Cisco | Networking Academy®
Mind Wide Open™

CCNA Discovery 4.0

Working at a Small-to-Medium Business or ISP

Student Lab Manual

Lab 1.2.3 Mapping ISP Connectivity Using Traceroute

Objectives

- Run the Windows **tracert** utility from a local host computer to a website on a different continent.
- Interpret the traceroute output to determine which ISPs the packets passed through on their way from the local host to the destination website.
- Draw a diagram of the traceroute path, showing the routers and ISP clouds passed through from the local host to the destination website, including IP addresses for each device.

Background / Preparation

In this activity, you will use the Windows **tracert** utility to map Internet connectivity between your local ISP and the other ISPs that it uses to provide global Internet access. You will also map connectivity to the following major Regional Internet Registries (RIRs). However, your instructor may choose different destination websites.

- AfriNIC (African Network Information Centre) – Africa Region
- APNIC (Asia Pacific Network Information Centre) – Asia/Pacific Region
- ARIN (American Registry for Internet Numbers) – North America Region
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin America and some Caribbean Islands
- RIPE NCC (Réseaux IP Européens) – Europe, the Middle East, and Central Asia

This activity can be done individually, in pairs, or in teams. It can be done as an in-class activity or as a homework assignment, depending on whether the classroom computers have access to the Internet.

The following resources are required:

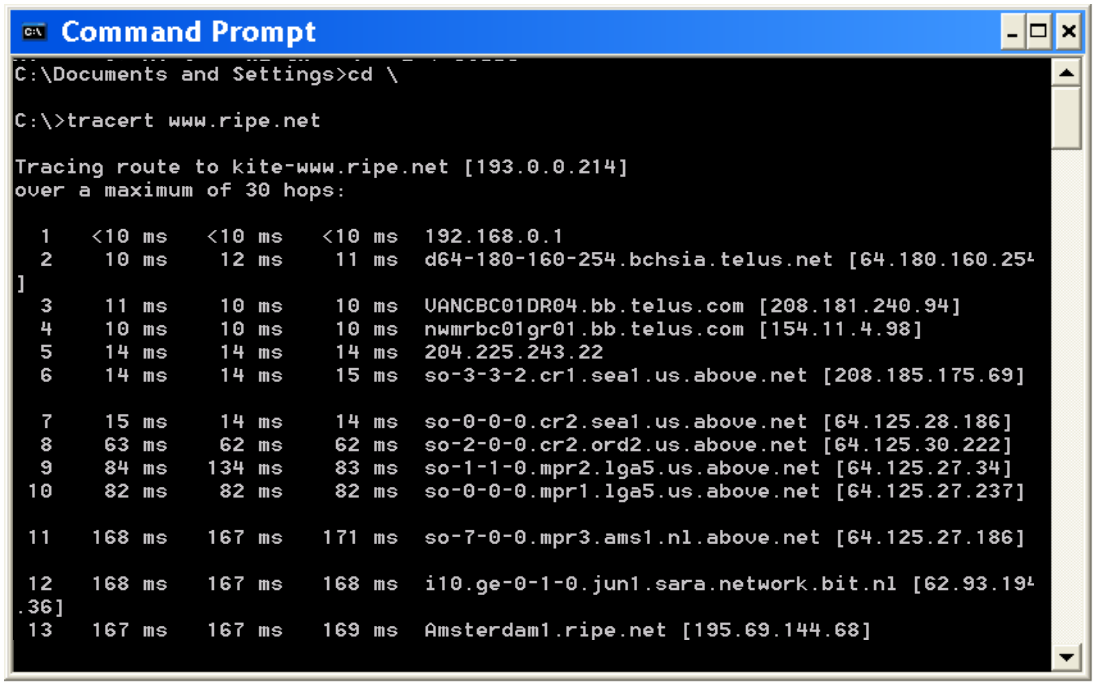
- Host computer with the Windows operating system
- Access to the command prompt
- Internet connection
- Routes Traced worksheet for each destination URL. The worksheet is attached to this lab. Each student completes their own worksheets and gives them to the instructor.
- Global Connectivity Map, which is attached at the end of this lab
- Access to the PC command prompt

Step 1: Run the tracert utility from a host computer

a. Verify that the host computer has a connection to the Internet.

b. Open a Command Prompt window by clicking **Start > Run** and typing **cmd**. Alternatively, you may click **Start > All programs > Accessories > Command Prompt**.

c. At the prompt, type **tracert** and your first destination website. The output should look similar to the following:



d. Save the **tracert** output in a text file as follows:

1) Right-click the title bar of the Command Prompt window and choose **Edit > Select All**.

2) Right-click the title bar of the Command Prompt window again and choose **Edit > Copy**.

3) Open the **Windows Notepad** program: **Start > All Programs > Accessories > Notepad.**

4) To paste the output into Notepad, choose **Edit > Paste**.

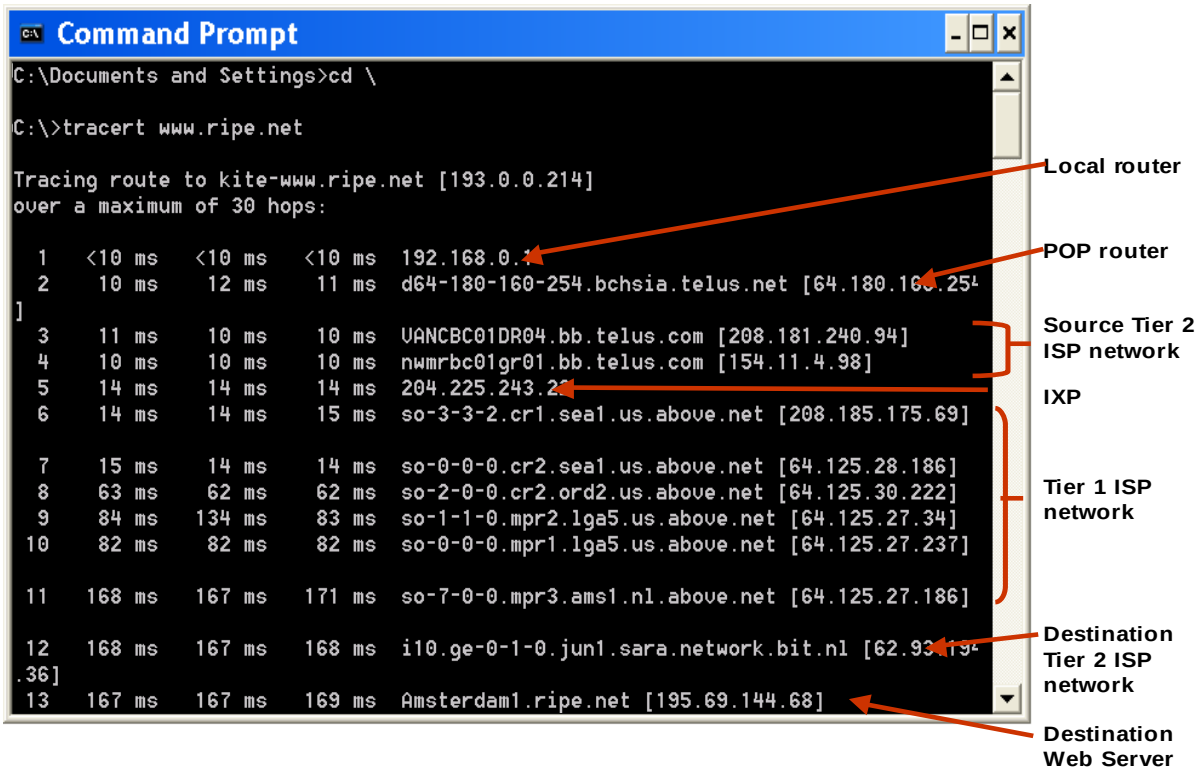
5) Choose **File > Save As** and save the Notepad file to your desktop as tracert1.txt.

e. Run **tracert** for each destination website and save the output in sequentially numbered files.

f. Run **tracert** from a different computer network, for example, from the public library or from a friend's computer that accesses the Internet using a different ISP (for instance, cable instead of DSL). Save a copy of that output in Notepad and print it out for later reference.

Step 2: Interpret tracert outputs to determine ISP connectivity

Routes traced may go through many hops and a number of different ISPs depending on the size of your ISP and the location of the source and destination hosts. In the example output shown below, the tracert packets travel from the source PC to the local router default gateway to the ISPs Point of Presence (POP) router and then to an Internet Exchange Point (IXP). From there they pass through two Tier 2 ISP routers and then though several Tier 1 ISP routers as they move across the Internet backbone. When they leave the Tier 1 ISPs backbone, they move through another Tier 2 ISP on the way to the destination server at www.ripe.net.



a. Open the first traceroute output file and answer the following questions.

1) What is the IP address of your local POP router?

_____

2) How many hops did the traceroute packet take on its journey from the host computer to the destination?

_____

3) How many different ISPs did the traceroute packet pass through on its journey from the host computer to the destination?

_____

4) List the IP addresses and URLs of all the devices in the traceroute output in the order that they appear on the Routes Traced worksheet.

5) In the Network Owner column of the worksheet, identify which ISP owns each router. If the router belongs to your LAN, write “LAN”. The last two parts of the URL indicates the ISP name. For example, a router that has “sprint.net” in its URL belongs to the network of an ISP called Sprint.

6) Did the traceroute pass through an unidentified router between two ISPs? This might be an IXP. Run the **whois** command utility or **whois** function of a visual traceroute program to identify ownership of that router. Alternatively, go to http://www.arin.net/whois to determine to whom the IP is assigned.

b. Complete the worksheet using the traceroute output file for each of the other destination URLs.

c. Compare your results from the different traceroute output files. Did your ISP connect to different ISPs to reach different destinations?

_____

d. If you ran a traceroute from a different computer network, check the output for that traceroute file as well. Was the number of hops different to reach the same destination from different local ISPs? Which ISP was able to reach the destination in fewer hops?

_____

Step 3: Map the connectivity of your ISP

a. For each traceroute output, draw a diagram on a separate sheet of paper showing how your local ISP interconnects with other ISPs to reach the destination URL, as follows:

1) Show all of the devices in sequence from the LAN router to the destination website server. Label all of the devices with their IP addresses.

2) Draw a box around the local POP router that you identified, and label the box “POP”.

3) Draw an ISP cloud around all the routers that belong to each ISP, and label the cloud with the ISP name.

4) Draw a box around any IXP routers that you identified, and label the box “IXP”.

b. Use the Global Connectivity Map to create a combined drawing showing only ISP clouds and IXP boxes.

Worksheet for Routes Traced

Destination URL: _____ **Total Number of Hops:** _____

Router IP Address	Router URL (if any)	Network Owner (LAN, Name of ISP or IXP)

Global Connectivity Map

Lab 3.2.4 Evaluating a Cabling Upgrade Plan

Objectives

- Examine the existing floor plan of a customer.
- Propose a cable upgrade plan to accommodate extra floor space.

Background / Preparation

A medium sized company has existing space on the second floor of an office tower and has just acquired the rest of the second floor. They have asked you to examine their existing floor plan and assist them in the placement of a new IDF, placement of cables to support all of the new office space, and to help determine if any new devices are required.

This lab can be done individually or in groups.

The following resources are required:

- Existing Floor Plan (provided)

Step 1: Examine the existing floor plan.

a. From the information provided on the existing floor plan, label the following items:

1) POP – Point of Presence
2) MDF – Main Distribution Facility
3) IDF – Intermediate Distribution Facility
4) Vertical/Backbone Cabling
5) Horizontal Cabling

b. What type of cabling could be used for the vertical/backbone cabling? Explain your answer.

_____

Step 2: Evaluate plan for new floor space.

AnyCompany has just merged with a small web design group and has acquired the remaining space on the second floor to accommodate the web design team. This new space is represented on the diagram as the floor space highlighted on the right side of the floorplan. It has been decided to add a second IDF to support the workstations in the new area.

a. Suggest a possible location for the new IDF. What room / location did you choose and explain why you think it is suitable?

_____

_____

b. What type of cable would you suggest for the vertical cabling required to connect the new IDF to the existing MDF? Explain your reasons.

_____

_____

c. The new space contains mostly offices. Assume that each office will be provisioned with 2 data drops. Also plan for 2 drops in the auditorium to support Internet access for presentations and training sessions. How many additional data drops need to be ordered?

_____

d. You have been asked to determine the number of new 24 port switches required for the new IDF. Remember to plan on approximately 25% growth. How many new switches will Company ABC need to purchase?

_____

e. How many horizontal cables will terminate on patch panels in the new IDF?
_____

Step 3: Examine the floor space and wiring plan.

a. What equipment other than switches would you expect to find in the new IDF?

_____

b. What equipment other than switches would you expect to find in the MDF?

_____

_____

c. Using existing cable runs, could you use UTP to connect the devices in room 2.20 or 2.30 directly into a switch in the MDF?

_____

Step 4. Reflection

With one or two classmates, discuss the following:

a. Is it better to have an IDF in this floor space or should the company run the horizontal cables for each device directly back to the existing MDF?

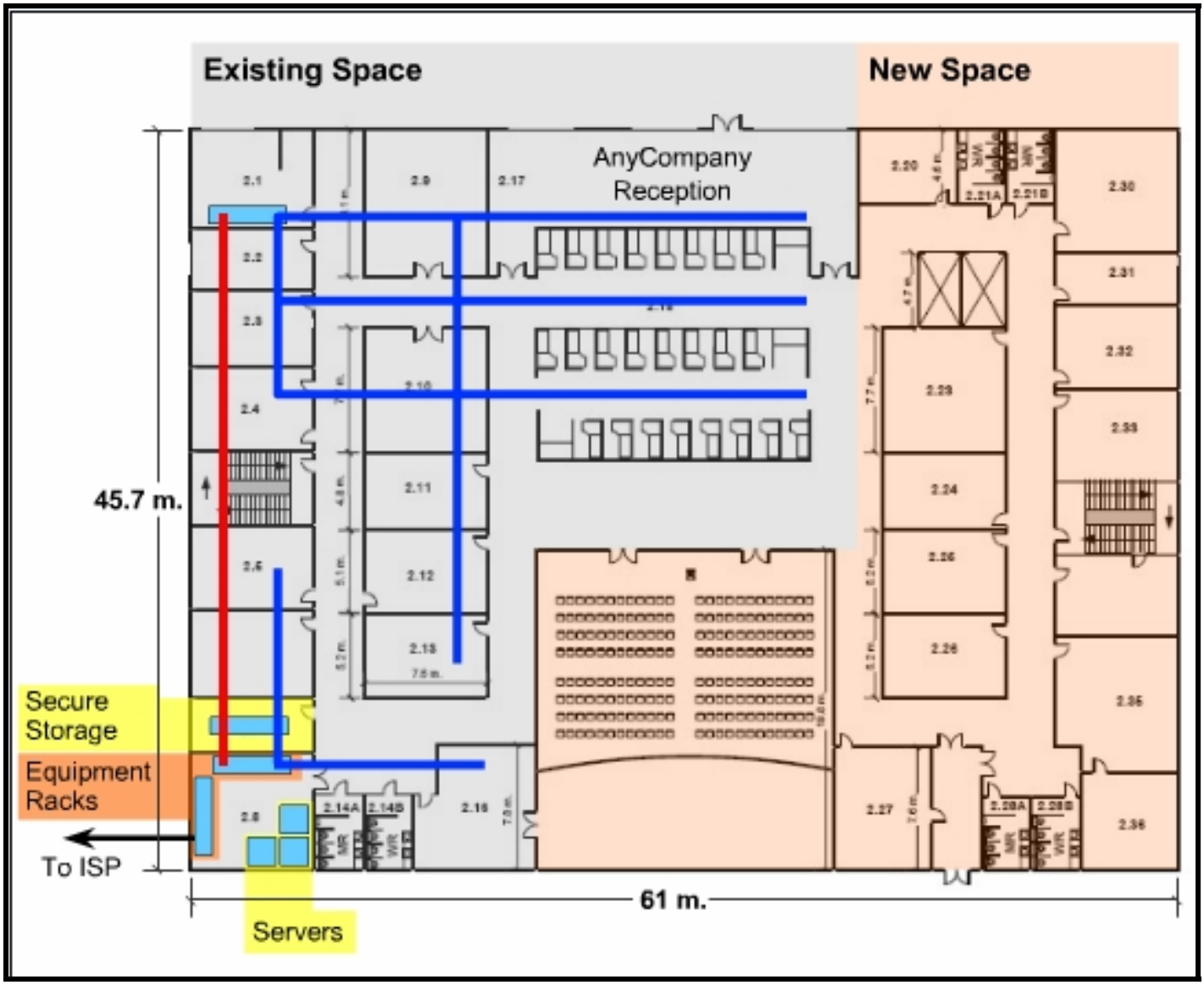
_____

_____

_____

b. How many cables will be required from the MDF to the IDF to support the switches? Explain your answer.

_____



Lab 4.1.5 Subnetting a Network

Objective

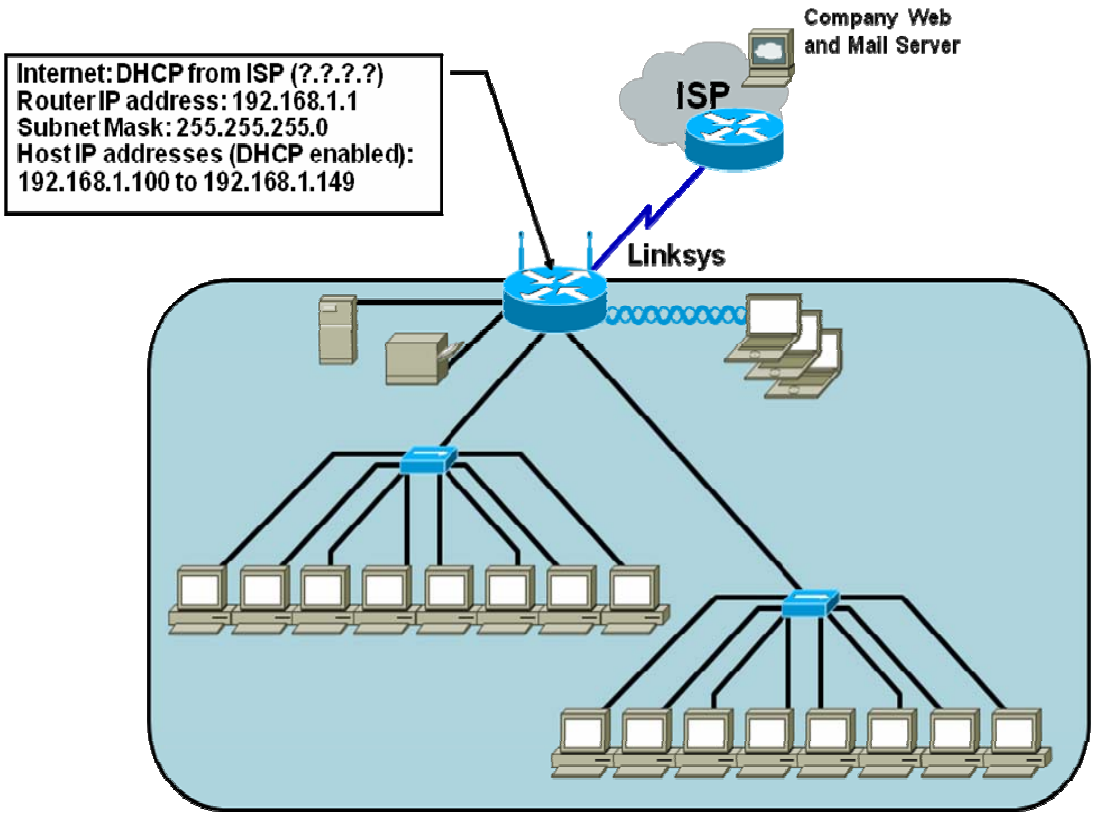
- Create an IP addressing plan for a small network.

Background / Preparation

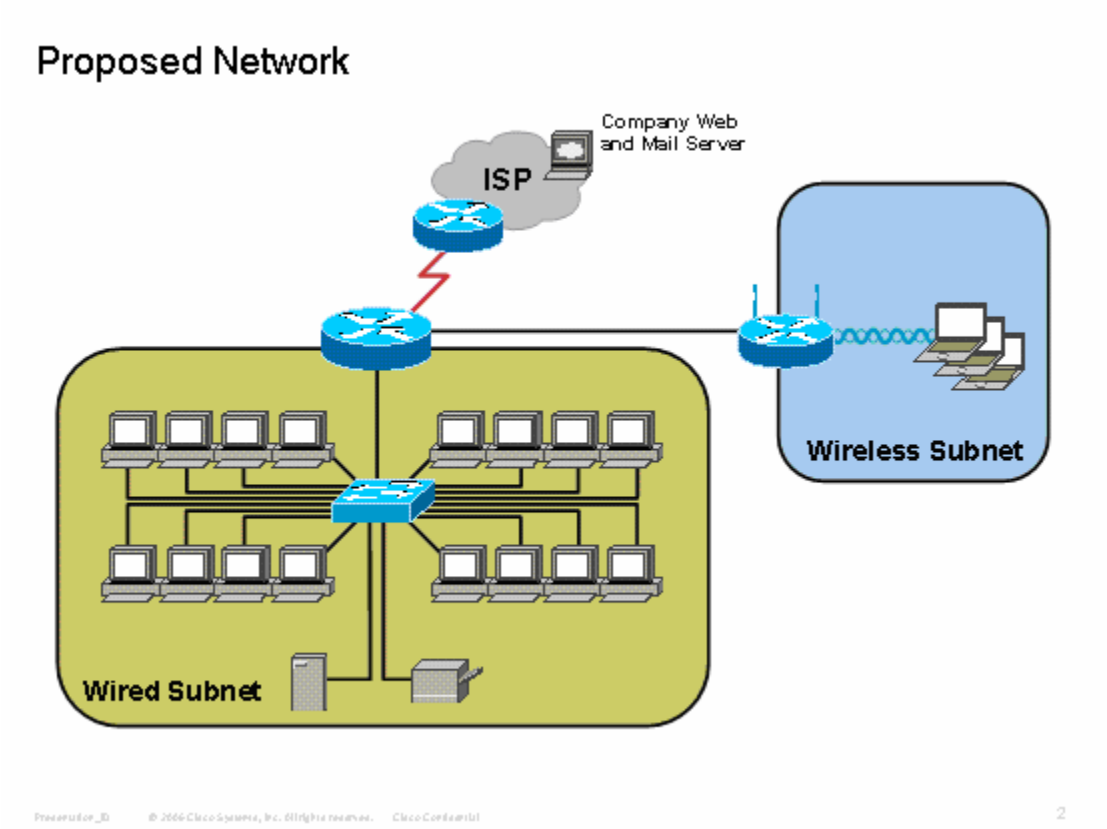
In this activity, you will play the role of an onsite installation and support technician from an ISP.

A customer has called the ISP complaining of e-mail problems and occasional poor Internet performance. On an earlier site visit, the technician had created diagram of the customer's existing network shown here.

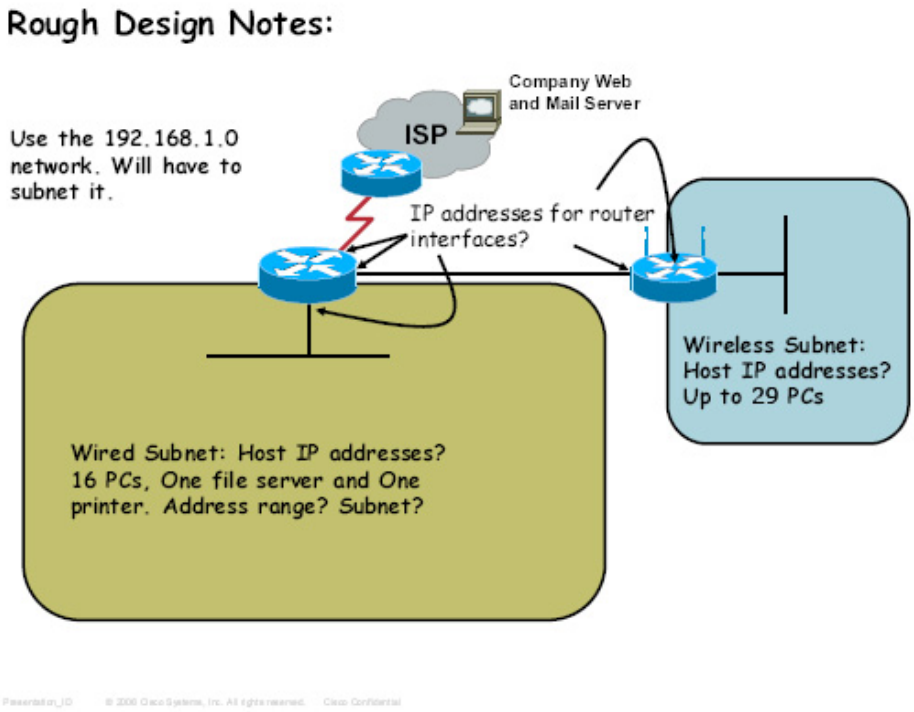
Existing Network



The ISP is preparing a design for a network upgrade. The interim topology diagram for the proposed network is shown below.



There is still a requirement for an IP addressing plan. One of the ISP network designers has made some notes on a simplified sketch of the proposed network, and has written some requirements. The designer asks you to create an IP address plan for the network upgrade.



Step 1: Analyze the network

a. Referring to the Rough Design Notes, determine the minimum number of hosts that a subnet needs to support the new network design.

   1) The largest subnet must be able to support _____ hosts.

   2) To support that many hosts, the number of host bits required is _____.

b. What is the minimum number of subnets required for the new network design? _____

c. Can this network be subnetted according to the requirements? _____

   For example: If four subnets are required and the largest subnet has to support 128 hosts, this is a problem, because a subnet in a class C network that has been partitioned four ways can support only 62 hosts.

d. Fill in the blanks to summarize the subnetting requirements of this new network design:

   This network requires _____ subnets, each supporting 29 hosts. Therefore, _____ host ID bits are reserved for the subnet ID. With those values, this network supports _____ subnets, each subnet having _____ hosts.

Step 2: Calculate the custom subnet mask

Now that the number of subnet ID bits is known, the subnet mask can be calculated. A class C network has a default subnet mask of 24 bits, or 255.255.255.0. What will the custom subnet mask be?

The custom subnet mask for this network will be _____._____._____._____, or /_____.

Step 3: Specify the host IP addresses

Now that the subnet mask is identified, the network addressing scheme can be created. The addressing scheme includes the subnet number, the subnet broadcast address, and the range of IP addresses assignable to hosts.

a. Complete the table showing all the possible subnets for the 192.168.1.0 network.

Subnet	Subnet Address	Host IP Address Range	Broadcast Address

b. for it to be completed. Hosts will be assigned IP addresses as follows: (fill in the table below)

Device	Interface	IP Address	Connects to	IP Address
1841	Serial 0/0/0	11.11.11.100	ISP Router	11.11.11.1
	Fa 0/0	____.____.____.____	Wired hosts	Wired host Range: ____.____.____.____ To ____.____.____.____
	Fa 0/1	____.____.____.____	Linksys Internet	____.____.____.____
Linksys	Internet	____.____.____.____	1841 Fa 0/1	____.____.____.____
	LAN Gateway	____.____.____.____	Wireless Hosts	Wireless host Range: ____.____.____.____ To ____.____.____.____

Step 4: Consider other subnetting options

What if there were more than 30 hosts that needed to be supported on either the wired or wireless portion of the network. You could borrow fewer bits, which would create fewer subnets, but each one would support a greater number of hosts per subnet.

a. How many bits would be borrowed to create four subnets? _____

b. How many bits would be left for hosts on each subnet? _____

c. What is the maximum number of hosts each subnet could support?
_____

d. What would the subnet mask be in dotted decimal and slash number (/#) format?
_____

e. If you start with the same 192.168.1.0 network as before and subnet it into four subnets, what would the subnet numbers be?

_____

Step 5: Reflection

a. Does subnetting help reduce the problem of IP address depletion? Explain your answer.

_____

_____

_____

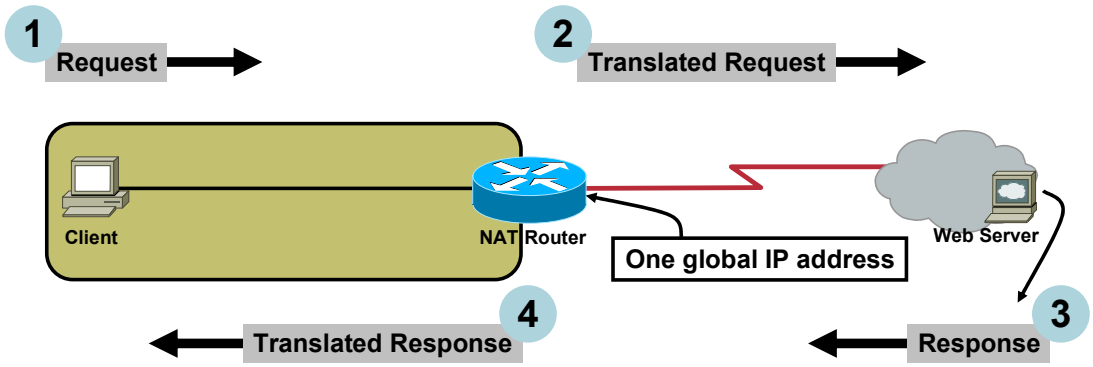
_____

_____

b. The Rough Design Notes diagram noted that the wireless subnet would have up to 30 PCs connecting. In pairs or in small groups, discuss whether or not that creates a situation in which IP addresses might get wasted. Does it matter, and why or why not?

c. There are alternate methods of subnetting using CIDR and VLSM. Would VLSM be a worthwhile option for subnetting this network? Discuss in small groups.

Lab 4.2.4 Determining PAT Translations



1. **Client on a private network sends a request to a web server on the public Internet.**
2. **NAT router translates source address and forwards the request to the web server**
3. **The web server responds to the client's translated address**
4. **The NAT router translates the client address (destination) back to the original private address**

Objectives

- Explain the active network connections open on a computer when viewing a particular web page.
- Determine what an internal IP address and port number are translated to using port address translation (PAT).

Background / Preparation

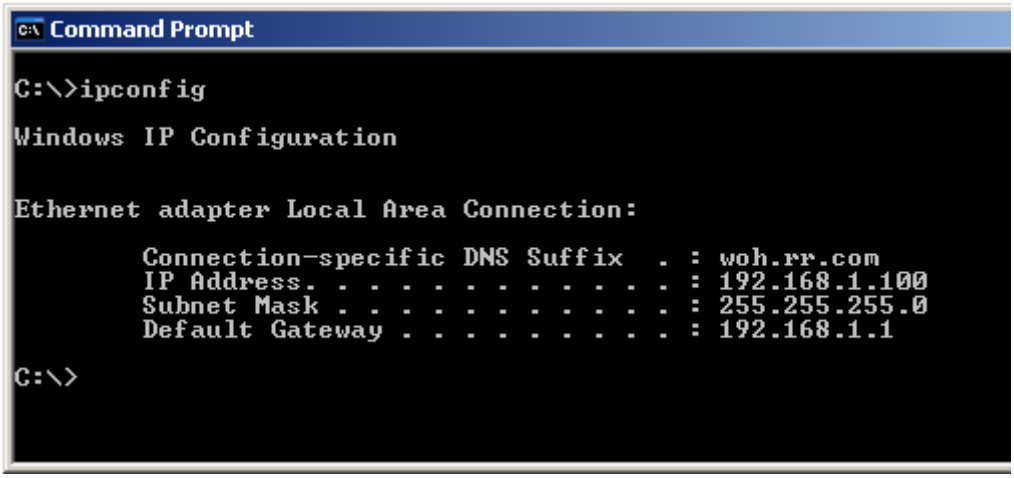
Port address translation (PAT) is a form of network address translation (NAT). With PAT, the router translates multiple internal (usually private) addresses to a single public IP address on an interface that is connected to the Internet. Port numbers are used, in combination with IP addresses, to keep track of individual connections. In this lab, you use the **ipconfig** and **netstat** commands to view open ports on a computer. You will be able to see the initial IP address and port combination, and determine the translated IP address and port combination.

The following resources are required:

- Computer running Windows XP Professional
- Connection to a gateway router or an ISR using PAT
- Internet connection
- Access to the PC command prompt.

Step 1: Determine the IP address of the computer

a. Open a **Command Prompt** window by clicking **Start > Run** and typing **cmd**. Alternatively, you may click **Start > All programs > Accessories > Command Prompt**. At the prompt, type the **ipconfig** command to display the IP address of the computer.



b. What is the IP address of the computer? _____

c. Is there a port number shown, and why or why not? _____

_____

_____

Step 2: Determine the IP addresses of the gateway router or ISR

Check with your instructor to get the IP addresses for the ISR NAT router gateway.

Internal Ethernet address: _____

External Internet address: _____

Step 3: Display baseline netstat results

a. At the command prompt, type the **netstat –n** command.

b. What type of information does the **netstat –n** command return?

_____

_____

c. Where does the IP address found in Step 1 appear? Is there a port number associated with it? Why or why not? _____

_____

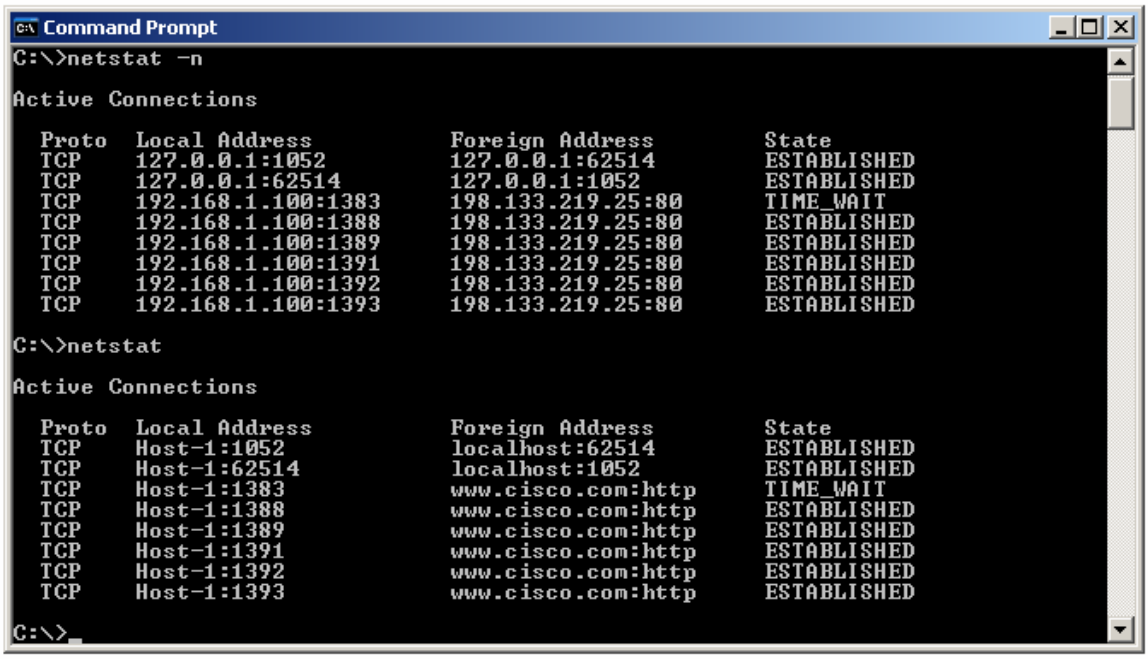
Step 4: Display active network connections

a. Ping **www.cisco.com** and record the address.

_____

b. Open a web browser and enter **www.cisco.com** in the address bar.

c. Go back to the Command Prompt window. Type the **netstat –n** command again, and then type the command without the **–n** option. The output looks similar to the following figure, depending on what other network applications and connections are open when you issued the command.



d. What is the difference in the output between the **netstat** and **netstat –n** commands?

_____

_____

e. Write down the connection entries for the client IP address and the IP address of the www.cisco.com web server.

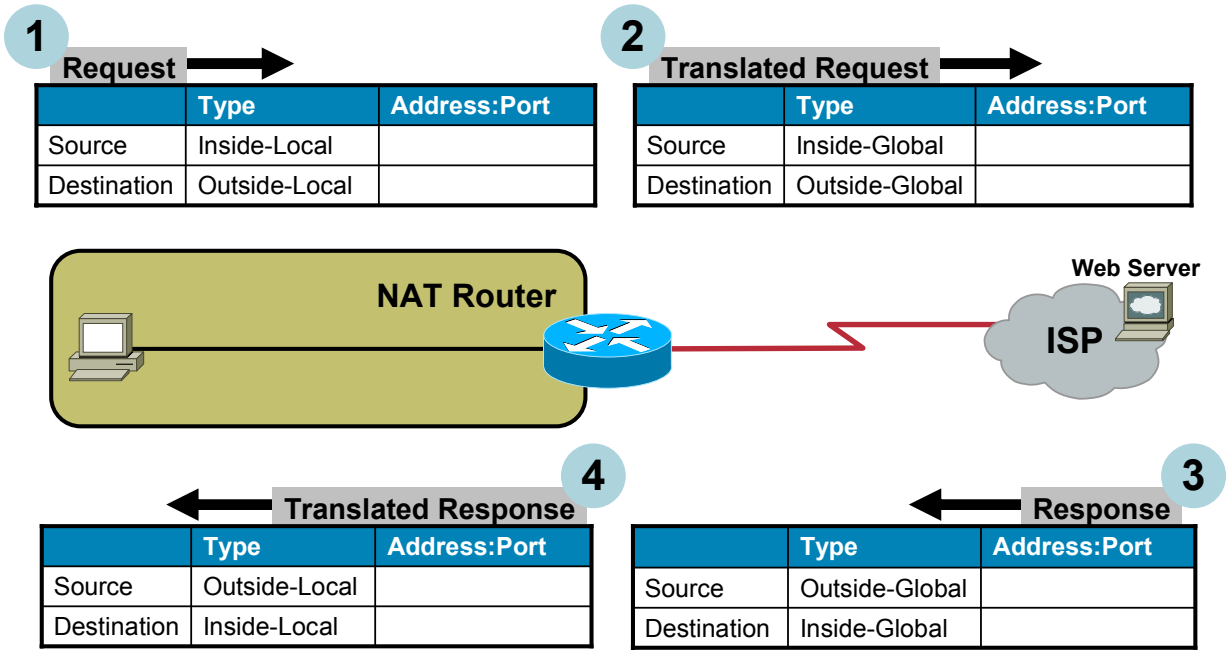
Local client IP address and port number: _____

Foreign IP Address and port number: _____

f. Are there more **netstat** entries the second time? _____

Step 5: Determine translated addresses

Use the information recorded in steps 2 and 4 and the topology diagram shown at the beginning of the lab to fill in the Address:Port columns.



	Type	Address:Port
Source	Inside-Local	
Destination	Outside-Local	

	Type	Address:Port
Source	Inside-Global	
Destination	Outside-Global	

	Type	Address:Port
Source	Outside-Local	
Destination	Inside-Local	

	Type	Address:Port
Source	Outside-Global	
Destination	Inside-Global	

Step 6: Reflection

a. Port address translation (PAT) is also called NAT with overload. What does the term “overload” refer to?

_____

_____

b. The NAT terminology used in the lab includes four types of addresses: inside-local, inside-global, outside-local, and outside-global. In many connections that pass through NAT routers, two of these addresses are often the same. Which two of these four addresses normally remain unchanged, and why do you think that is the case?

_____

_____

Lab 5.1.2 Powering Up an Integrated Services Router

Objectives

- Set up a new Cisco 1841 Integrated Services Router (ISR).
- Connect a computer to the router console interface.
- Configure HyperTerminal so that the computer can communicate with the router.

Background / Preparation

This lab focuses on the initial setup of the Cisco 1841 ISR. If a Cisco 1841 ISR is not available, you can use another router model. The information in this lab applies to other routers. A Cisco ISR combines routing and switching functions, security, voice, and LAN and WAN connectivity into a single device, which makes it appropriate for small-sized to medium-sized businesses and for ISP-managed customers.

Some steps in this lab are normally only performed once during initial setup. These steps are indicated as optional.

The following resources are required:

- Cisco 1841 ISR or other comparable router
- Power cable
- Windows PC with terminal emulation program
- RJ45-to-DB9 connector console cable

Step 1: Position router and connect ground wire (Optional)

NOTE: This step is optional and is required only if the router is being set up for the first time. Read through it to become familiar with the process.

a. Position the router chassis to allow unrestricted airflow for chassis cooling. Keep at least 1 inch (2.54 cm) of clear space beside the cooling inlet and exhaust vents.

CAUTION: Do not place any items that weigh more than 10 pounds (4.5 kilograms) on top of the chassis**,** and do not stack routers on top of each other.

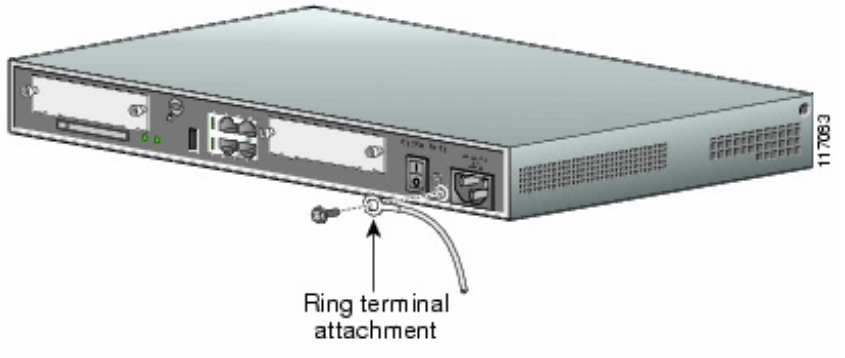
b. Connect the chassis to a reliable earth ground using a ring terminal and size 14 AWG (2 mm) wire using these steps:

NOTE: Your instructor should inform you where a reliable earth ground is.

1) Strip one end of the ground wire to expose approximately 3/4 inch (20 mm) of conductor.

2) Crimp the 14 AWG (2 mm) green ground wire to a UL Listed/CSA certified ring terminal using a crimping tool that is recommended by the ring terminal manufacturer. The ring terminal provided on the back panel of the Cisco 1841 ISR router is suitable for a Number 6 grounding screw.

3) Attach the ring terminal to the chassis as shown in the figure below. Use a Number 2 Phillips screwdriver and the screw that is supplied with the ring terminal and tighten the screw.



Grounding the Router

4) Connect the other end of the ground wire to a suitable earth ground that the instructor indicates.

Step 2: Install the CompactFlash memory card (Optional)

NOTE: This step is optional and is required only if the router is being set up for the first time. To avoid wear on the memory card and ejector mechanism, do not actually perform this step. Read through it to become familiar with the process.

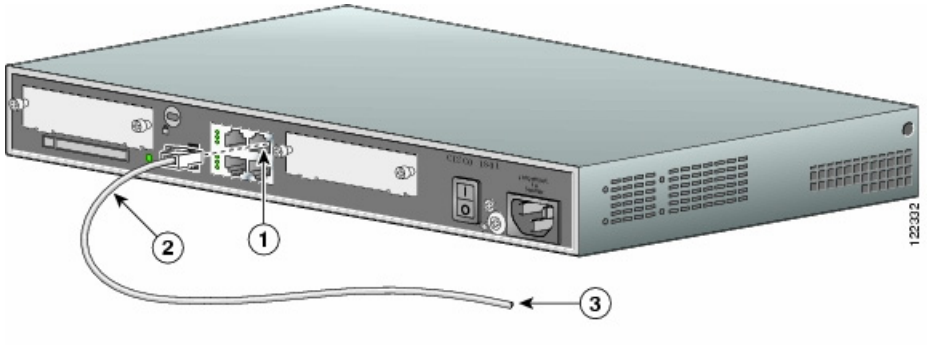
a. Attach a grounding strap to your wrist to avoid electroshock damage to the card. Seat the external CompactFlash memory card properly into the slot. This step depends on the type of router. Not all routers have flash cards.

b. If the router has a CompactFlash memory card, check that the ejector mechanism is fully seated. The ejector button is next to the CompactFlash memory card.

c. Connect the power cable to the ISR and to the power outlet.

Step 3: Connect the PC and configure the terminal emulation program

a. Connect the PC to the ISR using an RJ-45-to-DB-9 connector console cable, as shown in the figure below. To view the router startup messages, connect the PC to the ISR, power up the PC and start the terminal emulation program before powering up the router.



Connecting the PC to the Router

1. ISR RJ45 console port	2. Light blue RJ45-to-DB9 connector console cable
3. To PC COM port	

CAUTION: To ensure adequate cooling, never operate the router unless the cover and all modules and cover plates are installed.

b. Load a terminal emulation program, such as HyperTerminal, on the PC.

c. Select a COM port that matches the port where the RJ-45-to-DB-9 connector is connected to the PC. The COM port is usually COM1 or COM2.

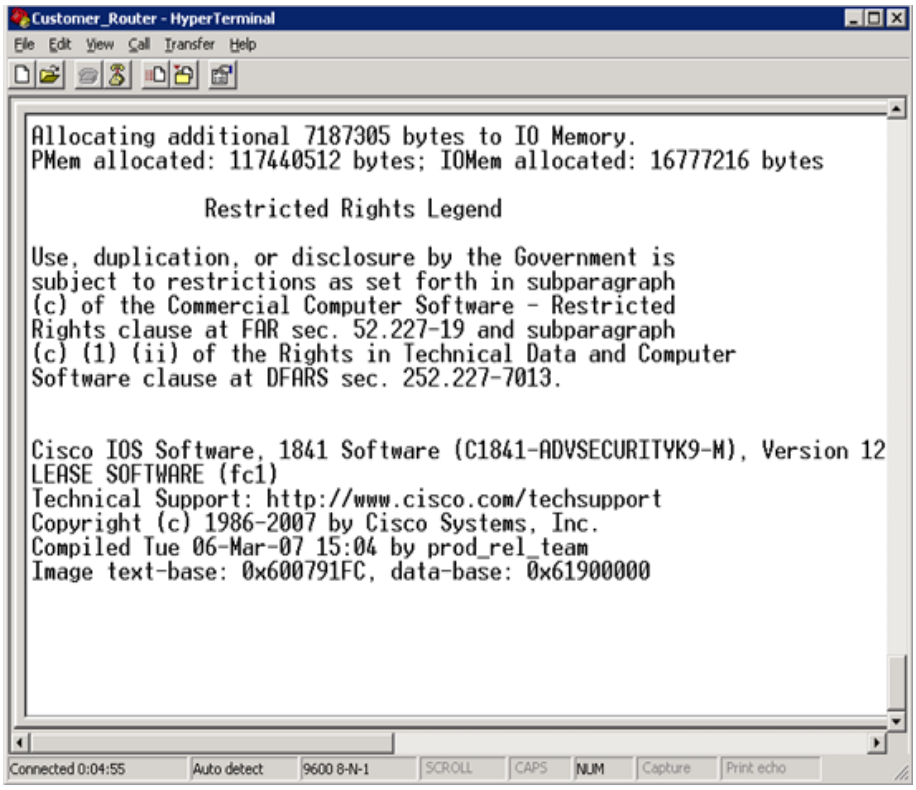
d. Configure the terminal emulation parameters as follows:

- 9600 baud
- 8 data bits
- no parity
- 1 stop bit
- no flow control and no parity

Step 4: Power up the ISR

a. Move the power switch on the back of the ISR to the ON position. During this step, the LEDs on the chassis turn on and off, not necessarily at the same time. The LED activity depends on what is installed in the ISR.

b. Observe the startup messages as they appear in the terminal emulation program window. While these messages are appearing, do not press any keys on the keyboard. Pressing a key interrupts the router startup process. Some examples of startup messages displayed are the amount of main memory installed and the image type of the Cisco IOS software that the computer is using. Can you find these example startup messages in the following figure?



c. The figure shows that there is 117 MB of memory installed on this router, and the Cisco IOS image type is C1841-ADVSECURITYK9-M. Startup messages are generated by the operating system of the router. The messages vary depending on the software installed on the router. These messages scroll by quickly and take a few minutes to stop.

When the Cisco 1841 ISR is correctly powered up, the **SYS PWR** LED is an unblinking green light, and the fans operate. When the router is finished starting up, the following system message appears in the terminal emulation window:

```
Press RETURN to get started!
```

Step 4: Troubleshoot a non-working router

If the **SYS PWR** LED does not blink green, the fans do not operate, and the correct system message does not appear in the terminal emulation window, turn off the router and verify that the power cable is securely attached to the router and plugged into the power source. If the router is does not power on, ask the instructor for assistance.

Step 5: Reflection

a. Is there anything about this procedure that is risky?

_____

_____

b. Why do the router cover, all modules, and cover plates need to be installed?

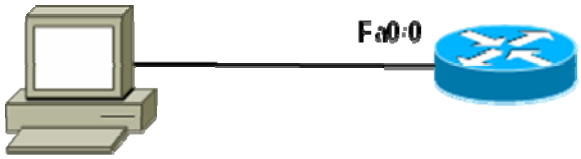
_____

_____

c. How many routers can you safely stack on top of each other?

1) 0
2) 1
3) 2
4) 3

Lab 5.2.3 Configuring an ISR with SDM Express



Objectives

- Configure basic router global settings – router name, users, and login passwords – using Cisco SDM Express.
- Configure LAN and Internet connections on a Cisco ISR using Cisco SDM Express.

Background / Preparation

Cisco Router and Security Device Manager (SDM) is a Java-based web application and a device-management tool for Cisco IOS Software-based routers. The Cisco SDM simplifies router and security configuration through the use of smart wizards, which allows you to deploy, configure, and monitor a Cisco router without requiring knowledge of the command-line interface (CLI). The Cisco SDM is supported on a wide range of Cisco routers and Cisco IOS Software releases. Many newer Cisco routers come with SDM preinstalled. If you are using an 1841 router, SDM (and SDM Express) is pre-installed.

This lab assumes the use of a Cisco 1841 router. You can use another router model as long as it is capable of supporting SDM. If you are using a supported router that does not have SDM installed, you can download the latest version free of charge from the following location: http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

From the URL shown above, view or download the document “Downloading and Installing Cisco Router and Security Device Manager.” This document provides instructions for installing SDM on your router. It lists specific model numbers and IOS versions that can support SDM, and the amount of memory required.

Cisco SDM Express is a component of SDM. SDM Express automatically runs a GUI wizard that allows you to perform an initial basic configuration of a Cisco router using a browser and the web interface of the router. SDM Express will only be activated when the router is in its factory-default state. In this lab, you will use Cisco SDM Express to configure LAN and Internet connections on a Cisco ISR.

The following resources are required:

- Cisco 1841 ISR router with SDM version 2.4 installed (critical – see Note 2 in Step 1)

- Cisco 1841 ISR router configured with factory default settings and with a serial port add-in module (critical – see Notes 1 and 3 in Step 1)
- (Optional) Other Cisco router model with SDM installed
- Windows XP computer with Internet Explorer 5.5 or higher and SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810). (See Note 3 in Step 1)
- Straight-through or crossover category 5 Ethernet cable
- Access to PC network TCP/IP configuration

Step 1: Configure the PC to connect to the router and then launch Cisco SDM

a. Power up the router.

b. Power up the PC.

c. Disable any popup blocker programs. Popup blockers prevent SDM Express windows from displaying.

d. Connect the PC NIC to the FastEthernet 0/0 port on the Cisco 1841 ISR router with the Ethernet cable.

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

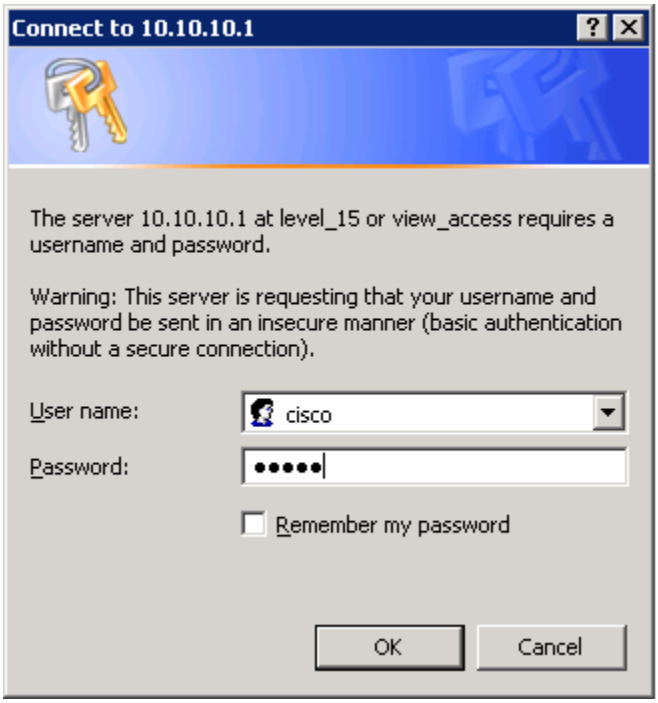
e. Configure the IP address of the PC to be 10.10.10.2 with a subnet mask of 255.255.255.248.

f. SDM does not load automatically on the router. You must open the web browser to reach the SDM. Open the web browser on the PC and connect to the following URL: http://10.10.10.1

NOTE 1 – If browser connection to router fails: If you cannot connect and see the login screen, check your cabling and connections and make sure the IP configuration of the PC is correct. The router may have been previously configured to an address of 192.168.1.1 on the Fa0/0 interface. Try setting the IP address of the PC to 192.168.1.2 with a subnet mask of 255.255.255.0 and connect to http://192.168.1.1 using the browser. If you have difficulty with this procedure, contact your instructor for assistance.

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor.

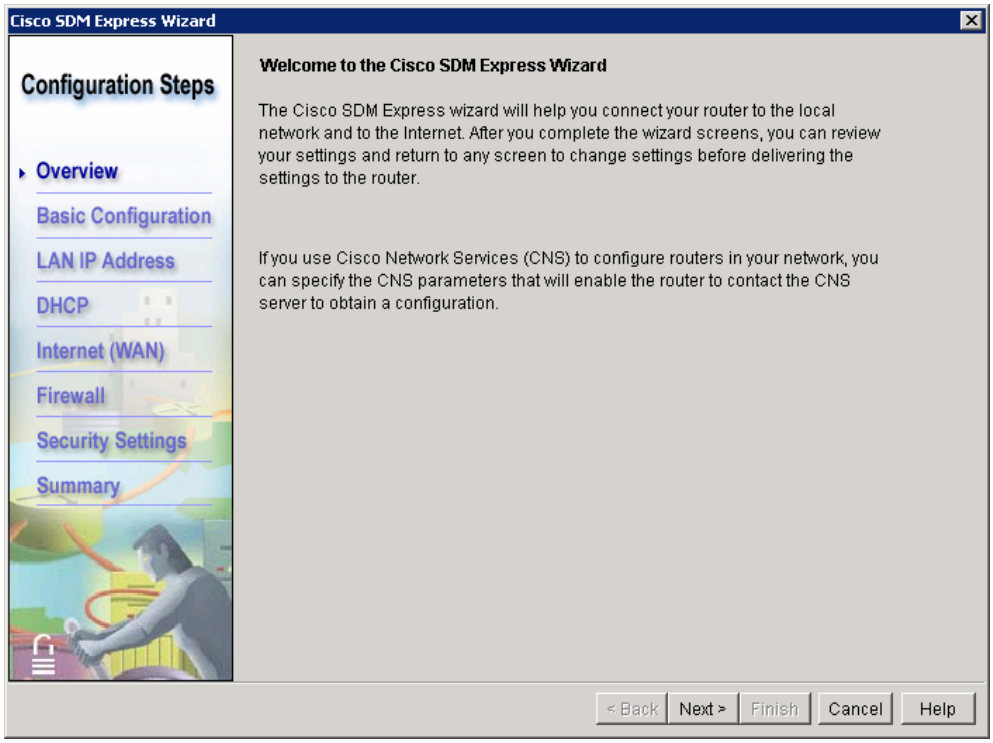
g. In the **Connect to** dialog box, enter **cisco** for the username and **cisco** for the password. Click **OK**. The main SDM web application will start and you will be prompted to use HTTPS. Click **Cancel**. In the Security Warning window, click **Yes** to trust the Cisco application.



h. In the Welcome to the Cisco SDM Express Wizard window, read the message and then click **Next**.

i. Verify that you are using the latest version of SDM. The initial SDM screen that displays immediately after the login shows the current version number. It is also displayed on the main SDM screen shown below, along with IOS version.

NOTE 2: If the current version is not 2.4 or higher, notify your instructor before continuing with this lab. You will need to download the latest zip file from the URL listed above and save it to the PC. From the Tools menu of the SDM GUI, use the **Update SDM** option to specify the location of the zip file and start the update.



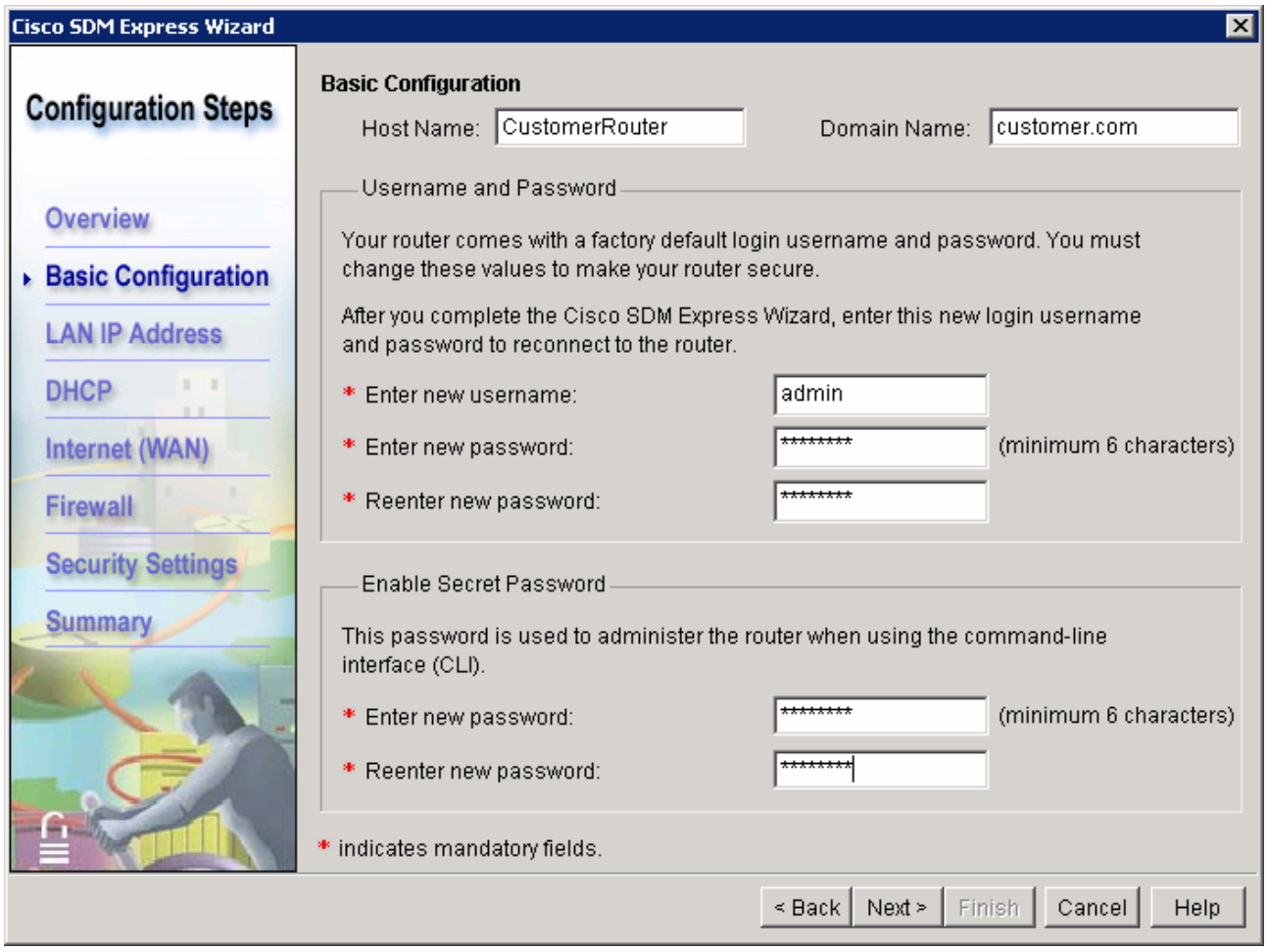
NOTE 3 – If SDM Express Wizard fails to start: If you connect to the router and SDM Express starts but the SDM Express Setup Wizard shown above does not start automatically, the router may be partially configured and needs to be reset to its factory defaults. If the SDM Express main screen is displayed, choose the **Reset to Factory Defaults** option, repeat Steps 1a through 1e, and log in again. If the full SDM application starts (not SMD Express), choose the **Reset to Factory Defaults** option from the **File** menu on the main SDM screen, repeat Steps 1a through 1e, and log in again. If you have difficulty with this procedure, contact your instructor for assistance.

Also note that the Windows XP computer you are using must have Internet Explorer 5.5 or higher and SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810). If it does not, SDM will not start. You will need to download and install JRE on the PC before continuing with the lab.

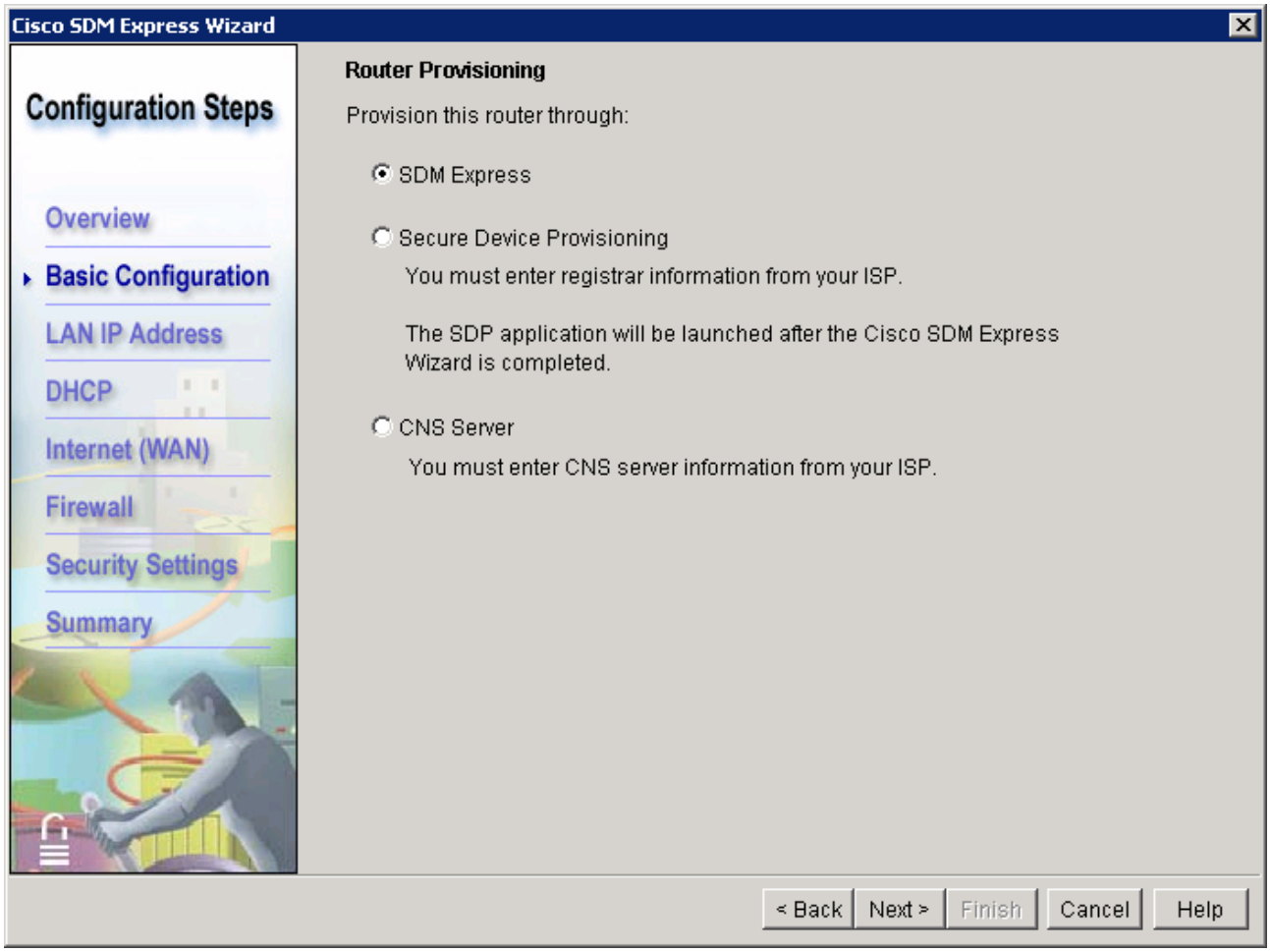
Step 2: Perform initial basic configuration

a. In the Basic Configuration window, enter the following information. When you complete the basic configuration, click **Next** to continue.

- In the Host Name field, enter **CustomerRouter**.
- In the Domain Name field, enter the domain name **customer.com**.
- Enter the username **admin** and the password **cisco123** for SDM Express users and Telnet users. This password gives access to SDM locally, through the console connection, or remotely using Telnet.
- Enter the **enable secret password** of **cisco123**. This entry creates an encrypted password that prevents casual users from entering privileged mode and modifying the configuration of the router using the CLI.

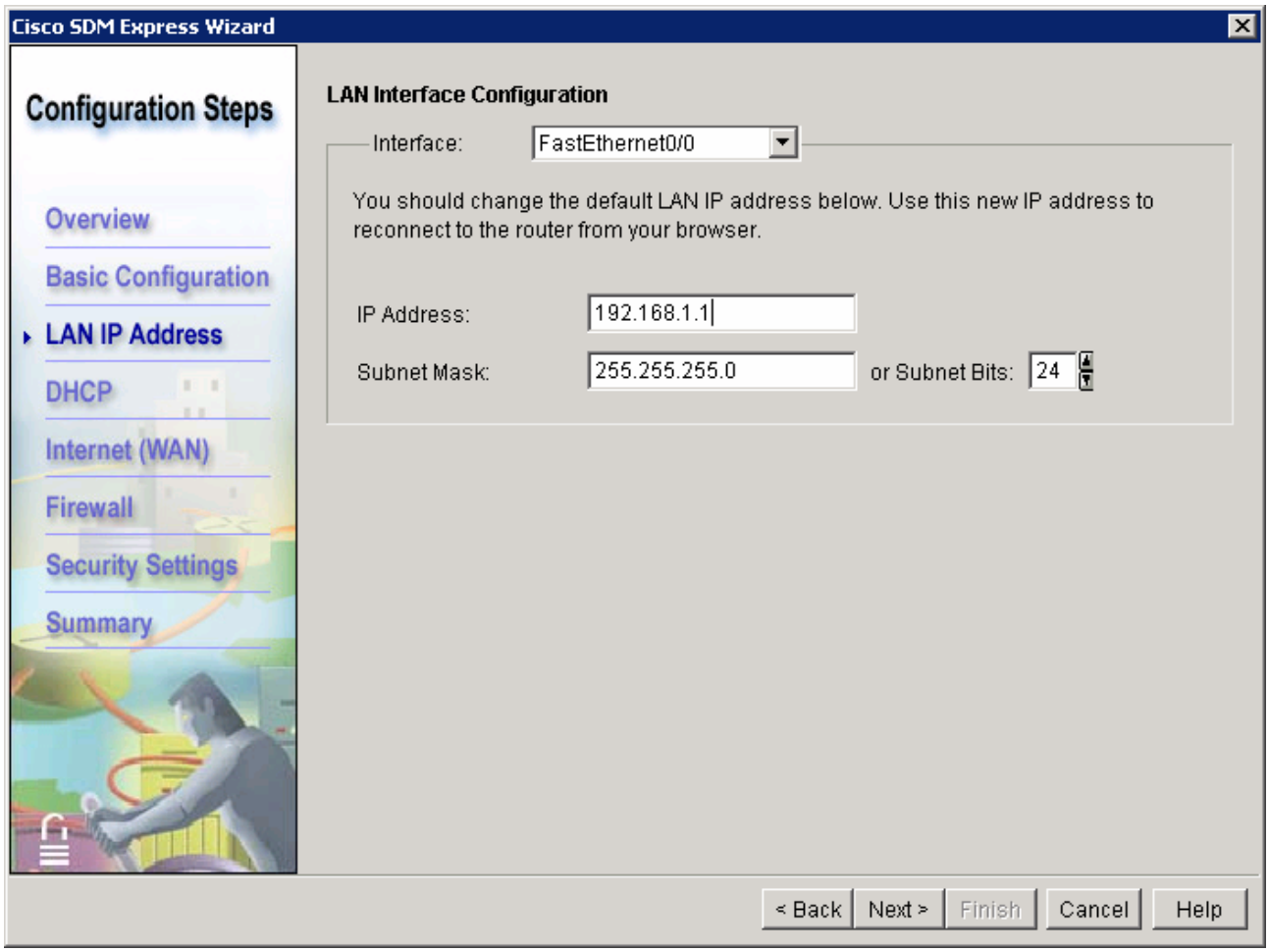


b. From the Router Provisioning window, click the radio button next to SDM Express and then click **Next**.



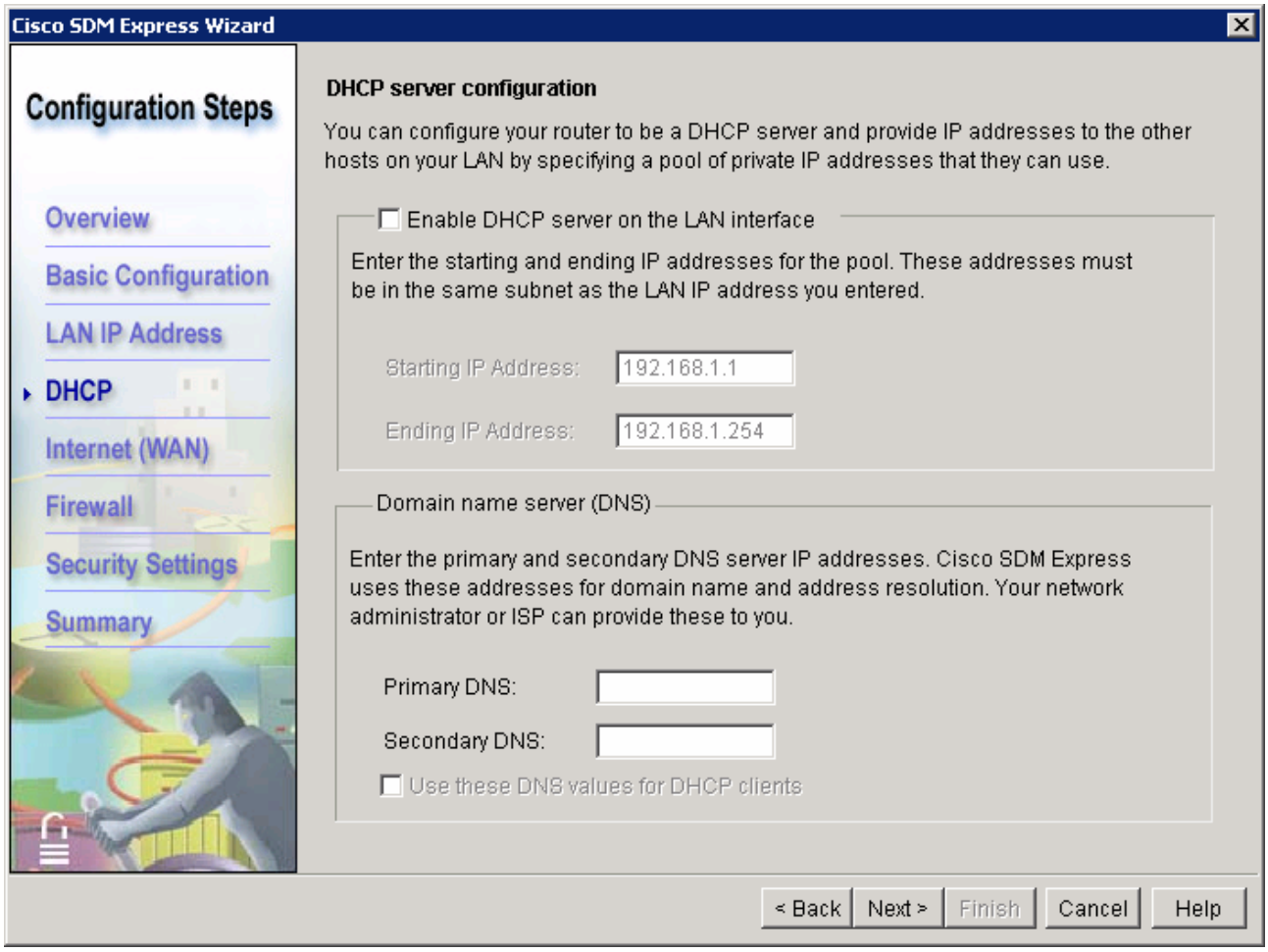
Step 3: Configure the LAN IP address

In the LAN Interface Configuration window, choose **FastEthernet0/0** from the Interface list. For interface FastEthernet 0/0, enter the IP address of 192.168.1.1 and subnet mask of 255.255.255.0. You can also enter the subnet mask information in a different format: entering a count of the number of binary digits or bits in the subnet mask, such as 255.255.255.0 or 24 subnet bits.



Step 4: De-select DHCP server

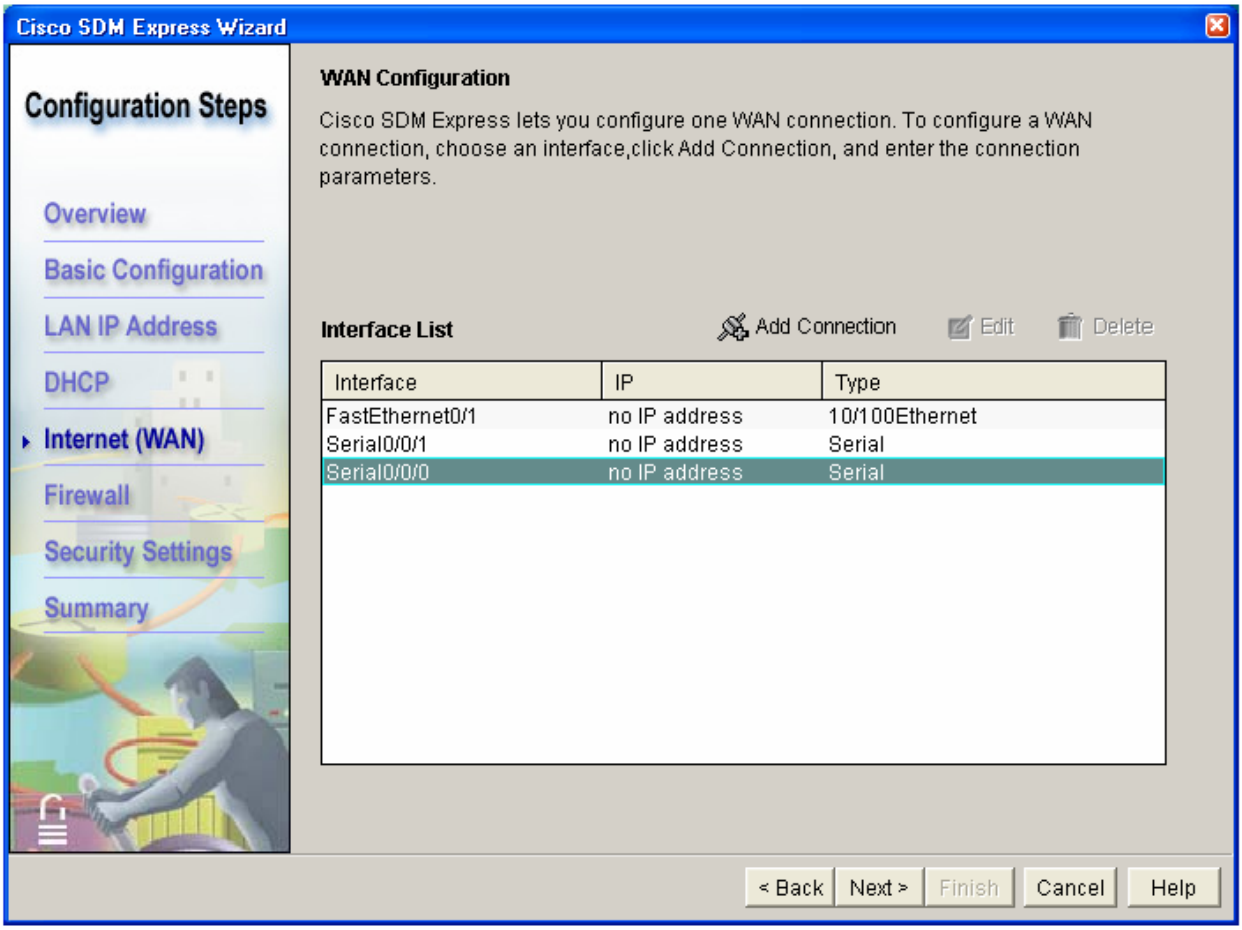
At this point, do not enable the DHCP server. This procedure is covered in a later section of this course. In the DHCP server configuration window, ensure that the Enable DHCP server on the LAN interface check box is cleared before proceeding. Click **Next** to continue.



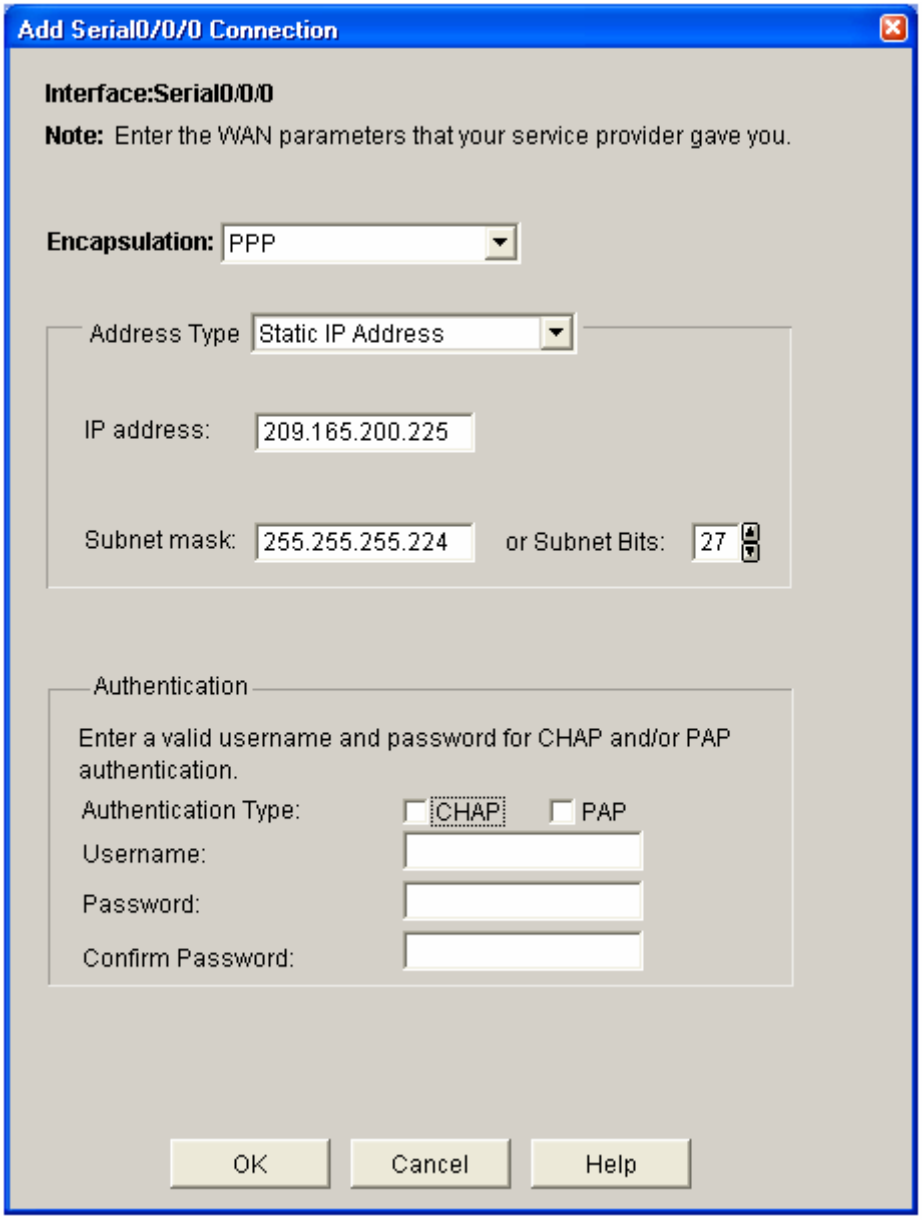
Step 5: Configure the WAN interface

a. In the WAN Configuration window, choose **Serial0/0/0** interface from the list and click the **Add Connection** button. The Add Connection window appears.

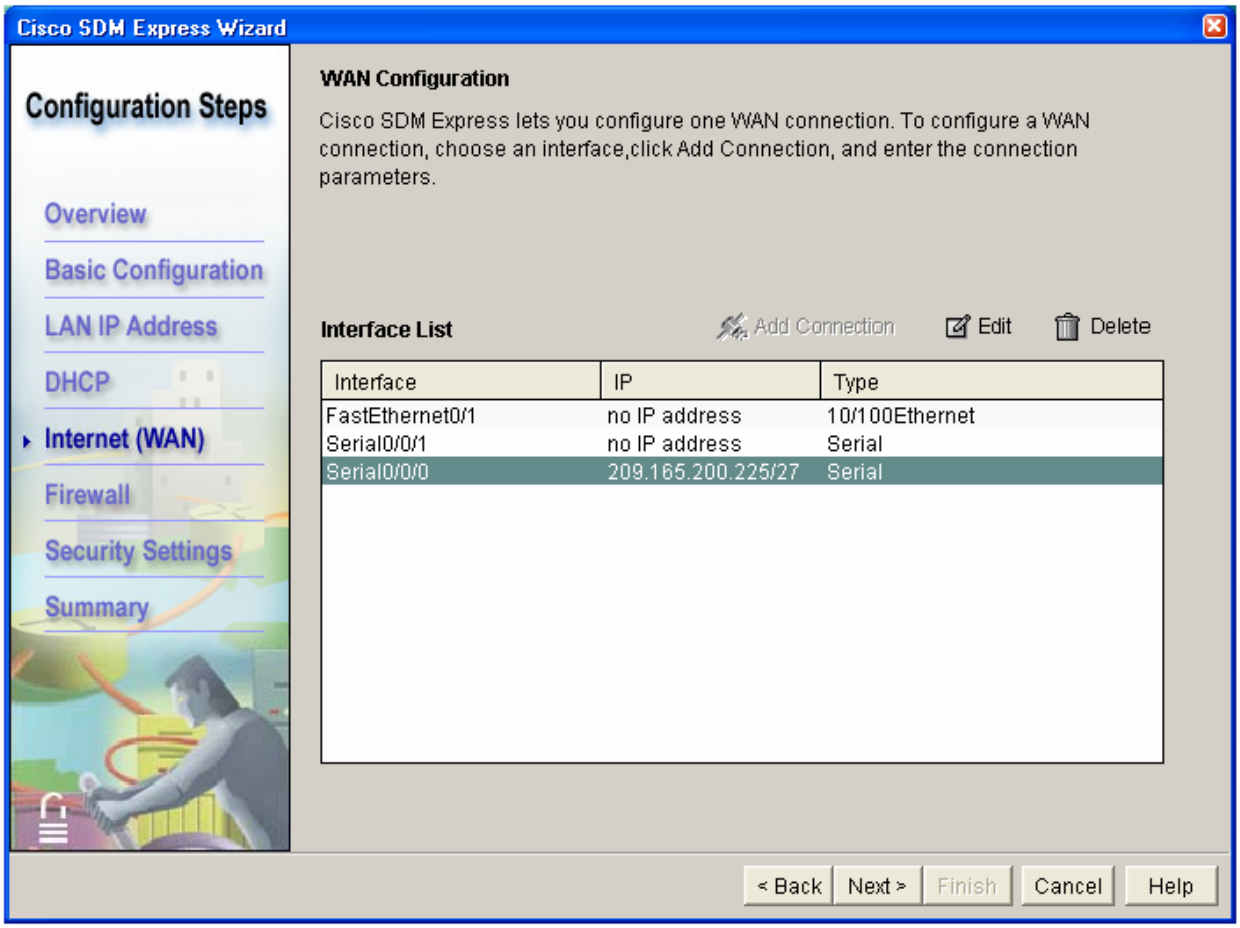
NOTE: With the 1841 router, the serial interface is designated by 3 digits – C/S/P, where C=Controller#, S=Slot# and P=Port#. The 1841 has two modular slots. The designation Serial0/0/0 indicates that the serial interface module is on controller 0, in slot 0, and that the interface to be used is the first one (0). The second interface is Serial0/0/1. The serial module is normally installed in slot 0 but may be may be installed in slot 1. If this is the case, the designation for the first serial interface on the module would be Serial0/1/0 and the second would be Serial0/1/1.



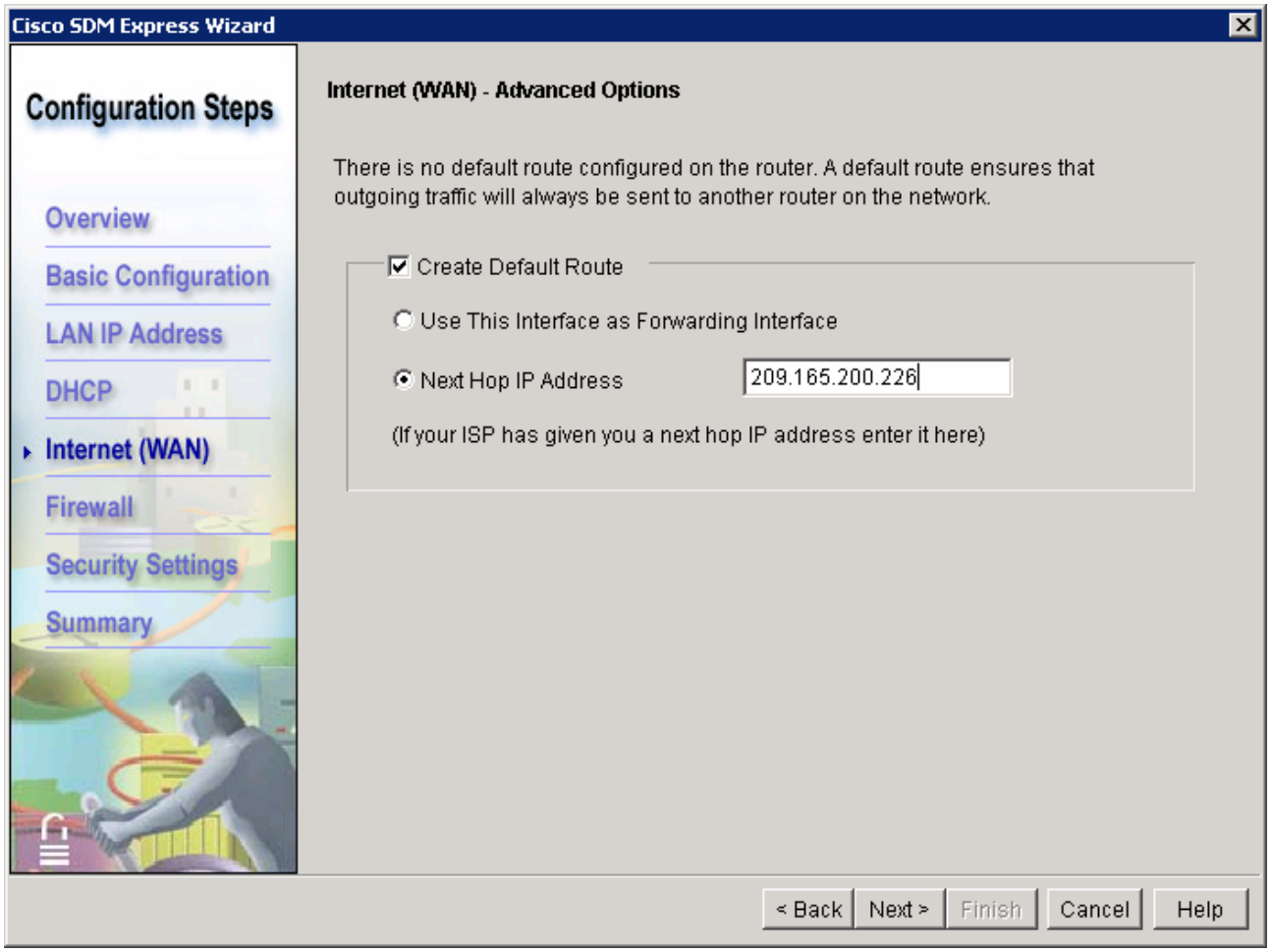
b. From the Add Serial0/0/0 Connection dialog box, choose **PPP** from the Encapsulation list. From the Address Type list, choose **Static IP Address**. Enter **209.165.200.225** for the IP address and **255.255.255.224** for the Subnet mask. Click **OK** to continue. Notice that this subnet mask translates to a /27, or 27 bits for the mask.



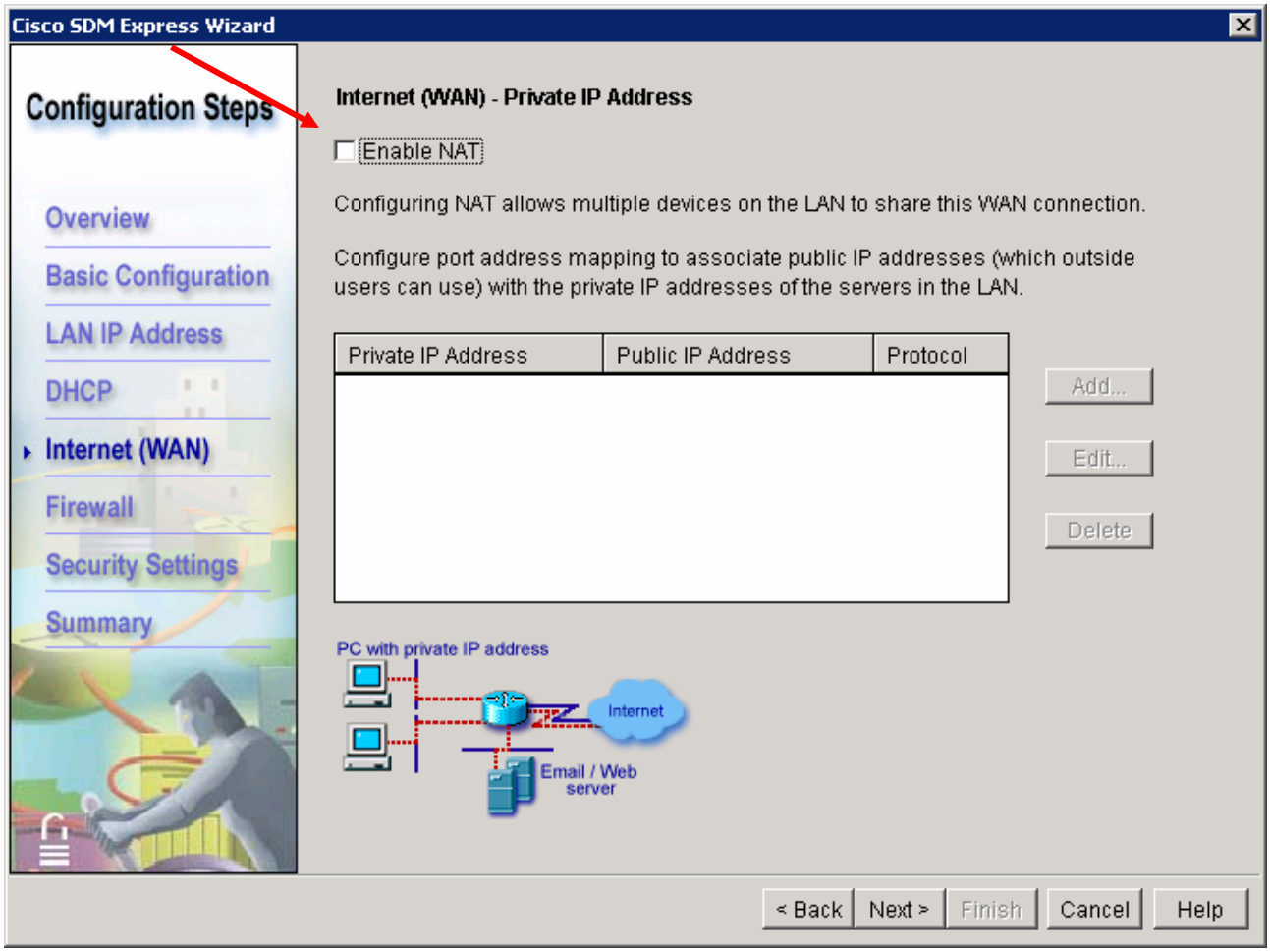
c. Notice that the IP address that you just set for the serial WAN interface now appears in the Interface List. Click **Next** to continue.



d. Enter the IP address **209.165.200.226** as the Next Hop IP Address for the Default Route. Click **Next** to continue.

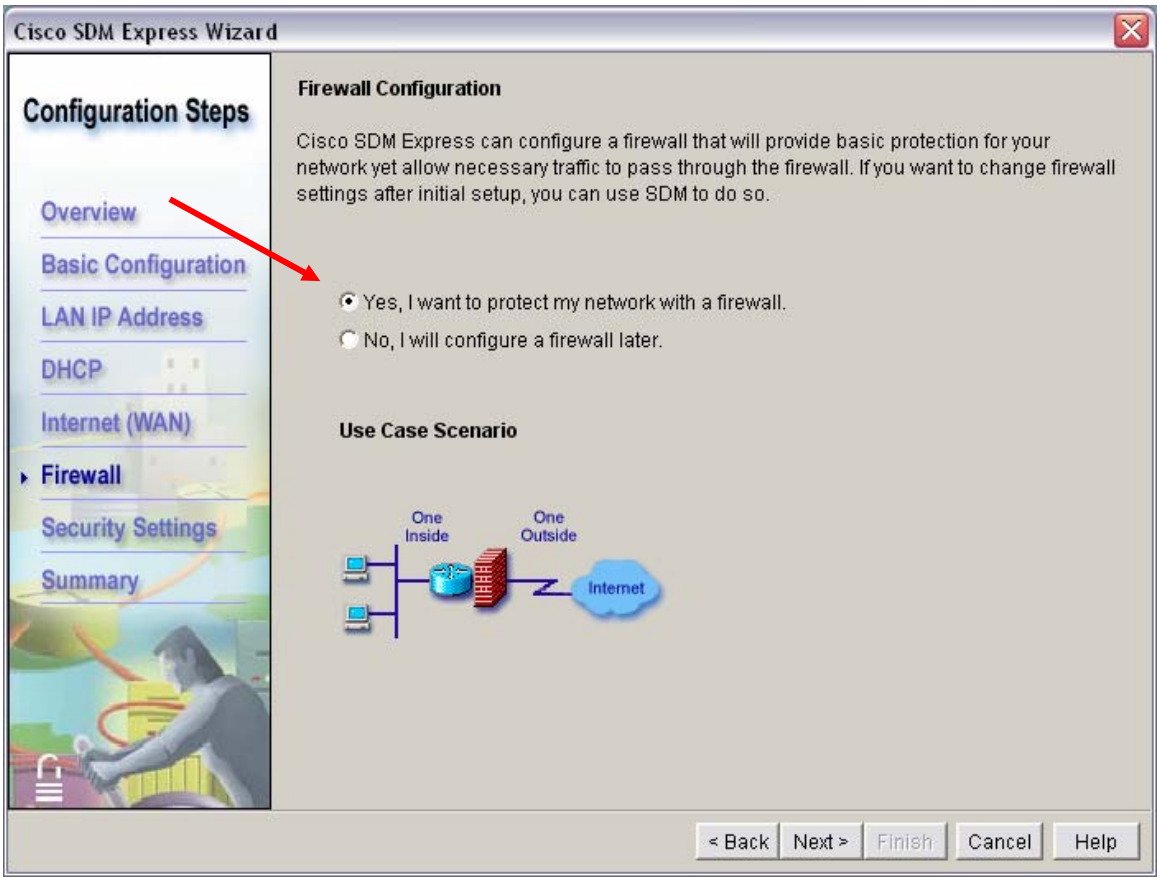


e. Ensure that the check box next to Enable NAT is cleared. This procedure is covered in a later section of this course. Click **Next** to continue.

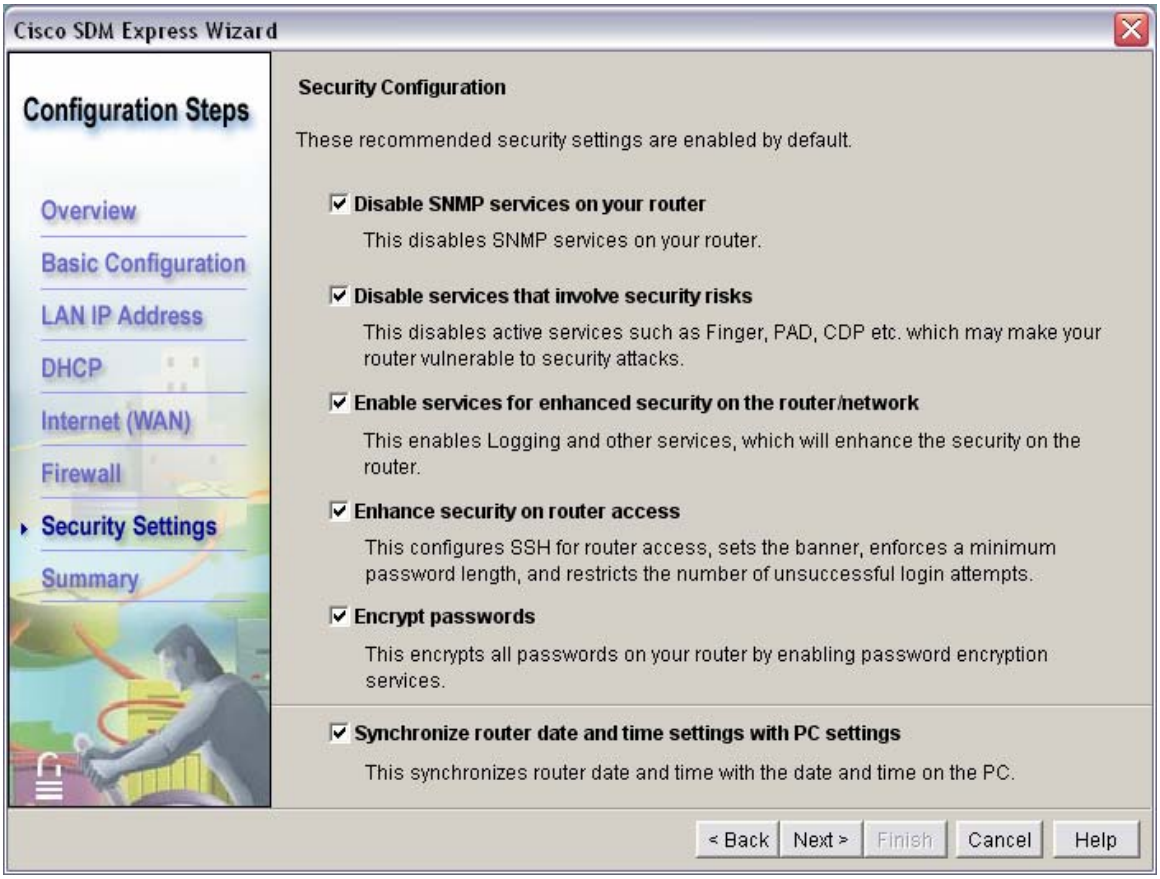


Step 6: Enable the firewall and security settings

a. Depending on the router IOS version, the next step may be Firewall Configuration. In the Firewall Configuration window, click the radio button that enables the firewall and then click **Next**. The Security Configuration window appears.

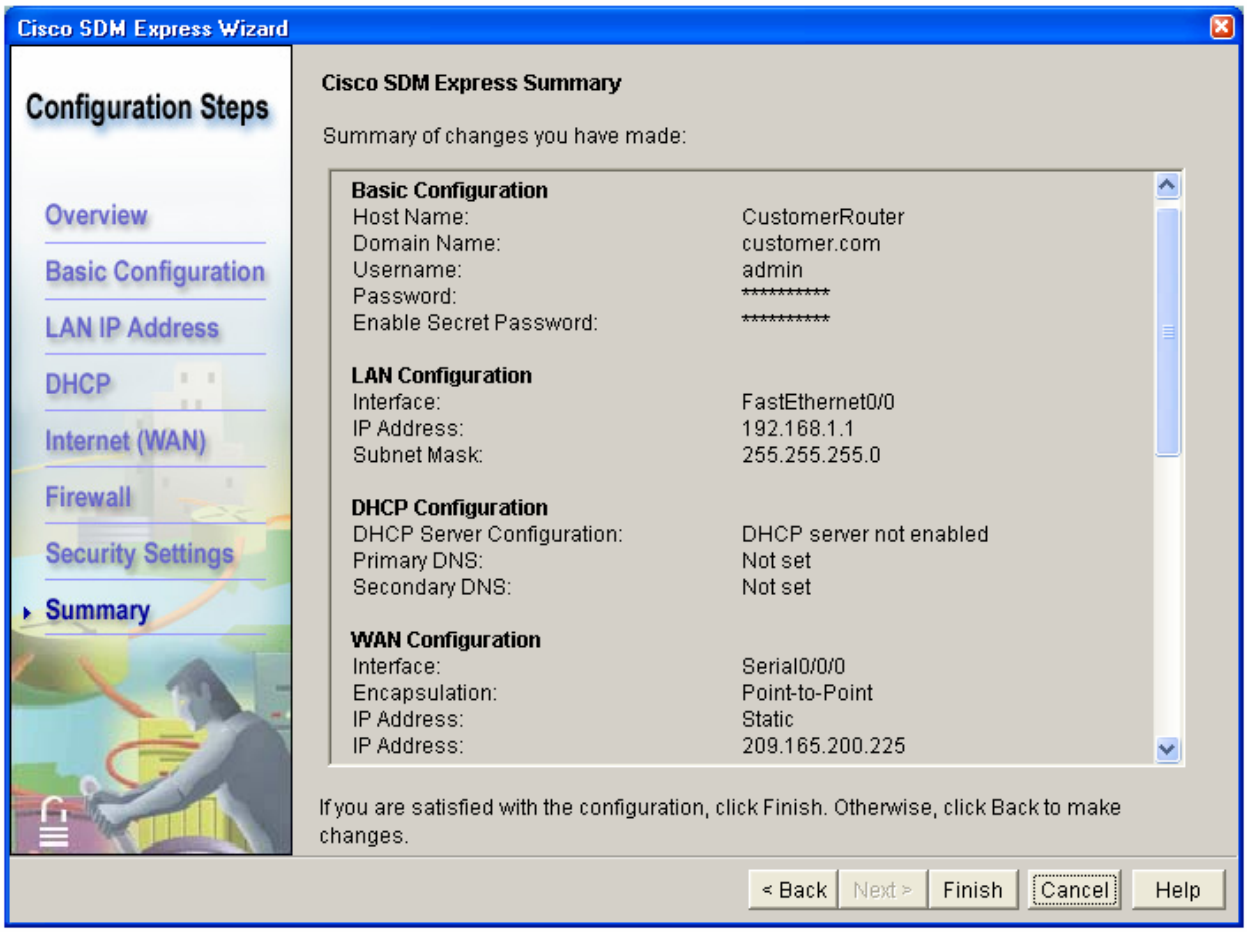


b. Leave all the default security options checked in the Security Configuration window and then click **Next**.



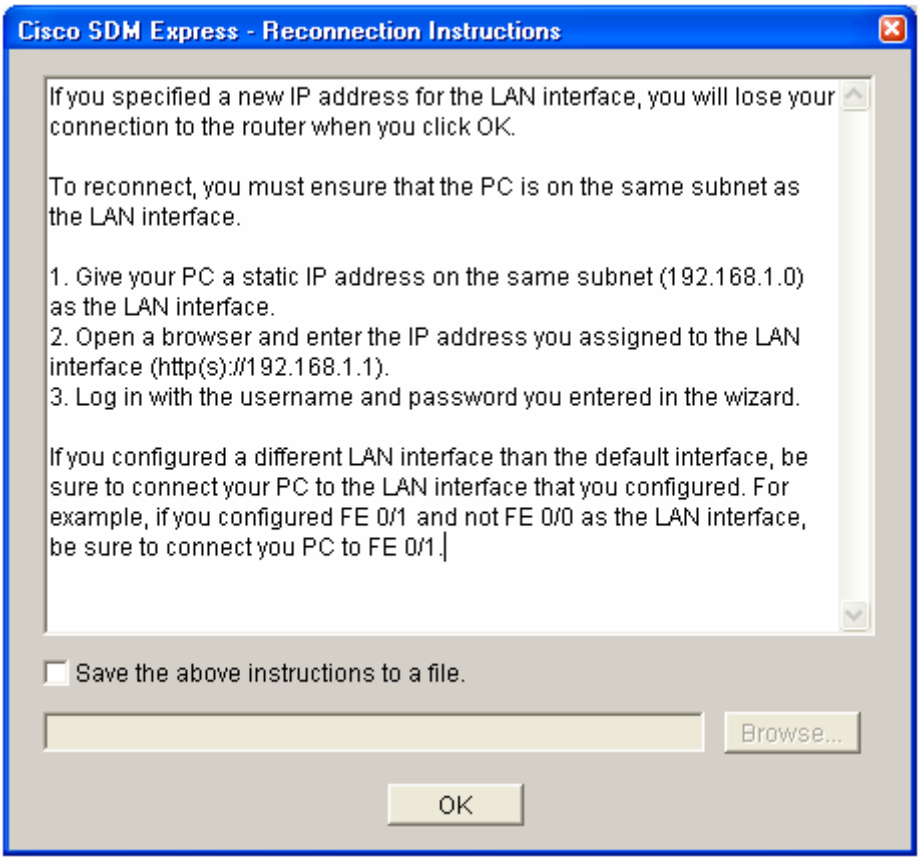
Step 7: Review and complete the configuration

a. If you are not satisfied with the Cisco SDM Express Summary, click **Back** to fix any changes and then click **Finish** to commit the changes to the router.

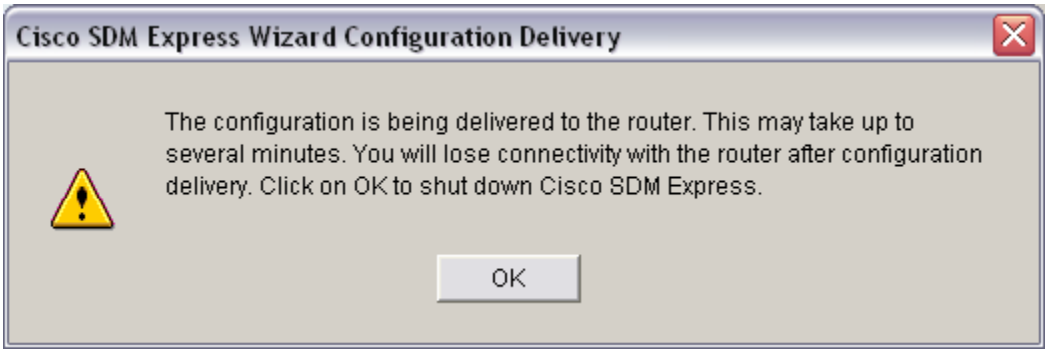


b. Click **OK** after reading the Reconnection Instructions. Save these instructions to a file for future reference, if desired.

NOTE: Before the next time you connect, you will need to change the IP address of the PC to be compatible with the new address that you configured to FastEthernet 0/0. The Reconnection instructions are shown below.



c. When the delivery of the configuration to the router is complete. Click **OK** to close Cisco SDM Express.



Step 8: Reflection

a. What feature makes configuring the router easy? _____

_____

b. Summarize the steps that are configured by the Cisco SDM Express

_____

_____

_____

_____

_____

_____

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

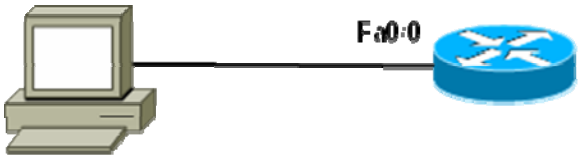
NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

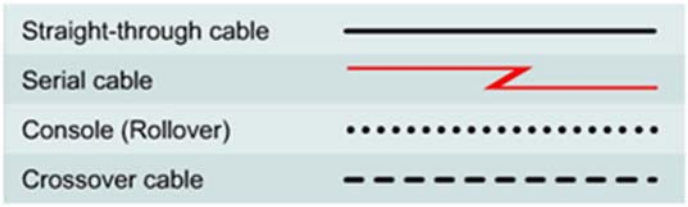
```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the HTTP/HTTPS server of the router, using the following Cisco
IOS commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>

   Replace <username> and <password> with the username and password that
   you want to configure.
```


4) Configure SSH and Telnet for local login and privilege level 15:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Lab 5.2.5 Configuring Dynamic NAT with SDM





Objective

- Configure Network Address Translation (NAT) using Port Address Translation (PAT) on a Cisco ISR router with the Cisco SDM Basic NAT Wizard.

Background / Preparation

Cisco Router and Security Device Manager (SDM) is a Java-based web application and a device-management tool for Cisco IOS Software-based routers. The Cisco SDM simplifies router and security configuration through the use of smart wizards, which allows you to deploy, configure, and monitor a Cisco router without requiring knowledge of the command-line interface (CLI). The Cisco SDM is supported on a wide range of Cisco routers and Cisco IOS Software releases. Many newer Cisco routers come with SDM preinstalled. If you are using an 1841 router, SDM (and SDM Express) is pre-installed.

This lab assumes the use of a Cisco 1841 router. You can use another router model as long as it is capable of supporting SDM. If you are using a supported router that does not have SDM installed, you can download the latest version free of charge from the following location: http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

From the URL shown above, view or download the document “Downloading and Installing Cisco Router and Security Device Manager.” This document provides instructions for installing SDM on your router. It lists specific model numbers and IOS versions that can support SDM, and the amount of memory required.

Cisco SDM is the full SDM product, and SMD Express is a subset. SDM will be activated automatically when the router has been previously configured and is not in its factory default state. In this lab, you will use the Cisco SDM Basic NAT Wizard to configure Network Address Translation using a single external global IP address. This address can support connections to the Internet from many internal private addresses.

NOTE: You must complete Lab 5.2.3, “Configuring an ISR with SDM Express,” on the router to be used before performing this lab. This lab assumes that the router has been previously configured with basic settings using SDM Express.

The following resources are required.

- Cisco 1841 ISR router with SDM version 2.4 installed and with basic configuration completed (critical – see Note 2 in Step 1)
- (Optional) Other Cisco router model with SDM installed
- Windows XP computer with Internet Explorer 5.5 or higher and SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810).
- Straight-through or crossover category 5 Ethernet cable
- Access to PC network TCP/IP configuration

Step 1: Establish a connection from the PC to the router

a. Power up the router.

b. Power up the PC.

c. Disable any popup blocker programs. Popup blockers prevent SDM windows from displaying.

d. Connect the PC NIC to the FastEthernet 0/0 (Fa0/0) port on the Cisco 1841 ISR router with the Ethernet cable.

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

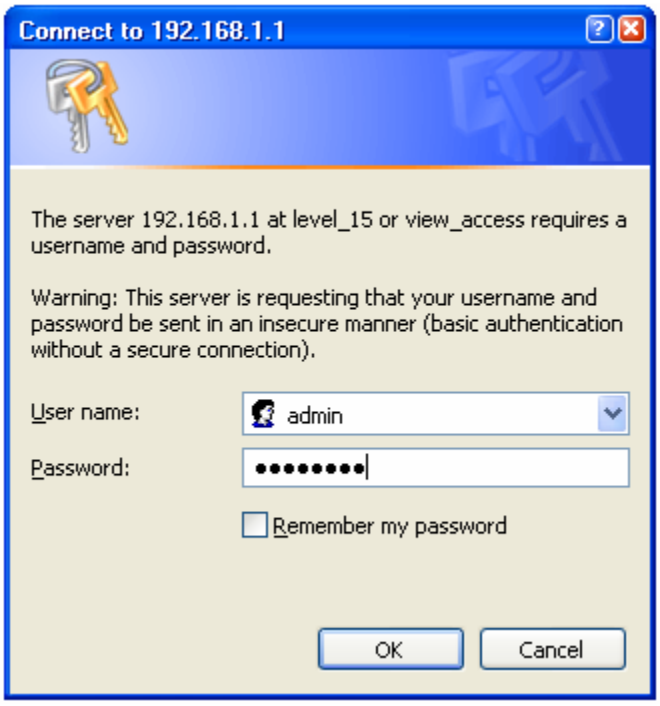
e. Configure the IP address of the PC to be 192.168.1.2 with a subnet mask of 255.255.255.0.

f. SDM does not load automatically on the router. You must open the web browser to reach the SDM. Open the web browser on the PC and connect to the following URL: http://192.168.1.1

NOTE 1 – If browser connection to router fails" If you cannot connect and see the login screen, check your cabling and connections and make sure the PC's IP configuration is correct. If the router was not previously configured, it may still be in the default state with an IP address of 10.10.10.1 on the Fa0/0 interface. Try setting the IP address of the PC to 10.10.10.2 with a subnet mask of 255.255.255.248 and connect to http://10.10.10.1 using the browser. If you have difficulty with this procedure, contact your instructor for assistance.

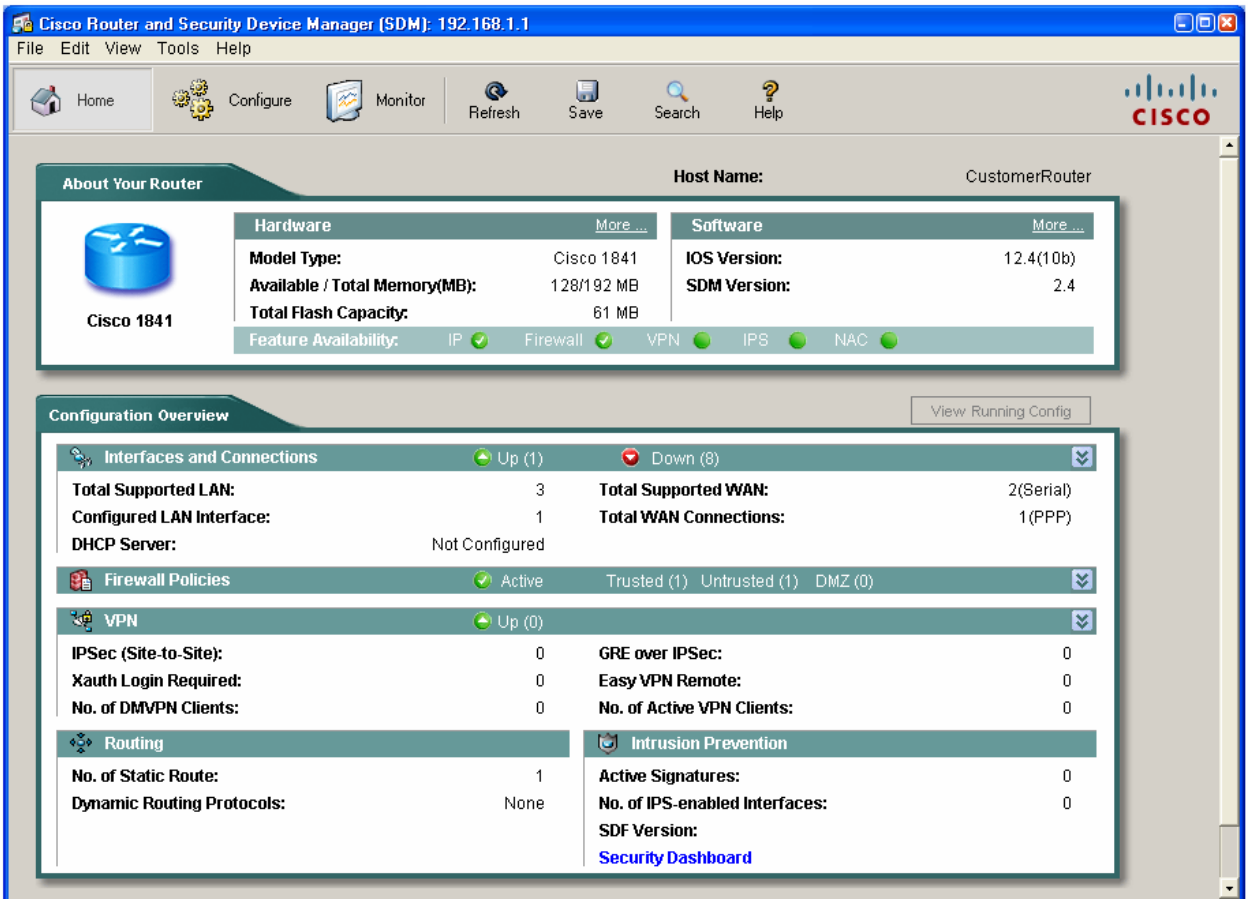
SDM Routers - If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor

g. In the **Connect to** dialog box, enter **admin** for the username and **cisco123** for the password. These were configured in the previous lab. Click **OK**. The main SDM web application will start and you will be prompted to use HTTPS. Click **Cancel**. In the Security Warning window, click **Yes** to trust the Cisco application.



h. Verify that you are using the latest version of SDM. The initial SDM screen that displays immediately after the login shows the current version number. It is also displayed on the main SDM screen shown below, along with IOS version.

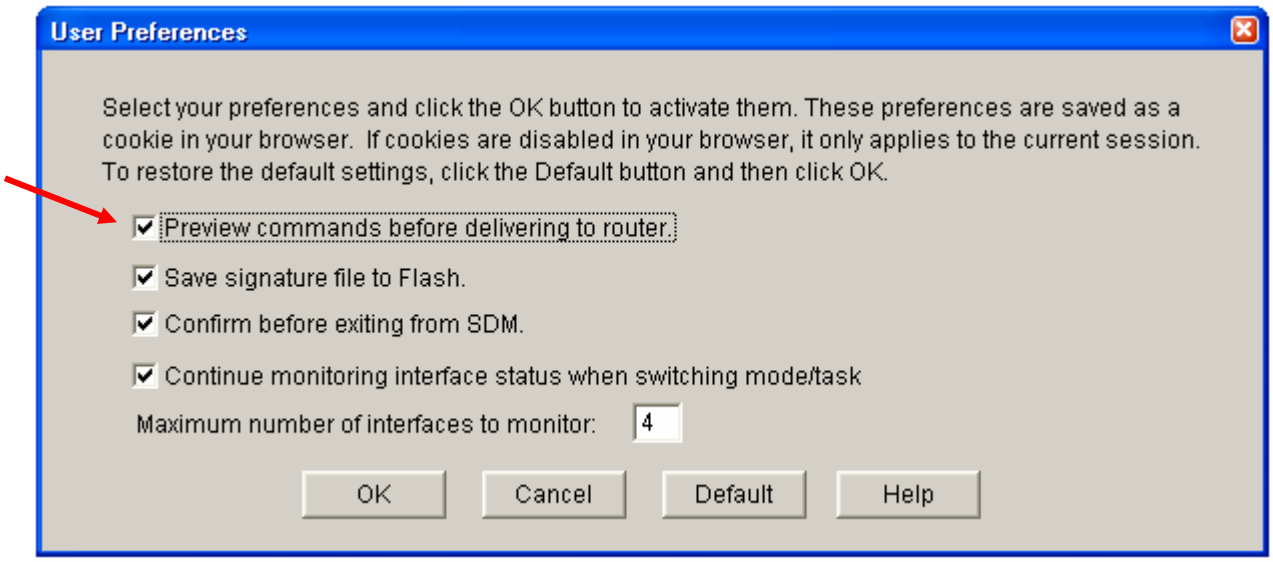
NOTE 2: If the current version is not 2.4 or higher, notify your instructor before continuing with this lab. You will need to download the latest zip file from the URL listed above and save it to the PC. From the **Tools** menu of the SDM GUI, use the **Update SDM** option to specify the location of the zip file and install the update.



Step 2: Configure SDM to show Cisco IOS CLI commands.

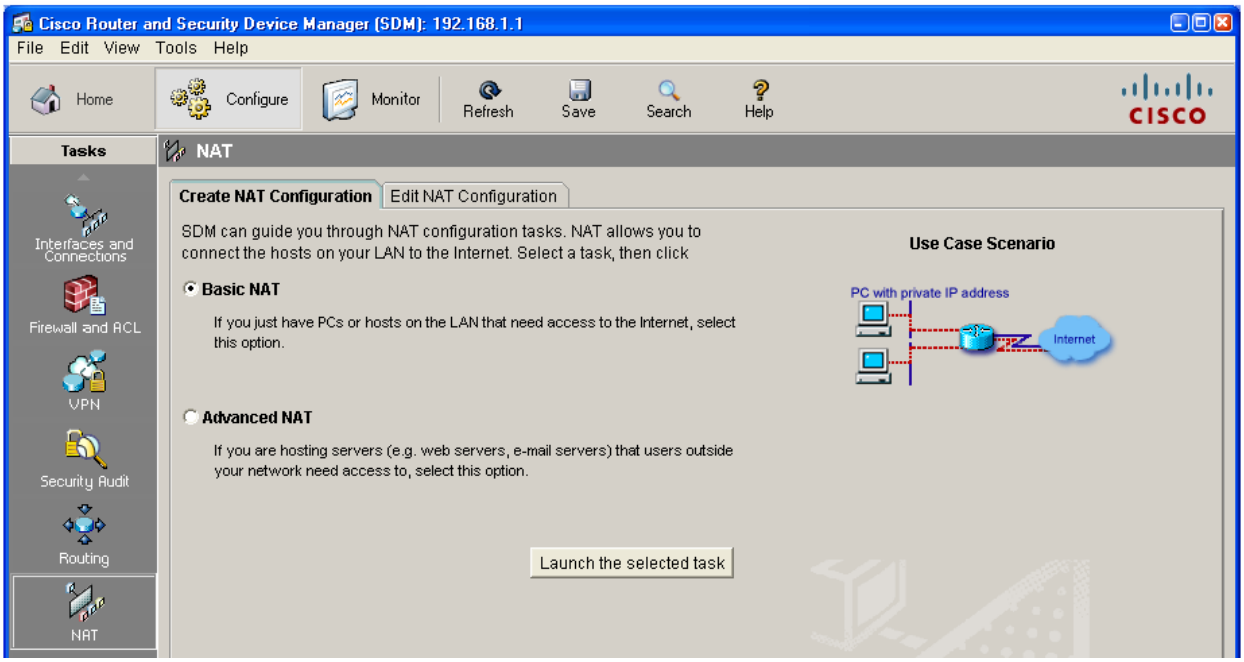
a. From the **Edit** menu in the main SDM window, select **Preferences**.

b. Check the **Preview commands before delivering to router** check box. With this check box checked, you can see the Cisco IOS CLI commands that you will use to perform a configuration function on the router before these commands are sent to the router. You can learn about Cisco IOS CLI commands this way.

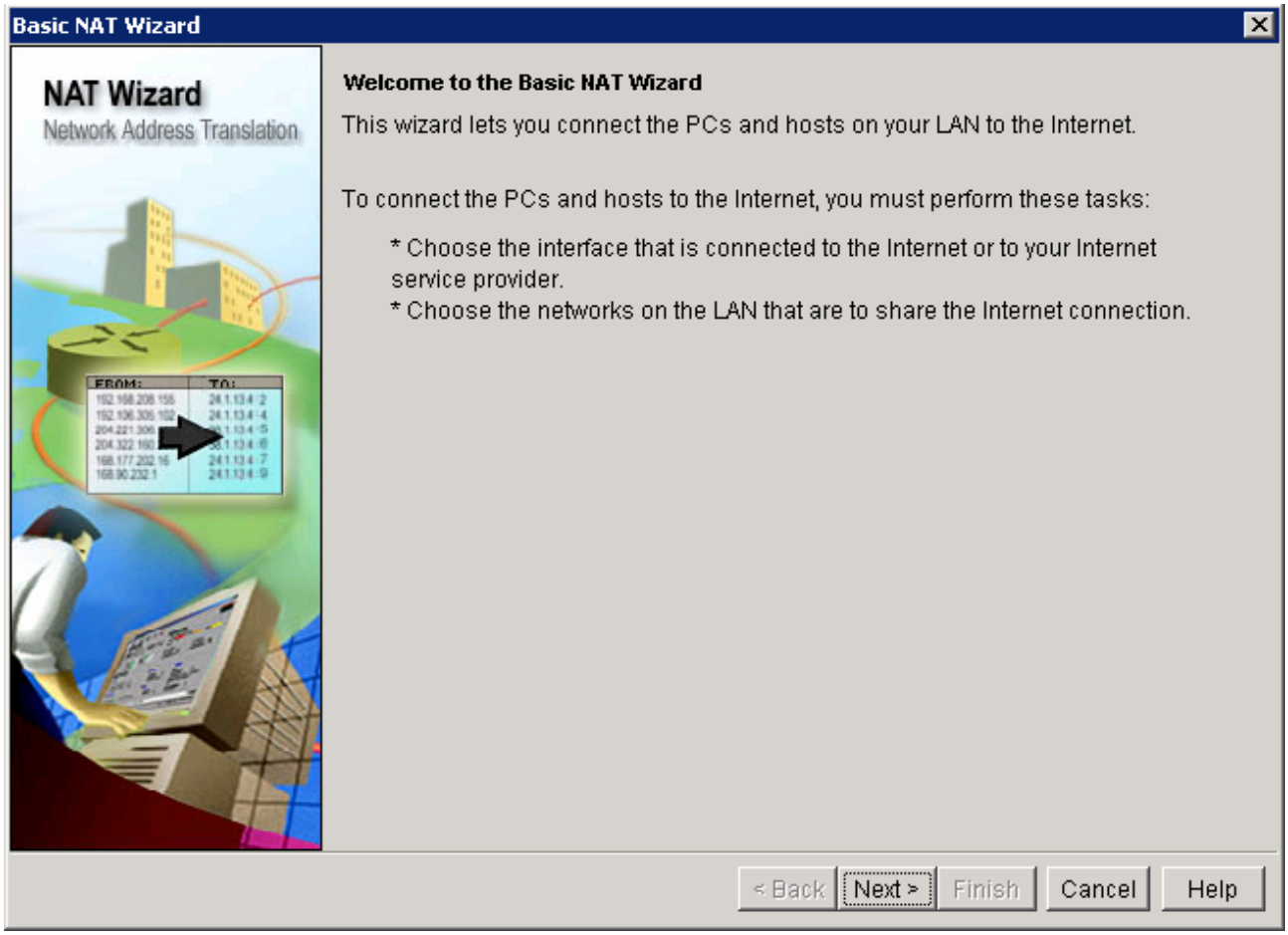


Step 3: Launch the Basic NAT Wizard

a. From the **Configure** menu, click the **NAT** button to view the NAT configuration page. Click the **Basic NAT** radio button and then click **Launch the selected task**.

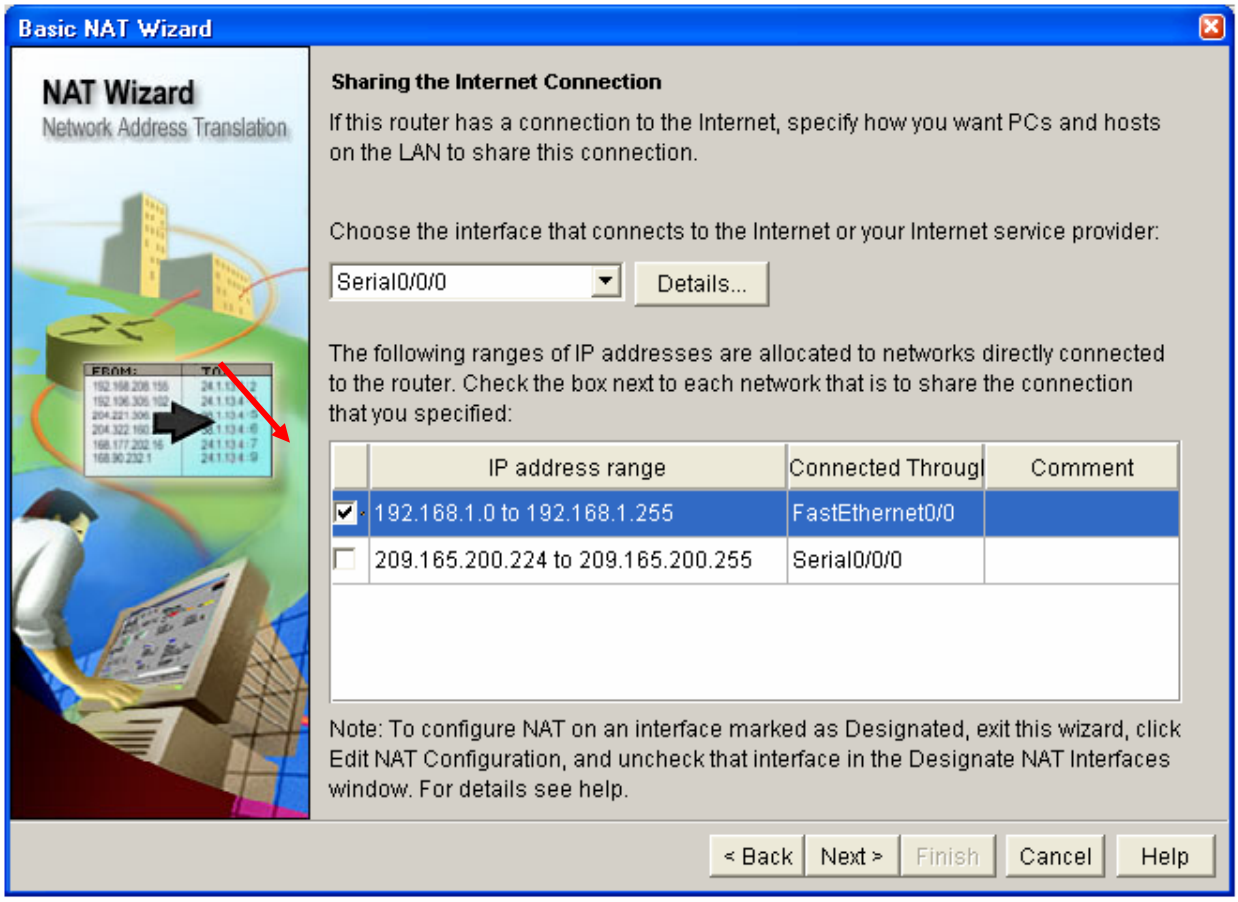


b. In the Welcome to the Basic NAT Wizard window, click **Next**.

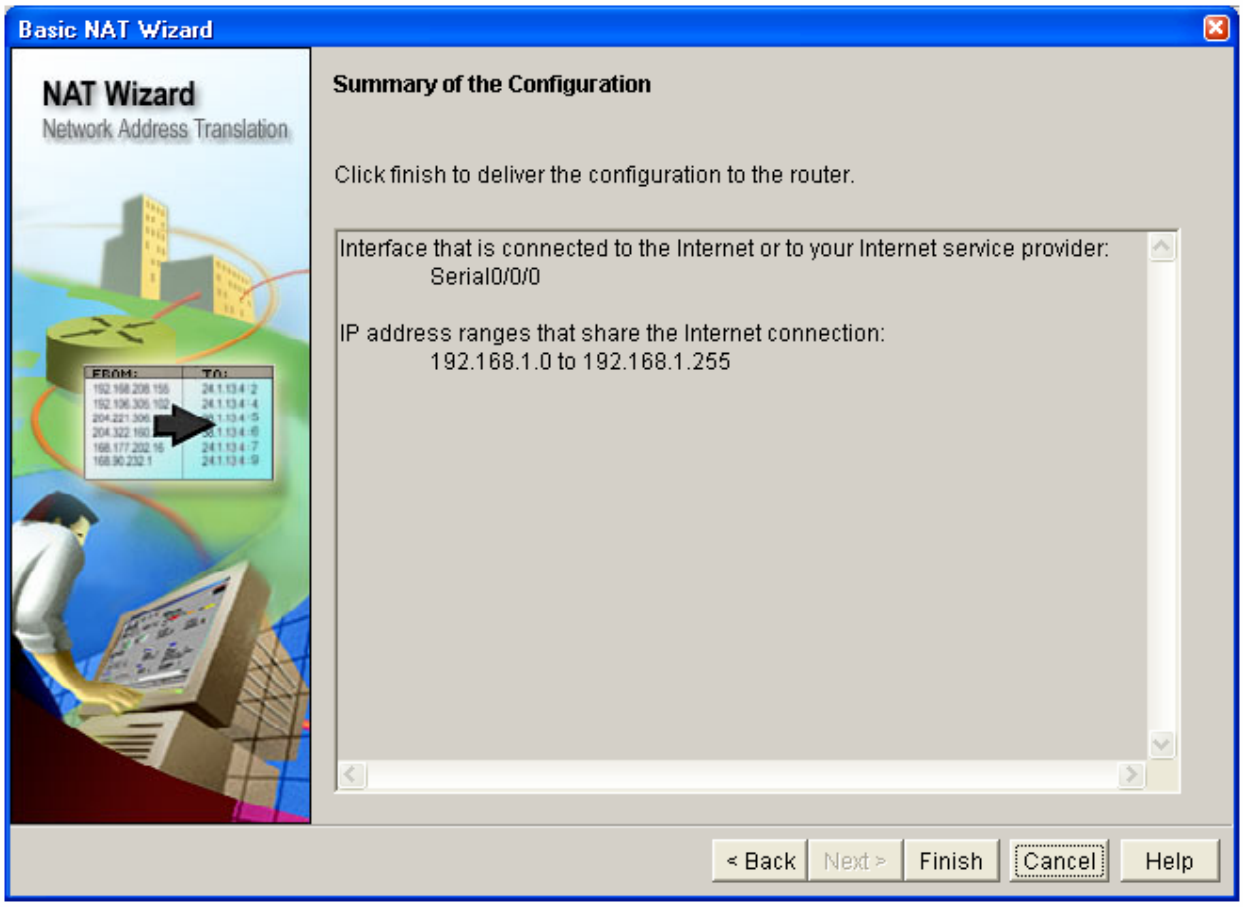


Step 4: Select the WAN interface for NAT

a. Choose the WAN interface **Serial0/0/0** from the list. Check the box for the IP address range that represents the internal network of 192.168.1.0 to 192.168.1.255. This is the range that requires conversion using the NAT process.



b. Click **Next** and, once you have read the Summary of the Configuration, click **Finish.**

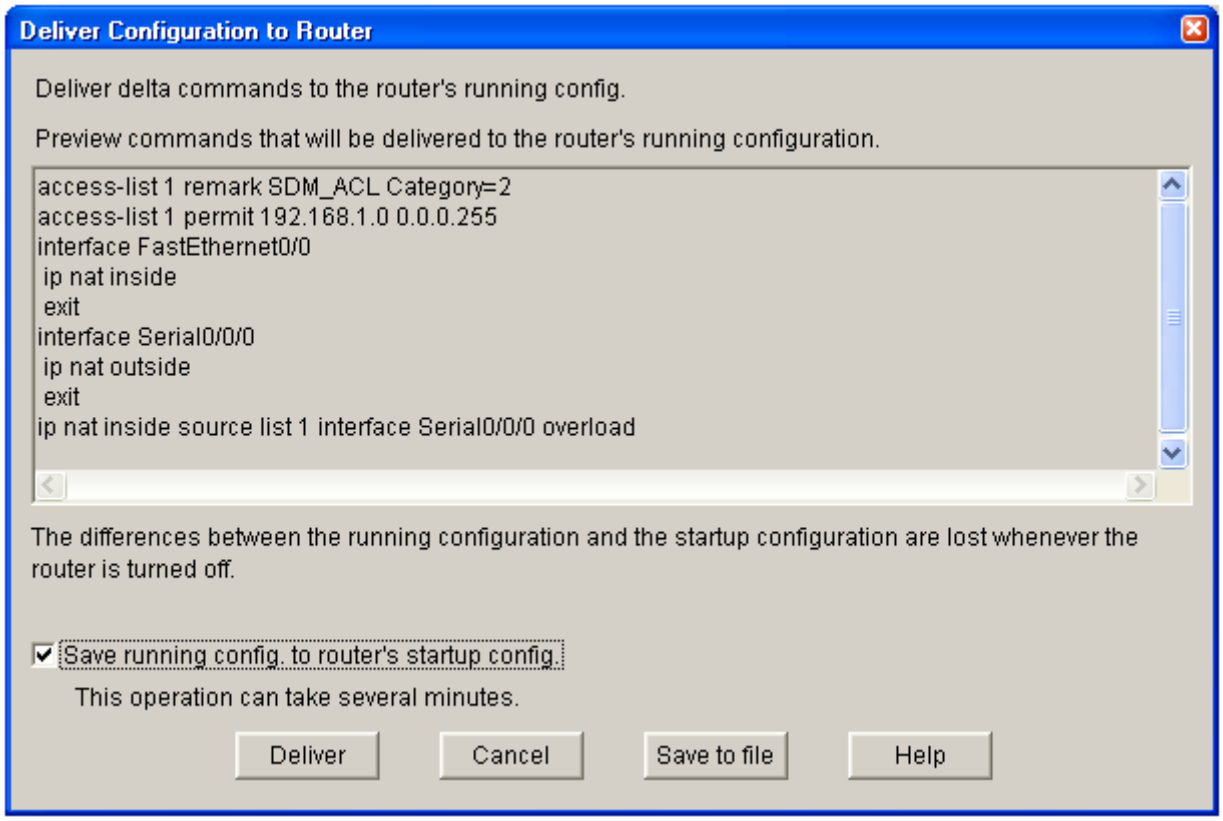


c. In the Deliver Configuration to Router window, review the CLI commands that were generated by the Cisco SDM. These are the commands that will be delivered to the router to configure NAT. The commands can also be manually entered from the CLI to accomplish the same task. Check the box for **Save running config. to router's startup config**.

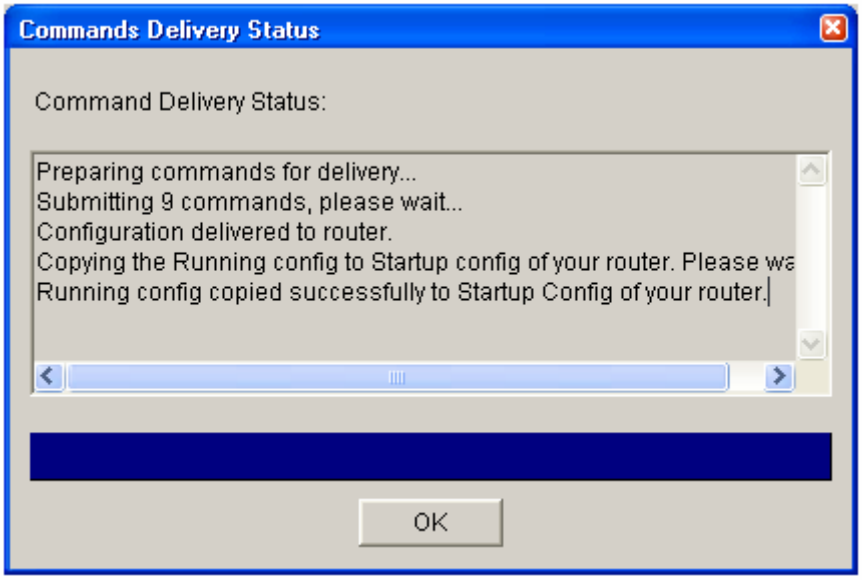
NOTE: By default, the commands that you just generated will only update the router's running configuration file when delivered. If the router is restarted, the changes you made will be lost. Checking this box will update the startup config file as well, and when the router is restarted, it will load the new commands into the running config.

If you choose to not save the commands to the startup config at this time, use the **File > Write to Startup config** option in SDM or use the **copy running-config startup-config** command from the CLI using a terminal or Telnet session.

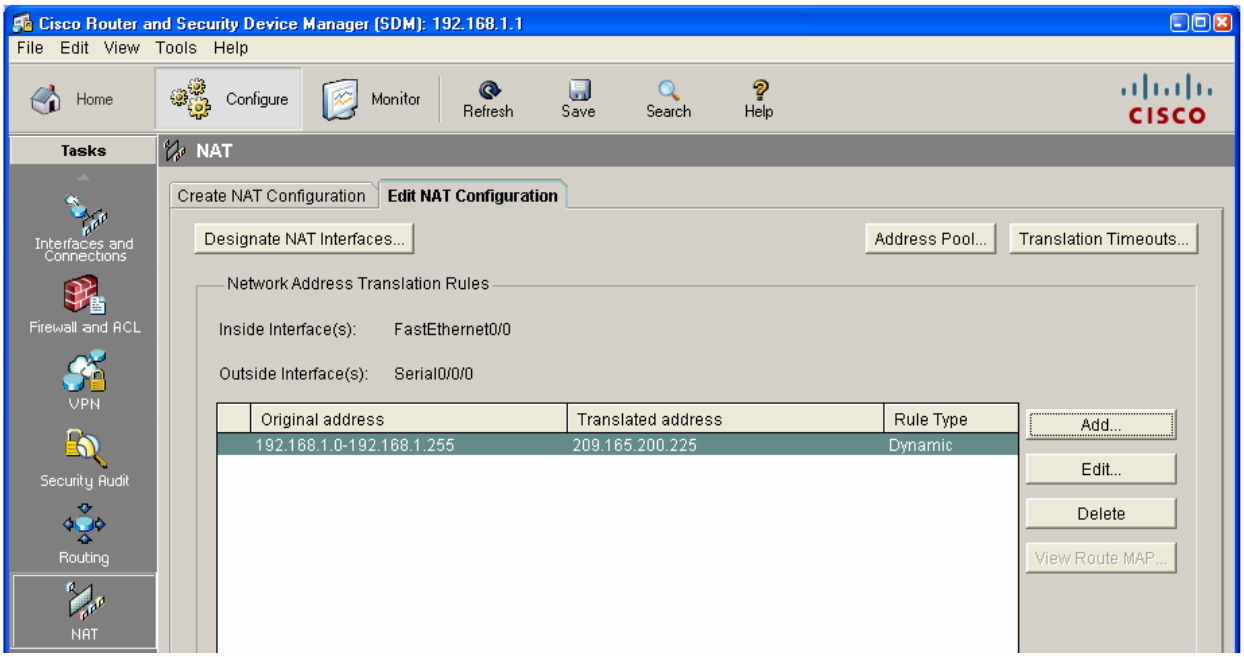
d. Click **Deliver** to finish configuring the router.



e. In the Commands Delivery Status window, notice the text that says that the running config was successfully copied to the startup config. Click **OK** to exit the Basic NAT wizard.



f. The final NAT screen shows that the Inside Interface is Fa0/0 and the outside interface is S0/0/0. The internal private (Original) addresses will be translated dynamically to the external public address.



Step 5: Reflection

a. If a PC or a LAN within your organization does not require Internet access, what do you think would be one way to stop the PC from gaining access to the Internet?

_____

_____

_____

b. Consider the skills that you need to configure NAT using Cisco IOS CLI commands. What do you think the benefits and disadvantages are to using the Cisco SDM?

_____

_____

_____

_____

_____

_____

c. Why do you think that the default, after the commands have been generated, is to only update the router's running configuration file when delivered? Why not always update the startup config file as well? What are the advantages and disadvantages of one over the other?

_____

_____

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

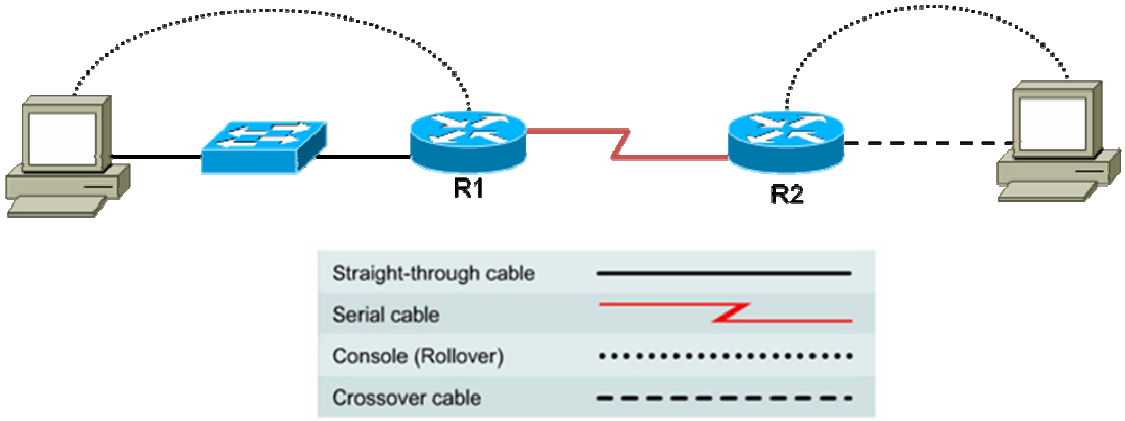
http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the router's HTTP/HTTPS server, using the following Cisco IOS
commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>

   Replace <username> and <password> with the username and password that
   you want to configure.

4)  Configure SSH and Telnet for local login and privilege level 15:
   Router(config)# line vty 0 4
   Router(config-line)# privilege level 15
   Router(config-line)# login local
   Router(config-line)# transport input telnet
   Router(config-line)# transport input telnet ssh
   Router(config-line)# exit
```

Lab 5.3.5 Configuring Basic Router Settings with IOS CLI



Router Designation	Router Name	Fast Ethernet 0 Address	Serial 0 Address	Interface Type	Subnet mask for both interfaces
Router 1	R1	172.16.0.1	172.17.0.1	DCE	255.255.0.0
Router 2	R2	172.18.0.1	172.17.0.2	DTE	255.255.0.0

Objectives

- Configure the device host name for a router.
- Configure console, privileged mode and virtual terminal passwords.
- Configure Ethernet and Serial interfaces.
- Verify connectivity between hosts and routers.

Background / Preparation

Set up a network similar to the one in the topology diagram. Any router that meets the interface requirements displayed in that diagram – such as 800, 1600, 1700, 1800, 2500, and 2600 routers, or a combination – may be used. Refer to the Router Interface Summary table at the end of the lab to correctly determine the interface identifiers to be used based, on the equipment in the lab. Depending on the router model, output may vary somewhat from that shown in this lab. The steps in this lab are intended to be executed on each router unless you are specifically instructed otherwise.

The following resources are required:

- Two routers, each with an Ethernet and Serial interface. These should be non-SDM routers, if possible, since the required SDM startup configuration is deleted when the startup-config is erased.
- Two Windows XP computers
- Straight-through category 5 Ethernet cable (PC1 to switch)
- Crossover category 5 Ethernet cable (PC2 to router R2)

- Null Serial cable
- Console cable(s) (from PCs 1 and 2 to routers R1 and R2)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

From each PC start a HyperTerminal session to the attached router.

NOTE: Go to the "Erasing and reloading the router" instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

NOTE: SDM Routers - If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor.

Step 1: Configure host IP settings

a. Make sure that the PCs are connected according to the topology diagram.

b. Configure static IP addresses on them as follows:

PC attached to R1 switch:

IP address: 172.16.0.2
Subnet mask: 255.255.0.0
Default gateway: 172.16.0.1

PC attached to R2 directly:

IP address: 172.18.0.2
Subnet mask: 255.255.0.0
Default gateway: 172.18.0.1

Step 2: Log in to each router and configure a hostname and password

c. Configure a hostname for each of the two routers.

```
Router>enable
Router#configure terminal
Router(config)#hostname R1
```

Repeat this process for router R2 (use **R2** for the name of the second router).

d. Configure a console password and enable login for each of the two routers.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Repeat this process for router R2.

e. Configure the password on the virtual terminal lines for each of the two routers.

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Repeat this process for router R2.

f. Configure the enable and enable secret passwords for each of the two routers.

```
R1(config)#enable password cisco
R1(config)#enable secret class
R1(config)#exit
```

Repeat this process for router R2.

NOTE: Remember the enable secret password is encrypted from the configuration view. Also do not type **enable secret password class**. If you do, the secret password will be **password**, not **class**. The enable secret password takes precedence over the enable password. Once an enable secret password is entered, the enable password no longer is accepted.

Step 3: Show the router running configuration

a. From the privileged EXEC prompt, issue the **show running-config** command. This command can be abbreviated as **sh run**.

```
R1#show running-config

*** Some output omitted ***

Building configuration...
Current configuration : 605 bytes
!
hostname R1
!
enable secret 5 $1$eJB4$SH2vZ.aiT7/tczUJP2zwT1
enable password cisco
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
!
interface Serial0/1
 no ip address
 shutdown

line con 0
 password cisco
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

b. Is there an encrypted password? _____

c. Are there any other passwords? _____

d. Are any of the other passwords encrypted? _____

Step 4: Configure the serial interface on R1

From global configuration mode, configure serial interface Serial 0 on Router R1. Refer to the Router **Interface Summary** chart at the end of the lab for the proper designation of the serial interface on the router that you are using for this lab.

```
R1(config)#interface serial 0/0
R1(config-if)#ip address 172.17.0.1 255.255.0.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
```

NOTE: Enter the clock rate only on the router serial interface to which the DCE interface end of the cable is attached. The cable type (DTE or DCE) is printed on the outside of each end of the null serial cable. When in doubt, enter the **clock rate** command on both router serial interfaces. The command will be ignored on the router to which the DTE end is attached. The command **no shutdown** turns on the interface. The command **shutdown** turns the interface off.

Step 5: Display information about the serial interface on R1

a. Enter the **show interface** command on R1. Refer to the **Router Interface Summary** chart.

```
R1#show interface serial 0/0

Serial0/0 is down, line protocol is down
  Hardware is PowerQUICC Serial
  Internet address is 172.17.0.1/16
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters 00:01:55
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     6 packets output, 906 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=down  DTR=up  RTS=up  CTS=down
```

b. List at least three details discovered by issuing this command.

Serial 0/0 is: _____ Line protocol is: _____

Internet address is: _____

Encapsulation: _____

To what OSI layer is the Encapsulation referring? _____

c. If the serial interface was configured, why did the **show interface serial 0/0** say that the interface is down?

_____

Step 6: Configure the serial interface on R2

From global configuration mode, configure serial interface Serial 0 on Router R1. Refer to the **Router Interface Summary** chart at the end of the lab for the proper designation of the serial interface on the router that you are using for this lab.

```
R2(config)#interface serial 0/0
R2(config-if)#ip address 172.17.0.2 255.255.0.0
R2(config-if)#clock rate 64000
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
```

NOTE: Enter the clock rate only on the router serial interface to which the DCE interface end of the cable is attached. The cable type (DTE or DCE) is printed on the outside of each end of the null serial cable. When in doubt, enter the **clock rate** command on both router serial interfaces. The command will be ignored on the router to which the DTE end is attached. The command **no shutdown** turns on the interface. The command **shutdown** turns the interface off.

Step 7: Display information about the serial interface on R2

a. Enter the **show interfaces** command on R1. Refer to the **Router Interface Summary** chart.

```
R2#show interface serial 0/0

Serial0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 172.17.0.2/16
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:08, output 00:00:08, output hang never
  Last clearing of "show interface" counters 00:04:54
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     3 packets input, 72 bytes, 0 no buffer
     Received 3 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     6 packets output, 933 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

b. List at least three details discovered by issuing this command.

Serial 0 is: _____ Line protocol is: _____

Internet address is: _____

Encapsulation: _____

To what OSI layer is the Encapsulation referring? _____

c. Why did the **show interface serial 0/0** say that the interface is up?

_____

Step 8: Verify that the serial connection is functioning

a. Use the **ping** command to test connectivity to the serial interface of the other router. From R1, ping the R2 router serial interface.

```
R1#ping 172.17.0.2
```

Does the ping work? _____

b. From R2, ping the R1 router serial interface.

```
R2#ping 172.17.0.1
```

Does the ping work? _____

c. If the answer is **no** for either question, troubleshoot the router configurations to find the error. Then ping the interfaces again until the answer to both questions is **yes**.

Step 9: Configure the FastEthernet interface on R1

From global configuration mode, configure the Ethernet interface on router R1. Refer to the **Router Interface Summary** chart at the end of the lab for the proper designation of the Ethernet interface on the router that you are using for this lab.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#ip address 172.16.0.1 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#exit
```

NOTE: Ethernet interfaces do not have a DTE or DCE distinction; therefore, it is not necessary to enter the **clock rate** command.

Step 10: Display information about the FastEthernet interface on R1

a. Enter the **show interface** command on R1. Refer to the **Router Interface Summary** chart.

```
R1#show interface FastEthernet 0/0

FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3076.8460 (bia 000c.3076.8460)
  Internet address is 172.16.0.1/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:18, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     52 packets output, 5737 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
```



```
     0 babbles, 0 late collision, 0 deferred
     52 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

b. List at least three details discovered by issuing this command.

FastEthernet 0 is: _____ Line protocol is: _____

Internet address is: _____

Encapsulation: _____

To what OSI layer is the Encapsulation referring? _____

c. Why did the **show interface FastEthernet 0/0** say that the interface is up?

_____

Step 11: Configure the FastEthernet interface on R2

From global configuration mode, configure the Ethernet interface on Router R2. Refer to the **Router Interface Summary** chart at the end of the lab for the proper designation of the Ethernet interface on the router that you are using for this lab.

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#ip address 172.18.0.1 255.255.0.0
R2(config-if)#no shutdown
R2(config-if)#exit
R2(config)#exit
```

NOTE: Ethernet interfaces do not have a DTE or DCE distinction; therefore, it is not necessary to enter the **clock rate** command.

Step 12: Display information about the FastEthernet interface on R2

a. Enter the **show interface FastEthernet 0/0** command on R1. Refer to the **Router Interface Summary** chart.

```
R2#show interfaces FastEthernet 0/0

FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 000c.3076.8460 (bia 000c.3076.8460)
  Internet address is 172.16.0.1/16
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto Speed, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:05, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     14 packets output, 1620 bytes, 0 underruns
```



```
0 output errors, 0 collisions, 1 interface resets
0 babbles, 0 late collision, 0 deferred
14 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out
```

b. List at least three details discovered by issuing this command.

FastEthernet 0/0 is: _____ Line protocol is: _____

Internet address is: _____

Encapsulation: _____

To what OSI layer is the Encapsulation referring? _____

c. Why did the **show interfaces FastEthernet 0/0** say that the interface is up?

_____

Step 13: Save the configuration on both routers

Save the running configuration to the startup configuration at the privileged EXEC mode.

```
R1#copy running-config startup-config
R2#copy running-config startup-config
```

NOTE: Save the running configuration for the next time that the router is restarted. The router can be restarted either by a software **reload** command or a power shutdown. The running configuration will be lost if the running configuration is not saved. The router uses the startup configuration when the router is started.

Step 14: Check the overall router configurations

Issue the **show running-config** command from the privileged EXEC mode on both routes and verify all of the configuration commands you have entered so far. Note that this command can be abbreviated as **sh run**.

```
R1#show running-config
R2#show running-config
```

Step 15: Verify that the FastEthernet connection is functioning

a. Open a **Command Prompt** window by clicking **Start > Run** and typing **cmd**. Alternatively, you may click **Start > All programs > Accessories > Command Prompt**.

b. Use the **ping** command to test connectivity to the FastEthernet interface of each router from its associated PC. From PC1, ping the R1 router FastEthernet interface.

```
R1#ping 172.16.0.1
```

Does the ping work? _____

c. From PC1, ping the R2 router FastEthernet interface.

```
R2#ping 172.18.0.1
```

Does the ping work? _____

d. If the answer is **no** for either question, troubleshoot the router configurations to find the error. Then ping the interfaces again until the answer to both questions is **yes**.

Step 16: (Optional challenge) Test connectivity

a. From PC1, ping the R1 router FastEthernet interface (default gateway).

```
C:\>ping 172.16.0.1
```


Does the ping work? _____

a. From the PC1 command prompt, use the ping command to test end-to-end connectivity from PC1 (172.16.0.2) to PC2 (172.18.0.2).

```
C:\>ping 172.18.0.2
```

Does the ping work? _____

b. The ping from PC1 to PC2 does not work because router R1 has no knowledge of the Ethernet network on R2 and router R2 has no knowledge of the Ethernet network on R1. The pings cannot get from PC1 to PC2; even if they could, they could not return.

Step 17: (Optional challenge) Configure static and default routes

a. For the pings to work from one PC to the other, a default route and a static route must be configured on each router, or there must be a dynamic routing protocol set up between them.

b. Set up the default routes on the two routers as follows:

```
R1(config)#ip route 0.0.0.0  0.0.0.0 172.17.0.2
R2(config)#ip route 0.0.0.0  0.0.0.0 172.17.0.1
```

c. Set up the static routes on the two routers as follows:

```
R1(config)#ip route 172.18.0.0 255.255.0.0 172.17.0.2
R2(config)#ip route 172.16.0.0 255.255.0.0 172.17.0.1
```

d. Repeat the pings from Step 16. They should now be successful.

e. Use the **show ip route** command on each router to see the default and static routes.

```
R1(config)#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.17.0.2 to network 0.0.0.0

C    172.17.0.0/16 is directly connected, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
S    172.18.0.0/16 [1/0] via 172.17.0.2
S*   0.0.0.0/0 [1/0] via 172.17.0.2


R2(config)#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 172.17.0.1 to network 0.0.0.0
```

```
C    172.17.0.0/16 is directly connected, Serial0/0
S    172.16.0.0/16 [1/0] via 172.17.0.1
C    172.18.0.0/16 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 172.17.0.1
```

Erasing and reloading the router

a. Enter the privileged EXEC mode by typing **enable**.

```
Router>enable
```

b. In privileged EXEC mode, enter the **erase startup-config** command.

```
Router#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

c. Press **Enter** to confirm.

The response is:

```
Erase of nvram: complete
```

d. In privileged EXEC mode, enter the **reload** command.

```
Router(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

e. Type **n** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm]
```

f. Press **Enter** to confirm.

In the first line of the response is:

```
Reload requested by console.
```

After the router has reloaded the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

g. Type **n** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started!
```

h. Press **Enter**.

The router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
NOTE: In order to find out exactly how the router is configured, look at the interfaces. Doing this will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.				

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

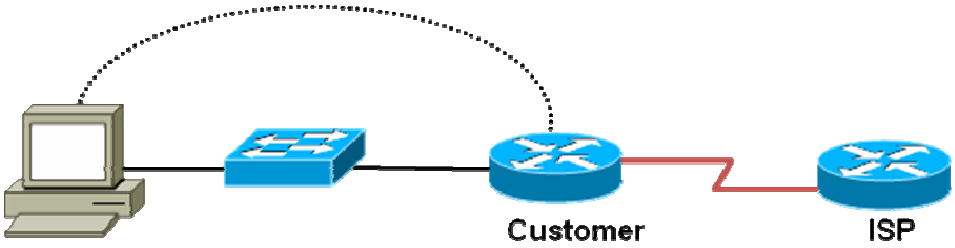
```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the router's HTTP/HTTPS server, using the following Cisco IOS
commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>

   Replace <username> and <password> with the username and password that
   you want to configure.
```


4) Configure SSH and Telnet for local login and privilege level 15:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Cisco Networking Academy®
Mind Wide Open™

Lab 5.3.8 Configuring NAT and DHCP with IOS CLI



Router Designation	Router Name	Fast Ethernet 0 Address and subnet mask	Serial 0 Address and subnet mask	Interface Type	Loopback Address
Router 1	Customer	192.168.1.1 255.255.255.0	209.165.200.225 255.255.255.224	DCE	N/A
Router 2	ISP	N/A	209.165.200.226 255.255.255.224	DTE	209.165.200.1 255.255.255.224

Objectives

- Configure a Customer router and host for DHCP.
- Configure a customer premise router for overloaded NAT, also known as Port Address Translation (PAT).
- Verify DHCP and NAT translations from within the customer network to ISP.

Background / Preparation

Set up a network similar to the one shown in the topology diagram. Any router that meets the interface requirements displayed in that diagram – such as 800, 1600, 1700, 1800, 2500, and 2600 routers, or a combination – may be used. Refer to the Router Interface Summary table at the end of the lab to correctly determine the interface identifiers to be used, based on the equipment in the lab. Depending on the router model, output may vary somewhat from that shown in this lab. The steps in this lab are intended to be executed on each router unless you are specifically instructed otherwise.

The following resources are required:

- Two routers, one with an Ethernet and Serial interface and the other with a Serial interface
- One Windows XP computer
- Straight-through Category 5 Ethernet cable (PC1 to switch)
- Null Serial cable

- Console cables (from PC 1 to routers R1 and R2)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

From the PC, start a HyperTerminal session with the router.

NOTE: Go to the "Erasing and reloading the router" instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

NOTE: SDM Routers - If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor.

Step 1: Cable and configure the routers

a. Based on the topology diagram, connect the PC, switch, and routers using the appropriate cabling.

b. Configure each router with the following parameters: hostname, console access and password, vty access and password, and enable secret password. If necessary, refer to Lab 5.3.5, "Configuring Basic Router Settings with IOS CLI," for instructions on setting hostname, passwords, and interface addresses.

c. Configure the router interfaces with the appropriate IP address and mask. Make sure that the interfaces are in usable condition and can ping a directly connected interface or host.

d. Configure the ISP router with a loopback address to be used to test the customer router. The loopback address represents a distant network.

```
ISP(config)#interface loopback 0
ISP(config-if)#ip address 209.165.200.1 255.255.255.224
```

Step 2: Configure a default route on the customer router

a. On the customer router, configure a default route pointing toward the ISP. All packets destined for networks that are *not* in the customer routing table are forwarded to the ISP router, which has a much larger routing table and connections to other Internet providers. Notice how this default route uses the neighbor router IP address as the last number.

```
Customer(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

b. Why is a default route *not* used on the ISP? A default route on the ISP router would be a bad configuration if it pointed toward a customer site. Any routes not found in the ISP routing table would be automatically sent to the customer router. Of course, the customer router would not know what to do with the packet and would send the packet to the default route of the customer router, which is the ISP. A routing loop would occur.

Step 3: Configure and test the DHCP pool

a. On the customer router, configure a DHCP pool for the internal clients.

```
Customer(config)#ip dhcp excluded-address 192.168.1.1
Customer(config)#ip dhcp pool INTERNAL
Customer(dhcp-config)#network 192.168.1.0 255.255.255.0
Customer(dhcp-config)#domain-name abc-xyz-widgets.inc
Customer(dhcp-config)#default-router 192.168.1.1
```

b. On the customer host PC, click **Start > Control Panel > Network Connections** to verify that the NIC is configured for DHCP. If necessary, open a command prompt and issue the **ipconfig /release** and **ipconfig /renew** commands.

c. On the customer host PC, open a command prompt. Click **Start > Run,** and then type **cmd** and press **Enter**. Alternatively, click **Start > All Programs > Accessories > Command Prompt**. Issue the **ipconfig /all** command.

d. What IP address is issued to the PC? _____

e. What is the MAC address of the host PC? _____

f. From the host PC, ping the default gateway (the router Ethernet interface). Does the ping succeed? _____ Troubleshoot as necessary and do not proceed until the ping is successful.

Step 4: Display DHCP binding on the customer router

a. To see the IP address and host hardware (MAC) address combination assigned by the DHCP server in the router, issue the **show ip dhcp binding** command on the customer router.

```
Customer#show ip dhcp binding
IP address   Client-ID/          Lease expiration        Type
             Hardware address
192.168.1.2  0100.0bdb.04a5.cd  May 26 2007 11:19 AM    Automatic
```

b. Do the IP address and Hardware address displayed match those recorded for the host PC in Step 3? _____

Step 5: Configure NAT/PAT

a. On the customer router, use the **access-list** command to identify the addresses that need to be translated. The network number is stated, but instead of a normal mask that usually comes next, a wildcard mask is used (0.0.0.255).

```
Customer(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

b. On the customer router, define where NAT looks for the IP addresses it needs to translate (source list 1 refers to access list 1 that you just created). Also define which interface IP address to use as the real address for each packet that comes through the FastEthernet interface destined for the Serial interface. The **overload** parameter at the end of the command shown below means that the serial port IP address is used and that port numbers are used to track the packets. Approximately 4,000 addresses can realistically be translated using this method, even though it is technically possible to translate even more.

```
Customer(config)#ip nat inside source list 1 interface serial 0/0 overload
```

c. Apply NAT to the inside and outside interfaces.

```
Customer(config)#interface serial 0/0
Customer(config-if)#ip nat outside
Customer(config-if)#exit
Customer(config)#interface fastethernet 0/0
Customer(config)#ip nat inside
Customer(config)#end
```

Step 6: Test NAT/PAT

a. From the host PC command prompt, ping the ISP router loopback address.

```
ping 209.165.200.1
```

b. Was the ping successful? _____ If not, perform appropriate troubleshooting.

c. On the customer router, issue the command to verify the NAT translation.

```
Customer#show ip nat translation
Pro  Inside global       Inside local    Outside local     Outside global
icmp 209.165.200.225:512 192.168.1.2:512 209.165.200.1:512 209.165.200.1:512
```


d. List the following IP addresses:

What is the inside global IP address shown? _____

What is the inside local IP address shown? _____

What is the outside local IP address shown? _____

What is the outside global IP address shown? _____

e. On the ISP router, configure the router to show all ICMP packets that come into the router.

```
ISP#debug ip icmp
ICMP packet debugging is on
```

f. From the host PC command prompt, issue a continuous ping.

```
ping 209.165.200.1 –t
```

g. On the ISP router, notice the debug output.

```
ISP#
00:49:10: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
00:49:11: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
00:49:12: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
00:49:13: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
00:49:14: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
00:49:15: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
00:49:16: ICMP: echo reply sent, src 209.165.200.1, dst 209.165.200.225
```

h. What is the source IP address of the ICMP reply? _____

i. What is the destination IP address of the ICMP reply? _____

j. Does this debug prove or disprove the fact that internal IP addresses are hidden and how can you tell?

_____

_____

k. On the host PC, stop the ping by pressing **CTRL-X**.

l. On the ISP router, stop the debug process. Note that the router takes a few moments for the output to quit displaying.

```
ISP#undebug all
```

Step 7: Clear NAT Translations

a. From the customer host PC command prompt, open a Telnet session to the ISP router.

```
telnet 209.165.200.226
```

This Telnet session will create another translation on the customer router.

b. On the customer router, issue the command to verify the NAT translation.

```
Customer#show ip nat translation
Pro  Inside global       Inside local    Outside local     Outside global
tcp 209.165.200.225:1297 192.168.1.2:1297 209.165.200.226:23 209.165.200.226:23
```

The port number on the inside addresses may be different, because they are randomly generated source port numbers.

c. Close the command window on the customer host PC to terminate the Telnet session.

d. On the customer router, issue the command to verify the NAT translation.


```
Customer#show ip nat translation
```

e. Is the translation for the customer host PC still active on the customer router? _____

NAT translations remain active for different periods of time, depending on the type of translation. TCP NAT translations can remain active for up to 24 hours by default. Port translations have shorter time limits, but can still remain active for minutes, even hours after the session between the two hosts has timed out. The default timeouts for UDP range from 1 minute to 5 minutes. For more information on NAT timeouts, view the Cisco IOS Network Address Translation Overview white paper on the Cisco.com website.

http://cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a0080091cb9.shtml

f. On the customer router, issue the command to clear all NAT translations active in the router.

```
Customer#clear ip nat translation *
```

Verify that the translation for the customer host PC is no longer active on customer router.

Step 8: Reflection

a. What would be an advantage of using the NAT method shown in this lab over a static configuration as shown in the curriculum?

_____

_____

b. List an instance of when a company might not use NAT/PAT.

_____

_____

Erasing and reloading the router

g. Enter the privileged EXEC mode by typing **enable**.

```
Router>enable
```

h. In privileged EXEC mode, enter the **erase startup-config** command.

```
Router#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

i. Press **Enter** to confirm.

The response is:

```
Erase of nvram: complete
```

j. In privileged EXEC mode, enter the **reload** command.

```
Router(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

k. Type **n** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm]
```

l. Press **Enter** to confirm.

In the first line of the response is:

```
Reload requested by console.
```

After the router has reloaded the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

m. Type **n** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started!
```

n. Press **Enter**.

The router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
NOTE: In order to find out exactly how the router is configured, look at the interfaces. Doing this will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.				

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the router's HTTP/HTTPS server, using the following Cisco IOS
commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>
```

Replace <username> and <password> with the username and password that you want to configure.

4) Configure SSH and Telnet for local login and privilege level 15:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Lab 5.4.2 Powering Up a Cisco Catalyst 2960 Switch

Objectives

- Set up a new Cisco LAN switch.
- Connect a computer to the router console interface.
- Configure HyperTerminal so that the computer can communicate with the router.

Background / Preparation

This lab focuses on the initial setup of the Cisco 2960 switch. If a Cisco 2960 switch is not available, you can use another switch model. The information in this lab applies to other switches. The Cisco 2960 switch is a fixed-configuration, standalone device that does not use modules or flash card slots. It is appropriate for small-sized to medium-sized businesses and for ISP-managed customers.

The following resources are required:

- Cisco 2960 or other comparable switch
- Power cable
- Windows PC with terminal emulation program
- Console cable

Step 1: Position and ground the switch (Optional)

NOTE: This step is optional and is required only if the switch is being set up for the first time. Read through it to become familiar with the process.

a. Position the switch chassis to allow unrestricted airflow for chassis cooling. Keep at least 3 inches (7.6 cm) of clear space beside the cooling inlet and exhaust vents.

b. Connect the chassis to a reliable earth ground using a ring terminal and size 14 AWG (2 mm) wire using these steps:

NOTE: Your instructor should inform you where a reliable earth ground is.

1) Strip one end of the ground wire to expose approximately 3/4 inch (20 mm) of conductor.

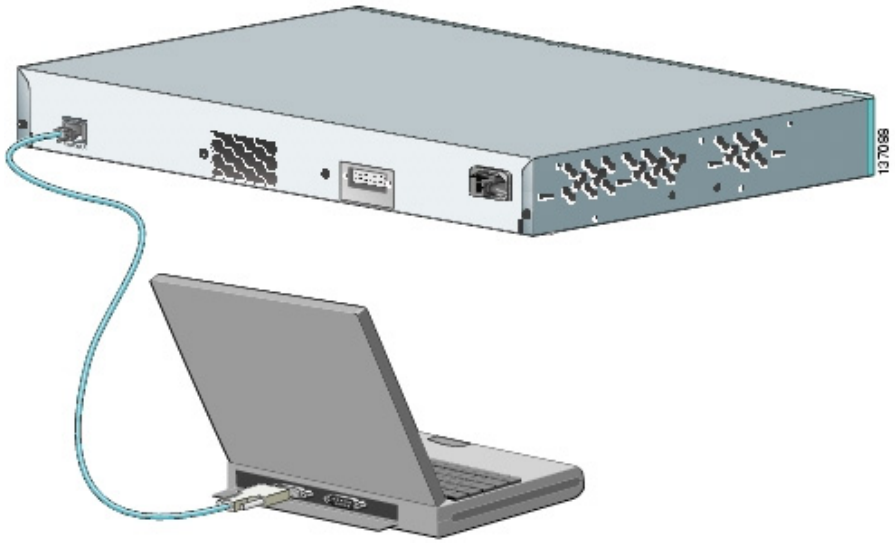
2) Crimp the 14 AWG (2 mm) green ground wire to a UL Listed/CSA certified ring terminal using a crimping tool that is recommended by the ring terminal manufacturer.

3) Attach the ring terminal to the chassis. Use a Number 2 Phillips screwdriver and the screw that is supplied with the ring terminal and tighten the screw.

Step 2: Connect the computer to the switch

Connect the PC to the Cisco 2960 switch using an RJ-45-to-DB-9 connector console cable, as shown in the figure below. To view the switch startup messages, connect the PC to the switch, power up the PC and start the terminal emulation program before powering up the switch.

CAUTION: To ensure adequate cooling, never operate the switch unless the cover is installed.



Step 3: Configure the PC terminal emulation program

a. Load the terminal emulation program on the PC.

b. Select a COM port that matches the port where the RJ-45-to-DB-9 connector is connected to the PC. The COM port is usually COM1 or COM2.

c. Configure the terminal emulation parameters as follows:

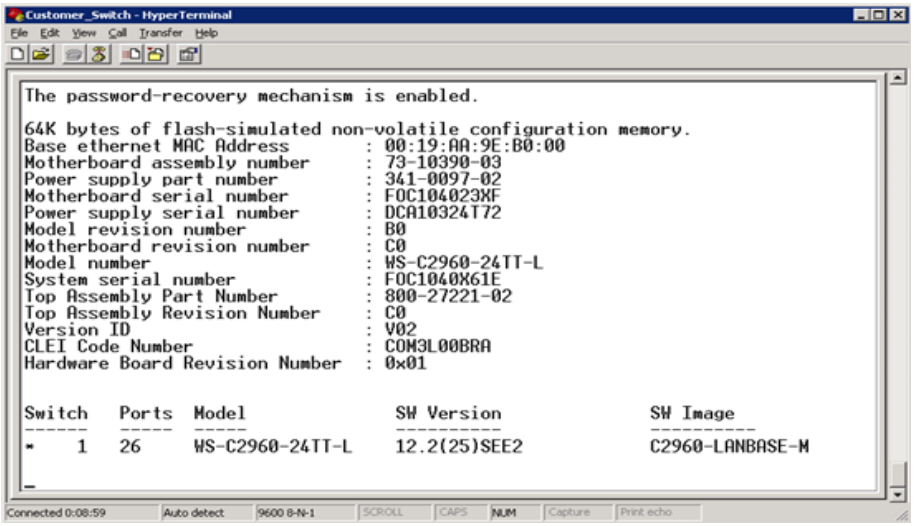
- 9600 baud
- 8 data bits
- no parity
- 1 stop bit
- no flow control and no parity

Step 4: Power up the switch

a. Connect the power cable to the Cisco 2960 switch and to the electrical outlet to power the switch on. The 2960 switch does not have a power switch, but other switches may have one.

As the switch powers on, the power-on self-test (POST) begins. POST is a series of tests that run automatically to ensure that the switch is functioning properly. POST lasts approximately 1 minute. When the switch begins POST, the **System, Status, Duplex**, and **Speed** LEDs turn green. The **System** LED blinks green, and the other LEDs remain solid green.

b. Observe the startup messages as they appear in the terminal emulation program window. While these messages are appearing, do not press any keys on the keyboard. Pressing a key interrupts the switch startup process. Some examples of startup messages displayed are the amount of flash memory installed and the Cisco IOS software version the computer is using. Can you find these example startup messages in the following figure?



The figure shows that there is 64 KB of flash memory installed in the switch, and that the Cisco IOS software version is 12.2(25)SEE2. Startup messages are generated by the operating system of the switch. The messages vary depending on the software installed on the switch. These messages can scroll by quickly and can take a few minutes to stop.

When the POST completes successfully, the **System** LED remains green. The other LEDs turn off and then reflect the switch operating status.

c. When the switch is finished starting up, the following system message appears in the terminal emulation window:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

NOTE: If the message above does not appear, the switch may have been previously configured and needs to be restored to factory default settings according to the procedure described at the end of this lab.

d. Now turn the switch off by disconnecting the power cord from the switch.

Step 5: Troubleshoot a non-working switch

If the switch fails POST, the **System** LED turns amber. If your switch fails POST, unplug the switch and tell your instructor.

Step 6: Reflection

a. Which LED shows after the POST completes successfully and what color does it show?

4) **Status** LED blinks green
5) **Speed** LED blinks green
6) **Status** LED blinks amber
7) **System** LED is solid green

b. What is the minimum amount of space required around the Cisco 2960 switch ventilation openings?

1) 1 inch (2.54 cm)
2) 2 inches (5.08 cm)
3) 3 inches (7.6 cm)

c. When the Cisco 2960 switch is finished starting up for the first time, what task are you asked to perform?

   1) You are asked to perform an initial configuration of the switch.

   2) You are not asked to do anything. The switch system prompt appears.

   3) If your switch is configured with Cisco SDM, you are told that con0 is available.

Erasing and Reloading the Switch

For the majority of the labs in CCNA Discovery, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. The following instructions prepare the switch prior to performing the lab so that previous configuration options do not interfere. Instructions are provided for the 2900 and 2950 series switches.

d. Enter into privileged EXEC mode by typing **enable**. If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

e. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

f. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

g. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step b using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present, you must power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in. If the VLAN information was successfully deleted in Step b, go to Step e and restart the switch using the **reload** command.

h. Restart the software using the **reload** command.

NOTE: This step is not necessary if the switch was restarted using the power cycle method.

4) At the privileged EXEC mode, enter the **reload** command:

```
Switch(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```


5) Type **n,** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response is:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt is:

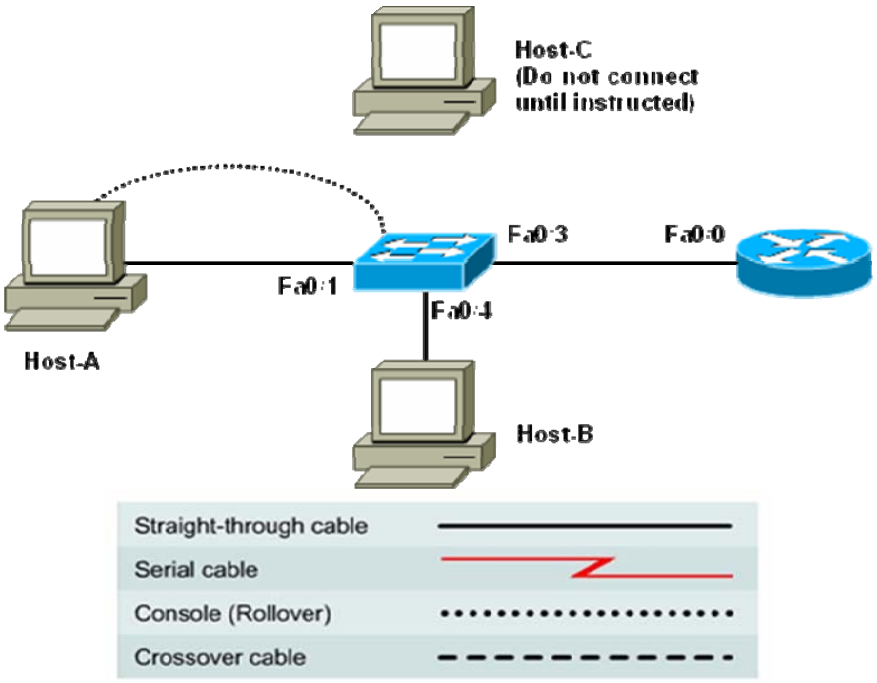
```
Would you like to enter the initial configuration dialog? [yes/no]:
```

6) Type **n,** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started! [Enter]
```

Lab 5.4.4 Configuring the Cisco 2960 Switch



Device Designation	Host Name / Interface	IP Address	Subnet Mask	Default Gateway
PC 1	Host-A	192.168.1.2	255.255.255.0	192.168.1.1
PC 2	Host-B	192.168.1.4	255.255.255.0	192.168.1.1
PC 3	Host-C	192.168.1.6	255.255.255.0	192.168.1.1
Switch	CustomerSwitch VLAN 1 interface	192.168.1.5	255.255.255.0	192.168.1.1
Router	CustomerRouter F0/0 interface	192.168.1.1	255.255.255.0	N/A

Objectives

- Configure initial switch global settings
- Configure hosts PCs and attach them to the switch
- Configure a router and attach it to the switch
- Configure a switch management VLAN IP address.
- Configure basic port security.
- Configure port duplex and speed settings.

Background / Preparation

This lab focuses on the basic configuration of the Cisco 2960 switch using Cisco IOS commands. The information in this lab applies to other switches, however, command syntax may vary. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network. To use an IP-based management product or Telnet with a Cisco switch, you must configure a management IP address.

In this lab, you will configure VLAN 1 to provide IP access to management functions. You will also test connectivity from a host to the switch to verify the management IP address. In addition, you will configure port security, port speed, and duplex settings.

The following resources are required:

- Cisco 2960 switch or other comparable switch
- Router with Ethernet interface to connect to switch
- Three Windows-based PCs, one with a terminal emulation program
- RJ-45-to-DB-9 connector console cable
- Three straight-through Ethernet cables
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

NOTE: Go to the “Erasing and Reloading the Switch” instructions at the end of this lab. Perform those steps on the switch in this lab assignment before continuing.

NOTE: Go to the “Erasing and reloading the router” instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

NOTE: SDM Routers - If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor.

Step 1: Connect the hosts to the switch and configure them.

a. Connect Host-A to Fast Ethernet switch port Fa0/1, and connect Host-B to port Fa0/4. Configure the hosts to use the same IP subnet for the address and mask as on the switch, as shown in the topology diagram above.

b. Do **NOT** connect Host-C to the switch yet.

Step 2: Connect the router to the switch and configure the router.

NOTE: If necessary, refer to Lab 5.3.5, “Configuring Basic Router Settings with IOS CLI,” for instructions on setting hostname, passwords, and interface addresses.

a. Connect the router to Fast Ethernet switch port Fa0/3.

b. Configure router with a hostname of **CustomerRouter**.

c. Configure console access and password, vty access and password, and enable secret password.

d. Configure the router Fa0/0 interface as shown in the topology diagram above.

Step 3: Perform an initial configuration on the switch.

a. Configure the hostname of the switch as CustomerSwitch:


```
Switch>enable
Switch#Config Terminal
Switch(config)#hostname CustomerSwitch
```

b. Set the privilege exec mode password to cisco:

```
CustomerSwitch(config)#enable password cisco
```

c. Set the privilege exec mode secret password to cisco123:

```
CustomerSwitch(config)#enable secret cisco123
```

d. Set the console password to cisco123:

```
CustomerSwitch(config)#line console 0
CustomerSwitch(config-line)#password cisco123
```

e. Configure the console line to require a password at login:

```
CustomerSwitch(config-line)#login
```

f. Set the vty password to cisco123:

```
CustomerSwitch(config-line)#line vty 0 15
CustomerSwitch(config-line)#password cisco123
```

g. Configure the vty to require a password at login:

```
CustomerSwitch(config-line)#login
CustomerSwitch(config-line)#end
```

Step 4: Configure the management interface on VLAN 1.

a. Enter global configuration mode. Remember to use the new password.

```
CustomerSwitch>enable
CustomerSwitch#configure terminal
```

b. Enter the interface configuration mode for VLAN 1:

```
CustomerSwitch(config)#interface vlan 1
```

c. Set the IP address, subnet mask, and default gateway for the management interface. The IP address must be valid for the local network where the switch is installed.

```
CustomerSwitch(config-if)#ip address 192.168.1.5 255.255.255.0
CustomerSwitch(config-if)#exit
CustomerSwitch(config)#ip default-gateway 192.168.1.1
CustomerSwitch(config)#end
```

Step 5: Verify configuration of the switch.

a. Verify that the IP address of the management interface on the switch VLAN 1 and the IP address of Host-A are on the same local network. Use the **show running-configuration** command to check the IP address configuration of the switch:

```
CustomerSwitch#show running-configuration
Building configuration...

Current configuration : 1283 bytes
!
version 12.2
no service pad
hostname CustomerSwitch
!
enable secret 5 $1$XUe/$ch4WQ/SpcFCDd2iqd9bda/
```

```
enable password cisco
!
interface FastEthernet0/1
!
*** Output Omitted ***
!
interface FastEthernet0/24
!
interface Vlan1
 ip address 192.168.1.5 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
line con 0
 password cisco123
 login
line vty 0 4
 password cisco123
 login
line vty 5 15
 password cisco123
 login
!
end
```

b. Save the configuration using the following command:

```
CustomerSwitch#copy running-configuration startup-configuration
```

Step 6: Verify connectivity using ping and Telnet.

a. To verify that the switch and router are correctly configured, ping the router Fa0/0 interface (default gateway) IP address from the Switch CLI.

b. Were the pings successful? _____

c. To verify that the hosts and switch are correctly configured, ping the switch IP address from Host-A.

d. Were the pings successful? _____

e. If the ping is not successful, verify the connections and configurations again. Check to ensure that all cables are correct and that connections are seated. Check the host, switch and router configurations.

f. Open a command prompt on Host-A, and enter the **telnet** command followed by the IP address assigned to switch management VLAN 1.

g. Enter the vty password configured in Step 3. What was the result?

_____

h. At the switch prompt, issue the **show version** command.

```
CustomerSwitch>show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version
12.2(0.0.16)FX, CISCO
DEVELOPMENT TEST VERSION
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Tue 17-May-05 01:43 by yenanh

ROM: Bootstrap program is C2960 boot loader
```

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M), Version 12.2 [lqian-
flo_pilsner 100]

 Switch uptime is 3 days, 20 hours, 8 minutes
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-0.0.16.FX.bin"

cisco WS-C2960-24TC-L (PowerPC405) processor with 61440K/4088K bytes of
memory.
Processor board ID FHH0916001J
Last reset from power-on
Target IOS Version 12.2(25)FX
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:FC:FF:E8:80
Motherboard assembly number     : 73-9832-02
Motherboard serial number       : FHH0916001J
Motherboard revision number     : 01
System serial number            : FHH0916001J
Hardware Board Revision Number  : 0x01

Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
*    1   26     WS-C2960-24TC-L    12.2(0.0.16)FX        C2960-
LANBASE-M

Configuration register is 0xF
```

i. What is the Cisco IOS version of this switch? _____

j. Type **quit** at the switch command prompt to terminate the Telnet session.

Step 7: Determine which MAC addresses that the switch has learned.

a. From the Windows command prompt, determine the Layer 2 addresses of the PC network interface card for each host by using the **ipconfig /all** command.

Host-A: _____

Host-B: _____

Host-C: _____

b. Determine which MAC addresses the switch has learned by using the **show mac-address-table** command at the privileged exec mode prompt:

```
CustomerSwitch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000b.be7f.ed40    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    000b.db04.a5cd    DYNAMIC     Fa0/1
```

```
   1    000c.3076.8380    DYNAMIC     Fa0/3
   1    000d.1496.36ad    DYNAMIC     Fa0/4
Total Mac Addresses for this criterion: 7
```

c. How many dynamic addresses are there? _____

d. Do the MAC addresses match the host MAC addresses? _____

e. Review the options that the **mac-address-table** command has by using the **?** option:

```
CustomerSwitch(config)#mac-address-table ?
  address       address keyword
  aging-time    aging-time keyword
  count         count keyword
  dynamic       dynamic entry type
  interface     interface keyword
  multicast     multicast info for selected wildcard
  notification  MAC notification parameters and history table
  static        static entry type
  vlan          VLAN keyword
  |             Output modifiers
  <cr>
```

f. Set up a static MAC address on the Fast Ethernet interface 0/4. Use the address that was recorded for Host-B in Step 7. The MAC address XXXX.YYYY.ZZZZ is used in the example statement only.

```
CustomerSwitch(config)#mac-address-table static XXXX.YYYY.ZZZZ interface
fastethernet 0/4 vlan 1
```

g. Verify the MAC address table entries:

```
CustomerSwitch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000b.be7f.ed40    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    000b.db04.a5cd    DYNAMIC     Fa0/1
   1    000c.3076.8380    DYNAMIC     Fa0/3
   1    000d.1496.36ad    STATIC      Fa0/4
```

How many total MAC addresses are there now? _____

h. What type are they? _____

Step 8: Configure basic port security.

a. Determine the options for setting port security on Fast Ethernet interface 0/4.

```
CustomerSwitch#configure terminal
CustomerSwitch(config)#interface fastEthernet 0/4
CustomerSwitch(config-if)#switchport port-security ?
   aging Port-security aging commands
   mac-address Secure mac address
   maximum Max secure addrs
   violation Security Violation Mode
```

b. To allow the switch port FastEthernet 0/4 to accept only one device, configure port security as follows:

```
CustomerSwitch(config-if)#switchport mode access
CustomerSwitch(config-if)#switchport port-security
CustomerSwitch(config-if)#switchport port-security mac-address sticky
CustomerSwitch(config-if)#end
```

c. Check the port security settings.

```
CustomerSwitch#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
               (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      Fa0/4           1          0                0         Shutdown
---------------------------------------------------------------------------
```

d. What is the security action for port fa0/4? _____

e. What is the maximum secure address count? _____

f. Display the running configuration

NOTE: Some output omitted in following display.

```
CustomerSwitch#show running-config
Building configuration...
Current configuration : 1452 bytes
version 12.2
hostname CustomerSwitch
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
!
*** Output Omitted ***

mac-address-table static 000b.db04.a5cd vlan 1 interface
FastEthernet0/4
!
end
```

g. Are there statements that directly reflect the security implementation in the listing of the running configuration? _____

Step 9: Connect a different PC to the secure switch port.

a. Disconnect Host-B from FastEthernet 0/4 and connect Host-C to the port. Host-C has not yet been attached to the switch. Ping the switch address 192.168.1.5 to generate some traffic.

b. Record any observations at the PC and the switch terminal session.

_____

_____

```
01:11:12: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/4, putting
Fa0/4 in err-disable state
01:11:12: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, cause
d by MAC address 000c.3076.8380 on port FastEthernet0/4.
01:11:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/4, chang
ed state to down
01:11:14: %LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to down
```

c. To see the configuration information for just FastEthernet port 0/4, enter the following command at the privileged EXEC mode prompt:

```
CustomerSwitch#show interface fastethernet 0/4
```

d. What is the state of this interface?

FastEthernet0/4 is _____ , and line protocol is _____.

Step 10: Reactivate the port.

a. If a security violation occurs and the port is shut down, use the **no shutdown** command to reactivate it.

```
CustomerSwitch(config)#interface fastEthernet 0/4
CustomerSwitch(config-if)#no shutdown
```

b. Try reactivating this port a few times by switching between the original port 0/4 host and the new one. Plug in the original host, type the **no shutdown** command on the interface, and ping using the Command prompt. You must ping multiple times or use the **ping 192.168.1.5 –n 200** command, which sets the number of ping packets to 200, instead of 4.

c. Switch hosts and try again.

Step 11: Set speed and duplex options for a port.

a. Switch port settings default to Auto-duplex and Auto-speed. If a computer with a 100 Mbps NIC is attached to the port, it automatically goes into full-duplex 100 Mbps mode. If a hub is attached to the switch port, it normally goes into half-duplex 10 Mbps mode.

b. Issue the **show interfaces** command to see the setting for ports Fa0/1 and Fa0/5. This command generates a large amount of output. Press the Space bar until you can see all the information for these ports. What are the duplex and speed settings for these ports?

Port Fa0/2 _____

Port Fa0/4 _____

Port Fa0/5 _____

c. It is sometimes necessary to set the speed and duplex of a port to ensure that it operates in a particular mode. You can set the speed and duplex with the **duplex** and **speed** commands while in interface configuration mode. To force Fast Ethernet port 5 to operate at half duplex and 10 Mbps, issue the following commands:

```
Switch>enable
Switch#Config Terminal
Switch(config-if)#interface fastEthernet 0/5
Switch(config-if)#speed 10
Switch(config-if)#duplex half
Switch(config-if)#end
Switch#
```

d. Issue the **show interfaces** command again. What is the duplex and speed setting for Fa0/5 now?

_____

Step 12: Exit the switch.

a. Type **exit** to leave the switch and return to the welcome screen:

```
Switch#exit
```

b. Once the steps are completed turn off all the devices. The remove and store the cables and adapter.

Step 13: Reflection.

a. Which password needs to be entered to switch from user mode to privilege exec mode on the Cisco switch, and why?

_____

_____

b. Which symbol is used to show a successful ping in the Cisco IOS software?

_____

c. What is the benefit of using port security? _____

_____

d. What other port-related security steps could be taken to further improve switch security?

_____

Erasing and Reloading the Switch

For the majority of the labs in CCNA Discovery, it is necessary to start with an unconfigured switch. Using a switch with an existing configuration may produce unpredictable results. The following instructions prepare the switch prior to performing the lab so that previous configuration options do not interfere. Instructions are provided for the 2900 and 2950 series switches.

a. Enter into privileged EXEC mode by typing **enable**. If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

e. Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?[Enter]
Delete flash:vlan.dat? [confirm] [Enter]
```

If there was no VLAN file, this message is displayed:

```
%Error deleting flash:vlan.dat (No such file or directory)
```

f. Remove the switch startup configuration file from NVRAM.

```
Switch#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue? [confirm]
```

Press **Enter** to confirm.

The response should be:

```
Erase of nvram: complete
```

g. Check that VLAN information was deleted.

Verify that the VLAN configuration was deleted in Step b using the **show vlan** command. If previous VLAN configuration information (other than the default management VLAN 1) is still present, you must power cycle the switch (hardware restart) instead of issuing the **reload** command. To power cycle the switch, remove the power cord from the back of the switch or unplug it, and then plug it back in. If the VLAN information was successfully deleted in Step b, go to Step e and restart the switch using the **reload** command.

h. Restart the software using the **reload** command.

NOTE: This step is not necessary if the switch was restarted using the power cycle method.

1) At the privileged EXEC mode, enter the **reload** command:

```
Switch(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

2) Type **n,** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm] [Enter]
```

The first line of the response is:

```
Reload requested by console.
```

After the switch has reloaded, the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```


3) Type **n,** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started! [Enter]
```

Erasing and reloading the router

b. Enter the privileged EXEC mode by typing **enable**.

```
Router>enable
```

d. In privileged EXEC mode, enter the **erase startup-config** command.

```
Router#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

e. Press **Enter** to confirm.

The response is:

```
Erase of nvram: complete
```

f. In privileged EXEC mode, enter the **reload** command.

```
Router(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

g. Type **n** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm]
```

h. Press **Enter** to confirm.

In the first line of the response is:

```
Reload requested by console.
```

After the router has reloaded the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

i. Type **n** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started!
```

j. Press **Enter**.

The router is ready for the assigned lab to be performed.

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the router's HTTP/HTTPS server, using the following Cisco IOS
commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>

   Replace <username> and <password> with the username and password that
   you want to configure.

4)  Configure SSH and Telnet for local login and privilege level 15:
   Router(config)# line vty 0 4
   Router(config-line)# privilege level 15
   Router(config-line)# login local
   Router(config-line)# transport input telnet
   Router(config-line)# transport input telnet ssh
   Router(config-line)# exit
```

Lab 5.5.4 Planning a WAN Upgrade

Objective

- Create a business proposal based on a scenario of an organization that requires a WAN upgrade.

Background / Preparation

You are currently employed at an ISP. A local business has contacted your company to inquire about establishing a WAN connection between their main office and a second office that will be opening in the next few months. You have been assigned to the new business account. Your job is to provide a proposal that outlines what the ISP can offer the business to meet their requirements for a new WAN connection.

You first visit the site to examine their existing setup. Currently, there is only one employee who gains access to the head office using dial-up access and a 56 K modem. This employee requires access to a database server that stores the data for the company's contact management software application. The new office will initially have 10 people who need to access the database server, but the business anticipates the second office having 30 employees within 1 year.

After running some benchmarking tests, you determine that each connection to the database uses 50 Kbps to function optimally. You also discover that if the database server cannot be reached, the application fails to function and the employee can no longer work. After talking with the customer, you learn that the availability of the new WAN connection is critical to the business and that service disruption needs to be kept to a minimum.

The ISP you work for has a variety of WAN connection options for business customers. This is a list of available options that you can offer the customer:

WAN Connection	Upstream Bandwidth	Downstream Bandwidth	SLA Availability	Cost
Dial-up	33.6 Kbps	53 Kbps	No	$12.95/month
ADSL	1.0 Mbps	3.0 Mbps	No	$64.95/month
Fractional T1	768 Kbps	768 Kbps	Yes	$149.95/month
T1	1.544 Mbps	1.544 Mbps	Yes	$299.95/month
Fractional T3	9.264 Mbps	9.264 Mbps	Yes	$1399.95/month
T3	45 Mbps	45 Mbps	Yes	$2499.95/month

Step 1: Identify the business requirements for the WAN upgrade

Outline the business requirements for a WAN connection between the two offices. Document these requirements in the WAN Upgrade Proposal included in this lab.

Step 2: List available WAN options for the business

List the ISP offerings for WAN connections that meet or exceed the requirements for the WAN connection between the two offices. Include this information in your proposal.

Step 3: Identify the best WAN connection option for the business

Based on the list of suitable WAN connection options, identify the most appropriate WAN connection for the business. Justify your answer.

Step 4: Group discussion

Assemble in groups of two or more to discuss your answers. Identify any items you missed when filling out the WAN Upgrade Proposal and correct your proposal as needed.

WAN Upgrade Proposal

Objective

- Establish WAN connectivity between the two offices for a company.

Existing Environment

Main Office

- Presently 45 employees connected over a 100 Mbps Ethernet network
- Main database server that stores data for contact management application
- Single external user using dial-up to connect to corporate network to access database server

Second Office

- Opening in a few months
- Across town from main office
- Initially to have 10 people, but is anticipated to grow to 30 people over the next year

Business Requirements

The new WAN connection between the two offices must meet these minimum specifications to satisfy the business requirements:

1.
2.

Available WAN Connection Options

WAN Connection	Upstream Bandwidth	Downstream Bandwidth	SLA Availability	Cost

Recommendation

The following WAN connection is recommended to satisfy the requirements:

_____

_____

_____

Lab 5.5.5 Configuring a Remote Router Using SSH

Objectives

- Configure a router to accept SSH connections.
- Configure SSH client software on a PC.
- Establish a connection to a Cisco ISR using SSH version 2.
- Check the existing running configuration.

Background / Preparation

In the past, the most common network protocol used to remotely configure network devices has been Telnet. However, protocols such as Telnet do not provide for authentication or encryption of the information between a Telnet client and server. As a result, a network sniffer can be used to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that can be used to establish a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log into a remote machine and execute commands; however, it can also transfer files using the associated SFTP or SCP protocols.

For SSH to function, the network devices communicating must support it. In this lab, you will enable the SSH server on a router to be configured and then connect to that router using a PC with an SSH client installed. For use on a local network, the connection is normally made using Ethernet and IP. Network devices connected via other types of links, such as serial, can also be managed using SSH, as long as they support IP. Like Telnet, SSH is an in-band, TCP/IP-based Internet protocol.

In this lab, you can use either Cisco SDM or Cisco IOS CLI commands to configure SSH on the router.

The Cisco 1841 ISR supports the use of SSH versions 1 and 2; version 2 is preferred. The SSH client used in this lab is PuTTY, which can be downloaded free of charge.

The Cisco SDM is supported on a wide range of Cisco routers and Cisco IOS Software releases. Many newer Cisco routers come with SDM pre-installed. If you are using an 1841 router, SDM (and SDM Express) is pre-installed. This lab assumes the use of a Cisco 1841 router. You can use another router model as long as it is capable of supporting SDM. If you are using a supported router that does not have SDM installed, you can download the latest version free of charge from the following location: http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm

From the URL shown above, view or download the document "Downloading and Installing Cisco Router and Security Device Manager." This document provides instructions for installing SDM on your router. It lists specific model numbers and IOS versions that can support SDM, and the amount of memory required.

NOTE: If you are using SDM to configure SSH, you must complete Lab 5.2.3, "Configuring an ISR with SDM Express," on the router to be used, before performing this lab. This lab assumes that the router has been previously configured with basic settings.

NOTE: If you are working with a router that does not have SDM installed, use Cisco IOS CLI commands to configure SSH. Instructions are provided for manual configuration of SSH using Cisco IOS CLI commands for routers that are not running SDM in Step 2 of this lab. To perform the basic router configuration, refer to Lab 5.3.5, "Configuring Basic Router Settings with IOS CLI."

NOTE: SDM Router with startup-config erased - If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor.

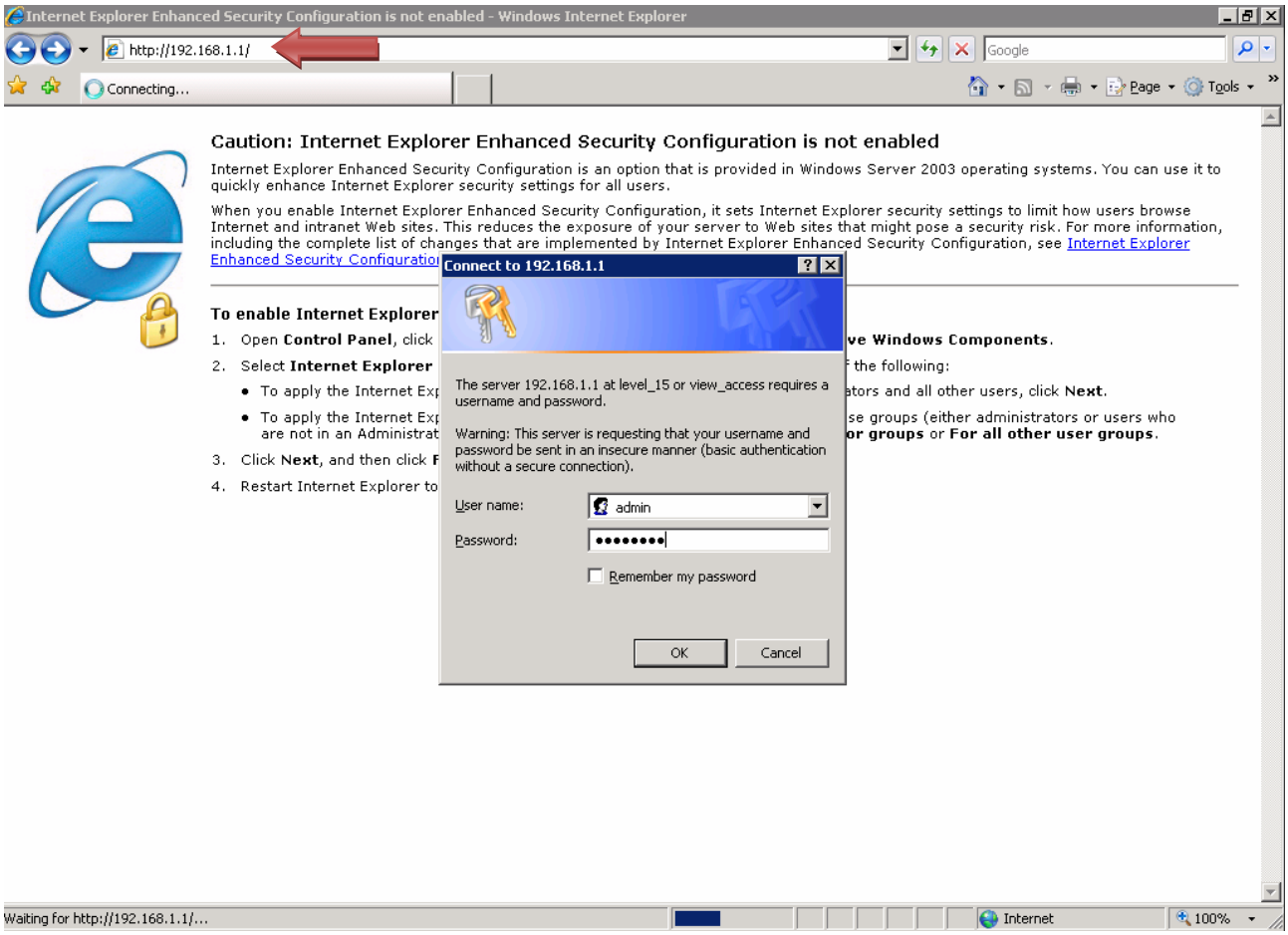
The following resources are required.

- Cisco 1841 ISR router with SDM version 2.4 installed and with basic configuration completed (critical – see Note 2 in Step 1)
- (Optional) Other Cisco router model with SDM installed
- (Optional) Other Cisco router model without SDM installed (IOS version 12.2 or higher – must support SSH)
- Windows XP computer with Internet Explorer 5.5 or higher and SUN Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810)
- Latest release of putty.exe client installed on the PC and accessible on the desktop
- Straight-through or crossover category 5 Ethernet cable (for SDM and SSH)
- (Optional) Console cable – if router is to be configured using the CLI
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

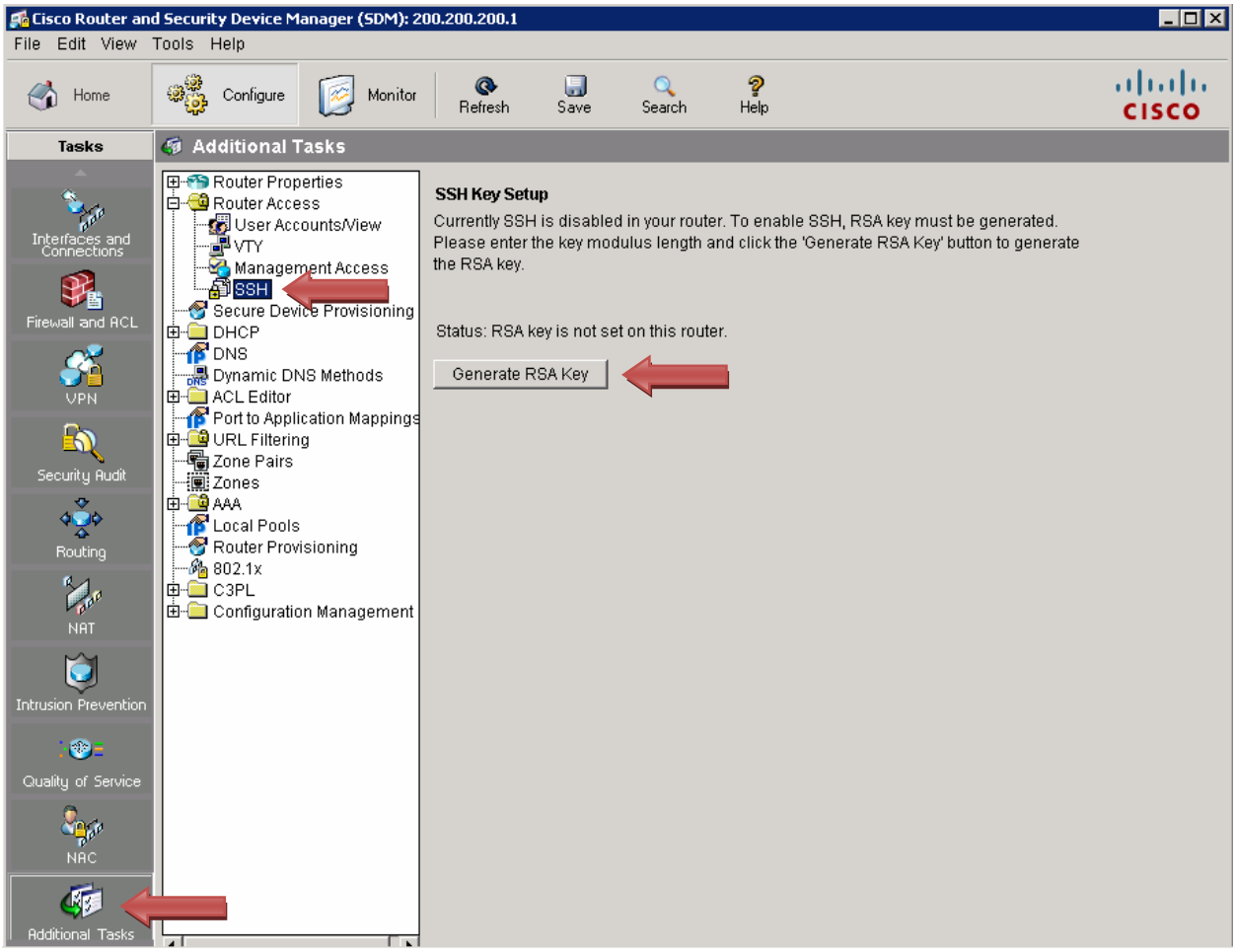
Step 1: Configure the ISR to accept SSH connections using SDM

NOTE – If router does not have SDM installed: If you are configuring a router for SSH that does not have SDM installed, read through the Step 1 to see how SSH is set up as a separate task when using SDM, and then go to Step 2; otherwise, complete Step 1 and go to Step 3.

a. Open the web browser and connect to http://192.168.1.1. When prompted, enter **admin** for the username and **cisco123** for the password. Click **OK**. Cisco SDM loads.

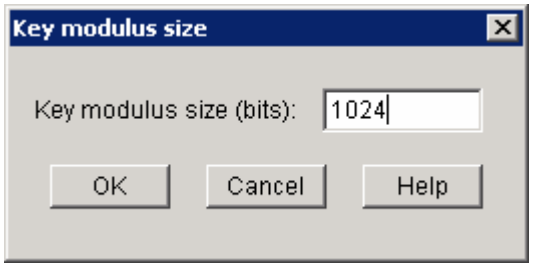


b. After SDM is loaded, click the **Configure** button on the tool bar. On the Tasks pane, click **Additional Tasks**. On the Additional Tasks pane, expand **Router Access** and click the **SSH** task. Then click the **Generate RSA Key** button.

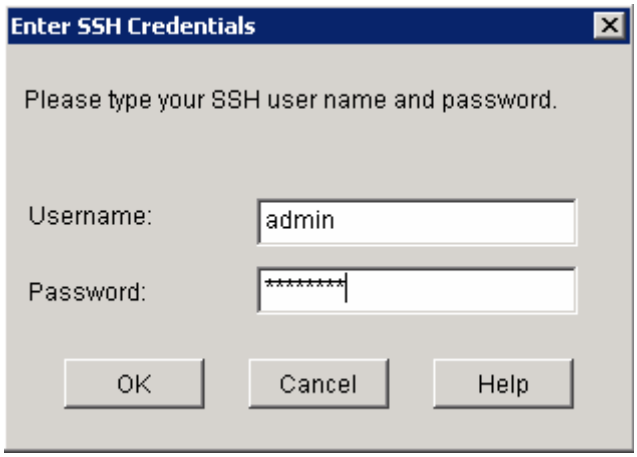


NOTE – If SSH is already set up: If the **SSH Key Setup** message says: “RSA key exists and SSH is enabled in your router” and **Status** is “RSA key is set on this router,” it is probably because you completed Lab 5.2.3, “Configuring an ISR with SDM Express.” Recall that in that lab, when you configured security, one of the recommended security settings enabled by default is “Enhance security on this router.” If this box is checked, it automatically configures SSH for router access, sets the banner to warn intruders, enforces minimum password length, and restricts the number of unsuccessful login attempts.

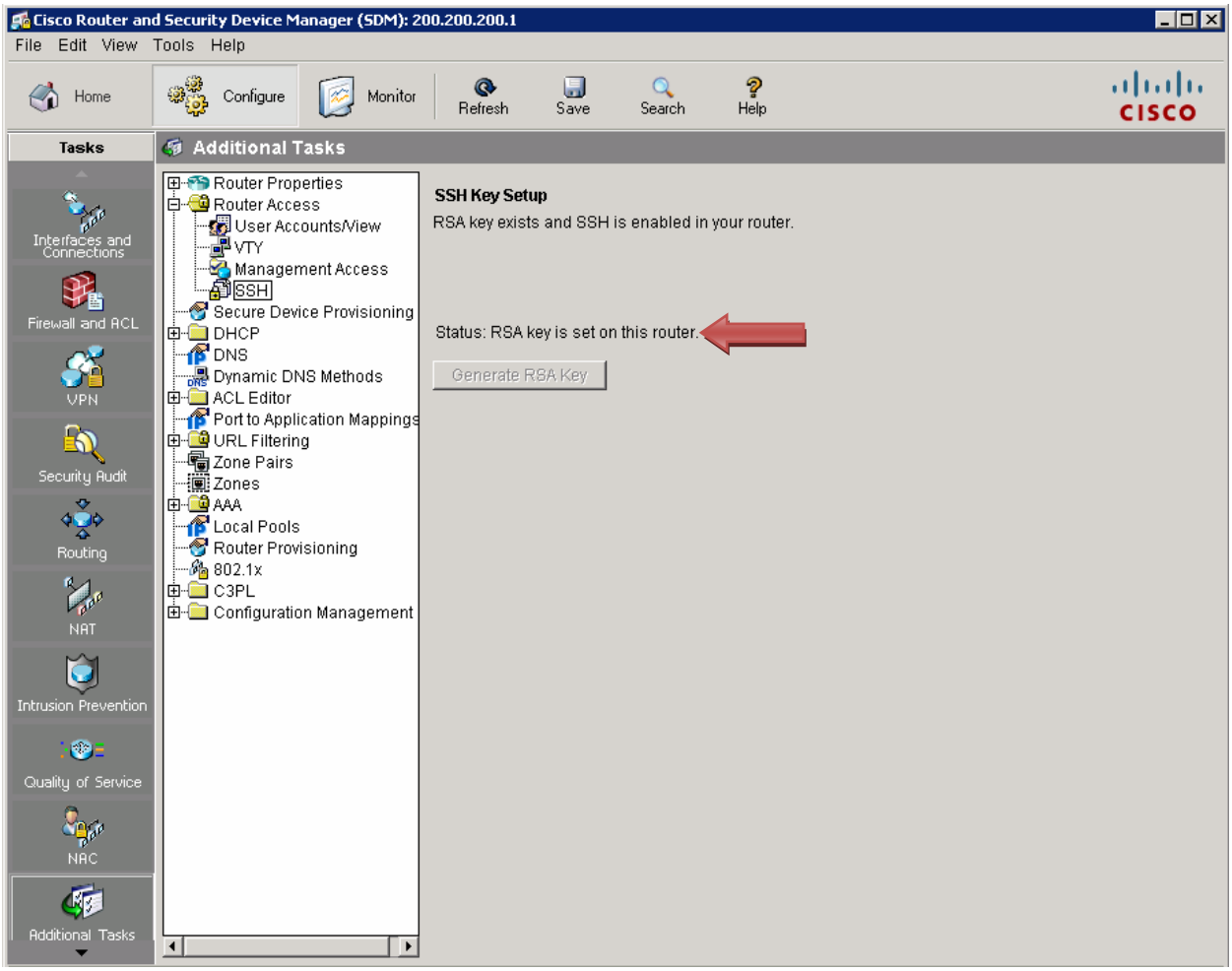
c. In the Key modulus size dialog box, enter a key size of **1024** bits. Click **OK**.



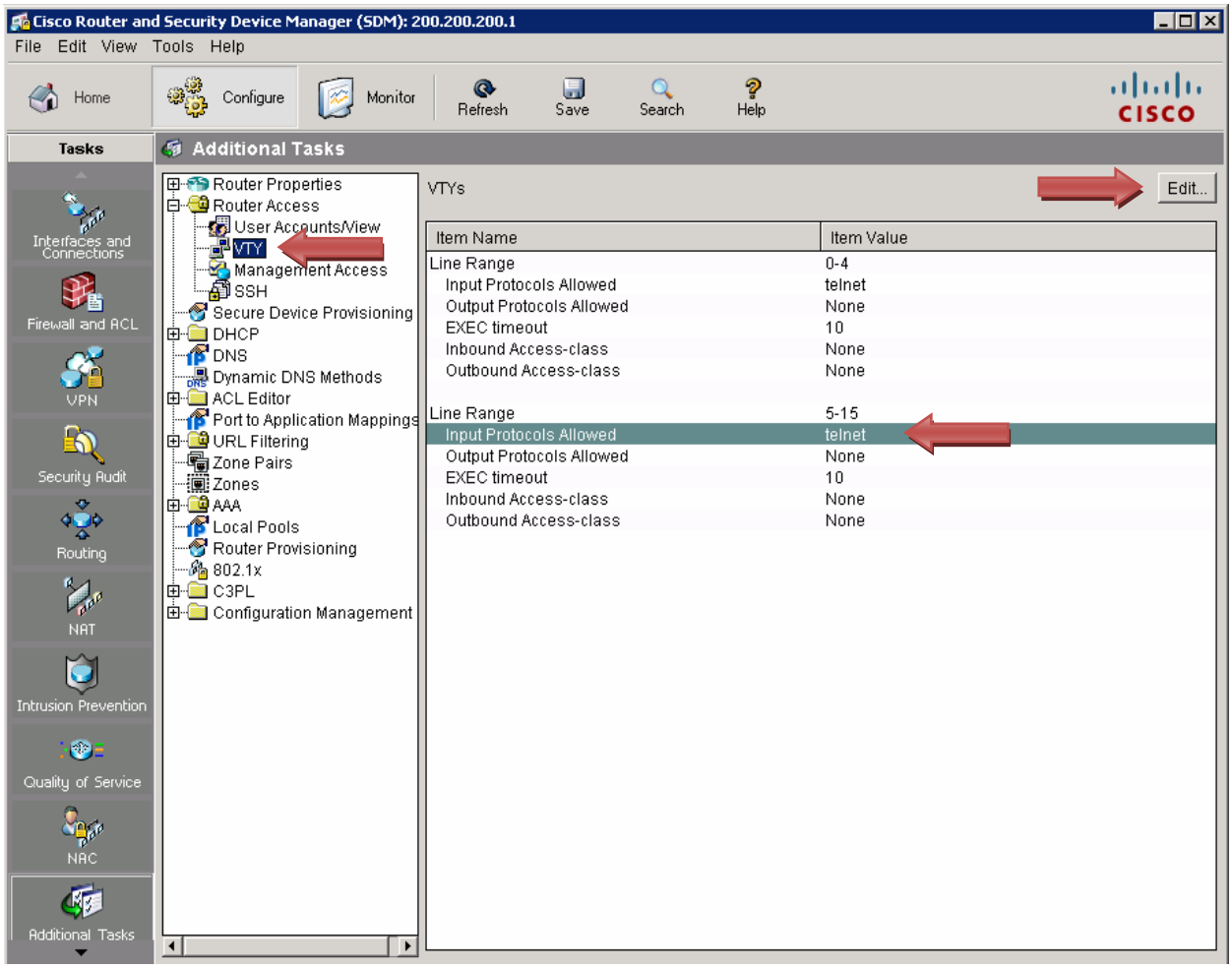
d. In the Enter SSH Credentials dialog box, enter **admin** for the username and **cisco123** for the password. Click **OK**.



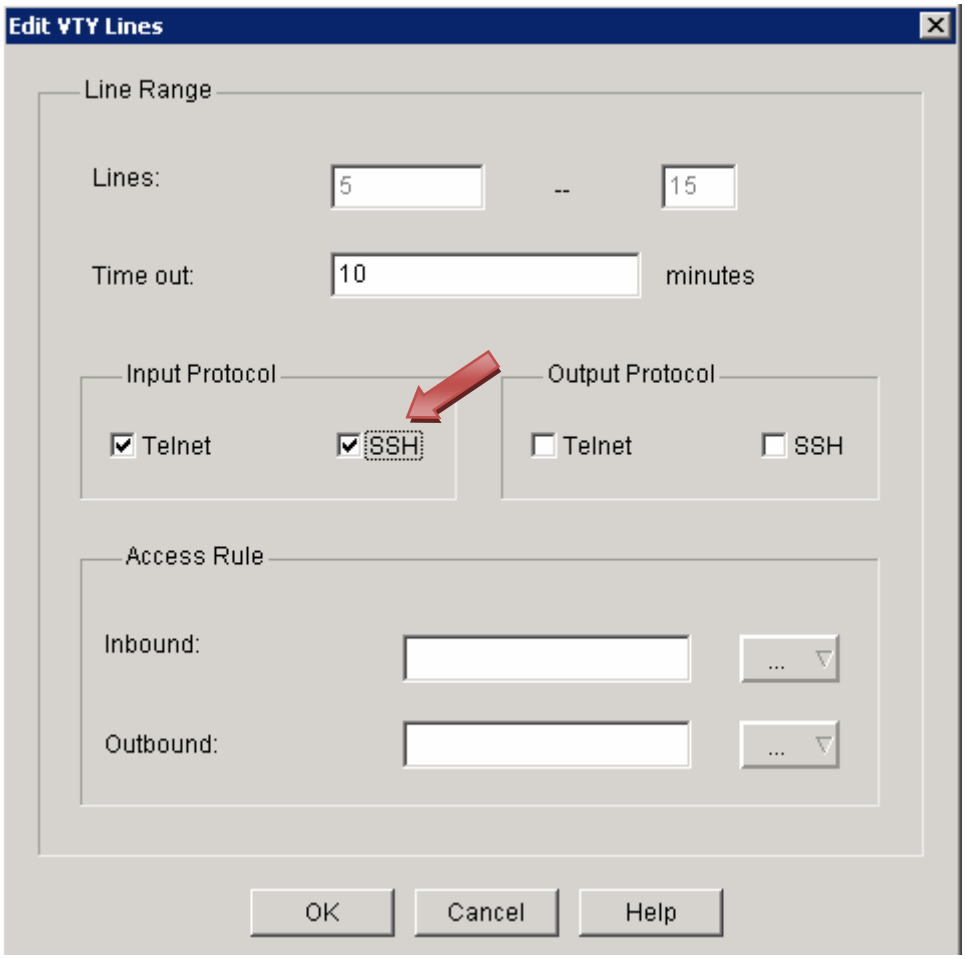
e. Notice that the Rivest, Shamir, and Adelman (RSA) key is now set on the router.



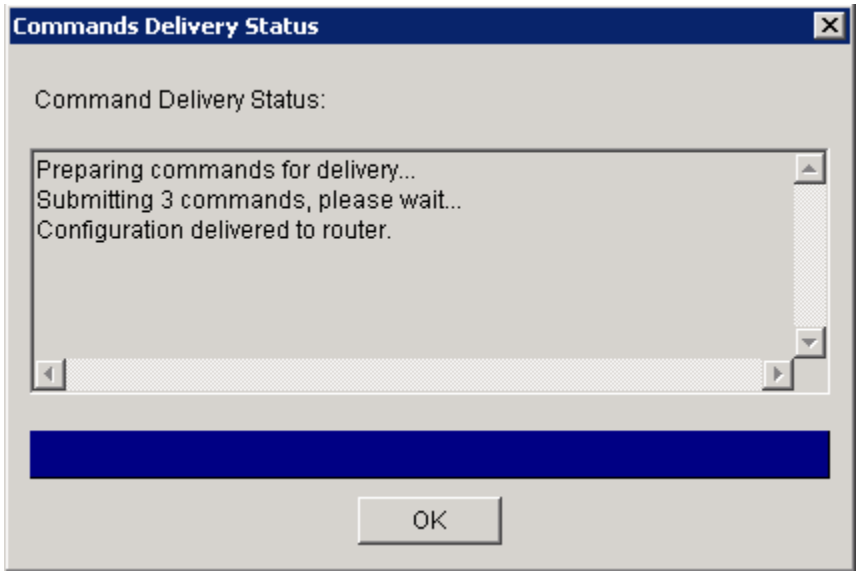
f. In the Additional Tasks pane, click the **VTY** option. Select **Input Protocols Allowed** and then click the **Edit** button.



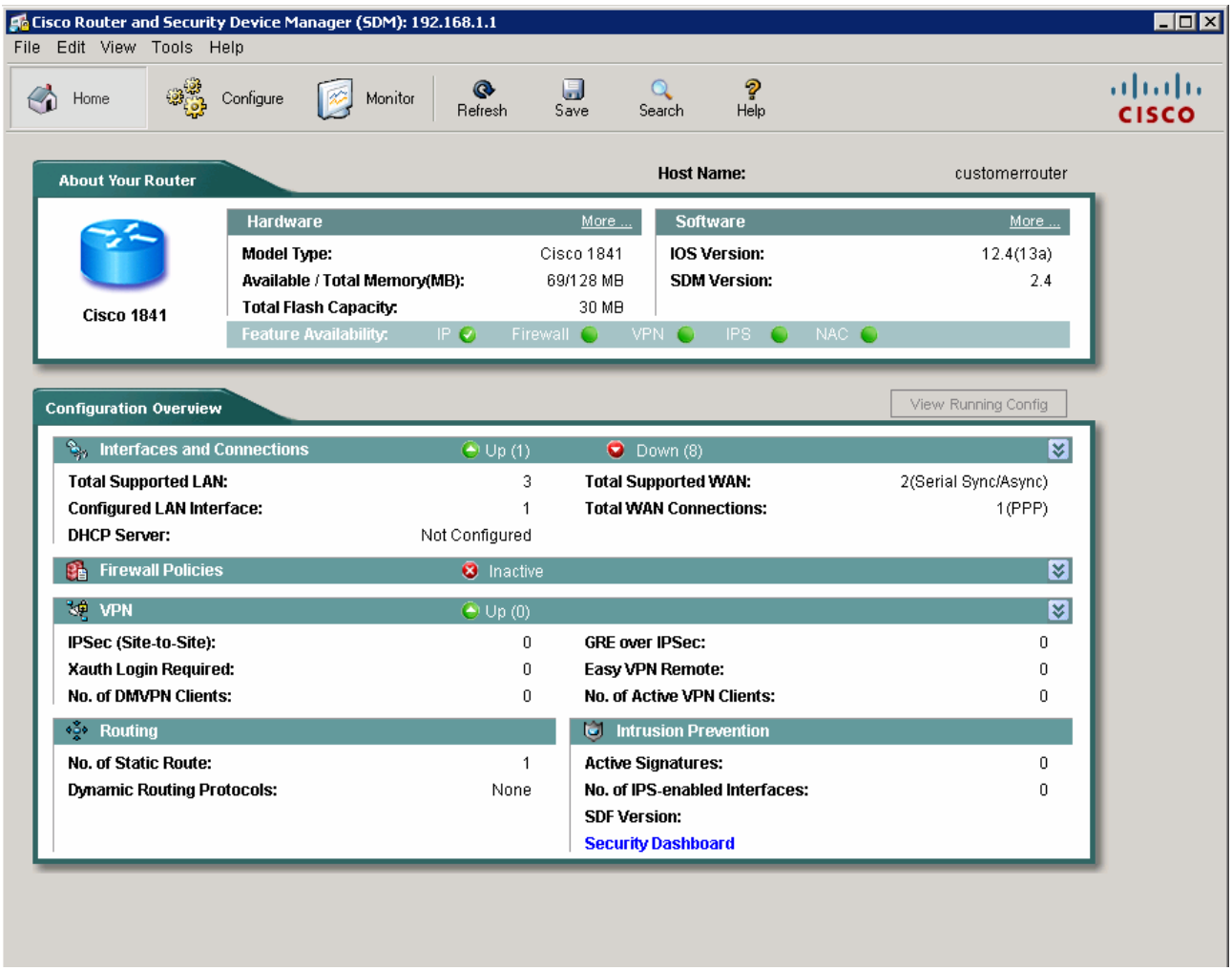
g. Check the box next to **SSH** and then click **OK**.



h. When the Commands Delivery Status window opens, click **OK**.



i. Close the Cisco SDM by clicking the **X** in the upper right corner of the window.



j. Click **Yes** to confirm the closing of the SDM.

Step 2: (OPTIONAL) Configure SSH on non-SDM router

NOTE: If you are configuring a router for SSH that already has SDM installed, you can skip Step 2 and go directly to Step 3.

a. If you are configuring a router to receive SSH connections that does not have SDM installed, connect the router console port with a PC and the HyperTerminal program, as described in Lab 5.1.2, "Powering up an ISR."

b. Log in to the router. From the privileged EXEC mode prompt, enter the Cisco IOS CLI commands as shown below. These commands do not include all of the passwords that need to be set. Refer to Lab 5.3.4, "Configuring Basic Router Settings with IOS CLI," for additional information on configuration settings.

NOTE: The router should be running IOS 12.0 or higher. In this example, the router is a Cisco model 2620XM with IOS 12.2(7r).

c. Configure the basic router and interface information:

```
Router#config terminal
Router(config)#hostname CustomerRouter
CustomerRouter(config)#ip domain-name customer.com
CustomerRouter(config)#username admin privilege 15 password 0 cisco123
CustomerRouter(config)#interface FastEthernet 0/0
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
```

d. Configure the remote incoming vty terminal lines to accept Telnet and SSH:

```
CustomerRouter(config)#line vty 0 4
CustomerRouter(config-line)#privilege level 15
CustomerRouter(config-line)#login local
CustomerRouter(config-line)#transport input telnet ssh
CustomerRouter(config-line)#exit
```

e. Generate the RSA encryption key pair for the router to use for authentication and encryption of SSH data that is transmitted. Enter **768** for the number of modulus bits. The default is 512.

```
CustomerRouter(config)#crypto key generate rsa

How many bits in the modulus [512] 768

CustomerRouter(config)#exit
```

f. Verify that SSH has been enabled and the version being used.

```
CustomerRouter#show ip ssh
```

g. Fill in the following information based on the output of the **show ip ssh** command:

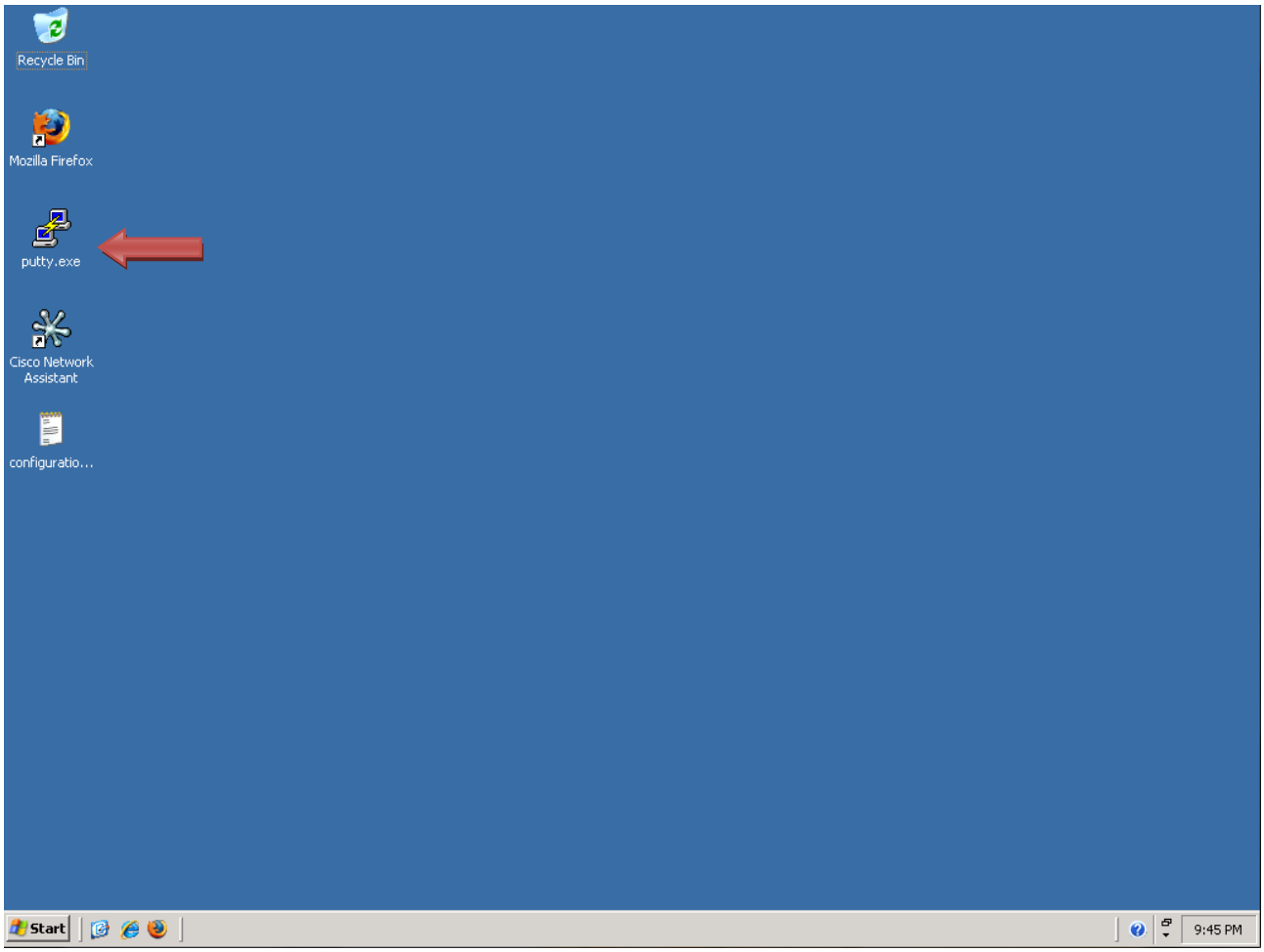
SSH version enabled: _____
Authentication timeout: _____
Authentication retries: _____

h. Save the running-config to the startup-config:

```
CustomerRouter#copy running-config startup-config
```

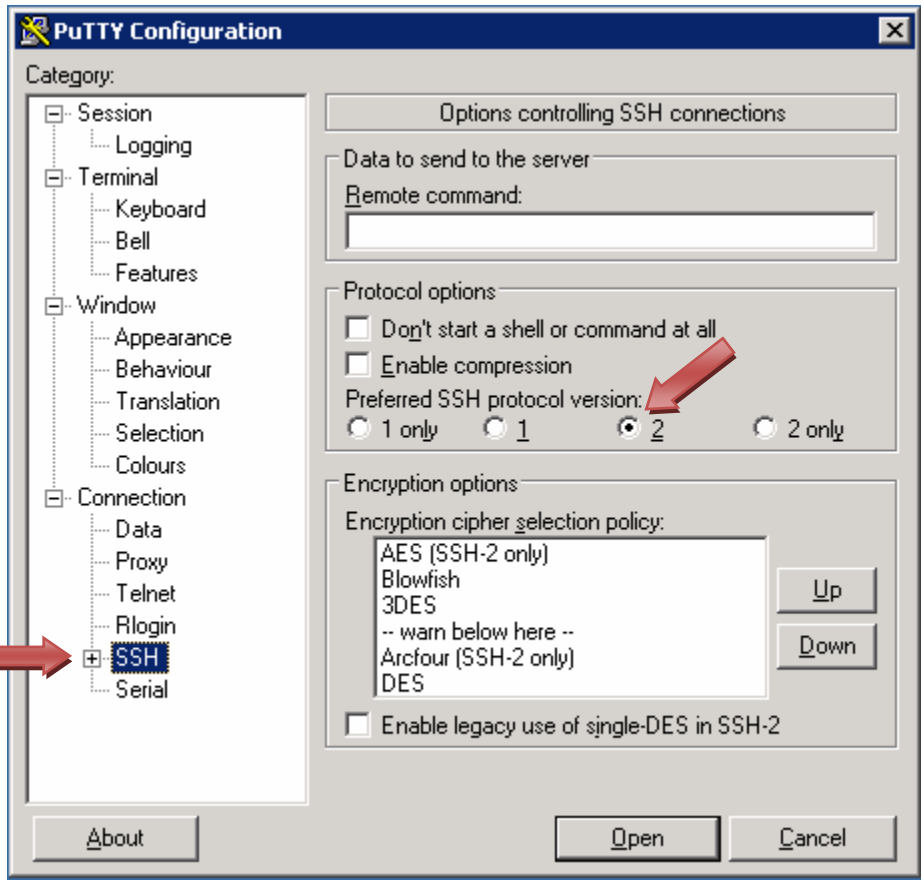

Step 3: Configure the SSH client and connect the PC to the ISR

a. Obtain a copy of putty.exe and place the application on the desktop. Launch PuTTY by double-clicking the **putty.exe** icon.

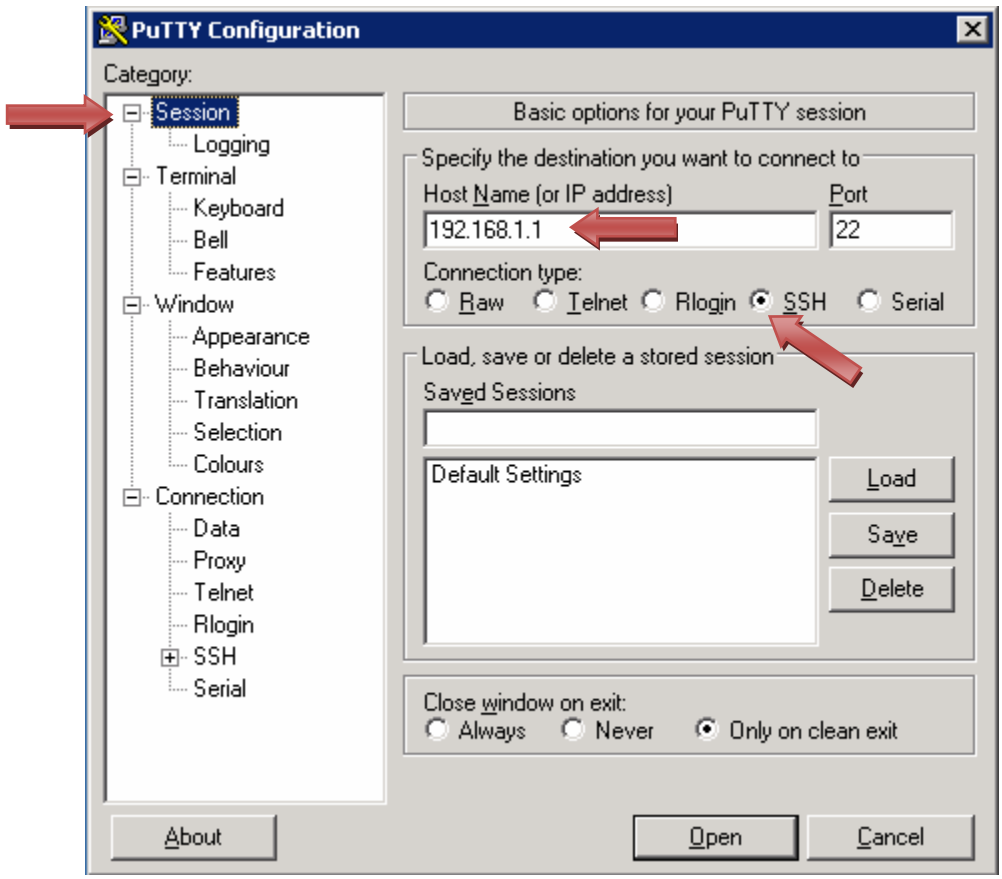


b. From the Category pane, select **SSH** and verify that the preferred SSH protocol version is set to **2**.

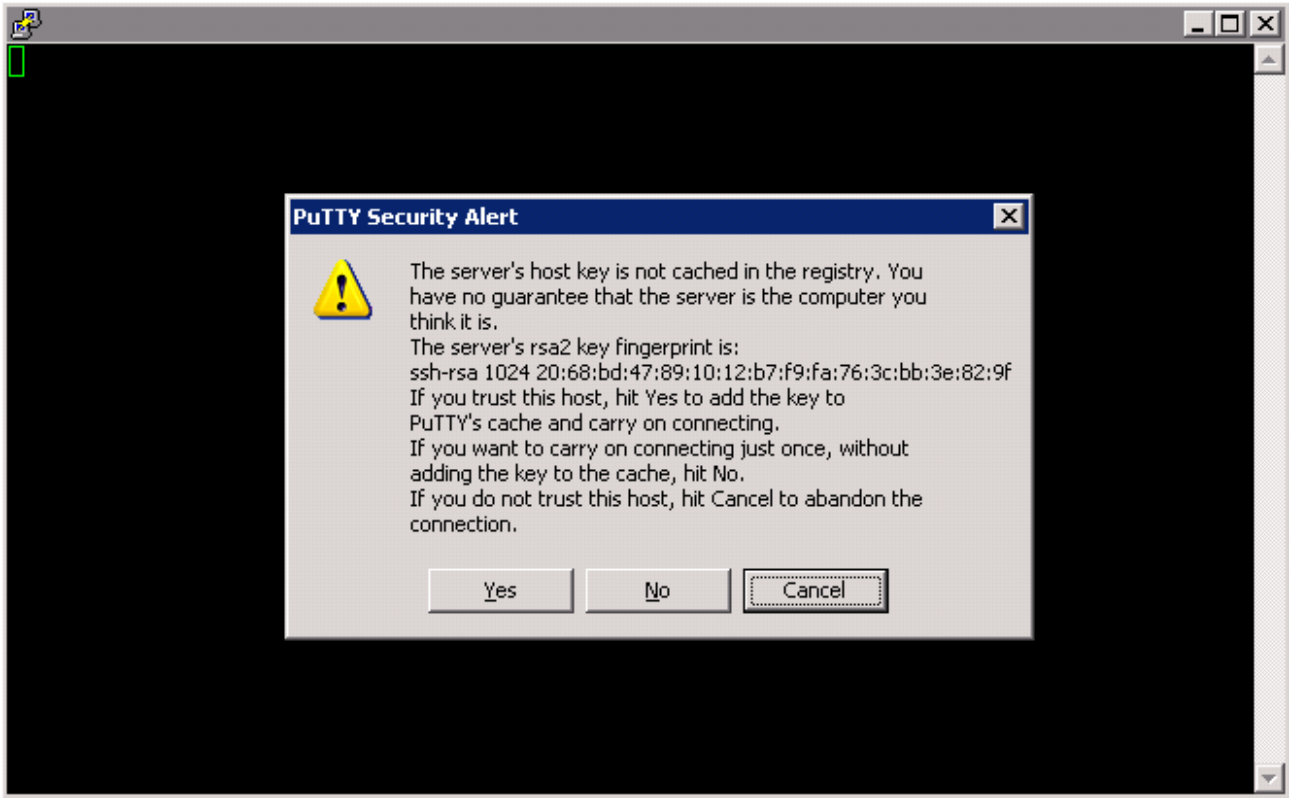
NOTE: The Putty client will still connect even if the SSH server is running SSH version 1.



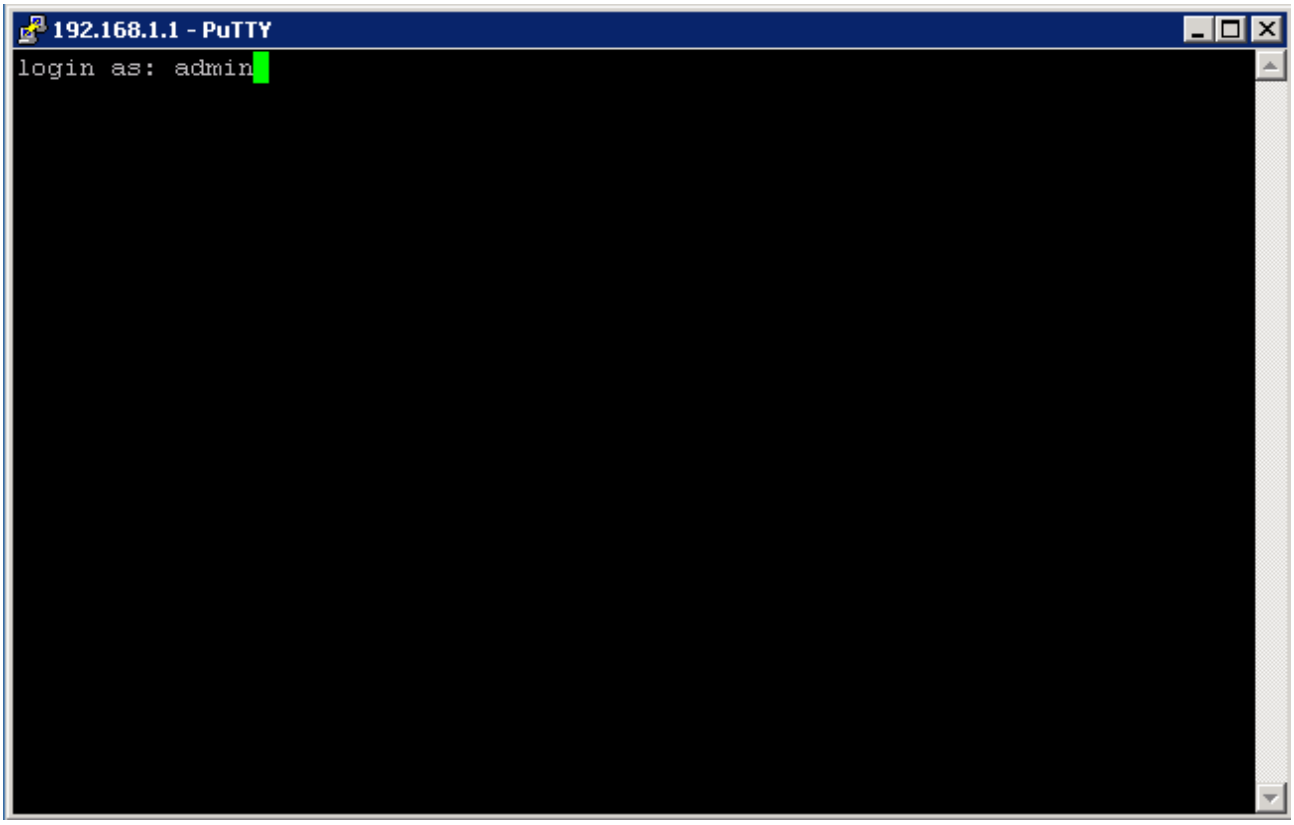
c. From the Category pane, select **Session** and enter the IP address of the router LAN interface, which is 192.168.1.1. Verify that SSH is selected for the connection type. Click **Open**.



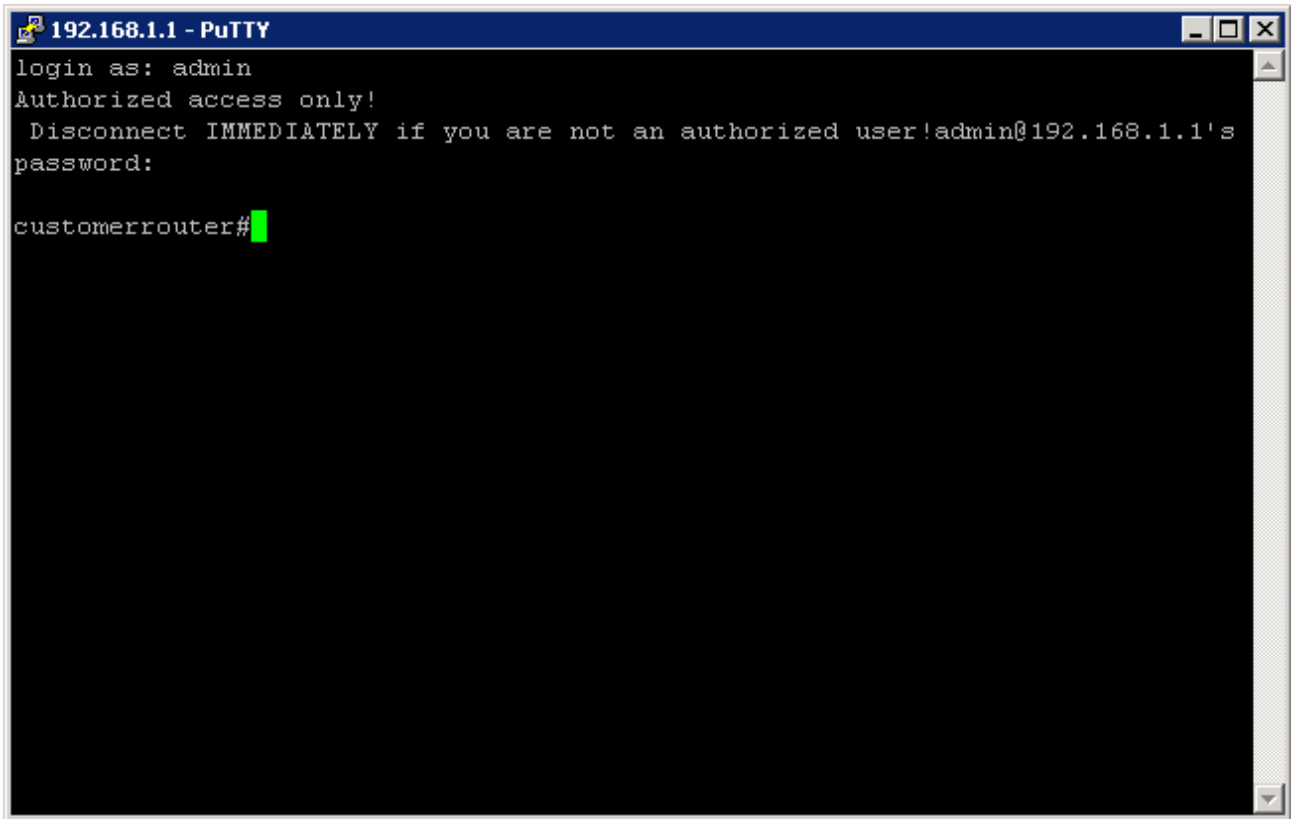
d. The first time a connection is made to the SSH service on the Cisco 1841 ISR using an SSH client, a connection key is cached in the local machine registry. In the PuTTY Security Alert window, click **Yes** to continue.



e. At the login prompt, type the administrator username, **admin**, and press **Enter**.



f. At the password prompt, type the administrator password, **cisco123**, and click **Enter**. .

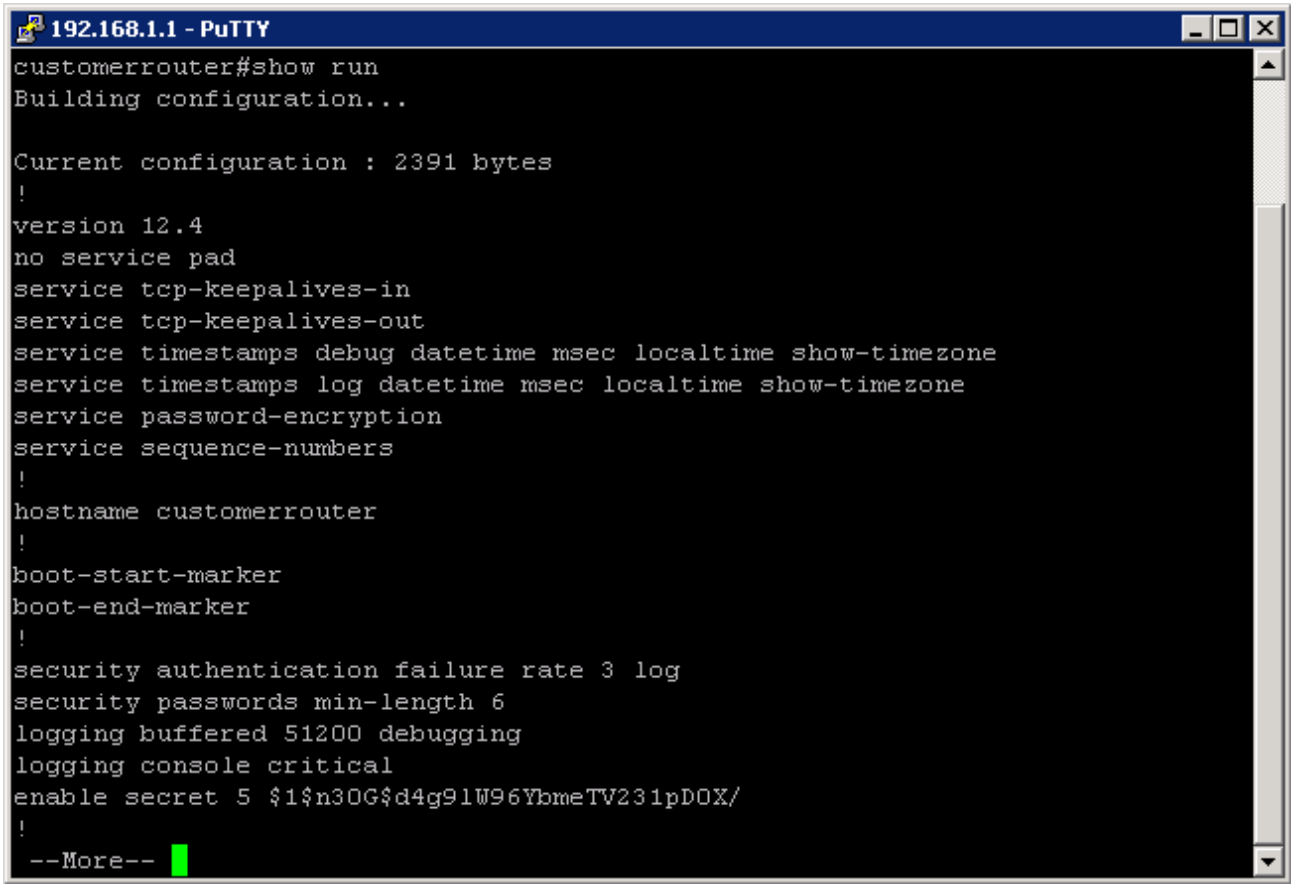


Step 4: Check the configuration of the Cisco 1841 ISR

a. To verify the configuration of the router, type **show run** at the privileged mode prompt, and press **Enter**.

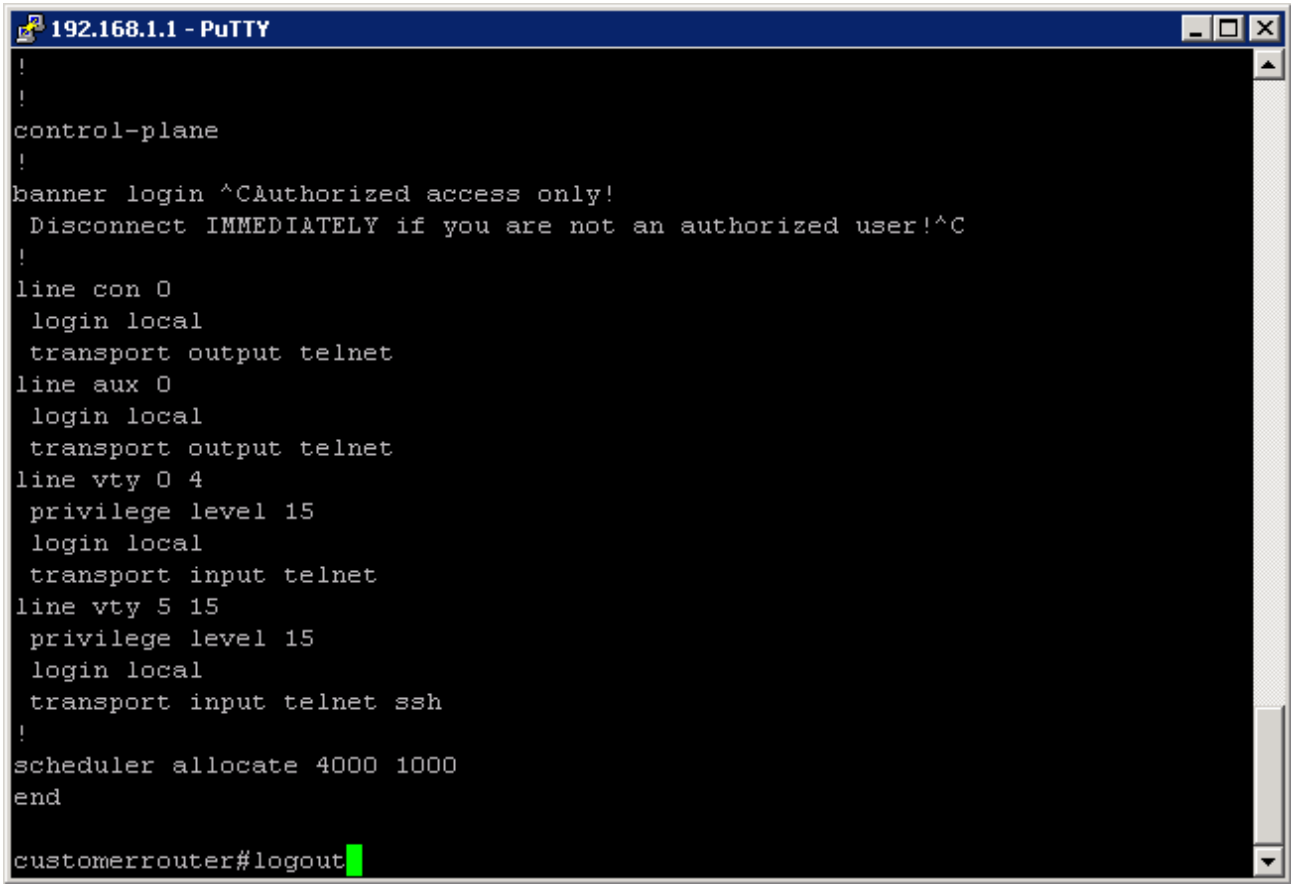
NOTE: There is no need to switch from user mode to privileged mode because after you configure from SDM Express and SDM, privileged mode is the default mode.

b. Press the **Spacebar** to scroll through the current configuration of the router.



Step 5: Log out of the Cisco 1841 ISR

To log out of the router when you are finished verifying the configuration, type **logout** at the privileged mode prompt, and then press **Enter**.



Step 6: Reflection

a. When comparing Telnet and SSH, what are some advantages and disadvantages?

_____

_____

b. What is the default port for SSH? _____ What is the default port for Telnet? _____

_____

_____

c. What Cisco IOS software version was displayed in the running-config?

_____

_____

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the router's HTTP/HTTPS server, using the following Cisco IOS
commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>

   Replace <username> and <password> with the username and password that
   you want to configure.

4)  Configure SSH and Telnet for local login and privilege level 15:
   Router(config)# line vty 0 4
```

```
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Lab 6.1.2 Creating a Network Diagram from Routing Tables

Objectives

- Interpret router outputs.
- Identify networks and IP addresses for each router.
- Draw a diagram of the network topology.
- Reflect upon and document the network implementation.

Background / Preparation

In this lab you will create a network topology diagram based only on the output of the **show ip route** command from two routers. The **show ip route** command displays the current state of the routing table. Routers R1 and R2 are directly connected over a WAN link and both are running the RIP dynamic routing protocol. In addition to the WAN link, each of the routers is connected to its own local networks.

Step 1: Examine the routing table entries for the router R1

a. Examine the **show ip route** output from router R1 shown below.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
C    192.168.2.0/24 is directly connected, FastEthernet0/1
R    192.168.3.0/24 [120/1] via 172.17.0.2, 00:00:17, Serial0/0
R    192.168.4.0/24 [120/1] via 172.17.0.2, 00:00:17, Serial0/0
```

b. How many networks does router R1 know about? _____

c. How many networks are directly connected to this router? _____

d. How many networks have been learned from another router? _____

e. Using the codes at the beginning of the show ip route output, what does the “R” mean?
_____

f. In the routes learned via RIP, to which device does the IP address 172.17.0.2 belong? _____

g. In the routes learned via RIP, to which device is Serial0/0 referring and what does it mean?
_____

Step 2: Examine the routing table entries for router R2

a. Examine the **show ip route** output from router R2 shown below..

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
R    192.168.1.0/24 [120/1] via 172.17.0.1, 00:00:17, Serial0/0
R    192.168.2.0/24 [120/1] via 172.17.0.1, 00:00:17, Serial0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
C    192.168.4.0/24 is directly connected, FastEthernet0/1
```

b. How many networks does router R2 know about? _____

c. How many networks are directly connected to this router? _____

d. How many networks have been learned from another router? _____

e. In the routes learned via RIP, to which device does the IP address 172.17.0.1 belong? _____

f. In the routes learned via RIP, to which device is Serial0/0 referring and what does it mean?

_____

Step 3: Document router interfaces and IP addresses

a. Based on the **show ip route** output from routers R1 and R2, fill in the table with the router name, the names of all interfaces in use, and their IP addresses and subnet masks. Use the first available IP address for each of the local network FastEthernet interfaces.

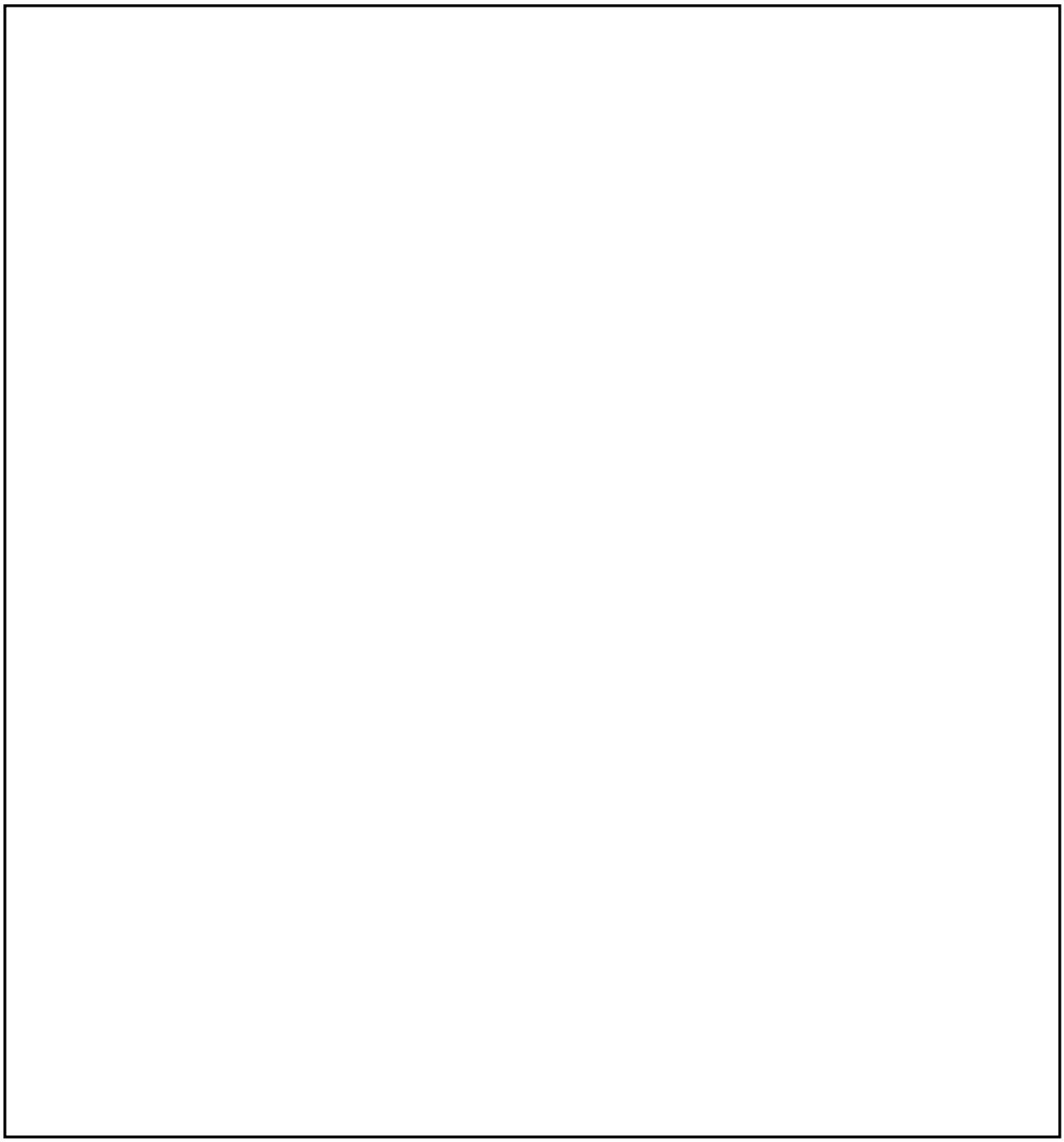
Device Name	**Interface**	**IP Address**	**Subnet Mask (Dotted decimal and /xx)**
R1			
R1			
R1			
R2			
R2			
R2			

b. In this example, can the exact IP address of all router interfaces be determined by looking at the routing tables? ____

c. Which router interface IP addresses can be determined from the routing tables?
_____

Step 4: Create a network topology diagram

Based on the **show ip route** output from routers R1 and R2, and the information you entered in the table, draw the network topology here. Be sure to include all devices, connections, interfaces, IP addresses, subnet masks, and network numbers.



Step 5: Reflection

a. What do you think would happen to the entries in the routing table on R1 if one of the Ethernet networks on R2 was disconnected?

_____

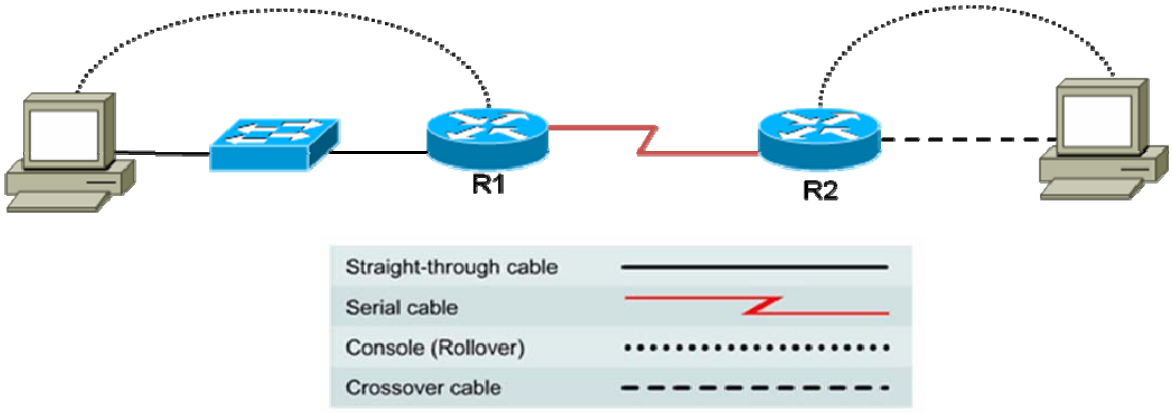
_____

b. What do you think would happen to the entries in the routing tables on R1 and R2 if the Serial interface on R2 was shut down?

_____

_____

Lab 6.1.5 Configure and Verify RIP



Router Designation	Router Name	Fast Ethernet 0 Address	Serial 0 Address	Interface Type	Subnet mask for both interfaces
Router 1	R1	172.16.0.1	172.17.0.1	DCE	255.255.0.0
Router 2	R2	172.18.0.1	172.17.0.2	DTE	255.255.0.0

Objective

- Implement RIP routing and verify that network routes are being exchanged dynamically.

Background / Preparation

Set up a network similar to the one in the diagram above. You can use any router or combination of routers that meets the interface requirements in the diagram, such as 800, 1600, 1700, 1800, 2500, or 2600 routers. Refer to the chart at the end of the lab to correctly identify the interface identifiers to be used based on the equipment in the lab. Depending on the model of router, your output may vary from the output shown in this lab. The lab steps are intended to be executed on each router, unless you are specifically instructed otherwise.

Before you begin the lab, start a HyperTerminal session.

NOTE: Use the erase and reload instructions at the end of this lab on all routers before continuing.

The following resources are required:

- Two routers, each with an Ethernet and Serial interface. These should be non-SDM routers, if possible, since the required SDM startup configuration is deleted when the startup-config is erased.
- Two Windows XP computers
- Straight-through category 5 Ethernet cable (PC1 to switch)
- Crossover category 5 Ethernet cable (PC2 to router R2)
- Null Serial cable
- Console cable(s) (from PCs 1 and 2 to routers R1 and R2)
- Access to the PC command prompt

- Access to PC network TCP/IP configuration

Step 1: Build the network and configure the routers

a. Build a network as shown in the topology diagram

b. In global configuration mode, configure the hostnames as shown in the chart in the topology diagram. Next, configure the interfaces according to the chart. You can use either the command-line interface (CLI) or Security Device Manager (SDM) GUI interface, if available.

NOTE: Refer to Lab 5.3.5 if you have difficulty with the basic router configuration. That lab provides instructions for using the Cisco IOS command line interface.

Step 2: Check the routing table entries

a. View the IP routing table for R1 using the **show ip route** command:

```
R1>show ip route
<output omitted>
Gateway of last resort is not set
C 172.16.0.0/16 is directly connected, FastEthernet0/0
C 172.17.0.0/16 is directly connected, Serial0/0/0
```

b. What is the significance of the “C” to the left of the 172.16.0.0 and 172.17.0.0 network entries in the routing table?

_____

Step 3: Configure the routing protocol of the routers

There are two versions of RIP: version 1 and version 2. It is important to specify RIP version 2 (RIPv2) in this configuration, because RIPv2 is the most current version. Some routers default to RIPv2, but it is best to not assume that is the case.

a. In global configuration mode, enter the following on R1:

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 172.16.0.0
R1(config-router)#network 172.17.0.0
R1(config-router)#exit
R1(config)#exit
```

b. Save the R1 router configuration:

```
R1#copy running-config startup-config
```

c. In global configuration mode, enter the following on R2:

```
R2(config)#router rip version 2
R2(config-router)#version 2
R2(config-router)#network 172.17.0.0
R2(config-router)#network 172.18.0.0
R2(config-router)#exit
R2(config)#exit
```

d. Save the R2 router configuration:

```
R2#copy running-config startup-config
```

Step 4: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure the host attached to R1 with an IP address, subnet mask and default gateway that is compatible with the IP address of the Fast Ethernet interface (172.16.0.0).

b. Configure the host attached to R2 with an IP address, subnet mask and default gateway that is compatible with the IP address of the Fast Ethernet interface (172.18.0.0).

c. Verify that the internetwork is functioning by pinging the Fast Ethernet interface of the other router.

d. From the host attached to R1, is it possible to ping the R2 router Fast Ethernet interface?

_____

e. From the host attached to R2, is it possible to ping the R1 router Fast Ethernet interface?

_____

f. If the answer is no for either question, troubleshoot the router configurations to find the error. Then do the pings again until the answer to both questions is yes. Be sure to check physical cabling for problems and bad connections and make sure that you are using the correct cable types.

Step 5: Show the routing tables for each router

a. In enable or privileged EXEC mode, examine the routing table entries using the **show ip route** command on router R1.

```
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B -
BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
C    172.16.0.0/16 is directly connected, FastEthernet0/0
R    172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:17, Serial0/0
```

b. What are the entries in the R1 routing table?

_____

_____

c. What is the significance of the “R” to the left of the 172.18.0.0 network entry in the routing table?

_____

d. What does “via 172.17.0.2” mean for this network route?

_____

e. What does “Serial0/0” mean for this network route?

_____

f. Examine the routing table entries using the **show ip route** command on router R1.

```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
```

```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    172.17.0.0/16 is directly connected, Serial0/0
R    172.16.0.0/16 [120/1] via 172.17.0.1, 00:00:13, Serial0/0
C    172.18.0.0/16 is directly connected, FastEthernet0/0
```

g. What are the entries in the R2 routing table?

_____

_____

Step 6: Use debug to observe RIP communications

Using the **debug ip rip** command, you can see real-time communication and updates passing between routers that are running RIP.

NOTE: Running debug commands puts a significant load on the CPU of the router. Do not use debug commands on a production network, if possible.

a. On router R1, enter the **debug ip rip** command from privileged EXEC mode. Examine the exchange of routes between the two routers. The output should look similar to that shown here.

```
R1#debug ip rip
RIP protocol debugging is on
R1#
00:51:28: RIP: sending v2 update to 224.0.0.9 via Serial0/0 (172.17.0.1)
00:51:28: RIP: build update entries
00:51:28:       172.16.0.0/16 via 0.0.0.0, metric 1, tag 0
00:51:49: RIP: received v2 update from 172.17.0.2 on Serial0/0
00:51:49:      172.18.0.0/16 via 0.0.0.0 in 1 hops
00:51:57: RIP: sending v2 update to 224.0.0.9 via FastEthernet0/0
(172.16.0.1)
00:51:57: RIP: build update entries
00:51:57:       172.17.0.0/16 via 0.0.0.0, metric 1, tag 0
00:51:57:       172.18.0.0/16 via 0.0.0.0, metric 2, tag 0
```

b. Enter the command **undebug all** to stop all debugging activity.

```
R1#undebug all
All possible debugging has been turned off
R1#
```

c. What interface does router R1 send and receive updates through? _____

d. Why does the route to 172.17.0.0 have metric of 1 and the route to 172.18.0.0 have a metric of 2?

_____

e. Log off by typing **exit** and turn off the router.

Step 7: Reflection

a. What do you think would happen to the routing table on router R1 if the Ethernet network on router R2 went down?

_____

_____

b. What do you think would happen if router R1 was configured to run RIPv1, and R2 was configured to run RIPv2?

_____

_____

Erasing and reloading the router

a. Enter into privileged EXEC mode by typing **enable**:

```
Router>enable
```

b. In privileged EXEC mode, enter the **erase startup-config** command:

```
Router#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

c. Press **Enter** to confirm.

The response is:

```
Erase of nvram: complete
```

d. In privileged EXEC mode, enter the **reload** command:

```
Router(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

e. Type **n** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm]
```

f. Press **Enter** to confirm.

In the first line of the response is:

```
Reload requested by console.
```

After the router has reloaded, the line prompt is:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

g. Type **n** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started!
```

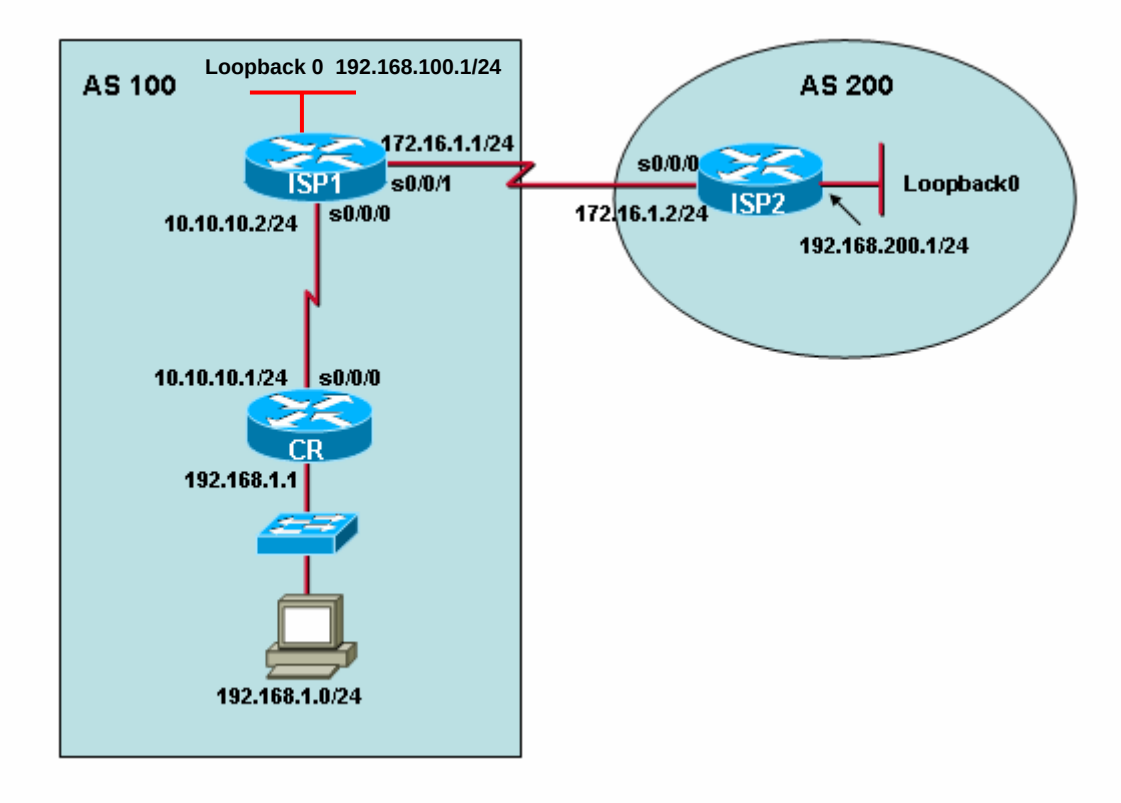
h. Press **Enter**.

The router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	**Ethernet Interface #1**	**Ethernet Interface #2**	**Serial Interface #1**	**Serial Interface #2**
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

To find out exactly how the router is configured, look at the interfaces. This will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in a Cisco IOS command to represent the interface.

Lab 6.2.5 Configuring BGP with Default Routing



Objectives

- Configure the customer router with an internal network that will be advertised by ISP1 via Border Gateway Protocol (BGP).
- Configure BGP to exchange routing information between ISP1 in AS 100 and ISP2 in AS 200.

Background / Preparation

A small company needs access to the Internet. They have arranged for services to be provided by their local ISP (ISP1). ISP1 connects to the Internet through ISP2 using an external routing protocol. BGP4 is the most popular routing protocol between ISPs on the Internet. In this lab, the customer router will connect to the ISP using a default route and ISP1 will connect to ISP2 via BGP4.

The following resources are required:

- Customer router (1841 or other)
- Switch (optional if crossover cable is used between PC and customer router)
- 2 ISP routers (1841 or other routers that support BGP)
- PC with terminal emulation program installed
- Console cable to configure routers
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

On the PC, start a HyperTerminal session to each router.

NOTE: Go to the "Erasing and reloading the router" instructions at the end of this lab. Perform those steps on all routers in this lab assignment before continuing.

NOTE: SDM Routers - If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. Refer to the procedure at the end of this lab or contact your instructor.

Step 1: Configure basic information on each router

a. Build and configure the network according to the topology diagram, but do not configure a routing protocol. If necessary, refer to Lab 5.3.5, "Configuring Basic Router Settings with IOS CLI," for instructions on setting hostname, passwords, and interface addresses.

b. Configure the host PC IP address and subnet mask on the customer network to be compatible with the CR router FastEthernet interface with a default gateway of 192.168.1.1.

c. Use **ping** to test connectivity between the directly connected routers. Was the CR router able to reach the ISP2 router? ____ Was the customer host able to reach ISP1? ____

d. Configure a loopback interface with an IP address for the ISP1 and ISP2 routers, as shown in the topology diagram. A loopback interface is a virtual interface that simulates a real network for testing purposes. Configure Loopback Interface on ISP1 router.

```
ISP1>enable
ISP1#configure terminal
ISP1(config)#interface loopback0
ISP1(config-if)#ip address 192.168.100.1 255.255.255.0
```

e. Configure Loopback Interface on ISP2 router.

```
ISP2>enable
ISP2#configure terminal
ISP2(config)#interface loopback0
ISP2(config-if)#ip address 192.168.200.1 255.255.255.0
```

Step 2: Configure the default and static routes

a. On the CR router, configure the default route so that users will have access to ISP1:

```
CR(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.2
```

b. On the ISP1 router, configure a static route back to the customer's network:

```
ISP1(config)#ip route 192.168.1.0 255.255.255.0 10.10.10.1
```

c. Test connectivity by issuing a ping from the host to ISP1 at 10.10.10.2.

NOTE: If pings are not successful, troubleshoot router and PC configurations and connections as necessary.

Step 3: Configure BGP on both ISP routers

a. Configure BGP on the ISP1 router:

```
ISP1(config)#router bgp 100
ISP1(config-router)#neighbor 172.16.1.2 remote-as 200
ISP1(config-router)#network 192.168.1.0
ISP1(config-router)#network 192.168.100.0
ISP1(config-router)#end
ISP1#copy running-config startup-config
```


NOTE: It is always good practice to save your configuration frequently, especially after completing major configuration steps.

b. Configure BGP on the ISP2 router:

```
ISP2(config)#router bgp 200
ISP2(config-router)#neighbor 172.16.1.1 remote-as 100
ISP2(config-router)#network 192.168.200.0
ISP2(config-router)#end
ISP2#copy running-config startup-config
```

Step 4: View the Routing Tables

The BGP configuration is complete. Check the routing table for each router.

NOTE: Output may vary slightly depending on the model of router used.

a. `ISP2#show ip route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/0
C    192.168.200.0/24 is directly connected, Loopback0
B    192.168.1.0/24 [20/0] via 172.16.1.1, 00:40:38
B    192.168.100.0/24 [20/0] via 172.16.1.1, 00:40:38
```

1) Is network 192.168.1.0 in the routing table of ISP2? _____
2) What letter is at the left of the entry for 192.168.1.0? ____
3) What does the letter mean? _____

   _____
4) Is network 192.168.100.0 in the routing table? _____
5) Which router advertised network 192.168.1.0? _____

b. `ISP1#show ip route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
C       172.16.1.0 is directly connected, Serial0/1
B    192.168.200.0/24 [20/0] via 172.16.1.2, 00:33:45
     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0
S    192.168.1.0/24 [1/0] via 10.10.10.1
         C    192.168.100.0/24 is directly connected, Loopback0
```

1) What network(s) did ISP1 learn from ISP2? _____

2) How did ISP1 learn about network 192.168.1.0? _____

_____

3) Will ISP1 advertise any networks to the customer router? _____

c. `CR#show ip route`

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter
area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.10.10.2 to network 0.0.0.0

     10.0.0.0/24 is subnetted, 1 subnets
C       10.10.10.0 is directly connected, Serial0/0
C    192.168.1.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.10.10.2
```

1) Why are networks 192.168.100.0 and 192.168.200.0 not in CRs routing table?

_____

Step 5: Verify connectivity

a. Ping from the host PC on the CR Ethernet network to the Loopback Interface on ISP2.

b. Ping from the ISP2 router to the host PC on the Ethernet network of CR.

NOTE: If pings are not successful, troubleshoot router and PC configurations and connections as necessary.

Step 6: View BGP information on the ISP routers

a. On the ISP1 router, view the BGP routing.

```
ISP1#show ip bgp
BGP table version is 4, local router ID is 192.168.100.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.10.10.1               0         32768 i
*> 192.168.100.0    0.0.0.0                  0         32768 i
*> 192.168.200.0    172.16.1.2               0             0 200 i
```

b. On the ISP2 router, view the BGP routing.

```
ISP2#show ip bgp
BGP table version is 4, local router ID is 192.168.200.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      172.16.1.1               0             0 100 i
*> 192.168.100.0    172.16.1.1               0             0 100 i
*> 192.168.200.0    0.0.0.0                  0         32768 i
```

Step 7: Reflection

Why doesn't ISP1 advertise any networks to the customer router?

_____

_____

Erasing and reloading the router

a. Enter into privileged EXEC mode by typing **enable**.

```
Router>enable
```

c. In privileged EXEC mode, enter the **erase startup-config** command.

```
Router#erase startup-config
```

The responding line prompt is:

```
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
```

d. Press **Enter** to confirm.

The response is:

```
Erase of nvram: complete
```

e. In privileged EXEC mode, enter the **reload** command.

```
Router(config)#reload
```

The responding line prompt is:

```
System configuration has been modified. Save? [yes/no]:
```

f. Type **n** and then press **Enter**.

The responding line prompt is:

```
Proceed with reload? [confirm]
```

g. Press **Enter** to confirm.

In the first line of the response is:

```
Reload requested by console.
```

After the router has reloaded the line prompt ise:

```
Would you like to enter the initial configuration dialog? [yes/no]:
```

h. Type **n** and then press **Enter**.

The responding line prompt is:

```
Press RETURN to get started!
```

i. Press **Enter**.

The router is ready for the assigned lab to be performed.

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)
NOTE: In order to find out exactly how the router is configured, look at the interfaces. Doing this will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.				

SDM router basic IOS configuration to bring up SDM

If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config as follows. Further details regarding the setup and use of SDM are can be found in the SDM Quick Start Guide:

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

```
1) Set the router Fa0/0 IP address
(This is the interface that a PC will connect to using a browser to bring
up SDM. The PC IP address should be set to 10.10.10.2  255.255.255.248)
```

NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

```
   Router(config)# interface Fa0/0
   Router(config-if)# ip address 10.10.10.1 255.255.255.248
   Router(config-if)# no shutdown

2)  Enable the router's HTTP/HTTPS server, using the following Cisco IOS
commands:
   Router(config)#ip http server
   Router(config)#ip http secure-server
   Router(config)#ip http authentication local

3) Create a user account with privilege level 15 (enable privileges).
   Router(config)# username <username> privilege 15 password 0 <password>
```

Replace <username> and <password> with the username and password that you want to configure.

4) Configure SSH and Telnet for local login and privilege level 15:

```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

Lab 7.3.1 Editing the HOSTS File in Windows

Objective

- Edit the local HOSTS file on a Windows PC to map a name to an IP address for easier identification.

Background / Preparation

You are employed at an ISP. You have been sent to a customer location to troubleshoot an issue with one of the customer's servers. There is a user on the network who constantly needs to access the server to administer a development website that the company is working on. Currently, the customer does not have any local servers that perform the function of associating a name to the server's IP address. However, the website that the customer is working on requires the use of a name in the URL to access the site properly. Since this is the only workstation that needs to access the server based on a name, you decide to use the local HOSTS file on the Windows workstation to resolve the issue with name resolution. Your plan is to edit the local HOSTS file and add a name mapping for the web server. You will test the functionality of the name resolution using the **ping** command from the command prompt.

The following resources are required:

- PC running Windows XP
- Administrator privileges on the PC

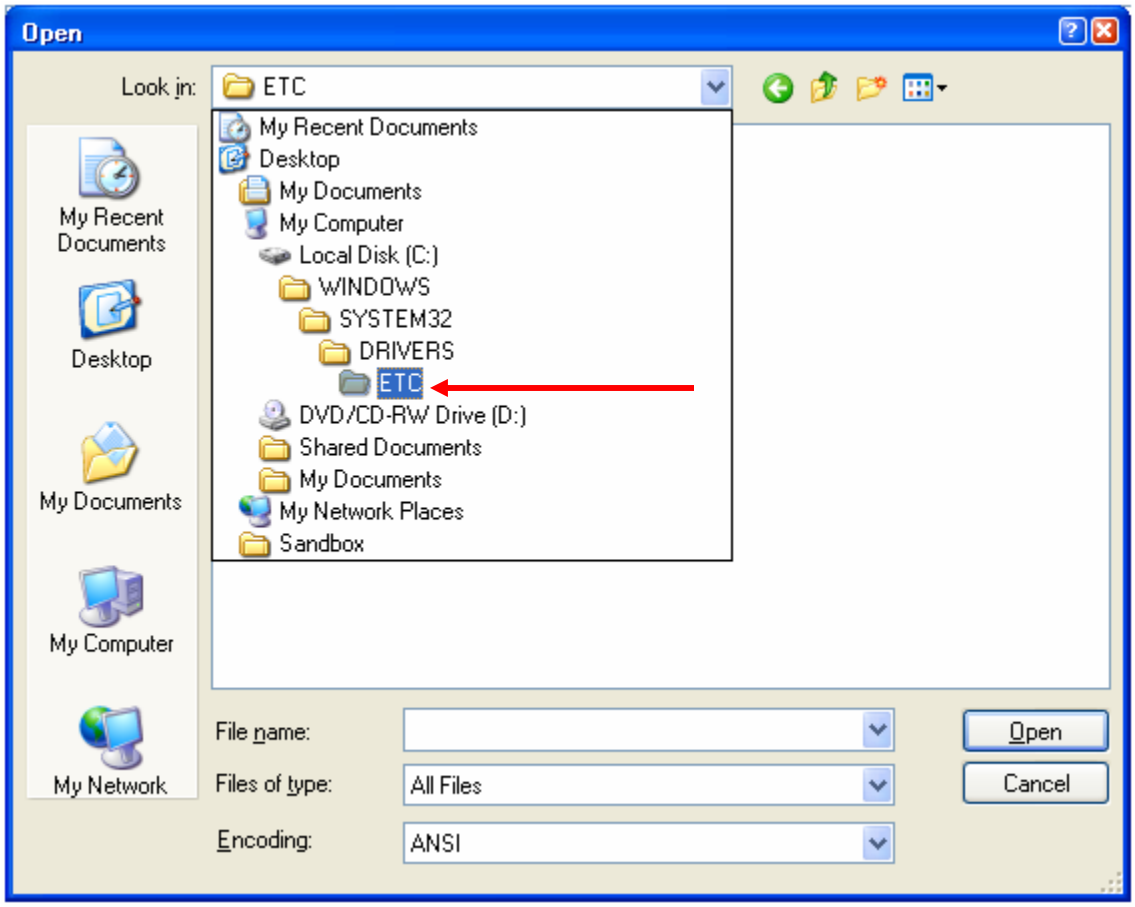
NOTE: The screen layout of your Windows-based operating system may be slightly different than what appears here, but the procedure is the same.

Step 1: Locate the HOSTS file in Windows

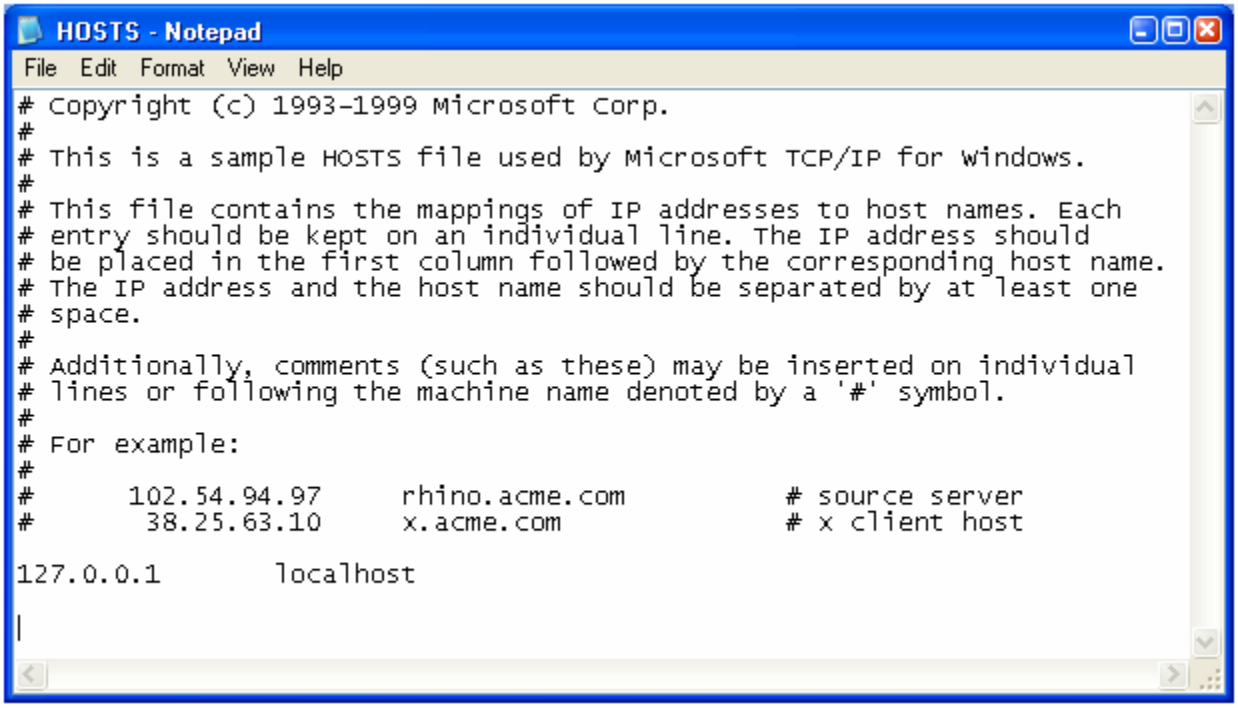
a. Click the **Start** button and choose **All Programs** > **Accessories**, and then click the **Notepad** program.

b. In Notepad, choose **File > Open**. Change the **Files of Type** to **All Files** to be able to see files other than text files. Navigate to C:\WINDOWS\SYSTEM32\DRIVERS\ETC.

c. Select the **HOSTS** file and click **Open**.

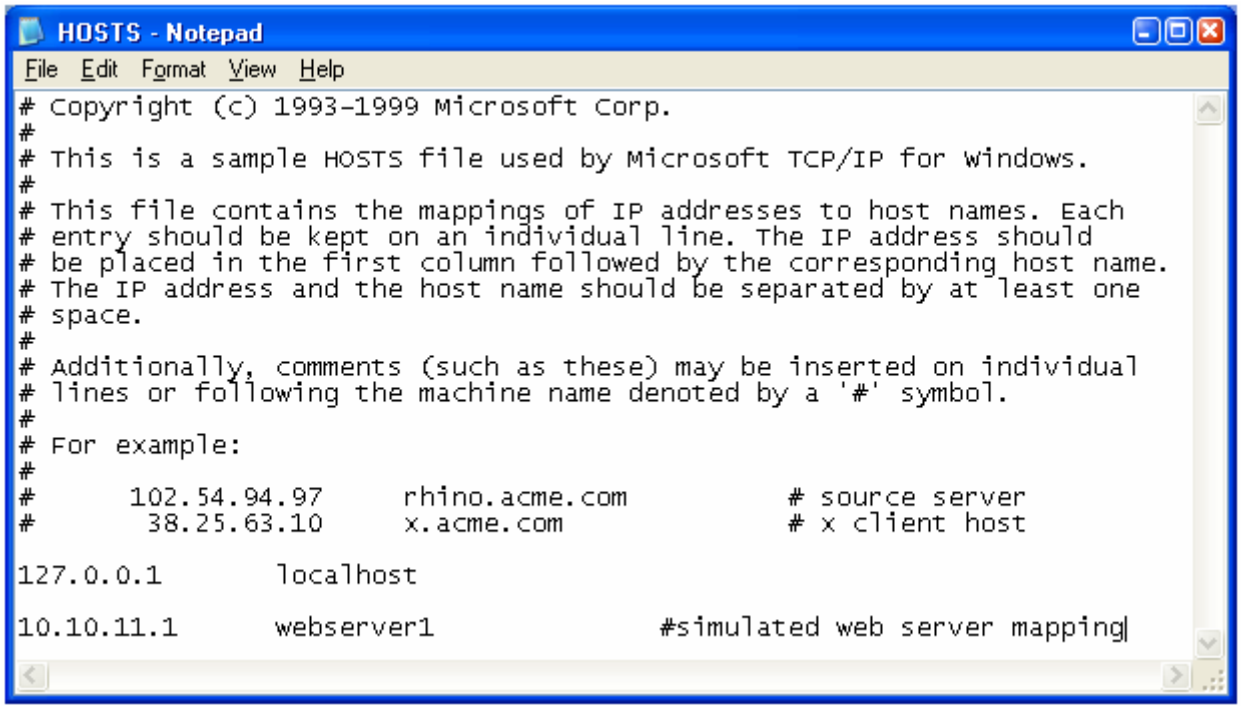


The **HOSTS** file opens in Notepad.



Step 2: Edit the HOSTS file

a. At the bottom of the **HOSTS** file, there is a list of hosts that have already been recorded. Add a new entry for the web server. Enter **10.10.11.1**, press the Tab key, and then enter **webserver1**. Press the Tab key again, and add a comment preceded by a # sign. The # sign is used to signify a comment.



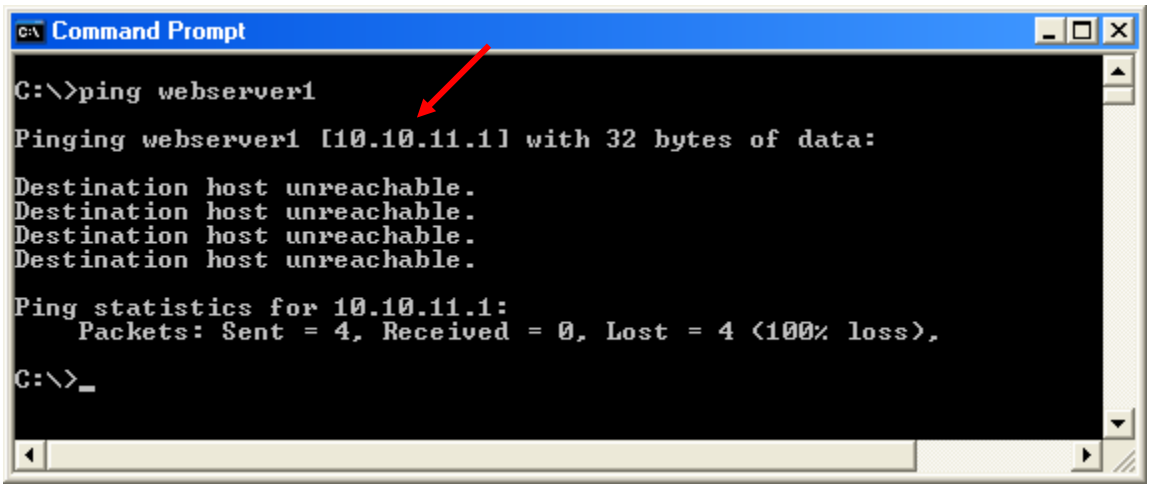
b. Save the updated **HOSTS** file.

Step 3: Test the new name mapping

a. To open the command prompt, click the **Start** button and then click **Run**. In the **Run** dialog box, type **CMD** and then click **OK**. Alternately, you can choose **Start** > **All Programs** > **Accessories** > **Command Prompt** to open a command window.

b. In the command prompt window, type **ping webserver1** and press the **Enter** key.

The name **webserver1** was resolved to **10.10.11.1** just before the subsequent echo requests were sent out. This indicates that the **HOSTS** file was modified correctly and is functioning correctly in the name resolution process on this workstation. Since this is a simulation and there is no real webserver1, the destination host is unreachable. If there were a webserver1 that could be reached from this host, it would most likely have replied to the ping.



Step 4: Reflection

a. Which other files are located in the **\ETC** folder with the **HOSTS** file?

_____

_____

b. Which character is used to comment out description text in the **HOSTS** file?

_____

Lab 7.3.3.a Examining Cached DNS Information on a Windows DNS Server

Objective

- View the cached DNS information on a Windows DNS server after making a DNS request that is looked up.

Background / Preparation

In this lab, you will examine the information that is cached in a local DNS server after it has performed a lookup. You will see the configured Root servers on the DNS server. You will also see the cached top level, second level, and host records within each level after the lookup is complete. It is important to understand that the entire process of finding the information using the various levels of the DNS hierarchy only takes fractions of a second to complete.

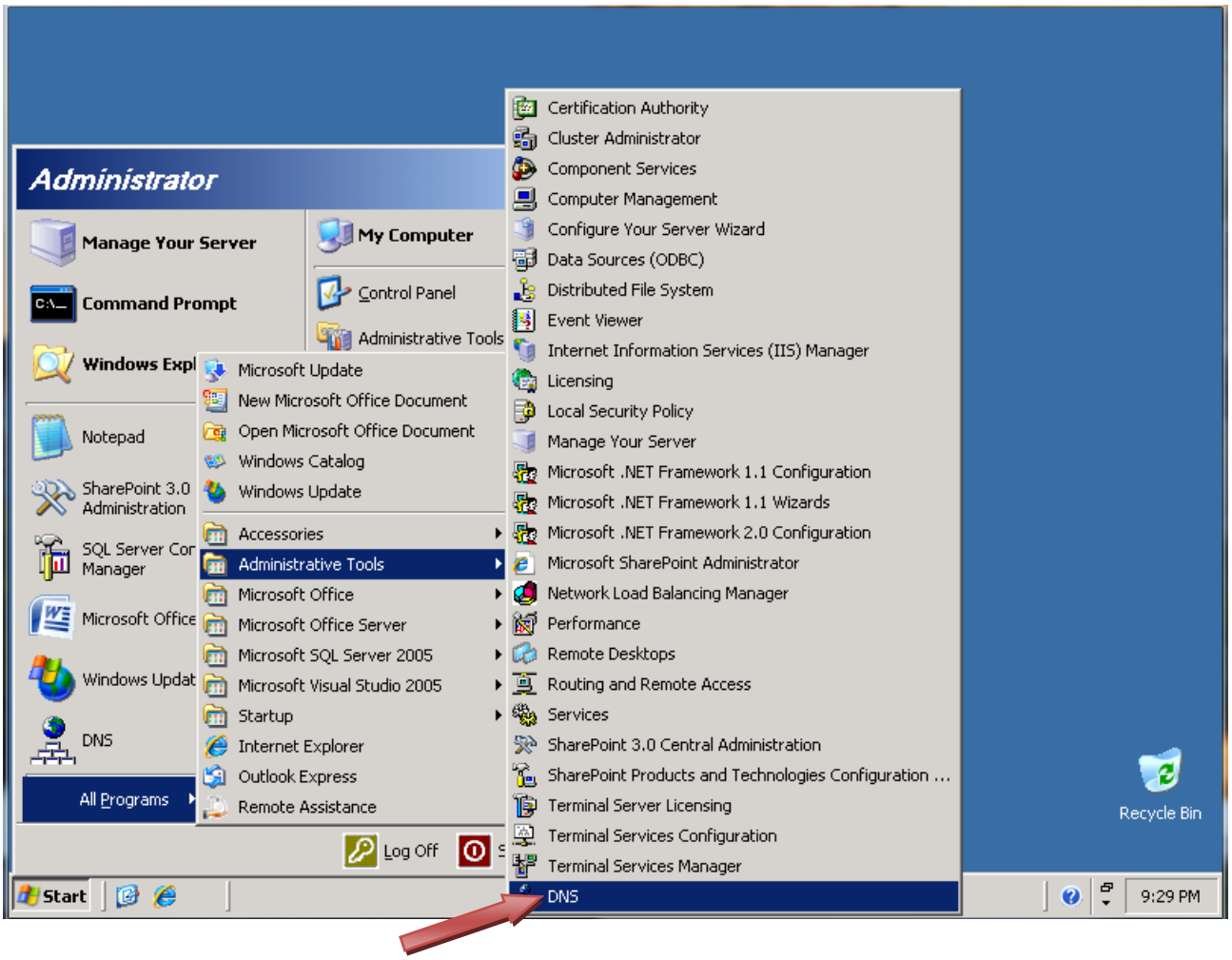
The following resources are required:

- Windows 2003 Server with DNS running
- Administrative access to server
- Internet connectivity

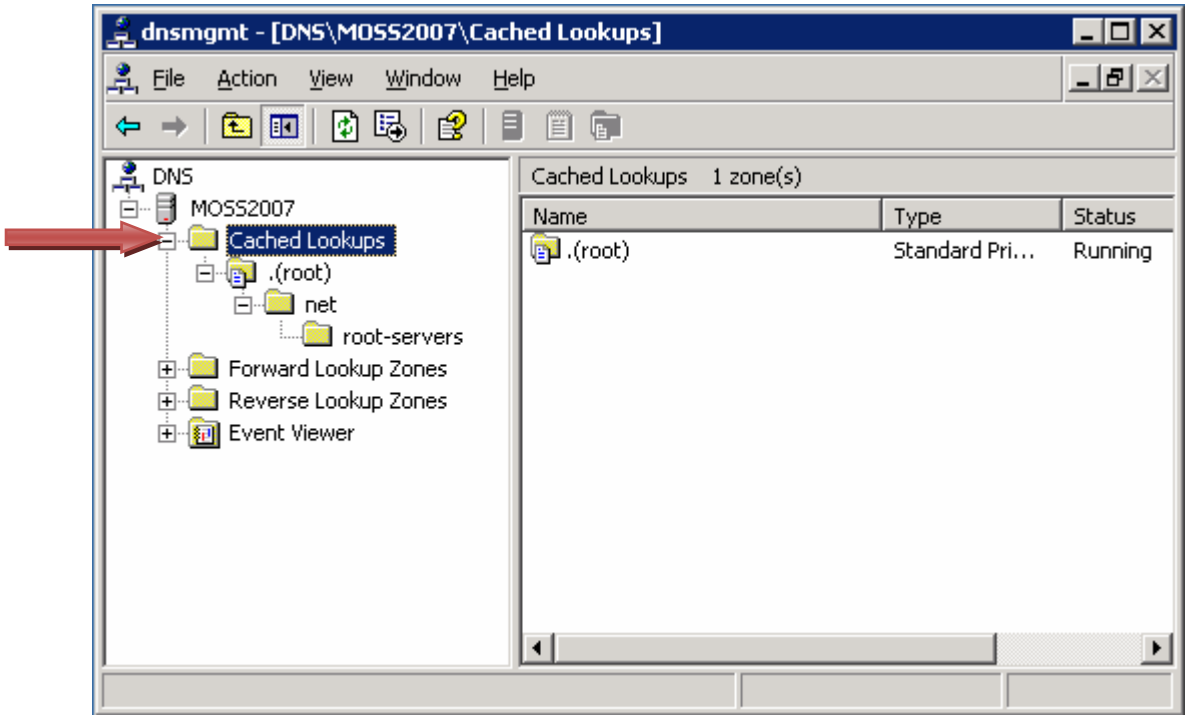
NOTE: If you do not have access to a Windows DNS server, the instructor may demonstrate this lab. If the equipment is not available to perform the lab, or if it cannot be demonstrated, read through the steps of the lab to gain a better understanding of DNS and how DNS servers operate.

Step 1: Use the Windows Server DNS Administrative Tool

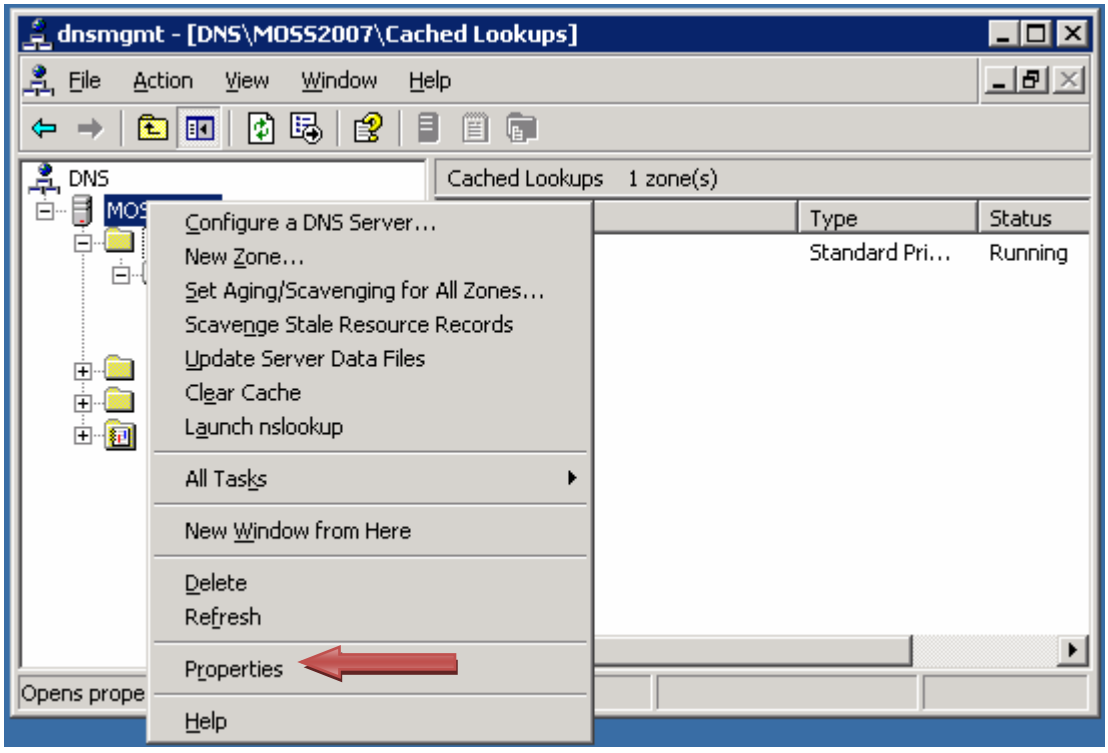
a. Click **Start > All Programs** > **Administrative Tools**, and then click **DNS** to launch the DNS administrative tool.



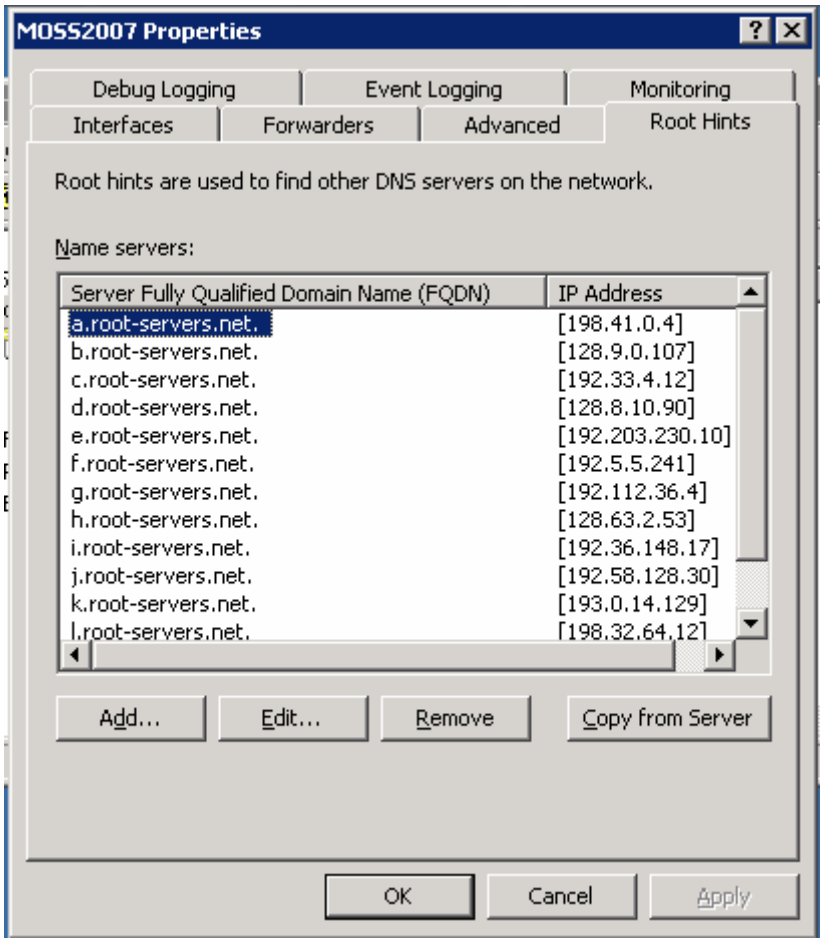
b. Expand the **Cached Lookups** folder and all subfolders to see that there are no cached lookups.



c. Next, to verify that the server has been configured to use the Root servers on the Internet, right-click the DNS server and click **Properties**.

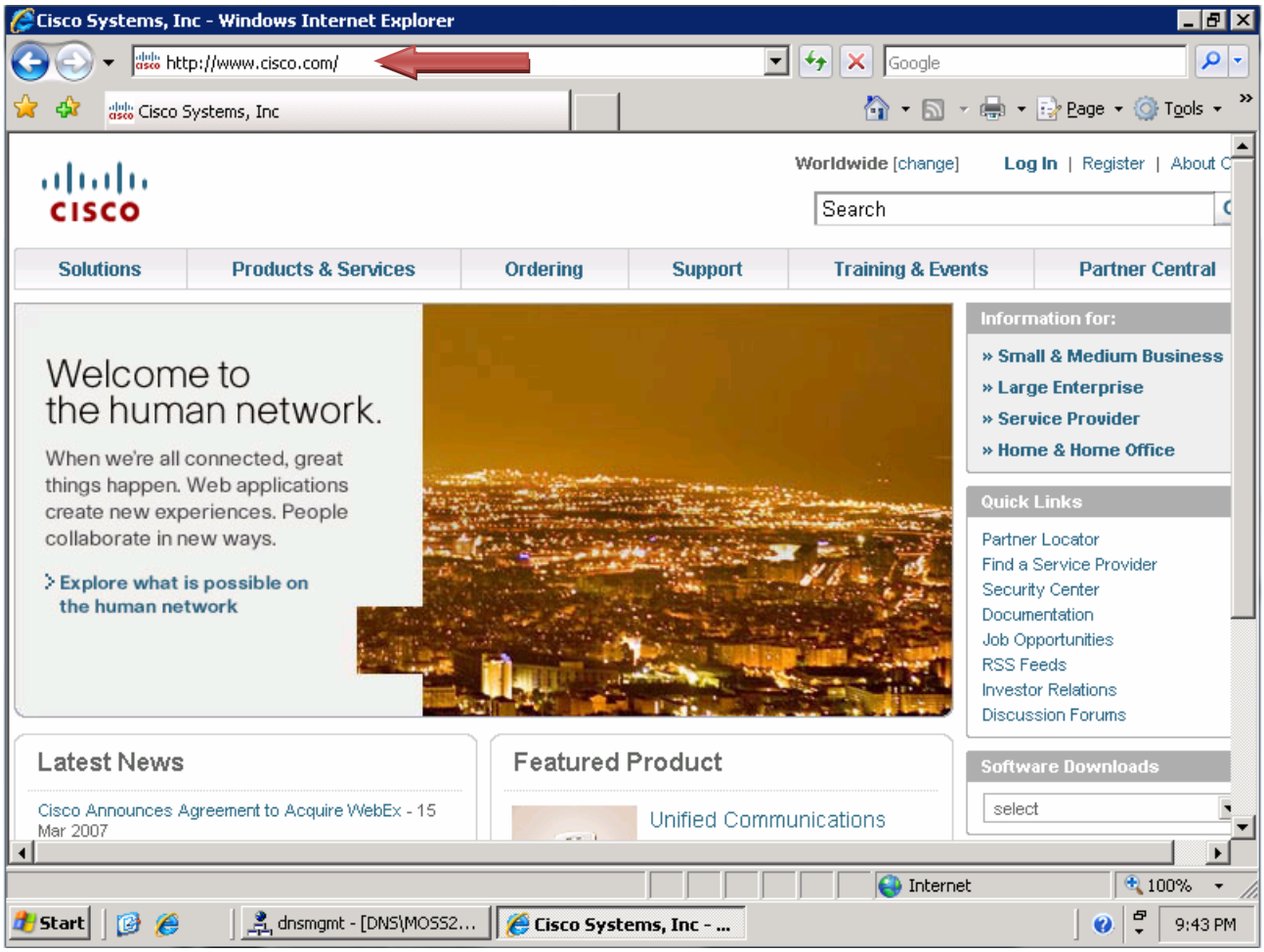


d. From the **Properties** dialog box, select the **Root Hints** tab and verify the presence of the Root servers. Click **OK** to close the **Properties** dialog box.



Step 2: Perform a DNS lookup

On the DNS server, open Internet Explorer and browse to http://www.cisco.com. Once the web page opens, close the web browser.



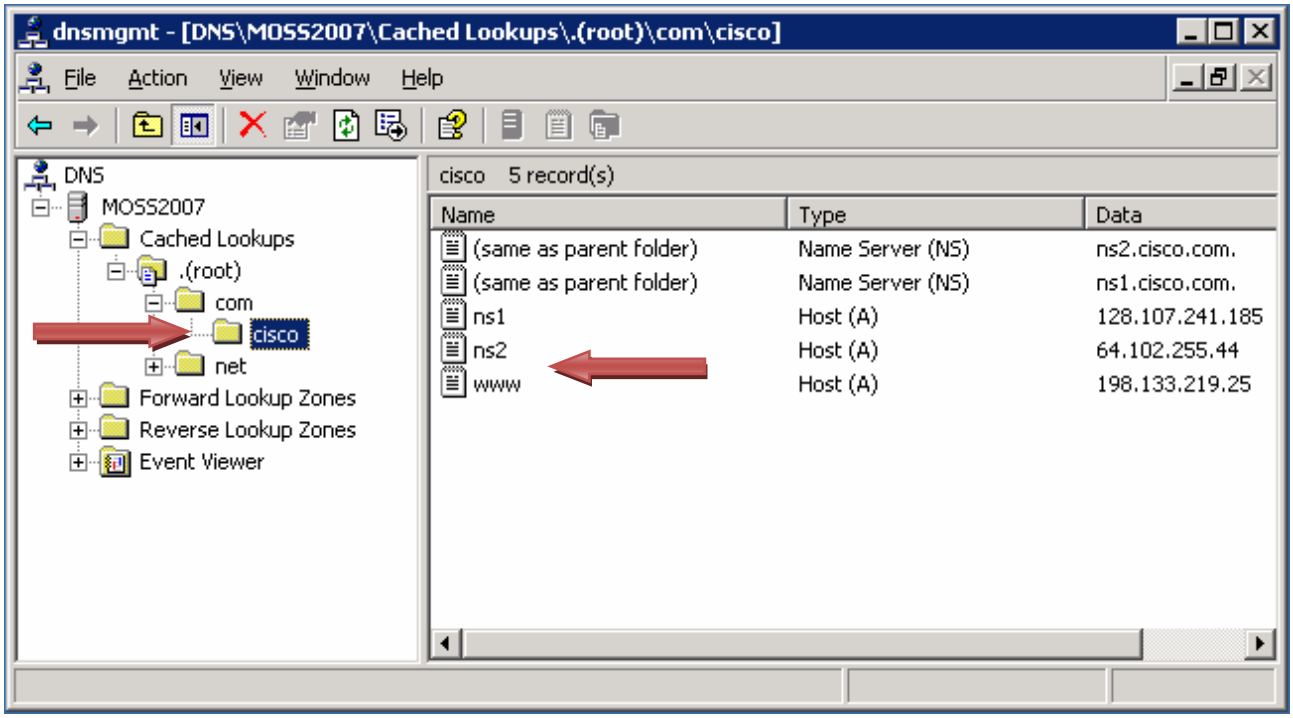
Step 3: Examine the Cached DNS entries

a. Switch back to the DNS Administrative tool.

b. From the **Cached Lookups** root folder, click the **Refresh** button on the toolbar.

c. Expand all the subfolders below the **Cached Lookups** folder to reveal the cached DNS entries.

Notice that you now have a folder structure that expands down to Cisco. Within the Cisco folder notice the two Name Server type records, which identify the two name servers that manage the Cisco.com DNS zone. Also notice the Host record for www that maps to 198.133.219.25.



Step 4: Reflection

a. The DNS server had to do a query to the cisco.com domain name servers to resolve the server name (www.cisco.com) to an IP address. What do you think would happen the next time this website is visited again within a few minutes?

_____

_____

b. What would happen if there are no requests for this website for a longer period of time?

_____

_____

Lab 7.3.3.b Creating Primary and Secondary Forward Lookup Zones

Objective

- Create primary and secondary forward lookup zones on Windows DNS servers.

Background / Preparation

You have been asked to implement a DNS zone for a customer that has registered a second-level domain on the Internet. The customer would like to host the DNS zone on two spare servers. You go on site to configure the zone on each of the two DNS servers. One server will function as the primary DNS server and the other will function as the secondary DNS server.

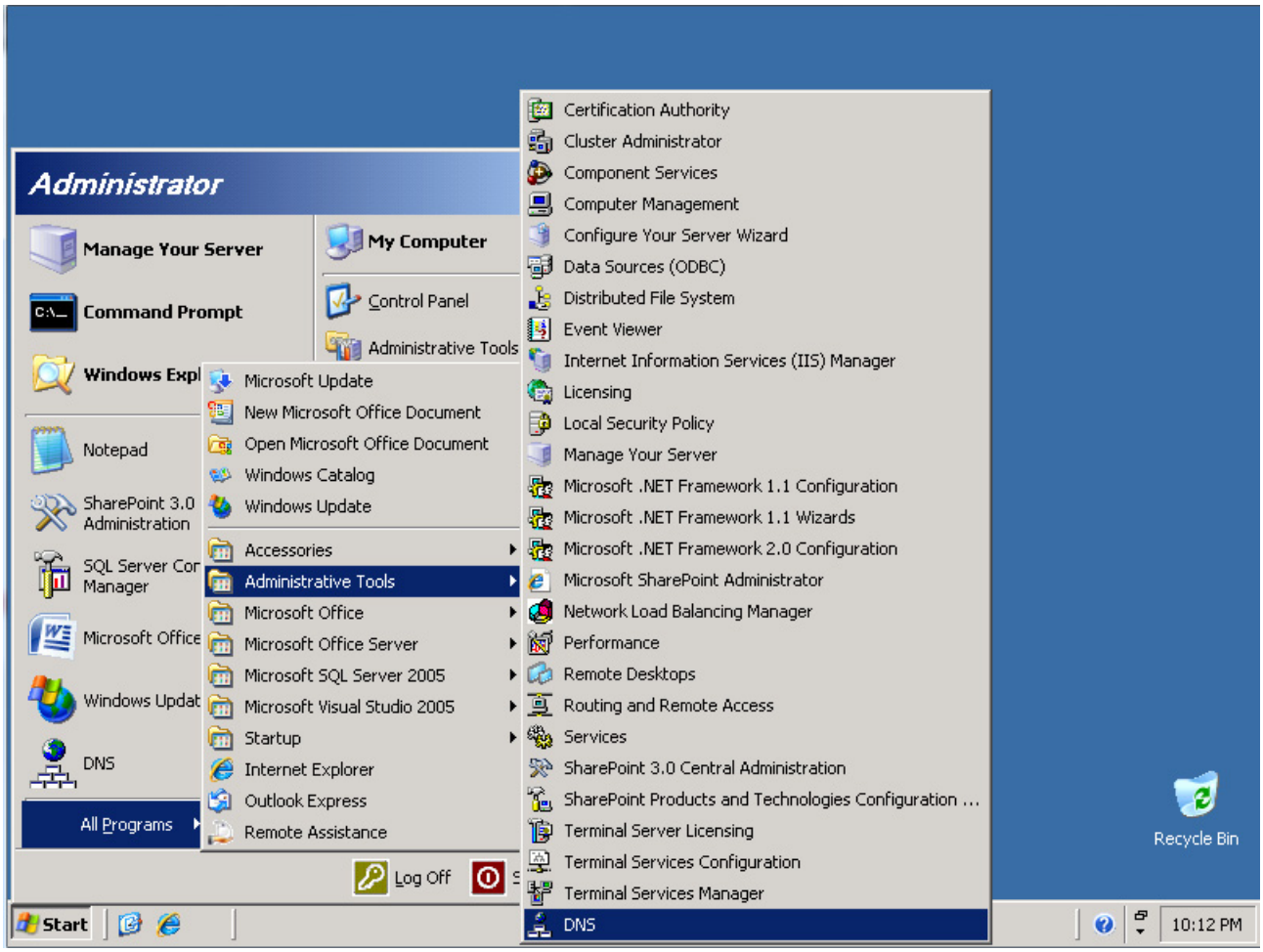
The following resources are required:

- Two Windows 2003 Servers with DNS running
- Administrative access to servers
- Internet connectivity

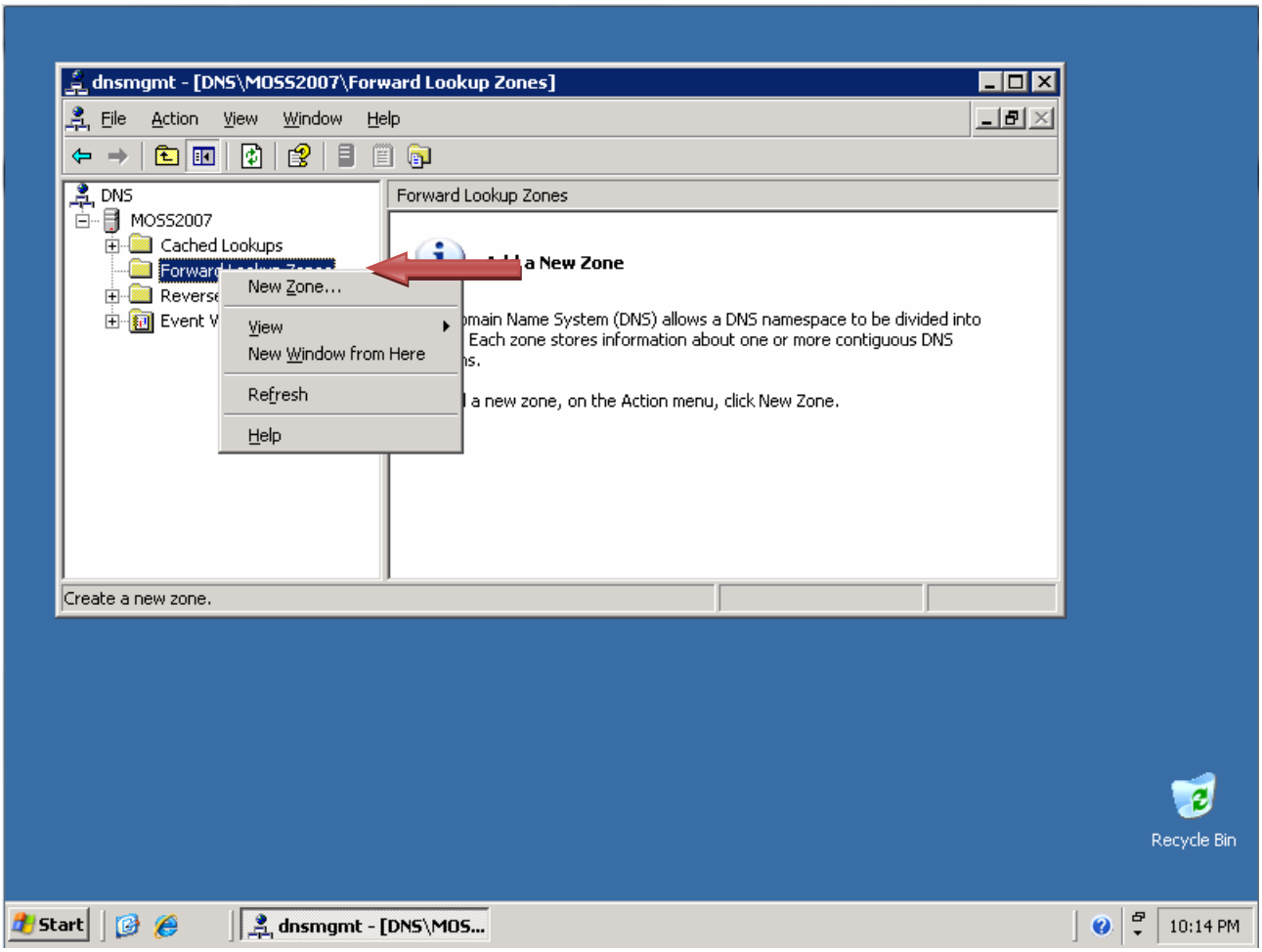
NOTE: If you do not have access to the Windows DNS servers, the instructor may demonstrate this lab. If the equipment is not available to perform the lab, or if it cannot be demonstrated, read through the steps of the lab to gain a better understanding of DNS and how DNS servers operate.

Step 1: Create a primary forward lookup zone on Windows

a. Click **Start > All Programs > Administrative Tools**, and then click **DNS** to launch the DNS administrative tool.

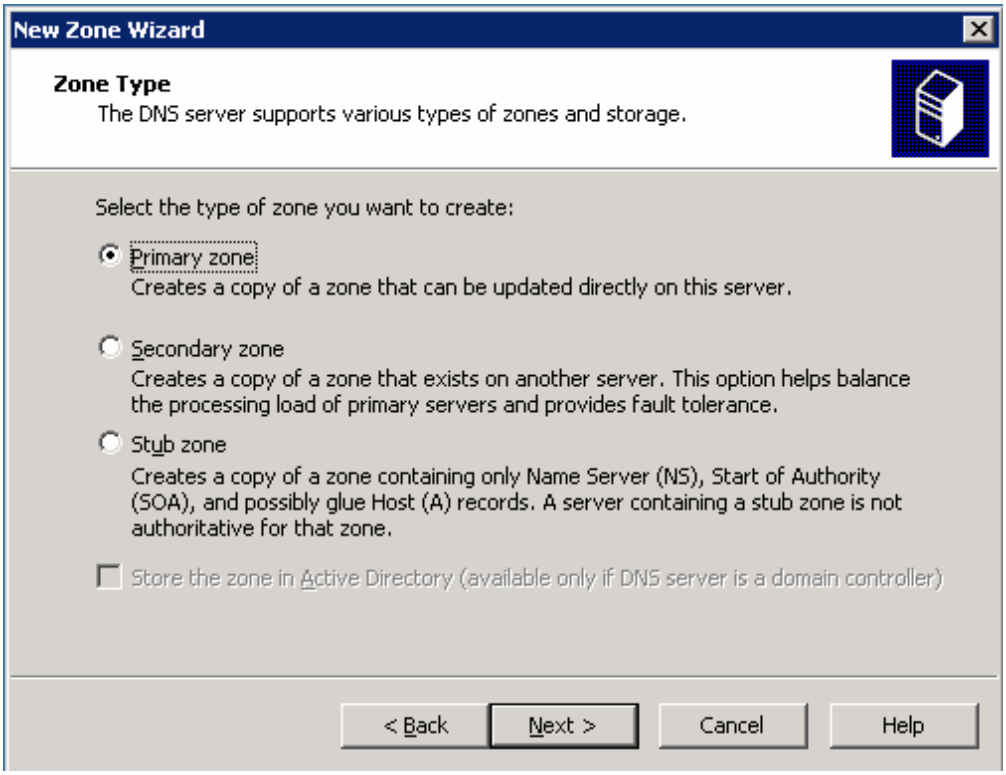


b. Right-click **Forward Lookup Zones** and then click **New Zone**.

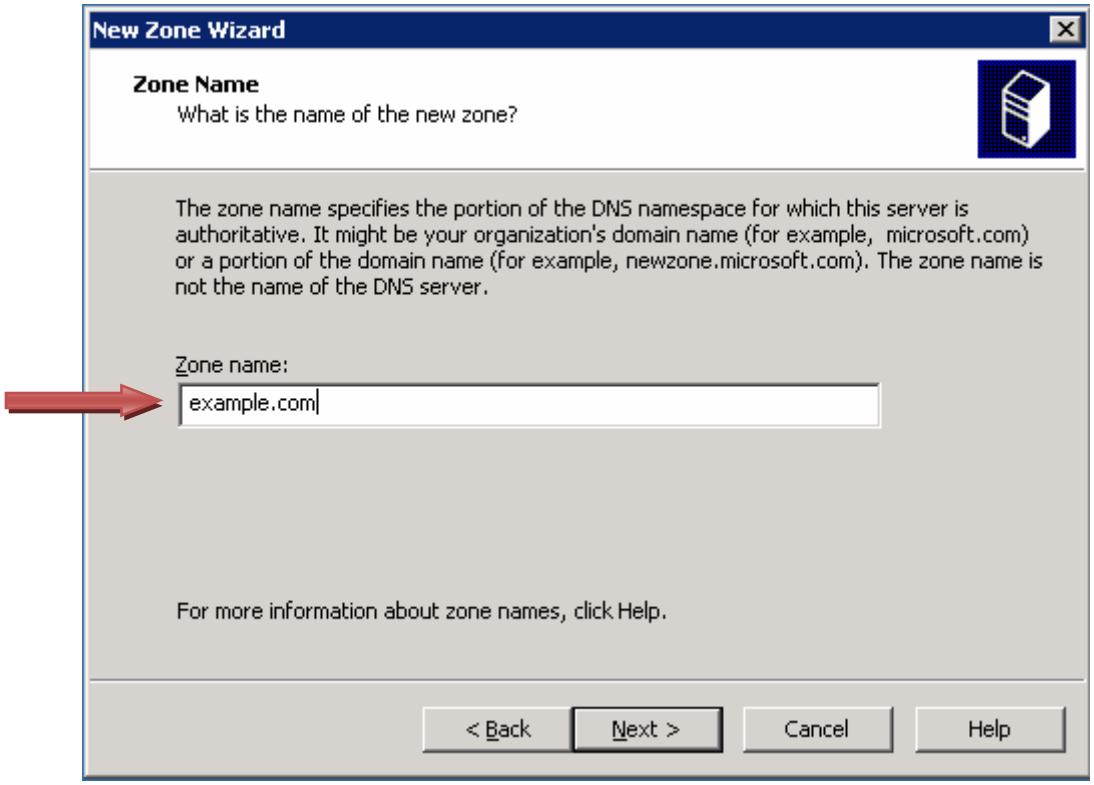


c. When the **New Zone Wizard** displays, click **Next**.

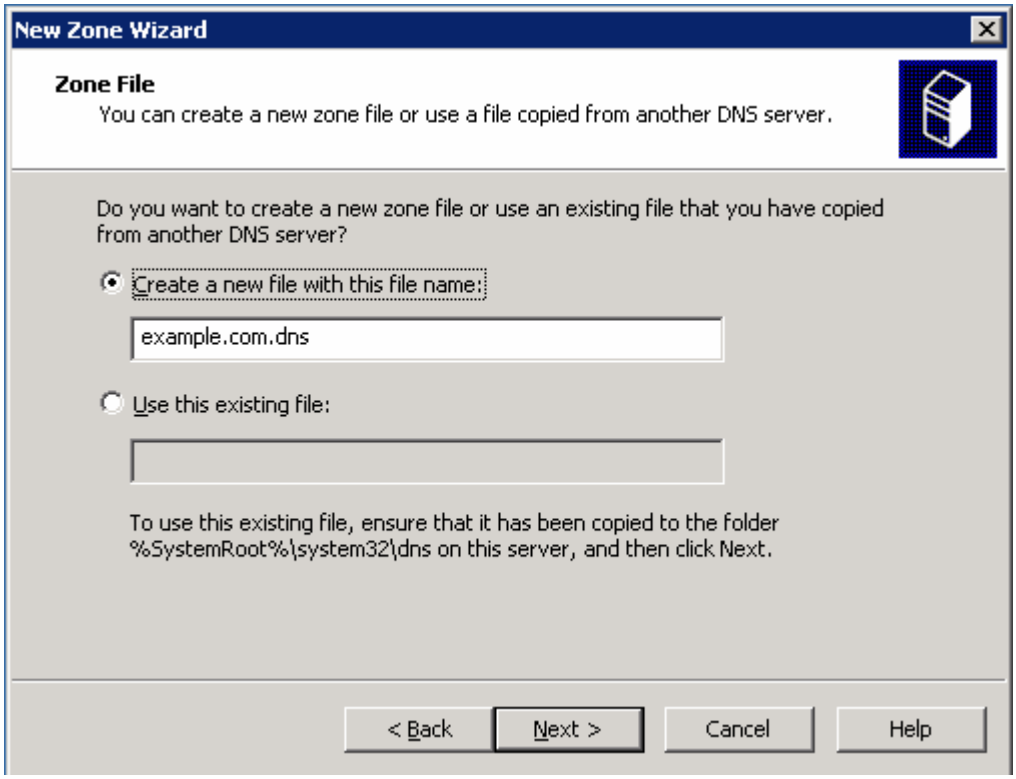
d. By default, the **Primary zone** radio button is selected. Click **Next** to create a **Primary zone**.



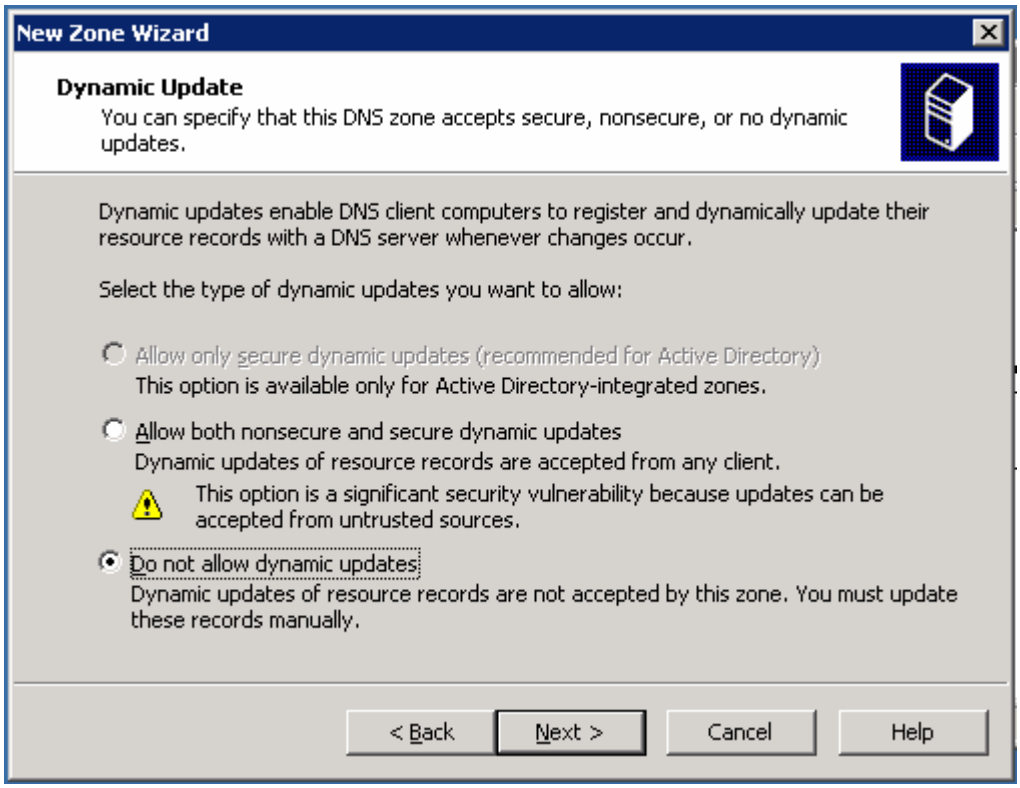
e. Enter the domain name, **example.com**, into the Zone name field and click **Next**.



f. Click **Next** to create a new file with this name.



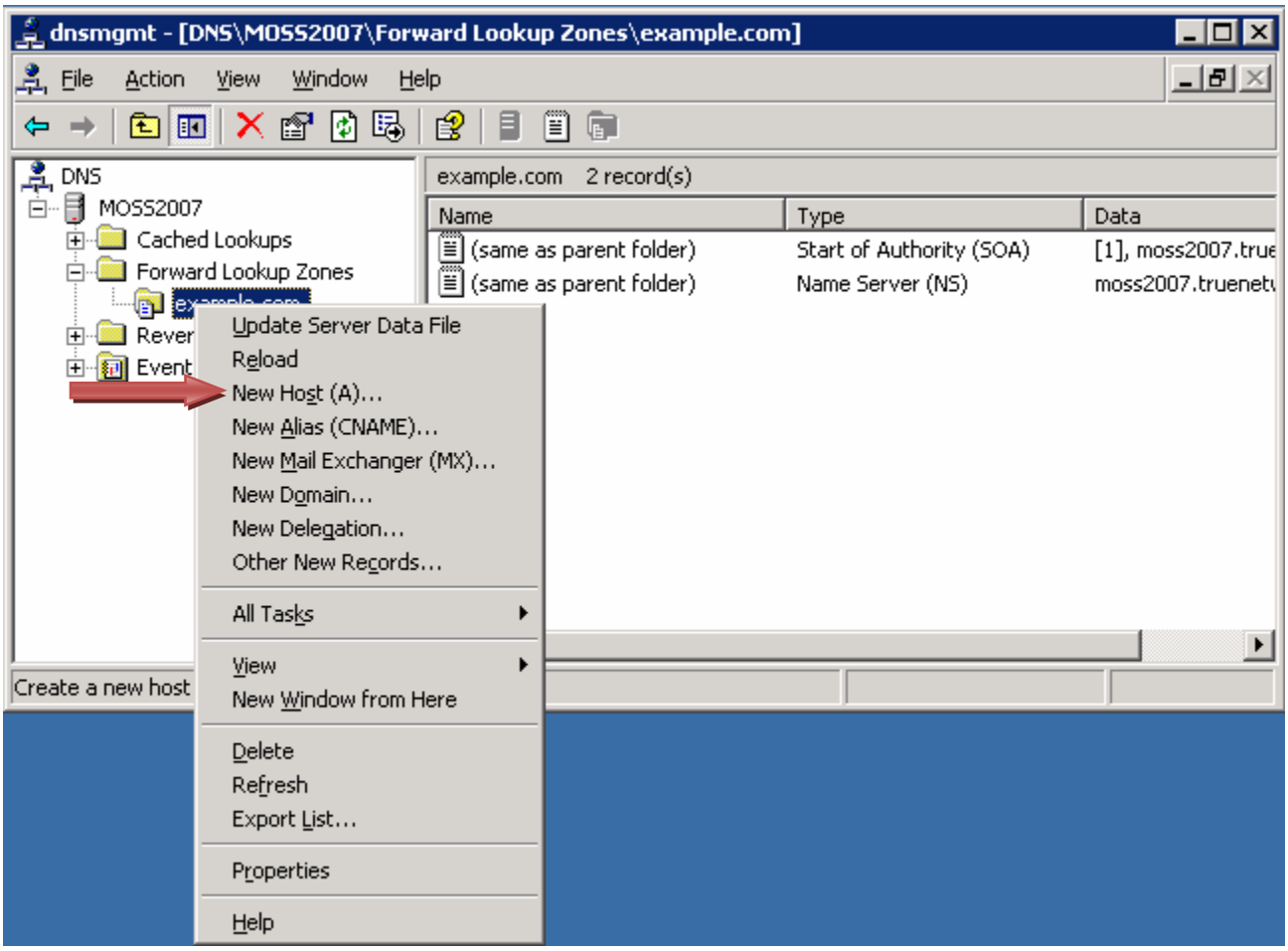
g. Notice the option to enable dynamic updates. It is disabled by default for security. You will leave it disabled as well. Click **Next**.



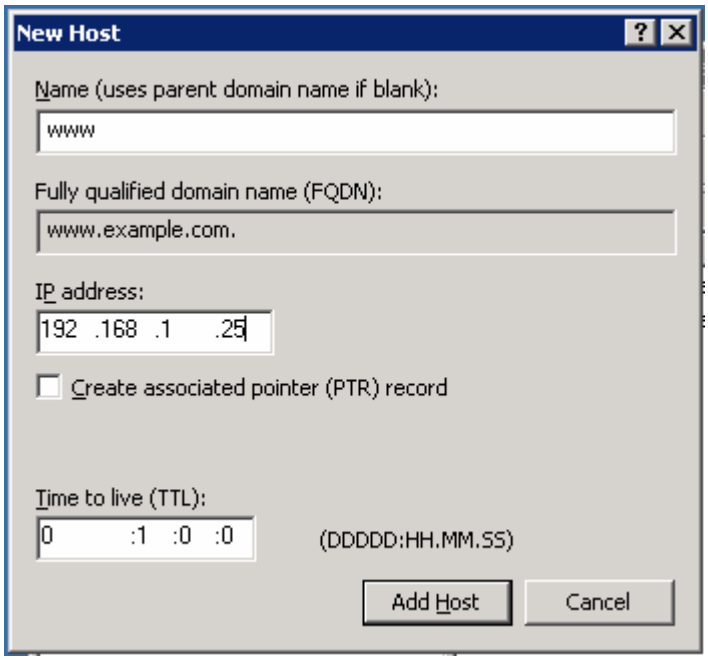
h. Click **Finish** to create the primary forward lookup zone.

Step 2: Add a Host record to the Primary forward lookup zone

a. Right-click the **example.com** forward lookup zone and choose **New Host (A)**.

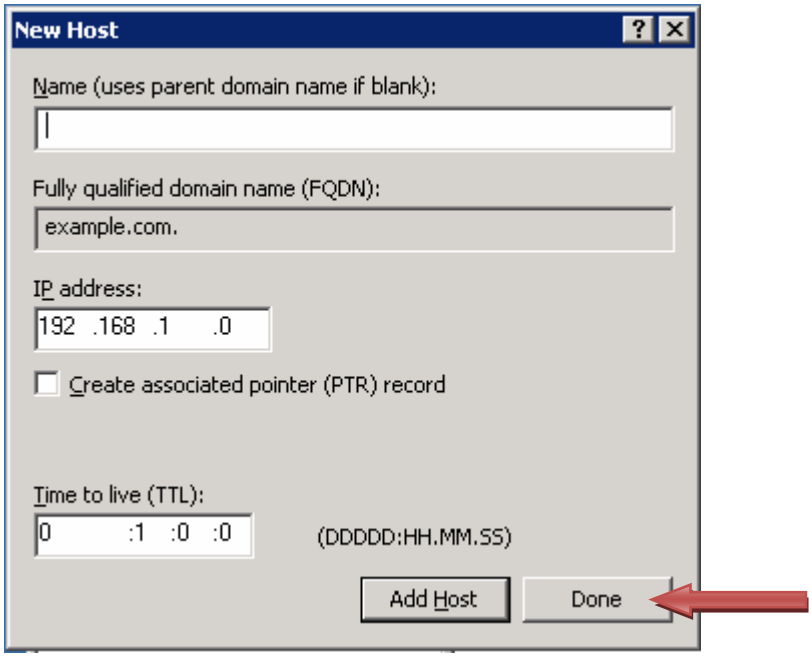


b. In the Name field type **www**. In the IP address field, type **192.168.1.25**. Leave the other settings at their default value. This creates a host named www.example.com, which will resolve to 192.168.1.25. Click the **Add Host** button at the bottom.

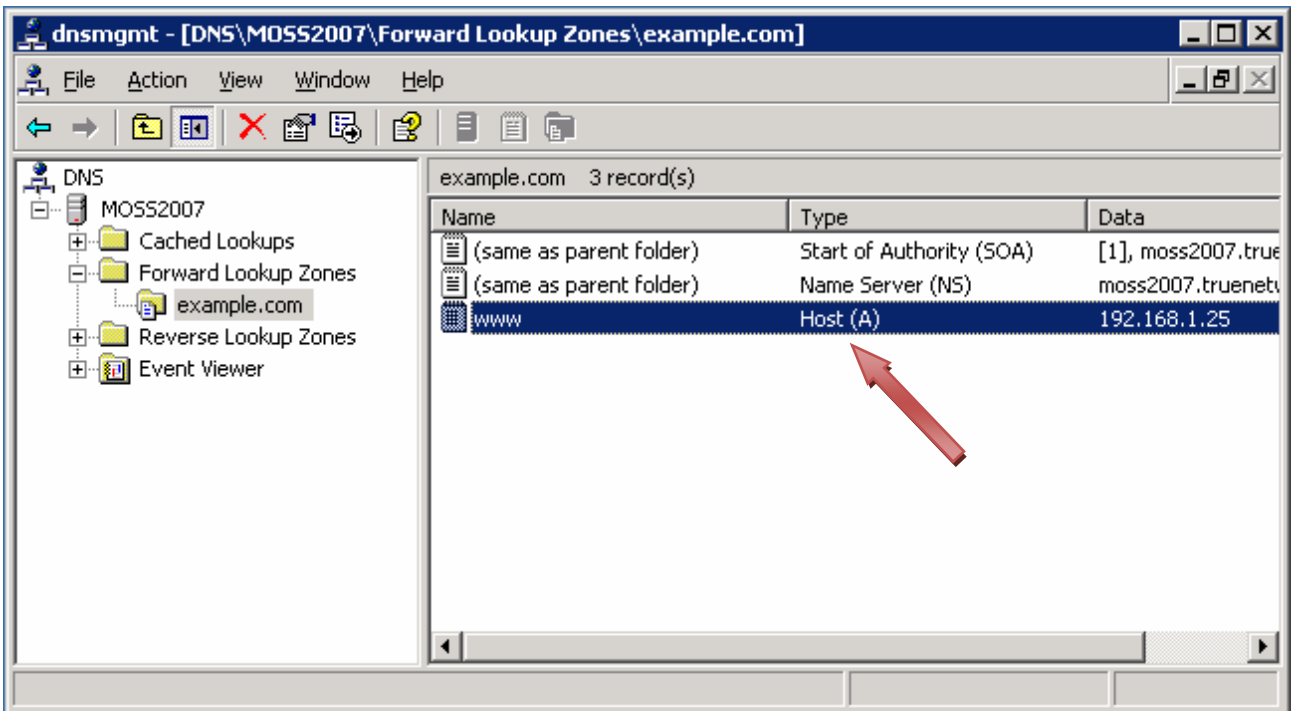


c. Click **OK**.

d. Click **Done**.



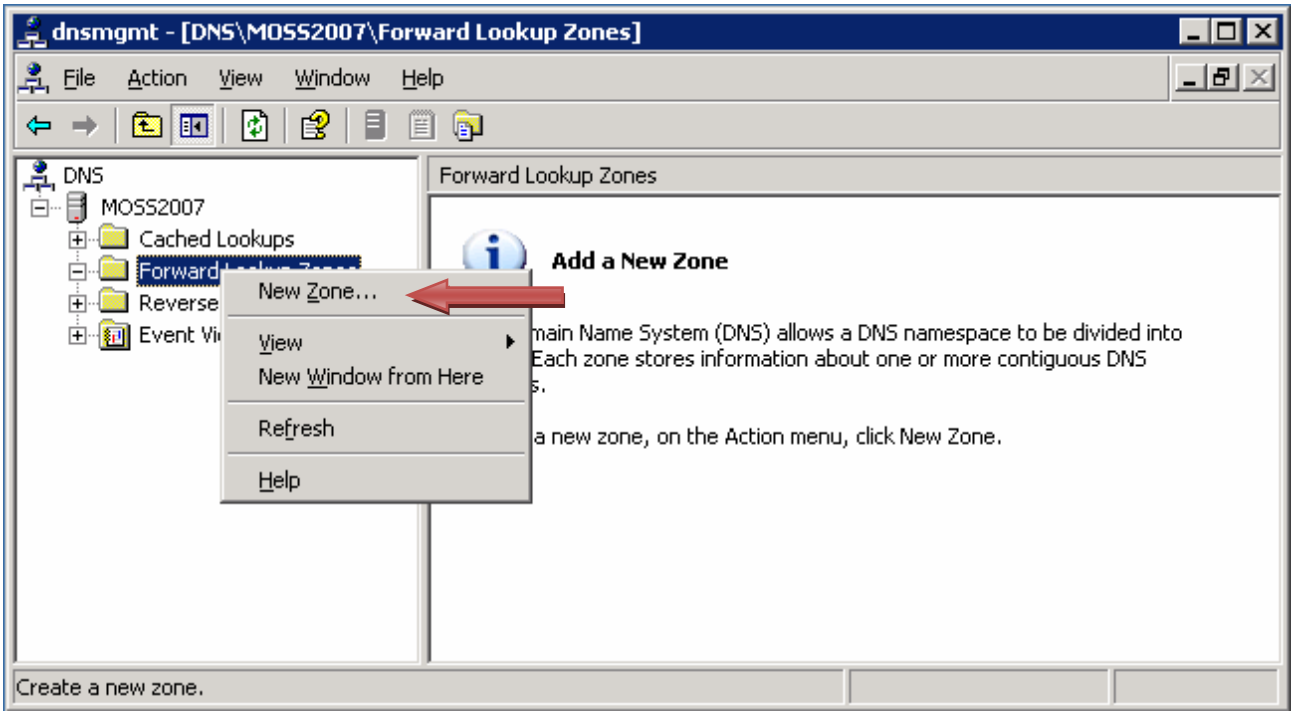
The host record is now in your DNS zone.



Step 3: Create a secondary forward lookup zone

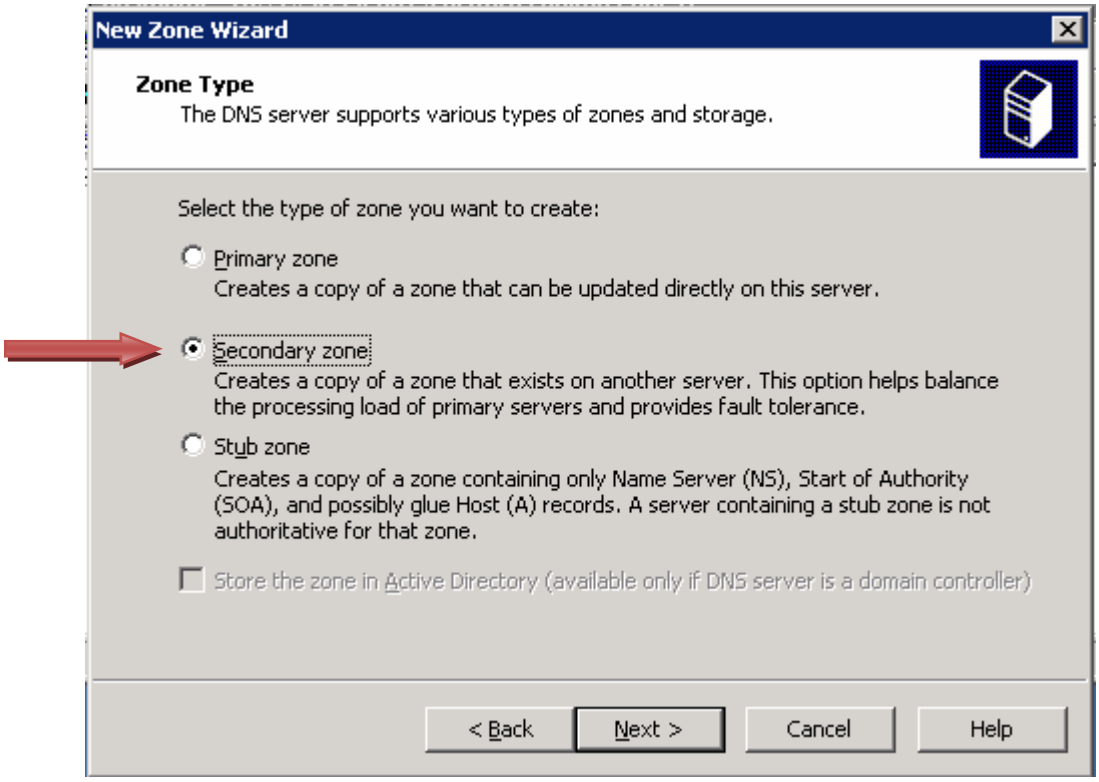
a. On the second Windows DNS server, launch the DNS administrative tool. Follow the instructions from Step 1.

b. Right-click **Forward Lookup Zones** and choose **New Zone**.

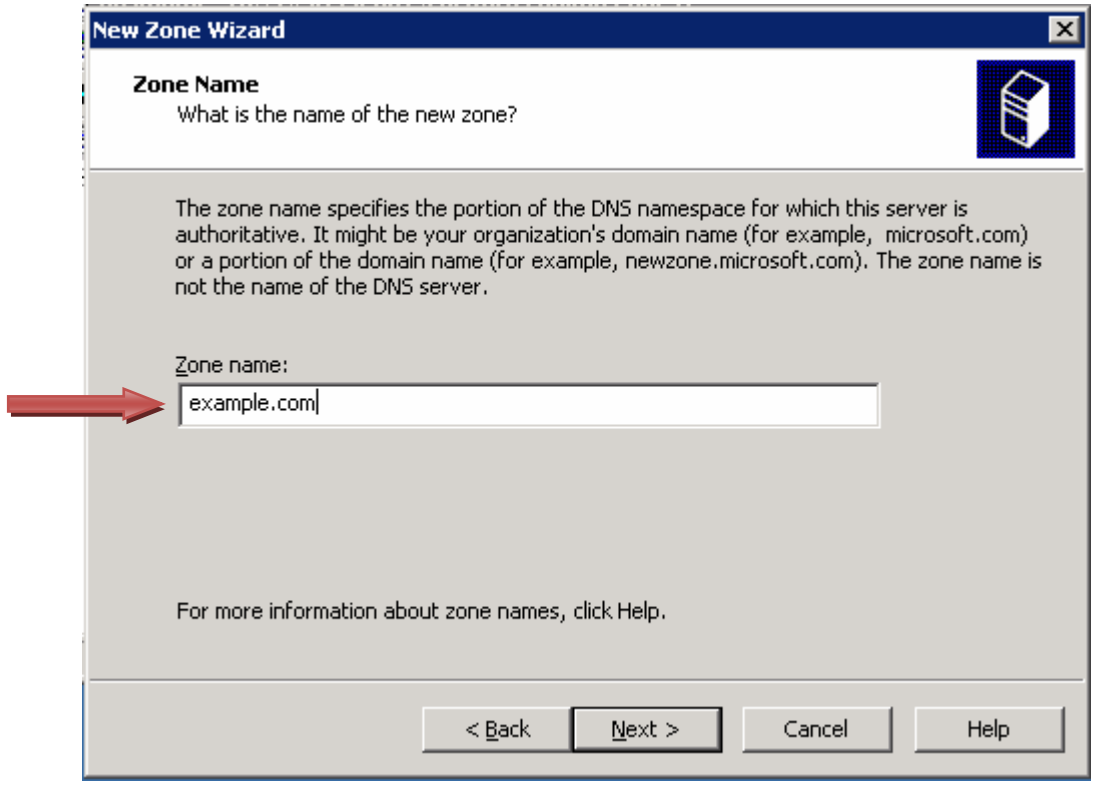


c. When the **New Zone Wizard** displays, click **Next**.

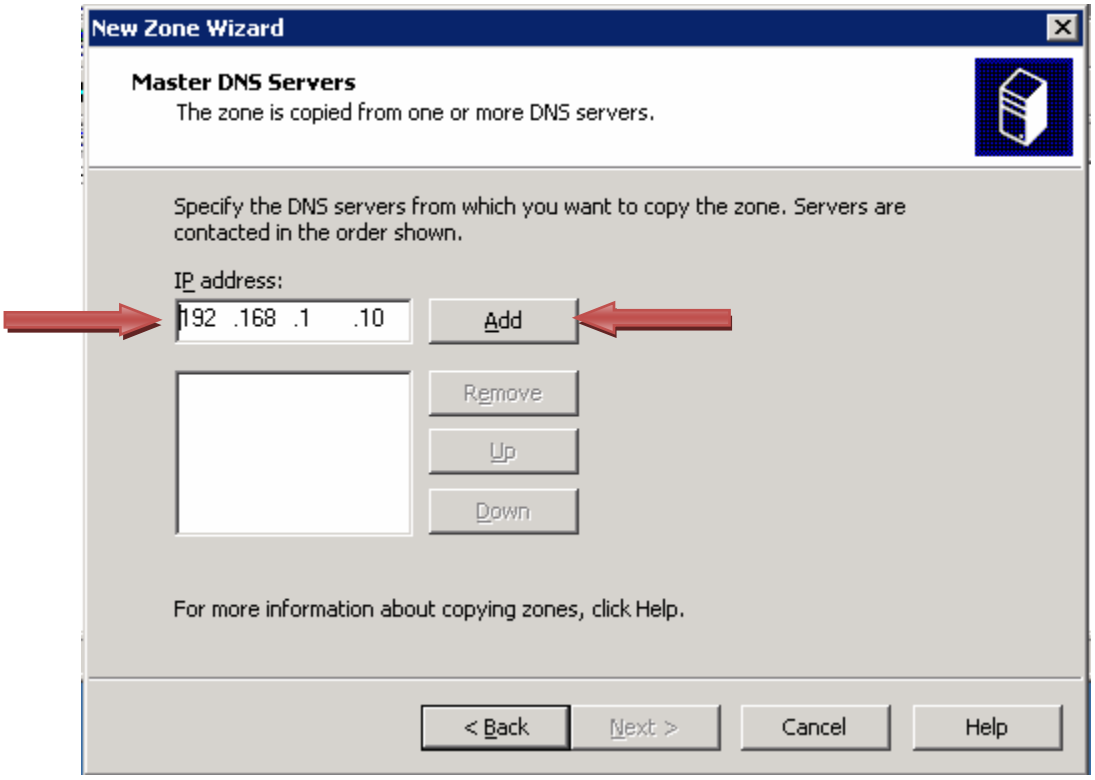
d. Click the **Secondary zone** radio button, and then click **Next**.



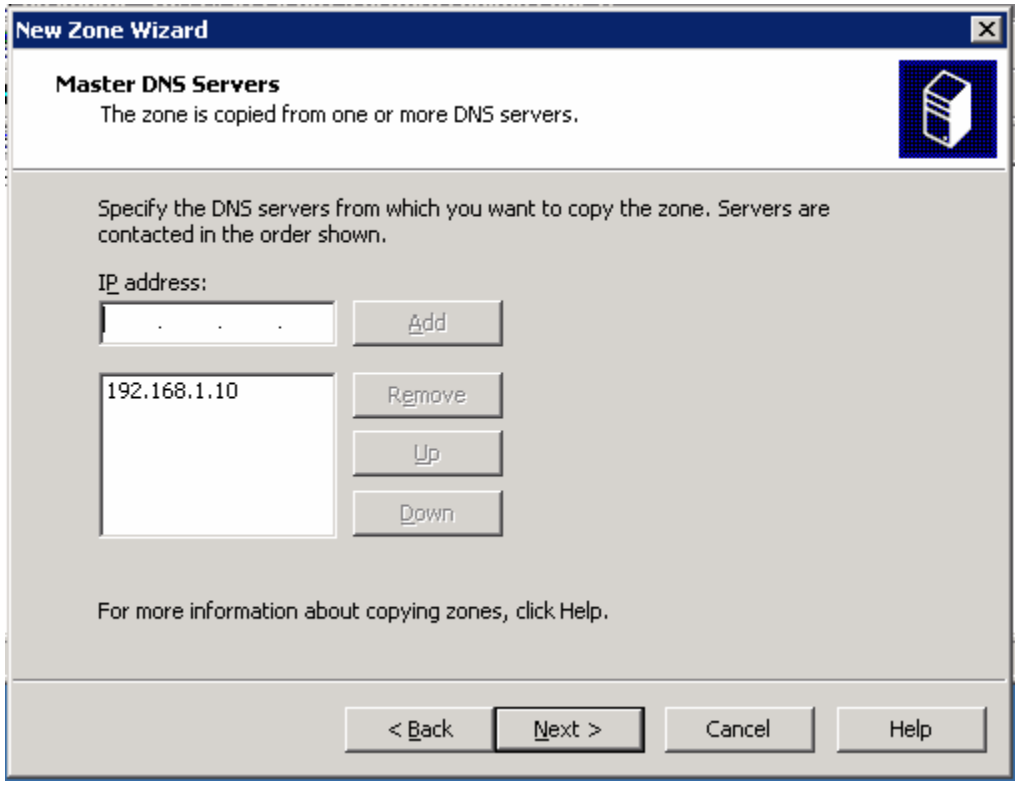
e. Type **example.com** in the Zone name field, and then click **Next**.



f. In the IP address field, type **192.168.1.10**, which is the IP address of the primary server. Then click **Add**.

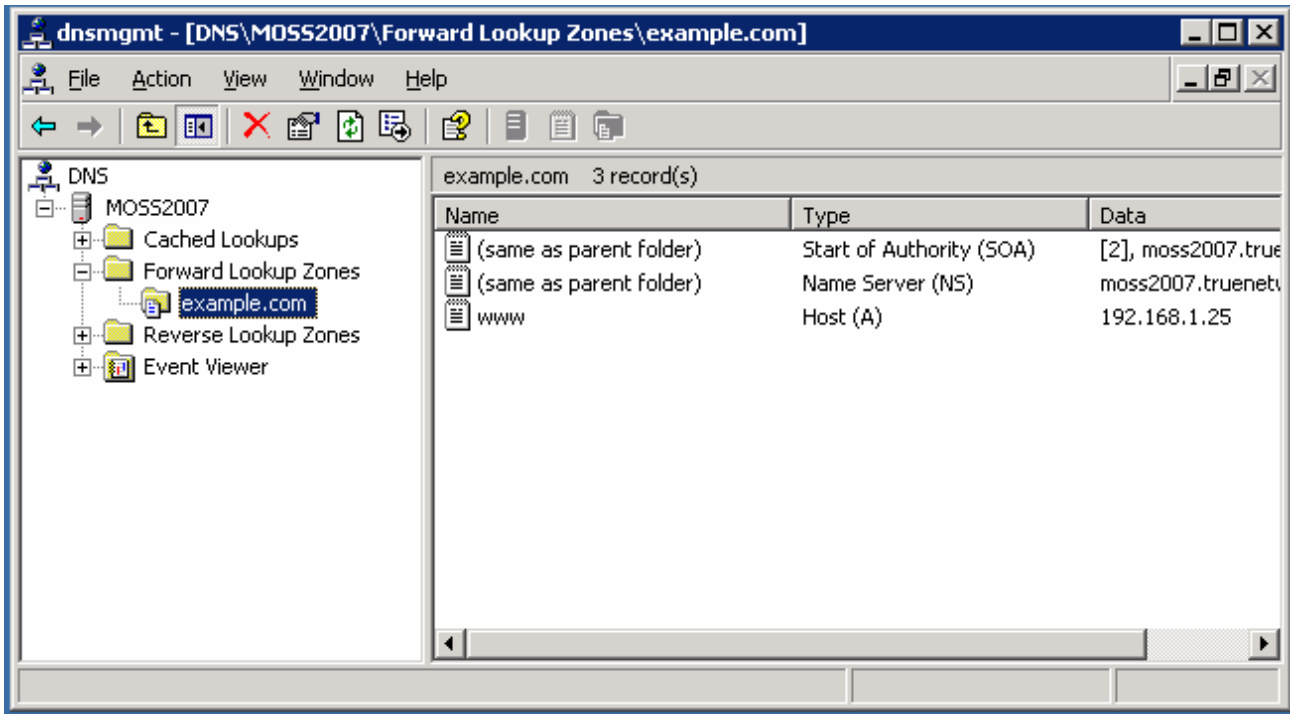


g. Click **Next**.

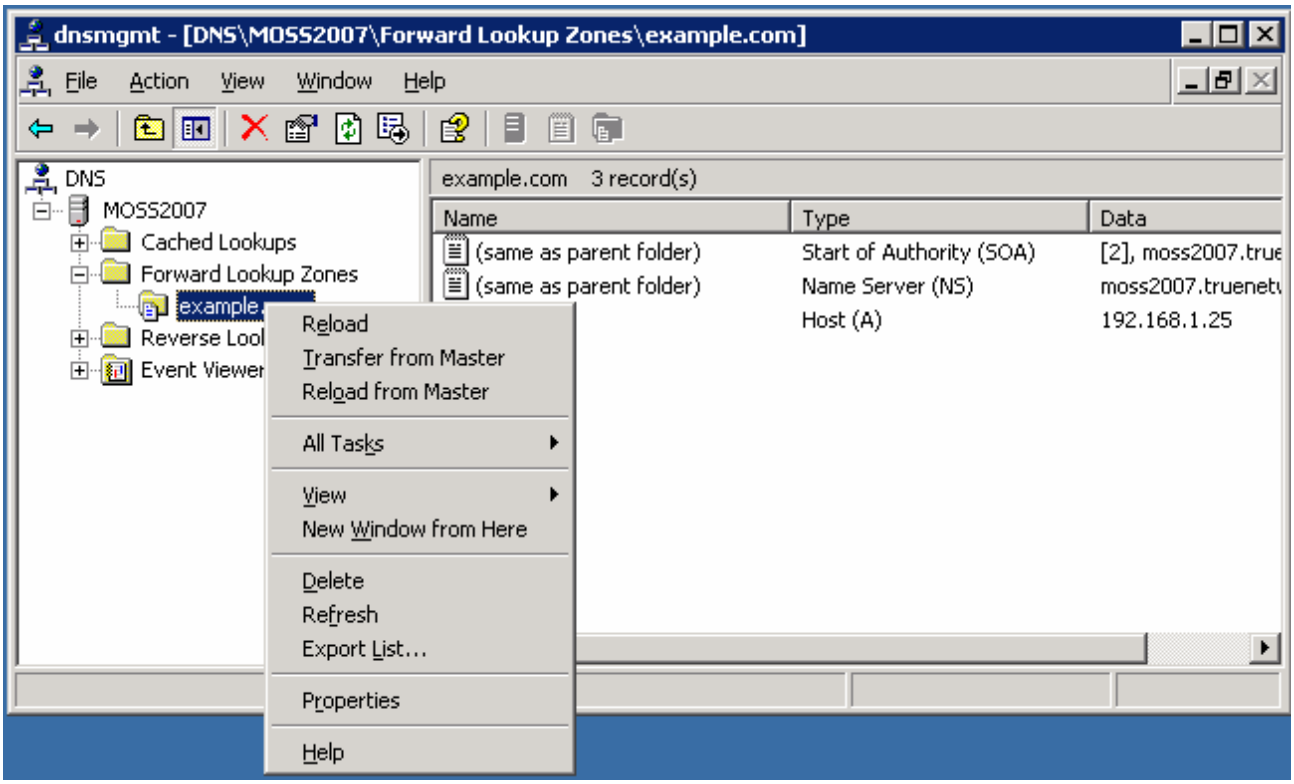


h. Click **Finish**.

i. When you view the secondary zone, notice that the www host record created on the primary server has transferred down to the secondary server.



j. To verify that it is a secondary zone and is read-only, right-click the zone and notice that there is not an option to create any records.



Step 4: Reflection

What is the major benefit of having a primary and secondary DNS server in a zone?

_____

Lab 8.1.3 Securing Local Data and Transmitted Data

Objectives

- Use Windows New Technology Files System (NTFS) permissions to secure local data on a Windows XP Professional edition computer.
- Use Internet Explorer 7 to access secure web sites.

Background / Preparation

This is a 2-part lab. The parts can be performed together or independently.

Part 1 – Error! Not a valid link.

In part 1 you will secure data on a computer using the NTFS file system.

Scenario: A couple of users at a small business share a workstation. Confidential data is stored locally on the hard drive of the computer. You have been asked to help protect the data and secure it so that only one local user can access the data. Using NTFS permissions, you will secure that local data.

There are two local users, Bob and Joe. Bob will require Modify access to a folder called “Bob’s Files” located below a folder called “Local Data on the C drive.” Joe will not have access to “Bob’s Files.”

Part 2 – Identifying a secure communication channel when transmitting data over the Internet

In part 2 you will use Internet Explorer to identify secure and unsecure web sites.

Scenario: You are in charge of educating end users in a small business on secure access to web sites. You will need to educate the end users on how to recognize a legitimate secured website versus an illegitimate secured website.

The following resources are required:

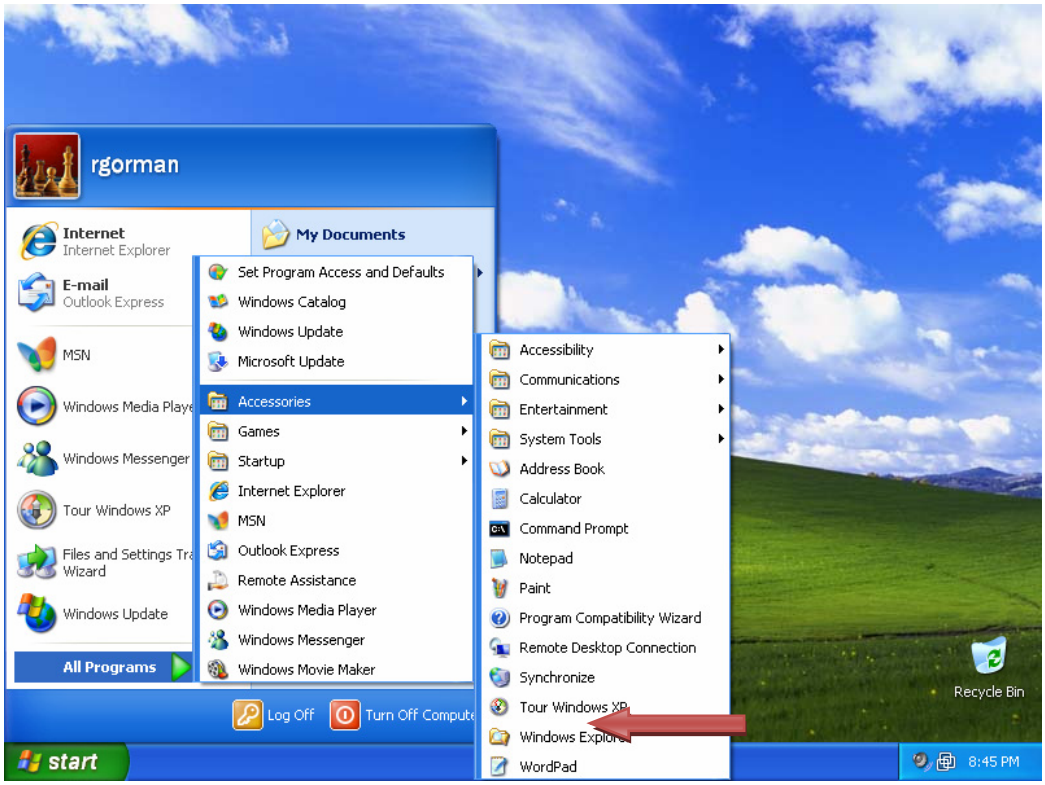
- Windows XP Professional computer with administrative access
- NTFS File System on the computer and Simple File Sharing turned off (under the Folder Options of Windows Explorer.)
- User accounts preconfigured for users Bob and Joe
- Internet connectivity

Part 1 – Securing local data

Step 1: Secure Bob's Files folder

a. Log in to the Windows XP computer as administrator.

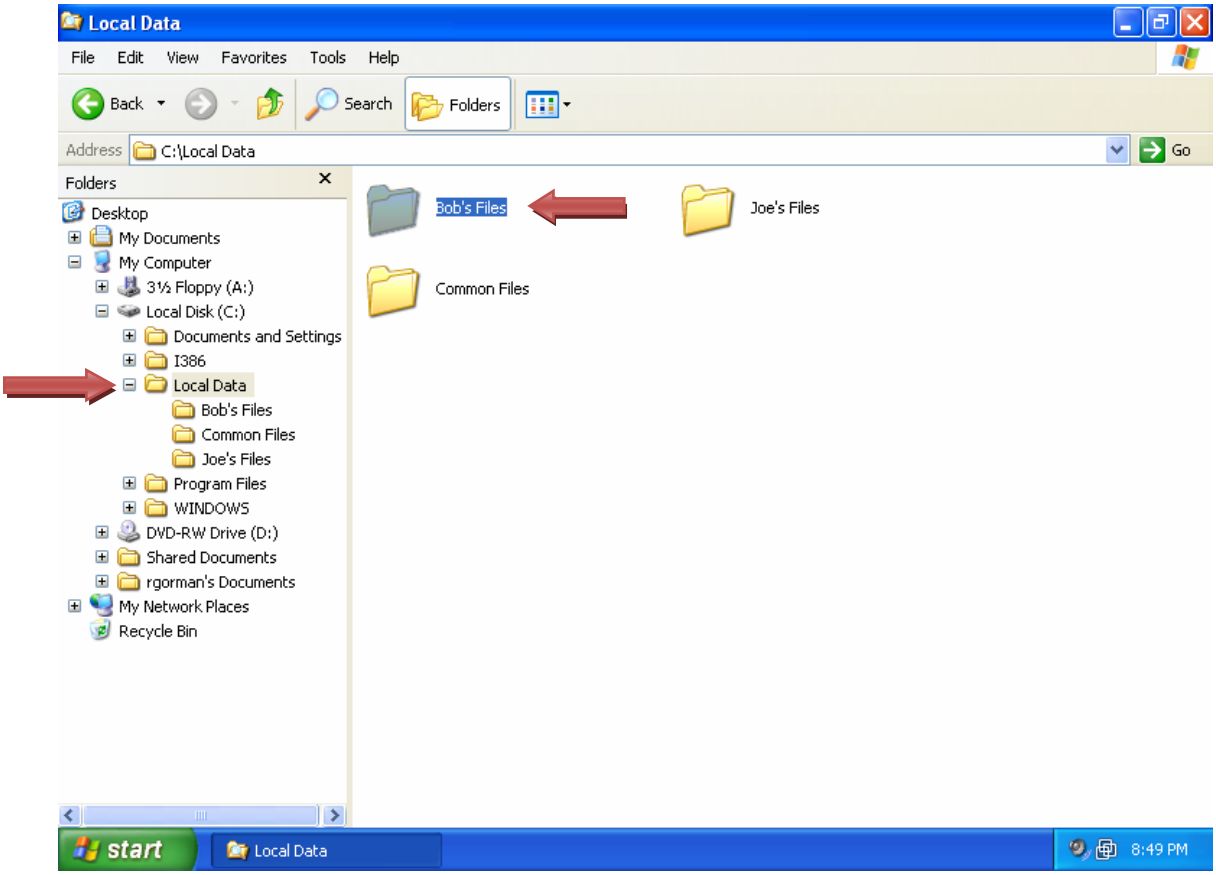
b. From the **Accessories** menu, launch Windows Explorer.



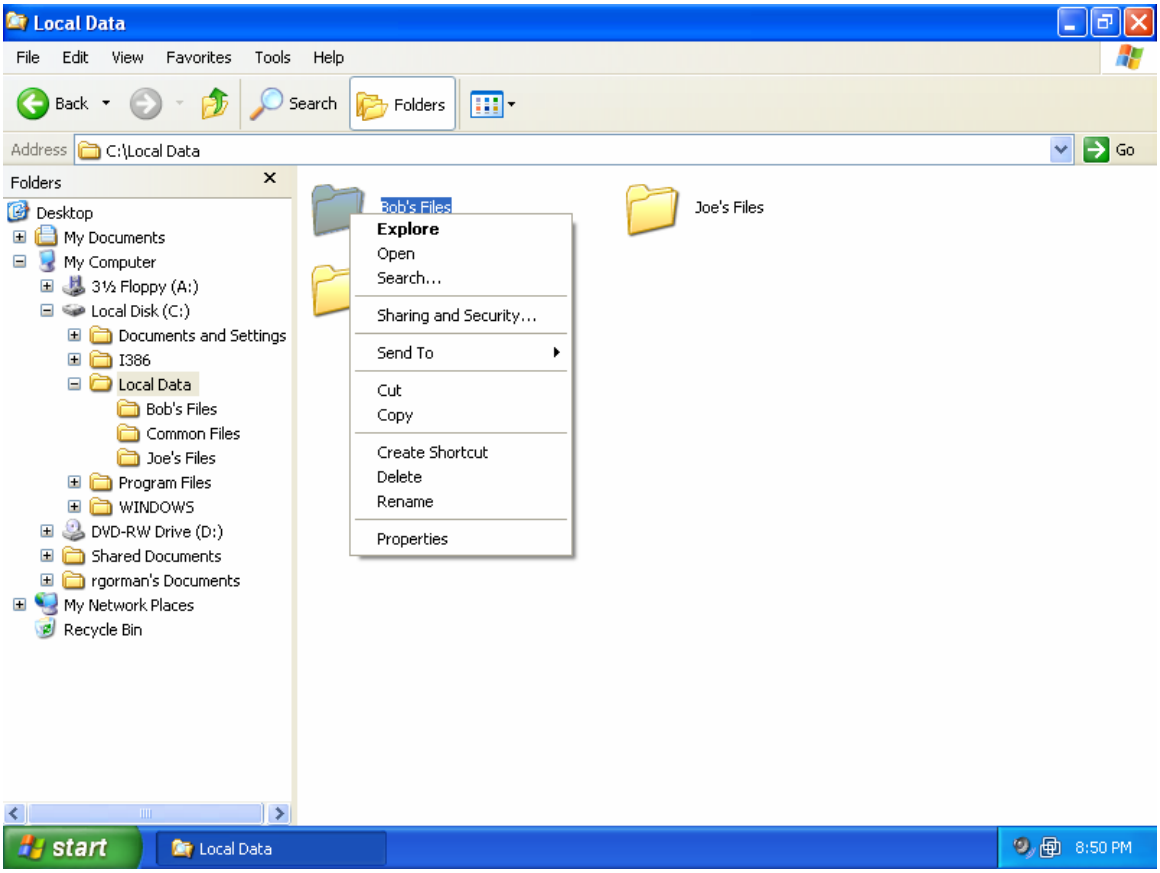
c. Use Windows Explorer to create a folder on Local Disk (C:) called **Local Data**. From the **File** menu, click **New**, and then click **Folder**.

d. Click the **Local Data** folder and then right-click in the open area at the right side of the screen. Click **New** and then click **Folder** and create a folder called **Bob's Files.** Repeat this process to create the folders **Common Files** and **Joe's Files.**

e. Navigate to the **Local Data** folder, where you can see the **Bob's Files** folder.

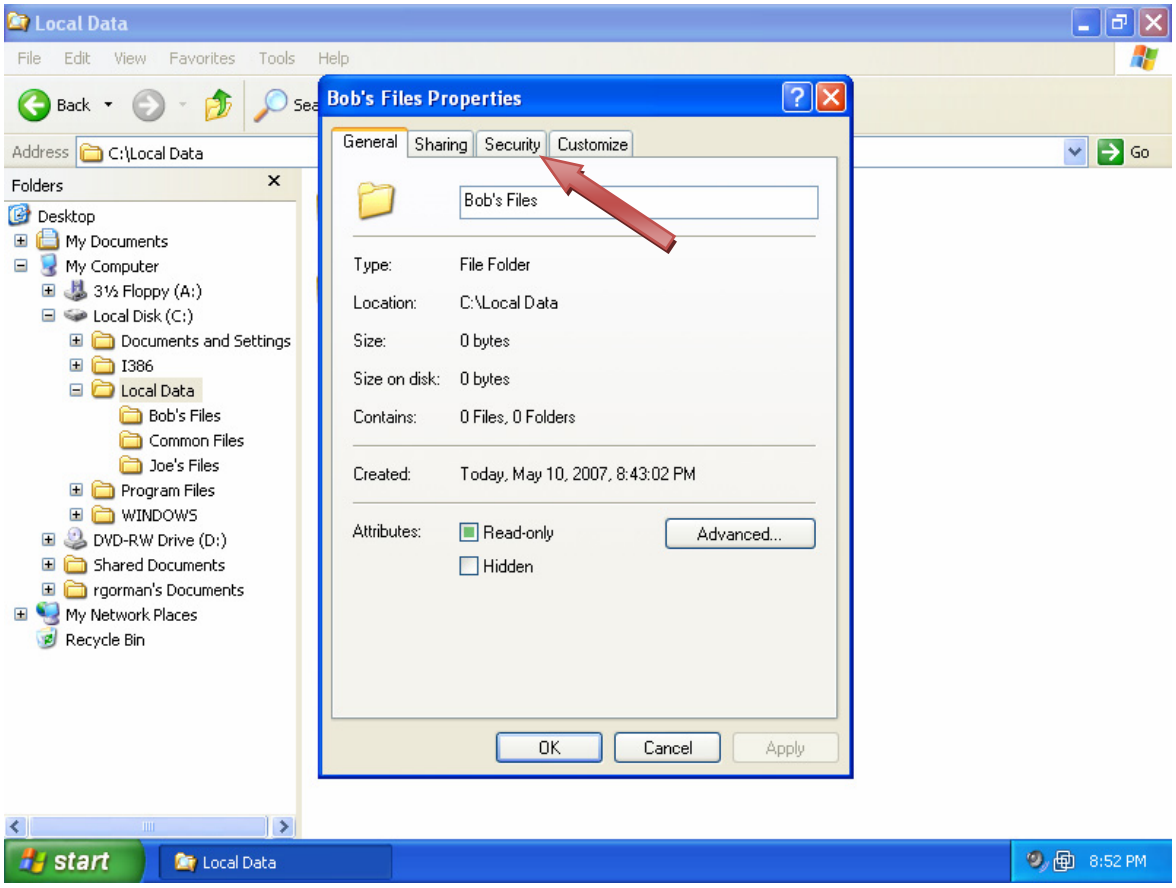


f. Right-click the **Bob's Files** folder and choose **Properties**.

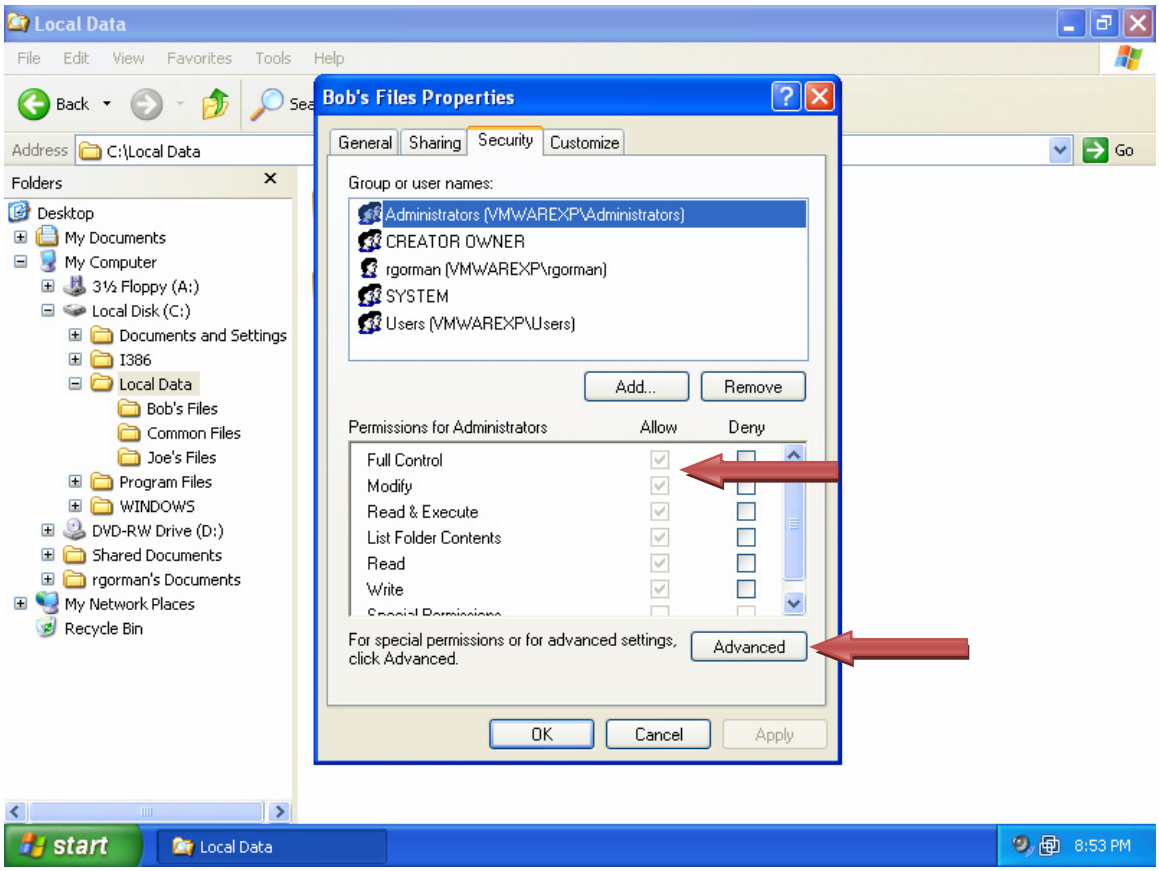


g. From the **Bob's Files Properties** dialog box, click the **Security** tab.

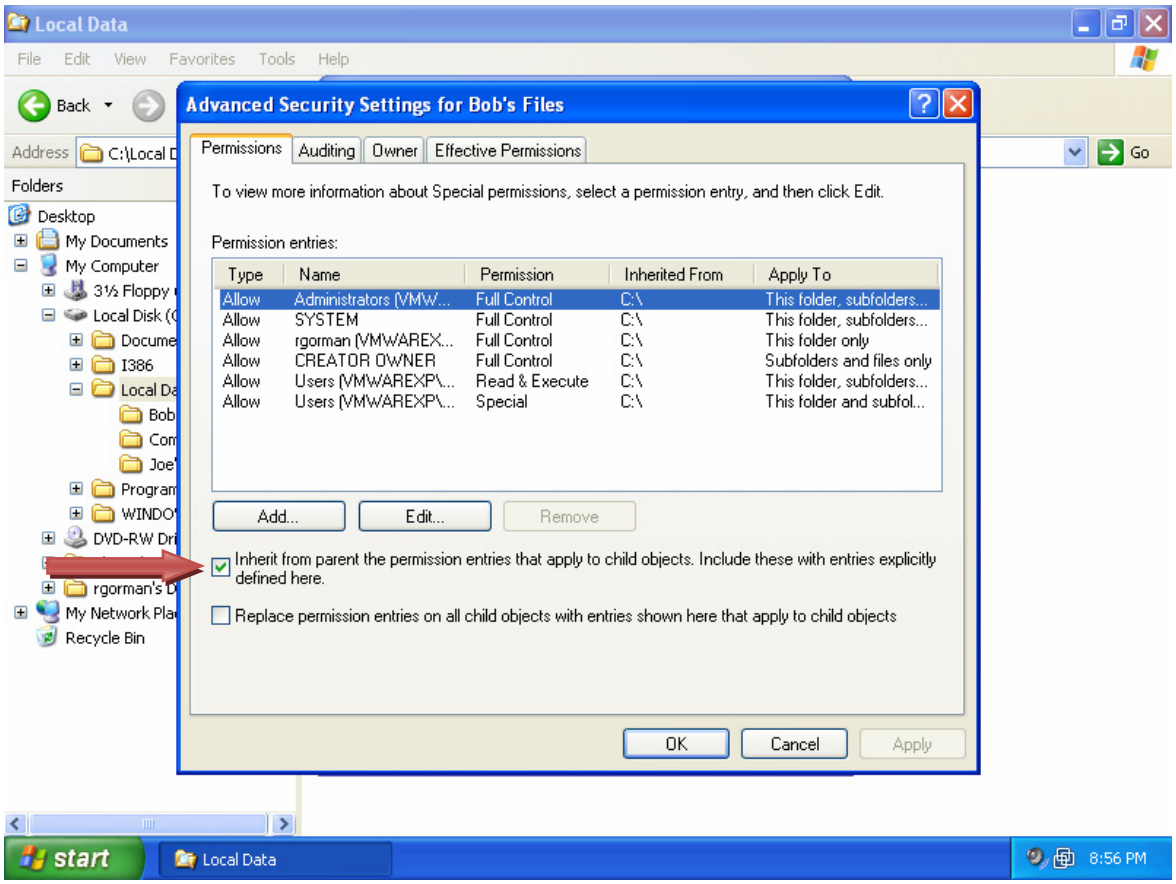
NOTE: You must be working on a drive that has the NTFS file system installed; otherwise, you will not see the **Security** tab.



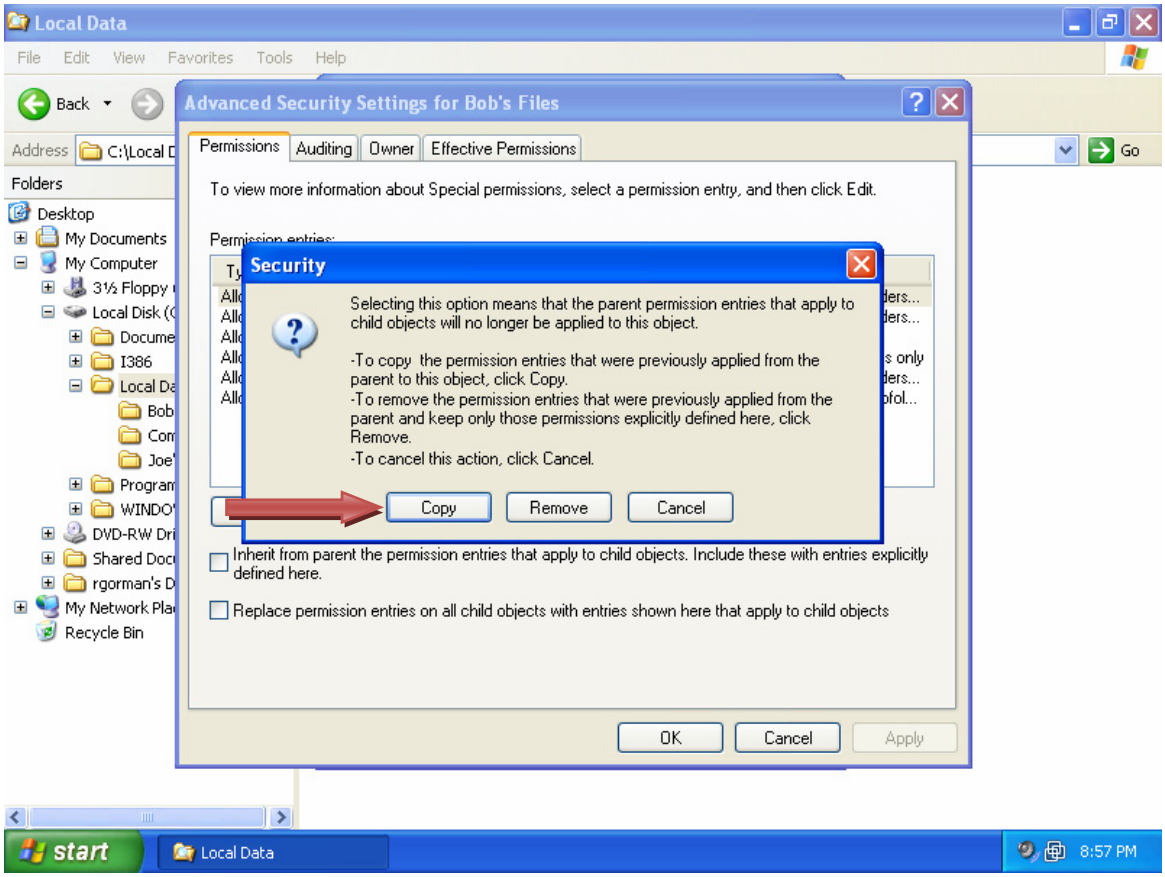
h. Notice that the permissions are dimmed and not modifiable. This restriction is due to the permissions that were inherited from a parent folder. To secure the folder, you will need to disable the inherited permissions. From the **Security** tab, click the **Advanced** button.



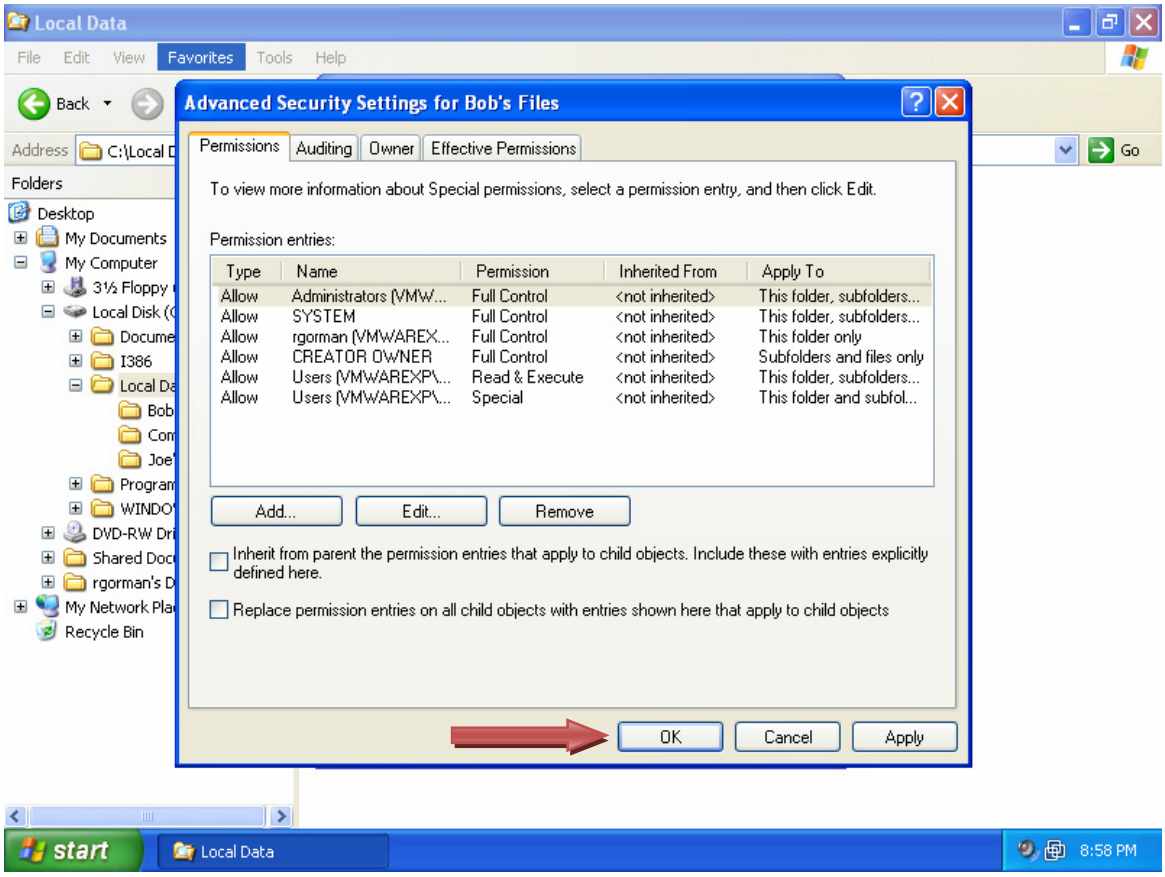
i. Uncheck the check box next to **Inherit from parent the permission entries that apply to child objects**.



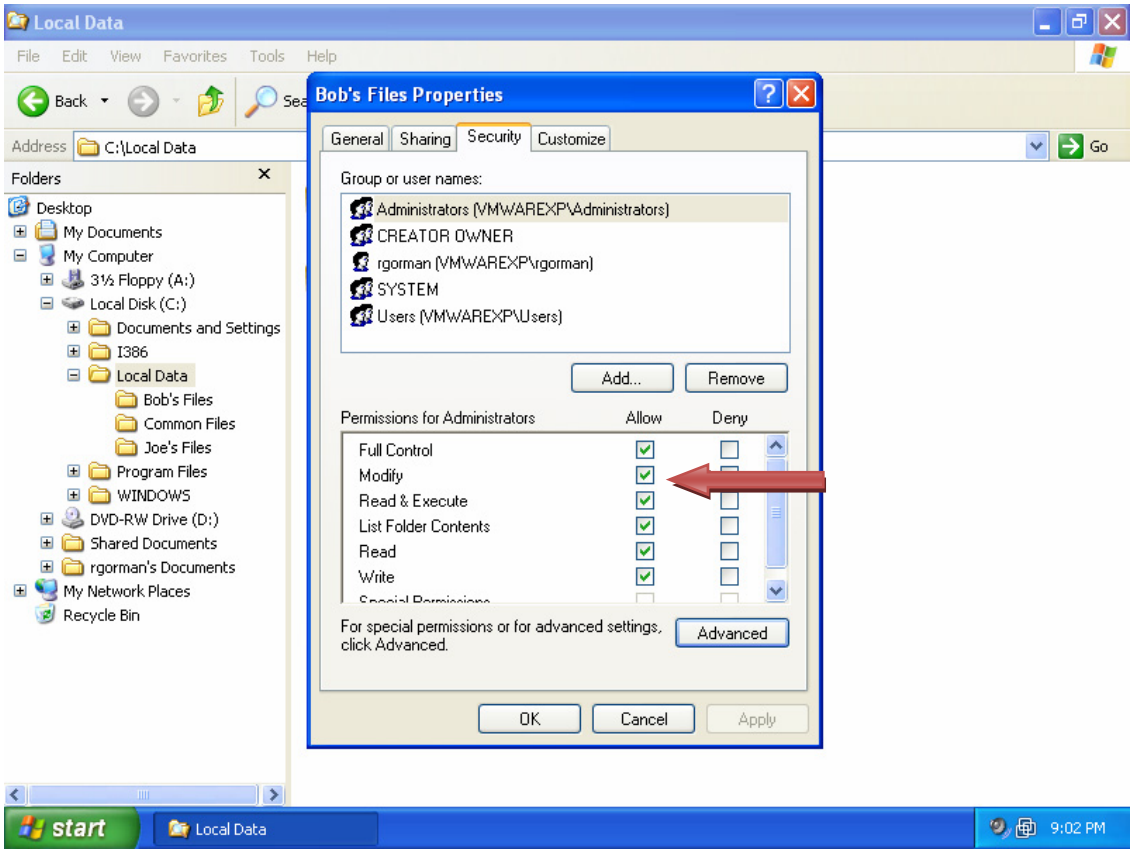
j. Click **Copy** to retain the existing permissions.



k. Click **OK.**

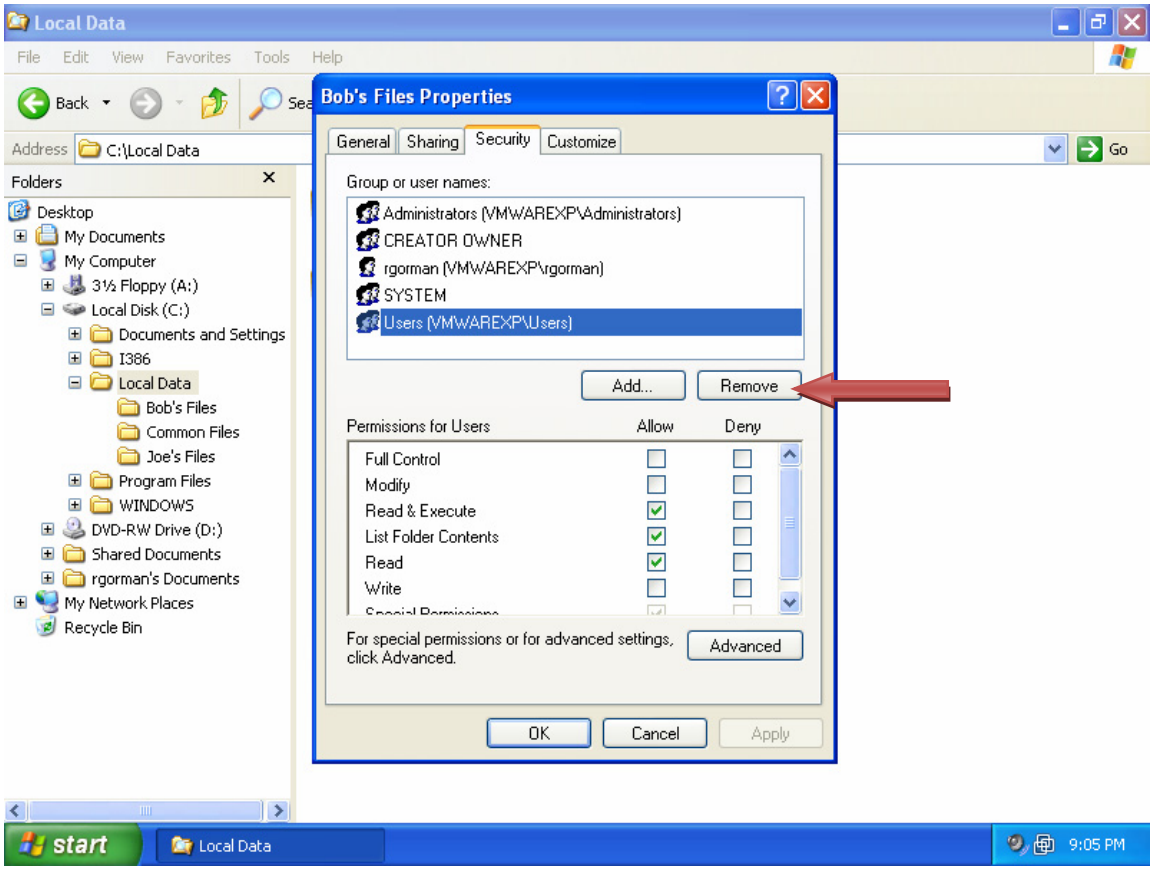


Now that inheritance is turned off, you are able to modify the permissions.

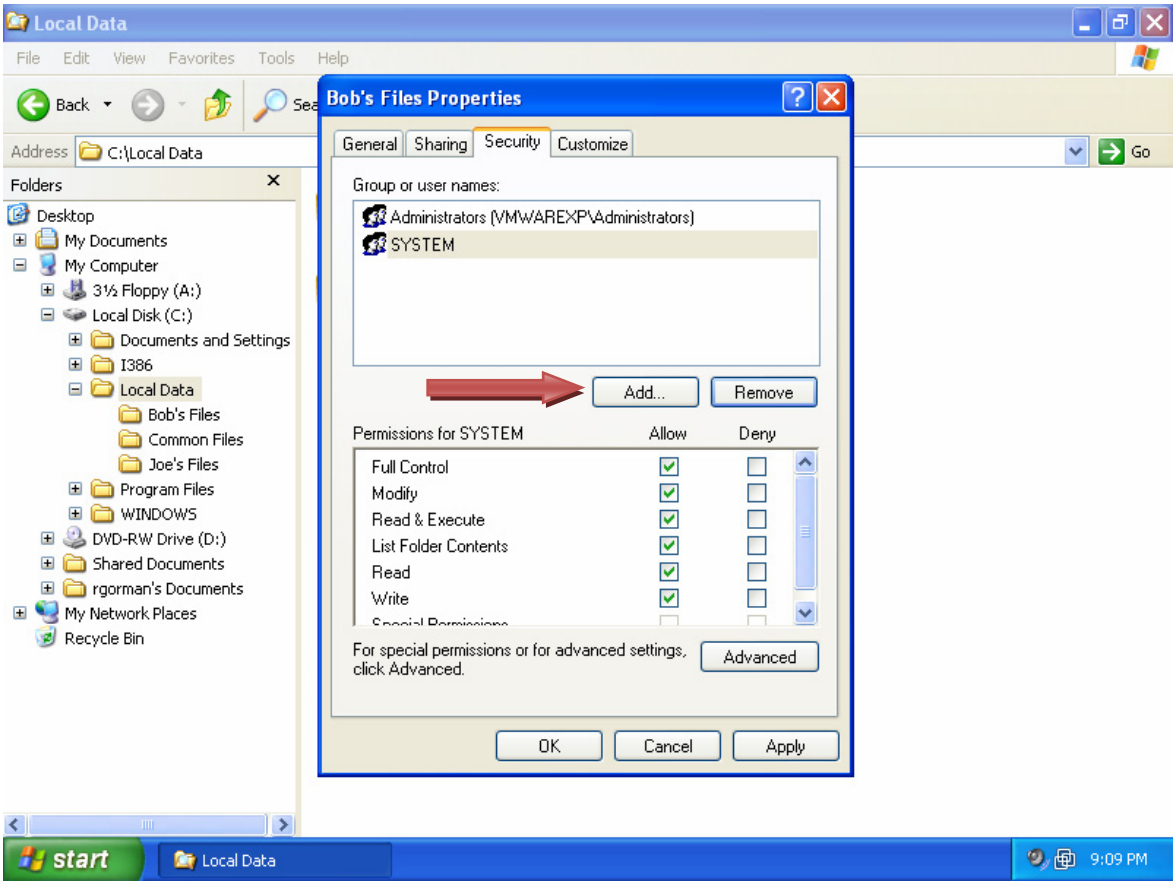


l. Select the **Users** group and click **Remove**. Continue to select the other remaining users and groups, except for Administrators and SYSTEM, and click **Remove**.

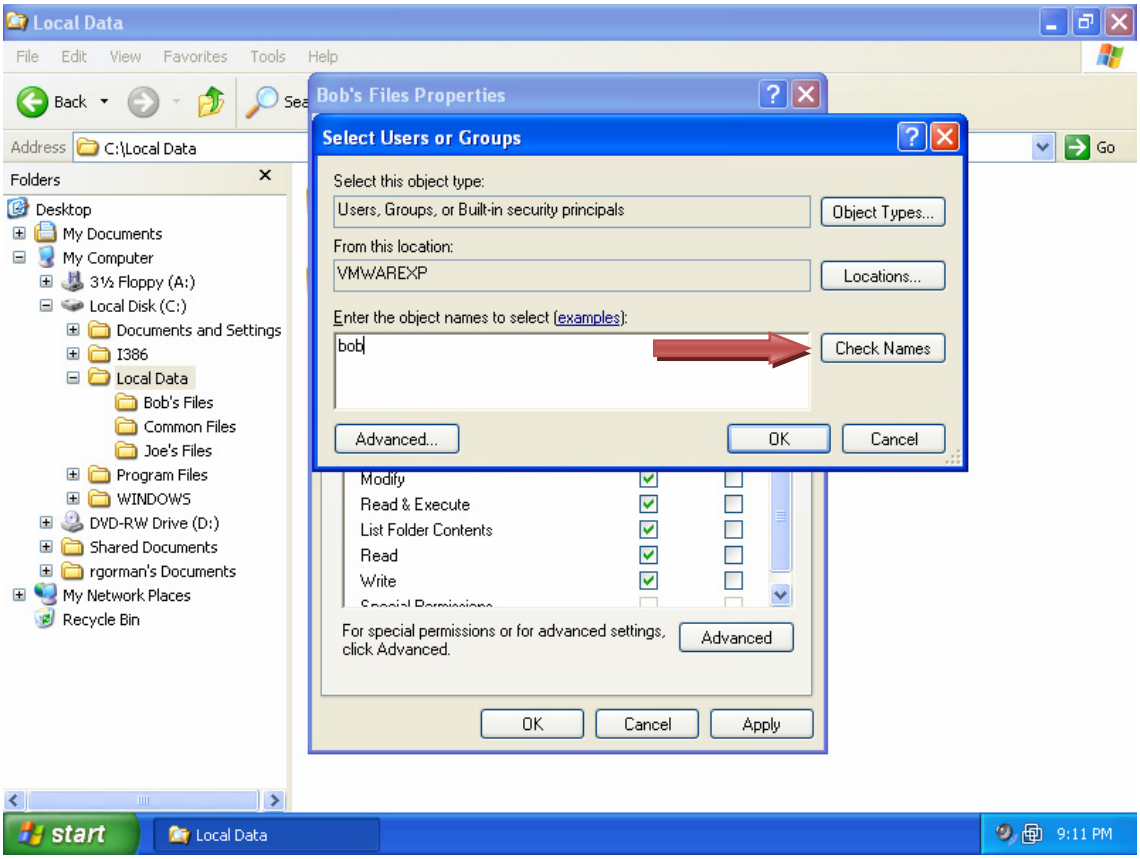
NOTE: Always grant the SYSTEM and Administrators groups Full Control access to directories and files to ensure that files can be backed up, recovered, and scanned properly by the computer system.



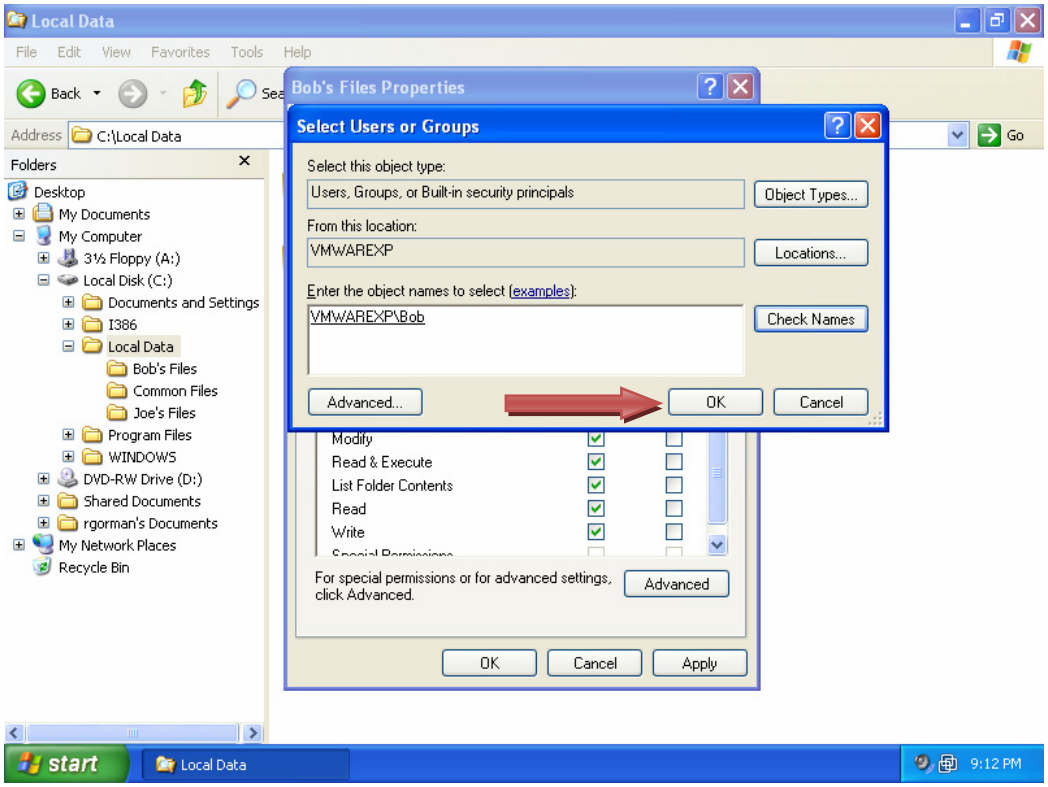
m. Now add Bob to the list. Click **Add**.



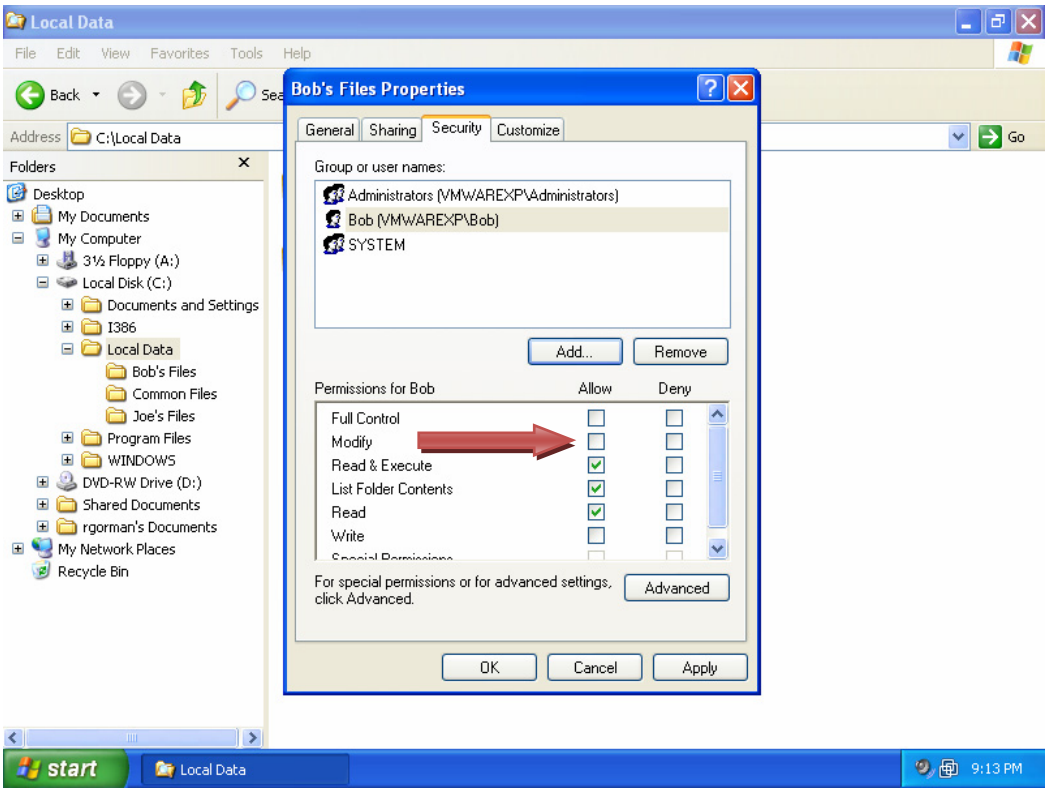
n. Type **Bob** in the text box and click the **Check Names** button to verify his account.



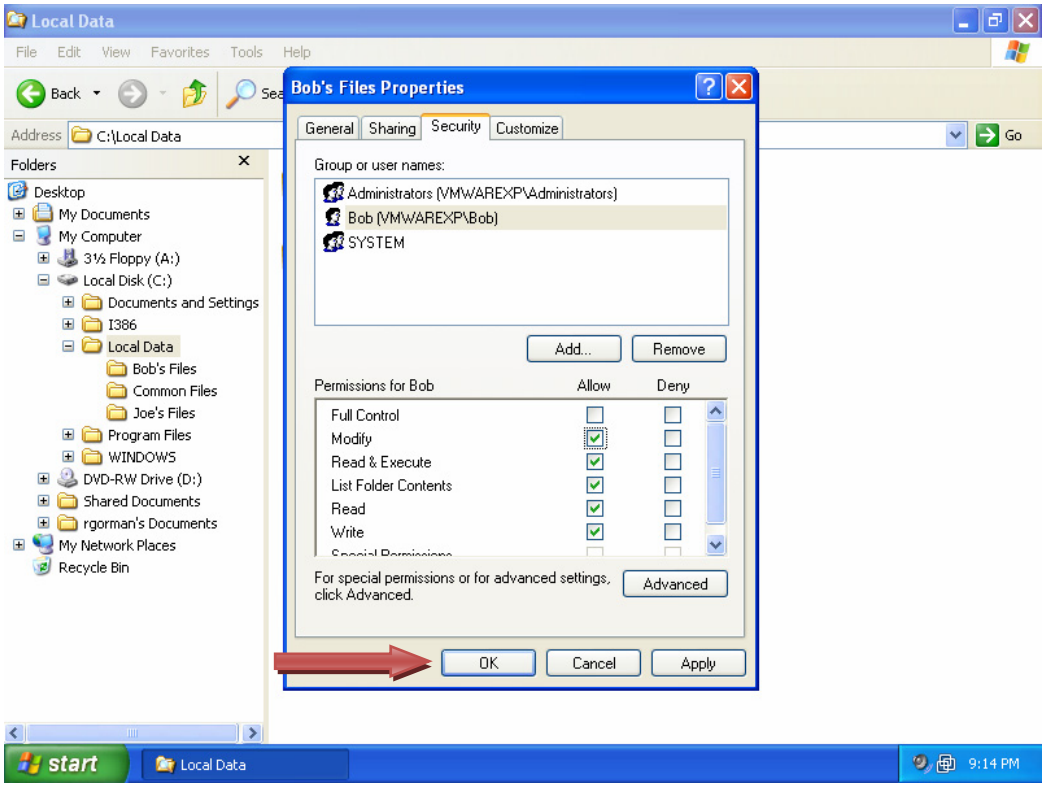
o. Now that Bob has been verified, click **OK**.



p. Bob is now added to the list. Notice that he currently has the Read & Execute, List Folder Contents, and Read permissions. Because Bob will need to write new files and delete existing files, grant Bob Modify permission. Check the check box in the **Allow** column next to **Modify**.

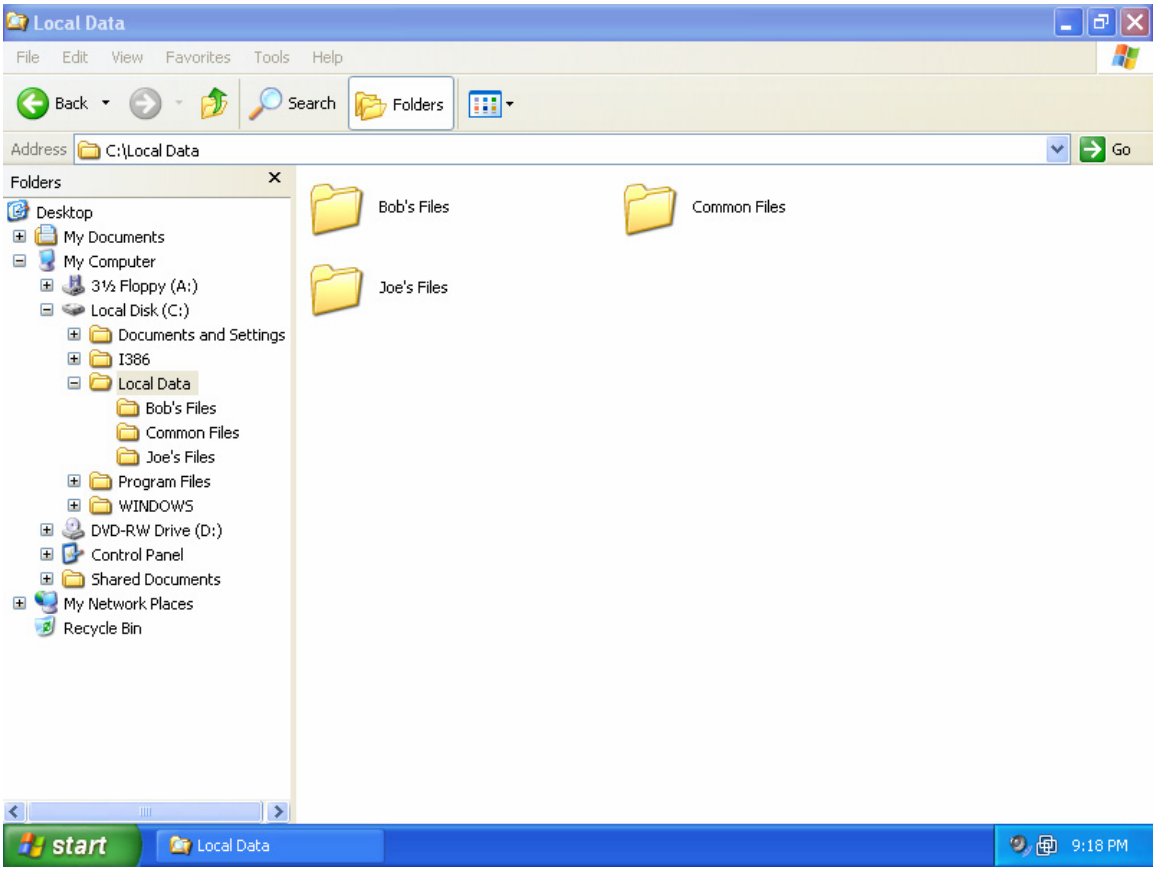


q. Now that Bob has been granted Modify permission, click **OK** to set the security.

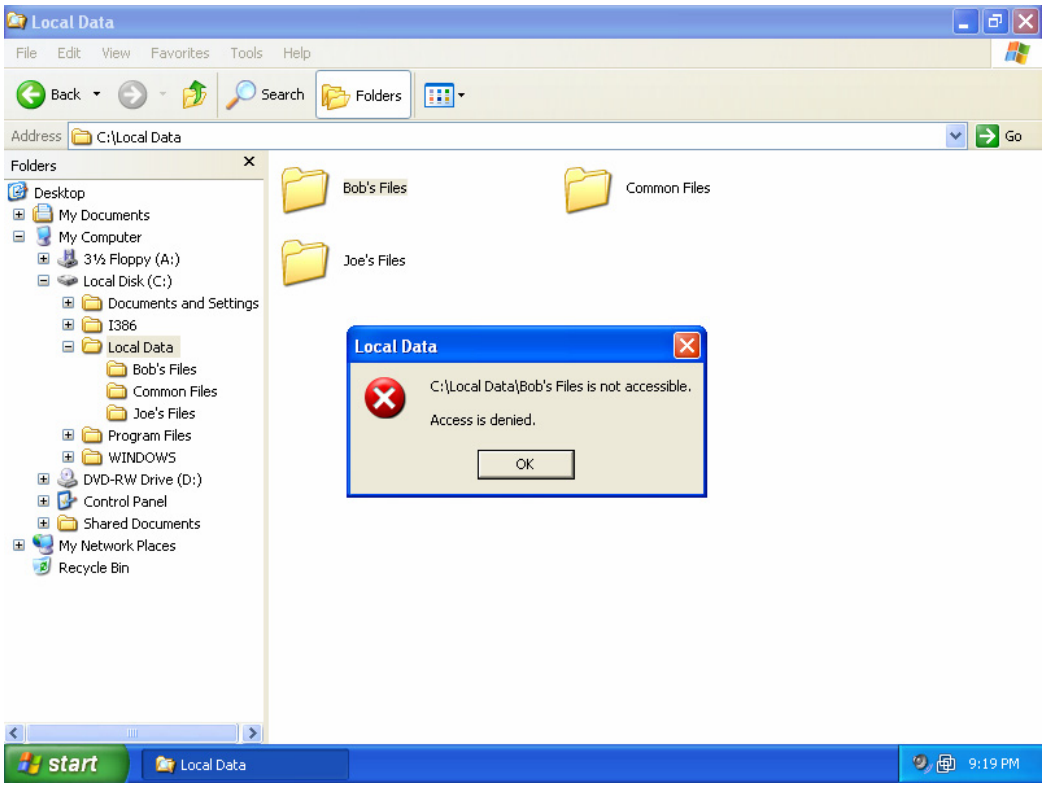


Step 2: Test Joe's access to Bob's Files

a. Log in to the local PC as Joe and try to access the **Bob's Files** directory.



b. Notice a popup dialog box indicating that Joe does not have permission to access these files. Because Joe does not have Administrative access to the PC, he is prevented from gaining access to **Bob's Files**.



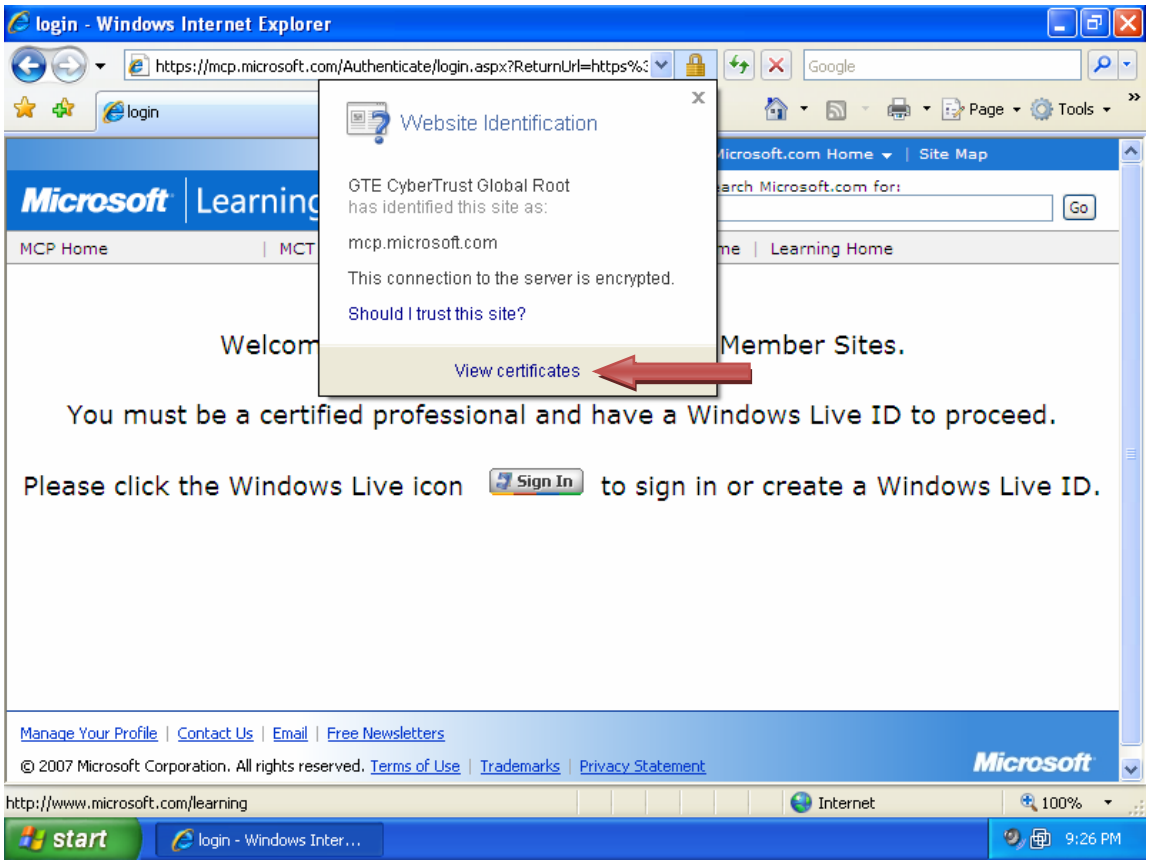
Part 2 – Identifying a secure communication channel when transmitting data over the Internet

Step 1: Identify a secure web page

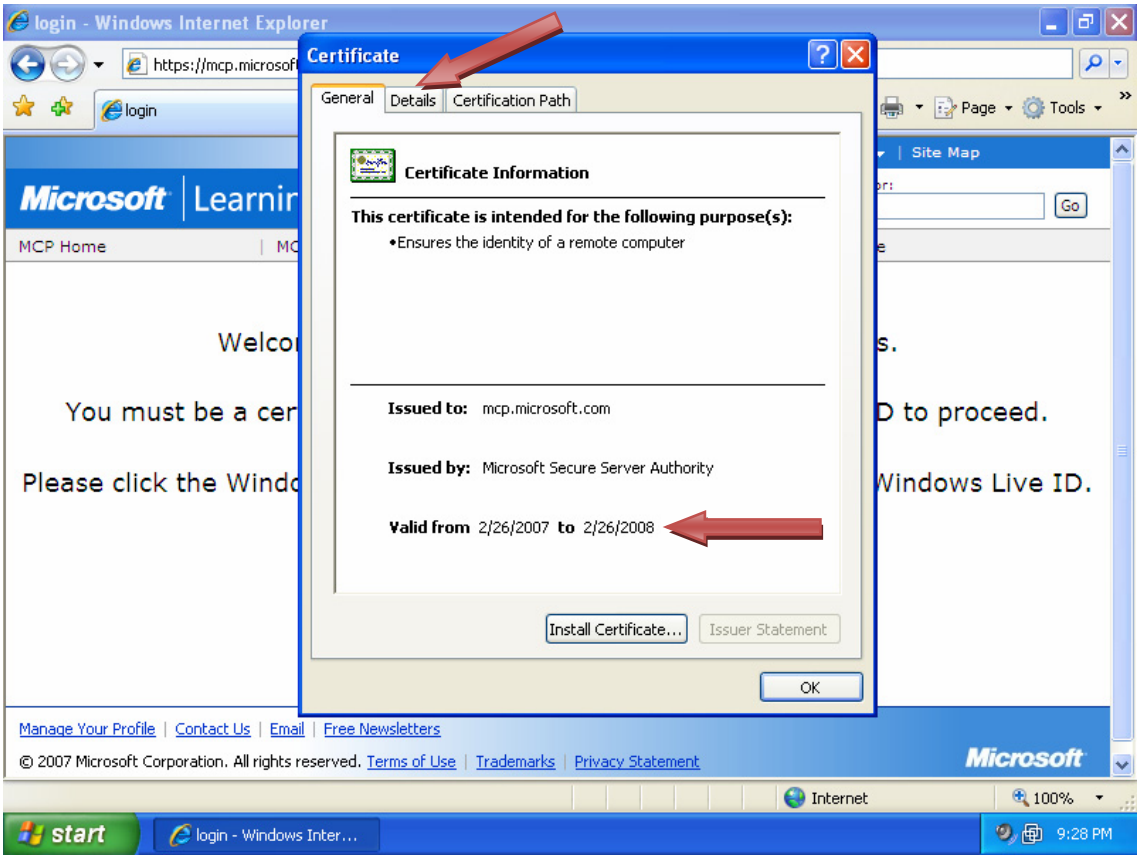
a. Launch Internet Explorer and navigate to http://www.microsoft.com/learning. This site is a typical unsecured page. Click the **MCP Members Site** link.

b. Notice that the URL changed from HTTP to HTTPS. HTTPS is the secure version of HTTP and uses SSL for its security. Notice also that there is a **lock** icon located to the right of the URL. The presence of the **lock** icon indicates that the site is secure. Click the **lock** to see more information about the secure site.

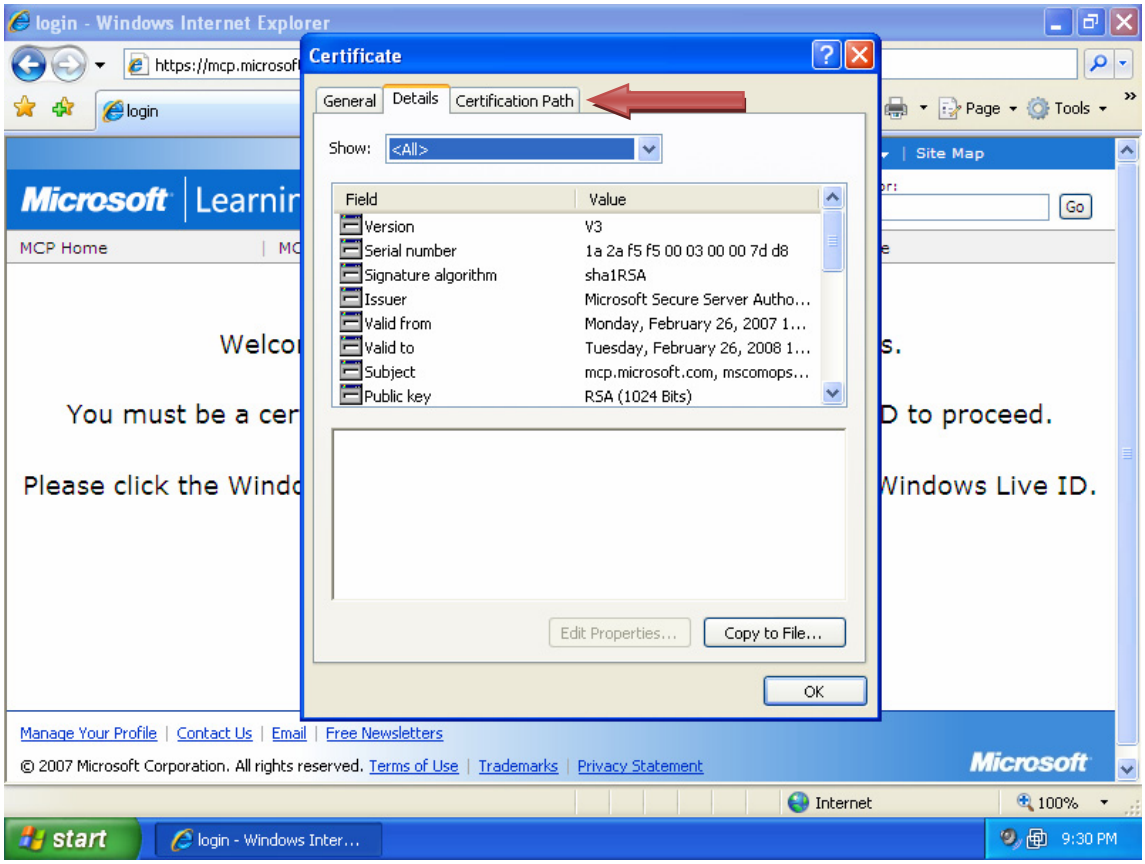
c. The popup window displays information about the issuer of the security certificate for this website. It also indicates that the connection to that server is secure. Click the **View certificates** link at the bottom of the popup window.



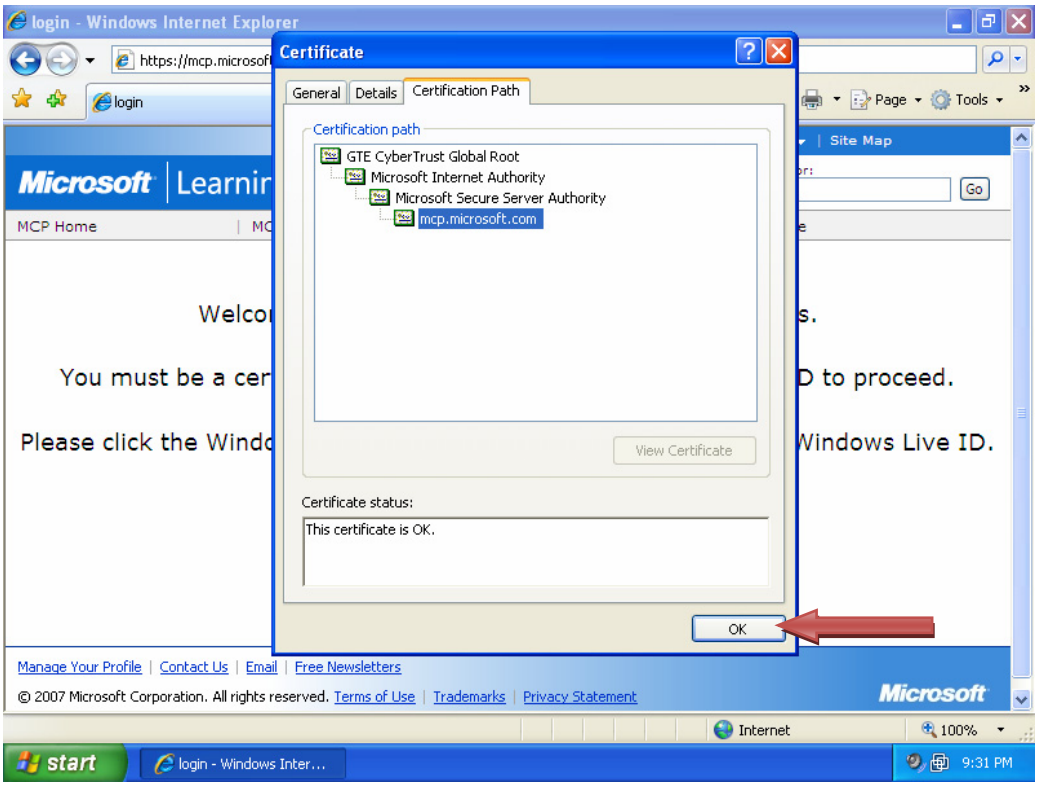
d. The Certificate window opens and displays the certificate that has been installed on the web server to allow it to use SSL. Notice the **Valid from** date range at the bottom. Certificates are only valid for a specific period of time, and then they must be renewed. The renewal process ensures that web server administrators continually validate their servers with the certificate authority who issued the certificate. Click the **Details** tab for more information.



e. The **Details** tab shows information about the certificate. Click the **Certification Path** tab.

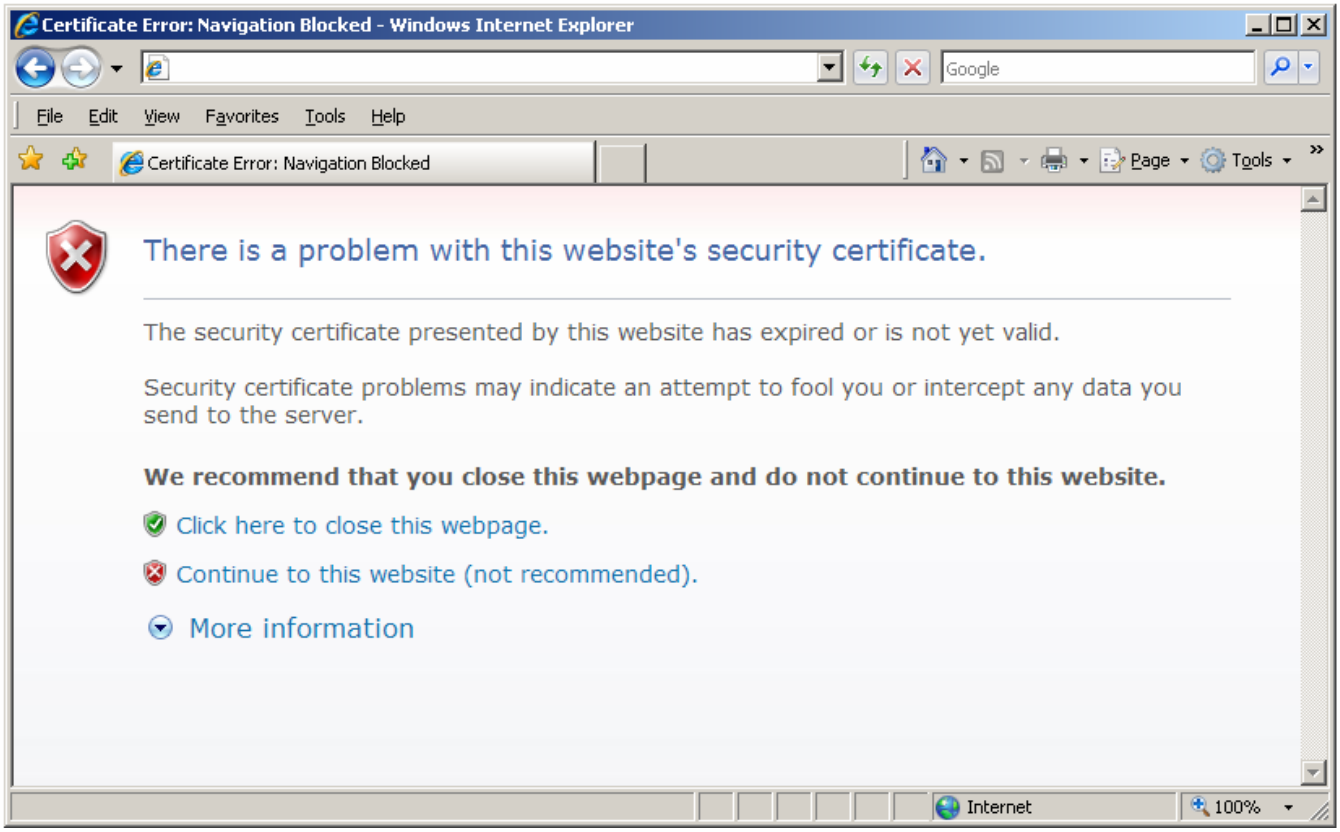


f. The **Certification Path** tab displays a hierarchical list of certification authorities that have been authorized to issue the web server certificate. Click **OK** to close the Certificate window.



Step 2: Examine secure access to an untrusted source warning

a. If the security certificate presented by a website is not from a trusted authority, Internet Explorer displays the screen shown below to alert you to the fact that there is a problem. It gives you options for closing the webpage or continuing to the website.



b. Unless you know the website to be legitimate you may not be able to trust the server or the content it provides. If you navigate to the certification path, as previously described, you will not see a list of trusted certification authorities. You may be working with secure (HTTPS) website but one that is self-certified and not certified by approved authorities.

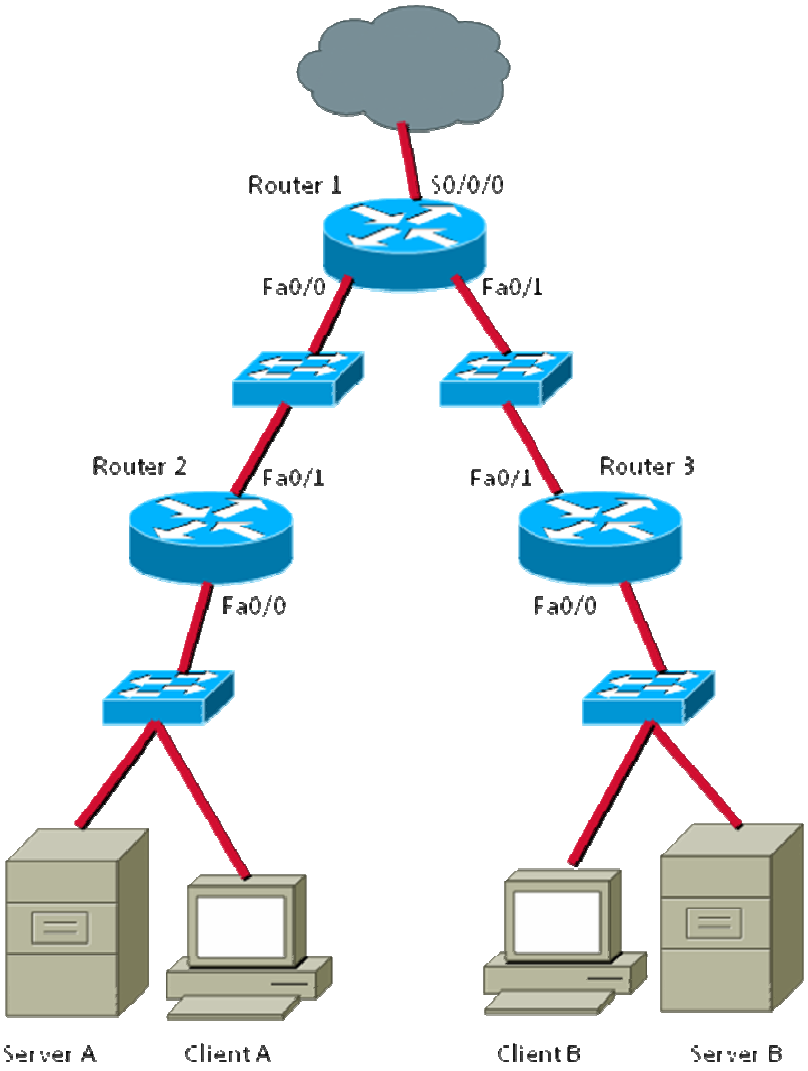
Lab 8.2.1 Planning for Access Lists and Port Filters

Objective

- Based on the predefined network diagram, determine where to implement access lists and port filters to help protect the network.

Background

You are the support technician sent onsite to assess the current network for a business customer that would like to reduce the risk of a security breach on the network.



Identifying where to place access lists

Step 1: Restrict Client A to one subnet

You are asked to restrict Client A to only the subnet to which it is currently attached. Client A needs to be able to access Server A, but it does not need to access the Internet or Server B. Where would you place the access list?

Router	Interface	Allow or Deny?	Input or Output filter?	Why?

Step 2: Restrict Client A access to Server A but allow access to Server B and the Internet

You are asked to restrict Client B from accessing Server A, but Client B needs Internet access and access to Server B. Where would you place the access list?

Router	Interface	Allow or Deny?	Input or Output filter?	Why?

Step 3: Allow only Client A to access the routers using only SSH

You have been asked to secure access to the routers for only Client A, which will be the management PC for those routers. You want to limit access to only SSH from Client A and prevent Telnet access. Where would you place the access list?

Hint: More than one interface on more than one router is needed to control SSH and Telnet access to the routers.

Router	Interface	Input or Output filter?	Port	Allow or Deny?	Why?

Lab 8.2.5 Researching an Anti-X Software Product

Objective

- Research an Anti-X software package that meets the requirements for a small business.

Background

You have been asked to recommend an Anti-X software package for a small business. The business is concerned about viruses and malware, because it has been a problem in the past. The customer also wants to be able to centrally manage the Anti-X solution. The customer would like to have all Anti-X alerting viewable in one location, and would like to receive e-mail alerts when an infection has occurred.

Step 1: Identify three products

Using the Internet, research products from three different companies that meet the requirements of the small business. The Anti-X product needs to have the following features:

- Anti-virus
- Anti-spyware
- Anti-malware
- Central management
- E-mail alerts

Company	Product

Step 2: Compare pricing

Now that you have identified three different products that meet the requirements of the customer, compare the pricing. The business has 27 workstations and 3 servers. Be sure to account for licensing of all the computer systems to generate the overall price. Examine the cost and show all itemized components that comprise the overall price.

Company	Product	Price

Lab 8.3.1 Interpreting a Service Level Agreement

Objectives

- Describe the purpose of a Service Level Agreement (SLA).
- Review general customer SLA requirements.
- Analyze a sample SLA and answer question regarding content and suitability based on customer needs.

Background / Preparation

An SLA is a formal agreement between a customer and a service provider. The SLA defines the types and levels of service that the customer can expect to receive, as well as any penalties that may exist for non-conformance. In this lab, you will review the purpose of an SLA and the types of customer requirements it can cover. You will then analyze a sample SLA between an ISP and a Customer of a medium-size business and answer questions regarding the provisions of the SLA. You may work alone or in small groups.

The following resource is required:

- Sample SLA (in this lab)

Step 1: Review typical customer needs

A Typical customer will have the following requirements regarding an SLA. These requirements should be included in the SLA with the service provider:

- **Service description** – Describes the service volume and the times when the service is needed. It also describes the times when the service does not need to be covered by the SLA. The services described could be those typically found in a small- to medium-size manufacturing company: e-mail service, electronic data interchange, online accounting, secure remote worker support, remote instrumentation and control systems, and backup and recovery services.
- **Availability** – Describes the availability of each service in hours per day and days per month that the service can be available.
- **Performance** – Describes the peak and off-peak distribution of the volume of data the customer expects to generate for each service.
- **Reliability** – Describes the reliability percentage required for each service.
- **Response time tracking and reporting** – Describes the performance need of the users for each service.
- **Security** –- Describes the security policies of the customer as they pertain to the services to be covered by the SLA.
- **Budget Cycle** – Identifies the budget cycle of the customer.
- **Penalties for Service Outages** – Provides an estimate for the cost to the customer for a service outage for each of the services the customer wants covered by an SLA.
- **Costs** – Provides a table of costs that the customer has paid in the past for the services provided by other SLAs.

Step 2: Analyze a sample SLA and identify key components

a. Read over the sample SLA that follows and answer these questions regarding content, ISP responsibilities, and customer requirements.

b. According to this agreement, can the ISP be held liable for damage to equipment owned by the customer [Client] or data loss that occurs due to accidental actions by ISP vendor staff or other persons? _____

c. What are some examples of One Time Services included in the SLA?
_____

d. What are some examples of Ongoing Services included in the SLA?
_____

e. When will regular downtime maintenance be scheduled and how many business days notice must the ISP give of any scheduled downtime?
_____

f. What does the ISP's network monitoring system do when an error condition is detected?
_____

g. What is the stated availability of the Systems Administrators in the event of a system failure?
_____

h. What is "usage monitoring" and how does the ISP provide this service?
_____

i. Regarding problem severity and ISP response time, what is the difference in response between "Level 1 – normal business hours" and "Level 3 – normal business hours"?
_____

j. On what factors are the penalties for service outages based?
_____

(Sample)

Service Level Agreement

Between

[Client]

and

ISP Services Vendor, Inc.

As of [Date]

I. General Term of the Service Level Agreement

This Service Level Agreement (SLA) documents the agreement between [Client] and the ISP Services Vendor, Inc. (ISPSV) for delivery of ISP services including services delivered, levels of service, communications, and pricing. This agreement is in effect from [start_date] to [end_date] unless otherwise modified by an amendment. All terms are in effect until modified by an amendment.

Amendments can be added to the agreement at any time that the parties agree. If there are substantial service changes, then some time may be required to implement. The timing of the amendment will be included in the amendment. Changes to the agreement that result in changes in charges may require 30 days to implement.

Either party can terminate this agreement in whole or in part with 30 days notice. The SLA is reviewed on its anniversary. Billing rates may be adjusted based on service level changes.

II. Warranty and Liability

It is the mission of the ISPSV is to provide high quality, cost effective ISP facilities services to the surrounding community.

We commit to protecting the equipment and data supported under this SLA from deliberate damage from ISPSV or other persons provided access to the equipment by ISPSV. However, we will not be held liable for and damage to equipment owned by the Client or data loss that occurs due to accidental actions by ISP VENDOR staff or other persons.

III. Services Provided to [Client]

This table indicates which services are to be included in this SLA. Pricing of services is via the ISPSV pricing model and attached as an amendment to this SLA.

	Service	Comments
	One Time Services	
	Rack & Computer Installation	
	Backup Implementation	
	Firewall Configuration	
	Ongoing Services	
	Server Hosting	
	Backup and Recovery	
	Unix System Administration	
	Windows System Administration	
	Application Administration	

IV. System Availability

Systems will be available 7X24 except for regularly scheduled maintenance downtime. The downtime maintenance schedule will be negotiated with each client and will occur between 7pm and 7am. Clients will be given at least three (3) business days notice of any scheduled downtime.

The ISP facility is staffed with professional systems administrators from 7 am to 7 pm on workdays. The systems administrators are on call 7X24 for system failures.

V. System Monitoring

Basic operating monitoring, periodically testing systems for proper functioning, is provided for all systems housed in the ISP facilities. The monitoring, pages the on-call systems administrator when error conditions are detected.

External operating monitoring can be arranged through a contract with ExternalAlertServices who provides external monitoring. This can be arranged with the client paying the fees (approximately $25/month/url) for this service.

Usage monitoring provides users with statistics on web site “hits”. The ISP facility maintains a WebTrends server for this purpose. Data from the WebTrends server is available to clients on a monthly basis.

VI. System Notifications

The ISP facilities will provide a set of email lists for each server and application. The membership of these is determined and maintained by the client. The lists are:

- **[system]-info**

  Will be notified of system logged messages on the operational status of the system.

- **[system]-announce**

  Will receive all ISP facilities messages about planned maintenance, systems outages, or other events.

- **[system]-[application]-info**

  Will be notified of system logged messages on the operational status of the application.

- **[system]-[application]-announce**

  Will receive all ISP facilities messages about planned maintenance, systems outages, or other events

VII. Change Management Process

All requests for changes to systems or applications, whether originated by the client or by ISPSV staff must go through the ISPSV change management process for approval. The process starts with a request submitted via ISP Management Change Process (MCP). Requests will be logged then sent via email to the authorized Client for approval. The Client will return the request via email with approval or denial of the request.

With the exception of emergencies, requests will not be done without Client approval. In the case of an emergency, the client will be contacted as quickly as feasible and informed of the changes.

- **Communications Methods**
  - **Standard Requests**

    All standard requests for account changes or other non-emergency requests must be submitted via ISP MCP. The request must include:

    - Client Name
    - System Name
    - Application Name
    - Nature of the Request
    - Date the Change is Needed
    - Problem Severity (level 1, 2, 3 or 4)

  - **Emergency Requests**

    Emergency requests must be submitted either in person or via the ISP facilities hot line at (123) 456-7890. If the call transfers to voice mail leave a message which includes your name and a call back phone number. The on call Systems Administrator will be automatically paged within 5 minutes and will return your call.

  - **Escalation**

    If problems are not resolved to the client's satisfaction by the above methods, the client can escalate the response by contacting ISP VENDOR management in the following order: 1. Facilities Director, 2. Marketing Director, 3. President.

- **Systems Request Authority**

  We will maintain four lists to grant people authority. These lists are in the client addendum and are as follows:

  - **Master authority list**

    List of people who can add or remove people from the remaining lists.

  - **Account change authority list**

    List of people who can request Account changes.

  - **Systems changes authority list**

    List of people who can request System changes.

  - **Application changes authority list**

    List of people who can request Application changes.

VIII. Problem Severity and Response Time

ISPSV will respond to problems according to the following severity levels:

Problem Severity	Initial Response Time	Follow-up w/Client
Level 1 – normal business hours	Respond to client within 30 minutes of notification 100% of the time	Hourly
Level 1 – off hours	Respond to client within 1 hour of notification 95% of the time	Hourly
Level 2 – normal business hours	Respond to client within 4 hours of notification 100% of the time	Daily
Level 3 – normal business hours	Respond to client within 1 working day of notification 100% of the time	Weekly
Level 4 – normal business hours	Respond to client within 3 working days of notification 100% of the time	Monthly

o Severity Level 1:

Major Business Impact – defined as a problem that causes complete loss of service to the Client production environment and work can not reasonably continue. Workarounds to provide the same functionality are not possible and can not be found in time to minimize the impact on the Client's business. The problem has one or more of the following characteristics:

- A large number of users cannot access the system.
- Critical functionality is not available. The application cannot continue because a vital feature is inoperable, data cannot be secured, backed up, etc.

o Severity Level 2:

Significant Business Impact – this classification applies when processing can proceed but performance is significantly reduced and/or operation of the system is considered severely limited. No workaround is available, however operation can continue in a restricted fashion. The problem has one or more of the following characteristics:

- Internal software error, causing the system to fail, but restart or recovery is possible.
- Severely degraded performance.
- Some important functionality is unavailable, yet the system can continue to operate in a restricted fashion.

o Severity Level 3:

Minor Business Impact – a problem that causes minimal loss of service. The impact of the problem is minor or an inconvenience, such as a manual bypass to restore product functionality. The problem has one or more of the following characteristics:

- A software error for which there is a Client acceptable workaround.
- Minimal performance degradation.
- Software error requiring manual editing of configuration or script files around a problem.

o Severity Level 4:

No Business Impact – a problem that causes no loss of service and in no way impedes use of the system. The impact of the problem has one or more of the following characteristics:

- A software enhancement for which there is a Client acceptable workaround.
- Documentation error.

IX. Penalties for Service Outages

Problem Severity Level	Service Affected	Penalty Assessed

X. ISP facilities Policies

See ISPSV Policies document for all policies including Security, Change Management, Scheduled Maintenance, Backup and Restore Procedure, Appropriate Use Policy, and Hardware Requirements.

XI. Billing

ISPSV bills on a monthly basis, directly charging the appropriate client account with the agreed upon charges.

XII. Signatures

This Service Level Agreement has been read and accepted by the authorized representatives of ISPSV and [Client].

Signature (ISPSV) Date	Signature ([Client]) Date
Name	Name
Title	Title

Appendix 1: Services and Pricing

System or Application	Services	Price

Appendix 2: System Requests Contact Lists

Name	Email	Work	Cell	Home
Master Contact				
Account Change				
System Change				
App Change				

Lab 8.3.2 Conducting a Network Capture with Wireshark

Objectives

- Perform a network traffic capture with Wireshark to become familiar with the Wireshark interface and environment.
- Analyze traffic to a web server
- Create a filter to limit the network capture to ICMP packets.
- Ping a remote host to observe how the ICMP packet filter operates during the network capture.

Background / Preparation

In this lab, you will install Wireshark, a well-known network protocol analyzer and monitoring tool. Wireshark captures all packets sent or received by the computer NIC. It can be installed either in the lab or on a PC at home. You will use it to trace and view various types of network protocols and traffic. Wireshark was formerly known as Ethereal.

Wireshark software is freeware and is available from www.wireshark.org. The software installer, wireshark-setup-0.99.5.exe, should be available on the local Networking Academy server.

You can perform this lab individually, in pairs, or in teams.

The following resources are required:

- A Windows XP-based PC with an Ethernet network and at least two hosts
- Wireshark Version 0.99.5 software (or most current version)
- Internet connectivity (optional but desirable)
- Access to the PC command prompt
- Access to PC network TCP/IP configuration

Step 1: Install and launch Wireshark

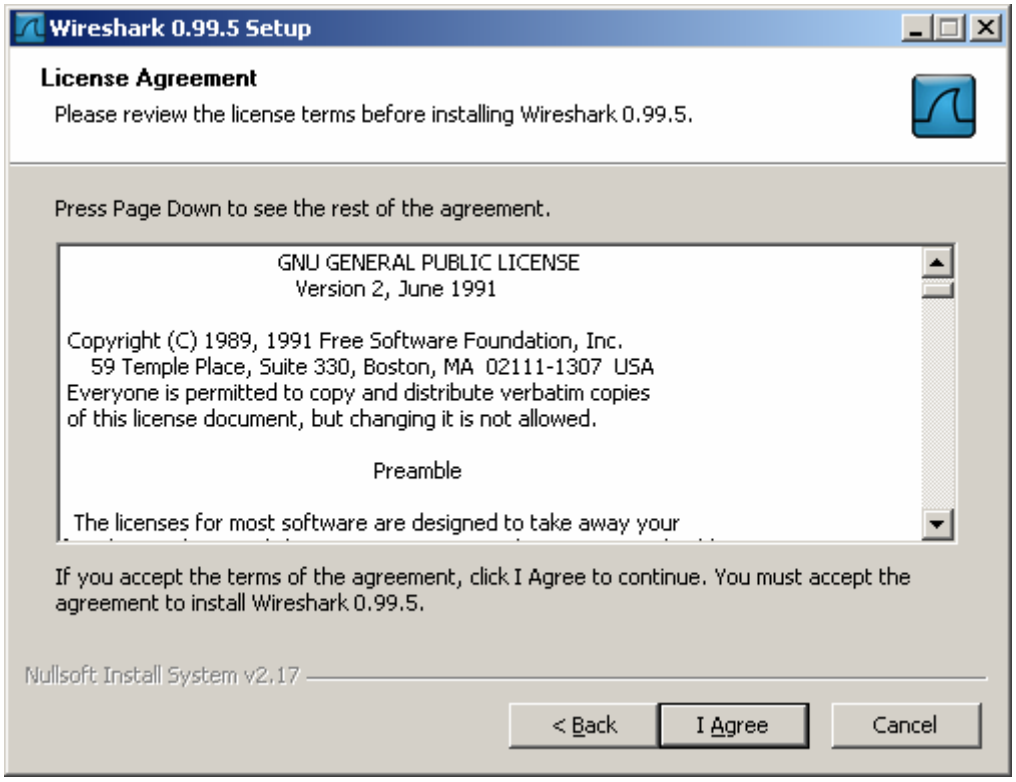
If Wireshark has been loaded on the PC previously, go to the Wireshark program folder **Start > All Programs > Wireshark > Wireshark** and click the application icon.

If Wireshark has not been installed, follow these steps:

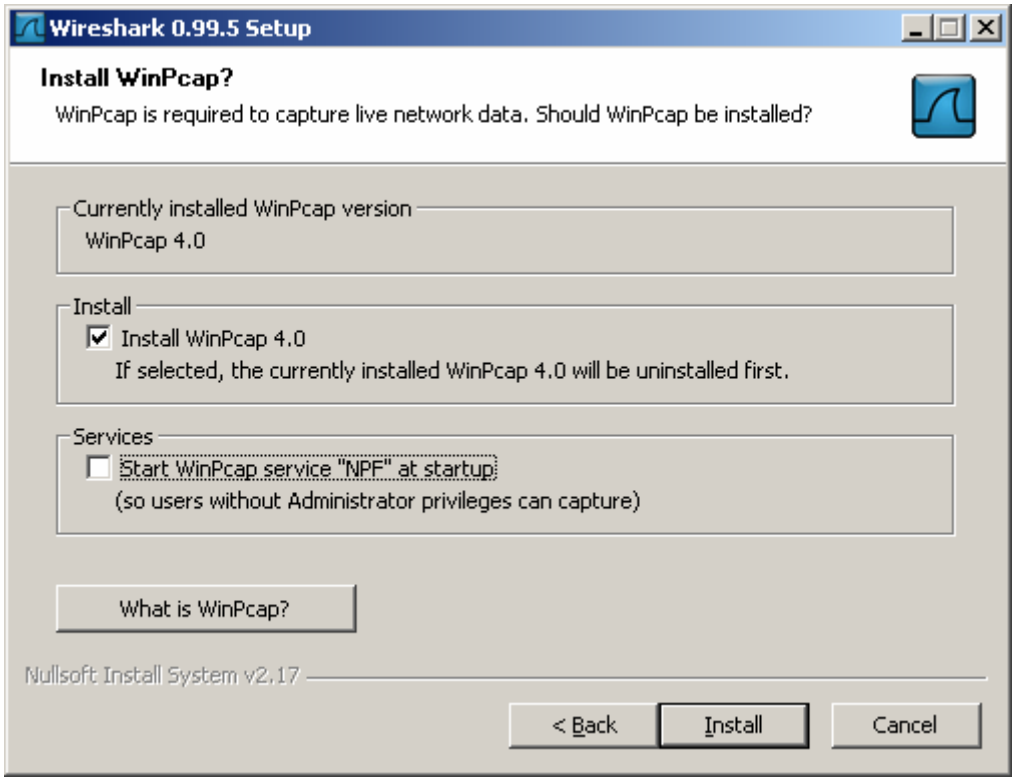
a. Given the local network path to the Wireshark software installer, wireshark-setup-0.99.5.exe, download the installer to the PC desktop.

b. Double-click the installer and follow the installation prompts, accepting the defaults.

1) Click **I Agree**.



2) Make sure to install WinPcap on the PC. WinPcap includes a driver to support packet capture. Wireshark uses this library to capture live network data with Windows.



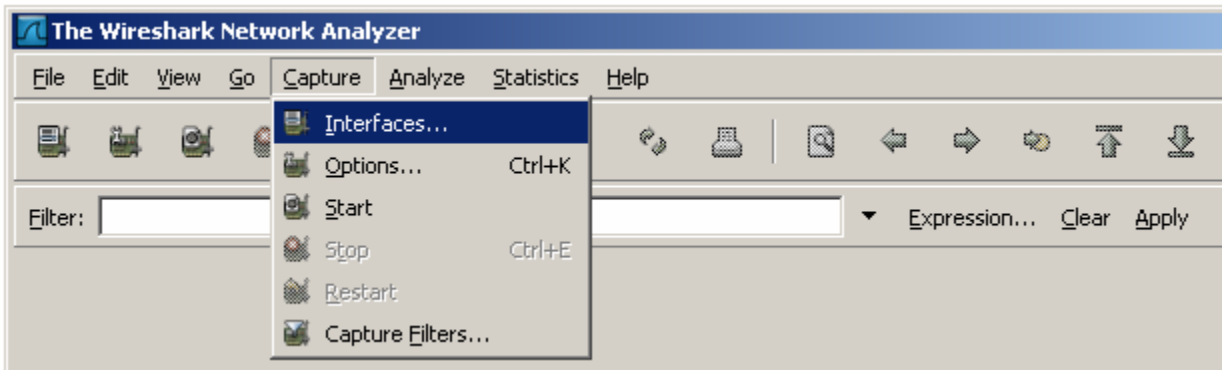
c. Click **Install** and follow the remaining prompts to the end of the installation process.

d. After the software is installed, click the checkbox to launch Wireshark.

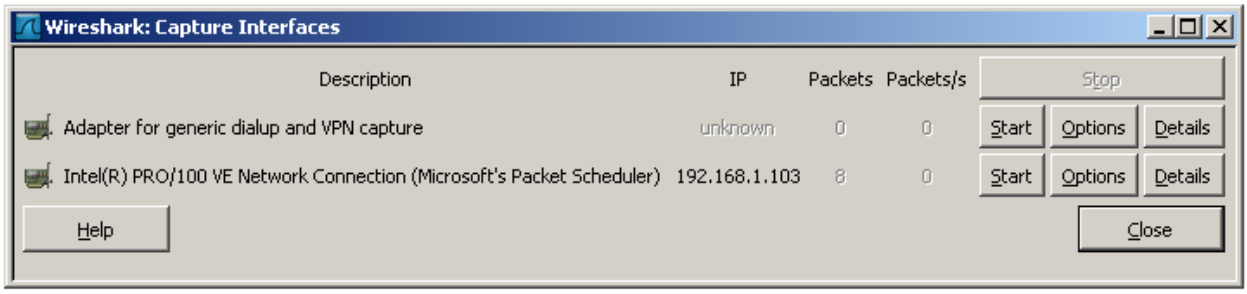
Step 2: Select an interface to use for capturing packets

a. Start the Wireshark application.

b. From the **Capture** menu, click **Interfaces**.



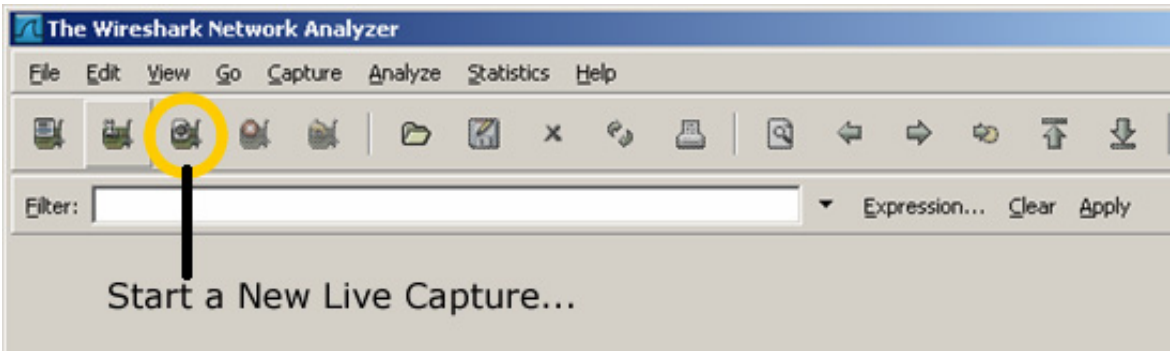
3) Click the **Start** button for the Ethernet interface (NIC) that you want to use to capture network traffic.



Step 3: Start a network capture

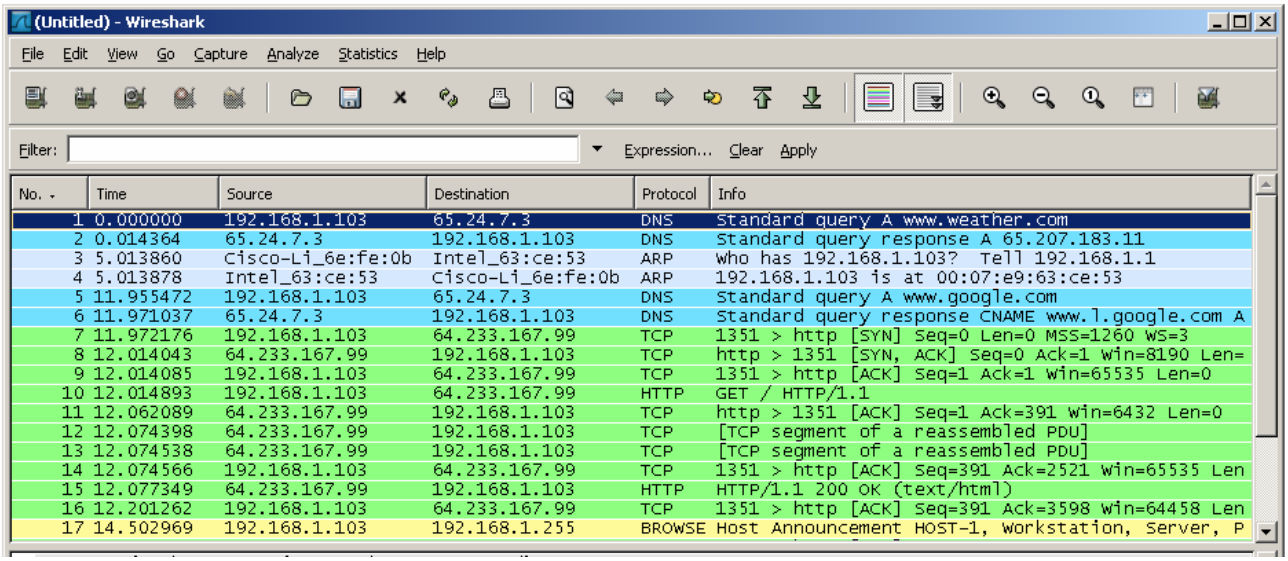
a. Scroll through the menus and view the toolbar on the Wireshark startup Interface.

b. Click the **New Live Capture** button and observe the information gathered by Wireshark. Allow the capture to continue for a few minutes so that you can observe the different types of traffic on the network.



Step 4: Analyze Web traffic information (optional)

a. If Internet connectivity is available, open a browser and go to www.google.com. Minimize the Google window and return to Wireshark. You should see captured traffic similar to that shown below. Locate the **Source**, **Destination**, and **Protocol** columns on the Wireshark display screen.



4) The connection to the Google server will start with a query to the DNS server to look up the server IP address. The destination server IP address will most likely start with 64.x.x.x. What is the source and destination of the first packet sent to the Google server?

_____

b. Open another browser window and go to the **ARIN Whois** database http://www.arin.net/whois/ or use another **whois** lookup tool and enter the IP address of the destination server. To what organization is this IP address assigned?

_____

c. What are the protocols used to establish the connection to the web server and deliver the web page to your local host? _____

d. What is the color used to highlight the traffic between your host and the Google web server?

_____

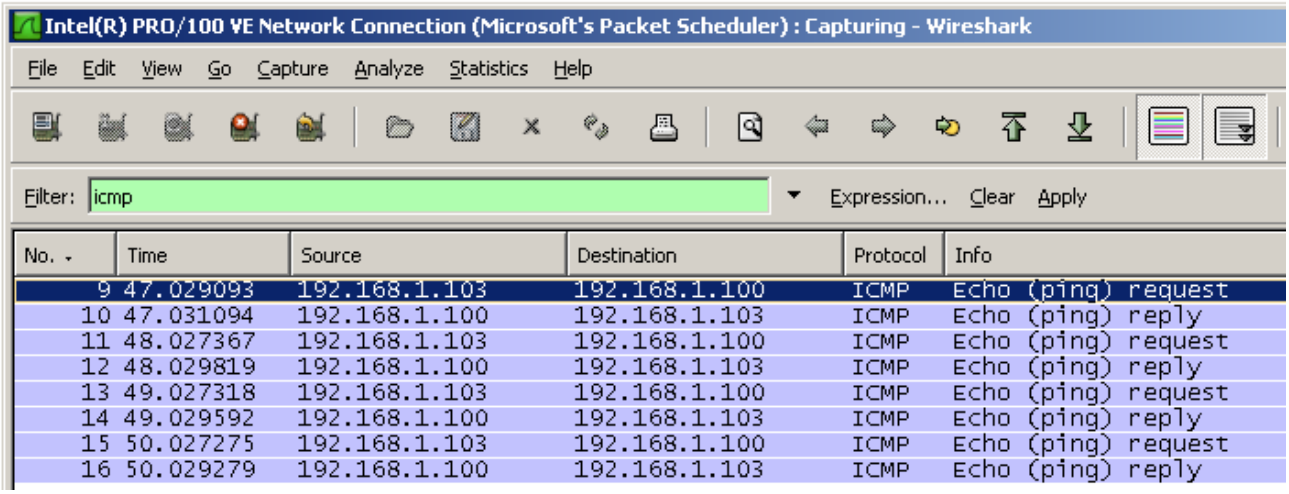
Step 5: Filter a network capture

a. Open a command prompt window by clicking **Start > All Programs > Run** and typing **cmd**. Alternatively, click **Start > All Programs > Accessories** and select **Command Prompt**.

b. Ping a host IP address on your local network and observe the Wireshark capture window. Scroll up and down the window in which the traffic is displayed. What types of protocols are in use?

_____

c. In the **Filter** text box, type **icmp** and click **Apply**. Internet Control Message Protocol (ICMP) is the protocol that **ping** uses to test network connectivity to another host.



d. When icmp is typed in the **Filter** text box, what kind of traffic is was displayed?

_____

e. Click the **Filter: Expression** button on the Wireshark window. Scroll down the list and view the filter possibilities there. Are TCP, HTTP, ARP and other protocols listed? _____

Step 6: Reflection

a. There are hundreds of filters listed in the Filter: Expression option. It may be possible that, in a large network, there would be enormous amounts and many different types of traffic. Which three filters in the long list do you think might be most useful to a network administrator?

_____

b. Is Wireshark a tool for out-of-band or in-band network monitoring? _____ Explain your answer.

_____

_____

Lab 8.4.2 Planning a Backup Solution

Objective

- Based on the business scenario, plan an appropriate backup solution.

Background / Preparation

You have been asked to plan and propose a backup solution for a small business customer of the ISP for which you work. The small business is concerned about losing valuable company data, and in the last three years, they have lost data due to hardware failure and user error. They want to ensure they have the quickest data recovery plan available built into the solution. The customer is willing to take on all local administrative tasks to monitor and manage the local backup system.

Current data requirements:

Server 1: 50GB

Server 2: 100GB

Server 3: 10GB

Based on their current growth in the amount of data, the company anticipates 10% growth in total volume of data each year.

The company has decided that they would like a backup solution that allows them to have 4 weeks worth of daily backups, and an additional 12 months worth of monthly archives. They would also like a solution that will last 5 years without outgrowing its capacity.

NOTE: You can assume that they are not able to purchase a tape autoloader or library system, which means that the capacity of the backup media needs to accommodate all the data in one unit.

Step 1: Choose the media and backup hardware

Based on the media types described in this course, use the Internet to identify a suitable media with the capacity that meets the requirements of the business. You are also required to investigate the cost of purchasing additional hardware, if required, and the price of the media. Also based on the history requirements, identify the number of backup media. Enter your recommendations in the table below.

NOTE: The company's normal business hours are Monday through Friday, 8:00 a.m. to 6:00 p.m., but employees can come in as early as 7:00 a.m. and stay until as late as 8:00 p.m. Therefore, the company has decided that backups cannot start until after 10:00 p.m. and must be completed before 6:00 a.m. The equipment and backup media selected must be fast enough to back up all data from all servers within this time period.

Equipment / Media	Price	Quantity

Step 2: Design a backup plan and procedure

Now that you have decided on the backup media, it is time to assemble the backup proposal and procedure for the company to manage their backup system. You need to decide what backup type is most appropriate for the business and how the business should schedule the swapping of the media. The business needs to have a procedure developed that is simple and easy to follow. Media needs to be labeled properly so the customer knows what is backed up on each day. Be sure to address the customer's needs in your proposed backup plan. Also identify any other open issues or questions that may still need to be asked to achieve a good solution for the customer. Describe your plan in the following steps:

a. Describe the equipment recommended and explain why you selected this equipment:

_____
_____
_____
_____
_____

b. Describe location of the equipment in the network and the network link speeds to the equipment:

_____
_____
_____
_____

c. Describe the backup media to be used and also explain why you selected this media:

_____
_____
_____
_____

d. Describe the backup schedule:

_____
_____
_____
_____

e. Describe the backup and restore procedure, including: what kind of backup (Normal, Differential, Incremental), how it will be tested, what kind of maintenance the equipment requires. How tapes will be labeled and where tapes that have been backed up will be stored. When backups need to be restored, what is the specific procedure for a file, a folder, a drive (use extra sheets it necessary)?

_____

_____

_____

_____

_____

_____

_____

Summary Lab 9.0.1 Putting it All Together

Objective(s)

- Create an IP addressing plan for a small network.
- Implement a network equipment upgrade
- Verify device configurations and network connectivity

Background / Preparation

In this activity, you will play the role of an onsite installation and support technician from an ISP. You receive a work order specifying your responsibilities which include analyzing the customer's existing network configuration and implementing a new configuration to improve network performance. You will use additional equipment as necessary and develop an IP subnetting scheme to address the customer's needs. On an earlier site visit, one of the ISP technicians had created a diagram of the customer's existing network as shown below.

The following equipment is required:

- ISP router with 2 Serial and one FastEthernet interface (preconfigured by instructor)
- Ethernet 2960 switch to connect to ISP router (preconfigured by instructor)
- Customer 1841 router (or other router with two FastEthernet interfaces and at least one Serial interface to connect to the ISP)
- Linksys WRT300N (or other Linksys that supports wireless)
- Ethernet 2960 switch to connect wired PCs
- Windows XP-based PC to act as wireless client (wireless NIC)
- Windows XP-based PC to act as wired client (Ethernet NIC)
- Cat 5 cabling as necessary
- Serial cabling as necessary
- ISP work order (in this lab)
- Device Configuration Checklist (in this lab)
- Network Equipment Installation Checklist (in this lab)
- Configuration Verification and Connectivity Checklist (in this lab)

Part A - Review the existing network and customer work order.

Step 1: You have received the following work order from your manager at the ISP.

Review the work order to get a general understanding of what is to be done for the customer.

ABC-XYZ-ISP Inc.

Official Work Order

Customer: AnyCompany1 or AnyCompany2 **Date:** _____

(Circle the customer name assigned by your instructor)

Address: 1234 Fifth Street, Anytown,

Customer Contact: Fred Pennypincher, Chief Financial Officer

Phone number: 123-456-7890

Description of work to be performed

Review the existing network and upgrade it by adding an 1841 router and standalone 2960 switch to supplement and offload the existing Linksys WRT300N. The new switch will support connections from wired clients on one subnet. The existing Linksys will support wireless clients on another subnet. Configure the 1841 as a DHCP server for the wired network and the Linksys which supports wireless users.

The wired and wireless client traffic from each subnet will be routed though the new 1841 customer router. The RIP v2 routing protocol is to be used between the 1841 and the ISP and the encapsulation on the WAN link between is PPP. The customer router must use a static address and the ISP router serial interface IP address it must communicate with is: _____

If your local network is connected to the ISP as AnyCompany1, the IP address of the ISP serial 0 interface is 10.100.1.5 /22.

If your local network is connected to the ISP as AnyCompany2, the IP address of the ISP serial 1 interface is 172.27.100.25 /22.

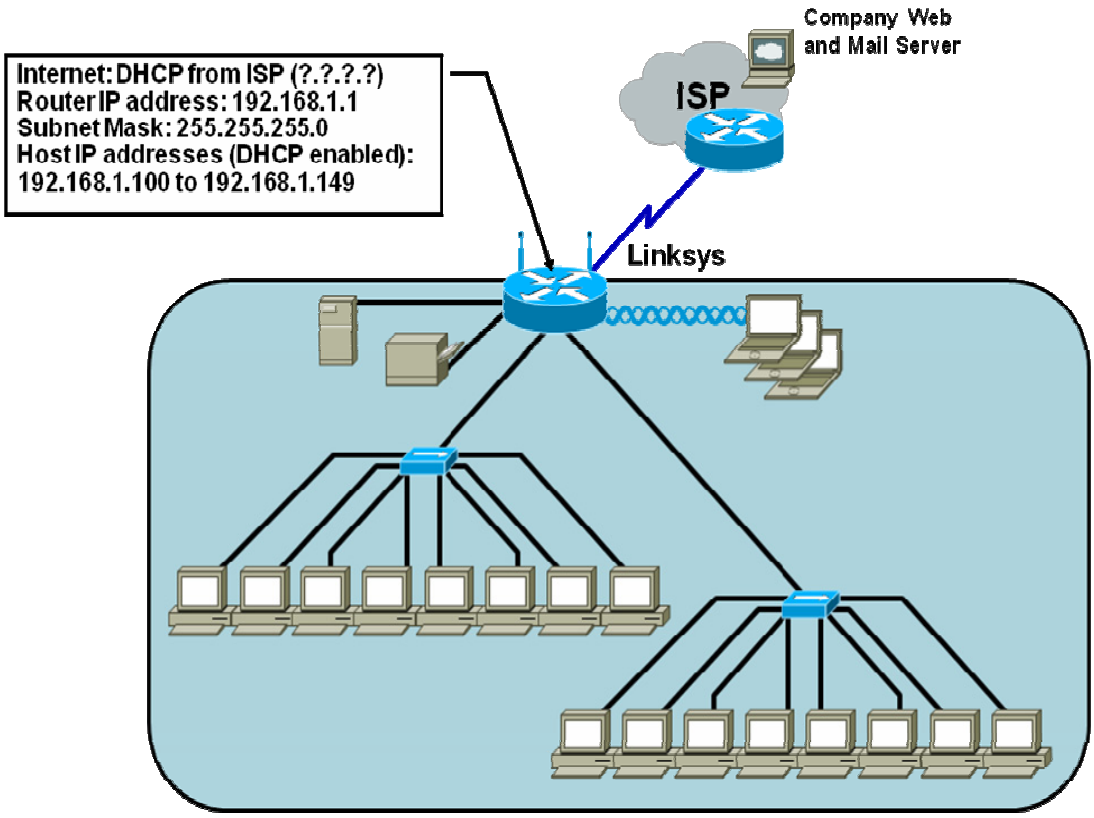
Assigned to:

Guy Netwiz

Approved by:

Bill Broadband, ISP Manager

Customer's Existing Network



Part B – Develop the subnet scheme.

The customer has been assigned an IP address and subnet mask: _____

If local network customer is AnyCompany1, use 192.168.111.0 /24.

If local network customer is AnyCompany2, use 192.168.222.0 /24.

Develop a subnet scheme using this address that will allow the customer network to support two subnets of up to 30 clients each, and allow for growth to as many as 6 subnets in the future.

The first subnet will be used for the wired clients. The second subnet will be used to assign an IP address to the Linksys external Internet interface. The internal wireless network clients will use the default IP addressing (network 192.168.1.0 /24) assigned by the Linksys. The Linksys will use NAT/PAT to convert internal wireless client addresses to the external address. The internal wireless clients will not require a subnet from the base address.

Step 1: Determine the number of hosts and subnets. (Points: ____of ____)

a. The largest subnet must be able to support 30 hosts. To support that many hosts, the number of host bits required is _____.

b. What is the minimum number of subnets required for the new network design that also allows for future growth? _____

c. How many host ID bits are reserved for the subnet ID to allow for this number of subnets with each subnet having 30 hosts? _____

d. What is the maximum possible number of subnets with this scheme? _____

Step 2: Calculate the custom subnet mask. (Points: ____of ____)

a. Now that the number of subnet ID bits is known, the subnet mask can be calculated. A class C network has a default subnet mask of 24 bits, or 255.255.255.0. What will the custom subnet mask be?

b. The custom subnet mask for this network will be _____._____._____._____, or /_____.

Step 3: Identify subnet and host IP addresses. (Points: ____of ____)

a. Now that the subnet mask is identified, the network addressing scheme can be created. The addressing scheme includes the subnet numbers, the subnet broadcast address, and the range of IP addresses assignable to hosts.

b. Complete the table showing all the possible subnets for the 192.168.111.0 network (If you are working with AnyCompany1) or 192.168.222.0 network (If you are working with AnyCompany2).

Subnet	Subnet Address	Host IP Address Range	Broadcast Address

Part C – Document network device interfaces and physical topology.

Step 1: Document the 1841 interfaces and Host IP addresses. (Points: ____of ____)

Fill in the following table with the IP addresses, subnet masks and connection information for the customer router interfaces. If an interface is not used enter N/A. This information will be used in configuring the customer router. If you are using a router other than an 1841, use the interface chart at the end of the lab to determine the proper interface designations.

Interface (1841)	IP Address / subnet mask	Connects to device / interface	Connects to device IP Address (if applicable)
Serial 0/0/0			
Serial 0/0/1			
Fa 0/0			
Fa 0/1			

Step 2: Document the Linksys interfaces and host IP addresses. (Points: ____of ____)

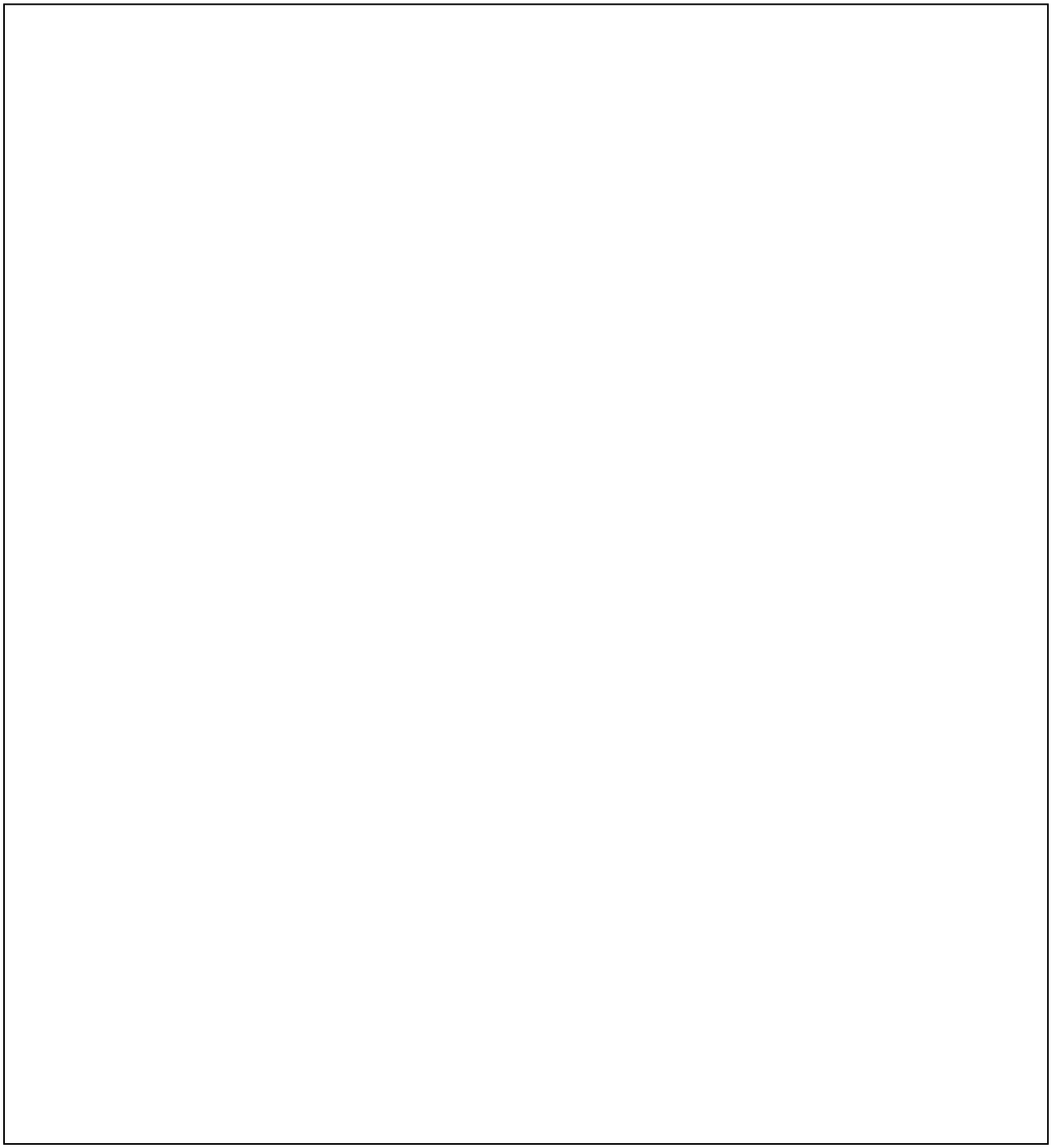
Fill in the following table with the IP addresses, subnet masks and connection information for the Linksys interfaces.

Note: The Linksys should be reset to its factory default setting and should not be configured, except for changing the SSID.

Interface (Linksys)	IP Address / subnet mask	Connects to device / interface	Connects to device IP Address (if applicable)
Internet Interface (external address)			
LAN gateway (internal address)			
DHCP Wireless Hosts address range			

Step 3: Diagram the upgraded network. (Points: ____of ____)

In the space provided here, draw a physical network diagram, showing all network devices, PCs and cabling. Identify all devices and interfaces according to the interface chart and indicate the IP address and subnet mask (using /xx format) for each interface, based on the entries from the previous steps.



Part D – Configure devices and verify default settings.

Step 1: Verify default settings for the 1841 customer router.

a. Connect to the customer router and verify that is in the factory default state.

b. If using SDM to configure basic settings, use the Reset to Factory Defaults option from the SDM GUI main menu. Also verify that your router has SDM version 2.4 or later installed. If not, contact your instructor.

c. If using IOS CLI to configure the router, erase the startup-config and issue the reload command from privileged mode.

NOTE: If the startup-config is erased in an SDM router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic config. Contact your instructor if this is the case.

Step 2: Configure the 1841 customer router. (Points: ____of ____)

a. Use the following checklist to assist in configuring the 1841 customer router. Check off the configuration items as you complete them. Note that some of the basic router settings can be configured using SDM if available.

b. Display the running-config of the router and save it as a file for reference.

Device Configuration Checklist

Device Manuf. / Model Number: _____ **IOS version**: _____

	Configuration Item	Configuration value	Notes / IOS Commands or SDM used
	Configure the router host name	AnyCompany1 or AnyCompany2	
	Configure passwords	Console: cisco Enable: cisco Enable Secret: class VTY terminals: cisco	
	Configure FastEthernet interface 0/0	IP Addr: _____ SN mask: _____	
	Configure FastEthernet interface 0/1	IP Addr: _____ SN mask: _____	
	Configure the WAN interface Serial 0/0/0 (ISP provides clock rate, encapsulation PPP)	IP Addr: _____ SN mask: _____	
	Configure DHCP server for internal networks (wired and linksys wireless pools)	Subnet 1: _____ Subnet 2: _____	
	Configure Static route to the wireless network		
	Configure a default route to the ISP router		
	Configure RIP version 2 to advertise the customer networks	Net: _____ Net: _____ Net: _____	
	Display the running-config and verify all settings		
	Save running-config to startup-config		

Step 3: Verify default settings for the Linksys and set the SSID.

a. Log in to the Linksys and verify that it is in the factory default state. Use the factory default of no user ID and password of admin. The router internal IP address should be set to 192.168.1.1 and a subnet mask of 255.255.255.0. The DHCP address range should be 192.168.1.100 through 192.168.1.149. All security settings should be default, with no MAC filtering etc.

b. If necessary, reset the ISR using the **Administration** tab and the **Factory Defaults** option.

c. Change the default Service Set Identifier (SSID) of linksys to AnyCompany1 (or AnyCopmany2) and ensure that it is broadcast.

Step 4: Verify default settings for the 2960 switch.

Log in to the switch and verify that it is in the factory default state. Use IOS CLI to reset the switch by deleting vlan.dat, erasing the startup-config and issuing the reload command from privileged mode. It may be necessary to power cycle the switch for the changes to take effect.

Step 5: Verify host PCs are DHCP clients.

Use the **Control Panel > Network Connections** option to verify that both the wired and wireless host PCs are set to obtain their IP addresses automatically via DHCP.

Part E – Connect network devices and verify connectivity.

Step 1: Connect the network devices. (Points: ____of ____)

Use the following checklist to assist in connecting network devices using the proper cables. Check off the installation items as you complete them.

Network Equipment Installation Checklist

✓	Devices connected	From Device /Interface	To Device /Interface	Cable type
	Connect the Linksys to the 1841.			
	Connect the 1841 to the ISP router			
	Connect the 1841 to the switch			
	Connect wired PC to switch			
	Connect wireless PC to Linksys SSID entered in Part D Step 2			

Step 2: Verify device configurations and network connectivity. (Points: ____of ____)

Use the following checklist to verify the IP configuration of each host and test network connectivity. You will also display the various running-configs and routing tables. Check off the items as you complete them.

Configuration Verification and Connectivity Checklist

	Verification Item	Record results here
	From command prompt of wired PC, display the IP address, subnet mask and default gateway.	
	From command prompt of wireless PC, display the IP address, subnet mask and default gateway.	
	Login to Linksys GUI from wireless host and record the LAN IP address and subnet mask, the Internet IP address and subnet mask and default gateway	
	Ping from the wired host to 1841 default gateway	
	Ping from the wired host to ISP S0/0 interface	
	Ping from the wired host to ISP Lo0 interface	
	Ping from the wireless host to 1841 default gateway	
	Ping from the wireless host to ISP S0/0 interface	
	Ping from the wireless host to ISP Lo0 interface	
	Display the IP routing table for the customer router. What routes are known and how were they learned?	
	Capture the running–config from the customer 1841 router in a text file on the desktop to show to the instructor. Name the file using your initials.	

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
800 (806)	Ethernet 0 (E0)	Ethernet 1 (E1)		
1600	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
1700	Fast Ethernet 0 (FA0)	Fast Ethernet 1 (FA1)	Serial 0 (S0)	Serial 1 (S1)
1800	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2500	Ethernet 0 (E0)	Ethernet 1 (E1)	Serial 0 (S0)	Serial 1 (S1)
2600	Fast Ethernet 0/0 (FA0/0)	Fast Ethernet 0/1 (FA0/1)	Serial 0/0 (S0/0)	Serial 0/1 (S0/1)

NOTE: In order to find out exactly how the router is configured, look at the interfaces. Doing this will identify the type of router as well as how many interfaces the router has. There is no way to effectively list all of the combinations of configurations for each router class. What is provided are the identifiers for the possible combinations of interfaces in the device. This interface chart does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in IOS command to represent the interface.