Microsoft®

Module 2: Assigning IP Addresses in a Multiple-Subnet Network

Contents

Overview	1
Lesson: Configuring IP Addressing for Simple Networks	2
Lesson: Configuring IP Addressing for Complex Networks	13
Lesson: Using IP Routing Tables	25
Lesson: Overcoming the Limitations of the IP Addressing Scheme	35
Lab: Assigning IP Addresses in a Multiple-Subnet Network	47

Instructor Notes

Presentation:
225 minutes

Lab:
15 minutes

This module provides students with the information and skills that they need to construct and assign Internet Protocol (IP) addresses to host computers on a network that is running the suite of Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. IP addresses enable computers running any operating system on any platform to communicate by providing unique identifiers. To send data between multiple subnets, IP must select a route. Understanding the IP routing procedures will assist students in constructing and assigning the appropriate IP addresses for hosts on a network.

After completing this module, students will be able to:

- Explain how to configure IP addressing for simple TCP/IP networks.
- Explain how to configure IP addressing for complex TCP/IP networks.
- Describe routing protocols and how they are used.
- Overcome limitations that are caused by class-based routing.

Required materials

To teach this module, you need the Microsoft® Office PowerPoint® file 2276C_02.ppt.

Important It is recommended that you use PowerPoint 2002 or later to display the slides for this course. If you use PowerPoint Viewer or an earlier version of PowerPoint, some features of the slides might not be displayed correctly.

Preparation tasks

To prepare for this module:

- Read all of the materials for this module.
- Complete the practices.
- Review the referenced RFCs.

How to Teach This Module

This section contains information that will help you to teach this module.

Lesson: Configuring IP Addressing for Simple Networks

This section describes the instructional methods for teaching this lesson.

Multimedia: The Components of an IP Address

This presentation shows how media access control (MAC) addresses are linked to IP addresses to create an efficient addressing scheme for networks. It also explains the different IP address classes and how the length of the network ID and host ID varies in the different classes.

What Is a Subnet Mask?

Use this topic to show students how computers use a subnet mask to calculate the network ID of an IP address. At this point, they do not need to understand binary. Keep the presentation and the level of each octet at 255 or 0. Binary subnet masks are covered in the next lesson.

Multimedia: The Role of Routing in the Network Infrastructure

This presentation shows how routers join subnets together into a network. This discussion includes the difference between local and remote routing, the way routers share network status information, and how gateways and routers interact to send packets to their destination. This media is used to introduce the concept of a default gateway.

What Is a Default Gateway?

Emphasize to students that a default gateway is required whenever more than one network is involved. Mention that this applies even to small networks if they have access to the Internet. Use the Internet as an example of a large network where clients cannot maintain all of their own routing information and need to use a default gateway.

What Are the Classes of IP Addresses?

Emphasize to students that the Internet service provider (ISP) decides which class is appropriate for IP addresses, based on the organization's size, and that only Classes A, B, and C are used for host computers. Emphasize how the first octet identifies the class.

How IP Communication Within a Single Network Works

This topic shows students that on a local network, hosts can deliver packets directly to other hosts without using a default gateway. Be sure that students understand that when calculating whether a destination is local or remote, the sending computer uses only its own subnet mask because it does not know the subnet mask of the destination computer.

How IP Communication Between Networks Works

This topic shows students how packets are delivered between networks by using a router. Emphasize that the source and destination IP addresses remain constant during packet delivery, but that the destination MAC address is the next hop in the path to the destination.

Practice: Configuring IP Addressing for Simple Networks

In this practice, students determine the network ID of an IP address and determine whether two IP addresses are on the same network. Be sure to review answers with the students to ensure that they understand. The next lesson builds on this information.

Lesson: Configuring IP Addressing for Complex Networks

This section describes the instructional methods for teaching this lesson.

How Dotted Decimal Notation Relates to Binary Numbers

Work through the examples in this topic to ensure that students understand the basic concept of binary numbers and how they are converted to dotted decimal notation. Show students how to perform this calculation by using the Calculator. Briefly explain manual conversion.

What Is a Subnet?

Most students should be familiar with the concept of a subnet, so try not to spend too much time on this topic. The main point to reinforce is the concept of subnetting. Review the considerations and steps for creating a subnet, and emphasize that students will base their subnetting implementations on the organization's network requirements.

How Bits Are Used in a Subnet Mask

Use the animated slide to describe the relationship between the number of subnets and the number of hosts. Emphasize to students that in a subnet mask, expressed in binary notation, a 1 represents a bit in the network ID, and a 0 represents a bit in the host ID. Relate this back to the 255 and 0 used in simple networks.

How the Computer Determines Whether an IP Address Is a Local or Remote Address

Many students are not comfortable with binary math. ANDing is the correct term for the binary math that is performed. However, the important thing for students to understand is that a 1 in the subnet mask corresponds with a bit in the network ID and a 0 in the subnet mask corresponds with a bit in the host ID.

Guidelines for Choosing a Subnet Mask

After completing this topic, students should understand how to choose the correct number of bits for their situation using the 2^n–2 formula and be able to calculate subnet IDs. Relate the shortcut method for calculating subnets to the longer binary method. Mention to students that they can download subnet calculators that perform this work without manual calculations.

Practice: Configuring IP Addressing for Complex Networks

In this practice, students convert numbers between binary and decimal, calculate the number of subnets available from a given number of bits, and calculate subnets. Be sure to review the answers with students.

Lesson: Using IP Routing Tables

This section describes the instructional methods for teaching this lesson.

What Is a Router?

Students should already understand that routers move packets between networks. Emphasize that routers work together to deliver packets by maintaining routing tables.

What Are Static and Dynamic Routing?

This topic is included so that students can use static routing if necessary. Point out that, for the most part, they will use dynamic routing. Maintaining static routing is much more work than dynamic routing.

How the IP Protocol Selects a Route

Review the steps outlined here, and use the procedure to review the role of the default gateway.

How IP Uses the Routing Table

In addition to describing the example in this slide, use your computer to demonstrate the IP routing table to students.

Guidelines for Troubleshooting IP Routing by Using the Routing Table

Emphasize to students that the routing table is helpful in isolating some connectivity problems.

Practice: Using IP Routing

In this practice, students will view and modify the IP routing table. Be sure that students do not save changes to the DEN-CL1 virtual machine after this practice or the default gateway will be incorrect.

Lesson: Overcoming the Limitations of the IP Addressing Scheme

This section describes the instructional methods for teaching this lesson.

Multimedia: How IP Addresses Are Wasted

This presentation explains the reason for assigning IP addresses to MAC addresses and shows how the use of default subnet masks can lead to the wasting of registered IP addresses by inefficiently reserving more addresses than an organization will need. It then shows three common strategies for avoiding the inefficient use of IP addresses: private networks, supernets, and variable-length subnet masks (VLSMs). The presentation concludes by introducing the next version of IP, IP version 6 (IPv6), which shipped with Microsoft Windows Server™ 2003 and has limited support in Microsoft Windows® XP Service Pack 1 (SP1). This presentation briefly describes how IPv6 will replace the current version of IP and make vast numbers of addresses available for Internet hosts.

What Are Private and Public IP Addresses?

Emphasize the requirement for registered IP addresses, and ensure that students understand that unregistered private addresses are used only for computers that are not required to be accessible from the Internet. The vast majority of organizations use private IP addresses in conjunction with a proxy or network address translation (NAT).

What Is VLSM?

Ensure that students understand that with VLSM, a network can be divided into different-size subnets. This allows a subnet to be properly sized for the number of hosts required. With VLSM, each subnet can have a different subnet mask.

What Is CIDR?

Explain that classless interdomain routing (CIDR) is used for supernetting and to combine smaller class-based networks into larger networks to reduce the load on routers. This is done on Internet routers.

How CIDR Is Used for Supernetting

Explain supernetting as the reverse of subnetting. The calculations to understand the required number of bits are similar.

What Is IPv6?

Ensure that students understand that increased address space is not the only benefit of IPv6. Eventually, this version will replace IPv4.

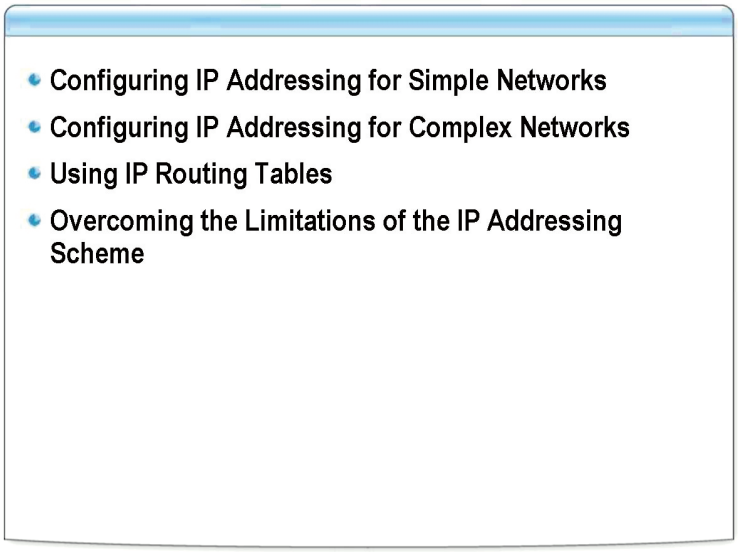
Practice: Overcoming the Limitations of the IP Addressing Scheme

In this practice, students will determine the number of bits required for supernetting and will supernet eight Class C networks. Be sure to review the answers with students.

Lab: Assigning IP Addresses in a Multiple-Subnet Network

Remind the students that they can review the module for assistance in completing the lab. Tell students that a detailed answer key for each lab is provided in the Labdocs folder on the Student Materials compact disc.

Overview



Introduction

This module describes how to construct and assign an Internet Protocol (IP) address to host computers on a network that is running the suite of Transmission Control Protocol/Internet Protocol (TCP/IP) protocols. IP addresses enable computers running any operating system on any platform to communicate by providing unique identifiers. To send data between multiple subnets, IP must select a route. Understanding the IP routing procedures will assist you in constructing and assigning the appropriate IP addresses for hosts on your network.

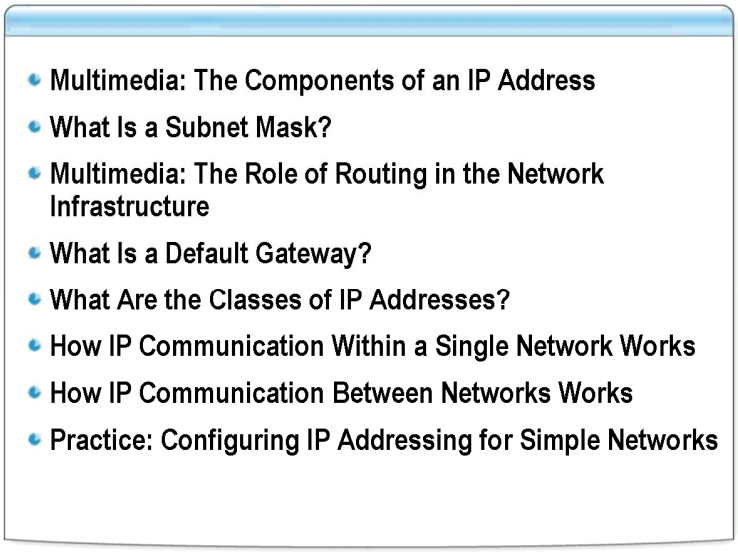
Note In this module, the term *host* refers to any device on the network that has an IP address. The term *client* refers to a computer running a Microsoft® Windows® operating system on a network running TCP/IP.

Objectives

After completing this module, you will be able to:

- Explain how to configure IP addressing for simple TCP/IP-based networks.
- Explain how to configure IP addressing for complex TCP/IP-based networks.
- Describe how routing tables are used.
- Overcome limitations that are caused by class-based routing.

Lesson: Configuring IP Addressing for Simple Networks



Introduction

The primary function of IP is to add address information to data packets and route them across the network. To understand how IP accomplishes this, it is necessary for you to be familiar with the concepts that determine the intermediate and final destination addresses of data packets. Understanding how IP uses address information will enable you to ensure that IP routes data to the correct destination.

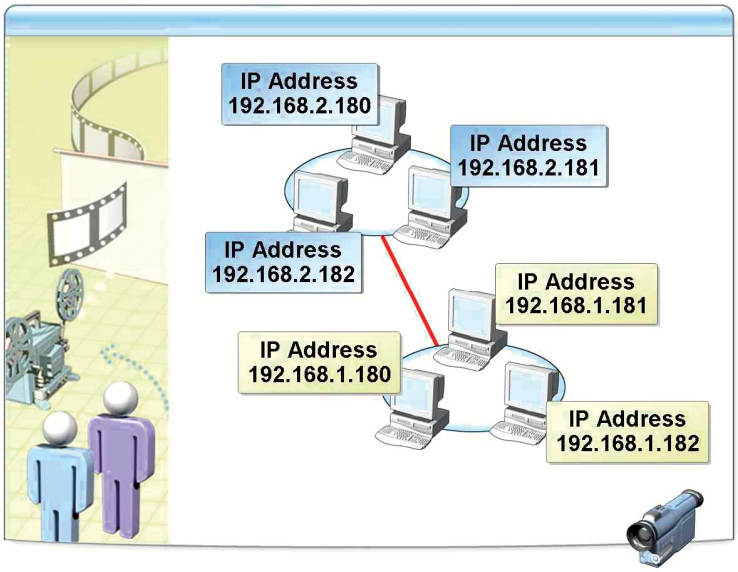
A simple network is one in which IP networks are based on full octets. Basing networks on full octets allows a simple subnet mask composed of only 255s and 0s.

Lesson objectives

After completing this lesson, you will be able to:

- Describe the components of an IP address.
- Describe what a subnet mask is and its purpose.
- Explain how routers are used to move packets between networks.
- Explain what a default gateway is.
- Describe the classes of IP addresses and their characteristics.
- Describe the communication process within a single IP network.
- Describe the communication process between IP networks.
- Perform the calculations that are used in routing between simple networks.

Multimedia: The Components of an IP Address



**********ILLEGAL FOR NON-TRAINER USE**********

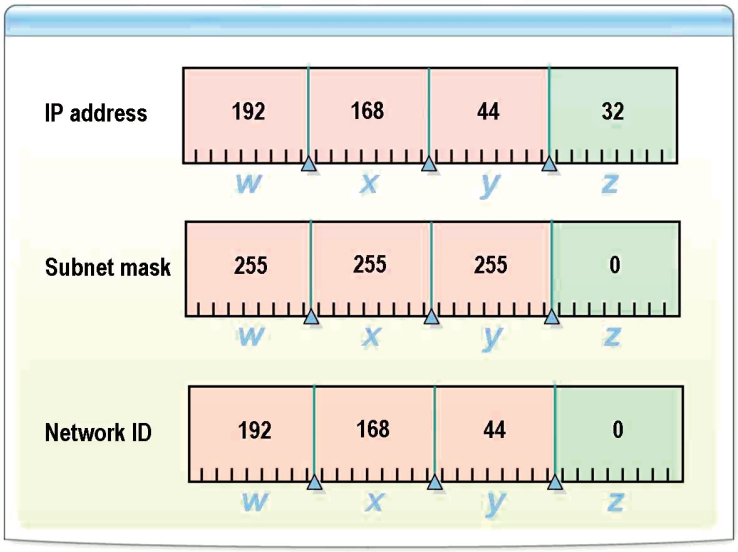
File location

To view the multimedia presentation *The Components of an IP Address*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

After this presentation, you will be able to describe how the numbers in an IP address are grouped to designate network and host addresses.

What Is a Subnet Mask?



Definition

A *subnet mask* defines the part of an IP address that is the network ID and the part of an IP address that is the host ID. A subnet mask is composed of four octets, similar to an IP address.

In simple IP networks, the subnet mask defines full octets as part of the network ID and host ID. A 255 represents an octet that is part of the network ID, and a 0 represents an octet that is part of the host ID. In complex IP networks, octets can be subdivided.

Why a subnet mask is required

When a computer delivers an IP packet, it uses the subnet mask to validate whether the destination is on the same network or on a remote network. If the destination is on the same network, the packet can be delivered by the computer. If the destination is on a different network, the computer must send the packet to a router for delivery.

Valid subnet masks

In a simple IP network, a subnet mask is composed of only 255s and 0s. Other values are not used. In addition, 255s appear at the beginning of the subnet mask and 0s appear at the end. In a valid subnet mask, 0s cannot be interspersed with 255s. Examples of valid and invalid subnet masks are shown in the following table.

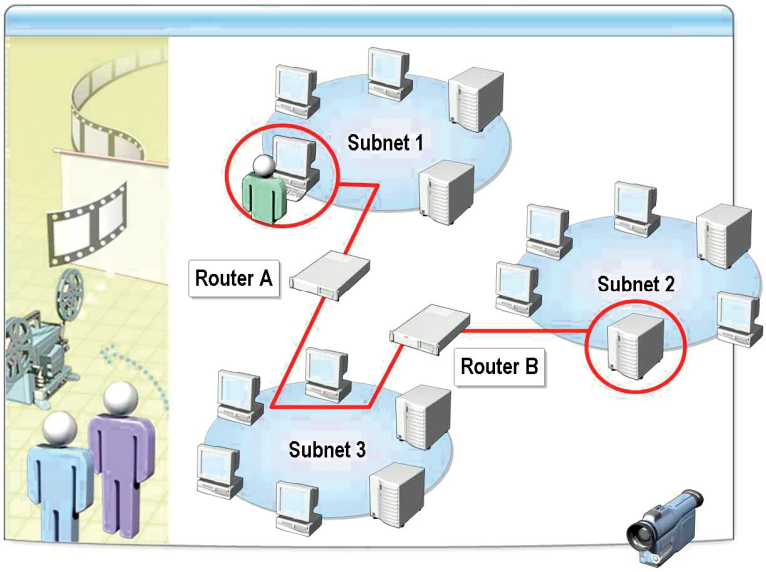
Valid subnet masks	Invalid subnet masks
255.0.0.0	0.0.255.255
255.255.0.0	255.0.255.0
255.255.255.0	0.255.255.0

Calculating the network ID of an IP address

To calculate the network ID of an IP address, the address must be compared to the subnet mask configured on that host. For each octet in the subnet mask that has a value of 255, the corresponding octet of the IP address is part of the network ID. Several examples are shown in the following table.

Description	Example 1	Example 2
IP address	192.168.44.32	172.31.99.220
Subnet mask	255.255.255.0	255.255.0.0
Network ID	192.168.44.0	172.31.0.0
Host ID	0.0.0.32	0.0.99.220

Multimedia: The Role of Routing in the Network Infrastructure



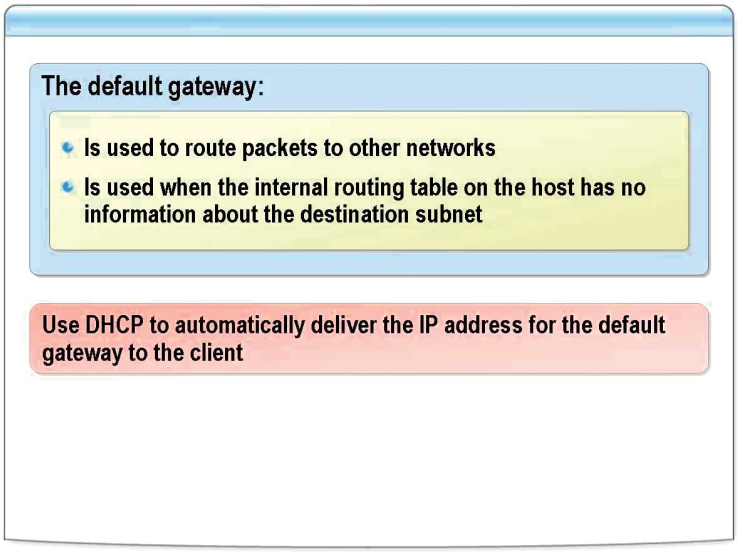
File location

To view the multimedia presentation *The Role of Routing in the Network Infrastructure*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objective

After this presentation, you will be able to describe how IP addresses are used by routers to pass data between networks and subnetworks.

What Is a Default Gateway?



Definition

A *default gateway* is a device, usually a router, on a TCP/IP internetwork that can forward IP packets to other networks. An *internetwork* is a group of networks that are connected by routers. When a host does not have enough information to deliver an IP packet, the host delivers the packet to a default gateway. The default gateway is then responsible for delivering the packet to the destination.

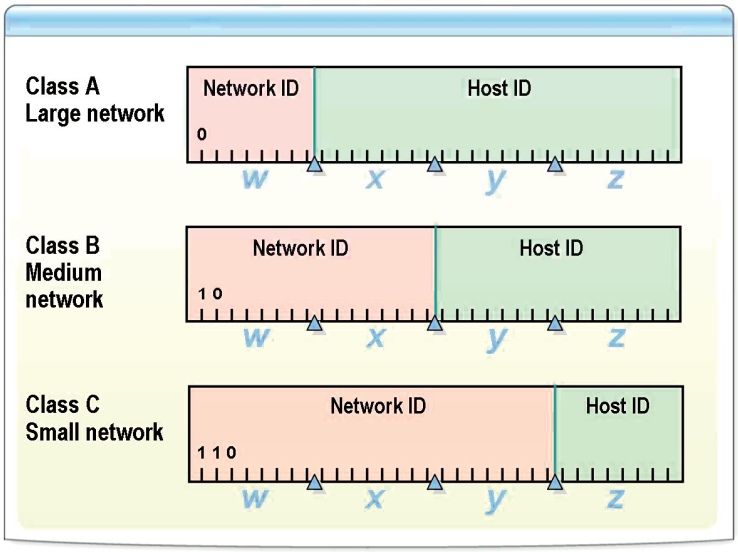
The role of the default gateway

In an internetwork, any given subnet might have several routers that connect it to other subnets, both local and remote. At least one of the routers is configured as the default gateway for the subnet. When a host on the network uses IP to send a packet to a destination subnet, IP consults the internal routing table to determine the appropriate router for the packet to reach the destination subnet. If the routing table does not contain any routing information about the destination subnet, the packet is forwarded to the default gateway. The host assumes that the default gateway contains the required routing information.

How to configure the client for the default gateway

In most cases, the Dynamic Host Configuration Protocol (DHCP) is used to automatically assign a default gateway to a DHCP client. In the event that you need to assign the default gateway manually on clients running Microsoft Windows Server™ 2003, Windows 2000, Windows 98, or Windows 95, you configure the Default Gateway Address property on the General tab in the Network Connections Properties dialog box.

What Are the Classes of IP Addresses?



Introduction

IP addresses are organized into classes. You obtain registered addresses through an Internet service provider (ISP). Your ISP obtains addresses from a Regional Internet Registry. The number of hosts on the network determines the class of addresses that are required.

IP address classes

The IP address classes are named Class A through Class E. Classes A, B, and C are IP addresses that can be assigned to hosts as unique IP addresses. Class D is used for multicasting, and Class E is reserved for experimental use. Packet delivery to Class A, B, and C addresses is referred to as a *unicast*, because the packets are delivered to a single host.

Class A, B, and C networks have a default subnet mask associated with them. This subnet mask defines the portion of the IP address that is used for the host ID. The portion of the address that is used for the host ID determines the number of hosts on a network. The following table lists the characteristics of each IP address class.

Class	First octet	Default subnet mask	Number of networks	Number of hosts per network
A	1–127	255.0.0.0	126	16,777,214
B	128–191	255.255.0.0	16,384	65,534
C	192–223	255.255.255.0	2,097,152	254
D	224–239	n/a	n/a	n/a
E	240–255	n/a	n/a	n/a

Class A

Any IP address in which the first octet has a value between 1 and 127 is a part of a Class A network. There are only 126 available Class A networks, each with up to 16,777,214 hosts.

Because Class A networks are very large, they are allocated to very large organizations. It is no longer possible for individual companies to obtain Class A networks.

Note All IP addresses on the network 127.0.0.0 refer to the local host. The IP addresses on this network are used for diagnostics only.

Class B

An IP address in which the first octet has a value between 128 and 191 is part of a Class B network. There are 16,384 Class B networks, each with up to 65,534 hosts.

Class B networks are assigned to a variety of large companies and universities. For example, the 131.107.0.0 network is allocated to Microsoft Corporation.

Class C

An IP address in which the first octet has a value between 192 and 223 is part of a Class C network. There are 2,097,152 Class C networks, each with up to 254 hosts.

Class C addresses are assigned to many small and medium-size organizations. In some cases, companies are assigned a Class C network for each of their locations.

Class D

Class D addresses are not assigned to individual hosts. Class D addresses are assigned to groups of computers called multicast groups. Using multicast groups is an efficient way to deliver information on a network when multiple hosts need the same information at the same time.

If six computers were receiving a video at the same time, the video would need to be transmitted over the network six times using Class A, B, or C addresses. When multicasting is used, the video is transmitted to the multicast address and received by all six computers in a single transfer.

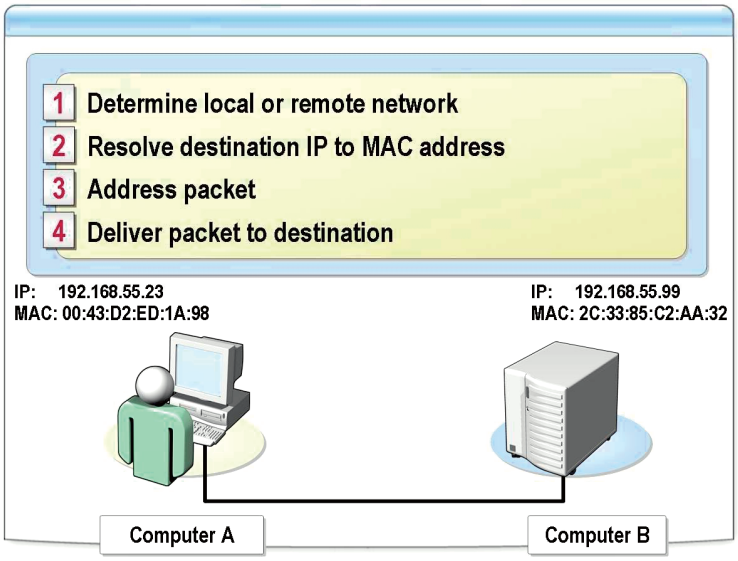
Multicast addresses are typically selected by application developers. The applications use a consistent multicast address each time, and all computers running the application use the same multicast address.

Class E

Class E addresses are reserved for experimental use and are never used on TCP/IP networks except for the broadcast address. The address 255.255.255.255 is a broadcast. Packets addressed to this IP address are delivered to all hosts on the local network.

Broadcasts are used when applications are not configured with the IP address of the host that they should be contacting. For example, DHCP clients use broadcasts to communicate with a DHCP server and obtain an IP address.

How IP Communication Within a Single Network Works



Introduction

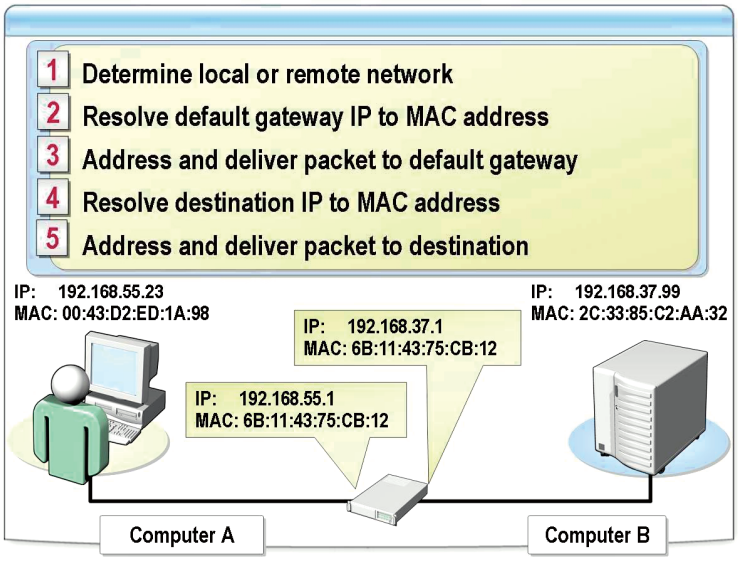
On a single network, each computer can deliver packets to the destination by itself. There is no need for a router to help with packet delivery. The sending computer resolves the destination IP address to a media access control (MAC) address and sends the packet on to the network.

Packet delivery within a single network

The following steps describe how IP communication within a single network works:

1. Computer A uses its own subnet mask to determine that it is on the same network as Computer B.
2. Computer A uses the Address Resolution Protocol (ARP) to resolve the IP address of Computer B to a MAC address.
3. The packet is addressed with the source IP address of Computer A, destination IP address of Computer B, source MAC address of Computer A, and destination MAC address of Computer B.
4. The packet is delivered to Computer B.

How IP Communication Between Networks Works



Introduction

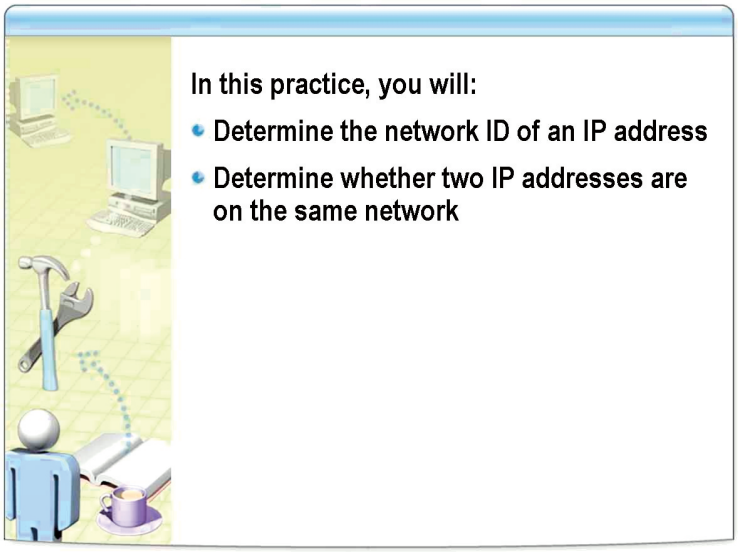
Packets delivered between networks use a default gateway. The default gateway moves packets from one network to another. The sending computer delivers packets to the default gateway, and the default gateway delivers the packets to the destination.

Packet delivery between networks

The following steps describe how IP communication between networks works:

1. Computer A uses its own subnet mask to determine that it is on a different network than Computer B.
2. Computer A uses ARP to resolve the default gateway IP address to a MAC address.
3. The packet is addressed with the source IP address of Computer A, destination IP address of Computer B, source MAC address of Computer A, and destination MAC address of the default gateway. The packet is delivered to the default gateway.
4. The default gateway uses ARP to resolve the IP address of Computer B to a MAC address.
5. The packet is addressed with the source IP address of Computer A, destination IP address of Computer B, source MAC address of the default gateway, and destination MAC address of Computer B. The packet is delivered to Computer B.

Practice: Configuring IP Addressing for Simple Networks



Objectives

In this practice, you will:

- Determine the network ID of an IP address.
- Determine whether two IP addresses are on the same network.

Instructions

No virtual machines are required for this practice.

Practice

► Determine the network ID of an IP address

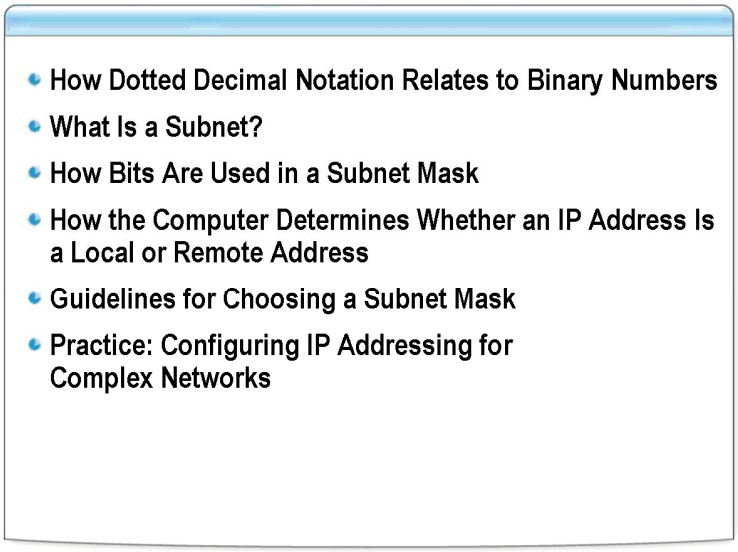
Enter the address class and default subnet mask, and then determine the network ID of the address.

IP address	Address class	Subnet mask	Network ID
10.50.43.222	**A**	**255.0.0.0**	**10.0.0.0**
206.73.118.92	**C**	**255.255.255.0**	**206.73.118.0**
172.29.78.133	**B**	**255.255.0.0**	**172.29.0.0**
239.192.10.5	**D**	**n/a**	**n/a**
157.54.255.2	**B**	**255.255.0.0**	**157.54.0.0**
192.168.200.200	**C**	**255.255.255.0**	**192.168.200.0**

► Determine whether two IP addresses are on the same network

IP address #1	Subnet mask	IP address #2	Same (Y/N)
192.168.22.65	255.255.255.0	192.168.25.200	**No**
10.38.99.10	255.0.0.0	10.208.99.10	**Yes**
192.168.199.208	255.255.255.0	192.168.199.1	**Yes**
172.18.165.36	255.255.0.0	172.31.218.118	**No**

Lesson: Configuring IP Addressing for Complex Networks



Introduction

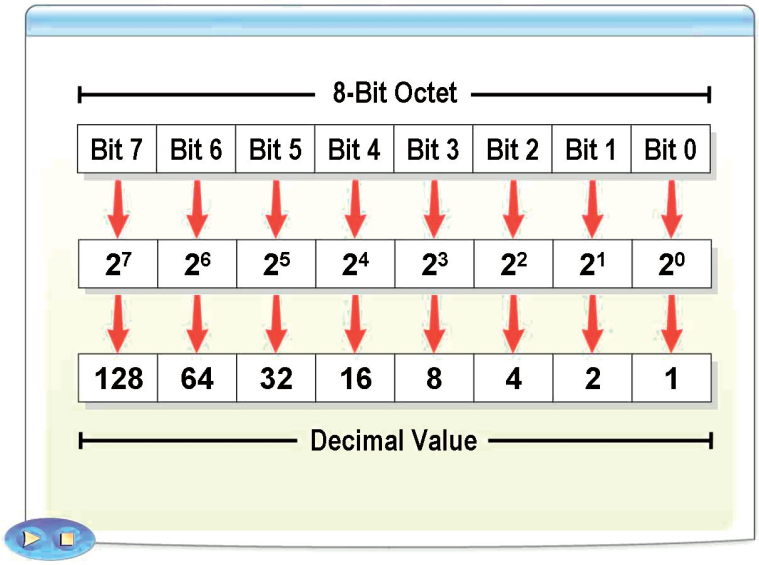
Complex networks are often not able to use the default subnet mask assigned to Class A, B, or C networks. They must be subdivided into smaller networks, called subnets. This lesson describes how to convert dotted decimal notation to binary and calculate the subnet mask for subdivided networks.

Lesson objectives

After completing this lesson, you will be able to:

- Convert an IP address in dotted decimal notation to binary numbers.
- Describe what a subnet is.
- Explain how bits are used in a subnet mask.
- Describe how a computer determines whether an IP address is a local or remote address.
- Apply guidelines for choosing a subnet mask.
- Configure IP addressing for a complex network.

How Dotted Decimal Notation Relates to Binary Numbers



Introduction

When you assign IP addresses, you use dotted decimal notation, which is based on the decimal number system. However, in the background, computers use IP addresses in binary. To understand how to choose a subnet mask for complex networks, you must understand IP addresses in binary.

Within an 8-bit octet, each bit position has an assigned decimal value. A bit that is set to 0 always has a zero value. A bit that is set to 1 can be converted to a decimal value. The low-order bit, the rightmost bit in the octet, represents a decimal value of 1. The high-order bit, the leftmost bit in the octet, represents a decimal value of 128. The highest decimal value of an octet is 255—that is, all bits are set to 1.

Most of the time, you will use a calculator to convert decimal numbers to binary and vice versa. The Calculator application included in Windows is capable of performing decimal-to-binary conversions.

Example of an IP address in binary and dotted decimal formats

The following table shows the binary format and dotted decimal notation of an IP address.

Binary format	Dotted decimal notation
10000011 01101011 00000011 00011000	131.107.3.24

How to calculate the decimal value of a binary number

To calculate the decimal value of a binary representation:

1. Starting with the leftmost digit of the octet, multiply each number in the octet by decreasing powers of 2, beginning with 2^7.
2. Add these values to obtain the number.

   For example, for the number 10000011:

   $1\times2^7 = 1\times128 = 128$

   $0\times2^6 = 0\times64 = 0$

   $0\times2^5 = 0\times32 = 0$

   $0\times2^4 = 0\times16 = 0$

   $0\times2^3 = 0\times8 = 0$

   $0\times2^2 = 0\times4 = 0$

   $1\times2^1 = 1\times2 = 2$

   $1\times2^0 = 1\times1 = 1$

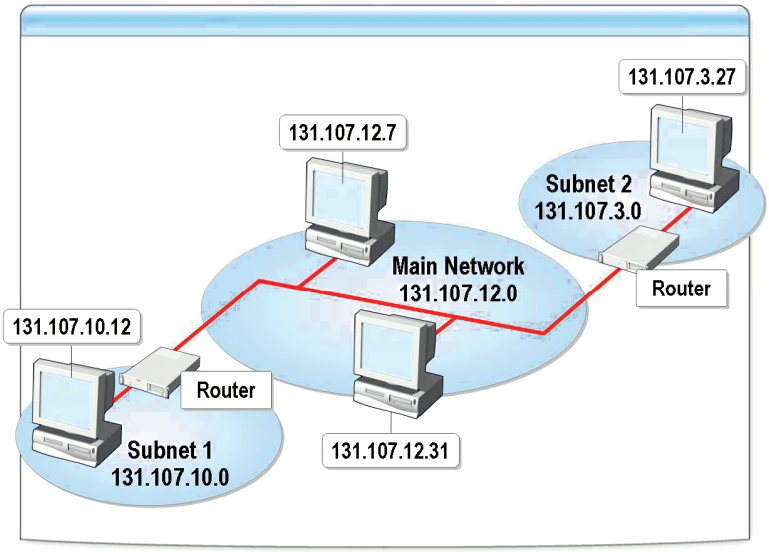
   $128+0+0+0+0+0+2+1 = 131$

Values for converting from binary to decimal

The following table shows the bit values and the decimal values for all the bits in one octet.

Binary format	Bit values	Decimal value
00000000	0	0
00000001	1	1
00000011	2+1	3
00000111	4+2+1	7
00001111	8+4+2+1	15
00011111	16+8+4+2+1	31
00111111	32+16+8+4+2+1	63
01111111	64+32+16+8+4+2+1	127
11111111	128+64+32+16+8+4+2+1	255

What Is a Subnet?



Definition

A *subnet* is a physical segment of a network that is separated from the rest of the network by a router or routers. When a Class A, B, or C network is assigned to your organization, it often must be subdivided to match the physical layout of your network or design specifications. A larger network is subdivided into subnets.

To create subnets, you must allocate some of the bits in the host ID to the network ID. This allows you to create more networks.

Subnet IP addresses

The IP address for each subnet is derived from the main network ID. When you divide a network into subnets, you must create a unique ID for each subnet. To create subnets, you must allocate some of the bits in the host ID to the network ID. This allows you to create more networks. The process of creating subnets is called *subnetting*.

Benefits of using a subnet

Using subnets allows you to:

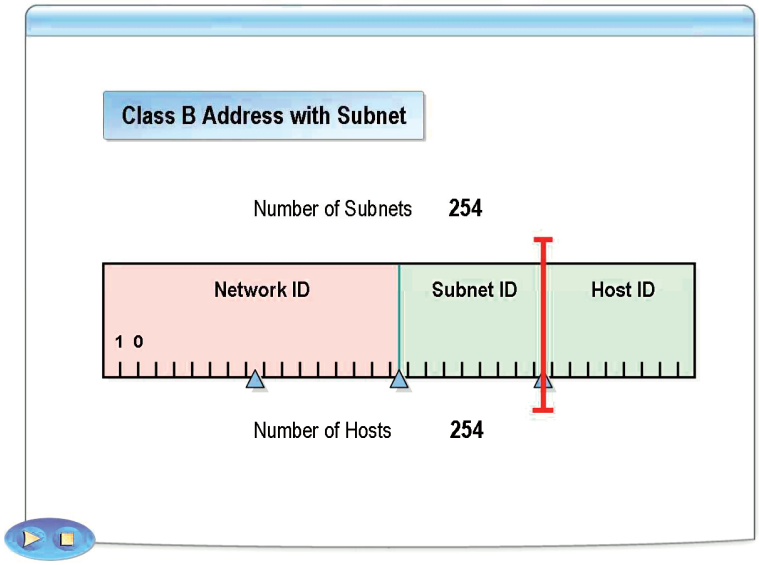
- Use a single Class A, B, or C network across multiple physical locations.
- Reduce network congestion by segmenting traffic and reducing the number of broadcasts that are sent on each segment.
- Overcome limitations of current technologies, such as exceeding the maximum number of hosts allowed per segment. For example, Ethernet is limited to 1024 hosts on a network. Breaking the segment into further segments increases the total number of hosts allowed.

Considerations for creating a subnet

Before you implement subnetting, you must determine your current requirements and take into consideration future requirements so that you can allow for growth. To create a subnet:

1. Determine the number of physical segments on your network.
2. Determine the number of required host addresses for each physical segment. Each interface on the physical segment requires at least one IP address. Typical TCP/IP hosts have a single interface.
3. Based on your requirements as determined in steps 1 and 2, define:
   - One subnet mask for your entire network.
   - A unique subnet ID for each physical segment.
   - A range of host IDs for each subnet.

How Bits Are Used in a Subnet Mask



Introduction

Before you define a subnet mask, you must estimate the number of segments and hosts per segment that you are likely to require in the future. This will enable you to use the appropriate number of bits for the subnet mask.

Using bits in the subnet mask

In simple networks, subnet masks are composed of four octets, and each octet has a value of 255 or 0. If the octet is 255, that octet is part of the network ID. If the octet is 0, that octet is part of the host ID.

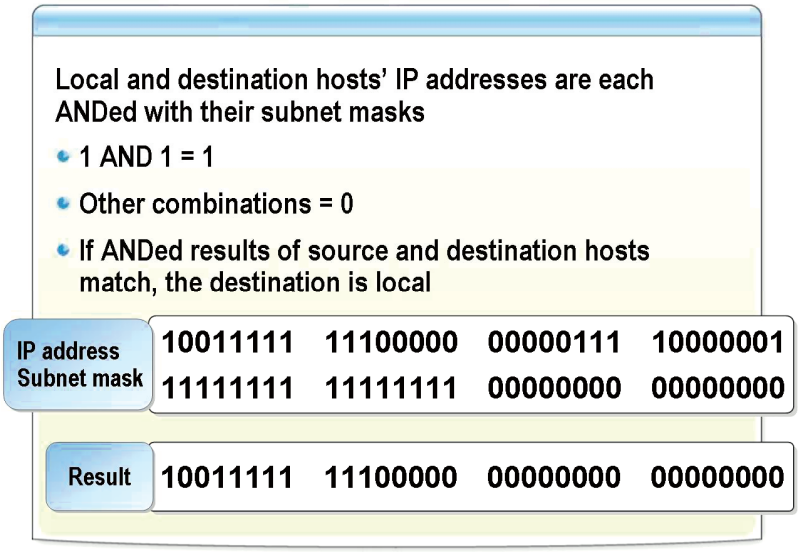
In complex networks, you must convert the subnet mask to binary and evaluate each bit in the subnet mask. A subnet mask is composed of contiguous 1s and 0s. The 1s start at the leftmost bit and continue uninterrupted until the bits change to all 0s.

The network ID of a subnet mask can be identified by the 1s. The host ID can be identified by the 0s. Any bits taken from the host ID and allocated to the network ID must be contiguous with the original network ID. For each bit that is 1, that bit is part of the network ID. For each bit that is 0, that bit is part of the host ID. The mathematical process used to compare an IP address and a subnet mask is called ANDing.

When more bits are used for the subnet mask, more subnets are available, but fewer hosts are available on each subnet. Using more bits than are needed will allow for growth in the number of subnets but will limit growth in the number of hosts. Using fewer bits than are needed will allow for growth in the number of hosts but will limit growth in the number of subnets.

Note For more information about subnetting, see Request for Comments (RFCs) 950 and 1860 under **Additional Reading** on the Student Materials compact disc.

How the Computer Determines Whether an IP Address Is a Local or Remote Address



Introduction

When IP routes a data packet, it must determine whether the destination IP address is on the local network or on a remote network. Understanding how IP makes this determination provides you with the knowledge that you will need when you isolate issues associated with IP addressing.

What is ANDing?

ANDing is the internal process that IP uses to determine whether a packet is destined for a host on a local network or a remote network. It is also used to find routes that match the destination address of packets being sent or forwarded.

When IP forwards a packet to its destination, it must first AND the sending host's IP address with its subnet mask. Before the packet is sent, IP ANDs the destination IP address with the same subnet mask. If both results match, IP recognizes that the packet belongs to a host on the local network. If the results do not match, the packet is sent to an IP router.

How IP ANDs the IP address to a subnet mask

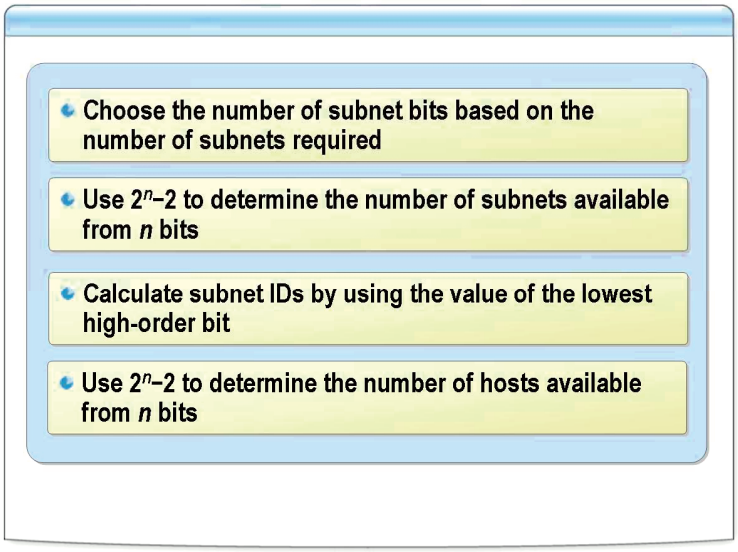
To AND the IP address to a subnet mask, IP compares each bit in the IP address to the corresponding bit in the subnet mask. If both bits are 1s, the resulting bit is 1. If there is any other combination, the resulting bit is 0.

Examples of bit combinations

For combinations of 1 and 0, the results are as follows:

- 1 AND 1 = 1
- 1 AND 0 = 0
- 0 AND 0 = 0
- 0 AND 1 = 0

Guidelines for Choosing a Subnet Mask



Introduction

The process for selecting a subnet mask might seem confusing and complex at first. However, if you understand the process in binary and follow a few simple guidelines, the process is quite easy.

To make the subnetting process even easier, you can use a subnet calculator. A subnet calculator takes the network address and the number of subnets required and creates a list of the appropriate subnets and the subnet mask. Many of these calculators can be found on the Internet by searching for *subnet calculator*.

Choosing the number of bits

The first step in subnetting is selecting the number of bits that must be taken from the host ID and allocated to the network ID. The number of bits in the subnet mask is determined by the number of subnets that are required and the number of hosts that are required on each subnet. It is typical to first calculate subnet bits based on the number of subnets that are required and then confirm that the number of hosts is sufficient. The following examples use this procedure; the procedure can also be used in reverse.

The formula $2^n–2$ calculates the number of subnets that can be created with *n* bits. The value of 2^n calculates the number of combinations that *n* bits can create. Two combinations are removed because class-based networking environments cannot use subnet masks where the subnetted bits are all 1s or all 0s. However, most networking environments are not class-based, and the removal of two subnets is not required. The following table lists the number of subnets available from a given number of bits.

Subnet bits	Calculation	Number of subnets
3	$2^3–2$	8–2 = 6
5	$2^5–2$	32–2 = 30
7	$2^7–2$	128–2 = 126

Calculating subnet IDs

The subnet IDs are calculated by taking every combination of bits possible from the subnet bits and adding them to the original network ID. In the following table, the network 172.20.0.0 is being subnetted using three bits from the host ID. The bolded bits are the subnet bits.

Description	Binary	Decimal
Original network	10101100.00010100.00000000.00000000	172.20.0.0
Original subnet mask	11111111.11111111.00000000.00000000	255.255.0.0
New subnet mask	11111111.11111111.**111**00000.00000000	255.255.224.0
Subnet 1	10101100.00010100.**000**00000.00000000	172.20.0.0
Subnet 2	10101100.00010100.**001**00000.00000000	172.20.32.0
Subnet 3	10101100.00010100.**010**00000.00000000	172.20.64.0
Subnet 4	10101100.00010100.**011**00000.00000000	172.20.96.0
Subnet 5	10101100.00010100.**100**00000.00000000	172.20.128.0
Subnet 6	10101100.00010100.**101**00000.00000000	172.20.160.0
Subnet 7	10101100.00010100.**110**00000.00000000	172.20.192.0
Subnet 8	10101100.00010100.**111**00000.00000000	172.20.224.0

Shortcut to calculating subnet IDs

Using the preceding method is impractical when you are using more than 4 bits for your subnet mask because it requires listing and converting many bit combinations.

To define a range of subnet IDs:

1. List the number of bits in the high order used for the subnet ID. For example, if 3 bits are used for the subnet mask, the binary octet is 11100000.
2. Convert the bit with the lowest value to decimal format. This is the increment value used to determine each successive subnet ID. For example, if you use 3 bits, the lowest value is 32.
3. Starting with 0, increment the value for each successive subnet until you have enumerated the maximum number of subnets.

Determining valid IP addresses

To quickly calculate the number of hosts available on a subnet, you can use the formula $2^n–2$, where n is the number of bits in the host ID. The following table lists the number of hosts available based on the number of bits allocated to the host ID.

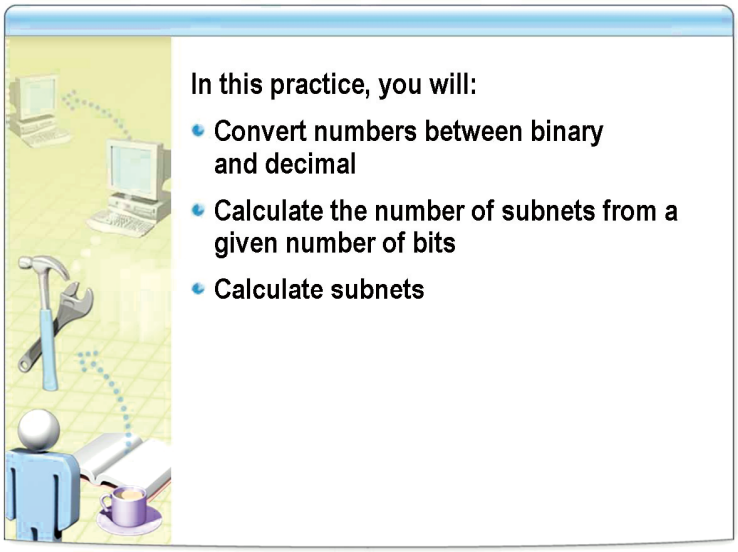
Host ID bits	Calculation	Number of subnets
5	$2^5–2$	32–2 = 30
8	$2^8–2$	256–2 = 254
13	$2^{13}–2$	8192–2 = 8190

Within a subnet, not all combinations of host bits can be used. When all host bits are set to 0, the combination represents the subnet. When all host bits are set to 1, the combination represents a broadcast on that subnet. When the formula 2^n–2 is used to calculate the number of hosts on a subnet, the –2 represents removing the subnet address and the broadcast address.

The following table lists several subnets, the first host on each subnet, the last host on each subnet, and the broadcast address. The bolded bits are the subnet bits.

Description	Binary	Decimal
Original network	10101100.00010100.00000000.00000000	172.20.0.0
Original subnet mask	11111111.11111111.00000000.00000000	255.255.0.0
New subnet mask	11111111.11111111.**111**00000.00000000	255.255.224.0
Subnet 1	10101100.00010100.**000**00000.00000000	172.20.0.0
First host on subnet 1	10101100.00010100.**000**00000.00000001	172.20.0.1
Last host on subnet 1	10101100.00010100.**000**11111.11111110	172.20.31.254
Broadcast on subnet 1	10101100.00010100.**000**11111.11111111	172.20.31.255
Subnet 2	10101100.00010100.**001**00000.00000000	172.20.32.0
First host on subnet 2	10101100.00010100.**001**00000.00000001	172.20.32.1
Last host on subnet 2	10101100.00010100.**001**11111.11111110	172.20.63.254
Broadcast on subnet 2	10101100.00010100.**001**11111.11111111	172.20.63.255

Practice: Configuring IP Addressing for Complex Networks



Objectives

In this practice, you will:

- Convert numbers between binary and decimal.
- Calculate the number of subnets from a given number of bits.
- Calculate subnets.

Instructions

No virtual machines are required for this practice.

Practice

► **Convert numbers between binary and decimal**

1. On your computer, click **Start**, point to **All Programs**, point to **Accessories**, and then click **Calculator**.
2. On the **View** menu, click **Scientific**.
3. If necessary, click **Dec**. This sets the Calculator to decimal mode.
4. Type **255**, and then click **Bin**. You now see the binary value of 255, which is 11111111. Be aware that if there are leading 0s, the Calculator does not display them.
5. Click **C** to clear the display.
6. Type **10011001**, and then click **Dec**. You now see the decimal value of 10011001, which is 153.

► Calculate the number of subnets from a given number of bits

- Using the formula 2^n–2, fill in the following table.

Number of bits	Number of possible subnets
3	**6**
4	**14**
5	**30**
8	**254**

► Calculate subnets

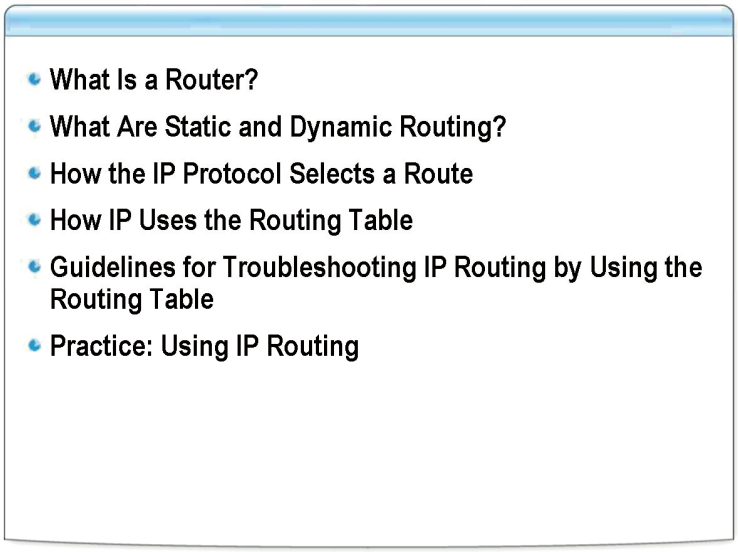
- Fill in the following table and calculate the new subnets.

Description	Binary	Decimal
Original network	10101100.00011101.00000000.00000000	172.29.0.0
Original subnet mask	11111111.11111111.00000000.00000000	255.255.0.0
New subnet mask	11111111.11111111.**1111**0000.00000000	255.255.224.0
Subnet 1	10101100.00011101.**0000**0000.00000000	172.29.0.0
Subnet 2	10101100.00011101.**0001**0000.00000000	172.29.16.0
Subnet 3	10101100.00011101.**0010**0000.00000000	172.29.32.0
Subnet 4	10101100.00011101.**00110000.00000000**	**172.29.48.0**
Subnet 5	10101100.00011101.**01000000.00000000**	**172.29.64.0**
Subnet 6	10101100.00011101.**01010000.00000000**	**172.29.80.0**
Subnet 7	10101100.00011101.**01100000.00000000**	**172.29.96.0**
Subnet 8	10101100.00011101.**01110000.00000000**	**172.29.112.0**
Subnet 9	10101100.00011101.**10000000.00000000**	**172.29.128.0**
Subnet 10	10101100.00011101.**10010000.00000000**	**172.29.144.0**
Subnet 11	10101100.00011101.**10100000.00000000**	**172.29.160.0**
Subnet 12	10101100.00011101.**10110000.00000000**	**172.29.176.0**
Subnet 13	10101100.00011101.**11000000.00000000**	**172.29.192.0**
Subnet 14	10101100.00011101.**11010000.00000000**	**172.29.208.0**
Subnet 15	10101100.00011101.**11100000.00000000**	**172.29.224.0**
Subnet 16	10101100.00011101.**11110000.00000000**	**172.29.240.0**

► Prepare for the next practice

1. Start the DEN-DC1 virtual machine.
2. Start the DEN-CL1 virtual machine.

Lesson: Using IP Routing Tables



Introduction

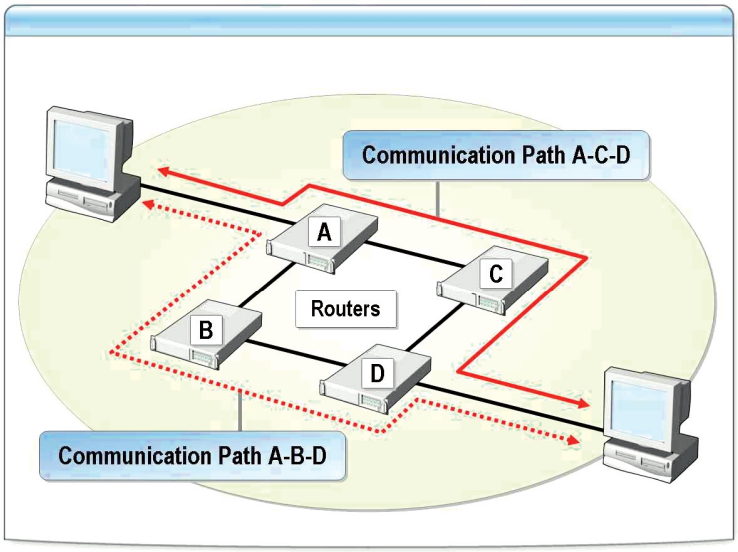
In a multiple-subnet network, routers pass IP packets from one subnet to another. This process is known as *routing* and is a primary function of IP. To make routing decisions, IP consults a routing table. To troubleshoot communication problems, you must understand how routers use routing tables in an internetwork.

Lesson objectives

After completing this lesson, you will be able to:

- Describe what a router is and its role in the network.
- Describe static and dynamic routing.
- Describe how IP selects a route.
- Describe how IP uses the routing table.
- Apply guidelines for troubleshooting IP routing by using the routing table.
- View and configure the routing table.

What Is a Router?



Definition

In an internetwork, a *router* connects subnets to each other and connects the internetwork to other networks. Knowing how the router forwards data packets to their destination IP addresses enables you to ensure that host computers on your network are correctly configured to transmit and receive data.

Routers operate at the network layer of the Open Systems Interconnection (OSI) reference model, so they can connect networks running different data-link layer protocols and different network media.

Example of a router on a small internetwork

On a small internetwork, such as a single location, a router's job can be quite simple. When two local area networks (LANs) are connected by one router, the router receives packets from one network and forwards only those destined for the other network.

Example of routers on a large internetwork

On a large internetwork, such as a 10-site wide area network (WAN), routers connect several different networks together, and in many cases, networks have more than one router connected to them. This enables packets to take different paths to a given destination. If one router on the network fails, packets can bypass it and still reach their destinations.

How routers select a path

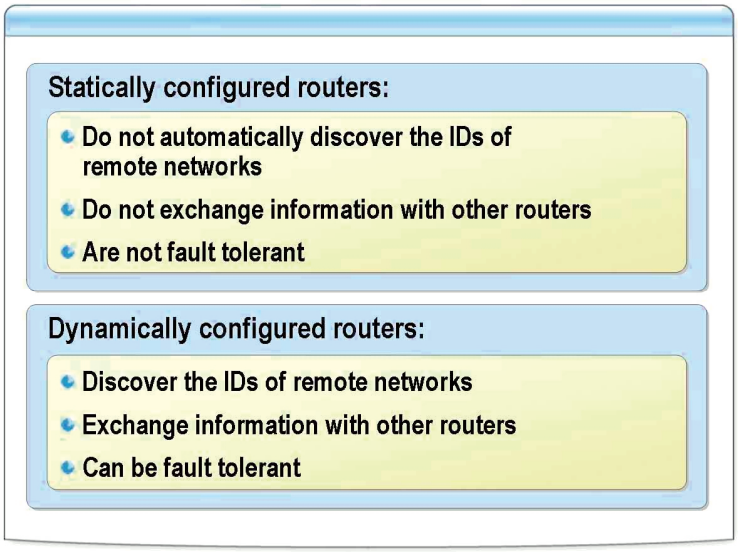
In an internetwork, a router selects the most efficient route to a packet's destination. The most efficient route is the lowest-cost route. Usually, cost is based on hops. (Each time a packet passes through a router is called a *hop*.)

Routers share information about the networks to which they are attached with other routers in the immediate vicinity. As a result, a composite picture of the internetwork eventually develops. On a large internetwork, such as the Internet, no single router possesses the entire image. Instead, the routers work together by passing each packet from router to router, one hop at a time.

How a router moves packets between networks

Routers use the destination IP addresses in packets and routing tables to forward packets between networks. The routing table might contain all the network addresses and possible paths through the network, along with the cost of reaching each network. Routers route packets based on the available paths and their costs.

What Are Static and Dynamic Routing?



Introduction

The process that routers use to obtain routing information differs based on whether the router performs static or dynamic IP routing. Understanding each of these routing methods will give you the information that you need to maintain routing tables so that IP can use the most efficient route to transmit data to its destination.

Static routing

Static routing uses fixed routing tables. Static routers require you to build and update tables manually.

Statically configured routers:

- Do not automatically discover the network IDs of remote networks. You must configure these network IDs manually.
- Do not inform each other of route changes.
- Do not exchange routes with dynamic routers.
- Are not fault tolerant. This means that when the router fails, neighboring routers do not sense the fault and so do not inform other routers.

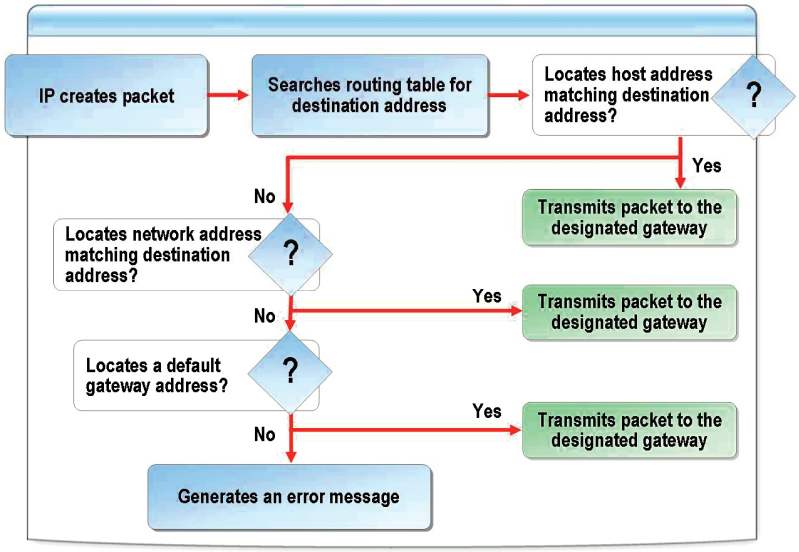
Dynamic routing

Dynamic routing automatically updates the routing tables. Dynamic routing is a function of TCP/IP routing protocols, such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

Dynamically configured routers:

- Can automatically discover the network IDs of remote networks.
- Automatically inform other routers of route changes.
- Use routing protocols to periodically transmit or transmit on demand the contents of their routing tables to the other routers on the network.
- Are fault tolerant (in a multiple-path routing topology). When the router fails, the fault is detected by neighboring routers, which send the changed routing information to the other routers in the internetwork.

How the IP Protocol Selects a Route



Introduction

To send data packets from one network to another, IP must select the appropriate path. When a router receives a packet, the network interface adapter passes the packet to IP. IP examines the destination address and compares it to a routing table. A routing table is a series of entries, called *routes*, that contain information about the location of the network IDs for the internetwork. IP then makes a decision as to how to forward the packet.

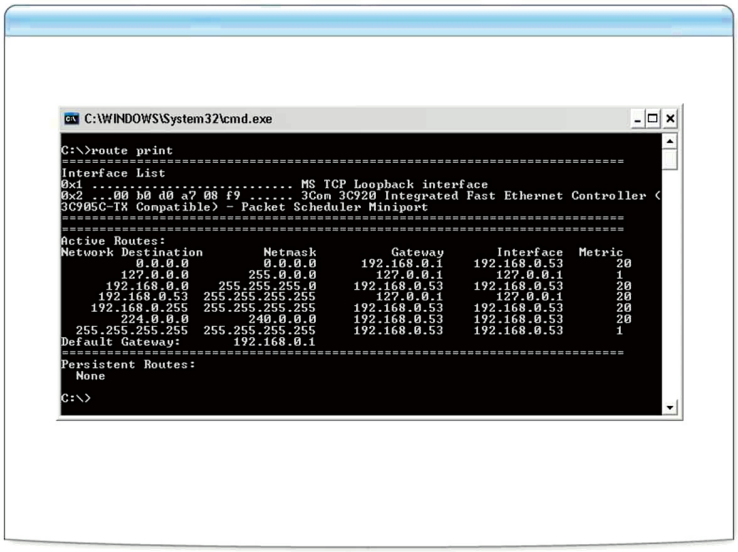
The routing procedure

The IP protocol selects a route by using the following procedure:

1. IP compares the destination IP address for the packet with the routing table entries, looking for a route. A host route in the routing table has the destination IP address in the Network Address column and the value 255.255.255.255 in the Netmask column.
2. If there is no host route for the destination, the system then scans the routing table Network Address and Netmask columns for a network route that matches the destination. If more than one entry in the routing table matches the destination, IP uses the entry with the greatest number of bits set to 1 in the Netmask column. If multiple matching entries in the routing table have the same number of bits set to 1 in the Netmask column, IP uses the entry with the lower value in the Metric column.
3. If there are no network routes to the destination, the system searches for a default gateway entry that has a value of 0.0.0.0 in the Network Address and Netmask columns.
4. If there is no default route, the system generates an error message. If the system transmitting the datagram is a router, it discards the packet and sends an Internet Control Message Protocol (ICMP) Destination Unreachable message back to the end system that originated the datagram. If the system transmitting the datagram is the source host, the error message gets passed back up to the application that generated the data.

5. When the system locates a viable routing table entry, IP passes the forwarding, or *next-hop*, IP address and interface to the ARP module. ARP consults the ARP cache or performs an ARP exchange to obtain the hardware address of the router.
6. After it has the router's hardware address, ARP passes the packet to the network adapter driver for transmission. The network adapter constructs a frame using the router's hardware address in its Destination Address field and transmits the packet.

How IP Uses the Routing Table



**********ILLEGAL FOR NON-TRAINER USE**********

Introduction

To make IP routing decisions, IP consults the routing table, which is stored in memory on a host computer or router. Because all IP hosts perform some form of IP routing, routing tables are not exclusive to IP routers.

How the router uses the routing table

The routing table stores information about IP networks and how they can be reached, either directly or indirectly. There are a series of default entries based on the configuration of the host and additional entries that can be entered either manually, by using TCP/IP utilities, or dynamically, through interaction with routers. When an IP packet is to be forwarded, the router uses the routing table to determine:

- *The next-hop IP address*. For a direct delivery, the forwarding IP address is the destination IP address in the IP packet. For an indirect delivery, the forwarding IP address is the IP address of a router.
- *The interface to be used for the forwarding*. The interface identifies the physical or logical interface, such as a network adapter that is used to forward the packet to either its destination or the next router.

Types of entries in the IP routing table

The following table lists the fields of a route entry and describes the information that they contain.

Route field	Information
Network ID	The network ID or destination corresponding to the route. The ID can be class-based, a subnet, a supernet, or an IP address for a host route. In Windows Server 2003, this is the Network Destination column.
Network mask	The mask used to match a destination IP address to the network ID. In the routing table, this is the Netmask column.
Next hop	The IP address of the next hop. In the routing table in Windows Server 2003, this is the Gateway column.

(*continued*)

Route field	Information
Interface	An indication of which network interface is used to forward the IP packet.
Metric	A number used to indicate the cost of the route so that the best route can be selected. Commonly used to indicate the number of hops to the network ID.

Types of routes

The following table describes the types of routes.

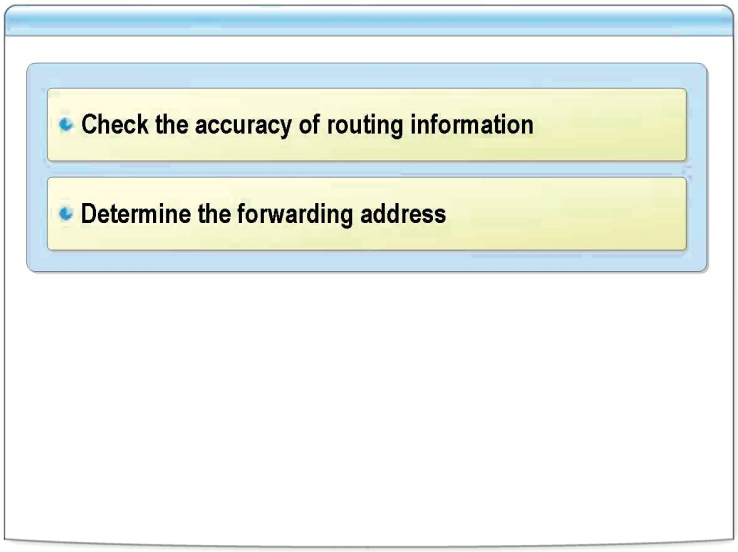
Type of route	Description
Directly attached network ID	A route for network IDs that are directly attached. The Next Hop field can be blank or can contain the IP address of the interface on that network.
Remote network ID	A route for network IDs that are not directly attached but are available across other routers. The Next Hop field is the IP address of a local router.
Host route	A route to a specific IP address. Host routes allow routing to occur on a per-IP-address basis. The network ID is the IP address of the specified host, and the network mask is 255.255.255.255.
Default route	A route that is used when a more specific network ID or host route is not found. The network ID is 0.0.0.0 with a network mask of 0.0.0.0.
Persistent routes	A route added by using the **–p** switch. When used with the Add command, this switch adds the route to the routing table and to the Windows Server 2003 registry. The route is automatically added to the routing table each time TCP/IP is initialized.

The default routing table for a client running Windows Server 2003

The following table shows the default routing table for a client running Windows Server 2003 with a single network adapter, IP address 192.168.0.53, subnet mask 255.255.255.0, and default gateway 192.168.0.1.

Network destination	Net mask	Gateway	Interface	Metric	Purpose
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.53	20	Default route
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	Loopback or testing network
192.168.0.0	255.255.255.0	192.168.0.53	192.168.0.53	20	Directly attached network
192.168.0.53	255.255.255.255	127.0.0.1	127.0.0.1	20	Local host
192.168.0.255	255.255.255.255	192.168.0.53	192.168.0.53	20	Network broadcast
224.0.0.0	240.0.0.0	192.168.0.53	192.168.0.53	20	Multicast
255.255.255.255	255.255.255.255	192.168.0.53	192.168.0.53	1	Limited broadcast

Guidelines for Troubleshooting IP Routing by Using the Routing Table



Introduction

You can use the routing tables in Windows to assist you in isolating connectivity issues. Examining the tables will help you to determine whether an incorrect entry is contributing to a problem.

How to use the table to identify route errors

If the route for a packet sent out by a host is incorrect, the packet will not arrive at its destination, and an error message will be sent to the host. You can examine the routing table to determine the route that was attempted.

To determine the forwarding, or next-hop, IP address from a route in the routing table:

- If the gateway address is the same as the interface address, the forwarding IP address is set to the destination IP address of the IP packet.
- If the gateway address is not the same as the interface address, the forwarding IP address is set to the gateway address.

Examples of matching routes

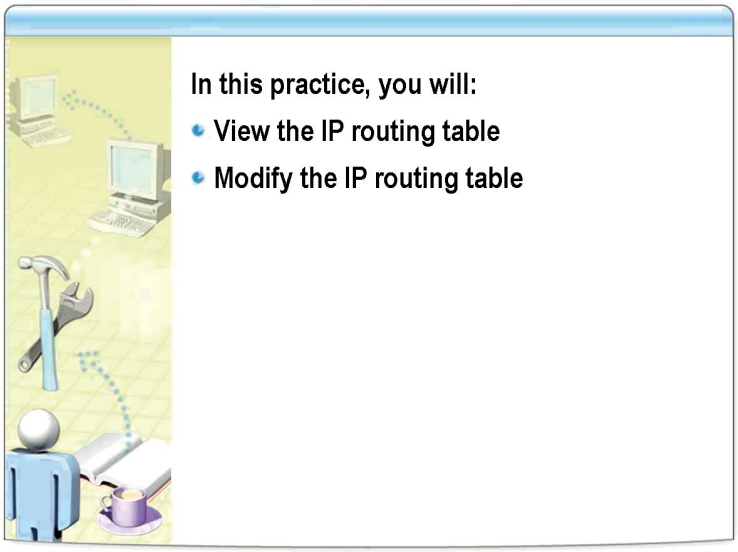
When traffic is sent to 192.168.0.55, the most specific matching route is the route for the directly attached network (192.168.0.0, 255.255.255.0). The forwarding IP address is set to the destination IP address (157.60.16.48), and the interface is the network adapter that has been assigned the IP address 157.60.27.90.

When sending traffic to 131.107.1.100, the most specific matching route is the default route (0.0.0.0, 0.0.0.0). The forwarding IP address is set to the gateway address (192.168.0.1), and the interface is the network adapter that has been assigned the IP address 192.168.0.53.

How to view the IP routing table

To view the IP routing table on a computer running Windows Server 2003, type **route print** at a command prompt. You can also use the **netstat –r** command.

Practice: Using IP Routing



Objectives

In this practice, you will:

- View the IP routing table.
- Modify the IP routing table.

Instructions

Ensure that the DEN-DC1 and DEN-CL1 virtual machines are running.

Practice

► **View the IP routing table**

1. On DEN-CL1, log on to the **CONTOSO** domain as **Administrator**, with a password of **Pa$$w0rd**.
2. Click **Start**, click **Run**, type **cmd**, and then click **OK**.
3. Type **route print** and then press ENTER.

   Are there any persistent routes listed?

   No. No persistent routes have been created.

   The network destination for the default gateway is listed as 0.0.0.0. What is the IP address of the default gateway?

   10.10.0.1.

   ---

4. Type **ipconfig /all**, and then press ENTER.

   What is the IP address of the default gateway?

   10.10.0.1.

► **Modify the IP routing table**

1. Type **route delete 0.0.0.0** and then press ENTER.
2. Type **ipconfig /all** and then press ENTER.

   What is the IP address of the default gateway?

   There is no default gateway listed.

   _____

3. At a command prompt, type **route add 0.0.0.0 mask 0.0.0.0 10.10.0.254** and then press ENTER.
4. At the command prompt, type **ipconfig /all** and then press ENTER.

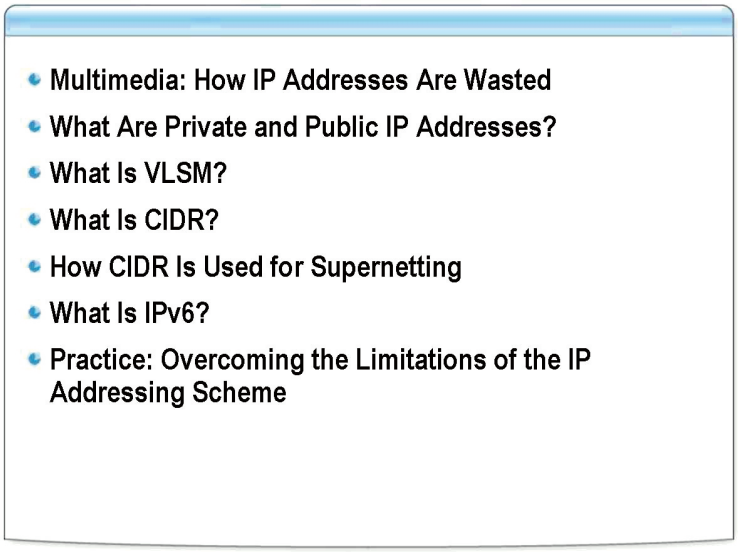
   What is the IP address of the default gateway?

   10.10.0.254.

   _____

Important Shut down DEN-DC1 and DEN-CL1 without saving your changes.

Lesson: Overcoming the Limitations of the IP Addressing Scheme



Introduction

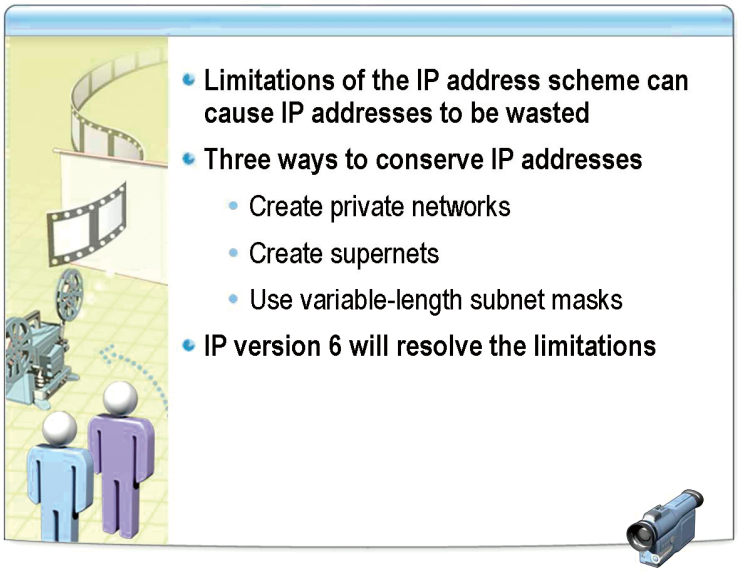
There are limitations of the IP addressing scheme that can prevent you from using the best scheme for your network and that result in a large number of addresses that remain unused. In this lesson, you will learn how you can overcome some of these limitations and increase the effectiveness of your IP addressing scheme.

Lesson objectives

After completing this lesson, you will be able to:

- Describe how IP addresses are wasted.
- Describe private and public IP addresses.
- Describe what variable-length subnet masks (VLSMs) are and how to use them.
- Describe classless interdomain routing (CIDR).
- Describe how CIDR is used for supernetting.
- Explain IP version 6 (IPv6).
- Overcome the limitations of the IP addressing scheme.

Multimedia: How IP Addresses Are Wasted



**********ILLEGAL FOR NON-TRAINER USE**********

File location

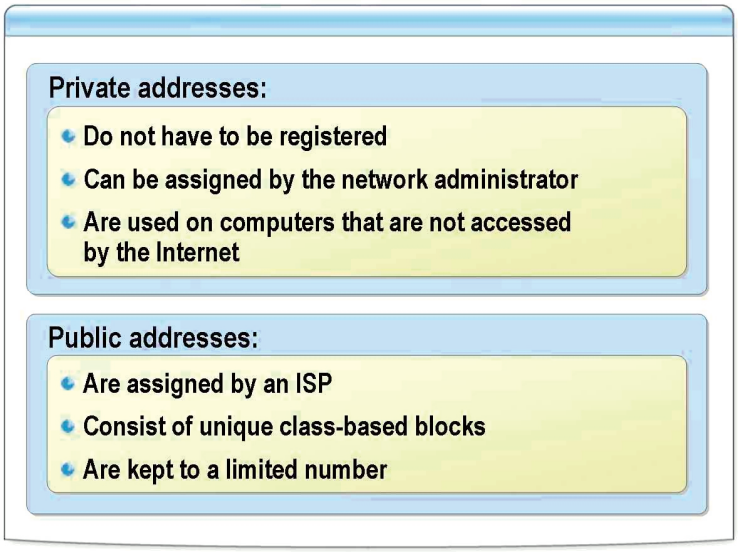
To view the multimedia presentation *How IP Addresses Are Wasted*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objectives

After this presentation, you will be able to describe:

- How the limitations of the IP address scheme can cause IP addresses to be wasted.
- Three ways to conserve IP addresses.

What Are Private and Public IP Addresses?



Introduction

All the computers on your network that are accessible from the Internet require a registered IP address; however, not every computer that can access the Internet requires a registered IP address. You can use private or public IP addresses, depending on network requirements.

Private IP addresses

Private IP addresses are special network addresses that are intended for use on private networks and are not registered to anyone. You can assign these addresses without obtaining them from an ISP. You can use private addresses for computers that are not required to be accessible from the Internet.

Note Networks use a firewall or some other security technology to protect their systems from intrusion by outside computers. These firewalls provide computers with access to Internet resources without making them accessible to other systems on the Internet.

A private IP address is never assigned as a public address and never duplicates public addresses.

IP addresses reserved for private networks

The following IP addresses are reserved for private networks:

- 10.0.0.0 through 10.255.255.255
- 172.16.0.0 through 172.31.255.255
- 192.168.0.0 through 192.168.255.255

Note For more information about private IP addresses, see RFC 1918 under **Additional Reading** on the Student Materials compact disc.

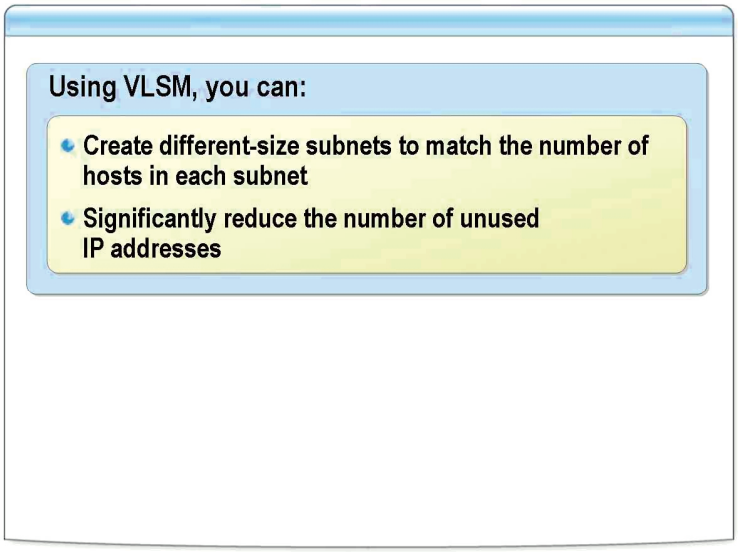
How a host with a private IP address sends requests to the Internet

A host that has a private address must send its Internet traffic requests to an application layer gateway (such as a proxy server) that has a valid public address. Or the host must have network address translation (NAT) to translate the private address into a valid public address and then send its requests to the Internet.

Public addresses

When public addresses are assigned, routes are programmed into the routers of the Internet so that traffic sent to the assigned public addresses can reach those locations. Traffic sent to destination public addresses is transmitted across the Internet.

What Is VLSM?



Definition

VLSM is a method of creating different-size subnet masks to conserve IP addresses. When you use fixed-length subnet masks on an internetwork that has subnets with different requirements for the maximum number of hosts, a large proportion of the addresses might be wasted. By using VLSM, you can allocate the appropriate number of IP addresses to each subnet rather than using fixed-length subnet masks.

How equal-size subnets waste IP addresses

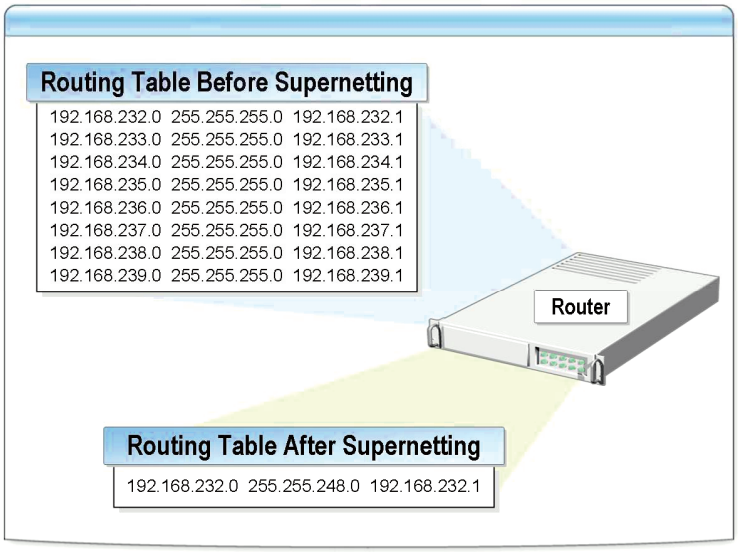
Subnetting was originally used to subdivide a class-based network ID into a series of equal-size subnets. For example, a 4-bit subnetting of a Class B network ID produced 16 equal-size subnets. However, the number of hosts per subnet is rarely if ever of equal size. This inequality results in many wasted IP addresses.

How VLSM conserves IP addresses

Subnetting does not require equal-size subnets, so you can conserve IP addresses by using VLSM to create different-size subnets that best match the number of hosts in each subnet. For example, on a network segmented into three departments, you could subnet a Class C network as follows:

Description	Hosts	Network ID	Subnet mask
Head Office	126	192.168.10.0	255.255.255.128
Department 1	62	192.168.10.128	255.255.255.192
Department 2	62	192.168.10.192	255.255.255.192

What Is CIDR?



Definition

CIDR reduces the size of routing tables by allowing the aggregation of multiple class-based networks into a single routing table entry. This is called *supernetting*.

Why CIDR is required

When class-based routing is used, routers have a routing table entry for each class-based network. This is not a problem on most WANs and LANs, but it is a problem for very large networks such as the Internet. An Internet router could conceivably be forced to track over two million networks.

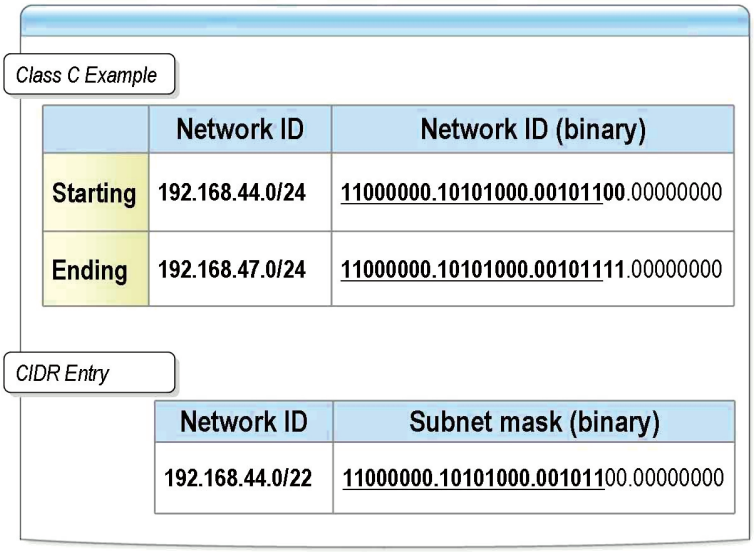
Supernetting is often used to conserve Class B addresses by combining contiguous groups of Class C addresses. The Class C addresses must have the same high-order bits, and the subnet mask is shortened by borrowing bits from the network ID and assigning them to the host ID portion to create a custom subnet mask.

Example of using CIDR for 2000 hosts

When a company has 2000 hosts on its TCP/IP network that must be accessed from the Internet, the company can attempt to obtain the following from an ISP:

- A single Class B network ID. This approach would waste 63,000 addresses.
- Eight different Class C addresses that can support 8 x 254 = 2032 hosts. This means poorer routing performance, because each router requires eight entries in its routing table for each of the eight networks to which packets can be forwarded.
- A single block of addresses that allows 2000 hosts. Using supernetting, an ISP allocates a block of eight contiguous Class C network IDs in such a way that they can be expressed as a single routing table entry.

How CIDR Is Used for Supernetting



Introduction

When you use CIDR to implement supernetting, you are combining multiple addresses into a single network ID, thereby increasing the efficiency of IP address allocation and reducing the number of unused IP addresses.

How CIDR creates the entry for the routing table

To supernet several Class C networks, bits must be taken from the network ID and allocated to the host ID. This is done by modifying the subnet mask.

In the following table, four Class C network IDs are allocated, starting with network ID 192.168.44.0. The bolded bits are the network IDs.

Description	Binary	Decimal
Original network 1	**11000000.10101000.00101100**.00000000	192.168.44.0
Original network 2	**11000000.10101000.00101101**.00000000	192.168.45.0
Original network 3	**11000000.10101000.00101110**.00000000	192.168.46.0
Original network 4	**11000000.10101000.00101111**.00000000	192.168.47.0
Original subnet mask	**11111111.11111111.11111111**.00000000	255.255.255.0
Supernetted network	**11000000.10101000.00101**00.00000000	192.168.44.0
New subnet mask	**11111111.11111111.11111**00.00000000	255.255.252.0
First host	**11000000.10101000.00101**00.00000001	192.168.44.1
Last host	**11000000.10101000.00101**11.11111110	192.168.47.254
Broadcast	**11000000.10101000.00101**11.11111111	192.168.47.255

The first 22 bits of the original Class C network IDs are the same. The last two bits of the third octet vary from 00 to 11. The supernetted network uses only the first 22 bits as part of the network ID.

Note Because subnet masks are used to define supernetting, class-based network IDs must be allocated in groups corresponding to multiples of 2.

CIDR notation

Subnet masks are a fairly cumbersome way of expressing how many bits are in the network ID of an IP address. CIDR notation is a faster way to express the same information. To indicate that 22 bits are part of the network ID, add **/22** after the IP address—for example, **192.168.44.0/22**.

Address-space perspective

The use of CIDR to allocate addresses promotes a new perspective on IP network IDs. The CIDR block 192.168.40.0, 255.255.252.0 can be thought of in two ways:

- As a block of eight Class C network IDs
- As an address space in which 22 bits are fixed and 10 bits are assignable

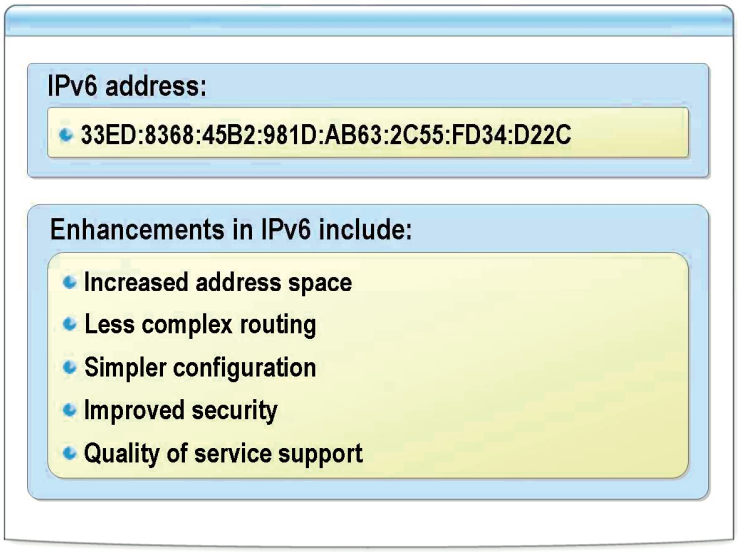
In the latter perspective, IP network IDs lose their class-based heritage and become separate IP address spaces, subsets of the original IP address space defined by the 32-bit IP address. This is the current and correct perspective, as the original Internet address classes have been made obsolete by CIDR.

Each IP network ID (class-based, subnetted, or CIDR block) is an address space in which certain bits are fixed (the network ID bits) and certain bits are variable (the host bits). The host bits are assignable as host IDs or, by using subnetting techniques, can be used in whatever manner best suits the needs of the organization.

Requirements for using CIDR

For routers to support CIDR, they must be able to exchange routing information in the form of network ID–network mask pairs. RIP for IP version 2, OSPF, and Border Gateway Protocol version 4 (BGPv4) are routing protocols that support CIDR. RIP for IP version 1 does not support CIDR.

What Is IPv6?



Definition

IP version 6 (IPv6) is an enhanced network-layer protocol that replaces IPv4, which is currently used in most TCP/IP networks. The most obvious change in IPv6 is the size of the address. IPv6 uses 128-bit addresses that are expressed in hexadecimal. An example of an IPv6 address is 33ED:8368:45B2:981D:AB63:2C55:FD34:D22C.

IPv6 improvements

IPv6 offers a number of improvements over IPv4, including the following:

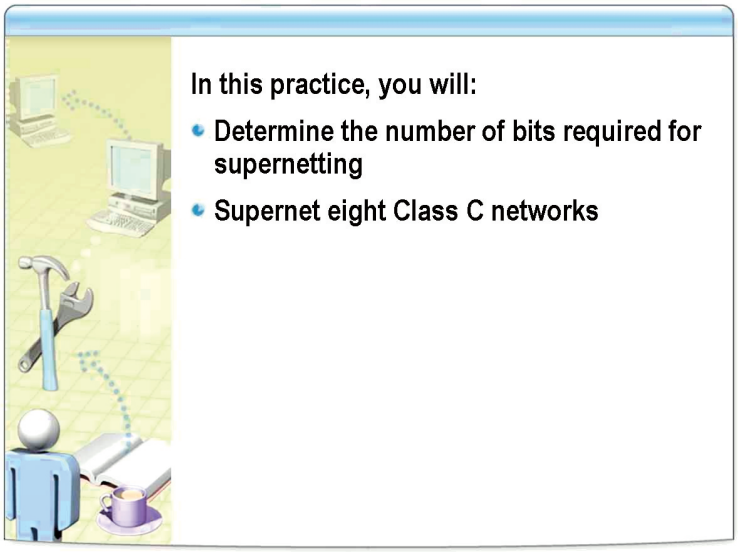
- *IPv6 has increased address space*. By using a 128-bit address instead of the 32-bit addresses of IPv4, the number of available addresses is increased millions of times. This will eliminate IP shortages on the Internet and allow every computer, and other devices, to have a unique Internet addressable IP address. NAT will no longer be required to work around IP shortages.
- *IPv6 routing is less complex*. The Internet currently uses a mix of class-based and classless routing, which increases routing complexity. IPv6 does not have address classes and will reduce routing complexity on the Internet.
- *IPv6 configuration is simpler*. IPv6 addresses can be assigned to hosts automatically without implementing DHCP. Automatic address assignment is built in to the protocol.
- *IPv6 is more secure*. IPv6 is designed to allow secure communication by using Internet Protocol Security (IPSec). Current implementations of IPSec on IPv4 are options and sometimes interoperate poorly.
- *IPv6 supports quality of service*. Quality of service (QOS) for IPv4 is optional and has limited functionality. In IPv6, QOS is built into the protocol.

IPv6 implementation

Implementation of IPv6 on the Internet and on corporate networks has been slow. This is for several reasons:

- Wide use of NAT for corporate environments has reduced the need for additional IP addresses.
- The return of unused IP addresses from organizations has resulted in more efficient use of IPv4 addresses.

Practice: Overcoming the Limitations of the IP Addressing Scheme



Objectives

In this practice, you will:

- Determine the number of bits required for supernetting.
- Supernet eight Class C networks.

Instructions

No virtual machines are required for this practice.

Practice

► **Determine the number of bits required for supernetting**

- Using the formula 2^n, fill in the following table.

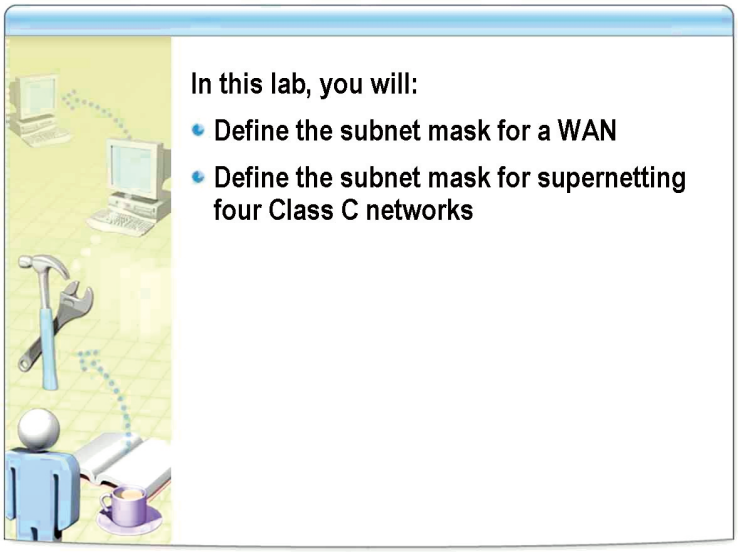
Number of bits	Number of subnets
1	**2**
2	**4**
3	**8**
5	**32**

► Supernet eight Class C networks

- Fill in the following table and calculate the new network, first host, last host, and broadcast addresses.

Description	Binary	Decimal
Original network 1	**11000000.10101000.11101000**.00000000	192.168.232.0
Original network 2	**11000000.10101000.11101001**.00000000	192.168.233.0
Original network 3	**11000000.10101000.11101010**.00000000	192.168.234.0
Original network 4	**11000000.10101000.11101011**.00000000	192.168.235.0
Original network 5	**11000000.10101000.11101100**.00000000	192.168.236.0
Original network 6	**11000000.10101000.11101101**.00000000	192.168.237.0
Original network 7	**11000000.10101000.11101110**.00000000	192.168.238.0
Original network 8	**11000000.10101000.11101111**.00000000	192.168.239.0
Original subnet mask	**11111111.11111111.11111111**.00000000	255.255.255.0
New subnet mask	**11111111.11111111.11111**000.00000000	255.255.248.0
New network	**11000000.10101000.11101**000.00000000	**192.168.232.0**
First host	**11000000.10101000.11101.00000001**	**192.168.232.1**
Last host	**11000000.10101000.11101.11111110**	**192.168.239.254**
Broadcast	**11000000.10101000.11101.11111111**	**192.168.239.255**

Lab: Assigning IP Addresses in a Multiple-Subnet Network



Objectives

After completing this lab, you will be able to:

- Define the subnet mask for a WAN.
- Define the subnet mask for supernetting four Class C networks.

Estimated time to complete this lab: 15 minutes

Exercise 1
Defining the Subnet Mask for a WAN

Your company is designing an integrated WAN for eight locations using a Class B network (172.23.0.0). The IP structure for the WAN should include room for future growth of at least four additional locations and maximize the number of hosts on each subnet. Each location must have its own subnet. Use the following table to define the subnets.

Description	Binary	Decimal
Original network	**10101100.00010111**.00000000.00000000	172.23.0.0
Original subnet mask	**11111111.11111111**.00000000.00000000	255.255.0.0
New subnet mask		
Subnet 1		
Subnet 2		
Subnet 3		
Subnet 4		

Exercise 2
Defining the Subnet Mask for Supernetting Four Class C Networks

Your company has been assigned four Class C networks for a single location. To reduce complexity on your network, you have decided to combine all four networks into a single supernetted network. Use the following table to define the subnet mask, network ID, first host, last host, and broadcast addresses for the supernetted network.

Description	Binary	Decimal
Original network 1	**11000000.10101000.11001100**.00000000	192.168.204.0
Original network 2	**11000000.10101000.11001100**.00000000	192.168.205.0
Original network 3	**11000000.10101000.11001100**.00000000	192.168.206..0
Original network 4	**11000000.10101000.11001100**.00000000	192.168.207.0
Original subnet mask	**11111111.11111111.11111111**.00000000	255.255.255.0
Supernetted network		
New subnet mask		
First host		
Last host		
Broadcast		