

Gemini Communication Ltd.

Innovation & Leadership

Basics of Networking

Ref. 1010001100

BASICS OF NETWORKING

BASIC NETWORKING DEVICES IN LAN SET UP.

- Hub
- Bridges
- Switch
- Router
- UTP Cable
- STP Cable.
- RJ 45 Connectors

HUB

- A Hub is a passive and Layer 1 device, shared media, used in star topology network.

- Properties of Hub:

They amplify signals

They propagate signals through the network

They do not require filtering

They do not require path determination or switching.

Hub is a collision domain-The network area with which data packets originate and collide is called collision domain.

The Work Station handling capacity is limited.The total bandwidth is presented at all the ports in a Hub.

BRIDGES

Bridges operate at Layer 2, the data link layer

- Bridges eliminate unnecessary traffic and minimise the chances of collisions occurring on a network by dividing it into segments and filtering traffic based on station or MAC address.
- It creates the MAC address table by “self learning”.
- They control broadcasts to the network .
- They maintain address tables.
- Bridges are software based and slower in nature.

SWITCH

- A switch is an active device which has the same characteristics of a Bridge .
- The advantage of switch is hardware based and faster in nature.

ROUTER

- Routers are used to connect separate networks and to access the internet.
- Routers provide end to end routing by passing the data packets and routing traffic between different networks based on network protocol or Layer 3 information.
- Router matches information in the routing table with the data's destination IP address and sends incoming data to correct subnetwork and host.

CSMA/CD

- In Computer networking , **Carrier Sense Multiple Access, Collision Detection (CSMA/CD)** is a network control protocol in which a carrier sensing scheme is used.
- CSMA/CD is an access method that allows only one station to transmit at a time on a shared medium.

ETHERNET STANDARD

- It operates at a base band signaling rate of 10 Mbps, which is referred to as 10Base.
- 10 Base 2 –Known as thin ethernet allows network segments up to 185 meters on coaxial cable.
- 10 Base 5-Known as thick ethernet ,allows network segments upto 500 meters on coaxial cable.
- 10 Base T-Provides access using inexpensive UTP cables typically upto 100 meters.

UTP CABLE

- **Unshielded twisted pair (UTP)** is the most common cable used in computer networking .
- It is a thin, flexible cable that is easy to string between walls. UTP costs less per foot than any other type of LAN cable .It is more prone to electrical noise and interference than other types of networking media. Its unrepeated length limit is 100 meters



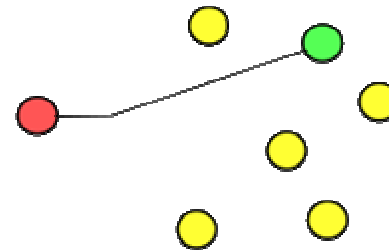
STP CABLE

- STP cabling includes metal shielding over each individual pair of copper wires. This type of shielding protects cable from external EMI (electromagnetic interferences)
- STP cables are more expensive than UTP cable.



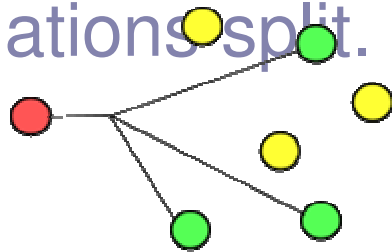
UNICAST

- Unicast
unicast is the sending of information packets to a single destination .



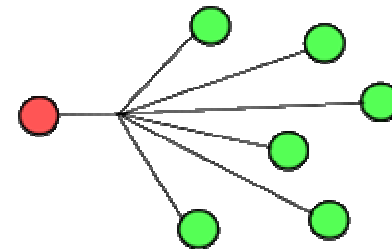
MULTICAST

- **Multicast** is the delivery of information to a group of destinations simultaneously using the most efficient strategy to deliver the messages over each link of the network only once, creating copies only when the links to the destinations split.



BROADCAST

- In computer networking, **broadcasting** refers to transmitting a packet that will be received (conceptually) by every device on the network



PROTOCOLS

- A protocol is a set of messages with a specific format

TYPES OF PROTOCOLS

- Routing Protocols
- Routed Protocols

ROUTED PROTOCOLS

- Routed Protocols provide enough information in its network layer address to allow a packet to be forwarded from host to host based on the addressing scheme. Packets generally are conveyed from end system to end system.
- TYPES
- AppleTalk
- IPX
- IP

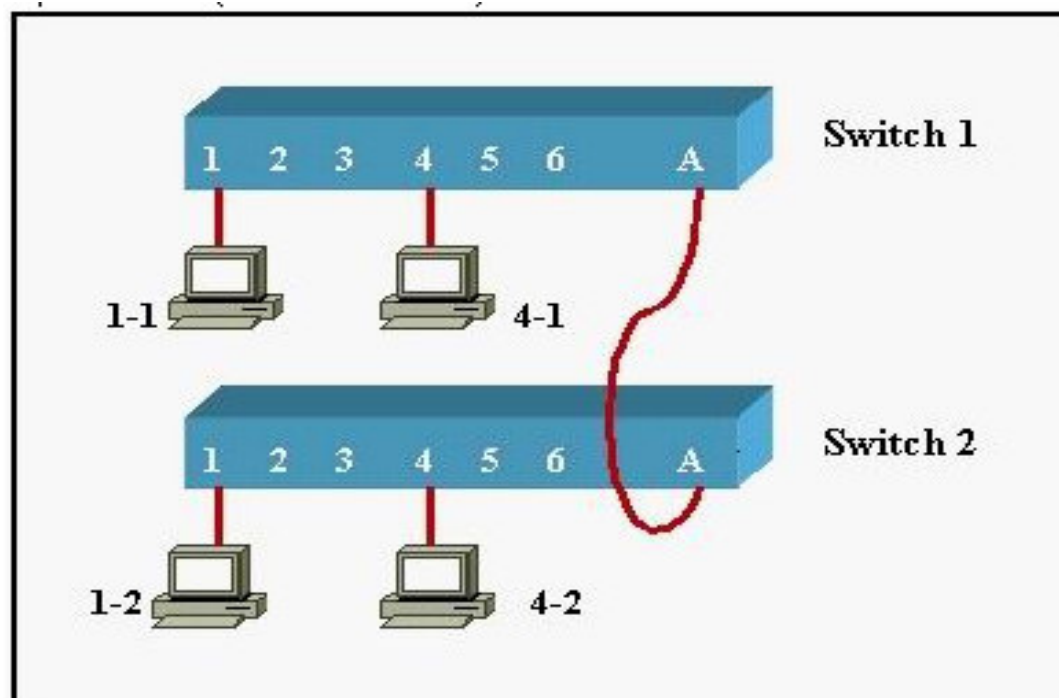
ROUTING PROTOCOLS

- A routing protocol allows the routers to communicate with other routers to update and maintain tables. Routing protocol messages move between routers.
- TYPES
- RIP
- IGRP
- OSPF
- EIGRP

VLAN

- VLAN divides a single LAN into 'X' number of Virtual LANs.
VLAN technology creates virtual LANs that utilize the benefits of independent Lan, while retaining access to the entire LAN.
A virtual LAN removes selected traffic and places it within a virtual LAN
The result is less traffic on the entire LAN

VLAN CONNECTION



SWITCH 1-Ports 1-3(Vlan 1)

Ports 4-6(Vlan 2)

SWITCH 2-Ports 1-3(Vlan 1)

Ports 4-6(Vlan 2)

TYPES OF VLANS

- PORT BASED VLANS
- IP BASED VLANS
- MAC ADDRESS BASED VLANS

DIFFERENCE BETWEEN L2 & L3 SWITCHES

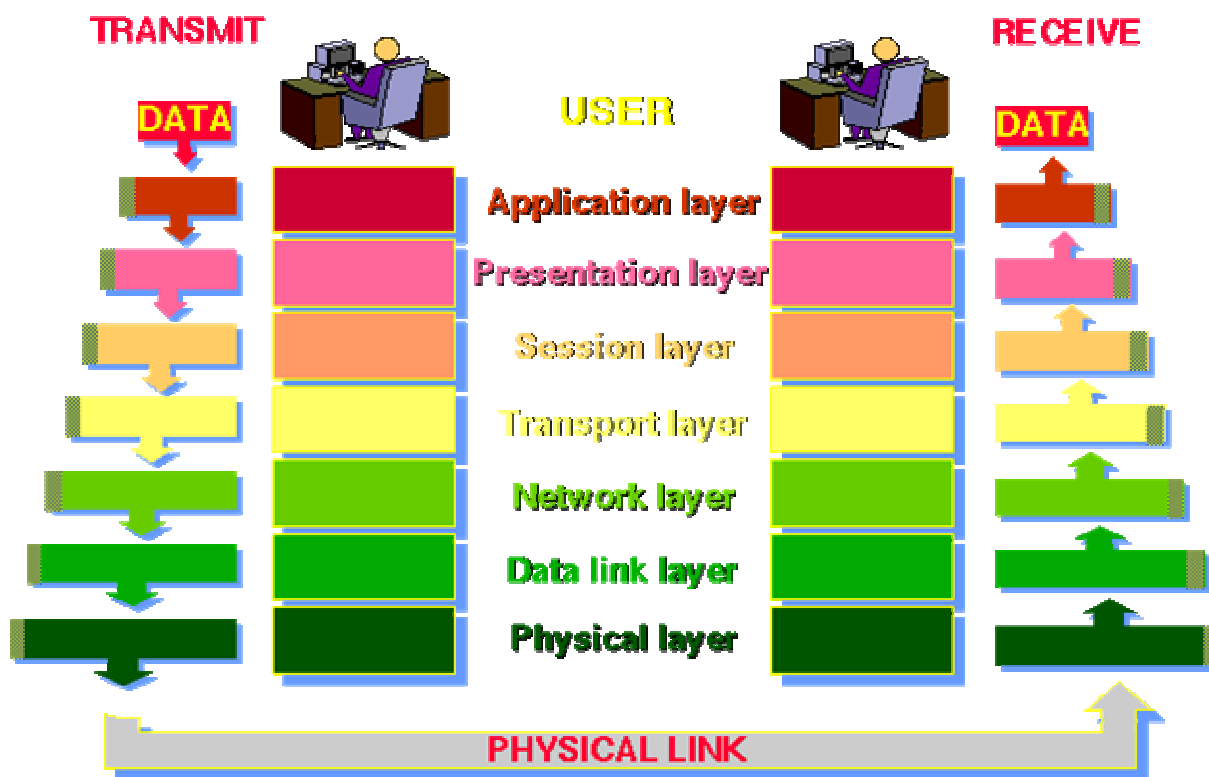
- The only difference between Layer 2 and Layer 3 is that Layer 3 switching hub support routing function

BENEFITS OF LAYER3 SWITCHING

- **INTER VLAN CONNECTIVITY**
- **ENHANCED PERFORMANCE**
- **SIMPLIFIED MANAGEMENT**
- **ENHANCED SECURITY**
- **LOW COST**
- **FLEXIBLE NETWORK SEGMENTATION**
- **BETTER USE OF SERVER RESOURCES**

LAYERS OF NETWORKING

THE 7 LAYERS OF OSI



- **Physical layer**

- The physical layer is the most basic network layer, providing only the means of transmitting raw bits rather than packets over a physical data link connecting network nodes. No packet headers nor trailers are consequently added to the data by the physical layer

- **Data link**

- This is the layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segments. The data link layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical layer. Examples of data link protocols are Ethernet for local area networks and PPP, HDLC and ADCCP for point-to-point connections.

- **Network layer**

- The network layer is level three of the seven level OSI model as well as of the five layer. In the four layer TCP/IP reference model it is called Internet layer, which is the second layer from below. It responds to service requests from the transport layer and issues service requests to the data link layer

- **Transport layer**

- In computing and telecommunitaion , the transport layer is the second highest layer in the four and five layer TCP/IP rreference odels, where it responds to service requests from the application layer and issues service requests to the network layer. It is also the name of layer four of the seven layer OSI model, where it responds to service requests from the session layer and issues service requests to the network layer. The definitions of the transport layer are slightly different in these two models. The following text primarily refers to the TCP/IP model

- **Session layer**

- The session layer is level five of the seven level OSI model It responds to service requests from the presentation layer and issues service requests to the transport layer. The Session layer provides the mechanism for managing the dialogue between end-user application processes. It provides for either full duplex or half-duplex operation and establishes checkpointing, adjournment, termination, and restart procedures

- **presentation layer**

- The presentation layer is the sixth level of the seven layer OSI model. It responds to service requests from the application layer and issues service requests to the session layer. The presentation layer is responsible for the delivery and formatting of information to the application layer for further processing or display. It relieves the application layer of concern regarding syntactical differences in data representation within the end-user systems. *Note:* An example of a presentation service would be the conversion of an EBCDIC-coded text file to an ASCII-coded file

- **Application layer**

- The application layer is the seventh level of the seven-layer OSI model. It interfaces directly to and performs common application services for the application processes; it also issues requests to the presentation layer. The

PORT NOS

Application Layer	FTP	HTTP	HTTPS	TELNET	DNS	SMTP	TFTP	POP3	SNMP
Port no	21	80	8080	23	53	25	69	110	161
Transport Layer	TCP					UDP			

Port no are unique and industry standard

IP ADDRESS

- An IP address is 32 bit logical address.
- Each IP address is divided into 4 octets (8 bits each)
- An IP address is based on the internet protocol.
- IP addresses exist at Layer 3, the network layer of the OSI reference model.
- Every LAN must have its own unique IP address, an IP address is essential for internetworking over WAN to take place.
- An IP address exists at Layer 3, the network layer of OSI reference model.

MAC ADDRESS



Media Access Control address (MAC address) is a unique identification attached to most network adapters (NICs). It is a number that acts like a name for a particular network adapter, so, for example, the network cards (or built-in network adapters) in two different computers will have different names, or MAC addresses, as would an Ethernet adapter and a wireless adapter in the same computer, and as would multiple network cards in a router. MAC address is 48 bit in nature .

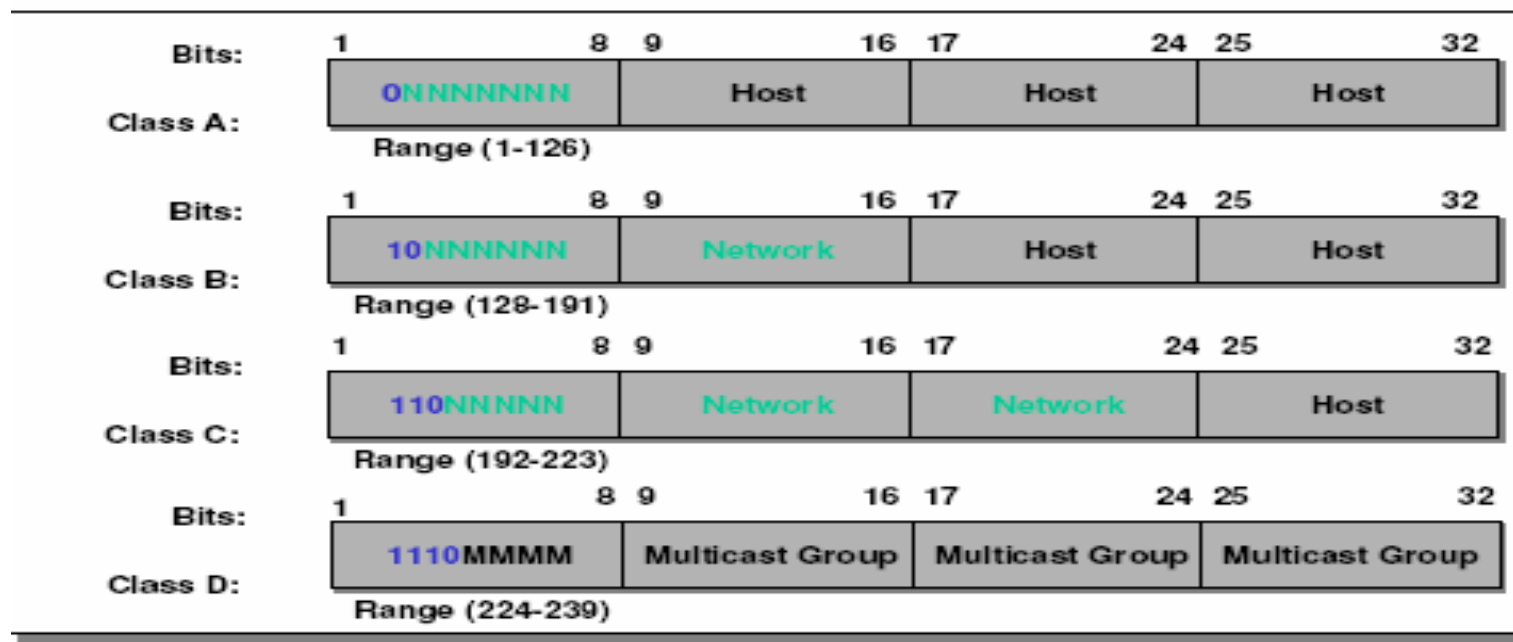
IP CLASSES

IP Classes

	8 Bits	8 Bits	8 Bits	8 Bits
•Class A:	Network	Host	Host	Host
•Class B:	Network	Network	Host	Host
•Class C:	Network	Network	Network	Host
•Class D:	Multicast			
•Class E:	Research			

IP ADDRESS CLASSES

IP Address Classes



Subnet Mask

- The subnet mask is the network address plus the bits reserved for identifying the sub network. (By convention, the bits for the network address are all set to 1, though it would also work if the bits were set exactly as in the network address.) In this case, therefore, the subnet mask would be 11111111.11111111.11110000.00000000. It's called a mask because it can be used to identify the subnet to which an IP address belongs by performing a on the mask and the IP address. The result is the sub network address
- :Subnet Mask 255.255.240.000
 11111111.11111111.11110000.00000000
- IP Address 150.215.017.009
 10010110.11010111.00010001.00001001
- Subnet Address 150.215.016.000
 10010110.11010111.00010000.00000000

NAT

NAT (Network Address Translation or Network Address Translator) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the *inside* network and the other is the *outside*. Typically, a company maps its local inside network addresses to one or more global outside .

Types of NAT

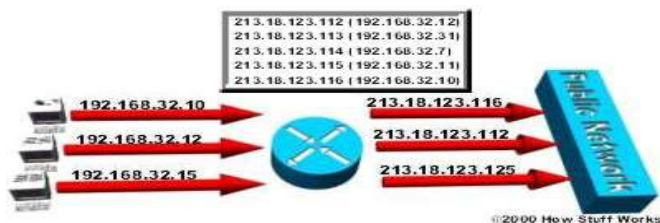
Static NAT

Static NAT is a one-to-one mapping between an unregistered IP address and a registered IP address.



Dynamic NAT

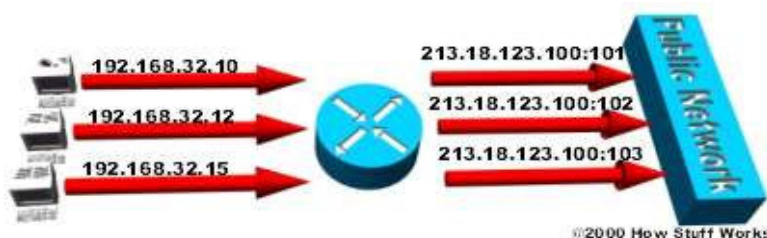
Static NAT



More commonly, Dynamic NAT is implemented, where a pool of public IP addresses is shared by an entire private IP subnet. When a private host initiates a connection, a public IP address is selected. The mapping of the computer's non-routable IP address matched to the selected IP address is stored in the NAT Table. As long as the outgoing connection is maintained, the private host can be reached by incoming packets sent to the specified public address. When the binding expires, the address is returned to the pool for reuse.

TYPES OF NAT

Overloading



A variation of Dynamic NAT known as Network Address Port Translation (NAPT) maps multiple unregistered IP addresses to a single registered IP address by multiplexing streams differentiated by the TCP/UDP port number.

Thank You

Leave IT to us

Contact : info@gcl.in