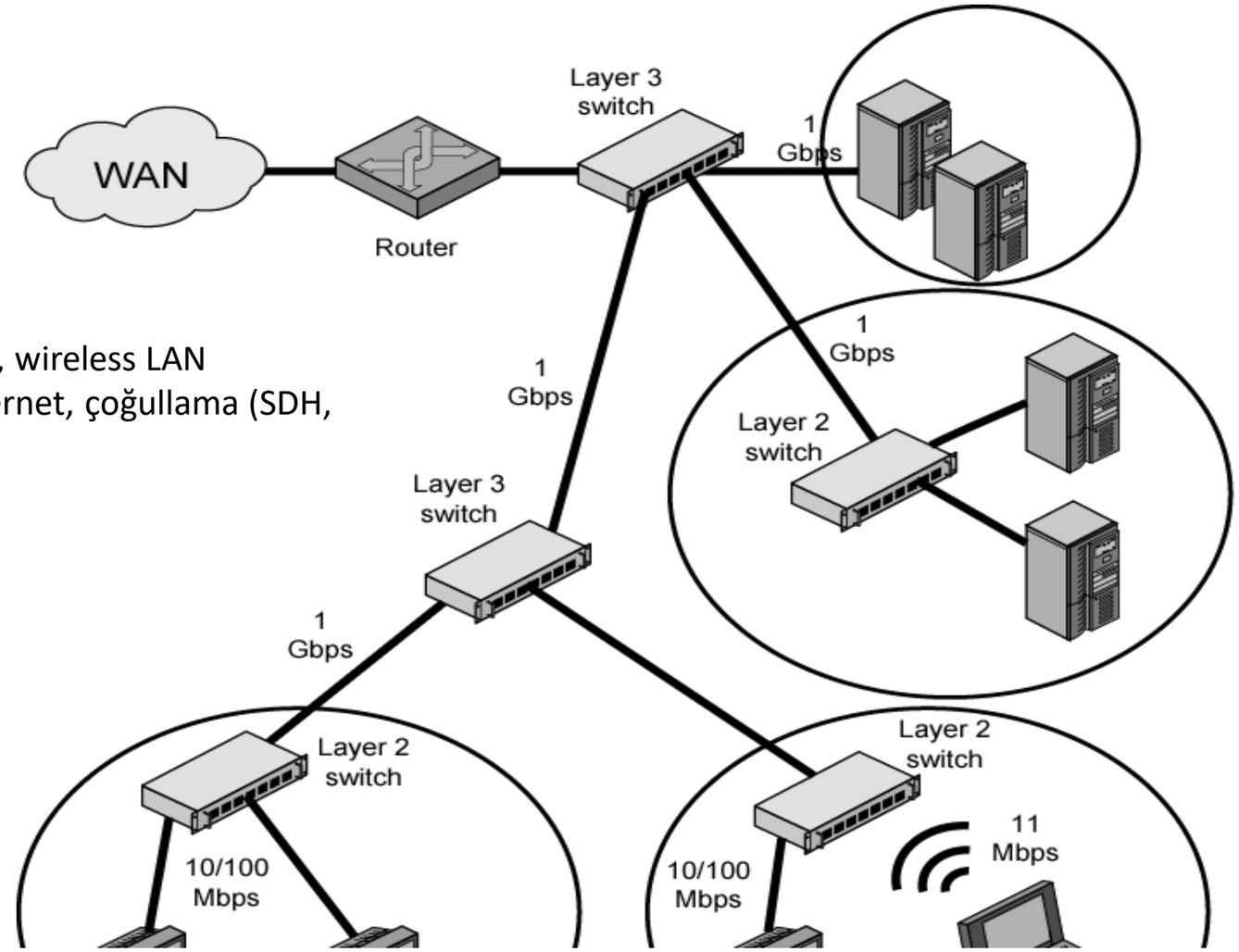



Multi-switch VLAN-based
Collapsed backbone design

# Typical Large LAN Organization Diagram

- ADSL: modem, R/G, Switch, wireless LAN
- WAN: Geniş alan ağlar: internet, çoğullama (SDH, PDH), …

Layer-3: Anaomurga switch
Layer-2: Kenar switch



# Dedicated Server Networks

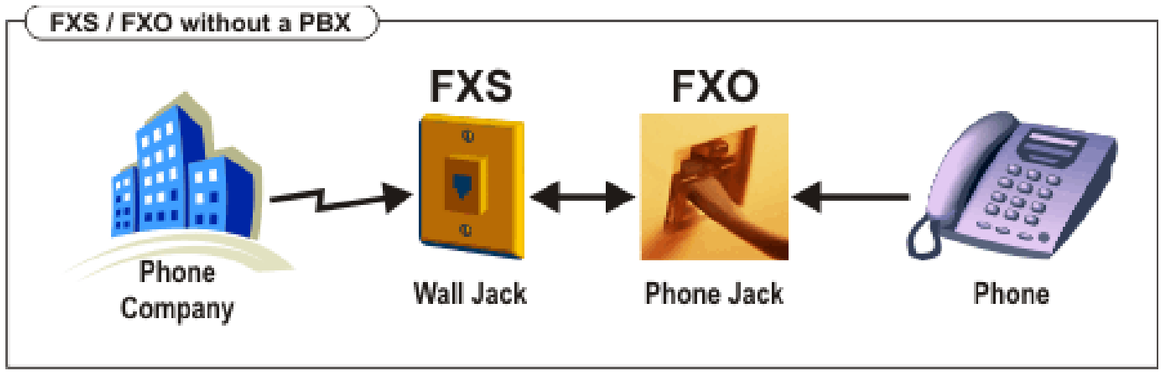
- There is a fundamental LAN duality between dedicated server LANs and peer-to-peer LANs without servers. Since 90% of all LANs have a dedicated server, this section focuses mostly on server-based LANs. A dedicated server is a computer that is permanently assigned a specific server task; for example, a web server, email server, file server, or printer server. Servers also run a special operating system called a server network operating system. When many servers are part of a network, it can be called a server farm. Servers are data-storing devices that collect data. .000
- There is a fundamental LAN duality between dedicated server LANs and peer-to-peer LANs without servers. Since 90% of all LANs have a dedicated server, this section focuses mostly on server-based LANs.
- A dedicated server is a computer that is permanently assigned a specific server task; for example, a web server, email server, file server, or printer server.
- Servers also run a special operating system called a server network operating system.
- When many servers are part of a network, it can be called a server farm.
- Servers are data-storing devices that collect data.

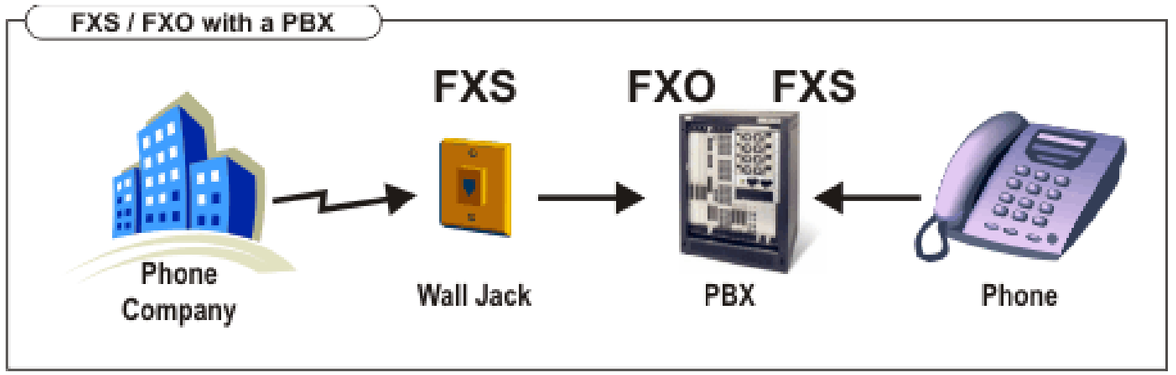
# FXS ve FXO

- FXS ve FXO: Sabit telefon hatlarını IP paketlere dönüştürür. Router ya da Gateway’lere modül olarak bağlanır.
- Günümüzde birçok işletme, geleneksel telefon hatlarının yerini almak için ve iyi bir nedenle, İnternet Üzerinden Ses Protokolü (VoIP) telefon sistemlerini ofislerinde uyguluyor. VoIP, herhangi bir yerden ve herhangi bir zamanda arama yapma ve alma yeteneği, maliyet tasarrufu, daha güvenilir bir sinyal ve daha fazlasını içeren önemli avantajlar sağlar. Ancak VoIP'yi uygulamaya başlamadan önce FXS ve FXO bağlantı noktaları arasındaki farkı anlamanız gerekir.
- Bir aramanın çalışması için, bir FXO bağlantı noktasından bir telekomünikasyon hattının bir FXS bağlantı noktasına bağlanması gerekir ve bunun tersi de geçerlidir. Arama yapma süreci basittir: FXS ve FXO portlarınız bağlandığında, duvardaki FXS portu aracılığıyla telefon şirketinden bir sinyal alacaksınız. Bu sinyal daha sonra cihaza bağlı FXO portuna iletilir, böylece telefonu açtığınızda çevir sesini duyarsınız. Ardından, Çift Tonlu Çoklu Frekans (DTMF) rakamları olarak FXS bağlantı noktasına iletilen telefon numarasını çevirerek arama yapmanızı sağlar.Gelen bir arama aldığınızda, FXS portu aramayı alır ve ardından FXO portu üzerinden uç cihazınıza bir zil voltajı gönderir. Telefon çalacak ve aramayı cevaplamak için açabilirsiniz.
- FXS duvardaki telefon bir fiştir ve FXO telefondaki bir fiştir.
- FXS çevir sesini sağlar ve FXO bunu ister.
- FXS, çağrı alan bir bağlantı noktasıdır; FXO, onu başlatan bir bağlantı noktasıdır.

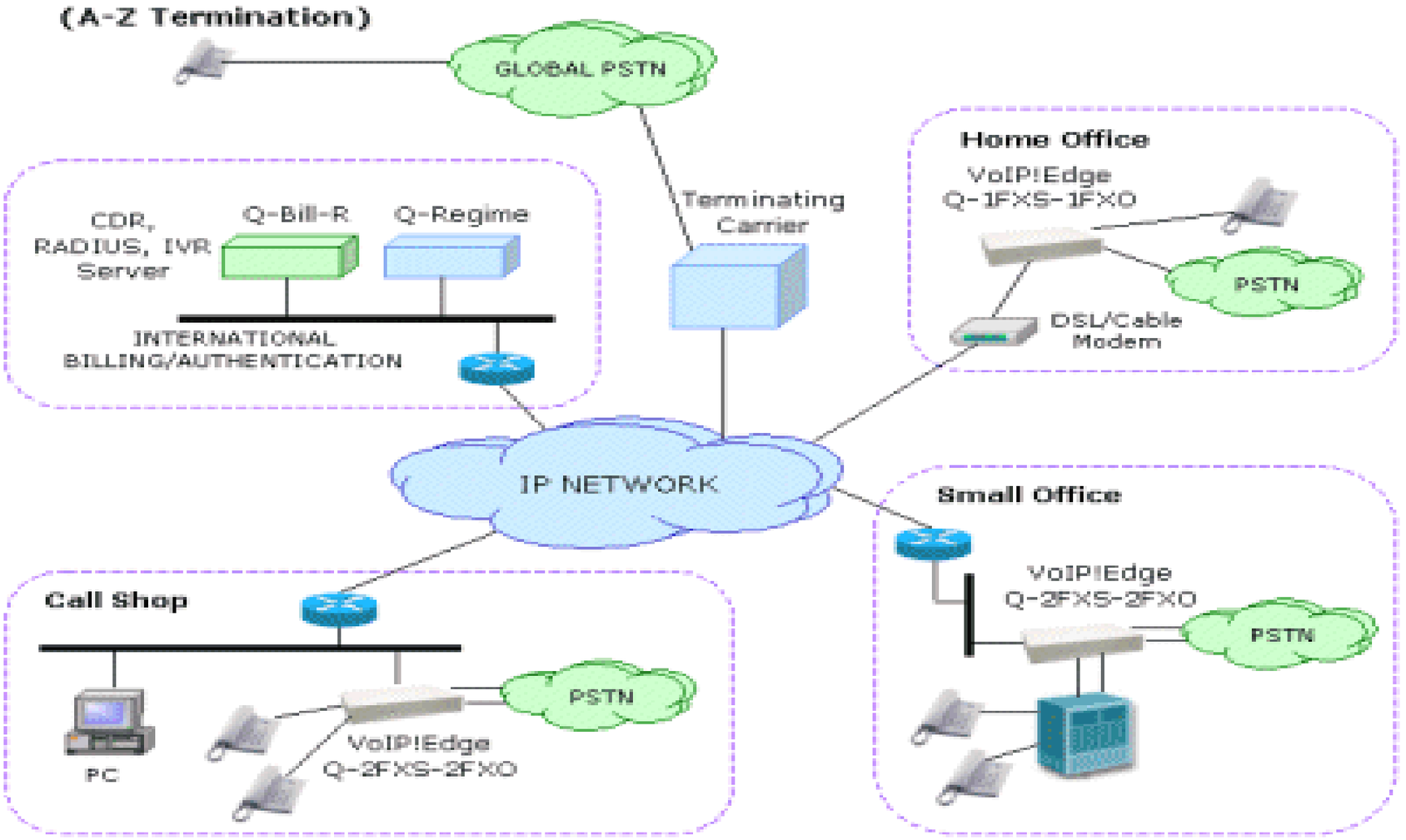
# FXS ve FXO

- FXS ve FXO, Anolog telefon hatlarının kullandığı portlara (fiziksel bağlantıda kullanılan ara birimlere) verilen isimdir (POTS – Eski Düz Telefon Hizmeti olarak da bilinir).
- FXS – Yabancı Santral Abone arabirimi, analog hattı asıl olarak aboneye ulaştıran port' tur. Diğer bir deyişle bu port, çevir sesini, elektrik akımı ve zil voltajını getiren "duvardaki priz"dir. Bir telefon PBX olmadan direkt olarak bir telefon firması tarafından sağlanan FXS arabirimine bağlıdır.
- FXO – Yabancı Santral Ofis arabirimi analog hattı alan port'tur. Telefon ya da faks makinasındaki fiş ya da analog telefon sisteminizdeki fiş(lerdir). Almacın açık veya kapalı oluşuna göre (döngüsel kapanma) hattı alır. FXO portu faks ya da telefon gibi bir cihaza takılı olduğundan, bu cihaz çoğu kez 'FXO cihazı' diye çağrılır.
- Eğer bir PBX'iniz varsa o zaman telefon şirketi tarafından verilen telefon hatlarını ve ardından da telefonları PBX'e bağlarsınız. Bu yüzden PBX'de hem FXO (telefon şirketinin verdiği FXS portlarına bağlanmak için) hem de FXS (telefon veya faks cihazlarına bağlanmak için) portları bulunmalıdır.
- **Bir arama yapmak istediğinizde:** Telefonu kaldırırsınız (FXO cihaz). FXS portu almacı kaldırdığınızı algılar. Telefon numarasını çevirirsiniz, bu FXS portuna Çift Tonlu Çoklu Frekans olarak geçer.
- **Gelen arama:** FXS portu bir arama alır ve sonra takılı FXO cihazına bir zil voltajı gönderir. Telefon çalar. Almacı kaldırır kaldırmaz aramaya cevap verebilirsiniz.

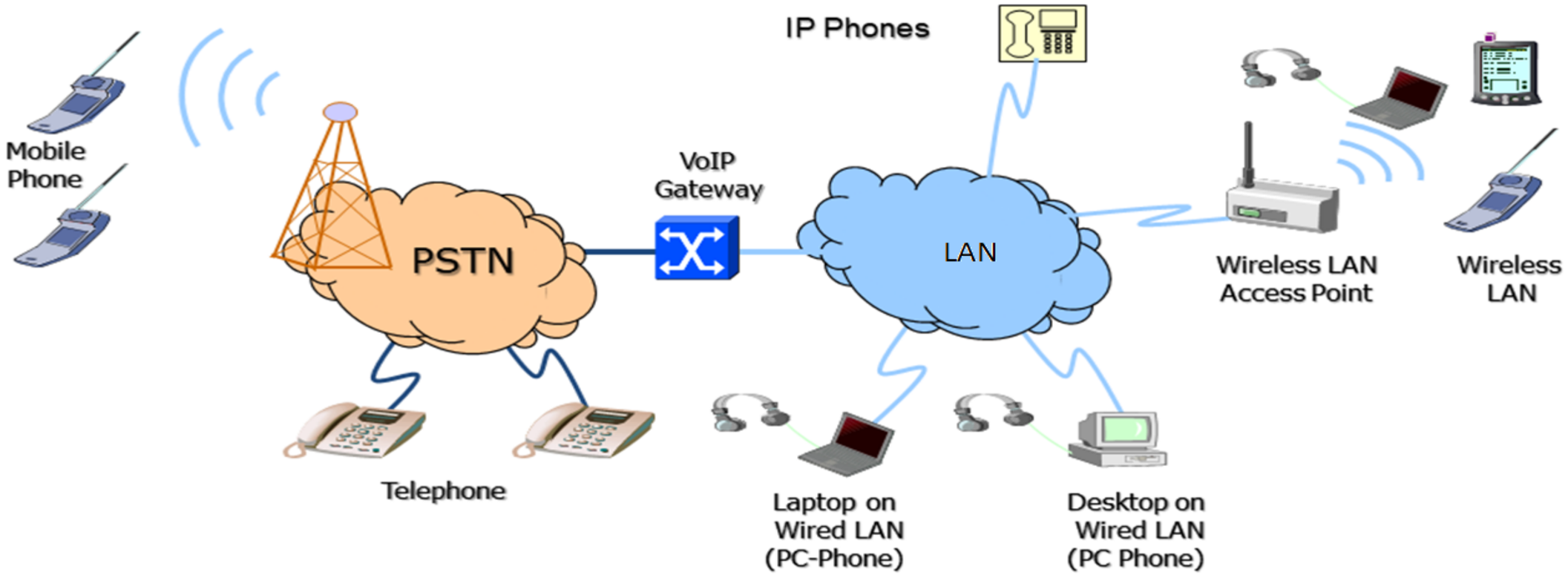


# Internet-based telephone calling services

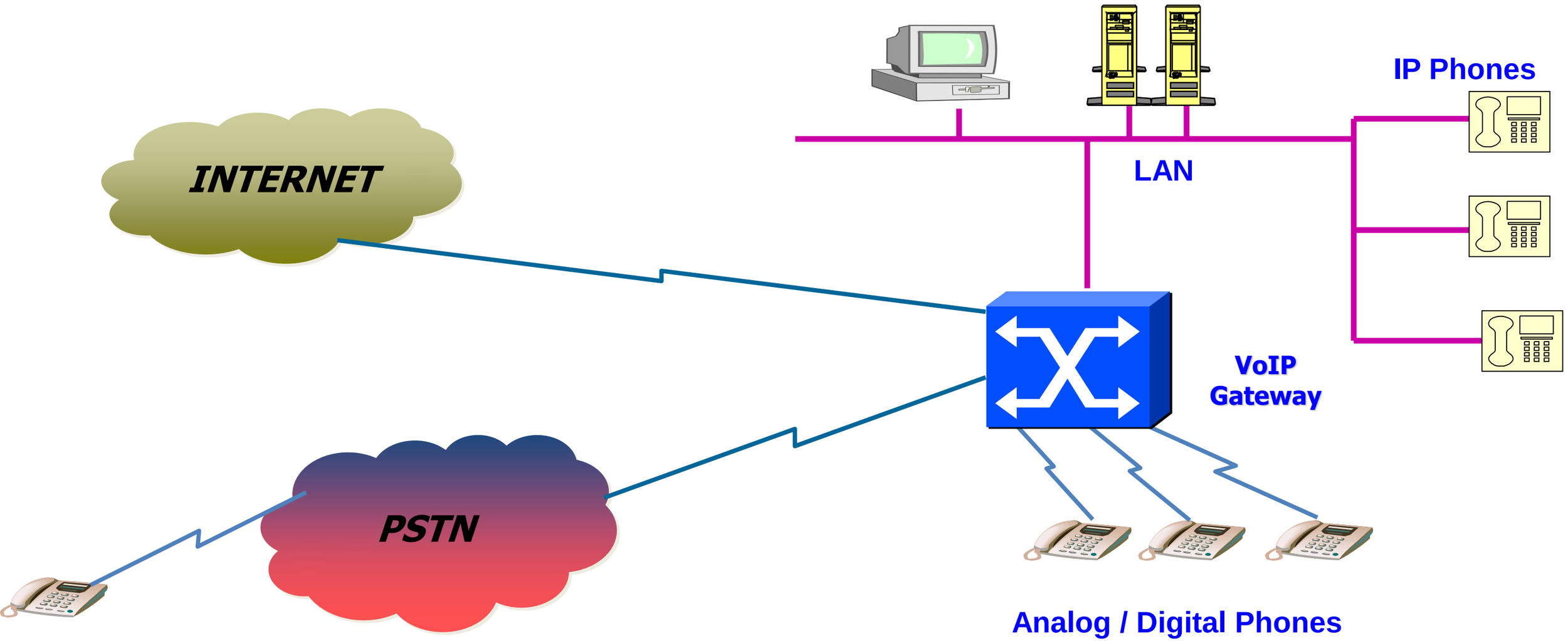


# IP GATEWAY




What device is used to connect telephone lines from a PSTN exchange to a LAN?GW

# IP PBx & VoIP

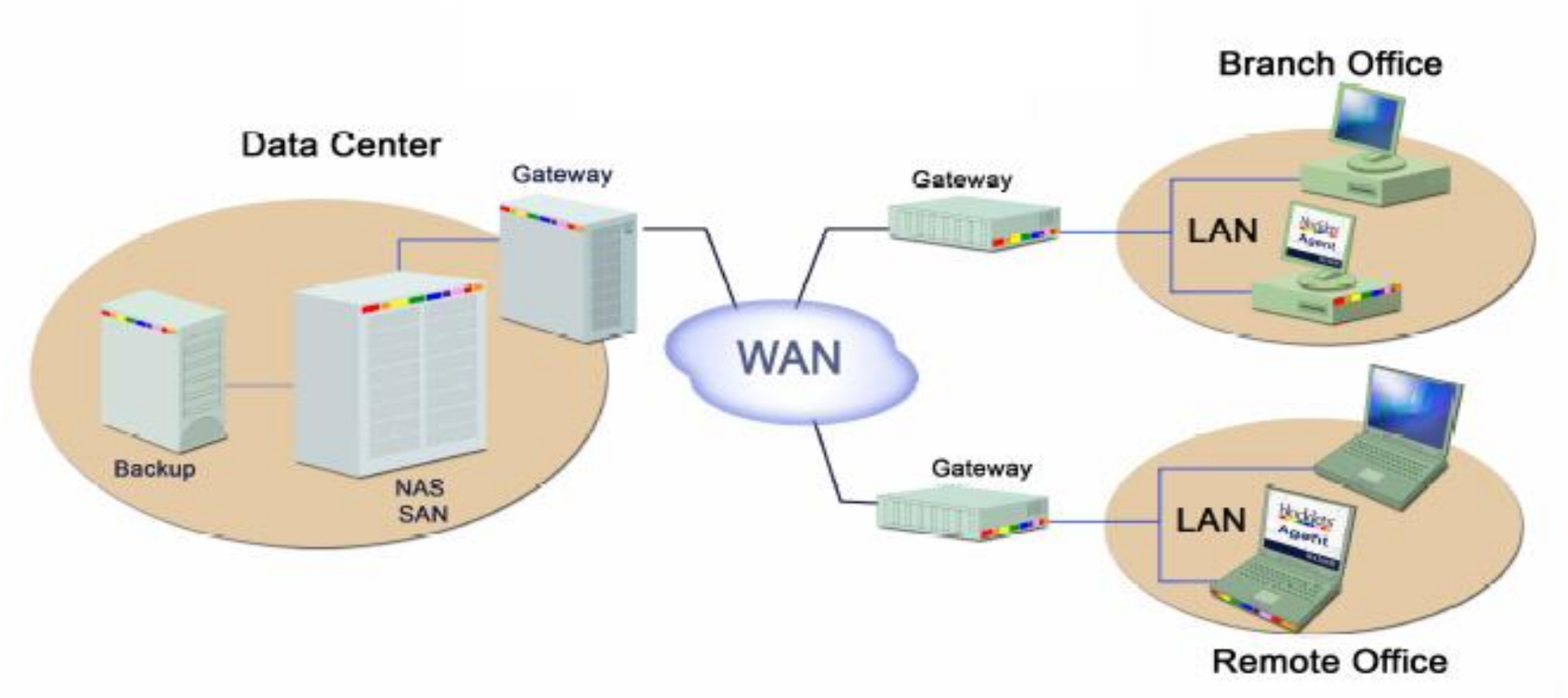

IP Phones
INTERNET
LAN
VoIP
Gateway
PSTN
Analog / Digital Phones

# WAN Access Technologies

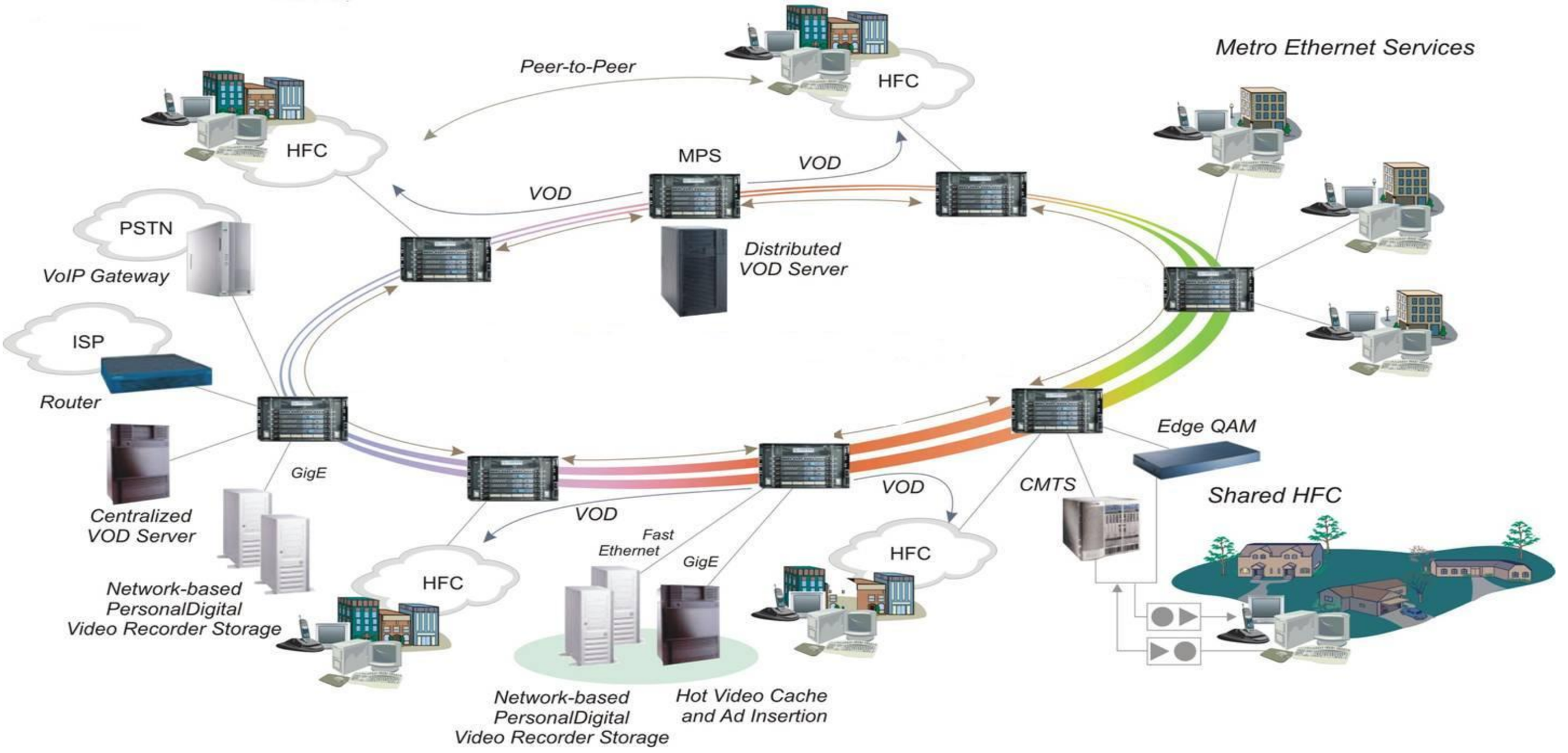
# WAN Erişim Teknolojileri

- Public Switched Telephone Network (PSTN)
- World-wide and voice oriented (handles voice and data)
- Data/voice can be transferred  within the PSTN using different technologies (data transfer rate bps)
- Dial-up lines: Analog signals passing through telephone lines. Requires modems (56 kbps transfer rate).
- ISDN lines:
  - Integrated Services Digital Network
  - Digital transmission over the telephone lines
  - Can carry (multiplex) several signals on a single line
- DSL: Digital subscribe line, ADSL (asymmetric DSL) : receiver operated at 8.4 Mbps, transmit at 640 kbps
- E-Carrier lines: carries several signals over a single line
- PDH - SDH
- Leased Line (kiralık Hat)
- Frame Relay
- X.25
- ATM: Asynchronous Transfer Mode , Fast and high capacity transmitting technology. Packet technology.
- Ana omutrga switch, Router, Gateway

# Geniş Alan Ağlara Erişim

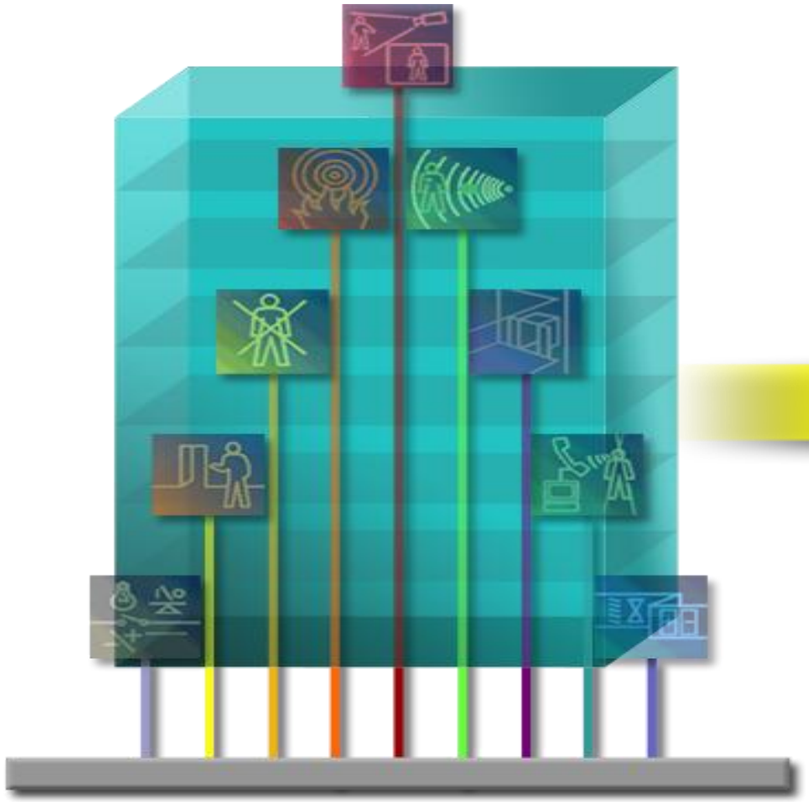


# City Backbone Network Infrastructure

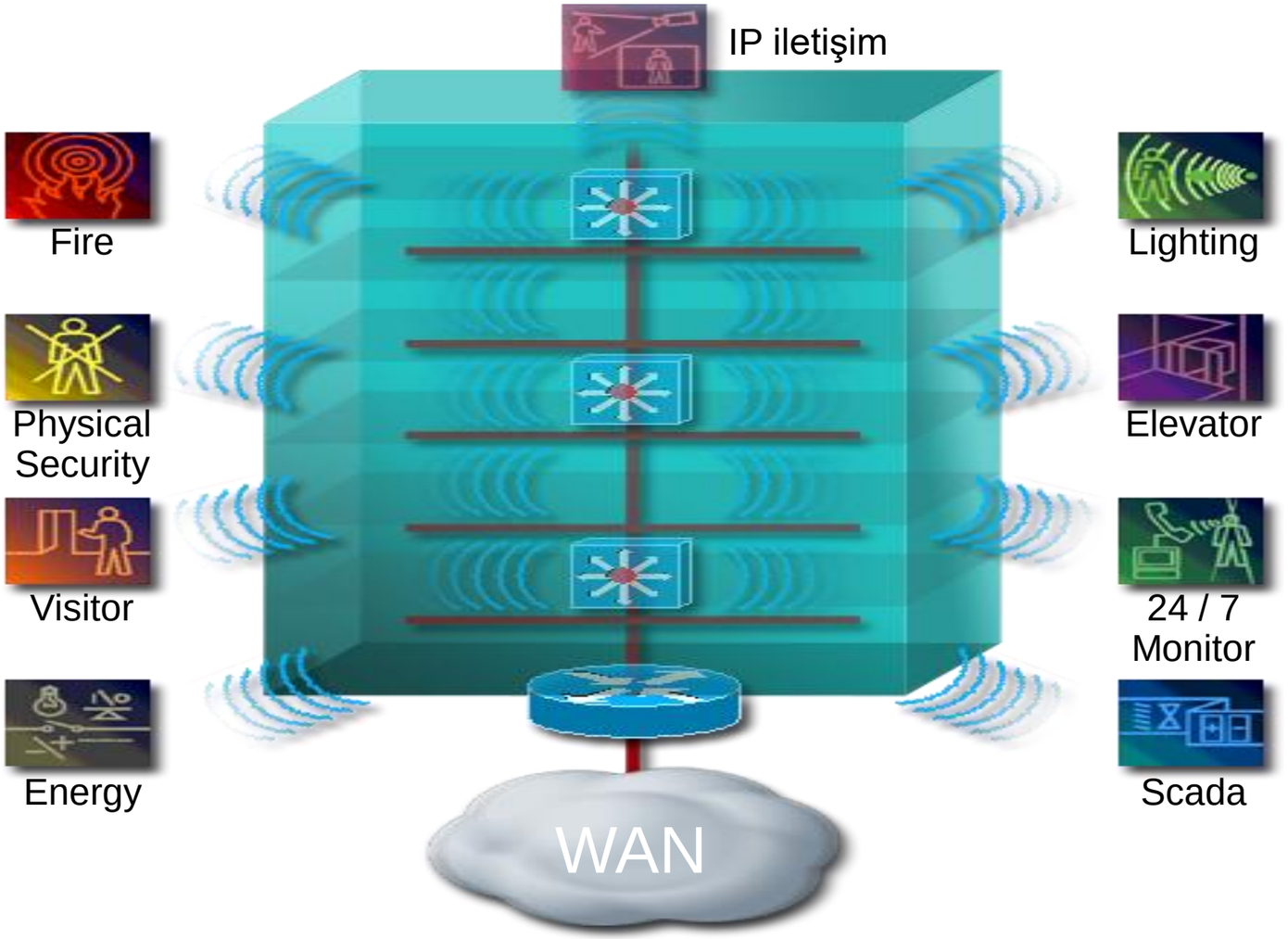


# BUILDING INFRASTRUCTURE

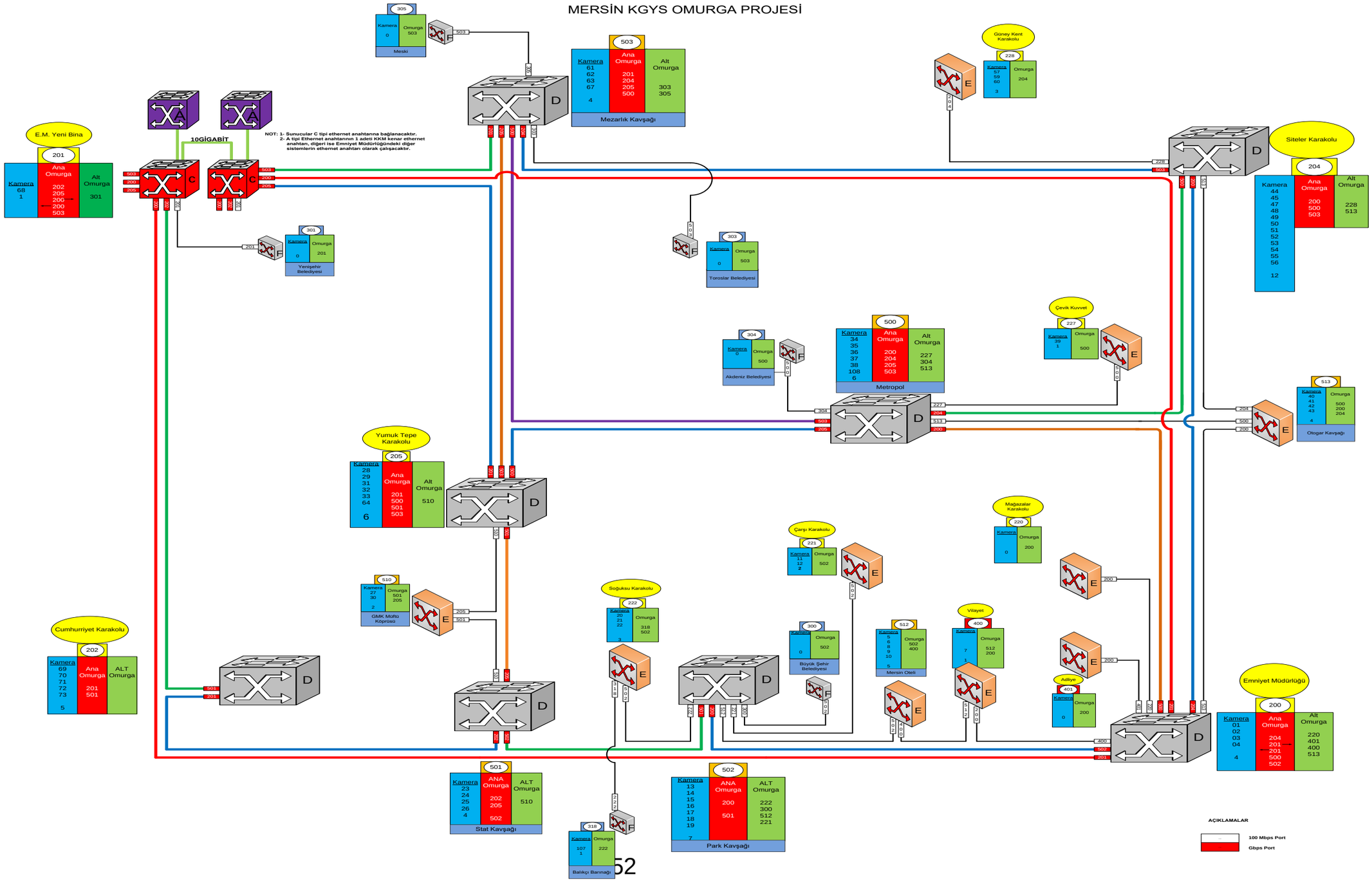
## LEGACY
Disparate Networks



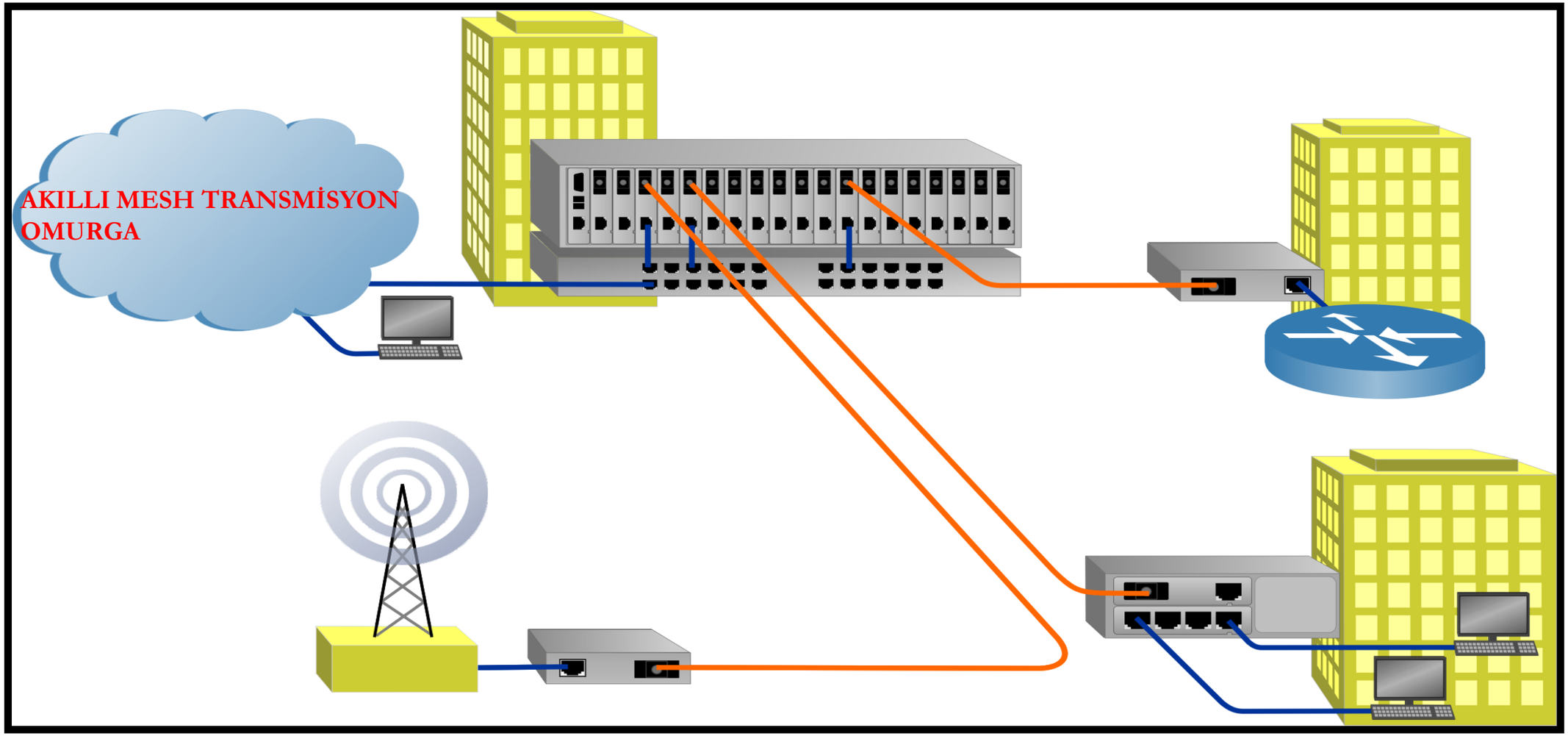
## TODAY
Network



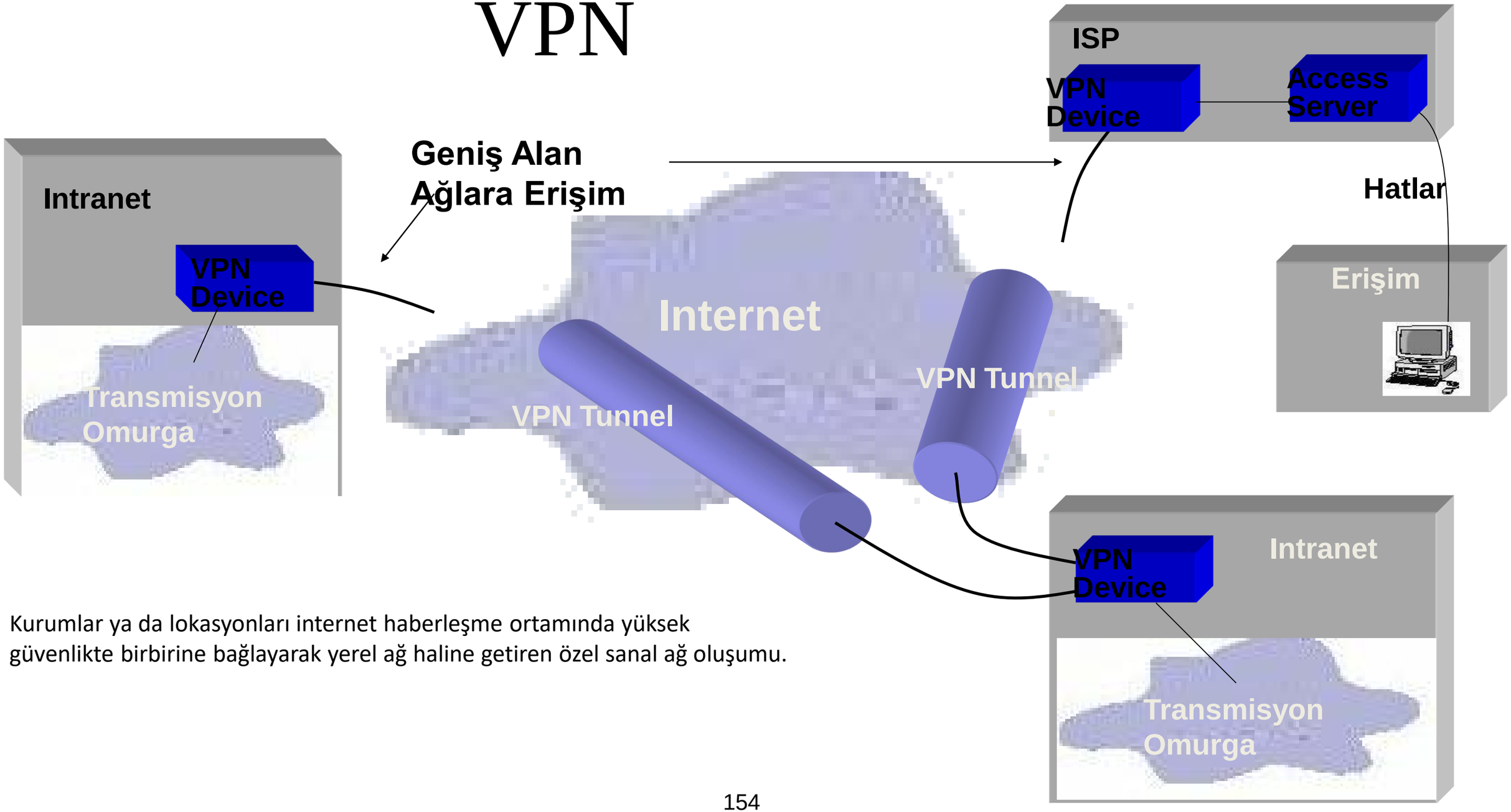
GİGA BİT MESH ANA OMURGA



# Gigabit - AĞ ANAHTARLAMA



# VPN




Kurumlar ya da lokasyonları internet haberleşme ortamında yüksek güvenlikte birbirine bağlayarak yerel ağ haline getiren özel sanal ağ oluşumu.

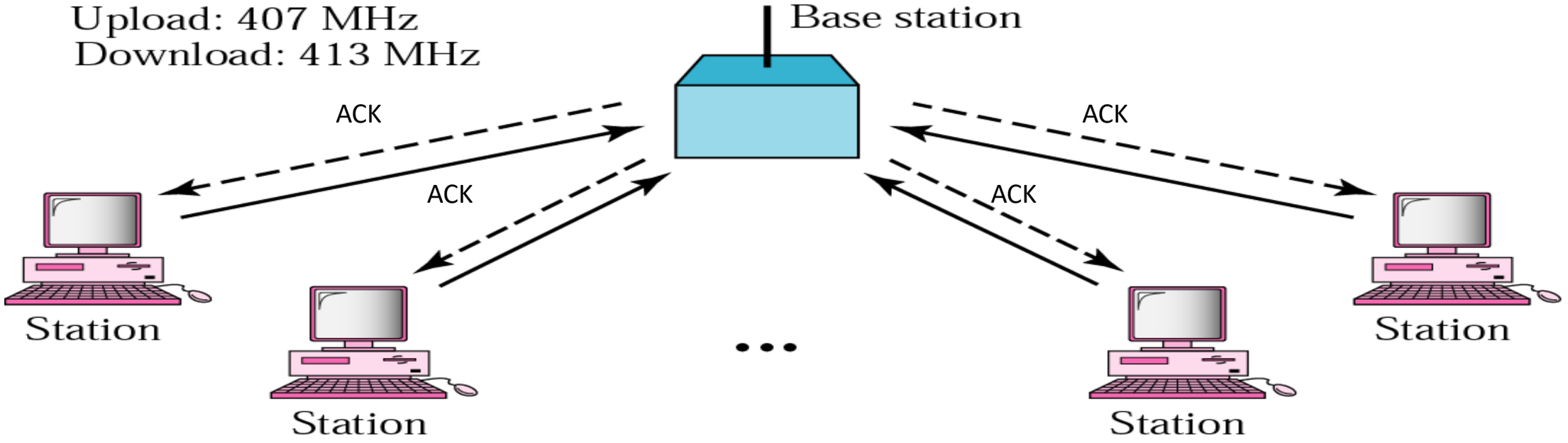
# Wireless Ethernet

# Contention Protocols

- **ALOHA**
  - Developed in the 1970s for a packet radio network by Hawaii University.
  - Whenever a station has a data, it transmits. Sender finds out whether transmission was successful or experienced a collision by listening to the broadcast from the destination station. Sender retransmits after some random time if there is a collision.
- **Slotted ALOHA**
  - Improvement: Time is slotted and a packet can only be transmitted at the beginning of one slot. Thus, it can reduce the collision duration.

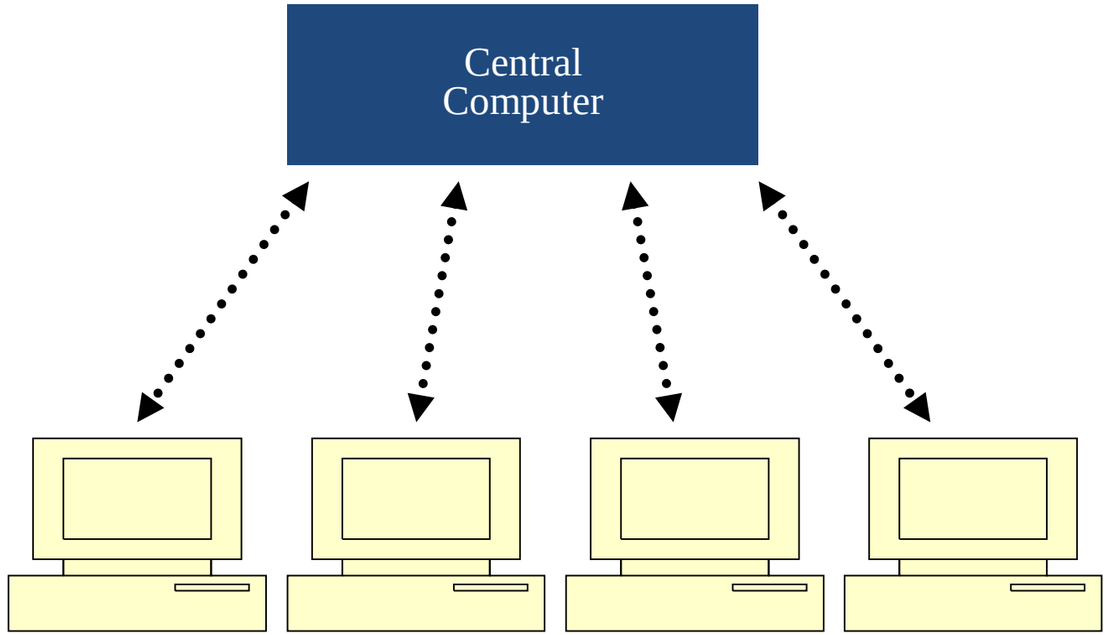
# ALOHA Network

- Developed by Norm Abramson at the Univ. of Hawaii
  - the guy had interest in surfing and packet switching
  - mountainous islands → land-based network difficult to install
  - fully decentralized protocol



# Aloha

- Nodes sends the message when it has data to send.
- If it receives an ack, it considers the transmission completed, otherwise it retransmits after a random delay.
- Simple, distributed protocol, but not very efficient
  - 18% maximum utilization
- Slotted Aloha: more efficient.
  - Reduces chances of collision
  - 37% maximum utilization



# Wireless Ethernet (IEEE 802.11)

- Kablosuz LAN'lar kablolardan vazgeçer ve sinyalleri havadan iletmek için radyo veya kızılötesi frekansları kullanır.
- WLAN'lar, kablolamayı ortadan kaldırdıkları ve çeşitli konumlardan ve gezgin çalışanlar için (hastanede olduğu gibi) ağ erişimini kolaylaştırdıkları için popülaritesi artmaktadır.
- En yaygın kablosuz ağ standardı, genellikle Kablosuz Ethernet veya Kablosuz LAN olarak adlandırılan IEEE 802.11'dir.

# Wireless LAN Topology

- WLAN topolojileri Ethernet'dekiyle aynıdır: fiziksel yıldız, mantıksal veri yolu
- Kablosuz LAN aygıtları aynı radyo frekanslarını kullanır, bu nedenle sırayla ağı kullanmaları gerekir.
- Hub'lar yerine, WLAN'lar erişim noktaları (AP) adı verilen cihazları kullanır. Maksimum iletim aralığı yaklaşık 30-130m. Genellikle, bir bina veya kurumsal kampüste çeşitli alanlarda kablosuz erişimi mümkün kılan bir dizi AP kurulur.
- Her WLAN bilgisayarı, radyo sinyallerini AP'ye ileten bir NIC kullanır.
- Erişim kolaylığı nedeniyle, güvenlik potansiyel bir sorundur, bu nedenle IEEE 802.11, gizli dinlemeyi önlemek için 40 bit veri şifreleme kullanır.
- Kablosuz LAN'lar CSMA / CA kullanır, burada (CA =  collision avoidance). CA ile, bir istasyon başka bir istasyonun iletimini bitirene kadar ve herhangi bir şey göndermeden önce ek bir rastgele süre bekler.
- Şu anda iki farklı WLAN MAC tekniği kullanılmaktadır: Fiziksel Taşıyıcı Algılama Yöntemi ve Sanal Taşıyıcı Algılama Yöntemi.

# Types of Wireless Ethernet

- Two forms of the IEEE 802.11b standard currently exist, utilizing the 2.5 GHz band:
  - **Direct Sequence Spread Spectrum** (DSSS) uses the entire frequency band to transmit information. DSSS is capable of data rates of up to 11 Mbps with fallback rates of 5.5, 2 and 1 Mbps. Lower rates are used when interference or congestion occurs.
  - **Frequency Hopping Spread Spectrum** (FHSS) divides the frequency band into a series of channels and then changes its frequency channel about every half a second, using a pseudorandom sequence. FHSS is more secure, but is only capable of data rates of 1 or 2 Mbps.
- **IEEE 802.11a** uses Orthogonal Frequency Division Multiplexing (OFDM), operates in the 5 GHz band with data rates of up to 54 Mbps.
- **IEEE 802.11g** uses OFDM in the 2.5 GHz band, operates at up to 54 Mbps, and is compatible with 802.11b

# Infrared Wireless LANs

- **Infrared WLANs** are less flexible than IEEE 802.11 WLANs because, as with TV remote controls that are also infrared based, they require line of sight to work.
- Infrared Hubs and NICs are usually mounted in fixed positions to ensure they will hit their targets.
- The main advantage of infrared WLANs is reduced wiring.
- A new version, called **diffuse infrared**, operates without a direct line of sight by bouncing the infrared signal off of walls, but is only able to operate within a single room and at distances of only about 50-75 feet.

# Bluetooth

- Bluetooth is a 1 Mbps wireless standard developed for **piconets**, small personal or home networks.
- It may soon be standardized as IEEE 802.15.
- Although Bluetooth uses the same 2.4 GHz band as Wireless LANs it is not compatible with the IEEE 802.11 standard and so can not be used in locations that use the Wireless LANs.
- Bluetooth's controlled MAC technique uses a master device that polls up to 8 "slave" devices.
- Examples of Bluetooth applications include; linking a wireless mouse, a telephone headset, or a Palm handheld computer to a home network.

# Kaynaklar


- Analog Electronics,  Bilkent Unıversity
- Electric Circuits Ninth Edition, James W. Nilsson Professor Emeritus Iowa State University, Susan A. Riedel Marquette University, Prentice Hall, 2008.
- Fundamentals of Electrical Engineering, Don H. Johnson, Connexions, Rice University, Houston, Texas, 2016.
- Introduction to Electrical and Computer Engineering, Christopher Batten - Computer Systems Laboratory School of Electrical and Computer Engineering, Cornell University, ENGRG 1060 Explorations in Engineering Seminar, Summer 2012.
- Basics of Electrical Electronics and Communication Engineering, K. A. NAVAS Asst.Professor in ECE, T. A. Suhail Lecturer in ECE, Rajath Publishers, 2010.
- https://www.ics.uci.edu/

# Usage Notes

- These slides were gathered from the presentations published on the internet. I would like to thank  who prepared slides and documents.
- Also, these slides are made publicly available on the web for anyone to use
- If you choose to use them, I ask that you alert me of any mistakes which were made and allow me the option of incorporating such changes (with an acknowledgment) in my set of slides.

Sincerely,

Dr. Cahit Karakuş

**cahitkarakus@gmail.com**