
Module 2: Assigning IP Addresses in a Multiple Subnet Network

Contents

Overview	1
Lesson: Assigning IP Addresses	2
Lesson: Creating a Subnet	19
Lesson: Using IP Routing Tables	29
Lesson: Overcoming Limitations of the IP Addressing Scheme	45



Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2003 Microsoft Corporation. All rights reserved.

Microsoft, MS-DOS, Windows, Windows NT, Active Directory, Microsoft Press, MSDN, PowerPoint, and Windows Media are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Instructor Notes

Presentation:
160 minutes**Lab:**
00 minutes

This module provides students with the information and skills 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/IP (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:

- Convert IP address from decimal notation to binary format.
- Create a subnet.
- Calculate a subnet mask.
- Use an IP routing table.
- Reduce the number of unused IP addresses.
- Implement supernetting.

Required materials

To teach this module, you need the Microsoft® PowerPoint® file 2276A_02.ppt.

Preparation tasks

To prepare for this module:

- Read all of the materials for this module.
- Complete the practices.
- Review the referenced Request for Comments (RFCs).

How to Teach This Module

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

Lesson: Assigning IP Addresses

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 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 high order bits define the class.

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 use dotted decimal notation.

How to Convert Dotted Decimal Notation to Binary Format

Emphasize to students that, although they can use a calculator to do the conversions, it is helpful to them if they can calculate the conversion manually.

Multimedia: How Subnet Masks Work

This presentation shows how a subnet mask defines which part of an IP address defines the host ID and which part defines the network ID. It also illustrates the importance of understanding how binary numbers are used in defining a subnet mask.

Lesson: Creating a Subnet

This section describes the instructional methods for teaching this lesson.

What Is a Subnet?

Most students will be familiar with the concept of a subnet, so do not 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 the requirements they must follow when they create a subnet mask.

Defining Subnet IDs

Review the longer process for defining subnet identifiers (IDs) before you discuss the shortcut. This will assist students in understanding how the shortcut works.

Practice: Calculating the Subnet Mask

Review the scenario and work through the practice for any students who are having difficulties. Explain that you must take numbers from the host ID for the subnet ID.

Lesson: Using IP Routing Tables

This section describes the instructional methods for teaching this lesson.

Multimedia: The Role of Routing in the Network Infrastructure

This presentation shows how routers join subnets together into a network. This 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 destinations.

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

The main emphasis of this topic is the concept of ANDing (doing a bitwise comparison), so make sure that students understand how it works. Tell students that the logic behind the concept of ANDing is that 1 = true, 0 = false, and true is only true when combined with true; therefore, one is only one when combined with one.

Practice: Determining Whether an IP Address Is a Local or Remote Address

Review the scenario and work through the practice for any students who are having difficulties.

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.

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 the Routing Table Forwards Packets

Use your computer to demonstrate the IP routing table to students.

Using the Routing Table in Windows Server 2003

Emphasize to students that the routing table will be crucial in helping them to isolate connectivity issues.

Lesson: Overcoming 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. The strategies are: private networks, supernets, and variable length subnet masks. The presentation finishes by introducing the next version of IP, IP version 6, which will ship in Microsoft Windows® Server 2003 and has limited support in Windows XP SP1. The media 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 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.

What Is Supernetting?

Emphasize to students that supernetting conserves IP addresses and is used for large networks.

Using CIDR to Implement Supernetting

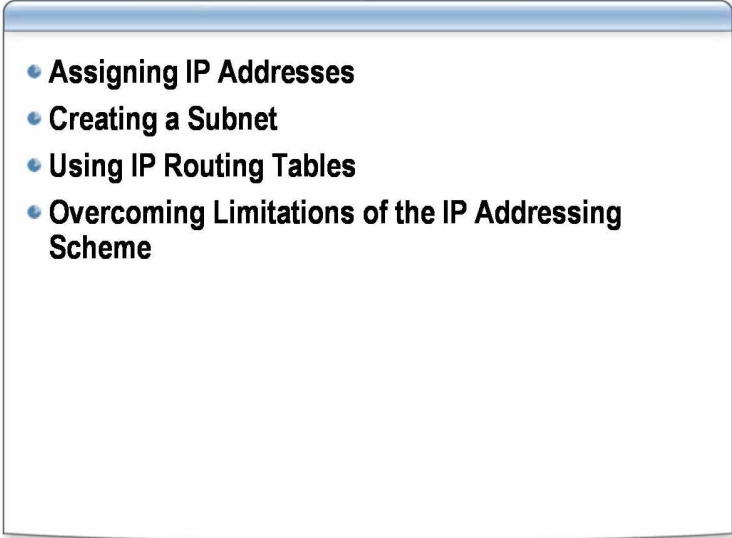
Review the example and make sure students understand how Classless Inter-Domain Routing (CIDR) creates the entry for the block of addresses.

Customization Information

This section identifies the lab setup requirements for a module and the configuration changes that occur on student computers during the labs. This information is provided to assist you in replicating or customizing Microsoft Official Curriculum (MOC) courseware.

There are no labs in this module, and as a result, there are no lab setup requirements or configuration changes that affect replication or customization.

Overview

- 
- Assigning IP Addresses
 - Creating a Subnet
 - Using IP Routing Tables
 - Overcoming Limitations of the IP Addressing Scheme

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

Introduction

The information in 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/IP (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.

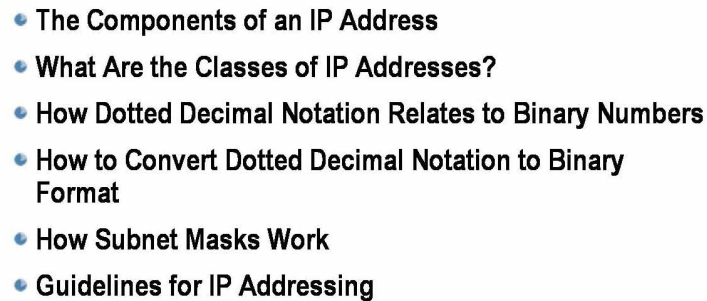
Note In this module, the term *host* refers to any device on the network that has an IP address. The term *client* refers to a computer running a Microsoft® Windows® operating system on a network running TCP/IP.

Objectives

After completing this module, you will be able to:

- Convert IP address from decimal notation to binary format.
- Construct and assign IP addresses.
- Create a subnet.
- Calculate a subnet mask.
- Use an IP routing table.
- Reduce the number of wasted IP addresses.
- Implement supernetting.

Lesson: Assigning IP Addresses

- 
- The Components of an IP Address
 - What Are the Classes of IP Addresses?
 - How Dotted Decimal Notation Relates to Binary Numbers
 - How to Convert Dotted Decimal Notation to Binary Format
 - How Subnet Masks Work
 - Guidelines for IP Addressing

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

Introduction

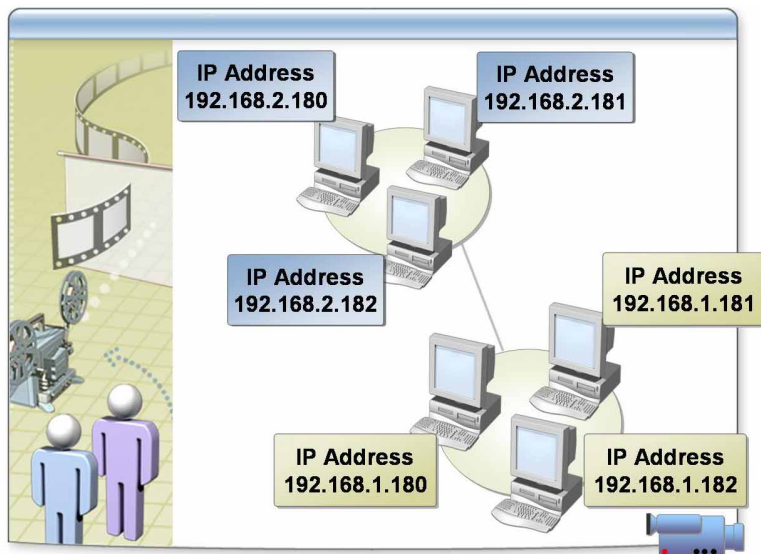
The primary function of IP is to add address information to data packets and route them across the network. To understand how IP accomplishes this, it is necessary for you to be familiar with the concepts that determine the intermediate and final destination addresses of data packets. Understanding how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

Lesson objectives

After completing this lesson, you will be able to:

- Describe the components of an IP address.
- Describe the IP address classes.
- Convert dotted decimal notation to binary numbers.
- Describe how subnet masks work.
- Assign an IP address.

Multimedia: The Components of an IP Address



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

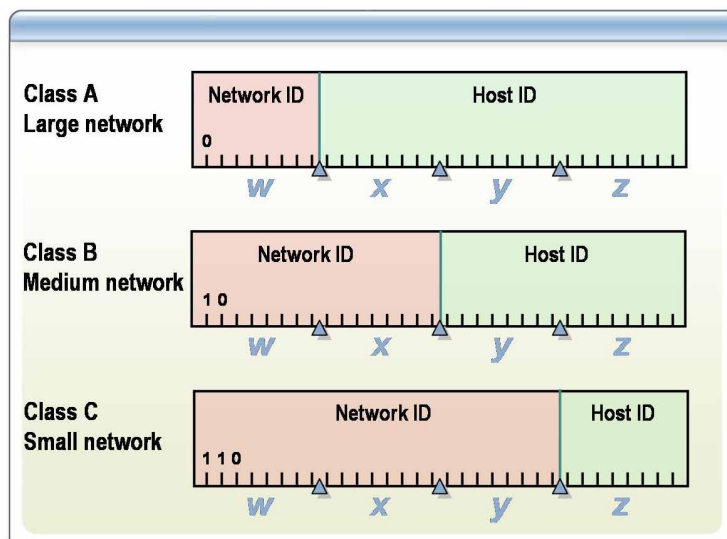
File location

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

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

What Are the Classes of IP Addresses?



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

Introduction

IP addresses are organized into classes. You obtain registered addresses through an Internet service provider (ISP) or the Internet Assigned Numbers Authority (IANA). The size and type of the network determines the address class.

IP address classes

The class of address defines which bits are used to identify the network, the network ID, and which bits are used to identify the host computer, the host ID. It also defines the possible number of networks and the number of hosts per network. There are five classes of IP addresses: classes A through E. TCP/IP in Windows Server 2003, and all previous versions of Windows, supports host address assignment for classes A, B, and C.

Network and host ID fields

The four octets that make up an IP address are conventionally represented by w, x, y, and z respectively. The following table shows how the octets are distributed in classes A, B, and C.

Class	IP address	Network ID	Host ID
A	w.x.y.z	w	x.y.z
B	w.x.y.z	w.x	y.z
C	w.x.y.z	w.x.y	z

Class A

Class A addresses are assigned to networks with a large number of hosts. Class A allows for 126 networks by using the first octet for the network ID. The first, or high-order bit in this octet, is always set to zero. The next seven bits in the octet complete the network ID. The 24 bits in the remaining octets represent the host ID, allowing for 126 networks and approximately 17 million hosts per network. Class A network number values *for w* begin at 1 and end at 127.

Class B

Class B addresses are assigned to medium-sized to large-sized networks. Class B allows for 16,384 networks by using the first two octets for the network ID. The two high-order bits in the first octet are always set to 1 0. The remaining 6 bits, together with the next octet, complete the network ID. The 16 bits in the third and fourth octet represent the host ID, allowing for approximately 65,000 hosts per network. Class B network number values *for w* begin at 128 and end at 191.

Class C

Class C addresses are used for small local area networks (LANs). Class C allows for approximately 2 million networks by using the first three octets for the network ID. The three high-order bits in a class C address are always set to 1 1 0. The next 21 bits in the first three octets complete the network ID. The 8 bits of the last octet represent the host ID allowing for 254 hosts per network. Class C network number values for *w* begin at 192 and end at 223.

Classes D and E

Classes D and E are not allocated to hosts. Class D addresses are used for multicasting, and Class E addresses are not available for general use: they are reserved for future use.

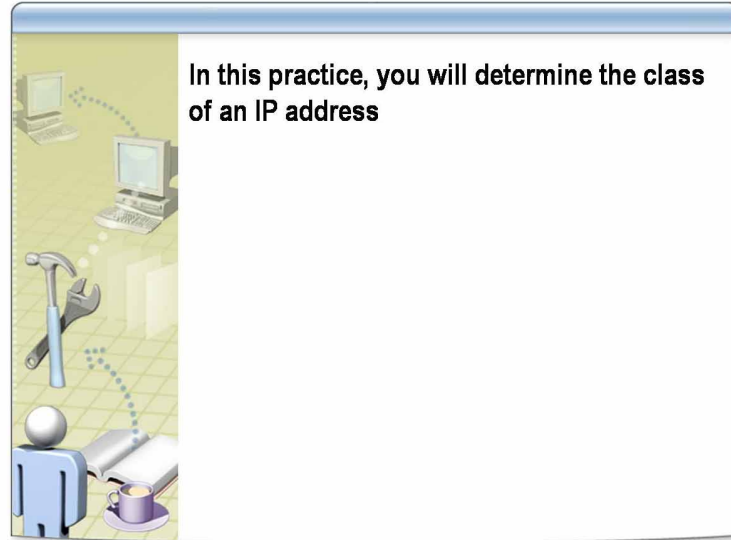
Using a default subnet mask

When classes are used for IP addresses, every address class has a default subnet mask. When you divide a network into segments, or subnets, you can use the default subnet mask for the class to divide the network IP address. All TCP/IP hosts require a subnet mask, even on a single-segment network. The default subnet mask you will use depends on the address class. All bits that correspond to the network ID are set to 1. The decimal value in each octet is 255. All bits that correspond to the host ID are set to 0.

The following table describes the bit values and number of networks and hosts for the A, B, and C address classes.

Class	First Bits	First Byte Values	Network ID bits	Host ID bits	Number of networks	Number of hosts
A	0	1-127	8	24	126	16,777,214
B	10	128-191	16	16	16,384	65,534
C	110	192-223	24	8	2,097,152	254

Practice: Determining the Class of an IP Address



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

Objective In this practice, you will determine the address class for several IP addresses.

Practice

► Determine the class of each IP Address

1. Write the address class next to each IP address.

Address	Class
172.16.2.1	B
10.15.7.100	A
192.168.0.100	C
126.0.0.1	A
1.1.1.1.	A

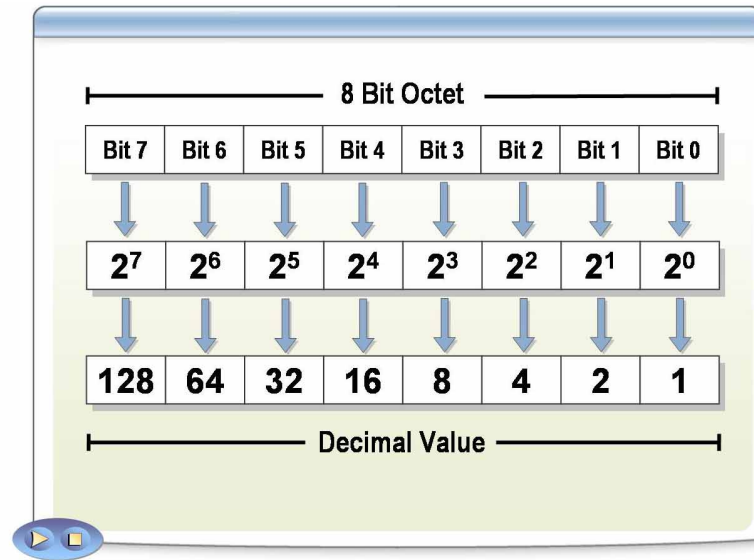
2. Which address class(es) will allow you to have more than 1,000 hosts per network?

Answer: Class A (16,777,214) and class B (65,534)

3. Which address class(es) will allow only 254 hosts per network?

Answer: Class C

How Dotted Decimal Notation Relates to Binary Numbers



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

Introduction

When you assign IP addresses, you use dotted decimal notation, which is based on the decimal number system. Computers use a binary format. For you to use dotted decimal notation, you must understand the relationship between these numbering systems.

Computers use a binary number system of base 2 (2 digits, 0 and 1) rather than the decimal system of base 10 (10 digits, 0 to 9). In the IP addressing scheme, computers use the binary format of four 8-bit octets, which yields 32 bits. IP addresses are normally expressed in dotted decimal notation which is four numbers separated by periods, for example, 192.168.0.200. Each of the four numbers represents an octet, ranging from the value 00000000 to 11111111. In decimal notation, the equivalents of these values are 0 to 255.

Each bit position in an octet 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 right-most bit in the octet, represents a decimal value of one. The high-order bit represents a decimal value of 128. The highest decimal value of an octet is 255—that is, when all bits are set to 1.

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 and moving from left to right.
2. Add these values to obtain the number.

For example, for the number 10000011;

$$1 * 2^7 = 1 * 128 = 128$$

$$0 * 2^6 = 0 * 64 = 0$$

$$0 * 2^5 = 0 * 32 = 0$$

$$0 * 2^4 = 0 * 16 = 0$$

$$0 * 2^3 = 0 * 8 = 0$$

$$0 * 2^2 = 0 * 4 = 0$$

$$1 * 2^1 = 1 * 2 = 2$$

$$1 * 2^0 = 1 * 1 = 1$$

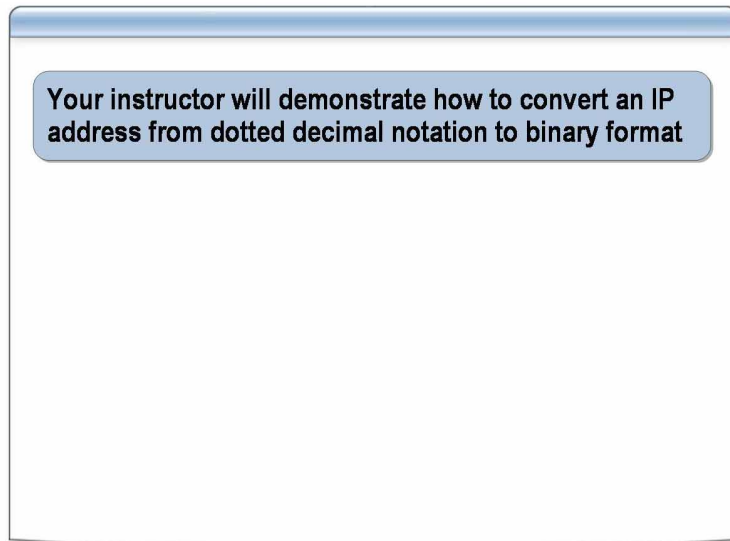
$$128 + 0 + 0 + 0 + 0 + 0 + 2 + 1 = 131$$

Example of 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	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

How to Convert Dotted Decimal Notation to Binary Format



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

Introduction

Although you can use the calculator in Windows Server 2003 to convert dotted decimal notation to binary format, it helps you to understand the conversion if you can do the calculation manually.

The following table represents the decimal number 131 in binary format 10000011.

Base	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Decimal	128	64	32	16	8	4	2	1
Binary	1	0	0	0	0	0	1	1
131 =	128	0	0	0	0	0	2	1

Procedure for converting an octet from decimal to binary

To manually convert a number from decimal notation to binary format:

1. Construct a table similar to the preceding one.
2. Determine the largest base 2 number possible in the octet (1 2 4 8 16 32 64 128) which is still less than the decimal number.
3. Place a "1" in the column of that number and zeros to the left.
4. Subtract the base 2 number's decimal equivalent from the decimal number.
5. If there is a remainder, repeat steps 2-4 until no remainder exists.

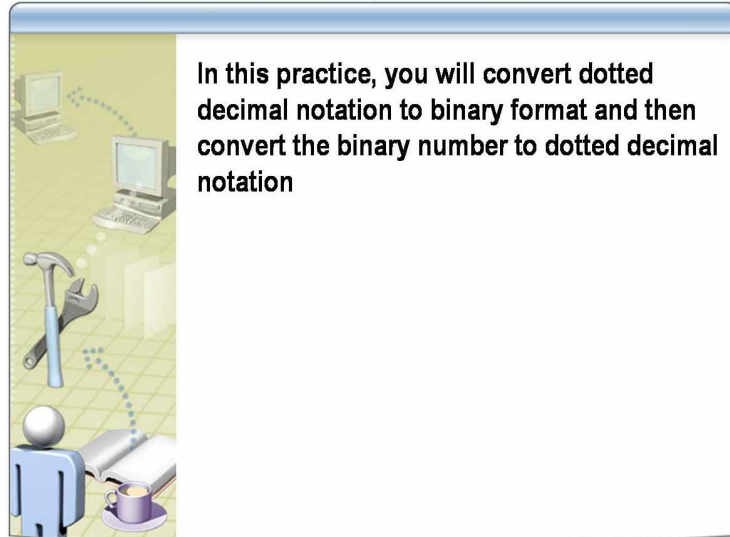
The 1s and 0s in your table represent the binary equivalent of your decimal number.

Procedure for using the Windows calculator to convert a number from decimal to binary

To use the Microsoft Windows Calculator to convert a number from decimal to binary:

1. Click **Start**, click **Run**, type **calc.exe** and then click **OK**.
The Calculator window appears.
2. On the **View** menu, click **Scientific**.
3. Using the calculator keys, enter a number.
4. Click **Bin**.

Practice: Converting Numbers Between Decimal and Binary



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

Objective In this practice, you will convert numbers between decimal and binary.

Scenario You have been given a set of IP addresses to apply to client computers, and you suspect that one of them has a different network ID. You decide to convert the IP address to its binary equivalent to later determine the correct network ID.

Practice ► **Convert the following numbers from decimal to binary**

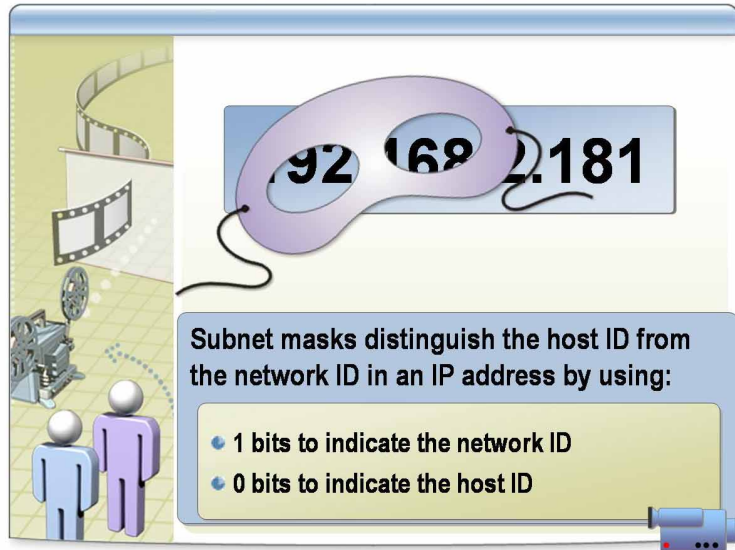
1. Log on to your computer with your *ComputerUser* account (where *Computer* is the name of your computer) with a password of **P@ssw0rd**.
2. Click **Start**, point to **All Programs**, click **Accessories**, and then click **Calculator**.
3. On the **View** menu, click **Scientific**.
4. Click **Dec**, type **44** and then click **Bin**.
5. Repeat for each conversion.

Decimal	Binary
44	Answer: 101100
97	Answer: 1100001
255	Answer: 11111111
192.168.1.100	Answer: 11000000.10101000.00000001.01100100
255.255.255.248	Answer: 11111111.11111111.11111111.11111000

► Convert the following numbers from binary to decimal

Binary	Decimal
1111111	Answer: 127
11111111 11111111 11111111 11111000	Answer: 255.255.255.248
00001010. 01100100.00000111.00010101	Answer: 10.100.7.21

Multimedia: How Subnet Masks Work



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

File location

To view the multimedia presentation, *How Subnet Masks Work*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objectives

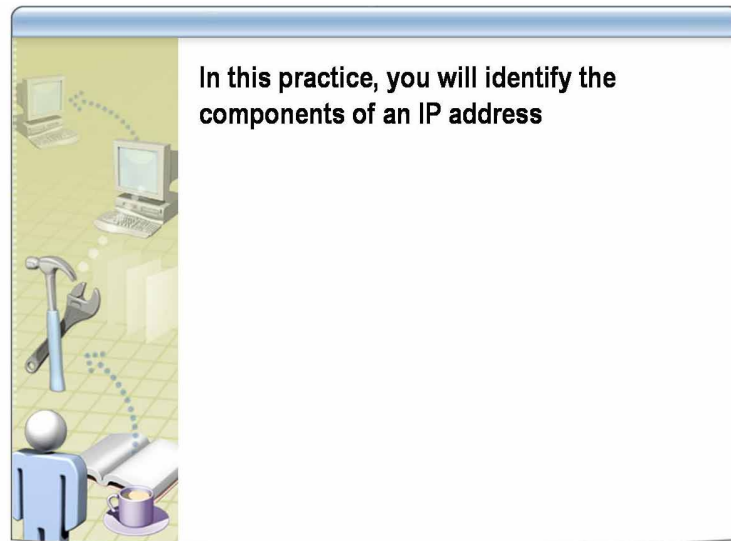
Upon completion of this presentation, you will be able to describe how subnet masks are used to distinguish the host ID from the network ID in an IP address.

Example of the binary equivalent of a dotted decimal number

A subnet mask's 1 bits indicate the network identifier, and its 0 bits indicate the host identifier. For example, the following is the binary equivalent of 255.255.255.0:

11111111 11111111 00000000 00000000

Practice: Identifying the Components of an IP Address



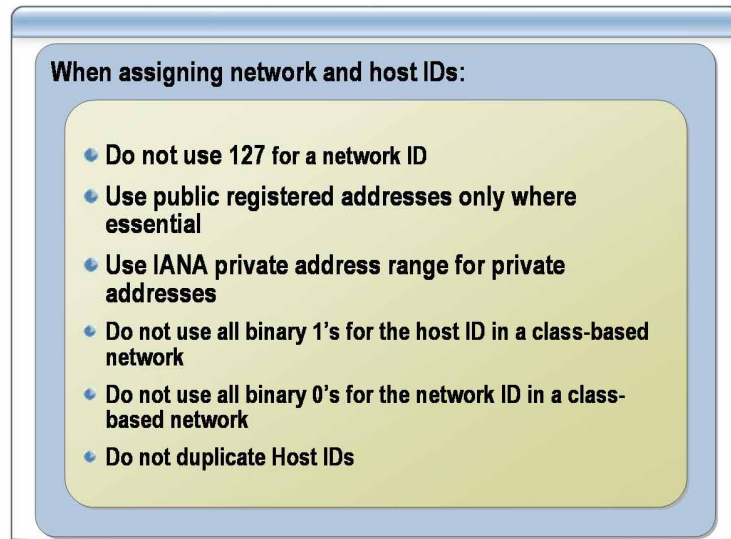
*****ILLEGAL FOR NON-TRAINER USE*****

Objective	In this practice, you will identify the components of an IP address.
Scenario	You are an administrator and need to identify the network and host ID for a given IP address so that you can determine whether a router is needed to communicate between the two computers.
Practice	<p>► Identify the class of IP address and the default subnet mask</p> <ol style="list-style-type: none">1. Use the first octet of the IP address to identify the default class and associated subnet mask for the address.2. Calculate the network ID by using the numeric values in the IP address that correspond to 255 in the subnet mask, and then fill in the remaining portion with zeros (0s).3. Calculate the host ID by using the numeric values in the IP address that correspond to 0 in the subnet mask.

4. Repeat for each IP address in the following table. The first IP address is completed for you as an example.

IP Address	Subnet Mask	Network ID	Host ID
192.168.0.100	Answer: C/255.255.255.0	Answer: 192.168.0	Answer: 100
10.7.1.1	A/255.0.0.0	10.0.0.0	7.1.1
172.16.1.1	B /255.255.0.0	172.16.0.0	1.1
129.102.197.23	B/255.255.0.0	129.102.0.0	192.23
199.32.123.54	C/255.255.255.0	199.32.123.0	54
1.1.1.1	A/255.0.0.0	1.0.0.0	1.1.1
221.22.64.7	C/255.255.255.0	221.22.64.0	7
93.44.127.235	A/255.0.0.0	93.0.0.0	44.127.235
23.46.92.184	A/255.0.0.0	23.0.0.0	46.92.184
152.79.234.1	B/255.255.0.0	152.79.0.0	234.1
200.100.50.25	C/255.255.255.0	200.100.50.0	25

Guidelines for IP Addressing



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

Introduction

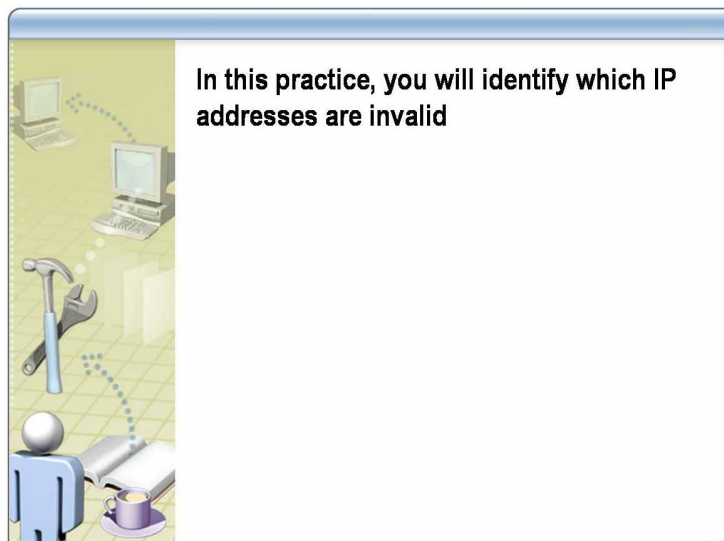
There are no exact rules that govern how to assign IP addresses on your network, however, there are guidelines that you can use to ensure you assign valid network and host identifiers.

Assigning valid network and host identifiers

When you assign IP addresses, consider the following guidelines:

- You must not use 127 for the first octet of the network ID. This value is reserved for diagnostic purposes.
- Use public registered addresses only where essential to do so.
- Use addresses from the private address ranges reserved by the IANA for private IP addressing.
- You must not use all 1s (binary) for the host ID in a class-based network. If all bits are set to 1, the address is interpreted as a broadcast address.
- You must not use all 0s for the host ID in a class-based network. If host bits are set to 0, some TCP/IP implementations interpret this as a broadcast address.
- You must not duplicate host IDs within a network segment.

Practice: Identifying Invalid IP Addresses



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

Introduction

In this practice, you will identify which of the following IP addresses cannot be assigned to a host and then explain why it is invalid.

Practice

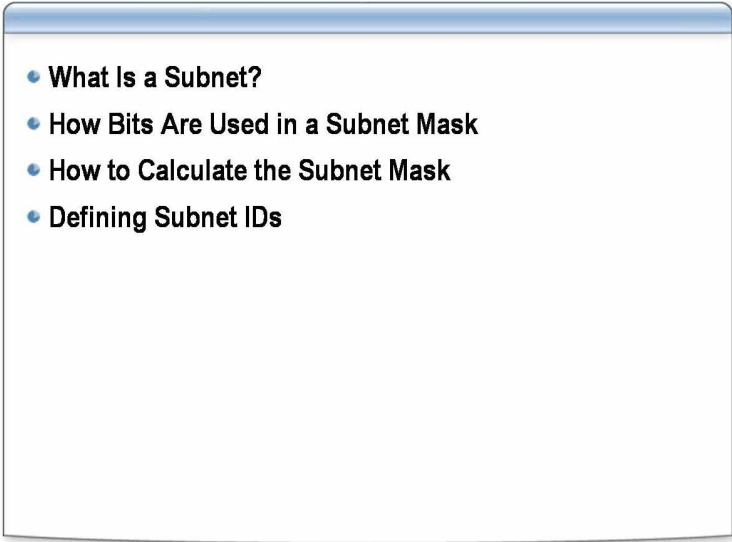
► **Determine which of the following IP addresses cannot be assigned to a host**

- Review the following class-based IP addresses. Identify the portion of the IP address that would be invalid if it were assigned to a host, and then explain why it is invalid. Assume a default subnet mask is applied according to the class of the address.
 - a. 131.107.256.80 _____
 - b. 222.222.255.222 _____
 - c. 231.200.1.1 _____
 - d. 126.1.0.0 _____
 - e. 0.127.4.100 _____
 - f. 190.7.2.0 _____
 - g. 127.1.1.1 _____
 - h. 198.121.254.255 _____
 - i. 255.255.255.255 _____

Answers:

- a. 131.107.256.80: 256. The highest possible value in an octet is 255.
- b. 222.222.255.222: valid host IP address
- c. 231.200.1.1: 231 is a class D address and is not supported as a host address.
- d. 126.1.0.0: valid host IP address
- e. 0.127.4.100: Zero is invalid in the first octet. It indicates this network only.
- f. 190.7.2.0: valid host IP address.
- g. 127.1.1.1: 127 addresses are reserved for diagnostics.
- h. 198.121.254.255: 255 as a host ID indicates a broadcast.
- i. 255.255.255.255: 255 is a broadcast address.

Lesson: Creating a Subnet

- 
- What Is a Subnet?
 - How Bits Are Used in a Subnet Mask
 - How to Calculate the Subnet Mask
 - Defining Subnet IDs

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

Introduction

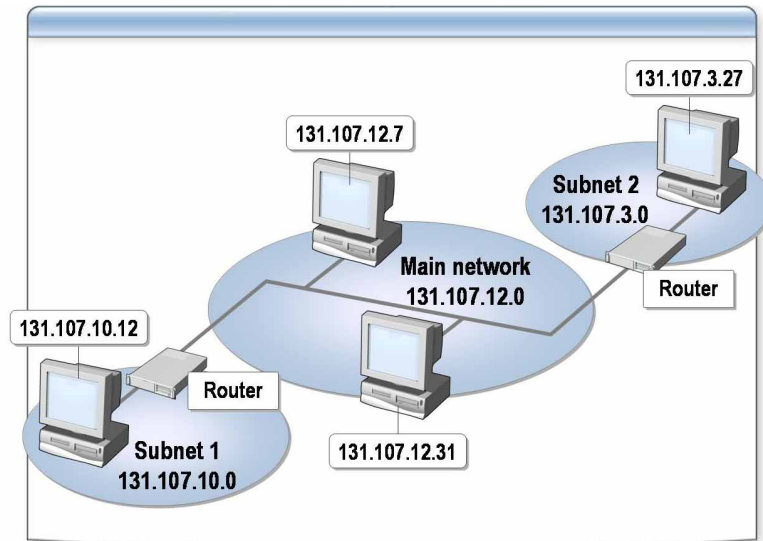
You can expand a network by using physical devices, such as routers, to add network segments, or subnets. You can also use routers to divide your network into smaller subnets, thereby increasing the efficiency of the network.

Lesson objectives

After completing this lesson, you will be able to:

- Describe a subnet.
- Describe subnet mask bits.
- Calculate a subnet mask and range of IP addresses.
- Define subnet IDs.

What Is a Subnet?



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

Introduction

A subnet is a physical segment of a network that is separated from the rest of the network by a router or routers. You can have multiple subnets on your network. A network of multiple subnets connected by routers is often referred to as an internetwork. When you create subnets, you must break up the network ID for the hosts on the subnets. Assigning the appropriate subnet and host ID enables you to locate a host on the network. You can also determine which hosts are on the same subnet by matching network IDs.

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 the subnet ID, you partition the bits in the host ID into two parts. You use one part to identify the subnet and the other part to identify the host. The process of creating the subnet ID is called subnetting or subnetworking.

Benefits of using a subnet

Organizations use subnets to apply one network across multiple physical segments. Using subnets allows you to:

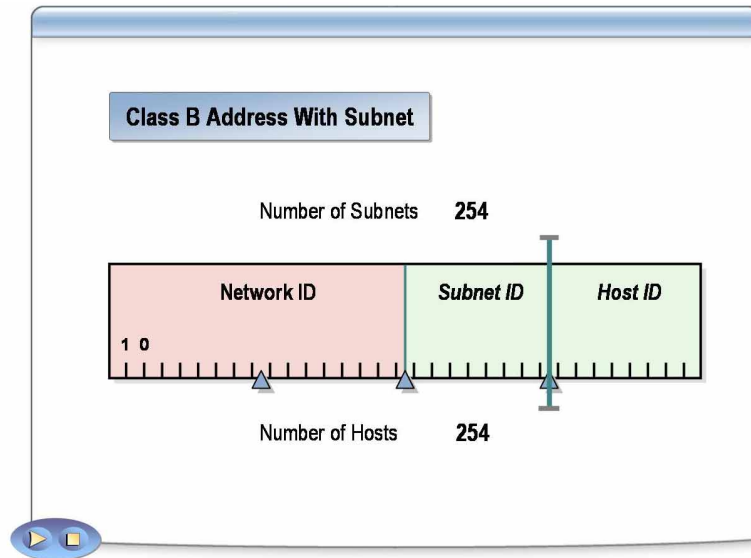
- Mix different network technologies, such as Ethernet and Token Ring.
- Overcome limitations of current technologies such as exceeding the maximum number of hosts allowed per segment. Breaking the segment into further segments, increases the total number of hosts allowed.
- Reduce network congestion by segmenting traffic and reducing the number of broadcasts that are sent on each segment.

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 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



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

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

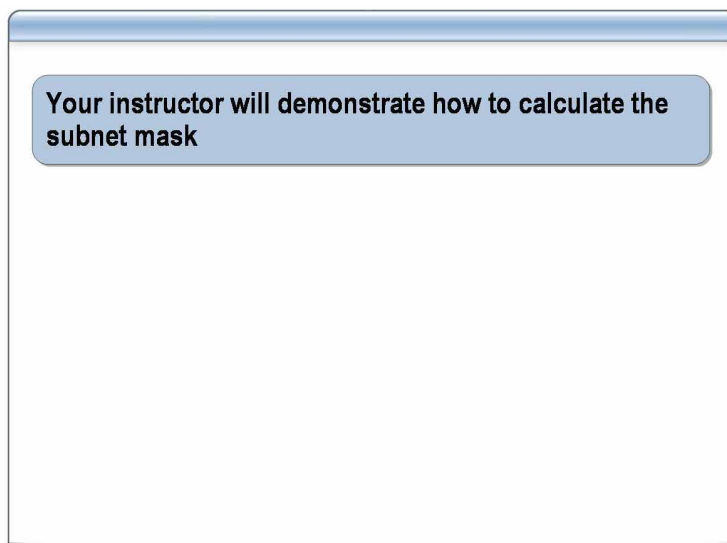
As the preceding illustration shows, when more bits are used for the subnet mask, more subnets are available, but fewer hosts are available per subnet. If you use more bits than needed, it will allow for growth in the number of subnets but will limit the growth in the number of hosts. If you use fewer bits than needed, it will allow for growth in the number of hosts but will limit the growth in the number of subnets.

Contiguous mask bits

When industry standards for subnetting were initially defined, it was recommended that subnet IDs be derived from high-order bits. It is now a requirement that the subnet ID uses contiguous high-order bits of the local address portion of the subnet mask. In support of this, most router vendors do not support the use of low-order or noncontiguous bits in subnet IDs.

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

How to Calculate the Subnet Mask



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

Introduction

When you divide your network into subnets, you must define a subnet mask.

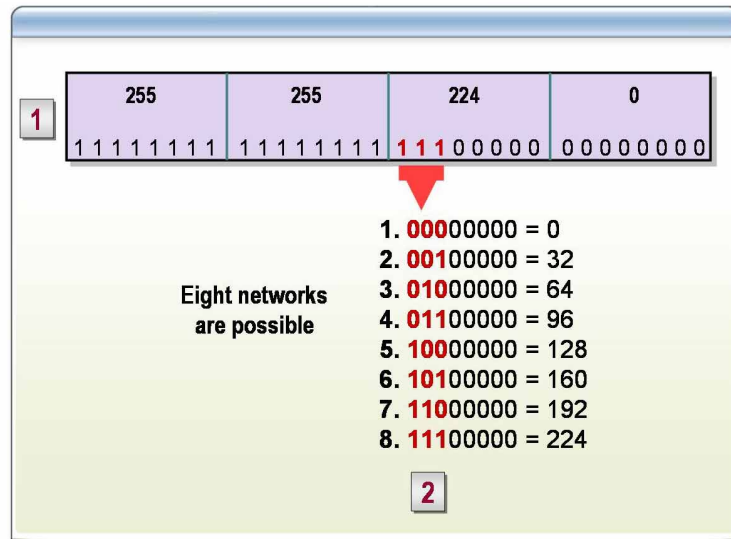
Procedure

To define a subnet mask:

1. When you have determined the number of physical segments in your network environment, determine the next-highest power of 2 that is larger than your desired number of subnets. For example, if you need 6 subnets, the next-highest power of 2 from 6 is 8.
2. Determine the exponent required to express this next-highest power of 2. The exponent is the number of bits needed for subnetting. For example, 8 is 2^3 . The exponent and the number of bits needed for subnetting is 3.
3. Create the binary bit mask for the octet being subnetted by setting the high-order bits for the number of bits needed to subnet to 1. Then, convert the binary mask value to decimal. For our example, 3 bits are needed. The binary bit mask becomes 11100000. The decimal value for binary 11100000 is 224. The final subnet mask, assuming that we are subnetting a class B network ID, is 255.255.224.0.

Note For more information about calculating the subnet mask, see Appendix B "Decimal Equivalent Mask Values" on the Student Materials compact disc.

Defining Subnet IDs



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

Introduction

To define the subnet ID for a subnet, you use the same number of host bits that are used for the subnet mask. You evaluate the possible bit combinations and then convert them to a decimal format.

How to define a range of subnet IDs

To define a range of subnet IDs for an internetwork:

1. Using the same number of bits as are used for the subnet mask, list all possible bit combinations. In the previous example, 3 bits are required.
2. Convert to decimal the subnet ID bits for each subnet. Each decimal value represents a single subnet. This value is used to define the range of host IDs for a subnet.

Shortcut to defining subnet IDs

Using the previous 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 high order used for the subnet ID. For example, if 5 bits are used for the subnet mask, the binary octet is 11111000.
2. Convert the bit with the lowest value to decimal format. This is the increment value to determine each successive subnet ID. For example, if you use 5 bits, the lowest value is 8.
3. Starting with zero, increment the value for each successive subnet until you have enumerated the maximum number of subnets.

How to determine the number of valid subnets

To determine the number of valid subnets, raise 2 to the power of the number of bits being used for subnetting. For example, when you are using 5 bits to subnet, the number of subnets is 2^5 , or 32.

Special case subnet addresses

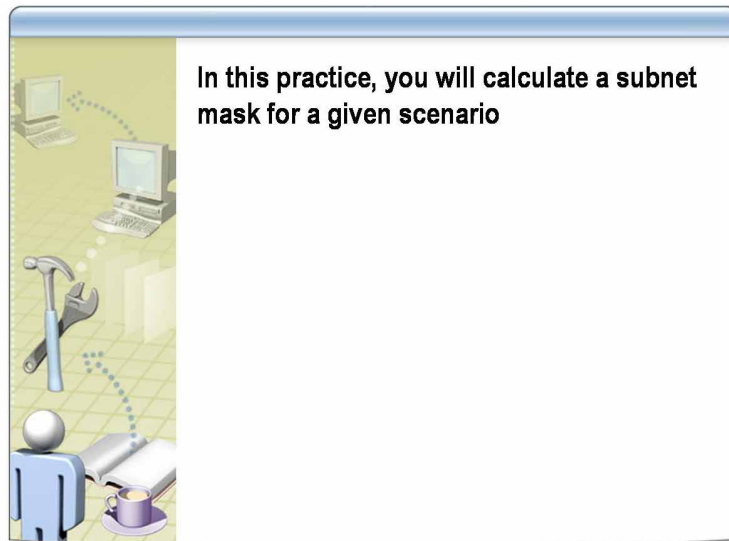
Request for Comment (RFC) 950 originally forbade the use of the subnetted network IDs where the bits being used for subnetting are set to all 0s (the all-zeros subnet) and all 1s (the all-ones subnet). The all-zeros subnet caused problems for early routing protocols and the all-ones subnet conflicts with a special broadcast address called the all-subnets directed broadcast address.

However, RFC 1812 now permits the use of the all-zeros and all-ones subnets in a classless environment. Classless environments use modern routing protocols that do not have a problem with the all-zeros subnet and the all-subnets directed broadcast is no longer relevant.

The all-zeros and all-ones subnets may cause problems for hosts or routers operating in a classful mode. Before you use the all-zeros and all-ones subnets, verify that they are supported by your hosts and routers. All implementations of TCP/IP for Windows support the use of the all-zeros and all-ones subnets.

Note For more information about special-case subnet addresses, see RFC 950 and RFC 1812 under **Additional Reading** on the Student Materials compact disc.

Practice: Calculating a Subnet Mask



In this practice, you will calculate a subnet mask for a given scenario

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

Introduction

In this practice, given a number of subnets and an IP address, you will calculate the appropriate subnet mask, subnet IDs, and host IDs.

Scenario

You have been asked to subnet an existing class B network into 14 segments.

Practice

► Determine the appropriate subnet mask

1. Determine the next highest power of 2 from 14.

Answer: 16

2. Determine exponent for the next-highest power of 2, which is the number of bits required for subnetting.

Answer: 4

3. Convert the required number of bits to decimal format in high order (from left to right).

Answer 11110000 = 240

4. Append the converted number to the existing subnet mask. What is the required subnet mask?

Answer: 255.255.240.0.

► Define the subnet IDs

1. Using the same number of bits as are used for the subnet mask, list all possible bit combinations.

Answer:

0000

0001

0010

0011

0100

0101

0110

0111

1000

1001

1010

1011

1100

1101

1110

1111

2. Convert to decimal the subnet ID bits for each subnet. Each decimal value represents a single subnet. List the subnets and the range of host IDs listed in the following table.

Answer:

Bit values	Decimal values	Beginning range values	Ending range values
00000000	0	w.x.32.1	w.x.63.254
00010000	16	w.x.32.1	w.x.63.254
00100000	32	w.x.64.1	w.x.95.254
00110000	48	w.x.96.1	w.x.127.254
01000000	64	w.x.128.1	w.x.159.254
01010000	80	w.x.160.1	w.x.191.254
01100000	96	w.x.192.1	w.x.223.254
01110000	112	w.x.192.1	w.x.223.254
10000000	128	w.x.32.1	w.x.63.254
10010000	144	w.x.32.1	w.x.63.254
10100000	160	w.x.64.1	w.x.95.254
10110000	176	w.x.96.1	w.x.127.254
11000000	192	w.x.128.1	w.x.159.254
11010000	208	w.x.160.1	w.x.191.254
11100000	224	w.x.192.1	w.x.223.254
11110000	240	w.x.192.1	w.x.223.254

Lesson: Using IP Routing Tables

- What Is a Router?
- Using a Default Gateway
- The Role of Routing in the Network Infrastructure
- How the Computer Determines Whether an IP Address is a Local or Remote Address
- What Is Static and Dynamic Routing?
- How the IP Protocol Selects a Route
- How IP Uses the Routing Table
- Using the Routing Table in Windows Server 2003

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

Introduction

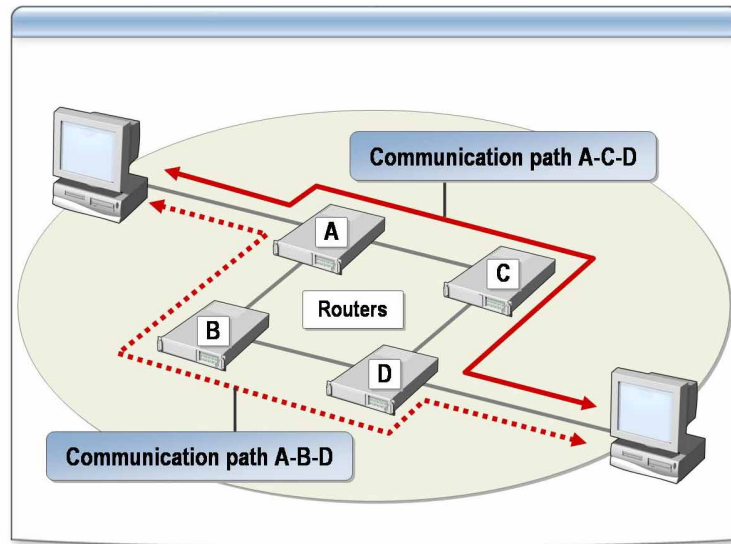
In a multiple subnet network, routers pass IP packets from one subnet to another. This process is known as routing and is a primary function of IP. To make routing decisions, IP consults a routing table. To modify and maintain these tables, you must understand how routers use routing tables in an internetwork.

Lesson objectives

After completing this lesson, you will be able to:

- Describe a router and its role in a network.
- Use a default gateway.
- Determine whether an IP address is a local or remote address.
- Describe the difference between static and dynamic routing.
- Describe how the IP protocol selects a route.
- Describe the routing table format.
- Modify a routing table.

What Is a Router?



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

Introduction

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, a router's job can be quite simple. When two LANs are connected by one router, the router simply 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, 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 should fail, packets can bypass it and still reach their destinations.

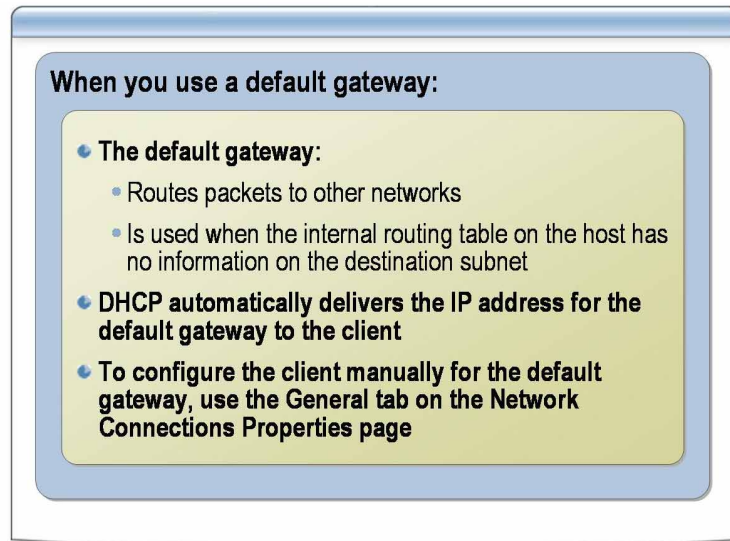
How routers work together

In a complex internetwork, a router must select the most efficient route to a packet's destination. Usually, this is the path that enables a packet to reach the destination with the fewest number of hops (that is, by passing through the smallest number of routers). 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 may contain all the network addresses and possible paths throughout the network, along with the cost of reaching each network. Routers route packets based on the available paths and their costs.

Using a Default Gateway



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

Introduction

A default gateway is a device, usually a router, on a TCP/IP internetwork that can forward IP packets to other networks. When you configure a client on a subnet and the client requires network access beyond their local network, you must ensure that the default gateway is specified. In most cases, the IP address for the default gateway is automatically delivered by Dynamic Host Control Protocol (DHCP). However, in some cases, you may need to configure the client to use the default gateway.

The role of the default gateway

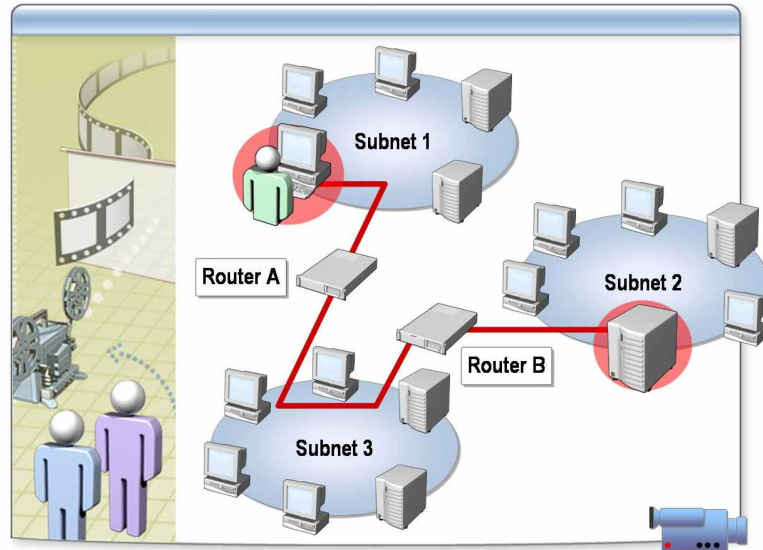
In an internetwork, any given subnet might have several routers that connect it to other subnets, both local and remote. At least one of the routers is configured as the default gateway for the subnet. When a host on the network uses IP to send a packet to a destination subnet, IP consults the internal 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, DHCP is used to automatically assign the default gateway. In the event that you need to assign the default gateway manually on clients running Windows Server 2003, Windows 2000, Windows 95, and Windows 98, you configure the property **Default Gateway Address** by using the **General** tab on the **Network Connections Properties** page.

For clients running Windows Server 2003, you can use DHCP to automatically assign the default gateway.

Multimedia: The Role of Routing in the Network Infrastructure

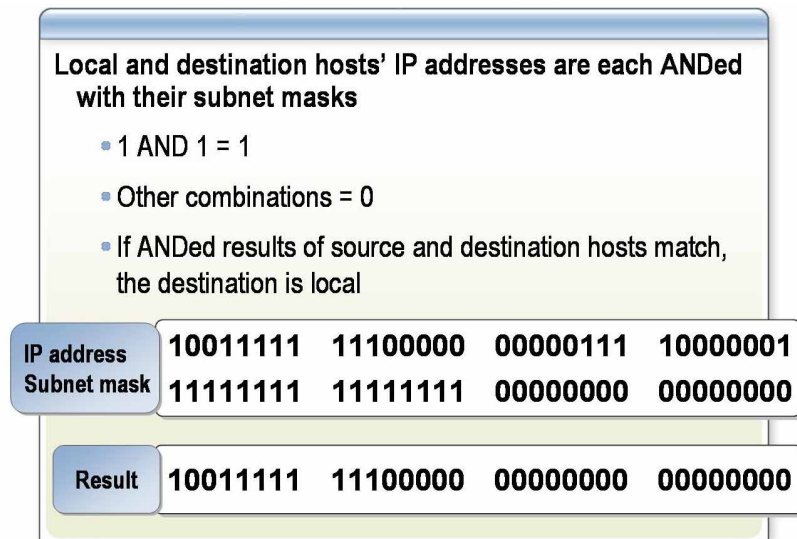


*****ILLEGAL FOR NON-TRAINER USE*****

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

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



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

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 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

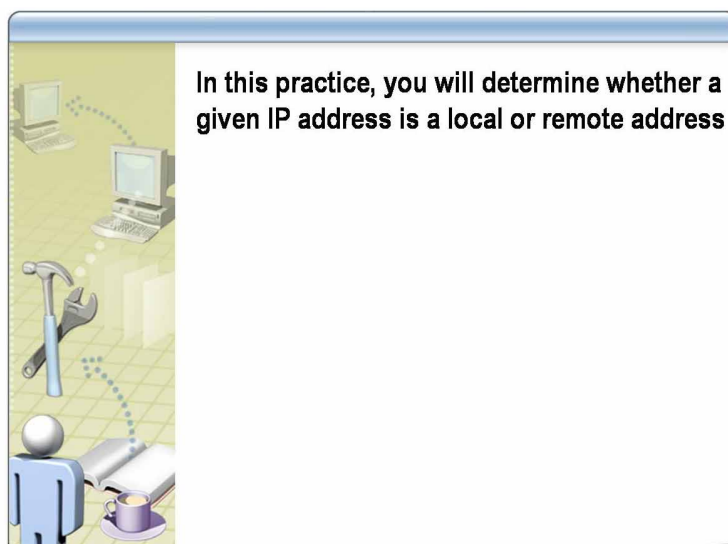
To AND the IP address to a subnet mask, IP compares each bit in the IP address to the corresponding bit in the subnet mask. If both bits are 1s, the resulting bit is 1. If there is any other combination, the resulting bit is 0.

Example of bit combinations

For combinations of 1 and 0, the results are:

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

Practice: Determining Whether an IP Address Is a Local or Remote Address



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

Introduction In this practice, given your own IP address and subnet mask, you will determine if another address is local or remote.

Scenario You are isolating connectivity issues between two hosts and need to determine if IP considers these local to each other or remote.

Practice ► **Convert both IP addresses to binary and then AND them to determine if they are local to each other or remote**

Your IP address	176.149.115.8	10110000 10010101 01110011 00001000
Subnet mask	255.255.252.0	11111111 11111111 11111100 00000000
Result	176.149.112.0	10110000 10010101 01110000 00000000

Destination IP address	176.149.117.201	10110000 10010101 01110101 11001001
Subnet mask	255.255.252.0	11111111 11111111 11111100 00000000
Result	176.149.116.0	10110000 10010101 01110100 00000000

- Is the destination address local or remote?

Answer: Remote. 112 is not equal to 116.

- **Convert both IP addresses to binary and then AND them to determine whether they are local to each other or remote**

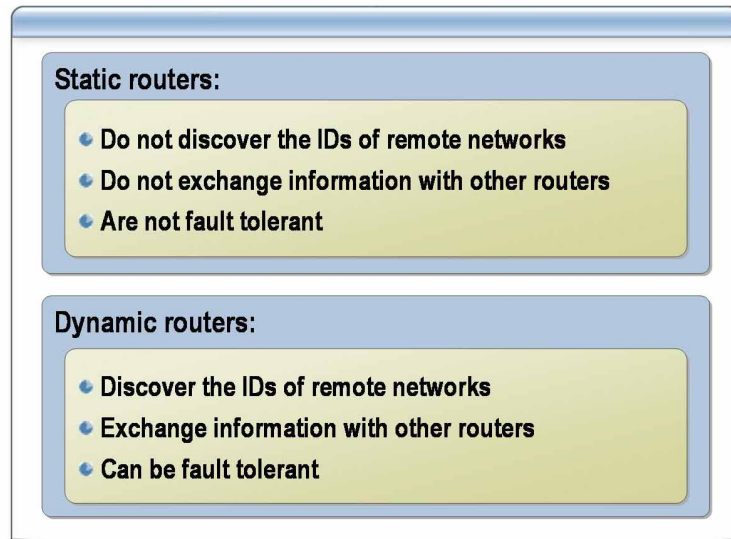
Your IP address	176.149.115.8	10110000 10010101 01110011 00001000
Subnet mask	255.255.252.0	11111111 11111111 11111100 00000000
Result	176.149.112.0	10110000 10010101 01110000 00000000

Destination IP address	176.149.114.66	10110000 10010101 01110010 01000010
Subnet mask	255.255.252.0	11111111 11111111 11111100 00000000
Result	176.149.112.0	10110000 10010101 01110000 00000000

- Is the destination address local or remote?

Answer: Local. 112 is equal to 112.

What Is Static and Dynamic Routing?



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

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 you need to maintain routing tables so that IP uses 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. Static routers:

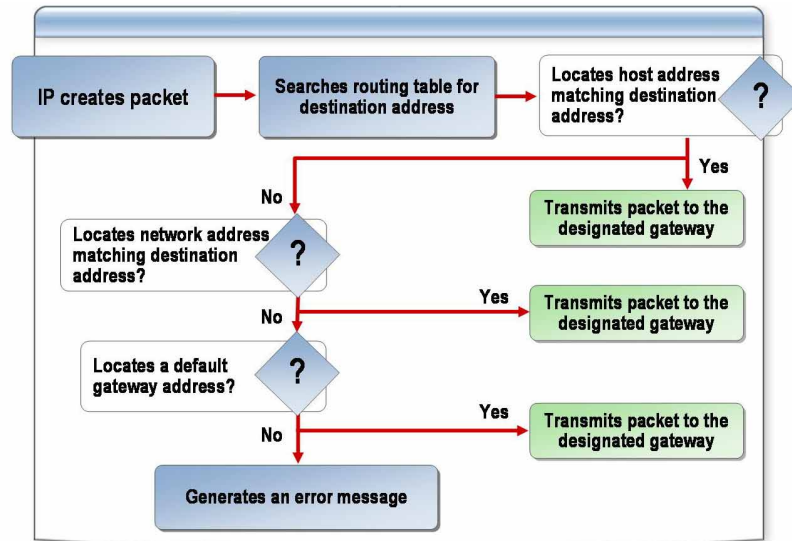
- Do not discover the network IDs of remote networks. You must configure these network IDs manually.
- Do not inform each other of route changes.
- Do not exchange routes with dynamic routers.
- Are not fault tolerant. This means that, when the router goes out of operation, neighboring routers do not 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). Dynamic routers:

- Can discover the network IDs of remote networks.
- Automatically inform other routers of route changes.
- Use routing protocols to periodically or on demand transmit the contents of their routing tables to the other routers on the network.
- Are fault-tolerant (in a multi-path routing topology). When the router goes out of operation, 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



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

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 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's Network Address and Netmask columns for a network route that matches the destination. If there is more than one entry in the routing table that matches the destination, IP uses the entry with the most amount of bits set to 1 in the Netmask column. If there is more than one entry in the routing table that matches the destination with the most amount 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-Host 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 Address Resolution Protocol (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 on the medium. The network adapter constructs a frame using the router's hardware address in its Destination Address field and transmits it on the network medium.

How IP Uses the Routing Table

```

C:\>route print

Interface List
=====
0x1 ..... MS TCP Loopback interface
0x2 ...00 b0 d0 a7 08 f9 ..... 3Com 3C920 Integrated Fast Ethernet Controller (
3C905C-TX Compatible) - Packet Scheduler Miniport
=====

Active Routes:
=====
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          192.168.0.1      192.168.0.53      20
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.0.0                255.255.255.0    192.168.0.53     192.168.0.53      20
192.168.0.53              255.255.255.255  127.0.0.1        127.0.0.1         20
192.168.0.255             255.255.255.255  192.168.0.53     192.168.0.53      20
224.0.0.0                 240.0.0.0        192.168.0.53     192.168.0.53      20
255.255.255.255           255.255.255.255  192.168.0.53     192.168.0.53      1
Default Gateway:          192.168.0.1

Persistent Routes:
None

C:\>

```

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

Introduction

To make IP routing decisions, IP consults a routing table that 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 according to 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 Windows Server 2003, this is the Netmask column.
Next hop	The IP address of the next hop. In the Windows Server 2003 IP routing table, this is the Gateway column.
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 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.

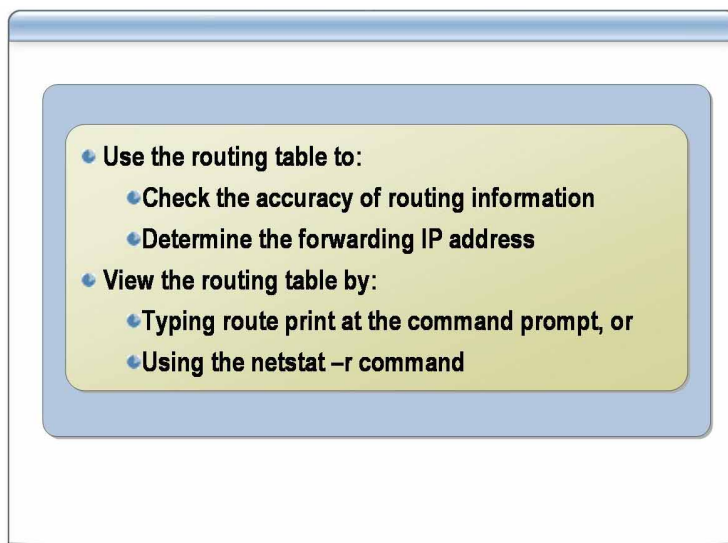
Type of route	Description
Directly attached network ID	A route for network IDs that are directly attached. The next hop field can be blank or contain the IP address of the interface on that network.
Remote network ID	A route for network IDs that are not directly attached but are available across other 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 with 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 the TCP/IP protocol is initialized.

The default routing table for a host running Windows Server 2003

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

Network Destination	Netmask	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

Using the Routing Table in Windows Server 2003



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

Introduction

You can use the routing tables in Windows Server 2003 to assist you in isolating connectivity issues. Examining the tables will help you to determine if an incorrect entry is contributing to the issue.

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

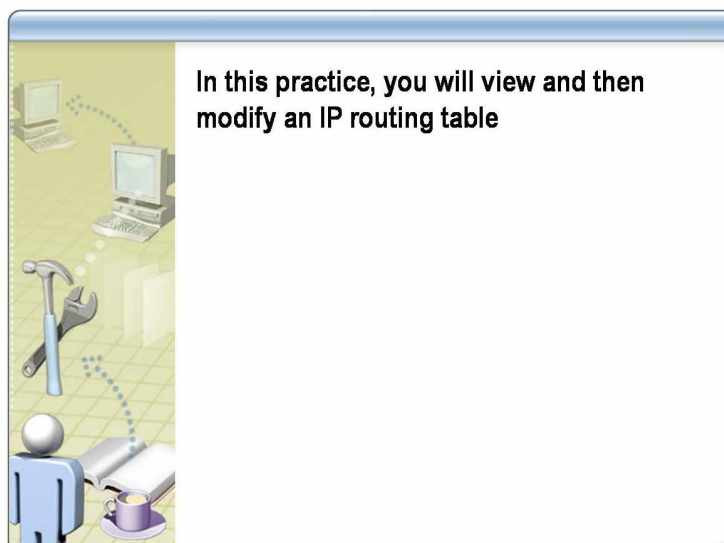
When traffic is sent to 192.168.0.55, the most specific matching route is the route for the directly attached network (192.168.0.0, 255.255.255.0). The forwarding IP address is set to the destination IP address (157.60.16.48), and the interface is the network adapter that has been assigned the IP address 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 the command prompt. You can also use the **netstat -r** command.

Practice: Viewing and Modifying a Routing Table



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

Introduction

In this practice, you will view and modify the routing table.

Scenario

You have been asked to check a client's routing table for persistent routes and confirm that the IP address of the default gateway is correct. In addition, you must make sure that you can change the default gateway in case it becomes necessary to do so.

Practice

► View the IP routing table

1. Using Run as, open a command prompt as *Computer*\Administrator (where *Computer* is the name of your computer), type **route print** and press ENTER.
2. Locate the **Persistent Routes** attribute.
3. Are there any persistent routes listed?

Answer: No. No persistent routes have been created.

4. Locate the **Default Gateway** attribute.
5. What is the IP address of the default gateway?

Answer: 192.168.x.200 (where x is the number of the classroom)

6. At the command prompt, type **ipconfig /all** and press ENTER.
7. What is the IP address of the default gateway?

Answer: 192.168.x.200

► Modify the IP routing table

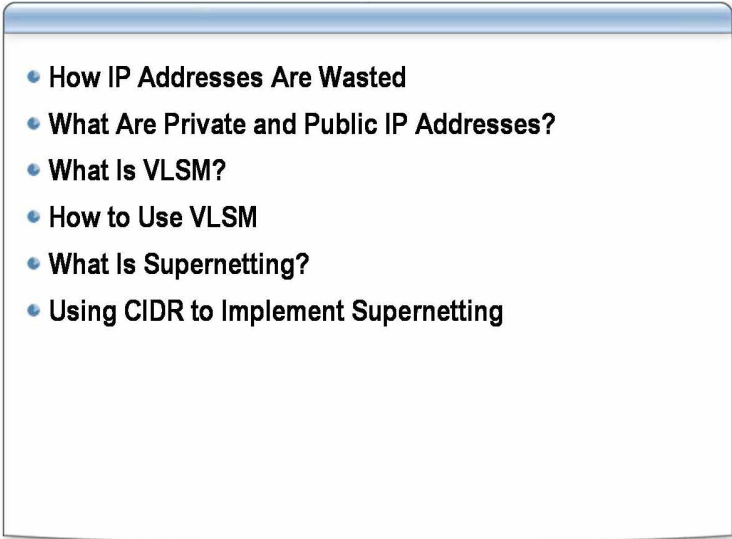
1. At the command prompt, type **route delete 0.0.0.0** and press ENTER.
2. At the command prompt, type **ipconfig /all** and press ENTER.
3. What is the IP address of the default gateway?

Answer: There is no default gateway listed.

4. At the command prompt, type **route add 0.0.0.0 mask 0.0.0.0 192.168.x.200** and press ENTER.
5. At the command prompt, type **ipconfig /all** and press ENTER.
6. What is the IP address of the default gateway?

Answer: 192.168.x.200

Lesson: Overcoming Limitations of the IP Addressing Scheme

- 
- How IP Addresses Are Wasted
 - What Are Private and Public IP Addresses?
 - What Is VLSM?
 - How to Use VLSM
 - What Is Supernetting?
 - Using CIDR to Implement Supernetting

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

Introduction

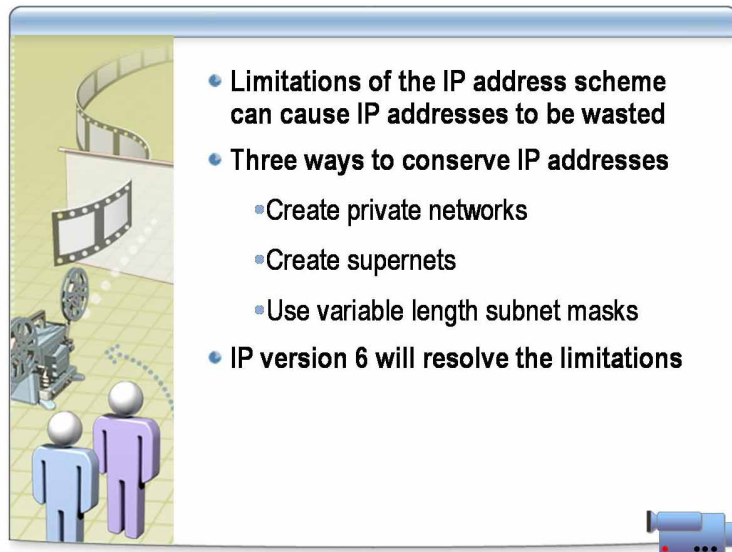
There are limitations of the IP addressing scheme that can prevent you from using the best scheme for your network, and that result in a large number of addresses that remain unused. In this lesson, you will learn how you can overcome some of these limitations and increase the effectiveness of your IP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

Lesson objectives

After completing this lesson, you will be able to:

- Describe the ways in which IP addresses are wasted.
- Describe the differences between private and public addresses.
- Use Variable Length Subnet Masks (VLSM) to more efficiently assign IP addresses
- Use Classless Inter-Domain Routing (CIDR) to implement supernetting.

Multimedia: How IP Addresses Are Wasted



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

File location

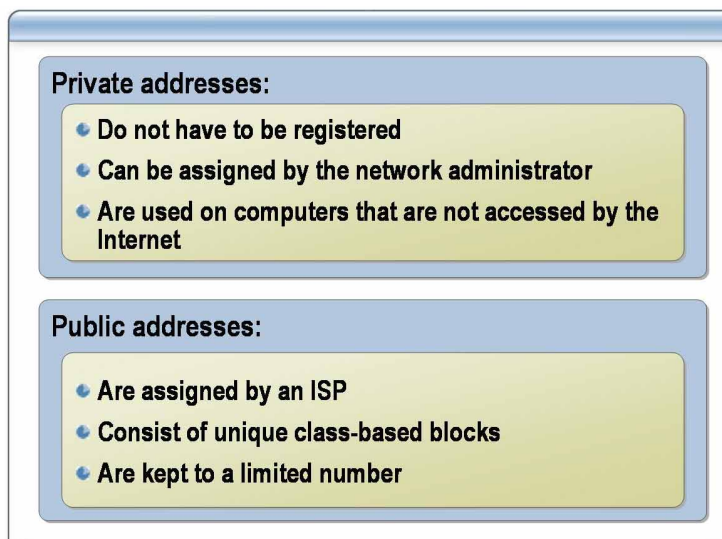
To view the multimedia presentation, *How IP Addresses are Wasted*, open the Web page on the Student Materials compact disc, click **Multimedia**, and then click the title of the presentation.

Objectives

Upon completion of 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?



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

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 or the IANA. 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 a network address translator (NAT) to translate the private address into a valid public address and then send its requests on the Internet.

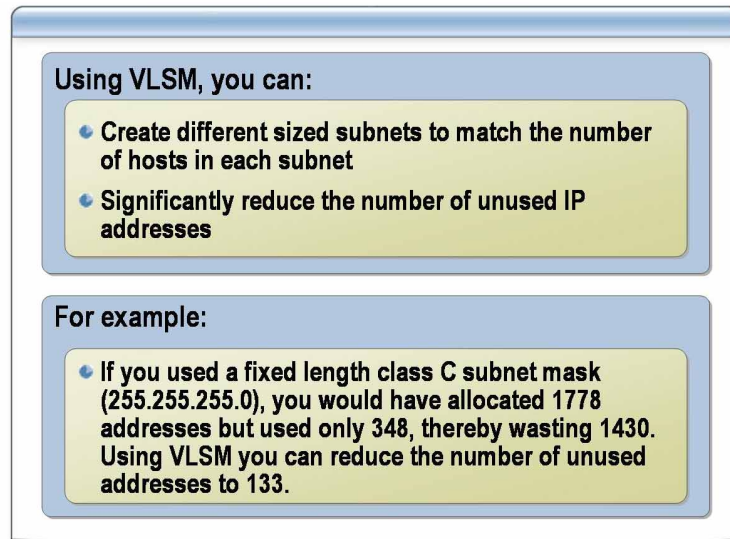
Public addresses

Public addresses are assigned by IANA and consist of class-based network IDs or blocks of CIDR-based addresses (called CIDR blocks) that are guaranteed to be globally unique on the Internet. There are a limited number of publicly assignable addresses.

When the 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.

For example, when an organization is assigned a CIDR block in the form of a network ID and subnet mask, that network ID-subnet mask pair also exists as a route in the routers of the Internet. IP packets destined to an address within the CIDR block are routed to the proper destination.

What Is VLSM?



Using VLSM, you can:

- Create different sized subnets to match the number of hosts in each subnet
- Significantly reduce the number of unused IP addresses

For example:

- If you used a fixed length class C subnet mask (255.255.255.0), you would have allocated 1778 addresses but used only 348, thereby wasting 1430. Using VLSM you can reduce the number of unused addresses to 133.

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

Introduction

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

How equal-sized subnets wastes IP addresses

Subnetting was originally used to subdivide a class-based network ID into a series of equal-sized subnets. For example, a 4-bit subnetting of a class B network ID produced 16 equal-sized subnets. In actuality, 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-sized subnets, so you can conserve IP addresses by using VLSM to create different-sized subnets that best match the number of hosts in each subnet. VLSM is a recursive process that uses subnetting to subnet network IDs that are already subnetted. The process continues until you have unique subnet IDs that waste as few IP addresses per subnet as possible. Because all subnetted network IDs are unique, they can be distinguished from each other by their corresponding subnet mask.

Example of how IP addresses are wasted

In the following table, there are seven subnets that need addresses.

Subnet	Hosts
1	2
2	2
3	62
4	97
5	28
6	153
7	4

If you used a fixed length 24-bit subnet mask (255.255.255.0), you would have allocated 1778 addresses but used only 348, thereby wasting 1430. Using VLSM, you can reduce the number of wasted addresses in this case to 133.

Note Another means of conserving public IP addresses is to use the private address space.

How to Use VLSM

Your instructor will demonstrate how to reduce the number of IP addresses by using VLSM

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

Introduction

You can reduce the number of IP addresses that remain unused by using VLSM.

For example, given the class-based network ID of 157.54.0.0/16, a required configuration is one subnet with up to 32,000 hosts, 15 subnets with up to 2,000 hosts, and eight subnets with up to 250 hosts.

Note The notation /16 in 157.54.0.0/16 refers to the number of 1 bits used in the subnet mask (255.255.0.0). This is referred to as CIDR notation.

Procedure for one subnet with up to 32,000 hosts

To achieve a requirement of one subnet with approximately 32,000 hosts, subnet 1 bit of the class-based network ID of 157.54.0.0. This produces 2 subnets—157.54.0.0/17 and 157.54.128.0/17. This subnetting allows up to 32,766 hosts per subnet. 157.54.0.0/17 is chosen as the network ID, which fulfills the requirement.

The following table shows one subnet with up to 32,766 hosts per subnet.

Subnet Number	Network ID (Dotted Decimal)	Network ID (Network Prefix)
1	157.54.0.0, 255.255.128.0	157.54.0.0/17

Procedure for 15 subnets with up to 2,000 hosts

To achieve a requirement of 15 subnets with approximately 2,000 hosts, subnet 4 bits of the subnetted network ID of 157.54.128.0/17. This produces 16 subnets (157.54.128.0/21, 157.54.136.0/21 through 157.54.240.0/21, 157.54.248.0/21), allowing up to 2,046 hosts per subnet. The first 15 subnetted network IDs (157.54.128.0/21 through 157.54.240.0/21) are chosen as the network IDs, which fulfills the requirement.

The following table shows 15 subnets with up to 2,046 hosts per subnet.

Subnet Number	Network ID (Dotted Decimal)	Network ID (Network Prefix)
1	157.54.128.0, 255.255.248.0	157.54.128.0/21
2	157.54.136.0, 255.255.248.0	157.54.136.0/21
3	157.54.144.0, 255.255.248.0	157.54.144.0/21
4	157.54.152.0, 255.255.248.0	157.54.152.0/21
5	157.54.160.0, 255.255.248.0	157.54.160.0/21
6	157.54.168.0, 255.255.248.0	157.54.168.0/21
7	157.54.176.0, 255.255.248.0	157.54.176.0/21
8	157.54.184.0, 255.255.248.0	157.54.184.0/21
9	157.54.192.0, 255.255.248.0	157.54.192.0/21
10	157.54.200.0, 255.255.248.0	157.54.200.0/21
11	157.54.208.0, 255.255.248.0	157.54.208.0/21
12	157.54.216.0, 255.255.248.0	157.54.216.0/21
13	157.54.224.0, 255.255.248.0	157.54.224.0/21
14	157.54.232.0, 255.255.248.0	157.54.232.0/21
15	157.54.240.0, 255.255.248.0	157.54.240.0/21

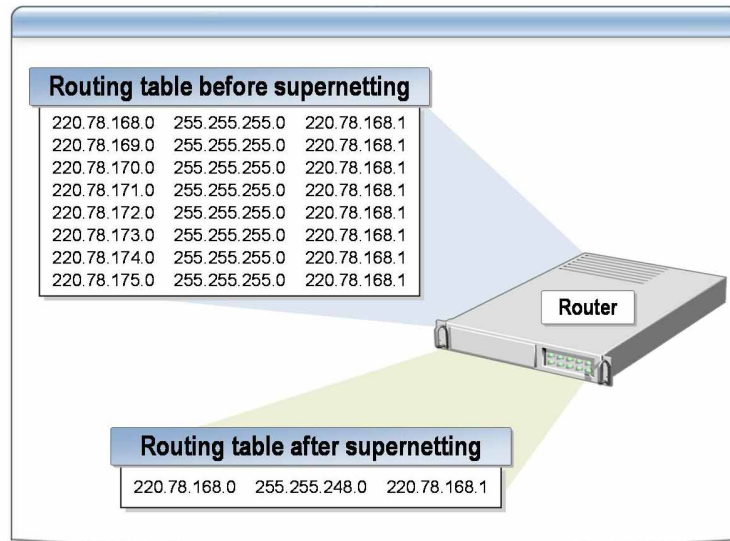
Procedure for eight subnets with up to 250 hosts

To achieve a requirement of 8 subnets with up to 250 hosts, subnet 3 bits of the subnetted network ID of 157.54.248.0/21. This produces 8 subnets (157.54.248.0/24, 157.54.249.0/24 through 157.54.254.0/24, 157.54.255.0/24) and allowing up to 254 hosts per subnet. All eight subnetted network IDs (157.54.248.0/24 through 157.54.255.0/24) are chosen as the network IDs, which fulfills the requirement.

The following table shows 8 subnets with 254 hosts per subnet.

Subnet Number	Network ID (Dotted Decimal)	Network ID (Network Prefix)
1	157.54.248.0, 255.255.255.0	157.54.248.0/24
2	157.54.249.0, 255.255.255.0	157.54.249.0/24
3	157.54.250.0, 255.255.255.0	157.54.250.0/24
4	157.54.251.0, 255.255.255.0	157.54.251.0/24
5	157.54.252.0, 255.255.255.0	157.54.252.0/24
6	157.54.253.0, 255.255.255.0	157.54.253.0/24
7	157.54.254.0, 255.255.255.0	157.54.254.0/24
8	157.54.255.0, 255.255.255.0	157.54.255.0/24

What Is Supernetting?



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

Introduction

CIDR is a method of assigning and aggregating addresses. One common function of CIDR is supernetting (also known as route aggregation), the process of combining multiple consecutive network IDs of the same IP address class into a single block. For example, you can implement supernetting to collapse multiple network ID entries into a single entry corresponding to the entire class C network IDs allocated to your organization.

How It Works

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 supernetting for 2000 hosts

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

- A single class B network ID. This approach would waste 63,000 addresses.
- Eight different class C addresses that can support $8 \times 254 = 2032$ 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 2,000 hosts. Using supernetting, IANA or 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.

Using CIDR to Implement Supernetting

Class C Example		
	Network ID	Subnet mask (binary)
Starting	220.78.168.0	<u>11011100</u> 01001110 10101000 00000000
Ending	220.78.175.0	<u>11011100</u> 01001110 10101111 00000000

CIDR Entry		
Network ID	Subnet mask	Subnet mask (binary)
220.78.168.0	255.255.248.0	<u>11111111</u> 11111110 11111000 00000000

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

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

Conceptually, CIDR creates the routing table entry: Starting Network ID count, where Starting Network ID is the first class C network ID and the count is the number of class C network IDs allocated. In practice, a supernetted subnet mask is used to convey the same information.

Example of how CIDR creates the routing table entry

In the following table, eight class C network IDs are allocated starting with network ID 220.78.168.0.

Network ID	Subnet mask	Subnet mask (binary)
Starting Network ID	220.78.168.0	<u>11011100</u> 01001110 10101000 00000000
Ending Network ID	220.78.175.0	<u>11011100</u> 01001110 10101111 00000000

Note that the first 21 bits (underlined) of all the preceding class C network IDs are the same. The last three bits of the third octet vary from 000 to 111. The following table describes the values of the CIDR entry in the routing tables of the Internet routers.

Network ID	Subnet mask	Subnet mask (binary)
220.78.168.0	255.255.248.0	<u>11111111</u> 11111111 11111000 00000000

In network prefix or CIDR notation, the CIDR entry is 220.78.168.0/21. The number 21 refers to the number of 1 bits used in the subnet mask.

Note Because subnet masks are used to express the count, class-based network IDs must be allocated in groups corresponding to powers of 2.

Address Space Perspective

The use of CIDR to allocate addresses promotes a new perspective on IP network IDs. The CIDR block [220.78.168.0, 255.255.248.0] can be thought of in two ways:

- A block of eight class C network IDs.
- An address space in which 21 bits are fixed and 11 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.

