09-01-2023

INDIAN INSTITUTE OF TECHNOLOGY ROORKEE

Introduction to Computer Science and Engineering

CSN-101

Computer Network

Prof. Partha Pratim Roy
Associate professor, CSE Department
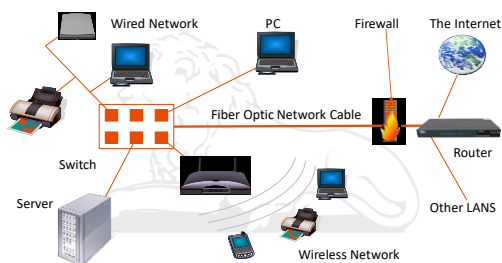Indian Institute of Technology Roorkee

---

Introduction: Computer Network

- A computer network is a group of computers/devices(Nodes) that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.
- The nodes of a computer network may include personal computers, servers, networking hardware, or other specialized or general-purpose hosts.
- The interconnections between nodes are formed from a broad spectrum of telecommunication network technologies, based on physically wired, optical, and wireless technologies.
- A communication protocol is a set of rules for exchanging information over a network.

IIT ROORKEE 2

Network Diagram

Wired Network — PC — Firewall — The Internet — Fiber Optic Network Cable — Router — Other LANS — Switch — Server — Wireless Network

IIT ROORKEE 3

Uses of Network

- **Simultaneous Access**
  - There are moments in any business when several workers may need to use the same data at the same time.
- **Shared Peripheral Devices**
- **Personal Communications**
  - Videoconferencing
  - Voice over Internet Protocol (VoIP):-VoIP transmits the sound of voice over a computer network using the Internet Protocol (IP) rather than sending the signal over traditional phone wires
- **Easier Data Backup**

IIT ROORKEE 4

Networking Devices(Nodes)

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

IIT ROORKEE 5

Network Interface Card

- NIC is used to physically connect host devices to the network media.
- A NIC is a printed circuit board that fits into the expansion slot of a bus on a computer motherboard.
- It can also be a peripheral device. NICs are sometimes called network adapters.
- Each NIC is identified by a unique code called a Media Access Control (MAC) address.
- This address is used to control data communication for the host on the network.

IIT ROORKEE 6

Repeaters

- A repeater is a network device used to regenerate a signal.
- Repeaters regenerate analog or digital signals that are distorted by transmission loss due to attenuation.
- A repeater does not make an intelligent decision concerning forwarding packets

Hubs

- Hubs concentrate on connections.
- In other words, they take a group of hosts and allow the network to see them as a single unit. This is done passively, without any other effect on the data transmission.
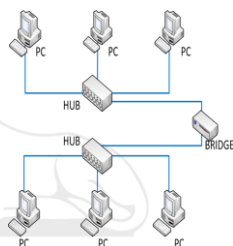- Active hubs concentrate hosts and also regenerate signals.

100BaseT Hub

10BaseT Hub

Bridges

- Bridges convert network data formats and perform basic data transmission management.
- Bridges provide connections between LANs.
- They also check data to determine if it should cross the bridge. This makes each part of the network more efficient

Switches

- Switches add more intelligence to data transfer management.
- They can determine if data should remain on a LAN and transfer data only to the connection that needs it.
- Another difference between a bridge and switch is that a switch does not convert data transmission formats
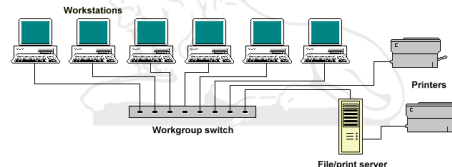
Routers

- Routers have all the capabilities listed above.
- Routers can regenerate signals, concentrate multiple connections, convert data transmission formats, and manage data transfers.
- They can also connect to a WAN, which allows them to connect LANs that are separated by great distances.

Gateway

- A gateway is a piece of networking hardware used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
- Gateways are distinct from routers or switches in that they communicate using more than one protocol to connect a bunch of networks
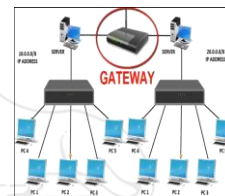
Firewall

- A firewall is a network device or software for controlling network security and access rules.
- Firewalls are inserted in connections between secure internal networks and potentially insecure external networks such as the Internet.
- Firewalls are typically configured to reject access requests from unrecognized sources while allowing actions from recognized ones.
- The vital role firewalls play in network security grows in parallel with the constant increase in cyber attacks.
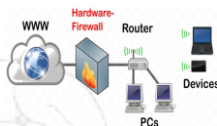

Network Media

- **The function of the media is to carry a flow of information through a LAN.**
- **Wired Media:-** A widely adopted family that uses copper and fiber media in local area network (LAN) technology are collectively known as Ethernet
  - **Copper Cable**
    - Coaxial Cables
    - Shielded Twisted Pair(STP)
    - Unshielded Twisted Pair
  - **Fiber Optic Cable**
- **Wireless Media:-** use the atmosphere, or space, as the medium.

Copper Cable

- The most common, easiest, quickest, and cheapest form of network media to install.
- The disadvantage of sending data over copper wire is that the further the signal travels, the weaker it becomes.
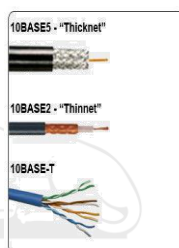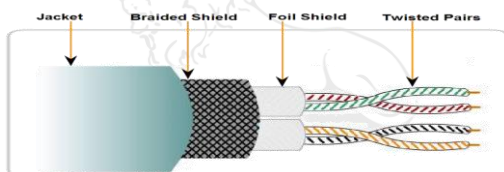

Coaxial Cable

- It can run longer distances than Twisted pair Cables.
  - Speed: 10-100Mbps
  - Cost: Inexpensive
  - Media and connector size: Medium
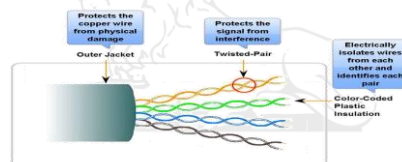 - Maximum cable length: 500m
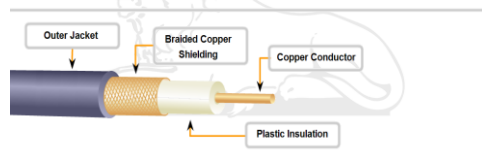
Shielded Twisted Pair(STP)

- Speed: 0-100Mbps
- Cost: Moderate
- Media and connector size: Medium to large
- Maximum cable length: 100m

Unshielded Twisted Pair

- UTP is a four-pair wire medium used in a variety of networks.
- Each of the eight copper wires in the UTP cable is covered by insulating material
- Speed: 10-100-1000 Mbps*

UTP Implementation

- EIA/TIA specifies an RJ-45 connector for UTP cable.
- The letters RJ stand for registered jack.

Fiber Optic Cable

- Glass fiber carrying light pulses, each pulse a bit.
- Based on the Total Internal Reflection of Light.
- High-speed point-to-point transmission 10-100's Gbps
- low error rate:
  - repeaters spaced far apart
  - immune to electromagnetic noise

Communication Protocols

- **Internet Protocol Suite**
  - Also called TCP/IP, is the foundation of all modern networking.
  - It defines the addressing, identification, and routing specifications for IPv4 and for IPv6.
  - It is the defining set of protocols for the Internet.
- **IEEE 802**
  - It is a family of IEEE standards dealing with local area networks and metropolitan area networks.
  - They operate mostly at levels 1 and 2 of the OSI model.
- **Ethernet**
  - It is a family of protocols used in wired LANs, described by a set of standards together called IEEE 802.3
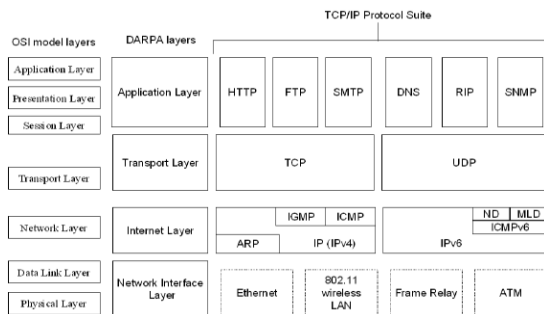
Communication Protocols

- **Wireless LAN**
  - It is standardized by IEEE 802.11 and shares many properties with wired Ethernet.
- **SONET/SDH**
  - Synchronous optical networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized multiplexing protocols that transfer multiple digital bit streams over optical Fibre using lasers.
- **Asynchronous Transfer Mode(ATM)**
  - It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells.
  - Good choice for a network that handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video.

TCP/IP Protocol Suite

OSI Layers

- The **Open System Interconnection Reference Model** (OSI Reference Model or **OSI Model**) is a description for layered communications and computer network protocol & transmission design.
- It divides data movement into seven layers which, from top to bottom, are the Application, Presentation, Session, Transport, Network, Data Link, and Physical Layers. It is therefore often referred to as the **OSI Seven Layer Model**.
- The concept of a 7 layer model was provided by the work of Charles Bachman, then of Honeywell.

OSI Layers

Layer	Function	#
Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1

II T ROORKEE
25

TCP/IP Protocol Suite

- The Internet Protocol Suite (commonly known as TCP/IP) is the set of communication protocols used for the Internet and other similar networks.
- The TCP/IP protocol suite was developed prior to the OSI model. Therefore, the layers in the TCP/IP protocol suite do not match exactly with those in the OSI model.
- The original TCP/IP protocol suite was defined as four software layers built upon the hardware.
- It is named from two of the most important protocols in it:
  - the Transmission Control Protocol (TCP) and
  - the Internet Protocol (IP), which were the first two networking protocols defined in this standard.

II T ROORKEE
26

TCP/IP Protocol

Layer	Protocol
Application	DNS, TFTP, TLS/SSL, FTP, Gopher, HTTP, IMAP, IRC, NNTP, POP3, SIP, SMTP, SMPP, SNMP, SSH, Telnet, Echo, RTP, PNRP, rlogin, ENRP
	Routing protocols like BGP and RIP which run over TCP/UDP, may also be considered part of the Internet Layer.
Transport	TCP, UDP, DCCP, SCTP, IL, RUDP, RSVP
Internet	IP (IPv4, IPv6), ICMP, IGMP, and ICMPv6
	OSPF for IPv4 was initially considered IP layer protocol since it runs per IP-subnet, but has been placed on the Link since RFC 2740.
Link	ARP, RARP, OSPF (IPv4/IPv6), IS-IS, NDP

II T ROORKEE
27

Types of Networks

1. **Personal Area Network (PAN)**
2. **Local Area Network (LAN)**
3. **Campus Area Network (CAN)**
4. **Metropolitan Area Network (MAN)**
5. **Wide Area Network (WAN)**
6. **Storage-Area Network (SAN)**
7. **Virtual Private Network (VPN)**
8. **Client Server Network**
9. **Peer to Peer Network (P2P)**

II T ROORKEE
28

Personal Area Network

- Personal Area Network (PAN) is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants.
- Also Known as HAN (Home Area Network)
- PANs can be used for communication amongst the personal devices themselves (interpersonal communication), or for connecting to a higher level network and the Internet (an uplink) where one "master" device takes up the role as internet router.

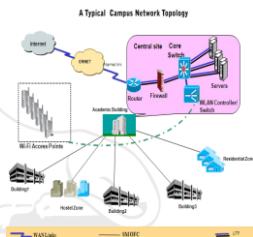II T ROORKEE
29

Local Area Network

- Xerox Corporation worked in collaboration with DEC and Intel to create Ethernet, which is the most pervasive LAN architecture used today.
- Ethernet has evolved and has seen significant improvements in regard to speed and efficiency.
- An upside of a LAN is fast data transfer with data speed that can reach up to 10Gbps.
- Other significant LAN technologies are Fiber Distributed Data Interface (FDDI) and token ring.

II T ROORKEE
30

Campus Area Network

- Larger than LANs, but smaller than metropolitan area networks these types of networks are typically seen in universities, large K-12 school districts or small businesses.
- They can be spread across several buildings that are fairly close to each other so users can share resources

Metropolitan Area Network

- A MAN is larger than a LAN but smaller than or equal in size to a WAN.
- The size range anywhere from 5 to 50km in diameter.
- MANs are typically owned and managed by a single entity.
- This could be an ISP or telecommunications company that sells its services to end-users in that metropolitan area.
- For all intents and purposes, a MAN has the same characteristics as a WAN with distance constraints.


Wide Area Network

- A Wide Area Network exist over a large area
- Data travels through telephone or cable lines
- Usually requires a Modem
- The world's largest Wide Area Network in the Internet


Storage Area Network

- SAN may be referred to as a Sub network or special purpose network.
- Its special purpose is to allow users on a larger network to connect various data storage devices with clusters of data servers.
- SANs can be accessed in the same fashion as a drive attached to a server.
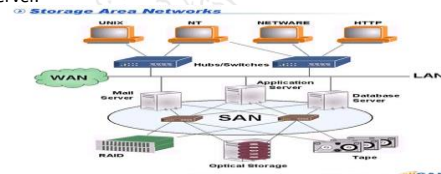

Virtual Private Network

- VPN is a private network that can access public networks remotely. VPN uses encryption and security protocols to retain privacy while it accesses outside resources.
- When employed on a network, VPN enables an end user to create a virtual tunnel to a remote location. Typically, telecommuters use VPN to log in to their company networks from home.
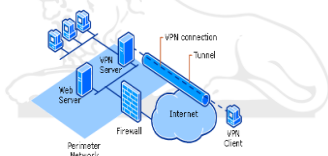
Client/Server Network

- In a client/server arrangement, network services are located on a dedicated computer called a server.
- The server responds to the requests of clients.
- The server is a central computer that is continuously available to respond to requests from clients for file, print, application, and other services.
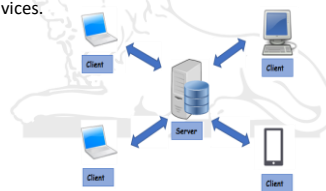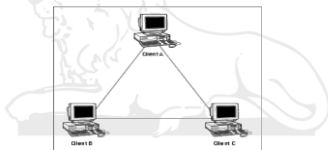

6

Peer to Peer Network

- Usually very small networks
- Each workstation has equivalent capabilities and responsibilities
- Does not require a switch or a hub.
- These types of networks do not perform well under heavy data loads.

Network Topologies

- Network topology defines the structure of the network.
- **Physical topology:-** It define the actual layout of the wire or media.
  - Bus
  - Ring
  - Star
  - Tree(Hierarchical)
  - Mesh
- **Logical topology:-** It defines how the hosts access the media to send data.
  - Broadcast
  - Token passing
- **Hybrid Topology**

Bus Topology

- All devices are connected to a central cable, called bus or backbone.
- There are terminators at each end of the bus that stops the signal and keeps it from traveling backwards.
- There is no central controller.
- Backbone cable can be laid along the most efficient path, and then connected to the nodes by drop lines of various lengths
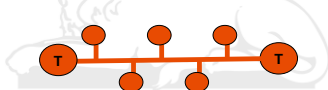
Ring Topology

- All devices are connected to one another in the shape of a closed loop.
- Each device is connected directly to two other devices, one on either side of it.
- **Advantages**:
- Avoids the collisions that are possible in the bus topology.
- Each pair of stations has a point-to-point connection.
- A signal is passed along the ring in one direction, from device to another, until it reaches its destination.
- Each device incorporates a repeater.
- Relatively easy to install and reconfigure.
- Fault isolation is simplified.
- **Disadvantages**:
- A break in the ring (such as station disabled) can disable the entire network.
- Unidirectional traffic.
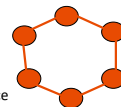
Star Topology

- All devices are connected to a central hub.
- Nodes communicate across the network by passing data through the hub or switch.
- **Advantages:**
- 1. Easy to install and reconfigure.
- 2. Robustness, if one link fails; only that link is affected. All other links remain active.
- 3. Easy fault identification and isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.
- **Disadvantages:**
- 1. The devices are not linked to each other.
- 2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.

Tree/Hierarchical Topology

- **Advantages:**
1. It allows more devices to be attached to a single central hub and can therefore increase the distance a signal can travel between devices.
2. It allows the network to isolate and prioritize communications from different computers.

- **Disadvantages:**
1. The devices are not linked to each other.
2. If one device wants to send data to another, it sends it to the controller, which then relays the data to the other connected device.
3. The addition of secondary hubs brings two further advantages.
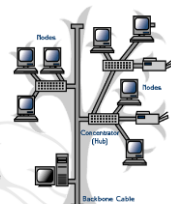
Mesh Topology

- Each host has its connections to all other hosts.
- Mesh topology is implemented to provide as much protection as possible from interruption of service.
1. A nuclear power plant might use a mesh topology in the networked control systems.
2. Although the Internet has multiple paths to any one location, it does not adopt the full mesh topology.
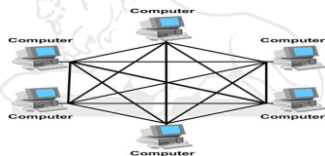
Wireless Networks

- Wireless network is a type of computer network that uses wireless data connections for connecting network nodes.
- Example
  – Bluetooth
  – Wi-Fi

Bluetooth

- Bluetooth is a short-range wireless technology standard used for exchanging data between fixed and mobile devices over short distances.
- It is using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz.
- The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard.

Wi-Fi

- Wi-Fi Stands for Wireless Fidelity.
- Wi-Fi, is a Local Area Wireless technology.
- Wi-Fi networks use radio technologies to transmit and receive data at high speed.
- It is based on the IEEE 802.11 family of standards.
- Access point: The access point is a wireless LAN transceiver or " base station" that can connect one or many wireless devices simultaneously to the internet
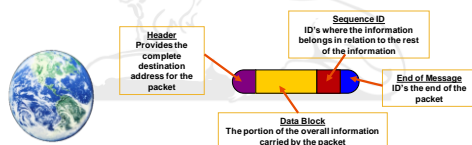
The Internet

- ***The simplest definition of the Internet is that it's a network of computer networks***
- A page on the Internet—whether it's full of words, images or both—doesn't come to you in one shipment. It's translated into digital information, chopped into 1500 byte pieces called PACKETS, and sent to you like a puzzle that needs to be reassembled. Each part of the packet has a specific function:
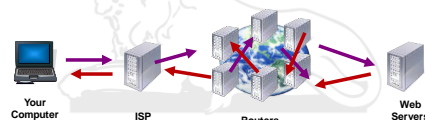

The Internet

- ***How Information Travel Through the Internet:***
- When you connect to a Web site through an ISP and start exchanging information, there isn't a fixed connection between your computer and the Web server computer hosting the Web site. Instead, information is exchanged using the best possible path at that particular time. Special computers called routers determine these paths, avoiding slow links and favoring fast ones.

Thanks...