Study Material By Manikrao Dhore
Sub: Computer Networks
Section I: Unit-I CN Fundamentals

Major Goal of The Subject: To empower the students to understand the engineering process for enabling efficient, robust and scalable communication through computer networks

Course Outcome:
CO1: Select line encoding, modulation, topology, essential components of physical layer, data transmission rates to design computer networks.

Section I: Unit-I Data Communication Networking Fundamentals and Physical Layer:
[CO1 → PO1, PO2, PO5 – CO Strength - 3,2,2]

Communication Model: Source, Transmitter, Transmission System, Receiver, Destination, Data Terminal Equipment (DTE), Data Communication Equipment (DCE). **Transmission Configurations:** Point to Point and Multipoint. **Transmission Modes:** Synchronous and Asynchronous. **Transmission Methods**: Serial and Parallel. Communication. **Communication Modes:** Simplex, Half Duplex, and Full Duplex. **Line Coding:** Unipolar NRZ, Polar NRZ, NRZ Inverted, Bipolar Encoding, Manchester Encoding, Differential Manchester Encoding. **Modulation:** Analog Modulation: Amplitude, Frequency, Phase. Pulse Modulation Techniques: PCM, PAM, PWM, PPM. **Digital Modulation:** ASK, FSK, MSK, GMSK, PSK, BPSK, PSK, QAM, CPM, OFDM and multicarrier modulations.**[3 Hrs]**

Networking Fundamentals: **Types of Computer Networks:** LAN, MAN, WAN, PAN, Internet, internet and Intranet. **Network Architectures:** Client-Server; Peer To Peer. **Network Architecture Modes:** Infrastructure and Ad-hoc mode. **Network Topologies:** Mesh, Star and Hierarchical. **Reference Models:** OSI, TCP/IP. Design Issues for Layers. Is ATM still used? Is ISDN dying? Is Frame Relay outdated? Is SNA still present in the Market? **[3 Hrs]**

Physical Layer: **Transmission Mediums:** Air, Water, Vacuum, Coaxial, Cat5, Cat5e, Cat6, Cat6a, Cat7, Cat8, OFC - Single and Multicore. **Networking Devices Wired and Wireless:** NIC, Repeater, Bridge, Switch, Modem, Router, Gateways and Access Point. **[2 Hrs]**

Course Outcome 1: Select Network Architecture, Topology and Essential Components To Design Computer Networks.

Why to Study Computer Networks?

Can we live without:
Personal Perspective: Email , Web Browsing, Social Networks, Whatsapp, Instagram, Share it, video-conferencing , Video-on-demand, Online banking/shopping, Online gaming

Business Perspective: Make data, programs and equipment available irrespective of physical Location, Employee records, inventory, financial statements, Custom software, Security software, Share printers, scanners, E-commerce based companies :Amazon, EBay, Flipkart etc, Resource Sharing, Low Cost, Reliability, Centralized management, Scalability, Access to Remote Information.

History of Telecommunication

Prehistoric : Smoke signals/Fire (Visual), Drums (Sound) Message can be conveyed 100 miles in an hour (through relays).

Before Common Era (BCE): Mail, Pigeons, Hydraulic Semaphore

1790	Semaphore Lines (Optical telegraph)	1983	Domain Name System (DNS)
1800	Heliograph (Solar telegraph)	1986	Internet Engineering Task Force
1830	Electric telegraph	1988	OSI Reference Model released
1870	Telephone	1989	– Routing Protocols: BGP, RIP
1890	Radio	1990	Commercialization of Internet (ISPs)
1920	Television	1991	World Wide Web (WWW)
1960	Satellite	1995	Instant Messaging, P2P, e-commerce (eBay, Amazon)
1960	Fiber Optics–Packet switching	1998	Google Search
1969	Four nodes (UCLA, Stanford, UCSB and Univ. of Utah) n/w 50kbps links	1999	WiFi (wireless)
1969	–ARPANET (Advanced Research Projects Agency)	2003	Skype
1972	ARPANET connected 15 nodes, Email was introduced, Different networks emerged -–ALOHANet (microwave), –DARPA Satellite–BBN Commercial	2004	Facebook
1974	TCP/IP	2005	:YouTube
1976	Ethernet by Metcalfe (Internet)	2006	Twitter
1977	OSI Model Prepration	2008	Cloud based services (E.g. Dropbox)
1981	213 hosts on ARPANET	2010	Instagram (Photosharing)
1982	TCP/IP formalized	2011	Google+
1982	SMTP (Email)		
1983	OSI Adopted		

What is Computer Network – Definition?

Interconnecting number of autonomous computers with one another over a shared communication medium for sharing information and resources.

Local Area Network (LAN) :

LAN is privately owned networks use to interconnects computers within a single building or campus up to few kilometers in size. For the LAN diameters spans over 550 meters to 2.5 Kilometers. Nowadays organizations have Campus Wide Network which is an extension of LAN using OFC at backbone and diameter up to 10 Kilometers. LANs are setup using IEEE802.3 standard. (**Active**).

VIT Network:

Network Name: Intranet
Standard: IEEE802.3u
Transmission Media: Guided Media: OFC OC-48 at backbone and Cat 5e and Cat 6 for extensions
Cabling Standard: TIA/EIA-568C.2
Signaling: Baseband (Digital)
Frequency: 100 MHz, 250MHz, 350MHz for Cat 5e
Data Encoding: 4B/5B and Differential Manchester
Modulation: PAM5
Protocol: CSMA/CD 1-Persistent within segments
Technology: Fast Ethernet (Ethernet-I at Physical Layer and Ethernet II at MAC Layer)
Data Transfer Rate (Bandwidth): 100 Mbps
Topology: Star Topology using Switched Ethernet with Point to Point Links
Backbone: OFC OC-48
Protocol Stack: TCP/IP
Network Architecture: Client-Server
Transmission Mode: Full Duplex
Collision Domain: Legacy Support
Transmission Technology: Dynamic Broadcast for Backbone and PTP for all non-stackable output ports

Metropolitan Area Network (MAN) :

MAN is a **network** that interconnects computers in an entire city. MAN is formed by interconnecting multiple LANs in a city. MAN : 10 km to 25 km City. Uses IEEE 802.6 Standard (**Disbanded**) . Does not contain switching elements. Uses DQDB (Distributed Queue Dual Bus)

Wide Area Network (WAN) :

WAN is a telecommunication or computer network span over the area often country or continent. WAN: 100km to 1000 km Country and Continent. Uses Packet Switching and Data Switching Exchanges. Uses IEEE 802.1 standard.

Personal Area Network (PAN) :

PAN is the interconnection of mobile devices within the range of an individual person. typically within a range of 10 meters. PAN : 10 meters. Uses IEEE 802.15 standard (**Active**).

IEEE 802 standards covers only LAN, MAN, WAN, SAN, ISDN and Wireless

802.1Internetworking 802.2 :LLC 802.3 :Ethernet 802.4 :Token Bus 802.5 :Token Ring 802.6 :MAN 802.7 :Broadband 802.8 :Fiber Optics 802.9 :ISDN	802.10 : Network Security 802.11 : WLAN, Wi-FI 802.12 : 100VG - Any LAN 802.13 : 802.14 : Cable Modem 802.15.2 : Bluetooth 802.15.4 : WSN, ZigBee 802.16 : Wi-MAX, WMAN 802.17 : Resilient packet ring	802.18 :Radio Regulatory TAG 802.19 :Coexistance TAG 802.20 : Mobile Broadband 802.21 : Media Independent Handoff 802.22 : Wireless Regional Area Networks 802.25 : Omni-Range Area Network

Internet

The Internet is the global system of interconnected computer networks that use the Internet protocol suite (TCP/IP) to link devices worldwide. Internet is WAN hence covers Country, Continent or entire planet. Uses Packet Switching and networks are connected by routers.

Internetwork:

Connecting homogeneous or heterogeneous LAN and MAN to extend network reach. Uses IEEE 802 standards. It covers LAN/MAN architecture, internetworking among 802 LANs, MANs and wide area networks, 802 Link Security and 802 overall network management

Network Architectures:

Client – Server:

Server: Powerful (High End) machine consisting databases, applications, Internet Protocol servers (Blade Server) at central place. **Client:** Employee having low end machine to access the information.

Peer to Peer Network:

A network of computers configured to allow certain files and folders to be shared with everyone or with selected users. Peer-to-peer networks are quite common in small offices that do not use a dedicated file server.

Distributed Network (DN):

Distributed network is a distributed computing network system in which computer programming functionality and the data to be worked on are spread out across more than one computer. Usually, this is implemented over a computer network.

Software Defined Networking (SDN): Software-defined networking (SDN) technology is an approach to computer networking that allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via open interfaces and abstraction of lower-level functionality.

Infrastructure network:

Infrastructure mode supports central connection points for clients. An Infrastructure mode network requires the use of an Access Point. The Access Point controls Wireless communication and offers several important advantages over an Ad-hoc network. For example, a Infrastructure based network supports increased levels of security, potentially faster data transmission speeds and integration with a wired network.

Ad-hoc network:

An Ad-hoc network allows each device to communicate directly with each other. There is no central Access Point controlling device communication. Ad-hoc networks are only able to communicate with other Ad-hoc devices, they are not able to communicate with any Infrastructure devices or any other devices connected to a wired network. In addition, Ad-hoc mode security is less sophisticated compared to an Infrastructure mode.

What defines the OSI model ?

- How n/w devices contact each other?
- Methods by which device knows when to transmit data and when not to
- Methods to ensure that n/w transmission is received correctly and by the right recipient
- How to ensure that network devices maintain a proper DTR of data flow ?
- How bits are represented on the n/w media?
- How to sequence the layers with Connection / Connectionless?
- How to organize network functions into seven layers?
- How to organize peer to peer mode?

OSI Model (Open System Interconnection)

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data Link
1. Physical

Application Layer

- Provides network services to application processes with the help of tools and utilities such as browsers, E- mail, file transfer, terminal emulation.
- Interface to TDI or Third Party

- Gateways for different network file formats

Presentation Layer

- Data representation
- Format of text, images, audio, video and Unicode
- Data structures
- Ensure data is readable by receiving system
- Negotiates data transfer syntax for application layer
- Resolves differences between format

Session Layer

- Inter-host communication
- Establishes, manages and terminates sessions between applications
- Controlling dialogues between applications in the end systems
- Dialogue discipline, Grouping and Recovery
    - Logging Process
    - Remote Terminal Access in half duplex
    - Transaction Processing checkpoints, backups
    - Token management in half duplex mode

Transport Layer

- End-to-end connection reliability
- Concerned with data transports issues between hosts
- Data transport reliability
- Establishes, maintains, and terminates virtual circuits. / multiple network connections
- Fault detection and recovery / Error Control
- Flow control management
- Error free delivery of data
- Fragmentation and reassembly (into packets as per network layer specification)
- Decision about service type

Network Layer

- Addresses Resolution
- Controlling Subnet
- Providing best path
- Accounting
- Large Packet Mgt.
- Provides connectivity and path selection between two end systems
- Domain of routing / Route decision and selection
- Congestion Control Mgt.
- Heterogeneous n/w problem mgt
- Determines Quality of Service

Data Link Layer

- Access to media
- Provides reliable transfer of data across media.
- Physical addressing, network topology, error notification, flow control.
- Framing : Break packets into frames according to the specifications of physical layer standard I.e encapsulation and de-capsulation of data
- Error Control and Recovery for physical Channel
- Link Management
- Collision Avoidance and collision content resolution

Physical Layer

- Binary transmission, Wires / Cables, Connectors, Voltages, Modulations, Demodulations, Line encoding, Data rates, Initial Connection, Turn down connection, Pin assignments, Concentrators / Hubs/ Repeaters, Wiring Schemes

Needs of DOD

- Ability to connect multiple networks ie homogeneous as well as heterogeneous (Internetworking)
- Network must be able to survive the loss of subnet hardware
- Multiple transmission lines
- Connectionless services
- Real Time Speech Transmission

TCP / IP Model

4. Application Layer
3. Host to Host Layer
2. Internet Layer
1. Network Access Layer

OSI	TCP/IP
ISO in 1977 and adopted in 1983	DoD in 1974 by Vint Cerf & Robert Kahn
Developed by dedicated team	Developed by open process
Copyrighted and carry a purchase fees	Free
Proprietary	Non-proprietary
Intended to be a Inter-National standard	Never indented to be
Designed with layers	Not designed with layers
Devised first and protocols invented latter	Protocol came first and then model
Seven Layers	Four Layers
T-Layer is connection oriented	Both- less and oriented
N/w –Layer is both	N/w layer is connection less
Gives interface, service and protocols	No clear distinction
Generalized	Not Generalized
Strongly describes protocol stack	Poorly describes protocol stack
Separate Layers	Can view in layers
Not Popular	Very Popular

Design Issues for Layers:

- Mechanism for identifying sender and receiver : Addressing
- Rules for Data Transfer: Unidirectional (Simplex), Bi-directional (Half and Full Duplex)
- Methods for Error Control : Error Detection and Error Correction
- Queuing mechanism for Fast Sender and Slow Receiver
- Methods to process arbitrarily long messages
- Algorithms for Route decisions
- Multiplexing and demultiplexing for multiple connections: Centralized , Decentralized and Dynamic
- Logical decompositions of complex network

- Standard interfaces between n/w layers
- Symmetry in functions
- Standard communication network language

Transmission Mediums: CAT5, 5e, 6, 6a, 7, OFC and Radio Spectrum

There are two types of copper cable used in LANs:

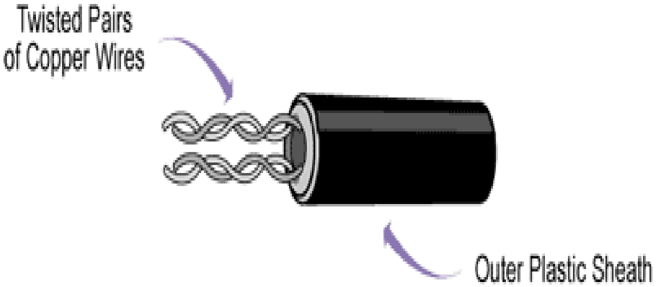
- Twisted pair cable is the most widely used medium.
- Coaxial cable is found in older installations.

Twisted Pair Cable

- Twisted pair cable consists of two or more pairs of thin, stranded, insulated copper wires .
- Twisted around each other used to cancel EMI/RFI.
- Twisted pair cable is available in two standard varieties:
- Unshielded twisted pair (UTP) and Shielded twisted pair (STP).
- Recently, a new type of twisted pair cable has been offered by some manufacturers: screened twisted pair (ScTP).

UTP Cable

- Wire pair acts as a signal communication link
- Diameter : 0.4 to 0.9 mm or 0.016 to 0.36 inch
- Data Rate : 64 Kbps to 10 Gbps
- Frequency Range : 0 to 350 MHz
- Repeater Spacing : 100 m to 2 Km (10 Km in analog)
- Susceptible to interference and noise (Cross Talk)



- Uses : Telephone local loops, PBX and LAN
- Can Transmit analog as well as digital
- Cheaper than coaxial

- Light in weight , flexible, and easy to install.
- It relies on precisely twisted pairs of wire to minimize EMI/RFI, and is not shielded by an external conductor.
- The number of twists decides EMI/RFI noise minimization factor
- UTP looks similar in appearance to standard telephone cable, but it meet higher criteria to perform as data-grade cable.

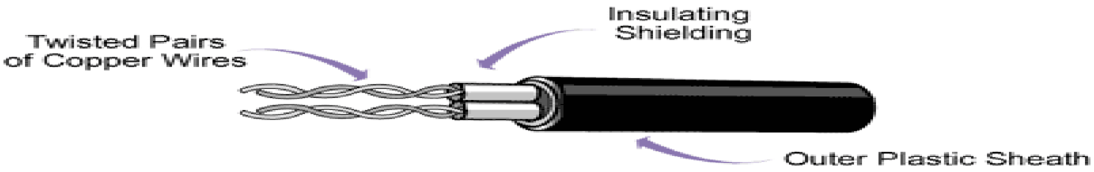
Standards for Rating UTP Cable

- **Category 1 (CAT-1)** --For analog and digital voice (telephone) and low-speed data applications (Being used nowadays for telephone network only)
- **Category 2 (CAT-2)** --For voice, Integrated Services Digital Network (ISDN), and medium-speed data up to 4 Mbps. (obsolete)
- **Category 3 (CAT-3)** --For high-speed data and LAN traffic up to 16 Mbps (Used nowadays for Alarm Control Mechanisms in Apartments and Industry)
- **Category 4 (CAT-4)** --For long-distance LAN traffic up to 20 Mbps (obsolete)
- **Category 5 (CAT-5)** --For 100-Mbps LAN technologies such as 100-Mbps Ethernet over 100 MHz (Older LAN Standard. obsolete)
- **Category 5e (CAT-5e)** --Enhanced category 5 provides for full duplex Fast Ethernet support (used nowadays) with 1 Gbps upto 100 meters. Frequency 100 and 250 MHz.
- **Category 6 (CAT-6)** – 10 Gbps upto 164 feet 50/55 meters— anything beyond that will rapidly decay to only 1 Gigabit (the same as Cat5E). Frequency 350 MHz
- **Category 6a (CAT-6a)** -- 10 Gigabit speeds for the full 328 feet of Ethernet cable. Frequency 550 MHz.
- **Category 7 (CAT-7)** -- The maximum allowed length of a Cat-6 cable is 100 meters (330 ft) when used for 10/100/1000baseT and 55 meters (180 ft) when used for 10GbaseT. Frequency 600 MHz.
- Higher category UTP cables are made from higher quality materials.
- Each higher category is also made with tighter cable twists for increased resistance to

STP Cable

- STP cable consists of two or more twisted pairs of copper wire surrounded by flexible insulation, a foil shield, and an outer plastic sheath.
- In some types of multiwire STP cable, individual twisted pairs may be surrounded by their own foil shield.

- The foil shield helps dissipate EMI, particularly at data rates of 16 Mbps or higher.



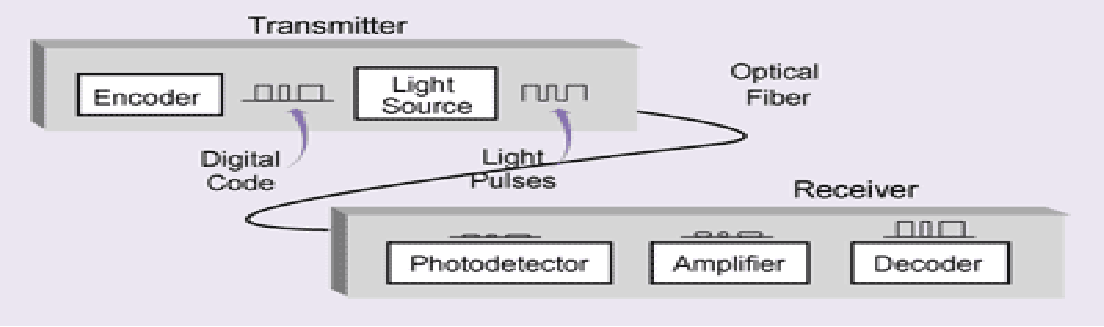
- STP wiring was the original cable specified for ring topology networks
- Used in Token Ring and Fiber Distributed Data Interface (FDDI).
- STP provides considerably more resistance to EMI/RFI than UTP
- It is also more bulky
- Less flexible
- More expensive to install.

Fiber Optic Cable

- A fiber optic cable is a thin strand of glass or plastic, coated with a protective plastic jacket. It is so thin that even the glass fibers bend easily.
- A beam of light can be trapped within a fiber, so that the optical cable essentially becomes a pipe that carries light around corners. An optical fiber can carry a light signal for a long distance typically up to 2 km.
- Because light is not appreciably affected by electromagnetic fields, optical signals are immune to EMI/RFI. This makes fiber a good choice for "noisy" environments with many electrical motors, such as elevator shafts and factories.
- Because fiber does not corrode, it is well suited for high-humidity and underwater environments. Optical fiber is also a highly secure medium, because it is difficult to splice (cannot flow) into a fiber optic cable without detection.
- The primary disadvantage of fiber optic cable is its cost. Fiber optic cable and equipment are relatively expensive in terms of both materials cost and installation.
- However, industries that need the high capacity and secure features of fiber find it well worth the investment. For example, nearly all long-distance telecommunication lines are fiber optic.

Fiber Communication System

- The basic model for a communication system includes a transmitter and receiver, connected by optical fiber cabling.
- In typical fiber optic systems, each device contains both a transmitter and receiver, combined in a single transceiver unit.

- Because fiber optic cable must be cut to present the light beam to a receiver, only point-to-point connections can be made; a bus cannot be constructed
- 

Transmitter

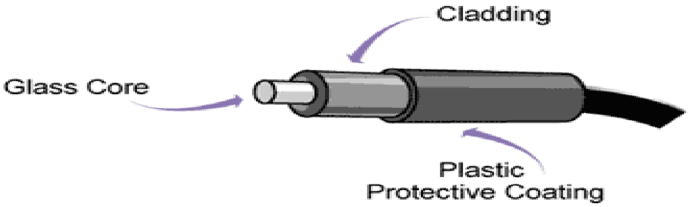
- Encoder that converts the input data signal into digital electrical pulses
- Light source that converts the digital electrical signal to light pulses
- Connector that couples the light source to the fiber through which the light rays travel
- The transmitter accepts digital electrical signals from a computer.
- A diode converts the digital code into a pattern of light pulses that are sent out to the receiver through the optical fiber.
- Light emitting diodes (LEDs) use less power and are considerably less expensive than lasers. LEDs can be used with multimode cable, and are the most common light source. LEDs provide a bandwidth of approximately 250MHz .
- Laser diodes are used with single-mode fiber for long-distance transmission. Laser light is more powerful because laser light waves are radiated in phase, which means the crests(H-peak) and troughs(L-peak) of all light waves are perfectly aligned with one another. This alignment or coherence creates a signal with much less attenuation and dispersion than noncoherent light. Laser diodes can provide much higher bandwidth 10 GHz.
- Frequency Range : 250 MHz to 10 GHz

Receiver

- A receiver converts the modulated light pulses back to electrical signals and decodes them. The receiver, contained within the destination computer system, includes:
  - Photo detector that converts the light pulses into electric signals
  - Amplifier, if needed
  - Message decoder

WARNING:

- Never look into a fiber optic cable to see whether light is present. The infrared laser light used in fiber optic LANs is invisible; however, it can permanently damage your eyesight in an instant.



- Core--A solid fiber of highly refractive clear glass or plastic that serves as the central conduit for light.

- Cladding--A layer of clear glass or plastic with a lower index of refraction. When light traveling down the core reaches the boundary between the core and cladding, the change in refractive index causes the light to completely refract or bend back into the core. The cladding of each fiber completely contains light signals within each core, preventing crosstalk. This effect is called "total internal reflection."

- Coating--A reinforced plastic outer jacket that protects the cable from damage.

Dimensions (Diameter)

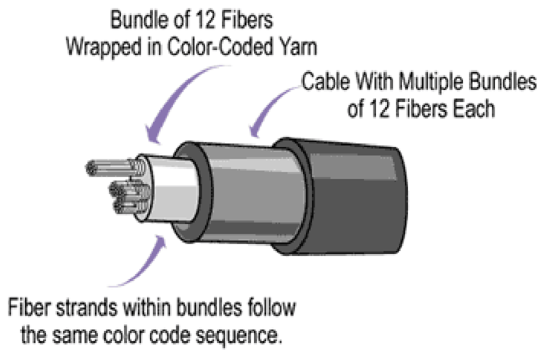
- Fiber optic cable is very thin. The diameters of fiber optic cores and cladding are specified in µm. The thinnest fiber optic cable (single-mode) typically has a core diameter of 5 to 10 µm I.e. 0.005 to 0.010 mm. Thicker fiber optic cable (multimode) ranges from 50 to 100 µm in core diameter. In comparison, human hair is approximately 100 µm thick.

- Fiber optic cable is specified in terms of its core and cladding diameter. For example, the most common type of fiber optic cable for LAN installations is 62.5/125-m cable, where 62.5 refers to the core diameter and 125 refers to the cladding diameter.

- The core diameter is also known as the aperture, because it determines the maximum angle from which the cable can accept light. Total internal reflection only occurs when light strikes the cladding at a shallow angle. If the angle is too steep, some or all of the light will penetrate the cladding itself, causing signal loss.

- Each fiber optic core conducts light in one direction only. Therefore, to send and receive, devices are usually connected by two fiber optic strands. These may be single strand simplex cables, or duplex cables containing two fiber optic strands. Duplex cables are more commonly used than simplex cables.

- Fiber cables can also consist of several bundles. These are used for high-capacity backbones for outdoor connections between campus buildings. Because light signals are completely contained within each fiber, no coating or shielding is necessary between fibers. However, reinforcing strands are usually added to increase the pulling strength of the cable.

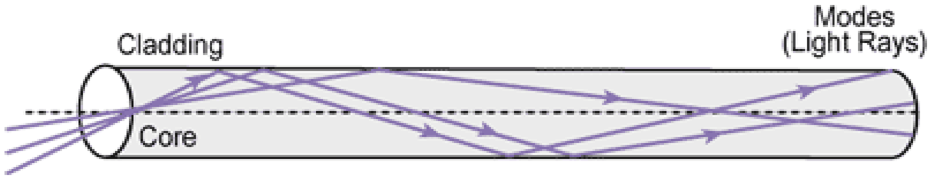

Bundle of 12 Fibers
Wrapped in Color-Coded Yarn
Cable With Multiple Bundles
of 12 Fibers Each
Fiber strands within bundles follow
the same color code sequence.

FOC General Types

- Multimode fiber is wide enough to carry more than one light signal. Each signal is called a "mode.”
- Single-mode fiber is thin and can carry only one light signal.

Multimode Fiber

- Each light signal or light ray that passes through a cable is called a "mode." Multimode fiber optic cable is wider than single-mode cable, thus it has enough room for more than one light ray. These light signals are separated by different angles of reflection as they travel down the core.
- Because multimode signaling separates light signals by angle, not all light rays travel the same distance. Some light rays will travel nearly straight through the core, while others bounce off the cladding many times before reaching the far end of the fiber.
- With modes traveling different distances, but at the same speed, the spread of the signal increases over time, and can cause data errors due to the overlapping of light pulses. This problem is known as modal dispersion. The construction of a multimode fiber can either cause or fix this problem.



Types of multimode fiber

1. Step-Index Fiber

The standard type of optical fiber, called "step-index fiber", consists of only two transparent layers (core and cladding), and index of refraction is same.

2. Graded-Index Fiber

The core of a graded-index fiber cable has several transparent layers, each with a different refractive index. This planned inconsistency allows light modes to travel at different speeds through the core. The speed at which the modes travel depends upon the part of the core it is traveling through. Modes traveling down the center of the core do so at a slower speed than those refracting off the cladding.

Single Mode Fiber

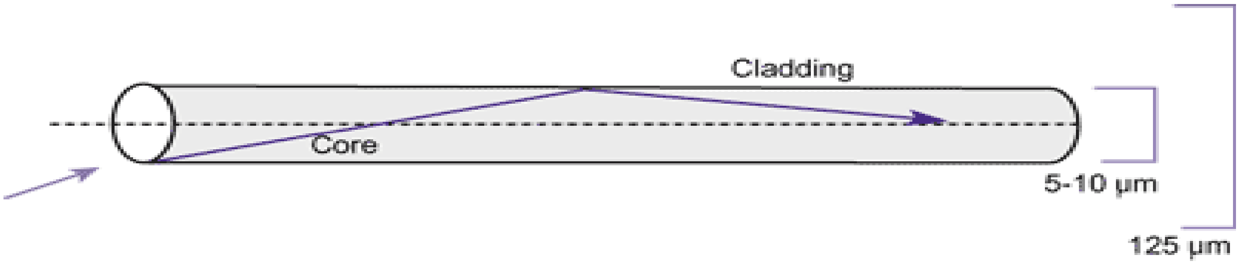
- Single-mode fibers have diameters sized to the wavelength they are designed to carry. A typical single-mode fiber core diameter is 8 µm. Only one mode will propagate through fiber with this core diameter. The narrower fiber diameter causes a light signal to travel in a straighter path, with less reflection and dispersion. However, the narrower core also makes single-mode fiber more difficult and expensive to install.

- Single-mode fibers require laser diode transmitters. By using this coherent light source, single-mode fiber optic cable can support longer transmission distances than multimode fiber. Distances range from a few miles to as many as 20 miles.

- Fiber optic cable is difficult to install correctly; therefore, it requires well-trained, careful installation technicians. This, combined with the time-consuming nature of each connection, make fiber optic cable the most expensive cable to install. Because of this need for training and experience, many organizations hire specialists to install fiber optic networks.

- Connections and splices of fiber optic cable are particularly difficult to make. Each end of the cable must be cut off at perfect right angles, the ends polished by hand or machine, and the cable precisely aligned to the connector.

- Single-mode fibers are generally step-index fibers. Because only one mode travels along the fiber, the problem of diffusion does not occur in single-mode fibers.



Optical Carrier Levels: OC-n

Optical Carrier Level	**Data Rate**
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-48	2.488 Gbps
OC-192	10 Gbps
OC-256	13.271 Gbps
OC-768	40 Gbps

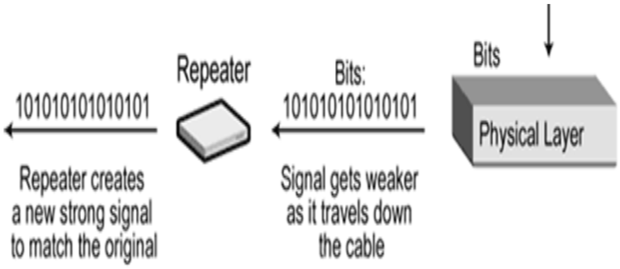
What do the fiber terms 9/125, 50/125 and 62.5/125 refer to?

The first set of numbers - 9, 50 and 62.5 refer to the diameter of the fiber cable's core. The second set of numbers - 125 refer to the diameter of the outside of the fiber cable's cladding. The cladding is a special coating that keeps the light from escaping the glass core. 9/125 refers to a single mode fiber cable. 50/125 and 62.5/125 refer to multimode fiber cable

Network Devices:

REPEATER:

Repeater is the physical layer device used to extend the length of LAN according to IEEE 5-4-3 rule.


Bits
Physical Layer
Bits:
101010101010101
Repeater
101010101010101
Signal gets weaker as it travels down the cable
Repeater creates a new strong signal to match the original

Firewire 75ohm COAX BNC Repeater　　**Repeater connecting two segments**

It works on bit, hence called Layer-1 device. It solves the problem of attenuation. It repeats the signal as well as noise. It regenerates the bit pattern to boost the signal. Used to extend the max length and follows 5-4-3 rule. It is non discriminating device because all incoming signals are passed on to each connected segment. They are transparent to the sending and receiving devices. Repeaters are fast, simple to use, and inexpensive. Repeater cannot connect two different media access types. It cannot recognize the contents or format of a frame or convert one type of Data Link header to another. Repeaters are not amplifiers. It boosts the signal and does not amplify it. Nowadays instead of repeaters, extenders are used to extend the diameter of LAN.

EX 10/100/1000 Ethernet Extender

LAN Extenders are used to extends 10/100/1000Base-T Ethernet up to 10,000 feet (3 KM) over two wire twisted cable.

HUB

Netgear EN104TP 4-Port 10 Mbps Ethernet Hub RJ-45 with Uplink Button

Sixteen 10Mbps UTP Ports and One BNC Port Ethernet HUB

- Serves as the center of a star-topology LAN. Multiport repeater or a concentrator
- Not intelligent and only Boost the signals. Simply broadcasts the bits on all other interfaces
- Does not filter data packets based on destination. Fault tolerance
- Inexpensive compared to switches or routers. Failure can also happen if power to the hub is lost.
- A network can be designed so that all traffic flows through one or more hubs
- A network connected by simple hubs is one large collision domain. As more users share the same collision domain, performance gradually decreases
- Automatically counts as the regenerations

Bridge

D-Link Bridge

- Operate at MAC sub layer
- connects and passes packets between two networks
- More intelligent than hub
- analyzes incoming packets and forwards (or drops) based on addressing information.
- Control broadcasts to the network
- Maintain address tables
- Plug and Play in nature
- High packet filtering and forwarding rate
- Does not offer protection against broadcast storms
- Spanning Tree protocol restricts the effective topology of bridged networks
- Does not support handshaking protocol, such as ICMP with IP
- Cannot reorder packets
- MAC address has no topological meaning

- Bridges divide a network into separate collision domains, because they use NIC addresses to filter or forward traffic between different network segments.
- This segmentation provides a larger share of the available bandwidth to each end station in each smaller collision domain.
- Isolate traffic between LAN segments that have nodes that only occasionally send traffic across the bridge
- Bridges can connect networks running different high-level protocols, without requiring additional software.
- There is a limit to the size of bridge-based networks. Each time a frame traverses a bridge it is delayed as the bridge software reads the source and destination addresses, checks its address database, and determines whether to forward the frame to each port.
- While network segments attached to a bridge belong to different collision domains, they all belong to the same broadcast domain.

Router / Rowter /Rooter

Cisco Router 1841

- Forward packets between one network to another.
- Path determination using metrics.
- Can choose best path that exists between S and D
- Reconfigures topology quickly to reduce service loss
- Station supports is unlimited
- Barrier against broadcast storms
- Capability of fragment and reassemble
- Provides congestion feedback

- A router can also provide firewall service and economical WAN access. Routers are essentially software devices. They process complex protocol suites, sometimes many suites, using powerful processors and memory.
- Makes intelligent packet-forwarding decisions based on each packet's network address.
- As Network Layer devices, routers are protocol dependent. They can interconnect networks that have the same communications architecture, but possibly different lower level architectures.
- The enhanced intelligence of a router allows it to support redundant network paths, and select the best forwarding path based on several factors in addition to the destination MAC address. This increased intelligence can also result in enhanced data security, improved bandwidth utilization, and more control over network operations.
- **a router determines the logical boundaries between groups of network segments.**
- Ability to support mesh network topologies that provide active redundant paths.
- Unlike switches and bridges, which require a loop-free topology, routing protocols impose no constraints on network topologies, even on those that contain redundant paths and active loops.
- Routers can perform load balancing over parallel equal-cost paths to make the best use of available bandwidth

Router Disadvantages

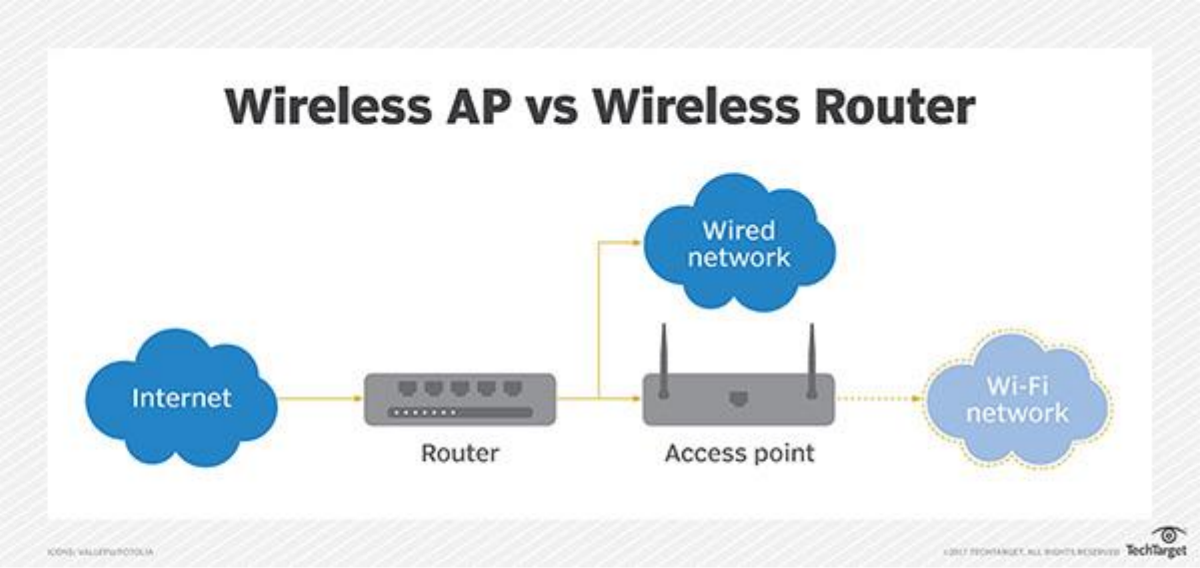
- Routers also have several disadvantages as follows.
- The additional software processing performed by a router can increase packet latency, reducing the router's performance when compared to simpler switch architecture.
- To be "routable," an architecture must have a Network Layer. Not all do; those protocols must be bridged. "Unroutable“ protocols include DEC-LAT terminal communications protocol, IBM's SNA, and NetBIOS/NETBEUI.

When to Use Routers

- Routers are needed when network applications require limiting broadcast traffic.
- Support for redundant paths
- Intelligent packet forwarding, or WAN access.

Access Point:

Access Points are used to create Wi-Fi network from wired network and extending a **wireless** network. Nowadays access points are used as both router and to create wi-fi networks.

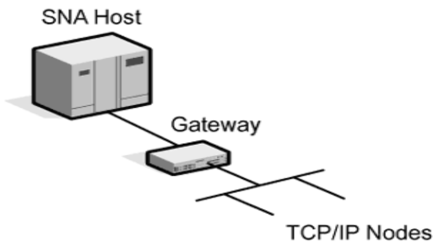


Gateways

Cisco PGW Packet Data Network Gateway

A gateway, also called a protocol converter, converts data between two distinct types of protocol architectures. A gateway operates at all protocol levels above the Data Link Layer, and is transparent to both ends of the connection.

A gateway is the only internetworking device that can change the form of a network transmission from that of one communications architecture to that of another. For example, a gateway can connect a Transmission Control Protocol/Internet Protocol (TCP/IP) network to an SNA network, as shown on the Gateway Diagram. Protocol conversion is a software-intensive (slow) process, different for each specific pair of protocol stacks. A gateway receives frames from one communications architecture, and must convert them to another architecture by building new headers for every layer of the protocol stack.



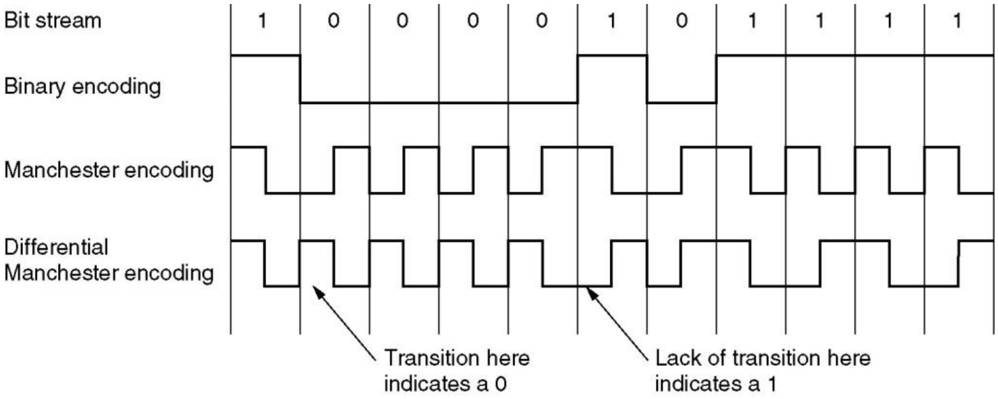
Tree Topology : Generalization of bus topology
Server – switch – segments
Or Tree with IMP and Controllers

Star Topology

1. Logically bus but organization is ptp
2. Cable configuration is point to point
3. Transmission in both direction
4. 10 to 100 Mbps
5. Broadcast
6. Any machine master
7. WS can transmit at any time
8. IEEE 802.3
9. Easy to Install , reconfiguration and fault isolation
10. More HW and Cabling
11. Campus Network
12. Cable break / puncture is dangerous
13. Frame Gap is needed
14. Minimum frame size
15. Passive and Active Hubs and switches

Additional Inputs:
Manchester and Differential Manchester Encoding:
Encoding is different than modulation. It is about representation of data. Encoding is about assigning different binary codes according to a particular algorithm.

802.3 baseband systems uses Manchester's encoding
1-bit => 0.85 volt
0-bit => -0.85 volt
Gives DC value => 0 volt
1 => High to Low at middle
0 => Low to High at middle


Bit stream
1 0 0 0 0 1 0 1 1 1 1
Binary encoding
Manchester encoding
Differential Manchester encoding
Transition here indicates a 0
Lack of transition here indicates a 1

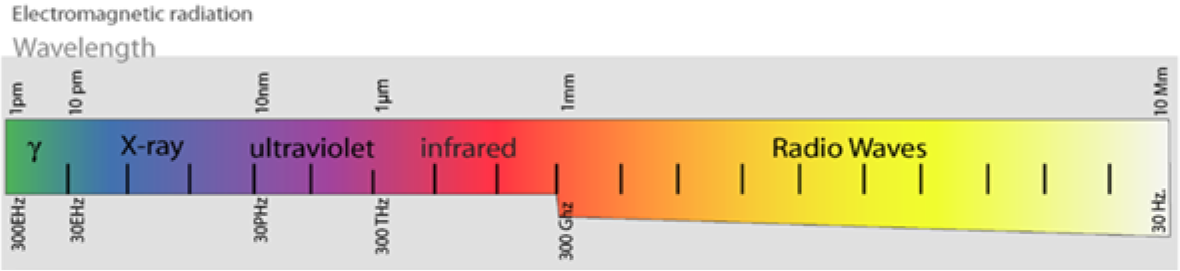
Radio Spectrum:

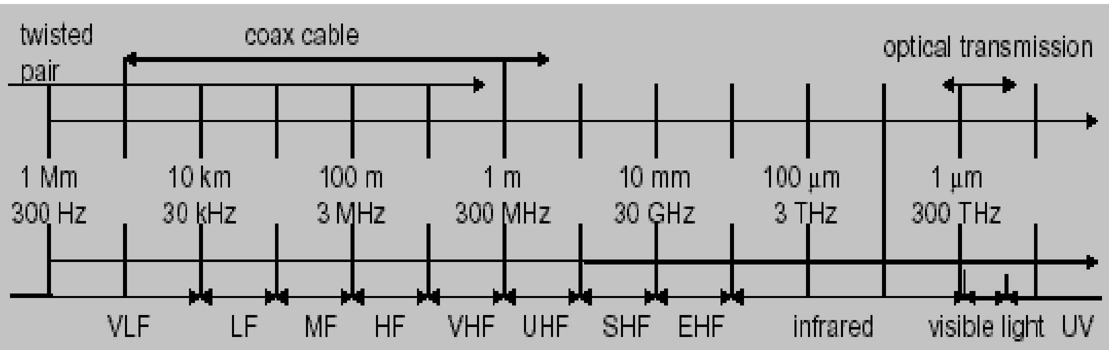
- **Radio** is an electromagnetic phenomenon in which energy travels in waves through an given medium. **Radio** is a way to send electromagnetic signals over a long distance, to deliver information from one place to another. **Radio** is the wireless transmission of signals by modulation of electromagnetic waves with frequencies below those of visible light.
- **Radiation** is energy that travels and spreads out as it goes. e.g. **Visible Light** that comes from a lamp in your house

- **Radio Spectrum** is the part of the electromagnetic spectrum from 3 Hz to 3000 GHz (3 THz).
- **Radio Spectrum** is a name given to a bunch of types of radiation

- **Electromagnetic Energy** : It's a combination of electrical power and magnetic vibrations

- **RF propagation** refers to how well radio signal radiates or travels into free space.





VLF = Very Low Frequency

LF = Low Frequency

MF = Medium Frequency

HF = High Frequency

VHF = Very High Frequency

UHF = Ultra High Frequency

SHF = Super High Frequency

EHF = Extra High Frequency

UV = Ultraviolet Light

Frequency and wave length:

$$\lambda = c/f$$

wave length λ, speed of light $c \cong 3\text{x}10^8$m/s, frequency f

	Band		Application
ELF :	0Hz – 3KHz	:	Unused
VLF :	3 KHz - 30 KHz	:	Submarine Navigation
LF :	30 KHz - 300KHz	:	Submarine Navigation, ATC
MF :	300 KHz - 3 MHz	:	AM Radio
HF :	3 MHz - 30 MHz	:	SW Radio
VHF :	30 MHz - 300 MHz	:	TV, FM Radio and Paging
UHF :	300 MHz - 3 GHz	:	Mobile, UHF TV, Directed Microwave Link 2.4 GHz ISM
SHF :	3 GHz - 30 GHz	:	Fixed Satellite (C, Ku, Ka Bands)
EHF :	30 GHz - 300 GHz	:	Radio astronomy, remote sensing

Wireless LANS : The IEEE 802.11 Physical Layer

WLAN are very popular nowadays for Hotel, Buildings, Airport, and Garden

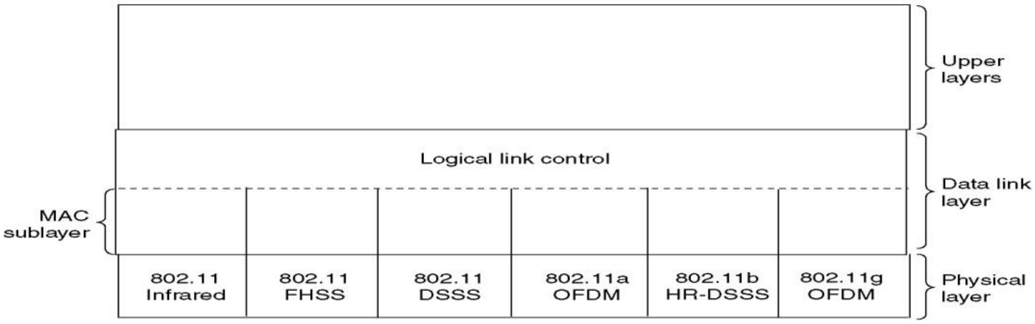
Advantages

- Very flexible within the reception area
- Ad-hoc networks without previous planning possible
- Almost no wiring difficulties
- More robust against disasters like earthquakes, fire or users pulling a plug...

Disadvantages

- typically very low bandwidth compared to wired networks (1-10 Mbit/s)

The 802.11 Protocol Stack

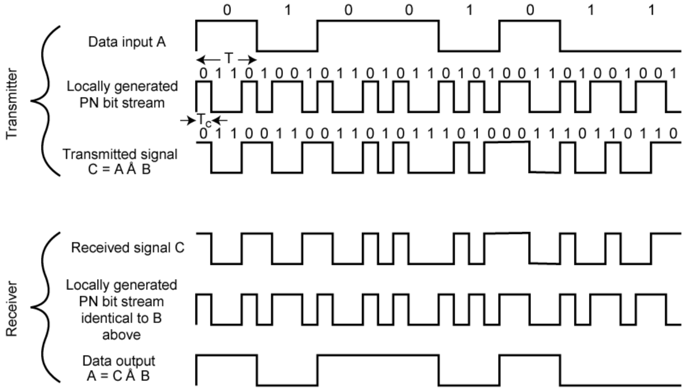


802.11 Direct Sequence Spread Spectrum(DSSS)

– Spread spectrum Technology / Broadband Technology
Input: data bit and 11 bit barker code

- Combine input with spreading code using XOR
- Input bit 1 inverts spreading code bit
- Input zero bit doesn't alter spreading code bit
- Data rate equal to original spreading code
- Each information bit is transmitted as a pseudorandom sequence of chips
- To recover the original data, same PN Sequence is multiplied to received signal
- Speed 2 Mbps
- Uses phase shift modulation : DBPSK
- Operates at 2.4 GHz band

Example: Using 4-bit chip/PN code



802.11 Frequency Hopping Spread Spectrum (FHSS)

- A method of transmitting signals by rapidly switching a carrier among many frequency channels : 79 Channel each 1 MHz wide
- This uses a pseudorandom sequence known to both transmitter and receiver
- Operates at 2.4 GHz
- Modulation : GFSK

Two versions

- Fast Hopping: several frequencies per user bit
- Slow Hopping: several user bits per frequency

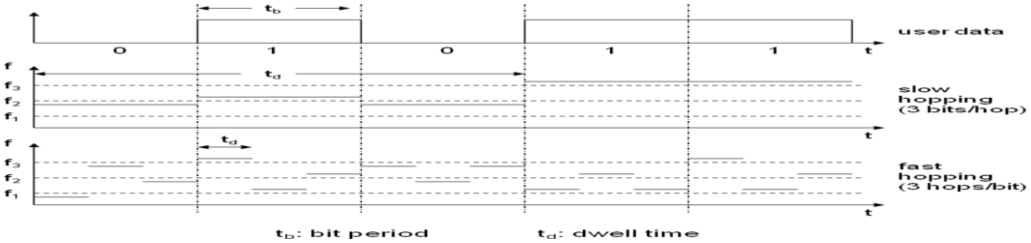
Advantages

- frequency selective fading and interference limited to short period
- simple implementation
- uses only small portion of spectrum at any time

Disadvantages

- not as robust as DSSS
- simpler to detect

Example of FHSS


t_b
user data
0
1
0
1
1
t
f
t_d
f_3
f_2
f_1
slow hopping (3 bits/hop)
t
f
t_d
f_3
f_2
f_1
fast hopping (3 hops/bit)
t
t_b: bit period
t_d: dwell time