Addis Ababa University

አዲስ፡አበባ፡ዩኒቨርሲቲ

Seek Wisdom, Elevate your Intellect and Serve Humanity

Data Communication and Computer Networks

INSY3071

Chapter 5

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 one to one 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.

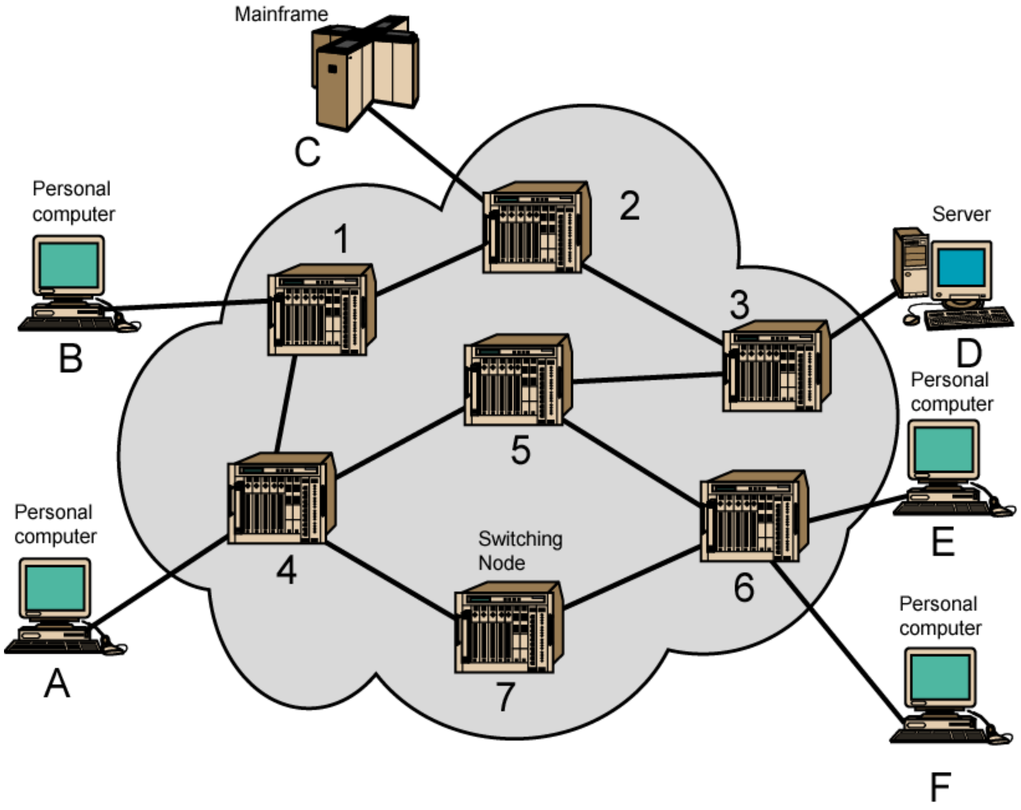
Switched Networks

- 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).
- A collection of nodes and connections forms a communications network.
- 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 Technology

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

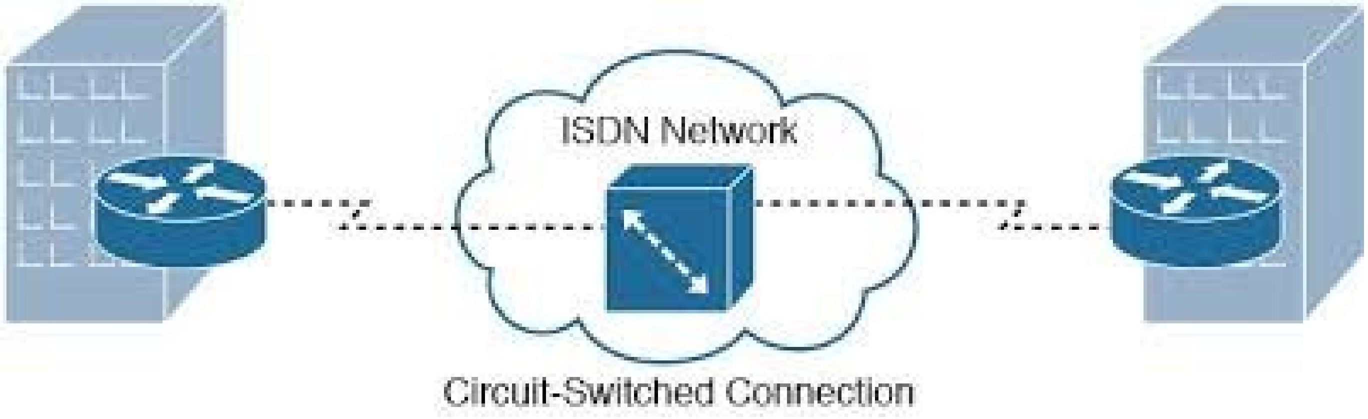
Circuit Switching Networks

- The two most common types of circuit switched networks
  - The Public Switched Telephone Network (PSTN)
  - 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

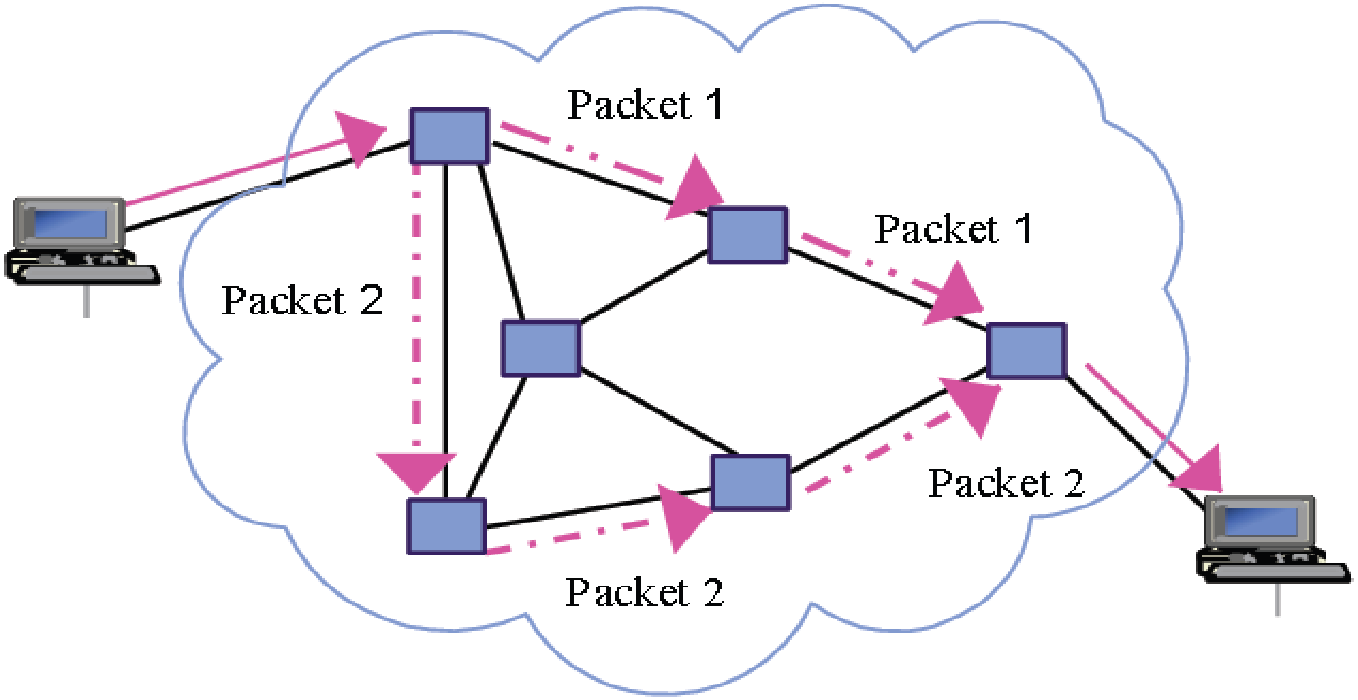
- Packet switching splits traffic data in to packets that are routed over a shared network
- Packet switched network do not require a circuit to be established
- The switches in packet switched network (PSN) determine the links that packets must be sent over based on the addressing information in each packet
- Packet switching is designed to address the problems of circuit switching.

Packet Switching

- Packet-switched networks move data in separate, small blocks (packets) based on the destination address in each packet.
- 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

- 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:

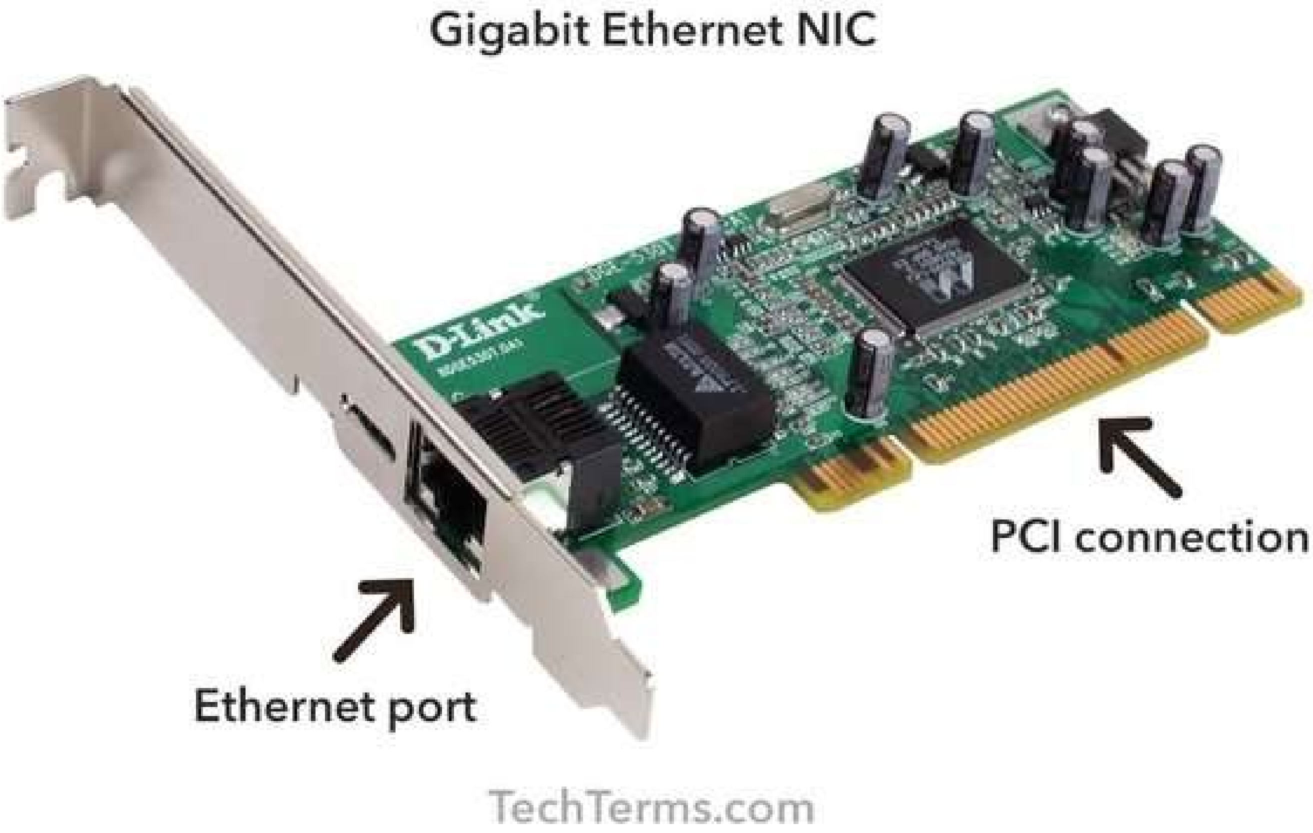
- Receives the data packet from the Network Layer
- Attaches its MAC address to the data packet
- Attaches the MAC address of the destination device to the data packet
- Converts data in to packets suitable for the particular network (Ethernet, Token Ring, FDDI)
- Converts packets in to electrical, light 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)
- In reality a 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)
- Similarly priced to Hubs – making them popular
- 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

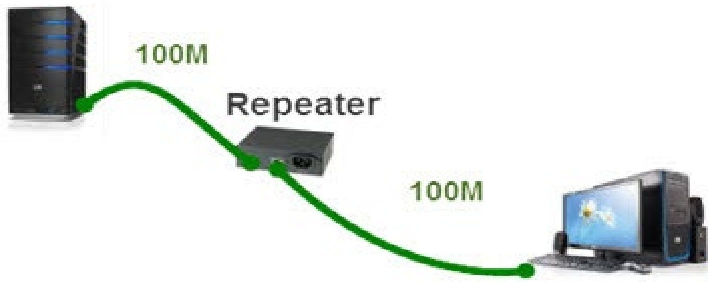
Repeater

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,
- limited number only can be used in network



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

Bridge

- Builds a Bridging Table, keeps track of devices on each segment
- Filters packets, does not forward them, by examining their MAC address
- 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

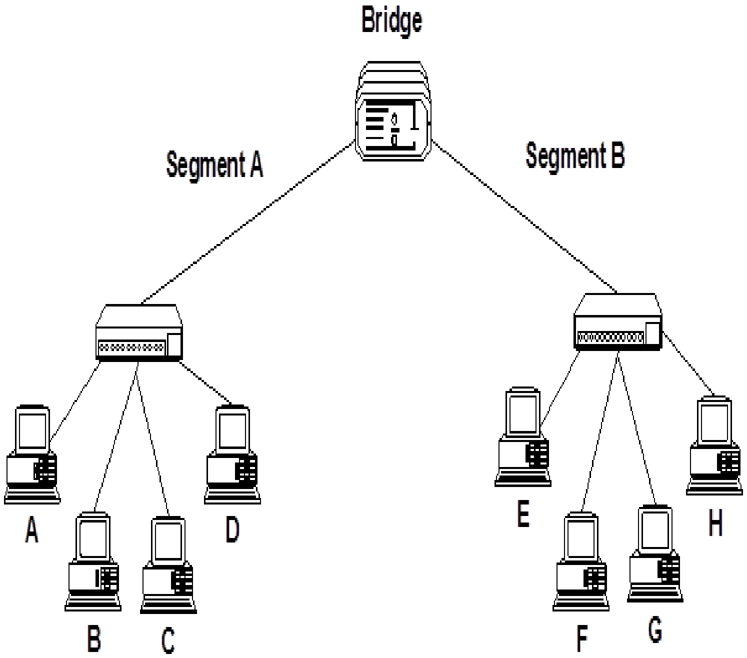
Disadvantages –

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

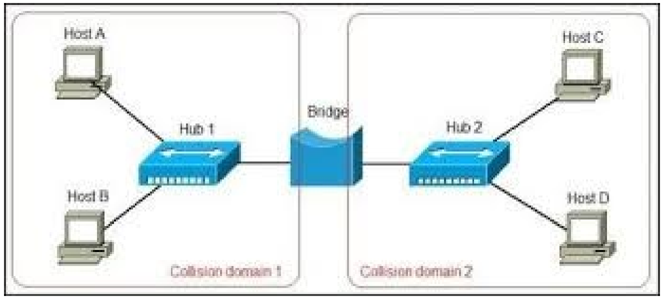
Bridge

- 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 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

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

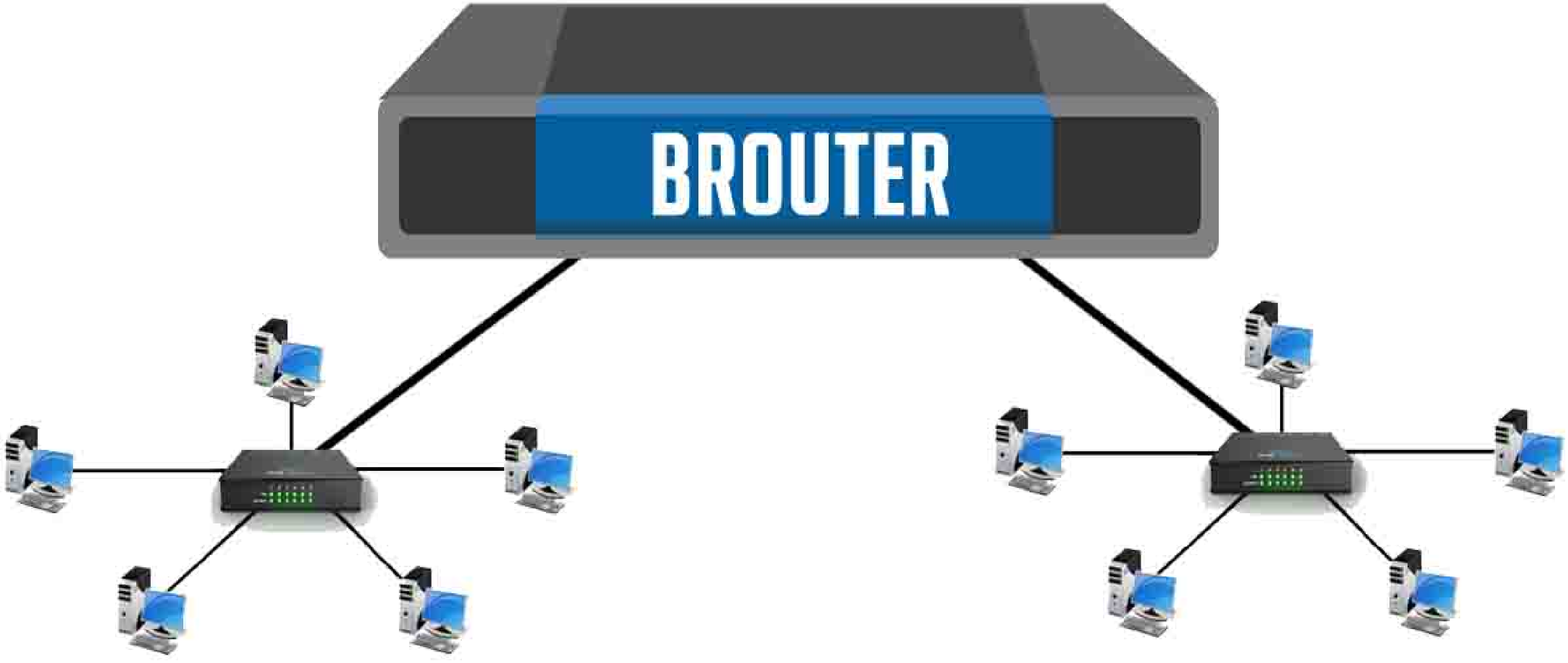
Disadvantages

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

Router

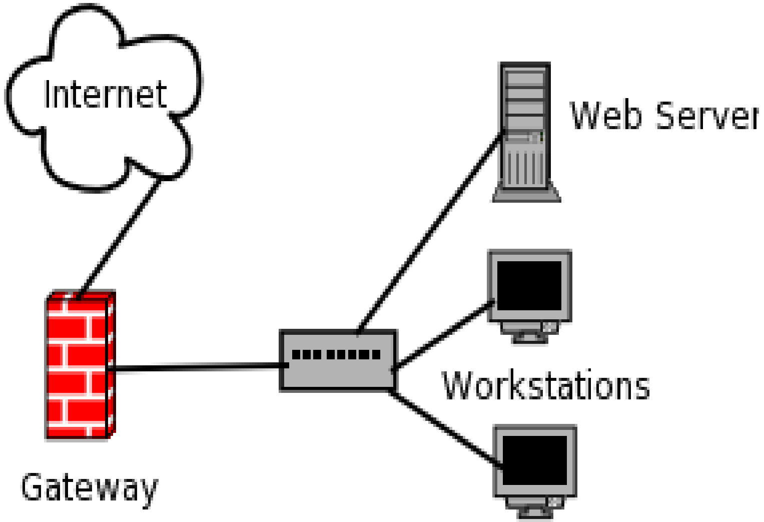
Brouter

- 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

- 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

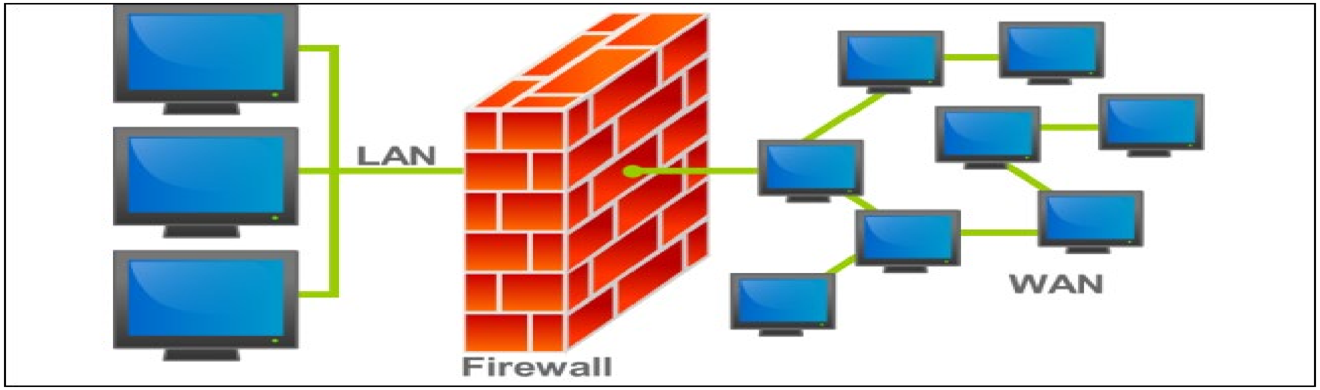
- Address Gateway – connects networks using the same protocol, but using different directory spaces such as Message Handling Service
- Protocol Gateway – connects network using different protocols. Translates source protocol so destination can understand it
- Application Gateway – translates between 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.

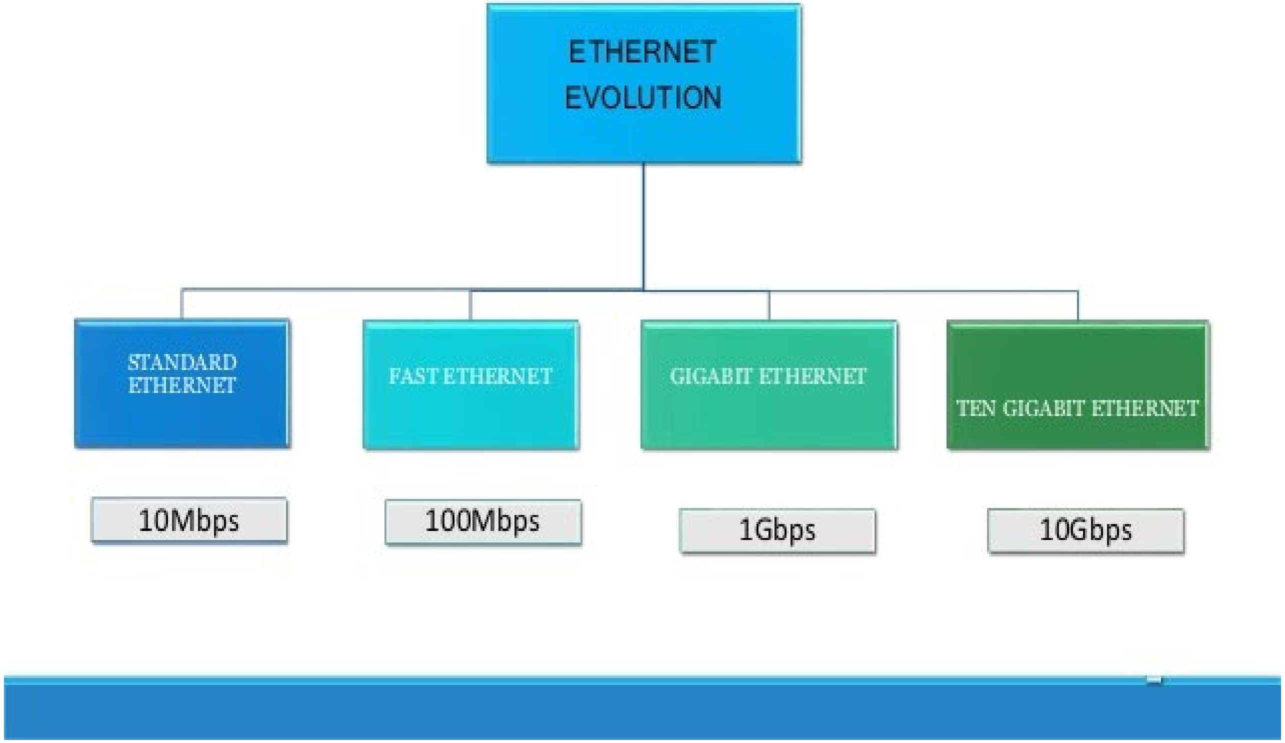
Ethernet Networks

- **Ethernet** is a family of computer networking technologies commonly used in local area networks, metropolitan area networks and wide area networks (WAN).
- The Institute of Electrical and Electronics Engineers (IEEE) specifies in the family of standards called IEEE 802.3.
- 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 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) and 10 Mbps between each pair of nodes when used with a switch.
- 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

Fats Ethernet (100BASE-T)

- 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 stnadard

Ethernet Networks

Gigabit Ethernet:

- a transmission technology based on the **Ethernet** frame format and protocol used in local area networks (LANs), provides a data rate of 1 billion bits per second (one **gigabit**).
- is defined in the **IEEE 802.3ab** standard and is currently being used as the backbone in many enterprise networks

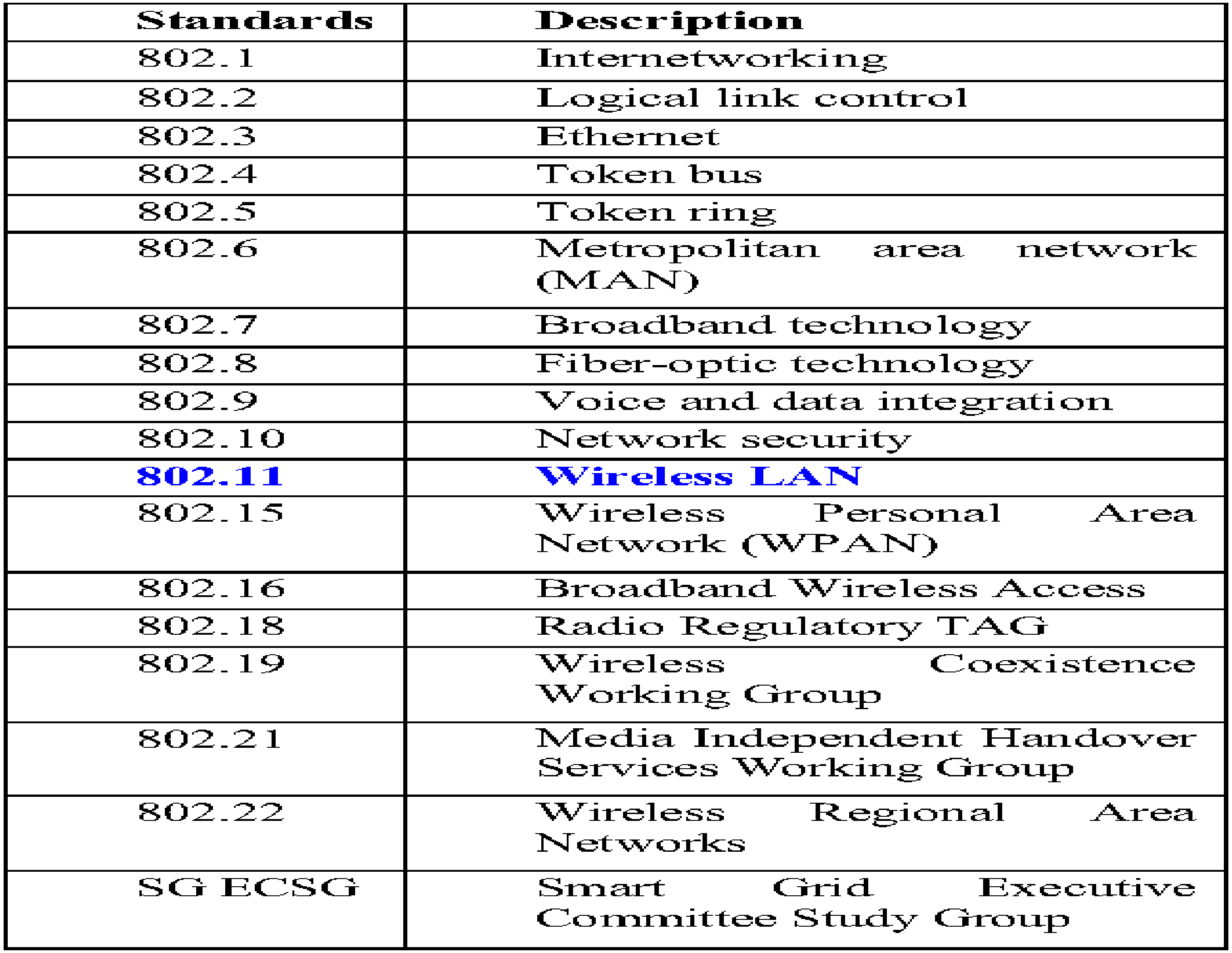
Ethernet Networks

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

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