Chapter 6

Switching Technologies and Network Devices

Switched Networks

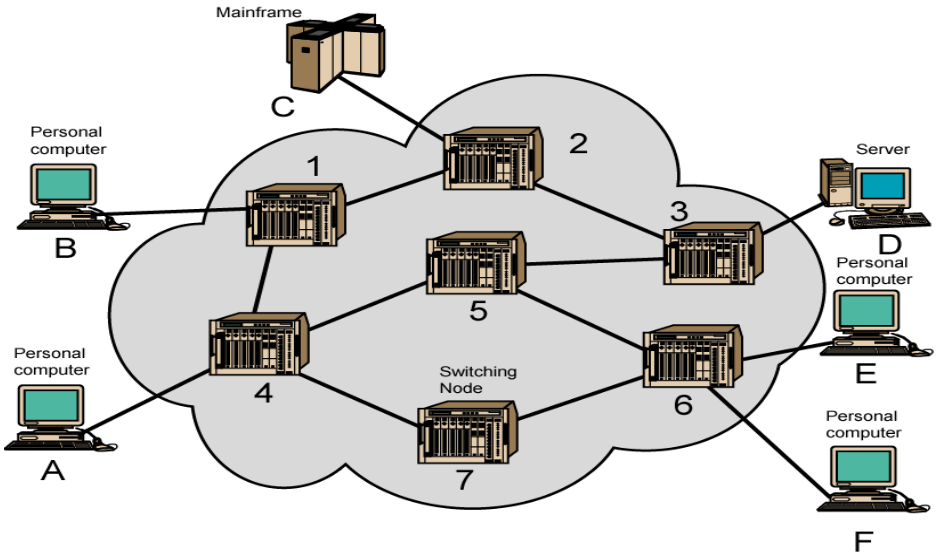
- A network is a set of connected devices
- Switching is the act of connecting multiple devices to make communication possible.
- Switched network consists of series of switch
- Long distance transmission between stations (called "end devices") is typically done over a network of switching nodes.
- A collection of nodes and connections forms a communications network.

Switched Networks

- Switching nodes do not concern with content of data. Their purpose is to provide a switching facility that will move the data from node to node until they reach their destination (the end device).
- In a switched communications network, data entering the network from a station are routed to the destination by being switched from node to node.
- Switching methods are used to connect the multiple communicating devices with one another.

Switching Technology

- Switching is the technique by which nodes control or switch data to transmit it between specific points on a network
- Two types of Switching Technologies
  - Circuit Switching
  - Packet Switching



Circuit Switching

- A circuit switched network is one that establishes a dedicated circuit or channel between nodes and terminals (end to end) before the users may communicate
- Circuit switching dynamically establishes a dedicated virtual connection for voice or data between a sender and a receiver
- Before communication can start, it is necessary to establish the connection through the network of the service provider

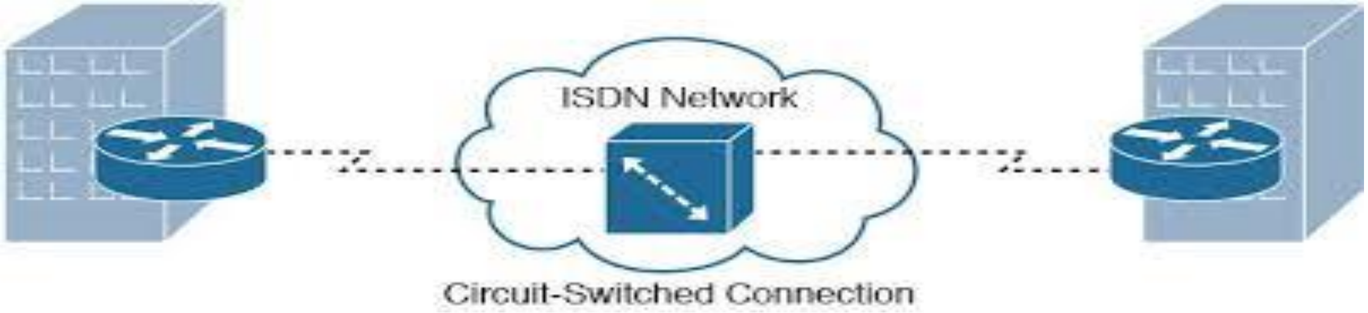
Circuit Switching Networks

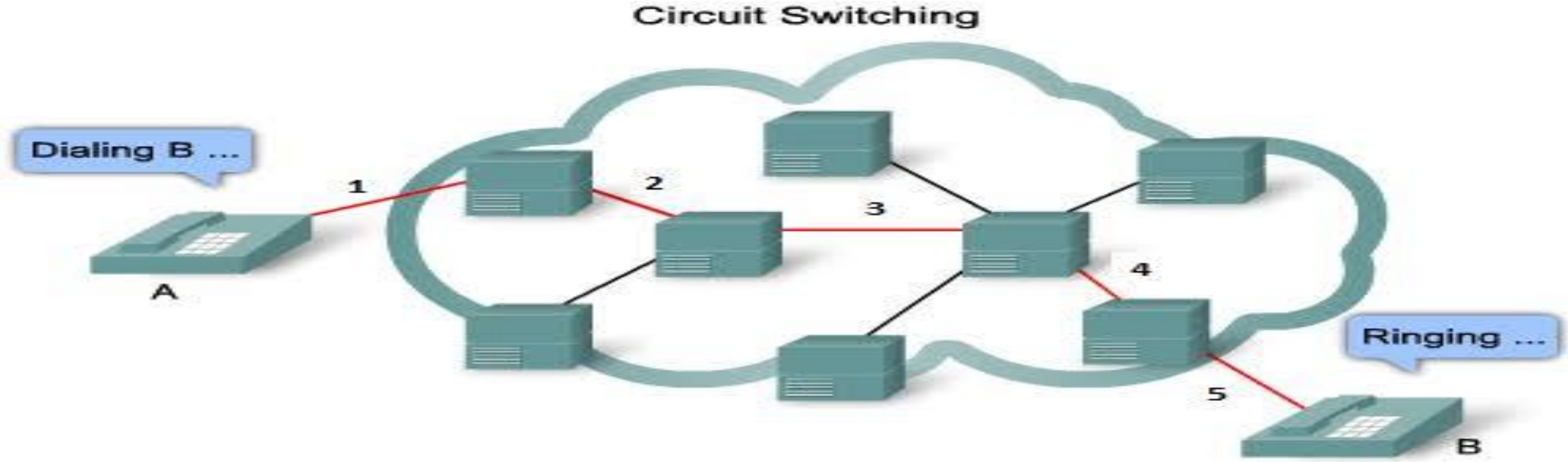
- The two most common types of circuit switched networks
  - The Public Switched Telephone Network (PSTN)
  - Plain Old Telephone System (POTS)
  - The Integrated Service Digital Network (ISDN)
- The actual communication in circuit switched network requires three phases
  - Connection Setup
  - Data Transfer
  - Circuit disconnect

Circuit Switching Properties

- Inefficiency
  - Channel capacity is dedicated for the whole duration of a connection. If no data, capacity is wasted
- Delay
  - Long initial delay: circuit establishment takes time
- Developed for voice
  - Resources dedicated to a particular call
- Data rate is fixed
  - Both ends must operate at the same rate during the entire period of connection

Circuit Switching





Packet Switching

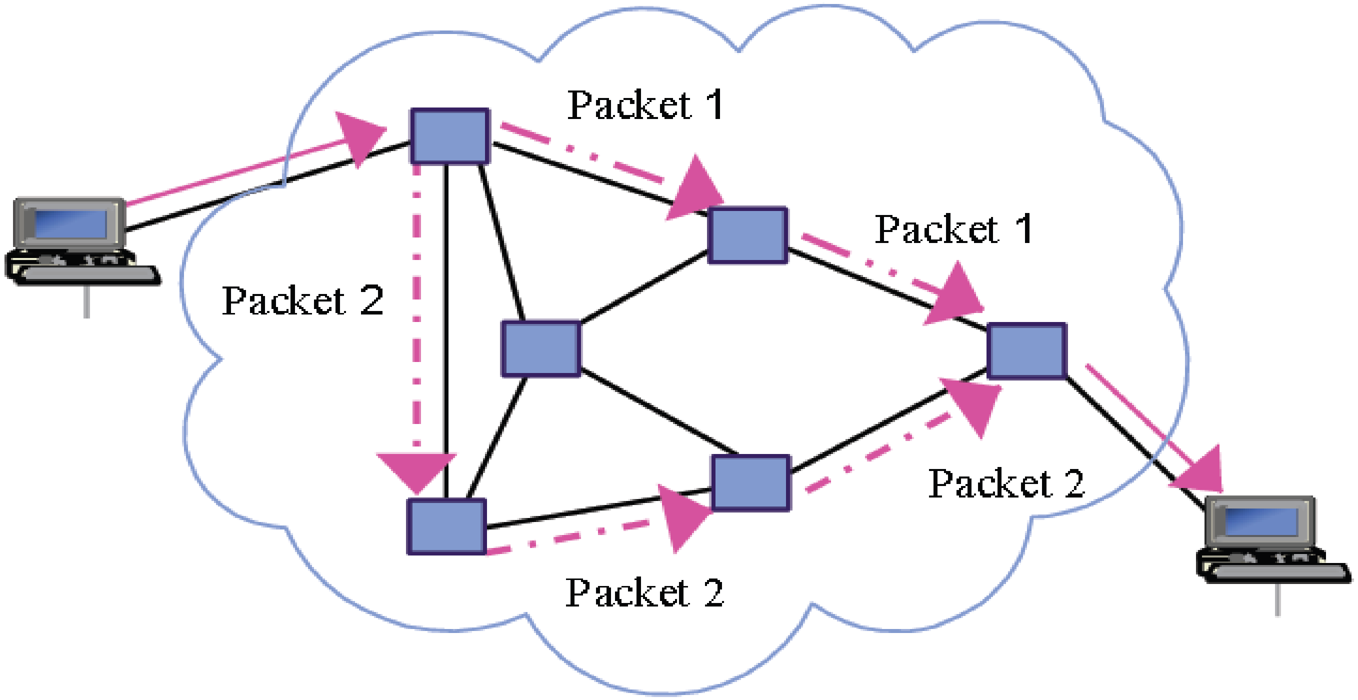
- Packet switching splits traffic data in to packets that are routed over a shared network
- Packet-switched networks move data in separate, small blocks (packets) based on the destination address in each packet.
- Packet switched network do not require a circuit to be established
- The switches in packet switched network (PSN) determine the links that packets must be sent over based on the addressing information in each packet

Packet Switching

- When the path is established temporarily while a packet is travelling through it, and then breaks down again, it is called a **virtual circuit** (VC)
- Because the internal links between the switches are shared between many users, the cost of packet switching network is lower than that of circuit-switching network
- Packet switching is designed to address the problems of circuit switching.

Packet Switching

- Packet switching is a WAN technology in which users share common carrier resources.



Networking Devices

- NIC
- Hub
- Switch
- Repeater
- Bridge
- Router
- Brouter
- Others? -Explore!

Network Interface Card (NIC)

At source:

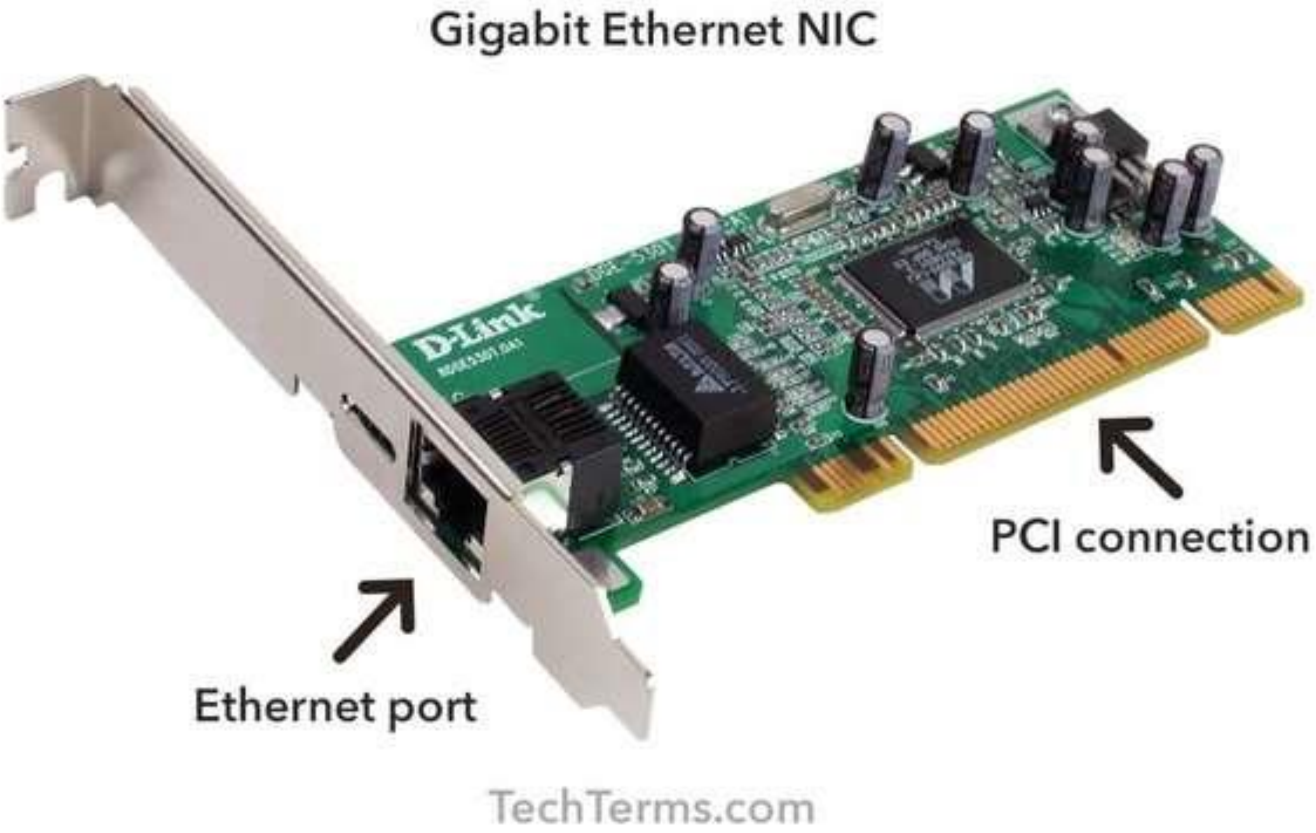
- Receives the data packet from the Network Layer
- Attaches its MAC address to the data packet
- Attaches the MAC address of the destination device to the data packet
- Converts packets in to electrical, light or radio signals
- Provides the physical connection to the media

Network Interface Card (NIC)

As a destination device

- Provides the physical connection to the media
- Translates the signal in to data
- Reads the MAC address to see if it matches its own address
- If it does match, passes the data to the Network Layer

Network Interface Card (NIC)



Hub

- A central point of a star topology
- Allows the multiple connection of devices
- Can be more than a basic Hub – providing additional services (Managed Hubs, Switched Hubs, Intelligent Hubs)
- Hub is a Repeater with multiple ports
- Functions in a similar manner to a Repeater
- Works at the Physical Layer of the OSI model
- Passes data no matter which device it's addressed to; and this feature adds to congestion

Hub

Advantages

- Cheap,
- can connect different media types

Disadvantages

- Extends the collision domain
- can not filter information,
- passes packets to all connected segments

Switch

- A multiport Bridge, functioning at the Data Link Layer
- Each port of the bridge decides whether to forward data packets to the attached network
- Keeps track of the Mac addresses of all attached devices (just like a bridge)
- Switch is active hub
- Acts like a Hub, but filters like a Bridge
- Each port on a Switch is a collision domain

Switch

Advantages

- Limits the collision domain,
- can provide bridging,
- can be configured to limit broadcast domain

Disadvantages

- More expensive than a hub or bridge,
- configuration of additional functions can be very complex

Repeater

- Allows the connection of network segments
- Extends the network beyond the maximum length of a single segment
- Functions at the Physical Layer of the OSI model
- A multi-port repeater is known as a Hub
- Connects segments of the same network, even if they use different media
- Has three basic functions
  - Receives a signal which it cleans up
  - Re-times the signal to avoid collisions
  - Transmits the signal on to the next segment

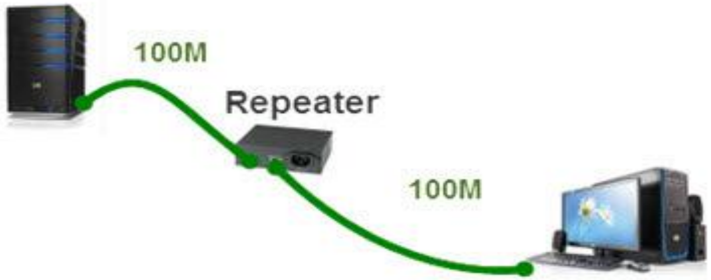
Repeater

Advantages

- Can connect different types of media
- can extend a network in terms of distance
- does not increase network traffic

Disadvantages

- Extends the collision domain,
- can not connect different network architectures,



Bridge

- Like a Repeater or Hub it connects segments of a network
- Works at Data Layer – not Physical layer
- Uses Mac address to make decisions
- Acts as a ’filter’, by determining whether or not to forward a packet on to another segment
- Filters packets, does not forward them, by examining their MAC address
- Builds a Bridging Table, keeps track of devices on each segment

Bridge

- It forwards packets whose destination address is on a different segment from its own
- It divides a network in to multiple collision domains – so reducing the number of collisions

Bridge

Advantages –

- Limits the collision domain,
- can extend network distances,
- uses MAC address to filter traffic, eases congestion,
- can connect different types of media, some can connect differing architectures

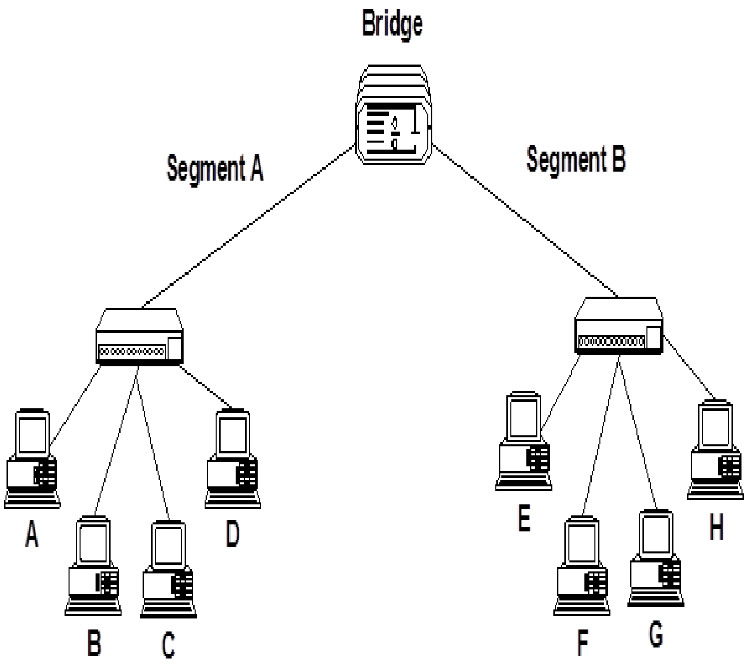
Disadvantages –

- more expensive than a repeater,
- slower than a repeater – due to additional processing of packets

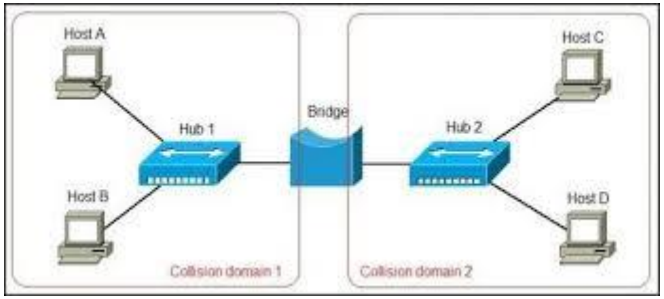
Bridge

- Uses the Spanning Tree Protocol (STP) – to decide whether to pass a packet on to a different network segment

A Transmits to C, bridge **will not** pass it to Segment B

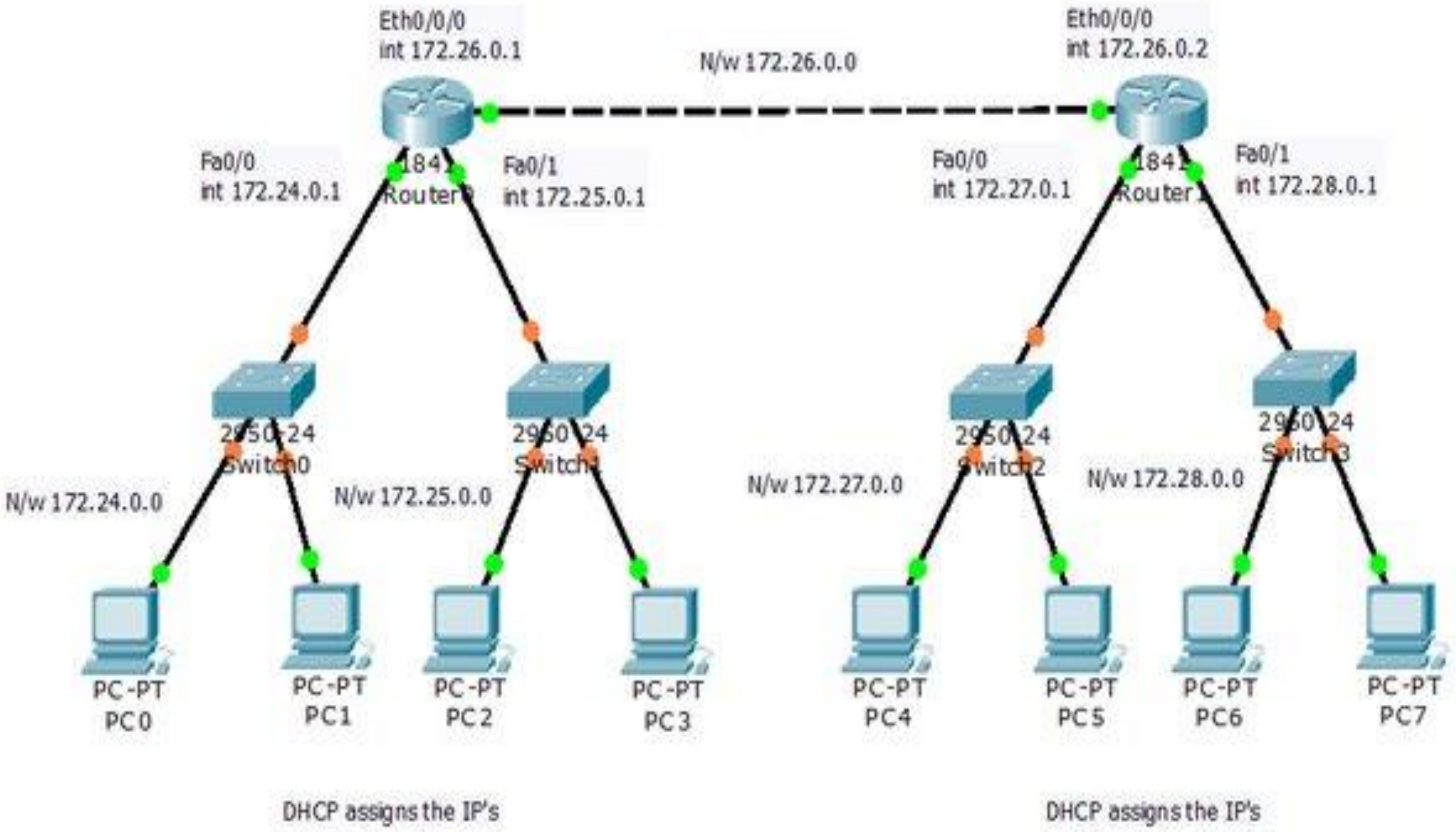


G Transmits to B, bridge **will** pass it to Segment A



Router

- Works at the Network Layer in an intelligent manner
- Can connect different network segments, if they are in the same building or even on the opposite side of the globe
- Works in LAN, MAN and WAN environments
- Allows access to resources by selecting the best path
- Can interconnect different networks – Ethernet with wireless
- Changes packet size and format to match the requirements of the destination network


Eth0/0/0
int 172.26.0.1
N/w 172.26.0.0
Eth0/0/0
int 172.26.0.2
Fa0/0
int 172.24.0.1
1841
Router0
Fa0/1
int 172.25.0.1
Fa0/0
int 172.27.0.1
1841
Router1
Fa0/1
int 172.28.0.1
2950-24
Switch0
2950-24
Switch1
2950-24
Switch2
2950-24
Switch3
N/w 172.24.0.0
N/w 172.25.0.0
N/w 172.27.0.0
N/w 172.28.0.0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
PC-PT
PC6
PC-PT
PC7
DHCP assigns the IP's
DHCP assigns the IP's

Router

- Two primary functions – to determine the ‘best path’ and to share details of routes with other routers
- Routing Table – a database which keeps track of the routes to networks and the associated costs
  - Static Routing – routes are manually configured by a network administrator
  - Dynamic Routing – adjust automatically to changes in network topology, and information it receives from other routers
- Routing Protocol – uses a special algorithm to route data across a network eg RIP

Router

Advantages

- Limits the collision domain,
- can function in LAN or WAN,
- connects differing media and architectures,
- can determine best path/route,
- can filter broadcasts

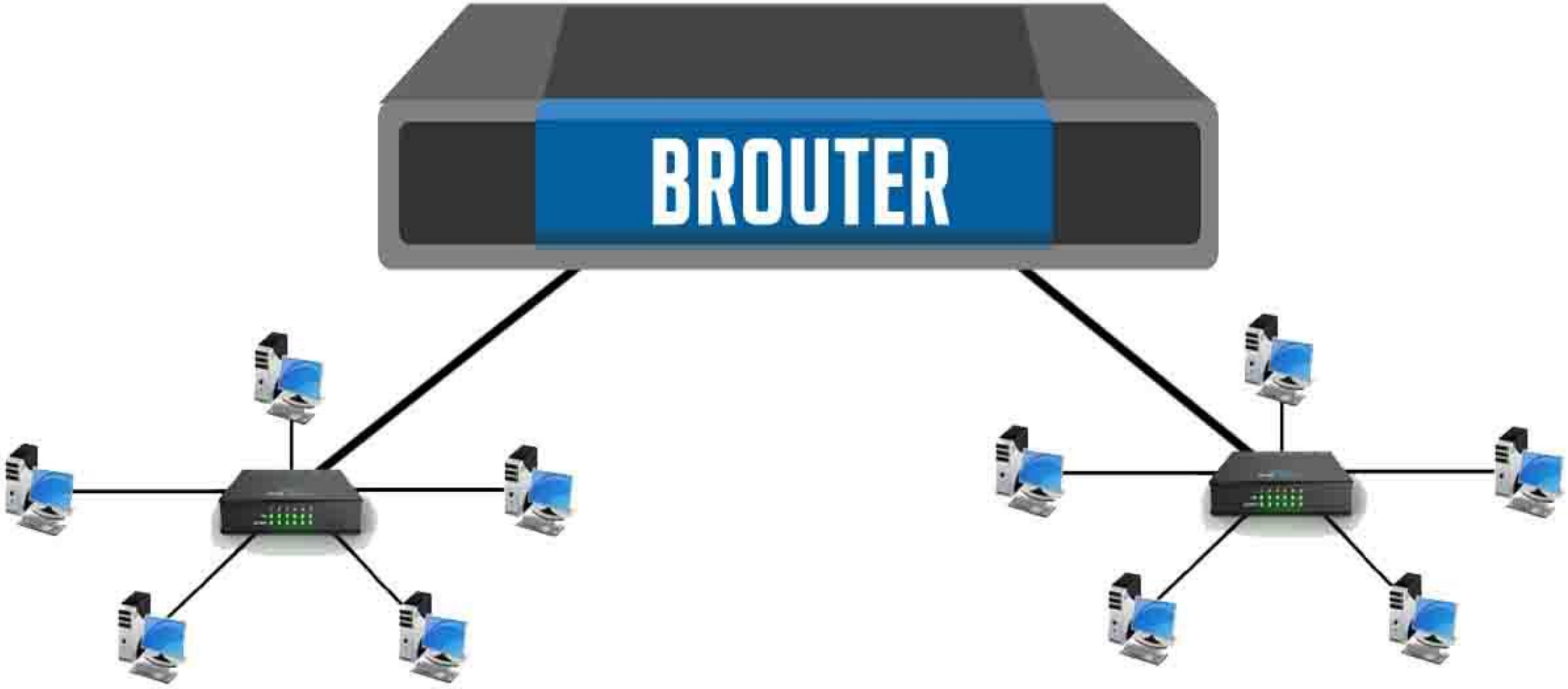
Disadvantages

- Expensive,
- must use routable protocols
- can be difficult to configure (static routing),
- slower than a bridge

Router

Brouter

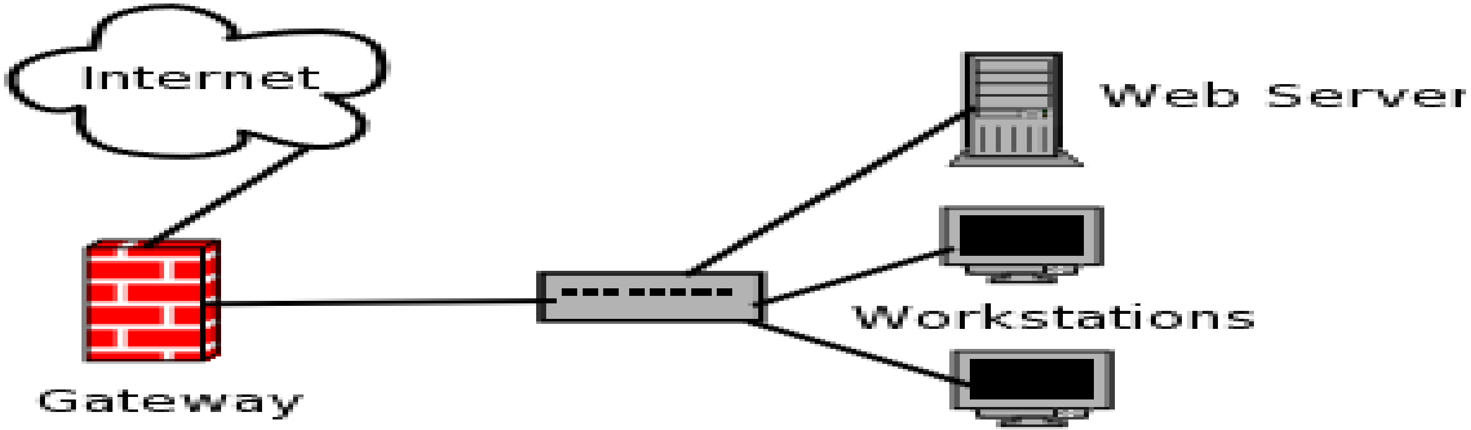
- Functions both as Bridge and a Router – hence name
- Can work on networks using different protocols
- Can be programmed only to pass data packets using a specific protocol, forward to a segment – in this case it is functioning in a similar manner to a Bridge
- If a Brouter is set to route data packets to the appropriate network with a routed protocol such as IP, it is functioning as a Router

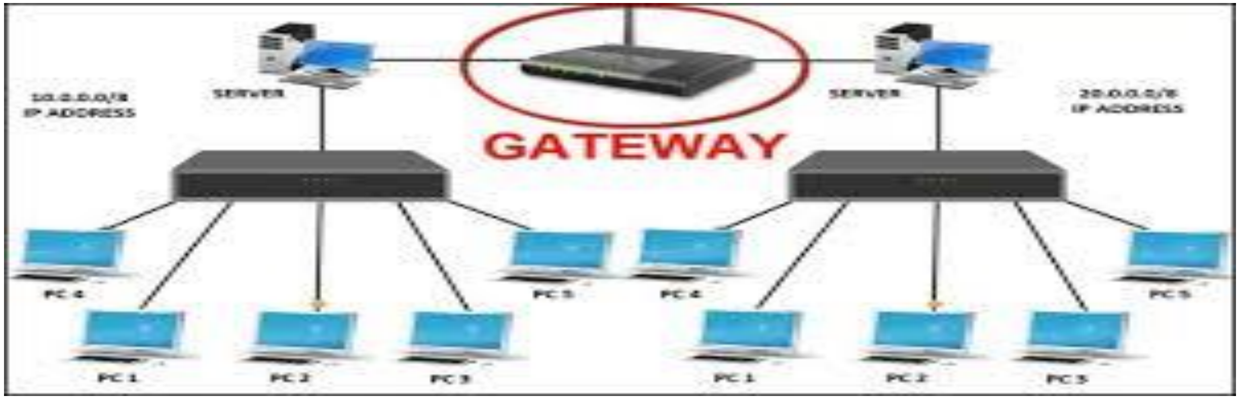

BROUTER

Gateways

- A gateway is a hardware device that acts as a "gate" between two networks.
- It may be a router, firewall, server, or other device that enables traffic to flow in and out of the network.
- Allow different networks to communicate by offering a translation service from one protocol stack to another
- They work at all levels of the OSI model – due to the type of translation service they are providing

Gateways


Internet
Web Server
Workstations
Gateway


10.0.0.0/8
IP ADDRESS
SERVER
GATEWAY
SERVER
20.0.0.0/8
IP ADDRESS
PC 4
PC 5
PC 4
PC 5
PC 1
PC 2
PC 3
PC 1
PC 2
PC 3

Gateways

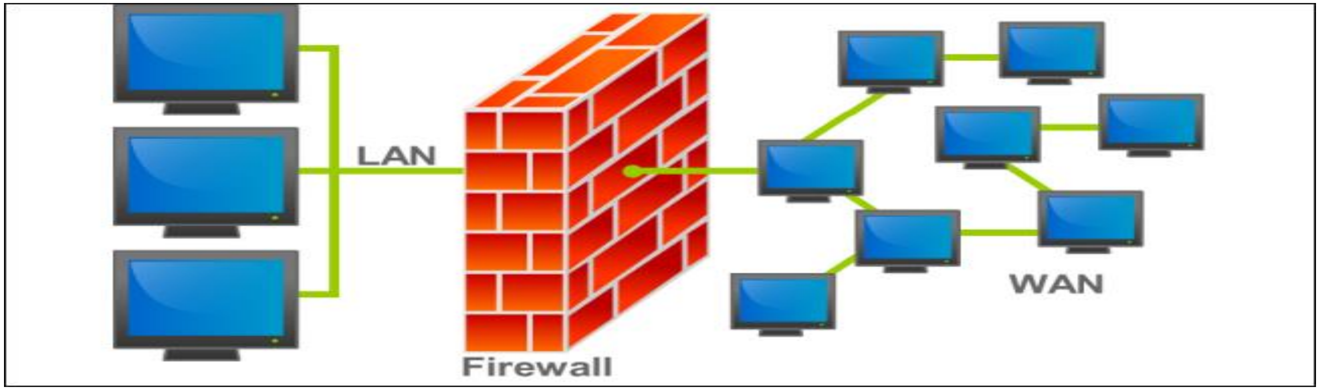
- Address Gateway – connects networks using the same protocol, but using different directory spaces such as Message Handling Service
- Protocol Gateway – connects network using different protocols. Translates source protocol so destination can understand it
- Application Gateway – translates between applications such as from an Internet email server to a messaging server

Firewall

- A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet.
- Firewalls can be implemented on both hardware and software.

Firewall

- Firewalls are commonly used to prevent unauthorized users from accessing private networks connected to internet.
- All message entering and leaving through intranet pass through the firewall.
- Firewall examines each message and blocks those that do not meet the specified security criteria



MODEM

- Modem stands for **Modulator** and **Demodulator .**
- A modem is used to send digital data over phone line.
- The sending modem modulates the data into analog signal compatible to phone line.
- The receiving modem demodulates the signal back into digital data.
- Wireless modems convert digital data into wave signals.

Ethernet Networks
LAN Technology

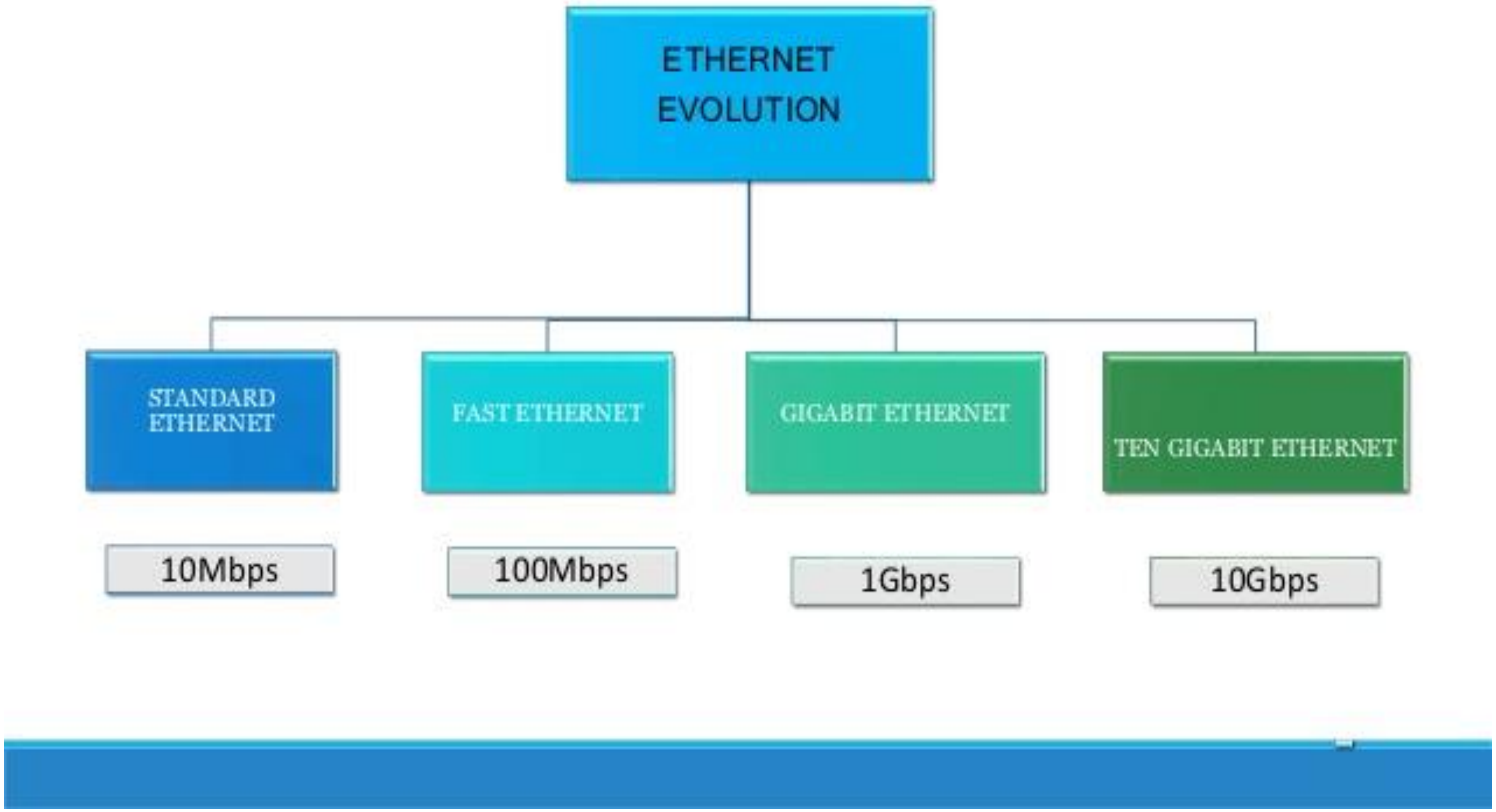
Ethernet Networks

- **Ethernet** is a family of computer networking technologies commonly used in **local area networks**, metropolitan area networks and wide area networks.
- The Institute of Electrical and Electronics Engineers (IEEE) specifies in the family of standards called IEEE 802.3.
- Ethernet operates in the lower two layers of the OSI model: the of the Data Link layer and the Physical layer.
- Ethernet describes how network devices can format and transmit data packets so other devices on the same local or campus area network segment can recognize, receive and process them.

Ethernet Networks

- An Ethernet cable is the physical, covered wiring over which the data travels.
- Compared to wireless LAN technology, Ethernet is typically less vulnerable to disruptions -- whether from radio wave interference, physical barriers or bandwidth hogs.
- It can also offer a greater degree of network security and control than wireless technology, as devices must connect using physical cabling
- Ethernet works at Layer 1 and Layer 2 of the OSI network protocol model

Ethernet Networks



ETHERNET EVOLUTION

STANDARD ETHERNET

FAST ETHERNET

GIGABIT ETHERNET

TEN GIGABIT ETHERNET

10Mbps

100Mbps

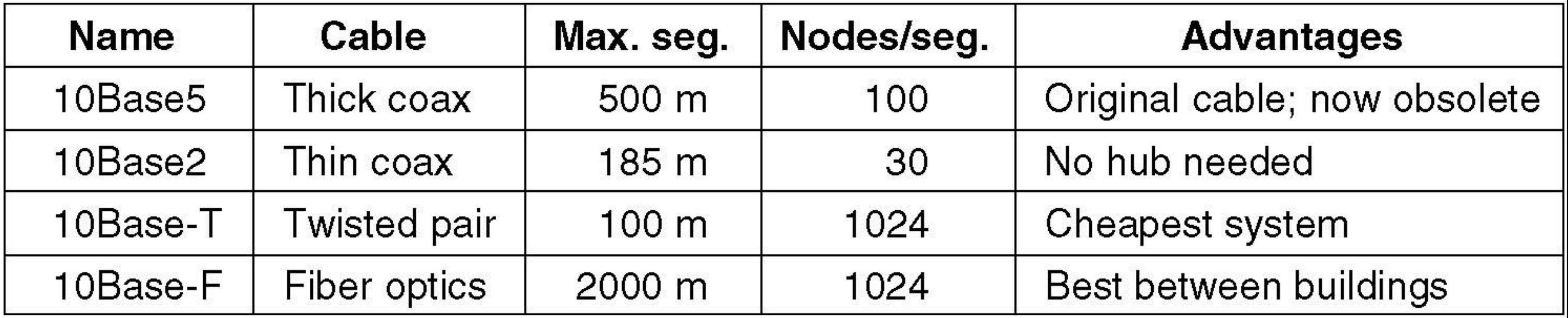
1Gbps

10Gbps

Ethernet Networks

- The first versions of Ethernet used coaxial cable to connect computers in a bus topology. Each computer was directly connected to the backbone. These early versions of Ethernet were known as Thicknet, (10BASE5) and Thinnet (10BASE2).
- 10BASE5, or Thicknet, used a thick coaxial that allowed for cabling distances of up to 500 meters before the signal required a repeater.
- 10BASE2, or Thinnet, used a thin coaxial cable that was smaller in diameter and more flexible than Thicknet and allowed for cabling distances of 185 meters.

four most common kinds of 10 Mbps Ethernet cabling



Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

- 10 - 10 Mbps
- Base - Baseband (against broadband with more bandwidth than standard telephone service)
- 5 (2) - maximum segment length; rounded to units of 100 meters (for coax)
- T - twisted pair, F - Fiber
- a hub is used in 10Base-T and 10Base-F to which each station is connected by a dedicated cable
- 10Base5 is also called Thick Ethernet and 10Base2 Thin Ethernet
- 10Base5 and 10Base2 use bus topology; 10Base-T and 10Base-F use star topology

Ethernet Networks

Standard Ethernet (10Base-T)

- An Ethernet standard that transmits at 10 Mbps over twisted wire pairs (telephone wire).
- 10Base-**T** is a shared media LAN when used with a hub (all nodes share the 10 Mbps)
- The physical topology was changed to a star topology using hubs.
- 10Base-T was the first vendor-independent standard implementation of Ethernet on twisted pair wiring.
- The “**10*BASE-T***“, **10** refers to 10 Mbps, **Base** refers to baseband signaling, **T** refers to twisted pair cable

Ethernet Networks

Fast Ethernet (100BASE-T)

- A significant development that enhanced LAN performance was the introduction of switches to replace hubs in Ethernet-based networks
- Fast Ethernet is a local area network (LAN) transmission standard that provides a data rate of 100 megabits per second (referred to as "100BASE-T").
- Workstations with existing 10 megabit per second (10BASE-T) Ethernet card can be connected to a Fast Ethernet network.
- IEEE 802.3u standard

Ethernet Networks

Gigabit Ethernet:

- The increasing use of Voice over IP (VoIP) and multimedia services requires connections that are faster than 100 Mbps Ethernet.
- Gigabit Ethernet is used to describe Ethernet implementations that provide bandwidth of 1000 Mbps (1 Gbps) or greater.
- Gigabit Ethernet is defined in the **IEEE 802.3ab** standard and is currently being used as the backbone in many enterprise networks

Ethernet Networks

10 Gigabit Ethernet:

- An **Ethernet** standard that transmits at **10** gigabits per second (**10** Gbps).
- Introduced in 2002 and abbreviated "**10** GbE," "10GE" or "**10G Ethernet**," it extended **Gigabit Ethernet** by **10**-fold for high-speed storage networks (SANs), enterprise backbones, as well as wide area and metropolitan area networks
- **IEEE 802.3ae** standard

Table 1.3: Common Ethernet Cable Types

Ethernet Name	Cable Type	Maximum Speed	Maximum Transmission Distance	Notes
10Base5	Coax	10Mbps	500 meters per segment	Also called Thicknet, this cable type uses vampire taps to connect devices to cable.
10Base2	Coax	10Mbps	185 meters per segment	Also called Thinnet, a very popular implementation of Ethernet over coax.
10BaseT	UTP	10Mbps	100 meters per segment	One of the most popular network cabling schemes.
100BaseT	UTP	100Mbps	100 meters per segment	One of the most popular network cabling schemes.
100BaseVG	UTP	100Mbps	213 meters (Cat 5); 100 meters (Cat 3)	
100BaseT4	UTP	100Mbps	100 meters per segment	Requires four pairs of Cat 3, 4, or 5 UTP cable.
100BaseTX	UTP, STP	100Mbps	100 meters per segment	Two pairs of Category 5 UTP or Type 1 STP.
10BaseF	Fiber	10Mbps	Varies (ranges from 500 meters to 2000 meters)	Ethernet over fiber-optic implementation.
100BaseFX	Fiber	100Mbps	2000 meters	100Mbps Ethernet over fiber-optic implementation.
1000BaseT	Copper	1000Mbps	100 meters	
1000BaseSX (Gigabit Ethernet)	Multimode Fiber	1000Mbps	260 meters	Uses SC fiber connectors.
1000BaseTX (Gigabit Ethernet)	Category 5 UTP	1000Mbps	100 meters	Uses same connectors as 10BaseT.
1000BaseLX	Multimode Fiber	1000Mbps	550 meters	Uses longer wavelength laser than 1000BaseSX.
FDDI	Multimode Fiber	100Mbps	10 kilometers	Uses MIC connector.

IEEE Standards

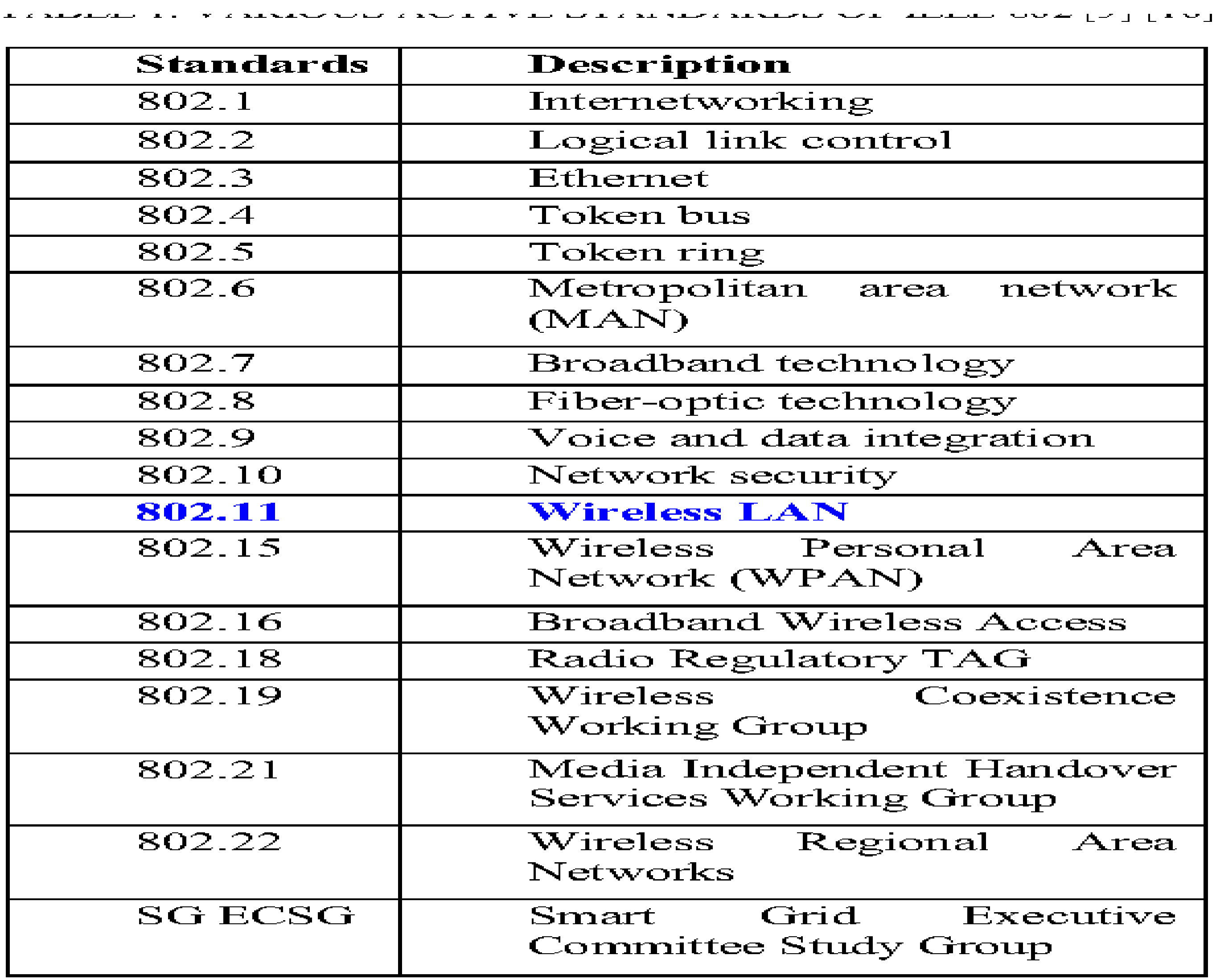


TABLE I: VARIOUS ACTIVE STANDARDS OF IEEE 802 [9] [10]

Standards	Description
802.1	Internetworking
802.2	Logical link control
802.3	Ethernet
802.4	Token bus
802.5	Token ring
802.6	Metropolitan area network (MAN)
802.7	Broadband technology
802.8	Fiber-optic technology
802.9	Voice and data integration
802.10	Network security
802.11	**Wireless LAN**
802.15	Wireless Personal Area Network (WPAN)
802.16	Broadband Wireless Access
802.18	Radio Regulatory TAG
802.19	Wireless Coexistence Working Group
802.21	Media Independent Handover Services Working Group
802.22	Wireless Regional Area Networks
SG ECSG	Smart Grid Executive Committee Study Group