INTRO

Introduction to Cisco Networking Technologies

Version 2.1

Lab Guide

Text Part Number: 97-2302-01

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece
Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania
Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland
Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Lab Guide

Overview

This guide presents the instructions and other information concerning the activities for this course. You can find the solutions in the activity Answer Key.

Outline

This guide includes these activities:

- Lab 1-1: Building a Simple Serial Connection
- Lab 2-1: Building a Simple Ethernet Network
- Lab 3-1: Creating an Ethernet Hub-Connected Network
- Lab 3-2: Creating an Ethernet Switch-Connected Network
- Lab 4-1: Adding a Default Gateway
- Lab 5-1: Converting Decimal to Binary and Binary to Decimal
- Lab 5-2: Classifying Network Addressing
- Lab 5-3: Computing Useable Subnetworks and Hosts
- Lab 5-4: Calculating Subnet Masks
- Lab 5-5: Modifying the IP Subnet Mask
- Lab 6-1: Establishing a Telnet Connection to a Remote Terminal Server
- Lab 8-1: Establishing a Telnet Connection to the Cisco Remote Lab
- Lab 8-2: Completing Switch Startup and Initial Configuration
- Lab 8-3: Completing Router Startup and Initial Configuration
- Lab 8-4: Using the Router CLI
- Lab 8-5: Operating and Configuring a Cisco IOS Device
- Lab 9-1: Gathering Information About Neighboring Devices and Using System Files

Lab 1-1: Building a Simple Serial Connection

Complete this lab activity to practice what you learned in the related module.

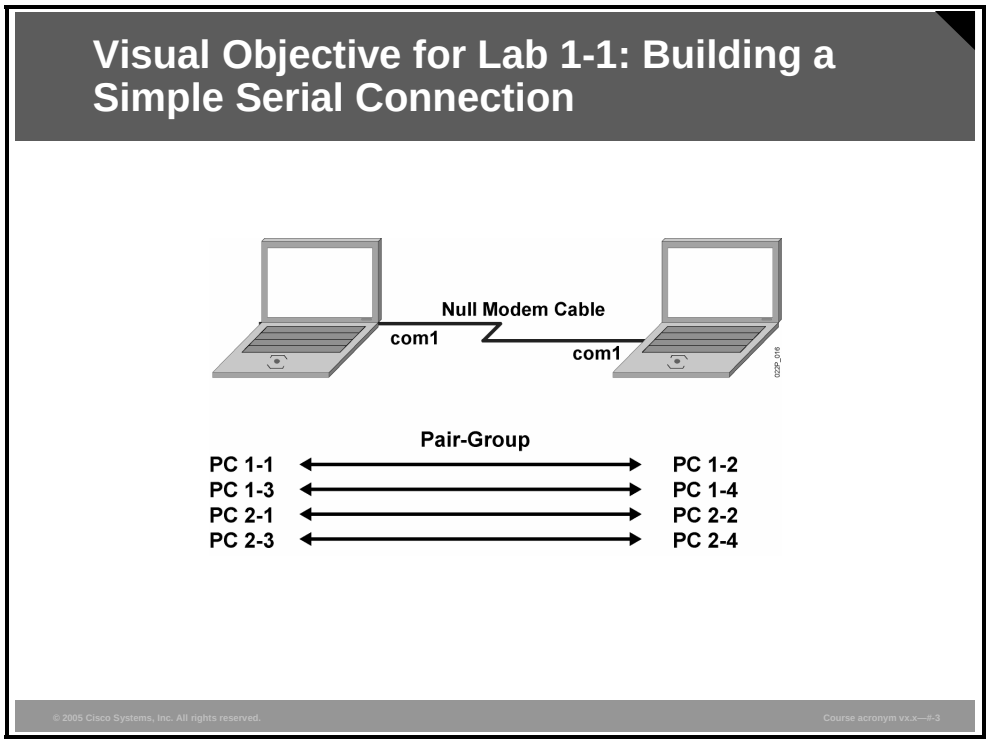
Activity Objective

In this activity, you will construct a simple serial connection. After completing this activity, you will be able to meet these objectives:

- Connect PCs using a serial null modem cable
- Use HyperTerminal to test connectivity

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Two PCs and supplied straight-through cable and (if necessary) serial null modem cables
- PCs running the Microsoft Windows 2000 or XP operating system

Command List

There are no commands used in this activity.

Job Aids

There are no job aids for this lab activity.

Task 1: Interconnect the Serial Communication Ports Between Your Assigned PCs

To begin the lab activity, you will physically connect the supplied serial cable.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Start the PC.
2.	Locate the communication port (COM**)** on your PC.
3.	Attach one end of the supplied serial cable, ensuring that the D-shaped plug fits without undue pressure.
4.	Finger-tighten the plug screws so that the plug will not accidentally fall out of the connector.
5.	When your partner has also completed this task, proceed to next task.

Activity Verification

You have completed this task when you attain this result:

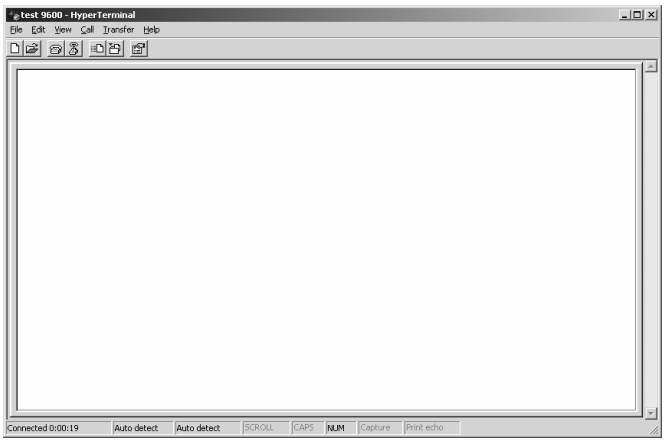
- You successfully interconnected your PC with the PC of your partner, using the provided null modem cable.

Task 2: Open the HyperTerminal Application

You will open the HyperTerminal application.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the Microsoft Windows Start menu, make the following choices in order: ■ **Programs** ■ **Accessories** ■ **Communications** ■ **HyperTerminal** ■ **INTRO 9600.ht.**	
2.	You should now see the terminal window of HyperTerminal active on your screen.	
3.	Observe that in the bottom row of the window; the third box shows the current settings: Bit rate = 9600, number of bits = 8, parity = none, and number of stop bits = 1	

Activity Verification

You have completed this task when you attain this result:

- You have viewed the settings stated in Step 3 of this task.

Task 3: Exchange Messages with the PC of Your Partner

You will exchange text between PCs by entering the text from the keyboard. You should be working with your partner to see (and hear) how your partner is receiving your text and report how you are receiving text from your partner.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Enter the following characters from the keyboard: **This is a message from PC x** (where "x" is your PC ID). **What is your name?**
2.	Do you see the characters that you are typing? Note in the space provided your observations regarding the output.
3.	Check the PC of your partner to see how the message looked.

Activity Verification

You have completed this task when you attain this result:

- You successfully sent text between the PCs.

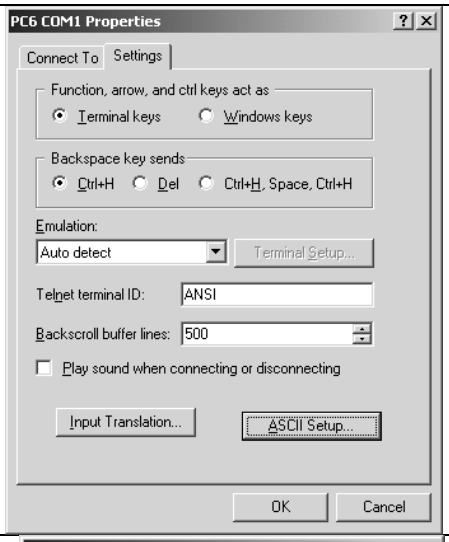
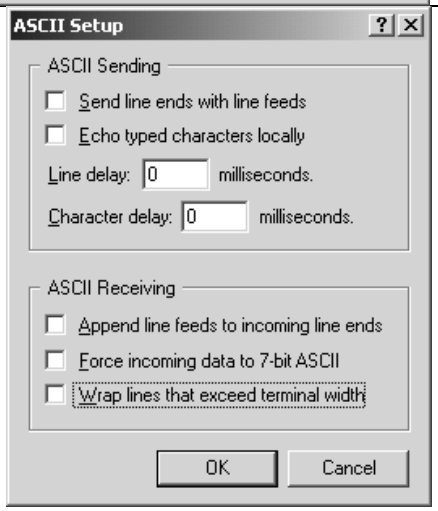
Task 4: Change Your HyperTerminal Configuration Settings

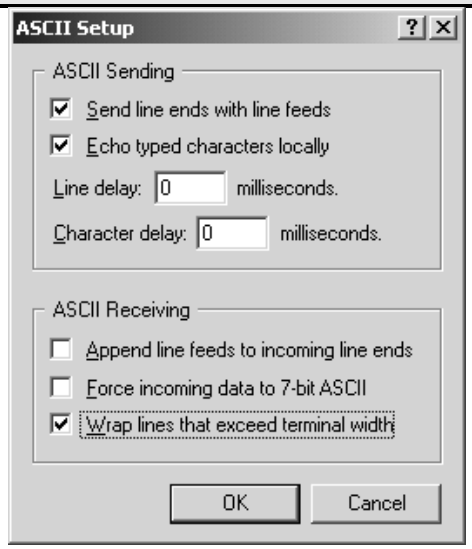
You should have seen the following problems with the viewing of the text messages.

1. There was no echo of the characters sent, which makes it hard to type accurately. This can be modified by setting local echo.
2. When a carriage return was received, the cursor returned to the beginning of the line and did *not* start a new line. This can be modified by setting the carriage return to carriage return plus line feed.
3. When a line reached the right edge of the application window, the characters might go out of view. This can be modified by setting automatic line wrap.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the HyperTerminal application window, choose **File** and then **Properties**. Then choose the **Settings** tab.	
2.	Click the **ASCII Setup** button.	
3.	Make the following choices by checking the appropriate check boxes: ■ **Send line ends with line feeds** ■ **Echo typed characters locally** ■ **Wrap lines that exceed terminal width**	

Step	Action	What You See
4.	When you have finished, the ASCII Setup window should resemble that shown in the figure.	
5.	Click the **OK** button, then click **OK** in the Properties window.	

Task 5: Retest Your Messages

You should now see that the problem with the viewing of the text messages has been corrected.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Enter the following characters from the keyboard**:** **This is a message from PC x** (where "x" is your PC ID)**.** **What is your name?**
2.	You should now see the characters as you are typing them.

Activity Verification

You have completed this task when you attain this result:

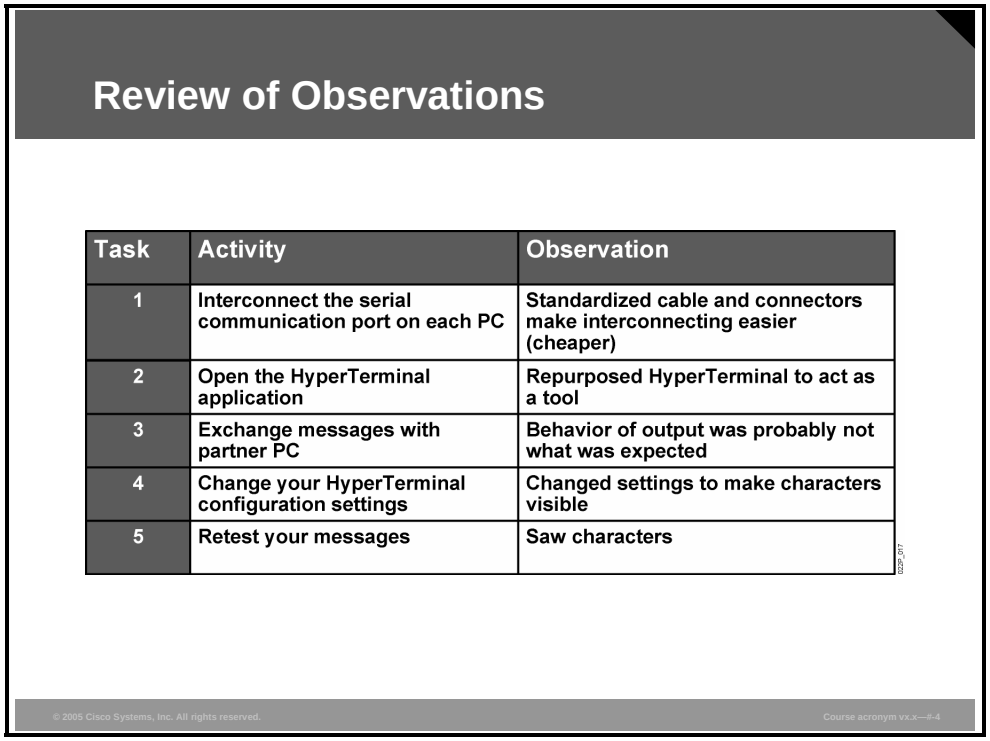
- You resend text with the new settings.

Lab 1-1: Debrief

This debriefing session covers the activities in the “Building a Simple Serial Connection” lab. The topics addressed include a review of the correct steps for building the serial connection, a discussion of the OSI model in relation to the components of the connection, a definition of the connection in terms of a set of network characteristics, and a definition of the tools that were used.

Review of Observations

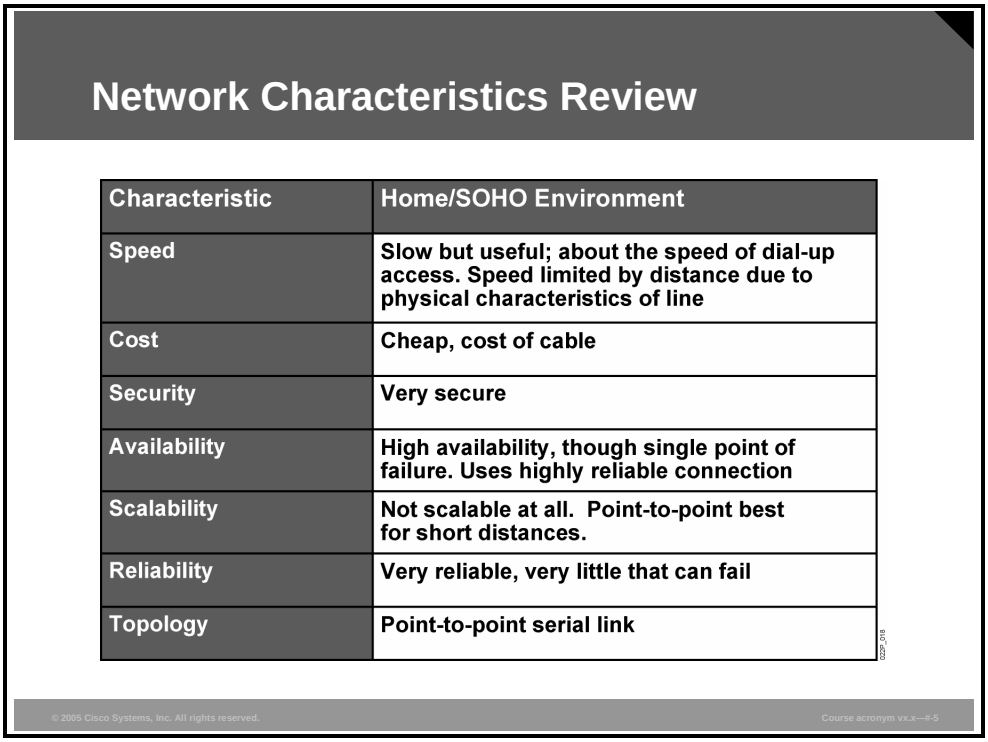
In this portion of the debriefing session, you will review the observations that were noted during the building of the serial connection.



This figure shows the observations that you should have made during the lab.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.

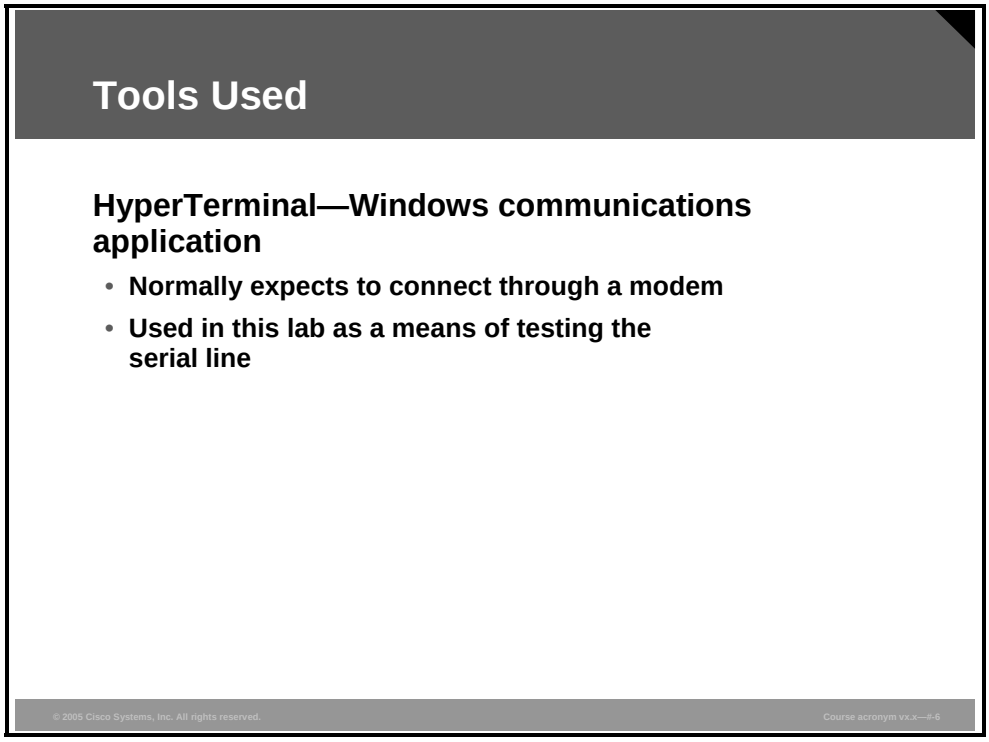


These are the characteristics for the simple serial connection that you created:

- **Speed:** The speed is slow but useful.
- **Cost:** This network connection is cheap (cost of cable).
- **Security:** This network is very secure.
- **Availability:** The availability is high.
- **Scalability:** The network is not scalable at all.
- **Reliability:** The network is very reliable.
- **Topology:** The topology is a point-to-point serial link.

Tools

In this lab, one tool was used.



HyperTerminal is a Windows communications software application that provides terminal emulation and is used for testing the serial line.

Lab 2-1: Building a Simple Ethernet Network

Complete this lab activity to practice what you learned in the related module.

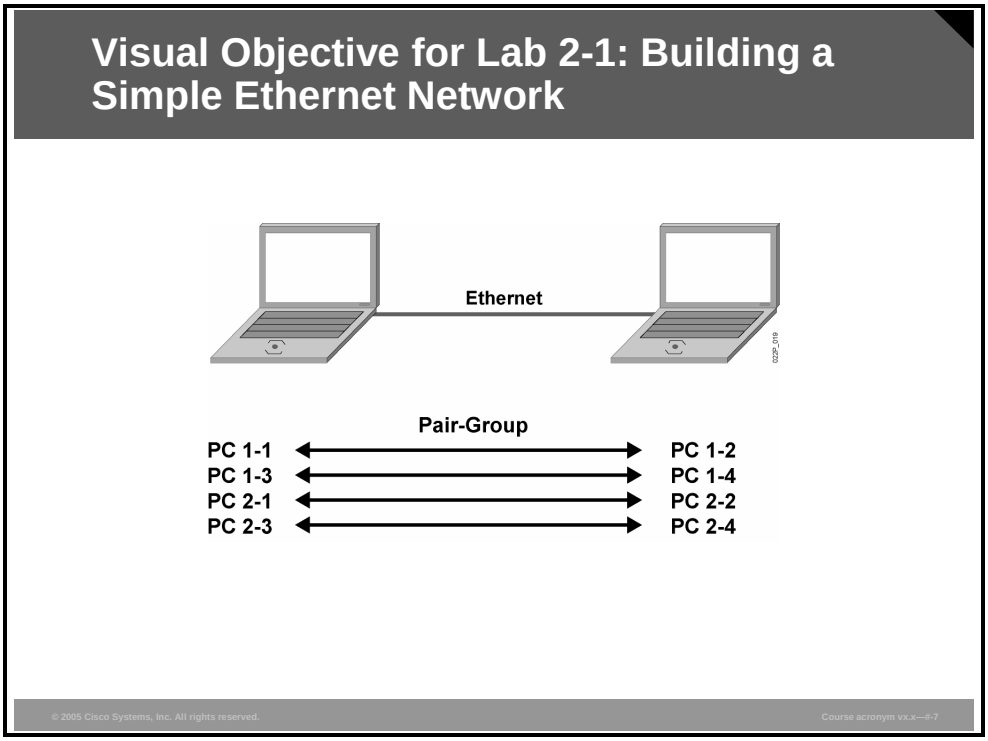
Activity Objective

In this activity, you will construct a simple Ethernet network. After completing this activity, you will be able to meet these objectives:

- Connect two PCs using an Ethernet data crossover cable
- Configure the PC Ethernet adapter
- Use Windows commands as tools to confirm the configuration, attributes, and behavior of the Ethernet connection
- Use Ethereal packet sniffer software to examine the frames that traverse the Ethernet link
- Place the networking entities and attributes appropriately in relation to the OSI model
- Identify the tools used to test and verify the network connection

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Two PCs and supplied Ethernet data and Ethernet data crossover cables
- PCs running the Windows 2000 or XP operating system
- Ethereal packet sniffer application software installed on the PCs

Note	Some companies do not permit packet sniffer software to be installed on their networks. Be sure that you are in compliance with the regulations of your company before performing this lab.

Command List

The table describes the commands used in this activity.

Command	Description
ipconfig	Displays current IP configuration of PC Ethernet adapters
ping *ip-address*	Sends IP echo request packets to supplied IP address
arp -a	Displays the current entries in the ARP table

Job Aids

There are no job aids for this lab activity.

Activity Preparation

Your instructor will provide the cables that you need to complete this lab activity. You will use the same PC workgroup name that you were assigned in the previous lab.

The table shows the IP configuration information for the PCs.

PC Name	Assigned IP Address	Assigned Subnet Mask
Pair Group 1a		
PC 1-1	192.168.1.11	255.255.255.240
PC 1-2	192.168.1.12	255.255.255.240
Pair Group 1b		
PC 1-3	192.168.1.21	255.255.255.240
PC 1-4	192.168.1.22	255.255.255.240
Pair Group 2a		
PC 2-1	192.168.1.11	255.255.255.240
PC 2-2	192.168.1.12	255.255.255.240
Pair Group 2b		
PC 2-3	192.168.1.21	255.255.255.240
PC 2-4	192.168.1.22	255.255.255.240

Task 1: Connect the PCs Using the Supplied Cable

To begin the activity you need to physically connect your PC with your partner's PC. If you insert the incorrect cable, however, you will *not* damage the adapter.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Connect your PC with your partner's PC, choosing one of the two supplied cables.
2.	Be sure to observe the RJ-45 connector wiring.

Activity Verification

You have completed this task when you attain this result:

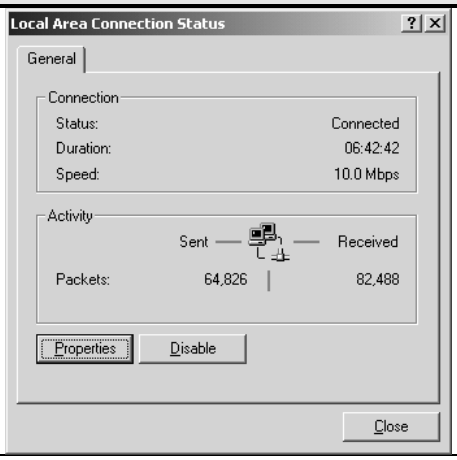
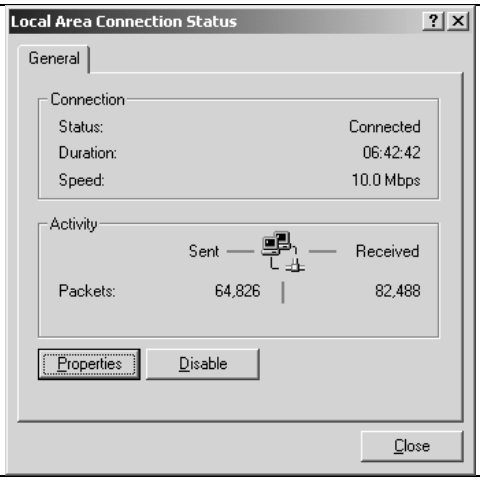
- You successfully connected your PC with the PC of your partner by using the Ethernet cable.

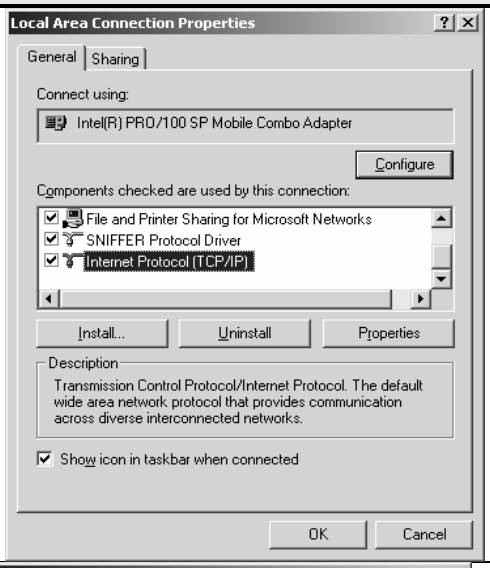
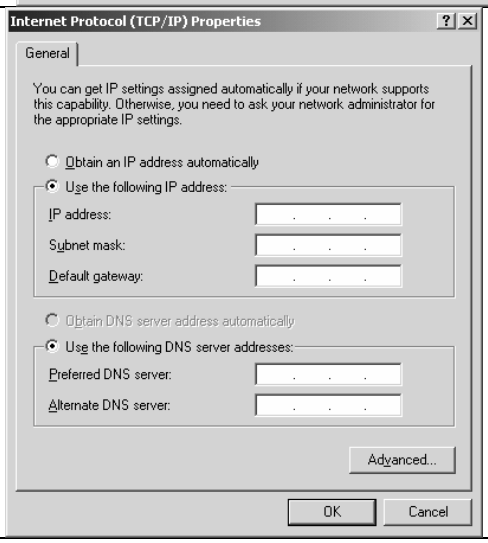
Task 2: Configure the PC Ethernet Adapter

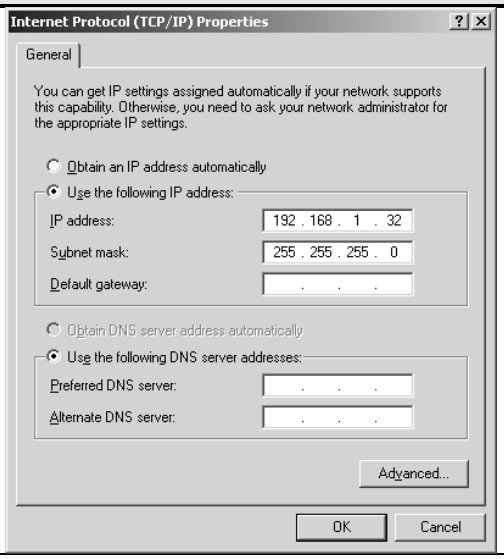
You will configure the Ethernet adapter on your PC.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the Windows screen, click **Start** and make the following choices: ■ **Settings** ■ **Network and Dial-Up Connections** ■ **Local Area Connection**	
2.	You should now see your local area connection status.	
3.	From the Local Area Connection Status window, click the **Properties** button.	

Step	Action	What You See
4.	From the Local Area Connection Properties window, scroll down and choose **Internet Protocol (TCP/IP)** and then click the **Properties** button.	
5.	From the Internet Protocol (TCP/IP) Properties window, click the **Use the following IP address** button.	

Step	Action	What You See
6.	Enter the IP address and subnet mask values assigned to your PC. Refer to the table in the Activity Preparation section at the beginning of the lab. All other fields should be left empty.	
7.	Click the **OK** button, which will close the Internet Protocol (TCP/IP) Properties window.	
8.	Click the **OK** button, which will close the Local Area Connection Properties window.	
9.	Close the Network and Dial-Up Connections window.	

Activity Verification

You have completed this task when you attain this result:

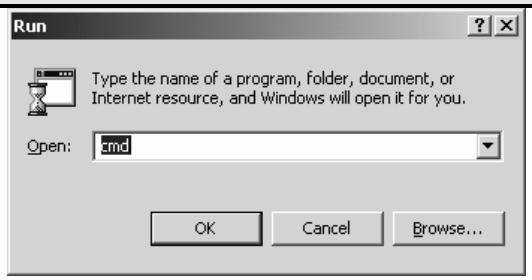
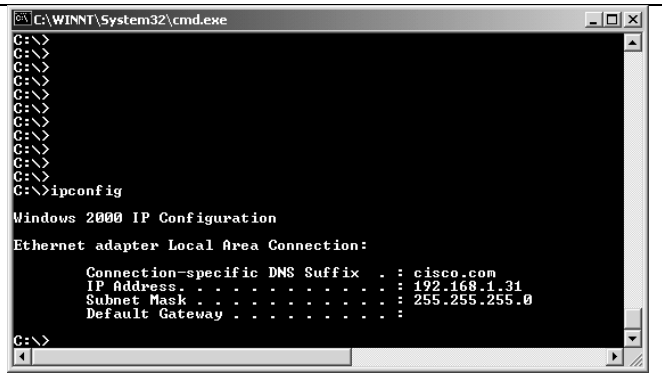
- You successfully configured the IP information.

Task 3: Use the ipconfig Command to Confirm Your IP Address Configuration

You will confirm your IP address configuration by using the **ipconfig** command.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From Windows: ■ Click **Start.** ■ Choose **Run.** ■ Enter **cmd** in the Open field. ■ Click the **OK** button.	
2.	From the command window, enter **ipconfig** and press the **Enter** key. The output should display the IP address and subnet mask that you entered. This information should match the assigned information. When all is correct, you can proceed to the next task.	

Activity Verification

You have completed this task when you attain this result:

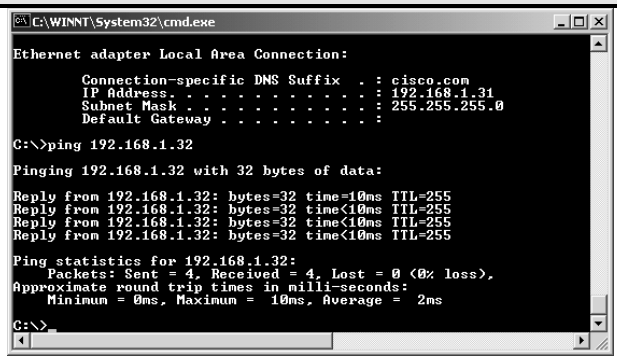
- You used the **ipconfig** command to verify your IP configuration values.

Task 4: Test Your Connection

In this task, you will test your connection by using the **ping** command. This task requires that your partners have completed their configuration successfully. Confirm that they are ready before you proceed.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the command window, enter **ping** *ip-address* (where "ip-address" is the address of your partner's PC). If you are successful, your output should resemble the figure.	
2.	If your **ping** command was successful, you can proceed to the next task. If not, you may need to check your configuration. You may also need to check that your partner's PC has also been configured correctly.	

Activity Verification

You have completed this task when you attain this result:

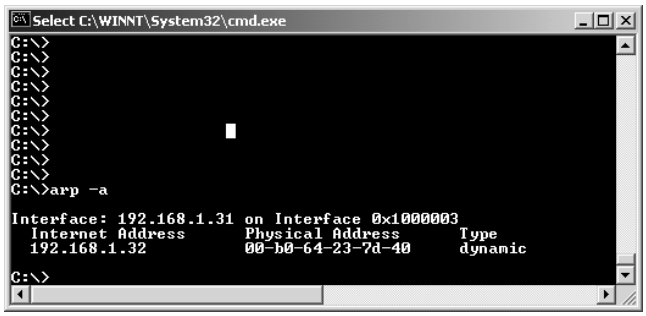
- You used the **ping** command to verify connectivity to your partner's PC.

Task 5: Display the Contents of Your ARP Table

You will now display the contents of your ARP table.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the command window, enter **arp –a**.	
2.	Record in the space provided the physical address associated with the IP address of your partner's PC, as shown in the output.	
3.	Minimize the cmd window. You will use it in a later task.	

Activity Verification

You have completed this task when you attain this result:

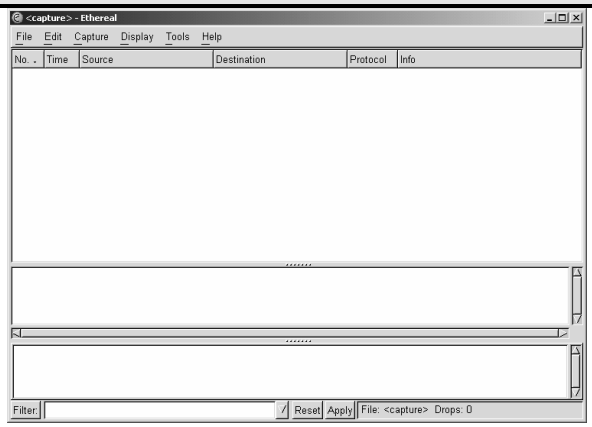
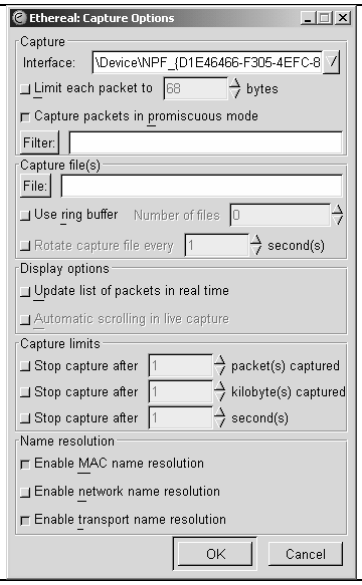
- You used the **arp –a** command to display and record the physical address of your partner's PC.

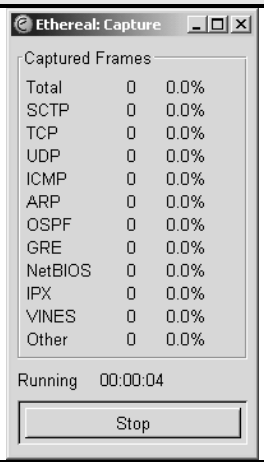
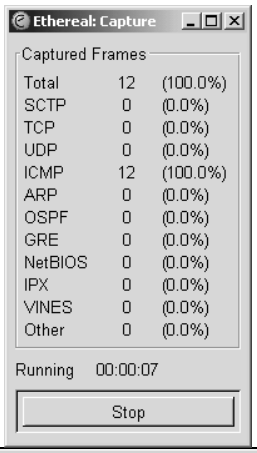
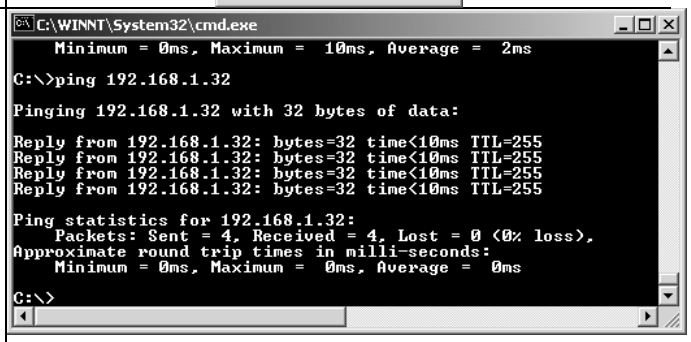
Task 6: Use the Ethereal Packet Sniffer

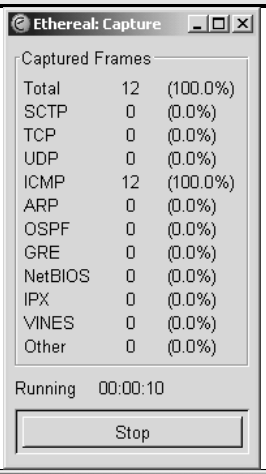
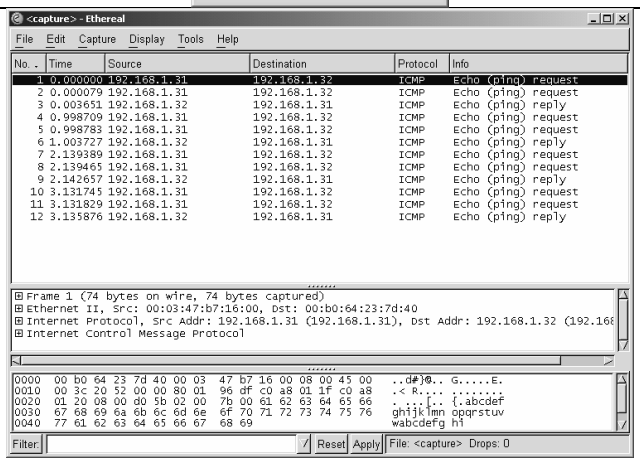
In this task, you will use a packet sniffer application to capture and examine frames. You will also be using this application in following labs. The program may at first seem quite confusing, but you will concentrate on the output display and ignore the many options that are available.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From your desktop, launch the Ethereal application using the shortcut.	
2.	From the menu, make the following choices: ■ **Capture** ■ **Start** The Ethereal Capture Options window opens.	

Step	Action	What You See
3.	There are no special options to choose, so click the **OK** button. The Ethereal: Capture window opens.	
4.	Reopen the minimized cmd window and ping your partner's PC.	
5.	You should see the packet count incrementing in the Ethereal: Capture window.	
6.	When the ping is complete, minimize the cmd window again.	

Step	Action	What You See
7.	Return to the Ethereal: Capture window and click the **Stop** button.	
8.	The main screen should now display the captured packets. Your display should resemble the figure. The Ethereal display area is in three sections: ■ The first section has the packet capture information. This has a number of columns: No., Time, Source, Destination, Protocol, and Info. ■ The middle section decodes information in OSI Layer 1, Layer 2, and Layer 3. To see this detailed information, click the plus (+) sign to open and then the minus (-) sign to close. ■ The third section displays the first 68 bytes of the packet in hexadecimal form, with the corresponding ASCII values adjacent.	
9.	Experiment to find out what information you can obtain about the packets that you captured in Step 5 of this task.	
10.	Answer the following questions in the space provided: What is the smallest time increment of the time column? What protocol is used for the echo request packet? What is the Ethertype number of the IP protocol in hexadecimal?	

Activity Verification

You have completed this task when you attain these results:

- You used the Ethereal packet sniffer application software to capture and display ping packets.
- You answered the questions about the sniffer display correctly.

Task 7: Relate the Ethernet Connection to the OSI Model

In this task, you will relate the Ethernet network connection that you have built to the OSI model.

Activity Procedure

In the spaces provided in the table, indicate the correct layer for the following:

- ARP protocol
- Ethernet frame
- IP packet
- Ethernet data cable

OSI Layer	Item, Entity, or Attribute
1 (Physical)	
2 (Data link)	
3 (Network)	

Activity Verification

You have completed this task when you attain this result:

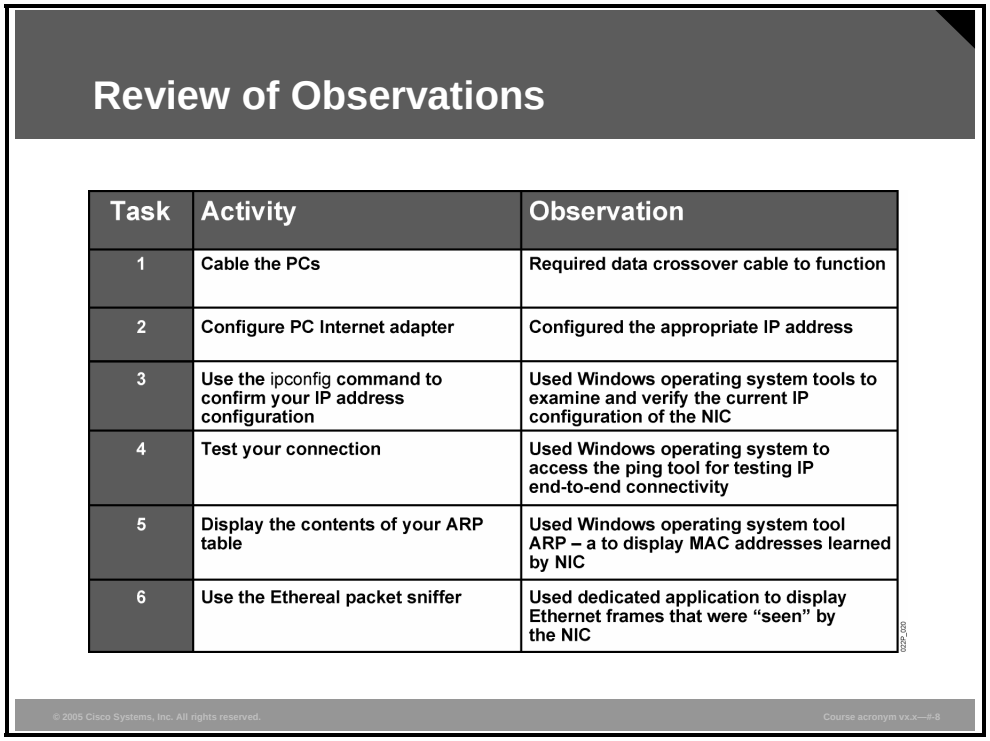
- You correctly completed the OSI information table.

Lab 2-1: Debrief

This debriefing session covers the activities in the “Building a Simple Ethernet Network” lab. The topics addressed include a review of the correct steps for building an Ethernet network, a discussion of the OSI model in relation to the components of the Ethernet network, a definition of the Ethernet network in terms of a set of network characteristics, and a review of tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the “Building a Simple Ethernet Network” lab.



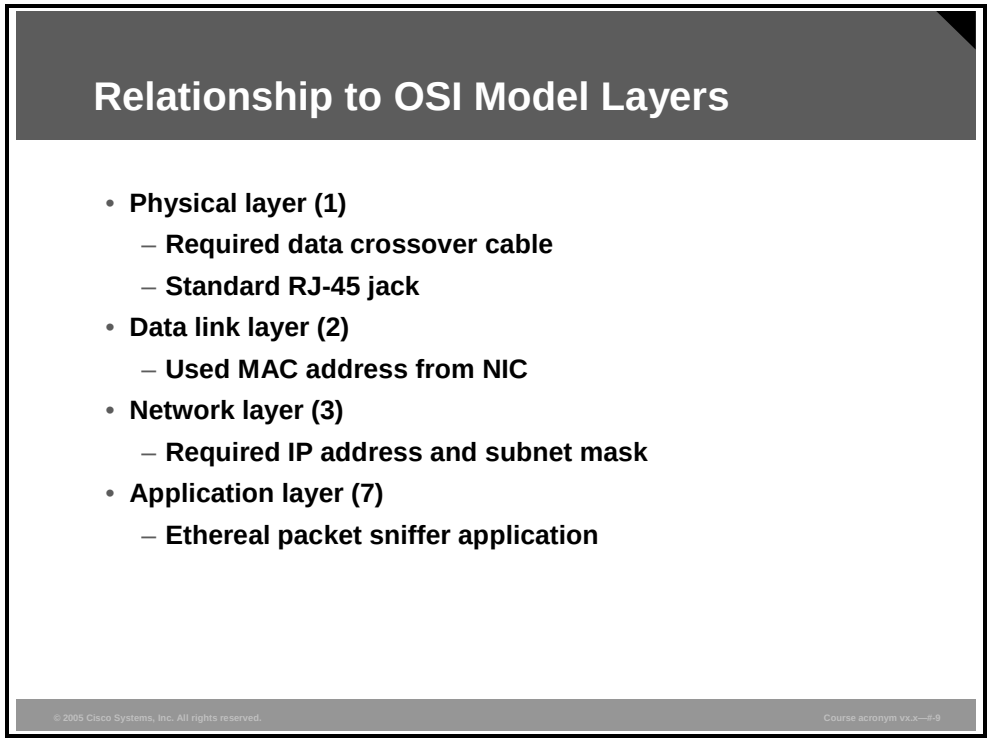
The figure shows the observations that you should have made during the lab activity in which you created a simple Ethernet network, as follows:

- **Task 1:** You had to select a data crossover cable to connect the PCs.
- **Task 2:** Using the Windows operating system, you had to configure the IP protocol parameters associated with the Ethernet NIC.
- **Task 3:** After you have entered the configuration information, it is always good practice to verify that the information is correct.
- **Task 4:** Once the configuration is done, the connection needed to be tested. You tested it using the IP **ping** command. Ping is based on the IP ICMP protocol, which is discussed in another module.

- **Task 5:** The Windows **ARP** command is used to display the learned MAC addresses associated with IP addresses. On a point-to-point link, only one association should be displayed, that of the NIC of your partner's PC.
- **Task 6:** A packet sniffer application was used to display the contents of all frames seen by the NIC. The sniffer display was in the format of the OSI seven-layer model. The sniffer will be used in subsequent labs to investigate the behavior of a more complex Ethernet network and also the behavior of the TCP/IP protocol.

Relationship to OSI Model Layers

Using the OSI model, you can identify the entities and attributes that were used in this lab.

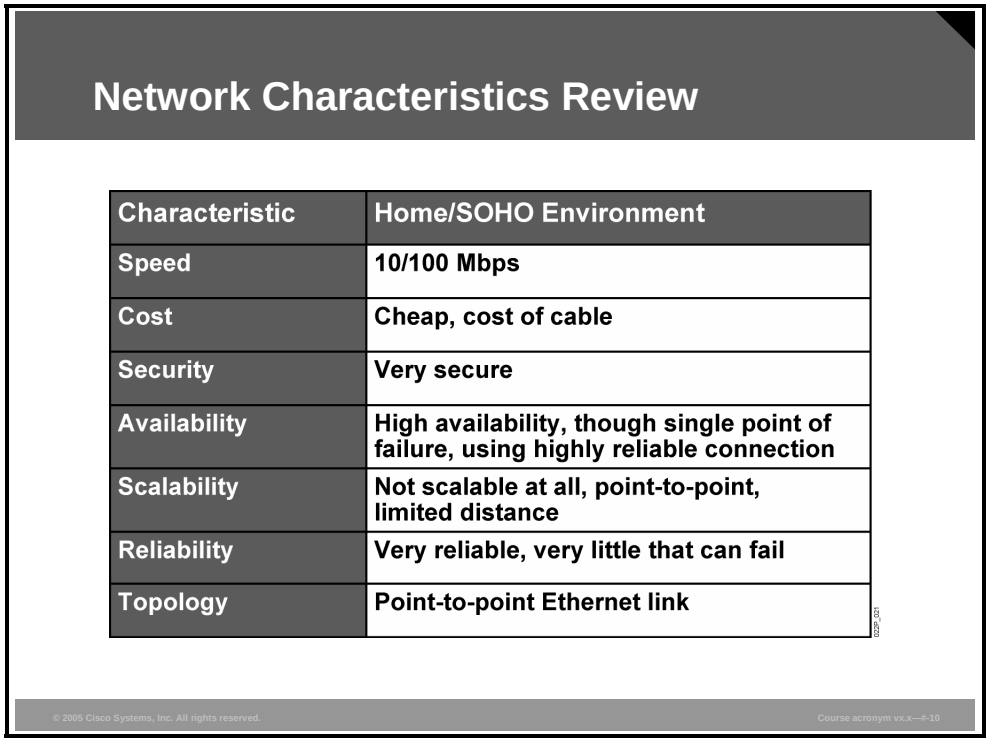


You can observe these layers of the OSI model in relation to the lab:

- **Physical layer (1):** A data crossover cable was required. This cable is necessary when you are connecting identical networking devices.
- **Data link layer (2):** The MAC address that was programmed into the NIC was used. This address would not normally be changed; however, it is possible to change it.
- **Network layer (3):** To test the Ethernet connection, you needed to use the IP protocol. The IP protocol requires two parameters: an address and a subnet mask. These parameters were provided in the lab information.
- **Application layer (7):** A packet sniffer application was used. Although it is quoted as operating at the application layer, the sniffer software works with the NIC card to get the frame data.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.

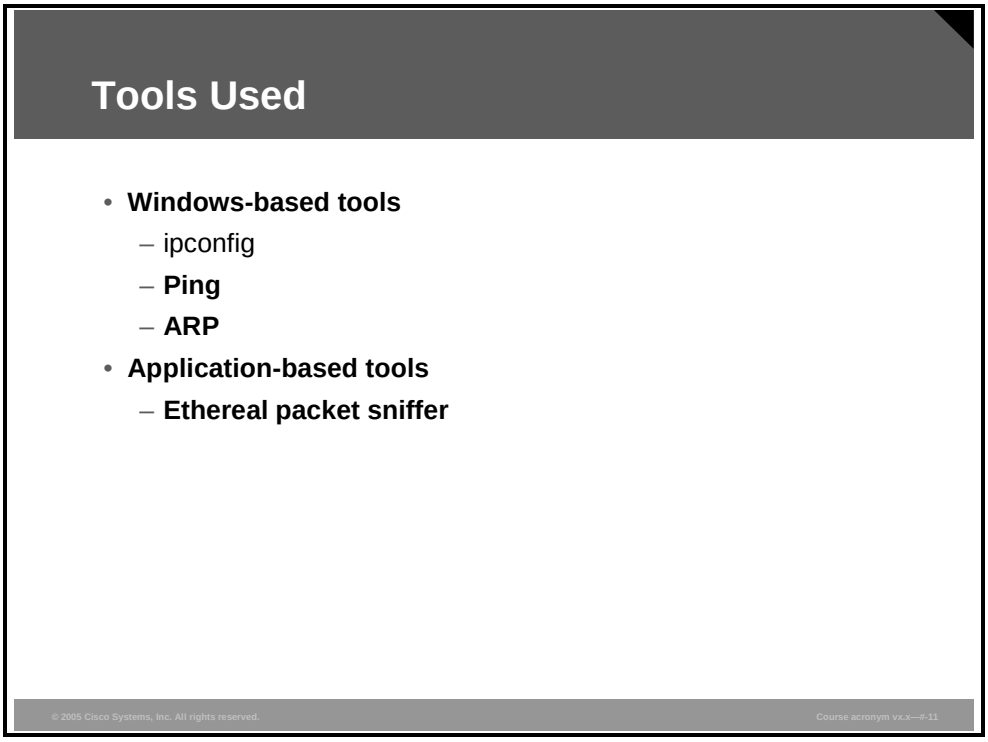


The change of subnet mask does not change the fundamental characteristics of the Ethernet switch-connected network:

- **Speed**: In the home or SOHO environment, the current Ethernet speeds are 10 or 100 Mbps, although other than cost, there is nothing to stop the adoption of the faster Ethernet speeds of 1 Gbps and 10 Gbps.
- **Cost**: The cost of this type of implementation is low even by home user standards. Most PCs and portables have Ethernet NICs built in, and the cost of the cable is the only add-on.
- **Security:** Using Ethernet in point-to-point mode means that there is *no* security issue, other than ensuring that the PCs themselves do not have any viruses or Trojan horse software.
- **Availability:** The probability that the network is available is very high. It is limited to the availability of the PCs (both need to be available).
- **Scalability:** This network is not scalable at all. This type of connection is not realistic and is only being considered as a means of incrementally investigating the operation and characteristics of the Ethernet protocol.
- **Reliability:** The chance of data being transferred with errors is extremely low; the intrinsic reliability is therefore high.
- **Topology:** The topology is point-to-point.

Tools

In this lab, a number of tools were used.



Lab 3-1: Creating an Ethernet Hub-Connected Network

Complete the lab activity to practice what you learned in the related module.

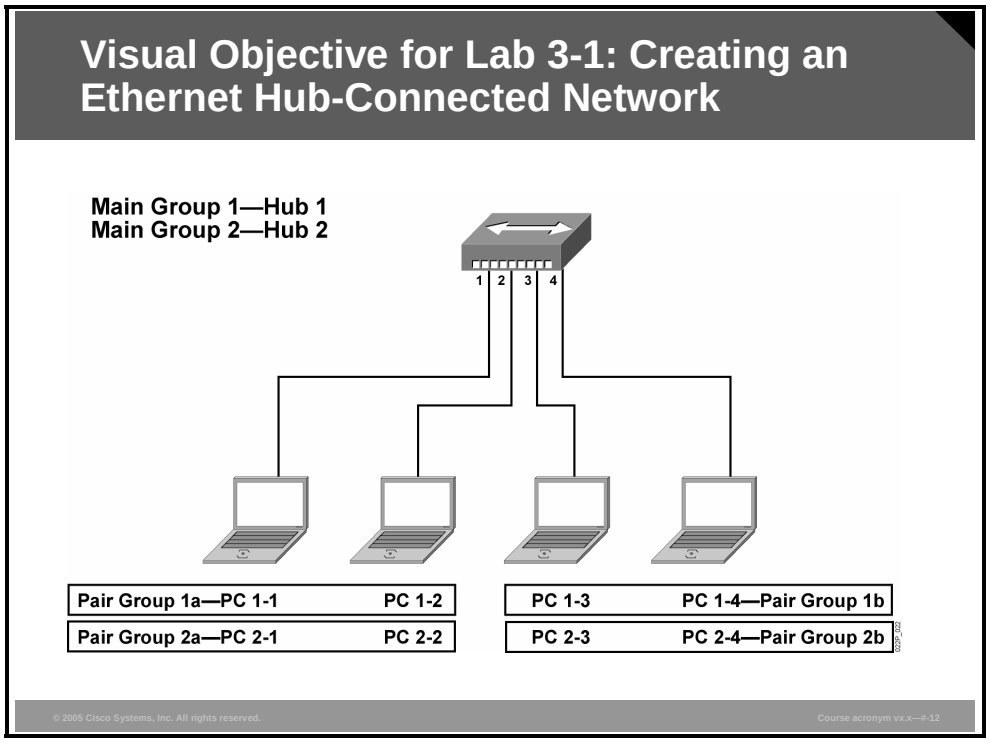
Activity Objective

In this activity, you will connect a simple hub-connected Ethernet network and examine its behavior. After completing this activity, you will be able to meet these objectives:

- Connect four PCs using an Ethernet hub
- Test network and connectivity
- Use Windows commands as tools to confirm the configuration, attributes, and behavior of the Ethernet connection
- Use Ethereal packet sniffer software to examine the frames that are received by the NIC of the PC
- Use the OSI model to appropriately place the networking entities and attributes

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Four PCs, one four-port hub, supplied Ethernet data, and Ethernet data crossover cables
- PC running Windows 2000 or XP operating system
- Ethereal packet sniffer application software installed on the PCs

Command List

The table describes the commands used in this activity.

Command	Description
ipconfig	Displays current IP configuration of PC Ethernet adapters
ping *ip-address*	Sends IP echo request packets to supplied IP address
arp -a	Displays all the current entries in the ARP table
arp -d	Removes all the current entries in the ARP table

Job Aids

There are no job aids for this lab activity.

Activity Preparation

This table shows the IP configuration information for the PCs.

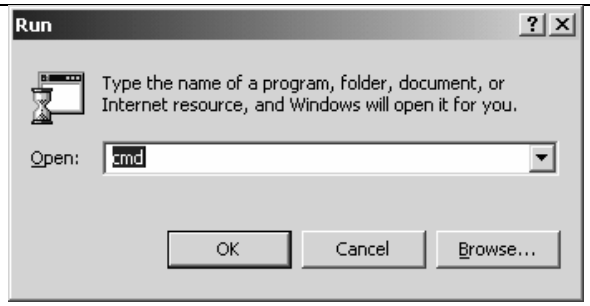
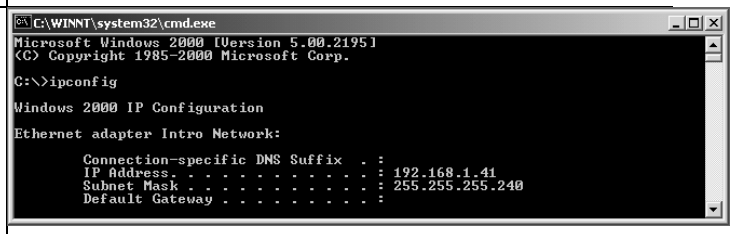
PC Name	Assigned IP Address	Assigned Subnet Mask
Pair Group 1a		
PC 1-1	192.168.1.11	255.255.255.240
PC 1-2	192.168.1.12	255.255.255.240
Pair Group 1b		
PC 1-3	192.168.1.21	255.255.255.240
PC 1-4	192.168.1.22	255.255.255.240
Pair Group 2a		
PC 2-1	192.168.1.11	255.255.255.240
PC 2-2	192.168.1.12	255.255.255.240
Pair Group 2b		
PC 2-3	192.168.1.21	255.255.255.240
PC 2-4	192.168.1.22	255.255.255.240

Task 1: Install the Hub and Verify the IP Address Configuration

In this task, you will confirm that the PCs of the other pair group are not reachable by the use of the **ping** command. By using the Ethereal packet sniffer application, you will observe that no frames were sent by their PCs in response to the **ping** command.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Working with the other members of your main group, connect the Ethernet network adapter (NIC) to the hub port assigned to your PC as designated. Make sure that you select the correct type of cable. You should know whether it should be a data crossover or straight-through cable.	
2.	Ensure that the hub is connected to a power outlet and switched on. Normally, a green link light on the hub shows that there is a successful link or physical layer connection.	
3.	Confirm that your IP address configuration matches that assigned to your PC in the lab visual objective.	
4.	From Windows: ■ Click **Start**. ■ Choose **Run**. ■ Enter **cmd** in the Open field. ■ Click the **OK** button.	
5.	From the command window, enter **ipconfig**. The output will display the current IP address and subnet mask configured on your PC. This information should match the assigned information in the Activity Preparation table at the beginning of this lab. When all is correct, proceed to next task.	

Activity Verification

You have completed this task when you attain these results:

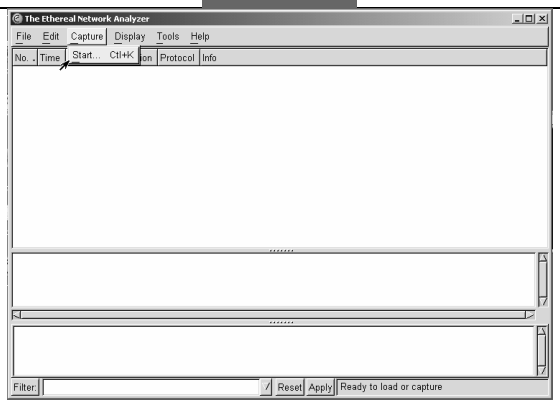
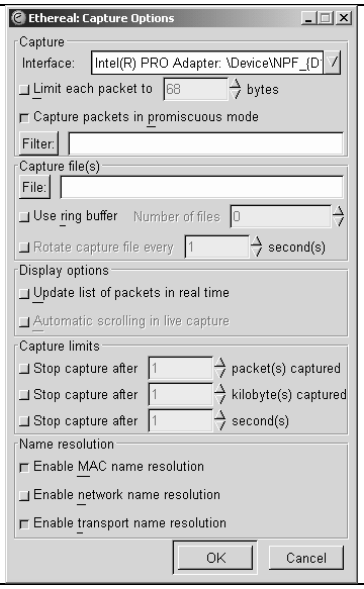
- You successfully attached your PC with the PC of your partners to the Ethernet hub, using the appropriate cable type.
- You used the **ipconfig** command to verify your IP configuration values.

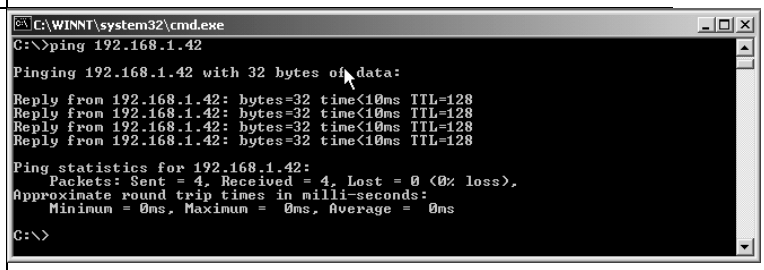
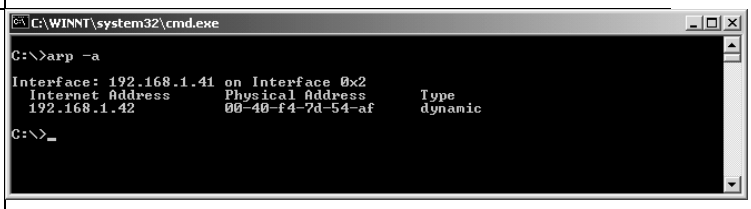
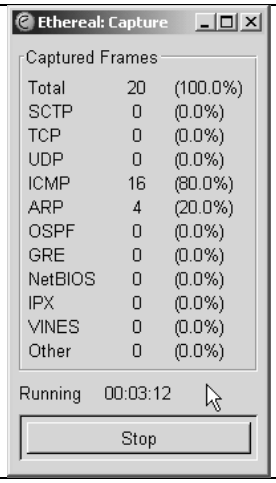
Task 2: Run Packet Capture and View the Recorded Frames

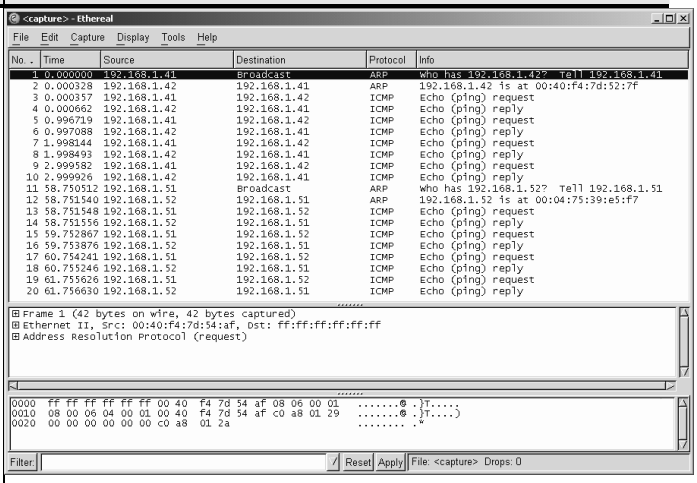
This task uses ping packets to examine the operation of a hub. Because both pair groups run this task simultaneously, the frames that are recorded will demonstrate that a hub will not filter out any frames from any attached devices by its operation. This task should confirm that the operation of a hub does *not* filter frames, because frames from all sources are seen and recorded by the sniffer application.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From your desktop, launch the Ethereal application using the shortcut.	
2.	Choose **Capture** > **Start** from the main menu. This action opens the Ethereal: Capture Options window.	
3.	There are no special options to choose, so click the **OK** button. The Ethereal: Capture window opens.	

Step	Action	What You See
4.	From the command window, enter **arp –d**. This action ensures that you start with an empty ARP table. If your ARP table is already empty, you will receive a message: “The specified entry was not found.”	
5.	From the command window, enter **ping** *ip-address*. (where “ip-address" is the address of your pair group partner’s PC—refer to the Activity Preparation table at the beginning of this lab). Your output should resemble the figure.	
6.	From the command window, enter **arp –a.** This will display the current entries in the ARP table of the PC. (You need to issue this command within 300 seconds of issuing the **ping** command.) The ARP entries are automatically removed after 300 seconds so that the PC does not have “old” information when requests are made to the ARP process.	
7.	Check that all PCs in the group have completed their ping tests before proceeding.	
8.	Return to the Capture window and click the **Stop** button.	

Step	Action	What You See
9.	Using the displayed information, record the source and destination IP addresses in the spaces provided in the “Source and Destination IP Addresses Pair” table, one entry for each unique pair. Record the protocols in the spaces provided in the “Protocols” table.	

Source and Destination IP Addresses Pair

Source IP Addresses	Destination IP Addresses

Protocols

Protocols

Activity Verification

You have completed this task when you attain these results:

- You used the **arp –d** command to clear the ARP table of entries.
- You used the **ping** command to verify connectivity to your partner’s PC.
- You used the **arp –a** command to display the current ARP table entries.
- You used the Ethereal packet sniffer application software to capture and display Ethernet frames and decode their contents.
- You completed the “Source and Destination IP Addresses Pair” table and “Protocol” table using the information from the sniffer display.

Task 3: Relate to the OSI Model

You will relate the Ethernet hub-connected network to the OSI model.

Activity Procedure

In the spaces provided below, indicate the correct layer for the following:

- ICMP
- ARP protocol
- Ethernet frame
- IP packet
- Ethernet hub
- Ethernet cable

OSI Layer	Item, Entity, or Attribute
1 (Physical)	
2 (Data link)	
3 (Network)	

Activity Verification

You have completed this task when you attain this result:

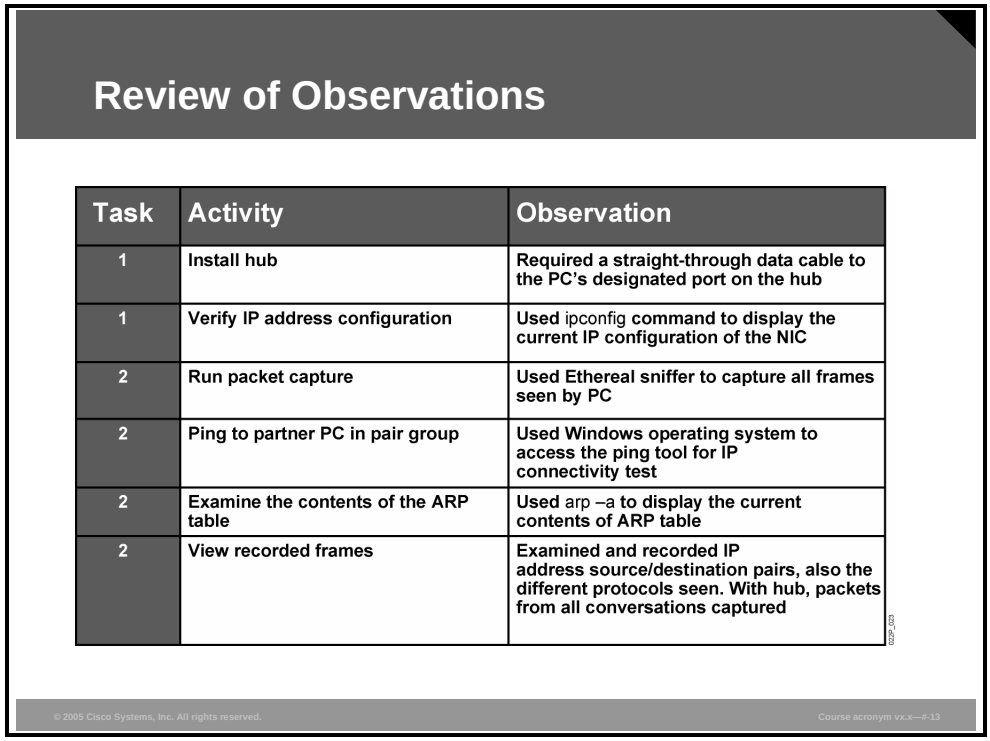
- You successfully completed the OSI information table.

Lab 3-1: Debrief

This debriefing session covers the activities in the "Creating an Ethernet Hub-Connected Network" lab. The topics addressed include a review of the correct steps for adding a hub, a discussion of the OSI model in relation to the components of the hub-connected network, a definition of the network in terms of a set of network characteristics, and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the addition of the hub in the lab.



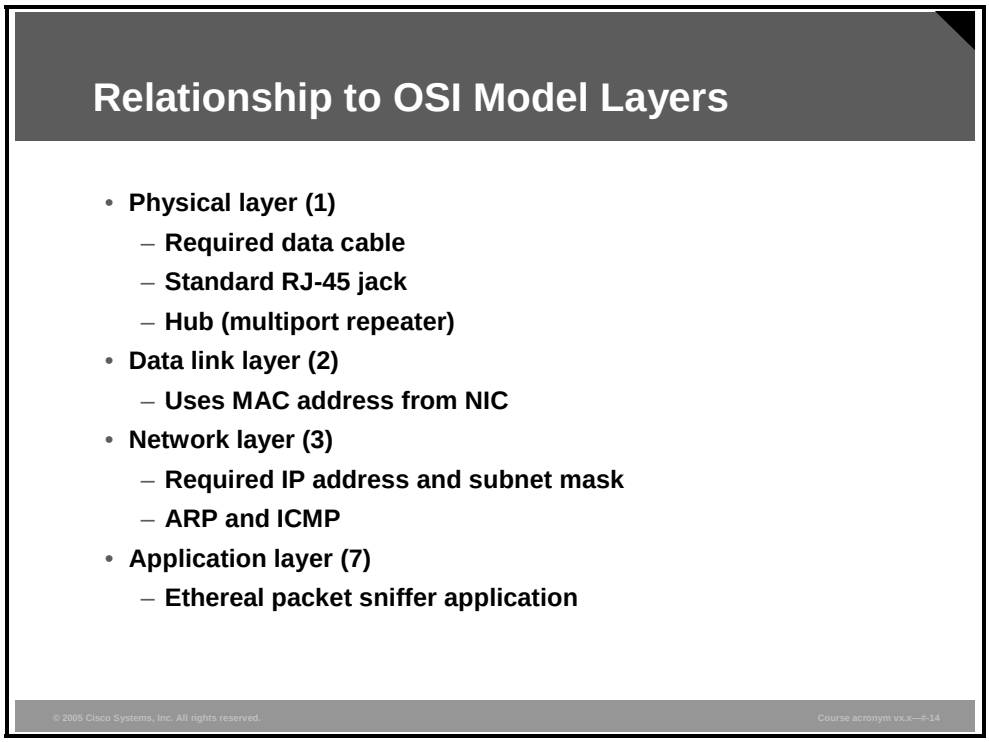
The figure shows the observations that you should have made during the lab activity as you created an Ethernet hub-connected network, as follows:

- **Task 1:** It was necessary to use a straight-through cable, because the connection was between an end system (PC) and a network device (hub). Attachment should have been to the designated ports, because fault restoration of even a small network can be facilitated by properly following the network documentation.
- **Task 1 continues:** The Windows operating system **ipconfig** command was used to ensure that the current IP address matches that required for the lab.
- **Task 2:** The Ethereal packet sniffer was used to record the frames received while the main group did pings between each PC within its pair group.
- **Task 2 continues:** The **ping** command was used to generate packets to test connectivity and reveal the operation of a hub.

- **Task 2 continues:** The **arp -a** command was used to display the current contents of the ARP table. Having a saved (cached) binding between the IP address and the MAC address saves unnecessary ARP requests. However, using a binding that is no longer accurate means that the host would not be reachable. Therefore, the timing out (aging) of entries is a balance between unnecessary network activity and the probability that the network has changed in some way.
- **Task 2 continues:** Your recording of the captured frames in the "Source and Destination IP Addresses Pair" table should reveal that the hub does not filter frames in any way. The recording of the protocols would show that ARP and ICMP were used. ICMP is used by ping. Within ICMP, you would have observed that there were ICMP echo requests and echo replies.

Relationship to OSI Model Layers

Using the OSI model, you can identify the entities and attributes that were used in this lab.



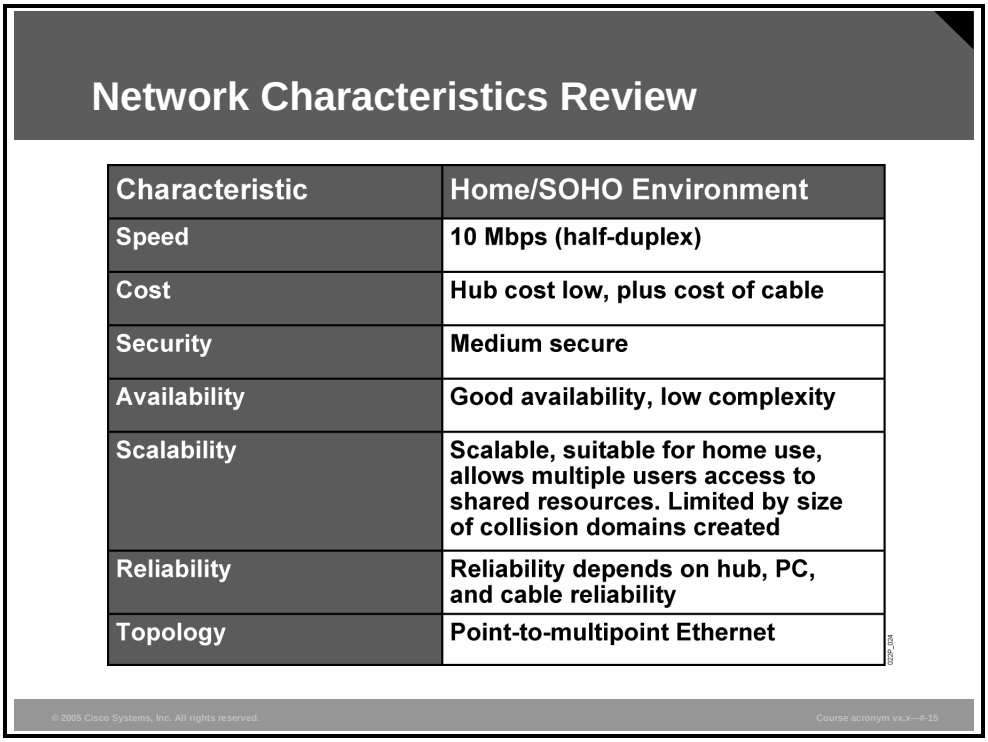
You can observe these layers of the OSI model in relation to the Ethernet network that you constructed:

- **Physical layer (1):** A straight-through data cable was required. The hub is also a Layer 1 device. Another name for a hub is "multiport repeater." The hub operates purely on the electrical voltages and has no knowledge of the upper-layer protocols.
- **Data link layer (2):** The Ethernet frame is the Layer 2 entity observed in the lab.
- **Network layer (3):** The packet protocols ARP and ICMP that were observed operated at Layer 3.
- **Application layer (7):** A packet sniffer application was used.

Being able to recognize at which layer of the OSI model the various protocols, packets, and frames operate will help in both comprehending and troubleshooting the network operation.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.



The point of these characteristics is to allow you to consider them whenever you are planning or implementing a change to a network. The scope of their implications depends on the specifics of the change.

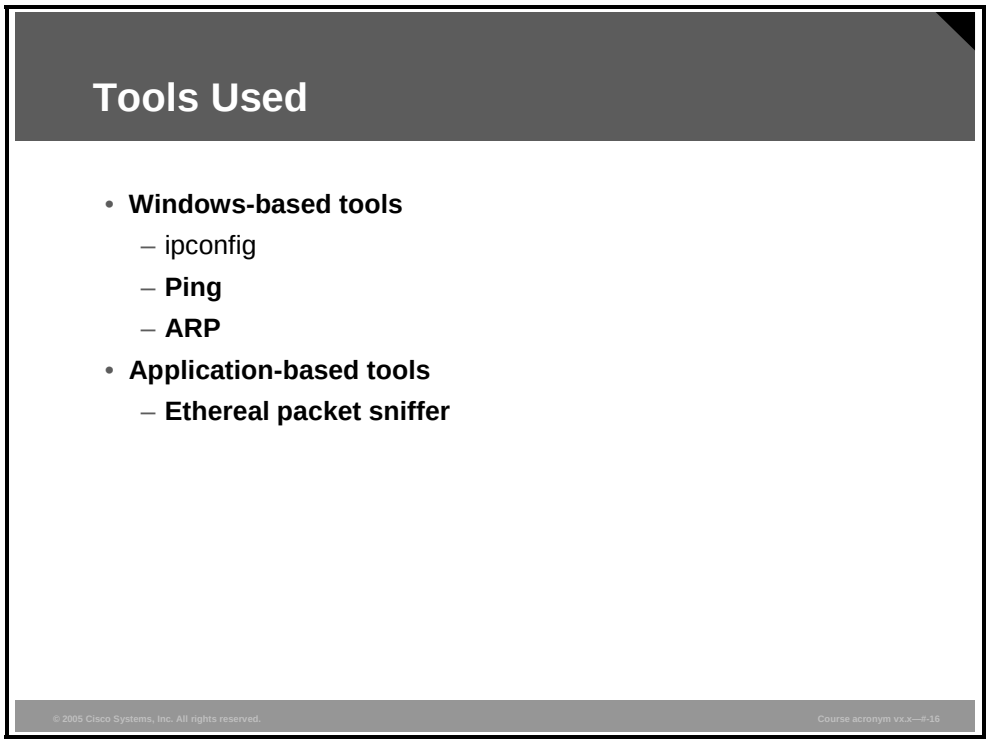
The Ethernet hub-connected network can be described in the following terms:

- **Speed:** The speed is slower than that of a directly connected point-to-point network. Hubs operate at 10 Mbps and in half-duplex mode only, further reducing the data transfer rate of the network. Hubs have been superseded in networks by switches.
- **Cost:** The cost of this type of network is low even by home user standards. Most PCs and portables have Ethernet NICs built in, and the cost of the hub is comparatively low. The cost for this type of device is measured in dollars per port.
- **Security:** Using Ethernet in a shared topology means that security is a bigger consideration. A hub does not filter frames; indeed, it repeats any frame received on one port out all the other ports. As you have seen, a packet sniffer application can capture these frames and allow them to be examined by anyone with a PC attached to the hubbed network. This fact should not be a problem in a home environment but may be problematic in a SOHO environment.
- **Availability:** The probability that the hubbed network will be available to carry traffic is high because the components of the network should have good individual reliability.

- **Scalability:** This type of network is scalable to a certain extent. During the early days of networking, hubs were the major component. However, their mode of operation means that high traffic volumes cause the network to slow down (decrease throughput) because of collisions and saturation of the Ethernet media.
- **Reliability:** You can think of two types of reliability in this example. First is the integrity of the data transmission (the chance of data being transferred with errors is extremely low). Collision will affect frames, but the FCS will mean that they are not accepted as being valid data. Second is the reliability of the network components, including PC hubs, cables, power supplies, and power source.
- **Topology:** The topology is point-to-multipoint.

Tools

In this lab, a number of tools were used.



Both Windows-based tools (including the **ipconfig** and **ping** commands) and the application-based Ethereal packet sniffer tool were used to construct this type of network.

Lab 3-2: Creating an Ethernet Switch-Connected Network

Complete the lab activity to practice what you learned in the related module.

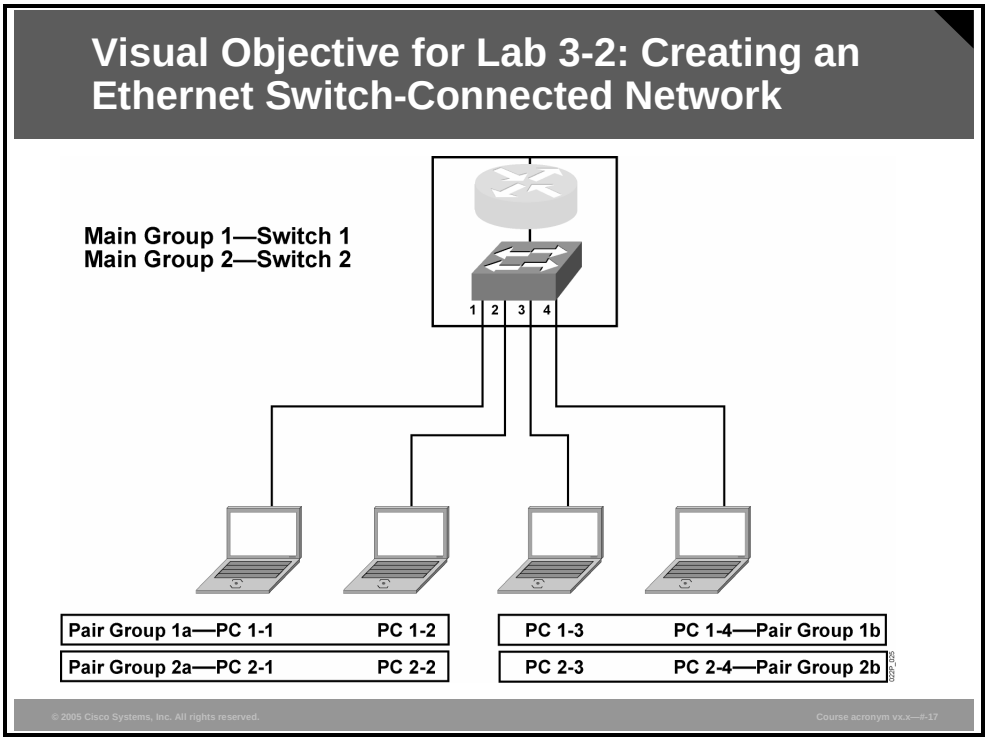
Activity Objective

In this activity, you will connect an Ethernet switch-connected network and examining its behavior. After completing this activity, you will be able to meet these objectives:

- Connect four PCs in your main group using an Ethernet switch
- Test network and connectivity
- Use Windows commands as tools to confirm the configuration, attributes, and behavior of the Ethernet connection
- Use Ethereal packet sniffer software to examine the frames that are received by the NIC of the PC
- Use the OSI model to appropriately place the networking entities and attributes
- Identify the tools used to test and verify the network connection

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Four PCs, one four-port switch, supplied Ethernet data cables
- PC running Windows 2000 or XP operating system
- Ethereal packet sniffer application software installed on the PCs

Note	Some companies do not permit packet sniffer software to be installed on their networks. Be sure that you are in compliance with the regulations of your company before performing this lab.

Command List

The table describes the commands used in this activity.

Command	Description
ipconfig	Displays current IP configuration of PC Ethernet adapters
ping *ip-address*	Sends IP echo request packets to supplied IP address
arp -d	Removes the current entries in the ARP table

Job Aids

There are no job aids for this lab activity.

Activity Preparation

The instructor will provide the cables that you need to complete this lab activity. You will use the same PC workgroup name that you were assigned in the previous lab.

IP Address and Subnet Mask

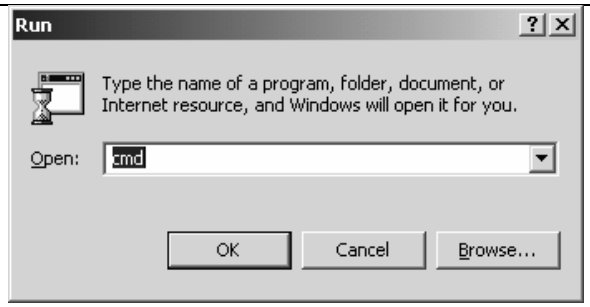
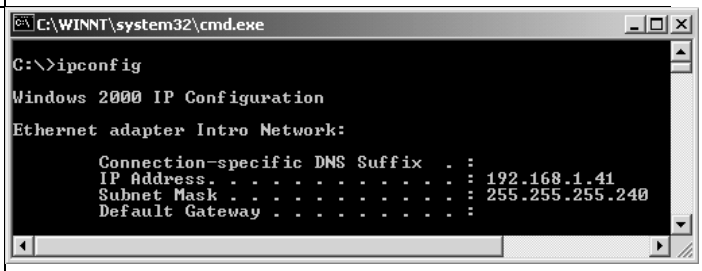
PC Name	Assigned IP Address	Assigned Subnet Mask	Switch Port Number
Main Group 1—Pair Group 1a			
PC 1-1	192.168.1.11	255.255.255.240	Switch 1 port 1
PC 1-2	192.168.1.12	255.255.255.240	Switch 1 port 2
Main Group 1—Pair Group 1b			
PC 1-3	192.168.1.21	255.255.255.240	Switch 1 port 3
PC 1-4	192.168.1.22	255.255.255.240	Switch 1 port 4
Main Group 2—Pair Group 2a			
PC 2-1	192.168.1.11	255.255.255.240	Switch 2 port 1
PC 2-2	192.168.1.12	255.255.255.240	Switch 2 port 2
Main Group 2—Pair Group 2b			
PC 2-3	192.168.1.21	255.255.255.240	Switch 2 port 3
PC 2-4	192.168.1.22	255.255.255.240	Switch 2 port 4

Task 1: Install the Switch and Verify the IP Address Configuration

In this task, you will install a switch and verify the IP address configuration.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Working with the other members of your main group, install the Ethernet switch by connecting a cable from your Ethernet network adapter to the switch port assigned to your PC, as shown in the "IP Address and Subnet Mask" table in the Activity Preparation section at the beginning of this lab.	
2.	Ensure that the switch is connected to a power outlet and that it is switched on. Normally, a green light on the switch shows that you have a successful link or physical layer connection. Confirm that your IP address configuration matches that assigned to your PC in the "IP Address and Subnet Mask" table in the Activity Preparation section at the beginning of this lab.	
3.	From Windows, click **Start** and then: ■ Choose **Run.** ■ Enter **cmd** in the Open field. ■ Click the **OK** button.	
4.	From the command window, enter **ipconfig**. The output should display the IP address and subnet mask that you entered. This information should match the assigned information. When all is correct, proceed to next task.	

Activity Verification

You have completed this task when you attain these results:

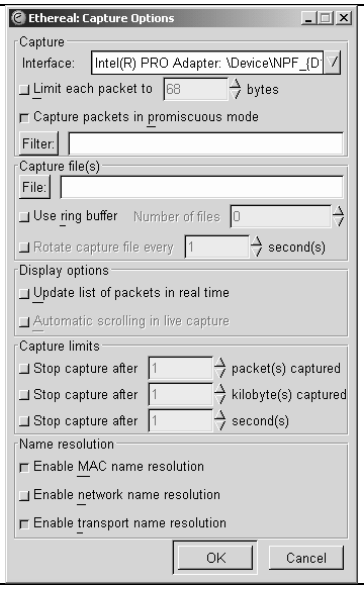
- You successfully attached a PC to the Ethernet switch, using the appropriate cable type.
- You successfully used the **ipconfig** command to verify the IP configuration of the PC.

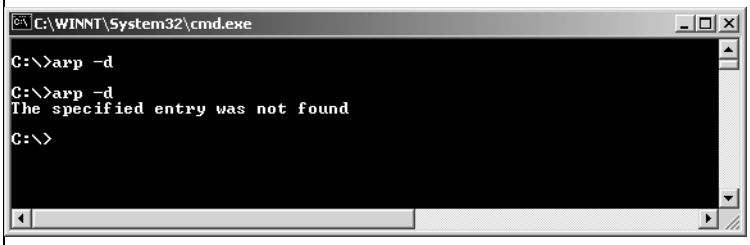
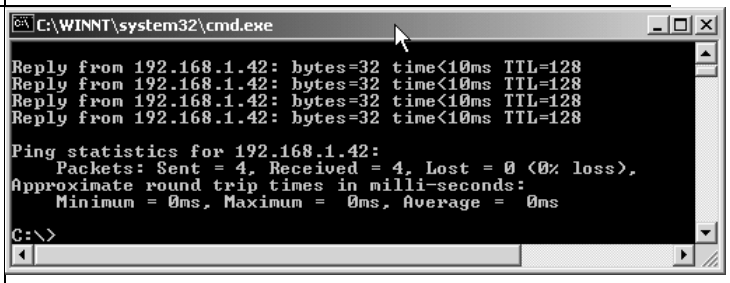
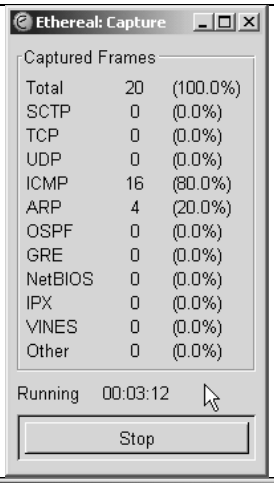
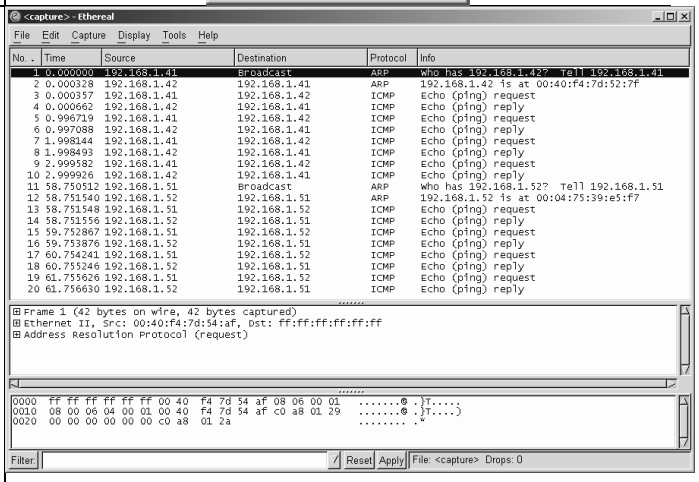
Task 2: Run Packet Capture and View the Recorded Frames

This task uses ping packets to examine the operation of a switch. Because both pair groups run this task simultaneously, the frames that are recorded will demonstrate that a switch will intelligently filter out some frames from attached devices. This task should confirm that the operation of a switch filters frames, because frames from all sources are *not* seen and recorded by the Ethereal application.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From your desktop, launch the Ethereal application using the shortcut.	
2.	Choose **Capture** > **Start** from the main menu. The Ethereal: Capture Options window opens.	
3.	There are no special options to choose, so click the **OK** button. The Ethereal: Capture window opens.	

Step	Action	What You See
4.	From the command window, enter **arp –d**. This action ensures that you start with an empty ARP table. The figure shows typical output; the message "The specified entry was not found" indicates that there were no entries in the table to be deleted.	
5.	From the command window, enter **ping** *ip-address*. (where "ip-address" is the address of your pair group partner's PC—refer to the "IP Address and Subnet Mask" table in the Activity Preparation section at the beginning of this lab.). Your output should resemble the figure.	
6.	Check that *all* PCs in the group have completed their ping tests before proceeding.	
7.	Return to the Capture window and click the **Stop** button.	
8.	Using the displayed information, record the source and destination IP addresses in the "Source and Destination IP Addresses Pair" table provided here, one entry for each unique pair. Record the protocols in the following "Protocols" table.	

Source and Destination IP Addresses Pair

Source IP addresses	Destination IP addresses

Protocols

Protocols

Activity Verification

You have completed this task when you attain these results:

- You successfully used the **ping** command to verify connectivity to your partner's PC.
- You successfully used the **arp –d** command to clear the ARP table of entries.
- You successfully used the **Ethereal packet sniffer** application software to capture and display Ethernet frames and decode their contents.
- You successfully completed the tables using the information from the sniffer display.

Task 3: Relate to the OSI Model

You will relate the Ethernet switch-connected network to the OSI model.

Activity Procedure

In the spaces provided, indicate the correct layer for the following:

- Ethernet frame
- IP packet
- ARP packet
- ICMP echo packet
- Ethernet switch
- Ethernet cable

OSI Layer	Item, Entity, or Attribute
1 (Physical)	
2 (Data link)	
3 (Network)	

Activity Verification

You have completed this task when you attain this result:

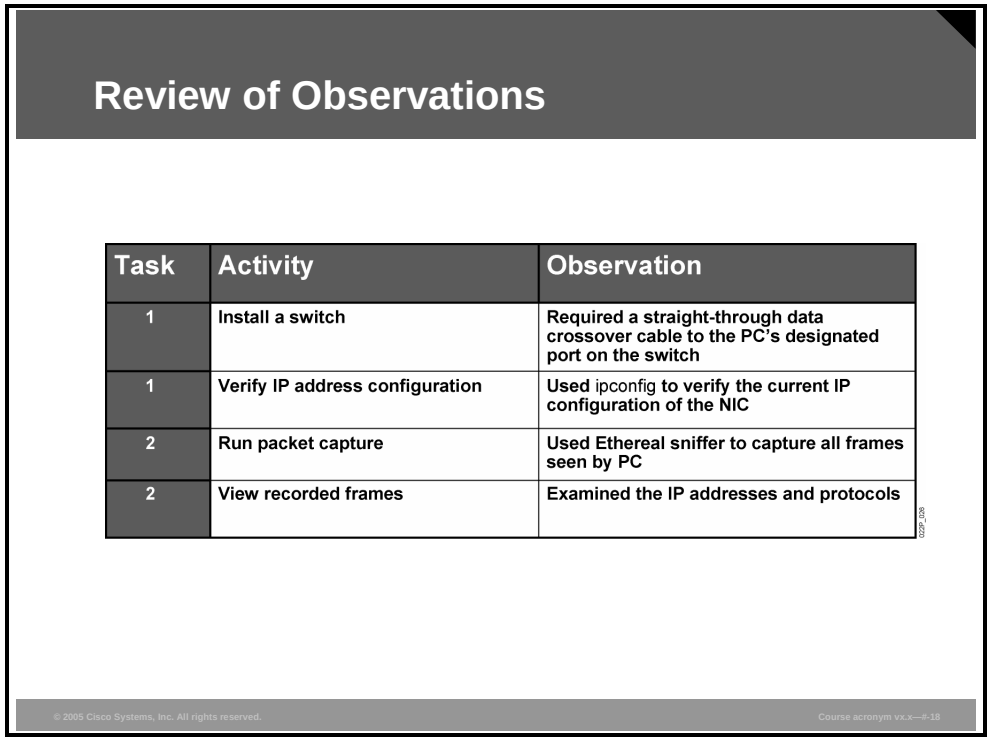
- You successfully completed the OSI information table.

Lab 3-2: Debrief

This debriefing session covers the activities in the "Creating an Ethernet Switch-Connected Network" lab. The topics addressed include a review of the correct steps for adding a switch, a discussion of the OSI model in relation to the components of the switch-connected network, a definition of the network in terms of a set of network characteristics, and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the addition of the switch in the lab.



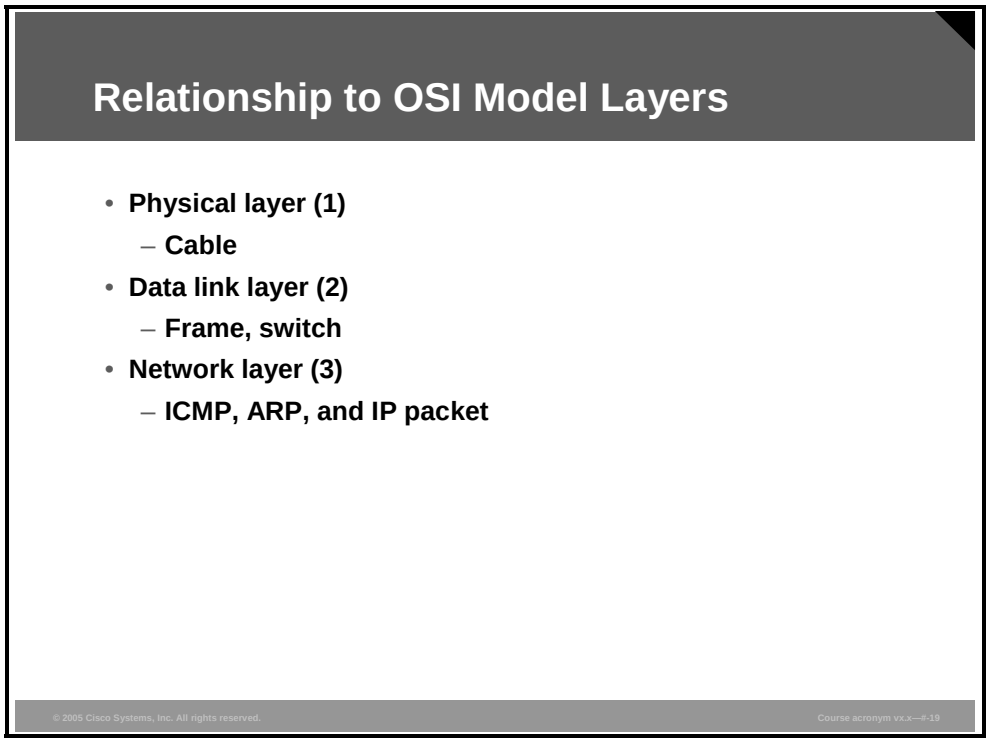
The figure shows the observations that you should have made during the lab activity in which you created an Ethernet switch-connected network, as follows:

- **Task 1:** It was necessary to use a straight-through cable, because the connection was between an end system (PC) and a network device (switch). Attachment should have been to the designated ports; even in a small network, fault restoration is facilitated by following the documentation.
- **Task 1 continues:** The Windows operating system **ipconfig** command was used to ensure that the current IP address matches that required for the lab.
- **Task 2:** The Ethereal packet sniffer was used to record the frames received while the main group did pings between each PC within the pair group.

- **Task 2 continues:** The captured frames showed that the PC saw only a subset of frames—those directed to the PC or broadcast frames. This confirms that a switch does intelligently filter frames.
- **Task 2 continues:** The **arp -a** command was used to display the current contents of the ARP table. Having a saved (cached) binding between the IP address and the MAC address saves unnecessary ARP requests. However, using a binding that is no longer accurate means that the host would *not* be reachable. Therefore, the timing out (aging) of entries is a balance between unnecessary network activity and the probability that the network has changed in some way.
- **Task 2 continues:** Recording the captured frames by completing the "Source and Destination IP Addresses Pair" table should reveal that the hub does *not* filter frames in *any* way. The recording of the protocols would show ARP and ICMP where used. ICMP is used by ping. Within ICMP, you would have observed that there were ICMP echo requests and echo replies.

Relationship to OSI Model Layers

Using the OSI model, you can identify the entities and attributes that were used in this lab.

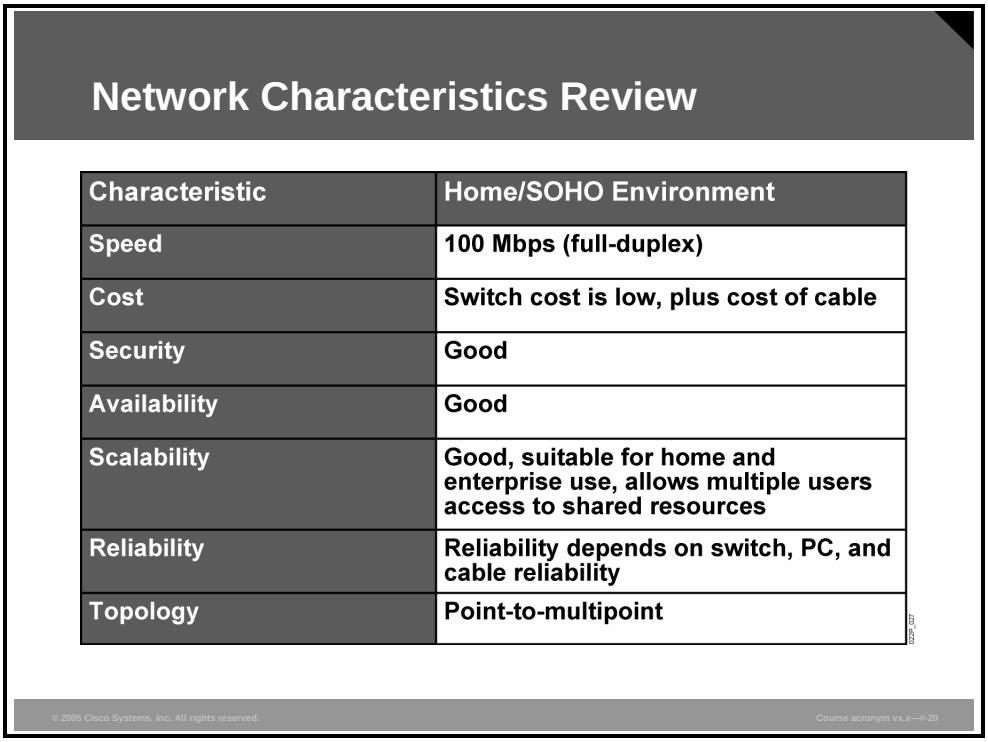


You can observe these layers of the OSI model in relation to the Ethernet network that was constructed:

- **Physical layer (1):** A straight-through data cable was required.
- **Data link layer (2):** The Ethernet frame is a Layer 2 entity, as is the Ethernet switch. The Ethernet switch examines frame addresses and intelligently filters or forwards frames out of specific ports.
- **Network layer (3):** The protocols ICMP and ARP that were observed operated at Layer 3. The packet that was used by the protocols is also a Layer 3 entity.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.

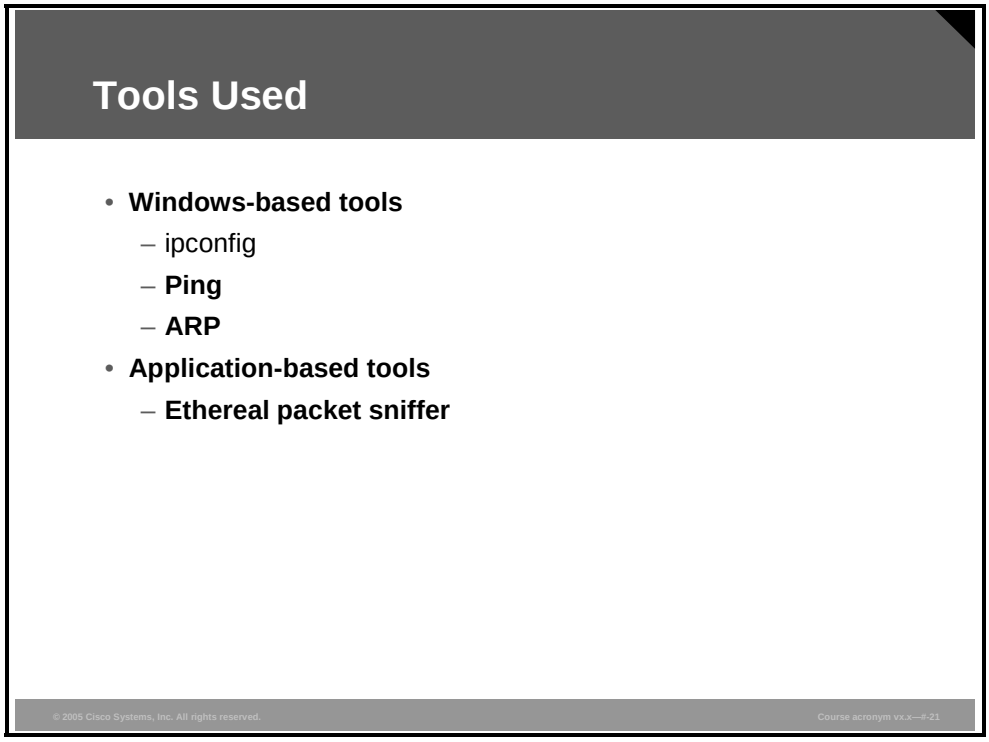


The Ethernet switch-connected network can be described in the following terms:

- **Speed:** The speed is 100 Mbps, and the port will operate at full-duplex mode.
- **Cost:** The cost of this type of network is low even by home user standards. The cost of switches depends on a number of factors. The price of a home or SOHO switch would be considered medium-to-low.
- **Security:** Using a switch on a network reduces the opportunity for a local packet capture program to monitor and save frames that are not destined for that PC. From this aspect, the security of a switching is good.
- **Availability:** The probability that the switched network will be available is high, because the components that constitute the network should have good reliability.
- **Scalability:** This type of network is very scalable. Depending on the sophistication of the switches selected, an enterprise could build a scalable network based on switches as one of its network components.
- **Reliability:** The chance of data being transferred with errors is extremely low, and collisions are eliminated with full-duplex operation.
- **Topology:** The topology is point-to-multipoint.

Tools

In this lab, a number of tools were used.



Lab 4-1: Adding a Default Gateway

Complete the lab activity to practice what you learned in the related module.

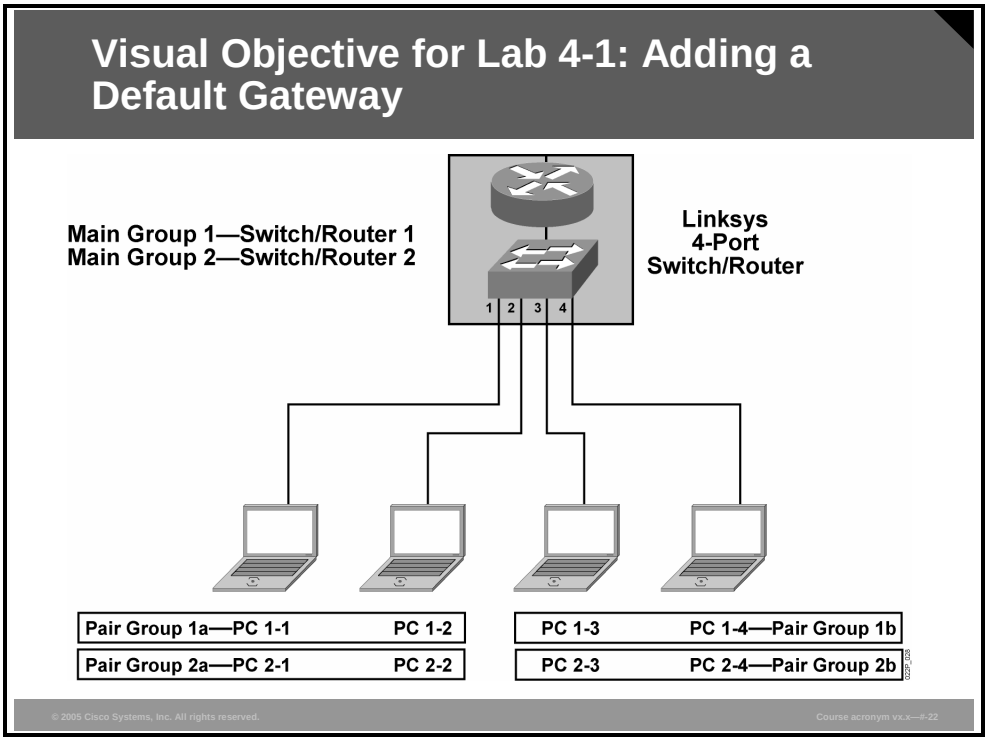
Activity Objective

In this activity, you will observe that the use of the router identified by the default gateway IP address is necessary when connecting to IP addresses that have been determined not to be on the local subnetwork. After completing this activity, you will be able to meet these objectives:

- Test the absence of current IP connectivity to nonlocal hosts
- Add a default gateway IP address
- Retest connectivity
- Use Ethereal packet sniffer software to examine the frames
- Use the OSI model to appropriately place the networking entities and attributes

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Four PCs, one four-port switch/router, supplied Ethernet data cables
- PC running Windows 2000 or XP operating system
- Ethereal packet sniffer application installed on the PCs

Command List

The table describes the commands used in this activity.

Command	Description
ipconfig	Displays current IP configuration of PC Ethernet adapters
ping *ip-address*	Sends IP echo request packets to supplied IP address
arp –d	Removes the current entries in the ARP table

Job Aids

There are no job aids for this lab activity.

Activity Preparation

The instructor will provide the cables that you need to complete this lab activity. You will use the same PC workgroup name that you were assigned in the previous lab.

IP Address and Subnet Mask

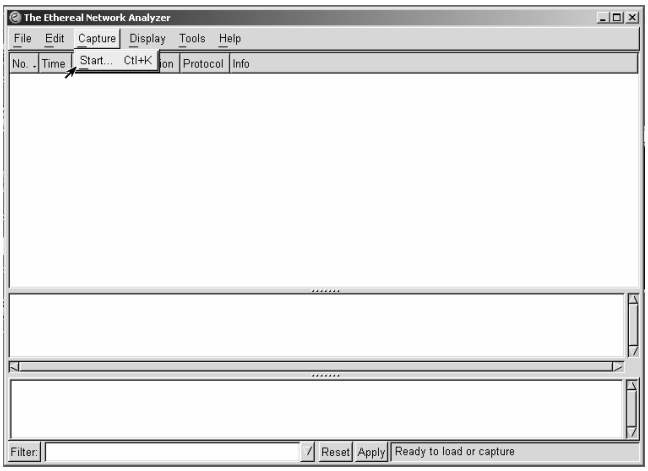
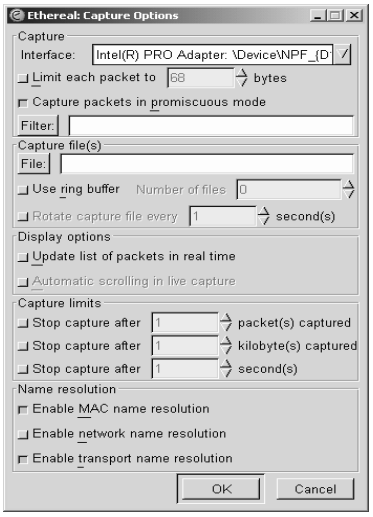
PC Name	Assigned IP Address	Assigned Subnet Mask	Switch Port Number
Main Group 1—Pair Group 1a			
PC 1-1	192.168.1.11	255.255.255.240	Switch 1 port 1
PC 1-2	192.168.1.12	255.255.255.240	Switch 1 port 2
Main Group 1—Pair Group 1b			
PC 1-3	192.168.1.21	255.255.255.240	Switch 1 port 3
PC 1-4	192.168.1.22	255.255.255.240	Switch 1 port 4
Main Group 2—Pair Group 2a			
PC 2-1	192.168.1.11	255.255.255.240	Switch 2 port 1
PC 2-2	192.168.1.12	255.255.255.240	Switch 2 port 2
Main Group 2—Pair Group 2b			
PC 2-3	192.168.1.21	255.255.255.240	Switch 2 port 3
PC 2-4	192.168.1.22	255.255.255.240	Switch 2 port 4

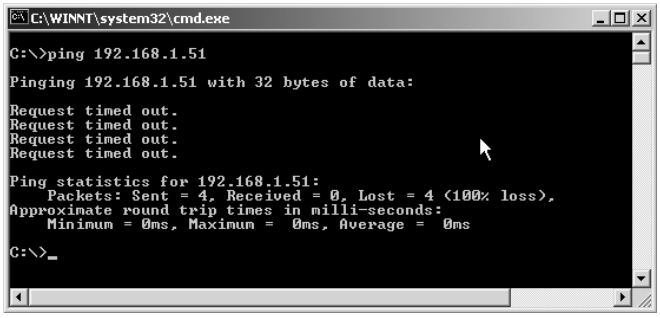
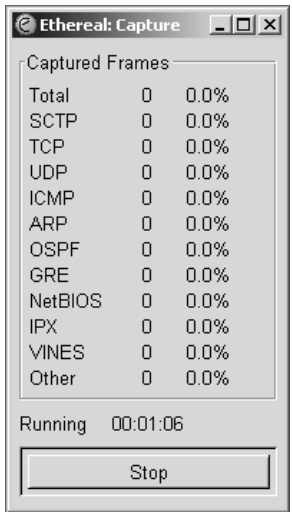
Task 1: Confirm That a Ping to the Other Pair Group PC Is Unsuccessful

In this task, you will confirm that the PCs of the other pair group are not reachable by the use of the **ping** command. By using the Ethereal packet sniffer application, you will observe that no frames were sent by their PCs in response to the **ping** command that is executed.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the desktop, launch the Ethereal application using the shortcut.	
2.	Choose **Capture** > **Start** from the main menu. The Ethereal: Capture Options window opens.	
3.	There are no special options to choose, so click the **OK** button. The Ethereal: Capture window opens.	

Step	Action	What You See
4.	From the command window, enter **arp –d**. This action ensures that the ARP table is empty of entries.	
5.	From the command window, enter **ping** *ip-address* (where "ip-address" is the address of a PC in the other pair group—refer to the "IP Address and Subnet Mask" table in the Activity Preparation section at the beginning of this lab). The output should resemble the figure.	
6.	Return to the Capture window and click the **Stop** button.	
7.	No frames should be recorded. This indicates that the PC determined that the network address was *not* reachable locally, and that, because there was no default gateway router configured, there was no way that the PC could reach the given IP address.	

Activity Verification

You have completed this task when you attain this result:

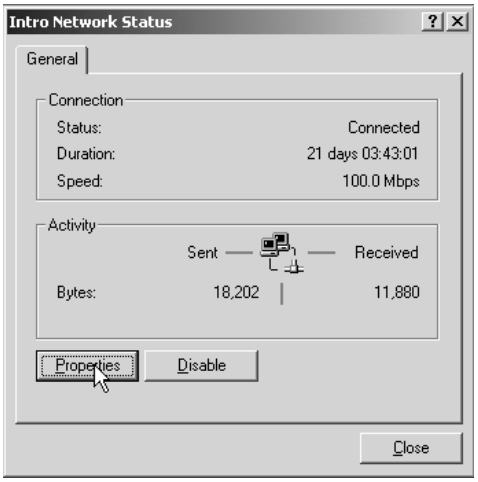
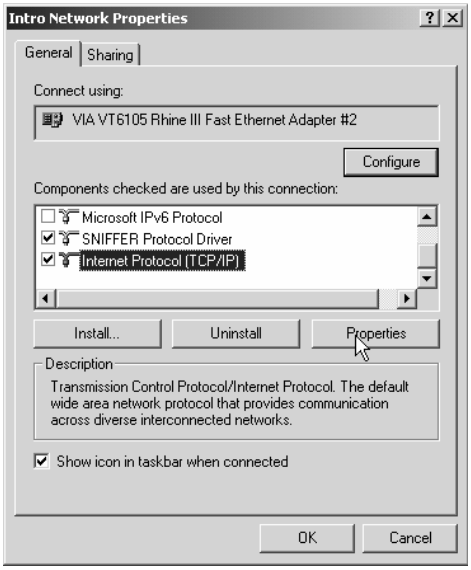
- You unsuccessfully used the **ping** command to reach the other pair group PCs.

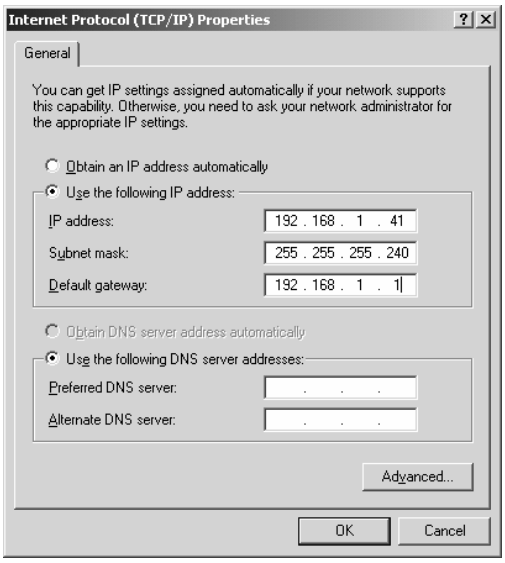
Task 2: Add the PC Default Gateway

You will add a default gateway.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the Windows screen, click the network icon on the task bar at the bottom of the screen to open the status window for your Ethernet LAN adapter.	
2.	From the Status window, click the **Properties** button.	
3.	From the Properties window, scroll down and choose **Internet Protocol (TCP/IP)** and then click the **Properties** button.	

Step	Action	What You See
4.	From the Internet Protocol (TCP/IP) Properties window, go to the default gateway field and enter the address **192.168.1.1**.	
5.	Click the **OK** button. This action will close the Internet Protocol (TCP/IP) Properties window.	
6.	Click the **OK** button. This action will close the Properties window.	
7.	Click the **CLOSE** button. This action will close the Status window.	

Activity Verification

You have completed this task when you attain this result:

- You used the Ethereal packet sniffer application software to capture and display Ethernet frames and observed that no frames were sent in response to the **ping** command.

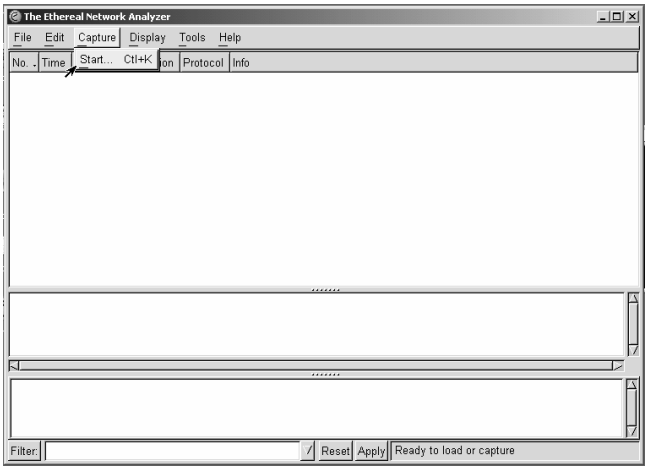
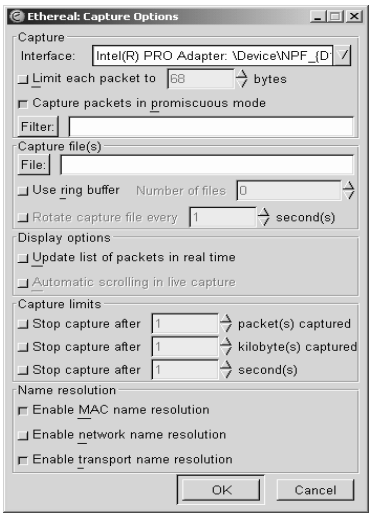
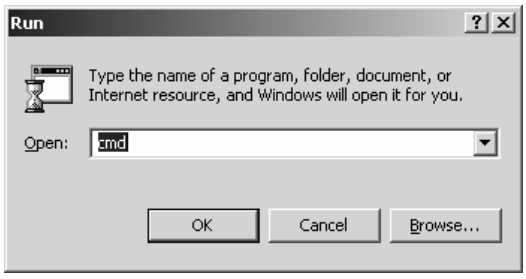
Task 3: Retest Your Connectivity to the Other Pair Group PCs

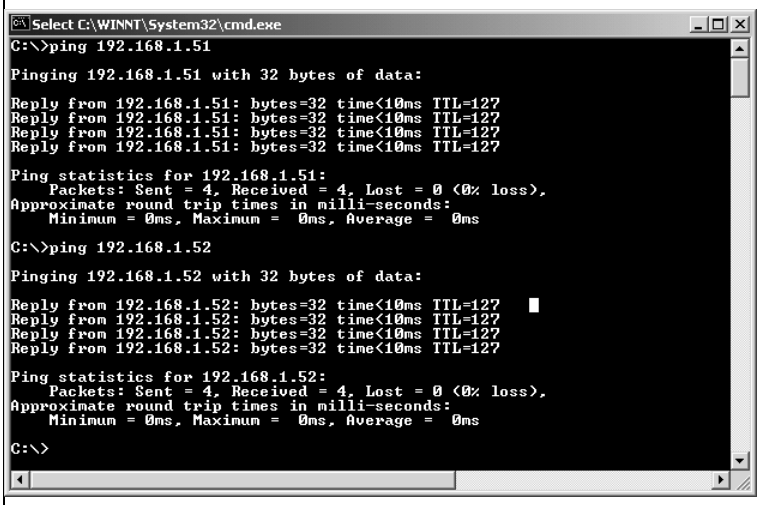
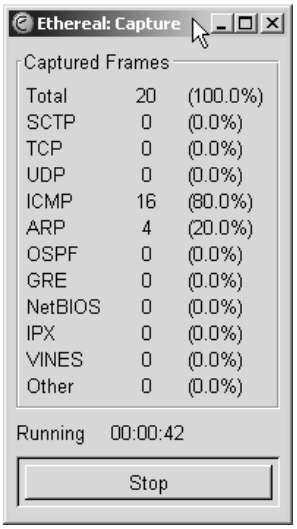
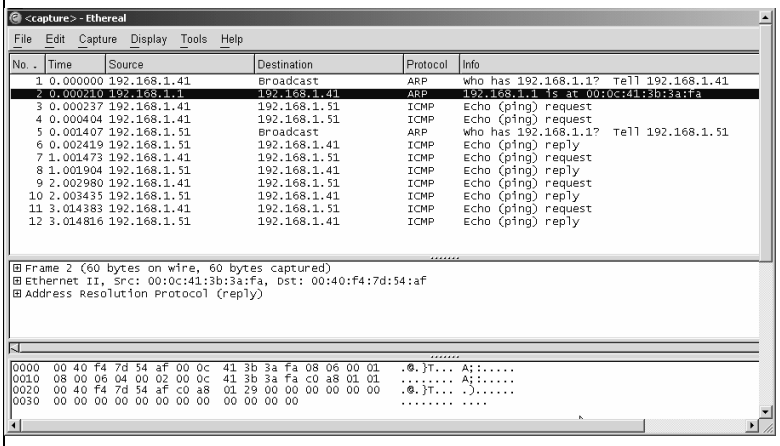
Confirm that your partner pair group has reached this point in the lab before proceeding.

In this task, you will retest the connectivity of your PC. Successful pinging confirms that both PCs have modified their subnet masks correctly to the new value.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Reactivate the Ethereal application or launch it using the shortcut.	
2.	Choose **Capture** > **Start** from the menu. The Ethereal: Capture Options window opens.	
3.	There are no special options to choose, so click the **OK** button. The Ethereal: Capture window opens.	
4.	From Windows: ■ Click **Start.** ■ Choose **Run.** ■ Enter **cmd** in the Open field. ■ Click the **OK** button.	

Step	Action	What You See
5.	From the command window, enter **ping** *ip-address*. (where "ip-address" is the address of a PC in the other pair group). The output should resemble the figure.	
6.	Return to the Ethereal Capture window and click the **Stop** button.	
7.	Your output should resemble the figure.	
8.	Observe from the Capture window that the frames demonstrate that communication between the two pair groups is now possible through the default gateway router at IP address 192.168.1.1.	

Activity Verification

You have completed this task when you attain these results:

- You added a default gateway router address to IP configuration.
- You successfully used the **ping** command to the other pair group PCs.
- You observed the captured frames, which showed packets traversing by means of the default gateway router.

Task 4: Relate to the OSI Model

You will relate the network that you built to the OSI model.

Activity Procedure

In the spaces provided, indicate the correct layer for the following:

- ICMP
- ARP protocol
- Ethernet frame
- IP packet
- IP address
- Router
- Ethernet switch
- Ethernet cable

OSI Layer	Item, Entity, or Attribute
1 (Physical)	
2 (Data link)	
3 (Network)	

Activity Verification

You have completed this task when you attain this result:

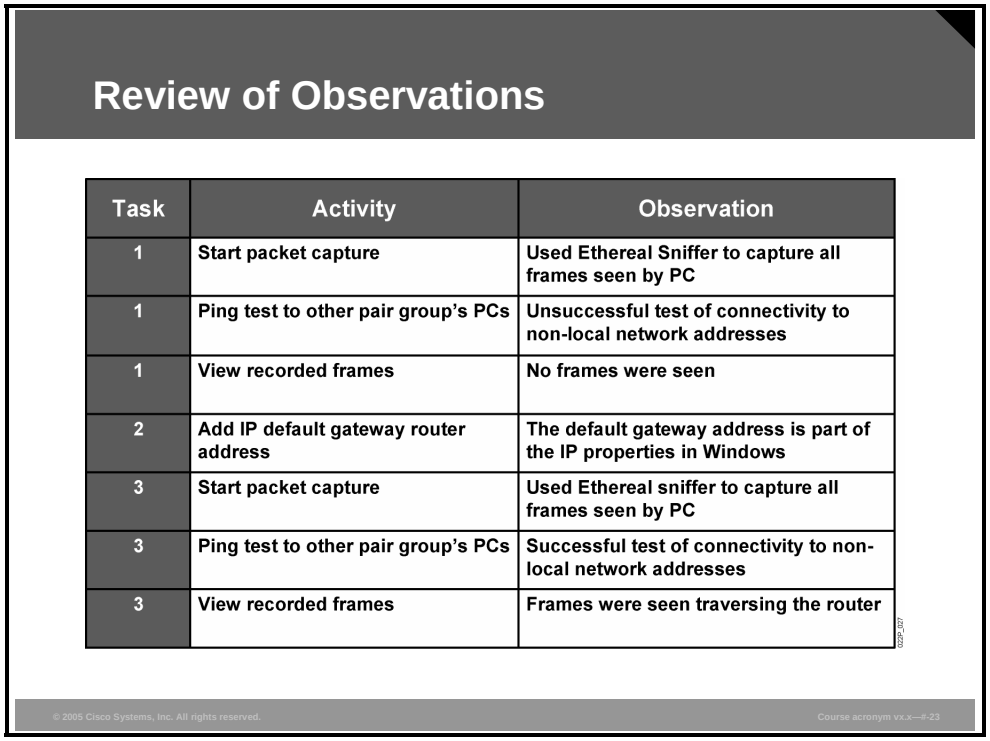
- You successfully completed the OSI information table.

Lab 4-1: Debrief

This debriefing session covers the activities in the "Adding a Default Gateway" lab. The topics addressed include a review of the correct steps for adding a default gateway router address to the IP configuration, a discussion of the OSI model in relation to the components of the Ethernet network, a definition of the Ethernet network in terms of a set of network characteristics, and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the "Adding a Default Gateway" lab.



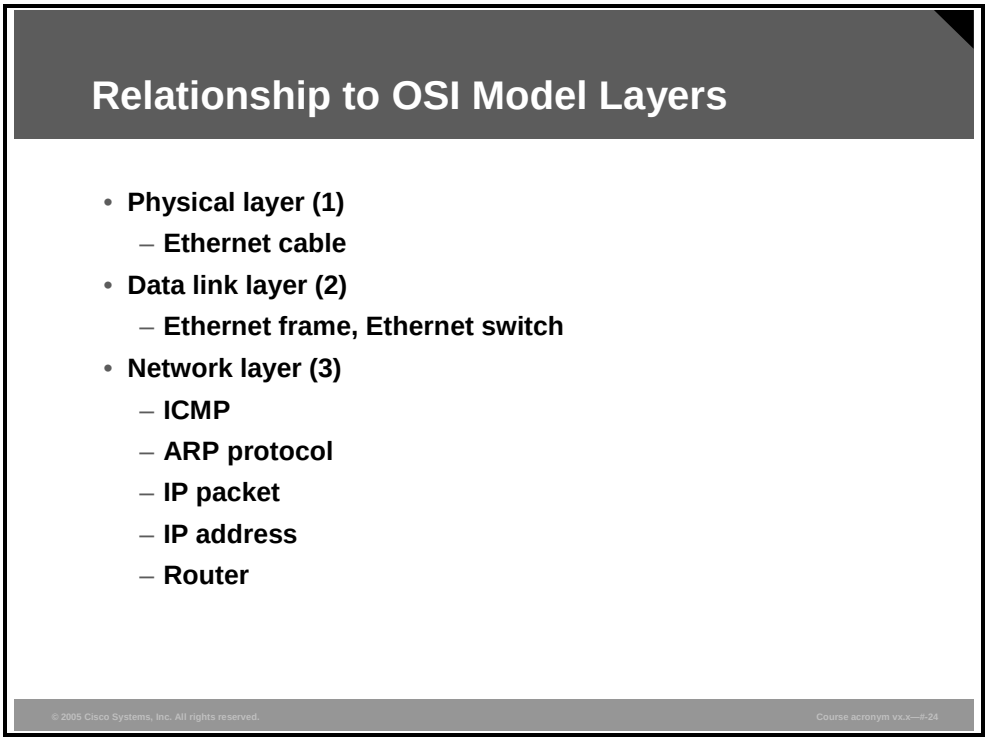
The figure shows the observations you should have made during the lab, as follows:

- **Task 1:** The Ethereal packet capture was started.
- **Task 1 continues:** The ping to the IP addresses of the PCs of the other pair group failed.
- **Task 1 continues :** There were no frames sent, indicating that the PC was using the subnet mask to determine that the address was not on the local network. Because there was no default gateway configured, the PC was unable to forward the packets.
- **Task 2:** The options in the Internet Protocol (TCP/IP) Properties window were used to add the default gateway address of 192.168.1.1.
- **Task 3:** The Ethereal packet capture was restarted.

- **Task 3 continues :** The ping to the IP addresses of the PCs of the other pair group was successful this time.
- **Task 3 continues :** The frames sent to the default gateway IP address indicated that the PC was using the subnet mask to determine that the address was not on the local network. Because there was now a default gateway configured, the PC was able to forward the packets.

Relationship to OSI Model Layers

Using the OSI model, you can identify the entities and attributes that were used in this lab.

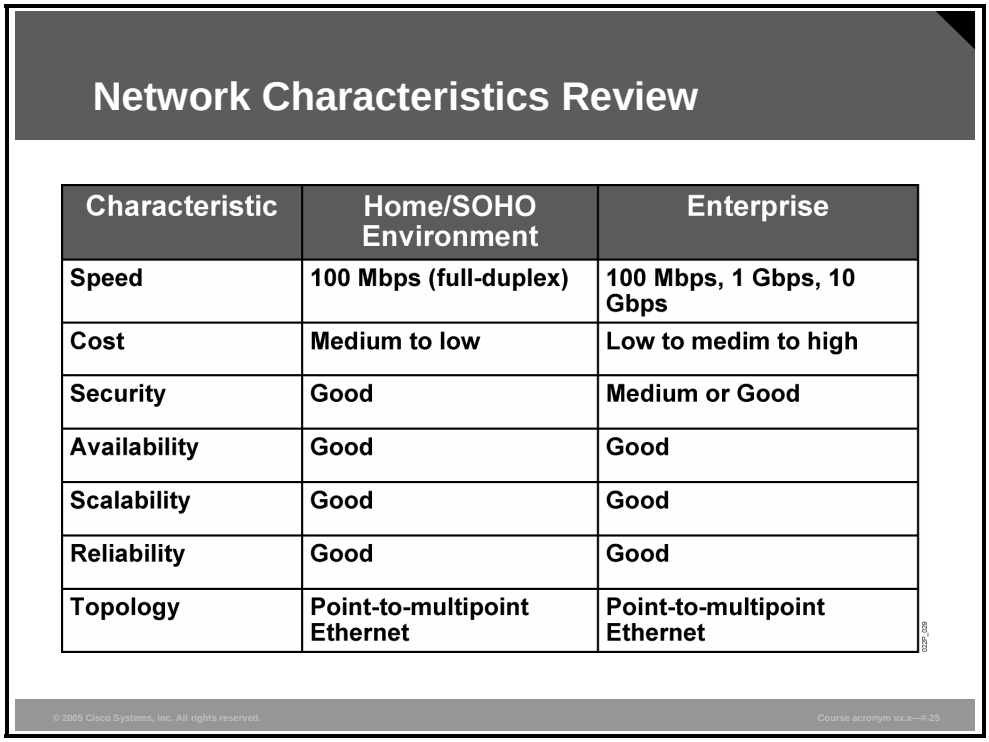


You can observe these layers of the OSI model in relation to the lab:

- **Physical layer (1):** Cabling resides at this layer.
- **Data link layer (2):** The Ethernet frame is a Layer 2 entity, as is the Ethernet switch. The Ethernet switch examines frame addresses and intelligently filters or forwards frames out of specific ports.
- **Network layer (3):** The default gateway router is a Layer 3 entity.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.

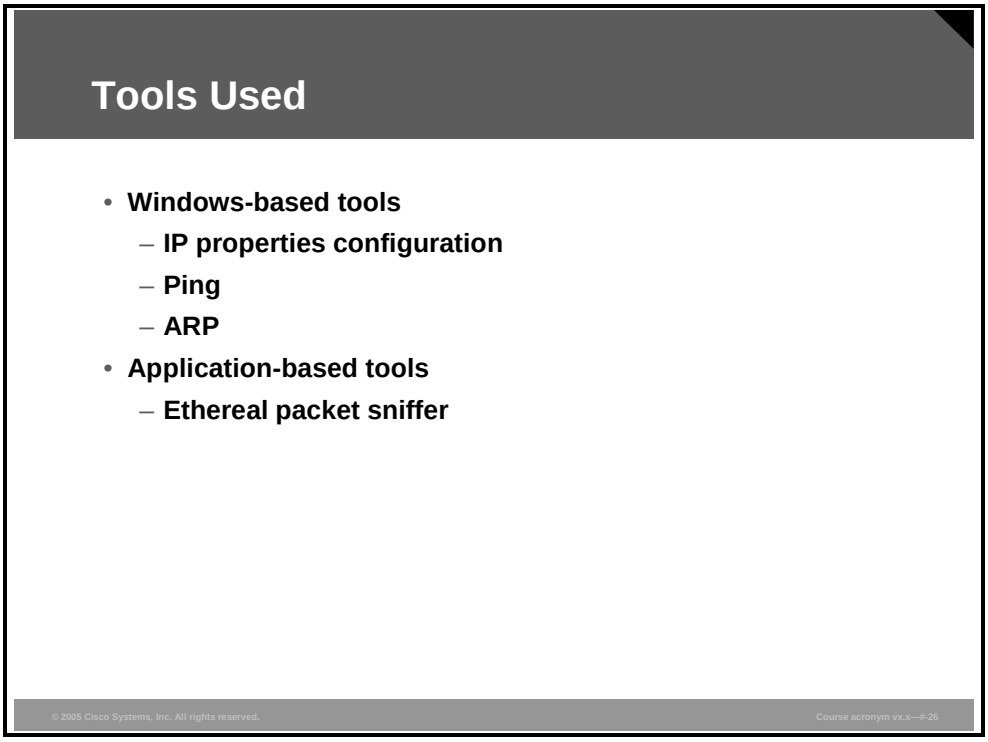


The addition of a default gateway does not change the fundamental Ethernet switch-connected network characteristics. However, there are the following differences in the perception of the characteristics, depending on whether the context is a home or SOHO environment or an Enterprise environment:

- **Speed:** In the home or SOHO environment, the speed is 100 Mbps and the network will operate at full-duplex mode. In the enterprise environment, however, speeds can range from 100 Mbps to 1 Gbps or 10 Gbps.
- **Cost:** In the home or SOHO environment, the cost would be considered medium-to-low, while for the enterprise, the cost would be anywhere between low and high. This is because the cost of enterprise routers varies, depending on performance and functionality.
- **Security:** In a home or SOHO environment, security could be considered good from a switching perspective. In an enterprise environment, security could be considered medium to good—switching does limit the possibility of frame capture by sniffing software, but there are methods that can compromise this relative security.
- **Availability:** The availability is good.
- **Scalability:** The scalability is good.
- **Reliability:** The reliability is good.
- **Topology:** The topology is point-to-multipoint.

Tools

In this lab, a number of tools were used.



Lab 5-1: Converting Decimal to Binary and Binary to Decimal

Complete the lab activity to practice what you learned in the related module.

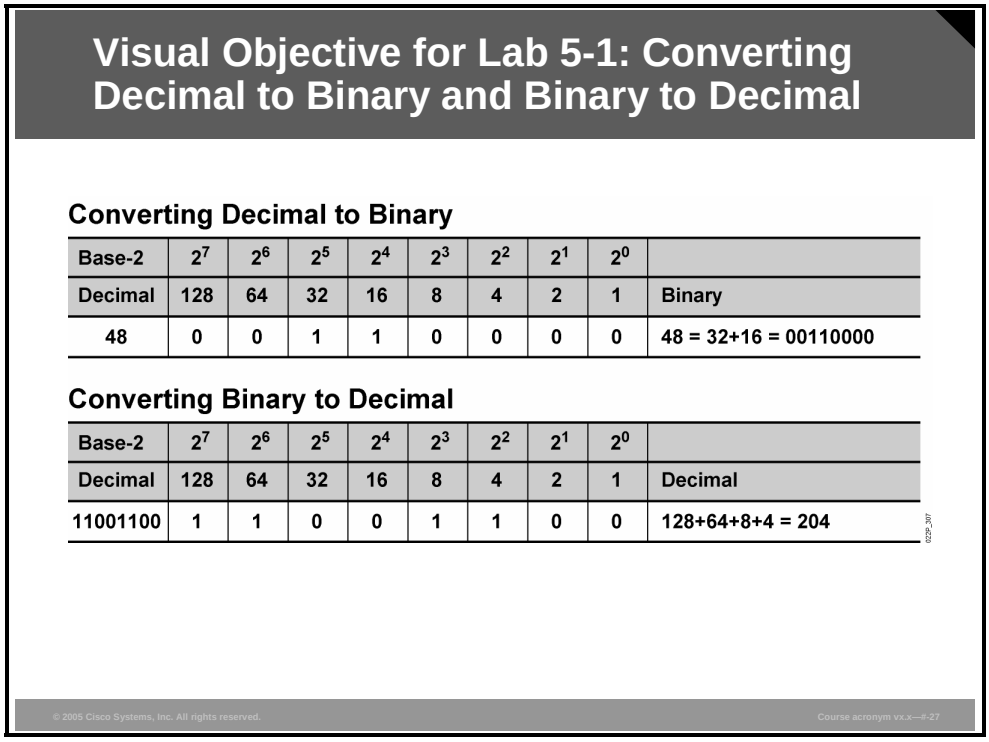
Activity Objective

In this activity, you convert decimal and binary numbers. After completing this activity, you will be able to meet these objectives:

- Convert decimal numbers to binary
- Convert binary numbers to decimal

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

There are no resources for this lab activity.

Command List

There are no commands used in this activity.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

There is no preparation for this lab activity.

Task 1: Convert from Decimal Notation to Binary Format

Complete the following table, which provides practice in converting a number from decimal notation to binary format.

Base-2	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**
48	0	0	1	1	0	0	0	0	48 = 32+16 = 00110000
146	1	0	0	1					
222									
119									
135									
60									

Task 2: Convert from Binary Notation to Decimal Format

Complete the following table, which provides practice in converting a number from binary notation to decimal format.

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11001100	1	1	0	0	1	1	0	0	128+64+8+4 = 204
10101010	1	0	1	0					
11100011									
10110011									
00110101									
10010111									

Activity Verification

You have completed this lab when you attain these results:

- You can accurately convert decimal format numbers to binary notation.
- You can accurately convert binary notation numbers to decimal format.

Lab 5-1: Answer Key

Task 1: Convert from Decimal Nation to Binary Format

Base-2	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**
48	0	0	1	1	0	0	0	0	48 = 32+16 = 00110000
146	1	0	0	1	0	0	1	0	146 = 128+16+2 = 10010010
222	1	1	0	1	1	1	1	0	222 = 128+64+16+8+4+2 = 1101110
119	0	1	1	1	0	1	1	1	119 = 64+32+16+4+2+1 = 01110111
135	1	0	0	0	0	1	1	1	135 = 128+4+2+1 = 10000111
60	0	0	1	1	1	1	0	0	60 = 32+16+8+4 = 00111100

Task 2: Convert from Binary Notation to Decimal Format

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11001100	1	1	0	0	1	1	0	0	128+64+8+4 = 204
10101010	1	0	1	0	1	0	1	0	128+32+8+2 = 170
11100011	1	1	1	0	0	0	1	1	128+64+32+2+1 = 227
10110011	1	0	1	1	0	0	1	1	128+32+16+2+1 = 179
00110101	0	0	1	1	0	1	0	1	32+16+4+1 = 53
10010111	1	0	0	1	0	1	1	1	128+16+4+2+1 = 151

Lab 5-2: Classifying Network Addressing

Complete the lab activity to practice what you learned in the related module.

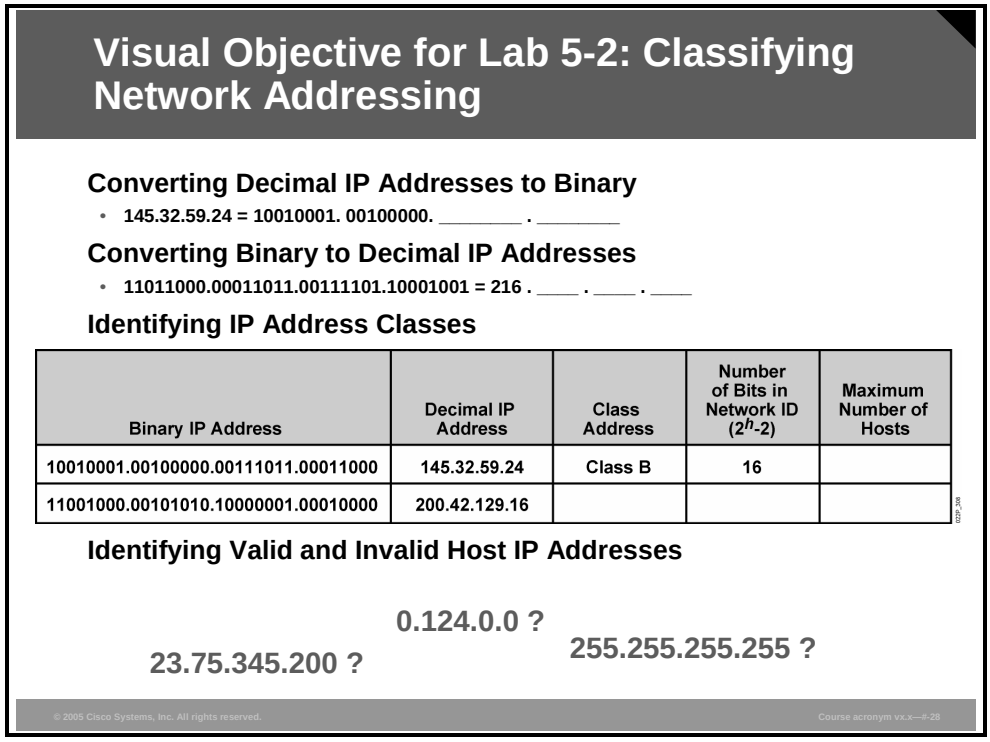
Activity Objective

In this activity, you classify network addresses with IPv4 and IPv6. After completing this activity, you will be able to meet these objectives:

- Convert decimal IP addresses to binary numbers
- Convert binary numbers to IP addresses
- Identify classes of IP addresses
- Identify valid and invalid host IP addresses

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

There are no resources for this lab activity.

Command List

There are no commands used in this activity.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

There is no preparation for this lab activity.

Task 1: Convert from Decimal IP Address to Binary Format

Complete the following steps:

Step 1 Complete the following table to express 145.32.59.24 in binary format.

Base-2	**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**
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59									
24									

Binary Format IP Address	10010001. 00100000. _____ . _____

Step 2 Complete the following table to express 200.42.129.16 in binary format.

Base-2	**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**
200									
42									
129									
16									

Binary Format IP Address	

Step 3 Complete the following table to express 14.82.19.54 in binary format.

Base-2	**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**
14									
82									
19									
54									

Binary Format IP Address	

Task 2: Convert from Binary Format to Decimal IP Address

Complete the following steps:

Step 1 Complete the following table to express 11011000.00011011.00111101.10001001 in decimal IP address format.

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11011000	1	1	0	1	1	0	0	0	216
00011011									
00111101									
10001001									

Decimal Format IP Address	216. _____ . _____ . _____

Step 2 Complete the following table to express 11000110.00110101.10010011.00101101 in decimal IP address format.

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11000110									
00110101									
10010011									
00101101									

Decimal Format IP Address	

Step 3 Complete the following table to express 01111011.00101101.01000011.01011001 in decimal IP address format.

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
01111011									
00101101									
01000011									
01011001									

Decimal Format IP Address	

Task 3: Identify IP Address Classes

Complete the following table to identify the address class, number of bits in the network ID, and maximum number of hosts.

Binary IP Address	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts (2^h-2)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	
11001000.00101010.10000001.00010000	200.42.129.16			
00001110.01010010.00010011.00110110	14.82.19.54			
11011000.00011011.00111101.10001001	216.27.61.137			
10110011.00101101.01000011.01011001	179.45.67.89			
11000110.00110101.10010011.00101101	198.53.147.45			

Task 4: Identify Valid and Invalid Host IP Addresses

Complete the following table to identify which host IP addresses are valid and which are not valid.

Decimal IP Address	Valid or Invalid	If Invalid, Indicate Reason
23.75.345.200		
216.27.61.134		
102.54.94		
255.255.255.255		
142.179.148.200		
200.42.129.16		
0.124.0.0		

Activity Verification

You have completed this lab when you attain these results:

- You can accurately convert decimal format IP addresses to binary format.
- You can accurately convert binary format IP addresses to decimal format.
- You can identify the address class of a given IP address.
- You can identify valid and invalid IP addresses.

Lab 5-2: Answer Key

Task 1: Convert from Decimal IP Address to Binary Format

Step 1 Table to express 145.32.59.24 in binary format:

Base-2	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**
145	1	0	0	1	0	0	0	1	10010001
32	0	0	1	0	0	0	0	0	00100000
59	0	0	1	1	1	0	1	1	00111011
24	0	0	0	1	1	0	0	0	00011000
Binary Format IP Address									10010001.00100000.00111011.00011000

Step 2 Table to express 200.42.129.16 in binary format:

Base-2	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**
200	1	1	0	0	1	0	0	0	11001000
42	0	0	1	0	1	0	1	0	00101010
129	1	0	0	0	0	0	0	1	10000001
16	0	0	0	1	0	0	0	0	00010000
Binary Format IP Address									11001000.00101010.10000001.00010000

Step 3 Table to express 14.82.19.54 in binary format:

Base-2	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**
14	0	0	0	0	1	1	1	0	00001110
82	0	1	0	1	0	0	1	0	01010010
19	0	0	0	1	0	0	1	1	00010011
54	0	0	1	1	0	1	1	0	00110110
Binary Format IP Address									00001110.01010010.00010011.00110110

Task 2: Convert from Binary Format to Decimal IP Address

Step 1 Table to express 11011000.00011011.00111101.10001001 in decimal IP address format:

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11011000	1	1	0	1	1	0	0	0	216
00011011	0	0	0	1	1	0	1	1	27
00111101	0	0	1	1	1	1	0	1	61
10001001	1	0	0	0	1	0	0	1	137

Decimal Format IP Address	216.27.61.137

Step 2 Table to express 11000110.00110101.10010011.00101101 in decimal IP address format:

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
11000110	1	1	0	0	0	1	1	0	198
00110101	0	0	1	1	0	1	0	1	53
10010011	1	0	0	1	0	0	1	1	147
00101101	0	0	1	0	1	1	0	1	45

Decimal Format IP Address	198.53.147.45

Step 3 Table to express 01111011.00101101.01000011.01011001 in decimal IP address format:

Base-2	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
Binary	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**	**Decimal**
01111011	0	1	1	1	1	0	1	1	123
00101101	0	0	1	0	1	1	0	1	45
01000011	0	1	0	0	0	0	1	1	67
01011001	0	1	0	1	1	0	0	1	89

Decimal Format IP Address	123.45.67.89

Task 3: Identify IP Address Classes

Binary IP Address	Decimal IP Address	Address Class	Number of Bits in Network ID	Maximum Number of Hosts (2^h-2)
10010001.00100000.00111011.00011000	145.32.59.24	Class B	16	2^{16}-2 = 65,534
11001000.00101010.10000001.00010000	200.42.129.16	Class C	24	2^8-2 = 254
00001110.01010010.00010011.00110110	14.82.19.54	Class A	8	2^{24}-2 = 16,777,214
11011000.00011011.00111101.10001001	216.27.61.137	Class C	24	2^8-2 = 254
10110011.00101101.01000011.01011001	179.45.67.89	Class B	16	2^{16}-2 = 65,534
11000110.00110101.10010011.00101101	198.53.147.45	Class C	24	2^8-2 = 254

Task 4: Identify Valid and Invalid Host IP Addresses

Decimal IP Address	Valid or Invalid	If Invalid, Indicate Reason
23.75.345.200	Invalid	"345" exceeds an 8-bit value (max=255)
216.27.61.134	Valid	
102.54.94	Invalid	One octet is missing
255.255.255.255	Invalid	Valid number but is an administrative number that should not be assigned to a host
142.179.148.200	Valid	
200.42.129.16	Valid	
0.124.0.0	Invalid	A Class A address cannot use 0 as the first octet

Lab 5-3: Computing Useable Subnetworks and Hosts

Complete the lab activity to practice what you learned in the related module.

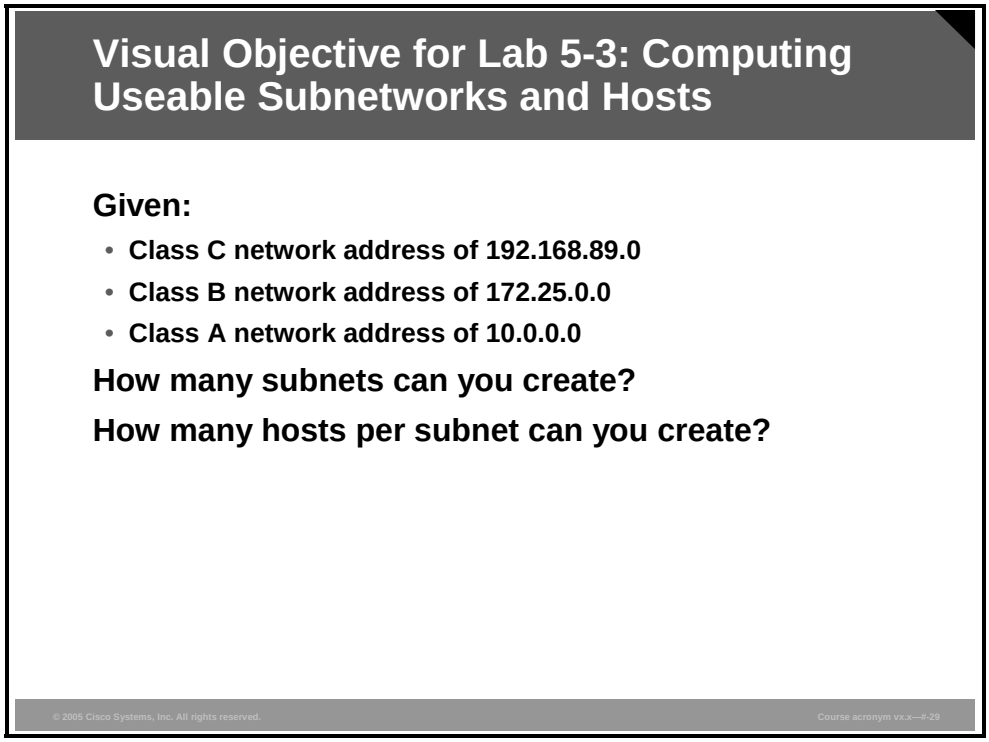
Activity Objective

In this activity, you determine the number of bits to borrow from the host ID to create the required number of subnets for a given IP address. After completing this activity, you will be able to meet these objectives:

- Determine the number of bits required to create different subnets
- Determine the maximum number of hosts addresses available a given subnet

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

There are no resources for this lab activity.

Command List

There are no commands used in this activity.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

There is no preparation for this lab activity.

Task 1: Determine the Number of Bits Required to Subnet a Class C Network

Given a Class C network address of 192.168.89.0, complete the table to identify the number of bits that are required to define the specified number of subnets for the network and then determine the number of hosts per subnet.

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
2		
5		
12		
24		
40		

Task 2: Determine the Number of Bits Required to Subnet a Class B Network

Given a Class B network address of 172.25.0.0, complete the table to identify the number of bits that are required to define the specified number of subnets for the network and then determine the number of hosts per subnet.

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
5		
8		
14		
20		
35		

Task 3: Determine the Number of Bits Required to Subnet a Class A Network

Given a Class A network address of 10.0.0.0, complete the table to identify the number of bits that are required to define the specified number of subnets for the network and then determine the number of hosts per subnet.

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
10		
14		
20		
40		
80		

Activity Verification

You have completed this lab when you attain these results:

- Given a Class A, B, or C network, you can identify the number of bits to borrow to create a given number of subnets.
- Given a Class A, B, or C network, you can determine the number of hosts on the network given a number of subnets and number of bits to borrow.

Lab 5-3: Answer Key

Task 1: Determine the Number of Bits Required to Subnet a Class C Network

Given a Class C network address of 192.168.89.0, the completed table is:

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
2	1	2^7-2 = 126
5	3	2^5-2 = 30
12	4	2^4-2 = 14
24	5	2^3-2 = 6
40	6	2^2-2 = 2

Task 2: Determine the Number of Bits Required to Subnet a Class B Network

Given a Class B network address of 172.25.0.0, the completed table is:

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
5	3	2^7-2 = 8,190
8	3	2^7-2 = 8,190
14	4	2^{12}-2 = 4,094
20	5	2^{11}-2 = 2,046
35	6	2^{10}-2 = 1,022

Task 3: Determine the Number of Bits Required to Subnet a Class A Network

Given a Class A network address of 10.0.0.0, the completed table is:

Number of Subnets	Number of Bits to Borrow (*s*)	Number of Hosts per Subnet (2^h-2)
10	4	2^{20}-2 = 1,048,574
14	4	2^{20}-2 = 1,048,574
20	5	2^{19}-2 = 524,286
40	6	2^{18}-2 = 262,142
80	7	2^{17}-2 = 131,070

Lab 5-4: Calculating Subnet Masks

Complete the lab activity to practice what you learned in the related module.

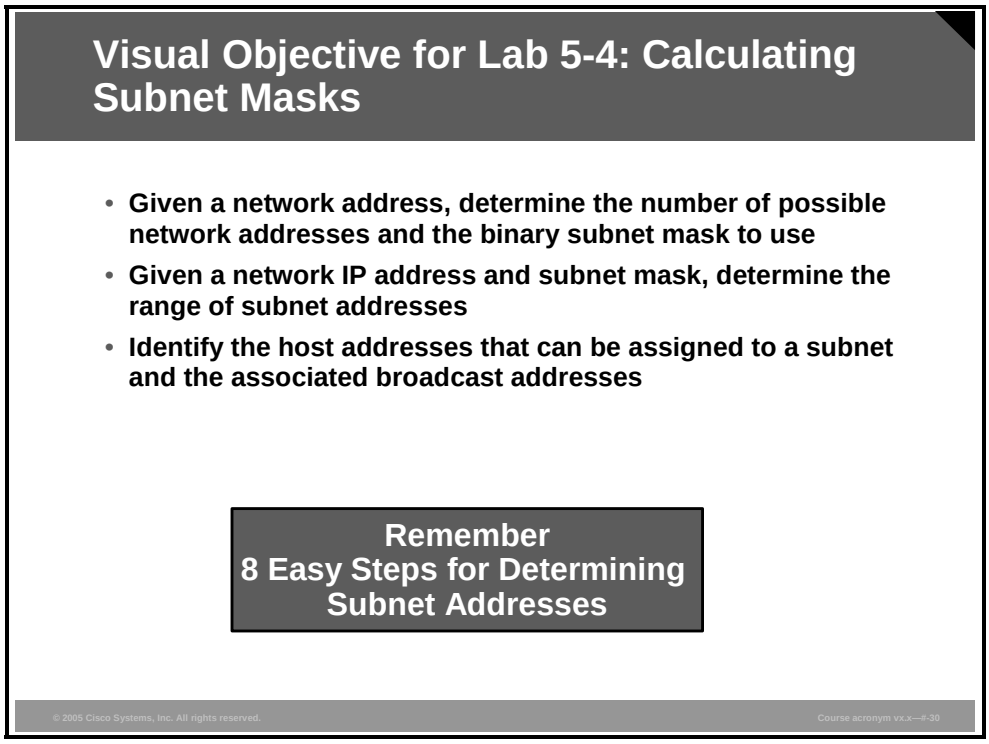
Activity Objective

In this activity, you calculate subnet masks. After completing this activity, you will be able to meet these objectives:

- Given a network address, determine the number of possible network addresses and the binary subnet mask to use
- Given a network IP address and subnet mask, determine the range of subnet addresses
- Identify the host addresses that can be assigned to a subnet and the associated broadcast addresses

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

There are no resources for this lab activity.

Command List

There are no commands used in this activity.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

There is no preparation for this lab activity.

Task 1: Determine the Number of Possible Network Addresses

Given a Class A network and the net bits identified, complete the following table to identify the subnet mask and the number of host addresses possible for each mask.

Classful Address	Decimal Subnet Mask	Binary Subnet Mask	Number of Hosts per Subnet (2^h-2)
/20			
/21			
/22			
/23			
/24			
/25			
/26			
/27			
/28			
/29			
/30			

Task 2: Given a Network Address, Define Subnets

Assume that you have been assigned the 172.25.0.0 /16 network. You need to establish eight subnets. Complete the following questions.

1. How many bits do you need to borrow to define 12 subnets?

   _____

2. Specify the classful address and subnet mask in binary and decimal that allows you to create 12 subnets.

   _____

3. Use the 8-step method to define the 12 subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits four times.	
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
. . .			

Task 3: Given Another Network Address, Define Subnets

Assume that you have been assigned the 192.168.1.0 /24 network.

1. How many bits do you need to borrow to define six subnets?

   _____

2. Specify the classful address and subnet mask in binary and decimal that allows you to create six subnets.

   _____

3. Use the 8-step method to define the six subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits four times.	
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Task 4: Given a Network Address and Classful Address, Define Subnets

Assume that you have been assigned the 192.168.111.129 address in a /28 network block.

1. Specify the subnet mask in binary and decimal.

   _____

2. How many subnets can you define with the specified mask?

   _____

3. How many hosts will be in each subnet?

   _____

4. Use the 8-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	

Step	Description	Example
4.	Copy the significant bits four times.	
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

5. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Task 5: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.25.112.0 address in a /23 network block.

1. Specify the subnet mask in binary and decimal.

   _____

2. How many subnets can you define with the specified mask?

   _____

3. How many hosts will be in each subnet?

   _____

4. Use the 8-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits four times.	
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

5. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Task 6: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.20.0.129 address in a /25 network block.

1. Specify the subnet mask in binary and decimal.

   _____

2. How many subnets can you define with the specified mask?

   _____

3. How many hosts will be in each subnet?

4. Use the 8-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	
2.	Write the mask or classful prefix length in binary.	
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits four times.	
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0			
1			
2			
3			
4			
5			
6			
7			

Activity Verification

You have completed this lab when you attain these results:

- Given a network address, you can determine the number of possible network addresses and the binary subnet mask to use.
- Given a network IP address and subnet mask, you can apply the mask to determine the range of subnet addresses.
- You can apply subnet masks to identify the host addresses that can be assigned to a subnet and the associated broadcast addresses.

Lab 5-4: Answer Key

Task 1: Determine the Number of Possible Network Addresses

Classful Address	Decimal Subnet Mask	Binary Subnet Mask	Number of Hosts per Subnet (2^h-2)
/20	255.255.240.0	11111111.11111111.11110000.00000000	4,094
/21	255.255.248.0	11111111.11111111.11111000.00000000	2,046
/22	255.255.252.0	11111111.11111111.11111100.00000000	1,022
/23	255.255.254.0	11111111.11111111.11111110.00000000	510
/24	255.255.255.0	11111111.11111111.11111111.00000000	254
/25	255.255.255.128	11111111.11111111.11111111.10000000	126
/26	255.255.255.192	11111111.11111111.11111111.11000000	62
/27	255.255.255.224	11111111.11111111.11111111.11100000	30
/28	255.255.255.240	11111111.11111111.11111111.11110000	14
/29	255.255.255.248	11111111.11111111.11111111.11111000	6
/30	255.255.255.252	11111111.11111111.11111111.11111100	2

Task 2: Given a Network Block, Define Subnets

Assume that you have been assigned the 172.25.0.0 /16 network block. You need to establish eight subnets. Complete the following questions.

1. How many bits do you need to borrow to define 12 subnets? 4

2. Specify the classful address and subnet mask in binary and decimal that allows you to create 12 subnets.
   Classful address: /20
   Subnet mask (binary): 11111111.11111111.11110000.00000000
   Subnet mask (decimal): 255.255.240.0

3. Use the 8-step method to define the 12 subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000
2.	Write the mask or classful prefix length in binary.	11110000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	0000 0000 ~~1111~~ ~~0000~~

Step	Description	Example
4.	Copy the significant bits four times.	0000 0000 (first subnet) 0000 0001 (first host address) 0000 1110 (last host address) 0000 1111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	0001 0000 (next subnet)

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.25.0.0	172.25.1.0 to 172.25.14.0	172.25.15.0
1	172.25.16.0	172.25.17.0 to 172.25.30.0	172.25.31.0
2	172.25.32.0	172.25.33.0 to 172.25.46.0	172.25.47.0
3	172.25.48.0	172.25.49.0 to 172.25.62.0	172.25.63.0
4	172.25.64.0	172.25.65.0 to 172.25.78.0	172.25.79.0
5	172.25.80.0	172.25.81.0 to 172.25.92.0	172.25.93.0
6	172.25.94.0	172.25.95 to 172.25.108.0	172.25.109.0
7	172.25.110.0	172.25.111.0 to 172.25.124.0	172.25.125.0

Task 3: Given Another Network Block, Define Subnets

Assume that you have been assigned the 192.168.1.0 /24 network block.

1. How many bits do you need to borrow to define six subnets? 3

2. Specify the classful address and subnet mask in binary and decimal that allows you to create six subnets.
   Classful address: /27
   Subnet mask (binary): 11111111.11111111.11111111.11100000
   Subnet mask (decimal): 255.255.255.224

3. Use the 8-step method to define the six subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000
2.	Write the mask or classful prefix length in binary.	11100000
3.	Draw a line to delineate the significant bits in the	000 00000

Step	Description	Example
	assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	~~111 00000~~
4.	Copy the significant bits four times.	000 00000 (first subnet) 000 00001 (first host address) 000 11110 (last host address) 000 11111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	001 00000 (next subnet)

4. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	192.168.1.0	192.168.1.1 to 192.168.1.30	192.168.1.31
1	192.168.1.32	192.168.1.33 to 192.168.1.62	192.168.1.63
2	192.168.1.64	192.168.1.65 to 192.168.1.94	192.168.1.95
3	192.168.1.96	192.168.1.97 to 192.168.1.126	192.168.1.127
4	192.168.1.128	192.168.1.129 to 192.168.1.158	192.168.1.159
5	192.168.1.160	192.168.1.161 to 192.168.1.190	192.168.1.191

Task 4: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 192.168.111.0 /28 network block.

1. Specify the subnet mask in binary and decimal.
   Subnet mask (binary): 11111111.11111111.11111111.11110000
   Subnet mask (decimal): 255.255.255.224

2. How many subnets can you define with the specified mask? 16

3. How many hosts will be in each subnet? 14

4. Use the 8-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	10000001
2.	Write the mask or classful prefix length in binary.	11110000
3.	Draw a line to delineate the significant bits in the assigned IP address.	1000 0001 ~~1111 0000~~

Step	Description	Example
	Cross out the mask so that you can view the significant bits in the IP address.	
4.	Copy the significant bits four times.	1000 0000 (first subnet) 1000 0001 (first host address) 1000 1110 (last host address) 1000 1111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	1001 0000 (next subnet)

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	192.168.111.0	192.168.111.1 to 192.168.111.126	192.168.111.127
1	192.168.111.128	192.168.111.129 to 192.168.111.142	192.168.111.143
2	192.168.111.144	192.168.111.145 to 192.168.111.158	192.168.111.159
3	192.168.111.160	192.168.111.161 to 192.168.111.174	192.168.111.175
4	192.168.111.176	192.168.111.177 to 192.168.111.190	192.168.111.191
5	192.168.111.192	192.168.111.193 to 192.168.111.206	192.168.111.207
6	192.168.111.208	192.168.111.209 to 192.168.111.222	192.168.111.223

Task 5: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.25.0.0 /23 network block.

1. Specify the subnet mask in binary and decimal.
   Subnet mask (binary): 11111111.11111111.11111110.00000000
   Subnet mask (decimal): 255.255.254.0

2. How many subnets can you define with the specified mask?
   126

3. How many hosts will be in each subnet?
   510

4. Use the 8-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	01110000.00000000
2.	Write the mask or classful prefix length in binary.	11111110.00000000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	0111000 0.00000000 ~~1111111 0.~~00000000
4.	Copy the significant bits four times.	0111000 0.00000000 (first subnet) 0111000 0.00000001 (first host address) 0111000 1.11111110 (last host address) 0111000 1.11111111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	0111001 0.00000000 (next subnet)

5. Complete the following table to define each subnet.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.25.0.0	172.25.0.1 to 172.25.1.254	172.25.1.255
1	172.25.2.0	172.25.2.1 to 172.25.3.254	172.25.3.255
2	172.25.4.0	172.25.4.1 to 172.25.5.254	172.25.5.255
3	172.25.6.0	172.25.6.1 to 172.25.7.254	172.25.7.255
4	172.25.8.0	172.25.8.1 to 172.25.9.254	172.25.9.255
. . .			

Task 6: Given a Network Block and Classful Address, Define Subnets

Assume that you have been assigned the 172.20.0.0 /25 network block.

1. Specify the subnet mask in binary and decimal.
   Subnet mask (binary): 11111111.11111111.11111111.10000000
   Subnet mask (decimal): 255.255.255.128

2. How many subnets can you define with the specified mask?
   510

3. How many hosts will be in each subnet?
   126

4. Use the 8-step method to define the subnets.

Step	Description	Example
1.	Write down the octet that is being split in binary.	00000000.10000001
2.	Write the mask or classful prefix length in binary.	11111111.10000000
3.	Draw a line to delineate the significant bits in the assigned IP address. Cross out the mask so that you can view the significant bits in the IP address.	1 0000001 ~~1 0000000~~
4.	Copy the significant bits four times.	00000000.10000000 (first subnet) 00000000.10000001 (first host address) 00000000.11111110 (last host address) 00000000.11111111 (broadcast address)
5.	In the first line, define the network address by placing zeros in the remaining host bits.	
6.	In the last line, define the directed-broadcast address by placing all ones in the host bits.	
7.	In the middle lines, define the first and last host ID for this subnet.	
8.	Increment the subnet bits by one to determine the next subnet address. Repeat Steps 4 through 8 for all subnets.	00000001.10000000 (next subnet)

5. Complete the following table to define the subnets.

Subnet Number	Subnet Address	Range of Host Addresses	Directed-Broadcast Address
0	172.20.0.0	172.20.0.1 to 172.20.0.126	172.20.0.127
1	172.20.0.128	172.20.0.129 to 172.20.0.254	172.20.0.255
2	172.20.1.0	172.20.1.1 to 172.20.1.126	172.20.1.127
3	172.20.1.128	172.20.1.129 to 172.20.1.254	172.20.1.255
4	172.20.2.0	172.20.2.1 to 172.20.2.126	172.20.2.127
5	172.20.2.128	172.20.2.129 to 172.20.2.254	172.20.2.255
. . .			

Lab 5-5: Modifying the IP Subnet Mask

Complete the lab activity to practice what you learned in the related module.

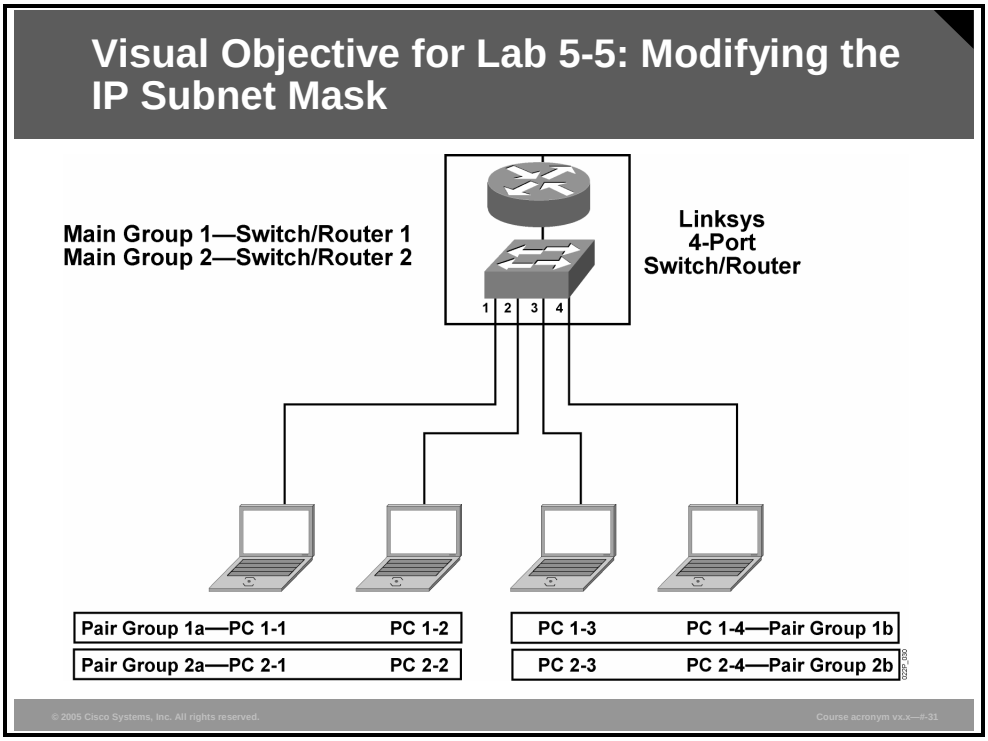
Activity Objective

In this activity, you modify a subnet mask. After completing this activity, you will be able to meet these objectives:

- Use Windows commands as tools to confirm the IP configuration
- Confirm current IP connectivity
- Change the value of the subnet mask
- Retest connectivity
- Use Ethereal packet sniffer software to examine the frames
- Use the OSI model to appropriately place the networking entities and attributes

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Four PCs, one four-port hub, supplied Ethernet data cables
- PC running Windows 2000 or XP operating system
- Ethereal packet sniffer application software installed on the PCs

Note	Some companies do not permit packet sniffer software to be installed on their networks. Be sure that you are in compliance with the regulations of your company before performing this lab.

Command List

The table describes the commands used in this activity.

Command	Description
ipconfig	Displays current IP configuration of PC Ethernet adapters
ping *ip-address*	Sends IP echo request packets to supplied IP address
arp -d	Removes the current entries in the ARP table

Job Aids

There are no job aids for this lab activity.

Activity Preparation

It is assumed that the network configuration and topology are identical to those at the end of Lab 4-1.

IP Address and Subnet Mask

PC Name	Assigned IP Address	Assigned Subnet Mask	Switch Port Number
Pair Group 1a			
PC 1-1	192.168.1.11	255.255.255.240	Switch 1 port 1
PC 1-2	192.168.1.12	255.255.255.240	Switch 1 port 2
Pair Group 1b			
PC 1-3	192.168.1.21	255.255.255.240	Switch 1 port 3
PC 1-4	192.168.1.22	255.255.255.240	Switch 1 port 4
Pair Group 2a			
PC 2-1	192.168.1.11	255.255.255.240	Switch 2 port 1
PC 2-2	192.168.1.12	255.255.255.240	Switch 2 port 2
Pair Group 2b			
PC 2-3	192.168.1.21	255.255.255.240	Switch 2 port 3
PC 2-4	192.168.1.22	255.255.255.240	Switch 2 port 4

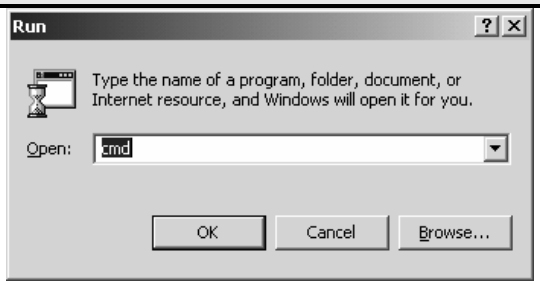
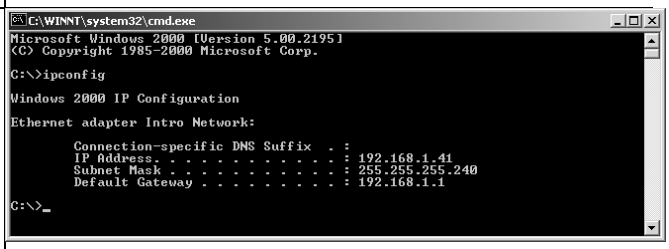
Note All PCs use an IP default gateway address of 192.168.1.1.

Task 1: Verify the IP Address Configuration

Using the “IP Address and Subnet Mask” table in the Activity Preparation section at the beginning of this lab, you will first confirm that the configured IP address is correctly assigned.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From Windows: ■ Click **Start**. ■ Choose **Run**. ■ Enter **cmd** in the Open field. ■ Click the **OK** button.	
2.	From the command window, enter **ipconfig**. The displayed output should match the assigned information in the ”IP Address and Subnet Mask” table in the Activity Preparation section.	

Activity Verification

You have completed this task when you attain this result:

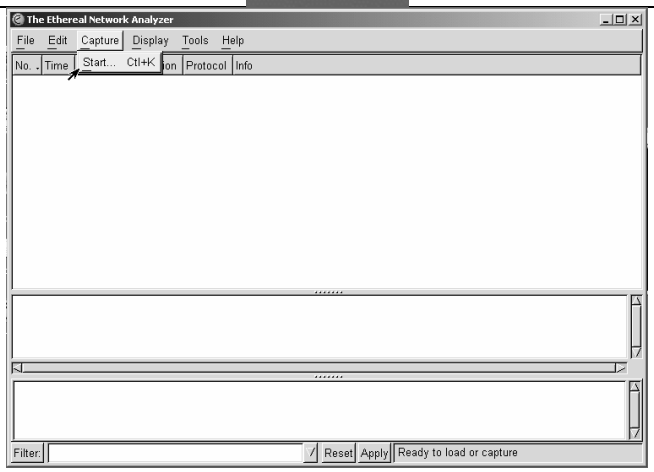
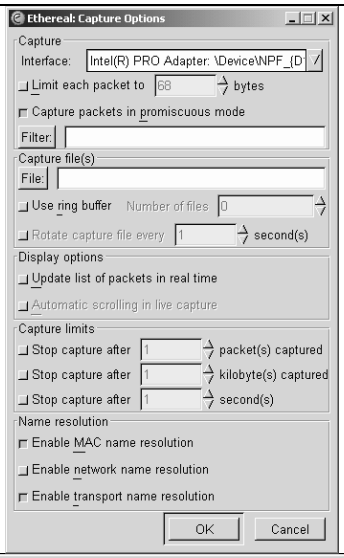
- You correctly used the **ipconfig** command to verify the IP configuration of the PC.

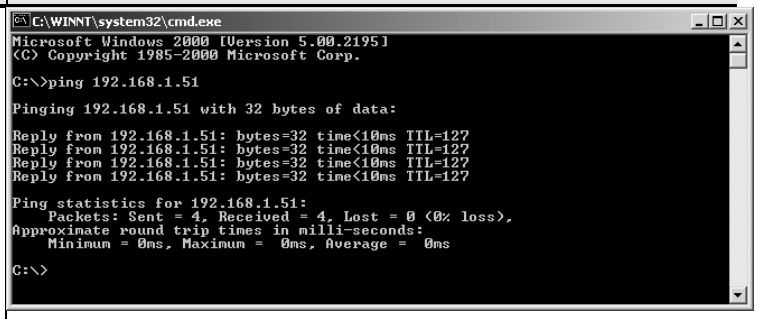
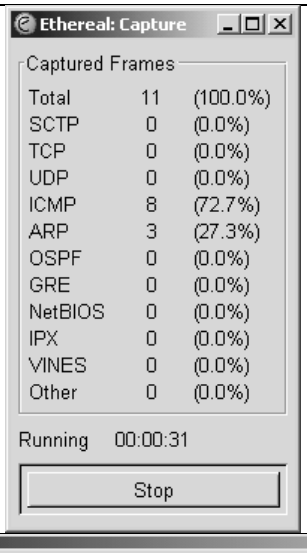
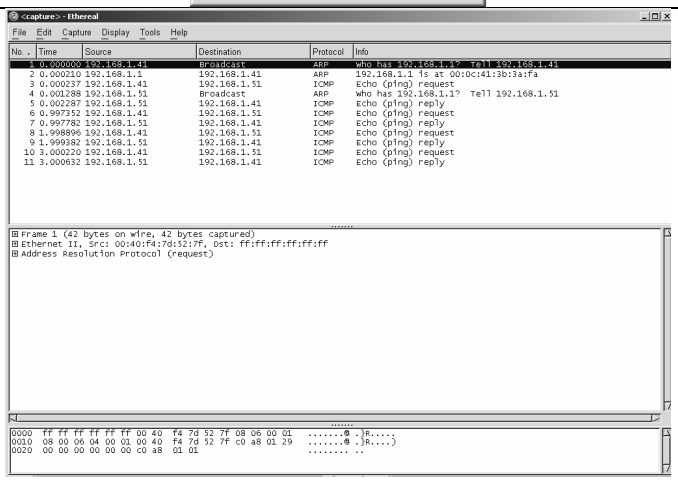
Task 2: Confirm That a Ping to the Other Pair Group Is Successful

In this task, you will test your connection by using the **ping** command. Confirm that the other pair group has reached this point in the lab before proceeding.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the desktop, launch the Ethereal application using the shortcut.	
2.	Choose **Capture** > **Start** from the main menu. The Ethereal Capture Options window opens.	
3.	There are no special options to choose, so click the **OK** button. The Ethereal Capture window opens.	
4.	From the command window, enter **arp –d**. This action ensures that the ARP table is empty of entries.	

Step	Action	What You See
5.	From the command window, enter **ping** *ip-address* (where "ip-address" is the address of the PCs in the other pair group). Record the TTL (Time to Live) value:_____ You should recall that the TTL is decreased by one each time a packet passes through a router. Your output should resemble the figure.	
6.	Return to the Capture window and click the **Stop** button.	
7.	The captured frames should show that the packets went through the default gateway router as 192.168.1.1. This result indicates that the PC determined that the network address was *not* reachable locally.	

Activity Verification

You have completed this task when you attain these results:

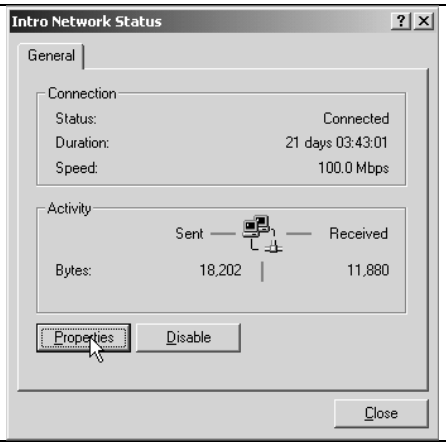
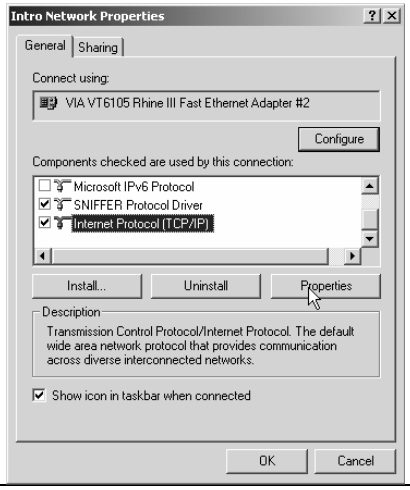
- You used the **ping** command to verify successful connectivity through the default gateway router to the other pair group PCs.
- You used the Ethereal packet sniffer application software to capture and display Ethernet frames and observed their behavior.

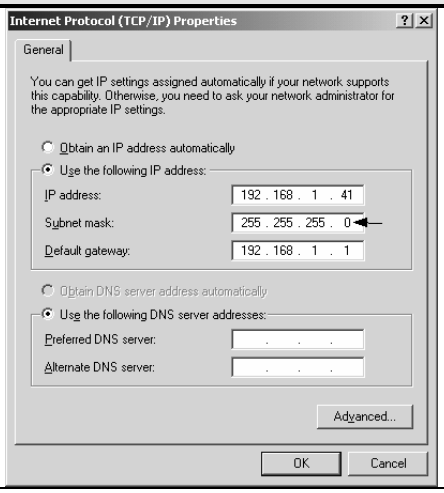
Task 3: Change the IP Subnet Mask of the PC

You will change the subnet mask on your PC.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the Windows screen, click the network icon on the task bar at the bottom of the screen to open the status window for your Ethernet LAN adapter.	
2.	From your Ethernet LAN adapter Status window, click the **Properties** button.	
3.	From your Ethernet LAN adapter Properties window, scroll down and choose **Internet Protocol (TCP/IP)**. Then click the **Properties** button.	

Step	Action	What You See
4.	From the Internet Protocol (TCP/IP) Properties window, locate the Subnet mask field and change the mask to **255.255.255.0**.	
5.	Click the **OK** button. This will close the Internet Protocol (TCP/IP) Properties window.	
6.	Click the **OK** button. This will close your Ethernet LAN adapter Properties window.	
7.	Click the **CLOSE** button. This action will close your Ethernet LAN adapter Status window.	

Activity Verification

You have completed this task when you attain this result:

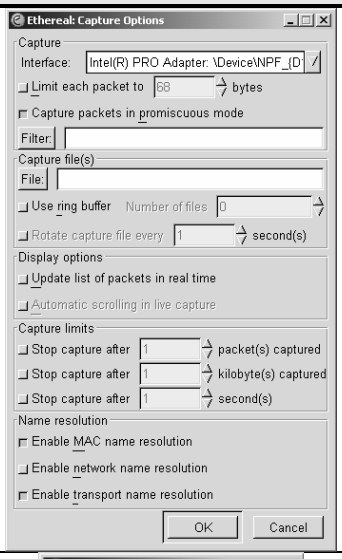
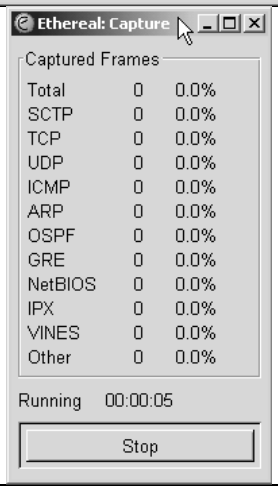
- You changed the IP subnet mask to the new given value of 255.255.255.0.

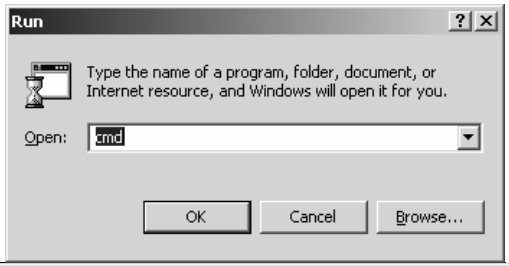
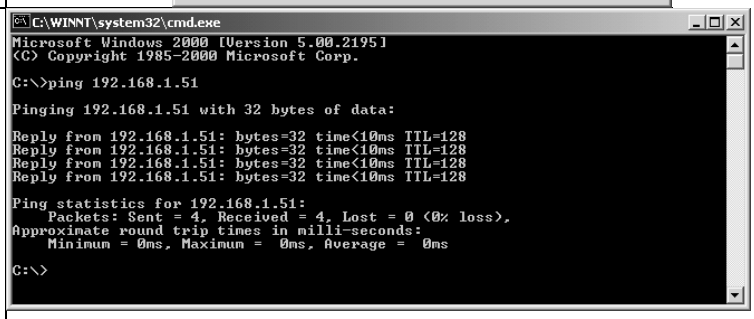
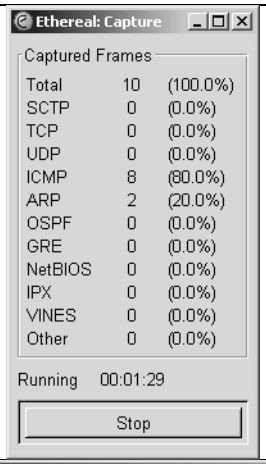
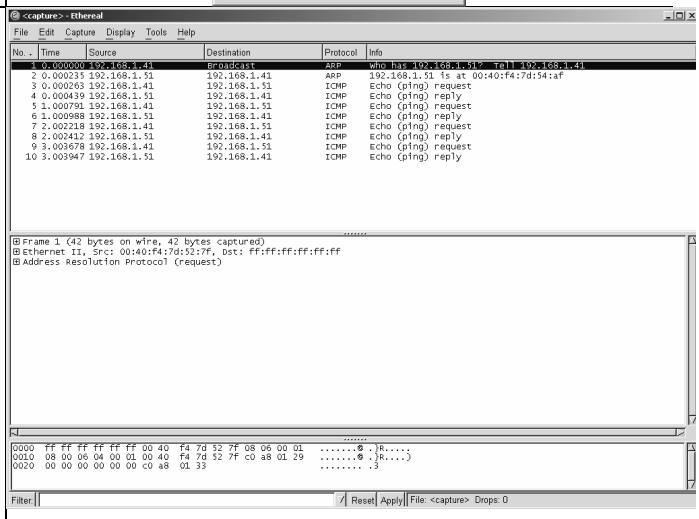
Task 4: Retest Connectivity to the Other Pair Group PCs

In this task, you will retest your connectivity. (Confirm that the other pair group has reached this point in the lab before proceeding.) Successful pinging with a TTL of 128 confirms that both PCs have modified their subnet masks correctly to the new value.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Choose **Capture** > **Start** from the menu. The Ethereal: Capture Options window opens.	
2.	There are no special options to choose, so click the **OK** button. The Ethereal Capture window opens.	

Step	Action	What You See
3.	From Windows: ■ Click **Start**. ■ Choose **Run**. ■ Enter **cmd** in the Open field. ■ Click the **OK** button.	
4.	From the command window, enter **ping** *ip-address* (where "ip-address" is the address of a PC in the other pair group). Compare the TTL value with that recorded in Step 5 of Task 1. The output should resemble the figure.	
5.	Return to the Capture window and click the **Stop** button.	
6.	Your output should resemble the figure.	

Step	Action	What You See
7.	Observe from the capture window the frame behavior that demonstrates that direct communication between the two pair groups is now possible. This result is confirmed by the TTL value from the ping increasing by 1 to 128, and by the observation that your PC is using ARP to find the MAC address of the destination PC and *not* the MAC address of the default gateway router.	

Activity Verification

You have completed this task when you attain this result:

- You used the **ping** command to verify successful direct connectivity to other pair group PCs without using the default gateway router.

Task 5: Relate to the OSI Model

You will relate the subnet mask change to the OSI model.

Activity Procedure

In the spaces provided, indicate the correct layer for the following:

- ICMP
- ARP protocol
- Ethernet frame
- IP packet
- IP address
- TTL field
- Ethernet switch
- Ethernet cable

OSI Layer	Item, Entity, or Attribute
1 (Physical)	
2 (Data link)	
3 (Network)	

Activity Verification

You have completed this task when you attain this result:

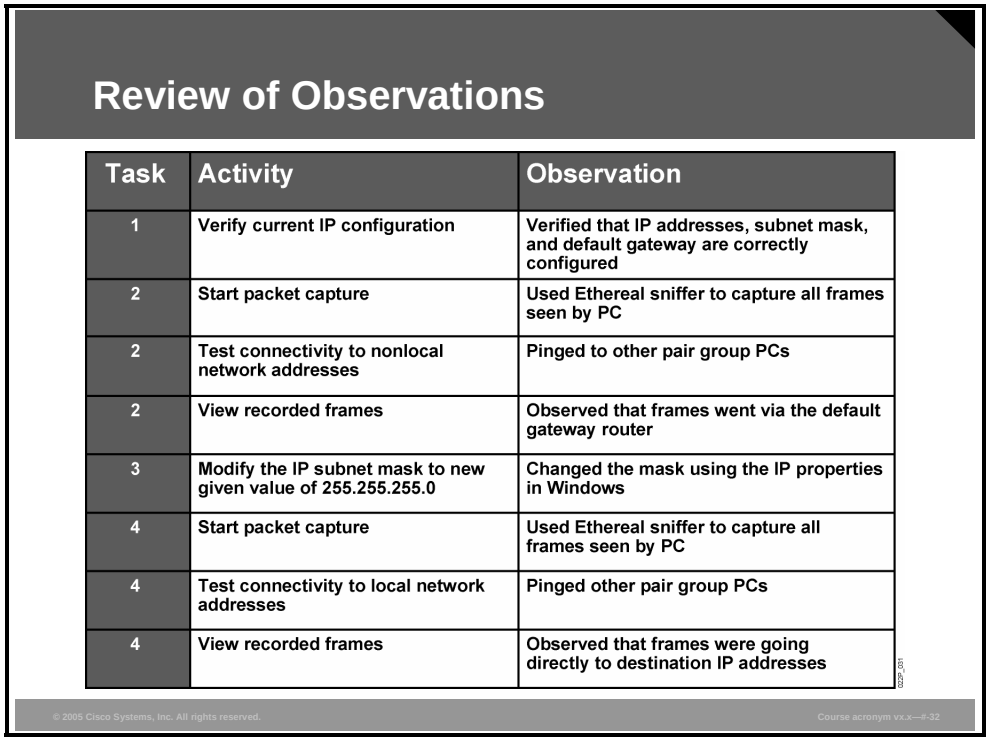
- You successfully completed the OSI information table.

Lab 5-5: Debrief

This debriefing session covers the activities in the “Modifying the IP Subnet Mask” lab. The topics addressed include a review of the correct steps for modifying the IP subnet mask, a discussion of the OSI model in relation to the components of the Ethernet network, a definition of the Ethernet network in terms of a set of network characteristics, and a review of tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the “Modifying the IP Subnet Mask” lab.



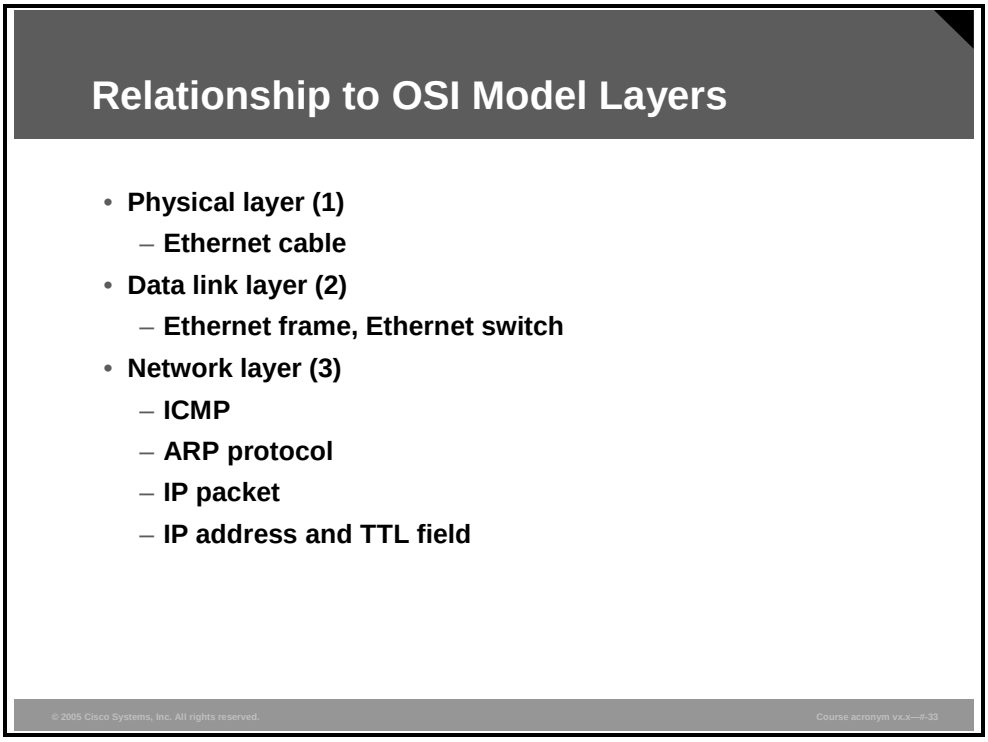
The figure shows the observations that you should have made during the lab, as follows:

- **Task 1:** The Windows operating system **ipconfig** command was used to verify that the current IP address, subnet mask, and IP default gateway information matches that required for the lab.
- **Task 2:** The Ethereal packet sniffer was used to capture all frames that were seen by the PC NIC card.
- **Task 2 continues:** The **ping** command was used to generate packets to the other pair group PCs.
- **Task 2 continues:** Observation of the captured frames showed that they were sent through the configured IP default gateway, indicating that the PC somehow treated the ping requests for these destinations differently from the ping requests for your own pair-group addresses, which were treated as directly reachable.

- **Task 3:** The Internet Protocol (TCP/IP) Properties window was used to modify the subnet mask to the new given value of 255.255.255.0.
- **Task 4:** The Ethereal packet sniffer was used to capture all frames that were seen by the PC NIC card.
- **Task 4 continues:** The **ping** command was used to generate packets to the other pair group PCs.
- **Task 4 continues:** Observation of the captured frames showed that they were treated as directly reachable. The PC correctly interpreted the subnet mask bits indicating that the IP addresses used were local to the subnet.

Relationship to OSI Model Layers

Using the OSI model, you can identify the entities and attributes that were used in this lab.

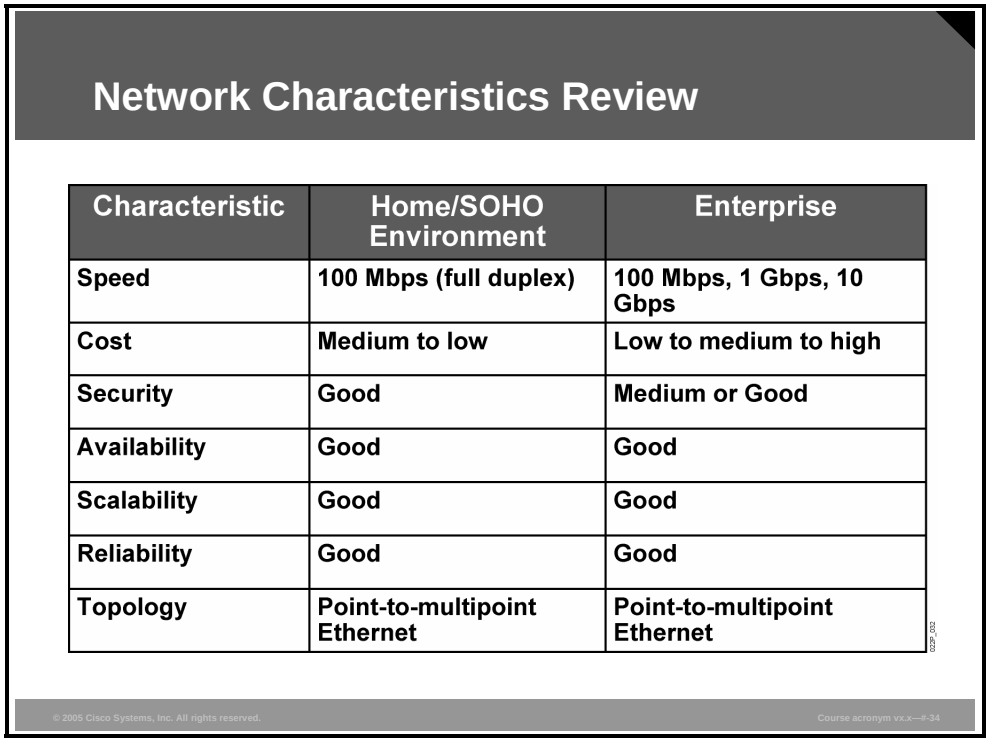


You can observe these layers of the OSI model in relation to the lab:

- **Physical layer (1):** A straight-through data cable was required.
- **Data link layer (2):** The Ethernet frame is a Layer 2 entity, as is the Ethernet switch. The Ethernet switch examines frame addresses and intelligently filters or forwards frames out of specific ports.
- **Network layer (3):** The protocols ICMP and ARP that were observed operate at Layer 3. The packet, which was used by the protocols, is also a Layer 3 entity.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.

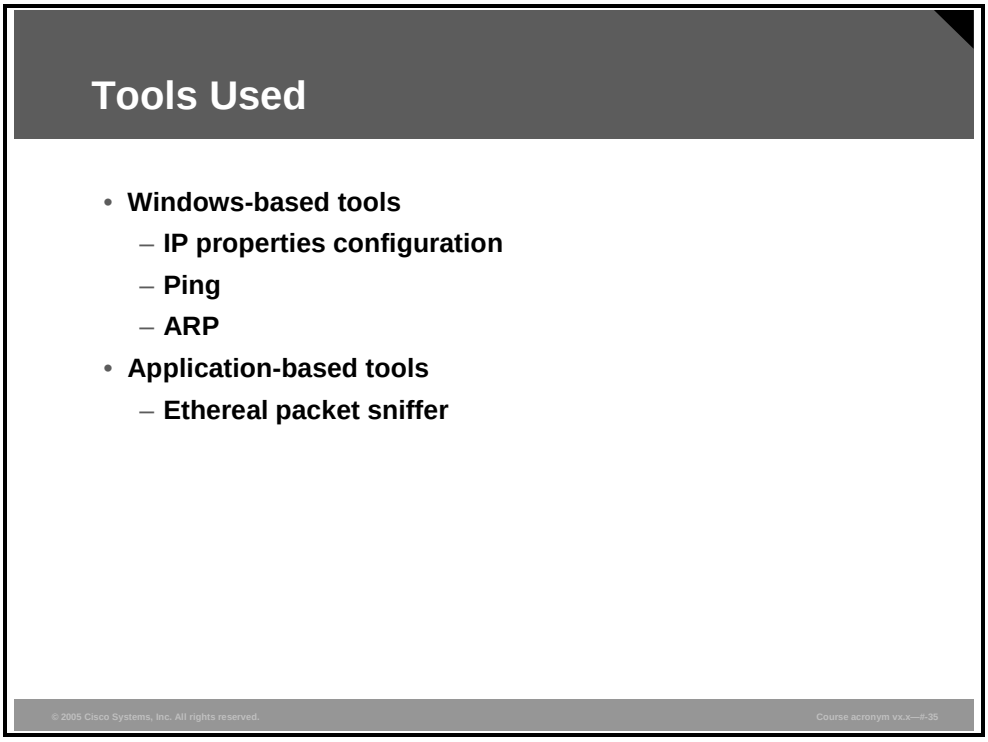


The change of subnet mask does not change these fundamental characteristics of the Ethernet switch-connected network:

- **Speed:** In the home or SOHO environment, the speed is 100 Mbps and the network will operate at full-duplex mode. In the enterprise environment, however, speeds can range from 100 Mbps to 1 Gbps or 10 Gbps.
- **Cost:** In the home or SOHO environment, the cost would be considered medium-to-low. The enterprise cost would be considered to be between low and high, because the cost of enterprise routers varies, depending on performance and functionality.
- **Security:** In a home or SOHO environment, security could be considered good from a switching perspective. In an enterprise environment, security could be considered medium-to-good—while switching does limit the possibility of frame capture by sniffing software, there are methods that can compromise this relative security.
- **Availability:** The availability is good.
- **Scalability:** The scalability is good.
- **Reliability:** The reliability is good.
- **Topology:** The topology is point-to-multipoint.

Tools

In this lab, a number of tools were used.



Lab 6-1: Establishing a Telnet Connection to a Remote Terminal Server

Complete this lab activity to practice what you learned in the related module.

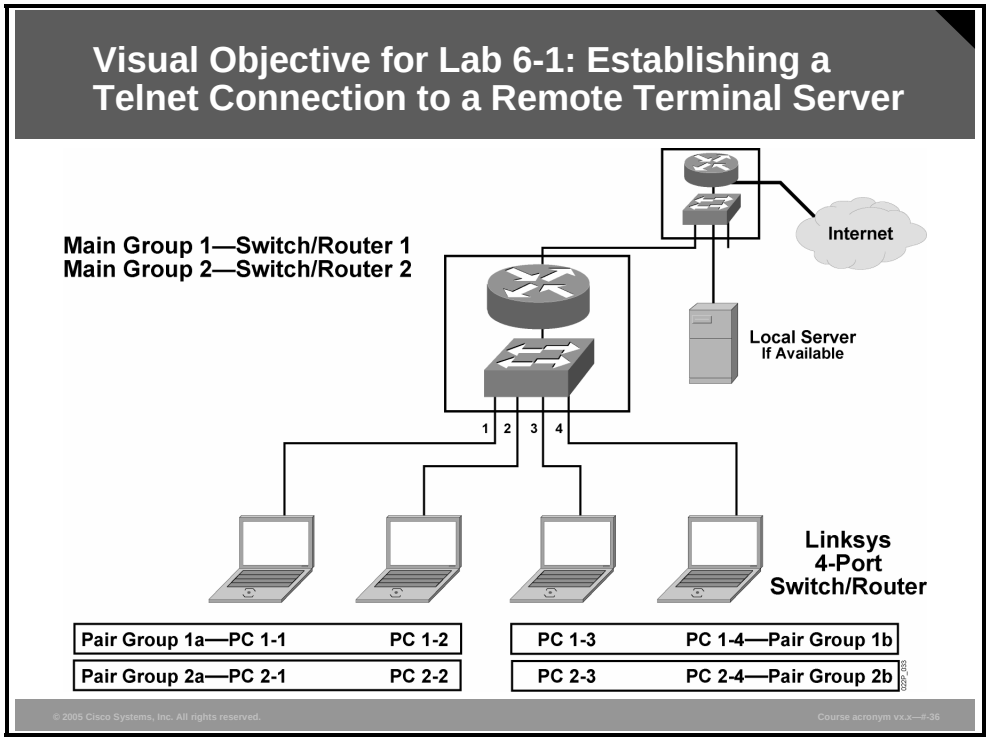
Activity Objective

In this activity, you will establish a Telnet connection to a remote terminal server that requires authorization. After completing this activity, you will be able to meet these objectives:

- Capture network traffic while using Telnet to access the terminal server
- Observe the initial TCP startup process and record TCP control flags: SYN and ACK
- Observe that the Telnet protocol transmits its data unencrypted, which can lead to passwords being compromised

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- Four PCs, one four-port switch, supplied Ethernet data cables
- PCs running Windows 2000 or XP operating system
- Ethereal packet sniffer application software installed on the PCs

Note	Some companies do not permit packet sniffer software to be installed on their networks. Be sure that you are in compliance with the regulations of your company before performing this lab.

Command List

The table describes the command used in this activity.

Command	Description
telnet *ip address*	Starts a Telnet client application to the specified address

Job Aids

There are no job aids for this lab activity.

Activity Preparation

It is assumed that the network configuration and topology are identical to those at the end of Lab 5-1.

Required Information (Provided by Instructor)

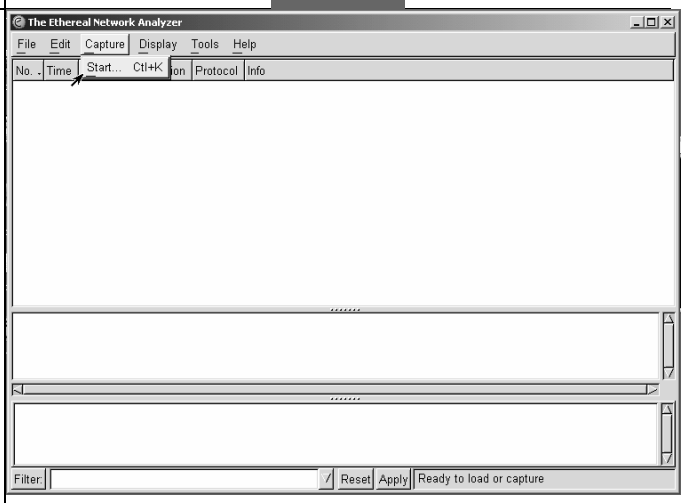
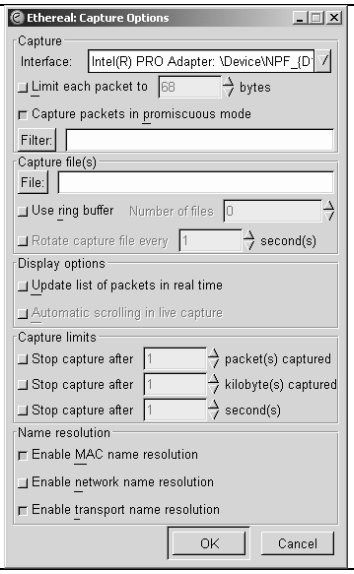
Description	Default Value	Instructor-Supplied Value
Remote IP address	128.107.245.71	
Remote username	student	
Remote password	cisco	

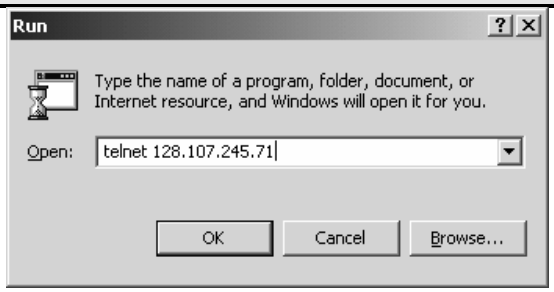
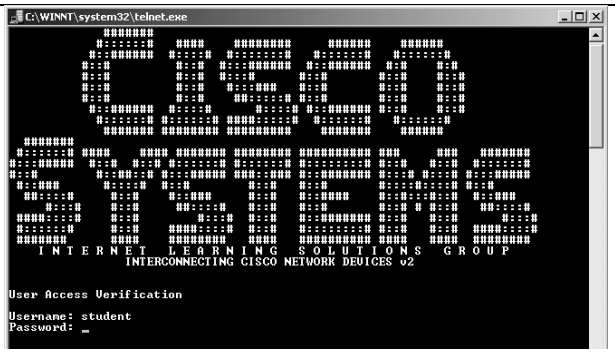
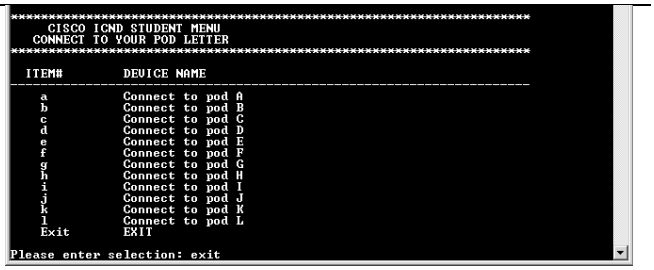
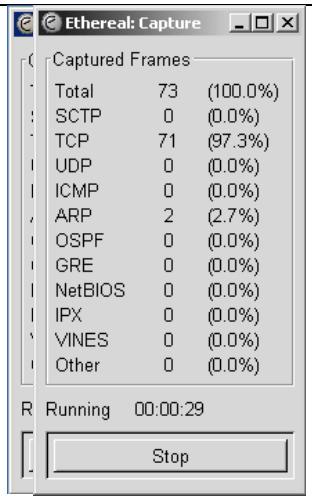
Task 1: Establish a Telnet Session to a Remote Host

In this task, you will you will start a packet capture using Ethereal. Next, you will establish a Telnet connection to a remote host, complete the login sequence, and then exit.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the desktop, launch the Ethereal application using the shortcut. Expand the application window to full screen.	
2.	Choose **Capture** > **Start** from the menu. The Ethereal Capture Options window opens.	
3.	There are no special options to choose, so click the **OK** button. The Ethereal Capture window opens.	

Step	Action	What You See
4.	From Windows: ■ Click **Start.** ■ Choose **Run.** ■ Enter **telnet** *ip-address* (where "ip-address" is the remote IP address from the "Required Information" table in the Activity Preparation section at the beginning of this lab).	
5.	Using the information from the "Required Information" table in the Activity Preparation section at the beginning of this lab, enter the username and password at the prompts.	
6.	At the prompt, enter **exit** to terminate the session.	
7.	Return to the Ethereal Capture window and click the **Stop** button.	

Activity Verification

You have completed this task when you attain this result:

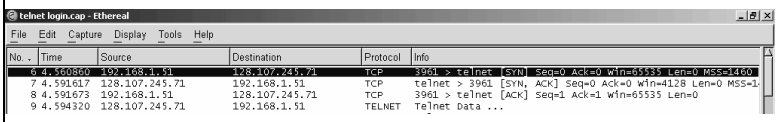
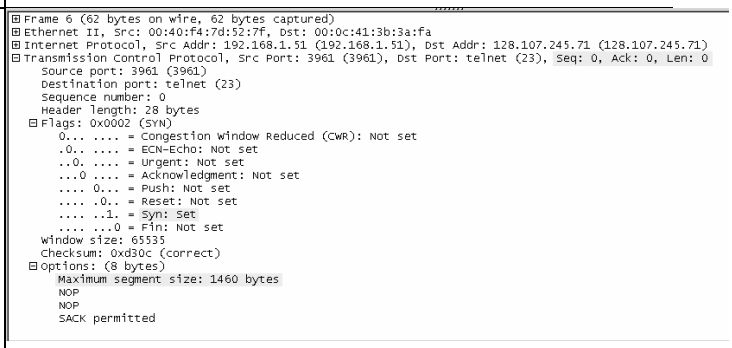
- You connected to a remote host by Telnet, completed the login sequence, and exited.

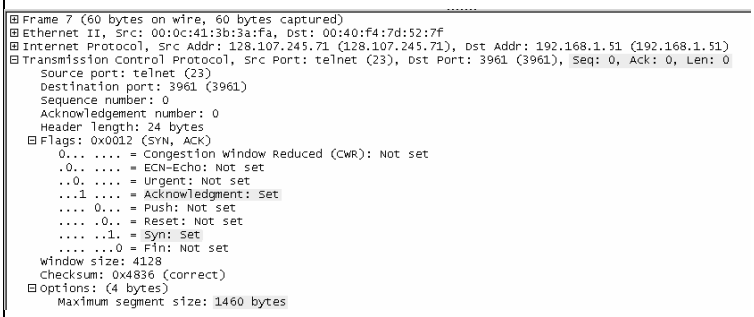
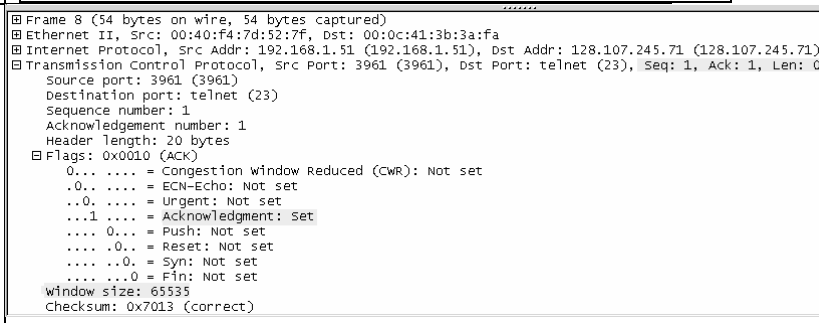
Task 2: Examine the TCP Three-Way Handshake

In this task, you will test your connection by use of the **ping** command. Confirm that the other pair group has reached this point in the lab before proceeding.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	At the bottom of the main window of Ethereal, enter **ip.addr==128.107.245.71** in the Filter field. (If you used a different address, then enter that address instead.) Click the **Apply** button. This action has the effect of displaying only the captured packets to or from this address.	
2.	In the top window, click the first packet.	
3.	In the middle window, you see the detail of that packet. Expand the Transmission Control Protocol information field by clicking the plus (**+**) sign. Expand the Flags and the Options fields by clicking the plus (**+**) sign next to them. You may need to increase the size of the middle window to display all values simultaneously. Your output should resemble the figure.	
4.	In the space provided, enter the sending sequence number, number, header length, flags, window size, and maximum segment size.	Sending sequence number: Header length Flags: Window size Maximum segment size:

Step	Action	What You See
5.	In the top window, click the second frame in the session. This may *not* be the absolute frame number because you are displaying *only* those frames that you are interested in.	
6.	Observe the receiving sequence number, acknowledgment number, header length, flags, window size and maximum segment size. Record these values in the spaces provided.	Receiving sequence number: Acknowledgment number: Header length: Flags: Window size Maximum segment size:
7.	In the top window, click the third frame in the session.	
8.	Observe the sending sequence number, acknowledgment number, header length, flags, and windowsize. Record these opposite.	Sending sequence number: Acknowledgment number: Header length: Flags: Window size
9.	The sending and receiving ends are now synchronized, and the connection is established.	

Activity Verification

You have completed this task when you attain these results:

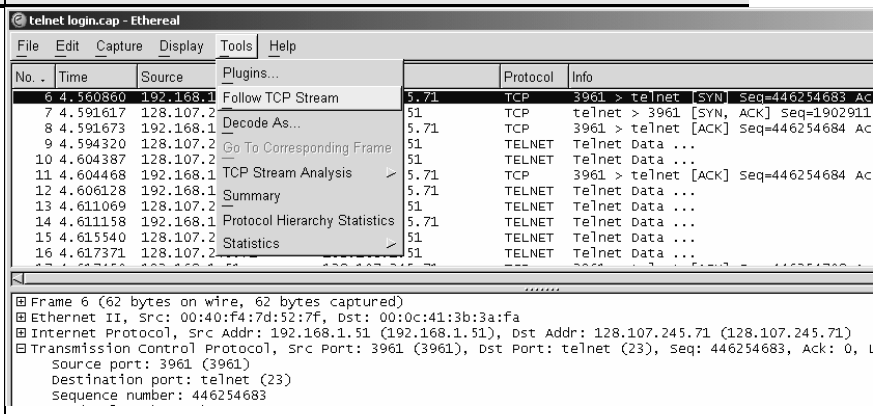
- You established a Telnet session to a destination terminal server, completed the login sequence, and then exited the session.
- You analyzed the sniffer packet capture to observe:
  - TCP establishment sequence
  - Sequence, acknowledgment numbers, and header length
  - TCP control flags: SYN and ACK
  - Window size and maximum segment size

Task 3: Observe the Entire TCP Session

In this task, you will use an Ethereal tool that links together all the packets in a TCP session and displays them.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	In the top window, right-click the first TCP packet. Then choose **Tools** > **Follow TCP Stream**.	
2.	The resulting output should resemble the figure.	
3.	Notice that although the password was *not* echoed back, it was sent as clear text. This is considered a security flaw in Telnet. A new protocol, SSH, has been employed to encrypt the remote connection process and make it more secure. Although this technique is beyond the scope of this course, it is interesting to observe the difference.	

Activity Verification

You have completed this task when you attain this result:

- You viewed the entire Telnet session from the captured packets by using a tool within the Ethereal application.

Task 4: Relate to the OSI Model

You will relate the subnet mask change to the OSI model.

Activity Procedure

In the spaces provided, indicate the correct layer for the following:

- IP packet
- IP address
- TCP port number
- TCP flags
- Telnet protocol

OSI Layer	Item, Entity, or Attribute
1 (Physical)	
2 (Data link)	
3 (Network)	
4 (Transport)	
5 to 7 (Application)	

Activity Verification

You have completed this task when you attain this result:

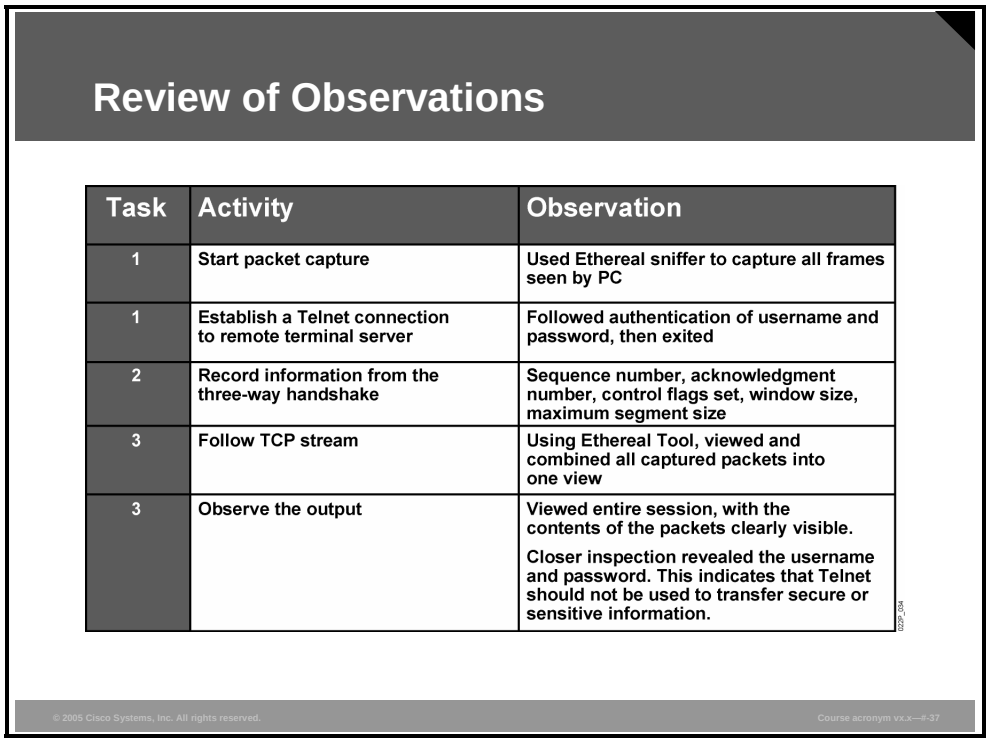
- You successfully completed the OSI information table.

Lab 6-1: Debrief

This debriefing session covers the activities in the "Establishing a Telnet Connection to a Remote Terminal Server" lab. The topics addressed include a review of the correct steps for establishing the Telnet connection, a discussion of the related OSI model layers, a definition of the network in terms of a set of network characteristics, and a review of tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of establishing a Telnet connection.

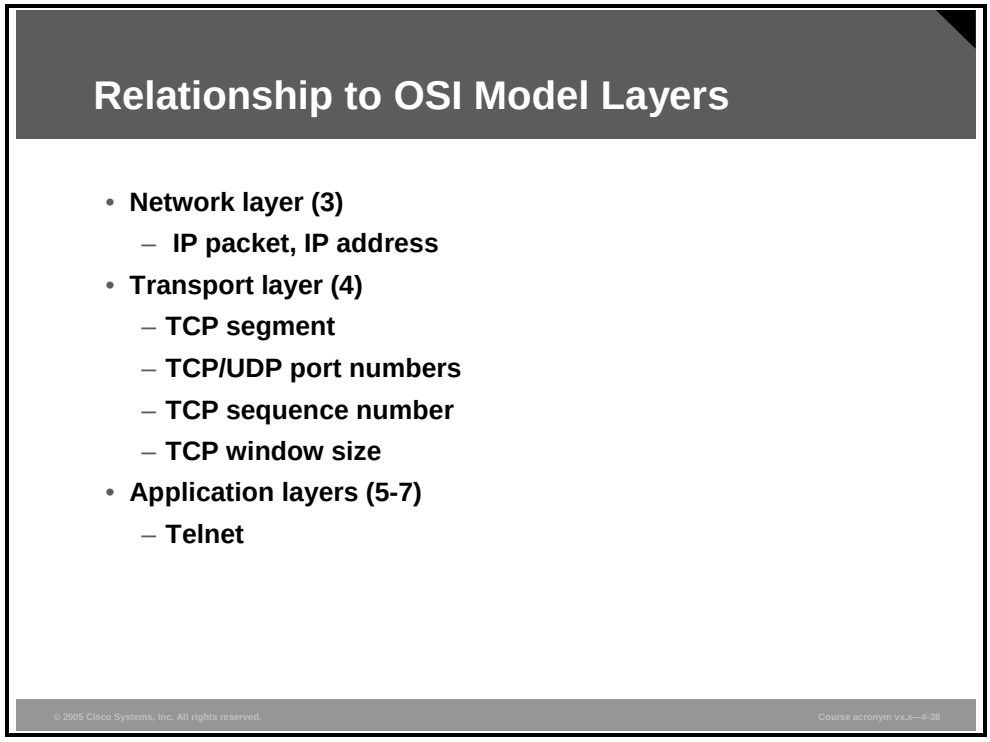


The figure shows the observations that you should have made during the lab, as follows:

- **Task 1:** The Ethereal packet sniffer software was used to capture all the frames that were seen.
- **Task 1 continues:** You followed the authentication of your username and password and then exited.
- **Task 2:** Information about the three-way handshake (including sequence number, acknowledgment number, length, flags set, window size, and maximum segment size) was recorded.
- **Task 3:** Using Ethereal, you viewed the packets and then combined all captured packets into one view.
- **Task 3 continues:** This task showed the entire session, with the contents of the packets clearly visible. Closer inspection revealed the username and password, indicating that Telnet should *not* be used to transfer secure or sensitive information.

Relationship to OSI Model Layers

Using the OSI model, you can identify the entities and attributes that were used in this lab.

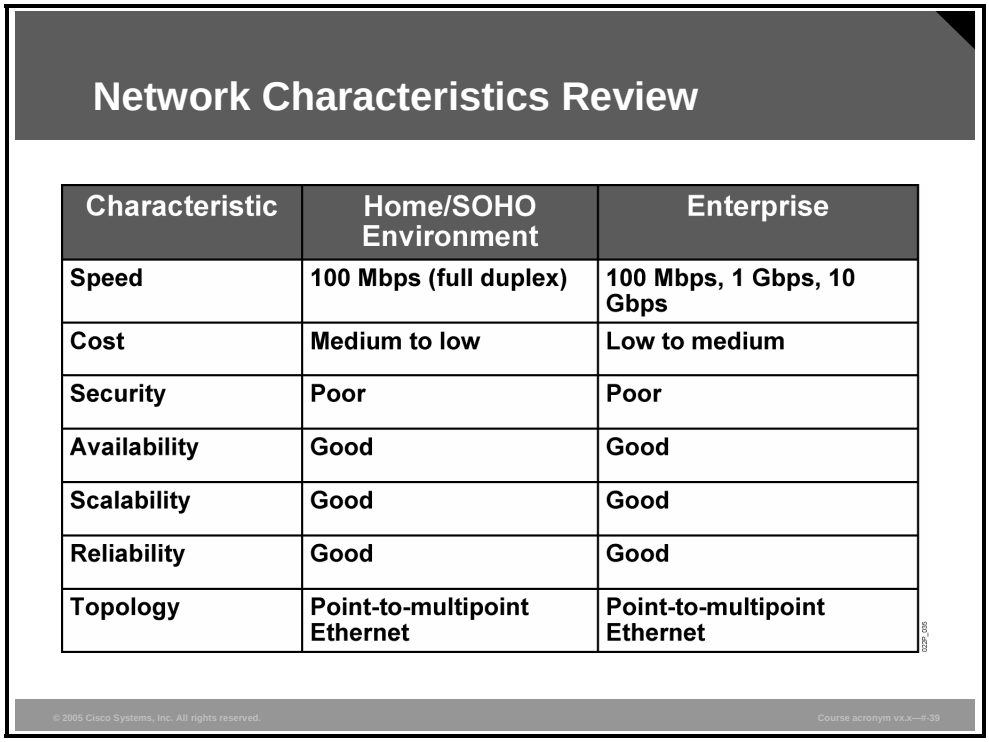


You can observe these layers of the OSI model in relation to the lab:

- **Network layer (3):** The IP packet and IP address are Layer 3 entities.
- **Transport layer (4):** The TCP segment, TCP/UDP port numbers, TCP sequence number, and TCP window size are Layer 4 entities.
- **Application layers (5 to 7):** Telnet operates in Layers 5 through 7.

Network Characteristics

You are already familiar with a set of network characteristics that are used to describe each network type that is being created in this course.

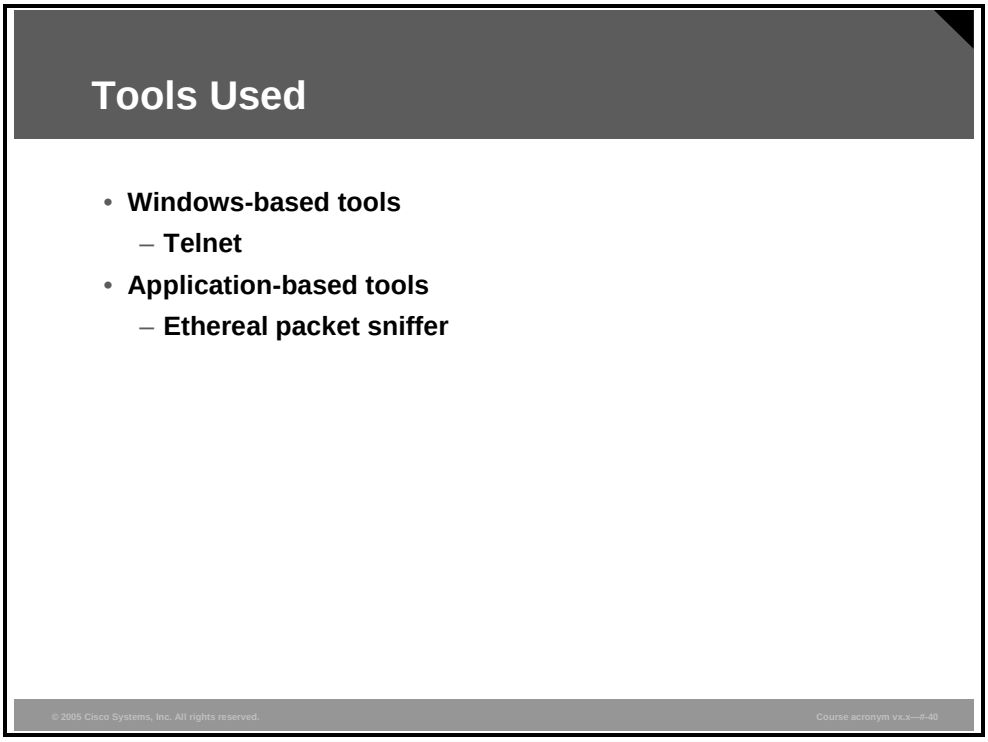


These are some differences in network characteristics in this environment, depending on whether the environment is home, SOHO, or enterprise.

- **Speed:** In the home or SOHO environment, the speed is 100 Mbps and the network will operate at full-duplex mode. In the enterprise environment, however, speeds can range from 100 Mbps to 1 or 10 Gbps.
- **Cost:** In the home or SOHO environment, the cost is medium-to-low, while in the enterprise environment, the cost can range from low to high.
- **Security:** Security is low because the Telnet application sends information, including passwords, as clear text.
- **Availability:** The availability in both environments is good.
- **Scalability:** The scalability in both environments is good.
- **Reliability:** The reliability in both environments is good.
- **Topology:** The topology in both environments is point-to-multipoint.

Tools

In this lab, a number of tools were used.



Lab 8-1: Establishing a Telnet Connection to the Cisco Remote Lab

Complete this lab activity to practice what you learned in the related module.

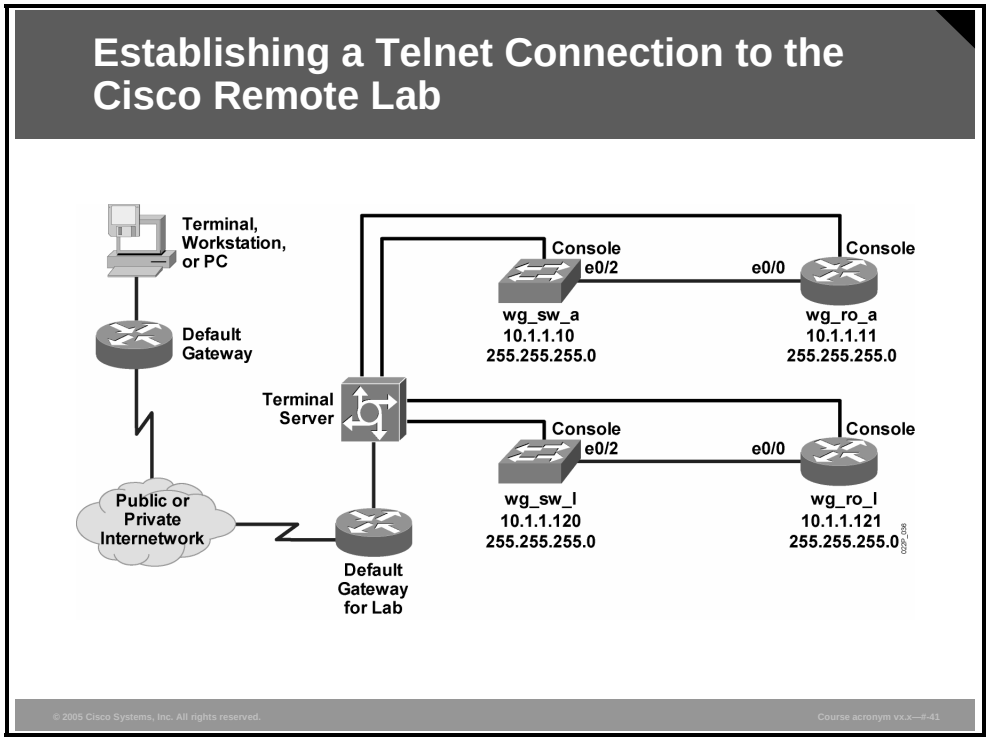
Activity Objective

In this activity, you will establish a Telnet connection to the terminal server to access the devices in your pod. After completing this activity, you will be able to meet these objectives:

- Run Telnet to connect to the remote lab
- Verify connectivity to the remote lab terminal server

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- PC connected to an onsite lab or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device (if you are using a remote lab)
- INTRO pod assigned by your instructor

Command List

The table describes the command used in this activity.

Command	Description
telnet *ip-address*	Starts a terminal emulation program from a PC, router, or switch that permits you to access network devices remotely over the network

Job Aids

There are no job aids for this lab activity.

Activity Preparation

Your instructor will provide the setup information that you need to complete this and the subsequent lab activities. Your instructor will also assign you to a pod, identified by the letters A through L. Complete the following information as provided by your instructor.

Required Information (Provided by Instructor)

Value	Information Provided by Your Instructor
Your workgroup	
IP address of your terminal	
IP address of the default gateway	
Subnet mask	
IP address of the terminal server	
Username to access the terminal server	
Password to access the terminal server	
IP address of the TFTP server	

Task 1: Run Telnet to Connect to the Remote Lab

To begin the lab, you will use the Telnet utility to establish a connection to the remote lab equipment for this course.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From the Microsoft Windows Start menu, choose **Run**. The Run window appears.	
2.	In the Open field, enter the **telnet** command followed by the IP address for your terminal server, provided by your instructor. For example, if the terminal server address that you were provided is 10.1.1.254, you would enter **telnet 10.1.1.254**. If your Telnet session successfully connects to the terminal server, you should see an opening menu similar to the figure.	********** CISCO ICND STUDENT MENU CONNECT TO YOUR POD LETTER ********** ITEM# DEVICE NAME 1 Connect to pod A 2 Connect to pod B 3 Connect to pod C 4 Connect to pod D 5 Connect to pod E 6 Connect to pod F 7 Connect to pod G 8 Connect to pod H 9 Connect to pod I 10 Connect to pod J 11 Connect to pod K 12 Connect to pod L 13 EXIT Please enter selection:
3.	At the “Please enter selection” prompt, enter your workgroup letter and press **Return**. Your output should look similar to the figure.	********** POD L To exit back out to the menu press "CTRL+SHIFT+6" then "X". You must clear the line before re-connecting to a device. ********** 1 Connect to workgroup switch L 2 Connect to workgroup router L 3 Clear connection to w/g switch L 4 Clear connection to w/g router L 5 Return to main menu Please enter selection:

Activity Verification

You have completed this task when you attain this result:

- You successfully used Telnet to connect to the remote lab.

Task 2: Use the Pod Menu to Connect to Your Workgroup Switch

The pod menu lists your pod letter at the top. In the example in Task 1, the current pod is pod L. From the menu, you can connect to either your workgroup switch or your workgroup router. Once you connect to a network device from the terminal server, you will need to use a special keystroke sequence, Ctrl-Shift-6, then x**,** to return to the menu. (To do this, hold down the **Shift** key, press the **Control** key and the **6** key, and then press the **x** key.)

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Enter **1** to connect to your workgroup switch. You should see something similar to this example in your Telnet session.	`Please enter selection: 1` `Trying h26 (10.10.10.10, 2058)... Open`
2.	Press **Return** to access the device prompt.	
3.	To return to the menu, press **Ctrl-Shift-6**, then **x**. The pod menu appears again. When you return to the pod menu, your session to your workgroup switch is still open. You should clear all open connections on a terminal server before exiting. If you do not close your open sessions, the Cisco IOS software will prompt you to close your open connections. To close a session, you must choose the appropriate option from the menu.	
4.	Enter option **3** to clear the connection to your workgroup switch. When the "[confirm]" prompt appears, press **Return**. What does the prompt say now? (Write your answer in the space provided.)	
5.	Enter option **2** to connect to your workgroup router. What does the prompt say now? (Write your answer in the space provided.) As with the switch, you may need to press **Return** one time to see the prompt on your terminal screen.	
6.	Enter **Ctrl-Shift-6**, then **x**, to return to the pod menu.	
7.	Enter option **4** to clear the connection to your workgroup router. When the "[confirm]" prompt appears, press **Return**.	
8.	Enter option **5** to return to the main menu from the pod menu.	
9.	Exit the terminal server by entering the option from the pod menu to exit. If there is no option to exit on the menu, contact your instructor for instructions.	
10.	If you see the "You have open connections [confirm]" prompt, enter **yes** and press **Return**. Depending on which operating system is running on your PC, you may need to press **Return** after terminating your Telnet session.	
11.	Notify your instructor that you have completed the lab activity.	

Activity Verification

You have completed this task when you attain this result:

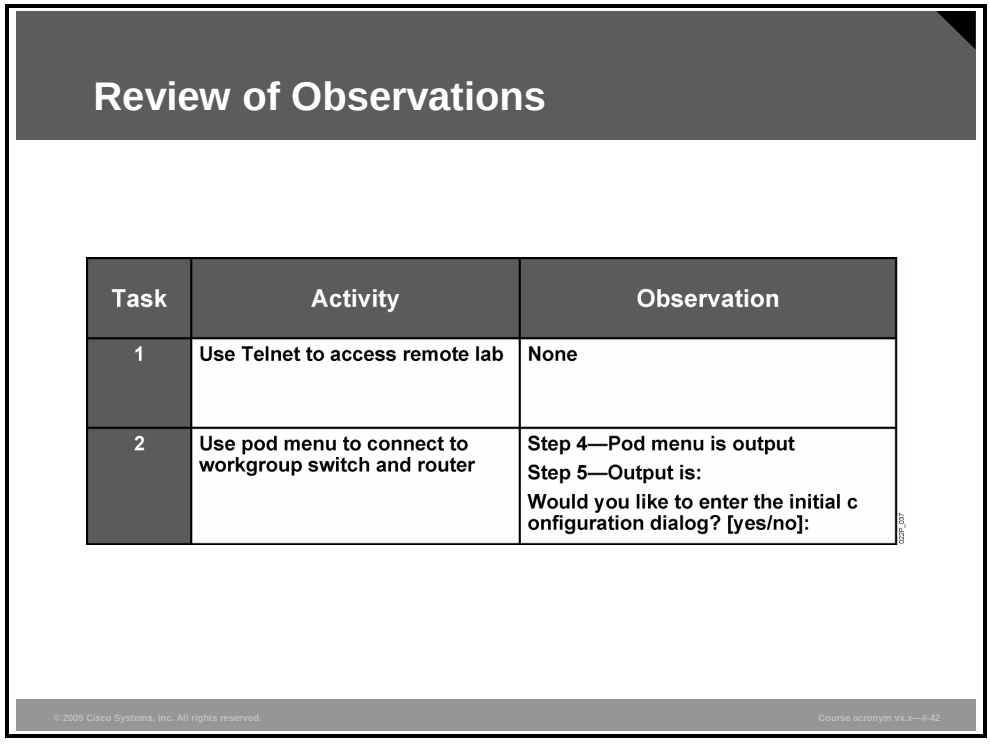
- You successfully used the pod menu to connect to your workgroup switch.

Lab 8-1: Debrief

This debriefing session covers the activities in the “Cisco Remote Lab Connection” lab. The topics addressed include a review of the correct steps for connecting to the remote lab and a review of tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of connecting to the remote lab.



The figure shows the observations that you should have made during the lab, as follows:

- **Task 2, Step 4:** The output returns to the pod menu:

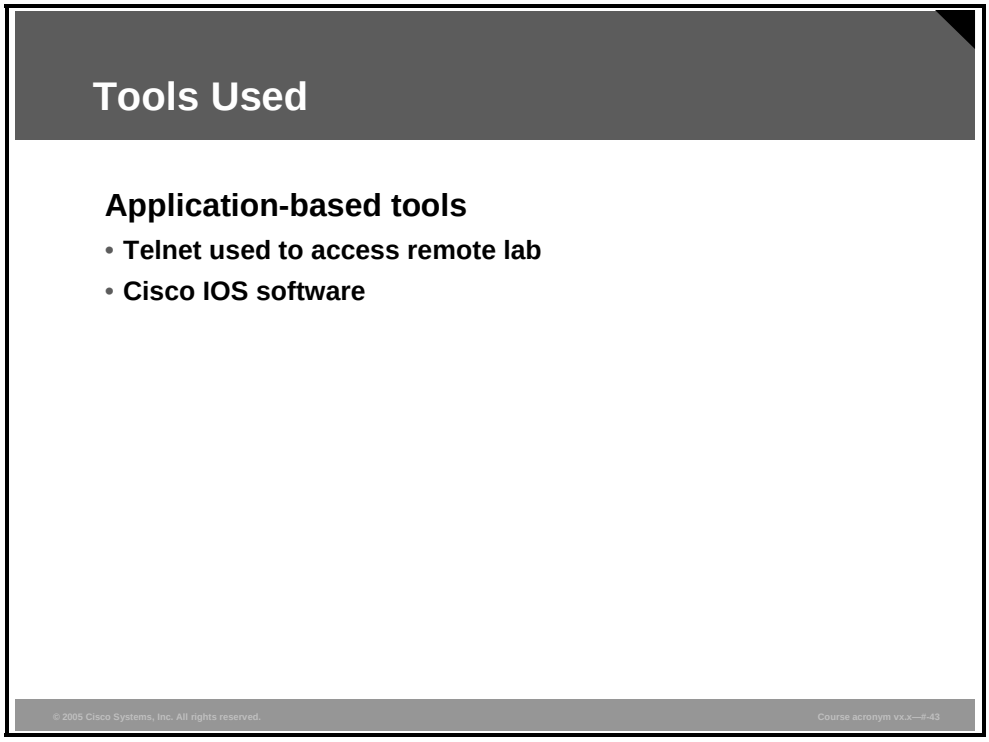
```
**********************************************************
   POD X


To exit back out to the menu press "CTRL+SHIFT+6" then "X".
 You must clear the line before re-connecting to a device.
-- Text omitted --
Please enter selection:
```

- **Task 2, Step 5:** The output should indicate that the router is waiting for input:

```
% Please answer 'yes' or 'no'.
Would you like to enter the initial configuration dialog?
  [yes/no]:
```

Tools

In this lab, a number of tools were used.



- **Telnet:** This IP application was used as a tool to provide access to the remote terminal server, which allows connection to the switches and routers that form the lab.
- **Cisco IOS:** The Cisco IOS operating system CLI comprises many commands that are used as tools to configure, test, and maintain Cisco routers and switches. The Cisco IOS software also contains commands that allow a menu system to be built to allow users to access only specific commands or do preset actions. This function is most frequently used to support terminal servers, which allow connections to only specific serial lines.

Lab 8-2: Completing Switch Startup and Initial Configuration

Complete this lab activity to practice what you learned in the related module.

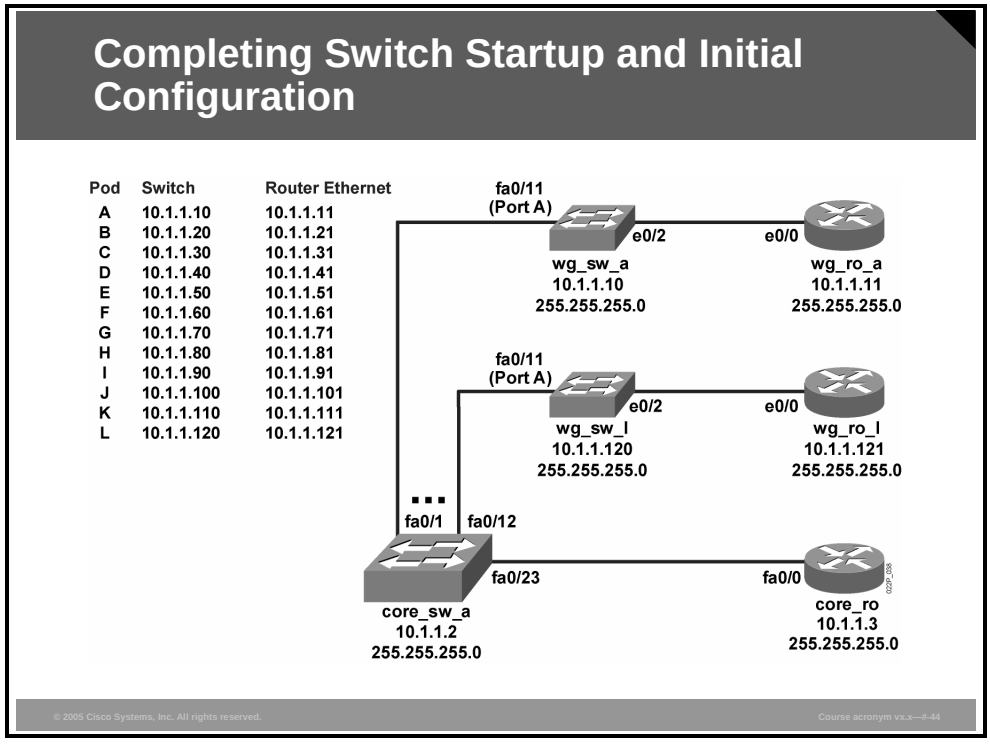
Activity Objective

In this activity, you will connect to your workgroup switch and complete the initial device setup, and you will explore the help facility. After completing this activity, you will be able to meet these objectives:

- Restart the switch and verify the initial configuration messages
- Complete the initial device setup on the Cisco Catalyst 2950

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- PC connected to an onsite lab or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device (if you are using a remote lab)
- INTRO pod assigned by your instructor

Command List

The table describes the commands used in this activity.

Command	Description
configure terminal	Activates the configuration mode from the terminal.
copy running-config startup-config	Copies the switch running configuration file to another destination.
enable	Activates the privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured.
erase startup-config	Erases the startup configuration in memory (Catalyst 2950).
hostname	Sets the system name.
interface vlan 1	Enters the interface configuration mode for VLAN 1 to set the switch management IP address (Catalyst 2950).
ip address	Sets the IP address and mask of the switch.
ip default-gateway	Sets the default gateway of the switch.
login	Sets login identifier on the console or virtual terminal ports (Catalyst 2950).
password	Assigns a password to the console or virtual terminal ports (Catalyst 2950).
show interface vlan 1	Displays the switch IP address information (Catalyst 2950).

Job Aids

There are no job aids for this lab activity.

Activity Preparation

Your instructor will assign you to a pod, identified by the letters A through L. The table identifies the switch IP address, host name, and subnet mask for each pod. You will need this information to complete the lab activity.

Pod	Switch Host Name	Workgroup Switch IP Address	Subnet Mask
Pod A	wg_sw_a	10.1.1.10	255.255.255.0
Pod B	wg_sw_b	10.1.1.20	255.255.255.0
Pod C	wg_sw_c	10.1.1.30	255.255.255.0
Pod D	wg_sw_d	10.1.1.40	255.255.255.0
Pod E	wg_sw_e	10.1.1.50	255.255.255.0
Pod F	wg_sw_f	10.1.1.60	255.255.255.0
Pod G	wg_sw_g	10.1.1.70	255.255.255.0
Pod H	wg_sw_h	10.1.1.80	255.255.255.0
Pod I	wg_sw_i	10.1.1.90	255.255.255.0
Pod J	wg_sw_j	10.1.1.100	255.255.255.0
Pod K	wg_sw_k	10.1.1.110	255.255.255.0
Pod L	wg_sw_l	10.1.1.120	255.255.255.0

Task 1: Connect to Your Workgroup Switch

In this task, you will use Telnet to connect to your workgroup switch so that you can verify the initial configuration messages. After that, you will complete the setup for your Catalyst 2950 switch.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Use Telnet to access the terminal server for the lab exercises. You should see a menu that is similar to the example.	********** CISCO ICND STUDENT MENU CONNECT TO YOUR POD LETTER ********** ITEM# DEVICE NAME ---------- 1 Connect to pod A 2 Connect to pod B 3 Connect to pod C 4 Connect to pod D 5 Connect to pod E 6 Connect to pod F 7 Connect to pod G 8 Connect to pod H 9 Connect to pod I 10 Connect to pod J 11 Connect to pod K 12 Connect to pod L 13 EXIT Please enter selection:
2.	At the "Please enter selection" prompt, enter your workgroup number and press **Return**. Your output should look similar to the example. The menu, called the pod menu, lists your pod letter at the top. In the example, the current pod is Pod L.	********** POD L To exit back out to the menu press "CTRL+SHIFT+6" then "X". You must clear the line before re-connecting to a device. ********** 1 Connect to workgroup switch L 2 Connect to workgroup router L 3 Clear connection to w/g switch L 4 Clear connection to w/g router L 5 Return to main menu Please enter selection:
3.	Enter **1** and press **Return** to connect to your workgroup switch. Your output should look similar to the example.	Please enter selection: 1 Trying h26 (10.10.10.10, 2058)... Open

Activity Verification

You have completed this task when you attain this result:

- The switch initial configuration messages were displayed on your console.

Task 2: Verify That the Switch Is Unconfigured

In this task, you will verify that the switch has no configuration.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Press **Return** until the following prompt appears: "Continue with configuration dialog? [yes/no]."	
2.	If you see the prompt, go to Task 3 of this lab activity. If you do not see the "Continue with configuration dialog?" prompt, complete Steps 3 through 7.	
3.	Press **Return** to enter the switch console session. You should see a display similar to the example when you enter the switch console session:	`Switch>`
4.	Enter the **enable** command to access privileged EXEC mode.	

5.	To ensure that you start with a fresh configuration, erase the startup configuration. To do this, enter the **erase startup-config** command from the privileged EXEC mode. You should see a display similar to the example.	`Switch#`**`erase startup-config`**
		`Erasing the nvram filesystem will remove all files! Continue? [confirm]y[OK]`
		`Erase of nvram: complete`

6.	Enter the **reload** command. You are prompted to confirm the reload.	`Proceed with reload? [confirm]`

Step	Action	What You See
7.	At the “Proceed with reload?” prompt, press **Return** to confirm erasure and to confirm reloading. You should see a display similar to the example.	2d04h: %SYS-5-RELOAD: Reload requested C2950 Boot Loader (C2950-HBOOT-M) Version 12.1(11r)EA1, RELEASE SOFTWARE (fc1) Compiled Mon 22-Jul-02 18:57 by antonino WS-C2950-24 starting... Base ethernet MAC Address: 00:08:a4:45:ce:80 Xmodem file system is available. Initializing Flash... flashfs[0]: 84 files, 3 directories flashfs[0]: 0 orphaned files, 0 orphaned directories flashfs[0]: Total bytes: 7741440 flashfs[0]: Bytes used: 6131200 flashfs[0]: Bytes available: 1610240 flashfs[0]: flashfs fsck took 7 seconds. ...done initializing flash. Boot Sector Filesystem (bs:) installed, fsid: 3 Parameter Block Filesystem (pb:) installed, fsid: 4 Loading "flash:/c2950-i6q4l2-mz.121-20.EA1.bin"...## File "flash:/c2950-i6q4l2-mz.121-20.EA1.bin" uncompressed and installed, entry point: 0x80010 000 executing... Restricted Rights Legend Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph(c) of the Commercial Computer Software – Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013. cisco Systems, Inc. 170 West Tasman Drive San Jose, California 95134-1706 Cisco Internetwork Operating System Software IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(20)EA1, RELEASE SOFTWARE (fc1) Copyright (c) 1986-2004 by cisco Systems, Inc. Compiled Wed 04-Feb-04 21:21 by yenanh Image text-base: 0x80010000, data-base: 0x805A8000

Step	Action	What You See
		Initializing flashfs... flashfs[1]: 84 files, 3 directoriesv flashfs[1]: 0 orphaned files, 0 orphaned directories flashfs[1]: Total bytes: 7741440 flashfs[1]: Bytes used: 6131200 flashfs[1]: Bytes available: 1610240 flashfs[1]: flashfs fsck took 7 seconds. flashfs[1]: Initialization complete. Done initializing flashfs. POST: System Board Test : Passed POST: Ethernet Controller Test : Passed ASIC Initialization Passed POST: FRONT-END LOOPBACK TEST : Passed cisco WS-C2950-24 (RC32300) processor (revision B0) with 20713K bytes of memory. Processor board ID FAB0602W38Q Last reset from system-reset Running Standard Image 24 FastEthernet/IEEE 802.3 interface(s) 32K bytes of flash-simulated non-volatile configuration memory. Base ethernet MAC Address: 00:08:A4:45:CE:80 Motherboard assembly number: 73-5781-08 Power supply part number: 34-0965-01 Motherboard serial number: FAB060273IB Power supply serial number: PHI05460C2K Model revision number: B0 Model number: WS-C2950-24 System serial number: FAB0602W38Q --- System Configuration Dialog --- Would you like to enter the initial configuration dialog? [yes/no]:

Activity Verification

You have completed this task when you attain this result:

- You were able to verify that the switch has no configuration.

Task 3: Complete the Initial Device Setup on the Cisco Catalyst 2950

In this task, you will complete the setup on the workgroup switch and verify the configuration.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	At the “Continue with configuration dialog?” prompt, enter **no**. You will return to CLI mode on the switch. You should see the Switch> prompt.	
2.	Enter the **enable** command to begin the privileged EXEC mode. The prompt changes to Switch#.	
3.	At the Switch# prompt, enter the **configure terminal** command. The prompt changes to Switch(config)#.	
4.	At the Switch(config)# prompt, enter the **interface VLAN 1** command to enter the interface configuration mode for VLAN 1 (the management VLAN). The prompt changes to Switch(config-if)#.	
5.	Enter the IP address of the switch with the **ip address 10.1.1.*x* 255.255.255.0** command. See the table in the Activity Preparation section of this lab activity to determine the IP address of the switch for your assigned pod.	
6.	Enter the **no shutdown** command to enable the interface.	
7.	To return to global configuration mode, enter the **exit** command. The prompt changes to Switch(config)#.	
8.	Enter the **ip default-gateway 10.1.1.3** command to assign the default gateway for the switch. You should still have the Switch(config)# prompt.	
9.	To set the switch host name, enter the **hostname wg_sw_*x*** command (where “x” is the letter for your pod). After you entered the **hostname** command, what did your prompt change to? (Enter your answer in the space provided.)	
10.	At the wg_sw_x(config)# prompt (where “x” is the letter for your pod), enter the **end** command. What is the prompt now? (Enter your answer in the space provided.)	

Step	Action	What You See

11.	To view the help system, enter a question mark (**?**). You should see a display similar to the example.	`_sw_z#?wg`
		`Exec commands:`
		`  access-enable  Create a temporary Access-List`
		`  entry`
		`  access-template  Create a temporary Access-List`
		`  entry`
		`  archive  manage archive files`
		`  cd  Change current directory`
		`  clear  Reset functions`
		`  clock  Manage the system clock`
		`  cluster  cluster exec mode commands`
		`  configure  Enter configuration mode`
		`  connect  Open a terminal connection`
		`  copy  Copy from one file to another`
		`  debug  Debugging functions (see also 'undebug')`
		`  delete  Delete a file`
		`  dir  List files on a filesystem`
		`  disable  Turn off privileged commands`
		`  disconnect  Disconnect an existing network`
		`  connection`
		`  enable  Turn on privileged commands`
		`  erase  Erase a filesystem`
		`  exit  Exit from the EXEC`
		`  format  Format a filesystem`
		`  fsck  Fsck a filesystem`
		`--More—`

12.	Press the **Space Bar** to continue the display. You should see a display similar to the example.	`help  Description of the interactive help system`
		`  lock  Lock the terminal`
		`  login  Log in as a particular user`
		`  logout  Exit from the EXEC`
		`  mkdir  Create new directory`
		`  more  Display the contents of a file`
		`  name-connection  Name an existing network connection`
		`  no  Disable debugging functions`
		`  ping  Send echo messages`
		`  pwd  Display current working directory`
		`  rcommand  Run command on remote switch`
		`  reload  Halt and perform a cold restart`
		`  rename  Rename a file`
		`  resume  Resume an active network connection`
		`  rmdir  Remove existing directory`
		`  rsh  Execute a remote command`
		`  send  Send a message to other tty lines`
		`  set  Set system parameter (not config)`
		`  setup  Run the SETUP command facility`
		`  show  Show running system information`
		`  systat  Display information about terminal lines`
		`  telnet  Open a telnet connection`
		`--More--`

13.	To scroll line by line, press the **Return** key three times. You should see a new line of help information for each time that you press Return.	`terminal  Set terminal line parameters`
		`  test  Test subsystems, memory, and interfaces`
		`  traceroute  Trace route to destination`
		`--More--`

Step	Action	What You See
14.	To exit the help system, enter **q**. The console prompt appears.	
15.	Enter the **show ip interface** command to verify your switch IP address.	

Activity Verification

You have completed this task when you attain this result:

- You were able to accurately enter the IP address, network mask, and default gateway.

Task 4: Configure Passwords

In this task, you will configure passwords to protect access to the enable mode, to protect access using the console line, and to protect access over the network using the virtual lines.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	To configure the enable password to access privileged EXEC mode, enter the global configuration mode by issuing the **configure terminal** command.
2.	From the Switch(config)# prompt, enter **enable password cisco**.
3.	Set the enable secret privileged EXEC mode password to “sanfran” using the command **enable secret sanfran**.
4.	Enter line configuration mode for the console line using the **line console 0** command.
5.	Set the line console password to “cisco” using the **password cisco** command.
6.	To enable password checking on the console port, enter the **login** command.
7.	Enter the **exit** command to return to global configuration mode.
8.	Enter line configuration mode for the vty ports using the **line vty 0 15** command.
9.	Set the vty password to “sanjose” using the **password sanjose** command.
10.	Enter the **end** command to return to the privileged EXEC mode.

Activity Verification

You have completed this task when you attain these results:

- You configured the enable secret and enable passwords on the switch.
- You configured the console and virtual terminal passwords on the switch.

Task 5: Save and Display Switch Configuration

In this task, you will save the configuration that currently resides in running memory into NVRAM. In this way, the configuration will be available after the switch is restarted or is powered off and then on again.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See

1.	Enter **copy run** and press the **Tab** key. You should see the complete command filled in to read “copy running-config.” Enter a question mark (**?**) to see your options.	wg_sw_z#**copy run**
		wg_sw_z#**copy running-config ?**
		  flash: Copy to flash: file system
		  ftp: Copy to ftp: file system
		  null: Copy to null: file system
		  nvram: Copy to nvram: file system
		  rcp: Copy to rcp: file system
		  running-config Update (merge with) current
		  system configuration
		  startup-config Copy to startup configuration
		  system: Copy to system: file system
		  tftp: Copy to tftp: file system
		
		wg_sw_z#**copy running-config** _ (cursor remains
		  on this line)

2.	At the cursor, enter **st** and press the **Tab** key. The command changes to **copy running-config startup-config**. Press **Enter**, and the prompt appears.	Destination filename [startup-config]?
3.	Press **Return** to save the current running configuration to the startup configuration in NVRAM.	

Step	Action	What You See
4.	To view the running configuration, enter **show running-config**. Your output should look similar to the example, keeping in mind that each pod has a unique IP address.	wg_sw_z#**show running-config** Building configuration... Current configuration: ! version 12.1 no service pad service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname wg_sw_z ! enable secret 5 1r7f9$IuDPMp8kGFa3bKtaiEhV91 enable password cisco ! ip subnet-zero ! interface FastEthernet0/1 interface FastEthernet0/2 interface FastEthernet0/3 interface FastEthernet0/4 interface FastEthernet0/5 interface FastEthernet0/6 interface FastEthernet0/7 interface FastEthernet0/8 interface FastEthernet0/9 interface FastEthernet0/10 interface FastEthernet0/11 interface FastEthernet0/12 interface FastEthernet0/13 interface FastEthernet0/14 interface FastEthernet0/15 interface FastEthernet0/16 interface FastEthernet0/17 interface FastEthernet0/18 interface FastEthernet0/19 interface FastEthernet0/20 interface FastEthernet0/21 interface FastEthernet0/22 interface FastEthernet0/23 interface FastEthernet0/24 interface VLAN1 ip address 10.1.1.130 255.255.255.0 no ip route-cache ip default-gateway 10.1.1.3 ip http server ! line con 0 password cisco login line vty 0 4 password sanjose login line vty 5 15 login ! end wg_sw_z#
5.	Notify your instructor that you have completed the lab activity.	

Activity Verification

You have completed this task when you attain this result:

- You verified your configuration and saved it to NVRAM.

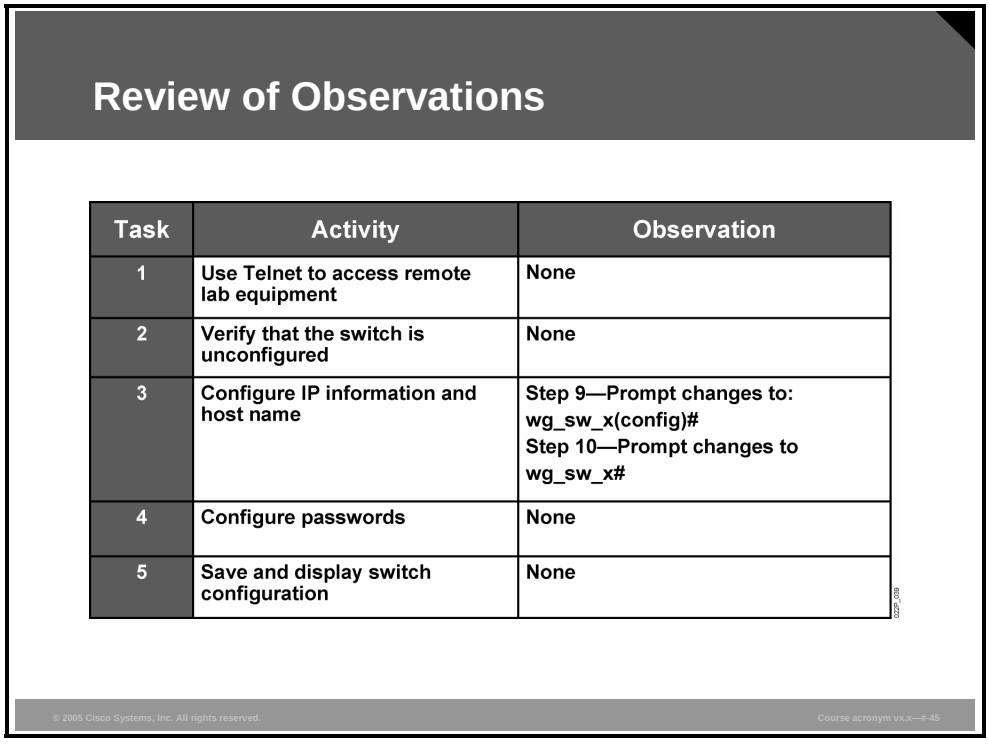
Note	In field implementations, the switch must have an IP address before you can use the network or web-based means to manage it.

Lab 8-2: Debrief

This debriefing session covers the activities in the “Switch Startup and Initial Configuration” lab. The topics addressed include a review of the correct steps for starting and configuring the switch and a review of tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of starting and configuring the switch lab.

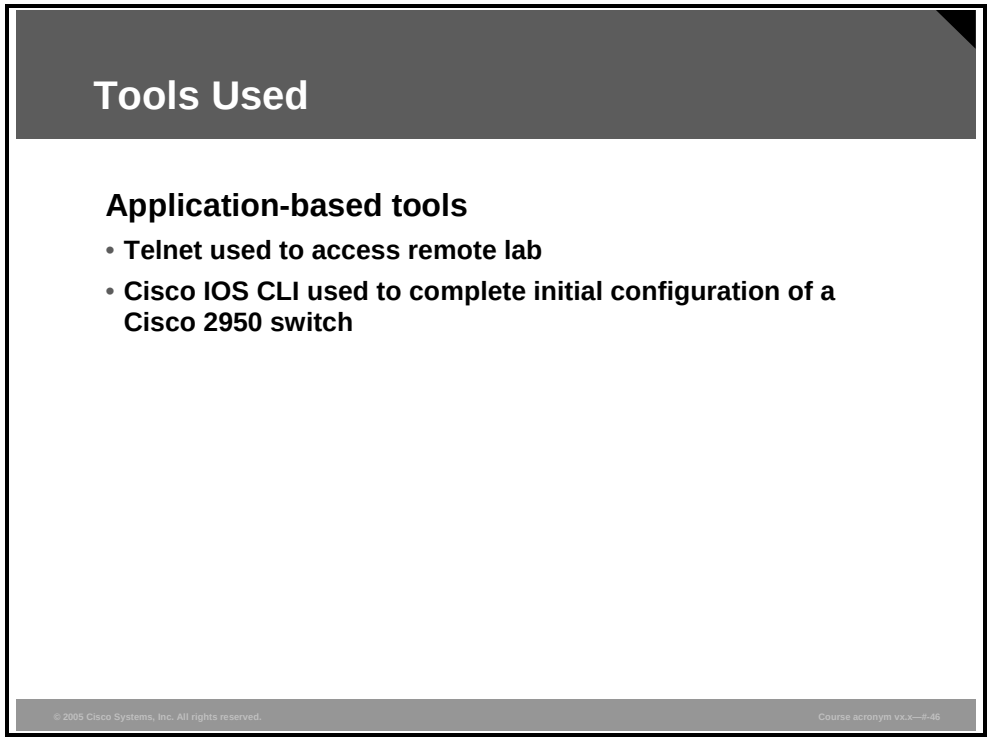


The figure shows the observations that you should have made during the lab, as follows:

- **Task 3, Step 9:** You should have seen that the prompt changed immediately after the **hostname** command was entered.
- **Task 3, Step 10:** You should have seen that the prompt changed on leaving configuration mode.

Tools

In this lab, a number of tools were used.



- **Telnet:** This IP application was used as a tool to provide access to the remote terminal server, which allows connection to the switches and routers that form the lab.
- **Cisco IOS software:** The Cisco IOS CLI comprises many commands that are used as tools to configure, test, and maintain Cisco routers and switches.

Lab 8-3: Completing Router Startup and Initial Configuration

Complete this lab activity to practice what you learned in the related module.

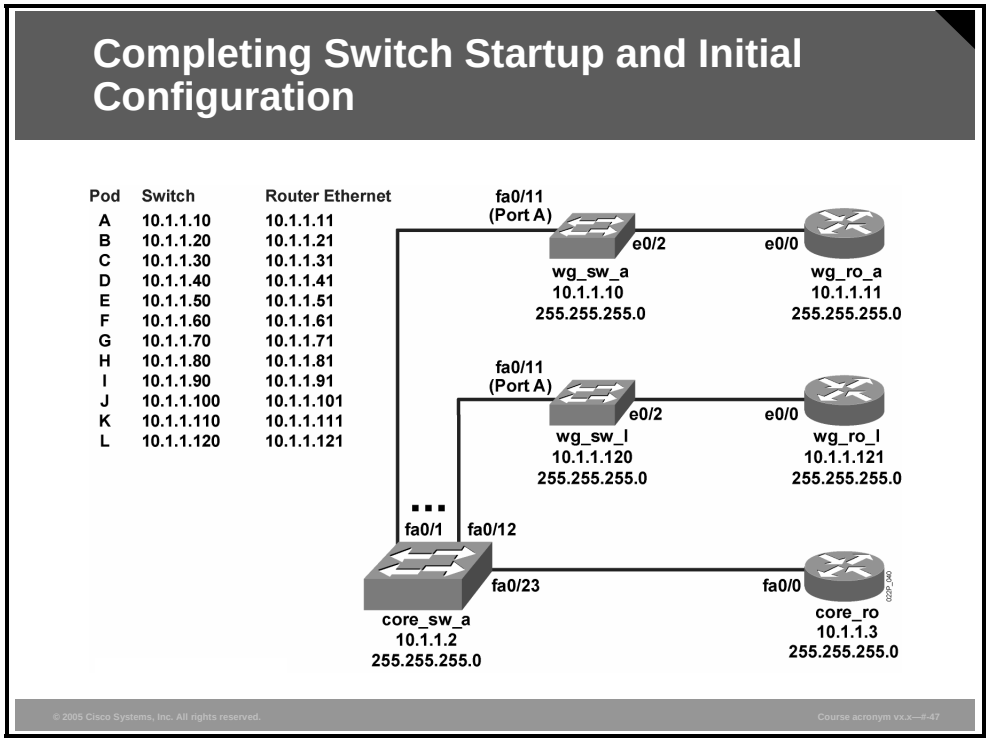
Activity Objective

In this activity, you will connect to the router, verify connectivity, examine the startup process, and perform a minimal configuration. After completing this activity, you will be able to meet these objectives:

- Start the router and verify the startup messages
- Use setup to configure the minimum parameters for router operation

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- PC connected to an onsite lab or a PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device (if you are using a remote lab)
- INTRO pod assigned by your instructor

Command List

The table describes the commands used in this activity.

Command	Description
enable	Enters the privileged EXEC mode command interpreter
erase startup-config	Erases the startup configuration from memory
reload	Reboots the router to make your changes take effect

Job Aids

There are no job aids for this lab activity.

Activity Preparation

Your instructor will assign you to a pod, identified by the letters A through L. The table identifies the router IP address, host name, subnet mask, and bits of subnetting in the subnet mask for each pod. You will need this information to complete the lab activity.

Pod	Router First Ethernet IP Address	Router Host Name	Subnet Mask	Bits of Subnetting in Subnet Mask
Pod A	10.1.1.11	wg_ro_a	255.255.255.0	16
Pod B	10.1.1.21	wg_ro_b	255.255.255.0	16
Pod C	10.1.1.31	wg_ro_c	255.255.255.0	16
Pod D	10.1.1.41	wg_ro_d	255.255.255.0	16
Pod E	10.1.1.51	wg_ro_e	255.255.255.0	16
Pod F	10.1.1.61	wg_ro_f	255.255.255.0	16
Pod G	10.1.1.71	wg_ro_g	255.255.255.0	16
Pod H	10.1.1.81	wg_ro_h	255.255.255.0	16
Pod I	10.1.1.91	wg_ro_i	255.255.255.0	16
Pod J	10.1.1.101	wg_ro_j	255.255.255.0	16
Pod K	10.1.1.111	wg_ro_k	255.255.255.0	16
Pod L	10.1.1.121	wg_ro_l	255.255.255.0	16

Task 1: Connect to Your Workgroup Router

In this task, you will start the workgroup router and verify that the router starts correctly.

Note	The steps in this activity indicate the prompts and output that most routers display. However, different routers with different interfaces may display somewhat different prompts during the setup mode. As you complete this lab activity, take extra care to ensure that you configure the router correctly for your environment. Ask your instructor if you have questions about how to configure any router feature.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Use Telnet to access the terminal server for the lab exercises. You should see a menu that is similar to the example.	```********** ********** CISCO ICND STUDENT MENU CONNECT TO YOUR POD LETTER ********** ********** ITEM# DEVICE NAME ---------- ---------- 1 Connect to pod A 2 Connect to pod B 3 Connect to pod C 4 Connect to pod D 5 Connect to pod E 6 Connect to pod F 7 Connect to pod G 8 Connect to pod H 9 Connect to pod I 10 Connect to pod J 11 Connect to pod K 12 Connect to pod L 13 EXIT Please enter selection:```
2.	At the “Please enter selection” prompt, choose your workgroup and press **Return**. Your output should look similar to the example. The menu, called the pod menu, lists your pod letter at the top. In the example, the current pod is Pod L.	```********** ********** POD L To exit back out to the menu press "CTRL+SHIFT+6" then "X". You must clear the line before re-connecting to a device. ********** ********** 1 Connect to workgroup switch L 2 Connect to workgroup router L 3 Clear connection to w/g switch L 4 Clear connection to w/g router L 5 Return to main menu Please enter selection:```

Step	Action	What You See

3.	Enter option **2** and press **Return** to connect to your workgroup router. When the router starts, your output should look similar to the example.	`Please enter selection: 2`
		`Trying h27 (10.10.10.10, 2059)... Open`
		
		`% Please answer 'yes' or 'no'.`
		`Would you like to enter the initial configuration dialog? [yes/no]:`

Activity Verification

You have completed this task when you attain this result:

- The router initial configuration messages are displayed on your console.

Task 2: Verify That the Router Is Unconfigured

In this task, you will ensure that the router has no configuration by erasing the startup configuration and reloading the router operating system.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	At the “Would you like to enter the initial configuration dialog?” prompt, enter **no** and press **Return**. The following prompt may appear (depending on your router): “Would you like to terminate autoinstall? [yes].”	
2.	Enter **yes**. The following prompt appears: “Press Return to get started!”	

Step	Action	What You See
3.	Press **Return** to begin the router initialization. Your output should look similar to the example.	00:00:17: %LINK-3-UPDOWN: Interface BRI0/0, changed state to up 00:00:17: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up 00:00:17: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down 00:00:17: %LINK-3-UPDOWN: Interface Serial0/1, changed state to down 00:00:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0, changed state to down 00:00:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up 00:00:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, Router>changed state to down 00:00:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1, changed state to down 00:05:48: %LINK-5-CHANGED: Interface BRI0/0, changed state to administratively down 00:05:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:1, changed state to down 00:05:49: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0:2, changed state to down 00:05:50: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down 00:05:50: %LINK-5-CHANGED: Interface Serial0/0, changed state to administratively down 00:05:50: %LINK-5-CHANGED: Interface Serial0/1, changed state to administratively down 00:05:51: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to down 00:05:53: %IP-5-WEBINST_KILL: Terminating DNS process 00:05:53: %SYS-5-RESTART: System restarted -- Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-JS-M), Version 12.0(8), RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems, Inc. Compiled Mon 29-Nov-99 15:26 by kpma
4.	Press **Return** to force the router to issue a prompt. You should see the Router> prompt.	Router>
5.	Check the output to answer the following question. Which Cisco IOS software version is running on your router? (Enter your answer in the space provided.)	
6.	At the Router> prompt, enter the **enable** command to begin privileged EXEC mode. Your prompt should change to Router#.	
7.	To erase the startup configuration from NVRAM, enter the **erase startup-config** command. You should see a warning notice similar to this example.	Router#**erase startup-config** Erasing the nvram filesystem will remove all files! Continue? [confirm]

Step	Action	What You See
8.	Press **Return** to confirm that you want to erase the startup configuration from NVRAM. A message appears.	`[OK]` `Erase of nvram: complete`

Step	Action	What You See
9.	Enter the **reload** command to reload the router. You should confirm by entering **y**. You should see output similar to the example (depending on your router) as the router reloads. What interfaces are available on your router? (Enter your answer in the space provided.)	Router#**reload** Proceed with reload? [confirm]y 00:25:01: %SYS-5-RELOAD: Reload requested System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1) Copyright © 1999 by cisco Systems, Inc. TAC:Home:SW:IOS:Specials for info C2600 platform with 65536 Kbytes of main memory program load complete, entry point: 0x80008000, size: 0x5fb4cc Self decompressing the image : ## #### [OK] Restricted Rights Legend Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph © of the Commercial Computer Software – Restricted Rights clause at FAR sec. 52.227-19 and subparagraph © (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013. Cisco Systems, Inc. 170 West Tasman Drive San Jose, California 95134-1706 Cisco Internetwork Operating System Software IOS © C2600 Software (C2600-JS-M), Version 12.0(8), RELEASE SOFTWARE (fc1) Copyright © 1986-1999 by cisco Systems, Inc. Compiled Mon 29-Nov-99 15:26 by kpma Image text-base: 0x80008088, data-base: 0x80B081E0 cisco 2610 (MPC860) processor (revision 0x300) with 53248K/12288K bytes of memory. Processor board ID JAD06090BMD (2719249260) M860 processor: part number 0, mask 49 Bridging software. X.25 software, Version 3.0.0. SuperLAT software (copyright 1990 by Meridian Technology Corp). TN3270 Emulation software. Basic Rate ISDN software, Version 1.1. 1 Ethernet/IEEE 802.3 interface(s) 2 Serial(sync/async) network interface(s) 1 ISDN Basic Rate interface(s) 32K bytes of non-volatile configuration memory. 16384K bytes of processor board System flash (Read/Write) --- System Configuration Dialog ---

Step	Action	What You See
		`Would you like to enter the initial configuration dialog? [yes/no]:`

Activity Verification

You have completed this task when you attain this result:

- You accurately entered the passwords, host name, and Ethernet IP address.

Task 3: Use Initial Configuration Dialog

In this task, you will ensure that the router has no configuration by erasing the startup configuration and reloading the router operating system.

Activity Procedure

Complete these steps.

Step	Action	What You See
1.	At the "Would you like to enter the initial configuration dialog?" prompt, enter **yes**. A prompt similar to the example appears.	`Would you like to enter basic management setup? [yes/no]:`
2.	At the "Would you like to enter basic management setup?" prompt, enter **no**. A prompt similar to the example appears:	`First, would you like to see the current interface summary? [yes]:`

3.	To review the interfaces on your router, enter **yes**. Your output should look similar to the example.	`Any interface listed with OK? value "NO" does not have a valid configuration`
		
		`Interface IP-Address OK? Method Status Protocol`
		`Ethernet0/0 unassigned NO unset up up`
		`Serial0/0 unassigned NO unset down down`
		`BRI0/0 unassigned NO unset up down`
		`BRI0/0:1 unassigned YES unset down down`
		`BRI0/0:2 unassigned YES unset down down`
		`Serial0/1 unassigned NO unset down down`
		
		`Configuring global parameters:`
		
		`Enter host name [Router]:`

4.	At the "Enter host name" prompt, enter **wg_ro_*x***, where "x" is the pod letter assigned to you for this lab activity. Your output should look similar to the example.	`The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.` `Enter enable secret:`

Step	Action	What You See
5.	Enter **sanfran** as the enable secret password. The password is case-sensitive, so enter it exactly as given. Your output should look similar to the example.	`The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.` `Enter enable password:`
6.	Enter **cisco** as the enable password provided. The password is case-sensitive, so enter it exactly as given. Your output should look similar to the example.	`The virtual terminal password is used to protect access to the router over a network interface.` `Enter virtual terminal password:`
7.	Enter **sanjose** as the password used to access virtual terminal services, such as when you Telnet into the router. The password is case-sensitive, so enter it exactly as given.	
8.	At the "Configure SNMP Network Management?" prompt, enter **no** because you will not work with SNMP network management in this course.	`Configure SNMP Network Management? no`

9.	Enter **no** at the "Configure LAT?," "Configure AppleTalk?," and "Configure DECnet?" prompts. At the "Configure IP?" prompt, enter **yes**.	`Configure LAT? [yes]: no`
		`Configure AppleTalk? [no]: no`
		`Configure DECnet? [no]: no`
		`Configure IP? [yes]: yes`

10.	Enter **no** at the "Configure IGRP routing?" and "Configure RIP routing?" prompts as shown in the example.	`Configure IGRP routing? [yes]: no` `Configure RIP routing? [no]: no`

11.	You will then see several questions. Enter **no** at each prompt. This series of questions concludes the Layer 3 protocol prompts.	`Configure CLNS? [no]:`
		`Configure bridging? [no]:`
		`Configure IPX? [no]:`
		`Configure Vines? [no]:`
		`Configure XNS? [no]:`
		`Configure Apollo? [no]:`

12.	Next, the router prompts you to configure several Layer 1 and Layer 2 protocols. Your output should look similar to the example.	`BRI interface needs isdn switch-type to be configured`
		`Valid switch types are :`
		`[0] none.....Only if you don't want to configure BRI.`
		`[1] basic-1tr6....1TR6 switch type for Germany`
		`[2] basic-5ess....AT&T 5ESS switch type for the US/Canada`
		`[3] basic-dms100..Northern DMS-100 switch type for US/Canada`
		`[4] basic-net3....NET3 switch type for UK and Europe`
		`[5] basic-ni......National ISDN switch type`
		`[6] basic-ts013...TS013 switch type for Australia`
		`[7] ntt.....NTT switch type for Japan`
		`[8] vn3.....VN3 and VN4 switch types for France`
		`Choose ISDN BRI Switch Type [2]:`

13.	Enter **2** to choose the basic-5ess switch type. Your output should look similar to the example.	`Async lines accept incoming modems calls. If you will have`
		`users dialing in via modems, configure these lines.`
		`Configure Async lines? [yes]:`

Step	Action	What You See
14.	At the “Configure Async lines? [yes]” prompt, enter **no** because you will not configure asynchronous lines now. Next, you are prompted to enter configuration information for the interfaces on the router. Each router will list the interfaces as discovered on that particular device. The prompt shown in the example appears.	`Do you want to configure Ethernet0/0 interface? [yes]:`
15.	Enter **yes** to configure the Ethernet0/0 interface. The prompt shown in the example appears.	`Configure IP on this interface? [yes]:`

16.	Enter **yes** to configure IP on the interface. See the table in the Activity Preparation section of this lab activity to determine the IP address for your assigned pod. Your output should look similar to the example.	`IP address for this interface:` **`10.1.1.131`**
		`Subnet mask for this interface [255.0.0.0] :` **`255.255.255.0`**
		`Class A network is 10.0.0.0, 24 subnet bits; mask is /24`
		`Do you want to configure Serial0/0 interface?`

17.	Enter **no** to the “Do you want to configure Serial0/0 interface?” prompt. The prompt shown in the example appears.	`Do you want to configure BRI0/0 (BRI d-channel) interface? :`
18.	Enter **no**. The prompt shown in the example appears.	`Do you want to configure Serial0/1 interface? :`

Step	Action	What You See
19.	Enter **no**. The line indicating that a script was created is the first indication that you have successfully completed configuring this router. Your output should look similar to the example.	The following configuration command script was created: hostname wg_ro_z enable secret 5 1yJLB$MsUC7/JlfVxSt1Wj0gwp.1 enable password cisco line vty 0 4 password sanjose no snmp-server ! no appletalk routing no decnet routing ip routing no clns routing no bridge 1 no ipx routing no vines routing no xns routing no apollo routing isdn switch-type basic-5ess ! interface Ethernet0/0 ip address 10.1.1.131 255.255.255.0 no mop enabled ! interface Serial0/0 shutdown no ip address ! interface BRI0/0 shutdown no ip address ! interface Serial0/1 shutdown no ip address dialer-list 1 protocol ip permit dialer-list 1 protocol ipx permit ! end [0] Go to the IOS command prompt without saving this config. [1] Return back to the setup without saving this config. [2] Save this configuration to nvram and exit. Enter your selection [2]:

Step	Action	What You See
20.	When the router displays the results of your initial configuration inputs, check that these parameters are correct. Then enter **2** to save this configuration to NVRAM. Your output should look similar to the example.	00:00:17: %LINK-3-UPDOWN: Interface BRI0/0, changed state to up 00:00:17: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up 00:00:17: %LINK-3-UPDOWN: Interface Serial0/0, changed state to down 00:00:17: %LINK-3-UPDOWN: Interface Serial0/1, changed state to up 00:00:18: %LINEPROTO-5-UPDOWN: Line protocol on Interface BRI0/0, changed state to down --- output omitted --- 00:13:18: %IP-5-WEBINST_KILL: Terminating DNS process 00:13:23: %SYS-5-RESTART: System restarted -- Cisco Internetwork Operating System Software IOS (tm) C2600 Software (C2600-JS-M), Version 12.0(8), RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems, Inc. Compiled Mon 29-Nov-99 15:26 by kpma
21.	Press **Return** to get the prompt. You should see wg_ro_x as the prompt, where “x” is the letter of your pod.	
22.	Press **Ctrl-Shift-6**, then **x**, to return to the pod menu.	********** CISCO ICND STUDENT MENU CONNECT TO YOUR POD LETTER ********** ITEM# DEVICE NAME 1 Connect to pod A 2 Connect to pod B 3 Connect to pod C 4 Connect to pod D 5 Connect to pod E 6 Connect to pod F 7 Connect to pod G 8 Connect to pod H 9 Connect to pod I 10 Connect to pod J 11 Connect to pod K 12 Connect to pod L 13 EXIT Please enter selection:
23.	Enter **5** and press **Return** to choose the option to return to the main menu.	
24.	Enter **exit** and press **Return** to terminate your Telnet session.	
25.	Notify your instructor that you have completed the task.	

Activity Verification

You have completed this task when you attain these results:

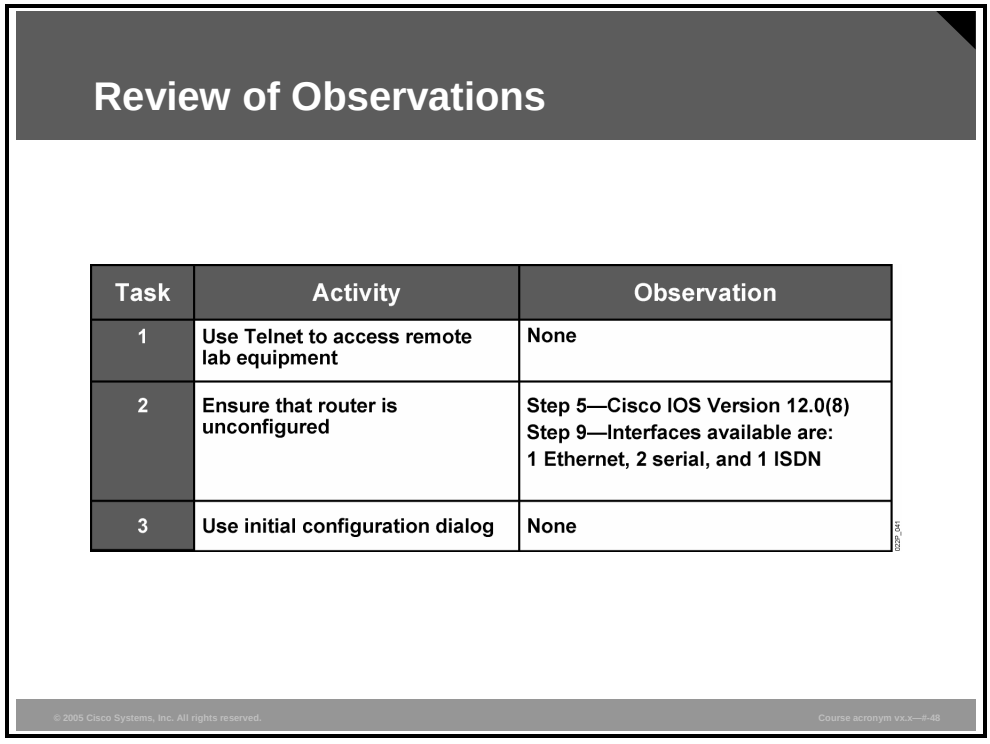
- You configured the router not to use SNMP.
- You selected IP as the routed protocol with no routing protocols.
- You configured the switch type for your BRI connection.
- You configured the first Ethernet interface as the sole interface with IP enabled.

Lab 8-3: Debrief

This debriefing session covers the activities included in the “Cisco Router Startup and Initial Configuration” lab. The topics addressed include a review of the correct steps for starting and configuring the router and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of starting and configuring the router lab.



The figure shows the observations that you should have made during the lab, as follows:

- **Task 2, Step 5** The initial output showed the Cisco IOS version:

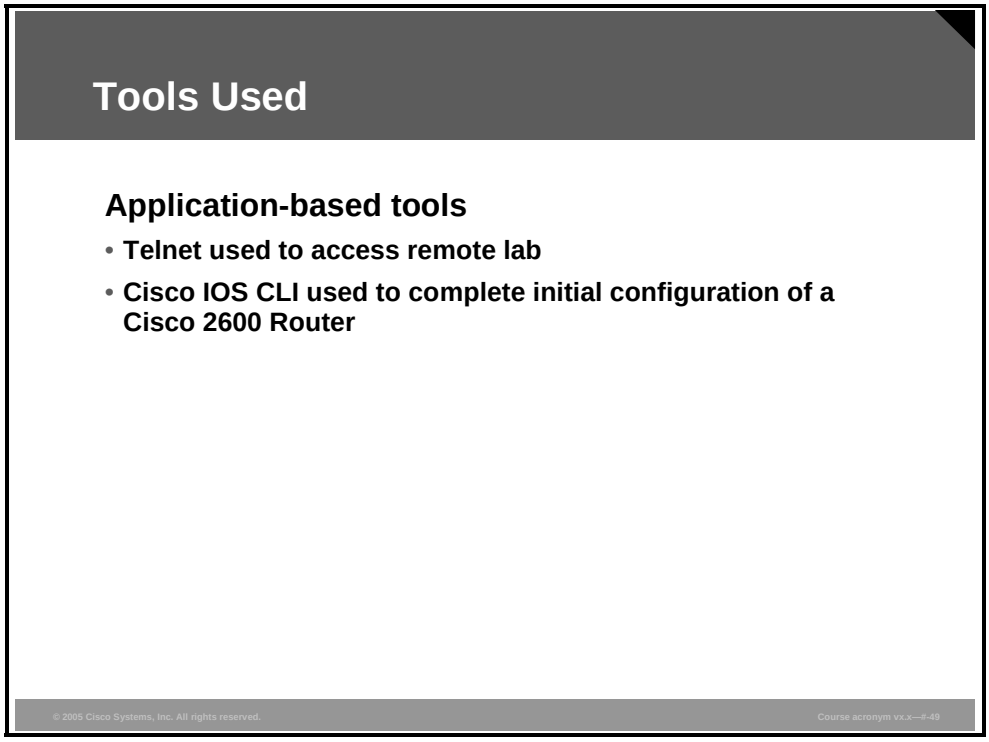
```
-- text omitted --

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JS-M), Version 12.0(8), RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
-- text omitted --
```

- **Task 2, Step 9:** The output following the **reload** command listed the interfaces that were discovered during the startup process:

```
-- text omitted --

1 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
-- text omitted --
```

Tools

In this lab, a number of tools were used.



- **Telnet:** This IP application was used as a tool to provide access to the remote terminal server, which allows connection to the switches and routers that form the lab.
- **Cisco IOS software:** The Cisco IOS operating system CLI comprises many commands that are used as tools to configure, test, and maintain Cisco routers and switches.

Lab 8-4: Using the Router CLI

Complete this lab activity to practice what you learned in the related module.

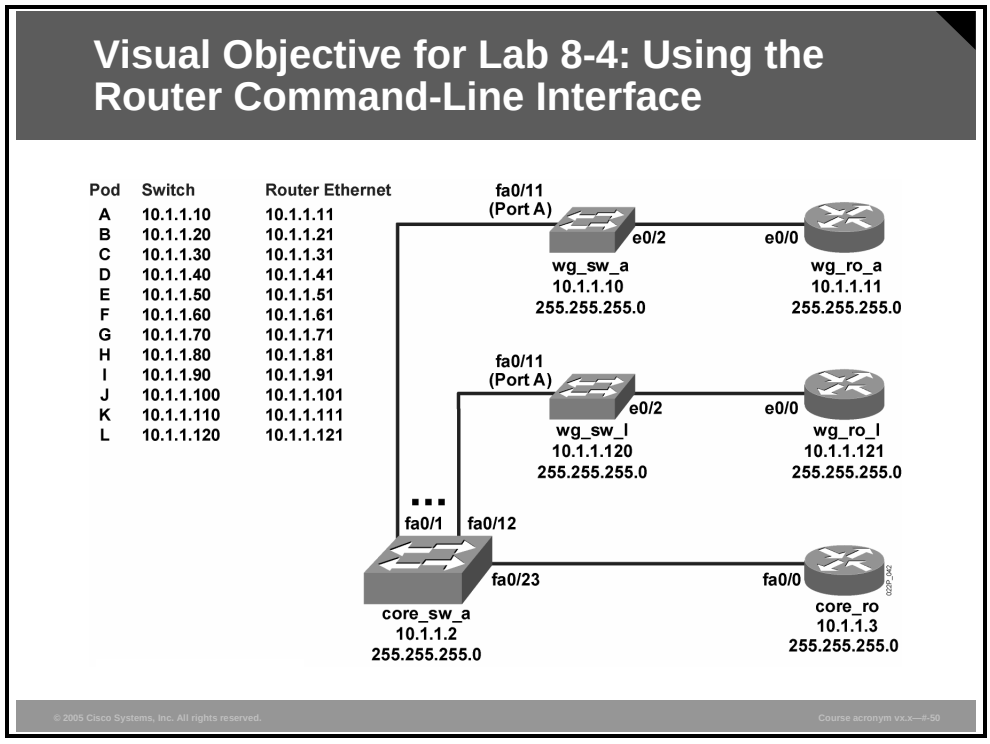
Activity Objective

In this activity, you will demonstrate and practice the use of CLI features. After completing this activity, you will be able to meet these objectives:

- Explore context-sensitive help on a Cisco router
- Edit incorrect commands in the router CLI
- Examine the router status using **show** commands

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- PC connected to an onsite lab or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device (if you are using a remote lab)
- INTRO pod assigned by your instructor

Command List

The table describes the commands used in this activity.

Command	Description
? or **help**	In user mode, Cisco IOS software lists a subset of the available commands. After you enter **enable** and enter your enable password for privileged mode, a much larger list of available commands is displayed.
clock	Manages the system clock.
enable	Activates privileged mode. In privileged mode, more commands are available. This command requires you to enter the enable password if an enable password is configured. If an enable secret password is also configured, the enable secret password overrides the enable password.
show clock	Displays the system clock.
show history	Displays recently entered commands.
show interfaces	Displays information on all of the router interfaces.
show running-config	Displays the active configuration.
show terminal	Displays the current settings for the terminal.
show version	Displays the configuration of the router hardware and the various software versions.
terminal history size	Sets the command history buffer size.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

In previous lab activities, you learned how to access your lab equipment for this class. You should have experience with Telnet on your PC and connecting to the terminal server. The terminal server menus should be familiar, and you should be able to access the terminal server and connect to either the switch or the router. You should also have set up the basic configuration for your router. You selected IP as the routing protocol to use. The only interface that you have configured with IP is your first Ethernet interface.

Task 1: Explore Context-Sensitive Help

In this task, you will use context-sensitive help in both user and privileged EXEC modes to locate commands and complete command syntax.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	From your PC, open a Telnet session to the terminal server. The main menu appears.	
2.	Choose your workgroup from the main menu. The pod menu appears.	
3.	Choose your workgroup router from the pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating that it is opening the session to your console.	
4.	Enter the help command (**?**) at the user EXEC prompt. Press **Return**. What happened? (Enter your answer in the space provided.) Press the **space bar**. What happened? (Enter your answer in the space provided.)	
5.	Enter privileged mode using the command **enable**. (You will need to give a password when requested.) What prompt indicates that the router is in privileged mode? (Enter your answer in the space provided.)	
6.	Enter the help (**?**) command at the privileged EXEC mode prompt. Use help to determine the keyword command that manages the system clock. What keyword command manages the system clock? (Enter your answer in the space provided.)	
7.	Your console should be displaying a prompt of "--More--" as it waits for you to press a key before displaying more output. Enter **q**. What happened? (Enter your answer in the space provided.)	
8.	Enter the **clock ?** command. What is the system response? (Enter your answer in the space provided.)	

Step	Action	What You See

9.	Set the system clock to the current time and date. Remember to use context-sensitive help to guide you through the process.	wg_ro_z#**clock ?**
		  set Set the time and date
		wg_ro_z#**clock set ?**
		  hh:mm:ss Current Time
		
		wg_ro_z#**clock set 13:13:13 ?**
		  <1-31> Day of the month
		  MONTH Month of the year
		
		wg_ro_z#**clock set 13:13:13 3 may 2002**
		wg_ro_z#

10.	At the Router# prompt, enter **sh?**. What command was returned as a result of this action? (Enter your answer in the space provided.)	
11.	Press the **Tab** key. What happened? (Enter your answer in the space provided.)	
12.	On the same line, enter the help command (**?**). What happened? (Enter your answer in the space provided.)	
13.	Enter the **show clock** command. What is displayed on your terminal screen? (Enter your answer in the space provided.)	

Activity Verification

You have completed this task when you attain this result:

- You used the system help facility and the command-completion facility.

Task 2: Edit an Incorrect Command

In this task, you will use Cisco IOS software enhanced editing features to correct command-line errors.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Enter the following comment line at the prompt. Enter the comment *without* the exclamation point (!). An exclamation point (!) before the text line indicates that you are entering a comment. **This command changes the clock speed for the router.** Press **Return**. What happened? (Enter your answer in the space provided.)
2.	Enter the following comment line preceded by the exclamation point (!). **!ths comand changuw the clck sped for the rotter.** Press **Return**.
3.	Press **Ctrl-P** or the **Up Arrow** key. What happened? (Enter your answer in the space provided.)
4.	Complete the following editing commands: Press **Ctrl-A**. What happened? (Enter your answer in the space provided.) Press **Ctrl-F**. What happened? (Enter your answer in the space provided.) Press **Ctrl-E**. What happened? (Enter your answer in the space provided.) Press **Ctrl-B**. What happened? (Enter your answer in the space provided.)
5.	Using the editing commands, correct the comment line to read: **This command changes the clock speed for the router.**

Activity Verification

You have completed this task when you attain this result:

- You used the built-in editor and used those keystrokes for cursor navigation.

Task 3: Examine the Router Status

In this task, you will enter Cisco IOS software **show** commands to observe and verify the status of the router.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Enter the **show history** command. What happened? (Enter your answer in the space provided.) Press **Ctrl-P** several times. What happened? (Enter your answer in the space provided.) Now press **Ctrl-N**. What happened? (Enter your answer in the space provided.)
2.	Press **Return** to display a new prompt.
3.	Enter the **show version** command. Enter the values displayed for the following items: Cisco IOS software: _____ Cisco IOS software version: _____ System uptime: _____ System image file name: _____ Number of Ethernet interfaces: _____ Number of serial interfaces: _____ Number of ISDN BRI interfaces: _____ Amount of NVRAM: _____
4.	Enter the **show interfaces** command. What are the interface names, MTU, and bandwidth for your first Ethernet and first serial interfaces? **First Ethernet** Interface name: _____ MTU: _____ Bandwidth: _____ **First serial** Interface name: _____ MTU: _____ Bandwidth: _____

Step	Action
5.	Enter the **show running-config** command. What are the values for the following parameters when you enter the **show running-config** command? Version: _____ Host name: _____
6.	Return to the privileged EXEC mode prompt.
7.	Enter the help command (**?**). What command sets the terminal line parameters? (Enter your answer in the space provided.)
8.	Enter the command that sets the terminal line parameters, followed by the help command (**?**). What keyword enables and controls the command history function? (Enter your answer in the space provided.)
9.	Using the command and the keyword (from Steps 7 and 8), set the command history buffer size to 50 lines. Use context-sensitive help to guide you through the process.
10.	Enter the **show terminal** command to verify the history size.
11.	Enter the **exit** command at the privileged EXEC mode prompt. What happened? (Enter your answer in the space provided.)
12.	Enter **Ctrl-Shift-6**, then **x**, to suspend your session and return to the terminal server pod menu.
13.	Exit the terminal server by entering the appropriate menu options to exit first the pod menu, then the main menu. You should return to the operating system prompt in your command window after exiting the Telnet session.
14.	Notify your instructor that you have finished the lab activity.

Activity Verification

You have completed this task when you attain these results:

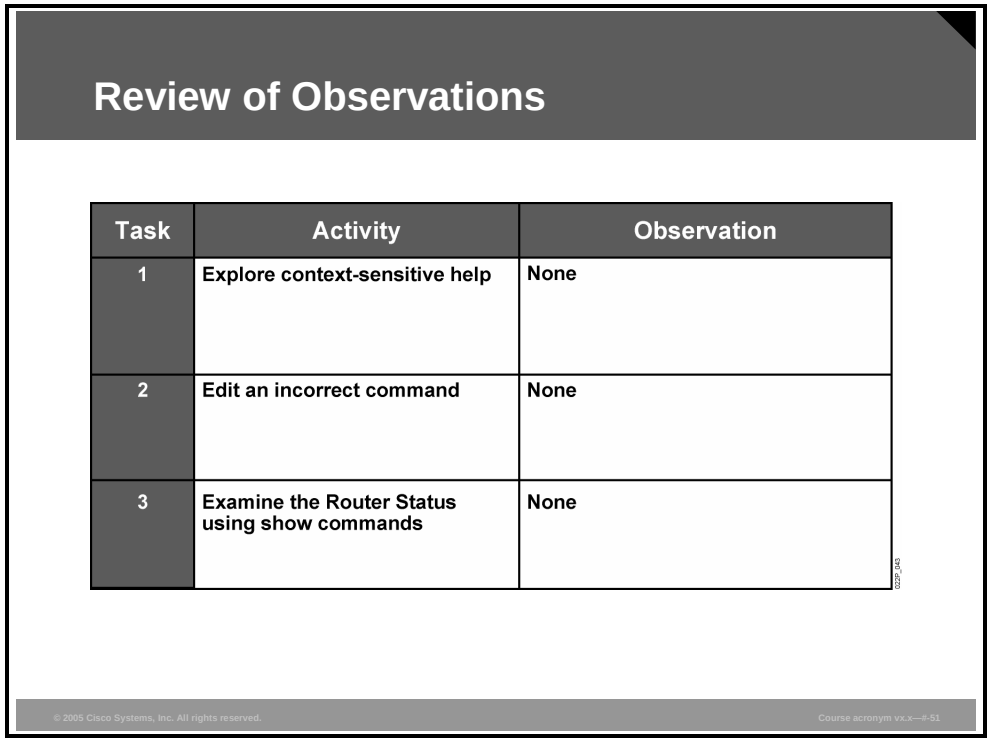
- You interpreted basic **show** commands and can determine the software version and hardware capabilities of a Cisco IOS platform.
- You selected IP as the routed protocol with no routing protocols.

Lab 8-4: Debrief

This debriefing session covers the activities in the “Using the Router Command-Line Interface” lab. The topics addressed include a review of the observations made during the lab and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of using the router command line interface.



The figure shows the observations that you should have made during the lab, as follows:

- **Task 1, Step 4:** The help facility displayed a list of commands available. If there was more output than the 23 lines of the screen could display, the screen paused while waiting for your input. You then pressed the Space Bar and the rest of the lines were displayed.
- **Task 1, Step 5:** The prompt changed from wg_ro_x> to wg_ro_x#.
- **Task 1, Step 6:** You used the **clock** command.
- **Task 1, Step 7:** When you entered **q**, you exited the “more” mode, bringing you back to the EXEC mode.
- **Task 1, Step 8:** The output should have been as follows:

```
wg_ro_x#clock ?
  set  Set the time and date
```

- **Task 1, Step 10:** The output should have been as follows:

```
wg_ro_x#sh?
show
```

- **Task 1, Step 11:** Pressing the **Tab** key caused "sh" to be completed as "show**."**
- **Task 1, Step 12:** The question mark (?) caused a list of possible command modifiers to be displayed:

```
wg_ro_x#show ?
access-expression  List access expression
access-lists       List access lists
accounting         Accounting data for active sessions
adjacency          Adjacent nodes
aliases            Display alias commands
alps               Alps information
-- text omitted --
```

- **Task 1, Step 13:** Your output should have resembled the following:

```
wg_ro_x#show clock
13:13:19.991 UTC Fri May 3 2002
```

- **Task 2, Step 1:** Your output should have resembled the following (the text was interpreted as a command and was rejected with a "^" symbol pointing to the first error found):

```
wg_ro_x#This command changes the clock speed for the router
      ^
      % Invalid input detected at '^' marker.
```

- **Task 2, Step 3:** Pressing **Ctrl-P** or the **Up Arrow** key caused the previous command to be recalled.
- **Task 2, Step 4:**

  Pressing **Ctrl-A** caused the cursor to go to the beginning of command line.

  Pressing **Ctrl-F** caused the cursor to advance one character on the command line.

  Pressing **Ctrl-E** caused the cursor to go to the end of command line.

  Pressing **Ctrl-B** caused the cursor to go back one character on the command line.

- **Task 3, Step 1:** The **show history** command displays the history buffer (10 lines by default).

  Pressing **Ctrl-P** scrolls up one line of the history buffer.

  Pressing **Ctrl-N** scrolls down one line of the history buffer.

- **Task 3, Step 3:** The following answers were found in the **show version** command output:

  Cisco IOS software: `IOS (tm) C2600 Software (C2600-JS-M)`

  Cisco IOS software version: `Version 12.0(8)`

  System uptime: `wg_ro_x uptime is 19 minutes`

  System image file name: `System image file is "flash:c2600-js-mz.120-8.bin"`

  Number of Ethernet interfaces: `1 Ethernet/IEEE 802.3 interface(s)`

  Number of serial interfaces: `2 Serial(sync/async) network interface(s)`

  Number of ISDN BRI interfaces: `1 ISDN Basic Rate interface(s)`

  Amount of NVRAM: `32K bytes of non-volatile configuration memory`

- **Task 3, Step 4:** The following answers were found in the **show interfaces** command output:

  `Ethernet0/0 is up, MTU 1500 bytes, BW 10000 Kbit`

  `Serial0/0, MTU 1500 bytes, BW 1544 Kbit`

- **Task 3, Step 5:** The following answers were found in the **show running-config** command output.

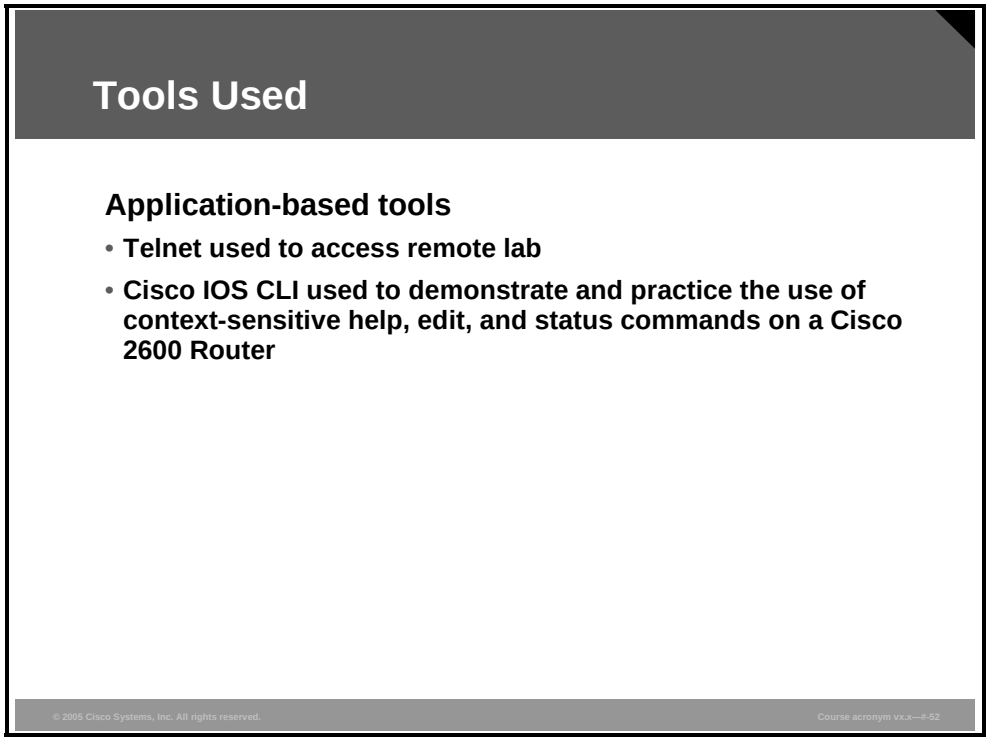
  Version:: `version 12.0`

  Host name:: `hostname wg_ro_x`

- **Task 3, Step 7:** The **terminal** command sets the terminal line parameters.
- **Task 3, Step 8:** The **terminal history** command sets the terminal line history parameters.
- **Task 3, Step 11:** When the **exit** command is used in EXEC mode, the session is terminated and the user has to log in again.

Tools

In this lab, a number of tools were used.



Lab 8-5: Operating and Configuring a Cisco IOS Device

Complete this lab activity to practice what you learned in the related module.

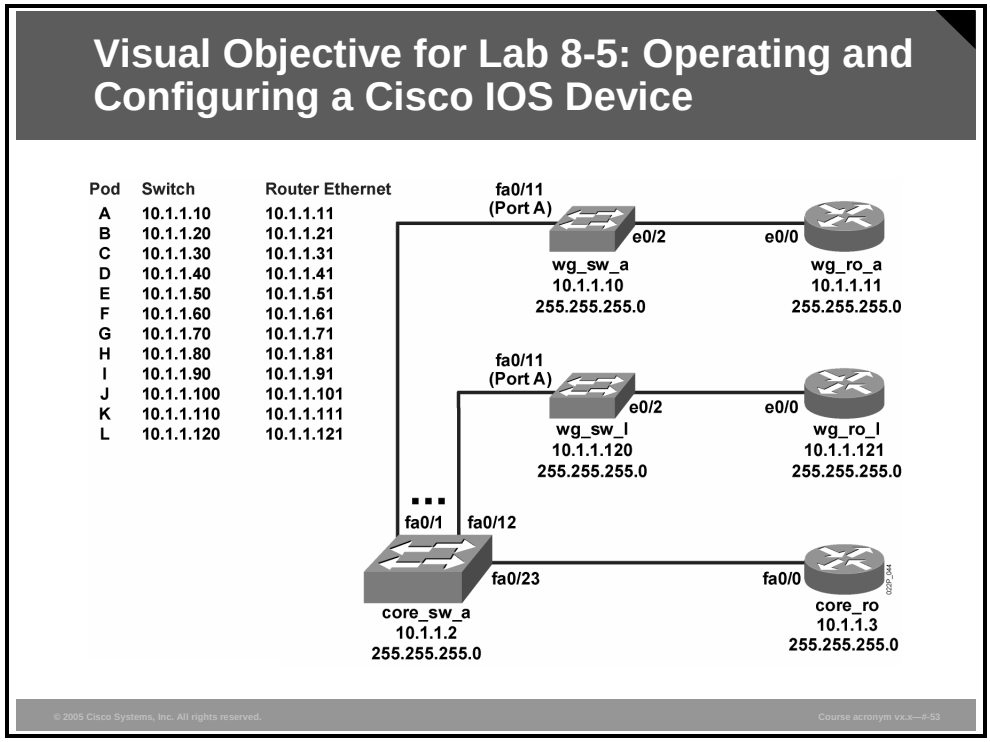
Activity Objective

In this activity, you will use basic Cisco IOS commands to check the basic capacity and configuration of your router and configure a serial interface on the routers. After completing this activity, you will be able to meet these objectives:

- Modify a running and startup router configuration
- Configure a serial interface on the workgroup router

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- PC connected to an onsite lab or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device (if you are using a remote lab)
- INTRO pod assigned by your instructor

Command List

The table describes the commands used in this activity.

Command	Description
? or **help**	In user mode, Cisco IOS software lists a subset of the available commands. After you enter **enable** and enter your enable password for privileged mode, you will see a much larger list of available commands.
bandwidth	Sets the bandwidth value for an interface.
banner motd	Configures the Message-of-the-Day banner.
configure terminal	From privileged EXEC mode, enters global configuration mode.
copy running-config startup-config	Saves the running configuration into NVRAM as the startup configuration.
description *description*	Helps you remember what is attached to this interface.
enable	Activates the privileged EXEC mode. In privileged EXEC mode, more commands are available. This command requires you to enter the enable password if an enable password is configured. If an enable secret password is also configured, the enable secret password overrides the enable password.
exec-timeout 0 0	Configures the console not to time out.
exit	Exits the current configuration mode.
interface *interface*	Specifies an interface and enters interface configuration mode.
line console 0	Specifies the console line and enters line configuration mode.
logging synchronous	Synchronizes unsolicited messages and debug output with solicited Cisco IOS software output.
login	Sets password checking at login.
shutdown/no shutdown	Disables or enables an interface.
password	Sets a password on a line.
quit	Exits the console session and logs out of the router.
show	Displays an aspect of router status or operation; use **show ?** for more information.
show controllers serial	Displays information that is specific to the interface hardware.
show interfaces	Displays information on all of the router interfaces.
show running-config	Displays the router configuration settings that are currently in effect.
show startup-config	Displays the configuration settings of the router NVRAM.
show version	Displays the configuration of the router hardware and the various software versions.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

In the previous lab activities, you learned how to access your lab equipment for this class. You should have experience with Telnet on your PC and should know how to connect to the terminal server. The terminal server menus should be familiar to you, and you should be able to access the terminal server and connect to either the switch or the router. You should also have performed the basic configuration of your router. The only interface you have configured with IP is your first Ethernet interface. You should be familiar with the system help facility, the command completion feature, and the general nature of the **show** commands.

Task 1: Modify a Running and Startup Router Configuration

In this task, you will use context-sensitive help in both user mode and privileged EXEC mode to locate commands and complete command syntax.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	From your PC, open a Telnet session to the terminal server. The main menu appears.
2.	Choose your workgroup from the main menu. The pod menu appears.
3.	Choose your workgroup router from the pod menu and press **Return**. Press **Return** to begin your router session after you receive the prompt from the terminal server indicating that it is opening the session to your console.
4.	Enter global configuration mode.
5.	Use the **configure terminal** command to specify that configuration commands will originate from the terminal.
6.	Using your help (**?**) command, locate the command that defines a banner. What command defines a Message-of-the-Day banner? (Enter your answer in the space provided.)
7.	Create a two- or three-line Message-of-the-Day banner. Use context-sensitive help to guide you through the process. What must you enter after the Message-of-the-Day banner command to indicate the end of the banner message? (Enter your answer in the space provided.)
8.	Enter interface configuration mode for your first serial interface using the **interface** command. What command string puts you in interface configuration mode for the first serial interface? (Enter your answer in the space provided.)
9.	Define an interface description for your first serial interface using the following command: **`description First serial interface configured as a DTE interface`**
10.	Return to the global configuration mode by entering the **exit** command.
11.	Enter interface configuration mode for your first Ethernet interface using the **interface** command.
12.	Define an interface description for your first Ethernet interface using the following command: **`description First Ethernet interface connects to your workgroup switch (wg_sw_x)`**

Step	Action
13.	Return to the global configuration mode by entering **exit**. If the router console port detects no activity for a specified time, the router will terminate the session automatically. You can disable the session termination feature by setting the timeout period to infinity; the default timeout is 10 minutes.
14.	Configure the console by entering the **line console 0** command.
15.	Disable the EXEC timeout by using the **exec-timeout 0 0** command. This action sets the EXEC timeout to 0 minutes and 0 seconds.
16.	Use the **login** and **password cisco** commands to require login at the console line and set the login password for the console line to **cisco.**
17.	Use the **logging synchronous** line configuration command to synchronize messages sent to the console display.
18.	Return to privileged EXEC mode.
19.	Enter the **show running-config** command to verify your new configuration.(Enter the new values in the spaces provided.) Description for your first serial interface: _____ Description for your first Ethernet interface: _____ MOTD banner: _____ EXEC timeout set for the console: _____ Console-line login password: _____ Logging command present? _____
20.	Enter the **show startup-config** command. Write the values in the space provided. Description for your first serial interface: _____ Description for your first Ethernet interface: _____ Message-of-the-Day banner: _____ EXEC timeout set for the console: _____ Console-line login password: _____ Logging command present? _____ The startup configuration should be different from the running configuration. Why? _____
21.	Enter the **copy running-config startup-config** command to copy the currently running configuration into NVRAM.
22.	Enter the **show startup-config** command.
23.	Exit the privileged EXEC mode using the **quit** command and log in again using the console password that you configured (**cisco**). Logging in requires the new password. You should also see the Message-of-the-Day banner.

Activity Verification

You have completed this task when you attain this result:

- You successfully configured the Message-of-the-Day banner, interface descriptions, bandwidth for the serial interface, line console EXEC timeout, the line console 0 password, and password for the virtual terminals.

Task 2: Configure a Serial Interface on the Workgroup Router

In this task, you will configure a serial interface on your workgroup router. When you finish, you will verify the configuration changes and save the parameters to the startup configuration file.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	At the privileged EXEC mode prompt, verify that your first serial interface is cabled as a DTE interface by using the **show controllers serial interface** command to choose your first serial interface. Your output should look similar to the example. Note that the third line in the display indicates the cable type. For an interface with a DCE cable attached, the display would begin "DCE V.35." Note: Your output may show either "TX and RX clocks detected" or "clocks stopped."	wg_sw_z#**show controllers serial 0/0** Interface Serial0/0 Hardware is PowerQUICC MPC860 **DTE V.35** TX and RX clocks detected. idb at 0x810B4ED0, driver data structure at 0x810BA3DC SCC Registers: General [GSMR]=0x2:0x00000000, Protocol-specific [PSMR]=0x8 Events [SCCE]=0x0000, Mask [SCCM]=0x0000, Status [SCCS]=0x03 Transmit on Demand [TODR]=0x0, Data Sync [DSR]=0x7E7E Interrupt Registers: Config [CICR]=0x00367F80, Pending [CIPR]=0x04000040 Mask [CIMR]=0x00200000, In-srv [CISR]=0x00000000 Command register [CR]=0x5C0 Port A [PADIR]=0x0030, [PAPAR]=0xFFFF [PAODR]=0x0010, [PADAT]=0x4BFF Port B [PBDIR]=0x09C0F, [PBPAR]=0x0600E [PBODR]=0x0000E, [PBDAT]=0x39FFD Port C [PCDIR]=0x00C, [PCPAR]=0x200 [PCSO]=0x820, [PCDAT]=0xDF0, [PCINT]=0x00F Receive Ring rmd(68012230): status 9000 length 60C address 34A6AA4 rmd(68012238): status 9000 length 60C address 3487384 rmd(68012240): status 9000 length 60C address 3487A04 rmd(68012248): status 9000 length 60C address 3488084 --More--
2.	Enter **q** at the "--More--" prompt to quit displaying the output of the **show controllers serial 0/0** command.	

Step	Action	What You See
3.	Enter interface configuration mode and configure your first serial interface. Set the bandwidth to 64 kbps. Refer to the command list for this lab activity for the correct command syntax. Do you need to set the clock rate to 64000 on your first serial interface? (Enter your answer in the space provided.)	
4.	Enter the command on your router to enable your first serial interface. Refer to the command list for this lab activity for the correct command syntax. What command do you use to enable the serial interface? (Enter your answer in the space provided.) In what mode must the router be before you can enter this command? (Enter your answer in the space provided.) What is the state of the interface after you enter this command? (Enter your answer in the space provided.) What is the protocol for the interface after you enter this command? (Enter your answer in the space provided.) What command would you use to determine the state of the interface, and what mode must you be in to enter that command? (Enter your answer in the space provided.) In a point-to-point configuration, what would happen if you enabled the first serial interface on your router but did not enable the directly connected interface on the corresponding router? (Enter your answer in the space provided.)	
5.	Enter the **copy running-config startup-config** command.	
6.	Notify your instructor that you have completed the lab activity.	

Activity Verification

You have completed this task when you attain these results:

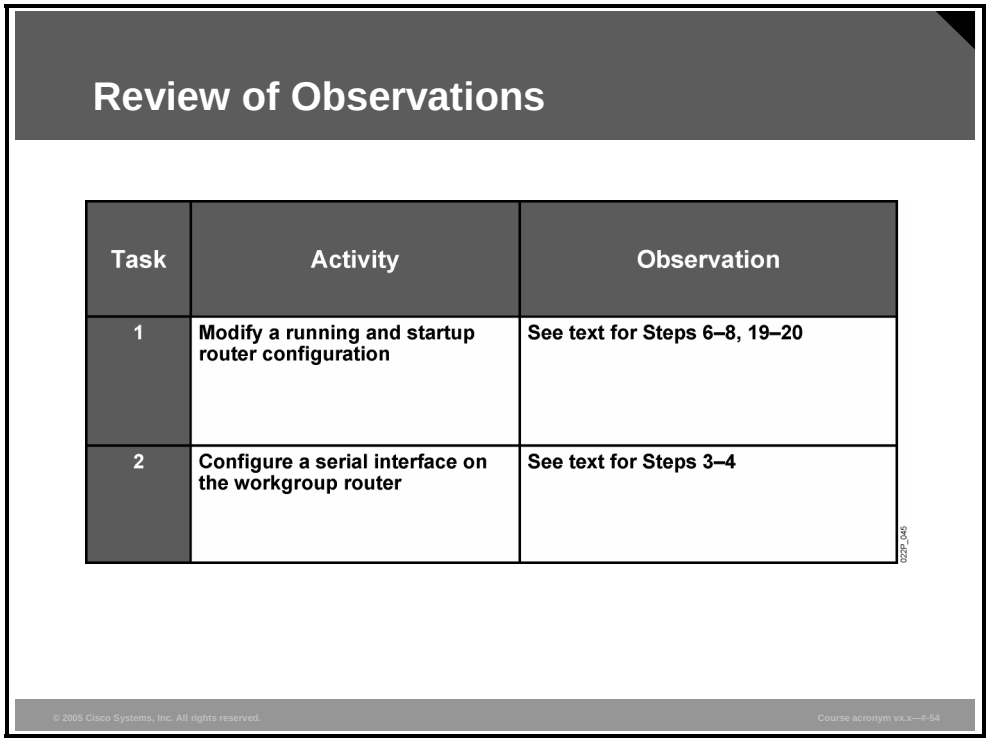
- You identified the difference between the running configuration and the startup configuration.
- You saved your running configuration to the startup configuration.
- You displayed the controller characteristics of your first serial interface and performed a basic configuration of a serial interface.

Lab 8-5: Debrief

This debriefing session covers the activities in the “Operating and Configuring a Cisco IOS Device” lab. The topics addressed include a review of the observations made during the lab and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of operating and configuring a Cisco IOS device.



The figure shows the observations that you should have made during the lab, as follows:

- **Task 1, Step 6:** The **banner motd** global configuration command defined a Message-of-the-Day banner.
- **Task 1, Step 7:** To terminate the Message-of-the-Day text, the same delimiter character must be entered that was used to start the text. If “#” was the start character, then it must be used as the ending delimiter.
- **Task 1, Step 8:** The **interface serial 0/0** global configuration command accesses interface configuration mode for the first serial interface.

- **Task 1, Step 19:** The answers were found in this **show running-config** command output:

  Description for your first serial interface:

  ```
  description First serial interface configured as a DTE interface
  ```

  Description for your first Ethernet interface:

  ```
  description First Ethernet interface connects to your workgroup
  switch (wg_sw_x)
  ```

  MOTD banner: `Yes`

  ```
  banner motd ^C
  **** Authorized Use Only *****
  ^C
  ```

  EXEC timeout set for the console: `exec-timeout 0 0`

  Console-line login password: `password cisco`

  Logging command present? `Yes : logging synchronous`

- **Task 1, Step 20:** The answers were found in the **show startup-config** command output.

  Description for your first serial interface: None

  Description for your first Ethernet interface: None

  MOTD banner: None

  EXEC timeout set for the console: `exec-timeout 0 0`

  Console-line login password: None

  Logging command present? No

- **Task 2, Step 3:** There is *no* need to enter clock rate on interface serial 0/0, because the cable connected to it is DTE mode (seen in the output of the **show controllers serial 0/0** command). Therefore, it receives the clock from the other end of the connection (DCE).

- **Task 2, Step 4:** The following are answers to the questions asked in this step (It was necessary to refer to the command list and to use the **show interface serial 0/0** command to answer some of the questions.):

  The command that you use to enable the serial interface is **no shutdown.**

  The router must be in interface configuration mode before you can enter this command.

  The state of the interface after you enter this command is up or down. The state depends also on the remote end of the connection.

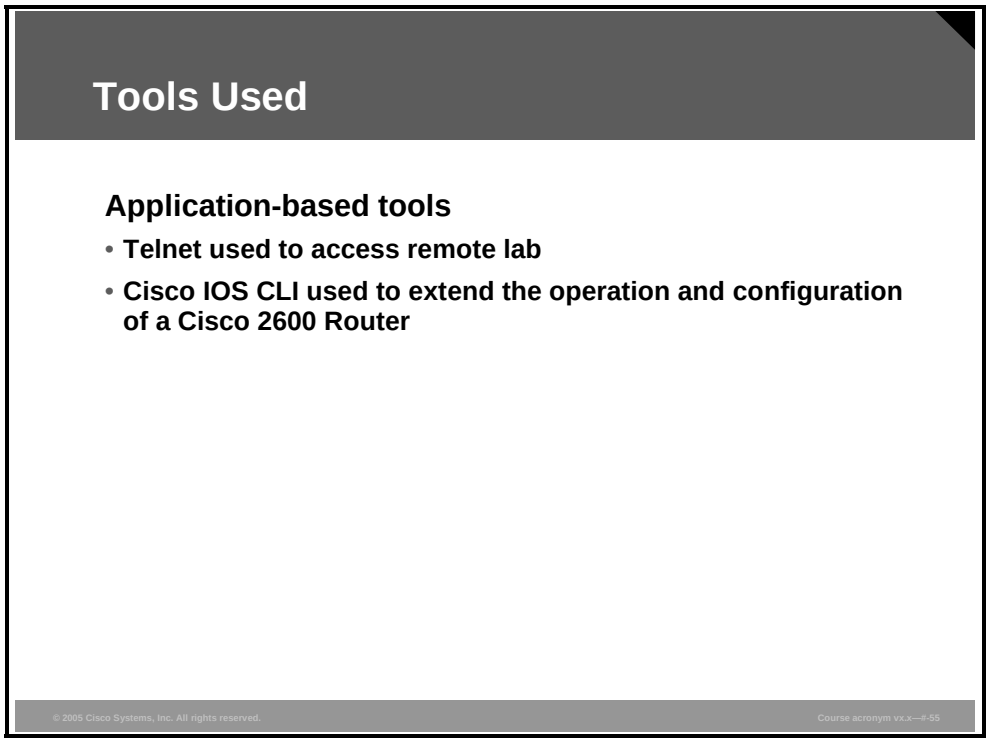
  The protocol for the interface after you enter this command is HDLC.

  The command that you would use to determine the state of the interface is **show interface serial 0/0**, and the mode that you must be in to enter that command is EXEC mode.

In a point-to-point configuration, if you enabled the first serial interface on your router but did not enable the directly connected interface on the corresponding router, the interface would be down because it would *not* be receiving clocking from the DCE end.

Tools

In this lab, a number of tools were used.



Lab 9-1: Gathering Information About Neighboring Devices and Using System Files

Complete this lab activity to practice what you learned in the related module.

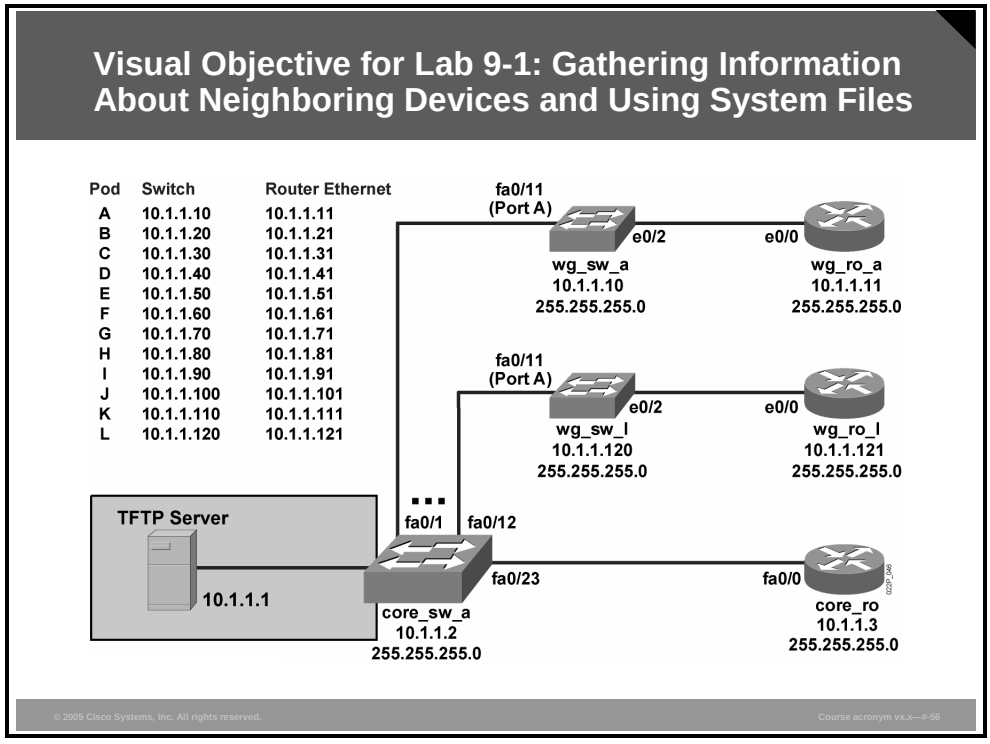
Activity Objective

In this activity, you will use CDP commands to discover information on the directly connected Cisco devices and use Telnet to access remote Cisco devices. After completing this activity, you will be able to meet these objectives:

- Use CDP to discover the local workgroup network from the switch
- Discover the local workgroup network from the router using the **show cdp** commands
- Use Telnet to access a remote host on the network
- Determine the storage location of the Cisco IOS image
- Copy a configuration from a TFTP server to the startup configuration on a Cisco router

Visual Objective

The figure illustrates what you will accomplish in this activity.



Required Resources

These are the resources and equipment required to complete this activity:

- PC connected to an onsite lab or PC with an Internet connection to access the remote lab
- Terminal server connected to a console port of each lab device (if you are using a remote lab)
- INTRO pod assigned by your instructor

Command List

The table describes the commands used in this activity.

Command	Description
copy tftp startup-config	Copies a configuration file from a TFTP server to NVRAM.
disconnect ***line-number***	Disconnects a Telnet session from the local device. The "line-number" is the line number of your Telnet session.
enable	Activates privileged EXEC mode on your device.
erase startup-config	Erases NVRAM.
ping *ip-address*	Common tool used to troubleshoot the accessibility of devices. It uses ICMP echo requests and ICMP echo replies to determine whether a remote host is active. The **ping** command also measures the amount of time it takes to receive the echo reply.
show cdp ?	Obtains a context-sensitive list of options or arguments for the **show cdp** command.
show cdp neighbors	Displays the CDP updates received on each local interface of the device.
show cdp neighbors detail	Displays details about CDP updates received on each local interface of the device.
show flash	Lists bootflash or flash PC card information, including file code names, version numbers, volume ID, and sizes.
show startup-config	Displays the configuration settings of the device NVRAM.
show sessions	Displays a list of hosts where you have established Telnet connectivity.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.
telnet *ip-address*	Starts a terminal emulation program from a PC, router, or switch that permits you to access network devices remotely over the network.

Job Aids

There are no job aids for this lab activity.

Activity Preparation

Up to this point in this course, you have learned the layout of the specific lab equipment used by your class. You have learned basic navigation in both the switch and the router, and you have performed some basic configuration on both the workgroup switch and the workgroup router. Those are all foundation skills that you will need in your work with Cisco Systems networks. In this lab activity, you will use specific applications and protocols to manage your network. These instructions assume that your equipment has been connected properly and that your PCs have access to a terminal server connected to the lab equipment.

This lab activity focuses first on CDP, an OSI Layer 2 protocol used between Cisco devices. CDP is a relatively simple protocol but is a highly effective tool for determining connectivity between two adjacent devices.

In the later tasks of this lab activity, you will work with basic device management tools such as Telnet and TFTP. Like CDP, these are tools that you will use frequently in working with Cisco networks.

Note	The devices to use for this lab activity are named in the format of wg_sw_*x*; and wg_ro_*x,* where “x” is the letter of your workgroup.

Your instructor will provide the information that you need to complete this task and the subsequent lab activity. Complete the following information as provided by your instructor.

Value	Information Provided by Your Instructor
Saved configuration file name	
TFTP server IP address	

Task 1: Use CDP to Discover the Local Workgroup Network from the Switch

CDP is used to determine directly connected adjacent Cisco devices. In this task, you will use CDP to discover the directly connected neighbors of your workgroup switch. You will discover the neighbors and record information about them based solely on the CDP updates your workgroup switch receives.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	From your PC, open a Telnet session to the terminal server. The main menu appears.
2.	Choose your workgroup from the main menu. The pod menu appears.
3.	Choose your workgroup switch from the pod menu.
4.	Enter the **show cdp ?** command to view a list of the command arguments available for the switch. What CDP options are available? (Enter your answer in the space provided.) (The Catalyst 2950 has more **show cdp** command options than the Catalyst 1900.)
5.	Enter the **show cdp neighbors** command at the wg_sw_*x*> prompt, where "x" is the pod letter assigned to you for this lab activity.
6.	Use the output from the **show cdp neighbors** command to partially complete these items: Device identifier: _____ IP address: _____ Local port: _____ Capabilities: _____ Platform: _____ Remote port: _____
7.	Extend the output of the **show cdp neighbors** command by entering the **show cdp neighbors detail** command. Complete the missing information from Step 6 using the new information that you just obtained. What additional information does the **detail** keyword give you about neighboring devices? (Enter your answer in the space provided.)

Activity Verification

You have completed this task when you attain this result:

- You showed information about a neighboring device using CDP.

Task 2: Discover the Local Workgroup Network from the Router

In the previous task, you used CDP to determine Cisco devices directly connected to your workgroup switch. In this task, you will use CDP to discover the directly connected neighbors of your workgroup router. After completing this task, you should be able to draw a diagram of the network as seen from your workgroup switch and router.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Access the console port of your workgroup router wg_ro_*x*, where "x" is the pod letter assigned to you for this lab activity.
2.	Enter the **show cdp ?** command to view a list of the command arguments available for the router.
3.	Enter the **show cdp neighbors** command at the wg_ro_*x*> prompt, where "x" is the pod letter assigned to you for this lab activity.
4.	Extend the output by entering the **show cdp neighbors detail** command. What additional information is displayed? (Write your answer in the space provided.)
5.	Use the output from the **show cdp neighbors detail** command to complete these items: Device identifier: _____ IP address: _____ Local port: _____ Capabilities: _____ Platform: _____ Remote port: _____

Activity Verification

You have completed this task when you attain this result:

- You showed information about a neighboring device using CDP.

Task 3: Use Telnet to Access a Remote Host

CDP permits you to learn the Layer 3 addressing of an adjacent device, as you saw in the previous two tasks. If you need to configure a device but do not know the IP address, you can use CDP to discover that address. Once you have the IP address of the device, you can use the built-in Telnet application to establish a connection to the device. In this task, you will establish a Telnet session from your workgroup router to your workgroup switch, briefly suspend that Telnet session, and then resume the connection prior to ending it.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Access the console port of your workgroup router wg_ro_x, where “x” is the pod letter assigned to you for this lab activity.
2.	Enter the **telnet** *ip-address* enabled EXEC command, where “ip-address” is the IP address of the device to which you are connecting. Use the address of your pod workgroup switch as your Telnet address. What is the IP address of your workgroup switch? (Enter your answer in the space provided.) A successful Telnet connection is indicated by a different prompt. What is your current console prompt? (Enter your answer in the space provided.) Is there a difference between Cisco IOS commands available from a vty port and those available on a local console port? (Enter your answer in the space provided.)
3.	To suspend your Telnet session to the switch, enter **Ctrl-Shift-6**, then press **Ctrl-Shift-6** and **x**. What is your prompt now? (Enter your answer in the space provided.) How do you return to the Telnet session on the switch? (Enter your answer in the space provided.) It is necessary to use two **Ctrl-Shift-6** keystrokes if you are using a terminal server to avoid suspending the session from the switch and returning to the terminal server menu. If you were connected directly to the router and had an open Telnet session to the switch, you would use the following keystrokes: **Ctrl-Shift-6** followed by **x**. If you enter those keystrokes with a terminal server, you see the pod menu.
4.	Return to the Telnet session on the switch.
5.	Suspend the Telnet session to the switch again.

Step	Action
6.	Enter the **show sessions** command on your router console. Which connection is your Telnet session to the switch? (Enter your answer in the space provided.)
7.	Disconnect the session to your workgroup switch using the **disconnect** *line-number* command, where "line-number" is the line number of your session. Does this log you out of the switch? (Enter your answer in the space provided.)

Activity Verification

You have completed this task when you attain these results:

- You connected to another network device as a remote terminal using Telnet.
- You can accurately document the devices, interfaces, and addresses as they currently exist in the network.

Task 4: Determine the Storage Location of the Cisco IOS Image

In this task, you will obtain the current configuration register setting and determine the system image load location.

Activity Procedure

Complete the steps shown in the table.

Step	Action
1.	Obtain the current configuration register setting on your router by using the **show version** command. Where in the command output is the configuration register displayed? (Enter your answer in the space provided.) What is the current configuration register setting? (Enter your answer in the space provided.) According to the current configuration register setting, where could the router obtain the system image file? (Enter your answer in the space provided.)
2.	Record the values for each parameter from the **show version** command in the space provided. Platform type of the router: _____ Name of the Cisco IOS image file: _____ Version of the Cisco IOS software: _____ Original location of the image file: _____ The total amount of memory in NVRAM: _____
3.	Using the system image file name for your router, write the file name component for the definition provided. File extension: _____ Type of router platform: _____ Supported feature set: _____ File version number: _____

Activity Verification

You have completed this task when you attain this result:

- You identified the load location of the Cisco IOS image.

Task 5: Copy a Configuration from a TFTP Server

In this task, you will erase your startup configuration from NVRAM, and then download a configuration that your instructor has loaded on the TFTP server back into NVRAM.

Activity Procedure

Complete the steps shown in the table.

Step	Action	What You See
1.	Enter the proper **show** command to verify your first Ethernet interface. Refer to the command list for this lab activity to determine which **show** command to use. What command do you use to verify that the Ethernet interface is enabled? (Enter your answer in the space provided.) Enter that command on the router now.	
2.	Ping the TFTP server to verify that your router has connectivity to it. If the **ping** command fails, the next step will not work. Contact your instructor for help if needed.	
3.	Enter the command to erase the startup configuration in NVRAM on your workgroup router.	
4.	Enter the **show startup-config** command. Your output should look similar to the example (depending on your router).	`startup-config is not present`
5.	Use the **copy tftp startup-config** command to copy a saved configuration file on the TFTP server to NVRAM on your workgroup router. Refer to the Activity Preparation section of this lab activity for the saved configuration file name and TFTP server IP address.	
6.	Enter the **show flash** command to verify that you correctly entered the **copy** command. (If you accidentally enter the wrong **copy** command, you can erase the Cisco IOS image in the flash memory of your router.) Notify your instructor if your image does not match the image you finished with in Task 4 of this lab activity.	
7.	Enter the **show startup-config** command to verify that the contents of the NVRAM have been downloaded correctly. You should now see a different configuration from the one you have in your running configuration.	
8.	Enter **copy running-config startup-config** to overwrite the startup configuration in NVRAM.	
9.	Enter the **show startup-config** command to verify that the startup configuration and the running configuration are identical.	
10.	Notify your instructor that you have completed the lab activity.	

Activity Verification

You have completed this task when you attain this result:

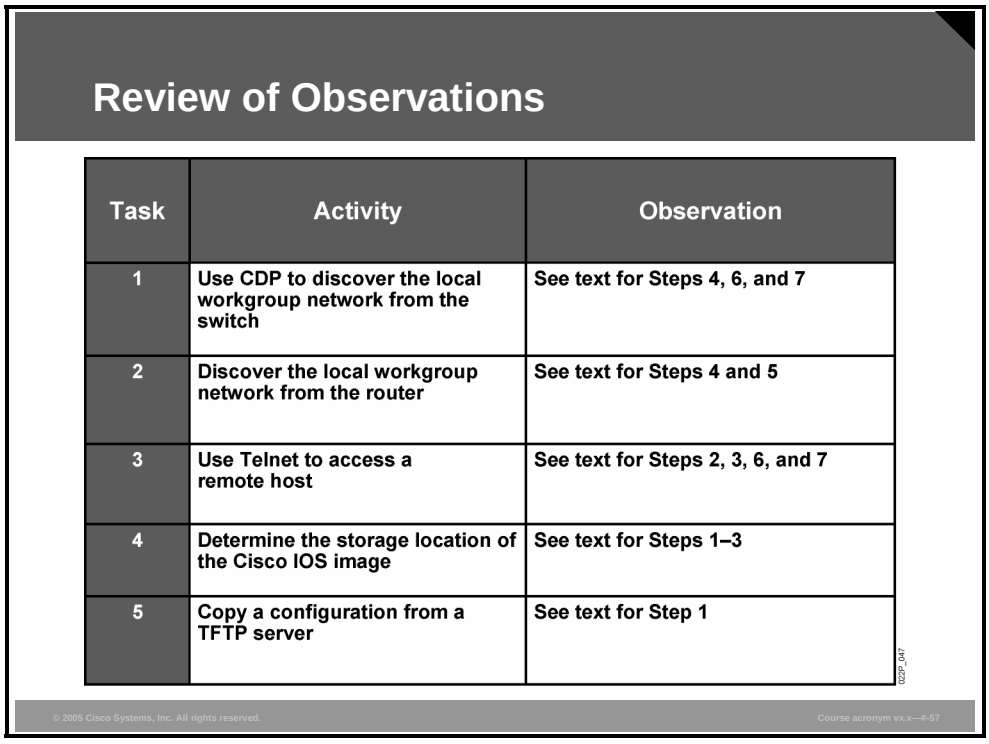
- You copied a configuration file from a TFTP server to the startup configuration of your router.

Lab 9-1: Debrief

This debriefing session covers the activities in the "Gathering Information About Neighboring Devices and Using System Files" lab. The topics addressed include a review of the correct steps for gathering information about neighboring devices and a review of the tools that were used.

Review of Observations

In this portion of the debriefing session, you will review the observations that you noted during the process of gathering information about neighboring devices and using system files.



The figure shows the observations that you should have made during the lab, as follows:

- **Task 1, Step 4:** The list of arguments associated with the **show cdp ?** is as follows:

```
entry      Information for specific neighbor entry
interface  CDP interface status and configuration
neighbors  CDP neighbor entries
traffic    CDP statistics
|          Output modifiers
```


- **Task 1, Step 6:** The output of the **show cdp neighbor** command will enable you to complete the following neighbor information as shown here.

Device Identifier	IP Address	Local Port	Capabilities	Platform	Remote Port
wg_ro_x	Not available from show cdp neighbor	Fas 0/2	R	2610	e 0/0
core_sw_a	Not available from show cdp neighbor	Fas 0/11	S I	WS-C2950-2	Fas 0/12

Completed neighbor information from Task 1, Step 6

Device Identifier	IP Address	Local Port	Capabilities	Platform	Remote Port
wg_ro_x	**10.1.1.131**	Fas 0/2	R	2610	e 0/0
core_sw_a	**10.1.1.2**	Fas 0/11	S I	WS-C2950-2	Fas 0/12

- **Task 1, Step 7:** The extra information given by the **show cdp neighbors detail** is as follows:

  For a router: Layer 3 addresses of interface, Cisco IOS version information, VTP version number

  For a switch: Cisco IOS version information, VTP version number, VTP management domain name, native VLAN, duplex mode, management address

- **Task 2, Step 4:** The extra information given by the **show cdp neighbors detail** is as follows:

  Layer 3 addresses of interface, Cisco IOS version information.

- **Task 2, Step 5:** The output of the **show cdp neighbors detail** command was used to complete the following neighbor information as shown here.

Device Identifier	IP Address	Local Port	Capabilities	Platform	Remote Port
wg_sw_x	10.1.1.130	Eth 0/0	Switch, IGMP	WS-C2950-24	Fast 0/2

- **Task 3, Step 2:** The IP address of your workgroup switch could be obtained from either the previous task or from the visual objective figure.

  A successful Telnet connection is indicated by the prompt changing to wg_sw_x (where "x" is your pod letter). You needed to use the vty password of "sanjose" to gain access to the switch.

  The only difference between Cisco IOS commands available from a vty port and those available on a local console port would be because of platform differences; that is, one is a switch and the other is a router.

  The IP address of your workgroup switch could be obtained either from the previous task or from the visual objective. It should resemble "10.1.1.x."

- **Task 3, Step 3:** Your prompt should change back to wg_ro_x (where "x" is your pod letter).

  To return to the Telnet session on the switch, you can enter the **resume** command or press the **Enter** key

- **Task 3, Step 6:** The output of the **show sessions** command will identify the session number (if more than one session is open) and also use the asterisk (*) character to show the current session. In the following example, connection number 1 is indicated.

```
wg_ro_x>show sessions
Conn Host                Address           Byte  Idle Conn
Name
*  1 10.1.1.130          10.1.1.130         0     0 10.1.1.130
```

- **Task 3, Step 7:** Disconnecting the session from the switch logs you out of the switch. This can be proven by opening another Telnet session to the switch, which requires that you provide the password to gain access to the Cisco IOS prompt.

- **Task 4, Step 1:** The configuration register setting is displayed as the last line of the output of the **show version** command.

  The current configuration register setting should be 0x2102.

  The current configuration register setting indicates that the system image file should be loaded from the flash memory**:** 0 x 2 1 0 2**.**

- **Task 4, Step 2:** The output of the **show version** command allowed you to answer the following questions:

  Platform type of the router: Cisco 2610

  Name of the Cisco IOS image file: c2600-js-mz.120-8.bin

  Version of the Cisco IOS software: 11.3(2)XA4

  Original location of the image file: flash:

  The total amount of memory in NVRAM: 32 Kb

An example of the **show version** output is as follows:

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-JS-M), Version 12.0(8), RELEASE
  SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Mon 29-Nov-99 15:26 by kpma
Image text-base: 0x80008088, data-base: 0x80B081E0


ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE
(fc1)


wg_ro_x uptime is 2 days, 20 hours, 57 minutes
System restarted by reload at 13:05:09 UTC Fri May 3 2002
System image file is "flash:c2600-js-mz.120-8.bin"


cisco 2610 (MPC860) processor (revision 0x300) with
53248K/12288K
  bytes of memory.
Processor board ID JAD06090BMD (2719249260)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology
Corp).
TN3270 Emulation software.
Basic Rate ISDN software, Version 1.1.
1 Ethernet/IEEE 802.3 interface(s)
2 Serial(sync/async) network interface(s)
1 ISDN Basic Rate interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)


Configuration register is 0x2102
```

- **Task 4, Step 3:** Using the system image file name **c2600-js-mz.120-8.bin**:

  File extension: bin (binary is *not* a configuration)

  Type of router platform: c2600 (all Cisco 2600 series routers)

  Supported feature set: js (j = enterprise and s = extended capabilities)

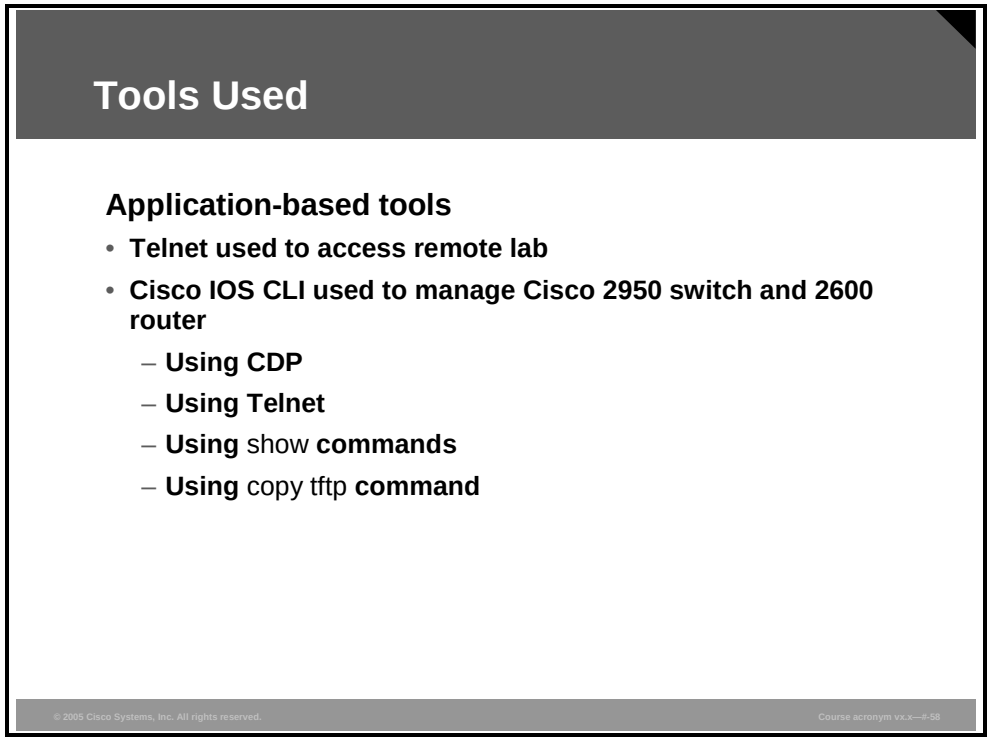
  File version number: 120-8 (version 12.0(8))

- **Task 5, Step 1:** The results of the **show interface** command will identify the first Ethernet interface.

  Using the **show interface e 0/0** command will display the status of the interface as either up, down, or administratively down.

Tools

In this lab, a number of tools were used.



- **Telnet:** This IP application was used as a tool to provide access to the remote terminal server that allows connection to the switches and routers that form the lab.

