UNIT-5

Network Addressing & Management

5.1 Introduction To Network Addressing:

Each device on a network has an address that is unique within the network. Any device that wishes to send data to another device includes the address of the destination device along with the data. The device whose address matches with the destination address accepts the data while all other devices ignore it. If the destination address of the data does not match with the address of any device on the network it is forwarded to a different network with the help of a router.

The middle layer protocols used on the network are responsible for providing a unique address to each device on the network.

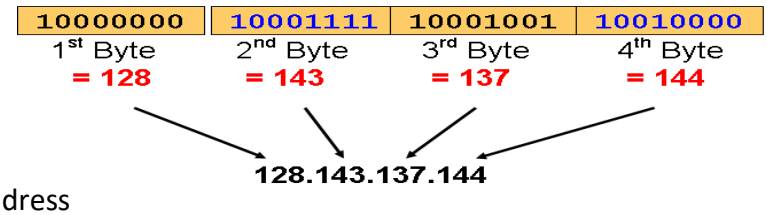
The following are the middle layer protocols available:

1. TCP /IP (Transmission Control Protocol/ Internet Protocol)
2. IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange)
3. NETBIOS (NETBIOS Enhanced User Interface).

5.2 Know About TCP/IP Addressing Scheme:

- ✓ TCP/IP uses a 32 bit addressing scheme to identify the devices of a network.
- ✓ 32 bits are divided into 4 octets, of eight bit each.
- ✓ An IP address is a 32 bit long identifier
- ✓ The format of representing an IP address is called the ***dotted decimal*** **notation**
- ✓ Each byte is identified by a decimal number in the range [0-255]

Dotted Decimal Notation example



Example:

The 32-bit binary address

11000110.10101100.10101000.00001010

Represents the IP address 198.172.168.10

5.2.1 COMPONENTS OF IP ADDRESS:

IP address is divided into the following components:

1. **Host address**: This is the address of the device within the network.
2. **Network address:** This is the address of the network itself, and is used by other networks to identify this network.

There may be several computers in a particular network. The IP address of all these computers begin with the same network address.

Ex:

198.172.168.11

198.172.168.12

Network Address

Host Address

Example:

Network address is: 128.143.0.0

Host number is: 137.144

TCP/IP allows network administrators the flexibility to decide the number of octets for the network and host address with the help of IP address classes.

5.2.2 IP ADDRESS CLASSES:

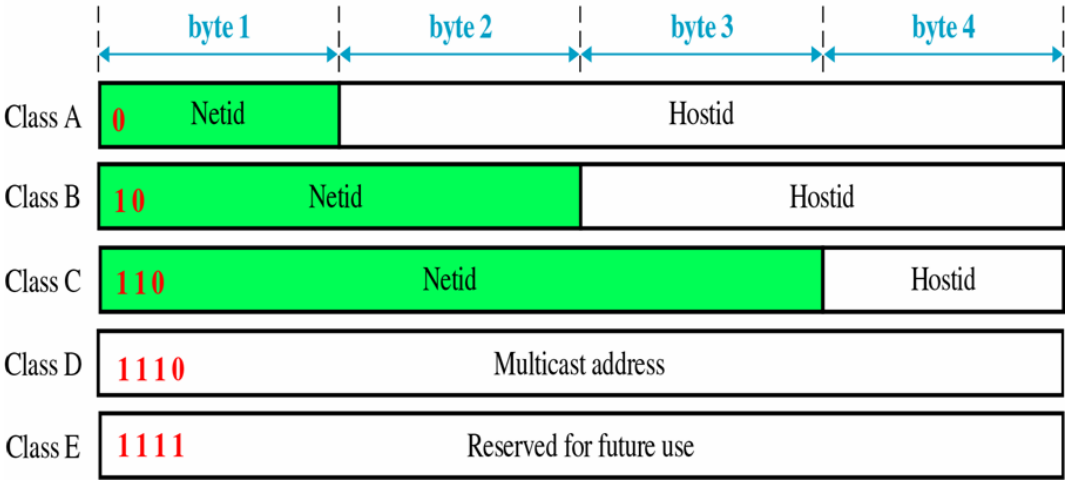
- ✓ IP address classes provide network administrators with the flexibility to select an IP address format depending on the needs of the network.
- ✓ ***Ex:-***On a network with 50 computers it is sufficient that only last octet used to represent the host address. If a network has 2000 computers, then the last two octets should be used to represent the host address.
- ✓ The process of determining the number of octets that represent the network and host addresses is standardized with the use of IP address classes.

Classes –

There are currently 5 different classes of address.

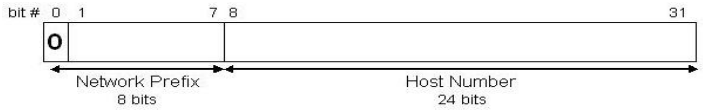
a)Class A b)Class B c)Class C d)Class D e)Class E

- ✓ Class A: Network prefix is 8 bits long
- ✓ Class B: Network prefix is 16 bits long
- ✓ Class C: Network prefix is 24 bits long
- ✓ Each IP address contained a **key** which identifies the class:
  - **Class A:** IP address starts with **"0"**
  - **Class B:** IP address starts with **"10"**
  - **Class C:** IP address starts with **"110"**
  - **Class D**: IP address starts with **"1110"**
  - **Class E:** IP address starts with **"1111"**



Classfull IP Addresses - Class A:

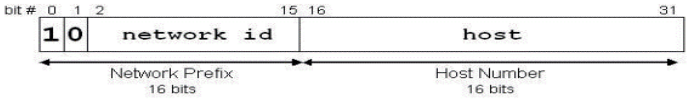
- ✓ In this class, the first octet is used for the network address, and the remaining three octets can represent a host address.



- ✓ Class A network can have up to 16,777,216(256*256*256) devices.
- ✓ Class A can have 127 different type of networks connected.
- ✓ The first octet can take a value between 1 and 127.
- ✓ Remaining 3 octets can take value from 0 to 255.
- ✓ Range of Class A is from 1.0.0.0 to 127.255.255.255
- ✓ Examples: 10.35.4.186 and 126.254.186.99 are examples of Class A addresses.
- ✓ Class A networks are used by large organizations and large ISPs with a large number of hosts.

Classfull IP Addresses - Class B:

- ✓ Class B uses the first two octets for the network address and the last two octets for the host address.



- ✓ Class B networks can have up to a maximum of 65,536 hosts (used 65,534)
- ✓ The first octet of a Class B address can range from 128 through 191.
- ✓ Remaining octets however can range from 0 through 255.
- ✓ Range of Class B is from 128.0.0.0 to 191.255.255.255
- ✓ Examples: 130.59.5.34 and 168.192.220.10
- ✓ Class B networks are also used by large organizations and universities.
- ✓ Class A and Class B addresses are mainly suited for large organizations.

The performance of the network goes down if all the computers are connected in a single network.
Mainly Class A and Class B, uses huge number of hosts per network that increases the difficulty of managing a network.

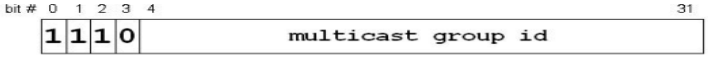
Classfull IP Addresses - Class C:

- ✓ The first, second, and third octets are used to denote the network address in Class C while fourth octet denotes the host address

- ✓ Class C network can accommodate only 256 hosts (used 254).
- ✓ The first octet can take a value between **192** and **223.**
- ✓ Remaining 3 octet can take value from 0 to 255
- ✓ Range of Class C is from 192.0.0.0 to 223.255.255.255
- ✓ Example--192.168.10.20 is an example of Class C address.
- ✓ Class C is most commonly used IP address class in LANs because most LANs do not have more than 255 hosts.

Classfull IP Addresses - Class D:

- ✓ Class D addresses are not provided for addressing networks.
- ✓ Class D addresses are used for *multicast*, the process of sending the same data to the multiple computers on a network or across different networks.



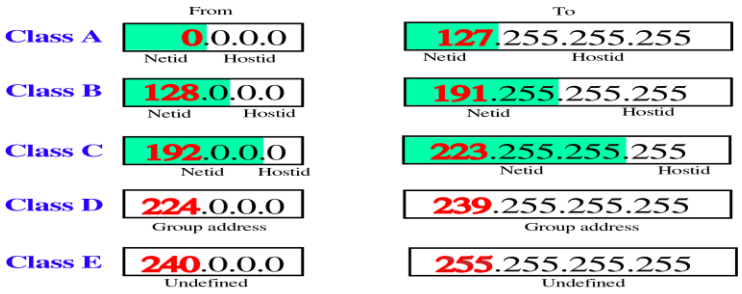
- ✓ The first octet of a Class D address can range from 224 through 239.
- ✓ Remaining octets however can range from 0 through 255.
- ✓ Range of Class D is from 224.0.0.0 to 239.255.255.255
- ✓ Example--225.38.254.254 is an example of Class D address.

Class Full IP Addresses - Class E:

- ✓ Like class D addresses, Class E addresses are also not available for network addressing.
- ✓ In fact, Class E addresses are reserved for experimental purposes. These addresses made available for normal use in the future.

- ✓ Range of Class E is from 240.0.0.0 to 255.255.255.255

Class ranges of Internet addresses:



Range of classes:

IP address Class	IP address range
Class A	1.0.0.0 to 127.255.255.255
Class B	128.0.0.0 to 191.255.255.255
Class C	192.0.0.0 to 223.255.255.255

Limitations of IP address classes

The performance of the network goes down if all the computers are connected in a single network.

Ex: Imagine an Ethernet LAN with 3,000 Computers. Ethernet broadcast the data to all hosts, and therefore, the traffic in this LAN would be extremely high resulting in poor network performance.

If we connect huge number of hosts per network that increases the difficulty of managing a network.

Problem 1: Inflexible. Assume a company requires 10,000 addresses

Class A and B addresses are overkill (>64,000 addresses)

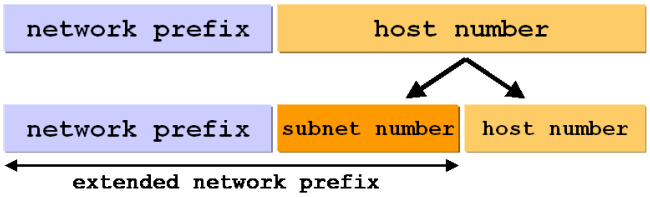
Class C address is insufficient

Problem 2: Flat address space. Routing on the backbone Internet needs to have an entry for each network address. In 1993, the size of the routing tables started to outgrow the capacity of routers.

Problem 3: Too few network addresses for large networks.

5.2.3 IP SUBNETTING:

- ✓ "Subnetting is a process of dividing large network into the smaller networks. Each of these smaller networks are called **subnets**."
- ✓ The process of creating subnets is called **subnetting** which improves the network performance.
- ✓ The host part of an IP address is divided into a subnet number and a host number.



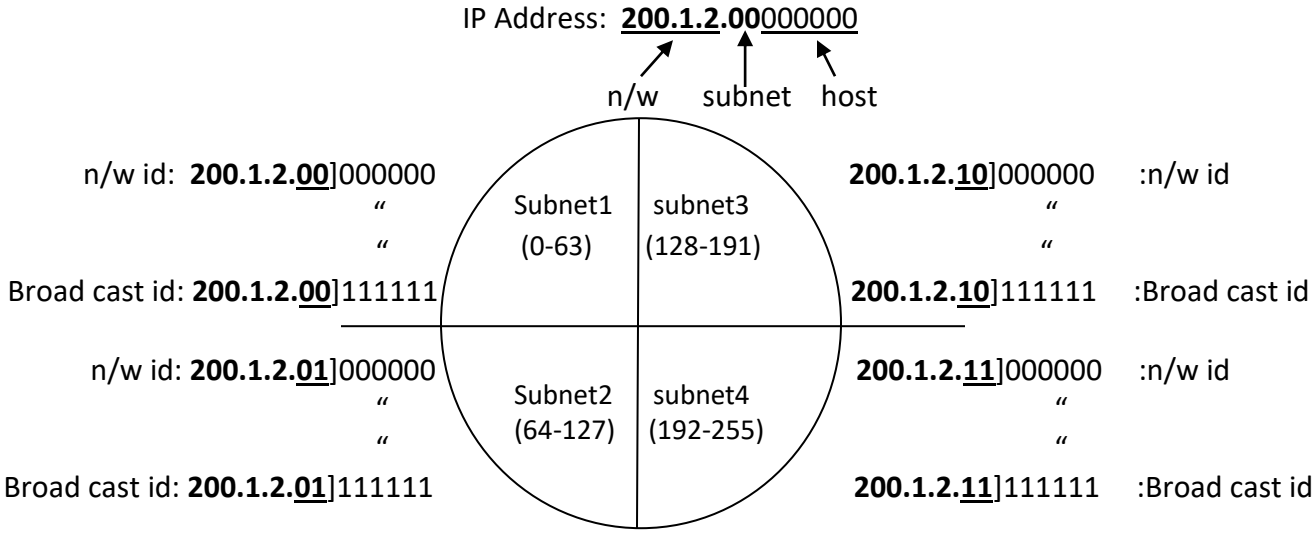
- ✓ The extended network prefix is also called subnet mask.
- ✓ The assignment of subnets is done locally. The entire network still appears as one IP network to the outside world.
- With subnetting, IP addresses use a 3-layer hierarchy:

  Network Subnet Host

- ✓ **Broadcast Transmission:** Transmission of data packets to multiple hosts. **two types.**
  1. **Limited broadcast:** Host of a network transmits data packets to multiple hosts with in the n/w.
  2. **Directed broadcast:** Host of a network transmits data packets to multiple host of different n/w.
- ✓ In broadcast the last IP Address value of network is used as destination IP address(broadcast address) for the entire network.
- ✓ The first value IP address is used for network address.

Creating Subnets in a Network:

- ✓ Consider a class C IP address **200.1.2.0** Last octet (0) represents host address.
- ✓ "The subnet address is created by modifying the bits of last octet".
  - ➢ Assume that the network represented by 200.1.2.0 through 200.1.2.255 needs to be divided into 4 subnets.
  - ➢ The ***number of bits used for subnet identification*** depends on the ***number of subnets*** into which the network is divided. The number of subnets is a power of 2.
  - ➢ Eg:-To create 4 subnets, the number 4 is represented as 2^2. As a result the first 2 bits of the last octet is modified to obtain four subnets.
  - ➢ If ***n*** bits of an octet represent the host address, the maximum number of valid hosts is **2^n-2**
  - ➢ In last octet with all bits as 0 represent the **subnet address**.(eg:-here 200.1.2.0)and 1 represent the **broadcast address for the network**(eg:-200.1.2.255). The first 2 bits of the last octet is modified to obtain four(2^2) subnets.



s.no	Subnet address in dotted-decimal format	Subnet address in binary system
Subnet0	200.1.2.0	11001000.00000001.00000010.00000000
Subnet1	200.1.2.64	11001000.00000001.00000010.01000000
Subnet2	200.1.2.128	11001000.00000001.00000010.10000000
Subnet3	200.1.2.192	11001000.00000001.00000010.11000000

- ✓ Subnet masks are also written in dotted decimal notation, with the addition of a slash followed by the number of bits in the network and subnet part.
- ✓ **Example:** The subnet 200.1.2.0 can also be represented as 200.1.2.0/26, 200.1.2.64/26, 200.1.2.128/26

  26 in last part=Network ID + subnet

  =24 Network ID bits+2 SubnetID bits

SUBNET MASKING:

"***Subnet mask*** is a mask used to determine what subnet an IP address belongs to."

1. **In binary notation:**
   all bits in Network ID
   Subnet ID } is represented by – **1**'s
   Host ID is represented by - **0'**s
2. **In decimal notation**:
   subnet mask value 1 to 255 - network address
   value 0 [Zero] - host address.

→ If we have not subnetted the network, masking extracts the ***network address*** from an IP address.

→ If we have subnetted, masking extracts the ***subnetwork*** address from an IP address.

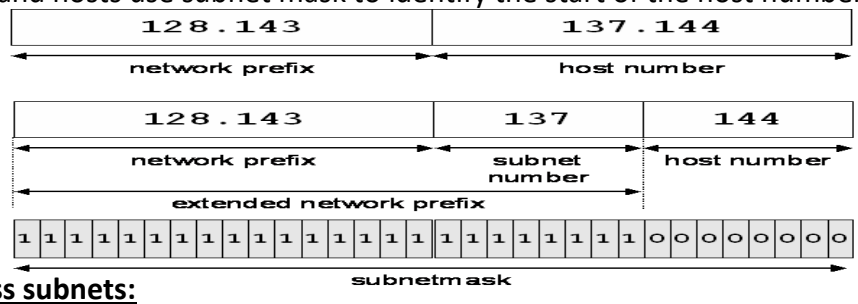
a) Masking without subnetting:

To be compatible, routers use a mask even if there is no subnetting.

Class	Default SubnetMask	Address(Example)	Network Address (Example)
A	255.0.0.0	15.32.56.7	15.0.0.0
B	255.255.0.0	135.67.13.9	135.67.0.0
C	255.255.255.0	201.34.12.72	201.34.12.0

b) Masking with subnetting:

Routers and hosts use subnet mask to identify the start of the host numbers.



Communication across subnets:

- ✓ Hosts in one network does not communicate directly with hosts in another network. So Routers are used.Router determines whether the source and destination hosts are in same subnets. If they are in different subnet, router forwards data to the respective router of that particular network.
- ✓ Router uses AND operation to find in which subnet the host exists.
  - ➢ Consider 200.1.2.0 through 200.1.2.255 is divided into four subnets. We have to communicate to the destination address 200.1.2.130.
  - ➢ In order to communicate, we have *to find its subnet address*

To find the subnetwork address,

1. Convert destination IP Address and subnet mask into binary form.
2. Apply AND operation to them and the result will be the subnet address.

- In subnet mask-all host ID bits is represented by 0's and all NetworkID+subnetID bits by 1's
- As per given example, NetworkID+SubnetID -26 bits(n/w-24,subnet-2) HostID -6 bits.
  Subnetmask for this example is **11111111.11111111.11111111.11000000**

Subnetmask – 1111 1111.1111 1111.1111 1111.1100 0000
Destination IP address -- 1100 1000.0000 0001.0000 0010.1000 0010 } AND

---

subnetaddress - 1100 1000.0000 0001.0000 0010.1000 0000
200 . 1 . 2 . 128

Advantages of Subnetting:

1) Subnetting breaks large network into smaller network because smaller networks are easier to manage.
2) Subnetting reduces network traffic by removing collision and broadcast traffic, that overall improve performance.
3) Subnetting allows you to save money by reducing requirement for IP range.

Subnet considerations:

The following factors are to be for dividing a network into subnets:

1) Number of subnets required(defined by exponent of 2, i.e; $2^{subnetIdbits}$)
2) Number of subnets required in future
3) Number of hosts in the largest network.($2^{hostIDbits}$)

Subnet limitations:

1) Limitation on the number of hosts that can be accommodated in a single subnet.
2) Wastage of host address in subnets.

5.2.4 Classify the Two Types Of Internet Protocol Addressing Ipv4 & Ipv6:

IPv4	IPv6
IPv4 addresses are 32 bit length.	IPv6 addresses are 128 bit length.
IPv4 addresses are binary numbers represented in decimals.	IPv6 addresses are binary numbers represented in hexadecimals.
IPSec support is only optional.	Inbuilt IPSec support.
Fragmentation is done by sender and forwarding routers.	Fragmentation is done only by sender.
No packet flow identification.	Packet flow identification is available within the IPv6 header using the Flow Label field.
Checksum field is available in IPv4 header	No checksum field in IPv6 header.
Options fields are available in IPv4 header.	No option fields, but IPv6 Extension headers are available.
Address Resolution Protocol (ARP) is available to map IPv4 addresses to MAC addresses.	Address Resolution Protocol (ARP) is replaced with a function of Neighbor Discovery Protocol (NDP).
Internet Group Management Protocol (IGMP) is used to manage multicast group membership.	IGMP is replaced with Multicast Listener Discovery (MLD) messages.
Broadcast messages are available.	Broadcast messages are not available. Instead a link-local scope "All nodes" multicast IPv6 address (FF02::1) is used for broadcast similar functionality.
Manual configuration (Static) of IPv4 addresses or DHCP (Dynamic configuration) is required to configure IPv4 addresses.	Auto-configuration of addresses is available.

Need For Ipv6/ Features of IPv6:

1) **Scarcity of IPv4 Addresses:**
   - The IPv4 addressing system uses 32-bit address space. 32-bit address space allows for 4,294,967,296 IPv4 addresses, but Many addresses which are allocated to many companies were not used and this created scarcity of IPv4 addresses.
   - Because of scarcity, many organizations implemented NAT (Network Address Translation) to map multiple private IPv4 addresses to a single public IPv4 address. But NAT also have many limitations. NAT do not support network layer security standards
2) **Larger address space:** An IPV6 address is 128 bit long.
3) **New options:** IPV6 has new options to allow for additional functionalities.

4) **Allowance for extension:** IPV6 is designed to allow the extension of the protocol if required by new technologies or applications.
5) **Security**: It offers built-in support to IPSec (Internet Protocol Security). The encryption and decryption authentication option in IPV6 provide confidentiality of packet.
6) **Supports mobile users:** A user can use the same IP address to connect from different locations.
7) **Supports Anycasting:** Anycasting is used to regulate traffic as well as to increase the speed of accessing web sites.
8) **Built-in support for auto configuration:** IPv6 compatible devices with IPv6 installed on them can create their own IP Address using the MAC address & obtaining the n/w address.
9) **Quality of service (QoS):** Quality of Service (QoS) is available in IPv6 and it relies on the 8 bits of the IPv4 Type of Service (TOS) field and the identification of the payload. IPv4 Type of Service (TOS) field has limited functionality and payload identification is not possible when the IPv4 datagram packet payload is encrypted.

5.2.5 Classful Addressing and Classless Addressing in IPv4:

Classful Addressing in IPv4:

Refer 5.2.2 topic

Classless Addressing in IPv4:

Classless Inter Domain Routing (CIDR):

- ✓ CIDR does not follow the convention of IP address classes. The use of IP address classes results in lots of wasted addresses. The shortage of IP addresses was prevented by CIDR.
- ✓ **Classless Inter Domain Routing** provides the flexibility of borrowing bits of Host part of the IP address
- ✓ "CIDR allows variable number of bits to represent a network address." Therefore, CIDR provides more flexibility in allocating IP addresses for networks than classfull addressing.

Example: CIDR address 132.168.26.32/18.

Here,the first **18 bits** represent- network address

the last **14 bits** represent-host address.

This IP address can't be categorized as class A, class B or class C.

- ✓ CIDR allows allocation of IP addresses that are suited to the actual requirement of the network.

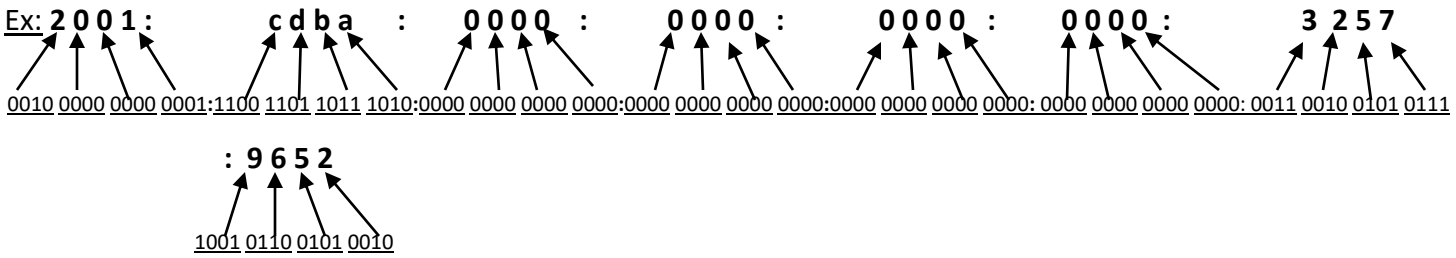
Example: Imagine a network with 32 hosts. Now the network would need to use a class C address, such as 200.1.2.3 and as a result, 223 IP addresses would be wasted. On the other hand, with CIDR address, only the last 5 bits (2^5=32) are allocated for the host addresses. Therefore, a CIDR address such as 200.1.2.3/27 can be assigned to the network.

5.2.6 Internet Protocol Version6 (IPV6):

IPV6 was developed to address the limitations of IPV4. The limitation of IPV4 is that it uses 32-bit addressing. To overcome this space limitation of IPV4, IPV6 uses a 128-bit addressing.

IPV6 (Internetworking Protocol Version6), also known as **IPng** (Internetworking Protocol, next generation) was proposed.

- ✓ IPV6 contains a total of 8 blocks each containing 16 bits.
- ✓ Each block is then converted into 4-digit Hexadecimal numbers separated by colon symbols.
- ✓ Each block is separated by '**:**' symbol:



- The format of IPv6 address is

  xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
- where each x is a hexadecimal digit representing 4 bits or a nibble.
- IPv6 addresses **range** from

  0000:0000:0000:0000:0000:0000:0000:0000 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff.
- An IPv6 address can be simplified by the following two methods.
  1. **Omit leading zeros:** Omit the leading zeros in any 16-bits.

  E**xample:** IPv6 address 2001:0DB8:0000:0000:0022:F376:FF3B:AC99 may be written as

  2001: DB8: 0 : 0 : 22:F376:FF3B:AC99.
  2. **Double colon:** Use double colons (::) in place of a series of zeros.

  Example: The above address can be further simplified as 2001:DB8**::**22:F376:FF3B:AC99.

Types of IPv6 Addresses:

IPv6 addresses are broadly classified into 4 categories:

1. Unicast addresses:

- Unicast is a type of communication where data is sent from one computer to another computer.
- Unicast is a one-to-one type of network communication. Different data streams are generated for each Unicast connection.
- In Unicast type of communication, there is only one sender, and only one receiver.

Example:

1. Browsing a website. (Webserver is the sender and your computer is the receiver.)
2. Downloading a file from a FTP Server. (FTP Server is the sender and your computer is the receiver.)

2. Multicast addresses*:*

- Multicast is a type of communication where multicast traffic addressed for a group of devices on the network.
- IPv6 multicast traffic are sent to a group and only members of that group receive the Multicast traffic.
- IPv6 Multicast Groups are identified by IPv6 Multicast Addresses.

3. Anycast addresses:

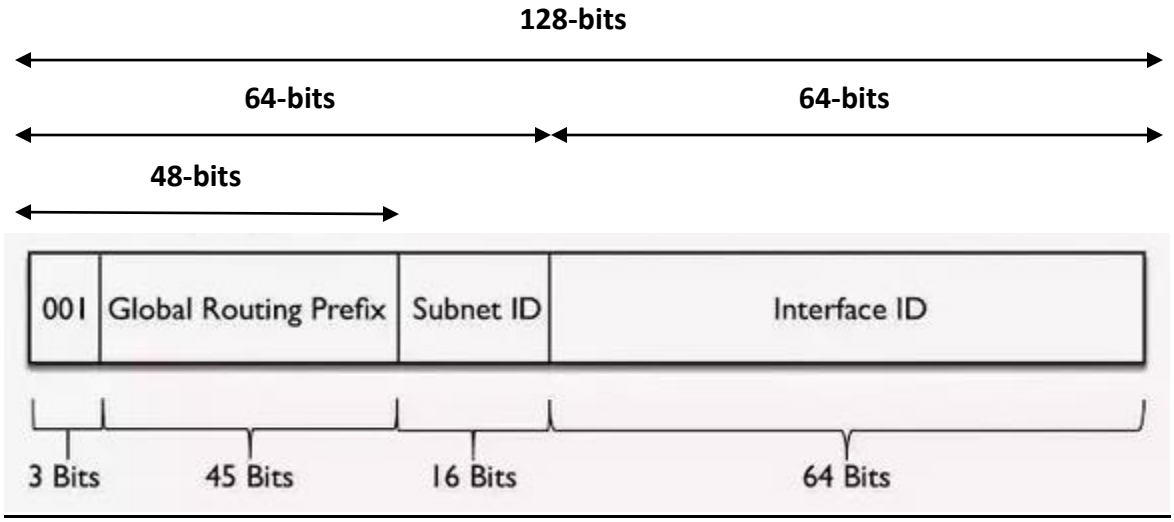
- Anycast is a type of IPv6 network communication in which IPv6 datagrams from a source are routed to the nearest device (in terms of routing distance) from a group servers which provide the same service. Every nodes which provide the same service are configured with same Anycast destination address.

4. Loopback:

- Used by a node to send an IPv6 packet to itself. An IPv6 loopback address functions the same as an IPv4 loopback address. The IPv6 loopback address is 0000:0000:0000:0000:0000:0000:0000:0001/128, which can be also represented as ::1.

Unicast addressing:

1. An IPv6 unicast address is used to identify a single interface in a node. Also called Global unicast address.
2. An IPv6 Unicast address identifies only one node in networks. Global Unicast Addresses are similar to IPv4 public addresses.
3. Global Unicast Addresses are globally routable addresses on IPv6 Internet.
4. RFC 3587 states that out of the 128 bits in IPv6 addresses, left most three bits are must be fixed as 001.
5. Remaining 45 bits are reserved for global **routing prefix** (n/w address). 16 bits after that can be used for **subnetting** and the 64 remaining bits are the **host bits**.
6. The first fixed three bits (001) and the 45-bit global routing prefix (45+3 = 48 bits) together can be assigned to an organization as their IPv6 prefix.
7. Since the leftmost three bits are reserved as "001" for Global unicast IPv6 addresses, the range of Global Unicast Addresses available now are from 2000 to 3FFF, as shown below.



- The prefix is the part of the IPv6 address that indicates the network.
- Which means that, currently first 48 bits of an IPv6 address are used to identify the network globally.
- The next 16 bits are used for subnetting (which makes 48+16=64 bits, network part) and the remaining 64 bits are used for identifying the hosts (host part).

Multicast Addressing:

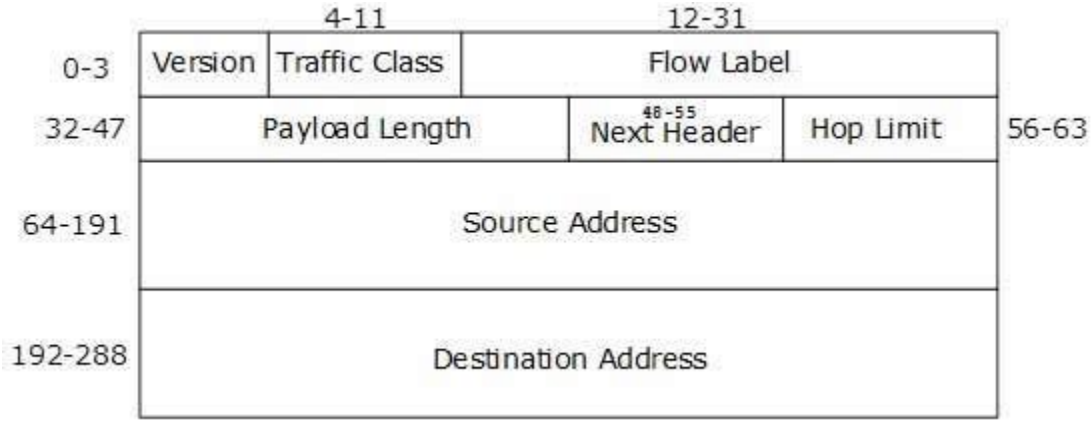
- A IPv6 multicast address identifies multiple interfaces.
- A multicast transmission sends packets to all interfaces that are part of a multicast group.

FF02::1	All nodes on the local network segment
FF02::2	All routers on the local network segment

Anycast Addressing:

- Anycast type of IPv6 addresses can be used only as destination addresses.
- Anycast type of IPv6 addresses are typically assigned only to IPv6 routers. Anycast addresses are from IPv6 unicast address range.

IPv6 header format:



- **Version** (4-bit)- version number of Internet Protocol = 6.
- **Traffic class** (8-bits)-It is used for Type of Service to let the Router Known what services should be provided to this packet.
- **Flow label** (20-bit field) - This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information.
- **Payload length** (16-bits)-This field is used to tell the routers how much information a particular packet contains in its payload
- **Next header**(8-bits)-Identifies the type of header that immediately follows the IPv6 header. Uses the same values as the IPv4 protocol field.
- **Hop limit**(8-bits)-This field is used to stop packet to loop in the network infinitely.
- **Source address**(128 bits.)-The address of the initial sender of the packet.
- **Destination address**(128 bits-The address of the intended recipient of the packet

5.3 State the Need for Protocols in Computer Networks:

Protocol:

"Protocol is a set of rules that governs the communication between computers on a network"

- Source node sending the data to destination node, sending node should provide the address of the destination node. This addressing and transmission of data between computers on a n/w is handled by 'Network Protocols'.

Need:

→ **Addressing method used by the devices:**
The computers can address each other by their names or by the address assigned to each computer.

→ **Data format:**
Computers and devices should send & receive data in a format that can be understood by one another.

→ **Reliability of data transfer:**
n/w protocols ensure that data transfers on a n/w are reliable.

→ **Speed of communication:**
n/w protocols play an important role in determining the speed of data transfer on the n/w.

→ single protocol that cannot manage all these tasks. Therefore, different protocols have been developed to operate at various layers of the OSI model.

→ Protocols at **Transport Layer:** ensure reliable transmission of data on the network.

→ Protocols at **Network Layer:** protocols are responsible for addressing data to computers on a n/w.

→ Protocols at **Application, Session, Presentation layers:** determine the kind of data that is accessible to users and manner of accessing the data.

5.4 Know About Protocols:

Higher Layer Protocols operate at session, presentation and application layers of OSI Reference model. These protocols provide users an interface to access data.

The common higher-layer protocols are:

1. HTTP
2. FTP
3. SMTP
4. TELNET

5.4.1 HTTP(Hyper Text Transfer Protocol):

- ✓ HTTP is a protocol used to access data on the World Wide Web (WWW).
- ✓ HTTP uses TCP for transmission of data between the user's computer and the web site. HTTP uses port number 80 of TCP.
- ✓ When a user type the URL (Uniform Resource Locator) of a web site in the web browser's address bar, an HTTP request is generated.
- ✓ The browser is an HTTP client, and requests of HTTP clients are handled by the HTTP server.
- ✓ A **web server** is a computer on which the files of a particular web site are located. Once the HTTP server accepts the client request, the user can view the web page in the browser.
  This request- response model is governed by a protocol called HTTP.

FIG:Interaction between a web browser and a web server.

Interaction between a web browser and a web server: -

The following steps describe the interaction between a web browser (the client) and a web server (the server) as follows:

1. The user on the client computer types the URL.
   Ex: - http://www.yahoo.com/index.html
   http - protocol
   www.yahoo.com-domain name
   index.html - file name
2. The browser request DNS for the IP address corresponding to www.yahoo.com
3. DNS replies with the IP address for www.yahoo.com for ex: 120.10.23.21
4. The browser makes a TCP connection with the computer 120.10.23.21 (which is a yahoo server)
5. The browser then sends over a request asking for file/index.html.
6. The www.yahoo.com server sends the file /index.html.
7. The TCP connection is released.
8. The browser displays all the text in/index.html.

- ✓ HTTP uses TCP, which ensures that the data transfer between the two connected computers is reliable.
- ✓ HTTP is stateless protocol, which means that the connection between the two computers is terminated as soon as data transfer ends
- ✓ To ensure secure transmission of data over the internet, HTTPS (HTTP over secure socket layer) was introduced. HTTP encrypts all the data that travels over the internet so that data is not read by unauthorized users. The data is decrypted by the web server so that information is read only by the web server.

HTTP commands: HTTP protocol uses these commands when a client requests a server for a web page.

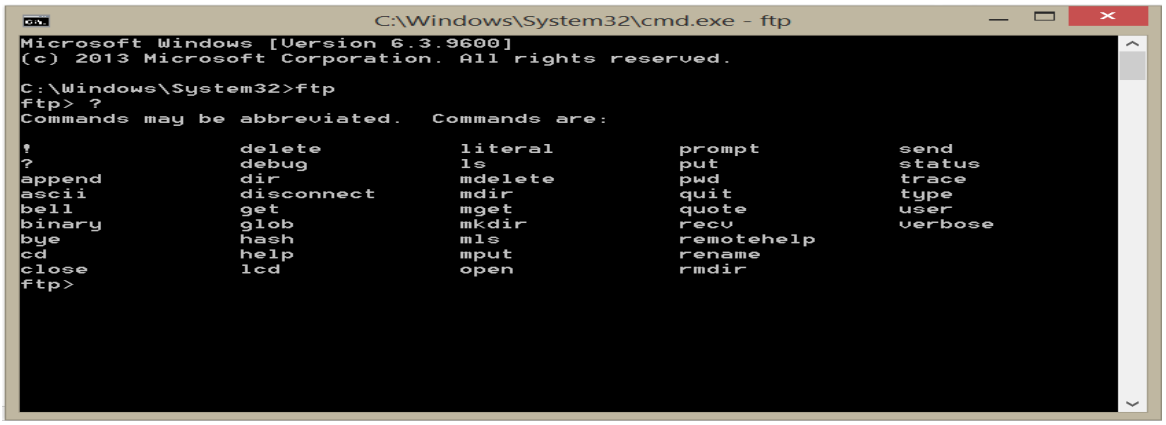
HTTP command	DESCRIPTION
GET	sends a request for a webpage.
HEAD	requests the server to read the header of a web page.
PUT	requests the server to store a web page.
POST	similar to PUT, but is used for updating a web page.
DELETE	deletes a web page.
LINK	connects two pages by hyperlinks.
UNLINK	disconnects two pages by hyperlinks.

5.4.2 File Transfer Protocol (FTP):

- ✓ FTP is a protocol designed to handle file transfers between two computers over the network.
- ✓ To use FTP for transferring files, we need client and server.
- ✓ An FTP server is a computer on which FTP is installed and contains the files to be copied or downloaded.
- ✓ An FTP client is a computer that downloads files from the FTP server.
- ✓ When the FTP client requests access to an FTP server, the server authenticates the client with the help of username and password.
- ✓ The Microsoft windows OS includes a default FTP client software to connect to FTP server.

To access an FTP server on a computer running windows 9x/ME/2000/XP, perform the following steps:

1. Click **start, run** and Type **cmd**, and click OK



2. Type **FTP,** and press enter. The command prompt changes to FTP, indicating that the default FTP client software is private.
3. Type **open demo.wftpserver.com** and press enter.
4. Now you are connected to the FTP server of the web site. You will be asked to enter the user name: **demo-user** and password: **demo-user.**
5. Once authenticated, you can access the files on the web site using "**get** filename**"**

Note: - "open" is an FTP command to connect to an FTP server.

.

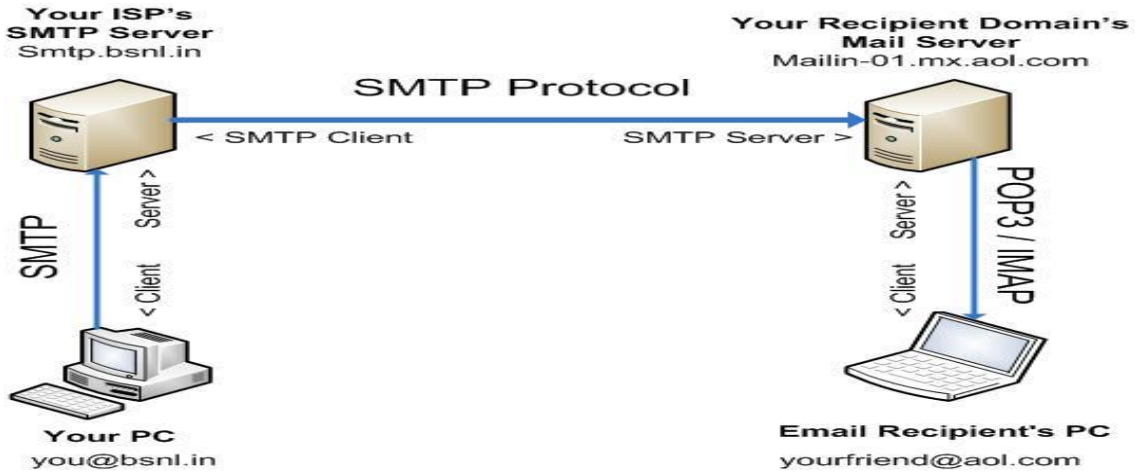
5.4.3 SMTP (Simple Mail Transfer Protocol):

- ✓ SMTP is a protocol is used for sending and receiving email messages between two computers on a network. It uses TCP/IP protocol.
- ✓ SMTP transfers the email messages from the SMTP server of the sender to the SMTP server of the receiver. SMTP is a push protocol.
- ✓ Address used by SMTP consists of 2 parts:
  a)Mailbox name. b)Mail server name(Domain name)

Ex: poly@gmail.com in this email address, **poly**-mailbox name, and **gmail.com**-mail server name.

- ✓ A network on which SMTP is installed is called an SMTP server.

- ✓ It performs the following steps:
  - At the sender's end, an SMTP server takes the message sent by a user's computer.
  - The SMTP server at the sender's end then transfer the message to the SMTP server of the receiver.
  - The SMTP server at the recipient's end than takes the email message and gives it to the POP server at the receiver's end.



  - When a user sends an e-mail it reaches the **SMTP server**. The SMTP server breaks the destination email address into the mailbox name and the domain name, and delivers these messages to the SMTP server and stores them separately depending on the mailbox name.
  - To transfer mails from the mail server to a different computer, a protocol such as POP/IMAP is used. POP3/IMAP4 are pull protocols.

POP3(Post Office Protocol):

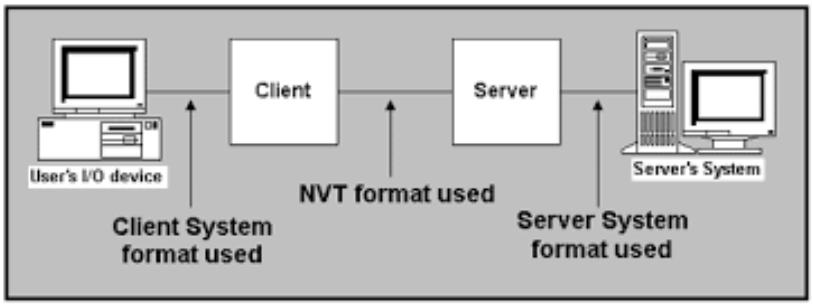
- POP3 is used for fetching emails from a mail server to a user's computer.
- **Advantages:**
  - ✓ The ability to read and modify mails without remaining connected to the internet is the main advantage.
  - ✓ Mailboxes present on the server usually have limited storage space, leaving all the e-mails on the server may take up a significant portion of the disk space on the server. These problem can be prevented by continuously retrieving mails from the server.
- **Disadvantages: -**
  - ✓ All e-mail messages are downloaded on to a single computer and therefore, a user can access the mail from the same computer.
  - ✓ As e-mails stored in a single computer, a virus attack may arise all data.

IMAP4(Internet Message Access Protocol):

- Allows users to download email messages from a mail server to a local computer.
- IMAP always maintain a copy of the email messages on the mail server, unless the user explicitly deletes them.
- **Advantages:**
  -Allows users to access multiple mailboxes simultaneously.
  -Allows users to create customized mailboxes on mail server.
  -Allows users to access e-mails from multiple locations.
- **Disadvantages:**
  -Message storage is limited.
  -Reading messages while offline requires use of your e-mail programs in Offline mode.

5.4.4 TELNET (Remote Login):

- ✓ TELNET stands for **TErminaL NETwork.**
- ✓ The TELNET PROTOCOL allows remote login services, so that a user on a client computer can connect to a server on a remote system.
- ✓ TELNET has two parts:
    1. client
    2. server
- ✓ When a user want to access an application program located on a remote machine, he or she performs remote login.
- ✓ The user sends the keystrokes to the terminal driver where the local operating system accepts the characters but does not interpret them.



- ✓ The characters are sent to the TELNET client, which transforms the characters to a universal character set called **Network Virtual Terminal(NVT)** Characters and delivers them to the local TCP/IP stack.
- ✓ The commands or text in NVT form travel through the Internet and arrive at the TCP/IP stack at the remote machine.
- ✓ The characters are passed to the TELNET server which changes the characters understandable by remote machine; the characters are then passed to the *pseudoterminal driver* which pretends that the characters are coming from a terminal.
- ✓ The operating system then passes the characters to the appropriate application program

5.5 Overview of Network Management:

Network Management:

"Network management means managing computer networks involves monitoring and controlling various network devices, such as computers, hubs, routers, switches and cables."

To ensure smooth functioning of a network, you need to prevent problems that may affect the performance of a network. By preventing such problems, you can operate the network at peak performance. The administrator should be in a position to detect such problems and troubleshoot them. The common problems encountered in a network are non-optimum or over utilization of bandwidth, network intrusion by unauthorized sources, and device or link (cable) failures.

The reliable and timely transfer of data over a network is an area of concern for any organization that uses a computer network. Any loss or delay of critical data may affect the activities of the organization. For example, imagine an organization with offices in Miami, Chicago, and New York City.

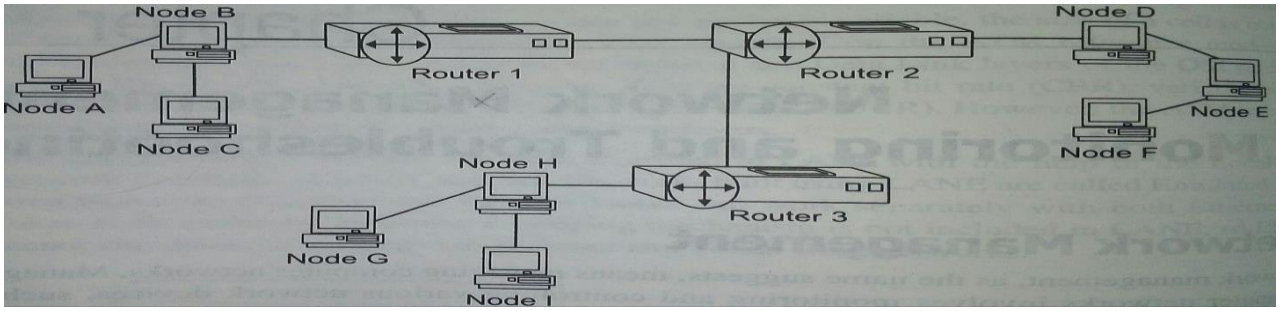


Figure: **Networks Connected with Routers**

- If a router fails, the communication between the offices is affected.
- Therefore, the administrator at each office needs to ensure the proper functioning of devices, such as Network Interface Cards (NICs), repeaters, hubs, switches, and routers.
- if a device failure can also result in unnecessary traffic on the network

Example: Imagine that Node A sends data to Node D. on receiving data, Node D acknowledges the receipt. However, if node D is down, then it cannot receive the data, and therefore, cannot send the acknowledgement of data to Node A. in the case, Node A assumes that Node D has not received the data and resends it. This increases the network traffic and can affect the performance of the network.

There may be several other possibilities that may affect network performance. Therefore, the administrator needs to perform certain tasks to manage the network.

Administrator tasks:

- **Creating proper documentation of the network configuration**: This documentation should include detailed on the past, current, and proposed network configurations, which helps in understanding the network layouts and proposed scalability.
- **Using hardware and devices that alert the administrator when failure in the network occurs**: The common tools that alert administrators about and assisting recovering from a network failure are protocol analyzers and cable testers.
- **Using network management protocols**: such as Simple Network Management Protocol (**SNMP)**, Common Management Information Protocol (**CMIP)**, and Remote Monitoring (**RMON)**. These protocols and tools detect and notify administrators about network problems.
- **Collecting periodic information pertaining to the network**: The information should help in:
  - Identifying bottlenecks that slow down the network.
  - Identifying hardware and software requirements for future upgrades.
  - Measuring network performance using graphs and predicting future network performance.
- **Controlling and providing data security by assigning appropriate permissions to user accounts:** This avoids access to sensitive data and resources on the network for unauthorized users.
- **Controlling and reducing the cost involved in operating the network.**

5.6 ISO Network Management Model:

The ISO network management model helps in standardizing the activities for managing network. This model identifies a set of areas where network management is required. These areas include configuration management, fault management, performance management, security management, and accounting management.

components:

Configuration Management
Fault Management
Performance Management
Security Management
Accounting Management

Figure 8.2: **ISO Network Management Model.**

1. Configuration management:

Configuration management is concerned with the process of **collecting information related to the configuration of different devices** when the network is designed. It helps in identifying the effects of various versions of hardware and software that are running on the network. For example, imagine that ten computers, such as the operating system or the protocol supported by the NIC, to select an appropriate protocol for the network.

This configuration information helps the administrator plan in case of changes in network requirements in the future.

2. Fault Management:

Fault Management is concerned with the monitoring of network devices. The administrator must be aware of any device or link failures in the network. In addition, the data transferred between devices may be corrupt due to a virus or a corruption of protocols used on the network.

Methods:

- → **To track and manage network operation**, a Network Management System (NMS), which is a combination of hardware and software, is used.
- → **To monitor network devices, protocols** such as SNMP and RMON are used.
- → **To monitor network traffic**, a protocol analyzer, which is a combination of hardware and software, is used.
- → **To identify cable faults in the network**, a hardware device such as a cable tester is used.

3. Performance Management

Performance Management is concerned with the **process of collecting and analyzing data from the network components**. After analyzing the data, the administrator matches the data against the *thresholds* or *benchmarks* that are set for the network. a benchmark is a condition against which the performance of the network is measured.

4. Security Management

Security Management is concerned with the steps involved in **assuring the security of data and devices on the network**. With the help of security management, the administrator can control unauthorized access of network resources by granting access permissions.

Example: the administrator can permit a certain user to only read a file, while permitting other users to read/modify the file.

5. Accounting Management

Accounting Management is concerned with the **cost required to operate a network** so that individual or group uses on the network can be regulates appropriately.

Example: imagine two networks connected to each other through routers. When data is from one network to another, the administrator should decide how the data travels after reaching the router on the other network. The administrator or the router decides the number of hops it takes to send the data. The path with the least number of hops is the lowest cost path and reduces the operational cost of the network.

5.7 Network Monitoring and Troubleshooting:

These protocols are used in managing a network. The network management protocols covered are SNMP and RMON.

5.8 Simple Network Management Protocol (SNMP):

- SNMP is a network management protocol that facilitates the exchange of management information between network devices.
- SNMP enables the administrator to detect, manage, and troubleshoot network problems and helps in planning network growth.
- Initially this protocol was developed to monitor and troubleshoot network devices, such as routers and bridges from a computer, usually the network server.
- However, SNMP can monitor and provide status information between computers running windows 2000, routers and gateways, mainframe computers, terminal servers, and writing hubs,.

SNMP components:

- SNMP manager
- SNMP agent

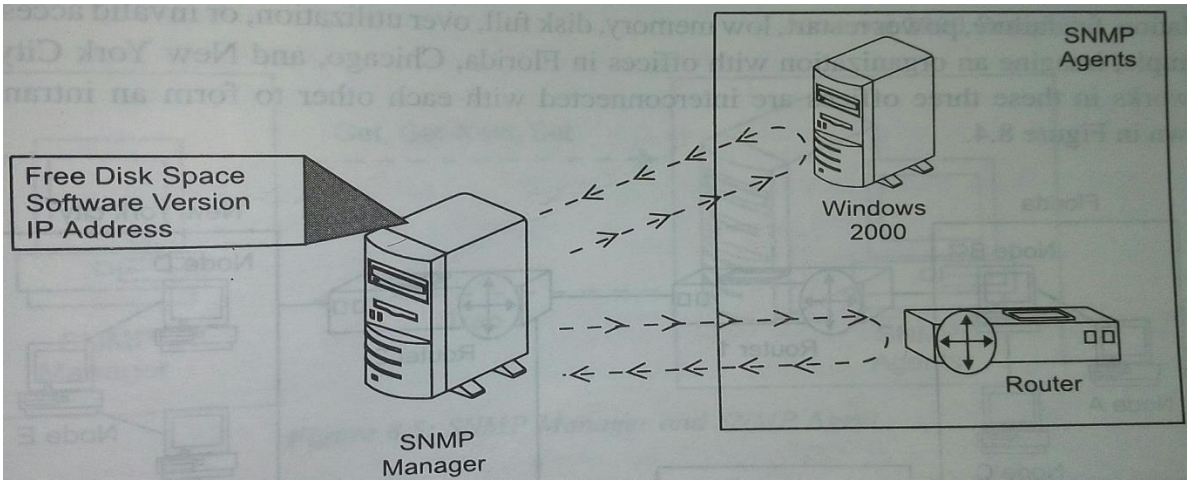


Figure: SNMP manager and agent

- this figure shows The information is retrieved with the help of **messages.**
- The information provided by the SNMP agents can include: free disk space, software version running on the SNMP agents, and the IP addresses of the SNMP agent.

1. **SNMP Manager:**
   - ✓ The computer on which the SNMP management software is installed is called the SNMP manager.
   - ✓ It is also called the SNMP management System or server component.
   - ✓ The SNMP server queries the SNMP agent on the device for the required information.
   - ✓ The SNMP agent sends critical alarms of events to the SNMP server.
   - ✓ The time interval at which the information is sent to the events to the SNMP manager is defined at the time of configuring SNMP.
   - ✓ SNMP uses different messages that help the SNMP manager to communicate with SNMP agents.
   - ✓ The messages are **Get, Get – Next, Set, and Trap**.
   - ✓ The Get and Get – Next messages: enable the administrator to retrieve information about the managed devices, such as computers, routers, bridges, and hubs, on the SNMP based network.
   - ✓ The Set message: enables the administrator to change the values, such as free disk space and utilization in the Management Information Base (MIB).
   - ✓ A MIB is used to store the properties of managed devices.

- ✓ The Trap message: alerts the administrator about events in the remote computer, such as password violation, fan failure, power restart, low memory, disk full, over utilization, or invalid access.

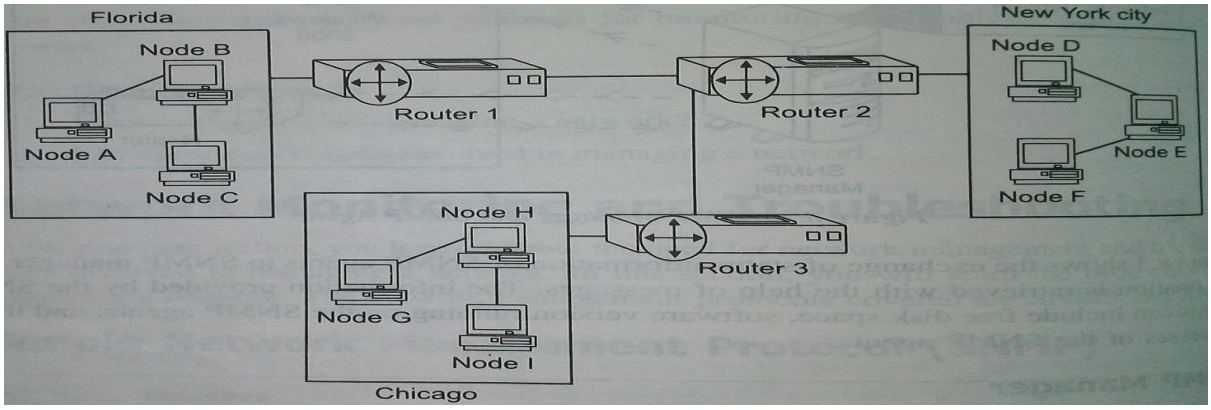


Figure: Networks Connected with Routers

2. SNMP Agent:

- ✓ The SNMP agent is **software** installed and configured on a managed device that runs on the SNMP based network.
- ✓ The SNMP agent contains a database called **MIB**.
- ✓ The information about the managed device is stored in the MIB.
- ✓ The managed device collects the network management information from MIB database and makes it available to the server using the SNMP agent.

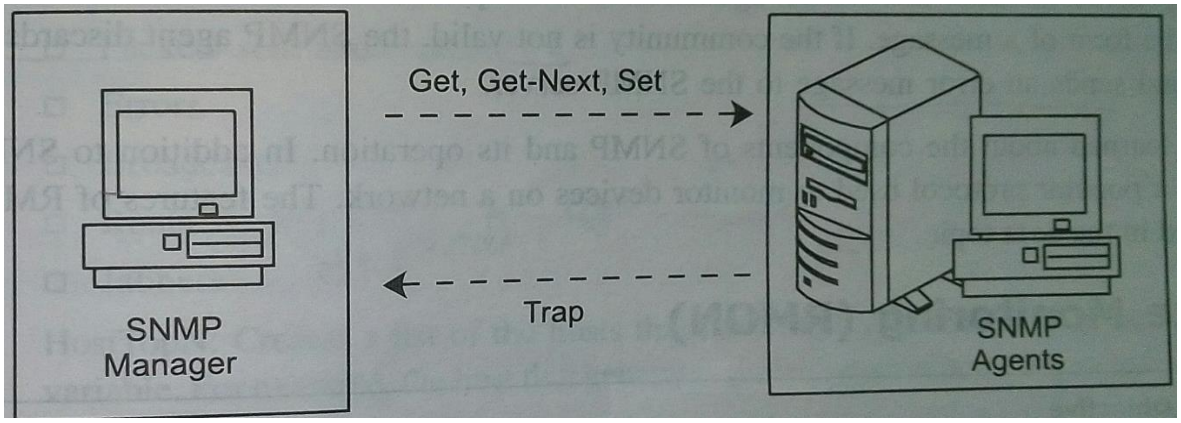


Figure: SNMP Manager and SNMP Agent

Figure shows the Get, Get – Next, and Set messages. These messages help the administrator to retrieve information about the managed devices, such as computers, routers, bridges, and hubs, on the SNMP based network. Similarly, the Trap message alerts the administrator about any violation that occurs on the SNMP agent.

5.9 How SNMP Works:

1. The SNMP server and the SNMP agent communicate and check the host information using SNMP messages.
2. The Get, Get – next, Set, and Trap messages help in carrying out the working of SNMP.
3. These messages are sent using the **User Datagram Protocol (UDP).** The **Internet Protocol (IP)** is used for routing the SNMP message between the SNMP manager and SNMP agent.

4. The SNMP manager sends a message to the SNMP agent to get certain information about the managed device running on the SNMP based network.
5. The information could be about the type of protocols, about the version of the managed device, or about the available hard disk space.
6. This information is stored in a MIB, which helps the administrator to manage the network
7. The message sent from the server to the SNMP agents contains community name, defined as a group of SNMP agents. The grouping of SNMP agents helps in the process of administration.
8. On receiving the SNMP message, the SNMP agent validates the *community name*.
9. if the community name is valid, the SNMP agent sends the requested information to the SNMP server in the form of messages.
10. if the community name is not valid, the SNMP agent discards the message and sends an error message to the SNMP server.

5.10 Remote Monitoring (RMON):

RMON, a protocol based on the MIB and which is used by SNMP, helps in monitoring network faults. After installing RMON, the administrator can monitor the flow of data packets on the network and can generate the summary of data traffic on the network.

RMON also helps the administrator perform real-time monitoring of data over the network. By installing RMON on the LAN, the administrator can monitor the data locally on the **probe**, which is a network device that analyzes RMON information, can monitor traffic and set off an alarm when a certain condition occurs. It can be used to periodically audit traffic and gather statistics sent to the management console. RMON probes are often placed permanently in to networks. There are nine groups available with RMON.

There are 9 Groups in RMON:

1. **Statistics:** Contains information such as packets dropped, packets sent, and packets broadcast by each device on the network.
2. **History:** provides a summary of each device on the network.
3. **Alarm:** stores the threshold values of the network device. An alarm or a message is sent to the administrator if the value collected in the form of information exceeds the threshold value.
4. **Host:** stores the traffic statistics of each host on the network. The information includes:
   - Packets sent and received
   - Errors
   - Broadcasts
   - Runts
   - Jabbers
5. **Host Top N:** Creates a list of the hosts that the highest values for some measured variable. For example, the host that generates the highest traffic or errors on the network.
6. **Matrix:** stores the source and the destination address of each device on the network.
7. **Packet – capture:** captures all the packets on the network.
8. **Filter:** filters the packets that are captured.
9. **Events:** controls the events that are sent to the server on the network.

Network security:

Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats. A network security system usually consists of many components.

Network security components often include:

- Anti-virus and anti-spyware
- Firewall, to block unauthorized access to your network
- Intrusion prevention systems (IPS), to identify fast-spreading threats, such as zero-day or zero-hour attacks
- Virtual Private Networks (VPNs), to provide secure remote access

Need for Network Security:

- The easiest way to protect a network from an outside attack is to close it off completely from the outside world. A closed network provides connectivity only to trusted known parties and sites; a closed network does not allow a connection to public networks.
- Because they have no Internet connectivity, networks designed in this way can be considered safe from Internet attacks.

Routing Table

✓ A routing table typically contains the path information for data packets to reach a particular internetwork. The routing table also contains a default path, which is used when no path information is available to reach a particular internetwork.

the following information is stored in a routing table:

- **Network ID:** The network ID is the network address of a particular internetwork, or a node address of a particular internetwork.
- **Subnet mask:** The subnet mask is a 32-bit value used to distinguish one network from another.
- **Gateway address:** This field contains either the physical or network layer address of the node or network to which the data packets are to be forwarded.
- **Interface:** The interface is the port that is used to forward data packets.
- **Metric:** The value of metric is proportional to the cost of the route. The cost of the route is calculated considering factors such as number of hops, delay, bandwidth or throughput, and reliability. A low metric value indicates a low-cost path, so the path with the lowest metric value is preferable.

Table: contents of Routing Table

Network ID	Net mask	Gateway Address	Interface	Metric
172.17.128.0	255.255.0.0	172.17.128.119	172.17.128.119	1

The nodes use any of the following methods to build a routing table:

- **Static routing table:** The network administrator manually provides the nodes with a list of available routers, and information regarding the routers to be selected to reach a particular network.
- **Dynamic routing table:** Network layer protocols allow routers to periodically update the routing table of the nodes or routers with new routing information present in the routing table of the router.
- **Default gateway:** This is the address to which data packets are forwarded by the nodes or routers when no specific route is found by the node or router in its routing table

→On the other hand, routers build the routing table by a process known as advertising.

Every time a new router is added to a network, the router sends information on its address, and the networks connected to it, to all the routers in the network. this is called advertising. Routers continue to advertise information at periodic intervals.