



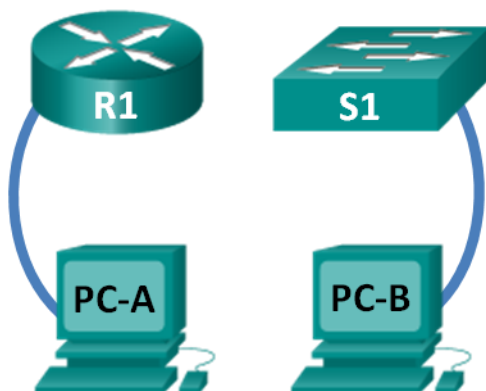
CCNA Routing and Switching: Introduction to Networks 6.0 Instructor Lab Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA Routing and Switching: Introduction to Networks course as part of an official Cisco Networking Academy Program.

Lab - Initializing and Reloading a Router and Switch (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Set Up Devices in the Network as Shown in the Topology

Part 2: Initialize the Router and Reload

Part 3: Initialize the Switch and Reload

Background / Scenario

Before starting a CCNA hands-on lab that makes use of either a Cisco router or switch, ensure that the devices in use have been erased and have no startup configurations present. Otherwise, the results of your lab may be unpredictable. This lab provides a detail procedure for initializing and reloading a Cisco router and a Cisco switch.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Part 1: Set Up Devices in the Network as Shown in the Topology

Step 1: Cable the network as shown in the topology.

Attach console cables to the devices shown in the topology diagram.

Step 2: Power on all the devices in the topology.

Wait for all devices to finish the software load process before moving to Part 2.

Part 2: Initialize the Router and Reload

Step 1: Connect to the router.

Console into the router and enter privileged EXEC mode using the **enable** command.

```
Router> enable
Router#
```

Step 2: Erase the startup configuration file from NVRAM.

Type the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM).

```
Router# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 3: Reload the router.

Issue the **reload** command to remove an old configuration from memory. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

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

```
*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.
```

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

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

Step 4: Bypass the initial configuration dialog.

After the router reloads, you are prompted to enter the initial configuration dialog. Enter **no** and press Enter.

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

Step 5: Terminate the autoinstall program.

You will be prompted to terminate the autoinstall program. Respond **yes** and then press Enter.

```
Would you like to terminate autoinstall? [yes]: yes
Router>
```

Part 3: Initialize the Switch and Reload

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash

Directory of flash:/

   2  -rwx           1919   Mar 1 1993 00:06:33 +00:00  private-config.text
   3  -rwx           1632   Mar 1 1993 00:06:33 +00:00  config.text
   4  -rwx          13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
   5  -rwx        11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-mz.150-2.SE.bin
   6  -rwx           616    Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Step 3: Delete the VLAN file.

- a. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

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

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.


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

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

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

Reflection

1. Why is it necessary to erase the startup configuration before reloading the router?

The startup configuration file is loaded into memory and becomes the running-config after the router reloads. Erasing this file allows the router to return to its basic configuration after a reload.

2. You find a couple configurations issues after saving the running configuration to the startup configuration, so you make the necessary changes to fix those issues. If you were to reload the device now, what configuration would be restored to the device after the reload?

The configuration at the time of the last save is restored to the device after a reload. Any changes made to the running configuration after the last save would be lost.

Class Activity - Draw Your Concept of the Internet (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Demonstrate that networks are made of many different components.

Background / Scenario

Draw and label a map of the Internet as you interpret it now. Include your home or school/university location and its respective cabling, equipment, devices, etc. Some items you may want to include:

- Devices or equipment
- Media (cabling)
- Link addresses or names
- Sources and destinations
- Internet service providers

Upon completion, save your work in a hard-copy format, it will be used for future reference at the end of this chapter. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your work in class.

For an example to get you started, please visit: <http://www.kk.org/internet-mapping>.

Note: This webpage requires Adobe Flash.

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to help students to reflect on their perceptions of how a network is set up for personal use. Discussion should be facilitated by the instructor as a result of this activity. Facilitation of the discussion should include student-to-student discussions of each other's work.

Required Resources

- Internet access
- Paper and pencils or pens (if students are creating a hard copy)

Reflection

1. After reviewing your classmates' drawings, were there computer devices that you could have included on your diagram? If so, which ones and why?

Answers will vary.

2. After reviewing your classmates' drawings, how were some of the model designs the same or different? What modifications would you make to your drawing after reviewing the other drawings?

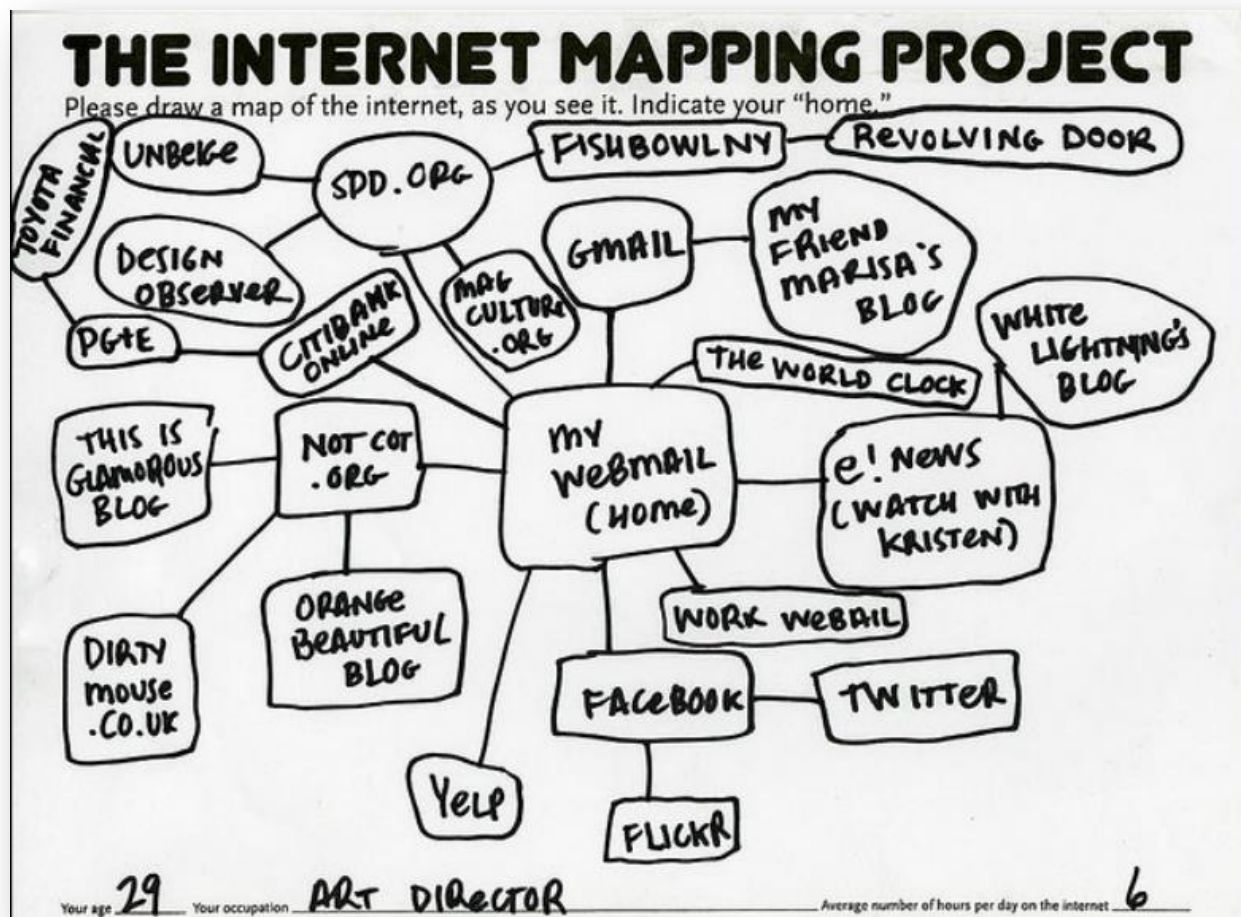
Answers will vary.

3. In what way could icons on a network drawing provide a streamlined thought process and facilitate your learning? Explain your answer.

Class Activity - Draw Your Concept of the Internet

Students should note that having a set of representative icons will assist them in learning how to draw/design network representation. It consolidates information, and is easily understood by others who understand what the icons represent. It is a form of shorthand for people in the same industry.

Initial Network Diagrams and Network Components – will vary. A very basic network design representation from the website is depicted below (this diagram is for Instructor reference.)



Lab - Researching Network Collaboration Tools (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Use Collaboration Tools

Part 2: Share Documents with Google Drive

Part 3: Explore Conferencing and Web Meetings

Part 4: Create Wiki Pages

Background / Scenario

Network collaboration tools provide people with the opportunity to work together efficiently and productively without the constraints of location or time zone. Collaborative tools include document sharing, web meetings, and wikis.

Required Resources

Device with Internet access

Part 1: Use Collaboration Tools

Step 1: List at least two collaboration tools that you currently use.

Answers will vary but could include: Google Drive, Cisco Webex, Citrix Go to Meeting, and Confluence Wiki.

Step 2: List at least two reasons for using collaboration tools.

Answers will vary but could include: centralization, less email, reduced travel, and less environmental impact.

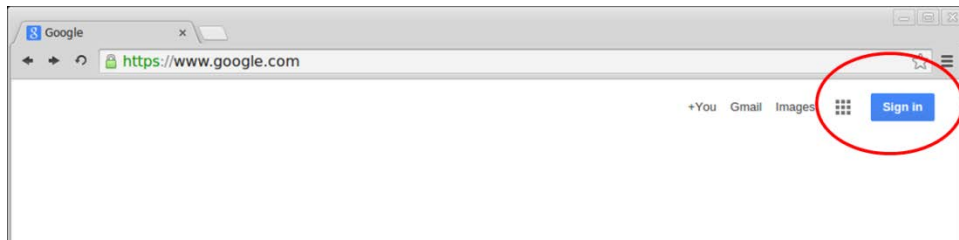
Part 2: Share Documents with Google Drive

In Part 2, you will explore the document sharing functions by using Google Drive to set up document sharing. Google Drive is a web-based office suite and data storage service that allows users to create and edit documents online while collaborating in real-time with other users. Google Drive provides 15 GB of storage with every free Google account. You can purchase additional storage if needed.

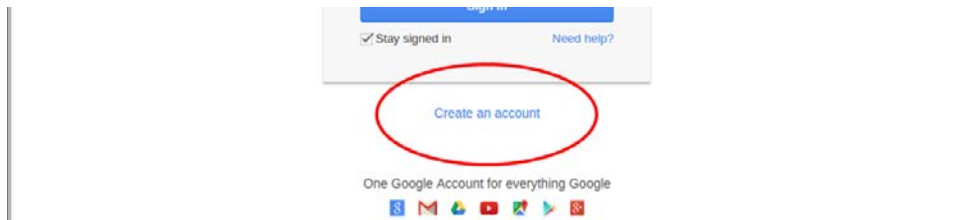
Step 1: Create a Google account.

To use any of Google's services, you must first create a Google account. This account is used with any of Google's services, including Gmail.

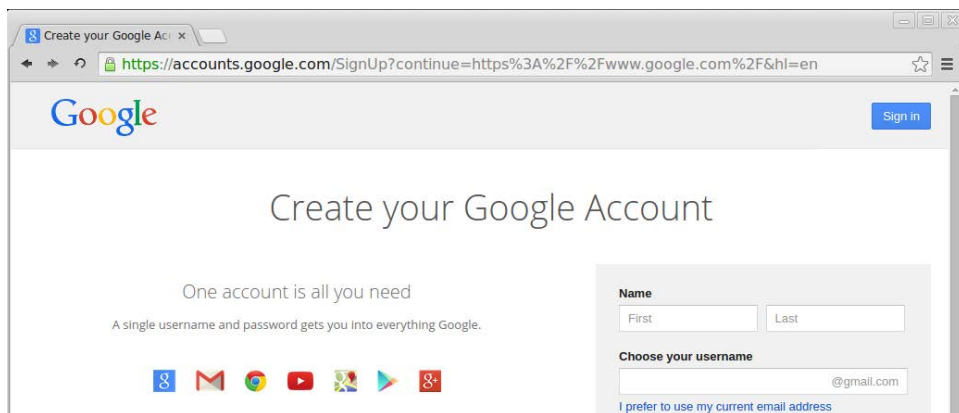
- a. Browse to www.google.com and click **Sign in** (located at the top-right corner of the web page).



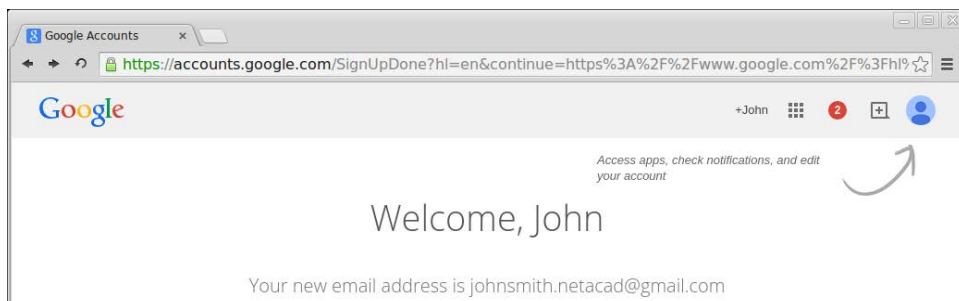
- b. On the Google Accounts web page, if you already have a Google account, you can sign in. If you do not have an account, click **Create an account**.




- c. On the Create your Google Account web page, fill out the form to the right. Provide all the required information. The name you enter in the **Choose your username** field becomes the account name. It is not necessary to supply your mobile phone or current email address. You must agree to the Google Terms of Service and Privacy Policy before clicking **Next step**.

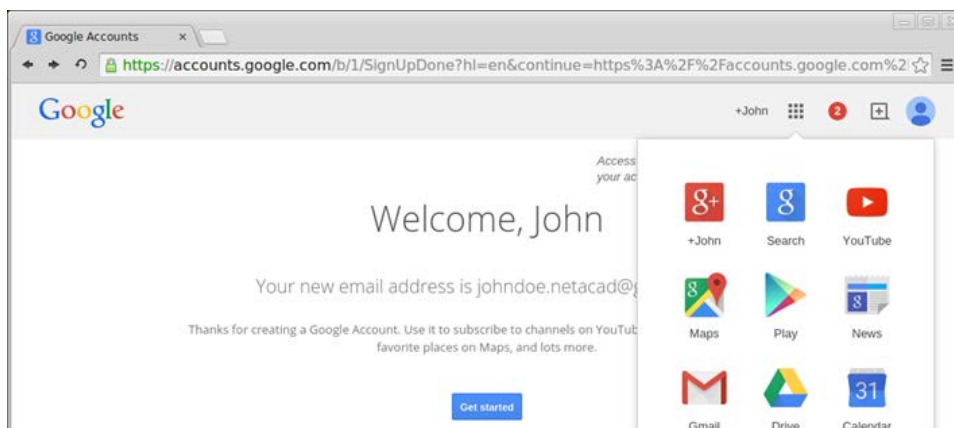



- d. The next web page allows you to add a profile photo. Click **Create your profile** to complete the account creation process.
- e. You have successfully created your Google account when the Welcome screen appears.

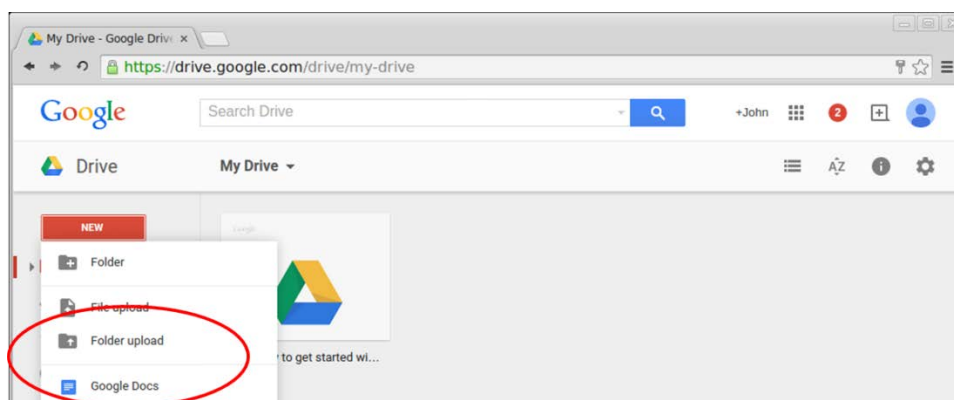


Step 2: Create a new document.

- Click the Apps () icon to access a list of Google Services. Use the credentials you created in Step 1 to sign in to all of the Google services.



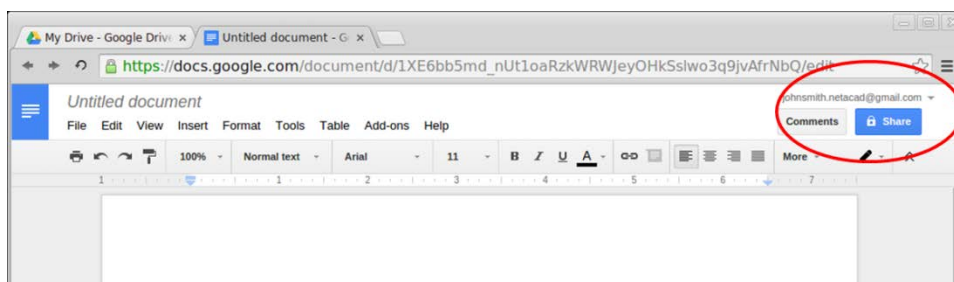
- Click the Drive () icon to access your Google Drive.
- Click **New** to display a drop-down menu that allows you to select the type of document to create. Choose **Google Docs** to create a word document.



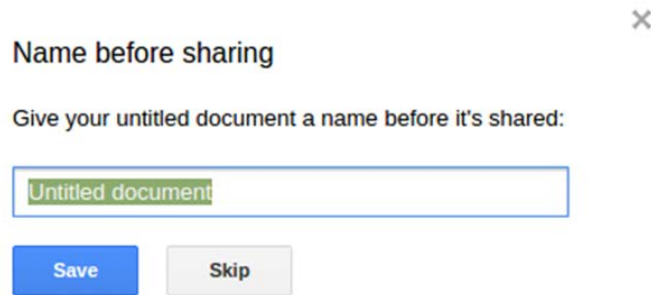
- The new document displays. Many of the functions of the Google editor work similarly to Microsoft Word.

Step 3: Share a Google document.

- After the blank Google document opens, you can share it with others by clicking the **Share** button (at the top-right corner of the web page).



- b. Name your new document, and then click the **Save** button. Because you created the document, you are the document owner.



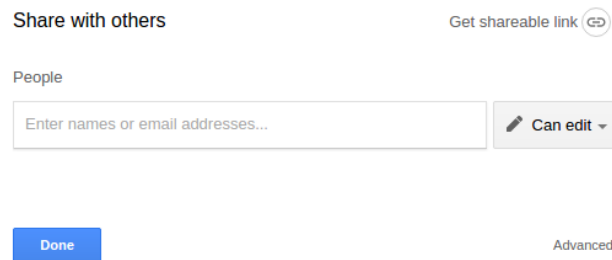
Name before sharing

Give your untitled document a name before it's shared:


Untitled document

Save Skip

- c. In the **Share with others** dialog box, enter the names, groups, or email addresses with whom to share this document. You can choose to allow others to view, comment, or edit the document.



Share with others

Get shareable link 

People

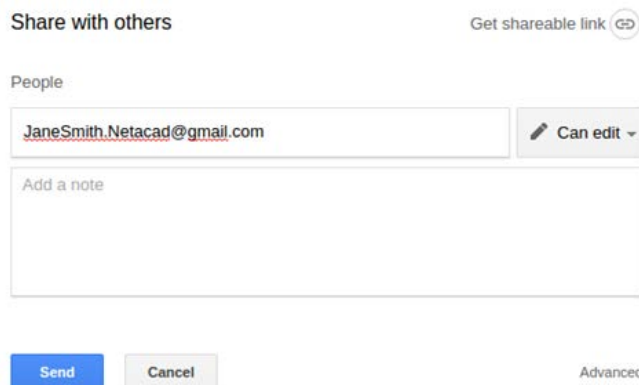
Enter names or email addresses...

Can edit ▼


Done

Advanced

- d. When you start entering information into the **Share with others** dialog box, you may also add a note.



Share with others

Get shareable link 

People

JaneSmith.Netacad@gmail.com

Can edit ▼

Add a note

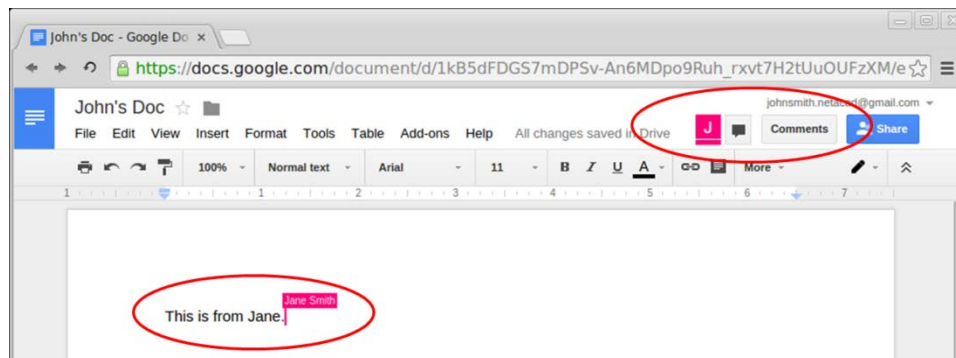
Send Cancel

Advanced

- e. Click the **Send** button. This will navigate you back to the open document.

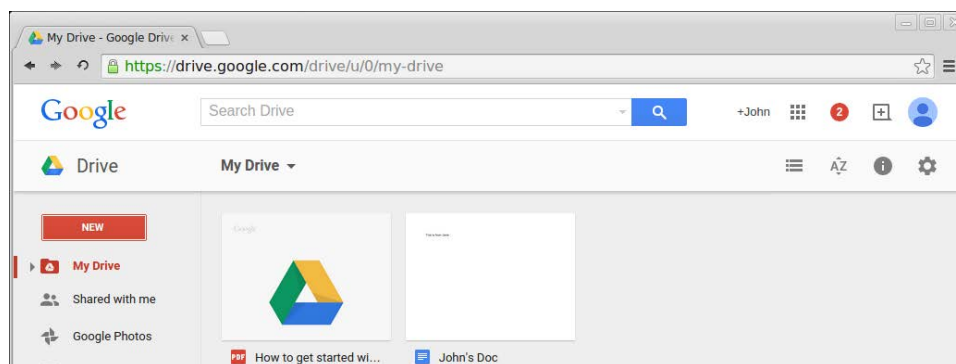
Lab - Researching Network Collaboration Tools

- f. All users can see who currently has the document open. Users currently viewing the document are represented by the icons at the top right corner. You can determine where the other users are making changes by locating the other users' cursors in the document.



- g. This new document is automatically saved on the Google Drive. You can close the document by closing the associated browser window or tab.

Note: You can navigate directly to the Google Drive using <https://drive.google.com> and view the list of documents created by you or shared with you.



Part 3: Explore Conferencing and Web Meetings

Web meetings combine file and presentation sharing with voice, video, and desktop sharing. Cisco WebEx Meeting Center is one of the leading web meeting products available today.

In Part 3 of this lab, you will watch a video produced by Cisco that reviews the features contained within WebEx Meeting Center. The video is located on YouTube at the following link: http://www.youtube.com/watch?v=fyaWHEF_aWg

Instructor Note: For additional WebEx conferencing tools, you can register for a free WebEx Meeting Basics account at www.webex.com.

Part 4: Create Wiki Pages

“Wiki” is a word from the Hawaiian language. It means fast. In networking terms, a wiki is a web-based collaboration tool that permits almost anyone to post information, files, or graphics to a common site for other users to immediately read and modify. A wiki provides access to a home page that has a search tool to assist you in locating the articles that interest you. A wiki can be installed for the Internet community or behind a corporate firewall for employee use. The user not only reads wiki contents, but also participates by creating content within a web browser.

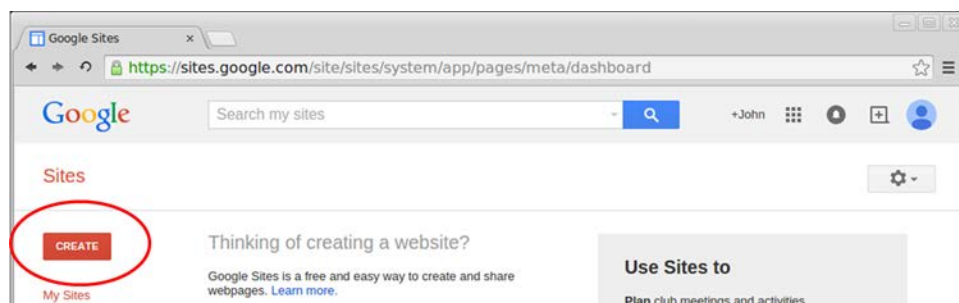
Although many different wiki servers are available, the following common features have been formalized into every wiki:

- Any web browser can be used to view or edit pages or create new content.
- Edit and auto links are available to edit a page and automatically link pages. Text formatting is similar to creating an email.
- A search engine is used for quick content location.
- Access control can be set by the topic creator, which defines who is permitted to edit content.
- A wiki is a grouping of web pages with different collaboration groups.

In this part of the lab, you will use the Google account that you created in Part 2 and create a wiki page in Google Sites.

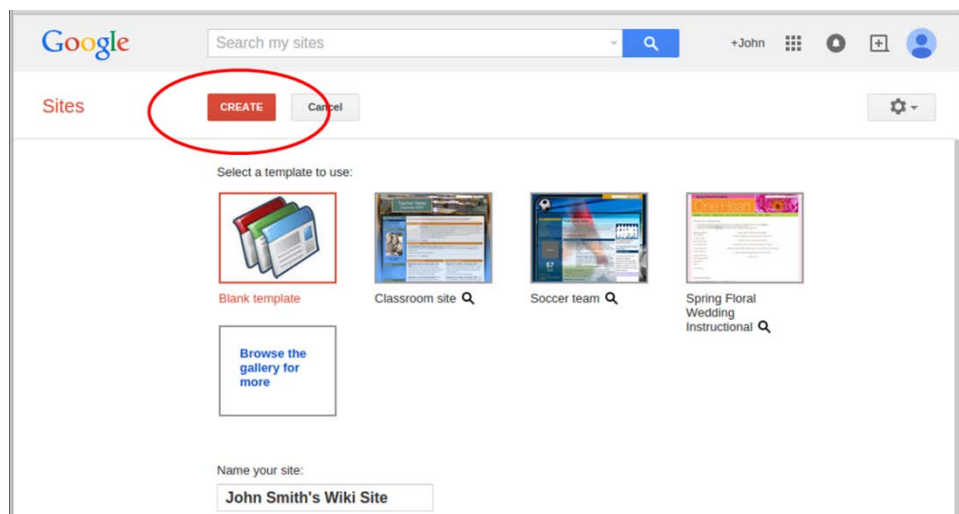
Step 1: Sign in to Google Sites.

Navigate to <http://sites.google.com> and sign in using the Google account that you created in Part 2. Click **CREATE** to create a new Google site.




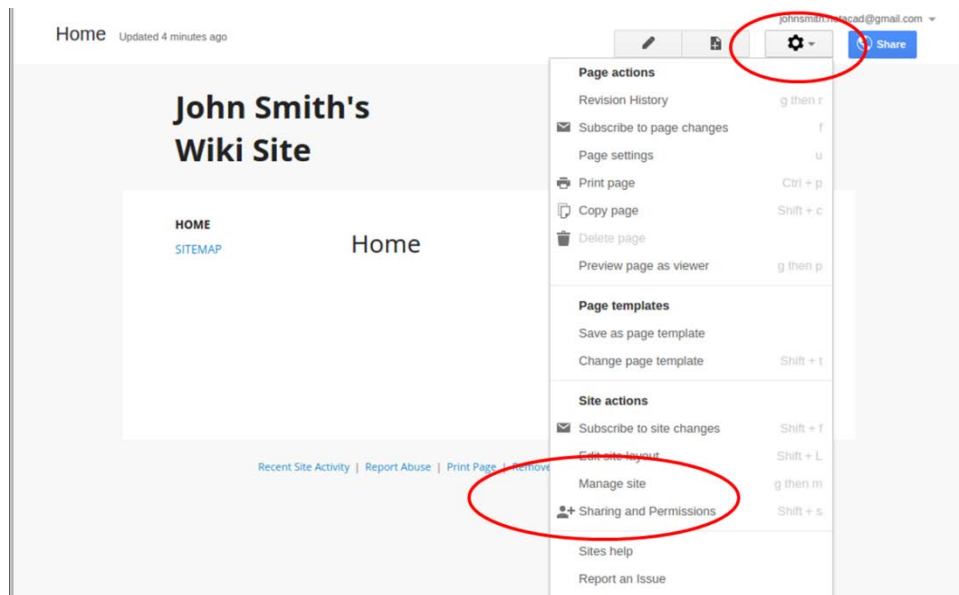
Step 2: Name your new wiki site.

In the **Name your site** field, type in a name for your new wiki site. You will need to use a unique name for your site. Google also requires that you enter the code (displayed at the bottom of the screen) to prevent automated scripts, called web robots, from creating multiple sites. After you have entered your site name, click the **CREATE** button. If someone has used your site name already, you are prompted to enter another name. You may need to re-enter the code at the bottom of the page and click **CREATE SITE** to continue.

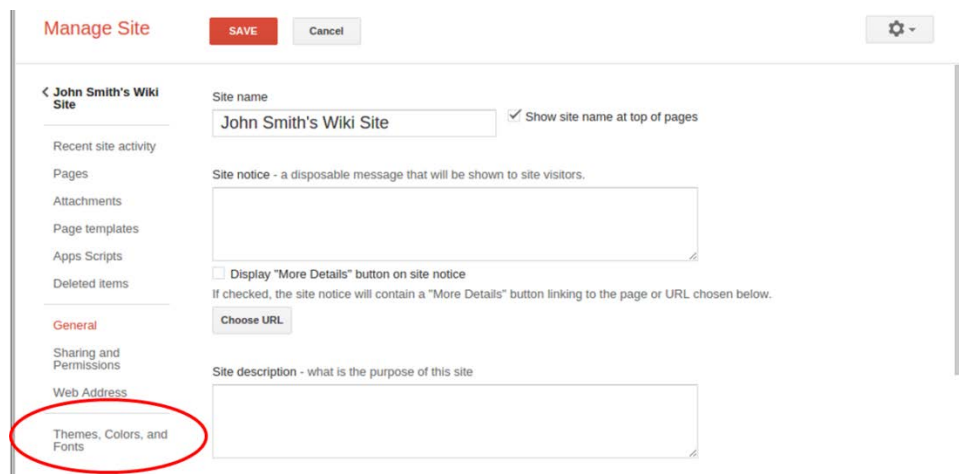


Step 3: Edit the look of your new wiki site.

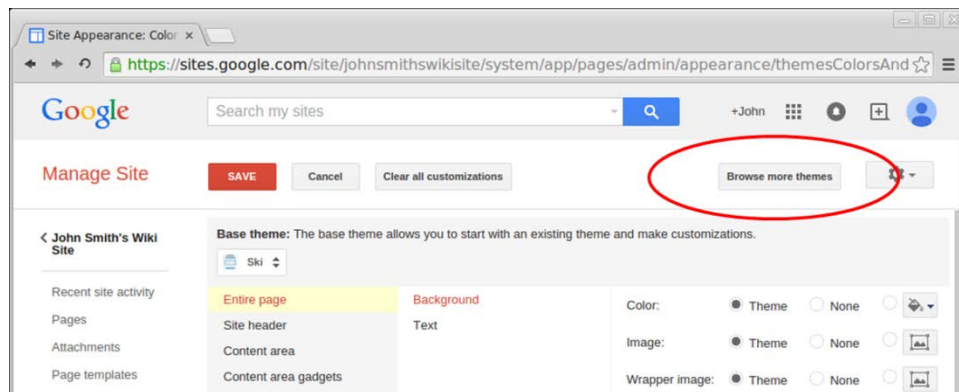
- a. Google provides templates to customize the look of your new wiki site. Click the More Action () icon for the drop-down menu, and then click **Manage site**.



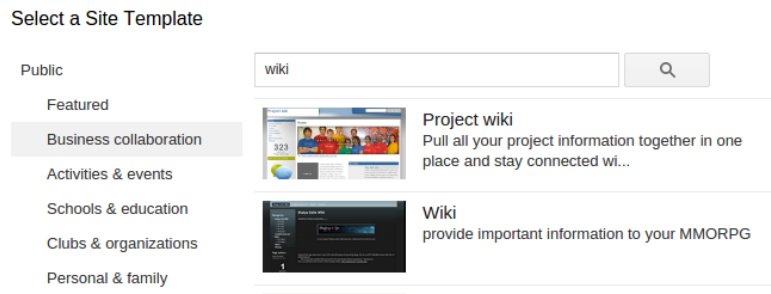
- b. Click **Themes, Colors, and Fonts** at the bottom of the left sidebar.



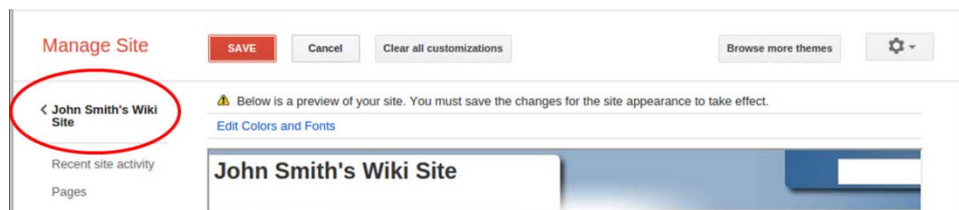
- c. Currently, the site is using the Base theme. Click **Browse more themes** to select a Wiki site template.




- d. Search and select a wiki template for your site. Click **Select** to continue.



- e. The preview of your home page appears. You can also customize the colors and fonts on your home page. Click **Edit Colors and Fonts**. When you are satisfied with your new home page, click **Save** to accept the changes.
- f. After you have saved your theme selection, click your site name under **Manage Site**.

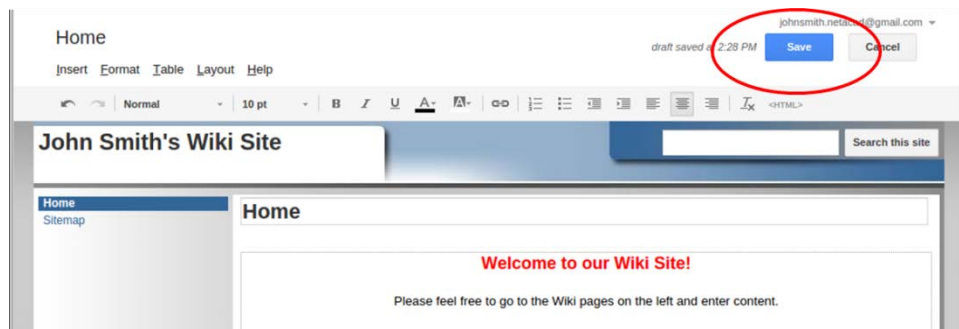


Step 4: Update the Home page.


- a. The Home page is the first page visitors see when they navigate to your website. Click the Edit page () icon to edit the content of this page. You can add text, pictures, etc. to this page.

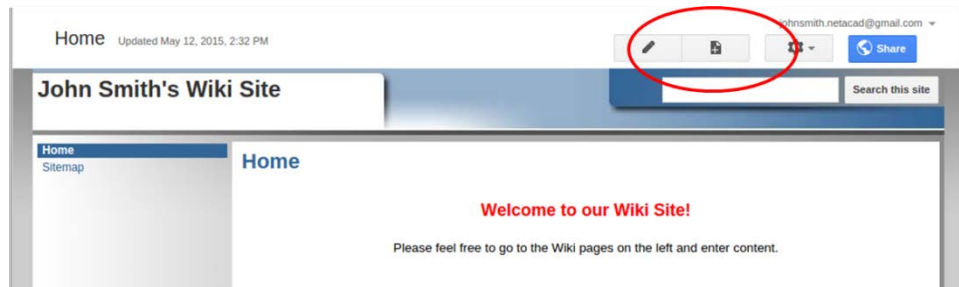


- b. Click **Save** to save the changes and exit the page edit mode.

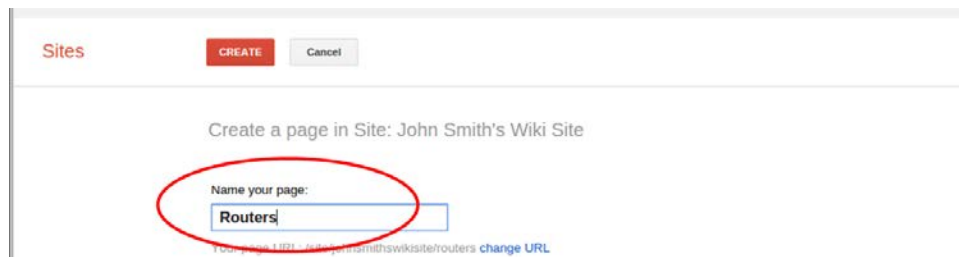


Step 5: Create a wiki page.

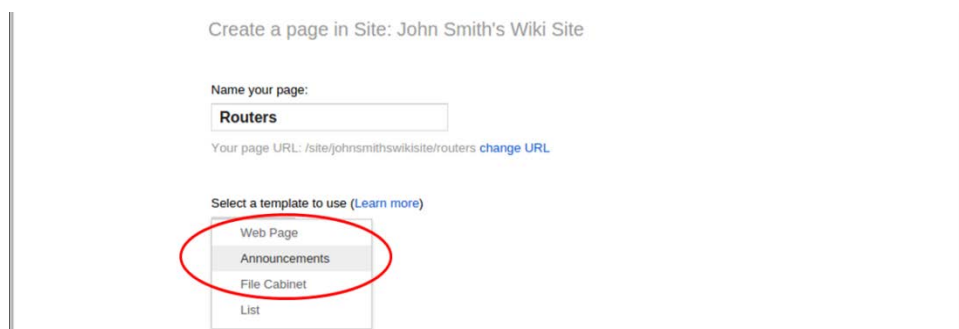
- a. Click the Create page () icon to create a new page for posting.



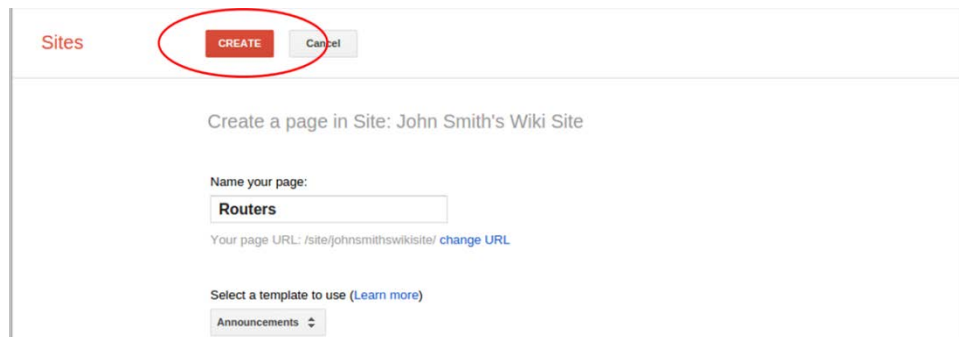
- b. In the **Name your page** field, enter a page name. In the example below, the name Routers is used as the topic for this page.



- c. Click the **Web Page** drop-down menu and select **Announcements**. Google uses this term to indicate a wiki page.

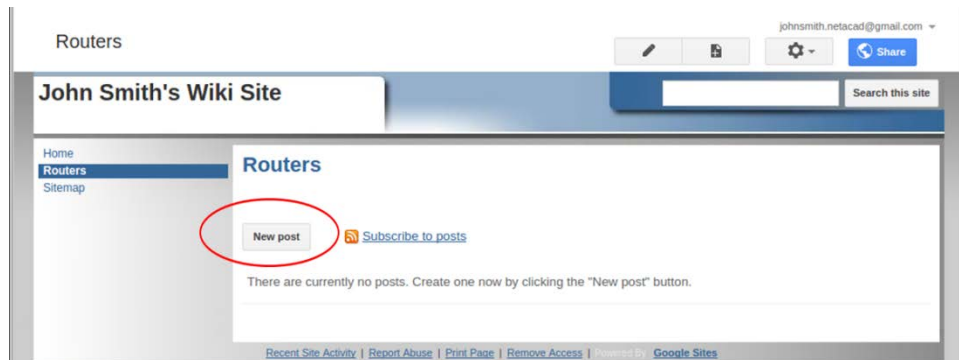


- d. Click **CREATE** to create your new wiki page.



The screenshot shows the 'Create' dialog box in Google Sites. At the top, there are 'CREATE' and 'Cancel' buttons, with 'CREATE' circled in red. Below the buttons, the text reads 'Create a page in Site: John Smith's Wiki Site'. There is a text input field labeled 'Name your page:' with 'Routers' entered. Below that, it says 'Your page URL: /site/johnsmithswikisite/ change URL'. At the bottom, there is a section 'Select a template to use (Learn more)' with a dropdown menu currently showing 'Announcements'.

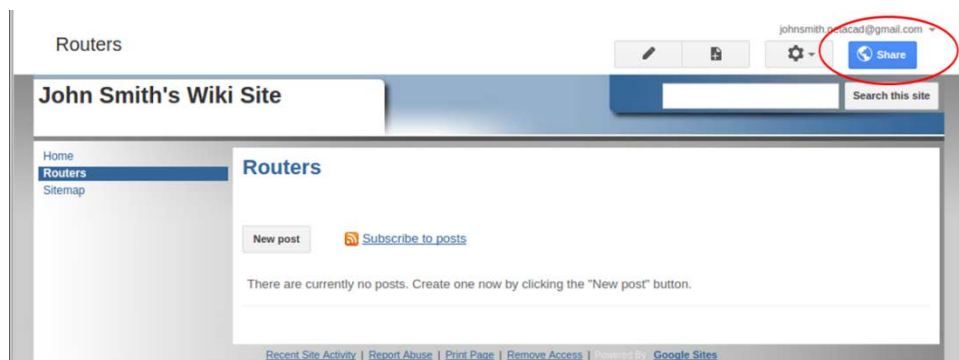
- e. Your new wiki page, called Routers, displays. The new page has a **New post** menu option that allows information to be added to the page. (Notice that the left sidebar has a new link to allow your site visitors access to this page.)



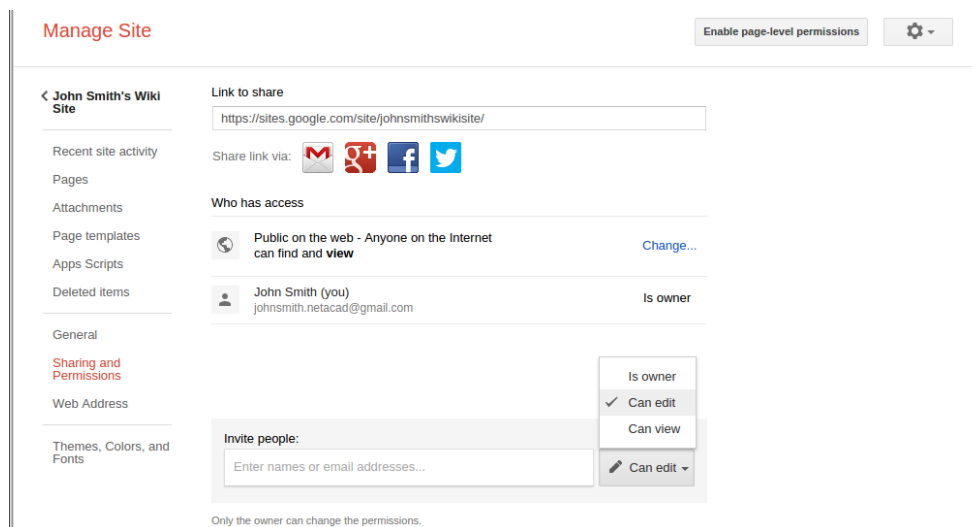
Step 6: Share your web site.

A wiki site is not really a wiki site unless other people can contribute. There are a number of ways to share your new site.

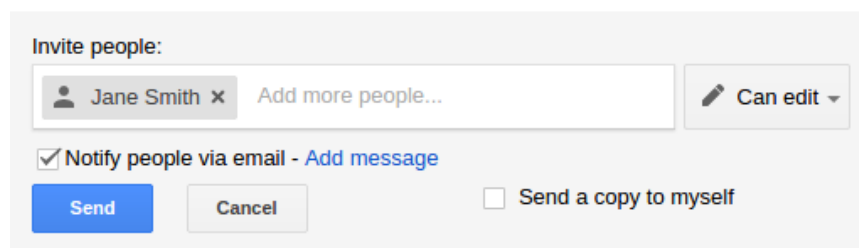
- a. On your wiki site, click **Share**.



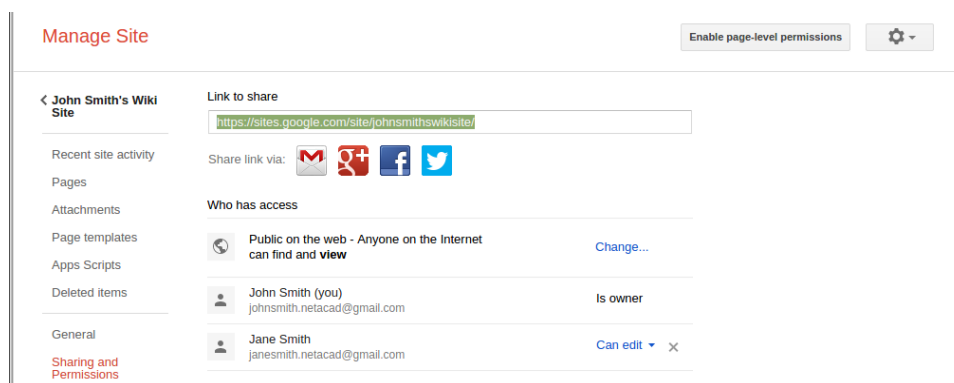
- b. You can invite specific individuals to view or edit this website. You may also grant ownership to others.



- c. You can specify how to notify people about the wiki by entering their email address. Click **Send** to share the wiki with others.



- d. The **Manage Site** page displays the people who have access to your site. Notice Jane Smith was added to the list of people with access. Click your site name to return to your home page.



Step 7: Provide the URL of your site.

You can provide the URL to your new site by adding your site name to the end of the Google site URL, as shown here: `http://sites.google.com/site/(sitename)`.

Step 8: Find additional information.

You can find a quick overview of how a wiki works at <http://www.youtube.com/watch?v=-dnL00TdmLY>.

Other examples of wikis and their web sites include:

- Wikipedia — <http://www.wikipedia.org/>
- Atlassian Confluence (a popular business wiki) — <http://www.atlassian.com/software/confluence/>
- Wikispaces (another free wiki) — <http://www.wikispaces.com/>

Reflection

1. Can you think of other collaboration tools used in the business world today?

Answers will vary.

2. What collaboration tools do you see as useful to a network administrator?

Answers will vary.

Lab - Researching Converged Network Services (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Survey Your Understanding of Convergence

Part 2: Research ISPs Offering Converged Services

Part 3: Research Local ISPs Offering Converged Services

Part 4: Select Best Local ISP Converged Service

Part 5: Research Local Company or Public Institution Using Convergence Technologies

Background / Scenario

Convergence in the context of networking is a term used to describe the process of combining voice, video, and data communications over a common network infrastructure. Technology advances have made convergence readily available to large, medium, and small businesses, as well as for the home consumer. In this lab, you will research the converged services available to you.

Required Resources

Device with Internet access

Part 1: Survey Your Understanding of Convergence

Instructor Note: In Part 1, the instructor may wish to lead a discussion with students on their understanding of convergence, its definition, and the possible technologies used. This lab may be assigned as homework.

Step 1: Describe convergence as you understand it and provide examples of its use in the home.

Write a definition of convergence and list at least two examples.

Convergence - Converged networks are capable of delivering voice, video streams, text, and graphics between many different types of devices over the same communication channel and network structure. On a converged network, there are still many points of contact and many specialized devices, such as personal computers, phones, TVs, and tablet computers, but there is one common network infrastructure. An example of a converged network at home is a Triple Play service from Charter.com. Voice, Video (TV), and phone are bundled together and come into the home on one cable, typically hybrid fiber coax.

Part 2: Research ISPs Offering Converged Services

In Part 2, you will research and find two or three ISPs who offer converged services for the home, regardless of geographical location.

Step 1: Research various ISPs that offer converged services.

List some of the ISPs that you found in your search.

Comcast

Charter

AT&T

Step 2: Fill in the following form for the ISPs you selected.

Internet Service Provider	Product Name of Converged Service
Comcast	Xfinity Triple Play
Time Warner Cable	TV, Internet, and Phone
AT&T	AT&T U-Verse

Part 3: Researching Local ISPs Offering Converged Services

In Part 3, you will research and find two or three local ISPs who offer converged services for the home in your geographic area.

Step 1: Research various ISPs that offer converged services.

List at least two of the ISPs that you found in your search.

Answers will vary based on geographic location.

Step 2: Fill in the following form for the ISPs you selected.

Internet Service Provider	Product Name of Converged Service	Cost per Month	Download Speed
Comcast	Xfinity Triple Play	\$89.99	Varies 10 to 16 Mbps
Time Warner Cable	TV, Internet, and Phone	\$99.99	10 Mbps
AT&T	U-Verse	\$59.00	3 Mbps

Part 4: Select Best Local ISP Converged Service Offering

Select your top choice from the list of local ISPs that you selected and provide reasons why you chose that particular one.

Answers will vary and will typically be based on price per month and relative priority of Internet speeds versus number of TV channels offered in the basic packages. Student may choose Comcast for higher download speeds for Internet. Emphasize to students that home users' priorities can affect their choice of service. For example, users who stream movies exclusively may want higher download speeds versus a user who mainly does casual surfing of the Internet and checks email.

Part 5: Research Local Companies or Public Institutions Using Convergence Technologies

In Part 5, you will research and locate a company in your area that currently uses convergence technologies in their business.

Step 1: Research and find a local company using convergence.

In the following table, list the company, industry, and convergence technologies used.

Name of Company	Industry	Convergence Technologies
Cisco Systems, Inc.	Information Technology	Phone, Video, Data
Woodward, Inc.	Aerospace	Phone, Video, Data

Reflection

1. Identify at least two advantages of using convergence technologies?

Blending voice, video, and data signals onto one communication infrastructure allows companies to better manage the technology because the network will use a common set of rules and standards. The need for separate distribution equipment to offer voice and data will no longer be necessary.

2. Identify at least two disadvantages of using convergence technologies?

Until the technologies fully mature, configuration and management of voice, video, and data flowing on one channel can be a challenge. Giving voice precedence over data using Quality of Service (QoS) technologies can be quite complex for companies that do not have trained IT personnel on staff.

Lab - Researching IT and Networking Job Opportunities (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Research Job Opportunities

Part 2: Reflect on Research

Background / Scenario

Jobs in Information Technology (IT) and computer networking continue to grow. Most employers require some form of industry standard certification, degree, or other qualifications from their potential employees, especially those with limited experience. The Cisco CCNA certification is a known and established entry-level networking certification that is respected in the industry. There are additional levels and kinds of Cisco certifications that one can attain, and each certification may enhance employment opportunities as well as salary range.

In this lab, you will complete targeted job searching on the web to find what types of IT and computer networking jobs are available; what kinds of skills and certifications you will need; and the salary ranges associated with the various job titles.

Required Resources

Device with Internet access

Part 1: Research Job Opportunities

In Part 1, you will use a web browser to visit the popular job listing websites monster.com and salary.com.

Step 1: Open a web browser and go to a job listing website.

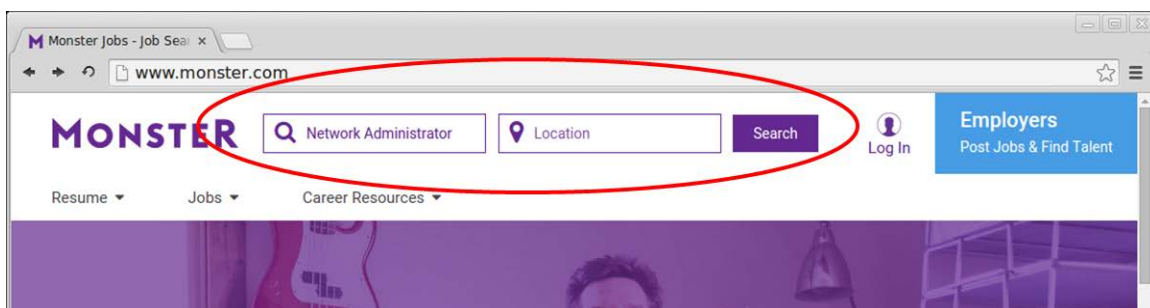
In the URL address bar type <http://monster.com> and press Enter.

Note: For job listings outside of the U.S., use the following link to search for your country:

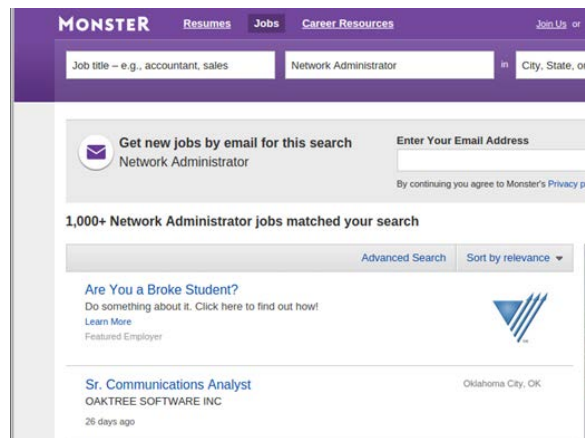
<http://www.monster.com/geo/siteselection/>

Step 2: Search for networking related jobs.

- Type the word *Network Administrator* in the job title box. Click **SEARCH** to continue.



- b. Notice the search results:



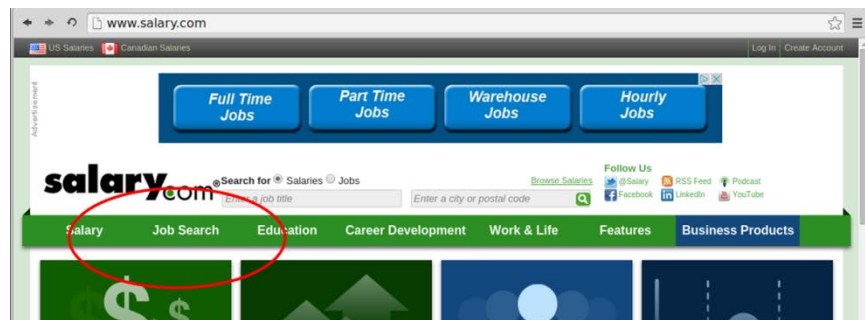
- c. Now, focus your search by adding terms to the search for Network Administrator. Try terms like Cisco CCNA, CCNP, CCNA Security, CCNA Voice, etc.
- d. Now try refining your search by adding different geographical locations. Did you find jobs in the locations you entered?

Answers will vary.

- e. Try searching a different website. Go to <http://salary.com> and click the **Job Search** menu bar button.

Note: For salary listings outside of the U.S., use the following link to search for your country:

<http://www.payscale.com/rccountries.aspx>



Lab - Researching IT and Networking Job Opportunities

- f. Add a search term like *Information Technology* to the job title field box and click **Submit**.

- g. In the image below, note the large number of matching search results. Additional tools for refining your search are available in the left column.

- h. Spend time searching for jobs and looking through the search results. Take note of what skills are required for different job titles and the range of starting salaries.

Part 2: Reflect on Research

In Part 2, answer these questions based on your research findings.

- a. What job titles did you search for?

Lab - Researching IT and Networking Job Opportunities

b. What skills or certifications were required?

c. Did you find any jobs that you previously did not know existed? If so, what were they?

d. Did you find any jobs that you are interested in? If so, which ones and what skills or certifications do they require?

Class Activity - Draw Your Concept of the Internet Now (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Identify the common components of a network.

Background / Scenario

In this activity, you will use the knowledge you have acquired throughout Chapter 1, and the modeling activity document that you prepared at the beginning of this chapter. You may also refer to the other activities completed in this chapter, including Packet Tracer activities.

Draw a map of the Internet as you see it now. Use the icons presented in the chapter for media, end devices, and intermediary devices.

In your revised drawing, you may wish to include some of the following:

- WANs
- LANs
- Cloud computing
- Internet Service Providers (tiers)

Save your drawing in hard-copy format. If it is an electronic document, save it to a server location provided by your instructor. Be prepared to share and explain your revised work in class.

Instructor Note: This optional Modeling Activity may be selected as a graded assignment, because its purpose is to validate the learning gained in Chapter 1 about:

- WANs
- LANs
- Cloud computing
- Internet Service Providers (tiers)

Required Resources

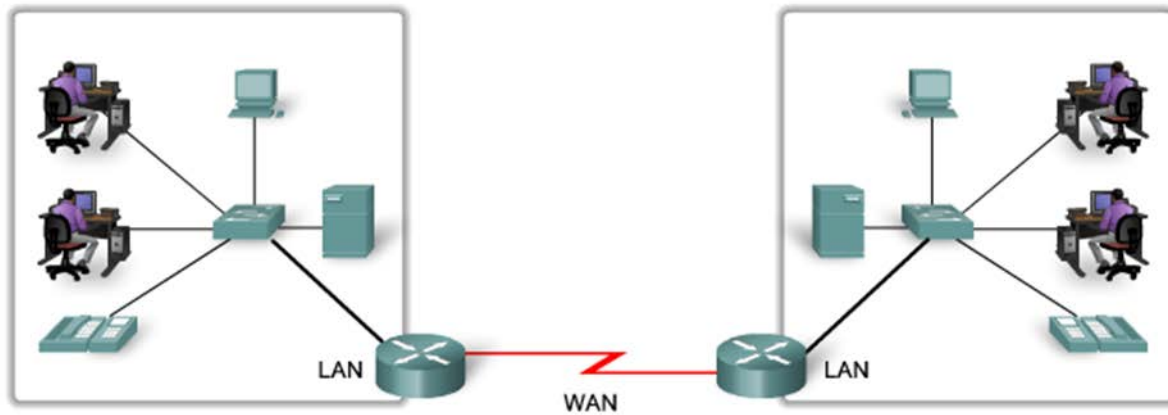
- Beginning of chapter modeling activity drawing
- Packet Tracer (may be optional if students sketch their own drawing)
- Paper and pencils or pens

Reflection

After completing Chapter 1, are you more aware of the devices, cabling, and physical components of a small-to-medium size network? Explain your answer.

(Answers will vary per student – but this reflection question will generate some good class discussion and foster community between students and the Instructor)

Modeling Activity Graphic Representation (designs will vary)



Instructor Note: This is a representative model that might be “built” as a result of this activity.

Identify elements of the model that map to IT-related content:

- Devices/Equipment
- Media (cabling)
- Social Media Links
- Sources & Destinations
- Local Area Networks
- Wide Area Networks

Class Activity - It Is Just an Operating System! (Instructor Version – Optional Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe the command structure of Cisco IOS software.

Background / Scenario

Imagine that you are employed as an engineer for a car manufacturing company. The company is currently working on a new car model. This model will have selected functions which can be controlled by the driver giving specific voice commands.

You must design the set of commands used by this voice-activated control system.

Some of functions of the car that can be controlled by voice commands are:

- Lights
- Wipers
- Radio
- Telephone set
- Air conditioning
- Ignition

Your task is to devise a simple set of spoken commands that will be used to control these systems and identify how they are going to be executed.

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to help students reflect on their perceptions of how a network is set up using voice commands (much like the IOS command structure). Facilitation of the discussion should include student-to-student discussions of each other's work.

Required Resources

- Paper and pencils or pens, or computer

Reflection

How can devising a set of voice commands assist in operating a vehicle? How could these same commands be used on a computer or network operating system?

Some suggested answers for discussion include:

- Discuss that the options for putting together a set of spoken words will constitute the command set. An obvious choice is using simple English words as the command set. Other choices include words in different languages, using command numbers or shortcuts. Note, however, that this would make the command set significantly less intuitive.
- Talk about the students' choice to make the command set direct, without hierarchy, or whether they grouped commands according to their function. Highlight that, for example, a help command without any further context would not be usable because it does not indicate what exactly the user needs help to. There are two ways of providing a context to a command:

Class Activity - It Is Just an Operating System!

- Ask students if they explicitly expressed the context with each command (for example, radio volume up/radio volume down; phone volume up/phone volume down) which is the direct, flat approach. Or did they introduce modes; groupings of commands that refer to a particular context and once positioned in that context, did not have to be reemphasized. For example, after placing the instruction in the radio mode, the commands volume up and volume down are unambiguous.
- Discuss the advantages of both approaches. For a small set of commands, the direct approach is more suitable. For a larger set of commands which may possibly grow into extensive, multi-word sentences, using modes helps to keep the command set organized and limits the length of individual commands, and is preferred.
- How did students decide how the voice command recognition would be started so that the car did not mistakenly interpret a casual conversation of passengers as commands? Possibilities include saying a specific, otherwise unused word, or pressing a button on the steering wheel. Also, discuss how students handled a system that should prompt the user to enter the voice commands, and how the user would be informed that the spoken command was not properly understood or valid.
- How did the students handle access to more safety-critical commands such as lights and ignition?)How were these commands protected or isolated so that no inadvertent manipulation could occur? Possibilities include saying a specific, otherwise unused word, or pressing a button on the steering wheel.
- Ask students to discuss which part of the software running on the car's built-in computer would be processing the voice commands and what software would be actually executing the commands. The software that performs speech recognition and translates voice commands into a form the computer can understand is the command interface used to interact with the car. However, the commands need to be processed by the central operating software of the car that controls all its functions and orchestrates all its systems. As an example, saying "engine on" involves processing the voice command in the command interface, and then the operating system processes this command by activating the starter motor for a certain period of time, enabling the flow of the fuel, etc., coordinating multiple systems of a car to make it work.

Identify elements of the model that map to IT-related content:

- Different systems of the car which can be controlled by voice commands relate to different components of routers and switches that can be configured.
- Vocal commands relate to IOS commands
- The choice of short English words or phrases as the command set relates to the general style of IOS CLI.
- The mode-oriented organization of the voice command set relates to the mode-oriented IOS CLI.
- Starting the voice recognition process relates to starting a CLI EXEC session by pressing Enter. Also, the voice prompts by the car relate to the prompts on the command line.
- Potentially disruptive commands, such as lights off or engine on relates to potentially disruptive IOS commands (reload, erase flash: or delete startup-config).
- The voice interface and the car's operating system relate to the IOS EXEC (the command interpreter) and the IOS itself.

Lab - Establishing a Console Session with Tera Term (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Access a Cisco Switch through the Serial Console Port

Part 2: Display and Configure Basic Device Settings

Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

Note: Netlab users or other remote access equipment should complete only Part 2.

Instructor Note: Rollover and mini-USB console cables are no longer automatically shipped with the newer ISR G2 routers, such as Cisco 1941, Cisco 2901, or Cisco 2911. These console cables can be purchased from Cisco Systems, Inc. or other third-party vendors.

Background / Scenario

Various models of Cisco routers and switches are used in all types of networks. These devices are managed using a local console connection or a remote connection. Nearly all Cisco devices have a serial console port to which you can connect. Some newer models, such as the 1941 Integrated Services Router (ISR) G2 used in this lab, also have a USB console port.

In this lab, you will learn how to access a Cisco device via a direct local connection to the console port, using the terminal emulation program called Tera Term. You will also learn how to configure the serial port settings for the Tera Term console connection. After you have established a console connection with the Cisco device, you can display or configure device settings. You will only display settings and configure the clock in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used in the labs are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of the lab for the correct interface identifiers.

Note: Make sure that the switch and router have been erased and have no startup configuration. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with a terminal emulation program, such as Tera Term)
- Rollover (DB-9 to RJ-45) console cable to configure the switch or router via the RJ-45 console port

- Mini-USB cable to configure the router via the USB console port

Instructor Note: If Tera Term is not installed on the PC, it can be downloaded from the following link by selecting **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

Instructor Note: A USB driver must be installed prior to connecting a Microsoft Windows-based PC to a Cisco IOS device with a USB cable. The driver can be found on www.cisco.com with the related Cisco IOS device. The USB driver can be downloaded from the following link:

<http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

Instructor Note: You must have a valid Cisco Connection Online (CCO) account to download the USB driver file.

Part 1: Access a Cisco Switch through the Serial Console Port

You will connect a PC to a Cisco switch using a rollover console cable. This connection will allow you to access the CLI and display settings or configure the switch.

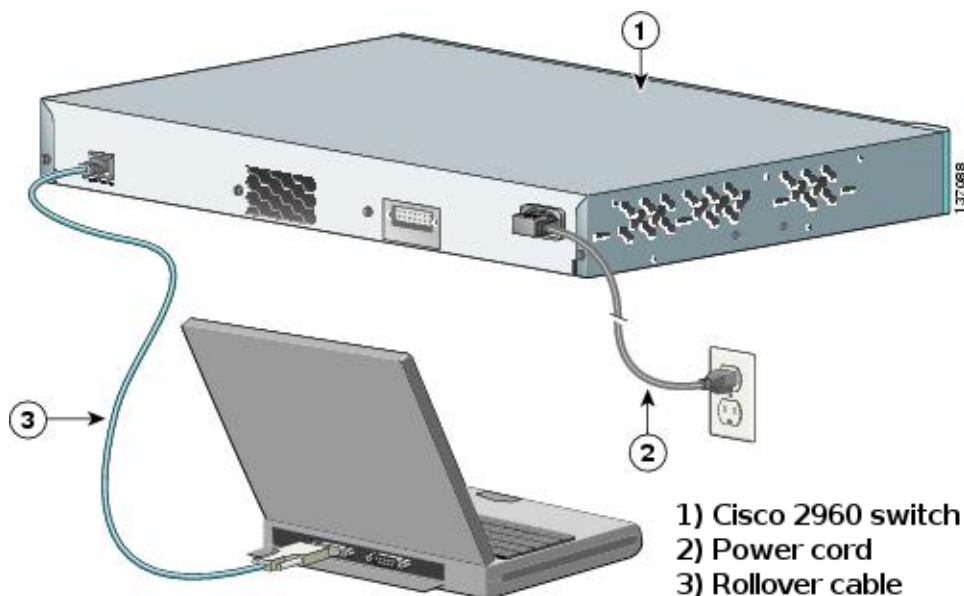
Step 1: Connect a Cisco switch and computer using a rollover console cable.

- Connect the rollover console cable to the RJ-45 console port of the switch.
- Connect the other cable end to the serial COM port on the computer.

Note: Serial COM ports are no longer available on most computers. A USB-to-DB9 adapter can be used with the rollover console cable for console connection between the computer and a Cisco device. USB-to-DB9 adapters can be purchased at any computer electronics store.

Note: If using a USB-to-DB9 adapter to connect to the COM port, you may be required to install a driver for the adapter provided by the manufacturer of your computer. To determine the COM port used by the adapter, please see Part 3 Step 4. The correct COM port number is required to connect to the Cisco IOS device using a terminal emulator in Step 2.

- Turn on the Cisco switch and computer.



Step 2: Configure Tera Term to establish a console session with the switch.

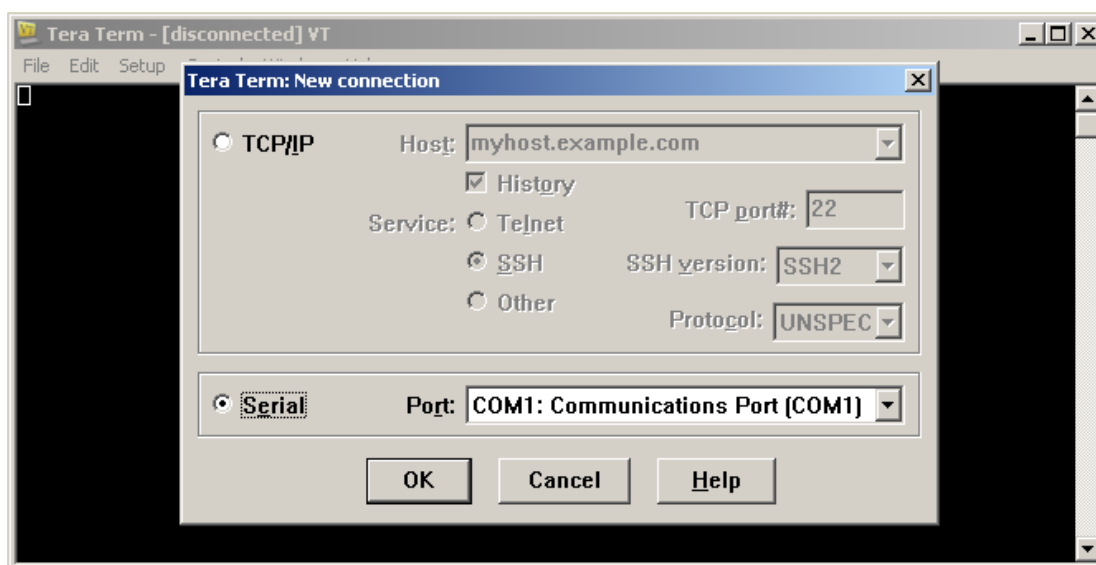
Tera Term is a terminal emulation program. This program allows you to access the terminal output of the switch. It also allows you to configure the switch.

- Start Tera Term by clicking the **Windows Start** button located in the task bar. Locate **Tera Term** under **All Programs**.

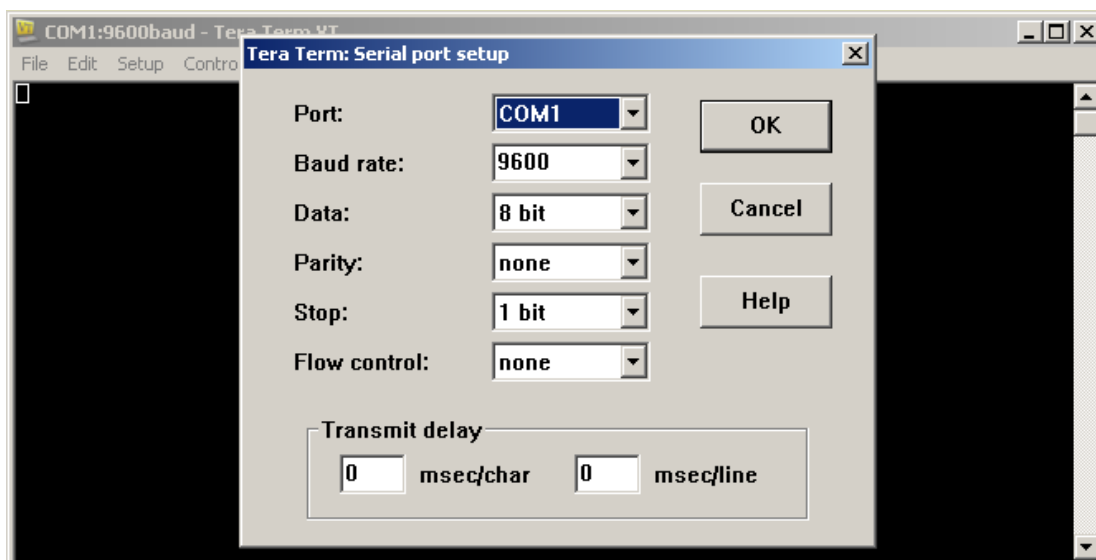
Note: If the program is not installed on the system, Tera Term can be downloaded from the following link by selecting **Tera Term**:

<http://logmett.com/index.php?/download/free-downloads.html>

- In the New Connection dialog box, click the **Serial** radio button. Verify that the correct COM port is selected and click **OK** to continue.



- From the Tera Term **Setup** menu, choose the **Serial port...** to verify the serial settings. The default parameters for the console port are 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. The Tera Term default settings match the console port settings for communications with the Cisco IOS switch.



- d. When you can see the terminal output, you are ready to configure a Cisco switch. The following console example displays the terminal output of the switch while it is loading.

Part 2: Display and Configure Basic Device Settings

In this section, you are introduced to the user and privileged executive modes. You will determine the IOS version, display the clock settings, and configure the clock on the switch.

Step 1: Display the switch IOS image version.

- a. After the switch has completed its startup process, the following message is displayed. Enter **n** to continue.

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

Note: If you do not see the above message, please contact your instructor to reset your switch to the initial configuration.

- b. While you are in the user EXEC mode, display the IOS version for your switch.

```
Switch> show version
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
```

```
ROM: Bootstrap program is C2960 boot loader
```

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)
```

```
Switch uptime is 2 minutes
```

```
System returned to ROM by power-on
```

```
System image file is "flash://c2960-lanbasek9-mz.150-2.SE.bin"
```

```
<output omitted>
```

Which IOS image version is currently in use by your switch?

c2960-lanbasek9-mz.150-2.SE.bin. Answers will vary depending on the switch.

Step 2: Configure the clock.

As you learn more about networking, you will see that configuring the correct time on a Cisco switch can be helpful when you are troubleshooting problems. The following steps manually configure the internal clock of the switch.

- a. Display the current clock settings.

```
Switch> show clock
*00:30:05.261 UTC Mon Mar 1 1993
```

- b. The clock setting is changed from within the privileged EXEC mode. Enter the privileged EXEC mode by typing **enable** at the user EXEC mode prompt.

```
Switch> enable
```

- c. Configure the clock setting. The question mark (?) provides help and allows you to determine the expected input for configuring the current time, date, and year. Press Enter to complete the clock configuration.

```
Switch# clock set ?
hh:mm:ss Current Time
```

```
Switch# clock set 15:08:00 ?
<1-31> Day of the month
MONTH Month of the year
```

```
Switch# clock set 15:08:00 Oct 26 ?
<1993-2035> Year
```

```
Switch# clock set 15:08:00 Oct 26 2012
```

```
Switch#
```

```
*Oct 26 15:08:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:31:43
UTC Mon Mar 1 1993 to 15:08:00 UTC Fri Oct 26 2012, configured from console by
console.
```

- d. Enter the **show clock** command to verify that the clock setting has updated.

```
Switch# show clock
15:08:07.205 UTC Fri Oct 26 2012
```

Part 3: (Optional) Access a Cisco Router Using a Mini-USB Console Cable

If you are using a Cisco 1941 router, or other Cisco IOS devices with a mini-USB console port, you can access the device console port using a mini-USB cable connected to the USB port on your computer.

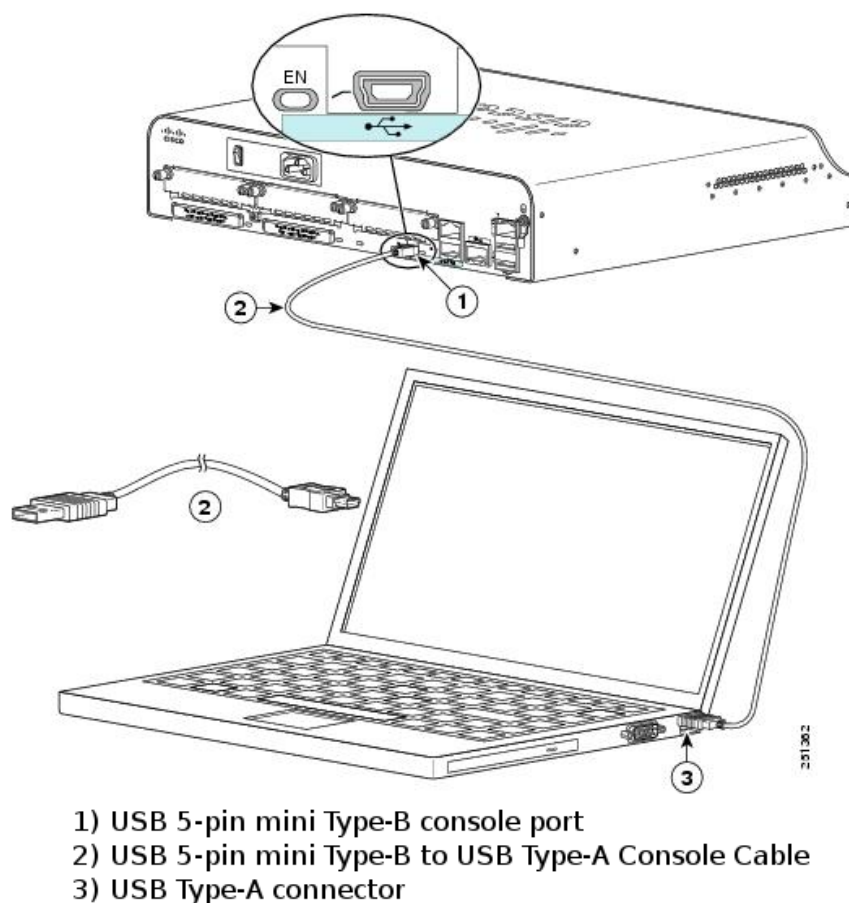
Note: The mini-USB console cable is the same type of mini-USB cables that are used with other electronics devices, such as USB hard drives, USB printers, or USB hubs. These mini-USB cables can be purchased from Cisco Systems, Inc. or other third-party vendors. Please verify that you are using a mini-USB cable, not a micro-USB cable, to connect to the mini-USB console port on a Cisco IOS device.



Note: You must use either the USB port or the RJ-45 port. Do not use both ports simultaneously. When the USB port is used, it takes priority over the RJ-45 console port.

Step 1: Set up the physical connection with a mini-USB cable.

- Connect the mini-USB cable to the mini-USB console port of the router.
- Connect the other cable end to a USB port on the computer.
- Turn on the Cisco router and computer.



Step 2: Verify that the USB console is ready.

If you are using a Microsoft Windows-based PC and the USB console port LED indicator (labeled EN) does not turn green, please install the Cisco USB console driver.

A USB driver must be installed prior to connecting a Microsoft Windows-based PC to a Cisco IOS device with a USB cable. The driver can be found on www.cisco.com with the related Cisco IOS device. The USB driver can be downloaded from the following link:

<http://www.cisco.com/cisco/software/release.html?mdfid=282774238&flowid=714&softwareid=282855122&release=3.1&relind=AVAILABLE&rellifecycle=&reltype=latest>

Note: You must have a valid Cisco Connection Online (CCO) account to download this file.

Note: This link is related to the Cisco 1941 router. However, the USB console driver is not Cisco IOS device-model specific. This USB console driver only works with Cisco routers and switches. The computer requires a reboot after finishing the installation of the USB driver.

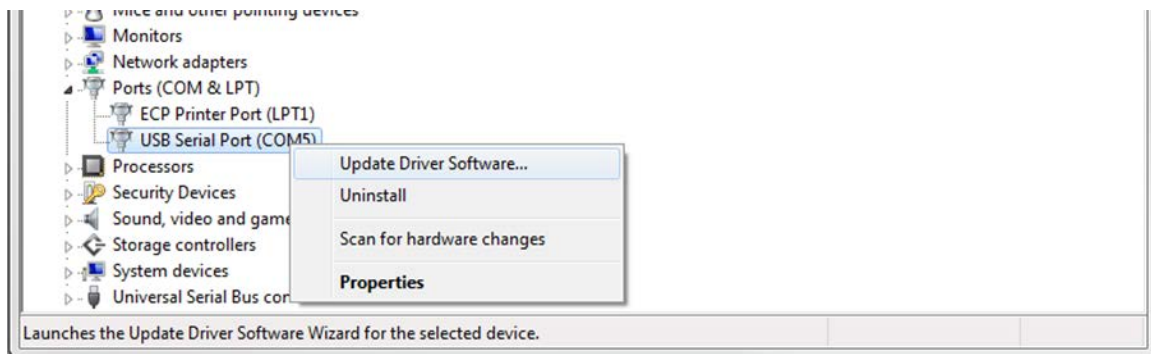
Note: After the files are extracted, the folder contains instructions for installation, removal, and the necessary drivers for different operating systems and architectures. Please choose the appropriate version for your system.

When the LED indicator for the USB console port has turned green, the USB console port is ready for access.

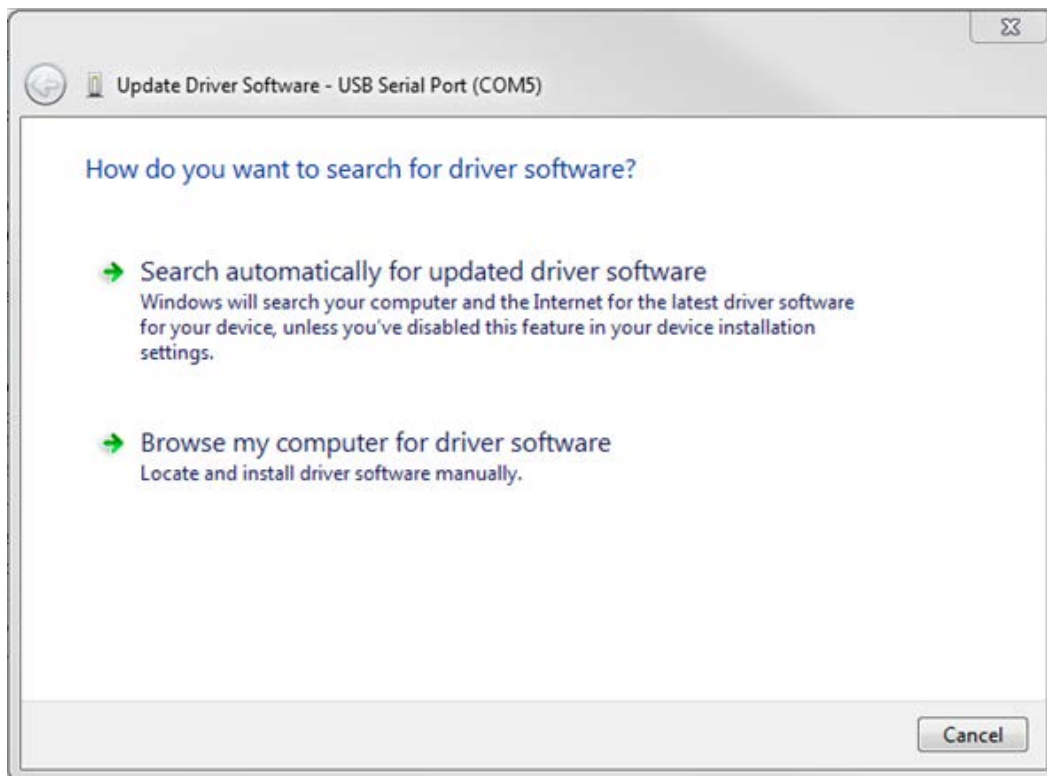
Step 3: (Optional) Enable the COM port for the Windows 7 PC.

If you are using a Microsoft Windows 7 PC, you may need to perform the following steps to enable the COM port:

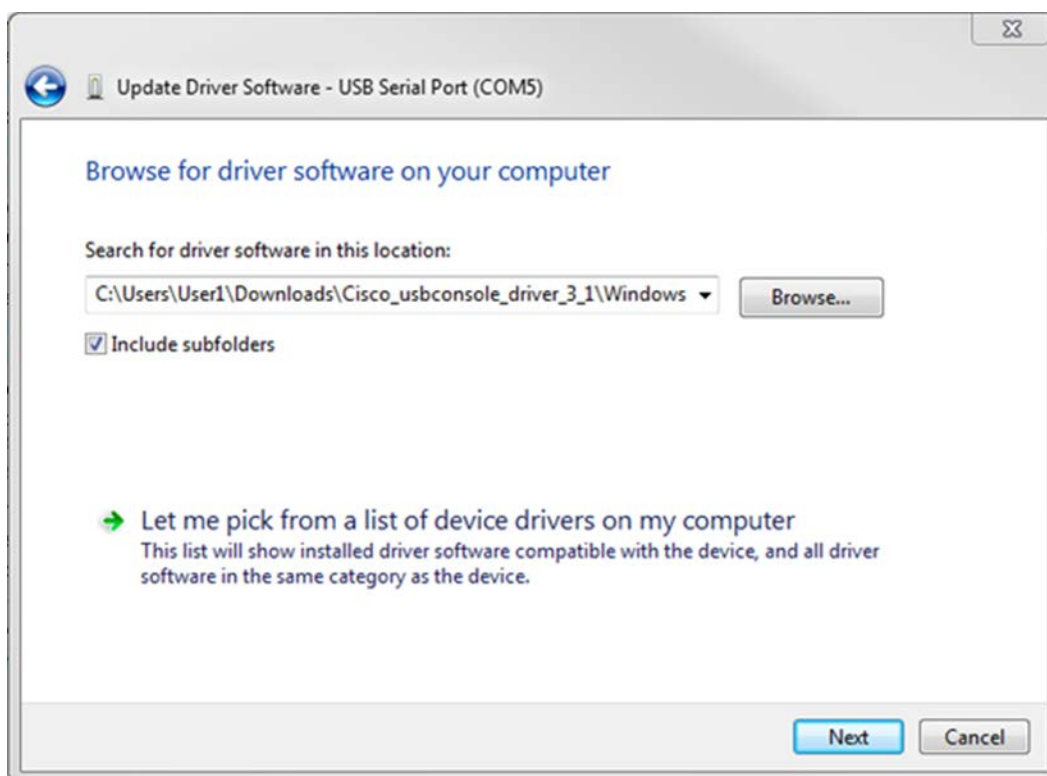
- Click the **Windows Start** icon to access the **Control Panel**.
- Open the **Device Manager**.
- Click the **Ports (COM & LPT)** tree link to expand it. Right-click the **USB Serial Port (COM5)** icon and choose **Update Driver Software**.



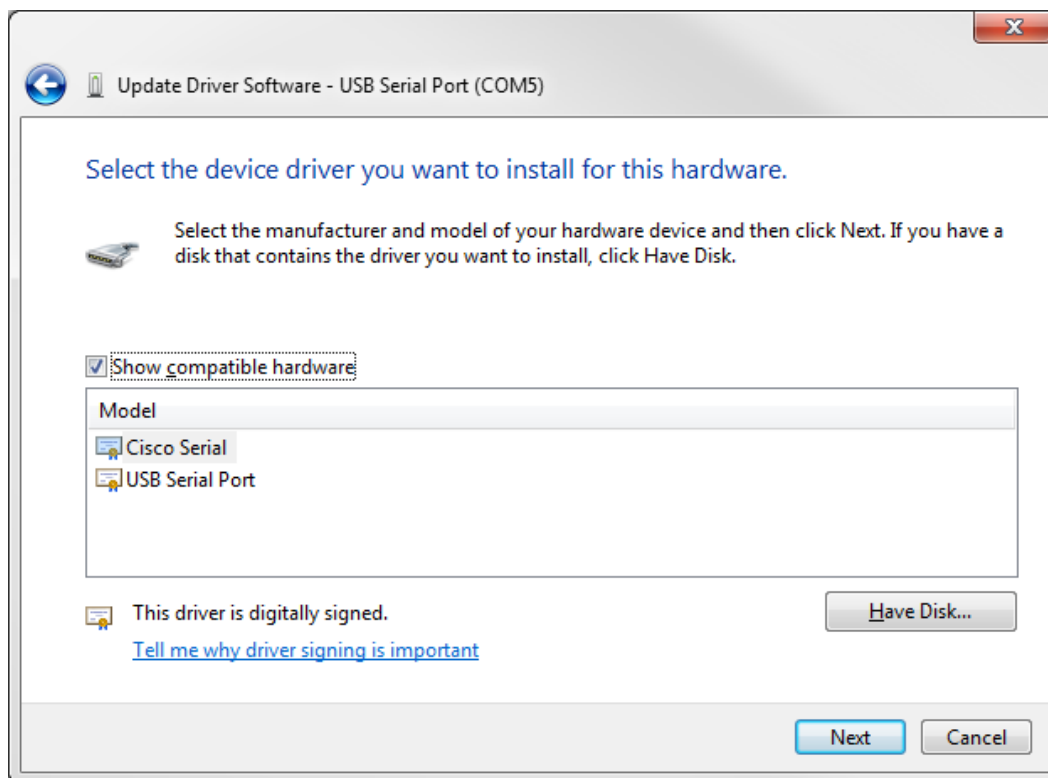
- d. Choose **Browse my computer for driver software**.



- e. Choose **Let me pick from a list of device drivers on my computer** and click **Next**.

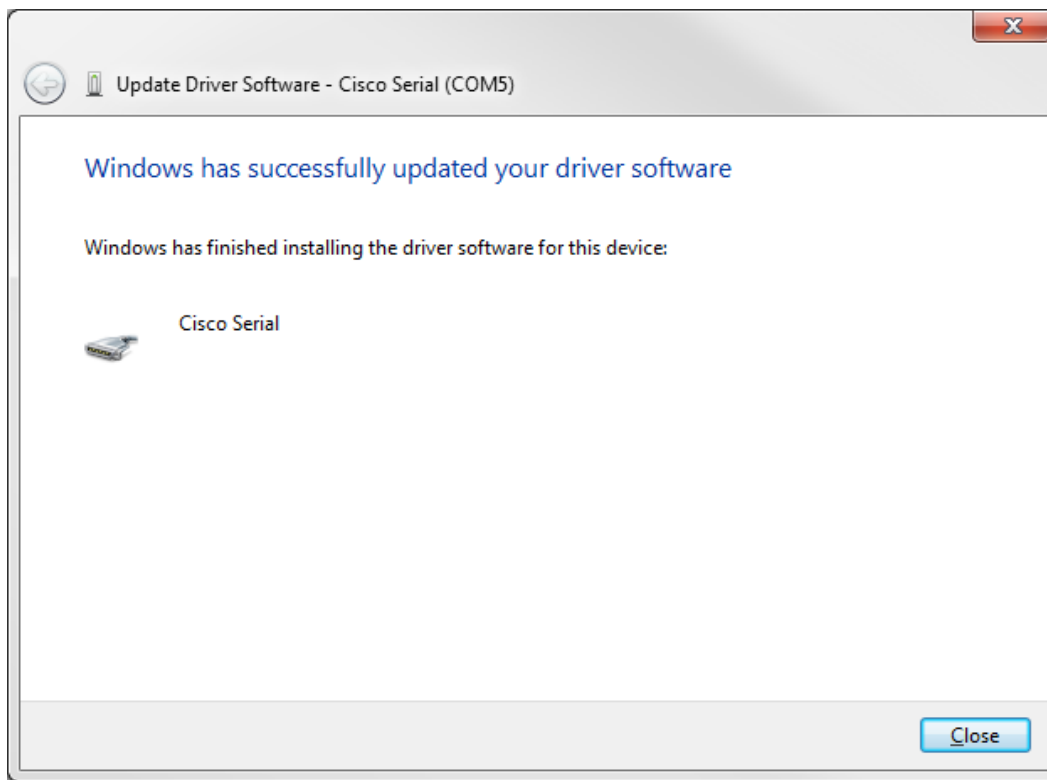


- f. Choose the **Cisco Serial** driver and click **Next**.

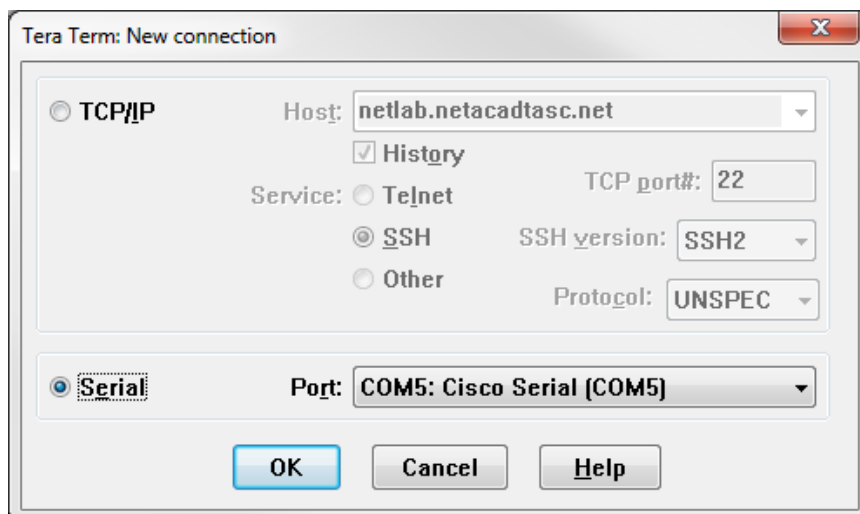


Lab - Establishing a Console Session with Tera Term

- g. Note the port number assigned at the top of the window. In this sample, COM 5 is used for communication with the router. Click **Close**.



- h. Open Tera Term. Click the **Serial** radio button and choose the appropriate serial port, which is **Port COM5: Cisco Serial (COM 5)** in this example. This port should now be available for communication with the router. Click **OK**.



Reflection

1. How do you prevent unauthorized personnel from accessing your Cisco device through the console port?

Physically secure the device and use password protection

2. What are the advantages and disadvantages of using the serial console connection compared to the USB console connection to a Cisco router or switch?

It depends on the port availability on the PC and the router or switch. If the PC has a serial port and a DB9-to-RJ45 cable is available, it is generally easier to connect to the router or switch using the serial console port. If the PC does not have a serial port, a third party USB-to-Serial adapter can be used. Cisco switches do not have mini-USB console ports, so connecting via USB is not an option. If you are frequently connecting to a Cisco router that has a mini USB console port, this can be the most effective method after the Cisco drivers are installed because nearly all newer PCs have USB ports.

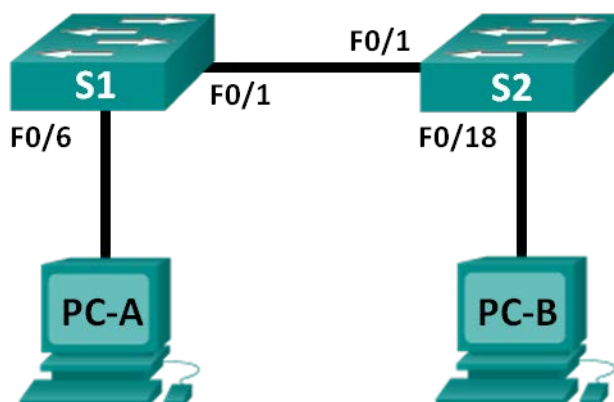
Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Lab - Building a Simple Network (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
PC-A	NIC	192.168.1.10	255.255.255.0
PC-B	NIC	192.168.1.11	255.255.255.0

Objectives

Part 1: Set Up the Network Topology (Ethernet only)

Part 2: Configure PC Hosts

Part 3: Configure and Verify Basic Switch Settings

Background / Scenario

Networks are constructed of three major components: hosts, switches, and routers. In this lab, you will build a simple network with two hosts and two switches. You will also configure basic settings including hostname, local passwords, and login banner. Use **show** commands to display the running configuration, IOS version, and interface status. Use the **copy** command to save device configurations.

You will apply IP addressing for this lab to the PCs to enable communication between these two devices. Use the **ping** utility to verify connectivity.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. Refer to Appendix A for the procedure to initialize and reload a switch.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)

- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Instructor Note: The Ethernet ports on the 2960 switches are autosensing and will accept either a straight-through or a cross-over cable for all connections. If the switches used in the topology are other than the 2960 model, then it is likely that a cross-over cable will be needed to connect the two switches.

Part 1: Set Up the Network Topology (Ethernet only)

In Part 1, you will cable the devices together according to the network topology.

Step 1: Power on the devices.

Power on all devices in the topology. The switches do not have a power switch; they will power on as soon as you plug in the power cord.

Step 2: Connect the two switches.

Connect one end of an Ethernet cable to F0/1 on S1 and the other end of the cable to F0/1 on S2. You should see the lights for F0/1 on both switches turn amber and then green. This indicates that the switches have been connected correctly.

Step 3: Connect the PCs to their respective switches.

- a. Connect one end of the second Ethernet cable to the NIC port on PC-A. Connect the other end of the cable to F0/6 on S1. After connecting the PC to the switch, you should see the light for F0/6 turn amber and then green, indicating that PC-A has been connected correctly.
- b. Connect one end of the last Ethernet cable to the NIC port on PC-B. Connect the other end of the cable to F0/18 on S2. After connecting the PC to the switch, you should see the light for F0/18 turn amber and then green, indicating that the PC-B has been connected correctly.

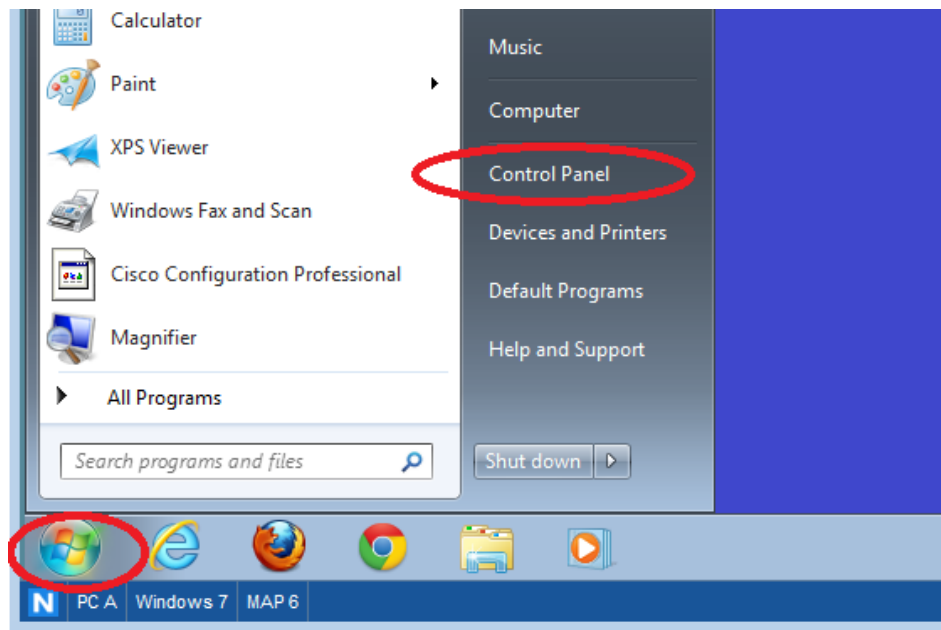
Step 4: Visually inspect network connections.

After cabling the network devices, take a moment to carefully verify the connections to minimize the time required to troubleshoot network connectivity issues later.

Part 2: Configure PC Hosts

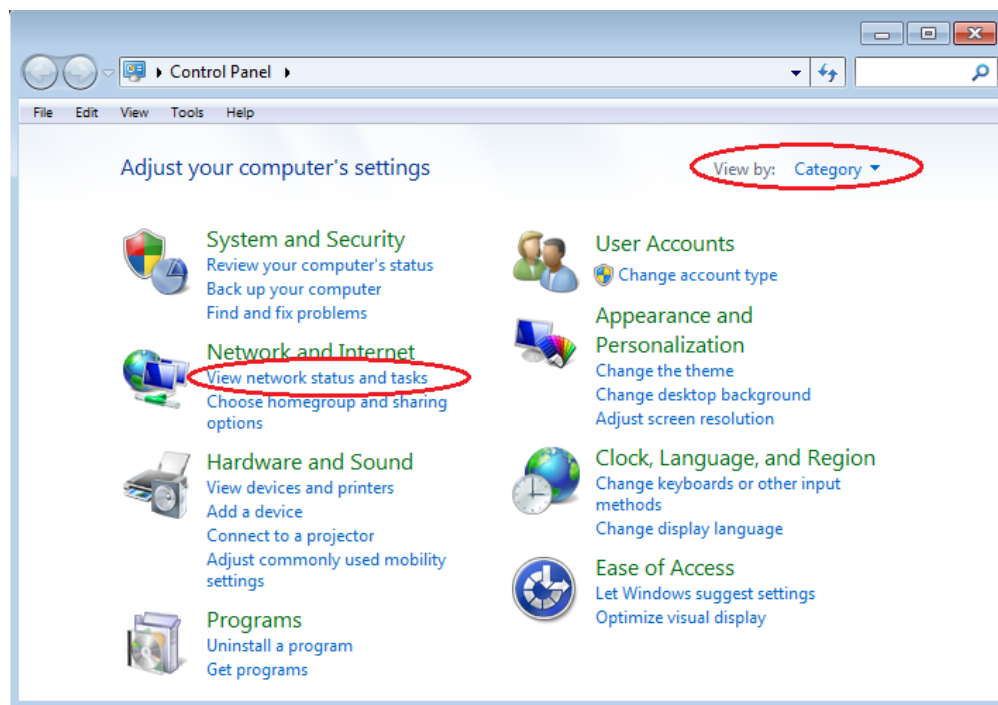
Step 1: Configure static IP address information on the PCs.

- a. Click the **Windows Start** icon and then select **Control Panel**.

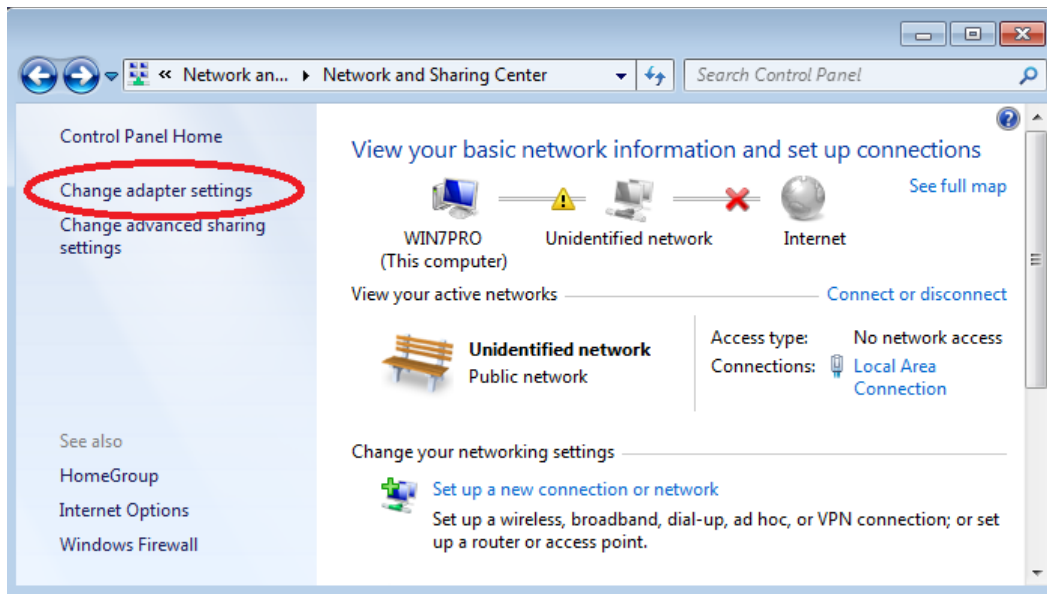


- b. In the Network and Internet section, click the **View network status and tasks** link.

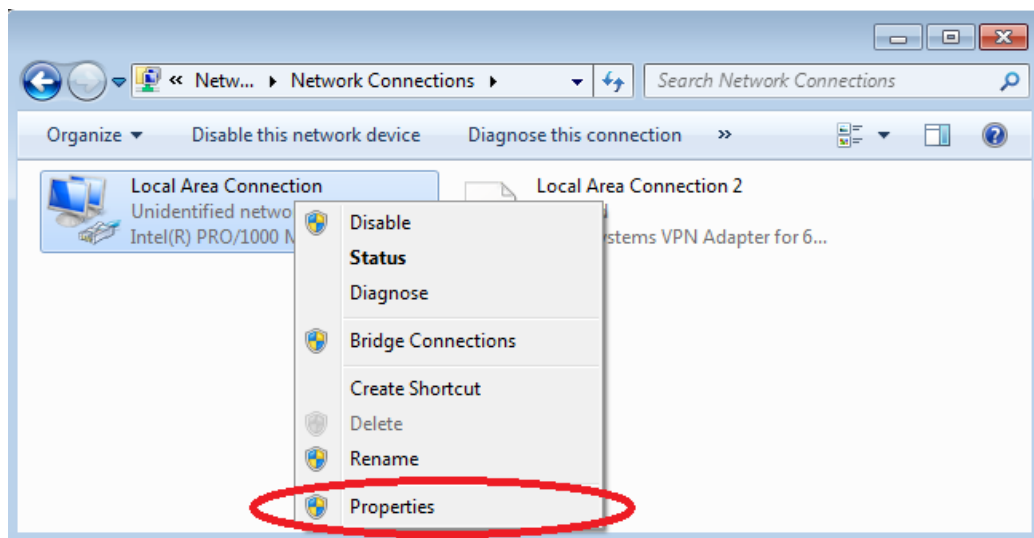
Note: If the Control Panel displays a list of icons, click the drop-down option next to the **View by:** and change this option to display by **Category**.



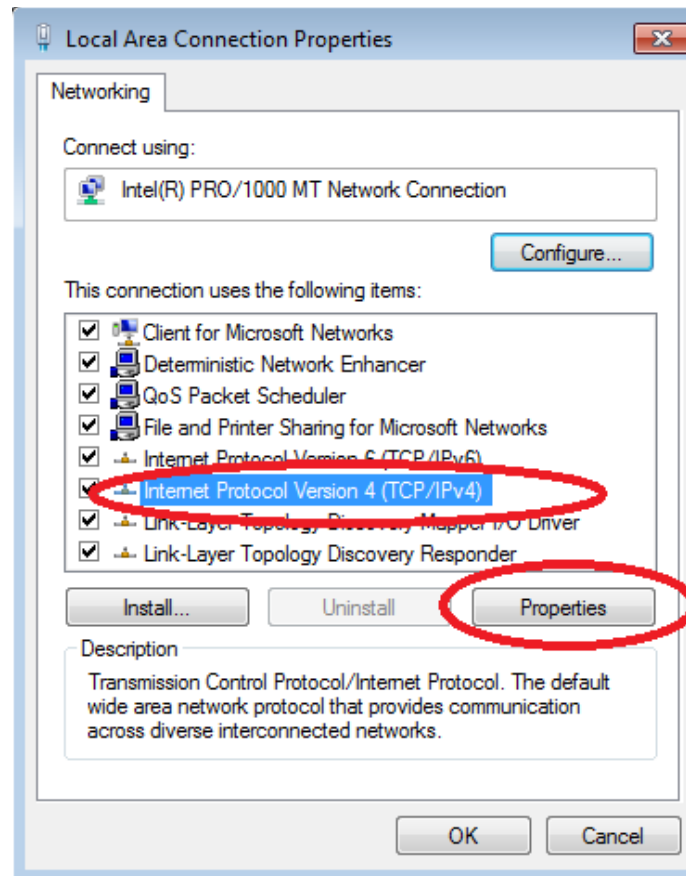
- c. In the left pane of the Network and Sharing Center window, click the **Change adapter settings** link.



- d. The Network Connections window displays the available interfaces on the PC. Right-click the **Local Area Connection** interface and select **Properties**.

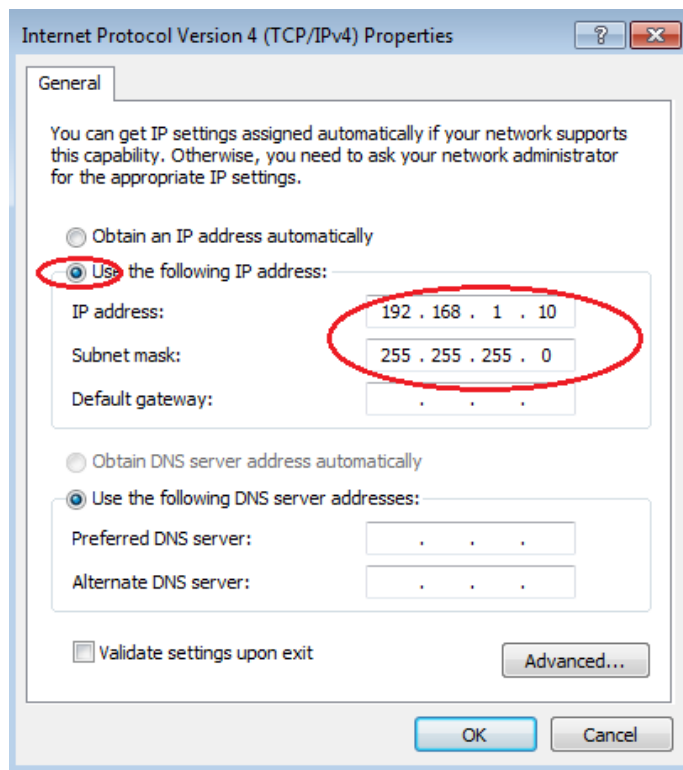


- e. Select the **Internet Protocol Version 4 (TCP/IPv4)** option and then click **Properties**.



Note: You can also double-click **Internet Protocol Version 4 (TCP/IPv4)** to display the Properties window.

- f. Click the **Use the following IP address** radio button to manually enter an IP address, subnet mask, and default gateway.



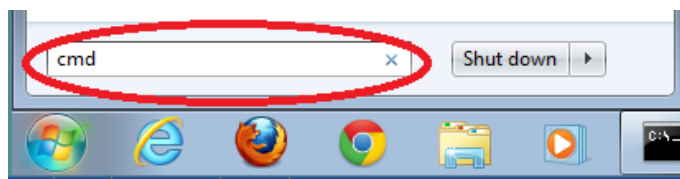
Note: In the above example, the IP address and subnet mask have been entered for PC-A. The default gateway has not been entered, because there is no router attached to the network. Refer to the Addressing Table on page 1 for PC-B's IP address information.

- g. After all the IP information has been entered, click **OK**. Click **OK** on the Local Area Connection Properties window to assign the IP address to the LAN adapter.
- h. Repeat the previous steps to enter the IP address information for PC-B.

Step 2: Verify PC settings and connectivity.

Use the command prompt (**cmd.exe**) window to verify the PC settings and connectivity.

- a. From PC-A, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



- b. The cmd.exe window is where you can enter commands directly to the PC and view the results of those commands. Verify your PC settings by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information.

```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC-A
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . : 00-50-56-BE-6C-89
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::d428:7de2:997c:b05a%11(Preferred)
   IPv4 Address. . . . . : 192.168.1.10(Preferred)
   Subnet Mask . . . . . : 255.255.255.0
   Default Gateway . . . . . :
   DHCPv6 IAID . . . . . : 234884137
   DHCPv6 Client DUID. . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-54-44
```

- c. Type **ping 192.168.1.11** and press Enter.

```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.11

Pinging 192.168.1.11 with 32 bytes of data:
Reply from 192.168.1.11: bytes=32 time=1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128
Reply from 192.168.1.11: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\NetAcad>
```

Were the ping results successful? _____ **Yes**

If not, troubleshoot as necessary.

Note: If you did not get a reply from PC-B, try to ping PC-B again. If you still do not get a reply from PC-B, try to ping PC-A from PC-B. If you are unable to get a reply from the remote PC, then have your instructor help you troubleshoot the problem.

Instructor Note: If the first ICMP packet times out, this could be a result of the PC resolving the destination address. This should not occur if you repeat the ping as the address is now cached.

Part 3: Configure and Verify Basic Switch Settings

Step 1: Console into the switch.

Using Tera Term, establish a console connection to the switch from PC-A.

Step 2: Enter privileged EXEC mode.

You can access all switch commands in privileged EXEC mode. The privileged EXEC command set includes those commands contained in user EXEC mode, as well as the **configure** command through which access to the remaining command modes are gained. Enter privileged EXEC mode by entering the **enable** command.

```
Switch> enable
Switch#
```

The prompt changed from **Switch>** to **Switch#** which indicates privileged EXEC mode.

Step 3: Enter configuration mode.

Use the **configuration terminal** command to enter configuration mode.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

The prompt changed to reflect global configuration mode.

Step 4: Give the switch a name.

Use the **hostname** command to change the switch name to **S1**.

```
Switch(config)# hostname S1
S1(config)#
```

Step 5: Prevent unwanted DNS lookups.

To prevent the switch from attempting to translate incorrectly entered commands as though they were hostnames, disable the Domain Name System (DNS) lookup.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Step 6: Enter local passwords.

To prevent unauthorized access to the switch, passwords must be configured.

```
S1(config)# enable secret class
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

Step 7: Enter a login MOTD banner.

A login banner, known as the message of the day (MOTD) banner, should be configured to warn anyone accessing the switch that unauthorized access will not be tolerated.

The **banner motd** command requires the use of delimiters to identify the content of the banner message. The delimiting character can be any character as long as it does not occur in the message. For this reason, symbols, such as the **#**, are often used.

```
S1(config)# banner motd #
Enter TEXT message. End with the character '#'.

```

```
Unauthorized access is strictly prohibited and prosecuted to the full extent
of the law. #
S1(config)# exit
S1#
```

Step 8: Save the configuration.

Use the **copy** command to save the running configuration to the startup file on non-volatile random access memory (NVRAM).

```
S1# copy running-config startup-config
Destination filename [startup-config]? [Enter]
Building configuration...
[OK]
S1#
```

Step 9: Display the current configuration.

The **show running-config** command displays the entire running configuration, one page at a time. Use the spacebar to advance paging. The commands configured in Steps 1 – 8 are highlighted below.

```
S1# show running-config
Building configuration...

Current configuration : 1409 bytes
!
! Last configuration change at 03:49:17 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!

<output omitted>

!
banner motd ^C
```

```
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
  password cisco
  login
line vty 0 4
  login
line vty 5 15
  login
!
end

S1#
```

Step 10: Display the IOS version and other useful switch information.

Use the **show version** command to display the IOS version that the switch is running, along with other useful information. Again, you will need to use the spacebar to advance through the displayed information.

```
S1# show version
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Sat 28-Jul-12 00:29 by prod_rel_team

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE
(fc1)

S1 uptime is 1 hour, 38 minutes
System returned to ROM by power-on
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.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.

Lab - Building a Simple Network

cisco WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.

Processor board ID FCQ1628Y5LE

Last reset from power-on

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 : 0C:D9:96:E2:3D:00

Motherboard assembly number : 73-12600-06

Power supply part number : 341-0097-03

Motherboard serial number : FCQ16270N5G

Power supply serial number : DCA1616884D

Model revision number : R0

Motherboard revision number : A0

Model number : WS-C2960-24TT-L

System serial number : FCQ1628Y5LE

Top Assembly Part Number : 800-32797-02

Top Assembly Revision Number : A0

Version ID : V11

CLEI Code Number : COM3L00BRF

Hardware Board Revision Number : 0x0A

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
*	1 26	WS-C2960-24TT-L	15.0(2)SE	C2960-LANBASEK9-M

Configuration register is 0xF

S1#

Step 11: Display the status of the connected interfaces on the switch.

To check the status of the connected interfaces, use the **show ip interface brief** command. Press the spacebar to advance to the end of the list.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
FastEthernet0/1	unassigned	YES	unset	up	up
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down

```
FastEthernet0/10      unassigned      YES unset  down      down
FastEthernet0/11      unassigned      YES unset  down      down
FastEthernet0/12      unassigned      YES unset  down      down
FastEthernet0/13      unassigned      YES unset  down      down
FastEthernet0/14      unassigned      YES unset  down      down
FastEthernet0/15      unassigned      YES unset  down      down
FastEthernet0/16      unassigned      YES unset  down      down
FastEthernet0/17      unassigned      YES unset  down      down
FastEthernet0/18      unassigned      YES unset  down      down
FastEthernet0/19      unassigned      YES unset  down      down
FastEthernet0/20      unassigned      YES unset  down      down
FastEthernet0/21      unassigned      YES unset  down      down
FastEthernet0/22      unassigned      YES unset  down      down
FastEthernet0/23      unassigned      YES unset  down      down
FastEthernet0/24      unassigned      YES unset  down      down
GigabitEthernet0/1    unassigned      YES unset  down      down
GigabitEthernet0/2    unassigned      YES unset  down      down
S1#
```

Step 12: Repeat Steps 1 to 12 to configure switch S2.

The only difference for this step is to change the hostname to S2.

Step 13: Record the interface status for the following interfaces.

Interface	S1		S2	
	Status	Protocol	Status	Protocol
F0/1	Up	Up	Up	Up
F0/6	Up	Up	Down	Down
F0/18	Down	Down	Up	Up
VLAN 1	Up	Up	Up	Up

Why are some FastEthernet ports on the switches are up and others are down?

The FastEthernet ports are up when cables are connected to the ports unless they were manually shutdown by the administrators. Otherwise, the ports would be down.

Reflection

What could prevent a ping from being sent between the PCs?

Wrong IP address, media disconnected, switch powered off or ports administratively down, firewall.

Note: It may be necessary to disable the PC firewall to ping between PCs.

Appendix A: Initializing and Reloading a Switch

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash
```

```
Directory of flash:/
```

2	-rwx	1919	Mar 1 1993 00:06:33 +00:00	private-config.text
3	-rwx	1632	Mar 1 1993 00:06:33 +00:00	config.text
4	-rwx	13336	Mar 1 1993 00:06:33 +00:00	multiple-fs
5	-rwx	11607161	Mar 1 1993 02:37:06 +00:00	c2960-lanbasek9-mz.150-2.SE.bin
6	-rwx	616	Mar 1 1993 00:07:13 +00:00	vlan.dat

```
32514048 bytes total (20886528 bytes free)
```

```
Switch#
```

Step 3: Delete the VLAN file.

- If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

- When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

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

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

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

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

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

Device Configs

Switch S1 (complete)

```
S1#sh run
```

```
Building configuration...
```

```
Current configuration : 1514 bytes
```

```
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
```

```
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!
```



```
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited and prosecuted to the full extent of the
law. ^C
!
line con 0
  password cisco
  login
line vty 0 4
  login
line vty 5 15
  login
!
end
```

Switch S2 (complete)

```
S2#sh run
Building configuration...

*Mar  1 03:20:01.648: %SYS-5-CONFIG_I: Configured from console by console
Current configuration : 1514 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S2
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
```

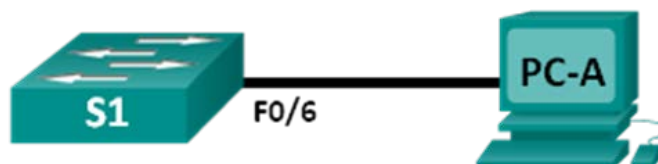
```
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
```

```
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
no ip address  
!  
ip http server  
ip http secure-server  
!  
banner motd ^C  
Unauthorized access is strictly prohibited and prosecuted to the full extent of the  
law. ^C  
!  
line con 0  
password cisco  
login  
line vty 0 4  
login  
line vty 5 15  
login  
!  
end
```

Lab - Configuring a Switch Management Address (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask
S1	VLAN 1	192.168.1.2	255.255.255.0
PC-A	NIC	192.168.1.10	255.255.255.0

Objectives

Part 1: Configure a Basic Network Device

Part 2: Verify and Test Network Connectivity

Background / Scenario

Cisco switches have a special interface, known as a switch virtual interface (SVI). The SVI can be configured with an IP address, commonly referred to as the management address. The management address is used for remote access to the switch to display or configure settings.

In this lab, you will build a simple network using Ethernet LAN cabling and access a Cisco switch using the console and remote access methods. You will configure basic switch settings, IP addressing, and demonstrate the use of a management IP address for remote switch management. The topology consists of one switch and one host using only Ethernet and console ports.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the available commands and output produced might vary from what is shown in the labs.

Note: Make sure that the switch has been erased and has no startup configuration. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure a Basic Network Device

In Part 1, you will set up the network and configure basic settings, such as hostnames, interface IP addresses, and passwords.

Step 1: Cable the network.

- a. Cable the network as shown in the topology.
- b. Establish a console connection to the switch from PC-A.

Step 2: Configure basic switch settings.

In this step, you will configure basic switch settings, such as hostname, and configure an IP address for the SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch will be managed. Telnet and SSH are two of the most common management methods. However, Telnet is a very insecure protocol. All information flowing between the two devices is sent in plaintext. Passwords and other sensitive information can be easily viewed if captured by a packet sniffer.

- a. Assuming the switch did not have a configuration file stored in NVRAM, you will be at the user EXEC mode prompt on the switch. The prompt will be `Switch>`. Enter privileged EXEC mode.

```
Switch> enable
Switch#
```

- b. Use the privileged EXEC **show running-config** command to verify a clean configuration file. If a configuration file was previously saved, it will have to be removed. Depending on the switch model and IOS version, your configuration may look slightly different. However, there should not be any configured passwords or IP address set. If your switch does not have a default configuration, ask your instructor for help.
- c. Enter global configuration mode and assign the switch hostname.

```
Switch# configure terminal
Switch(config)# hostname S1
S1(config)#
```

- d. Configure the switch password access.

```
S1(config)# enable secret class
S1(config)#
```

- e. Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

- f. Configure a login MOTD banner.

```
S1(config)# banner motd #
Enter Text message. End with the character '#'.
Unauthorized access is strictly prohibited. #
```

- g. Verify your access setting by moving between modes.

```
S1(config)# exit
S1#
S1# exit
Unauthorized access is strictly prohibited.
S1>
```

What shortcut keys are used to go directly from global configuration mode to privileged EXEC mode?

Ctrl+Z

- h. Return to privileged EXEC mode from user EXEC mode.

```
S1> enable
Password: class
S1#
```

Note: The password will not show up on the screen when entering.

- i. Enter global configuration mode to set the SVI IP address to allow remote switch management.

```
S1# config t
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.2 255.255.255.0
S1(config-if)# no shut
S1(config-if)# exit
S1(config)#
```

- j. Restrict console port access. The default configuration is to allow all console connections with no password needed.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# exit
S1(config)#
```

- k. Configure the VTY line for the switch to allow Telnet access. If you do not configure a VTY password, you will not be able to telnet to the switch.

```
S1(config)# line vty 0 4
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
```

```
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Step 3: Configure an IP address on PC-A.

- a. Assign the IP address and subnet mask to the PC, as shown in the Addressing Table. The procedure for assigning an IP address on a PC running Windows 7 is described below:

- 1) Click the **Windows Start** icon > **Control Panel**.
- 2) Click **View By:** > **Category**.
- 3) Choose **View network status and tasks** > **Change adapter settings**.
- 4) Right-click **Local Area Network Connection** and select **Properties**.
- 5) Choose **Internet Protocol Version 4 (TCP/IPv4)**, click **Properties** > **OK**.
- 6) Click the **Use the following IP address** radio button and enter the IP address and subnet mask.

Part 2: Verify and Test Network Connectivity

You will now verify and document the switch configuration, test end-to-end connectivity between PC-A and S1, and test the remote management capability of the switch.

Step 1: Display the S1 device configuration.

- a. Return to your console connection using Tera Term on PC-A. Issue the **show run** command to display and verify your switch configuration. A sample configuration is shown below. The settings you configured are highlighted in yellow. The other configuration settings are IOS defaults.

```
S1# show run
Building configuration...

Current configuration : 1508 bytes
!
! Last configuration change at 00:06:11 UTC Mon Mar 1 1993
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2

<output omitted>

interface FastEthernet0/24
!
```

```
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C
Unauthorized access is strictly prohibited. ^C
!
line con 0
password cisco
login
line vty 0 4
password cisco
login
line vty 5 15
login
!
end
```

- b. Verify the status of your SVI management interface. Your VLAN 1 interface should be up/up and have an IP address assigned. Notice that switch port F0/6 is also up because PC-A is connected to it. Because all switch ports are initially in VLAN 1, by default, you can communicate with the switch using the IP address you configured for VLAN 1.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.2	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	down	down
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down

FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

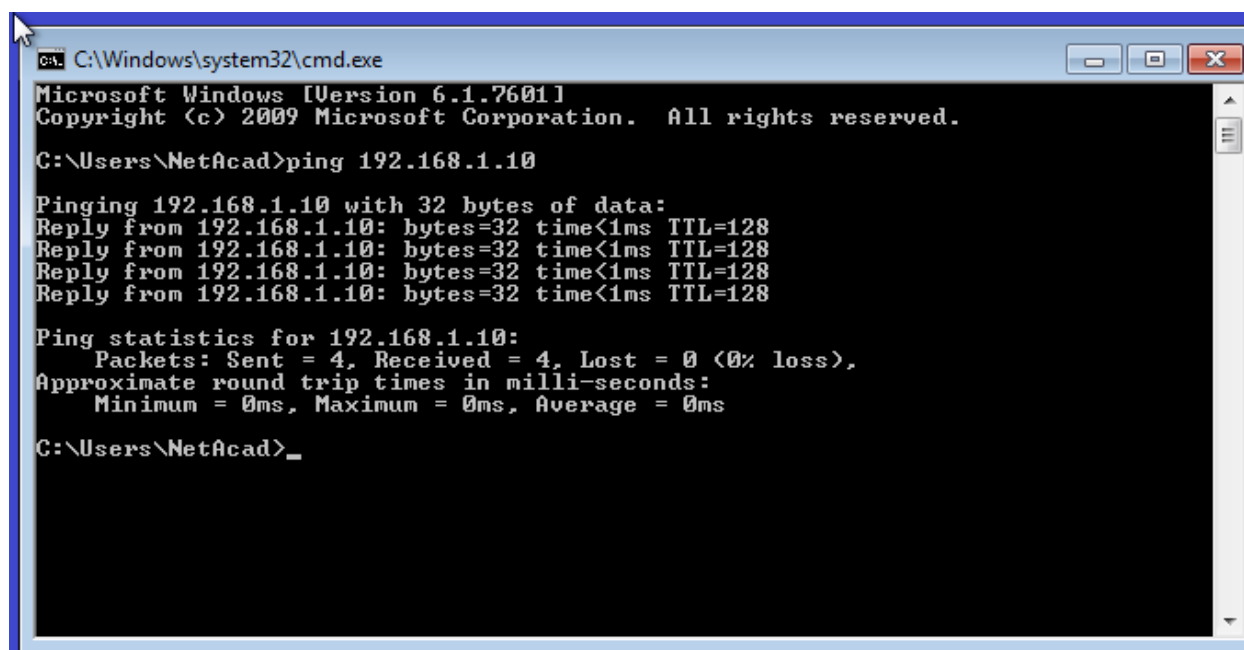
Step 2: Test end-to-end connectivity.

Open a command prompt window (cmd.exe) on PC-A by clicking the **Windows Start** icon and entering **cmd** into the **Search for programs and files** field. Verify the IP address of PC-A by using the **ipconfig /all** command. This command displays the PC hostname and the IPv4 address information. Ping PC-A's address and the management address of S1.

- Ping the PC-A address first.

```
C:\Users\NetAcad> ping 192.168.1.10
```

Your output should be similar to the following screen:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\NetAcad>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NetAcad>_
```

- Ping the SVI management address of S1.

```
C:\Users\NetAcad> ping 192.168.1.2
```

Your output should be similar to the following screen. If ping results are not successful, troubleshoot the basic device configurations. You should check both the physical cabling and IP addressing if necessary.

```
C:\Users\NetAcad>
C:\Users\NetAcad>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time=2ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 1ms

C:\Users\NetAcad>
```

Step 3: Test and verify the remote management of S1.

You will now use Telnet to remotely access the switch S1 using the SVI management address. In this lab, PC-A and S1 reside side by side. In a production network, the switch could be in a wiring closet on the top floor while your management PC is located on the ground floor. Telnet is not a secure protocol. However, you will use it in this lab to test remote access. All information sent by Telnet, including passwords and commands, is sent across the session in plaintext. In subsequent labs, you will use SSH to remotely access network devices.

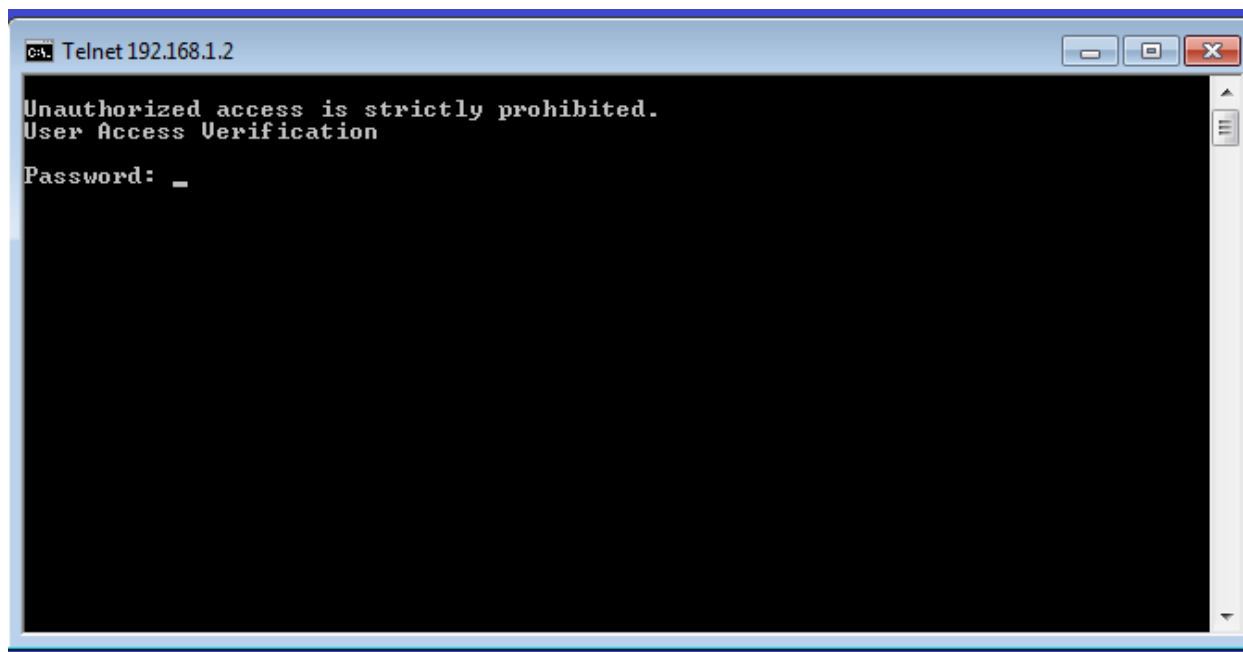
Note: Windows 7 does not natively support Telnet. The administrator must enable this protocol. To install the Telnet client, open a command prompt window and type `pkgmgr /iu:"TelnetClient"`.

```
C:\Users\NetAcad> pkgmgr /iu:"TelnetClient"
```

- a. With the command prompt window still open on PC-A, issue a Telnet command to connect to S1 via the SVI management address. The password is **cisco**.

```
C:\Users\NetAcad> telnet 192.168.1.2
```

Your output should be similar to the following screen:



```
C:\> Telnet 192.168.1.2

Unauthorized access is strictly prohibited.
User Access Verification
Password: _
```

- b. After entering the **cisco** password, you will be at the user EXEC mode prompt. Type **enable** at the prompt. Enter the **class** password to enter privileged EXEC mode and issue a **show run** command.

Step 4: Save the configuration file.

- a. From your Telnet session, issue the **copy run start** command at the prompt.

```
S1# copy run start
Destination filename [startup-config]? [Enter]
Building configuration ..
S1#
```

- b. Exit the Telnet session by typing **quit**. You will be returned to the Windows 7 command prompt.

Reflection

Why must you use a console connection to initially configure the switch? Why not connect to the switch via Telnet or SSH?

No IP addressing parameters are configured yet. Initially, a switch has no networking configured.

Device Configs

Switch S1(Complete)

```
S1#show run
Building configuration...
!
Current configuration : 1508 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
```

```
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
```

Lab - Configuring a Switch Management Address

```
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
 ip address 192.168.1.2 255.255.255.0  
!  
ip http server  
ip http secure-server  
!  
banner motd ^C  
Unauthorized access is strictly prohibited. ^C  
!  
line con 0  
 password cisco  
 login  
line vty 0 4  
 password class  
 login  
line vty 5 15  
 login  
!  
end
```

Class Activity - Tutor me! (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Configure initial settings on a network device using the Cisco IOS software.

Background / Scenario

(Students will work in pairs. Packet Tracer is required to be used with this activity.)

Assume that a new colleague has asked you for an orientation to the Cisco IOS CLI. This colleague has never worked with Cisco devices before.

You explain the basic CLI commands and structure, because you want your colleague to understand that the CLI is a simple, yet powerful, command language that can be easily understood and navigated.

Use Packet Tracer and one of the activities available in this chapter as a simple network model. Focus on these areas:

- While the commands are technical, do they resemble any statements from plain English?
- How is the set of commands organized into subgroups or modes? How does an administrator know which mode he or she is currently using?
- What are the individual commands to configure the basic settings of a Cisco device? How would you explain this command in laymen's terms? Use parallels to real life whenever appropriate.

Suggest how to group different commands together according to their modes so that a minimum number of moves between modes will be needed.

Instructor Note: This optional Modeling Activity may be used as a graded assignment. However, its purpose is to help students reflect on the knowledge acquired from Chapter 2, focusing on how the Cisco IOS is used directly to configure intermediary devices. Instructor facilitation of the discussion should encourage student-to-student discussions of each other's work.

Required Resources

- Packet Tracer
- Any simple network model activity available from Chapter 2

Reflection

1. After completing Chapter 2, do you feel as though you have a concrete understanding of what the Cisco IOS does and how it operates? What were some of the difficulties you encountered when explaining the basic CLI commands and structure to your colleague? If you were the "new colleague," what would be some of the difficulties that you would have learning the basic CLI commands and structure?

2. Answer the following questions, and discuss your answers with the entire class:
 - a. While the commands are technical, do they resemble any statements from plain English?

- b. How is the set of commands organized into subgroups or modes? How does an administrator know which mode he or she is currently using?
- c. What are the individual commands to configure the basic settings of a Cisco device? How would you explain this command in laymen's terms? Use parallels to real life whenever appropriate.
- d. With the help of your colleague, try to suggest how to group different commands together according to their modes so that a minimum number of moves between modes will be needed.

(Answers will vary (represented below are Chapter 2 content-based variations):

- a. While the commands are technical, do they resemble any statements from plain English?
Absolutely. Keywords like enable, password, banner, address, shutdown are ordinary words whose meaning in CLI is appropriately adapted but still carrying a strong relevancy to their common usage.
- b. How is the set of commands organized into subgroups, or modes? How does an administrator know which mode is he/she using currently?
First, the level of access to CLI can either be a user (user EXEC) level, or an administrator level (privileged EXEC). From the administrator level, the configuration mode can be accessed that is internally divided into global configuration mode, line configuration mode, interface configuration mode and other modes as necessary. The administrator is informed about the current mode in the prompt where the > symbol represents user access level, # represents administrator access level, and optional keywords in parentheses designate the configuration mode and possible submodes.
- c. What are the individual commands to access and configure the basic settings of a Cisco device? How would you explain these commands in layman terms? Use parallels to real life whenever appropriate.
- enable** – become empowered to complete control over a device
- configure terminal** – Start the configuration editor, accepting changes from the terminal
- hostname** – Assign a name to a device
- service password-encryption** – Causes the device to obscure all entered passwords in the configuration so that they cannot be eavesdropped
- line con 0** – Enter the configuration of the line, or the “socket”, labeled with CONSOLE 0 on the device and used to manage the device
- line vty 0 4** – Enter the configuration of 5 virtual “sockets” that allow managing the device remotely, through the network
- password** – Set up a password to be used when accessing the device
- login** – Protect the access using a login procedure requiring a password defined used the password command
- exit** – Leave the current mode and exit to the higher placed mode.
- enable secret** – The secret phrase which protects the usage of the enable command

banner – The message displayed to a user that tries to access the device

interface Vlan 1 – enter the configuration mode of the interface called Vlan1

description – Assign a textual comment to an interface to help the administrator know what is the purpose and location of the interface

ip address – Assign a numerical IP address to an interface

no shutdown – Removes the shutdown command and thereby making an interface active

end – Exit the configuration editor

Moving through the configuration and making changes to the device settings is like navigating in a maze. Each configuration mode is like a chamber in a maze. Even if you know the map of the maze, you may still move through the maze in a disorganized way, possibly never finding a way out. Similarly, even if you know the meaning of individual commands and the modes in which they are located, the way you move through these modes when configuring a device depends mostly on you.

- d. With the help of your colleague, try to suggest how to group different commands together according to their modes so that a minimum number of moves between modes is needed.

One of possible effective command sequences for configuring a device is:

```
enable
configure terminal
hostname AtlantaSw
service password-encryption
banner login ^
```

```
Access to this device permitted only to authorized personnel!
```

```
^
enable secret V3ry5ecr3tP4ssw0rd
line con 0
  password 5ecr3tP4ssw0rd
  login
  exit
line vty 0 4
  password 5ecr3tP4ssw0rd
  login
  exit
interface Vlan 1
  ip address 192.0.2.11 255.255.255.0
  no shutdown
end
```

An ineffective way of configuring would be, for example:

```
enable
configure terminal
line con 0
  password 5ecr3tP4ssw0rd
  exit
hostname AtlantaSw
service password-encryption
line vty 0 4
```


Class Activity - Tutor me!

```
password 5ecr3tP4ssw0rd
exit
banner login ^
```

```
Access to this device permitted only to authorized personnel!
```

```
^
line con 0
  login
  exit
interface Vlan 1
  ip address 192.0.2.11 255.255.255.0
  exit
line vty 0 4
  login
  exit
enable secret V3ry5ecr3tP4ssw0rd
interface Vlan 1
  no shutdown
end
```

(Note that while both configurations lead to the same resulting set of settings, the second configuration is slightly larger (because of repetitive entering individual modes again and again) and is very difficult to follow because the flow of commands is practically random and does not follow their logical sequence and modal commonality Instructor)

Identify elements of the model that map to IT content:

- Commands
- Modes
- Efficient orientation in configuration mode
- Real-world customer relations skills

Class Activity – Designing a Communications System (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain the role of protocols and standards organizations in facilitating interoperability in network communications.

Background / Scenario

You have just purchased a new automobile for your personal use. After driving the car for a week or so, you find that it is not working correctly. Discussing the problem with several of your peers, you decide to take it to an automotive repair facility that they highly recommend. It is the only repair facility located in close proximity.

When you arrive at the repair facility, you find that all the mechanics speak another language. You are having difficulty explaining the automobile's performance problems, but the repairs really need to be done. You are not sure you can drive it back home to research other options.

You must find a way to work with the repair facility to ensure your automobile is fixed correctly.

How will you communicate with the mechanics? Design a communications model to ensure that the car is properly repaired.

Instructor Note: This Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of how a communications system facilitates the transfer of data from source to destination (personally and in corporate practice). Discussion should be initiated as a result of this activity.

Reflection

What steps did you identify as important to communicating your repair request? Justify your answer.

To resolve this issue, some steps might include:

Establishing a language for communication (could be voice, written, or kinesthetic/physical).

Very carefully (in small steps), explaining the problem experienced with the automobile (again voice, written/pictures, or kinesthetic/physical representations).

Asking the mechanic to confirm his/her understanding of the problem.

Waiting for the repair to be done.

Driving the automobile to ensure repairs were successful.

Closing the meeting by paying for the repairs and thanking the mechanic.

Identify elements of the model that map to IT content:

- Establishing a language to communicate (Application protocol)
- Dividing the message into small steps to facilitate understanding of the problem to be solved a little at a time (Transfer protocol).
- Checking to see if the message has been delivered and correctly understood to the mechanic who will be performing the repairs. (Internet protocol)
- Delivery of automobile and wait time for repairs (Network Access protocol)



Lab - Researching Networking Standards (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Research Networking Standards Organizations

Part 2: Reflect on Internet and Computer Networking Experiences

Background / Scenario

Using web search engines like Google, research the non-profit organizations that are responsible for establishing international standards for the Internet and the development of Internet technologies.

Required Resources

Device with Internet access

Part 1: Research Networking Standards Organizations

In Part 1, you will identify some of the major standards organizations and important characteristics, such as the number of years in existence, the size of their membership, the important historical figures, some of the responsibilities and duties, organizational oversight role, and the location of the organization's headquarters.

Use a web browser or websites for various organizations to research information about the following organizations and the people who have been instrumental in maintaining them.

You can find answers to the questions below by searching the following organizational acronyms and terms: ISO, ITU, ICANN, IANA, IEEE, EIA, TIA, ISOC, IAB, IETF, W3C, RFC, and Wi-Fi Alliance.

1. Who is Jonathan B. Postel and what is he known for? (Search hint: Jon Postel)

Jonathan Postel was an American computer scientist who made significant contributions to the development of the Internet standards, to the creation of Internet Assigned Numbers Authority (IANA) and as the RFC Editor.

2. Which two related organizations are responsible for managing the top-level domain name space and the root Domain Name System (DNS) name servers on the Internet? (Search hint: ICANN, IANA)

International Corporation for Assigned Names and Numbers (ICANN) and Internet Assigned Numbers Authority (IANA)

3. Vinton Cerf has been called one of main fathers of the Internet. What Internet organizations did he chair or help found? What Internet technologies did he help to develop? (Search hint: Vint Cerf, IAB, ISOC, ICANN)

Lab - Researching Networking Standards

Vinton Cerf co-founded Internet Society (ISOC) with Bob Kahn in 1992, helped with the creation of ICANN, and served as the chair of Internet Architecture Board (IAB) from 1989 – 1991.

4. What organization is responsible for publishing Request for Comments (RFC)? (Search hint: IETF)

Internet Engineering Task Force (IETF)

5. What do RFC 349 and RFC 1700 have in common? (Search hint: Request for Comments, Google – RFC 349, RFC 1700)

Port Numbers. The current list can be found at <http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml>

6. What RFC number is the ARPAWOCKY? What is it? (Search hint: Request for Comments, Google – ARPAWOCKY)

RFC 527. The first humorous RFC which then led to IETF launching April fool's day RFC in 1989.

7. Who founded the World Wide Web Consortium (W3C)? (Search hint: W3C)

Founded by Tim Berners-Lee at MIT

8. Name 10 World Wide Web (WWW) standards that the W3C develops and maintains? (Search hint: W3C)

Some samples: Common Gateway Interface (CGI), Document Object Model (DOM), HyperText Markup Language (HTML), Extensible Markup Language (XML)

9. Where is the Institute of Electrical and Electronics Engineers (IEEE) headquarters located and what is the significance of its logo? (Search hint: IEEE)

Institute of Electrical and Electronics Engineers (IEEE) is headquartered in New York City, New York, United States. The IEEE logo is a diamond-shaped design which illustrates the right hand grip rule embedded in Benjamin Franklin's kite.

10. What is the IEEE standard for the Wi-Fi Protected Access 2 (WPA2) security protocol? (Search hint: WPA2)

WPA2 is based on IEEE 802.11i standard. It is commonly used on Wi-Fi wireless network.

11. Is the Wi-Fi Alliance a non-profit standards organization? What is their goal? (Search hint: WiFi Alliance)

Yes, Wi-Fi Alliance is a non-profit trade association, and its goals are to ensure interoperability and backward compatibility and provide innovation support.

12. Who is Hamadoun Touré? (Search hint: ITU)

Hamadoun Touré of Mali is the Secretary General of the International Telecommunication Union (ITU).

13. What is the International Telecommunication Union (ITU) and where is it headquartered? (Search hint: ITU)

ITU is an agency of the United Nations dedicated to the information and communication technologies. ITU's headquarters are located in Geneva, Switzerland.

14. Name the three ITU sectors. (Search hint: ITU)

The three ITU sectors are: Radio communication, Standardization and Development.

15. What does the RS in RS-232 stand for and which organization introduced it? (Search hint: EIA)

RS stands for Recommended Standard. RS-232 was introduced by the Radio Section of Electronic Industries Alliance (EIA).

16. What is SpaceWire? (Search hint: Spacewire, IEEE)

SpaceWire is a standard for high-speed links and networks for use onboard spacecraft.

17. What is the mission of the ISOC and where are its headquarters located? (Search hint: ISOC)

The Internet Society (ISOC) headquarters are located in Reston, Virginia and Geneva, Switzerland. Its mission is "to assure the open development, evolution and use of the Internet for the benefit of all people throughout the world".

18. What organizations does the IAB oversee? (Search hint: IAB)

IAB oversees Internet Engineering Task Force (IETF) and Internet Research Task Force (IRTF).

19. What organization oversees the IAB? (Search hint: IAB, ISOC)

ISOC oversees IAB.

20. When was the ISO founded and where are its headquarters located? (Search hint: ISO)

International Organization for Standardization (ISO) was founded in 1947 and its headquarters are located in Geneva, Switzerland.

Part 2: Reflect on Internet and Computer Networking Experiences

Take a moment to think about the Internet today in relation to the organizations and technologies you have just researched. Then answer the following questions.

1. How do the Internet standards allow for greater commerce? What potential problems could we have if we did not have the IEEE?

Each company would develop its own protocols and products which may not work with equipment from other companies.

2. What potential problems could we have if we did not have the W3C?

We would not have a “common” language on the Internet to display information and communicate with each other.

3. What can we learn from the example of the Wi-Fi Alliance with regard to the necessity of networking standards?

If equipment manufacturers follow the same standards/rules, it allows for interoperability and backward compatibility. This encourages competition, allows for consumer choices and encourages the manufacturers to create better products.

Lab – Installing Wireshark (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding or to provide additional practice or both.

Objectives

Download and Install Wireshark

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. This lab provides instructions for downloading and installing Wireshark.

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access)

Instructor Note: Using a packet sniffer such as Wireshark may be considered a breach of the security policy of the school. It is recommended that permission be obtained before running Wireshark for this lab. If using a packet sniffer such as Wireshark is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

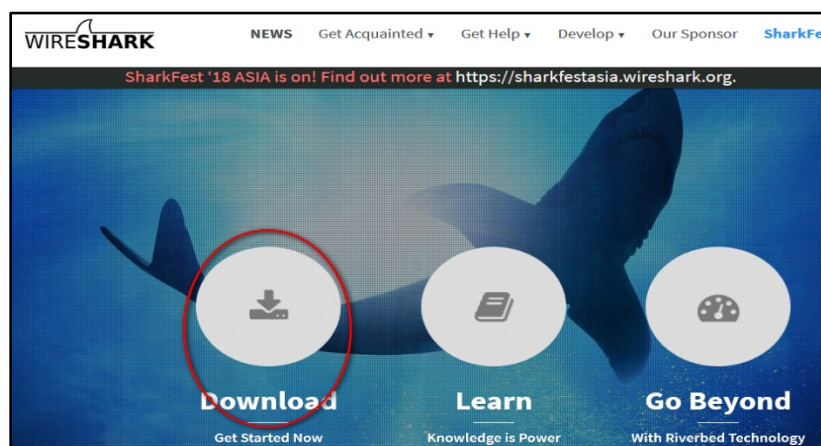
Download and Install Wireshark

Wireshark has become the industry standard packet-sniffer program used by network engineers. This open source software is available for many different operating systems, including Windows, Mac, and Linux. In this lab, you will download and install the Wireshark software program on your PC.

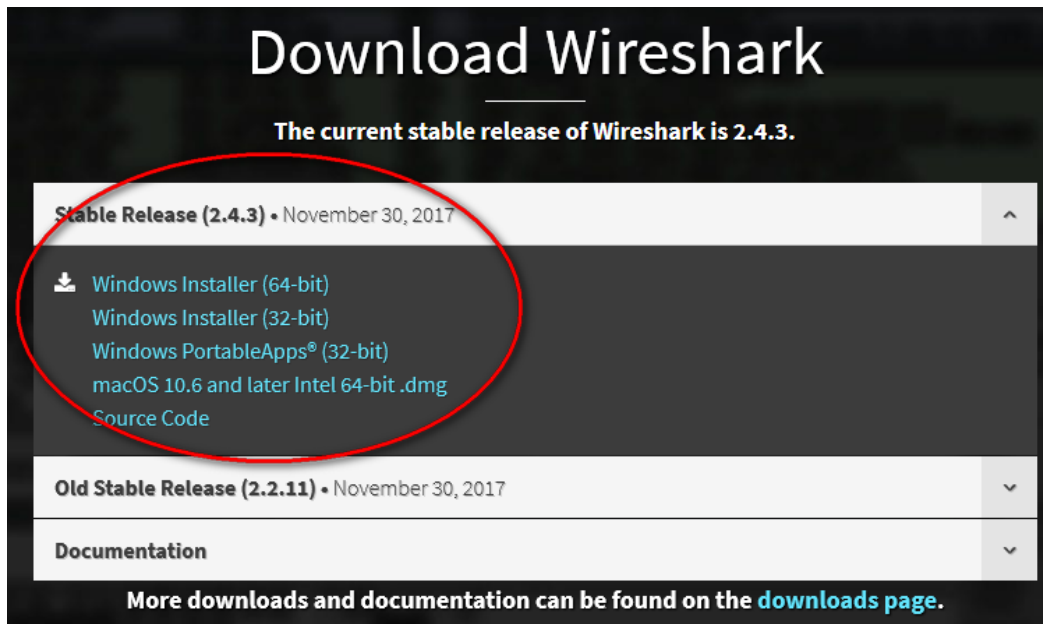
Note: Before downloading Wireshark, check with your instructor about the software download policy of your academy.

Step 1: Download Wireshark.

- Wireshark can be downloaded from www.wireshark.org.
- Click the icon above **Download**.



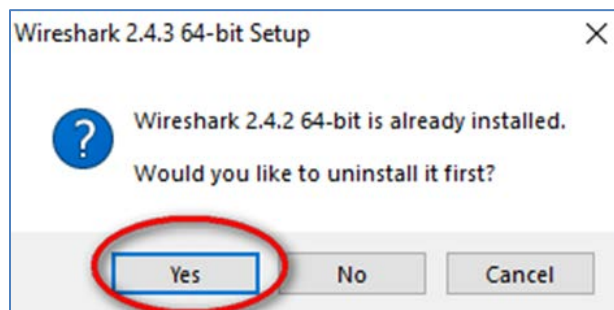
- c. Choose the software version you need based on your PC architecture and operating system. For instance, if you have a 64-bit PC running Windows, choose **Windows Installer (64-bit)**.



After making a selection, the download should start. The location of the downloaded file depends on the browser and operating system that you use. For Windows users, the default location is the **Downloads** folder.

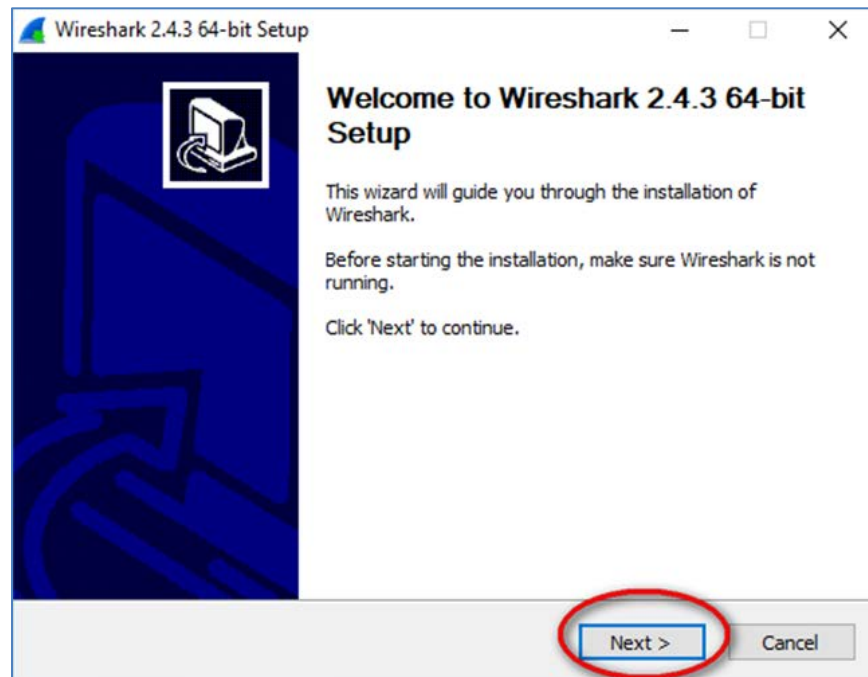
Step 2: Install Wireshark.

- a. The downloaded file is named **Wireshark-win64-x.x.x.exe**, where **x** represents the version number. Double-click the file to start the installation process.
- b. Respond to any security messages that may display on your screen. If you already have a copy of Wireshark on your PC, you will be prompted to uninstall the old version before installing the new version. It is recommended that you remove the old version of Wireshark prior to installing another version. Click **Yes** to uninstall the previous version of Wireshark.

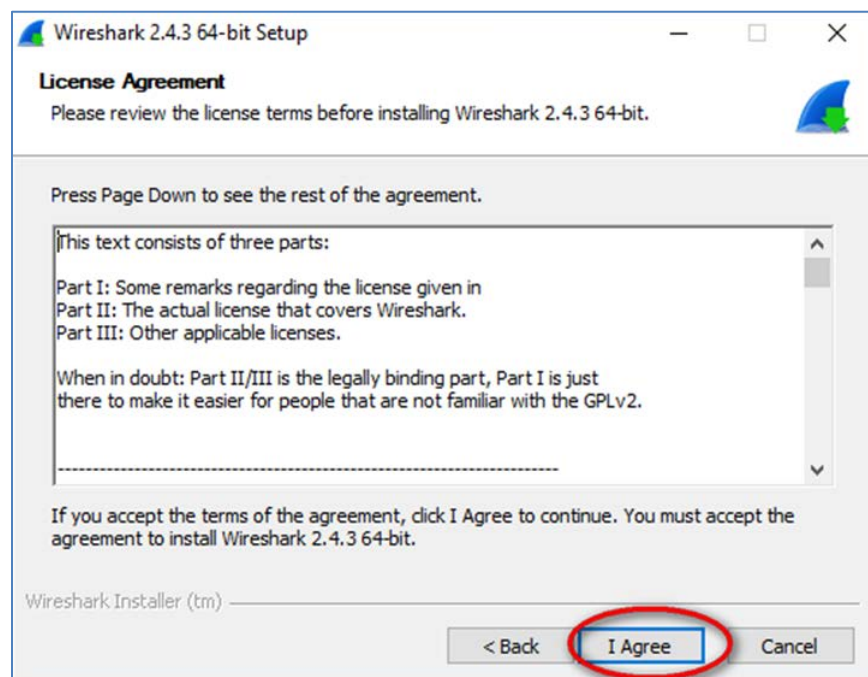


Lab – Installing Wireshark

- c. If this is the first time that you have installed Wireshark, or after you have completed the uninstall process, you will navigate to the **Wireshark Setup** wizard. Click **Next**.

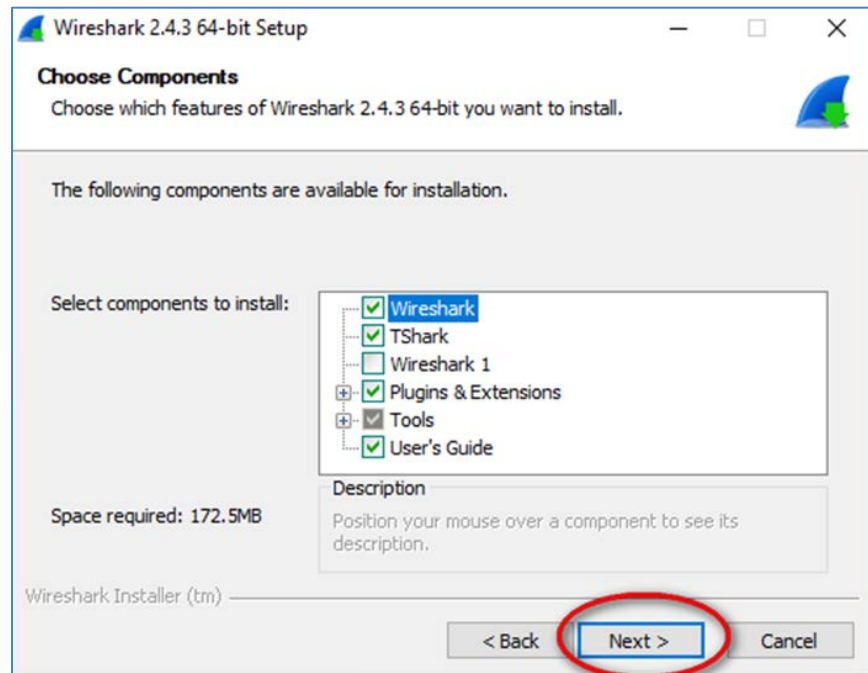


- d. Continue advancing through the installation process. Click **I Agree** when the License Agreement window displays.

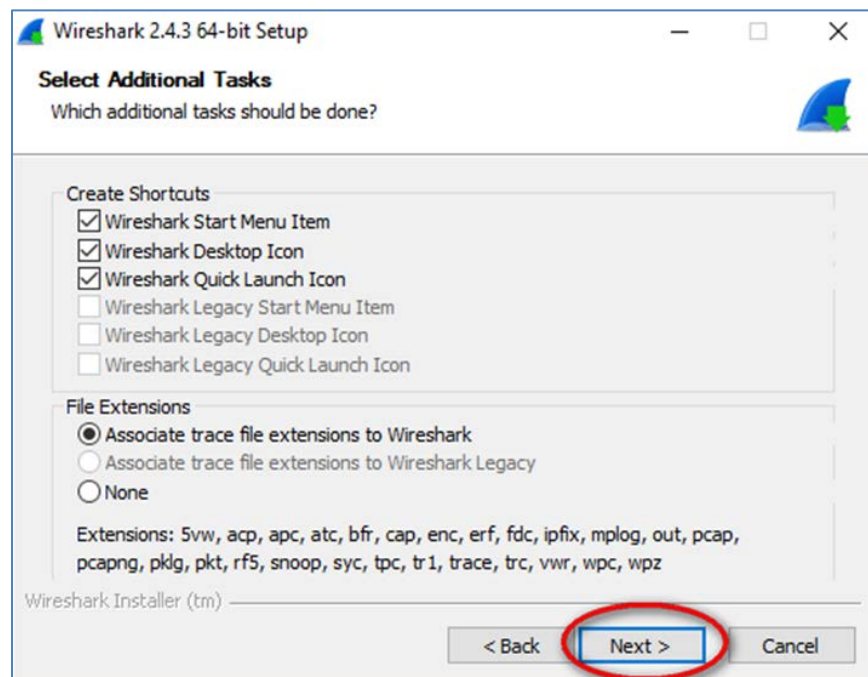


Lab – Installing Wireshark

- e. Keep the default settings on the **Choose Components** window and click **Next**.

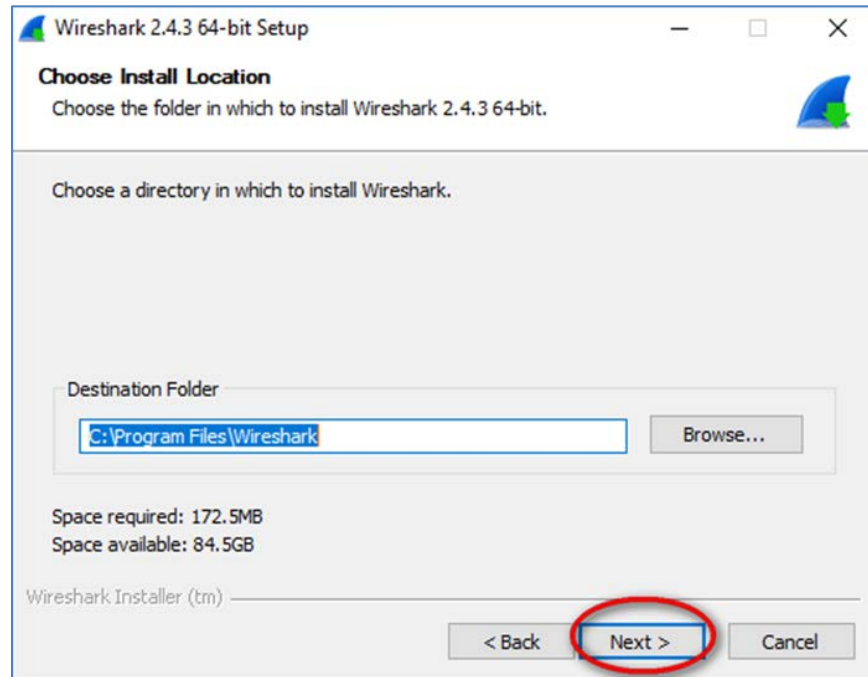


- f. Choose your desired shortcut options and click **Next**.

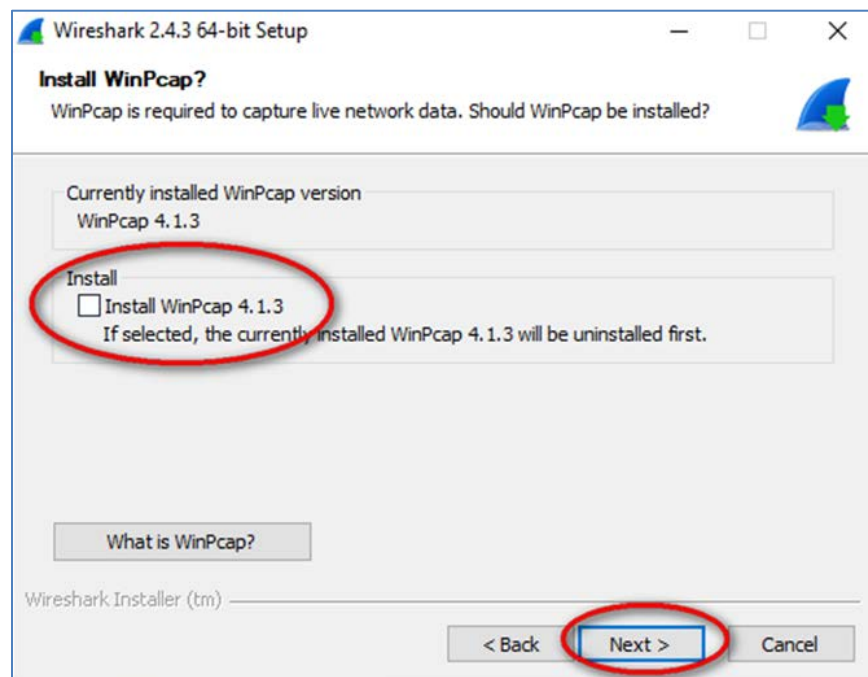


Lab – Installing Wireshark

- g. You can change the installation location of Wireshark, but unless you have limited disk space, it is recommended that you keep the default location.



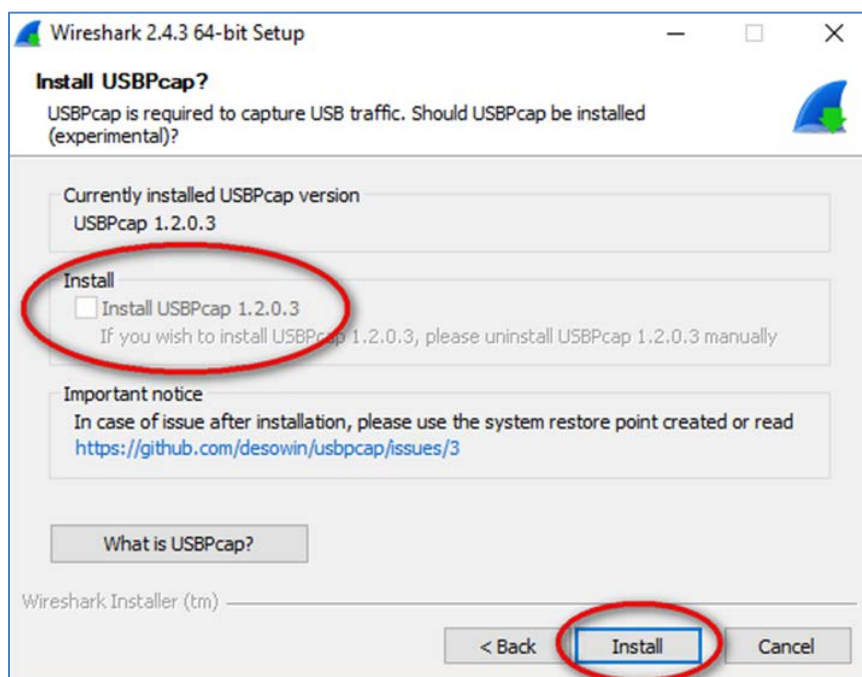
- h. To capture live network data, WinPcap must be installed on your PC. If WinPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of WinPcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install WinPcap x.x.x** (version number) check box.
- i. Finish the **WinPcap Setup** wizard if installing WinPcap.



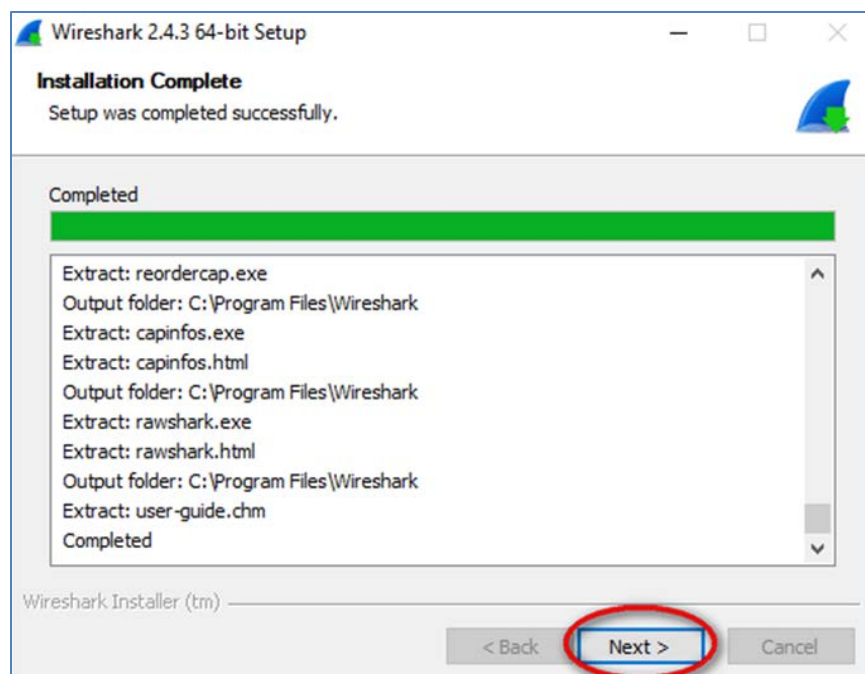
- j. In addition, USBPcap can be installed on your PC. If USBPcap is already installed on your PC, the Install check box will be unchecked. If your installed version of USBPcap is older than the version that comes with Wireshark, it is recommended that you allow the newer version to be installed by clicking the **Install USBPcap x.x.x** (version number) check box.

Note: Because USBcap is still experimental, it is recommended that you **DO NOT** install USBcap unless you need to capture USB traffic.

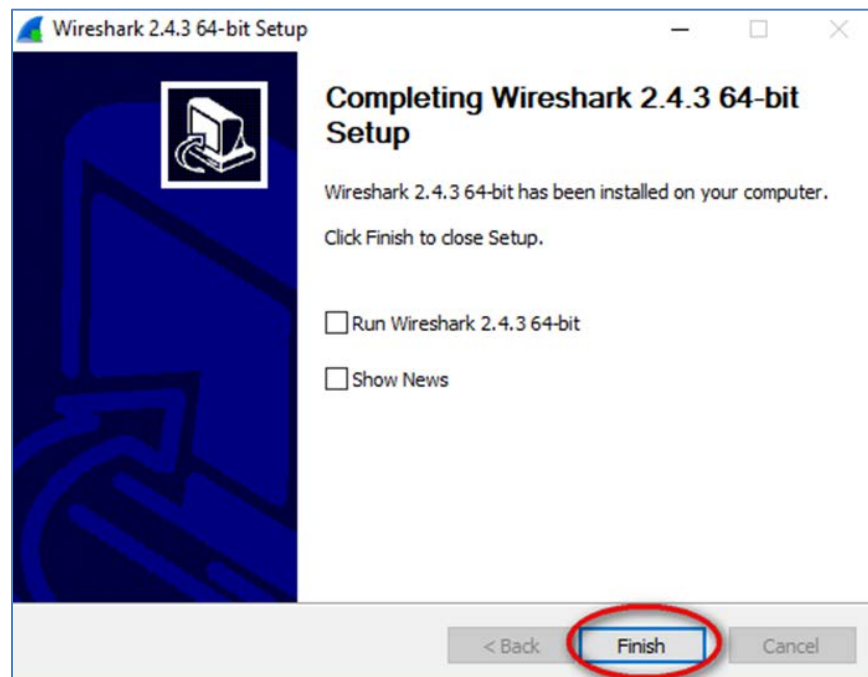
- k. Finish the **USBPcap Setup** wizard if installing USBPcap.



- l. Wireshark starts installing its files, and a separate window displays with the status of the installation. Click **Next** when the installation is complete.



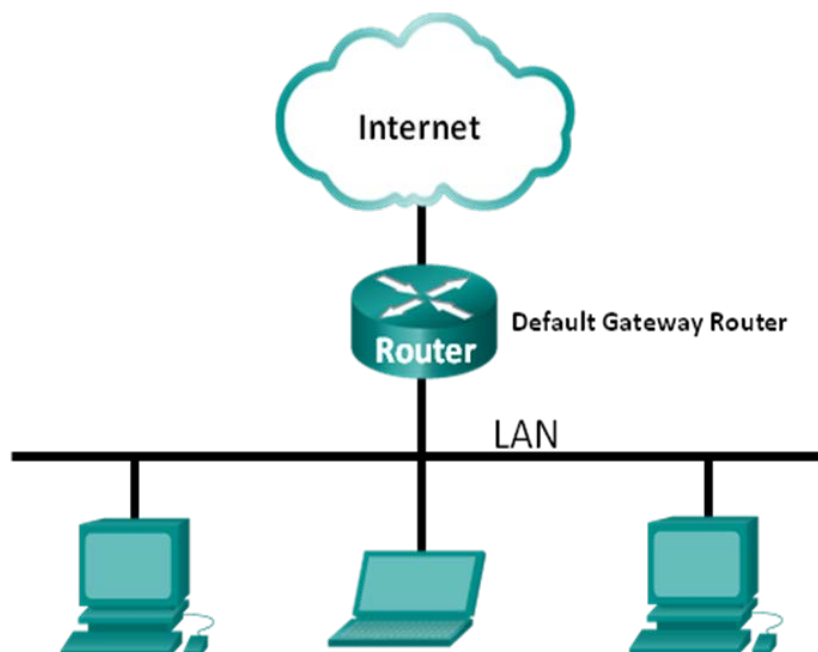
- m. Click **Finish** to complete the Wireshark install process.



Lab - Using Wireshark to View Network Traffic (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access)
- Additional PCs on a local-area network (LAN) will be used to reply to ping requests.

Instructor Note: This lab assumes that the student is using a PC with internet access and can ping other PCs on the local area network.

Using a packet sniffer such as Wireshark may be considered a breach of the security policy of the school. It is recommended that permission be obtained before running Wireshark for this lab. If using a packet sniffer such as Wireshark is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

Part 1: Capture and Analyze Local ICMP Data in Wireshark

In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC interface addresses.

For this lab, you will need to retrieve your PC IP address and its network interface card (NIC) physical address, also called the MAC address.

- Open a command window, type **ipconfig /all**, and then press Enter.
- Note the IP address of your PC interface, its description, and its MAC (physical) address.

```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-C73CB0M
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 00-26-B9-DD-00-91
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d009:d939:110f:1b7f%20 (Preferred)
IPv4 Address. . . . . : 192.168.1.147 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
```

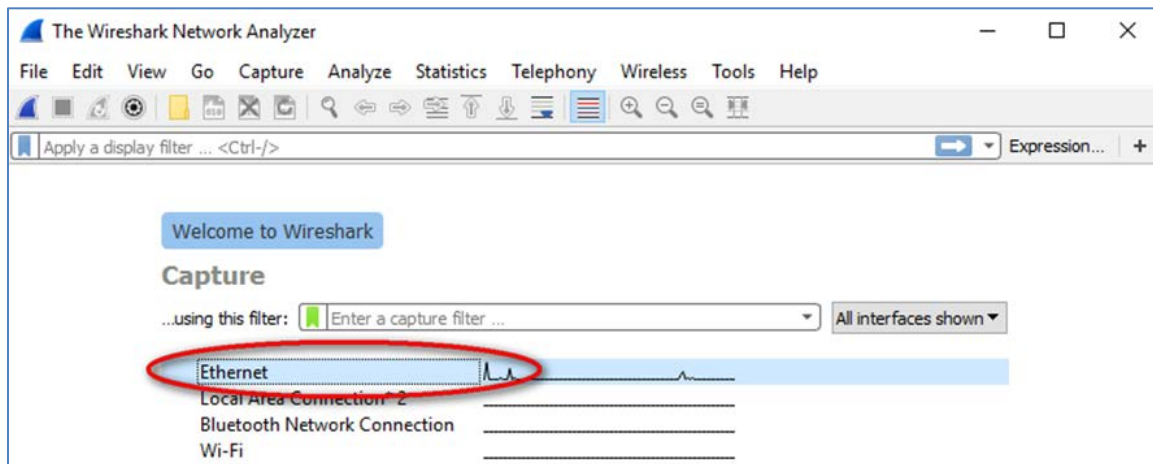
- Ask a team member or team members for their PC IP address and provide your PC IP address to them. Do not provide them with your MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

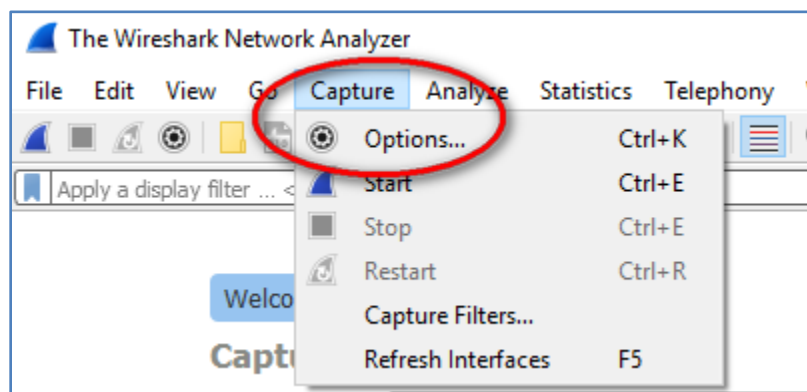
- On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

Lab - Using Wireshark to View Network Traffic

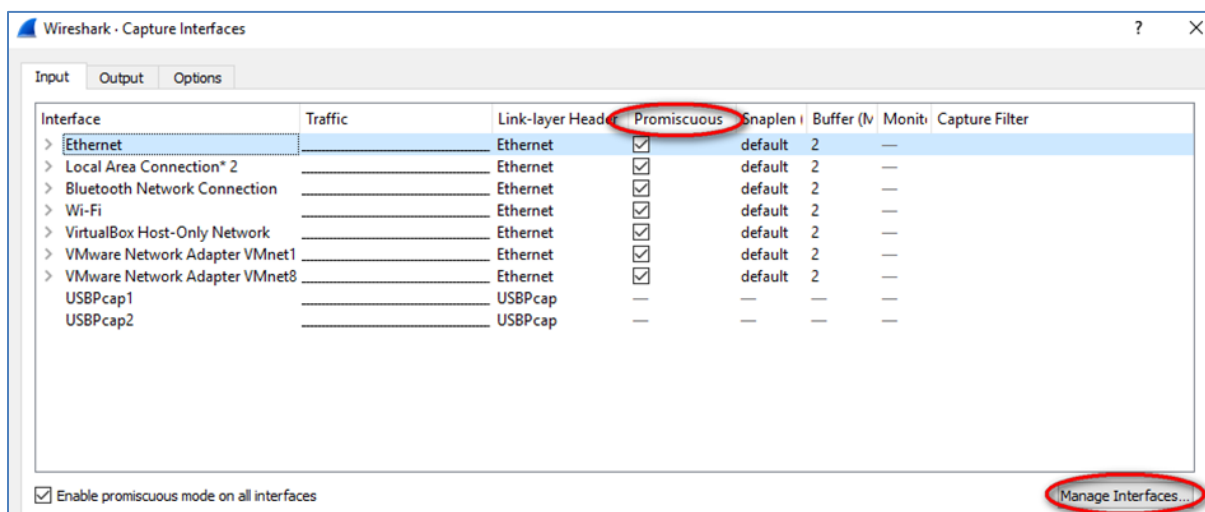
- b. After Wireshark starts, click the capture interface to be used. Because we are using the wired Ethernet connection on the PC, make sure the Ethernet option is on the top of the list.



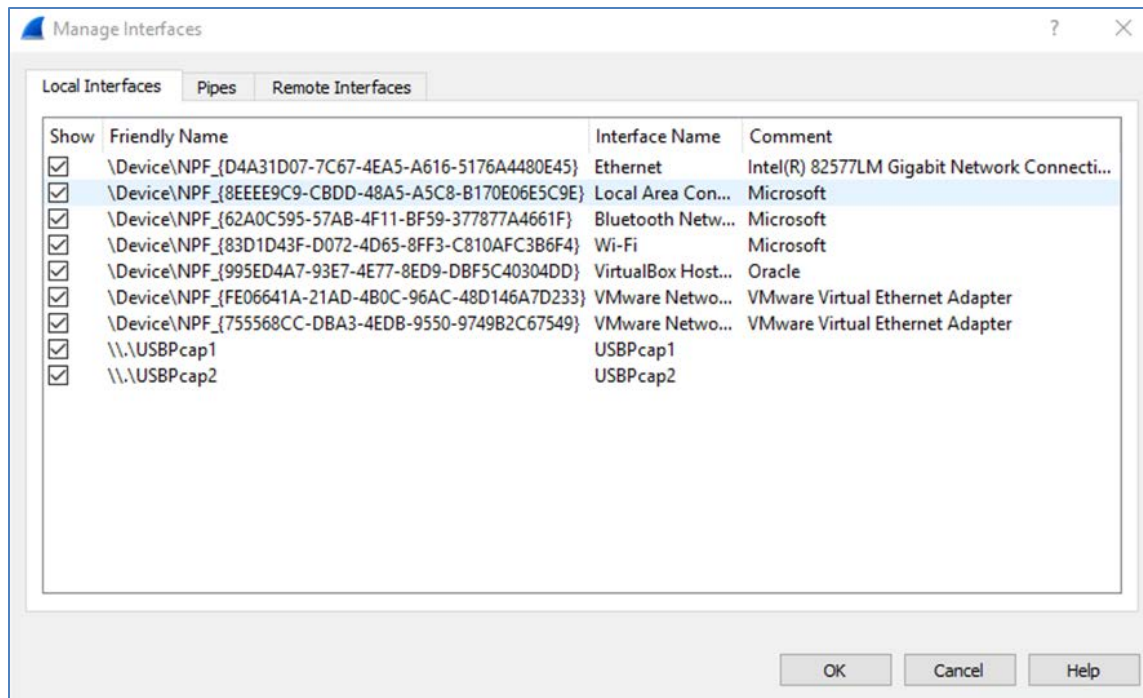
You can manage the capture interface by clicking **Capture** and **Options**:



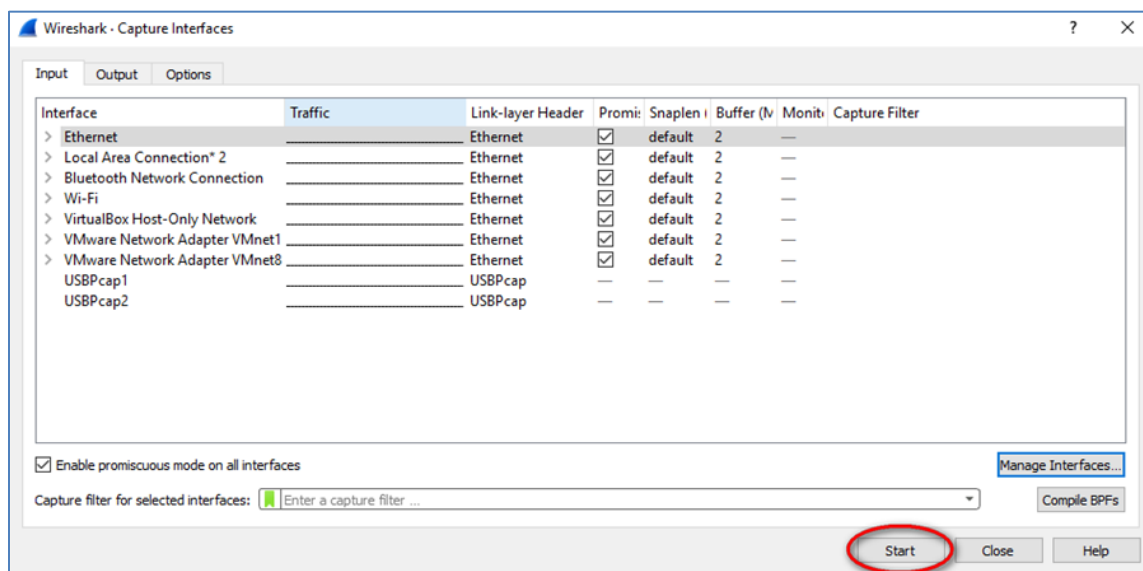
- c. A list of interfaces will display. Make sure the capture interface is checked under **Promiscuous**.



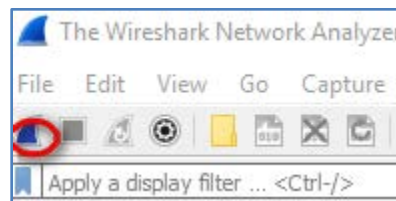
Note: We can further manage the interfaces on the PC by clicking **Manage Interfaces**. Verify that the description matches what you noted in Step 1b. Close the **Manage Interfaces** window after verifying the correct interface.



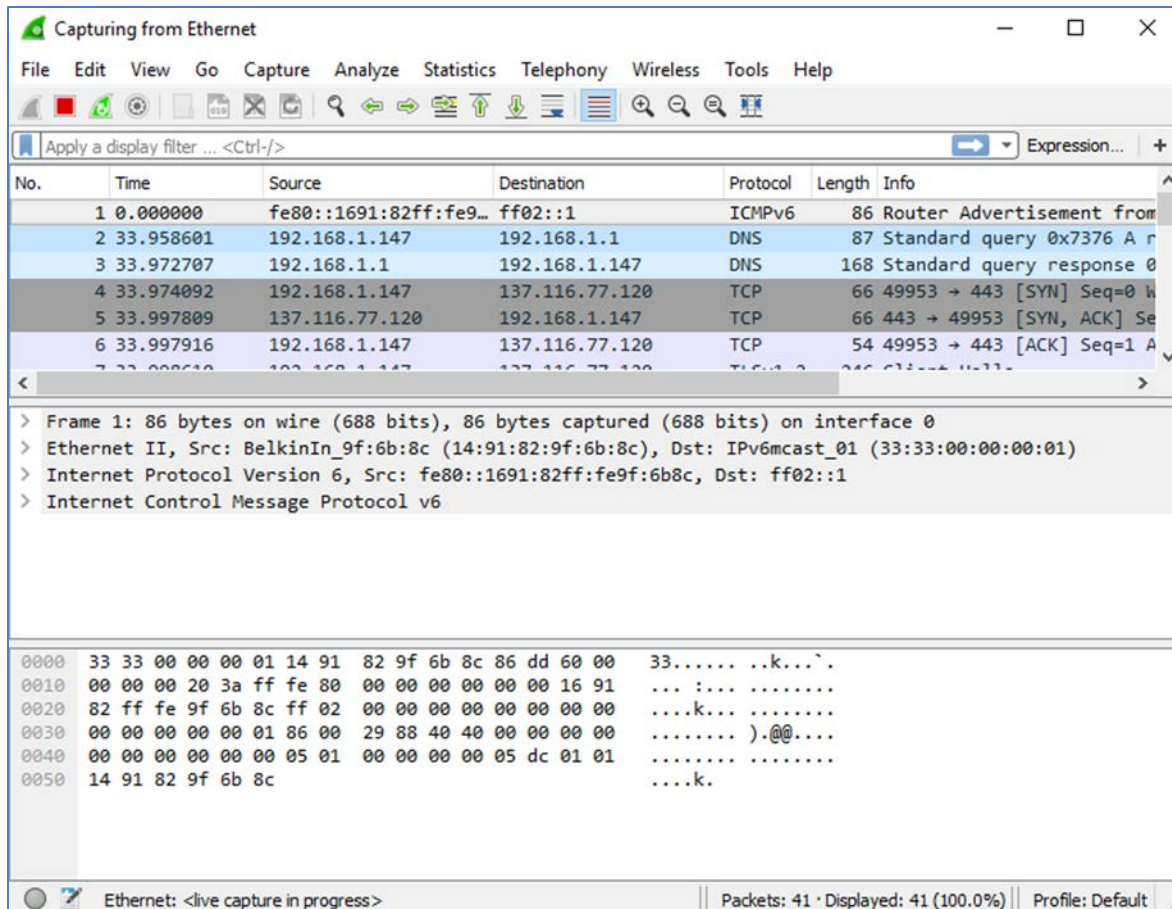
- d. After you have checked the correct interface, click **Start** to start the data capture.



Note: You can also start the data capture by clicking the **Wireshark** icon in the main interface.



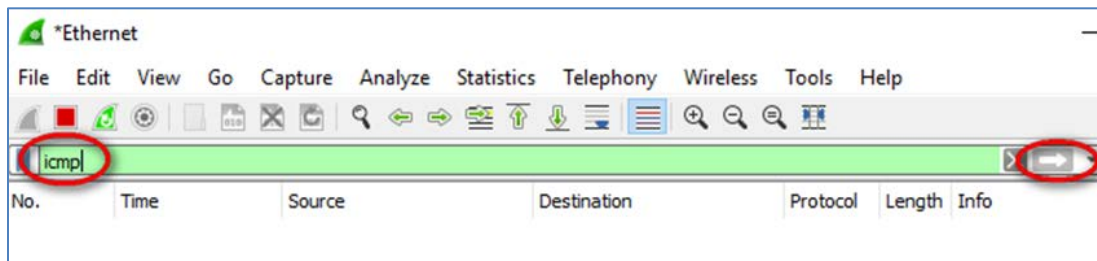
Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



- e. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in

Lab - Using Wireshark to View Network Traffic

the **Filter** box at the top of Wireshark and press **Enter** or click on the **Apply** button (arrow sign) to view only ICMP (ping) PDUs.



- f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member.

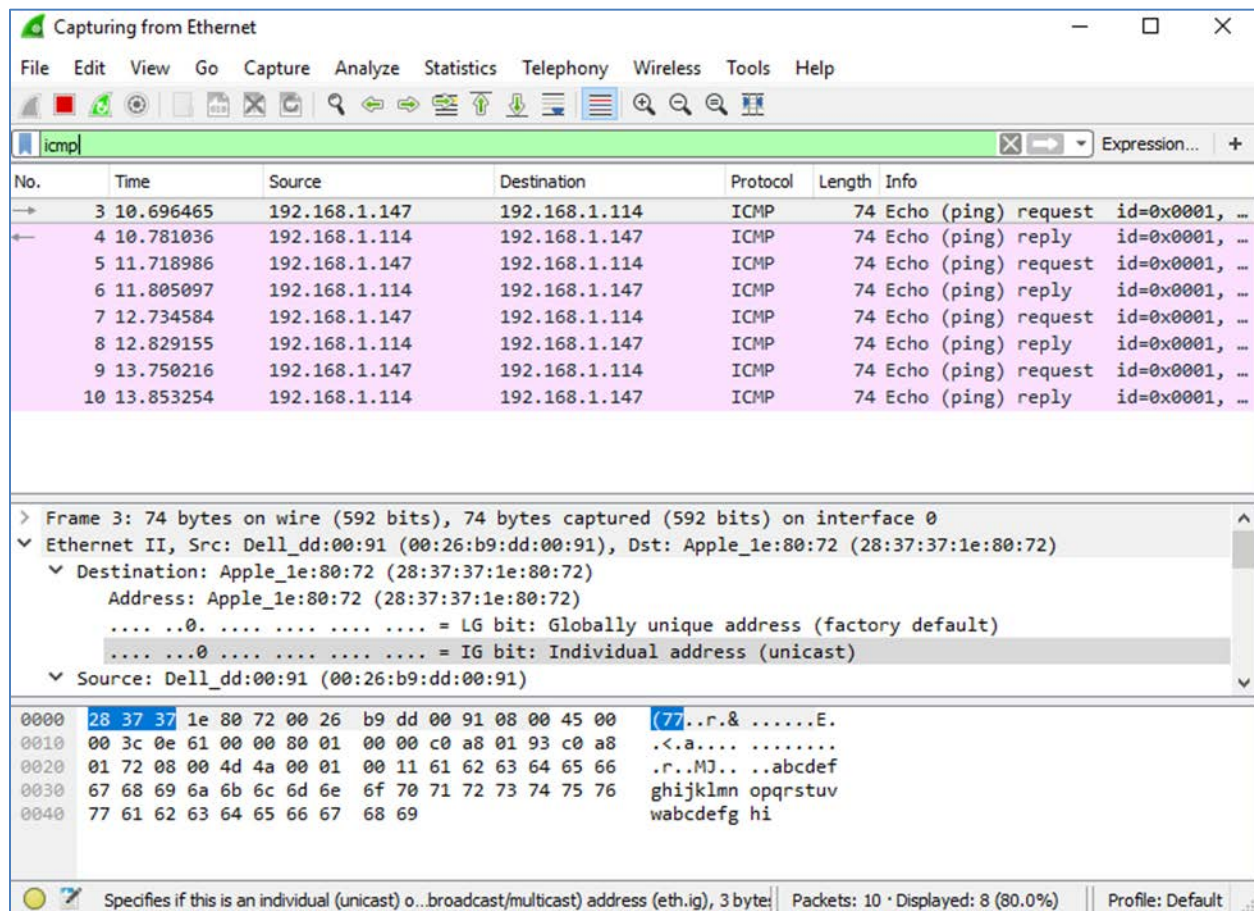
```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ping 192.168.1.114

Pinging 192.168.1.114 with 32 bytes of data:
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64
Reply from 192.168.1.114: bytes=32 time<1ms TTL=64

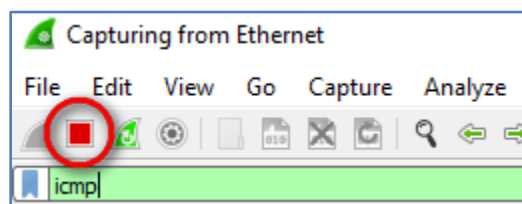
Ping statistics for 192.168.1.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Notice that you start seeing data appear in the top window of Wireshark again.



Note: If the PC of your team member does not reply to your pings, this may be because the PC firewall of the team member is blocking these requests. Please see Appendix A: Allowing ICMP Traffic Through a Firewall for information on how to allow ICMP traffic through the firewall using Windows 7.

- g. Stop capturing data by clicking the **Stop Capture** icon.



Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed; 2) the middle section lists PDU information for the frame selected

Lab - Using Wireshark to View Network Traffic

in the top part of the screen and separates a captured PDU frame by its protocol layers; and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.

The screenshot shows the Wireshark interface with the following sections:

- Top section:** A list of captured packets. The first packet (No. 3) is an ICMP Echo (ping) request from 192.168.1.147 to 192.168.1.114.
- Middle section:** Details of the selected packet (Frame 3). It shows the Ethernet II header, Internet Protocol Version 4 header, and Internet Control Message Protocol (ICMP) details, including Type 8 (Echo (ping) request) and Code 0.
- Bottom section:** Raw data of the selected packet, displayed in hexadecimal and ASCII. The ASCII part shows the ICMP Echo request data: (77..r.&E.

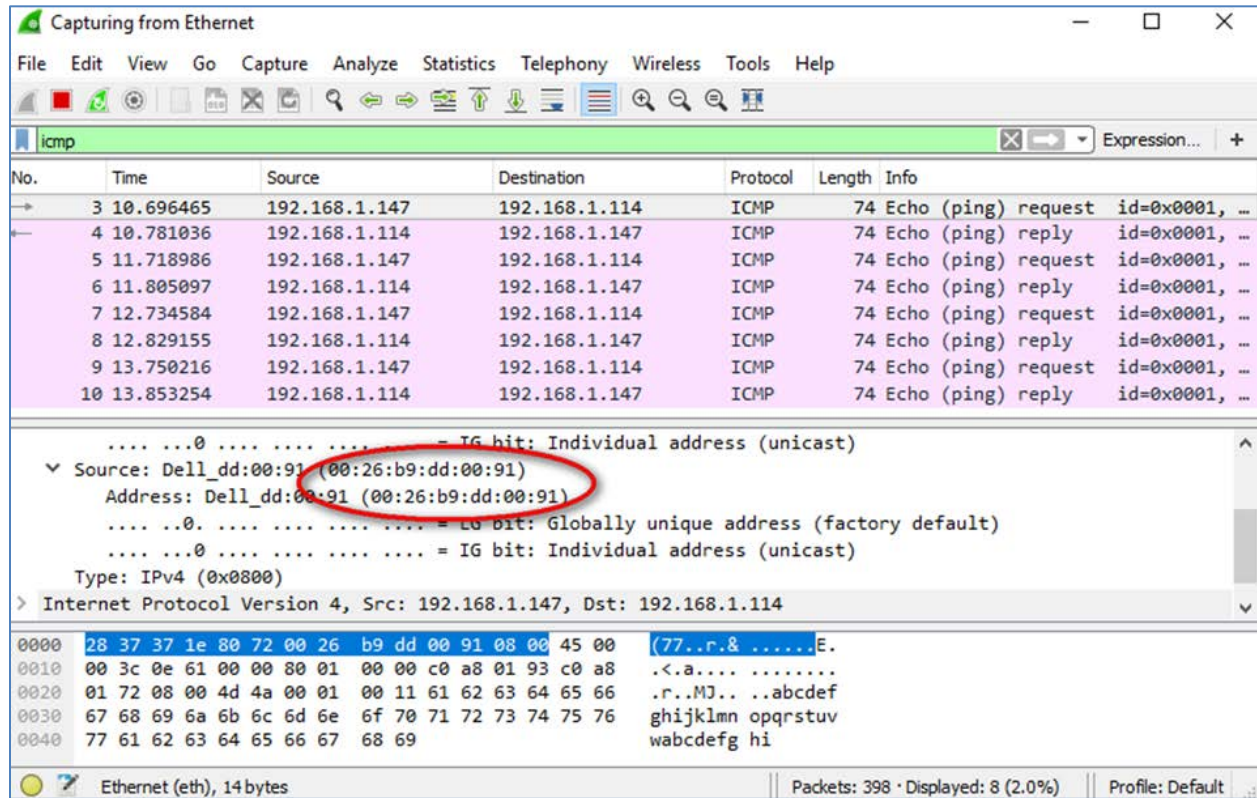
- a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the **Source** column has your PC IP address, and the **Destination** column contains the IP address of the teammate PC that you pinged.

The screenshot shows the Wireshark interface with the following sections:

- Top section:** A list of captured packets. The first two packets are highlighted. The first packet (No. 3) is an ICMP Echo (ping) request from 192.168.1.147 to 192.168.1.114. The second packet (No. 4) is an ICMP Echo (ping) reply from 192.168.1.114 to 192.168.1.147.

Lab - Using Wireshark to View Network Traffic

- b. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the destination and source MAC addresses.



Does the source MAC address match your PC interface (shown in Step 1.b)? ☐ Yes

Does the destination MAC address in Wireshark match your team member MAC address?

☐ Yes

How is the MAC address of the pinged PC obtained by your PC?

The MAC address is obtained through an ARP request.

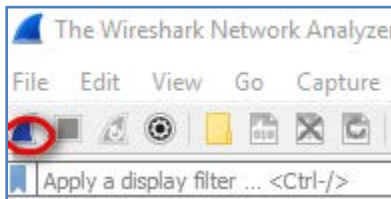
Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

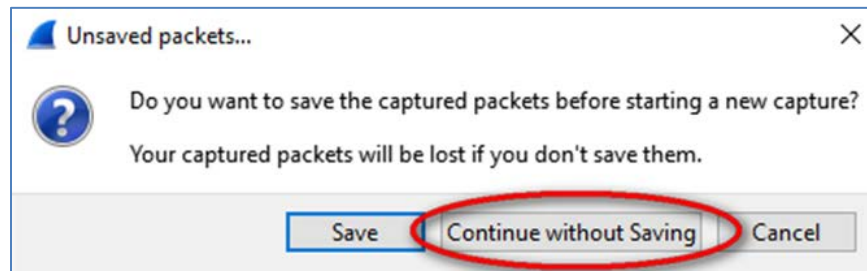
In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

Step 1: Start capturing data on the interface.

- a. Start the data capture again.



- b. A window prompts you to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.



- c. With the capture active, ping the following three website URLs:
 - 1) www.yahoo.com
 - 2) www.cisco.com

3) www.google.com

```
C:\> ping www.yahoo.com

Pinging atsv2-fp.wg1.b.yahoo.com [98.139.180.180] with 32 bytes of data:
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=60ms TTL=53
Reply from 98.139.180.180: bytes=32 time=43ms TTL=53
Reply from 98.139.180.180: bytes=32 time=42ms TTL=53

Ping statistics for 98.139.180.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 42ms, Maximum = 60ms, Average = 47ms

C:\> ping www.cisco.com

Pinging e2867.dsca.akamaiedge.net [23.13.155.188] with 32 bytes of data:
Reply from 23.13.155.188: bytes=32 time=20ms TTL=56
Reply from 23.13.155.188: bytes=32 time=21ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56
Reply from 23.13.155.188: bytes=32 time=19ms TTL=56

Ping statistics for 23.13.155.188:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 19ms, Maximum = 21ms, Average = 19ms

C:\> ping www.google.com

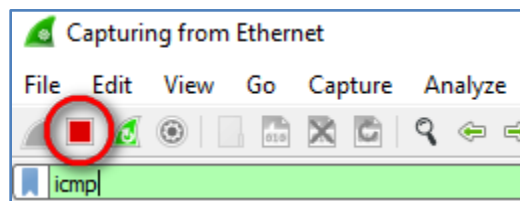
Pinging www.google.com [216.58.194.100] with 32 bytes of data:
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=56ms TTL=54
Reply from 216.58.194.100: bytes=32 time=55ms TTL=54
Reply from 216.58.194.100: bytes=32 time=57ms TTL=54

Ping statistics for 216.58.194.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 57ms, Average = 56ms

C:\>
```

Note: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

- d. You can stop capturing data by clicking the **Stop Capture** icon.



Step 2: Examining and analyzing the data from the remote hosts.

- a. Review the captured data in Wireshark and examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

1st Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:_____

2nd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:_____

3rd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:_____

IP addresses: 98.139.180.180, 23.13.155.188, 216.58.194.100 (these IP addresses may vary)

MAC address: This will be the same for all three locations. It is the physical address of the default-gateway LAN interface of the router.

- b. What is significant about this information?

The MAC addresses for all three locations are the same.

- c. How does this information differ from the local ping information you received in Part 1?

A ping to a local host returns the MAC address of the PC NIC. A ping to a remote host returns the MAC address of the default gateway LAN interface.

Reflection

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

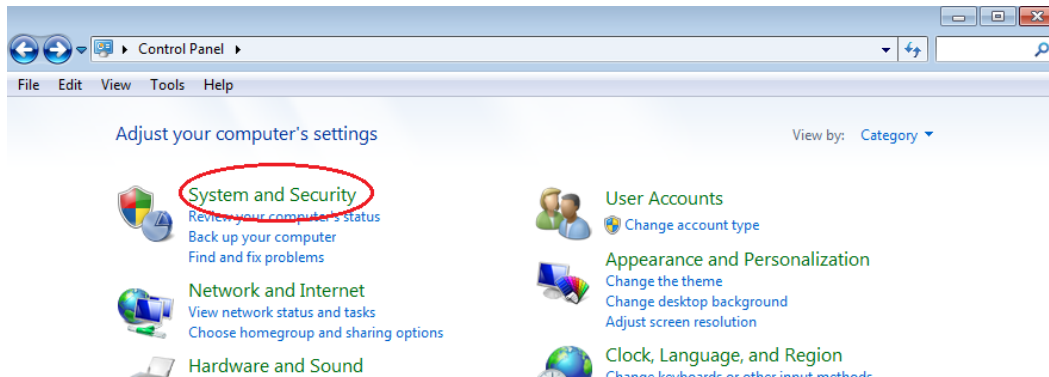
MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the Layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.

Appendix A: Allowing ICMP Traffic Through a Firewall

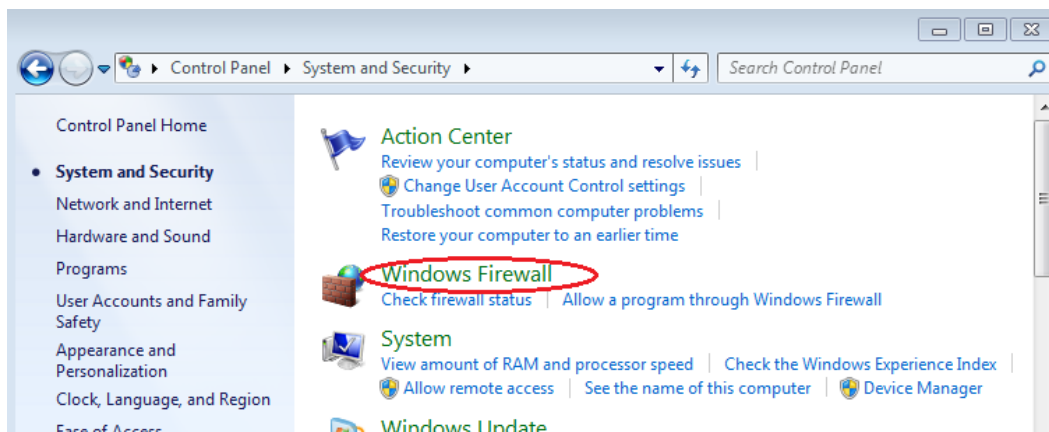
If the members of your team are unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

Step 1: Create a new inbound rule allowing ICMP traffic through the firewall.

- a. From the **Control Panel**, click the **System and Security** option.



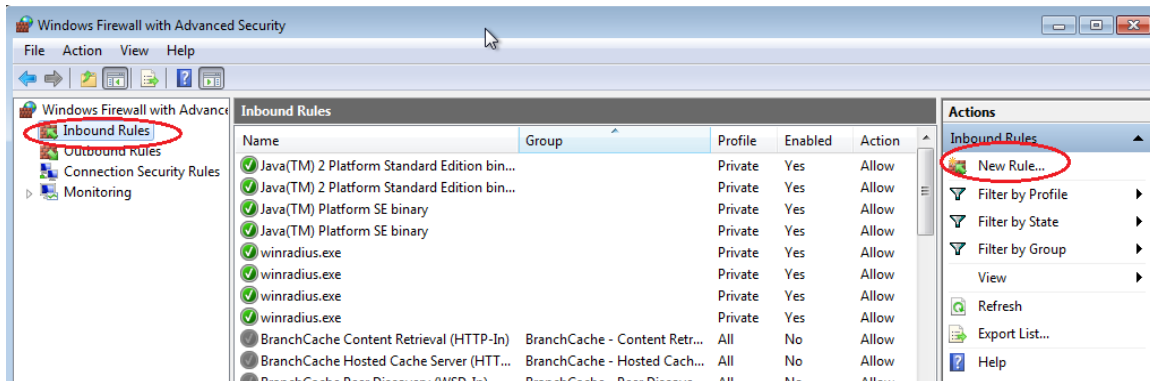
- b. From the **System and Security** window, click **Windows Firewall**.



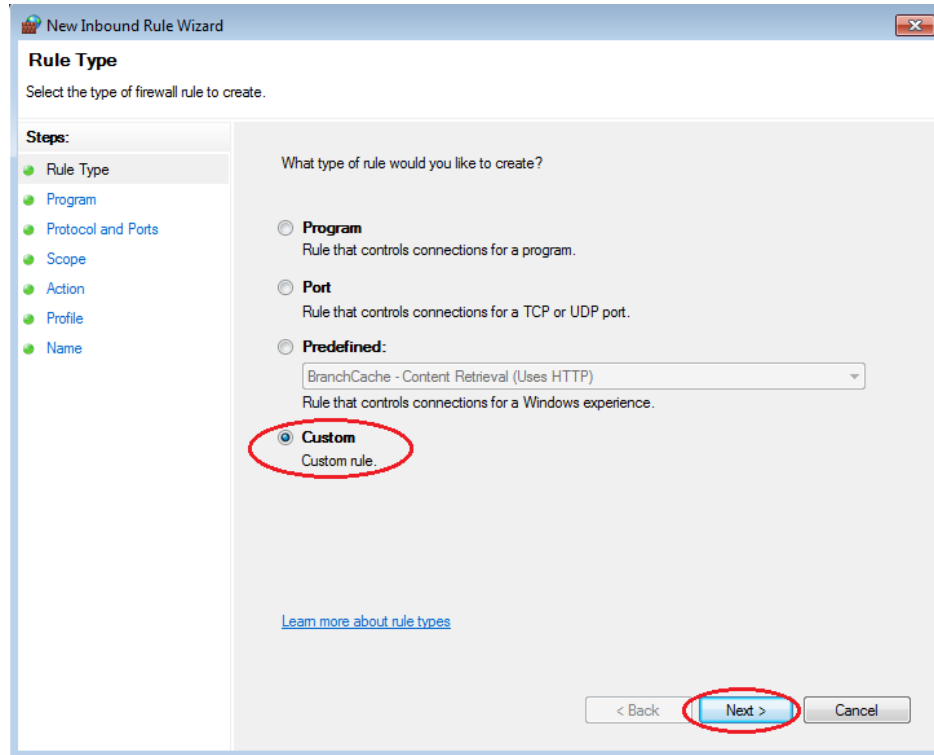
- c. In the left pane of the **Windows Firewall** window, click **Advanced settings**.



- d. On the **Advanced Security** window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule...** on the right sidebar.

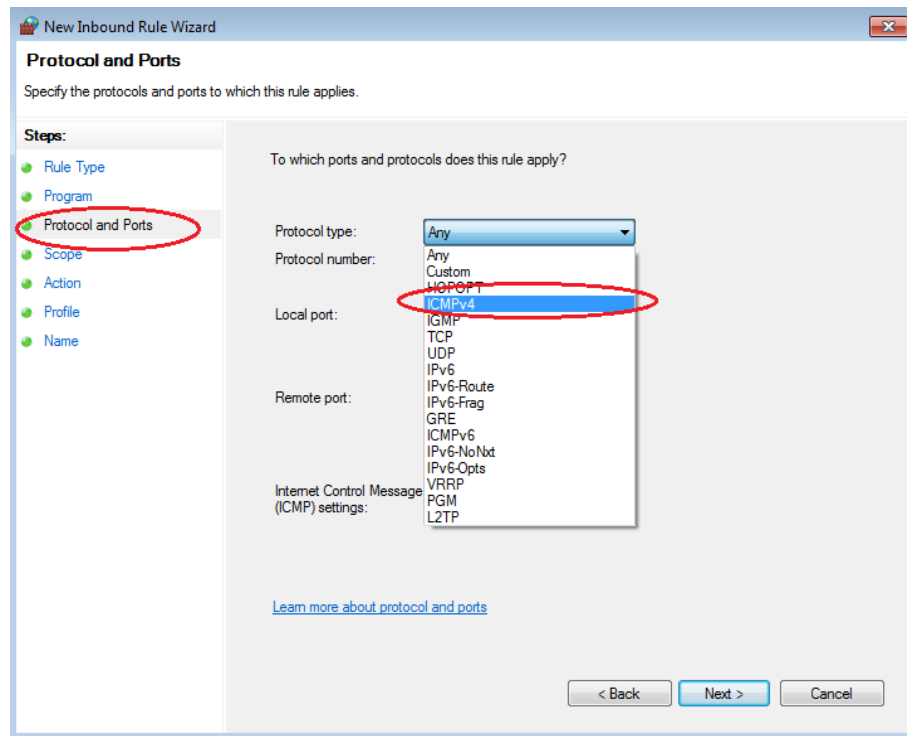


- e. This launches the **New Inbound Rule** wizard. On the **Rule Type** screen, click the **Custom** radio button and click **Next**.

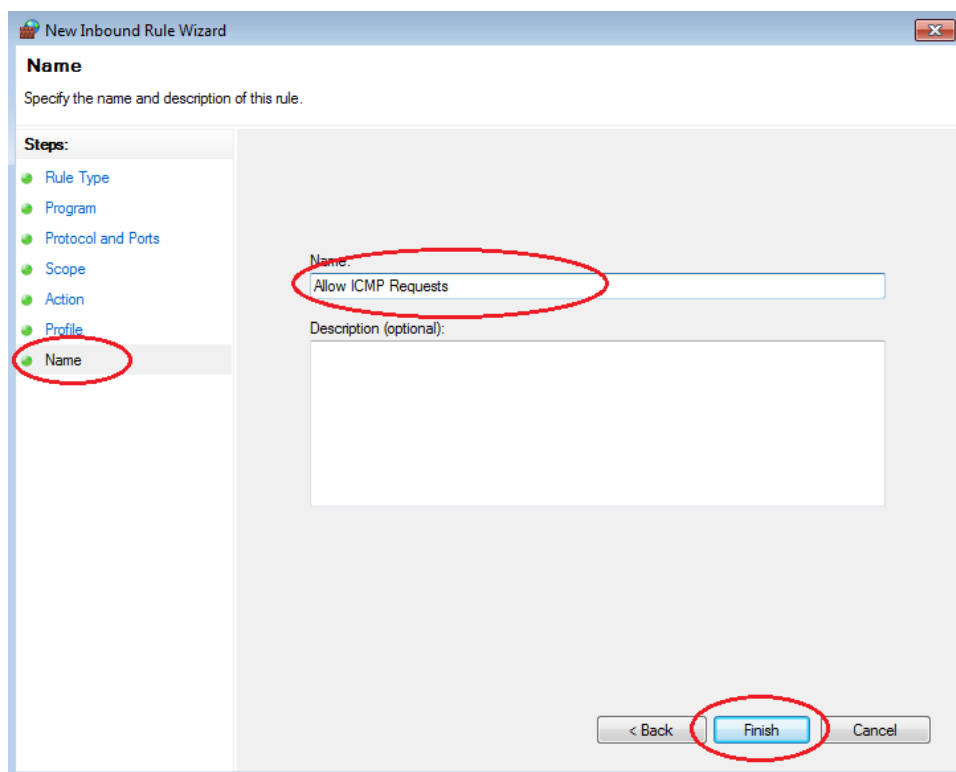


Lab - Using Wireshark to View Network Traffic

- f. In the left pane, click the **Protocol and Ports** option and using the **Protocol Type** drop-down menu, select **ICMPv4**, and then click **Next**.



- g. In the left pane, click the **Name** option and in the **Name** field, type **Allow ICMP Requests**. Click **Finish**.

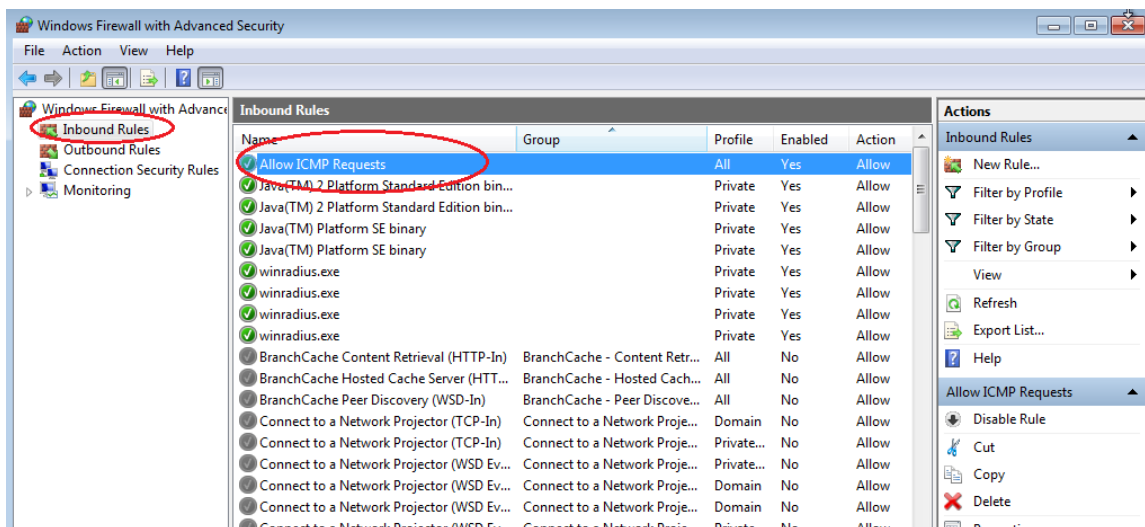


This new rule should allow your team members to receive ping replies from your PC.

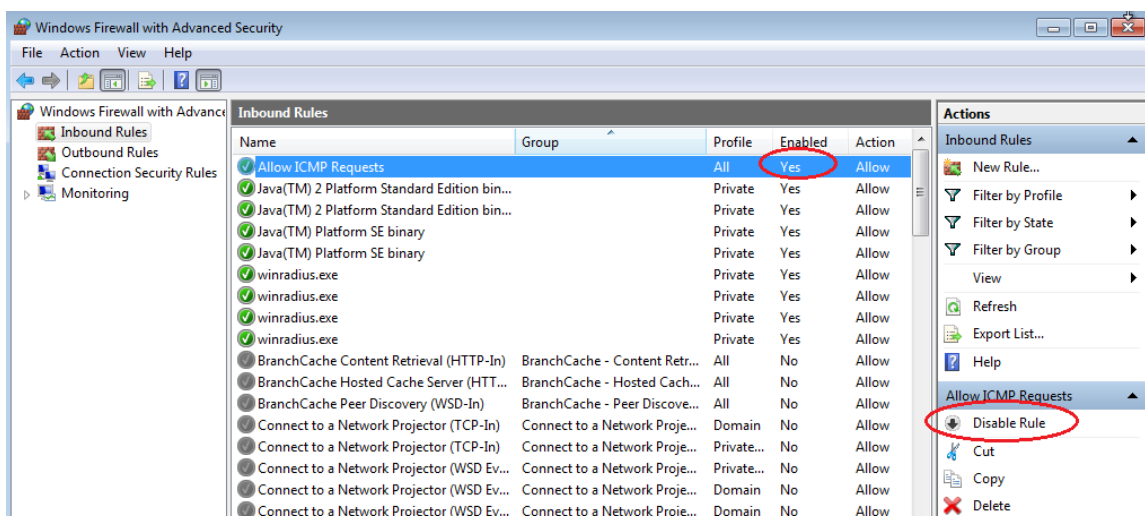
Step 2: Disabling or deleting the new ICMP rule.

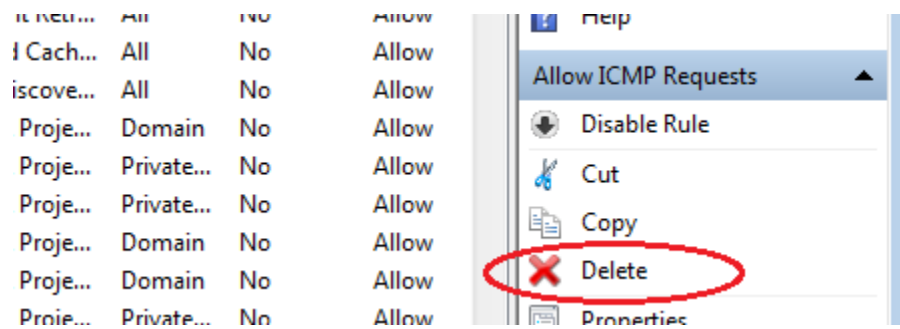
After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of inbound rules.

- On the **Advanced Security** window, click **Inbound Rules** in the left pane and then locate the rule you created in Step 1.



- To disable the rule, click the **Disable Rule** option. When you choose this option, you will see this option change to **Enable Rule**. You can toggle back and forth between **Disable Rule** and **Enable Rule**; the status of the rule also shows in the **Enabled** column of the **Inbound Rules** list.





Class Activity - Guaranteed to Work! (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain the role of protocols and standards organizations in facilitating interoperability in network communications.

Background / Scenario

You have just completed the Chapter 3 content regarding network protocols and standards.

Assuming you resolved the beginning of this chapter's modeling activity, how would you compare the following steps taken to design a communications system to the networking models used for communications?

Steps to Communicate	Possible Answers	Associated TCP/IP Model Layer
Establishing a language to communicate		
Dividing the message into small steps, delivered a little at a time, to facilitate understanding of the problem		
Checking to see if the message has been delivered correctly to the mechanic who will be performing the repairs		
Delivery of automobile and wait time for repairs		

Instructor Note: This optional Modeling Activity may be used as a graded assignment. It should demonstrate how network protocols and standards facilitate the transfer of data from source to destination, in both personal and in corporate practice. Facilitation of the discussion should include student-to-student discussions to show how students' perceptions have been changed.

Required Resources

- Blank "Steps to Communicate" table (above) for students to record their answers based upon their Chapter 3 content knowledge.

Reflection

How does your network model in developing an automotive repair communications plan compare to a network communications interoperability plan?

Students' tables might look like this (with variations)

Steps to Communicate	Possible Answers	Associated TCP/IP Model Layer
Establishing a language to communicate	Voice/Language (English,	Application Layer

Class Activity - Guaranteed to work!

	Spanish, French, etc.) Written pictures Kinesthetic/physical	(HTTP, VoIP, POP, etc.)
Dividing the message into small steps, delivered a little at a time, to facilitate understanding of the problem	Small descriptions shared a little at a time	Transport Layer (Segments)
Checking to see if the message has been delivered correctly to the mechanic who will be performing the repairs	Asking the mechanic to repeat the full problem which is occurring with the automobile.	Internet Layer (Packets)
Delivery of automobile and wait time for repairs	Physical delivery of the automobile left for repairs – agreement upon the delivery/wait time for repairs	Network Access Layer (Bits)

Identify elements of the model that map to IT-related content:

- Establishing a language to communicate (Application protocol)
- Dividing the message into small steps, delivered a little at a time, to facilitate understanding of the problem to be solved (Transport protocol).
- Checking to see if the message has been delivered correctly to the mechanic who will be performing the repairs. (Internet protocol)
- Delivery of automobile and wait time for repairs (Network Access protocol)

Class Activity – Managing the Medium (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe the purpose and function of the data link layer in preparing communication for transmission on specific media.

Background /Scenario

You and your colleague are attending a networking conference. There are many lectures and presentations held during this event, and because they overlap, each of you can attend only a limited set of sessions. Therefore, you decide to split up, each of you attending a separate set of presentations, and after the event ends, you share the slides and the knowledge each of you gained during the event.

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of how a network is prepared to use specific media in data transmission for personal and corporate practice. Facilitation of the discussion should be initiated as a result of this activity

Required Resources

- Recording capabilities (paper, tablet, etc.) for reflective comments to be shared with the class.

Reflection

- How would you personally organize a conference where multiple sessions are held at the same time? Would you put all of them into a single conference room, or would you use multiple rooms? What would be the reason? Explain your answer.

If multiple independent sessions are being held, it is necessary to put them into separate rooms. Otherwise, the speakers would overlap, making it very hard, if not impossible, to understand what the presenters are saying. Keeping separate sessions in separate rooms is not done for the purpose of security (although there can be private sessions only for invited guests with restrictions on who can join and what can be shared after the session) but rather for the purpose of keeping the communication separated for better clarity and efficiency.

Our networks are separated into multiple data-link layer domains (broadcast domains) for the purpose of containing the communication of similar properties – workgroups, applications, floors, security requirements, etc. This is similar to separating all sessions into multiple conference rooms according to their topics.

- Assume that the conference room is properly fitted with audiovisual equipment to display large-size video and amplify the speaker's voice. If a person wanted to attend a specific session, does it matter which seat the person takes, or is it sufficient for the person to sit anywhere as long as it is in appropriate conference room?

Class Activity – Managing the Medium

It is sufficient to visit the proper conference room. A particular seat is not important as long as from each seat, an attendee can hear and listen without obstructions.

The relative independence on the particular seat is similar to the relative independence of a node within a network from its particular host address. For the purpose of communication within a single network, it is sufficient that the nodes are in the same data-link layer domain and have unique addresses but it is not important what exact addresses these are. Two nodes in a common data-link layer domain can talk to each other and hear each other immediately.

3. What are the potential consequences or benefits if the speech from one conference room somehow leaked into another?

It would definitely be at least annoying and distracting, if not directly damaging to the flow of the session.

In real networks, there are situations where two data-link layer domains originally intended to be separate become joined (incorrect wiring, misconfiguration, bug...) and leak information from one to another. This is not a correct situation. Even if nodes from two different data-link layer domains are to communicate together, their connection must be done in a controlled way using routers that interconnect separate data-link layer domains – similar to a person attending a single session and then, afterwards, sharing the knowledge with (i.e. routing the knowledge to) another person who did not attend.

4. If questions or inquiries arise during a presentation, should an attendee simply shout out his/her question, or should there be some process of assuring that attendees are given an opportunity to ask questions that everyone can hear? What would happen without this process?

Questions, comments, inquiries etc. from the audience should be given in a controlled manner. Otherwise, two or more people will be talking at the same time, causing their neighbors to not understand any of them, and each speaker would need to repeat what he/she said. Usually, a raised hand indicates that a person has something to say.

In networks, there are two main methods of accessing the medium – either deterministic or random. Raising a hand and waiting to be given a turn is a deterministic approach, similar to token passing. Seizing an opportunity to raise a question in a moment of silence without waiting to be given a turn is a random, or stochastic approach. Note that either of these approaches allows for the information to be exchanged both ways – between the audience and the presenter, i.e. a sort of duplex is present. However, because a conference room is a domain of a shared medium where only one person can speak at a time, otherwise collisions occur, the duplex here is a half-duplex.

5. Can a session run out of time without going through the entire intended content if an interesting topic elicits a larger discussion where many attendees have questions? If you did not want this to happen, what would be the best way to ensure that it does not occur?

Absolutely – with increasing amount of information to be shared over the same medium, each speaker must wait for others to finish their speech. This in turn delays every speaker, possibly resulting in the presenter not making it through the whole content of the presentation. With increasing number of stations in a network, especially if the communication has a one-to-all nature, it may become more and more difficult to transmit data in time.

Class Activity – Managing the Medium

6. Imagine that the session is in a panel format, which allows more free discussion of attendees with the panelists and among themselves. If a person wants to address another person within the same room, can he/she do it directly? If so, how is this possible? How would a panelist invite another person to join who is not presently in the room?

Within the same room, attendees can address themselves directly – they are in the same domain, on the same medium, they can hear each other immediately. There is no need for any intermediate process to deliver the data. Even if there is a device that aids to relay the information just to the intended recipient within the room (such as one person asking another to relay his message to the faraway neighbor), if any person stood out and started shouting, everyone could hear it.

If a panelist wanted to invite another person to the room, he/she would need to ask the assistants to search for that person and invite him. These assistants would need to purposefully route the invitation further until it reaches the invited person.

Communication within the same network is done immediately. Communication with nodes outside the network is mediated by routers.

7. What benefit, if any, was achieved by the isolation of multiple sessions into separate conference rooms if, after the event, people could meet and share the information?

As explained, the isolation was not done to provide security in the first place. The isolation was to contain the communication of the same or similar properties into a well-managed environment that allows the participants to interact directly, and to talk in a mediated, routed way to those who are not within the same domain. This reduced the number of possible collisions and also reduces the impact of broadcasts (shouting) on the network.

Identify elements of the model that map to IT-related content:

- **Conference room** – Data-link layer domain, broadcast domain
- **Seat in a conference room** – Corresponds to a particular L3 or L2 address
- **Questions, inquiries** – Correspond to bi-directional, duplex communication
- **Method of asking a question** – Corresponds to media access control method
- **Shouting over a conference room** – Corresponds to broadcast

Lab A - Identifying Network Devices and Cabling (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Identify Network Devices

Part 2: Identify Network Media

Background / Scenario

As a member of the networking support staff, you must be able to identify different networking equipment. You must also understand the function of equipment in the appropriate part of the network. In this lab, you will have access to network devices and media. You will identify the type and characteristics of the network equipment and media.

Instructor Note: This is an open-ended lab. Devices and cabling to be identified will be dependent on what the academy and instructor have available (either standalone or in racks). Although real equipment is preferable, the instructor can supplement real devices with good quality photos of devices, if desired.

Instructor Note: Instructors are encouraged to contact the local telephone company (telco) and cable operators for cabling examples. A tour of the academy data center (with approval of the IT director) can be a valuable experience for the students. The instructor can coordinate with the IT or Networking department to tag various devices in a real environment for identification.

Part 1: Identify Network Devices

Your instructor will provide various network devices for identification. Each will be tagged with an ID number.

Instructor Note: The various network devices displayed can be hubs, switches, routers, wireless access point, wireless router (Linksys), and NICs. Devices can be placed on a table or located in racks where the student can have access to examine each device. Have students record the device ID number, manufacturer, and model, type of device (hub, router or switch, etc), functionality (wireless, router, switch or combination), number and type of interfaces, and other notable physical characteristics.

Fill in the table below with the device tag ID number, manufacturer, device model, type (hub, switch, and router), functionality (wireless, router, switch, or combination), and other physical characteristics, such as number of interface types. The first line is filled out as a reference.

ID	Manufacturer	Model	Type	Functionality	Physical Characteristics
1	Cisco	1941	Router	Router	2 GigabitEthernet Ports 2 EHWIC slots 2 CompactFlash slots 1 ISM slot 2 Console ports: USB, RJ-45
2					
3					
4					
5					
6					

Part 2: Identify Network Media

Your instructor will provide various network media for identification. You will name the network media, identify the media type (copper, fiber optic, or wireless), and provide a short media description including what device types it connects. Use the table below to record your findings. The first line in the table has been filled out as a reference.

Instructor Note: The following is a list of network media for your reference.

Copper: Ethernet (STP, UTP, straight and cross, Cat 5, Cat 5E, Cat 6, etc), Telephone cable (2-wire supports ADSL so it is a valid network cable), Coaxial cable (cable network), Serial cables (DB 60 and smart serial, male/female).

Fiber optic: (multi-mode, single mode, various connector types).

Wireless: NIC, Wi-Fi Antennae (from Linksys or similar).

Lab A - Identifying Network Devices and Cabling

ID	Network Media	Type	Description and to What It Connects
1	UTP	Copper	Connect wired NIC and Ethernet ports on network devices Cat 5 straight-through wired. Connects PCs and routers to switches and wiring panels.
2			
3			
4			
5			
6			

Reflection

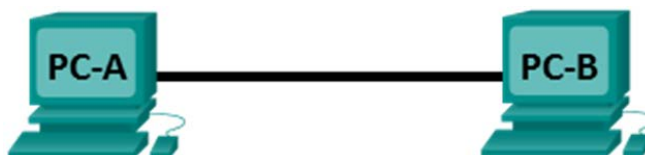
After you have identified the network equipment, where would you find more information about the equipment?

RFC, equipment manufacturer website or literature

Lab - Building an Ethernet Crossover Cable (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-A	NIC	192.168.10.1	255.255.255.0	N/A
PC-B	NIC	192.168.10.2	255.255.255.0	N/A

Objectives

Part 1: Analyze Ethernet Cabling Standards and Pinouts

Part 2: Build an Ethernet Crossover Cable

Part 3: Test an Ethernet Crossover Cable

Background / Scenario

In this lab, you will build and terminate an Ethernet crossover cable and test it by connecting two PCs together and pinging between them. You will first analyze the Telecommunications Industry Association/Electronic Industries Association (TIA/EIA) 568-A and 568-B standards and how they apply to Ethernet cables. You will then construct an Ethernet crossover cable and test it. Finally, you will use the cable you just constructed to connect two PCs together and test it by pinging between them.

Note: With autosensing capabilities available on many devices, such as the Cisco 1941 Integrated Services Router (ISR) switch, you may see straight-through cables connecting like devices.

Instructor Note: This optional lab can be quite challenging for some students. Many RJ-45 connectors may be used before a successful cable is built. If resources are limited, you may wish to have two students build one cable instead of having each student construct one individually.

Required Resources

- One length of cable, either Category 5 or 5e. Cable length should be 0.6 to 0.9m (2 to 3 ft.)
- 2 RJ-45 connectors
- RJ-45 crimping tool
- Wire cutter
- Wire stripper
- Ethernet cable tester (optional)

- 2 PCs (Windows 7 or 8)

Part 1: Analyze Ethernet Cabling Standards and Pinouts

The TIA/EIA has specified unshielded twisted pair (UTP) cabling standards for use in LAN cabling environments. TIA/EIA 568-A and 568-B stipulates the commercial cabling standards for LAN installations; these are the standards most commonly used in LAN cabling for organizations and they determine which color wire is used on each pin.

With a crossover cable, the second and third pairs on the RJ-45 connector at one end of the cable are reversed at the other end, which reverses the send and receive pairs. The cable pinouts are the 568-A standard on one end and the 568-B standard on the other end. Crossover cables are normally used to connect hubs to hubs or switches to switches, but they can also be used to directly connect two hosts to create a simple network.

Note: With modern networking devices, a straight-through cable can often be used even when connecting like devices because of their autosensing feature. With autosensing, the interfaces detect whether the send and receive circuit pairs are correctly connected. If they are not, the interfaces reverse one end of the connection. Autosensing also alters the speed of the interfaces to match the slowest one. For example, if connecting a Gigabit Ethernet (1000 Mb/s) router interface to a Fast Ethernet (100 Mb/s) switch interface, the connection uses Fast Ethernet.

The Cisco 2960 switch has autosensing turned on, by default; therefore, connecting two 2960 switches together works with either a crossover or a straight-through cable. With some older switches, this is not the case and a crossover cable must be used.

In addition, the Cisco 1941 router Gigabit Ethernet interfaces are autosensing and a straight-through cable may be used to connect a PC directly to the router interface (bypassing the switch). With some older routers, this is not the case and a crossover cable must be used.

When directly connecting two hosts, it is generally advisable to use a crossover cable.

Step 1: Analyze diagrams and tables for the TIA/EIA 568-A standard Ethernet cable.

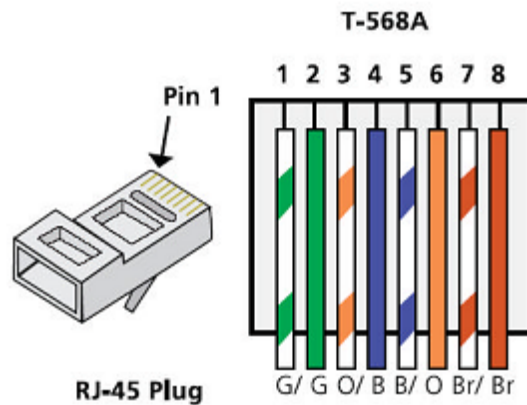
The following table and diagrams display the color scheme and pinouts, as well as the function of the four pairs of wires used for the 568-A standard.

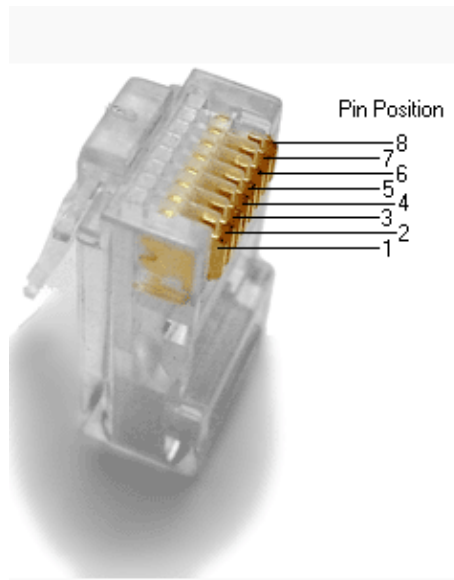
Note: In LAN installations using 100Base-T (100 Mb/s), only two pairs out of the four are used.

568-A 10/100/1000Base-TX Ethernet

Pin Number	Pair Number	Wire Color	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	White/Green	Transmit	BI_DA+
2	2	Green	Transmit	BI_DA-
3	3	White/Orange	Receive	BI_DB+
4	1	Blue	Not Used	BI_DC+
5	1	White/Blue	Not Used	BI_DC-
6	3	Orange	Receive	BI_DB-
7	4	White/Brown	Not Used	BI_DD+
8	4	Brown	Not Used	BI_DD-

The following diagrams display how the wire color and pinouts align with an RJ-45 jack for the 568-A standard.



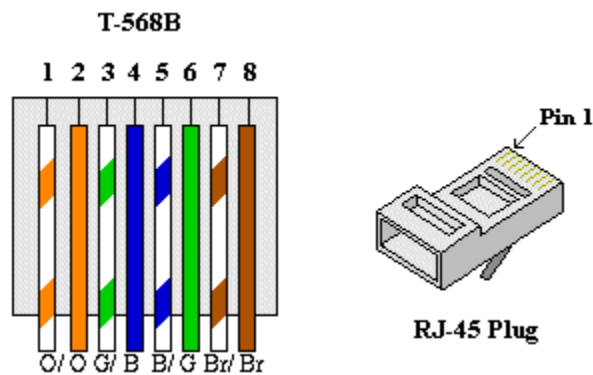


Step 2: Analyze diagrams and tables for the TIA/EIA 568-B standard Ethernet cable.

The following table and diagram display the color scheme and pinouts for the 568-B standard.

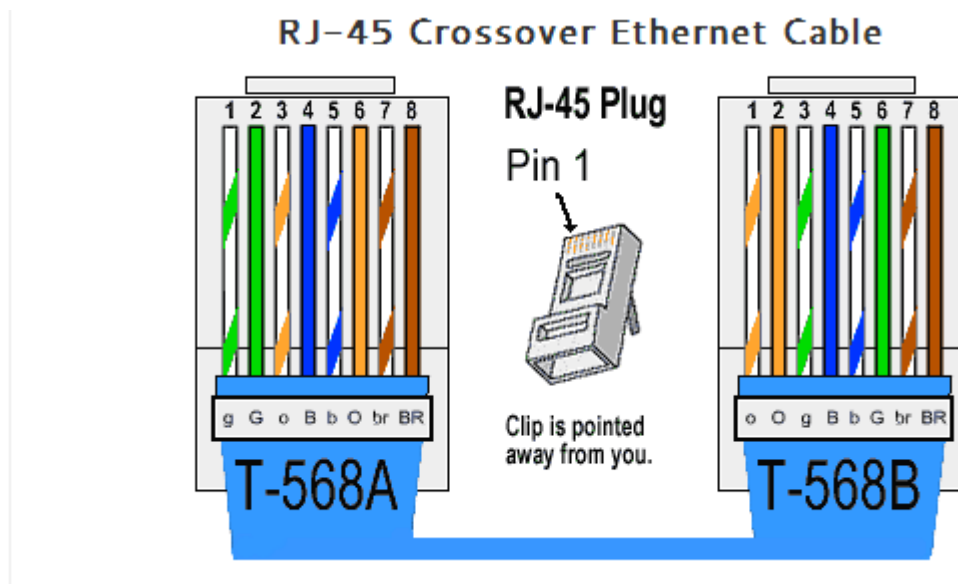
568-B 10/100/1000-BaseTX Ethernet

Pin Number	Pair Number	Wire Color	10Base-T Signal 100Base-TX Signal	1000Base-T Signal
1	2	White/Orange	Transmit	BI_DA+
2	2	Orange	Transmit	BI_DA-
3	3	White/Green	Receive	BI_DB+
4	1	Blue	Not Used	BI_DC+
5	1	White/Blue	Not Used	BI_DC-
6	3	Green	Receive	BI_DB-
7	4	White/Brown	Not Used	BI_DD+
8	4	Brown	Not Used	BI_DD-



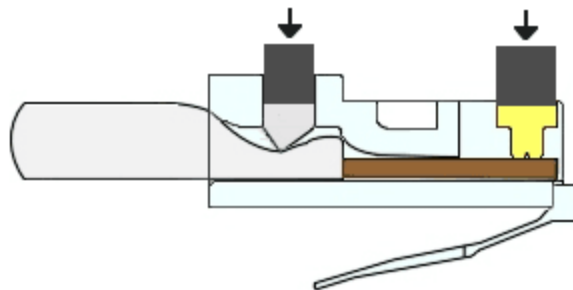
Part 2: Build an Ethernet Crossover Cable

A crossover cable has the second and third pairs on the RJ-45 connector at one end, reversed at the other end (refer to the table in Part 1, Step 2). The cable pinouts are the 568-A standard on one end and the 568-B standard on the other end. The two following diagrams illustrate this concept.



Step 1: Build and terminate a TIA/EIA 568-A cable end.

- Determine the cable length required. (Your instructor will let you know the cable length you should make.)
Note: If you were making a cable in a production environment, the general guideline is to add another 12 in. (30.48 cm) to the length.
- Cut off a piece of cable to the desired length and using your wire stripper, remove 5.08 cm (2 in.) of the cable jacket from both ends.
- Hold the four pairs of twisted cables tightly where the jacket was cut away. Reorganize the cable pairs into the order of the 568-A wiring standard. Refer to the diagrams, if necessary. Take as much care as possible to maintain the twists in the cable; this provides noise cancellation.
- Flatten, straighten, and line up the wires using your thumb and forefinger.
- Ensure that the cable wires are still in the correct order for the 568-A standard. Using your wire cutters, trim the four pairs in a straight line to within 1.25 to 1.9 cm (1/2 to 3/4 in.).
- Place an RJ-45 connector on the end of your cable, with the prong on the underside pointing downward. Firmly insert the wires into the RJ-45 connector. All wires should be seen at the end of the connector in their proper positions. If the wires are not extending to the end of the connector, take the cable out, rearrange the wires as necessary, and reinsert the wires back into the RJ-45 connector.
- If everything is correct, insert the RJ-45 connector with cable into the crimping tool. Crimp down hard enough to force the contacts on the RJ-45 connector through the insulation on the wires, thus completing the conducting path. See the following diagram for an example.



Step 2: Build and terminate a TIA/EIA 568-B cable end.

Repeat steps 1a to 1g using the 568-B color wiring scheme for the other end.

Part 3: Test an Ethernet Crossover Cable

Step 1: Test the cable.

Many cable testers will test for length and mapping of wires. If the cable tester has a wire map feature, it verifies which pins on one end of the cable are connected to which pins on the other end.

If your instructor has a cable tester, test the crossover cable for functionality. If it fails, check with your instructor first as to whether you should re-cable the ends and re-test.

Step 2: Connect two PCs together via NICs using your Ethernet crossover cable.

- Working with a lab partner, set your PC to one of the IP addresses shown in the Addressing Table (see page 1). For example, if your PC is **PC-A**, your IP address should be set to **192.168.10.1** with a **24-bit subnet mask**. Your partner's IP address should be **192.168.10.2**. The default gateway address can be left empty.
- Using the crossover cable you made, connect the two PCs together via their NICs.
- On the PC-A command prompt, ping the PC-B IP address.

Note: The Windows firewall may have to be temporarily disabled for pings to be successful. If the firewall is disabled, make sure you re-enable it at the conclusion of this lab.

- Repeat the process and ping from PC-B to PC-A.

Assuming IP addressing and firewall are not issues, your pings should be successful if the cables were properly made.

Reflection

- Which part of making cables did you find the most difficult?

Answers will vary. Inserting the cables in the proper order into the RJ-45 connector is usually the hardest part.

- Why do you have to learn how to make a cable if you can easily buy pre-made cables?

A cable may go bad in a production environment. It may be too time consuming or costly to replace and it is often simpler to merely re-cable each end if necessary.

Lab – Viewing Wireless and Wired NIC Information (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Identify and Work with PC NICs

Part 2: Identify and Use the System Tray Network Icons

Background / Scenario

This lab requires you to determine the availability and status of the network interface cards (NICs) on the PC that you use. Windows provides a number of ways to view and work with your NICs.

In this lab, you will access the NIC information of your PC and change the status of these cards.

Required Resources

- 1 PC (Windows 7 or 8 with two NICs, wired and wireless, and a wireless connection)

Note: At the start of this lab, the wired Ethernet NIC in the PC was cabled to one of the integrated switch ports on a wireless router and the Local Area Connection (wired) was enabled. The wireless NIC was disabled initially. If the wired and wireless NICs are both enabled the PC will receive two different IP addresses and the wireless NIC will take precedence.

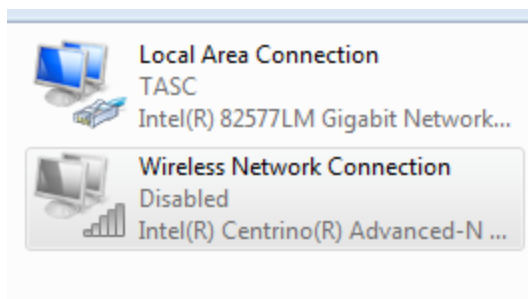
Part 1: Identify and Work with PC NICs

In Part 1, you will identify the NIC types in the PC that you are using. You will explore different ways to extract information about these NICs and how to activate and deactivate them.

Note: This lab was performed using a PC running on the Windows 7 operating system. You should be able to perform the lab with one of the other Windows operating systems listed; however, menu selections and screens may vary.

Step 1: Use the Network and Sharing Center.

- Open the **Network and Sharing Center** by clicking the Windows **Start** button > **Control Panel** > **View network status and tasks** under Network and Internet heading in the Category View.
- In the left pane, click the **Change adapter settings** link.
- The Network Connections window displays, which provides the list of NICs available on this PC. Look for your Local Area Connection and Wireless Network Connection adapters in this window.

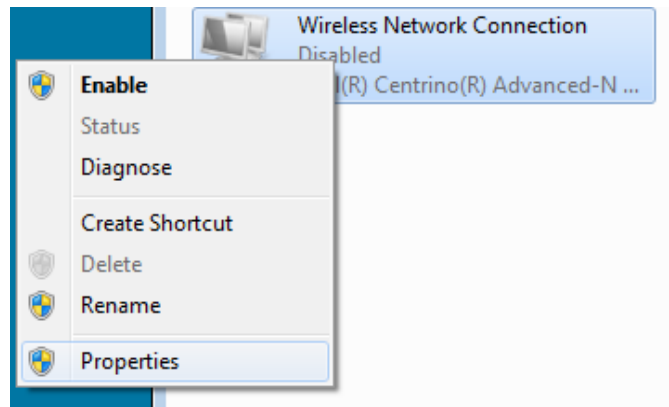


Lab – Viewing Wireless and Wired NIC Information

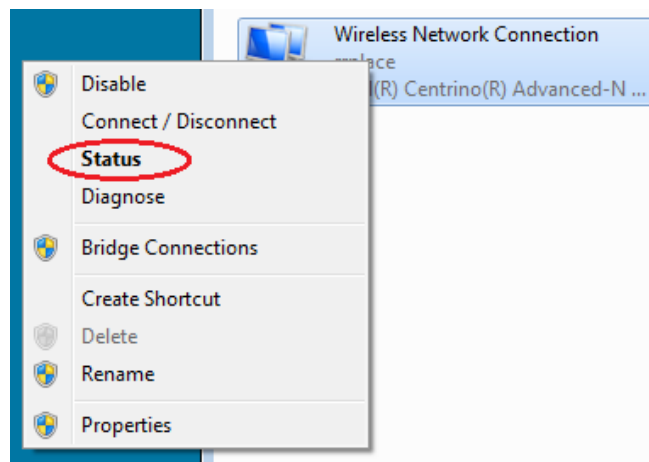
Note: Virtual Private Network (VPN) adapters and other types of network connections may also be displayed in this window.

Step 2: Work with your wireless NIC.

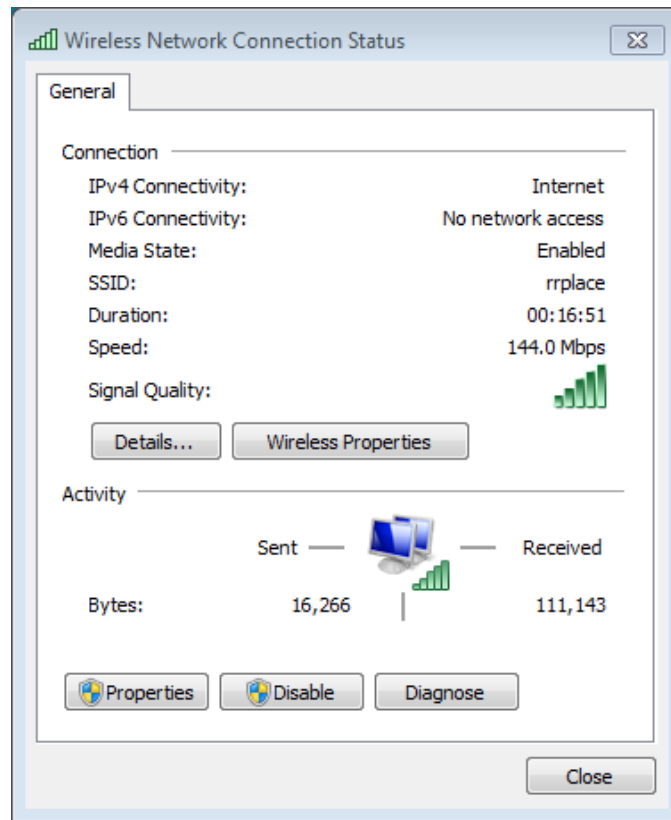
- a. Select the **Wireless Network Connection** option and right-click it to bring up a drop-down list. If your wireless NIC is disabled, you will have an option to **Enable** it. If your NIC was already enabled, then **Disable** would be the first option on this drop-down menu. If your **Wireless Network Connection** is currently disabled, then click **Enable**.



- b. Right-click the **Wireless Network Connection**, and then click **Status**.



- c. The Wireless Network Connection Status window displays where you can view information about your wireless connection.



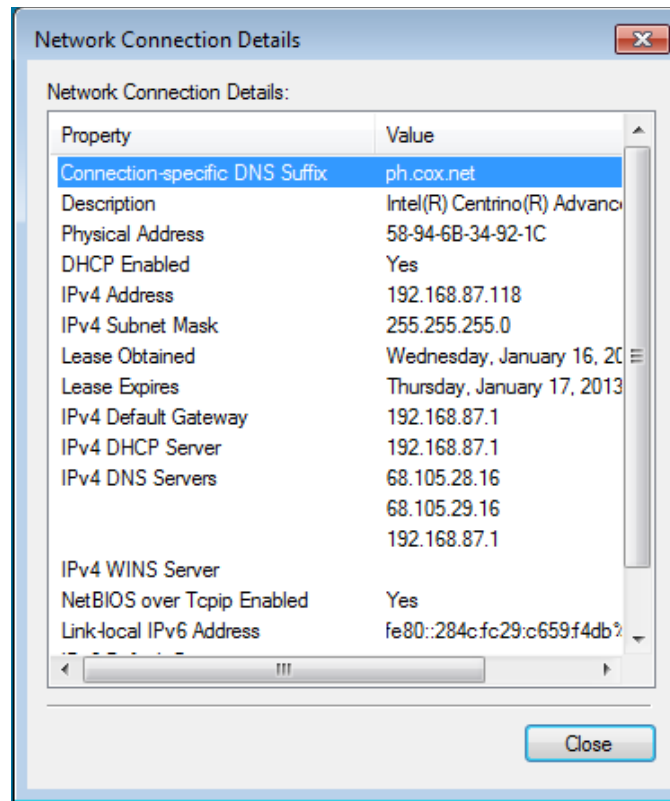
What is the Service Set Identifier (SSID) for the wireless router of your connection?

_____ rrplace (in above example)

What is the speed of your wireless connection?

_____ 144.0 Mb/s (in above example)

- d. Click **Details** to display the Network Connection Details window.



What is the MAC address of your wireless NIC?

_____ 58-94-6b-34-92-1c (in above example)

Do you have multiple IPv4 DNS Servers listed?

_____ Yes (in above example)

Why would multiple DNS Servers be listed?

Answers will vary, but multiple DNS Servers are listed in case the first DNS server becomes unresponsive. Reasons may include the server is down for maintenance or is experiencing a problem. If the first DNS server does not respond, then the second DNS Server is used, and so on.

- e. When you have reviewed the network connection details, click **Close**.
- f. Open a command window prompt and type **ipconfig /all**.


```
Wireless LAN adapter Wireless Network Connection:

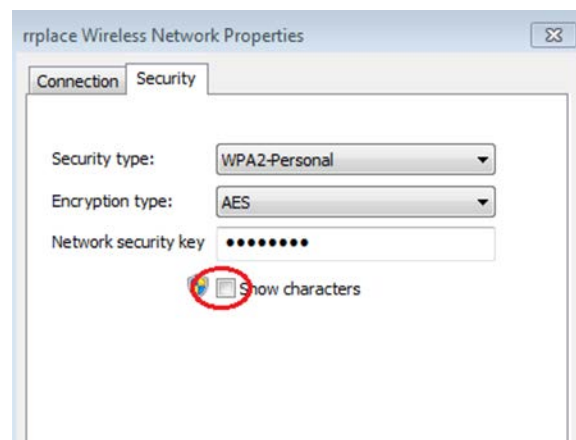
Connection-specific DNS Suffix . : ph.cox.net
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address . . . . . : 58-94-6B-34-92-1C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::284c:fc29:c659:f4db%11(Preferred)
IPv4 Address. . . . . : 192.168.87.118(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, January 17, 2013 8:30:40 AM
Lease Expires . . . . . : Friday, January 18, 2013 8:30:41 AM
Default Gateway . . . . . : 192.168.87.1
DHCP Server . . . . . : 192.168.87.1
DHCPv6 IAID . . . . . : 307795051
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-AC-22-0A-5C-26-0A-24-2A-60
DNS Servers . . . . . : 68.105.28.16
                       : 68.105.29.16
                       : 192.168.87.1
NetBIOS over Tcpip. . . . . : Enabled
```

Notice that the information displayed here is the same information that was displayed in the Network Connection Details window in Step d.

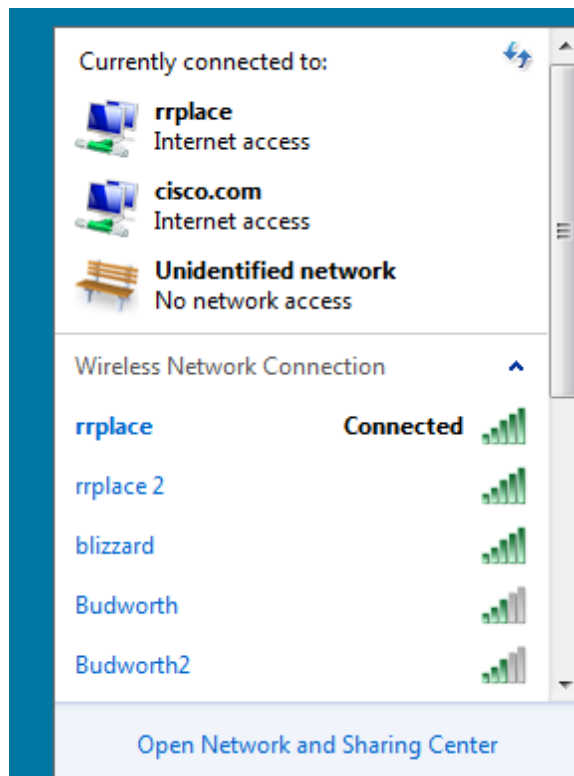
- g. Close the command window and the Network Connection Details windows. This should bring you back to the Wireless Network Connection Status window. Click **Wireless Properties**.
- h. In the **Wireless Network Properties** window, click the **Security** tab.



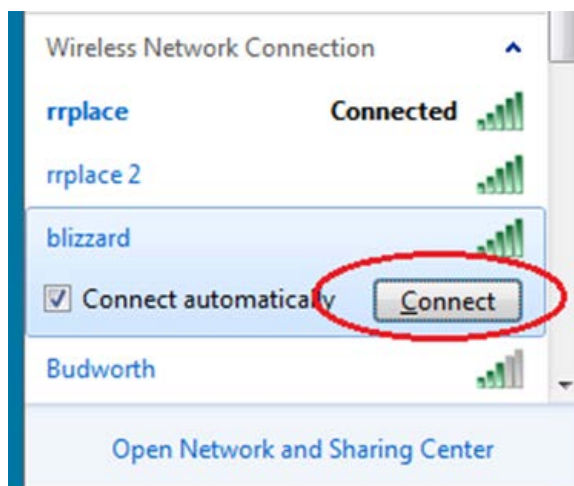
- i. The type of security the connected wireless router has implemented displays. Click the **Show characters** check box to display the actual Network security key, instead of the hidden characters, and then click **OK**.



- j. Close the Wireless Network Properties and the Network Connection Status windows. Select and right-click the **Wireless Network Connection** option > **Connect/Disconnect**. A pop-up window should appear at the bottom right corner of your desktop that displays your current connections, along with a list of SSIDs that are in range of the wireless NIC of your PC. If a scrollbar appears on the right side of this window, you can use it to display additional SSIDs.



- k. To join one of the other wireless network SSIDs listed, click the SSID that you want to join, and then click **Connect**.



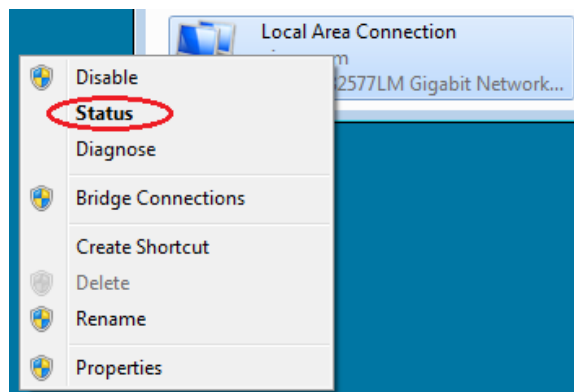
- l. If you have selected a secure SSID, you are prompted to enter the **Security key** for the SSID. Type the security key for that SSID and click **OK**. You can click the **Hide characters** check box to prevent people from seeing what you type in the **Security key** field.



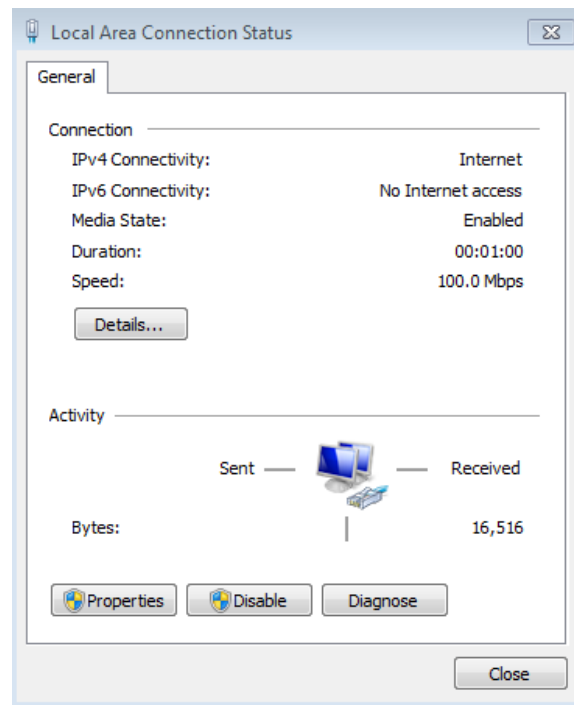
Step 3: Work with your wired NIC.

- a. On the Network Connections window, select and right-click the **Local Area Connection** option to display the drop-down list. If the NIC is disabled, enable it, and then click the **Status** option.

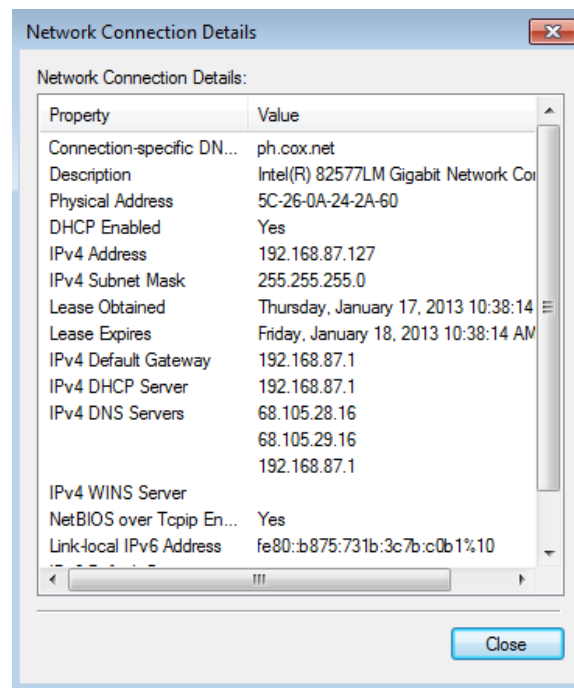
Note: You must have an Ethernet cable attaching your PC NIC to a switch or similar device to see the status. Many wireless routers have a small 4-port Ethernet switch built-in. You can connect to one of the ports using a straight-through Ethernet patch cable.



- b. The Local Area Connection Status window will open. This window displays information about your wired connection to the LAN.



- c. Click **Details...** to view the address information for your LAN connection.



- d. Open a command window prompt and type **ipconfig /all**. Find your Local Area Connection information and compare this with the information displayed in the Network Connection Details window.

```
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . : ph.cox.net
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 5C-26-0A-24-2A-60
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10<Preferred>
IPv4 Address. . . . . : 192.168.87.127<Preferred>
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, January 17, 2013 10:38:14 AM
Lease Expires . . . . . : Friday, January 18, 2013 10:38:14 AM
Default Gateway . . . . . : 192.168.87.1
DHCP Server . . . . . : 192.168.87.1
DHCPv6 Iaid . . . . . : 240920074
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-AC-22-0A-5C-26-0A-24-2A-60
DNS Servers . . . . . : 68.105.28.16
                       : 68.105.29.16
                       : 192.168.87.1
NetBIOS over Tcpip. . . . . : Enabled
```

- e. Close all windows on your desktop.

Part 2: Identify and Use the System Tray Network Icons

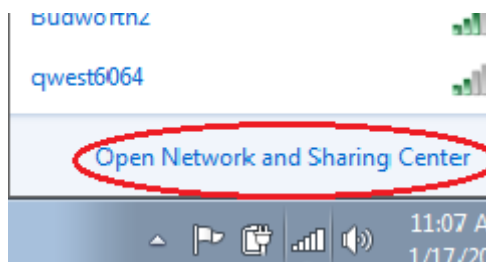
In Part 2, you will use the network icons in your system tray to determine and control the NICs on your PC.

Step 1: Use the Wireless Network icon.

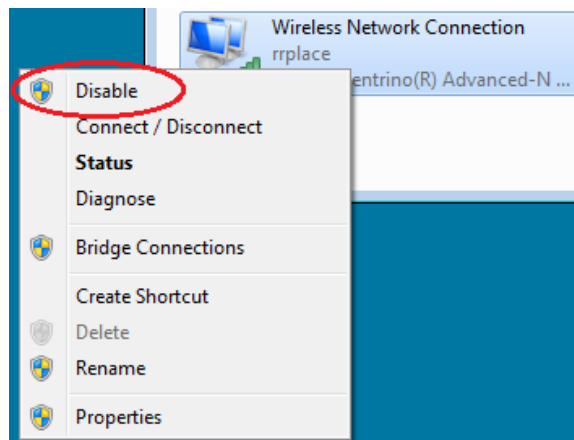
- a. Click the system tray **Wireless Network** icon to view the pop-up window that displays the SSIDs that are in-range of your wireless NIC. When the system tray displays the Wireless Network icon, the wireless NIC is active.



- b. Click the **Open Network and Sharing Center** link. **Note:** This is a shortcut way to bring up this window.



- c. In the left pane, click the **Change adapter settings** link to display the Network Connections window.
- d. Select and right-click the **Wireless Network Connection**, and then click **Disable** to disable your wireless NIC.



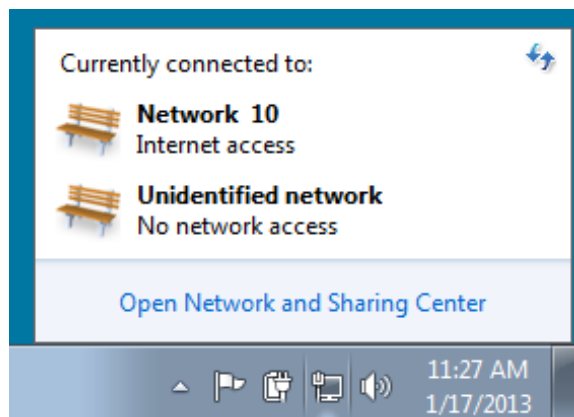
- e. Examine your system tray. The **Wireless Network Connection** icon should be replaced by the **Wired Network** icon, which indicates that you are using your wired NIC for network connectivity.



Note: If both NICs are active, the **Wireless Network** icon is the one that is displayed.

Step 2: Use the Wired Network icon.

- a. Click the **Wired Network** icon. Notice that the Wireless SSIDs are no longer displayed in this pop-up window, but you still have the ability to get to the Network and Sharing Center window from here.



- b. Click the **Open Network and Sharing Center** link > **Change adapter settings** and **Enable** your **Wireless Network Connection**. The **Wireless Network** icon should replace the **Wired Network** icon in your system tray.



Step 3: Identify the Network Problem icon.

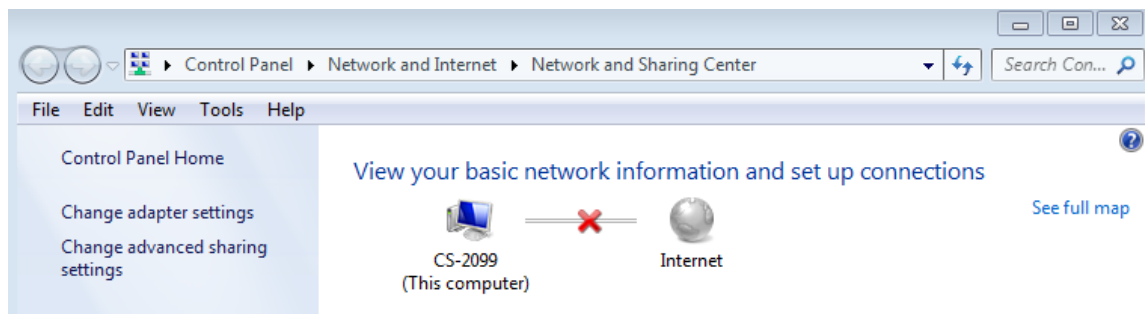
- a. On the Network Connections window, disable both the **Wireless Network Connection** and the **Local Area Connection**.

Lab – Viewing Wireless and Wired NIC Information

- b. The system tray now displays the **Network Disabled** icon, which indicates that network connectivity has been disabled.



- c. You can click this icon to return to the Network and Sharing Center window (examine the network diagram at the top).



You can click the red **X** to have the PC troubleshoot the problem with the network connection. Troubleshooting attempts to resolve the network issue for you.

- d. If troubleshooting did not enable one of your NICs, then you should do this manually to restore the network connectivity of your PC.

Note: If a network adapter is enabled and the NIC is unable to establish network connectivity, then the **Network Problem** icon appears in the system tray.



If this icon appears, you can troubleshoot this issue just like you did in Step 3c.

Reflection

Why would you activate more than one NIC on a PC?

Answers may vary. Multiple NICs can be used if more than one path is needed for the PC. One example of this would be if the PC is being used as a Proxy Server.

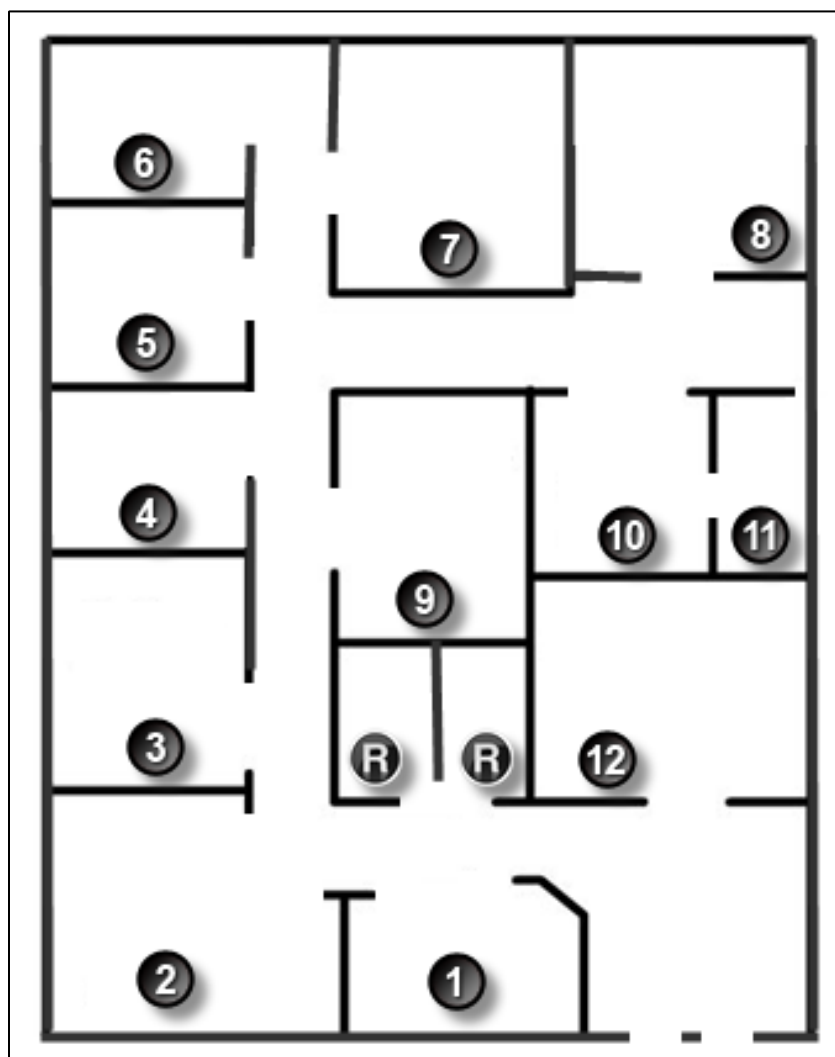
Class Activity - Linked In! (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Connect devices using wired and wireless media.

Physical Topology



Background /Scenario

Note: This activity is best completed in groups of 2-3 students.

Your small business is moving to a new location! Your building is brand new, and you must come up with a physical topology so that network port installation can begin.

Class Activity - Linked In!

Your instructor will provide you with a blueprint created for this activity. The area on the blueprint, indicated by Number 1, is the reception area and the area numbered RR is the restroom area.

All rooms are within Category 6 UTP specifications (100 meters), so you have no concerns about hard-wiring the building to code. Each room in the diagram must have at least one network connection available for users/intermediary devices.

Do not go into excessive detail on your design. Just use the content from the chapter to be able to justify your decisions to the class.

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their comprehension of the data link layer from a physical perspective – wired and wireless connectivity. A facilitated discussion should be initiated as a result of this activity.

Required Resources

- Packet Tracer software

Reflection

1. Where would you locate your network main distribution facility, while keeping security in mind?

Room 11 is the smallest room and would serve well as the main distribution facility or network center. It is situated away from plumbing, which could interfere with copper quality. It is also located away from most of the other offices/rooms for security purposes and has only one entry door.

2. How many intermediary devices you would use and where would you place them?

One or two switches could be placed in Room 11 – for scalability and access to other end devices. One router for connectivity to the ISP could be placed in Room 11, as well. One or two wireless ISRs could be placed in the diagram, possibly in Room 7 or 12 for wireless access throughout the physical space.

3. What kind of cabling you would use (UTP, STP, wireless, fiber optics, etc.) and where would the ports be placed?

Each room would incorporate at least one UTP jack for intermediary device connectivity or singular user access. The central network room (main distribution facility) would need more than one network port as it serves internal (LAN) connections and external (WAN) connections – for the WAN, fiber optics would probably be run for ISP connectivity.

4. What types of end devices you would use (wired, wireless, laptops, desktops, tablets, etc.)?

Using the answers stated above, it would be feasible to use a combination of wired, wireless laptops, desktops, servers, tablets, etc. Security and scalability are considered in this model.

Identify elements of the model that map to real-world content:

- Network security is considered when connecting a network at the network access layer.

Class Activity - Linked In!

- Types of cabling and different modes of technology are included as considerations in designing a network at the network access layer.
- Different data technologies are options are available to designers to facilitate data traffic flow at the network access layer.

Class Activity - Join My Social Circle! (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe the impact of ARP requests on network and host performance.

Background / Scenario

Note: This activity can be completed individually in class or outside of class.

A lot of our network communication is in the form of email, messaging (text or instant), video contact, and social media postings.

For this activity, choose one of the following types of network communications and answer the questions in the Reflection section.

- Text or instant message
- Audio/video conference
- Email
- Online gaming

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of source and destination host identification as compared to social media. Students' answers should generate discussion about how we are identified as we communicate through these types of networks.

Required Resources

- Recording capabilities (paper, tablet, etc.) so that reflective comments can be shared with the class.

Reflection

1. Is there a procedure you must follow to register others and yourself so that you can form a communications account? Why do you think that a procedure is needed?

In each of these services, you are bringing the person you want to communicate with “directly into your network”. You are doing this in order to have contact with your friends and be able to communicate directly. You do not want to have an intermediary person relay messages between you and your friends in your network. By registering yourself and your friends to your contact list, you are building your own (social) communication network.

During the registration process, you as a person with a civil name are assigned a service-specific user identifier that identifies you in the particular communication service. When you add your friends to your contact list, you are looking for their service-specific user identifiers. This service-specific user identifier may have different formats:

- **Email service:** Has an email address
- **ICQ accounts:** Have a number
- **Skype, LinkedIn, or Facebook accounts:** Have a username

Class Activity - Join My Social Circle!

When you contact the person, you select their civil name in your contact list and the system contacts the user using the associated user identifier. A single person may have different user identifiers depending on how many social networks he or she subscribes to.

In communication networks, there is a similar process. Although a network node (for example, a PC) is a single entity, it may have several network interface cards (NICs). In IP networks, this would be a process of associating the peer's IP address in the same network with its Layer 2 data-link layer address. On Ethernet and WiFi, IP uses a supporting protocol called Address Resolution Protocol (ARP) to perform this translation.

2. How do you initiate contact with the person or people with whom you wish to communicate?
-

The exact sequence of steps depends on the service you are using to communicate with your peer. However, there will always be common steps: First, decide within which network your peer is reachable. Second, look up the person's contact in your contact list, and use it to send your peer a message. Depending on the service, the message will be received only by this person (email or instant messaging services) or it may be visible by other people in the recipient's network (LinkedIn or Facebook message boards). However, there is no doubt who the intended recipient is.

When Node A needs to send a message to Node B in an IP network, it determines which network the peer (Node B) is located within. Node A performs a destination IP (or next-hop IP) into Layer 2 address translation in order to determine how to address Node B's NIC. If there are switches on the path between Node A and B, Node A can send a message that can only be delivered to Node B's NIC. If there are WiFi stations that can hear each other, Node A's message to Node B can be seen by others.

3. How do you ensure that your conversations are received only by those with whom you wish to communicate?
-

The primary prerequisite is that the message is clearly addressed to a single intended recipient. This is the purpose of using a contact list that associates individual persons with their unique user identifiers. If we do not know the user identifier of the recipient, we have to send the message to everyone or not at all. In IP networks, this is accomplished by the resolution of the recipient (or next-hop) IP address into its unique Layer 2 address, using ARP or a similar mechanism. It is then up to the network technology to make sure that the message is sent only to the intended recipient.

Some technologies do not allow messages to be sent in a way that prevents third parties from seeing the message. For example, in Ethernet deployments using hubs or WiFi, the transmission is always visible to all nodes in the network. Only the intended recipient will process the message, but others can see it. This is similar to message boards on LinkedIn or Facebook where, although intended for a single recipient, many or all other users can see the messages.

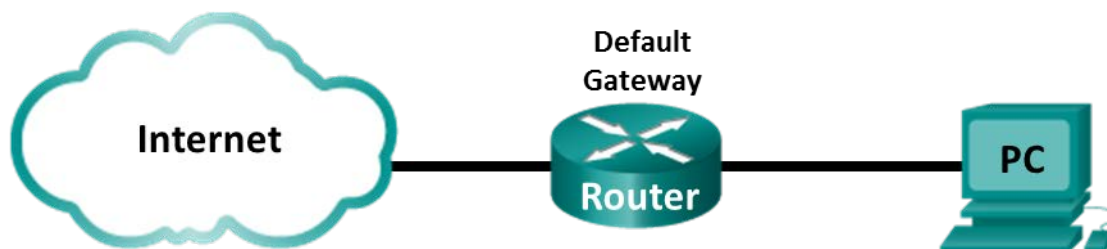
Identify elements of the model that map to IT-related content:

- Different social network technologies correspond to different network technologies.
- User IDs for one particular person, depending on the social network the person is subscribed to, correspond to different Layer 2 addressing used by different network technologies.
- Contact lists correspond to tables where Layer 3-to-Layer 2 mappings are stored (e.g. ARP tables in Ethernet or IP/DLCI tables in Frame Relay).
- Subscribing to a social network corresponds to the process of obtaining access to a particular network and the related network technology.
- Looking up a person in one's contact list corresponds to lookups in the L3/L2 mapping tables.

Lab – Using Wireshark to Examine Ethernet Frames (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding or to provide additional practice or both.

Topology



Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In the first part of this lab, you will review the fields contained in an Ethernet II frame. In Part 2, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

Instructor Note: This lab assumes that the student is using a PC with internet access. It also assumes that Wireshark has been pre-installed on the PC. The screenshots in this lab were taken from Wireshark v2.4.3 for Windows 10 (64bit).

Required Resources

- 1 PC (Windows 7, 8, or 10 with internet access with Wireshark installed)

Part 1: Examine the Header Fields in an Ethernet II Frame

In Part 1, you will examine the header fields and content in an Ethernet II frame. A Wireshark capture will be used to examine the contents in those fields.

Step 1: Review the Ethernet II header field descriptions and lengths.

Preamble	Destination Address	Source Address	Frame Type	Data	FCS
8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 – 1500 Bytes	4 Bytes

Step 2: Examine the network configuration of the PC.

This PC host IP address is 192.168.1.147 and the default gateway has an IP address of 192.168.1.1.

```
Microsoft Windows [Version 10.0.16299.64]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\> ipconfig /all

Windows IP Configuration

Host Name . . . . . : DESKTOP-C73CB0M
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

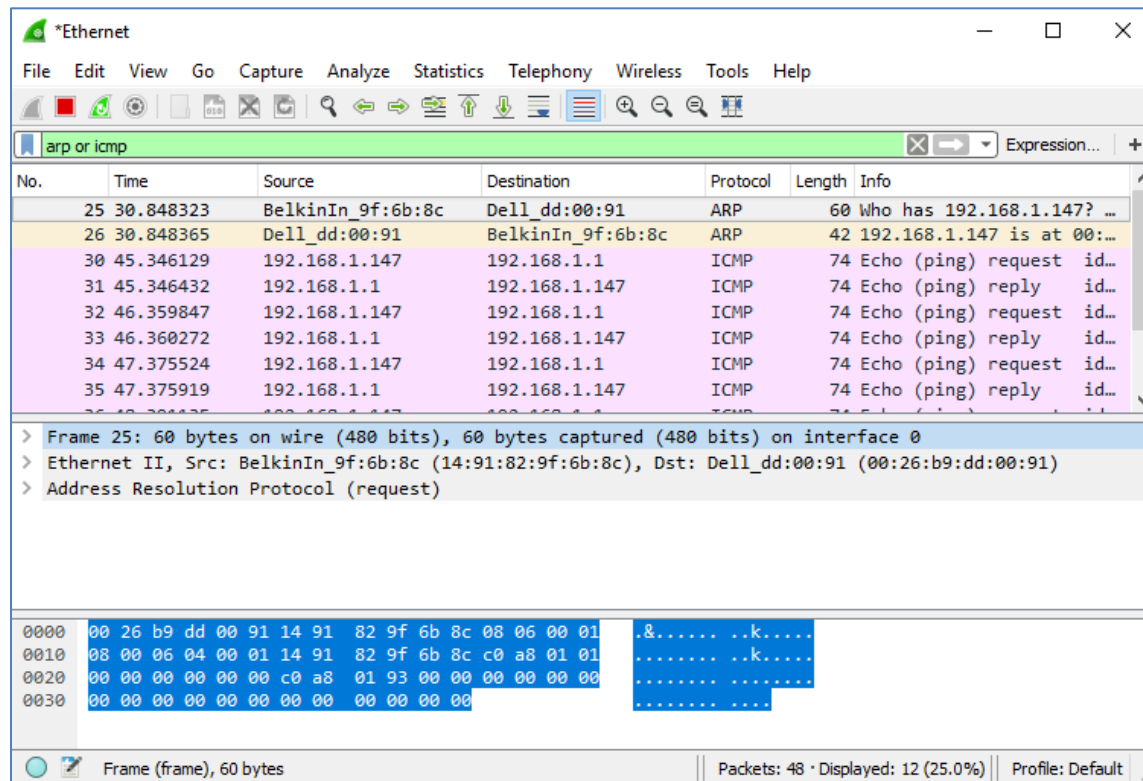
Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 00-26-B9-DD-00-91
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::d009:d939:110f:1b7f%20 (Preferred)
IPv4 Address. . . . . : 192.168.1.147 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
```

Step 3: Examine Ethernet frames in a Wireshark capture.

The Wireshark capture below shows the packets generated by a ping being issued from a PC host to its default gateway. A filter has been applied to Wireshark to view the ARP and ICMP protocols only. The

Lab – Using Wireshark to Examine Ethernet Frames

session begins with an ARP query for the MAC address of the gateway router, followed by four ping requests and replies.



The screenshot shows the Wireshark interface with a packet capture filter set to 'arp or icmp'. The packet list shows several packets, including an ARP request (No. 25) and several ICMP Echo (ping) requests and replies. The packet details pane shows the structure of the selected packet (No. 25), which is an Ethernet II frame containing an ARP request. The packet bytes pane shows the raw data of the selected packet, with a hex dump and ASCII representation.

No.	Time	Source	Destination	Protocol	Length	Info
25	30.848323	BelkinIn_9f:6b:8c	Dell_dd:00:91	ARP	60	Who has 192.168.1.147? ...
26	30.848365	Dell_dd:00:91	BelkinIn_9f:6b:8c	ARP	42	192.168.1.147 is at 00:...
30	45.346129	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id...
31	45.346432	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id...
32	46.359847	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id...
33	46.360272	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id...
34	47.375524	192.168.1.147	192.168.1.1	ICMP	74	Echo (ping) request id...
35	47.375919	192.168.1.1	192.168.1.147	ICMP	74	Echo (ping) reply id...

Frame 25: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: Dell_dd:00:91 (00:26:b9:dd:00:91)
Address Resolution Protocol (request)

0000 00 26 b9 dd 00 91 14 91 82 9f 6b 8c 08 06 00 01 .&.....k....
0010 08 00 06 04 00 01 14 91 82 9f 6b 8c c0 a8 01 01k....
0020 00 00 00 00 00 00 c0 a8 01 93 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Frame (frame), 60 bytes | Packets: 48 · Displayed: 12 (25.0%) | Profile: Default

Step 4: Examine the Ethernet II header contents of an ARP request.

The following table takes the first frame in the Wireshark capture and displays the data in the Ethernet II header fields.

Field	Value	Description
Preamble	Not shown in capture	This field contains synchronizing bits, processed by the NIC hardware.
Destination Address	Broadcast (ff:ff:ff:ff:ff:ff)	Layer 2 addresses for the frame. Each address is 48 bits long, or 6 octets, expressed as 12 hexadecimal digits, 0 – 9 , A–F. A common format is 12 : 34 : 56 : 78 : 9A : BC. The first six hex numbers indicate the manufacturer of the network interface card (NIC), the last six hex numbers are the serial number of the NIC. The destination address may be a broadcast, which contains all ones, or a unicast. The source address is always unicast.
Source Address	BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)	
Frame Type	0x0806	For Ethernet II frames, this field contains a hexadecimal value that is used to indicate the type of upper-layer protocol in the data field. There are numerous upper-layer protocols supported by Ethernet II. Two common frame types are these: Value Description 0x0800 IPv4 Protocol 0x0806 Address Resolution Protocol (ARP)
Data	ARP	Contains the encapsulated upper-level protocol. The data field is between 46 – 1,500 bytes.
FCS	Not shown in capture	Frame Check Sequence, used by the NIC to identify errors during transmission. The value is computed by the sending machine, encompassing frame addresses, type, and data field. It is verified by the receiver.

What is significant about the contents of the destination address field?

All hosts on the LAN will receive this broadcast frame. The host with the IP address of 192.168.1.1 (default gateway) will send a unicast reply to the source (PC host). This reply contains the MAC address of the NIC of the default gateway.

Why does the PC send out a broadcast ARP prior to sending the first ping request?

Before the PC can send a ping request to a host, it needs to determine the destination MAC address before it can build the frame header for that ping request. The ARP broadcast is used to request the MAC address of the host with the IP address contained in the ARP.

What is the MAC address of the source in the first frame? _____ It varies; in this case, it is 14:91:82:9f:6b:8c

What is the Vendor ID (OUI) of the Source NIC? _____ It varies, in this case, it is BelkinIn (Belkin International Inc.)

What portion of the MAC address is the OUI?

_____ The first 3 octets of the MAC address indicate the OUI.

What is the NIC serial number of the source? _____ It may vary, it is 9f:6b:8c in this case

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

In Part 2, you will use Wireshark to capture local and remote Ethernet frames. You will then examine the information that is contained in the frame header fields.

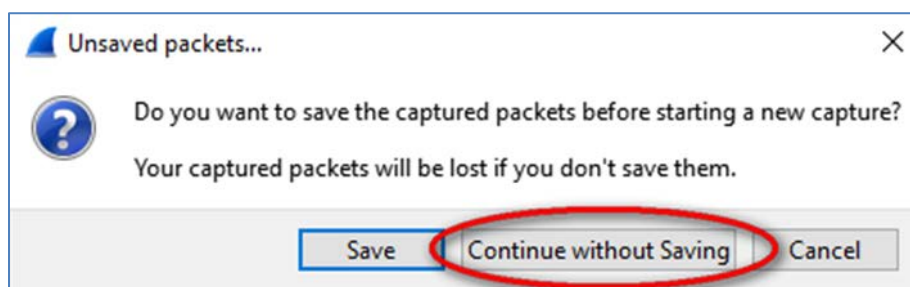
Step 1: Determine the IP address of the default gateway on your PC.

Open a command prompt window and issue the **ipconfig** command.

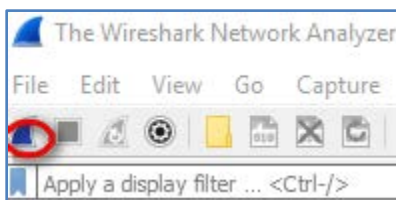
What is the IP address of the PC default gateway? _____ Answers will vary

Step 2: Start capturing traffic on your PC NIC.

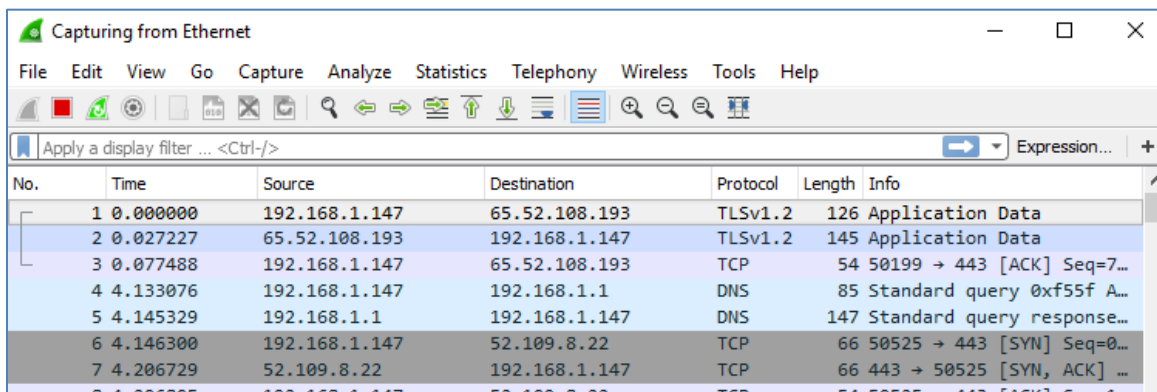
- a. Close Wireshark. No need to save the captured data.



- b. Open Wireshark, start data capture.



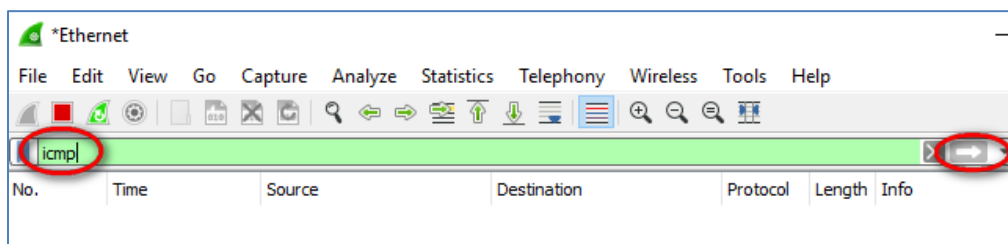
- c. Observe the traffic that appears in the packet list window.



Step 3: Filter Wireshark to display only ICMP traffic.

You can use the filter in Wireshark to block visibility of unwanted traffic. The filter does not block the capture of unwanted data; it only filters what to display on the screen. For now, only ICMP traffic is to be displayed.

In the Wireshark **Filter** box, type **icmp**. The box should turn green if you typed the filter correctly. If the box is green, click **Apply** (the right arrow) to apply the filter.

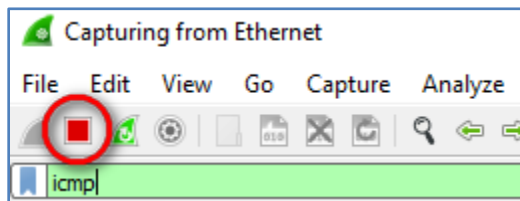


Step 4: From the command prompt window, ping the default gateway of your PC.

From the command window, ping the default gateway using the IP address that you recorded in Step 1.

Step 5: Stop capturing traffic on the NIC.

Click the **Stop Capture** icon to stop capturing traffic.

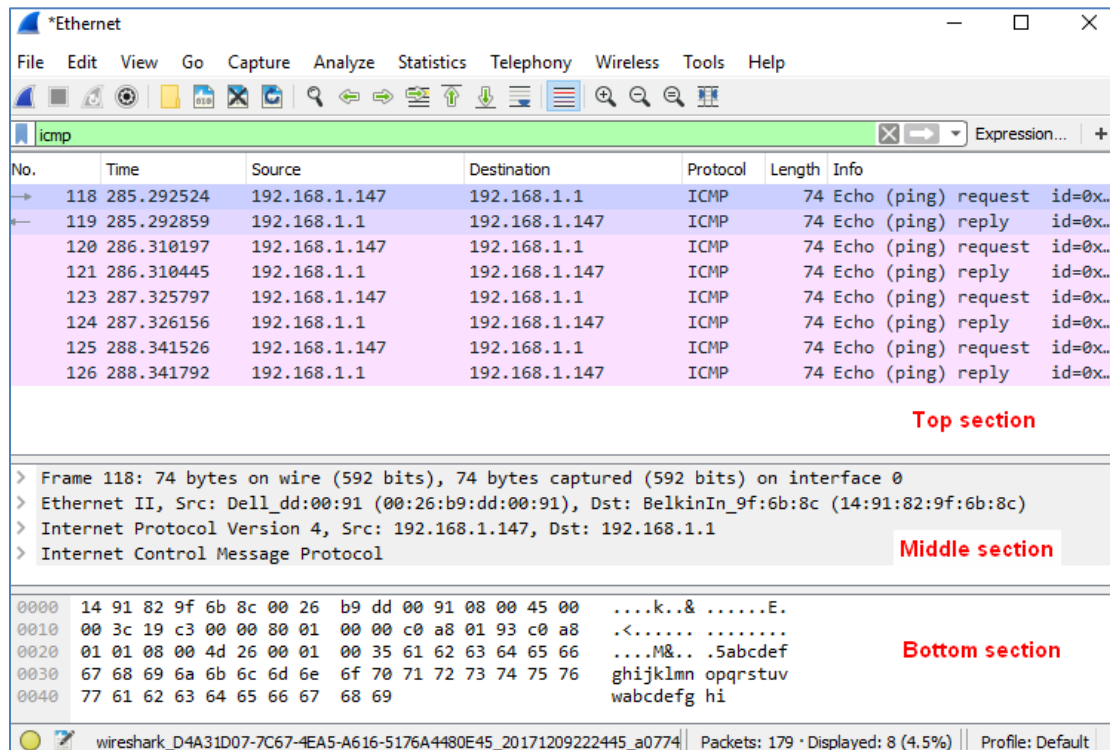


Step 6: Examine the first Echo (ping) request in Wireshark.

The Wireshark main window is divided into three sections: the packet list pane (top), the **Packet Details** pane (middle), and the **Packet Bytes** pane (bottom). If you selected the correct interface for packet capturing in

Lab – Using Wireshark to Examine Ethernet Frames

Step 3, Wireshark should display the ICMP information in the packet list pane of Wireshark, similar to the following example.



- In the packet list pane (top section), click the first frame listed. You should see **Echo (ping) request** under the **Info** heading. This should highlight the line blue.
- Examine the first line in the packet details pane (middle section). This line displays the length of the frame; 74 bytes in this example.

- The second line in the packet details pane shows that it is an Ethernet II frame. The source and destination MAC addresses are also displayed.

What is the MAC address of the PC NIC? _____ 00:26:b9:dd:00:91 in example

What is the default gateway's MAC address? _____ 14:91:82:9f:6b:8c in example

- You can click the plus (+) sign at the beginning of the second line to obtain more information about the Ethernet II frame. Notice that the plus sign changes to a minus (-) sign.

What type of frame is displayed? _____ 0x0800 or an IPv4 frame type.

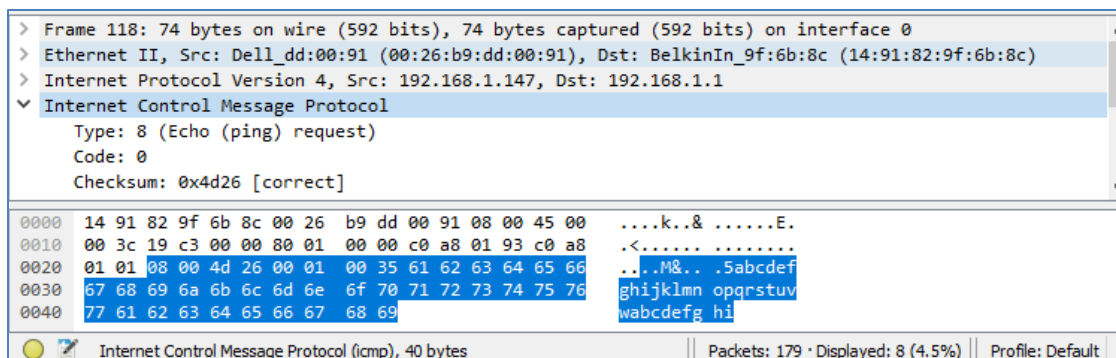
- The last two lines displayed in the middle section provide information about the data field of the frame. Notice that the data contains the source and destination IPv4 address information.

What is the source IP address? _____ 192.168.1.147 in the example

What is the destination IP address? _____ 192.168.1.1 in the example

Lab – Using Wireshark to Examine Ethernet Frames

- f. You can click any line in the middle section to highlight that part of the frame (hex and ASCII) in the **Packet Bytes** pane (bottom section). Click the **Internet Control Message Protocol** line in the middle section and examine what is highlighted in the **Packet Bytes** pane.



What do the last two highlighted octets spell? _____ hi

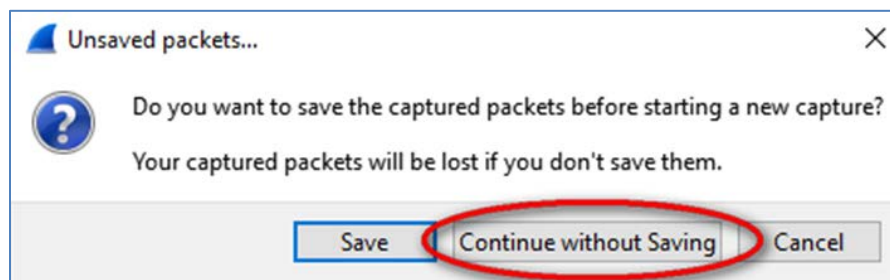
- g. Click the next frame in the top section and examine an Echo reply frame. Notice that the source and destination MAC addresses have reversed, because this frame was sent from the default gateway router as a reply to the first ping.

What device and MAC address is displayed as the destination address?

_____ The host PC, 00:26:b9:dd:00:91 in example.

Step 7: Restart packet capture in Wireshark.

Click the **Start Capture** icon to start a new Wireshark capture. You will receive a popup window asking if you would like to save the previous captured packets to a file before starting a new capture. Click **Continue without Saving**.



Step 8: In the command prompt window, ping www.cisco.com.

Step 9: Stop capturing packets.

Step 10: Examine the new data in the packet list pane of Wireshark.

In the first echo (ping) request frame, what are the source and destination MAC addresses?

Source: _____ This should be the MAC address of the PC.

Destination: _____ This should be the MAC address of the Default Gateway.

What are the source and destination IP addresses contained in the data field of the frame?

Source: _____ This is still the IP address of the PC.

Destination: _____ This is the address of the server at www.cisco.com, 23.13.155.188 in the example.

Compare these addresses to the addresses you received in Step 6. The only address that changed is the destination IP address. Why has the destination IP address changed, while the destination MAC address remained the same?

Layer 2 frames never leave the LAN. When a ping is issued to a remote host, the source will use the default gateway MAC address for the frame destination. The default gateway receives the packet, strips the Layer 2 frame information from the packet and then creates a new frame header with the MAC address of the next hop. This process continues from router to router until the packet reaches its destination IP address.

Reflection

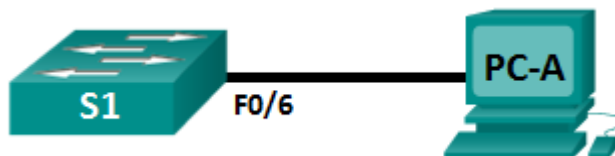
Wireshark does not display the preamble field of a frame header. What does the preamble contain?

The preamble field contains seven octets of alternating 1010 sequences, and one octet that signals the beginning of the frame, 10101011.

Lab – Viewing Network Device MAC Addresses (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Devices and Verify Connectivity

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Background / Scenario

Every device on an Ethernet LAN is identified by a Layer 2 MAC address. This address is assigned by the manufacturer and stored in the firmware of the NIC. This lab will explore and analyze the components that make up a MAC address, and how you can find this information on a switch and a PC.

You will cable the equipment as shown in the topology. You will configure the switch and PC to match the addressing table. You will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use various commands to retrieve information from the devices to answer questions about your network equipment.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure, ask your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with a terminal emulation program, such as Tera Term)
- Console cable to configure the Cisco switch via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Devices and Verify Connectivity

In this part, you will set up the network topology and configure basic settings, such as the interface IP addresses and device name. For device name and address information, refer to the Topology and Addressing Table.

Step 1: Cable the network as shown in the topology.

- Attach the devices shown in the topology and cable as necessary.
- Power on all the devices in the topology.

Step 2: Configure the IPv4 address for the PC.

- Configure the IPv4 address, subnet mask, and default gateway address for PC-A.
- From the command prompt on PC-A, ping the switch address.

Were the pings successful? Explain.

No. The switch has not been configured yet.

Step 3: Configure basic settings for the switch.

In this step, you will configure the device name and the IP address, and disable DNS lookup on the switch.

- Console into the switch and enter global configuration mode.

```
Switch> enable
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

- Assign a hostname to the switch based on the Addressing Table.

```
Switch(config)# hostname S1
```

- Disable DNS lookup.

```
S1(config)# no ip domain-lookup
```

- Configure and enable the SVI interface for VLAN 1.

```
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# end
*Mar  1 00:07:59.048: %SYS-5-CONFIG_I: Configured from console by console
```

Step 4: Verify network connectivity.

Ping the switch from PC-A. Were the pings successful? _____

The pings should be successful.

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Every device on an Ethernet LAN has a MAC address that is assigned by the manufacturer and stored in the firmware of the NIC. Ethernet MAC addresses are 48-bits long. They are displayed using six sets of

Lab – Viewing Network Device MAC Addresses

hexadecimal digits that are usually separated by dashes, colons, or periods. The following example shows the same MAC address using the three different notation methods:

00-05-9A-3C-78-00

00:05:9A:3C:78:00

0005.9A3C.7800

Note: MAC addresses are also called physical addresses, hardware addresses, or Ethernet hardware addresses.

You will issue commands to display the MAC addresses on a PC and a switch, and you will analyze the properties of each one.

Step 1: Analyze the MAC address for the PC-A NIC.

Before you analyze the MAC address on PC-A, look at an example from a different PC NIC. You can issue the **ipconfig /all** command to view the MAC address of your NIC. An example screen output is shown below. When using the **ipconfig /all** command, notice that MAC addresses are referred to as physical addresses. Reading the MAC address from left to right, the first six hex digits refer to the vendor (manufacturer) of this device. These first six hex digits (3 bytes) are also known as the organizationally unique identifier (OUI). This 3-byte code is assigned to the vendor by the IEEE organization. To find the manufacturer, you can use a tool like www.macvendorlookup.com or go to the IEEE web site to find the registered OUI vendor codes. The IEEE web site address for OUI information is <http://standards.ieee.org/develop/regauth/oui/public.html>. The last six digits are the NIC serial number assigned by the manufacturer.

- a. Using the output from the **ipconfig /all** command, answer the following questions.

```
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82577LM Gigabit Network Connection
Physical Address. . . . . : 5C-26-0A-24-2A-60
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b875:731b:3c7b:c0b1%10(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 240920024
```

What is the OUI portion of the MAC address for this device?

5C-26-0A

What is the serial number portion of the MAC address for this device?

24-2A-60

Using the example above, find the name of the vendor that manufactured this NIC.

Dell Inc.

- b. From the command prompt on PC-A, issue the **ipconfig /all** command and identify the OUI portion of the MAC address for the NIC of PC-A.

Answers will vary based on manufacturer.

Identify the serial number portion of the MAC address for the NIC of PC-A.

Answers will vary based on manufacturer serial number code.

Identify the name of the vendor that manufactured the NIC of PC-A.

Answers will vary based on manufacturer OUI.

Step 2: Analyze the MAC address for the S1 F0/6 interface.

You can use a variety of commands to display MAC addresses on the switch.

- Console into S1 and use the **show interfaces vlan 1** command to find the MAC address information. A sample is shown below. Use output generated by your switch to answer the questions.

```
S1# show interfaces vlan 1
Vlan1 is up, line protocol is up
  Hardware is EtherSVI, address is 001b.0c6d.8f40 (bia 001b.0c6d.8f40)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:14:51, 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 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    34 packets output, 11119 bytes, 0 underruns
    0 output errors, 2 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
```

What is the MAC address for VLAN 1 on S1?

Answers will vary based on the switch the student is using. Using the output from above, the answer would be 001b.0c6d.8f40.

What is the MAC serial number for VLAN 1?

Answers will vary based on the switch the student is using. Using the output from above, the answer would be 6d-8f-40.

What is the OUI for VLAN 1?

Answers will vary based on the switch the student is using. Using the output from above, the answer would be 00-1b-0c.

Lab – Viewing Network Device MAC Addresses

Based on this OUI, what is the name of the vendor?

Cisco Systems

What does bia stand for?

Burned in address.

Why does the output show the same MAC address twice?

The MAC address can be changed via a software command. The actual address (bia) will still be there. It is shown in the parenthesis.

- b. Another way to display the MAC address on the switch is to use the **show arp** command. Use the **show arp** command to display MAC address information. This command maps the Layer 2 address to its corresponding Layer 3 address. A sample is shown below. Use output generated by your switch to answer the questions.

S1# **show arp**

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	001b.0c6d.8f40	ARPA	Vlan1
Internet	192.168.1.3	0	5c26.0a24.2a60	ARPA	Vlan1

What Layer 2 addresses are displayed on S1?

S1 VLAN 1 and PC-A MAC addresses. If the student also records the MAC addresses, their answers will vary.

What Layer 3 addresses are displayed on S1?

S1 and PC-A IP addresses

Step 3: View the MAC addresses on the switch.

Issue the **show mac address-table** command on S1. A sample is shown below. Use output generated by your switch to answer the questions.

Instructor Note: The **show mac address-table** command can vary based on the model switch you are using. For example, the syntax on some switches is **show mac-address-table**.

S1# **show mac address-table**

Mac Address Table

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU

Lab – Viewing Network Device MAC Addresses

```
All    0180.c200.0004    STATIC    CPU
All    0180.c200.0005    STATIC    CPU
All    0180.c200.0006    STATIC    CPU
All    0180.c200.0007    STATIC    CPU
All    0180.c200.0008    STATIC    CPU
All    0180.c200.0009    STATIC    CPU
All    0180.c200.000a    STATIC    CPU
All    0180.c200.000b    STATIC    CPU
All    0180.c200.000c    STATIC    CPU
All    0180.c200.000d    STATIC    CPU
All    0180.c200.000e    STATIC    CPU
All    0180.c200.000f    STATIC    CPU
All    0180.c200.0010    STATIC    CPU
All    ffff.ffff.ffff    STATIC    CPU
1      5c26.0a24.2a60    DYNAMIC    Fa0/6
```

Total Mac Addresses for this criterion: 21

Did the switch display the MAC address of PC-A? If you answered yes, what port was it on?

Yes. Port should be F0/6. Answers will vary for the MAC address. In the example above, the MAC address would be 5c26.0a24.2a60.

Reflection

1. Can you have broadcasts at the Layer 2 level? If so, what would the MAC address be?

You can have broadcasts at Layer 2. ARP will use broadcasts to find MAC address information. The broadcast address is FF.FF.FF.FF.FF.FF.

2. Why would you need to know the MAC address of a device?

There could be a variety of reasons. In a large network, it may be easier to pinpoint location and identity of a device by its MAC address instead of its IP address. The MAC OUI will list the manufacturer, which may help narrow down the search. Security measures can be applied at Layer 2, so knowledge of allowable MAC addresses is needed.

Device Config

Switch S1

```
S1# show run
```

```
Building configuration...
```

```
Current configuration : 1335 bytes
```

```
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
```

Lab – Viewing Network Device MAC Addresses

```
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
system mtu routing 1500  
!  
no ip domain-lookup  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22
```

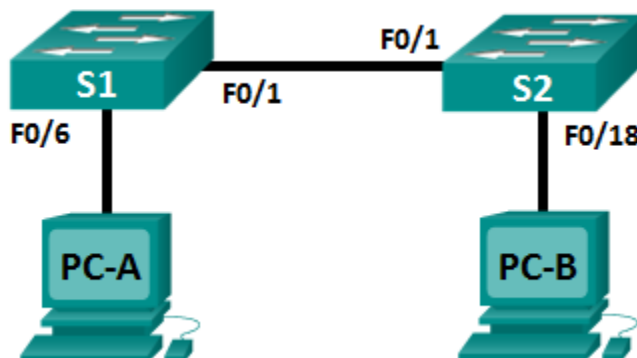
Lab – Viewing Network Device MAC Addresses

```
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.168.1.1 255.255.255.0  
!  
ip http server  
ip http secure-server  
logging esm config  
!  
line con 0  
line vty 5 15  
!  
end
```

Lab – Viewing the Switch MAC Address Table (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	N/A
PC-B	NIC	192.168.1.2	255.255.255.0	N/A

Objectives

Part 1: Build and Configure the Network

Part 2: Examine the Switch MAC Address Table

Background / Scenario

The purpose of a Layer 2 LAN switch is to deliver Ethernet frames to host devices on the local network. The switch records host MAC addresses that are visible on the network, and maps those MAC addresses to its own Ethernet switch ports. This process is called building the MAC address table. When a switch receives a frame from a PC, it examines the frame's source and destination MAC addresses. The source MAC address is recorded and mapped to the switch port from which it arrived. Then the destination MAC address is looked up in the MAC address table. If the destination MAC address is a known address, then the frame is forwarded out of the corresponding switch port associated with that MAC address. If the MAC address is unknown, then the frame is broadcasted out of all switch ports, except the one from which it came. It is important to observe and understand the function of a switch and how it delivers data on the network. The way a switch operates has implications for network administrators whose job it is to ensure secure and consistent network communication.

Switches are used to interconnect and deliver information to computers on local area networks. Switches deliver Ethernet frames to host devices identified by network interface card MAC addresses.

In Part 1, you will build a multi-switch topology with a trunk linking the two switches. In Part 2, you will ping various devices and observe how the two switches build their MAC address tables.

Note: The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the switches have been erased and have no startup configurations. If you are unsure contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Fast Ethernet interfaces on Cisco 2960 switches are autosensing and an Ethernet straight-through cable may be used between switches S1 and S2. If using another model Cisco switch, it may be necessary to use an Ethernet crossover cable.

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology.

Step 2: Configure PC hosts.

Step 3: Initialize and reload switches as necessary.

Step 4: Configure basic settings for each switch.

- Configure device name as shown in the topology.
- Configure IP address as listed in Addressing Table.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the privileged EXEC password.

Part 2: Examine the Switch MAC Address Table

A switch learns MAC addresses and builds the MAC address table, as network devices initiate communication on the network.

Step 1: Record network device MAC addresses.

- Open a command prompt on PC-A and PC-B and type **ipconfig /all**. What are the Ethernet adapter physical addresses?

PC-A MAC Address: _____

PC-B MAC Address: _____

Answers will vary.

- Console into switch S1 and S2 and type the **show interface F0/1** command on each switch. On the second line of command output, what is the hardware addresses (or burned-in address [bia])?

S1 Fast Ethernet 0/1 MAC Address: _____

S2 Fast Ethernet 0/1 MAC Address: _____

Answers will vary but from the example output below the S1 F0/1 MAC address is 0cd9.96d2.3d81 and the S2 F0/1 MAC address is 0cd9.96d2.4581.

```
S1# show interface f0/1
```

```
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96d2.3d81 (bia 0cd9.96d2.3d81)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
S1#
```

```
S2# show interface f0/1
```

```
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96d2.4581 (bia 0cd9.96d2.4581)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<output omitted>
S2#
```

Step 2: Display the switch MAC address table.

Console into switch S2 and view the MAC address table, both before and after running network communication tests with ping.

- Establish a console connection to S2 and enter privileged EXEC mode.
- In privileged EXEC mode, type the **show mac address-table** command and press Enter.

```
S2# show mac address-table
```

Even though there has been no network communication initiated across the network (i.e., no use of ping), it is possible that the switch has learned MAC addresses from its connection to the PC and the other switch.

Are there any MAC addresses recorded in the MAC address table?

The switch may have one or more MAC addresses in its table, based on whether or not the students entered a ping command when configuring the network. The switch will most likely have learned MAC addresses through S1's F0/1 switch port. The switch will record multiple MAC addresses of hosts learned through the connection to the other switch on F0/1.

```
S2# show mac address-table
```

```
Mac Address Table
```

```
-----
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
A11	0100.0ccc.cccc	STATIC	CPU
A11	0100.0ccc.cccd	STATIC	CPU
A11	0180.c200.0000	STATIC	CPU
A11	0180.c200.0001	STATIC	CPU
A11	0180.c200.0002	STATIC	CPU
A11	0180.c200.0003	STATIC	CPU
A11	0180.c200.0004	STATIC	CPU
A11	0180.c200.0005	STATIC	CPU


```
All 0180.c200.0006 STATIC CPU
All 0180.c200.0007 STATIC CPU
All 0180.c200.0008 STATIC CPU
All 0180.c200.0009 STATIC CPU
All 0180.c200.000a STATIC CPU
All 0180.c200.000b STATIC CPU
All 0180.c200.000c STATIC CPU
All 0180.c200.000d STATIC CPU
All 0180.c200.000e STATIC CPU
All 0180.c200.000f STATIC CPU
All 0180.c200.0010 STATIC CPU
All ffff.ffff.ffff STATIC CPU
  1 0cd9.96d2.3d81 DYNAMIC Fa0/1
  1 1cc1.de91.c35d DYNAMIC Fa0/1
Total Mac Addresses for this criterion: 22
S2#
```

What MAC addresses are recorded in the table? To which switch ports are they mapped and to which devices do they belong? Ignore MAC addresses that are mapped to the CPU.

There may be multiple MAC addresses recorded in the MAC address table, especially MAC addresses learned through S1's F0/1 switch port. In the example output above, the S1 F0/1 MAC address and PC-A MAC address are mapped to S2 F0/1.

If you had not previously recorded MAC addresses of network devices in Step 1, how could you tell which devices the MAC addresses belong to, using only the output from the **show mac address-table** command? Does it work in all scenarios?

The output of the **show mac address-table** command shows the port that the MAC address was learned on. In most cases this would identify which network device the MAC address belongs to, except in the case of multiple MAC addresses associated to the same port. This happens when switches are connected to other switches and record all of the MAC addresses for devices connected to the other switch.

Step 3: Clear the S2 MAC address table and display the MAC address table again.

- In privileged EXEC mode, type the **clear mac address-table dynamic** command and press **Enter**.

```
S2# clear mac address-table dynamic
```

- Quickly type the **show mac address-table** command again. Does the MAC address table have any addresses in it for VLAN 1? Are there other MAC addresses listed?

No. The student will most likely discover that the MAC address for the other switch's F0/1 switch port has been quickly reinserted in the MAC address table.

```
S2# show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
All     0100.0ccc.cccc   STATIC  CPU
All     0100.0ccc.cccd   STATIC  CPU
All     0180.c200.0000   STATIC  CPU
All     0180.c200.0001   STATIC  CPU
All     0180.c200.0002   STATIC  CPU
All     0180.c200.0003   STATIC  CPU
All     0180.c200.0004   STATIC  CPU
All     0180.c200.0005   STATIC  CPU
All     0180.c200.0006   STATIC  CPU
All     0180.c200.0007   STATIC  CPU
All     0180.c200.0008   STATIC  CPU
All     0180.c200.0009   STATIC  CPU
All     0180.c200.000a   STATIC  CPU
All     0180.c200.000b   STATIC  CPU
All     0180.c200.000c   STATIC  CPU
All     0180.c200.000d   STATIC  CPU
All     0180.c200.000e   STATIC  CPU
All     0180.c200.000f   STATIC  CPU
All     0180.c200.0010   STATIC  CPU
All     ffff.ffff.ffff   STATIC  CPU
1       0cd9.96d2.3d81   DYNAMIC Fa0/1
Total Mac Addresses for this criterion: 21
S2#
```

Wait 10 seconds, type the **show mac address-table** command, and press Enter. Are there new addresses in the MAC address table? _____ Answers will vary. There may be.

Step 4: From PC-B, ping the devices on the network and observe the switch MAC address table.

- a. From PC-B, open a command prompt and type **arp -a**. Not including multicast or broadcast addresses, how many device IP-to-MAC address pairs have been learned by ARP?

Answers will vary. The ARP cache may have no entries in it, or it may have the gateway IP address to MAC address mapping.

```
C:\Users\PC-B> arp -a
Interface: 192.168.1.2 --- 0xb
   Internet Address      Physical Address      Type
   192.168.1.1           30-f7-0d-a3-17-c1    dynamic
C:\Users\PC-B>
```

- b. From the PC-B command prompt, ping PC-A, S1, and S2. Did all devices have successful replies? If not, check your cabling and IP configurations.
-

If the network was cabled and configured correctly the answer should be yes.

- c. From a console connection to S2, enter the **show mac address-table** command. Has the switch added additional MAC addresses to the MAC address table? If so, which addresses and devices?

There may only be one additional MAC address mapping added to the table, most likely the MAC address of PC-A.

```
S2# show mac address-table
```

```
Mac Address Table
```

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU
All	ffff.ffff.ffff	STATIC	CPU
1	0021.700c.050c	DYNAMIC	Fa0/18
1	0cd9.96d2.3d81	DYNAMIC	Fa0/1
1	0cd9.96d2.3dc0	DYNAMIC	Fa0/1
1	1cc1.de91.c35d	DYNAMIC	Fa0/1

```
Total Mac Addresses for this criterion: 24
```

```
S2#
```

From PC-B, open a command prompt and retype **arp -a**. Does the PC-B ARP cache have additional entries for all network devices that were sent pings?

Answers may vary, but the ARP cache on PC-B should have more entries.

```
C:\Users\PC-B> arp -a
```

```
Interface: 192.168.1.2 --- 0xb
```

Internet Address	Physical Address	Type
192.168.1.3	1c-c1-de-91-c3-5d	dynamic
192.168.1.11	0c-d9-96-d2-3d-c0	dynamic
192.168.1.12	0c-d9-96-d2-45-c0	dynamic

C:\Users\PC-B>

Reflection

On Ethernet networks, data is delivered to devices by their MAC addresses. For this to happen, switches and PCs dynamically build ARP caches and MAC address tables. With only a few computers on the network this process seems fairly easy. What might be some of the challenges on larger networks?

ARP broadcasts could cause broadcast storms. Because ARP and switch MAC tables do not authenticate or validate the IP addresses to MAC addresses it would be easy to spoof a device on the network.

Device Configs

Switch S1

```
S1#show running-config
Building configuration...

version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

```
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.168.1.11 255.255.255.0
```

```
!  
ip default-gateway 192.168.1.1  
ip http server  
ip http secure-server  
!  
line con 0  
line vty 0 4  
password cisco  
login  
line vty 5 15  
login  
!  
end
```

Switch S2

```
S2#show running-config  
Building configuration...  
  
version 12.2  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname S2  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
system mtu routing 1500  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!
```

```
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.12 255.255.255.0
!
 ip default-gateway 192.168.1.1
 ip http server
 ip http secure-server
!
```

Lab - Using IOS CLI with Switch MAC Address Tables

```
line con 0
line vty 0 4
  password cisco
  login
line vty 5 15
  login
!
end
```


Class Activity - MAC and Choose... (Instructor Version – Optional Class Activity))

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Describe basic switching concepts.

Background / Scenario

Note: This activity is best completed in groups of 2-3 students.

Please view the video titled “The History of Ethernet”, and located at the following link:

<http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet>

Topics discussed in the video include not only where we have come from in Ethernet development, but where we are going with Ethernet technology in the future!

After viewing the video, go to the web and search for information about Ethernet.

Collect three pictures of old, current, and possible future Ethernet physical media and devices. Focus your search on switches if possible. Share these pictures with the class and discuss.

Use the questions in the Reflection section to guide your search.

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of how Ethernet has developed to today's standards, including its use in LANs and WANs for the transmission of frames. Facilitation of the discussion should include student-to-student discussions of each other's work.

Required Resources

- Internet access to the video titled “History of Ethernet”, and located at <http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet>
- Hard or soft-copy media to record answers to questions and to share in class.

Reflection

1. How was Ethernet used when it was first developed?

Students may mention that Ethernet was first developed to be used with printers (video information).

2. How has Ethernet stayed the same over the past 25 years? What changes are being made to make it more useful/applicable to today's data transmission methods?

Ethernet still uses copper cabling and wireless transmission, while the speed and distance of the transmissions are being developed to meet current and future data transmission methods.

3. How have Ethernet physical media and intermediary devices changed?

The speed and distance of data communications have increased exponentially. Intermediary devices have been designed to use different types of cabling endpoints to support the increase in speed and distance.

4. How have Ethernet physical media and intermediary devices stayed the same?
-

Switches still handle most Ethernet transmissions, whether they are Layer 2 or Layer 3. However, the framing is the same except for minor modifications to the frames' introductory sections, which indicate what type of frame is being transmitted, etc.

5. How do you think the Ethernet will change in the future? What factors could influence these changes?
-

Device connections and speed/distance developments will change how networks will access other networks, but the underlying technology of Ethernet and the framing of Ethernet transmissions will probably stay the same. Wireless is an example of this. It is legacy and current/futuristic.

Reality

Identify elements of the model that map to IT-related content:

- Ethernet is a technology-based idea with cabling, speed. Methods of signaling are all involved in deciding which method of Ethernet to use in a network.
- Switches use Ethernet technology at both the LAN and WAN sides of a network.
- Even though Ethernet is legacy in its inception, it is still fully current in application on today's networks, especially in framing formats with slight modifications.

Class Activity - The Road Less Traveled...Or Is It? (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain how network devices use routing tables to direct packets to a destination network.

Background /Scenario

During the upcoming weekend, you decide to visit a schoolmate who is currently at home sick. You know his street address but you have never been to his town before.

Instead of looking up the address on the map, you decide to take it easy and to simply ask town residents for directions after you arrive by train.

The citizens you ask for directions are very helpful. However, they all have an interesting habit. Instead of explaining the entire route to your destination, they all tell you, "Take this road and as soon as you arrive at the nearest crossroad, ask somebody there again."

Somewhat bemused at this apparent oddity, you follow these instructions and finally arrive, crossroad by crossroad, and road by road, at your friend's house.

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of how a network uses pathways to send and receive data communications. Facilitation of the discussion should be initiated as a result of this activity.

Reflection

1. Would it have made a significant difference if you were told about the whole route or a larger part of the route instead of just being directed to the nearest crossroad?

It would not really make a difference. The key fact to remember here is that to reach any part of the route behind the nearest crossroad, we must first reach that crossroad. If residents at each crossroad can be assumed to know their town well, it is not really helpful to ask about what is beyond the first crossroad as we must still reach it, and on each crossroad, we will be directed appropriately. Please make the students aware, however, that congestion can also affect whether an route is better than another to use.

2. Would it have been more helpful to ask about the specific street address or just about the street name?

Asking about the street name, omitting the house number, is sufficient. Once we get to the destination street, we can easily look up the house ourselves. People at crossroads will be able to direct us even without telling them the exact house number. They do not need to know each and every house in every street – it is sufficient they know the streets themselves.

3. What would happen if the person you asked for directions did not know where the destination street was or directed you through an incorrect road?
-
-

The Road Less Traveled...Or Is It?

In that case, we would be in risk of getting either misrouted and following a longer route to the destination than necessary, or we may even end up going in circles or getting lost.

4. Assuming that on your way back home, you again choose to ask residents for directions. Is it guaranteed that you will be directed via the same route you took to get to your friend's home? Explain your answer.

There is no such guarantee. Each person at a crossroad makes an individual and independent choice about the best path. It is quite possible that if the residents do not have the same knowledge or ideas about the routes within their town, you would be going back to the train station via a different route.

5. Is it necessary to explain where you depart from when asking directions to an intended destination?

Describing where you departed from is not helpful when choosing path towards a destination. It is only the destination itself that matters when selecting the best route towards it.

Identify elements of the model that map to IT-related content:

- Crossroads – Correspond to stops along the way (routers)
- Roads – Correspond to interface links between routers
- Street – Corresponds to a network
- Irrelevancy of house number when asking for the path to the destination street – Corresponds to routers knowing about networks, not about individual hosts
- Asking about the path to destination at each crossroad – Corresponds to path selection performed on each router
- Train station, friend's house – Corresponds to source and destination
- Relevancy of only the destination when asking for a path – Corresponds to destination-based routing
- Different possible paths to and from the friend – Correspond to independent routing to and from a destination

Lab - Exploring Router Physical Characteristics (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Examine Router External Characteristics

Part 2: Examine Router Internal Characteristics Using Show Commands

Background / Scenario

In this lab, you will examine the outside of the router to become familiar with its characteristics and components, such as its power switch, management ports, LAN and WAN interfaces, indicator lights, network expansion slots, memory expansion slots, and USB ports.

You will also identify the internal components and characteristics of the IOS by consoling into the router and issuing various commands, such as **show version** and **show interfaces**, from the CLI.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Instructor Note: Depending on equipment availability, the instructor may wish to use the lab as a guided lecture/demonstration to point out the router characteristics and discuss them with the class.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

Part 1: Examine Router External Characteristics

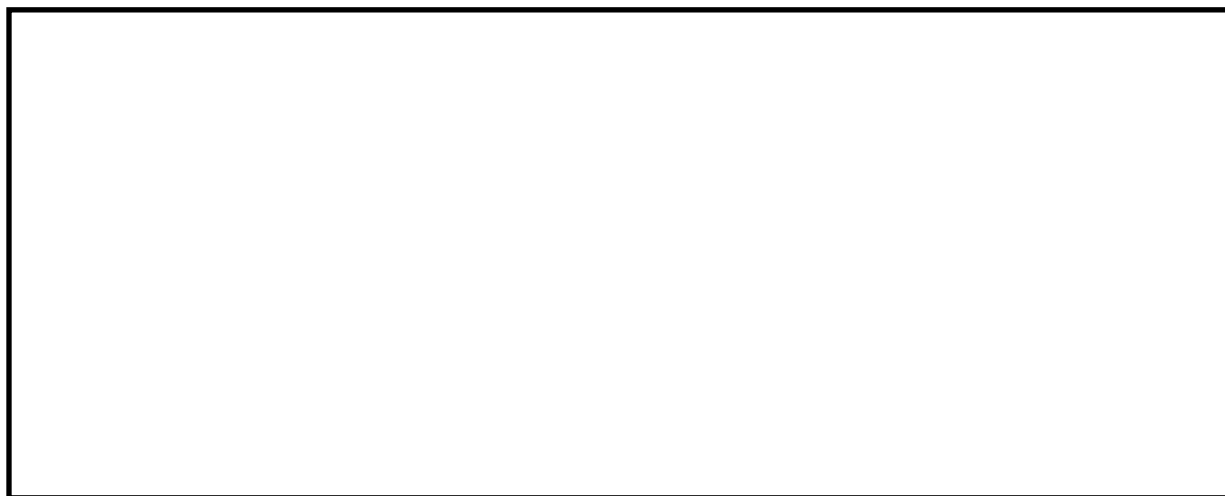
Use the images below, as well as your own direct inspection of the backplane of a Cisco router, to answer the following questions. Feel free to draw arrows and circle the areas of the image that correctly identify the parts.

Note: The router depicted in the images below is a Cisco 1941 router, which may be different from the make and model of the routers in your particular academy. You can find device information and specifications for the Cisco 1941 series routers at the Cisco.com website. Additional information, including answers to many of the questions below can be found here:

http://www.cisco.com/en/US/prod/collateral/routers/ps10538/data_sheet_c78_556319.html

Step 1: Identify the various parts of a Cisco router.

The image shown in this step is of the backplane of a Cisco 1941 ISR. Use it to answer the questions in this step. In addition, if you are examining a different model router, a space has been provided here for you to draw the backplane and identify components and interfaces as specified in the questions that follow.



- a. Circle and label the router's power switch. Is the power switch on your router in the same area as the router depicted in the image?

Answers may vary depending on the academy's lab routers. Students should draw a line around the on/off switch in the image

- b. Circle and label the management ports. What are the built-in management ports? Are the management ports the same on your router? If not, how are they different?

Answers may vary depending on the academy's lab routers. Students should draw a circle around the console port, auxiliary port, and mini USB console port in the image.

- c. Circle and label the router's LAN interfaces. How many LAN interfaces does the router in the image have and what is the interface technology type? Are the LAN interfaces the same on your router? If not, how are they different?
-

Lab - Exploring Router Physical Characteristics

Answers may vary depending on the academy's lab routers. Students should draw a circle around the Gigabit Ethernet 0/0 and 0/1 interfaces in the image.

- d. Circle and label the router's WAN interfaces. How many WAN interfaces does the router in the image have and what is the interface technology type? Are the WAN interfaces the same on your router? If not, how are they different?

Answers may vary depending on the academy's lab routers. Students should draw a circle around the Serial 0 and Serial 1 interfaces in the image.

- e. The Cisco 1941 ISR is a modular platform and comes with module expansion slots for varied network connectivity requirements. Circle and label the module slots. How many module slots are there? How many are used? What type of module expansion slots are they? Are the module slots the same on your router? If not, how are they different?

Answers may vary depending on the academy's lab routers. The image depicts a Cisco 1941 ISR with two module expansion slots for Enhanced High-Speed WAN interface cards, EHWIC 0 and EHWIC 1. EHWIC 0 is occupied by a Smart Serial WAN interface card. EHWIC1 will accept a double wide expansion card. The EHWIC slot replaces the high-speed WAN interface card (HWIC) slot and can natively support HWICs, WAN interface cards (WICs), voice interface cards (VICs), and voice/WAN interface cards (VWICs).

- f. The Cisco 1941 router comes with CompactFlash memory slots for high speed storage. Circle and label the CompactFlash memory slots. How many memory slots are there? How many are used? How much memory can they hold? Are the memory slots the same on your router? If not, how are they different?

Answers may vary depending on the academy's lab routers. The image depicts a Cisco 1941 ISR with two CompactFlash memory slots, CF0 and CF1. CF0 is occupied by a 256 MB CompactFlash memory card used to store the Cisco IOS system image file.

- g. The Cisco 1941 router comes with USB 2.0 ports. The built-in USB ports support eToken devices and USB flash memory. The USB eToken device feature provides device authentication and secure configuration of Cisco routers. The USB flash feature provides optional secondary storage capability and an additional boot device. Circle and label the USB ports. How many USB ports are there? Are there USB ports on your router?

Answers may vary depending on the academy's lab routers. The image depicts a Cisco 1941 ISR with two USB 2.0 ports.

- h. The Cisco 1941 router also comes with a mini-B USB console port. Circle and label the mini-B USB console port.

Answers may vary depending on the academy's lab routers. The image depicts a Cisco 1941 ISR with a mini USB console port next to the regular console port.

Step 2: Examine the router activity and status lights.

The following images highlight the activity and status lights of the front panel and backplane of a powered up and connected Cisco 1941 ISR.

Note: Some of the indicator lights are obscured from view in the image of the backplane of the Cisco 1941 router below.



- a. In the top image above, examine the indicator lights on the front panel of the router? The lights are labeled SYS, ACT, and POE. What do the labels refer to? What do the lights in the image indicate about the status of the router? These labels would be readable if they were not lit.

The SYS, ACT, and POE lights refer to: system status, network activity, and power over Ethernet. The lights in the image show that the router's system is successfully powered on, that there is network activity, and that Power over Ethernet is not activated.

- b. In the backplane image above, examine the indicator lights on the router. There are three visible activity lights, one for each of the connected interfaces and management ports. Examine the interface lights on your router. How are the lights labeled, and what is their meaning?

The lights in the image show that the serial and Gigabit Ethernet interfaces are active and that the Console management port is enabled and active. The Gigabit Ethernet interfaces have two lights each, one labeled S for sending and the other labeled L for link. The console port and mini USB console port have an EN label for enabled. The serial interfaces each have a light labeled Conn for connected.

- c. Aside from the management ports and network interfaces, what other indicator lights are on the backplane of the router and what might their purpose be?

The backplane of the router also show CF0 and CF1 lights for the CompactFlash memory slots as well as an ISM/WLAN light which would indicate the presence of either a Cisco Internal Services Module or wireless LAN card.

Part 2: Examine Router Internal Characteristics Using Show Commands

Step 1: Establish a console connection to the router and use the show version command.

- a. Using Tera Term, console into the router and enter privileged EXEC mode using the **enable** command:

```
Router> enable
```

```
Router#
```

- b. Display information about the router by using the **show version** command. Use the Spacebar on the keyboard to page through the output.

```
Router# show version
```

```
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2011 by Cisco Systems, Inc.
```

```
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
Router uptime is 1 day, 14 hours, 46 minutes
```

```
System returned to ROM by power-on
```

```
System restarted at 07:26:55 UTC Mon Dec 3 2012
```

```
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"
```

```
Last reload type: Normal Reload
```

```
Last reload reason: power-on
```

```
<output omitted>
```

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

```
Cisco CISC01941/K9 (revision 1.0) with 487424K/36864K bytes of memory.
```

```
Processor board ID FGL16082318
```

```
2 Gigabit Ethernet interfaces
```

```
2 Serial(sync/async) interfaces
```

```
1 terminal line
```

```
1 Virtual Private Network (VPN) Module
```

```
DRAM configuration is 64 bits wide with parity disabled.
```

```
255K bytes of non-volatile configuration memory.
```

Lab - Exploring Router Physical Characteristics

```
250880K bytes of ATA System CompactFlash 0 (Read/Write)
<output omitted>
```

```
Technology Package License Information for Module:'c1900'
```

Technology	Technology-package		Technology-package Next reboot
	Current	Type	
ipbase	ipbasek9	Permanent	ipbasek9
security	securityk9	Permanent	securityk9
data	None	None	None

```
Configuration register is 0x2102
```

- c. Based on the output of the **show version** command, answer the following questions about the router. If you are examining a different model router, include the information about it here.

- 1) What is the version of the Cisco IOS and what is the system image filename?

```
IOS version 15.2(4)M3, c1900-universalk9-mz.SPA.152-4.M3.bin
```

- 2) What is the Bootstrap program version in ROM BIOS?

```
System Bootstrap version 15.0(1r)M15
```

- 3) How long has the router been running without a restart (also known as its uptime)?

```
1 day, 14 hours, 46 minutes
```

- 4) How much dynamic random-access memory (DRAM) memory does the router have?

```
487424K/36864K = 512MB total
```

- 5) What is the router's processor board ID number?

```
The processor board ID number is FGL16082318
```

- 6) What network interfaces does the router have?

```
2 Gigabit Ethernet interfaces and 2 Serial interfaces
```

- 7) How much CompactFlash memory for IOS storage is there?

```
250880K of CompactFlash memory
```

- 8) How much nonvolatile random-access memory (NVRAM) memory for configuration file storage is there?

```
255K of NVRAM
```

- 9) What is the setting of the configuration register?

0x2102

Step 2: Use the show interface command to examine the network interfaces.

- a. Use the **show interface gigabitEthernet 0/0** command to see the status of the Gigabit Ethernet 0/0 interface.

Note: After typing part of the command, for example, **show interface g**, you can use the **Tab** key on your keyboard to complete the gigabitEthernet command parameter.

```
Router# show interface gigabitEthernet 0/0
GigabitEthernet0/0 is administratively down, line protocol is down
  Hardware is CN Gigabit Ethernet, address is 442b.031a.b9a0 (bia 442b.031a.b9a0)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input 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
    3 packets input, 276 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    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
```

- b. Given the output of the **show interface gigabitEthernet 0/0** command depicted above, or using the output from your router, answer the following questions:

What is the hardware type and MAC address of the Gigabit Ethernet interface?

The hardware type is CN Gigabit Ethernet and the burned in address (bia) or MAC address is 442b.031a.b9a0

What is the interface media type? Is the interface up or down?

According to the output the interface media type is RJ45 and the Gigabit Ethernet interface is administratively down and the line protocol is down.

- c. Use the **show interfaces serial 0/0/0** command to view the status of the Serial 0/0/0 interface.

```
Router# show interface serial 0/0/0
Serial0/0/0 is administratively down, line protocol is down
  Hardware is WIC MBRD Serial
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input 07:41:21, 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
    1 packets input, 24 bytes, 0 no buffer
    Received 1 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 unknown protocol drops
    0 output buffer failures, 0 output buffers swapped out
    1 carrier transitions
  DCD=down DSR=down DTR=down RTS=down CTS=down
```

- d. Given the output command depicted above, answer the following questions:

What is the frame encapsulation type?

According to the output above, the frame encapsulation type is HDLC.

What is the hardware type? Is the interface up or down?

The hardware type is WIC MBRD Serial and the interface is administratively down and line protocol down.

Reflection

1. Why might you need to use an EHWIC expansion slot?

Answers will vary. You may need to have a WAN connection to your ISP over a WAN interface technology that does not come with the router by default.

2. Why might you need to upgrade the Flash memory?

Answers will vary. You may want to store an additional IOS image file or upgrade to a larger IOS image.

3. What is the purpose of the mini-USB port?

The purpose of the mini USB port is to give you the ability to console into the router if you do not have a COM serial port on your laptop or computer.

4. What is the purpose of the ISM/WLAN indicator light on the backplane of the router? What does it refer to?

The Cisco 1941 router can support a Cisco Internal Services Module that can enhance the intelligence and abilities of the router to perform activities like intrusion prevention scanning. The Cisco 1941 router can also be equipped with a Wireless LAN card for supporting wireless local area networks.

Class Activity - Can You Read This Map? (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Explain how network devices use routing tables to direct packets to a destination network.

Background /Scenario

Note: It is suggested that students work in pairs; however, if preferred, students can complete this activity individually.

Your instructor will provide you with output generated by a router's show ip route command. Use Packet Tracer to build a topology model using this routing information.

At a minimum, the following should be used in your topology model:

- 1 Catalyst 2960 switch
- 1 Cisco Series 1941 Router with one HWIC-4ESW switching port modular card and IOS version 15.1 or higher
- 3 PCs (can be servers, generic PCs, laptops, etc.)

Use the note tool in Packet Tracer to indicate the addresses of the router interfaces and possible addresses for the end devices you chose for your model.

Label all end devices, ports, and addresses ascertained from the show ip route output/routing table information in your Packet Tracer file. Save your work in hard or soft copy to share with the class.

Instructor Note: This Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of how a network is configured and then checked for routing table information.

Print out or project the Table 1 graphic found in the Required Resources section of this document. Students should be able to assist each other as they read the routing table provided and then construct the model using Packet Tracer software. Facilitation of small group discussion should be initiated as a result of this activity.

Instructor Note: It is suggested, but not required, that students work in pairs for this activity.

Required Resources

- Packet Tracer software program.
- Routing **Table 1** – students can use the table to assist each other as they read the information provided and then construct the model using Packet Tracer.

Table 1

```
R1# show ip route
Codes: L - local, C - connected, S - static, 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
i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
+ - replicated route, % - next hop override

Gateway of last resort is not set

192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.0.0/24 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/1
L 192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

Reflection

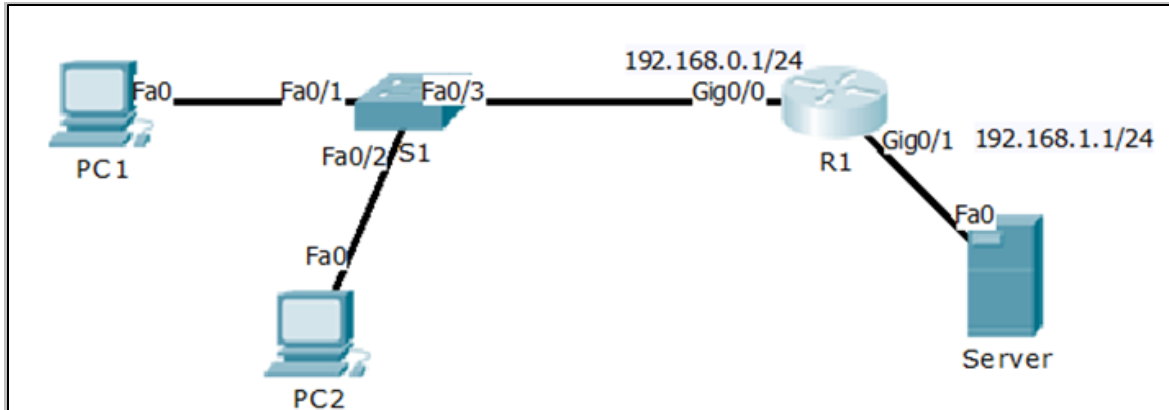
What was the hardest part of designing this network model? Explain your answer.

Answers will vary within groups – some students may mention source or destination identifiers or some may mention the actual IP addresses being cited in the routing table – the important concept here is that students can comfortably identify where information is coming from on the final routing table as depicted.

Topologies will vary by group – some students will place their switch off of the Gig0/1 port, etc.

Optional: As an **advanced modeling activity**, students can create a simple one-router network with four Gigabit interfaces connected to end devices, configure the router and LANs with passwords, IP addresses, banners, etc., and then produce a routing table to support the network information.

Possible topology built by the students could look like this:



Identify elements of the model that map to IT-related content:

- Reading a routing table can verify how a network has been addressed logically.
- A routing table can assist with identifying the physical topology of the network.
- A routing table identifies to the reader which ports are operating and on which networks they are operating

Lab - Building a Switch and Router Network (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.0.3	255.255.255.0	192.168.0.1

Objectives

Part 1: Set Up the Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Display Device Information

Background / Scenario

This is a comprehensive lab to review previously covered IOS commands. In this lab, you will cable the equipment as shown in the topology diagram. You will then configure the devices to match the addressing table. After the configurations have been saved, you will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use IOS commands to retrieve information from the devices to answer questions about your network equipment.

This lab provides minimal assistance with the actual commands necessary to configure the router. Test your knowledge by trying to configure the devices without referring to the content or previous activities.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Ensure that the routers and switches have been erased and have no startup configurations. Consult with your instructor for the procedure to initialize and reload a router and switch.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)

- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

Part 1: Set Up Topology and Initialize Devices

Step 1: Cable the network as shown in the topology.

- a. Attach the devices shown in the topology diagram, and cable, as necessary.
- b. Power on all the devices in the topology.

Step 2: Initialize and reload the router and switch.

If configuration files were previously saved on the router and switch, initialize and reload these devices back to their basic configurations.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords. Refer to the Topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Assign static IP information to the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.
- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.
- c. Ping PC-B from a command prompt window on PC-A.

Why were the pings not successful?

The router interfaces (default gateways) have not been configured yet so Layer 3 traffic is not being routed between subnets.

Step 2: Configure the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Assign a device name to the router.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Assign **class** as the privileged EXEC encrypted password.

- f. Assign **cisco** as the console password and enable login.
- g. Assign **cisco** as the VTY password and enable login.
- h. Encrypt the clear text passwords.
- i. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- j. Configure and activate both interfaces on the router.
- k. Configure an interface description for each interface indicating which device is connected to it.
- l. Save the running configuration to the startup configuration file.
- m. Set the clock on the router.

Note: Use the question mark (?) to help with the correct sequence of parameters needed to execute this command.

- n. Ping PC-B from a command prompt window on PC-A.

Were the pings successful? Why?

Yes. The router is routing the ping traffic across the two subnets. The default settings for the 2960 switch will automatically turn up the interfaces that are connected to devices.

Part 3: Display Device Information

In Part 3, you will use **show** commands to retrieve information from the router and switch.

Step 1: Retrieve hardware and software information from the network devices.

- a. Use the **show version** command to answer the following questions about the router.

```
R1# show version
```

```
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4)M3, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Thu 26-Jul-12 19:34 by prod_rel_team
```

```
ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)
```

```
R1 uptime is 10 minutes
```

```
System returned to ROM by power-on
```

```
System image file is "flash0:c1900-universalk9-mz.SPA.152-4.M3.bin"
```

```
Last reload type: Normal Reload
```

```
Last reload reason: power-on
```

```
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 CISC01941/K9 (revision 1.0) with 446464K/77824K bytes of memory.
Processor board ID FTX1636848Z
2 Gigabit Ethernet interfaces
2 Serial(sync/async) interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
250880K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

```
-----  
Device#          PID          SN  
-----  
*0              CISC01941/K9      FTX1636848Z
```

Technology Package License Information for Module:'c1900'

```
-----  
Technology      Technology-package      Technology-package  
                Current      Type      Next reboot  
-----  
ipbase          ipbasek9      Permanent  ipbasek9  
security        None          None       None  
data            None          None       None
```

Configuration register is 0x2142 (will be 0x2102 at next reload)

What is the name of the IOS image that the router is running?

Image version may vary, but answers should be something like c1900-universalk9-mz.SPA.152-4.M3.bin.

How much DRAM memory does the router have?

Answers may vary, but the default DRAM memory configuration on a 1941 router is 512MB or 524,288K bytes. The total can be calculated by adding the two DRAM numbers together from the output of the show version command: Cisco CISC01941/K9 (revision 1.0) with 446464K/77824K bytes of memory.

How much NVRAM memory does the router have?

Answers may vary, but the output from the show version on 1941 router is: 255K bytes of non-volatile configuration memory.

How much Flash memory does the router have?

Answers may vary, but the default output from the show version command on the 1941 router is 250880K bytes of ATA System CompactFlash 0 (Read/Write).

- b. Use the **show version** command to answer the following questions about the switch.

```
Switch# show version
```

```
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(2)SE, RELEASE SOFTWARE (fc1)
```

```
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2012 by Cisco Systems, Inc.
```

```
Compiled Sat 28-Jul-12 00:29 by prod_rel_team
```

```
ROM: Bootstrap program is C2960 boot loader
```

```
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(53r)SEY3, RELEASE SOFTWARE (fc1)
```

```
S1 uptime is 1 hour, 2 minutes
```

```
System returned to ROM by power-on
```

```
System image file is "flash:/c2960-lanbasek9-mz.150-2.SE.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 WS-C2960-24TT-L (PowerPC405) processor (revision R0) with 65536K bytes of memory.
```

```
Processor board ID FCQ1628Y5LE
```

```
Last reset from power-on
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       : 0C:D9:96:E2:3D:00
Motherboard assembly number     : 73-12600-06
Power supply part number        : 341-0097-03
Motherboard serial number       : FCQ16270N5G
Power supply serial number      : DCA1616884D
Model revision number           : R0
Motherboard revision number     : A0
Model number                    : WS-C2960-24TT-L
System serial number            : FCQ1628Y5LE
Top Assembly Part Number        : 800-32797-02
Top Assembly Revision Number    : A0
Version ID                      : V11
CLEI Code Number               : COM3L00BRF
Hardware Board Revision Number  : 0x0A
```

Switch	Ports	Model	SW Version	SW Image
-----	-----	-----	-----	-----
*	1 26	WS-C2960-24TT-L	15.0(2)SE	C2960-LANBASEK9-M

Configuration register is 0xF

Switch#

What is the name of the IOS image that the switch is running?

Image version may vary, but answers should be something like c2960-lanbasek9-mz.150-2.SE.bin.

How much dynamic random access memory (DRAM) does the switch have?

Answers may vary, but the default DRAM memory configuration on a 2960-24TT-L switch is 65536K of memory.

How much nonvolatile random-access memory (NVRAM) does the switch have?

Answers may vary, but the default non-volatile memory configuration on a 2960-24TT-L switch is 64K bytes.

What is the model number of the switch?

Answers may vary, but the answer should appear in this form: WS-C2960-24TT-L.

Step 2: Display the routing table on the router.

Use the **show ip route** command on the router to answer the following questions.

```
R1# show ip route
```

```
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.0.0/24 is directly connected, GigabitEthernet0/0
L       192.168.0.1/32 is directly connected, GigabitEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, GigabitEthernet0/1
L       192.168.1.1/32 is directly connected, GigabitEthernet0/1
```

What code is used in the routing table to indicate a directly connected network? _____

The C designates a directly connected subnet. An L designates a local interface. Both answers are correct.

How many route entries are coded with a C code in the routing table? _____ 2

What interface types are associated to the C coded routes?

Answers may vary depending of router type, but on the 1941 the correct answer is G0/0 and G0/1.

Step 3: Display interface information on the router.

Use the **show interface g0/1** to answer the following questions.

```
R1# show interfaces g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
  Hardware is CN Gigabit Ethernet, address is fc99.4775.c3e1 (bia fc99.4775.c3e1)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 100Mbps, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:06, output 00:00:04, 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
 17 packets input, 5409 bytes, 0 no buffer
Received 17 broadcasts (0 IP multicasts)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 13 multicast, 0 pause input
14 packets output, 1743 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
3 unknown protocol drops
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
```

What is the operational status of the G0/1 interface?

GigabitEthernet0/1 is up, line protocol is up

What is the Media Access Control (MAC) address of the G0/1 interface?

Answers will vary but will appear in the form of: xxxx.xxxx.xxxx, where each x will be replaced with a hexadecimal number.

How is the Internet address displayed in this command?

Internet address is 192.168.1.1/24.

Step 4: Display a summary list of the interfaces on the router and switch.

There are several commands that can be used to verify an interface configuration. One of the most useful of these is the **show ip interface brief** command. The command output displays a summary list of the interfaces on the device and provides immediate feedback to the status of each interface.

- a. Enter the **show ip interface brief** command on the router.

```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Embedded-Service-Engine0/0 unassigned      YES unset  administratively down down
GigabitEthernet0/0       192.168.0.1     YES manual  up              up
GigabitEthernet0/1       192.168.1.1     YES manual  up              up
Serial0/0/0              unassigned      YES unset  administratively down down
Serial0/0/1              unassigned      YES unset  administratively down down
R1#
```

- b. Enter the **show ip interface brief** command on the switch.

```
Switch# show ip interface brief
Interface                IP-Address      OK? Method Status          Protocol
Vlan1                   unassigned      YES manual  up              up
FastEthernet0/1         unassigned      YES unset  down            down
FastEthernet0/2         unassigned      YES unset  down            down
FastEthernet0/3         unassigned      YES unset  down            down
FastEthernet0/4         unassigned      YES unset  down            down
```


FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

Switch#

Reflection

1. If the G0/1 interface showed administratively down, what interface configuration command would you use to turn the interface up?

R1(config-if)# **no shut**

2. What would happen if you had incorrectly configured interface G0/1 on the router with an IP address of 192.168.1.2?

PC-A would not be able to ping PC-B. This is because PC-B is on a different network than PC-A which requires the default-gateway router to route these packets. PC-A is configured to use the IP address of 192.168.1.1 for the default-gateway router, but this address is not assigned to any device on the LAN. Any packets that need to be sent to the default-gateway for routing will never reach their destination.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the router type and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs

Router R1

```
R1# show run
Building configuration...

Current configuration : 1360 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
```

Lab - Building a Switch and Router Network

```
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description Connection to PC-B.
ip address 192.168.0.1 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
description Connection to S1.
ip address 192.168.1.1 255.255.255.0 duplex auto
speed auto
!
interface Serial0/0/0
no ip address
shutdown
clock rate 2000000
!
interface Serial0/0/1
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
banner motd ^C
Unauthorized access prohibited!
^C
!
line con 0
password 7 13061E010803
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
```

Lab - Building a Switch and Router Network

```
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 070C285F4D06
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Class Activity - The Internet of Everything (IoE) (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain how network devices use routing tables to direct packets to a destination network.

Background /Scenario

Today, more than 99% of our world remains unconnected. Tomorrow, we will be connected to almost everything. 37 billion devices will be connected to the Internet by 2020. From trees to water to cars, the organic and the digital will work together for a more intelligent and connected world. This tomorrow of networking is known as “The Internet of Everything” or “IoE.”

If traffic, transportation, networking and space exploration depend on digital information sharing, how will that information be identified from its source to its destination?

In this activity, you will begin to think about not only what will be identified in the IoE world, but how everything will be addressed in the same world!

Activity directions for class or individual students:

- 1) Navigate to the IoE main page located at <http://www.cisco.com/c/r/en/us/internet-of-everything-ioe>.
- 2) Next, watch some videos or read through some content from the IoE main page that interests you.
- 3) Write 5 comments or questions about what you saw or read. Be prepared to share with the class.

Instructor Note: This is an individual or an in-class Modeling Activity (MA). It is not intended to be a graded assignment. Its purpose is to encourage student reflection about their perception of networks and how they will be identified in the future. IPv6 is necessary to support the Internet of Everything.

Required Resources

- Internet connectivity for research on the cisco.com site. Headphones may also be useful if students are individually completing this activity within a group setting.
- Recording capabilities (paper, tablet, etc.) for comments or questions regarding the videos, blogs and/or .pdfs read or viewed for Step 3.

Reflection

Why do you think there is a need to address trees? Windmills? Cars? Refrigerators? Why will just about anything be able to use an IP address?

The research for the scenario will be varied. Some concepts worth mentioning or discussing include:

- To support the new IoE concepts/implementation and growing number of devices that connect to the internet, an exponential amount of addresses will be needed. Might need to briefly discuss HOW trees can be connected to the Internet (i.e., different kinds of sensors which transmit data – see http://www.ericsson.com/article/connected_tree_2045546582_c)
- Knowing how to use IPv6 addressing will be important to network administrators, ISPs/TSPs, and the general public as we move to more and more network types/classifications of networks.

Identify elements of the model that map to IT-related content:

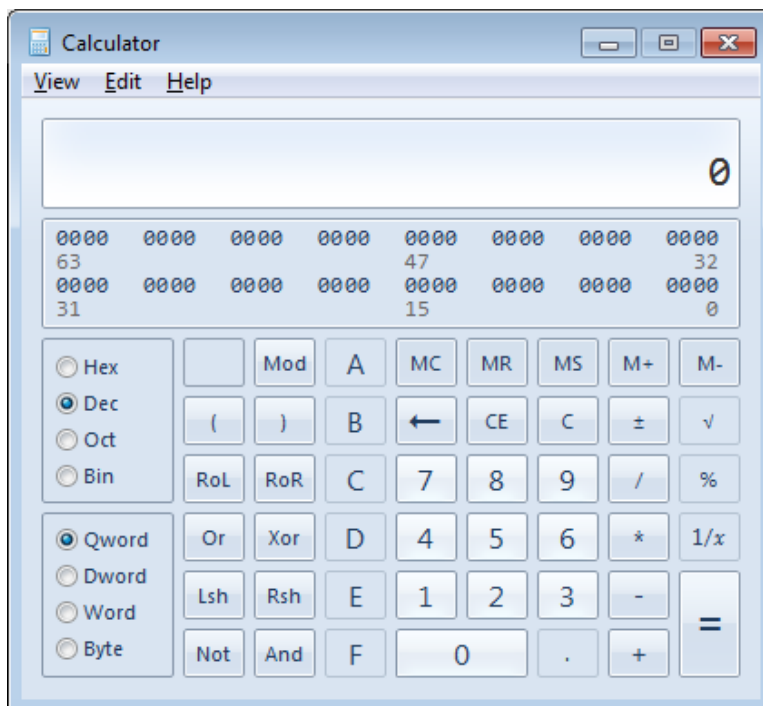
- Network types (subnets, etc.)

Class Activity - The Internet of Everything

- Network and host identification as related to network types
- Quality of network transmission as related to network identification

Lab – Using the Windows Calculator with Network Addresses (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.



Objectives

Part 1: Access the Windows Calculator

Part 2: Convert between Numbering Systems

Part 3: Convert Host IPv4 Addresses and Subnet Masks into Binary

Part 4: Determine the Number of Hosts in a Network Using Powers of 2

Part 5: Convert MAC Addresses and IPv6 Addresses to Binary

Background / Scenario

Network technicians use binary, decimal, and hexadecimal numbers when working with computers and networking devices. Microsoft provides a built-in Calculator application as part of the operating system. The Windows 7 version of Calculator includes a Standard view that can be used to perform basic arithmetic tasks such as addition, subtract, multiplication, and division. The Calculator application also has advanced programming, scientific, and statistical capabilities.

In this lab, you will use the Windows 7 Calculator application Programmer view to convert between the binary, decimal, and hexadecimal number systems. You will also use the Scientific view powers function to determine the number of hosts that can be addressed based on the number of host bits available.

Required Resources

- 1 PC (Windows 7 or 8)

Note: If using an operating system other than Windows 7, the Calculator application views and functions available may vary from those shown in this lab. However, you should be able to perform the calculations.

Part 1: Access the Windows Calculator

In Part 1, you will become familiar with the Microsoft Windows built-in calculator application and view the available modes.

Step 1: Click the Windows Start button and select All Programs.

Step 2: Click the Accessories folder and select Calculator.

Step 3: After Calculator opens, click the View menu.

What are the four available modes?

Standard, Scientific, Programmer, and Statistics

Note: The Programmer and Scientific modes are used in this lab.

Part 2: Convert between Numbering Systems

In the Windows Calculator Programmer view, several number system modes are available: Hex (Hexadecimal or base 16), Dec (Decimal or base 10), Oct (Octal or base 8), and Bin (Binary or base 2).

We are accustomed to using the decimal number system that uses the digits 0 to 9. The decimal numbering system is used in everyday life for all counting, money, and financial transactions. Computers and other electronic devices use the binary numbering system with only the digits 0 and 1 for data storage, data transmission and numerical calculations. All computer calculations are ultimately performed internally in binary (digital) form, regardless of how they are displayed.

One disadvantage of binary numbers is that the binary number equivalent of a large decimal number can be quite long. This makes them difficult to read and write. One way to overcome this problem is to arrange binary numbers into groups of four as hexadecimal numbers. Hexadecimal numbers are base 16, and a combination of numbers from 0 to 9 and the letters A to F are used to represent the binary or decimal equivalent. Hexadecimal characters are used when writing or displaying IPv6 and MAC addresses.

The octal numbering system is very similar in principle to hexadecimal. Octal numbers represent binary numbers in groups of three. This numbering system uses digits 0 to 7. Octal numbers are also a convenient way to represent a large binary number in smaller groups, but this numbering system is not commonly used.

In this lab, the Windows 7 Calculator is used to convert between different numbering systems in the Programmer mode.

a. Click the **View** menu and select **Programmer** to switch to Programmer mode.

Note: For Windows XP and Vista, only two modes, Standard and Scientific, are available. If you are using one of these operating systems, you can use the Scientific mode to perform this lab.

Which number system is currently active? _____ Dec

Which numbers on the number pad are active in decimal mode? _____ 0 thru 9

b. Click the **Bin** (Binary) radio button. Which numbers are active on the number pad now?

_____ 0 and 1

Why do you think the other numbers are grayed out?

Lab – Using the Windows Calculator with Network Addresses

The only digits used in binary (base 2) are 0 and 1.

- c. Click the **Hex** (Hexadecimal) radio button. Which characters are activated on the number pad now?

0 thru 9 and A, B, C, D, E, and F. Hexadecimal (base 16) has 16 possible values.

- d. Click the **Dec** radio button. Using your mouse, click the number **1** followed by the number **5** on the number pad. The decimal number 15 is now entered.

Note: The numbers and letters on the keyboard can also be used to enter the values. If using the numerical keypad, type the number **15**. If the number does not enter into the calculator, press the **Num Lock** key to enable the numeric keypad.

Click the **Bin** radio button. What happened to the number 15?

It was converted to a binary number 1111. This binary number 1111 represents the decimal number 15.

- e. Numbers are converted from one numbering system to another by selecting the desired number mode. Click the **Dec** radio button again. The number converts back to decimal.
- f. Click the **Hex** radio button to change to Hexadecimal mode. Which hexadecimal character (0 through 9 or A to F) represents decimal 15? **F**
- g. As you were switching between the numbering systems, you may have noticed the binary number 1111 is displayed during the conversion. This assists you in relating the binary digits to other numbering system values. Each set of 4 bits represents a hexadecimal character or potentially multiple decimal characters.

15							
0000	0000	0000	0000	0000	0000	0000	0000
63				47			32
0000	0000	0000	0000	0000	0000	0000	1111
31				15			0

- h. Clear the values in the window by clicking **C** above the 9 on the calculator keypad. Convert the following numbers between the binary, decimal, and hexadecimal numbering systems.

Decimal	Binary	Hexadecimal
86	0101 0110	56
175	1010 1111	AF
204	1100 1100	CC
19	0001 0011	13
77	0100 1101	4D
42	0010 1010	2A
56	0011 1000	38
147	1001 0011	93
228	1110 0100	E4

- i. As you record the values in the table above, do you see a pattern between the binary and hexadecimal numbers?

Every hexadecimal digit can be converted into four binary numbers separately. For example, hex 0A is 1010 in binary.

Part 3: Convert Host IPv4 Addresses and Subnet Masks into Binary

Internet Protocol version 4 (IPv4) addresses and subnet masks are represented in a dotted decimal format (four octets), such as 192.168.1.10 and 255.255.255.0, respectively. This makes these addresses more readable to humans. Each of the decimal octets in the address or a mask can be converted to 8 binary bits. An octet is always 8 binary bits. If all 4 octets were converted to binary, how many bits would there be?

32

- a. Use the Windows Calculator application to convert the IP address 192.168.1.10 into binary and record the binary numbers in the following table:

Decimal	Binary
192	1100 0000
168	1010 1000
1	0000 0001
10	0000 1010

- b. Subnet masks, such as 255.255.255.0, are also represented in a dotted decimal format. A subnet mask will always consist of four 8-bit octets, each represented as a decimal number. Using the Windows Calculator, convert the 8 possible decimal subnet mask octet values to binary numbers and record the binary numbers in the following table:

Decimal	Binary
0	0000 0000
128	1000 0000
192	1100 0000
224	1110 0000
240	1111 0000
248	1111 1000
252	1111 1100
254	1111 1110
255	1111 1111

- c. With the combination of IPv4 address and the subnet mask, the network portion can be determined and the number of hosts available in a given IPv4 subnet can also be calculated. The process is examined in Part 4.

Part 4: Determine the Number of Hosts in a Network Using Powers of 2

Given an IPv4 network address and a subnet mask, the network portion can be determined along with the number of hosts available in the network.

- a. To calculate the number of hosts on a network, you must determine the network and host portion of the address.

Using the example of 192.168.1.10 with a subnet of 255.255.248.0, the address and subnet mask are converted to binary numbers. Align the bits as you record your conversions to binary numbers.

Decimal IP Address and Subnet Mask	Binary IP Address and Subnet Mask
192.168.1.10	11000000.10101000.00000001.00001010
255.255.248.0	11111111.11111111.11111000.00000000

Because the first 21 bits in the subnet mask are consecutive numeral ones, the corresponding first 21 bits in the IP address in binary is 11000000101010000000; these represent the network portion of the address. The remaining 11 bits are 00100001010 and represent the host portion of the address.

What is the decimal and binary network number for this address?

Decimal: 192.168.0.0 Binary: 11000000.10101000.00000000.00000000

What is the decimal and binary host portion for this address?

Decimal: 1.10 Binary: 00000000.00000000.00000001.00001010

Because the network number and the broadcast address use two addresses out of the subnet, the formula to determine the number of hosts available in an IPv4 subnet is the number 2 to the power of the number of host bits available, minus 2:

$$\text{Number of available hosts} = 2^{(\text{number of host bits})} - 2$$

- b. Using the Windows Calculator application, switch to the Scientific mode by clicking the **View** menu, then select **Scientific**.
- c. Input **2**. Click the x^y key. This key raises a number to a power.
- d. Input **11**. Click **=**, or press Enter on the keyboard for the answer.
- e. Subtract **2** from the answer by using the calculator if desired.
- f. In this example, there are 2046 hosts are available on this network ($2^{11}-2$).
- g. If given the number of host bits, determine the number of hosts available and record the number in the following table.

Number of Available Host Bits	Number of Available Hosts
5	30
14	16382
24	16777214
10	1022

- h. For a given subnet mask, determine the number of hosts available and record the answer in the following table.

Subnet Mask	Binary Subnet Mask	Number of Available Host Bits	Number of Available Hosts
255.255.255.0	11111111.11111111.11111111.00000000	8	254
255.255.240.0	11111111.11111111.11110000.00000000	12	4094
255.255.255.128	11111111.11111111.11111111.10000000	7	126
255.255.255.252	11111111.11111111.11111111.11111100	2	2
255.255.0.0	11111111.11111111.00000000.00000000	16	65534

Part 5: Convert MAC Addresses and IPv6 Addresses to Binary

Both Media Access Control (MAC) and Internet Protocol version 6 (IPv6) addresses are represented as hexadecimal digits for readability. However, computers only understand binary digits and use these binary digits for computations. In this part, you will convert these hexadecimal addresses to binary addresses.

Step 1: Convert MAC addresses to binary digits.

- a. The MAC or physical address is normally represented as 12 hexadecimal characters, grouped in pairs and separated by hyphens (-). Physical addresses on a Windows-based computer are displayed in a format of xx-xx-xx-xx-xx-xx, where each x is a number from 0 to 9 or a letter from A to F. Each of the hex characters in the address can be converted to 4 binary bits, which is what the computer understands. If all 12 hex characters were converted to binary, how many bits would there be?

MAC address is 48 bits, 12 hexadecimal characters and 4 bits per character

- b. Record the MAC address for your PC.
-

Lab – Using the Windows Calculator with Network Addresses

Answers will vary depending on PC. Example: CC-12-DE-4A-BD-88

- c. Convert the MAC address into binary digits using the Windows Calculator application.

Answers will vary. For example: CC (11001100), 12 (0001 0010), DE (1101 1110) 4A (0100 1010), BD (1011 1101), 88 (1000 1000)

Step 2: Convert an IPv6 address into binary digits.

IPv6 addresses are also written in hexadecimal characters for human convenience. These IPv6 addresses can be converted to binary numbers for computer use.

- a. IPv6 addresses are binary numbers represented in human-readable notations:
2001:0DB8:ACAD:0001:0000:0000:0000:0001 or in a shorter format: 2001:DB8:ACAD:1::1.
- b. An IPv6 address is 128 bits long. Using the Windows Calculator application, convert the sample IPv6 address into binary numbers and record it in the table below.

Hexadecimal	Binary
2001	0010 0000 0000 0001
0DB8	0000 1101 1011 1000
ACAD	1010 1100 1010 1101
0001	0000 0000 0000 0001
0000	0000 0000 0000 0000
0000	0000 0000 0000 0000
0000	0000 0000 0000 0000
0001	0000 0000 0000 0001

Reflection

1. Can you perform all the conversions without the assistance of the calculator? What can you do to make it happen?

Lots of practice. For example, a binary game found on Cisco Learning Network at <https://learningnetwork.cisco.com/> can help with conversion between binary and decimal numbering systems.

2. For most IPv6 addresses, the network portion of the address is usually 64 bits. How many hosts are available on a subnet where the first 64 bits represent the network? Hint: All host addresses are available in the subnet for hosts.

There are 64 bits left for host addresses which is over 18.4 trillion ($2^{64} - 2$) hosts available in a 64-bit (/64) subnet.

Lab – Converting IPv4 Addresses to Binary (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

Part 2: Use Bitwise ANDing Operation to Determine Network Addresses

Part 3: Apply Network Address Calculations

Background / Scenario

Every IPv4 address is comprised of two parts: a network portion and a host portion. The network portion of an address is the same for all devices that reside in the same network. The host portion identifies a specific host within a given network. The subnet mask is used to determine the network portion of an IP address. Devices on the same network can communicate directly; devices on different networks require an intermediary Layer 3 device, such as a router, to communicate.

To understand the operation of devices on a network, we need to look at addresses the way devices do—in binary notation. To do this, we must convert the dotted decimal form of an IP address and its subnet mask to binary notation. After this has been done, we can use the bitwise ANDing operation to determine the network address.

This lab provides instructions on how to determine the network and host portion of IP addresses by converting addresses and subnet masks from dotted decimal to binary, and then using the bitwise ANDing operation. You will then apply this information to identify addresses in the network.

Part 1: Convert IPv4 Addresses from Dotted Decimal to Binary

In Part 1, you will convert decimal numbers to their binary equivalent. After you have mastered this activity, you will convert IPv4 addresses and subnet masks from dotted decimal to their binary form.

Step 1: Convert decimal numbers to their binary equivalent.

Fill in the following table by converting the decimal number to an 8-bit binary number. The first number has been completed for your reference. Recall that the eight binary bit values in an octet are based on the powers of 2, and from left to right are 128, 64, 32, 16, 8, 4, 2, and 1.

Decimal	Binary
192	11000000
168	10101000
10	00001010
255	11111111
2	00000010

Step 2: Convert the IPv4 addresses to their binary equivalent.

An IPv4 address can be converted using the same technique you used above. Fill in the table below with the binary equivalent of the addresses provided. To make your answers easier to read, separate the binary octets with a period.

Decimal	Binary
192.168.10.10	11000000.10101000.00001010.00001010
209.165.200.229	11010001.10100101.11001000.11100101
172.16.18.183	10101100.00010000.00010010.10110111
10.86.252.17	00001010.01010110.11111100.00010001
255.255.255.128	11111111.11111111.11111111.10000000
255.255.192.0	11111111.11111111.11000000.00000000

Part 2: Use Bitwise ANDing Operation to Determine Network Addresses

In Part 2, you will use the bitwise ANDing operation to calculate the network address for the provided host addresses. You will first need to convert an IPv4 decimal address and subnet mask to their binary equivalent. Once you have the binary form of the network address, convert it to its decimal form.

Note: The ANDing process compares the binary value in each bit position of the 32-bit host IP with the corresponding position in the 32-bit subnet mask. If there two 0s or a 0 and a 1, the ANDing result is 0. If there are two 1s, the result is a 1, as shown in the example here.

Step 1: Determine the number of bits to use to calculate the network address.

Description	Decimal	Binary
IP Address	192.168.10.131	11000000.10101000.00001010.10000011
Subnet Mask	255.255.255.192	11111111.11111111.11111111.11000000
Network Address	192.168.10.128	11000000.10101000.00001010.10000000

How do you determine what bits to use to calculate the network address?

The bits that are set to 1 in the binary subnet mask are used to calculate the network address.

In the example above, how many bits are used to calculate the network address?

_____ 26 bits

Step 2: Use the ANDing operation to determine the network address.

- a. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	172.16.145.29	10101100.00010000.10010001.00011101
Subnet Mask	255.255.0.0	11111111.11111111.00000000.00000000
Network Address	172.16.0.0	10101100.00010000.00000000.00000000

- b. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	192.168.10.10	11000000.10101000.00001010.00001010
Subnet Mask	255.255.255.0	11111111.11111111.11111111.00000000
Network Address	192.168.10.0	11000000.10101000.00001010.00000000

- c. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	192.168.68.210	11000000.10101000.01000100.11010010
Subnet Mask	255.255.255.128	11111111.11111111.11111111.10000000
Network Address	192.168.68.128	11000000.10101000.01000100.10000000

- d. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	172.16.188.15	10101100.00010000.10111100.00001111
Subnet Mask	255.255.240.0	11111111.11111111.11110000.00000000
Network Address	172.16.176.0	10101100.00010000.10110000.00000000

- e. Enter the missing information into the table below:

Description	Decimal	Binary
IP Address	10.172.2.8	00001010.10101100.00000010.00001000
Subnet Mask	255.224.0.0	11111111.11100000.00000000.00000000
Network Address	10.160.0.0	00001010.10100000.00000000.00000000

Part 3: Apply Network Address Calculations

In Part 3, you must calculate the network address for the given IP addresses and subnet masks. After you have the network address, you should be able to determine the responses needed to complete the lab.

Step 1: Determine whether IP addresses are on same network.

- a. You are configuring two PCs for your network. PC-A is given an IP address of 192.168.1.18, and PC-B is given an IP address of 192.168.1.33. Both PCs receive a subnet mask of 255.255.255.240.

What is the network address for PC-A? _____ 192.168.1.16

What is the network address for PC-B? _____ 192.168.1.32

Will these PCs be able to communicate directly with each other? _____ No

What is the highest address that can be given to PC-B that allows it to be on the same network as PC-A?
_____ 192.168.1.30

- b. You are configuring two PCs for your network. PC-A is given an IP address of 10.0.0.16, and PC-B is given an IP address of 10.1.14.68. Both PCs receive a subnet mask of 255.254.0.0.

Lab – Converting IPv4 Addresses to Binary

What is the network address for PC-A? _____ 10.0.0.0

What is the network address for PC-B? _____ 10.0.0.0

Will these PCs be able to communicate directly with each other? _____ Yes

What is the lowest address that can be given to PC-B that allows it to be on the same network as PC-A?
_____ 10.0.0.1

Step 2: Identify the default gateway address.

- a. Your company has a policy to use the first IP address in a network as the default gateway address. A host on the local-area network (LAN) has an IP address of 172.16.140.24 and a subnet mask of 255.255.192.0.

What is the network address for this network?

_____ 172.16.128.0

What is the default gateway address for this host?

_____ 172.16.128.1

- b. Your company has a policy to use the first IP address in a network as the default gateway address. You have been instructed to configure a new server with an IP address of 192.168.184.227 and a subnet mask of 255.255.255.248.

What is the network address for this network?

_____ 192.168.184.224

What is the default gateway for this server?

_____ 192.168.184.225

Reflection

Why is the subnet mask important in determining the network address?

The subnet mask provides the number of bits to use for the network portion of an address. The network address cannot be determined without it.

Lab– Identifying IPv4 Addresses (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Identify IPv4 Addresses

Part 2: Classify IPv4 Addresses

Background / Scenario

In this lab, you will examine the structure of Internet Protocol version 4 (IPv4) addresses. You will identify the various types of IPv4 addresses and the components that help comprise the address, such as network portion, host portion, and subnet mask. Types of addresses covered include public, private, unicast, and multicast.

Instructor Note: This optional activity can be done individually in class or assigned as homework. The lab can also be done in class with students working in pairs. If the lab is done in class, it should be followed up by discussion with correct answers. All public IP addresses used in this lab are owned by Cisco.

Required Resources

- Device with Internet access
- Optional: IPv4 address calculator

Part 1: Identify IPv4 Addresses

In Part 1, you will be given several examples of IPv4 addresses and will complete tables with appropriate information.

Step 1: Analyze the table shown below and identify the network portion and host portion of the given IPv4 addresses.

The first two rows show examples of how the table should be completed.

Key for table:

N = all 8 bits for an octet are in the network portion of the address

n = a bit in the network portion of the address

H = all 8 bits for an octet are in the host portion of the address

h = a bit in the host portion of the address

IP Address/Prefix	Network/Host N,n = Network, H,h = Host	Subnet Mask	Network Address
192.168.10.10/24	N.N.N.H	255.255.255.0	192.168.10.0
10.101.99.17/23	N.N.nnnnnnnh.H	255.255.254.0	10.101.98.0
209.165.200.227/27	N.N.N.nnnhhhhh	255.255.255.224	209.165.200.224
172.31.45.252/24	N.N.N.H	255.255.255.0	172.31.45.0
10.1.8.200/26	N.N.N.nnhhhhhh	255.255.255.192	10.1.8.192
172.16.117.77/20	N.N.nnnnhhhh.H	255.255.240.0	172.16.112.0
10.1.1.101/25	N.N.N.nhhhhhhh	255.255.255.128	10.1.1.0
209.165.202.140/27	N.N.N.nnnhhhhh	255.255.255.224	209.165.202.128
192.168.28.45/28	N.N.N.nnnhhhhh	255.255.255.240	192.168.28.32

Step 2: Analyze the table below and list the range of host and broadcast addresses given a network/prefix mask pair.

The first row shows an example of how the table should be completed.

IP Address/Prefix	First Host Address	Last Host Address	Broadcast Address
192.168.10.10/24	192.168.10.1	192.168.10.254	192.168.10.255
10.101.99.17/23	10.101.98.1	10.101.99.254	10.101.99.255
209.165.200.227/27	209.165.200.225	209.165.200.254	209.165.200.255
172.31.45.252/24	172.31.45.1	172.31.45.254	172.31.45.255
10.1.8.200/26	10.1.8.193	10.1.8.254	10.1.8.255
172.16.117.77/20	172.16.112.1	172.16.127.254	172.16.127.255
10.1.1.101/25	10.1.1.1	10.1.1.126	10.1.1.127
209.165.202.140/27	209.165.202.129	209.165.202.158	209.165.202.159
192.168.28.45/28	192.168.28.33	192.168.28.46	192.168.28.47

Part 2: Classify IPv4 Addresses

In Part 2, you will identify and classify several examples of IPv4 addresses.

Step 1: Analyze the table shown below and identify the type of address (network, host, multicast, or broadcast address).

The first row shows an example of how the table should be completed.

IP Address	Subnet Mask	Address Type
10.1.1.1	255.255.255.252	host
192.168.33.63	255.255.255.192	broadcast
239.192.1.100	255.252.0.0	multicast
172.25.12.52	255.255.255.0	host
10.255.0.0	255.0.0.0	host
172.16.128.48	255.255.255.240	network
209.165.202.159	255.255.255.224	broadcast
172.16.0.255	255.255.0.0	host
224.10.1.11	255.255.255.0	multicast

Step 2: Analyze the table shown below and identify the address as public or private.

IP Address/Prefix	Public or Private
209.165.201.30/27	Public
192.168.255.253/24	Private
10.100.11.103/16	Private
172.30.1.100/28	Private
192.31.7.11/24	Public
172.20.18.150/22	Private
128.107.10.1/16	Public
192.135.250.10/24	Public
64.104.0.11/16	Public

Step 3: Analyze the table shown below and identify whether the address/prefix pair is a valid host address.

IP Address/Prefix	Valid Host Address?	Reason
127.1.0.10/24	No	Loopback
172.16.255.0/16	Yes	Host address
241.19.10.100/24	No	Reserved
192.168.0.254/24	Yes	Host address
192.31.7.255/24	No	Broadcast
64.102.255.255/14	Yes	Host address
224.0.0.5/16	No	Multicast
10.0.255.255/8	Yes	Host address
198.133.219.8/24	Yes	Host address

Reflection

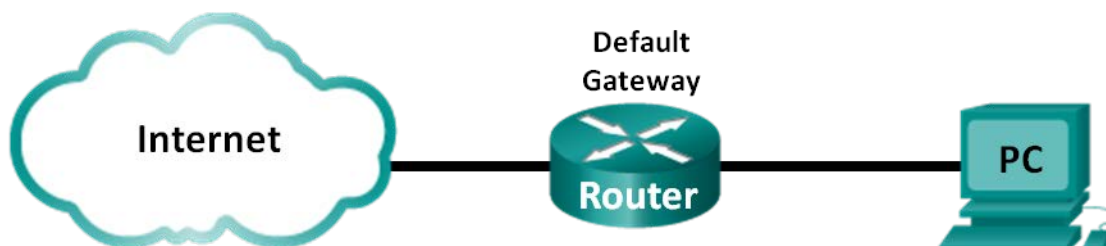
Why should we continue to study and learn about IPv4 addressing if the available IPv4 address space is depleted?

Many organizations will continue to use the private IPv4 address space for their internal networking needs. The public IPv4 addresses will be used for many years to come.

Lab – Identifying IPv6 Addresses (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Objectives

Part 1: Identify the Different Types of IPv6 Addresses

Part 2: Examine a Host IPv6 Network Interface and Address

Part 3: Practice IPv6 Address Abbreviation

Background / Scenario

With the depletion of the Internet Protocol version 4 (IPv4) network address space and the adoption and transition to IPv6, networking professionals must understand how both IPv4 and IPv6 networks function. Many devices and applications already support IPv6. This includes extensive Cisco device Internetwork Operating System (IOS) support and workstation/server operating system support, such as that found in Windows and Linux.

This lab focuses on IPv6 addresses and the components of the address. In Part 1, you will identify the IPv6 address types, and in Part 2, you will view the IPv6 settings on a PC. In Part 3, you will practice IPv6 address abbreviation.

Instructor Note: This optional lab has three sections that can be split up into two parts (Part 1/2 and Part 3). It can be performed in multiple sessions, or assigned as homework.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)

Part 1: Identify the Different Types of IPv6 Addresses

In Part 1, you will review the characteristics of IPv6 addresses to identify the different types of IPv6 addresses.

Step 1: Review the different types of IPv6 addresses.

An IPv6 address is 128 bits long. It is most often presented as 32 hexadecimal characters. Each hexadecimal character is the equivalent of 4 bits ($4 \times 32 = 128$). A non-abbreviated IPv6 host address is shown here:

2001:0DB8:0001:0000:0000:0000:0000:0001

A hextet is the hexadecimal, IPv6 version of an IPv4 octet. An IPv4 address is 4 octets long, separated by dots. An IPv6 address is 8 hextets long, separated by colons.

An IPv4 address is 4 octets and is commonly written or displayed in decimal notation.

255.255.255.255

An IPv6 address is 8 hextets and is commonly written or displayed in hexadecimal notation.

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

In an IPv4 address, each individual octet is 8 binary digits (bits). Four octets equals one 32-bit IPv4 address.

11111111 = 255

11111111.11111111.11111111.11111111 = 255.255.255.255

In an IPv6 address, each individual hextet is 16 bits long. Eight hextets equals one 128-bit IPv6 address.

1111111111111111 = FFFF

1111111111111111.1111111111111111.1111111111111111.1111111111111111.

1111111111111111.1111111111111111.1111111111111111.1111111111111111 =

FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF

If we read an IPv6 address starting from the left, the first (or far left) hextet identifies the IPv6 address type. For example, if the IPv6 address has all zeros in the far left hextet, then the address is possibly a loopback address.

0000:0000:0000:0000:0000:0000:0000:0001 = loopback address

::1 = loopback address abbreviated

As another example, if the IPv6 address has FE80 in the first hextet, then the address is a link-local address.

FE80:0000:0000:0000:C5B7:CB51:3C00:D6CE = link-local address

FE80::C5B7:CB51:3C00:D6CE = link-local address abbreviated

Study the chart below to help you identify the different types of IPv6 address based on the numbers in the first hextet.

First Hextet (Far Left)	Type of IPv6 Address
0000 to 00FF	Loopback address, any address, unspecified address, or IPv4-compatible
2000 to 3FFF	Global unicast address (a routable address in a range of addresses that is currently being handed out by the Internet Assigned Numbers Authority [IANA])
FE80 to FEBF	Link-local (a unicast address which identifies the host computer on the local network)
FC00 to FCFF	Unique-local (a unicast address which can be assigned to a host to identify it as being part of a specific subnet on the local network)
FF00 to FFFF	Multicast address

There are other IPv6 address types that are either not yet widely implemented, or have already become deprecated, and are no longer supported. For instance, an **anycast address** is new to IPv6 and can be used by routers to facilitate load sharing and provide alternate path flexibility if a router becomes unavailable. Only routers should respond to an anycast address. Alternatively, **site-local addresses** have been deprecated and replaced by unique-local addresses. Site-local addresses were identified by the numbers FEC0 in the initial hextet.

In IPv6 networks, there are no network (wire) addresses or broadcast addresses as there are in IPv4 networks.

Step 2: Match the IPv6 address to its type.

Match the IPv6 addresses to their corresponding address type. Notice that the addresses have been compressed to their abbreviated notation and that the slash network prefix number is not shown. Some answer choices must be used more than once.

IPv6 Address	Answer
2001:0DB8:1:ACAD::FE55:6789:B210	1. ____
::1	2. ____
FC00:22:A:2::CD4:23E4:76FA	3. ____
2033:DB8:1:1:22:A33D:259A:21FE	4. ____
FE80::3201:CC01:65B1	5. ____
FF00::	6. ____
FF00::DB7:4322:A231:67C	7. ____
FF02::2	8. ____

Answer Choices

- a. Loopback address
- b. Global unicast address
- c. Link-local address
- d. Unique-local address
- e. Multicast address

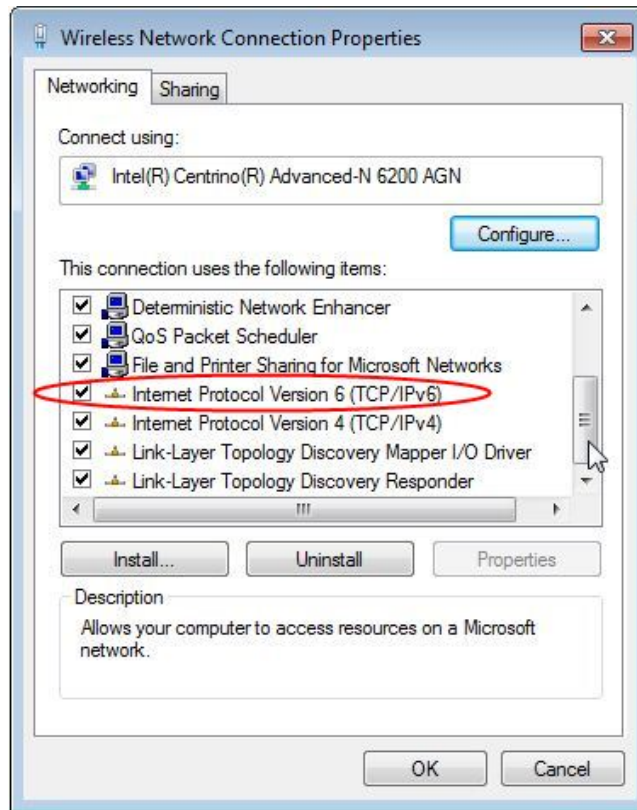
Answers: 1. B, 2. A, 3. D, 4. B, 5. C, 6. E, 7. E, 8. E

Part 2: Examine a Host IPv6 Network Interface and Address

In Part 2, you will check the IPv6 network settings of your PC to identify your network interface IPv6 address.

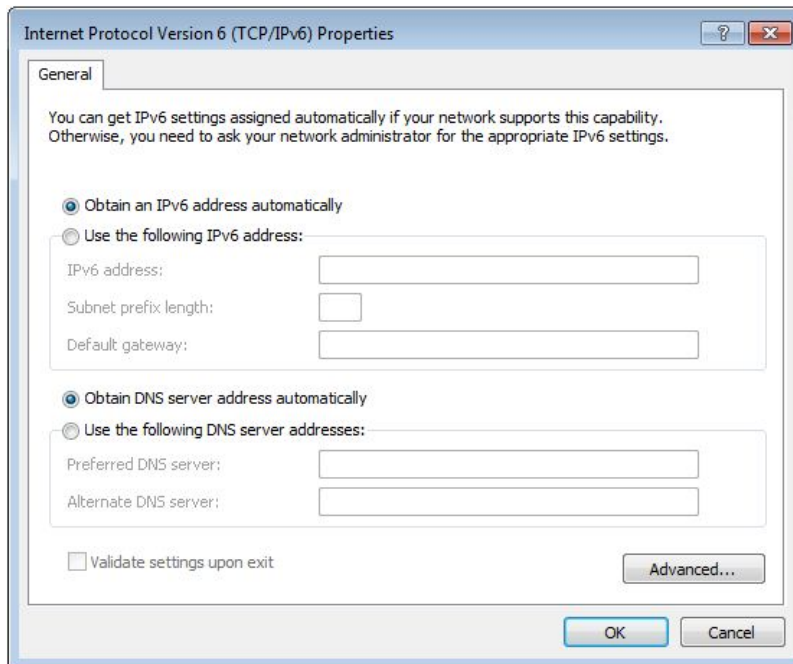
Step 1: Check your PC IPv6 network address settings.

- a. Verify that the IPv6 protocol is installed and active on your PC-A (check your Local Area Connection settings).
- b. Click the Windows **Start** button and then **Control Panel** and change **View by: Category** to **View by: Small icons**.
- c. Click the **Network and Sharing Center** icon.
- d. On the left side of the window, click **Change adapter settings**. You should now see icons representing your installed network adapters. Right-click your active network interface (it may be a **Local Area Connection** or a **Wireless Network Connection**), and then click **Properties**.
- e. You should now see your Network Connection Properties window. Scroll through the list of items to determine whether IPv6 is present, which indicates that it is installed, and if it is also check marked, which indicates that it is active.



- f. Select the item **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**. You should see the IPv6 settings for your network interface. Your IPv6 properties window is likely set to **Obtain an IPv6 address automatically**. This does not mean that IPv6 relies on the Dynamic Host Configuration Protocol (DHCP). Instead of using DHCP, IPv6 looks to the local router for IPv6 network information and then auto-configures its own IPv6 addresses. To manually configure IPv6, you must provide the IPv6 address, the subnet prefix length, and the default gateway.

Note: The local router can refer host requests for IPv6 information, especially Domain Name System (DNS) information, to a DHCPv6 server on the network.



- g. After you have verified that IPv6 is installed and active on your PC, you should check your IPv6 address information. To do this, click the **Start** button, type **cmd** in the *Search programs and files* form box, and press Enter. This opens a Windows command prompt window.
- h. Type **ipconfig /all** and press Enter. Your output should look similar to this:

```
C:\Users\user> ipconfig /all
```

```
Windows IP Configuration
```

```
<output omitted>
```

```
Wireless LAN adapter Wireless Network Connection:
```

```
Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) Centrino(R) Advanced-N 6200 AGN
Physical Address. . . . . : 02-37-10-41-FB-48
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8d4f:4f4d:3237:95e2%14(Preferred)
IPv4 Address. . . . . : 192.168.2.106(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Sunday, January 06, 2013 9:47:36 AM
Lease Expires . . . . . : Monday, January 07, 2013 9:47:38 AM
Default Gateway . . . . . : 192.168.2.1
DHCP Server . . . . . : 192.168.2.1
DHCPv6 IAID . . . . . : 335554320
DHCPv6 Client DUID. . . . . : 00-01-00-01-14-57-84-B1-1C-C1-DE-91-C3-5D

DNS Servers . . . . . : 192.168.1.1
```

8.8.4.4

<output omitted>

- i. You can see from the output that the client PC has an IPv6 link-local address with a randomly generated interface ID. What does it indicate about the network regarding IPv6 global unicast address, IPv6 unique-local address, or IPv6 gateway address?

It indicates that there is no IPv6 enabled gateway router providing global address, local address, or subnet information on the network.

- j. What kind of IPv6 addresses did you find when using **ipconfig /all**?

Answers will vary, but most likely they will be link-local addresses also.

Part 3: Practice IPv6 Address Abbreviation

In Part 3, you will study and review rules for IPv6 address abbreviation to correctly compress and decompress IPv6 addresses.

Step 1: Study and review the rules for IPv6 address abbreviation.

Rule 1: In an IPv6 address, a string of four zeros (0s) in a hextet can be abbreviated as a single zero.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00

2001:0404:0001:1000:**0:0**:0EF0:BC00 (abbreviated with single zeros)

Rule 2: In an IPv6 address, the leading zeros in each hextet can be omitted, trailing zeros cannot be omitted.

2001:**0404:0001**:1000:0000:0000:**0EF0**:BC00

2001:404:1:1000:0:0:EF0:BC00 (abbreviated with leading zeros omitted)

Rule 3: In an IPv6 address, a single continuous string of four or more zeros can be abbreviated as a double colon (::). The double colon abbreviation can only be used one time in an IP address.

2001:0404:0001:1000:**0000:0000**:0EF0:BC00

2001:404:1:1000:**::**EF0:BC00 (abbreviated with leading zeroes omitted and continuous zeros replaced with a double colon)

The image below illustrates these rules of IPv6 address abbreviation:

```
FF01:0000:0000:0000:0000:0000:0000:1
= FF01:0:0:0:0:0:0:1
= FF01::1
```

```
E3D7:0000:0000:0000:51F4:00C8:C0A8:6420
= E3D7::51F4:C8:C0A8:6420
```

```
3FFE:0501:0008:0000:0260:97FF:FE40:EFAB
= 3FFE:501:8:0:260:97FF:FE40:EFAB
= 3FFE:501:8::260:97FF:FE40:EFAB
```

Step 2: Practice compressing and decompressing IPv6 addresses.

Using the rules of IPv6 address abbreviation, either compress or decompress the following addresses:

- 1) 2002:0EC0:0200:0001:0000:04EB:44CE:08A2

2002:EC0:200:1::4EB:44CE:8A2

- 2) FE80:0000:0000:0001:0000:60BB:008E:7402

FE80::1:0:60BB:8E:7402

- 3) FE80::7042:B3D7:3DEC:84B8

FE80:0000:0000:0000:7042:B3D7:3DEC:84B8

- 4) FF00::

FF00:0000:0000:0000:0000:0000:0000

- 5) 2001:0030:0001:ACAD:0000:330E:10C2:32BF

2001:30:1:ACAD::330E:10C2:32BF

Reflection

1. How do you think you must support IPv6 in the future?

Answers will vary.

Lab – Identifying IPv6 Addresses

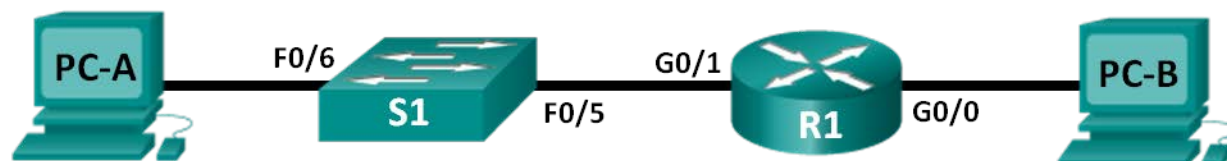
2. Do you think IPv4 networks continue on, or will everyone eventually switch over to IPv6? How long do you think it will take?

Answers will vary.

Lab - Configuring IPv6 Addresses on Network Devices (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IPv6 Address	Prefix Length	Default Gateway
R1	G0/0	2001:DB8:ACAD:A::1	64	N/A
	G0/1	2001:DB8:ACAD:1::1	64	N/A
S1	VLAN 1	2001:DB8:ACAD:1::B	64	N/A
PC-A	NIC	2001:DB8:ACAD:1::3	64	FE80::1
PC-B	NIC	2001:DB8:ACAD:A::3	64	FE80::1

Objectives

Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Part 2: Configure IPv6 Addresses Manually

Part 3: Verify End-to-End Connectivity

Background / Scenario

Knowledge of the Internet Protocol version 6 (IPv6) multicast groups can be helpful when assigning IPv6 addresses manually. Understanding how the all-router multicast group is assigned and how to control address assignments for the Solicited Nodes multicast group can prevent IPv6 routing issues and help ensure best practices are implemented.

In this lab, you will configure hosts and device interfaces with IPv6 addresses and explore how the all-router multicast group is assigned to a router. You will use **show** commands to view IPv6 unicast and multicast addresses. You will also verify end-to-end connectivity using the **ping** and **traceroute** commands.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Instructor Note: The **default bias** template used by the Switch Database Manager (SDM) does not provide IPv6 address capabilities. Verify that SDM is using either the **dual-ipv4-and-ipv6** template or the **lanbase-routing** template. The new template will be used after reboot even if the config is not saved.

```
S1# show sdm prefer
```

Follow these steps to assign the **dual-ipv4-and-ipv6** template as the default SDM template:

```
S1# configure terminal
```

```
S1(config)# sdm prefer dual-ipv4-and-ipv6 default
```

```
S1(config)# end
```

```
S1# reload
```

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing and an Ethernet straight-through cable may be used between the router and PC-B. If using another model Cisco router, it may be necessary to use an Ethernet crossover cable.

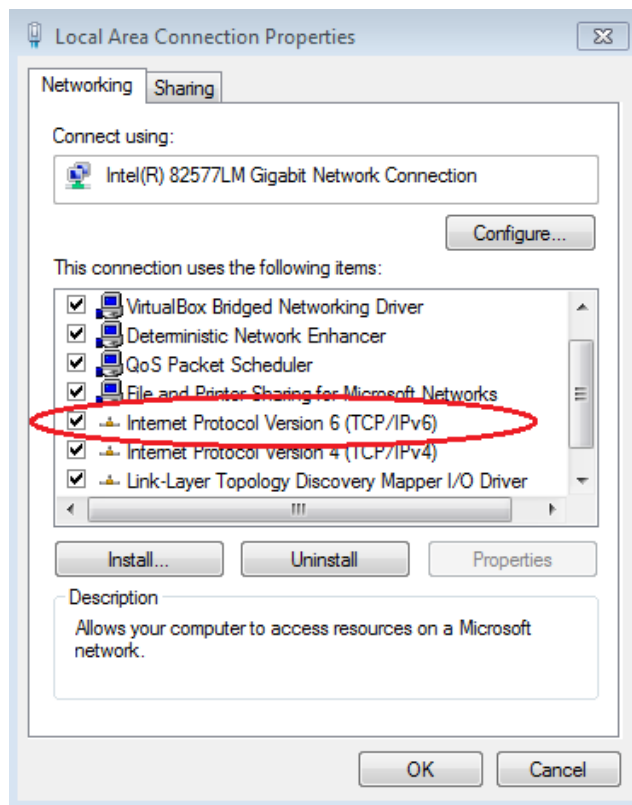
Part 1: Set Up Topology and Configure Basic Router and Switch Settings

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Verify that the PC interfaces are configured to use the IPv6 protocol.

Verify that the IPv6 protocol is active on both PCs by ensuring that the **Internet Protocol Version 6 (TCP/IPv6)** check box is selected in the Local Area Connection Properties window.



Step 4: Configure the router.

- Console into the router and enable privileged EXEC mode.
- Assign the device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the clear text passwords.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- Save the running configuration to the startup configuration file.

Step 5: Configure the switch.

- Console into the switch and enable privileged EXEC mode.
- Assign the device name to the switch.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.

- g. Encrypt the clear text passwords.
- h. Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- i. Save the running configuration to the startup configuration file.

Part 2: Configure IPv6 Addresses Manually

Step 1: Assign the IPv6 addresses to Ethernet interfaces on R1.

- a. Assign the IPv6 global unicast addresses, listed in the Addressing Table, to both Ethernet interfaces on R1.

```
R1(config)# interface g0/0
R1(config-if)# ipv6 address 2001:db8:acad:a::1/64
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ipv6 address 2001:db8:acad:1::1/64
R1(config-if)# no shutdown
R1(config-if)# end
R1#
```

Instructor Note: The IPv6 global prefix 2001:DB8::/32 is a reserved prefix for use in documentation, as described in RFC 3849.

- b. Issue the **show ipv6 interface brief** command to verify that the correct IPv6 unicast address is assigned to each interface.

```
R1# show ipv6 interface brief
Em0/0                                [administratively down/down]
    unassigned
GigabitEthernet0/0                   [up/up]
    FE80::D68C:B5FF:FECE:A0C0
    2001:DB8:ACAD:A::1
GigabitEthernet0/1                   [up/up]
    FE80::D68C:B5FF:FECE:A0C1
    2001:DB8:ACAD:1::1
<output omitted>
```

- c. Issue the **show ipv6 interface g0/0** command. Notice that the interface is listing two Solicited Nodes multicast groups, because the IPv6 link-local (FE80) Interface ID was not manually configured to match the IPv6 unicast Interface ID.

Note: The link-local address displayed is based on EUI-64 addressing, which automatically uses the interface Media Access Control (MAC) address to create a 128-bit IPv6 link-local address.

```
R1# show ipv6 interface g0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::D68C:B5FF:FECE:A0C0
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:1
```

```
FF02::1:FFCE:A0C0
```

```
MTU is 1500 bytes
```

```
<output omitted>
```

- d. To get the link-local address to match the unicast address on the interface, manually enter the link-local addresses on each of the Ethernet interfaces on R1.

```
R1# config t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
R1(config)# interface g0/0
```

```
R1(config-if)# ipv6 address fe80::1 link-local
```

```
R1(config-if)# interface g0/1
```

```
R1(config-if)# ipv6 address fe80::1 link-local
```

```
R1(config-if)# end
```

```
R1#
```

Note: Each router interface belongs to a separate network. Packets with a link-local address never leave the local network; therefore, you can use the same link-local address on both interfaces.

- e. Re-issue the **show ipv6 interface g0/0** command. Notice that the link-local address has been changed to **FE80::1** and that there is only one Solicited Nodes multicast group listed.

```
R1# show ipv6 interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
```

```
IPv6 is enabled, link-local address is FE80::1
```

```
No Virtual link-local address(es):
```

```
Global unicast address(es):
```

```
2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64
```

```
Joined group address(es):
```

```
FF02::1
```

```
FF02::1:FF00:1
```

```
MTU is 1500 bytes
```

```
<output omitted>
```

What multicast groups have been assigned to interface G0/0?

The all-nodes multicast group (FF02::1) and the Solicited Nodes multicast group (FF02::1:FF00:1).

Step 2: Enable IPv6 routing on R1.

- a. On a PC-B command prompt, enter the **ipconfig** command to examine IPv6 address information assigned to the PC interface.

Has an IPv6 unicast address been assigned to the network interface card (NIC) on PC-B? _____ **No**

- b. Enable IPv6 routing on R1 using the **IPv6 unicast-routing** command.

```
R1 # configure terminal
```

```
R1(config)# ipv6 unicast-routing
```

```
R1(config)# exit
```

```
R1#
```

```
*Dec 17 18:29:07.415: %SYS-5-CONFIG_I: Configured from console by console
```

- c. Use the **show ipv6 interface g0/0** command to see what multicast groups are assigned to interface G0/0. Notice that the all-router multicast group (FF02::2) now appears in the group list for interface G0/0.

Note: This will allow the PCs to obtain their IP address and default gateway information automatically using Stateless Address Autoconfiguration (SLAAC).

```
R1# show ipv6 interface g0/0
```

```
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::1
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:A::1, subnet is 2001:DB8:ACAD:A::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
  MTU is 1500 bytes
<output omitted>
```

- d. Now that R1 is part of the all-router multicast group, re-issue the **ipconfig** command on PC-B. Examine the IPv6 address information.

Why did PC-B receive the Global Routing Prefix and Subnet ID that you configured on R1?

R1 G0/0 is now part of the All-router multicast group, FF02::2. This allows it to send Router Advertisement (RA) messages with the Global Network Address and Subnet ID information to all nodes on the LAN. Notice that it also sent the link-local address, FE80::1, as the Default Gateway. The PCs will receive their IP address and default gateway via SLAAC.

Step 3: Assign IPv6 addresses to the management interface (SVI) on S1.

- a. Assign the IPv6 address listed in the Addressing Table to the management interface (VLAN 1) on S1. Also assign a link-local address for this interface. IPv6 command syntax is the same as on the router.

```
S1(config)# interface vlan 1
S1(config-if)# ipv6 address 2001:db8:acad:1::b/64
S1(config-if)# ipv6 address fe80::b link-local
S1(config-if)# end
S1#
*Mar  1 03:25:26.681: %SYS-5-CONFIG_I: Configured from console by console
```

- b. Verify that the IPv6 addresses are properly assigned to the management interface using the **show ipv6 interface vlan1** command.

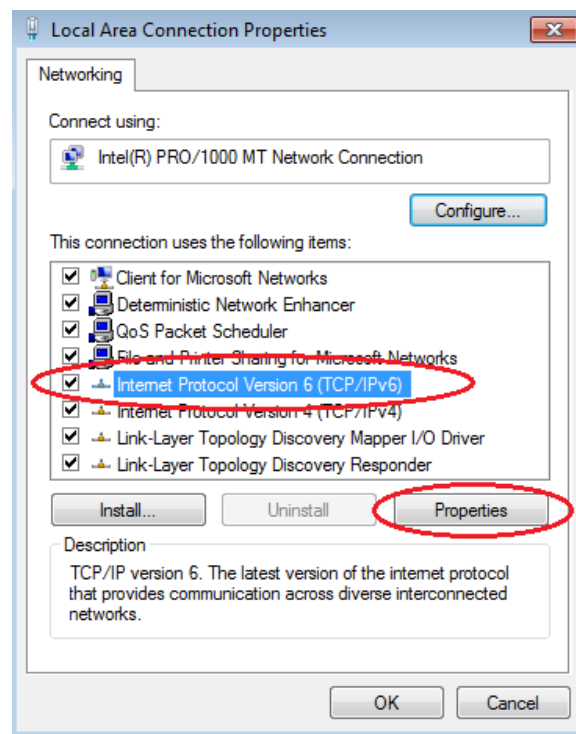
```
S1# show ipv6 interface vlan1
Vlan1 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::B
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::B, subnet is 2001:DB8:ACAD:1::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF00:B
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
```

```
ICMP redirects are enabled
ICMP unreachable are sent
Output features: Check hwidb
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
ND NS retransmit interval is 1000 milliseconds
S1#
```

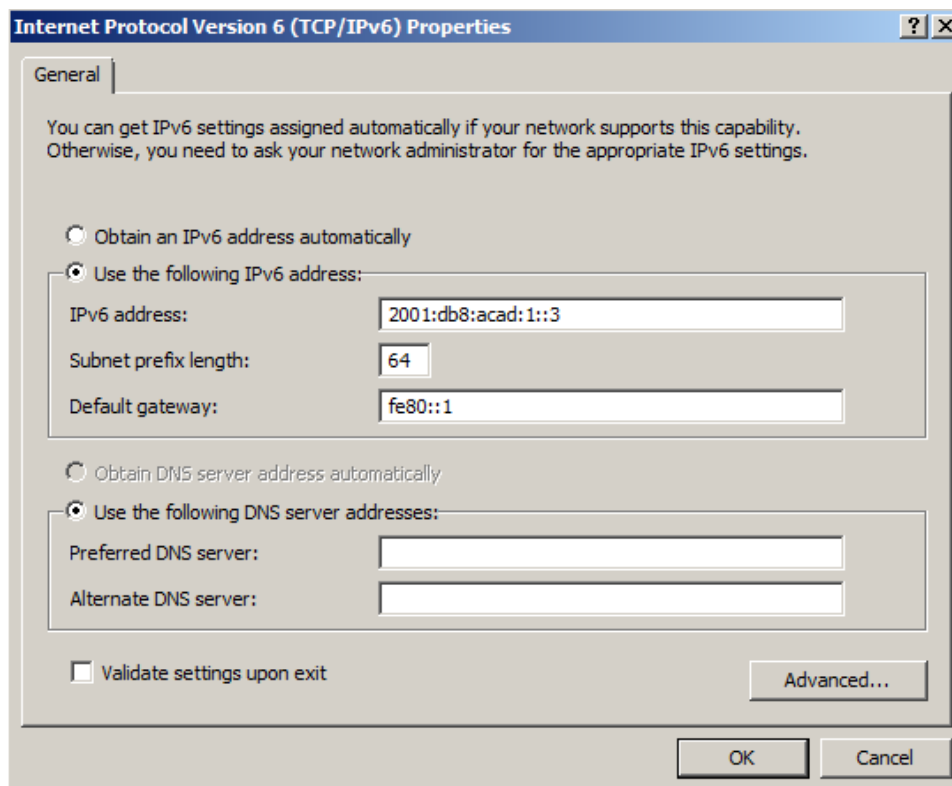
Note: The default 2960 Switch Database Manager (SDM) template does not support IPv6. It may be necessary to issue the command **sdm prefer dual-ipv4-and-ipv6 default** to enable IPv6 addressing before applying an IPv6 address to the VLAN 1 SVI.

Step 4: Assign static IPv6 addresses to the PCs.

- Open the Local Area Connection Properties window on PC-A. Select **Internet Protocol Version 6 (TCP/IPv6)** and click **Properties**.



- Click the **Use the following IPv6 address** radio button. Refer to the Addressing Table and enter the **IPv6 address**, **Subnet prefix length**, and **Default gateway** information. Click **OK**.



- c. Click **Close** to close the Local Area Connection Properties window.
- d. Repeat Steps 4a to c to enter the static IPv6 information on PC-B. For the correct IPv6 address information, refer to the Addressing Table.
- e. Issue the **ipconfig** command from the command line on PC-B to verify the IPv6 address information.

Part 3: Verify End-to-End Connectivity

- a. From PC-A, ping **FE80::1**. This is the link-local address assigned to G0/1 on R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Note: You can also test connectivity by using the global unicast address, instead of the link-local address.

- b. Ping the S1 management interface from PC-A.

```
C:\>ping 2001:db8:acad:1::b

Pinging 2001:db8:acad:1::b with 32 bytes of data:
Reply from 2001:db8:acad:1::b: time=14ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=2ms
Reply from 2001:db8:acad:1::b: time=3ms

Ping statistics for 2001:db8:acad:1::b:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 14ms, Average = 5ms

C:\>_
```

- c. Use the **tracert** command on PC-A to verify that you have end-to-end connectivity to PC-B.

```
C:\>tracert 2001:db8:acad:a::3

Tracing route to 2001:db8:acad:a::3 over a maximum of 30 hops
  1  <1 ms    <1 ms    <1 ms    2001:db8:acad:1::1
  2   5 ms    <1 ms    <1 ms    2001:db8:acad:a::3

Trace complete.

C:\>
```

- d. From PC-B, ping PC-A.

```
C:\>ping 2001:db8:acad:1::3

Pinging 2001:db8:acad:1::3 with 32 bytes of data:
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms
Reply from 2001:db8:acad:1::3: time<1ms

Ping statistics for 2001:db8:acad:1::3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

- e. From PC-B, ping the link-local address for G0/0 on R1.

```
C:\>ping fe80::1

Pinging fe80::1 with 32 bytes of data:
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms
Reply from fe80::1: time<1ms

Ping statistics for fe80::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

Note: If end-to-end connectivity is not established, troubleshoot your IPv6 address assignments to verify that you entered the addresses correctly on all devices.

Reflection

1. Why can the same link-local address, FE80::1, be assigned to both Ethernet interfaces on R1?

Link-local packets never leave the local network, so the same link-local address can be used on an interface associated to a different local network.

2. What is the Subnet ID of the IPv6 unicast address 2001:db8:acad::aaaa:1234/64?

0 (zero) or 0000 (zeros). The 4th hextet is the Subnet ID of an IPv6 address with a prefix of /64. In the example the 4th hextet contains all zeros and the IPv6 Omitting All 0 Segment rule is using the double colon to depict the Subnet ID and the first two hextets of the Interface ID.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs

Router R1 (After part 1 of this lab)

```
R1#sh run
```

```
Building configuration...
```

```
Current configuration : 1443 bytes
```

```
!  
version 15.2  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname R1  
!
```

Lab - Configuring IPv6 Addresses on Network Devices

```
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
banner motd ^C
*****
```


Lab - Configuring IPv6 Addresses on Network Devices

```
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
  password 7 01100F175804
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 104D000A0618
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1 (After part 1 of this lab)

```
S1#sh run
Building configuration...

Current configuration : 1624 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
```

```
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
```

```
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
!
ip http server
ip http secure-server
!
banner motd ^C
*****
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
  password 7 121A0C041104
  login
line vty 0 4
  password 7 121A0C041104
  login
line vty 5 15
  password 7 121A0C041104
  login
!
end
```

Router R1 (Final)

```
R1#show run
Building configuration...

Current configuration : 1577 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
```

Lab - Configuring IPv6 Addresses on Network Devices

```
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip cef
ipv6 unicast-routing
ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:A::1/64
!
interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:ACAD:1::1/64
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
```

```
banner motd ^C
*****
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
  password 7 01100F175804
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  password 7 104D000A0618
  login
  transport input all
!
scheduler allocate 20000 1000
!
end
```

Switch S1 (Final)

```
S1#sh run
Building configuration...

Current configuration : 1733 bytes
!
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
```

```
system mtu routing 1500
!
no ip domain-lookup
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
```

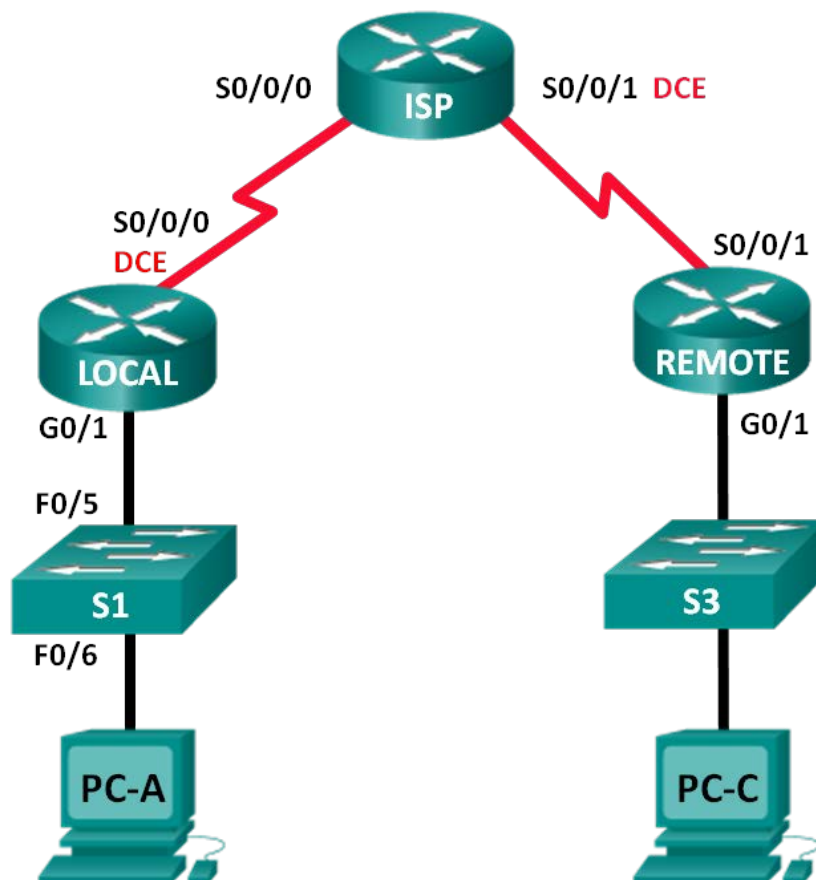
```
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
  no ip address
  ipv6 address FE80::B link-local
  ipv6 address 2001:DB8:ACAD:1::B/64
!
ip http server
ip http secure-server
!
!
banner motd ^C
*****
* Warning: Unauthorized access is prohibited! *
*****
^C
!
line con 0
  password 7 121A0C041104
  login
line vty 0 4
  password 7 121A0C041104
  login
line vty 5 15
  password 7 121A0C041104
  login
!
```

```
end
```


Lab – Testing Network Connectivity with Ping and Traceroute (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
LOCAL	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
REMOTE	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectives

Part 1: Build and Configure the Network

Part 2: Use Ping Command for Basic Network Testing

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

Part 4: Troubleshoot the Topology

Background / Scenario

Ping and traceroute are two tools that are indispensable when testing TCP/IP network connectivity. Ping is a network administration utility used to test the reachability of a device on an IP network. This utility also measures the round-trip time for messages sent from the originating host to a destination computer. The ping utility is available on Windows, Unix-like operating systems (OS), and the Cisco Internetwork Operating System (IOS).

The traceroute utility is a network diagnostic tool for displaying the route and measuring the transit delays of packets travelling an IP network. The tracert utility is available on Windows, and a similar utility, traceroute, is available on Unix-like OS and Cisco IOS.

In this lab, the **ping** and **traceroute** commands are examined and command options are explored to modify the command behavior. Cisco devices and PCs are used in this lab for command exploration. Cisco routers will use Enhanced Interior Gateway Routing Protocol (EIGRP) to route packets between networks. The necessary Cisco device configurations are provided in this lab.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 3 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 1: Build and Configure the Network

In Part 1, you will set up the network in the topology and configure the PCs and Cisco devices. The initial configurations for the routers and switches are provided for your reference. In this topology, EIGRP is used to route packets between networks.

Step 1: Cable the network as shown in the topology.

Step 2: Erase the configurations on the routers and switches, and reload the devices.

Step 3: Configure PC IP addresses and default gateways according to the Addressing Table.

Step 4: Configure the LOCAL, ISP, and REMOTE routers using the initial configurations provided below.

At the switch or router global config mode prompt, copy and paste the configuration for each device. Save the configuration to startup-config.

Instructor Note: The command “no auto-summary” for EIGRP is included for compatibility with older routers and IOS versions. With the 1941 router and IOS 15 specified for this lab, no auto-summary is the default,

Initial configurations for the LOCAL router:

```
hostname LOCAL
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 56000
 no shutdown
interface g0/1
 ip add 192.168.1.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0 0.0.0.255
 no auto-summary
```

Initial configurations for ISP:

```
hostname ISP
no ip domain-lookup
interface s0/0/0
 ip address 10.1.1.2 255.255.255.252
```

```
no shutdown
interface s0/0/1
ip add 10.2.2.2 255.255.255.252
clock rate 56000
no shutdown
router eigrp 1
network 10.1.1.0 0.0.0.3
network 10.2.2.0 0.0.0.3
no auto-summary
end
```

Initial configurations for REMOTE:

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
ip address 10.2.2.1 255.255.255.252
no shutdown
interface g0/1
ip add 192.168.3.1 255.255.255.0
no shutdown
router eigrp 1
network 10.2.2.0 0.0.0.3
network 192.168.3.0 0.0.0.255
no auto-summary
end
```

Step 5: Configure the S1 and S3 switches with the initial configurations.

Instructor Note: If Netlab is used, switch interface FastEthernet 0/1 – 0/4 should be shutdown for this lab. Use the following commands on S1 and S3:

```
Switch (config)# interface range f0/1 - 4
Switch (config)# shutdown
```

Initial configurations for S1:

```
hostname S1
no ip domain-lookup
interface vlan 1
ip add 192.168.1.11 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.1.1
end
```

Initial configurations for S3:

```
hostname S3
no ip domain-lookup
interface vlan 1
ip add 192.168.3.11 255.255.255.0
```

```
no shutdown
exit
ip default-gateway 192.168.3.1
end
```

Step 6: Configure an IP host table on the LOCAL router.

The IP host table allows you to use a hostname to connect to a remote device rather than an IP address. The host table provides name resolution for the device with the following configurations. Copy and paste the following configurations for the LOCAL router. The configurations will allow you to use the hostnames for **ping** and **traceroute** commands on the LOCAL router.

```
ip host REMOTE 10.2.2.1 192.168.3.1
ip host ISP 10.1.1.2 10.2.2.2
ip host LOCAL 192.168.1.1 10.1.1.1
ip host PC-C 192.168.3.3
ip host PC-A 192.168.1.3
ip host S1 192.168.1.11
ip host S3 192.168.3.11
end
```

Part 2: Use Ping Command for Basic Network Testing

In Part 2 of this lab, use the **ping** command to verify end-to-end connectivity. Ping operates by sending Internet Control Message Protocol (ICMP) echo request packets to the target host and then waiting for an ICMP response. It can record the round trip time and any packet loss.

You will examine the results with the **ping** command and the additional ping options that are available on Windows-based PCs and Cisco devices.

Step 1: Test network connectivity from the LOCAL network using PC-A.

All the pings from PC-A to other devices in the topology should be successful. If they are not, check the topology and the cabling, as well as the configuration of the Cisco devices and the PCs.

- a. Ping from PC-A to its default gateway (LOCAL's GigabitEthernet 0/1 interface).

```
C:\Users\User1> ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

In this example, four (4) ICMP requests, 32 bytes each, were sent and the responses were received in less than one millisecond with no packet loss. The transmission and reply time increases as the ICMP requests and responses are processed by more devices during the journey to and from the final destination.

- b. From PC-A, ping the addresses listed in the following table and record the average round trip time and Time to Live (TTL).

Destination	Average Round Trip Time (ms)	TTL
192.168.1.1 (LOCAL)	0	255
192.168.1.11 (S1)	0*	255
10.1.1.1 (LOCAL)	0	255
10.1.1.2 (ISP)	20	254
10.2.2.2 (ISP)	20	254
10.2.2.1 (REMOTE)	40	253
192.168.3.1 (REMOTE)	40	253
192.168.3.11 (S3)	40*	252
192.168.3.3 (PC-C)	40	125

***Instructor Note:** The average round trip time was increased if the message “Request timed out” was displayed during the first ICMP request. The delay was caused by ARP, and this resulted in packet loss.

Notice the average round trip time to 192.168.3.3 (PC-C). The time increased because the ICMP requests were processed by three routers before PC-A received the reply from PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

Step 2: Use extended ping commands on a PC.

The default **ping** command sends four requests at 32 bytes each. It waits 4,000 milliseconds (4 seconds) for each response to be returned before displaying the “Request timed out” message. The **ping** command can be fine tuned for troubleshooting a network.

- a. At the command prompt, type **ping** and press Enter.

```
C:\Users\User1> ping
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -t                Ping the specified host until stopped.
                      To see statistics and continue - type Control-Break;
                      To stop - type Control-C.
```

-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated and has no effect on the type of service field in the IP Header).
-r count	Record route for count hops (IPv4-only).
-s count	Timestamp for count hops (IPv4-only).
-j host-list	Loose source route along host-list (IPv4-only).
-k host-list	Strict source route along host-list (IPv4-only).
-w timeout	Timeout in milliseconds to wait for each reply.
-R	Use routing header to test reverse route also (IPv6-only).
-S srcaddr	Source address to use.
-4	Force using IPv4.
-6	Force using IPv6.

- b. Using the **-t** option, ping PC-C to verify that PC-C is reachable.

```
C:\Users\User1> ping -t 192.168.3.3
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

To illustrate the results when a host is unreachable, disconnect the cable between the REMOTE router and the S3 switch, or shut down the GigabitEthernet 0/1 interface on the REMOTE router.

```
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.1.3: Destination host unreachable.
Reply from 192.168.1.3: Destination host unreachable.
```

While the network is functioning correctly, the **ping** command can determine whether the destination responded and how long it took to receive a reply from the destination. If a network connectivity problem exists, the **ping** command displays an error message.

- c. Reconnect the Ethernet cable or enable the GigabitEthernet interface on the REMOTE router (using the **no shutdown** command) before moving onto the next step. After about 30 seconds, the ping should be successful again.

```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
```

- d. Press **Ctrl+C** to stop the ping command.

Step 3: Test network connectivity from the LOCAL network using Cisco devices.

The **ping** command is also available on Cisco devices. In this step, the **ping** command is examined using the LOCAL router and the S1 switch.

- a. Ping PC-C on the REMOTE network using the IP address of 192.168.3.3 from the LOCAL router.

```
LOCAL# ping 192.168.3.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/64/68 ms
```

The exclamation point (!) indicates that the ping was successful from the LOCAL router to PC-C. The round trip takes an average of 64 ms with no packet loss, as indicated by a 100% success rate.

- b. Because a local host table was configured on the LOCAL router, you can ping PC-C on the REMOTE network using the hostname configured from the LOCAL router.

```
LOCAL# ping PC-C
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

- c. There are more options available for the **ping** command. At the CLI, type **ping** and press Enter. Input **192.168.3.3** or **PC-C** for the Target IP address. Press Enter to accept the default value for other options.

```
LOCAL# ping
```

```
Protocol [ip]:
```

```
Target IP address: PC-C
```

```
Repeat count [5]:
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]:
```

```
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/63/64 ms
```

- d. You can use an extended ping to observe when there is a network issue. Start the **ping** command to 192.168.3.3 with a repeat a count of 500. Then, disconnect the cable between the REMOTE router and the S3 switch or shut down the GigabitEthernet 0/1 interface on the REMOTE router.

Reconnect the Ethernet cable or enable the GigabitEthernet interface on the REMOTE router after the exclamation points (!) have replaced by the letter U and periods (.). After about 30 seconds, the ping should be successful again. Press **Ctrl+Shift+6** to stop the **ping** command if desired.

```
LOCAL# ping
```

```
Protocol [ip]:
```

```
Target IP address: 192.168.3.3
```

```
Repeat count [5]: 500
```

```
Datagram size [100]:
```

```
Timeout in seconds [2]:
```

```
Extended commands [n]:
```

```
Sweep range of sizes [n]:
```

```
Type escape sequence to abort.
```

```
Sending 500, 100-byte ICMP Echos to 192.168.3.3, timeout is 2 seconds:
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!U.....
...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```



```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!
Success rate is 95 percent (479/500), round-trip min/avg/max = 60/63/72 ms
```

The letter U in the results indicates that a destination is unreachable. An error protocol data unit (PDU) was received by the LOCAL router. Each period (.) in the output indicates that the ping timed out while waiting for a reply from PC-C. In this example, 5% of the packets were lost during the simulated network outage.

Note: You can also use the following command for the same results:

```
LOCAL# ping 192.168.3.3 repeat 500
```

or

```
LOCAL# ping PC-C repeat 500
```

- e. You can also test network connectivity with a switch. In this example, the S1 switch pings the S3 switch on the REMOTE network.

```
S1# ping 192.168.3.11
```

Type escape sequence to abort.

```
Sending 5, 100-byte ICMP Echos to 192.168.3.11, timeout is 2 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 67/67/68 ms
```

The **ping** command is extremely useful when troubleshooting network connectivity. However, ping cannot indicate the location of problem when a ping is not successful. The **tracert** (or **tracert**) command can display network latency and path information.

Part 3: Use Tracert and Traceroute Commands for Basic Network Testing

The commands for tracing routes can be found on PCs and network devices. For a Windows-based PC, the **tracert** command uses ICMP messages to trace the path to the final destination. The **tracert** command utilizes the User Datagram Protocol (UDP) datagrams for tracing routes to the final destination for Cisco devices and other Unix-like PCs.

In Part 3, you will examine the traceroute commands and determine the path that a packet travels to its final destination. You will use the **tracert** command from the Windows PCs and the **tracert** command from the Cisco devices. You will also examine the options that are available for fine tuning the traceroute results.

Step 1: Use the tracert command from PC-A to PC-C.

- a. At the command prompt, type **tracert 192.168.3.3**.

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to PC-C [192.168.3.3]
```

```
Over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	24 ms	24 ms	24 ms	10.1.1.2
3	48 ms	48 ms	48 ms	10.2.2.1
4	59 ms	59 ms	59 ms	PC-C [192.168.3.3]

```
Trace complete.
```

The tracert results indicates the path from PC-A to PC-C is from PC-A to LOCAL to ISP to REMOTE to PC-C. The path to PC-C traveled through three router hops to the final destination of PC-C.

Step 2: Explore additional options for the tracert command.

- a. At the command prompt, type **tracert** and press Enter.

```
C:\Users\User1> tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                Do not resolve addresses to hostnames.
    -h maximum_hops   Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                Force using IPv4.
    -6                Force using IPv6.
```

- b. Use the **-d** option. Notice that the IP address of 192.168.3.3 is not resolved as PC-C.

```
C:\Users\User1> tracert -d 192.168.3.3
Tracing route to 192.168.3.3 over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    192.168.1.1
  2  24 ms     24 ms     24 ms     10.1.1.2
  3  48 ms     48 ms     48 ms     10.2.2.1
  4  59 ms     59 ms     59 ms     192.168.3.3

Trace complete.
```

Step 3: Use the traceroute command from the LOCAL router to PC-C.

- a. At the command prompt, type **traceroute 192.168.3.3** or **traceroute PC-C** on the LOCAL router. The hostnames are resolved because a local IP host table was configured on the LOCAL router.

```
LOCAL# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 28 msec 32 msec

LOCAL# traceroute PC-C
Type escape sequence to abort.
Tracing the route to PC-C (192.168.3.3)
VRF info: (vrf in name/id, vrf out name/id)
  1 ISP (10.1.1.2) 16 msec 16 msec 16 msec
  2 REMOTE (10.2.2.1) 28 msec 32 msec 28 msec
  3 PC-C (192.168.3.3) 32 msec 32 msec 28 msec
```

Step 4: Use the traceroute command from the S1 switch to PC-C.

- a. On the S1 switch, type **traceroute 192.168.3.3**. The hostnames are not displayed in the traceroute results because a local IP host table was not configured on this switch.

```
S1# traceroute 192.168.3.3
Type escape sequence to abort.
Tracing the route to 192.168.3.3
VRF info: (vrf in name/id, vrf out name/id)
 1 192.168.1.1 1007 msec 0 msec 0 msec
 2 10.1.1.2 17 msec 17 msec 16 msec
 3 10.2.2.1 34 msec 33 msec 26 msec
 4 192.168.3.3 33 msec 34 msec 33 msec
```

The **traceroute** command has additional options. You can use the **?** or just press Enter after typing **traceroute** at the prompt to explore these options.

The following link provides more information regarding the **ping** and **traceroute** commands for a Cisco device:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800a6057.shtml

Part 4: Troubleshoot the Topology

Step 1: Erase the configurations on the REMOTE router.

Step 2: Reload the REMOTE router.

Step 3: Copy and paste the following configuration into the REMOTE router.

```
hostname REMOTE
no ip domain-lookup
interface s0/0/1
 ip address 10.2.2.1 255.255.255.252
 no shutdown
interface g0/1
 ip add 192.168.8.1 255.255.255.0
 no shutdown
router eigrp 1
 network 10.2.2.0 0.0.0.3
 network 192.168.3.0 0.0.0.255
 no auto-summary
end
```

Step 4: From the LOCAL network, use ping and tracert or traceroute commands to troubleshoot and correct the problem on the REMOTE network.

- a. Use the **ping** and **tracert** commands from PC-A.

You can use the **tracert** command to determine end-to-end network connectivity. This tracert result indicates that PC-A can reach its default gateway of 192.168.1.1, but PC-A does not have network connectivity with PC-C.

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to 192.168.3.3 over a maximum of 30 hops
  1    <1 ms    <1 ms    <1 ms  192.168.1.1
  2  192.168.1.1  reports: Destination host unreachable.
```

Trace complete.

One way to locate the network issue is to ping each hop in the network to PC-C. First determine if PC-A can reach the ISP router Serial 0/0/1 interface with an IP address of 10.2.2.2.

```
C:\Users\Utraser1> ping 10.2.2.2
```

```
Pinging 10.2.2.2 with 32 bytes of data:
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
Reply from 10.2.2.2: bytes=32 time=41ms TTL=254
```

```
Ping statistics for 10.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 20ms, Maximum = 21ms, Average = 20ms
```

The ping was successful to the ISP router. The next hop in the network is the REMOTE router. Ping the REMOTE router Serial 0/0/1 interface with an IP address of 10.2.2.1.

```
C:\Users\User1> ping 10.2.2.1
```

```
Pinging 10.2.2.1 with 32 bytes of data:
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
Reply from 10.2.2.1: bytes=32 time=41ms TTL=253
```

```
Ping statistics for 10.2.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 40ms, Maximum = 41ms, Average = 40ms
```

PC-A can reach the REMOTE router. Based on the successful ping results from PC-A to the REMOTE router, the network connectivity issue is with 192.168.3.0/24 network. Ping the default gateway to PC-C, which is the GigabitEthernet 0/1 interface of the REMOTE router.

```
C:\Users\User1> ping 192.168.3.1
```

```
Pinging 192.168.3.1 with 32 bytes of data:
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
Reply from 192.168.1.1: Destination host unreachable.
```

```
Ping statistics for 192.168.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

PC-A cannot reach the GigabitEthernet 0/1 interface of the REMOTE router, as displayed by the results from the **ping** command.

The S3 switch can also be pinged from PC-A to verify the location of the networking connectivity issue by typing **ping 192.168.3.11** at the command prompt. Because PC-A cannot reach GigabitEthernet 0/1 of the REMOTE router, PC-A probably cannot ping the S3 switch successfully, as indicated by the results below.

```
C:\Users\User1> ping 192.168.3.11
```

```
Pinging 192.168.3.11 with 32 bytes of data:
```

```
Reply from 192.168.1.1: Destination host unreachable.
```

```
Reply from 192.168.1.1: Destination host unreachable.
```

```
Reply from 192.168.1.1: Destination host unreachable.
```

```
Reply from 192.168.1.1: Destination host unreachable.
```

```
Ping statistics for 192.168.3.11:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

The tracert and ping results conclude that PC-A can reach the LOCAL, ISP, and REMOTE routers, but not PC-C or the S3 switch, nor the default gateway for PC-C.

- b. Use the **show** commands to examine the running configurations for the the REMOTE router.

```
REMOTE# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.8.1	YES	manual	up	up
Serial0/0/0	unassigned	YES	unset	administratively down	down
Serial0/0/1	10.2.2.1	YES	manual	up	up

```
REMOTE# show run
```

```
<output omitted>
```

```
interface GigabitEthernet0/0
```

```
no ip address
```

```
shutdown
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
interface GigabitEthernet0/1
```

```
ip address 192.168.8.1 255.255.255.0
```

```
duplex auto
```

```
speed auto
```

```
!
```

```
interface Serial0/0/0
```

```
no ip address
```

```
shutdown
```

```
clock rate 2000000
```

```
!
```

```
interface Serial0/0/1
```

```
ip address 10.2.2.1 255.255.255.252
```

```
<output omitted>
```

The outputs of the **show run** and **show ip interface brief** commands indicate that the GigabitEthernet 0/1 interface is up/up, but was configured with an incorrect IP address.

- c. Correct the IP address for GigabitEthernet 0/1.

```
REMOTE# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
REMOTE(config)# interface GigabitEthernet 0/1
REMOTE(config-if)# ip address 192.168.3.1 255.255.255.0
```

- d. Verify that PC-A can ping and tracer to PC-C.

```
C:\Users\User1> ping 192.168.3.3
Pinging 192.168.3.3 with 32 bytes of data:
Reply from 192.168.3.3: bytes=32 time=44ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125
Reply from 192.168.3.3: bytes=32 time=40ms TTL=125
Reply from 192.168.3.3: bytes=32 time=41ms TTL=125

Ping statistics for 192.168.3.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 40ms, Maximum = 44ms, Average = 41ms
```

```
C:\Users\User1> tracert 192.168.3.3
```

```
Tracing route to PC-C [192.168.3.3]
Over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	24 ms	24 ms	24 ms	10.1.1.2
3	48 ms	48 ms	48 ms	10.2.2.1
4	59 ms	59 ms	59 ms	PC-C [192.168.3.3]

```
Trace complete.
```

Note: This can also be accomplished using **ping** and **tracert** commands from the CLI on the the LOCAL router and the S1 switch after verifying that there are no network connectivity issues on the 192.168.1.0/24 network.

Reflection

1. What could prevent ping or traceroute responses from reaching the originating device beside network connectivity issues?

Firewall on the PCs, access lists command, routing issues, interface is down, network delay

2. If you ping a non-existent address on the remote network, such as 192.168.3.4, what is the message displayed by the **ping** command? What does this mean? If you ping a valid host address and receive this response, what should you check?
-

Request timed out or periods (.). This means that there was no response in the default time period. Some of the items you may check: router is down, destination host is down, return route to your device and latency of the response is not more than the default time period

3. If you ping an address that does not exist in any network in your topology, such as 192.168.5.3, from a Windows-based PC, what is the message displayed by the **ping** command? What does this message indicate?

Destination host unreachable. This message indicates that there is no route to the destination as the network is not listed by the routing table.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs

Router LOCAL

```
LOCAL# show running-config
Building configuration...
```

```
Current configuration : 1462 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
```

```
!  
hostname LOCAL  
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
no aaa new-model  
memory-size iomem 15  
!  
!  
!  
!  
!  
!  
!  
no ip domain lookup  
ip host REMOTE 10.2.2.1 192.168.3.1  
ip host ISP 10.1.1.2 10.2.2.2  
ip host LOCAL 192.168.1.1 10.1.1.1  
ip host PC-C 192.168.3.3  
ip host PC-A 192.168.1.3  
ip host S1 192.168.1.11  
ip host S3 192.168.3.11  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!
```



```
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 56000
!
interface Serial0/0/1
 no ip address
 shutdown
!
!
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.1.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 login
 transport input all
!
scheduler allocate 20000 1000
!
end
```

ROUTER ISP

```
ISP# show running-config
Building configuration...

Current configuration : 1265 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
memory-size iomem 15
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
```

```
!  
interface GigabitEthernet0/0  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  ip address 10.1.1.2 255.255.255.252  
!  
interface Serial0/0/1  
  ip address 10.2.2.2 255.255.255.252  
  clock rate 56000  
!  
!  
router eigrp 1  
  network 10.1.1.0 0.0.0.3  
  network 10.2.2.0 0.0.0.3  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane  
!  
!  
!  
line con 0  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all
```

```
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router REMOTE

```
REMOTE# show running-config
Building configuration...
```

```
Current configuration : 1440 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname REMOTE
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
memory-size iomem 10
!
!
!
!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
!
!
```

```
!  
!  
!  
!  
!  
!  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/0  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  ip address 192.168.3.1 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
interface Serial0/0/1  
  ip address 10.2.2.1 255.255.255.252  
!  
!  
router eigrp 1  
  network 10.2.2.0 0.0.0.3  
  network 192.168.3.0  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
!  
!  
!  
control-plane
```

```
!  
!  
!  
line con 0  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  login  
  transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

Switch S1

```
S1# show running-config  
Building configuration...  
  
Current configuration : 1565 bytes  
!  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
no aaa new-model  
system mtu routing 1500  
!  
!  
no ip domain-lookup  
!
```

```
!  
!  
!  
!  
!  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
!  
!  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!
```

```
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip default-gateway 192.168.1.1
 ip http server
 ip http secure-server
!
!
!
 line con 0
 line vty 5 15
!
end
```

Switch S3

```
S3# show running-config
Building configuration...

Current configuration : 1563 bytes
!
!
```



```
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S3
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
!
!
!
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
```

```
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.3.11 255.255.255.0
!
```

Lab – Testing Network Connectivity with Ping and Traceroute

```
ip default-gateway 192.168.3.1
ip http server
ip http secure-server
!
!
line con 0
line vty 5 15
!
end
```

Lab - Mapping the Internet (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Test Network Connectivity Using Ping

Part 2: Trace a Route to a Remote Server Using Windows Tracert

Background

Route tracing computer software is a utility that lists the networks data has to traverse from the user's originating end device to a distant destination network.

This network tool is typically executed at the command line as:

```
tracert <destination network name or end device address>
```

(Microsoft Windows systems)

or

```
traceroute <destination network name or end device address>
```

(UNIX and similar systems)

Route tracing utilities allow a user to determine the path or routes as well as the delay across an IP network. Several tools exist to perform this function.

The **traceroute** (or **tracert**) tool is often used for network troubleshooting. By showing a list of routers traversed, it allows the user to identify the path taken to reach a particular destination on the network or across internetworks. Each router represents a point where one network connects to another network and through which the data packet was forwarded. The number of routers is known as the number of "hops" the data traveled from source to destination.

The displayed list can help identify data flow problems when trying to access a service such as a website. It can also be useful when performing tasks such as downloading data. If there are multiple websites (mirrors) available for the same data file, one can trace each mirror to get a good idea of which mirror would be the fastest to use.

Two trace routes between the same source and destination conducted some time apart may produce different results. This is due to the "meshed" nature of the interconnected networks that comprise the Internet and the Internet Protocols ability to select different pathways over which to send packets.

Command-line-based route tracing tools are usually embedded with the operating system of the end device.

Scenario

Using an Internet connection, you will use three route tracing utilities to examine the Internet pathway to destination networks. This activity should be performed on a computer that has Internet access and access to the command line. First, you will use the Windows embedded tracert utility.

Instructor Note: Many schools do not have access to the command prompt. Traceroutes are included in Appendix A for your use. Depending on the situation, this lab can be assigned in the classroom, as homework or can be performed by the instructor as a walk-through demonstration.

Some institutions disable ICMP echo replies used by both ping and traceroute utilities. Before students begin this activity, make sure there are no local restrictions related to ICMP datagrams. This activity assumes that ICMP datagrams are not restricted by any local security policy.

Required Resources

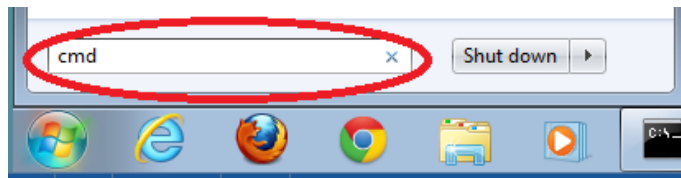
1 PC (Windows 7 or 8 with Internet access)

Part 1: Test Network Connectivity Using Ping

Step 1: Determine whether the remote server is reachable.

To trace the route to a distant network, the PC used must have a working connection to the Internet.

- The first tool we will use is ping. Ping is a tool used to test whether a host is reachable. Packets of information are sent to the remote host with instructions to reply. Your local PC measures whether a response is received to each packet, and how long it takes for those packets to cross the network. The name ping comes from active sonar technology in which a pulse of sound is sent underwater and bounced off of terrain or other ships.
- From your PC, click the **Windows Start** icon, type **cmd** in the **Search programs and files** box, and then press Enter.



- At the command-line prompt, type **ping www.cisco.com**.

```
C:\>ping www.cisco.com

Pinging e144.dscb.akamaiedge.net [23.1.48.170] with 32 bytes of data:
Reply from 23.1.48.170: bytes=32 time=56ms TTL=57
Reply from 23.1.48.170: bytes=32 time=55ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57
Reply from 23.1.48.170: bytes=32 time=54ms TTL=57

Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

- The first output line displays the Fully Qualified Domain Name (FQDN) e144.dscb.akamaiedge.net. This is followed by the IP address 23.1.48.170. Cisco hosts the same web content on different servers throughout the world (known as mirrors). Therefore, depending upon where you are geographically, the FQDN and the IP address will be different.
- From this portion of the output:

```
Ping statistics for 23.1.48.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 54ms, Maximum = 56ms, Average = 54ms
```

Four pings were sent and a reply was received from each ping. Because each ping was responded to, there was 0% packet loss. On average, it took 54 ms (54 milliseconds) for the packets to cross the network. A millisecond is 1/1,000th of a second.

Instructor Note: If the first ICMP packet times out, this could be a result of the PC resolving the destination address. This should not occur if you repeat the ping as the address is now cached.

Streaming video and online games are two applications that suffer when there is packet loss, or a slow network connection. A more accurate determination of an Internet connection speed can be determined by sending 100 pings, instead of the default 4. Here is how to do that:

```
C:\>ping -n 100 www.cisco.com
```

And here is what the output from that looks like:

```
Ping statistics for 23.45.0.170:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 46ms, Maximum = 53ms, Average = 49ms
```

- f. Now ping Regional Internet Registry (RIR) websites located in different parts of the world:

For Africa:

```
C:\> ping www.afrinic.net
```

```
C:\>ping www.afrinic.net

Pinging www.afrinic.net [196.216.2.136] with 32 bytes of data:
Reply from 196.216.2.136: bytes=32 time=314ms TTL=111
Reply from 196.216.2.136: bytes=32 time=312ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111
Reply from 196.216.2.136: bytes=32 time=313ms TTL=111

Ping statistics for 196.216.2.136:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 312ms, Maximum = 314ms, Average = 313ms
```

For Australia:

```
C:\> ping www.apnic.net
```

```
C:\>ping www.apnic.net

Pinging www.apnic.net [202.12.29.194] with 32 bytes of data:
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=287ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49
Reply from 202.12.29.194: bytes=32 time=286ms TTL=49

Ping statistics for 202.12.29.194:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 286ms, Maximum = 287ms, Average = 286ms
```

For Europe:

```
C:\> ping www.ripe.net
```

```
C:\>ping www.ripe.net

Pinging www.ripe.net [193.0.6.139] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 193.0.6.139:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

For South America:

```
C:\> ping www.lacnic.net
```

```
C:\>ping www.lacnic.net

Pinging www.lacnic.net [200.3.14.147] with 32 bytes of data:
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=158ms TTL=51
Reply from 200.3.14.147: bytes=32 time=157ms TTL=51

Ping statistics for 200.3.14.147:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 157ms, Maximum = 158ms, Average = 157ms
```

All these pings were run from a computer located in the United States. What happens to the average ping time in milliseconds when data is traveling within the same continent (North America) as compared to data from North America traveling to different continents?

Answer varies based on location. In the data above, the average ping time in milliseconds dramatically increases.

What is interesting about the pings that were sent to the European website?

At the time that these pings were sent, the site was unreachable. Successful pings to a destination indicate the destination is up and running. A number of reasons can lead to unsuccessful pings. A site can be unreachable because it has been configured not to respond to ICMP packets, the firewall is blocking ICMP or there is no route to the site from the machine generating the pings.

Part 2: Trace a Route to a Remote Server Using Tracert

Step 1: Determine what route across the Internet traffic takes to the remote server.

Now that basic reachability has been verified by using the ping tool, it is helpful to look more closely at each network segment that is crossed. To do this, the **tracert** tool will be used.

- a. At the command-line prompt, type **tracert www.cisco.com**.

```
C:\>tracert www.cisco.com

Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2  38 ms     38 ms     37 ms     10.18.20.1
  3  37 ms     37 ms     37 ms     G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4  43 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5  43 ms     43 ms     65 ms     0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
  6  45 ms     45 ms     45 ms     0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
  7  46 ms     48 ms     46 ms     TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

  8  45 ms     45 ms     45 ms     a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

- b. 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: **Windows Start** icon > **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**.

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

```
C:\> tracert www.afrinic.net
```

```
C:\> tracert www.lacnic.net
```

- d. Interpreting **tracert** outputs.

Routes traced can go through many hops and a number of different Internet Service Providers (ISPs), depending on the size of your ISP, and the location of the source and destination hosts. Each “hop” represents a router. A router is a specialized type of computer used to direct traffic across the Internet. Imagine taking an automobile trip across several countries using many highways. At different points in the trip, you come to a fork in the road in which you have the option to select from several different highways. Now further imagine that there is a device at each fork in the road that directs you to take the correct highway to your final destination. That is what a router does for packets on a network.

Because computers talk in numbers, rather than words, routers are uniquely identified using IP addresses (numbers with the format x.x.x.x). The **tracert** tool shows you what path through the network a packet of information takes to reach its final destination. The **tracert** tool also gives you an idea of how fast traffic is going on each segment of the network. Three packets are sent to each router in the path, and the return time is measured in milliseconds. Now use this information to analyze the **tracert** results to www.cisco.com. Below is the entire traceroute:


```
C:\>tracert www.cisco.com

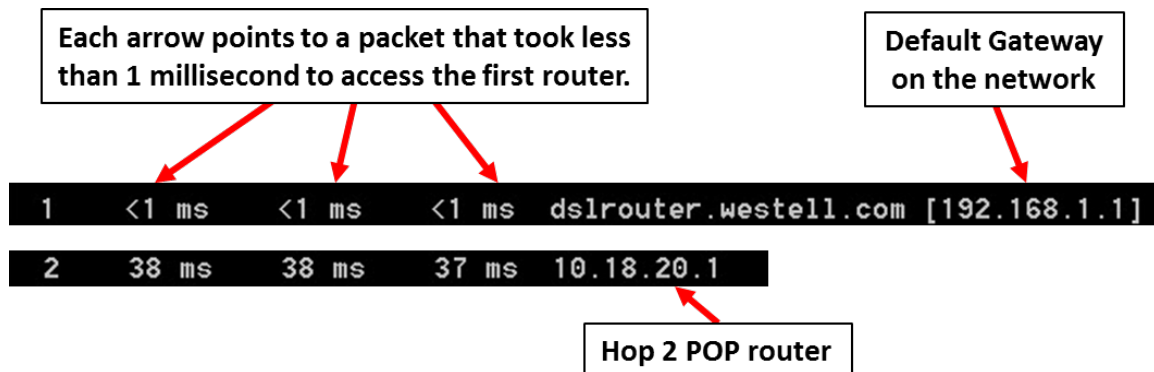
Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]
over a maximum of 30 hops:

 1  <1 ms  <1 ms  <1 ms  dslrouter.westell.com [192.168.1.1]
 2  38 ms  38 ms  37 ms  10.18.20.1
 3  37 ms  37 ms  37 ms  G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.196.190]
 4  43 ms  43 ms  42 ms  so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
 5  43 ms  43 ms  65 ms  0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
 6  45 ms  45 ms  45 ms  0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
 7  46 ms  48 ms  46 ms  TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]

 8  45 ms  45 ms  45 ms  a23-1-144-170.deploy.akamaitechnologies.com [23.
1.144.170]

Trace complete.
```

Below is the breakdown:



In the example output shown above, the tracert packets travel from the source PC to the local router default gateway (hop 1: 192.168.1.1) to the ISPs Point of Presence (POP) router (hop 2: 10.18.20.1). Every ISP has numerous POP routers. These POP routers are at the edge of the ISP's network and are the means by which customers connect to the Internet. The packets travel along the Verizon network for two hops and then jump to a router that belongs to alter.net. This could mean that the packets have traveled to another ISP. This is significant because sometimes there is packet loss in the transition between ISPs, or sometimes one ISP is slower than another. How could we determine if alter.net is another ISP or the same ISP?

- e. There is an Internet tool known as whois. The whois tool allows us to determine who owns a domain name. A web-based whois tool is found at <http://whois.domaintools.com/>. This domain is also owned by Verizon according to the web-based whois tool.

```
Registrant:
Verizon Business Global LLC
Verizon Business Global LLC
One Verizon Way
Basking Ridge NJ 07920
US
domainlegalcontact@verizon.com +1.7033513164 Fax: +1.7033513669

Domain Name: alter.net
```

To summarize, Internet traffic starts at a home PC and travels through the home router (hop 1). It then connects to the ISP and travels through its network (hops 2-7) until it arrives at the remote server (hop 8). This is a relatively unusual example in which there is only one ISP involved from start to finish. It is typical to have two or more ISP involved as displayed in the following examples.

- f. Now examine an example that involves Internet traffic crossing multiple ISPs. Below is the tracert for www.afrinic.net:

```
C:\>tracert www.afrinic.net

Tracing route to www.afrinic.net [196.216.2.136]
over a maximum of 30 hops:

  1    1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2   39 ms   38 ms   37 ms   10.18.20.1
  3   40 ms   38 ms   39 ms   G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.8
1.197.182]
  4   44 ms   43 ms   43 ms   so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5   43 ms   43 ms   42 ms   0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
  6   43 ms   71 ms   43 ms   0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
  7   47 ms   47 ms   47 ms   te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137
]
  8   43 ms   55 ms   43 ms   vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
  9   52 ms   51 ms   51 ms   ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

10  130 ms   132 ms   132 ms   ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
11  139 ms   145 ms   140 ms   ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.13
7]
12  148 ms   140 ms   152 ms   ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14
]
13  144 ms   144 ms   146 ms   ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29
]
14  151 ms   150 ms   150 ms   ae-23-23.ebr2.London1.Level3.net [4.69.148.193]
15  150 ms   150 ms   150 ms   ae-58-223.csw2.London1.Level3.net [4.69.153.138]
16  156 ms   156 ms   156 ms   ae-227-3603.edge3.London1.Level3.net [4.69.166.1
54]
17  157 ms   159 ms   160 ms   195.50.124.34
18  353 ms   340 ms   341 ms   168.209.201.74
19  333 ms   333 ms   332 ms   csw4-pk1-gi1-1.ip.isnet.net [196.26.0.101]
20  331 ms   331 ms   331 ms   196.37.155.180
21  318 ms   316 ms   318 ms   fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
22  332 ms   334 ms   332 ms   196.216.2.136

Trace complete.
```

What happens at hop 7? Is level3.net the same ISP as hops 2-6, or a different ISP? Use the whois tool to answer this question.

The Internet traffic goes from being on alter.net to level3.net. The whois tool reveals that this is a separate company/separate ISP.

What happens in hop 10 to the amount of time it takes for a packet to travel between Washington D.C. and Paris, as compared with the earlier hops 1-9?

In hops 1-9 most packets traverse their link in 50 ms or less. On the Washington D.C. to Paris link, the time increases to 132 ms.

What happens in hop 18? Do a whois lookup on 168.209.201.74 using the whois tool. Who owns this network?

The time to traverse one link in the network goes up from 159 ms to 340 ms. From the increased time, the traffic probably is moved to a different network from the Level3 backbone network. Using the whois tool, IP address (168.209.201.74) is owned by the African Network Information Center.

- g. Type **tracert www.lacnic.net**.

```
C:\>tracert www.lacnic.net

Tracing route to www.lacnic.net [200.3.14.147]
over a maximum of 30 hops:

  1  <1 ms    <1 ms    <1 ms    dslrouter.westell.com [192.168.1.1]
  2  38 ms     38 ms     37 ms     10.18.20.1
  3  38 ms     38 ms     39 ms     G3-0-9-2204.ALBVNY-LCR-02.verizon-gni.net [130.8
1.196.190]
  4  42 ms     43 ms     42 ms     so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81
.22.46]
  5  82 ms     47 ms     47 ms     0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
  6  46 ms     47 ms     56 ms     204.255.168.194
  7  157 ms    158 ms    157 ms    ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
  8  156 ms    157 ms    157 ms    xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]

  9  161 ms    161 ms    161 ms    xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]

 10  158 ms    157 ms    157 ms    ae0-0.ar3.nu.registro.br [200.160.0.249]
 11  176 ms    176 ms    170 ms    gw02.lacnic.registro.br [200.160.0.213]
 12  158 ms    158 ms    158 ms    200.3.12.36
 13  157 ms    158 ms    157 ms    200.3.14.147

Trace complete.
```

What happens in hop 7?

The time it takes for a packet to traverse the network dramatically increases over fourfold from ~40 ms to ~180 ms. Did students do a whois on registro.br using the web-based whois tool: <http://whois.domaintools.com/>. If they did, the information they received was not that helpful. Did your students go to: <http://translate.google.com/> to get a translation of Núcleo de Informação e Coordenação do Ponto? More helpful would have been a search engine request for “top domain .br”. This would have revealed that we are now on a Brazilian network. Internet detective work can be fun!

Reflection

What are the functional differences between the commands ping and tracer?

The ping command generates ICMP packets with TTL=255, the maximum value allowed by the IP protocol. The TTL is set to 255 because ICMP packets generated by ping are designed to go from source to destination, a situation when the distance is unknown.

Each hop in the tracer results displays the routes that the packets take when traveling to the final destination. The tracer command creates ICMP packets and the tracer packets are crafted to reach the next router only. By initially setting the TTL=1 and increasing its value as it receives "TTL expired" messages from the routers in the path from source to destination, tracer is able to display all the routers in the path.

Appendix A

```
C:\> tracert www.cisco.com
```

```
Tracing route to e144.dscb.akamaiedge.net [23.1.144.170]  
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	dslrouter.westell.com [192.168.1.1]
2	38 ms	38 ms	37 ms	10.18.20.1
3	37 ms	37 ms	37 ms	G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.196.190]
4	43 ms	43 ms	42 ms	so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
5	43 ms	43 ms	65 ms	0.so-4-0-2.XT2.NYC4.ALTER.NET [152.63.1.57]
6	45 ms	45 ms	45 ms	0.so-3-2-0.XL4.EWR6.ALTER.NET [152.63.17.109]
7	46 ms	48 ms	46 ms	TenGigE0-5-0-0.GW8.EWR6.ALTER.NET [152.63.21.14]
8	45 ms	45 ms	45 ms	a23-1-144-170.deploy.akamaitechnologies.com [23.1.144.170]

```
Trace complete.
```

```
C:\> tracert www.afrinic.net
```

```
Tracing route to www.afrinic.net [196.216.2.136]  
over a maximum of 30 hops:
```

1	1 ms	<1 ms	<1 ms	dslrouter.westell.com [192.168.1.1]
2	39 ms	38 ms	37 ms	10.18.20.1
3	40 ms	38 ms	39 ms	G4-0-0-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.197.182]
4	44 ms	43 ms	43 ms	so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
5	43 ms	43 ms	42 ms	0.so-4-0-0.XT2.NYC4.ALTER.NET [152.63.9.249]
6	43 ms	71 ms	43 ms	0.ae4.BR3.NYC4.ALTER.NET [152.63.16.185]
7	47 ms	47 ms	47 ms	te-7-3-0.edge2.NewYork2.level3.net [4.68.111.137]
8	43 ms	55 ms	43 ms	vlan51.ebr1.NewYork2.Level3.net [4.69.138.222]
9	52 ms	51 ms	51 ms	ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]

Lab - Mapping the Internet

10	130 ms	132 ms	132 ms	ae-42-42.ebr2.Paris1.Level3.net [4.69.137.53]
11	139 ms	145 ms	140 ms	ae-46-46.ebr1.Frankfurt1.Level3.net [4.69.143.137]
12	148 ms	140 ms	152 ms	ae-91-91.csw4.Frankfurt1.Level3.net [4.69.140.14]
13	144 ms	144 ms	146 ms	ae-92-92.ebr2.Frankfurt1.Level3.net [4.69.140.29]
14	151 ms	150 ms	150 ms	ae-23-23.ebr2.London1.Level3.net [4.69.148.193]
15	150 ms	150 ms	150 ms	ae-58-223.csw2.London1.Level3.net [4.69.153.138]
16	156 ms	156 ms	156 ms	ae-227-3603.edge3.London1.Level3.net [4.69.166.154]
17	157 ms	159 ms	160 ms	195.50.124.34
18	353 ms	340 ms	341 ms	168.209.201.74
19	333 ms	333 ms	332 ms	csw4-pkl-gil-1.ip.isnet.net [196.26.0.101]
20	331 ms	331 ms	331 ms	196.37.155.180
21	318 ms	316 ms	318 ms	fa1-0-1.ar02.jnb.afrinic.net [196.216.3.132]
22	332 ms	334 ms	332 ms	196.216.2.136

Trace complete.

```
C:\> tracert www.lacnic.net
```

Tracing route to lacnic.net [200.3.14.10]
over a maximum of 30 hops:

1	<1 ms	<1 ms	<1 ms	dslrouter.westell.com [192.168.1.1]
2	38 ms	37 ms	37 ms	10.18.20.1
3	37 ms	38 ms	40 ms	G3-0-9-2204.ALBYNY-LCR-02.verizon-gni.net [130.81.196.190]
4	43 ms	42 ms	43 ms	so-5-1-1-0.NY325-BB-RTR2.verizon-gni.net [130.81.22.46]
5	46 ms	75 ms	46 ms	0.ae2.BR3.NYC4.ALTER.NET [152.63.16.49]
6	43 ms	43 ms	43 ms	204.255.168.194
7	178 ms	182 ms	178 ms	ge-1-1-0.100.gw1.gc.registro.br [159.63.48.38]
8	172 ms	180 ms	182 ms	xe-5-0-1-0.core1.gc.registro.br [200.160.0.174]
9	177 ms	172 ms	181 ms	xe-4-0-0-0.core2.nu.registro.br [200.160.0.164]
10	173 ms	180 ms	176 ms	ae0-0.ar3.nu.registro.br [200.160.0.249]
11	184 ms	183 ms	180 ms	gw02.lacnic.registro.br [200.160.0.213]
12	180 ms	179 ms	180 ms	200.3.12.36
13	182 ms	180 ms	180 ms	www.lacnic.net [200.3.14.10]

Trace complete.

Class Activity - The Internet of Everything...Naturally! (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain the need for IPv6 network addresses.

Background /Scenario

Note: This activity may be completed individually or in small/large groups.

This chapter discussed the ways that small to medium-sized businesses are connected to networks in groups. The IoE was introduced in the modeling activity at the beginning of this chapter.

For this activity, choose one of the following:

- Online banking
- World news
- Weather forecasting/climate
- Traffic conditions

Devise an IPv6 addressing scheme for the area you have chosen. Your addressing scheme should include how you would plan for:

- Subnetting
- Unicasts
- Multicasts

Keep a copy of your scheme to share with the class or learning community. Be prepared to explain:

- how subnetting, unicasts, and multicasts could be incorporated
- where your addressing scheme could be used
- how small to medium-size businesses would be affected by using your plan

Instructor Note: This optional Modeling Activity is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their perceptions of how a network could use IPv6 and the undecillion addresses available both for personal and corporate practice. Instructors should facilitate class discussion and idea sharing as a result of this activity.

Required Resources

- Paper, pens or pencils, or tablets
- Packet Tracer (if you would like to display how your network would look physically)
- Hard or soft copy of the final network topology with IPv6 addressing indicated for sharing with the class.

Reflection

What was the hardest part of designing this network model? Explain your answer.

Answers will vary within groups (as will the topologies developed). Some students may mention designing a main group and then subnetted groups from the main group, some may indicate the actual addressing of the network, some may indicate they had difficulty with where unicasts and multicasts could occur.

A possible solution to the scenario might include:

Weather Forecasting/Climate

The area in which you live has many hot days during summer months. Electricity costs skyrocket on those days.

Your local electrical area includes 6 local cities and all of these cities are then incorporated into one, large state. Multiple states are incorporated into one large country. To decrease costs and increase productivity of electricity, you could install windmills or solar panels that would generate electrical current to your immediate area and larger geographic areas. The windmills or solar panels could be controlled using network accessibility.

Using an IPv6 addressing scheme:

- Each windmill (or solar panel) will be assigned an IPv6 address.
- Windmills and/or solar panels will be turned on to generate electricity by, city, state or country (subnetting).
- Cities, states or countries will receive additional electricity based on unicast or multicast operation of the windmills/solar panels.

Note: Depending on the focus or use of this activity, students could actually draw a schematic of their windmills or solar panels and address them to show mastery of the subnetting concept. They could also group the windmills or solar panels to show unicast or multicast transmissions types.

Other possible scenarios might include:

1. Energy Efficiency

- Each household light bulb could be connected to the network and remotely managed. Each one would therefore need an IPv6 address.

- Each home appliance should also be connected to the network and would also need IPv6.

- The network structure could group all appliances of a home into one subnet. Route summaries could be created to group neighborhoods together. Unicast messages would be used to manage single devices. Appliances of the same type could have a multicast group (all TVs, for instance) and managed in bulk.

2. Weather Forecast

- Sensor on trees would need IPv6 addresses to be connected to the network

- Mobile weather stations would also need IPv6 (several stations per city, for accuracy)

- Floating weather stations would gather info about the oceans and rivers and also need IPv6

- Once again route summaries would group/represent physical locations. Multicast groups could be created based on station placement (land, river, and ocean) and unicast addresses used to manage a specific station

3. Traffic Conditions

- Each traffic light would need an IPv6 to be connected to the network.

- Road traffic sensors (to provide the rate vehicle/minute) could also be connected to the network and would need IPv6 addresses.

- Multicast groups could be created based on device type (sensor or traffic light) and unicast addresses could be used to manage a specific device.

Identify elements of the model that map IT-related content:

- Internet of Everything (IoE) – green technology
- Subnetting
- IPv6 addressing
- Unicasts
- Multicasts

Class Activity - Call Me! (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain why routing is necessary for hosts on different subnets to communicate.

Background /Scenario

In this chapter, you will be learning how devices can be grouped into subnets, or smaller network groups, from a large network.

In this modeling activity, you are asked to think about a number you probably use every day, a number such as your telephone number. As you complete the activity, think about how your telephone number compares to strategies that network administrators might use to identify hosts for efficient data communication.

Complete the two sections listed below and record your answers. Save the two sections in either hard- or soft-copy format to use later for class discussion purposes.

- Explain how your smartphone or landline telephone number is divided into identifying groups of numbers. Does your telephone number use an area code? An ISP identifier? A city, state, or country code?
- In what ways does separating your telephone number into managed parts assist in contacting or communicating with others?

Instructor Note: This is an individual or an in-class small/large group modeling activity. It is not intended to be a graded assignment. Its purpose is to encourage students to reflect on their current knowledge of how networks are grouped using a numerical basis. Facilitation of the discussion should be initiated as a result of this Activity.

Instructor Note: Please have students adjust their answers to incorporate a country area code if necessary.

Required Resources

- Recording capabilities (paper, tablet, etc.) for reflective comments to be shared with the class.

Reflection

Why do you think ISPs need your telephone number when setting up your account parameters?

Example telephone number and identifying groups in that telephone number (if your country uses another identifier, it would need to be incorporated into this section's answers:

Area Code (or ISP identifier)	City	Telephone Identifier
571	555	1212

571 directs calls from my telephone showing the general, geographic location of my ISP or state. I wish to call someone in another state or through a different ISP, the area code or ISP identifier will be different.

555 indicates the city from which I am calling and this helps to route my communications to the correct switches or routers.

1212 indicates my personal smartphone or landline telephone identifier when combined with the first two groups. This enables my telephone to receive the communication after being processed, generally, through my area code/ISP and city identifiers.

Identify elements of the model that map to IT-related content:

- Hierarchies are employed when using addressing schemes
- Connectivity is influenced by the addressing scheme identifiers

Lab – Calculating IPv4 Subnets (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Determine IPv4 Address Subnetting

Part 2: Calculate IPv4 Address Subnetting

Background / Scenario

The ability to work with IPv4 subnets and determine network and host information based on a given IP address and subnet mask is critical to understanding how IPv4 networks operate. The first part is designed to reinforce how to compute network IP address information from a given IP address and subnet mask. When given an IP address and subnet mask, you will be able to determine other information about the subnet.

Instructor Note: This activity can be done in class or assigned as homework. If the assignment is done in class, you may wish to have students work alone or in teams of 2 students each. It is suggested that the first problem is done together in class to give students guidance as to how to proceed for the rest of the assignment.

The public IP addresses used in this lab are owned by Cisco.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)
- Optional: IPv4 address calculator

Part 1: Determine IPv4 Address Subnetting

In Part 1, you will determine the network and broadcast addresses, as well as the number of hosts, given an IPv4 address and subnet mask.

REVIEW: To determine the network address, perform binary ANDing on the IPv4 address using the subnet mask provided. The result will be the network address. Hint: If the subnet mask has decimal value 255 in an octet, the result will ALWAYS be the original value of that octet. If the subnet mask has decimal value 0 in an octet, the result will ALWAYS be 0 for that octet.

Example:

IP Address	192.168.10.10
Subnet Mask	255.255.255.0
	=====
Result (Network)	192.168.10.0

Knowing this, you may only have to perform binary ANDing on an octet that does not have 255 or 0 in its subnet mask portion.

Example:

IP Address	172.30.239.145
Subnet Mask	255.255.192.0

Analyzing this example, you can see that you only have to perform binary ANDing on the third octet. The first two octets will result in 172.30 due to the subnet mask. The fourth octet will result in 0 due to the subnet mask.

IP Address 172.30.239.145

Subnet Mask 255.255.192.0

=====

Result (Network) 172.30.?.0

Perform binary ANDing on the third octet.

Decimal **Binary**

239 11101111

192 11000000

=====

Result **192** 11000000

Analyzing this example again produces the following result:

IP Address 172.30.239.145

Subnet Mask 255.255.192.0

=====

Result (Network) 172.30.192.0

Continuing with this example, determining the number of hosts per network can be calculated by analyzing the subnet mask. The subnet mask will be represented in dotted decimal format, such as 255.255.192.0, or in network prefix format, such as /18. An IPv4 address always has 32 bits. Subtracting the number of bits used for the network portion (as represented by the subnet mask) gives you the number of bits used for hosts.

Using our example above, the subnet mask 255.255.192.0 is equivalent to /18 in prefix notation. Subtracting 18 network bits from 32 bits results in 14 bits left for the host portion. From there, it is a simple calculation:

$$2^{(\text{number of host bits})} - 2 = \text{Number of hosts}$$

$$2^{14} = 16,384 - 2 = 16,382 \text{ hosts}$$

Determine the network and broadcast addresses and number of host bits and hosts for the given IPv4 addresses and prefixes in the following table.

IPv4 Address/Prefix	Network Address	Broadcast Address	Total Number of Host Bits	Total Number of Hosts
192.168.100.25/28	192.168.100.16	192.168.100.31	4	14
172.30.10.130/30	172.30.10.128	172.30.10.131	2	2
10.1.113.75/19	10.1.96.0	10.1.127.255	13	8190
198.133.219.250/24	198.133.219.0	198.133.219.255	8	254
128.107.14.191/22	128.107.12.0	128.107.15.255	10	1022
172.16.104.99/27	172.16.104.96	172.16.104.127	5	30

Part 2: Calculate IPv4 Address Subnetting

When given an IPv4 address, the original subnet mask and the new subnet mask, you will be able to determine:

- Network address of this subnet

- Broadcast address of this subnet
- Range of host addresses of this subnet
- Number of subnets created
- Number of hosts per subnet

The following example shows a sample problem along with the solution for solving this problem:

Given:	
Host IP Address:	172.16.77.120
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.240.0
Find:	
Number of Subnet Bits	4
Number of Subnets Created	16
Number of Host Bits per Subnet	12
Number of Hosts per Subnet	4,094
Network Address of this Subnet	172.16.64.0
IPv4 Address of First Host on this Subnet	172.16.64.1
IPv4 Address of Last Host on this Subnet	172.16.79.254
IPv4 Broadcast Address on this Subnet	172.16.79.255

Let's analyze how this table was completed.

The original subnet mask was 255.255.0.0 or /16. The new subnet mask is 255.255.240.0 or /20. The resulting difference is 4 bits. Because 4 bits were borrowed, we can determine that 16 subnets were created because $2^4 = 16$.

The new mask of 255.255.240.0 or /20 leaves 12 bits for hosts. With 12 bits left for hosts, we use the following formula: $2^{12} = 4,096 - 2 = 4,094$ hosts per subnet.

Binary ANDing will help you determine the subnet for this problem, which results in the network 172.16.64.0.

Finally, you need to determine the first host, last host, and broadcast address for each subnet. One method to determine the host range is to use binary math for the host portion of the address. In our example, the last 12 bits of the address is the host portion. The first host would have all significant bits set to zero and the least significant bit set to 1. The last host would have all significant bits set to 1 and the least significant bit set to 0. In this example, the host portion of the address resides in the 3rd and 4th octets.

Description	1 st Octet	2 nd Octet	3 rd Octet	4 th Octet	Description
Network/Host	nnnnnnnn	nnnnnnnn	nnnnhhhh	hhhhhhhh	Subnet Mask
Binary	10101100	00010000	01000000	00000001	First Host
Decimal	172	16	64	1	First Host
Binary	10101100	00010000	01001111	11111110	Last Host
Decimal	172	16	79	254	Last Host
Binary	10101100	00010000	01001111	11111111	Broadcast
Decimal	172	16	79	255	Broadcast

Step 1: Fill out the tables below with appropriate answers given the IPv4 address, original subnet mask, and new subnet mask.

a. Problem 1:

Given:	
Host IP Address:	192.168.200.139
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.224
Find:	
Number of Subnet Bits	3
Number of Subnets Created	8
Number of Host Bits per Subnet	5
Number of Hosts per Subnet	30
Network Address of this Subnet	192.168.200.128
IPv4 Address of First Host on this Subnet	192.168.200.129
IPv4 Address of Last Host on this Subnet	192.168.200.158
IPv4 Broadcast Address on this Subnet	192.168.200.159

b. Problem 2:

Given:	
Host IP Address:	10.101.99.228
Original Subnet Mask	255.0.0.0
New Subnet Mask:	255.255.128.0
Find:	
Number of Subnet Bits	9
Number of Subnets Created	512
Number of Host Bits per Subnet	15
Number of Hosts per Subnet	32,766
Network Address of this Subnet	10.101.0.0
IPv4 Address of First Host on this Subnet	10.101.0.1
IPv4 Address of Last Host on this Subnet	10.101.127.254
IPv4 Broadcast Address on this Subnet	10.101.127.255

c. Problem 3:

Given:	
Host IP Address:	172.22.32.12
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.224.0
Find:	
Number of Subnet Bits	3
Number of Subnets Created	8
Number of Host Bits per Subnet	13
Number of Hosts per Subnet	8,190
Network Address of this Subnet	172.22.32.0
IPv4 Address of First Host on this Subnet	172.22.32.1
IPv4 Address of Last Host on this Subnet	172.22.63.254
IPv4 Broadcast Address on this Subnet	172.22.63.255

d. Problem 4:

Given:	
Host IP Address:	192.168.1.245
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.252
Find:	
Number of Subnet Bits	6
Number of Subnets Created	64
Number of Host Bits per Subnet	2
Number of Hosts per Subnet	2
Network Address of this Subnet	192.168.1.244
IPv4 Address of First Host on this Subnet	192.168.1.245
IPv4 Address of Last Host on this Subnet	192.168.1.246
IPv4 Broadcast Address on this Subnet	192.168.1.247

e. Problem 5:

Given:	
Host IP Address:	128.107.0.55
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.255.0
Find:	
Number of Subnet Bits	8
Number of Subnets Created	256
Number of Host Bits per Subnet	8
Number of Hosts per Subnet	254
Network Address of this Subnet	128.107.0.0
IPv4 Address of First Host on this Subnet	128.107.0.1
IPv4 Address of Last Host on this Subnet	128.107.0.254
IPv4 Broadcast Address on this Subnet	128.107.0.255

f. Problem 6:

Given:	
Host IP Address:	192.135.250.180
Original Subnet Mask	255.255.255.0
New Subnet Mask:	255.255.255.248
Find:	
Number of Subnet Bits	5
Number of Subnets Created	32
Number of Host Bits per Subnet	3
Number of Hosts per Subnet	6
Network Address of this Subnet	192.135.250.176
IPv4 Address of First Host on this Subnet	192.135.250.177
IPv4 Address of Last Host on this Subnet	192.135.250.182
IPv4 Broadcast Address on this Subnet	192.135.250.183

Reflection

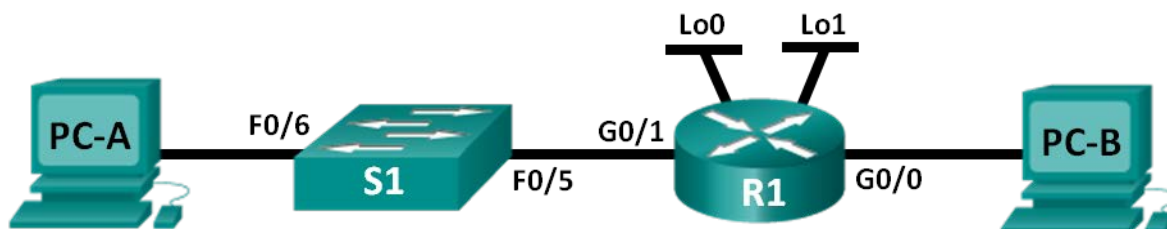
Why is the subnet mask so important when analyzing an IPv4 address?

The subnet mask determines everything about the address: the network, number of host bits, number of hosts and the broadcast address. Merely looking at an IPv4 address tells you nothing. You need the subnet mask to fill in all the important pieces of information.

Lab - Designing and Implementing a Subnetted IPv4 Addressing Scheme (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0			N/A
	G0/1			N/A
	Lo0			N/A
	Lo1			N/A
S1	VLAN 1	N/A	N/A	N/A
PC-A	NIC			
PC-B	NIC			

Objectives

Part 1: Design a Network Subnetting Scheme

Part 2: Configure the Devices

Part 3: Test and Troubleshoot the Network

Background / Scenario

In this lab, starting from a single network address and network mask, you will subnet the network into multiple subnets. The subnet scheme should be based on the number of host computers required in each subnet, as well as other network considerations, like future network host expansion.

After you have created a subnetting scheme and completed the network diagram by filling in the host and interface IP addresses, you will configure the host PCs and router interfaces, including loopback interfaces. The loopback interfaces are created to simulate additional LANs attached to router R1.

After the network devices and host PCs have been configured, you will use the **ping** command to test for network connectivity.

This lab provides minimal assistance with the actual commands necessary to configure the router. However, the required commands are provided in Appendix A. Test your knowledge by trying to configure the devices without referring to the appendix.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at this end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Gigabit Ethernet interfaces on Cisco 1941 routers are autosensing. An Ethernet straight-through cable may be used between the router and PC-B. If using another Cisco router model, it may be necessary to use an Ethernet crossover cable.

Part 1: Design a Network Subnetting Scheme

Step 1: Create a subnetting scheme that meets the required number of subnets and required number of host addresses.

In this scenario, you are a network administrator for a small subdivision within a larger company. You must create multiple subnets out of the 192.168.0.0/24 network address space to meet the following requirements:

- The first subnet is the employee network. You need a minimum of 25 host IP addresses.
- The second subnet is the administration network. You need a minimum of 10 IP addresses.
- The third and fourth subnets are reserved as virtual networks on virtual router interfaces, loopback 0 and loopback 1. These virtual router interfaces simulate LANs attached to R1.
- You also need two additional unused subnets for future network expansion.

Note: Variable length subnet masks will not be used. All of the device subnet masks will be the same length.

Answer the following questions to help create a subnetting scheme that meets the stated network requirements:

- 1) How many host addresses are needed in the largest required subnet? _____ **25**
- 2) What is the minimum number of subnets required? _____

The requirements stated above specify two company networks plus two loopback virtual networks, plus two additional networks for future expansion. So, the answer is a minimum of six networks.

- 3) The network that you are tasked to subnet is 192.168.0.0/24. What is the /24 subnet mask in binary?

11111111.11111111.11111111.00000000

- 4) The subnet mask is made up of two portions, the network portion, and the host portion. This is represented in the binary by the ones and the zeros in the subnet mask.

In the network mask, what do the ones represent? _____

The ones represent the network portion.

In the network mask, what do the zeros represent? _____

The zeroes represent the host portion.

- 5) To subnet a network, bits from the host portion of the original network mask are changed into subnet bits. The number of subnet bits defines the number of subnets. Given each of the possible subnet masks depicted in the following binary format, how many subnets and how many hosts are created in each example?

Hint: Remember that the number of host bits (to the power of 2) defines the number of hosts per subnet (minus 2), and the number of subnet bits (to the power of two) defines the number of subnets. The subnet bits (depicted in bold type face) are the bits that have been borrowed beyond the original network mask of /24. The /24 is the slash prefix notation and corresponds to a dotted decimal mask of 255.255.255.0.

(/25) 11111111.11111111.11111111.**1**0000000

Dotted decimal subnet mask equivalent: _____

255.255.255.128

Number of subnets? _____, Number of hosts? _____

Two subnets (2^1) and 128 hosts (2^7) – 2 = 126 hosts per subnet

(/26) 11111111.11111111.11111111.**11**000000

Dotted decimal subnet mask equivalent: _____

255.255.255.192

Number of subnets? _____, Number of hosts? _____

Four subnets (2^2) and 64 hosts (2^6) – 2 = 62 hosts per subnet

(/27) 11111111.11111111.11111111.**111**00000

Dotted decimal subnet mask equivalent: _____

255.255.255.224

Number of subnets? _____ Number of hosts? _____

Eight subnets (2^3) and 32 hosts (2^5) – 2 = 30 hosts per subnet

(/28) 11111111.11111111.11111111.**1111**0000

Dotted decimal subnet mask equivalent: _____

255.255.255.240

Number of subnets? _____ Number of hosts? _____

Sixteen subnets (2^4) and 16 hosts (2^4) – 2 = 14 hosts per subnet

(/29) 11111111.11111111.11111111.**11111**000

Dotted decimal subnet mask equivalent: _____

255.255.255.248

Number of subnets? _____ Number of hosts? _____

Thirty two subnets (2^5) and 8 hosts ($2^3 - 2 = 6$ hosts per subnet)

(/30) 11111111.11111111.11111111.11111100

Dotted decimal subnet mask equivalent: _____

255.255.255.252

Number of subnets? _____ Number of hosts? _____

Sixty four subnets (2^6) and 4 hosts ($2^2 - 2 = 2$ hosts per subnet)

- 6) Considering your answers, which subnet masks meet the required number of minimum host addresses?

/25, /26, /27

- 7) Considering your answers, which subnet masks meets the minimum number of subnets required?

/27, /28, /29, /30 will give the required number of subnets.

- 8) Considering your answers, which subnet mask meets both the required minimum number of hosts and the minimum number of subnets required?

/27 will give you eight subnets, which is greater than the minimum of five required, and 30 hosts per subnet, which is greater than the 25 hosts required for the first subnet.

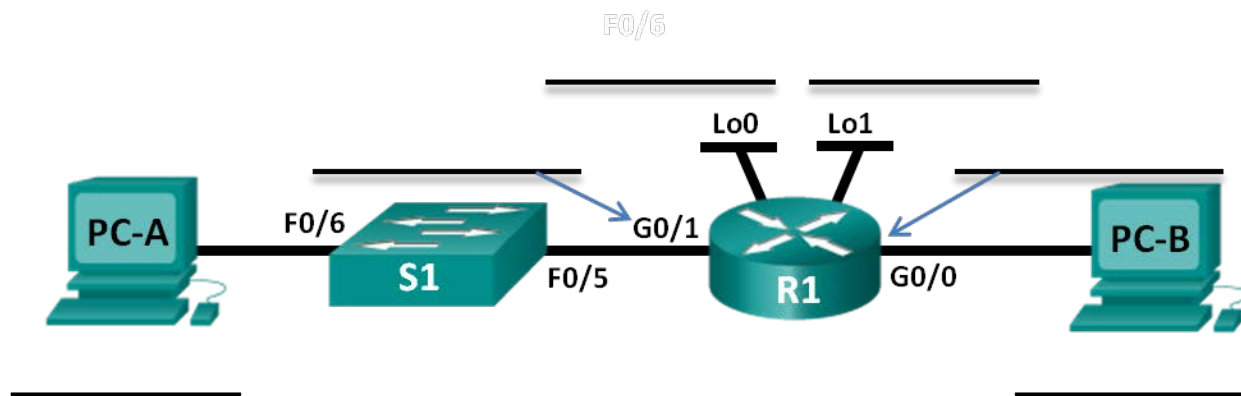
- 9) When you have determined which subnet mask meets all of the stated network requirements, you will derive each of the subnets starting from the original network address. List the subnets from first to last below. Remember that the first subnet is 192.168.0.0 with the newly acquired subnet mask.

Subnet Address	/	Prefix	Subnet Mask (dotted decimal)
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____
_____	/	_____	_____

192.168.0.0, 192.168.0.32, 192.168.0.64, 192.168.0.96, 192.168.0.128, 192.168.0.160, 192.168.0.192, 192.168.0.224 All prefix is /27. All subnet mask is (dotted decimal) 255.255.255.224.

Step 2: Complete the diagram showing where the host IP addresses will be applied.

On the following lines provided, fill in the IP addresses and subnets masks in slash prefix notation. On the router, use the first usable address in each subnet for each of the interfaces, Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0, and loopback 1. Fill in an IP address for both PC-A and PC-B. Also enter this information into the Addressing Table on Page 1.



The addresses of the router Gigabit Ethernet 0/0, Gigabit Ethernet 0/1, loopback 0 and loopback 1 interfaces would be: 192.168.0.1/27, 192.168.0.33/27, 192.168.0.65/27, 192.168.0.97/27. If the Gigabit 0/0 interface is the first subnet then PC-B's IP address would be a number between 192.168.0.2 and 192.168.0.30. If the Gigabit 0/1 interface is the second subnet, then PC-A's IP address would be a number between 192.168.0.34 and 192.168.0.62.

Part 2: Configure the Devices

In Part 2, set up the network topology and configure basic settings on the PCs and router, such as the router Gigabit Ethernet interface IP addresses, and the PC's IP addresses, subnet masks, and default gateways. Refer to the Addressing Table for device names and address information.

Note: Appendix A provides configuration details for the steps in Part 2. You should attempt to complete Part 2 prior to reviewing Appendix A.

Step 1: Configure the router.

- Enter into privileged EXEC mode and then global config mode.
- Assign the **R1** as the hostname for the router.
- Configure both the **G0/0** and **G0/1** interfaces with IP addresses and subnet masks, and then enable them.
- Loopback interfaces are created to simulate additional LANs on R1 router. Configure the loopback interfaces with IP addresses and subnet masks. After they are created, loopback interfaces are enabled, by default. (To create the loopback addresses, enter the command **interface loopback 0** at the global config mode)

Note: You can create additional loopbacks for testing with different addressing schemes, if desired.

- Save the running configuration to the startup configuration file.

Step 2: Configure the PC interfaces.

- Configure the IP address, subnet mask, and default gateway settings on PC-A.
- Configure the IP address, subnet mask, and default gateway settings on PC-B.

Part 3: Test and Troubleshoot the Network

In Part 3, you will use the **ping** command to test network connectivity.

- Test to see if PC-A can communicate with its default gateway. From PC-A, open a command prompt and ping the IP address of the router Gigabit Ethernet 0/1 interface. Do you get a reply? _____

Lab - Designing and Implementing a Subnetted IPv4 Addressing Scheme

If the PC and router interface have been configured correctly then the ping should be successful. If not, check items d and e below.

- b. Test to see if PC-B can communicate with its default gateway. From PC-B, open a command prompt and ping the IP address of the router Gigabit Ethernet 0/0 interface. Do you get a reply? _____

If the PC and router interface have been configured correctly then the ping should be successful. If not, check items d and e below.

- c. Test to see if PC-A can communicate with PC-B. From PC-A, open a command prompt and ping the IP address of PC-B. Do you get a reply? _____

If both PCs and the router Gigabit Ethernet interfaces have been configured correctly, then the pings should be successful. If not, check items d and e below.

- d. If you answered “no” to any of the preceding questions, then you should go back and check all of your IP address and subnet mask configurations, and ensure that the default gateways have been correctly configured on PC-A and PC-B.
- e. If you verify that all of the settings are correct, and you can still not ping successfully, then there are a few additional factors that can block ICMP pings. On PC-A and PC-B within Windows, make sure that the Windows Firewall is turned off for the Work, Home, and Public networks.
- f. Experiment by purposely misconfiguring the gateway address on PC-A to 10.0.0.1. What happens when you try and ping from PC-B to PC-A? Do you receive a reply?
- _____
- _____

With deliberate misconfigurations, the answer should be no.

Reflection

1. Subnetting one larger network into multiple smaller subnetworks allows for greater flexibility and security in network design. However, what do you think some of the drawbacks are when the subnets are limited to being the same size?
- _____
- _____

Answers will vary. Students may suggest that, because some subnetworks require many ip addresses and others require only a few, having all of the subnets the same size is not the most efficient way to divide the subnets.

2. Why do you think the gateway/router IP address is usually the first usable IP address in the network?
- _____
- _____

Answers will vary. It may be suggested that the router or gateway is like a door to the network and therefore it is logical that its address is at the beginning of the network. It is purely a convention however, and therefore the router does not have to have the first or last address in the network.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Appendix A: Configuration Details for Steps in Part 2

Step 1: Configure the router.

- Console into the router and enable privileged EXEC mode.

```
Router> enable
Router#
```

- Enter into configuration mode.

```
Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

- Assign a device name to the router.

```
Router(config)# hostname R1
R1(config)#
```

- Configure both the **G0/0** and **G0/1** interfaces with IP addresses and subnet masks, and enable them.

```
R1(config)# interface g0/0
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# no shutdown
R1(config-if)# interface g0/1
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# no shutdown
```


- e. Loopback interfaces are created to simulate additional LANs off of router R1. Configure the loopback interfaces with IP addresses and subnet masks. When they are created, loopback interfaces are enabled, by default.

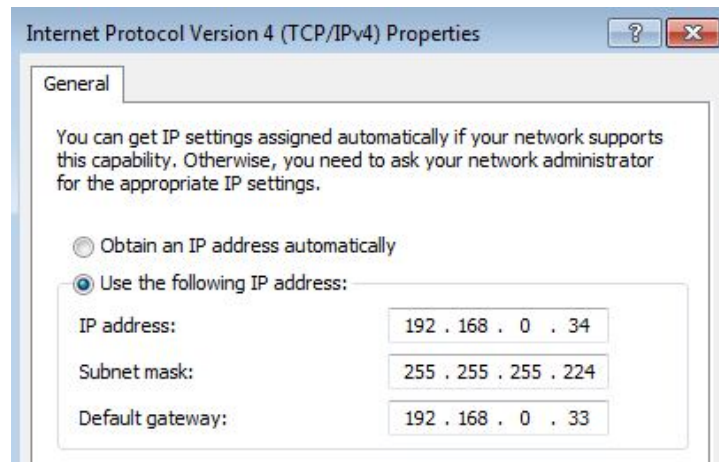
```
R1(config)# interface loopback 0
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# interface loopback 1
R1(config-if)# ip address <ip address> <subnet mask>
R1(config-if)# end
```

- f. Save the running configuration to the startup configuration file.

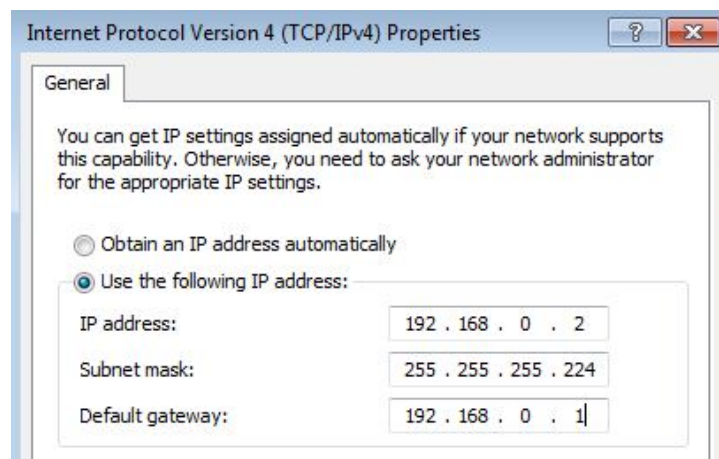
```
R1# copy running-config startup-config
```

Step 2: Configure the PC interfaces.

- a. Configure the IP address, subnet mask, and default gateway settings on PC-A.



- b. Configure the IP address, subnet mask, and default gateway settings on PC-B.



Device Configs

Router R1

```
R1#show run
Building configuration...

Current configuration : 1518 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
no ipv6 cef
ip auth-proxy max-login-attempts 5
ip admission max-login-attempts 5
!
!
!
!
!
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
!
!
!
redundancy
!
!
!
!
interface Loopback0
 ip address 192.168.0.65 255.255.255.224
!
```

```
interface Loopback1
 ip address 192.168.0.97 255.255.255.224
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.0.1 255.255.255.224
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.0.33 255.255.255.224
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
```

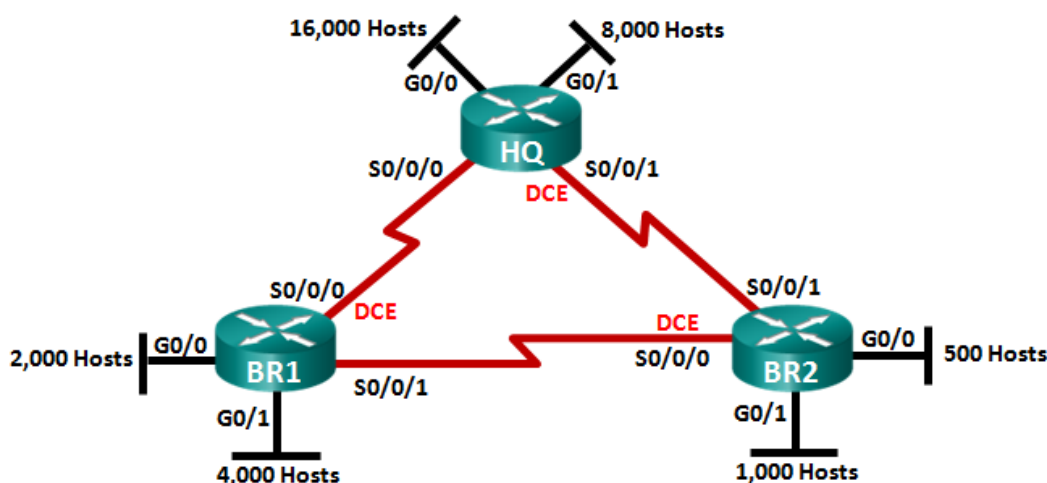
Lab - Designing and Implementing a Subnetted IPv4 Addressing Scheme

```
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Lab – Designing and Implementing a VLSM Addressing Scheme (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Objectives

Part 1: Examine Network Requirements

Part 2: Design the VLSM Address Scheme

Part 3: Cable and Configure the IPv4 Network

Background / Scenario

Variable Length Subnet Mask (VLSM) was designed to avoid wasting IP addresses. With VLSM, a network is subnetted and then re-subnetted. This process can be repeated multiple times to create subnets of various sizes based on the number of hosts required in each subnet. Effective use of VLSM requires address planning.

In this lab, use the 172.16.128.0/17 network address to develop an address scheme for the network displayed in the topology diagram. VLSM is used to meet the IPv4 addressing requirements. After you have designed the VLSM address scheme, you will configure the interfaces on the routers with the appropriate IP address information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). Other routers and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

This lab can be performed in multiple sessions if time is an issue. Parts 1 and 2 are paper based and can be assigned as homework. Part 3 is Hands-on and requires lab equipment.

It is worth noting to the students that as a network administrator, you would not have a single network with over 1000 hosts. You would break these down further in a production network.

Required Resources

- 3 routers (Cisco 1941 with Cisco IOS software, Release 15.2(4)M3 universal image or comparable)
- 1 PC (with terminal emulation program, such as Tera Term, to configure routers)
- Console cable to configure the Cisco IOS devices via the console ports
- Ethernet (optional) and serial cables, as shown in the topology
- Windows Calculator (optional)

Part 1: Examine Network Requirements

In Part 1, you will examine the network requirements to develop a VLSM address scheme for the network displayed in the topology diagram using the 172.16.128.0/17 network address.

Note: You can use the Windows Calculator application and the www.ipcalc.org IP subnet calculator to help with your calculations.

Step 1: Determine how many host addresses and subnets are available.

How many host addresses are available in a /17 network? _____ 32,766

What is the total number of host addresses needed in the topology diagram? _____ 31,506

How many subnets are needed in the network topology? _____ 9

Step 2: Determine the largest subnet.

What is the subnet description (e.g. BR1 G0/1 LAN or BR1-HQ WAN link)? _____ HQ G0/0 LAN

How many IP addresses are required in the largest subnet? _____ 16,000

What subnet mask can support that many host addresses?

_____ /18 or 255.255.192.0

How many total host addresses can that subnet mask support? _____ 16,382

Can you subnet the 172.16.128.0/17 network address to support this subnet? _____ yes

What are the two network addresses that would result from this subnetting?

_____ 172.16.128.0/18

_____ 172.16.192.0/18

Use the first network address for this subnet.

Step 3: Determine the second largest subnet.

What is the subnet description? _____ HQ G0/1 LAN

How many IP addresses are required for the second largest subnet? _____ 8,000

What subnet mask can support that many host addresses?

_____ /19 or 255.255.224.0

How many total host addresses can that subnet mask support? _____ 8,190

Can you subnet the remaining subnet again and still support this subnet? _____ **yes**

What are the two network addresses that would result from this subnetting?

_____ **172.16.192.0/19**

_____ **172.16.224.0/19**

Use the first network address for this subnet.

Step 4: Determine the next largest subnet.

What is the subnet description? _____ **BR1 G0/1 LAN**

How many IP addresses are required for the next largest subnet? _____ **4,000**

What subnet mask can support that many host addresses?

_____ **/20 or 255.255.240.0**

How many total host addresses can that subnet mask support? _____ **4,094**

Can you subnet the remaining subnet again and still support this subnet? _____ **yes**

What are the two network addresses that would result from this subnetting?

_____ **172.16.224.0/20**

_____ **172.16.240.0/20**

Use the first network address for this subnet.

Step 5: Determine the next largest subnet.

What is the subnet description? _____ **BR1 G0/0 LAN**

How many IP addresses are required for the next largest subnet? _____ **2,000**

What subnet mask can support that many host addresses?

_____ **/21 or 255.255.248.0**

How many total host addresses can that subnet mask support? _____ **2,046**

Can you subnet the remaining subnet again and still support this subnet? _____ **yes**

What are the two network addresses that would result from this subnetting?

_____ **172.16.240.0/21**

_____ **172.16.248.0/21**

Use the first network address for this subnet.

Step 6: Determine the next largest subnet.

What is the subnet description? _____ **BR2 G0/1 LAN**

How many IP addresses are required for the next largest subnet? _____ **1,000**

What subnet mask can support that many host addresses?

_____ **/22 or 255.255.252.0**

How many total host addresses can that subnet mask support? _____ **1,022**

Can you subnet the remaining subnet again and still support this subnet? _____ **yes**

What are the two network addresses that would result from this subnetting?

_____ 172.16.248.0/22

_____ 172.16.252.0/22

Use the first network address for this subnet.

Step 7: Determine the next largest subnet.

What is the subnet description? _____ BR2 G0/0 LAN

How many IP addresses are required for the next largest subnet? _____ 500

What subnet mask can support that many host addresses?

_____ /23 or 255.255.254.0

How many total host addresses can that subnet mask support? _____ 510

Can you subnet the remaining subnet again and still support this subnet? _____ yes

What are the two network addresses that would result from this subnetting?

_____ 172.16.252.0/23

_____ 172.16.254.0/23

Use the first network address for this subnet.

Step 8: Determine the subnets needed to support the serial links.

How many host addresses are required for each serial subnet link? _____ 2

What subnet mask can support that many host addresses?

_____ /30 or 255.255.255.252

- a. Continue subnetting the first subnet of each new subnet until you have four /30 subnets. Write the first three network addresses of these /30 subnets below.

_____ 172.16.254.0/30

_____ 172.16.254.4/30

_____ 172.16.254.8/30

- b. Enter the subnet descriptions for these three subnets below.

_____ HQ - BR1 Serial Link

_____ HQ - BR2 Serial Link

_____ BR1 - BR2 Serial Link

Part 2: Design the VLSM Addressing Scheme

Step 1: Calculate the subnet information.

Use the information that you obtained in Part 1 to fill in the following table.

Subnet Description	Number of Hosts Needed	Network Address /CIDR	First Host Address	Broadcast Address
HQ G0/0	16,000	172.16.128.0/18	172.16.128.1	172.16.191.255
HQ G0/1	8,000	172.16.192.0/19	172.16.192.1	172.16.223.255
BR1 G0/1	4,000	172.16.224.0/20	172.16.224.1	172.16.239.255
BR1 G0/0	2,000	172.16.240.0/21	172.16.240.1	172.16.247.255
BR2 G0/1	1,000	172.16.248.0/22	172.16.248.1	172.16.251.255
BR2 G0/0	500	172.16.252.0/23	172.16.252.1	172.16.253.255
HQ S0/0/0 – BR1 S0/0/0	2	172.16.254.0/30	172.16.254.1	172.16.254.3
HQ S0/0/1 – BR2 S0/0/1	2	172.16.254.4/30	172.16.254.5	172.16.254.7
BR1 S0/0/1 – BR2 S0/0/0	2	172.16.254.8/30	172.16.254.9	172.168.254.11

Step 2: Complete the device interface address table.

Assign the first host address in the subnet to the Ethernet interfaces. HQ should be given the first host address on the Serial links to BR1 and BR2. BR1 should be given the first host address for the serial link to BR2.

Device	Interface	IP Address	Subnet Mask	Device Interface
HQ	G0/0	172.16.128.1	255.255.192.0	16,000 Host LAN
	G0/1	172.16.192.1	255.255.224.0	8,000 Host LAN
	S0/0/0	172.16.254.1	255.255.255.252	BR1 S0/0/0
	S0/0/1	172.16.254.5	255.255.255.252	BR2 S0/0/1
BR1	G0/0	172.16.240.1	255.255.248.0	2,000 Host LAN
	G0/1	172.16.224.1	255.255.240.0	4,000 Host LAN
	S0/0/0	172.16.254.2	255.255.255.252	HQ S0/0/0
	S0/0/1	172.16.254.9	255.255.255.252	BR2 S0/0/0
BR2	G0/0	172.16.252.1	255.255.254.0	500 Host LAN
	G0/1	172.16.248.1	255.255.252.0	1,000 Host LAN
	S0/0/0	172.16.254.10	255.255.255.252	BR1 S0/0/1
	S0/0/1	172.16.254.6	255.255.255.252	HQ S0/0/1

Part 3: Cable and Configure the IPv4 Network

In Part 3, you will cable the network topology and configure the three routers using the VLSM address scheme that you developed in Part 2.

Step 1: Cable the network as shown in the topology.

Step 2: Configure basic settings on each router.

- Assign the device name to the router.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the clear text passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.

Step 3: Configure the interfaces on each router.

- Assign an IP address and subnet mask to each interface using the table that you completed in Part 2.
- Configure an interface description for each interface.
- Set the clocking rate on all DCE serial interfaces to 128000.

```
HQ(config-if)# clock rate 128000
```
- Activate the interfaces.

Step 4: Save the configuration on all devices.

Step 5: Test Connectivity.

- From HQ, ping BR1's S0/0/0 interface address.
- From HQ, ping BR2's S0/0/1 interface address.
- From BR1, ping BR2's S0/0/0 interface address.
- Troubleshoot connectivity issues if pings were not successful.

Note: Pings to the GigabitEthernet interfaces on other routers will not be successful. The LANs defined for the GigabitEthernet interfaces are simulated. Because no devices are attached to these LANs they will be in down/down state. A routing protocol needs to be in place for other devices to be aware of those subnets. The GigabitEthernet interfaces also need to be in an up/up state before a routing protocol can add the subnets to the routing table. These interfaces will remain in a down/down state until a device is connected to the other end of the Ethernet interface cable. The focus of this lab is on VLSM and configuring the interfaces.

Reflection

Can you think of a shortcut for calculating the network addresses of consecutive /30 subnets?

Answers may vary. A /30 network has 4 address spaces: the network address, 2 host addresses, and a broadcast address. Another technique for obtaining the next /30 network address would be to take the network address of the previous /30 network and add 4 to the last octet.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs

Router BR1 (Final Configuration)

```
BR1#sh run
Building configuration...

Current configuration : 1555 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BR1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
```

Lab – Designing and Implementing a VLSM Addressing Scheme

```
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description LAN with 2,000 hosts.
ip address 172.16.240.1 255.255.248.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
description LAN with 4,000 hosts.
ip address 172.16.224.1 255.255.240.0
duplex auto
speed auto
!
interface Serial0/0/0
description Connection to HQ S0/0/0.
ip address 172.16.254.2 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
description Connection to BR2 S0/0/0.
ip address 172.16.254.9 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
banner motd ^C
Warning: Unauthorized access is prohibited!
^C
!
line con 0
password 7 14141B180F0B
login
line aux 0
line 2
```

```
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 094F471A1A0A
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router HQ (Final Configuration)

```
HQ#sh run
Building configuration...

Current configuration : 1554 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname HQ
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH6lwAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 15
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
no ip address
```

```
shutdown
!
interface GigabitEthernet0/0
  description LAN with 16,000 hosts.
  ip address 172.16.128.1 255.255.192.0
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  description LAN with 8,000 hosts.
  ip address 172.16.192.1 255.255.224.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  description Connection to BR1 S0/0/0.
  ip address 172.16.254.1 255.255.255.252
!
interface Serial0/0/1
  description Connection to BR2 S0/0/1.
  ip address 172.16.254.5 255.255.255.252
  clock rate 128000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
banner motd ^C
  Warning: Unauthorized access is prohibited!
^C
!
line con 0
  password 7 02050D480809
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
```

```
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 00071A150754
login
transport input all
!
scheduler allocate 20000 1000
!
end
```

Router BR2 (Final Configuration)

```
BR2#sh run
Building configuration...

Current configuration : 1593 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname BR2
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
!
no ip domain lookup
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
interface Embedded-Service-Engine0/0
no ip address
shutdown
!
interface GigabitEthernet0/0
description LAN with 500 hosts.
ip address 172.16.252.1 255.255.254.0
duplex auto
```

Lab – Designing and Implementing a VLSM Addressing Scheme

```
speed auto
!
interface GigabitEthernet0/1
description LAN with 1,000 hosts.
ip address 172.16.248.1 255.255.252.0
duplex auto
speed auto
!
interface Serial0/0/0
description Connection to BR1 S0/0/1.
ip address 172.16.254.10 255.255.255.252
clock rate 128000
!
interface Serial0/0/1
description Connection to HQ S0/0/1.
ip address 172.16.254.6 255.255.255.252
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
banner motd ^C
Warning: Unauthorized access is prohibited!
^C
!
line con 0
password 7 070C285F4D06
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
password 7 0822455D0A16
login
transport input all
!
scheduler allocate 20000 1000
!
end
```


Class Activity - Can You Call Me Now? (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Calculate the necessary subnet mask in order to accommodate a given number of hosts.

Background /Scenario

Note: This activity may be completed individually or in small/large groups using Packet Tracer software.

- You are setting up a dedicated, computer addressing scheme for patient rooms in a hospital. The switch will be centrally located in the nurses' station, as each of the five rooms will be wired so that patients can just connect to a RJ45 port built into the wall of their room. Devise a physical and logical topology for only one of the six floors using the following addressing scheme requirements: There are six floors with five patient rooms on each floor for a total of thirty connections. Each room needs a network connection.
- Subnetting must be incorporated into your scheme.
- Use one router, one switch, and five host stations for addressing purposes.
- Validate that all PCs can connect to the hospital's in-house services.

Keep a copy of your scheme to share later with the class or learning community. Be prepared to explain how subnetting, unicasts, multicasts and broadcasts would be incorporated, and where your addressing scheme could be used.

Instructor Note: This optional Modeling Activity may or may not be a graded assignment. Its purpose is to check students' mastery of hierarchical subnets and subnet masking operation. A facilitated chapter review discussion can be initiated as a result of this activity.

Required Resources

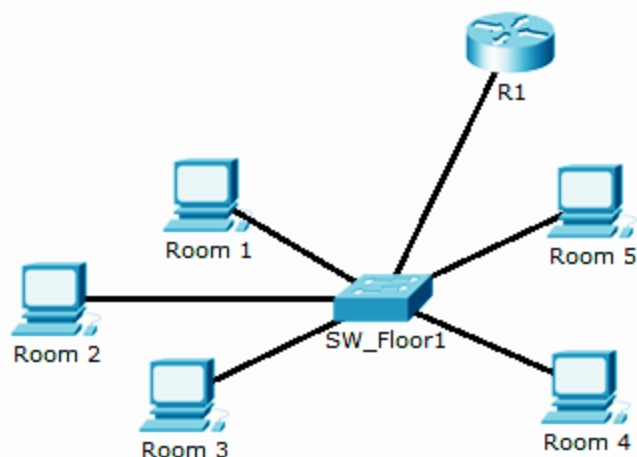
- Packet Tracer software

Reflection

How would you change your addressing scheme if you were going to add an additional network connection to the hospital rooms with a total of 10 connections per floor or 2 ports per room?

If the number of network connections were doubled, a subnet mask of 255.255.255.240 with a prefix of /28 would be necessary to support connectivity.

Another possible solution to the original activity might be:



R1 - Fa0/0 (default gateway for this particular subnet)
IP Address 192.168.1.1
Subnet Mask 255.255.255.248
Prefix /29

Room 1
IP Address 192.168.1.2
Subnet Mask 255.255.255.248
Prefix /29

Room 2
IP Address 192.168.1.3
Subnet Mask 255.255.255.248
Prefix /29

Room 3
IP Address 192.168.1.4
Subnet Mask 255.255.255.248
Prefix /29

Room 4
IP Address 192.168.1.5
Subnet Mask 255.255.255.248
Prefix /29

Room 5
IP Address 192.168.1.6
Subnet Mask 255.255.255.248
Prefix /29

Identify elements of the model that map to IT-related content:

- Hierarchies are employed when using addressing schemes. The hospital's floors represent subnetworks and the patient connections represent host addresses.
- Connectivity is influenced by the addressing scheme identifiers. The switch represents a valid intermediary device for data processing between statically addressed end devices.

Class Activity - We Need to Talk (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain how transport layer protocols and services support communications across data networks.

Background / Scenario

Note: This activity works best with medium-sized groups of 6 to 8 students per group.

This chapter helps you understand how transport layer protocols and services support network data communications.

The instructor will whisper a complex message to the first student in a group. An example of the message might be “Our final exam will be given next Tuesday, February 5th, at 2 p.m. in Room 1151.”

That student whispers the message to the next student in the group. Each group follows this process until all members of each group have heard the whispered message. Here are the rules you are to follow:

- You can whisper the message only once to your neighbor.
- The message must keep moving from one person to the other with no skipping of participants. The instructor should ask a student to keep time of the full message activity from first participant to last participant stating the messages. The first or last person would mostly likely be the best one to keep this time.
- The last student will say aloud exactly what he or she heard.

The instructor will then restate the original message so that the group can compare it to the message that was delivered by the last student in the group.

Instructor Note: You should have a different complex message for each group of students. Initiate discussion about what happened in the activity. Focus on these five questions:

- 1) Was the message **complete** when it reached the last student?
- 2) Was the message **correct** as delivered to the last student?
- 3) How long did it take for the message to get to the last student?
- 4) If you were depending on this message to drive your personal/business calendar, studying schedule, etc., would the contents of this message need to be fully correct when you received them?
- 5) Would the length of time taken to deliver the message be important to the sender and recipient?

Instructor Note: This is an optional in-class Modeling Activity (MA). It is not intended to be a graded assignment. Its purpose is to initiate student discussion about their perception of how data is transferred from source to destination, both personally and in corporate practice. This MA introduces students to TCP/UDP, transport layer content.

Required Resources

- Timer for the student who is keeping a record of the conversation's duration.

Reflection

1. Would the contents of this message need to be fully correct when you received them if you were depending on this message to drive your personal/business calendar, studying schedule, etc.?

2. Would the length of time taken to deliver the message be an important factor to the sender and recipient?
-
-

In the discussion initiated as a result of this activity, students should mention:

- The importance of messages being delivered fully from sender to recipient (TCP vs. UDP - was the message method correct to use in this situation?)
- The importance of details within the message being correct from sender to recipient (Guaranteed vs. Non-guaranteed delivery - was the message correct as delivered to the last person?)
- The importance of timing of a message – to the details of the message and to the date/time needed to take action on the message (Segment establishment and delivery vs. full message delivery - did it take very long for the message to get to the last student?)

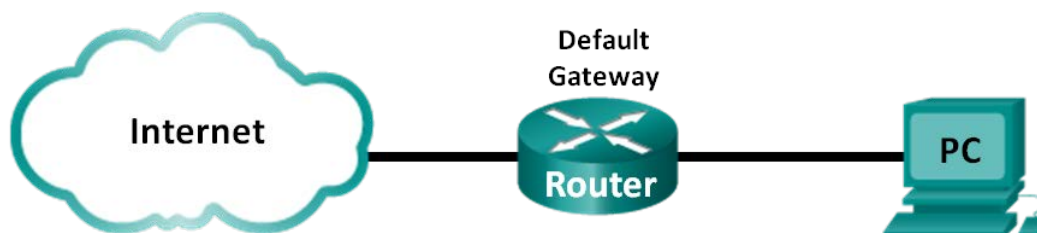
Identify elements of the model that map to IT-related content:

- Protocols can establish a method of sending and receiving information over a network (TCP/UDP protocols).
- Quality of delivery of data over a network may be affected by which protocol is used during a network conversation (Best Effort Delivery).
- Timing issues and factors for delivery of data over a communications system are affected by how much data is sent at one time and by the type of transported data (Segment establishment and delivery – both TCP and UDP).

Lab - Using Wireshark to Observe the TCP 3-Way Handshake (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Prepare Wireshark to Capture Packets

Part 2: Capture, Locate, and Examine Packets

Background / Scenario

In this lab, you will use Wireshark to capture and examine packets generated between the PC browser using the HyperText Transfer Protocol (HTTP) and a web server, such as www.google.com. When an application, such as HTTP or FTP (File Transfer Protocol) first starts on a host, TCP uses the three-way handshake to establish a reliable TCP session between the two hosts. For example, when a PC uses a web browser to surf the internet, a three-way handshake is initiated, and a session is established between the PC host and web server. A PC can have multiple, simultaneous, active TCP sessions with various websites.

Note: This lab cannot be completed using Netlab. This lab assumes that you have internet access.

Instructor Note: Using a packet sniffer, such as Wireshark, may be considered a breach of the security policy of the school. It is recommended that permission be obtained before running Wireshark for this lab. If using a packet sniffer is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

Required Resources

1 PC (Windows 7, 8, or 10 with a command prompt access, internet access, and Wireshark installed)

Part 1: Prepare Wireshark to Capture Packets

In Part 1, you will start the Wireshark program and select the appropriate interface to begin capturing packets.

Step 1: Retrieve the PC interface addresses.

For this lab, you need to retrieve the IP address of your PC and its network interface card (NIC) physical address, also called the MAC address.

Lab - Using Wireshark to Observe the TCP 3-Way Handshake

- a. Open a command prompt window, type **ipconfig /all**, and press Enter.

```
Physical Address. . . . . : 00-24-D7-1C-50-44
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80dd:5657:ad20:f4b3%16 (Preferred)
IPv4 Address. . . . . : 192.168.1.146 (Preferred)
Subnet Mask . . . . . : 255.255.255.0
```

- b. Write down the IP and MAC addresses associated with the selected Ethernet adapter. That is the source address to look for when examining captured packets.

The PC host IP address: _____

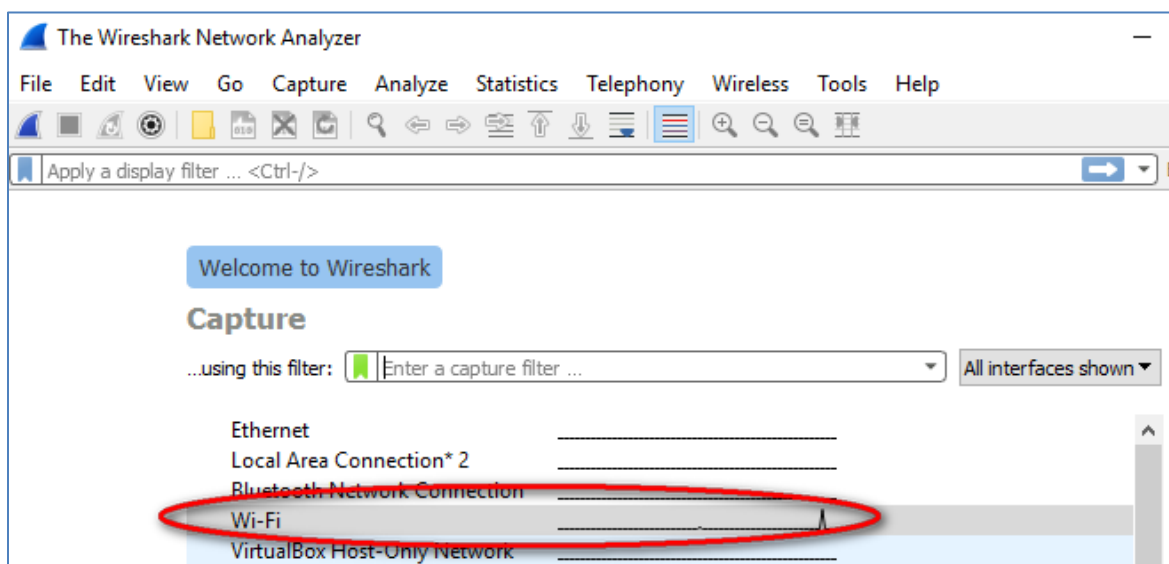
Answers will vary. In this case, it is 192.168.1.146.

The PC host MAC address: _____

Answers will vary. In this case, it is 00:24:D7:1C:50:44.

Step 2: Start Wireshark and select the appropriate interface.

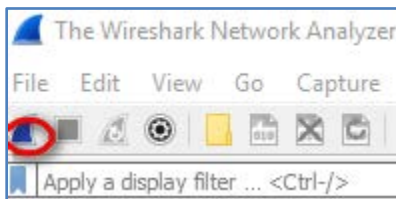
- a. Click the Windows **Start** button. In the pop-up menu, double-click **Wireshark**.
- b. After Wireshark starts, select the active interface for data capture. The active interface will show traffic activities.



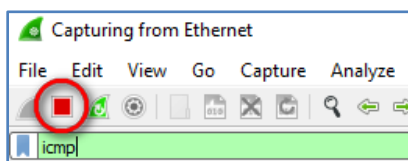
Part 2: Capture, Locate, and Examine Packets

Step 1: Capture the data.

- a. Click the **Start** button to start the data capture.

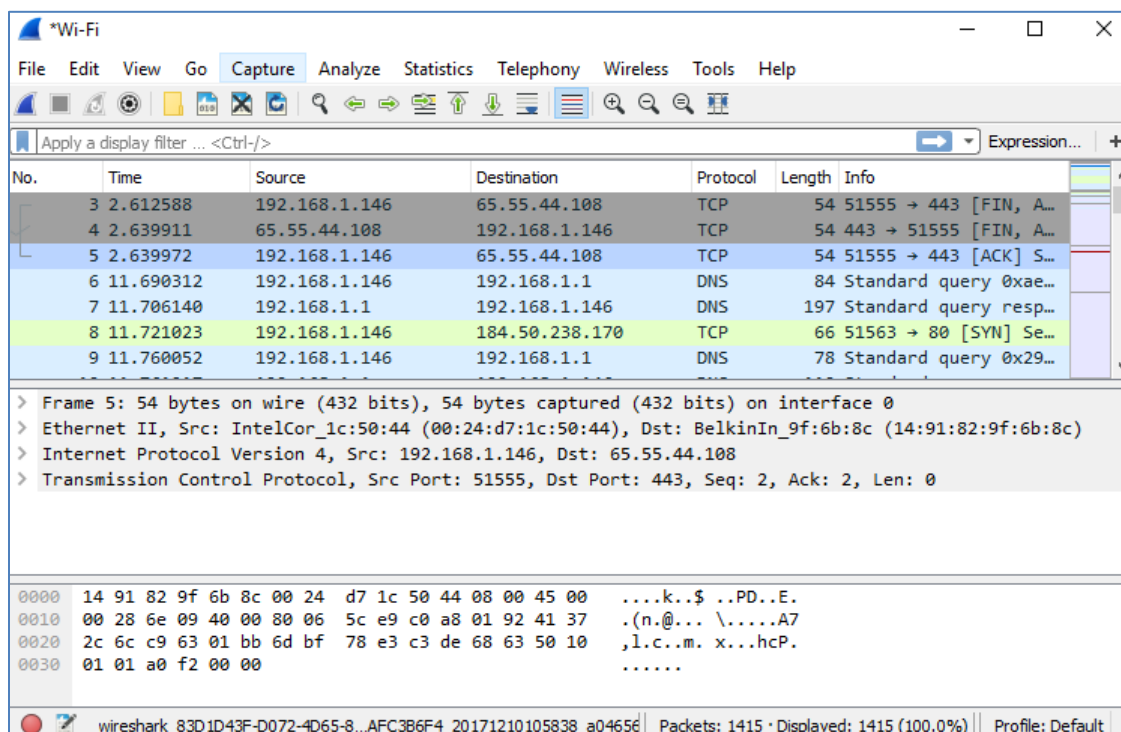


- b. Open a web browser and visit www.google.com.
c. Minimize the browser and return to Wireshark. Stop the data capture.



Note: Your instructor may provide you with a different website. If so, enter the website name or address here:

The capture window is now active. Locate the **Source**, **Destination**, and **Protocol** columns.



Step 2: Locate appropriate packets for the web session.

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 the Address Resolution Protocol (ARP), Domain Name System (DNS), and the TCP three-way handshake. If the PC already had an ARP entry for the default gateway, then it means that it started with the DNS query to resolve `www.google.com`.

- Frame 6 shows the DNS query from the PC to the DNS server, which is attempting to resolve the domain name `www.google.com` to the IP address of the web server. The PC must have the IP address before it can send the first packet to the web server.

What is the IP address of the DNS server that the computer queried? _____

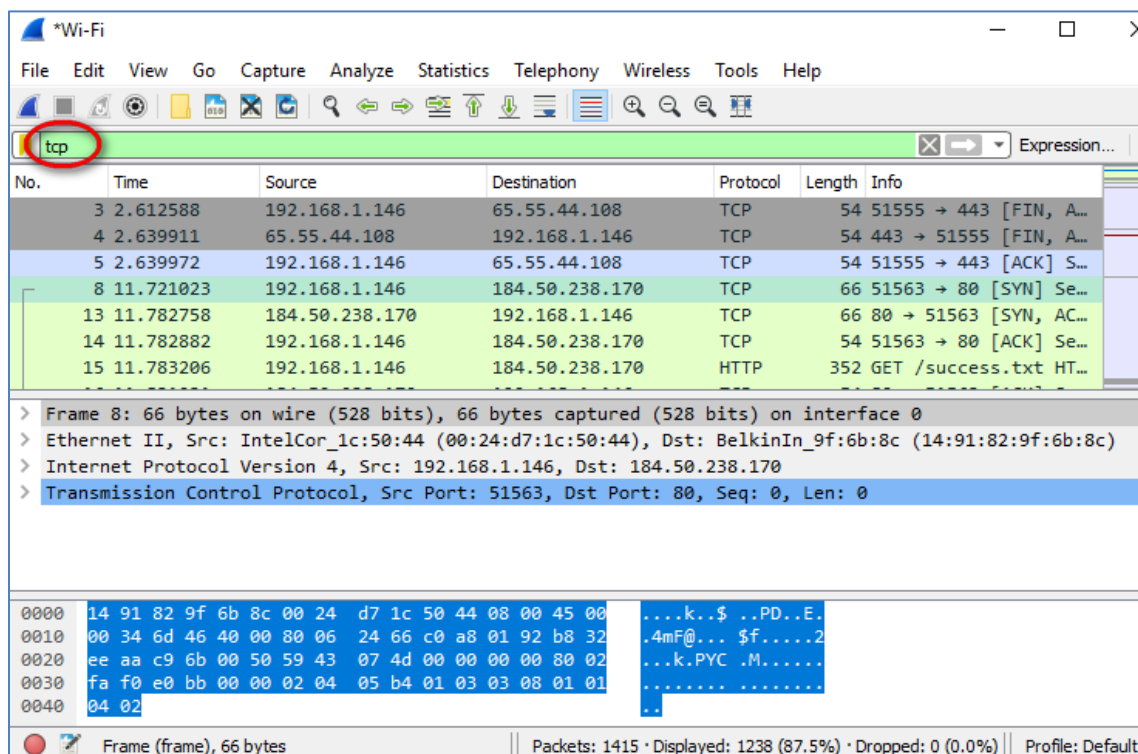
192.168.1.1

- Frame 7 is the response from the DNS server. It contains the IP address of `www.google.com`.
- Find the appropriate packet for the start of your three-way handshake. In the example, frame 8 is the start of the TCP three-way handshake.

What is the IP address of the Google web server? _____

In this example, it is 184.50.238.170.

- If you have many packets that are unrelated to the TCP connection, it may be necessary to use the Wireshark filter tool. Type `tcp` in the filter entry area within Wireshark and press **Enter**.



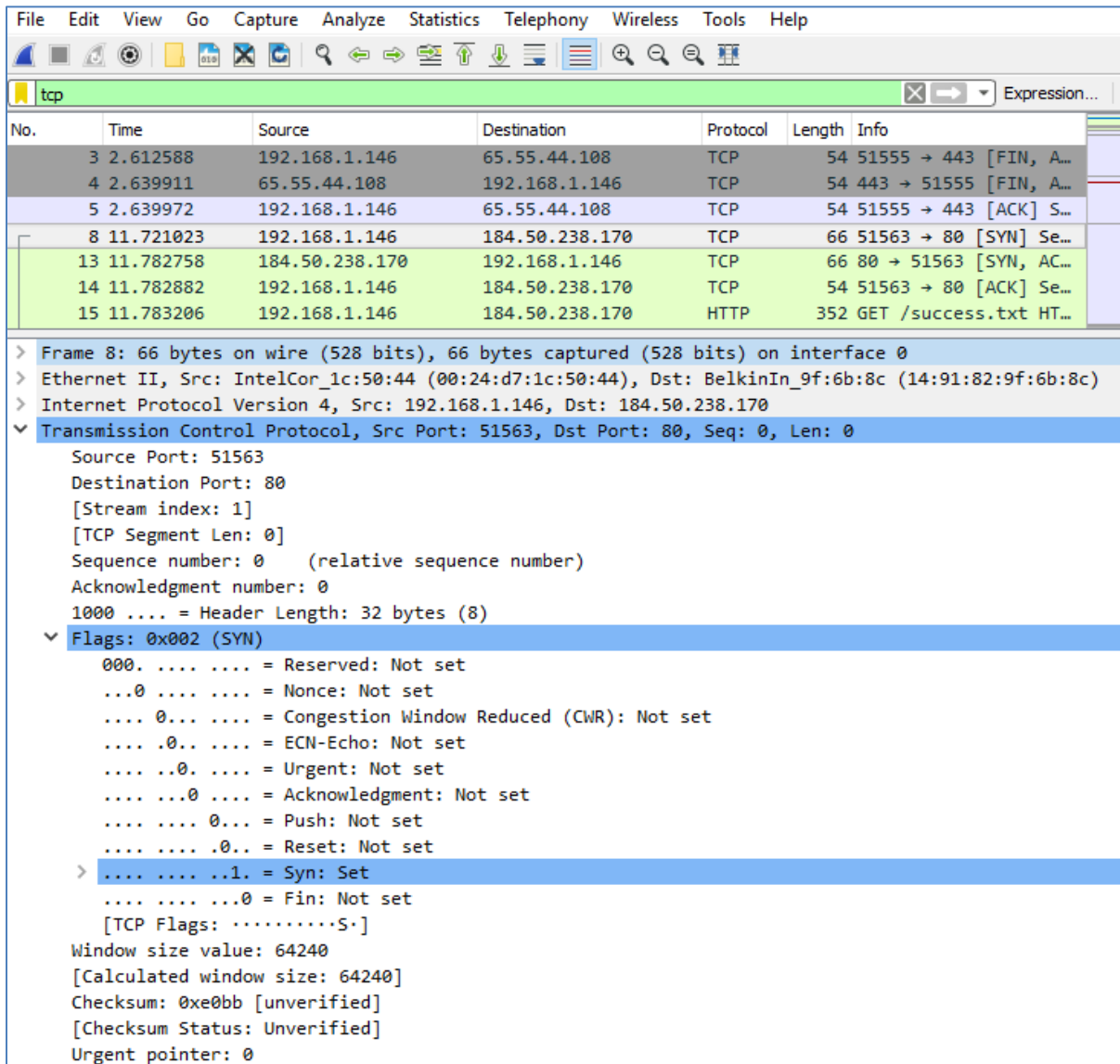
Step 3: Examine the information within packets including IP addresses, TCP port numbers, and TCP control flags.

- In our example, frame 8 is the start of the three-way handshake between the PC and the Google web server. In the packet list pane (top section of the main window), select the frame. This highlights the line and displays the decoded information from that packet in the two lower panes. Examine the TCP information in the packet details pane (middle section of the main window).

Lab - Using Wireshark to Observe the TCP 3-Way Handshake

- Click the + icon to the left of the Transmission Control Protocol in the packet details pane to expand the view of the TCP information.
- Click the + icon to the left of the Flags. Look at the source and destination ports and the flags that are set.

Note: You may have to adjust the top and middle windows sizes within Wireshark to display the necessary information.



What is the TCP source port number? _____ Answers will vary. In this example, the source port is 51563.

How would you classify the source port? _____ Dynamic or Private

What is the TCP destination port number? _____ Port 80

How would you classify the destination port? _____ Well-known, registered (HTTP or web protocol)

Which flag (or flags) is set? _____ SYN flag

Lab - Using Wireshark to Observe the TCP 3-Way Handshake

What is the relative sequence number set to? _____ 0

- d. To select the next frame in the three-way handshake, select **Go** on the Wireshark menu and select **Next Packet in Conversation**. In this example, this is frame 13. This is the Google web server reply to the initial request to start a session.

The screenshot shows the Wireshark interface with a packet capture of a TCP 3-way handshake. The packet list shows frames 3 through 15. Frame 13 is selected, which is a TCP SYN-ACK packet from 184.50.238.170 to 192.168.1.146. The packet details pane shows the following information:

- Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
- Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
- Internet Protocol Version 4, Src: 184.50.238.170, Dst: 192.168.1.146
- Transmission Control Protocol, Src Port: 80, Dst Port: 51563, Seq: 0, Ack: 1, Len: 0
 - Source Port: 80
 - Destination Port: 51563
 - [Stream index: 1]
 - [TCP Segment Len: 0]
 - Sequence number: 0 (relative sequence number)
 - Acknowledgment number: 1 (relative ack number)
 - 1000 = Header Length: 32 bytes (8)
 - Flags: 0x012 (SYN, ACK)
 - 000. = Reserved: Not set
 - ...0 = Nonce: Not set
 - 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
 - [TCP Flags:A..S.]
 - Window size value: 29200
 - [Calculated window size: 29200]
 - Checksum: 0x3a72 [unverified]
 - [Checksum Status: Unverified]
 - Urgent pointer: 0

What are the values of the source and destination ports? _____

Source Port is now 80, and Destination Port is now 51563

Which flags are set? _____

The Syn flag (SYN) and Acknowledgment flag (ACK)

What are the relative sequence and acknowledgment numbers set to?

The relative sequence number is 0, and the relative acknowledgment number is 1.

Lab - Using Wireshark to Observe the TCP 3-Way Handshake

- e. Finally, examine the third packet of the three-way handshake in the example. Click frame 14 in the top window to display the following information in this example:

The screenshot shows the Wireshark interface with a packet capture of a TCP 3-way handshake. The packet list on the left shows several frames, with frame 14 selected. The packet details pane on the right shows the structure of frame 14, which is a TCP ACK segment.

No.	Time	Source	Destination	Protocol	Length	Info
3	2.612588	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [FIN, A...
4	2.639911	65.55.44.108	192.168.1.146	TCP	54	443 → 51555 [FIN, A...
5	2.639972	192.168.1.146	65.55.44.108	TCP	54	51555 → 443 [ACK] S...
8	11.721023	192.168.1.146	184.50.238.170	TCP	66	51563 → 80 [SYN] Se...
13	11.782758	184.50.238.170	192.168.1.146	TCP	66	80 → 51563 [SYN, AC...
14	11.782882	192.168.1.146	184.50.238.170	TCP	54	51563 → 80 [ACK] Se...
15	11.783206	192.168.1.146	184.50.238.170	HTTP	352	GET /success.txt HT...

Frame 14: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
Internet Protocol Version 4, Src: 192.168.1.146, Dst: 184.50.238.170
Transmission Control Protocol, Src Port: 51563, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
Source Port: 51563
Destination Port: 80
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
0101 = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 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
[TCP Flags:A....]
Window size value: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0xec52 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0

Examine the third and final packet of the handshake.

Which flag (or flags) is set? _____

Acknowledgment flag (ACK)

The relative sequence and acknowledgment numbers are set to 1 as a starting point. The TCP connection is established and communication between the source computer and the web server can begin.

- f. Close the Wireshark program.

Reflection

1. There are hundreds of filters available in Wireshark. A large network could have numerous filters and many different types of traffic. List three filters that might be useful to a network administrator?

Answers will vary but could include TCP, specific IP Addresses (source or destination), and protocols such as HTTP.

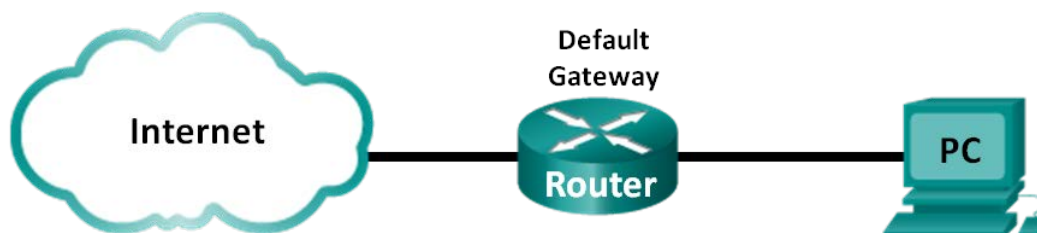
2. What other ways could Wireshark be used in a production network?

Wireshark is often used for security purposes for after-the-fact analysis of normal traffic or after a network attack. New protocols or services may need to be captured to determine what port or ports are used.

Lab - Using Wireshark to Examine a UDP DNS Capture (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Record the IP Configuration Information of a PC

Part 2: Use Wireshark to Capture DNS Queries and Responses

Part 3: Analyze Captured DNS or UDP Packets

Background / Scenario

If you have ever used the internet, you have used the Domain Name System (DNS). DNS is a distributed network of servers that translates user-friendly domain names like www.google.com to an IP address. When you type a website URL into your browser, your PC performs a DNS query to the DNS server IP address. Your PC DNS server query and the DNS server response make use of the User Datagram Protocol (UDP) as the transport layer protocol. UDP is connectionless and does not require a session setup as does TCP. DNS queries and responses are very small and do not require the overhead of TCP.

In this lab, you will communicate with a DNS server by sending a DNS query using the UDP transport protocol. You will use Wireshark to examine the DNS query and response exchanges with the same server.

Note: This lab cannot be completed using Netlab. This lab assumes that you have internet access.

Instructor Note: Using a packet sniffer, such as Wireshark, may be considered a breach of the security policy of the school. It is recommended that permission be obtained before running Wireshark for this lab. If using a packet sniffer is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

Required Resources

1 PC (Windows 7, 8, or 10 with command prompt access, internet access, and Wireshark installed)

Part 1: Record a PC's IP Configuration Information

In Part 1, you will use the `ipconfig /all` command on your local PC to find and record the MAC and IP addresses of your PC network interface card (NIC), the IP address of the specified default gateway, and the

Lab - Using Wireshark to Examine a UDP DNS Capture

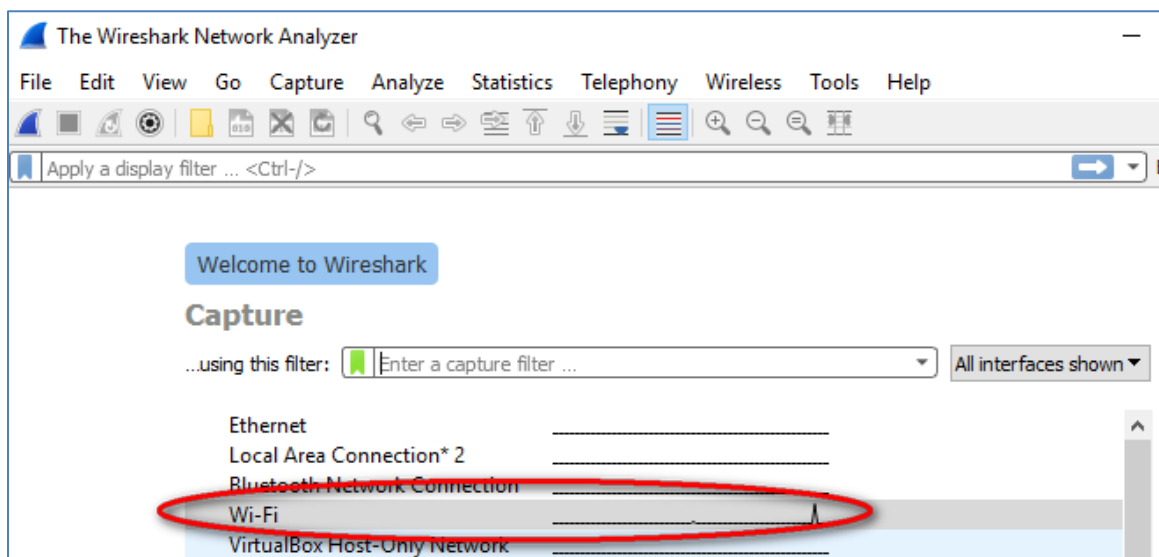
DNS server IP address specified for the PC. Record this information in the table provided. The information will be used in parts of this lab with packet analysis.

IP address	Answers will vary. 192.168.1.146
MAC address	Answers will vary. 00:24:D7:1C:50:44
Default gateway IP address	Answers will vary. 192.168.1.1
DNS server IP address	Answers will vary. 192.168.1.1

Part 2: Use Wireshark to Capture DNS Queries and Responses

In Part 2, you will set up Wireshark to capture DNS query and response packets to demonstrate the use of the UDP transport protocol while communicating with a DNS server.

- Click the Windows **Start** button and navigate to the Wireshark program.
- Select an interface for Wireshark to capture packets. Select (highlight) the active capturing interface.



- After selecting the desired interface, click **Start** to capture the packets.
- Open a web browser and type **www.google.com**. Press **Enter** to continue.
- Click **Stop** to stop the Wireshark capture when you see the Google home page.

Part 3: Analyze Captured DNS or UDP Packets

In Part 3, you will examine the UDP packets that were generated when communicating with a DNS server for the IP addresses for **www.google.com**.

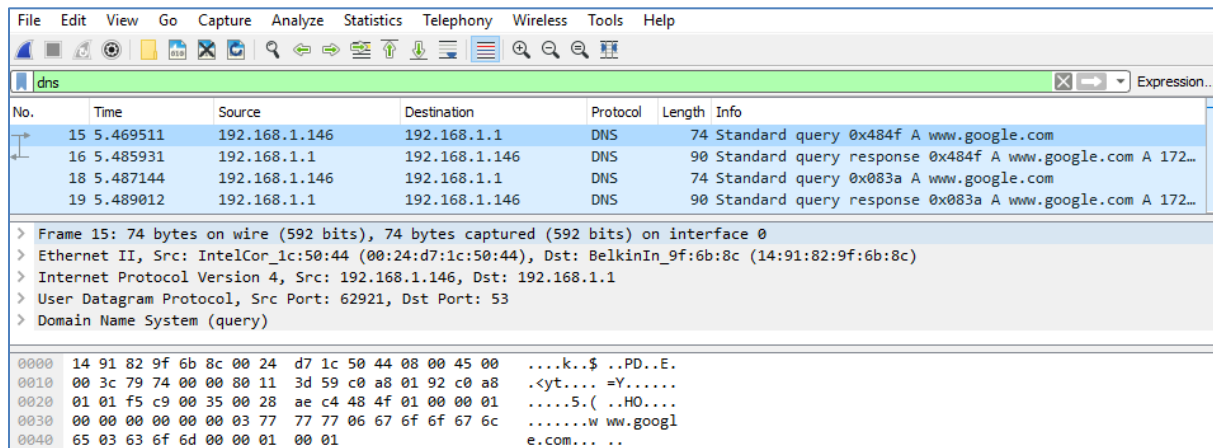
Step 1: Filter DNS packets.

- In the Wireshark main window, type **dns** in the entry area of the **Filter** toolbar and press **Enter**.

Note: If you do not see any results after the DNS filter was applied, close the web browser. In the command prompt window, type **ipconfig /flushdns** to remove all previous DNS results. Restart the

Lab - Using Wireshark to Examine a UDP DNS Capture

Wireshark capture and repeat the instructions in Part 2b –2e. If this does not resolve the issue, type **nslookup www.google.com** in the command prompt window as an alternative to the web browser.



No.	Time	Source	Destination	Protocol	Length	Info
15	5.469511	192.168.1.146	192.168.1.1	DNS	74	Standard query 0x484f A www.google.com
16	5.485931	192.168.1.1	192.168.1.146	DNS	90	Standard query response 0x484f A www.google.com A 172...
18	5.487144	192.168.1.146	192.168.1.1	DNS	74	Standard query 0x083a A www.google.com
19	5.489012	192.168.1.1	192.168.1.146	DNS	90	Standard query response 0x083a A www.google.com A 172...

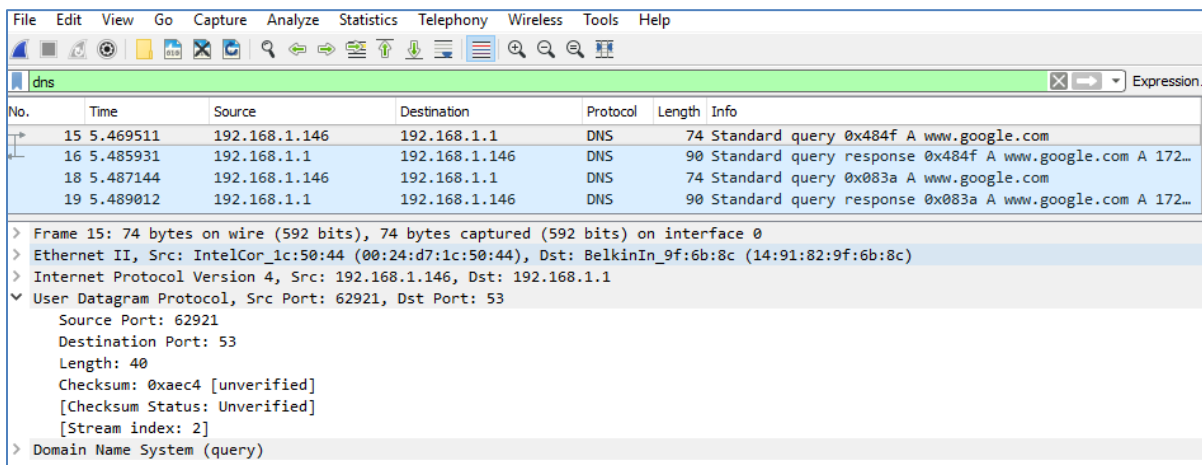
Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0	
Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)	
Internet Protocol Version 4, Src: 192.168.1.146, Dst: 192.168.1.1	
User Datagram Protocol, Src Port: 62921, Dst Port: 53	
Domain Name System (query)	

Offset	Hex	ASCII
0000	14 91 82 9f 6b 8c 00 24 d7 1c 50 44 08 00 45 00k..\$.PD..E.
0010	00 3c 79 74 00 00 80 11 3d 59 c0 a8 01 92 c0 a8	.<yt....=Y.....
0020	01 01 f5 c9 00 35 00 28 ae c4 48 4f 01 00 00 015.(..HO....
0030	00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw ww.googl
0040	65 03 63 6f 6d 00 00 01 00 01	e.com... ..

- In the packet list pane (top section) of the main window, locate the packet that includes **Standard query** and **A www.google.com**. See frame 15 as an example.

Step 2: Examine a UDP segment using DNS query.

Examine the UDP by using a DNS query for www.google.com as captured by Wireshark. In this example, Wireshark capture frame 15 in the packet list pane is selected for analysis. The protocols in this query are displayed in the packet details pane (middle section) of the main window. The protocol entries are highlighted in gray.



No.	Time	Source	Destination	Protocol	Length	Info
15	5.469511	192.168.1.146	192.168.1.1	DNS	74	Standard query 0x484f A www.google.com
16	5.485931	192.168.1.1	192.168.1.146	DNS	90	Standard query response 0x484f A www.google.com A 172...
18	5.487144	192.168.1.146	192.168.1.1	DNS	74	Standard query 0x083a A www.google.com
19	5.489012	192.168.1.1	192.168.1.146	DNS	90	Standard query response 0x083a A www.google.com A 172...

Frame 15: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0	
Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)	
Internet Protocol Version 4, Src: 192.168.1.146, Dst: 192.168.1.1	
User Datagram Protocol, Src Port: 62921, Dst Port: 53	
Domain Name System (query)	

User Datagram Protocol	
Source Port:	62921
Destination Port:	53
Length:	40
Checksum:	0xaec4 [unverified]
[Checksum Status:	Unverified]
[Stream index:	2]

- In the first line in the packet details pane, frame 15 had 74 bytes of data on the wire. This is the number of bytes to send a DNS query to a name server requesting the IP addresses of www.google.com.
- The Ethernet II line displays the source and destination MAC addresses. The source MAC address is from your local PC because your local PC originated the DNS query. The destination MAC address is from the default gateway because this is the last stop before this query exits the local network.

Is the source MAC address the same as the one recorded from Part 1 for the local PC?

The answer should be yes. If not, please verify that Wireshark is using the same interface for capturing the packets.

Lab - Using Wireshark to Examine a UDP DNS Capture

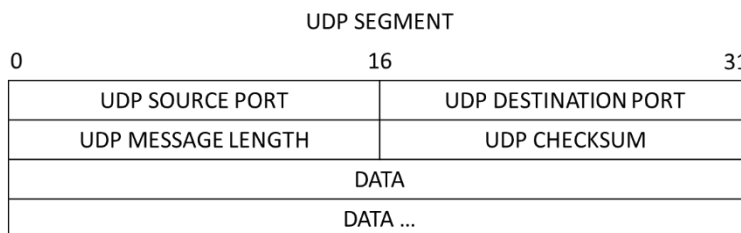
- c. In the Internet Protocol Version 4 line, the IP packet Wireshark capture indicates that the source IP address of this DNS query is 192.168.1.146 and the destination IP address is 192.168.1.1. In this example, the destination address is the default gateway. The router is the default gateway in this network.

Can you identify the IP and MAC addresses for the source and destination devices?

Device	IP Address	MAC Address
Local PC	Answers will vary. 192.168.1.146	Answers will vary. 00:24:D7:1C:50:44
Default Gateway	Answers will vary. 192.168.1.1	Answers will vary. 14:91:82:9F:6B:8C

The IP packet and header encapsulates the UDP segment. The UDP segment contains the DNS query as the data.

- d. A UDP header only has four fields: source port, destination port, length, and checksum. Each field in a UDP header is only 16 bits as depicted below.

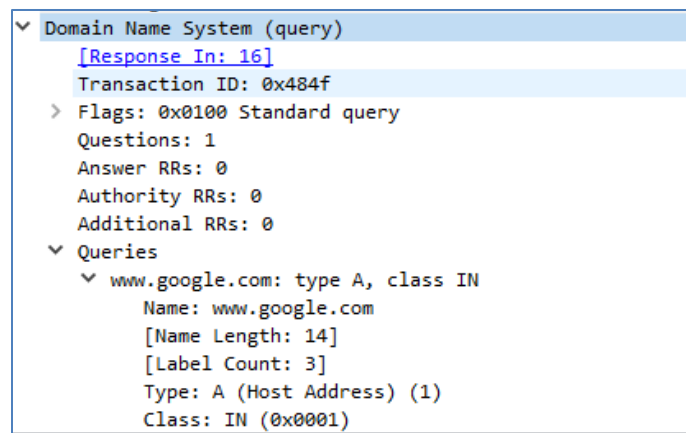


Expand the User Datagram Protocol in the packet details pane by clicking the plus (+) sign. Notice that there are only four fields. The source port number in this example is 60868. The source port was randomly generated by the local PC using port numbers that are not reserved. The destination port is 53. Port 53 is a well-known port reserved for use with DNS. DNS servers listen on port 53 for DNS queries from clients.

```
▼ User Datagram Protocol, Src Port: 62921, Dst Port: 53
  Source Port: 62921
  Destination Port: 53
  Length: 40
  Checksum: 0xaec4 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 2]
```


Lab - Using Wireshark to Examine a UDP DNS Capture

In this example, the length of the UDP segment is 40 bytes. Out of 40 bytes, 8 bytes are used as the header. The other 32 bytes are used by DNS query data. The 32 bytes of DNS query data is highlighted in the following illustration in the packet bytes pane (lower section) of the Wireshark main window.



The checksum is used to determine the integrity of the packet after it has traversed the internet.

The UDP header has low overhead because UDP does not have fields that are associated with the three-way handshake in TCP. Any data transfer reliability issues that occur must be handled by the application layer.

Record your Wireshark results in the table below:

Frame size	
Source MAC address	
Destination MAC address	
Source IP address	
Destination IP address	
Source port	
Destination port	

Is the source IP address the same as the local PC IP address you recorded in Part 1? _____

Yes

Is the destination IP address the same as the default gateway noted in Part 1? _____

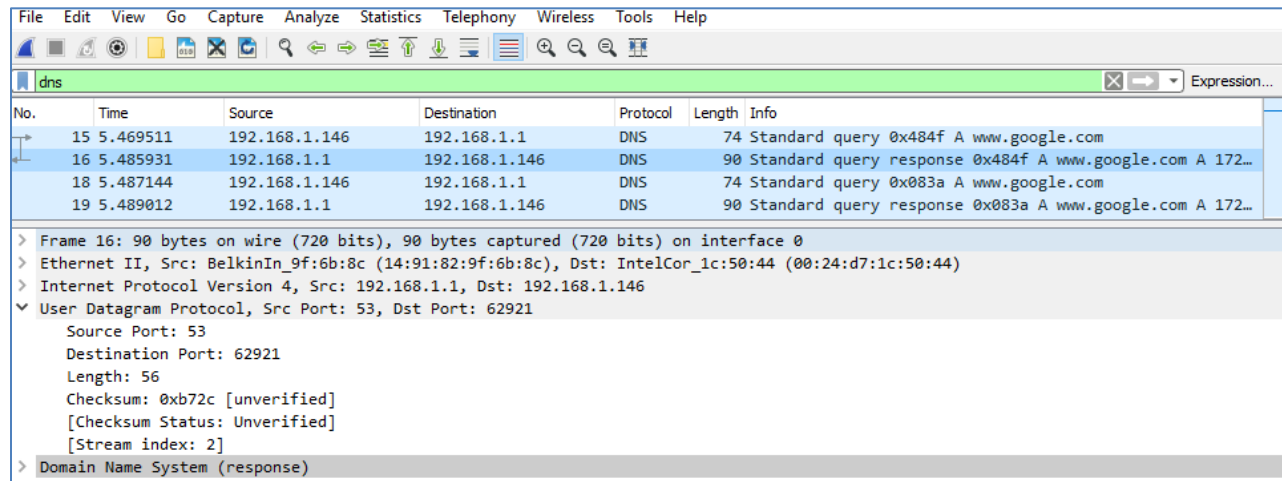
Yes, if the default gateway is also performing DNS.

Step 3: Examine a UDP using DNS response.

In this step, you will examine the DNS response packet and verify that the DNS response packet also uses the UDP.

Lab - Using Wireshark to Examine a UDP DNS Capture

- a. In this example, frame 16 is the corresponding DNS response packet. Notice the number of bytes on the wire is 90. It is a larger packet compared to the DNS query packet.



The screenshot shows the Wireshark interface with a capture of DNS traffic. The packet list shows four frames: a query (frame 15), a response (frame 16), another query (frame 18), and another response (frame 19). Frame 16 is selected, and its details are shown in the packet details pane. The details pane shows the Ethernet II frame, the Internet Protocol Version 4 packet, and the User Datagram Protocol (UDP) segment. The UDP segment shows a source port of 53 and a destination port of 62921. The Domain Name System (response) section is expanded, showing the response details.

No.	Time	Source	Destination	Protocol	Length	Info
15	5.469511	192.168.1.146	192.168.1.1	DNS	74	Standard query 0x484f A www.google.com
16	5.485931	192.168.1.1	192.168.1.146	DNS	90	Standard query response 0x484f A www.google.com A 172...
18	5.487144	192.168.1.146	192.168.1.1	DNS	74	Standard query 0x083a A www.google.com
19	5.489012	192.168.1.1	192.168.1.146	DNS	90	Standard query response 0x083a A www.google.com A 172...

Frame 16: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
> Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
> Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.146
v User Datagram Protocol, Src Port: 53, Dst Port: 62921
Source Port: 53
Destination Port: 62921
Length: 56
Checksum: 0xb72c [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
> Domain Name System (response)

- b. In the Ethernet II frame for the DNS response, what device is the source MAC address and what device is the destination MAC address?

The source MAC address is the default gateway and the destination MAC address is the local host.

- c. Notice the source and destination IP addresses in the IP packet. What is the destination IP address? What is the source IP address?

Destination IP address: _____ Source IP address: _____

The answer will vary. In this example, the destination is 192.168.1.146 and the source is 192.168.1.1.

What happened to the roles of source and destination for the local host and default gateway?

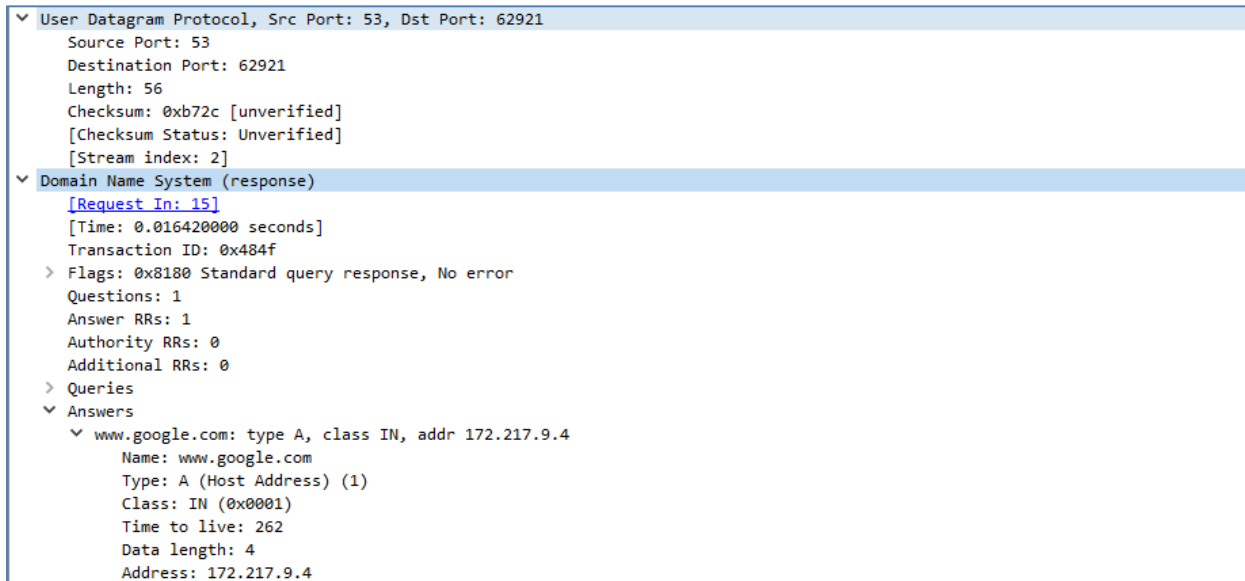
The local host and the default gateway have reversed their roles in DNS query and response packets.

- d. In the UDP segment, the role of the port numbers has also reversed. The destination port number is 62921. Port number 62921 is the same port that was generated by the local PC when the DNS query was sent to the DNS server. Your local PC listens for a DNS response on this port.

The source port number is 53. The DNS server listens for a DNS query on port 53 and then sends a DNS response with a source port number of 53 back to the originator of the DNS query.

Lab - Using Wireshark to Examine a UDP DNS Capture

When the DNS response is expanded, notice the resolved IP addresses for www.google.com in the **Answers** section.



Reflection

What are the benefits of using UDP instead of TCP as a transport protocol for DNS?

UDP as a transport protocol provides quick session establishment, quick response, minimal overhead, no need for retries, segment reassembly, and acknowledgment of received packets.

Lab – Researching Network Security Threats (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Explore the SANS Website

Part 2: Identify Recent Network Security Threats

Part 3: Detail a Specific Network Security Threat

Background / Scenario

To defend a network against attacks, an administrator must identify external threats that pose a danger to the network. Security websites can be used to identify emerging threats and provide mitigation options for defending a network.

One of the most popular and trusted sites for defending against computer and network security threats is SysAdmin, Audit, Network, Security (SANS). The SANS site provides multiple resources, including a list of the top 20 Critical Security Controls for Effective Cyber Defense and the weekly @Risk: The Consensus Security Alert newsletter. This newsletter details new network attacks and vulnerabilities.

In this lab, you will navigate to and explore the SANS site, use the SANS site to identify recent network security threats, research other websites that identify threats, and research and present the details about a specific network attack.

Required Resources

- Device with Internet access
- Presentation computer with PowerPoint or other presentation software installed

Part 1: Exploring the SANS Website

In Part 1, navigate to the SANS website and explore the available resources.

Step 1: Locate SANS resources.

Navigate to www.SANS.org. From the home page, highlight the **Resources** menu.

List three available resources.

Reading Room, Webcasts, Newsletters, Blogs, Top 25 Programming Errors, Top 20 Critical Controls, Security Policy Project

Step 2: Locate the Critical Security Controls.

The **Critical Security Controls** listed on the SANS website are the culmination of a public-private partnership involving the Department of Defense (DoD), National Security Association, Center for Internet Security (CIS), and the SANS Institute. The list was developed to prioritize the cyber security controls and spending for DoD. It has become the centerpiece for effective security programs for the United States government. From the **Resources** menu, select **Critical Security Controls**, or similar.

Select one of the Controls and list three of the implementation suggestions for this control.

Answers will vary. Critical Control 5: Malware Defenses. Employ automated tools to continuously monitor workstations, servers, and mobile devices. Employ anti-malware software and signature auto-update features. Configure network computers to not auto-run content from removable media.

Step 3: Locate the Newsletters menu.

Highlight the **Resources** menu, select **Newsletters**. Briefly describe each of the three newsletters available.

SANS NewsBites - A high level summary of the most important news articles that deal with computer security. The newsletter is published twice a week and includes links for more information.

@RISK: The Consensus Security Alert - A weekly summary of new network attacks and vulnerabilities. The newsletters is also provides insights on how recent attacks worked.

Ouch! – A security awareness document that provides end users with information about how they can help ensure the safety of their network.

Part 2: Identify Recent Network Security Threats

In Part 2, you will research recent network security threats using the SANS site and identify other sites containing security threat information.

Step 1: Locate the @Risk: Consensus Security Alert Newsletter Archive.

From the **Newsletters** page, select **Archive** for the @RISK: The Consensus Security Alert. Scroll down to **Archives Volumes** and select a recent weekly newsletter. Review the **Notable Recent Security Issues and Most Popular Malware Files** sections.

List some recent attacks. Browse multiple recent newsletters, if necessary.

Answers will vary. Win.Trojan.Quarian, Win.Trojan.Changeup, Andr.Trojan.SMSSend-1, Java.Exploit.Agent-14, Trojan.ADH.

Step 2: Identify sites providing recent security threat information.

Besides the SANS site, identify some other websites that provide recent security threat information.

Answers will vary but could include www.mcafee.com/us/mcafee-labs.aspx, www.symantec.com/news.cnet.com/security/, www.sophos.com/en-us/threat-center/, us.norton.com/security_response/.

List some of the recent security threats detailed on these websites.

Answers will vary. Trojan.Ransomlock, Inostealer.Vskim, Trojan.Fareit, Backdoor.Sorosk, Android.Boxer, W32.Changeup!gen35

Part 3: Detail a Specific Network Security Attack

In Part 3, you will research a specific network attack that has occurred and create a presentation based on your findings. Complete the form below based on your findings.

Step 1: Complete the following form for the selected network attack.

Name of attack:	Code Red
Type of attack:	Worm
Dates of attacks:	July 2001
Computers / Organizations affected:	Infected an estimated 359,000 computers in one day.
How it works and what it did:	
<p>Instructor Note: Most of the following is from Wikipedia.</p> <p>Code Red exploited buffer-overflow vulnerabilities in unpatched Microsoft Internet Information Servers. It launched Trojan code in a denial-of-service attack against fixed IP addresses. The worm spread itself using a common type of vulnerability known as a buffer overflow. It used a long string repeating the character 'N' to overflow a buffer, which then allowed the worm to execute arbitrary code and infect the machine.</p> <p>The payload of the worm included the following:</p> <ul style="list-style-type: none">• Defacing the affected website with the message: HELLO! Welcome to http://www.worm.com! Hacked By Chinese!• It tried to spread itself by looking for more IIS servers on the Internet.• It waited 20–27 days after it was installed to launch DoS attacks on several fixed IP addresses. The IP address of the White House web server was among them.• When scanning for vulnerable machines, the worm did not check whether the server running on a remote machine was running a vulnerable version of IIS or whether it was running IIS at	

all.
Mitigation options:
To prevent the exploitation of the IIS vulnerability, organizations needed to apply the IIS patch from Microsoft.
References and info links:
CERT Advisory CA-2001-19 eEye Code Red advisory Code Red II analysis

Step 2: Follow the instructor's guidelines to complete the presentation.

Reflection

1. What steps can you take to protect your own computer?

Answers will vary but could include keeping the operating system and applications up to date with patches and service packs, using a personal firewall, configuring passwords to access the system and bios, configuring screensavers to timeout and requiring a password, protecting important files by making them read-only, encrypting confidential files and backup files for safe keeping.

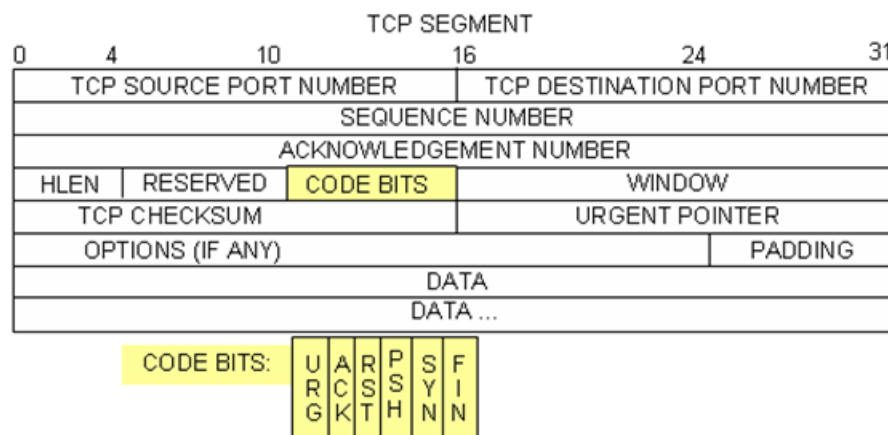
2. What are some important steps that organizations can take to protect their resources?

Answers will vary but could include the use of firewalls, intrusion detection and prevention, hardening of network devices, endpoint protection, network vulnerability tools, user education, and security policy development.

Lab - Using Wireshark to Examine TCP and UDP Captures

In Wireshark, detailed TCP information is available in the packet details pane (middle section). Highlight the first TCP datagram from the host computer, and expand the TCP datagram. The expanded TCP datagram appears similar to the packet detail pane shown below.

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.146, Dst: 198.246.117.106
▼ Transmission Control Protocol, Src Port: 54712, Dst Port: 21, Seq: 0, Len: 0
  Source Port: 54712
  Destination Port: 21
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x002 (SYN)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    .... 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
    [TCP Flags: .....S.]
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0x13e8 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
```



The image above is a TCP datagram diagram. An explanation of each field is provided for reference:

- The **TCP Source Port Number** belongs to the TCP session host that opened a connection. The value is normally a random value above 1,023.
- The **TCP Destination Port Number** is used to identify the upper layer protocol or application on the remote site. The values in the range 0–1,023 represent the “well-known ports” and are associated with popular services and applications (as described in RFC 1700), such as Telnet, FTP, and HTTP. The combination of the source IP address, source port, destination IP address, and destination port uniquely identifies the session to the sender and receiver.

Note: In the Wireshark capture below, the destination port is 21, which is FTP. FTP servers listen on port 21 for FTP client connections.

- The **Sequence Number** specifies the number of the last octet in a segment.
- The **Acknowledgment Number** specifies the next octet expected by the receiver.
- The **Code bits** have a special meaning in session management and in the treatment of segments. Among interesting values are:
 - ACK — Acknowledgment of a segment receipt.
 - SYN — Synchronize, only set when a new TCP session is negotiated during the TCP three-way handshake.
 - FIN — Finish, the request to close the TCP session.
- The **Window size** is the value of the sliding window. It determines how many octets can be sent before waiting for an acknowledgment.
- The **Urgent pointer** is only used with an Urgent (URG) flag when the sender needs to send urgent data to the receiver.
- The **Options** has only one option currently, and it is defined as the maximum TCP segment size (optional value).

Using the Wireshark capture of the first TCP session startup (SYN bit set to 1), fill in information about the TCP header.

From the PC to CDC server (only the SYN bit is set to 1):

Source IP address	192.168.1.146*
Destination IP address	198.246.117.106
Source port number	54712*
Destination port number	21
Sequence number	0 (relative)
Acknowledgement number	Not applicable for this capture
Header length	32 bytes
Window size	8192

*Student answers will vary.

Lab - Using Wireshark to Examine TCP and UDP Captures

In the second Wireshark filtered capture, the CDC FTP server acknowledges the request from the PC. Note the values of the SYN and ACK bits.

```
> Frame 2: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
> Internet Protocol Version 4, Src: 198.246.117.106, Dst: 192.168.1.146
▼ Transmission Control Protocol, Src Port: 21, Dst Port: 54712, Seq: 0, Ack: 1, Len: 0
  Source Port: 21
  Destination Port: 54712
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  1000 .... = Header Length: 32 bytes (8)
  ▼ Flags: 0x012 (SYN, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....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
    [TCP Flags: .....A..S.]
  Window size value: 8192
  [Calculated window size: 8192]
  Checksum: 0xabcd [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > Options: (12 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), SACK permitted
  > [SEQ/ACK analysis]
```

Fill in the following information regarding the SYN-ACK message.

Source IP address	198.246.117.106
Destination IP address	192.168.1.146*
Source port number	21
Destination port number	54712*
Sequence number	0 (relative)
Acknowledgment number	1 (relative)
Header length	32 bytes
Window size	8192

*Student answers will vary.

Lab - Using Wireshark to Examine TCP and UDP Captures

In the final stage of the negotiation to establish communications, the PC sends an acknowledgment message to the server. Notice only the ACK bit is set to 1, and the sequence number has been incremented to 1.

```
> Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
> Ethernet II, Src: IntelCor_1c:50:44 (00:24:d7:1c:50:44), Dst: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c)
> Internet Protocol Version 4, Src: 192.168.1.146, Dst: 198.246.117.106
▼ Transmission Control Protocol, Src Port: 54712, Dst Port: 21, Seq: 1, Ack: 1, Len: 0
  Source Port: 54712
  Destination Port: 21
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  ▼ Flags: 0x010 (ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ....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
    [TCP Flags: .....A.....]
  Window size value: 8192
  [Calculated window size: 8192]
  [Window size scaling factor: 1]
  Checksum: 0xec50 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
```

Fill in the following information regarding the ACK message.

Source IP address	192.168.1.146*
Destination IP address	198.246.117.106
Source port number	54712*
Destination port number	21
Sequence number	1 (relative)
Acknowledgement number	1 (relative)
Header length	20
Window size	8192

*Student answers will vary.

How many other TCP datagrams contained a SYN bit?

One. The first packet sent by the host at the beginning of a TCP session.

After a TCP session is established, FTP traffic can occur between the PC and FTP server. The FTP client and server communicate with each other, unaware that TCP has control and management over the session.

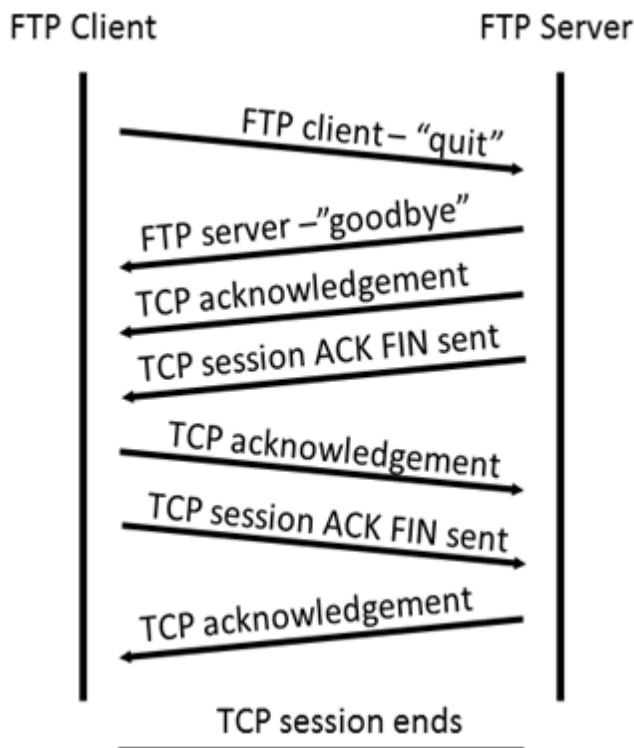
Lab - Using Wireshark to Examine TCP and UDP Captures

When the FTP server sends a *Response: 220* to the FTP client, the TCP session on the FTP client sends an acknowledgment to the TCP session on the server. This sequence is visible in the Wireshark capture below.

4	0.116212	198.246.117.106	192.168.1.146	FTP	81 Response: 220 Microsoft FTP Service
5	0.121669	192.168.1.146	198.246.117.106	FTP	68 Request: OPTS UTF8 ON
6	0.180369	198.246.117.106	192.168.1.146	FTP	112 Response: 200 OPTS UTF8 command successful - UTF8 enc...

>	Frame 4: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
>	Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)
>	Internet Protocol Version 4, Src: 198.246.117.106, Dst: 192.168.1.146
>	Transmission Control Protocol, Src Port: 21, Dst Port: 54712, Seq: 1, Ack: 1, Len: 27
>	File Transfer Protocol (FTP)
>	220 Microsoft FTP Service\r\n
>	Response code: Service ready for new user (220)
>	Response arg: Microsoft FTP Service

When the FTP session has finished, the FTP client sends a command to “quit”. The FTP server acknowledges the FTP termination with a *Response: 221 Goodbye*. At this time, the FTP server TCP session sends a TCP datagram to the FTP client, announcing the termination of the TCP session. The FTP client TCP session acknowledges receipt of the termination datagram, then sends its own TCP session termination. When the originator of the TCP termination (the FTP server) receives a duplicate termination, an ACK datagram is sent to acknowledge the termination and the TCP session is closed. This sequence is visible in the diagram and capture below.



Lab - Using Wireshark to Examine TCP and UDP Captures

By applying an **ftp** filter, the entire sequence of the FTP traffic can be examined in Wireshark. Notice the sequence of the events during this FTP session. The username **anonymous** was used to retrieve the Readme file. After the file transfer completed, the user ended the FTP session.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.116212	198.246.117.106	192.168.1.146	FTP	81	Response: 220 Microsoft FTP Service
5	0.121669	192.168.1.146	198.246.117.106	FTP	68	Request: OPTS UTF8 ON
6	0.180369	198.246.117.106	192.168.1.146	FTP	112	Response: 200 OPTS UTF8 command successful - UTF8 encoding r
18	34.993981	192.168.1.146	198.246.117.106	FTP	70	Request: USER anonymous
19	35.052234	198.246.117.106	192.168.1.146	FTP	126	Response: 331 Anonymous access allowed, send identity (e-ma
21	39.133664	192.168.1.146	198.246.117.106	FTP	61	Request: PASS
22	39.188301	198.246.117.106	192.168.1.146	FTP	75	Response: 230 User logged in.
26	43.325986	192.168.1.146	198.246.117.106	FTP	82	Request: PORT 192,168,1,146,213,185
29	43.381803	198.246.117.106	192.168.1.146	FTP	84	Response: 200 PORT command successful.
30	43.390255	192.168.1.146	198.246.117.106	FTP	60	Request: NLST
35	43.447231	198.246.117.106	192.168.1.146	FTP	108	Response: 125 Data connection already open; Transfer startin
36	43.448271	198.246.117.106	192.168.1.146	FTP	78	Response: 226 Transfer complete.
40	55.104521	192.168.1.146	198.246.117.106	FTP	82	Request: PORT 192,168,1,146,213,186
43	55.171392	198.246.117.106	192.168.1.146	FTP	84	Response: 200 PORT command successful.
44	55.182471	192.168.1.146	198.246.117.106	FTP	67	Request: RETR Readme
49	55.247925	198.246.117.106	192.168.1.146	FTP	108	Response: 125 Data connection already open; Transfer startin
53	55.294530	198.246.117.106	192.168.1.146	FTP	78	Response: 226 Transfer complete.
56	61.170643	192.168.1.146	198.246.117.106	FTP	60	Request: QUIT
58	61.723390	198.246.117.106	192.168.1.146	FTP	68	Response: 221 Goodbye.

Apply the TCP filter again in Wireshark to examine the termination of the TCP session. Four packets are transmitted for the termination of the TCP session. Because TCP connection is full-duplex, each direction must terminate independently. Examine the source and destination addresses.

In this example, the FTP server has no more data to send in the stream. It sends a segment with the FIN flag set in frame 59. The PC sends an ACK to acknowledge the receipt of the FIN to terminate the session from the server to the client in frame 60.

In frame 61, the PC sends a FIN to the FTP server to terminate the TCP session. The FTP server responds with an ACK to acknowledge the FIN from the PC in frame 65. Now the TCP session terminated between the FTP server and PC.

57	61.457683	192.168.1.146	198.246.117.106	TCP	60	[TCP Retransmission] 54712 → 21 [PSH, ACK] Seq=113 Ac...
58	61.723390	198.246.117.106	192.168.1.146	FTP	68	Response: 221 Goodbye.
59	61.723391	198.246.117.106	192.168.1.146	TCP	54	21 → 54712 [FIN, ACK] Seq=409 Ack=119 Win=130816 Len=0
60	61.723507	192.168.1.146	198.246.117.106	TCP	54	54712 → 21 [ACK] Seq=119 Ack=410 Win=7784 Len=0
61	61.729268	192.168.1.146	198.246.117.106	TCP	54	54712 → 21 [FIN, ACK] Seq=119 Ack=410 Win=7784 Len=0
62	61.752612	198.246.117.106	192.168.1.146	TCP	68	[TCP Out-Of-Order] 21 → 54712 [FIN, PSH, ACK] Seq=395...
63	61.752678	192.168.1.146	198.246.117.106	TCP	66	[TCP Dup ACK 60#1] 54712 → 21 [ACK] Seq=120 Ack=410 W...
64	62.028356	198.246.117.106	192.168.1.146	TCP	66	[TCP Dup ACK 58#1] 21 → 54712 [ACK] Seq=410 Ack=119 W...
65	62.028357	198.246.117.106	192.168.1.146	TCP	54	21 → 54712 [ACK] Seq=410 Ack=120 Win=130816 Len=0

> Frame 59: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0

> Ethernet II, Src: BelkinIn_9f:6b:8c (14:91:82:9f:6b:8c), Dst: IntelCor_1c:50:44 (00:24:d7:1c:50:44)

> Internet Protocol Version 4, Src: 198.246.117.106, Dst: 192.168.1.146

> Transmission Control Protocol, Src Port: 21, Dst Port: 54712, Seq: 409, Ack: 119, Len: 0

Part 2: Identify UDP Header Fields and Operation Using a Wireshark TFTP Session Capture

In Part 2, you use Wireshark to capture a TFTP session and inspect the UDP header fields.

Step 1: Set up this physical topology and prepare for TFTP capture.



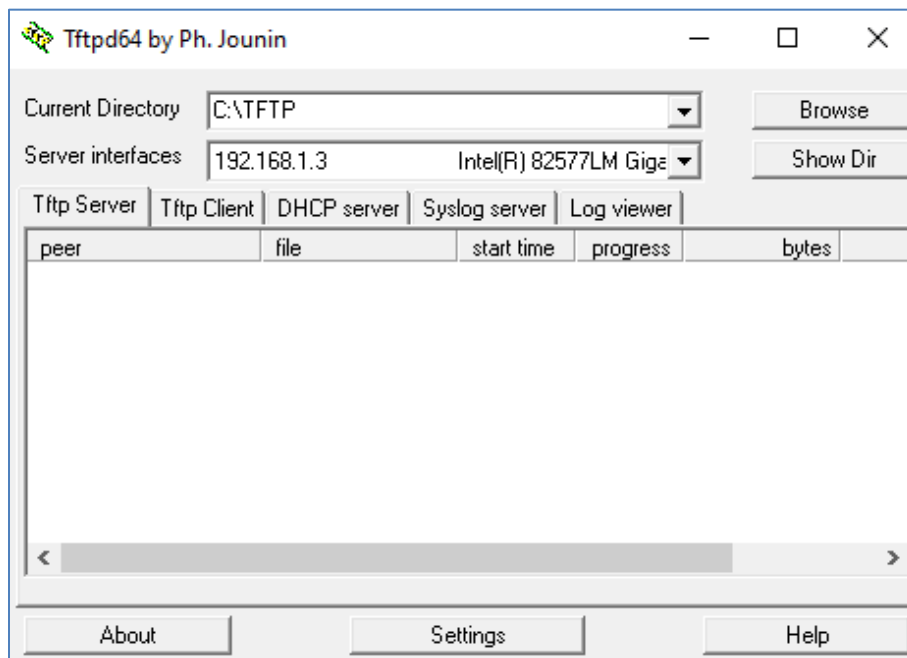
- Establish a console and Ethernet connection between PC-A and S1.
- Manually configure the IP address on the PC to 192.168.1.3. It is not required to set the default gateway.
- Configure the switch. Assign an IP address of 192.168.1.1 to VLAN 1. Verify connectivity with the PC by pinging 192.168.1.3. Troubleshoot as necessary.

```
Switch> enable
Switch# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# host S1
S1(config)# interface vlan 1
S1(config-if)# ip address 192.168.1.1 255.255.255.0
S1(config-if)# no shut
*Mar  1 00:37:50.166: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
*Mar  1 00:37:50.175: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1,
changed state to up
S1(config-if)# end
S1# ping 192.168.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/203/1007 ms
d. Save the running configuration to NVRAM.
S1# copy run start
```

Step 2: Prepare the TFTP server on the PC.

- If it does not already exist, create a folder on the PC C: drive called **TFTP**. The files from the switch will be copied to this location.
- Start **tfptd32** or **Tftpd64** on the PC.
- Click **Browse** and change the current directory to **C:\TFTP**.

The TFTP server should look like this:



Notice that in **Current Directory**, it lists the TFTP Server (PC-A) interface with the IP address of **192.168.1.3**.

- d. Test the ability to copy a file using TFTP from the switch to the PC. Troubleshoot as necessary.

```
S1# copy start tftp
```

```
Address or name of remote host []? 192.168.1.3
```

```
Destination filename [s1-config]?
```

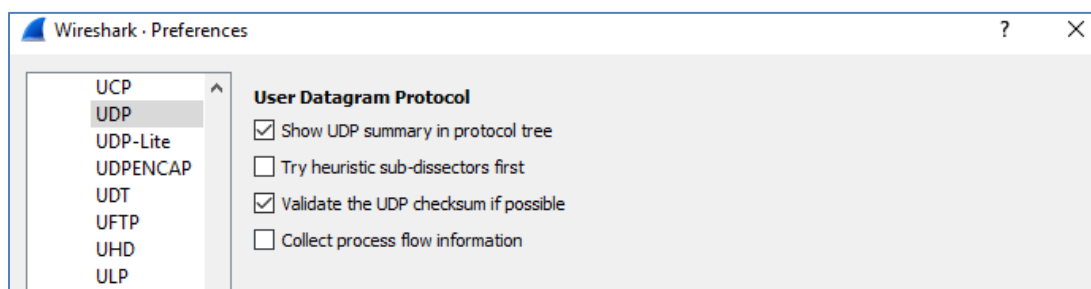
```
!!
```

```
1083 bytes copied in 0.84 secs
```

If you see that the file has been copied, then you are ready to go on to the next step. If the file has not been copied, troubleshoot as needed. If you get the **%Error opening tftp (Permission denied)** error, determine whether your firewall is blocking TFTP and whether you are copying the file to a location where your username has adequate permission, such as the desktop.

Step 3: Capture a TFTP session in Wireshark

- a. Open Wireshark. From the **Edit** menu, choose **Preferences** and click the (+) sign to expand **Protocols**. Scroll down and select **UDP**. Click the **Validate the UDP Checksum if Possible** check box and click **OK**.



Instructor Note: This is a change from previous versions of this lab because the technology has changed. Search for “checksum offloading in Wireshark”.

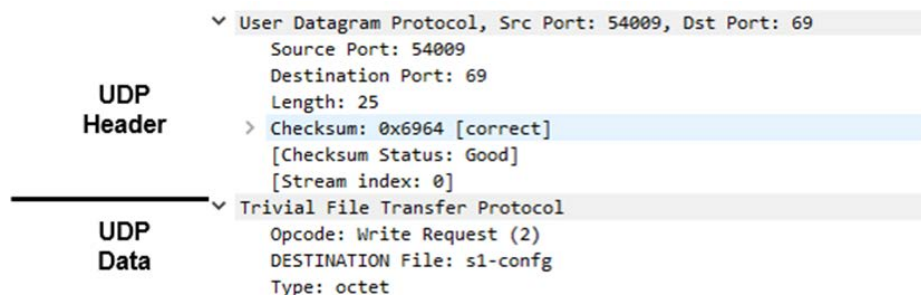
- Start a Wireshark capture.
- Run the **copy start tftp** command on the switch.
- Stop the Wireshark capture.

No.	Time	Source	Destination	Protocol	Length	Info
10	17.006137	192.168.1.1	192.168.1.3	TFTP	64	Write Request, File: s1-config, Transfer type
11	17.008212	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 0
12	17.012084	192.168.1.1	192.168.1.3	TFTP	558	Data Packet, Block: 1
13	17.012376	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 1
14	17.014029	192.168.1.1	192.168.1.3	TFTP	558	Data Packet, Block: 2
15	17.014133	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 2
16	17.017114	192.168.1.1	192.168.1.3	TFTP	105	Data Packet, Block: 3 (last)
17	17.017219	192.168.1.3	192.168.1.1	TFTP	46	Acknowledgement, Block: 3

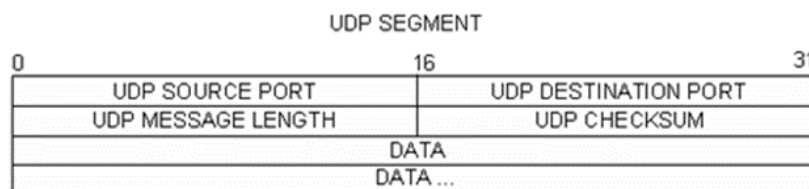
- Set the filter to **tftp**. Your output should look similar to the output shown above. This TFTP transfer is used to analyze transport layer UDP operations.

Instructor Note: If students point out UDP acknowledgments, explain that the UDP header does not contain an acknowledgment field. It is the responsibility of the upper-layer protocol, in this case TFTP, to manage data transfer and receipt information. This will be shown during the UDP datagram examination.

Detailed UDP information is available in the Wireshark packet details pane. Highlight the first UDP datagram from the host computer and move the mouse pointer to the packet details pane. It may be necessary to adjust the packet details pane and expand the UDP record by clicking the protocol expand box. The expanded UDP datagram should look similar to the diagram below.



The figure below is a UDP datagram diagram. Header information is sparse, compared to the TCP datagram. Similar to TCP, each UDP datagram is identified by the UDP source port and UDP destination port.



Lab - Using Wireshark to Examine TCP and UDP Captures

Using the Wireshark capture of the first UDP datagram, fill in information about the UDP header. The checksum value is a hexadecimal (base 16) value, denoted by the preceding 0x code:

Source IP address	192.168.1.1
Destination IP address	192.168.1.3
Source port number	54009*
Destination port number	69
UDP message length	25 bytes*
UDP checksum	0x6964 [correct]*

*Student answers will vary.

How does UDP verify datagram integrity?

A checksum is sent in the UDP datagram, and the datagram checksum value is recomputed upon receipt. If the computed checksum is identical to the sent checksum, then the UDP datagram is assumed to be complete.

Examine the first frame returned from the tftpd server. Fill in the information about the UDP header:

Source IP address	192.168.1.3
Destination IP address	192.168.1.1
Source port number	65001*
Destination port number	54009*
UDP message length	12 bytes*
UDP checksum	Checksum: 0x8372, incorrect, should be 0xab99 (maybe caused by "UDP checksum offload"?)*

*Student answers will vary.

```
▼ User Datagram Protocol, Src Port: 65001, Dst Port: 54009
  Source Port: 65001
  Destination Port: 54009
  Length: 12
  > Checksum: 0x8372 incorrect, should be 0xab99 (maybe caused by "UDP checksum offload"?
    [Checksum Status: Bad]
    [Stream index: 1]
▼ Trivial File Transfer Protocol
  Opcode: Acknowledgement (4)
  [DESTINATION File: s1-config]
  Block: 0
```

Notice that the return UDP datagram has a different UDP source port, but this source port is used for the remainder of the TFTP transfer. Because there is no reliable connection, only the original source port used to begin the TFTP session is used to maintain the TFTP transfer.

Also, notice that the UDP Checksum is incorrect. This is most likely caused by UDP checksum offload. You can learn more about why this happens by searching for "UDP checksum offload".

Reflection

This lab provided the opportunity to analyze TCP and UDP protocol operations from captured FTP and TFTP sessions. How does TCP manage communication differently from UDP?

TCP manages communication much differently than UDP does because reliability and guaranteed delivery require additional control over the communication channel. UDP has less overhead and control, and the upper-layer protocol must provide some type of acknowledgment control. Both protocols, however, transport data between clients and servers using application layer protocols and are appropriate for the upper-layer protocol each supports.

Challenge

Because neither FTP nor TFTP are secure protocols, all transferred data is sent in clear text. This includes any user IDs, passwords, or clear-text file contents. Analyzing the upper-layer FTP session will quickly identify the user ID, password, and configuration file passwords. Upper-layer TFTP data examination is more complicated, but the data field can be examined, and the configuration's user ID and password information extracted.

Cleanup

Unless directed otherwise by your instructor:

- 1) Remove the files that were copied to your PC.
- 2) Erase the configurations on S1.
- 3) Remove the manual IP address from the PC and restore internet connectivity.

Device Configs

Switch S1

```
S1#show run
Building configuration...

!
hostname S1
!
interface Vlan1
 ip address 192.168.1.1 255.255.255.0
!
end
```

Class Activity - We Need to Talk, Again (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain how transport layer protocols and services support communications across data networks.

Background /Scenario

Note: It is important that the students have completed the Introductory MA for this chapter. This activity works best in medium-sized groups of 6 to 8 students.

The instructor will whisper a complex message to the first student in a group. An example of the message might be “We are expecting a blizzard tomorrow. It should be arriving in the morning and school will be delayed 2 two hours so bring your homework.”

That student whispers the message to the next student in the group. Each group follows this process until all members of each group have heard the whispered message. Here are the rules you are to follow:

Here are the rules you are to follow:

- You can whisper the message in short parts to your neighbor AND you can repeat the message parts after verifying your neighbor heard the correct message.
- Small parts of the message may be checked and repeated again (clockwise OR counter-clockwise to ensure accuracy of the message parts) by whispering. A student will be assigned to time the entire activity.
- When the message has reached the end of the group, the last student will say aloud what she or he heard. Small parts of the message may be repeated (i.e., re-sent), and the process can be restarted to ensure that ALL parts of the message are fully delivered and correct.
- The Instructor will restate the original message to check for quality delivery.

Instructor Note: Please initiate discussion about what happened in the Activity. Focus on these three questions:

1. Was the message complete when it reached the last student?
2. Was the message correct as delivered to the last person?
3. Did it take very long for the message to get to the last student?

If you were depending on this message to drive your personal/business calendar, studying schedule, etc., would the contents of this message need to be clear and correct when you received them?

Would the length of time taken to deliver the message be important to the sender and recipient?

Compare the Introductory MA of this chapter to the Review MA (this activity). What differences do you notice about the delivery of the message?

Please remind students that TCP and UDP protocols ensure that:

- Network communications with different levels of importance are sent and received according to their levels of importance.
- The type of data will affect whether TCP or UDP will be used as the method of delivery.
- The time in which the message must be delivered will affect whether TCP or UDP will be used as the method of delivery.

Reflection

1. Would the contents of this message need to be clear and correct when you received them, if you were depending on this message to drive your personal/business calendar, studying schedule, etc.,?

The importance of full messages being delivered fully from sender to recipient – TCP guarantees full delivery.

2. Would the length of time taken to deliver the message be an important factor to the sender and recipient?

The importance of **timing** – to the details of the message and to the date/time needed to take action on the message is important to all facets of data transmission – windowing and sliding windows takes care of this in TCP – UDP does not.

3. Compare the Introductory MA of this chapter to this activity. What differences do you notice about the delivery of the message?

Representative (discussion) answers may look like the following suggestions:

- The message took a lot longer to get from the initiator to the last recipient.
- More (if not all) of the message arrived and the content was probably better (if not completely accurate)

Identify elements of the model that map to IT-related content:

- Establishing a method of transporting information over a network is important to obtain complete delivery of network data (TCP is guaranteed – UDP is not).
- Ensuring quality of delivery of data over a network is affected by the type of transport used. TCP will check for checksum errors and will acknowledge and synchronize each segment. In contrast, UDP has no error correction.
- Selecting TCP or UDP based on a time-factor for delivery of data over a communications system. Windows are set and adjusted in TCP if congestion is found on the network; whereas, UDP keeps transmitting.
- While unreliable, UDP has its value: the message in first activity was delivered much faster than in the second. If the message was simpler (such as a message consisting of a single digit, for example), the first transport method (UDP) could prove itself much better than the second (TCP).

Class Activity – Application Investigation (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain how the Application layer provides support to end-user applications.

Background / Scenario

It is the beginning of your work week. Your employer has decided to install IP telephones in your workplace, which results in the network being inoperable until next week.

However, your work must continue. You have emails to send and quotes to write for your manager's approval. Due to possible security issues, you are not allowed to use personal or external computer systems, equipment, or off-site equipment and systems.

Your instructor may ask you to complete the questions from both scenarios below. Answer the questions fully for the scenario(s). Be prepared to discuss your answers in class.

Emails

- What method(s) can you use to send email communication?
- How can you send the same email to multiple recipients?
- How can you get a large attachment to multiple recipients?
- Are these methods cost effective to your corporation?
- Do these methods violate any security policies of your corporation?

Quote for Manager's Approval

- You have a desktop application software package installed on your computer. Will it be relatively easy to produce the quote your manager needs for the new contract due by the end of the week? What limitations will be experienced while trying to complete the quote?
- How will you present the quote to your manager for approval? How do you think he or she will send the quote to the client for their approval?
- Are these methods cost effective to your corporation? Justify your answer.

Instructor Note: This optional Modeling Activity is introductory in nature. Its purpose is to focus on how the application layer is necessary in order for networking to operate effectively. To save classroom time (for discussion), students may complete only one of the two scenarios.

Reflection

What steps did you identify as important to communicating without network applications available to you for a week in your workplace? Which steps were not important? Justify your answer.

Class Activity – Application Investigation

To resolve this issue, some alternatives to pursue might include:

Emails:

What method(s) can you use to send email communication? Correspondence might have to take the form of post-office mail or hand delivery. Messages may be handwritten or printed locally.

How could you send the same email to multiple recipients? Once the handwritten letter is finished, copies can be made for all recipients. Then, the copies can be sent individually to the recipients.

If a large attachment was necessary to send, how would you get it to multiple recipients? Multiple copies would have to be made of the large attachment to send with the locally-produced letter.

Are these methods cost effective to your corporation? No, this would take a lot of time, resources, and steps to ready the mail and attachment for delivery

Quote for Manager's Approval:

You have a desktop application software package installed on your computer. Will it be relatively easy to produce the quote your manager needs for the new contract due by the end of the week? Yes, the local application software should not be affected by having no access to the network.

When you finish writing the quote, how will you present it to your manager for approval? How will he or she send the quote to the client for their consideration for approval? The quote will need to be printed (or saved to media). The hard copy (or media copy) will need to be delivered personally to the manager. Post-office mail probably would need to be used to send the quote to the client in this example.

Are these methods cost effective to your corporation? No, it takes time to print the quote, deliver it to the manager, get it ready for post-office delivery, etc.

Identify elements of the model that map to IT content:

- Network applications make communication in the workplace easier.
- Network applications affect the amount of work done on a daily basis.
- Processing time is increased without the use of network applications.
- Network applications reduce the cost of completing business communications.

Lab - Researching Peer-to-Peer File Sharing (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Identify P2P Networks, File Sharing Protocols, and Applications

Part 2: Research P2P File Sharing Issues

Part 3: Research P2P Copyright Litigations

Background / Scenario

Peer-to-peer (P2P) computing is a powerful technology that has many uses. P2P networks can be used to share and exchange files, and other electronic materials.

The use of P2P networks to upload, download, or share copyrighted material, such as movies, music, and software, can violate the rights of copyright owners. In the P2P file-sharing context, infringement may occur when one person purchases an authorized copy and then uploads it to a P2P network to share with others. Both the individual who makes the file available and those making copies may be found to have infringed the rights of the copyright owners and may be violating copyright law.

Another problem with P2P file sharing is that very little protection is in place to ensure that the files exchanged in these networks are not malicious. P2P networks are an ideal medium for spreading malware, such as computer viruses, worms, Trojan horses, spyware, adware, and other malicious programs.

In this lab, you will research available P2P file sharing software and identify issues that can arise from the use of this technology.

Required Resources

Device with Internet access

Part 1: Identify P2P Networks, File Sharing Protocols, and Applications

In Part 1, you will research P2P networks and identify popular P2P protocols and applications.

Step 1: Define P2P networking.

- a. What is a P2P network?

A P2P network allows each computer in the network to act as a client or server for the other computers in the network. This allows shared access to various resources without the need for a central server.

- b. Identify at least two advantages that P2P provides over client-server architecture.

In P2P networks, clients provide resources, which may include bandwidth, storage space, and computing power. This property is one of the primary advantages of using P2P networks because it makes the setup and running costs small for the original content distributor. As nodes arrive and demand on the system increases, the total capacity of the system increases and the likelihood of failure decreases. If one peer on the network fails to function properly, the whole network is not compromised or damaged. In contrast, with a typical client-server architecture, clients share their demands with the system but not their resources. In this case, as more clients join the system, fewer resources are available to serve each client. If the central server fails, the entire network is taken down. The decentralized nature of P2P networks removes the single point of failure that can be inherent in a client-server based system.

- c. Identify at least two disadvantages of P2P networks.

A P2P network is decentralized, which makes it difficult to administer. Security is difficult to implement and maintain, which allows for the possibility of copyrighted material and malware to be transmitted over a P2P network.

Step 2: Identify P2P file sharing protocols and applications.

- a. Identify at least two P2P file sharing protocols used today.

Answers will vary, but can include: Ares, BitTorrent, Direct Connect, FastTrack, eDonkey, Gnutella, MANOLITO/MP2PN, OpenNap, 100BAo, Aimster, Applejuice, Freenet, GnucleusLAN, GoBoogy, KuGoo, OpenFT, MUTE, Soribada, Soulseek, and Xunlei.

- b. Identify at least two popular P2P file sharing applications available today.

Answers will vary, but can include: ABC [Yet Another Bit Torrent Client], Ares Galaxy, Azureus, BCDC++, BearShare, BitComet, BitSpirit, BitTornado, BitTorrent.Net, DC++, eMule, G3 Torrent, Gnotella, Gnucleus, Grokster, GTK-gnutella, iMesh, Kazaa, LimeWire, Mactella, mIMAC, MLdonkey, Morpheus, Napigator, NeoModus Direct, onect, Overnet, QTorrent, Shareaza, uTorrent, Warez P2P, and WinMX.

- c. What P2P file sharing protocol is attributed to producing the most P2P traffic on the Internet today?

Answers may vary, but after the demise of LimeWire most of the P2P traffic is likely from BitTorrent. As of January 2012, BitTorrent was utilized by 150 million active users (according to BitTorrent, Inc.). At any given instant, BitTorrent has (on average) more active users than YouTube and Facebook combined. This refers to the number of active users at any instant, not the total number of unique users.

Part 2: Research P2P File Sharing Issues

In Part 2, you will research P2P copyright infringement and identify other issues that can occur with P2P file sharing.

Step 1: Research P2P copyright infringement.

- a. What does the acronym DMCA stand for and what is it?

The Digital Millennium Copyright Act (DMCA) is a United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures (commonly known as digital rights management or DRM) that control access to copyrighted works. It also criminalizes the act of circumventing an access control, whether or not there is an actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet. This law passed on October 12, 1998, by a unanimous vote in the United States Senate and was signed into law by President Bill Clinton on October 28, 1998.

- b. Name two associations that actively pursue P2P copyright infringement?

The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have instituted legal actions against a number of P2P file sharing sites and individuals.

- c. What are the penalties for copyright infringement?

Penalties, both civil and criminal, can be severe. Civil penalties may include actual damages and profits, or statutory damages (maximum amount of \$30,000 per work that is infringed). The court can also award reasonable attorney's fees and costs and increase the damages in the case of willful infringement (maximum amount of \$150,000 per work that is infringed). Criminal penalties can include fines and imprisonment.

- d. What are the file sharing copyright laws in your area? Are they more strict or less strict than those in other areas of the world? How aggressively do enforcement agencies in your area pursue those who share copyrighted material?

Answers will vary depending on locale.

Step 2: Research other P2P issues.

- a. What types of malware can be transported through P2P file sharing?

Answers may vary, but can include: adware, computer viruses, spyware, Trojan horses, and worms.

- b. What is Torrent poisoning?

Torrent poisoning is the act of using the BitTorrent protocol to intentionally share corrupt data or data with misleading file names. The practice of uploading fake torrents is sometimes carried out by anti-piracy organizations as an attempt to prevent the P2P sharing of copyrighted content and to gather the IP addresses of downloaders.

- c. How could identity theft occur through the use of P2P file sharing?

If the P2P client software is incorrectly configured, it may provide access to the personal information and files stored on your computer.

Part 3: Research P2P Copyright Litigations

In Part 3, you will research and identify historical legal actions that have occurred as a result of P2P copyright infringement.

- a. What was the first well-known P2P application that specialized in MP3 file sharing and was closed by court order?

Napster was originally released in 1999 and then closed by court order in July 2001. It was co-founded by Shawn Fanning, John Fanning, and Sean Parker. At its peak, there were 25 million users, 80 million songs, and the system never crashed.

- b. What was one of the largest P2P file sharing lawsuits ever?

In May of 2011, the law firm Dunlap, Grubb, and Weaver (U.S. Copyright Group) sued 24,583 BitTorrent users for sharing the film titled "Hurt Locker." The case was the largest BitTorrent lawsuit.

Reflection

How can you be sure that the files you are downloading from P2P networks are not copyrighted and are safe from malware?

There is no absolute assurance that P2P files are free of malware and not copyrighted. Use P2P file sharing applications at your own risk.

Lab - Observing DNS Resolution (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Observe the DNS Conversion of a URL to an IP Address

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

Background / Scenario

The Domain Name System (DNS) is invoked when you type a Uniform Resource Locator (URL), such as <http://www.cisco.com>, into a web browser. The first part of the URL describes which protocol is used. Common protocols are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), and File Transfer Protocol (FTP).

DNS uses the second part of the URL, which in this example is www.cisco.com. DNS translates the domain name (www.cisco.com) to an IP address to allow the source host to reach the destination host. In this lab, you will observe DNS in action and use the **nslookup** (name server lookup) command to obtain additional DNS information. Work with a partner to complete this lab.

Required Resources

1 PC (Windows 7 or 8 with Internet and command prompt access)

Part 1: Observe the DNS Conversion of a URL to an IP Address

- Click the **Windows Start** button, type **cmd** into the search field, and press Enter. The command prompt window appears.
- At the command prompt, ping the URL for the Internet Corporation for Assigned Names and Numbers (ICANN) at **www.icann.org**. ICANN coordinates the DNS, IP addresses, top-level domain name system management, and root server system management functions. The computer must translate www.icann.org into an IP address to know where to send the Internet Control Message Protocol (ICMP) packets.

The first line of the output displays www.icann.org converted to an IP address by DNS. You should be able to see the effect of DNS, even if your institution has a firewall that prevents ping, or if the destination server has prevented you from ping, or if the destination server has prevented you from ping, or if the destination server has prevented you from ping.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.icann.org** to translate into an IPv4 address if desired.

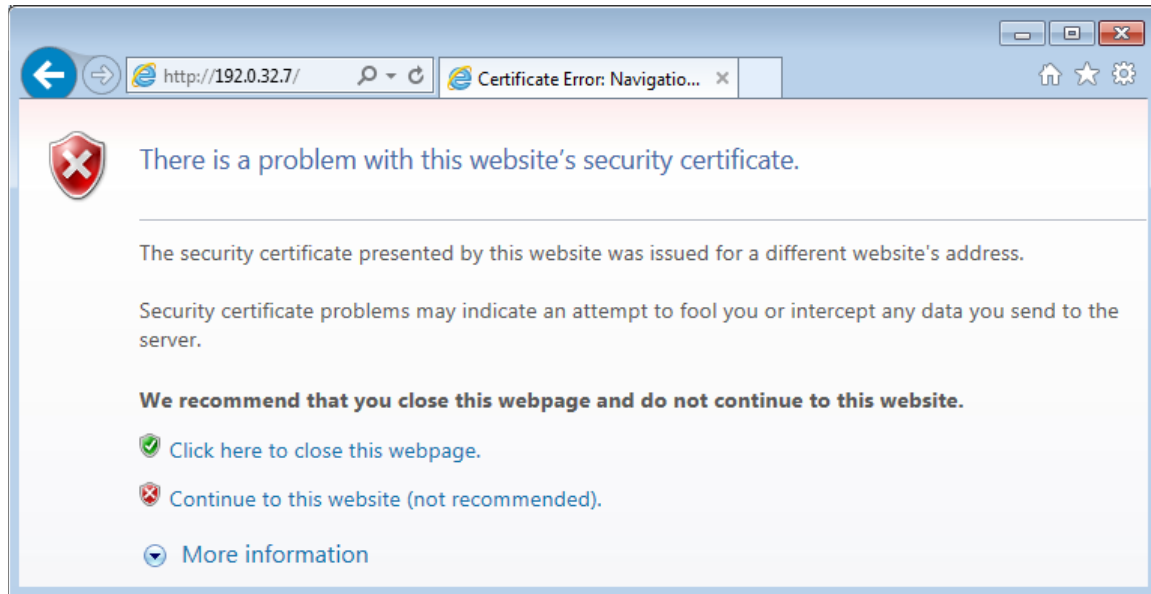
```
C:\>ping www.icann.org

Pinging www.vip.icann.org [192.0.32.7] with 32 bytes of data:
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=23ms TTL=246
Reply from 192.0.32.7: bytes=32 time=24ms TTL=246
Reply from 192.0.32.7: bytes=32 time=28ms TTL=246

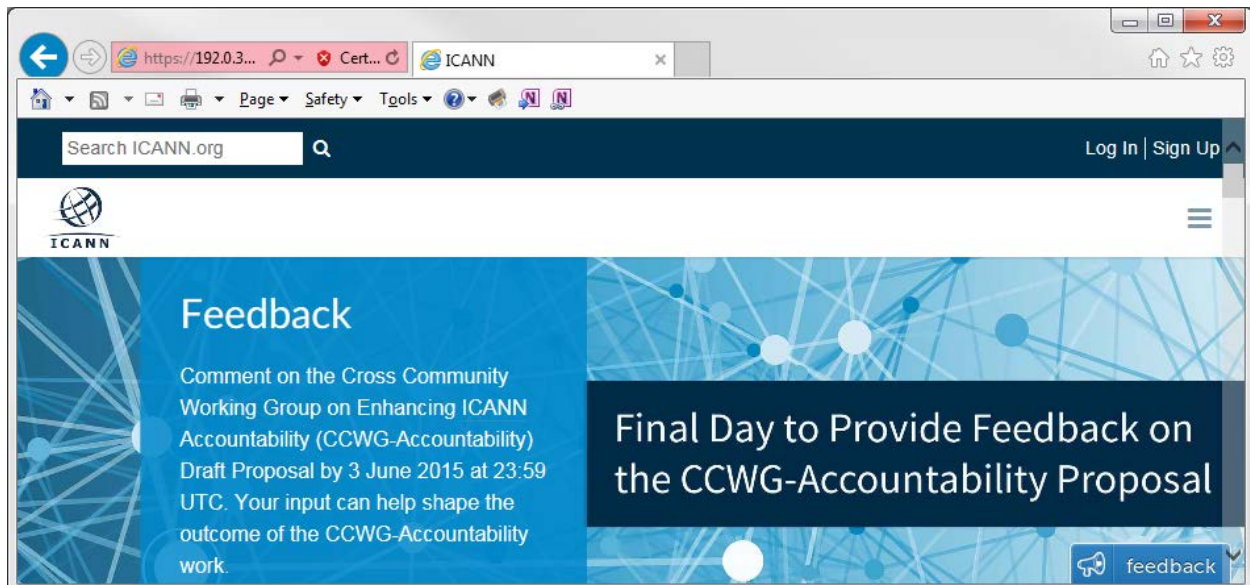
Ping statistics for 192.0.32.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 23ms, Maximum = 28ms, Average = 24ms
```

Record the IP address of www.icann.org. _____ 192.0.32.7

- c. Type the IP address from **step b** into a web browser, instead of the URL. Click **Continue to this website (not recommended)**, to proceed.



- d. Notice that the ICANN home web page is displayed.



Most humans find it easier to remember words, rather than numbers. If you tell someone to go to **www.icann.org**, they can probably remember that. If you told them to go to 192.0.32.7, they would have a difficult time remembering an IP address. Computers process in numbers. DNS is the process of translating words into numbers. There is a second translation that takes place. Humans think in Base 10 numbers. Computers process in Base 2 numbers. The Base 10 IP address 192.0.32.7 in Base 2 numbers is 11000000.00000000.00100000.00000111. What happens if you cut and paste these Base 2 numbers into a browser?

The web site does not display. The software code used in web browsers recognizes Base 10 numbers. It does not recognize Base 2 numbers.

- e. Now type **ping** www.cisco.com.

Note: If the domain name is resolved to an IPv6 address, use the command **ping -4 www.cisco.com** to translate into an IPv4 address if desired.

```
C:\>ping www.cisco.com

Pinging e144.dscc.akamaiedge.net [23.1.144.170] with 32 bytes of data:
Reply from 23.1.144.170: bytes=32 time=51ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58
Reply from 23.1.144.170: bytes=32 time=50ms TTL=58

Ping statistics for 23.1.144.170:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 51ms, Average = 50ms
```

- f. When you ping www.cisco.com, do you get the same IP address as the example? Explain.

Answer will vary depending upon where you are geographically. Cisco hosts its web content on a series of mirror servers. This means that Cisco uploads the exact same content to geographically diverse (spread out all over the world) servers. When someone tries to reach www.cisco.com, the traffic is directed to the closest mirror server.

- g. Type the IP address that you obtained when you pinged www.cisco.com into a browser. Does the web site display? Explain.

The **cisco.com** web site does not display. There are at least two possible explanations for this: 1. Some web servers are configured to accept IP addresses sent from a browser and some are not. 2. It may be a firewall rule in the Cisco security system that prohibits an IP address from being sent via a browser.

Part 2: Observe DNS Lookup Using the nslookup Command on a Web Site

- a. At the command prompt, type the **nslookup** command.

```
C:\>nslookup
Default Server:  dslrouter.westell.com
Address:  192.168.1.1

>
```

What is the default DNS server used? _____

Site dependent

Notice how the command prompt changed to a greater than (>) symbol. This is the **nslookup** prompt. From this prompt, you can enter commands related to DNS.

At the prompt, type **?** to see a list of all the available commands that you can use in **nslookup** mode.

- b. At the prompt, type **www.cisco.com**.

```
> www.cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name: e144.dscb.akamaiedge.net
Addresses: 2600:1408:7:1:9300::90
           2600:1408:7:1:8000::90
           2600:1408:7:1:9800::90
           23.1.144.170
Aliases: www.cisco.com
          www.cisco.com.akadns.net
          wwwds.cisco.com.edgekey.net
          wwwds.cisco.com.edgekey.net.globalredir.akadns.net
```

What is the translated IP address? _____

From a specific location, 23.1.144.170.

Note: The IP address from your location will most likely be different because Cisco uses mirrored servers in various locations around the world.

Is it the same as the IP address shown with the **ping** command? _____ **Yes**

Under addresses, in addition to the 23.1.144.170 IP address, there are the following numbers: 2600:1408:7:1:9300::90, 2600:1408:7:1:8000::90, 2600:1408:7:1:9800::90. What are these?

IPv6 (IP version 6) IP addresses at which the web site is reachable.

- c. At the prompt, type the IP address of the Cisco web server that you just found. You can use **nslookup** to get the domain name of an IP address if you do not know the URL.

```
> 23.1.144.170
Server: dslrouter.westell.com
Address: 192.168.1.1

Name: a23-1-144-170.deploy.akamaitechnologies.com
Address: 23.1.144.170
```

You can use the **nslookup** tool to translate domain names into IP addresses. You can also use it to translate IP addresses into domain names.

Using the **nslookup** tool, record the IP addresses associated with www.google.com.

Answers may vary. At the time of writing, the IP addresses are 173.194.75.147, 173.194.75.105, 173.194.75.99, 173.194.75.103, 173.194.75.106, and 173.194.75.104.

```
> www.google.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:400c:c01::93
           173.194.75.147
           173.194.75.105
           173.194.75.99
           173.194.75.103
           173.194.75.106
           173.194.75.104
```

Part 3: Observe DNS Lookup Using the nslookup Command on Mail Servers

- a. At the prompt, type **set type=mx** to use **nslookup** to identify mail servers.

```
> set type=mx
```

- b. At the prompt, type **cisco.com**.

```
> cisco.com
Server: dslrouter.westell.com
Address: 192.168.1.1

Non-authoritative answer:
cisco.com      MX preference = 10, mail exchanger = rcdn-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = alln-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = ams-mx-01.cisco.com
cisco.com      MX preference = 15, mail exchanger = rtp-mx-01.cisco.com

ams-mx-01.cisco.com  internet address = 64.103.36.169
rcdn-mx-01.cisco.com internet address = 72.163.7.166
```

A fundamental principle of network design is redundancy (more than one mail server is configured). In this way, if one of the mail servers is unreachable, then the computer making the query tries the second mail server. Email administrators determine which mail server is contacted first by using **MX preference** (see above image). The mail server with the lowest **MX preference** is contacted first. Based upon the output above, which mail server will be contacted first when the email is sent to cisco.com?

rcdn-mx-01.cisco.com

- c. At the nslookup prompt, type **exit** to return to the regular PC command prompt.
- d. At the PC command prompt, type **ipconfig /all**.
- e. Write the IP addresses of all the DNS servers that your school uses.

Site-dependent

Reflection

What is the fundamental purpose of DNS?

People process in words. Computers process in numbers. People have a difficult time remembering a long string of numbers. Therefore, DNS exists to translate the “numbers” world of computers to the “words” world of people.

Lab - Exploring FTP (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Use FTP from a Command Prompt

Part 2: Use FTP in a Browser

Part 3: Download an FTP File Using WS_FTP LE (Optional)

Background / Scenario

The File Transfer Protocol (FTP) is part of the TCP/IP suite. FTP is used to transfer files from one network device to another network device. Windows includes an FTP client application that you can execute from the command prompt. There are also free graphical user interface (GUI) versions of FTP that you can download. The GUI versions are easier to use than typing from a command prompt. FTP is frequently used for the transfer of files that may be too large to send using email.

When using FTP, one computer is normally the server and the other computer is the client. When accessing the server from the client, you need to provide a username and password. Some FTP servers have a user named **anonymous**. You can access these types of sites by simply typing “anonymous” for the user, without a password. Usually, the site administrator has files that can be copied but does not allow files to be posted with the anonymous user. Furthermore, FTP is not a secure protocol because the data is not encrypted during transmission.

In this lab, you will learn how to use anonymous FTP from the Windows command-line C:\> prompt. You will access an anonymous FTP server using your browser. Finally, you will use the GUI-based FTP program, WS_FTP LE.

Required Resources

1 PC (Windows 7 or 8 with access to the command prompt, Internet access, and WS_FTP LE installed (optional))

Part 1: Use FTP from a Command Prompt

Instructor Note: This lab uses the anonymous FTP site for the Center for Disease Control and Prevention. This site was chosen because it has been kept current. If the instructor prefers a different anonymous FTP site, a list is available at: <http://www.ftp-sites.org/>, or search for “anonymous FTP sites”.

Instructor Note: Because many schools do not have access to the C:\> prompt, or have security policies that will block FTP, instructors may assign this lab as homework or may demonstrate the lab on the instructor's computer, if the C:\> prompt and FTP are allowed.

- Click the **Windows Start** button, type **cmd** in the search field, and press **Enter** to open a command window.
- At the C:\> prompt type **ftp ftp.cdc.gov**. At the prompt that says **User (ftp.cdc.gov:(none)):** type **anonymous**. For the password, do not type anything. Press **Enter** to be logged in as an anonymous user.

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\User1>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp>
```

Notice that the `C:\>` prompt has been replaced with the `ftp>` prompt. Type **ls** to list the files and directories. At the time that this lab was authored, there was a `Readme` file.

```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
aspnet_client
pub
Readme
```

- c. At the prompt, type **get Readme**. This downloads the file to your local computer from the anonymous FTP server the Center for Disease Control has setup. The file will be copied into the directory shown in the `C:\>` prompt (`C:\Users\User1` in this case).

Instructor Note: The students require a folder where `ftp.exe` has read and write access for the download and viewing of the `Readme` file from the `ftp` site. The folder `C:\Users\User1` is used as an example.

```
ftp> get Readme
200 PORT command successful.
150 Opening ASCII mode data connection for Readme(1428 bytes).
226 Transfer complete.
ftp: 1428 bytes received in 0.00Seconds 1428000.00Kbytes/sec.
ftp>
```

- d. Type **quit** to leave FTP and return to the `C:\>` prompt. Type **more Readme** to see the contents of the document.

```
ftp> quit
221 Goodbye.

C:\Users\User1>more Readme

Welcome to the Centers for Disease Control and Prevention and Agency for
Toxic Substances and Disease Registry FTP server. Information maintained on
this server is in the public domain and is available at anytime for your use.
CDC/ATSDR requests that you provide a valid e-mail address when responding to
the FTP server's password prompt.

FTP POLICY

CDC/ATSDR's file structure is designed to make information easily accessible
for faster response. All FTP directories and sub-directories should contain
the following files:

      README.TXT          Contains general information and Disclaimer text.
                          (ASCII)
```

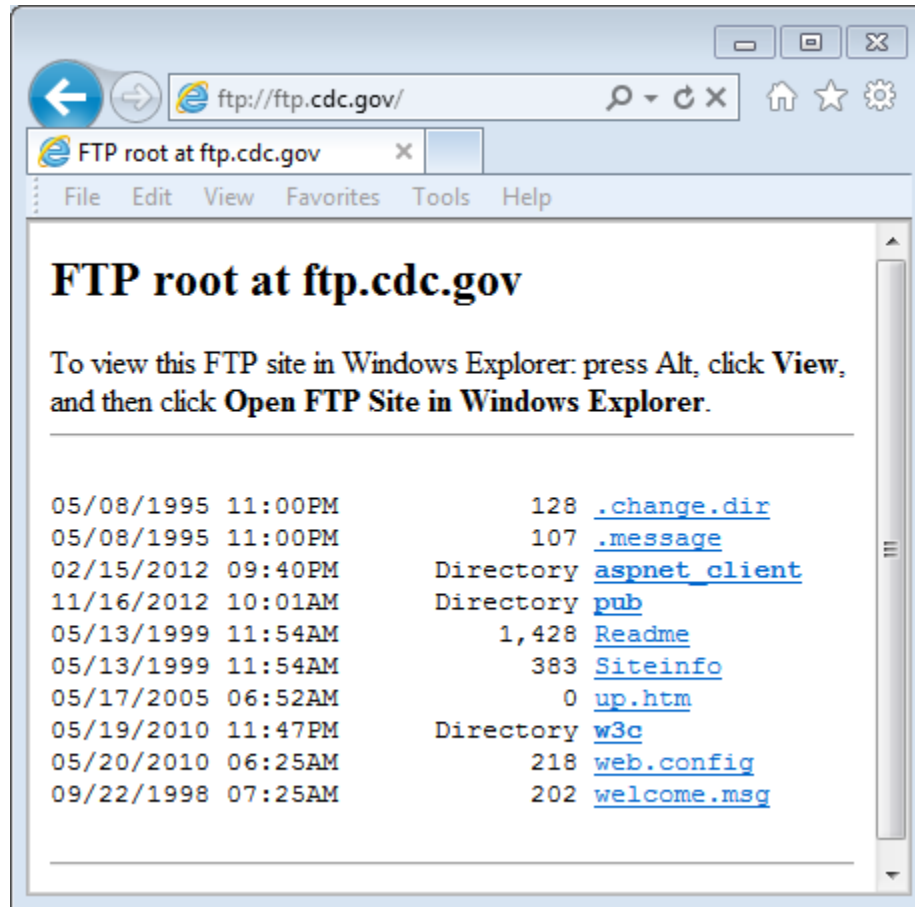
- e. What is a drawback of using the FTP from the command line?

It could get tedious to download files this way all the time.

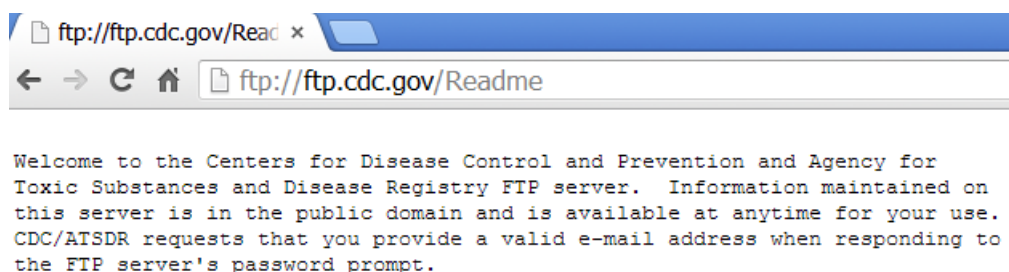
Part 2: Use FTP in a Browser

It is possible to use a browser as an anonymous FTP client.

- a. In a browser, type <ftp://ftp.cdc.gov/>.



- b. Click the **Readme** file.



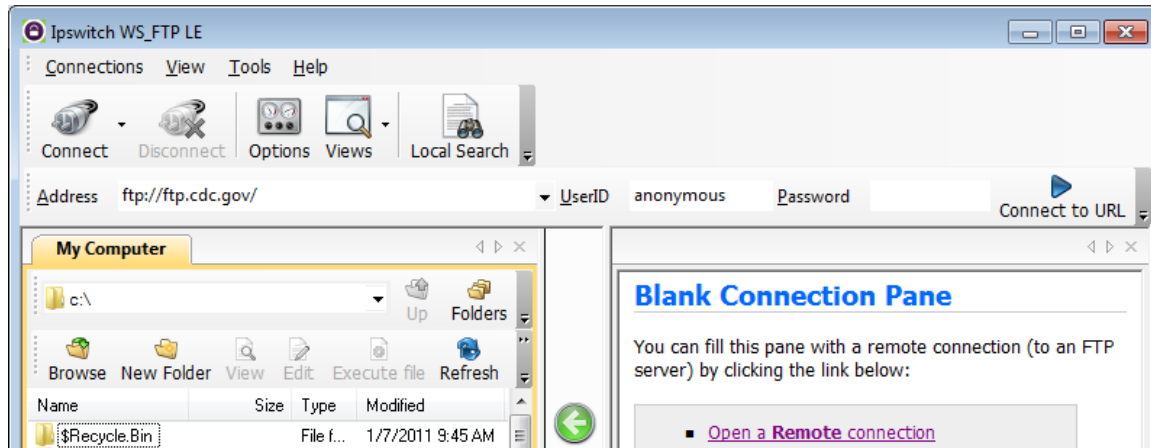
- c. Close browser to disconnect the FTP connection.

Part 3: Download an FTP File Using WS_FTP LE (Optional)

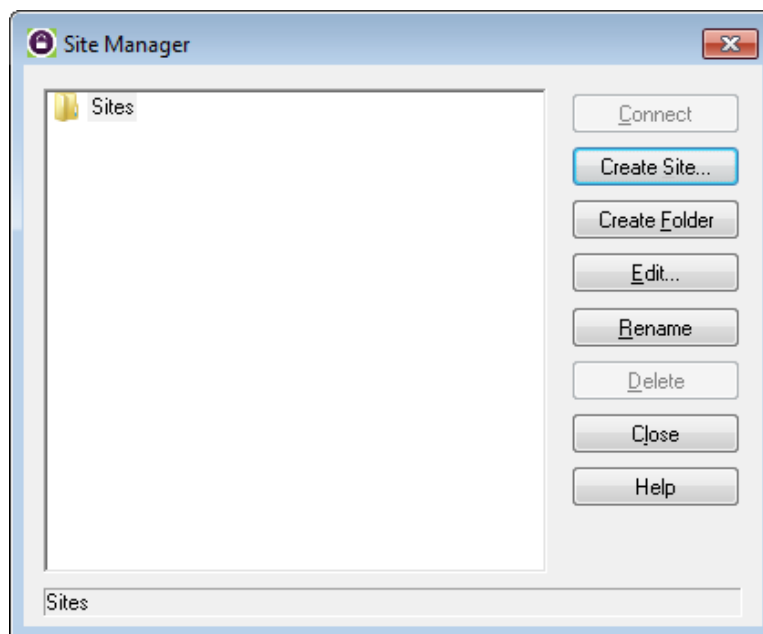
In Part 3, you will download a file using WS_FTP LE (a free FTP transfer tool).

Instructor Note: Instructors will need to install WS_FTP LE on each student computer. At the time of authoring this was available at: <http://www.wsftple.com/download.aspx>. If this URL has changed, use your favorite search engine to look for “download WS_FTP LE” or “download free FTP”.

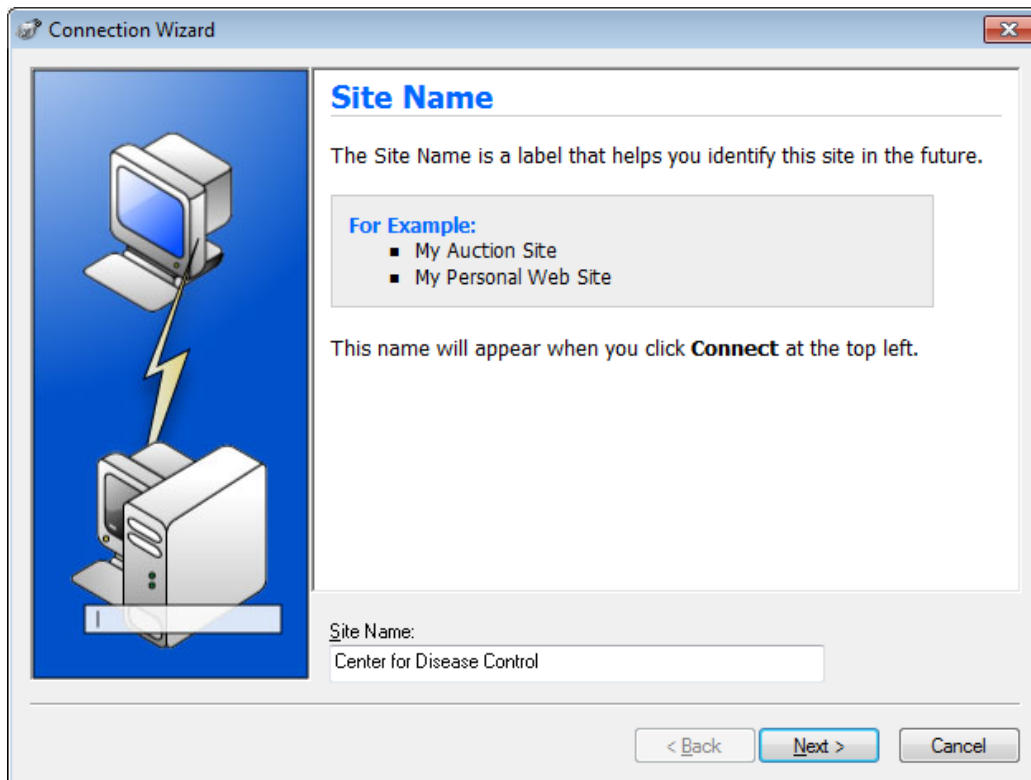
- a. Start **WS_FTP LE**. If the Ipswitch WS_FTP LE window displays, click **Next** to continue and skip to step c. Otherwise, click the **Open a Remote Connection** link.



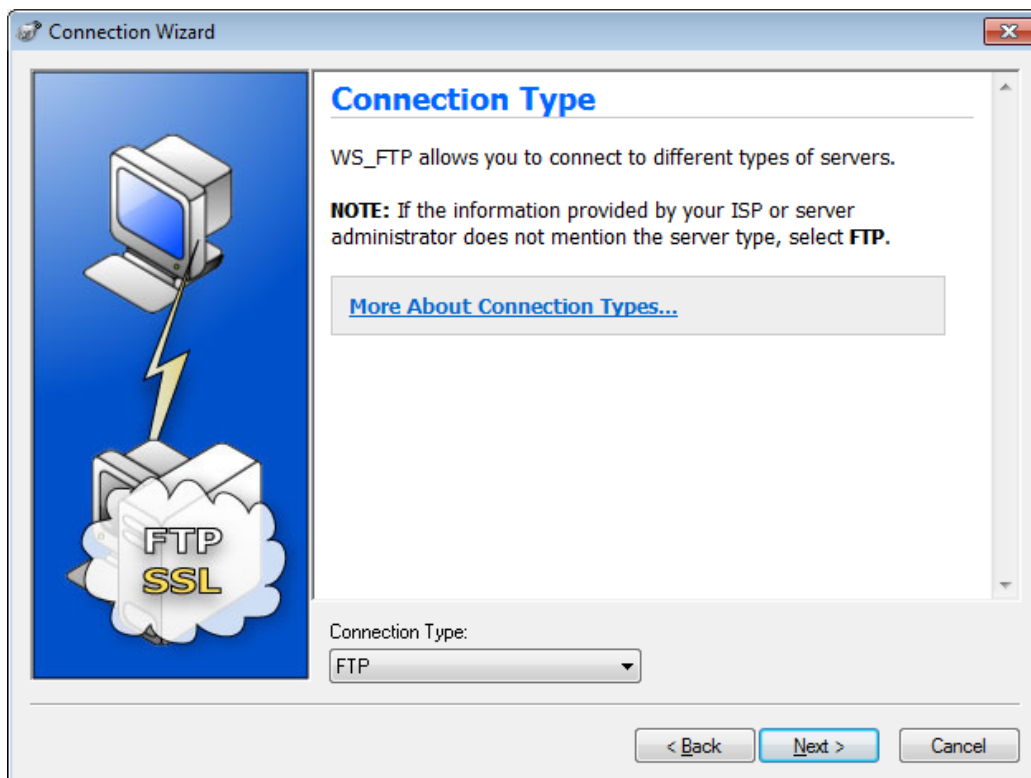
- b. Click **Create Site....**



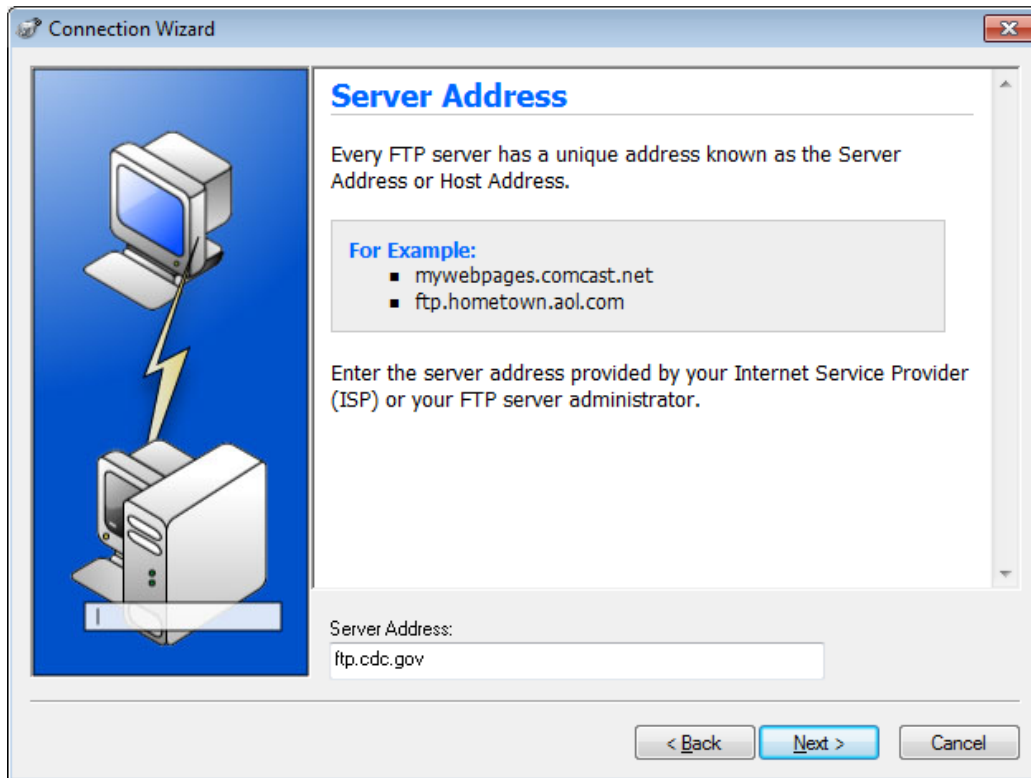
- c. In the **Site Name** field, type **Center for Disease Control** and click **Next** to continue.



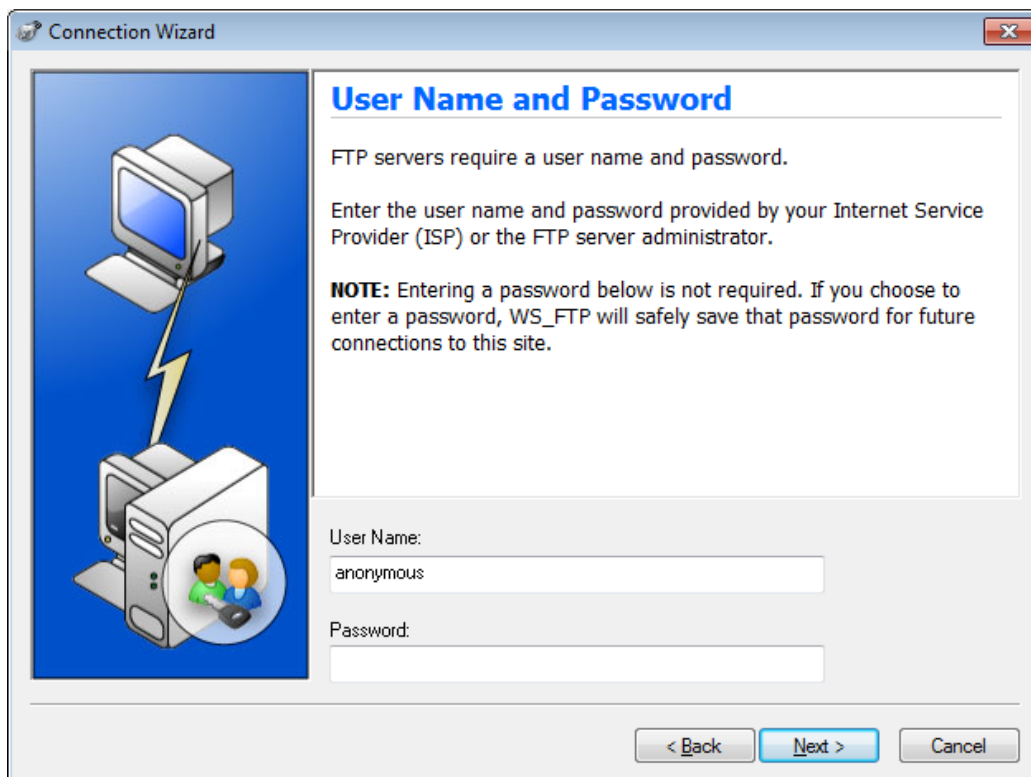
- d. Click the **Connection Type** drop-down list, select **FTP** (the default connection type), and click **Next**.



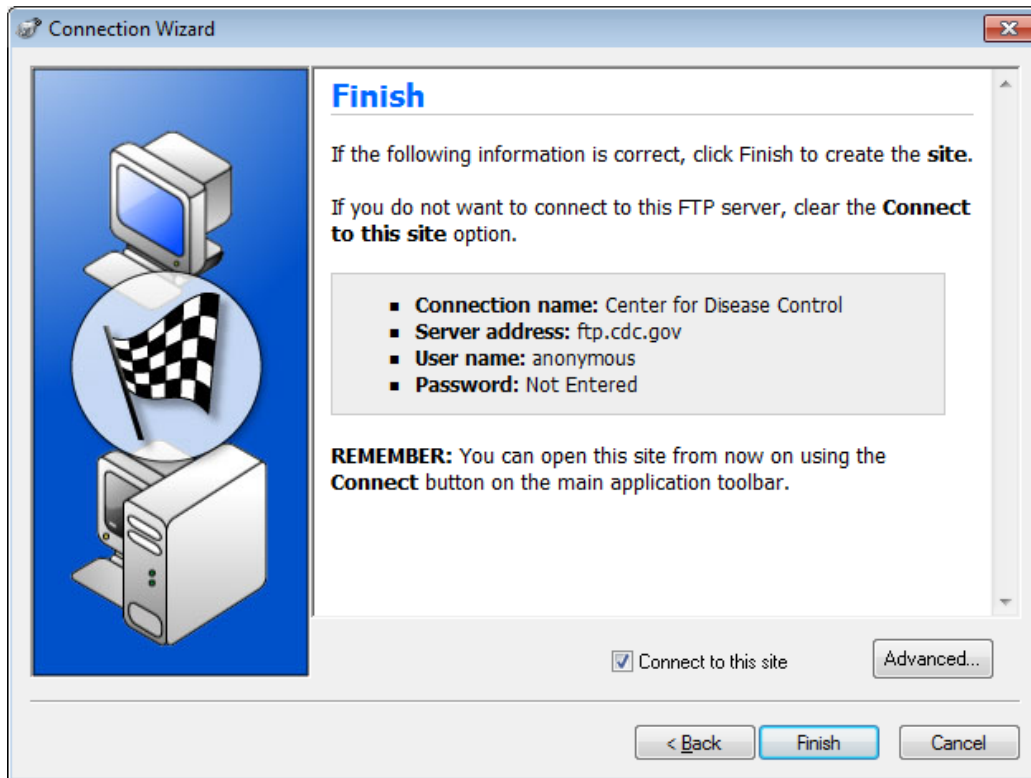
- e. In the **Server Address** field, type <ftp.cdc.gov>, and click **Next**.



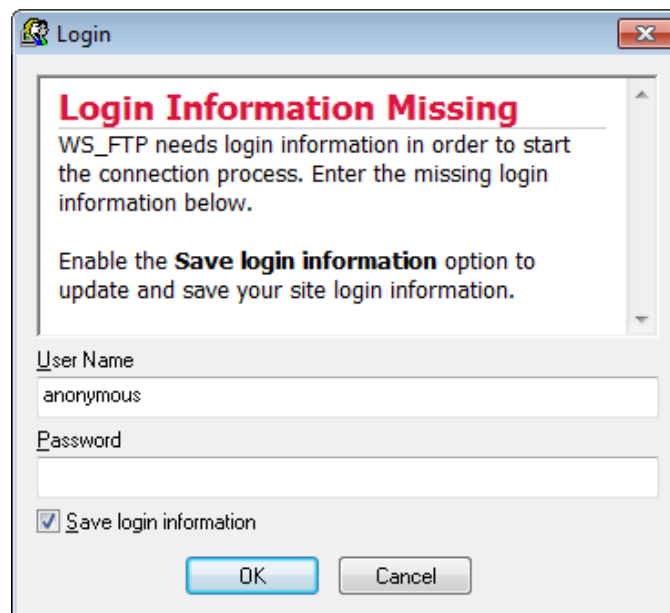
- f. In the **User Name** field, type **anonymous**, and leave the password field blank. Click **Next**.



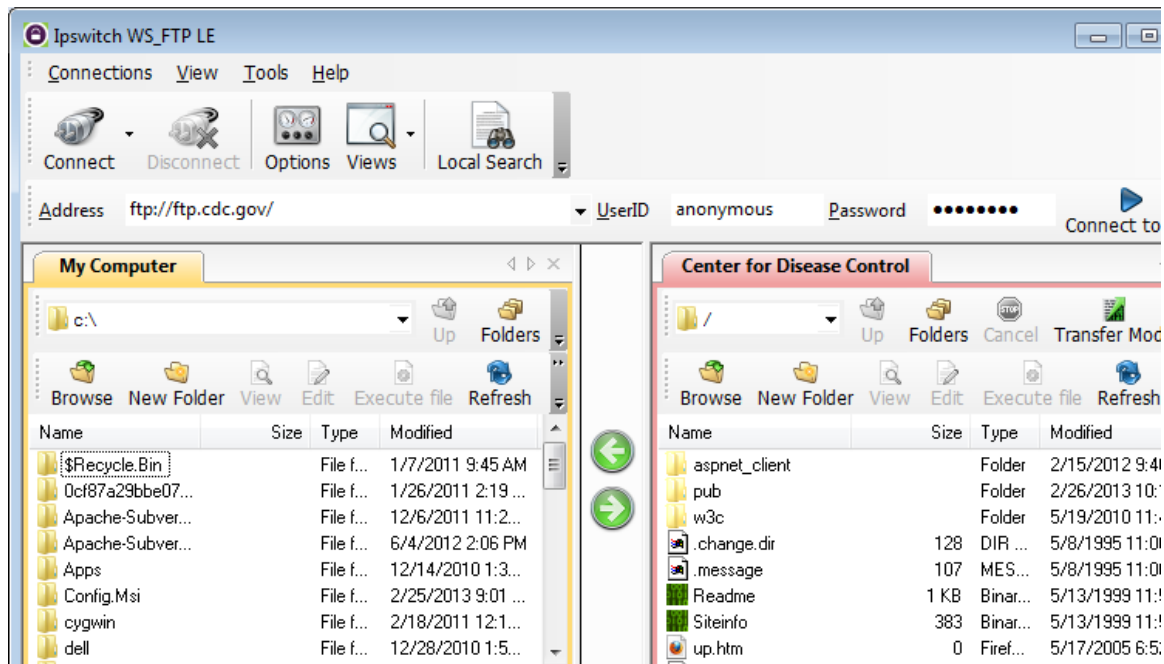
- g. Click **Finish**.



- h. When the Login Information Missing dialog box displays, click **OK**. Do not type a password in the **Password** field.

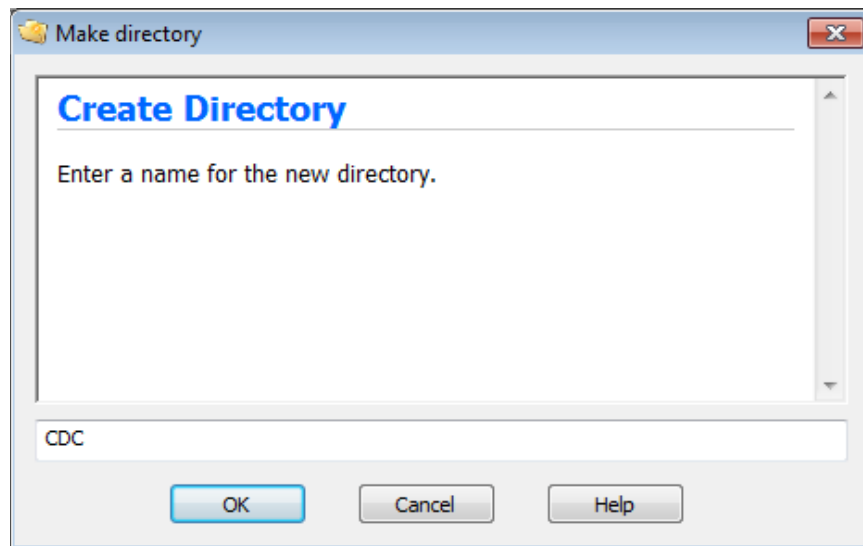


- i. You are now anonymously connected to the Center for Disease Control FTP site.

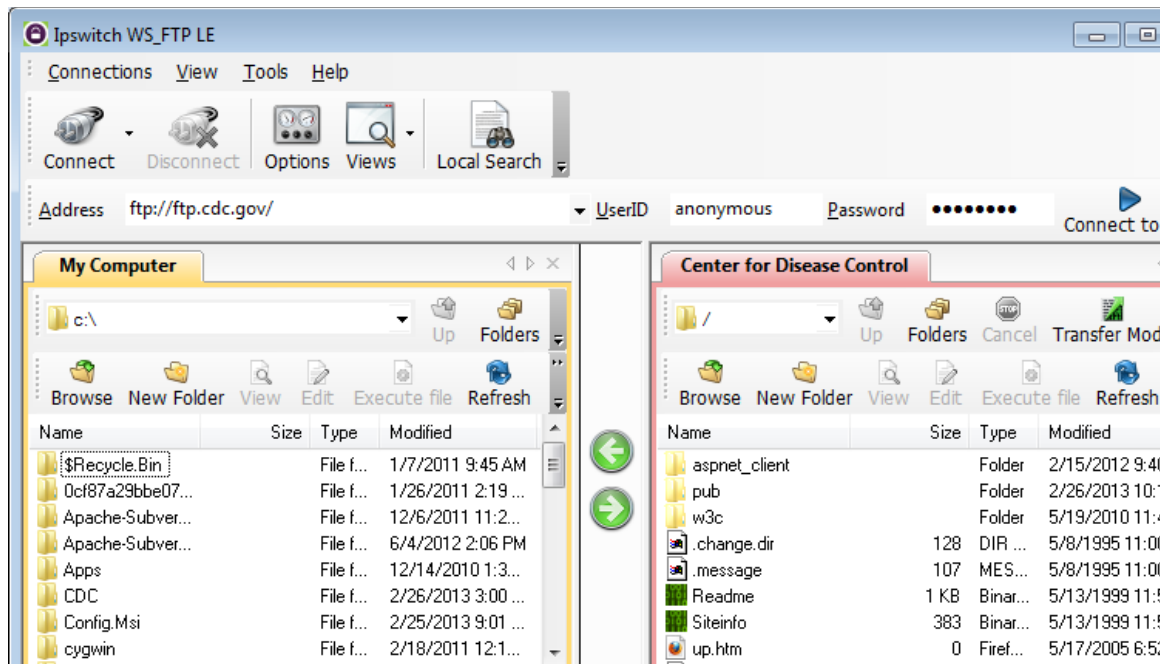


- j. On the WS_FTP LE toolbar menu under My Computer, click **New Folder** to create a folder on your local C:\ drive.
- k. In the Make Directory dialog box name the folder as **CDC** and click **OK**.

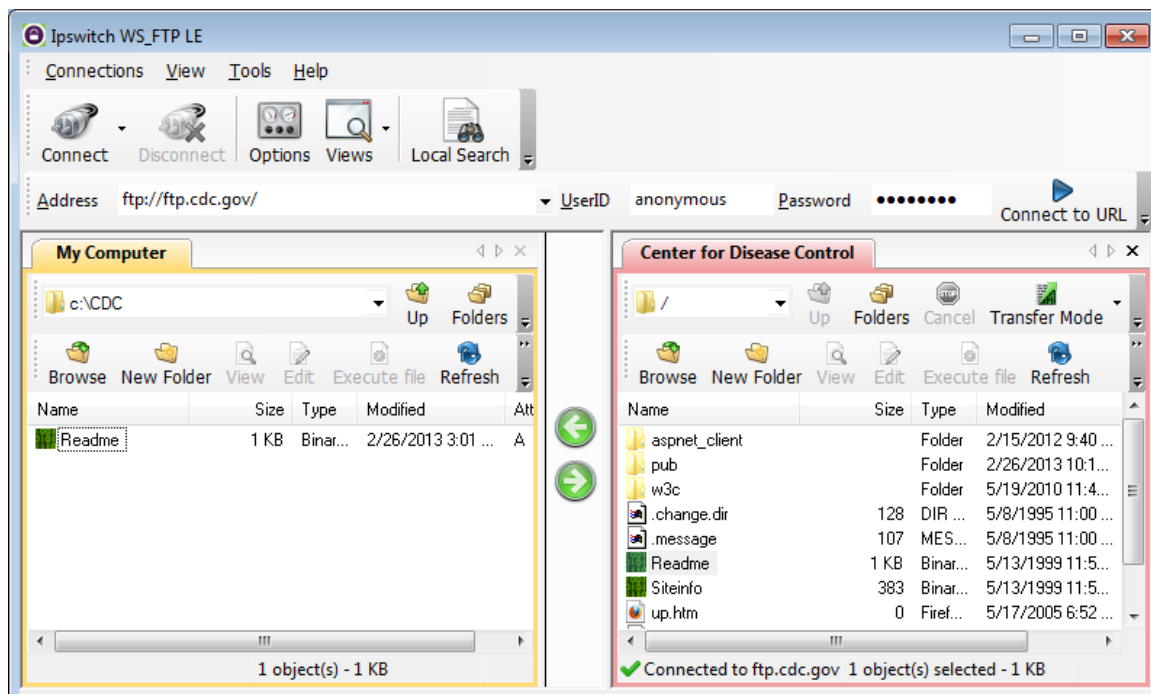
Note: If the folder already exists, you can use the same folder or create another folder with a different name. If using the same CDC folder, you can replace the existing Readme file with the downloaded Readme file.



- l. After the directory is created, in the **My Computer** tab page, double-click the directory to open it.



- m. Drag the **Readme** file from the right side of the application (the remote CDC FTP server) into the CDC folder on to the local **C:** drive.



- n. Double-click the **Readme** file in the **C:\CDC** folder on your local **C:** drive. If prompted for an application to open the document, choose any word processing software. You should see a message that looks something like this:

Welcome to the Centers for Disease Control and Prevention and Agency for Toxic Substances and Disease Registry FTP server. Information maintained on this server is in the public domain and is available at anytime for your use.

- o. Which was easier, using FTP from the **cmd** prompt, or using WS_FTP LE? _____
After it has been installed, a GUI FTP application such as WS_FTP LE is easier to use, especially if working with a large number of big files.
- p. Verify that the Center for Disease Control window is highlighted. Click **Disconnect** to disconnect from the <ftp.cdc.gov> site when finished.
- q. The remote site will be removed from the saved list of FTP sites. In the Ipswitch WS_FTP LE window, click the **Open a Remote Connection** link. Select the **Center for Disease Control** site, and click **Delete** to remove the FTP site. Click **Yes** to confirm the deletion. Click **Close** to exit the Site Manager.
- r. Remove the **C:\CDC** folder.
Instructor Note: Please remove C:\CDC or other folders that the students created in this lab.
- s. Close Ipswitch WS_FTP_LE.

Reflection

List the advantages for using FTP from the command prompt, the browser, and an FTP client, such as WS_FTP LE?

Command line provides quick access, but is more difficult when accessing some features. A browser allows for the quick view of text files. Client software provides the most functionality with expert features, such as batch downloads.

Class Activity - Make It Happen! (Instructor Version - Optional Class Activity)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain the operation of the application layer in providing support to end-user applications.

Background /Scenario

Refer to the modeling activity from the beginning of this chapter as the basis for this activity.

Your IP telephones were installed in a half day vs. the full week originally anticipated. Your network has been restored to full capacity and network applications are available for your use. You have the same emails to answer and quotes to write for your manager's approval.

Use the same scenario you completed in the introduction modeling activity to answer the following questions:

Emails

- What method(s) can you use to send email correspondence now that the network is working?
- What format will your emails be sent over the network?
- How can you now send the same message to multiple recipients?
- How can you send the large attachments to multiple recipients using network applications?
- Would using network applications prove to be a cost-effective communication method for your corporation?

Quote for Manager's Approval

- Because you have desktop application programs installed on your computer, will it be relatively easy to produce the quote your manager needs for the new contract due by the end of the week? Explain your answer.
- When you finish writing the quote, how will you present it to your manager for approval? How will he or she send the quote to the client for their approval?
- Is using network applications a cost-effective way to complete business transactions? Justify your answer.
- Save a hard copy or an electronic copy of your answers. Be prepared to discuss your answers in class.

Instructor Note: This optional Modeling Activity's purpose is to review the content learned in Chapter 4. The focus is on how the application layer uses network applications to operate effectively.

To save classroom time (for discussion), students may be assigned to complete only one scenario (Emails or Quote for Manager's Approval).

Stress that students must carefully read through the first paragraph of this modeling activity to know the parameters of the assignment.

Reflection

Having network applications and services available to you may increase production, decrease costs, and save time. Would this be true with the scenario you chose? Justify your answer.

Representative (discussion) answers may look like the following suggestions:

Emails:

- What method(s) can you use to send email correspondence now that the network is working? Most likely, POP or IMAP email delivery in conjunction with a network email software program will be used.
- What format will your emails be sent over the network? POP or IMAP
- How can you now send the same message to multiple recipients? The SAME copy of the email can be sent to multiple recipients in a matter of seconds.
- How can you send the large attachments to multiple recipients using the network applications? Write the email, address it to the recipients and send the large attachments with the email (no printing required!).
- Would using network applications prove to be cost-effective communications methods for your corporation? This method would save time, resources, and provide a quality-driven product (everyone gets the same information)

Quote for Manager's Approval:

- You have a word processing, spreadsheet and database program installed locally on your computer. Will it be relatively easy to produce the quote your manager needs for the new contract due by the end of the week? The local workstation software will assist in creating the quote for the manager at no different cost in this scenario.
- When you finish writing the quote, how will you present it to your manager for approval? Usually, it will be sent as an email with attachment(s) to the manager.
- How will he/she send the quote to the client for their consideration for approval? Most likely, it will be emailed to the client (sometimes, though, an additional hard/paper copy or media copy is sent of the quote to the client for their approval or sign-off)
- Is using network applications a cost-effective way to complete business transactions? Using network applications is more time-efficient and does definitely save resources.

Identify elements of the model that map to IT-related content:

- Costs involved in daily business production decrease when using network applications
- Time-efficiency is increased if working with network applications
- Quality communication is enhanced by using network applications

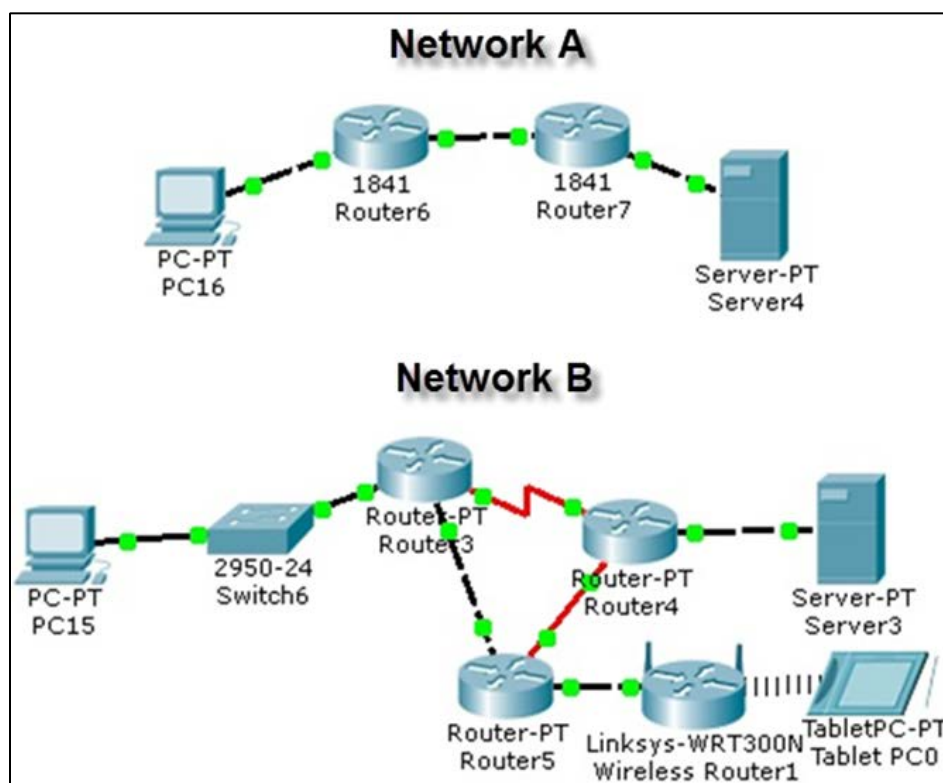
Class Activity - Did You Notice...? (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Objectives

Explain how a small network of directly connected segments is created, configured and verified.

Topology



Background /Scenario

Take a look at the two networks in the topology diagram. Answer the following questions and record your answers in the Reflection section to share with the class.

- Visually compare and contrast Network A and Network B. How are the two networks the same?
- Make note of the devices used in each network design. Because the devices are labeled, you already know what types of end and intermediary devices they are. How are the two networks different? Is the number of devices present in one network the only differentiating factor? Justify your answer.
- Which network would you select if you owned a small to medium-sized business? Justify your selected network based on cost, speed, ports, expandability, and manageability.

Instructor Note: This Modeling Activity is not intended to be a graded assignment. Rather students should note similarities and differences regarding the network equipment shown and the types of networks created. Addressing of the two networks should also be a factor in their comparisons of both networks. Facilitation of the discussion should include student-to-student discussions of each other's work.

Required Resources

- Recording capabilities (paper, tablet, etc.) for reflective comments to be shared with the class.

Reflection

Reflect upon your comparisons of the two network scenarios. What are some things you noted as points of interest?

Multiple students may select Network B as their choice of the best network for a small to medium-sized business. But this may not necessarily be the best choice.

Network A is less costly in equipment. It also provides a more streamlined design, which should assist with network speed issues. Since there is no switch present in this particular network, expandability would be an issue and limited to the ports already present on the ISRs. Manageability would be easy, as there are fewer devices to keep documented and up to date.

Network B is more costly than Network A in equipment alone. It provides for redundancy which is important to the cost of performing business functions. It allows for wireless transmission, not just Ethernet as in Network A. Incorporating wireless technology increases the possibility of security breaches and can increase manageability considerations. Speed could be enhanced if the devices used load balancing and static routes to assist with load balancing.

Therefore, all categories considered, either network would be acceptable to use for a small to medium-sized business. Network A and B offer different positives and negatives, and it would be up to the small to medium-sized business to prioritize cost, speed, ports, expandability and manageability. They would eventually go on from their prioritization list with a look to the future and select the best design for the business. This is similar to separating all sessions into multiple conference rooms according to their topics.

Identify elements of the model that map to real-world content:

- Cost, speed, ports, expandability and manageability are all factors to consider when designing a small to medium-sized network.

Lab – Researching Network Security Threats (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Part 1: Explore the SANS Website

Part 2: Identify Recent Network Security Threats

Part 3: Detail a Specific Network Security Threat

Background / Scenario

To defend a network against attacks, an administrator must identify external threats that pose a danger to the network. Security websites can be used to identify emerging threats and provide mitigation options for defending a network.

One of the most popular and trusted sites for defending against computer and network security threats is SysAdmin, Audit, Network, Security (SANS). The SANS site provides multiple resources, including a list of the top 20 Critical Security Controls for Effective Cyber Defense and the weekly @Risk: The Consensus Security Alert newsletter. This newsletter details new network attacks and vulnerabilities.

In this lab, you will navigate to and explore the SANS site, use the SANS site to identify recent network security threats, research other websites that identify threats, and research and present the details about a specific network attack.

Required Resources

- Device with Internet access
- Presentation computer with PowerPoint or other presentation software installed

Part 1: Exploring the SANS Website

In Part 1, navigate to the SANS website and explore the available resources.

Step 1: Locate SANS resources.

Navigate to www.SANS.org. From the home page, highlight the **Resources** menu.

List three available resources.

Reading Room, Webcasts, Newsletters, Blogs, Top 25 Programming Errors, Top 20 Critical Controls, Security Policy Project

Step 2: Locate the Critical Security Controls.

The **Critical Security Controls** listed on the SANS website are the culmination of a public-private partnership involving the Department of Defense (DoD), National Security Association, Center for Internet Security (CIS), and the SANS Institute. The list was developed to prioritize the cyber security controls and spending for DoD. It has become the centerpiece for effective security programs for the United States government. From the **Resources** menu, select **Critical Security Controls**, or similar.

Select one of the Controls and list three of the implementation suggestions for this control.

Answers will vary. Critical Control 5: Malware Defenses. Employ automated tools to continuously monitor workstations, servers, and mobile devices. Employ anti-malware software and signature auto-update features. Configure network computers to not auto-run content from removable media.

Step 3: Locate the Newsletters menu.

Highlight the **Resources** menu, select **Newsletters**. Briefly describe each of the three newsletters available.

SANS NewsBites - A high level summary of the most important news articles that deal with computer security. The newsletter is published twice a week and includes links for more information.

@RISK: The Consensus Security Alert - A weekly summary of new network attacks and vulnerabilities. The newsletters is also provides insights on how recent attacks worked.

Ouch! – A security awareness document that provides end users with information about how they can help ensure the safety of their network.

Part 2: Identify Recent Network Security Threats

In Part 2, you will research recent network security threats using the SANS site and identify other sites containing security threat information.

Step 1: Locate the @Risk: Consensus Security Alert Newsletter Archive.

From the **Newsletters** page, select **Archive** for the @RISK: The Consensus Security Alert. Scroll down to **Archives Volumes** and select a recent weekly newsletter. Review the **Notable Recent Security Issues and Most Popular Malware Files** sections.

List some recent attacks. Browse multiple recent newsletters, if necessary.

Answers will vary. Win.Trojan.Quarian, Win.Trojan.Changeup, Andr.Trojan.SMSSend-1, Java.Exploit.Agent-14, Trojan.ADH.

Step 2: Identify sites providing recent security threat information.

Besides the SANS site, identify some other websites that provide recent security threat information.

Answers will vary but could include www.mcafee.com/us/mcafee-labs.aspx, www.symantec.com/news.cnet.com/security/, www.sophos.com/en-us/threat-center/, us.norton.com/security_response/.

List some of the recent security threats detailed on these websites.

Answers will vary. Trojan.Ransomlock, Inostealer.Vskim, Trojan.Fareit, Backdoor.Sorosk, Android.Boxer, W32.Changeup!gen35

Part 3: Detail a Specific Network Security Attack

In Part 3, you will research a specific network attack that has occurred and create a presentation based on your findings. Complete the form below based on your findings.

Step 1: Complete the following form for the selected network attack.

Name of attack:	Code Red
Type of attack:	Worm
Dates of attacks:	July 2001
Computers / Organizations affected:	Infected an estimated 359,000 computers in one day.
How it works and what it did:	
<p>Instructor Note: Most of the following is from Wikipedia.</p> <p>Code Red exploited buffer-overflow vulnerabilities in unpatched Microsoft Internet Information Servers. It launched Trojan code in a denial-of-service attack against fixed IP addresses. The worm spread itself using a common type of vulnerability known as a buffer overflow. It used a long string repeating the character 'N' to overflow a buffer, which then allowed the worm to execute arbitrary code and infect the machine.</p> <p>The payload of the worm included the following:</p> <ul style="list-style-type: none">• Defacing the affected website with the message: HELLO! Welcome to http://www.worm.com! Hacked By Chinese!• It tried to spread itself by looking for more IIS servers on the Internet.• It waited 20–27 days after it was installed to launch DoS attacks on several fixed IP addresses. The IP address of the White House web server was among them.• When scanning for vulnerable machines, the worm did not check whether the server running on a remote machine was running a vulnerable version of IIS or whether it was running IIS at	

all.
Mitigation options:
To prevent the exploitation of the IIS vulnerability, organizations needed to apply the IIS patch from Microsoft.
References and info links:
CERT Advisory CA-2001-19 eEye Code Red advisory Code Red II analysis

Step 2: Follow the instructor's guidelines to complete the presentation.

Reflection

1. What steps can you take to protect your own computer?

Answers will vary but could include keeping the operating system and applications up to date with patches and service packs, using a personal firewall, configuring passwords to access the system and bios, configuring screensavers to timeout and requiring a password, protecting important files by making them read-only, encrypting confidential files and backup files for safe keeping.

2. What are some important steps that organizations can take to protect their resources?

Answers will vary but could include the use of firewalls, intrusion detection and prevention, hardening of network devices, endpoint protection, network vulnerability tools, user education, and security policy development.

Lab - Accessing Network Devices with SSH (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure the Router for SSH Access

Part 3: Configure the Switch for SSH Access

Part 4: SSH from the CLI on the Switch

Background / Scenario

In the past, Telnet was the most common network protocol used to remotely configure network devices. Telnet does not 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 device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols.

The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will 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.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term, and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- d. Assign **class** as the privileged EXEC encrypted password.
- e. Assign **cisco** as the console password and enable login.
- f. Assign **cisco** as the VTY password and enable login.
- g. Encrypt the plaintext passwords.
- h. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- i. Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- j. Save the running configuration to the startup configuration file.

Step 4: Configure PC-A.

- a. Configure PC-A with an IP address and subnet mask.
- b. Configure a default gateway for PC-A.

Step 5: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Configure the Router for SSH Access

Using Telnet to connect to a network device is a security risk because all information is transmitted in a clear text format. SSH encrypts the session data and provides device authentication, which is why SSH is recommended for remote connections. In Part 2, you will configure the router to accept SSH connections over the VTY lines.

Step 1: Configure device authentication.

The device name and domain are used as part of the crypto key when it is generated. Therefore, these names must be entered prior to issuing the **crypto key** command.

- a. Configure device name.

```
Router(config)# hostname R1
```

- b. Configure the domain for the device.

```
R1(config)# ip domain-name ccna-lab.com
```

Step 2: Configure the encryption key method.

```
R1(config)# crypto key generate rsa modulus 1024
```

```
The name for the keys will be: R1.ccna-lab.com
```

```
% The key modulus size is 1024 bits
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 1 seconds)
```

```
R1(config)#
```

```
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Step 3: Configure a local database username.

```
R1(config)# username admin privilege 15 secret adminpass
```

Note: A privilege level of 15 gives the user administrator rights.

Step 4: Enable SSH on the VTY lines.

- a. Enable Telnet and SSH on the inbound VTY lines using the **transport input** command.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input telnet ssh
```

- b. Change the login method to use the local database for user verification.

```
R1(config-line)# login local
```

```
R1(config-line)# end
```

```
R1#
```

Step 5: Save the running configuration to the startup configuration file.

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

```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
[OK]
```

```
R1#
```

Step 6: Establish an SSH connection to the router.

- Start Tera Term from PC-A.
- Establish an SSH session to R1. Use the username **admin** and password **adminpass**. You should be able to establish an SSH session with R1.

Part 3: Configure the Switch for SSH Access

In Part 3, you will configure the switch in the topology to accept SSH connections. After the switch has been configured, establish an SSH session using Tera Term.

Step 1: Configure the basic settings on the switch.

- Console into the switch and enable privileged EXEC mode.
- Enter configuration mode.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Encrypt the plain text passwords.
- Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the VLAN 1 interface on the switch according to the Addressing Table.
- Save the running configuration to the startup configuration file.

Step 2: Configure the switch for SSH connectivity.

Use the same commands that you used to configure SSH on the router in Part 2 to configure SSH for the switch.

- Configure the device name as listed in the Addressing Table.
- Configure the domain for the device.
`S1(config)# ip domain-name ccna-lab.com`
- Configure the encryption key method.
`S1(config)# crypto key generate rsa modulus 1024`
- Configure a local database username.
`S1(config)# username admin privilege 15 secret adminpass`
- Enable Telnet and SSH on the VTY lines.
`S1(config)# line vty 0 15`
`S1(config-line)# transport input telnet ssh`
- Change the login method to use the local database for user verification.
`S1(config-line)# login local`
`S1(config-line)# end`

Step 3: Establish an SSH connection to the switch.

Start Tera Term from PC-A, and then SSH to the SVI interface on S1.

Are you able to establish an SSH session with the switch?

Yes. SSH can be configured on a switch using the same commands that were used on the router.

Part 4: SSH From the CLI on the Switch

The SSH client is built into the Cisco IOS and can be run from the CLI. In Part 4, you will SSH to the router from the CLI on the switch.

Step 1: View the parameters available for the Cisco IOS SSH client.

Use the question mark (?) to display the parameter options available with the **ssh** command.

```
S1# 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
  -vrf    Specify vrf name
  WORD    IP address or hostname of a remote system
```

Step 2: SSH to R1 from S1.

- a. You must use the **-l admin** option when you SSH to R1. This allows you to log in as user **admin**. When prompted, enter **adminpass** for the password.

```
S1# ssh -l admin 192.168.1.1
Password:
*****
Warning: Unauthorized Access is Prohibited!
*****
```

```
R1#
```

- b. You can return to S1 without closing the SSH session to R1 by pressing **Ctrl+Shift+6**. Release the **Ctrl+Shift+6** keys and press **x**. The switch privileged EXEC prompt displays.

```
R1#
```

```
S1#
```

- c. To return to the SSH session on R1, press Enter on a blank CLI line. You may need to press Enter a second time to see the router CLI prompt.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]
```

```
R1#
```

- d. To end the SSH session on R1, type **exit** at the router prompt.

```
R1# exit
```

```
[Connection to 192.168.1.1 closed by foreign host]
```

```
S1#
```

What versions of SSH are supported from the CLI?

Answers may vary. This can be determined by using the **ssh -v ?** on the command line. The 2960 switch running IOS version 15.0(2) supports SSH v1 and V2.

```
S1# ssh -v ?
```

```
1 Protocol Version 1
```

```
2 Protocol Version 2
```

Reflection

How would you provide multiple users, each with their own username, access to a network device?

Answers may vary. You would add each user's username and password to the local database using the **username** command. It is also possible to use a RADIUS or TACACS server, but this has not been covered yet.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs - Final

Router R1

```

service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username admin privilege 15 secret 4 QHjxdsVkjtP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
!

```

```
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
!
banner motd ^C
*****
  Unauthorized Access is Prohibited!
*****
^C
!
line con 0
  password 7 00071A150754
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0
  password 7 110A1016141D
  login local
  transport input telnet ssh
```

```
line vty 1 4
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
username admin privilege 15 secret 4 QHjxdsVkjtP7VxKIcPsLdTiMIvyLkyjTlHbmYxZigc
no aaa new-model
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
```

```
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip http server
 ip http secure-server
!
!
banner motd ^C
*****
  Unauthorized Access is Prohibited!
*****
^C
!
```

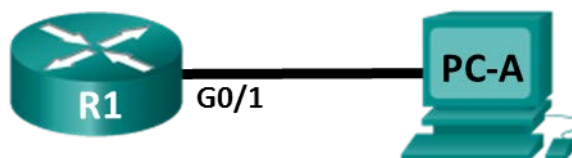
Lab - Accessing Network Devices with SSH

```
line con 0
password 7 060506324F41
login
line vty 0 4
password 7 060506324F41
login local
transport input telnet ssh
line vty 5 15
password 7 00071A150754
login local
transport input telnet ssh
!
end
```

Lab - Examining Telnet and SSH in Wireshark (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding or to provide additional practice or to do both.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure the Devices for SSH Access

Part 2: Examine a Telnet Session with Wireshark

Part 3: Examine a SSH Session with Wireshark

Background / Scenario

In this lab, you will configure a router to accept SSH connectivity, and use Wireshark to capture and view Telnet and SSH sessions. This will demonstrate the importance of encryption with SSH.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 PC (Windows 7, 8, or 10 with terminal emulation program, such as Tera Term, and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Configure the Devices for SSH Access

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the router.

Step 1: Cable the network as shown in the topology.

Step 2: Initialize and reload the router.

Step 3: Configure the basic settings on the router.

- a. Console into the router and enable privileged EXEC mode.
- b. Enter configuration mode.
- c. Configure the device name as listed in the Addressing Table.
- d. Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were host names.
- e. Assign **class** as the privileged EXEC encrypted password.
- f. Assign **cisco** as the console password and enable login.
- g. Assign **cisco** as the VTY password and enable login.
- h. Encrypt the plain text passwords.
- i. Create a banner that will warn anyone accessing the device that unauthorized access is prohibited.
- j. Configure and activate the G0/1 interface using the information contained in the Addressing Table.

Step 4: Configure R1 for SSH access.

- a. Configure the domain for the device.
`R1(config)# ip domain-name ccna-lab.com`
- b. Configure the encryption key method.
`R1(config)# crypto key generate rsa modulus 1024`
- c. Configure a local database username.
`R1(config)# username admin privilege 15 secret adminpass`
- d. Enable Telnet and SSH on the VTY lines.
`R1(config)# line vty 0 4`
`R1(config-line)# transport input telnet ssh`
- e. Change the login method to use the local database for user verification.
`R1(config-line)# login local`
`R1(config-line)# end`

Step 5: Save the running configuration to the startup configuration file.

Step 6: Configure PC-A.

- a. Configure PC-A with an IP address and subnet mask.
- b. Configure a default gateway for PC-A.

Step 7: Verify network connectivity.

Ping R1 from PC-A. If the ping fails, troubleshoot the connection.

Part 2: Examine a Telnet Session with Wireshark

In Part 2, you will use Wireshark to capture and view the transmitted data of a Telnet session on the router. You will use Tera Term to telnet to R1, sign in, and then issue the **show run** command on the router.

Note: If a Telnet/SSH client software package is not installed on your PC, you must install one before continuing. Two popular freeware Telnet/SSH packages are Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) and PuTTY (www.putty.org).

Note: Telnet is not available from the command prompt in Windows 7, by default. To enable Telnet for use in the command prompt window, click **Start > Control Panel > Programs > Programs and Features > Turn Windows features on or off**. Click the **Telnet Client** check box, and then click **OK**.

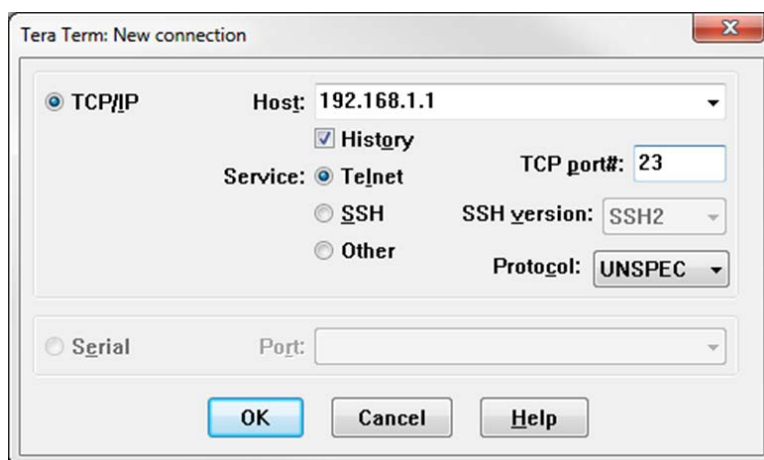
Step 1: Capture data.

- Start Wireshark.
- Start capturing data on the LAN interface.

Note: If you are unable to start the capture on the LAN interface, you may need to open Wireshark using the **Run as Administrator** option.

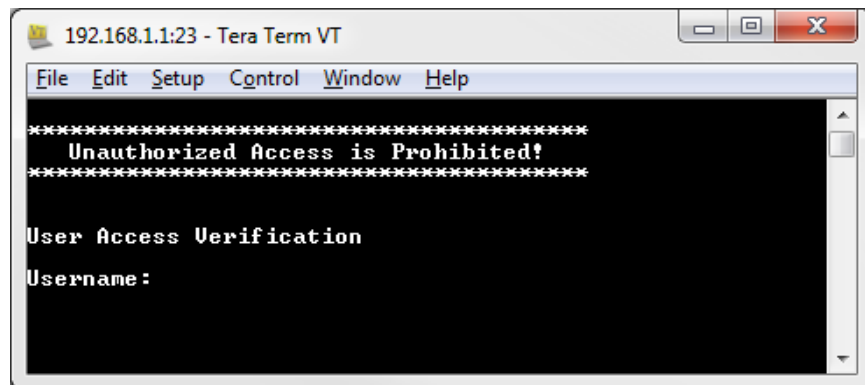
Step 2: Start a Telnet session to the router.

- Open Tera Term and select the **Telnet** Service radio button and in the Host field, enter **192.168.1.1**.



What is the default TCP port for Telnet sessions? _____ Port 23

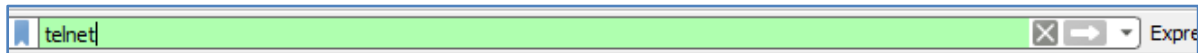
- b. At the **Username:** prompt, enter **admin** and at the **Password:** prompt, enter **adminpass**. These prompts are generated because you configured the VTY lines to use the local database with the **login local** command.



- c. Issue the **show run** command.
R1# **show run**
- d. Enter **exit** to exit the Telnet session and out of Tera Term.
R1# **exit**

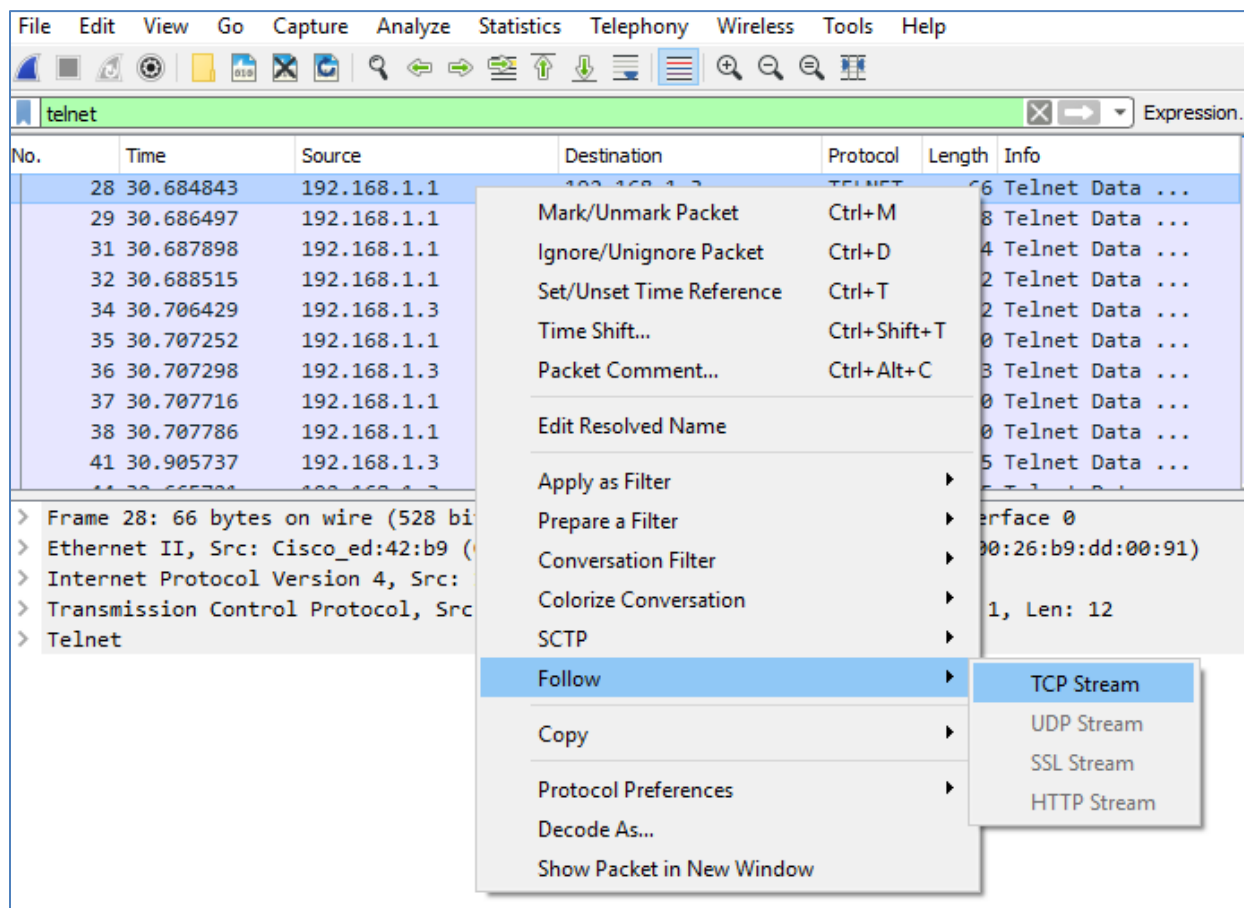
Step 3: Stop the Wireshark capture.

Step 4: Apply a Telnet filter on the Wireshark capture data.



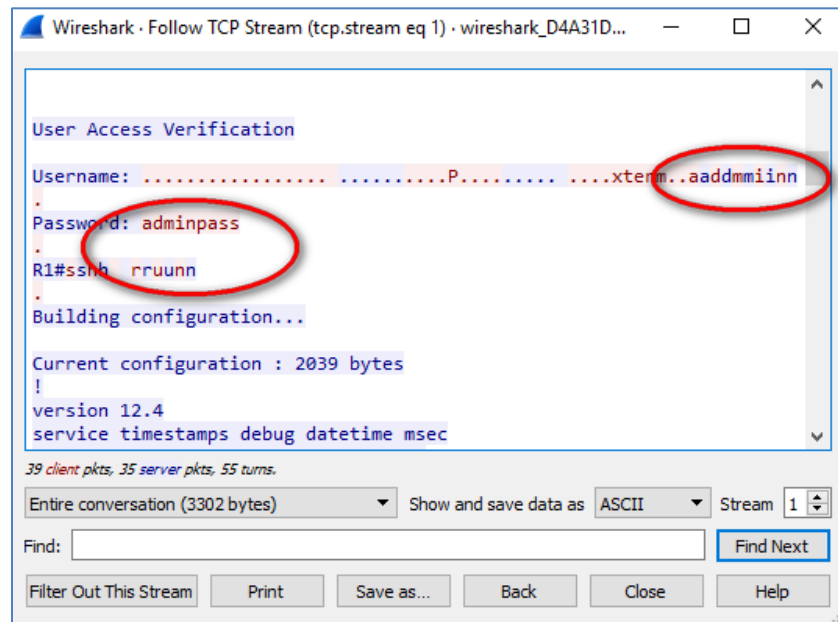
Step 5: Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

- Right-click one of the **Telnet** lines in the **Packet list** section of Wireshark, and from the drop-down list, select **Follow TCP Stream**.



- The **Follow TCP Stream** window displays the data for your Telnet session with the router. The entire session is displayed in clear text, including your password. Notice that the username and **show run**

command that you entered are displayed with duplicate characters. This is caused by the echo setting in Telnet to allow you to view the characters that you type on the screen.



- c. After you have finished reviewing your Telnet session in the **Follow TCP Stream** window, click **Close**.

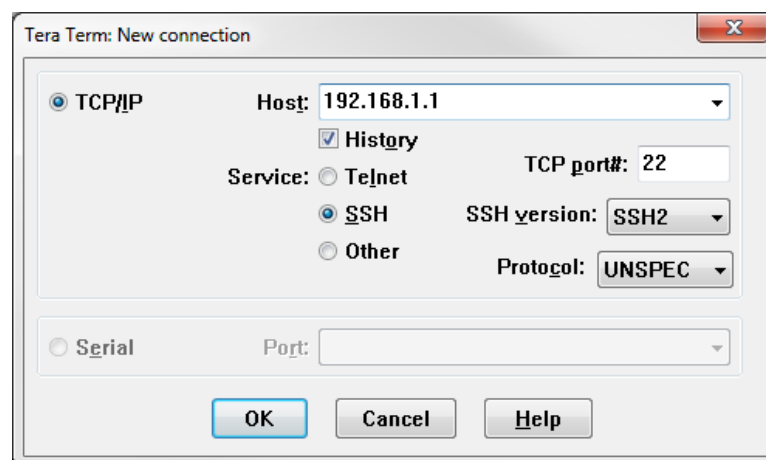
Part 3: Examine an SSH Session with Wireshark

In Part 4, you will use the Tera Term software to establish an SSH session with the router. Wireshark will be used to capture and view the data of this SSH session.

Step 1: Open Wireshark and start capturing data on the LAN interface.

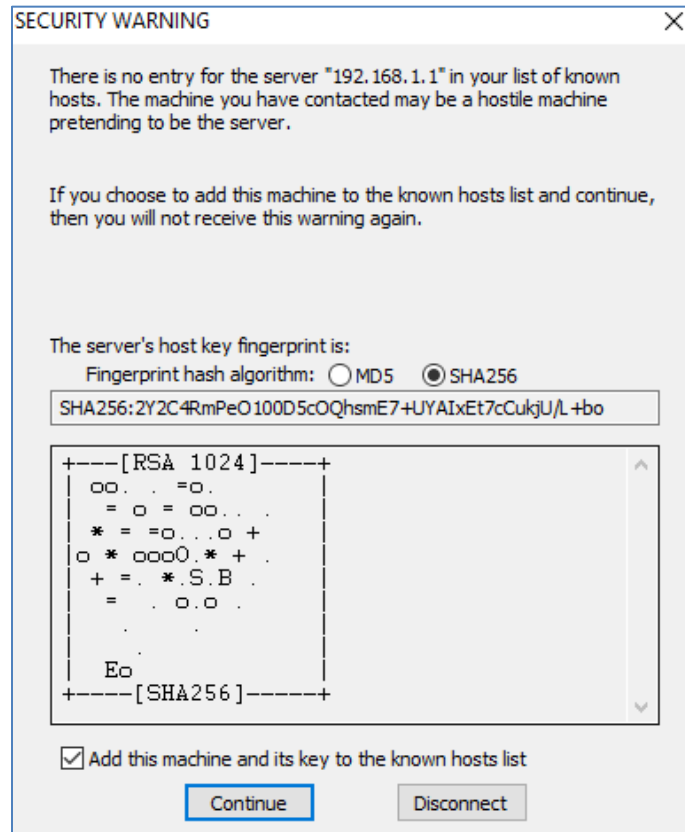
Step 2: Start an SSH session on the router.

- a. Open Tera Term and enter the G0/1 interface IP address of R1 in the **Host:** field of the **Tera Term: New Connection** window. Ensure that the **SSH** radio button is selected and then click **OK** to connect to the router.

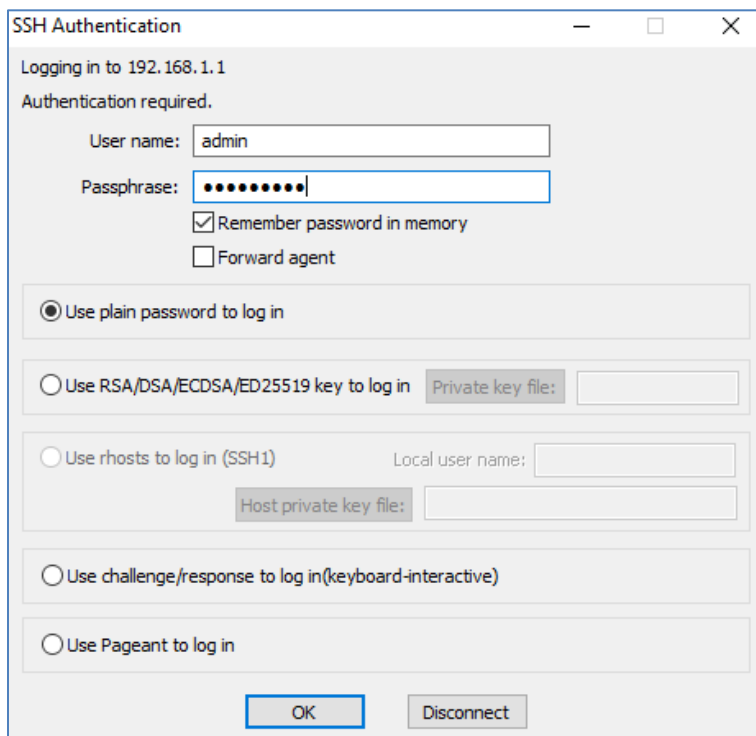


What is the default TCP port used for SSH sessions? _____ Port 22

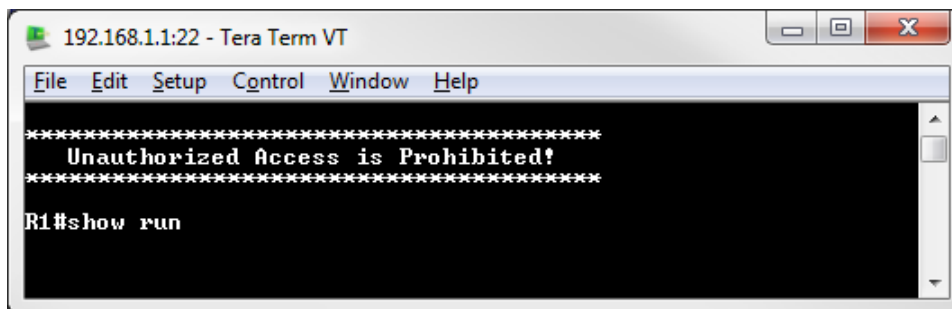
- b. The first time you establish an SSH session to a device, a **SECURITY WARNING** is generated to let you know that you have not connected to this device before. This message is part of the authentication process. Read the security warning and click **Continue**.



- c. In the **SSH Authentication** window, enter **admin** for the username and **adminpass** for the passphrase. Click **OK** to sign into the router.



- d. You have established an SSH session on the router. The Tera Term software looks very similar to a command window. At the command prompt, issue the **show run** command.

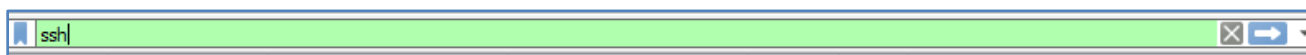


- e. Exit the SSH session by issuing the **exit** command.

R1# **exit**

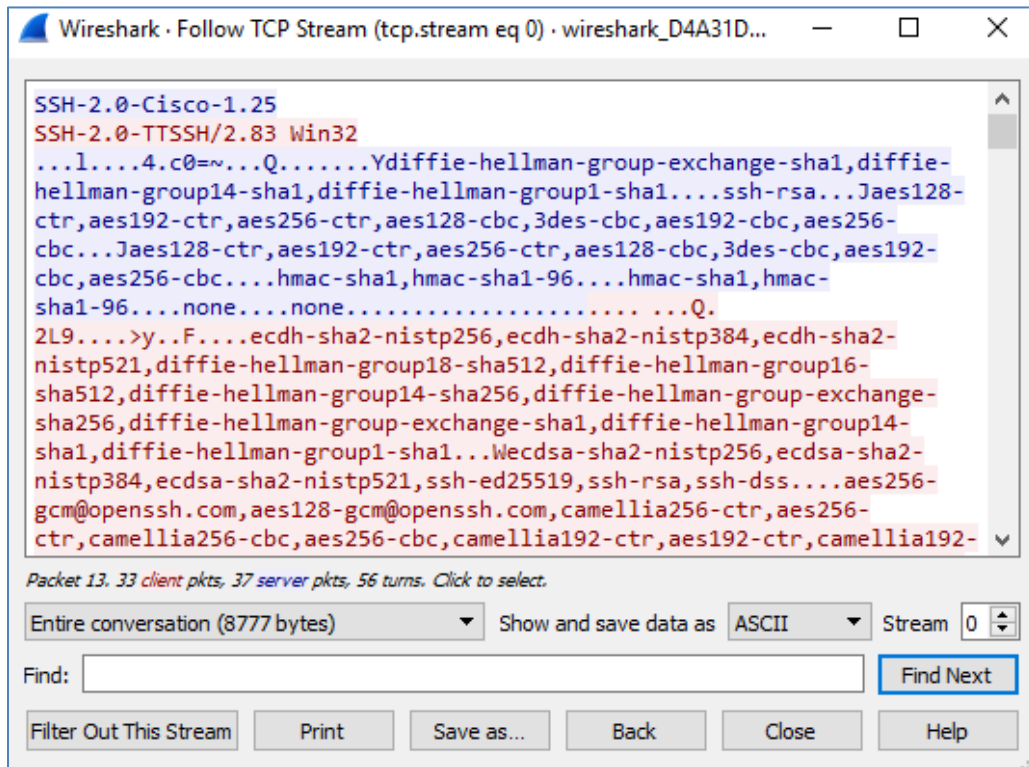
Step 3: Stop the Wireshark capture.

Step 4: Apply an SSH filter on the Wireshark Capture data.



Step 5: Use the Follow TCP Stream feature in Wireshark to view the SSH session.

- Right-click one of the **SSHv2** lines in the Packet list section of Wireshark, and in the drop-down list, select the **Follow TCP Stream** option.
- Examine the **Follow TCP Stream** window of your SSH session. The data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.



Why is SSH preferred over Telnet for remote connections?

Answers may vary.

Similar to Telnet, SSH is used to access and execute commands on a remote system. However, the SSH protocol allows users to communicate with remote systems securely by encrypting the communications. This prevents any sensitive information, such as usernames and passwords, from being captured during the transmission.

By using public-key cryptography to support communication between remote computers, SSH eliminates the need for initial private key exchange between the communicating parties. With SSH, the private key is never sent, as it uses a pair of keys (public and private) for encryption. Messages encrypted with a public key can only be decrypted with the corresponding private key. Because the private key never leaves the endpoints, the system is inherently secure.

When a user establishes an SSH connection for the first time, the SSH client program exchanges the public keys. The user is trusting the security of the network during the key exchange. When the user clicks **Continue** in the SSH client, the user is accepting the remote system into the list of known hosts.

- c. After examining your SSH session, click **Close**.
- d. Close Wireshark.

Reflection

How would you provide multiple users, each with his or her own username, access to a network device?

Answers may vary. You would add each user username and password to the local database via the **username** command. It is also possible to use a RADIUS or TACACS server, but this has not been covered yet.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs - Final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
```

```
!  
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
no aaa new-model  
memory-size iomem 10  
!  
no ip domain lookup  
ip domain name ccna-lab.com  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjTlHbmYxZigc  
!  
interface GigabitEthernet0/0  
  no ip address  
  shutdown  
  duplex auto  
  speed auto  
!  
interface GigabitEthernet0/1  
  description Connection to S1-F0/5.  
  ip address 192.168.1.1 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface Serial0/0/0  
  no ip address  
  shutdown  
  clock rate 2000000  
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
control-plane  
!  
!  
banner motd ^C  
*****  
  Unauthorized Access is Prohibited!  
*****  
^C  
!
```



```
line con 0
password 7 00071A150754
login
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport input all
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0
password 7 110A1016141D
login local
transport input telnet ssh
line vty 1 4
login local
transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Lab – Securing Network Devices (Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Basic Device Settings

Part 2: Configure Basic Security Measures on the Router

Part 3: Configure Basic Security Measures on the Switch

Background / Scenario

It is recommended that all network devices be configured with at least a minimum set of best practice security commands. This includes end user devices, servers, and network devices, such as routers and switches.

In this lab, you will configure the network devices in the topology to accept SSH sessions for remote management. You will also use the IOS CLI to configure common, basic best practice security measures. You will then test the security measures to verify that they are properly implemented and working correctly.

Note: The routers used with CCNA hands-on labs are Cisco 1941 ISRs with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary table at the end of the lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS software, release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports

- Ethernet cables as shown in the topology

Part 1: Configure Basic Device Settings

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, device access, and passwords on the devices.

Step 1: Cable the network as shown in the topology.

Attach the devices shown in the topology and cable as necessary.

Step 2: Initialize and reload the router and switch.

Step 3: Configure the router and switch.

- Console into the device and enable privileged EXEC mode.
- Assign the device name according to the Addressing Table.
- Disable DNS lookup to prevent the router from attempting to translate incorrectly entered commands as though they were hostnames.
- Assign **class** as the privileged EXEC encrypted password.
- Assign **cisco** as the console password and enable login.
- Assign **cisco** as the VTY password and enable login.
- Create a banner that warns anyone accessing the device that unauthorized access is prohibited.
- Configure and activate the G0/1 interface on the router using the information contained in the Addressing Table.
- Configure the default SVI on the switch with the IP address information according to the Addressing Table.
- Save the running configuration to the startup configuration file.

Part 2: Configure Basic Security Measures on the Router

Step 1: Encrypt the clear text passwords.

```
R1(config)# service password-encryption
```

Step 2: Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include combining letters, numbers and special characters in the password and setting a minimum length.

Note: Best practice guidelines require the use of strong passwords, such as those shown here, in a production environment. However, the other labs in this course use the cisco and class passwords for ease in performing the labs.

- Change the privileged EXEC encrypted password to meet guidelines.

```
R1(config)# enable secret Enablep@55
```

- Require that a minimum of 10 characters be used for all passwords.

```
R1(config)# security passwords min-length 10
```

Step 3: Enable SSH connections.

- a. Assign the domain name as **CCNA-lab.com**.

```
R1(config)# ip domain-name CCNA-lab.com
```

- b. Create a local user database entry to use when connecting to the router via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 15) access by default.

```
R1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

- c. Configure the transport input for the VTY lines so that they accept SSH connections, but do not allow Telnet connections.

```
R1(config)# line vty 0 4
```

```
R1(config-line)# transport input ssh
```

- d. The VTY lines should use the local user database for authentication.

```
R1(config-line)# login local
```

```
R1(config-line)# exit
```

- e. Generate a RSA crypto key using a modulus of 1024 bits.

```
R1(config)# crypto key generate rsa modulus 1024
```

Step 4: Secure the console and VTY lines.

- a. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time. The following commands cause the line to log out after five minutes of inactivity.

```
R1(config)# line console 0
```

```
R1(config-line)# exec-timeout 5 0
```

```
R1(config-line)# line vty 0 4
```

```
R1(config-line)# exec-timeout 5 0
```

```
R1(config-line)# exit
```

```
R1(config)#
```

- b. The following command impedes brute force login attempts. The router blocks login attempts for 30 seconds if someone fails two attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
R1(config)# login block-for 30 attempts 2 within 120
```

What does the **2 within 120** mean in the above command?

If two failed attempts are made within a 2 minute (120 seconds) time span, login access will be blocked.

What does the **block-for 30** mean in the above command?

If login access is blocked, the device will wait 30 seconds before allowing login access again.

Step 5: Verify that all unused ports are disabled.

Router ports are disabled by default, but it is always prudent to verify that all unused ports are in an administratively down state. This can be quickly checked by issuing the **show ip interface brief** command.

Any unused ports that are not in an administratively down state should be disabled using the **shutdown** command in interface configuration mode.

```
R1# show ip interface brief
Interface                               IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0            unassigned      YES NVRAM   administratively down  down
GigabitEthernet0/0                     unassigned      YES NVRAM   administratively down  down
GigabitEthernet0/1                     192.168.1.1     YES manual   up                    up
Serial0/0/0                            unassigned      YES NVRAM   administratively down  down
Serial0/0/1                            unassigned      YES NVRAM   administratively down  down
R1#
```

Step 6: Verify that your security measures have been implemented correctly.

- a. Use Tera Term to telnet to R1.

Does R1 accept the Telnet connection? Explain.

No, the connection is refused. Telnet was disabled with the **transport input ssh** command.

- b. Use Tera Term to SSH to R1.

Does R1 accept the SSH connection? Yes

- c. Intentionally mistype the user and password information to see if login access is blocked after two attempts.

What happened after you failed to login the second time?

The connection to R1 was disconnected. If you attempt to reconnect within 30 seconds, the connection will be refused.

- d. From your console session on the router, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 30 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

```
R1# show login
A default login delay of 1 second is applied.
No Quiet-Mode access list has been configured.

Router enabled to watch for login Attacks.
If more than 2 login failures occur in 120 seconds or less,
logins will be disabled for 30 seconds.

Router presently in Quiet-Mode.
Will remain in Quiet-Mode for 14 seconds.
Denying logins from all sources.
R1#
```

- e. After the 30 seconds has expired, SSH to R1 again and login using the **SSHadmin** username and **Admin1p@55** for the password.

After you successfully logged in, what was displayed? _____ The R1 login banner.

- f. Enter privileged EXEC mode and use **Enablep@55** for the password.

If you mistype this password, are you disconnected from your SSH session after two failed attempts within 120 seconds? Explain.

No. The **login block-for 30 attempts 2 within 120** command only monitors session login attempts.

- g. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Part 3: Configure Basic Security Measures on the Switch

Step 1: Encrypt the clear text passwords.

```
S1(config)# service password-encryption
```

Step 2: Strengthen Passwords on the switch.

Change the privileged EXEC encrypted password to meet strong password guidelines.

```
S1(config)# enable secret Enablep@55
```

Note: The security **password min-length** command is not available on the 2960 switch.

Step 3: Enable SSH Connections.

- a. Assign the domain-name as **CCNA-lab.com**

```
S1(config)# ip domain-name CCNA-lab.com
```

- b. Create a local user database entry for use when connecting to the switch via SSH. The password should meet strong password standards, and the user should have user EXEC access. If privilege level is not specified in the command, the user will have user EXEC (level 1) access by default.

```
S1(config)# username SSHadmin privilege 1 secret Admin1p@55
```

- c. Configure the transport input for the VTY lines to allow SSH connections but not allow Telnet connections.

```
S1(config)# line vty 0 15
```

```
S1(config-line)# transport input ssh
```

- d. The VTY lines should use the local user database for authentication.

```
S1(config-line)# login local
```

```
S1(config-line)# exit
```

- e. Generate an RSA crypto key using a modulus of 1024 bits.

```
S1(config)# crypto key generate rsa modulus 1024
```

Step 4: Secure the console and VTY lines.

- a. Configure the switch to log out a line that has been idle for 10 minutes.

```
S1(config)# line console 0
```

```
S1(config-line)# exec-timeout 10 0
```

```
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

- b. To impede brute force login attempts, configure the switch to block login access for 30 seconds if there are 2 failed attempts within 120 seconds. This timer is set especially low for the purpose of this lab.

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

Step 5: Verify all unused ports are disabled.

Switch ports are enabled, by default. Shut down all ports that are not in use on the switch.

- a. You can verify the switch port status using the **show ip interface brief** command.

```
S1# show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	down	down
FastEthernet0/2	unassigned	YES	unset	down	down
FastEthernet0/3	unassigned	YES	unset	down	down
FastEthernet0/4	unassigned	YES	unset	down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	down	down
FastEthernet0/8	unassigned	YES	unset	down	down
FastEthernet0/9	unassigned	YES	unset	down	down
FastEthernet0/10	unassigned	YES	unset	down	down
FastEthernet0/11	unassigned	YES	unset	down	down
FastEthernet0/12	unassigned	YES	unset	down	down
FastEthernet0/13	unassigned	YES	unset	down	down
FastEthernet0/14	unassigned	YES	unset	down	down
FastEthernet0/15	unassigned	YES	unset	down	down
FastEthernet0/16	unassigned	YES	unset	down	down
FastEthernet0/17	unassigned	YES	unset	down	down
FastEthernet0/18	unassigned	YES	unset	down	down
FastEthernet0/19	unassigned	YES	unset	down	down
FastEthernet0/20	unassigned	YES	unset	down	down
FastEthernet0/21	unassigned	YES	unset	down	down
FastEthernet0/22	unassigned	YES	unset	down	down
FastEthernet0/23	unassigned	YES	unset	down	down
FastEthernet0/24	unassigned	YES	unset	down	down
GigabitEthernet0/1	unassigned	YES	unset	down	down
GigabitEthernet0/2	unassigned	YES	unset	down	down

```
S1#
```

- b. Use the **interface range** command to shut down multiple interfaces at a time.

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
```

S1#

- c. Verify that all inactive interfaces have been administratively shut down.

S1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	manual	up	up
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/2	unassigned	YES	unset	administratively down	down
FastEthernet0/3	unassigned	YES	unset	administratively down	down
FastEthernet0/4	unassigned	YES	unset	administratively down	down
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up
FastEthernet0/7	unassigned	YES	unset	administratively down	down
FastEthernet0/8	unassigned	YES	unset	administratively down	down
FastEthernet0/9	unassigned	YES	unset	administratively down	down
FastEthernet0/10	unassigned	YES	unset	administratively down	down
FastEthernet0/11	unassigned	YES	unset	administratively down	down
FastEthernet0/12	unassigned	YES	unset	administratively down	down
FastEthernet0/13	unassigned	YES	unset	administratively down	down
FastEthernet0/14	unassigned	YES	unset	administratively down	down
FastEthernet0/15	unassigned	YES	unset	administratively down	down
FastEthernet0/16	unassigned	YES	unset	administratively down	down
FastEthernet0/17	unassigned	YES	unset	administratively down	down
FastEthernet0/18	unassigned	YES	unset	administratively down	down
FastEthernet0/19	unassigned	YES	unset	administratively down	down
FastEthernet0/20	unassigned	YES	unset	administratively down	down
FastEthernet0/21	unassigned	YES	unset	administratively down	down
FastEthernet0/22	unassigned	YES	unset	administratively down	down
FastEthernet0/23	unassigned	YES	unset	administratively down	down
FastEthernet0/24	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	unassigned	YES	unset	administratively down	down
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down

S1#

Step 6: Verify that your security measures have been implemented correctly.

- Verify that Telnet has been disabled on the switch.
- SSH to the switch and intentionally mistype the user and password information to see if login access is blocked.
- After the 30 seconds has expired, SSH to S1 again and log in using the **SSHadmin** username and **Admin1p@55** for the password.
Did the banner appear after you successfully logged in? _____ **Yes**
- Enter privileged EXEC mode using **Enablep@55** as the password.
- Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

Reflection

1. The **password cisco** command was entered for the console and VTY lines in your basic configuration in Part 1. When is this password used after the best practice security measures have been applied?

This password will not be used any longer. Even though the password command still appears in the line sections of the running-config, this command was disabled as soon as the **login local** command was entered for those lines.

2. Are preconfigured passwords shorter than 10 characters affected by the **security passwords min-length 10** command?

No. The security passwords min-length command only affects passwords that are entered after this command is issued. Any pre-existing passwords remain in effect. If they are changed, they will need to be at least 10 characters long.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/0/0)	Serial 0/1/1 (S0/0/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configs - Final

Router R1

```
service timestamps debug datetime msec
```

Lab – Securing Network Devices

```
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
security passwords min-length 10
enable secret 4 jowh6xYPeJucL2dB/ulkSjK2YGee/Usr./fiqFhbxTQ
no aaa new-model
!
no ip domain lookup
ip domain name CCNA-lab.com
ip cef
login block-for 30 attempts 2 within 120
no ipv6 cef
!
username SSHadmin secret 4 242gliTpEQCwPzaoNHLFrFqBSTmqPiFhU9fJFdhRKbU
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
banner motd ^C

  Unauthorized Access is Prohibited!
```

```
^C
!
line con 0
  exec-timeout 5 0
  password 7 094F471A1A0A57
  login
line aux 0
line 2
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
  stopbits 1
line vty 0 4
  exec-timeout 5 0
  password 7 104D000A0618
  login local
  transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 jowh6xYPEJucL2dB/ulkSjK2YGee/Usr./fiqFhbxTQ
!
username SSHadmin secret 4 242gliTpEQCwPzaoNHLFrFqBSTmqPiFhU9fJFdhRKbU
!
system mtu routing 1500
!
no ip domain-lookup
ip domain-name CCNA-lab.com
login block-for 30 attempts 2 within 120
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
```

```
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
shutdown
!
interface FastEthernet0/8
shutdown
!
interface FastEthernet0/9
shutdown
!
interface FastEthernet0/10
shutdown
!
interface FastEthernet0/11
shutdown
!
interface FastEthernet0/12
shutdown
!
interface FastEthernet0/13
shutdown
!
interface FastEthernet0/14
shutdown
!
interface FastEthernet0/15
shutdown
!
interface FastEthernet0/16
shutdown
!
interface FastEthernet0/17
shutdown
!
```

```
interface FastEthernet0/18
shutdown
!
interface FastEthernet0/19
shutdown
!
interface FastEthernet0/20
shutdown
!
interface FastEthernet0/21
shutdown
!
interface FastEthernet0/22
shutdown
!
interface FastEthernet0/23
shutdown
!
interface FastEthernet0/24
shutdown
!
interface GigabitEthernet0/1
shutdown
!
interface GigabitEthernet0/2
shutdown
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip http server
ip http secure-server
!
banner motd ^C

  Unauthorized Access is Prohibited!

^C
!
line con 0
 password 7 110A1016141D
 login
line vty 0 4
 password 7 110A1016141D
 login local
 transport input ssh
line vty 5 15
 login local
!
```

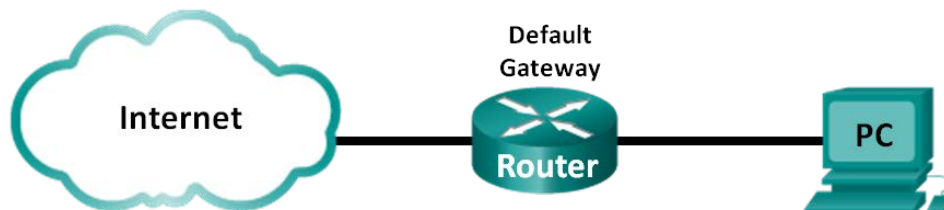
end

Lab - Testing Network Latency with Ping and Traceroute

(Instructor Version)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Use Ping to Document Network Latency

Part 2: Use Traceroute to Document Network Latency

Background / Scenario

To obtain realistic network latency statistics, this activity must be performed on a live network. Be sure to check with your instructor for any local security restrictions against using the **ping** command on the network.

Instructor Note: Some institutions disable ICMP echo replies throughout the network. Before students begin this activity, make sure there are no local restrictions related to ICMP datagrams. This activity assumes that ICMP datagrams are not restricted by any local security policy.

The purpose of this lab is to measure and evaluate network latency over time, and during different periods of the day to capture a representative sample of typical network activity. This will be accomplished by analyzing the return delay from a distant computer with the **ping** command. Return delay times, measured in milliseconds, will be summarized by computing the average latency (mean) and the range (maximum and minimum) of the delay times.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)

Part 1: Use Ping to Document Network Latency

In Part 1, you will examine network latency of several websites in different parts of the globe. This process can be used in an enterprise production network to create a performance baseline.

Step 1: Verify connectivity.

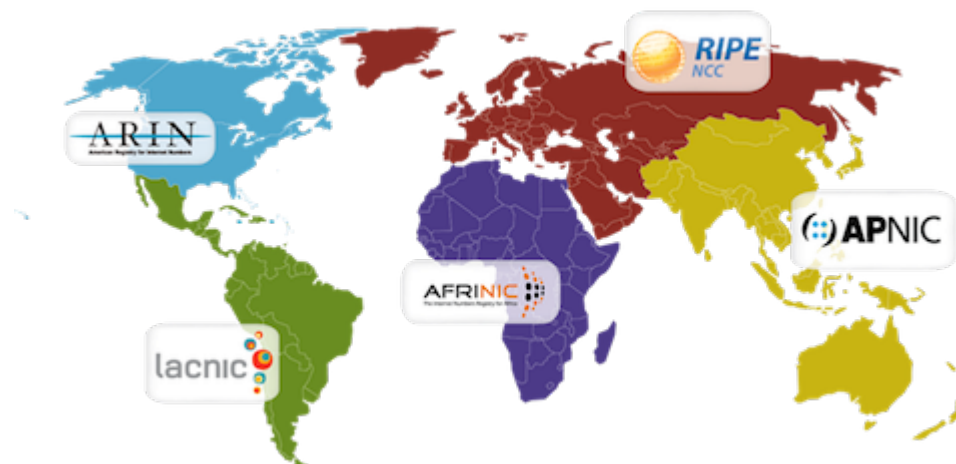
Ping the following Regional Internet Registry (RIR) websites to verify connectivity:

```

C:\Users\User1> ping www.arin.net
C:\Users\User1> ping www.lacnic.net
C:\Users\User1> ping www.afrinic.net
C:\Users\User1> ping www.apnic.net
  
```

Note: Because www.ripe.net does not reply to ICMP requests, it cannot be used for this lab.

Note: If the websites are resolved to IPv6 addresses, the option -4 can be used to resolve to IPv4 addresses if desired. The command becomes **ping -4 www.arin.net**.



Step 2: Collect network data.

You will collect a sufficient amount of data to compute statistics on the **ping** output by sending out 25 echo requests to each address listed in Step 1. Record the results for each website to text files.

- At the command prompt, type **ping** to list the available options.

```
C:\Users\User1> ping
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-4] [-6] target_name
```

Options:

-t	Ping the specified host until stopped. To see statistics and continue - type Control-Break; To stop - type Control-C.
-a	Resolve addresses to hostnames.
-n count	Number of echo requests to send.
-l size	Send buffer size.
-f	Set Don't Fragment flag in packet (IPv4-only).
-i TTL	Time To Live.
-v TOS	Type Of Service (IPv4-only. This setting has been deprecated

<output omitted>

- Using the **ping** command with the count option, you can send 25 echo requests to the destination as illustrated below. Furthermore, it will create a text file with filename of **arin.txt** in the current directory. This text file will contain the results of the echo requests.

```
C:\Users\User1> ping -n 25 www.arin.net > arin.txt
```

Note: The terminal remains blank until the command has finished, because the output has been redirected to a text file, **arin.txt**, in this example. The **>** symbol is used to redirect the screen output to the file and overwrite the file if it already exists. If appending more results to the file is desired, replace **>** with **>>** in the command.

- Repeat the **ping** command for the other websites.


```
C:\Users\User1> ping -n 25 www.afrinic.net > afrinic.txt
C:\Users\User1> ping -n 25 www.apnic.net > apnic.txt
C:\Users\User1> ping -n 25 www.lacnic.net > lacnic.txt
```

Step 3: Verify data collection.

To see the results in the file created, use the **more** command at the command prompt.

```
C:\Users\User1> more arin.txt

Pinging www.arin.net [192.149.252.76] with 32 bytes of data:
Reply from 192.149.252.76: bytes=32 time=108ms TTL=45
Reply from 192.149.252.76: bytes=32 time=114ms TTL=45
Reply from 192.149.252.76: bytes=32 time=112ms TTL=45
<output omitted>
Reply from 192.149.252.75: bytes=32 time=111ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45
Reply from 192.149.252.75: bytes=32 time=112ms TTL=45

Ping statistics for 192.149.252.75:
    Packets: Sent = 25, Received = 25, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 107ms, Maximum = 121ms, Average = 111ms
```

Note: Press the Spacebar to display the rest of the file or press **q** to exit.

To verify that the files have been created, use the **dir** command to list the files in the directory. Also the wildcard ***** can be used to filter only the text files.

```
C:\Users\User1> dir *.txt
Volume in drive C is OS
Volume Serial Number is 0A97-D265

Directory of C:\Users\User1

02/07/2013  12:59 PM                1,642 afrinic.txt
02/07/2013  01:00 PM                1,615 apnic.txt
02/07/2013  12:40 PM                1,641 arin.txt
02/07/2013  12:58 PM                1,589 lacnic.txt
               4 File(s)              6,487 bytes
               0 Dir(s) 34,391,453,696 bytes free
```

Record your results in the following table.

	Minimum	Maximum	Average
www.afrinic.net	359 ms	389 ms	369 ms
www.apnic.net	201	210	204
www.arin.net	107	121	112
www.lacnic.net	216	226	218

Compare the delay results. How is delay affected by geographical location?

In most instances, the response time is longer when compared to the physical distance to the destination.

Part 2: Use Traceroute to Document Network Latency

The routes traced may go through many hops and a number of different ISPs depending on the size of the ISPs and the location of the source and destination hosts. The **traceroute** commands can also be used to observe network latency. In Part 2, the **tracert** command is used to trace the path to the same destinations in Part 1. The command **tracert** is the Windows version of the traceroute command.

The **tracert** command uses ICMP TTL Exceed packets and ICMP echo replies to trace the path.

Step 1: Use the tracert command and record the output to text files.

Copy the following commands to create the traceroute files:

```
C:\Users\User1> tracert www.arin.net > traceroute_arin.txt
C:\Users\User1> tracert www.lacnic.net > traceroute_lacnic.txt
C:\Users\User1> tracert www.afrinic.net > traceroute_afrinic.txt
C:\Users\User1> tracert www.apnic.net > traceroute_apnic.txt
```

Note: If the websites are resolved to IPv6 addresses, the option -4 can be used to resolve to IPv4 addresses if desired. The command becomes **tracert -4 www.arin.net > traceroute_arin.txt**.

Step 2: Use the more command to examine the traced path.

- a. Use the **more** command to access the content of these files:

```
C:\Users\User1> more traceroute_arin.txt
```

```
Tracing route to www.arin.net [192.149.252.75]
```

```
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	11 ms	12 ms	11 ms	10.39.0.1
3	10 ms	15 ms	11 ms	172.21.0.116
4	19 ms	10 ms	11 ms	70.169.73.90
5	13 ms	10 ms	11 ms	chnddsrj01-ae2.0.rd.ph.cox.net [70.169.76.229]
6	72 ms	71 ms	70 ms	mrfdssrj02-ae0.0.rd.dc.cox.net [68.1.1.7]
7	72 ms	71 ms	72 ms	68.100.0.146
8	74 ms	83 ms	73 ms	172.22.66.29
9	75 ms	71 ms	73 ms	172.22.66.29
10	74 ms	75 ms	73 ms	wsip-98-172-152-14.dc.dc.cox.net [98.172.152.14]
11	71 ms	71 ms	71 ms	host-252-131.arin.net [192.149.252.131]
12	73 ms	71 ms	71 ms	www.arin.net [192.149.252.75]

```
Trace complete.
```

In this example, it took less than 1 ms to receive a reply from the default gateway (192.168.1.1). In hop count 6, the round trip to 68.1.1.7 took an average of 71 ms. For the round trip to the final destination at www.arin.net took an average of 72 ms.

Between lines 5 and 6, there is more network delay as indicated by the round trip time increase from an average of 11 ms to 71 ms

- b. Perform the same analysis with the rest of the tracert results.

What can you conclude regarding the relationship between the roundtrip time and geographical location?

In most instances, the response time is longer when compared to the physical distance to the destination.

Part 3: Extended Traceroute

Although **tracert** has different implementations depending on the platform, all versions allow the user to adjust its behavior. In Windows this can be done providing options and switches in the **tracert** command line.

- a. Reverse name resolution (resolving an IP address to a domain name) can add a delay to **tracert** results and yield inaccurate results. To ensure **tracert** won't attempt to reverse resolve hop IP addresses, add the **-d** option to the **tracert** command line:

```
C:\Users\User1> tracert -d www.arin.net > traceroute_d_arin.txt
C:\Users\User1> tracert -d www.lacnic.net > traceroute_d_lacnic.txt
C:\Users\User1> tracert -d www.afrinic.net > traceroute_d_afrinic.txt
C:\Users\User1> tracert -d www.apnic.net > traceroute_d_apnic.txt
```

- b. Use the **more** command to access the content of these files:

```
C:\Users\User1> more traceroute_d_arin.txt
```

```
Tracing route to www.arin.net [192.149.252.75]
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.1.1
2	11 ms	12 ms	11 ms	10.39.0.1
3	10 ms	15 ms	11 ms	172.21.0.116
4	19 ms	10 ms	11 ms	70.169.73.90
5	13 ms	10 ms	11 ms	70.169.76.229
6	72 ms	71 ms	70 ms	68.1.1.7
7	72 ms	71 ms	72 ms	68.100.0.146
8	74 ms	83 ms	73 ms	172.22.66.29
9	75 ms	71 ms	73 ms	172.22.66.29
10	74 ms	75 ms	73 ms	98.172.152.14
11	71 ms	71 ms	71 ms	192.149.252.131
12	73 ms	71 ms	71 ms	192.149.252.75

Trace complete.

What is different about the **tracert** output when the **-d** option was added?

tracert didn't reverse resolve the IP addresses. It simply presented the IP addresses associated with the path hops.

Note: Windows **tracert** will present a list of available options and their descriptions when issued without any options.

Note: Cisco IOS implementation of **traceroute** also allows for fine tuning but it does not rely on command line options. Cisco IOS extended traceroute presents a number of simple questions to allow the administrator to provide values for the desired parameters.

Instructor Note: Redirecting **tracert** output to a text file is useful for data collection and analysis but will keep the student from watching the command's operation. It may be interesting to encourage students to issue **tracert** and **tracert -d** without redirecting the output to a text file; **tracert -d** is much faster than **tracert** as it doesn't need to reverse resolve hop IP addresses.

Reflection

1. The **tracert** and **ping** results can provide important network latency information. What do you need to do if you want an accurate baseline picture regarding network latency for your network?

Answers will vary. You will need to perform careful delay analysis over successive days and during different periods of the day.

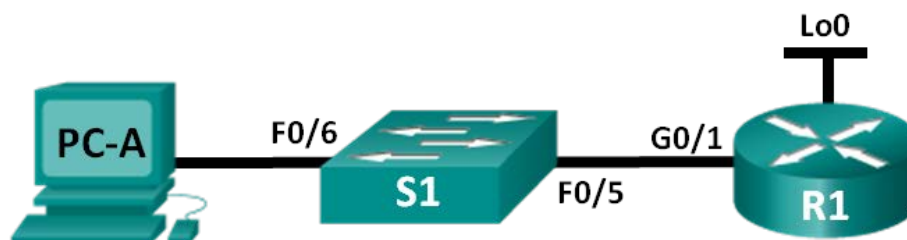
2. How can you use the baseline information?

You can compare baseline data against current data to determine if there has been a change in network response times. This analysis may assist with troubleshooting network issues and scheduling of routine data transfer during off-peak hours.

Lab – Using the CLI to Gather Network Device Information (Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Set Up Topology and Initialize Devices

Part 2: Configure Devices and Verify Connectivity

Part 3: Gather Network Device Information

Background / Scenario

Documenting a working network is one of the most important tasks a network professional can perform. Having proper documentation of IP addresses, model numbers, IOS versions, ports used, and testing security, can go a long way in helping to troubleshoot a network.

In this lab, you will build a small network, configure the devices, add some basic security, and then document the configurations by issuing various commands on the router, switch and PC to gather your information.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Part 1: Set Up the Topology and Initialize Devices

In Part 1, you will set up the network topology, clear any configurations if necessary, and configure basic settings on the router and switch.

Step 1: Cable the network as shown in the topology.

- a. Attach the devices as shown in the topology and cable as necessary.
- b. Power on all devices in the topology.

Step 2: Initialize and reload the router and the switch.

Part 2: Configure Devices and Verify Connectivity

In Part 2, you will set up the network topology and configure basic settings on the router and switch. Refer to the topology and Addressing Table at the beginning of this lab for device names and address information.

Step 1: Configure the IPv4 address for the PC.

Configure the IPv4 address, subnet mask, and default gateway address for PC-A based on the Addressing Table.

Step 2: Configure the router.

- a. Console into the router and enter privileged EXEC mode.
- b. Set the correct time on the router.
- c. Enter global configuration mode.
 - 1) Assign a device name to the router based on the topology and Addressing Table.
 - 2) Disable DNS lookup.
 - 3) Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
 - 4) Assign **class** as the privileged EXEC encrypted password.
 - 5) Assign **cisco** as the console password and enable console login access.
 - 6) Encrypt clear text passwords.
 - 7) Create a domain name of **cisco.com** for SSH access.
 - 8) Create a user named **admin** with a secret password of **cisco** for SSH access.
 - 9) Generate a RSA modulus key. Use **1024** for the number of bits.
- d. Configure VTY line access.
 - 1) Use the local database for authentication for SSH.

- 2) Enable SSH only for login access.
- e. Return to global configuration mode.
 - 1) Create the Loopback 0 interface and assign the IP address based on the Addressing Table.
 - 2) Configure and activate interface G0/1 on the router.
 - 3) Configure interface descriptions for G0/1 and L0.
 - 4) Save the running configuration file to the startup configuration file.

Step 3: Configure the switch.

- a. Console into the switch and enter privileged EXEC mode.
- b. Set the correct time on the switch.
- c. Enter global configuration mode.
 - 1) Assign a device name on the switch based on the topology and Addressing Table.
 - 2) Disable DNS lookup.
 - 3) Create a MOTD banner that warns anyone accessing the device that unauthorized access is prohibited.
 - 4) Assign **class** as the privileged EXEC encrypted password.
 - 5) Encrypt the clear text passwords.
 - 6) Create a domain name of **cisco.com** for SSH access.
 - 7) Create a user named **admin** with a secret password of **cisco** for SSH access.
 - 8) Generate an RSA key. Use **1024** for the number of bits.
 - 9) Create and activate an IP address on the switch based on the topology and Addressing Table.
 - 10) Set the default gateway on the switch.
 - 11) Assign **cisco** as the console password and enable console login access.
- d. Configure VTY line access.
 - 1) Use local database for authentication for SSH.
 - 2) Enable SSH only for login access.
 - 3) Save the running configuration file to the startup configuration file.
- e. Enter proper mode to configure interface descriptions for F0/5 and F0/6.

Step 4: Verify network connectivity.

- a. From a command prompt on PC-A, ping the S1 VLAN 1 IP address. Troubleshoot your physical and logical configurations if the pings were not successful.
- b. From the PC-A command prompt, ping your default gateway IP address on R1. Troubleshoot your physical and logical configurations if the pings were not successful.
- c. From the PC-A command prompt, ping the loopback interface on R1. Troubleshoot your physical and logical configurations if the pings were not successful.
- d. Console back into the switch and ping the G0/1 IP address on R1. Troubleshoot your physical and logical configurations if the pings were not successful.

Part 3: Gather Network Device Information

In Part 3, you will use a variety of commands to gather information about the devices on your network, as well as some performance characteristics. Network documentation is a very important component of managing your network. Documentation of both physical and logical topologies is important, as is verifying platform models and IOS versions of your network devices. Having knowledge of the proper commands to gather this information is essential for a network professional.

Step 1: Gather information on R1 using IOS commands.

One of the most basic steps is to gather information on the physical device, as well as information on the operating system.

- a. Issue the appropriate command to discover the following information:

Instructor Note: Your answers for all of step 1 will vary based on router model and IOS. Note that the answer for Technology Package only applies to routers running IOS 15.0 and greater.

Router Model: _____
Cisco 1941 Router

IOS Version: _____
15.2(4)M3

Total RAM: _____
512MB

Total NVRAM: _____
255K bytes

Total Flash Memory: _____
250880K bytes

IOS Image File: _____
c1900-universalk9-mz.SPA.152-4.M3.bin

Configuration Register: _____
0x2102

Technology Package: _____
ipbasek9

What command did you issue to gather the information?

The **show version** command can be used from either the user EXEC or privileged EXEC prompt.

- b. Issue the appropriate command to display a summary of important information about the router interfaces. Write down the command and record your results below.

Note: Only record interfaces that have IP addresses.

The **show ip interface brief** command can be used from either the user EXEC or privileged EXEC prompt.

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/1	192.168.1.1	YES	NVRAM	up	up
Loopback0	209.165.200.225	YES	NVRAM	up	up

<some output omitted>

- c. Issue the appropriate command to display the routing table. Write down the command and record your results below.

The **show ip route** command can be used from either the user EXEC or privileged EXEC prompt.

```
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
209.165.200.0/24 is variably subnetted, 2 subnets, 2 masks
C    209.165.200.224/27 is directly connected, Loopback0
L    209.165.200.225/32 is directly connected, Loopback0
```

- d. What command would you use to display the Layer 2 to Layer 3 mapping of addresses on the router? Write down the command and record your results below.

The **show arp** command can be used from either the user EXEC or privileged EXEC prompt.

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	30f7.0da3.1821	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	0	c80a.a9fa.de0d	ARPA	GigabitEthernet0/1
Internet	192.168.1.11	2	0cd9.96d2.34c0	ARPA	GigabitEthernet0/1

- e. What command would you use to see detailed information about all the interfaces on the router or about a specific interface? Write down the command below.

The **show interfaces** command can be used from either the user EXEC or privileged EXEC prompt.

- f. Cisco has a very powerful protocol that operates at Layer 2 of the OSI model. This protocol can help you map out how Cisco devices are connected physically, as well as determining model numbers and even IOS versions and IP addressing. What command or commands would you use on router R1 to find out information about switch S1 to help you complete the table below?

Device ID	Local Interface	Capability	Model #	Remote Port ID	IP Address	IOS Version
S1.cisco.com	G 0/1	Switch	WS-2960-24TT-L	F 0/5	192.168.1.11	15.0(2)SE1

The **show cdp neighbors detail** command can be used from either the user EXEC or privileged EXEC prompt.

- g. A very elementary test of your network devices is to see if you can telnet into them. Remember, Telnet is not a secure protocol. It should not be enabled in most cases. Using a Telnet client, such as Tera Term or PuTTY, try to telnet to R1 using the default gateway IP address. Record your results below.

Tera Term Output: Connection refused.

- h. From PC-A, test to ensure that SSH is working properly. Using an SSH client, such as Tera Term or PuTTY, SSH into R1 from PC-A. If you get a warning message regarding a different key, click **Continue**. Log in with the appropriate username and password you created in Part 2. Were you successful?

Yes.

The various passwords configured on your router should be as strong and protected as possible.

Note: The passwords used for our lab (**cisco** and **class**) do not follow the best practices needed for strong passwords. These passwords are used merely for the convenience of performing the labs. By default, the console password and any vty passwords configured would display in clear text in your configuration file.

- i. Verify that all of your passwords in the configuration file are encrypted. Write down the command and record your results below.

Command: _____

The **show running-config** or **show run** command can be used from the privileged EXEC prompt.

Is the console password encrypted? _____ Yes

Is the SSH password encrypted? _____ Yes

Step 2: Gather information on S1 using IOS commands.

Many of the commands that you used on R1 can also be used with the switch. However, there are some differences with some of the commands.

Instructor Note: Answers for all of Step 2 will vary based on Switch model, ports used, and MAC addresses.

- a. Issue the appropriate command to discover the following information:

Switch Model: _____ WS-C2960-24TT-L

IOS Version: _____ 15.0(2)SE1

Total NVRAM: _____ 64K

IOS Image File: _____ c2960-lanbasek9-mz.150-2.SE1.bin

What command did you issue to gather the information?

The **show version** command can be used from either the user EXEC or privileged EXEC prompt.

- b. Issue the appropriate command to display a summary of status information about the switch interfaces. Write down the command and record your results below.

Note: Only record active interfaces.

The **show ip interface brief** command can be used from either the user EXEC or privileged EXEC prompt.

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	192.168.1.11	YES	NVRAM	up	up
FastEthernet0/5	unassigned	YES	unset	up	up
FastEthernet0/6	unassigned	YES	unset	up	up

<some output omitted>

- c. Issue the appropriate command to display the switch MAC address table. Record the dynamic type MAC addresses only in the space below.

The **show mac address-table** command can be used from either the user EXEC or privileged EXEC prompt.

Mac Address Table

Vlan	Mac Address	Type	Ports
----	-----	-----	-----
1	30f7.0da3.1821	DYNAMIC	Fa0/5
1	c80a.a9fa.de0d	DYNAMIC	Fa0/6

- d. Verify that Telnet VTY access is disabled on S1. Using a Telnet client, such as Tera Term or PuTTY, try to telnet to S1 using the 192.168.1.11 address. Record your results below.

Tera Term Output: Connection refused.

- e. From PC-A, test to ensure that SSH is working properly. Using an SSH client, such as Tera Term or PuTTY, SSH into S1 from PC-A. If you get a warning message regarding a different key, click **Continue**. Log in with an appropriate username and password. Were you successful?

Yes.

- f. Complete the table below with information about router R1 using the appropriate command or commands necessary on S1.

Device Id	Local Interface	Capability	Model #	Remote Port ID	IP Address	IOS Version
R1.cisco.com	F 0/5	Router	CISCO1941/K9	G 0/1	192.168.1.1	15.2(4)M3

The **show cdp neighbors detail** command can be used from either the user EXEC or privileged EXEC prompt.

- g. Verify that all of your passwords in the configuration file are encrypted. Write down the command and record your results below.

Command: _____

The **show running-config** or **show run** command can be used from the privileged EXEC prompt.

Is the console password encrypted? _____ Yes

Step 3: Gather information on PC-A.

Using various Windows utility commands, you will gather information on PC-A.

- a. From the PC-A command prompt, issue the **ipconfig /all** command and record your answers below.

```
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix . : 
    Description . . . . . : Realtek PCIe GBE Family Controller
    Physical Address. . . . . : C8-0A-A9-FA-DE-0D
    DHCP Enabled. . . . . : No
    Autoconfiguration Enabled . . . . : Yes
    IPv4 Address. . . . . : 192.168.1.3 (Preferred)
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
<output omitted>
```

What is the PC-A IP address?

192.168.1.3

What is the PC-A subnet mask?

255.255.255.0

What is the PC-A default gateway address?

192.168.1.1

What is the PC-A MAC address?

Answers will vary.

Lab – Using the CLI to Gather Network Device Information

- b. Issue the appropriate command to test the TCP/IP protocol stack with the NIC. What command did you use?

```
C:\> ping 127.0.0.1
```

```
Pinging 127.0.0.1 with 32 bytes of data:  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128  
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

- c. Ping the loopback interface of R1 from the PC-A command prompt. Was the ping successful?

Yes.

- d. Issue the appropriate command on PC-A to trace the list of router hops for packets originating from PC-A to the loopback interface on R1. Record the command and output below. What command did you use?

```
C:\> tracert 209.165.200.225  
  
Tracing route to 209.165.200.225 over a maximum of 30 hops  
  0      1 ms      1 ms      1 ms  209.165.200.225  
Trace complete.
```

- e. Issue the appropriate command on PC-A to find the Layer 2 to Layer 3 address mappings held on your NIC. Record your answers below. Only record answers for the 192.168.1.0/24 network. What command did you use?

```
C:\> arp -a
```

```
Interface: 192.168.1.3 --- 0xb  
Internet Address      Physical Address      Type  
192.168.1.1           30-f7-0d-a3-18-21    dynamic  
192.168.1.11          0c-d9-96-d2-34-c0    dynamic  
192.168.1.255         ff-ff-ff-ff-ff-ff    static
```

Reflection

Why is it important to document your network devices?

Having the proper information including: IP addresses, physical port connections, IOS versions, copies of configuration files, and the amount of memory storage, can greatly aid you when troubleshooting and performing network baseline tests. Having good documentation can also help you recover from network outages and replacing equipment when necessary.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs

Router R1

```
R1#sh run
Building configuration...

Current configuration : 1545 bytes
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
```

Lab – Using the CLI to Gather Network Device Information

```
enable secret 4 06YFDUHH61wAE/kLkDq9BGholQM5EnRtoyr8cHAUg.2
!
no aaa new-model
no ip domain lookup
ip domain name cisco.com
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
!
username admin secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
!
ip ssh version 1
!
interface Loopback0
  description Emulate ISP Connection
  ip address 209.165.200.225 255.255.255.224
!
interface Embedded-Service-Engine0/0
  no ip address
  shutdown
!
interface GigabitEthernet0/0
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface GigabitEthernet0/1
  description Connected to LAN
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface Serial0/0/0
  no ip address
  shutdown
  clock rate 2000000
!
interface Serial0/0/1
  no ip address
  shutdown
  clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
```

```
!  
!  
control-plane  
!  
!  
banner motd ^CWarning! Unauthorized access is prohibited.^C  
!  
line con 0  
  password 7 060506324F41  
  login  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  login local  
  transport input ssh  
!  
scheduler allocate 20000 1000  
!  
End
```

Switch S1

```
S1#sh run  
Building configuration...  
  
Current configuration : 1752 bytes  
!  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2  
!  
username admin secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY  
no aaa new-model
```



```
system mtu routing 1500
!
!
no ip domain-lookup
ip domain-name cisco.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh version 1
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
description Connected to R1
!
interface FastEthernet0/6
description Connected to PC-A
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
```

```
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
 ip default-gateway 192.168.1.1
 ip http server
 ip http secure-server
!
 banner motd ^CWarning! Unauthorized access is prohibited.^C
!
 line con 0
  password 7 00071A150754
  login
 line vty 0 4
  login local
  transport input ssh
 line vty 5 15
  login local
  transport input ssh
!
end
```

Class Activity - Design and Build a Small Business Network (Capstone Project) (Instructor Version – Optional Class Activity)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Objectives

Explain how a small network of directly connected segments is created, configured and verified.

Background /Scenario

Note: This activity is best completed in groups of 2-3 students.

Design and build a network from scratch.

- Your design must include a minimum of one router, one switch, and one PC.
- Fully configure the network and use IPv4 or IPv6 (subnetting must be included as a part of your addressing scheme).
- Verify the network using at least five show commands.
- Secure the network using SSH, secure passwords and console passwords (minimum).

Create a rubric to use for informal peer grading. Present your Capstone Project to the class and be able to answer questions from your peers and Instructor!

Instructor Note: This optional Modeling Activity is suggested to be a graded assignment after completing Chapters 1-11. Students should be able to show how small networks are designed, configured, verified and secured. Documentation is a large factor of this project and students must be able to explain their network design and verification through the use of `show` commands.

Required Resources

- Packet Tracer
- Student/group-created rubric for assessment of the assignment

Reflection

1. What was the most difficult portion of this activity?

Answers will vary.

2. Why do you think network documentation is so important to this activity and in the real world?

Documentation is imperative to good network management and without it, network administrators have to recreate topologies, physically check addressing, etc. This takes time, which could be used elsewhere.

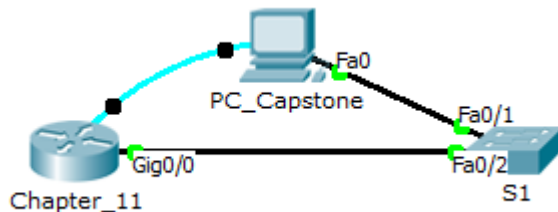
Class Activity - Design and Build a Small Business Network (Capstone Project)

A suggested rubric and documentation examples are provided below:

Note: This rubric includes a total of 100 points for the points earned category (if minimum standards are met). Instructors may wish to consider adding bonus points for additional/advanced work in any requirement category.

Requirement	Points Earned
Physical Topology – minimum 1 router, 1 switch, 1 PC	(20 suggested)
Logical Addressing – subnetting used?	(20 suggested)
Connectivity test – ping the router	(20 suggested)
Show commands (at least 5 documented as baseline)	(20 suggested)
Security – SSH, secure passwords, console security – documented by show running-configuration	(20 suggested)

Create a small network of directly connected segments, at a minimum 1 router, 1 switch and 1 PC, and include a screenshot of the network in your final documentation.



Configure the network to include switches, routers, and end devices and use your own network addressing. You must use subnetting of some type and you can use either IPv4 or IPv6 logical addressing. Create a table showing your physical addressing scheme for the router, switch, and PC and include it in your final documentation.

Device Name	IP Address	Subnet Mask
Chapter_11	Gig0/0 – 192.168.1.30	255.255.255.224
S1	VLAN1 – 192.168.1.20	255.255.255.224
PC_Capstone	Fa0 – 192.168.1.10	255.255.255.224

Verify the network by using show commands (at least 5) to provide a performance baseline. Be able to discuss why you chose the show commands you selected and what the output means (use all Packet Tracer activities for Chapters 1-11). Keep screenshots of your output and include in your final documentation.

```
Chapter_11# show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.10 42 0006.2AAC.4D31 ARPA GigabitEthernet0/0
Internet 192.168.1.20 15 0006.2A79.8B1E ARPA GigabitEthernet0/0
Internet 192.168.1.30 - 0060.7032.3601 ARPA GigabitEthernet0/0
Chapter_11#
```

```
S1#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.10 13 0006.2AAC.4D31 ARPA Vlan1
Internet 192.168.1.20 - 0006.2A79.8B1E ARPA Vlan1
Internet 192.168.1.30 13 0060.7032.3601 ARPA Vlan1
S1#
```

```
Chapter_11#show protocols
Global values:
  Internet Protocol routing is enabled
GigabitEthernet0/0 is up, line protocol is up
  Internet address is 192.168.1.30/27
GigabitEthernet0/1 is administratively down, line protocol is down
Vlan1 is administratively down, line protocol is down
```

```
Chapter_11#show ip route
Codes: L - local, C - connected, S - static, 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

  192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/27 is directly connected, GigabitEthernet0/0
L       192.168.1.30/32 is directly connected, GigabitEthernet0/0
Chapter_11#
```

S1#show vlan

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig1/1, Gig1/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
1002	fddi	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0
1004	fdnet	101004	1500	-	-	-	ieee	-	0	0
1005	trnet	101005	1500	-	-	-	ibm	-	0	0

Remote SPAN VLANs

Primary	Secondary	Type	Ports

S1#

Chapter_11#show int

GigabitEthernet0/0 is up, line protocol is up (connected)

Hardware is CN Gigabit Ethernet, address is 0060.7032.3601 (bia 0060.7032.3601)
Internet address is 192.168.1.30/27
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); 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
7 packets input, 196 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
0 watchdog, 1017 multicast, 0 pause input
0 input packets with dribble condition detected
9 packets output, 252 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

GigabitEthernet0/1 is administratively down, line protocol is down (disabled)

Hardware is CN Gigabit Ethernet, address is 0060.7032.3602 (bia 0060.7032.3602)
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is RJ45
output flow-control is unsupported, input flow-control is unsupported

ARP type: ARPA, ARP Timeout 04:00:00,
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0 (size/max/drops); 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
0 watchdog, 1017 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 unknown protocol drops
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier
0 output buffer failures, 0 output buffers swapped out

Vlan1 is administratively down, line protocol is down

Hardware is CPU Interface, address is 000b.be45.b842 (bia 000b.be45.b842)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input 21:40:21, 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
1682 packets input, 530955 bytes, 0 no buffer
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
563859 packets output, 0 bytes, 0 underruns
0 output errors, 23 interface resets
0 output buffer failures, 0 output buffers swapped out
Chapter_11#

```
Chapter_11#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.1(4)M4, REL
EASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 23-Feb-11 14:19 by pt_team

ROM: System Bootstrap, Version 15.1(4)M4, RELEASE SOFTWARE (fc1)
cisco1941 uptime is 1 hours, 47 seconds
System returned to ROM by power-on
System image file is "flash0:c1900-universalk9-mz.SPA.151-1.M4.bin"
Last reload type: Normal Reload

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 CISC01941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

License Info:

License UDI:

-----
Device#      PID                      SN
-----
*0           CISC01941/K9             FTX152453SZ

Technology Package License Information for Module:'c1900'

-----
Technology    Technology-package      Technology-package
Current       Type                    Next reboot
-----
ipbase        ipbasek9               Permanent          ipbasek9
security      None                   None               None
data          None                   None               None

Configuration register is 0x2102

Chapter_11#
```

Secure the network using common configuration to include SSH, secure passwords, console security, etc. and show the commands configured by enacting a show running-configuration screen as output. Include in your final documentation.

Chapter_11#show run

Building configuration...

Current configuration : 842 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

security passwords min-length 8

!

hostname Chapter_11

!

login block-for 120 attempts 3 within 60

!

license udi pid CISCO1941/K9 sn FTX152453SZ

!

spanning-tree mode pvst

!

interface GigabitEthernet0/0

ip address 192.168.1.30 255.255.255.224

duplex auto

speed auto

!

interface GigabitEthernet0/1

no ip address

duplex auto

speed auto

shutdown

!

interface Vlan1

no ip address

shutdown

!

ip classless

!

line con 0

password 7 0822455D0A16

login

!

line aux 0

!

line vty 0 4

password 7 0822455D0A165445415F5952

login

!

end

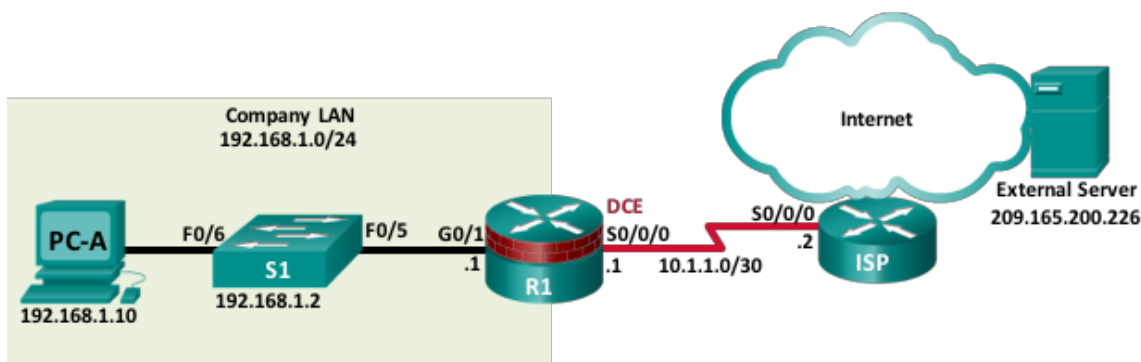
Identify elements of the model that map to real-world applications:

All facets of this activity map to IT-related content and real-world applications because this is a culminating activity for all 11 Chapters.

Lab - Troubleshooting Connectivity Issues (Instructor Version – Recommend Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	Lo0	209.165.200.226	255.255.255.255	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.10	255.255.255.0	192.168.1.1

Objectives

Part 1: Identify the Problem

Part 2: Implement Network Changes

Part 3: Verify Full Functionality

Part 4: Document Findings and Configuration Changes

Background / Scenario

In this lab, the company that you work for is experiencing problems with their Local Area Network (LAN). You have been asked to troubleshoot and resolve the network issues. In Part 1, you will connect to devices on the LAN and use troubleshooting tools to identify the network issues, establish a theory of probable cause, and test that theory. In Part 2, you will establish a plan of action to resolve and implement a solution. In Part 3, you will verify full functionality has been restored. Part 4 provides space for you to document your troubleshooting findings along with the configuration changes that you made to the LAN devices.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions may be used.

Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Required Resources

- 2 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 1 PC (Windows 7 or 8 with terminal emulation program, such as Tera Term)
- Ethernet and Serial cables as shown in the topology

Troubleshooting Configurations

The following settings must be configured on the devices shown in the topology. Paste the configurations onto the specified devices prior to starting the lab.

PC:

IP Address: **192.168.1.10**
Subnet Mask: **255.255.255.0**
Default Gateway: **(leave blank)**

Instructor: You may choose to configure the PC settings; otherwise, student will know that the missing default gateway setting is a problem.

S1:

```
no ip domain-lookup
hostname S1
ip domain-name ccna-lab.com
username admin01 privilege 15 secret 9
$9$lJgfiLCHj.Xp/q$ha2w.oyQPTMhBGPeR.FZo3NZRJ9T1FdqvgRCFyBYnNs
interface FastEthernet0/1
 shutdown
interface FastEthernet0/2
 shutdown
interface FastEthernet0/3
 shutdown
interface FastEthernet0/4
 shutdown
interface FastEthernet0/5
 duplex full
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

R1:

```
hostname R1
no ip domain-lookup
ip domain-name ccna-lab.com
username admin01 privilege 15 secret 9
$9$8a4jGjbPPpeeoE$WyPsIiOaYT4ATlJzrR6T9E6vIdESOGF.NYX53arPmtA
interface GigabitEthernet0/0
shutdown
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex half
speed auto
no shutdown
interface Serial0/0/0
ip address 10.1.2.1 255.255.255.252
no shutdown
interface Serial0/0/1
no ip address
shutdown
line vty 0 4
login local
transport input ssh
crypto key generate rsa general-keys modulus 1024
end
```

ISP:

```
hostname ISP
no ip domain-lookup
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
no shut
interface Lo0
ip address 209.165.200.226 255.255.255.255
ip route 0.0.0.0 0.0.0.0 10.1.1.1
end
```

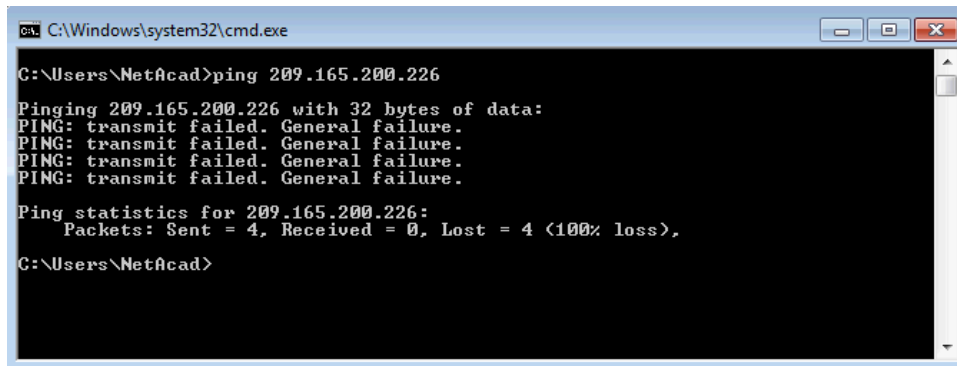
Part 1: Identify the Problem.

The only available information about the network problem is that the users are experiencing slow response times and that they are not able to reach an external device on the Internet at IP address 209.165.200.226. To determine probable cause(s) for these network issues, you will need to utilize network commands and tools on the LAN equipment shown in the topology.

Note: The user name **admin01** with a password of **cisco12345** will be required to log into the network equipment.

Step 1: Troubleshoot from the PC.

- a. From the PC command prompt, **ping** the external server IP Address **209.165.200.226**.



```
C:\Windows\system32\cmd.exe

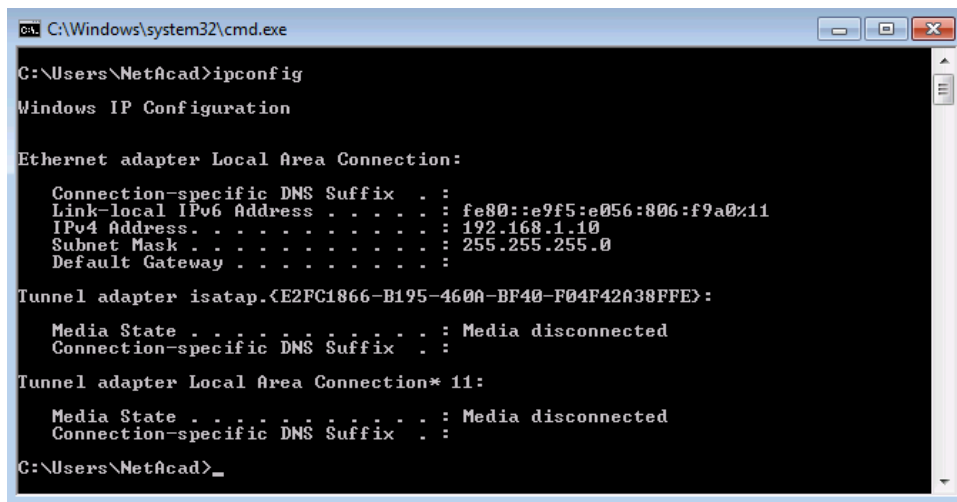
C:\Users\NetAcad>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\NetAcad>
```

- b. Use the **ipconfig** command to determine the network settings on the PC.



```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e9f5:e056:806:f9a0%11
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

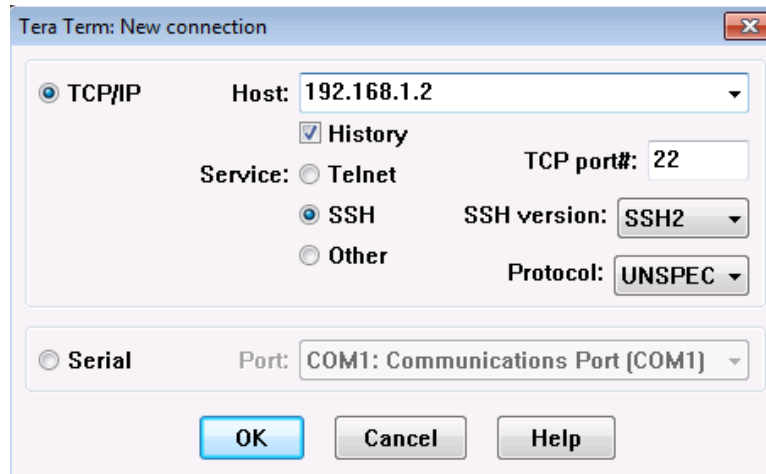
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\NetAcad>
```

Step 2: Troubleshoot from S1 using a SSH client session.

Note: Any SSH client software can be used. Tera Term is used in the examples in this lab.

- a. SSH to S1 using its IP Address of 192.168.1.2 and log into the switch using **admin01** for the user name and **cisco12345** for the password.



- b. Issue the **terminal monitor** command on S1 to allow log messages to be sent to the VTY line of your SSH session. After a few seconds you notice the following error message being displayed in your SSH window.

```
S1# terminal monitor
```

```
S1#
```

```
*Mar  1 02:08:11.338: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
FastEthernet0/5 (not half duplex), with R1.ccna-lab.com GigabitEthernet0/1
(half duplex).
```

```
S1#
```

- c. On S1, issue the **show interface f0/5** command to view the duplex setting of the interface.

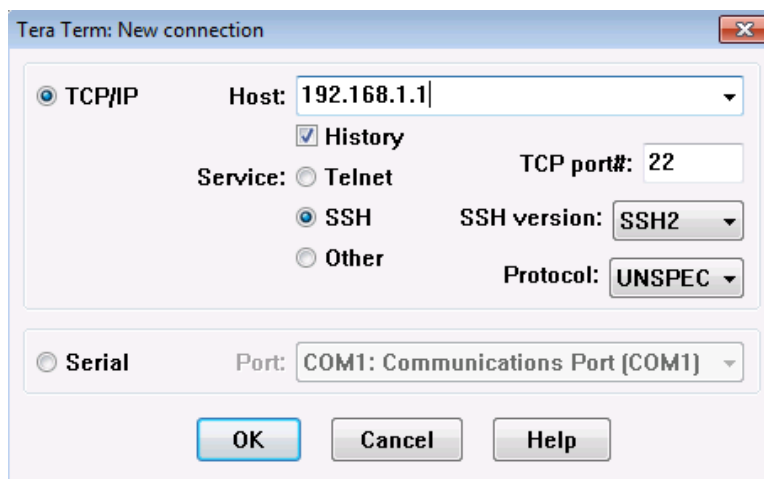
```
S1# show interface f0/5
```

```
FastEthernet0/5 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a05 (bia 0cd9.96e8.8a05)
  MTU 1500 bytes, BW 100000 Kbit/sec, 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, 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 00:00:35, 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: 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
    849 packets input, 104642 bytes, 0 no buffer
    Received 123 broadcasts (122 multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

```
0 watchdog, 122 multicast, 0 pause input
0 input packets with dribble condition detected
4489 packets output, 361270 bytes, 0 underruns
0 output errors, 0 collisions, 1 interface resets
0 unknown protocol drops
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
S1#
```

Step 3: Troubleshoot on R1 using an SSH client.

- SSH to R1's LAN interface and log in using **admin01** for the user name and **cisco12345** as the password.



- Issue the **terminal monitor** command on R1 to allow log messages to be sent to the VTY line of your SSH session for R1. After a few seconds the duplex mismatch message appears on R1's SSH session.

```
R1# terminal monitor
```

```
R1#
```

```
*Nov 23 16:12:36.623: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/1 (not full duplex), with S1.ccna-lab.com FastEthernet0/5 (full
duplex).
```

```
R1#
```

- Issue the **show interface G0/1** command on R1 to display the duplex setting.

```
R1# show interfaces g0/1
```

```
GigabitEthernet0/1 is up, line protocol is up
```

```
Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c1 (bia d48c.b5ce.a0c1)
```

```
Internet address is 192.168.1.1/24
```

```
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```
Half Duplex, 100Mbps, media type is RJ45
```

```
output flow-control is unsupported, input flow-control is unsupported
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input 00:00:15, 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
  641 packets input, 101892 bytes, 0 no buffer
    Received 453 broadcasts (0 IP multicasts)
      0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 361 multicast, 0 pause input
  1043 packets output, 123698 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    235 unknown protocol drops
    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
```

R1#

- d. Issue the **ping 209.165.200.226** command on R1 to test connectivity to the external server.

R1# **ping 209.165.200.226**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

R1#

- e. Issue the **show ip interface brief** command on R1 to verify interface IP Address settings.

R1# **show ip interface brief**

Interface	IP-Address	OK?	Method	Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/0	unassigned	YES	unset	administratively down	down
GigabitEthernet0/1	192.168.1.1	YES	manual	up	up
Serial0/0/0	10.1.2.1	YES	manual	up	up
Serial0/0/1	unassigned	YES	unset	administratively down	down

R1#

- f. Issue the **show ip route** command on R1 to verify the router's default gateway setting.

R1# **show ip route**

Codes: L - local, C - connected, S - static, 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

i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP

a - application route

+ - replicated route, % - next hop override

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C    10.1.2.0/30 is directly connected, Serial0/0/0
L    10.1.2.1/32 is directly connected, Serial0/0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C    192.168.1.0/24 is directly connected, GigabitEthernet0/1
L    192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

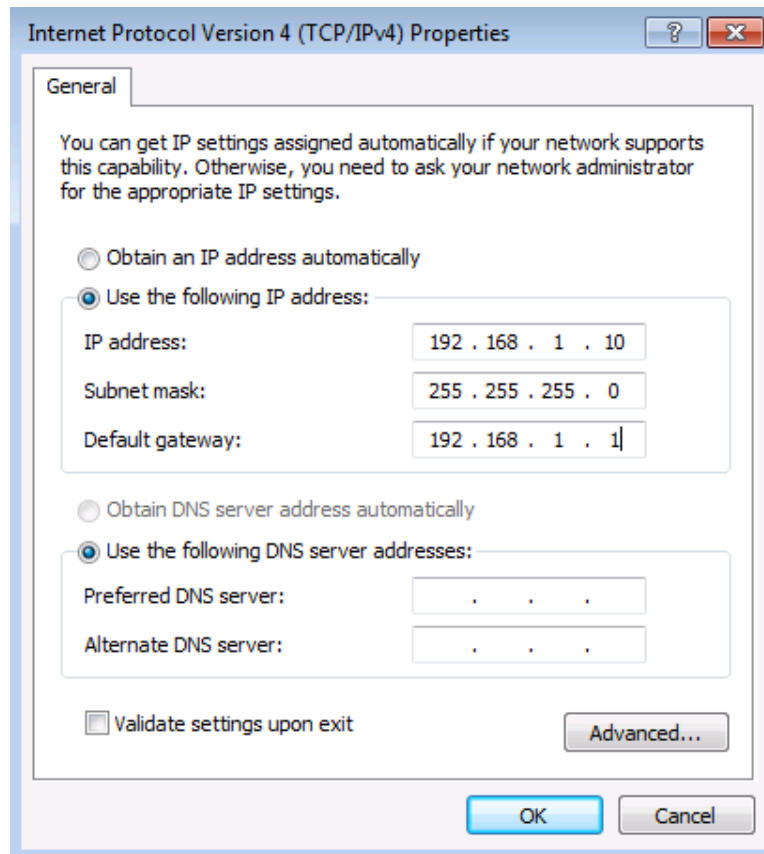
List the probable causes for the network problems that employees are experiencing.

1. The Default Gateway is not set on the PC.
2. Interface G0/1 is set to Half-Duplex on R1.
3. An incorrect IP Address is set on S0/0/0 on R1.
4. The Gateway of last resort is not set on R1.

Part 2: Implement Network Changes

You have communicated the problems that you discovered in Part 1 to your supervisor. She has approved these changes and has requested that you implement them.

Step 1: Set the Default Gateway on the PC to 192.168.1.1.



Step 2: Set the duplex setting for interface G0/1 on R1 to full duplex.

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
*Nov 23 17:23:36.879: %CDP-4-DUPLEX_MISMATCH: duplex mismatch discovered on
GigabitEthernet0/1 (not full duplex), with S1.ccna-lab.com FastEthernet0/5
(full duplex).
R1(config)#
R1(config)# interface g0/1
R1(config-if)# duplex full
R1(config-if)# exit
*Nov 23 17:24:08.039: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
down
R1(config)#
*Nov 23 17:24:10.363: %LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to
up
*Nov 23 17:24:10.459: %SYS-5-CONFIG_I: Configured from console by console
R1(config)#
```

Step 3: Reconfigure the IP address for S0/0/0 to IP Address 10.1.1.1/30 on R1.

```
R1(config)# interface s0/0/0
```

```
R1(config-if)# ip address 10.1.1.1 255.255.255.252
R1(config-if)# exit
```

Step 4: Configure the Gateway of last resort on R1 with a 10.1.1.2 default route.

```
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.2
R1(config)# end
```

Part 3: Verify Full Functionality

Verify that full functionality has been restored.

Step 1: Verify that all interfaces and routes have been set correctly and that routing has been restored on R1.

- a. Issue the **show ip route** command to verify that the default gateway has been set correctly.

```
R1# show ip route
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, 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, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override
```

Gateway of last resort is 10.1.1.2 to network 0.0.0.0

```
S*    0.0.0.0/0 [1/0] via 10.1.1.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C      10.1.1.0/30 is directly connected, Serial0/0/0
L      10.1.1.1/32 is directly connected, Serial0/0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.1.0/24 is directly connected, GigabitEthernet0/1
L      192.168.1.1/32 is directly connected, GigabitEthernet0/1
R1#
```

- b. Issue the **show ip interface s0/0/0** command to verify that the IP Address on S0/0/0 is set correctly.

```
R1# show ip interface s0/0/0
Serial0/0/0 is up, line protocol is up
  Internet address is 10.1.1.1/30
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  <output omitted>
  IPv4 WCCP Redirect exclude is disabled
R1#
```

- c. Issue the **ping 209.165.200.226** command to verify that the external server is reachable now.

```
R1# ping 209.165.200.226
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

R1#

- d. Issue the **show interface g0/1** command to verify that the duplex setting is full duplex.

R1# show interface g0/1

GigabitEthernet0/1 is up, line protocol is up

Hardware is CN Gigabit Ethernet, address is d48c.b5ce.a0c1 (bia d48c.b5ce.a0c1)

Internet address is 192.168.1.1/24

MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Full Duplex, 100Mbps, media type is RJ45

output flow-control is unsupported, input flow-control is unsupported

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:00:04, output 00:00:04, 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

559 packets input, 74066 bytes, 0 no buffer

Received 279 broadcasts (0 IP multicasts)

0 runs, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 208 multicast, 0 pause input

742 packets output, 81462 bytes, 0 underruns

0 output errors, 0 collisions, 2 interface resets

133 unknown protocol drops

0 babbles, 0 late collision, 0 deferred

1 lost carrier, 0 no carrier, 0 pause output

0 output buffer failures, 0 output buffers swapped out

R1#

Step 2: Verify End-to-End connectivity from the LAN PC.

- Issue the **ipconfig** command from the command prompt on the PC.

```
C:\Windows\system32\cmd.exe

C:\Users\NetAcad>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::e9f5:e056:806:f9a0%11
    IPv4 Address. . . . . : 192.168.1.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Tunnel adapter isatap.{E2FC1866-B195-460A-BF40-F04F42A38FFE}:

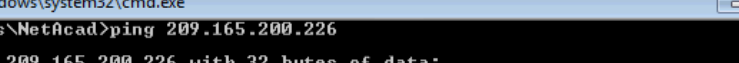
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter Local Area Connection* 11:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\NetAcad>
```

- b. Issue the **ping 209.165.200.226** command from the CMD window on the PC



The screenshot shows a Windows command prompt window with the title bar "C:\Windows\system32\cmd.exe". The command prompt shows the user typing "C:\Users\NetAcad>ping 209.165.200.226". The output of the command is displayed as follows:

```
C:\Users\NetAcad>ping 209.165.200.226

Pinging 209.165.200.226 with 32 bytes of data:
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254
Reply from 209.165.200.226: bytes=32 time=1ms TTL=254

Ping statistics for 209.165.200.226:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\NetAcad>
C:\Users\NetAcad>
```

Part 4: Document Findings and Configuration Changes

Use the space provided below to document the issues found during your troubleshooting and the configurations changes made to resolve those issues.

[illegible]

Documentation will vary but should include the date when troubleshooting was conducted, devices that were tested, commands used along with the output generated by those commands, issues found, and configuration changes made to resolve those issues.

Reflection

This lab had you troubleshoot all devices before making any changes. Is there another way to apply the troubleshooting methodology?

Answers may vary. Another way the troubleshooting methodology could be applied would be to complete all 6 steps on a device before moving on to another device. e.g. After you determined that the default gateway was not set on the PC, you would add the default gateway setting and verify functionality. If network issues still exist, you would then move on to the next device, S1 in this example. When the troubleshooting process had been completed on S1 and issues still exist, you would then move on to R1. This process would continue until full network functionality was achieved.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.

Device Configs - Final

Router R1

```
R1# show run
Building configuration...
Current configuration : 1531 bytes
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
no aaa new-model
memory-size iomem 15
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
```

```
!  
cts logging verbose  
!  
username admin01 privilege 15 secret 9  
$9$8a4jGjbPPpeeoE$WyPsIiOaYT4ATlJzrR6T9E6vIdESOGF.NYX53arPmtA  
!  
redundancy  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.1.1 255.255.255.0  
duplex full  
speed auto  
!  
interface Serial0/0/0  
ip address 10.1.1.1 255.255.255.252  
clock rate 2000000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
ip route 0.0.0.0 0.0.0.0 10.1.1.2  
!  
control-plane  
!  
line con 0  
line aux 0  
line 2  
no activation-character  
no exec  
transport preferred none  
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
stopbits 1  
line vty 0 4
```



```
login local
transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
S1# show run
Building configuration...
Current configuration : 1585 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
username admin01 privilege 15 secret 9
$9$lJgfiLCHj.Xp/q$ha2w.oyQPTMhBGPeR.FZo3NZRJ9T1FdqvgRCFyBYnNs
no aaa new-model
system mtu routing 1500
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
shutdown
!
interface FastEthernet0/2
shutdown
!
interface FastEthernet0/3
shutdown
!
interface FastEthernet0/4
shutdown
!
interface FastEthernet0/5
```

```
duplex full
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
ip address 192.168.1.2 255.255.255.0
!
ip http server
ip http secure-server
```

```
!  
line con 0  
line vty 0 4  
  login local  
  transport input ssh  
line vty 5 15  
  login local  
  transport input ssh  
!  
end
```

Router ISP

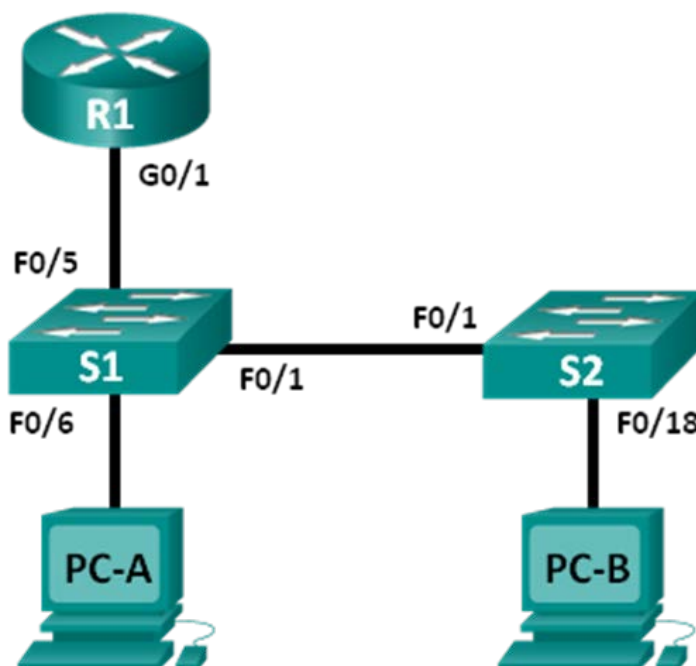
```
ISP# show run  
Building configuration...  
Current configuration : 1390 bytes  
!  
version 15.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname ISP  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
memory-size iomem 15  
!  
no ip domain lookup  
ip cef  
no ipv6 cef  
!  
multilink bundle-name authenticated  
!  
cts logging verbose  
!  
redundancy  
!  
interface Loopback0  
  ip address 209.165.200.226 255.255.255.255  
!  
interface Embedded-Service-Engine0/0  
  no ip address  
  shutdown  
!  
interface GigabitEthernet0/0  
  no ip address  
  shutdown
```

```
duplex auto
speed auto
!
interface GigabitEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
ip address 10.1.1.2 255.255.255.252
!
interface Serial0/0/1
no ip address
shutdown
clock rate 125000
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.1.1.1
!
control-plane
!
line con 0
line aux 0
line 2
no activation-character
no exec
transport preferred none
transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
stopbits 1
line vty 0 4
login
transport input none
!
scheduler allocate 20000 1000
!
end
```

Lab – Observing ARP with the Windows CLI, IOS CLI, and Wireshark (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S2	VLAN 1	192.168.1.12	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.2	255.255.255.0	192.168.1.1

Objectives

Part 1: Build and Configure the Network

Part 2: Use the Windows ARP Command

Part 3: Use the IOS Show ARP Command

Part 4: Use Wireshark to Examine ARP Exchanges

Background / Scenario

The Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IP address to a Layer 2 MAC address. When a frame is placed on the network, it must have a destination MAC address. To dynamically discover the MAC address for the destination device, an ARP request is broadcast on the LAN. The device that contains the destination IP address responds, and the MAC address is recorded in the ARP cache. Every device on the LAN keeps its own ARP cache, or small area in RAM that holds ARP results. An ARP cache timer removes ARP entries that have not been used for a certain period of time.

ARP is an excellent example of performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN. Conversely, unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address.

A network administrator should be aware of ARP, but may not interact with the protocol on a regular basis. ARP is a protocol that enables network devices to communicate with the TCP/IP protocol. Without ARP, there is no efficient method to build the datagram Layer 2 destination address. Also, ARP is a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association in a network. An attacker forges the MAC address of a device, and frames are sent to the wrong destination. Manually configuring static ARP associations is one way to prevent ARP spoofing. Finally, an authorized MAC address list may be configured on Cisco devices to restrict network access to only approved devices.

In this lab, you will use the ARP commands in Cisco routers and in Windows to display the ARP table. You will also clear the ARP cache and add static ARP entries.

Note: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and the output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

Note: Make sure that the routers and switches have been erased and have no startup configurations. If you are unsure, contact your instructor.

Instructor Note: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

Instructor Note: Some of the ARP commands in Windows Vista or later operating systems will require administrator privileges.

Required Resources

- 1 Router (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
- 2 Switches (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
- 2 PCs (Windows 7, 8, or 10 with terminal emulation program, such as Tera Term and Wireshark installed)
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet cables as shown in the topology

Note: The Fast Ethernet interfaces on Cisco 2960 switches are autosensing and an Ethernet straight-through cable may be used between switches S1 and S2. If using another Cisco switch model, it may be necessary to use an Ethernet crossover cable.

Part 1: Build and Configure the Network

Step 1: Cable the network according to the topology.

Step 2: Configure the IP addresses for the devices according to the Addressing Table.

Step 3: Verify network connectivity by pinging all the devices from PC-B.

Part 2: Use the Windows ARP Command

The **arp** command allows the user to view and modify the ARP cache in Windows. You access this command from the Windows command prompt.

Step 1: Display the ARP cache.

- a. Open a command window on PC-A and type **arp**.

```
C:\> arp
```

Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).

```
ARP -s inet_addr eth_addr [if_addr]
```

```
ARP -d inet_addr [if_addr]
```

```
ARP -a [inet_addr] [-N if_addr] [-v]
```

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.

-g Same as -a.

-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.

inet_addr Specifies an internet address.

-N if_addr Displays the ARP entries for the network interface specified by if_addr.

-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.

-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.

eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.

Example:

```
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
```

```
> arp -a .... Displays the arp table.
```

- b. Examine the output.

What command would be used to display all entries in the ARP cache?

```
arp -a
```

What command would be used to delete all ARP cache entries (flush ARP cache)?

```
arp -d *
```

What command would be used to delete the ARP cache entry for 192.168.1.11?

```
arp -d 192.168.1.11
```

- c. Type **arp -a** to display the ARP table.

```
C:\> arp -a
```

```
Interface: 192.168.1.3 --- 0x13
```

Internet Address	Physical Address	Type
192.168.1.1	50-3d-e5-aa-c0-a1	dynamic
224.0.0.22	01-00-5e-00-00-16	static

```
C:\> arp -a
```

```
No ARP Entries Found.
```

- d. Ping from PC-A to PC-B to dynamically add entries in the ARP cache.

```
C:\> ping 192.168.1.2
```

```
Interface: 192.168.1.3 --- 0x13
```

Internet Address	Physical Address	Type
192.168.1.1	50-3d-e5-aa-c0-a1	dynamic
192.168.1.2	00-21-70-cf-3d-cc	dynamic
224.0.0.22	01-00-5e-00-00-16	static

What is the physical address for the host with IP address of 192.168.1.2?

```
00-21-70-cf-3d-cc
```

Step 2: Adjust entries in the ARP cache manually.

To delete entries in ARP cache, issue the command **arp -d {inet-addr | *}**. Addresses can be deleted individually by specifying the IP address, or all entries can be deleted with the wildcard *****.

Verify that the ARP cache contains the following entries: the R1 G0/1 default gateway (192.168.1.1), PC-B (192.168.1.2) and both switches (192.168.1.11 and 192.168.1.12).

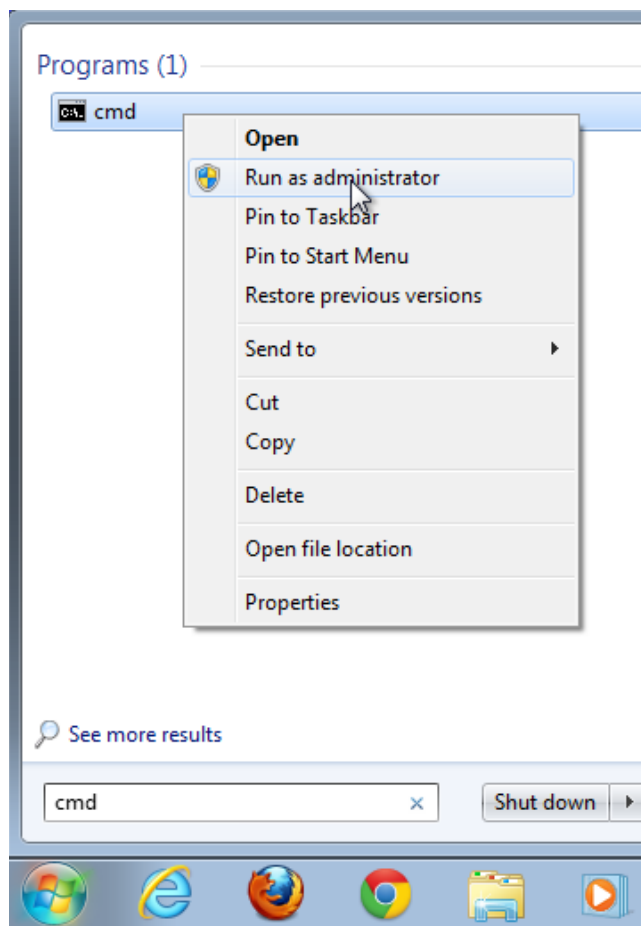
- From PC-A, ping all the addresses in the Address Table.
- Verify that all the addresses have been added to the ARP cache. If the address is not in ARP cache, ping the destination address and verify that the address was added to the ARP cache.

```
C:\> arp -a
```


Interface: 192.168.1.3 --- 0x13

Internet Address	Physical Address	Type
192.168.1.1	50-3d-e5-aa-c0-a1	dynamic
192.168.1.2	00-21-70-cf-3d-cc	dynamic
192.168.1.11	00-09-b7-e6-c0-40	dynamic
192.168.1.12	00-17-e0-2c-56-c0	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static

- c. As an administrator, access the command prompt. Click the **Start** icon, and in the *Search programs and file* box, type **cmd**. When the **cmd** icon appears, right-click the icon and select **Run as administrator**. Click **Yes** to allow this program to make changes.



- d. In the Administrator command prompt window, type **arp -d ***. This command deletes all the ARP cache entries. Verify that all the ARP cache entries are deleted by typing **arp -a** at the command prompt.

```
C:\windows\system32> arp -d *  
C:\windows\system32> arp -a  
No ARP Entries Found.
```

- e. Wait a few minutes. The Neighbor Discovery protocol starts to populate the ARP cache again.

```
C:\> arp -a
```

Interface: 192.168.1.3 --- 0xb

Internet Address	Physical Address	Type
192.168.1.255	ff-ff-ff-ff-ff-ff	static

- f. From PC-A, ping PC-B (192.168.1.2) and the switches (192.168.1.11 and 192.168.1.12) to add the ARP entries. Verify that the ARP entries have been added to the cache.

```
C:\> arp -a
```

```
Interface: 192.168.1.3 --- 0xb
```

192.168.1.1	50-3d-e5-aa-c0-a1	dynamic
192.168.1.2	00-21-70-cf-3d-cc	dynamic
192.168.1.11	00-09-b7-e6-c0-40	dynamic
192.168.1.12	00-17-e0-2c-56-c0	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static

- g. Record the physical address for switch S2.

Answers will vary. 0c-17-e0-2c-56-c0 in this case.

- h. Delete a specific ARP cache entry by typing **arp -d inet-addr**. At the command prompt, type **arp -d 192.168.1.12** to delete the ARP entry for S2.

```
C:\windows\system32> arp -d 192.168.1.12
```

- i. Type **arp -a** to verify that the ARP entry for S2 has been removed from the ARP cache.

```
C:\> arp -a
```

```
Interface: 192.168.1.3 --- 0x13
```

Internet Address	Physical Address	Type
192.168.1.1	50-3d-e5-aa-c0-a1	dynamic
192.168.1.2	00-21-70-cf-3d-cc	dynamic
192.168.1.11	00-09-b7-e6-c0-40	dynamic
224.0.0.22	01-00-5e-00-00-16	static

Part 3: Use the IOS show arp Command

The Cisco IOS can also display the ARP cache on routers and switches with the **show arp** or **show ip arp** command.

Step 1: Display ARP entries on router R1.

```
R1# show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.1.1	-	503d.e5aa.c0a1	ARPA	GigabitEthernet0/1
Internet	192.168.1.2	29	0021.70cf.3dcc	ARPA	GigabitEthernet0/1
Internet	192.168.1.3	10	0026.b9dd.0091	ARPA	GigabitEthernet0/1
Internet	192.168.1.12	37	0017.e02c.56c0	ARPA	GigabitEthernet0/1

```
R1#
```

Notice there is no Age (-) for the first entry, router interface G0/1 (the LAN default gateway). The Age is the number of minutes (min) that the entry has been in ARP cache and is incremented for the other entries. The Neighbor Discovery protocol populates the PC-A and PC-B IP and MAC address ARP entries.

Step 2: Add ARP entries on router R1.

You can add ARP entries to the ARP table of the router by pinging other devices.

- a. Ping switch S1.

```
R1# ping 192.168.1.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.11, timeout is 2 seconds:
..!!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 1/1/1 ms
```

- b. Verify that an ARP entry for switch S1 has been added to the ARP table of R1.

```
R1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.1 - 503d.e5aa.c0a1 ARPA GigabitEthernet0/1
Internet 192.168.1.2 32 0021.70cf.3dcc ARPA GigabitEthernet0/1
Internet 192.168.1.3 13 0026.b9dd.0091 ARPA GigabitEthernet0/1
Internet 192.168.1.11 0 0009.b7e6.c040 ARPA GigabitEthernet0/1
Internet 192.168.1.12 40 0017.e02c.56c0 ARPA GigabitEthernet0/1
```

Step 3: Display ARP entries on switch S1.

```
S1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.11 - 0009.b7e6.c040 ARPA VLAN1
Internet 192.168.1.12 42 0017.e02c.56c0 ARPA VLAN1
Internet 192.168.1.1 3 503d.e5aa.c0a1 ARPA VLAN1
Internet 192.168.1.3 16 0026.b9dd.0091 ARPA VLAN1
```

Step 4: Add ARP entries on switch S1.

By pinging other devices, ARP entries can also be added to the ARP table of the switch.

- a. From switch S1, ping PC-B.

```
S1# ping 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, min/avg/max = 1/201/1002 ms
..!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/2/8 ms
```

- b. Verify that the ARP entry for PC-B has been added to ARP table of S1.

```
S1# show ip arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 192.168.1.11 - 0009.b7e6.c040 ARPA VLAN1
Internet 192.168.1.12 44 0017.e02c.56c0 ARPA VLAN1
Internet 192.168.1.1 5 503d.e5aa.c0a1 ARPA VLAN1
Internet 192.168.1.3 17 0026.b9dd.0091 ARPA VLAN1
Internet 192.168.1.2 0 0021.70cf.3dcc ARPA VLAN1
```

Part 4: Use Wireshark to Examine ARP Exchanges

In Part 4, you will examine ARP exchanges by using Wireshark to capture and evaluate the ARP exchange. You will also examine network latency caused by ARP exchanges between devices.

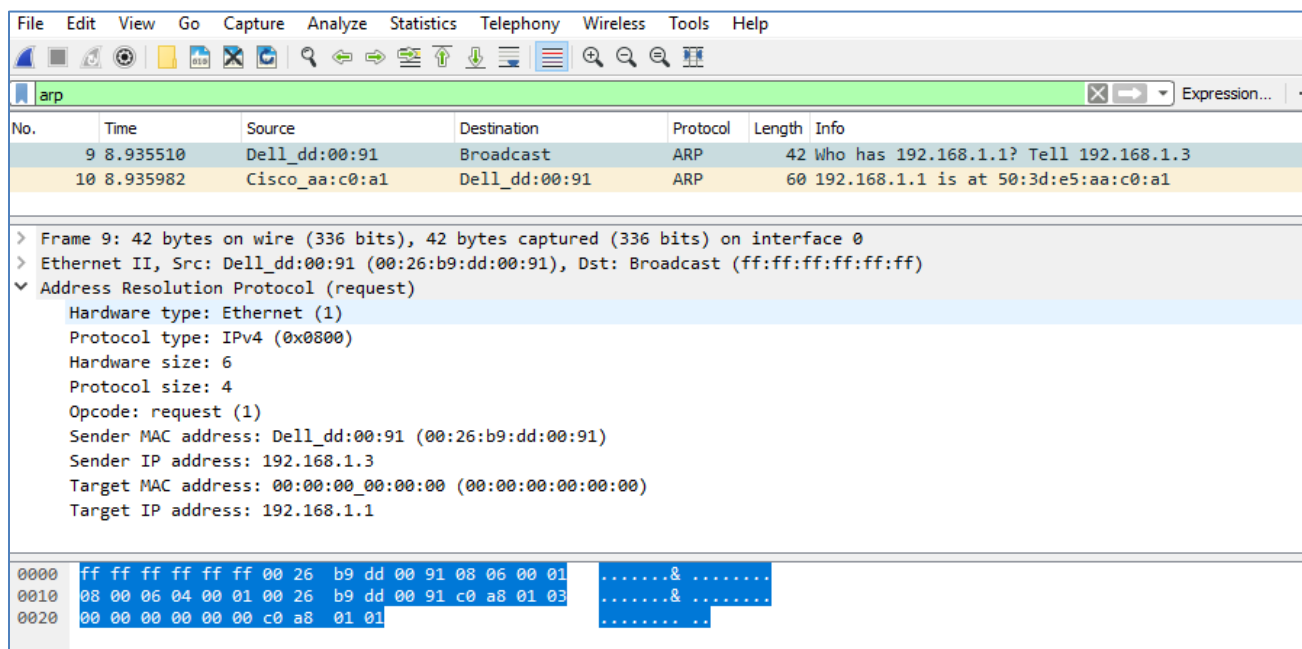
Step 1: Configure Wireshark for packet captures.

- Start Wireshark.
- Choose the network interface to use for capturing the ARP exchanges.

Step 2: Capture and evaluate ARP communications.

- Start capturing packets in Wireshark. Use the filter to display only ARP packets.
- Flush the ARP cache by typing the **arp -d *** command at the command prompt.
- Verify that the ARP cache has been cleared.
- Send a ping to the default gateway, using the **ping 192.168.1.1** command.
- Stop the Wireshark capture after pinging to the default gateway is finished.
- Examine the Wireshark captures for the ARP exchanges in the packet details pane.

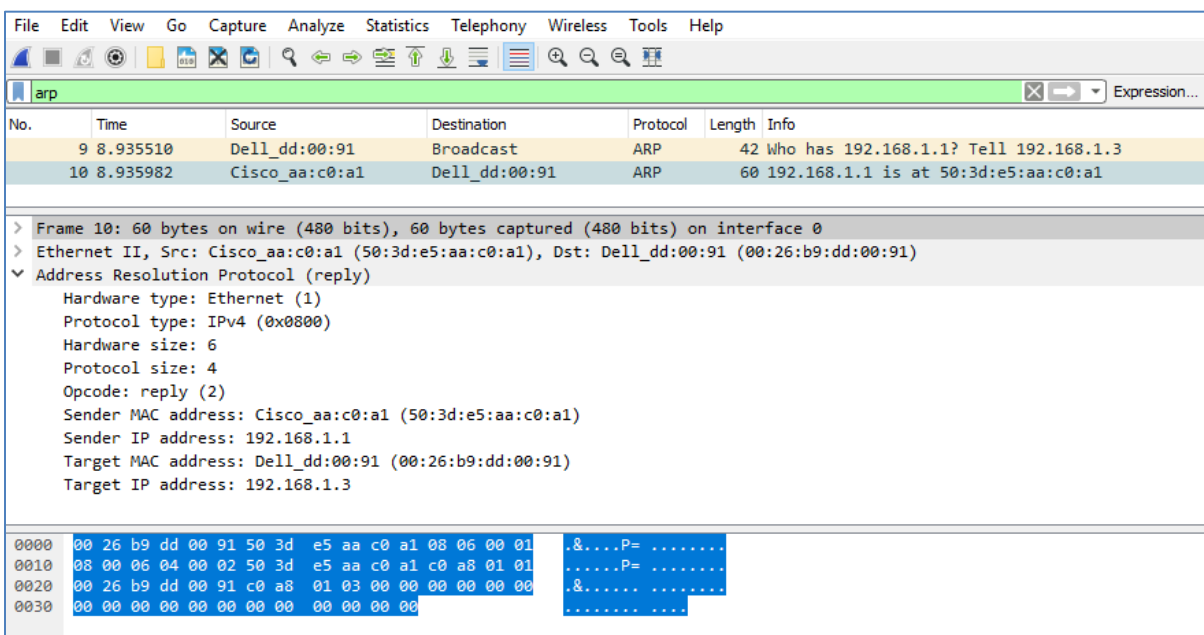
What was the first ARP packet? _____ ARP request



Fill in the following table with information about your first captured ARP packet.

Field	Value
Sender MAC address	00:26:b9:dd:00:91 - Answers will vary.
Sender IP address	192.168.1.3
Target MAC address	00:00:00:00:00:00
Target IP address	192.168.1.1

What was the second ARP packet? _____ ARP reply



Fill in the following table with information about your second captured ARP packet.

Field	Value
Sender MAC address	50:3d:e5:aa:c0:a1 - Answers will vary.
Sender IP address	192.168.1.1
Target MAC address	00:26:b9:dd:00:91 - Answers will vary.
Target IP address	192.168.1.3

Step 3: Examine network latency caused by ARP.

- Clear the ARP entries on PC-A.
- Clear the ARP entries on S2.

S2# **clear arp-cache**

- Start a Wireshark capture.
- Ping switch S2 (192.168.1.12). The ping should be successful after the first echo request.

Note: If all the pings were successful, S1 should be reloaded to observe network latency with ARP.

C:\> **ping 192.168.1.12**

```
Pinging 192.168.1.12 with 32 bytes of data:
Request timed out.
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time<1ms TTL=255
Reply from 192.168.1.12: bytes=32 time=1ms TTL=255
```

Lab – Observing ARP with the Windows CLI, IOS CLI and Wireshark

Ping statistics for 192.168.1.12:

Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 1ms, Average = 0ms

- e. Stop the Wireshark capture after the pinging is finished. Use the Wireshark filter to display only ARP and ICMP outputs. In Wireshark, type **arp or icmp** in the **Filter:** entry area.
- f. Examine the Wireshark capture. In this example, frame 5 is the first ICMP request sent by PC-A to S2. Because there is no ARP entry for S2, an ARP request was sent to the management IP address of S2 asking for the MAC address. During the ARP exchanges, the echo request did not receive a reply before the request was timed out. (frames 3 – 7)

After the ARP entry for S2 was added to the ARP cache, the last three ICMP exchanges were successful, as displayed in frames 11-12, 14-15, and 16-17.

As displayed in the Wireshark capture, ARP is an excellent example of performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN.

No.	Time	Source	Destination	Protocol	Length	Info
3	3.017248	Dell_dd:00:91	Broadcast	ARP	42	Who has 192.168.1.12? Tell 192.168.1.3
4	3.018038	Cisco_2c:56:c0	Dell_dd:00:91	ARP	60	192.168.1.12 is at 00:17:e0:2c:56:c0
5	3.018070	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=157/40192,
6	3.018917	Cisco_2c:56:c0	Broadcast	ARP	60	Who has 192.168.1.3? Tell 192.168.1.12
7	3.018939	Dell_dd:00:91	Cisco_2c:56:c0	ARP	42	192.168.1.3 is at 00:26:b9:dd:00:91
11	7.623769	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=158/40448,
12	7.624594	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=158/40448,
14	8.639461	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=159/40704,
15	8.640252	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=159/40704,
16	9.655142	192.168.1.3	192.168.1.12	ICMP	74	Echo (ping) request id=0x0001, seq=160/40960,
17	9.655975	192.168.1.12	192.168.1.3	ICMP	74	Echo (ping) reply id=0x0001, seq=160/40960,

Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: Dell_dd:00:91 (00:26:b9:dd:00:91), Dst: Cisco_2c:56:c0 (00:17:e0:2c:56:c0)

Internet Protocol Version 4, Src: 192.168.1.3, Dst: 192.168.1.12

Internet Control Message Protocol

Type: 8 (Echo (ping) request)

Code: 0

Checksum: 0x4cbe [correct]

[Checksum Status: Good]

Identifier (BE): 1 (0x0001)

Identifier (LE): 256 (0x0100)

Sequence number (BE): 157 (0x009d)

Sequence number (LE): 40192 (0x9d00)

[No response seen]

Data (32 bytes)

0000 00 17 e0 2c 56 c0 00 26 b9 dd 00 91 08 00 45 00 ...V..&E.

0010 00 3c 06 e2 00 00 80 01 00 00 c0 a8 01 03 c0 a8 <.....

0020 01 0c 08 00 4c be 00 01 00 9d 61 62 63 64 65 66L... ..abcdef

Reflection

1. How and when are static ARP entries removed?

They are deleted manually.

2. Why do you want to add static ARP entries in the cache?

A static ARP entry can mitigate ARP spoofing or poisoning in the network.

3. If ARP requests can cause network latency, why is it a bad idea to have unlimited hold times for ARP entries?

Unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address.

Router Interface Summary Table

Router Interface Summary				
Router Model	Ethernet Interface #1	Ethernet Interface #2	Serial Interface #1	Serial Interface #2
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Note: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface.				

Device Configs

Router R1

```
R1#show run
```

```
Building configuration...
```

```
Current configuration : 1165 bytes
```

```
!
```

```
version 15.2
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
no service password-encryption
```

```
!  
hostname R1  
!  
boot-start-marker  
boot-end-marker  
!  
!  
!  
no aaa new-model  
memory-size iomem 15  
!  
!  
ip cef  
no ipv6 cef  
multilink bundle-name authenticated  
!  
!  
interface Embedded-Service-Engine0/0  
no ip address  
shutdown  
!  
interface GigabitEthernet0/0  
no ip address  
shutdown  
duplex auto  
speed auto  
!  
interface GigabitEthernet0/1  
ip address 192.168.1.1 255.255.255.0  
duplex auto  
speed auto  
!  
interface Serial0/0/0  
no ip address  
shutdown  
clock rate 2000000  
!  
interface Serial0/0/1  
no ip address  
shutdown  
!  
ip forward-protocol nd  
!  
no ip http server  
no ip http secure-server  
!  
!  
control-plane  
!
```



```
!  
line con 0  
line aux 0  
line 2  
  no activation-character  
  no exec  
  transport preferred none  
  transport input all  
  transport output pad telnet rlogin lapb-ta mop udptn v120 ssh  
  stopbits 1  
line vty 0 4  
  login  
  transport input all  
!  
scheduler allocate 20000 1000  
!  
end
```

Switch S1

```
S1#show run  
Building configuration...  
  
Current configuration : 1305 bytes  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname S1  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
system mtu routing 1500  
!  
!spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3
```

```
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7  
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
ip address 192.168.1.11 255.255.255.0
```

```
!  
ip http server  
ip http secure-server  
!  
line con 0  
line vty 5 15  
!  
end
```

Switch S2

```
S2#show run  
Building configuration...  
  
Current configuration : 1313 bytes  
!  
version 15.0  
no service pad  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname S2  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
system mtu routing 1500  
!  
!  
spanning-tree mode pvst  
spanning-tree extend system-id  
!  
vlan internal allocation policy ascending  
!  
!  
interface FastEthernet0/1  
!  
interface FastEthernet0/2  
!  
interface FastEthernet0/3  
!  
interface FastEthernet0/4  
!  
interface FastEthernet0/5  
!  
interface FastEthernet0/6  
!  
interface FastEthernet0/7
```

```
!  
interface FastEthernet0/8  
!  
interface FastEthernet0/9  
!  
interface FastEthernet0/10  
!  
interface FastEthernet0/11  
!  
interface FastEthernet0/12  
!  
interface FastEthernet0/13  
!  
interface FastEthernet0/14  
!  
interface FastEthernet0/15  
!  
interface FastEthernet0/16  
!  
interface FastEthernet0/17  
!  
interface FastEthernet0/18  
!  
interface FastEthernet0/19  
!  
interface FastEthernet0/20  
!  
interface FastEthernet0/21  
!  
interface FastEthernet0/22  
!  
interface FastEthernet0/23  
!  
interface FastEthernet0/24  
!  
interface GigabitEthernet0/1  
!  
interface GigabitEthernet0/2  
!  
interface Vlan1  
  ip address 192.168.1.12 255.255.255.0  
!  
ip http server  
ip http secure-server  
!  
line con 0  
line vty 5 15  
!  
end
```

Lab – Researching Subnet Calculators (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Objectives

Part 1: Review Available Subnet Calculators

Part 2: Perform Network Calculations Using a Subnet Calculator

Background / Scenario

While it is important to understand how to convert a decimal IP address to its binary format and apply the bitwise ANDing operation to determine the network address, it is also a tedious and mistake-prone process. To assist with these calculations, many network administrators make use of an IP subnet calculator utility program. A number of these types of programs have been developed that can be downloaded or run directly from the Internet.

In this lab, you will be introduced to a few of the free IP subnet calculators that are available. You will use a web-based IP subnet calculator to perform the network operations in this lab.

Required Resources

Device with Internet access

Part 1: Review Available Subnet Calculators

In Part 1, you are introduced to two types of subnet calculators: client-based (programs that are downloaded and installed) and web-based (utilities that are run from a browser).

Step 1: Review client-based subnet calculators.

Solarwinds provides a free subnet calculator that can be downloaded and installed on a PC running a Windows operating system. You will be required to provide personal information (Name, Company, Location, Email Address, and Phone number) to be able to download this program. You can download and install the Solarwinds Subnet Calculator at www.solarwinds.com.

If you have a PC running Linux, it is recommended that you use the **ipcalc** utility (available with most Linux distributions). Use the **apt-get install ipcalc** command to install ipcalc on a PC running Linux.

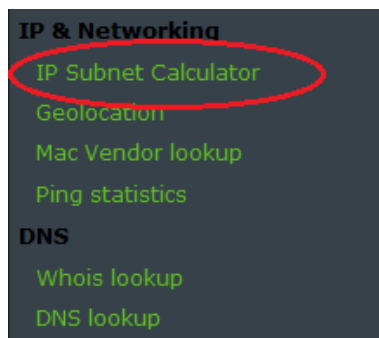
Step 2: Use a web-based subnet calculator.

Web-based subnet calculators do not require installation, but you do need Internet access to use them. The following web-based subnet calculator is accessible from any device that has Internet access, including smartphones and tablets.

a. From your browser, go to www.ipcalc.org and click the **IP Subnet Calculator** link.

Note: Several other useful utilities are also listed on the menu, such as MAC vendor lookup, whois lookup, and DNS lookup.

Note: At the time of this writing, a page formatting issue was encountered when viewing the www.ipcalc.org website using Internet Explorer (Version 9). While the site functioned correctly, you may want to consider using another browser (Firefox or Chrome) when accessing this site.



- b. On the IP Subnet Calculator screen, enter an IP address and subnet mask or an IP address and CIDR prefix notation. Examples of how to enter each of these are shown in the Introduction area.

:: IP Subnet Calculator ::

Introduction:

A subnet is a logically visible subdivision of an IP network. The practice of dividing a network into subnetworks is called subnetting.

This application will help you to compute information about IP subnetting. It's easy to use.

In the following form you can enter differents address format:

Description	Format
IP & CIDR Netmask	10.0.0.1/22
IP & Netmask	10.0.0.1 255.255.252.0
IP & Wildcard Mask	10.0.0.1 0.0.3.255

The behavior of this application is the same that the *ipcalc* binary of GNU/Linux system's !

Application:

- c. In the Application field, enter **192.168.50.50/27** and click **Calc!**. The next screen displays a table with network information in both decimal and binary formats.

Application:

Description	Value	Extra
Address	192.168.50.50	11000000.10101000.00110010.00110010
Netmask	255.255.255.224	11111111.11111111.11111111.11100000 /27
Network	192.168.50.32	11000000.10101000.00110010.00100000
Broadcast	192.168.50.63	
Host min	192.168.50.33	11000000.10101000.00110010.00100001
Host max	192.168.50.62	11000000.10101000.00110010.00111110
Host/net	30	Class C, Private Internet

- d. Using the information provided in the example above, answer the following questions.

What is the network address? _____ 192.168.50.32

What is the subnet mask? _____ 255.255.255.224

How many hosts will this network support? _____ 30

What is the lowest host address? _____ 192.168.50.33

What is the highest host address? _____ 192.168.50.62

What is the broadcast address? _____ 192.168.50.63

Part 2: Perform Network Calculations Using a Subnet Calculator

In Part 2, use the www.ipcalc.org web-based subnet calculator to fill in the tables provided.

Step 1: Fill in the following table for address 10.223.23.136/10:

Description	Decimal	Binary
Address	10.223.23.136	00001010.11011111.00010111.10001000
Subnet mask	255.192.0.0	11111111.11000000.00000000.00000000
Network address	10.192.0.0	00001010.11000000.00000000.00000000
Broadcast address	10.255.255.255	00001010.11111111.11111111.11111111
First host address	10.192.0.1	00001010.11000000.00000000.00000001
Last host address	10.255.255.254	00001010.11111111.11111111.11111110
Number of hosts available	4,194,302	N/A

What type of address, public, or private? _____ Private

Step 2: Fill in the following table for the 172.18.255.92 address with a subnet mask of 255.255.224.0:

Description	Decimal	Binary
Address	172.18.255.92	10101100.00010010.11111111.01011100
Subnet mask	255.255.224.0	11111111.11111111.11100000.00000000
Network address	172.18.224.0	10101100.00010010.11100000.00000000
Broadcast address	172.18.255.255	10101100.00010010.11111111.11111111
First host address	172.18.224.1	10101100.00010010.11100000.00000001
Last host address	172.18.255.254	10101100.00010010.11111111.11111110
Number of hosts available	8,190	N/A

What is the CIDR prefix notation for this network? _____ /19

What type of address, public, or private? _____ Private

Step 3: Fill in the following table using the 192.168.184.78 address with a subnet mask of 255.255.255.252:

Description	Decimal	Binary
Address	192.168.184.78	11000000.10101000.10111000.01001110
Subnet mask	255.255.255.252	11111111.11111111.11111111.11111100
Network address	192.168.184.76	11000000.10101000.10111000.01001100
Broadcast address	192.168.184.79	11000000.10101000.10111000.01001111
First host address	192.168.184.77	11000000.10101000.10111000.01001101
Last host address	192.168.184.78	11000000.10101000.10111000.01001110
Number of hosts available	2	N/A

What is the CIDR prefix notation for this network? _____ /30

What type of address, public, or private? _____ Private

Where would you most likely find a network like this being used?

Answers may vary, but a good use for a /30 network is on serial link between two routers. Only two host addresses are needed for this type of link.

Step 4: Fill in the following table for the 209.165.200.225/27 address:

Description	Decimal	Binary
Address	209.165.200.225	11010001.10100101.11001000.11100001
Subnet mask	255.255.255.224	11111111.11111111.11111111.11100000
Network address	209.165.200.224	11010001.10100101.11001000.11100000
Broadcast address	209.165.200.255	11010001.10100101.11001000.11111111
First host address	209.165.200.225	11010001.10100101.11001000.11100001
Last host address	209.165.200.254	11010001.10100101.11001000.11111110
Number of hosts available	30	N/A

What type of address, public, or private? _____ Public

Step 5: Fill in the following table for address 64.104.110.7/20:

Description	Decimal	Binary
Address	64.104.110.7	01000000.01101000.01101110.00000111
Subnet mask	255.255.240.0	11111111.11111111.11110000.00000000
Network address	64.104.96.0	01000000.01101000.01100000.00000000
Broadcast address	64.104.111.255	01000000.01101000.01101111.11111111
First host address	64.104.96.1	01000000.01101000.01100000.00000001
Last host address	64.104.111.254	01000000.01101000.01101111.11111110
Number of hosts available	4096	N/A

What type of address, public, or private? _____ **Public**

Reflection

1. What is an advantage of using a client-based subnet calculator?

Answers may vary. Client-based subnet calculators do not require Internet access.

2. What is an advantage of using a web-based subnet calculator?

Answers may vary, but web-based subnet calculators do not require download and installation. They can be accessed by any device with Internet access, including mobile devices such as a smart phones and tablets.

Lab – Subnetting Network Topologies (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Objectives

Parts 1 to 5, for each network topology:

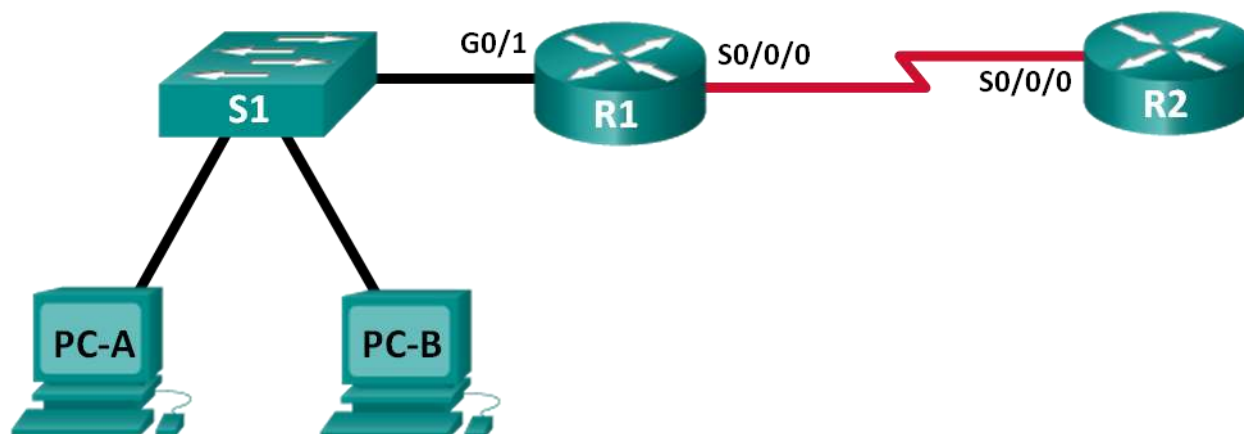
- Determine the number of subnets.
- Design an appropriate addressing scheme.
- Assign addresses and subnet mask pairs to device interfaces.
- Examine the use of the available network address space and future growth potential.

Background / Scenario

When given a network topology, it is important to be able to determine the number of subnets required. In this lab, several scenario topologies will be provided, along with a base network address and mask. You will subnet the network address and provide an IP addressing scheme that will accommodate the number of subnets displayed in the topology diagram. You must determine the number of bits to borrow, the number of hosts per subnet, and potential for growth as specified by the instructions.

Part 1: Network Topology A

In Part 1, you have been given the 192.168.10.0/24 network address to subnet, with the following topology. Determine the number of networks needed and then design an appropriate addressing scheme.



Step 1: Determine the number of subnets in Network Topology A.

- How many subnets are there? 2
- How many bits should you borrow to create the required number of subnets? 1
- How many usable host addresses per subnet are in this addressing scheme? 126
- What is the new subnet mask in dotted decimal format? 255.255.255.128
- How many subnets are available for future use? 0

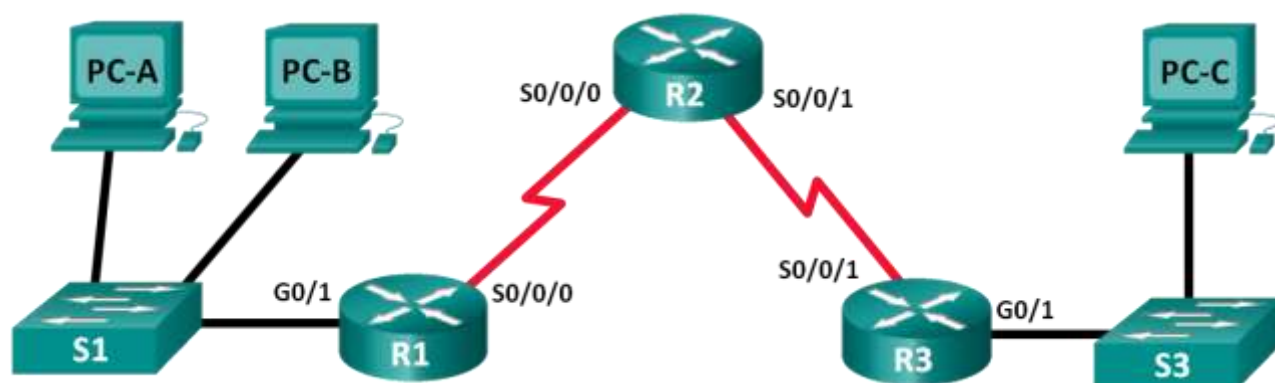
Step 2: Record the subnet information.

Fill in the following table with the subnet information:

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.10.0	192.168.10.1	192.168.10.126	192.168.10.127
1	192.168.10.128	192.168.10.129	192.168.10.254	192.168.10.255
2				
3				
4				
5				

Part 2: Network Topology B

The network topology from Part 1 has expanded to accommodate the addition of router R3 and its accompanying network, as illustrated in the following topology. Use the 192.168.10.0/24 network address to provide addresses to the network devices, and then design a new addressing scheme to support the additional network requirement.



Step 1: Determine the number of subnets in Network Topology B.

- How many subnets are there? 4
- How many bits should you borrow to create the required number of subnets? 2
- How many usable host addresses per subnet are in this addressing scheme? 62
- What is the new subnet mask in dotted decimal format? 255.255.255.192
- How many subnets are available for future use? 0

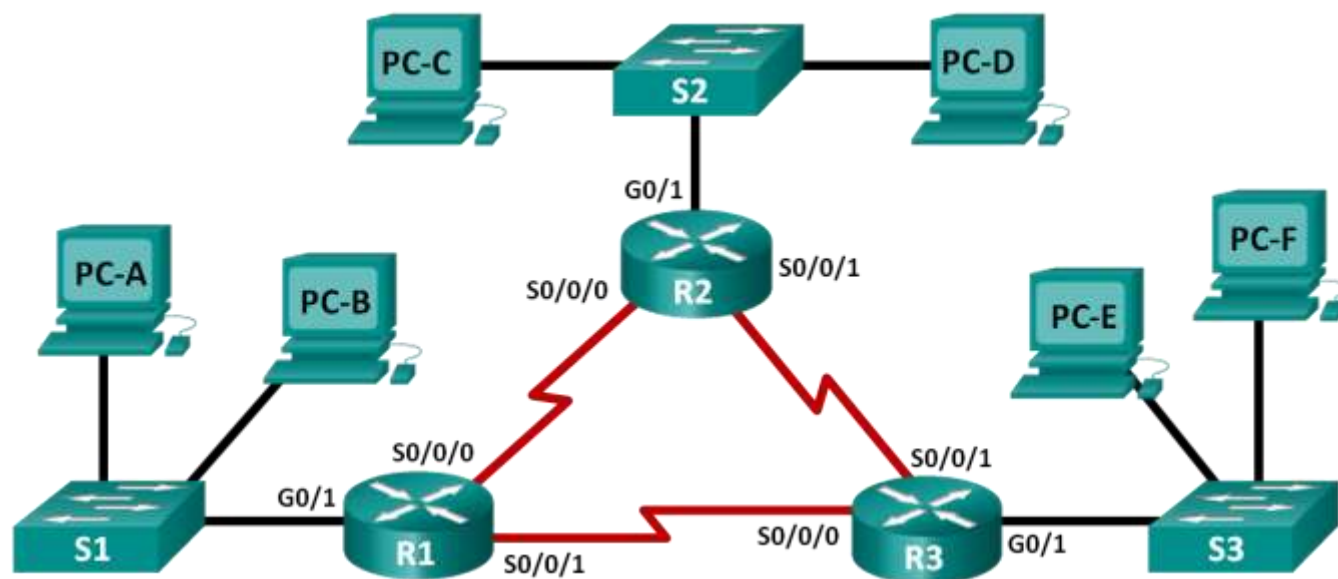
Step 2: Record the subnet information.

Fill in the following table with the subnet information:

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.10.0	192.168.10.1	192.168.10.62	192.168.10.63
1	192.168.10.64	192.168.10.65	192.168.10.126	192.168.10.127
2	192.168.10.128	192.168.10.129	192.168.10.190	192.168.10.191
3	192.168.10.192	192.168.10.193	192.168.10.254	192.168.10.255
4				
5				
6				
7				

Part 3: Network Topology C

The topology has changed again with a new LAN added to R2 and a redundant link between R1 and R3. Use the 192.168.10.0/24 network address to provide addresses to the network devices. Also provide an IP address scheme that will accommodate these additional devices. For this topology, assign a subnet to each network.



Step 1: Determine the number of subnets in Network Topology C.

- How many subnets are there? 6
- How many bits should you borrow to create the required number of subnets? 3
- How many usable host addresses per subnet are in this addressing scheme? 30
- What is the new subnet mask in dotted decimal format? 255.255.255.224
- How many subnets are available for future use? 2

Step 2: Record the subnet information.

Fill in the following table with the subnet information:

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.10.0	192.168.10.1	192.168.10.30	192.168.10.31
1	192.168.10.32	192.168.10.33	192.168.10.62	192.168.10.63
2	192.168.10.64	192.168.10.65	192.168.10.94	192.168.10.95
3	192.168.10.96	192.168.10.97	192.168.10.126	192.168.10.127
4	192.168.10.128	192.168.10.129	192.168.10.158	192.168.10.159
5	192.168.10.160	192.168.10.161	192.168.10.190	192.168.10.191
6	192.168.10.192	192.168.10.193	192.168.10.222	192.168.10.223
7	192.168.10.224	192.168.10.225	192.168.10.254	192.168.10.255
8				
9				
10				

Step 3: Assign addresses to network devices in the subnets.

- a. Fill in the following table with IP addresses and subnet masks for the router interfaces:

Instructor Note: These are suggested IP addresses based on using the first 6 subnets from the table above as assigned to each segment.

Device	Interface	IP Address	Subnet Mask
R1	GigabitEthernet 0/1	192.168.10.1	255.255.255.224
	Serial 0/0/0	192.168.10.33	255.255.255.224
	Serial 0/0/1	192.168.10.65	255.255.255.224
R2	GigabitEthernet 0/1	192.168.10.97	255.255.255.224
	Serial 0/0/0	192.168.10.34	255.255.255.224
	Serial 0/0/1	192.168.10.129	255.255.255.224
R3	GigabitEthernet 0/1	192.168.10.161	255.255.255.224
	Serial 0/0/0	192.168.10.66	255.255.255.224
	Serial 0/0/1	192.168.10.130	255.255.255.224

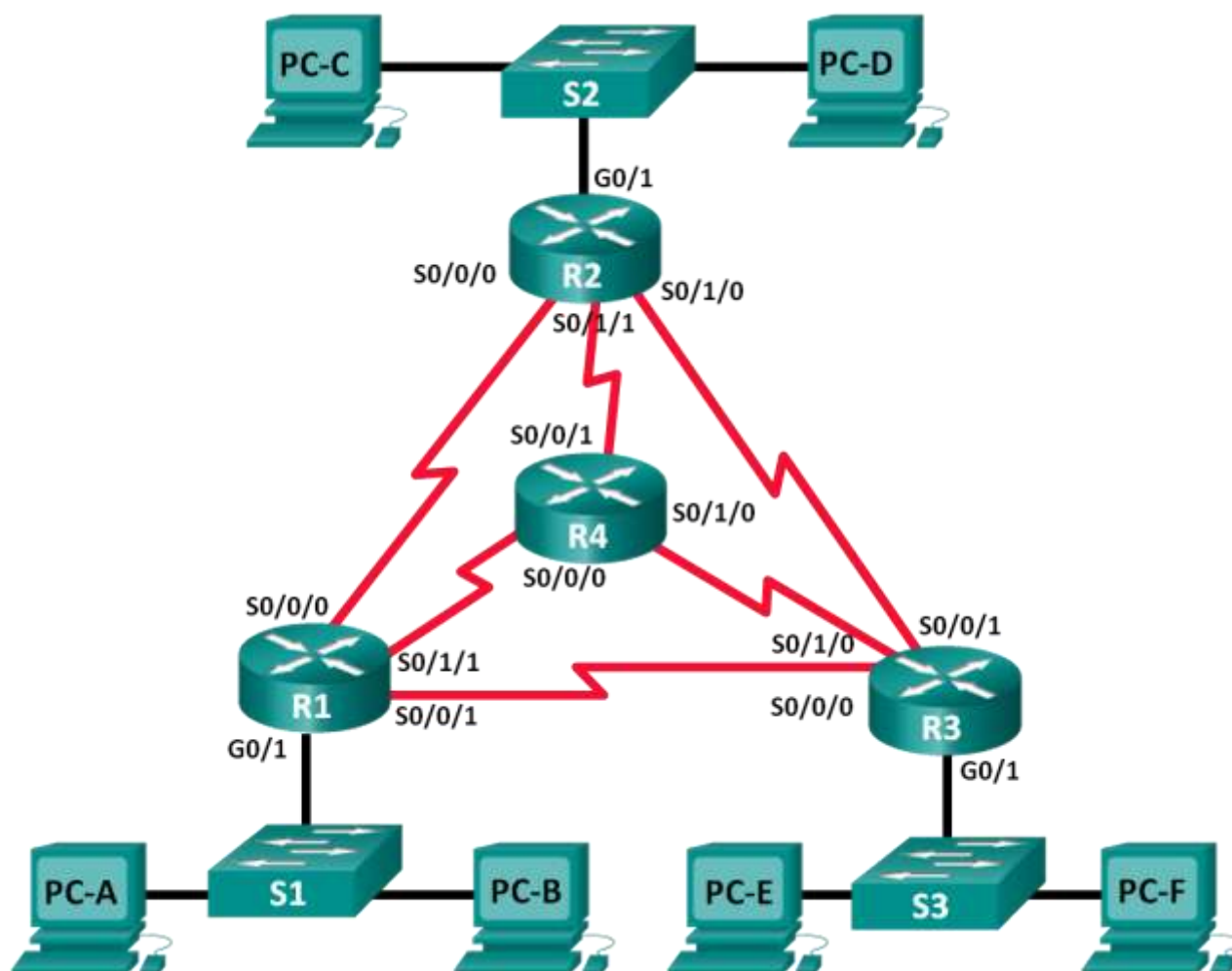
- b. Fill in the following table with the IP addresses and subnet masks for devices in the LAN as displayed in topology.

Instructor Note: These are suggested IP addresses based on using the first 6 subnets from the table above as assigned to each segment.

Device	Interface	IP Address	Subnet Mask	Default Gateway
PC-A	NIC	192.168.10.30	255.255.255.224	192.168.10.1
PC-B	NIC	192.168.10.29	255.255.255.224	192.168.10.1
S1	VLAN 1	192.168.10.2	255.255.255.224	192.168.10.1
PC-C	NIC	192.168.10.126	255.255.255.224	192.168.10.97
PC-D	NIC	192.168.10.125	255.255.255.224	192.168.10.97
S2	VLAN 1	192.168.10.98	255.255.255.224	192.168.10.97
PC-E	NIC	192.168.10.190	255.255.255.224	192.168.10.161
PC-F	NIC	192.168.10.189	255.255.255.224	192.168.10.161
S3	VLAN 1	192.168.10.162	255.255.255.224	192.168.10.161

Part 4: Network Topology D

The network was modified to accommodate changes in the organization. The 192.168.10.0/24 network address is used to provide the addresses in the network.



Step 1: Determine the number of subnets in Network Topology D.

- How many subnets are there? 9
- How many bits should you borrow to create the required number of subnets? 4
- How many usable host addresses per subnet are in this addressing scheme? 14
- What is the new subnet mask in dotted decimal format? 255.255.255.240
- How many subnets are available for future use? 7

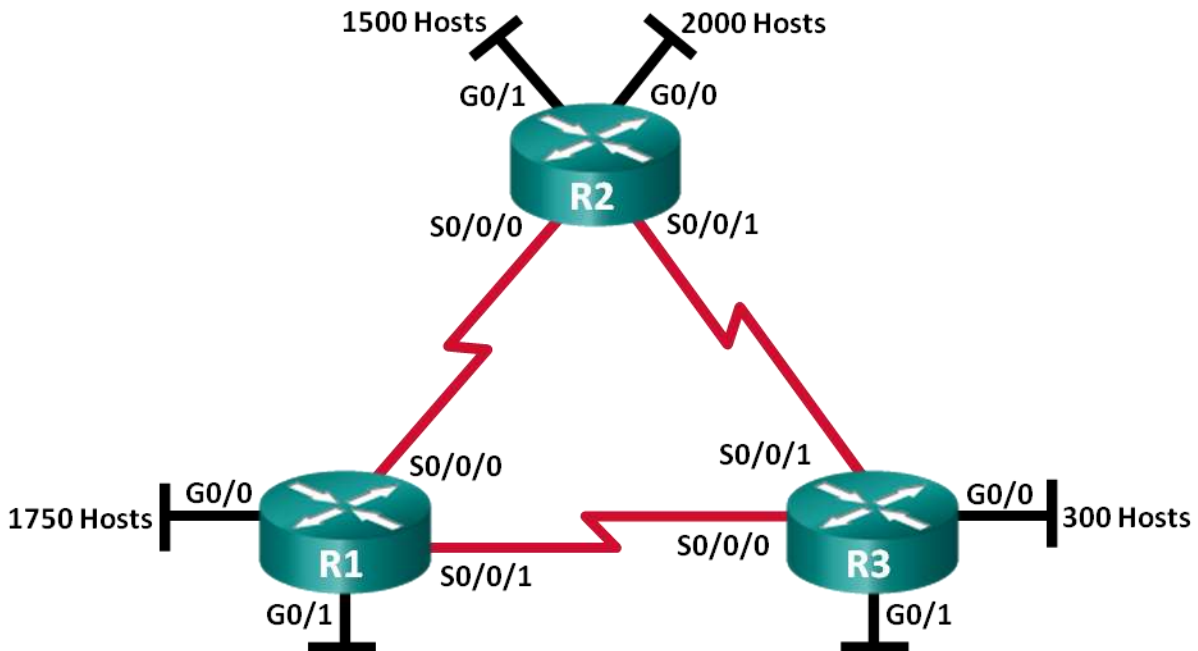
Step 2: Record the subnet information.

Fill in the following table with the subnet information.

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	192.168.10.0	192.168.10.1	192.168.10.14	192.168.10.15
1	192.168.10.16	192.168.10.17	192.168.10.30	192.168.10.31
2	192.168.10.32	192.168.10.33	192.168.10.46	192.168.10.47
3	192.168.10.48	192.168.10.49	192.168.10.62	192.168.10.63
4	192.168.10.64	192.168.10.65	192.168.10.78	192.168.10.79
5	192.168.10.80	192.168.10.81	192.168.10.94	192.168.10.95
6	192.168.10.96	192.168.10.97	192.168.10.110	192.168.10.111
7	192.168.10.112	192.168.10.111	192.168.10.126	192.168.10.127
8	192.168.10.128	192.168.10.129	192.168.10.142	192.168.10.143
9	192.168.10.144	192.168.10.145	192.168.10.158	192.168.10.159
10	192.168.10.160	192.168.10.161	192.168.10.174	192.168.10.175
11	192.168.10.176	192.168.10.177	192.168.10.190	192.168.10.191
12	192.168.10.192	192.168.10.193	192.168.10.206	192.168.10.207
13	192.168.10.208	192.168.10.209	192.168.10.222	192.168.10.223
14	192.168.10.224	192.168.10.225	192.168.10.238	192.168.10.239
15	192.168.10.240	192.168.10.241	192.168.10.254	192.168.10.255
16				
17				

Part 5: Network Topology E

The organization has a network address of 172.16.128.0/17 to be divided as illustrated in the following topology. You must choose an addressing scheme that can accommodate the number of networks and hosts in the topology.



Step 1: Determine the number of subnets in Network Topology E.

- How many subnets are there? 9
- How many bits should you borrow to create the required number of subnets? 4
- How many usable host addresses per subnet are in this addressing scheme? 2046
- What is the new subnet mask in dotted decimal format? 255.255.248.0
- How many subnets are available for future use? 7

Step 2: Record the subnet information.

Fill in the following table with the subnet information:

Subnet Number	Subnet Address	First Usable Host Address	Last Usable Host Address	Broadcast Address
0	172.16.128.0	172.16.128.1	172.16.135.254	172.16.135.255
1	172.16.136.0	172.16.136.1	172.16.143.254	172.16.143.255
2	172.16.144.0	172.16.144.1	172.16.151.254	172.16.151.255
3	172.16.152.0	172.16.152.1	172.16.159.254	172.16.159.255
4	172.16.160.0	172.16.160.1	172.16.167.254	172.16.167.255
5	172.16.168.0	172.16.168.1	172.16.175.254	172.16.175.255
6	172.16.176.0	172.16.176.1	172.16.183.254	172.16.183.255
7	172.16.184.0	172.16.184.1	172.16.191.254	172.16.191.255
8	172.16.192.0	172.16.192.1	172.16.199.254	172.16.199.255
9	172.16.200.0	172.16.200.1	172.16.207.254	172.16.207.255
10	172.16.208.0	172.16.208.1	172.16.215.254	172.16.215.255
11	172.16.216.0	172.16.216.1	172.16.223.254	172.16.223.255
12	172.16.224.0	172.16.224.1	172.16.231.254	172.16.231.255
13	172.16.232.0	172.16.232.1	172.16.239.254	172.16.239.255
14	172.16.240.0	172.16.240.1	172.16.247.254	172.16.247.255
15	172.16.248.0	172.16.248.1	172.16.255.254	172.16.255.255
16				
17				

Step 3: Assign addresses to network devices in the subnets.

- a. Fill in the following table with IP addresses and subnet masks for the router interfaces:

Instructor Note: These are suggested IP addresses based on using the first 9 subnets from the table above as assigned to each segment.

Device	Interface	IP Address	Subnet Mask
R1	GigabitEthernet 0/0	172.16.128.1	255.255.248.0
	GigabitEthernet 0/1	172.16.136.1	255.255.248.0
	Serial 0/0/0	172.16.144.1	255.255.248.0
	Serial 0/0/1	172.16.152.1	255.255.248.0
R2	GigabitEthernet 0/0	172.16.160.1	255.255.248.0
	GigabitEthernet 0/1	172.16.168.1	255.255.248.0
	Serial 0/0/0	172.16.144.2	255.255.248.0
	Serial 0/0/1	172.16.176.1	255.255.248.0
R3	GigabitEthernet 0/0	172.16.184.1	255.255.248.0
	GigabitEthernet 0/1	172.16.192.1	255.255.248.0
	Serial 0/0/0	172.16.152.2	255.255.248.0
	Serial 0/0/1	172.16.176.2	255.255.248.0

Reflection

1. What information is needed when determining an appropriate addressing scheme for a network?

Number of networks and hosts are needed when determining an appropriate addressing scheme for a network.

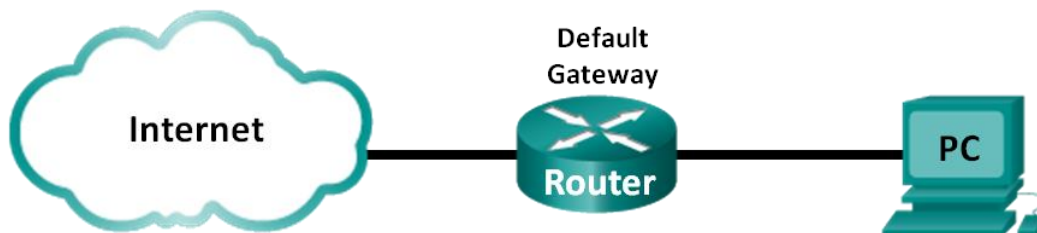
2. After the subnets are assigned, will all the host addresses be utilized in each subnet?

No. For the WAN serial links, only two addresses will be utilized. For the subnets with host PCs, all the addresses can be used in each subnet.

Lab - Viewing Host Routing Tables (Instructor Version)

Instructor Note: Red font color or Gray highlights indicate text that appears in the instructor copy only.

Topology



Objectives

Part 1: Access the Host Routing Table

Part 2: Examine IPv4 Host Routing Table Entries

Part 3: Examine IPv6 Host Routing Table Entries

Background / Scenario

To access a resource on a network, your host will determine the route to the destination host using its routing table. The host routing table is similar to that of a router, but is specific to the local host and much less complex. For a packet to reach a local destination, the local host routing table is required. To reach a remote destination, both the local host routing table and the router routing table are required. The **netstat -r** and **route print** commands provide insight into how your local host routes packets to the destination.

In this lab, you will display and examine the information in the host routing table of your PC using the **netstat -r** and **route print** commands. You will determine how packets will be routed by your PC depending on the destination address.

Note: This lab cannot be completed using Netlab. This lab assumes that you have Internet access.

Required Resources

- 1 PC (Windows 7, Vista, or XP with Internet and command prompt access)

Part 1: Access the Host Routing Table

Step 1: Record your PC information.

On your PC, open a command prompt window and type the **ipconfig /all** command to display the following information and record it:

IPv4 Address	Answers will vary. In this example, 192.168.1.11
MAC Address	Answers will vary. In this example, 90:4C:E5:BE:15:63
Default Gateway	Answers will vary. In this example, 192.168.1.1

Step 2: Display the routing tables.

In a command prompt window type the **netstat -r** (or **route print**) command to display the host routing table.

```

C:\Users\user1>netstat -r
=====
Interface List
13...90 4c e5 be 15 63 .....Atheros AR9285 802.11b/g/n WiFi Adapter
1.....Software Loopback Interface 1
25...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
26...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.11     25
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127.255.255.255            255.255.255.255  On-link          127.0.0.1        306
192.168.1.0                 255.255.255.0    On-link          192.168.1.11     281
192.168.1.11               255.255.255.255  On-link          192.168.1.11     281
192.168.1.255              255.255.255.255  On-link          192.168.1.11     281
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.1.11     281
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.1.11     281
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
14    58  ::/0          On-link
1    306  ::1/128       On-link
14    58  2001::/32     On-link
14    306  2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128 On-link
14    306  fe80::/64     On-link
14    306  fe80::1863:3bca:3f57:fef4/128 On-link
1    306  ff00::/8      On-link
14    306  ff00::/8      On-link
=====
Persistent Routes:
None

```

What are the three sections displayed in the output?

The output has three sections: Interface List, IPv4 Route Table, and IPv6 Route Table.

Step 3: Examine the Interface List.

The first section, Interface List, displays the Media Access Control (MAC) addresses and assigned interface number of every network-capable interface on the host.

```

=====
Interface List
13...90 4c e5 be 15 63 .....Atheros AR9285 802.11b/g/n WiFi Adapter
1.....Software Loopback Interface 1
25...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter
12...00 00 00 00 00 00 00 e0 Microsoft 6to4 Adapter
26...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
14...00 00 00 00 00 00 00 e0 Teredo Tunneling Pseudo-Interface
=====

```

The first column is the interface number. The second column is the list of MAC addresses associated with the network-capable interfaces on the hosts. These interfaces can include Ethernet, Wi-Fi and Bluetooth adapters. The third column shows the manufacturer and a description of the interface.

In this example, the first line displays the wireless interface that is connected to the local network.

Note: If you have a PC with an Ethernet interface and a Wireless adapter enabled, both interfaces would be listed in the Interface List.

What is the MAC address of the interface connected to your local network? How does the MAC address compare to the recorded MAC address in Step 1?

Answers will vary. The MAC address in this example is 90:4C:E5:BE:15:63 The MAC address should be the same as recorded in Step 1 using `ipconfig /all`.

The second line is loopback interface. The loopback interface is automatically assigned an IP address of 127.0.0.1 when the Transmission Control Protocol/Internet Protocol (TCP/IP) is running on a host.

The last four lines represent transition technology that allows communication in a mixed environment and includes IPv4 and IPv6.

Part 2: Examine IPv4 Host Routing Table Entries

In Part 2, you will examine the IPv4 host routing table. This table is in the second section as a result of the **netstat -r** output. It lists all the known IPv4 routes, including direct connections, local network, and local default routes.

IPv4 Route Table				
=====				
Active Routes:				
Network	Destination	Netmask	Gateway	Interface Metric
	0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.11 25
	127.0.0.0	255.0.0.0	On-link	127.0.0.1 306
	127.0.0.1	255.255.255.255	On-link	127.0.0.1 306
127.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1 306
	192.168.1.0	255.255.255.0	On-link	192.168.1.11 281
	192.168.1.11	255.255.255.255	On-link	192.168.1.11 281
	192.168.1.255	255.255.255.255	On-link	192.168.1.11 281
	224.0.0.0	240.0.0.0	On-link	127.0.0.1 306
	224.0.0.0	240.0.0.0	On-link	192.168.1.11 281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1 306
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.1.11 281
=====				
Persistent Routes:				
None				

The output is divided in five columns: Network Destination, Netmask, Gateway, Interface, and Metric.

- The Network Destination column lists the reachable network. The Network Destination is used with Netmask to match the destination IP address.
- The Netmask lists the subnet mask that the host uses to determine the network and host portions of the IP address.
- The Gateway column lists the address that the host uses to send the packets to a remote network destination. If a destination is directly connected, the gateway is listed as On-link in the output.
- The Interface column lists the IP address that is configured on the local network adaptor. This is used to forward a packet on the network.
- The Metric column lists the cost of using a route. It is used to calculate the best route to a destination. A preferred route has a lower metric number than other routes listed.

The output displays five different types of active routes:

- The local default route 0.0.0.0 is used when the packet does not match other specified addresses in the routing table. The packet will be sent to the gateway from the PC for further processing. In this example, the packet will be sent to 192.168.1.1 from 192.168.1.11.
- The loopback addresses, 127.0.0.0 – 127.255.255.255, are related to direct connection and provide services to the local host.
- The addresses for the subnet, 192.168.1.0 – 192.168.1.255, are all related to the host and the local network. If the final destination of the packet is in the local network, the packet will exit 192.168.1.11 interface.
 - The local route address 192.168.1.0 represents all devices on the 192.168.1.0/24 network.
 - The address of the local host is 192.168.1.11.
 - The network broadcast address 192.168.1.255 is used to send messages to all the hosts on the local network.
- The special multicast class D addresses 224.0.0.0 are reserved for use through either the loopback interface (127.0.0.1) or the host (192.168.1.11).
- The local broadcast address 255.255.255.255 can be used through either the loopback interface (127.0.0.1) or host (192.168.1.11).

Based on the contents of the IPv4 routing table, if the PC wanted to send a packet to 192.168.1.15, what would it do and where would it send the packet?

The PC would consult the IPv4 Route Table and match the destination IP address with the 192.168.1.0 Network Destination entry to reveal that the host is on the same network (On-link). The PC would then send the packet toward the final destination using its local interface (192.168.1.11).

If the PC wanted to send a packet to a remote host located at 172.16.20.23, what would it do and where would it send the packet?

The PC would consult the IPv4 Route Table and find that there is no exact match for the destination IP address. It would then choose the local default route (network 0.0.0.0, netmask 0.0.0.0) to reveal that it should forward the packet to the 192.168.1.1 gateway address (address of a gateway device such as a router interface on the local network). The PC would then forward the packet to the gateway using its local interface (192.168.1.11). The gateway device will then determine the next path for the packet to take in order to reach the final destination address of 172.16.20.23.

Part 3: Examine IPv6 Host Routing Table Entries

In Part 3, you will examine the IPv6 routing table. This table is in the third section displayed in the **netstat -r** output. It lists all the known IPv6 routes including direct connections, local network and local default routes.

```
IPv6 Route Table
=====
Active Routes:
  If Metric Network Destination      Gateway
  14      58 ::/0                    On-link
  1       306 ::1/128                 On-link
  14      58 2001::/32                 On-link
  14      306 2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128
                                         On-link
  14      306 fe80::/64                 On-link
  14      306 fe80::1863:3bca:3f57:fef4/128
                                         On-link
  1       306 ff00::/8                 On-link
  14      306 ff00::/8                 On-link
=====
Persistent Routes:
None
```

The output of the IPv6 Route Table differs in column headings and format because the IPv6 addresses are 128 bits versus only 32 bits for IPv4 addresses. The IPv6 Route Table section displays four columns:

- The If column lists the interface numbers of the IPv6-enabled network interfaces from the Interface List section of the **netstat -r** command.
- The Metric column lists the cost of each route to a destination. The lower cost is the preferred route, and the metric is used to select between multiple routes with the same prefix.
- The Network Destination column lists the address prefix for the route.
- The Gateway lists the next-hop IPv6 address to reach the destination. On-link is listed as the next-hop address if it is directly connected to the host.

In this example, the figure displays the IPv6 Route Table section generated by the **netstat -r** command to reveal the following network destinations:

- ::/0: This is the IPv6 equivalent of the local default route. The Gateway column provides the link-local address of the default router.
- ::1/128: This is equivalent to the IPv4 loopback address and provides services to the local host.
- 2001::/32: This is the global unicast network prefix.
- 2001:0:9d38:6ab8:1863:3bca:3f57:fef4/128: This is the global unicast IPv6 address of the local computer.
- fe80::/64: This is the local link network route address and represents all computers on the local-link IPv6 network.
- fe80::1863:3bca:3f57:fef4/128: This is the link-local IPv6 address of the local computer.
- ff00::/8: These are special reserved multicast class D addresses equivalent to the IPv4 224.x.x.x addresses.

The host routing table for IPv6 has similar information as the IPv4 routing table. What is the local default route for IPv4 and what is it for IPv6?

IPv4 is 0.0.0.0 0.0.0.0 (quad zero) and IPv6 is ::/0.

What is the loopback address and subnet mask for IPv4? What is the loopback IP address for IPv6?

IPv4 is 127.0.0.1 0.0.0.0 0.0.0.0 and IPv6 is ::1/128.

How many IPv6 addresses have been assigned to this PC?

Lab - Viewing Host Routing Tables

There are two IP addresses. The link-local address and the global unicast address.

How many broadcast addresses does the IPv6 routing table contain?

None, IPv6 does not use broadcast addresses.

Reflection

1. How is the number of bits for the network indicated for IPv4. How is it done for IPv6?

IPv4 uses a 32-bit dotted decimal subnet mask in the form of a.b.c.d. IPv6 uses a slash number.

2. Why is there both IPv4 and IPv6 information in the host routing tables?

Modern day PCs run both protocols and ISPs frequently assign both IPV4 and IPv6 addresses to support access to servers on the Internet that are running either protocol.