

11.4.3.3: Network Latency Documentation with Ping

Topology Diagram



Learning Objectives

- Use the `ping` command to document network latency.
- Compute various statistics on the output of a `ping` capture.
- Measure delay effects from larger datagrams.

Background

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.

The destination Server Computer must return ECHO replies, otherwise delay cannot be computed. Some computers have this feature disabled through a firewall, and some private networks block transit ECHO datagrams. For this experiment to be interesting, a sufficiently distant destination should be chosen. For example, destinations on the same LAN or within a few hops may return an unrepresentative low latency. With patience, a suitable destination will be found.

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.

Statistical analysis of throughput delay will be performed with the assistance of a spreadsheet application such as Microsoft Excel. Return delay times, measured in milliseconds, will be summarized with through computation of the average latency (mean), noting the latency value at the center of the ordered range of latency points (median), and identification of the most frequently occurring delay (mode). The Appendix contains a chart that can be submitted to the instructor when finished.

Delay will also be measured when the ICMP datagram size is increased.

Scenario

In the topology graphic above, the network cloud represents all of the network devices and cabling between the student computer and the destination Server Computer. It is normally these devices that introduce network latency. Network engineers routinely rely on networks outside of local administration for connectivity to external networks. Monitoring path latency does provide some measure of administrative diligence, which may be used in decision-making when evaluating suitable applications for wide area network (WAN) deployment.

This activity will require five days of testing. On each day, three tests will be performed. Preferably, one test will be made in the early morning, one around mid-day, and one in the evening. The idea is to note and document latency differences that occur during the different periods of the day. When finished there will be a total of 15 sets of this data.

To understand the delay effects from larger datagrams, ICMP datagrams will be sent with increasingly larger datagrams and analyzed.

Task 1: Use the `ping` Command to Document Network Latency.

Step 1: Verify connectivity between Student Computer and destination Server Computer.

To verify connectivity between the Student Computer and destination Server Computer, open a terminal window by clicking on start | run. Enter `cmd`, and then select `OK`. Attempt to ping a suitably distant destination, such as `www.yahoo.com`:

```
C:\> ping -n 1 www.yahoo.com
Pinging www.yahoo-ht3.akadns.net [209.191.93.52] with 32 bytes of data:
Reply from 209.191.93.52: bytes=32 time=304ms TTL=52
Ping statistics for 209.191.93.5:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 304ms, Maximum = 304ms , Average = 304 ms
```

Use the `ping /?` command to answer the following questions:

What is the purpose of the `-n` option and argument 1?

What option and argument would change the default size to 100 bytes? _____

Decide on a destination Server Computer, and write down the name: _____

Use the `ping` command to verify connectivity with the destination, and write down the results:

Packets sent	Packets Received	Packets Lost
--------------	------------------	--------------

If there are lost packets, use another destination and retest.

Step 2: Perform a delay test.

Write down the command that will send 100 ECHO requests to the destination:

Use the ping command to send 100 ECHO requests to your destination. When finished, copy the replies into Notepad. Notepad can be opened by clicking on Start | Programs | Accessories, and select Notepad. Save the file using the name format *day-sample#.txt*, where: *day* = the day the test was performed (1-5), and *sample#* = the sample period (1-3).

Alternately, output can be redirected to a file by appending `> day-sample#.txt` to the end of the `ping` command. NOTE: the terminal will remain blank until the command has finished.

Task 2: Compute Various Statistics on the Output of a ping Capture.

Step 1: Bring the text file into the Excel Spreadsheet Application.

If not already opened, start Microsoft Excel. Select menu options File | Open. Use Browse to move to the directory that holds the text file. Highlight the filename and select Open. To format a text file for use within Excel, insure all numeric values are separated from text characters. In the Text Import Wizard, Step 1, select Fixed Width. In Step 2, follow instructions in the window to separate numeric values from text values. Refer to Figure 1.

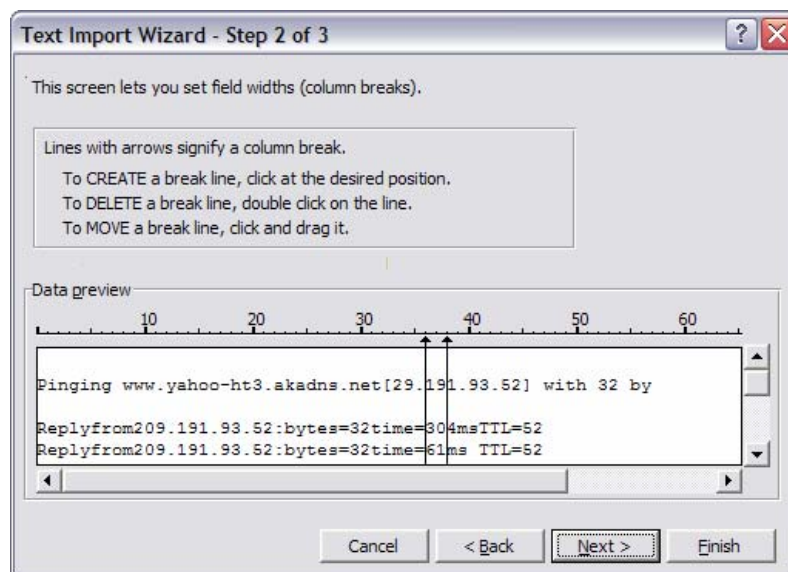


Figure 1. Excel Text Import Wizard.

Step 2. Compute mean, median and mode delay values.

When input formatting is satisfactory, select **Finish**. If the spreadsheet has numbers in different fields, manually fix the numbers. After the spreadsheet has been opened, format the columns so they are more readable. When complete, you should have a spreadsheet that looks similar to Figure 2.

	A	B	C	E	G	I
1				Bytes	Delay (ms)	TTL
2	Reply from	209.191.93.52:		32	304	52
3	Reply from	209.191.93.52:		32	61	52
4	Reply from	209.191.93.52:		32	56	52
5	Reply from	209.191.93.52:		32	54	52
6	Reply from	209.191.93.52:		32	65	52
7	Reply from	209.191.93.52:		32	55	52

Figure 2. Partial spreadsheet correctly formatted.

Record the number of dropped packets in your chart, column Dropped Packets. Dropped packets will have a consistently large delay value.

Finally, the delay values must be ordered (sorted) when computing the median and mode values. This is accomplished with the Data | Sort menu options. Highlight all of the data fields. Figure 3 shows a partial spreadsheet highlighted and the Data | Sort menu opened. If a header row was highlighted, click on the Header row radio button. Select the column that contains the Delay values, in Figure 3 it is Column G. When finished click OK.

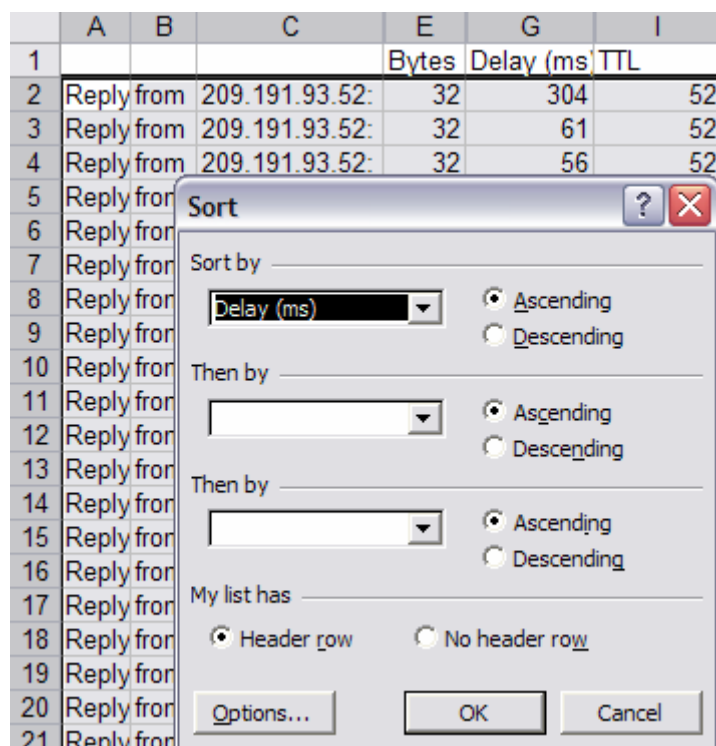


Figure 3. Ordering on the Delay column.

The formula used to compute the mean, or average, delay is the sum of the delays, divided by number of measurements. Using the example above, this would equate to the formula in cell G102:
`=average(G2:G101)`. Perform a visual 'sanity check' to verify your mean value is approximately the value shown. Record this number in your chart, under column Mean.

The formula used to compute the median delay, or the delay value in the center of the ordered range, is similar to the average formula, above. For the median value, the formula in cell G103 would be

=median(G2:G101). Perform a visual 'sanity check' to verify your median value is similar to what is shown midway in the data range. Record this number in your chart, under column Median.

The formula used to compute the modal delay, or the delay value that is the most frequently occurring, is also similar. For the mode value, the formula in cell G104 would be =mode(G2:G101). Perform a visual 'sanity check' to verify your mode value is the most frequently occurring value in the data range. Record this number in your chart, under column Mode.

The new spreadsheet file may be saved or discarded as desired, but the data text file should be retained.

Task 3: Measure Delay Effects from Larger Datagrams.

To determine if larger datagrams affect delay, increasingly larger ECHO requests will be sent to the destination. In this analysis, 20 datagrams will be incremented by 100 bytes per ping request. A spreadsheet will be created with the reply results, and a chart that plots size vs. delay will be produced.

Step 1: Perform a variable sized delay test.

The easiest way to accomplish this task is to use the Windows built-in FOR loop command. The syntax is:

```
FOR /L %variable IN (start,step,end) DO command [command-parameters]
```

The set is a sequence of numbers from start to end, by step amount. So (1,1,5) would generate the sequence 1 2 3 4 5 and (5,-1,1) would generate the sequence (5 4 3 2 1)

In the following command, *destination* is the destination. Issue the command:
FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i *destination*

Copy the output into Notepad, and save the file using the name `variablesizedelay.txt`.

To redirect output to a file, use the redirect append operator, `>>`, as shown below. The normal redirect operator, `>`, will clobber the file each time the ping command is executed and only the last reply will be saved. NOTE: the terminal will remain blank until the command has finished:

```
FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i destination >>  
variablesizedelay.txt
```

The output of one line is shown below. All 20 replies are arranged similarly:

```
C:\> FOR /L %i IN (100,100,2000) DO ping -n 1 -l %i www.yahoo.com

C:\> ping -n 1 -l 100 www.yahoo.com

Pinging www.yahoo-ht3.akadns.net [209.191.93.52] with 100 bytes of data:
Reply from 209.191.93.52: bytes=100 time=383ms TTL=52

Ping statistics for 209.191.93.52:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 383ms, Maximum = 383ms, Average = 383ms
```

Step 2: Bring the text file into the Excel Spreadsheet Application.

Open the new text file in Excel. Refer to Figure 4.

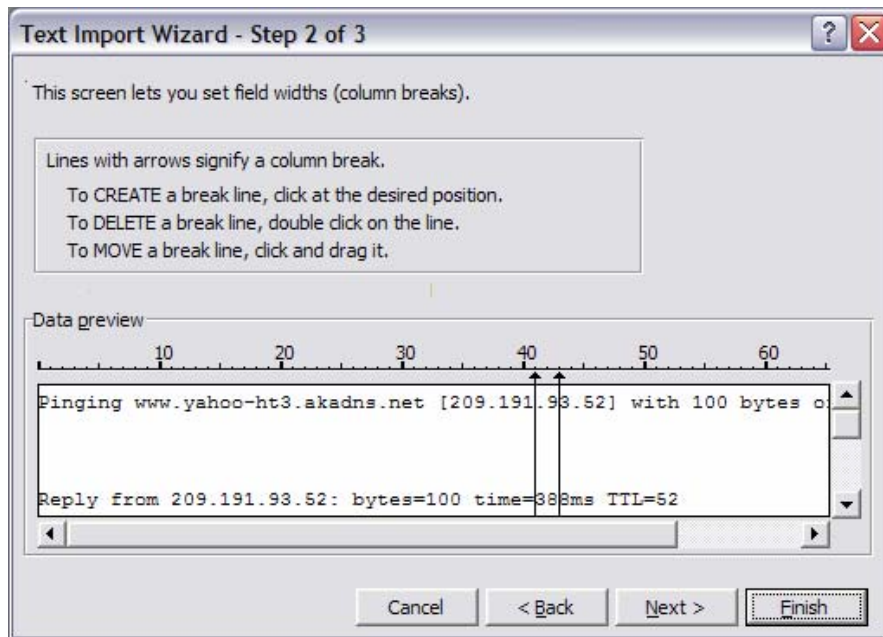


Figure 4. Excel Text Import Wizard.

The difference between this file and the previous file is that the variable size file has much more information than is really needed.

Step 3: Format the spreadsheet.

Clean and organize the spreadsheet data into two columns, Bytes and Delay. When finished, the spreadsheet should look similar to Figure 5.

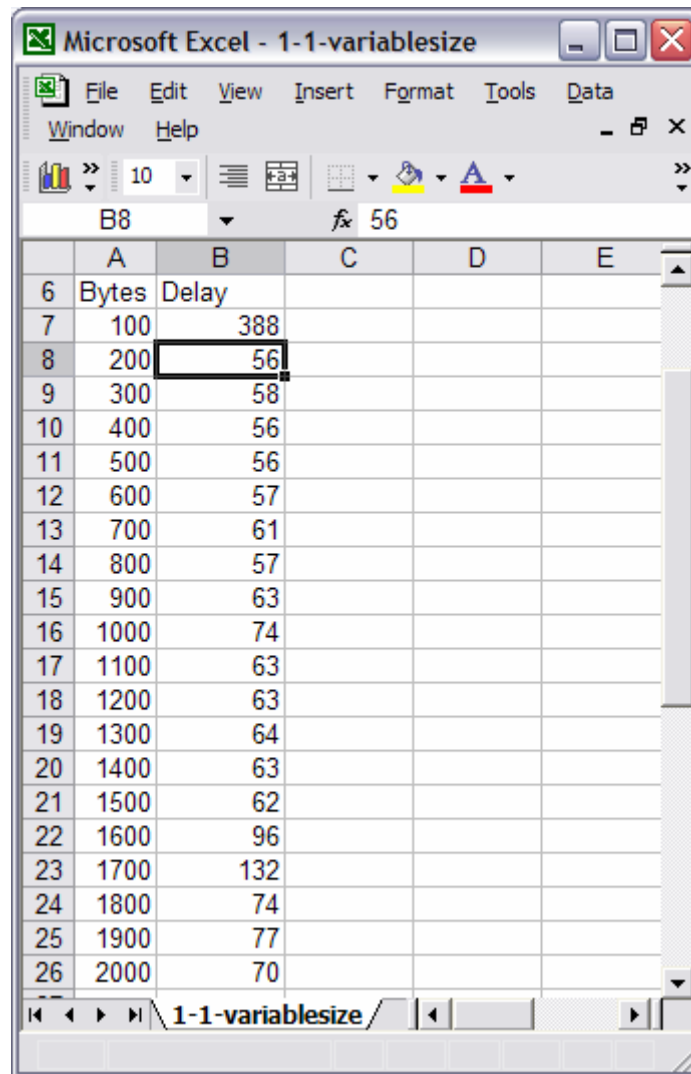


Figure 5. Formatted Spreadsheet.

Step 3: Create a chart of the data.

Highlight the Delay column data. Select menu options Insert | Chart. There are a number of charts that can be used to display delay data, some better than others. While a chart should be clear, there is room for individual creativity. The chart in Figure 6 is a Stacked Line chart.

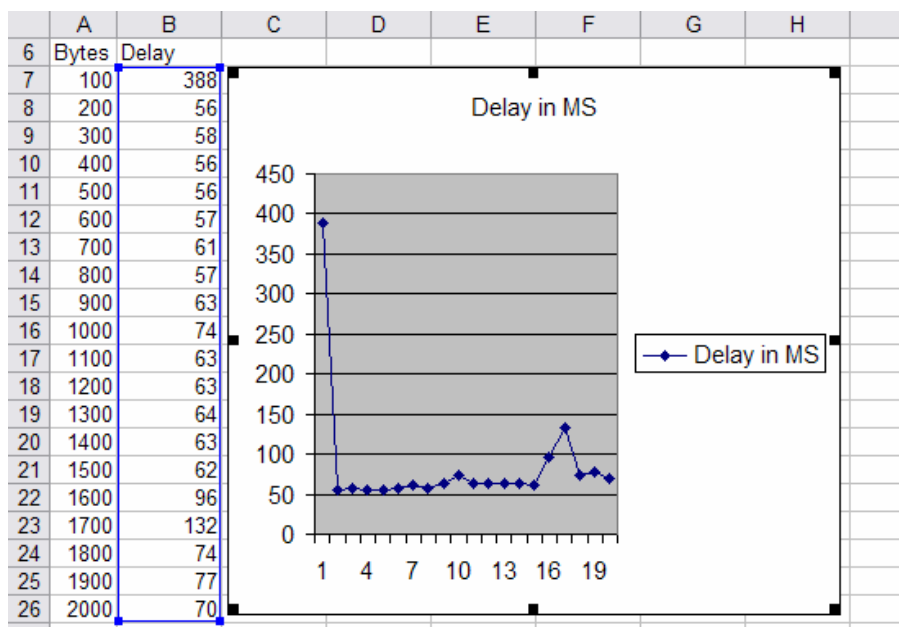


Figure 6. Plot of Delay vs. datagram size.

When finished, save your spreadsheet and chart and submit it to your instructor with the final delay analysis.

Are there any assumptions that can be made regarding delay when larger datagrams are sent across a network?

Task 4: Reflection

The `ping` command can provide important network latency information. Careful delay analysis over successive days and during different periods of the day can alert the network engineer to changes in network performance. For example, network devices may become overwhelmed during certain periods of the day, and network delay will spike. In this case, routine data transfers should be scheduled during off-peak times when delay is less. Also, many users subscribe to peer-to-peer applications such as KaZaA and Napster. When these file-sharing applications are active, valuable bandwidth will be diverted from critical business applications. If delays are caused by events within the organization, network analysis tools can be used to determine the source and corrective action taken. When the source originates from external networks, not under the control of the organization, subscribing with a different or additional Internet service provider (ISP) may prove beneficial.

Task 5: Challenge

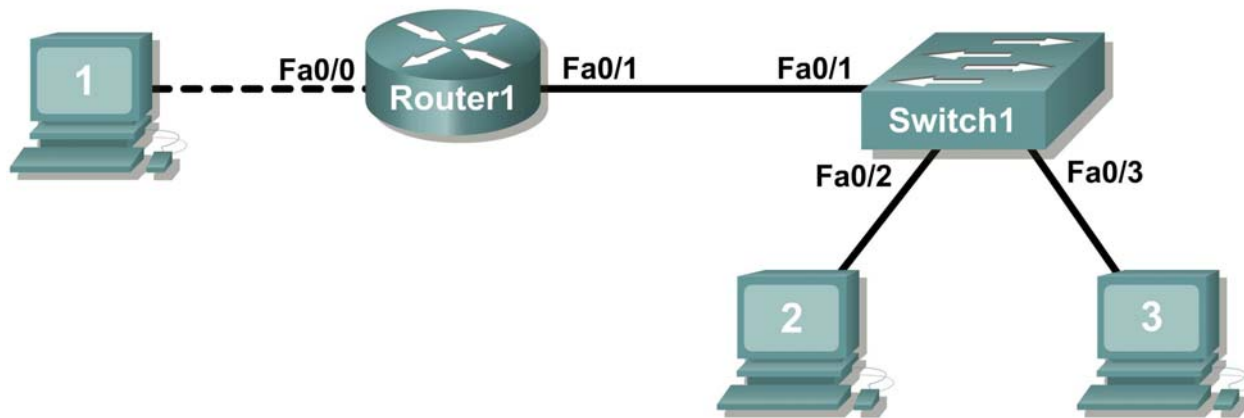
If permitted, download a large file and perform a separate delay test while the file is downloading. Write a one or two paragraph analysis that compares these delay results against a measurement made without the download.

Appendix

NAME: _____		Network Delay Documentation				
Source IP Address: _____		Destination IP Address: _____			TTL: _____	
Statistical Analysis of Network Latency with 32 byte datagrams						
Day (1-5)	Date (mm/dd/yyyy)	Time (hh:mm)	MEAN	MEDIAN	MODE	Dropped Packets
1						
2						
3						
4						
5						

Lab 11.5.1: Basic Cisco Device Configuration

Topology Diagram



Learning Objectives

- Configure Cisco router global configuration settings.
- Configure Cisco router password access.
- Configure Cisco router interfaces.
- Save the router configuration file.
- Configure a Cisco switch.

Background

Hardware	Qty	Description
Cisco Router	1	Part of CCNA Lab bundle.
Cisco Switch	1	Part of CCNA Lab bundle.
*Computer (host)	1	Lab computer.
Console (rollover) cable	1	Connects computer host 1 to Router console port.
UTP Cat 5 crossover cable	1	Connects computer host 1 to Router LAN interface Fa0/0
Straight Through Cable	3	Connects computer hosts to Switch and switch to router

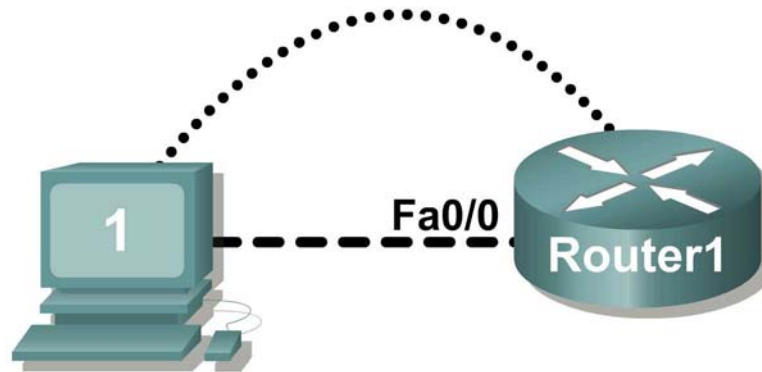
Table 1. Equipment and hardware required for this lab.

Gather the necessary equipment and cables. To configure the lab, make sure the equipment listed in Table 1 is available.

Common configuration tasks include setting the hostname, access passwords, and MOTD banner.

Interface configuration is extremely important. In addition to assigning a Layer 3 IP address, enter a description that describes the destination connection speeds troubleshooting time.

Task 1: Configure Cisco Router Global Configuration Settings.



Straight-through cable



Serial cable



Console (Rollover)



Crossover cable



Figure 1. Lab cabling.

Step 1: Physically connect devices.

Refer to Figure 1. Connect the console or rollover cable to the console port on the router. Connect the other end of the cable to the host computer using a DB-9 or DB-25 adapter to the COM 1 port. Connect the crossover cable between the host computer's network interface card (NIC) and Router interface Fa0/0. Connect a straight-through cable between the Router interface Fa0/1 and any of the switch's interfaces (1-24).

Ensure that power has been applied to the host computer, switch and router.

Step 2: Connect host computer to router through HyperTerminal.

From the Windows taskbar, start the HyperTerminal program by clicking on Start | Programs | Accessories | Communications | HyperTerminal.

Configure HyperTerminal with the proper settings:

Connection Description

Name: **Lab 11_2_11**

Icon: **Personal choice**

Connect to

Connect Using: **COM1** (or appropriate COM port)

COM1 Properties

Bits per second: **9600**
Data bits: **8**
Parity: **None**
Stop bits: **1**
Flow Control: **None**

When the HyperTerminal session window comes up, press the **Enter** key until there is a response from the router.

If the router terminal is in the configuration mode, exit by typing **NO**.

```
Would you like to enter the initial configuration dialog? [yes/no]: no  
  
Press RETURN to get started!  
Router>
```

When in privileged exec command mode, any misspelled or unrecognized commands will attempt to be translated by the router as a domain name. Since there is no domain server configured, there will be a delay while the request times out. This can take between several seconds to several minutes. To terminate the wait, simultaneously hold down the **<CTRL><SHIFT>6** keys then release and press **x**:

```
Router>enabel  
Translating "enabel"...domain server (255.255.255.255) %
```

Briefly hold down the keys <CTRL><SHIFT>6, release and press x

```
Name lookup aborted  
  
Router>
```

From the user exec mode, enter privileged exec mode:

```
Router> enable  
Router#
```

Verify a clean configuration file with the privileged exec command **show running-config**. If a configuration file was previously saved, it will have to be removed. Appendix 1 shows a typical default router's configuration. Depending on router's model and IOS version, your configuration may look slightly different. However, there should be no configured passwords or IP addresses. If your router does not have a default configuration, ask the instructor to remove the configuration.

Step 3: Configure global configuration hostname setting.

What two commands may be used to leave the privileged exec mode? _____

What shortcut command can be used to enter the privileged exec mode? _____

Examine the different configuration modes that can be entered with the command **configure**? Write down the list of configuration modes and description:

From the `privileged exec` mode, enter global configuration mode:

```
Router# configuration terminal  
Router (config) #
```

What three commands may be used to leave the global configuration mode and return to the privileged exec mode?

What shortcut command can be used to enter the global configuration mode? _____

Set the device hostname to `Router1`:

```
router (config) # hostname Router1  
Router1 (config) #
```

How can the hostname be removed?

Step 5: Configure the MOTD banner.

In production networks, banner content may have a significant legal impact on the organization. For example, a friendly "Welcome" message may be interpreted by a court that an attacker has been granted permission to hack into the router. A banner should include information about authorization, penalties for unauthorized access, connection logging, and applicable local laws. The corporate security policy should provide policy on all banner messages.

Create a suitable MOTD banner. Only system administrators of the ABC Company are authorized access, unauthorized access will be prosecuted, and all connection information will be logged.

Examine the different banner modes that can be entered. Write down the list of banner modes and description.

Router1(config)# banner ?

Choose a terminating character that will not be used in the message text. _____

Configure the MOTD banner. The MOTD banner is displayed on all connections before the login prompt. Use the terminating character on a blank line to end the MOTD entry:

```
Router1(config)# banner motd %  
Enter TEXT message. End with the character '%'  
***You are connected to an ABC network device. Access is granted to only  
current ABC company system administrators with prior written approval. ***  
  
*** Unauthorized access is prohibited, and will be prosecuted. ***  
  
*** All connections are continuously logged. ***  
  
%  
Router1(config)#
```

What is the global configuration command to remove the MOTD banner?

Task 2: Configure Cisco router password access.

Access passwords are set for the privileged exec mode and user entry point such as console, aux, and virtual lines. The privileged exec mode password is the most critical password, since it controls access to the configuration mode.

Step 1: Configure the privileged exec password.

Cisco IOS supports two commands that set access to the privileged exec mode. One command, **enable password**, contains weak cryptography and should never be used if the **enable secret** command is available. The **enable secret** command uses a very secure MD5 cryptographic hash algorithm. Cisco says “As far as anyone at Cisco knows, it is impossible to recover an enable secret based on the contents of a configuration file (other than by obvious dictionary attacks).” Password security relies on the password algorithm, and the password. . In production environments, strong passwords should be used at all times. A strong password consists of at least nine characters of upper and lower case letters, numbers, and symbols. In a lab environment, we will use weak passwords.

Set the privileged exec password to **cisco**.

```
Router1(config)# enable secret cisco
Router1(config)#
```

Step 2: Configure the console password.

Set the console access password to **class**. The console password controls console access to the router.

```
Router1(config)# line console 0
Router1(config-line)# password class
Router1(config-line)# login
```

What is the command to remove the console password? _____

Step 3: Configure the virtual line password.

Set the virtual line access password to **class**. The virtual line password controls Telnet access to the router. In early Cisco IOS versions, only five virtual lines could be set, 0 through 4. In newer Cisco IOS versions, the number has been expanded. Unless a telnet password is set, access on that virtual line is blocked.

```
Router1(config-line)# line vty 0 4
Router1(config-line)# password class
Router1(config-line)# login
```

There are three commands that may be used to exit the line configuration mode:

Command	Effect
	Return to the global configuration mode.
	Exit configuration and return to the privileged exec mode.

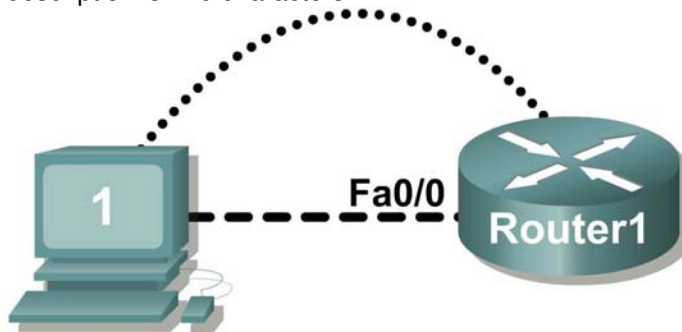
Issue the command **exit**. What is the router prompt? What is the mode?

Router1(config-line)# **exit**

Issue the command **end**. What is the router prompt? What is the mode?

Task 3: Configure Cisco Router Interfaces.

All cabled interfaces should contain documentation about the connection. On newer Cisco IOS versions, the maximum description is 240 characters.



Straight-through cable



Serial cable



Console (Rollover)



Crossover cable



Figure 2. Physical lab topology.

Figure 2 shows a network topology where a host computer is connected to Router1, interface Fa0/0.

Write down your subnet number and mask: _____

The first IP address will be used to configure the host computer LAN. Write down the first IP Address: _____

The last IP address will be used to configure the router fa0/0 interface. Write down the last IP Address: _____

Step 1: Configure the router fa0/0 interface.

Write a short description for the connections on Router1:

Fa0/0 ->

Apply the description on the router interface with the interface configuration command, **description**:

```
Router1(config)# interface fa0/0
Router1(config-if)# description Connection to Host1 with crossover cable
Router1(config-if)# ip address address mask
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Look for the interface to become active:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/0, changed state to up
```

Step 2: Configure the router Fa0/1 interface.

Write a short description for the connections on Router1:

Fa0/1 ->

Apply the description on the router interface with the interface configuration command, **description**:

```
Router1(config)# interface fa0/1
Router1(config-if)# description Connection to switch with straight-through
cable
Router1(config-if)# ip address address mask
Router1(config-if)# no shutdown
Router1(config-if)# end
Router1#
```

Look for the interface to become active:

```
*Mar 24 19:58:59.602: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
```

Step 3: Configure the host computer.

Configure the host computer for LAN connectivity. Recall that the LAN configuration window is accessed through Start | Control Panel | Network Connections. Right-click on the LAN icon, and select Properties. Highlight the Internet Protocol field, and select Properties. Fill in the following fields:

IP Address: The first host address _____
Subnet Mask: The subnet mask _____
Default Gateway: Router's IP Address _____

Click OK, and then Close. Open a terminal window, and verify network settings with the **ipconfig** command.

Step 4: Verify network connectivity.

Use the **ping** command to verify network connectivity with the router. If ping replies are not successful troubleshoot the connection:

What Cisco IOS command can be used to verify the interface status? _____

What Windows command can be used to verify host computer configuration? _____

What is the correct LAN cable between host1 and Router1? _____

Task 4: Save the Router Configuration File.

Cisco IOS refers to RAM configuration storage as running-configuration, and NVRAM configuration storage as startup-configuration. For configurations to survive rebooting or power restarts, the RAM configuration must be copied into non-volatile RAM (NVRAM). This does not occur automatically, NVRAM must be manually updated after any changes are made.

Step 1: Compare router RAM and NVRAM configurations.

Use the Cisco IOS **show** command to view RAM and NVRAM configurations. The configuration is displayed one screen at a time. A line containing “ -- more -- ” indicates that there is additional information to display. The following list describes acceptable key responses:

Key	Description
<SPACE>	Display the next page.
<RETURN>	Display the next line.
Q	Quit
<CTRL> c	Quit

Write down one possible shortcut command that will display the contents of NVRAM.

Display the contents of NVRAM. If the output of NVRAM is missing, it is because there is no saved configuration.:

```
Router1# show startup-config
 startup-config is not present
Router1#
```

Display the contents of RAM.

```
Router1#show running-config
```

Use the output to answer the following questions:

How large is the configuration file? _____

What is the enable secret password? _____

Does your MOTD banner contain the information you entered earlier? _____

Do your interface descriptions contain the information you entered earlier? _____

Write down one possible shortcut command that will display the contents of RAM. _____

Step 2: Save RAM configuration to NVRAM.

For a configuration to be used the next time the router is powered on or reloaded, it must be manually saved in NVRAM. Save the RAM configuration to NVRAM:

```
Router1# copy running-config startup-config
Destination filename [startup-config]? <ENTER>
Building configuration...
[OK]
```

Router1#

Write down one possible shortcut command that will copy the RAM configuration to NVRAM.

Review the contents of NVRAM, and verify that the configuration is the same as the configuration in RAM.

Task 5: Configure a Cisco Switch.

Cisco IOS switch configuration is (thankfully) similar to configuring a Cisco IOS router. The benefit of learning IOS commands is that they are similar to many different devices and IOS versions.

Step 1: Connect the host to the switch.

Move the console, or rollover, cable to the console port on the switch. Ensure power has been applied to the switch. In Hyperterminal, press Enter until the switch responds.

Step 2: Configure global configuration hostname setting.

Appendix 2 shows a typical default switch configuration. Depending on router model and IOS version, your configuration may look slightly different. However, there should be no configured passwords. If your router does not have a default configuration, ask the instructor to remove the configuration.

From the user exec mode, enter global configuration mode:

```
Switch> en  
Switch# config t  
Switch(config)#
```

Set the device hostname to Switch1.

```
Switch(config)# hostname Switch1  
Switch1(config)#
```

Step 3: Configure the MOTD banner.

Create a suitable MOTD banner. Only system administrators of the ABC company are authorized access, unauthorized access will be prosecuted, and all connection information will be logged.

Configure the MOTD banner. The MOTD banner is displayed on all connections before the login prompt. Use the terminating character on a blank line to end the MOTD entry. For assistance, review the similar step for configuring a router MOTD banner.

```
Switch1(config)# banner motd %
```

Step 4: Configure the privileged exec password.

Set the privileged exec password to **cisco**.

```
Switch1(config)# enable secret cisco  
Switch1(config)#
```

Step 5: Configure the console password.

Set the console access password to **class**.

```
Switch1(config)# line console 0  
Switch1(config-line)# password class  
Switch1(config-line)# login
```

Step 6: Configure the virtual line password.

Set the virtual line access password to `class`. There are 16 virtual lines that can be configured on a Cisco IOS switch, 0 through 15.

```
Switch1(config-line)# line vty 0 15  
Switch1(config-line)# password class  
Switch1(config-line)# login
```

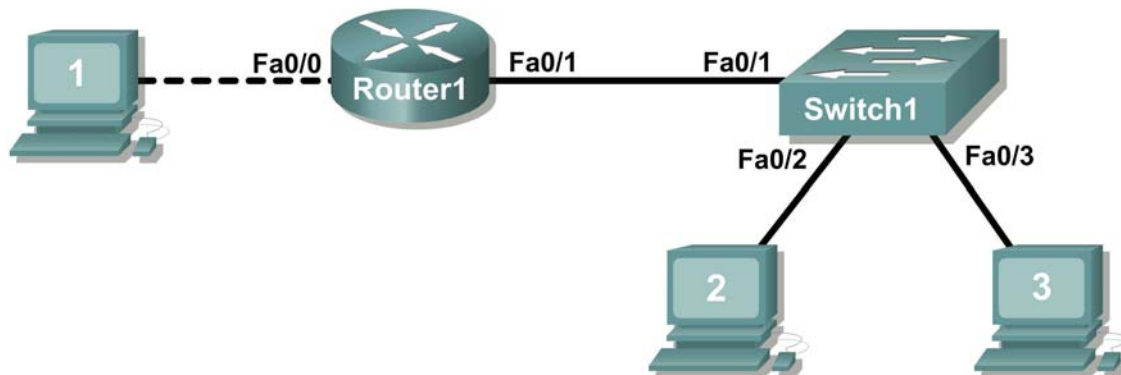


Figure 3. Network topology.

Step 7: Configure the interface description.

Figure 3 shows a network topology where Router1 is connected to Switch1, interface Fa0/1. Switch1 interface Fa0/2 is connected to host computer 2, and interface Fa0/3 is connected to host computer 3.

Write a short description for the connections on Switch1:

Router1 Interface	Description
Fa0/1	
Fa0/2	
Fa0/3	

Apply the descriptions on the switch interface with the interface configuration command, **description**:

```
Switch1(config)# interface fa0/1
Switch1(config-if)# description Connection to Router1
Switch1(config)# interface fa0/2
Switch1(config-if)# description Connection to host computer 2
Switch1(config)# interface fa0/3
Switch1(config-if)# description Connection to host computer 3
Switch1(config-if)# end
Switch1#
```

Step 7: Save RAM configuration to NVRAM.

For a configuration to be used the next time the switch is powered on or reloaded, it must be manually saved in NVRAM. Save the RAM configuration to NVRAM:

```
Switch1# copy run start
Destination filename [startup-config]? <ENTER>
Building configuration...
[OK]
Switch1#
```

Review the contents of NVRAM, and verify that the configuration is the same as the configuration in RAM.

Task 6: Reflection

The more you practice the commands, the faster you will become in configuring a Cisco IOS router and switch. It is perfectly acceptable to use notes at first to help configure a device, but a professional network engineer does not need a 'cheat sheet' to perform common configuration tasks. The following table lists commands covered in this lab:

Purpose	Command
Enter the global configuration mode.	configure terminal Example: Router> enable Router# configure terminal Router(config)#
Specify the name for the router.	hostname name Example: Router(config)# hostname Router1 Router(config)#
Specify an encrypted password to prevent unauthorized access to the privileged exec mode.	enable secret password Example: Router(config)# enable secret cisco Router(config)#

Specify a password to prevent unauthorized access to the console.	<pre>password password login Example: Router(config)# line con 0 Router(config-line)# password class Router(config-line)# login Router(config)#</pre>
Specify a password to prevent unauthorized telnet access. Router vty lines: 0 4 Switch vty lines: 0 15	<pre>password password login Example: Router(config)# line vty 0 4 Router(config-line)# password class Router(config-line)# login Router(config-line)#</pre>
Configure the MOTD banner.	<pre>Banner motd % Example: Router(config)# banner motd % Router(config)#</pre>
Configure an interface. Router- interface is OFF by default Switch- interface is ON by default	<pre>Example: Router(config)# interface fa0/0 Router(config-if)# description description Router(config-if)# ip address address mask Router(config-if)# no shutdown Router(config-if)#</pre>
Save the configuration to NVRAM.	<pre>copy running-config startup-config Example: Router# copy running-config startup-config Router#</pre>

Task 7: Challenge

It is often necessary, and always handy, to save the configuration file to an off-line text file. One way to save the configuration file is to use HyperTerminal Transfer menu option Capture.

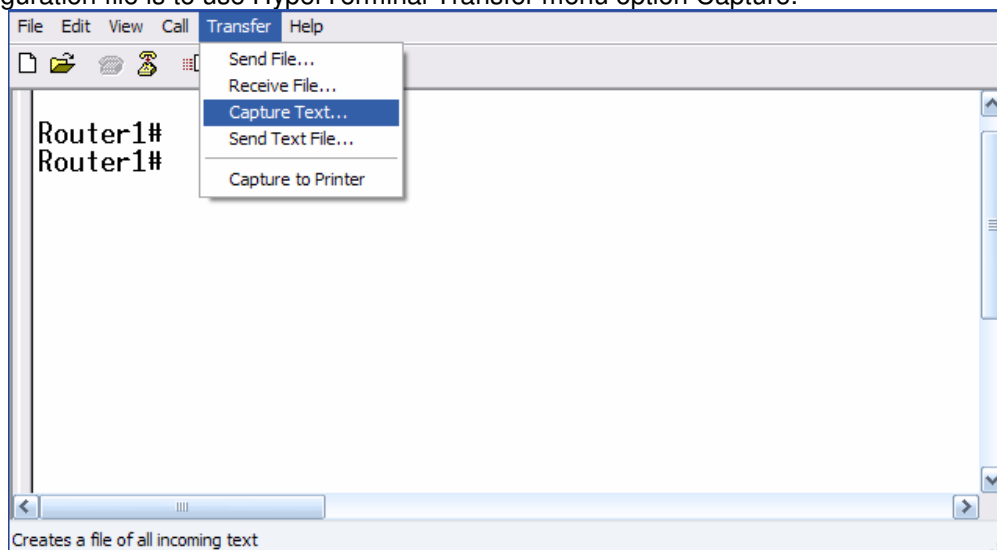


Figure 2. Hyperterminal Capture menu.

Refer to Figure 2. All communication between the host computer and router are saved to a file. The file can be edited, and saved. The file can also be edited, copied, and pasted into a router:

To start a capture, select Hyperterminal menu option Transfer | Capture Text. Enter a path and file name, and select Start.

Issue the privileged exec command **show running-config**, and press the <SPACE> key until all of the configuration has been displayed.

Stop the capture. Select menu option Transfer | Capture Text | Stop.

Open the text file and review the contents. Remove any lines that are not configuration commands, such as the `more` prompt. Manually correct any lines that were scrambled or occupy the same line. After checking the configuration file, highlight the lines and select Notepad menu Edit | Copy. This places the configuration in host computer memory.

To load the configuration file, it is ALWAYS best practice to begin with a clean RAM configuration. Otherwise, stale configuration commands may survive a paste action and have unintended consequences (also known as the Law of Unintended Consequences):

Erase the NVRAM configuration file:

```
Router1# erase start
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm] <ENTER>
[OK]
Erase of nvram: complete
```

Reload the router:

```
Router1# reload
Proceed with reload? [confirm] <ENTER>
```

When the router reboots, enter the global configuration mode:

```
Router> en
Router# config t
Router(config)#
```

Using the mouse, right-click inside the Hyperterminal window and select Paste To Host. The configuration will be loaded, very quickly, to the router. Watch closely for error messages, each message must be investigated and corrected.

Verify the configuration, and save to NVRAM.

Task 6: Cleanup

Before turning off power to the router and switch, remove the NVRAM configuration file from each device with the privileged exec command **erase startup-config**.

Delete any configuration files saved on the host computers.

Unless directed otherwise by the instructor, restore host computer network connectivity, then turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

Appendix 1- default Cisco IOS router configuration

```
Current configuration : 824 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
interface Vlan1
 no ip address
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
end
```

Appendix 2- default Cisco IOS switch configuration

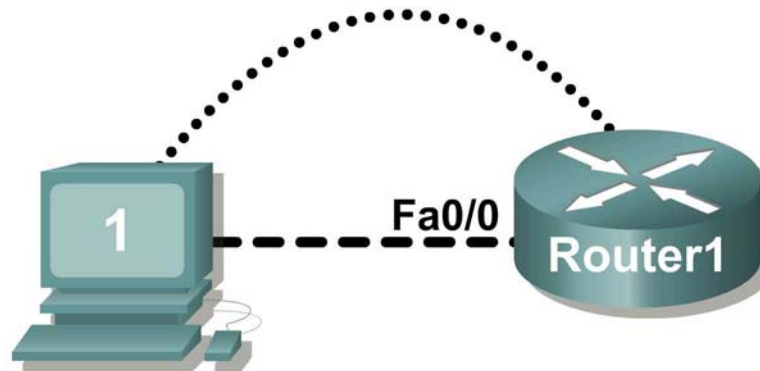
```
Current configuration : 1519 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
!
ip subnet-zero
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
interface FastEthernet0/1
 no ip address
!
interface FastEthernet0/2
 no ip address
!
interface FastEthernet0/3
 no ip address
!
interface FastEthernet0/4
 no ip address
!
interface FastEthernet0/5
 no ip address
!
interface FastEthernet0/6
 no ip address
!
interface FastEthernet0/7
 no ip address
!
interface FastEthernet0/8
 no ip address
!
interface FastEthernet0/9
 no ip address
!
interface FastEthernet0/10
 no ip address
!
interface FastEthernet0/11
 no ip address
!
interface FastEthernet0/12
```

```
no ip address
!  
interface FastEthernet0/13
no ip address
!  
interface FastEthernet0/14
no ip address
!  
interface FastEthernet0/15
no ip address
!  
interface FastEthernet0/16
no ip address
!  
interface FastEthernet0/17
no ip address
!  
interface FastEthernet0/18
no ip address
!  
interface FastEthernet0/19
no ip address
!  
interface FastEthernet0/20
no ip address
!  
interface FastEthernet0/21
no ip address
!  
interface FastEthernet0/22
no ip address
!  
interface FastEthernet0/23
no ip address
!  
interface FastEthernet0/24
no ip address
!  
interface GigabitEthernet0/1
no ip address
!  
interface GigabitEthernet0/2
no ip address
!  
interface Vlan1
no ip address
no ip route-cache
shutdown
!  
ip http server
!  
!  
line con 0
line vty 5 15
!  
!
```

end

Lab 11.5.2: Managing Device Configuration

Topology Diagram



Straight-through cable



Serial cable



Console (Rollover)



Crossover cable



Learning Objectives

- Configure network connectivity.
- Use TFTP to save and restore a Cisco IOS configuration.

Background

Hardware	Qty	Description
Cisco Router	1	Part of CCNA Lab bundle.
Computer (host)	1	Lab computer.
Console (rollover) cable	1	Connects computer host 1 to Router console port.
Crossover cable	1	Connects host1 NIC to Router1 Fa0/1

Table 1. Equipment and hardware required for this lab.

Gather the necessary equipment and cables. To configure the lab, make sure the equipment listed in Table 1 is available.

The host computer will be used as a TFTP server. This lab requires the use of SolarWinds TFTP server software. SolarWinds is a free TFTP application for Windows.

Scenario

In this lab, students will configure common settings on a Cisco Router, save the configuration to a TFTP server, then restore the configuration from a TFTP server.

Given an IP address of 10.250.250.0/24, and 6 bits used for subnets. Use the LAST valid subnet. Host1 should use the FIRST valid host address, and Router1 should use the LAST valid host address:

IP Address: 10.250.250.0		Subnet mask:	
Subnet	First host address	Last host address	Broadcast

Task 1: Configure Network Connectivity.

Step 1: Physically connect devices.

Refer to the Topology Diagram. Connect the console, or rollover, cable to the console port on the router and the other cable end to the host computer with a DB-9 or DB-25 adapter to the COM 1 port. Ensure power has been applied to both the host computer and router.

Step 2: Logically connect devices.

Using the IP address information from the scenario, configure the host1 computer.

Step 3: Connect host computer to router through HyperTerminal.

From the Windows taskbar, start the HyperTerminal program by clicking on Start | Programs | Accessories | Communications | Hyper Terminal.

When the HyperTerminal session window opens, press the **Enter** key until there is a response from the router.

Step 4: Configure Router1.

Configure Router1. Configuration tasks for Router1 include the following:

Task- refer to Appendix 1 for help with commands
Specify Router name- Router1
Specify an encrypted privileged exec password- cisco
Specify a console access password- class
Specify a telnet access password- class
Configure the MOTD banner.
Configure Router1 interface Fa0/0- set the description set the Layer 3 address issue no shutdown

NOTE **DO NOT SAVE THE CONFIGURATION IN NVRAM.

Step 5: Verify connectivity.

Verify connectivity between host1 and Router1:

```
Router1# ping 10.250.250.249
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.250.250.249, timeout is 2 seconds:

.!!!!

Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms

```
Router1#
```

Task 2: Use TFTP to Save and Restore a Cisco IOS Configuration.

Step 1: Install SolarWinds TFTP application.

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

Step 2: Start TFTP server.

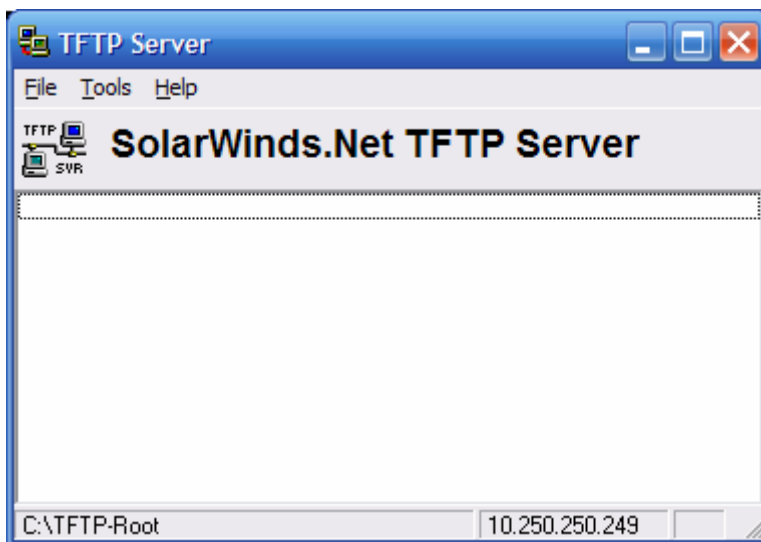


Figure 2. TFTP Server window.

Start the TFTP server by selecting Start | Programs | SolarWinds Free Tools | TFTP Server. Figure 2 shows an active TFTP Server window.

Step 3: Configure the TFTP server.

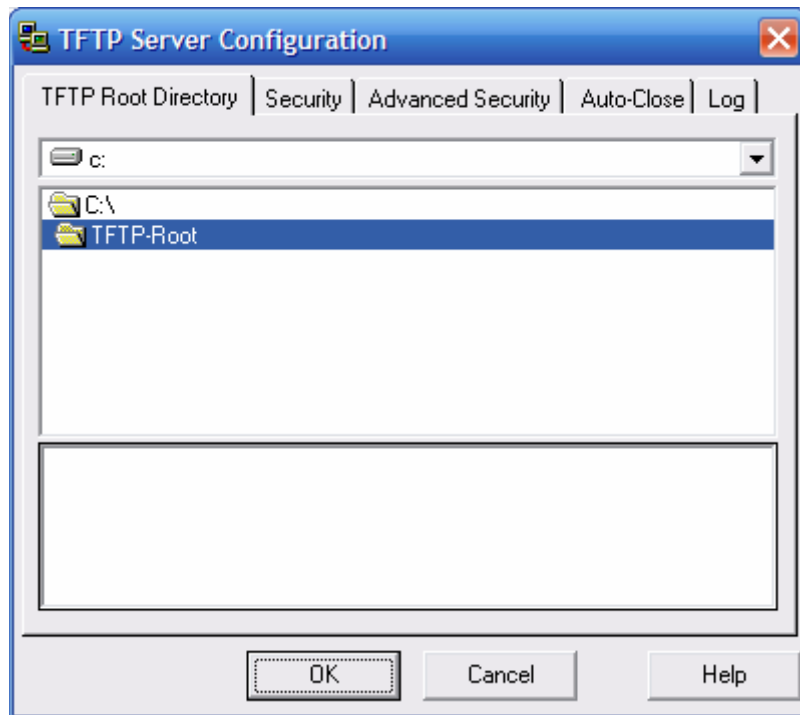


Figure 3. TFTP Server window.

To configure TFTP server, select menu option File | configure. Refer to Figure 3. Verify the following settings:

Setting	Value
TFTP Root Directory:	TFTP-Root
Security	Transmit and Receive Files
Advanced Security	10.250.250.250 To 10.250.250.250
Auto-Close	Never
Log	Enable Log Requests to the Following File. Leave the default file.

When finished, select OK.

Step 4. Save Router1 configuration to TFTP server.

From HyperTerminal, begin a TFTP upload to the TFTP server:

```
Router1#copy running-config tftp:  
Address or name of remote host []? 10.250.250.249  
Destination filename [router1-config]? <ENTER>  
!!  
1081 bytes copied in 2.008 secs (538 bytes/sec)  
Router1#
```

Verify a successful upload transfer. Open Log file c:\Program Files\SolarWinds\Free Tools\TFTP-Server.txt. Contents should be similar to the following:

```
3/25/2007 12:29 :Receiving router1-config from (10.250.250.250)
3/25/2007 12:29 :Received router1-config from (10.250.250.250), 1081 bytes
```

Verify the transferred file. Use Microsoft Word or Wordpad to examine the contents of file c:\TFTP-Root\router1-config. Contents should be similar to the following configuration:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$D02B$AuX05n0HPT239yYRoQ0oE.
!
no aaa new-model
ip cef
!
interface FastEthernet0/0
  description connection to host1
  ip address 10.250.250.250 255.255.255.252
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
interface Serial0/1/0
  no ip address
  shutdown
  no fair-queue
!
interface Serial0/1/1
  no ip address
  shutdown
  clock rate 2000000
!
ip http server
no ip http secure-server
!
control-plane
!
banner motd
*** ABC COMPANY NETWORK DEVICE ****
*** Authorized access only *****
```

```
*** Logging is enabled ****
!  
line con 0  
  password class  
  login  
line aux 0  
line vty 0 4  
  password class  
  login  
!  
scheduler allocate 20000 1000  
End
```

Step 5: Restore Router1 configuration from TFTP server.

Verify that NVRAM is clear, then reboot Router1:

```
Router1# show startup-config  
  startup-config is not present  
Router1# reload  
Proceed with reload? [confirm] <ENTER>
```

Connectivity must be established with the TFTP server. Router1 fa0/0 must be configured with an IP address, and the interface enabled:

```
Router> enable  
Router# conf t  
Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# interface fa0/0  
Router(config-if)# ip address 10.250.250.250 255.255.255.252  
Router(config-if)# no shutdown  
Router(config-if)# exit
```

```
*Mar 25 16:43:03.095: %SYS-5-CONFIG_I: Configured from console by console  
*Mar 25 16:43:04.967: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
FastEthernet0/0, changed state to up
```

Configure the hostname of the router to TEST

```
Router(config-if)#exit  
Router(config)#hostname TEST  
Router(config-if)#end  
TEST#
```

Verify connectivity with the ping command:

```
Router# ping 10.250.250.249  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.250.250.249, timeout is 2 seconds:  
.!!!!  
Success rate is 80 percent(4/5), round-trip min/avg/max = 1/1/1ms  
Router#
```

Download Router1 configuration file from the TFTP server:

```
Router# copy tftp startup-config
Address or name of remote host []? 10.250.250.249
Source filename []? router1-config
Destination filename [startup-config]? <ENTER>
Accessing tftp://10.250.250.249/router1-config...
Loading router1-config from 10.250.250.249 (via FastEthernet0/0): !
[OK - 1081 bytes]

1081 bytes copied in 9.364 secs (115 bytes/sec)
Router1#
*Mar 25 16:55:26.375: %SYS-5-CONFIG_I: Configured from
tftp://10.250.250.249/router1-config by console
Router1#
```

View the configuration in NVRAM to verify an accurate transfer. The configuration should be the same as what was configured in Task 1, Step 4.

Reload the router select no at the prompt that says "Configuration has been modified". The previous the configuration should be restored and the router's hostname should now be Router1.

Task 3: Reflection

TFTP is a fast, efficient way to save and load Cisco IOS configuration files.

Task 4: Challenge

Similar to uploading a configuration file, the IOS can also be stored off-line for future use. To discover the IOS filename, issue the Cisco IOS command **show version**. The filename is highlighted, below:

```
Router1# show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(10b),
RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 19-Jan-07 15:15 by prod_rel_team

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

Router1 uptime is 17 minutes
System returned to ROM by reload at 16:47:54 UTC Sun Mar 25 2007
System image file is "flash:c1841-advipservicesk9-mz.124-10b.bin"
```

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

A summary of U.S. laws governing Cisco cryptographic products may be found at:

<http://www.cisco.com/wvl/export/crypto/tool/stqrg.html>

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

```
Cisco 1841 (revision 6.0) with 174080K/22528K bytes of memory.
Processor board ID FHK110918KJ
2 Serial(sync/async) interfaces
DRAM configuration is 64 bits wide with parity disabled.
191K bytes of NVRAM.
62720K bytes of ATA CompactFlash (Read/Write)
```

Configuration register is 0x2102

Router1#

The commands to upload the IOS are similar to uploading the configuration file:

```
Router1# copy flash tftp
Source filename []? c1841-advipservicesk9-mz.124-10b.bin
Address or name of remote host []? 10.250.250.249
Destination filename [c1841-advipservicesk9-mz.124-10b.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
22063220 bytes copied in 59.564 secs (370412 bytes/sec)
Router1#
```

Task 5: Cleanup

Before turning off power to the router, remove the NVRAM configuration file if it was loaded. Use the privileged exec command **erase startup-config**.

Remove SolarWinds TFTP server from the host computer. Select Start | Control Panel. Open Add or Remove Applications. Select SolarWinds, then Remove. Accept defaults.

Delete any configuration files saved on the host computers.

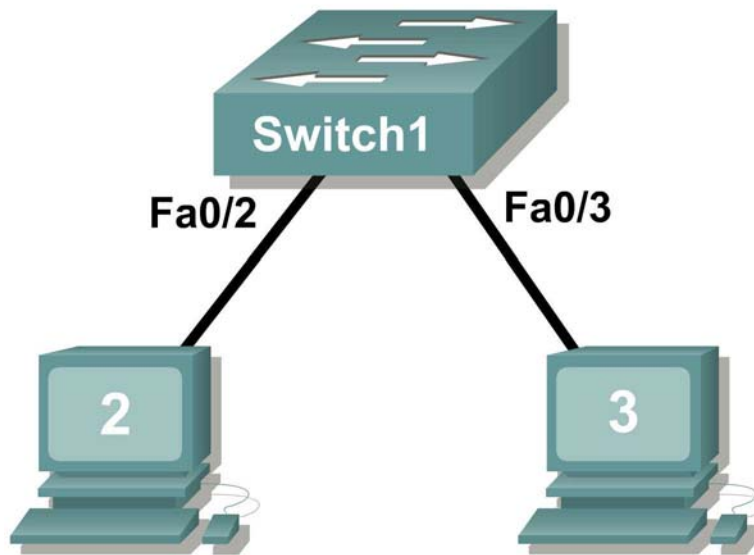
Unless directed otherwise by the instructor, restore host computer network connectivity, then turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

Appendix 1

Purpose	Command
Enter the global configuration mode.	configure terminal Example: Router> enable Router# configure terminal Router(config)#
Specify the name for the router.	hostname name Example: Router(config)# hostname Router1 Router(config)#
Specify an encrypted password to prevent unauthorized access to the privileged exec mode.	enable secret password Example: Router(config)# enable secret cisco Router(config)#
Specify a password to prevent unauthorized access to the console.	password password login Example: Router(config)# line con 0 Router(config-line)# password class Router(config-line)# login Router(config)#
Specify a password to prevent unauthorized telnet access. Router vty lines: 0 4 Switch vty lines: 0 15	password password login Example: Router(config)# line vty 0 4 Router(config-line)# password class Router(config-line)# login Router(config-line)#
Configure the MOTD banner.	Banner motd % Example: Router(config)# banner motd % Router(config)#
Configure an interface. Router- interface is OFF by default Switch- interface is ON by default	Example: Router(config)# interface fa0/0 Router(config-if)# description description Router(config-if)# ip address address mask Router(config-if)# no shutdown Router(config-if)#
Save the configuration to NVRAM.	copy running-config startup-config Example: Router# copy running-config startup-config Router#

Lab 11.5.3: Configure Host Computers for IP Networking

Topology Diagram



Learning Objectives

Upon completion of this lab, you will be able to:

- Design the logical lab topology.
- Configure the physical lab topology.
- Configure the logical LAN topology.
- Verify LAN connectivity.

Background

Hardware	Qty	Description
Cisco Router	1	Part of CCNA Lab bundle
Cisco Switch	1	Part of CCNA Lab bundle
*Computer (Host)	3	Lab computer
CAT-5 or better straight-through UTP cables	3	Connects Router1 and computers Host1 and Host2 to switch1

Table 1. Equipment and Hardware for this Lab

Gather the necessary equipment and cables. To configure the lab, make sure the equipment listed in Table 1 is available.

Scenario

In this lab students will create a small network that requires connecting network devices and configuring host computers for basic network connectivity. The Appendix is a reference for configuring the logical network.

Task 1: Design the Logical Lab Topology.

- Given an IP address of 192.168.254.0/24, and 5 bits used for subnets, fill in the following information:

Maximum number of usable subnets (including the 0th subnet): _____

Number of usable Hosts per subnet: _____

#	IP Address: 192.168.254.0		Subnet mask:	
	Subnet	First Host address	Last Host address	Broadcast
0				
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

- Before proceeding, verify your addresses with the instructor. The instructor will assign one subnetwork per student or team.

Task 2: Configure the Physical Lab Topology.

Step 1: Physically connect devices.

1. Cable the network devices as shown in Figure 1.

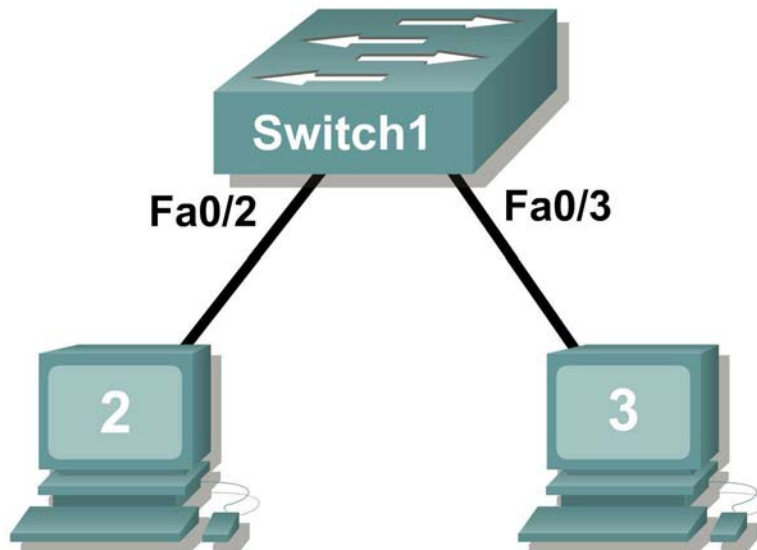


Figure 1. Cabling the Network

Is a crossover cable needed to connect Host computers to the switch? Why or why not?

If not already enabled, turn power on to all devices.

Step 2: Visually inspect network connections.

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

Task 3: Configure the Logical Topology.

Step 1: Document logical network settings.

1. Host computers will use the first two IP addresses in the subnetwork. Write down the IP address information for each device:

Device	Subnetwork	IP address	Mask
Host1			
Host2			

Figure 2. Logical Topology

- From the information given in Figure 2, write down the IP network addressing for each computer:

Host 1	
IP Address	
IP Mask	

Host 2	
IP Address	
IP Mask	

Step 2: Configure Host1 computer.

- On Computer1, click **Start > Control Panel > Network Connections**. Right-click the LAN icon, and choose **Properties**. On the **General** tab, select **Internet Protocol (TCP/IP)**, and then click the **Properties** button.

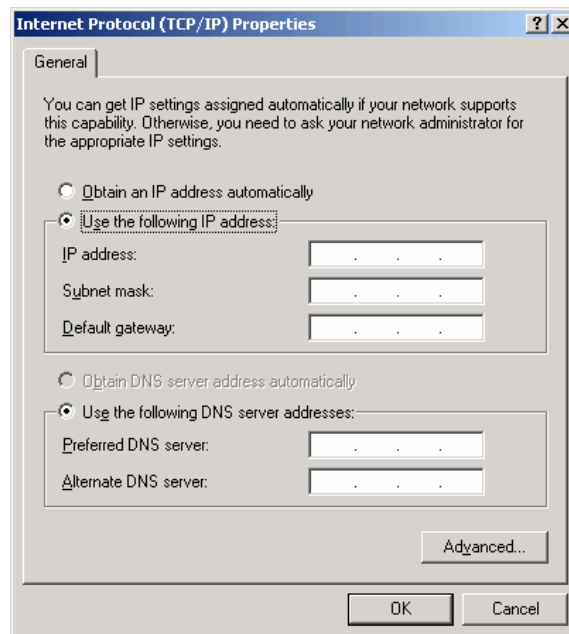


Figure 3. Host1 IP Address and Gateway Settings

- Refer to Figure 3 for Host1 IP address and gateway settings.
- When finished, click **OK**, then click **Close**. The computer may require a reboot for changes to be effective.
- Verify proper configuration of Host1 with the `ipconfig /all` command.

- Record the output below:

Setting	Value
Ethernet device	
Physical Address	
IP Address	
Subnet Mask	
Default Gateway	

Step 3: Configure Host2.

- Repeat Step 2 for Host2, using IP address information from the table filled out in Step 1.
- Verify proper configuration of Host1 with the `ipconfig /all` command.
- Record the output below:

Setting	Value
Ethernet device	
Physical Address	
IP Address	
Subnet Mask	
Default Gateway	

Task 4: Verify Network Connectivity.

Network connectivity can be verified with the Windows `ping` command.

- Use the following table to methodically verify connectivity with each network device:

From	To	IP Address	Ping results
Host1	Host2		
Host2	Host1		

- Take corrective action to establish connectivity if a test fails.

Note: If pings to host computers fail, temporarily disable the computer firewall and retest. To disable a Windows firewall, click **Start > Control Panel > Windows Firewall**, choose **Off**, and then click **OK**.

Task 5: Reflection

Review any physical or logical configuration problems encountered during this lab. Make sure you have a thorough understanding of the procedures used to configure a Windows host computer.

Task 6: Challenge

Ask your instructor or another student to introduce one or two problems in your network when you aren't looking or are out of the lab room. Problems can be either physical (wrong UTP cable) or logical (wrong IP address). To fix the problems:

1. Perform a good visual inspection. Look for green link lights on Switch1.
2. Use the table provided in Task 3, above, to identify failed connectivity. List the problems:

3. Write down your proposed solution(s):

4. Test your solution. If the solution fixed the problem, document the solution. If the solution did not fix the problem, continue troubleshooting.

Task 7: Clean Up

Unless directed otherwise by the instructor, restore host computer network connectivity, and then turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.

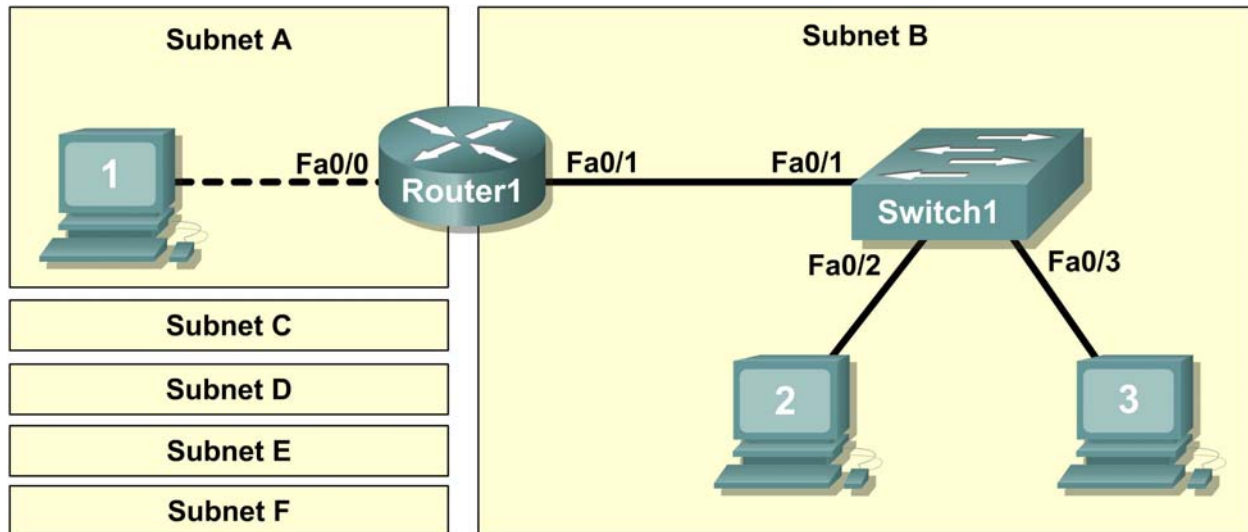
Appendix

Subnet addressing for last octet	.0	.64	.128	.192	.224	.240	.248	.252
.0	.0 (.1-.62)	.32 (.33-.62)	.64 (.65-.94)	.128 (.129-.158)	.192 (.193-.222)	.224 (.225-.254)	.240 (.241-.254)	.0 (.1-.62)
.4 (.5-.6)								
.8 (.9-.10)								
.12 (.13-.14)								
.16 (.17-.18)								
.20 (.21-.22)								
.24 (.25-.26)								
.28 (.29-.30)								
.32 (.33-.34)								
.36 (.37-.38)								
.40 (.41-.42)								
.44 (.45-.46)								
.48 (.49-.50)								
.52 (.53-.54)								
.56 (.57-.58)								
.60 (.61-.62)								
.64 (.65-.66)								
.68 (.69-.70)								
.72 (.73-.74)								
.76 (.77-.78)								
.80 (.81-.82)								
.84 (.85-.86)								
.88 (.89-.90)								
.92 (.93-.94)								
.96 (.97-.98)								
.100 (.101-.102)								
.104 (.105-.106)								
.108 (.109-.110)								
.112 (.113-.114)								
.116 (.117-.118)								
.120 (.121-.122)								
.124 (.125-.126)								
.128 (.129-.130)								
.132 (.133-.134)								
.136 (.137-.138)								
.140 (.141-.142)								
.144 (.145-.146)								
.148 (.149-.150)								
.152 (.153-.154)								
.156 (.157-.158)								
.160 (.161-.162)								
.164 (.165-.166)								
.168 (.169-.170)								
.172 (.173-.174)								
.176 (.177-.178)								
.180 (.181-.182)								
.184 (.185-.186)								
.188 (.189-.190)								
.192 (.193-.194)								
.196 (.197-.198)								
.200 (.201-.202)								
.204 (.205-.206)								
.208 (.209-.210)								
.212 (.213-.214)								
.216 (.217-.218)								
.220 (.221-.222)								
.224 (.225-.226)								
.228 (.229-.230)								
.232 (.233-.234)								
.236 (.237-.238)								
.240 (.241-.242)								
.244 (.245-.246)								
.248 (.249-.250)								
.252 (.253-.254)								
(1 bit) 10000000 1 subnet, 126 hosts	(2 bits) 11000000 3 subnets, 62 hosts	(3 bits) 11100000 7 subnets, 30 hosts	(4 bits) 11110000 15 subnets, 14 hosts	(5 bits) 11111000 31 subnets, 6 hosts	(6 bits) 11111100 63 subnets, 2 hosts			
Mask = 128₁₀	Mask = 192₁₀	Mask = 224₁₀	Mask = 240₁₀	Mask = 248₁₀	Mask = 252₁₀			

East Carolina University

Lab 11.5.4: Network Testing

Topology Diagram



Learning Objectives

Upon completion of this lab, you will be able to:

- Design the logical lab topology.
- Configure the physical lab topology.
- Configure the logical LAN topology.
- Verify LAN connectivity.

Background

Hardware	Qty	Description
Cisco Router	1	Part of CCNA Lab bundle
Cisco Switch	1	Part of CCNA Lab bundle
*Computer (Host)	3	Lab computer
CAT-5 or better straight-through UTP cables	3	Connects Router1, Host1, and Host2 to switch1
CAT-5 crossover UTP cable	1	Connects Host 1 to Router1
Console (rollover) cable	1	Connects Host1 to Router1 console

Table 1. Equipment and Hardware for this Lab

Gather the necessary equipment and cables. To configure the lab, make sure the equipment listed in Table 1 is available.

The Appendix contains Cisco IOS configuration syntax for this lab.

Scenario

In this lab, you will create a small network that requires connecting network devices and configuring host computers for basic network connectivity. SubnetA and SubnetB are subnets that are currently needed. SubnetC, SubnetD, SubnetE, and SubnetF are anticipated subnets, not yet connected to the network. The 0th subnet will be used.

Task 1: Design the Logical Lab Topology.

Given an IP address and mask of 172.20.0.0 / 24 (address / mask), design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
SubnetA	As shown in topology diagram
SubnetB	Between 80 – 100
SubnetC	Between 40 – 52
SubnetD	Between 20 – 29
SubnetE	12
SubnetF	5

Note: Always start with the subnet with the largest number of hosts and work your way down. Therefore, you should start with SubnetB and finish with SubnetA.

Step 1: Design SubnetB address block.

Begin the logical network design by satisfying the requirement of SubnetB, which requires the largest block of IP addresses. Using binary numbers to create your subnet chart, pick the first address block that will support SubnetB.

- Fill in the following table with IP address information for SubnetB:

Network Address	Mask	First Host Address	Last Host Address	Broadcast

- What is the bit mask? _____

Step 2: Design SubnetC address block.

Satisfy the requirement of SubnetC, the next largest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support SubnetC.

- Fill in the following table with IP address information for SubnetC:

Network Address	Mask	First Host Address	Last Host Address	Broadcast

- What is the bit mask? _____

Step 3: Design SubnetD address block.

Satisfy the requirement of SubnetD, the next largest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support SubnetD.

1. Fill in the following table with IP address information for SubnetD:

Network Address	Mask	First Host Address	Last Host Address	Broadcast

2. What is the bit mask? _____

Step 4: Design SubnetE address block.

Satisfy the requirement of SubnetE, the next largest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support SubnetE.

1. Fill in the following table with IP address information for SubnetE:

Network Address	Mask	First Host Address	Last Host Address	Broadcast

2. What is the bit mask? _____

Step 5: Design SubnetF address block.

Satisfy the requirement of SubnetF, the next largest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support SubnetF.

1. Fill in the following table with IP address information for SubnetF:

Network Address	Mask	First Host Address	Last Host Address	Broadcast

2. What is the bit mask? _____

Step 6: Design SubnetA address block.

Satisfy the requirement of SubnetA, the smallest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support SubnetA.

1. Fill in the following table with IP address information for SubnetA:

Network Address	Mask	First Host Address	Last Host Address	Broadcast

2. What is the bit mask? _____

Task 2: Configure the Physical Lab Topology.

Step 1: Physically connect lab devices.

1. Cable the network devices as shown in Figure 1. Pay special attention to the crossover cable required between Host1 and Router1.

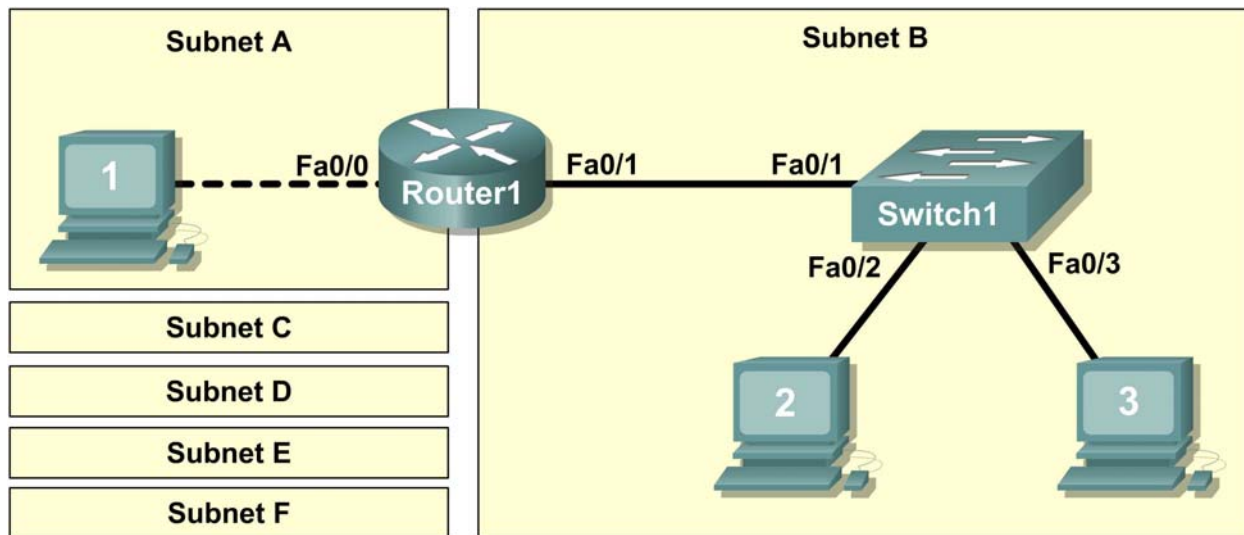


Figure 1. Cabling the Network

2. If not already enabled, turn power on to all devices.

Step 2: Visually inspect network connections.

After cabling the network devices, take a moment to verify the connections. Attention to detail now will minimize the time required to troubleshoot Layer 1 connectivity issues later.

Task 3: Configure the Logical Topology.

Step 1: Document logical network settings.

On SubnetA, Host1 will use the first IP address in the subnet. Router1, interface Fa0/0, will use the last host address. On SubnetB, host computers will use the first and second IP addresses in the subnet, respectively. Router1, interface Fa0/1, will use the last network host address.

To properly route Layer 2 frames between LAN devices, Switch1 does not require Layer 3 configuration. The IP address assigned to Switch 1, interface VLAN 1, is used to establish Layer 3 connectivity between external devices and the switch. Without an IP address, upper-layer protocols such as TELNET and HTTP will not work. The default gateway address permits the switch to respond to protocol requests from devices on distant networks. For example, the IP gateway address extends Layer 3 connectivity beyond Subnet B. Switch1 will use the next-to-last host address.

Write down the IP address information for each device:

Device	Subnet	IP Address	Mask	Gateway
Host1				
Router1-Fa0/0				
Host2				
Host3				

Switch1				
Router1-Fa0/1				

Step 2: Configure host computers.

1. On each computer, in turn, click **Start > Control Panel > Network Connections**. Right-click the LAN icon, and choose **Properties**. On the **General** tab, select **Internet Protocol (TCP/IP)**, and then click the, **Properties** button.
2. Verify that the Host1 Layer 3 IP address is on a different subnet than Host2 and Host3. Configure each host computer using the IP address information recorded in Step 1.
3. Verify proper configuration of each host computer with the `ipconfig` command and fill in the following table:

Device	IP Address	Mask	Default Gateway
Host1			
Host2			
Host3			

Step 3: Configure Router1.

1. From the Windows taskbar, start the HyperTerminal program by clicking **Start > Programs > Accessories > Communications > HyperTerminal**. Configure HyperTerminal for access to Router1. Configuration for Router1 includes the following tasks:

Tasks (Refer to the Appendix for help with commands)
Specify Router name: <code>Router1</code>
Specify an encrypted privileged EXEC password: <code>cisco</code>
Specify a console access password: <code>class</code>
Specify a telnet access password: <code>class</code>
Configure the MOTD banner
Configure Router1 interface Fa0/0: <ul style="list-style-type: none"> • Set the description • Set the Layer 3 address • Issue no shutdown
Configure Router1 interface Fa0/1: <ul style="list-style-type: none"> • Set the description • Set the Layer 3 address • Issue no shutdown

2. Save the configuration in NVRAM.
3. Display the contents of RAM:
4. Write the configuration specifications below:

Hostname: _____

Enable secret password: _____

Console access password: _____

Telnet access password: _____

MOTD banner: _____

5. Display configuration information for interface Fa0/0: **show interface Fa0/0**

FastEthernet 0/0 status (up / down): _____

Line protocol: _____

MAC Address: _____

6. Display configuration information for interface Fa0/1: **show interface Fa0/1**

FastEthernet 0/0 status (up / down): _____

Line protocol: _____

MAC Address: _____

7. Display brief IP address information about each interface: **show ip interface brief**

```
Interface          IP-Address          OK? Method Status  Protocol
FastEthernet0/0
FastEthernet0/1
```

8. Take corrective action with any problems, and retest.

Step 4: Configure Switch1.

1. Move the console cable from Router1 to Switch1.
2. Press **Enter** until a response is received.
3. Configuration for Switch1 includes the following tasks:

Tasks (Refer to the Appendix for help with commands)
Specify Switch name- <code>Switch1</code>
Specify an encrypted privileged exec password- <code>cisco</code>
Specify a console access password- <code>class</code>
Specify a telnet access password- <code>class</code>
Configure the MOTD banner
Configure Switch1 interface Fa0/1: Set the description
Configure Switch1 interface Fa0/2: Set the description
Configure Switch1 interface Fa0/3: Set the description
Configure management VLAN 1 IP address: <ul style="list-style-type: none">• Set the description• Set the Layer 3 address• Issue no shutdown
Configure default IP gateway address

4. Display the contents of RAM:

5. Write the configuration specifications below:

Hostname: _____
 Enable secret password: _____
 Console access password: _____
 Telnet access password: _____
 MOTD banner: _____
 Interface VLAN 1: _____
 Default IP gateway address: _____

6. Display configuration information for interface VLAN 1: **show interface vlan1**

VLAN 1 status (up / down): _____
 Line protocol: _____

Task 4: Verify Network Connectivity.

Step 1: Use the `ping` command to verify network connectivity.

Network connectivity can be verified with the `ping` command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure.

1. Use the following table to methodically verify connectivity with each network device:

From	To	IP Address	Ping results
Host1	LocalHost (127.0.0.1)		
Host1	NIC IP address		
Host1	Gateway (Router1, Fa0/0)		
Host1	Router1, Fa0/1		
Host1	Switch1		
Host1	Host2		
Host1	Host3		
Host2	LocalHost (127.0.0.1)		
Host2	NIC IP address		
Host2	Host3		
Host2	Switch1		
Host2	Gateway (Router1, Fa0/1)		
Host2	Router1, Fa0/0		
Host2	Host1		
Host3	LocalHost (127.0.0.1)		
Host3	NIC IP address		
Host3	Host2		

From	To	IP Address	Ping results
Host3	Switch1		
Host3	Gateway (Router1, Fa0/1)		
Host3	Router1, Fa0/0		
Host3	Host1		

- Take corrective action to establish connectivity if a test fails.

Note: If pings to host computers fail, temporarily disable the computer firewall and retest. To disable a Windows firewall, click **Start > Control Panel > Windows Firewall**, choose **Off**, and then click **OK**.

Step 2: Use the `tracert` command to verify local connectivity.

- From Host1, issue the `tracert` command to Host2 and Host3.
- Record the results:

From Host1 to Host2: _____

From Host1 to Host3: _____

Step 3: Verify Layer 2 connectivity.

- If not already connected, move the console cable from Router1 to Switch1.
- Press the **Enter** key until there is a response from Switch1.
- Issue the command `show mac-address-table`. This command will display static (CPU) and dynamic, or learned, entries.
- List the dynamic MAC addresses and corresponding switch ports:

MAC Address	Switch Port

- Verify that there are three dynamically learned MAC addresses, one each from Fa0/1, Fa0/2, and Fa0/3.

Task 5: Reflection

Review any physical or logical configuration problems encountered during this lab. Make sure you have a thorough understanding of the procedures used to verify network connectivity.

Task 6: Challenge

Ask your instructor or another student to introduce one or two problems in your network when you aren't looking or are out of the lab room. Problems can be either physical (wrong UTP cable) or logical (wrong IP address or gateway). To fix the problems:

- Perform a good visual inspection. Look for green link lights on Switch1.
- Use the table provided in Task 3, above, to identify failed connectivity. List the problems:

3. Write down your proposed solution(s):

4. Test your solution. If the solution fixed the problem, document the solution. If the solution did not fix the problem, continue troubleshooting.

Task 7: Clean Up

Unless directed otherwise by the instructor, restore host computer network connectivity, and then turn off power to the host computers.

Before turning off power to the router and switch, remove the NVRAM configuration file from each device with the privileged exec command **erase startup-config**.

Carefully remove cables and return them neatly to their storage. Reconnect cables that were disconnected for this lab.

Remove anything that was brought into the lab, and leave the room ready for the next class.

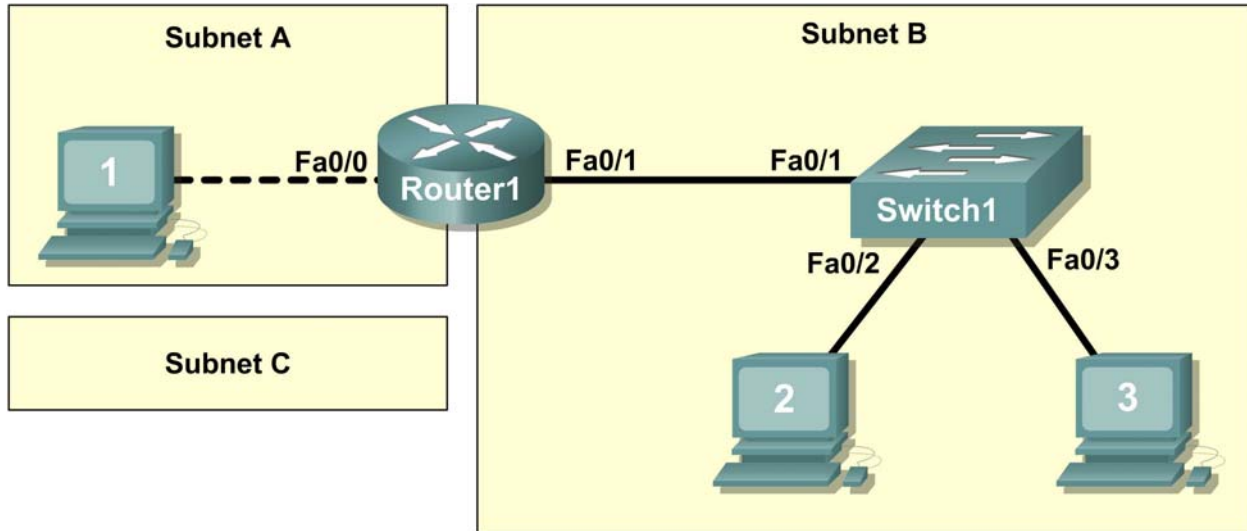
Appendix—List of Cisco IOS commands used in this lab

Purpose	Command
Enter the global configuration mode.	configure terminal Example: Router> enable Router# configure terminal Router(config)#
Specify the name for the Cisco device.	hostname name Example: Router (config)# hostname Router1 Router (config)#
Specify an encrypted password to prevent unauthorized access to the privileged EXEC mode.	Enable secret password Example: Router (config)# enable secret cisco Router (config)#
Specify a password to prevent unauthorized access to the console.	password password login Example: Router (config)# line con 0 Router (config-line)# password class Router (config-line)# login Router (config)#
Specify a password to prevent unauthorized Telnet access. Router vty lines: 0 4 Switch vty lines: 0 15	password password login Example: Router (config)# line vty 0 4 Router (config-line)# password class Router (config-line)# login Router (config-line)#
Configure the MOTD banner.	Banner motd % Example: Router (config)# banner motd % Router (config)#
Configure a Router interface. Router interface is OFF by default	Example: Router (config)# interface Fa0/0 Router (config-if)# description description Router (config-if)# ip address address mask Router (config-if)# no shutdown Router (config-if)#
Switch interface is ON by default (VLAN interface is OFF by default)	Example: Switch (config)# interface Fa0/0 Switch (config-if)# description description Switch (config)# interface vlan1 Switch (config-if)# ip address address mask Switch (config-if)# no shutdown Switch (config-if)#
Switch- create a default IP gateway	Switch (config)# ip default-gateway address
Save the configuration to NVRAM.	copy running-config startup-config Example:

	Router# copy running-config startup-config
--	---

Lab 11.5.5: Network Documentation with Utility Commands

Topology Diagram



Learning Objectives

- Design the logical lab topology.
- Configure the physical lab topology.
- Design and configure the logical LAN topology.
- Verify LAN connectivity.
- Document the network.

Background

Hardware	Qty	Description
Cisco Router	1	Part of CCNA Lab bundle.
Cisco Switch	1	Part of CCNA Lab bundle.
*Computer (host)	3	Lab computer.
CAT-5 or better straight-through UTP cables	3	Connects Router1, Host1, and Host2 to switch1.
CAT-5 crossover UTP cable	1	Connects host 1 to Router1
Console (rollover) cable	1	Connects Host1 to Router1 console

Table 1. Equipment and hardware for Eagle 1 lab.

Gather the necessary equipment and cables. To configure the lab, make sure the equipment listed in Table 1 is available.

In this lab router and host output will be copied from the devices and into Notepad for use in network documentation. Appendix1 contains tables that can be used to copy output into, or create your own tables.

Scenario

Network documentation is a very important tool for the organization. A well-documented network enables network engineers to save significant time in troubleshooting and planning future growth.

In this lab students will create a small network that requires connecting network devices and configuring Host computers for basic network connectivity. Subnet A and Subnet B are subnets that are currently needed. Subnet C is an anticipated subnet, not yet connected to the network. The 0th subnet will be used.

Task 1: Configure the logical lab topology.

Given an IP address of 209.165.200.224 / 27 (address / mask), design an IP addressing scheme that satisfies the following requirements:

Subnet	Number of Hosts
Subnet A	2
Subnet B	Between 2 - 6
Subnet C	Between 10 – 12

Step 1: Design Subnet C address block.

Begin the logical network design by satisfying the requirement for Subnet C, the largest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support Subnet C.

Fill in the following table with IP address information for Subnet C:

Network Address	Mask	First Host address	Last Host address	Broadcast

What is the bit mask? _____

Step 2: Design Subnet B address block.

Satisfy the requirement of Subnet B, the next largest block of IP addresses. Using binary numbers to create your subnet chart, pick the first address block that will support Subnet B.

Fill in the following table with IP address information for Subnet B:

Network Address	Mask	First Host address	Last Host address	Broadcast

What is the bit mask? _____

Step 3: Design Subnet A address block.

Satisfy the requirement of Subnet A, the smallest IP address block. Using binary numbers to create your subnet chart, pick the next available address block that will support Subnet A.

Fill in the following table with IP address information for Subnet A:

Network Address	Mask	First Host address	Last Host address	Broadcast

--	--	--	--

What is the bit mask? _____

Task 2: Configure the Physical Lab Topology.

Step 1: Physically connect lab devices.

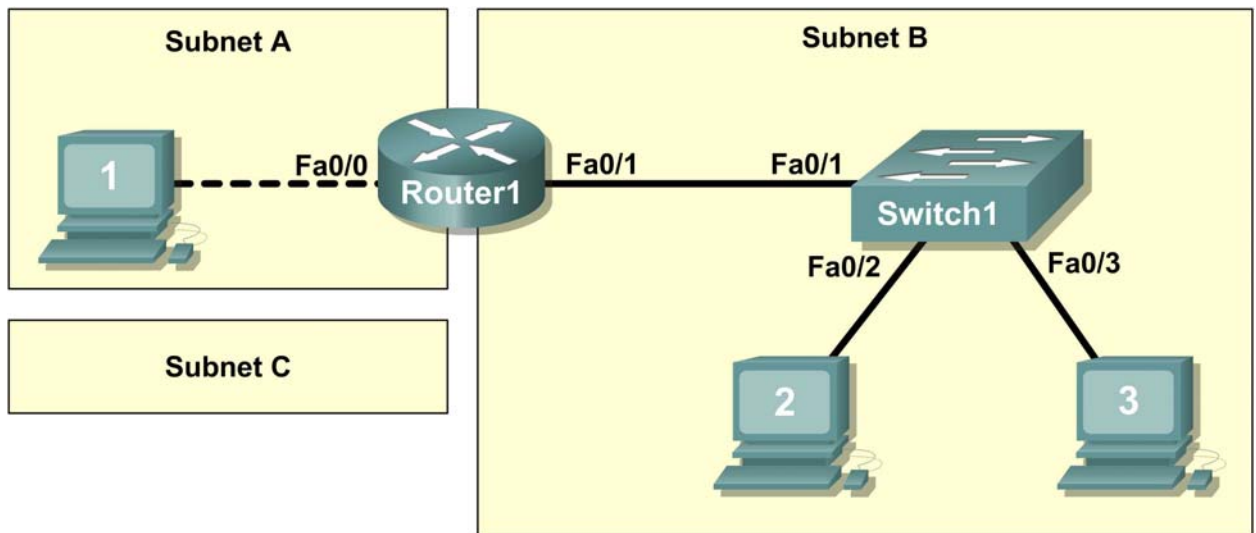


Figure 1. Cabling the network.

Cable the network devices as shown in Figure 1. Pay special attention to the crossover cable required between Host1 and Router1.

If not already enabled, turn power on to all devices.

Step 2: Visually inspect network connections.

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

Task 3: Configure the Logical Topology.

Step 1: Document logical network settings.

Host computers will use the first two IP addresses in the subnetwork. The network router will use the LAST network host address. Write down the IP address information for each device:

Device	Subnet	IP address	Mask	Gateway
Router1-Fa0/0				
Host1				
Router1-Fa0/1				
Host2				
Host3				
Switch1	N/A	N/A	N/A	N/A

Step 2: Configure host computers.

On each computer in turn, select start | Control Panel | Network Connections. Identify the Local Area Connection device icon. Use the mouse pointer to highlight the icon, right-click, and select properties. Highlight Internet Protocol (TCP/IP), and select Properties.

Verify that the Host1 Layer 3 IP address is on a different subnet than Host2 and Host3. Configure each host computer using the IP address information recorded in Step 1.

Verify proper configuration of each host computer with the `ipconfig /all` command. Record your information in Appendix1, Network Documentation:

Step 3: Configure Router1.

From the Windows taskbar, start the HyperTerminal program by clicking on Start | Programs | Accessories | Communications | HyperTerminal. Configure HyperTerminal for access to Router1. Configuration tasks for Router1 include the following:

Task
Specify Router name- Router1
Specify an encrypted privileged exec password- cisco
Specify a console access password- class
Specify a telnet access password- class
Configure the MOTD banner.
Configure Router1 interface Fa0/0- set the description set the Layer 3 address issue <code>no shutdown</code>
Configure Router1 interface Fa0/1- set the description set the Layer 3 address issue <code>no shutdown</code>

Save the configuration in NVRAM.

Display the contents of RAM:

Copy the output of the configuration into the Router1 configuration table, Appendix 1.

Copy the output of the `show interface fa0/0` and `show interface fa0/1` commands into the Router1 Interface configuration tables, Appendix 1.

Copy the output of the `show ip interface brief` command into the Router1 IP Address configuration table, Appendix 1.

Step 4: Configure Switch1.

Move the console cable from Router1 to Switch1. Press Enter until a response is received. Configuration tasks for Switch1 include the following:

Task
Specify Switch name- <code>Switch1</code>
Specify an encrypted privileged exec password- <code>cisco</code>
Specify a console access password- <code>class</code>
Specify a telnet access password- <code>class</code>
Configure the MOTD banner.
Configure Switch1 interface Fa0/1- set the description
Configure Switch1 interface Fa0/2- set the description
Configure Switch1 interface Fa0/3- set the description

Display the contents of RAM:

Copy the output of the configuration into the Switch1 configuration table, Appendix 1.

Copy the output of the `show mac address-table` command into the Switch1 MAC address table, Appendix 1.

Task 4: Verify Network Connectivity.

Step 1: Use the `ping` command to verify network connectivity.

Network connectivity can be verified with the `ping` command. It is very important that connectivity exists throughout the network. Corrective action must be taken if there is a failure.

****NOTE:** If pings to host computers fail, temporarily disable the computer firewall and retest. To disable a Windows firewall, select Start | Control Panel | Windows Firewall, select OFF, and OK.

Use the following table to methodically verify connectivity with each network device. Take corrective action to establish connectivity if a test fails:

From	To	IP Address	Ping results
Host1	LocalHost (127.0.0.1)		
Host1	NIC IP address		
Host1	Gateway (Router1, Fa0/0)		
Host1	Router1, Fa0/1		
Host1	Host2		
Host1	Host3		
Host2	LocalHost (127.0.0.1)		
Host2	NIC IP address		
Host2	Host3		
Host2	Gateway (Router1, Fa0/1)		
Host2	Router1, Fa0/0		
Host2	Host1		
Host3	LocalHost (127.0.0.1)		
Host3	NIC IP address		
Host3	Host2		
Host3	Gateway (Router1, Fa0/1)		
Host3	Router1, Fa0/0		
Host3	Host1		

Step 2: Use the `tracert` command to verify local connectivity.

In addition to connectivity testing, the `tracert` command may also be used as a crude throughput tester for network baselining. That is, with minimal traffic, `tracert` results can be compared against periods of high traffic. Results can be used to justify equipment upgrades or new purchases.

From Host1, issue the `tracert` command to Router1, Host2, and Host3. Record the results in the Host1 Tracert output, Appendix A.

From Host2, issue the `tracert` command to Host3, Router1, and Host1. Record the results in the Host2 Tracert output, Appendix A.

From Host3, issue the `tracert` command to Host2, Router1, and Host1. Record the results in the Host3 Tracert output, Appendix A.

Task 5: Document the Network.

With all the work performed so far, it would seem that there is nothing left to do. The network was physically and logically configured, verified, and command output copied into tables.

The last step in network documentation is to organize your output. As you organize, think what might be needed six months or a year from now. For example:

When was the network created?

When was the network documented?

Were there any significant challenges that were overcome?

Who performed the configuration (talent like this needs to be tracked)?

Who performed the documentation (talent like this needs to be tracked)?

These questions should be answered in the documentation, perhaps in a cover letter.

Be sure to include the following information:

A copy of the physical topology.

A copy of the logical topology.

Prepare your documentation in a professional format, and submit it to your instructor.

Task 6: Reflection

Review any physical or logical configuration problems encountered during this lab. Insure a thorough understanding of the procedures used to verify network connectivity.

Task 7: Challenge

Ask your instructor or another student to introduce one or two problems in your network when you aren't looking or are out of the lab room. Problems can be either physical (cables moved on the switch) or logical (wrong IP address or gateway).

Use your network documentation to troubleshoot and remedy the problems:

1. Perform a good visual inspection. Look for green link lights on Switch1.
2. Use your network documentation to compare what should be to what is:

3. Write down your proposed solution(s):

4. Test your solution. If the solution fixed the problem, document the solution. If the solution did not fix the problem, continue troubleshooting.

Task 6: Cleanup

Unless directed otherwise by the instructor, restore host computer network connectivity, then turn off power to the host computers.

Before turning off power to the router and switch, remove the NVRAM configuration file from each device with the privileged exec command **erase startup-config**.

Carefully remove cables and return them neatly to their storage. Reconnect cables that were disconnected for this lab.

Remove anything that was brought into the lab, and leave the room ready for the next class.

Appendix 1- Network Documentation

Host tables created from Task 3, Step 2:

Host1 Network Configuration	
Host Name	
IP Routing Enabled	
Ethernet adapter	
Description	
Physical Address	
IP Address	
Subnet Mask	
Default Gateway	

Host2 Network Configuration	
Host Name	
IP Routing Enabled	
Ethernet adapter	
Description	
Physical Address	
IP Address	
Subnet Mask	
Default Gateway	

Host3 Network Configuration	
Host Name	
IP Routing Enabled	
Ethernet adapter	
Description	
Physical Address	
IP Address	
Subnet Mask	
Default Gateway	

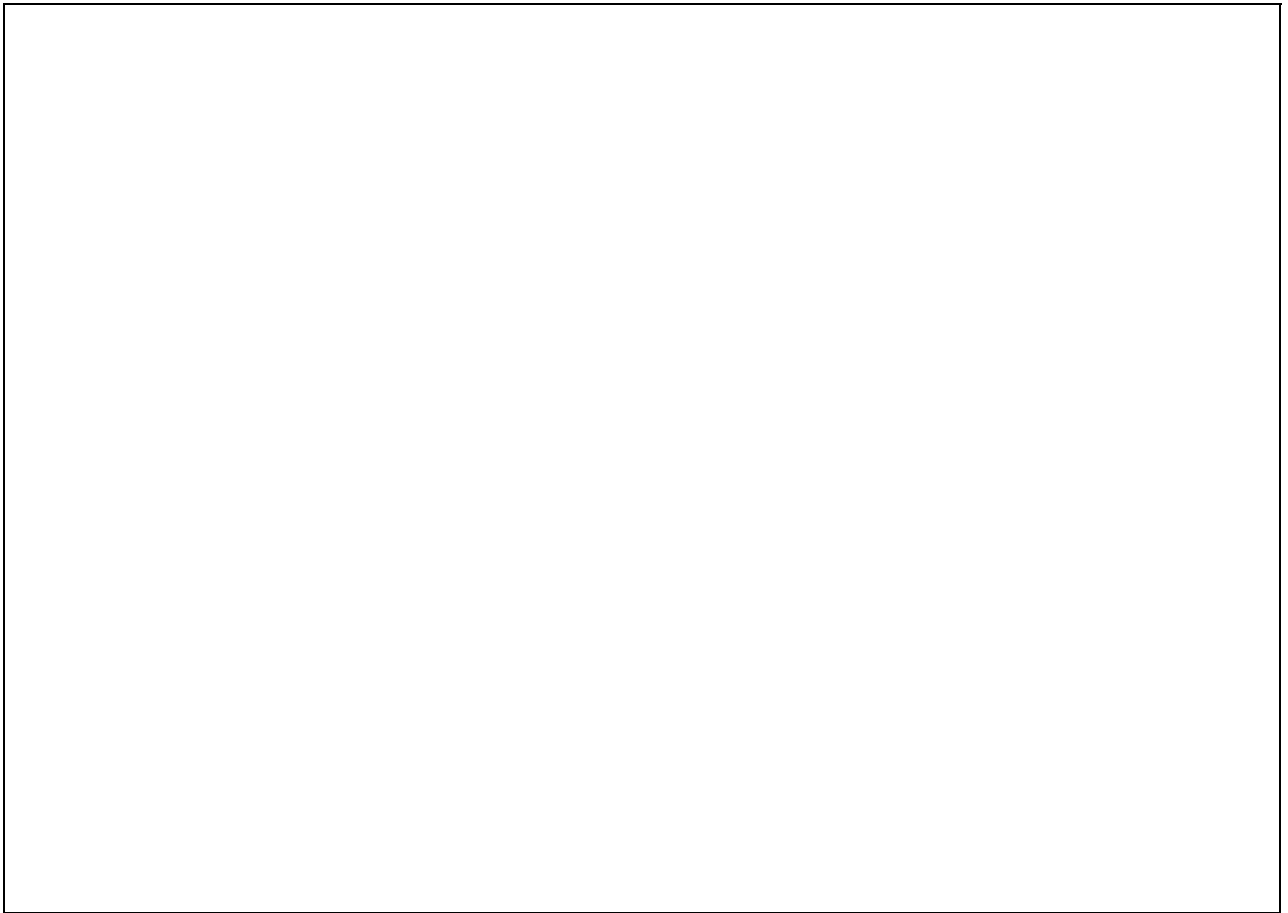
Router1 configuration from Task 3, Step 3:

Router1 Configuration

Router1 Interface Fa0/0 configuration from Task 2, Step 3:

--

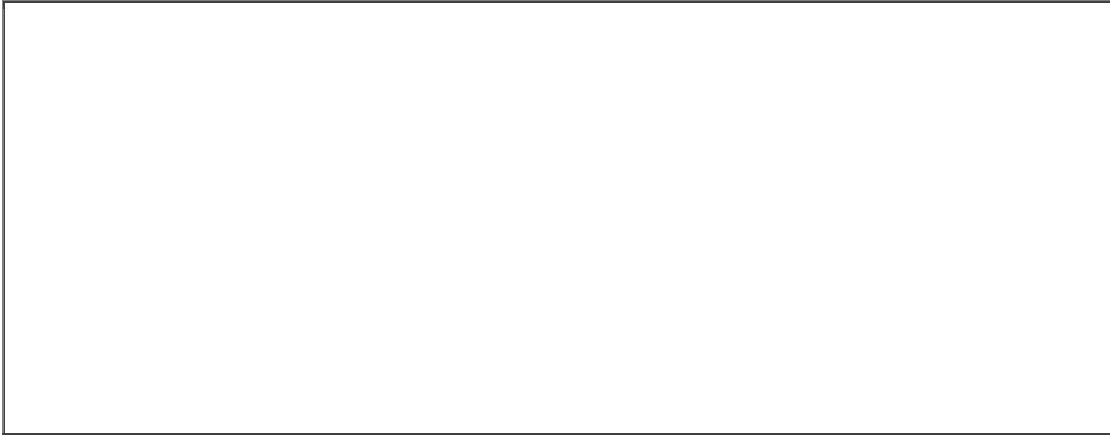
Router1 Interface fa0/1 configuration from Task 3, Step 3:



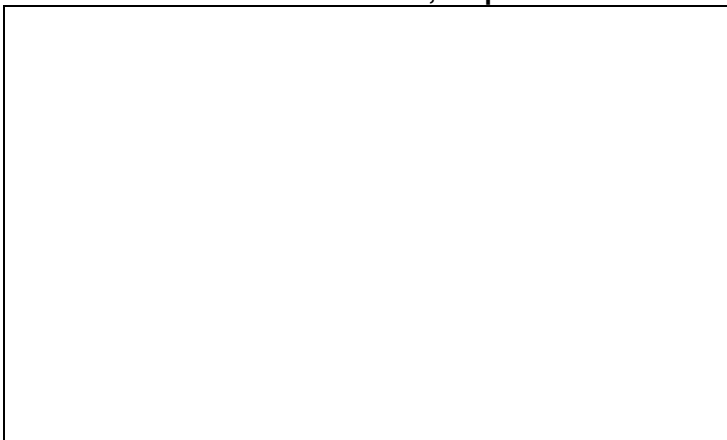
Router1 IP Address configuration from Task 3, Step 3:



Switch1 Configuration from Task 3, Step 4:

A large, empty rectangular box with a thin black border, intended for the user to paste or type the configuration commands for Switch1.

Switch1 MAC address-table from Task 3, Step 4:

A rectangular box with a thin black border, intended for the user to paste or type the output of the MAC address-table command for Switch1.

Traceroute results from Host1 Task 4, Step 2:

A large, empty rectangular box with a thin black border, intended for the user to paste or type the output of the traceroute command from Host1.

Traceroute results from Host2 Task 4, Step 2:

Traceroute results from Host3 Task 4, Step 2:

Lab 11.5.6: Final Case Study - Datagram Analysis with Wireshark

Learning Objectives

Upon completion of this exercise, students will be able to demonstrate:

- How a TCP segment is constructed, and explain the segment fields.
- How an IP packet is constructed, and explain the packet fields.
- How an Ethernet II frame is constructed, and explain the frame fields.
- Contents of an ARP REQUEST and ARP REPLY.

Background

This lab requires two captured packet files and Wireshark, a network protocol analyzer. Download the following files from Eagle server, and install Wireshark on your computer if it is not already installed:

- eagle1_web_client.pcap (discussed)
- eagle1_web_server.pcap (reference only)
- wireshark.exe

Scenario

This exercise details the sequence of datagrams that are created and sent across a network between a web client, PC_Client, and web server, eagle1.example.com. Understanding the process involved in sequentially placing packets on the network will enable the student to logically troubleshoot network failures when connectivity breaks. For brevity and clarity, network packet noise has been omitted from the captures. Before executing a network protocol analyzer on a network that belongs to someone else, be sure to get permission- in writing.

Figure 1 shows the topology of this lab.

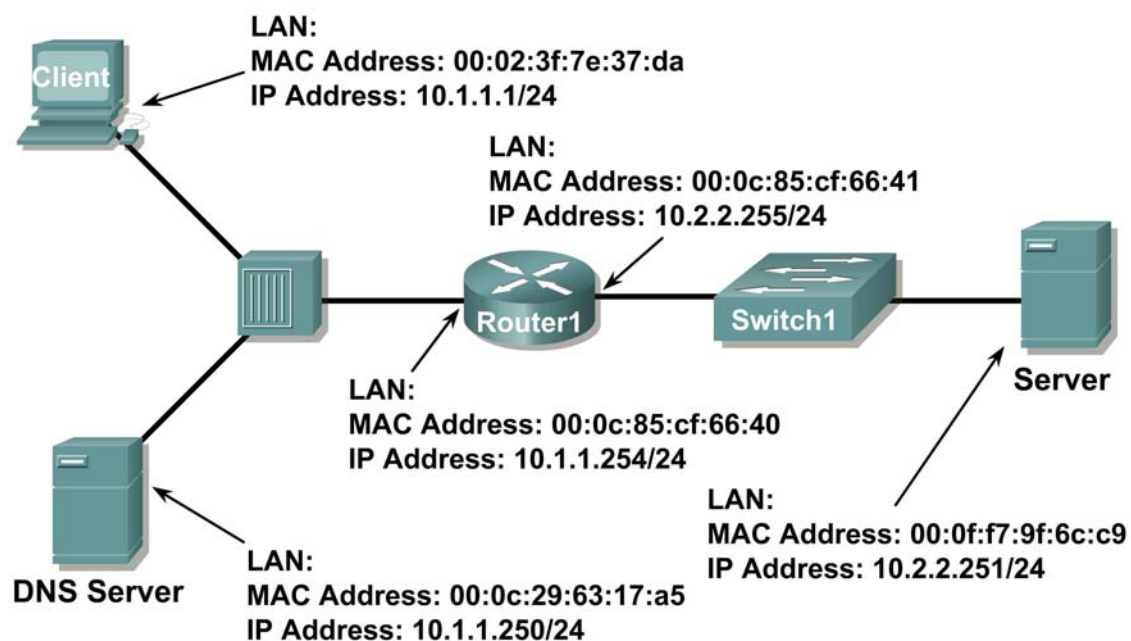


Figure 1. Network Topology.

Using Microsoft® command line tools, IP configuration information and the contents of ARP cache are displayed. Refer to Figure 2.

```
C: > ipconfig / all
Windows IP Configuration
Ethernet adapter Local Area Connection:
    Connection-specific DNS Suffix  . : 
    Description . . . . . : Intel(R) PRO/1000 MT
                             Network Connection
    Physical Address. . . . . : 00:02:3f:7e:37:da
    Dhcp Enabled. . . . . : No
    IP Address. . . . . : 10.1.1.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.1.1.254
    DNS Servers . . . . . : 10.1.1.250
C: > arp -a
No ARP Entries Found
C: >
```

Figure 2. PC Client initial network state.

A web client is started, and URL eagle1.example.com is entered, as shown in Figure 3. This begins the communication process to the web server, and where the captured packets start.

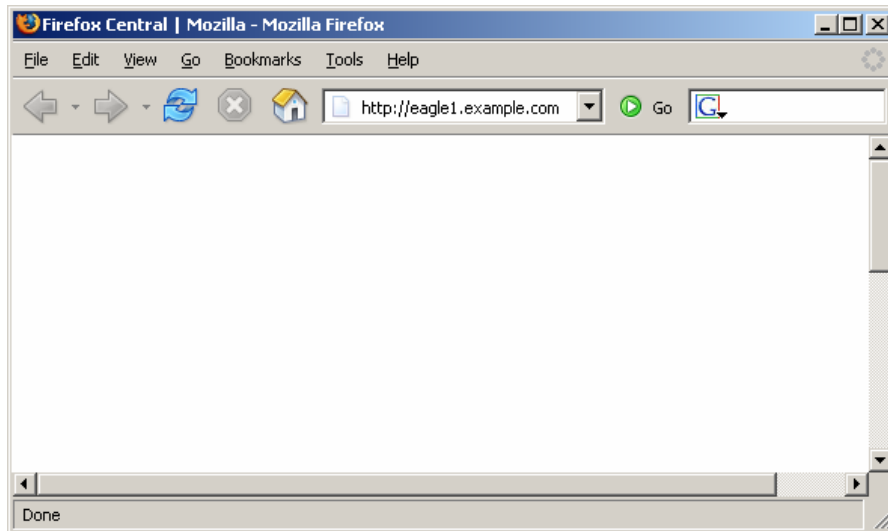


Figure 3. PC Client with web browser.

Task 1: Prepare the Lab.

Step 1: Start Wireshark on your computer.

Refer to Figure 4 for changes to the default output. Uncheck Main toolbar, Filter toolbar, and Packet Bytes. Verify that Packet List and Packet Details are checked. To insure there is no automatic translation in MAC addresses, de-select Name Resolution for MAC layer and Transport Layer.

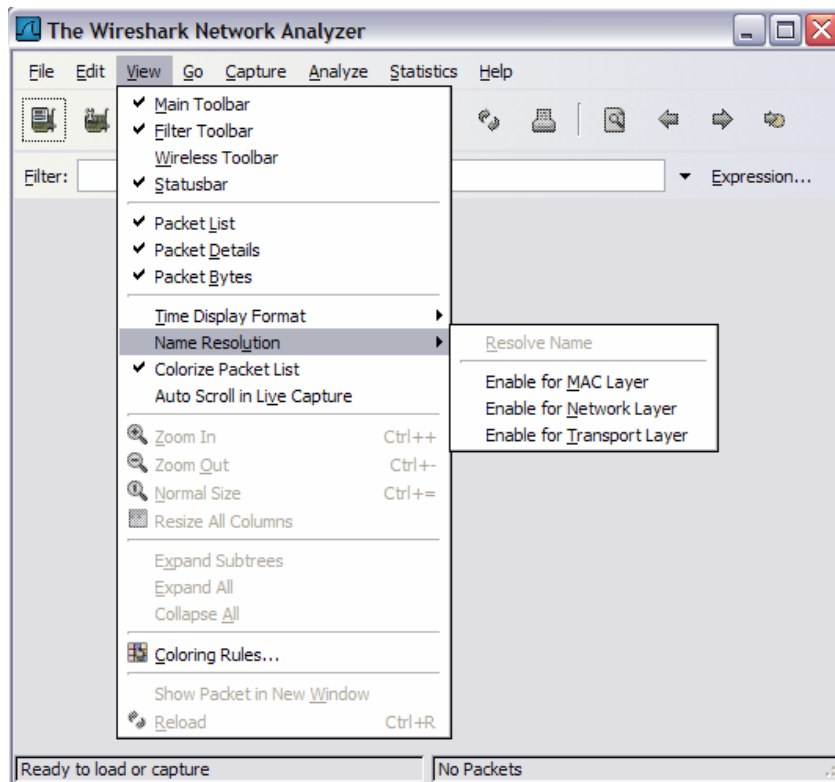


Figure 4. Wireshark default view changes.

Step 2: Load the web client capture, eagle1_web_client.pcap.

A screen similar to Figure 5 will be displayed. Various pull-down menus and sub-menus are available. There are also two separate data windows. The top Wireshark window lists all captured packets. The bottom window contains packet details. In the bottom window, each line that contains a check box, indicates that additional information is available.

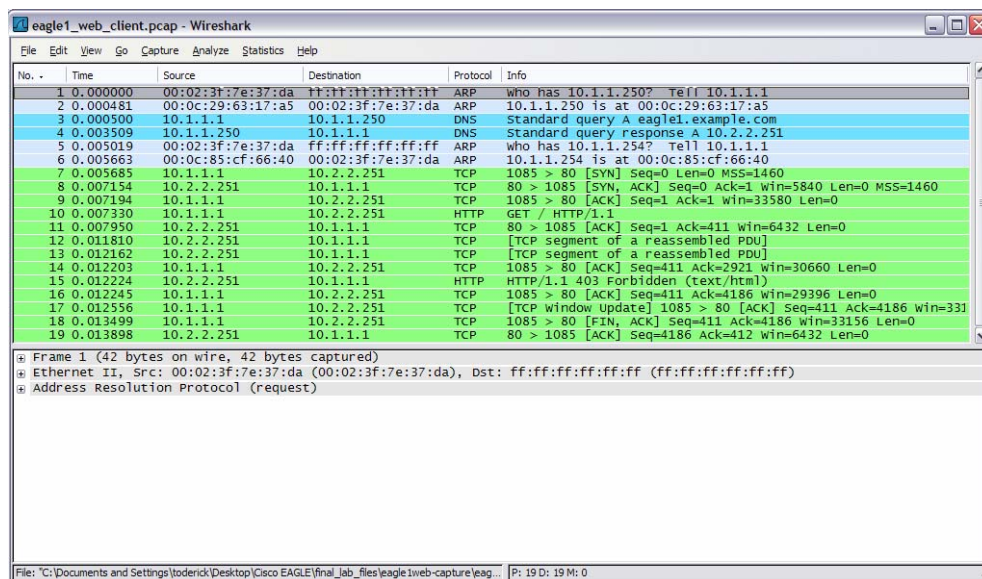


Figure 5. Wireshark with file eagle1_web_client.pcap loaded.

Task 2: Review the Process of Data Flowing through the Network.

Step 1: Review Transport layer operation.

When PC_Client builds the datagram for a connection with eagle1.example.com, the datagram travels down the various network Layers. At each Layer, important header information is added. Because this communication is from a web client, the Transport Layer protocol will be TCP. Consider the TCP segment, shown in Figure 6. PC_Client generates an internal TCP port address, in this conversation 1085, and knows the well-known web server port address, 80. Likewise, a sequence number has been internally generated. Data is included, provided by the Application Layer. Some information will not be known to PC_Client, so it must be discovered using other network protocols.

There is no acknowledgement number. Before this segment can move to the Network Layer, the TCP three-way handshake must be performed.

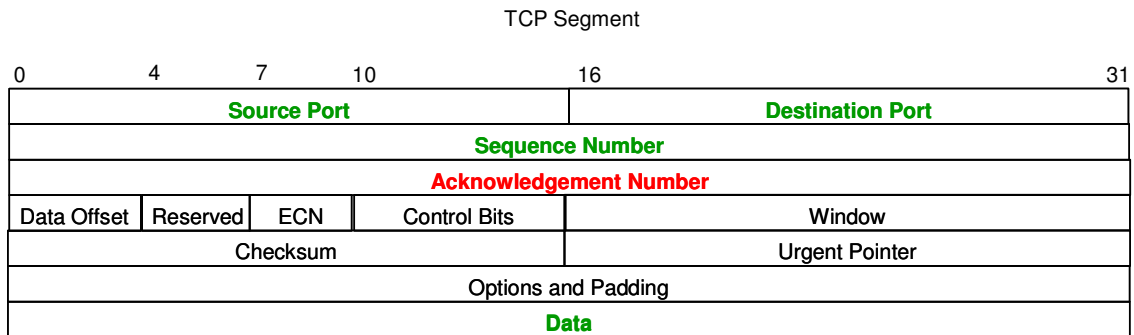


Figure 6. TCP Segment fields.

Step 2: Review Network layer operation.

At the Network Layer, the IPv4 (IP) PACKET has several fields ready with information. This is shown in Figure 7. For example, the packet Version (IPv4) is known, as well as the source IP address.

The destination for this packet is eagle1.example.com. The corresponding IP Address must be discovered through DNS (Domain Name Services). Until the upper layer datagram is received, fields related to the upper layer protocols are empty.

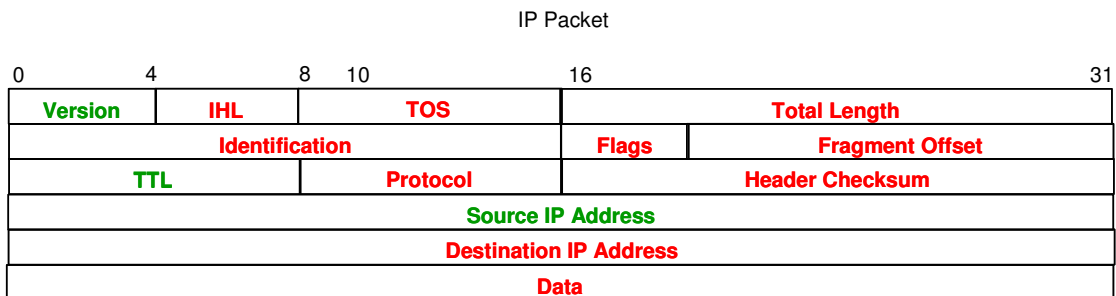


Figure 7. IP Packet fields.

Step 3: Review Data Link layer operation.

Before the datagram is placed on the physical medium, it must be encapsulated inside a frame. This is shown in Figure 8. PC_Client has knowledge of the source MAC address, but must discover the destination MAC address.

The destination MAC address must be discovered.

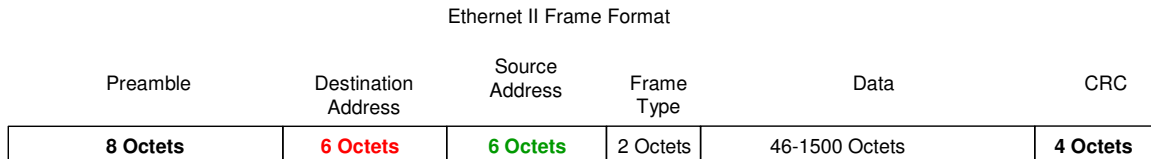


Figure 8. Ethernet II frame fields.

Task 3: Analyze Captured Packets.

Step 1: Review the data flow sequence.

A review of missing information will be helpful in following the captured packet sequence:

- a. The TCP segment cannot be constructed because the acknowledgement field is blank. A TCP 3-way handshake with eagle1.example.com must first be completed.
- b. The TCP 3-way handshake cannot occur because PC_Client does not know the IP address for eagle1.example.com. This is resolved with a DNS request from PC_Client to the DNS the server.
- c. The DNS server cannot be queried because the MAC address for the DNS server is not known. The ARP protocol is broadcast on the LAN to discover the MAC address for the DNS server.
- d. The MAC address for eagle1.example.com is unknown. The ARP protocol is broadcast on the LAN to learn the destination MAC address for eagle1.example.com.

Step 2: Examine the ARP request.

Refer to Wireshark, Packet List window, No. 1. The captured frame is an ARP (Address Resolution Protocol) Request. Contents of the Ethernet II frame can be viewed by clicking on the check box in the second line of the Packet Details window. Contents of the ARP Request can be viewed by clicking on the ARP Request line in the Packet Details window.

1. What is the source MAC address for the ARP Request? _____
2. What is the destination MAC address for the ARP Request? _____
3. What is the unknown IP address in the ARP Request? _____
4. What is the Ethernet II Frame Type? _____

Step 3: Examine the ARP reply.

Refer to Wireshark, Packet List window, No. 2. The DNS server sent an ARP Reply.

1. What is the source MAC address for the ARP Reply? _____
2. What is the destination MAC address for the ARP Request? _____
3. What is the Ethernet II Frame Type? _____
4. What is the destination IP address in the ARP Reply? _____
5. Based on the observation of the ARP protocol, what can be inferred about an ARP Request destination address and an ARP Reply destination address?

6. Why did the DNS server not have to send an ARP Request for the PC_Client MAC address?

Step 4: Examine the DNS query.

Refer to Wireshark, Packet List window, No. 3. PC_Client sent a DNS query to the DNS server. Using the Packet Details window, answer the following questions:

1. What is the Ethernet II Frame Type? _____
2. What is the Transport Layer protocol, and what is the destination port number?

Step 5: Examine the DNS query response.

Refer to Wireshark, Packet List window, No. 4. The DNS server sent a DNS query response to PC_Client. Using the Packet Details window, answer the following questions:

1. What is the Ethernet II Frame Type? _____
2. What is the Transport Layer protocol, and what is the destination port number?

3. What is the IP address for eagle1.example.com? _____
4. A colleague is a firewall administrator, and asked if you thought of any reason why all UDP packets should not be blocked from entering the internal network. What is your response?

Step 6: Examine the ARP request.

Refer to Wireshark, Packet List window, No. 5 and No 6. PC_Client sent an ARP Request to IP address 10.1.1.254.

1. Is this IP address different than the IP address for eagle1.example.com? Explain?

Step 7: Examine the TCP 3-way handshake.

Refer to Wireshark, Packet List window, No. 7, No. 8, and No. 9. These captures contain the TCP 3-way handshake between PC_Client and eagle1.example.com. Initially, only the TCP SYN flag is set on the datagram sent from PC_Client, sequence number 0. eagle1.example.com responds with the TCP ACK and SYN flags set, along with an acknowledgement of 1 and sequence of 0. In the Packet List window, there is an unexplained value, **MSS=1460**. MSS stands for Maximum Segment size. When a TCP segment is transported over IPv4, MSS is computed to be the maximum size of an IPv4 datagram minus 40 bytes. This value is sent during connection startup. This is also when TCP sliding windows are negotiated.

1. If the initial TCP sequence value from PC_Client is 0, why did eagle1.example respond with an acknowledgement of 1?

2. In eagle1.example.com, No. 8, What does the IP Flag value of 0x04 mean?

3. When PC_Client completes the TCP 3-way handshake, Wireshark Packet List No 9, what are the TCP flag states returned to eagle1.example.com?

Task 4: Complete the Final Analysis.

Step 1: Match the Wireshark output to the process.

It has taken a total of nine datagrams sent between PC_Client, DNS server, Gateway, and eagle1.example.com before PC_Client has sufficient information to send the original web client request to eagle1.example.com. This is shown in Wireshark Packet List No. 10, where PC_Client sent a web protocol GET request.

1. Fill in the correct Wireshark Packet List number that satisfies each of the following missing entries:
 - a. The TCP segment cannot be constructed because the acknowledgement field is blank. A TCP 3-way handshake with eagle1.example.com must first be completed. _____

- b. The TCP 3-way handshake cannot occur because PC_Client does not know the IP address for eagle1.example.com. This is resolved with a DNS request from PC_Client to the DNS the server. _____
 - c. The DNS server cannot be queried because the MAC address for the DNS server is not known. The ARP protocol is broadcast on the LAN to discover the MAC address for the DNS server. _____
 - d. The MAC address for the gateway to reach eagle1.example.com is unknown. The ARP protocol is broadcast on the LAN to learn the destination MAC address for the gateway. _____
1. Wireshark Packet List No. 11 is an acknowledgement from eagle1.example.com to the PC_Client GET request, Wireshark Packet List No. 10.
 2. Wireshark Packet List No. 12, 13 and 15 are TCP segments from eagle1.example.com. Wireshark Packet List No. 14 and 16 are ACK datagrams from PC_Client.
 3. To verify the ACK, highlight Wireshark Packet List No. 14. Next, scroll down to the bottom of the detail list window, and expand the [SEQ/ACK analysis] frame. The ACK datagram for Wireshark Packet List No. 14 is a response to which datagram from eagle1.example.com? _____
 4. Wireshark Packet List No. 17 datagram is sent from PC_Client to eagle1.example.com. Review the information inside the [SEQ/ACK analysis] frame. What is the purpose of this datagram?
 5. When PC_Client is finished, TCP ACK and FIN flags are sent, shown in Wireshark Packet List No. 18. eagle1.example.com responds with a TCP ACK, and the TCP session is closed.

Step 2: Use Wireshark TCP Stream.

Analyzing packet contents can be a daunting experience, time consuming and error prone. Wireshark includes an option that constructs the TCP Stream in a separate window. To use this feature, first select a TCP datagram from the Wireshark Packet List. Next, select Wireshark menu options Analyze | Follow TCP Stream. A window similar to Figure 9 will be displayed.

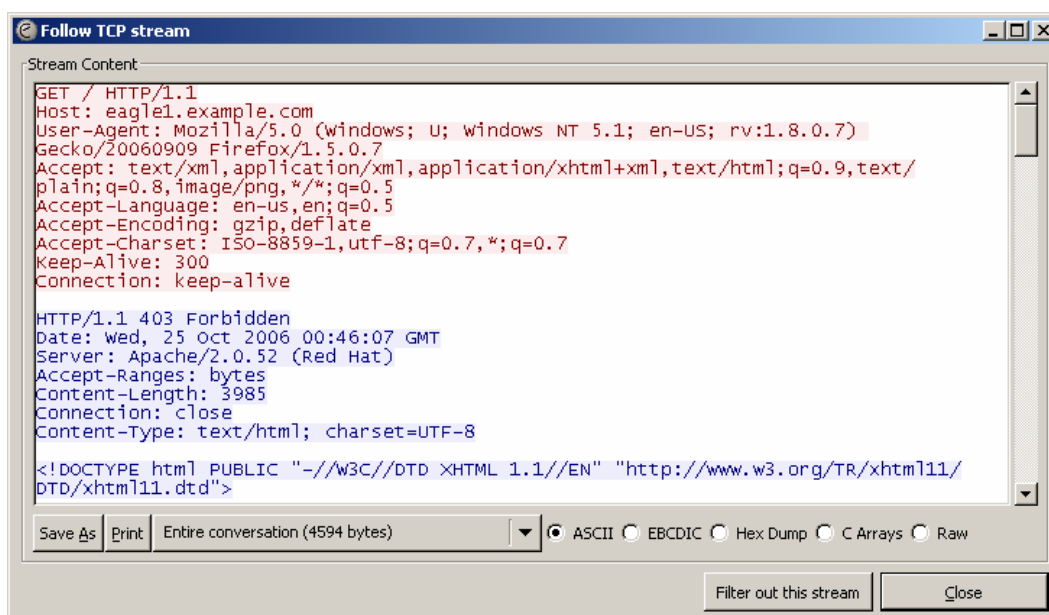


Figure 9. Output of the TCP stream.

Task 5: Conclusion

Using a network protocol analyzer can serve as an effective learning tool for understanding critical elements of network communication. Once the network administrator is familiar with communication protocols, the same protocol analyzer can become an effective troubleshooting tool when there is network failure. For example, if a web browser could not connect to a web server there could be multiple causes. A protocol analyzer will show unsuccessful ARP requests, unsuccessful DNS queries, and unacknowledged packets.

Task 6: Summary

In this exercise the student has learned how communication between a web client and web server communicate. Behind-the-scene protocols such as DNS and ARP are used to fill in missing parts of IP packets and Ethernet frames, respectively. Before TCP session can begin, the TCP 3-way handshake must build a reliable path and supply both communicating ends with initial TCP header information. Finally, the TCP session is destroyed in an orderly manner with the client issuing a TCP FIN flag.