RGPVNOTES.IN

Program : **B.E**

Subject Name: **Advance Computer Networks**

Subject Code: **CS-8004**

Semester: **8th**

Advance Computer Networks
Subject Notes: UNIT-III

 # Introduction to Router

A Router is a computer, just like any other computer including a PC. Routers have many of the same hardware and software components that are found in other computers including:

- CPU
- RAM
- ROM
- Operating System

1. Router is the basic backbone for the Internet.
2. The main function of the router is to connect two or more than two network and forwards the packet from one network to another.
3. A router connects multiple networks. This means that it has multiple interfaces that each belong to a different IP network. When a router receives an IP packet on one interface, it determines which interface to use to forward the packet onto its destination.
4. The interface that the router uses to forward the packet may be the network of the final destination of the packet (the network with the destination IP address of this packet), or it may be a network connected to another router that is used to reach the destination network.

#Configuring a Router

1. Find the IP address of the router. If this is a new installation or new router, determine the default IP address that may be printed on a label affixed to the router or in the documentation. If you can't find the router's IP address anywhere, you can do a web search for the router model to see what the default address is.
2. IP addresses are formatted as four groups of up to three digits, separated by periods.
3. Commonly found "default" Local IP addresses for routers are 192.168.0.1, 192.168.1.1, 192.168.2.1, 10.0.0.1. Note that all the addresses in the follow ranges: 192.168.0.0 - 192.168.255.255, 172.16.0.0 - 172.31.255.255 & 10.0.0.0 - 10.255.255.255 have been set aside for exclusive use in a LAN; and one address in the range of any of them of them would be assigned to the connected router.
4. Open a web browser on the computer that is connected to the router. Enter in the IP address of the router into the address bar and press Enter. Your browser will attempt to connect to the router's configuration menu.
5. Enter your username and password. In order to access the configuration page, you will need to be on the router's IP address and enter a valid username and password at the prompt. Most routers have a basic account set up that you will need to use to log on. This varies from model to model, but should be printed on the router or in the documentation.
6. The most typical username is "admin".The most typical passwords are "admin" and "password".
7. Many routers will only require a username and a blank password, and some allow you to leave all fields blank.
8. Enter a name for your wireless network. In the Wireless section, you should see a field labeled SSID or Name. Enter a unique name for your wireless network. Check the box to enable SSID broadcast. This will essentially "turn on" the wireless network so that it may be readily seen by anyone in range of the signal.
9. Choose a security method. Choose from the list of available security options. For the best security, choose WPA2-PSK as the encryption method. This is the most difficult security to crack, and will give you the most protection from hackers and intruders.
10. Create a passphrase. Once you've chosen your security method, enter in a passphrase for the network. This should be a difficult password, with a combination of letters, numbers, and symbols. Don't use any passwords that could be easily deduced from your network name or from knowing you.

11. Save your settings. Once you are finished naming and securing your wireless network, click the Apply or Save button. The changes will be applied to your router, which may take a few moments. Once the router has finished resetting, your wireless network will be enabled.
12. Change your router's username and password from the default. Once you have your network configured, you should change the username and password that you use to access your router. This will help protect your router from unauthorized changes. You can change these from the Administration section of the router configuration menu.
13. Block sites. If you want to prevent devices that are connected to your network from accessing certain websites, you can use built-in blocking tools to restrict access. These can be found in the Security/Block section of the router.
14. You can usually block by specific domain names, or by keywords.

#Interior protocols:

1. Autonomous system's routing is handled by Interior Gateway Protocols. Autonomous System (AS) is a collection of routers that share same routing table information. AS is a boundary line for routing protocol.
2. It could be your company, or group of companies. It is defined by a numeric value.
3. Switching from places to places between the routers, figure out.
4. The protocols are utilized to keep track of getting between destinations to other side of a network or to administrate the networks.
5. These protocols perform the communication between networks.

IGP's fall into two categories:

a) Distance Vector Protocols
   1. Routing Information Protocol (RIP)
   2. Interior Gateway Routing Protocol (IGRP)

b) Link State Protocols
   1. Open Shortest Path First (OSPF)
   2. Intermediate System to Intermediate System (IS-IS)

#Exterior protocols:

1. They are used for internet.
2. They handle the routing outside the autonomous system.
3. They are used by companies where there is more than one internet provider which allows it to have redundancy and load balancing.

Examples of an EGP:

1. Border Gateway Protocol (BGP)
2. Exterior Gateway Protocol (Replaced by BGP)

#Routing Information Protocol (RIP) Researchers developed Routing Information Protocol in the 1980s for use on small- or medium-sized internal networks that connected to the early Internet. RIP is capable of routing messages across networks up to a maximum of 15 hops.

RIP-enabled routers discover the network by first sending a message requesting router tables from neighboring devices. Neighbor routers running RIP respond by sending the full routing tables back to the requestor, whereupon the requestor follows an algorithm to merge all of these updates into its own table. At scheduled intervals, RIP routers then periodically send out their router tables to their neighbors so that any changes can be propagated across the network.

#Open Shortest Path First (OSPF) Open Shortest Path First was created to overcome some of its limitations of RIP including:

- 15 hop count restriction
- Inability to organize networks into a routing hierarchy, important for manageability and performance on large internal networks

- Significant spikes of network traffic generated by repeatedly re-sending full router tables at scheduled intervals.

OSPF is an open public standard with widespread adoption across many industry vendors. OSPF-enabled routers discover the network by sending identification messages to each other followed by messages that capture specific routing items rather than the entire routing table. It is the only link state routing protocol listed in this category.

#Distance Vector Routing –

1. The distance-vector routing Protocol is a type of algorithm used by routing protocols to discover routes on an interconnected network. The primary distance-vector routing protocol algorithm is the Bellman-Ford algorithm. Another type of routing protocol algorithm is the link-state approach.
2. Routing protocols that use distance-vector routing protocols include RIP (Routing Information Protocol), Cisco's GRP (Internet Gateway Routing Protocol), and Apple's RTMP (Routing Table Maintenance Protocol). The most common link-state routing protocol is OSPF (Open Shortest Path First). Dynamic routing, as opposed to static (manually entered) routing, requires routing protocol algorithms.
3. Dynamic routing protocols assist in the automatic creation of routing tables. Network topologies are subject to change at any time. A link may fail unexpectedly, or a new link may be added. A dynamic routing protocol must discover these changes, automatically adjust its routing tables, and inform other routers of the changes.
4. The process of rebuilding the routing tables based on new information is called convergence. Distance-vector routing refers to a method for exchanging route information. A router will advertise a route as a vector of direction and distance.
5. Direction refers to a port that leads to the next router along the path to the destination, and distance is a metric that indicates the number of hops to the destination, although it may also be an arbitrary value that gives one route precedence over another. Inter network routers exchange this vector information and build route lookup tables from it.
6. Distance vector protocols are RIP, Interior Gateway Routing Protocol (IGPR).
7. Algorithm where each router exchanges its routing table with each of its neighbours. Each router will then merge the received routing tables with its own table, and then transmit the merged table to its neighbours. This occurs dynamically after a fixed time interval by default, thus requiring significant link overhead.

a. Routing Method - Distance-Vector Type

8. There are problems, however, such as:
9. If exchanging data among routers every 90 seconds for example, it takes 90 x 10 seconds that a router detects a problem in router 10, routers ahead and the route cannot be changed during this period.
10. Traffic increases since routing information is continually exchanged.
11. There is a limit to the maximum amount of routing information (15 for RIP), and routing is not possible on networks where the number of hops exceeds this maximum.
12. Cost data is only the number of hops, and so selecting the best path is difficult.
13. However, routing processing is simple, and it is used in small-scale networks in which the points mentioned above are not a problem.

#Border Gateway Protocol

BGP (Border Gateway Protocol) is protocol that manages how packets are routed across the internet through the exchange of routing and reach ability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider. Traffic that is routed within a single network AS is referred to as internal BGP, or iBGP. More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or eBGP.

BGP offers network stability that guarantees routers can quickly adapt to send packets through another reconnection if one internet path goes down. BGP makes routing decisions based on paths, rules or

network policies configured by a network administrator. Each BGP router maintains a standard routing table used to direct packets in transit. This table is used in conjunction with a separate routing table, known as the routing information base (RIB), which is a data table stored on a server on the BGP router. The RIB contains route information both from directly connected external peers, as well as internal peers, and continually updates the routing table as changes occurs. BGP is based on TCP/IP and uses client-server topology to communicate routing information, with the client-server initiating a BGP session by sending a request to the server.

BGP sends updated router table information only when something changes -- and even then, it sends only the affected information. BGP has no automatic discovery mechanism, which means connections between peers have to be set up manually, with peer addresses programmed in at both ends.

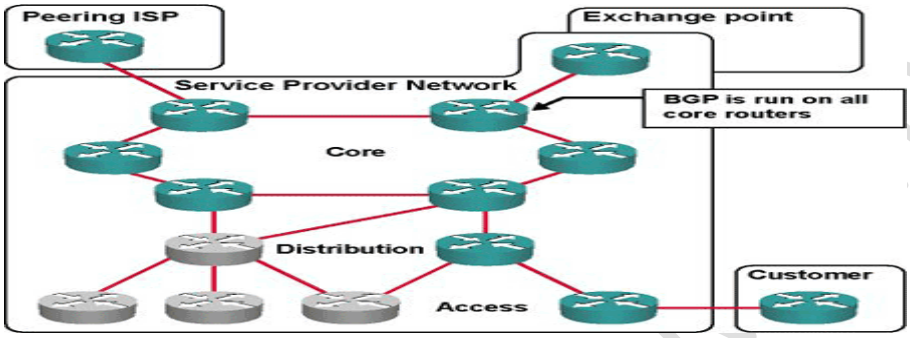

Figure No. 3.1 Border Gateway Protocol

BGP makes best-path decisions based on current reach ability, hop counts and other path characteristics. In situations where multiple paths are available -- as within a major hosting facility -- BGP can be used to communicate an organization's own preferences in terms of what path traffic should follow in and out of its networks. BGP even has a mechanism for defining arbitrary tags, called communities, which can be used to control route advertisement behavior by mutual agreement among peers. Ratified in 2006, BGP-4, the current version of BGP, supports both IPv6 and classless inter domain routing (CIDR), which enables the continued viability of IPv4. Use of the CIDR is a way to have more addresses within the network than with the current IP address assignment scheme.

#Exterior Gateway Protocol (EGP)

Exterior Gateway Protocol (EGP) is a protocol for exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems. EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Each router polls its neighbor at intervals between 120 to 480 seconds and the neighbor responds by sending its complete routing table. EGP-2 is the latest version of EGP.

#Unicast, Multicast and Broadcast

- **Unicast –**This type of information transfer is useful when there is a participation of single sender and single recipient. So, in short you can term it as a one-to-one transmission. For example, a device having IP address 10.1.2.0 in a network wants to send the traffic stream (data packets) to the device with IP address 20.12.4.2 in the other network, and then unicast comes into picture. This is the most common form of data transfer over the networks.

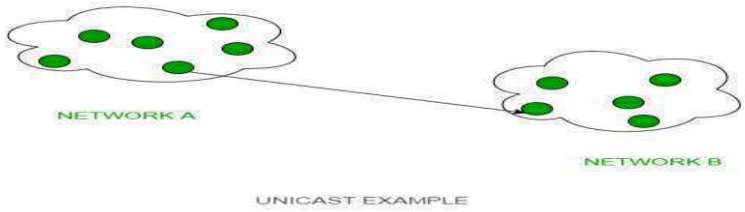

Figure No. 3.2 Unicasting

- **Broadcast** –Broadcasting transfer (one-to-all) techniques can be classified into two types :
- **Limited Broadcasting** –Suppose you have to send stream of packets to all the devices over the network that you reside, this broadcasting comes handy. For this to achieve, it will append 255.255.255.255 (all the 32 bits of IP address set to 1) called as Limited Broadcast Address in the destination address of the datagram (packet) header which is reserved for information transfer to all the recipients from a single client (sender) over the network.

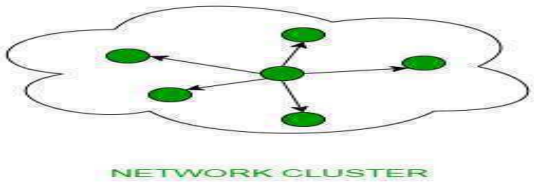

Figure No. 3.3 Limited Broadcasting

- **Direct Broadcasting –** This is useful when a device in one network wants to transfer packet stream to all the devices over the other network. This is achieved by translating all the Host ID part bits of the destination address to 1, referred as **Direct Broadcast Address** in the datagram header for information transfer.

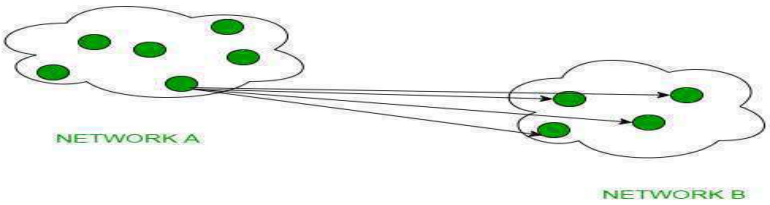

Figure No. 3.4 Directed Broadcasting

This mode is mainly utilized by television networks for video and audio distribution. One important protocol of this class in Computer Networks is Address Resolution Protocol (ARP) that is used for resolving IP address into physical address which is necessary for underlying communication.

- **Multicast** –In multicasting, one/more senders and one/more recipients participate in data transfer traffic. In this method traffic recline between the boundaries of unicast (one-to-one) and broadcast (one-to-all). Multicast lets server's direct single copies of data streams that are then simulated and routed to hosts that request it. IP multicast requires support of some other protocols like IGMP (Internet Group Management Protocol), Multicast routing for its working. Also in Class full IP addressing Class D is reserved for multicast groups.

#Multicast routing protocols

#DVMRP

The DVMRP is used for multicasting over IP networks without routing protocols to support multicast. The DVMRP is based on the RIP protocol but more complicated than RIP. DVRMP maintains a link-state database to keep track of the return paths to the source of multicast packages.

The DVMRP operates as follows:

- The first message for any source-group pair is forwarded to the entire multicast network, with respect to the time-to-live (TTL) of the packet.
- TTL restricts the area to be flooded by the message.
- All the leaf routers that do not have members on directly attached subnet works send back prune messages to the upstream router.
- The branch that transmitted a prune message is deleted from the delivery tree.
- The delivery tree, which is spanning to all the members in the multicast group, is constructed.

In the figure below, DVMRP is running on switches A, B, and C. IGMP is also running on Switch C, which is connected to the host directly. After the host sends an IGMP report to switch C, multicast streams are sent from the multicast resource to the host along the path built by DVMRP.

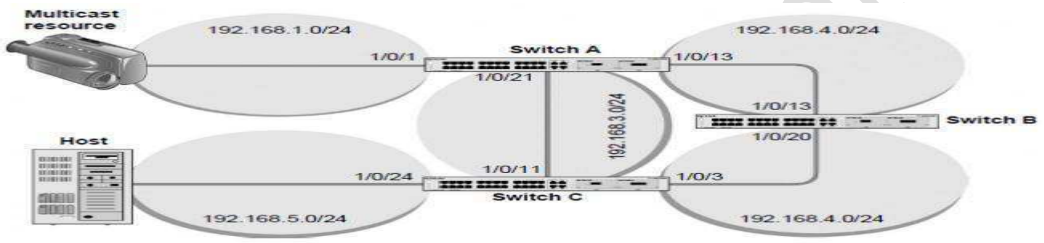

Figure No.3.5 Multicast Open Shortest Path First

#Multicast Open Shortest Path First

MOSPF (Multicast Open Shortest Path First) is an extension to the OSPF (Open Shortest Path First) protocol that facilitates interoperation between unicast and multicast routers. MOSPF is becoming popular for proprietary network multicasting and may eventually supersede RIP (Routing Information Protocol).

Multicast information goes out in OSPF link state advertisements (LSA). That information allows a MOSPF router to identify active multicast groups and the associated local area networks (LANs). MOSPF creates a distribution tree for each multicast source and group and another tree for active sources sending to the group. The current state of the tree is cached. Each time link state changes or the cache times out, the tree must be recomputed to accommodate new changes.

MOSPF uses both source and destination to send a datagram, based on information in the OSPF link state database about the autonomous system's topology. A group-membership-LSA makes it possible to identify the location of each group member. The shortest path for the datagram is calculated from that information.

MOSPF was designed to be backwards-compatible with non-multicast OSPF routers for forwarding regular unicast traffic.

#Core-Based Trees

CBT was the earliest center-based tree protocol, and is the simplest. When a receiver joins a multicast group, its local CBT router looks up the multicast address and obtains the address of the Core router for the group. It then sends a join message for the group towards the Core. At each router on the way to the

core, forwarding state is instantiated for the group, and an acknowledgment is sent back to the previous router. In this way, a multicast tree is built, as shown in figure

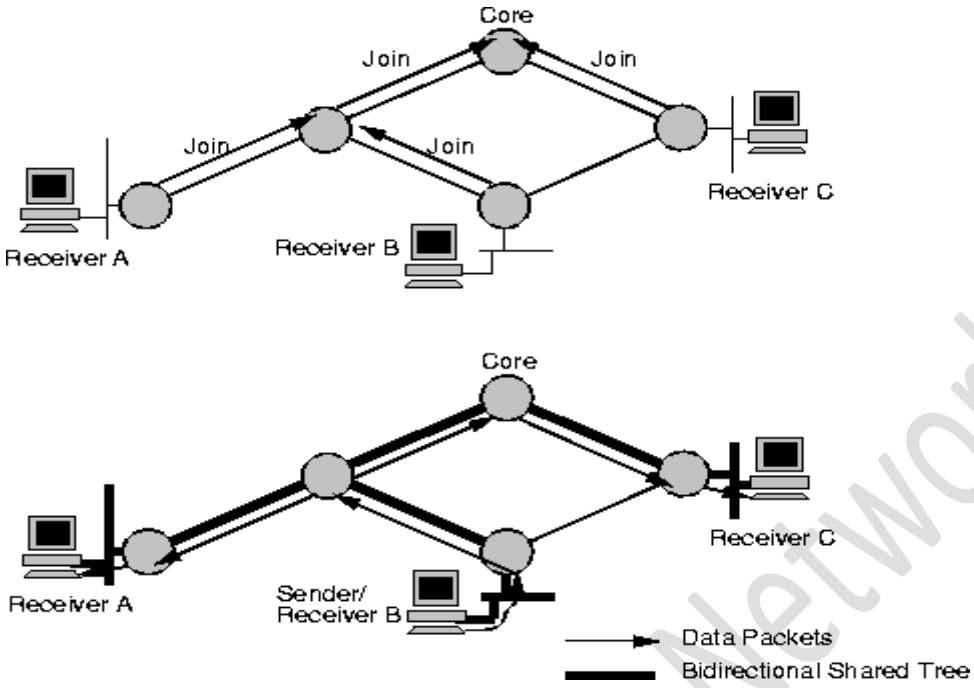

Figure No.3.6 Core-Based Trees

If a sender (that is a group member) sends data to the group, the packets reach its local router, which forwards them to any of its neighbors that are on the multicast tree. Each router that receives a packet forwards it out of all it its interfaces that are on the tree except the one the packet came from. The style of tree CBT builds is called a "bidirectional shared tree", because the routing state is "bidirectional" - packets can flow both up the tree towards the core and down the tree away from the core depending on the location of the source, and "shared" by all sources to the group.

CBT also allows multiple Core routers to be specified which adds a little redundancy in case the core becomes unreachable. CBT never properly solved the problem of how to map a group address to the address of a core. In addition, good core placement is a hard problem. Without good core placement, CBT trees can be quite inefficient, and so CBT is unlikely to be used as a global multicast routing protocol.

#Protocol-independent multicast (PIM)

Protocol-independent multicast (PIM) is a set of four specifications that define modes of Internet multicasting to allow one-to-many and many-to-many transmission of information.

The four modes are:

1. **Sparse Mode (SM)**
2. **Dense Mode (DM)**
3. **Source-Specific Multicast (SSM)**
4. **Bidirectional**

The most common mode in PIM is the sparse mode. It is used for transmission of data to nodes in multiple Internet domains, where it is expected that only a small proportion of the potential nodes will actually subscribe. Dense mode, in contrast to sparse mode, is used when it is expected that a large proportion of the potential nodes will subscribe to the multicast. In source-specific multicast, paths (also called trees) originate (or are rooted) at a single, defined source, whereas bidirectional PIM is not source-specific.

The term "protocol independent" means that PIM can function by making use of routing information supplied by a variety of communications protocols. In information technology, a protocol is a defined set of rules that end points in a circuit or network employ to facilitate communication.

MBone (Multicast Internet)

The MBone, now sometimes called the Multicast Internet, is an arranged use of a portion of the Internet for Internet Protocol (IP) multicasting (sending files - usually audio and video streams - to multiple users at the same time somewhat as radio and TV programs are broadcast over airwaves). Although most Internet traffic is unicast (one user requesting files from one source at another Internet address), the Internet's IP protocol also supports multicasting, the transmission of data packets intended for multiple addresses. Since most IP servers on the Internet do not currently support the multicasting part of the protocol, the MBone was set up to form a network within the Internet that could transmit multicasts. The MBone was set up in 1994 as an outgrowth of earlier audio multicasts by the Internet Engineering Task Force (IETF) and has multicast a number of programs, including some well-publicized rock concerts.

The MBone consists of known servers (mostly on UNIX workstations) that are equipped to handle the multicast protocol. Tunneling is used to forward multicast packets through routers on the network that don't handle multicasting. An MBone router that is sending a packet to another MBone router through a non-MBone part of the network encapsulates the multicast packet as a unicast packet. The non-MBone routers simply see an ordinary packet. The destination MBone router unencapsulates the unicast packet and forwards it appropriately. The MBone consists of a backbone with a mesh topology which is used by servers that redistribute the multicast in their region in a star topology. The MBone network is intended to be global and includes nodes in Europe.

The channel bandwidth for MBone multicasts is 500 kilobits per second and actual traffic is from 100-300 kilobits depending on content. MBone multicasts usually consist of streaming audio and video.

EIGRP (Enhanced Interior Gateway Routing Protocol)

EIGRP (Enhanced Interior Gateway Routing Protocol) is a network protocol that lets routers exchange information more efficiently than with earlier network protocols. EIGRP evolved from IGRP (Interior Gateway Routing Protocol) and routers using either EIGRP or IGRP can interoperate because the metric (criteria used for selecting a route) used with one protocol can be translated into the metrics of the other protocol. EIGRP can be used not only for Internet Protocol (IP) networks but also for AppleTalk and Novell NetWare networks.

Using EIGRP, a router keeps a copy of its neighbor's routing tables. If it can't find a route to a destination in one of these tables, it queries its neighbors for a route and they in turn query their neighbors until a route is found. When a routing table entry changes in one of the routers, it notifies its neighbors of the change only (some earlier protocols require sending the entire table). To keep all routers aware of the state of neighbors, each router sends out a periodic "hello" packet. A router from which no "hello" packet has been received in a certain period of time is assumed to be inoperative.

EIGRP uses the Diffusing-Update Algorithm (DUAL) to determine the most efficient (least cost) route to a destination. A DUAL finite state machine contains decision information used by the algorithm to determine the least-cost route (which considers distance and whether a destination path is loop-free).

#Classless Inter-Domain Routing CIDR

CIDR stands for Classless Inter-Domain Routing (occasionally, Classless Internet Domain Routing). CIDR was developed in the 1990s as a standard scheme for routing network traffic across the Internet.

CIDR is an alternative to traditional IP sub netting that organizes IP addresses into sub networks independent of the value of the addresses themselves. CIDR is also known as super netting as it effectively allows multiple subnets to be grouped together for network.

- CIDR reduced the problem of wasted address space by providing a new and more flexible way to specify network addresses in routers. CIDR lets one routing table entry represent an aggregation of networks that exist in the forward path that don't need to be specified on that particular gateway. This is much like how the public telephone system uses area codes to channel calls toward a certain part of the network. This aggregation of networks in a single address is sometimes referred to as a super net.
- Using CIDR, each IP address has a network prefix that identifies either one or several network gateways. The length of the network prefix in IPv4 CIDR is also specified as part of the IP address and varies depending on the number of bits needed, rather than any arbitrary class assignment structure.
- A destination IP address or route that describes many possible destinations has a shorter prefix and is said to be less specific. A longer prefix describes a destination gateway more specifically. Routers are required to use the most specific, or longest, network prefix in the routing table when forwarding packets. (In IPv6, a CIDR block always gets 64 bits for specifying network addresses.)
- CIDR Notation CIDR specifies an IP address range using a combination of an IP address and its associated network mask. CIDR notation uses the following format -

i. xxx.xxx.xxx.xxx/n

where n is the number of (leftmost) '1' bits in the mask. For example,

ii. 192.168.12.0/23

Applies the network mask 255.255.254.0 to the 192.168 network, starting at 192.168.12.0. This notation represents the address range 192.168.12.0 - 192.168.13.255. Compared to traditional class-based networking, 192.168.12.0/23 represents an aggregation of the two Class C subnets 192.168.12.0 and 192.168.13.0 each having a subnet mask of 255.255.255.0.

iii. 192.168.12.0/23 = 192.168.12.0/24 + 192.168.13.0/24

Additionally, CIDR supports Internet address allocation and message routing independent of the traditional class of a given IP address range. For example,

iv. 10.4.12.0/22

Represents the address range 10.4.12.0 - 10.4.15.255 (network mask 255.255.252.0). This allocates the equivalent of four Class C networks within the much larger Class A space.

- You will sometimes see CIDR notation used even for non-CIDR networks. In non-CIDR IP sub netting, however, the value of n is restricted to either 8 (Class A), 16 (Class B) or 24 (Class C). Examples:

i. 10.0.0.0/8

ii. 172.16.0.0/16.

iii. 192.168.3.0/24

- CIDR implementations

i. CIDR implementations require certain support be embedded within the network routing protocols. When first implemented on the Internet, the core routing protocols like BGP (Border Gateway Protocol) and OSPF (Open Shortest Path First) were updated to support CIDR. Obsolete or less popular routing protocols may not support CIDR.

i. CIDR aggregation requires the network segments involved to be contiguous (numerically adjacent) in the address space. CIDR cannot, for example, aggregate 192.168.12.0 and 192.168.15.0 into a single route unless the intermediate .13 and .14 address ranges are included (i.e., the 192.168.12/22 network).

#Multicast Tree

Multicast is communication between a single sender and multiple receivers on a network. Typical uses include the updating of mobile personnel from a home office and the periodic issuance of online newsletters. Together with any cast and unicast, multicast is one of the packet types in the Internet Protocol Version 6 (IPv6).Multicast is supported through wireless data networks as part of the Cellular Digital Packet Data (CDPD) technology.Multicast is also used for programming on the MBone, a system that allows users at high-bandwidth points on the Internet to receive live video and sound programming. In addition to using a specific high-bandwidth subset of the Internet, Mbone multicast also uses a protocol that allows signals to be encapsulated as TCP/IP packet when passing through parts of the Internet that cannot handle the multicast protocol directly.

Trees

As unicast traffic is forwarded throughout a network, its path takes it from source (S) to destination only.. There are two types of multicast distribution trees: Source Trees and Shared Trees.

Source Trees

A source tree is the most basic of multicast distribution trees. With this type of distribution the source (S) takes the most direct route to the receivers. Because the root, or hop point of this tree is based at the source, each source creates its own SPT.

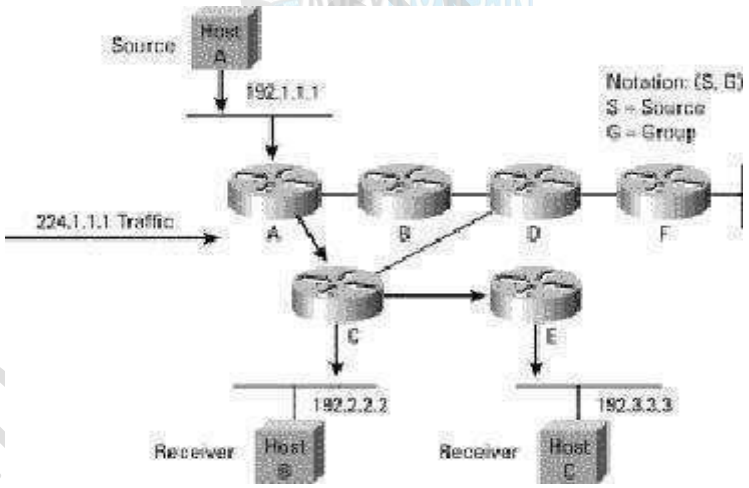

Figure No.3.7 Source Based Distribution Tree

In the diagram Host A is the source of multicast traffic in group 224.1.1.1, in which both Host B and C are receivers. If we were to look at the multicast routes for Router C (*show ip mroute*) it would show an entry of (192.1.1.1, 224.1.1.1). Remember this is the case for each and every source on the network.

Shared Trees

The more common way to distribute multicast traffic is by setting up shared distribution trees, also known as core-based trees (CBT). Recall that with SPT the root of the tree is at the source each source creates its own S,G entry. With CBT there is a shared (configured) root for multicast distribution. Often times this shared root is called the Rendezvous Point (RP) and is essential for the proper configuration of various multicast routing protocols. Each source must send their traffic to the RP for correct distribution

to all receivers. Instead of a S,G entry, this creates a *,G or "star comma G" entry within the multicast routing table. The asterisk represents "all sources." The diagram below illustrates a shared tree.

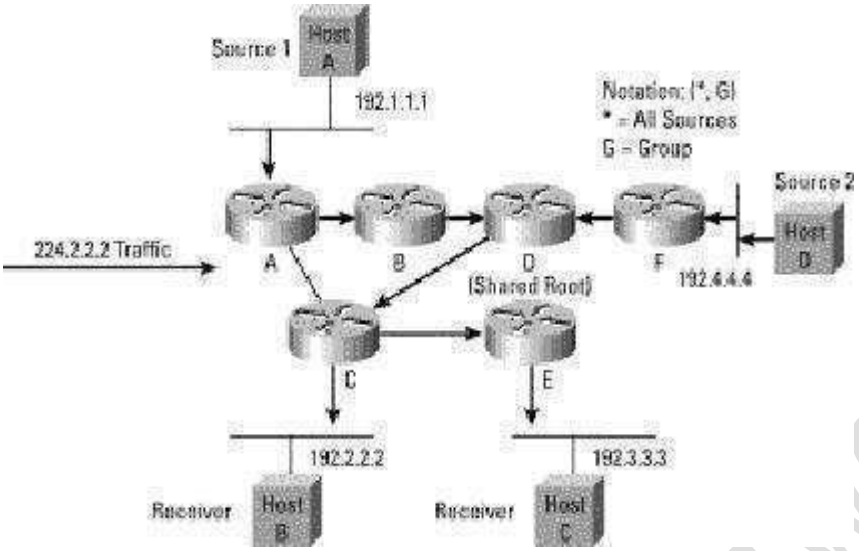

Figure No. 3.8 Shared Multicast Distribution Tree

The diagram shows Router D as the RP for the network. Keep in mind that specifying an RP is a global parameter and will be used for all sources. Also notice that the multicast traffic in this case does not necessarily take the shortest path. This is an important point when designing multicast networks. nd CBT for distribution. This is common when describing some multicast routing protocols such as PIM.

Comparative study of IPv6 and IPv4.

BASIS OF COMPARISON	IPV4	IPV6
Address Configuration	Supports Manual and DHCP configuration.	Supports Auto-configuration and renumbering
End-to-end connection integrity	Unachievable	Achievable
Address Space	It can generate 4.29 x 10^9 addresses.	It can produce quite a large number of addresses, i.e., 3.4 x 10^{38}.
Security features	Security is dependent on application	IPSEC is inbuilt in the IPv6 protocol
Address length	32 bits (4 bytes)	128 bits (16 bytes)
Address Representation	In decimal	In hexadecimal
Fragmentation performed by	Sender and forwarding routers	Only by the sender
Packet flow identification	Not available	Available and uses flow label field in the header

BASIS OF COMPARISON	IPV4	IPV6
Checksum Field	Available	Not available
Message Transmission Scheme	Broadcasting	Multicasting and Anycasting
Encryption and Authentication	Not Provided	Provided

Differences between IPv4 and IPv6

1. IPv4 has 32-bit address length whereas IPv6 has 128-bit address length.
2. IPv4 addresses represent the binary numbers in decimals. On the other hand, IPv6 addresses express binary numbers in hexadecimal.
3. IPv6 uses end-to-end fragmentation while IPv4 requires an intermediate router to fragment any datagram that is too large.
4. Header length of IPv4 is 20 bytes. In contrast, header length of IPv6 is 40 bytes.
5. IPv4 uses checksum field in the header format for handling error checking. On the contrary, IPv6 removes the header checksum field.
6. In IPv4, the base header does not contain a field for header length, and 16-bit payload length field replaces it in the IPv6 header.
7. The option fields in IPv4 are employed as extension headers in IPv6.
8. The Time to live field in IPv4 refers to as Hop limit in IPv6.
9. The header length field which is present in IPv4 is eliminated in IPv6 because the length of the header is fixed in this version.
10. IPv4 uses broadcasting to transmit the packets to the destination computers while IPv6 uses multicasting and any casting.
11. IPv6 provides authentication and encryption, but IPv4 doesn't provide it.

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in