Cisco | Networking Academy®
Mind Wide Open™

CCNA Discovery 4.1.3

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:

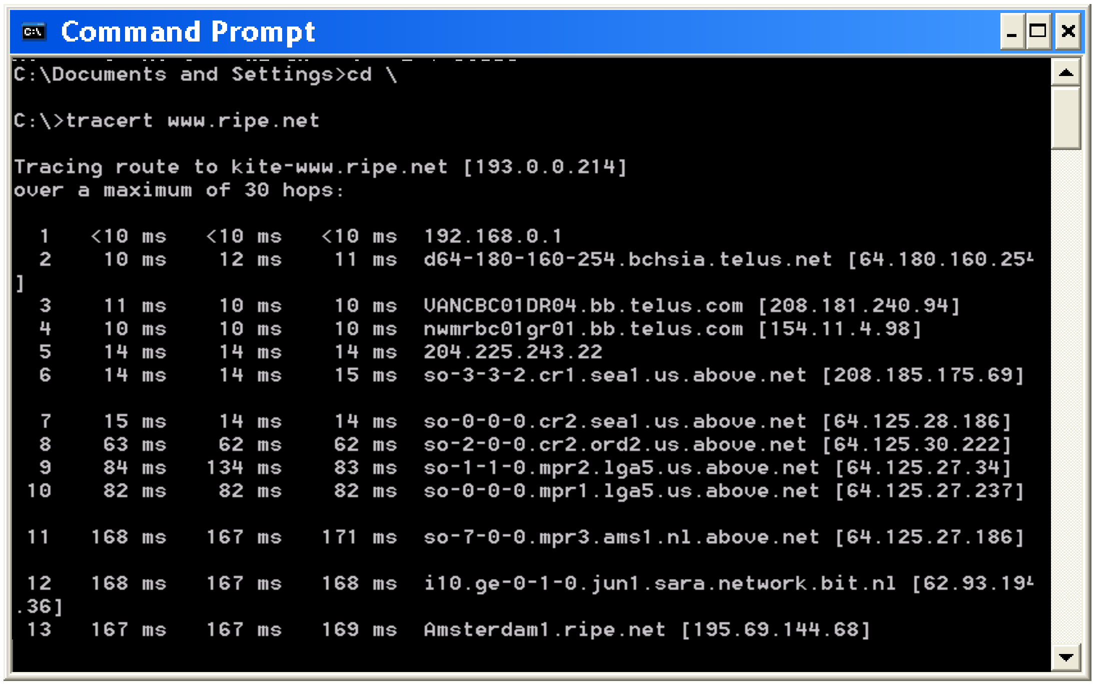
- Host computer with the Windows operating system
- Access to the command prompt
- Internet connection
- Routes Traced worksheet for each destination URL. The worksheet is attached to this lab. Each student completes their own worksheets and gives them to the instructor.
- Global Connectivity Map, which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



```
C:\Documents and Settings>cd \

C:\>tracert www.ripe.net

Tracing route to kite-www.ripe.net [193.0.0.214]
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  192.168.0.1
  2    10 ms    12 ms    11 ms  d64-180-160-254.bchsia.telus.net [64.180.160.254
]
  3    11 ms    10 ms    10 ms  VANCBC01DR04.bb.telus.com [208.181.240.94]
  4    10 ms    10 ms    10 ms  nwmrbc01gr01.bb.telus.com [154.11.4.98]
  5    14 ms    14 ms    14 ms  204.225.243.22
  6    14 ms    14 ms    15 ms  so-3-3-2.cr1.sea1.us.above.net [208.185.175.69]

  7    15 ms    14 ms    14 ms  so-0-0-0.cr2.sea1.us.above.net [64.125.28.186]
  8    63 ms    62 ms    62 ms  so-2-0-0.cr2.ord2.us.above.net [64.125.30.222]
  9    84 ms   134 ms    83 ms  so-1-1-0.mpr2.lga5.us.above.net [64.125.27.34]
 10    82 ms    82 ms    82 ms  so-0-0-0.mpr1.lga5.us.above.net [64.125.27.237]

 11   168 ms   167 ms   171 ms  so-7-0-0.mpr3.ams1.nl.above.net [64.125.27.186]

 12   168 ms   167 ms   168 ms  i10.ge-0-1-0.jun1.sara.network.bit.nl [62.93.194
.36]
 13   167 ms   167 ms   169 ms  Amsterdam1.ripe.net [195.69.144.68]
```

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**.

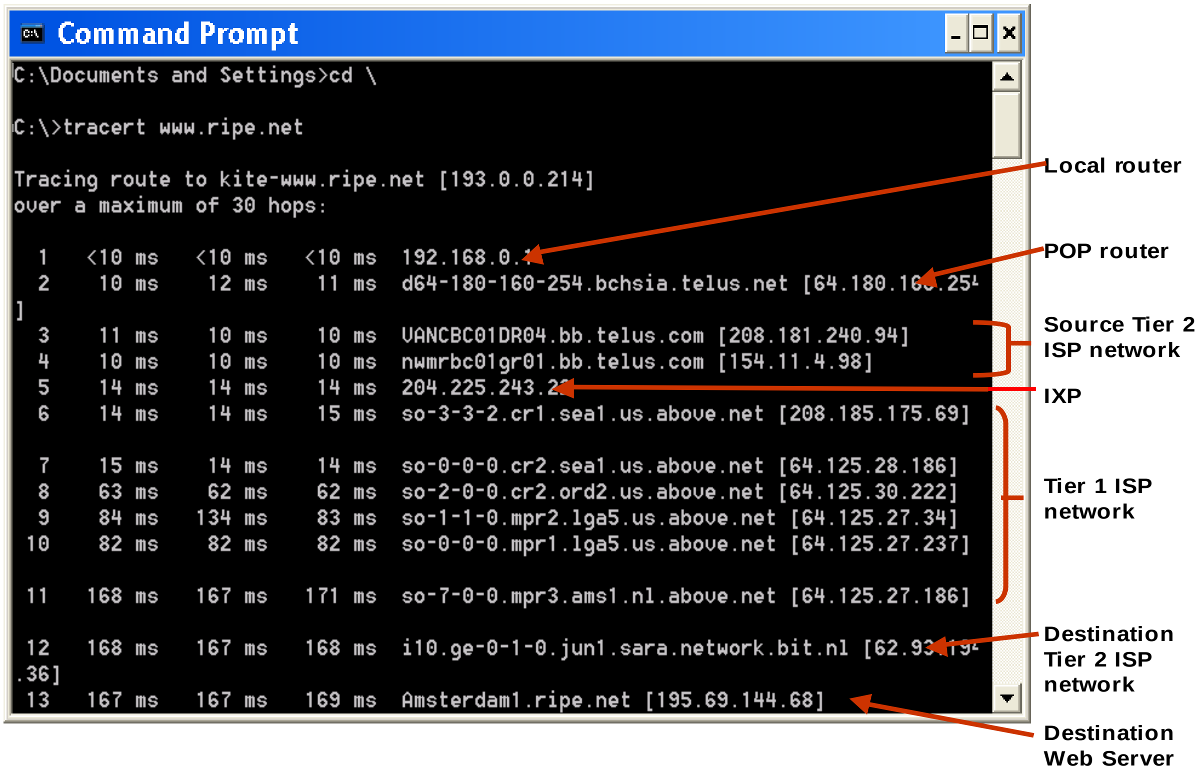
5) Choose **File > Save As** and save the Notepad file to your desktop as tracert1.txt.

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.



```
C:\Documents and Settings>cd \

C:\>tracert www.ripe.net

Tracing route to kite-www.ripe.net [193.0.0.214]
over a maximum of 30 hops:

  1    <10 ms   <10 ms   <10 ms  192.168.0.1
  2     10 ms    12 ms    11 ms  d64-180-160-254.bchsia.telus.net [64.180.160.254
]
  3     11 ms    10 ms    10 ms  VANCBC01DR04.bb.telus.com [208.181.240.94]
  4     10 ms    10 ms    10 ms  nwmrbc01gr01.bb.telus.com [154.11.4.98]
  5     14 ms    14 ms    14 ms  204.225.243.22
  6     14 ms    14 ms    15 ms  so-3-3-2.cr1.sea1.us.above.net [208.185.175.69]

  7     15 ms    14 ms    14 ms  so-0-0-0.cr2.sea1.us.above.net [64.125.28.186]
  8     63 ms    62 ms    62 ms  so-2-0-0.cr2.ord2.us.above.net [64.125.30.222]
  9     84 ms   134 ms    83 ms  so-1-1-0.mpr2.lga5.us.above.net [64.125.27.34]
 10     82 ms    82 ms    82 ms  so-0-0-0.mpr1.lga5.us.above.net [64.125.27.237]

 11    168 ms   167 ms   171 ms  so-7-0-0.mpr3.ams1.nl.above.net [64.125.27.186]

 12    168 ms   167 ms   168 ms  i10.ge-0-1-0.jun1.sara.network.bit.nl [62.93.194
.36]
 13    167 ms   167 ms   169 ms  Amsterdam1.ripe.net [195.69.144.68]
```

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

CCNA Discovery
Working at a Small-to-Medium Business or ISP

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 AnyCompany 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?

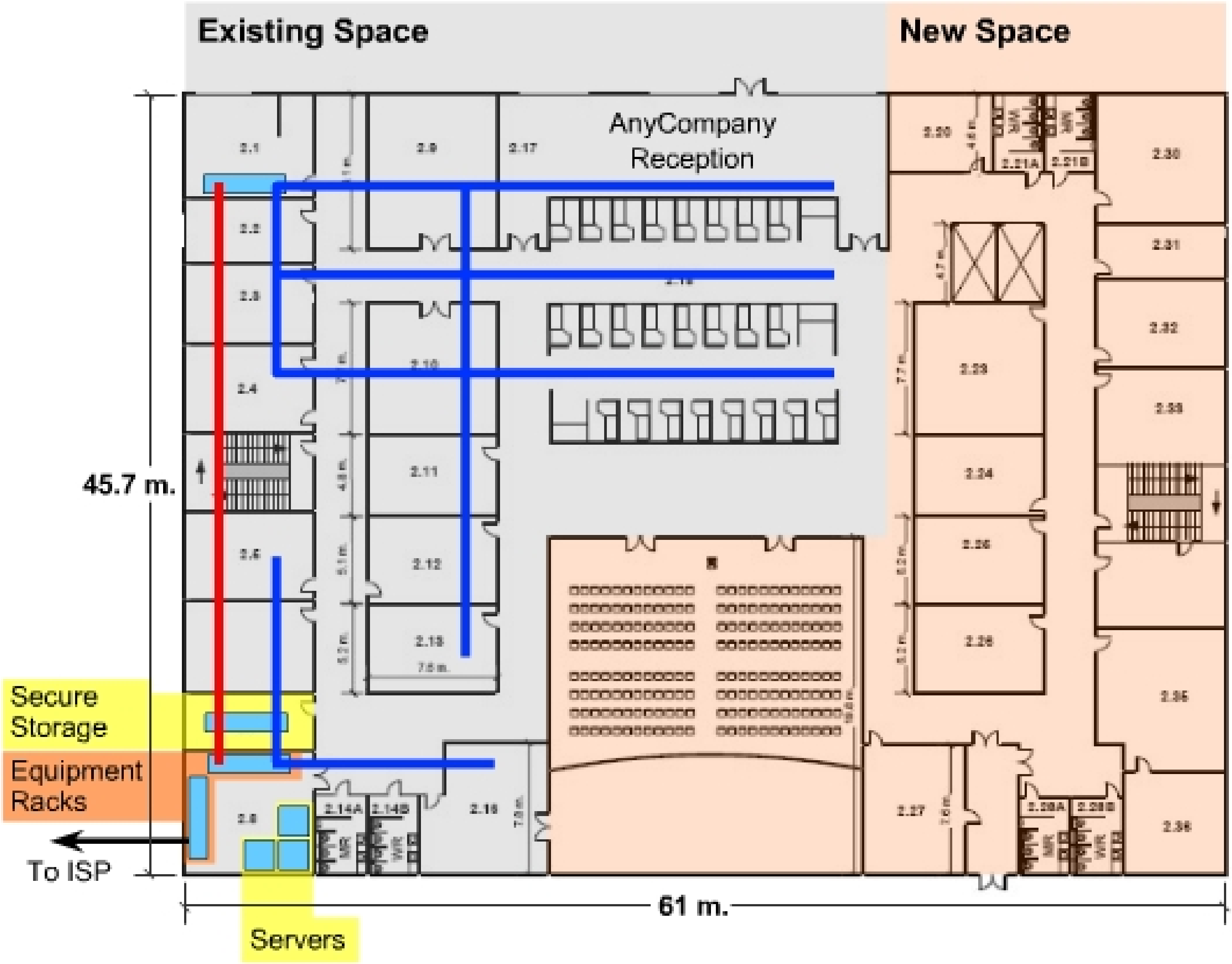
____

____

____

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

____


Existing Space
New Space
AnyCompany
Reception
2.1
2.2
2.3
2.4
2.5
2.8
2.9
2.10
2.11
2.12
2.13
2.14A
2.14B
2.16
2.17
2.20
2.21A
2.21B
2.23
2.24
2.25
2.26
2.27
2.28A
2.28B
2.30
2.31
2.32
2.33
2.35
2.36
MR
WR
7.6 m.
45.7 m.
61 m.
Secure
Storage
Equipment
Racks
To ISP
Servers

Lab 4.1.5 Subnetting a Network

Objective

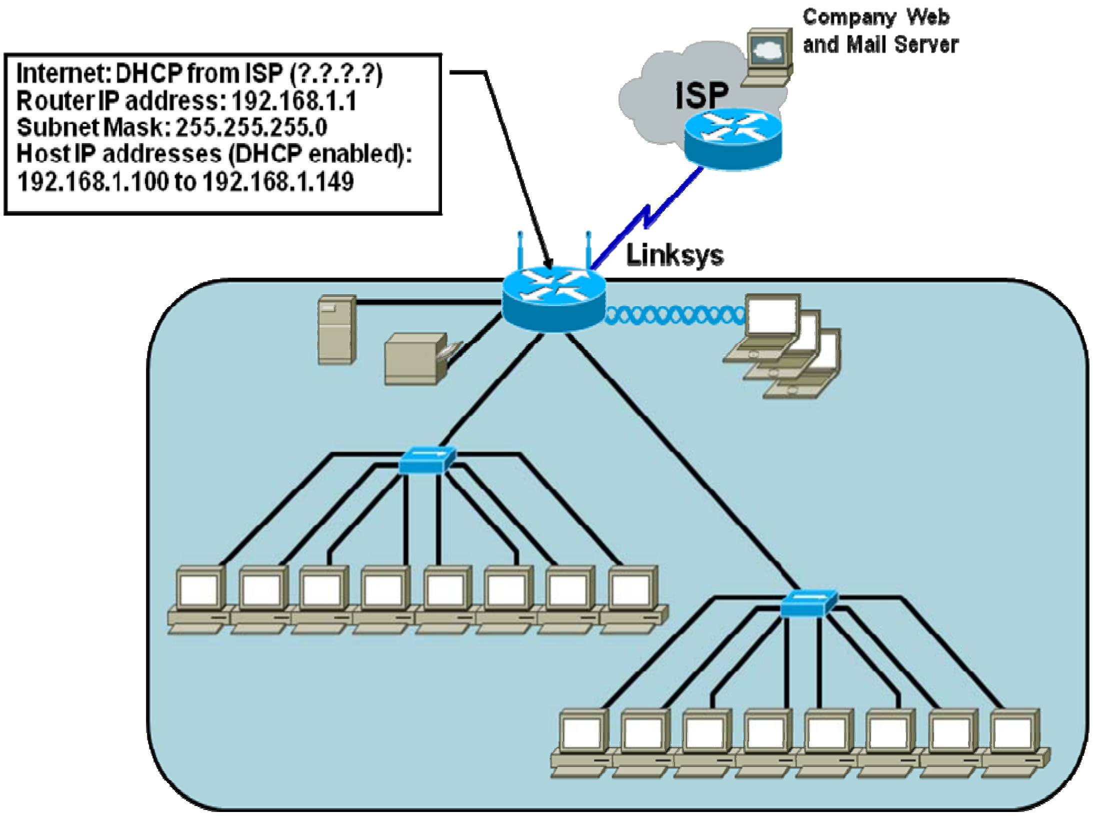
- Create an IP addressing plan for a small network.

Background / Preparation

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

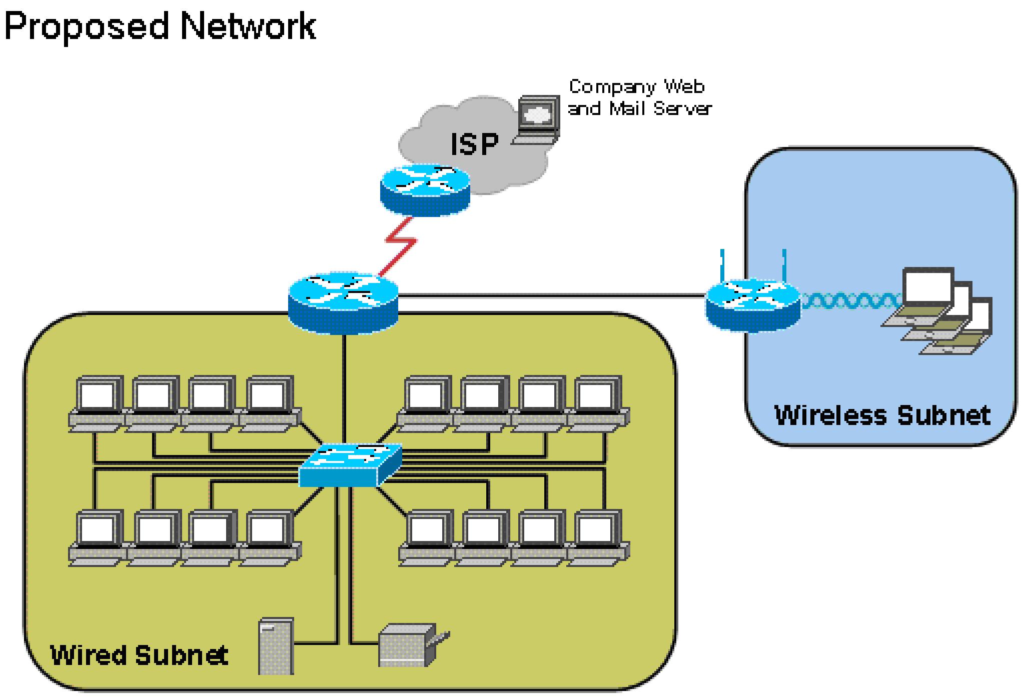
A customer has called the ISP complaining of e-mail problems and occasional poor Internet performance. On an earlier site visit, the technician had created diagram of the customer's existing network shown here.

Existing Network

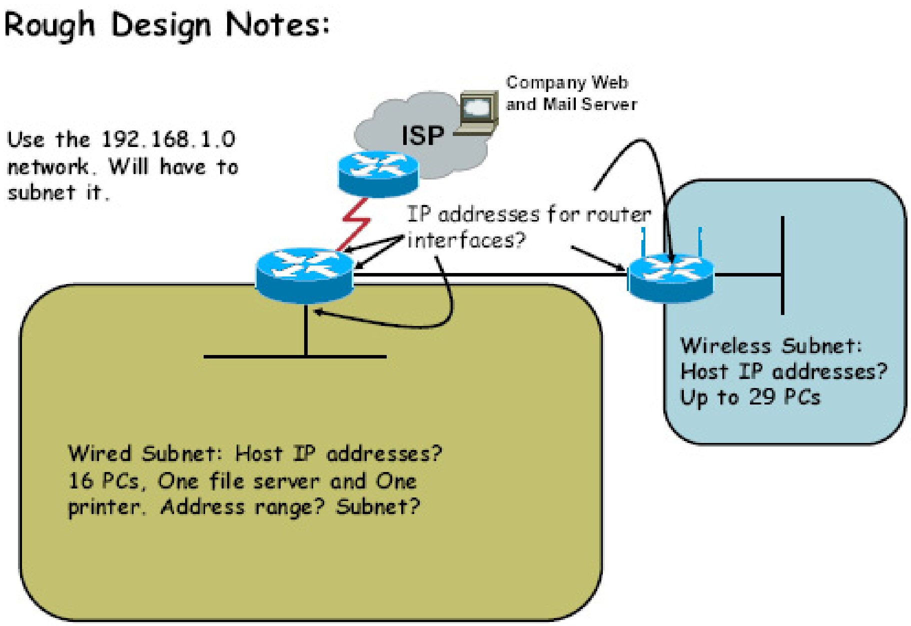


Internet: DHCP from ISP (?.?.?.?)
Router IP address: 192.168.1.1
Subnet Mask: 255.255.255.0
Host IP addresses (DHCP enabled):
192.168.1.100 to 192.168.1.149

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.


Rough Design Notes:
Company Web and Mail Server
ISP
Use the 192.168.1.0 network. Will have to subnet it.
IP addresses for router interfaces?
Wireless Subnet: Host IP addresses? Up to 29 PCs
Wired Subnet: Host IP addresses? 16 PCs, One file server and One printer. Address range? Subnet?

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.

____

____

____

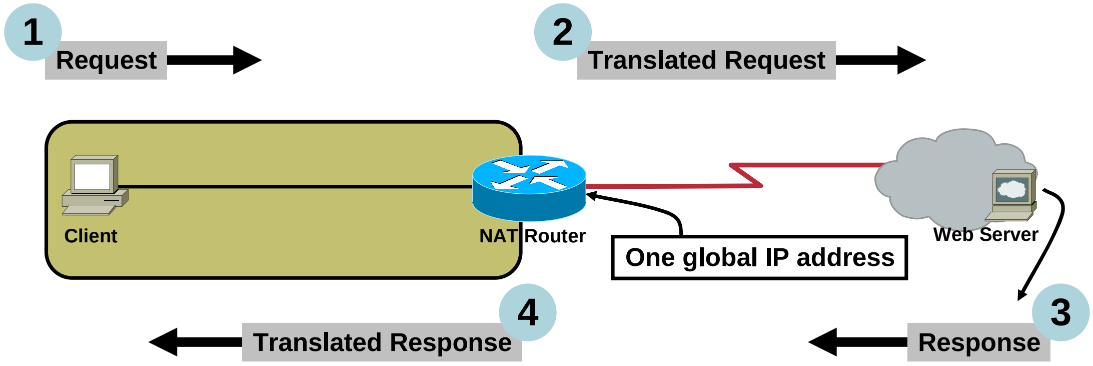
____

____

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

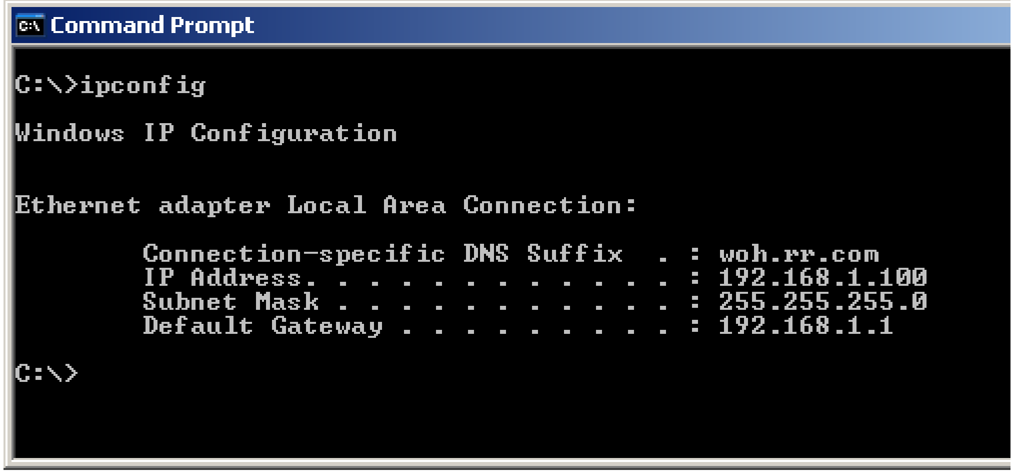
Port address translation (PAT) is a form of network address translation (NAT). With PAT, the router translates multiple internal (usually private) addresses to a single public IP address on an interface that is connected to the Internet. Port numbers are used, in combination with IP addresses, to keep 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.



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : woh.rr.com
        IP Address. . . . . . . . . . . . : 192.168.1.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>
```

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? ____

____

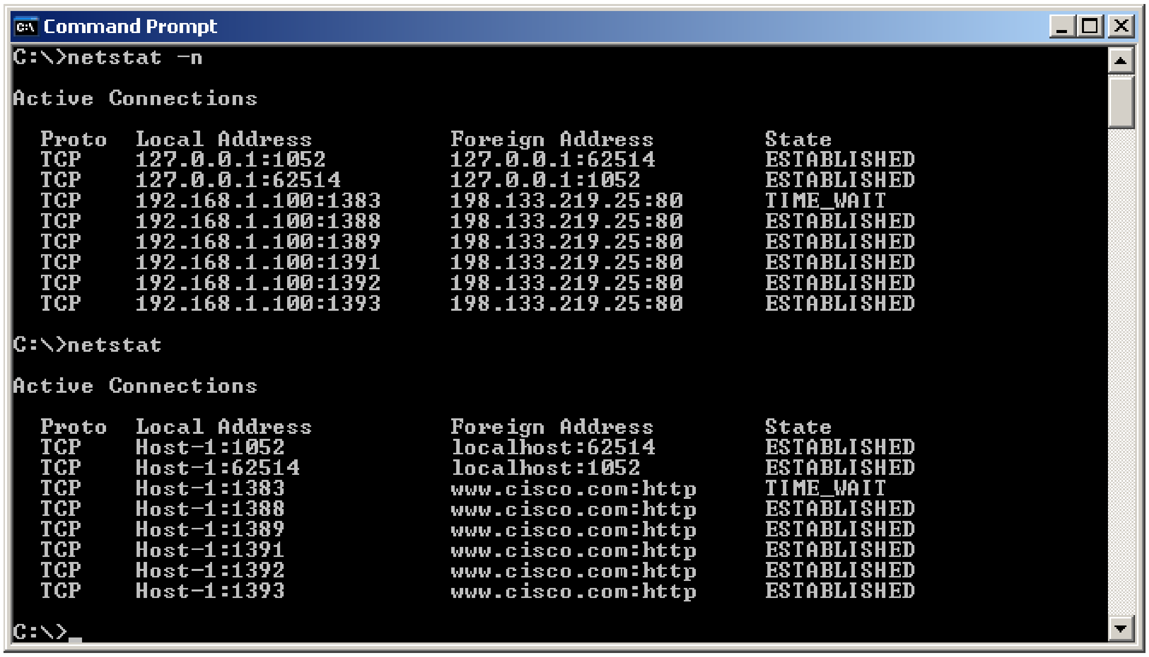
Step 4: Display active network connections

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.



```
C:\>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    127.0.0.1:1052         127.0.0.1:62514        ESTABLISHED
  TCP    127.0.0.1:62514        127.0.0.1:1052         ESTABLISHED
  TCP    192.168.1.100:1383     198.133.219.25:80      TIME_WAIT
  TCP    192.168.1.100:1388     198.133.219.25:80      ESTABLISHED
  TCP    192.168.1.100:1389     198.133.219.25:80      ESTABLISHED
  TCP    192.168.1.100:1391     198.133.219.25:80      ESTABLISHED
  TCP    192.168.1.100:1392     198.133.219.25:80      ESTABLISHED
  TCP    192.168.1.100:1393     198.133.219.25:80      ESTABLISHED

C:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    Host-1:1052            localhost:62514        ESTABLISHED
  TCP    Host-1:62514           localhost:1052         ESTABLISHED
  TCP    Host-1:1383            www.cisco.com:http     TIME_WAIT
  TCP    Host-1:1388            www.cisco.com:http     ESTABLISHED
  TCP    Host-1:1389            www.cisco.com:http     ESTABLISHED
  TCP    Host-1:1391            www.cisco.com:http     ESTABLISHED
  TCP    Host-1:1392            www.cisco.com:http     ESTABLISHED
  TCP    Host-1:1393            www.cisco.com:http     ESTABLISHED

C:\>_
```

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

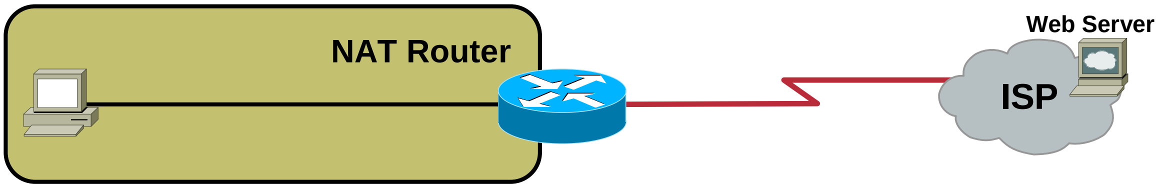
Use the information recorded in steps 2 and 4 and the topology diagram shown at the beginning of the lab to fill in the Address:Port columns.

1 Request →

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

2 Translated Request →

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



4 ← Translated Response

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

3 ← Response

	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 5.1.3 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 and observe the router startup sequence.
- Display router configuration information using the **show running-config** and **show startup-config** commands and restart the router using the **reload** command.
- Display router system, Cisco IOS software and configuration register information using the **show version** command.

Background / Preparation

Part 1 of this lab focuses on the initial setup of the Cisco 1841 ISR. Part 2 focuses on using **show** commands to display internal router system, Cisco IOS software, and configuration information. 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

Part 1: Initial Router Setup and Startup

Step 1: Position the router and connect the ground wire (optional).

Note: This step 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.

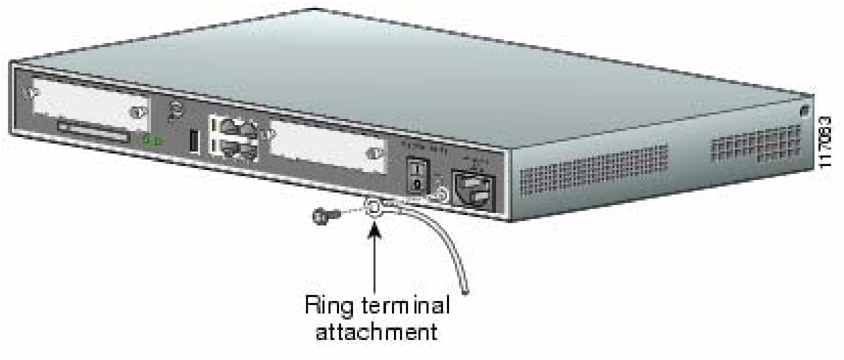
b. Connect the chassis to a reliable earth ground using a ring terminal and 14 AWG (2 mm) wire using these steps.

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. 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 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. Just read through it to become familiar with the process.

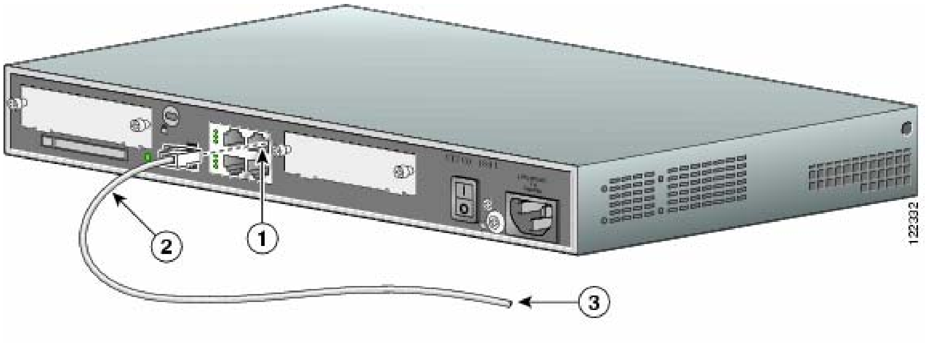
a. Attach a grounding strap to your wrist to avoid electroshock damage to the card. Seat the external CompactFlash memory card properly into the slot. This step depends on the type of router. Not all routers have flash cards.

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. 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 RJ-45 console port	2. Light-blue RJ-45-to-DB-9 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. Start 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.

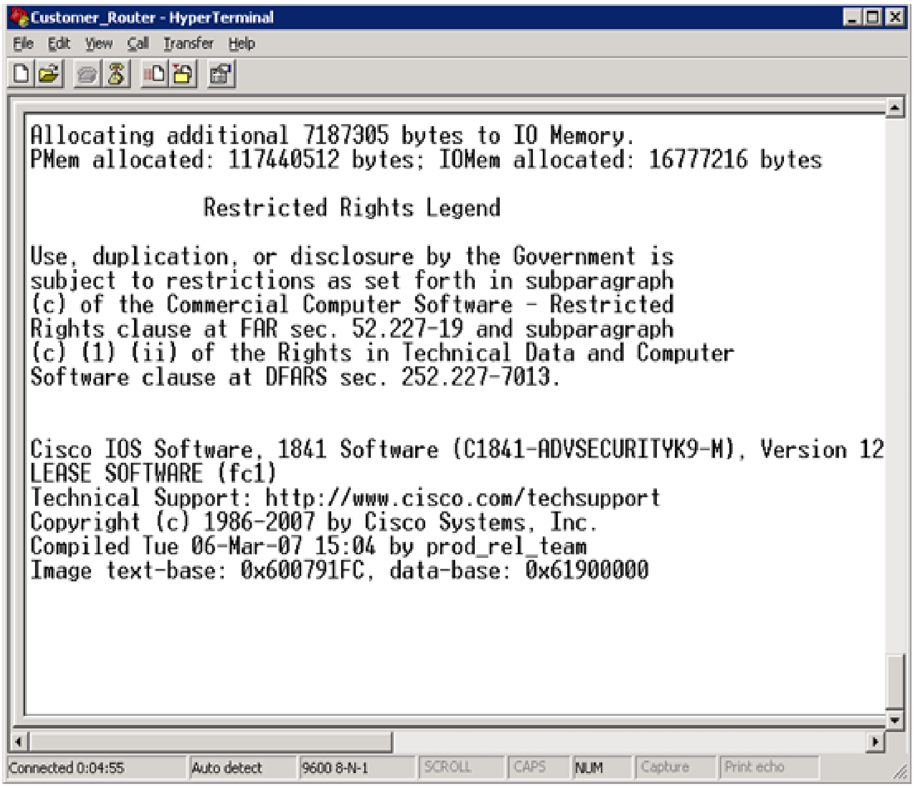
d. Configure the terminal emulation parameters as follows:

- 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 router is using. Can you find these example startup messages in the following figure?



```
Allocating additional 7187305 bytes to IO Memory.
PMem allocated: 117440512 bytes; IOMem allocated: 16777216 bytes

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.


Cisco IOS Software, 1841 Software (C1841-ADVSECURITYK9-M), Version 12
LEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Tue 06-Mar-07 15:04 by prod_rel_team
Image text-base: 0x600791FC, data-base: 0x61900000
```

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 a steady green light, and the fans operate. When the router is finished starting up, the following system messages appear in the terminal emulation window:

```
             --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]:

Press RETURN to get started!
```

d. After pressing **Return** (Enter) to get started, several system messages regarding the interface and line status appear. If the router is in its default configuration, the user mode prompt **Router>** is displayed.

   Note: It may be necessary to press **Enter** after the interface status messages are displayed.

Step 5: Troubleshoot a non-working router.

If the SYS PWR LED does not blink green, the fans do not operate, and the correct system messages do 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 does not power on, ask the instructor for assistance.

Part 2: Displaying Router Information Using show Commands

Step 1: Display the router running configuration.

a. From the router user prompt, enter privileged mode using the **enable** command, and then issue the **show running-config** command to see the current router configuration in RAM.

   If the router is in default configuration, the output is similar to that shown below. The default host name is Router, and none of the interfaces have IP addresses. This 1841 router has two built-in Fast Ethernet interfaces (0/0 and 0/1) and two serial interfaces (Serial0/0/0 and Serial0/0/1) if the serial card is installed in Slot 0. If the serial card is installed in Slot 1, the serial interfaces are listed as Serial0/1/0 and Serial0/1/1. This router also has a Fast Ethernet switch module installed with four ports (Fast Ethernet 0/1/0, 0/1/1, 0/1/2, and 0/1/3). In the default configuration, all interfaces are shutdown. In addition, there are no passwords set.

```
Router>enable
Router#show running-config
Building configuration...
Current configuration : 809 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
interface FastEthernet0/1/1
interface FastEthernet0/1/2
interface FastEthernet0/1/3
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
```

```
interface Vlan1
 no ip address
!
ip http server
no ip http secure-server
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

b. From the router privileged mode prompt, issue the **configure terminal** command to enter configuration mode. Change the router name using the **hostname** command, and then end configuration mode with the **end** command.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname Netacad
Netacad(config)#end
Netacad#
*Feb  8 01:13:00.999: %SYS-5-CONFIG_I: Configured from console by
console
Netacad#
```

c. What is the router prompt now? ____________________

d. From the router privileged mode prompt, issue the **show running-config** command again. How does the output differ from the first time you issued this command?

____

Step 2: Display the router startup configuration.

From the router privileged mode prompt, issue the **show startup-config** command to see the startup file stored in NVRAM. Is the output from this command the same as that from the **show running-config** command issued in Step 1d?

____

```
Router#show startup-config
```

Step 3: Save the running-config to the startup-config.

When the router is booted up, the startup-config file is loaded into router RAM and becomes the running-config file. Changes made to the running-config take effect immediately, but do not affect the startup-config. To make running-config changes permanent, they must be copied to the startup-config using the **copy running-config startup-config** command.

a. From the router privileged mode prompt, issue the **copy running-config startup-config** command to make the changes permanent. When prompted for the destination filename, press **Enter** to accept the default name of startup-config.

```
Netacad#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Netacad#
```

b. From the router privileged mode prompt, issue the **show startup-config** command again. Is the output from this command the same as that from the **show running-config** command issued in Step 1d? ____

c. To restart the router, from the router privileged mode prompt, issue the **reload** command. This performs a software restart and loads the startup-config file from NVRAM. What is the router prompt now? ____________________________

Step 4: Display the router system information using the show version command.

The **show version** command displays useful information about the router internal components, including the amount of RAM, Cisco IOS software version, the number and type of interfaces installed, and the configuration register, which controls how the router boots up. By default, the config register is set to hexadecimal 2102 (0x2102), which causes the router to load the operating system (Cisco IOS) from flash memory.

The information displayed by the **show version** command is displayed as part of router bootup. The output from the 1841 router is shown below. Your output may vary, depending on the router model, Cisco IOS software version, and internal components installed.

a. From the router privileged mode prompt, issue the **show version** command.

```
Netacad#show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

ROM: System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)

Netacad uptime is 55 minutes
System returned to ROM by reload at 00:35:23 UTC Fri Feb 8 2008
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FTX1111W0QF
6 FastEthernet interfaces
2 Serial(sync/async) interfaces
1 Virtual Private Network (VPN) Module
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
```

```
62720K bytes of ATA CompactFlash (Read/Write)

Configuration register is 0x2102
```

b. Using the output from the **show version** command, answer the following questions.

1. What is the Cisco IOS software version number? ______________

2. How long has the router been up (uptime)? ______________

3. What is the name of the system image file? ___________________________________

4. How many and what types of interfaces does this router have? ________________________

____

5. How many bytes of NVRAM does the router have? _______________

6. How many bytes of flash (RAM) memory does the router have? _______________

7. What is the configuration register setting? _______________

Step 5: Reflection

a. Is there anything about the router setup procedure that is risky?

____

____

b. Why does 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

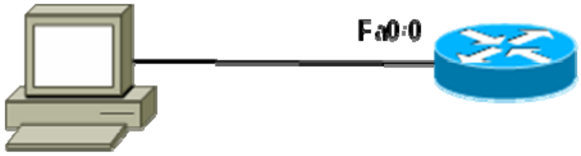
4) 3

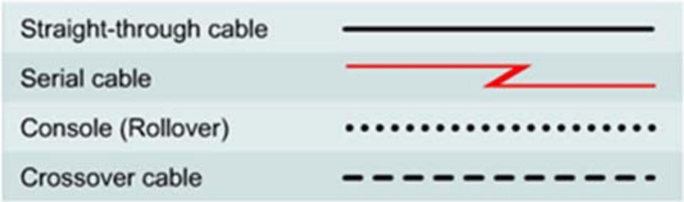
d. Why might you want to use the **show version** command?

____

____

Lab 5.2.3 Configuring an ISR with SDM Express





Straight-through cable	────────
Serial cable	──Z──
Console (Rollover)	••••••••••••
Crossover cable	– – – – – – –

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.

To get access to the SDM express application the instructor needs to logon to cisco.com with a CCO account. If you do not have a CCO account go to http://www.cisco.com/cgi-bin/login Under "Not Registered" select "Register now" to create an account.

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.

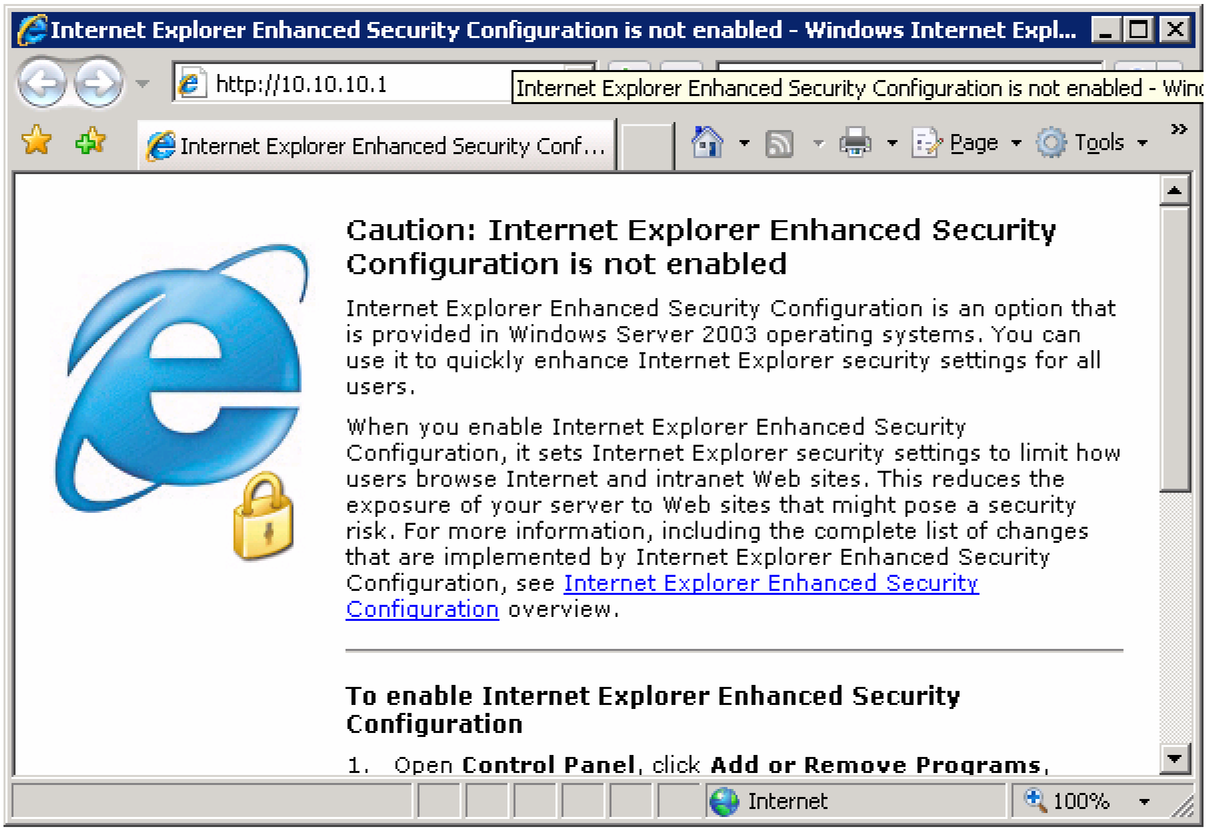
NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

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.


Internet Explorer Enhanced Security Configuration is not enabled - Windows Internet Expl...
http://10.10.10.1
Internet Explorer Enhanced Security Configuration is not enabled - Wind
Internet Explorer Enhanced Security Conf...
Page
Tools
Internet
100%

Caution: Internet Explorer Enhanced Security Configuration is not enabled

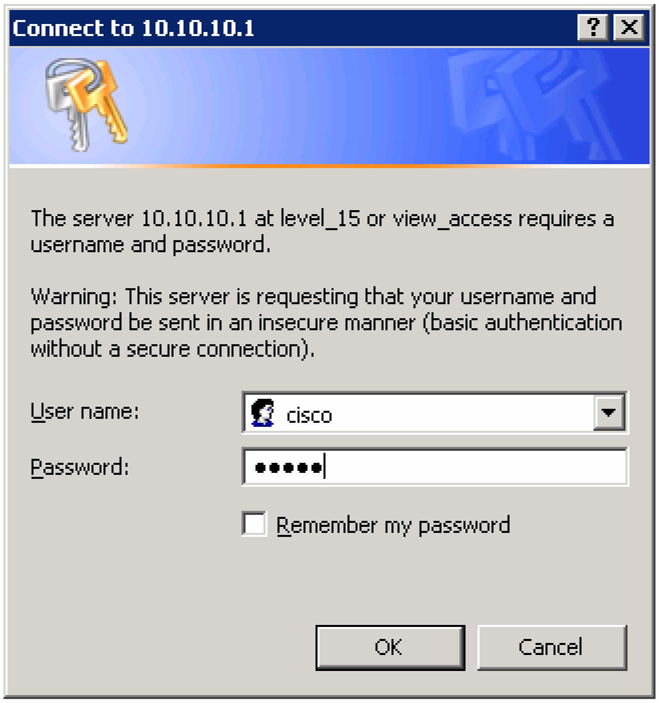
Internet Explorer Enhanced Security Configuration is an option that is provided in Windows Server 2003 operating systems. You can use it to quickly enhance Internet Explorer security settings for all users.

When you enable Internet Explorer Enhanced Security Configuration, it sets Internet Explorer security settings to limit how users browse Internet and intranet Web sites. This reduces the exposure of your server to Web sites that might pose a security risk. For more information, including the complete list of changes that are implemented by Internet Explorer Enhanced Security Configuration, see Internet Explorer Enhanced Security Configuration overview.

To enable Internet Explorer Enhanced Security Configuration

1. Open **Control Panel**, click **Add or Remove Programs**,

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.



The server 10.10.10.1 at level_15 or view_access requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: cisco

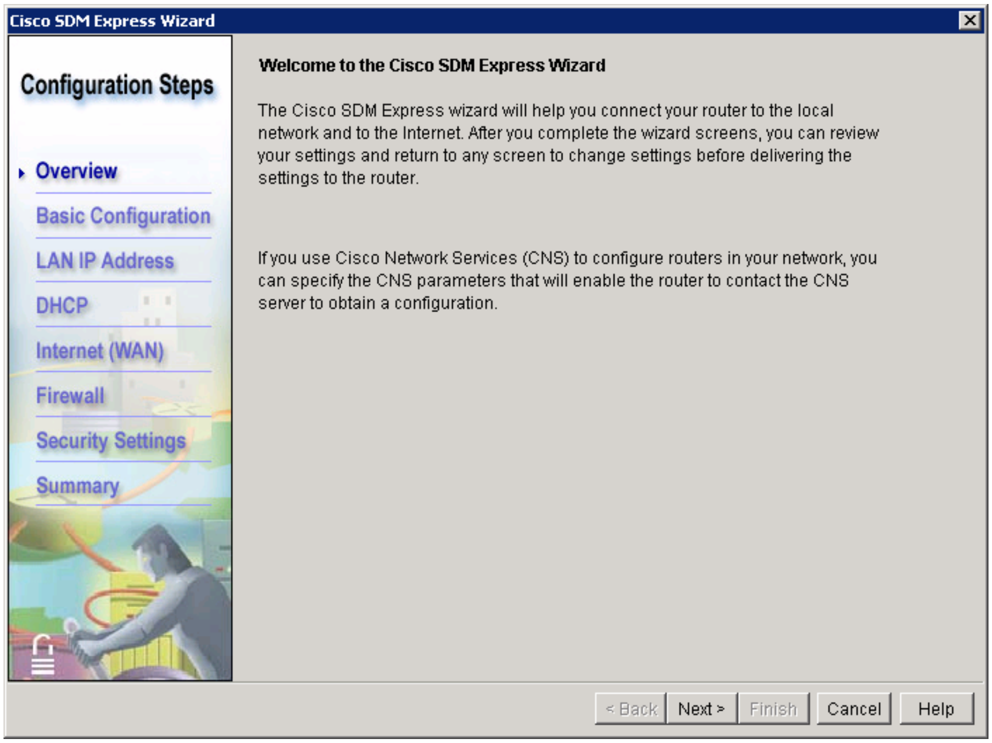
Password: •••••

☐ Remember my password

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.



Welcome to the Cisco SDM Express Wizard

The Cisco SDM Express wizard will help you connect your router to the local network and to the Internet. After you complete the wizard screens, you can review your settings and return to any screen to change settings before delivering the settings to the router.

If you use Cisco Network Services (CNS) to configure routers in your network, you can specify the CNS parameters that will enable the router to contact the CNS server to obtain a configuration.

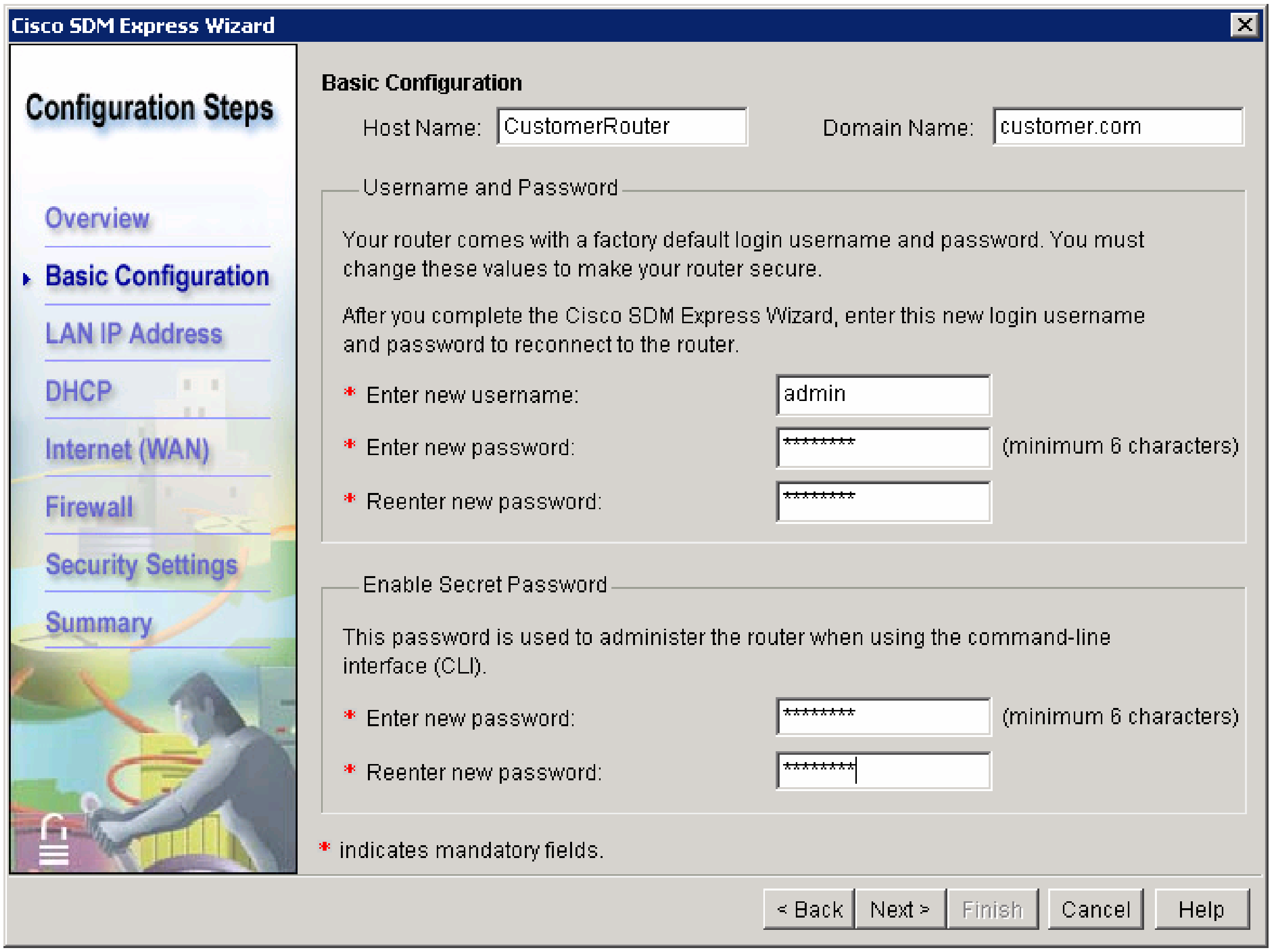
NOTE 3 – If SDM Express Wizard fails to start: If you connect to the router and SDM Express starts but the SDM Express Setup Wizard shown above does not start automatically, the router may be partially configured and needs to be reset to its factory defaults. If the SDM Express main screen is displayed, 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.



Basic Configuration

Host Name: CustomerRouter

Domain Name: customer.com

Username and Password

Your router comes with a factory default login username and password. You must change these values to make your router secure.

After you complete the Cisco SDM Express Wizard, enter this new login username and password to reconnect to the router.

* Enter new username: admin

* Enter new password: ********* (minimum 6 characters)

* Reenter new password: *********

Enable Secret Password

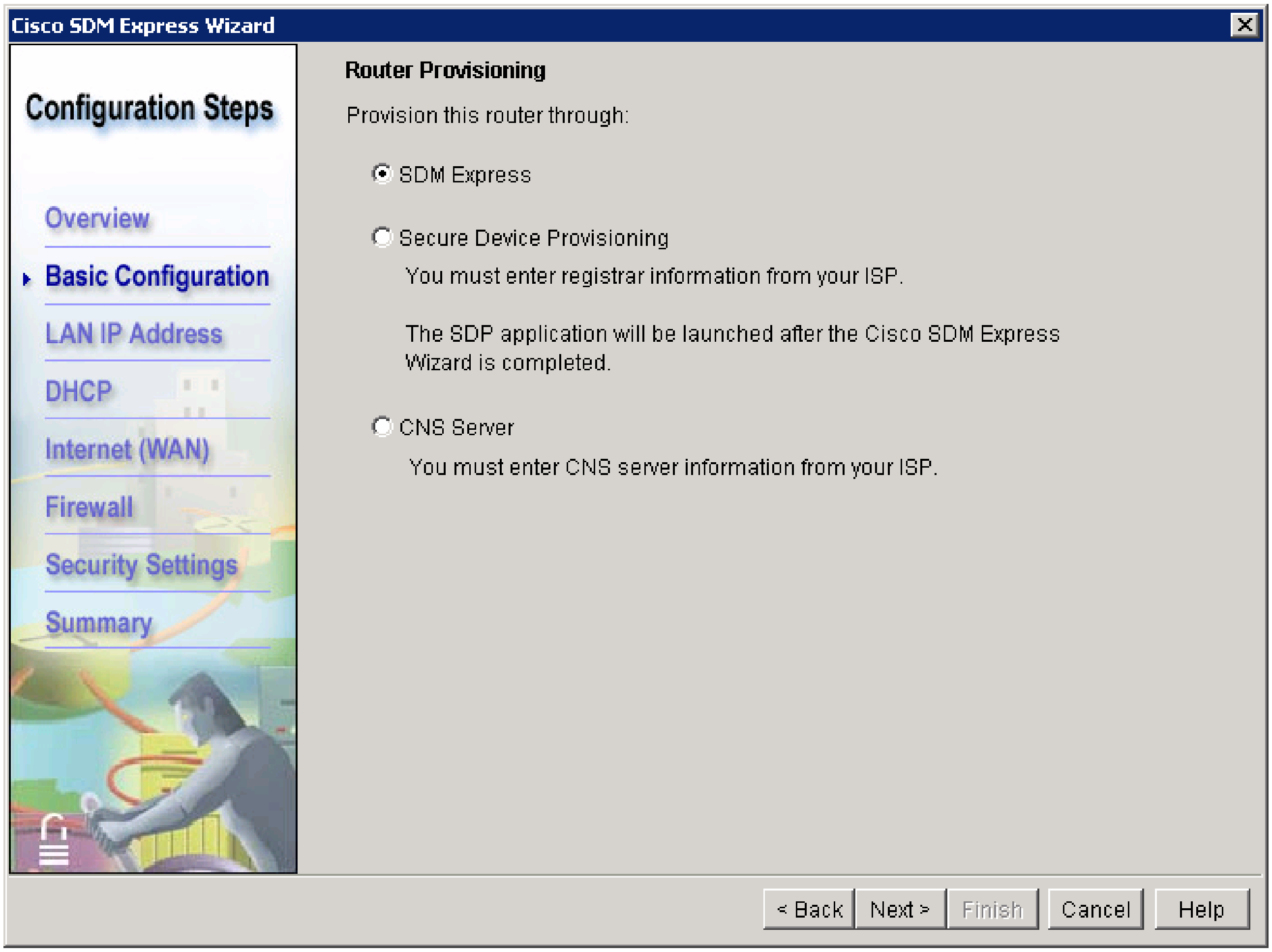
This password is used to administer the router when using the command-line interface (CLI).

* Enter new password: ********* (minimum 6 characters)

* Reenter new password: *********

* indicates mandatory fields.

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



Cisco SDM Express Wizard

Router Provisioning

Provision this router through:

● SDM Express

○ Secure Device Provisioning

You must enter registrar information from your ISP.

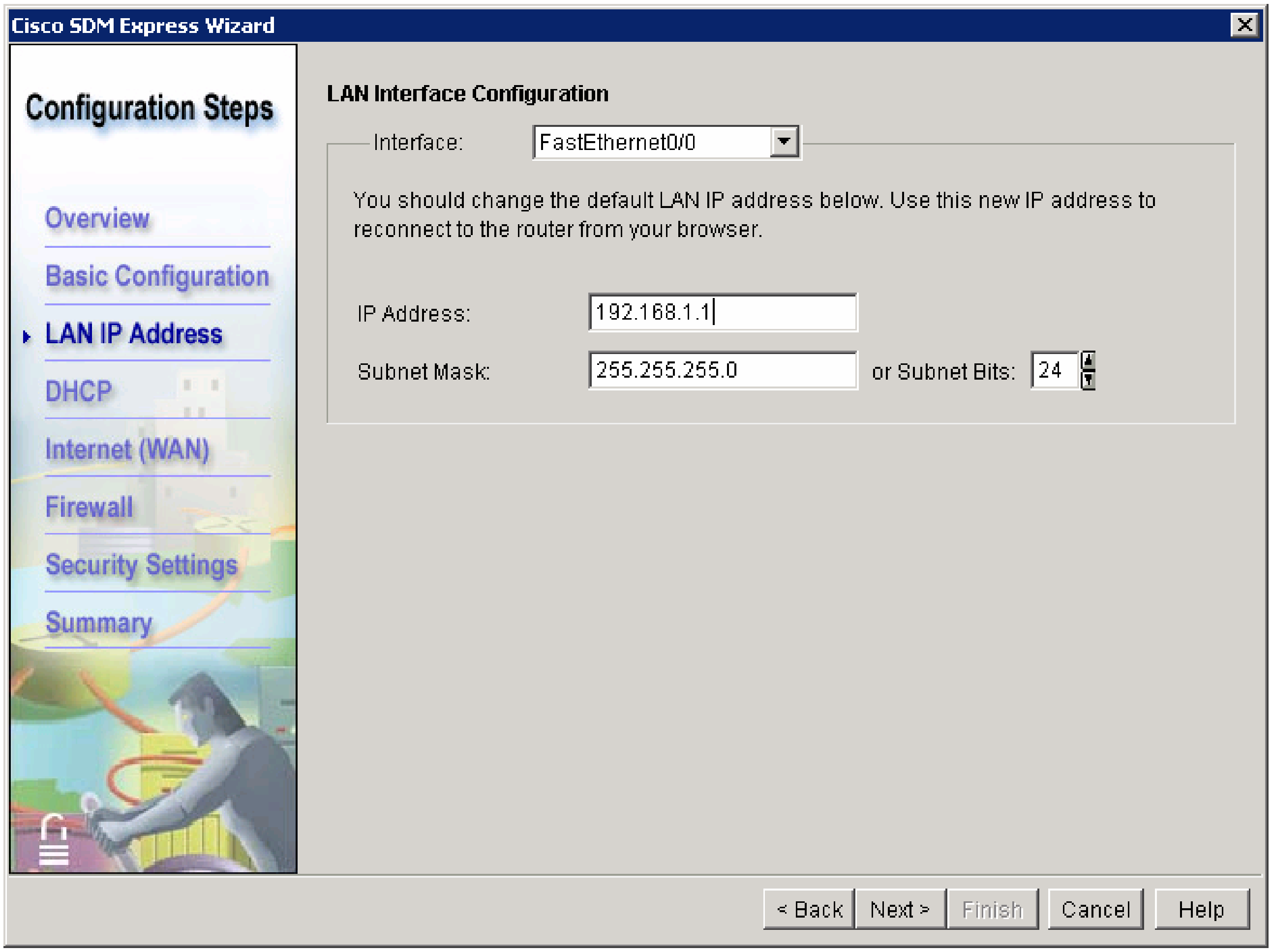
The SDP application will be launched after the Cisco SDM Express Wizard is completed.

○ CNS Server

You must enter CNS server information from your ISP.

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.



LAN Interface Configuration

Interface: FastEthernet0/0

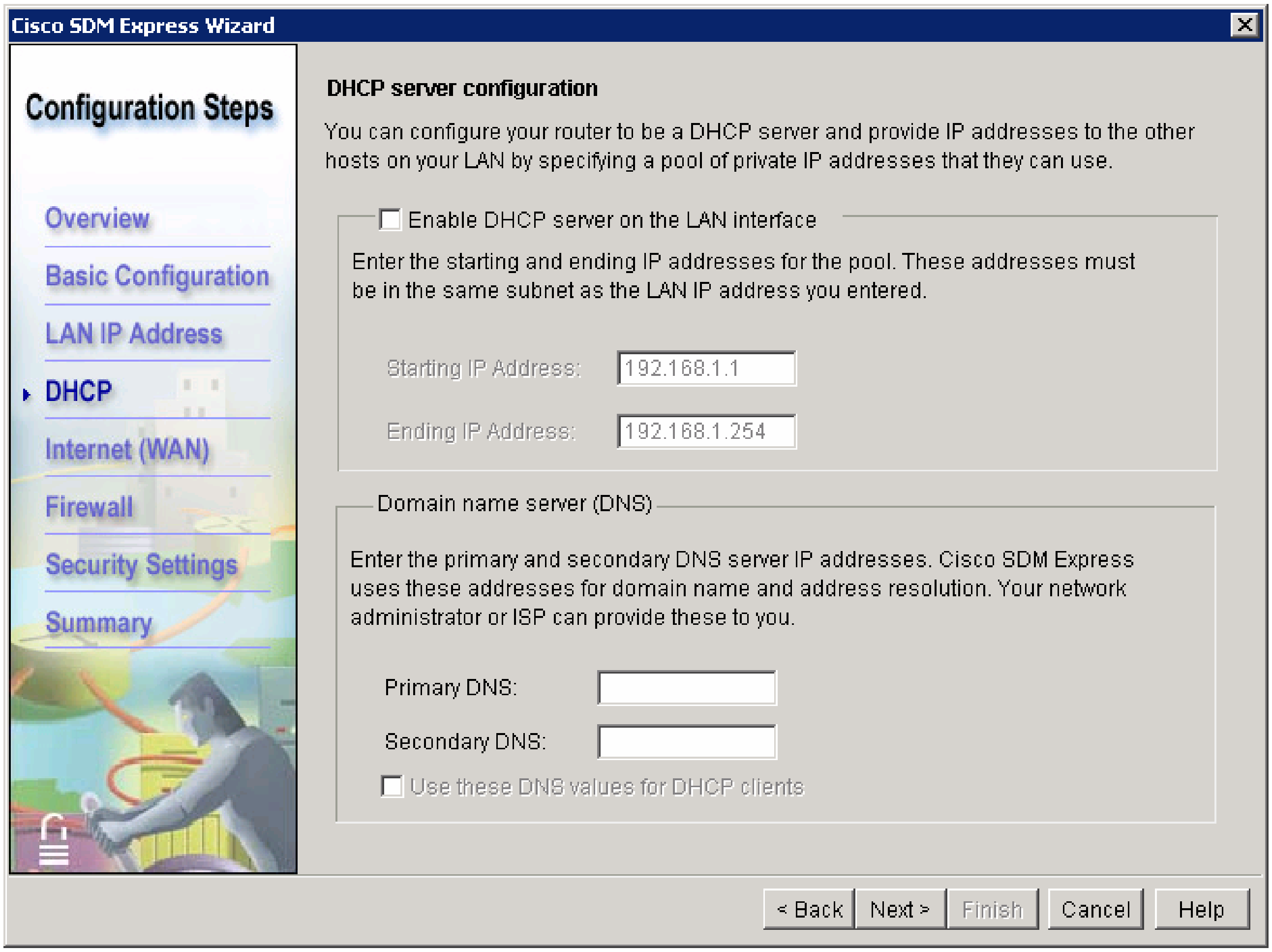
You should change the default LAN IP address below. Use this new IP address to reconnect to the router from your browser.

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0 or Subnet Bits: 24

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.



Cisco SDM Express Wizard

DHCP server configuration

You can configure your router to be a DHCP server and provide IP addresses to the other hosts on your LAN by specifying a pool of private IP addresses that they can use.

□ Enable DHCP server on the LAN interface

Enter the starting and ending IP addresses for the pool. These addresses must be in the same subnet as the LAN IP address you entered.

Starting IP Address: 192.168.1.1

Ending IP Address: 192.168.1.254

Domain name server (DNS)

Enter the primary and secondary DNS server IP addresses. Cisco SDM Express uses these addresses for domain name and address resolution. Your network administrator or ISP can provide these to you.

Primary DNS:

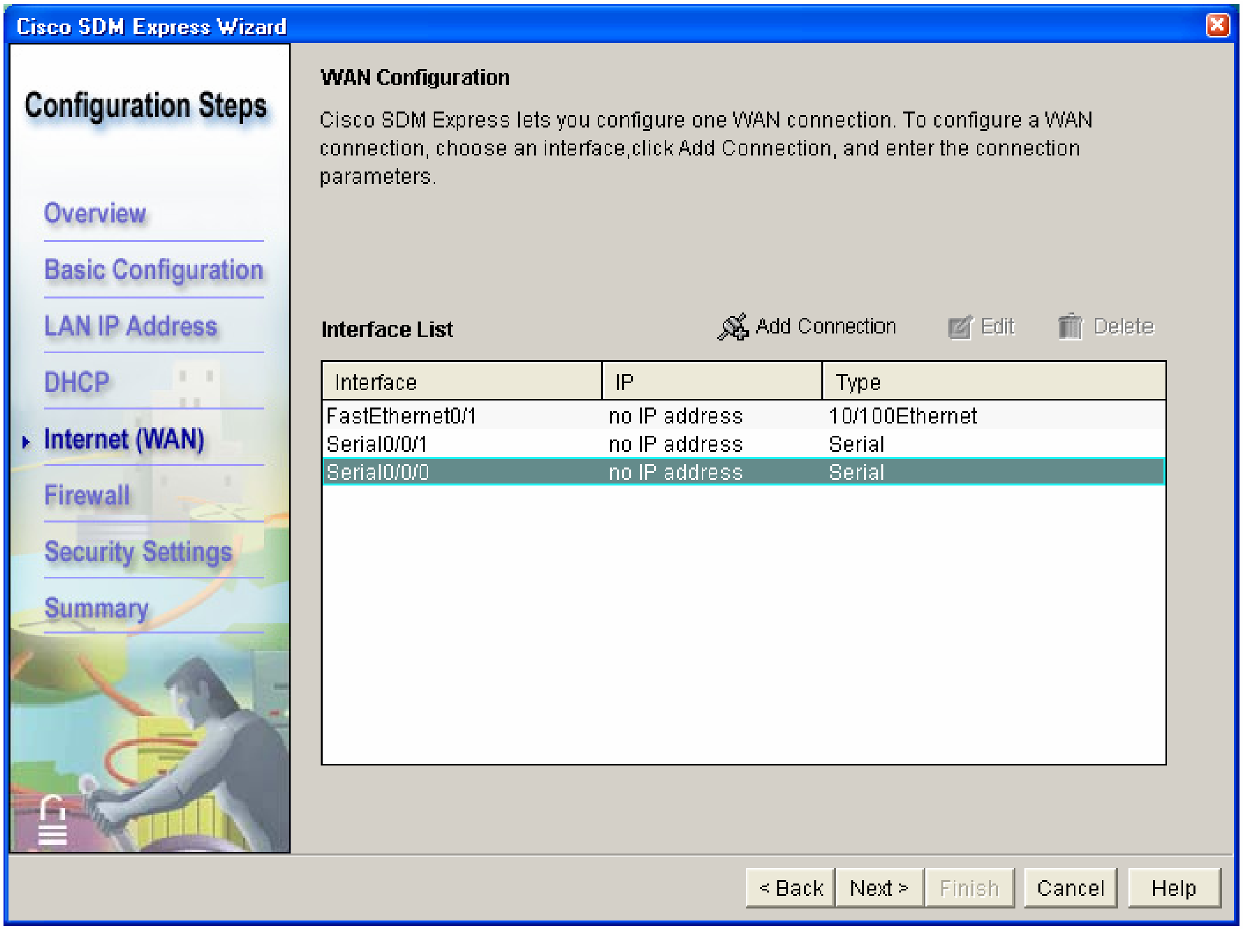
Secondary DNS:

□ Use these DNS values for DHCP clients

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.



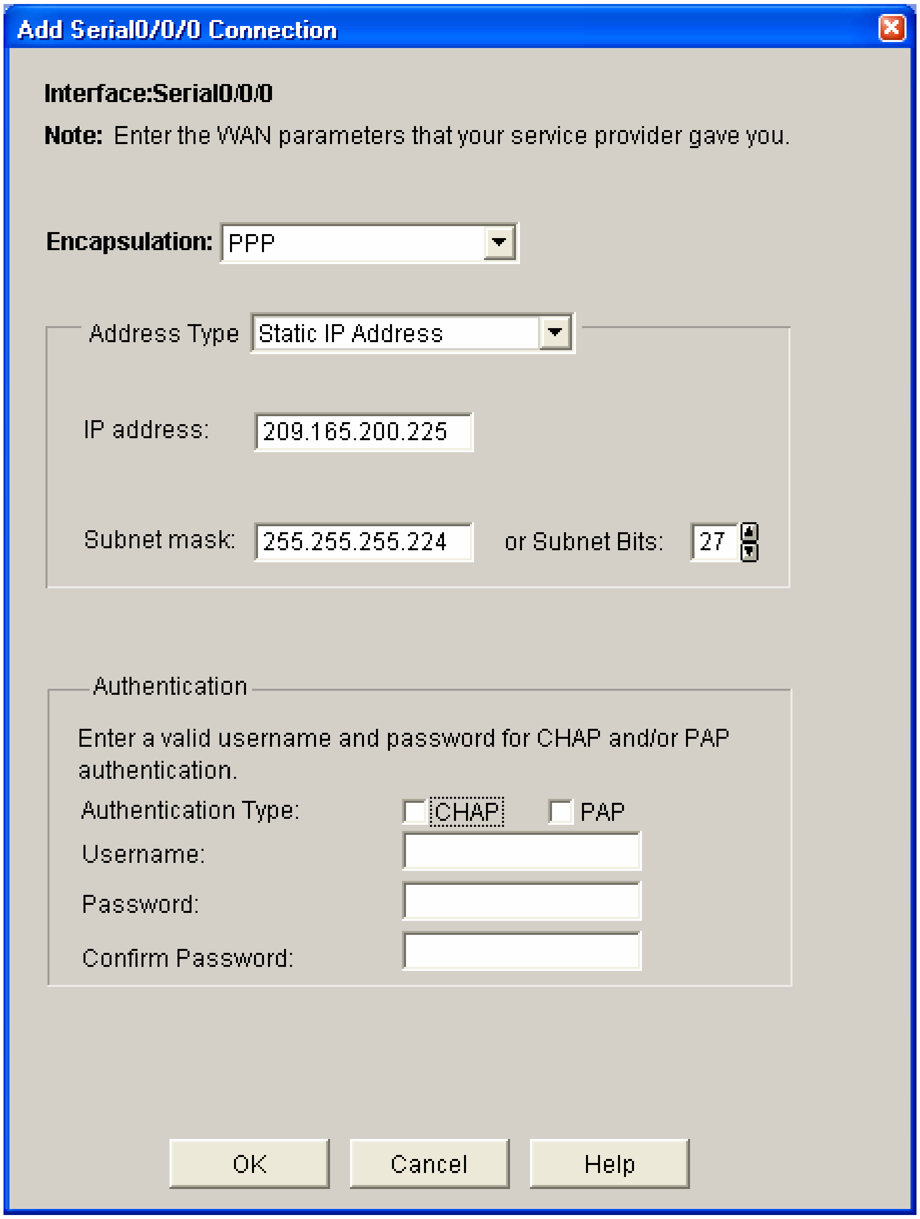
WAN Configuration

Cisco SDM Express lets you configure one WAN connection. To configure a WAN connection, choose an interface,click Add Connection, and enter the connection parameters.

Interface List

Interface	IP	Type
FastEthernet0/1	no IP address	10/100Ethernet
Serial0/0/1	no IP address	Serial
Serial0/0/0	no IP address	Serial

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.



Add Serial0/0/0 Connection

Interface:Serial0/0/0

Note: Enter the WAN parameters that your service provider gave you.

Encapsulation: PPP

Address Type: Static IP Address

IP address: 209.165.200.225

Subnet mask: 255.255.255.224 or Subnet Bits: 27

Authentication

Enter a valid username and password for CHAP and/or PAP authentication.

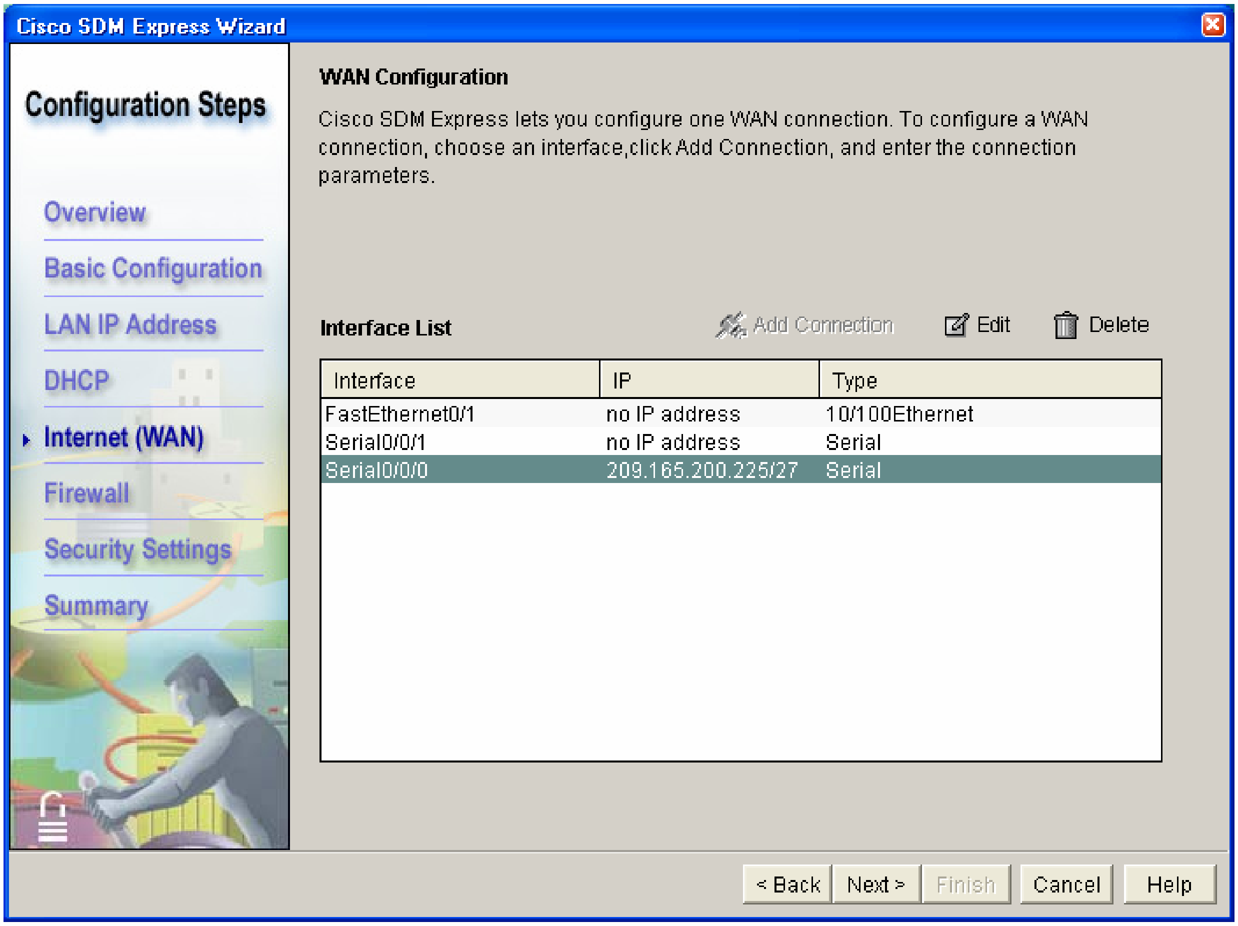
Authentication Type: □ CHAP □ PAP

Username:

Password:

Confirm Password:

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.



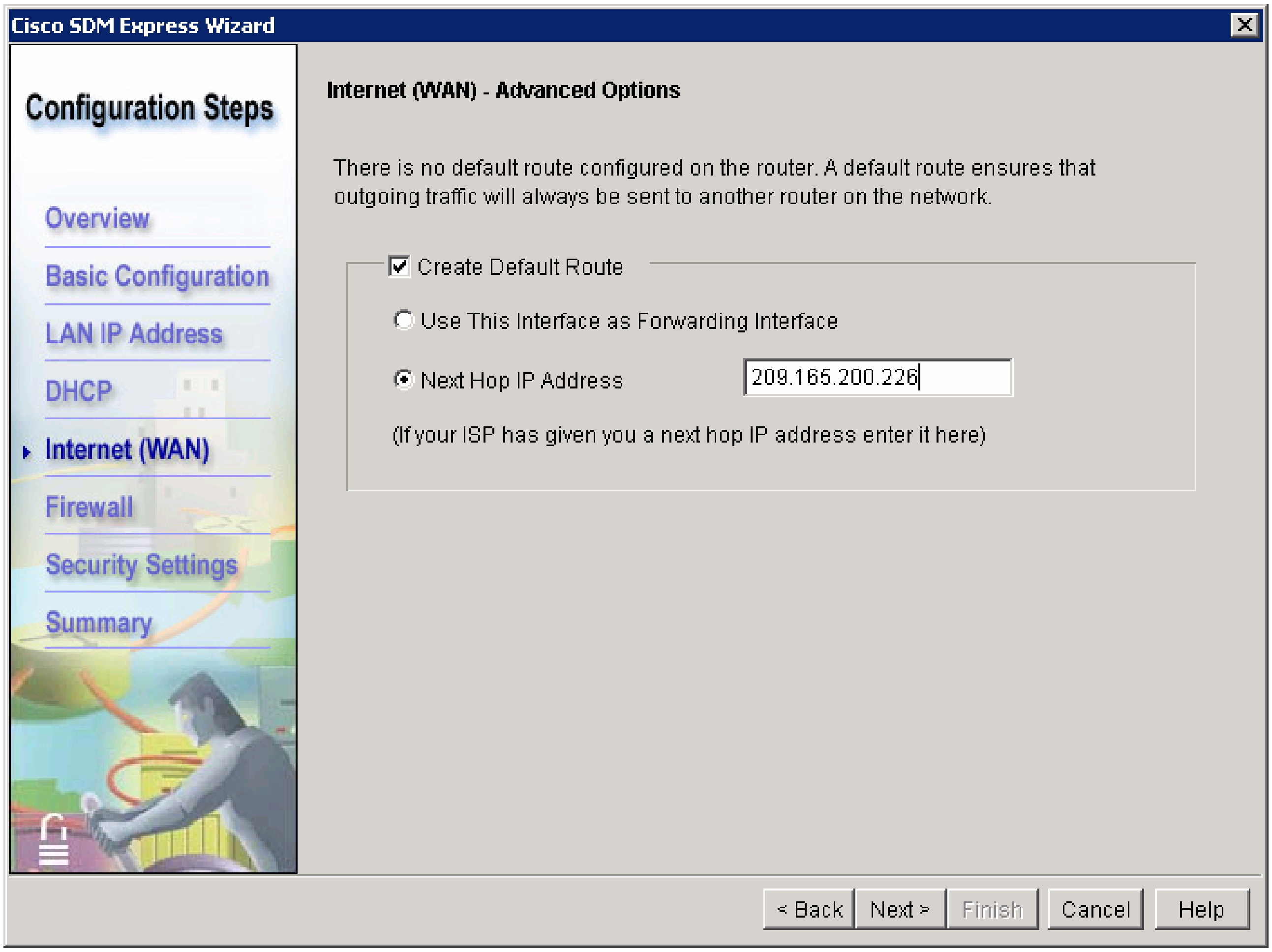
WAN Configuration

Cisco SDM Express lets you configure one WAN connection. To configure a WAN connection, choose an interface,click Add Connection, and enter the connection parameters.

Interface List

Interface	IP	Type
FastEthernet0/1	no IP address	10/100Ethernet
Serial0/0/1	no IP address	Serial
Serial0/0/0	209.165.200.225/27	Serial

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



Cisco SDM Express Wizard

Internet (WAN) - Advanced Options

There is no default route configured on the router. A default route ensures that outgoing traffic will always be sent to another router on the network.

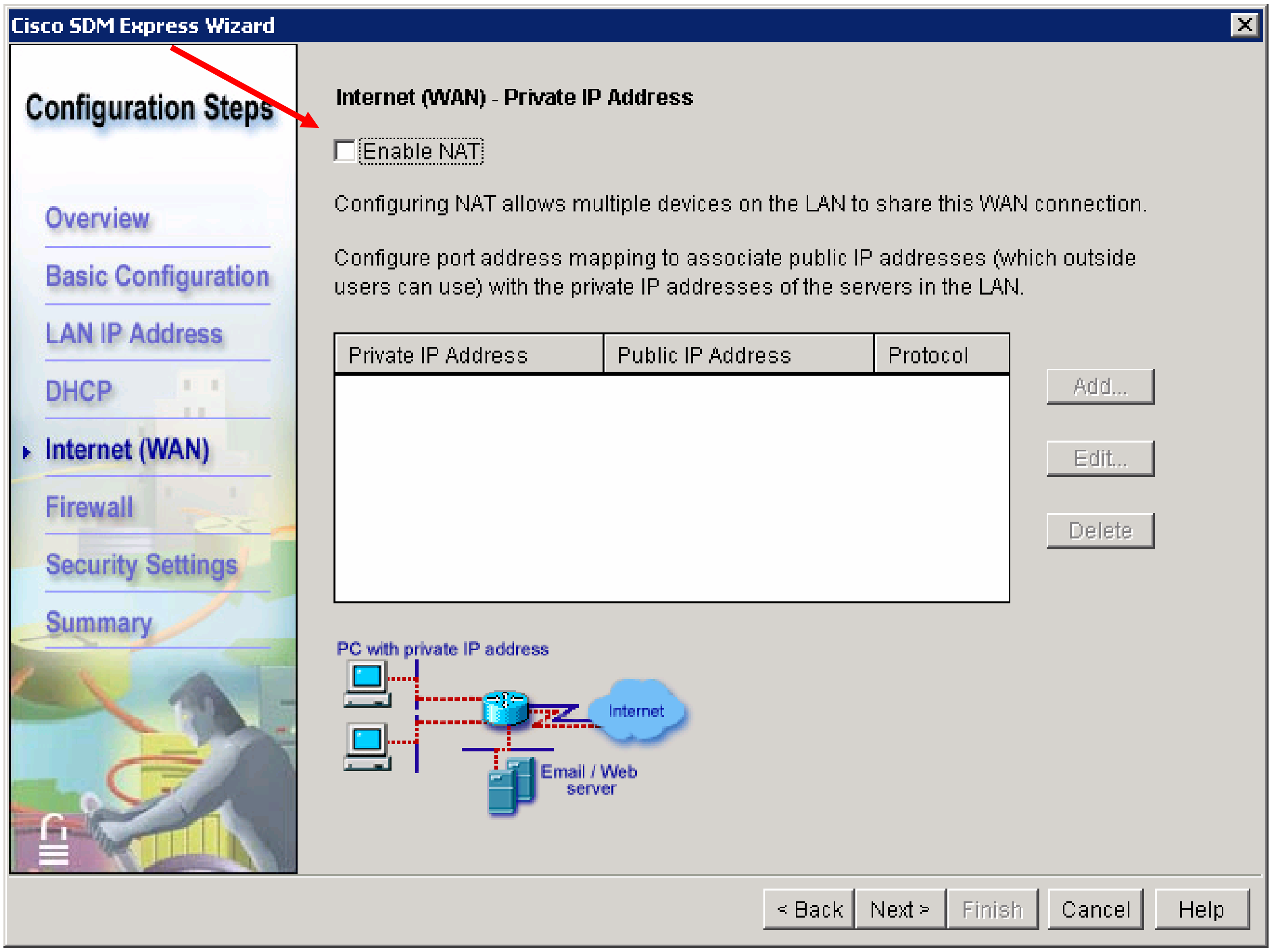
☑ Create Default Route

○ Use This Interface as Forwarding Interface

● Next Hop IP Address 209.165.200.226

(If your ISP has given you a next hop IP address enter it here)

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.



Cisco SDM Express Wizard

Internet (WAN) - Private IP Address

□ Enable NAT

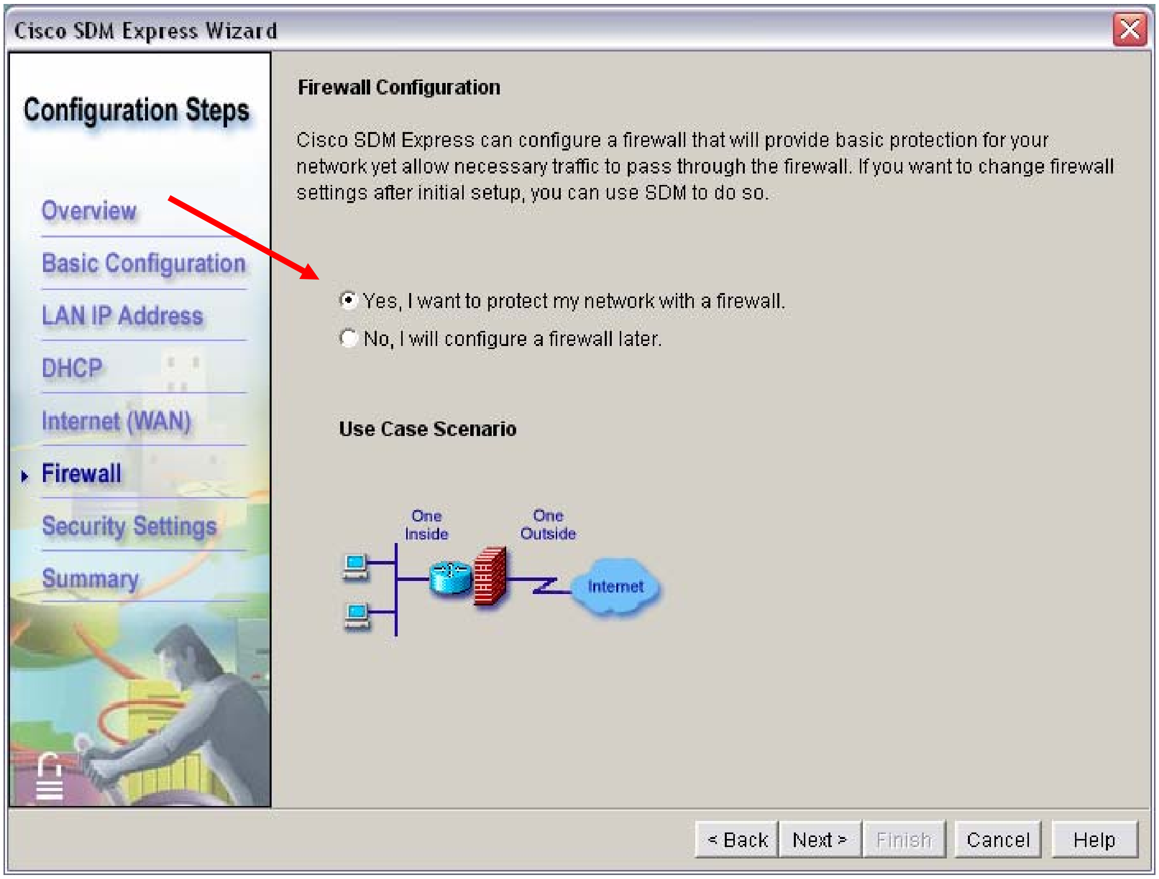
Configuring NAT allows multiple devices on the LAN to share this WAN connection.

Configure port address mapping to associate public IP addresses (which outside users can use) with the private IP addresses of the servers in the LAN.

Private IP Address	Public IP Address	Protocol

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.



Cisco SDM Express Wizard

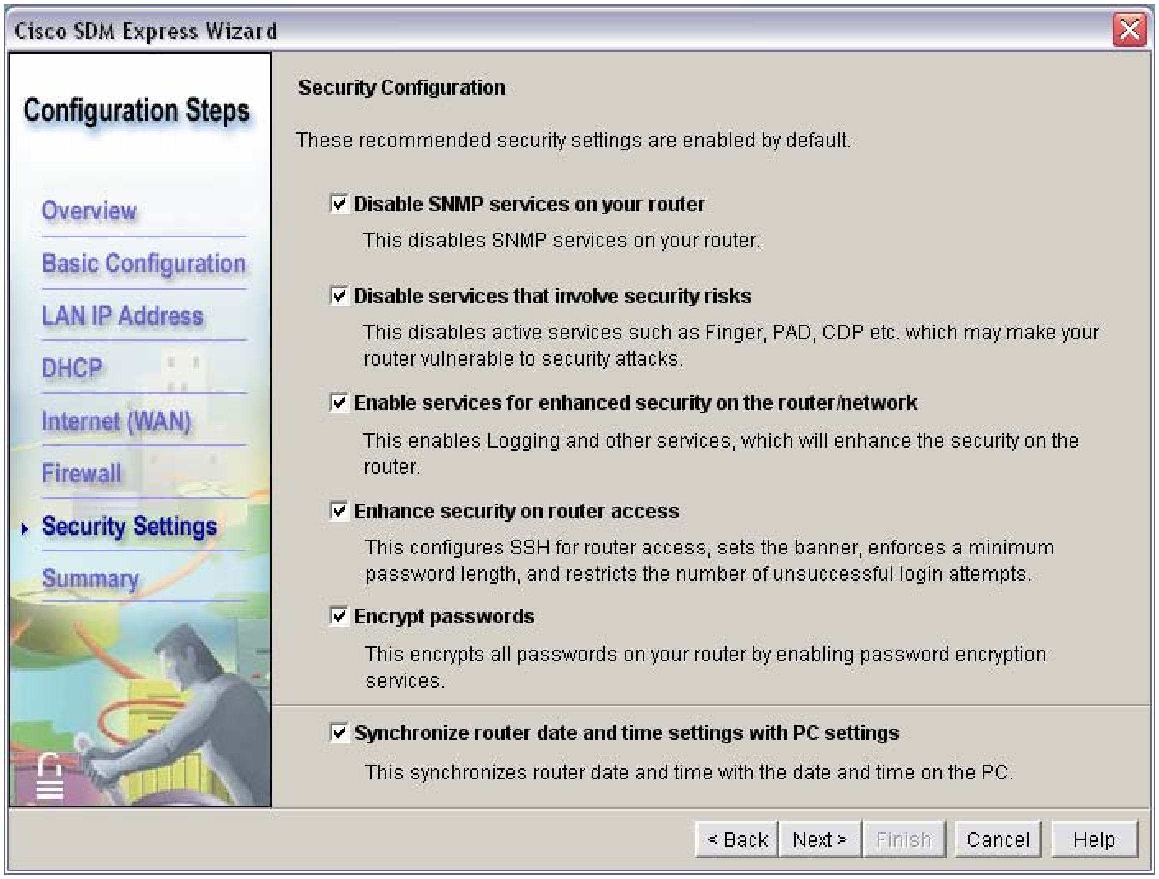
Firewall Configuration

Cisco SDM Express can configure a firewall that will provide basic protection for your network yet allow necessary traffic to pass through the firewall. If you want to change firewall settings after initial setup, you can use SDM to do so.

● Yes, I want to protect my network with a firewall.
○ No, I will configure a firewall later.

Use Case Scenario

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



Security Configuration

These recommended security settings are enabled by default.

☑ **Disable SNMP services on your router**

This disables SNMP services on your router.

☑ **Disable services that involve security risks**

This disables active services such as Finger, PAD, CDP etc. which may make your router vulnerable to security attacks.

☑ **Enable services for enhanced security on the router/network**

This enables Logging and other services, which will enhance the security on the router.

☑ **Enhance security on router access**

This configures SSH for router access, sets the banner, enforces a minimum password length, and restricts the number of unsuccessful login attempts.

☑ **Encrypt passwords**

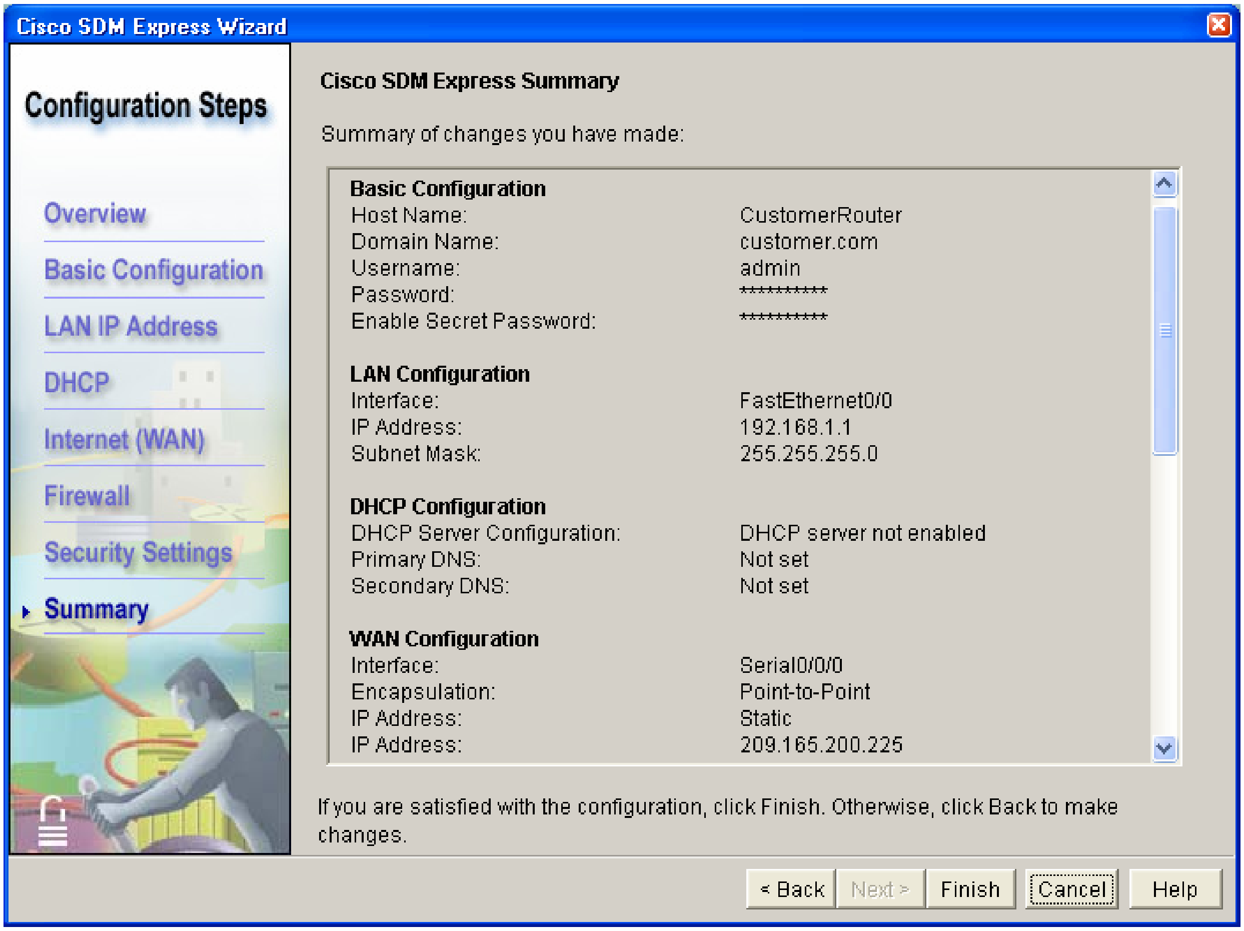
This encrypts all passwords on your router by enabling password encryption services.

☑ **Synchronize router date and time settings with PC settings**

This synchronizes router date and time with the date and time on the PC.

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.



Cisco SDM Express Summary

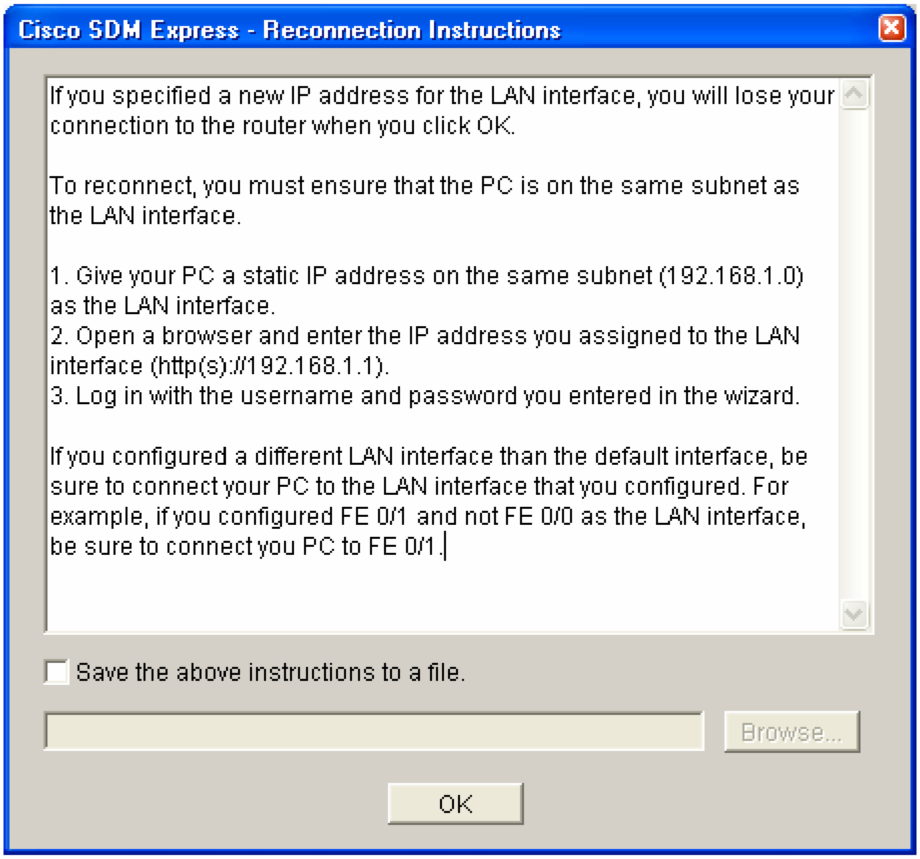
Summary of changes you have made:

```
Basic Configuration
Host Name:                          CustomerRouter
Domain Name:                        customer.com
Username:                           admin
Password:                           **********
Enable Secret Password:             **********

LAN Configuration
Interface:                          FastEthernet0/0
IP Address:                         192.168.1.1
Subnet Mask:                        255.255.255.0

DHCP Configuration
DHCP Server Configuration:          DHCP server not enabled
Primary DNS:                        Not set
Secondary DNS:                      Not set

WAN Configuration
Interface:                          Serial0/0/0
Encapsulation:                      Point-to-Point
IP Address:                         Static
IP Address:                         209.165.200.225
```

If you are satisfied with the configuration, click Finish. Otherwise, click Back to make changes.

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.



Cisco SDM Express - Reconnection Instructions

If you specified a new IP address for the LAN interface, you will lose your connection to the router when you click OK.

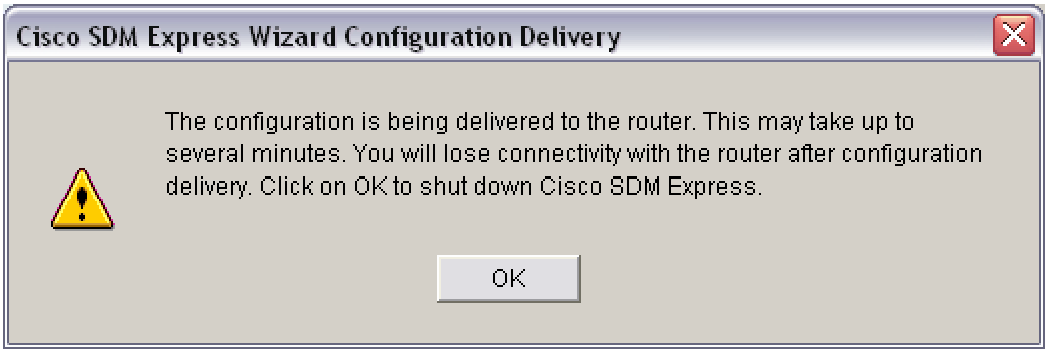
To reconnect, you must ensure that the PC is on the same subnet as the LAN interface.

1. Give your PC a static IP address on the same subnet (192.168.1.0) as the LAN interface.
2. Open a browser and enter the IP address you assigned to the LAN interface (http(s)://192.168.1.1).
3. Log in with the username and password you entered in the wizard.

If you configured a different LAN interface than the default interface, be sure to connect your PC to the LAN interface that you configured. For example, if you configured FE 0/1 and not FE 0/0 as the LAN interface, be sure to connect you PC to FE 0/1.

☐ Save the above instructions to a file.

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



Cisco SDM Express Wizard Configuration Delivery

The configuration is being delivered to the router. This may take up to several minutes. You will lose connectivity with the router after configuration delivery. Click on OK to shut down 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)
```

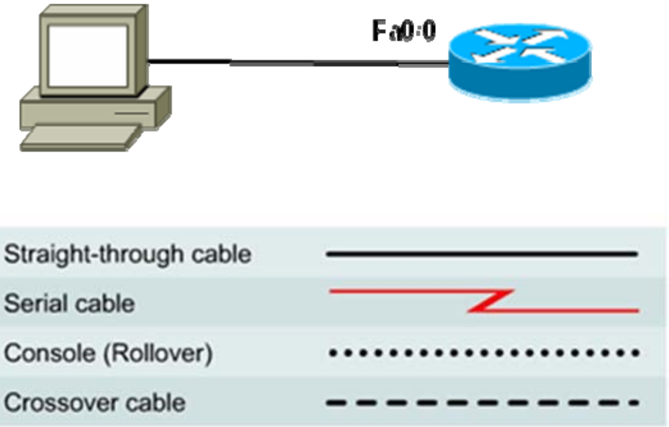
NOTE: An SDM router other than the 1841 may require connection to different port in order to access SDM.

```
   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 5.2.4 Configuring Dynamic NAT with SDM



Objectives

- 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. SDM simplifies router and security configuration through the use of smart wizards, which allow you to deploy, configure, and monitor a Cisco router without requiring knowledge of the command line interface (CLI). 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 http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm.

Note: To download the SDM application at the above URL, the instructor needs to provide a valid CCO account login ID and password. If you do not have a CCO account, go to http://www.cisco.com/cgi-bin/login. Under Not Registered, click Register Now to create an account.

From the SDM web page, 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 Cisco IOS software versions that support SDM, and the amount of memory required.

Cisco SDM is the full SDM product, and SMD Express is a subset. SDM is 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 NAT, 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,” before performing this lab. This lab assumes that the router has been previously configured with basic settings using SDM Express.

Required Resources

The following resources are required:

- Cisco 1841 ISR router with SDM version 2.4 or later installed and with basic configuration completed
- (Optional) Other Cisco router model with SDM installed
- Windows XP computer with Internet Explorer 5.5 or later 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 Fast Ethernet 0/0 (Fa0/0) port on the Cisco 1841 ISR router with the Ethernet cable.

Note: A router other than the 1841 may require a connection to a different port to access SDM.

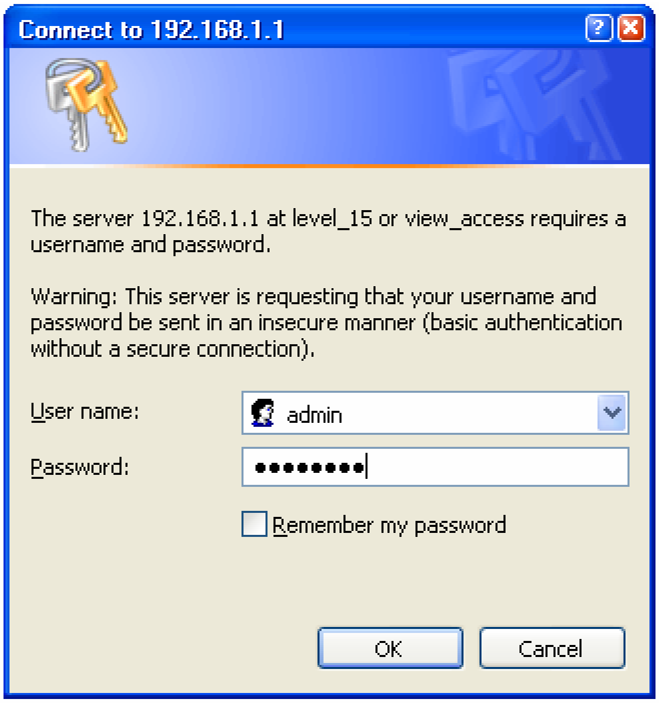
e. Configure the IP address of the PC as 192.168.1.2, with a subnet mask of 255.255.255.0.

f. SDM does not load automatically on the router. You must open a web browser to access SDM at http://192.168.1.1.

Note: If the browser cannot connect, check the cabling and connections and make sure that the PC 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. Then connect to http://10.10.10.1 using the browser. If you have difficulty with this procedure, ask the instructor for assistance.

Note: If the startup-config is erased from the router, SDM no longer comes up by default when the router is restarted. In this case, a basic router configuration must be rebuilt using Cisco IOS commands. See the procedure at the end of this lab or contact the instructor.

g. In the **Connect to** dialog box, enter **admin** for the username, and **cisco123** for the password. The login ID was configured in the previous lab. Click **OK**. The main SDM web application starts. You are prompted to use HTTPS. Click **Cancel**. In the Security Warning window, click **Yes** to trust the Cisco application.



Connect to 192.168.1.1

The server 192.168.1.1 at level_15 or view_access requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

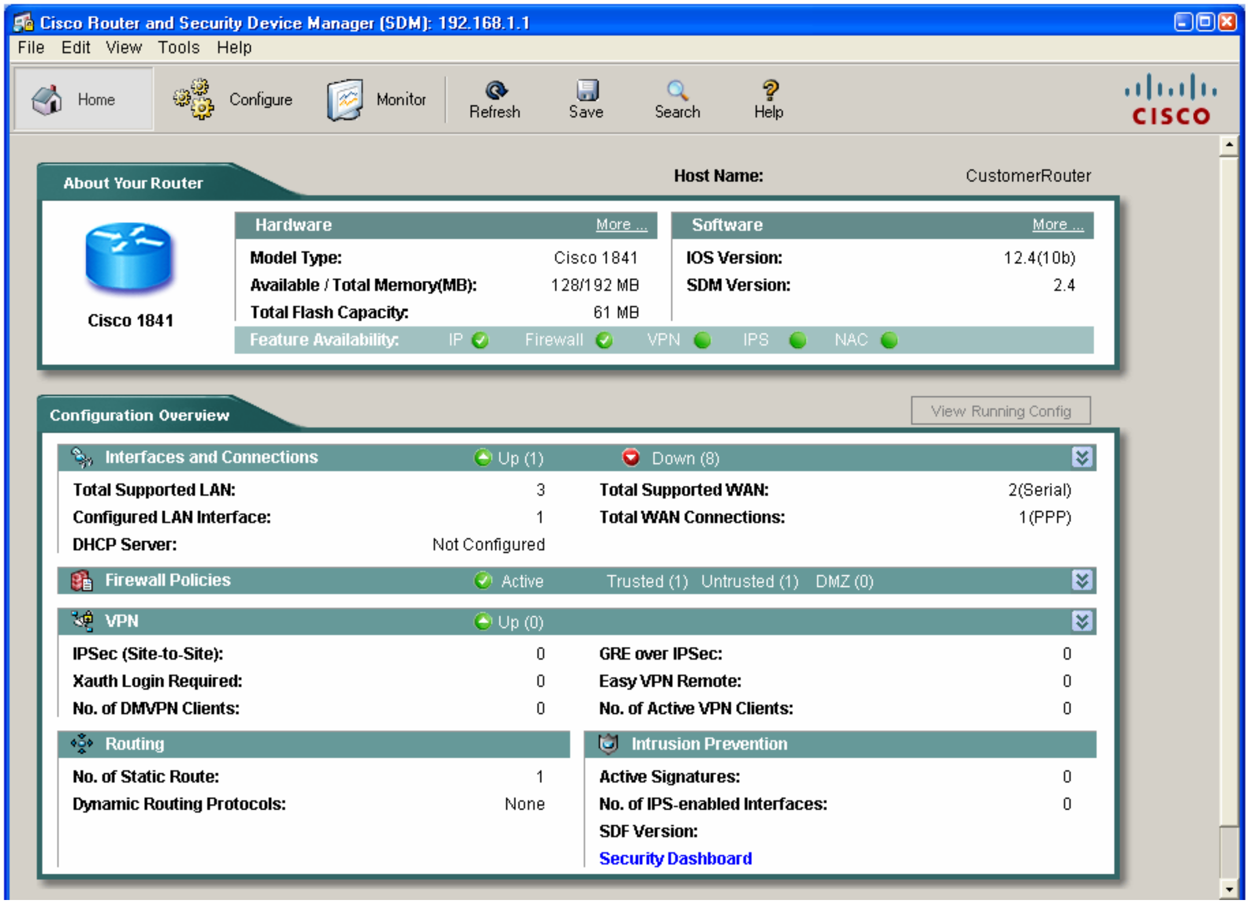
User name: admin

Password: ●●●●●●●●●

□ Remember my password

h. Verify that you are using version 2.4 or later of SDM. The initial SDM screen that displays immediately after the login shows the version that you are using. It is also displayed on the main SDM screen as shown below, along with the Cisco IOS software version.

Note: If the version is not 2.4 or later, notify the instructor before continuing with this lab. You must download the latest zip file from the SDM web page and save it to the PC. From the Tools menu of the SDM GUI, choose **Update SDM** to specify the location of the zip file and install the update.



About Your Router

Host Name: CustomerRouter

Cisco 1841

Hardware	
Model Type:	Cisco 1841
Available / Total Memory(MB):	128/192 MB
Total Flash Capacity:	61 MB

Software	
IOS Version:	12.4(10b)
SDM Version:	2.4

Feature Availability: IP ✓ Firewall ✓ VPN ● IPS ● NAC ●

Configuration Overview

Interfaces and Connections — Up (1) — Down (8)

Total Supported LAN:	3	Total Supported WAN:	2(Serial)
Configured LAN Interface:	1	Total WAN Connections:	1(PPP)
DHCP Server:	Not Configured		

Firewall Policies — Active — Trusted (1) Untrusted (1) DMZ (0)

VPN — Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

Routing

No. of Static Route:	1
Dynamic Routing Protocols:	None

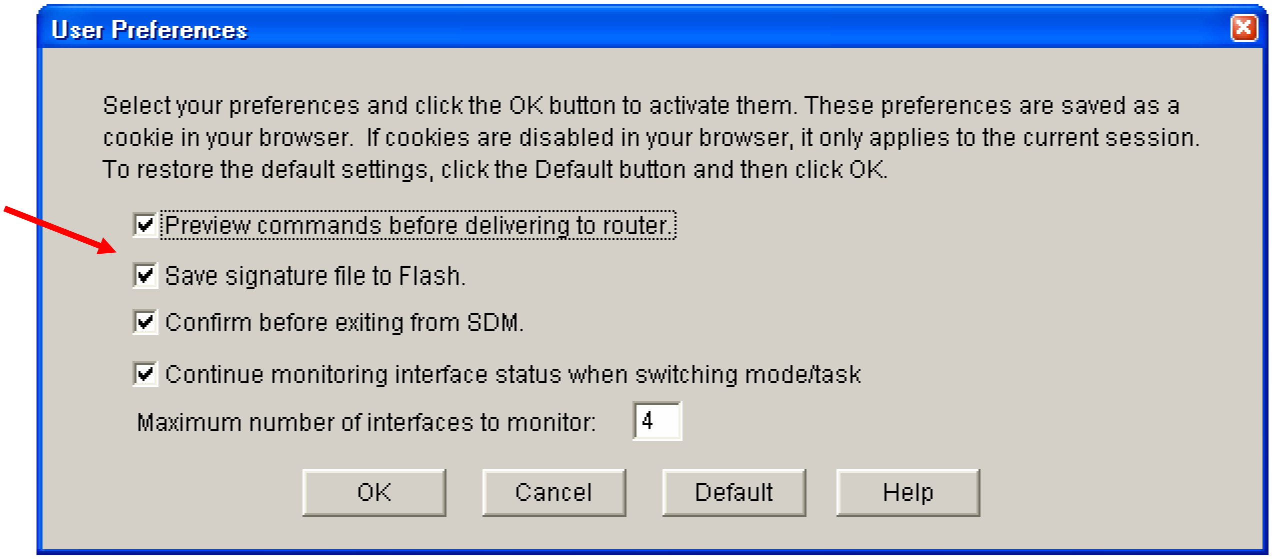
Intrusion Prevention

Active Signatures:	0
No. of IPS-enabled Interfaces:	0
SDF Version:	

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

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

b. Check the **Preview commands before delivering to router** box. When this option is checked, you can view the Cisco IOS CLI configuration commands before they are sent to the router, which is a good way to learn about the commands used.



Select your preferences and click the OK button to activate them. These preferences are saved as a cookie in your browser. If cookies are disabled in your browser, it only applies to the current session. To restore the default settings, click the Default button and then click OK.

☑ Preview commands before delivering to router.

☑ Save signature file to Flash.

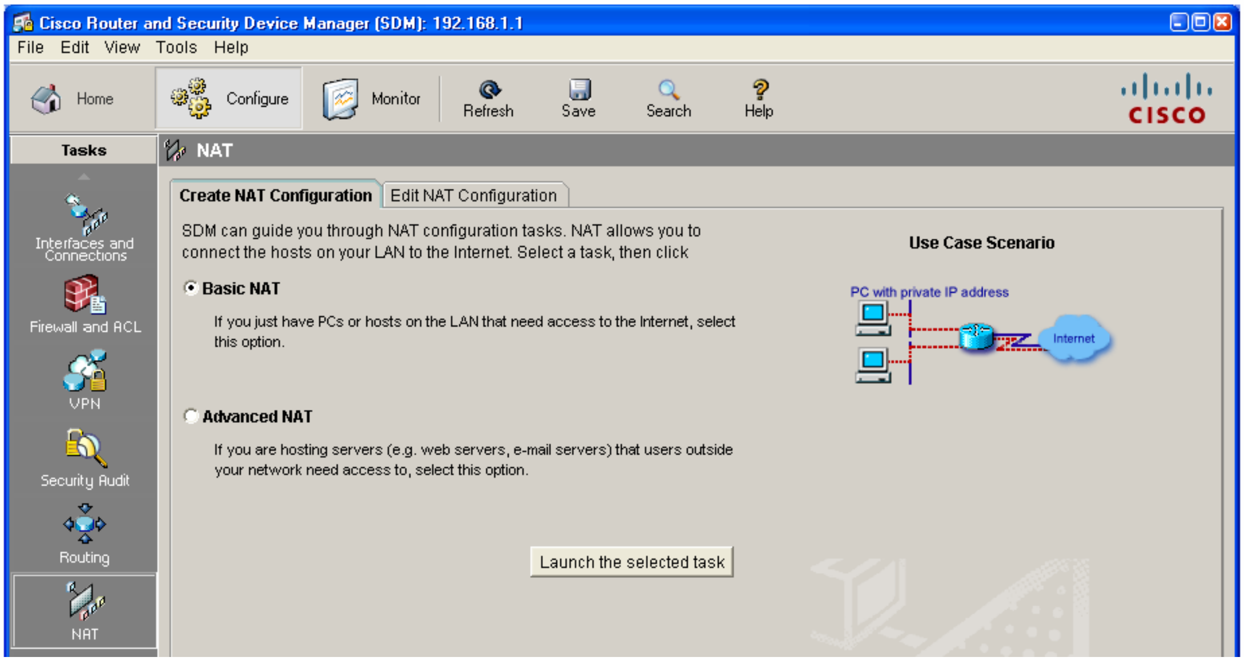
☑ Confirm before exiting from SDM.

☑ Continue monitoring interface status when switching mode/task

Maximum number of interfaces to monitor: 4

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**.



SDM can guide you through NAT configuration tasks. NAT allows you to connect the hosts on your LAN to the Internet. Select a task, then click

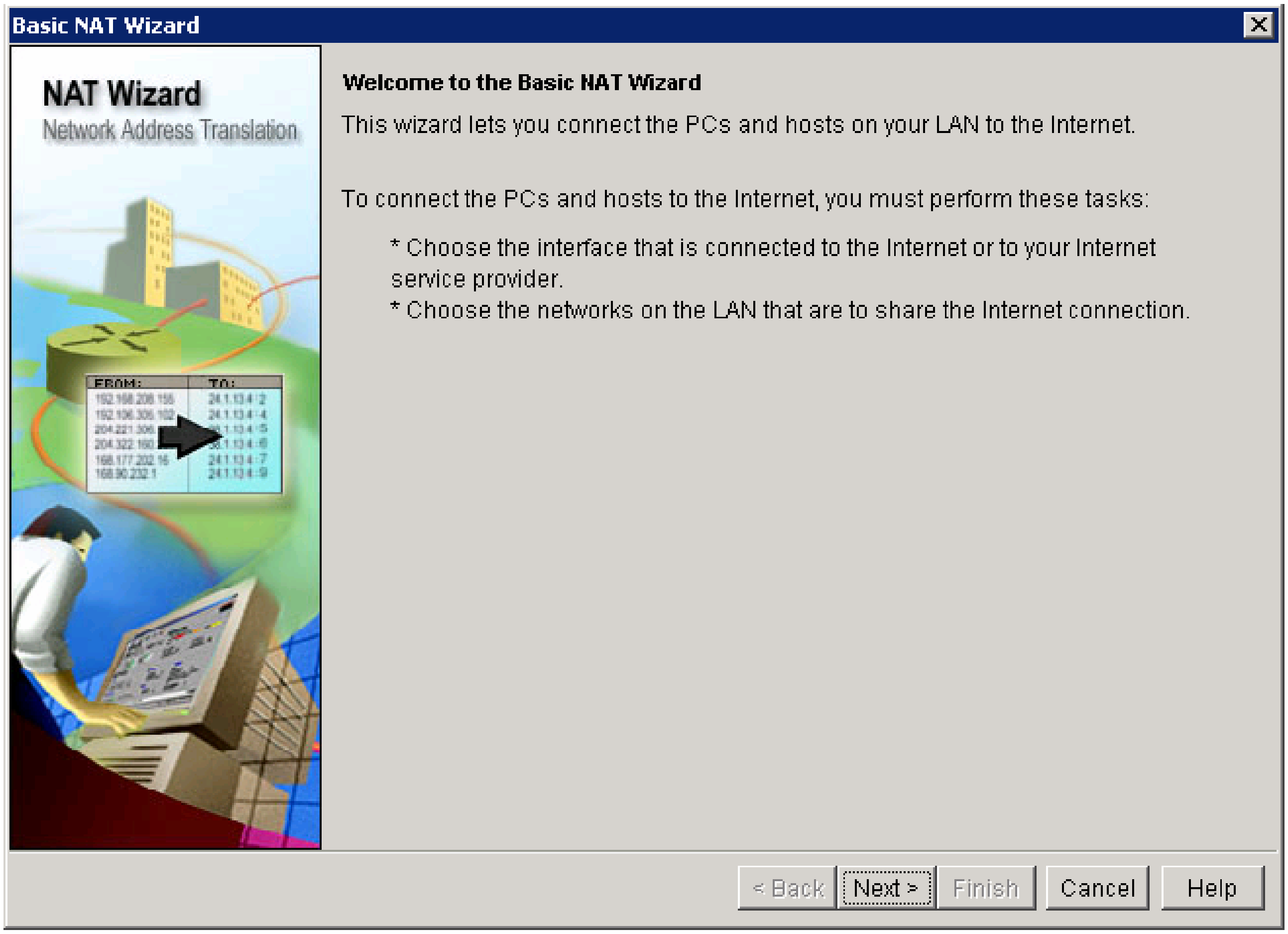
● Basic NAT

If you just have PCs or hosts on the LAN that need access to the Internet, select this option.

○ Advanced NAT

If you are hosting servers (e.g. web servers, e-mail servers) that users outside your network need access to, select this option.

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



Welcome to the Basic NAT Wizard

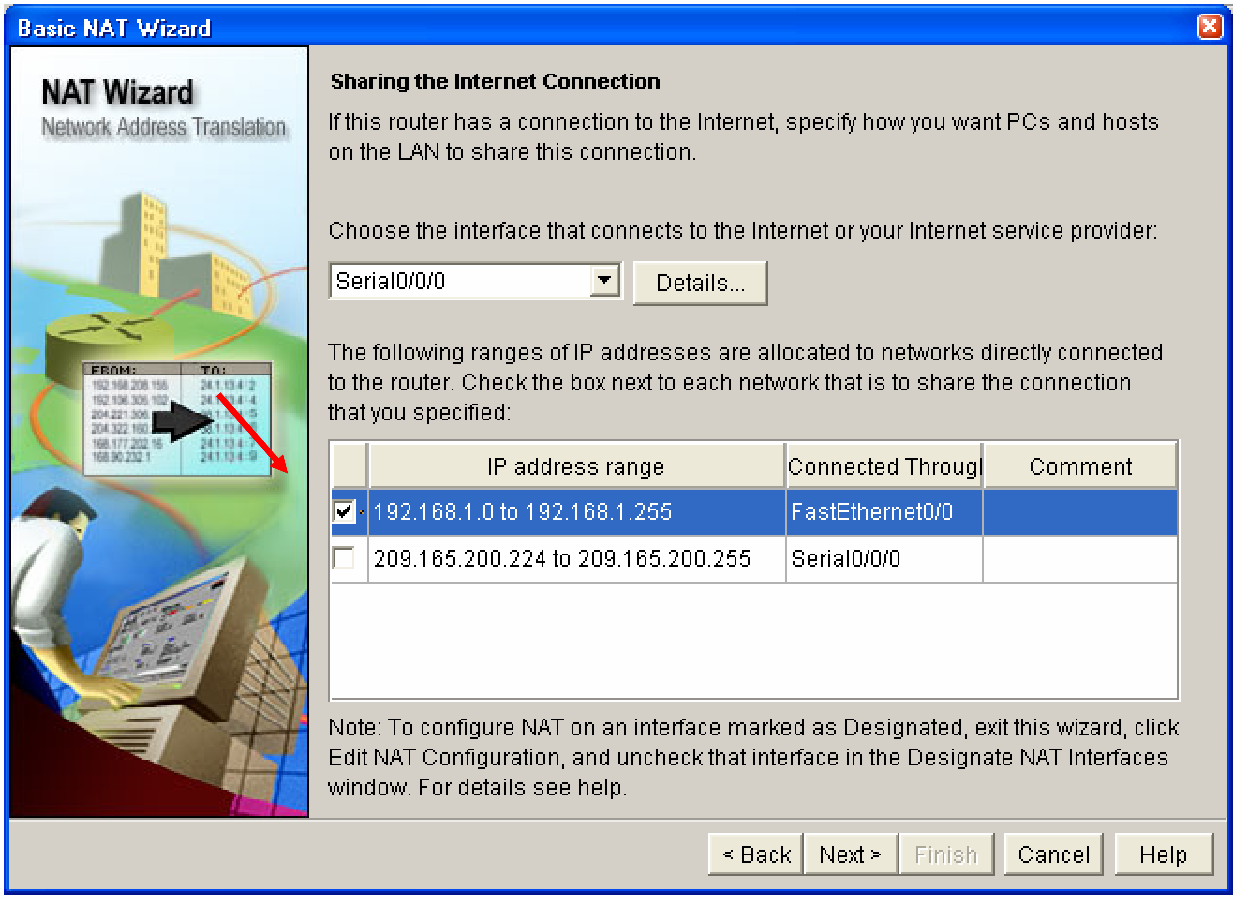
This wizard lets you connect the PCs and hosts on your LAN to the Internet.

To connect the PCs and hosts to the Internet, you must perform these tasks:

* Choose the interface that is connected to the Internet or to your Internet service provider.
* Choose the networks on the LAN that are to share the Internet connection.

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.



Basic NAT Wizard

Sharing the Internet Connection

If this router has a connection to the Internet, specify how you want PCs and hosts on the LAN to share this connection.

Choose the interface that connects to the Internet or your Internet service provider:

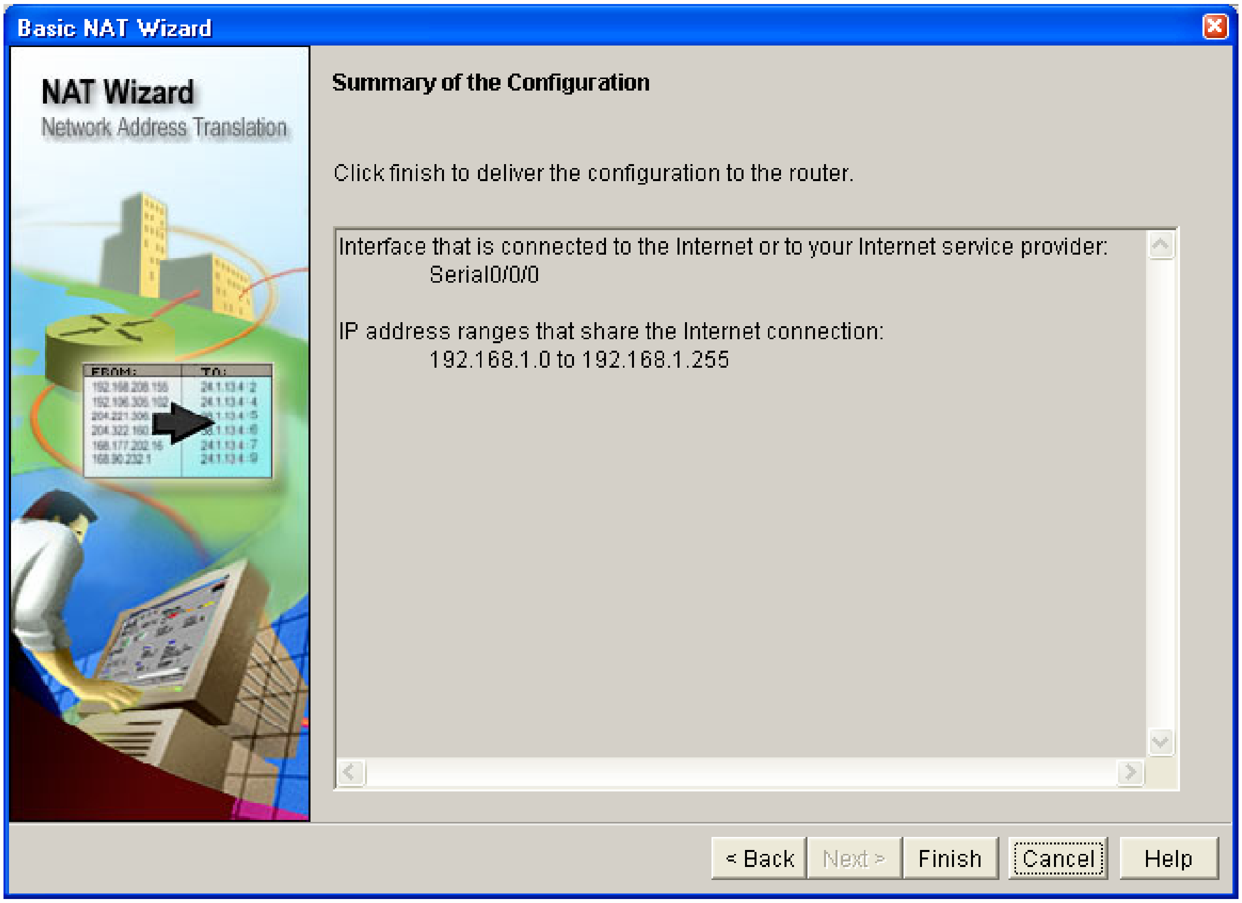
Serial0/0/0 ▾ Details...

The following ranges of IP addresses are allocated to networks directly connected to the router. Check the box next to each network that is to share the connection that you specified:

	IP address range	Connected Throug	Comment
☑	192.168.1.0 to 192.168.1.255	FastEthernet0/0	
☐	209.165.200.224 to 209.165.200.255	Serial0/0/0	

Note: To configure NAT on an interface marked as Designated, exit this wizard, click Edit NAT Configuration, and uncheck that interface in the Designate NAT Interfaces window. For details see help.

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



Summary of the Configuration

Click finish to deliver the configuration to the router.

Interface that is connected to the Internet or to your Internet service provider:
Serial0/0/0

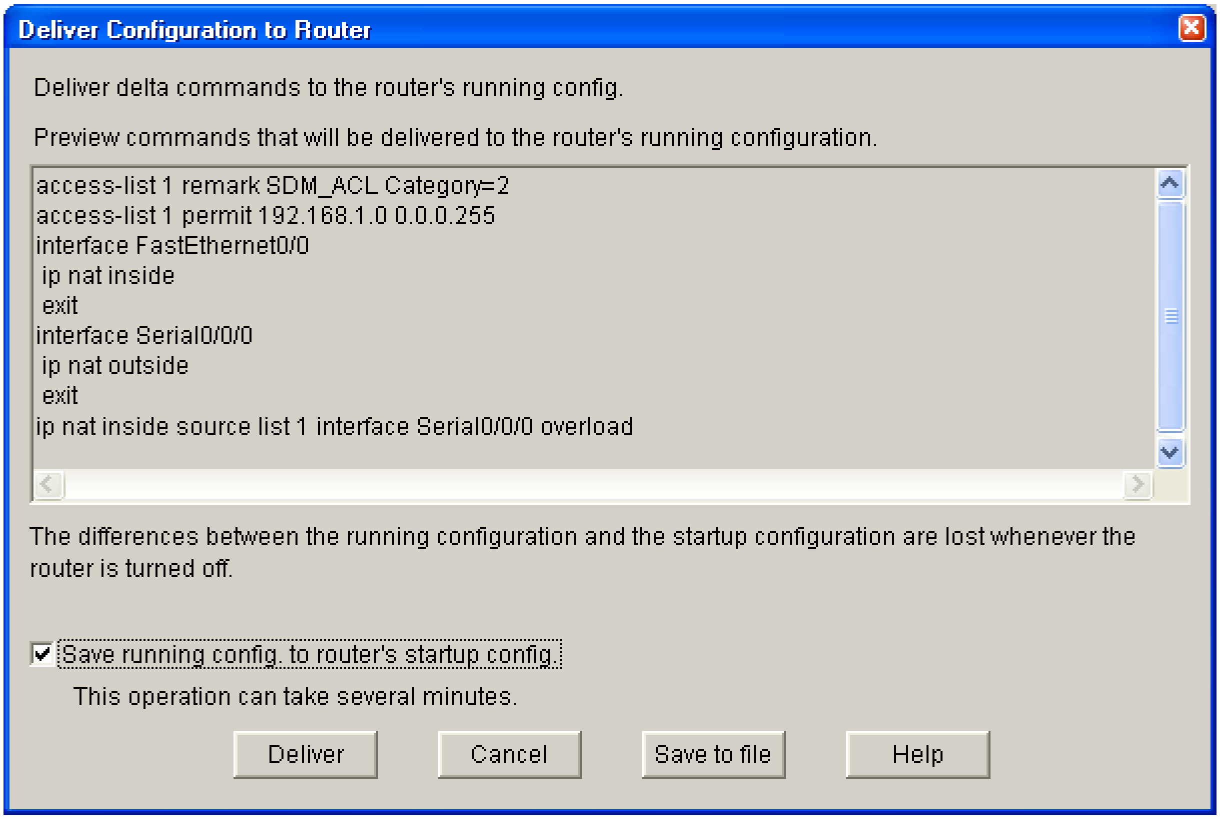
IP address ranges that share the Internet connection:
192.168.1.0 to 192.168.1.255

c. In the **Deliver Configuration to Router** window, review the CLI commands that were generated by the SDM. These are the commands that are 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 only update the running configuration file when delivered. If the router is restarted, the changes you made are lost. Checking this box updates the startup config file so that when the router is restarted, it loads 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.



Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

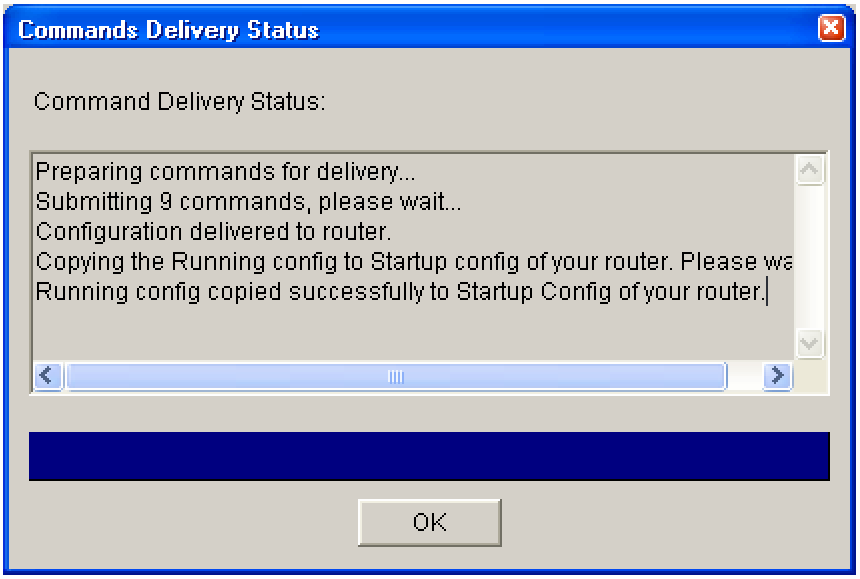
```
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 192.168.1.0 0.0.0.255
interface FastEthernet0/0
 ip nat inside
 exit
interface Serial0/0/0
 ip nat outside
 exit
ip nat inside source list 1 interface Serial0/0/0 overload
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

☑ Save running config. to router's startup config.

This operation can take several minutes.

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.

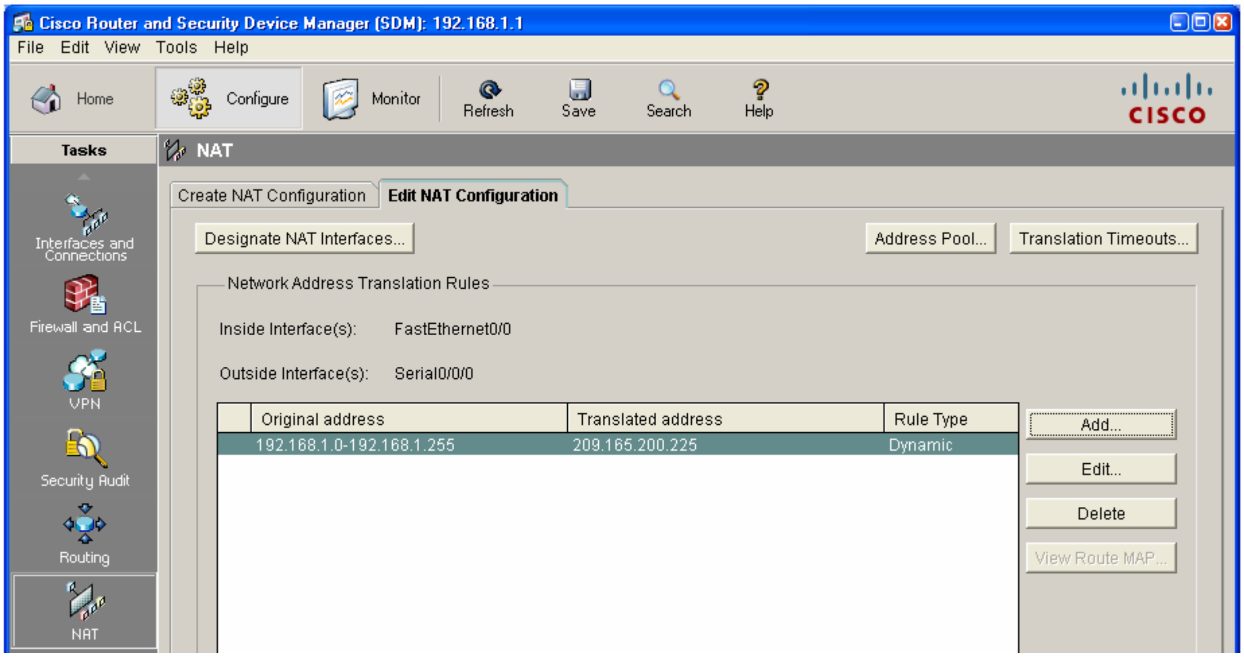


Commands Delivery Status

Command Delivery Status:

```
Preparing commands for delivery...
Submitting 9 commands, please wait...
Configuration delivered to router.
Copying the Running config to Startup config of your router. Please wa
Running config copied successfully to Startup Config of your router.
```

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 are translated dynamically to the external public address.



Cisco Router and Security Device Manager (SDM): 192.168.1.1

NAT

Network Address Translation Rules

Inside Interface(s): FastEthernet0/0

Outside Interface(s): Serial0/0/0

Original address	Translated address	Rule Type
192.168.1.0-192.168.1.255	209.165.200.225	Dynamic

Step 5: Reflection

a. If a PC or a LAN within an organization does not require Internet access, what is one way to stop the PC from gaining access to the Internet?

____

____

____

b. What are some advantages and disadvantages of using SDM to configure NAT compared to the CLI?

____

____

____

____

____

____

c. Why is the default to only update the running configuration file when delivered? Why not always update the startup config file? What are the advantages and disadvantages of one over the other?

____

____

____

____

Basic Cisco IOS Configuration to Bring Up SDM

If the startup config is erased in an SDM router, SDM no longer comes up by default when the router is restarted. It is then necessary to build a basic config as follows. Further details regarding the setup and use of SDM 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 connects 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 a connection to a different port 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.

```
Router(config)#ip http server
Router(config)#ip http secure-server
Router(config)#ip http authentication local
```

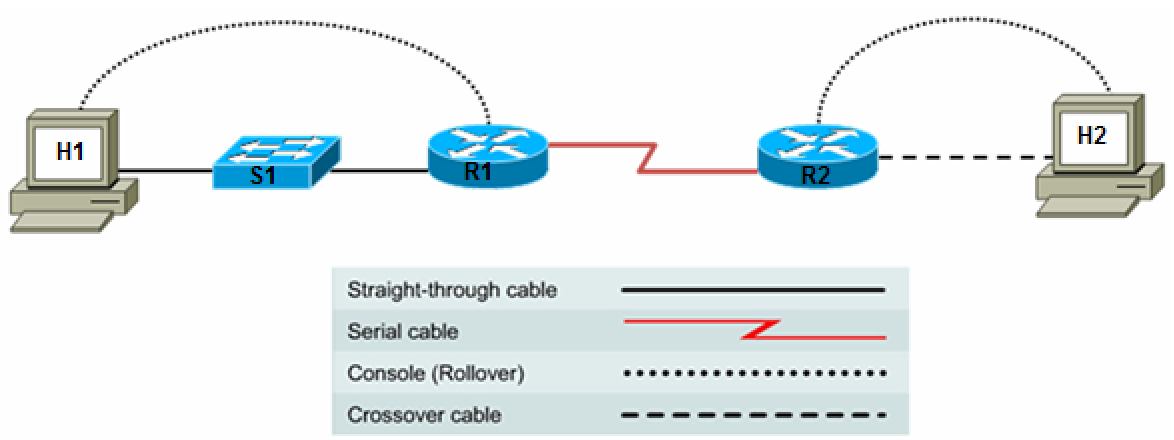
3) Create a user account with privilege level 15 (enable privileges). Replace *username* and *password* with the username and password that you want to configure.

```
Router(config)#username <username> privilege 15 password 0 <password>
```

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 the Cisco IOS CLI



Device	Host Name	Interface	IP Address	Subnet Mask
R1	R1	Serial 0/0/0 (DCE)	172.17.0.1	255.255.0.0
		FastEthernet 0/0	172.16.0.1	255.255.0.0
R2	R2	Serial 0/0/0 (DTE)	172.17.0.2	255.255.0.0
		FastEthernet 0/0	172.18.0.1	255.255.0.0

Objectives

- Configure the device host name for a router.
- Configure console, privileged EXEC mode, and vty passwords.
- Configure Ethernet and serial interfaces, including description.
- Configure a message of the day (MOTD) banner.
- Configure the routers to not perform domain lookup of host names.
- Configure synchronous console logging.
- Verify connectivity between hosts and routers.

Background / Preparation

In this lab, you build a multi-router network and configure the routers to communicate using the most common Cisco IOS configuration commands.

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- Two routers, each with an Ethernet and serial interface. These should be non-SDM routers, if possible, because the required SDM startup configuration is deleted when the startup-config is erased.
- Two Windows XP computers with HyperTerminal installed
- Two straight-through Category 5 Ethernet cables (H1 to S1 and S1 to R2)
- Crossover Category 5 Ethernet cable (H2 to R2)
- Null serial cable (R1 to R2)
- Console cables (H1 ro R1 and H2 to R2)
- Access to the host H1 and H2 command prompt
- Access to the host H1 and H2 network TCP/IP configuration

From each host computer, start a HyperTerminal session to the attached router.

Note: Before continuing, on all routers perform the steps in the section “Erasing and Reloading the Router” at the end of this lab.

Step 1: Configure host computer IP settings.

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

b. Configure the hosts with static IP addresses using the following settings.

H1 attached to the S1 switch:

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

H2 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 the basic settings.

Note: Perform each step for both routers.

a. Configure a host name for each of the two routers.

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

Note: Use **R2** for the name of the second router.

b. Configure a console password and enable login for each of the two routers. Examples are provided for R1. Repeat these commands on R2.

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

c. Configure the password on the vty 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)#
```

d. 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
```

Note: Remember that the enable secret password is encrypted when viewing the configuration. 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. When an enable secret password is configured, the enable password is no longer accepted. It will be necessary to enter the enable secret password to enter privileged EXEC mode. Some network administrators may choose to configure only the enable secret password.

e. Configure a message-of-the-day (MOTD) banner using the **banner motd** command. When a user connects to the router, the MOTD banner appears before the login prompt. In this example, the number sign (#) is used to start and end the message. The # is converted to ^C when the running-config is displayed.

```
R1(config)#banner motd #Unauthorized Use Prohibited#
```

f. Configure the router to not attempt to resolve host names using a DNS server. If this is not configured, the router assumes that any mistyped command is a host name and attempts to resolve it by looking for a DNS server. On some routers, it can take considerable time before the prompt returns.

```
R1(config)#no ip domain lookup
```

g. Configure the router so that console messages do not interfere with command input. This is helpful when exiting configuration mode, because it returns you to the command prompt and prevents having messages from breaking into the command line.

```
R1(config)#line console 0
R1(config-line)#logging synchronous
```

Step 3: View 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
!
no ip domain lookup
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
banner motd ^CUnauthorized Use Prohibited^C
!
line con 0
 password cisco
 logging synchronous
 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.

In global configuration mode, configure serial interface 0/0/0 on R1. See the Router Interface Summary table at the end of the lab for the proper designation of the serial interface on the router that you are using. Because the R1 serial 0/0/0 interface is acting as the DCE for the WAN link, it is necessary to configure the clock rate. When configuring an interface, always use the **no shutdown** command to enable it.

```
R1(config)#interface serial 0/0/0
R1(config-if)#description WAN link to R2
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-if)#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 is ignored on the router to which the DTE end is attached. The **no shutdown** command turns on the interface. The **shutdown** command turns the interface off.

Step 5: Display information about the serial interface on R1.

a. Enter the **show interfaces** command on R1.

```
R1#show interfaces serial 0/0/0

Serial0/0/0 is down, line protocol is down
  Hardware is PowerQUICC Serial
  Description: WAN link to R2
  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. What did you discover by issuing the **show interfaces** command?

Serial 0/0/0 status is _________ Line protocol is ___________

Internet address _____________________

Encapsulation _______________

To which OSI layer is the encapsulation referring? ________________

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

____

Step 6: Configure the serial interface on R2.

In global configuration mode, configure serial 0/0/0 on router R2. See the Router Interface Summary table at the end of the lab for the proper designation of the serial interface on the router that you are using.

```
R2(config)#interface serial 0/0/0
R2(config-if)#description WAN link to R1
R2(config-if)#ip address 172.17.0.2 255.255.0.0
R2(config-if)#no shutdown
R2(config-if)##exit
R2(config)#exit
```

Step 7: Display information about the serial interface on R2.

a. Enter the **show interfaces** command on R2.

```
R2#show interfaces serial 0/0/0

Serial0/0/0 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Description: WAN link to R1
  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. What did you discover by issuing the **show interfaces** command?

Serial 0/0/0 status is _________ Line protocol is ___________

Internet address _____________________

Encapsulation _______________

To which OSI layer is the encapsulation referring? ________________

c. Why did the **show interfaces serial 0/0/0** indicate 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 Fast Ethernet interface on R1.

In global configuration mode, configure the Fast Ethernet 0/0 interface on router R1. See the Router Interface Summary table at the end of the lab for the proper designation of the Ethernet interface on the router that you are using.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#description R1 LAN Default Gateway
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 Fast Ethernet interface on R1.

a. Enter the **show interfaces** command on R1.

```
R1#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)
  Description: R1 LAN Default Gateway
  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. What did you discover by issuing the **show interfaces** command?

Fast Ethernet 0/0 status is _________ Line protocol is ___________

Internet address ______________________

Encapsulation ________________

To which OSI layer is the encapsulation referring? _________________

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

____

Step 11: Configure the Fast Ethernet interface on R2.

In global configuration mode, configure the Fast Ethernet 0/0 interface on R2. Refer to the Router Interface Summary table at the end of the lab for the proper designation of the Ethernet interface on the router that you are using.

```
R2(config)#interface FastEthernet 0/0
R2(config-if)#description R2 LAN Default Gateway
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
```

Step 12: Display information about the Fast Ethernet interface on R2.

a. Enter the **show interfaces** command on R2.

```
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)
  Description: R2 LAN Default Gateway
  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. What did you discover by issuing the **show interfaces** command?

Fast Ethernet 0/0 status is _________ Line protocol is ___________

Internet address _____________________

Encapsulation _______________

To which OSI layer is the encapsulation referring? ________________

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

____

Step 13: Save the configuration on both routers.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
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 cycle. The running configuration is lost if it is not saved. The router uses the startup configuration when the router is started.

Step 14: Check both router configurations.

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

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

Step 15: Verify that the Fast Ethernet connection to each router is functioning.

a. On host H1, open a Command Prompt window by choosing **Start > Run** and typing **cmd**. Alternatively, you can choose **Start > All programs > Accessories > Command Prompt**.

b. Use the **ping** command to test connectivity to the Fast Ethernet interface of each router from its associated host computer. From H1, ping the R1 router Fast Ethernet interface.

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

Was the ping successful? _____

From host H2, ping the R2 router Fast Ethernet interface.

```
C:\>ping 172.18.0.1
```

Was the ping successful? ____

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 16: (Optional challenge) Test end-to-end connectivity.

In previous steps, you tested network connectivity by pinging from R1 to the serial interface of R2. You also pinged from each host to its respective default gateway. These pings were successful because, in each case, the source and destination IP addresses were on the same network. Now you will ping from R1 to the R2 Fast Ethernet interface and then from H1 to H2. The source and destination IP addresses for these pings are not on the same network.

a. From R1, ping the R2 Fast Ethernet interface.

```
R1#ping 172.18.0.1
```

Was the ping successful? ____

b. From host H1, use the **ping** command to test end-to-end connectivity from H1 (172.16.0.2) to H2 (172.18.0.2).

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

Was the ping successful? ____

The pings from R1 to the R2 Fast Ethernet interface and from H1 to H2 do not work because router R1 has no knowledge of how to get to the R2 Ethernet network (172.18.0.0). In addition, R2 has no knowledge of the Ethernet network on R1 (172.16.0.0). The pings cannot get from R1 or H1 to the R2 Ethernet network. Even if they could, they could not return. For the pings to work from one host computer to the other, default routes and/or static routes must be configured on the routers, or there must be a dynamic routing protocol set up between them.

Erasing and Reloading the Router

a. Enter 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#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.

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**.

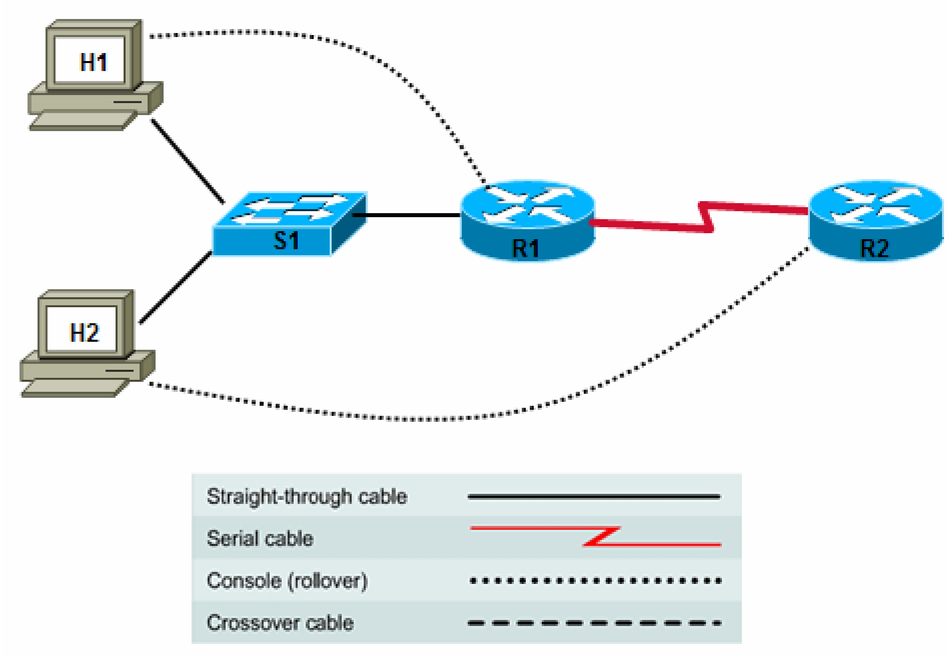
The router is ready for the assigned lab to be performed.

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 5.3.7 Configuring DHCP with SDM and the Cisco IOS CLI



Device	Host Name	Interface	IP Address	Subnet Mask
R1	Customer	Serial 0/0/1 (DTE)	209.165.200.225	255.255.255.224
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0
R2	ISP	Serial 0/0/0 (DCE)	209.165.200.226	255.255.255.224

Objectives

- Configure a customer router for DHCP using SDM.
- Configure a customer router for DHCP using the Cisco IOS CLI.
- Configure a DHCP client.
- Verify DHCP functionality.

Background / Preparation

In this lab, you set up a customer router to act as a DHCP server for internal client computers. DHCP assigns an address, subnet mask, and default gateway to hosts dynamically from a defined pool of addresses.

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 determine which 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.

Required Resources

The following resources are required:

- Cisco 1841 ISR router (or comparable) with SDM version 2.4 or above installed to act as the customer router
- Cisco 1841 router (or other router) to act as the ISP router
- Cisco 2960 switch (or other switch/hub) to connect hosts H1, H2, and the customer router
- Windows XP computer (host H1) with Internet Explorer 5.5 or later and Sun Java Runtime Environment (JRE) version 1.4.2_05 or later (or Java Virtual Machine (JVM) 5.0.0.3810)
- Windows XP computer (host H2)
- Straight-through Category 5 Ethernet cables
- Null serial cable (R1 to R2)
- Console cables (H1 to R1 and H2 to R2)
- Access to the host H1 and H2 command prompt
- Access to the host H1 and H2 network TCP/IP configuration

From hosts H1 and H2, start a HyperTerminal session with each router.

Note: Make sure that the routers and the switch have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Configure Basic Router Settings

Step 1: Build the network and configure host computer IP settings.

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

Note: A router other than the 1841 may require a connection to a port other than Fast Ethernet 0/0 to access SDM.

b. Configure host H1 with the following static IP information.

IP address: 192.168.1.101
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

c. Configure host H2 as a DHCP client. Choose **Start > Settings > Control Panel > Network Connections > Local Area Connection**. Click the **Properties** button and then **Internet Protocol (TCP/IP) Properties**. Select the options **Obtain an IP address automatically** and **Obtain a DNS server address automatically**.

d. On hosts H1 and H2, open a command prompt. Click **Start > Run,** and then type **cmd** and press **Enter**. Alternatively, choose **Start > All Programs > Accessories > Command Prompt**. Issue the **ipconfig /all** command. Record the MAC addresses for H1 and H2.

Host H1 MAC address ________________________

Host H2 MAC address ________________________

Step 2: Configure the customer router basic settings with the Cisco IOS CLI.

Configure the host name, passwords, interfaces, and HTTP service in preparation for the use of SDM. Also configure a default route to the ISP.

```
Router>enable
Router#config t
Router(config)#hostname Customer
```

```
Customer(config)#enable secret class
Customer(config)#username admin privilege 15 secret cisco123
Customer(config)#no ip domain-lookup
Customer(config)#line con 0
Customer(config-line)#password cisco
Customer(config-line)#logging synchronous
Customer(config-line)#login
Customer(config-line)#line vty 0 4
Customer(config-line)#password cisco
Customer(config-line)#login
Customer(config-line)#exit
Customer(config)#interface FastEthernet0/0
Customer(config-if)#description LAN Default Gateway
Customer(config-if)#ip address 192.168.1.1 255.255.255.0
Customer(config-if)#no shutdown
Customer(config-if)#interface Serial0/0/1
Customer(config-if)#ip address 209.165.200.225 255.255.255.224
Customer(config-if)#description WAN link to ISP
Customer(config-if)#no shutdown
Customer(config-if)#exit
Customer(config)#ip http server
Customer(config)#ip http authentication local
Customer(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

Step 3: Configure ISP router basic settings with the Cisco IOS CLI.

Configure the host name, passwords, and interfaces.

```
Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#exit
ISP(config)#interface serial 0/0/0
ISP(config-if)#description WAN link to Customer
ISP(config-if)#ip address 209.165.200.226 255.255.255.224
ISP(config-if)#clock rate 64000
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#ip http server
ISP(config)#exit
```

Step 4: Save the router configurations.

From privileged EXEC mode, save the running configuration to the startup configuration.

```
Customer#copy running-config startup-config
ISP#copy running-config startup-config
```

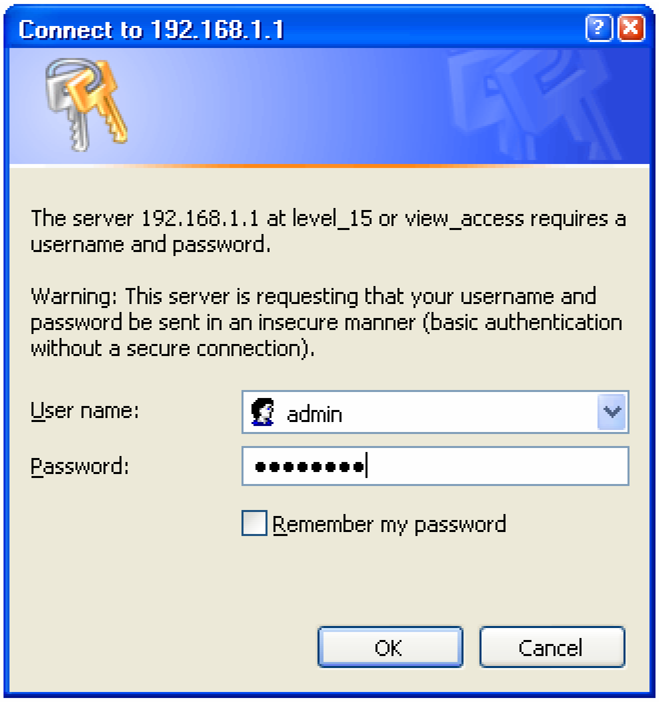
Step 5: Connect to Customer with host H1 using SDM.

a. On H1, disable any popup blocker programs. Popup blockers prevent SDM windows from displaying.

b. The SDM GUI does not load automatically on the router. You must open a web browser to access SDM. Go to http://192.168.1.1. (The IP address of the Customer FastEthernet 0/0 interface – the H1 default gateway)

   Note: If the browser cannot connect, check the cabling and connections and make sure that the PC IP configuration is correct.

c. In the **Connect to** dialog box, enter **admin** for the username, and **cisco123** for the password. The login information was configured in Step 2. Click **OK**. The main SDM web application starts. If you are prompted to use HTTPS, click **Cancel**. If a Security Warning window displays, click **Yes** to trust the Cisco application.



Connect to 192.168.1.1

The server 192.168.1.1 at level_15 or view_access requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

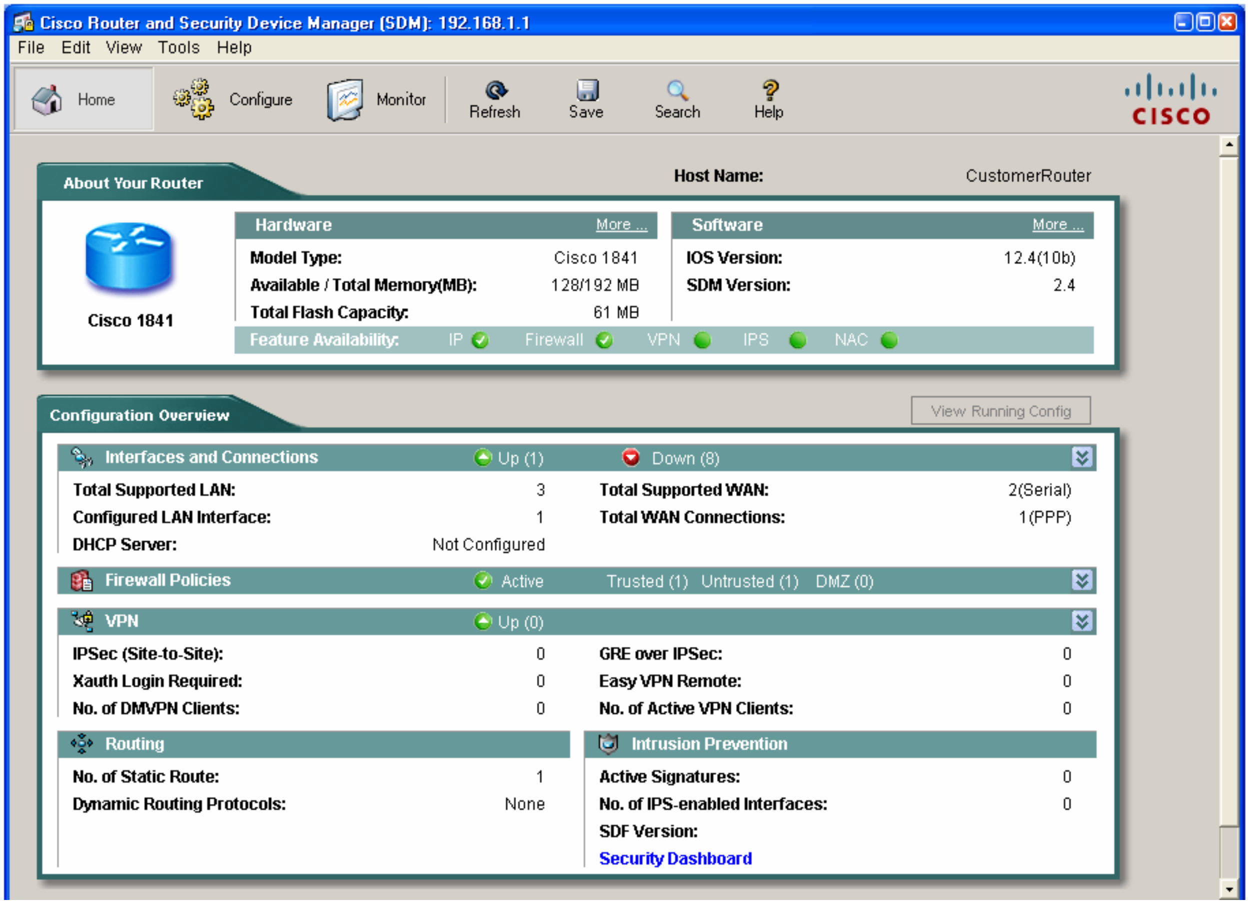
User name: admin

Password: ●●●●●●●●●

□ Remember my password

d. Verify that you are using SDM 2.4 or later. The initial SDM screen that displays immediately after the login shows the current version number. It is also displayed on the main SDM screen as shown below, along with the Cisco IOS version.

   Note: If the version is not 2.4 or later, notify the instructor before continuing with this lab. You must download the latest zip file from the SDM web page and save it to the PC. From the Tools menu of the SDM GUI, choose **Update SDM** to specify the location of the zip file and install the update.



Host Name: CustomerRouter

Hardware	
Model Type:	Cisco 1841
Available / Total Memory(MB):	128/192 MB
Total Flash Capacity:	61 MB

Software	
IOS Version:	12.4(10b)
SDM Version:	2.4

Feature Availability: IP ✓ Firewall ✓ VPN ● IPS ● NAC ●

Interfaces and Connections ● Up (1) ● Down (8)

Total Supported LAN:	3	Total Supported WAN:	2(Serial)
Configured LAN Interface:	1	Total WAN Connections:	1(PPP)
DHCP Server:	Not Configured		

Firewall Policies ✓ Active Trusted (1) Untrusted (1) DMZ (0)

VPN ● Up (0)

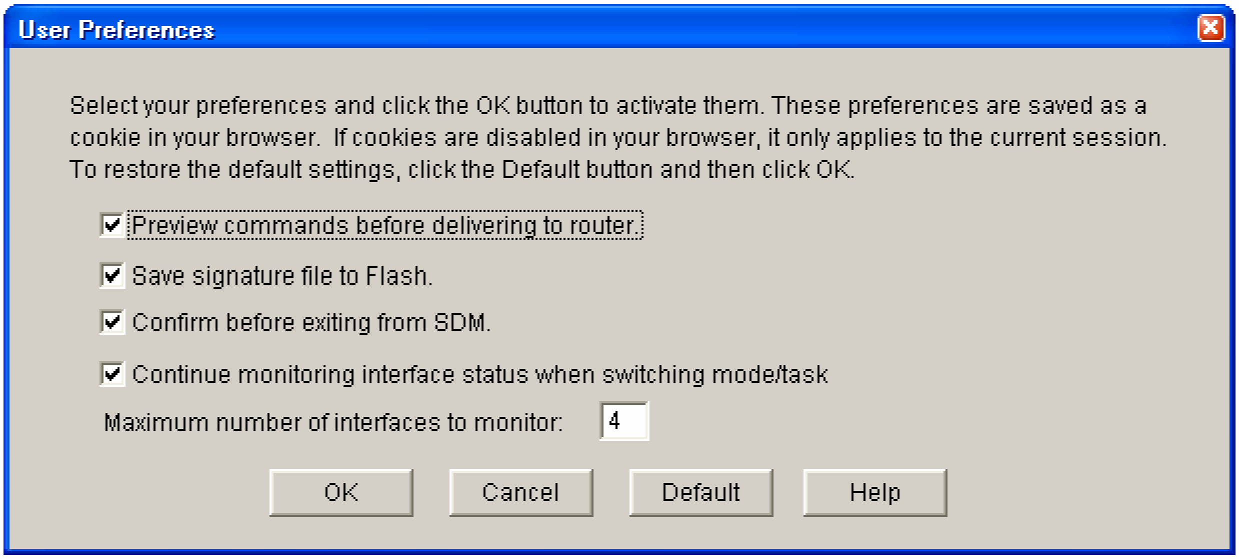
IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

Routing		Intrusion Prevention	
No. of Static Route:	1	Active Signatures:	0
Dynamic Routing Protocols:	None	No. of IPS-enabled Interfaces:	0
		SDF Version:	
		Security Dashboard	

Step 6: Configure SDM to show the Cisco IOS CLI commands.

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

b. Check the **Preview commands before delivering to router** box. When this option is checked, you can view the Cisco IOS CLI configuration commands before they are sent to the router, which is a good way to learn about the commands used.



Select your preferences and click the OK button to activate them. These preferences are saved as a cookie in your browser. If cookies are disabled in your browser, it only applies to the current session. To restore the default settings, click the Default button and then click OK.

☑ Preview commands before delivering to router.

☑ Save signature file to Flash.

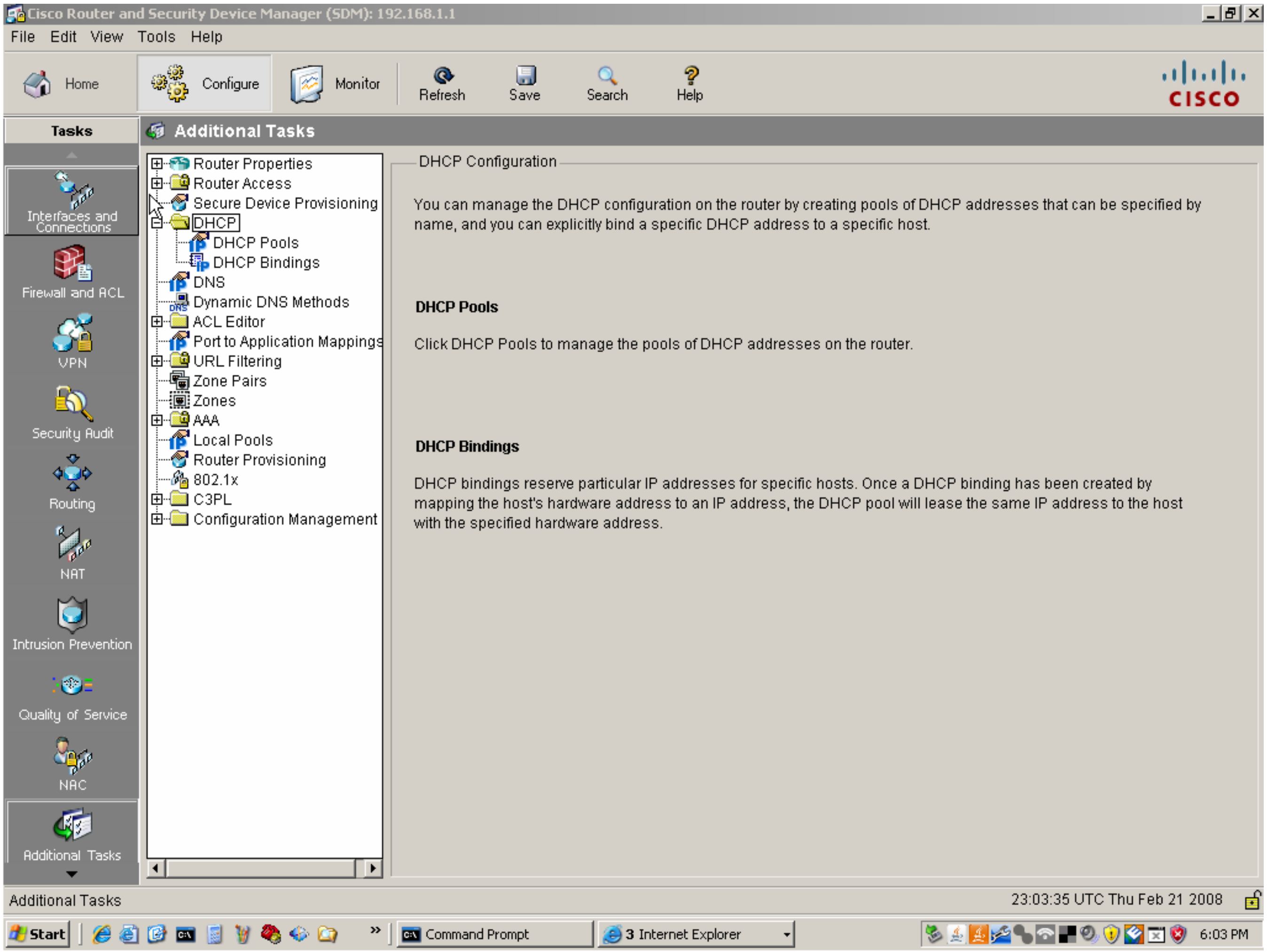
☑ Confirm before exiting from SDM.

☑ Continue monitoring interface status when switching mode/task

Maximum number of interfaces to monitor: 4

Step 7: Select additional tasks from the Configure menu.

a. Click the **Configure** button at the top of the SDM window and select **Additional Tasks** from the Task menu at the left of the screen. In the Additional Tasks menu, click the plus sign (+) next to DHCP to expand the menu, and then click **DHCP Pools**.



DHCP Configuration

You can manage the DHCP configuration on the router by creating pools of DHCP addresses that can be specified by name, and you can explicitly bind a specific DHCP address to a specific host.

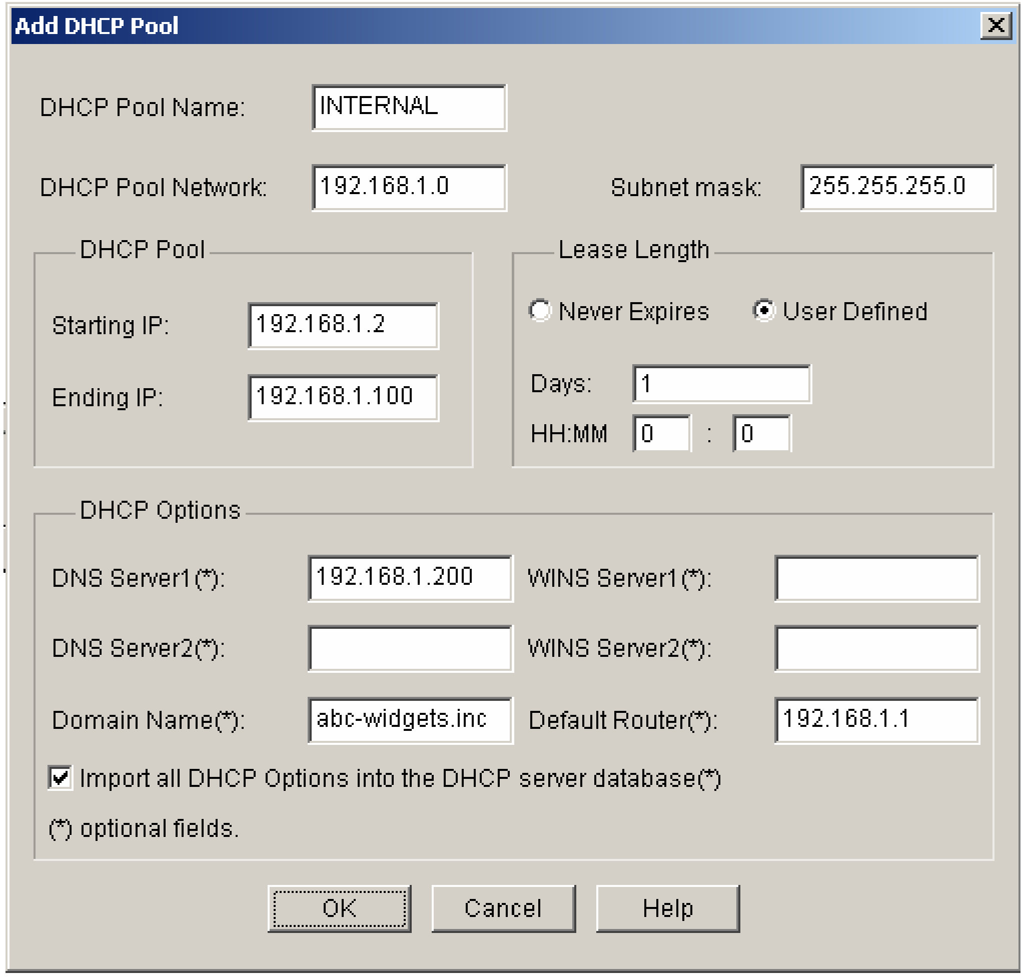
DHCP Pools

Click DHCP Pools to manage the pools of DHCP addresses on the router.

DHCP Bindings

DHCP bindings reserve particular IP addresses for specific hosts. Once a DHCP binding has been created by mapping the host's hardware address to an IP address, the DHCP pool will lease the same IP address to the host with the specified hardware address.

b. In the DHCP Pools screen, click the **Add** button to create a new DHCP pool. Enter the values shown in the following screen to define the DHCP pool name, network, subnet mask, start and end of the IP address range, DNS server address, domain name, and default gateway router. Click **OK** when you have entered all the values.



DHCP Pool Name: INTERNAL

DHCP Pool Network: 192.168.1.0 Subnet mask: 255.255.255.0

DHCP Pool

Starting IP: 192.168.1.2

Ending IP: 192.168.1.100

Lease Length

○ Never Expires ● User Defined

Days: 1

HH:MM 0 : 0

DHCP Options

DNS Server1(*): 192.168.1.200

WINS Server1(*):

DNS Server2(*):

WINS Server2(*):

Domain Name(*): abc-widgets.inc

Default Router(*): 192.168.1.1

☑ Import all DHCP Options into the DHCP server database(*)

(*) optional fields.

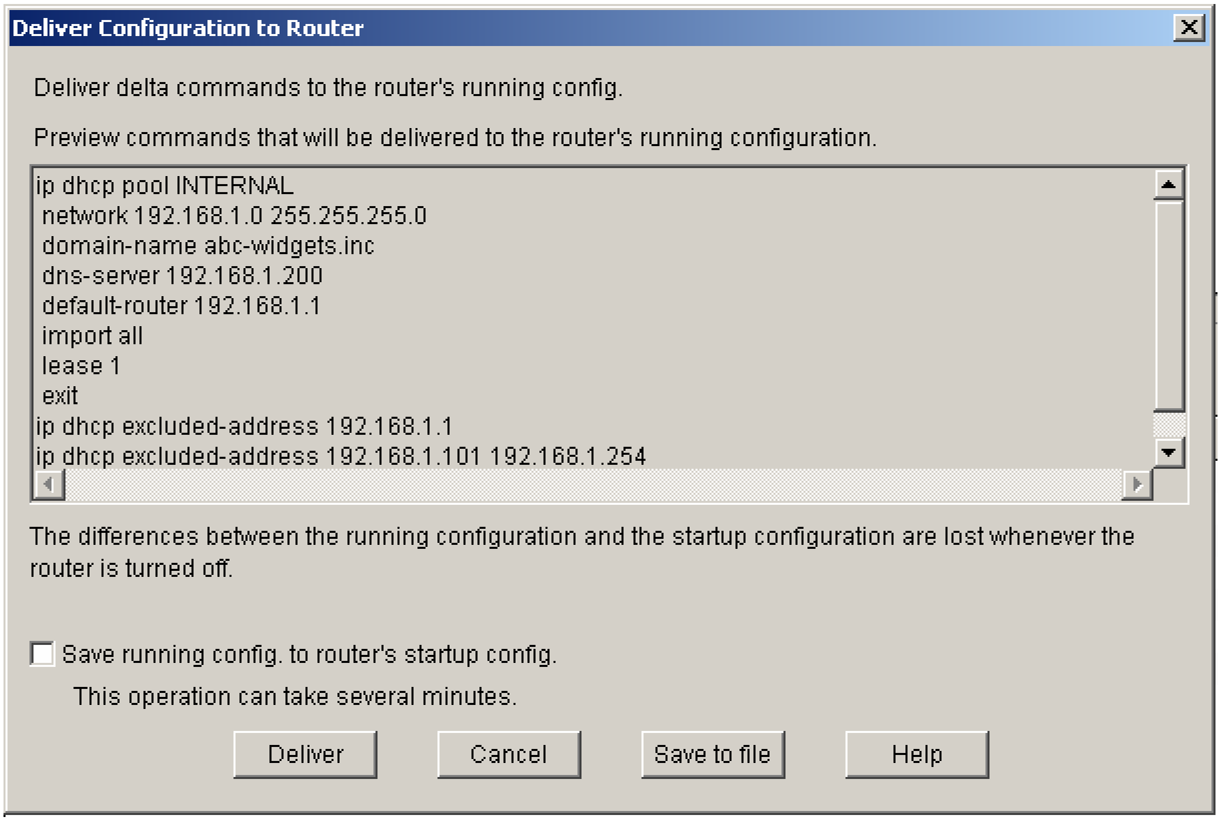
c. Why is the starting IP address set to 192.168.1.2 instead of 192.168.1.1?

____

____

d. In the **Deliver Configuration to Router** window, review the CLI commands that were generated by the SDM. These are the commands that are delivered to the router to configure DHCP. The commands can also be manually entered from the CLI to accomplish the same task, which you will do in Task 2 of this lab. Do *not* check the box **Save running config to router's startup config**. Click **Deliver** to finish configuring the router.

Note: By default, the commands that you just generated only update the running configuration file when delivered. When finished configuring the router for DHCP with SDM, you will configure DHCP using the CLI. When you restart the router, you want it to revert back to the configuration that you saved in Step 2.



Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

```
ip dhcp pool INTERNAL
 network 192.168.1.0 255.255.255.0
 domain-name abc-widgets.inc
 dns-server 192.168.1.200
 default-router 192.168.1.1
 import all
 lease 1
 exit
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.101 192.168.1.254
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

□ Save running config. to router's startup config.

This operation can take several minutes.

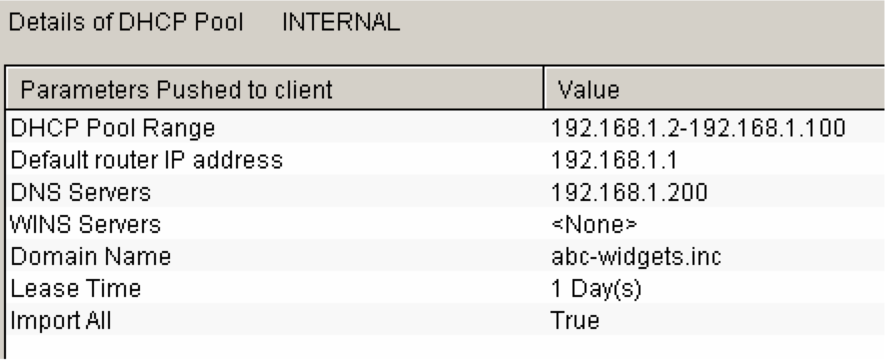
e. What is the purpose of the last two commands in this configuration?

____

____

____

f. After the commands are delivered, the final DHCP screen showing the details of the DHCP pool is displayed.



Details of DHCP Pool INTERNAL

Parameters Pushed to client	Value
DHCP Pool Range	192.168.1.2-192.168.1.100
Default router IP address	192.168.1.1
DNS Servers	192.168.1.200
WINS Servers	<None>
Domain Name	abc-widgets.inc
Lease Time	1 Day(s)
Import All	True

g. Choose **File > Exit** from the SDM main menu to end the SDM session. Click **Yes** to confirm exiting SDM.

Step 8: Test the DHCP pool configuration with SDM.

a. On the customer host H2, open a command prompt, and issue the **ipconfig** command.

b. What IP address is issued to H2? ___________________________

c. From host H1, ping the default gateway (the router Ethernet interface). Does the ping succeed? _______

Troubleshoot as necessary, and do not proceed until the ping is successful.

Task 2: Configure and Verify DHCP Using the CLI

Step 1: Restart the Customer router to remove the DHCP commands added by SDM.

a. Because you did not save the DHCP configuration created using SDM to NVRAM, restarting the router restores the basic configuration created in Task 1, Step 2. On the Customer router, issue the **reload** command.

b. When prompted to save the configuration, respond with **no**.

c. When prompted with **Proceed with reload? [confirm]**, press **Enter**.

d. Press Enter at the **Press RETURN to get started!** prompt. You should now see the **Customer>** prompt.

Step 2: Check the host DHCP client H2 IP configuration.

a. Open a command prompt window on H2 and issue the **ipconfig /release** and **ipconfig /renew** commands. Because there is no DHCP server currently configured, it may take a while to timeout.

b. At the command prompt, now issue the **ipconfig** command. What is the IP address and subnet mask for H2?

____

Step 3: Configure the DHCP server excluded addresses on the Customer router.

To prevent certain addresses from being assigned they must be excluded from the pool. This includes the IP address of the router Fast Ethernet 0/0 interface (the default gateway). In this lab, also exclude addresses from 192.168.1.101 through 192.168.1.254 to reserve them for other purposes, such as servers and printers, which need to have a fixed IP address.

a. To exclude addresses, issue the **ip dhcp excluded-address** command.

```
Customer(config)#ip dhcp excluded-address 192.168.1.1
Customer(config)#ip dhcp excluded-address 192.168.1.101 192.168.1.254
```

b. Why do you want to exclude addresses before the DHCP pool is even created?

____

____

Step 4: Configure the DHCP pool.

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

```
Customer(config)#ip dhcp pool INTERNAL
Customer(dhcp-config)#network 192.168.1.0 255.255.255.0
Customer(dhcp-config)#domain-name abc-widgets.inc
Customer(dhcp-config)#default-router 192.168.1.1
Customer(dhcp-config)#dns-server 192.168.1.200
```

Step 5: Test the DHCP pool for H2.

a. On H2, open a command prompt and issue the **ipconfig /release** and **ipconfig /renew** commands.

b. On H2, issue the **ipconfig /all** command.

c. What IP address is issued to H2? ___________________________

d. What is the subnet mask of H2? ____________________________.

e. What is the default gateway of H2? ____________________________

f. What is the connection-specific DNS suffix (domain name) of host H2? __________________________

g. What is the DHCP server IP address? ____________________________

h. What is the DNS server IP address? ____________________________

i. What is the MAC address of H2? ______________________________

j. From H2, 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 6: Test the DHCP pool for H1.

a. On H1, choose **Start > Settings > Control Panel > Network Connections > Local Area Connection** and change the IP configuration from static to dynamic to make H1 a DHCP client like host H2. Click the **Properties** button, and then click **Internet Protocol (TCP/IP) Properties**. Select **Obtain an IP address automatically** and **Obtain a DNS server address automatically**. Click **OK** to exit the configuration window.

b. Open a command prompt on H1 and issue the **ipconfig /release** and **ipconfig /renew** commands. Because there is no DHCP server currently configured, it may take a while to timeout.

c. At the command prompt, now issue the **ipconfig** command.

d. What IP address is issued to H1? ____________________________

Step 7: Display the DHCP binding on the Customer router.

a. To see the IP address and host hardware (MAC) address combination assigned by the DHCP server, 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  Feb 22 2008 11:19 AM    Automatic
192.168.1.3   0100.07e9.63ce.53  Feb 22 2008 11:27 AM    Automatic
```

b. Do the hardware addresses displayed match those recorded for hosts H1 and H2 in Task 1, Step 1? ______

c. On the Customer router, display the characteristics of the DHCP pool using the **show ip dhcp pool** command**.**

```
Customer#show ip dhcp pool
Pool INTERNAL :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 2
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index    IP address range              Leased addresses
 192.168.1.4      192.168.1.1 - 192.168.1.254     2
```

d. How many addresses have been leased? ______

e. In the output from the command, what do you think **Current Index** means?

____

Step 8: Reflection

a. What are some advantages and disadvantages of using DHCP?

____

____

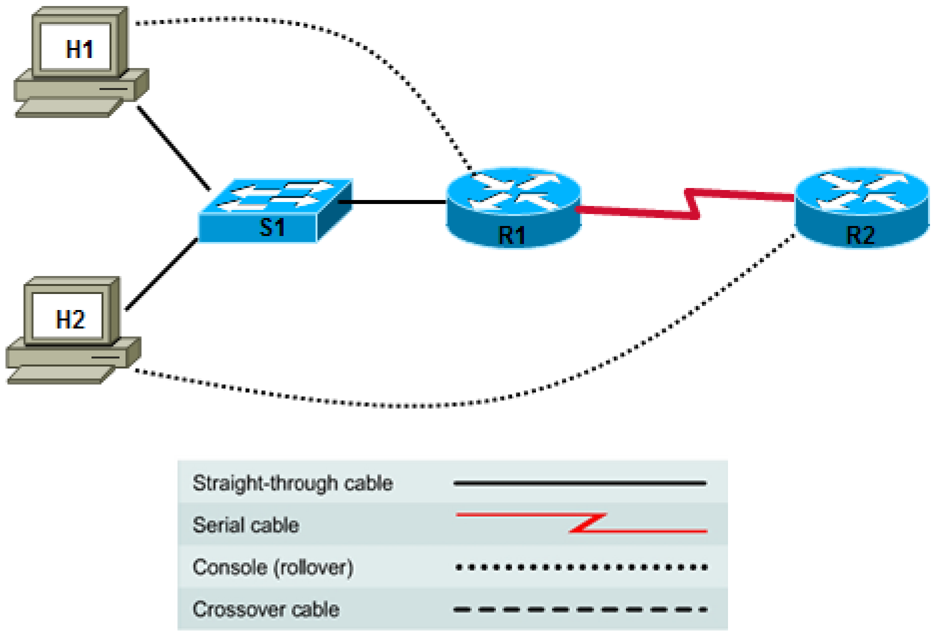
b. What are some advantages and disadvantages of using SDM to configure DHCP on a router as compared to the CLI?

____

____

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 5.3.8 Configuring PAT with SDM and Static NAT using Cisco IOS Commands



Device	Host Name	Interface	IP Address	Subnet Mask
R1	CustomerRouter	Serial 0/0/0 (DTE)	209.165.200.225	255.255.255.224
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0
R2	ISP	Serial 0/0/0 (DCE)	209.165.200.226	255.255.255.224

Objectives

- Configure basic router settings using the Cisco IOS CLI.
- Configure NAT Port Address Translation (PAT) with the Cisco SDM Basic NAT wizard.
- Verify NAT translations using Cisco IOS commands.
- Configure and verify static NAT using Cisco IOS commands.

Background / Preparation

In Task 1 of this lab, you use the Cisco SDM Basic NAT wizard to configure Network Address Translation (NAT) using a single external global IP address. This address can support connections to the Internet from many internal private addresses. This is also referred to as NAT Overload or Port Address Translation (PAT).

In Task 2, you use Cisco IOS commands to configure the customer router for static NAT to permanently map a public address to an internal server private address.

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.

The following resources are required:

- Cisco 1841 ISR router (or comparable) with SDM version 2.4 or later installed to act as the customer router
- Cisco 1841 router (or other router) to act as the ISP router
- Cisco 2960 switch (or other switch/hub) to connect hosts H1, H2, and the customer router
- Windows XP computer (host H1) 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)
- Windows XP computer (host H2)
- Straight-through Category 5 Ethernet cables
- Null serial cable (R1 to R2)
- Console cables (H1 ro R1 and H2 to R2)
- Access to the host H1 and H2 command prompt
- Access to the host H1 and H2 network TCP/IP configuration

From each host computer, start a HyperTerminal session to the attached router.

Note: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Configure Basic Router Settings and PAT

Step 1: Build the network and configure host computer IP settings.

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

Note: A router other than the 1841 may require a host connection to a port other than Fast Ethernet 0/0 to access SDM.

b. Configure the hosts with static IP addresses using the following settings.

Host H1:
IP address: 192.168.1.5
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

Host H2:
IP address: 192.168.1.9

Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1

Step 2: Configure the customer router basic settings with the Cisco IOS CLI.

Configure the host name, passwords, and interfaces in preparation for the use of SDM.

```
Router>enable
Router#config t
Router(config)#hostname CustomerRouter
CustomerRouter(config)#enable secret class
CustomerRouter(config)#username admin privilege 15 secret cisco123
CustomerRouter(config)#line con 0
CustomerRouter(config-line)#password cisco
CustomerRouter(config-line)#login
CustomerRouter(config-line)#line vty 0 4
CustomerRouter(config-line)#password cisco
CustomerRouter(config-line)#login
CustomerRouter(config-line)#exit
CustomerRouter(config)#interface FastEthernet0/0
CustomerRouter(config-if)#description LAN Default Gateway
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#interface Serial0/0/0
CustomerRouter(config-if)#ip address 209.165.200.225 255.255.255.224
CustomerRouter(config-if)#description WAN link to ISP
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
CustomerRouter(config)#ip http server
CustomerRouter(config)#ip http authentication local
```

Step 3: Configure the ISP router basic settings with the Cisco IOS CLI.

a. Establish a HyperTerminal session with the ISP route and erase the startup configuration using the **erase startup-config** command from the privileged mode prompt. Restart the router using the **reload** command.

b. Configure the host name, passwords, and interfaces.

```
Router>enable
Router#configure terminal
Router(config)#hostname ISP
ISP(config)#enable secret class
ISP(config)#line console 0
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config)#line vty 0 4
ISP(config-line)#password cisco
ISP(config-line)#login
ISP(config-line)#exit
ISP(config)#exit
ISP(config)#interface serial 0/0/0
ISP(config-if)#description WAN link to CustomerRouter
ISP(config-if)#ip address 209.165.200.226 255.255.255.224
ISP(config-if)#clock rate 64000
ISP(config-if)#no shutdown
ISP(config-if)#exit
ISP(config)#ip http server
ISP(config)#exit
```

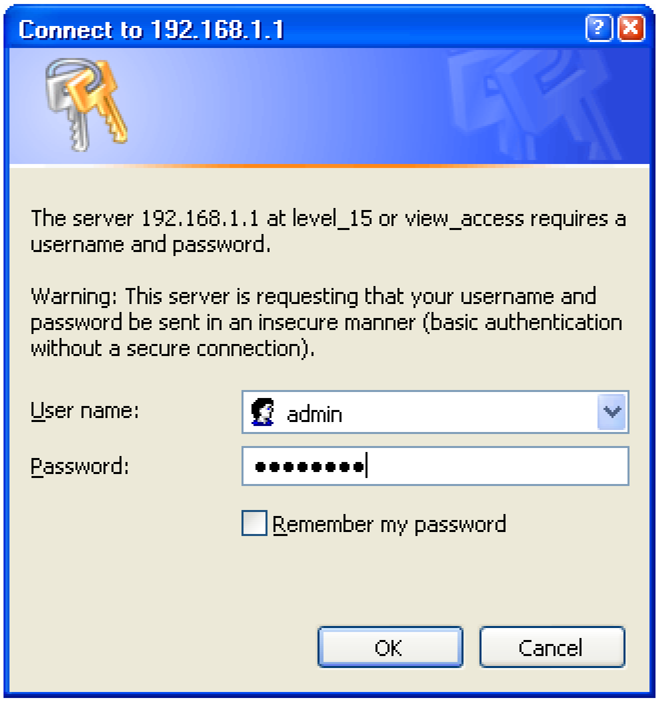
Step 4: Connect to CustomerRouter using SDM.

a. On host H1, disable any popup blocker programs. Popup blockers prevent SDM windows from displaying.

b. The SDM GUI does not load automatically on the router. You must open a web browser to access SDM. Go to http://192.168.1.1.

Note: If the browser cannot connect, check the cabling and connections and make sure that the PC IP configuration is correct.

c. In the **Connect to** dialog box, enter **admin** for the username and **cisco123** for the password. The login information was configured in Step 2. Click **OK**. The main SDM web application starts. If you are prompted to use HTTPS, click **Cancel**. If a Security Warning window displays, click **Yes** to trust the Cisco application.



Connect to 192.168.1.1

The server 192.168.1.1 at level_15 or view_access requires a username and password.

Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

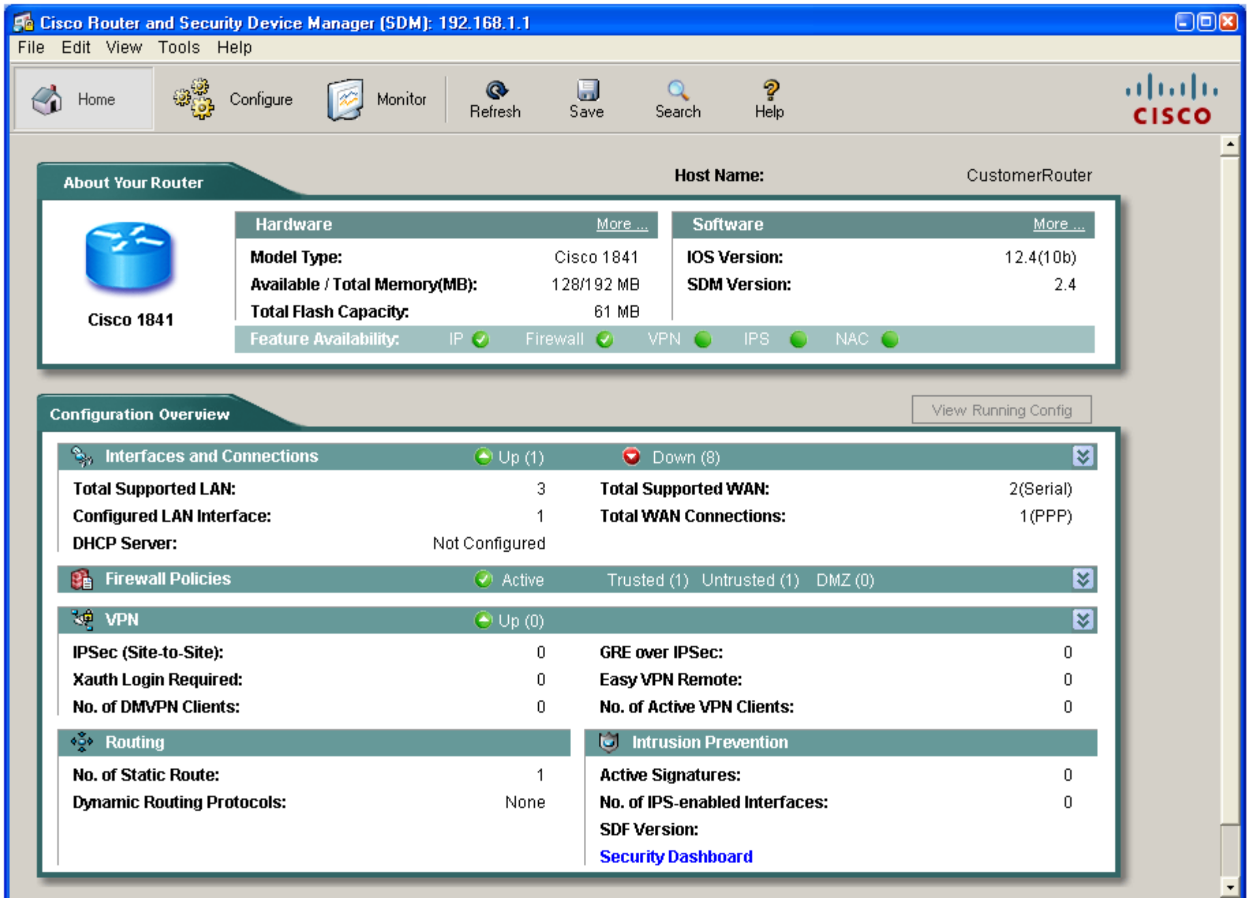
User name: admin

Password: ••••••••

□ Remember my password

d. Verify that you are using SDM 2.4 or later. The initial SDM screen that displays immediately after the login shows the current version number. It is also displayed on the main SDM screen as shown below, along with Cisco IOS version.

Note: If the version is not 2.4 or later, notify the instructor before continuing with this lab. You must download the latest zip file on the host H1 PC. From the Tools menu of the SDM GUI, choose **Update SDM** to specify the location of the zip file and install the update.


Cisco Router and Security Device Manager (SDM): 192.168.1.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
View Running Config

About Your Router

Host Name: CustomerRouter

Cisco 1841

Hardware	More ...
Model Type:	Cisco 1841
Available / Total Memory(MB):	128/192 MB
Total Flash Capacity:	61 MB

Software	More ...
IOS Version:	12.4(10b)
SDM Version:	2.4

Feature Availability: IP ✓ Firewall ✓ VPN ● IPS ● NAC ●

Configuration Overview

Interfaces and Connections — Up (1) Down (8)

Total Supported LAN:	3	Total Supported WAN:	2(Serial)
Configured LAN Interface:	1	Total WAN Connections:	1(PPP)
DHCP Server:	Not Configured		

Firewall Policies — ✓ Active Trusted (1) Untrusted (1) DMZ (0)

VPN — Up (0)

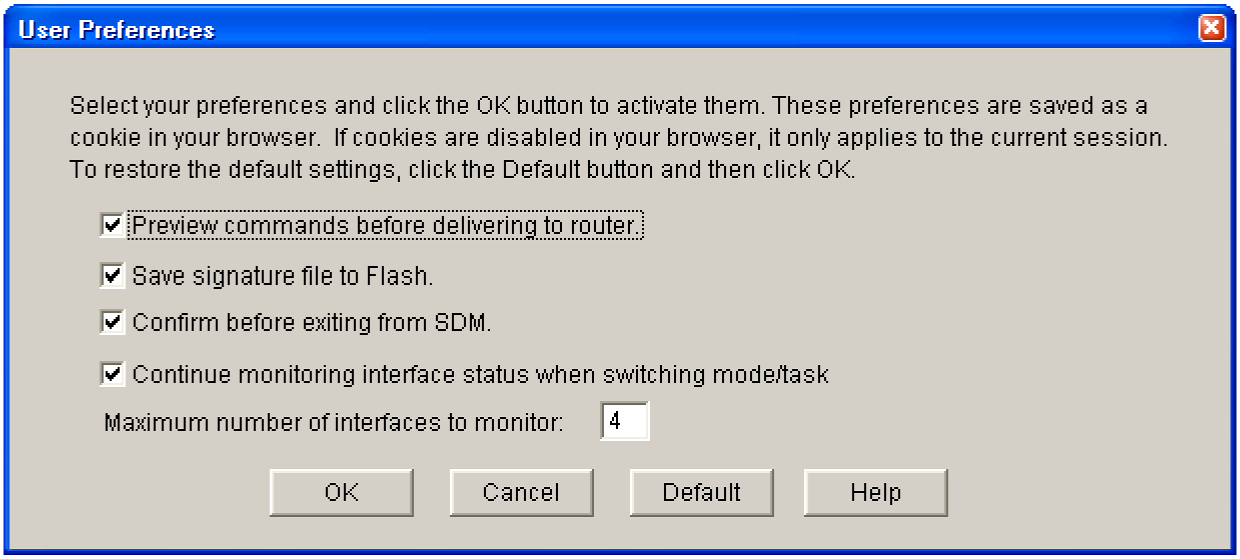
IPSec (Site-to-Site):	0	GRE over IPSec:	0
Xauth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

Routing		Intrusion Prevention	
No. of Static Route:	1	Active Signatures:	0
Dynamic Routing Protocols:	None	No. of IPS-enabled Interfaces:	0
		SDF Version:	
		Security Dashboard	

Step 5: Configure SDM to show the Cisco IOS CLI commands.

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

b. Check the **Preview commands before delivering to router** box. When this option is checked, you can view the Cisco IOS CLI configuration commands before they are sent to the router, which is a good way to learn about the commands used.



User Preferences

Select your preferences and click the OK button to activate them. These preferences are saved as a cookie in your browser. If cookies are disabled in your browser, it only applies to the current session. To restore the default settings, click the Default button and then click OK.

☑ Preview commands before delivering to router.

☑ Save signature file to Flash.

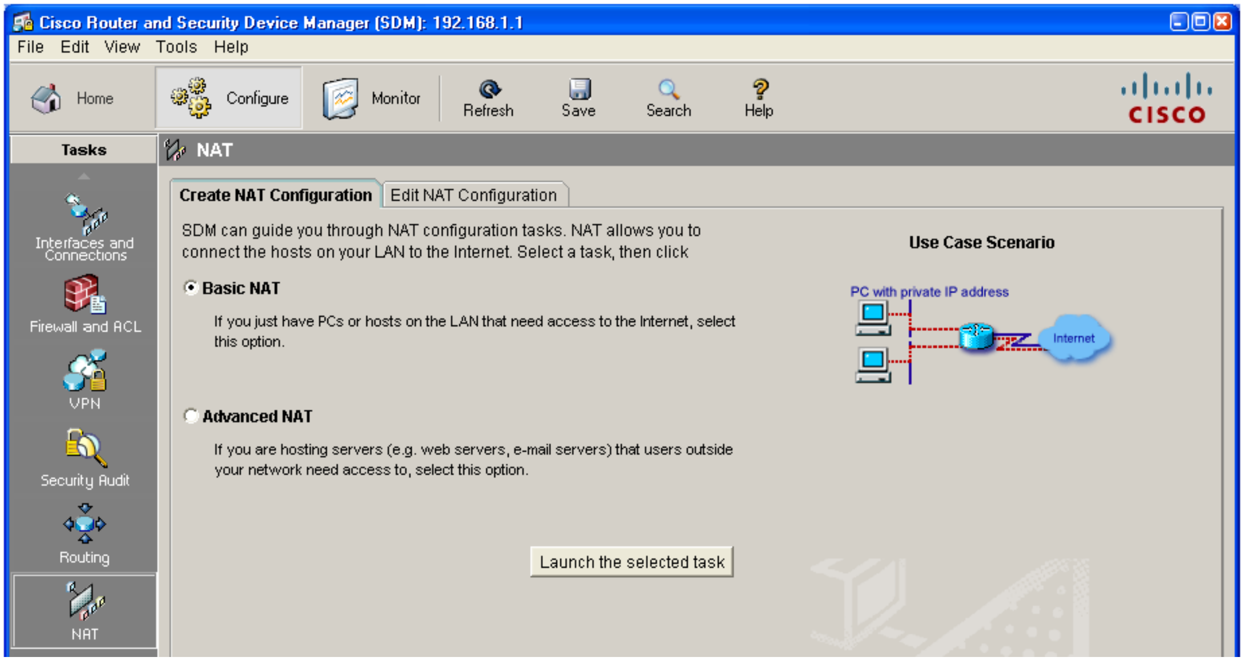
☑ Confirm before exiting from SDM.

☑ Continue monitoring interface status when switching mode/task

Maximum number of interfaces to monitor: 4

Step 6: 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**.



SDM can guide you through NAT configuration tasks. NAT allows you to connect the hosts on your LAN to the Internet. Select a task, then click

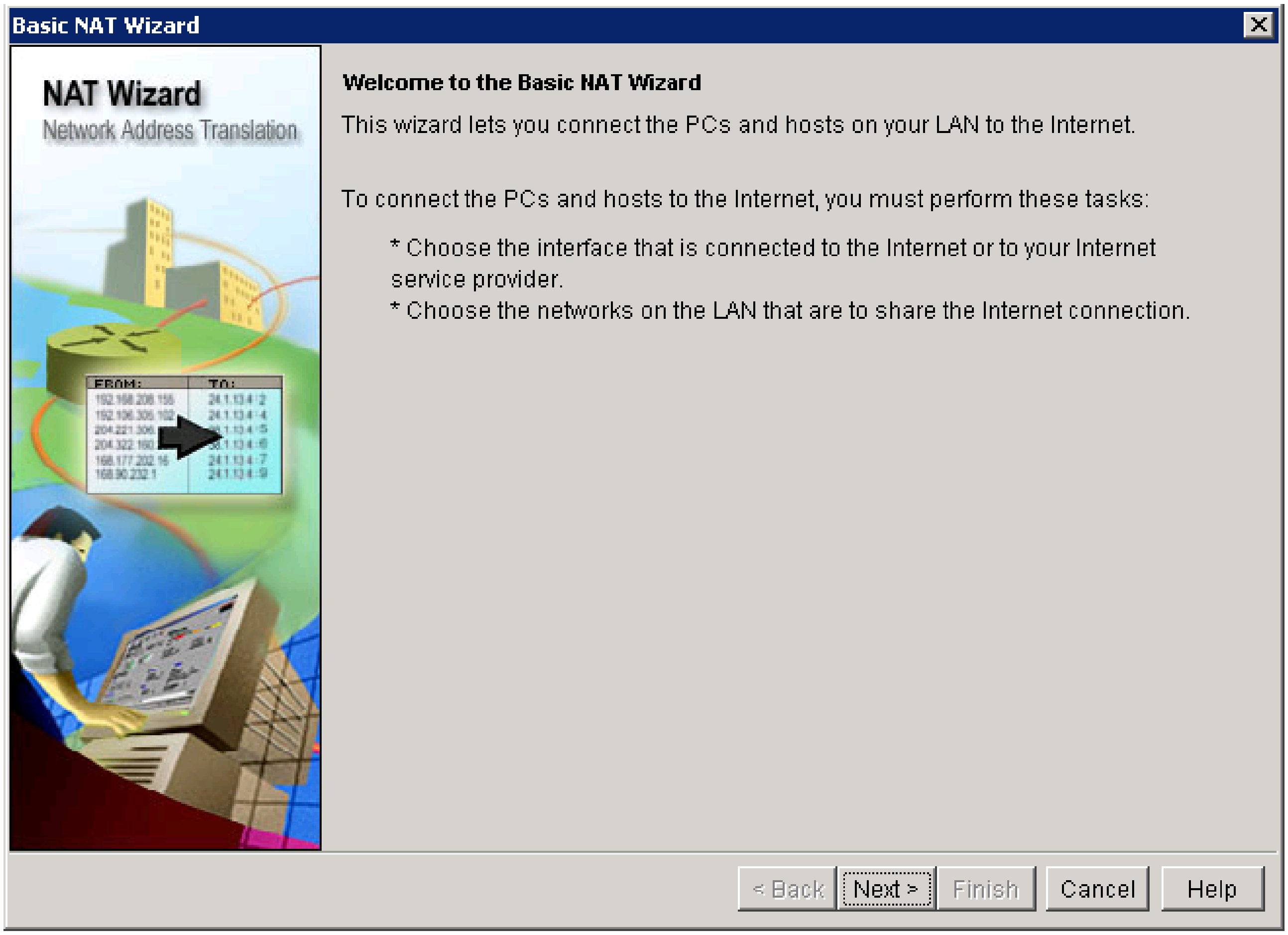
● Basic NAT

If you just have PCs or hosts on the LAN that need access to the Internet, select this option.

○ Advanced NAT

If you are hosting servers (e.g. web servers, e-mail servers) that users outside your network need access to, select this option.

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



Welcome to the Basic NAT Wizard

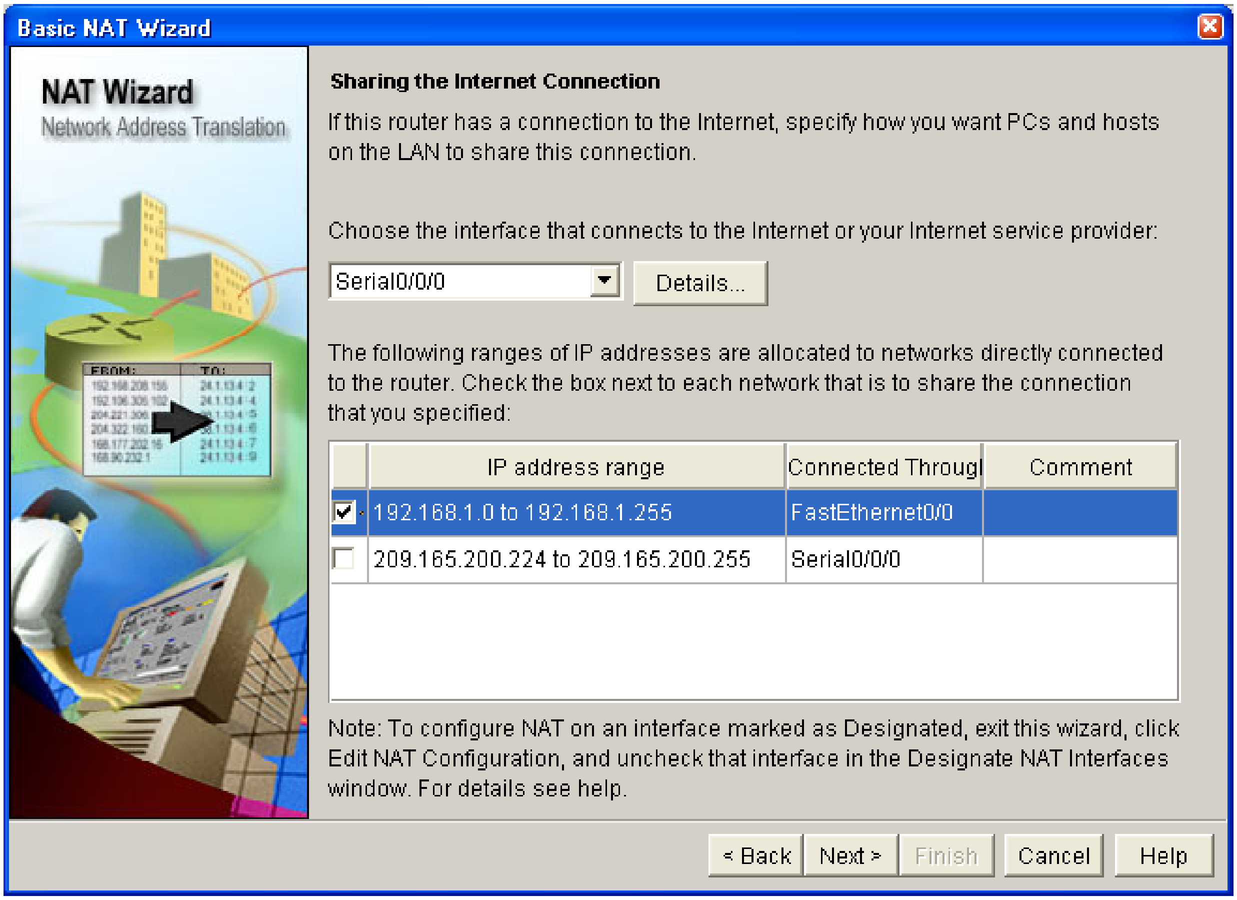
This wizard lets you connect the PCs and hosts on your LAN to the Internet.

To connect the PCs and hosts to the Internet, you must perform these tasks:

* Choose the interface that is connected to the Internet or to your Internet service provider.
* Choose the networks on the LAN that are to share the Internet connection.

Step 7: 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.



Sharing the Internet Connection

If this router has a connection to the Internet, specify how you want PCs and hosts on the LAN to share this connection.

Choose the interface that connects to the Internet or your Internet service provider:

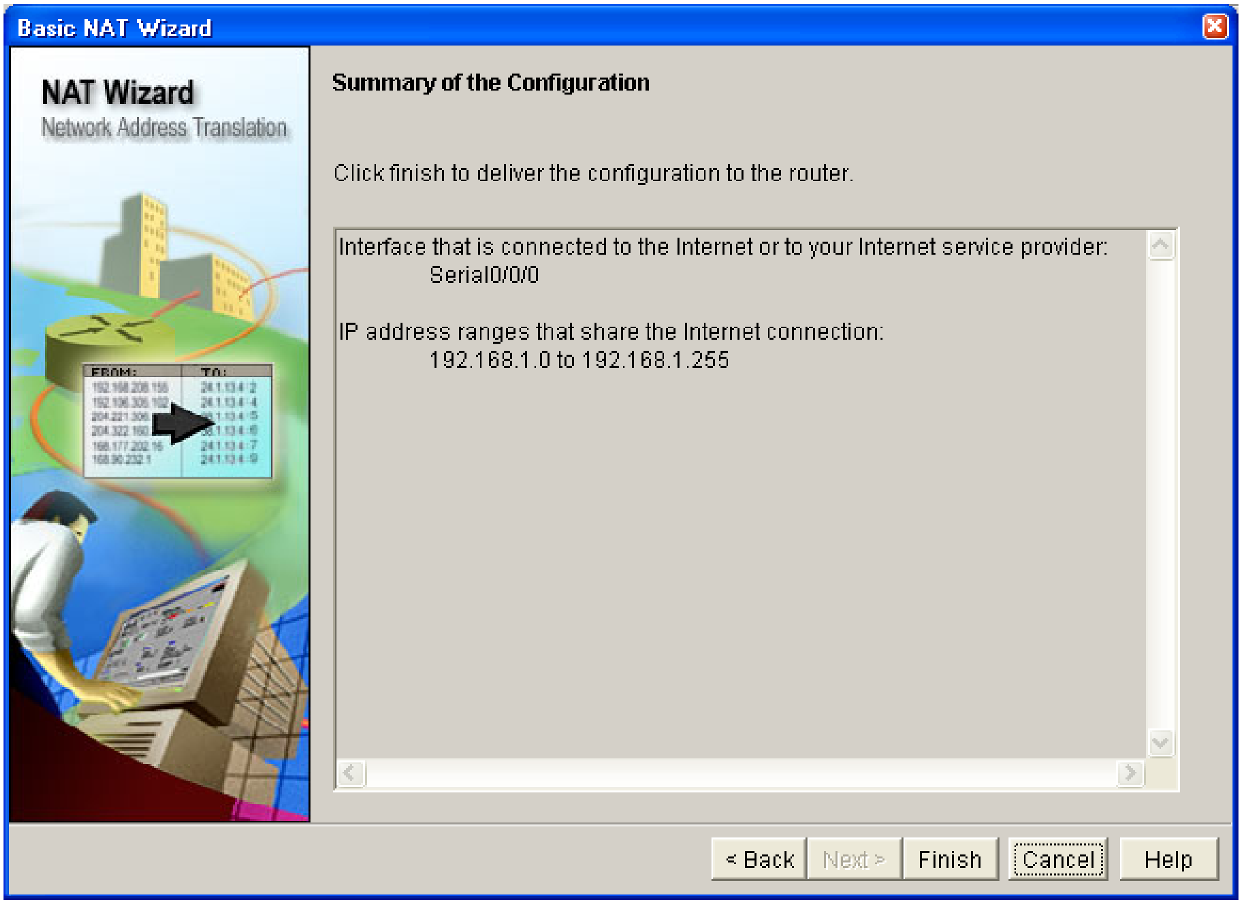
Serial0/0/0

The following ranges of IP addresses are allocated to networks directly connected to the router. Check the box next to each network that is to share the connection that you specified:

	IP address range	Connected Througl	Comment
☑	192.168.1.0 to 192.168.1.255	FastEthernet0/0	
□	209.165.200.224 to 209.165.200.255	Serial0/0/0	

Note: To configure NAT on an interface marked as Designated, exit this wizard, click Edit NAT Configuration, and uncheck that interface in the Designate NAT Interfaces window. For details see help.

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



Summary of the Configuration

Click finish to deliver the configuration to the router.

Interface that is connected to the Internet or to your Internet service provider:
Serial0/0/0

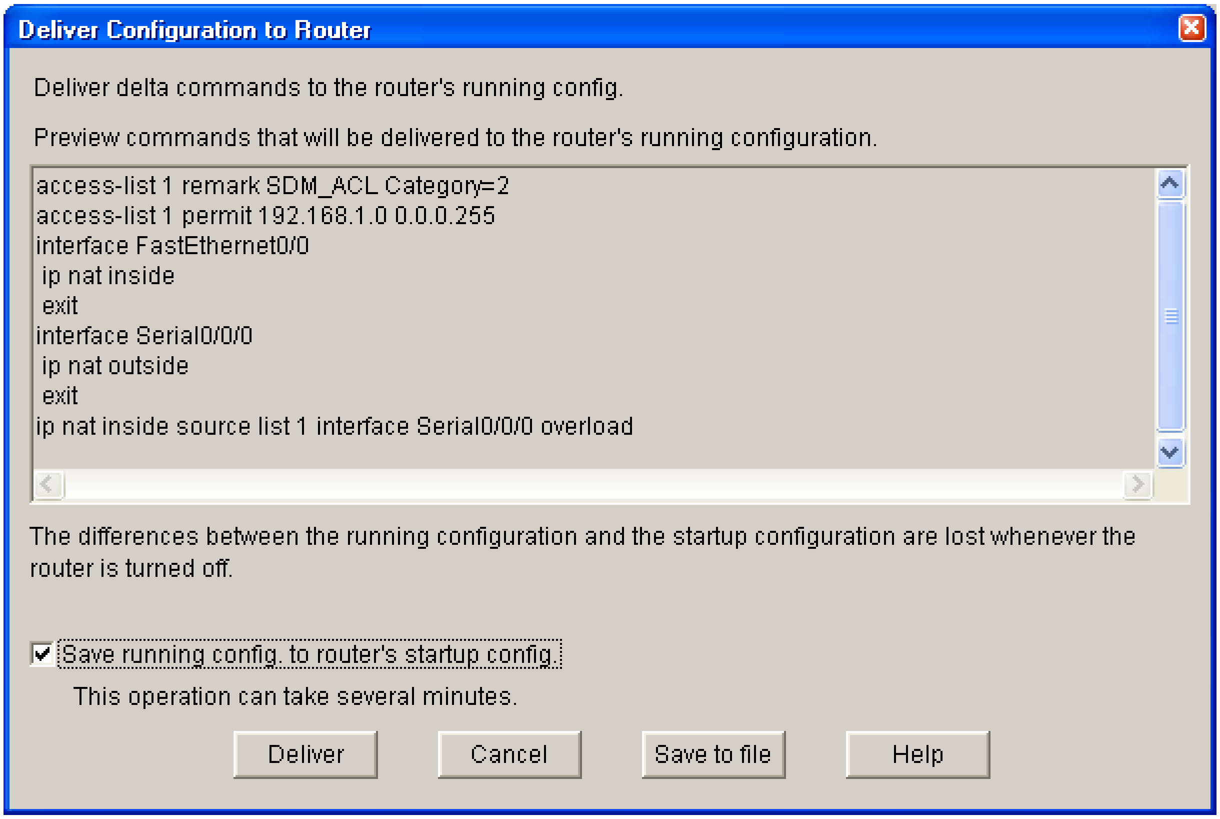
IP address ranges that share the Internet connection:
192.168.1.0 to 192.168.1.255

c. In the **Deliver Configuration to Router** window, review the CLI commands that were generated by the 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 only update the running configuration file when delivered. If the router is restarted, the changes you made are lost. Checking this box updates the startup config file so that when the router is restarted, it loads 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.



Deliver delta commands to the router's running config.

Preview commands that will be delivered to the router's running configuration.

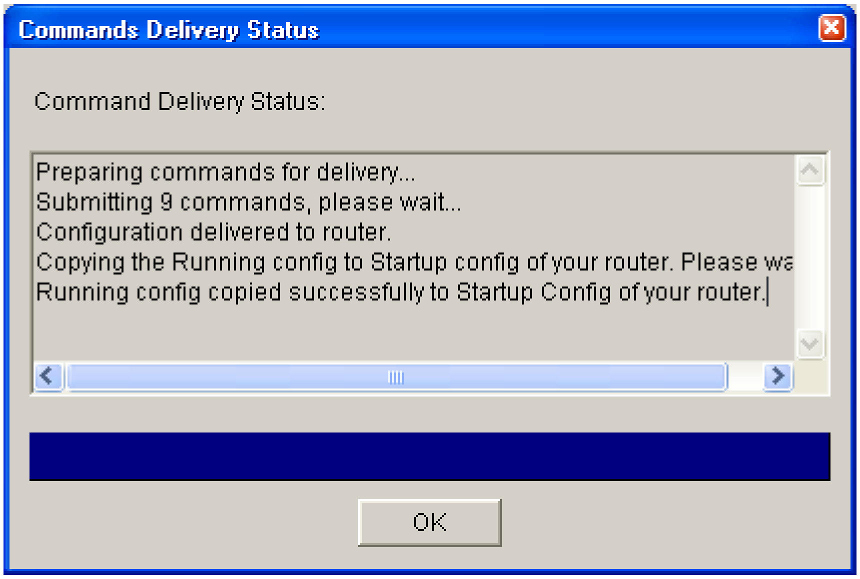
```
access-list 1 remark SDM_ACL Category=2
access-list 1 permit 192.168.1.0 0.0.0.255
interface FastEthernet0/0
 ip nat inside
 exit
interface Serial0/0/0
 ip nat outside
 exit
ip nat inside source list 1 interface Serial0/0/0 overload
```

The differences between the running configuration and the startup configuration are lost whenever the router is turned off.

☑ Save running config. to router's startup config.

This operation can take several minutes.

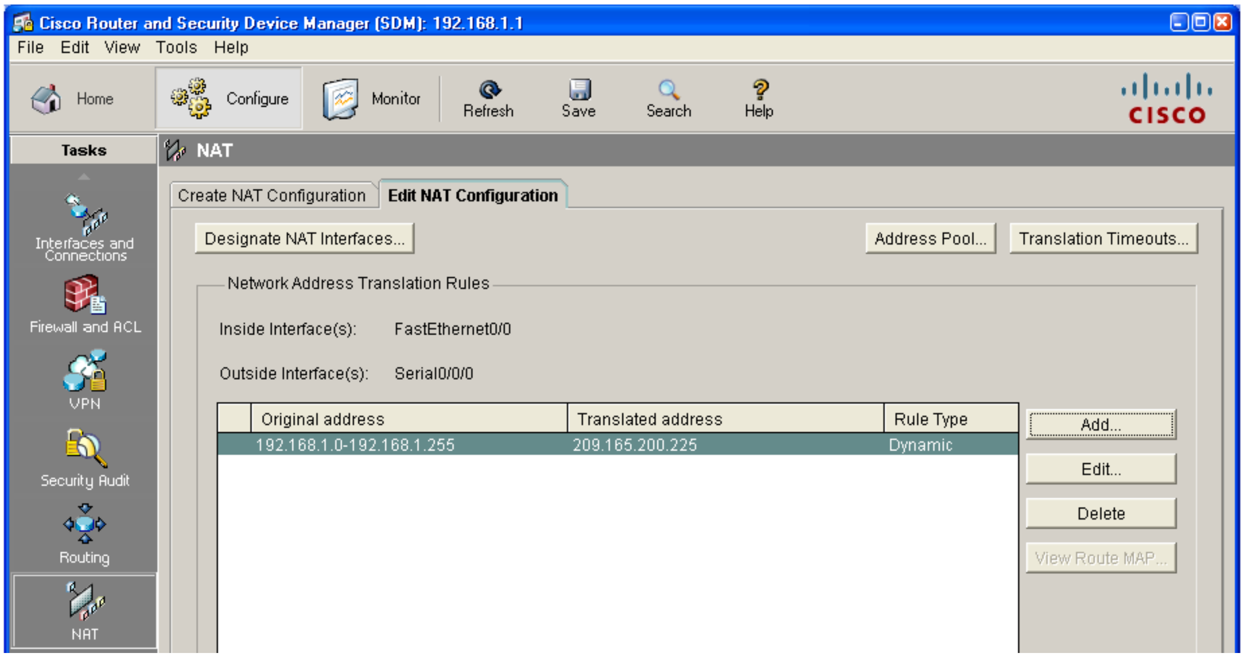
e. In the **Commands Delivery Status** window, notice the text that says that the running config was successfully copied to the startup config. Click **OK** to exit the Basic NAT wizard.



Command Delivery Status:

```
Preparing commands for delivery...
Submitting 9 commands, please wait...
Configuration delivered to router.
Copying the Running config to Startup config of your router. Please wa
Running config copied successfully to Startup Config of your router.
```

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 are translated dynamically to the external public address.



NAT

Network Address Translation Rules

Inside Interface(s): FastEthernet0/0

Outside Interface(s): Serial0/0/0

Original address	Translated address	Rule Type
192.168.1.0-192.168.1.255	209.165.200.225	Dynamic

g. Choose **File > Exit** from the SDM main menu to end the SDM session. Click **Yes** to confirm exiting SDM.

Step 8: Verify NAT functionality.

a. On host H1, open a command prompt window and ping the ISP router serial interface at 209.165.200.226. Are the pings successful? _____

b. From the CustomerRouter terminal window, issue the **show ip nat translations** command to see the H1 internal private address being translated to the serial 0/0/0 external public address.

```
CustomerRouter#show ip nat translations
Pro  Inside global       Inside local     Outside local       Outside global
icmp 209.165.200.225:512 192.168.1.2:512  209.165.200.226:512 209.165.200.226:512
```

c. What type of NAT address is the host H1 IP address? _________________

d. What type of NAT address is the CustomerRouter serial 0/0/0 public IP address? _________________

e. What type of NAT address is the ISP router serial 0/0/0 public IP address? _________________

f. Ping first from H1, and then from H2, in quick succession to the ISP router serial interface at 209.165.200.226. Were the pings successful? _____

g. Use the **show ip nat translations** command to see the H1 internal private address being translated to the serial 0/0/0 external public address.

```
CustomerRouter#show ip nat translation
Pro  Inside global       Inside local     Outside local       Outside global
icmp 209.165.200.225:512 192.168.1.2:512  209.165.200.226:512 209.165.200.226:512
icmp 209.165.200.225:513 192.168.1.9:512  209.165.200.226:512 209.165.200.226:513
```

h. What is the difference between the H1 and H2 translations?

____

i. Use the **clear ip nat translations *** command to clear the router NAT translation table, and issue the **show ip nat translations** command again to verify that they are gone.

```
CustomerRouter#clear ip nat translations *
CustomerRouter#show ip nat translation
```

j. From H1, ping the CustomerRouter serial interface at 209.165.200.225. Are the pings successful? _____

k. From the CustomerRouter terminal window, use the **show ip nat translations** command again to see the address translations.

l. Are there any translations this time? _____ Why?

____

m. On host H1, open a browser such as Internet Explorer, and enter the IP address of the ISP router serial interface at http://209.165.200.226 in the address area. What is the result?

____

n. Display the NAT translation table using the **show ip nat translations** command. Does the translation appear in the NAT table? _____

```
CustomerRouter#show ip nat translations
Pro  Inside global        Inside local      Outside local      Outside global
tcp  209.165.200.225:1059 192.168.1.2:1059  209.165.200.226:80 209.165.200.226:80
---  209.165.200.229      192.168.1.9
```

o. For the translation of the H1 IP inside local address, what is the protocol and the IP address:port number for the outside local and outside global (destination) addresses, and what does the outside port number represent?

____

Task 2: Configure and Verify Static NAT Using the Cisco IOS CLI

Step 1: Configure a static mapping for the server.

Host H2, with IP address 192.168.1.9/24, has been designated as the public web server. Thus, it needs a permanently assigned public IP address. This mapping is defined using a static NAT mapping.

a. To configure a static IP NAT mapping, use the **ip nat inside source static** command.

```
CustomerRouter(config)#ip nat inside source static 192.168.1.9
209.165.200.229
```

This permanently maps public address 209.165.201.229 to 192.168.1.9, the inside address of the web server. Any attempt to access public address 209.165.200.229 is passed by the router to host H2 at private address 192.168.1.9.

b. Display the NAT translation table using the **show ip nat translations** command. Does the static mapping appear in the output of the command? ________

```
CustomerRouter#show ip nat translations
Pro Inside global    Inside local   Outside local   Outside global
--- 209.165.200.229  192.168.1.9       ---             ---
```

Step 2: Test static NAT functionality

a. Ping from host H1 to the public static NAT address mapped to host H2. Are the pings successful? ________

b. Display the NAT translation table using the **show ip nat translations** command. Does the translation appear in the NAT table? ________

```
CustomerRouter#show ip nat translations
Pro  Inside global       Inside local     Outside local       Outside global
icmp 209.165.200.225:512 192.168.1.2:512 209.165.200.229:512 209.165.200.229:512
---  209.165.200.229     192.168.1.9     ---                 ---
```

c. What is the outside local and outside global address used in the translation?

____

d. From the ISP router HyperTerminal window, ping the H2 host with the static NAT translation at 192.168.1.9. Are the pings successful? _______

e. From the ISP router, ping the public static addressed mapped to the H2 internal server at 209.165.201.229. Are the pings successful? _______ Why?

____

f. What is the translation of the inside global address to the inside local host address?

____

```
CustomerRouter#show ip nat translations
Pro  Inside global     Inside local    Outside local     Outside global
icmp 209.165.200.229:5  192.168.1.9:5  209.165.200.226:5  209.165.200.226:5
---  209.165.200.229    192.168.1.9        ---                ---
```

Step 3: Save the router configurations.

In privileged EXEC mode, save the running configuration to the startup configuration.

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

Task 3: Reflection

a. 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?

____

____

____

____

____

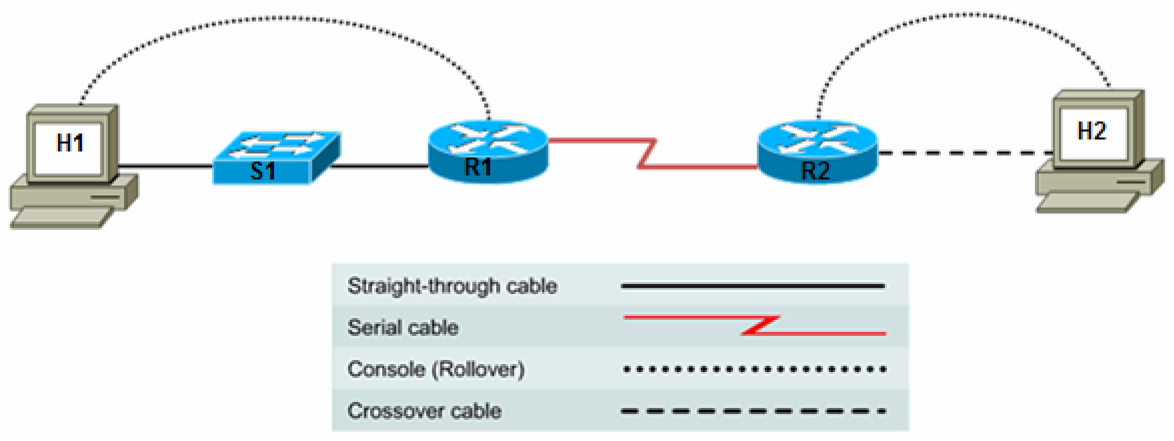
____

b. 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?

____

____

Lab 5.3.9a Managing Router Configuration Files Using HyperTerminal



Device	Host Name	Interface	IP Address	Subnet Mask
R1	R1	Serial 0/0/0 (DCE)	172.17.0.1	255.255.0.0
		FastEthernet 0/0	172.16.0.1	255.255.0.0
R2	R2	Serial 0/0/0 (DTE)	172.17.0.2	255.255.0.0
		FastEthernet 0/0	172.18.0.1	255.255.0.0

Objectives

- Establish a HyperTerminal session with a router, and use it to capture and save the running configuration as a text file for use as a backup.
- Edit the file using the Notepad text editor, and use HyperTerminal to restore the backup configuration to the router.
- Modify the file using Notepad, and use HyperTerminal to transfer the file and configure a different router.
- Verify network connectivity.

Background / Preparation

The HyperTerminal capture option can be very useful, not only for configuration files but for capturing command output and documentation purposes. It is a simple way to save whatever is displayed on the screen of the PC acting as a console to the router.

In this lab, you build a multi-router network and configure one of the routers. You will capture the running-config to a text file using HyperTerminal, and then edit the file using the Notepad text editor so that it can be used as a backup for the first router. You will then modify the file so that is can be used to configure the second router.

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- Two routers, each with an Ethernet and serial interface
- Two Windows XP computers
- Straight-through Category 5 Ethernet cable (H1 to switch)
- Crossover Category 5 Ethernet cable (H2 to router R2)
- Null serial cable
- Console cables (from H1 and H2 to routers R1 and R2)
- Access to the computer host command prompt
- Access to the computer host network TCP/IP configuration

From each computer, start a HyperTerminal session to the attached router.

Note: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Step 1: Configure host IP settings.

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

b. Configure static IP addresses on both hosts using the following settings.

Host H1:

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

Host H2:

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

Step 2: Log in to router R1 and configure the basic settings.

a. Configure the host name for R1.

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

b. Configure console, vty, and enable secret passwords. Configure synchronous logging for the console line.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
```

```
R1(config-line)#exit
R1(config)#enable secret class
R1(config)#exit
```

c. Configure a message-of-the-day (MOTD) banner and no ip domain lookup.

```
R1(config)#banner motd #Unauthorized Use Prohibited#
R1(config)#no ip domain lookup
```

d. Configure the R1 Fast Ethernet and serial interfaces.

```
R1(config)#interface serial 0/0/0
R1(config-if)#description WAN link to R2
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)#interface FastEthernet 0/0
R1(config-if)#description R1 LAN Default Gateway
R1(config-if)#ip address 172.16.0.1 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#end
```

Step 3: Display the R1 router configuration.

Issue the **show running-config** command in privileged EXEC mode, and verify all the configuration commands that you have entered. Note that this command can be abbreviated as **sh run**.

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

Step 4: Save the configuration on R1.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

```
R1#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 cycle. The running configuration will be lost if it is not saved. The router uses the startup configuration when the router is started.

Step 5: Start capturing the running configuration file.

a. Clear the screen using the **Edit > Clear Screen** and the **Edit > Clear Backscroll** options from the HyperTerminal main menu. This is not required to capture the file, but makes it easier to see what you are doing.

b. Use HyperTerminal to capture all text displayed on the screen to a text file by choosing **Transfer > Capture Text**.

c. Specify the name of the router plus you initials for the filename and use .txt for the extension. For example, R1-XYZ.txt, where XYZ are your initials. Browse to where you want to save the file. You will edit this file later in this lab.

Write down the name and location where you saved this file: ______________________________

d. Click the **Start** button to start capturing text.

e. Enter the **show running-config** command from privileged EXEC mode. This command displays the active configuration file for the router that is stored in RAM. Press the space bar when the "- More -" prompt appears.

Step 6: Stop capturing the configuration file.

To discontinue capturing the output, from the HyperTerminal menu, choose **Transfer > Capture Text > Stop**.

Step 7: Clean up the captured configuration file.

a. Start **Notepad**. From the Windows Desktop, choose **Start > Run**. Type **Notepad,** and then press **Enter**.

b. From the **Notepad** menu, choose **File > Open** and navigate to the file you captured. Click **Open**. Alternately, navigate to the saved .txt file and double click to open the file within **Notepad**.

c. The captured text file has information not required for configuring a router, for example, the “More” prompts. Remove any unnecessary information from the captured configuration. Be careful not to delete any part of the commands.

   To add comments to explain various parts of the configuration, use the exclamation mark (!). The router ignores any lines that start with an exclamation mark.

d. At the end of each configured interface, add the **no shutdown** command.

```
interface serial 0/0/0
description WAN link to R2
ip address 172.17.0.1 255.255.0.0
clock rate 64000
no shutdown
```

e. In the line **enable secret 5 $1$8SfN$BFKkGdAdqowyyoKm8WSmn/**, delete the number 5 and the encrypted string, and replace them with the password **class**.

f. Edit the line **banner motd ^CUnauthorized Use Prohibited^C** by replacing the ^C characters with number signs (#).

g. Delete the lines that contain:

   Show running-config
   Building configuration
   Current configuration
   - More -
   Lines that appear after the word "End"

h. An example of an unedited captured running configuration from an 1841 router is shown below. This router has a 4-port integrated Fast Ethernet switch. The lines that need to be kept are highlighted.

   Note: The Cisco IOS software inserts a number of commands by default. In most cases, you can remove these commands because the software automatically reinserts them. Generally, the commands you want to keep are the ones that you configured.

```
Building configuration...
Current configuration : 1073 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$8SfN$BFKkGdAdqowyyoKm8WSmn/
```

```
!
no aaa new-model
ip cef
!
no ip domain lookup
!
interface FastEthernet0/0
 description R1 LAN Default Gateway
 ip address 172.16.0.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface Serial0/0/0
 description WAN link to R2
 ip address 172.17.0.1 255.255.0.0
 no fair-queue
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd ^CUnauthorized Use Prohibited^C
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
end
```

i. The edited version of the 1841 running configuration is shown below. It is only necessary to specify the interfaces that you want to configure, as long as the startup-config file is erased prior to loading this file. The other interfaces will be shutdown by default.

   Note: If the startup-config is not erased prior to loading this file, these new commands are co-mingled with the existing configuration and may produce unpredictable results.

```
hostname R1
!
enable secret class
!
no ip domain lookup
!
interface FastEthernet0/0
 description R1 LAN Default Gateway
 ip address 172.16.0.1 255.255.0.0
 no shutdown
!
interface Serial0/0/0
 description WAN link to R2
 ip address 172.17.0.1 255.255.0.0
 clock rate 64000
 no shutdown
!
banner motd #Unauthorized Use Prohibited#
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

j. When finished editing the file in Notepad, be sure to save it.

Step 8: Erase the current startup configuration and restart the router.

Any form of backup that has not been tested could be a problem in a failure situation. This includes backup configurations. The backup configuration must be tested. The test should be scheduled during low network usage periods, because the router must be taken off line. All users that may be affected should be notified in advance to ensure that the downtime is not an inconvenience.

a. Before testing the backup configuration, erase the startup configuration. From the HyperTerminal session, enter the **erase startup-config** command at the enable router prompt to delete the configuration file from NVRAM.

b. When prompted whether to continue erasing the files, press **Enter** to continue.

c. Confirm that the startup configuration has been deleted by issuing the **show startup-config** command at the router prompt. What does the router show after this command is entered?

   ____

d. Issue the **reload** command at the privileged EXEC mode prompt to reboot the router. If prompted that the configuration has been modified, type **N** and press **Enter**.

e. When asked to proceed with the reload, press **Enter** to confirm. The router restarts.

f. When prompted to enter the initial configuration dialog, type **N** and press **Enter**.

g. When prompted to terminate autoinstall, type **Y** and press **Enter**. Press **Enter** again to go to the router prompt. What is the router prompt now? _________________________

Step 9: Reconfigure the R1 router from the saved text file.

a. Change to privileged EXEC mode. Why was a password not required?

____

b. Enter global config mode using the **configure terminal** command.

c. From the HyperTerminal menu, choose **Transfer > Send Text File**.

d. Navigate to the location where you saved the file previously, and select the file.

e. Each line in the text file is used to configure the router as it is read from the text file.

f. Observe the file as it loads and note any errors. The errors may be the result of typing errors.

g. What is the most obvious indication that the router configuration has been restored?

____

h. Type the **end** command, and press **Enter** or **Ctrl-Z** to exit global configuration mode.

i. Issue the **copy running-config startup-config** command to save the newly created router configuration NVRAM.

j. Verify that the running configuration is correct by using the **show running-config** command.

Step 10: Modify the R1 text file and use it to configure the R2 router.

a. Before configuring the R2 router, erase the startup configuration, as was done with router R1 in Step 8, and issue the **reload** command to reboot the router.

b. Using Windows Explorer or another method, copy the R1-XYZ.txt file and name it R2-XYZ.txt, where XYZ are your initials.

c. Edit the new R2 text file and modify the necessary parameters to match those in the device configuration table for router R2.

   Change the router host name.
   Remove the **clock rate** command from the serial 0/0/0 interface address and description, because this is the DTE side of the connection to R1.
   Change the Fast Ethernet 0/0 interface address and description.
   Add the **no shutdown** command to the Fast Ethernet 0/0 and serial 0/0/0 interfaces.

d. Save the modified R2 text file in Notepad.

e. Enter configuration mode by typing **enable** and then **configure terminal**. Make sure that the router prompt displays **Router(config)#**.

f. From the HyperTerminal menu, choose **Transfer > Send Text File**.

g. Navigate to the location where you saved the R2 text file and select the file.

h. Observe the file as is loads and note any errors. The errors may be the result of typing errors. If R2 is a different model router, erros can also result from Cisco IOS version variations and interface designation inconsistencies (for example, entering S0/0/0 when the router interface should be S0/0).

i. What is the most obvious indication that the router configuration has been restored?

____

j. Type the **end** command and press **Enter** or **Ctrl-Z** to exit global configuration mode.

k. Issue the **copy running-config startup-config** command to save the newly created router configuration NVRAM.

l. Verify that the running configuration is correct by using the **show running-config** command.

Step 11: Verify that the network is functioning.

a. From host H1, ping the R1 Fast Ethernet 0/0 interface IP address at 172.16.0.1. Are the pings successful? _______

b. From host H2, ping the R2 Fast Ethernet 0/0 interface IP address at 172.18.0.1. Are the pings successful? _______

c. From R1, ping the R2 serial 0/0/0 interface IP address at 172.17.0.2. Are the pings successful?____

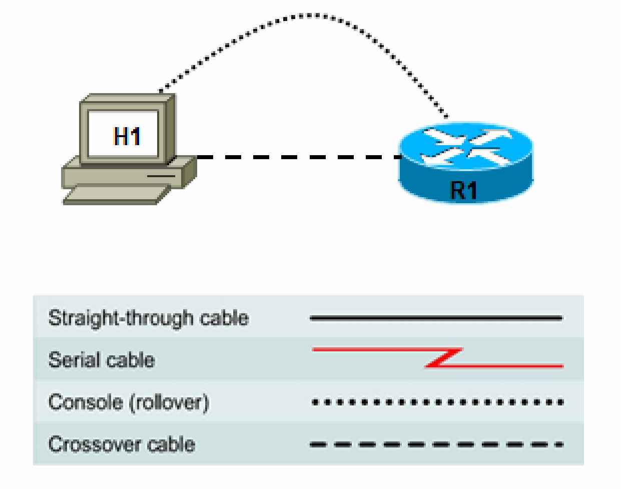
d. If any of the pings are not successful, troubleshoot the host and router configs until they are.

Note: You cannot ping from host H1 to H2, because routing has not been configured.

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 5.3.9b Managing Router Configuration Files Using TFTP



Device	Host Name	Interface	IP Address	Subnet Mask
R1	R1	Fast Ethernet 0/0	172.17.0.1	255.255.0.0

Objectives

- Download and install TFTP server software.
- Use TFTP to copy the router running configuration from a router to the TFTP server.
- Edit the file using the Notepad text editor, and copy the new configuration from the TFTP server to the router.

Background / Preparation

In this lab, you download and install TFTP server software and use it to back up the router running configuration to the TFTP server. You then edit the file using the Notepad text editor and copy the new configuration from the TFTP server to the router.

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One router with an Ethernet interface
- One Windows XP computer (or optional Discovery Server)
- Crossover Category 5 Ethernet cable (H1 to router R1)
- Console cable (from H1 to R1)

- Access to the computer host command prompt
- Access to the computer host network TCP/IP configuration

Note: Instead of using a PC and installing TFTP server software, you may use the Discovery Server, which has Linux-based TFTP server software pre-installed. Check with the instructor on the availability of a Discovery Server CD. The Discovery Server can take the place of host H1 in the topology diagram. The IP addresses used to configure host H1 and R1 in this lab are compatible with the Discovery Server.

From host H1, start a HyperTerminal session to the attached router.

Note: Make sure that the router has been erased and has no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Verify Connectivity

Step 1: Configure the TFTP server host.

Connect the router and host H1 according to the topology diagram. Configure the H1 IP address with the following settings.

IP address: 172.17.0.2
Subnet mask: 255.255.0.0
Default gateway: 172.17.0.1

Step 2: Log in to router R1 and configure the basic settings.

a. Configure the host name for R1.

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

b. Configure console, vty, and enable secret passwords. Configure synchronous logging for the console line.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret class
R1(config)#exit
```

c. Configure a message-of-the-day (MOTD) banner and no ip domain lookup.

```
R1(config)#banner motd #Unauthorized Use Prohibited#
R1(config)#no ip domain lookup
```

d. Configure the R1 Fast Ethernet interface.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#description R1 LAN Default Gateway
R1(config-if)#ip address 172.17.0.1 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#end
```

Step 3: Display the R1 router configuration.

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

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

Step 4: Verify basic connectivity.

Host H1 will be the TFTP server, and router R1 will be the TFTP client. To copy files to and from a TFTP server, you must have IP connectivity between the server and the client.

From host H1, ping the router Fast Ethernet interface at IP address 172.17.0.1. Are the pings successful?

____

If the pings are not successful, troubleshoot the host and router configurations until they are.

Step 5: Save the configuration on R1.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

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

Task 2: Use TFTP to Save a Cisco IOS Configuration

Step 1: Obtain and install the TFTP server application.

There are many free TFTP servers available. A search for “free TFTP server” identifies several you can choose from to download. This lab uses the free SolarWinds TFTP Server application. SolarWinds is a multithreaded TFTP server commonly used to upload and download executable images and configurations to routers and switches. It runs on most Microsoft® operating systems, including Windows® XP, Vista, 2000, and 2003. The SolarWinds software requires the Microsoft .NET 2.0 framework to install. This software can be downloaded free from www.microsoft.com.

Note: Check with the instructor for a copy of SolarWinds or another TFTP server that you can install.

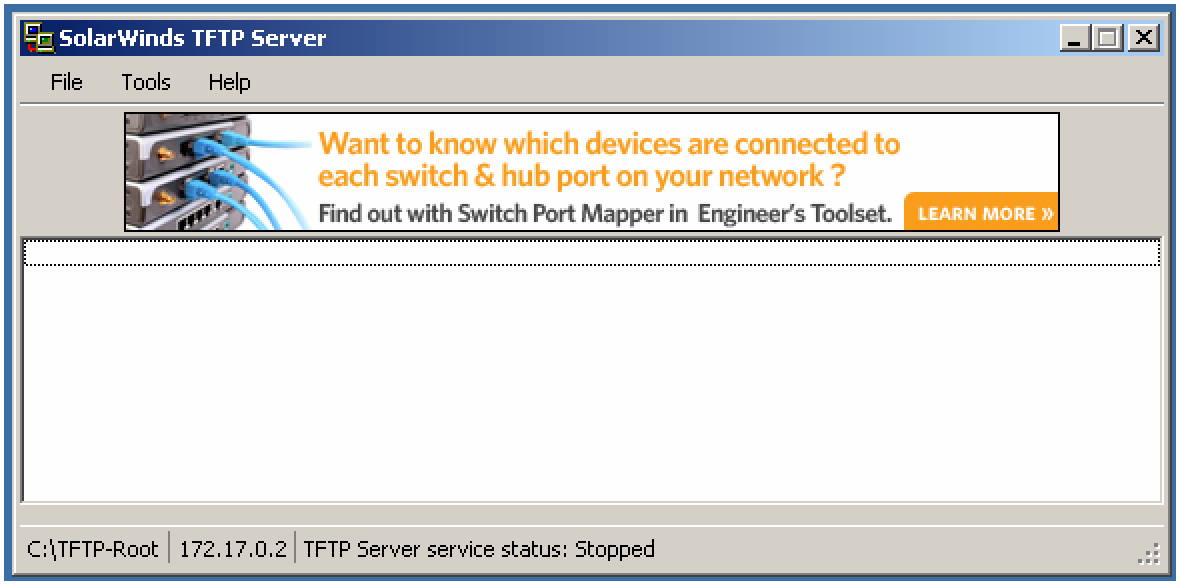
a. Go to the SolarWinds website and download the free TFTP server software and save it to your desktop.

   http://www.solarwinds.com/downloads

b. Double-click on the SolarWinds TFTP application to begin installation. Click Next. Agree to the license agreement, and accept the default settings. After the installation has finished, click Finish.

Step 2: Start the TFTP application.

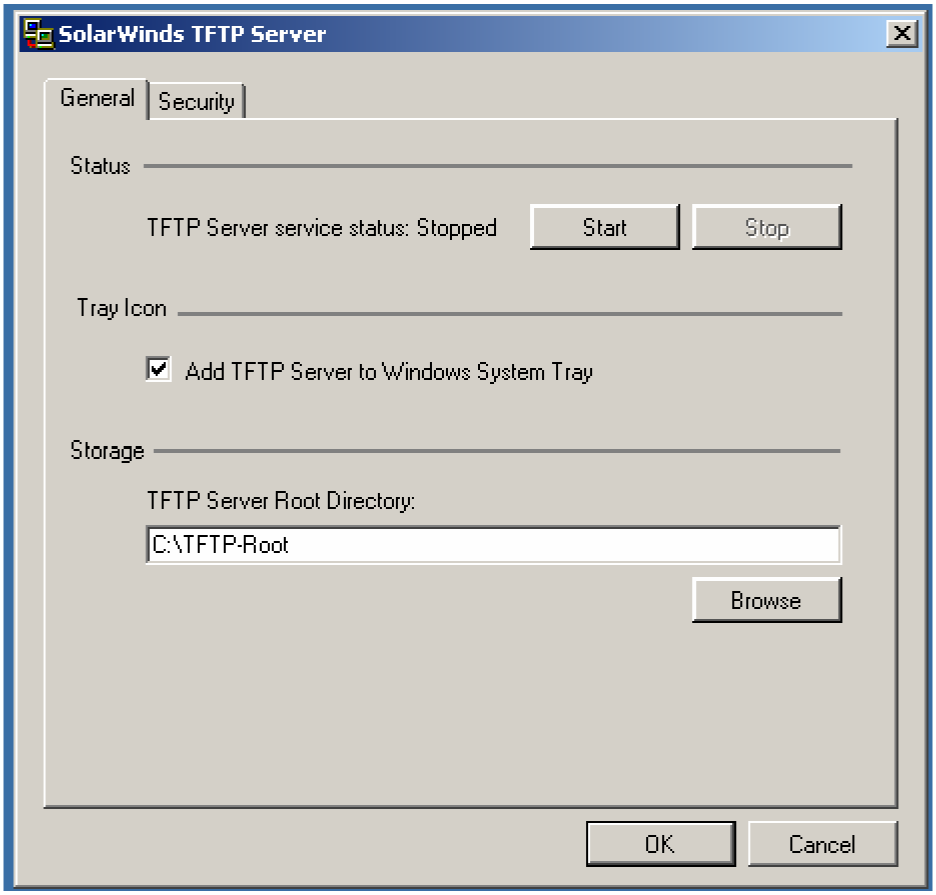
Start the TFTP server by choosing Start > Programs > SolarWinds TFTP Server > TFTP Server.


SolarWinds TFTP Server
File
Tools
Help
Want to know which devices are connected to each switch & hub port on your network ?
Find out with Switch Port Mapper in Engineer's Toolset.
LEARN MORE »

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Stopped

Step 3: Configure the TFTP server.

a. To configure the TFTP server, choose **File > Configure.** The screen displayed should be similar to the following. On the General tab, check that the default TFTP Server Root Directory is set to C:\TFTP-Root.

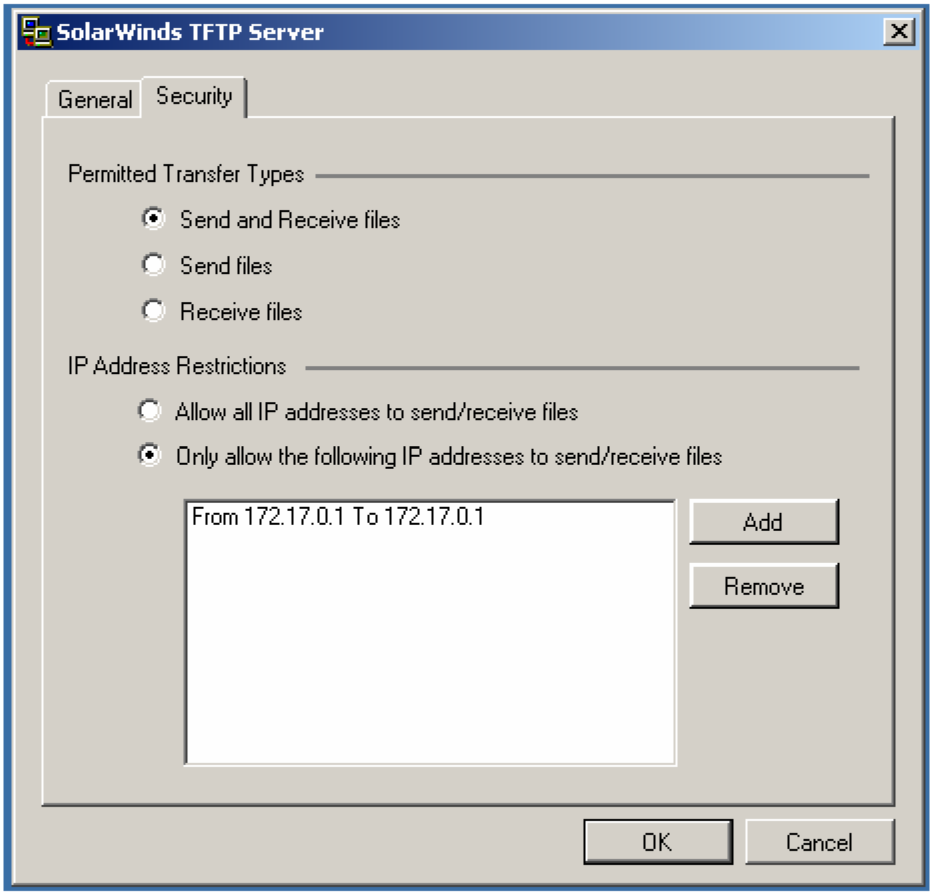


TFTP Server service status: Stopped

☑ Add TFTP Server to Windows System Tray

TFTP Server Root Directory:
C:\TFTP-Root

b. Click the **Security** tab. Check that **Permitted Transfer Types** is set to **Send and Receive files,** and set **IP Address Restrictions** to allow transfers from only the router R1 IP address (172.17.0.1 To 172.17.0.1).



Permitted Transfer Types

● Send and Receive files
○ Send files
○ Receive files

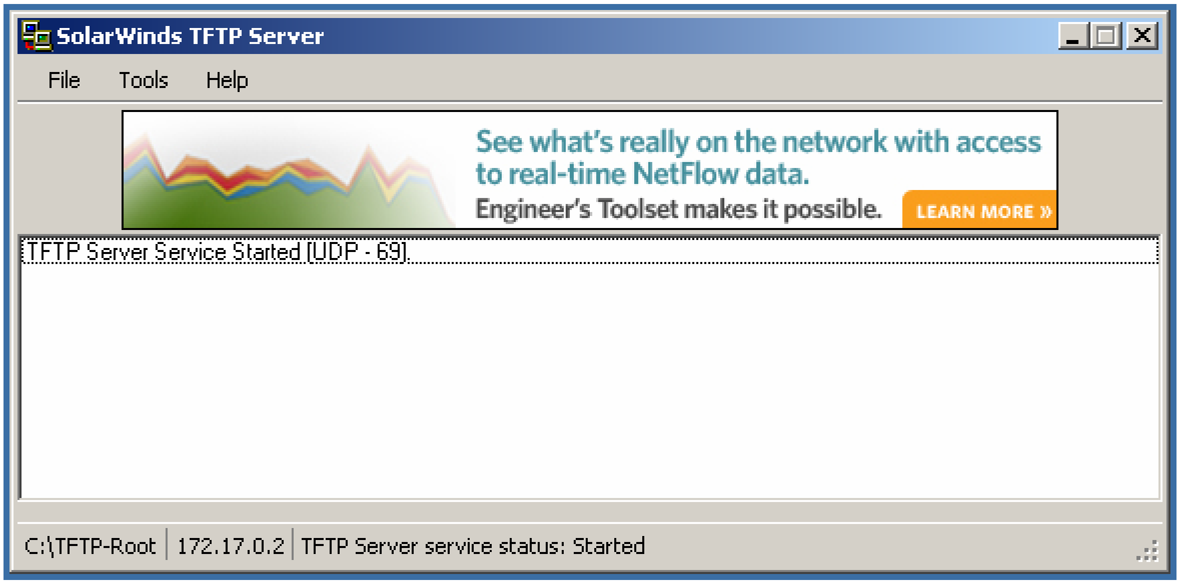
IP Address Restrictions

○ Allow all IP addresses to send/receive files
● Only allow the following IP addresses to send/receive files

From 172.17.0.1 To 172.17.0.1

c. In the **General** tab, click the **Start** button to activate the TFTP Server.

d. When finished, click **OK**. The screen should look similar to the following:


SolarWinds TFTP Server
File
Tools
Help
See what's really on the network with access to real-time NetFlow data.
Engineer's Toolset makes it possible.
LEARN MORE »

TFTP Server Service Started [UDP - 69].

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Started

e. On which well-known UDP port number is the TFTP server operating? __________

f. Leave the TFTP Server window open so that you can view the activity as the file is copied.

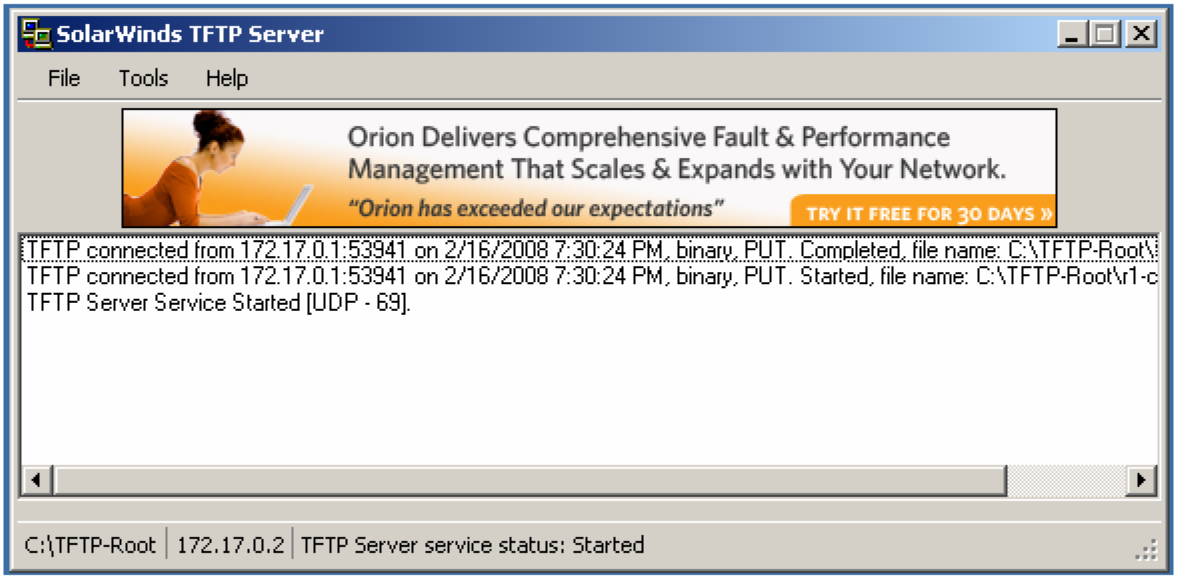
Step 4: Save the R1 configuration to the TFTP server.

From a HyperTerminal session on router R1, begin the TFTP upload to the TFTP server using the **copy running-config tftp** command. Respond to the prompts as shown below. The default name of the destination file is the name of the device name (r1), followed by a dash and confg. If successful, the output from the router terminal window should show exclamation marks and the number of bytes copied.

```
R1#copy running-config tftp

Address or name of remote host []? 172.17.0.2

Destination filename [r1-confg]? <ENTER>

!!

1078 bytes copied in 1.188 secs (907 bytes/sec)

R1#
```

Step 5: Verify the TFTP server activity.

Observe the TFTP Server window, which shows the connection entries for the transfer of the running-config file to the server. The output should look similar to the following.


SolarWinds TFTP Server
File
Tools
Help
Orion Delivers Comprehensive Fault & Performance Management That Scales & Expands with Your Network.
"Orion has exceeded our expectations"
TRY IT FREE FOR 30 DAYS »

```
TFTP connected from 172.17.0.1:53941 on 2/16/2008 7:30:24 PM, binary, PUT. Completed, file name: C:\TFTP-Root\
TFTP connected from 172.17.0.1:53941 on 2/16/2008 7:30:24 PM, binary, PUT. Started, file name: C:\TFTP-Root\r1-c
TFTP Server Service Started [UDP - 69].
```

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Started

Step 6: Verify the TFTP server file transfer.

Use Microsoft Word or Wordpad to examine the contents of file C:\TFTP-Root\r1-confg on the host H1 TFTP server. The contents should be similar to the following.

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
```

```
!
enable secret 5 $1$ofoK$Ur.oKj60xRxiVk3u1kDBu1
!
no aaa new-model
ip cef
!
no ip domain lookup
!
interface FastEthernet0/0
 description R1 LAN Default Gateway
 ip address 172.17.0.1 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1/0
!
interface FastEthernet0/1/1
!
interface FastEthernet0/1/2
!
interface FastEthernet0/1/3
!
interface Serial0/0/0
 no ip address
 shutdown
!
interface Serial0/0/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd #Unauthorized Use Prohibited#
!
line con 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
scheduler allocate 20000 1000
```

Task 3: Use TFTP to Restore a Cisco IOS Configuration

Step 1: Erase the R1 startup-config and restart the router.

a. Before testing the backup configuration, erase the router startup configuration. From the HyperTerminal session, enter the **erase startup-config** command at the enable router prompt. This deletes the configuration file from NVRAM.

b. When prompted to confirm the erasing, press **Enter** to continue.

c. Confirm that the startup configuration has been deleted by entering the **show startup-config** command at the router prompt.

d. Enter the **reload** command at the privileged EXEC mode prompt to reboot the router. If prompted whether to save the modified configuration, type **N** and press **Enter**.

e. When asked to proceed with the reload, press **Enter** to confirm. The router restarts.

f. When prompted to enter the initial configuration dialog, type **N** and press **Enter**.

g. When prompted to terminate autoinstall, type **Y** and press **Enter**. Press **Enter** again to go to the router prompt.

Step 2: Restore the R1 configuration from the TFTP server.

a. When the startup-config is erased and the router is reloaded, the router interfaces are shutdown by default and are no longer configured with IP addresses. This results in loss of connectivity between the router and the TFTP server. To copy the saved config file back to the router, connectivity must be re-established with the TFTP server.

b. Configure R1 Fast Ethernet 0/0 with an IP address and enable the interface.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fastethernet 0/0
Router(config-if)#ip address 172.17.0.1 255.255.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
```

c. Verify connectivity by pinging from host H1 to the R1 Fast Ethernet 0/0 IP address 172.17.0.1. Are the pings successful? ______

If the pings are not successful, troubleshoot until they are.

d. Download the R1 configuration file from the TFTP server using the **copy tftp startup-config** command. Respond to the prompts as shown below. If successful, the output from the router terminal window should show exclamation marks and the number of bytes copied.

```
Router#copy tftp startup-config
Address or name of remote host [172.17.0.2]? <ENTER>
Source filename [r1-confg]? <ENTER>
Destination filename [startup-config]? <ENTER>
Accessing tftp://172.17.0.2/r1-confg...
Loading r1-confg from 172.17.0.2 (via FastEthernet0/0): !
[OK - 1078 bytes]
[OK]
1078 bytes copied in 12.780 secs (84 bytes/sec)
Router#
*Feb 17 02:18:33.551: %SYS-5-CONFIG_NV_I: Nonvolatile storage configured
from tftp://172.17.0.2/r1-confg by console
Router#
```

e. View the configuration in NVRAM to verify that the transfer is accurate using the **show startup-config** command. The configuration should be the same as what you configured in Task 1, Step 2.

f. Reload the router and select **No** at the prompt that says “Configuration has been modified”.

g. The previous configuration should be restored, and the router host name should be R1.

Task 4: Reflection

How can TFTP be used to manage networking device files in an enterprise network?

____

____

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 5.4.3 Planning a WAN Upgrade

Objectives

- 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 the ISP to inquire about establishing a WAN connection between its main office and a second office that is opening in the next few months. You have been assigned to the new business account. You are asked to provide a proposal that outlines what the ISP can offer the business to meet its requirements for a new WAN connection.

You first visit the site to examine the existing setup. Currently, there is only one employee who accesses the head office using dialup and a 56 K modem. This employee requires access to a database server that stores the data for the company 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 one 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. These are the available options that you can offer the customer.

WAN Connection	Upstream Bandwidth	Downstream Bandwidth	SLA Availability	Cost
Dialup	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 the 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 connection for the business. Justify the answer you give.

Step 4: Group discussion.

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

WAN Upgrade Proposal

Objectives

- 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 dialup 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 5.5.2 Powering Up a 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 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 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 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.

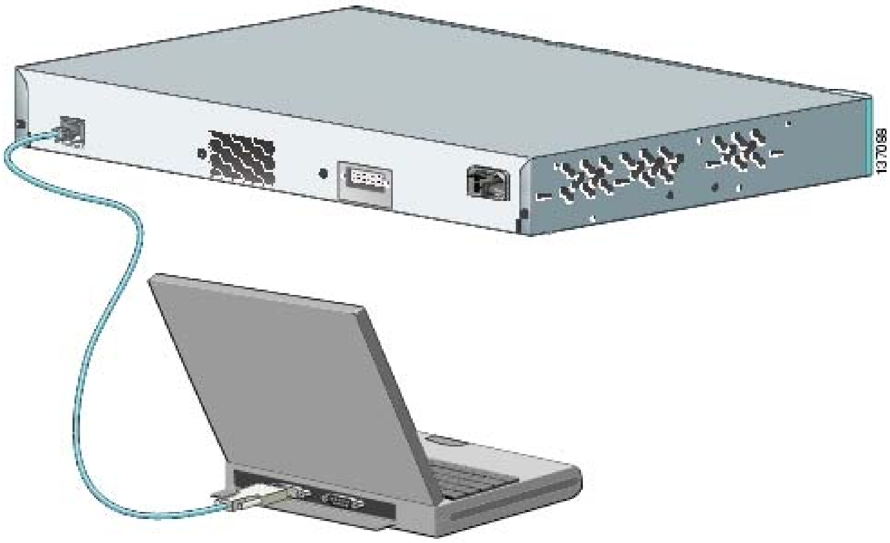
2) Crimp the 14 AWG (2 mm) green ground wire to a UL Listed/CSA-certified ring terminal using a crimping tool that is recommended by the ring terminal manufacturer.

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. 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:

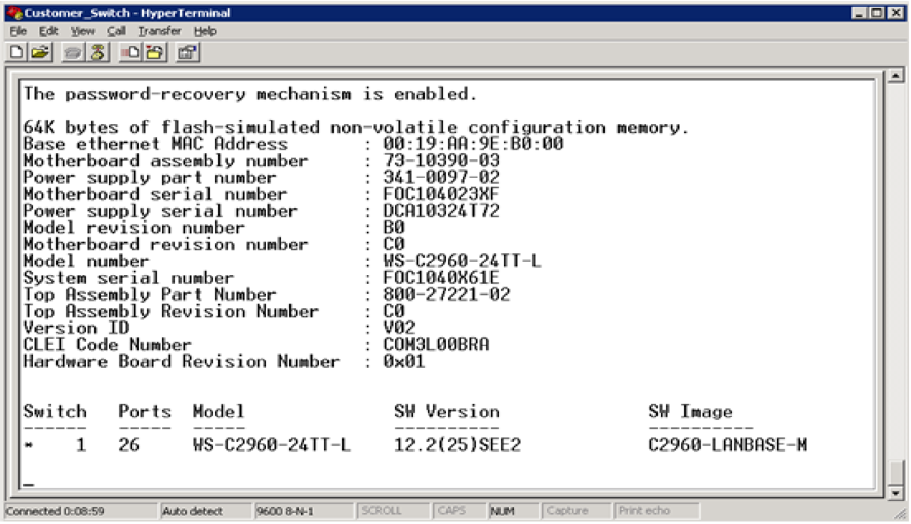
- 9600 baud
- 8 data bits
- no parity
- 1 stop bit
- no flow control and no parity

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 password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address          : 00:19:AA:9E:B0:00
Motherboard assembly number        : 73-10390-03
Power supply part number           : 341-0097-02
Motherboard serial number          : FOC104023XF
Power supply serial number         : DCA10324T72
Model revision number              : B0
Motherboard revision number        : C0
Model number                       : WS-C2960-24TT-L
System serial number               : FOC1040X61E
Top Assembly Part Number           : 800-27221-02
Top Assembly Revision Number       : C0
Version ID                         : V02
CLEI Code Number                   : COM3L00BRA
Hardware Board Revision Number     : 0x01


Switch   Ports  Model              SW Version            SW Image
------   -----  -----              ----------            ----------
*    1   26     WS-C2960-24TT-L    12.2(25)SEE2          C2960-LANBASE-M

_
```

c. 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.

d. 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 this message 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.

e. Turn off the switch 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 the switch fails POST, unplug the switch and tell the instructor.

Step 6: Reflection

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

   1) Status LED blinks green

   2) Speed LED blinks green

   3) Status LED blinks amber

   4) 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.

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

```
Switch>enable
```

b. 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)
```

c. 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
```

d. Check that the VLAN information was deleted in Step b by using the **show vlan** command. If the VLAN information was deleted, go to Step e and restart the switch using the **reload** 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.

e. Restart the software using the **reload** command in privileged EXEC mode.

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

```
Switch#reload
```

The responding line prompt is:

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

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:

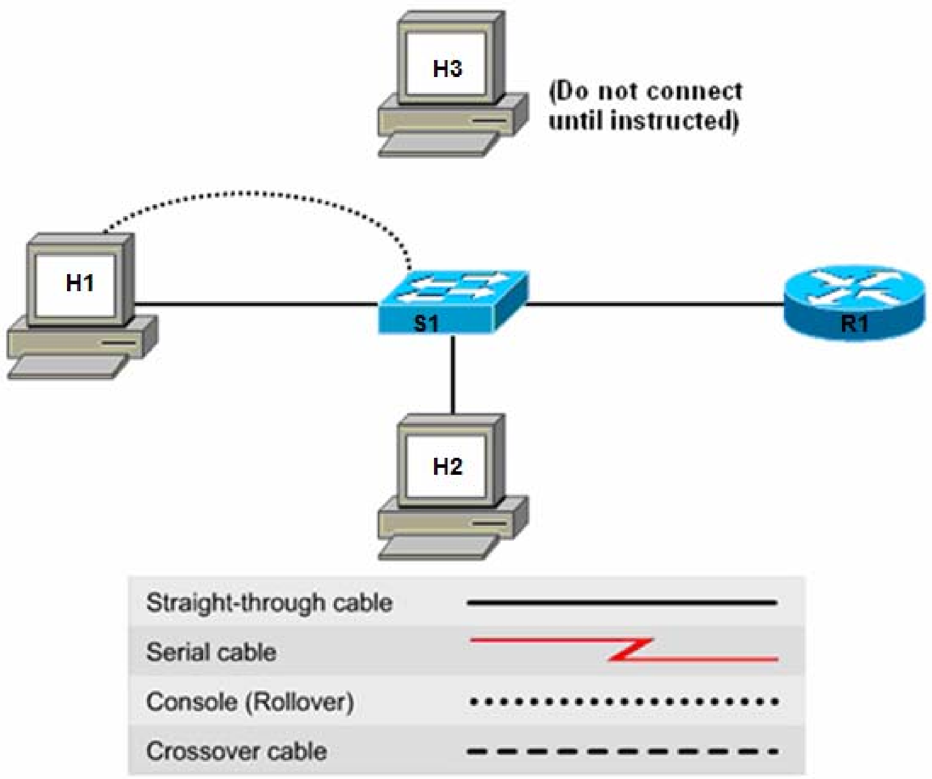
```
Would you like to enter the initial configuration dialog? [yes/no]:
```

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

The responding line prompt is:

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

Lab 5.5.4 Configuring the Cisco 2960 Switch



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
S1	CustomerSwitch	VLAN 1	192.168.1.5	255.255.255.0	192.168.1.1	N/A
R1	CustomerRouter	Fa0/1	192.168.1.1	255.255.255.0	N/A	Fa0/5
H1	H1	NIC	192.168.1.2	255.255.255.0	192.168.1.1	Fa0/11
H2	H2	NIC	192.168.1.4	255.255.255.0	192.168.1.1	Fa0/18
H3	H3	NIC	192.168.1.6	255.255.255.0	192.168.1.1	None

Objectives

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

Background / Preparation

In this lab, you connect multiple hosts and a router to the switch and test connectivity. You will configure port security, speed, and duplex settings for a switch port. This lab focuses on the basic configuration of the Cisco 2960 switch using Cisco IOS commands. 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. You will configure VLAN 1 to provide IP access to management functions. The information in this lab applies to other switches, however, command syntax may vary.

Required Resources

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 a PC network TCP/IP configuration

Note: Perform the instructions in the section “Erasing and Reloading the Switch” at the end of this lab before continuing.

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

a. Connect host H1 to Fast Ethernet S1 switch port Fa0/11, and connect H2 to port Fa0/18. Configure the hosts to use the same IP subnet for the address and mask as on the switch, as shown in the topology diagram and table above.

b. Do *not* connect host H3 to the switch yet.

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

Note: If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

a. Connect the router to switch port Fa0/5.

b. Configure the router with the host name **CustomerRouter**.

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

d. Configure the router Fa0/1 interface as shown in the topology table.

Step 3: Configure the switch.

a. Configure the switch with the host name **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)#no shutdown
CustomerSwitch(config-if)#exit
CustomerSwitch(config)#ip default-gateway 192.168.1.1
CustomerSwitch(config)#end
```

Step 5: Verify the 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 H1 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
!
!
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.

```
CustomerSwitch#copy running-config startup-config
```

Step 6: Verify connectivity using ping and Telnet.

a. To verify that the switch and router are correctly configured, ping the router Fa0/1 interface (default gateway) IP address from the switch CLI.

b. Are the pings successful? ________

c. To verify that the hosts and switch are correctly configured, ping the switch IP address from host H1.

d. Are 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 H1, and telnet the IP address assigned to switch management VLAN 1.

g. Enter the vty password configured in Step 3. What is the result? __________________________ 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
```

h. What is the Cisco IOS version of this switch? ____________________

i. 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, get the Layer 2 addresses of the PC network interface card for each host by using the **ipconfig /all** command.

Host H1: ____

Host H2: ____

Host H3: ____

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     Fa0/5
   1    000c.3076.8380    DYNAMIC     Fa0/11
   1    000d.1496.36ad    DYNAMIC     Fa0/18
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 **?** help feature.

```
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 0/18. Use the address that was recorded for H2 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 0/18 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     Fa0/5
   1    000c.3076.8380    DYNAMIC     Fa0/11
   1    000d.1496.36ad    STATIC      Fa0/18
```

h. How many total MAC addresses are there now? ____________________

i. What type are they? ____

Step 8: Configure basic port security.

a. Determine the options for setting port security on Fast Ethernet interface 0/18.

```
CustomerSwitch#configure terminal
CustomerSwitch(config)#interface fastEthernet 0/18
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. Remove the static mac address from FastEthernet interface 0/18. Use the address that was recorded for H2 in Step 7. The MAC address XXXX.YYYY.ZZZZ is used in the example statement only.

```
CustomerSwitch(config-if)#no mac-address-table static XXXX.YYYY.ZZZZ
interface fastethernet 0/18 vlan 1
```

c. To allow the switch port FastEthernet 0/18 to accept only one device, configure port security.

```
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)
---------------------------------------------------------------------------
      Fa0/18            1          0                 0         Shutdown
---------------------------------------------------------------------------
```

d. What is the security action for port Fa0/18 if a security violation occurs? _______________

e. What is the maximum secure address count? ____________

f. Display the running configuration.

Note: Some output is omitted in the 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 FastEthernet0/18
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
!
interface FastEthernet0/5
!

mac-address-table static 000b.db04.a5cd vlan 1 interface
FastEthernet0/18
!
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. If you do not have another PC available (H3) or you cannot disconnect the PC, go to alternative Step 9.

b. Disconnect host H2 from Fast Ethernet 0/18, and connect host H3 to the port. H3 has not yet been attached to the switch. From H3, ping the switch address 192.168.1.5 to generate some traffic.

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

____

____

```
01:11:12: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting
Fa0/18 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 FastEthernet0/18.
01:11:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, chang
ed state to down
01:11:14: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

d. View the configuration information for just Fast Ethernet port 0/18.

```
CustomerSwitch#show interface fastethernet 0/18
```

e. What is the state of this interface?

Fast Ethernet 0/18 is ________________ and the line protocol is _____________

Alternative Step 9: (Optional)

If you do not have a third PC (host H3) and you are working with a remote lab setup and cannot physically disconnect H2, you may be able to use the following procedure to change the MAC address of the H2. The following procedure works for a wide variety of NICs.

a. Choose **Start > Settings > Control Panel,** and double-click **Network Connections**.

b. Right-click on the NIC for which you want to change the MAC address, and click **Properties**.

c. In the General tab, click the **Configure** button.

d. In the Advanced tab, under the Property section, click on **Network Address or Locally Administered Address**.

e. On the right side, under Value, type in the new MAC address. Use the original MAC address, but change only the last value. For example, if the original MAC is 000C29C1510A, change it to 000C29C1510B.

f. Type **c:\>ipconfig /all** to verify the changes.

g. From H2, ping the switch VLAN 1 address at 192.168.1.5.

```
   c:\>ping 192.168.1.5
```

h. Record any observations from the PC and switch terminal session.

____

```
01:11:12: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/18, putting
Fa0/18 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 FastEthernet0/18.
01:11:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/18, chang
ed state to down
01:11:14: %LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to down
```

i. View the configuration information for just Fast Ethernet port 0/18.

```
CustomerSwitch#show interface fastethernet 0/18
```

j. What is the state of this interface?

Fast Ethernet 0/18 is ________________, and the line protocol is _____________.

Step 10: Reactivate the port.

a. Clear the sticky address entry for port Fa0/18 using the **clear port-security** command.

```
   S1#clear port-security sticky interface fa0/18 access
```

b. To return the interface from error disable to administratively up, enter the **shutdown** command followed by the **no shutdown** command.

```
S1(config)#interface fa0/18
S1(config-if)#shutdown
S1(config-if)#no shutdown
```

c. Enter the original host or change the MAC address to its original value. Ping from the command prompt. You can ping multiple times or use the **ping 192.168.1.5 –n 100** command, which sets the number of ping packets to 100, instead of 4.

Step 11: Set speed and duplex options for the ports.

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 Fa0/5, Fa0/11, and Fa0/18. This command generates a large amount of output. Press the spacebar until you can see all the information for these ports. What are the duplex and speed settings for these ports?

Port Fa0/5 ________________________________

Port Fa0/11 ________________________________

Port Fa0/18 ________________________________

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:

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

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. When the steps are completed, turn off all the devices. 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 privileged EXEC mode by typing **enable**. If prompted for a password, enter **class** (if that does not work, ask the instructor).

```
Switch>enable
```

b. 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)
```

c. 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
```

d. Check that the VLAN information was deleted in Step b by using the **show vlan** command. If the VLAN information was deleted, go to Step e and restart the switch using the **reload** 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.

e. Restart the software using the **reload** command in privileged EXEC mode.

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]:
```

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]:
```

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

The responding line prompt is:

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

Erasing and reloading the router

a. Enter 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.

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?

____

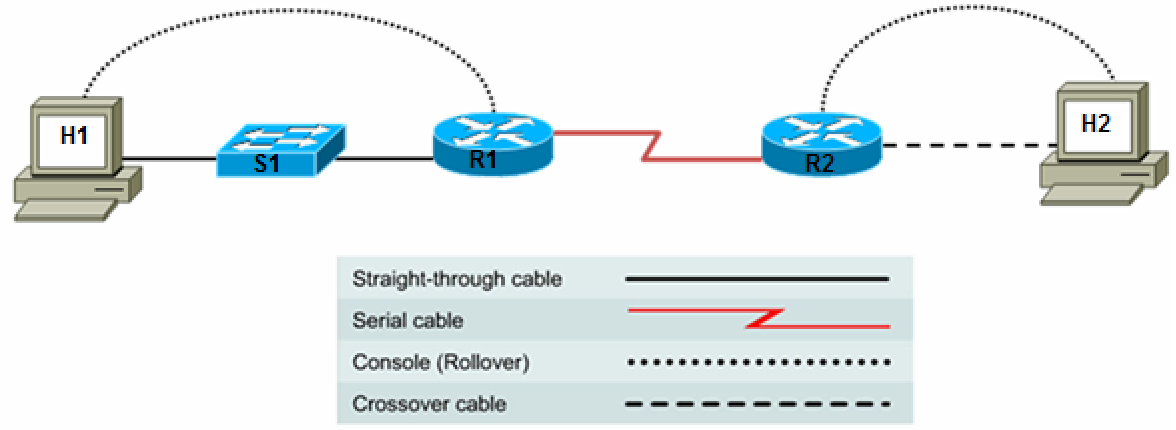
____

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 Configuring and Verifying RIP



Device	Host Name	Interface	IP Address	Subnet Mask
R1	R1	Serial 0/0/0 (DCE)	172.17.0.1	255.255.255.224
		Fast Ethernet 0/0	172.16.0.1	255.255.255.0
R2	R2	Serial 0/0/0 (DTE)	172.17.0.2	255.255.255.224
		Fast Ethernet 0/0	172.18.0.1	255.255.255.0

Objectives

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

Background / Preparation

RIP is one of the most commonly used and widely supported routing protocols in the networking industry. Knowledge of RIP and how to configure it using the Cisco IOS CLI is essential to success as a network technician. In this lab, you build a multi-router network and use RIP to automatically propagate routes, so hosts on remote networks can communicate.

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.

From hosts H1 and H2, start a HyperTerminal session with each router.

Note: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Required Resources

The following resources are required:

- Two routers, each with an Ethernet and serial interface. These should be non-SDM routers, if possible, because the required SDM startup configuration is deleted when the startup-config is erased.
- Two Windows XP computers
- Two straight-through Category 5 Ethernet cables (H1 to switch and switch to R1)
- Crossover Category 5 Ethernet cable (H2 to router R2)
- Null serial cable
- Console cables (from H1 and H2 to routers R1 and R2)
- Access to the H1 and H2 command prompt
- Access to the H1 and H2 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 host names and interfaces according to the chart.

Note: See Lab 5.3.5 if you have difficulty with the basic router configuration. That lab provides instructions for using the Cisco IOS CLI.

Step 2: Configure the hosts.

a. Configure host H1 attached to R1 with an IP address, subnet mask, and default gateway that is compatible with the IP address of the R1 Fast Ethernet interface (172.16.0.1/24).

Host H1 IP configuration:

IP address: 172.16.0.2
Subnet mask: 255.255.255.0
Default gateway: 172.16.0.1

b. Configure host H2 attached to R2 with an IP address, subnet mask, and default gateway that is compatible with the IP address of the R2 Fast Ethernet interface (172.18.0.1/24).

Host H2 IP configuration:

IP address: 172.18.0.2
Subnet mask: 255.255.255.0
Default gateway: 172.18.0.1

Step 3: Check the R1 routing table.

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
     172.16.0.0/24 is subnetted, 1 subnets
C    172.16.0.0 is directly connected, FastEthernet0/0
     172.17.0.0/27 is subnetted, 1 subnets
C    172.17.0.0 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?

____

c. Is there a route in the R1 routing table to the R2 Ethernet network 172.18.0.0? ______ Why?

____

Step 4: Test end-to-end connectivity.

a. From R1, ping the R2 router Fast Ethernet interface.

```
R1#ping 172.18.0.1
```

Are the pings successful? ____

b. From host H1, ping host H2 (from network 172.16.0.2 to network 172.18.0.2).

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

Are the pings successful? _____

c. Why are the pings not successful? ____

____

Step 5: 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
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 6: View 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

     172.16.0.0/24 is subnetted, 1 subnets
C    172.16.0.0 is directly connected, FastEthernet0/0
     172.17.0.0/27 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Serial0/0/0
R    172.18.0.0/16 [120/1] via 172.17.0.2, 00:00:02, Serial0/0/0
```

b. Which networks are shown 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 “Serial0/0/0” mean for this network route?

____

f. Examine the routing table entries on router R2.

```
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

R    172.16.0.0/16 [120/1] via 172.17.0.1, 00:00:05, Serial0/0/0
     172.17.0.0/27 is subnetted, 1 subnets
C    172.17.0.0 is directly connected, Serial0/0/0
     172.18.0.0/24 is subnetted, 1 subnets
C    172.18.0.0 is directly connected, FastEthernet0/0
```

g. Which networks are shown in the R2 routing table?

____

____

Step 7: Test end-to-end connectivity.

a. From R1, ping the R2 router Fast Ethernet interface.

```
R1#ping 172.18.0.1
```

Are the pings successful? ____

b. From the host H1 command prompt, ping H2 (from network 172.16.0.2 to network 172.18.0.2).

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

c. Are the pings successful? ____

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.

d. Why are the pings successful this time? ____

Step 8: 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 Serial0/0/0 (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 Serial0/0/0
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 a 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 9: Reflection

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

____

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

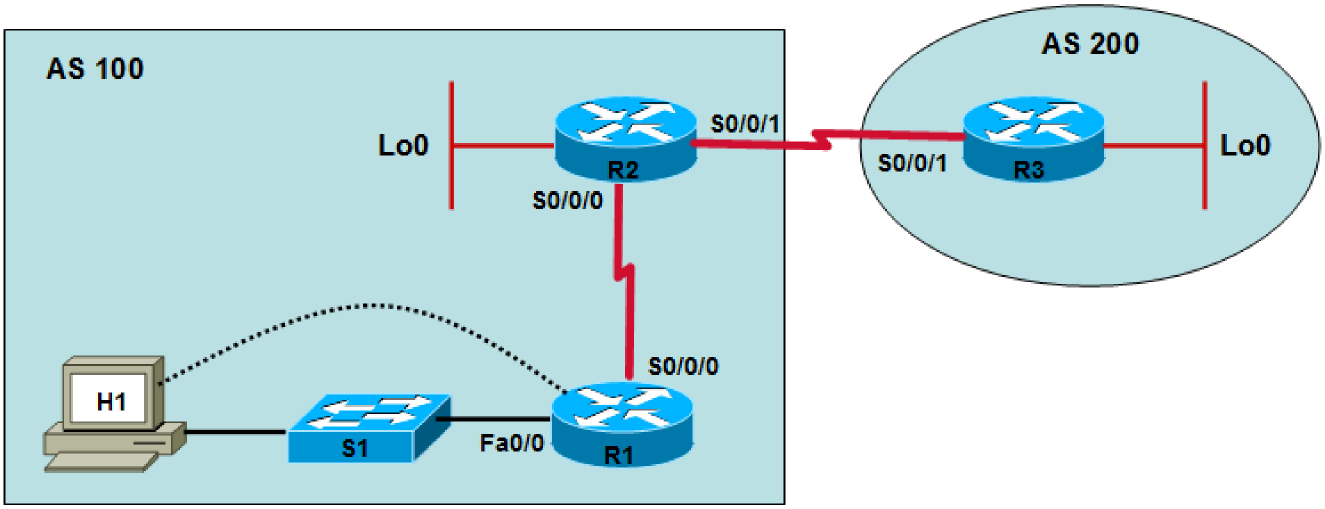
____

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 6.2.4 Configuring BGP with Default Routing



Device	Host Name	Interface	IP Address	Subnet Mask
R1	CR	Serial 0/0/0 (DTE)	10.10.10.1	255.255.255.0
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0
R2	ISP1	Serial 0/0/0 (DCE)	10.10.10.2	255.255.255.0
		Serial 0/0/1 (DCE)	172.16.1.1	255.255.255.0
		Loopback 0	192.168.100.1	255.255.255.0
R3	ISP2	Serial 0/0/1 (DTE)	172.16.1.2	255.255.255.0
		Loopback 0	192.168.200.1	255.255.255.0

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 connects to the ISP using a default route, and ISP1 connects to ISP2 via BGP4.

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, the output may vary from the output shown in this lab.

Note: Some Cisco router IOS images do not support BGP. You must have an IOS image that supports BGP and enough Flash memory and RAM available to load the image. The Discovery lab configuration document lists the Cisco 1841 router with 32 Mbytes flash, 128 Mbytes of DRAM and Basic IP IOS version 12.3 as a requirement for this course. An 1841 router with these specifications was used to perform this lab. If you are unsure if your router can be used for this lab, contact you instructor.

Required Resources

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)
- Windows XP computer with terminal emulation program installed
- Two straight-through Category 5 Ethernet cables (H1 to switch and switch to R1)
- Two null serial cables
- Console cable to configure routers
- Access to host H1 command prompt
- Access to host H1 network TCP/IP configuration

On host H1, start a HyperTerminal session to each router.

Note: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with your instructor if you are unsure of how to do this.

Step 1: Configure the 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, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

b. Configure the host H1 IP address and subnet mask on the customer network to be compatible with the CR router Fast Ethernet interface with a default gateway of 192.168.1.1.

c. Ping between the directly connected routers to test connectivity. Is the CR router able to reach the ISP2 router? ______ Is 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.

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

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 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 network.

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

c. Test connectivity by pinging from the host to ISP1 at 10.10.10.2.

Note: If pings are not successful, troubleshoot the router and host configurations and connections.

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 good practice to save the 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, Serial0/0/1
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, Serial0/0/1
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, Serial0/0/0
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 networks 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, Serial0/0/0
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 the CR routing table?

____

Step 5: Verify connectivity.

a. Ping from host H1 on the CR Ethernet network to the loopback interface on ISP2.

b. Ping from the ISP2 router to host H1 on the Ethernet network of CR.

Note: If pings are not successful, troubleshoot the router and host configurations and connections.

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 does ISP1 not advertise any networks to the customer router?

____

____

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

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

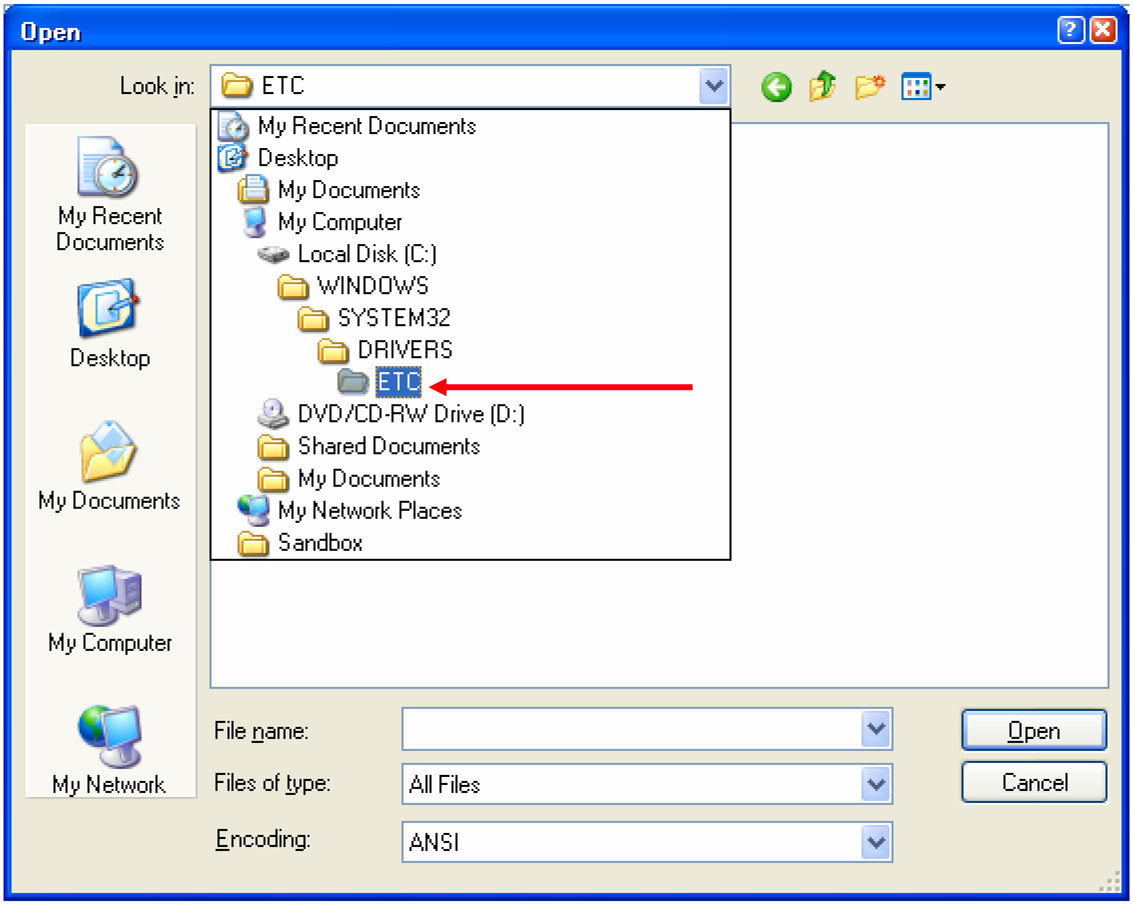
NOTE: The screen layout of your Windows-based operating system may be slightly different than what appears here, but the procedure is the same.

Step 1: Locate the HOSTS file in Windows

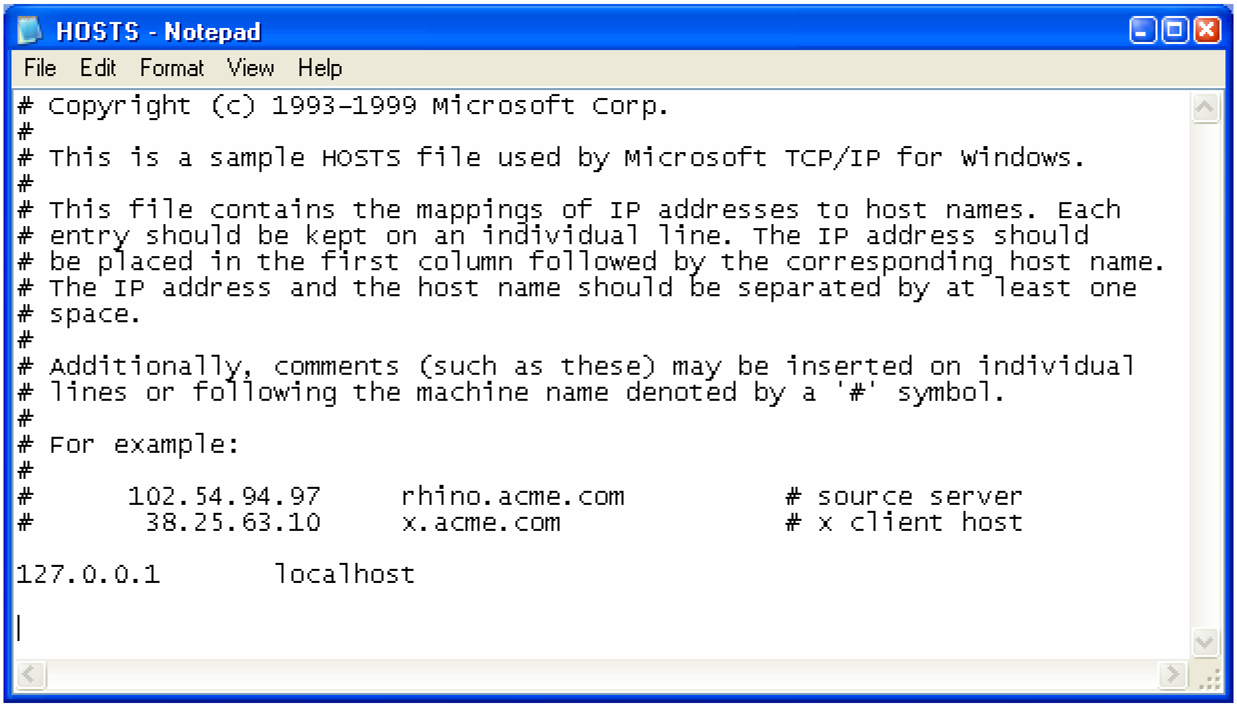
a. Click the **Start** button and choose **All Programs** > **Accessories**, and then click the **Notepad** program.

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**.



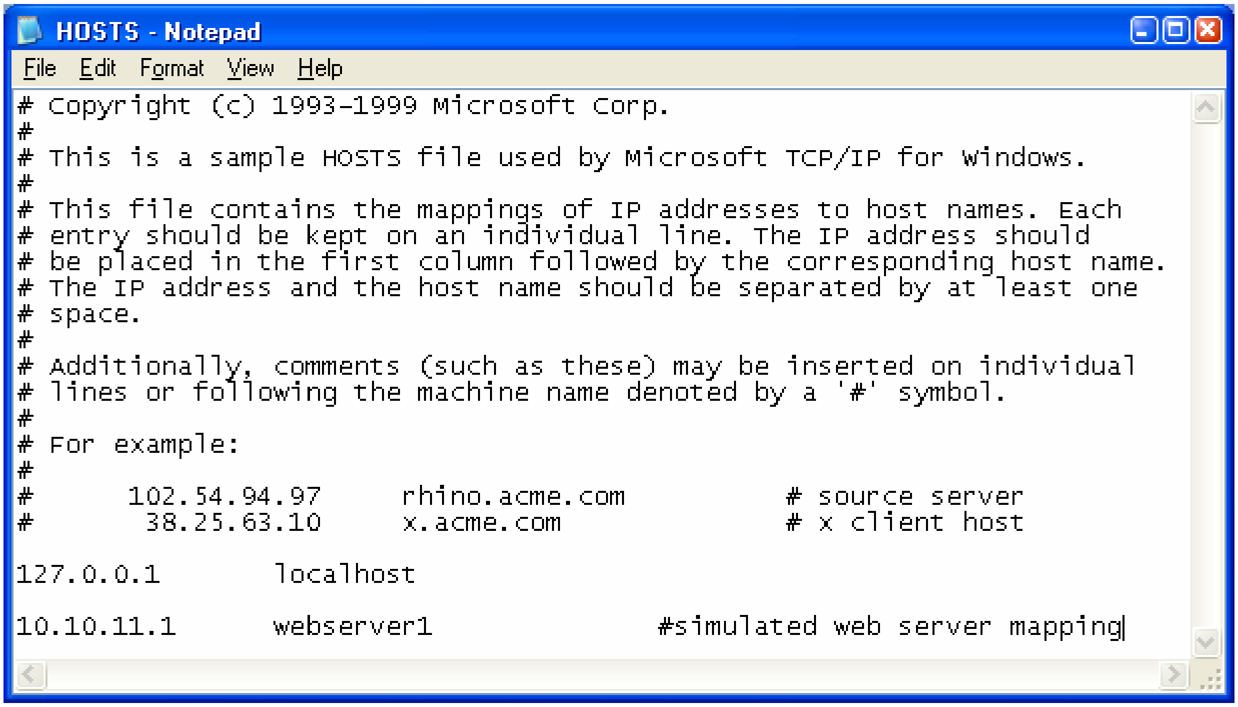
The **HOSTS** file opens in Notepad.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
```

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.



```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost

10.10.11.1      webserver1              #simulated web server mapping
```

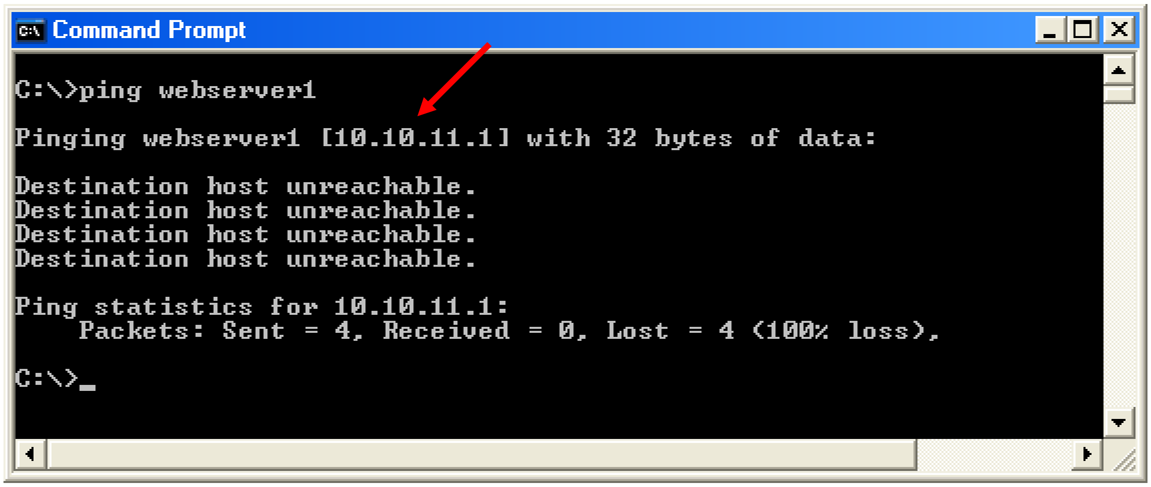
b. Save the updated **HOSTS** file.

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.



```
C:\>ping webserver1

Pinging webserver1 [10.10.11.1] with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 10.10.11.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>_
```

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 7.3.3a Examining Cached DNS Information on a 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.

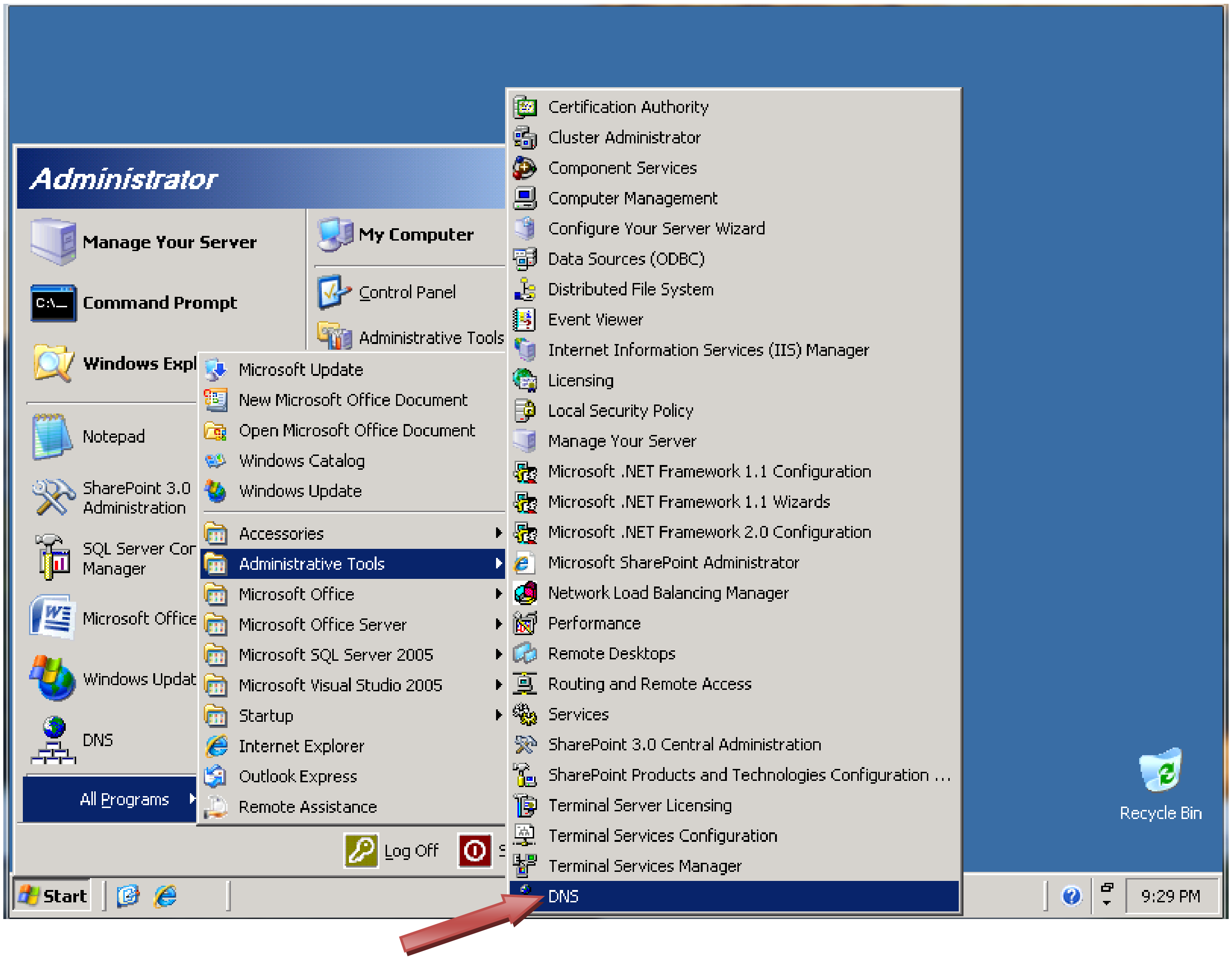
The following resources are required:

- Windows 2003 Server with DNS running
- Administrative access to server
- Internet connectivity

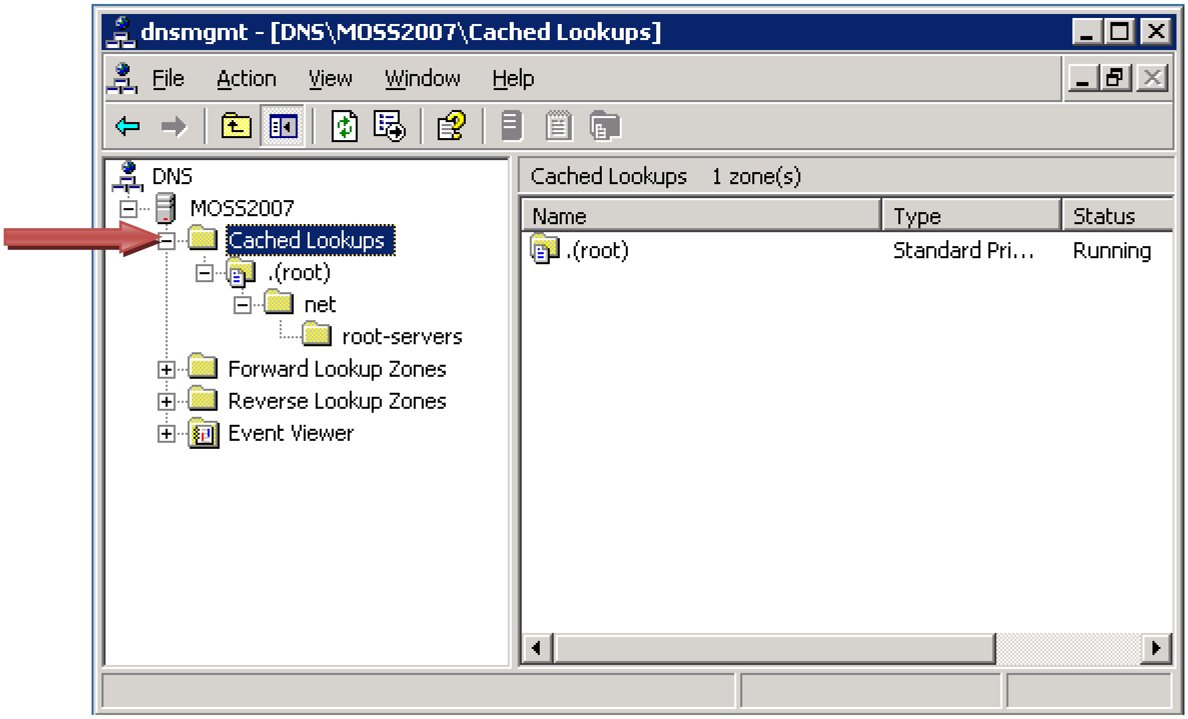
NOTE: If you do not have access to a Windows DNS server, the instructor may demonstrate this lab. If the equipment is not available to perform the lab, or if it cannot be demonstrated, read through the steps of the lab to gain a better understanding of DNS and how DNS servers operate.

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.

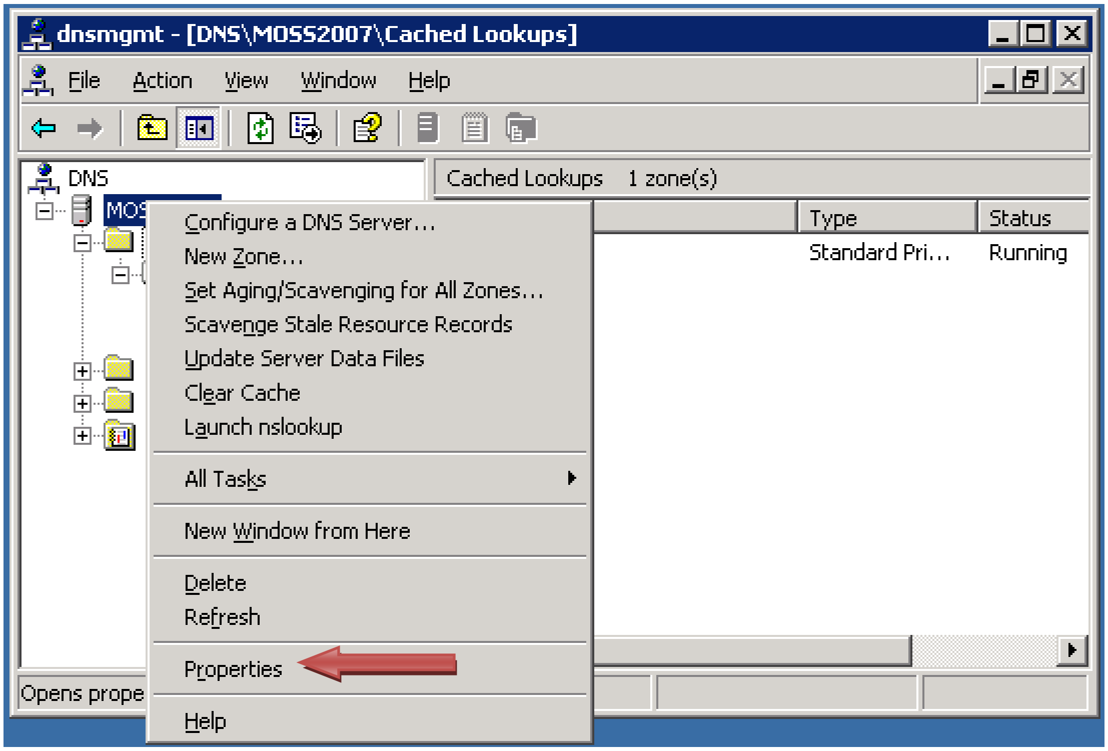


b. Expand the **Cached Lookups** folder and all subfolders to see that there are no cached lookups.

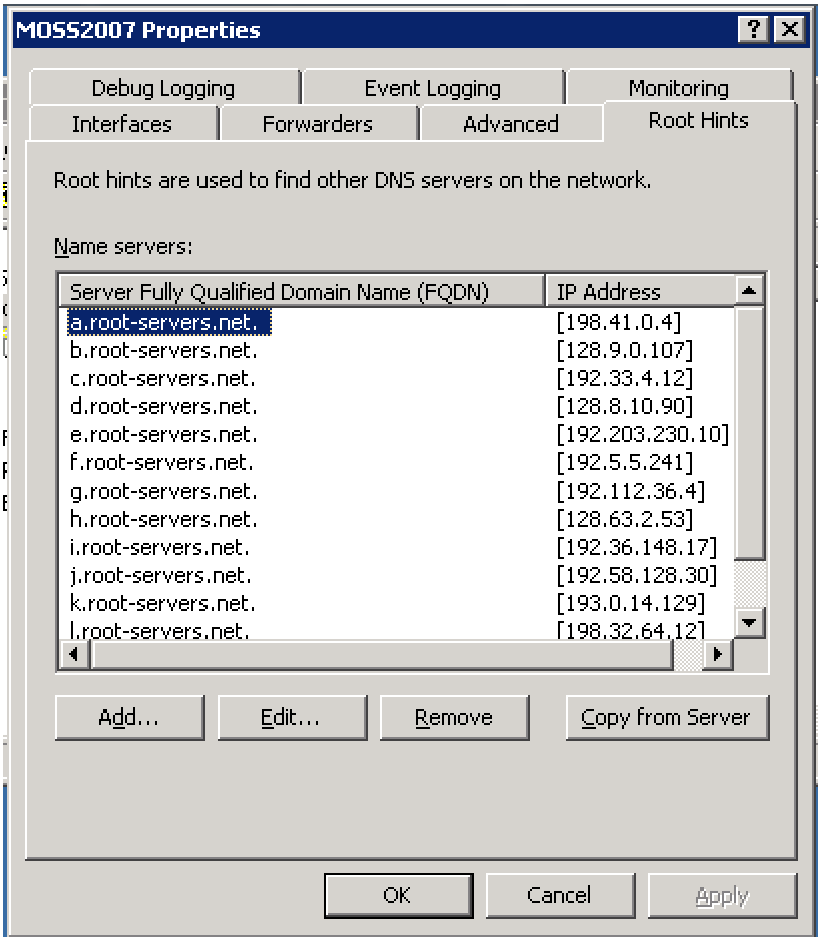


Name	Type	Status
.(root)	Standard Pri...	Running

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.



MOSS2007 Properties

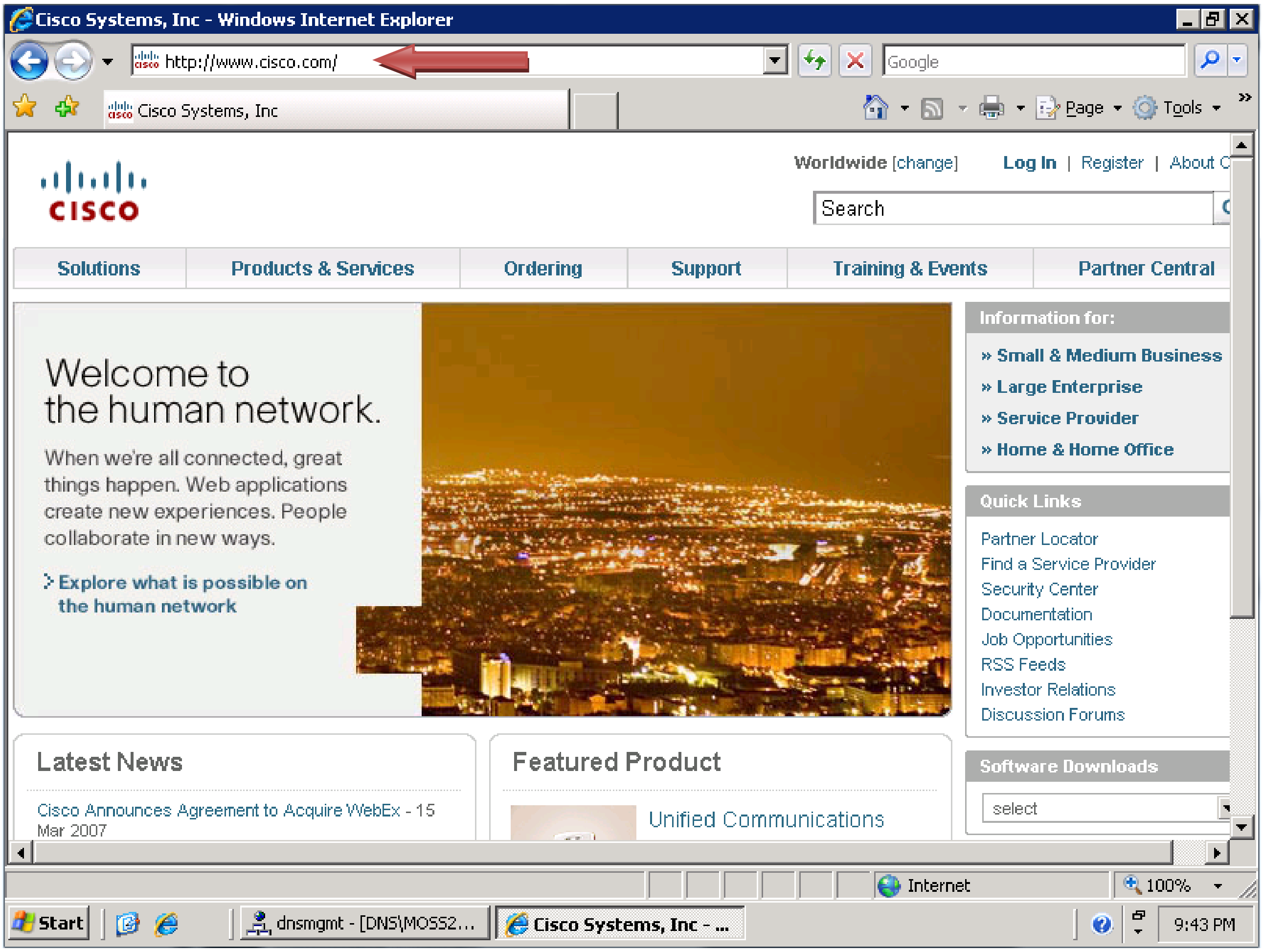
Root hints are used to find other DNS servers on the network.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
a.root-servers.net.	[198.41.0.4]
b.root-servers.net.	[128.9.0.107]
c.root-servers.net.	[192.33.4.12]
d.root-servers.net.	[128.8.10.90]
e.root-servers.net.	[192.203.230.10]
f.root-servers.net.	[192.5.5.241]
g.root-servers.net.	[192.112.36.4]
h.root-servers.net.	[128.63.2.53]
i.root-servers.net.	[192.36.148.17]
j.root-servers.net.	[192.58.128.30]
k.root-servers.net.	[193.0.14.129]
l.root-servers.net.	[198.32.64.12]

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.



Cisco Systems, Inc - Windows Internet Explorer

http://www.cisco.com/

Welcome to the human network.

When we're all connected, great things happen. Web applications create new experiences. People collaborate in new ways.

Explore what is possible on the human network

Latest News

Cisco Announces Agreement to Acquire WebEx - 15 Mar 2007

Featured Product

Unified Communications

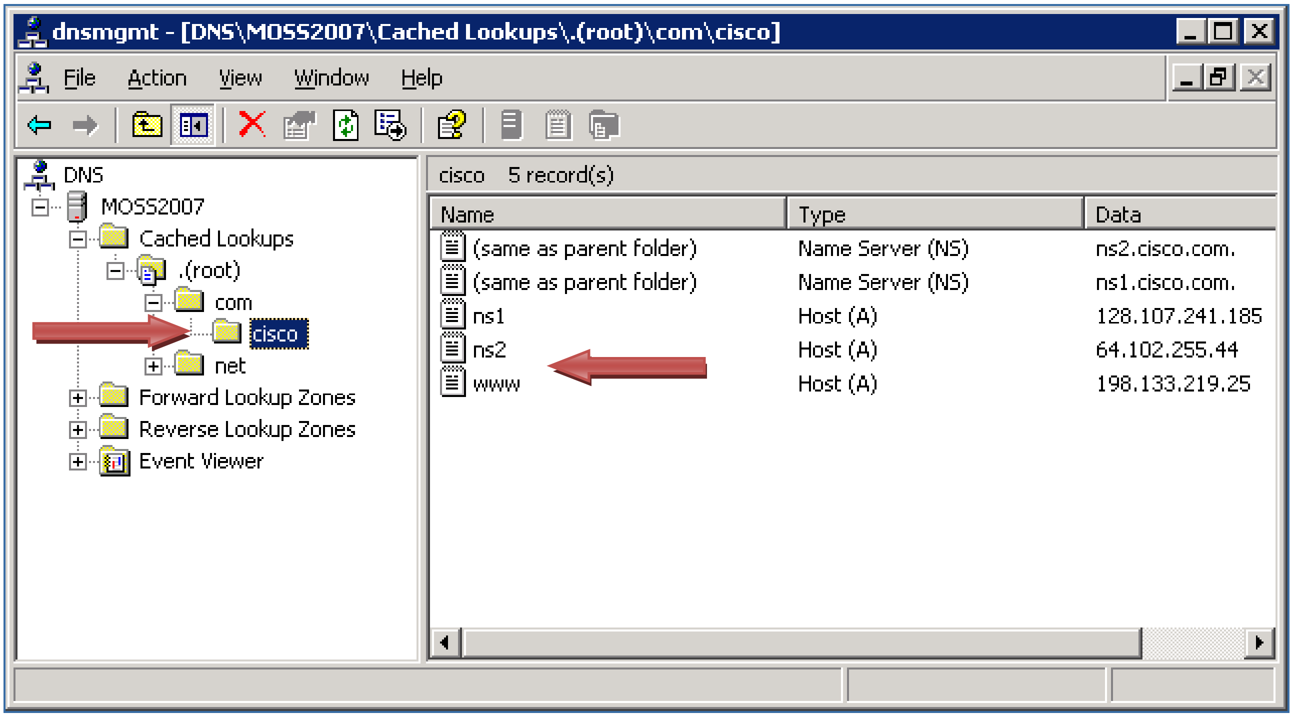
Step 3: Examine the Cached DNS entries

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.



dnsmgmt - [DNS\MOSS2007\Cached Lookups\.(root)\com\cisco]

cisco 5 record(s)

Name	Type	Data
(same as parent folder)	Name Server (NS)	ns2.cisco.com.
(same as parent folder)	Name Server (NS)	ns1.cisco.com.
ns1	Host (A)	128.107.241.185
ns2	Host (A)	64.102.255.44
www	Host (A)	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 7.3.3b 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.

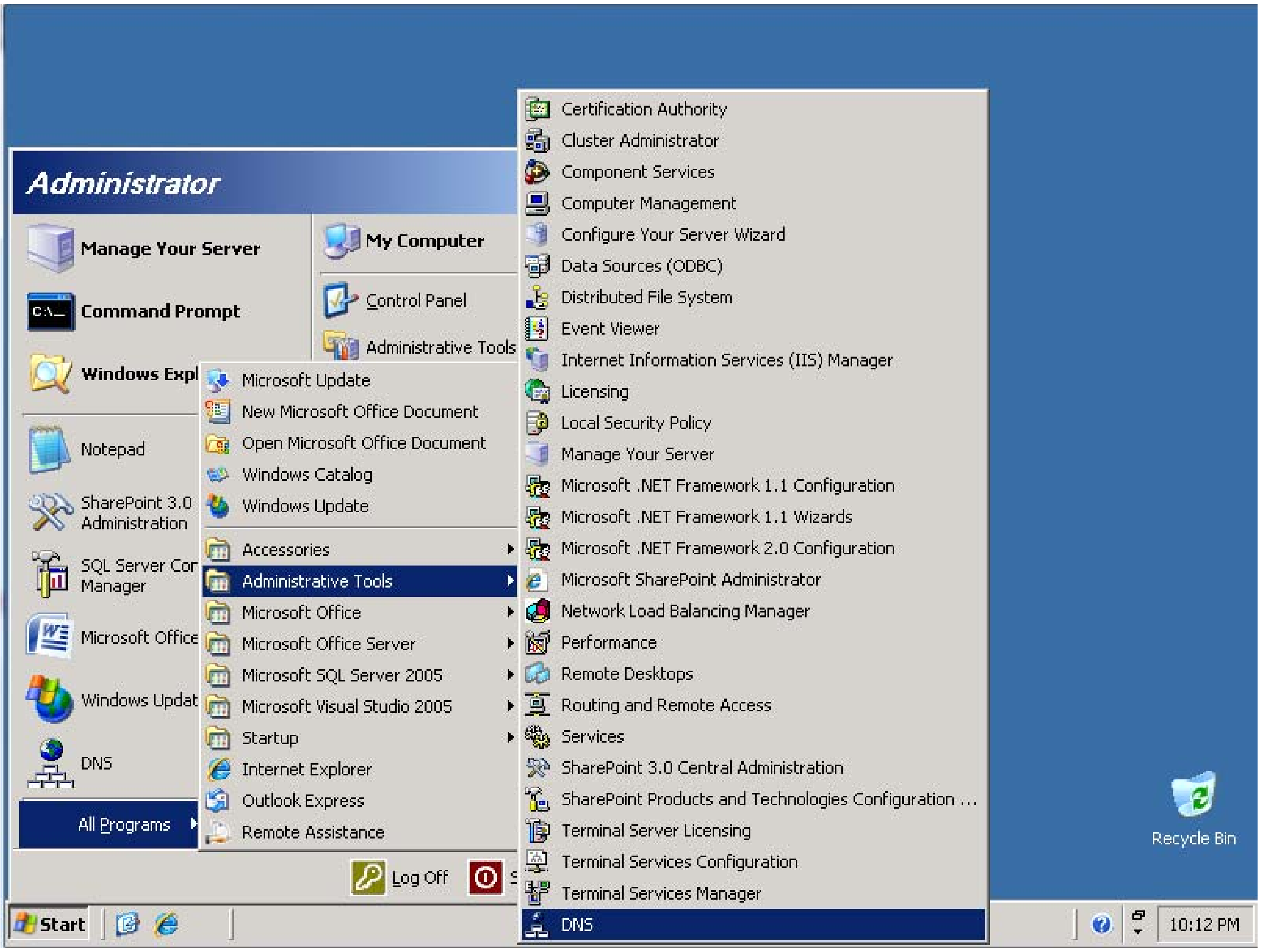
The following resources are required:

- Two Windows 2003 Servers with DNS running
- Administrative access to servers
- Internet connectivity

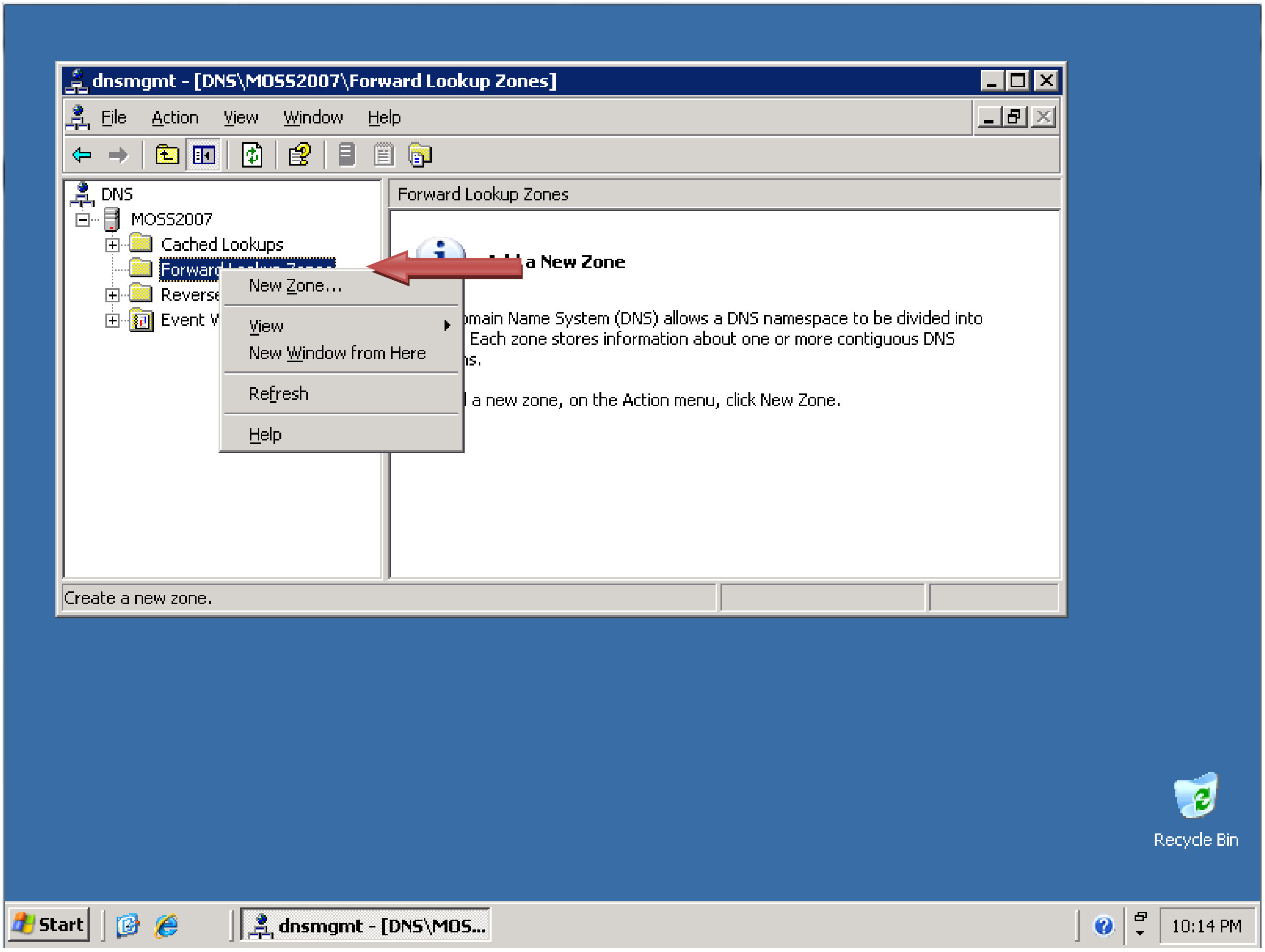
NOTE: If you do not have access to the Windows DNS servers, the instructor may demonstrate this lab. If the equipment is not available to perform the lab, or if it cannot be demonstrated, read through the steps of the lab to gain a better understanding of DNS and how DNS servers operate.

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**.

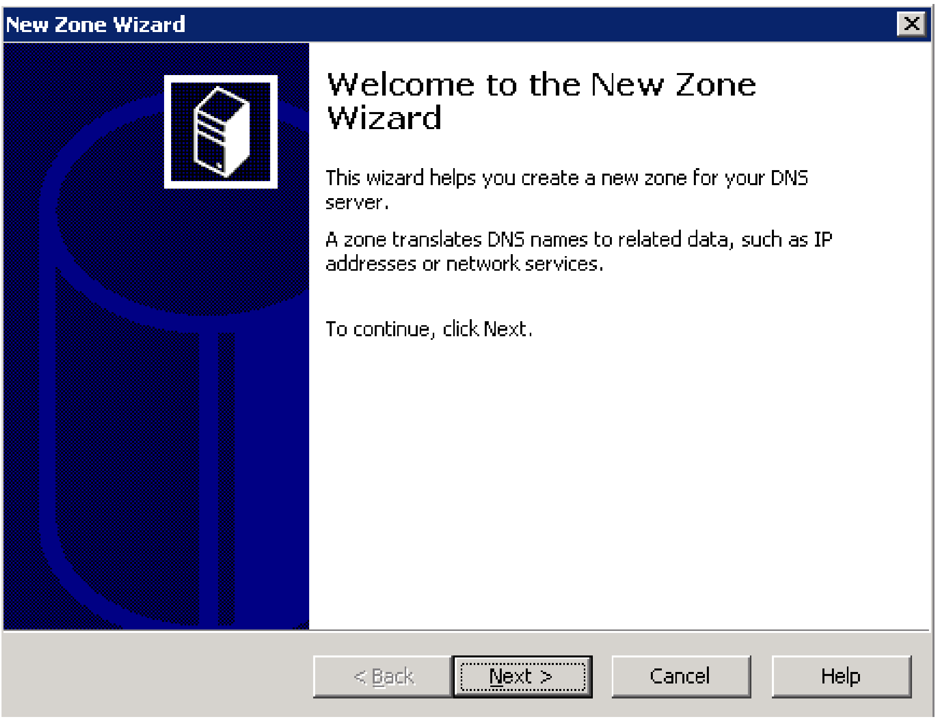


omain Name System (DNS) allows a DNS namespace to be divided into
Each zone stores information about one or more contiguous DNS
s.

a new zone, on the Action menu, click New Zone.

Create a new zone.

c. When the **New Zone Wizard** displays, click **Next**.



New Zone Wizard

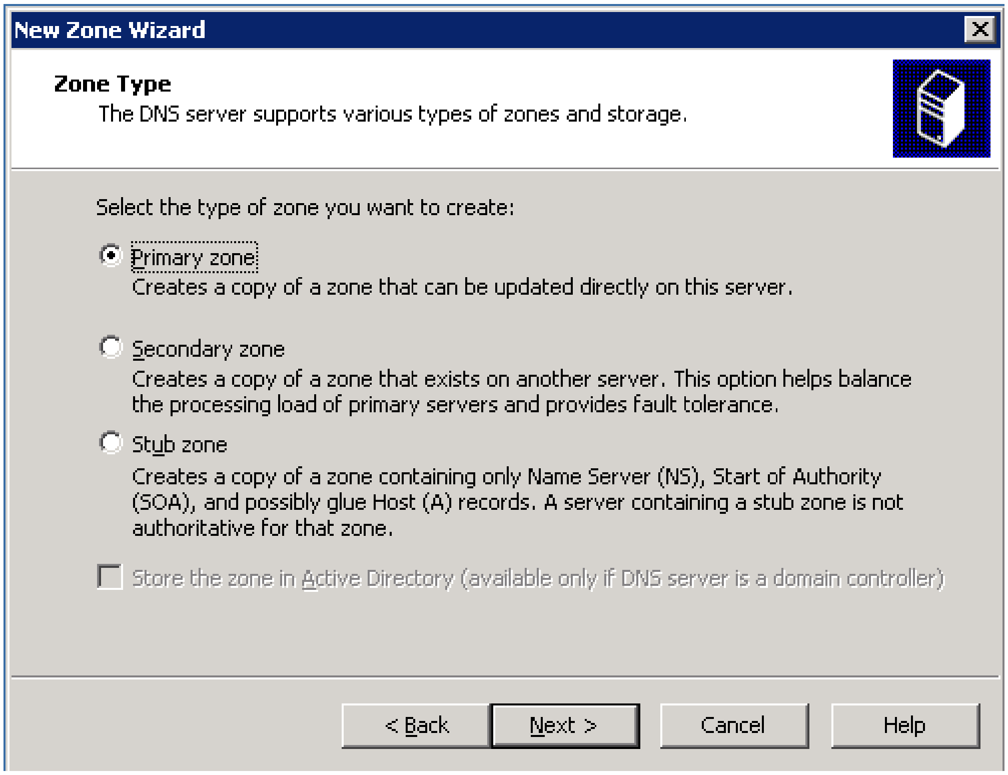
Welcome to the New Zone Wizard

This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.

d. By default, the **Primary zone** radio button is selected. Click **Next** to create a **Primary zone**.



New Zone Wizard

Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

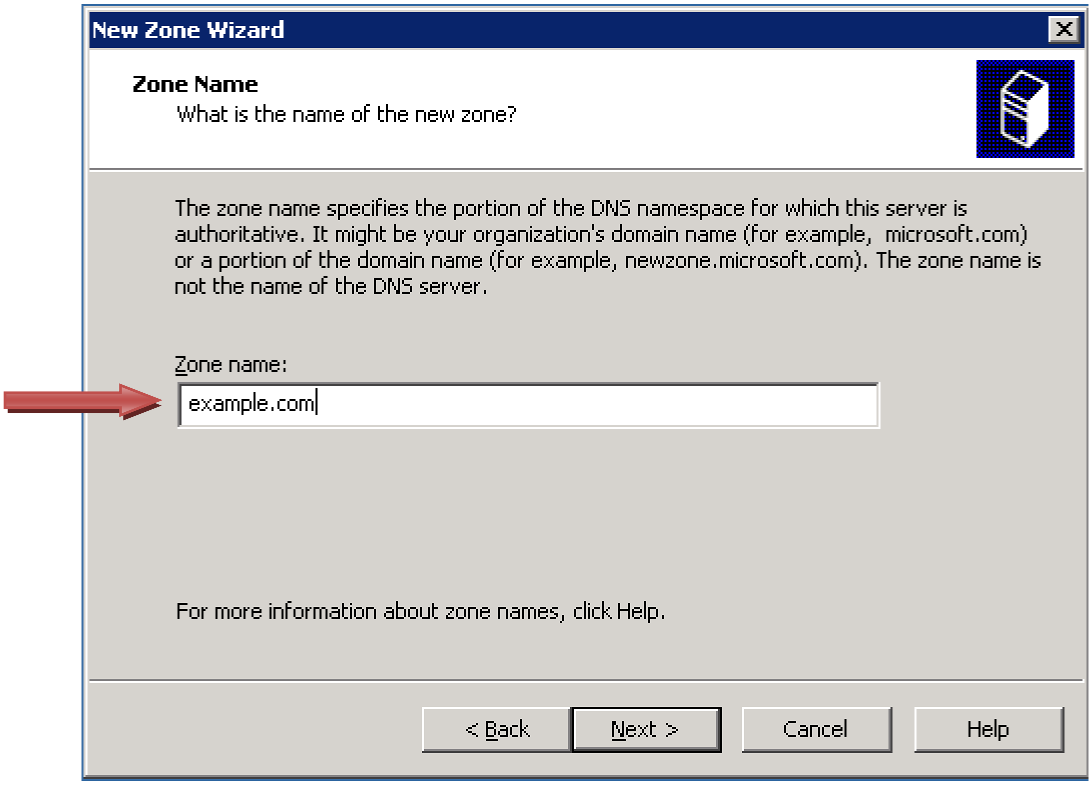
● Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a domain controller)

e. Enter the domain name, **example.com**, into the Zone name field and click **Next**.



New Zone Wizard

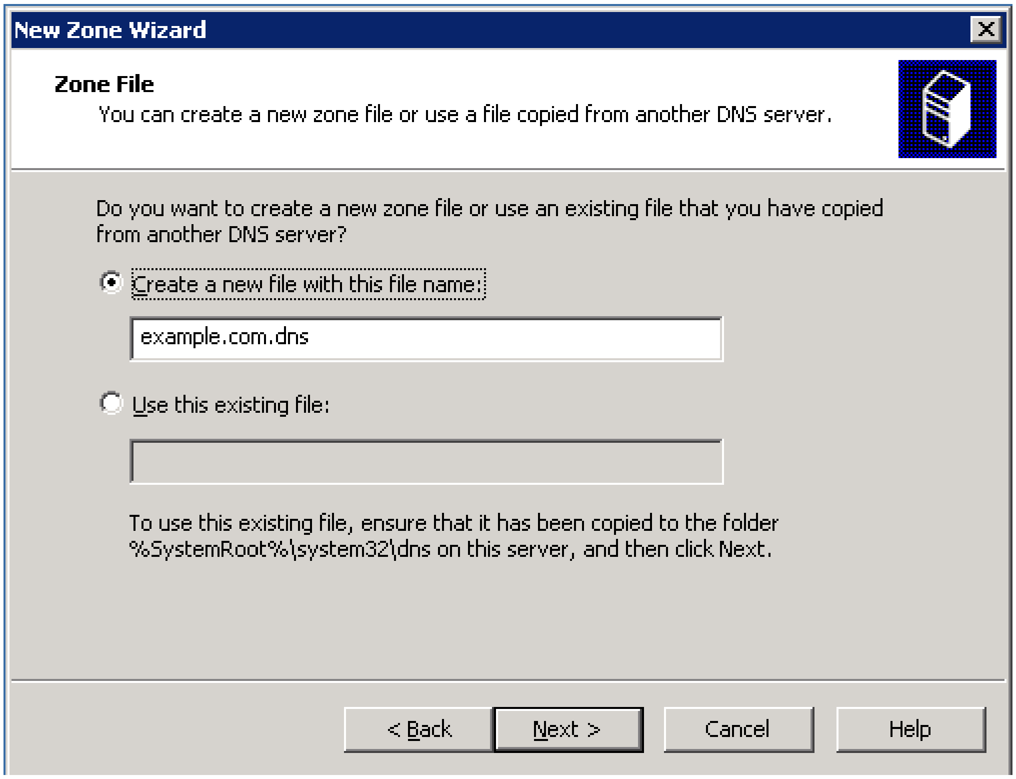
Zone Name
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: example.com

For more information about zone names, click Help.

f. Click **Next** to create a new file with this name.



New Zone Wizard

Zone File
You can create a new zone file or use a file copied from another DNS server.

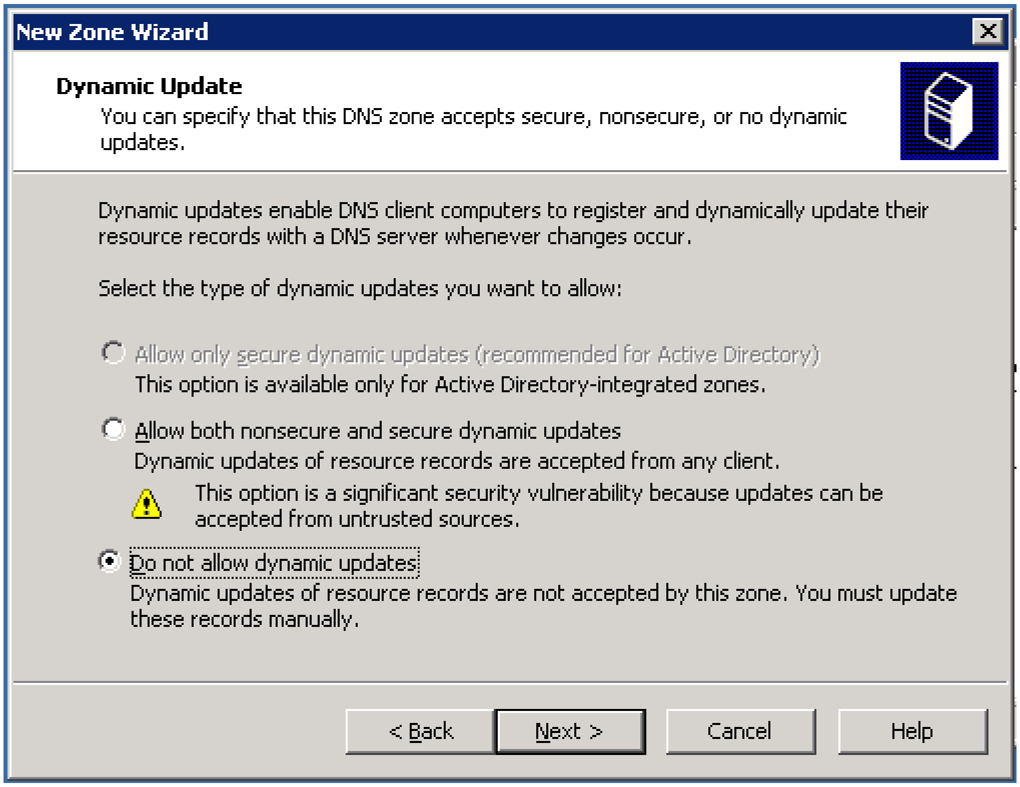
Do you want to create a new zone file or use an existing file that you have copied from another DNS server?

● Create a new file with this file name: example.com.dns

○ Use this existing file:

To use this existing file, ensure that it has been copied to the folder %SystemRoot%\system32\dns on this server, and then click Next.

g. Notice the option to enable dynamic updates. It is disabled by default for security. You will leave it disabled as well. Click **Next**.



Dynamic Update

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

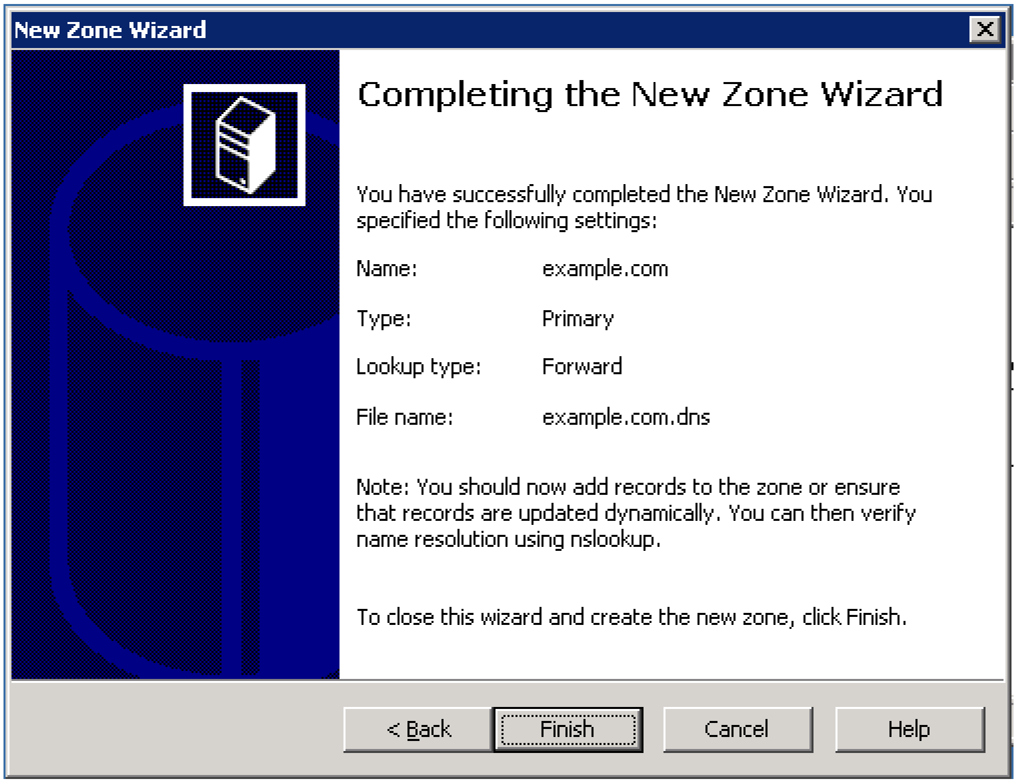
Select the type of dynamic updates you want to allow:

○ Allow only secure dynamic updates (recommended for Active Directory)
This option is available only for Active Directory-integrated zones.

○ Allow both nonsecure and secure dynamic updates
Dynamic updates of resource records are accepted from any client.
⚠ This option is a significant security vulnerability because updates can be accepted from untrusted sources.

● Do not allow dynamic updates
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

h. Click **Finish** to create the primary forward lookup zone.



Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

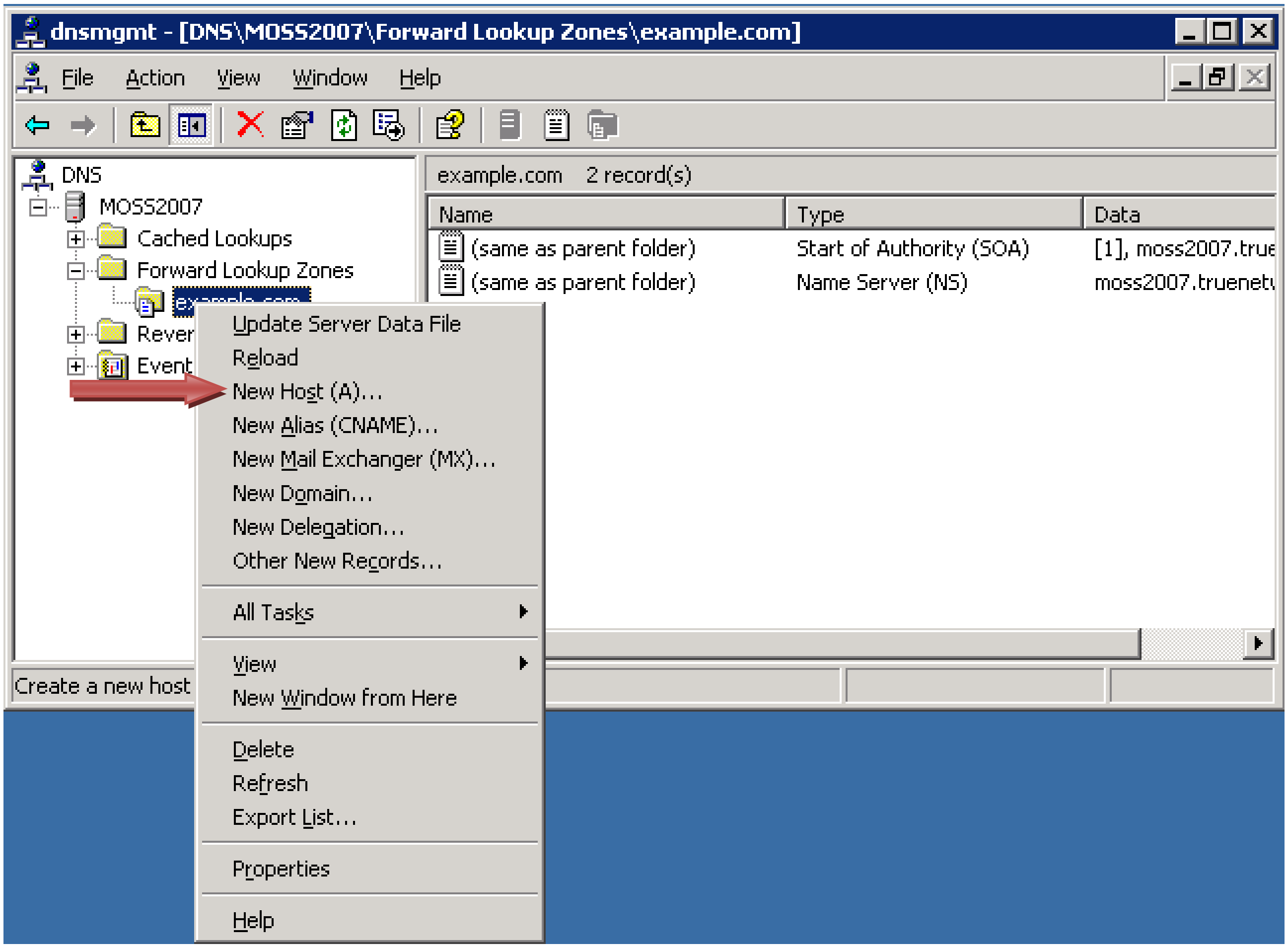
Name:	example.com
Type:	Primary
Lookup type:	Forward
File name:	example.com.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

Step 2: Add a Host record to the Primary forward lookup zone

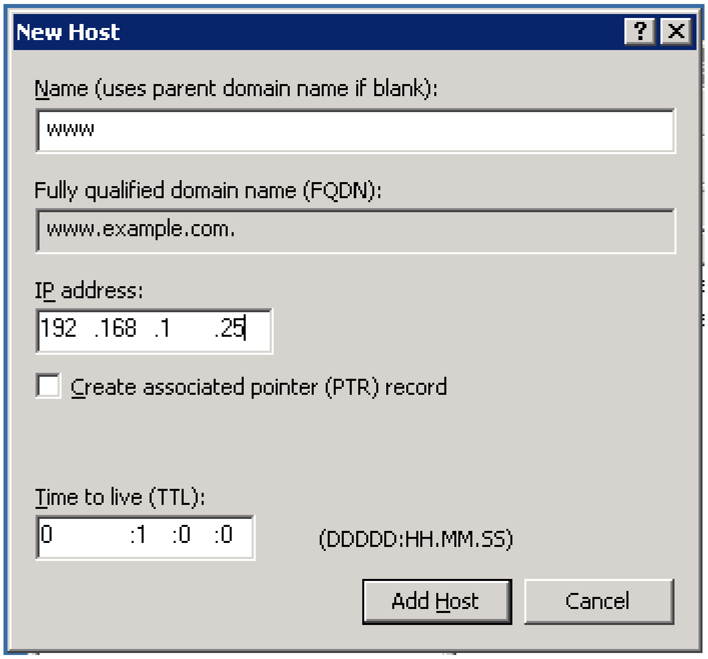
a. Right-click the **example.com** forward lookup zone and choose **New Host (A)**.



example.com 2 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], moss2007.true
(same as parent folder)	Name Server (NS)	moss2007.truenetv

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.



New Host

Name (uses parent domain name if blank):
www

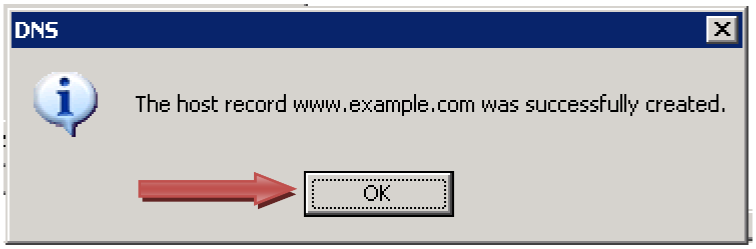
Fully qualified domain name (FQDN):
www.example.com.

IP address:
192 .168 .1 .25

□ Create associated pointer (PTR) record

Time to live (TTL):
0 :1 :0 :0 (DDDDD:HH.MM.SS)

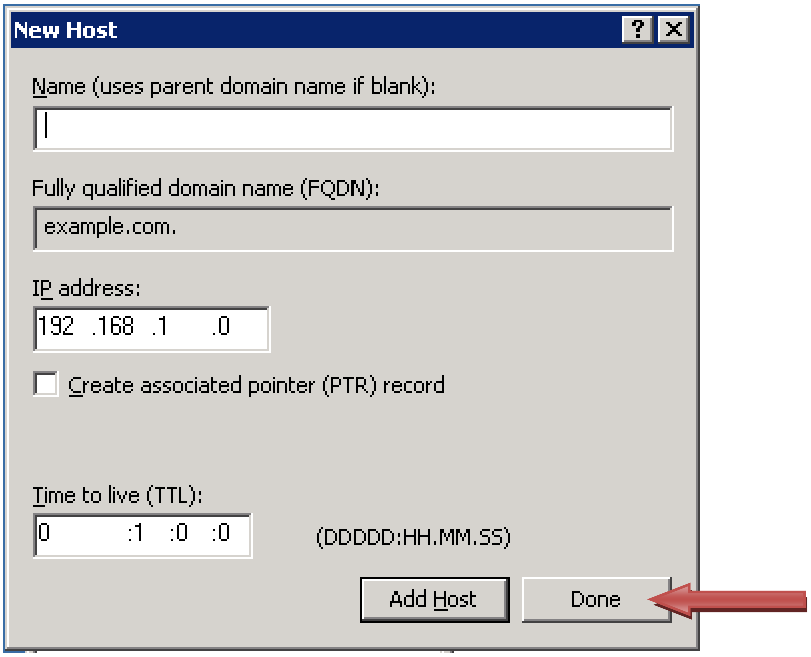
c. Click **OK**.



DNS

The host record www.example.com was successfully created.

d. Click **Done**.



New Host

Name (uses parent domain name if blank):

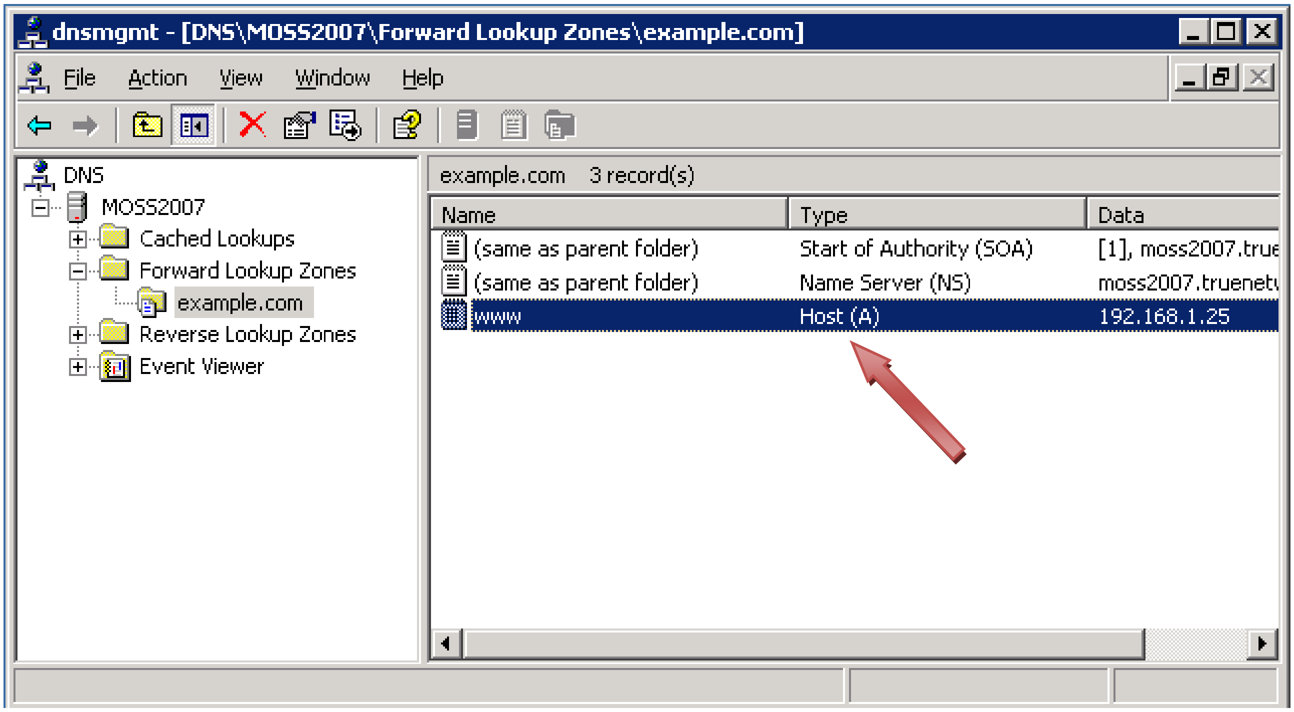
Fully qualified domain name (FQDN): example.com.

IP address: 192 .168 .1 .0

□ Create associated pointer (PTR) record

Time to live (TTL): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

The host record is now in your DNS zone.



dnsmgmt - [DNS\MOSS2007\Forward Lookup Zones\example.com]

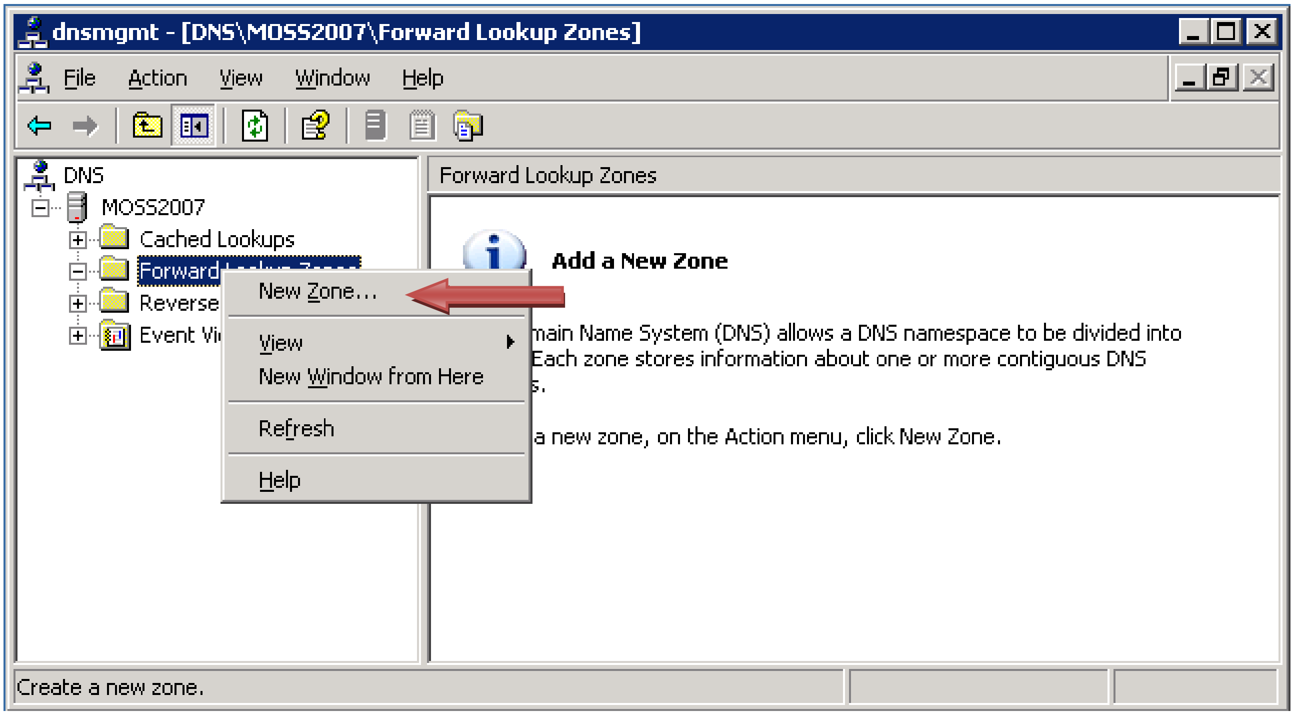
example.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], moss2007.true
(same as parent folder)	Name Server (NS)	moss2007.truenet
www	Host (A)	192.168.1.25

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**.

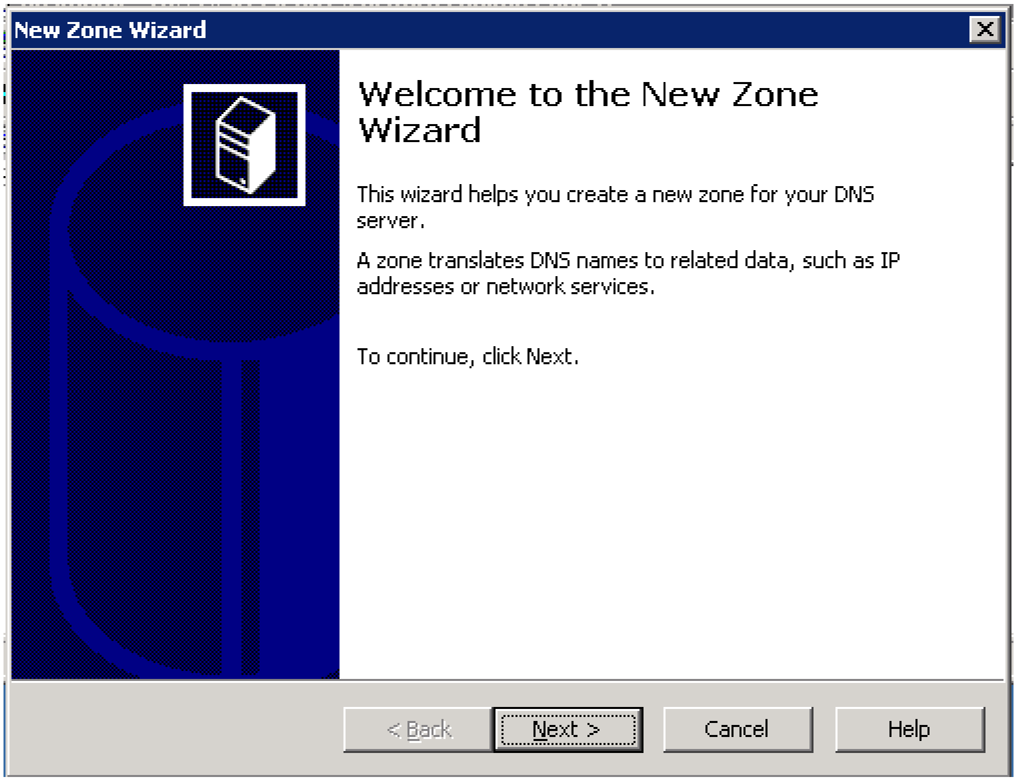


main Name System (DNS) allows a DNS namespace to be divided into
Each zone stores information about one or more contiguous DNS
s.

a new zone, on the Action menu, click New Zone.

Create a new zone.

c. When the **New Zone Wizard** displays, click **Next**.



New Zone Wizard

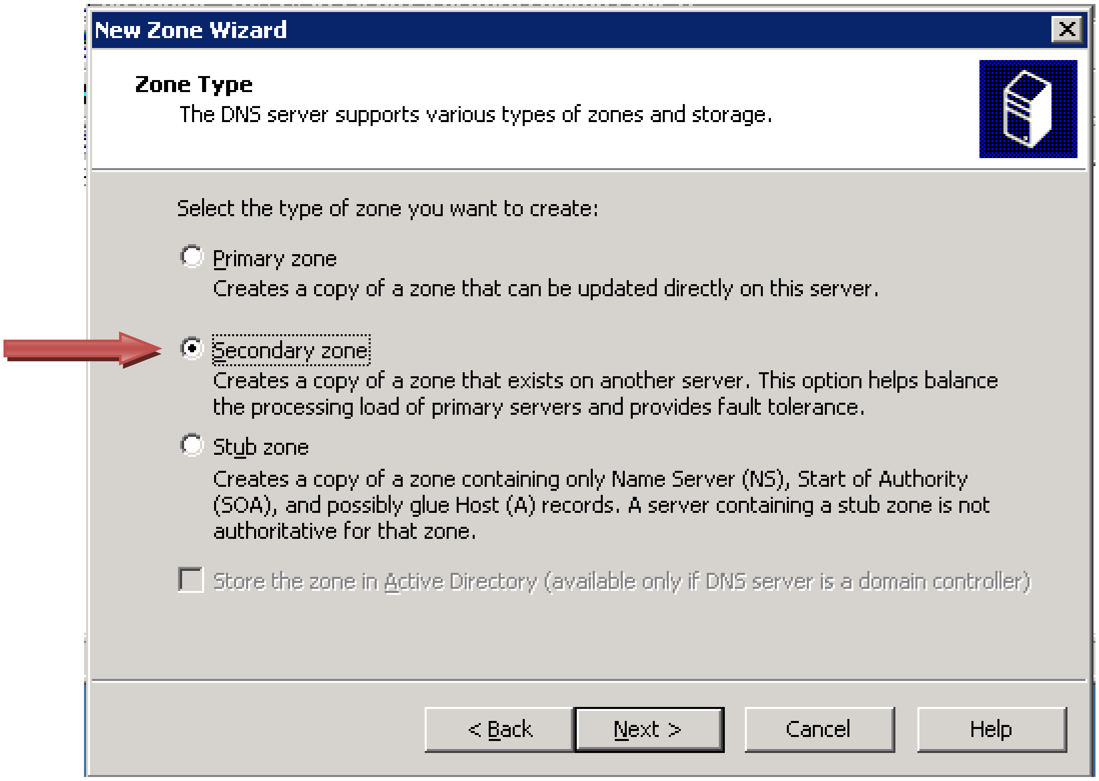
Welcome to the New Zone Wizard

This wizard helps you create a new zone for your DNS server.

A zone translates DNS names to related data, such as IP addresses or network services.

To continue, click Next.

d. Click the **Secondary zone** radio button, and then click **Next**.



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

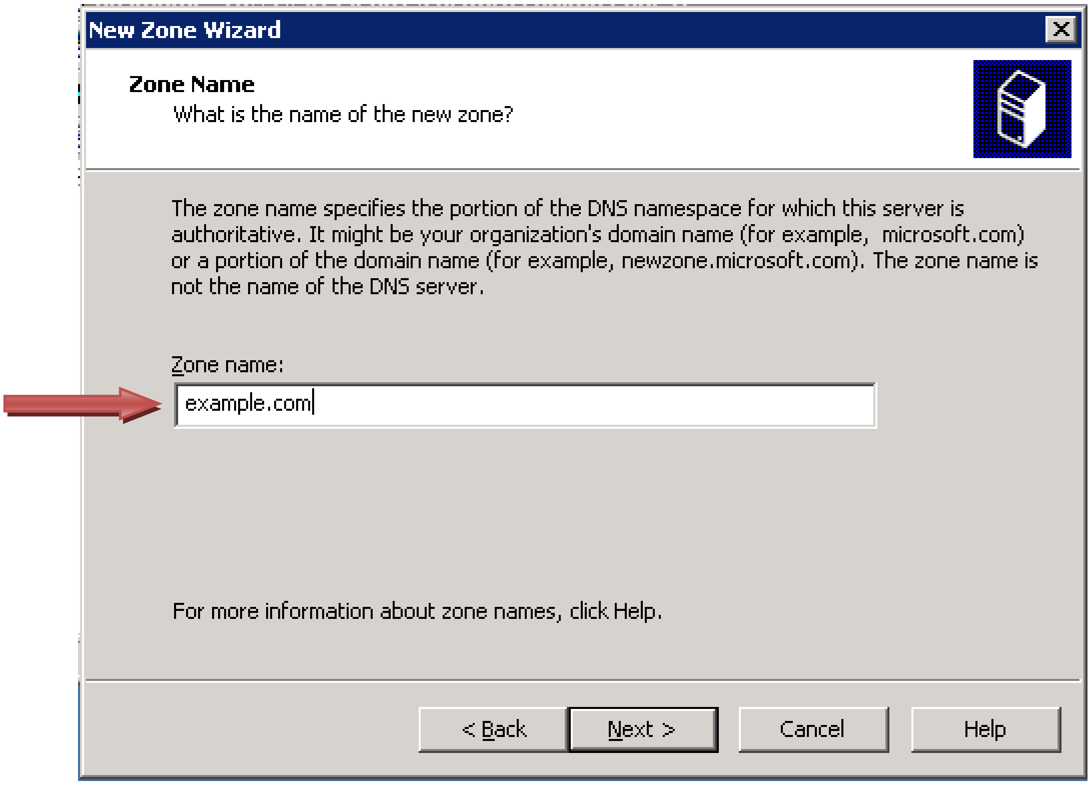
○ Primary zone
Creates a copy of a zone that can be updated directly on this server.

● Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

○ Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

□ Store the zone in Active Directory (available only if DNS server is a domain controller)

e. Type **example.com** in the Zone name field, and then click **Next**.



New Zone Wizard

Zone Name

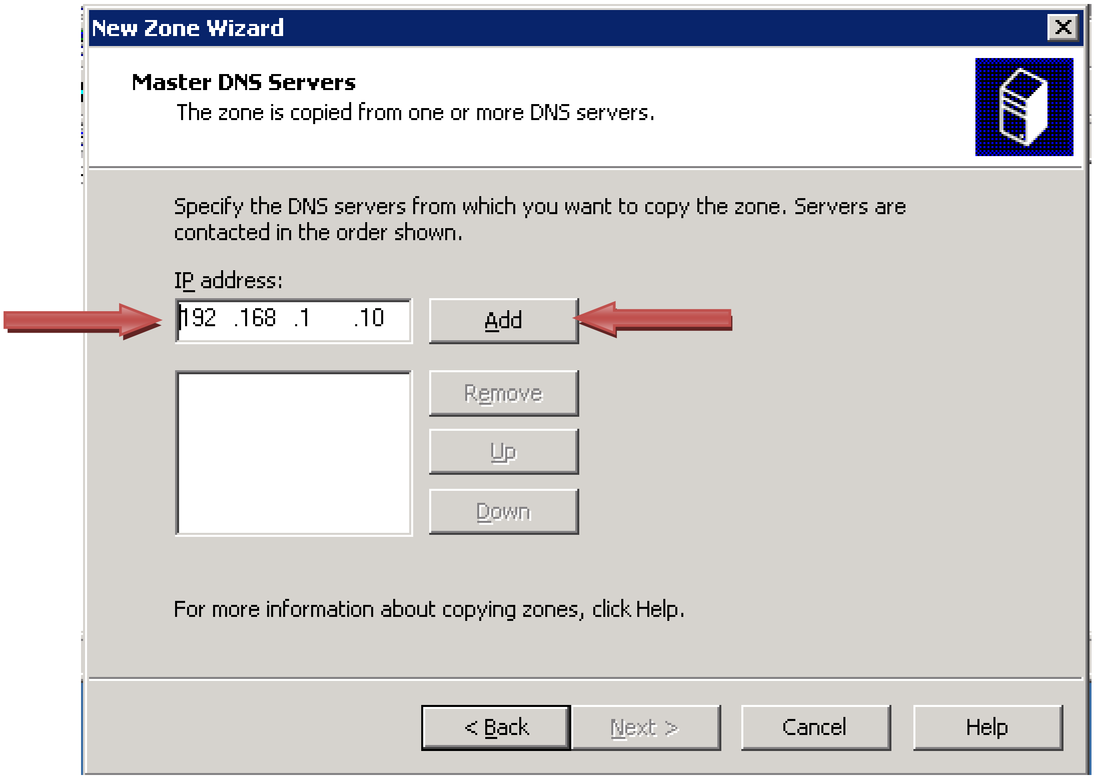
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: example.com

For more information about zone names, click Help.

f. In the IP address field, type **192.168.1.10**, which is the IP address of the primary server. Then click **Add**.



New Zone Wizard

Master DNS Servers

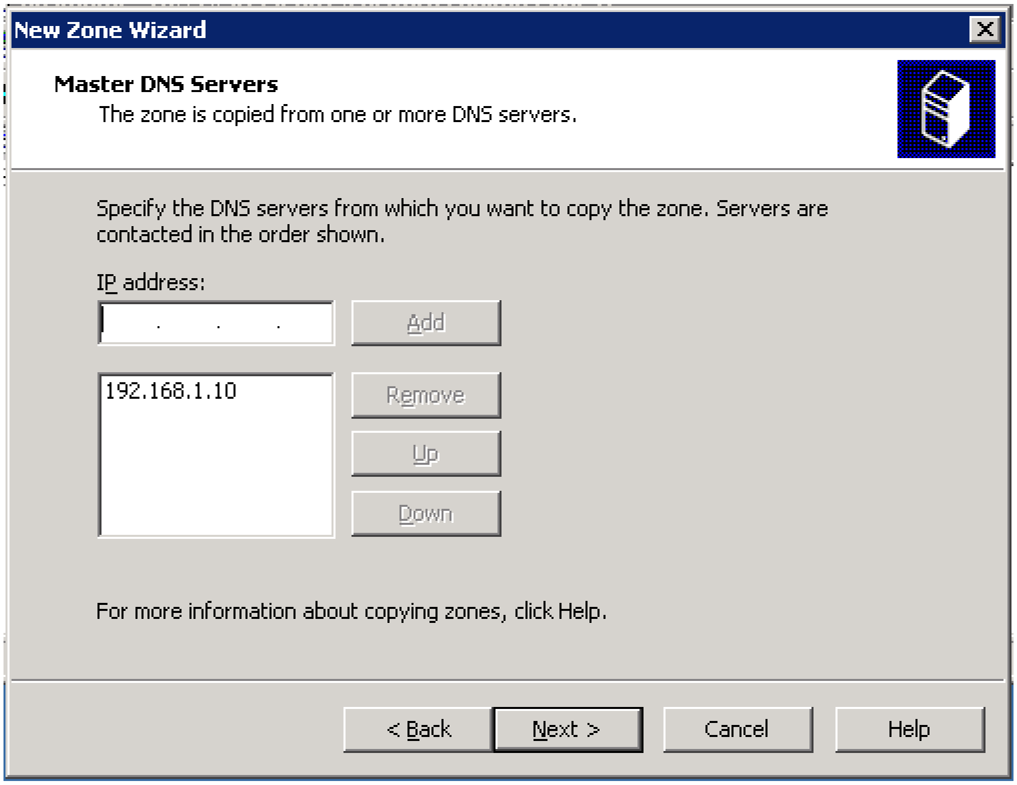
The zone is copied from one or more DNS servers.

Specify the DNS servers from which you want to copy the zone. Servers are contacted in the order shown.

IP address: 192 .168 .1 .10

For more information about copying zones, click Help.

g. Click **Next**.



New Zone Wizard

Master DNS Servers

The zone is copied from one or more DNS servers.

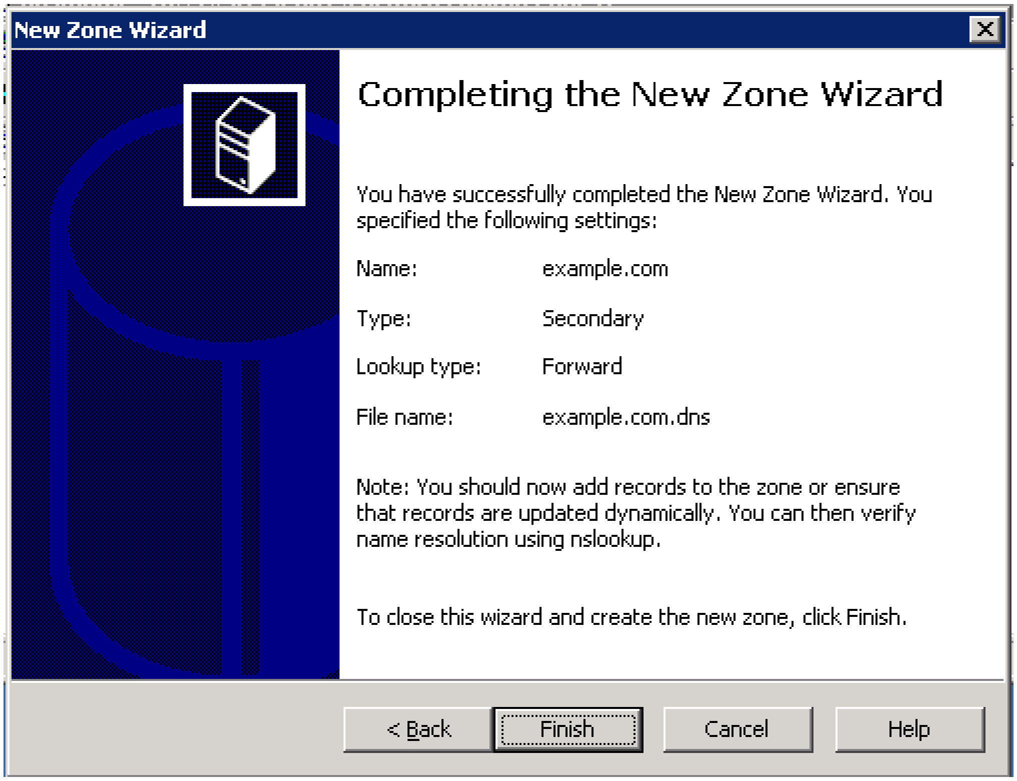
Specify the DNS servers from which you want to copy the zone. Servers are contacted in the order shown.

IP address:

192.168.1.10

For more information about copying zones, click Help.

h. Click **Finish**.



New Zone Wizard

Completing the New Zone Wizard

You have successfully completed the New Zone Wizard. You specified the following settings:

Name: example.com

Type: Secondary

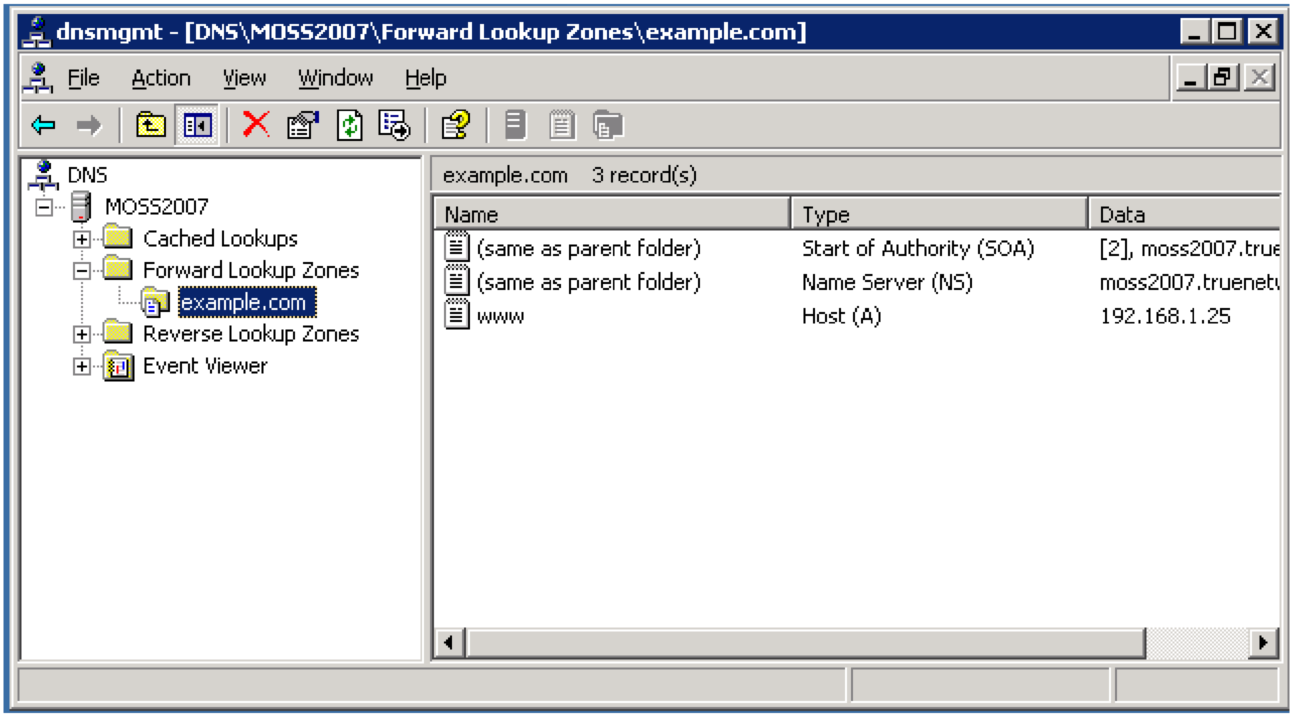
Lookup type: Forward

File name: example.com.dns

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

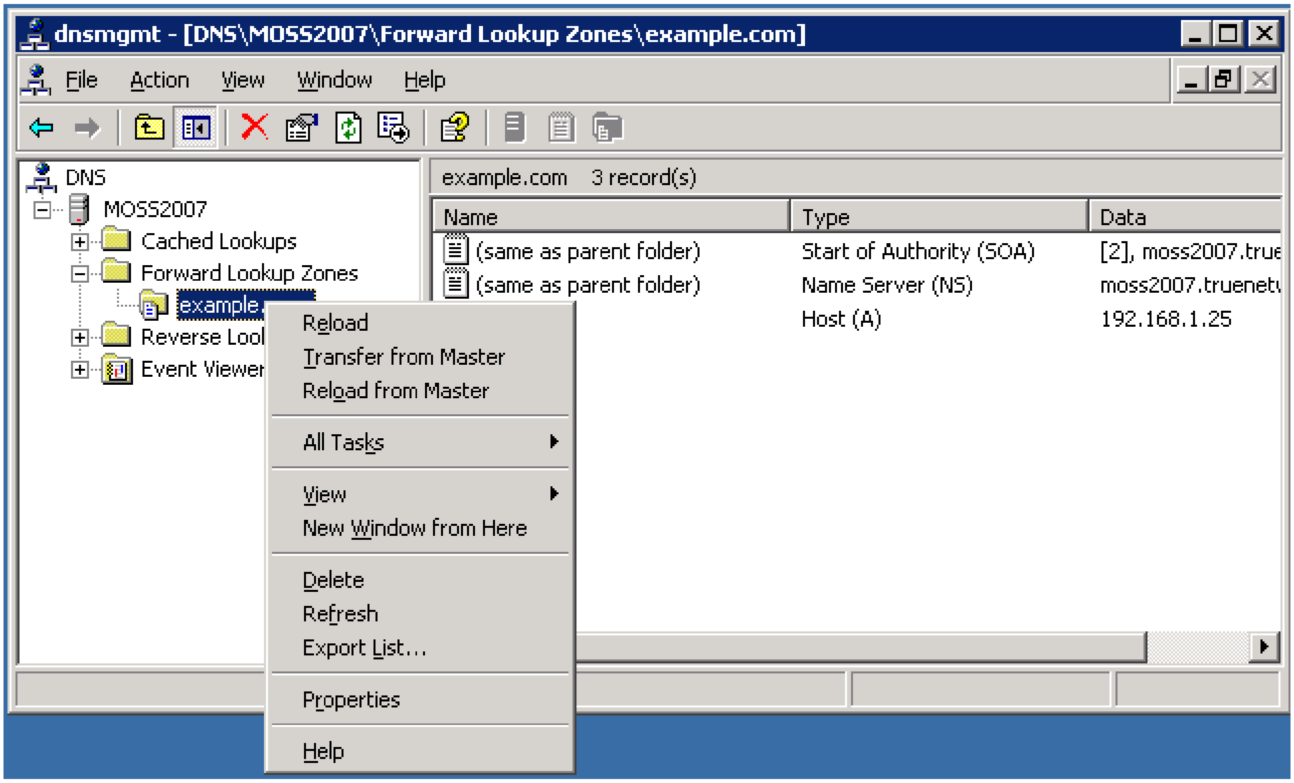
i. When you view the secondary zone, notice that the www host record created on the primary server has transferred down to the secondary server.



example.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2], moss2007.true
(same as parent folder)	Name Server (NS)	moss2007.truenet\
www	Host (A)	192.168.1.25

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.



example.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[2], moss2007.true
(same as parent folder)	Name Server (NS)	moss2007.truenet\
	Host (A)	192.168.1.25

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 – Securing local data

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:

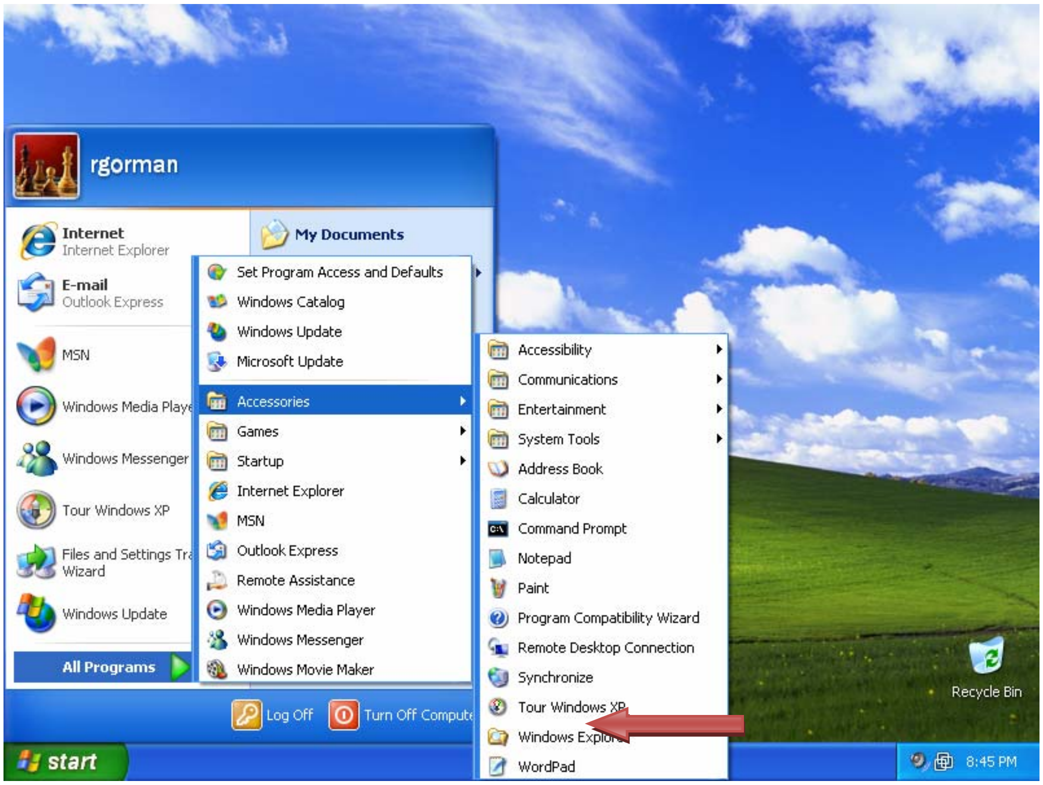
- Windows XP Professional computer with administrative access
- NTFS File System on the computer and Simple File Sharing turned off (under the Folder Options of Windows Explorer.)
- User accounts preconfigured for users Bob and Joe
- Internet connectivity

Part 1 – Securing local data

Step 1: Secure Bob's Files folder

a. Log in to the Windows XP computer as administrator.

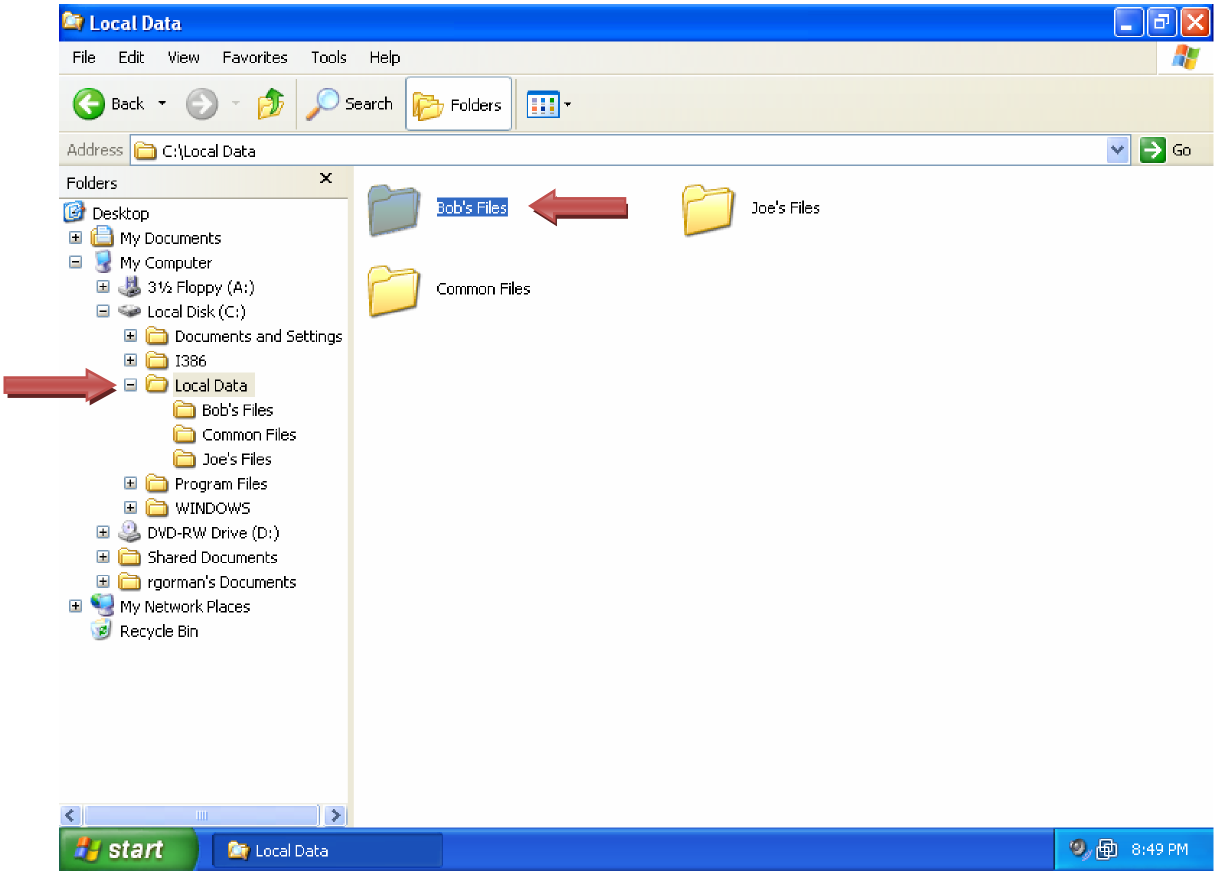
b. From the **Accessories** menu, launch Windows Explorer.



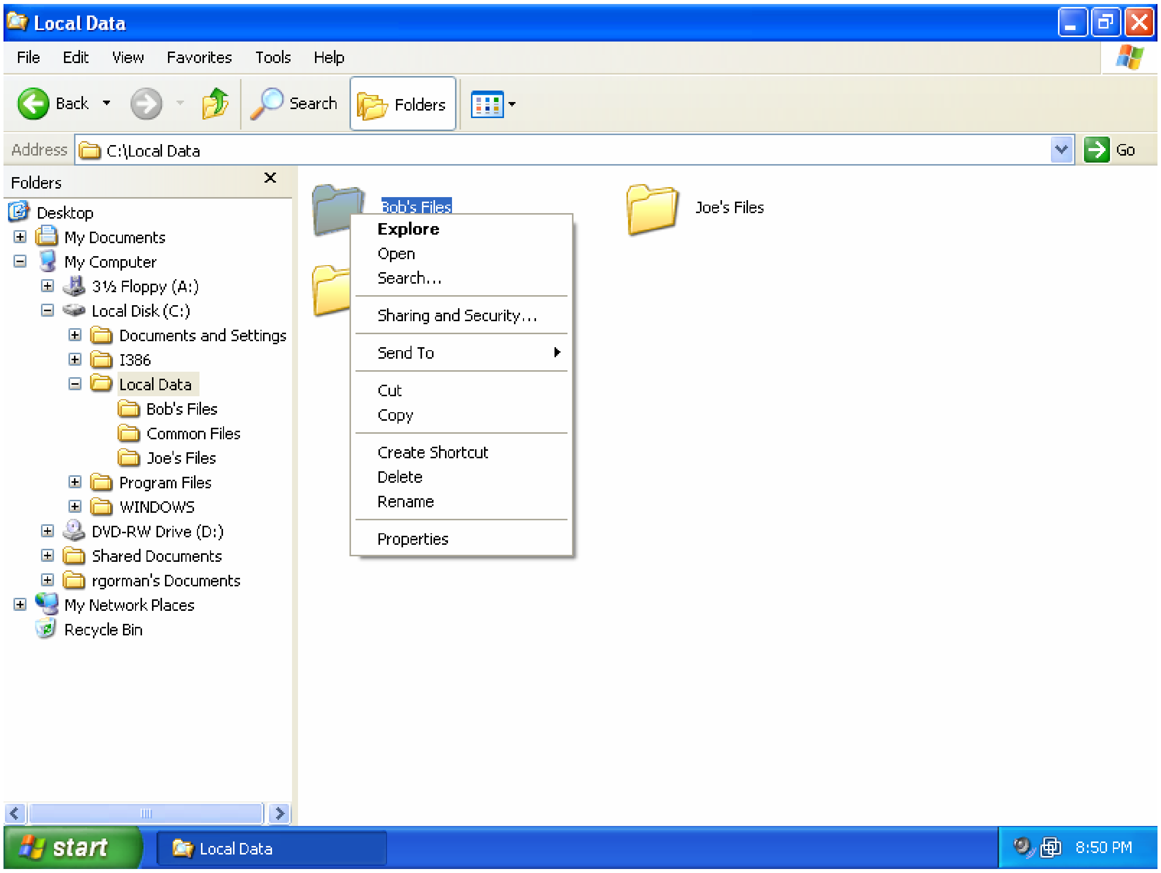
c. Use Windows Explorer to create a folder on Local Disk (C:) called **Local Data**. From the **File** menu, click **New**, and then click **Folder**.

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.

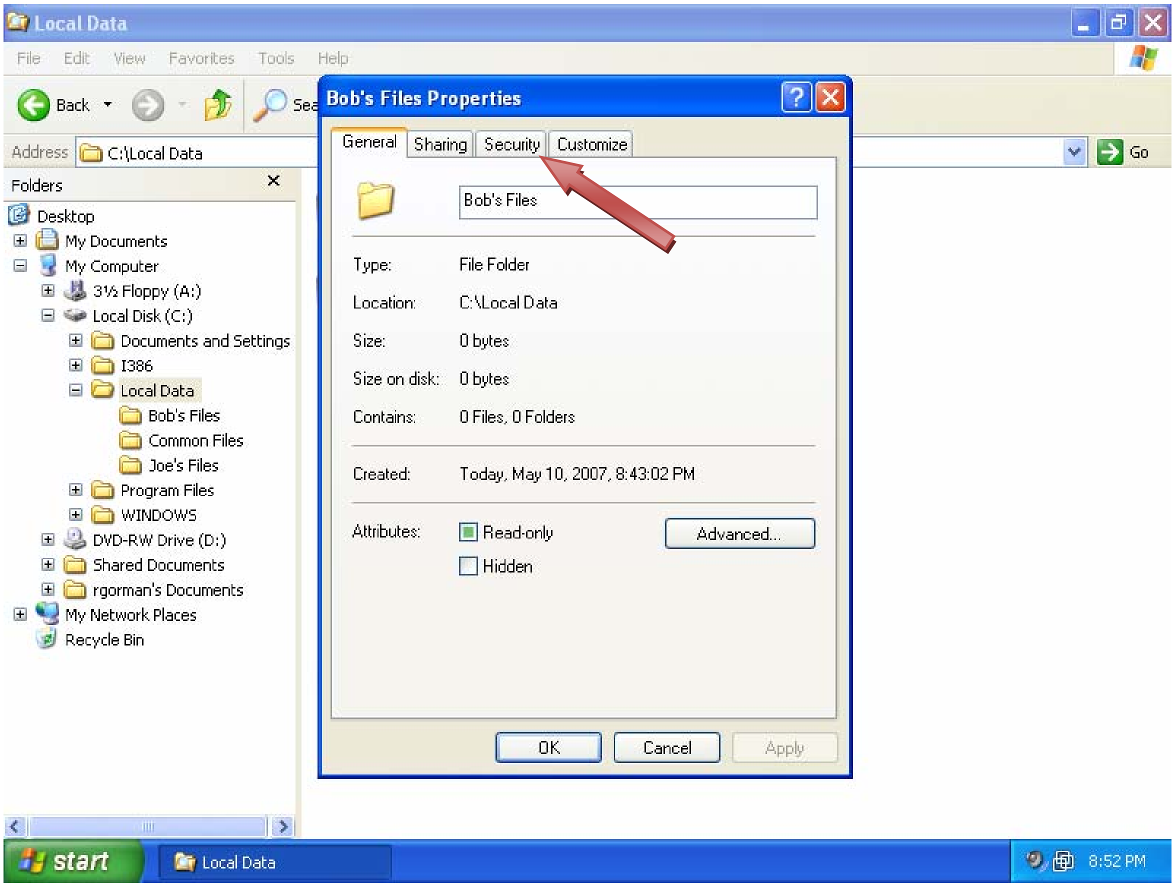


f. Right-click the **Bob's Files** folder and choose **Properties**.



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.



Bob's Files

Type: File Folder

Location: C:\Local Data

Size: 0 bytes

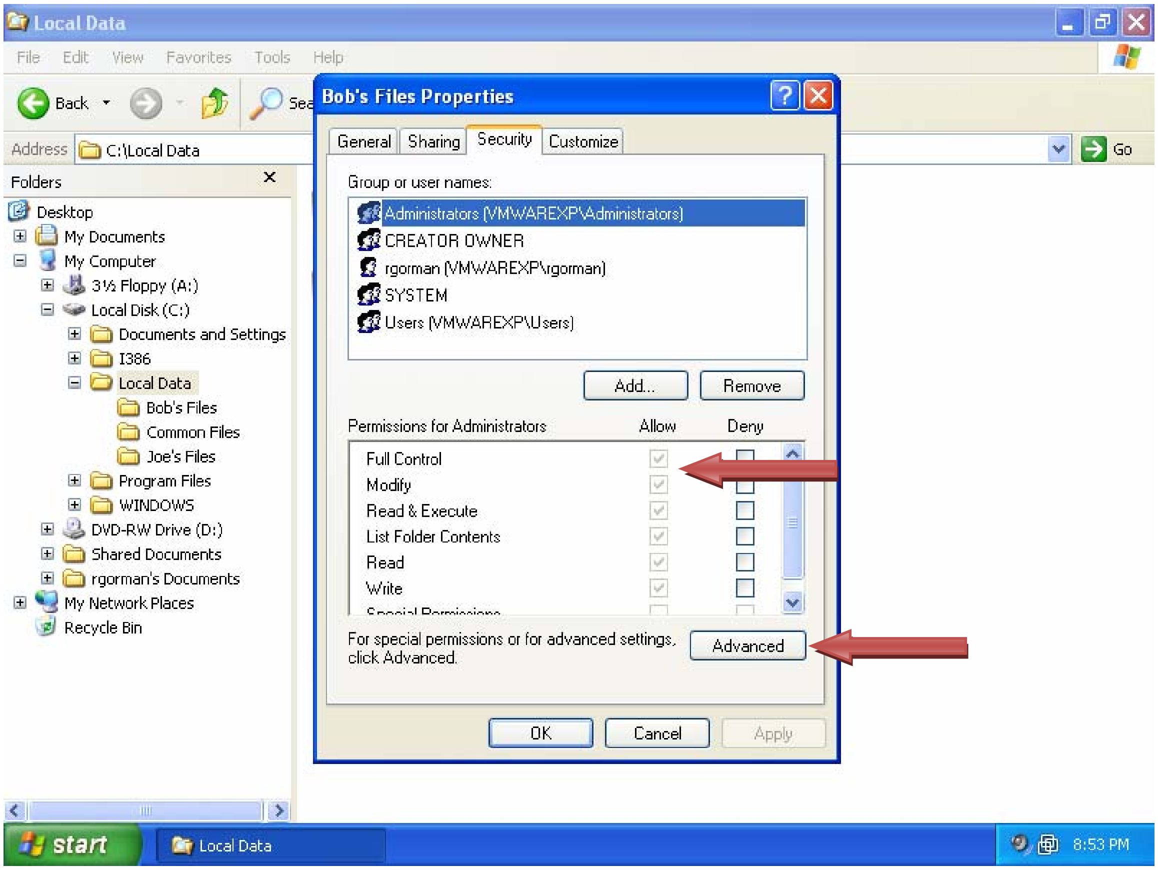
Size on disk: 0 bytes

Contains: 0 Files, 0 Folders

Created: Today, May 10, 2007, 8:43:02 PM

Attributes: ☑ Read-only ☐ Hidden

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.



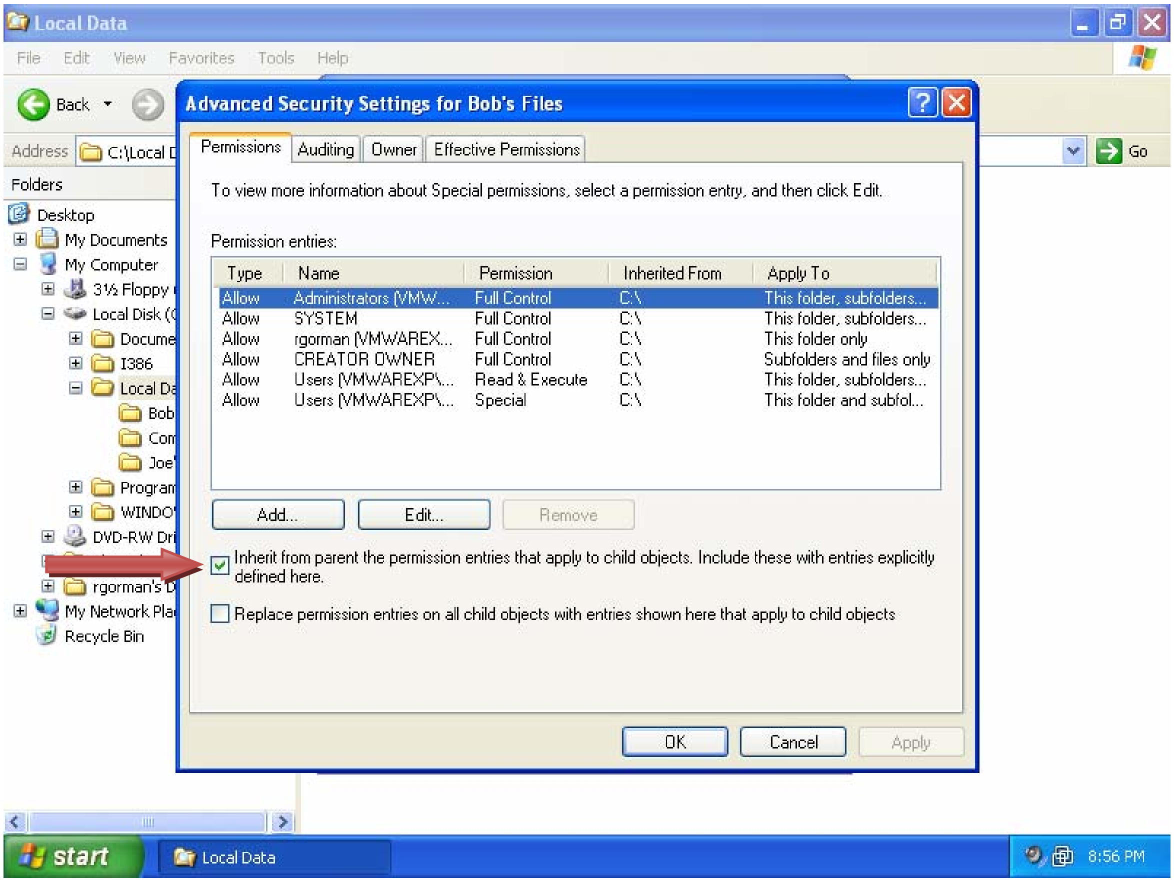
Group or user names:

- Administrators (VMWAREXP\Administrators)
- CREATOR OWNER
- rgorman (VMWAREXP\rgorman)
- SYSTEM
- Users (VMWAREXP\Users)

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

i. Uncheck the check box next to **Inherit from parent the permission entries that apply to child objects**.



Advanced Security Settings for Bob's Files

Permissions | Auditing | Owner | Effective Permissions

To view more information about Special permissions, select a permission entry, and then click Edit.

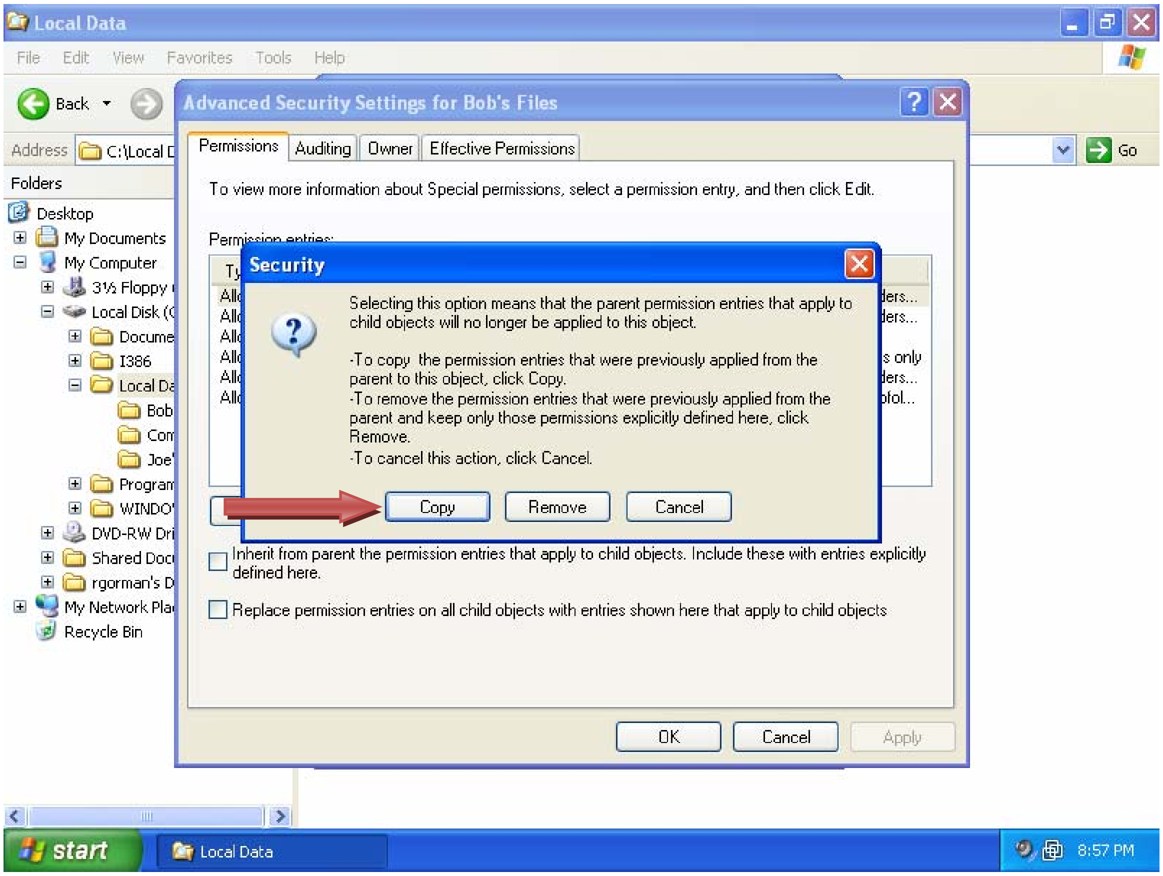
Permission entries:

Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (VMW...	Full Control	C:\	This folder, subfolders...
Allow	SYSTEM	Full Control	C:\	This folder, subfolders...
Allow	rgorman (VMWAREX...	Full Control	C:\	This folder only
Allow	CREATOR OWNER	Full Control	C:\	Subfolders and files only
Allow	Users (VMWAREXP\...	Read & Execute	C:\	This folder, subfolders...
Allow	Users (VMWAREXP\...	Special	C:\	This folder and subfol...

☑ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

j. Click **Copy** to retain the existing permissions.



To view more information about Special permissions, select a permission entry, and then click Edit.

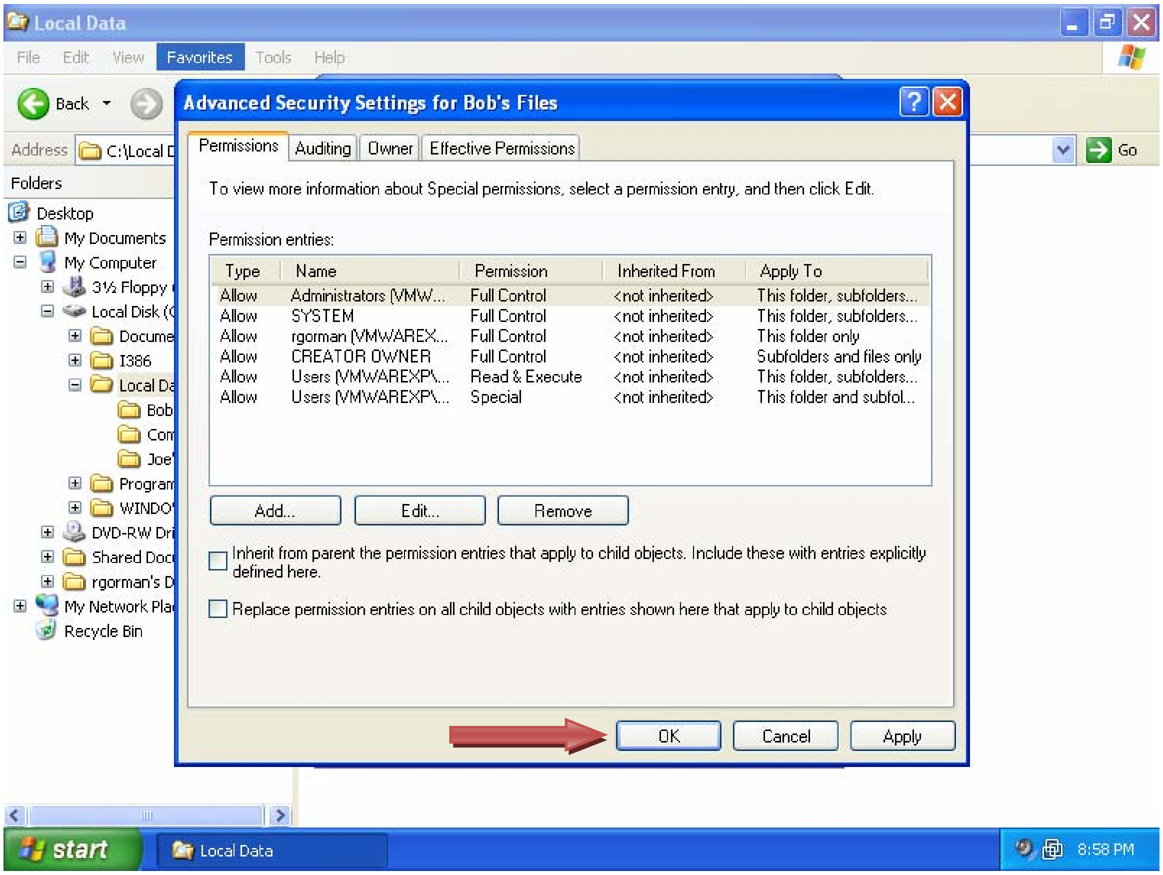
Selecting this option means that the parent permission entries that apply to child objects will no longer be applied to this object.

-To copy the permission entries that were previously applied from the parent to this object, click Copy.
-To remove the permission entries that were previously applied from the parent and keep only those permissions explicitly defined here, click Remove.
-To cancel this action, click Cancel.

☐ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

☐ Replace permission entries on all child objects with entries shown here that apply to child objects

k. Click **OK.**



Advanced Security Settings for Bob's Files

Permissions | Auditing | Owner | Effective Permissions

To view more information about Special permissions, select a permission entry, and then click Edit.

Permission entries:

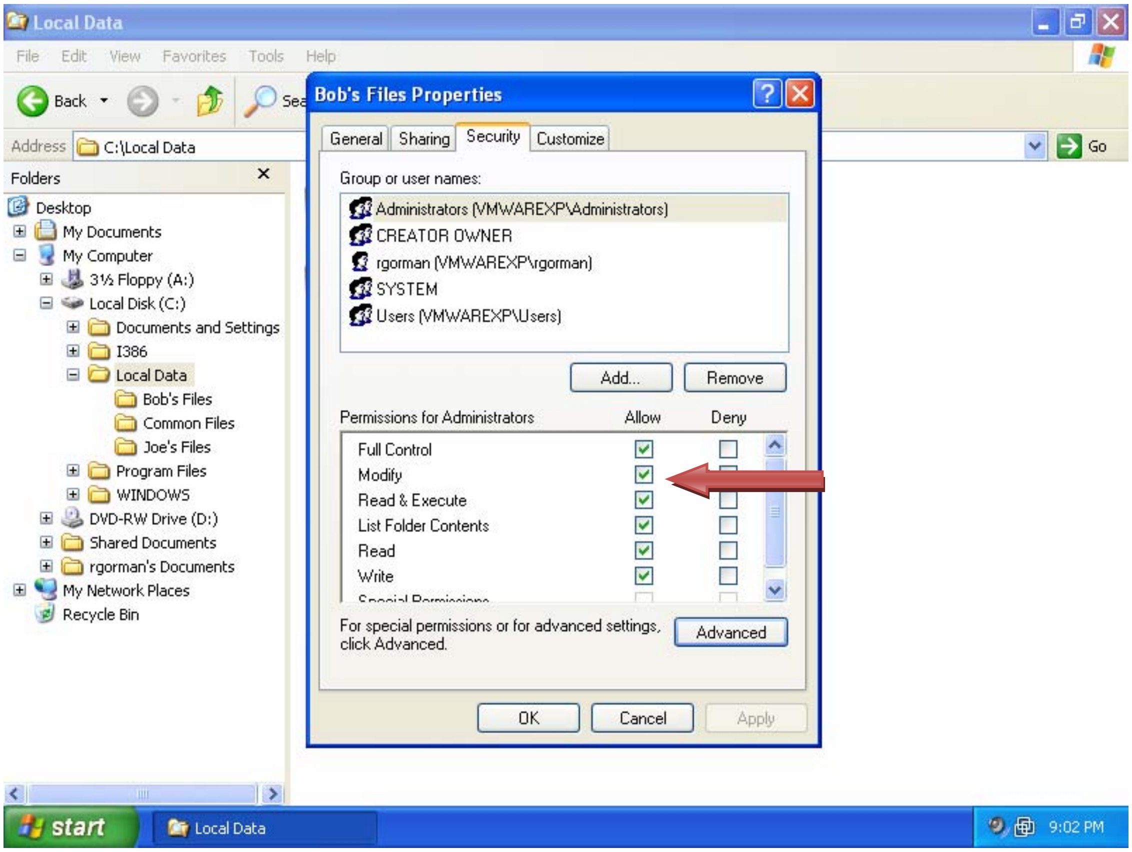
Type	Name	Permission	Inherited From	Apply To
Allow	Administrators (VMW...	Full Control	<not inherited>	This folder, subfolders...
Allow	SYSTEM	Full Control	<not inherited>	This folder, subfolders...
Allow	rgorman (VMWAREX...	Full Control	<not inherited>	This folder only
Allow	CREATOR OWNER	Full Control	<not inherited>	Subfolders and files only
Allow	Users (VMWAREXP\...	Read & Execute	<not inherited>	This folder, subfolders...
Allow	Users (VMWAREXP\...	Special	<not inherited>	This folder and subfol...

Add... Edit... Remove

□ Inherit from parent the permission entries that apply to child objects. Include these with entries explicitly defined here.

□ Replace permission entries on all child objects with entries shown here that apply to child objects

Now that inheritance is turned off, you are able to modify the permissions.



Bob's Files Properties

General | Sharing | Security | Customize

Group or user names:

- Administrators (VMWAREXP\Administrators)
- CREATOR OWNER
- rgorman (VMWAREXP\rgorman)
- SYSTEM
- Users (VMWAREXP\Users)

Add... Remove

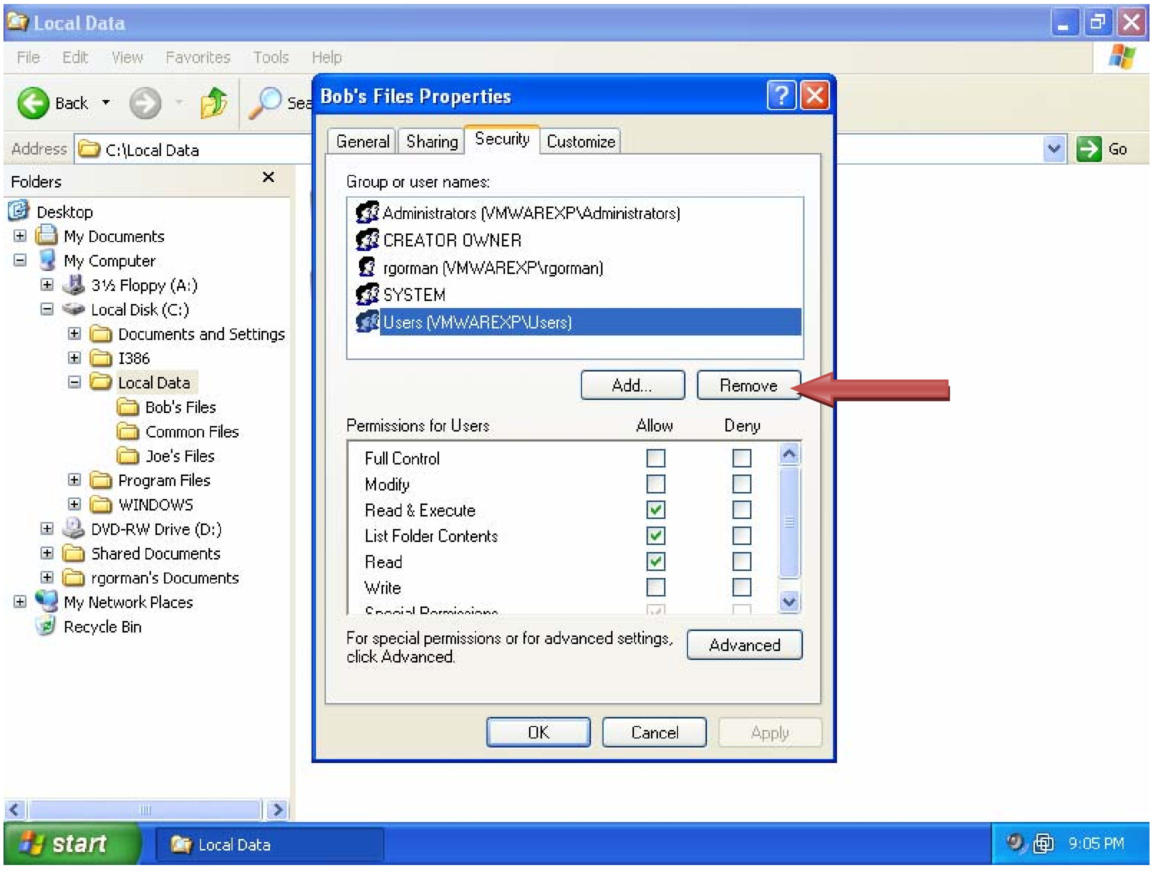
Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced. Advanced

OK Cancel Apply

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.

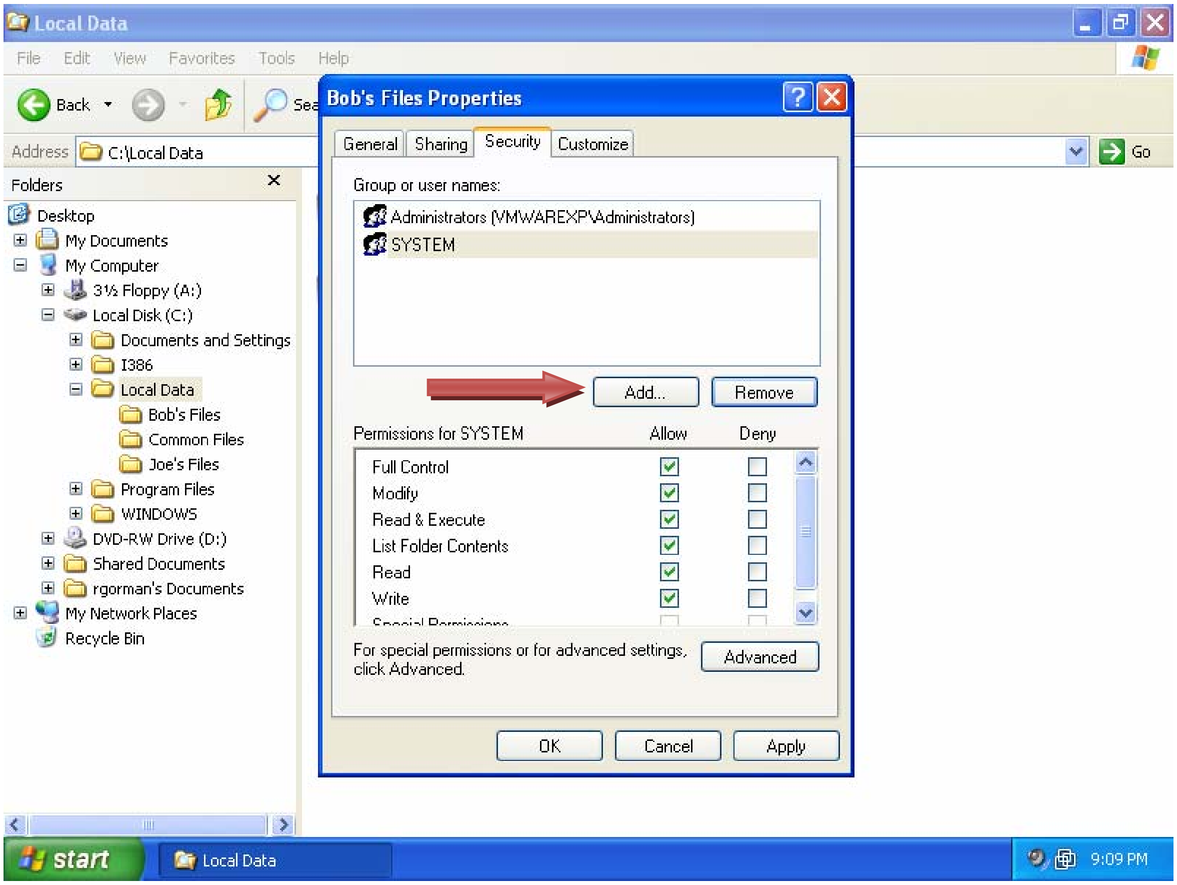


Group or user names:
- Administrators (VMWAREXP\Administrators)
- CREATOR OWNER
- rgorman (VMWAREXP\rgorman)
- SYSTEM
- Users (VMWAREXP\Users)

Permissions for Users	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

m. Now add Bob to the list. Click **Add**.



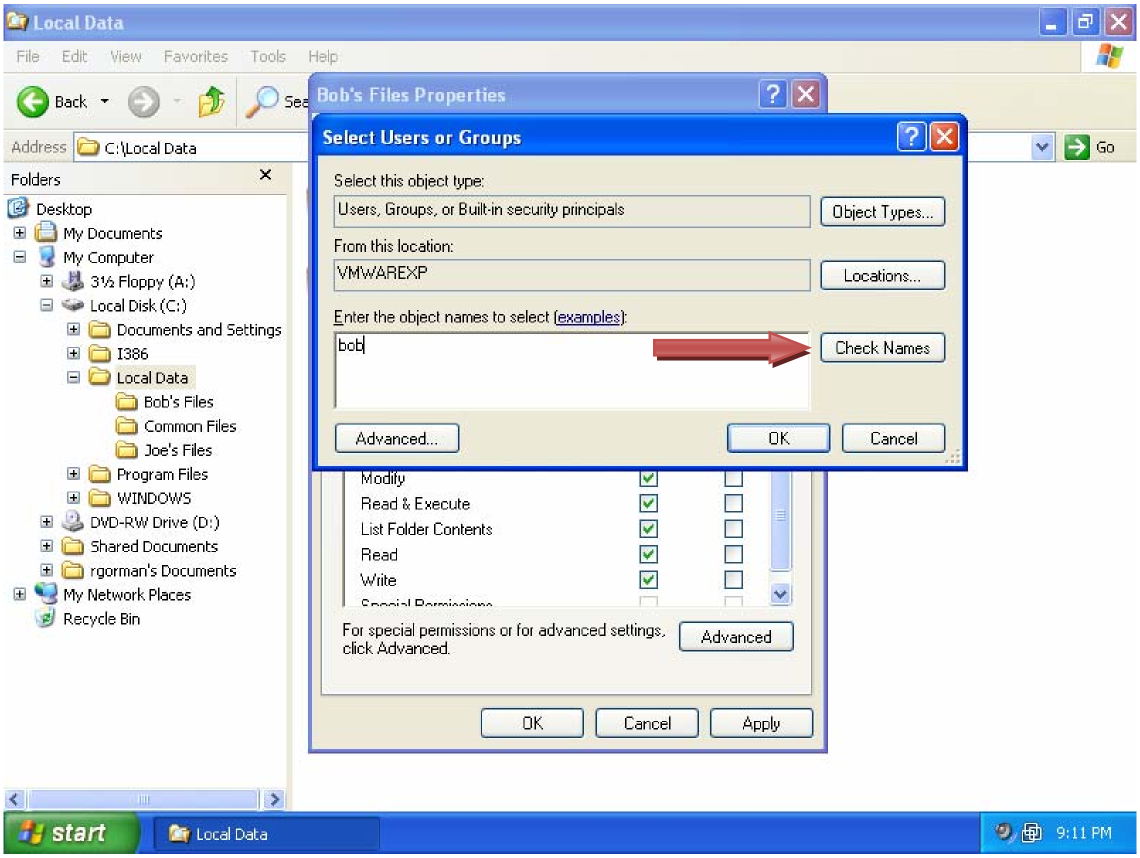
Group or user names:

Administrators (VMWAREXP\Administrators)
SYSTEM

Permissions for SYSTEM	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

n. Type **Bob** in the text box and click the **Check Names** button to verify his account.



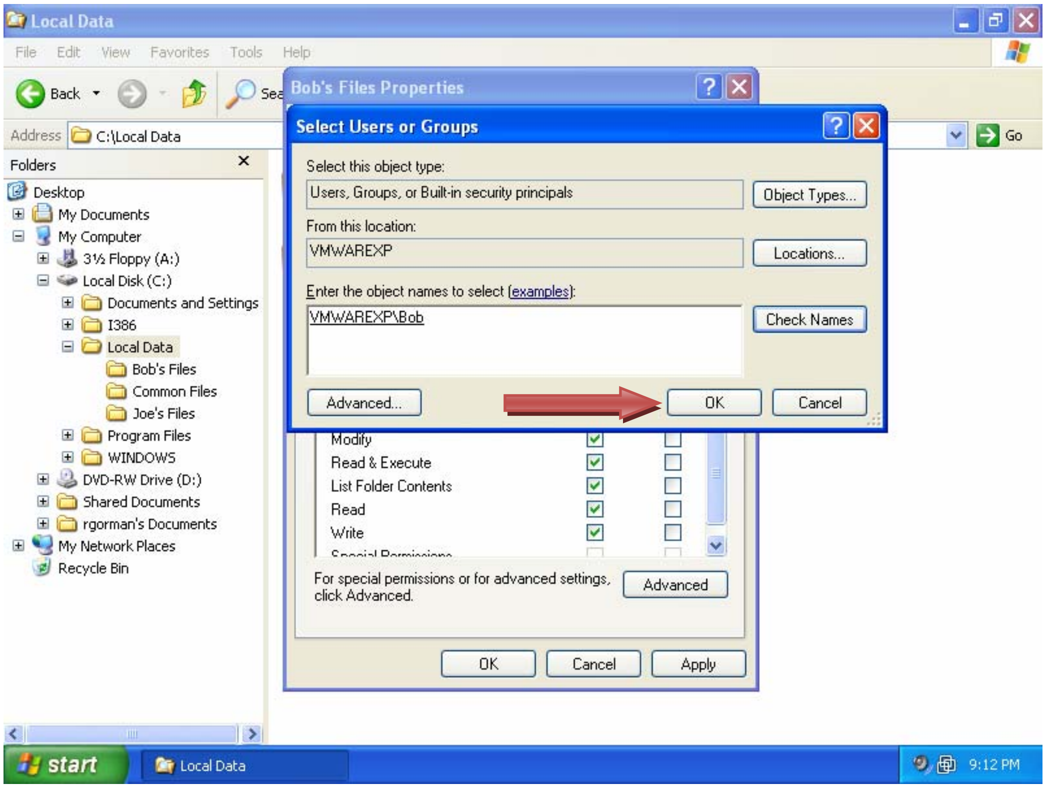
Select this object type:
Users, Groups, or Built-in security principals

From this location:
VMWAREXP

Enter the object names to select (examples):
bob

For special permissions or for advanced settings, click Advanced.

o. Now that Bob has been verified, click **OK**.

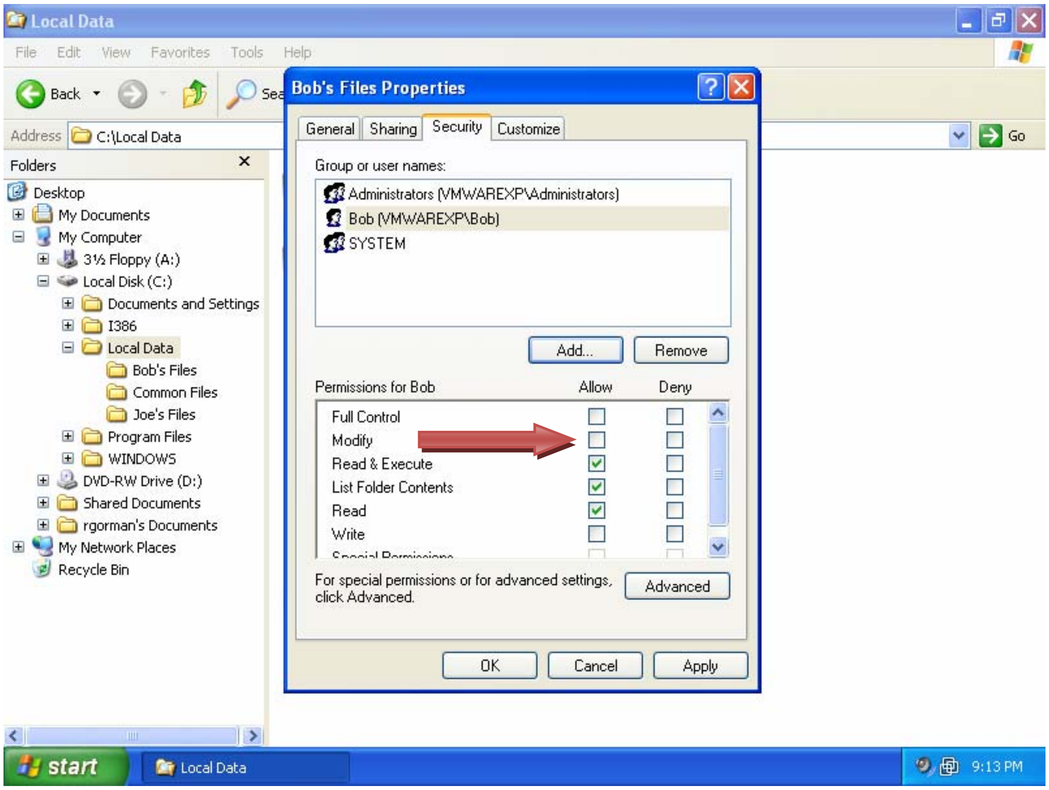


Select this object type: Users, Groups, or Built-in security principals

From this location: VMWAREXP

Enter the object names to select (examples): VMWAREXP\Bob

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**.



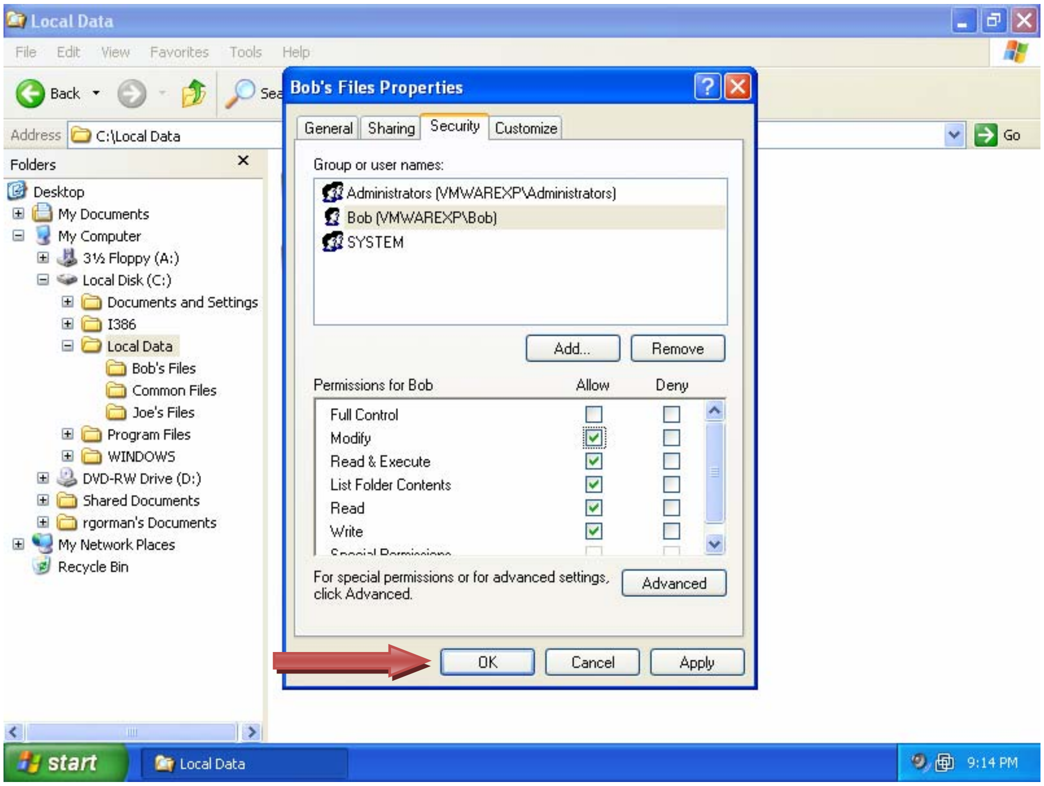
Group or user names:

Administrators (VMWAREXP\Administrators)
Bob (VMWAREXP\Bob)
SYSTEM

Permissions for Bob	Allow	Deny
Full Control	□	□
Modify	□	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	□	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

q. Now that Bob has been granted Modify permission, click **OK** to set the security.



Bob's Files Properties

General | Sharing | Security | Customize

Group or user names:

- Administrators (VMWAREXP\Administrators)
- Bob (VMWAREXP\Bob)
- SYSTEM

Add... Remove

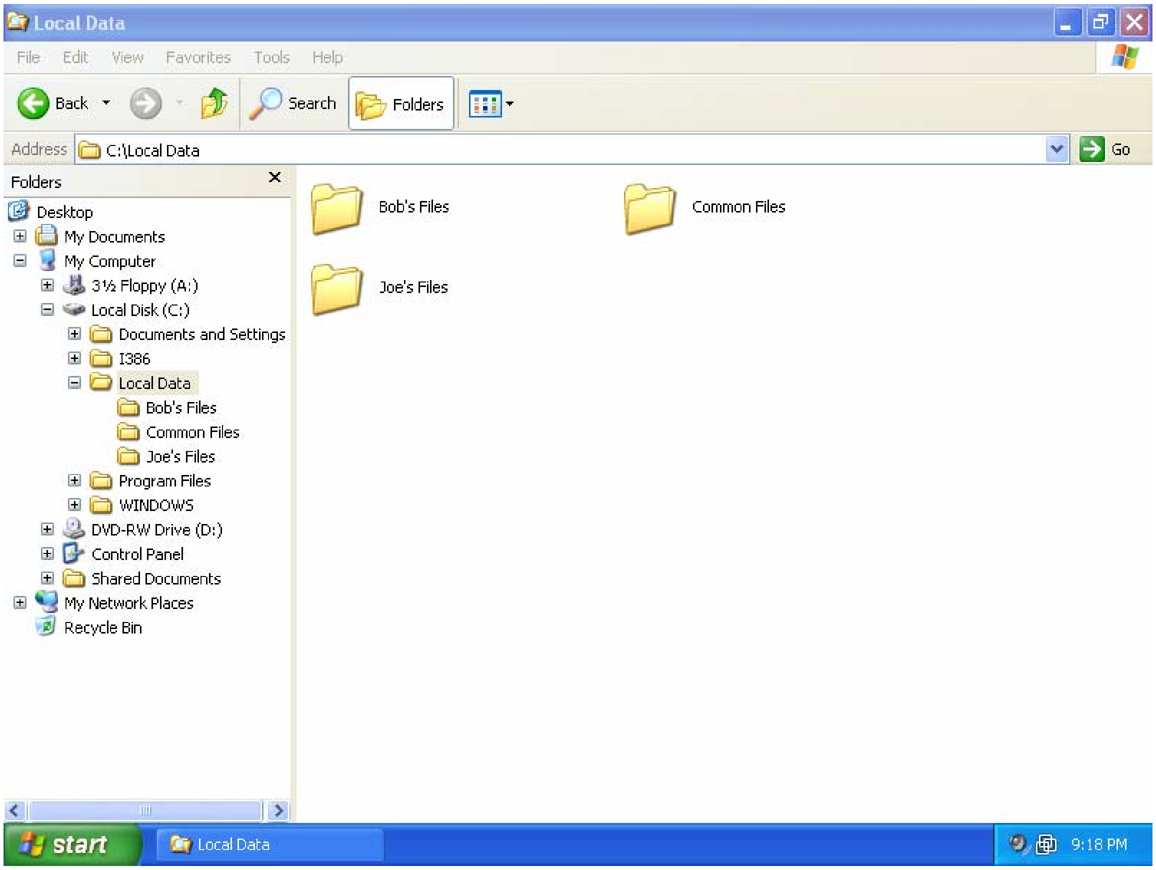
Permissions for Bob	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐
Special Permissions	☐	☐

For special permissions or for advanced settings, click Advanced. Advanced

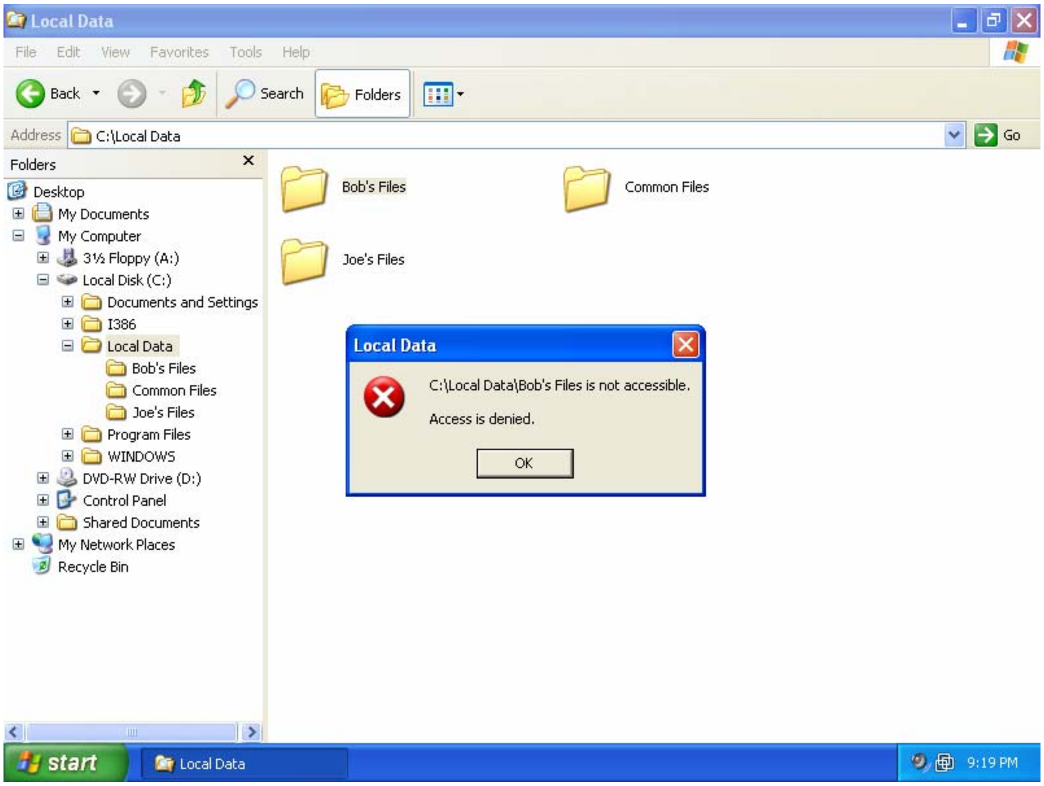
OK Cancel Apply

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**.



Local Data

C:\Local Data\Bob's Files is not accessible.

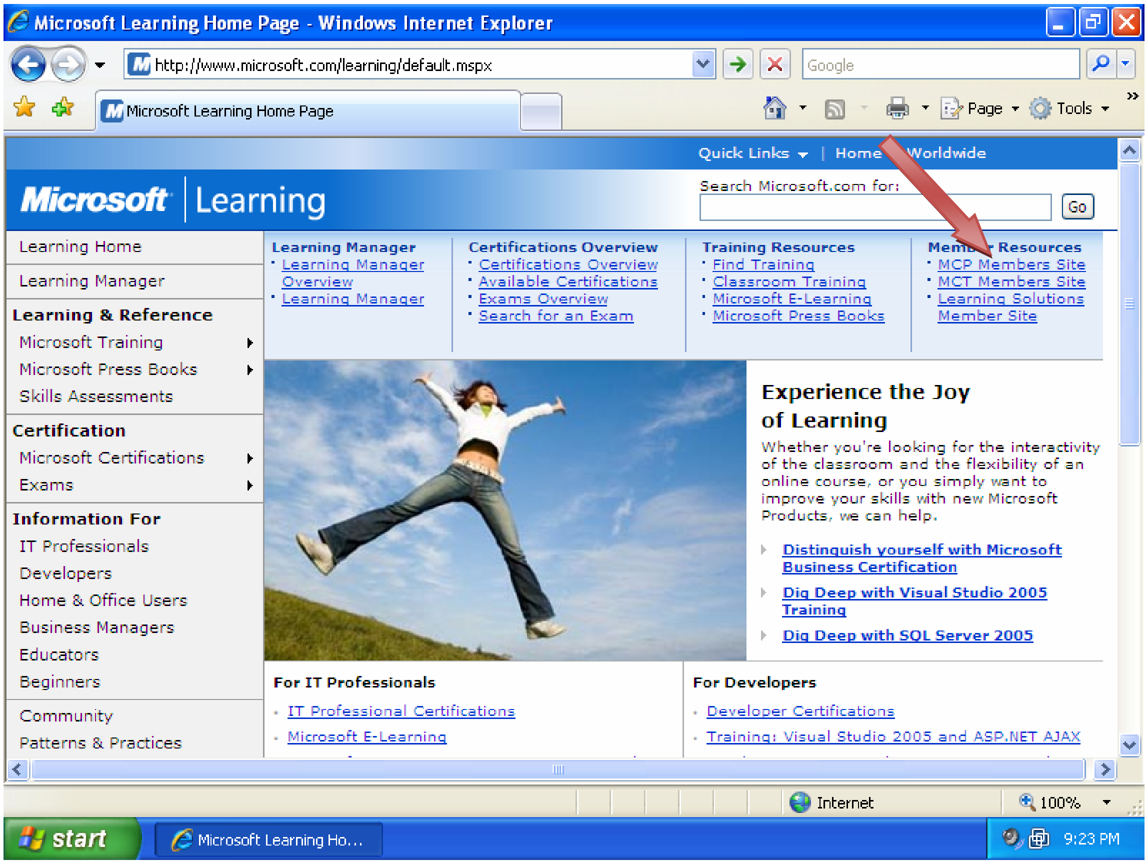
Access is denied.

OK

Part 2 – Identifying a secure communication channel when transmitting data over the Internet

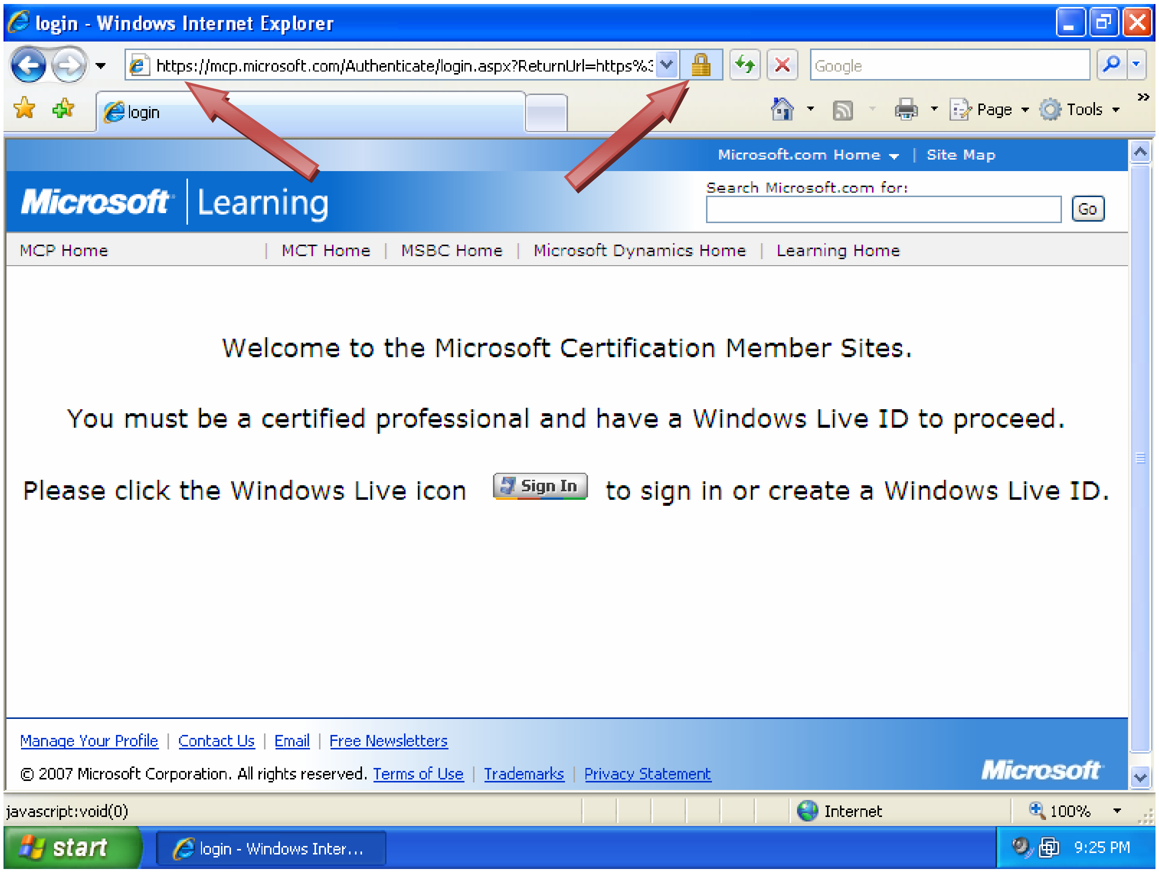
Step 1: Identify a secure web page

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.



Whether you're looking for the interactivity of the classroom and the flexibility of an online course, or you simply want to improve your skills with new Microsoft Products, we can help.

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.



https://mcp.microsoft.com/Authenticate/login.aspx?ReturnUrl=https%3

Welcome to the Microsoft Certification Member Sites.

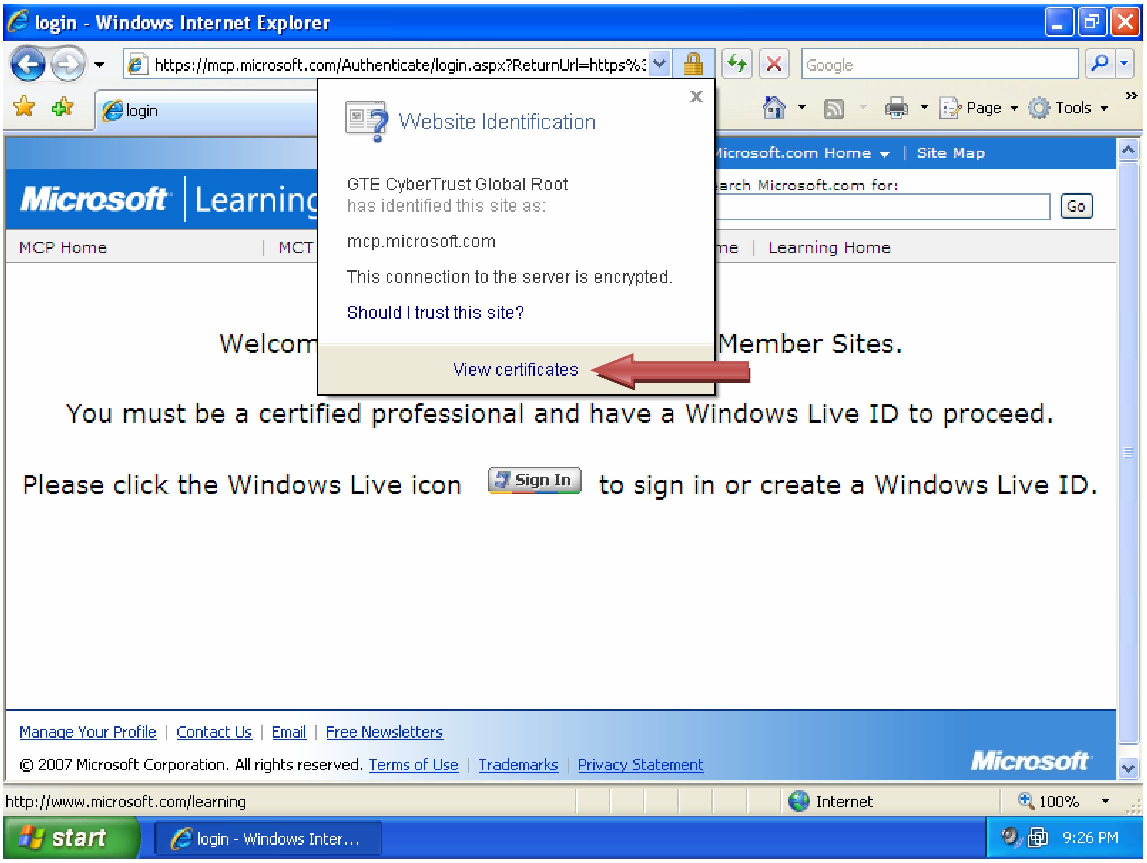
You must be a certified professional and have a Windows Live ID to proceed.

Please click the Windows Live icon Sign In to sign in or create a Windows Live ID.

© 2007 Microsoft Corporation. All rights reserved.

javascript:void(0)

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.



Website Identification

GTE CyberTrust Global Root
has identified this site as:

mcp.microsoft.com

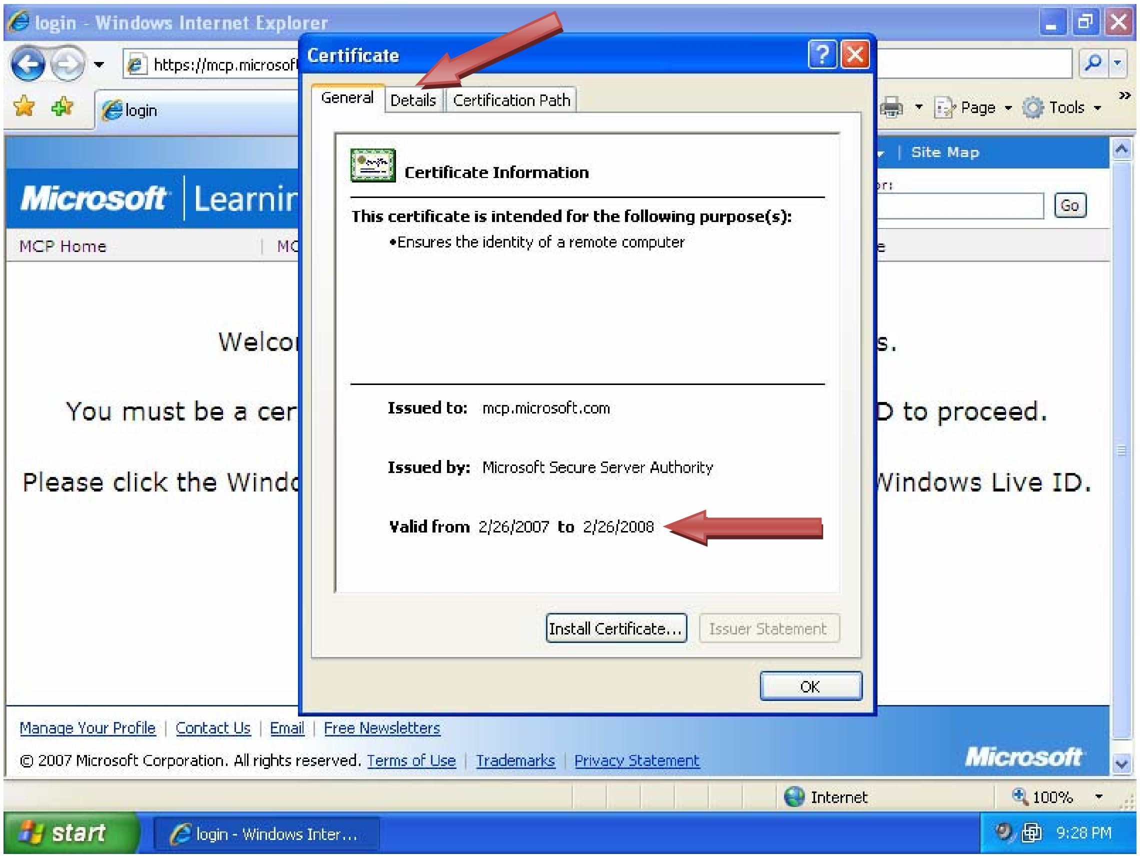
This connection to the server is encrypted.

Should I trust this site?

View certificates

login - Windows Internet Explorer
https://mcp.microsoft.com/Authenticate/login.aspx?ReturnUrl=https%3
Google
login
Page
Tools
Microsoft.com Home
Site Map
Search Microsoft.com for:
Go
Microsoft Learning
MCP Home
MCT
Learning Home
Welcome ... Member Sites.
You must be a certified professional and have a Windows Live ID to proceed.
Please click the Windows Live icon Sign In to sign in or create a Windows Live ID.
Manage Your Profile | Contact Us | Email | Free Newsletters
© 2007 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
http://www.microsoft.com/learning
Internet
100%
start
login - Windows Inter...
9:26 PM

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.



Certificate Information

This certificate is intended for the following purpose(s):

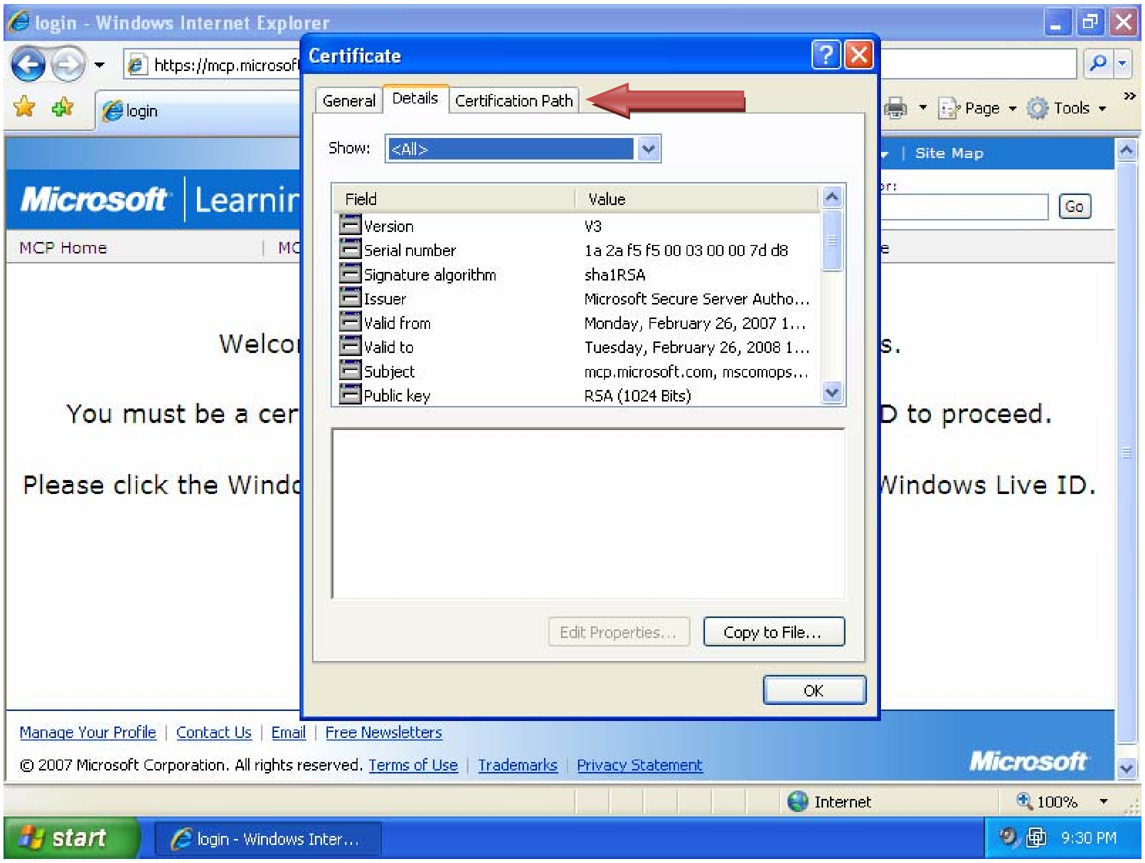
- Ensures the identity of a remote computer

Issued to: mcp.microsoft.com

Issued by: Microsoft Secure Server Authority

Valid from 2/26/2007 **to** 2/26/2008

e. The **Details** tab shows information about the certificate. Click the **Certification Path** tab.



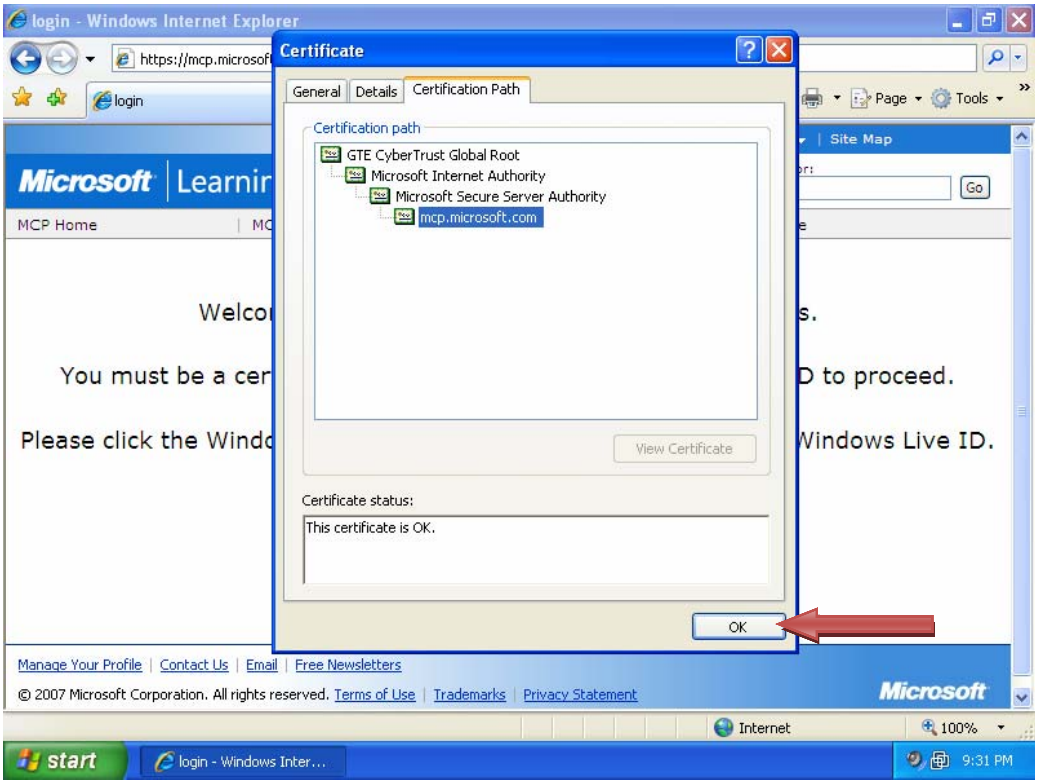
Welco... s.

You must be a cer... D to proceed.

Please click the Windo... Windows Live ID.

Field	Value
Version	V3
Serial number	1a 2a f5 f5 00 03 00 00 7d d8
Signature algorithm	sha1RSA
Issuer	Microsoft Secure Server Autho...
Valid from	Monday, February 26, 2007 1...
Valid to	Tuesday, February 26, 2008 1...
Subject	mcp.microsoft.com, mscomops...
Public key	RSA (1024 Bits)

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.



Certification path

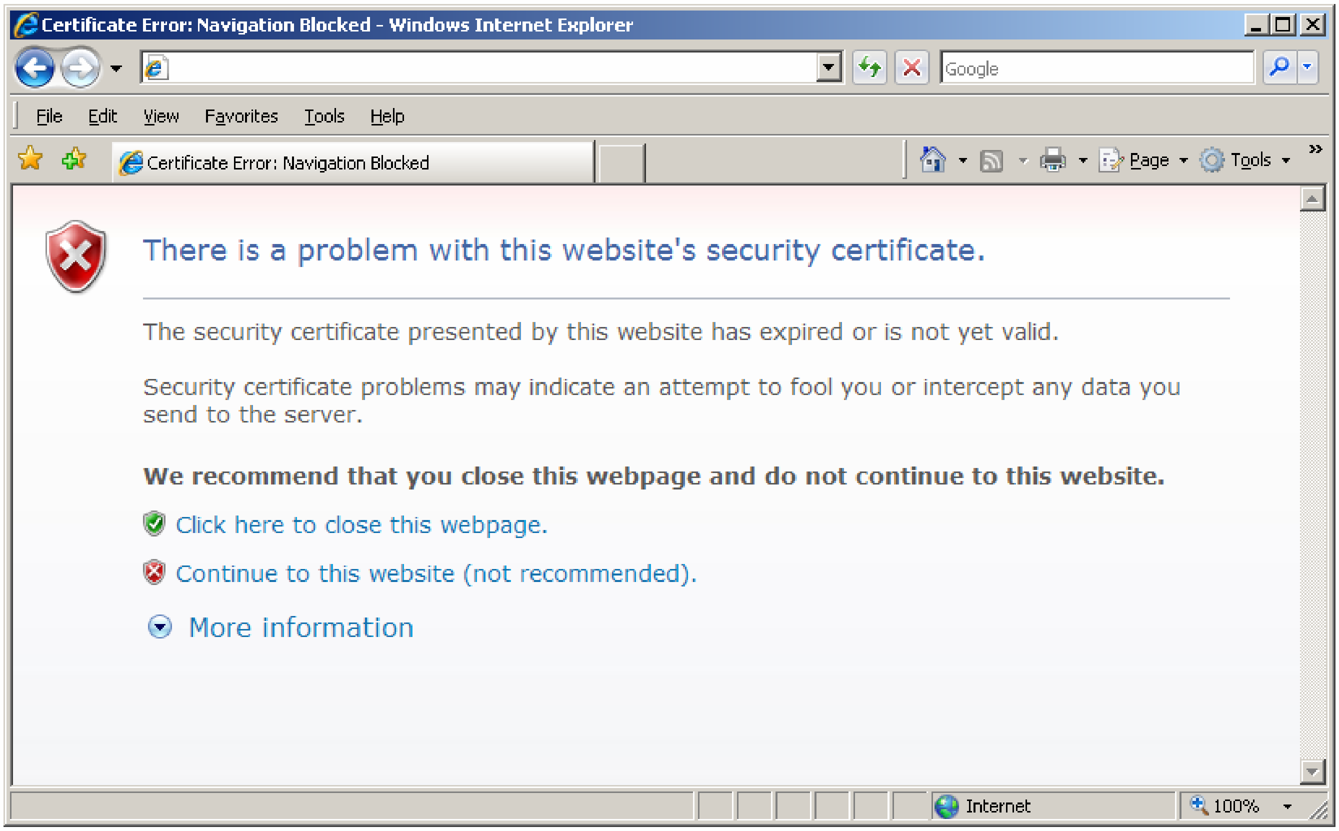
- GTE CyberTrust Global Root
  - Microsoft Internet Authority
    - Microsoft Secure Server Authority
      - mcp.microsoft.com

Certificate status:

This certificate is OK.

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.


Certificate Error: Navigation Blocked - Windows Internet Explorer
Google
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
Page
Tools
Internet
100%

There is a problem with this website's security certificate.

The security certificate presented by this website has expired or is not yet valid.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

More information

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.

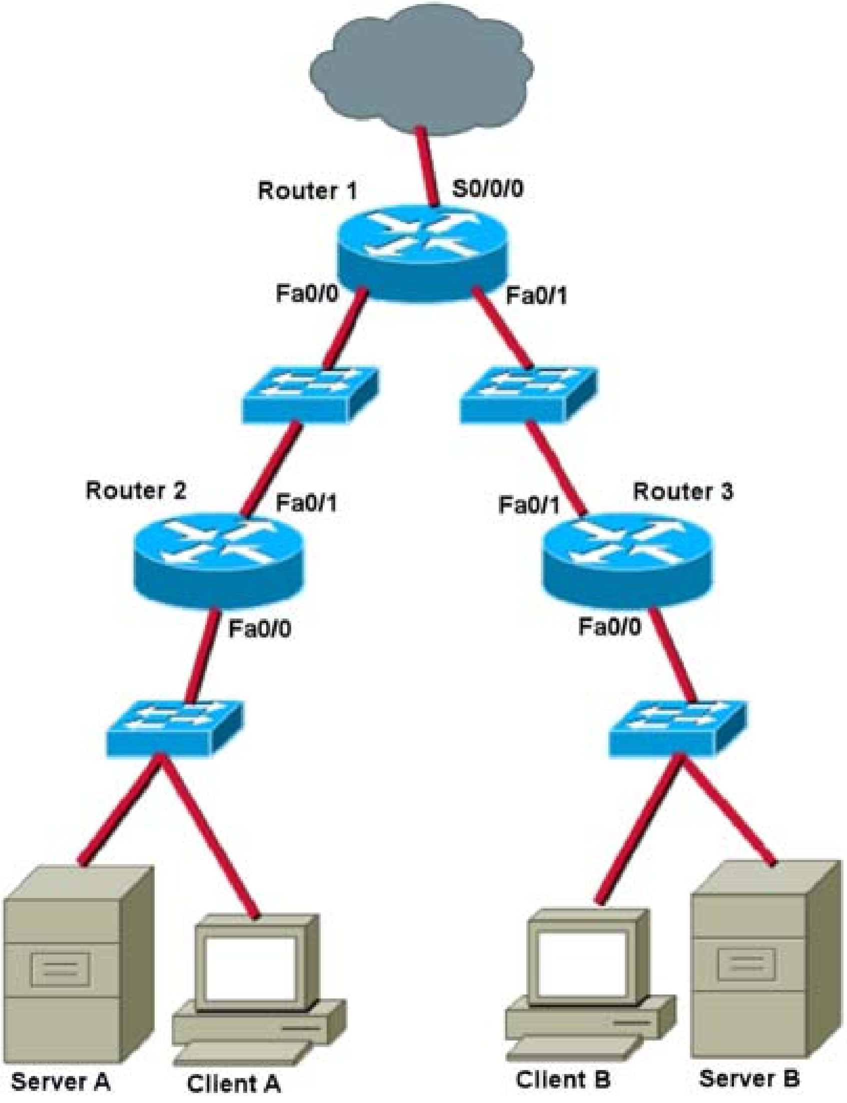
Lab 8.2.1 Planning for Access Lists and Port Filters

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 B 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

- ### 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.

- ### 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.

- ### 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.

- ### 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

Name

Title

Signature ([Client]) Date

Name

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

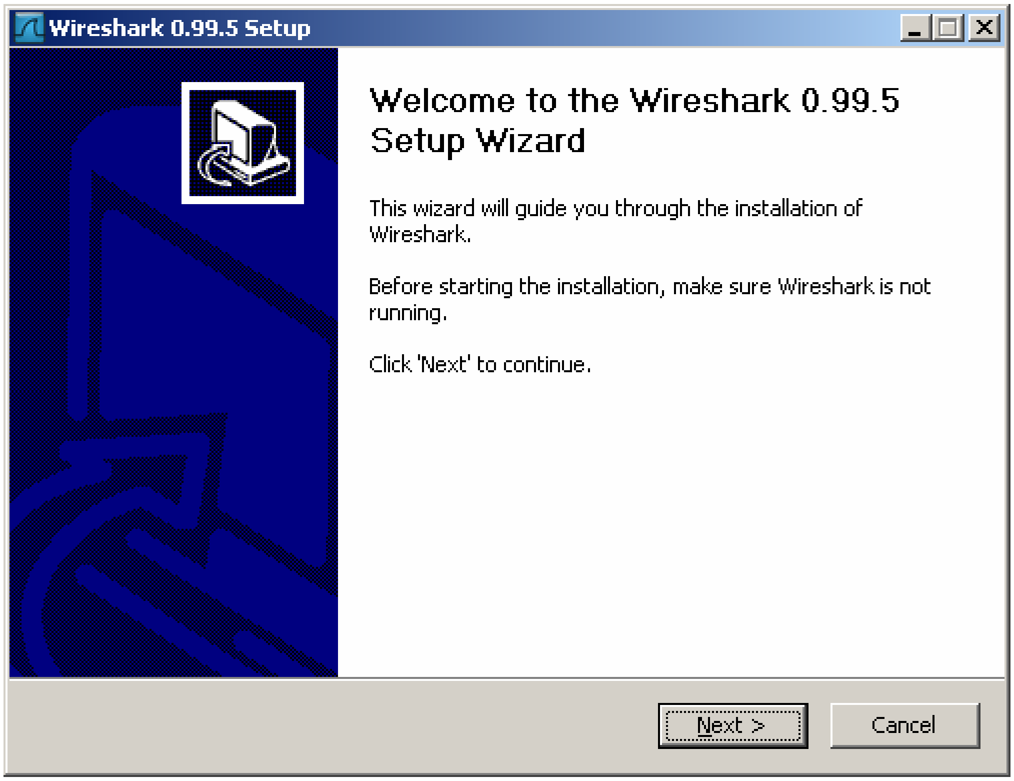
Step 1: Install and launch Wireshark

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.



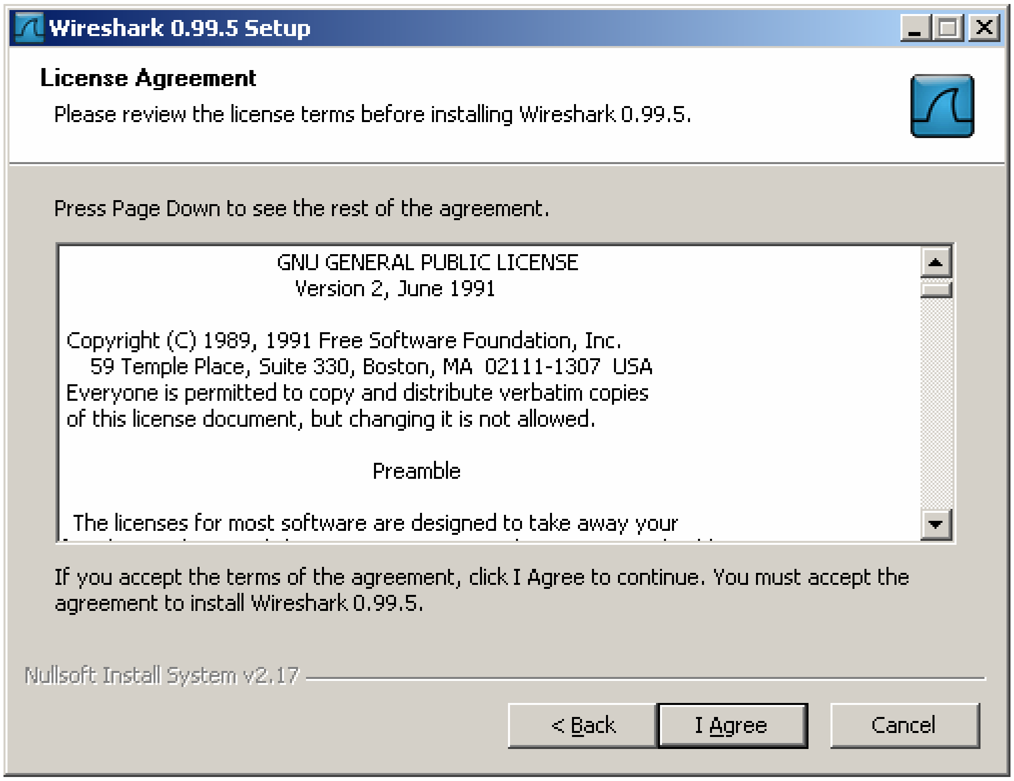
Welcome to the Wireshark 0.99.5 Setup Wizard

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

1) Click **I Agree**.



Wireshark 0.99.5 Setup

License Agreement

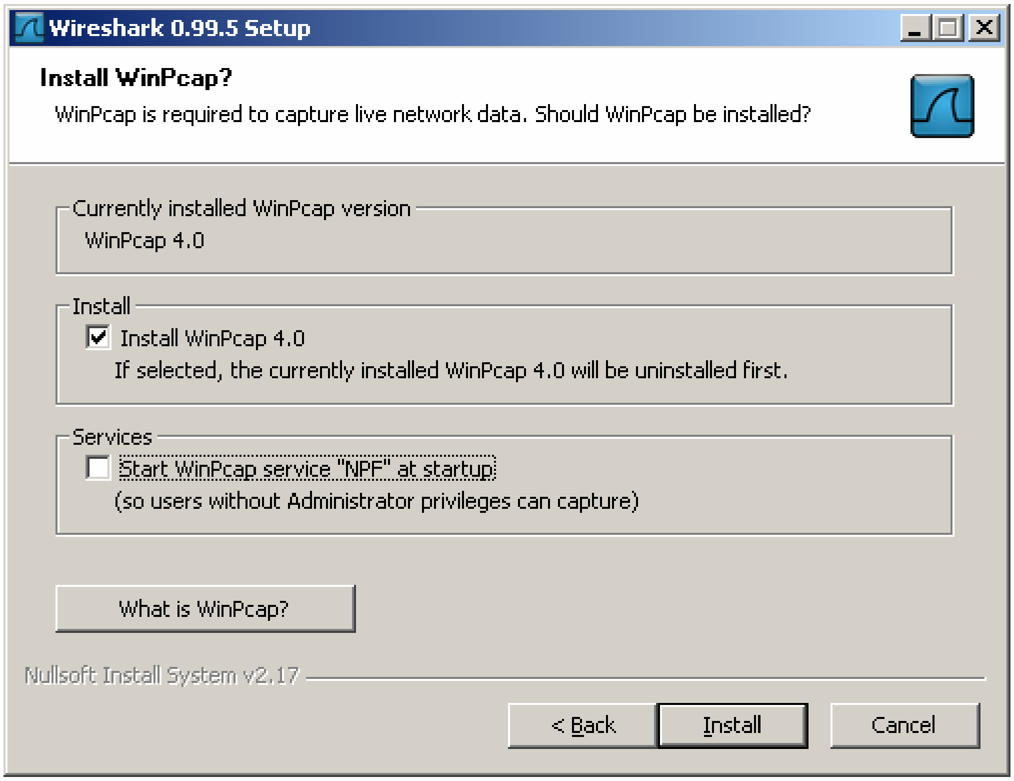
Please review the license terms before installing Wireshark 0.99.5.

Press Page Down to see the rest of the agreement.

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
   59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

                            Preamble

 The licenses for most software are designed to take away your
```

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Wireshark 0.99.5.

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.



Wireshark 0.99.5 Setup

Install WinPcap?

WinPcap is required to capture live network data. Should WinPcap be installed?

Currently installed WinPcap version
WinPcap 4.0

Install
☑ Install WinPcap 4.0
If selected, the currently installed WinPcap 4.0 will be uninstalled first.

Services
☐ Start WinPcap service "NPF" at startup
(so users without Administrator privileges can capture)

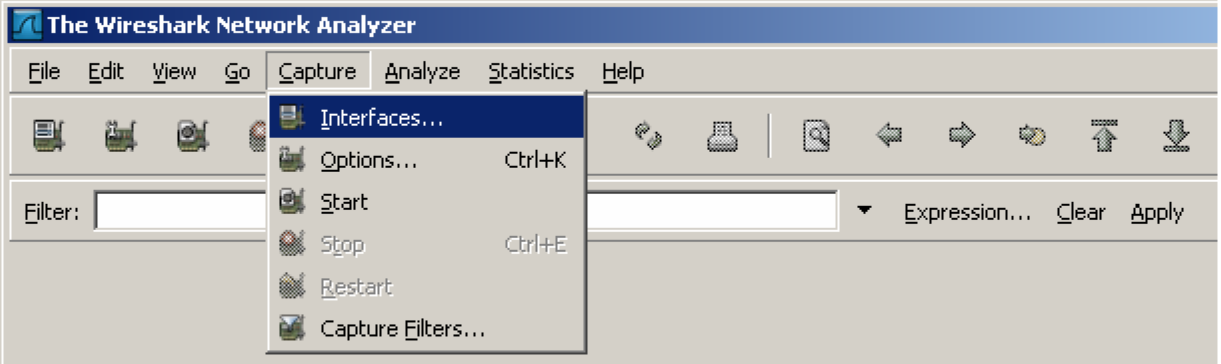
c. Click **Install** and follow the remaining prompts to the end of the installation process.

d. After the software is installed, click the checkbox to launch Wireshark.

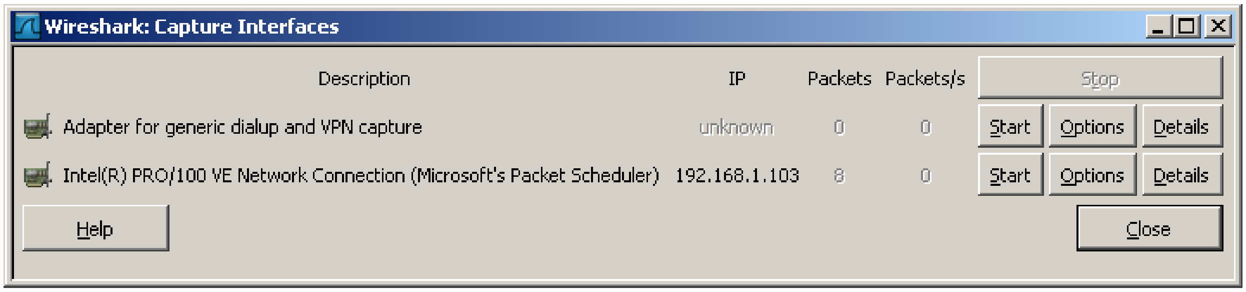
Step 2: Select an interface to use for capturing packets

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.

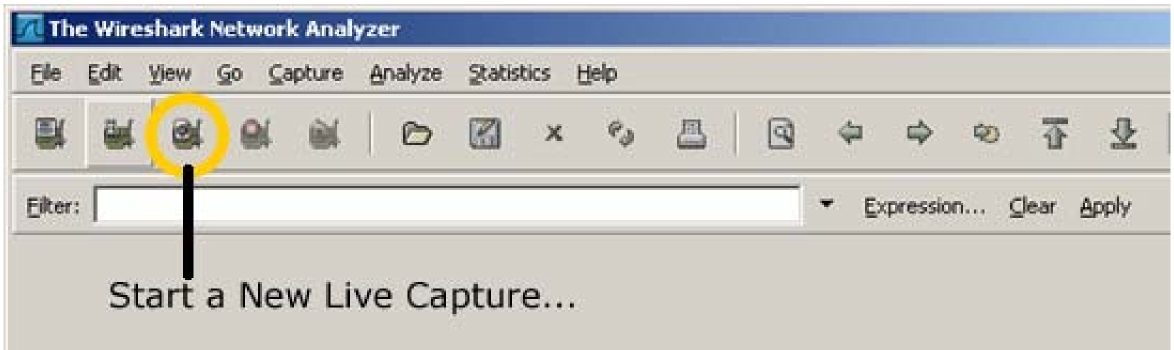

Wireshark: Capture Interfaces

Description	IP	Packets	Packets/s	Stop		
Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler)	192.168.1.103	8	0	Start	Options	Details

Step 3: Start a network capture

a. Scroll through the menus and view the toolbar on the Wireshark startup Interface.

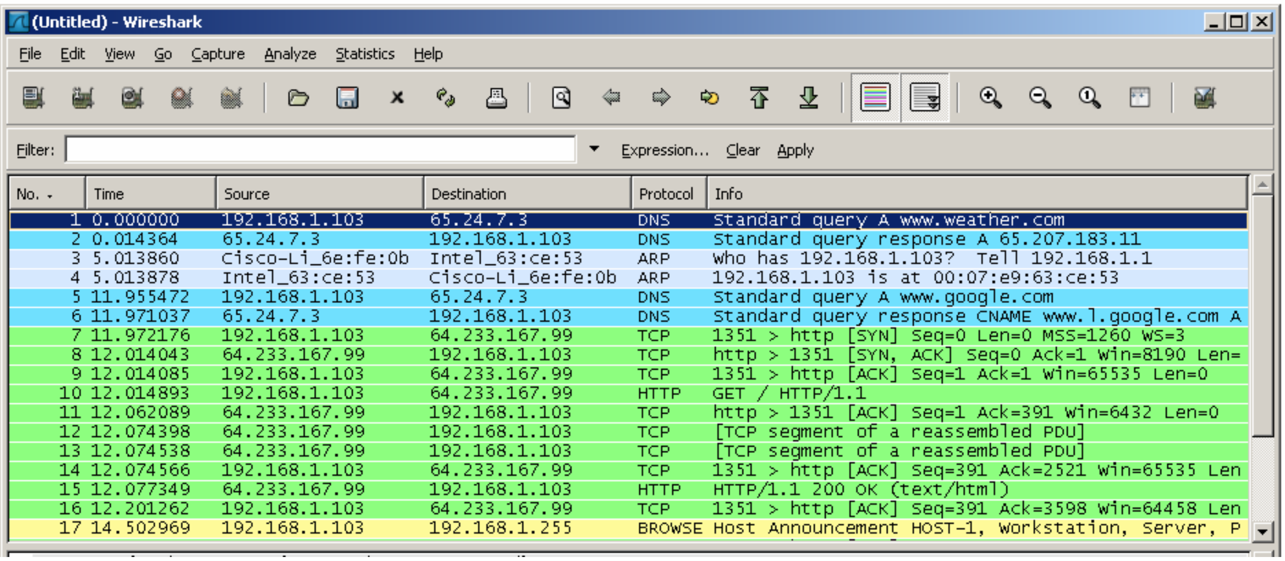
b. Click the **New Live Capture** button and observe the information gathered by Wireshark. Allow the capture to continue for a few minutes so that you can observe the different types of traffic on the network.



Start a New Live Capture...

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.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.103	65.24.7.3	DNS	Standard query A www.weather.com
2	0.014364	65.24.7.3	192.168.1.103	DNS	Standard query response A 65.207.183.11
3	5.013860	Cisco-Li_6e:fe:0b	Intel_63:ce:53	ARP	Who has 192.168.1.103? Tell 192.168.1.1
4	5.013878	Intel_63:ce:53	Cisco-Li_6e:fe:0b	ARP	192.168.1.103 is at 00:07:e9:63:ce:53
5	11.955472	192.168.1.103	65.24.7.3	DNS	Standard query A www.google.com
6	11.971037	65.24.7.3	192.168.1.103	DNS	Standard query response CNAME www.l.google.com A
7	11.972176	192.168.1.103	64.233.167.99	TCP	1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
8	12.014043	64.233.167.99	192.168.1.103	TCP	http > 1351 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=
9	12.014085	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10	12.014893	192.168.1.103	64.233.167.99	HTTP	GET / HTTP/1.1
11	12.062089	64.233.167.99	192.168.1.103	TCP	http > 1351 [ACK] Seq=1 Ack=391 Win=6432 Len=0
12	12.074398	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
13	12.074538	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
14	12.074566	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=2521 Win=65535 Len
15	12.077349	64.233.167.99	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
16	12.201262	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=3598 Win=64458 Len
17	14.502969	192.168.1.103	192.168.1.255	BROWSE	Host Announcement HOST-1, Workstation, Server, P

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?

____

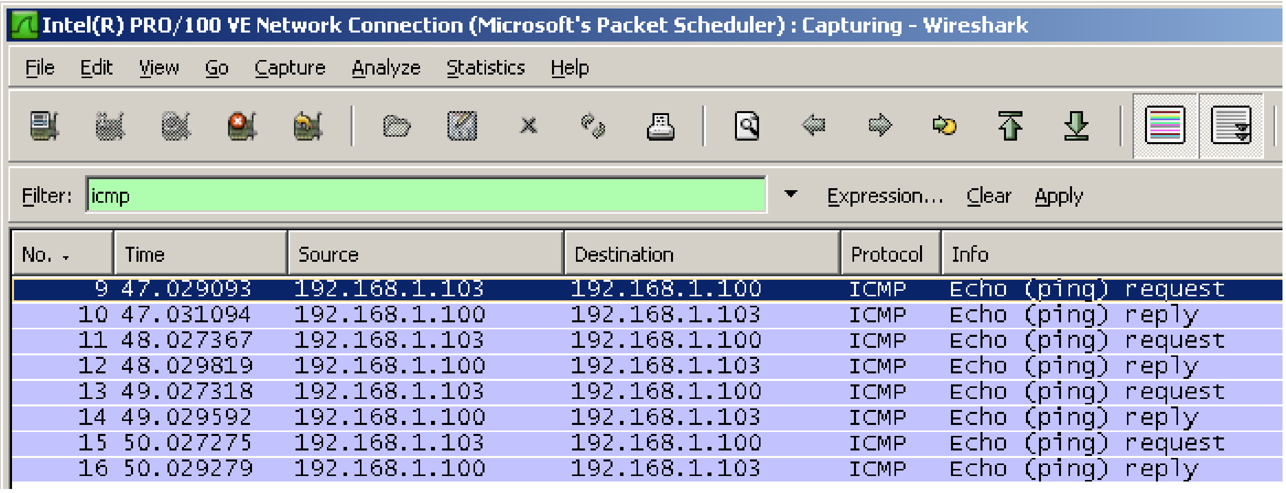
Step 5: Filter a network capture

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.


Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Help
Expression...
Clear
Apply

Filter: icmp

No.	Time	Source	Destination	Protocol	Info
9	47.029093	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
10	47.031094	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply
11	48.027367	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
12	48.029819	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply
13	49.027318	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
14	49.029592	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply
15	50.027275	192.168.1.103	192.168.1.100	ICMP	Echo (ping) request
16	50.029279	192.168.1.100	192.168.1.103	ICMP	Echo (ping) reply

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?

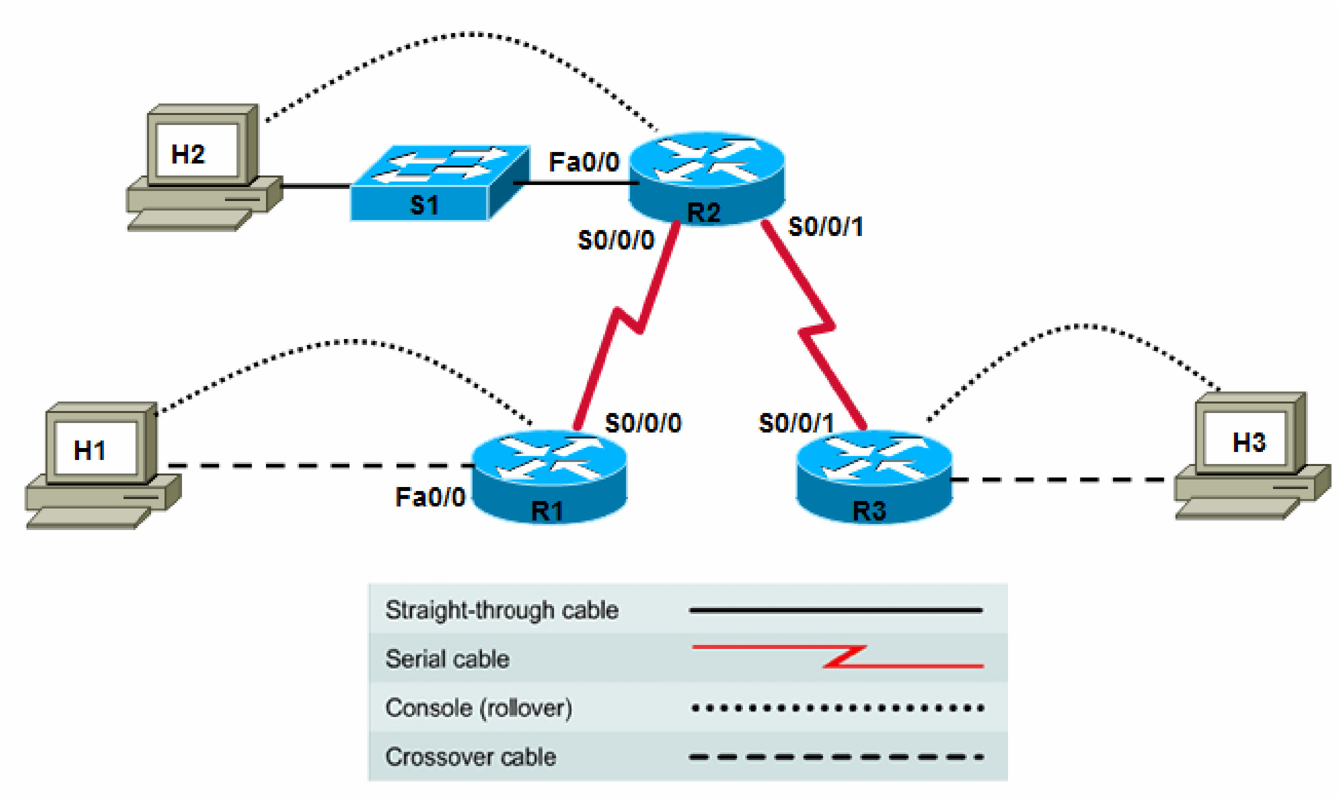
____

b. Is Wireshark a tool for out-of-band or in-band network monitoring? ____________ Explain your answer.

____

____

Lab 8.3.3a Managing Remote Network Devices with Telnet



Device	Host Name	Interface	IP Address	Subnet Mask	RIP v2 Network Statements
R1	R1	Serial 0/0/0 (DTE)	10.10.10.1	255.255.255.0	10.0.0.0
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0	192.168.1.0
R2	R2	Serial 0/0/0 (DCE)	10.10.10.2	255.255.255.0	10.0.0.0
		Serial 0/0/1 (DCE)	172.16.1.1	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.2.1	255.255.255.0	192.168.2.0
R3	R3	Serial 0/0/1 (DTE)	172.16.1.2	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.3.1	255.255.255.0	192.168.3.0
S1	S1	VLAN 1 (mgmt)	192.168.2.99	255.255.255.0	N/A

Objectives

- Establish a Telnet connection to a remote router.

- Verify that the Application Layer between the source and destination is working properly.
- Retrieve information about remote routers using **show** commands.
- Retrieve CDP information from routers not directly connected.
- Suspend and reestablish a Telnet session.
- Disconnect from a Telnet session.
- Engage in multiple Telnet sessions.
- Display active Telnet sessions.

Background / Preparation

This lab focuses on the Telnet (remote terminal) utility to access routers remotely. Telnet is used to connect from a local router to another remote router to simulate being at the console on the remote router. The local router acts as a Telnet client, and the remote router acts as a Telnet server. You can also Telnet from a workstation as a client into any router with IP connectivity on the network. If an Ethernet switch has an IP address assigned, you can Telnet into it from a workstation or any networking device that has IP connectivity. Telnet is a good testing and troubleshooting tool because it is an Application Layer utility. A successful Telnet demonstrates that the entire TCP/IP protocol stack on both the client and server are functioning properly.

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 identify the interface identifiers to be used based on the equipment in the lab. Depending on the model of router, the output may vary from the output shown in this lab.

Required Resources

The following resources are required:

- One router with two serial interfaces and one Fast Ethernet (1841 or other)
- Two routers with one serial interface and one Fast Ethernet (1841 or other)
- One 2960 switch (or comparable) for the R2 LAN
- Three windows XP computers (hosts H2 and H3 are mainly for configuring routers R2 and R3)
- Straight-through and crossover Category 5 Ethernet cables as required
- Two null serial cables
- Console cable to configure routers
- Access to host H1 command prompt
- Access to host H1 network TCP/IP configuration

On hosts H1, H2, and H3, start a HyperTerminal session to each router.

Note: Make sure that the routers and switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Verify Connectivity

Step 1: Configure basic information on each router and the switch.

a. Build and configure the network according to the topology diagram and device configuration table. If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions.

b. Configure RIPv2 on each router and advertise the networks shown in the device configuration table. If necessary, see Lab 6.1.5, “Configuring and Verifying RIP,” for instructions.

c. Configure basic settings on switch S1 to include host name, passwords, and VLAN 1 IP address. If necessary, see Lab 5.5.4, “Configuring the Cisco 2960 Switch,” for instructions.

Step 2: Configure each host.

Configure H1, H2, and H3 with an IP address, subnet mask, and default gateway that are compatible with the IP address of the router default gateway interface address for the LAN to which they are attached.

Step 3: Verify end-to-end connectivity.

a. Open a command prompt on host H1 and ping from the R1 LAN to host H3 on the R3 LAN.

```
C:\>ping 192.168.3.2
```

b. If host H3 is not attached to router R3, ping the R3 serial 0/0/0 interface IP address 172.16.1.2.

```
C:\>ping 172.16.1.2
```

Note: If the pings are not successful, troubleshoot the router and host configurations and connections.

Task 2: Establish a Telnet Session from a Host Computer

Step 1: Telnet from host H1 to remote router R2.

The Cisco IOS software has built-in Telnet client and server software. Nearly all computer operating systems have a Telnet client. Many server operating systems also have a Telnet server, although Microsoft Windows desktop operating systems typically do not.

In many cases, you will not have direct access to a router through the console so that you can access other networking devices. Usually, you Telnet to a router or switch from a host computer. Once you have gained access to the router or switch command prompt, you can Telnet to other networking devices that are accessible via the network.

a. From the command prompt on H1, telnet to the R2 router Fast Ethernet 0/0 interface.

```
C:\>telnet 192.168.2.1
```

b. Enter the password **cisco** to access the router.

c. What prompt did the router display? _____

Step 2: End the Telnet session from host H1 to remote router R2.

Exit the Telnet session from host H1 to R1 by typing **exit**.

Task 3: Perform Basic Telnet Operations Between the Routers

Step 1: Use the help feature to get telnet information.

a. From the router R1 HyperTerminal session, enter **telnet ?** at either the user EXEC or the privileged EXEC router prompt.

What is displayed? ____

b. What happens if you just type **telnet** and press **Enter**?

____

Step 2: Telnet from R1 to remote router R2.

Note: Telnet uses the vty lines on the remote router to connect. If the vty lines are not configured for login or there is no password set, you cannot connect to the remote router using Telnet.

a. Telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
```

```
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _____

Step 3: Look at the interfaces on remote router R2.

a. Issue the **show ip interface brief** command at the remote router prompt.

```
R2>show ip interface brief
```

b. List the interfaces that are up on remote router R2. ____________________________________

c. Another command that provides interface status information is **show protocols.** This command lists all interfaces for the Internet protocol. What information does this command provide that the **show ip interface brief** command does not? ____

```
R2>show protocols
```

Step 4: Display the routing table on the remote router.

Issue the **show ip route** command at the router prompt. Which routes has router R2 learned from RIP?

```
R2>show ip route
```

____

Step 5: Display the CDP neighbors for R2.

a. Use the Cisco Discovery Protocol (CDP) to view information about Cisco devices directly attached to R2. Enter show cdp neighbors command at the router prompt.

b. List all device IDs that are connected to the remote router. What is the platform for each device?

```
R2>show cdp neighbors
```

____

Step 6: Enter privileged EXEC mode.

Note: The previous commands could be issued at the user EXEC mode prompt R2>. To display the running configuration for a router, you must be in privileged EXEC mode.

a. Enter enable at the R2> command prompt, and use the password class.

b. What prompt did the router display? _______

c. What mode is this? ___________________________

Step 7: View the running configuration on remote router R2.

a. Enter **show running-config** at the remote router R2 prompt.

```
R2>show running-config
```

b. Where is this file located? ____

Step 8: Activate console message monitoring on remote router R2.

a. During the Telnet session with R2, turn on RIP debugging using the **debug ip rip** command in privileged EXEC mode. This allows you to see the periodic routing updates sent between RIP routers. Do you see any RIP messages? _________

```
R2#debug ip rip
RIP protocol debugging is on
```

b. To see console messages from R2 while connected from R1 via Telnet, issue the **terminal monitor** command from the R2 privileged prompt. Without this command, you cannot view R2 console messages and debug output remotely from R1. Do you see any RIP messages now? _________

```
R2#terminal monitor
```

c. Turn off the RIP debugging on R2 using either the **no debug ip rip** or **undebug all** command, and deactivate terminal monitoring on R2 using the **terminal no monitor** command.

```
R2#no debug ip rip
RIP protocol debugging is off

R2#terminal no monitor
```

Step 9: Suspend the current Telnet session on R2.

a. Press **Ctrl-Shift-6**, and then press the **x** key. This action only suspends the session and returns to the previous router. It does not disconnect from this router.

b. What prompt did the router display? _____

Step 10: Resume the Telnet session to R2.

a. Press the **Enter** key at the router prompt. What does the router respond with?

____

b. Pressing **Enter** resumes the Telnet session that was previously suspended in Step 9. What prompt did the router display? _____

Step 11: Close the Telnet session to R2.

a. Terminate the Telnet session by typing **exit**.

b. What does the router respond with? ____

c. What prompt did the router display? _______

Note: When the Telnet session is suspended, you can disconnect from that session using the **disconnect** command and the session number.

Task 4: Perform Telnet Operations Between Multiple Routers

Step 1: Telnet from R1 to remote router R2.

a. From R1, telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

b. Use the password **cisco** to enter the router.

Step 2: Suspend the current Telnet session to R2.

a. Press **Ctrl-Shift-6,** and then press the **x** key.

b. What prompt did the router display? _______

Step 3: Establish an additional Telnet session from R1 to R3.

a. From R2, telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

b. Use the password **cisco** to access the router.

c. What prompt did the router display? _____

Step 4: Suspend the Telnet session to R3.

a. Press **Ctrl-Shift-6**, and then press the **x** key.

b. What prompt did the router display? _____

Step 5: View the active Telnet sessions.

Enter the **show sessions** command at the R1 command prompt. How many sessions are in use? _____

Note: The default session is indicated by the asterisk (*). This is the session that resumes when you press **Enter**.

```
R1>show sessions
```

Step 6: Resume the previously suspended Telnet session.

Type **resume** and the number of the session that is to be resumed (1) and press **ENTER** at the router prompt. What did the router respond with? __________________________________

Step 7: View the active Telnet sessions.

a. Enter the **show sessions** command at the command prompt.

b. How many sessions are shown? _______________________

c. There were two the last time. What happened?

____

Step 8: Suspend the Telnet session to R3.

a. Press **Ctrl-Shift-6,** and then press the **x** key.

b. What prompt did the router display? _______

Step 9: Disconnect the sessions from R1 to R2 and R3.

Enter the **disconnect 1** command at the R1 prompt and press **Enter**. This disconnects session 1 to R2 and leaves one session to R3 still open. Type the command again to disconnect the Telnet session to R3.

```
R1>disconnect 1
Closing connection to 10.10.10.2 [confirm]
R1>disconnect 1
Closing connection to 172.16.1.2 [confirm]
```

Task 5: Experiment with Multiple Linked Sessions

When working with Telnet, one of the most common problems is remembering the device that you are focusing of the session. Many times people telnet to a router, and then telnet from that router to another and so on. Without host names, or if the routers have similar host names, confusion can result.

Step 1: Telnet to the R3 router.

a. From R1, telnet to the R3 router.

b. From the configuration prompt, type **no hostname**.

Step 2: Telnet to the R2 router.

a. From R3, telnet to the R2 router.

b. From the configuration prompt, type **no hostname**.

Step 3: Telnet back to the R3 router.

a. From R2, telnet back to the R3 router.

b. By looking at the prompt, is it evident whether the telnet worked or not? _____

Step 4: Telnet to the R1 router.

a. From R3, Telnet to the R1 router.

b. From the configuration prompt, type **no hostname**.

Step 5: Exit from all sessions.

a. Keep typing **exit** until the following prompt appears.

```
Router con0 is now available
Press RETURN to get started.
```

b. Scroll back up the HyperTerminal listing.

c. How many session-closed messages were displayed? _____

Task 6: Reflection

What are some advantages and disadvantages of using Telnet?

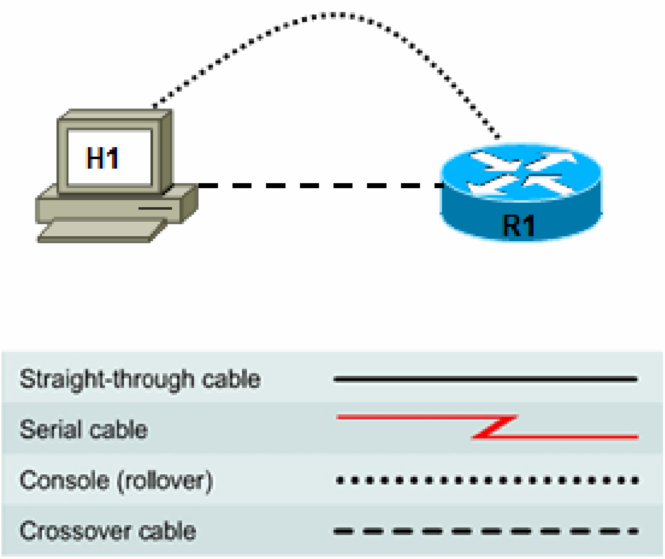
____

____

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 8.3.3b Configuring a Remote Router Using SSH



Objectives

- Use SDM to 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.
- Configure a non-SDM router for SSH using the Cisco IOS CLI.

Background / Preparation

In the past, Telnet was the most common network protocol used to remotely configure network devices. However, protocols such as Telnet do not authenticate or encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

Secure Shell (SSH) is a network protocol that establishes 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 in to 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 enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. 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.

You can use either Cisco SDM or Cisco IOS CLI commands to configure SSH on the router. The Cisco 1841 ISR supports 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. If you are working with a router that does not have SDM installed, use

Cisco IOS CLI commands to configure SSH. Instructions are provided in Step 2 of this lab. To perform the basic router configuration, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS 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 pre-installed. This lab uses a Cisco 1841 router, which has SDM (and SDM Express) pre-installed. You can use another router model that supports SDM. If the router does not have SDM installed, you can download the latest version free of charge at http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm. From this web page, you can also view or download “Downloading and Installing Cisco Router and Security Device Manager.” This document provides instructions and system requirements for installing SDM.

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 the startup-config is erased from an SDM router, SDM no longer comes up by default when the router is restarted. In this case, it is necessary to build a basic router configuration using Cisco IOS commands. See the procedure at the end of this lab or contact the instructor.

Required Resources

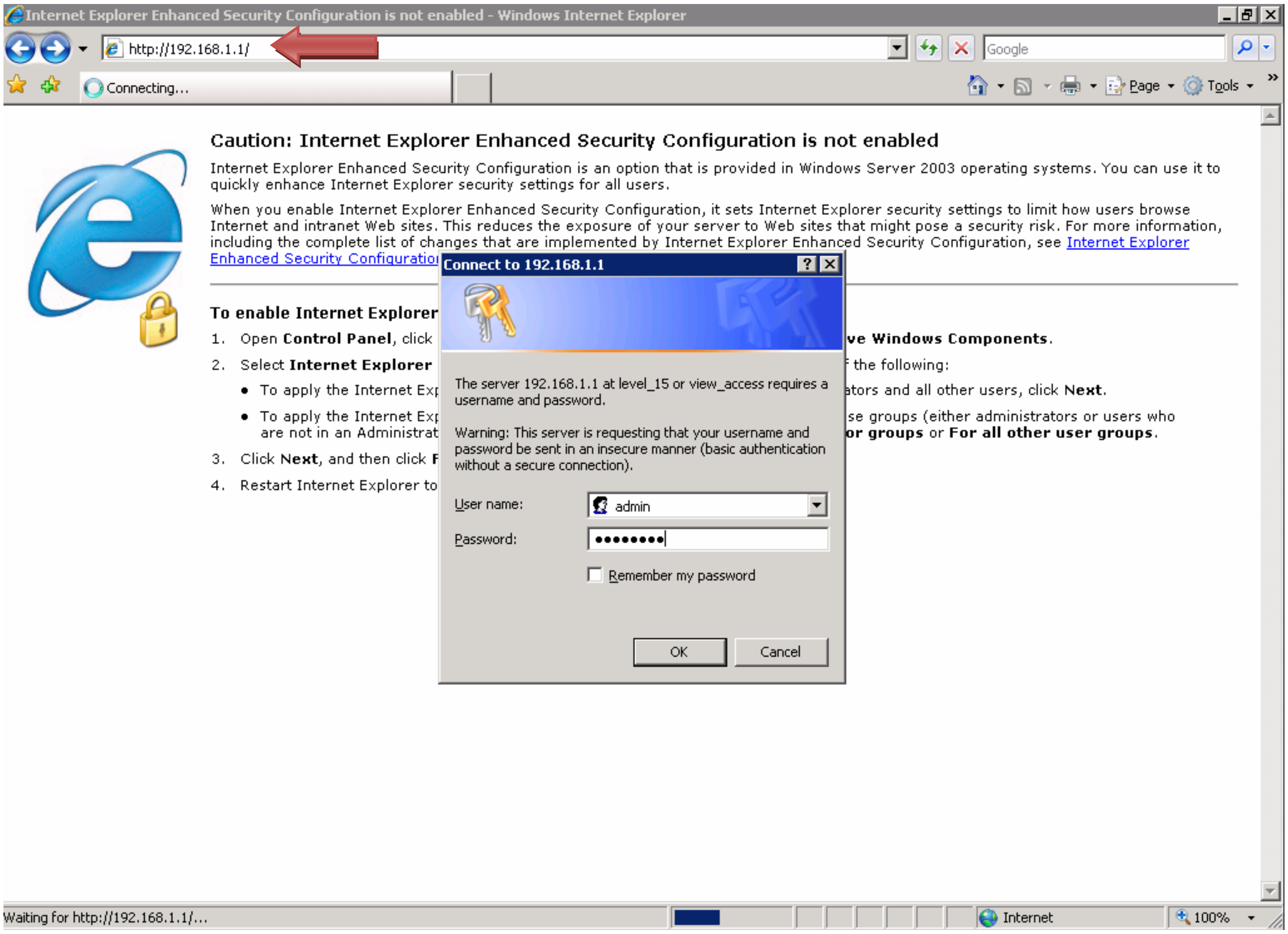
The following resources are required:

- Cisco 1841 ISR router with SDM version 2.4 installed and with basic configuration completed
- (Optional) Other Cisco router model with SDM installed
- (Optional) Other Cisco router model without SDM installed (Cisco IOS software version 12.2 or later; must support SSH)
- Windows XP computer with Internet Explorer 5.5 or later 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: Use SDM to configure the router to accept SSH connections.

Note: If you are configuring a router that does not have SDM installed, just read through Step 1 to see how SSH is set up as a separate task when using SDM, and then go to Step 2.

a. Connect to the router Fa0/0 interface. 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.



Internet Explorer Enhanced Security Configuration is not enabled - Windows Internet Explorer
http://192.168.1.1/
Google
Connecting...
Page
Tools
Connect to 192.168.1.1
OK
Cancel
Waiting for http://192.168.1.1/...
Internet
100%

Caution: Internet Explorer Enhanced Security Configuration is not enabled

Internet Explorer Enhanced Security Configuration is an option that is provided in Windows Server 2003 operating systems. You can use it to quickly enhance Internet Explorer security settings for all users.

When you enable Internet Explorer Enhanced Security Configuration, it sets Internet Explorer security settings to limit how users browse Internet and intranet Web sites. This reduces the exposure of your server to Web sites that might pose a security risk. For more information, including the complete list of changes that are implemented by Internet Explorer Enhanced Security Configuration, see Internet Explorer Enhanced Security Configuratio

The server 192.168.1.1 at level_15 or view_access requires a username and password.

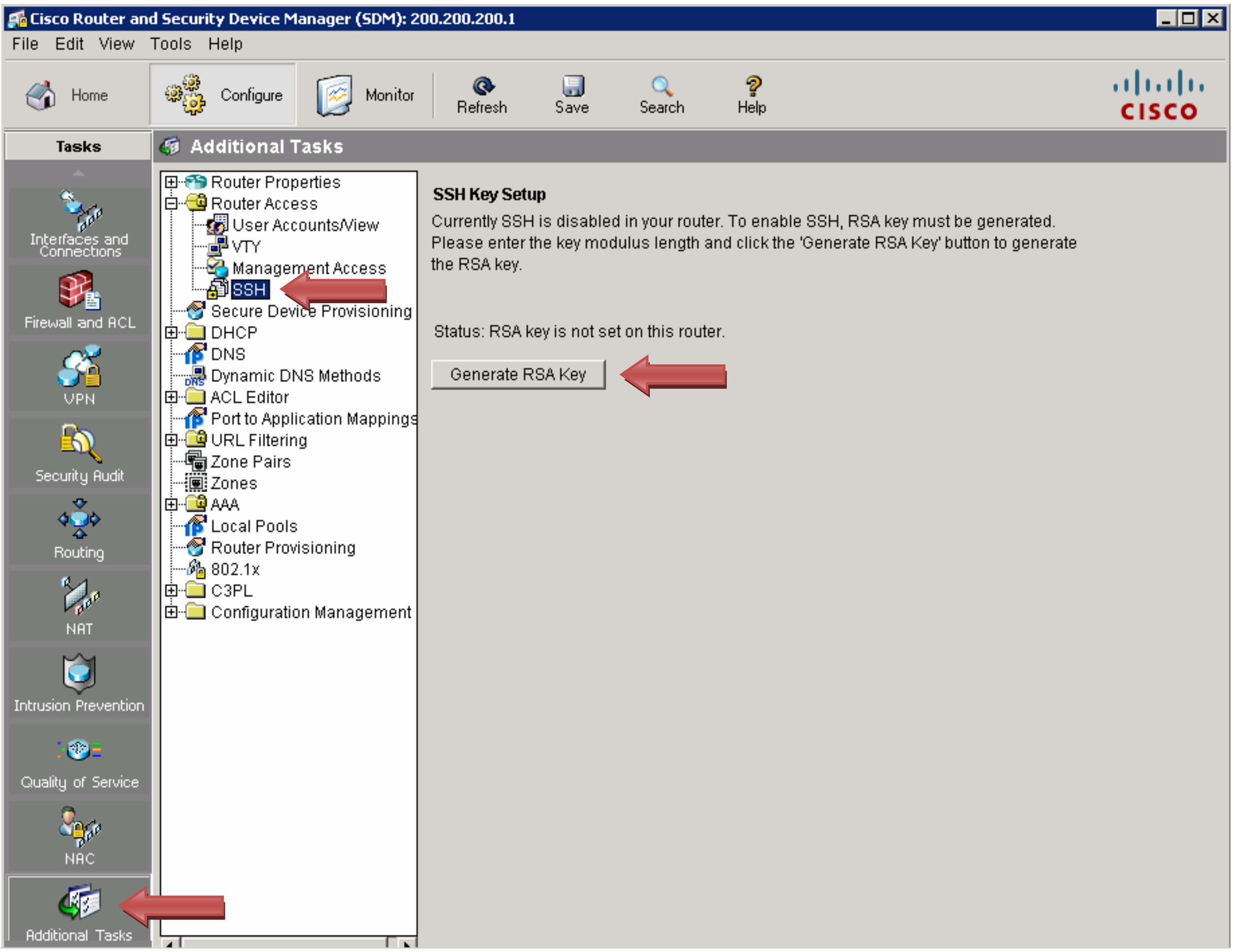
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

User name: admin

Password: ••••••••

□ Remember my password

b. Click the **Configure** button on the tool bar. In the Tasks pane, click **Additional Tasks**. In the Additional Tasks pane, expand **Router Access** and click the **SSH** task. Then click the **Generate RSA Key** button.



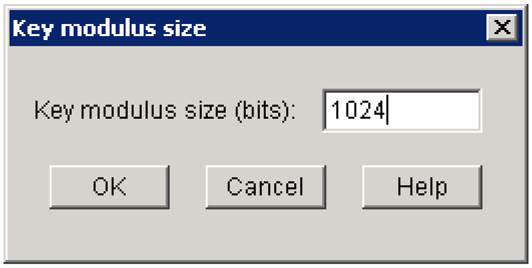
SSH Key Setup

Currently SSH is disabled in your router. To enable SSH, RSA key must be generated. Please enter the key modulus length and click the 'Generate RSA Key' button to generate the RSA key.

Status: RSA key is not set on this router.

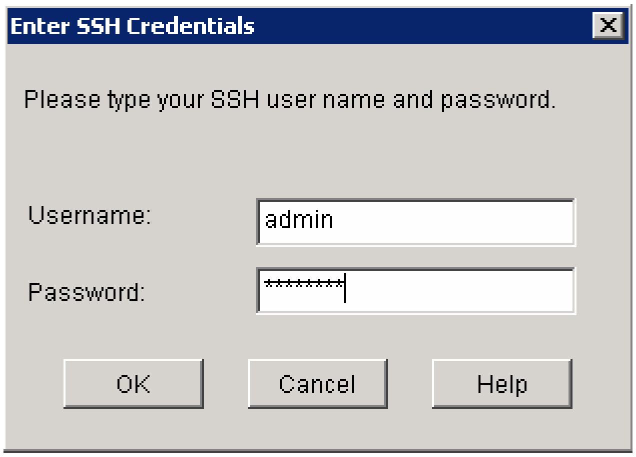
Note: If the **SSH Key Setup** message says: “RSA key exists and SSH is enabled in your router” and the **Status** is “RSA key is set on this router,” you probably completed Lab 5.2.3, “Configuring an ISR with SDM Express.” In that lab, when you configured security, one of the recommended security settings 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**.



Key modulus size (bits): 1024

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

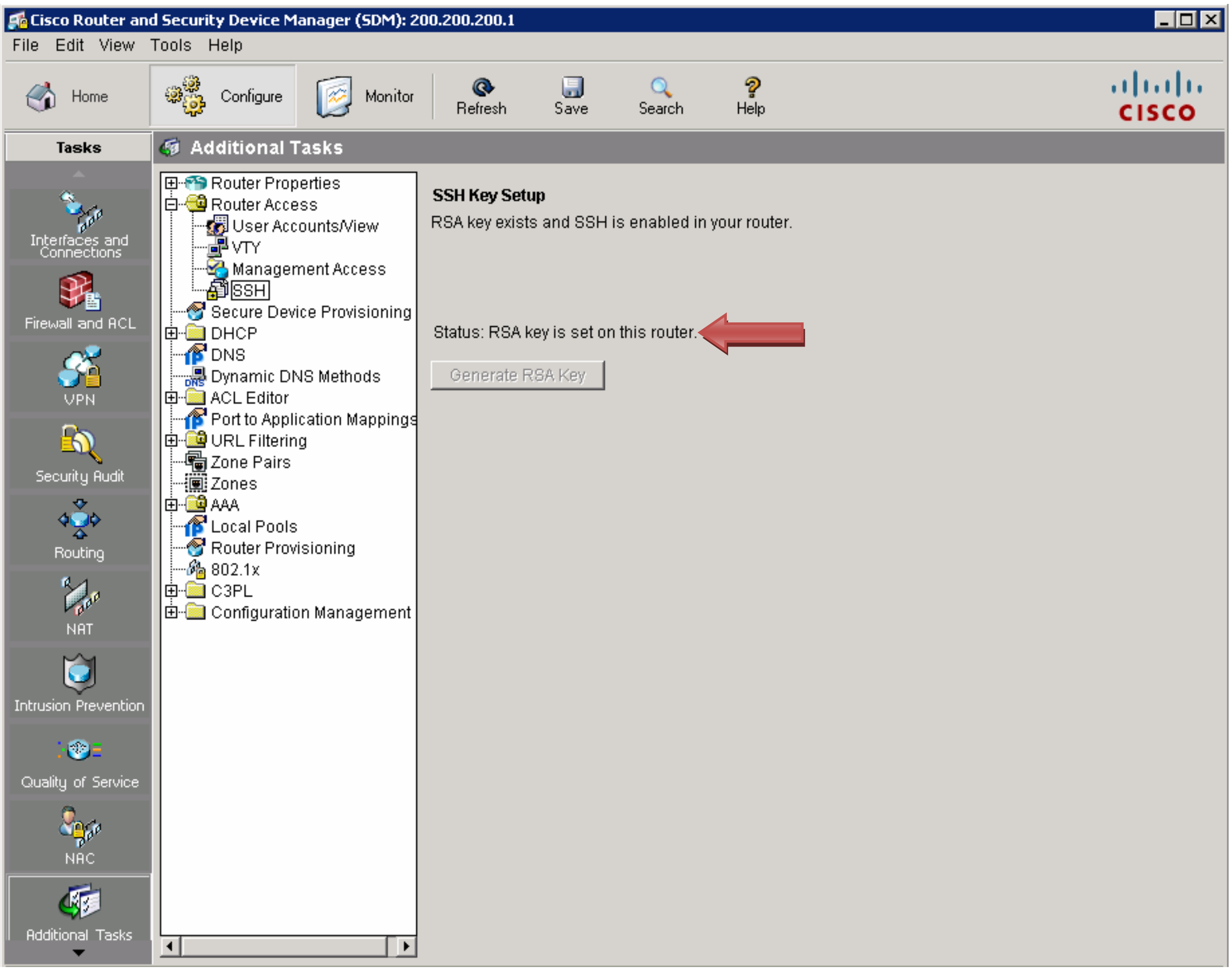


Please type your SSH user name and password.

Username: admin

Password: ********

e. Notice that the RSA key is now set on the router.



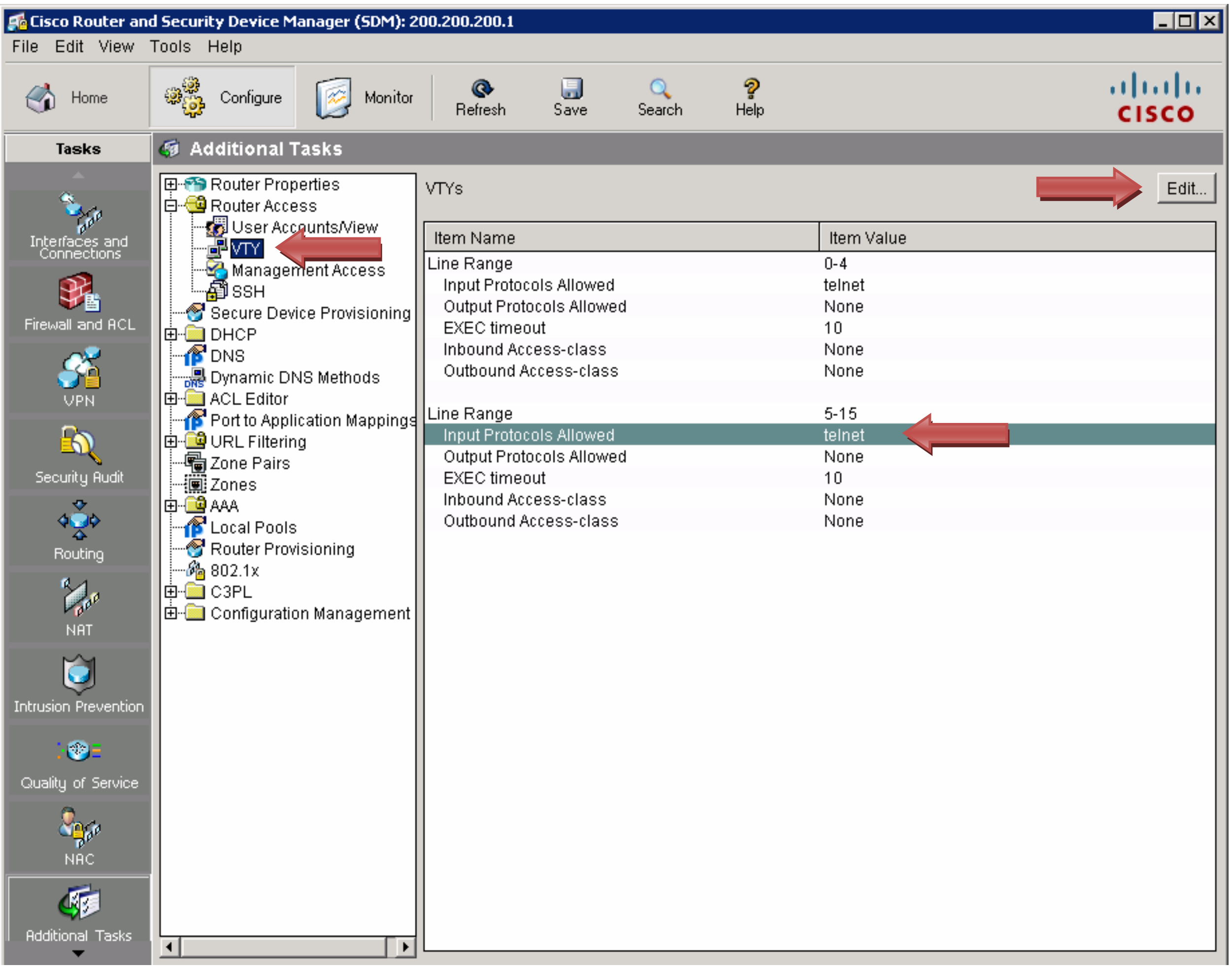
Cisco Router and Security Device Manager (SDM): 200.200.200.1

SSH Key Setup

RSA key exists and SSH is enabled in your router.

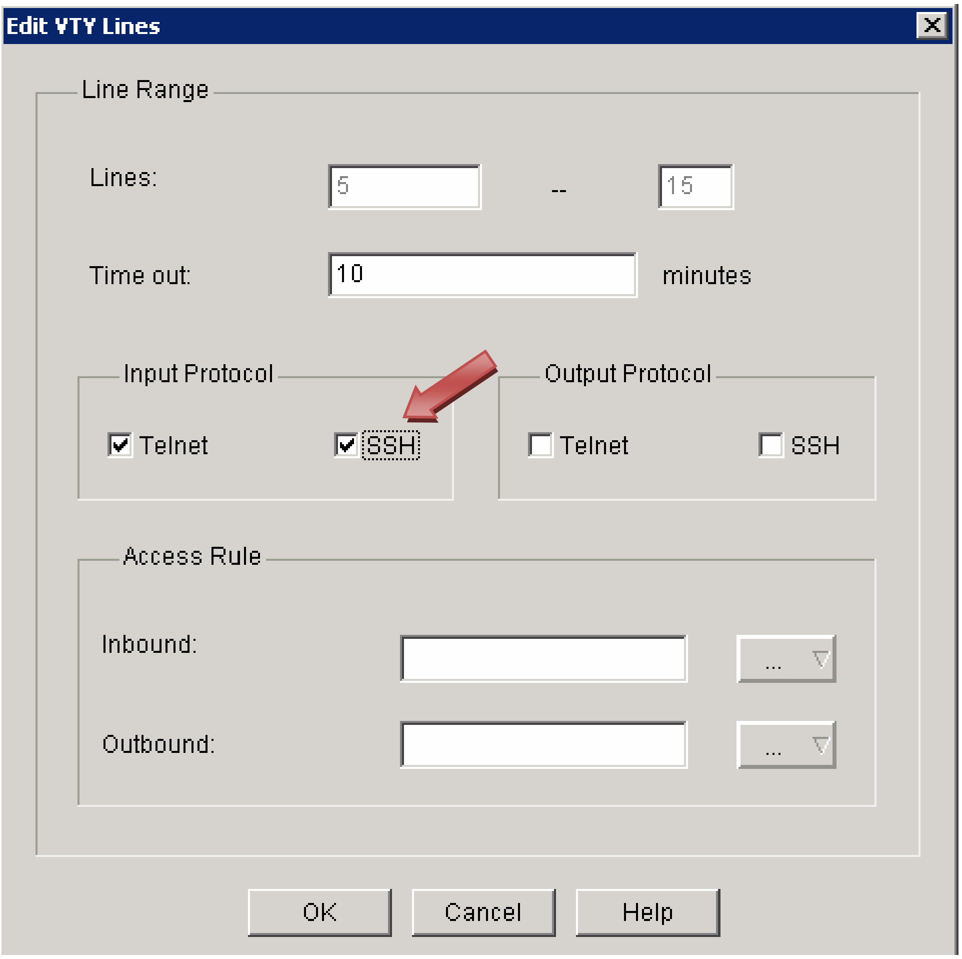
Status: RSA key is set on this router.

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

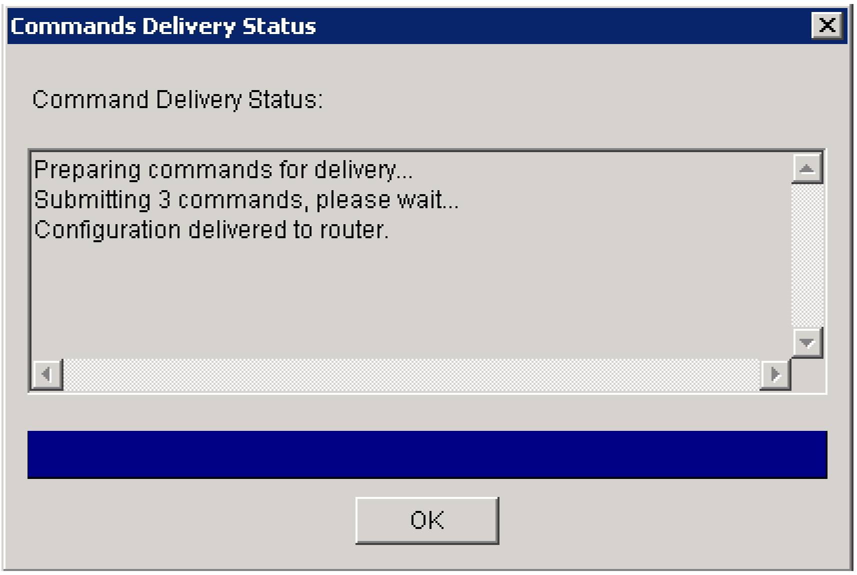


Item Name	Item Value
Line Range	0-4
Input Protocols Allowed	telnet
Output Protocols Allowed	None
EXEC timeout	10
Inbound Access-class	None
Outbound Access-class	None
Line Range	5-15
Input Protocols Allowed	telnet
Output Protocols Allowed	None
EXEC timeout	10
Inbound Access-class	None
Outbound Access-class	None

g. Check the **SSH** box for the Input Protocol, and then click **OK**.

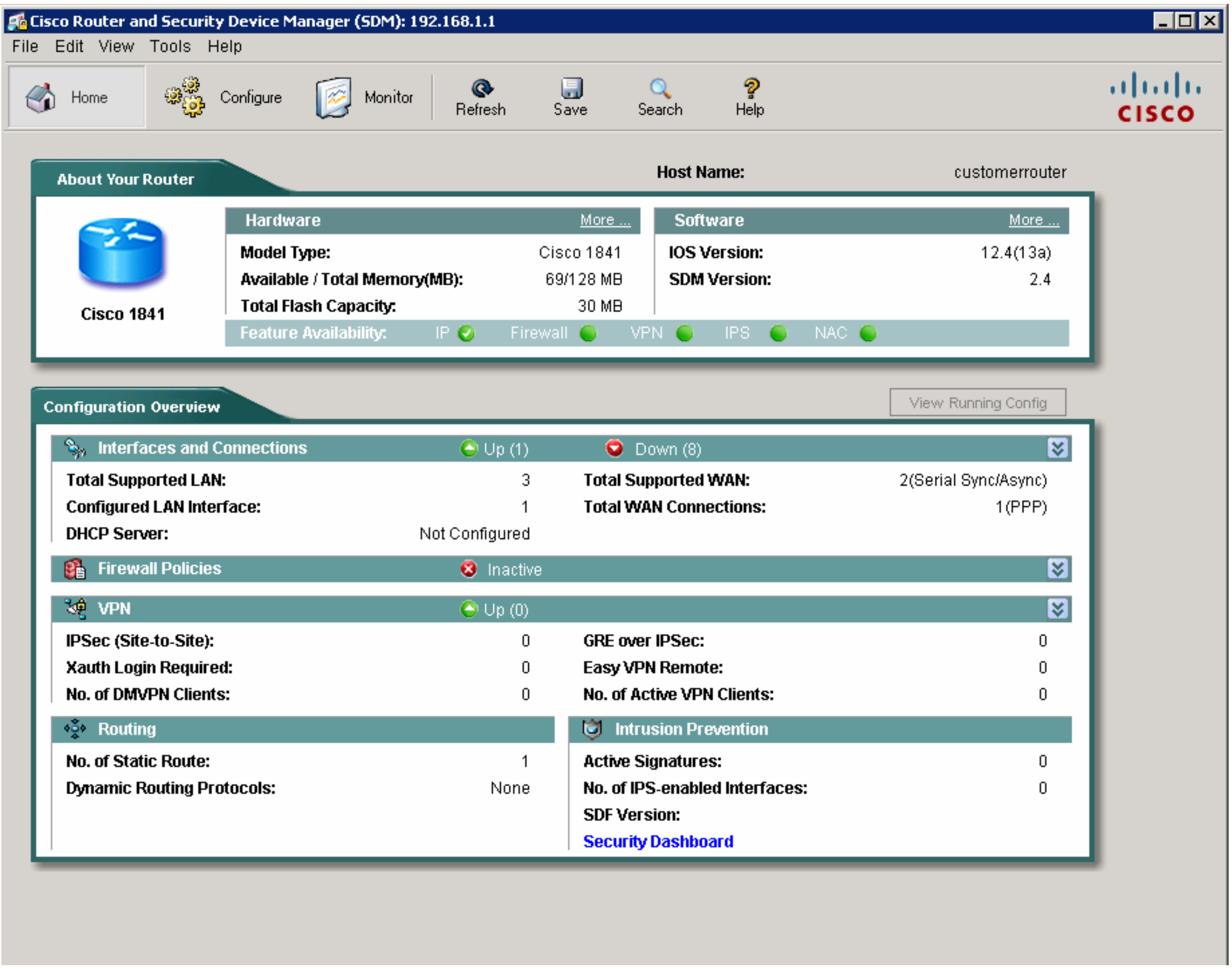


h. When the **Commands Delivery Status** window opens, click **OK**.



```
Preparing commands for delivery...
Submitting 3 commands, please wait...
Configuration delivered to router.
```

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


Cisco Router and Security Device Manager (SDM): 192.168.1.1
File Edit View Tools Help
Home
Configure
Monitor
Refresh
Save
Search
Help
CISCO
View Running Config

About Your Router

Host Name: customerrouter

Cisco 1841

Hardware More ...

Model Type: Cisco 1841

Available / Total Memory(MB): 69/128 MB

Total Flash Capacity: 30 MB

Software More ...

IOS Version: 12.4(13a)

SDM Version: 2.4

Feature Availability: IP ✓ Firewall ● VPN ● IPS ● NAC ●

Configuration Overview

Interfaces and Connections Up (1) Down (8)

Total Supported LAN: 3

Configured LAN Interface: 1

DHCP Server: Not Configured

Total Supported WAN: 2(Serial Sync/Async)

Total WAN Connections: 1(PPP)

Firewall Policies Inactive

VPN Up (0)

IPSec (Site-to-Site): 0

Xauth Login Required: 0

No. of DMVPN Clients: 0

GRE over IPSec: 0

Easy VPN Remote: 0

No. of Active VPN Clients: 0

Routing

No. of Static Route: 1

Dynamic Routing Protocols: None

Intrusion Prevention

Active Signatures: 0

No. of IPS-enabled Interfaces: 0

SDF Version:

Security Dashboard

j. Click **Yes** to confirm the closing of SDM, and go to Step 3. (Step 2 shows you how to configure SSH on a non-SDM router.)

Step 2: (Optional) Configure SSH on a 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. Connect the router console port with a PC and the HyperTerminal program, as described in Lab 5.1.3, “Powering up an Integrated Services Router.”

b. Log in to the router. At the privileged EXEC mode prompt, enter the Cisco IOS CLI commands as shown below. These commands do not include all the passwords that need to be set. See Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for the configuration settings.

   Note: The router must be running Cisco IOS software release 12.2 or later. In this example, the router is a Cisco 2620XM running Cisco IOS software release 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 is 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.

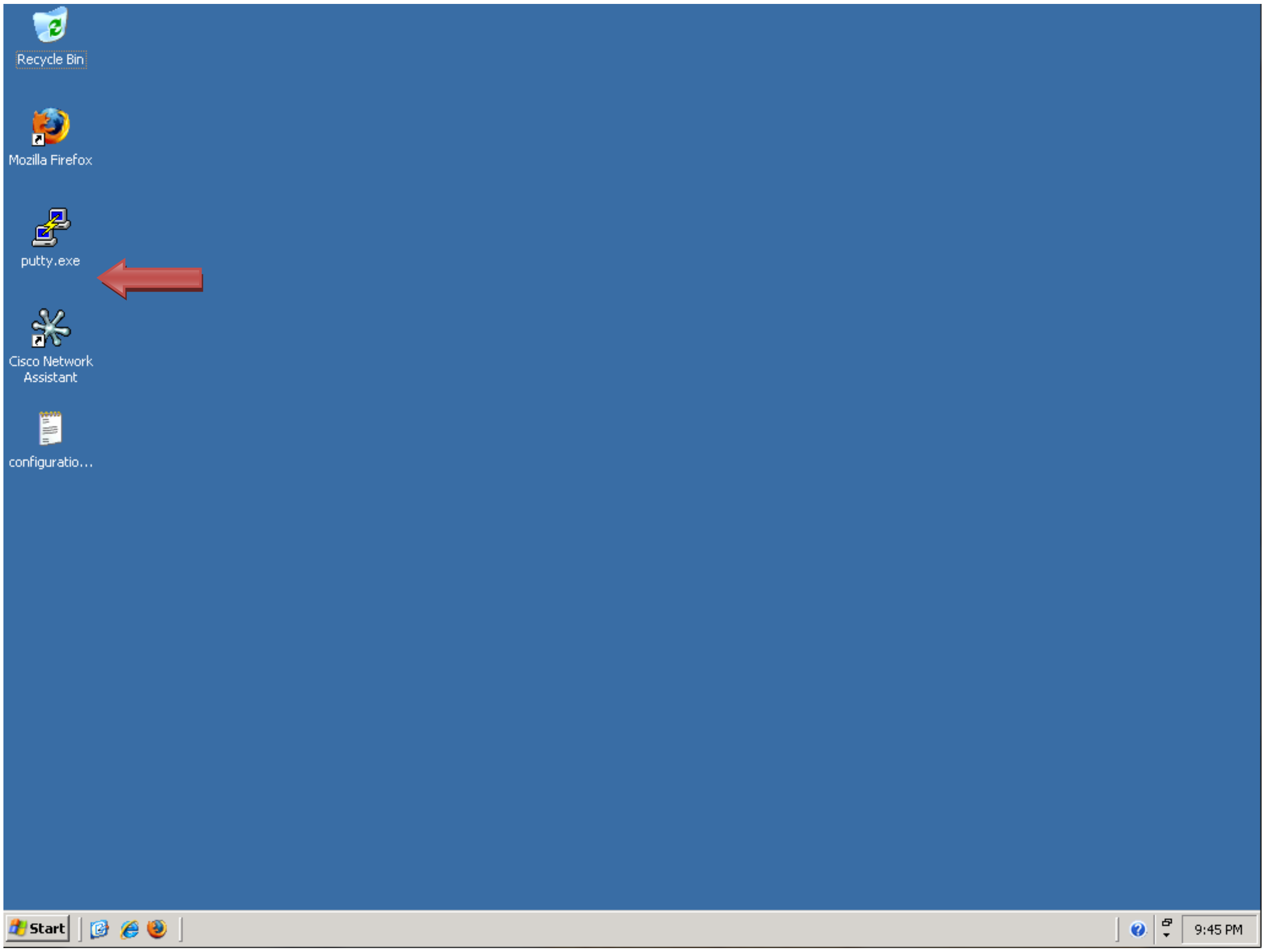
   SSH version enabled ___________________
   Authentication timeout ___________________
   Authentication retries ___________________

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

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

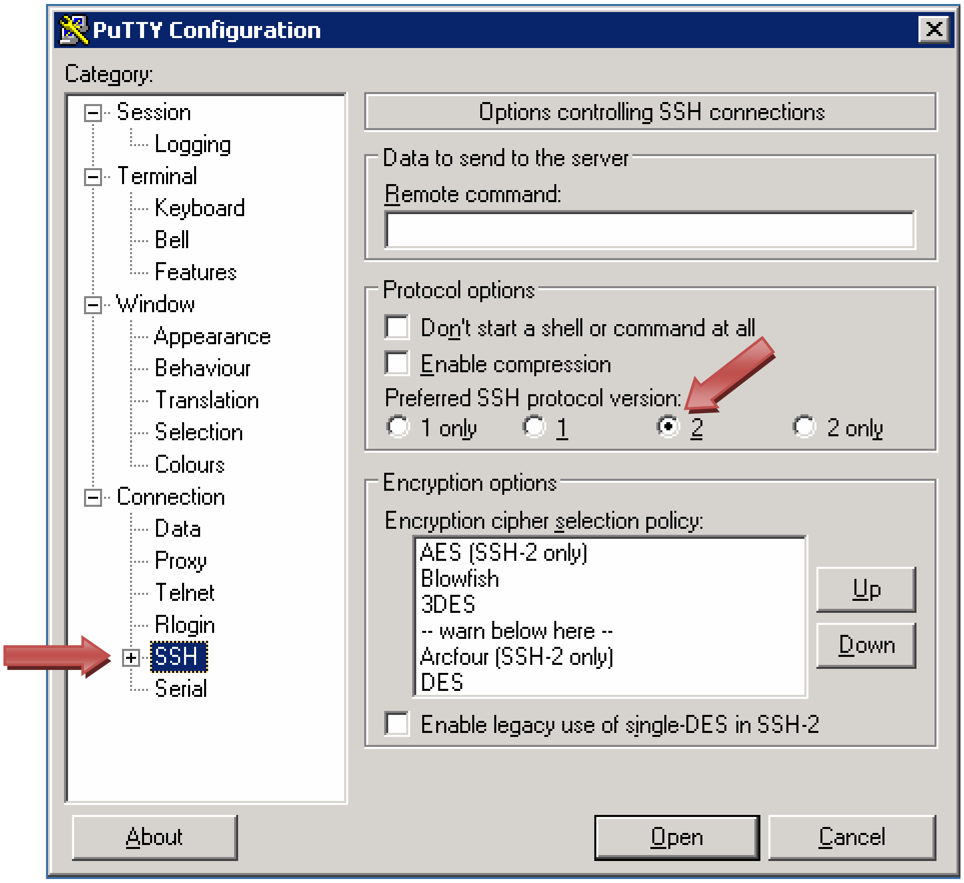
Step 3: Configure the SSH client and connect the PC to the ISR.

a. Download putty.exe and place the application on the desktop. Launch PuTTY by double-clicking the putty.exe icon.


Recycle Bin
Mozilla Firefox
putty.exe
Cisco Network Assistant
configuratio...
Start
9:45 PM

b. In the Category pane, click **SSH**. Verify that the preferred SSH protocol version is set to **2**.

Note: The Putty client still connects even if the SSH server is running SSH version 1.



Options controlling SSH connections

Data to send to the server

Remote command:

Protocol options

□ Don't start a shell or command at all

□ Enable compression

Preferred SSH protocol version:

○ 1 only ○ 1 ● 2 ○ 2 only

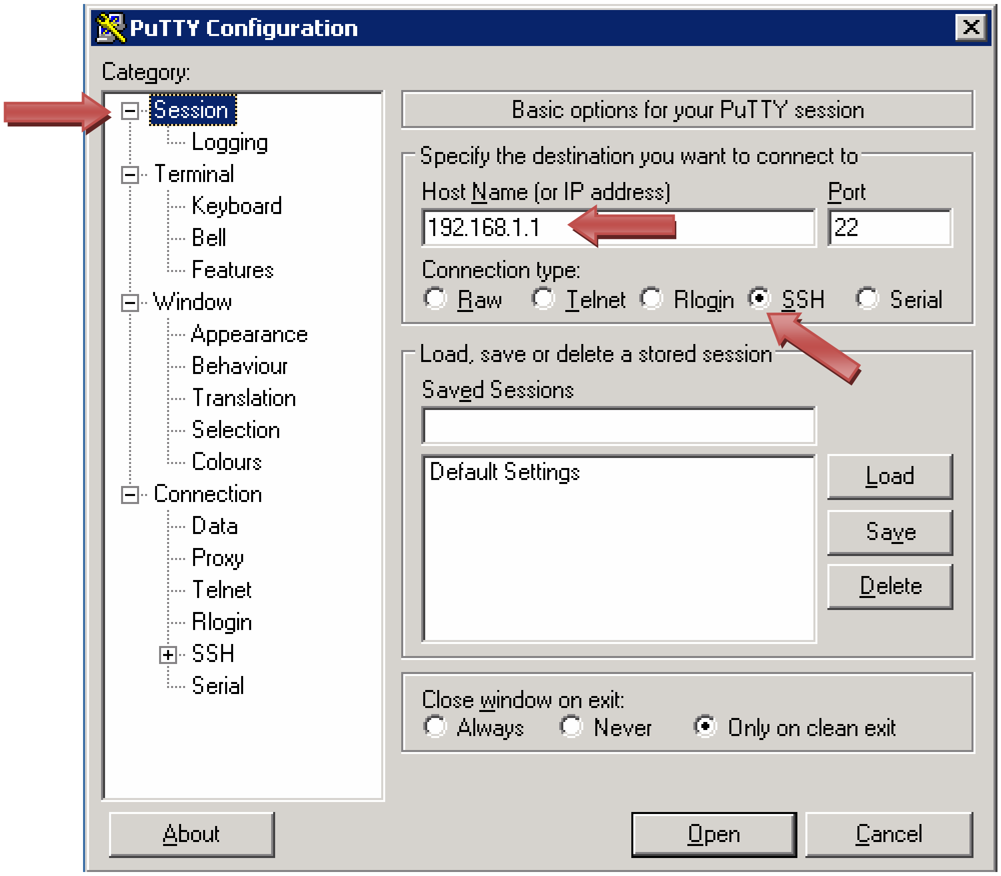
Encryption options

Encryption cipher selection policy:

AES (SSH-2 only)
Blowfish
3DES
-- warn below here --
Arcfour (SSH-2 only)
DES

□ Enable legacy use of single-DES in SSH-2

c. In the Category pane, click **Session**. 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**.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.1

Port: 22

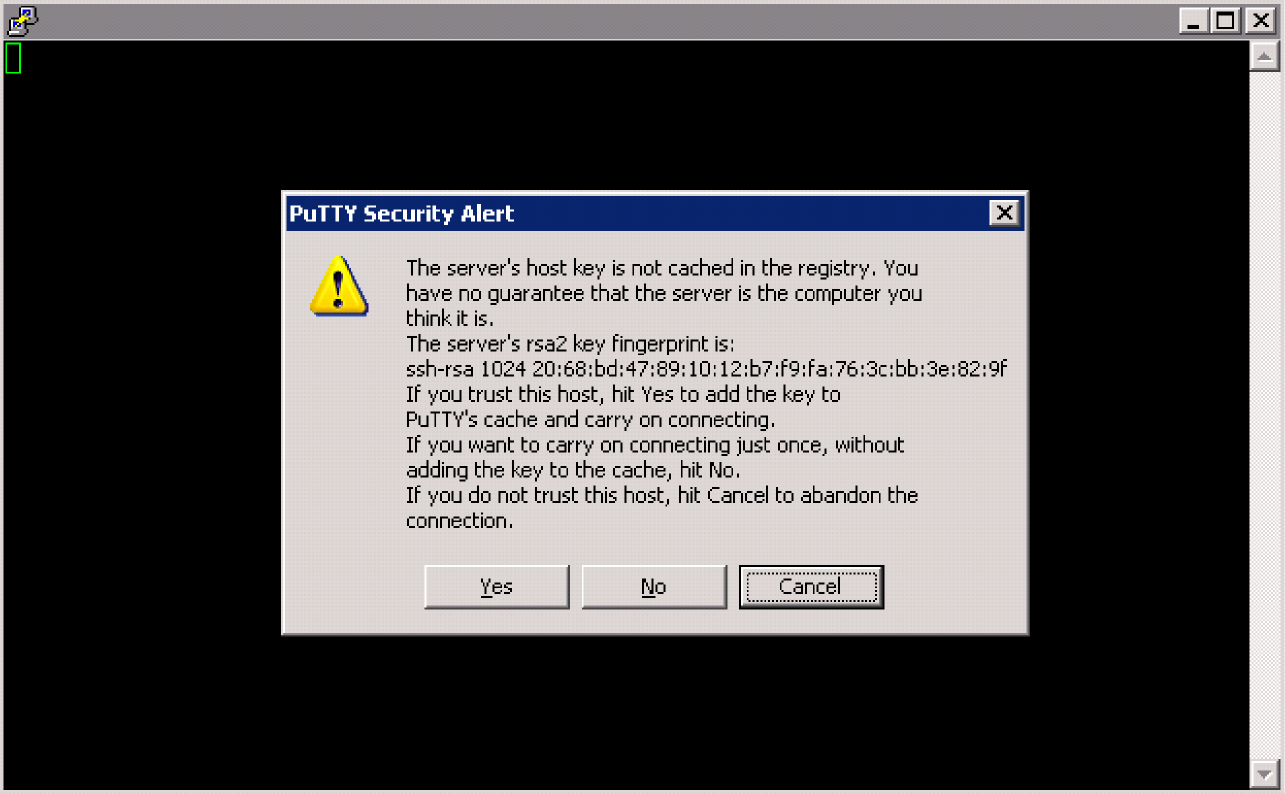
Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

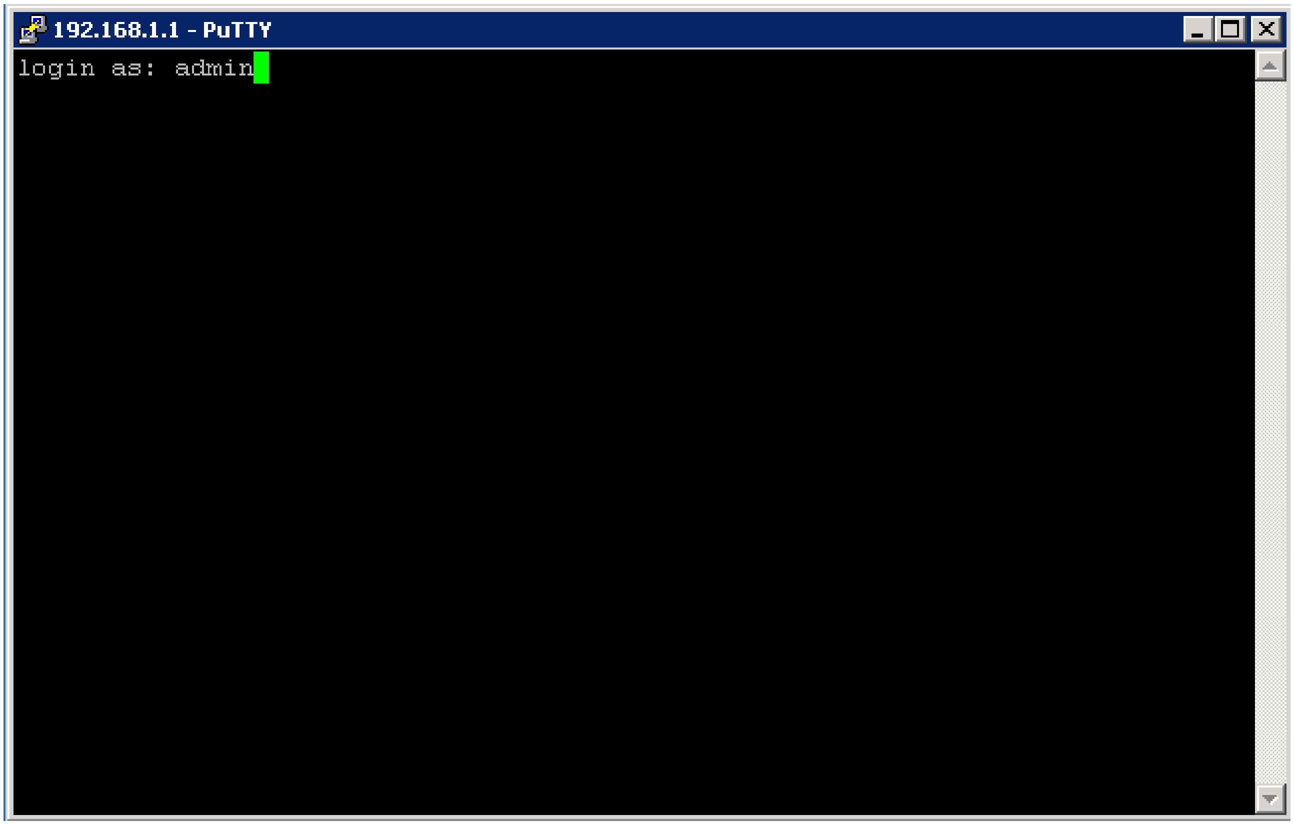
d. The first time a connection is made to SSH on the Cisco 1841 ISR using an SSH client, a connection key is cached in the local machine registry. In the PuTTY Security Alert window, click **Yes** to continue.



PuTTY Security Alert

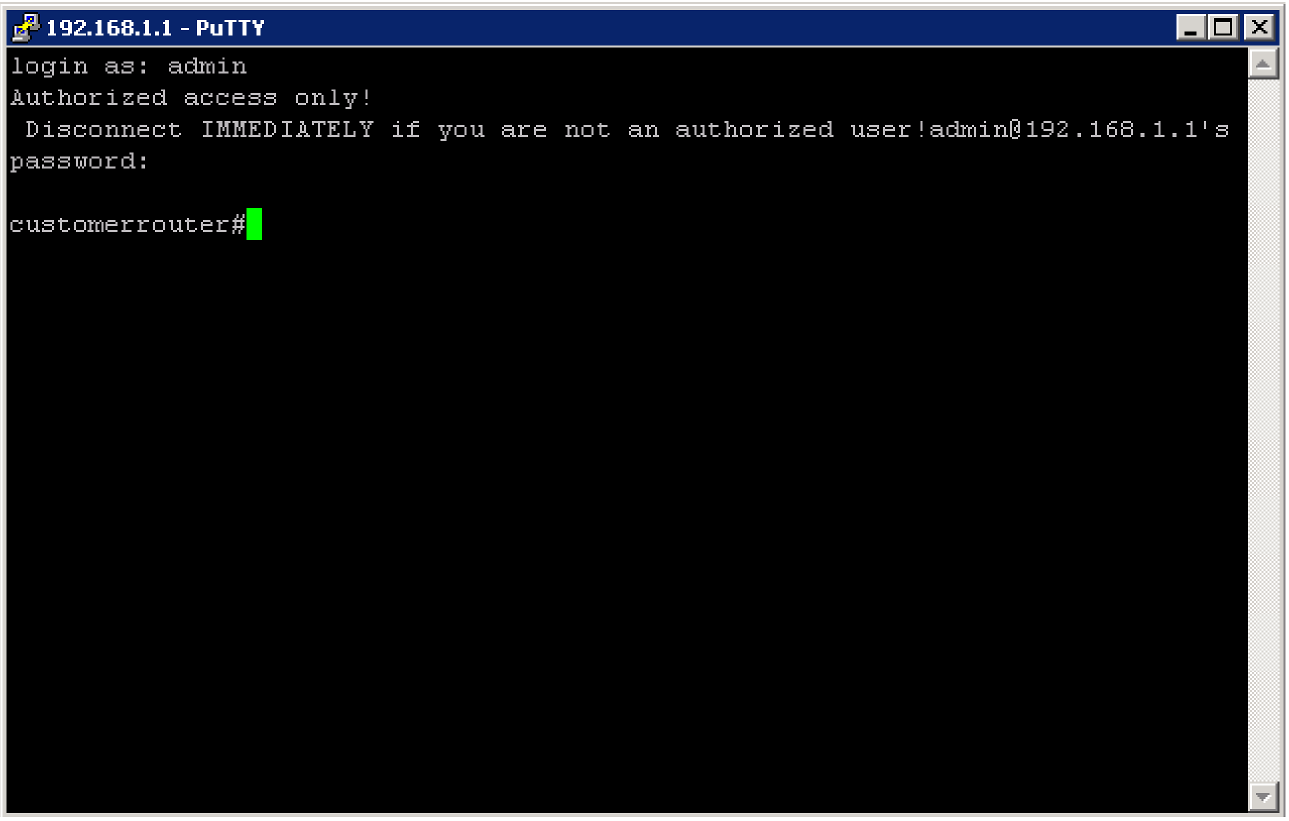
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 20:68:bd:47:89:10:12:b7:f9:fa:76:3c:bb:3e:82:9f
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

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



```
login as: admin
```

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



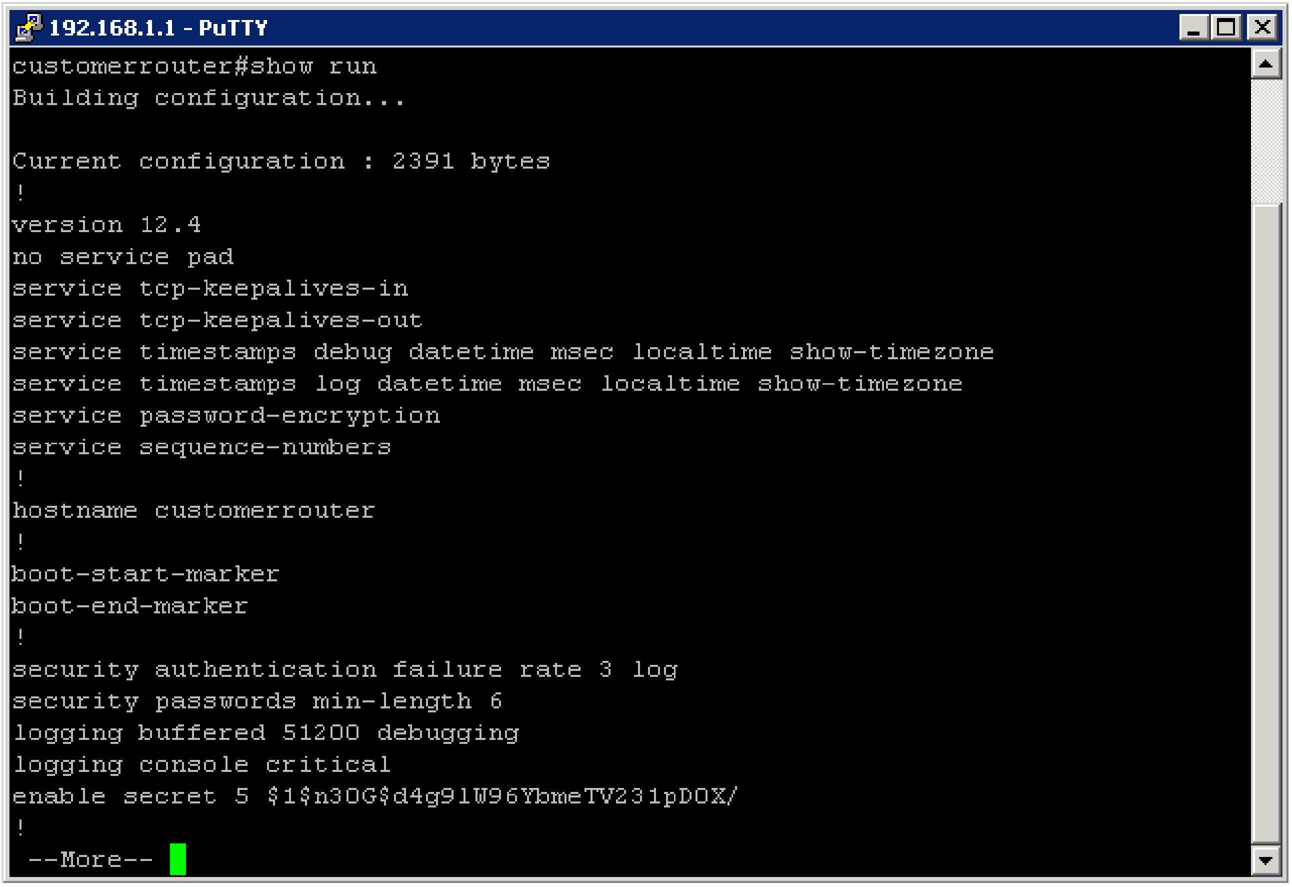
```
login as: admin
Authorized access only!
 Disconnect IMMEDIATELY if you are not an authorized user!admin@192.168.1.1's
password:

customerrouter#
```

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 if you are using SDM, because privileged mode is the default mode.

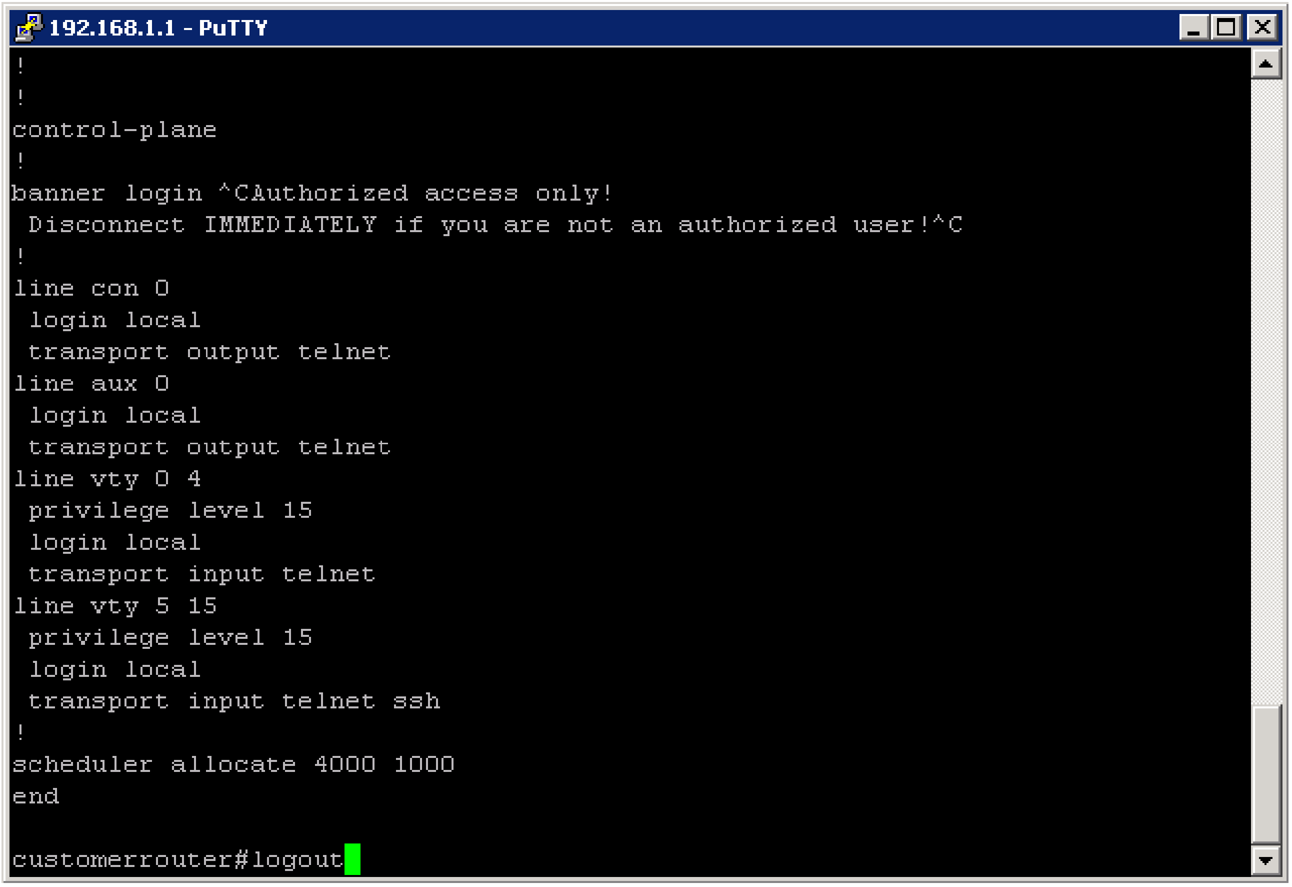
b. Press the **Spacebar** to scroll through the current configuration of the router.



```
customerrouter#show run
Building configuration...

Current configuration : 2391 bytes
!
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname customerrouter
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 debugging
logging console critical
enable secret 5 $1$n30G$d4g91W96YbmeTV231pDOX/
!
 --More--
```

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**.



```
!
!
control-plane
!
banner login ^CAuthorized access only!
 Disconnect IMMEDIATELY if you are not an authorized user!^C
!
line con 0
 login local
 transport output telnet
line aux 0
 login local
 transport output telnet
line vty 0 4
 privilege level 15
 login local
 transport input telnet
line vty 5 15
 privilege level 15
 login local
 transport input telnet ssh
!
scheduler allocate 4000 1000
end

customerrouter#logout
```

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?

____

Basic Cisco IOS Configuration to Bring Up SDM

If the startup config is erased in an SDM router, SDM no longer comes up by default when the router is restarted. It is then necessary to build a basic config as follows. Further details regarding the setup and use of SDM 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 connects 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 a connection to a different port 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.

```
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). Replace *username* and *password* with the username and password that you want to configure.

```
Router(config)#username <username> privilege 15 password 0 <password>
```

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 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)?

____

____

____

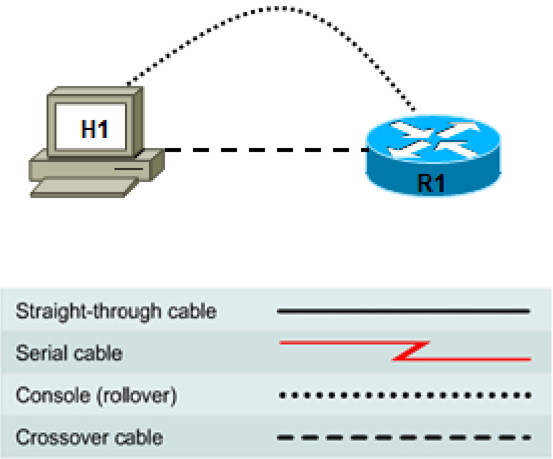
____

____

____

____

Lab 8.4.3a Managing Cisco IOS Images with TFTP



Device	Host Name	Interface	IP Address	Subnet Mask
R1	R1	Fast Ethernet 0/0	172.17.0.1	255.255.0.0

Objectives

- Analyze the Cisco IOS image and router flash memory.
- Use TFTP to copy the software image from a router to a TFTP server.
- Reload the backup software image from a TFTP server into flash on a router.

Background / Preparation

In this lab, you use the **show flash** command to view the files in the router flash memory and determine the amount of flash available. You use will use Trivial File Transfer Protocol (TFTP) server software to back up the router Cisco IOS image to the TFTP server. You then copy the Cisco IOS image from the TFTP server back to the router.

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. This lab uses a Cisco 1841 router with Cisco IOS 12.4. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One router with an Ethernet interface
- One Windows XP computer (or Discovery Server)
- Crossover Category 5 Ethernet cable (H1 to router R1)
- Console cable (from H1 to R1)

- Access to the computer host command prompt
- Access to the computer host network TCP/IP configuration

Note: Instead of using a PC and installing TFTP server software, you may use the Discovery Server, which has Linux-based TFTP server software pre-installed. Check with the instructor on the availability of a Discovery Server CD. The Discovery Server can take the place of host H1 in the topology diagram. The IP addresses used to configure host H1 and R1 in this lab are compatible with the Discovery Server.

From host H1, start a HyperTerminal session to the attached router.

Note: Make sure that the router has been erased and has no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Verify Connectivity

Step 1: Configure the TFTP server host.

Connect the router and host H1 according to the topology diagram. Configure the host H1 IP address with the following settings.

IP address: 172.17.0.2
Subnet mask: 255.255.0.0
Default gateway: 172.17.0.1

Step 2: Log in to router R1 and configure the basic settings.

a. Configure the host name for R1.

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

b. Configure a console, vty, and enable secret passwords. Configure synchronous logging for the console line.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret class
R1(config)#exit
```

c. Configure a message-of-the-day (MOTD) banner and no ip domain lookup.

```
R1(config)#banner motd #Unauthorized Use Prohibited#
R1(config)#no ip domain lookup
```

d. Configure the R1 Fast Ethernet interface.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#description R1 LAN Default Gateway
R1(config-if)#ip address 172.17.0.1 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#end
```

Step 3: Display the R1 router configuration.

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

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

Step 4: Verify basic connectivity.

Host H1 will be the TFTP server, and router R1 will be the TFTP client. To copy files to and from a TFTP server, you must have IP connectivity between the server and the client.

From host H1, ping the router Fast Ethernet interface at IP address 172.17.0.1. Are the pings successful? ________

If the pings are not successful, troubleshoot the host and router configurations until they are.

Step 5: Save the configuration on R1.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

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

Task 2: Collect Router Memory and Image Information

Step 1: Collect information to document the router.

a. From the router HyperTerminal session, issue the **show version** command.

```
Router>show version
```

b. What is the value of the config-register? _____________

c. How much flash memory does this router have? _____________

d. Is there at least 4 MB (4096 KB) of flash memory? _____ (This lab requires at least 4 MB.)

e. What is the version number of the boot ROM? _______________

(This lab requires 5.2 or later.)

Step 2: Collect information about flash memory.

a. Issue the `show flash` command.

```
Router>show flash
```

b. Is the Cisco IOS image already stored in flash? ______

c. If yes, what is the exact name of that file? ____

d. What is the size of the image in flash memory? ________________

e. How much flash is available or unused? _______________________

Note: There must be enough total flash memory to hold the new Cisco IOS image.

Task 3: Use TFTP to Save the Cisco IOS Image

Step 1: Obtain and install the TFTP server application.

There are many free TFTP servers available. A search for “free TFTP server” identifies several you can choose from to download. This lab uses the free SolarWinds TFTP Server application. SolarWinds is a multithreaded TFTP server commonly used to upload and download executable images and configurations to routers and switches. It runs on most Microsoft® operating systems, including Windows® XP, Vista, 2000, and 2003. The SolarWinds software requires the Microsoft .NET 2.0 framework to install.

Note: Check with the instructor for a copy of SolarWinds or another TFTP server that you can install.

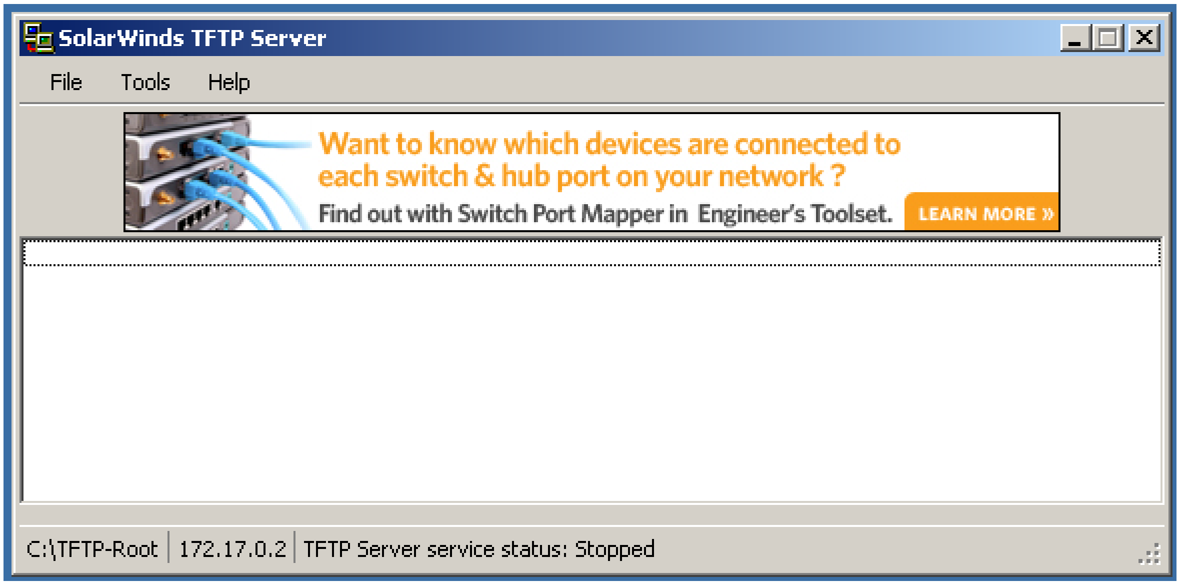
a. Go to the SolarWinds website and download the free TFTP server software and save it to your desktop.

   http://www.solarwinds.com/downloads/

b. Double-click on the SolarWinds TFTP application to begin installation. Select **Next**. Agree to the license agreement, and accept default settings. After the installation has finished, click **Finish**.

Step 2: Start the TFTP application.

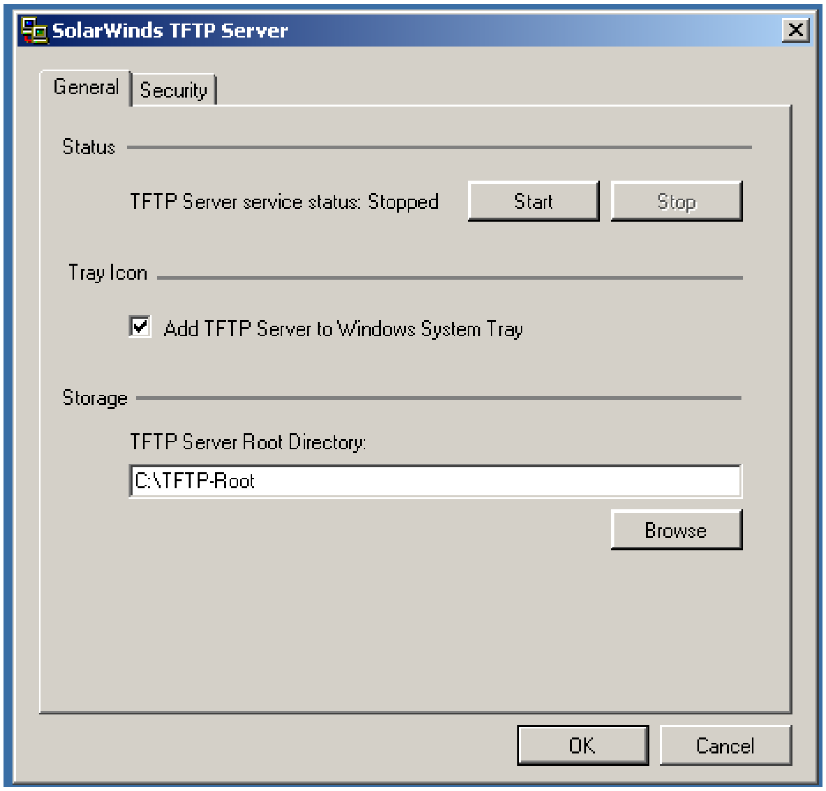
Start the TFTP server by choosing **Start > Programs > SolarWinds TFTP Server > TFTP Server**.


SolarWinds TFTP Server
File
Tools
Help
Want to know which devices are connected to each switch & hub port on your network ?
Find out with Switch Port Mapper in Engineer's Toolset.
LEARN MORE »

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Stopped

Step 3: Configure the TFTP server.

a. To configure the TFTP server, choose **File > Configure.** The screen displayed should be similar to the following. On the **General** tab, check that the default TFTP Server Root Directory is set to C:\TFTP-Root.



Status

TFTP Server service status: Stopped

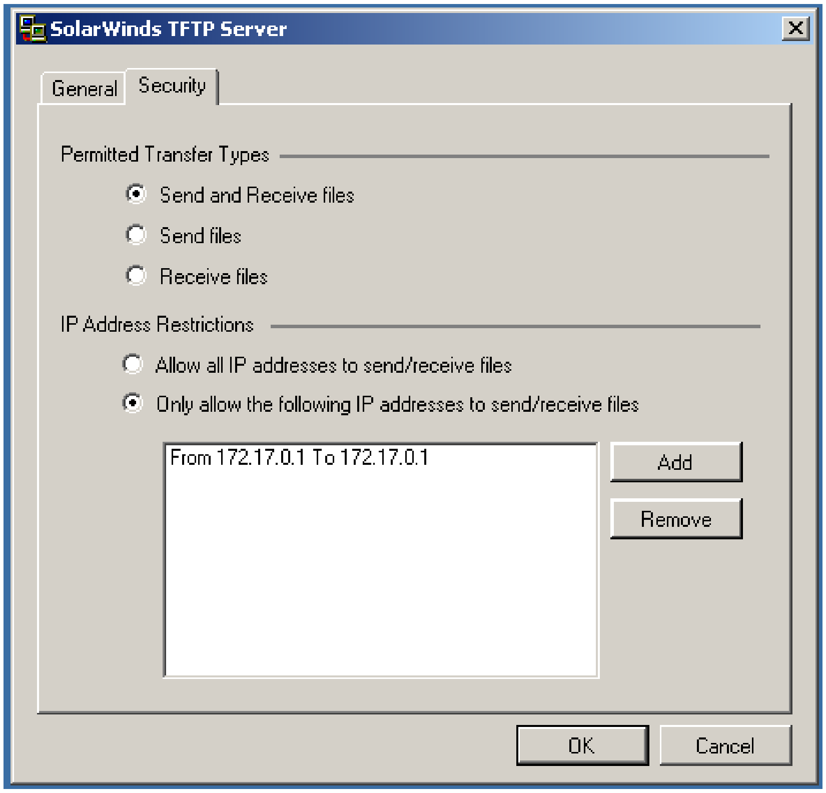
Tray Icon

☑ Add TFTP Server to Windows System Tray

Storage

TFTP Server Root Directory: C:\TFTP-Root

b. Click on the **Security** tab. Check that **Permitted Transfer Types** is set to **Send and Receive files,** and set **IP Address Restrictions** to allow transfers from only the router R1 Fast Ethernet 0/0 IP address (172.17.0.1 To 172.17.0.1).



Permitted Transfer Types

● Send and Receive files
○ Send files
○ Receive files

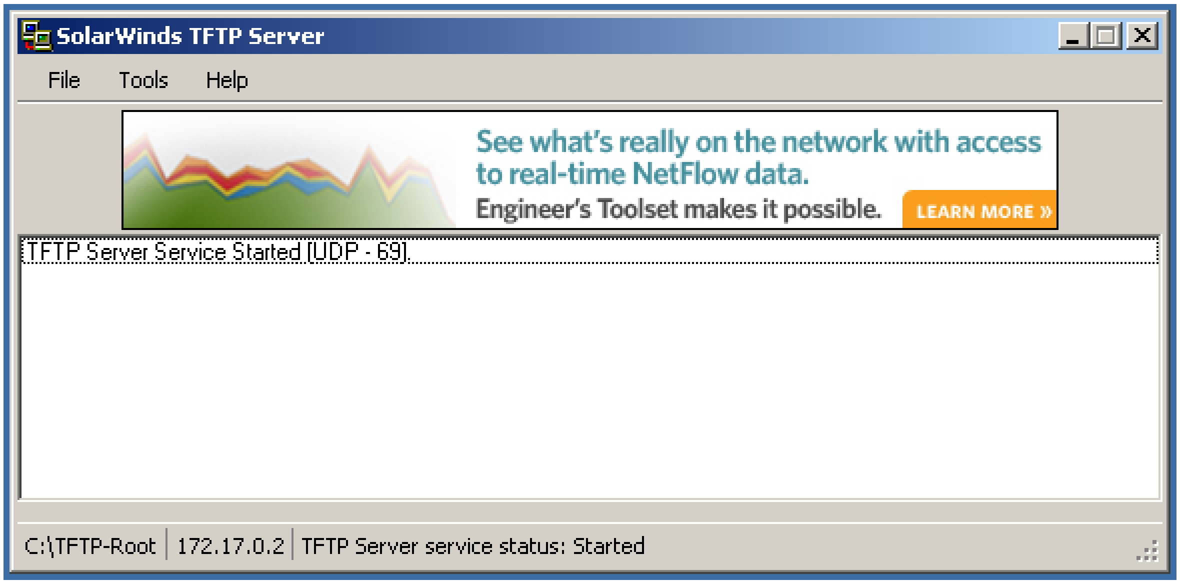
IP Address Restrictions

○ Allow all IP addresses to send/receive files
● Only allow the following IP addresses to send/receive files

From 172.17.0.1 To 172.17.0.1

c. In the **General** tab, click the **Start** button to activate the TFTP Server.

d. When finished, click **OK**. The screen should look similar to the following.


SolarWinds TFTP Server
File
Tools
Help
See what's really on the network with access to real-time NetFlow data.
Engineer's Toolset makes it possible.
LEARN MORE »

```
TFTP Server Service Started [UDP - 69]
```

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Started

e. On which well-known UDP port number is the TFTP server operating? __________

f. Leave the TFTP Server window open so that you can view the activity as the file is copied.

Step 4: Save the R1 Cisco IOS image file to the TFTP server.

a. Write down the Cisco IOS image filename that you will be copying.

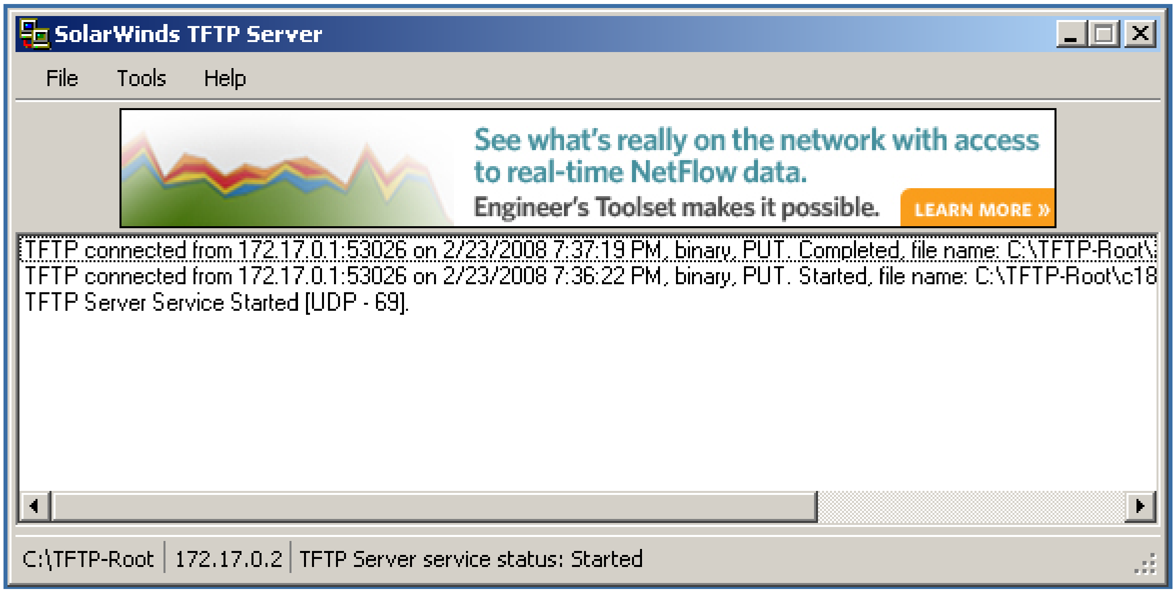
____

b. From the HyperTerminal session on router R1, begin uploading the Cisco IOS image to the TFTP server using the **copy flash tftp** command. Respond to the prompts as shown below, but replace the image filename shown with the one on your router.

```
R1#copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-10b.bin
Address or name of remote host []? 172.17.0.2
Destination filename [c1841-advipservicesk9-mz.124-10b.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
22063220 bytes copied in 58.264 secs (378677 bytes/sec)
```

Step 5: Verify the TFTP server activity.

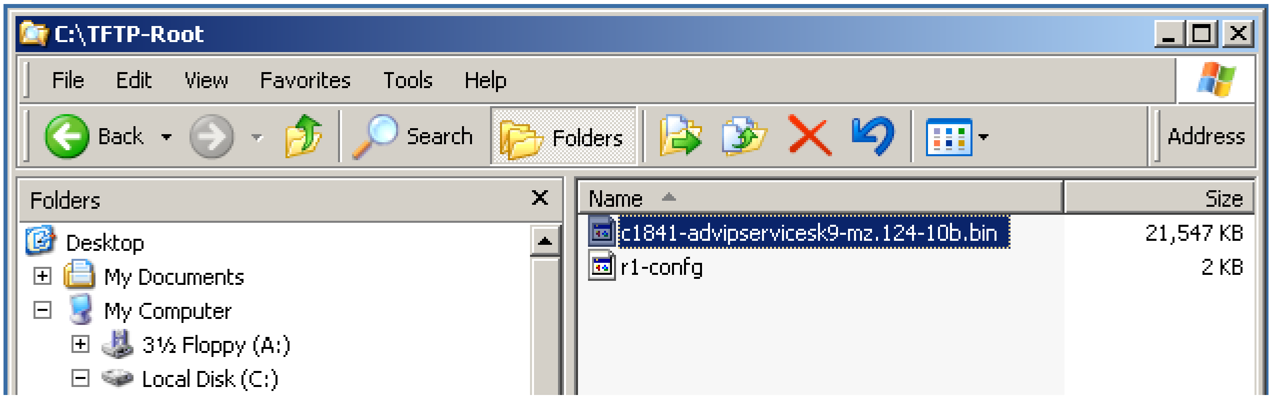
a. Observe the TFTP Server window, which shows the connection entries for the transfer of the running-config file to the server. The output should look similar to the following.


SolarWinds TFTP Server
File Tools Help
See what's really on the network with access to real-time NetFlow data.
Engineer's Toolset makes it possible.
LEARN MORE »

```
TFTP connected from 172.17.0.1:53026 on 2/23/2008 7:37:19 PM, binary, PUT, Completed, file name: C:\TFTP-Root\
TFTP connected from 172.17.0.1:53026 on 2/23/2008 7:36:22 PM, binary, PUT, Started, file name: C:\TFTP-Root\c18
TFTP Server Service Started [UDP - 69].
```

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Started

b. Use Windows Explorer to examine the contents of folder C:\TFTP-Root\ on the host H1 TFTP server. Verify the flash image size in the TFTP server directory. The file size in the **show flash** command should be the same size as the file stored on the TFTP server. If the file sizes are not identical, check with the instructor. The image file should be listed similar to the one shown in the screen below.



Name	Size
c1841-advipservicesk9-mz.124-10b.bin	21,547 KB
r1-confg	2 KB

Task 4: Use TFTP to Update the Cisco IOS Image

Step 1: Copy the image from the TFTP server.

a. Restore the image on the router. Start the copy from the privileged EXEC prompt. When prompted for the destination filename, use the filename from Task 3, Step 4.

```
R1#copy tftp flash
Address or name of remote host []? 172.17.0.2
Source filename []? c1841-advipservicesk9-mz.124-10b.bin
Destination filename [c1841-advipservicesk9-mz.124-10b.bin]?
%Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://172.17.0.2/c1841-advipservicesk9-mz.124-10b.bin...
```

```
Loading c1841-advipservicesk9-mz.124-10b.bin from 172.17.0.2 (via
FastEthernet0/
0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!
[OK - 22063220 bytes]

22063220 bytes copied in 70.036 secs (315027 bytes/sec)
```

b. Does the image fit in the available flash? _____

c. What is the size of the file being loaded? _________________

d. What happened on the router console screen as the file was being downloaded?

____

Step 2: Verify that the image file transfer was successful.

a. Restart the router using the **reload** command and observe the startup process to confirm that there were no flash errors. If there are none, the router Cisco IOS software should have started correctly.

b. Verify the new image in flash using the **show flash** command. How can you tell that the previous image was overwritten? ____

```
R1#show flash
-#- --length-- -----date/time------ path
1     22063220 Feb 23 2008 01:25:20 c1841-advipservicesk9-mz.124-10b.bin
2         1038 May 18 2007 14:25:40 home.shtml
3         1821 May 18 2007 14:25:40 sdmconfig-18xx.cfg
4       113152 May 18 2007 14:25:42 home.tar
5      1164288 May 18 2007 14:25:44 common.tar
6      6036480 May 18 2007 14:25:54 sdm.tar
7       861696 May 18 2007 14:26:04 es.tar
8       527849 May 18 2007 14:25:42 128MB.sdf
9      1684577 Mar 15 2007 07:23:20 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 Mar 15 2007 07:23:54 sslclient-win-1.1.0.154.pkg

31121408 bytes available (32874496 bytes used)
```

Task 5: Reflection

How can TFTP be used to manage networking device files in an enterprise network?

____

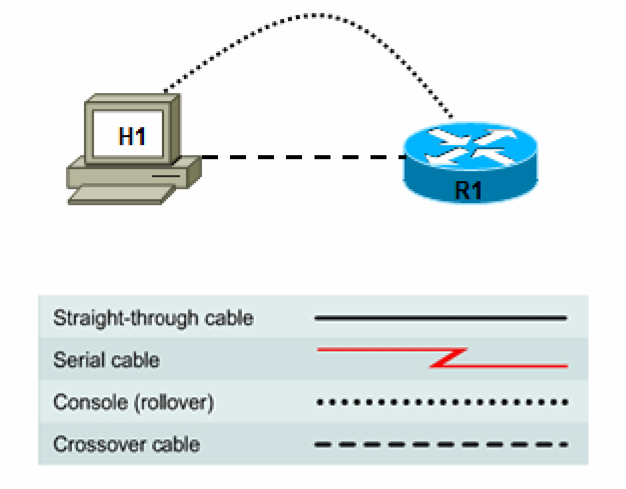
____

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 8.4.3b Managing Cisco IOS images with ROMMON and TFTP



Device	Host Name	Interface	IP Address	Subnet Mask
R1	R1	Fast Ethernet 0/0	172.17.0.1	255.255.0.0

Objectives

- Analyze the Cisco IOS image and router flash memory.
- Back up a Cisco IOS software image to a TFTP server.
- Use ROM monitor (ROMmon) and the **tftpdnld** command to restore an image from a TFTP server.

Background / Preparation

In this lab, you use the **show flash** command to view the Cisco IOS image in the router flash memory. You use TFTP server software to back up the image to the TFTP server. You then simulate the loss of the image and use the ROMmon **tftpdnld** command to copy the image from the TFTP server back to the router.

Important: Check with the instructor before performing Task 6 in this lab. The **tftpdnld** command erases all existing files in flash memory before downloading a new software image to the router. If there are files in the router flash memory that you do not want to lose, they must be backed up to the TFTP server and then copied back to flash memory after the Cisco IOS image has been restored. The process for copying files to and from a TFTP server is described in Lab 8.4.3a, “Managing Cisco IOS Images with TFTP.”

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. This lab uses a Cisco 1841 router with Cisco IOS software release 12.4. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One router with an Ethernet interface
- One Windows XP computer (or Discovery Server)
- Crossover Category 5 Ethernet cable (H1 to router R1)
- Console cable (from H1 to R1)
- Access to the computer host command prompt
- Access to the computer host network TCP/IP configuration

Note: Instead of using a PC and installing TFTP server software, you may use the Discovery Server, which has Linux-based TFTP server software pre-installed. Check with the instructor on the availability of a Discovery Server CD. The Discovery Server can take the place of host H1 in the topology diagram. The IP addresses used to configure host H1 and R1 in this lab are compatible with the Discovery Server.

From host H1, start a HyperTerminal session to the attached router.

Note: Make sure that the router has been erased and has no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Verify Connectivity

Step 1: Configure the TFTP server host.

Connect the router and host H1 according to the topology diagram. Configure host H1 IP address with the following settings.

IP address: 172.17.0.2
Subnet mask: 255.255.0.0
Default gateway: 172.17.0.1

Step 2: Log in to router R1 and configure the basic settings.

a. Configure the host name for R1.

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

b. Configure a console, vty, and enable secret passwords. Configure synchronous logging for the console line.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#enable secret class
R1(config)#exit
```

c. Configure a message-of-the-day (MOTD) banner using and no ip domain lookup.

```
R1(config)#banner motd #Unauthorized Use Prohibited#
R1(config)#no ip domain lookup
```

d. Configure the R1 Fast Ethernet interface.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#description R1 LAN Default Gateway
R1(config-if)#ip address 172.17.0.1 255.255.0.0
R1(config-if)#no shutdown
R1(config-if)#end
```

Step 3: Display the R1 router configuration.

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

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

Step 4: Verify basic connectivity.

Host H1 will be the TFTP server, and router R1 will be the TFTP client. To copy files to and from a TFTP server, you must have IP connectivity between the server and the client.

From host H1, ping the router Fast Ethernet interface at IP address 172.17.0.1. Are the pings successful? _____

If the pings are not successful, troubleshoot the host and router configs until they are.

Step 5: Save the configuration on R1.

Save the running configuration to the startup configuration from the privileged EXEC prompt.

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

Task 2: Collect Router Memory and Image Information

Step 1: Collect information to document the router.

a. From the router HyperTerminal session, issue the **show version** command.

```
Router>show version
```

b. What is the value of the config-register? _____________

c. How much flash memory does this router have? _____________

d. What is the version number of the boot ROM? _______________

Step 2: Collect information about flash memory.

a. Issue the **show flash** command.

```
Router>show flash
```

b. Is the Cisco IOS image already stored in flash? _____

c. If yes, what is the exact name of that file? ____

d. What is the size of the image in flash memory? ____________________

e. How much flash is available or unused? __________________________

f. To what value is the configuration register set? ____________________

Note: There must be enough flash memory to hold the new Cisco IOS image.

g. How many files are in Flash memory? ______________

```
R1>show flash
-#- --length-- -----date/time------ path
1     22063220 Mar 15 2007 07:03:50 c1841-advipservicesk9-mz.124-10b.bin
2         1038 May 18 2007 14:25:40 home.shtml
3         1821 May 18 2007 14:25:40 sdmconfig-18xx.cfg
4       113152 May 18 2007 14:25:42 home.tar
5      1164288 May 18 2007 14:25:44 common.tar
6      6036480 May 18 2007 14:25:54 sdm.tar
7       861696 May 18 2007 14:26:04 es.tar
8       527849 May 18 2007 14:25:42 128MB.sdf
9      1684577 Mar 15 2007 07:23:20 securedesktop-ios-3.1.1.27-k9.pkg
10      398305 Mar 15 2007 07:23:54 sslclient-win-1.1.0.154.pkg

31121408 bytes available (32874496 bytes used)
```

Task 3: Use TFTP to Save the Cisco IOS Image

Step 1: Obtain and install the TFTP server application.

There are many free TFTP servers available. A search for “free TFTP server” identifies several you can choose from to download. This lab uses the free SolarWinds TFTP Server application. SolarWinds is a multithreaded TFTP server commonly used to upload and download executable images and configurations to routers and switches. It runs on most Microsoft® operating systems, including Windows® XP, Vista, 2000, and 2003. The SolarWinds software requires the Microsoft .NET 2.0 framework to install.

Note: Check with the instructor for a copy of SolarWinds or another TFTP server that you can install.

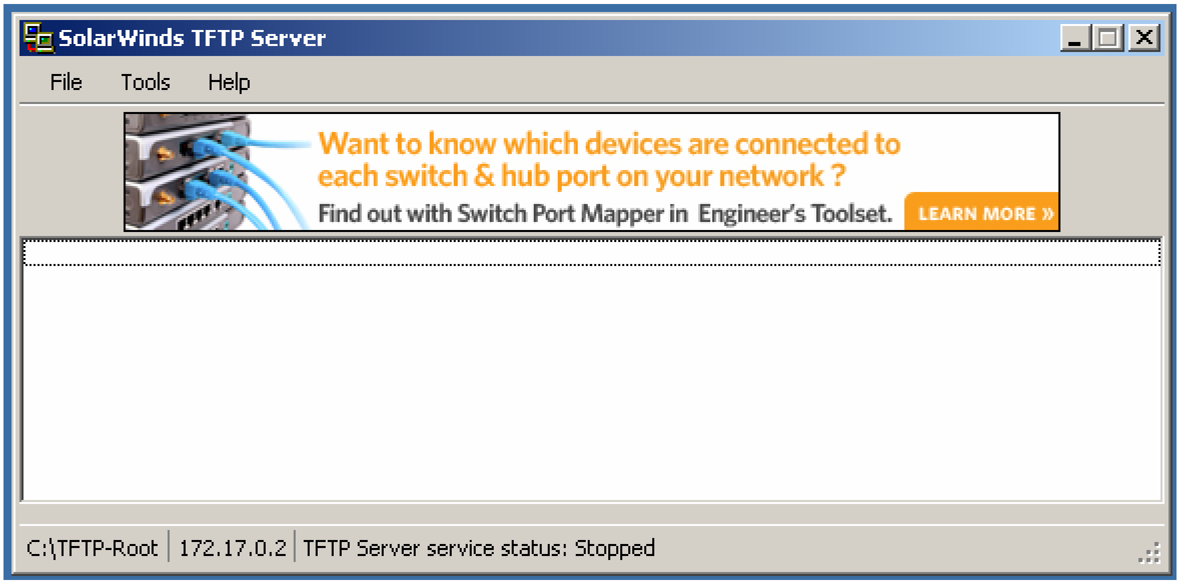
a. Go to the SolarWinds website and download the free TFTP server software and save it to your desktop.

http://www.solarwinds.com/downloads/

b. Double-click on the SolarWinds TFTP application to begin installation. Select **Next**. Agree to the license agreement, and accept default settings. After the installation has finished, click **Finish**.

Step 2: Start the TFTP application.

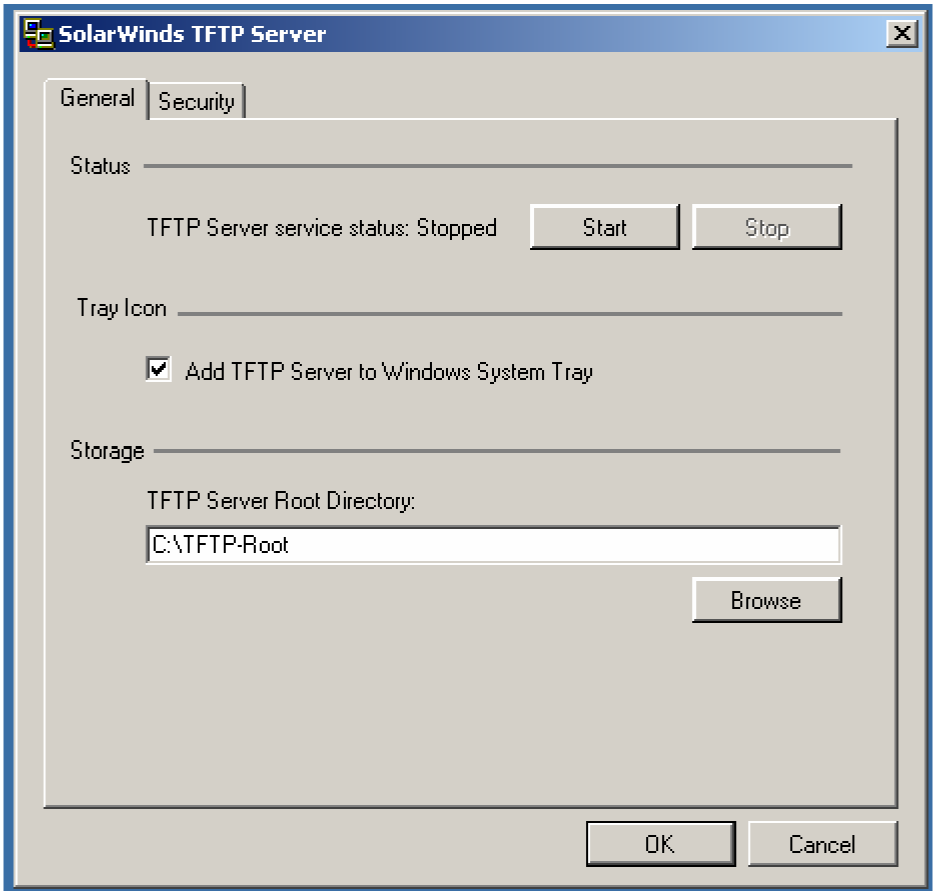
Start the TFTP server by choosing **Start > Programs > SolarWinds TFTP Server > TFTP Server**.


SolarWinds TFTP Server
File
Tools
Help
Want to know which devices are connected to each switch & hub port on your network ?
Find out with Switch Port Mapper in Engineer's Toolset.
LEARN MORE »

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Stopped

Step 3: Configure the TFTP server.

a. To configure the TFTP server, choose **File > Configure.** The screen displayed should be similar to the following. On the **General** tab, check that the default TFTP Server Root Directory is set to C:\TFTP-Root.



SolarWinds TFTP Server

General | Security

Status

TFTP Server service status: Stopped [Start] [Stop]

Tray Icon

☑ Add TFTP Server to Windows System Tray

Storage

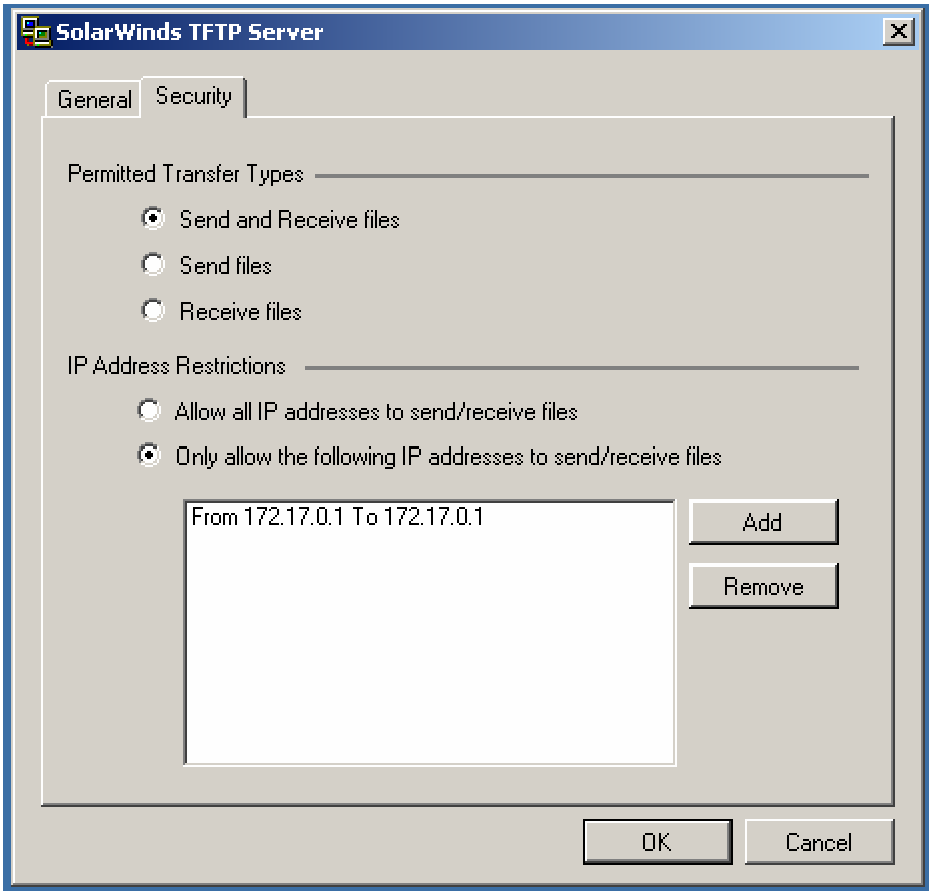
TFTP Server Root Directory:

C:\TFTP-Root

[Browse]

[OK] [Cancel]

b. Click on the **Security** tab. Check that **Permitted Transfer Types** is set to **Send and Receive files,** and set **IP Address Restrictions** to allow transfers from only the router R1 Fast Ethernet 0/0 IP address (172.17.0.1 To 172.17.0.1).



SolarWinds TFTP Server

Permitted Transfer Types

● Send and Receive files

○ Send files

○ Receive files

IP Address Restrictions

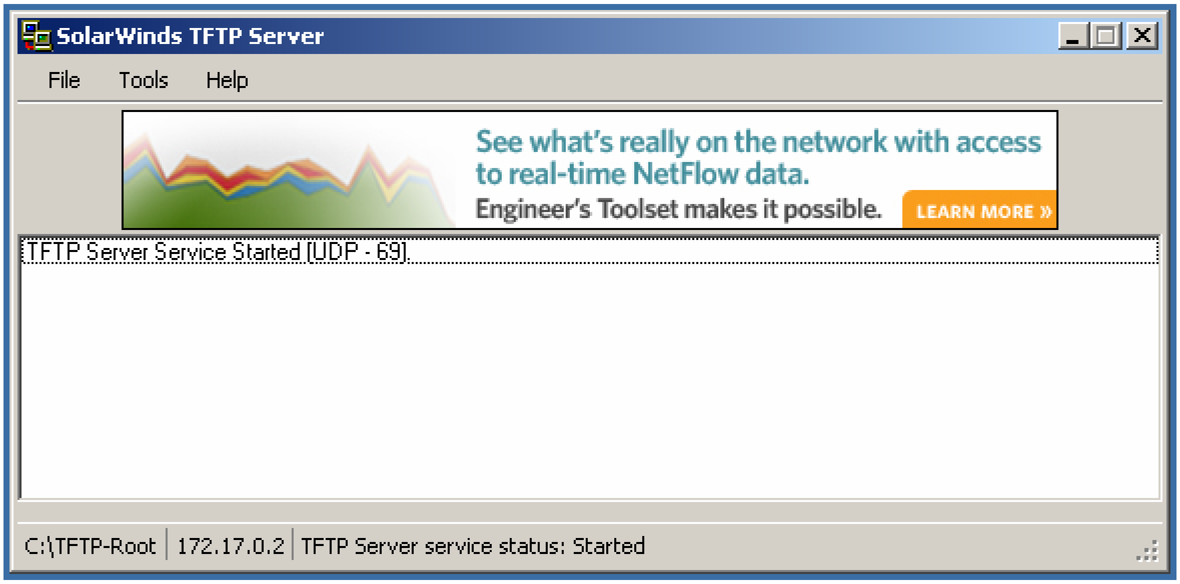
○ Allow all IP addresses to send/receive files

● Only allow the following IP addresses to send/receive files

From 172.17.0.1 To 172.17.0.1

c. In the **General** tab, click the **Start** button to activate the TFTP Server.

d. When finished, click **OK**. The screen should look similar to the following.



SolarWinds TFTP Server

```
TFTP Server Service Started [UDP - 69]
```

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Started

File
Tools
Help
See what's really on the network with access to real-time NetFlow data.
Engineer's Toolset makes it possible.
LEARN MORE »

e. On which well-known UDP port number is the TFTP server operating? __________

f. Leave the TFTP Server window open so that you can view the activity as the file is copied.

Step 4: Save the R1 Cisco IOS image file to TFTP server.

a. Write down the Cisco IOS image filename that you will be copying.

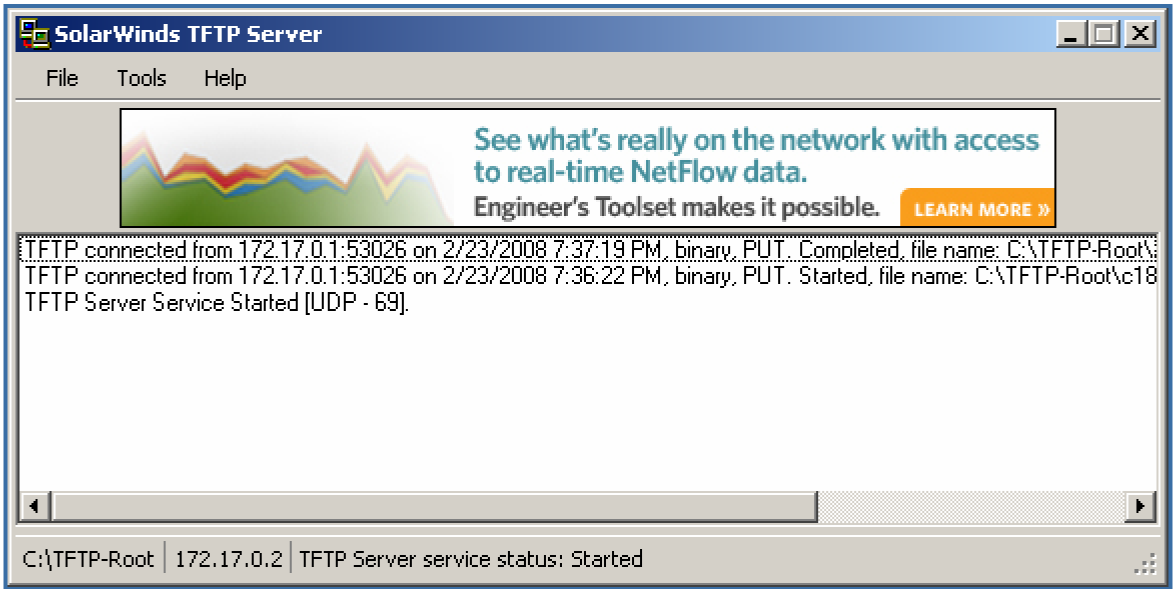
____

b. From the HyperTerminal session on router R1, begin uploading the Cisco IOS image to the TFTP server using the **copy flash tftp** command. Respond to the prompts as shown below, but replace the image filename shown with the one on your router.

```
R1#copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-10b.bin
Address or name of remote host []? 172.17.0.2
Destination filename [c1841-advipservicesk9-mz.124-10b.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
22063220 bytes copied in 58.264 secs (378677 bytes/sec)
```

Step 5: Verify the TFTP server activity.

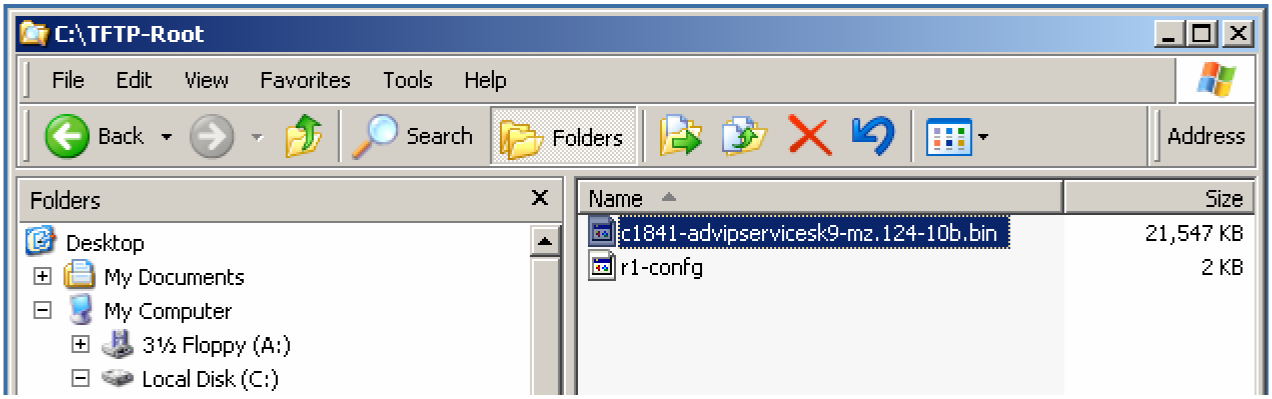
a. Observe the TFTP Server window, which shows the connection entries for the transfer of the running-config file to the server. The output should look similar to the following.


SolarWinds TFTP Server
File
Tools
Help
See what's really on the network with access to real-time NetFlow data.
Engineer's Toolset makes it possible.
LEARN MORE »

```
TFTP connected from 172.17.0.1:53026 on 2/23/2008 7:37:19 PM, binary, PUT, Completed, file name: C:\TFTP-Root\
TFTP connected from 172.17.0.1:53026 on 2/23/2008 7:36:22 PM, binary, PUT, Started, file name: C:\TFTP-Root\c18
TFTP Server Service Started [UDP - 69].
```

C:\TFTP-Root | 172.17.0.2 | TFTP Server service status: Started

b. Use Windows Explorer to examine the contents of folder C:\TFTP-Root\ on the host H1 TFTP server. Verify the flash image size in the TFTP server directory. The file size in the **show flash** command should be the same size as the file stored on the TFTP server. If the file sizes are not identical, check with the instructor. The IOS image file should be listed similar to the one shown in the screen below.



Name	Size
c1841-advipservicesk9-mz.124-10b.bin	21,547 KB
r1-config	2 KB

Task 4: Consider IOS Restoration Options

There are several options for restoring a corrupted or missing Cisco IOS image.

Option 1. Using ROMmon and tftpdnld (part of this lab) – This option can be used if the image is missing or corrupt. The router boots up in ROMmon mode if this is the case. Ethernet and IP connectivity must be available to access the TFTP server.

Option 2. Using ROMmon and xmodem (not part of this lab) – This option is used as an emergency when the Cisco IOS image is missing or corrupt and there is no possibility of downloading a new version from a TFTP server. The **xmodem** command is used at the console to download Cisco IOS software using ROMmon and HyperTerminal. This procedure can also be used if there are no TFTP servers or network connections, and a direct PC connection through the console (or through a modem connection) is the only viable option. Because this procedure relies on the console speed of the router and the serial port of the PC, it can take a long time to download an image. Depending on the image size and the console baud rate, the download can take several hours.

Option 3. Replacing the flash card (not part of this lab) – If the router only boots up in ROMmon mode, you may be able to recover the image if you have a similar router with a compatible flash card. You can download the correct Cisco IOS image on that router, and then move the flash card to the router that has a problem.

Task 5: Working in ROMmon Mode

Step 1: Configure the boot register to enter ROMmon mode.

Typically, if the Cisco IOS software image is corrupt, the router only boots up in ROMmon mode.

You will simulate the loss of the Cisco IOS image by changing the router config-register so that it boots up to the **rommon >** prompt. The config register is normally set to 0x2102 to enable the router to boot the Cisco IOS image from flash. See the **show version** command output in Task 2, Step 1 to see the config-register setting.

a. Change the configuration register to 0x2100 to cause the router to start up in ROMmon mode.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x2100
Router(config)#exit
Router#
```

b. Issue the **show version** command to verify that the new config register setting will take effect at the next reload. What is the last line of the **show version** output?

   ____

c. Issue the **reload** command to restart the router.

```
Router#reload
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 196608 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

Upgrade ROMMON initialized
rommon 1 >
```

Step 2: View available commands from the ROMmon prompt.

Enter a question mark (**?**) at the ROMmon prompt.

```
rommon 2 >?
alias                set and display aliases command
boot                 boot up an external process
break                set/show/clear the breakpoint
confreg              configuration register utility
cont                 continue executing a downloaded image
context              display the context of a loaded image
cookie               display contents of motherboard cookie PROM in hex
dev                  list the device table
dir                  list files in file system
dis                  disassemble instruction stream
dnld                 serial download a program module
frame                print out a selected stack frame
gioshow              show the gio version
help                 monitor builtin command help
history              monitor command history
iomemset             set IO memory percent
meminfo              main memory information
repeat               repeat a monitor command
reset                system reset
rommon-pref          Select ROMMON
set                  display the monitor variables
showmon              display currently selected ROM monitor
stack                produce a stack trace
sync                 write monitor environment to NVRAM
sysret               print out info from last system return
tftpdnld             tftp image download
unalias              unset an alias
unset                unset a monitor variable
xmodem               x/ymodem image download
```

Step 3: Find a valid image in flash.

In some cases, a Cisco IOS image fails to load properly, and the router boots to the ROMmon prompt, but the image may still be valid. There may also be more than one image in flash memory. You can use the **boot** command at the ROMmon prompt to attempt to load a single image, or you can select from multiple images in flash if they exist.

a. From the ROMmon prompt, issue the **dir flash:** command. Look for a valid Cisco IOS software image.

```
rommon 3 > dir flash:
program load complete, entry point: 0x8000f000, size: 0xcb80
Directory of flash:

2       22063220  -rw-     c1841-advipservicesk9-mz.124-10b.bin
5389    491213    -rw-     128MB.sdf
5509    1052160   -rw-     common.tar
5766    833024    -rw-     es.tar
5970    1038      -rw-     home.shtml
5971    4734464   -rw-     sdm.tar
7127    1821      -rw-     sdmconfig-18xx.cfg
7128    1684577   -rw-     securedesktop-ios-3.1.1.27-k9.pkg
7540    398305    -rw-     sslclient-win-1.1.0.154.pkg
rommon 4 >
```

b. Boot from any image that is listed in the previous step (typically files with a .bin extension). If the image is valid, it brings back normal operation.

```
rommon 4 >boot flash:c1841-advipservicesk9-mz.124-10b.bin
program load complete, entry point: 0x8000f000, size: 0x150a6d4
Self decompressing the image :
##########################################################################
########### ...
```

c. Restart the router using the **reload** command. It comes up in ROMmon mode again, because the config register is still set to 0x2100.

Step 4: Reset the config register so that the router boots from flash on the next reload.

From the ROMmon prompt, set the boot register back to 0x2102, before the Cisco IOS image transfer, using the **confreg** command. Depending on the router model and ROMmon prompt, you may need to use the **o/r** command.

Note: The number at the ROMmon prompt increments with each command issued.

```
rommon 5 > confreg 0x2102
or
> o/r 0x2102
```

The router responds with:

```
You must reset or power cycle for new config to take effect
rommon 6 >
```

Note: Do not reset the router at this time.

Task 6: Use ROMmon and tftpdnld to Restore a Cisco IOS Image (Optional)

Important: Check with the instructor before performing Task 6 in this lab. The **tftpdnld** command erases all existing files in flash memory before downloading a new software image to the router. If there are files in the router flash memory that you do not want to lose, they must be backed up to the TFTP server and then copied back to flash memory after the Cisco IOS image has been restored. The process for copying files to and from a TFTP server is described in Lab 8.4.3a, "Managing Cisco IOS Images with TFTP."

Note: If performing this task presents a problem to the lab environment, just read through the steps to become familiar with the procedure.

Step 1: Use the tftpdnld command to transfer the image.

a. Record the name of the Cisco IOS image displayed in the **show flash** output in Task 2, Step 2. This file was saved to the TFTP server.

____

b. The ROMmon TFTP transfer works only on the first LAN port. To use TFTP in ROMmon mode, you must first set a few environmental variables, including the IP address of the LAN interface, and then use the **tftpdnld** command to restore the image. To set a ROMmon environment variable, type the variable name, an equal sign (=), and the value for the variable. For example, to set the IP address to 172.17.0.1, type IP_ADDRESS=172.17.0.1.

Commonly required environment variables are:

IP_ADDRESS – IP address on the LAN interface

IP_SUBNET_MASK – Subnet mask for the LAN interface

DEFAULT_GATEWAY – Default gateway for the LAN interface

TFTP_SERVER – IP address of the TFTP server

TFTP_FILE – Cisco IOS filename on the server

Enter the environment variables as follows (be sure to replace the image name with the one for the router that you are using).

```
rommon 7 > IP_ADDRESS=172.17.0.1
rommon 8 > IP_SUBNET_MASK=255.255.0.0
rommon 9 > DEFAULT_GATEWAY=172.17.0.1
rommon 10 > TFTP_SERVER=172.17.0.2
rommon 11 > TFTP_FILE=c1841-advipservicesk9-mz.124-10b.bin
```

c. Use the **set** command to view and verify the ROMmon environment variables.

```
rommon 12 > set
PS1=rommon ! >
BSI=0
RANDOM_NUM=1770598170
WARM_REBOOT=
RET_2_RTS=18:04:12 UTC Mon Feb 25 2008
RET_2_RCALTS=1203962657
?=0
IP_ADDRESS=172.17.0.1
IP_SUBNET_MASK=255.255.0.0
TFTP_SERVER=172.17.0.2
TFTP_FILE=c1841-advipservicesk9-mz.124-10b.bin
```

d. Use the **tftpdnld** command to start the Cisco IOS image transfer from the TFTP server. As each datagram of the Cisco IOS file is received, an exclamation point (!) is displayed. When the entire Cisco IOS file is copied, the flash is erased and the new image file is written.

```
rommon 13 > tftpdnld

      IP_ADDRESS: 172.17.0.1
  IP_SUBNET_MASK: 255.255.0.0
 DEFAULT_GATEWAY: 172.17.0.1
     TFTP_SERVER: 172.17.0.2
       TFTP_FILE: c1841-advipservicesk9-mz.124-10b.bin
    TFTP_MACADDR: 00:1b:53:25:25:6e
    TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
    TFTP_TIMEOUT: 7200
   TFTP_CHECKSUM: Yes
```

```
       FE_PORT: 0
 FE_SPEED_MODE: Auto Detect

Invoke this command for disaster recovery only.
WARNING: all existing data in all partitions on flash: will be lost!
Do you wish to continue? y/n:  [n]:  y
.
Receiving c1841-advipservicesk9-mz.124-10b.bin from 172.17.0.2
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<output omitted>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!
File reception completed.
Validating checksum.
Copying file c1841-advipservicesk9-mz.124-10b.bin to flash:.
program load complete, entry point: 0x8000f000, size: 0xcb80

Format: Drive communication & 1st Sector Write OK...
Writing Monlib sectors.
.......................................................................
.......................................................................
................................
Monlib write complete

Format: All system sectors written. OK...
Format: Operation completed successfully.

Format of flash: complete
program load complete, entry point: 0x8000f000, size: 0xcb80
```

e. When the ROMmon prompt appears, restart the router using the **reset** command or type the letter **i**. The router should now boot from the new Cisco IOS image in flash.

```
rommon 14 > reset
```

Step 2: Verify that the image file transfer was successful.

a. Restart the router using the **reload** command and observe the startup process to confirm that there were no flash errors. If there are none, the router Cisco IOS software should have started correctly.

b. Verify the new image in flash using the **show flash** command.

```
R1#show flash
-#- --length-- -----date/time------ path
1     22063220 Feb 23 2008 01:25:20 c1841-advipservicesk9-mz.124-10b.bin

41947136 bytes available (22065152 bytes used)
```

c. How many files are in flash memory now? ____________

Task 7: Reflection

What are some advantages and disadvantages to using ROMmon and **tftpdnld** to restore a Cisco IOS image?

____

____

Router Interface Summary Table

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 9.1.1 Organizing CCENT Objectives by OSI Layer

Objectives

- Organize the CCENT objectives by which layer or layers they address.

Background / Preparation

In this lab, you associate the objectives of the CCENT exam with the corresponding OSI model layers. Some objectives fall into more than one category.

Note: The CCENT exam is the same as the ICND1 exam. The ICND1 and ICND2 exams together equal the CCNA exam.

This lab requires a computer with browser and Internet access.

Task 1: Access the CCENT Exam Web Page

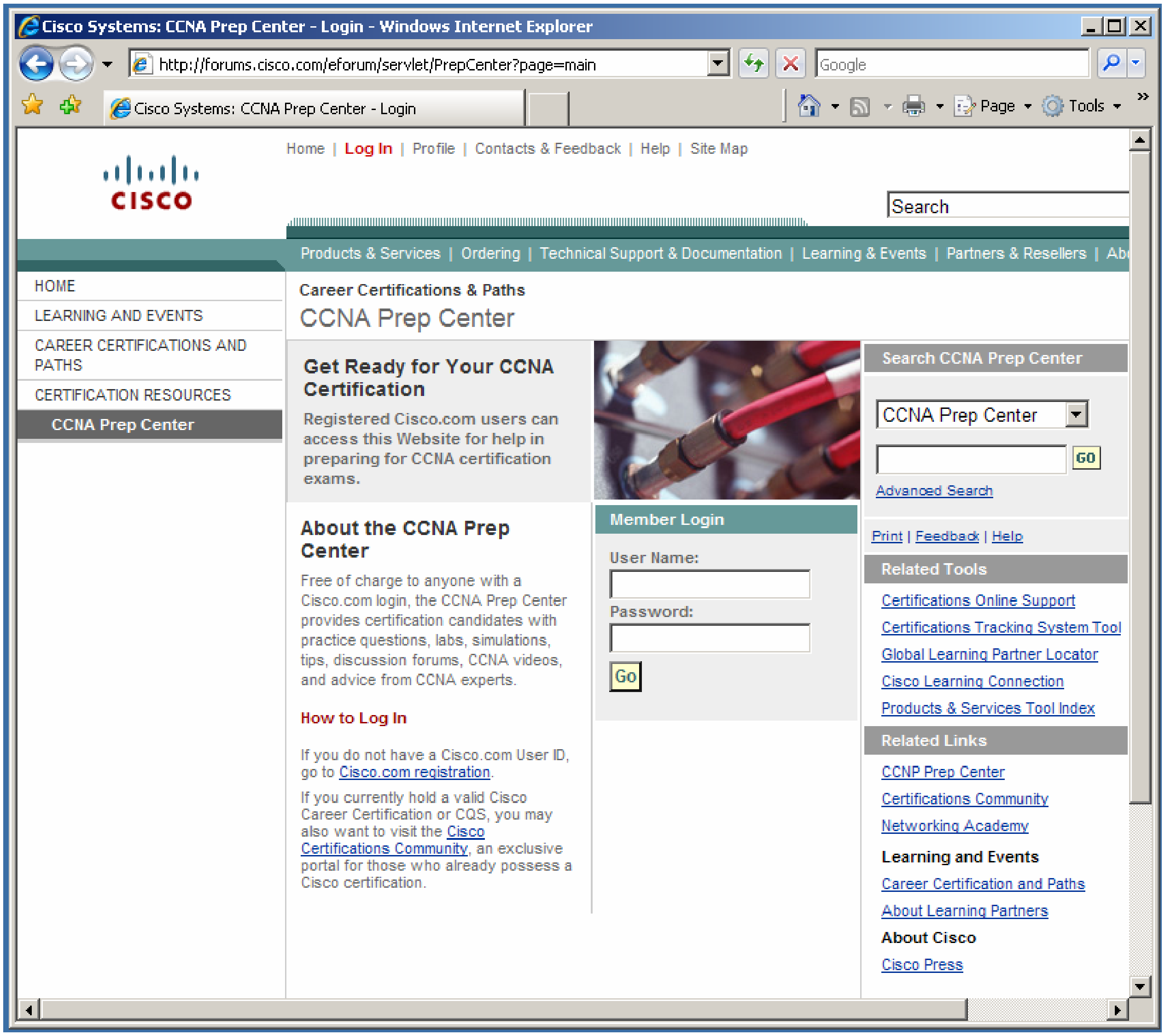
Note: Steps 1 and 2 use the 640-822 ICND1 exam page that is accessed via the CCNA Prep Center website and requires a Cisco.com login account. You can also go directly to the 640-822 ICND1 exam page located at **http://www.cisco.com/web/learning/le3/current_exams/640-822.html**, which does not require a login.

Step 1: Log in to the Cisco CCNA Prep Center website.

Registered Cisco.com users can access this website for help in preparing for CCNA certification exams.

http://forums.cisco.com/eforum/servlet/PrepCenter?page=main

In the **Member Login** area, enter your Cisco.com username and password, and click **Go.** If you do not have a Cisco.com user ID, click on the link for Cisco.com Registration in the **How to Log In** area.


Cisco Systems: CCNA Prep Center - Login - Windows Internet Explorer
http://forums.cisco.com/eforum/servlet/PrepCenter?page=main
Google
Cisco Systems: CCNA Prep Center - Login
Page
Tools
CISCO
Home | Log In | Profile | Contacts & Feedback | Help | Site Map
Search
Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | Ab
HOME
LEARNING AND EVENTS
CAREER CERTIFICATIONS AND PATHS
CERTIFICATION RESOURCES
CCNA Prep Center
Search CCNA Prep Center
CCNA Prep Center
GO
Advanced Search
Member Login
User Name:
Password:
Go
Print | Feedback | Help
Related Tools
Certifications Online Support
Certifications Tracking System Tool
Global Learning Partner Locator
Cisco Learning Connection
Products & Services Tool Index
Related Links
CCNP Prep Center
Certifications Community
Networking Academy
Learning and Events
Career Certification and Paths
About Learning Partners
About Cisco
Cisco Press

Career Certifications & Paths

CCNA Prep Center

Get Ready for Your CCNA Certification

Registered Cisco.com users can access this Website for help in preparing for CCNA certification exams.

About the CCNA Prep Center

Free of charge to anyone with a Cisco.com login, the CCNA Prep Center provides certification candidates with practice questions, labs, simulations, tips, discussion forums, CCNA videos, and advice from CCNA experts.

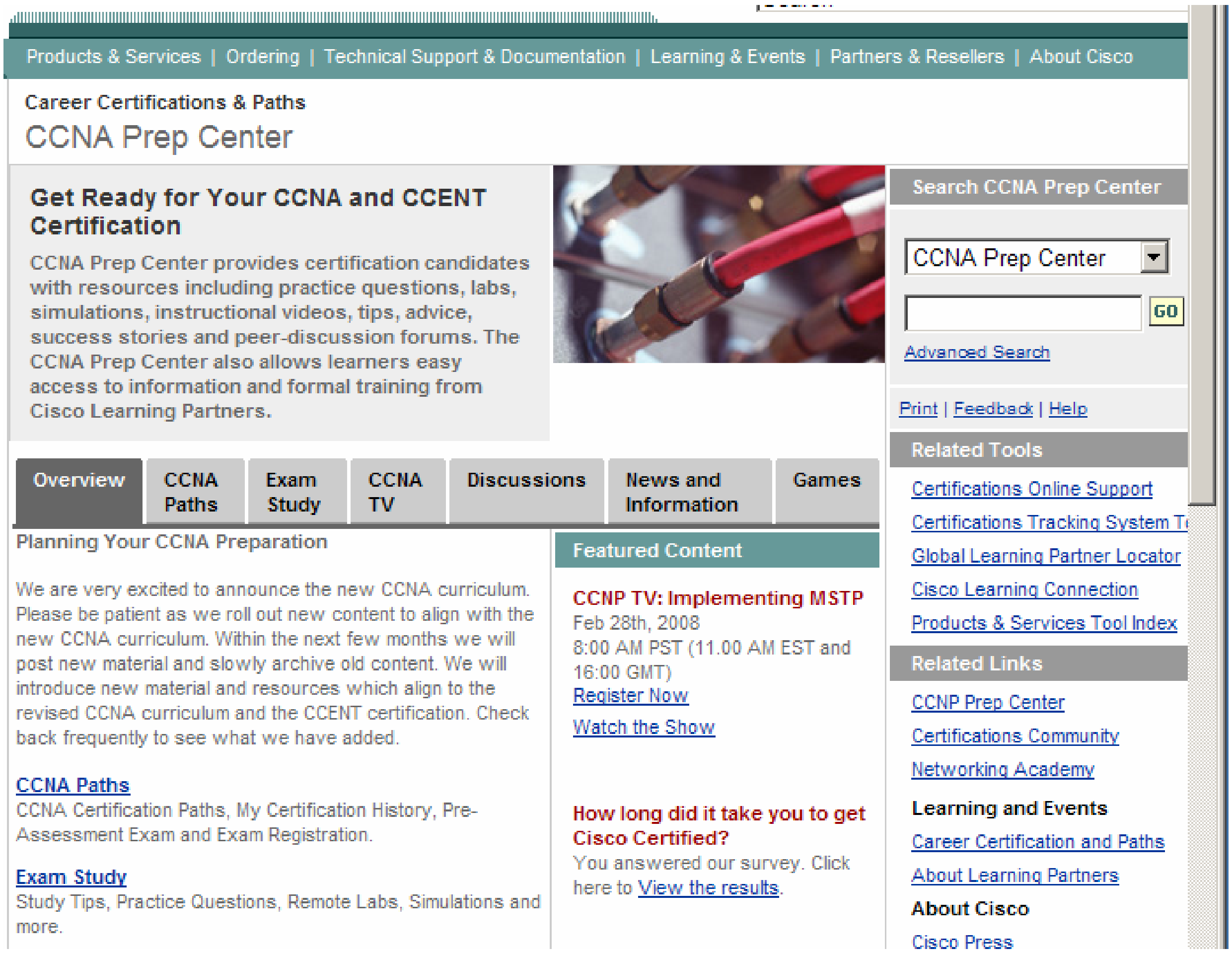
How to Log In

If you do not have a Cisco.com User ID, go to Cisco.com registration.

If you currently hold a valid Cisco Career Certification or CQS, you may also want to visit the Cisco Certifications Community, an exclusive portal for those who already possess a Cisco certification.

Step 2: View the ICND1/CCENT exam description and exam topics.

a. From the **CCNA Prep Center** main screen, click the **CCNA Paths** button.


Products & Services | Ordering | Technical Support & Documentation | Learning & Events | Partners & Resellers | About Cisco
Overview
CCNA Paths
Exam Study
CCNA TV
Discussions
News and Information
Games
CCNA Prep Center
GO

Career Certifications & Paths

CCNA Prep Center

Get Ready for Your CCNA and CCENT Certification

CCNA Prep Center provides certification candidates with resources including practice questions, labs, simulations, instructional videos, tips, advice, success stories and peer-discussion forums. The CCNA Prep Center also allows learners easy access to information and formal training from Cisco Learning Partners.

Search CCNA Prep Center

Advanced Search

Print | Feedback | Help

Related Tools

- Certifications Online Support
- Certifications Tracking System T
- Global Learning Partner Locator
- Cisco Learning Connection
- Products & Services Tool Index

Related Links

- CCNP Prep Center
- Certifications Community
- Networking Academy

Learning and Events

- Career Certification and Paths
- About Learning Partners

About Cisco

- Cisco Press

Planning Your CCNA Preparation

We are very excited to announce the new CCNA curriculum. Please be patient as we roll out new content to align with the new CCNA curriculum. Within the next few months we will post new material and slowly archive old content. We will introduce new material and resources which align to the revised CCNA curriculum and the CCENT certification. Check back frequently to see what we have added.

CCNA Paths

CCNA Certification Paths, My Certification History, Pre-Assessment Exam and Exam Registration.

Exam Study

Study Tips, Practice Questions, Remote Labs, Simulations and more.

Featured Content

CCNP TV: Implementing MSTP

Feb 28th, 2008

8:00 AM PST (11.00 AM EST and 16:00 GMT)

Register Now

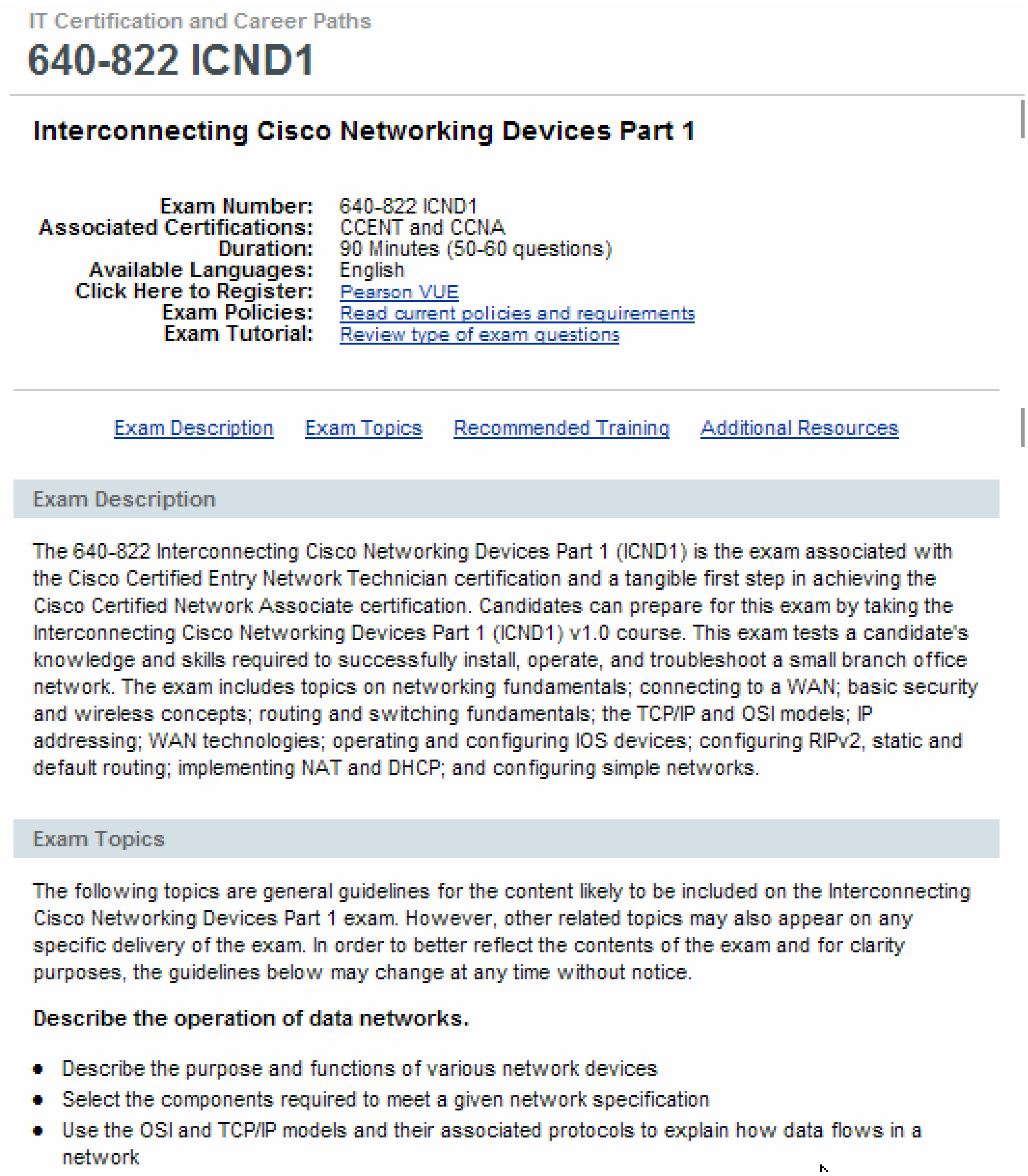
Watch the Show

How long did it take you to get Cisco Certified?

You answered our survey. Click here to View the results.

b. In the next screen, click the **640-822 ICND1** exam link. The **640-822 ICND1** screen appears. It contains a description of the exam and a list of exam topics.

Note: The following screen shot only shows a portion of the exam topics.



IT Certification and Career Paths

640-822 ICND1

Interconnecting Cisco Networking Devices Part 1

Exam Number:	640-822 ICND1
Associated Certifications:	CCENT and CCNA
Duration:	90 Minutes (50-60 questions)
Available Languages:	English
Click Here to Register:	Pearson VUE
Exam Policies:	Read current policies and requirements
Exam Tutorial:	Review type of exam questions

Exam Description

The 640-822 Interconnecting Cisco Networking Devices Part 1 (ICND1) is the exam associated with the Cisco Certified Entry Network Technician certification and a tangible first step in achieving the Cisco Certified Network Associate certification. Candidates can prepare for this exam by taking the Interconnecting Cisco Networking Devices Part 1 (ICND1) v1.0 course. This exam tests a candidate's knowledge and skills required to successfully install, operate, and troubleshoot a small branch office network. The exam includes topics on networking fundamentals; connecting to a WAN; basic security and wireless concepts; routing and switching fundamentals; the TCP/IP and OSI models; IP addressing; WAN technologies; operating and configuring IOS devices; configuring RIPv2, static and default routing; implementing NAT and DHCP; and configuring simple networks.

Exam Topics

The following topics are general guidelines for the content likely to be included on the Interconnecting Cisco Networking Devices Part 1 exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

Describe the operation of data networks.

- Describe the purpose and functions of various network devices
- Select the components required to meet a given network specification
- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

c. What are some of the main topic areas covered?

Task 2: Review the OSI Model Layers

Step 1: Review the OSI model layer names and functions.

In the table below, indicate the name of the OSI layer that is associated with each layer number, and the functions, terminology, and protocols related to each layer.

OSI Model Table

Layer Number	Layer Name	Functions / Terminology	Technologies / Protocols
7			
6			
5			
4			
3			
2			
1			

Step 2: Review the exam topics associated with OSI layers.

The following worksheets address all the exam topics listed on the Cisco.com website for the ICND1/ CCENT exam. Place an X under each layer of the OSI model that most closely relates to the topic or objective. Some objectives may apply to more than one layer.

a. **Describe the operation of data networks.**

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers
Describe the purpose and functions of various network devices					
Select the components required to meet a given network specification					
Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network					
Describe common networking applications including web applications					
Describe the purpose and basic operation of the protocols in the OSI and TCP models					
Describe the impact of applications (Voice Over IP and Video Over IP) on a network					
Interpret network diagrams					
Determine the path between two hosts across a network					
Describe the components required for network and Internet communications					
Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach					
Differentiate between LAN/WAN operation and features					

b. **Implement a small switched network**.

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers

Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts					
Explain the technology and media access control method for Ethernet technologies					
Explain network segmentation and basic traffic management concepts					
Explain the operation of Cisco switches and basic switching concepts					
Perform, save, and verify initial switch configuration tasks, including remote access management					
Verify network status and switch operation using basic utilities, including ping, traceroute, Telnet, SSH, ARP, ipconfig, and show and debug commands					
Implement and verify basic security for a switch (port security, deactivate ports)					
Identify, prescribe, and resolve common switched-network media issues, configuration issues, auto-negotiation, and switch hardware failures					

c. **Implement an IP addressing scheme and IP services to meet network requirements for a small branch office.**

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers
Describe the need and role of addressing in a network; create and apply an addressing scheme to a network					
Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment					
Explain the basic uses and operation of NAT in a small network connecting to one ISP					
Describe and verify DNS operation					
Describe the operation and benefits of using private and public IP addressing					
Enable NAT for a small network with a single ISP and connection using SDM, and verify operation using the CLI and ping					
Configure, verify, and troubleshoot DHCP and DNS operation on a router, using the CLI and SDM					
Implement static and dynamic addressing services for hosts in a LAN environment					
Identify and correct IP addressing issues					

d. **Implement a small routed network.**

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers
Describe basic routing concepts, including packet forwarding and the router lookup process)					
Describe the operation of Cisco routers, including					

the router bootup process, POST, router components					
Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts					
Configure, verify, and troubleshoot RIPv2					
Access and utilize the router CLI to set basic parameters					
Connect, configure, and verify operation status of a device interface					
Verify device configuration and network connectivity using ping, traceroute, Telnet, SSH, and other utilities					
Perform and verify routing configuration tasks for a static or default route given specific routing requirements					
Manage Cisco IOS configuration files, including saving, editing, upgrading, restoring					
Manage the Cisco IOS software					
Implement password and physical security					
Verify network status and router operation using basic utilities, including ping, traceroute, Telnet, SSH, ARP, ipconfig, and show and debug commands					

e. **Explain and select the appropriate administrative tasks required for a WLAN.**

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers
Describe standards associated with wireless media, including IEEE WI-FI Alliance, ITU/FCC					
Identify and describe the purpose of the components in a small wireless network, including SSID, BSS, ESS					
Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point					
Compare and contrast wireless security features and capabilities of WPA security, including open, WEP, WPA-1/2					
Identify common issues when implementing wireless networks					

f. **Identify security threats to a network and describe general methods to mitigate those threats.**

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers
Explain today's increasing network security threats and the need to implement a comprehensive security policy to mitigate the threats					
Explain general methods to mitigate common security threats to network devices, hosts, and applications					
Describe the functions of common security					

appliances and applications					
Describe security recommended practices, including initial steps to secure network devices					

g. **Implement and verify WAN links.**

640-822 CCENT Topic / Objective	Layer 1	Layer 2	Layer 3	Layer 4	Upper Layers
Describe different methods for connecting to a WAN					
Configure and verify a basic WAN serial connection					

Task 3: Reflection

Why is it useful to categorize the exam topics by the OSI layers with which they are associated?

____

____

____

Lab 9.1.3 Using Wireshark to Observe the TCP Three-way Handshake

Objectives

- Use Wireshark to monitor an Ethernet interface for recording packet flows
- Generate a TCP connection using a web browser
- Observe the initial TCP/IP three-way handshake

Background / Preparation

In this lab, you use the Wireshark network packet analyzer (also called a packet sniffer) to view the TCP/IP packets generated by the TCP three-way handshake. When an application that uses TCP first starts on a host, the protocol uses the three-way handshake to establish a reliable TCP connection between two hosts. You will observe the initial packets of the TCP flow: the SYN packet, then the SYN ACK packet, and finally the ACK packet.

Caution: Installing or using a packet sniffer application may be considered a breach of the security policy of an organization, leading to serious legal and financial consequences. It is recommended that permission is obtained before downloading, installing, or running a packet sniffer application.

Note: The term “packet” is used in this lab. Wireshark actually captures Ethernet frames, which contain IP packets. The Wireshark application uses the term “frame” when analyzing captures. The two terms are often used interchangeably, but recall that a frame is a Data Link Layer 2 encapsulation package, and a packet is a Network Layer 3 encapsulation.

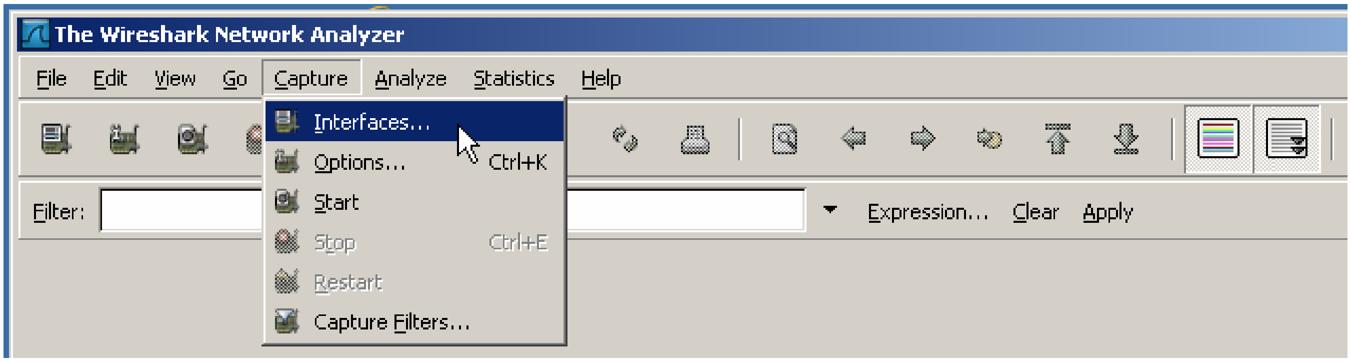
Task 1: Prepare Wireshark to Capture Packets

Step 1: Start Wireshark.

Double-click the Wireshark icon, which is located on the desktop.

Step 2: Select an interface to use for capturing packets.

a. From the Capture menu, choose **Interfaces**.

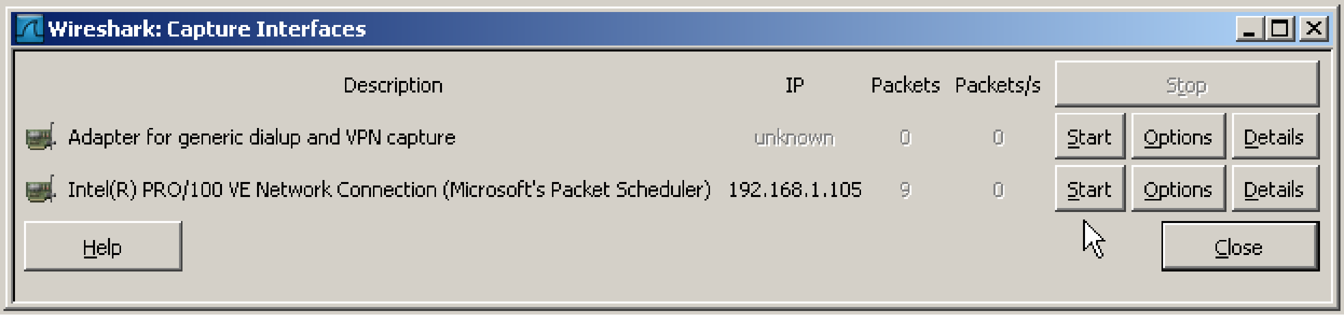


Step 3: Start a network capture.

a. Choose the local network Ethernet interface adapter for capturing network traffic. Click the **Start** button of the chosen interface.

b. Write down the IP address associated with the selected Ethernet adapter, because that is the source IP address to look for when examining captured packets.

The host IP address: ____________________________



Description	IP	Packets	Packets/s			
Adapter for generic dialup and VPN capture	unknown	0	0	Start	Options	Details
Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler)	192.168.1.105	9	0	Start	Options	Details

Task 2: Generate and Analyze Captured Packets

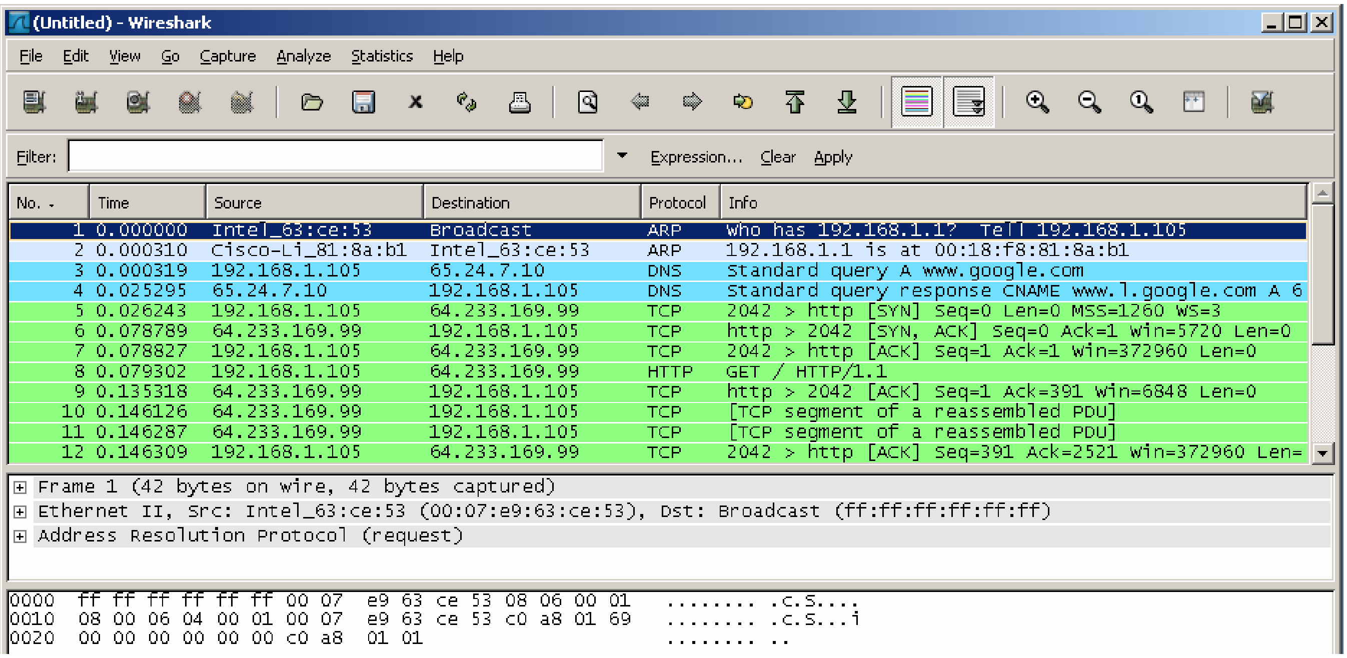
Step 1: Open a browser and access a website.

a. Go to www.google.com. Minimize the Google window, and return to Wireshark. You should see captured traffic similar to that shown below.

Note: Your instructor may provide you with a different website. If so, enter the website name or address here:

____

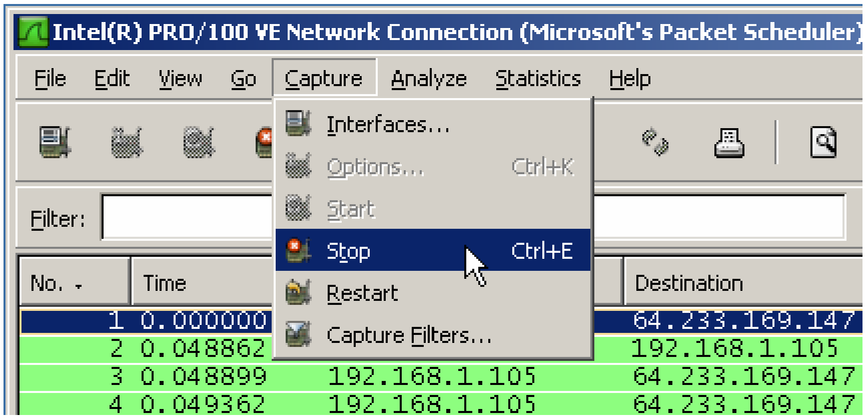
b. The capture windows are now active. Locate the Source, Destination, and Protocol columns on the Wireshark display screen. The HTTP data that carries web page text and graphics uses TCP for reliability.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. - Time      Source             Destination       Protocol Info
   1 0.000000  Intel_63:ce:53     Broadcast         ARP      Who has 192.168.1.1?  Tell 192.168.1.105
   2 0.000310  Cisco-Li_81:8a:b1  Intel_63:ce:53    ARP      192.168.1.1 is at 00:18:f8:81:8a:b1
   3 0.000319  192.168.1.105      65.24.7.10        DNS      Standard query A www.google.com
   4 0.025295  65.24.7.10         192.168.1.105     DNS      Standard query response CNAME www.l.google.com A 6
   5 0.026243  192.168.1.105      64.233.169.99     TCP      2042 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
   6 0.078789  64.233.169.99      192.168.1.105     TCP      http > 2042 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0
   7 0.078827  192.168.1.105      64.233.169.99     TCP      2042 > http [ACK] Seq=1 Ack=1 Win=372960 Len=0
   8 0.079302  192.168.1.105      64.233.169.99     HTTP     GET / HTTP/1.1
   9 0.135318  64.233.169.99      192.168.1.105     TCP      http > 2042 [ACK] Seq=1 Ack=391 Win=6848 Len=0
  10 0.146126  64.233.169.99      192.168.1.105     TCP      [TCP segment of a reassembled PDU]
  11 0.146287  64.233.169.99      192.168.1.105     TCP      [TCP segment of a reassembled PDU]
  12 0.146309  192.168.1.105      64.233.169.99     TCP      2042 > http [ACK] Seq=391 Ack=2521 Win=372960 Len=

⊞ Frame 1 (42 bytes on wire, 42 bytes captured)
⊞ Ethernet II, Src: Intel_63:ce:53 (00:07:e9:63:ce:53), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)

0000  ff ff ff ff ff ff 00 07  e9 63 ce 53 08 06 00 01   ........ .c.S....
0010  08 00 06 04 00 01 00 07  e9 63 ce 53 c0 a8 01 69   ........ .c.S...i
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..
```

Step 2: Stop the capture.

From the Wireshark Capture menu, choose **Stop**.



No.	Time		Destination
1	0.000000		64.233.169.147
2	0.048862		192.168.1.105
3	0.048899	192.168.1.105	64.233.169.147
4	0.049362	192.168.1.105	64.233.169.147

Step 3: Analyze the captured output.

If the computer was recently started and there has been no activity in accessing the Internet, you can see the entire process in the captured output, including ARP, DNS, and the TCP three-way handshake.

The capture screen in Task 2, Step 1 shows all the packets the computer needs to get to a website, starting with the initial ARP for the gateway router interface MAC address. (Your screen capture may vary.)

a. In the screen capture, the process starts with frame 1, which is an ARP broadcast from the source computer to determine the MAC address of the router default gateway. The gateway is the local LAN Fast Ethernet interface on the router. The computer needs to resolve the default gateway IP address to the interface MAC address before it can send the first frame or packet to the router.

What is the IP address of the router default gateway? ____________________

b. The second frame is the reply from the router telling the computer the MAC address of its Fast Ethernet interface.

What is the MAC address? ____________________

c. The third frame is a DNS query from the computer to the configured DNS server, attempting to resolve the domain name www.google.com to the IP address of the web server. The computer must have the IP address before it can send the first frame to the web server.

What is the IP address of the DNS server that the computer queried? ________________________

d. The fourth frame is the response from the DNS server with the IP address of www.google.com. You need to scroll to the right to see the IP address of the Google server in the DNS response, but you can see it in the next frame.

e. The fifth frame is the start of the TCP three-way handshake [SYN].

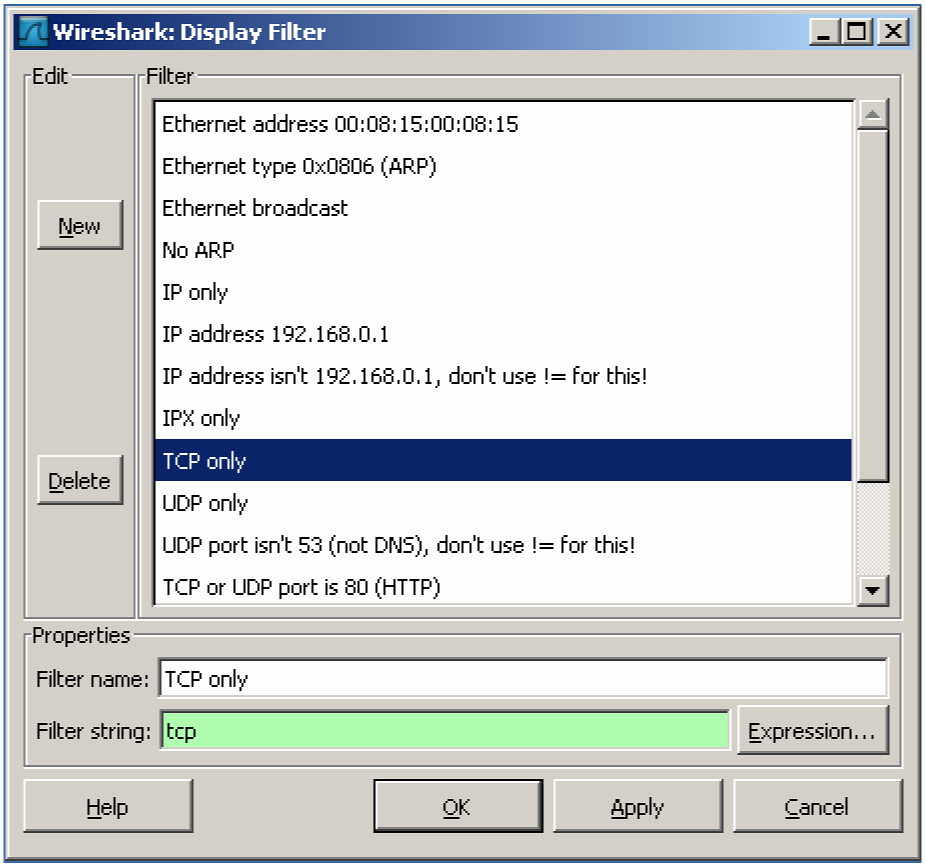
What is the IP address of the Google web server? ________________________

Step 4: Filter the capture to view only TCP packets.

If you have many packets that are unrelated to the TCP connection, it may be necessary to use the Wireshark filter capability.

a. To use a preconfigured filter, click the **Analyze** menu option, and then click **Display Filters**.

b. In the **Display Filter** window, click **TCP only**, and then click **OK**.

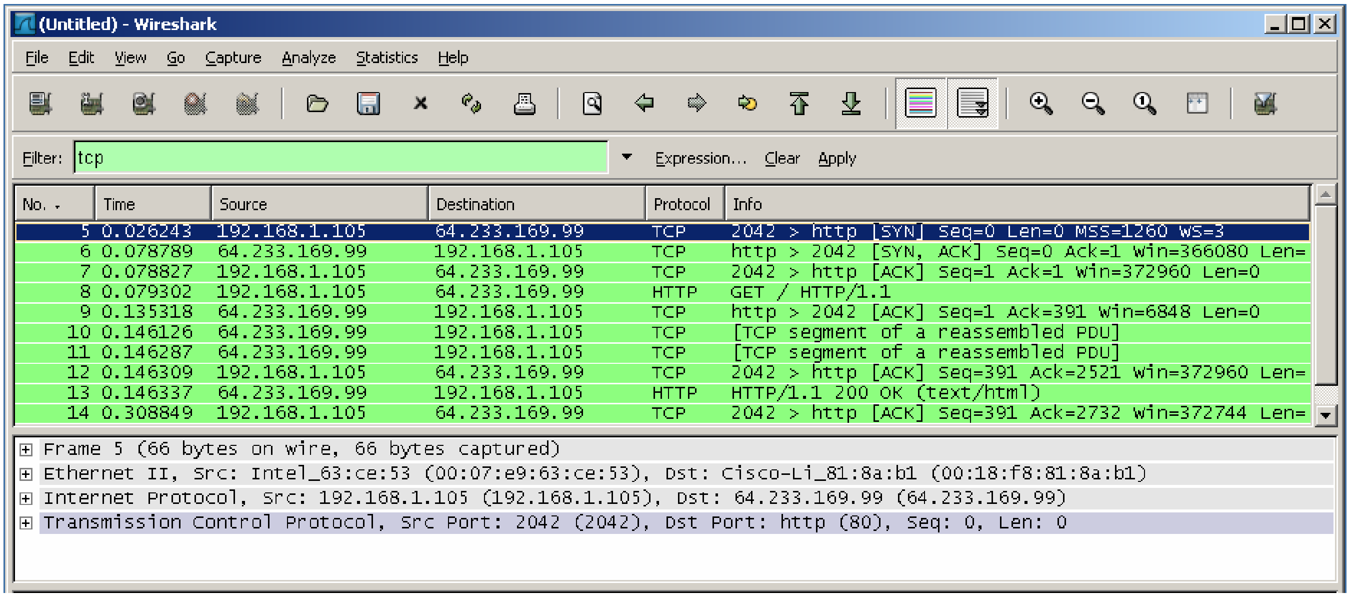


Ethernet address 00:08:15:00:08:15
Ethernet type 0x0806 (ARP)
Ethernet broadcast
No ARP
IP only
IP address 192.168.0.1
IP address isn't 192.168.0.1, don't use != for this!
IPX only
TCP only
UDP only
UDP port isn't 53 (not DNS), don't use != for this!
TCP or UDP port is 80 (HTTP)

Filter name: TCP only

Filter string: tcp

c. In the Wireshark window, scroll to the first captured TCP packet. This should be the first packet in the flow.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Expression... Clear Apply

Filter: tcp

```
No. .  Time      Source          Destination     Protocol Info
     5 0.026243  192.168.1.105   64.233.169.99   TCP      2042 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
     6 0.078789  64.233.169.99   192.168.1.105   TCP      http > 2042 [SYN, ACK] Seq=0 Ack=1 Win=366080 Len=
     7 0.078827  192.168.1.105   64.233.169.99   TCP      2042 > http [ACK] Seq=1 Ack=1 Win=372960 Len=0
     8 0.079302  192.168.1.105   64.233.169.99   HTTP     GET / HTTP/1.1
     9 0.135318  64.233.169.99   192.168.1.105   TCP      http > 2042 [ACK] Seq=1 Ack=391 Win=6848 Len=0
    10 0.146126  64.233.169.99   192.168.1.105   TCP      [TCP segment of a reassembled PDU]
    11 0.146287  64.233.169.99   192.168.1.105   TCP      [TCP segment of a reassembled PDU]
    12 0.146309  192.168.1.105   64.233.169.99   TCP      2042 > http [ACK] Seq=391 Ack=2521 Win=372960 Len=
    13 0.146337  64.233.169.99   192.168.1.105   HTTP     HTTP/1.1 200 OK (text/html)
    14 0.308849  192.168.1.105   64.233.169.99   TCP      2042 > http [ACK] Seq=391 Ack=2732 Win=372744 Len=
```

```
⊞ Frame 5 (66 bytes on wire, 66 bytes captured)
⊞ Ethernet II, Src: Intel_63:ce:53 (00:07:e9:63:ce:53), Dst: Cisco-Li_81:8a:b1 (00:18:f8:81:8a:b1)
⊞ Internet Protocol, Src: 192.168.1.105 (192.168.1.105), Dst: 64.233.169.99 (64.233.169.99)
⊞ Transmission Control Protocol, Src Port: 2042 (2042), Dst Port: http (80), Seq: 0, Len: 0
```

d. In the Info column, look for three packets similar to the first three shown in the window above. The first TCP packet is the [SYN] packet from the initiating computer. The second is the [SYN, ACK] response from the web server. The third packet is the [ACK] from the source computer, which completes the handshake.

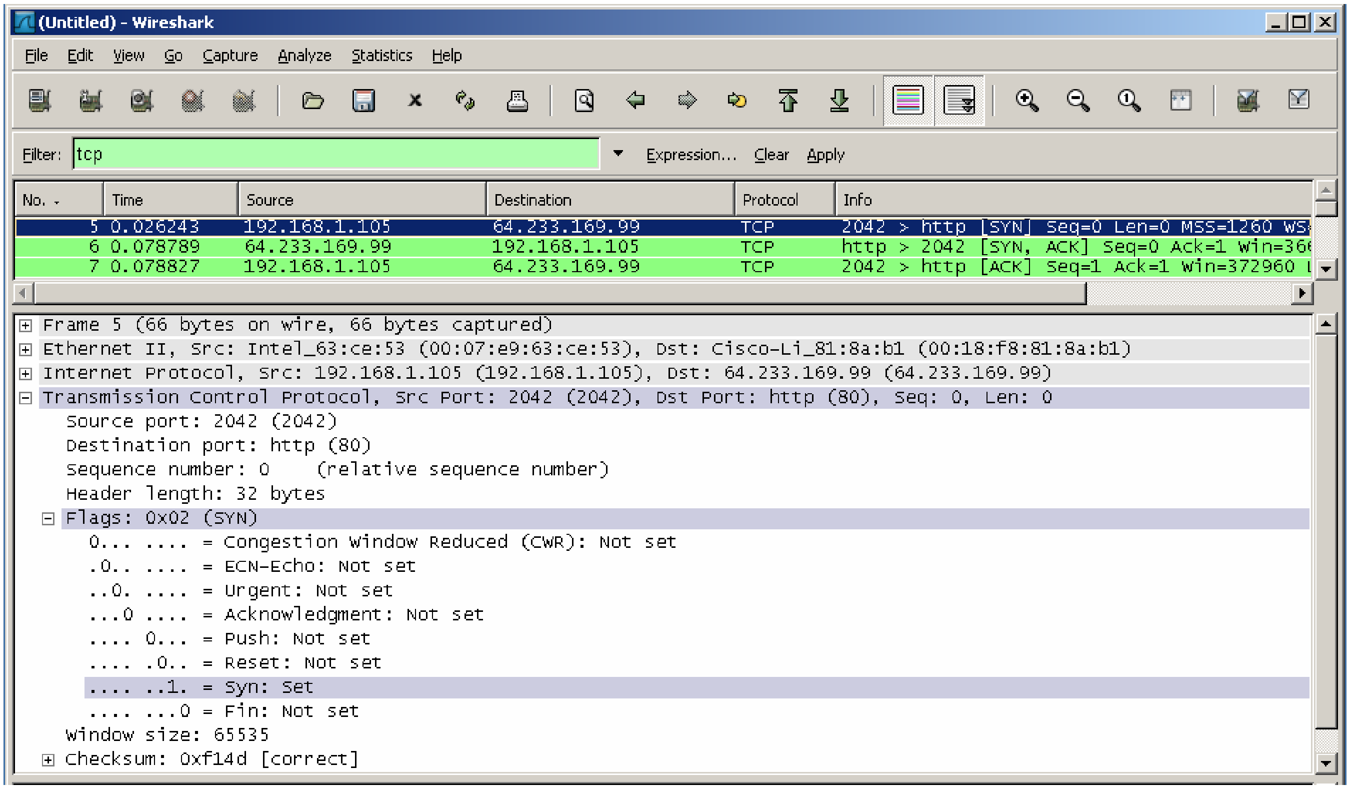
Step 5: Inspect the TCP initialization Sequence

a. In the top Wireshark window, click on the line containing the first packet identified in Step 4. This highlights the line and displays the decoded information from that packet in the two lower windows fill.

Note: The Wireshark windows below were adjusted to allow the information to be viewed in a compact size. The middle window contains the detailed decoding of the packet.

b. Click the **+** icon to expand the view of the TCP information. To contract the view, click the **–** icon.

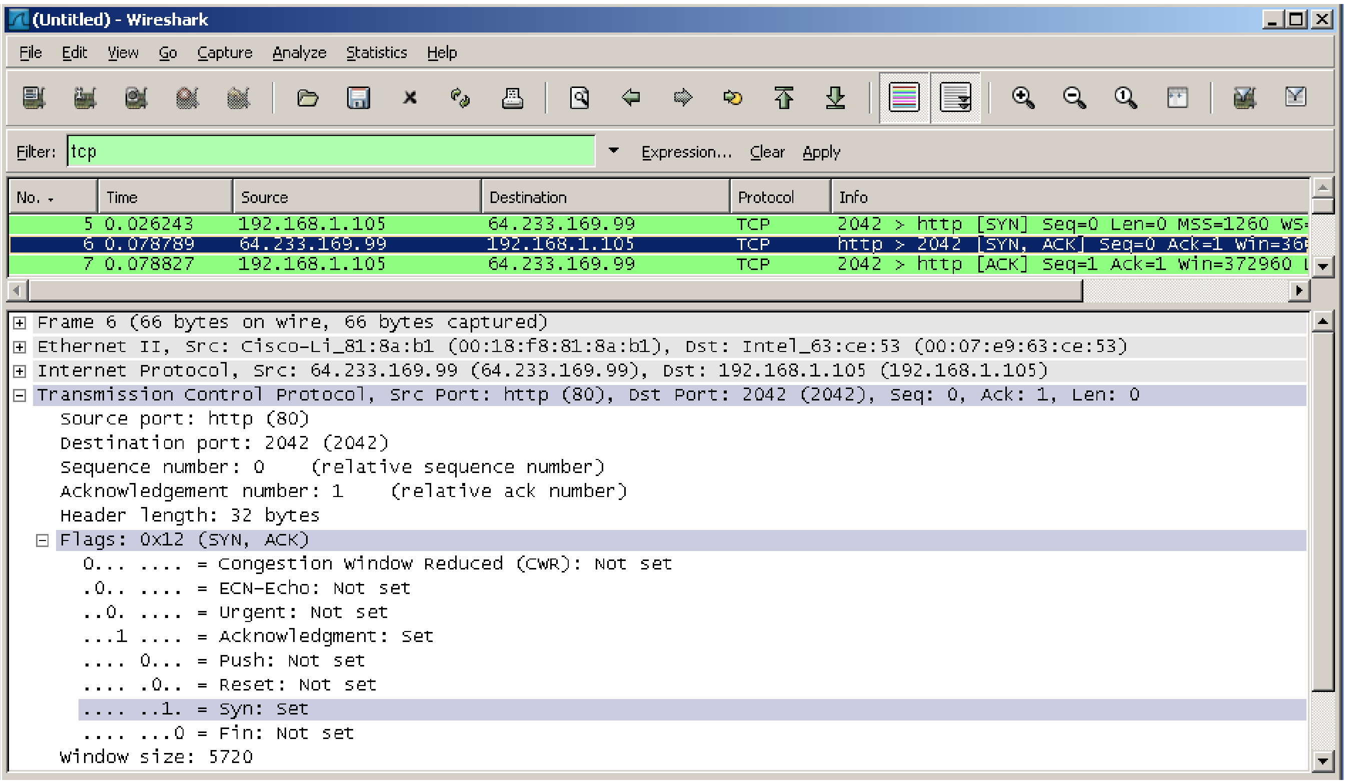
c. Notice in the first TCP packet that the relative sequence number is set to 0, and the SYN bit is set to 1 in the Flags field.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: tcp
Expression... Clear Apply

```
No. -  Time        Source          Destination     Protocol  Info
  5 0.026243    192.168.1.105   64.233.169.99   TCP       2042 > http [SYN] Seq=0 Len=0 MSS=1260 WS
  6 0.078789    64.233.169.99   192.168.1.105   TCP       http > 2042 [SYN, ACK] Seq=0 Ack=1 Win=36
  7 0.078827    192.168.1.105   64.233.169.99   TCP       2042 > http [ACK] Seq=1 Ack=1 Win=372960 L
```

```
⊞ Frame 5 (66 bytes on wire, 66 bytes captured)
⊞ Ethernet II, Src: Intel_63:ce:53 (00:07:e9:63:ce:53), Dst: Cisco-Li_81:8a:b1 (00:18:f8:81:8a:b1)
⊞ Internet Protocol, Src: 192.168.1.105 (192.168.1.105), Dst: 64.233.169.99 (64.233.169.99)
⊟ Transmission Control Protocol, Src Port: 2042 (2042), Dst Port: http (80), Seq: 0, Len: 0
    Source port: 2042 (2042)
    Destination port: http (80)
    Sequence number: 0    (relative sequence number)
    Header length: 32 bytes
  ⊟ Flags: 0x02 (SYN)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 65535
  ⊞ Checksum: 0xf14d [correct]
```

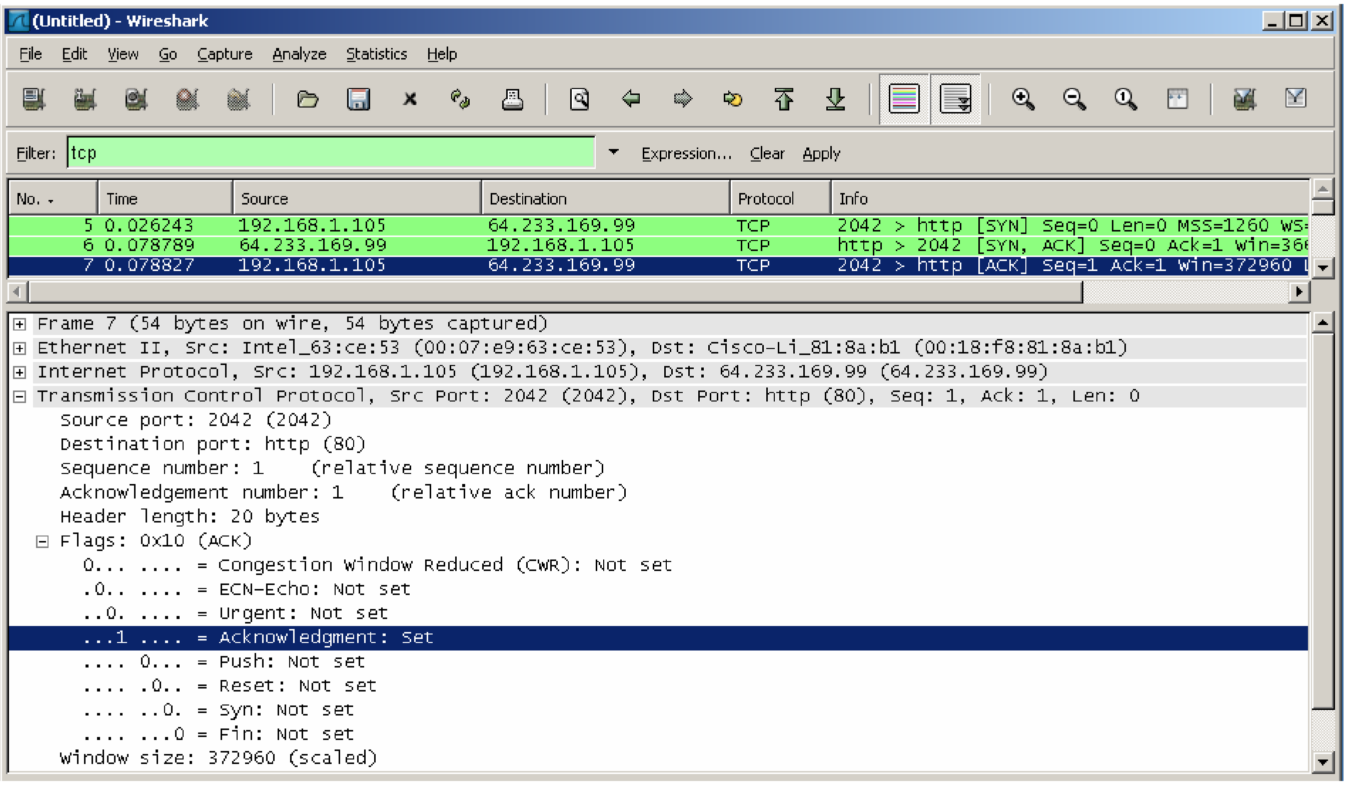
d. Notice in the second TCP packet of the handshake that the relative sequence number is set to 0, and the SYN bit and the ACK bit are set to 1 in the Flags field.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: tcp
Expression... Clear Apply

```
No. -  Time        Source           Destination     Protocol  Info
   5 0.026243     192.168.1.105    64.233.169.99   TCP       2042 > http [SYN] Seq=0 Len=0 MSS=1260 WS=
   6 0.078789     64.233.169.99    192.168.1.105   TCP       http > 2042 [SYN, ACK] Seq=0 Ack=1 Win=36
   7 0.078827     192.168.1.105    64.233.169.99   TCP       2042 > http [ACK] Seq=1 Ack=1 Win=372960 L
```

```
⊞ Frame 6 (66 bytes on wire, 66 bytes captured)
⊞ Ethernet II, Src: Cisco-Li_81:8a:b1 (00:18:f8:81:8a:b1), Dst: Intel_63:ce:53 (00:07:e9:63:ce:53)
⊞ Internet Protocol, Src: 64.233.169.99 (64.233.169.99), Dst: 192.168.1.105 (192.168.1.105)
⊟ Transmission Control Protocol, Src Port: http (80), Dst Port: 2042 (2042), Seq: 0, Ack: 1, Len: 0
    Source port: http (80)
    Destination port: 2042 (2042)
    Sequence number: 0    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 32 bytes
  ⊟ Flags: 0x12 (SYN, ACK)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...1 .... = Acknowledgment: Set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 5720
```

e. In the third and final frame of the handshake, only the ACK bit is set, and the sequence number is set to the starting point of 1. The acknowledgement number is also set to 1 as a starting point. The TCP connection is now established, and communication between the source computer and the web server can begin.


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: tcp
Expression... Clear Apply

```
No. -  Time        Source           Destination     Protocol  Info
   5 0.026243     192.168.1.105    64.233.169.99   TCP       2042 > http [SYN] Seq=0 Len=0 MSS=1260 WS=
   6 0.078789     64.233.169.99    192.168.1.105   TCP       http > 2042 [SYN, ACK] Seq=0 Ack=1 Win=36
   7 0.078827     192.168.1.105    64.233.169.99   TCP       2042 > http [ACK] Seq=1 Ack=1 Win=372960 L
```

```
⊞ Frame 7 (54 bytes on wire, 54 bytes captured)
⊞ Ethernet II, Src: Intel_63:ce:53 (00:07:e9:63:ce:53), Dst: Cisco-Li_81:8a:b1 (00:18:f8:81:8a:b1)
⊞ Internet Protocol, Src: 192.168.1.105 (192.168.1.105), Dst: 64.233.169.99 (64.233.169.99)
⊟ Transmission Control Protocol, Src Port: 2042 (2042), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0
    Source port: 2042 (2042)
    Destination port: http (80)
    Sequence number: 1    (relative sequence number)
    Acknowledgement number: 1    (relative ack number)
    Header length: 20 bytes
  ⊟ Flags: 0x10 (ACK)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...1 .... = Acknowledgment: Set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..0. = Syn: Not set
      .... ...0 = Fin: Not set
    Window size: 372960 (scaled)
```

f. Close Wireshark.

Task 3: Reflection

a. There are hundreds of filters available in Wireshark. A large network could have numerous filters and many different types of traffic. Which three filters in the list might be the most useful to a network administrator?

____

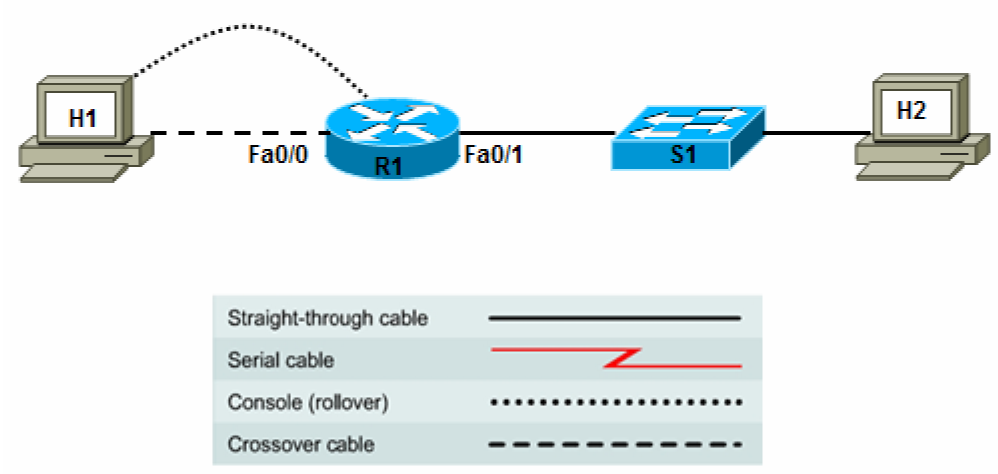
b. Is Wireshark a tool for out-of-band or in-band network monitoring? ______________

Explain your answer.

____

____

Lab 9.2.3 Identifying Cabling and Media Errors



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	R1	Fa0/0	192.168.1.1	255.255.255.0	N/A	N/A
		Fa0/1	192.168.2.1	255.255.255.0	N/A	Fa0/1
S1	S1	VLAN 1	192.168.2.99	255.255.255.0	192.168.2.1	N/A
H1	H1	NIC	192.168.1.11	255.255.255.0	192.168.1.1	N/A
H2	H2	NIC	192.168.2.22	255.255.255.0	192.168.2.1	Fa0/2

Objectives

- Identify Ethernet device and cabling connectivity.
- Build a simple, routed multi-LAN network and verify connectivity.
- Use the **show interfaces** and **show ip interface** Cisco IOS commands to observe the symptoms when using the wrong cable.

Background / Preparation

In this lab, you build a simple, multi-LAN routed Ethernet network using different types of cables to connect hosts and networking devices, while observing symptoms of connectivity problems.

Common cable or media issues that can cause connectivity problems include:

- Loose cable or too much tension on the cable – If all the pins cannot make a good connection, the circuit is down.
- Incorrect termination – Ensure that the correct standard is followed, and that all pins are correctly terminated in the connector.
- Damaged serial interface connector – Pins on the interface connection are bent or missing.
- Break or short in the cable – If there are problems along the circuit, the interface cannot sense the correct signals.

- Incorrect cable used – Interchanging straight-through, crossover, and rollover cables can produce unpredictable results and cause lack of connectivity.

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One 1841 router or other router with two Fast Ethernet interfaces
- One 2960 switch or comparable switch with Fast Ethernet interfaces
- Two Windows XP computers
- Two straight-through Category 5 Ethernet cables
- One crossover Category 5 Ethernet cable
- One RJ-45 rollover console cable
- Access to the command prompts for each host
- Access to the network TCP/IP configuration host

From a host computer, start a HyperTerminal session to the router and switch.

Note: Make sure that the routers and switches have been erased and have no startup configurations. Instructions for erasing the switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Review Ethernet Device Cabling

Step 1: Complete the Ethernet device interconnection table.

Enter the type of cable required to interconnect the devices listed. Use C for crossover and S for straight-through.

	Hub	**Switch**	**Router**	**Workstation**
Hub				
Switch				
Router				
Workstation				

Step 2: Analyze the cabling requirements for this lab.

a. What cable type is needed to connect host H1 to router R1, and why?

____

b. What cable type is needed to connect host H1, H2, and router R1 to switch S1, and why?

____

Task 2: Build the Network and Configure Devices

Step 1: Configure basic information on the router and switch.

a. Build and configure the network according to the topology diagram and device configuration table. Configure basic settings on R1. If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

b. Configure the basic settings on S1 to include the host name, passwords, and VLAN 1 IP address. If necessary, see Lab 5.5.4, “Configuring the Cisco 2960 Switch,” for instructions on configuring the switch settings.

c. Save the running configuration on R1 and S1 using the **copy running-config startup-config** command from privileged EXEC mode.

Step 2: Configure the hosts.

Configure H1 and H2 with an IP address, subnet mask, and default gateway, according to the device configuration table.

Task 3: Verify Cabling and Interface Link LEDs

Step 1: Visually inspect the network connections.

a. After cabling the network devices, verify the connections. Attention to detail now minimizes the time required to troubleshoot network connectivity issues later.

b. Are all cables and terminations in good condition? ___________

Step 2: Visually inspect the interface link LEDs.

a. What is the color of the link light for the switch port that H2 is attached to? ____________

b. What is the color of the link light on the H1 NIC? __________________________________

Task 4: Verify Interface Status and Connectivity

Step 1: Verify interface status using the show ip interface brief command.

a. From the HyperTerminal session on R1, use the **show ip interface brief** command to view a summary of the device interfaces. This command may be abbreviated to **sh ip int br**.

```
R1#show ip interface brief
Interface        IP-Address    OK? Method Status                Protocol
FastEthernet0/0  192.168.1.1   YES manual up                     up

FastEthernet0/1  192.168.2.1   YES manual up                     up

Serial0/0/0      unassigned    YES NVRAM  administratively down down

Serial0/0/1      unassigned    YES NVRAM  administratively down down

Vlan1            unassigned    YES NVRAM  up                     down
```

b. What is the interface and protocol status of Fast Ethernet 0/0 and 0/1? ____________

c. What does Status in column 4 show with regard to cabling and keepalives?

____

d. What does Protocol in column 5 refer to?

e. Why is the status for Serial0/0/0 shown as administratively down?

f. On router R1, enable the Serial0/0/0 interface using the **no shutdown** command.

```
R1(config)#interface s0/0/0
R1(config-if)#no shutdown
*Mar 1 16:00:02.707: %LINK-3-UPDOWN: Interface Serial0/0/0, changed state to down
```

g. Issue the **show ip interface brief** command again. What is the status for Serial0/0/0 now, and why?

```
R1#show ip interface brief
Interface        IP-Address    OK? Method Status                Protocol
FastEthernet0/0  192.168.1.1   YES manual up                     up

FastEthernet0/1  192.168.2.1   YES manual up                     up

Serial0/0/0      unassigned    YES NVRAM  down                   down

Serial0/0/1      unassigned    YES NVRAM  administratively down down

Vlan1            unassigned    YES NVRAM  up                     down
```

h. Why is the protocol down for the Serial0/0/0 interface?

Step 2: Verify Fast Ethernet interface status using the show interfaces command.

a. On R1, use the **show interfaces** command to view detailed information for interface Fast Ethernet 0/0.

```
R1#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256e (bia 001b.5325.256e)
  Description: LAN 192.168.1.0/24 Default Gateway
  Internet address is 192.168.1.1/24
  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)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:50, output 00:00:07, 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
     142 packets input, 20117 bytes
     Received 135 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
     693 packets output, 70950 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

b. What is the status and line protocol of this interface?

c. What is the reliability of this interface?

d. What is the encapsulation of this interface?

e. What are the duplex and speed settings of this interface?

f. Are there any runts, giants, input errors, CRC errors, output errors, collisions, or interface resets?

g. On R1, use the **show interfaces** command to view detailed information for interface Fast Ethernet 0/1.

```
R1#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up
  Hardware is Gt96k FE, address is 001b.5325.256f (bia 001b.5325.256f)
  Description: LAN 192.168.2.0/24 Default Gateway
  Internet address is 192.168.2.1/24
  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)
  Full-duplex, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:03, 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, 1 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5659 packets input, 536086 bytes
     Received 5642 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
     775 packets output, 68357 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

h. Are there any runts, giants, input errors, CRC errors, output errors, collisions, or interface resets?

____

Step 3: Verify connectivity.

a. On host H1, open a Command Prompt window by selecting **Start > Run** and typing **cmd**. Alternatively, you can select **Start > All programs > Accessories > Command Prompt**.

b. Ping from H1 to the R1 LAN default gateway.

```
C:\>ping 192.168.1.1
```

c. Use the **ping** command to test end-to-end connectivity. Ping from host H1 on the R1 192.168.1.0/24 LAN to host H2 on the R1 192.168.2.0/24 LAN.

```
C:\>ping 192.168.2.22
```

d. Were the pings successful? ________

Note: If the pings are not successful, troubleshoot the router and host configurations and connections.

Task 5: Observe the Effects of Using Different Cables

Note: The results of this task depend on the type of NIC on the host. If it is a newer NIC, it may be able to auto-detect the transmit (TX) and receive (RX) pairs and adjust accordingly. If this is the case, regardless of whether a straight-through or crossover cable is used, the link lights remain lit on the Fa0/0 interface, and the NIC and the **show ip interface brief** command shows up/up after a brief adjustment period.

Step 1: Change the cable from host H1 to router R1.

Replace the crossover cable from H1 to the R1 Fa0/0 interface with a straight-through cable.

Step 2: Visually inspect the interface link LEDs.

a. What is the color of the link light on the R1 interface Fa0/0 that host H1 is attached to? __________

b. What is the color of the link light on the host H1 NIC? __________________________________

Step 3: Verify interface status.

a. From the HyperTerminal session on R1, use the **show ip interface brief** command to view a summary of the device interfaces.

```
R1#show ip interface brief
Interface        IP-Address    OK? Method Status               Protocol
FastEthernet0/0  192.168.1.1   YES manual up                    down

FastEthernet0/1  192.168.2.1   YES manual up                    up

Serial0/0/0      unassigned    YES NVRAM  down                  down

Serial0/0/1      unassigned    YES NVRAM  administratively down down

Vlan1            unassigned    YES NVRAM  up                    down
```

b. What is the interface and protocol status of Fast Ethernet 0/0 and 0/1? ____________

c. On R1, use the **show interfaces fastethernet 0/0** command to view detailed information for each router Fast Ethernet interface.

```
R1#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is down
  Hardware is Gt96k FE, address is 001b.5325.256e (bia 001b.5325.256e)
  Description: LAN 192.168.1.0/24 Default Gateway
  Internet address is 192.168.1.1/24
  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, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:12:15, output 00:12:19, 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
     348 packets input, 42237 bytes
     Received 327 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
     1022 packets output, 101376 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

d. Are there any runts, giants, input errors, CRC errors, output errors, collisions, or interface resets?

____

Step 4: Change the cable again from host H1 to router R1.

Replace the cable from H1 to the R1 Fa0/0 interface with a rollover cable.

Step 5: Visually inspect the interface link LEDs.

a. What is the color of the link light on the R1 interface Fa0/0 that host H1 is attached to? __________

b. What is the color of the link light on the host H1 NIC? ________________________________

Step 6: Verify interface status.

a. View a summary of the device interfaces.

```
R1#show ip interface brief
Interface        IP-Address    OK? Method Status               Protocol
FastEthernet0/0  192.168.1.1   YES manual up                    down

FastEthernet0/1  192.168.2.1   YES manual up                    up

Serial0/0/0      unassigned    YES NVRAM  down                  down

Serial0/0/1      unassigned    YES NVRAM  administratively down down

Vlan1            unassigned    YES NVRAM  up                    down
```

b. What is the interface and protocol status of Fast Ethernet 0/0 and 0/1? ____________________

c. View detailed information for each router Fast Ethernet interface.

```
R1#show interfaces fastEthernet 0/0
FastEthernet0/0 is up, line protocol is down
  Hardware is Gt96k FE, address is 001b.5325.256e (bia 001b.5325.256e)
  Description: LAN 192.168.1.0/24 Default Gateway
  Internet address is 192.168.1.1/24
  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, 100Mb/s, 100BaseTX/FX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:12:15, output 00:12:19, 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
     348 packets input, 42237 bytes
     Received 327 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
     1022 packets output, 101376 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

d. Are there any runts, giants, input errors, CRC errors, output errors, collisions, or interface resets?

____

Step 7: Change the cable from host H2 to switch S1.

Replace the straight-through cable from host H2 to the switch S1 Fa0/2 interface with a crossover cable.

Step 8: Visually inspect the interface link LEDs.

a. What is the color of the link light on the S1 interface Fa0/2 that host H2 is attached to? __________

b. What is the color of the link light on the host H2 NIC? ________________________________

Step 9: Verify interface status.

a. From the HyperTerminal session on S1, use the **show ip interface brief** to view a summary of the device interfaces.

```
S1#show ip interface brief
Interface          IP-Address      OK? Method Status          Protocol

Vlan1              192.168.2.99    YES NVRAM  up                up

FastEthernet0/1    unassigned      YES unset  up                up

FastEthernet0/2    unassigned      YES unset  down              down
```

b. What is the interface and protocol status of FastEthernet 0/1 and 0/2? ____________

Note: Depending on the switch model and NIC, the LED may be green and the interface may show as up/up. Some switch ports and NICs will automatically adjust to either a straight-through or crossover.

c. On switch S1, use the **show interfaces fastethernet 0/0** to view detailed information for that interface.

```
S1#show interface f0/2
FastEthernet0/24 is down, line protocol is down (notconnect)
  Hardware is Fast Ethernet, address is 001d.4635.0c98 (bia
001d.4635.0c98)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, 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, 0 no buffer
     Received 0 broadcasts (0 multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

Task 7: Reflection

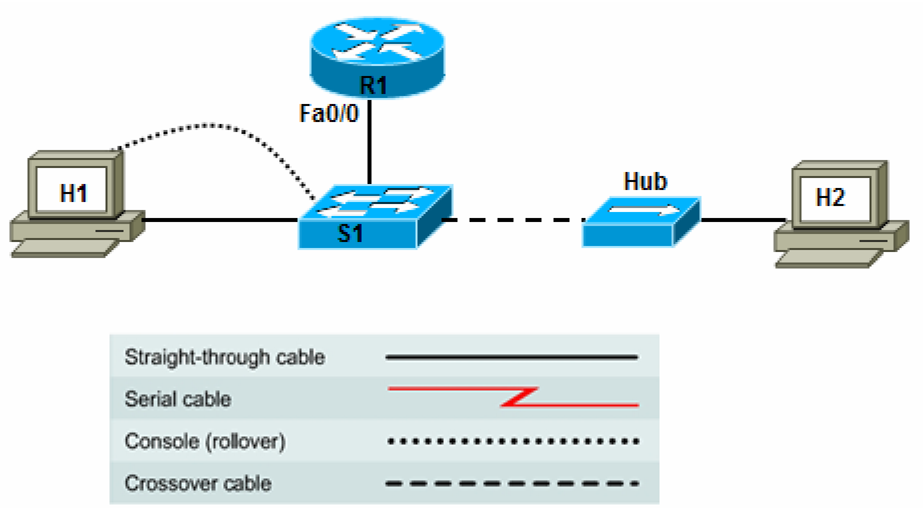
The note in Task 5 indicated that a modern NIC may be able to sense whether the cable is a straight-through or crossover and adjust accordingly. Why would a NIC not be able to adjust when a rollover cable was used instead of a straight-through or crossover?

____

____

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in the parenthesis is the legal abbreviation that is used in Cisco IOS commands to represent the interface.				

Lab 9.2.4 Troubleshooting LAN Connectivity



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	R1	Fast Ethernet 0/0	192.168.1.1	255.255.255.0	N/A	Fast Ethernet 0/2
S1	S1	VLAN 1	192.168.1.99	255.255.255.0	192.168.1.1	N/A
H1	H1	NIC	192.168.1.11	255.255.255.0	192.168.1.1	Fast Ethernet 0/1
H2	H2	NIC	192.168.1.22	255.255.255.0	192.168.1.1	N/A
Hub	Hub	1	N/A	N/A	N/A	Fast Ethernet 0/3

Objectives:

- Build a simple, switched network and verify connectivity.
- Troubleshoot LAN connectivity using the LEDs and **show** commands to find link problems and duplex and speed mismatches.

Background / Preparation

LAN troubleshooting usually centers on switches, because the majority of LAN users connect to the network via switch ports. Duplex and speed mismatches are more common on switches than on routers. Many devices are set to auto-negotiate speed and duplex settings. If one device on a link is configured to auto-negotiate and the other side is manually configured with speed and duplex settings, mismatches may occur, leading to collisions and dropped packets.

In this lab, you build a small, switched network with a router and a hub, in addition to workstations. You will alter the speed and duplex settings of device interfaces and observe the effects on link lights and interface status.

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, or 2600 routers, or a combination of these—can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router and switch, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One 1841 router or other router with a Fast Ethernet interface
- One 2960 switch or comparable switch with Fast Ethernet interfaces
- One hub with Ethernet interfaces
- Two Windows XP computers
- Three straight-through Category 5 Ethernet cables
- One crossover Category 5 Ethernet cable (optional if hub has an uplink port)
- One console cable
- Access to the command prompts for each host
- Access to the network TCP/IP configuration for each host

From the host computer, start a HyperTerminal session to the router and switch.

Note: Make sure that the routers and switches have been erased and have no startup configurations. Instructions for erasing the switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Configure Devices

Step 1: Configure basic information on the router and switch.

a. Build and configure the network according to the topology diagram and device configuration table. Configure basic settings on router R1. If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

b. Configure the basic settings on switch S1 to include the host name, passwords, and VLAN 1 IP address. If necessary, see Lab 5.5.4, “Configuring the Cisco 2960 Switch,” for instructions on configuring the switch settings.

c. Save the running configuration on R1 and S1 using the **copy running-config startup-config** command from privileged EXEC mode.

d. Connect the hub to switch S1 using a regular port on the hub and a crossover cable or using the hub uplink port (if present) and a straight-through cable.

Step 2: Configure the hosts.

Configure H1 and H2 with an IP address, subnet mask, and default gateway, according to the device configuration table.

Task 2: Verify Cabling, Interface LEDs, and Link Speed

Step 1: Visually inspect the network connections.

a. After cabling the network devices, verify the connections. Attention to detail now minimizes the time required to troubleshoot network connectivity issues later.

b. Are all cables and terminations in good condition? ___________

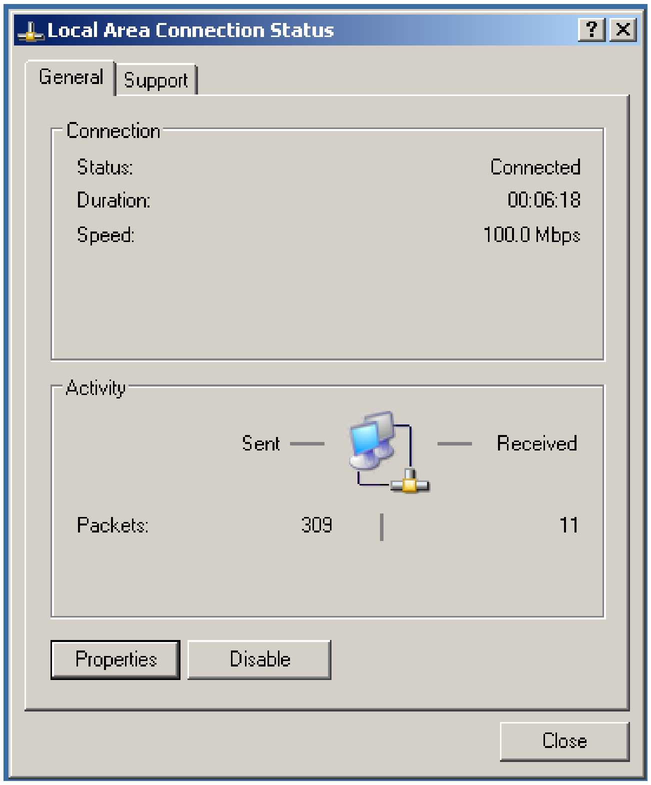
Step 2: Visually inspect the interface link LEDs.

a. What is the color of the link light for the switch port that H1 is attached to? __________

b. What is the color of the link light on the H1 NIC? ______________________________

Step 3: View the link speed for host H1 with local area connections.

a. On H1, choose **Start > Settings > Control Panel > Network Connections > Local Area Connection.**



Status: Connected
Duration: 00:06:18
Speed: 100.0 Mbps

Packets: 309 | 11

b. What is the connection speed? _________

Task 3: Verify Switch Interface Information

Step 1: Verify interface status.

a. From the HyperTerminal session on S1, use the **show ip interface brief** command to see the status summary of all interfaces.

```
S1#show ip interface brief
Interface        IP-Address      OK? Method Status       Protocol

Vlan1            192.168.1.99    YES manual up           up

FastEthernet0/1  unassigned      YES unset  up           up

FastEthernet0/2  unassigned      YES unset  up           up

FastEthernet0/3  unassigned      YES unset  up           up

FastEthernet0/4  unassigned      YES unset  down         down
```

```
FastEthernet0/5 unassigned      YES unset  down         down
```

b. Which interfaces have a status of **up** and a protocol that is **up**? ____________________________

Step 2: Verify end-to-end connectivity.

a. On H1, open a Command Prompt window by choosing **Start > Run** and typing **cmd**. Alternatively, you can choose **Start > All programs > Accessories > Command Prompt**.

b. Use the **ping** command to test end-to-end connectivity. Ping from H1 to the default gateway.

```
C:\>ping 192.168.1.1
```

c. Ping from host H1 to host H2.

```
C:\>ping 192.168.1.22
```

Note: If the pings are not successful, troubleshoot the router and host configurations and connections.

Step 3: Verify interface status and settings.

To view the speed and duplex settings on a port and whether manual or auto-negotiation features were used, use the s**how interface** *port* **status** command.

a. Display the status for port numbers Fast Ethernet 0/1 and Fast Ethernet 0/3.

```
S1#sh interfaces FastEthernet 0/1 status
Port      Name        Status       Vlan    Duplex  Speed   Type
Fa0/1                 connected    1       a-full  a-100   10/100BaseTX

S1#sh int f0/3 status
Port      Name        Status       Vlan    Duplex  Speed   Type
Fa0/3                 connected    1       a-half  a-10    10/100BaseTX
```

b. What is the duplex and speed for port Fast Ethernet 0/1? ______________

c. What does the “a-” at the beginning of “full” and “100” mean? _______________

d. What is the interface type? _______________

e. What is the duplex and speed for port Fast Ethernet 0/3? ______________

f. Why is the duplex and speed for Fast Ethernet 0/3 different than Fast Ethernet 0/1? _______________

Step 4: View interface error statistics.

a. To get a quick view of switch port error statistics, use the **show interface** *port* **counters errors** command.

```
S1#show int f0/1 counters errors

Port   Align-Err    FCS-Err   Xmit-Err    Rcv-Err UnderSize
Fa0/1          0          0          0          0         0

Port   Single-Col Multi-Col  Late-Col Excess-Col Carri-Sen Runts Giants
Fa0/1           0         0         0          0         0     0      0
```

b. Are there any errors or collisions for Fast Ethernet 0/1? ______________

c. Repeat the command for ports Fast Ethernet 0/2 and Fast Ethernet 0/3.

Task 4: Change Duplex Settings

Step 1: Set the duplex setting to full.

a. Change the duplex setting on Fast Ethernet 0/3 to force it to operate at full duplex.

```
S1(config)#interface FastEthernet 0/3
S1(config-if)#duplex full
S1(config-if)#end
S1#
```

b. What is the result of setting the port Fast Ethernet 0/3 duplex to full?

____

c. Issue the **show ip interface brief** command. What is the status and protocol for interface 0/3? ______________________

d. Why did this happen?

____

____

Step 2: Set the duplex setting to half duplex.

a. Change the duplex setting on Fast Ethernet 0/3 to force it to operate at half duplex.

```
S1(config)#interface FastEthernet 0/3
S1(config-if)#duplex half
S1(config-if)#end
S1#
```

b. What is the result of setting the port Fast Ethernet 0/3 duplex to half?

____

c. Issue the **show ip interface brief** command again. What is the status and protocol for interface Fast Ethernet 0/3? ______________________

d. Why did this happen?

____

____

Step 3: Set the duplex setting to auto-negotiate.

a. Change the duplex setting on Fast Ethernet 0/3 back to auto-negotiate.

```
S1(config)#interface FastEthernet 0/3
S1(config-if)#duplex auto
S1(config-if)#end
S1#
```

b. What is the result of setting the port Fast Ethernet 0/3 duplex back to auto?

____

Task 5: Change Speed Settings

Step 1: Set the speed to 100 Mbps.

a. Change the speed setting on Fast Ethernet 0/3 to 100 Mbps.

```
S1(config)#interface FastEthernet 0/3
S1(config-if)#speed 100
S1(config-if)#end
S1#
```

b. What is the result of setting the speed to 100?

____

c. Issue the **show ip interface brief** command. What is the status and protocol for interface Fast Ethernet 0/3? ________________________

d. Why did this happen?

____

Step 2: Set the speed setting to auto-negotiate.

a. Change the duplex setting on Fast Ethernet 0/3 back to auto-negotiate.

```
S1(config)#interface FastEthernet 0/3
S1(config-if)#speed auto
S1(config-if)#end
S1#
```

b. What is the result of setting the port Fast Ethernet 0/3 speed back to auto?

____

Task 6: Set Both Duplex and Speed Settings

Step 1: Set the duplex and speed settings for Fast Ethernet 0/1 to full and 100 Mbps.

It is sometimes necessary to set the speed and duplex of a port to ensure that it operates in a particular mode. To force Fast Ethernet port 0/1 to operate at full duplex and 100 Mbps, issue the following commands.

```
S1(config)#interface FastEthernet 0/1
S1(config-if)#duplex full
S1(config-if)#speed 100
S1(config-if)#end
S1#
```

Step 2: Verify the new settings.

a. When a port is in the default state of auto duplex and auto speed, duplex and speed commands do not appear in the running configuration for the interface. When the duplex and speed are set to force the port to operate in a particular mode, the commands used are displayed. Use the **show run interface** command to view only the portion of the running configuration that is associated with Fast Ethernet 0/1.

```
S1(config)#show run interface FastEthernet 0/1
Building configuration...

Current configuration : 57 bytes
```

```
!
interface FastEthernet0/1
 speed 100
 duplex full
end
```

b. Are there any console messages regarding the link status of Fast Ethernet 0/1? _______

Why? ____

Task 7: Check Settings and Characteristics of Neighboring Devices and Interfaces

Step 1: Check the characteristics of the neighbor attached to switch port Fast Ethernet 0/2.

a. Issue the **show cdp neighbors** command for the S1 Fast Ethernet 0/2 port.

```
S1#show cdp neighbors FastEthernet 0/2 detail
-------------------------
Device ID: R1
Entry address(es):
  IP address: 192.168.2.1
Platform: Cisco 1841,  Capabilities: Router Switch IGMP
Interface: FastEthernet0/2,  Port ID (outgoing port): FastEthernet0/1
Holdtime : 145 sec

Version :
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

advertisement version: 2
VTP Management Domain: ''
Duplex: full
Management address(es):
```

b. What is the name and platform of the attached device? ________________

c. What is the Cisco IOS version? ______________

d. What is the duplex setting for the attached port? ______________

e. Issue the **show cdp neighbors** command for S1 Fast Ethernet 0/3.

```
S1#sh cdp neig f0/3
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce  Holdtme   Capability    Platform   Port ID
```

f. Why is there no information shown for the attached device? ______________________________

____

Task 8: Change Router Duplex Settings

Step 1: Set the duplex setting for R1 Fast Ethernet 0/0 to half duplex.

a. To force R1 Fast Ethernet port 0/0 to operate at half duplex, issue the following commands.

```
R1(config)#interface FastEthernet 0/0
R1(config-if)#duplex half
R1(config-if)#end
```

b. Issue the **show ip interface brief** command on R1.

c. What is the status of Fast Ethernet 0/0? _______________

d. Issue the **show ip interface brief** command on S1.

e. What is the status of Fast Ethernet 0/2 (the port to which R1 is attached)? _______________

f. Can you ping the switch VLAN 1 address (192.168.1.99)? ____

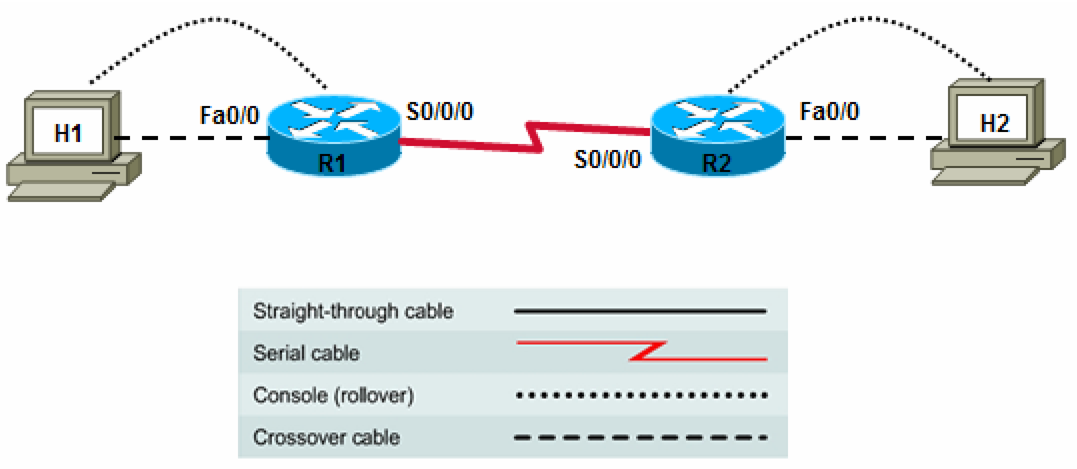
Why? ____

Task 9: Reflection

When LAN connectivity problems exist, always check link lights first and then check the cabling and terminations. Verify that interfaces are not shutdown. Verify that ports are set to auto-negotiate, if possible. If a device connected to a port cannot auto-negotiate or connectivity problems exist, forcing the port to operate at the specific duplex and speed of the attached device may be required. Check interface errors to determine if there is a problem with the physical interface itself. Always check both ends of the connection, if possible.

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab 9.2.5 Troubleshooting WAN Connectivity



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway
R1	R1	Fast Ethernet 0/0	192.168.1.1	255.255.255.0	N/A
		Serial 0/0/0 (DCE)	192.168.3.1	255.255.255.252	N/A
R2	R2	Fast Ethernet 0/0	192.168.2.1	255.255.255.0	N/A
		Serial 0/0/0 (DTE)	192.168.3.2	255.255.255.252	N/A
H1	H1	NIC	192.168.1.11	255.255.255.0	192.168.1.1
H2	H2	NIC	192.168.2.22	255.255.255.0	192.168.2.1

Objectives:

- Build a multi-router network and verify connectivity.
- Troubleshoot WAN connectivity using the LEDs and **show** commands to find link problems and encapsulation and timing mismatches.

Background / Preparation

Troubleshooting a serial WAN connection is different from troubleshooting Ethernet LAN connections. Most serial interface and line problems can be identified and corrected using information gathered from the **show interface serial** command. In addition to the transmission errors shown in the error counters, serial connections may experience problems caused by errors or mismatches in encapsulation and timing. In prototype networks, such as those created in a lab environment, a router can be configured to provide DCE clocking functions, eliminating the CSU or modem.

In this lab, you build a multi-router network with a serial WAN link. You will alter the encapsulation and clock speed settings for the serial interfaces and observe the effects on links lights and interface status.

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, or 2600 routers, or a combination of these, can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- Two 1841 routers or other routers with one Fast Ethernet and one serial interface
- Two Windows XP computers
- Two crossover Category 5 Ethernet cables
- Null serial cable (R1 to R2)
- At least one console cable
- Access to the command prompt for each host
- Access to the network TCP/IP configuration host

From the host computer, start a HyperTerminal session to the router.

Note: Make sure that the routers have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Configure Devices

Step 1: Configure the basic information on the routers.

a. Build and configure the network according to the topology diagram and device configuration table. Configure basic settings on router R1 and R2. If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

   Note: Be sure to configure the clock rate for the R1 serial 0/0/0 interface (DCE).

b. Save the running configuration on router R1 and R2 using the **copy running-config startup-config** command from privileged EXEC mode.

Step 2: Configure the hosts.

Configure H1 and H2 with an IP address, subnet mask, and default gateway according to the device configuration table.

Task 2: Verify Cabling and Interface LEDs

Step 1: Visually inspect the network connections.

a. After cabling the network devices, verify the connections. Attention to detail now minimizes the time required to troubleshoot network connectivity issues later.

b. Are all cables and terminations in good condition? ___________

Step 2: Visually inspect interface link LEDs.

a. What is the color of the link lights for the router R1 Fast Ethernet interface to which host H1 is attached? ____________________________

b. What is the color of the link light on the host H1 NIC? __________________________________

c. What is the color of the link light for the router R1 serial 0/0/0 to which router R2 is attached? __________

Task 3: Verify Router Interface Status and Connectivity

Step 1: Verify the status of the interfaces on R1.

a. From the HyperTerminal session on router R1, use the **show ip interface brief** command to see the status summary of all interfaces.

```
R1#show ip interface brief
Interface        IP-Address   OK? Method Status                Protocol
FastEthernet0/0  192.168.1.1  YES NVRAM  up                    up

FastEthernet0/1  unassigned   YES manual administratively down down

Serial0/0/0      192.168.3.1  YES manual up                    up

Serial0/0/1      unassigned   YES NVRAM  administratively down down

Vlan1            unassigned   YES NVRAM  up                    down
```

b. Which interfaces have a status of **up** and a protocol that is **up**? ____________________________

Step 2: View the details of the serial 0/0/0 interface on R1.

a. Issue the **show interface serial** command to view the details of the interface.

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: WAN link to R2
  Internet address is 192.168.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:05, output 00:00:08, 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: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     1154 packets input, 75892 bytes, 0 no buffer
     Received 914 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     908 packets output, 63486 bytes, 0 underruns
     0 output errors, 0 collisions, 8 interface resets
     0 output buffer failures, 0 output buffers swapped out
     25 carrier transitions

  DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

b. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol?__________

d. What is the Internet address? ____________________________

e. What is the encapsulation?____________

Step 3: Verify the status of the interfaces on R2.

a. From the HyperTerminal session on router R2, use the **show ip interface brief** command to see the status summary of all interfaces.

```
R2#show ip interface brief
Interface        IP-Address   OK? Method Status                Protocol
FastEthernet0/0  192.168.2.1  YES NVRAM  up                    up

FastEthernet0/1  unassigned   YES manual administratively down down

Serial0/0/0      192.168.3.2  YES manual up                    up

Serial0/0/1      unassigned   YES NVRAM  administratively down down

Vlan1            unassigned   YES NVRAM  up                    down
```

b. Which interfaces have a status of up and a protocol that is up? ____________________________

Step 4: View the details of serial 0/0/0 interface on R2.

a. Enter the **show interface serial** command to view the details of the interface.

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: WAN link to R1
  Internet address is 192.168.3.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:02, output 00:00:00, 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: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     179 packets input, 13104 bytes, 0 no buffer
     Received 169 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     195 packets output, 13252 bytes, 0 underruns
     0 output errors, 0 collisions, 3 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. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol?__________

d. What is the Internet address? ____________________________

e. What is the encapsulation?_____________

Step 5: Verify serial link connectivity between the routers.

From the HyperTerminal session on R1, ping the IP address of the R2 serial 0/0/0 interface.

```
R1#ping 192.168.3.2
```

Note: If the pings are not successful, troubleshoot the router configurations and connections.

Task 4: Change the Clock Rate

Step 1: On router R1, remove the clock rate from serial 0/0/0.

The R1 serial 0/0/0 interface is currently providing the DCE clock signal for the serial WAN link.

a. Use the **no clock rate** command to remove the clock from Serial 0/0/0.

```
R1(config)#interface serial 0/0/0
R1(config-if)#no clock rate
R1(config-if)#end
```

b. Which console messages, if any, are displayed when the clock rate is removed?

____

Step 2: View the details of the interface.

a. Issue the **show interface serial** command on R1.

Note: The following output is from a Cisco 1841 router. If you are not using an 1841 and you received an error message in the previous step, the line protocol is down.

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Description: WAN link to R2
  Internet address is 192.168.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:00, output 00:00:01, 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: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     80 packets input, 6205 bytes, 0 no buffer
     Received 80 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     81 packets output, 6229 bytes, 0 underruns
     0 output errors, 0 collisions, 5 interface resets
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
        DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

b. What is the status of the R1 serial 0/0/0 interface and line protocol? ______________________

Note: This lab uses Cisco 1841 routers with Cisco IOS software release 12.4(10). When the clock rate is removed from the DCE serial 0/0/0 interface, the 1841 router automatically reinserts the clock rate at a default speed of 2000000 bps (2 Mbps).

If a router such as a 2600 series is used, the serial 0/0/0 interface goes to up/down status when the clock rate is removed from the DCE interface serial 0/0/0.

Step 3: On router R1, reset the clock rate on serial 0/0/0.

a. Use the Cisco IOS help feature with the **clock rate** command to determine the range of clock rate settings.

```
R1(config)#interface serial 0/0/0
R1(config-if)#clock rate ?
```

b. What is the highest setting listed? _________________

c. On router R1, apply a clock rate of 128000 bps to serial 0/0/0.

```
R1(config)#interface serial 0/0/0
R1(config-if)#clock rate 128000
R1(config-if)#end
```

Note: Even though the **clock rate** command lists settings up to 8000000, depending on the router model and serial interface type, the router interface may not be able to support speeds above 128000. The 1841 router with a WIC 2T modular serial interface can support speeds up to 8000000 bps.

The following message is from a 2600 router with Cisco IOS software release 12.2 and a WIC 2A/S modular serial interface. The WIC 2A/S interface supports speeds up to 128000 but displays an error message when attempting to set the clock rate to anything higher.

```
R1(config-if)#clock rate 148000
%Error: Unsupported clock rate for this interface
```

Task 5: Remove the Serial Cable and Observe the Effects

Step 1: Remove the cable from router R1 serial 0/0/0.

Which console messages, if any, are displayed when the cable is removed?

____

Step 2: On router R1, use the show interface serial command.

a. Issue the **show interface serial** command to view the details of the interface.

```
R1#show interface serial 0/0/0
   Serial0/0/0 is down, line protocol is down
     Hardware is GT96K Serial
     Description: WAN link to R2
     Internet address is 192.168.3.1/30
     MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
     Encapsulation HDLC, loopback not set
     Keepalive set (10 sec)
     Last input 00:04:03, output 00:03:56, output hang never
     Last clearing of "show interface" counters 01:36:07
     Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
     Queueing strategy: weighted fair
     Output queue: 0/1000/64/0 (size/max total/threshold/drops)
        Conversations  0/1/256 (active/max active/max total)
        Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     954 packets input, 36318 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
     1163 packets output, 37144 bytes, 0 underruns
     0 output errors, 0 collisions, 119 interface resets
     0 output buffer failures, 0 output buffers swapped out
     145 carrier transitions
     DCD=up  DSR=up  DTR=down  RTS=down  CTS=up
```

b. What is the status of the R1 serial 0/0/0 interface and line protocol? __________

Step 3: Reconnect the serial cable to the R1 serial 0/0/0 interface.

a. Did the interface and line protocol come back up? ______

b. Are there any runts, giants, input errors, CRC errors, output errors, collisions, or interface resets?

____

Step 4: On router R1, clear the counters on serial 0/0/0.

a. Use the **clear counters serial** command to reset the interface statistics.

```
R1#clear counters serial 0/0/0
Clear "show interface" counters on this interface [confirm]
R1#
*Mar  5 21:30:54.258: %CLEAR-5-COUNTERS: Clear counter on interface
Serial0/0/0 by console
```

b. Issue the **show interface serial 0/0/0** command to view the details of the interface. Have the interface statistics been reset? _________

Task 6: Change the Encapsulation Type

Step 1: Verify the current serial status and Data Link Layer 2 encapsulation.

a. Issue the **show interface serial 0/0/0** command to view the details of the interface on R1.

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is down
  Hardware is GT96K Serial
  Description: WAN link to R2
  Internet address is 192.168.3.1/30
  MTU 1500 bytes, BW 1544 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 00:00:17, output hang never
  Last clearing of "show interface" counters 00:01:25
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
```

```
     9 packets input, 206 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
     20 packets output, 280 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
     6 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

b. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol?__________

d. What is the encapsulation?_____________

Step 2: Change the serial interface encapsulation on R1.

a. Use the Cisco IOS help feature with the **encapsulation** command to see which encapsulation type settings are available.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ?
```

b. Which encapsulation choices are available?

____

c. Change the encapsulation type to PPP.

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
```

d. What console messages are displayed?

____

____

Step 3: Verify the interface status and encapsulation on R1.

a. Issue the **show interface serial** to view the details of the R1 serial 0/0/0 interface.

```
R1#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is down
  Hardware is GT96K Serial
  Description: WAN link to R2
  Internet address is 192.168.3.1/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Listen, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:08, output 00:00:17, output hang never
  Last clearing of "show interface" counters 00:01:25
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     9 packets input, 206 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
     20 packets output, 280 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
     6 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

b. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol?__________

d. What is the encapsulation?____________

Step 4: Check the serial interface encapsulation on R2.

a. Issue the **show interface serial** command to view the details of the R2 serial 0/0/0 interface.

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is down
  Hardware is GT96K Serial
  Description: WAN link to R1
  Internet address is 192.168.3.2/30
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 00:00:03, output 00:00:01, 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: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     729 packets input, 30809 bytes, 0 no buffer
     Received 729 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     548 packets output, 30055 bytes, 0 underruns
     0 output errors, 0 collisions, 63 interface resets
     0 output buffer failures, 0 output buffers swapped out
     204 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
```

b. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol?__________

d. What is the encapsulation?____________

e. Why is the line protocol for both R1 and R2 now down?

____

Step 5: Change the serial interface encapsulation on R2.

a. Now change the encapsulation type on the R2 interface to PPP.

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
```

b. What console messages are displayed?

____

____

Step 6: Check the interface status on R2.

a. Issue the **show ip interface brief** command to view the status of all R2 interfaces.

```
R2#show ip interface brief
Interface        IP-Address   OK? Method  Status            Protocol
FastEthernet0/0  192.168.2.1  YES NVRAM   up                    up

FastEthernet0/1  unassigned   YES NVRAM   administratively down down

Serial0/0/0      192.168.3.2  YES NVRAM   up                    up

Serial0/0/1      unassigned   YES NVRAM   administratively down down

Vlan1            unassigned   YES NVRAM   up                    down
```

b. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol? __________

Step 7: Check the interface status on R1.

a. Issue the **show ip interface brief** command to view the status of all R1 interfaces.

```
R1#show ip interface brief
```

b. What is the status of serial 0/0/0? __________

c. What is the status of the line protocol? __________

d. Issue the **show running-config interface** command to view the commands used to configure the R1 serial 0/0/0 interface.

```
R1(config)#show run int Serial 0/0/0

Building configuration...

Current configuration : 137 bytes
!
interface Serial0/0/0
 description WAN link to R2
 ip address 192.168.3.1 255.255.255.252
 encapsulation ppp
 clockrate 128000
end
```

Step 8: Verify that the serial connection is functioning.

a. Ping from R1 to R2 to verify that there is connectivity between the two routers.

```
R1#ping 192.168.3.2
R2#ping 192.168.3.1
```

Can the serial interface on R2 be pinged from R1? __________

Can the serial interface on R1 be pinged from R2? __________

b. If the answer is no for either question, troubleshoot the router configurations to find the error. Repeat the pings until they are successful.

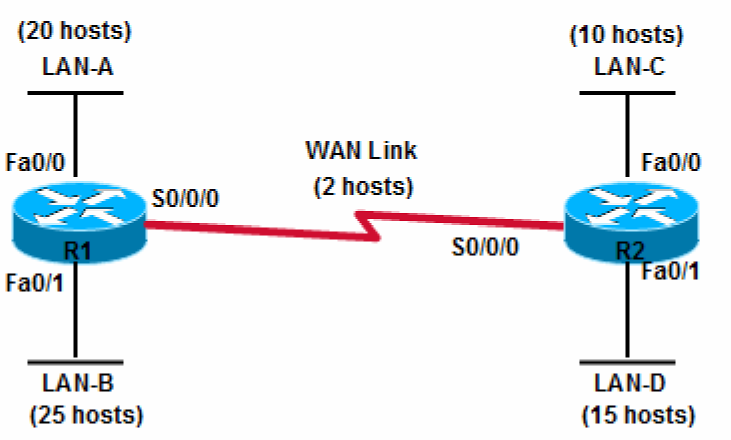
Task 7: Reflection

When WAN connectivity problems exist, always check link lights first and then check the cabling and terminations. Verify that interfaces are not shutdown. Verify that interfaces are set to the proper encapsulation and clock rate (if applicable). Check interface errors to determine if there is a problem with the physical interface itself. Always check both ends of the connection, if possible.

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 9.3.3 Designing an IP Subnetting Scheme for Growth



Objectives

- Analyze the subnetting requirements for a small company with multiple networks.
- Design a subnetting scheme that allows for 20% growth in the number of subnets and the number of hosts per subnet.
- Develop an IP addressing plan to apply addresses to networking devices and host computers.

Background / Preparation

When developing IP addressing schemes for subnetting, it is important to look at the subnet requirements of the network and plan for potential growth in the number of subnets and the number of hosts per subnet.

In this lab, you are given a block of addresses to work with. Based on the network requirements of the organization, subnet the block of addresses and allocate a subnet to each segment of the network. In the subnet scheme, you must allow for 20% growth in the number of subnets and in the number of hosts for a given subnet. After you have created the subnets, assign IP addresses to each of the router interfaces and allocate blocks of addresses for the hosts on each LAN.

This is a paper-based lab. Use the worksheets to complete the lab.

Task 1: Analyze the Network Topology for Subnetting Requirements

Step 1: Examine the network topology to determine the number of segments.

a. How many Ethernet networks currently exist? _______

b. How many WAN links currently exist? _______

c. How many total networks? _______

d. How many subnets? _________

e. How many subnets with 20% growth? _________

Step 2: Document the current number of hosts on each network segment.

a. Enter the network segment names in the table. Enter the number of hosts on each subnet, and then calculate the number of hosts the subnet must support if the number grows by 20%.

Segment name	Current number of hosts	Number of hosts after 20% growth

b. Which subnet must support the largest number of hosts? _____________

Task 2: Develop the Subnet Scheme

Step 1: Determine the number of subnets and hosts.

The customer has been assigned IP address block 172.20.99.0 /24 by their ISP. This provides 8 bits for hosts.

a. How many total addresses do they have to work with before subnetting? ___________________

b. What is the decimal subnet mask for a /24 mask? ______________________

c. What is the minimum number of subnets required for the network design to allow for 20% growth? _________

d. How many bits must be borrowed from the host portion of the IP address to allow for that number of subnets, and how many total subnets can be created? __________

e. How many hosts (including the 20% growth) must the largest subnet support? __________

f. To support that many hosts, the number of host bits required is ______________

g. Does this subnet scheme allow for the number of subnets and hosts per subnet needed? ________

Step 2: Calculate the custom subnet mask.

a. The address block assigned by the ISP is a /24 or 255.255.255.0. What is the custom subnet mask? _____._____._____._____, or /______

b. To which devices and interfaces is this mask assigned? __________________

Step 3: Identify the subnet and host IP addresses.

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 possible subnets for the 172.20.99.0 network. In the last column, enter the name of the network segment to which you are assigning the subnet.

Subnet	Subnet Address	Host IP Address Range	Broadcast Address	Network Segment
0				
1				
2				
3				
4				
5				
6				
7				

Task 3: Document network device and host interfaces.

Step 1: Document the network device interface IP addresses.

Fill in the following table with the IP addresses and subnet masks for the router interfaces.

Network Device Interface Addresses

Device	Network Segment	Interface	IP Address	Subnet Mask
R1	LAN-A	Fast Ethernet 0/0		
	LAN-B	Fast Ethernet 0/1		
	WAN	Serial 0/0/0		
R2	LAN-C	Fast Ethernet 0/0		
	LAN-D	Fast Ethernet 0/1		
	WAN	Serial 0/0/0		

Step 2: Document the host IP addresses.

Fill in the following table with the IP addresses and subnet masks for the first host on each LAN. Assign the next available address to the first host computer on the LAN.

Host Computer Interface Addresses

Device	Network Segment	Interface	IP Address	Subnet Mask	Default Gateway
Host 1	LAN-A	NIC			
Host 1	LAN-B	NIC			
Host 1	LAN-C	NIC			
Host 1	LAN-D	NIC			

Task 4: Reflection

a. With the initial block of addresses assigned by the ISP, and the requirements for future growth, is there any other subnetting scheme that could have worked? ___________

b. If the maximum number of hosts per network segment was only 14, could you have used another scheme? ____ Why? ____

____

c. Although it works for the scenario in item b above, would it be a good idea to use 4 bits for subnets and 4 bits for hosts? _____ Why? ____

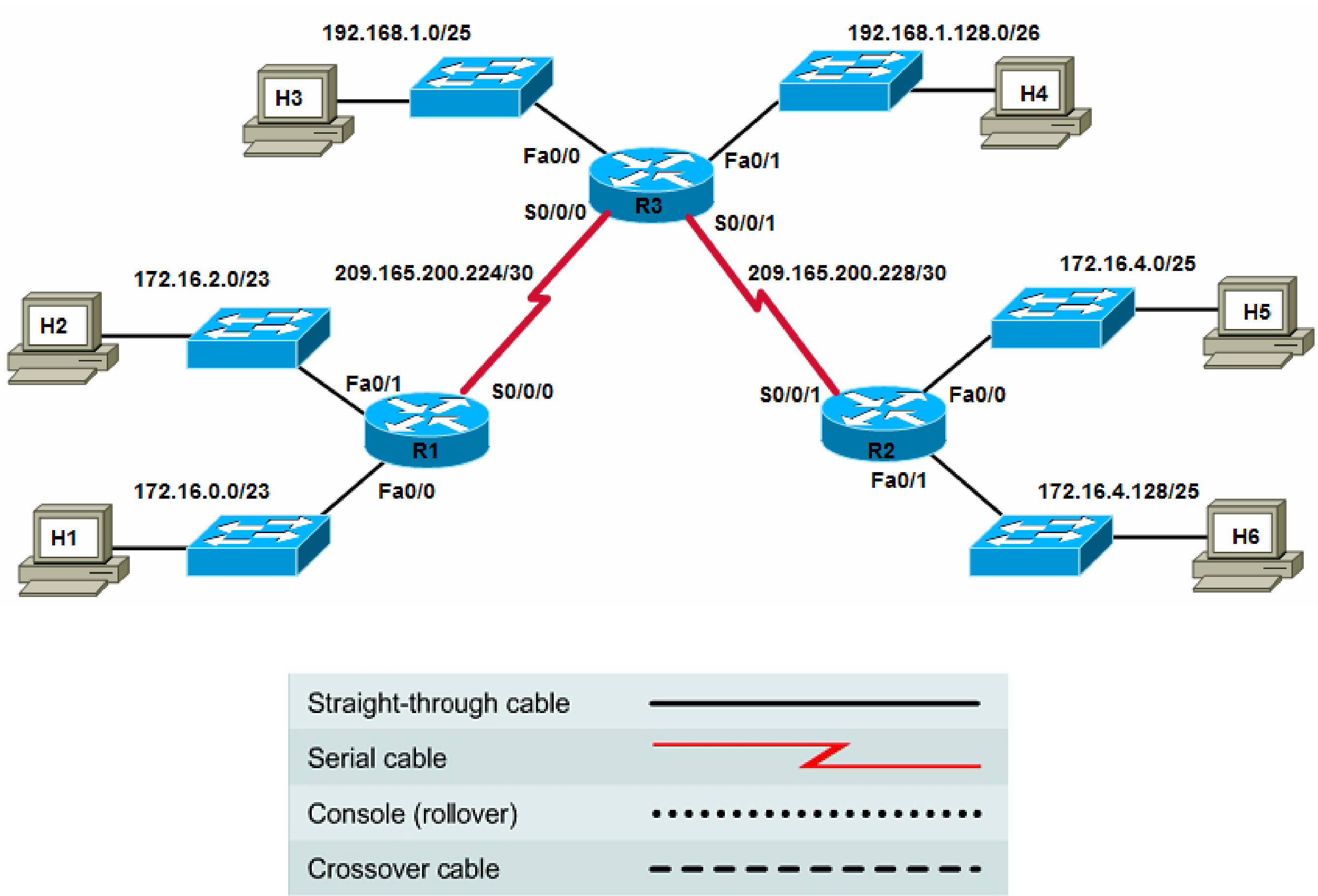
____

____

CCNA Discovery

Working at a Small-to-Medium Business or ISP

Lab 9.4.2 Correcting RIPv2 Routing Problems



Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway
R1	BRANCH1	Fast Ethernet 0/0	172.16.0.1	255.255.254.0	N/A
		Fast Ethernet 0/1	172.16.2.1	255.255.254.0	N/A
		Serial 0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
R2	BRANCH2	Fast Ethernet 0/0	172.16.4.1	255.255.255.128	N/A
		Fast Ethernet 0/1	172.16.4.129	255.255.255.128	N/A
		Serial 0/0/1	209.165.200.230	255.255.255.252	N/A
R3	HQ	Fast Ethernet 0/0	192.168.1.1	255.255.255.128	N/A
		Fast Ethernet 0/1	192.168.1.129	255.255.255.192	N/A
		Serial 0/0/0	209.165.200.225	255.255.255.252	N/A
		Serial 0/0/1 (DCE)	209.165.200.229	255.255.255.252	N/A
H1	H1	NIC	172.16.0.10	255.255.254.0	172.16.0.1
H2	H2	NIC	172.16.2.10	255.255.254.0	172.16.2.1

Device	Host Name	Interface	IP Address	Subnet Mask	Default Gateway
H3	H3	NIC	192.168.1.10	255.255.255.128	192.168.1.1
H4	H4	NIC	192.168.1.138	255.255.255.192	192.168.1.129
H5	H5	NIC	172.16.4.10	255.255.255.128	172.16.4.1
H6	H6	NIC	172.16.4.138	255.255.255.128	172.16.4.129

Objectives

- Cable a network according to the topology diagram.
- Load the routers with supplied scripts.
- Gather information about the non-converged portion of the network, along with any other errors.
- Analyze information using Cisco IOS show and debug commands to determine network errors.
- Propose solutions to network errors.
- Implement solutions to network errors.
- Document the corrected network.

Background / Preparation

Many different types of problems can cause dynamic routes to not appear in the routing table. With dynamic routing, routers receive routing updates from neighbors. If an expected route does not appear in the routing table of one of the routers, the cause is most likely a configuration error. This configuration error could occur on any of the routers connected between the source and the destination.

In this lab, you begin by loading configuration scripts on each of the routers. These scripts contain errors that prevent end-to-end communication across the network. After loading the corrupted scripts, troubleshoot each router to determine the configuration errors, and then use the appropriate commands to correct the configurations. When you have corrected all the configuration errors, all the hosts on the network should be able to communicate with each other.

The network should also have the following requirements met:

- RIPv2 routing is configured on all routers.
- RIP updates must be disabled on all router LAN interfaces.

Required Resources

The following resources are required:

- Two routers, each with two Fast Ethernet and one serial interface
- One router, with two Fast Ethernet and two serial interfaces
- Six switches or hubs (or crossover cables from hosts to routers)
- Six Windows XP computers
- Straight-through Category 5 Ethernet cables, as required
- Two null serial cables
- Console cables, as required
- Access to the host command prompt
- Access to the host network TCP/IP configuration

Note: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Task 1: Build the Network and Configure Devices

Step 1: Build a network similar to the one shown in the topology diagram.

Step 2: Configure the hosts.

Configure each host IP address, subnet mask, and default gateway according to the device configuration chart.

Task 2: Load Routers with the Supplied Scripts

Step 1: Load the script onto the BRANCH1 router.

```
hostname BRANCH1
!
line console 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
enable secret class
banner motd #Unauthorized Use Prohibited#
no ip domain lookup
!
interface FastEthernet0/0
ip address 172.16.0.1 255.255.254.0
duplex auto
speed auto
no shutdown
!
interface FastEthernet0/1
ip address 172.16.2.1 255.255.254.0
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 209.165.200.226 255.255.255.252
clock rate 64000
no shutdown
!
router rip
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 172.16.0.0
network 209.165.200.0
!
ip classless
!
line con 0
line vty 0 4
login
!
end
```

Step 2: Load the script onto the BRANCH2 router.

```
hostname BRANCH2
!
line console 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
enable secret class
banner motd #Unauthorized Use Prohibited#
no ip domain lookup
!
interface FastEthernet0/0
ip address 172.16.4.129 255.255.255.128
duplex auto
speed auto
no shutdown
!
interface FastEthernet0/1
ip address 172.16.4.1 255.255.255.128
duplex auto
speed auto
no shutdown
!
interface Serial0/0/1
ip address 209.165.200.230 255.255.255.252
no shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 209.165.200.0
!
ip classless
!
line con 0
line vty 0 4
login
!
end
```

Step 3: Load the script onto the HQ router.

```
hostname HQ
!
line console 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

```
enable secret class
banner motd #Unauthorized Use Prohibited#
no ip domain lookup
!
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.128
duplex auto
speed auto
no shutdown
!
interface FastEthernet0/1
ip address 192.168.1.129 255.255.255.192
duplex auto
speed auto
no shutdown
!
interface Serial0/0/0
ip address 209.165.200.225 255.255.255.252
no shutdown
!
interface Serial0/0/1
ip address 209.165.200.229 255.255.255.252
clock rate 64000
no shutdown
!
router rip
version 2
passive-interface FastEthernet0/0
passive-interface FastEthernet0/1
network 192.168.1.0
network 209.165.200.0

!
ip classless
!
line con 0
line vty 0 4
login
!
end
```

Task 3: Troubleshoot the BRANCH1 Router

Step 1: Begin troubleshooting at the host connected to BRANCH1.

a. From H1, is it possible to ping H2 (172.16.0.10)? ________

b. From H1, is it possible to ping H3 (192.168.1.10)? _______

c. From H1, is it possible to ping H5 (172.16.4.10)? ________

a. From H1, is it possible to ping the default gateway (172.16.0.1)? _______

Step 2: Examine BRANCH1 to find possible interface configuration errors.

a. View the status information summary for the router interfaces.

b. Are there any problems with the interface configurations? ________

c. If there are problems with the interface configurations, record the commands necessary to correct the configuration errors.

____

d. If you have recorded any commands, apply them to the router configuration now.

e. If any changes were made to the configuration, view the status information summary for the router interfaces again.

f. Does the information in the summary indicate any configuration errors? _______

g. If the answer is **yes**, troubleshoot the status of the interfaces again.

Step 3: Troubleshoot the routing configuration on BRANCH1.

a. What command displays the routing table? ____________________________

b. Which networks and routes are shown in the routing table?

____

____

____

____

____

____

c. Which command displays the commands used to configure the routing protocol on this router?

____

d. Are there any problems with the routing table because of the routing configuration?

____

____

e. If there are any problems, record the commands necessary to correct the configuration errors.

____

____

f. Are there any problems with the routing table that could be caused by errors in other parts of the network? ____

____

g. What version of RIP and which local networks are included in the RIP updates being sent from BRANCH1?

____

h. What commands could you use to determine the version of RIP updates? ________________

____

i. Use the **debug ip rip** command to determine which networks are included in the RIP updates being sent from BRANCH1.

____

j. Are there any problems with the version of RIP updates that are being sent out from the router?

____

____

k. If there are additional problems with the RIP configuration, record the commands necessary to correct the configuration errors.

____

____

____

Step 4: Fix the router configuration.

a. If you have recorded any commands in the previous step, apply them to the router configuration.

b. If any changes were made to the configuration, view the routing information again.

c. Does the information in the routing table indicate any configuration errors? _______

d. Does the information included in the RIP updates that are sent out indicate any configuration errors? _______

e. If the answer to either of these questions is yes, troubleshoot the routing configuration again.

f. Which networks and routes are shown in the routing table?

____

____

____

____

____

____

Step 5: Ping between the hosts again.

a. From H1, is it possible to ping H3 (192.168.1.10)? _______

b. From H1, is it possible to ping H4 (192.168.1.138)? ______

c. From H1, is it possible to ping H5 (172.16.4.10)? ________

d. From H1, is it possible to ping the serial 0/0/1 interface of the HQ router (209.165.200.229)? _______

Task 4: Troubleshoot HQ

Step 1: Begin troubleshooting at host H3.

a. From H3, is it possible to ping H1 (172.16.0.10)? _______

b. From H3, is it possible to ping H5 (172.16.4.10)? _______

c. From H3, is it possible to ping the default gateway (192.168.1.1)? ______

Step 2: Examine the HQ router to find possible configuration errors.

a. View the status information summary for the router interfaces. Are there any problems with the interface configurations? _______

b. If there are problems with the interface configurations, record the commands necessary to correct the configuration errors.

____

c. If you have recorded any commands, apply them to the router configuration now.

Step 3: Troubleshoot the routing configuration on HQ.

a. Which networks and routes are shown in the routing table?

____

____

____

____

____

____

b. If there any problems with the routing table, list them.

____

____

c. If there are problems, record the commands necessary to correct the configuration errors.

____

____

d. Which networks are included in the RIP updates?

____

____

____

e. Are there problems with the RIP updates that are being sent out from HQ? _________

f. If there are problems, record the commands necessary to correct the configuration errors.

____

____

g. If you have recorded any commands, apply them to the router configuration now.

Step 4: View the routing information.

a. If any changes were made to the configuration, view the routing information again.

b. Does the information in the routing table indicate any configuration errors on HQ? _______

c. Does the information included in the RIP updates that are sent out indicate any configuration errors on HQ? _______

d. If the answer to either of these questions is **yes**, troubleshoot the routing configuration again.

Step 5: Ping between the hosts again.

a. From H3, is it possible to ping H1 (172.16.0.10)? _______

b. From H3, is it possible to ping H5 (172.16.4.10)? _______

c. From H3, is it possible to ping the default gateway (192.168.1.1)? _______

Task 5: Troubleshoot BRANCH2

Step 1: Begin troubleshooting at host H5.

a. From H5, is it possible to ping H6 (172.16.4.138)? _______

b. From H5, is it possible to ping H1 (172.16.0.10)? ________

c. From H5, is it possible to ping the default gateway (172.16.4.1)? ________

Step 2: Examine BRANCH2 to find possible configuration errors.

a. View the status information summary for each interface on the router. Are there any problems with the configuration of the interfaces?

____

____

b. If there are problems, record the commands necessary to correct the configuration errors.

____

____

____

____

____

____

____

____

c. If you have recorded any commands, apply them to the router configuration now.

d. If any changes were made, view the summary of the status information for the router interfaces again.

e. Does the information in the interface status summary indicate any configuration errors? ______

f. If the answer is **yes**, troubleshoot the interface status of the interfaces.

Step 3: Troubleshoot the routing configuration on BRANCH2.

a. View the routing table.

b. Which networks and routes are shown in the routing table?

____

____

____

____

____

____

Step 4: Examine the routes that are being sent out in the routing updates from BRANCH2.

a. Are there any problems with the routing updates? If so, list them.

____

____

b. If there are problems, record the commands necessary to correct the configuration errors.

____

____

____

c. Apply any recorded commands to the router configuration.

Step 5: Ping the hosts again.

a. From H5, is it possible to ping H6 (172.16.4.138)? _______

b. From H5, is it possible to ping H1 (172.16.0.10)? ________

c. From H5, is it possible to ping the default gateway (172.16.4.1)? ________

d. From the HQ router, is it possible to ping H1 (172.16.0.10)? _________

e. From the HQ router, is it possible to ping H5 (172.16.4.10)? _________

Step 6: Examine the routing updates that are being received on BRANCH2.

a. Which networks are being received in the RIP updates on BRANCH2?

____

____

____

____

b. Are there any problems with these routing updates? If so, list them.

____

____

____

c. Display the routing table for the BRANCH2 router.

d. Is there a route to network 172.16.0.0 or 172.16.2.0 on BRANCH1? _______ Why?

____

____

e. Display the routing table for the HQ router.

f. How many routes does HQ have to the 172.16.0.0/16 network?

____

g. If there are problems with the routing configuration on BRANCH2, record the commands necessary to correct the configuration errors.

____

____

h. Do these commands need to be applied only to BRANCH2, or do they also need to be applied to any other routers in the network? ____

Task 6: Remove Auto-Summary

Step 1: Remove auto-summary from all three routers.

Use the **no auto-summary** command in router rip configuration mode to disable auto-summary and allow the routers to advertise the individual subnets on each router.

Step 2: View the routing information for BRANCH2.

a. View the routing table for BRANCH2. Does the information in the routing table indicate any configuration errors? _______

b. If the answer is **yes**, troubleshoot the routing configuration.

Step 3: View the routing information for BRANCH1.

Are routes to all networks and subnets now present? _________

Step 4: View the routing information for HQ.

Are routes to all networks and subnets now present? _______

Step 5: Test overall network connectivity by pinging between the hosts.

a. From H5, is it possible to ping H6 (172.16.4.138)? _______

b. From H5, is it possible to ping H1 (172.16.0.10)? ________

c. From H5, is it possible to ping H3 (192.168.1.10)? _______

d. From H1, is it possible to ping H3 (192.168.1.10)? _______

e. From the HQ router, is it possible to ping H1 (172.16.0.10)? _______

f. From the HQ router, is it possible to ping H5 (172.16.4.10)? _______

Task 7: Reflection

There were a number of configuration errors in the scripts that were provided for this lab. Use the space below to write a brief description of the errors that you found.

____

____

____

____

____

____

____

____

Task 8: Documentation

On each router, use the following commands and capture the output to a text (.txt) file. Save the file for future reference.

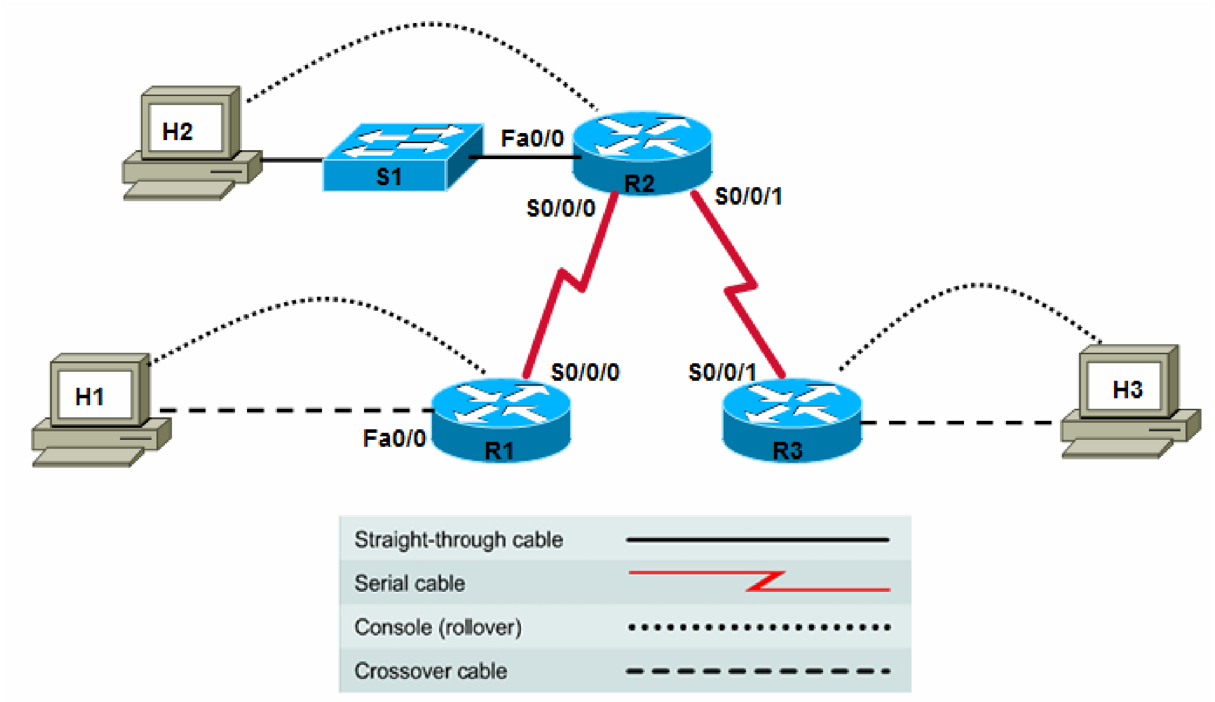
• **show running-config**

- **show ip route**
- **show ip interface brief**
- **show ip protocols**

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 9.5.3 Using Telnet and SSH to Access Networking Devices



Device	Host Name	Interface	IP Address	Subnet Mask	RIPv2 Network Statements
R1	R1	Serial 0/0/0 (DTE)	10.10.10.1	255.255.255.0	10.0.0.0
		Fast Ethernet 0/0	192.168.1.1	255.255.255.0	192.168.1.0
R2	R2	Serial 0/0/0 (DCE)	10.10.10.2	255.255.255.0	10.0.0.0
		Serial 0/0/1 (DCE)	172.16.1.1	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.2.1	255.255.255.0	192.168.2.0
R3	R3	Serial 0/0/1 (DTE)	172.16.1.2	255.255.255.0	172.16.0.0
		Fast Ethernet 0/0	192.168.3.1	255.255.255.0	192.168.3.0
S1	S1	VLAN 1 (mgmt)	192.168.2.99	255.255.255.0	N/A

Objectives

- Establish and manage Telnet connections to a remote router and switch.
- Verify that the Application Layer between the source and destination is working properly.
- Retrieve information about remote routers using **show** commands.
- Configure a router to accept SSH connections using the Cisco IOS CLI.
- Connect from one router using the SSH CLI client to a remote router running the SSH server.

Background / Preparation

Telnet is an excellent tool to use when troubleshooting problems with upper layer functions. Using Telnet to access networking devices enables technicians to enter commands on each device as if they were locally attached. In addition, the ability to reach devices using Telnet indicates that lower layer connectivity exists between the devices. Telnet is widely available on nearly any networking device.

Telnet is an unsecure protocol, which means that all data communicated can be captured and read. SSH is a more secure method for remote device access. Most newer versions of the Cisco IOS software contain an SSH server and an SSH client. In some devices, this service is enabled by default. Other devices require the SSH server to be manually enabled. Similarly, a remote computer with an SSH client installed can be used to start a secure CLI session.

This lab focuses on using Telnet and SSH to access routers remotely to gather information about them and verify upper layer connectivity. In this lab, you telnet from the workstation as a client and from a router into another remote router. In addition, you will configure SSH access on a router and connect using a router-based Cisco IOS CLI client.

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, or 2600 routers, or a combination of these, can be used. See the Router Interface Summary table at the end of the lab to determine which interface identifiers to use based on the equipment in the lab. Depending on the model of the router, output may vary from what is shown in this lab.

Required Resources

The following resources are required:

- One router with two serial interfaces and one Fast Ethernet (1841 or other)
- Two routers with one serial interface and one Fast Ethernet (1841 or other)
- One 2960 switch (or comparable) for the R2 LAN
- Three windows XP computers (hosts H2 and H3 are mainly for configuring routers R2 and R3)
- Straight-through and crossover Category 5 Ethernet cables, as required
- Two null serial cables
- Console cable to configure routers
- Access to host H1 command prompt
- Access to host H1 network TCP/IP configuration

On hosts H1, H2, and H3, start a HyperTerminal session to each router.

Note: Make sure that the routers and switches have been erased and have no startup configurations. Instructions for erasing are provided in the Lab Manual, located on Academy Connection in the Tools section. Check with the instructor if you are unsure of how to do this.

Part 1. Working with Telnet to Verify Device Configurations and Connectivity

Task 1: Build the Network and Verify Network Layer Connectivity

Step 1: Configure the basic information on each router and the switch.

a. Build and configure the network according to the topology diagram and device configuration table. If necessary, see Lab 5.3.5, “Configuring Basic Router Settings with the Cisco IOS CLI,” for instructions on setting the host name, passwords, and interface addresses.

b. Configure RIPv2 on each router, and advertise the networks shown in the device configuration table. If necessary, refer to Lab 6.1.5, “Configuring and Verifying RIP”, for instructions on configuring the RIP routing protocol.

c. Configure basic settings on the switch S1 to include host name, passwords and VLAN 1 IP address. If necessary, see Lab 5.5.4, “Configuring the Cisco 2960 Switch.”

Step 2: Configure the hosts.

Configure H1, H2, and H3 with an IP address, subnet mask, and default gateway that is compatible with the IP address of the router default gateway interface address for the LAN to which they are attached.

Step 3: Verify end-to-end Network Layer connectivity.

a. On H1, open a Command Prompt window by choosing **Start > Run** and typing **cmd**. Alternatively, you can choose **Start > All programs > Accessories > Command Prompt**.

b. Use the **ping** command to test end-to-end connectivity. Ping from H1 on the R1 LAN to H3 on the R3 LAN (for example, 192.168.3.2).

```
C:\>ping 192.168.3.2
```

c. If H3 is not attached to R3, ping the R3 serial 0/0/1 interface IP address 172.16.1.2.

```
C:\>ping 172.16.1.2
```

d. If the pings are successful to R3, what does that indicate about the OSI layer connectivity between H1 and R3?

____

Note: If the pings are not successful, troubleshoot the router and host configurations and connections.

Task 2: Establish a Telnet Session from a Host Computer

Step 1: Telnet from H1 to remote router R2.

The Cisco router IOS software has built-in Telnet client and server software. Nearly all computer operating systems have a Telnet client. Many server operating systems also have a Telnet server, although Microsoft Windows desktop operating systems typically do not.

In many cases, you will not have direct access to a router through the console so that you can Telnet to other routers. Usually, you telnet to a router from a host computer. From there, you can Telnet to other routers that are accessible via the network.

a. From the command prompt on H1, telnet to the R2 router Fast Ethernet 0/0 interface.

```
C:\>telnet 192.168.2.1
```

b. Enter the password **cisco** to access the router.

c. What prompt did the router display? _____

d. Issue the **show version** command.

e. What is the Cisco IOS software version for the remote router R2? _______________

f. How many and what type of interfaces does remote router R2 have.? _____

g. If the Telnet from H1 to R2 is successful, what does that indicate about the OSI layer connectivity between the devices?

____

Step 2: End the Telnet session from H1 to remote router R2.

Exit the Telnet session from host H1 to R2 by typing **exit**.

Task 3: Perform Basic Telnet Operations Between the Routers

Step 1: Telnet from R1 to remote router R2.

Note: Telnet uses the vty lines on the remote router to connect. If the vty lines are not configured for login or there is no password set, you cannot connect to the remote router using Telnet.

a. Telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _______

Step 2: Look at the interfaces on remote router R2.

a. Issue the **show ip interface brief** command at the remote router prompt.

```
R2>show ip interface brief
```

b. List the interfaces that are up on remote router R2. ___________________________________

Step 3: Display the routing table on the remote router.

Issue the **show ip route** command at the router prompt. Which routes has R2 learned from RIP?

____

```
R2>show ip route
```

Step 4: Display the CDP neighbors for R2.

a. Use the Cisco Discovery Protocol (CDP) to view information about Cisco devices directly attached to R2. Enter the **show cdp neighbors** command at the router prompt.

b. List all device IDs that are connected to the remote router. What is the platform for each device?

____

```
R2>show cdp neighbors
```

Step 5: Suspend the current Telnet session on R2.

a. Press **Ctrl-Shift-6,** and then press the **x** key. This action only suspends the session and returns to the previous router. It does not disconnect from this router.

b. What prompt did the router display? _______

Step 6: Resume the Telnet session to R2.

a. Press the **Enter** key at the router prompt. What does the router respond with?

____

Pressing the **Enter** key resumes the Telnet session that was previously suspended.

b. What prompt did the router display? _______

Step 7: Close the Telnet session to R2.

a. Terminate the Telnet session by typing **exit**..

b. What does the router respond with? ____

c. What prompt did the router display? _______

Note: When the Telnet session is suspended, you can disconnect from that session using the **disconnect** command and the session number.

Task 4: Perform Telnet Operations Between Multiple Routers

Step 1: Telnet from R1 to remote router R2.

a. From R1, telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

b. Use the password **cisco** to enter the router.

Step 2: Establish an additional Telnet session from R2 to R3.

a. From R2, telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

b. Use the password **cisco** to access the router.

c. What prompt did the router display? _______

Step 3: Suspend the Telnet session to R3.

a. Press **Ctrl-Shift-6,** and then press the **x** key.

b. What prompt did the router display? _______

Step 4: View the active Telnet sessions.

Enter the **show sessions** command at the R1 command prompt. How many sessions are in use? _____

Note: The default session is indicated by an asterisk (*). This is the session that resumes when you press **Enter**.

```
R2>show sessions
```

Step 5: Resume the Telnet session to R2.

a. Press **Enter** at the router prompt. What does the router respond with?

____

b. What prompt did the router display? _______

c. Why does the prompt say R3? ____

Step 6: Disconnect the sessions from R1 to R2 and R3.

a. Enter the **exit** command at the R3 prompt, and then press **Enter** to close the connection to R3.

```
R3>exit
[Connection to 172.16.1.2 closed by foreign host]
R2>
```

b. Suspend the R2 session from R1 (session 1 on R1) by pressing **Ctrl-Shift-6,** followed by the **x** key. Use the **disconnect** command to end the connection to R2.

```
R1>disconnect 1
Closing connection to 10.10.10.2 [confirm]
```

Task 4: Remove the vty Password from R3

Step 1: Telnet from R1 to remote router R3.

a. Telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

```
R1>telnet 172.16.1.2
Trying 172.16.1.2 ... Open
User Access Verification
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _______

Step 2: From privileged EXEC mode on R3, remove the vty password.

a. Issue the **enable** command at the R3> command prompt, and enter the password **class**.

b. What prompt did the router display? _______

c. Remove the password for the vty lines on R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#no password
R3(config-line)#end
R3#
```

d. Exit from the Telnet session on R3, and return to R1.

```
R3#exit
[Connection to 172.16.1.2 closed by foreign host]
R1#
```

Step 3: Telnet from R1 to remote router R3 again.

a. Telnet to the IP address of the R3 serial 0/0/1 interface 172.16.1.2.

```
R1>telnet 172.16.1.2
```

b. Are you able to telnet to R3? _______

c. What message did you receive and why?

____

____

Step 4: Connect to R3 via the console and reset the vty password.

a. Issue the **enable** command at the R3> command prompt, and enter the password **class**.

b. Reestablish the password for the vty lines on R3.

```
R3>enable
R3#config t
R3(config)#line vty 0 4
R3(config-line)#password cisco
R3(config-line)#end
```

```
R3#
```

Part 2. Working with SSH to Verify Device Configurations and Connectivity

Secure Shell, or SSH, is an RSA-encrypted version of Telnet. All information, including user IDs, passwords, and data, that passes between an SSH client and SSH server is encrypted. Because SSH is an Application Layer protocol, a successful SSH connection demonstrates that all OSI layers are functioning, including encryption at the Presentation Layer.

Task 1: Configure SSH on Router R2

Step 1: Telnet from R1 to remote router R2.

a. Telnet to the IP address of the R2 serial 0/0/0 interface 10.10.10.2.

```
R1>telnet 10.10.10.2
Trying 10.10.10.2 ... Open
User Access Verification
Password:
```

b. Use the password **cisco** to enter the router.

c. What prompt did the router display? _______

Step 2: Configure the SSH server on R2.

a. Create a domain name and a Telnet/SSH user ID and password for remote vty connections.

Note: By creating a user ID and password and specifying local login for the vty lines, any attempt to telnet or SSH to this router requires entry of the username and password created.

Because the admin user has a privilege level of 15 (the highest), and privilege level 15 is configured for the vty lines, the router prompt goes directly into privileged EXEC (enable) mode when connecting to R2 using either Telnet or SSH.

The use of a special user ID and password to secure Telnet and SSH vty access to the router does not affect the console (line con 0) password or the enable secret password.

```
Router#config terminal
R2(config)#ip domain-name customer.com
R2(config)#username admin privilege 15 password 0 cisco123
R2(config)#exit
```

b. Configure the vty terminal lines to accept incoming remote connections from Telnet and SSH clients, and validate the user ID against the local router username database.

```
R2(config)#line vty 0 4
R2(config-line)#privilege level 15
R2(config-line)#login local
R2(config-line)#transport input telnet ssh
R2(config-line)#exit
```

Note: If Telnet is not specified in the **transport input** command above, only SSH remote connections will be allowed to this router.

c. 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.

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.customer.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
```

```
How many bits in the modulus [512] 768
% Generating 768 bit RSA keys, keys will be non-exportable...[OK]
*Mar 20 13:17:50.123: %SSH-5-ENABLED: SSH 1.99 has been enabled

R2(config)#exit
```

d. Verify that SSH is enabled and the version used with the **show ip ssh** command.

```
R2#show ip ssh
```

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

SSH version enabled ____________________
Authentication timeout ___________________
Authentication retries ____________________

f. Issue the **show running-config** command. What indication is there that the SSH server has been configured on R2? ____

____

g. Save the running-config to the startup-config.

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

h. Exit the Telnet session on R2, and return to R1.

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1#
```

Task 2: Log in to R2 Using the R1 CLI SSH Client

Note: You can also log in to an SSH-enabled router or switch using a computer with a GUI client, such as PuTTY. This procedure is described in Lab 8.3.4, “Configuring a Remote Router Using SSH.”

Step 1: Use the Cisco IOS CLI help feature with the ssh command.

From the R1 terminal session, use the Cisco IOS help feature to display the login options for the R1 SSH client.

```
R1#ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system

R1#ssh -l admin ?
  -c    Select encryption algorithm
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  WORD  IP address or hostname of a remote system
```

Step 2: Log in to R2 using SSH.

In this step, you log in to the R2 SSH server from the R1 CLI SSH client. You establish a secure remote session with R2 from which you can issue show and configuration commands.

a. Log in to R2 specifying the login username **admin** and password **cisco123,** which were configured earlier, and the IP address of the R2 S0/0/0 interface.

```
R1#ssh -l admin 10.10.10.2

Password:
Unauthorized Use Prohibited
R2#
```

b. Why did you get the privileged EXEC (enable) mode router prompt?

____

c. On R2, issue the **show ssh** command to see the SSH connections to the router.

```
R2#show ssh
Connection Version Mode Encryption   Hmac       State           Username
0          1.99     IN   aes128-cbc  hmac-sha1  Session started  admin
0          1.99     OUT  aes128-cbc  hmac-sha1  Session started  admin
%No SSHv1 server connections running.
```

d. Exit from the SSH session on R2, and return to R1

```
R2#exit
[Connection to 10.10.10.2 closed by foreign host]
R1>
```

Note: Ctrl-Shift-6 followed by the **x** key, and the commands used previously with Telnet, are the same for SSH.

Task 3: Reflection

a. **HTTP Connectivity** - You can also verify Application Layer connectivity using the HTTP interface for a router or switch. If the command **ip http server** is present in the device running config, you can open a browser on a computer that has network connectivity to the router or switch IP address (or name, if DNS is enabled) and access the HTTP GUI management application in the device. This can be a basic HTTP interface for non-SDM routers or it can be SDM and SDM Express for SDM-enabled routers. Because HTTP is an Application Layer protocol, a successful HTTP connection demonstrates that all OSI layers are functioning.

b. Compare the advantages and disadvantages of Telnet and SSH.

____

____

____

c. If you can ping to a router interface but cannot connect to it using Telnet or SSH, what could the problem be, and which layers of the OSI model are affected?

____

____

____

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Lab 9.6.2 Identifying Necessary Knowledge, Skills, and Abilities

Objectives

- Identify the knowledge, skills, and abilities needed to perform the tasks for a specific hands-on lab.

Background / Preparation

In this lab, you review an existing hands-on lab, which you completed in a previous chapter, and analyze it to identify the types of knowledge, skill, and abilities required to successfully complete the lab.

The following resources are required:

- Lab 5.3.8 Configuring PAT with SDM and Static NAT using Cisco IOS Commands

Step 1: Review the definitions for KSAs.

The CDC website (http://www.cdc.gov/hrmo/ksahowto.htm) describes the importance of KSAs (Knowledge, Skills, and Abilities) in the federal job application process. These concepts are equally applicable to networking job applicants.

a. Review the definitions of these terms from the CDC website:

Knowledge statements refer to an organized body of information usually of a factual or procedural nature which, if applied, make adequate performance on the job possible. A body of information applied directly to the performance of a function.

Skill statements refer to the proficient manual, verbal, or mental manipulation of data or things. Skills can be readily measured by a performance test where quantity and quality of performance are tested, usually within an established time limit. Examples of proficient manipulation of things are skill in typing or skill in operating a vehicle. Examples of proficient manipulation of data are skill in computation using decimals; skill in editing for transposed numbers, etc.

Ability statements refer to the power to perform an observable activity at the present time. This means that abilities have been evidenced through activities or behaviors that are similar to those required on the job, e.g., ability to plan and organize work. Abilities are different from aptitudes. Aptitudes are only the potential for performing the activity.

b. List at least one example for each term from your own networking or other area of personal experience.

Knowledge examples: ____

____

____

Skill examples: ____

____

____

Ability examples: ____

____

____

Step 2: Review an existing lab.

Locate Lab 5.3.8, “Configuring PAT with SDM and Static NAT using Cisco IOS Commands.” Read through the lab to become familiar with the tasks and steps performed. You may also review a different lab with the approval of the instructor.

Step 3: Identify the knowledge, skills, and abilities required for the lab.

The tasks and steps from the lab are listed in the following table. Fill in the table with the knowledge, skills, and abilities required to perform each step.

Task/Step	**Knowledge / Skills / Abilities Required**
Task 1: Configure basic router settings and PAT	N/A
Step 1: Build the network and configure host computer IP settings	
Step 2: Configure CustomerRouter basic settings with the Cisco IOS CLI	
Step 3: Configure the ISP router basic settings with the Cisco IOS CLI	
Step 4: Connect to CustomerRouter using SDM	
Step 5: Configure SDM to show Cisco IOS CLI commands.	
Step 6: Launch the Basic NAT wizard	
Step 7: Select the WAN interface for NAT	
Step 8: Verify NAT functionality	
Task 2: Configure and verify static NAT using the Cisco IOS CLI	N/A
Step 1: Configure a static mapping for the server	
Step 2: Test static NAT functionality	

Step 3: Save the router configurations	

Lab 9.6.5 Exploring the Cisco Learning Network

Objectives

- Use the Cisco Learning Network website to find study materials and tools to help prepare for the CCENT exam.
- Take an exam interface tutorial and a sample ICND1/CCENT exam.
- Use the tools discovered to help develop an exam preparation plan.

Background / Preparation

In this lab, you explore the Cisco Learning Network and identify some of the tools and resources that are available. You also take an exam interface tutorial and a sample ICND1/CCENT exam. You access the Cisco Career Certifications website for a description of the ICND1/CCENT exam and a list of exam topics. You describe the use of the tools and resources discovered to help develop your exam preparation plan.

Note: The CCENT exam is the same as the ICND1 exam. The ICND1 and ICND2 exams together equal the CCNA exam.

This lab requires a computer with a browser and Internet access.

Task 1: Identify the Tools and Resources Available

Step 1: Review Cisco and Cisco Press resources.

Investigate all the tools and resources that are available to help you study. The CCENT tests the knowledge and skills obtained during this course, and all the content from Discovery 1.

The Cisco Learning Network

Free of charge to anyone with a Cisco.com login. The Cisco Learning Network provides certification candidates with practice questions, labs, simulations, tips, discussion forums, CCNA videos, and advice from CCNA experts.

Cisco Press Exam Prep Books

Cisco Press publishes a number of books that cover the CCENT exam objectives. These titles can be purchased through the Cisco Marketplace Bookstore, directly from Cisco Press.

http://www.cisco.com/pcgi-bin/marketplace/welcome.pl?STORE_ID=CISCO_BOOKSTORE&KEYCODE=Certifications

http://www.ciscopress.com/markets/detail.asp?st=44711

Cisco Press CCNA Discovery Learning Guides

The Cisco Press Learning Guides for the Discovery 1 course, *Networking for Home and Small Business,* and the Discovery 2 course, *Working at a Small to Medium Business or ISP*, are also excellent sources of information. These books are the official supplemental textbooks for these courses and provide additional examples, challenge questions, and activities.

Step 2: Identify other sources of exam prep information.

a. Open a browser and use a search engine to search for “cisco ccent exam prep”. List some of the websites found here.

____

b. List the various resources, including Cisco and Cisco Press, that you plan to use for CCENT exam preparation.

Task 2: Explore the Cisco Learning Network Website

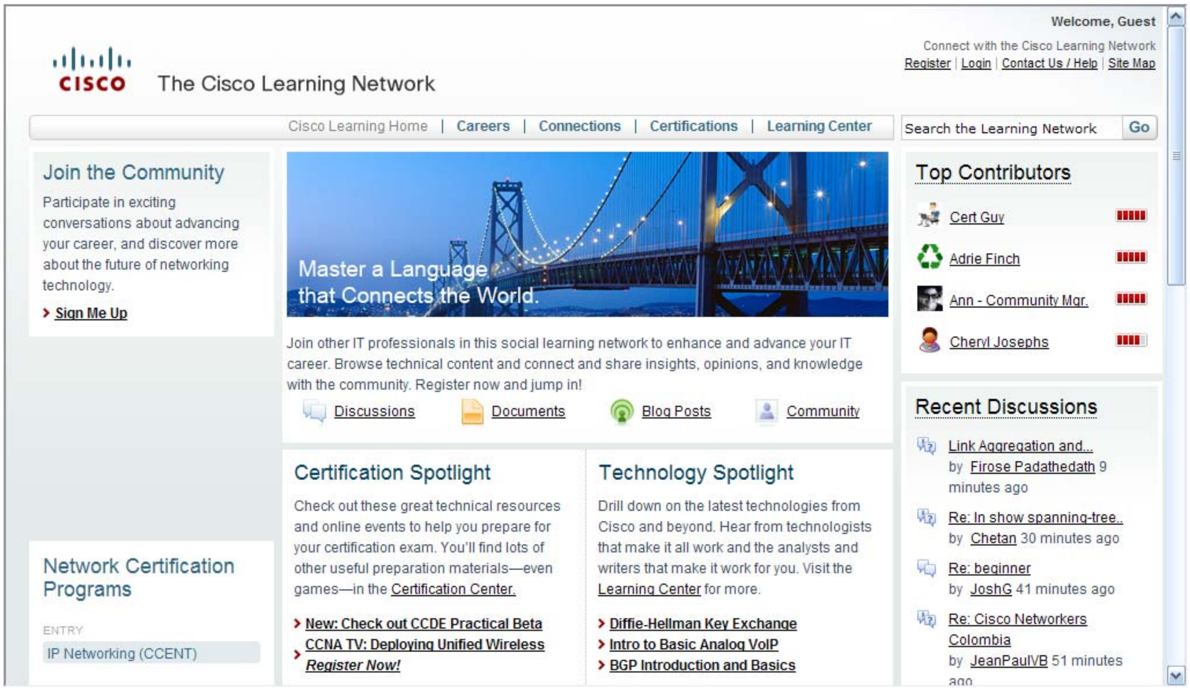
Step 1: Log in to the Cisco Learning Network website.

a. Registered Cisco.com users can access the website for help in preparing for CCNA certification exams.

http://www.cisco.com/go/learningnetwork

In the top right corner, click **Login**. You will be prompted to either enter your Cisco.com username and password or to create a new account.

b. Once authenticated, select the IP Networking (CCENT) link on the left side of the screen.



Welcome, Guest
Connect with the Cisco Learning Network
Register | Login | Contact Us / Help | Site Map

CISCO The Cisco Learning Network

Cisco Learning Home | Careers | Connections | Certifications | Learning Center

Search the Learning Network Go

Join the Community

Participate in exciting conversations about advancing your career, and discover more about the future of networking technology.

› Sign Me Up

Master a Language that Connects the World.

Join other IT professionals in this social learning network to enhance and advance your IT career. Browse technical content and connect and share insights, opinions, and knowledge with the community. Register now and jump in!

Discussions Documents Blog Posts Community

Top Contributors

Cert Guy
Adrie Finch
Ann - Community Mgr.
Cheryl Josephs

Recent Discussions

Link Aggregation and...
by Firose Padathedath 9 minutes ago

Re: In show spanning-tree..
by Chetan 30 minutes ago

Re: beginner
by JoshG 41 minutes ago

Re: Cisco Networkers Colombia
by JeanPaulVB 51 minutes ago

Certification Spotlight

Check out these great technical resources and online events to help you prepare for your certification exam. You'll find lots of other useful preparation materials—even games—in the Certification Center.

› New: Check out CCDE Practical Beta
› CCNA TV: Deploying Unified Wireless *Register Now!*

Technology Spotlight

Drill down on the latest technologies from Cisco and beyond. Hear from technologists that make it all work and the analysts and writers that make it work for you. Visit the Learning Center for more.

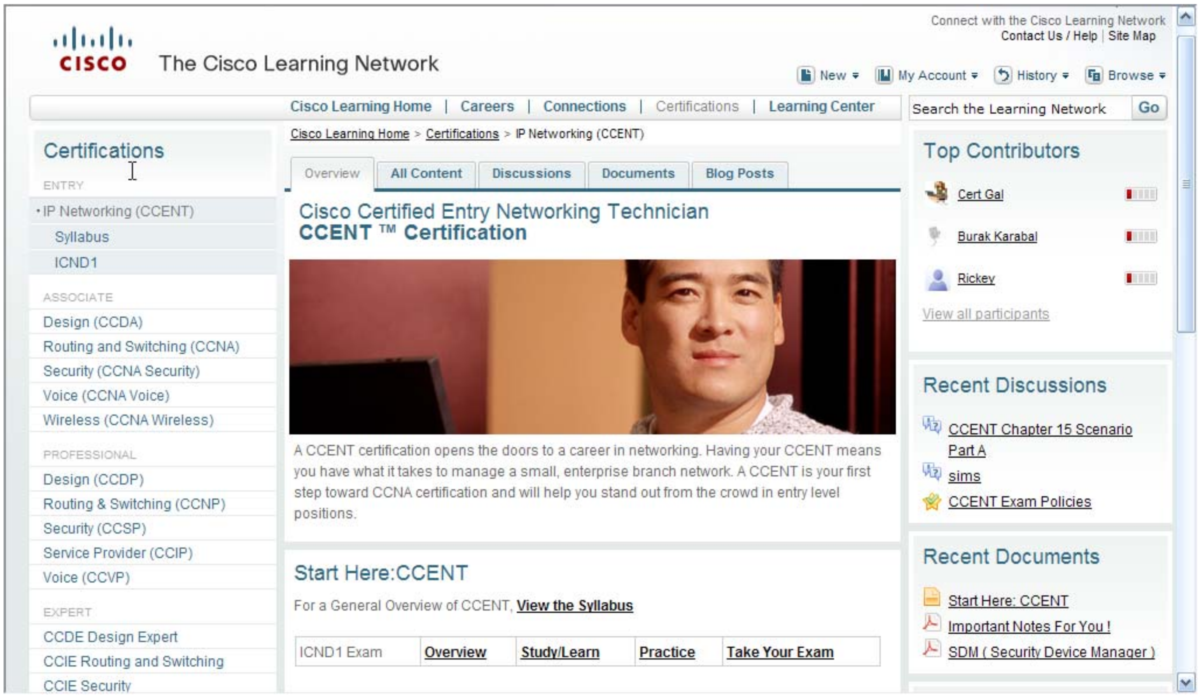
› Diffie-Hellman Key Exchange
› Intro to Basic Analog VoIP
› BGP Introduction and Basics

Network Certification Programs

ENTRY
IP Networking (CCENT)

Step 2: Identify the various resources available.

a. Examine the CCENT area of the Cisco Learning Network.



Cisco Certified Entry Networking Technician
CCENT ™ Certification

A CCENT certification opens the doors to a career in networking. Having your CCENT means you have what it takes to manage a small, enterprise branch network. A CCENT is your first step toward CCNA certification and will help you stand out from the crowd in entry level positions.

Start Here:CCENT

For a General Overview of CCENT, **View the Syllabus**

ICND1 Exam	**Overview**	**Study/Learn**	**Practice**	**Take Your Exam**

b. What are the main options available to help with exam preparation?

Step 3: Explore various resource topics.

a. Click the **Discussions** tab. What are some of the topics being discussed?

b. Click the **Documents** tab. What are some of the available documents?

c. Return to the **Overview** tab and then click on the **Study / Learn** link. What are some of the main areas included here?

d. What are some of the modules that are available under the **Quick Learning Modules** heading?

____

____

e. Click the **IPTV Video Archive** link. What are some of the shows that can be selected?

____

____

f. Are all the videos listed appropriate CCENT study topics?

____

____

g. Click the **Practice** tab. What are the main areas contained on this page?

____

____

h. Click on the **Games Arcade** link. What are some of the games that are available?

____

____

i. Which of these games could be part of your ICND1/CCENT exam preparation plan?

____

____

Task 3: Explore the Practice Area and Take Practice Exams

Step 1: Identify topics and take the Exam Interface Tutorial.

a. Click the **Practice** tab.

b. Under **Example of Exam Environment**, click **Exam Interface Tutorial.** The Cisco Learning and Assessment Team has developed this tutorial to help prepare for the Cisco certification exams.

c. Go though the tutorial to see the various types of questions that can appear on the CCENT and CCNA exams.

d. What are the different types of questions presented?

____

____

____

Step 2: Take a practice ICND1/CCENT exam.

a. Under the **Practice Questions** heading, how many ICND1 test modules are there? __________

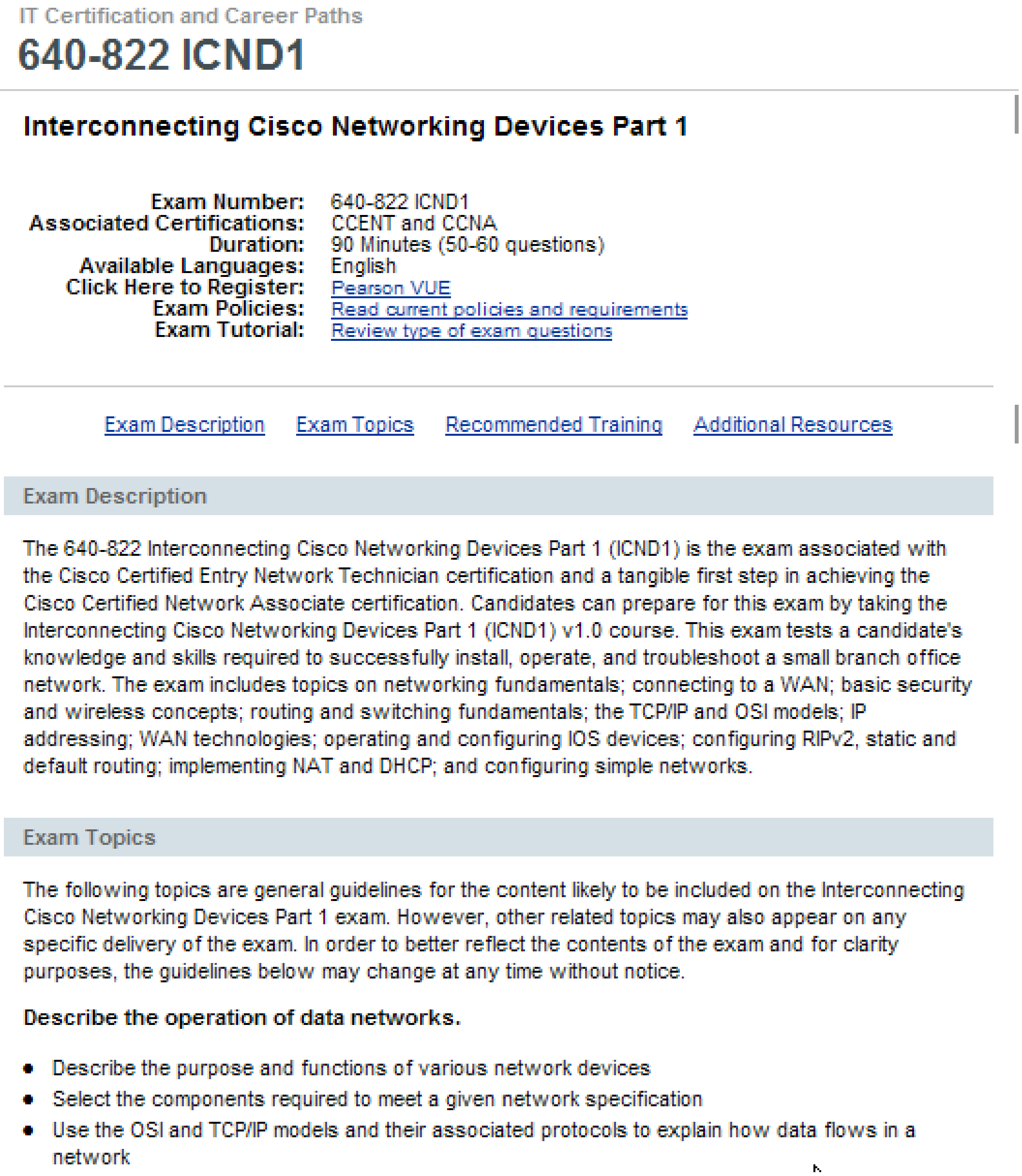
b. Click ICND1, Module 1 to start the practice questions for the first module. The correct answers and solutions are located in the Module Self-Check Answer Key. How many questions are there? ______ How many answers did you get correct? _________

c. If time permits, take the other ICND1 module practice questions.

Step 3: View the ICND1/CCENT exam descriptions and exam topics.

a. From the **Cisco Learning Network** main screen, click the **IP Networking (CCENT)** link, and then click the **ICND1** link. The **640-822 ICND1** screen appears. It contains a description of the exam and a list of exam topics. You can also register to take the exam at an approved testing center by clicking on the **Pearson VUE** link.

Note: The following screen shot only shows a portion of the exam topics.



IT Certification and Career Paths

640-822 ICND1

Interconnecting Cisco Networking Devices Part 1

Exam Number:	640-822 ICND1
Associated Certifications:	CCENT and CCNA
Duration:	90 Minutes (50-60 questions)
Available Languages:	English
Click Here to Register:	Pearson VUE
Exam Policies:	Read current policies and requirements
Exam Tutorial:	Review type of exam questions

Exam Description   Exam Topics   Recommended Training   Additional Resources

Exam Description

The 640-822 Interconnecting Cisco Networking Devices Part 1 (ICND1) is the exam associated with the Cisco Certified Entry Network Technician certification and a tangible first step in achieving the Cisco Certified Network Associate certification. Candidates can prepare for this exam by taking the Interconnecting Cisco Networking Devices Part 1 (ICND1) v1.0 course. This exam tests a candidate's knowledge and skills required to successfully install, operate, and troubleshoot a small branch office network. The exam includes topics on networking fundamentals; connecting to a WAN; basic security and wireless concepts; routing and switching fundamentals; the TCP/IP and OSI models; IP addressing; WAN technologies; operating and configuring IOS devices; configuring RIPv2, static and default routing; implementing NAT and DHCP; and configuring simple networks.

Exam Topics

The following topics are general guidelines for the content likely to be included on the Interconnecting Cisco Networking Devices Part 1 exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

Describe the operation of data networks.

- Describe the purpose and functions of various network devices
- Select the components required to meet a given network specification
- Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network

b. What is the length of the exam? __________

c. What are some of the main topic areas covered?

____

____

____

Task 4: Reflection

What is the benefit of taking the exam interface tutorial and sample exam questions?

____

____

____

How will you use the tools identified in your exam preparation plan?

____

____

____

Lab 9.6.6 Preparing for the ICND1 Exam

Objectives:

- Determine what activities you can give up or cut back to make time to prepare for the exam.
- Create a schedule to guide your exam preparation.
- Schedule the exam and visit the testing center.

Background / Preparation

In this lab, you determine how much time you have available to dedicate to preparing for the ICND1 exam, prioritize your activities, and schedule your preparation and exam.

Note: The CCENT exam is the same as the ICND1 exam. The ICND1 and ICND2 exams together equal the CCNA exam.

Task 1: Use the checklist to begin your exam preparation.

Step 1: Prioritize your activities. Complete? ___________

Task 2 in this lab can help you record how you spend your time each week. Once your activities are known, prioritize them in order to determine what activities you can give up or cut back to make time for exam preparation.

Step 2: Create an Exam Preparation Schedule Complete? ___________

Task 3 in this lab describes how to create a schedule for your exam preparation.

Step 2: Determine your study space. Complete? ___________

Decide where you will study for the exam. If you plan on preparing at home, ensure that you have a quiet, uncluttered place to work where you will not be distracted by noise or household activity.

Step 3: Obtain necessary resources. Complete? ___________

If you decide to use additional material, such as Cisco Press Books or sample exams, be sure that you obtain them before beginning your preparation. Also make sure you have access to the online curriculum and have Packet Tracer loaded on your computer.

Step 4: Inform your friends and family. Complete? ___________

Friends and family can be helpful during your exam preparation. They can assist you in your studies, or help ensure that you have ample uninterrupted study time to prepare.

Task 2: Record how you spend your time for one week.

Step 1: Using the calendar worksheet included in this lab, record how much time you spend each day on the listed activities.

a. The worksheet lists activities and responsibilities that are normally performed during the week. On each day, record the amount of time you spend on each activity. Blank lines are provided for activities that are not listed.

b. At the end of the week, total up the time you spent on each activity.

Example:

Activity	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Total
General Living (eating, sleeping, personal hygiene)	12	12	12	12	12	12	12	84
Attend School	7	7	7	7	7			35
Homework	1	1	1	1	1	1		6
Sports	2		2		2			6
Work/Chores	1	1	1	1	1	4	4	13
Social Activities (attending church, clubs, meetings, etc.)						2	2	4
Entertainment (watching TV, reading, attending sporting events, etc.)	1	1	1	1	1	5	6	16

Step 2: Prioritize your activities.

a. Use the chart to assign a priority to each of your listed activities. Priorities are high, medium, and low. If an activity is very important to you, or is a required activity (such as attending school), assign it a high priority. Medium priority activities are those that you feel improve your quality of life. Low priority activities are those activities that you do when there is nothing else to do.

b. Determine what priority preparing for the ICND1 exam has in your life. There is no right or wrong answer, think about this question and answer honestly.

c. Once you have assigned priorities to the activities, total the hours that you spend doing low and medium priority activities. Determine how many of these hours each week you can dedicate to preparing for the exam.

Example:

Activity	Hours per Week	Priority		
Attend School	35	[✓ High]	Medium	Low
Part-time Job	10	[✓ High]	Medium	Low
Sports	6	[✓ High]	Medium	Low
Work/Chores	13	[✓ High]	Medium	Low
Social Activities	4	High	[✓ Medium]	Low
Entertainment	16	High	Medium	[✓ Low]
Preparing for the ICND1 exam	??	High	[✓ Medium]	Low

In the example, the student assigns a low priority to the time spent on Entertainment Activities. Some of this time each week can be devoted to preparing for the ICND1 Exam. The amount of time depends on the priority that passing the exam has in relation to the other activities. The example student decides to spend 6 hours a week on studying for the exam, 1 hour on Monday, Tuesday and Thursday, and 3 hours on Saturday morning. If the preparation had a high priority, the student might schedule 10 or more hours a week to prepare.

What activity or activities can you give up in order to devote time to preparing to take the ICND1 exam?

____

____

How much time can you schedule each week to prepare? On which days can you dedicate time?

____

____

Task 3: Plan your CCENT Preparation Time.

Step 1: Use the CCENT study guides included with this chapter, or the 31 Days to the CCENT Cisco Press Book to organize your study.

a. Discuss with your instructor ways to complete your lab review. It may be possible to reserve time in the school lab, or to access equipment remotely. Consider equipment availability when you make your exam preparation schedule.

b. Use a calendar to record the study times. On each day that you schedule time for study, list the topic or topics that you want to review on that day. If you plan to review labs or Packet Tracer activities, ensure that you have enough time available to complete the activity. Continue until all of the topics are scheduled for review.

c. As you complete the review of each topic, make a note of how confident you feel with the material. During the last week before your exam, review the topics that you were unsure of during your preparation.

Step 2: Schedule your exam and visit the testing center.

a. Schedule the exam for the week after you complete your review.

b. Visit the testing center and learn about the testing procedures.

Reflection:

Why do you think it is important to list and prioritize your weekly activities before scheduling your exam?

____

____

What is the benefit of creating a schedule to organize your study activities?

____

____

Activity Worksheet

Activity	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Total
General Living (eating, sleeping, personal hygiene)								
Attend School								
Homework								
Sports								
Work/Chores								
Social Activities (attending church, clubs, meetings, etc.)								
Entertainment (watching TV, reading, attending sporting events, etc.)								

Priority Worksheet

Activity	Hours per Week	Priority
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
		High Medium Low
Preparing for the ICND1 exam		High Medium Low

Calendar Worksheet (Print at least two copies.)

Month ______________________

S	M	T	W	T	F	S

CCNA Discovery
Working at a Small-to-Medium Business or ISP

Summary Lab 10.0.1 Putting It All Together

Objectives

- Create an IP addressing plan for a small network.
- Implement a network equipment upgrade.
- Verify device configurations and network connectivity.
- Configure switch port security.

Background / Preparation

In this activity, you play the role of an on-site installation and support technician from an ISP. You receive a work order specifying your responsibilities, which include analyzing the existing network configuration of the customer and implementing a new configuration to improve network performance. You use additional equipment as necessary, and develop an IP subnetting scheme to address the customer needs. On an earlier site visit, one of the ISP technicians had created a diagram of the existing network as shown below.

Required Resources

The following equipment is required:

- ISP router with two serial interfaces and one Fast Ethernet interface (preconfigured by instructor)
- Ethernet 2960 switch to connect to the ISP router (preconfigured by instructor)
- Customer 1841 router (or other router with two Fast Ethernet 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 hosts
- Windows XP-based host to act as a wireless client (wireless NIC)
- Windows XP-based host to act as a wired client (Ethernet NIC)
- Category 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

You have received the following work order from the 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 the 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 to support wireless users.

The wired and wireless client traffic from each subnet is routed through the new 1841 customer router. RIPv2 is to be used between the 1841 and the ISP, and the encapsulation on the WAN link between them is PPP. The customer router must use a static address. The ISP router serial interface IP address it must communicate with is: ___________________________________

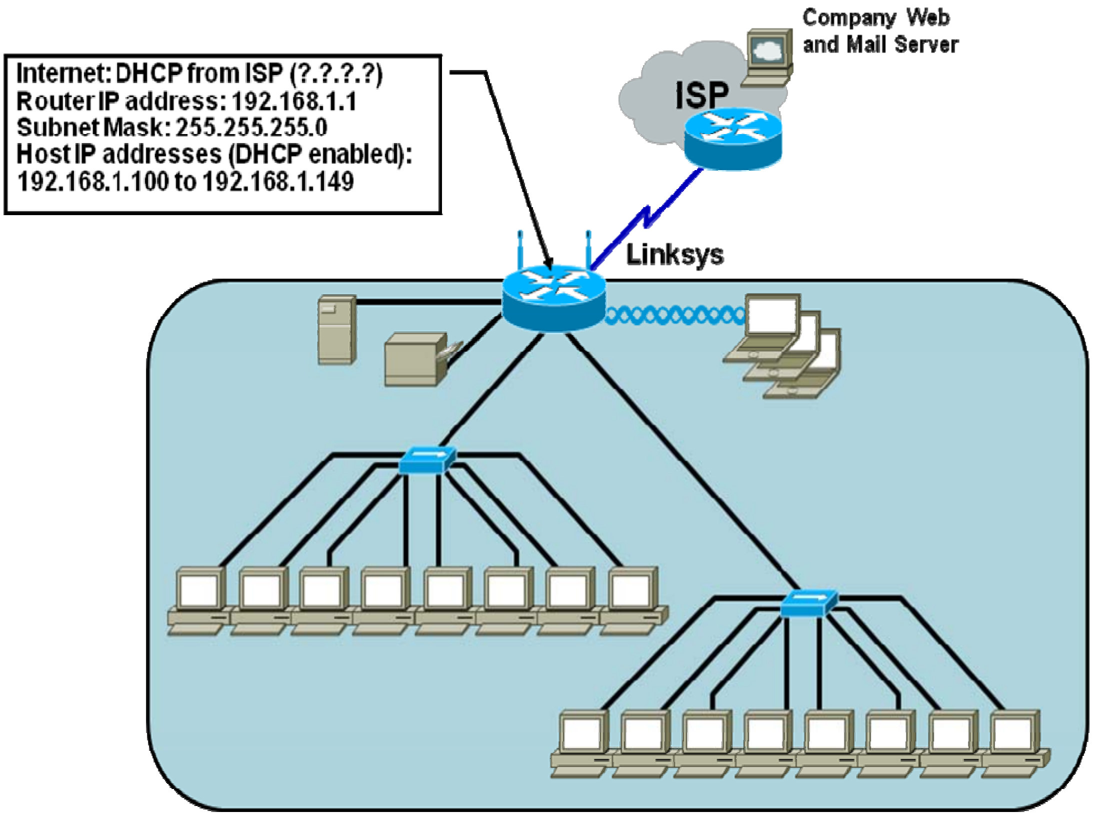
If your local network is connected to the ISP as AnyCompany1, the IP address of the ISP serial 0/0/0 interface is 10.100.1.5 /22.

If your local network is connected to the ISP as AnyCompany2, the IP address of the ISP serial 0/0/1 interface is 172.27.100.25 /22.

Assigned to: **Approved by:**

Guy Netwiz Bill Broadband, ISP Manager

Existing Network of the Customer



Internet: DHCP from ISP (?.?.?.?)
Router IP address: 192.168.1.1
Subnet Mask: 255.255.255.0
Host IP addresses (DHCP enabled):
192.168.1.100 to 192.168.1.149

Part B – Develop the Subnet Scheme

The customer has been assigned an IP address and subnet mask ______________________________

If the local network customer is AnyCompany1, use 192.168.111.0 /24.

If the local network customer is AnyCompany2, use 192.168.222.0 /24.

Develop a subnet scheme with this address that allows the customer network to support two subnets of up to 30 clients each, and allow for growth to as many as six subnets in the future.

The first subnet is for the wired clients. The second subnet is used to assign an IP address to the Linksys external Internet interface. The internal wireless network clients use the default IP addressing (network 192.168.1.0 /24) assigned by the Linksys. The Linksys uses NAT/PAT to convert internal wireless client addresses to the external address. The internal wireless clients do not require a subnet from the base address.

Step 1: Determine the number of hosts and subnets.

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.

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.

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

Step 3: Identify subnet and host IP addresses.

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.

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.

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 is 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.

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.

In the space provided here, draw a physical network diagram, showing all network devices, hosts, 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 it is in the factory default state.

b. If using SDM to configure basic settings, use the Reset to Factory Defaults option from the SDM main menu. Also verify that the router has SDM version 2.4 or later installed. If not, contact the instructor.

c. If using the Cisco 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 on an SDM router, SDM no longer comes up by default when the router is restarted. It is then necessary to build a basic config. Contact the instructor if this is the case.

Step 2: Configure the 1841 customer router.

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.

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 / 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 Fast Ethernet interface 0/0	IP Addr: ____________________ SN mask: ___________________	
	Configure Fast Ethernet 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 RIPv2 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. Set the router internal IP address to 192.168.1.1, with a subnet mask of 255.255.255.0. The DHCP address range is 192.168.1.100 through 192.168.1.149. All security settings are set to the default, with no MAC filtering, and so on.

b. If necessary, reset the ISR using the **Administration** tab and the **Factory Defaults** option.

c. Change the default Service Set Identifier (SSID) of the Linksys to AnyCompany1 (or AnyCopmany2) and ensure that it is broadcast.

Step 4: Verify the default settings for the 2960 switch.

Log in to the switch and verify that it is in the factory default state. Use the Cisco 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 that the hosts are DHCP clients.

Use the **Control Panel > Network Connections** option to verify that both the wired and wireless hosts are set to obtain their IP addresses automatically via DHCP.

Part E – Connect Network Devices and Verify Connectivity

Step 1: Connect the network devices.

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 the wired host to switch			
	Connect the wireless host to Linksys SSID entered in Part D, Step 3			

Step 2: Verify device configurations and network connectivity.

Use the following checklist to verify the IP configuration of each host and test network connectivity. 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 host, display the IP address, subnet mask, and default gateway	
	From command prompt of wireless host, display the IP address, subnet mask, and default gateway.	
	Log in to Linksys GUI from wireless host and record the LAN IP address and subnet mask, Internet IP address, 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.	

Part F – Configure Port Security for the Switch

Step 1: Display the MAC address table entry for the port to which the wired host is connected.

Use the **show mac-address-table int fa0/*X*** command, where *X* is the port number to which the wired host is connected. You may need to ping from the host to the router default gateway IP address to refresh the MAC address table entry. In this example, the port number is Fa0/2.

```
S1#show mac-address-table int f0/2
          Mac Address Table

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  1    000b.db04.a5cd    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 1
```

Step 2: Clear the dynamically learned MAC address entry.

Issue the **clear mac-address-table dynamic interface fa0/*X*** command, where *X* is the port number to which the wired host is attached.

Step 3: Shut down the port, configure it as an access port, and then issue the port security commands.

The **switchport port-security** command enables security on the port using the defaults. The defaults are one allowed MAC address, and shutdown is the violation action to be taken.

The **switchport port-security mac-address sticky** command allows the switch to learn the MAC address currently associated with the port. This address becomes part of the running configuration. If the running–config is saved to the startup-config, the MAC address is retained when the switch is reloaded.

To setup sticky port security perform the following steps:

First shut down the port to which the wired host is attached.

Use the **switchport mode access** command to force the port to be an access port to configure port security.

Use the **switchport port-security** command to enable port security

Use the **switchport port-security mac-address sticky** command to enable the port to learn the MAC address of the connected host.

Finally, enter the **no shutdown** command to re-enable the port so that it can learn the MAC address of the host.

Step 4: Ping from the wired host to the AnyCompanyX router default gateway.

Allow some time to pass and then issue the **show running-config interface Fa0/*X*** command to see the MAC address that the switch learned. Replace the *X* with the port number to which the wired host is attached.

Step 5: Display the port security using the show port-security interface command.

Issue the **show port-security interface Fa0/*X*** command, and replace the *X* with the port number to which the wired host is attached.

What is the port status? ____

What is the security violation count? ______________________________

What is the source Address? ________________________________

Step 6: Remove the wired host cable from the switch port and connect the cable from another PC.

a. Ping from the new wired host to any IP address to cause a security violation on port Fa0/X. You should see security violation messages.

b. Issue the **show port-security interface** command again for Fa0/X.

What is the port status? ____

What is the security violation count? ______________________________

What is the source address? ________________________________

Step 7: Reconnect the original host to its port and restore the port.

a. Clear the sticky address entry for port Fa0/X using the command **clear port-security sticky interface fa0/*X* access**. Replace the *X* with the port number to which the wired host is attached.

b. To return the interface from **error disable** to **administratively up**, enter the **shutdown** command followed by the **no shutdown** command.

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: To find out exactly how the router is configured, look at the interfaces. The interface identifies the type of router and how many interfaces the router has. There is no way to effectively list all 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 information in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

CCNA Discovery 4.1.3 Working at a Small to Medium Business or ISP - Hands-on Labs / CCENT Objectives Map

Lab#	Title	Objectives	CCENT/ICND1 Cert Objectives
1.2.3	Mapping ISP Connectivity Using Traceroute	• 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.	802.1.8 Determine the path between two hosts across a network. 802.1.10 Identify and correct common network problems at layers 1, 2, 3 and 7 using a layered model approach.
3.2.4	Evaluating a Cabling Upgrade Plan	• Examine the existing floor plan of a customer. • Propose a cable upgrade plan to accommodate extra floor space.	802.2.1 Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts. 802.4.3 Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts.
4.1.5	Subnetting a Network	• Create an IP addressing plan for a small network.	802.3.2 Create and apply an addressing scheme to a network. 802.3.3 Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment.
4.2.4	Determining PAT Translations	• 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).	802.3.4 Explain the basic uses and operation of NAT in a small network connecting to one ISP.

5.1.3	Powering up an Integrated Services Router	• 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. • Display router configuration information using the show running-config and show startup-config commands and restart the router using the reload command. • Display router system, Cisco IOS software and configuration register information using the show version command.	802.4.2 Describe the operation of Cisco routers (router bootup process, POST, router components).
5.2.3	Configuring an ISR with SDM Express	• 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.	802.4.11 Implement password and physical security (no SDM basic router configuration objective).
5.2.4	Configuring Dynamic NAT with SDM	• Configure Network Address Translation (NAT) using Port Address Translation (PAT) on a Cisco ISR router with the Cisco SDM Basic NAT Wizard.	802.3.7 Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI and ping.
5.3.5	Configuring Basic Router Settings with IOS CLI	• Configure the device host name for a router. • Configure console, privileged mode and vty passwords. • Configure Ethernet and Serial interfaces, including description. • Configure a message of the day (MOTD) banner. • Configure the routers to not perform domain lookup of host names. • Configure synchronous console logging. • Verify connectivity between hosts and routers.	802.4.3 Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts. 802.4.5 Access and utilize the router CLI to set basic parameters. 802.4.6 Connect, configure, and verify operation status of a device interface.
5.3.7	Configuring DHCP with SDM and the Cisco IOS CLI	• Configure a Customer router for DHCP using SDM. • Configure a Customer router for DHCP using IOS CLI. • Configure a DHCP client. • Verify DHCP functionality.	802.3.8 Configure, verify and troubleshoot DHCP and DNS operation on a router (CLI/SDM).

5.3.8	Configuring PAT with SDM and Static NAT using Cisco IOS Commands	• Configure basic router settings using the Cisco IOS CLI. • Configure NAT Port Address Translation (PAT) using the Cisco SDM Basic NAT Wizard. • Verify NAT translations using IOS show Commands. • Configure static NAT using Cisco IOS commands.	802.3.4 Explain the basic uses and operation of NAT in a small network connecting to one ISP. 802.3.7 Enable NAT for a small network with a single ISP and connection using SDM and verify operation using CLI and ping. 802.3.9 Implement static and dynamic addressing services for hosts in a LAN environment.
5.3.9a	Managing Router Configuration Files Using HyperTerminal	• Establish a HyperTerminal session with a router and use it to capture and save the running configuration as a text file for use as a backup. • Edit the file using the Notepad text editor and use HyperTerminal to restore the backup configuration router. • Modify the file using Notepad and use HyperTerminal to transfer the file and configure a different router. Verify network connectivity.	802.4.9 Manage IOS configuration files (save, edit, upgrade, restore).
5.3.9b	Managing Router Configuration Files Using TFTP	• Download and Install TFTP server software. • Use TFTP to copy the router running configuration to the TFTP server. • Edit the file using the Notepad text editor. • Copy the new configuration from the TFTP server to the router.	802.4.9 Manage IOS configuration files (save, edit, upgrade, restore).
5.4.3	Planning a WAN Upgrade	• Create a business proposal based on a scenario of an organization that requires a WAN upgrade.	802.1.11 Differentiate between LAN/WAN operation and features. 802.8.1 Describe different methods for connecting to a WAN.
5.5.2	Powering Up a Switch	• 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 switch.	802.2.4 Explain the operation of Cisco switches and basic switching concepts.

5.5.4	Configuring the Cisco 2960 Switch	- 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. - Verify network connectivity. - Configure basic port security. - Configure port duplex and speed settings.	802.2.5 Perform, save and verify initial switch configuration tasks including remote access management. 802.2.6 Verify network status and switch operation using basic utilities (ping, traceroute, Telnet, SSH, ARP, ipconfig), SHOW & DEBUG commands. 802.2.7 Implement and verify basic security for a switch (port security, deactivate ports).
6.1.2	Creating a Network Diagram from Routing Tables	- 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.	802.1.7 Interpret network diagrams
6.1.5	Configuring and Verifying RIP	- Implement RIP routing and verify that network routes are being exchanged dynamically.	802.4.4 Configure, verify, and troubleshoot RIPv2.
6.2.4	Configuring BGP with Default Routing	- 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 AS100 and ISP2 in AS 200.	802.4.8 Perform and verify routing configuration tasks for a static or default route given specific routing requirements.
7.3.1	Editing the HOSTS File in Windows	- Edit the local HOSTS file on a Windows PC to map a name to an IP address for easier identification.	No ICND1/CCENT requirements specified.
7.3.3a	Examining Cached DNS Information on a DNS Server	- View the cached DNS information on a Windows DNS server after making a DNS request that is looked up.	802.3.5 Describe and verify DNS operation.
7.3.3b	Creating Primary and Secondary Forward Lookup Zones	- Create primary and secondary forward lookup zones on Windows DNS servers.	802.3.5 Describe and verify DNS operation.
8.1.3	Securing Local Data and Transmitted Data	- 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.	802.6.2 Explain general methods to mitigate common security threats to network devices, hosts, and applications. 802.6.4 Describe security recommended practices including initial steps to secure network devices.

8.2.1.	Planning for Access Control Lists and Port Filters	• Based on the predefined network diagram, determine where to implement access lists and port filters to help protect the network	802.6.2 Explain general methods to mitigate common security threats to network devices, hosts, and applications. 802.6.4 Describe security recommended practices including initial steps to secure network device.
8.2.5	Researching an Anti-X Software Product	• Research an Anti-X software package that meets the requirements for a small business.	802.6.2 Explain general methods to mitigate common security threats to network devices, hosts, and applications. 802.6.3 Describe the functions of common security appliances and applications. 802.6.4 Describe security recommended practices including initial steps to secure network devices.
8.3.1	Interpreting a Service Level Agreement	• 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.	No ICND1/CCENT requirements specified.
8.3.2	Conducting a Network Capture with Wireshark	• 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.	802.1.3 Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network.
8.3.3a	Managing Remote Network Devices with Telnet	• Establish a Telnet connection to a remote router. • Verify that the application layer between source and destination is working properly. • Retrieve information about remote routers using show commands. Retrieve CDP information from routers not directly connected. Suspend and reestablish a Telnet session. • Disconnect a Telnet session. • Engage in multiple Telnet sessions. • Display active Telnet sessions.	802.4.7 Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities. 802.4.12 Verify network status and router operation using basic utilities (ping, traceroute, Telnet, SSH, arp and ipconfig), including SHOW & DEBUG commands.

8.3.3b	Configuring a Remote Router Using SSH	• Use SDM to 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. • Configure a non-SDM router for SSH using the Cisco IOS CLI	802.4.7 Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities.
8.4.2	Planning a Backup Solution	• Based on the business scenario, plan an appropriate backup solution	No ICND1/CCENT requirements specified.
8.4.3a	Managing Cisco IOS images with TFTP	• Analyze the IOS image and router Flash memory. • Use TFTP to copy the IOS software image from a router to a tftp server. • Reload the backup IOS software image from a TFTP server into flash on a router.	802.4.10 Manage Cisco IOS.
8.4.3b	Managing Cisco IOS images with ROMMON and TFTP	• Analyze the IOS image and router Flash memory. • Backup an IOS software image to a TFTP server. • Use ROM monitor (ROMmon) and tftpdnld to restore an IOS software image from a TFTP server.	802.4.10 Manage Cisco IOS.
9.1.1	Organizing CCENT Objectives by OSI Layer	• Organize the CCENT objectives by which layer or layers they address.	802.1.5 Describe the purpose and basic operation of the protocols in the OSI and TCP models.
9.1.3	Use Wireshark to observe the TCP three-way handshake.	• Use Wireshark to monitor an Ethernet interface for recording packet flows. • Generate a TCP connection using a web browser. • Observe the initial TCP/IP three-way handshake.	802.1.3 Use the OSI and TCP/IP models and their associated protocols to explain how data flows in a network.
9.2.3	Identifying Cabling and Media Errors	• Identify Ethernet device and cabling connectivity. • Build a simple, routed multi-LAN network and verify connectivity. • Use the show interfaces and show ip interface Cisco IOS commands to observe the symptoms when using the wrong cable.	802.2.1 Select the appropriate media, cables, ports, and connectors to connect switches to other network devices and hosts.
9.2.4	Troubleshooting LAN Connectivity	• Build a simple, switched network and verify connectivity. • Troubleshoot LAN connectivity using the LEDs and show commands to find link problems and duplex and speed mismatches.	802.2.8 Identify, prescribe, and resolve common switched network media issues, configuration issues, autonegotiation, and switch hardware failure.

9.2.5	Troubleshooting WAN Connectivity	• Build a multi-router network and verify connectivity. • Troubleshoot WAN connectivity using the LEDs and show commands to find link problems and encapsulation and timing mismatches.	802.4.3 Select the appropriate media, cables, ports, and connectors to connect routers to other network devices and hosts. 802.4.7 Verify device configuration and network connectivity using ping, traceroute, telnet, SSH or other utilities.
9.3.3	Designing an IP Subnetting Scheme for Growth	• Analyze the subnetting requirements for a small company with multiple networks. • Design a subnetting scheme that allows for 20% growth in the number of subnets and the number of hosts per subnet. • Develop an IP addressing plan to apply addresses to networking devices and host computers.	802.3.2 Create and apply an addressing scheme to a network.
9.4.2	Correcting RIPv2 routing problems	• Cable a network according to the topology diagram. • Load the routers with supplied scripts. • Gather information about the non-converged portion of the network, along with any other errors. • Analyze information using Cisco IOS show and debug commands to determine network errors. • Propose solutions to network errors. Implement solutions to network errors. • Document the corrected network.	802.3.10 Identify and correct IP addressing issues. 802.4.4 Configure, verify, and troubleshoot RIPv2.
9.5.3	Using Telnet and SSH to access networking devices	• Establish and manage Telnet connections to a remote router and switch. • Verify that the Application Layer between the source and destination is working properly. • Retrieve information about remote routers using show commands. • Configure a router to accept SSH connections using the Cisco IOS CLI. • Connect from one router using the SSH CLI client to a remote router running the SSH server.	802.4.7 Verify device configuration and network connectivity using ping, traceroute, Telnet, SSH or other utilities. 802.4.12 Verify network status and router operation using basic utilities (ping, traceroute, telnet, SSH, arp, ipconfig), including SHOW & DEBUG commands.

9.6.2	Identifying Necessary Knowledge, Skills and Abilities	• Identify the knowledge, skills, and abilities needed to perform the tasks for a specific hands-on lab	No ICND1/CCENT requirements specified.
9.6.5	Exploring the CCNA Prep Center	• Use the Cisco CCNA Prep Center website to find study materials and tools to help prepare for the CCENT exam. • Take an exam interface tutorial and a sample ICND1/CCENT exam. • Use the tools discovered to help develop an exam preparation plan.	No ICND1/CCENT requirements specified.
10.0.1	Putting It All Together	• Given a customer work order, implement a network upgrade. • Review an existing customer network. • Create an IP addressing scheme for the upgraded network. • Create a physical diagram of the new network. • Configure ISR router and Linksys. Verify device configurations and network connectivity.	802.1.7 Interpret network diagram. 802.3.2 Create and apply an addressing scheme to a network. 802.3.3 Assign and verify valid IP addresses to hosts, servers, and networking devices in a LAN environment. 802.4.12 Verify network status and router operation using basic utilities (ping, traceroute, Telnet, SSH, ARP, ipconfig), including SHOW & DEBUG commands. 802.5.3 Identify the basic parameters to configure on a wireless network to ensure that devices connect to the correct access point.