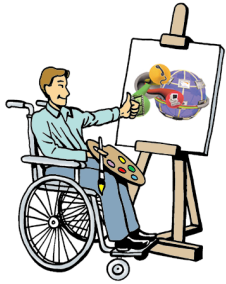

Lesson 1: The Internet Protocol

At a Glance



This lesson will provide a review of IP addressing and an introduction to IP multicasting. It is important to have a strong foundation in the Internet Protocol and addressing to understand how it is used for Voice over IP applications. Subnetting is covered to provide an understanding of how to subnet a network when creating a network design.

IP is a networking protocol that was originally developed to support the transmission of data. It is the Internet Protocol that provides the mechanism for identifying or addressing every device on a network, including the Internet.

The most common version of IP is version 4, which provides over 4 billion possible addresses. Because the use of IP has grown so great in a very short time period, it is expected that the addressing scheme of IPv4 will be inadequate. It is not so much a problem with the lack of possible addresses, as it is a problem with the way version 4 wastes addresses.

A new version known as IP version 6 (IPv6), or IP Next Generation (IPng), is under development to address the shortcomings of IPv4.

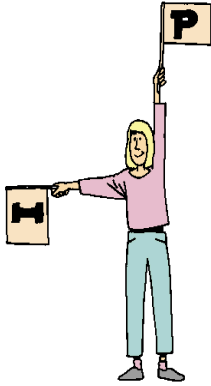
What You Will Learn

After completing this lesson, you will be able to do the following:

- Identify IP addresses according to their class
- Identify network and hosts portions of Class A, B, and C IP addresses
- Identify the advantages of IPv6 over IPv4
- Compare IP Multicasting with Unicasting and Broadcasting
- Describe the multicasting protocols, IGMP and DVMRP
- Demonstrate how to logically subnet a network and assign IP addresses

Student Notes:

Tech Talk



- **Anycast Address**—An IP address that allows a packet to be sent to a single individual within a group by specifying a specific route.
- **Broadcast Address**—An IP address that identifies all the devices on a subnetwork.
- **Cost**—A value or metric assigned by a network manager to a router port and used to determine the best path for a packet to travel across a network.
- **Distance Vector Protocols**—Routing protocols that determine the best path for a packet to travel across a network by determining the least number of hops, or pre-assigned costs, from the source to the destination.
- **Dynamic Host Configuration Protocol**—DHCP is a protocol used to automatically assign IP addresses to all devices on a network.
- **Multicast Address**—An IP address that identifies a specified group of devices on multiple subnetworks.
- **Resource Reservation Protocol**—RSVP is a protocol that allows network bandwidth to be reserved between the source and destination so that a specific level of quality can be assured during the transmission of information.
- **Unicast Address**—An IP address that identifies a single device on a network.

Internet Protocol Version 4 (IPv4)

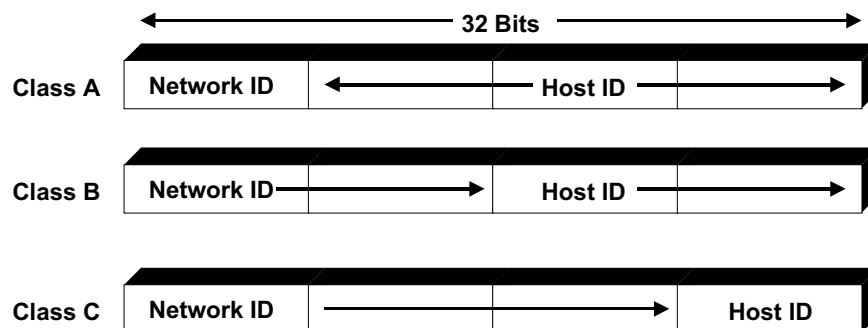
Layer 3 addresses are commonly called IP addresses because the Internet Protocol is the most common protocol found operating at the network layer. IP version 4 was developed in 1975 to provide an addressing scheme that can identify any device on any network connected to the Internet. No two devices can have the same IP address at the same time. Since it is a standard way of allocating addresses, many networks that are not connected to the Internet also use IP addressing.

Classful Addressing

Each computer in each network must have a unique address so that it will not be confused with any other computer in any other network. Some networks are very large with thousands of computers, while some are very small. Because most networks tend to grow and add computers, each network needs addresses for the machines it currently has, as well as for machines it might add in the future.

In IPv4, blocks of IP addresses are allocated to various networks. These blocks of addresses come in several sizes, called classes. Each address within a class is comprised of 32 bits represented by a four-octet dotted decimal notation, e.g., 134.177.3.35. The IP address is divided into a network portion and a host portion. The number of octets that are assigned to represent each portion of the IP number varies with the class.

Parts of an IP Address



Using this addressing scheme, the Internet committee assigns specific addresses to all the networks that comprise the Internet. The committee created classful addressing as a way of dividing the 4.3 billion addresses among the various sizes of networks.

There are five classes of addresses in IPv4.

- **Class A**—Class A addresses were created for the largest networks. Class A addresses use the first octet to indicate the network and the other three octets to indicate hosts on that network. The range of Class A addresses begins with 1.0.0.0 and ends with 127.255.255.255. There are 127 Class A networks. Each network with a Class A address can have 16,777,214 different host addresses. Most of the Class A addresses are assigned to the U.S. government and large companies involved with the Internet during its early development.
- **Class B**—Class B addresses are for medium sized networks. Class B addresses begin with 128.1.0.0 and end with 191.254.255.254. They use the first two octets to represent the network address and the last two octets to represent the host address. There are a maximum of 16,382 Class B networks. Each Class B network can have 65,534 different host machines. All the Class B addresses have been depleted.
- **Class C**—Class C addresses are for smaller networks. Class C addresses range from 192.0.1.0 to 223.255.254.255. They use the first three octets to represent the network address and the last octet to represent the host address. There are 2,097,150 Class C networks possible and each Class C network can have only up to 254 different host machines. Class C addresses are still available, but are rapidly declining.
- **Classes D and E**—Class D addresses are used for IP Multicasting, discussed later in this lesson. The Internet committee uses Class E for research. Addresses above 224.255.254.255 are used for these classes.

IPv4 Classes A-C

Class	Dotted-decimal Representation	Number of Addresses per Network	Organization Type
Class A	1.0.0.0 through 127.255.255.255	16,777,214	Large Companies and the Government
Class B	128.1.0.0 through 191.254.255.255	65,534	Medium-size companies
Class C	192.0.1.0 through 223.255.254.255	254	Small companies

Subnetworks

Network managers often divide large networks into small subsets called subnetworks. The addresses within a class are divided into three parts, the network portion, the subnetwork portion, and the host portion. Designating one of the octets from the host portion for the subset creates the subnetwork portion of the address. The subnetwork number is always a multiple of 32.

Class B Subnet Addresses

Class B Network Address	Class B Subnet Addressing
128.30.0.0	128.30.0.0
	128.30.32.0
	128.30.64.0
	128.30.96.0
	128.30.128.0
	128.30.160.0
	128.30.192.0
	128.30.224.0

Just as the postal service uses the house number, street name, city, state, country, and zipcode to deliver a letter to its destination, routers within a network use the network, subnetwork, and host portions of an IP address to determine the destination of the packet.

Address Mask

An address mask identifies to the router the network portion of an IP address by indicating which octets are part of the network number. A mask is also 32 bits long. From the address mask, it is possible to determine the IP Class of the network. There are two types of masks, the natural mask and the subnet mask.

A natural mask strictly identifies the network portion of the IP address. A subnet mask identifies the octets that are designated for both the network number and the subnet address.

Natural and Subnet Masks

Class	Mask Type	Dotted-Decimal Notation
Class A	Natural	255.0.0.0
	Subnet	255.255.0.0
Class B	Natural	255.255.0.0
	Subnet	255.255.255.0
Class C	Natural	255.255.255.0
	Subnet	255.255.255.240

Classless Internet Domain Routing

Classes A, B, and C provided only three choices for networks: 65,777,214 hosts, 65,534 hosts, or 254 hosts. If a company had 500 people, it could use a Class B addressing scheme. Using Class B gives the company 65,536 addresses, which waste approximately 65,000 possible addresses since the extra addresses cannot be used by another company. Alternatively, the company could build two Class C networks, which would give the company 508 addresses to assign. That arrangement does not leave the company room to expand easily.

The network routers maintain routing tables that record the IP addresses of all the networks connected to the Internet. With the number of small networks increasing, the router tables are not always large enough to maintain a complete record of all the network addresses. Additionally, routers exchange router tables with other routers. Transmission of these large tables can use significant bandwidth and consequently slow down transmission rates across the Internet.

Classless Internet Domain Routing (CIDR) was developed as a short-term solution to IPv4's inefficient use of addresses. Using CIDR, blocks of Class C addresses are assigned to a company based on the actual number of hosts in the company. The company address scheme remains under the umbrella of one network. This approach eliminates the wasteful use of addresses and reduces the number of networks attached to the Internet.

CIDR also divides Class C into four zones: North, South and Central America; Asia, Europe; and the Pacific. Internet routers only need maintain in their tables the other zone addresses and the addresses of the networks in their zone. From that information, a router can forward any packet that is destined to another zone.

Check Your Understanding

- ◆ In what IP class does the address 120.32.0.10 reside? What is the subnet mask for this address?
- ◆ In what IP class does the address 192.21.47.16 reside? What is the subnet mask for this address?
- ◆ In what IP class does the addresses 128.30.128.10 and 128.30.128.12 reside? If the subnet mask is 255.255.255.0, identify the network portion, subnetwork portion and the host portion of these addresses.

Internet Protocol Version 6 (IPv6)

Just as the post office added four more digits to zip codes, the Internet will, over the next few years, add 96 more bits to IP addresses, making them 128 bits long. That increase will allow every possible device to acquire an IP address, from desktop computers to information appliances. The new addressing scheme under development by the IETF is called IP version 6 (IPv6). IPv6 is a long-term solution designed to solve many of the problems with the current 32 bit addressing used by IP version 4.

The greatest advantage IPv6 has over IPv4 is the expanded address length, which resolves the depletion of available addresses. IPv6 also has other features that will improve the Internet Protocol.

- IPv6 does not require using the Dynamic Host Configuration Protocol (DHCP). DHCP is used to automatically assign IP addresses to all devices on a network. A DHCP server must exist on the network and the network manager must configure the server to assign IP addresses from a pre-set pool of numbers. In IPv4, either a device must have its address manually assigned or it must acquire its address dynamically from a DHCP server. In IPv6, once a device is assigned an address, the address becomes unique to the device. This allows the device to connect to the Internet from anywhere without reconfiguration. This feature is a major advantage for mobile users who often connect to the Internet from many different locations.
- Within an IP header there is space to add extensions for the sender to place customized options. In IPv4, any option added to the header slows the transmission of the packet because the network router must examine all the options. In IPv6, the router does not examine the options, so a packet with options attached will travel faster along the network.
- Since IPv6 allows options without slowing down the transmission of a packet, authentication and security options are now available for use with the Internet Protocol that were not available before. An authentication header may be added to provide some user authentication functionality. Also, an encapsulation security header may be added using the DES encryption algorithm to provide protection against data tampering.

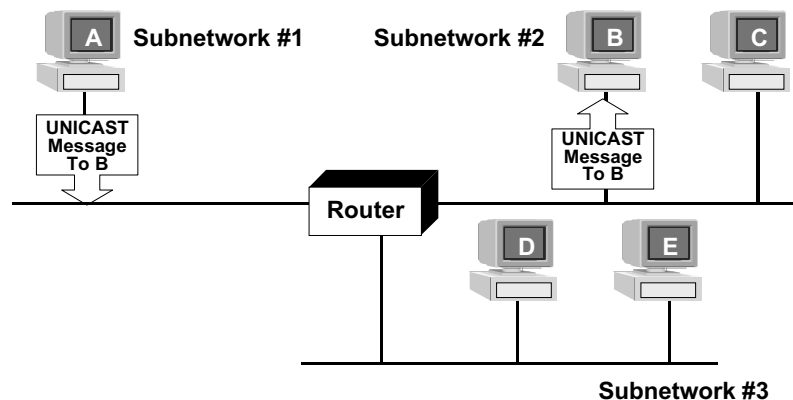
- Within both IPv4 and IPv6, specific addresses are used to define a group of hosts. Using this specific address, called a multicast address, a single packet can be sent to everyone in a group. In IPv6, another address, called an anycast address, allows a packet to be sent to a single individual within a group by specifying a specific route. The transmission performance of this packet is increased since the router does not have to determine the best route; it merely follows instructions within the anycast address.
- IPv6 provides greater support for multimedia applications such as real-time voice and audio. IPv6 uses the Resource Reservation Protocol (RSVP) to reserve bandwidth so the flow of information will travel with a guarantee of quality. It also prioritizes packets, so that the transmission of less important packets is done at a time that will not interfere with high priority packets requiring a continuous stream of delivery. This is a particularly important feature for implementing voice over IP. One of the major drawbacks to the transmission of voice or audio over the Internet has been the tendency for the sound to break up due to packet interruptions, resulting in an unpleasant experience.

Although transitioning from IPv4 to IPv6 will take years (some estimates indicate up to 10 years) the increase in performance, the unlimited IP addresses, and added flexibility of IPv6 will have a dramatic effect on unified networking.

IP Multicasting

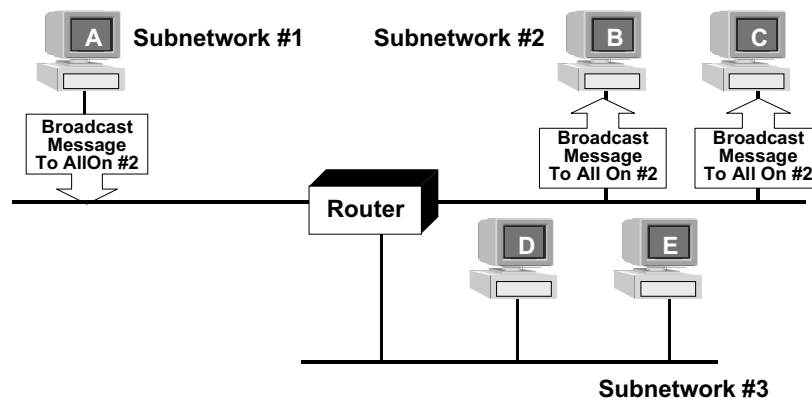
The vast majority of information traveling across a network is transmitted from an individual source to a single destination using a unicast address. A unicast address is an IP address that identifies a single device on a network. If the sender wishes to send a message to multiple destinations, a unicast address could be sent to each destination.

Unicasting



A single message could be sent to several devices on a subnetwork using a broadcast address. A broadcast message is an IP address used to send out a single message to an entire subnetwork. All devices on the subnetwork receive a copy of the message whether or not every device uses the message.

Broadcasting

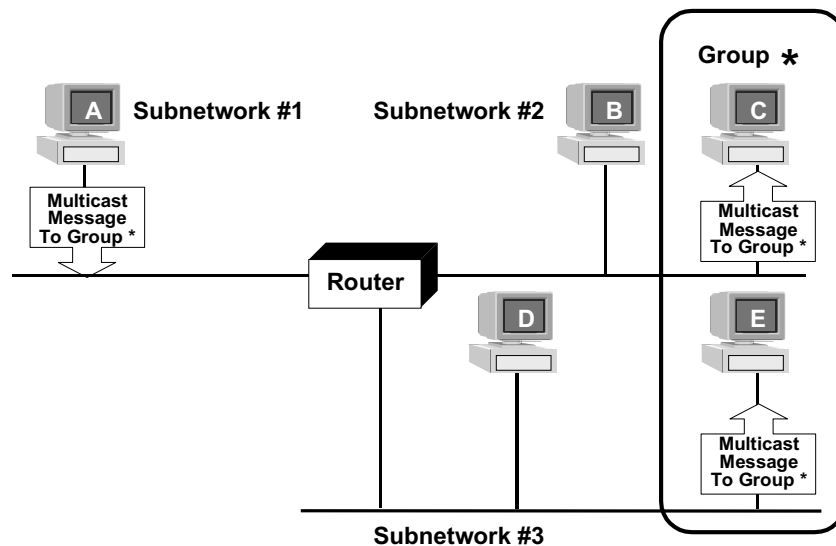


Either of these methods accomplishes the delivery of a single message to multiple destinations. However, both methods waste precious bandwidth. Unicasting wastes bandwidth by sending the same message multiple times. Broadcasting wastes bandwidth by sending devices messages that are not intended for them.

Networking is becoming an essential part of everyone's life. There are computer networks in businesses, schools from elementary to college, and in many homes. The need to conserve bandwidth is great. Most individuals who have used the World Wide Web have experienced the effects of bandwidth shortages, turning the WWW into what is often called the World Wide Wait.

IP multicasting provides a solution that allows a single message to be transmitted to multiple destinations and still conserve bandwidth. Using a multicast address, a single message can be sent to a specified group of devices across multiple subnetworks. Any device not in the group will not receive the message. It eliminates the need to send multiple messages. Membership in a group is controlled by the network manager and can be changed easily.

Multicasting



Using IP multicasting, organizations can increase the efficiency of their network by identifying various groups and using multicasting to deliver a single message to a group at the same time. For example, a manufacturer could identify a group of several retailers and send out a single transmission that contains updated inventories and price lists. Perhaps an educational organization wishes to conduct a training session at multiple locations using videoconferencing. Using IP multicast, the various locations are identified as a training group and with the use of the Internet, the videoconference transmissions are directed only to the training group. The same group could conduct a conference call using Voice over IP and multicasting technologies.

Check Your Understanding

- ◆ Define the difference between unicasting, broadcasting, and multicasting.
- ◆ Why does multicasting save bandwidth?
- ◆ What examples can you think of that represent a unicast message and a multicast message?

IP Multicast Addresses

In IPv4, the Class D addresses are used to identify multicast groups. The first four bits of the address is used to identify it as Class D, the last 29 bits identify the multicast group.

With Class A, B, and C, the IP address is directly mapped to the MAC (physical) address of the device using the Address Resolution Protocol (ARP). The router maintains a table that references which IP address corresponds to which MAC address. The router uses the table to determine to where a packet should be forwarded.

ARP Table

IP Address	MAC Address
168.192.10.254	08.00.20.92.b1.7f
168.192.10.5	08.00.20.92.b1.04
168.192.10.12	08.00.20.92.b1.52

MAC addresses are 48 bits long and portions of the address are reserved for the inclusion of either broadcast or multicast addresses, which are only 32 bits. Consequently, in IPv4, the IP multicast address is not mapped directly to the MAC address using a protocol. Instead the last 23 bits of the multicast are dropped into the last 23 bits of the MAC address.

Multicast Protocols

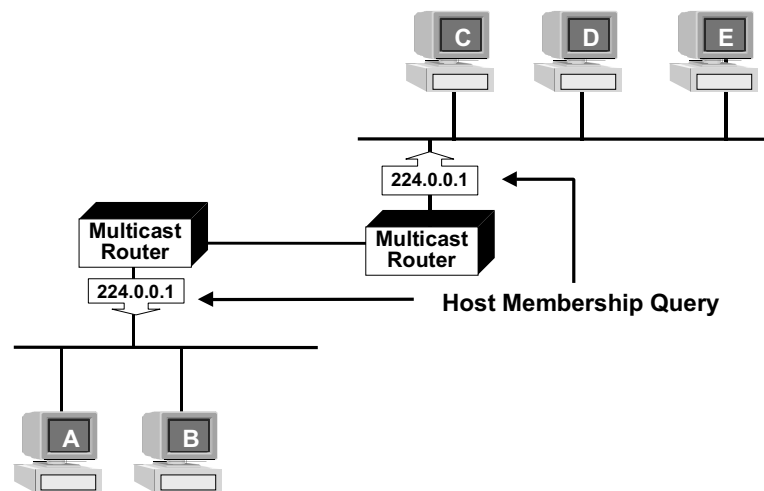
IP multicasting employs several protocols that provide identification of groups and manage the routing of multicast packets across a network.

Internet Group Management Protocol

In order for a device to be included in a group, the device must inform the router to which it is connected. The device must initiate a request to be included in the multicast group. A device may belong to multiple groups. The Internet Group Management Protocol (IGMP) is the protocol that provides the mechanism for hosts and routers to join or leave a group. Since 1989, when the original RFC 1112 defined IGMP, there have been two more updates, IGMPv2 and IGMPv3. The IEEE to date has not established the latter two updates as standards.

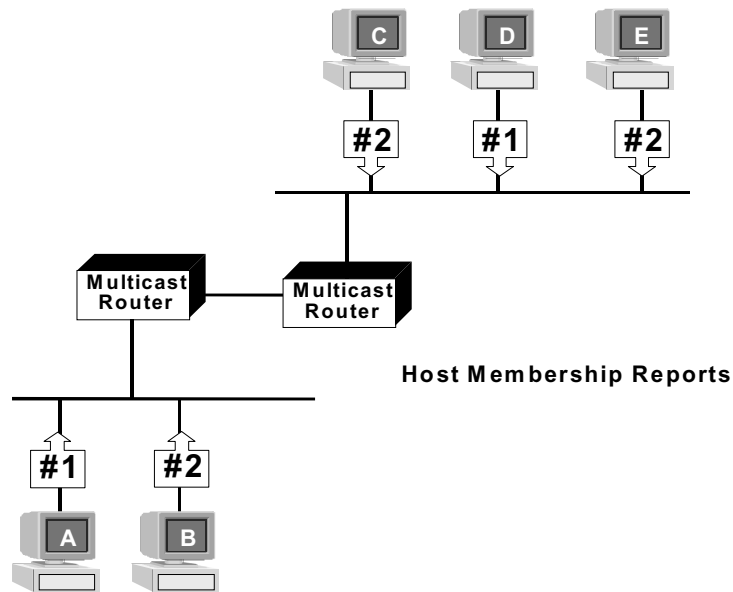
There are three basic steps to a host establishing membership in a group.

IGMP: Step One

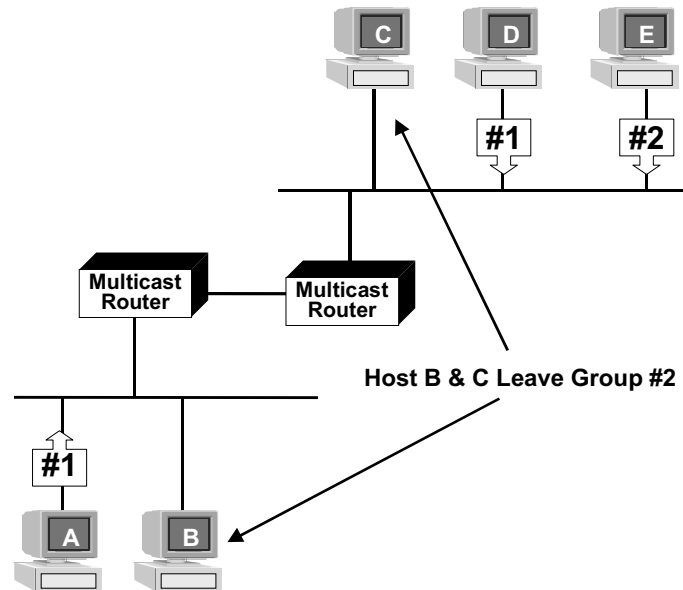


1. Multicast routers periodically transmit a "host membership query" to the "all host group," a multicast group that addresses all the hosts in a subnetwork. The message only goes as far as the direct next door neighbors. It does not go beyond the subnetwork to the next router down the line.

IGMP: Step Two



2. The host responds by sending back a "host membership report". This report informs the router of each group the host belongs. The host must send back a report for each group in which it belongs. Typically the host does not send a report unless it has received a request from the router. However, when a host first joins a group, it will send a report to the router to inform the router that it has joined a group.

IGMP: Step Three


3. The multicast router learns of the departure of a host from a group by simply not receiving a report from the host when requested. A host will leave a group when it no longer wishes to receive messages directed specifically to that group. When the router does not receive a report, it removes the host from the group's list and no longer forwards multicast messages to the host.

Only one router may send out queries per subnetwork. If there is more than one router on a subnetwork, then another multicast protocol must determine which router will send out the queries.

If implemented, both IGMPv2 and IGMPv3 will provide some improvements to the original protocol. IGMPv2 assigns the router with the lowest IP address the duty of sending queries to all host groups. This version also allows routers to send a query to a specific group, rather than to all groups. It also incorporates a "leave group" message that allows a host to send a message to all the routers, using the all routers group address (224.0.0.2), that it has left a group. IGMPv3 allows a host to specify what sources from which it does not want to receive transmissions.

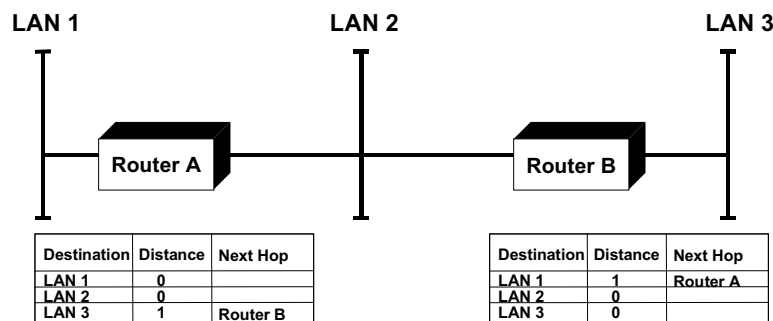
It is important to realize that not all routers are capable of multicasting. Only routers capable of implementing IGMP are multicast routers and not every multicast router is capable of performing unicasting. As a temporary solution until all routers are IGMP capable, multicasting over the Internet is performed by the use of virtual tunnels. The multicast packets are encapsulated into unicast packets for delivery through the tunnels. This system of tunnels is referred to as the Multicast Backbone or Mbone.

Distance Vector Multicast Routing Protocol

There are several different multicast routing protocols. The most widely used protocol is the Distance Vector Multicast Routing Protocol (DVMRP).

Unicast distance vector protocols determine the best path for a packet to travel across a network by determining the least number of hops from the source to the destination. Network managers can also assign a "cost" to each port on a router. As a packet travels from router to router, the costs of passing through each port are added together. Routers maintain tables that keep track of the distance (hops) or costs associated with each path and assign a packet to travel across a path with the least cost. A distance of zero in the table indicates the host is on the same LAN as the router. A distance of one indicates the host is on a LAN connected to the next router.

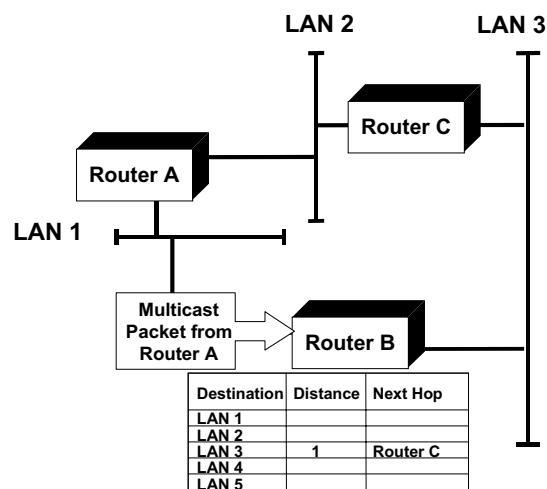
Unicast Distance Vector Routing Tables



DVMRP differs from unicast distance vector protocols in that it does not keep track of paths to destinations; rather it keeps track of paths back to the source by use of Reverse Path Multicasting. From this information, the protocol builds a multicasting web or tree of all the best paths to each group.

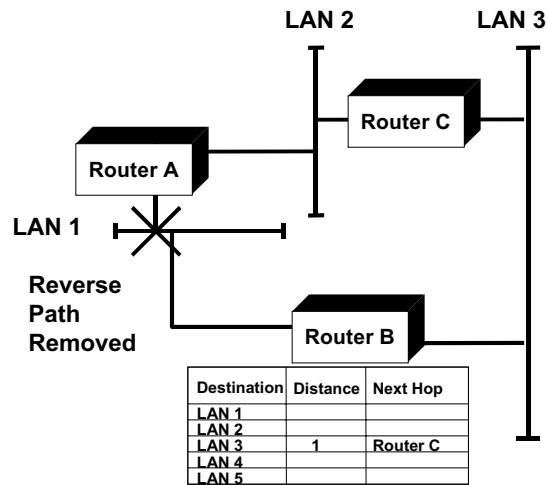
There are five basic steps to building a multicast tree.

DVMRP Step One

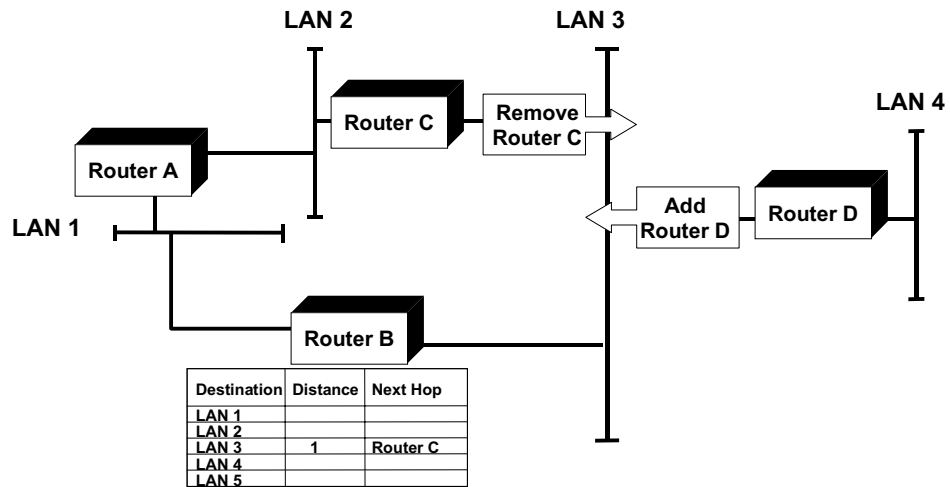


1. When a multicast router receives a multicast packet, it uses a unicast routing table to check if the reverse path to the source is the shortest path.

DVMRP Step Two



2. If the reverse path is the shortest, then the router forwards the packet across all the other paths except the one back to the source. If the reverse path is not the shortest, then the packet is discarded and this path is "pruned" from the tree.
3. The routing information is exchanged between every multicast router on the network.

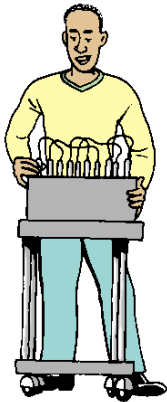
DVMRP Steps Four and Five


4. If a multicast router on the network does not have members of a specific group, it sends a message requesting the path to it be pruned for multicast messages not meant for its hosts.
5. A multicast router can also send "graft" requests for a new path to be added to the tree so its hosts are included in a specific multicast group.

Try It Out: Subnetting a Network

Materials Needed:

- Windows 95 PC
- Windows 95 PC Scientific Calculator installed
- Pen/Pencil and Paper



This activity is designed to teach you how to determine what the possible subnet masks, subnet addresses, and host addresses are available for a given IP address class. The activity will concentrate on Class B addressing, but the concepts may be applied to Class A and C.

You may wish to review the relationship between hexadecimal, binary, and decimal numbers from your previous courses before completing this activity.

Part One: Using the Windows 95 Scientific Calculator

IP addresses are made of 32 bits written as four sets of eight bits called *octets*. To a network device 134.177.3.35 looks like this:

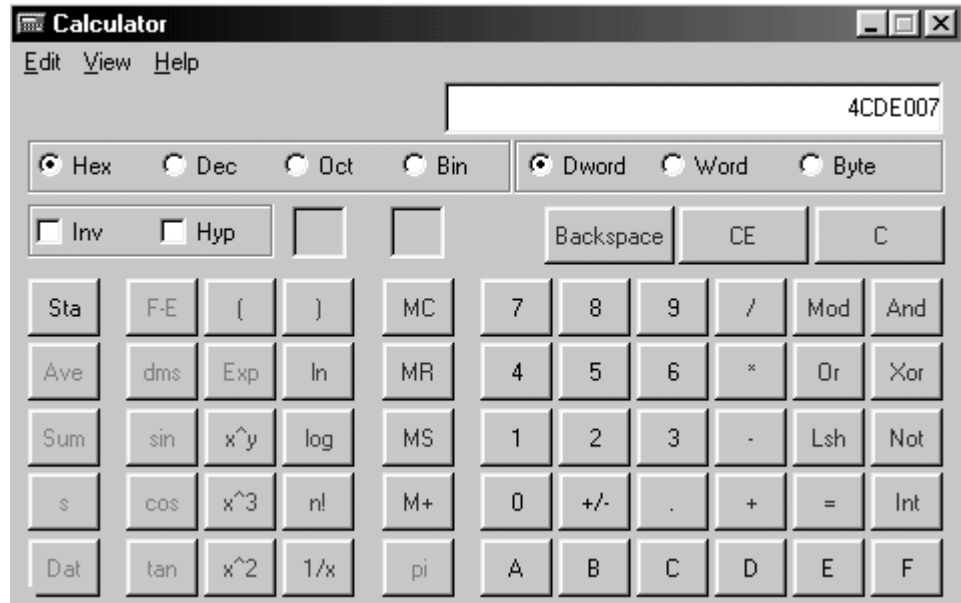
10000110.10110001.00000011.00100011

Your computer has a scientific calculator that converts decimal numbers to hexadecimal, octal, or binary numbers. Just go to **Start – Programs – Accessories – Calculator**. You will see a standard calculator; however, if you go to the **View** menu and select **Scientific** you will get the numbering system conversion calculator.

Conversion of address notations is easily accomplished using the scientific calculator included as an accessory in Windows.

1. Use the Start menu to find and run the calculator.

- In the Calculator window, pull down the View menu and select Scientific.



- At the top left of the window, four buttons labeled Hex (Hexadecimal or base 16), Dec (Decimal or base 10), Oct (Octal or base 8), Bin (Binary or base 2) will be displayed.
- To convert from the binary system to decimal, click on binary and type in a set of eight bits (e.g., 10000110). Now, click on the decimal system. The converted number will display automatically (e.g., 134). You can only convert one octet (eight bits) at one time.

This accessory is a handy tool for any network administrator when working with IP numbers and subnetting a network. In this activity, you may use the calculator to help you determine the address ranges for a subnetted network.

Part Two: Determining Subnet Masks, Subnet Addresses, and Host Addresses

In the lesson, a subnet mask for each class is listed in a table. For Class B addresses in the table, the listed subnet mask is 255.255.255.0. This is the mask if all eight bits of the third octet are used for the subnet number. In this case, the binary number 11111111.11111111.11111111.00000000 is represented by 255.255.255.0. The subnet mask 0 bits represent host numbers.

However, it is not mandatory that all eight bits be used. You could use any number of bits from one to all eight. If less than eight bits are used in the third octet, then more subnet masks may be created.

- Using your PC calculator, fill in the chart below with the decimal representations of the possible Class B subnet masks.

Possible Class B Subnet Masks	
Binary Number	Decimal Representation
11111111.11111111.10000000.00000000	
11111111.11111111.11000000.00000000	
11111111.11111111.11100000.00000000	
11111111.11111111.11110000.00000000	
11111111.11111111.11111000.00000000	
11111111.11111111.11111100.00000000	
11111111.11111111.11111110.00000000	
11111111.11111111.11111111.00000000	

2. What patterns are evident from this table?

The subnet mask identifies the bits used in the IP address to determine the subnet number. For example, the Class B mask 255.255.192.0 identifies that the first two bits of the third octet as the subnet number of the network address. In the case of the binary network number 10000000.00011110.10000000.00010001, the decimal representation is 128.30.128.17, with the subnet number 128.30.128.0 and the host number 17.

The Class B network with a mask of 255.255.192.0 allows four possible subnet numbers by using all the possible combinations of 0s and 1s.

3. Using the calculator, fill in the chart below with the decimal representations of the four possible subnet numbers for the mask 255.255.192.0 and a network number 128.30.0.0.

Binary Bit Pattern for Subnet Numbers	Decimal Representation
10000000.00011110. 00 000000.00000000	
10000000.00011110. 01 000000.00000000	
10000000.00011110. 10 000000.00000000	128.30.128.0
10000000.00011110. 11 000000.00000000	

The possible number of subnets is determined by taking the number 2 (since we are working in binary) to the exponent equal to the number of bits used, which in the above example is 2 (e.g., 2^2).

The possible number of host addresses per subnet is then determined by taking the number 2 to the exponent equal to the number of bits remaining less 2. Since any address with either all 1s or all 0s is reserved for special cases, those numbers must be subtracted out from the total number of hosts.

Looking at the chart for the network number 128.30.0.0, the number of bits remaining in the third octet and fourth octet is 14. So the number of possible hosts per subnet is $2^{14} - 2$ or 16,382.

4. Using the calculator and the chart from question #1, fill in the chart below for the total number of possible subnets and hosts per Class B masks.

Possible Subnet and Hosts Per Class B Subnet Mask				
Subnet Mask	No. of Subnet Bits Used	No. of Subnets	No. of Host Bits Used	No. of Hosts per Subnet
255.255.128.0				
255.255.192.0	2	4	14	16382
255.255.224.0				
255.255.240.0				
255.255.248.0				
255.255.252.0				
255.255.254.0				
255.255.255.0				

5. If your client has a growing company with 900 employees, what Class B subnet mask would you recommend using? Why?

After a network manager has chosen the subnet mask most appropriate for the company network, he or she must determine the actual addresses that will be assigned to each device within each subnetwork.

Going back to the previous network example, 128.30.0.0, you determined that there were four subnetworks, 128.30.0.0, 128.30.64.0, 128.30.128.0 and 128.30.192.0. In the lesson, it was noted that the dotted decimal representation of the host address is determined from the combination of the subnet value and the host value.

	Bit Representation	Decimal Representation
Subnet	10000000.00011110.00000000.00000000	128.30.0.0
Subnet Mask	11111111.11111111.11000000.00000000	255.255.192.0
Low Host Address	10000000.00011110.00000000.00000001	128.30.0.1
High Host Address	10000000.00011110.00111111.11111110	128.30.63.254

Notice that the complete host address is represented by a range from 0 to 63 as the subnet value and a range from 1 to 254 as the host value.

6. Determine the range of host addresses for the subnet 128.30.64.0 and fill in the chart below.

	Bit Representation	Decimal Representation
Subnet		128.30.64.0
Subnet Mask	11111111.11111111.11000000.00000000	255.255.192.0
Low Host Address		
High Host Address		

Part Three: A Simple Case Study

The Blue Mood Music Company has 16,000 employees. The company has established the network address as 180.1.0.0. Based only on this information, complete the questions and chart below.

1. What number of subnets do you recommend to accommodate the company now and in the future?
2. What subnet mask do you recommend?
3. Create a chart detailing the addressing for this network.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Accurate completion of charts and questions in Part Two.	50	
Thoughtful application of activity concepts in Part Three.	25	
Accurate addressing scheme in Part Three.	25	
TOTAL	100	

Stretch Yourself: Multicast Routing Protocols

Materials Needed:

- Windows 95 PC
- Internet Connection (optional)
- Any Word Processor (e.g., MS Word)
- Pen/Pencil and Paper
- Model material such as paper mache (optional)



In this lesson, you have been introduced to the Distance Vector Multicasting Routing Protocol. DVMRP is the routing protocol that was used to establish the Internet's MBone. There are several other multicast routing protocols that a network manager might use in establishing a multicast network.

The following are multicast routing protocols:

- Protocol Independent Multicast- Dense Mode (PIM-DM)
 - Multicast Open Shortest Path First (MOSPF)
 - Protocol Independent Multicast- Sparse Mode (PIM-SM)
 - Core-Based Trees (CBT)
1. Choose two of the four protocols listed.
 2. Research how these protocols differ from DVMRP and note if specific vendors or products implement these protocols.
 3. Create an instructional diagram or model demonstrating how each protocol works in comparison to DVMRP.
 4. Write a brief explanation of the diagram or model, including any information that would be helpful in deciding if one protocol should be implemented over another.
 5. Document your resources.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Thorough research of two protocols with resources documented	25	
Precise instructional diagram or model clearly demonstrating each protocol	50	
Informative explanation	25	
TOTAL	100	

Network Wizards:

Materials Needed:

- Windows 95 PC
- Windows 95 Scientific Calculator installed
- Any Word Processor (e.g., MS Word) or Spreadsheet (e.g., MS Excel)
- Pen/Pencil and Paper
- School Network Design (optional)
- Student Portfolio
- Student Network Design Proposal Working Draft



Part One: Subnet Your School Network

With the knowledge you have gained from the lesson and the Try It Out activity, your task in this activity is to create a subnetwork addressing scheme for your school network.

As a network designer, you need some questions answered before you design an IP address scheme.

1. How many subnets are there in the organization? In this case, you need to determine how many departments within the school should be allocated as their own subnet. Should the school network be grouped according to subject or grade level?
2. Will more subnets be needed in the future? Gather information from your principal about the future growth of the school. Will the organization of the departments be changed? Will additional departments be added?
3. How many hosts are there on the largest subnet existing today? Find out how many hosts (students and teachers) are in the largest department? You will have to create a subnetting scheme that will accommodate all the hosts on each subnet.
4. How many hosts will be on the largest subnet in the future? Is one department expected to grow more than another? Will one grade level increase in size?

Once you have gathered the answers to the questions above, create an IP addressing scheme with subnetting that will accommodate the school's current and future networking needs.

Include in your scheme a diagram of the school's layout with the subnets and address ranges for each subnet indicated. Write a paragraph explaining your recommendation to accompany your diagram.

After your teacher has reviewed your recommendations, make any corrections suggested and place your final product into your portfolio.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Thorough information gathering	25	
Accurate IP addressing appropriately accommodating the needs of the school	50	
Quality diagram and recommendation suitable for reproduction and inclusion in portfolio	25	
TOTAL	100	

Part Two: Network Design Portfolio Case Study

Analyzing the information you have gathered from your case study is a very important process to creating your network design. Over the next three weeks you should organize the information and determine if you have missed any necessary information.

When analyzing your data, translate the information into the network needs of your customer. The questions below are examples of some of the questions you should ask yourself.

1. What are the company's most important business requirements? For example, a company may maintain product inventories in a shared database across multiple locations.
2. What network requirements will best support the identified business requirements? Continuing the example in #1, the company needs continuous availability between the multiple locations. This requires that the connections be very reliable and that multiple paths for transmissions be available.
3. What are the company's security issues?
4. Does the company have remote access requirements? How many mobile users are there and where do they travel primarily? What about telecommuters? Will a VPN provide adequate access for the remote users?

As you progress through your analysis, discuss your progress with your fellow students or team members and your teacher. This will give you an opportunity to brainstorm what issues you may have overlooked.

Part Three: Network Addressing

As part of your analysis, you should create a network addressing recommendation. Use the same questions presented in Part One of this activity to design a networking scheme for your company.

When you created an addressing scheme for your school, you were working within a closed environment. Creating a scheme that fits around department organization or grade level makes sense in a school setting. However, your company case study may not be a closed environment. Your company may have multiple locations across the United States or even around the world. In such cases, assigning addresses based on geographical location provides several advantages.

- Grouping addresses based on a geographical location makes it easier to detect and resolve routing problems.
 - When a network problem occurs causing an outage, it is usually localized to a specific geographical location.
 - The individual network managers at each location have better control over the network.
1. Write a short explanation of the addressing needs of your case study, including information about the past and the future.
 2. Determine how you will allocate IP addresses and subnet the network. Will you use business functions (departments) or geographical locations for your subnet groups?
 3. Propose an IP addressing scheme for your case study and submit it to your teacher for review.
 4. Incorporate any changes or suggestions that your teacher provides to you and keep your completed scheme in your portfolio for inclusion in your network design proposal.

Rubric: Suggested evaluation criteria and weightings:

Criteria	%	Your Score
Thorough information gathering	25	
Accurate IP addressing appropriately accommodating the needs of the case study	50	
Quality recommendation suitable for reproduction and inclusion in network design proposal	25	
TOTAL	100	

Summary

The Internet Protocol

In this lesson, you learned the following:

- The identification of IP addresses according to their class
- The identification of the network and hosts portions of Class A, B, and C IP addresses
- The advantages of IPv6 over IPv4
- The comparison IP Multicasting with Unicasting and Broadcasting
- The multicasting protocols, IGMP and DVMRP
- How to logically subnet a network and assign IP addresses

Review Questions

The Internet Protocol

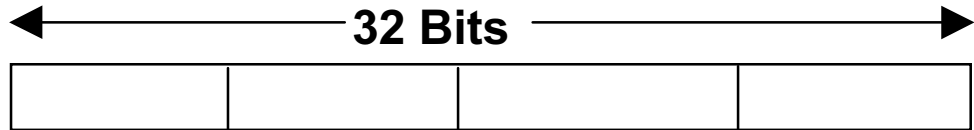
Part A:

1. What is the network address class for 201.45.3.6?
 - a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
2. What is the network address class for 25.0.49.193?
 - a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
3. What is the network address class for 157.128.231.244?
 - a. Class A
 - b. Class B
 - c. Class C
 - d. Class D
4. What is the network address class for 108.235.0.1?
 - a. Class A
 - b. Class B
 - c. Class C
 - d. Class D

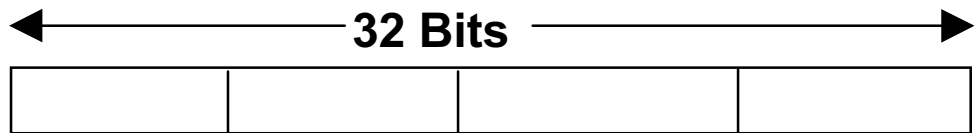
5. What is the network address class for 190.55.3.1?
 - a. Class A
 - b. Class B
 - c. Class C
 - d. Class D

Part B:

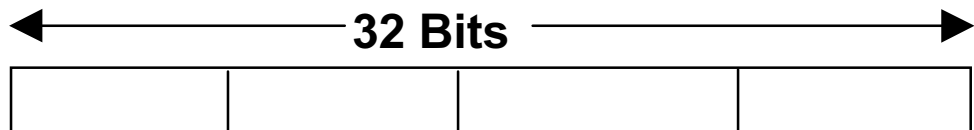
1. Identify the network and host portions of a Class A address by labeling the diagram below.



2. Identify the network and host portions of a Class B address by labeling the diagram below.



3. Identify the network and host portions of a Class C address by labeling the diagram below.



Part C:

Identify each statement as either true (T) or false (F).

1. IPv6 addresses are 128 bits long.

2. IPv4 and IPv6 must use DHCP to automatically assign IP addresses to network devices.

3. The IP header of a packet in IPv6 slows the transmission of a packet because it is very large.

4. The IP header in IPv6 has space for extension where the sender can place customized options.

5. IPv6 extensions include security and authentication options.

6. In IPv6, once an address is assigned to a network device the address becomes unique to that device.

7. IP Multicast is only supported by IPv6.

8. IPv6 uses an anycast address for sending a packet to a single destination within a group by specifying the route.

9. Since the router does not examine the IP header of a packet in IPv4, the header does not slow down the transmission of the packet.

10. IPv6 was developed to resolve the depletion of available addresses using IPv4.

Part D:

Define IP multicasting, unicasting, and broadcasting, and discuss the advantages of multicasting.

Part E:

1. Briefly describe how IGMP is used in IP multicasting.

2. Briefly describe how DVMRP establishes a multicast tree for routing multicast packets.

Scoring

Criteria	%	Your Score
Part A: Identify IP addresses according to their class.	20	
Part B: Identify network and hosts portions of Class A, B, and C IP addresses.	15	
Part C: Identify the advantages of IPv6 over IPv4.	30	
Part D: Compare IP Multicasting with Unicasting and Broadcasting.	15	
Part E: Describe the multicasting protocols, IGMP and DVMRP.	20	
TOTAL	100	
Try It Out:	100	
Stretch Yourself:	100	
Network Wizards: Demonstrate how to logically subnet a network and assign IP addresses.	100	
FINAL TOTAL	400	

Resources:

Deering, S., Hinden, R. (1998). Internet Protocol Version 6 (IPv6) Specification, RFC 2460. Available On-line: <ftp://ftp.isi.edu/in-notes/rfc2460.txt>.

Goncalves, M. (1999). Voice Over IP Networks. New York: McGraw-Hill.

Miller, C.K. (1999). Multicast Networking and Applications. Reading, Massachusetts: Addison Wesley Longman, Inc..

Nortel Networks. (1998). Fundamentals of IP Networking: A Self-study. Billerica, Massachusetts: Nortel Networks.

Nortel Networks. (1997). Voice Fundamentals from Analogue to ATM. Brampton, Ontario: Nortel Networks.

Palmer, M. (1998). Hands on Networking Essentials with Projects. Cambridge: Course Technology.