



CISCO NETWORKING ACADEMY PROGRAM



CCNA 1:

Networking Basics v3.1

Student Lab Manual

This document is exclusive property of Cisco Systems, Inc. Permission is granted to print and copy this document for non-commercial distribution and exclusive use by instructors in the CCNA 1: Networking Basics course as part of an official Cisco Networking Academy Program.





Lab 1.1.2 PC Hardware

Objective

- Become familiar with the basic peripheral components of a PC computer system.
- Identify PC connections including network attachment.
- Examine the internal PC configuration and identify major components.
- Observe the boot process for the Windows operating system.
- Use the Control Panel to find out information about the PC.

Background

Knowing the components of a PC is valuable when troubleshooting. This knowledge is also important to success in the networking field.

Before beginning, the instructor or lab assistant should have a typical desktop PC available with all peripherals. Peripherals include the keyboard, monitor, mouse, speakers or head phones, a network interface card (NIC), and a network cable. The system unit cover should be removed. If the cover is not removed, the tools should be provided to remove it. Work individually or in teams. In addition, the instructor needs to identify the location of the A+ or PC hardware training materials.

Step 1 Examine the computer and peripheral components

Examine the computer and peripheral components both front and back.

Note: The components and configuration of the PC may vary.

What are the manufacturer and model number of this computer?

Manufacturer:	
Model Number:	

What are the major external components of the PC including the peripherals?

Component Name	Manufacturer / Description / Characteristics
1.	
2.	
3.	
4.	
5.	

Step 2 Remove the PC system unit cover and examine internal components

List at least 8 major internal components inside the system unit. Use the procedure in step 5 to find the CPU and amount of RAM.

Component Name	Manufacturer / Description / Characteristics
1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	

Step 3 Assemble the PC components observe the boot process

Assemble the PC components, attach all peripherals, and boot the PC. Observe the boot process. The computer should boot to the Windows operating system. If the computer does not boot, contact the lab assistant. Observe the boot process.

Did the Windows operating system boot correctly? _____

Did the screen show how much memory there was as the system was booting? _____

Step 4 Gather basic information about the computer CPU and RAM

Gather basic information about the computer CPU and memory. The instruction to complete this step may vary slightly depending on the version of Windows. Consult with the instructor if lab assistance is required.

Click the **Start** button. Select **Settings** then **Control Panel**. Click on the **System** icon and then the **General** tab. View the information about the computer using the operating system.

What is the Central Processing Unit? _____

What is the speed in MHz of the CPU? _____

How much RAM is installed? _____

This concludes the lab. All equipment should be returned to the original state or as directed by the instructor.



Lab 1.1.6 PC Network TCP/IP Configuration

Objective

- Identify tools used to discover a computer network configuration with various operating systems.
- Gather information including connection, host name, Layer 2 MAC address and Layer 3 TCP/IP network address information.
- Compare network information to other PCs on the network.

Background

This lab assumes the use of any version of Windows. This is a non-destructive lab and can be done on any machine without concern of changing the system configuration.

Ideally, this lab is performed in a classroom or other LAN environment that connects to the Internet. This lab can be done from a single remote connection via a modem or DSL-type connection. The instructor will furnish IP addresses.

In the following instructions the lab runs twice. The two runs reflect the operating system differences between the Windows 95/98/ME systems and Windows NT/2000/XP systems. Students should perform the lab on both types of systems if possible.

Note: All users complete Step 1

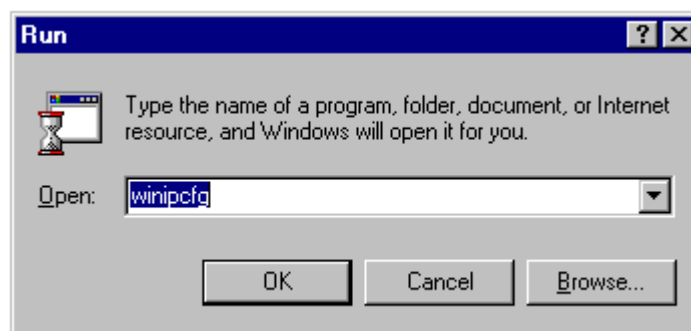
Step 1 Connect into the Internet

Establish and verify connectivity to the Internet. This ensures the computer has an IP address.

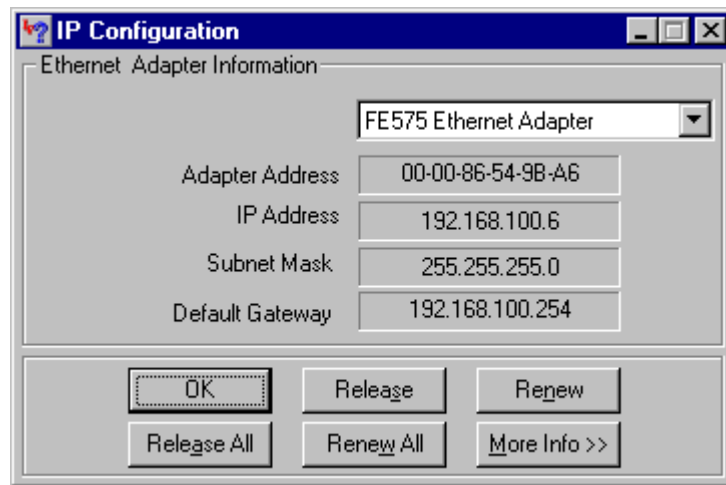
Note: Windows 95/98/Me users complete Steps 2 through 6.

Step 2 Gather basic TCP/IP configuration information

Using the taskbar, choose **Start** then **Run**. The following box will appear. Type `winiipcfg` and press the **Enter** key. `winiipcfg` spelling is critical while case is not. It is short for Windows IP Configuration.



This first screen shows the Adapter Address, or MAC address of the computer. The first screen also shows IP Address, Subnet Mask, and the Default Gateway. The following graphic shows the basic IP Configuration screen. Select the correct adapter if more than one is listed.



The IP address and the default gateway should be in the same network or subnet. Otherwise, this host would not be able to communicate outside the network. In the previous figure the subnet mask tells us that the first three octets must be the same to be in the same network. IP addressing will be discussed in Module 9.

Note: If this computer is on a LAN, the default gateway might not be seen if it is running behind a Proxy Server. Record the following information for this computer:

IP address: _____

Subnet Mask: _____

Default Gateway: _____

Step 3 Compare the TCP/IP configuration

If this computer is on a LAN, compare the information on several machines.

Are there any similarities? _____

What is similar about the IP addresses? _____

What is similar about the default gateways? _____

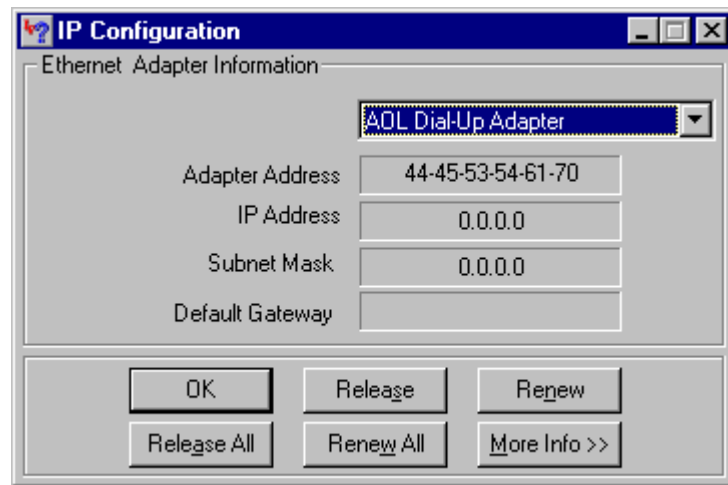
What is similar about the MAC addresses? _____

The IP addresses should share the same network portion. All machines in the LAN should share the same default gateway. While not a requirement, most LAN administrators try to standardize components like NICs. Therefore, all machines may share the first three Hex pairs in the adapter address. These three pairs identify the manufacturer of the adapter.

Record a couple of the IP Addresses

Step 4 Verify selection of network adapter

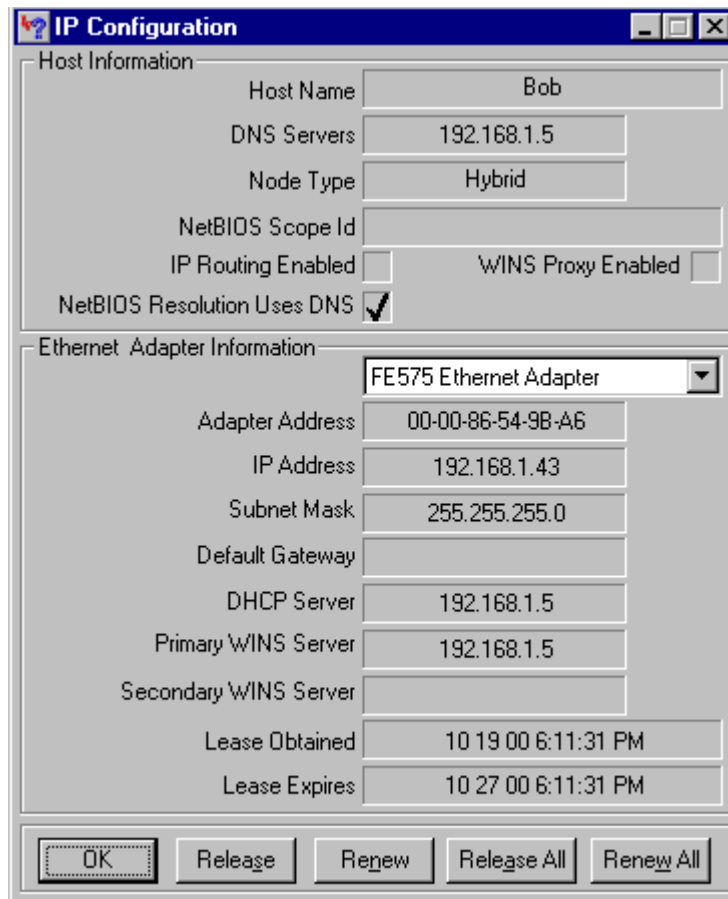
The adapter model of this computer should be displayed in the box at the top of the screen. Use the drop-down arrow in that box to see if there are any other configurations for this adapter, such as PPP. This could be true for a modem if this computer connects to the Internet with a dial-up account. On a server, it is possible to find another NIC or a machine with both a NIC and a modem. The following figure shows an AOL modem IP configuration screen. Notice that there is no IP address in the figure. This is what a home system could look like if the user did not log on to the Internet connection.



Be sure to return to the adapter that displays the NIC or modem data with an IP address

Step 5 Check additional TCP/IP configuration information

Click on the **More Info >>** button. The next figure shows the detailed IP Configuration screen.



The **More Info** button displays the Host Name, which includes the computer name and NetBIOS name. It also displays the DHCP server address, if used, and the date the IP lease starts and ends. Look over the remaining information. Entries for DNS and WINS servers may also be displayed. These entries are used in name resolution.

Write down the IP addresses of any servers listed: _____

Write down the computer Host Name: _____

Write down the Host Names of a couple of other computers: _____

Do all of the servers and workstations share the same network portion of the IP address as the student workstation? _____

Note: It would not be unusual for some or all of the servers and workstations to be in another network. It means that the default gateway of this computer is going to forward requests to the other network.

Step 6 Close the screen when finished examining network settings

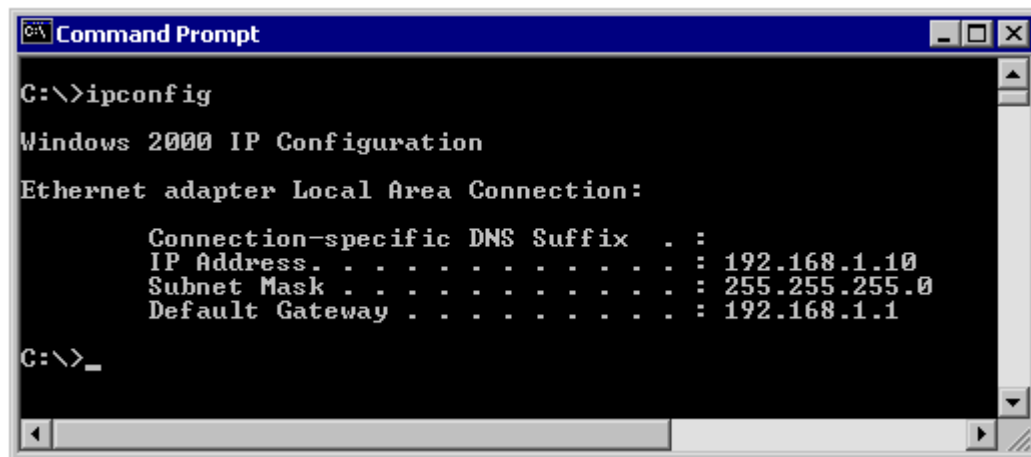
Repeat the previous steps as necessary to make sure that there are no problems in returning to, and interpreting, this screen.

Note: Windows NT/2000/XP users complete Steps 7 through 11.

Step 7 Gather TCP/IP configuration information

Use the Start menu to open the Command Prompt, an MS-DOS-like window. Press **Start > Programs > Accessories > Command Prompt** or **Start > Programs > Command Prompt**.

The following figure shows the Command screen. Type `ipconfig` and press the **Enter** key. The spelling of `ipconfig` is critical while case is not. It is short for IP Configuration.



```
Command Prompt
C:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.1.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.1.1

C:\>_
```

This first screen shows the IP address, subnet mask, and default gateway. The IP address and the default gateway should be in the same network or subnet, otherwise this host would not be able to communicate outside the network. In the figure the subnet mask tells us that the first three octets must be the same to be in the same network.

Note: If this computer is on a LAN, the default gateway might not be seen if it is running behind a Proxy Server. Record the following information for this computer.

Step 8 Record the following TCP/IP information for this computer

IP address: _____

Subnet Mask: _____

Default Gateway: _____

Step 9 Compare the TCP/IP configuration of this computer to others on the LAN

If this computer is on a LAN, compare the information of several machines.

Are there any similarities? _____

What is similar about the IP addresses? _____

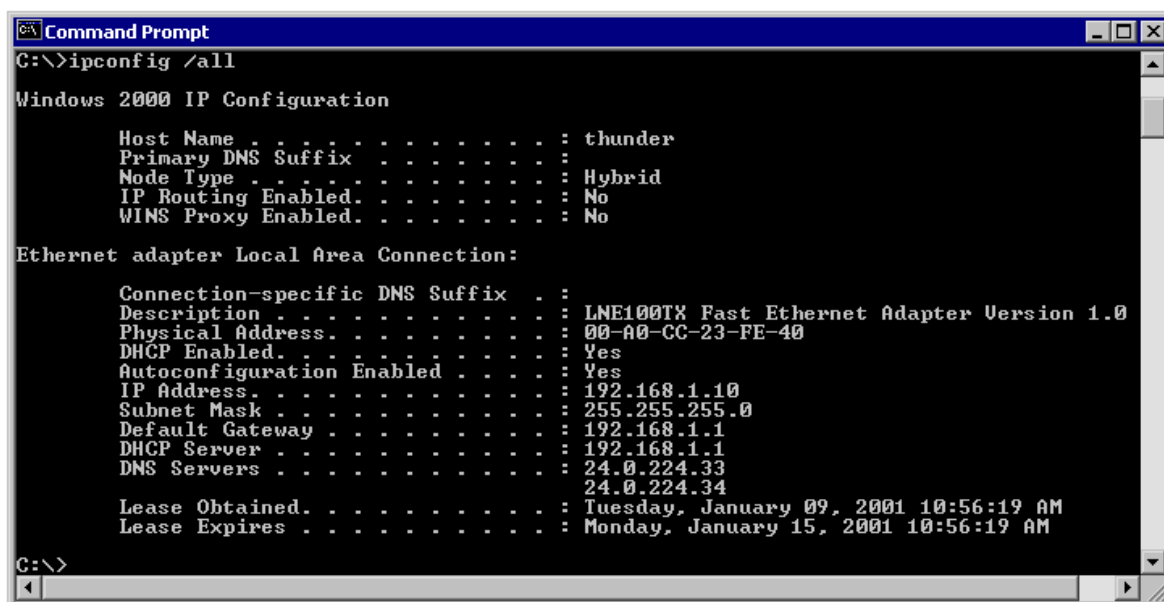
What is similar about the default gateways? _____

The IP addresses should share the same network portion. All machines in the LAN should share the same default gateway.

Record a couple of the IP Addresses:

Step 10 Check additional TCP/IP configuration information

To see detailed information, type `ipconfig /all` and press **Enter**. The figure shows the detailed IP configuration screen.



```
Command Prompt
C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . : thunder
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : LNE100TX Fast Ethernet Adapter Version 1.0
Physical Address. . . . . : 00-A0-CC-23-FE-40
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 24.0.224.33
                       24.0.224.34
Lease Obtained. . . . . : Tuesday, January 09, 2001 10:56:19 AM
Lease Expires . . . . . : Monday, January 15, 2001 10:56:19 AM

C:\>
```

The host name, including the computer name and NetBIOS name should be displayed. Also, the DHCP server address, if used, and the date the IP lease starts and ends should be displayed. Look over the information. Entries for the DNS, used in name resolution servers, may also be present.

The previous figure reveals that the router is performing both DHCP and DNS services for this network. This would likely be a small office or home office (SOHO) or small branch office implementation.

Notice the Physical Address (MAC) and the NIC model (Description).

In the LAN, what similarities about the Physical (MAC) Addresses are seen?

While not a requirement, most LAN administrators try to standardize components like NICs. Therefore, it would not be surprising to find all machines share the first three Hex pairs in the adapter address. These three pairs identify the manufacturer of the adapter.

Write down the IP addresses of any servers listed:

Write down the computer Host Name:

Write down the Host Names of a couple other computers:

Do all of the servers and workstations share the same network portion of the IP address as the student workstation? _____

It would not be unusual for some or all of the servers and workstations to be in another network. It means that the computer default gateway is going to forward requests to the other network.

Step 11 Close the screen

Close the screen when finished examining network settings.

Repeat the previous steps as necessary. Make sure that it is possible to return to and interpret this screen.

This concludes the lab.

Reflection

Based on observations, what can be deduced about the following results taken from three computers connected to one switch?

Computer 1

IP Address: 192.168.12.113

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Computer 2

IP Address: 192.168.12.205

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Computer 3

IP Address: 192.168.112.97

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Should they be able to talk to each other? Are they all on the same network? Why or why not? If something is wrong, what is most likely the problem?



Lab 1.1.7 Using ping and tracert from a Workstation

Objective

- Learn to use the TCP/IP Packet Internet Groper (**ping**) command from a workstation.
- Learn to use the Traceroute (**tracert**) command from a workstation.
- Observe name resolution occurrences using WINS and/or DNS servers.

Background

This lab assumes the use of any version of Windows. This is a non-destructive lab and can be done on any machine without concern of changing the system configuration.

Ideally, this lab is performed in a LAN environment that connects to the Internet. It can be done from a single remote connection via a modem or DSL-type connection. The student will need the IP addresses that were recorded in the previous lab. The instructor might also furnish additional IP addresses.

Note: Ping has been used in many DOS attacks and many school network administrators have turned off ping, echo reply, from the border routers. If the network administrator has turned off echo reply then it is possible for a remote host to appear to be offline when the network is operational.

Step 1 Establish and verify connectivity to the Internet

This ensures the computer has an IP address.

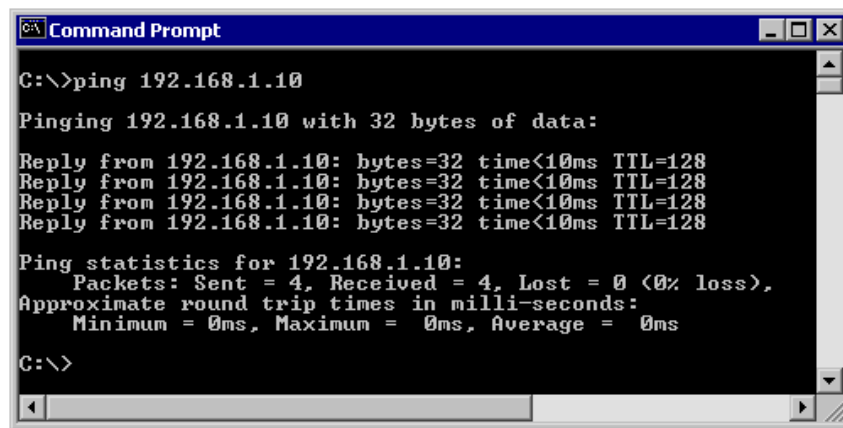
Step 2 Access the command prompt

Windows 95 / 98 / Me users – Use the Start menu to open the MS-DOS Prompt window. Press **Start > Programs > Accessories > MS-DOS Prompt** or **Start > Programs > MS-DOS**.

Windows NT / 2000 / XP users – Use the Start menu to open the Command Prompt window. Press **Start > Programs > Accessories > Command Prompt** or **Start > Programs > Command Prompt** or **Start > All Programs > Command Prompt**.

Step 3 ping the IP address of another computer

In the window, type **ping**, a space, and the IP address of a computer recorded in the previous lab. The following figure shows the successful results of **ping** to this IP address.



```
C:\>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128
Reply from 192.168.1.10: bytes=32 time<10ms TTL=128

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

C:\>
```

ping uses the ICMP echo request and echo reply feature to test physical connectivity. Since **ping** reports on four attempts, it gives an indication of the reliability of the connection. Look over the results and verify that the **ping** was successful. Is the **ping** successful? If not, perform appropriate troubleshooting. _____

If a second networked computer is available, try to **ping** the IP address of the second machine. Note the results. _____

Step 4 ping the IP address of the default gateway

Try to **ping** the IP address of the default gateway if one was listed in the last exercise. If the **ping** is successful, it means there is physical connectivity to the router on the local network and probably the rest of the world.

Step 5 ping the IP address of a DHCP or DNS servers

Try to **ping** the IP address of any DHCP and/or DNS servers listed in the last exercise. If this works for either server, and they are not in the network, what does this indicate?

Was the **ping** successful? _____

If not, perform appropriate troubleshooting.

Step 6 ping the Loopback IP address of this computer

Type the following command: **ping 127.0.0.1**

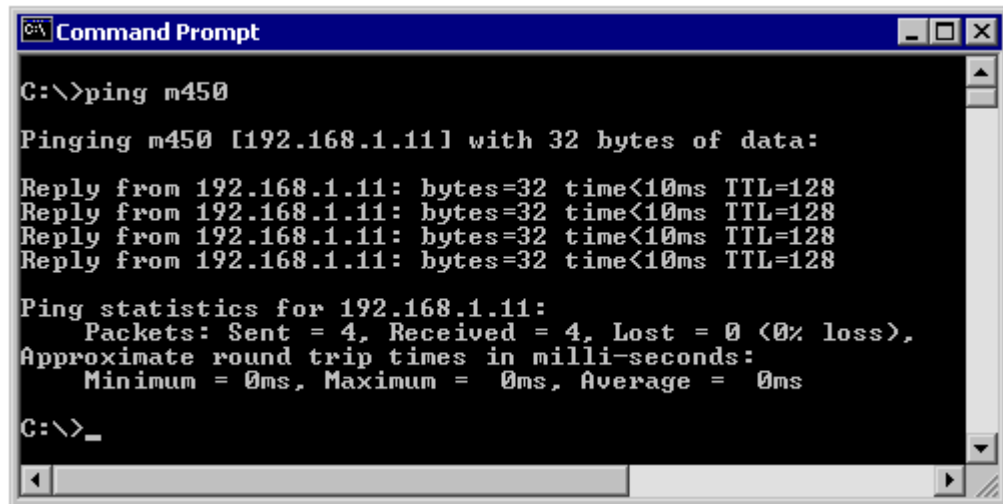
The 127.0.0.0 network is reserved for loopback testing. If the **ping** is successful, then TCP/IP is properly installed and functioning on this computer.

Was the **ping** successful? _____

If not, perform appropriate troubleshooting.

Step 7 ping the hostname of another computer

Try to **ping** the hostname of the computer that was recorded in the previous lab. The figure shows the successful result of the **ping** the hostname.



```
C:\>ping m450

Pinging m450 [192.168.1.11] with 32 bytes of data:

Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128
Reply from 192.168.1.11: bytes=32 time<10ms TTL=128

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

C:\>_
```

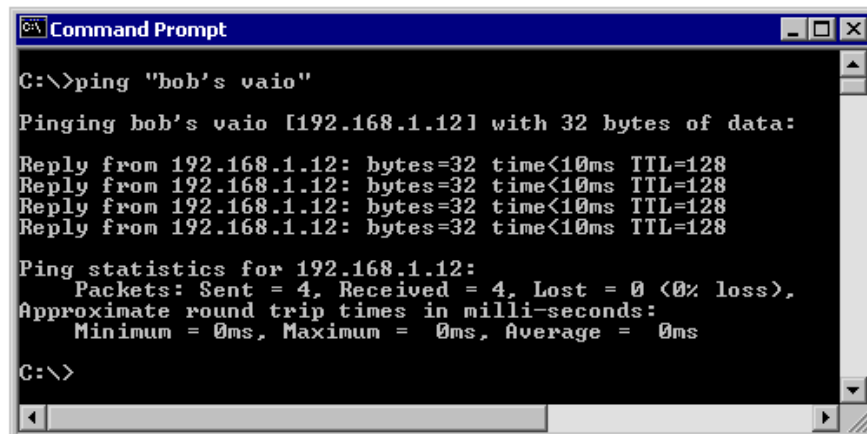
Look over the results. Notice that the first line of output shows the host name, m450 in the example, followed by the IP address. This means the computer was able to resolve the host name to an IP address. Without name resolution, the `ping` would have failed because TCP/IP only understands valid IP addresses, not names.

If the `ping` was successful, it means that connectivity and discovery of IP addresses can be done with only a hostname. In fact, this is how many early networks communicated. If successful, then `ping` a hostname also shows that there is probably a WINS server working on the network. WINS servers or a local "lmhosts" file resolve computer host names to IP addresses. If the `ping` fails, then chances are there is no NetBIOS name to IP addresses resolution running.

Note: It would not be uncommon for a Windows 2000 or XP networks to not support this feature. It is an old technology and often unnecessary.

If the last `ping` worked, try to `ping` the hostname of any another computer on the local network. The following figure shows the possible results.

Note: The name had to be typed in quotes because the command language did not like the space in the name.



```
C:\>ping "bob's vaio"

Pinging bob's vaio [192.168.1.12] with 32 bytes of data:

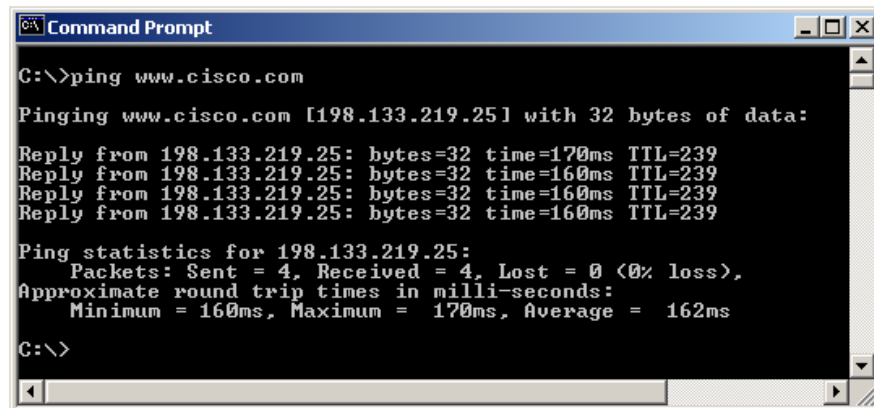
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128
Reply from 192.168.1.12: bytes=32 time<10ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Step 8 ping the Cisco web site

Type the following command: `ping www.cisco.com`



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

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:

Reply from 198.133.219.25: bytes=32 time=170ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239
Reply from 198.133.219.25: bytes=32 time=160ms TTL=239

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 160ms, Maximum = 170ms, Average = 162ms

C:\>
```

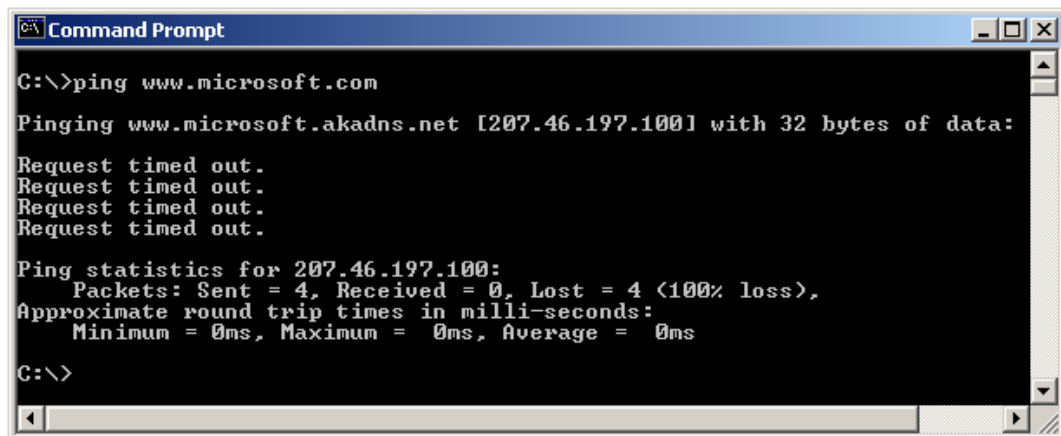
The first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP address. A Domain Name Service (DNS) server somewhere in the network was able to resolve the name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses.

Without this name resolution, the `ping` would have failed because TCP/IP only understands valid IP addresses. It would not be possible to use the web browser without this name resolution.

With DNS, connectivity to computers on the Internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks a DNS server higher in the Internet structure.

Step 9 ping the Microsoft web site

a. Type the following command: `ping www.microsoft.com`



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

Pinging www.microsoft.akadns.net [207.46.197.100] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.197.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

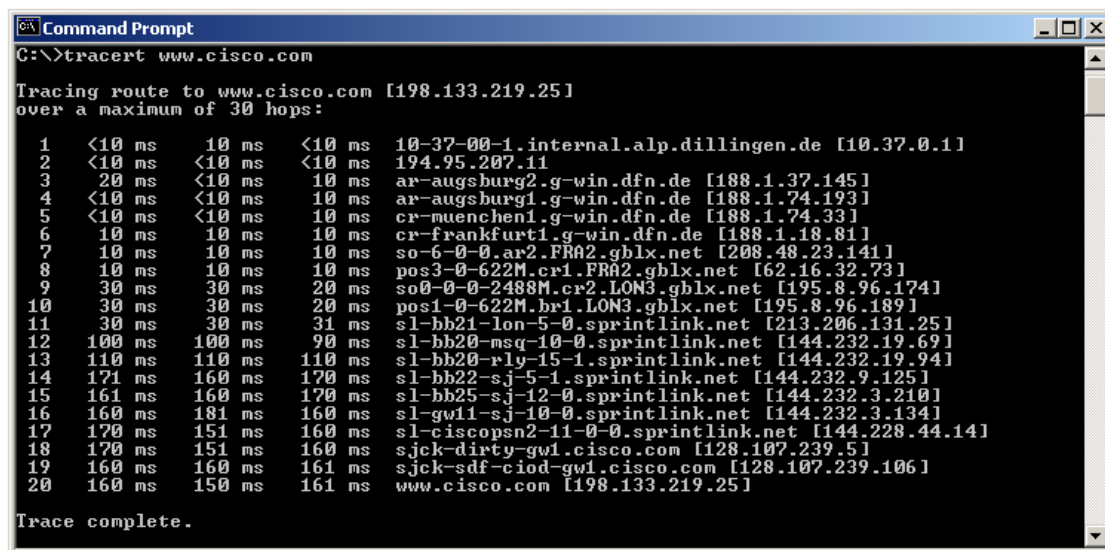
C:\>
```

Notice that the DNS server was able to resolve the name to an IP address, but there is no response. Some Microsoft routers are configured to ignore `ping` requests. This is a frequently implemented security measure.

`ping` some other domain names and record the results. For example, `ping www.msn.de`

Step 10 Trace the route to the Cisco web site

Type `tracert www.cisco.com` and press **Enter**.



```
Command Prompt
C:\>tracert www.cisco.com

Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:

  0  <10 ms    10 ms    <10 ms    10-37-00-1.internal.alp.dillingen.de [10.37.0.1]
  1  <10 ms    <10 ms    <10 ms    194.95.207.11
  2  20 ms     <10 ms    10 ms     ar-augsburg2.g-win.dfn.de [188.1.37.145]
  3  <10 ms    <10 ms    10 ms     ar-augsburg1.g-win.dfn.de [188.1.74.193]
  4  <10 ms    <10 ms    10 ms     cr-muenchen1.g-win.dfn.de [188.1.74.33]
  5  10 ms     10 ms     10 ms     cr-frankfurt1.g-win.dfn.de [188.1.18.81]
  6  10 ms     10 ms     10 ms     so-6-0-0.ar2.FRA2.gblx.net [208.48.23.141]
  7  10 ms     10 ms     10 ms     pos3-0-622M.cr1.FRA2.gblx.net [62.16.32.73]
  8  30 ms     30 ms     20 ms     so0-0-0-2488M.cr2.LON3.gblx.net [195.8.96.174]
  9  30 ms     30 ms     20 ms     pos1-0-622M.br1.LON3.gblx.net [195.8.96.189]
 10  30 ms     30 ms     31 ms     sl-bb21-lon-5-0.sprintlink.net [213.206.131.25]
 11 100 ms    100 ms    90 ms     sl-bb20-msq-10-0.sprintlink.net [144.232.19.69]
 12 110 ms    110 ms    110 ms    sl-bb20-rlg-15-1.sprintlink.net [144.232.19.94]
 13 171 ms    160 ms    170 ms    sl-bb22-sj-5-1.sprintlink.net [144.232.9.125]
 14 161 ms    160 ms    170 ms    sl-bb25-sj-12-0.sprintlink.net [144.232.3.210]
 15 160 ms    181 ms    160 ms    sl-gw11-sj-10-0.sprintlink.net [144.232.3.134]
 16 170 ms    151 ms    160 ms    sl-ciscopsn2-11-0-0.sprintlink.net [144.228.44.14]
 17 170 ms    151 ms    160 ms    sjck-dirty-gw1.cisco.com [128.107.239.5]
 18 160 ms    160 ms    161 ms    sjck-sdf-ciod-gw1.cisco.com [128.107.239.106]
 19 160 ms    150 ms    161 ms    www.cisco.com [198.133.219.25]
 20

Trace complete.
```

`tracert` is TCP/IP abbreviation for trace route. The preceding figure shows the successful result when running `tracert` from Bavaria in Germany. The first output line shows the FQDN followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers the `tracert` requests had to pass through to get to the destination.

`tracert` uses the same echo requests and replies as the `ping` command but in a slightly different way. Observe that `tracert` actually contacted each router three times. Compare the results to determine the consistency of the route. Notice in the above example that there were relatively long delays after router 11 and 13, possibly due to congestion. The main thing is that there seems to be relatively consistent connectivity.

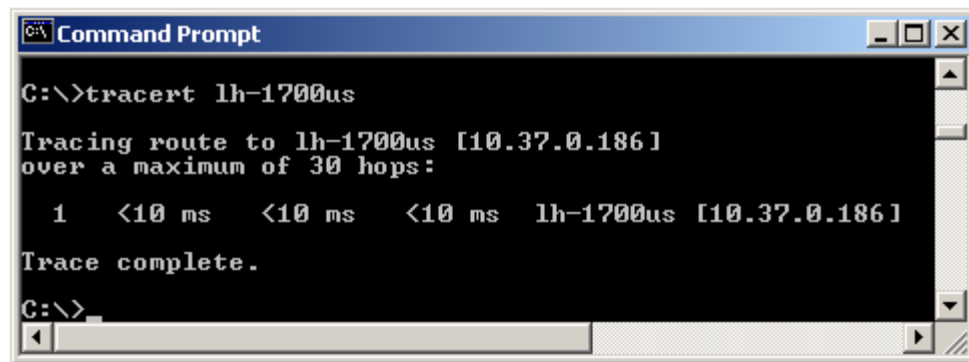
Each router represents a point where one network connects to another network and the packet was forwarded through.

Step 11 Trace other IP addresses or domain names

Try `tracert` on other domain names or IP addresses and record the results. An example is `tracert www.msn.de`.

Step 12 Trace a local host name or IP address

Try using the `tracert` command with a local host name or IP address. It should not take long because the trace does not pass through any routers.



```
C:\>tracert lh-1700us

Tracing route to lh-1700us [10.37.0.186]
over a maximum of 30 hops:

  1  <10 ms  <10 ms  <10 ms  lh-1700us [10.37.0.186]

Trace complete.

C:\>
```

This concludes the lab.

Reflection

If the above steps are successful and `ping` or `tracert` can verify connectivity with an Internet Web site, what does this indicate about the computer configuration and about routers between the computer and the web site? What, if anything, is the default gateway doing?



Lab 1.1.8 Web Browser Basics

Objective

- Learn how to use a web browser to access Internet sites.
- Become familiar with the concept of a URL.
- Use a search engine to locate information on the Internet.
- Access selected web sites to learn the definitions of networking terms.
- Use hyperlinks to jump from the current web site to other web sites.

Background

A web browser is a very powerful tool that many people use everyday to surf around different sites on the World Wide Web. A web browser can help find anything from airline flight information to the directions on how to get to a place. A browser is a client application program or software that is loaded on the PC to gain access to the Internet and local web pages.

The web site name, such as **www.cisco.com**, is a Universal Resource Locator (URL). This URL points to the World Wide Web server (WWW) in the Cisco domain (CISCO) under the Commercial domain (COM).

When the URL is typed, the browser makes a request of a Domain Name Server (DNS) to convert the URL to an IP address. The IP address is used to contact the site.

The browser can be used to access search engines by typing the name in the address bar. Some search engines include www.yahoo.com, www.excite.com, www.lycos.com and www.google.com.

There are several web sites that provide definitions of networking and computer related terms and acronyms. These can be used to help learn more about networking and to do research on the Internet. Two of these are www.whatis.com and www.webopedia.com.

Most web sites contain hyperlinks. Hyperlinks are words that are underlined and highlighted. By clicking on a hyperlink a user "jumps" to another page on the current site or to a page on another web site.

A computer configured with an up-to-date browser and access to the Internet is required.

Step 1 Start the web browser

If using a modem to make the connection, dial the number before starting the web browser. What version of Netscape or Internet Explorer is being used?

Step 2 Identify the location or address field

After the browser has been started, click and highlight the **Location** field in Netscape or the **Address** field in Internet Explorer in the toolbar at the top of the page. Press the **Delete** key to delete the current address.

Step 3 Type in a Web URL

Type in www.cisco.com and press **Enter**. This is how to navigate from one site to another on the World Wide Web (WWW).

Step 4 Type in another Web URL

To load a new page, type in a new URL such as www.cnn.com. Notice the status on the bottom bar of the browser. What does it say? _____

Step 5 Use the browser management buttons

Each of the buttons on top of the browser has a function. If the mouse is positioned over a button a box will appear identifying the button.

Click on the **Back** button. What did it do? _____

Click on the **Forward** button. Does it return to the CNN Web site? _____

Try clicking on the **Reload** or **Refresh** button. What do they do?

Type www.microsoft.com and press **Enter**. Click on the **Stop** button as the window is loading. What happens?

Step 6 Use a search engine

Type the URL for a search engine such as www.google.com. Search for the word **browser**. What was the result?

Step 7 Access networking terms definitions web sites

Enter the URL for www.webopedia.com. Enter the keyword of **browser**. What was the result?

What hyperlinks were available?

Enter the URL for www.whatis.com. Look up the keyword of **DNS**. Click on the Exact Match for DNS under **whatis.com terms**. What does it say about DNS?

This concludes the lab.

Reflection

Identify a way to navigate from one site to another.

If the same graphics or text is seen the next time the NBA site is visited, what should be done to ensure that updated news is seen?



Lab 1.1.9 Basic PC/Network Troubleshooting Process

Objective

- Learn the proper sequence for troubleshooting computer and network problems.
- Become familiar with the more common hardware and software problems.
- Given a basic problem situation, be able to troubleshoot and resolve the problem.

Background

The ability to effectively troubleshoot computer related problems is an important skill. The process of identifying the problem and solving it requires a systematic step-by-step approach. This lab will introduce some basic hardware and software related problems to solve. This lab will assist in becoming more familiar with PC components and the software required to use the Cisco curriculum. The process of solving a problem is fairly straightforward. Some of the suggestions here are more than what will be required to solve basic hardware and software problems. They will help provide a framework and guidelines when more complex problems arise. A list of sample problems to be introduced is provided in the instructor's version of the lab.

The Eight Basic Steps for PC and Network Troubleshooting Process

Step 1 Define the problem

Describe what is happening or not happening using proper terminology. For example: The PC cannot get to the Internet, or the PC cannot print.

Step 2 Gather the facts

Observe the symptoms and try to characterize or identify the source of the problem:

- Is it hardware related, check for lights and noises. Is it software related, are there errors on screen?
- Does the problem affect this computer or user only, or are others also impacted?
- Does it affect this software only, or more than one application?
- Is this the first time the problem has happened or has it happened before?
- Was anything on the PC changed recently?
- Get the opinions of others who may have more experience.
- Check web sites and troubleshooting knowledge databases.

Step 3 Consider the possibilities

Use the facts gathered. Identify one or more possible causes and potential solutions. Rank solutions in order of the most likely to the least likely cause.

Step 4 Create an action plan

Develop a plan that involves the single most likely solution. The other options can be tried if the original solution fails. Consider the following in the development of a plan:

- Check the simplest possible causes first. Is the power turned on or plugged in?
- Verify hardware first then software.
- If it is a network problem start at Layer 1 of the OSI model and work up the Layers. Studies show the majority of problems occur at Layer 1.
- Can substitution be used to isolate the problem? If the monitor does not work it could be the monitor, video adapter or cables. Try another monitor to see if it corrects the problem.

Step 5 Implement the plan

Make the change(s) from the plan to test the first possible solution.

Step 6 Observe the results

If the problem is solved, go on to document the solution. Double check to make sure everything still works.

If the problem is not resolved restore the changes and return to the plan to try the next solution. If this change is not reversed, it will be unclear whether the problem was a later change or the combination of two changes.

Step 7 Document the results

Always document the results to assist in solving similar problems. Documentation also helps to develop a documentation history for each device. If part of the devices are going to be replaced it might be nice to know if any are frequent sources of trouble or if they have recently been reconditioned.

Step 8 Introduce problems and troubleshoot

Work in teams of two. The desired goal will be to run one of the videos or movies from the on-line curriculum or the CD. Each team member solving the problem should fill in the table based on the symptoms observed, problems identified, and solutions to the problem.

Team member A, or the instructor:

1. Select two problems from a list of common hardware and software related problems.
2. Introduce the problems into the computer.
3. Create the hardware or software related problems with the computer while the other is out of the room.
4. Turn off the computer and monitor.

Team member B:

1. Identify the problems.
2. Correct the problems.

Switch places and go through the steps again.

Team Member A

	Symptom observed	Problem identified	Solution
1 st problem			
2 nd problem			

Team Member B

	Symptom observed	Problem identified	Solution
1 st problem			
2 nd problem			

This concludes the lab.



Lab 1.2.5 Decimal to Binary Conversion

Objective

- Learn to convert decimal values to binary values.
- Practice converting decimal values to binary values.

Background

Knowing how to convert decimal values to binary values is valuable when converting human readable IP addresses in dotted decimal format to machine-readable binary format. This is normally done for calculation of subnet masks and other tasks. The following is an example of an IP address in 32-bit binary form and dotted decimal form.

Binary IP Address: 11000000.10101000.00101101.01111001

Decimal IP Address: 192.168.45.121

A tool that makes the conversion of decimal values to binary values simple is the following table. The first row is created by counting right to left from one to eight, for the basic eight bit positions. The table will work for any size binary value. The value row starts with one and doubles, Base 2, for each position to the left.

Position Value	8	7	6	5	4	3	2	1
	128	64	32	16	8	4	2	1

128	207
	128
64	79
	64
8	15
	8
4	7
	4
2	3
	2
	1

The same conversion table and simple division can be used to convert binary values to decimal values.

Steps

To convert 207 to binary:

1. Start with the digit farthest to the left. Determine if the decimal value can be divided by it. Since it will go one time, put a 1 in row three of the conversion table under the 128 value and calculate the remainder, 79.
2. Since the remainder can be divided by the next value, 64, put a 1 in row three under the 64 value of the table.
3. Since the remainder cannot be divided by either 32 or 16, put 0s in row three of our table under the 32 and 16 values.

4. Continue until there is no remainder.
5. If necessary, use row four to check the work.

Position	8	7	6	5	4	3	2	1	
Value	128	64	32	16	8	4	2	1	
	1	1	0	0	1	1	1	1	
	128	64			8	4	2	1	= 207

6. Convert the following decimal values to binary values:

a. 123 _____

b. 202 _____

c. 67 _____

d. 7 _____

e. 252 _____

f. 91 _____

g. 116.127.71.3 _____

h. 255.255.255.0 _____

i. 192.143.255.255 _____

j. 12.101.9.16 _____

This concludes the lab.



Lab 1.2.6 Binary to Decimal Conversion

Objective

- Learn the process of converting binary values to decimal values.
- Practice converting binary values to decimal values.

Background

The following is an example of an IP address in 32-bit binary form and dotted decimal form.

Binary IP Address: 11000000.10101000.00101101.01111001
Decimal IP Address: 192.168.45.121

Binary data is made up of ones and zeros. Ones represent on and zeros represent off. Binary data can be grouped in varying increments, 110 or 1011. In TCP/IP binary data is usually grouped in eight digit groups called a Byte.

A Byte, 8 bits, can range from 00000000 to 11111111 creating 256 combinations with decimal values ranging from 0 to 255. IP addressing uses 4 bytes, or 32 bits, to identify both the network and specific device. The specific device can be a node or host. The example at the beginning of this lab is an example of an IP address in both binary decimal formats.

A tool that makes the conversion of binary to decimal values simple is the following table. The first row is created by counting right to left from one to eight for the basic eight bit positions. The table will work for any size binary value. The value row starts with one and doubles, base 2, for each position to the left.

Position Value	8	7	6	5	4	3	2	1
	128	64	32	16	8	4	2	1

Steps

1. Enter the binary bits in row three. For example 10111001
2. Put the decimal values in row four only for the third row 1s. Technically the row two values are being multiplied by row three.
3. Now just add row four across.

Position Value	8	7	6	5	4	3	2	1
	128	64	32	16	8	4	2	1
	1	0	1	1	1	0	0	1
	128		32	16	8			1

= 185

4. Convert the following binary values to decimals:

a. 1110 _____

b. 100110 _____

c. 11111111 _____

d. 11010011 _____

e. 01000001 _____

f. 11001110 _____

g. 01110101 _____

h. 10001111 _____

i. 11101001.00011011.10000000.10100100

j. 10101010.00110100.11100110.00010111



Lab 1.2.8 Hexadecimal Conversions

Objective

- Learn the process to convert hexadecimal values to decimal and binary values.
- Learn the process to convert decimal and binary values to hexadecimal values.
- Practice converting between decimal, binary and hexadecimal values.

Background / Preparation

The Hexadecimal (Hex) number system is used to refer to the binary numbers in a NIC or IPv6 address. The word hexadecimal comes from the Greek word for 16. Hexadecimal is often abbreviated "0x", zero and lower case x. Hex numbers use 16 unique digits to display any combination of eight binary digits as only two hexadecimal digits.

A Byte, or 8 bits, can range from 00000000 to 11111111. A Byte can create 256 combinations with decimal values ranging from 0 to 255 or Hex values 0 to FF. Each Hex value represents only four binary bits. The alpha (A-F) values are not case sensitive.

A tool that makes the conversion of hexadecimal to decimal values simple is the following table. Use the same techniques as covered in binary to decimal conversions. The first row is the two Hex positions. The value row starts as 1 and 16, base 16, for each position to the left.

Position
Value

2	1
16	1

Dec	Hex	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Note: Steps are provided at the end of this lab in the use of the Windows Scientific Calculator to check the work.

Steps for Hex to decimal conversion

1. Break the Hex value into pairs. Start at the right side. For example 77CE becomes 77 and CE. Insert a zero in the first position if necessary to complete the first pair.
2. Put each Hex pair in row three. The value in parenthesis is the decimal value of A-F.
3. To get the decimal values in row four, multiply the row two values by row three.

4. Now just add row four across.

Position	2	1	
Value	16	1	
	7	7	
	112	7	= 119

Position	2	1	
Value	16	1	
	C(12)	E(14)	
	192	14	= 206

Steps for decimal to Hex conversion

1. To be valid for the purpose of this lab, the decimal value will be between 0 and 256. The first Hex value is derived by dividing the decimal value by 16. If the value is greater than 9 it will need to be put in Hex form A-F.
2. The second value is the remainder from step 1. If the value is greater than 9 it will need to be put in Hex form A-F.
3. For example, 209 divided by 16 is 13 with a remainder of 1. 13 equals D in Hex. Therefore, 209 equals D1.

Steps for Hex to binary conversion

1. This is the easiest conversion. Remember that each Hex value converts to four binary bits, so work right to left.
2. For example, to convert **77AE** to binary. Start with E. Use the table at the beginning of this lab to go directly to binary. The other alternative is to convert the value to decimal, E = 14, and then use the last four positions of the table used in the decimal to binary conversions.

14 divided by 8 is 1 with a remainder of 6.

6 divided by 4 is 1 with a remainder of 2.

2 divided by 2 is 1 with no remainder.

Add zeros if necessary to end up with four bits.

Position	4	3	2	1	
Value	8	4	2	1	
	1	1	1	0	
	8	4	2		= 14

3. Using the same technique, A becomes 1010 and the total so far is 10101110.

Position	4	3	2	1	
Value	8	4	2	1	
	1	0	1	0	
	8		2		= 10

4. Using the same technique, the two 7s each become 0111 and the total is 01110111.10101110.

Position	4	3	2	1
Value	8	4	2	1
	0	1	1	1
		4	2	1

= 7

Steps for binary to Hex conversion

- Each Hex value equals four binary bits. Start by breaking the binary value into 4-bit units from right to left. Add any leading zeros required to end up with all 4-bit values. 01101110. 11101100 would become 0110 1110 1110 1100.
- Use the table at the beginning of this lab to go directly to Hex. The other alternative is to convert each 4-bit binary value to decimal, 0-15. Then convert the decimal to Hex, 0-F.

Position	4	3	2	1
Value	8	4	2	1
	1	1	0	0
	8	4		

= 12 or C

Position	4	3	2	1
Value	8	4	2	1
	1	1	1	0
	8	4	2	

= 14 or E

3. The result is 6E-EC.

Practice

Convert the following values to the other two forms:

	Decimal	Hex	Binary
1		a9	
2		FF	
3		Bad1	
4		E7-63-1C	
5	53		
6	115		
7	19		
8	212.65.119.45		
9			10101010

10			110
11			11111100.00111100
12			00001100.10000000.11110000.11111111

Checking conversions with the Windows Calculator

It is important to be able to perform the previous calculations manually. However, to check the work using the Windows Calculator applet, access the Calculator. Click **Start > Programs > Accessories** and then **Calculator**. Click on the **View** menu to make sure that the calculator is in **Scientific** mode. Click on the button for the type of number to be entered, Hex, Dec or Bin. Enter the number in that form. To convert from one form to another, click on one of the alternate buttons.



Lab 2.3.6 OSI Model and TCP/IP Model

Objective

- Describe the four layers of the TCP/IP model.
- Relate the seven layers of the OSI model to the four layers of the TCP/IP model.
- Name the primary TCP/IP protocols and utilities that operate at each layer.

Background

This lab will help to develop a better understanding of the seven layers of the OSI model. Specifically as they relate to the most popular functioning networking model in existence, the TCP/IP model. The Internet is based on TCP/IP. TCP/IP has become the standard language of networking. However, the seven layers of the OSI model are the ones most commonly used to describe and compare networking software and hardware from various vendors. It is very important to know both models and be able to relate or map the layers of one to the other. An understanding of the TCP/IP model and the protocols and utilities that operate at each layer is essential when troubleshooting.

Steps

1. Use the table below to compare the OSI layers with the TCP/IP protocol stack. In column two, indicate the proper name for each of the seven layers of the OSI model corresponding to the layer number. List the TCP/IP layer number and its correct name in the next two columns. Also list the term used for the encapsulation units, the related TCP/IP protocols and utilities that operate at each TCP/IP layer. More than one OSI layer will be related to certain TCP/IP layers.

OSI comparison with TCP/IP Protocol Stack

OSI #	OSI Layer Name	TCP/IP #	TCP/IP Layer Name	Encapsul. Units	TCP/IP Protocols at Each TCP/IP Layer	TCP Utilities
7						
6						
5						
4						
3						
2						
1						



Lab 2.3.7 OSI Model Characteristics and Devices

Objective

- Name the seven layers of the OSI model, in order. Use a mnemonic.
- Describe the characteristics, functions and keywords relating to each layer.
- Describe the packaging units used to encapsulate each layer.
- Name the physical devices or components that operate at each layer.

Background

This lab will help to develop a better understanding of the seven layers of the OSI model. Specifically as they relate to the most popular functioning networking model in existence, the TCP/IP model. The Internet is based on TCP/IP. TCP/IP has become the standard language of networking. However, the seven layers of the OSI model are the ones most commonly used to describe and compare networking software and hardware from various vendors. It is very important to know both models and be able to relate or map the layers of one to the other. An understanding of the TCP/IP model and the protocols and utilities that operate at each layer is essential when troubleshooting.

Steps

1. List the seven layers of the OSI model from the top to the bottom. Give a mnemonic word for each layer that can help you remember it. Then list the keywords and phrases that describe the characteristics and function of each.

Layer #	Name	Mnemonic	Key Words and Description of Function
7			
6			
5			
4			
3			
2			
1			

2. List the seven layers of the OSI model and the encapsulation unit used to describe the data grouping at each layer. Also list the networking devices that operate at each layer, if applicable.

Layer #	Name	Encapsulation Unit or Logical Grouping	Devices or Components that Operate at this Layer
7			
6			
5			
4			
3			
2			
1			

Lab 3.1.1 Safe Handling and Use of a Multimeter



Objective

- Learn how to use and handle a multimeter correctly.

Background

A multimeter is a powerful electrical testing tool that can detect voltage levels, resistance levels, and open or closed circuits. It can check both alternating current (AC) and direct current (DC) voltage. Open and closed circuits are indicated by resistance measurements in Ohms. Each computer and networking device consists of millions of circuits and small electrical components. A multimeter can be used to debug electrical problems within a computer or networking device, or with the media between networking devices.

Prior to starting the lab, the teacher or lab assistant should have one multimeter available for each team, and various batteries for testing. Work in teams of two. The following resources will be required:

- A digital multimeter. A Fluke 110 Series, 12B or similar for each team
- A manual for the multimeter
- A battery for each team to test. For example, a 9v, 1.5V or lantern.

Note: The multimeter is a sensitive piece of electronic test equipment. Do not drop it or handle it carelessly. Be careful not to accidentally nick or cut the red or black wire leads, called probes.

Because it is possible to check high voltages, extra care should be taken to avoid electrical shock.

Step 1

Insert the red and black leads into the proper jacks on the meter.

- a. The black probe should go in the COM jack and the red probe should go in the + (plus) jack.

Step 2

Turn on the multimeter. Click or turn to the on button.

- a. What is the model of multimeter?

- b. What action must be taken to turn the meter on?

Step 3

Switch or turn to different measurements. For example, voltage, and ohms.

- a. How many different switch positions does the multimeter have? _____
- b. What are they?

Step 4

Switch or turn the multimeter to the voltage measurement.

- a. What is the symbol for this? _____

Step 5

Put the tip of the red, positive lead on the positive side of a battery. Put the tip of the black, negative, lead on the other end of a battery.

- a. Is any number showing up on the multimeter? _____ If not, make sure to switch to the correct type of measurement. For example Vol, voltage, or V. If the voltage is negative, reverse the leads.

Reflection:

1. Name one thing that should not be done to a multimeter. _____
2. Name one important function of a multimeter. _____
3. If a voltage is negative when measuring a battery, what is wrong? _____

Lab 3.1.2 Voltage Measurement



Objective

- Demonstrate the ability to measure voltage with the multimeter safely.

Background

The digital multimeter is a versatile testing and troubleshooting device. This lab covers both direct current (DC) and alternating current (AC) voltage measurements. Voltage is measured in either AC or DC volts, indicated by a V. Voltage is the pressure that moves electrons through a circuit from one place to another. Voltage differential is essential to the flow of electricity. The voltage differential between a cloud in the sky and the earth is what causes lightning to strike.

Note: It is very important to be careful when taking voltage measurements to avoid an electrical shock.

Direct current (DC): DC voltage rises to a set level and then stays at that level and flows in one direction, positive or negative. Batteries produce DC voltage and are commonly rated at 1.5v or 9v and 6v. Typically, the battery in a car or truck is a 12v battery. When an electrical “load” such as a light bulb or motor is placed between the positive (+) and negative (-) terminals of a battery, electricity flows.

Alternating current (AC): AC voltage rises above zero, positive, and then falls below zero, negative. AC voltage changes direction very rapidly. The most common example of AC voltage is the wall outlet in a home or business. In North America, these outlets provide approximately 120 volts of AC directly to any electrical appliance that is plugged in. Examples of appliances are a computer,

toaster, or television. Some devices, such as small printers and laptop computers, have a small black box called a transformer, that plugs into a 120V AC wall outlet. The transformer converts the AC voltage to DC voltage for use by the device. Some AC outlets can provide a higher voltage of 220V for use by devices and equipment with heavier requirements, such as clothes dryers and arc welders.

Prior to starting the lab, the teacher or lab assistant should have one multimeter available for each team of students, and various items for testing voltage. Work in teams of two. The following resources will be required:

- Fluke 110, 12B, or equivalent multimeter
- An assortment of batteries: A cell, C cell, D cell, 9 Volts, 6 V lantern
- Duplex wall outlet, typically 120v
- Power supply for laptop or other networking electrical device

The following resources are optional:

- A lemon with a galvanized nail stuck in one side and a piece of uninsulated copper wire stuck in the opposite side
- Solar cell with leads attached
- Homemade generator, wire wound around a pencil 50 times and a magnet

Step 1 Select the Proper Voltage Scale

The method of selecting the voltage scale will vary depending on the type of meter. The Fluke 110 has two separate positions for voltage, one position with a wave over it for AC and one position with a solid and dashed line above it for DC. With the Fluke 12B, move the rotary selector to the V symbol for voltage, black V, in order to be able to measure voltage. Press the button that has the VDC and VAC symbol to select between direct current (DC) and alternating current (AC) measurements.

direct current measurements: The screen will show a V, for voltage, with a series of dots and a line over the top. There are several scales available depending on the voltage to be measured. They start from millivolts to voltages up to hundreds of volts. Millivolts is abbreviated mV = 1000th of a volt. Use the Range button to change the range of DC voltage to be measured based on what voltage is expected to be measured. Batteries less than 15 volts can typically be measured accurately with the VDC scale and 0.0 range. DC voltage measurements can be used to determine if batteries are good or if there is voltage coming out of an AC adapter. These are common and are used with hubs, modems, laptops, printers, and other peripherals. These adapters can take wall outlet AC voltage and step it down to lower AC voltages for the device attached or can convert the AC voltage to DC and step it down. Check the back of the adapter to see what the input, AC, and output voltages, AC or DC, should be.

alternating current measurements: The screen will show a V, for voltage, with a tilde (~) after it. This represents alternating current. There are several scales available depending on the voltage to be measured. They start from millivolts to voltages up to hundreds of volts. Millivolts is abbreviated mV = 1000th of a volt. Use the Range button to change the range of AC voltage to be measured based on what voltage is expected to be measured. Voltage from power outlets 120v or greater can typically be measured accurately with the VAC scale and 0.0 range. AC voltage measurements are useful in determining if there is adequate voltage coming from an AC outlet to power the equipment plugged in.

Step 2

Use a Fluke 110, 12B or equivalent multimeter to measure the voltage of each of the following. Be sure to turn the meter off when finished.

Item to Measure the Voltage Of	Set Selector and Range Scale to	Voltage Reading
Batteries: A cell (AA, AAA), C cell, D cell, 9 Volts, 6 V lantern		
Duplex wall outlet (typically 120v)		
Power supply (converts AC to lower AC or DC) for laptop, mobile phone, or other networking electrical device		
(Optional) A lemon with a galvanized nail stuck in one side and a piece of uninsulated copper wire stuck in the opposite side		

Reflection

Why might it be important to measure voltage when troubleshooting a network?

Lab 3.1.3 Resistance Measurement



Objective

- Demonstrate the ability to measure resistance and continuity with the multimeter.

Background

The digital multimeter is a versatile testing and troubleshooting device. This lab covers resistance measurements and related measurements called, continuity. Resistance is measured in Ohms, indicated by the Greek letter Omega or Ω . Copper wire conductors such as those commonly used in network cabling, normally have very low resistance or good continuity when checked from end to end. If there is a break in the wire, it is called “open,” which creates very high resistance. Air has nearly infinite resistance, indicated by the infinity symbol or ∞ .

The multimeter has a battery inside. The battery is used to test the resistance of a wire conductor or wire sheathing insulator. When the probes are applied to the ends of a conductor, the battery current flows and the meter measures the resistance encountered. If the battery in the multimeter is low or dead, it must be replaced or the multimeter will not be able to take resistance measurements.

With this lab, test common networking materials to become familiar with them and their resistance characteristics. First learn to use the resistance setting on the multimeter. Note the continuity feature as small resistances are measured. The instructions provided are for the Fluke 110 and 12B. Other meters will function in a similar way.

Prior to starting the lab, the teacher or lab assistant should have one multimeter available for each team and various networking-related items for testing resistance. Work in teams of two. The following resources will be required:

- Fluke 110 Series or 12B multimeter (or equivalent)
- 1000 Ohm resistor
- 10,000 Ohm resistor
- Pencil for creating graphite paths on paper
- Category 5 jack
- 0.2m, or approximately 6 to 8 inch, section of Category 5 UTP solid cable
- BNC terminated coaxial cable
- Unconnected DB9 to RJ-45 adapter
- Terminated Category 5 UTP patch cable

Step 1 Select the Resistance Scale on the Multimeter

Fluke 110:

Resistance Measurements: Move the rotary selector to the Omega symbol for Ohms (Ω) in order to measure resistance. Use the Range button to change the range of resistance to be measured based on what resistance is expected. The screen will show ohms(Ω), kilohms ($K\Omega$ = thousands of Ohms) or megohms ($M\Omega$ = millions of Ohms).

Continuity Measurements: Move the rotary selector to the Beeper Sound symbol to the left of the Ohms symbol. The Beeper Sound symbol is the setting to measure continuity. When there are less than 20 Ohms, the beep will sound. The beep means that the continuity is good. The continuity setting is used when there is a need for a good path for electricity, but no need for the exact amount of resistance.

Fluke 12B:

Resistance Measurements: Move the rotary selector to the Omega symbol for Ohms (Ω). The Omega symbol is the setting to measure resistance. Press the button with the Ohms symbol on it to select resistance mode instead of continuity. The screen should not show a diode symbol, a small black triangle pointing to a vertical bar. Use the Range button to change the range of resistance to be measured based on what resistance is expected.

Continuity Measurements: Move the rotary selector to the Omega symbol for Ohms (Ω). The Omega symbol is the setting to measure resistance. Press the button with the Ohms symbol on it to select continuity mode. The screen will show a diode symbol, a small black triangle pointing to a vertical bar. A diode is an electronic device that either passes or blocks electrical current. When there is good continuity the beep will sound. Good continuity means low resistance. The continuity setting is used when there is a need for a good path for electricity, but no need for the exact amount of resistance.

Step 2

Check the following resistances. Turn the meter off when finished or the battery will drain.

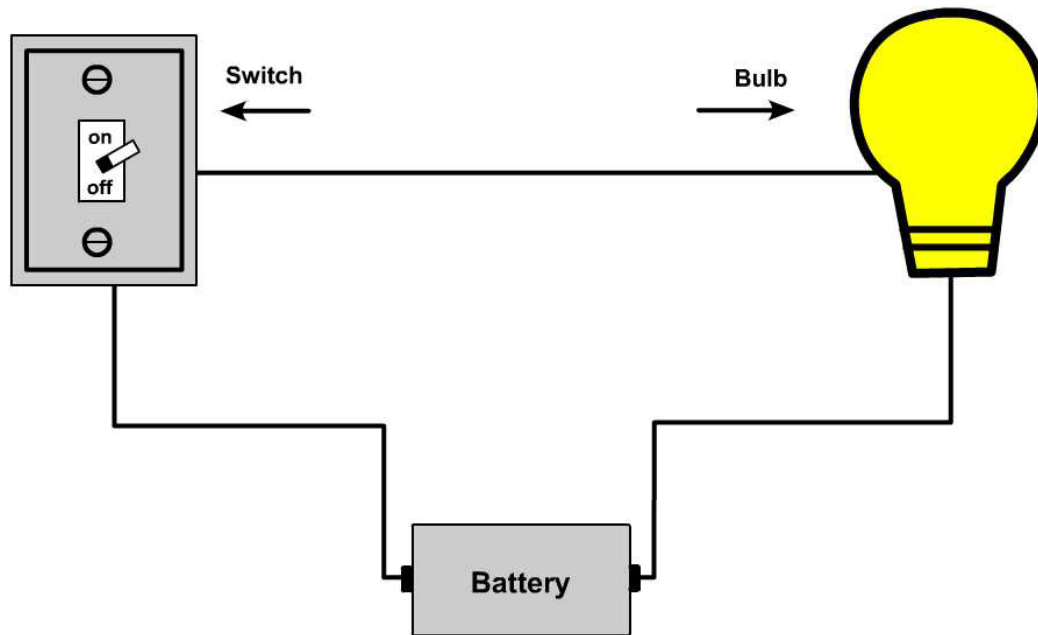
Item to Measure	Set Selector and Range Scale to	Resistance Reading
1000 Ω Resistor		
10 k Ω Resistor		

Graphite marking from a pencil on a piece of paper		
Category 5 jack		
0.2 m section of Category 5 UTP solid cable		
Touch red and black probe contacts together		
A human body (touch the tips of the probes with the fingers)		
BNC terminated coaxial cable		
Unconnected DB9 to RJ-45 adapter		
Terminated Category 5 UTP patch cable		

Reflection

What purpose might the multimeter serve in maintaining and troubleshooting a computer network?

Lab 3.1.5 Series Circuits



Objective

- Build series circuits.
- Explore the basic properties of series circuits.

Background

One of the basic concepts in electronics is a circuit. A Circuit is a continuous loop through which electrons flow. Throughout networking there are references to ground loop circuit, circuit versus packet switching, and virtual circuits, in addition to all the real circuits formed by networking media and networking devices. One of the fundamental electrical circuits is the series circuit. Most networking devices and networks are built from very complex circuits that are beyond the scope of the lessons included in this course. However, the process of building some series circuits will help with the terminology and concepts of networking. This lab also helps increase the overall understanding of some of the basic electrical circuit building blocks.

Prior to starting the lab, the teacher or lab assistant should have one multimeter available for each team of students and various items to create circuits. Work in teams of two. The following resources will be required:

- Fluke 110, 12B or equivalent multimeter
- Light switch
- Wire cutters or wire stripper
- Copper wire
- Two 6v light bulbs with bulb bases or LEDs with resistors
- 6v lantern battery

Step 1 Measure the Resistances of all devices

Measure the resistances of all devices and components, except the lantern battery. All resistances should be less than one Ohm (Ω), except the light bulbs. All the devices except the battery should register continuity with the tone, indicating a short circuit or a conducting path.

Check the following resistances. Turn the meter off when finished or it will drain the battery.

Item to Measure the Resistance of	Set Selector and Range Scale to	Resistance Reading
Pieces of wire to connect components		
Light switch		
Light bulbs		

Step 2

Measure the voltage of the battery with nothing attached to it, unloaded.

Item to Measure the Voltage of	Set Selector and Range Scale to	Voltage Reading
6 V Lantern battery with no load		

Step 3 Build a series circuit

Build a series circuit one device at a time. Use one battery, one switch, one bulb, and connecting wires.

Connect the battery positive lead to the end of one wire. Connect the negative lead to the other wire. If the switch is turned on, the bulb should light.

Disconnect one device and see that the circuit is broken. Did the bulb go out?

Step 4 Measure the battery voltage

Measure the voltage across the light bulb while the circuit is running.

The switch should be turned on and the light bulb should be lit.

What was the voltage across the light bulb with the light bulb on? _____

Step 5 Add the second bulb

Add a second bulb in series and measure the voltage across the light bulb again.

What was the voltage across the light bulb with the light bulb on? _____

Reflection

How do series circuits apply to networking?



Lab 3.1.9a Communications Circuits

Objective

- Design a simple communication system that is fast and reliable.
- Build the system using common materials.
- Test the system.

Background / Preparation

For reliable communications to take place on a network, things like the physical method of signaling and the meaning of each signal or series of signals must be defined ahead of time. Create a simple physical network and agree on some basic rules for communication in order to send and receive data. This will be a digital network based on the American Standard Code for Information Interchange (ASCII). It will be similar to the old telegraph Morse code-based systems. In these older systems the only means of communicating over long distances was by sending a series of dots and dashes as electrical signals over wires between locations. Although the technology used will be more simple than real systems, many of the key concepts of data communications between computers will arise. This lab will also help to clarify the functions of the layers of the OSI model.

Each team must design, build, and test a communications circuit with another team. The goals are to communicate as much data, as quickly and with as few errors, as possible. During this communication, spoken, written, or nonverbal communication of any kind, is not allowed. The only communication allowed is over the wire. The teams must agree on the physical connections and on the coding to use. One team will send a message to the other team. The other team must interpret the intended message without knowing ahead of time what the message was. Keep the OSI model in mind as the system is designed.

Prior to starting the lab, the teacher or lab assistant should have one multimeter available for each team of students and various items for construction of a simple communication network. Work in teams of two to four.

The following resources will be required. Review the purpose of each of the following required items because it will help in the design of the network.

Network Construction Item Required	Purpose
Fluke 110, 12B or equivalent multimeter	For testing communication connections
20' Category 5 UTP cable	For the physical communications lines. The cabling medium.
ASCII chart	To help with coding and interpretation of signals. If there is no hardcopy of the 7-bit ASCII code chart, search the Internet for the words "ASCII chart".
Light switch	To activate the signaling device in order to create the digital on/off, binary, signals

6v light bulbs with bulb bases or LEDs with resistors	To act as the signaling device
6v lantern battery	To power the signaling device
Wire cutters or wire strippers	To adjust the length and prepare the ends of the communication lines

Layer 1 issues

Connect two pairs of wire in order to have communication in both directions, half or full duplex.

Layer 2 issues

Communicate a frame start and stop sequence. This is a sequence of bits that is different than the character and the number bits transmitted.

Layer 3 issues

Invent an addressing scheme for hosts and networks, if it is more than point-to-point communication.

Layer 4 issues

Include some form of control to regulate quality of service. For example, error correction, acknowledgment, windowing, or flow controls.

Layer 5 issues

Implement a way of synchronizing or pausing long conversations.

Layer 6 issues

Use a means of data representation. For example, ASCII encoded as optical bits.

Layer 7 issues

Be able to communicate an idea supplied by the instructor or invent a message.

Reflection

1. What issues arose as the communications system was being built, that apply to data communications between computers?

2. Analyze the communications system in terms of the OSI layers.

Lab 3.1.9b Fluke 620 Basic Cable Testing



Objective

- Use a simple cable tester to verify whether a straight-through or crossover cable is good or bad.
- Use the Fluke 620 advanced cable tester to test cables for length and connectivity.

Background

Work with several cables that have already been made. Test them for basic continuity, breaks in wires, shorts, two or more wires touching, using a basic cable tester. In future labs similar cables will be created.

Simple Cable Testers: There are a number of basic cable testers available for less than U.S. \$100. They usually consist of one or two small boxes with RJ-45 jacks. Plug the cables to be tested the RJ-45 jacks. Many models are designed to test only Ethernet UTP cable.

Both ends of the cable are plugged in to the proper jacks. The tester will test all eight wires and indicate whether the cable is good or bad. Simple testers may have only a single light to indicate the cable is good or bad. Other testers may have eight lights to indicate which wire is bad. The testers have internal batteries to do continuity checks on the wires.

Advanced Cable Testers: Advanced cable testers, such as the Fluke 620 LAN CableMeter®, perform basic cable testing functions and more. The Fluke 620 Advanced cable testers can cost from hundreds to thousands of U.S. dollars. Advanced cable testers will be used in future labs to do wire

maps as well as other tasks. The 620 LAN CableMeter is a cable tester designed to verify connectivity of all LAN cable types. This rugged tester can measure cable length, test for faults and show the distance to the defect. Open faults include opens, shorts, reversed, crossed, or split pairs. Each 620 LAN CableMeter comes with one cable identifier.

The Fluke 620 is more advanced because it performs more functions:

- Requires only single-person verification
- Tests all LAN cable types, UTP, STP, FTP, Coax
- Detects a multitude of wiring problems including open, short, crossed, reversed, split pair
- Locates wiring or connection errors
- Measures cable length

Prior to starting the lab, the teacher or lab assistant should have basic cable testers or Fluke Cable meters available for each team of students. Also provided should be various lengths of wire with induced problems. Work in teams of two. The following resources will be required:

- Basic cable tester
- Advanced cable tester, Fluke 620 or an equivalent
- Two good Category 5 or higher cables, one crossover and one straight-through
- Two bad Category 5 or higher cables, one with a break and one with a short. Use different colors or labels.

Step 1 Test the Cables

Simple cable tester: Refer to the instructions from the manufacturer. Insert the ends of the cable to be tested into the jacks according to the instructions.

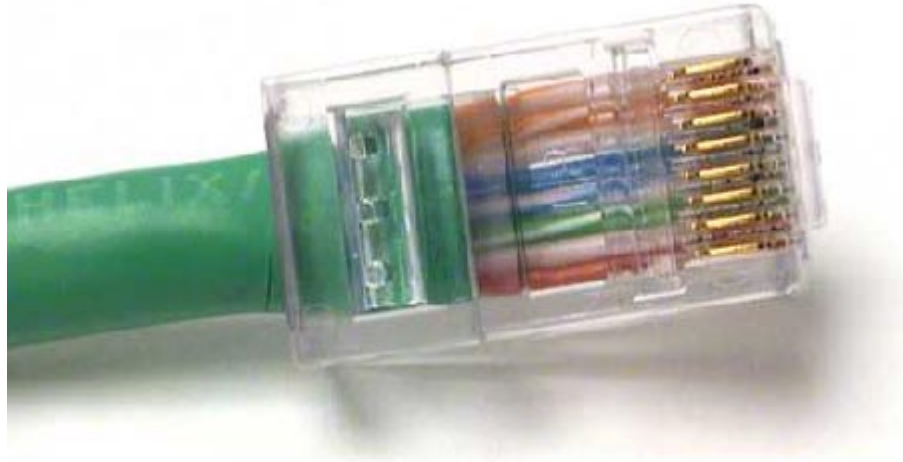
Fluke 620: Insert the RJ-45 from one end of the cable into the UTP/FTP jack on the tester. Turn the dial to test. All conductors will be tested to verify they are not broken or shorted.

Note: This test does not verify that the pins are connected correctly from one end to the other.

For each test, insert the cable into the RJ-45 jack(s) of the cable tester. Record the results in the following table.

	Color or cable number	Category type	Straight-through or crossover?	Length of cable	Test results Pass / Fail
Cable #1					
Cable #2					
Cable #3					
Cable #4					

Lab 3.1.9c Straight-Through Cable Construction



Objective

- Build a Category 5 or Category 5e Unshielded Twisted Pair (UTP) Ethernet network patch cable or patch cord.
- Test the cable for continuity and correct pinouts, the correct color of wire on the right pin.

Background

The cable constructed will be a four-pair, eight-wire, straight-through cable, which means that the color of wire on Pin 1 on one end of the cable will be the same as that of Pin 1 on the other end. Pin 2 will be the same as Pin 2, and so on. The cable will be wired to either TIA/EIA T568B or T568A standards for 10BASE-T Ethernet, which determines what color wire is on each pin. T568B, also called AT&T specification, is more common in the U.S., but many installations are also wired to T568A, also called ISDN.

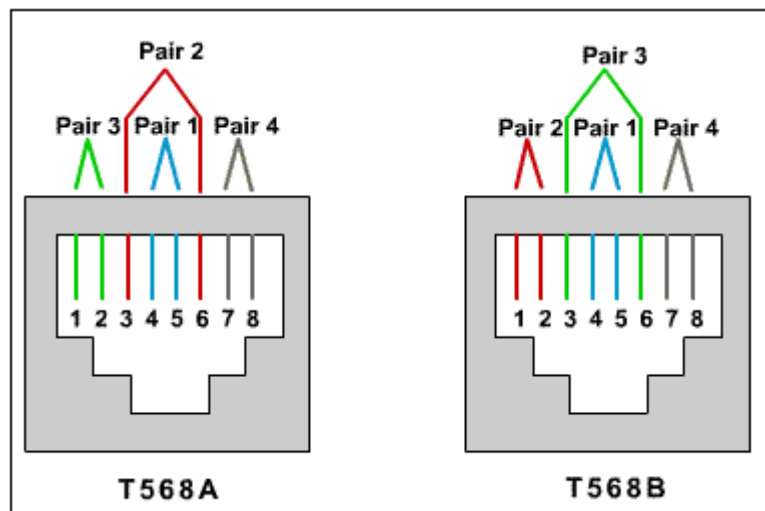
Prior to starting the lab, the teacher or lab assistant should have a spool of Category 5 Unshielded Twisted Pair (UTP) cable, RJ-45 (8-pin) connectors, an RJ-45 crimping tool and an Ethernet / RJ-45 continuity tester available. Work individually or in teams. The following resources will be required:

- One 0.6 to .9 m (2 to 3 ft) length of Category 5 cabling per person or team
- Four RJ-45 connectors, two are extra for spares
- RJ-45 crimping tools to attach the RJ-45 connectors to the cable ends
- Ethernet cabling continuity tester which can test straight-through or crossover type cables, T568A or T568B
- Wire cutters

Cabling Pin-out Information for T568B

Pin #	Pair #	Function	Wire Color	Used with 10/100BASE-T Ethernet?	Used with 100BASE-T4 and 1000BASE-T Ethernet?
1	2	Transmit	White/Orange	Yes	Yes
2	2	Transmit	Orange	Yes	Yes
3	3	Receive	White/Green	Yes	Yes
4	1	Not used	Blue	No	Yes
5	1	Not used	White/Blue	No	Yes
6	3	Receive	Green	Yes	Yes
7	4	Not used	White/Brown	No	Yes
8	4	Not used	Brown	No	Yes

Diagram showing both T568A and T568B cabling wire colors



Use the preceding table and diagram to create a T568B patch panel cable. Both cable ends should be wired the same when looking at the conductors.

Step 1

Determine the distance between devices or device and plug. Add at least 30.48 cm (12 in.) to the distance. The maximum length for this cable, according to TIA/EIA structured wiring standards is 3 m (9.84 ft), although this can vary. Standard lengths are 1.83 m (6ft) and 3.05 m (10 ft).

Step 2

Cut a piece of stranded Category UTP cable to the desired length. Use stranded cable for patch cables because it is more durable when bent repeatedly. Solid wire is used for cable runs that are punched down into jacks.

Step 3

Strip 5.08 cm (2 in.) of jacket off of one end of the cable.

Step 4

Hold the four pairs of twisted cables tightly where jacket was cut away. Reorganize the cable pairs into the order of the T568B wiring standard. Take care to maintain as much of the twists as possible since this provides noise cancellation.

Step 5

Hold the jacket and cable in one hand and untwist a short length of the green and blue pairs. Reorder the pairs to reflect the T568B wiring color scheme. Untwist and order the rest of the wire pairs according to the color scheme.

Step 6

Flatten, straighten, and line up the wires. Trim them in a straight line to within 1.25 to 1.9 cm (1/2 to 3/4 in.) from the edge of the jacket. Be sure not to let go of the jacket and the wires, which are now in the proper order. Minimize the length of untwisted wires because sections that are too long and near connectors are a primary source of electrical noise.

Step 7

Place an RJ-45 plug on the end of the cable, with the prong on the underside and the orange pair to the left side of the connector.

Step 8

Gently push the plug onto wires until the copper ends of the wires can be seen through the end of the plug. Make sure the end of the jacket is inside the plug. This provides for stress relief and to ensure that all wires are in the correct order. If the jacket is not inside the plug, the plug will not be properly gripped and will eventually cause problems. If everything is correct, crimp the plug hard enough to force the contacts through the insulation on the wires, completing the conducting path.



Step 9

Repeat Steps 3 through 8 to terminate the other end of the cable. Use the same scheme to finish the straight through cable.

Step 10

Test the finished cable. Have the instructor check the finished cable. How is it possible to tell if the cable is functioning properly?

Lab 3.1.9d Rollover Cable Construction

Objective

- Build a Category 5 or Category 5e Unshielded Twisted Pair (UTP) console rollover cable.
- Test the cable for continuity and correct pin-outs, the correct wire on the right pin.

Background

This will be a 4-pair "rollover" cable. This type of cable is typically 3.05 m (10 ft) long but can be as long as 7.62 m (25 ft). A rollover cable can be used to connect a workstation or dumb terminal to the console port on the back of a Cisco router or switch. Both ends of the cable built will have RJ-45 connectors on them. One end plugs directly into the RJ-45 console management port on the back of the router or switch. Plug the other end into an RJ-45-to-DB9 terminal adapter. This adapter converts the RJ-45 to a 9-pin female D connector for attachment to the PC or dumb terminal serial (COM) port. A DB25 terminal adapter is also available to connect with a PC or dumb terminal. This adapter uses a 25 pin connector. The following picture shows a rollover console cable kit that ships with most Cisco devices.



This cable is called a rollover because the pins on one end are all reversed on the other end as though one end of the cable was rotated or rolled over. In the last lab when building the straight-through cable, putting the second RJ-45 on upside down would have made a rollover cable instead of the straight through cable.

Prior to starting the lab, the teacher or lab assistant should have a spool of Category 5 or Category 5e UTP cable, RJ-45 (8-pin) connectors, an RJ-45 crimping tool and a continuity tester available. Work individually or in teams. The following resources will be required:

- One 3.05 to 6.1 m (10 to 20 ft) length of Category 5 cabling per person or per team

- Four RJ-45 connectors, two are extra for spares
- RJ-45 crimping tools to attach the RJ-45 connectors to the cable ends
- An RJ-45 to DB-9 female terminal adapter, available from Cisco
- Cabling continuity tester
- Wire cutters

Step 1

Use the table as a reference to help create a rollover console cable.

Router or switch Console port (DTE)	RJ-45 to RJ-45 Rollover Cable (left end)	RJ-45 to RJ-45 Rollover Cable (right end)	RJ-45 to DB9 Adapter	Console Device (PC workstation serial port)
Signal	From RJ-45 Pin No.	To RJ-45 Pin No.	DB9 Pin No.	Signal
RTS	1	8	8	CTS
DTR	2	7	6	DSR
TxD	3	6	2	RxD
GND	4	5	5	GND
GND	5	4	5	GND
RxD	6	3	3	TxD
DSR	7	2	4	DTR
CTS	8	1	7	RTS

Signal Legend: RTS = Request To Send, DTR = Data Terminal Ready, TxD = Transmit Data, GND = Ground (One for TxD and one for RxD), RxD = Receive Data, DSR = Data Set Ready, CTS = Clear To Send.

Step 2

Determine the distance between devices, then add at least 30.48 cm (12 in.) to the distance. Make the cable about 3.05 m (10 ft), unless connecting to router or switch from a greater distance. The maximum length for this cable is about 8m (approx 25 ft).

Step 3

Strip 5.08 cm (2 in.) of jacket off of one end of the cable.

Step 4

Hold the 4 pairs of twisted cables tightly where jacket was cut away. Reorganize the cable pairs and wires into the order of the T568B wiring standard. They can be ordered in any sequence, but use the T568B sequence to become more familiar with it.

Step 5

Flatten, straighten, and line up the wires, then trim them in a straight line to within 1.25 to 1.9 cm (1/2 to 3/4 in.) from the edge of the jacket. Be sure not to let go of the jacket and the wires, which are now in order.

Step 6

Place an RJ-45 plug on the end of the cable, with the prong on the underside and the orange pair to the left side of the connector.

Step 7

Gently push the plug onto wires until the copper ends of the wires can be seen through the end of the plug. Make sure the end of the jacket is inside the plug and all wires are in the correct order. If the jacket is not inside the plug, the plug will not be properly gripped and will eventually cause problems.

Step 8

If everything is correct, crimp the plug hard enough to force the contacts through the insulation on the wires, thus completing the conducting path.

Step 9

Repeat steps 2 through 6 to terminate the other end of the cable, but reversing every wire as indicated in the table above. Pin 1 to pin 8, pin 2 to pin 7, pin 3 to pin 6 and so on.

a. **Alternate Method** – Arrange the wires into the order of the T568B wiring standard. Place a RJ-45 plug on the end with the prong on the top side of the connector. This method will achieve the proper reversing of every pair of wires.

Step 10

Test the finished cable. Have the instructor check it. How is it possible to tell if the cable is functioning properly?



Lab 3.1.9e Crossover Cable Construction

Objective

- Build a Category 5 or Category 5e Unshielded Twisted Pair (UTP) Ethernet crossover cable to T568B and T568A standards.
- Test the cable for continuity and correct pin-outs, correct wire on the right pin.

Background

This will be a 4-pair "crossover" cable. A crossover cable means that the second and third pairs on one end of the cable will be reversed on the other end. The pin-outs will be T568A on one end and T568B on the other end. All 8 conductors (wires) should be terminated with RJ-45 modular connectors.

This patch cable will conform to the structured cabling standards. If the patch cable is used between hubs or switches, it is considered to be part of the "vertical" cabling. Vertical cabling is also called backbone cabling. A crossover cable can be used as a backbone cable to connect two or more hubs or switches in a LAN, or to connect two isolated workstations to create a mini-LAN. This will allow the connection of two workstations or a server and a workstation without the need for a hub between them. This can be very helpful for training and testing. To connect more than two workstations, a hub or a switch will be needed.

Prior to starting the lab, the teacher or lab assistant should have a spool of Category 5 or Category 5e UTP cable, RJ-45 (8-pin) connectors, a RJ-45 crimping tool and an Ethernet / RJ-45 continuity tester available. Work individually or in teams. The following resources will be required:

- One 0.6 to .9 m (2 to 3 ft) length of Category 5 cabling per person or team
- Four RJ-45 connectors, two are extra for spares
- RJ-45 crimping tools to attach the RJ-45 connectors to the cable ends
- Ethernet cabling continuity tester which can test crossover type cables, T568A to T568B
- Wire cutters

Step 1

Create a crossover cable using the following tables and diagrams. One end of the cable should be wired to the T568A standard. The other end should be wired to the T568B standard. This crosses the transmit pairs and the receive pairs, the second and third pair, to allow communication to take place.

Only four wires are used with 10BASE-T or 100BASE-TX Ethernet.

T568A Cabling

Pin #	Pair #	Function	Wire Color	Used with 10/100BASE-T Ethernet?	Used with 100BASE-T4 and 1000BASE-T Ethernet?
1	3	Transmit	White/Green	Yes	Yes
2	3	Transmit	Green	Yes	Yes
3	2	Receive	White/Orange	Yes	Yes
4	1	Not used	Blue	No	Yes
5	1	Not used	White/Blue	No	Yes
6	2	Receive	Orange	Yes	Yes
7	4	Not used	White/Brown	No	Yes
8	4	Not used	Brown	No	Yes

T568B Cabling

Pin #	Pair #	Function	Wire Color	Used with 10/100BASE-T Ethernet?	Used with 100BASE-T4 and 1000BASE-T Ethernet?
1	2	Transmit	White/Orange	Yes	Yes
2	2	Transmit	Orange	Yes	Yes
3	3	Receive	White/Green	Yes	Yes
4	1	Not used	Blue	No	Yes
5	1	Not used	White/Blue	No	Yes
6	3	Receive	Green	Yes	Yes
7	4	Not used	White/Brown	No	Yes
8	4	Not used	Brown	No	Yes

Step 2

Determine the distance between devices, or device and plug, and then add at least 30.48 cm (12 in.) to it. Standard lengths for this cable are 1.83 m (6 ft) and 3.05 m (10 ft).

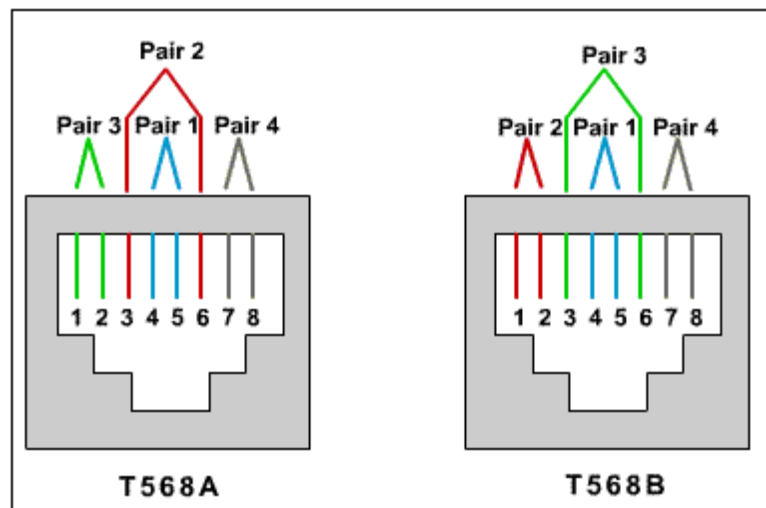
Step 3

Cut a piece of stranded UTP cable to the desired length. Use stranded cable for patch cables because it is more durable when bent repeatedly. Solid wire is fine for cable runs that are punched down into jacks.

Step 4

Strip 5.08 cm 9 (2in.) of jacket off one end of the cable.

Diagram showing both T568A and T568B cabling wire colors



Step 5

Hold the four pairs of twisted cables tightly where the jacket was cut away. Reorganize the cable pairs into the order of the **T568B** wiring standard. Take care to maintain the twists since this provides noise cancellation.

Step 6

Hold the jacket and cable in one hand. Untwist a short length of the green and blue pairs, and reorder them to reflect the **T568B** wiring color scheme. Untwist and order the rest of the wire pairs according to the color scheme.

Step 7

Flatten, straighten, and line up the wires. Trim them in a straight line to within 1.25 cm to 1.9 cm (1/2 to 3/4 in.) from the edge of the jacket. Be sure not to let go of the jacket and the wires, which are now in order. Minimize the length of untwisted wires because sections that are too long and near connectors are a primary source of electrical noise.

Step 8

Place an RJ-45 plug, prong down, on the end of the cable with the green pair on the left side of the T568A end, and the orange pair on the left side of the T568B end.

Step 9

Gently push the plug onto wires until the copper ends of the wires can be seen through the end of the plug. Make sure the end of the jacket is inside the plug and all wires are in the correct order. If the jacket is not inside the plug, the plug will not be properly gripped and will eventually cause problems. If everything is correct, crimp the plug hard enough to force the contacts through the insulation on the wires, thus completing the conducting path.

Step 10

Repeat steps 4-8 to terminate the other end of the cable using the **T568A** scheme to finish the crossover cable.

Step 11

Test the finished cable. Have the instructor check it. How is it possible to tell if the cable is functioning properly?



Lab 3.1.9f UTP Cable Purchase

Objective

- Introduce the variety and prices of network cabling and components in the market.
- Gather pricing information for UTP patch cables and bulk cable.

Background

Put together a price list for an upcoming cabling project. Gather pricing information for the horizontal (UTP) cabling. If UTP is not used in the immediate area, substitute shielded products. The items include the following:

- 24 – 1 m (3 ft) Category 5 or higher UTP patch cables
- 24 – 3 m (10 ft) Category 5 or higher UTP patch cables
- 2 – 15 m (50 ft) Category 5 or higher UTP patch cables
- 152.4 m (500 ft) UTP compare the price to shielded twisted pair
- 152.4 m (500 ft) UTP plenum

Step 1 Research cable pricing

Use at least three sources for pricing. On the Web try <http://www.cdw.com> and <http://www.google.com>. Perform searches from those sites looking for **Category 5 jumpers**, **Category 5 patch**, and **Category 5 bulk**. While the CDW site will give prices quickly, the Google search will turn up many interesting things from custom cable building firms to instructions for building cables. Also refer to networking equipment and supplies catalogs.

Step 2 Compile a table of the results

Site, Catalog or Store			
24 - 1 m (3 ft) Category 5 or higher			
24 - 3 m (10 ft) Category 5 or higher			
2 - 15 m (50 ft) Category 5 or higher			
152.4 m (500 ft) UTP			
152.4 m (500 ft) shielded twisted pair			
152.4 m (500 ft) UTP plenum			



Lab 3.2.8 Fiber-Optic Cable Purchase

Objective

- Introduce the variety and prices of network cabling and components in the market.
- Gather pricing information for fiber patch cables and fiber bulk cable.

Background

Put together a price list for an upcoming cabling project. Gather pricing information for the vertical or fiber cabling. Use Multimode (MM) fiber. The items include:

- 24 – 2 m (6 ft) MM patch cables
- 24 – 5 m (15 ft) MM patch cables
- 2 – 15 m (50 ft) MM patch cables
- 304.8 m (1000 ft) MM fiber optic cable

Step 1 Research Cable Pricing

Use at least three sources for pricing. On the Web, try <http://www.cdw.com> and <http://www.google.com>. Perform searches from those sites looking for fiber **optic jumpers**, **fiber optic patch**, and **fiber optic bulk**. While the CDW site will give prices quickly, the Google search will turn up many interesting things from custom cable building firms to instructions for building cables. Also refer to networking equipment and supplies catalogs.

Step 2 Compile a Table of the Results

Site, Catalog or Store			
24 - 2 m (6 ft) MM patch cables			
24 - 5 m (15 ft) MM patch cables			
2 - 15 m (50 ft) MM patch cables			
304.8 m (1000 ft) MM fiber optic cable			

Lab 4.2.9a Fluke 620 Cable Tester – Wire Map



Objective

- Learn the wire mapping features of the Fluke 620 LAN CableMeter or its equivalent.
- Learn how to use a cable tester to check for the proper installation of unshielded twisted-pair (UTP) Category 5 according to TIA/EIA-568 cabling standards in an Ethernet network.

Background / Preparation

Wire maps can be very helpful in troubleshooting cabling problems with UTP cable. A wire map allows the network technician to verify which pins on one end of the cable are connected to which pins on the other end.

Prior to starting the lab, the teacher or lab assistant should have several correctly wired Category 5 cables to test. The cables should be both straight-through and crossover. There should also be several Category 5 cables created with problems such as poor connections and split pairs to test. Cables should be numbered to simplify the testing process and to maintain consistency. A cable

tester should be available that can test at least continuity, cable length, and wire map. Work individually or in teams. The following resources will be required:

- Category 5 straight-wired cables of different colors
- Category 5 crossover-wired cable, which is T568A on one end and T568B on the other
- Category 5 straight-wired cables with open wire connections in the middle or one or more conductors shorted at one end of different colors and different lengths
- Category 5 straight-wired cable with a split pair mis-wire
- Fluke 620 LAN CableMeter or similar to test cable length, continuity, and wire map

Step 1

Turn the rotary switch selector on the tester to the WIRE MAP position. Press the **SETUP** button to enter the setup mode and observe the LCD screen on the tester. The first option should be CABLE. Press the **UP** or **DOWN** arrow buttons until the desired cable type of UTP is selected. Press **ENTER** to accept that setting and go to the next one. Continue pressing the UP/DOWN arrows and pressing **ENTER** until the tester is set to the following cabling characteristics:

Tester Option	Desired Setting – UTP
CABLE:	UTP
WIRING:	10BASE-T or EIA/TIA 4PR
CATEGORY:	CATEGORY 5
WIRE SIZE	AWG 24
CAL to CABLE?	NO
BEEPING:	ON or OFF
LCD CONTRAST	From 1 through 10 (brightest)

Step 2

Once the student has completed setting up the meter, press the "SETUP" button to exit setup mode.

For each cable to be tested use the following procedure. Place the near end of the cable into the RJ-45 jack labeled UTP/FTP on the tester. Place the RJ-45-RJ-45 female coupler on the far end of the cable, and then insert the cable Identifier into the other side of the coupler. The coupler and the cable identifier are accessories that come with the Fluke 620 LAN CableMeter.



Step 3

Using the tester Wire Map function and a Cable ID Unit, the wiring of both the near and far end of the cable can be determined. The top set of numbers displayed on the LCD screen is the near end, and

the bottom set is the far end. Perform a Wire Map test on each of the cables provided. Then fill in the following table based on the result for each Category 5 cable tested. For each cable, write down the number and color, whether the cable is straight-through or crossover, the tester screen test results, and what the problem is.

Cable No.	Cable Color	How cable is wired (straight-through or crossover)	Test Displayed Test Results (Note: Refer to the Fluke manual for detailed description of test results for wire map.)	Problem Description
1			Top: Bot:	
2			Top: Bot:	
3			Top: Bot:	
4			Top: Bot:	
5			Top: Bot:	

Lab 4.2.9b Fluke 620 Cable Tester – Faults



Objective

- Learn the Cable Test - Pass / Fail features of the Fluke 620 LAN CableMeter or an equivalent tester.
- Learn how to use a cable tester to check for the proper installation of unshielded twisted pair (UTP) for an Ethernet network.
- Test different cables to determine some problems that can occur from incorrect cabling installation and termination.

Background / Preparation

Basic cable tests can be very helpful in troubleshooting cabling problems with UTP. The Cabling infrastructure or cable plant in a building is expected to last at least ten years. Cabling-related problems are one of the most common causes of network failure. The quality of cabling components used, the routing and installation of the cable, and quality of the connector terminations will be the main factors in determining how trouble-free the cabling will be.

Prior to starting the lab, the teacher or lab assistant should have several correctly wired Category 5 cables to test. The cables should be both straight-through and crossover. There should also be several Category 5 cables created with problems. Cables should be numbered to simplify the testing process and to maintain consistency. The following resources will be required:

- Category 5 straight-through and crossover wired cables of different colors, some good and some bad
- Category 5 straight-through and crossover wired cables with open wire connections in the middle or one or more conductors shorted at one end that are different colors and different lengths
- Cable Tester, which is Fluke 620 LAN CableMeter or something similar, to test cable length

Step 1

Turn the rotary switch selector on the tester to the **TEST** position. Press the **SETUP** button to enter the setup mode and observe the LCD screen on the tester. The first option should be CABLE. Press the **UP** or **DOWN** arrow buttons until the desired cable type of **UTP** is selected. Press **ENTER** to accept that setting and go to the next one. Continue pressing the UP/DOWN arrows and pressing **ENTER** until the tester is set to options in the chart below. Once the options have been properly selected, press the SETUP button to exit setup mode.

Tester Option	Desired Setting – UTP
CABLE:	UTP
WIRING:	10BASE-T or EIA/TIA 4PR
CATEGORY:	CATEGORY 5
WIRE SIZE	AWG 24
CAL to CABLE?	NO
BEEPING:	ON or OFF
LCD CONTRAST	From 1 thru 10 (brightest)

Step 2

For each cable to be tested, use the following procedure. Place the near end of the cable into the RJ-45 jack labeled UTP/FTP on the tester. Place the RJ-45-RJ-45 female coupler on the far end of the cable. Then insert the cable identifier into the other side of the coupler. The coupler and the cable identifier are accessories that come with the Fluke 620 LAN CableMeter.



Step 3

Using the tester LENGTH function and a UTP Cable ID Unit, the length of the cable can be determined. Perform a basic cable test on each of the cables provided. Then fill in the following table

based on the result for each Category 5 cable tested. For each cable, write down the number and color, whether the cable is straight-through or crossover or coaxial, the tester screen test results, and what the problem is. For UTP cables, press the **DOWN** arrow or **UP** arrow to see all pairs.

Cable No.	Cable Color	Tester Test Results	Problem
1			
2			
3			
4			

Lab 4.2.9c Fluke 620 Cable Tester – Length



Objective

- Learn the Cable Length feature of the Fluke 620 LAN CableMeter or its equivalent.
- Learn how to use a cable tester to check the length of Ethernet cabling to verify that it is within the standards specified and that the wires inside are the same length.

Background / Preparation

Cable length tests can be very helpful in troubleshooting cabling problems with UTP. The Cabling infrastructure or cable plant in a building is expected to last at least ten years. Cabling related problems are one of the most common causes of network failure. The quality of cabling components used, the routing and installation of the cable, and quality of the connector terminations will be the main factors in determining how trouble-free the cabling will be.

Prior to starting the lab, the teacher or lab assistant should have several correctly wired Category 5 cables to test. The cables should be both straight- through and crossover. Cables should be numbered to simplify the testing process and to maintain consistency. A cable tester should be

available that can do cable length tests for UTP. Work individually or in teams. The following resources will be required:

- Category 5 straight-through or crossover cables of different colors, some good and some bad
- Cable Tester, which is Fluke 620 LAN CableMeter or similar, to test cable length

Step 1

Turn the rotary switch selector on the tester to the LENGTH position. Press the SETUP button to enter the setup mode and observe the LCD screen on the tester. The first option should be CABLE. Press the UP or DOWN arrow buttons until the desired cable type of UTP is selected. Press ENTER to accept that setting and go to the next one. Continue pressing the UP/DOWN arrows and pressing ENTER until the tester is set to options in the chart below. Once the options have been properly selected, press the SETUP button to exit setup mode.

Tester Option	Desired Setting – UTP
CABLE:	UTP
WIRING:	10BASE-T or EIA/TIA 4PR
CATEGORY:	CATEGORY 5
WIRE SIZE	AWG 24
CAL to CABLE?	NO
BEEPING:	ON or OFF
LCD CONTRAST	From 1 through 10 (brightest)

Step 2

For each cable to be tested use the following procedure. Place the near end of the cable into the RJ-45 jack labeled UTP/FTP on the tester. Place the RJ-45-RJ-45 female coupler on the far end of the cable, and then insert the cable identifier into the other side of the coupler. The coupler and the cable identifier are accessories that come with the Fluke 620 LAN CableMeter.



Step 3

Using the tester LENGTH function and a UTP Cable ID Unit, the length of the cable can be determined. Perform a basic cable test on each of the cables provided. Then fill in the following table based on the result for each cable tested. For each cable, write down the number and color, the cable length, the tester screen test results, and what the problem is, if there is a problem. For UTP cables, press the **DOWN** arrow or **UP** arrow to see all pairs.

Cable No.	Cable Color	Cable Length	Tester Test Results	Problem
1				
2				
3				
4				

Lab 4.2.9d Fluke LinkRunner – LAN Tests

LinkRunner™



Objective

- Become familiar with the capabilities of the Fluke LinkRunner
- Determine whether a cable drop is active
- Identify the cable drop speed, duplex capabilities, and service type
- Verify network layer connectivity with `ping`

Background / Preparation

In this lab, the student will work with Ethernet cable drops that are attached to networking devices such as hubs and switches. This is to determine the characteristics of the devices and cabling and identify potential networking problems. Use some of the key capabilities of the Fluke LinkRunner, such as drop activity and ping, to perform the analysis.

As networks run faster and become more complex, infrastructure cabling and devices must operate to precise levels in a tighter performance window. As a result, nearly 80% of network problems stem from simple wiring and connection problems. The following resources will be required:

- Ethernet hub and switch
- Several Ethernet straight-through patch cables
- Cable run from a wall-plate to switch through a patch panel

The following URLs provide information on the Fluke LinkRunner. The first one is a virtual demo of LinkRunner capabilities, and the second is a link to the downloadable LinkRunner Quick Reference Guide in various languages.

http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/_see+it+live.htm

http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/_manuals.htm

Step 1 Become familiar with the capabilities of the Fluke LinkRunner

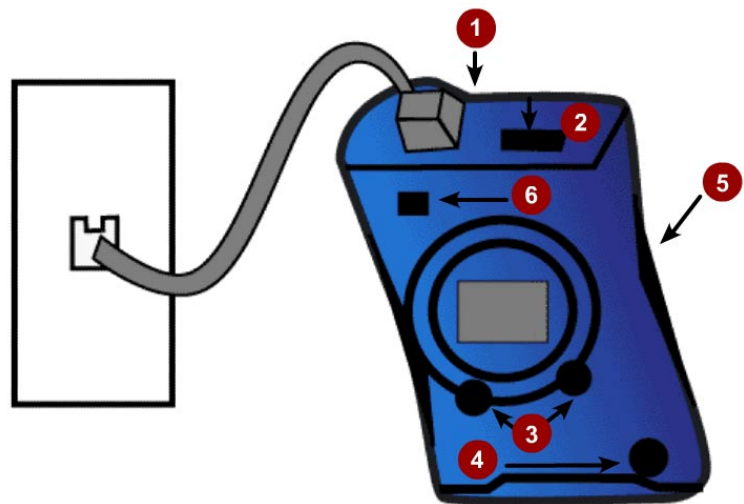
Access the virtual demo of the LinkRunner using the first URL listed above. Try different tests to become familiar with its capabilities.

Step 2 Obtain access to the LinkRunner Quick Reference Guide

Access the Quick Reference Guide online directly, or download it to a PC using the link provided above. The instructor may also have a copy of the Quick Reference Guide available. Selected pages of the Quick Reference Guide have been reproduced in this lab. The illustration below shows the connectors and buttons on the LinkRunner.

1. RJ-45 LAN port
2. RJ-45 MAP port (cable testing)
3. Selection buttons
Left - Highlight
Right - Action
4. Power Button
5. Batteries (2) AA
6. Link indicator light

Power off - Press and Hold
Backlight - Press once briefly



Step 3 Configure the LinkRunner

- a. From any screen, access the main configuration by pressing both buttons simultaneously. There is the option to configure LinkRunner or go into Ping configuration.
- b. Pressing the left button goes to LinkRunner configuration where there is the MAC address of the LinkRunner and the display can be toggled between feet and meters.

What is the Layer 2 media access control (MAC) address? _____

- c. Pressing the right button goes to ping configuration.

Step 4 Test active workstation links to a switch

- a. LinkRunner allows the determination of what type of service users are connected to, such as Ethernet, Token Ring, or Telco. On Ethernet segments it can be determined whether the drop is active, identify its speed, duplex capabilities, and auto negotiation settings.
- b. This test will determine if the cable drop is active while identifying its speed, duplex, and service type (10 or 10/100 indicates Ethernet).
- c. Turn on the LinkRunner by pressing the small button in the lower right corner.
- d. Disconnect a functioning LAN patch cable from a workstation and plug it into the RJ-45 LAN port on the LinkRunner. This is a nondestructive test in that it can be performed on a live network.

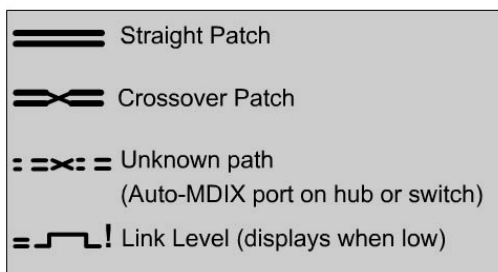
The cable should be attached to a wall plate, which then attaches to a switch through a patch panel in a wiring closet. Cabling should be in accordance with current structured cabling standards.

- e. Observe the display on the LinkRunner and record the information for Drop #1 in the following table. A sample display from the quick reference guide is shown below the table.
- f. Obtain another patch cable of any length, and plug one end directly into the switch. Plug the other end into the LinkRunner LAN port. Record the information for Drop #2 in the following table.

	Link Active ?	Cable Type / Link Status	Advertised speed / duplex	Actual link speed / duplex	Network utilization
Drop #1					
Drop #2					

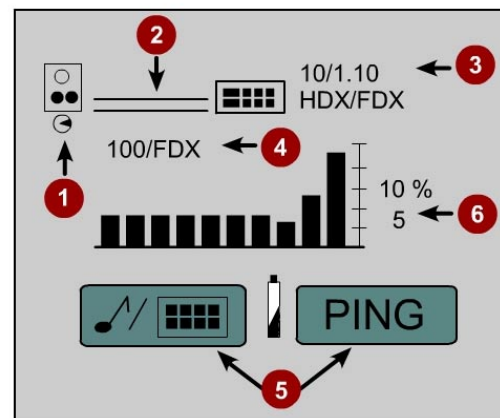
Is this an active Ethernet Port?

1. Activity Indicator
2. Cable/Link Status:



3. Advertised speed/duplex
4. Actual link speed/duplex
5. Softkeys (correspond to L/R selection buttons).
6. Network utilization

! Battery Low Indicator: display when low.



- g. Disconnect the end of the cable from the switch and observe the display. What was the result?

Step 5 Test a direct link to a hub

- a. Obtain another patch cable of any length, and plug one end directly into an active regular hub port. Plug the other end into the LinkRunner LAN port. Describe the results.
- b. How does this display differ from that of a cable drop attached to a switch?
- c. Disconnect the power from the hub and described the display now.

- d. Plug the hub back in.
- e. Move the cable from one of the regular of ports on the hub to the uplink port on the hub. Make sure the uplink is not active, so the button should not be pushed in. Describe the results.

f. Activate the uplink port by pushing in the button. What happened to the wires in the display?

g. Why did this occur?

Step 6 Use the DHCP Ping function to verify network layer connectivity

If the LAN port in a DHCP network environment is connected, LinkRunner will act as a DHCP client. It will acquire an IP address and verify basic connectivity to key devices by pinging the default gateway or router and DNS server. See the diagram below for a sample of the screen display.

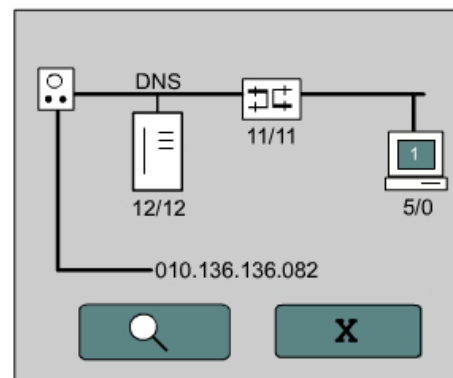
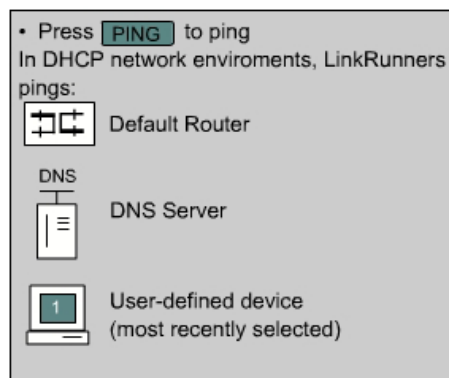
- a. Turn on the LinkRunner by pressing the small button in the lower right corner.
- b. Obtain a patch cable of any length and plug one end directly into the switch on a LAN with a DHCP server available. Plug the other end into the LinkRunner LAN port.
- c. The LinkRunner must be in DHCP mode in order to perform this test. Press the right softkey (Ping) once to see if the DHCP magnifying glass is displayed. If not, press the left softkey twice and place a checkmark in the DHCP option box.

Allow time for the LinkRunner to obtain an IP address from the DHCP server, and then press the right softkey, which is the ping.

Note: If the LinkRunner fails to obtain an IP address, verify that the DHCP option box is checked and that there is a DHCP server active on the network.

- d. What was the IP address that the LinkRunner obtained? _____
- e. Press the left Softkey or magnifying glass button, which provides ping details.
- f. What is the IP address of the default router or gateway? _____
- g. What is the round-trip time for the ping to the default router? _____
- h. What is the IP address of the DNS server? _____
- i. What is the round-trip time for the ping to the DNS server? _____
- j. If one response time is slower than the other, why is that? _____

Can I Ping?



Step 7 Ping user-defined IP address

The LinkRunner can be used to ping user-defined IP addresses for up to 4 common IP address ping targets. See the diagram below for a sample of the screen display used to edit the IP address for computer target 1. This test assumes that the LinkRunner has obtained a compatible IP address, subnet mask and default gateway as a DHCP client in the prior step. If not see the note in step 7j below.

- a. Turn on the LinkRunner by pressing the small button in the lower right corner.
- b. Disconnect any cables from the LinkRunner.
- c. Press the right SoftKey (wrench) to access configuration options.
- d. Press the right SoftKey again (ping and wrench). When working on a network with a DHCP server, turn off the LinkRunner DHCP client by removing the checkmark from the DHCP check box. Press the right SoftKey (checkmark) to uncheck it.
- e. Press the left SoftKey (down arrow) to get to the computer icon. Then press the right SoftKey (computer, IP, and wrench) to access the IP address configuration function.
- f. Press the right SoftKey (down arrow and computer) to cycle through the four IP targets. Zero indicates no ping for the computer target. Select IP target number 1.
- g. Press the left SoftKey (down arrow) to access the IP address, and press the right SoftKey (IP x.x.x.x) to begin configuring the IP address for target computer 1. See figure below.
- h. Identify the IP address of a lab server or a partner workstation and record it here.

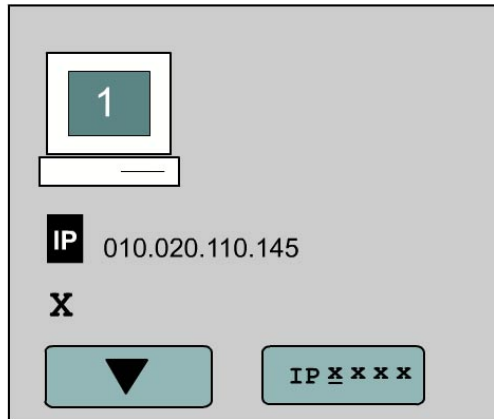
- i. Press the left SoftKey (right arrow) to advance the cursor from one number to the next in the IP address. Press the right to SoftKey (IP and Up arrow) to change the value of the number. All 12 decimal digits including zeros must be accounted for. While working with the first digit of any of the 4 octets, press the up arrow four or five times. What is the maximum number that the LinkRunner will allow to set the first number of an octet to? _____
- j. When finished with the last digit, the left SoftKey will become a down arrow. Press the left SoftKey until there is the X (exit), and then press the right SoftKey (X). Press the left SoftKey (down arrow again until you get to the X and press the right SoftKey again to exit the configuration function.

Note: If the LinkRunner did not obtain a compatible IP address and subnet mask from DHCP in prior Step 6, configure them before going on. Instead of selecting the computer icon to configure, select the LinkRunner icon and follow the same basic procedure as described above to set its IP address and subnet mask. The IP address of the default gateway for the LinkRunner should also be set at this point.
- k. After the IP address is set to be pinged, connect a patch cable from the LAN port on the LinkRunner to a wall plate jack, hub or switch on the network will be pinged. What does the cable display look like? _____
- l. Press the right SoftKey (ping) to start the ping function. There should be a workstation icon with a target number 1 on the screen. Does the workstation have a solid lines or dashed lines?

What does this mean?

- m. Press the left SoftKey (magnifying glass) to see the IP addresses of all devices being pinged and the round-trip time for each in milliseconds.
- n. Which devices were being pinged and what were the round-trip times for each?

- o. Press the right SoftKey (X) twice to exit the detailed view and ping function.



Step 8 Disconnect the equipment and store the cabling and devices

Lab 4.2.9e Fluke LinkRunner – Cable and NIC Tests

LinkRunner™



Objective

- Become familiar with the capabilities of the Fluke LinkRunner
- Verify cable length and integrity
- Determine where a cable terminates
- Verify PC NIC functionality

Background / Preparation

In this lab, the student will work with Ethernet cables to determine their characteristics and identify potential problems. The student will use some of the key capabilities of the Fluke LinkRunner such as cable mapping and NIC Test.

As networks run faster and become more complex, infrastructure cabling and devices must operate to precise levels in a tighter performance window. As a result, nearly 80% of network problems stem from simple wiring and connection problems. The following resources will be required:

- Ethernet straight-through patch cables, which are good and bad
- Ethernet crossover cables
- Ethernet cable from wall plate RJ-45 jack through a patch panel
- Hub and/or switch
- Computer with NIC

The following URLs provide information on the Fluke LinkRunner. The first one is a virtual demo of LinkRunner capabilities, and the second is a link to the downloadable LinkRunner Quick Reference Guide in various languages.

http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/_see+it+live.htm

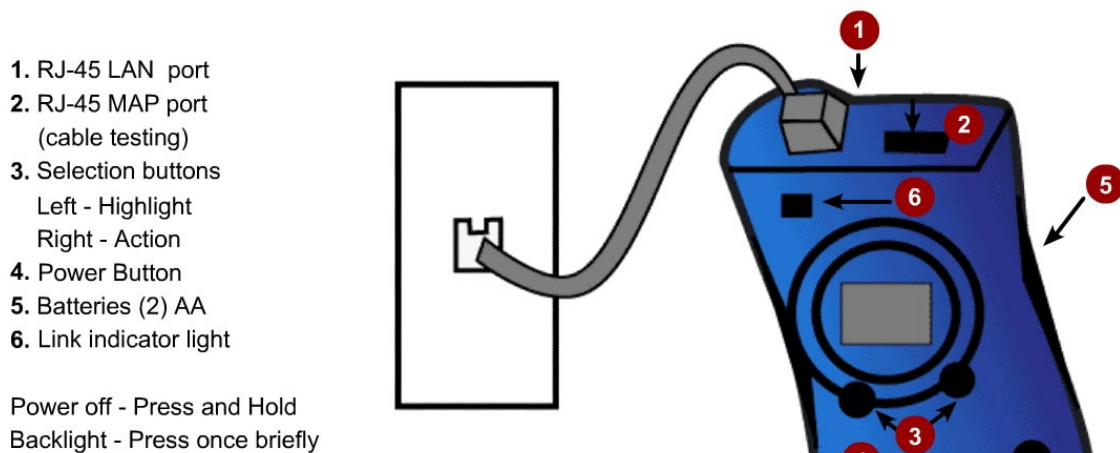
http://www.flukenetworks.com/us/LAN/Handheld+Testers/LinkRunner/_manuals.htm

Step 1 Become familiar with the capabilities of the Fluke LinkRunner

Access the virtual demo of the LinkRunner using the first URL listed above. Try different tests to become familiar with its capabilities.

Step 2 Obtain access to the LinkRunner Quick Reference Guide

The Quick Reference Guide may be accessed online directly or downloaded to a PC using the link provided above. The instructor may also have a copy of the Quick Reference Guide available. Selected pages of the Quick Reference Guide have been reproduced in this lab. The illustration below shows the connectors and buttons on the LinkRunner.



Step 3 Configure the LinkRunner

- From any screen, the main configuration can be accessed by pressing both buttons simultaneously. Now there is the option to configure LinkRunner or go into ping configuration
- Pressing the left button goes to LinkRunner configuration where there is the MAC address of the LinkRunner and the display can be toggled between feet and meters.

What is the layer 2 media access control (MAC) address?

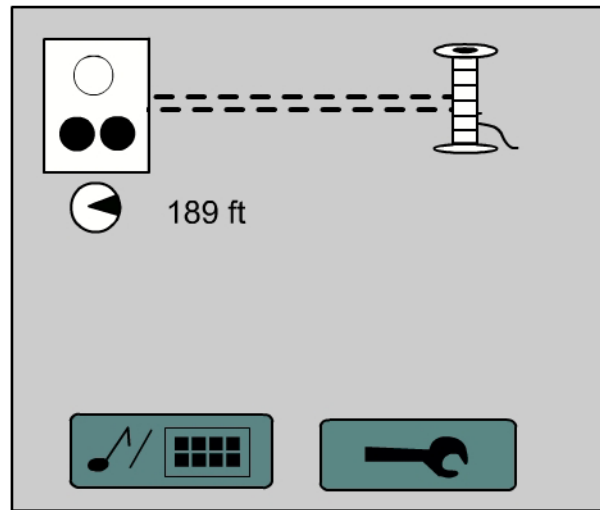
- Pressing the right button goes to ping configuration, which was covered in the prior lab.

Step 4 Test length and continuity for a long cable run

The LinkRunner Cable Test function helps to determine whether the cable length is within specification. This is a basic test of a long cable to determine that all four pairs of wires are intact and have the same length. The diagram below shows a good cable test.

Turn on the LinkRunner by pressing the small button in the lower right corner. What does the display look like now?

- a. Use a long straight-through cable drop which is not connected to a patch panel, hub, or switch at the other end. Plug one end of the cable into the RJ-45 LAN port on the LinkRunner. What does the display look like now? _____
- b. What is the length of the cable being tested? _____



Step 5 Test length and wire map for good and bad patch cables

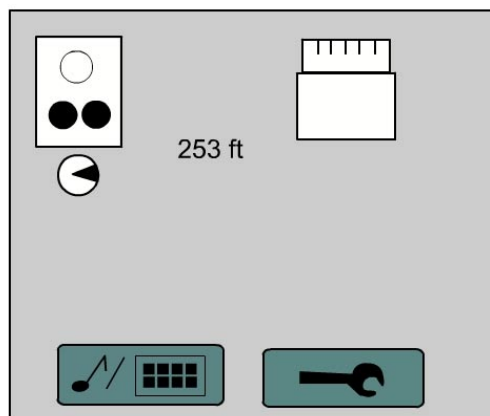
The Cable Test function helps to determine whether the cable length is within specification, if it is a straight or crossover, and whether it has any faults. These tests work for both structured and patch cables. This will test cable integrity for excessive length, opens, shorts, crossed wires, and split pairs.

- a. Turn on the LinkRunner by pressing the small button in the lower right corner.
- b. Use a good straight through patch cable. Plug one end of the cable into the RJ-45 LAN port on the LinkRunner and the other end into the LinkRunner RJ-45 MAP port. The diagram below shows the result of testing a good straight through cable. What is the length of the cable?

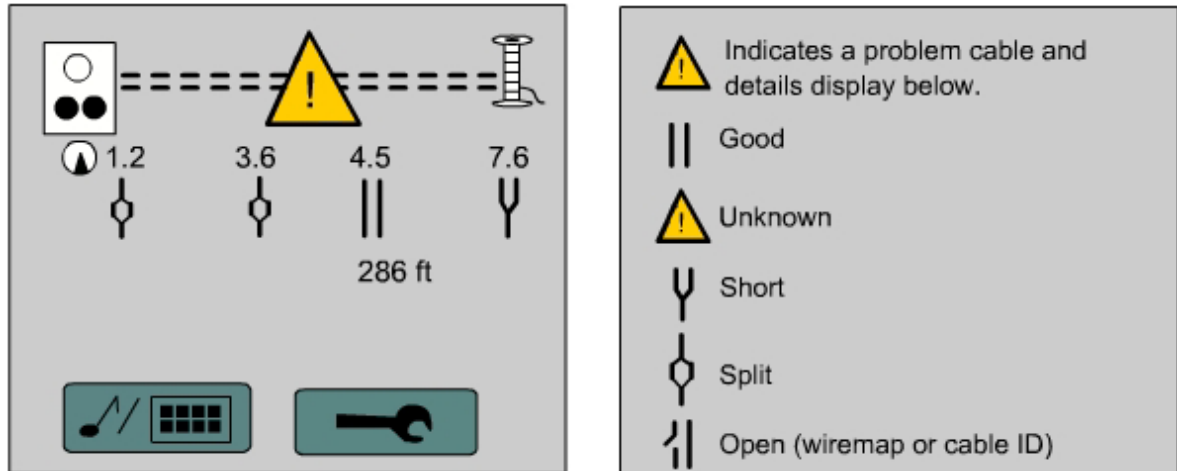
Explain how to tell if this is a straight through or crossover cable. _____

- c. Use a good crossover cable. Plug one end of the cable into the RJ-45 LAN port on the LinkRunner and the other end into the LinkRunner RJ-45 MAP port. What is the length of the cable? _____

Explain how to tell if this is a straight through or crossover cable. _____



- d. Use a bad straight through patch cable that is improperly wired or has some faults in the wires. Plug one end of the cable into the RJ-45 LAN port on the LinkRunner and the other end into the RJ-45 MAP port. The diagram below shows a problem cable with symbols indicating the type of problems that may be encountered. What problem was encountered?



Step 6 Test length and wire map for long cable runs

- Turn on the LinkRunner by pressing the small button in the lower right corner.
- Use a good workstation patch cable drop to a wall plate, which is connected to a patch panel at the other end but not to a hub or switch. Plug the cable into the RJ-45 LAN port on the LinkRunner. Plug the wire map adapter into the associated patch panel port on the opposite end. This will test the cable run from the patch cable in the work area through all horizontal cabling to the patch panel in the wiring closet.
- What is the length of the cable? _____
- Does the cable test OK? _____
- If not, indicate problems encountered.

Step 7 Use Link Pulse to test the connection to a hub/switch and identify the cable location

Link Pulse blinks the hub or switch port link light while simultaneously sending a tone on the wire to aid in cable location. Use the optional Microprobe Tone Receiver to pick up a tone and audibly locate cables. The optional Cable ID kit can be used to identify unmarked segments.

- Obtain a good patch cable of any length. Plug one end directly into an active regular hub or switch port. Plug the other end into the LinkRunner LAN port.
- Press the left SoftKey (musical note and hub symbol). What does this cause the link light on the hub or switch port to do?
- What does this test do and how could it be useful in locating or identifying where cables terminate?

Step 8 Test PC NIC functionality

- a. Turn on the LinkRunner by pressing the small button in the lower right corner.
 - b. Plug one end of a patch cable into the RJ-45 LAN port on the LinkRunner and the other end into the PC NIC. If the PC NIC link light comes on, then the NIC is good. Did the NIC test OK?
-

Step 9 Disconnect the equipment and store the cabling and devices



Lab 5.1.5 RJ-45 Jack Punch Down

Objective

- Learn the correct process for terminating or punching down an RJ-45 jack
- Learn the correct procedure for installing the jack in a wall plate

Background / Preparation

In this lab, the student will learn to wire an RJ-45 data jack for installation in a wall plate using a punch-down tool. These skills are useful when it is necessary to install a small amount of cabling in an office or residence. A punch tool is a device that uses spring-loaded action to push wires between metal pins, while at the same time skinning the sheath away from the wire. This ensures that the wire makes a good electrical connection with the pins inside the jack. The punch tool also cuts off any extra wire.

Category 5 or Category 5e cabling and Category 5 or 5e rated T568B jacks will be used. A Category 5/5e straight-through patch cable with an RJ-45 connector will normally plug into this data jack or outlet to connect a PC in a work area to the network. It is important to use Category 5 or 5e rated jacks and patch panels with Category 5 or 5e cabling in order to support Fast Ethernet (100 Mbps) and Gigabit Ethernet (1000 Mbps). The process of punching down wires into a data jack in an office area is the same as punching them down in a patch panel in a wiring closet. The following resources are required:

- 60 - 90 cm (2 - 3 feet) length of Category 5/5e cabling, which can be one per person or one per team
- Two Category 5/5e RJ-45 data jacks (one extra for spare) – If RJ-45 data jacks are installed on both ends of the cable, the installation can be tested by inserting cable with RJ-45 connectors and a simple cable continuity tester.
- Category 5/5e wall plate
- 110 type punch-down tool
- Wire cutters

Use the following procedure and diagram to punch down the wires into the RJ-45 jack and install the jack into the wall plate:

Step 1

Remove the jacket 2.54 cm (1 inch) from the end of the cable.

Step 2

Position wires in the proper channels on the jack maintaining the twists as closely as possible. The diagram below shows an example of how to place the wires on one type of jack. Most jacks will have the channels color-coded to indicate where the wires go. The photo of the jack on the next page shows one variety of jack. Jacks are typically stamped to indicate whether they are T568A or B as shown in the photo.

Step 3

Use the 110 punch-down tool shown below to push conductors into the channels. Make sure to position the cut side of the punch-down tool so that it faces the outside of the jack. If this is not done, it will cut the wire being punched down. Try tilting the handle of the punch tool a little to the outside, so it will cut better. If any wire remains attached after using the punch tool, simply twist the ends gently to remove them. Then place the clips on the jack, and tighten them. Make sure that no more than 1.27 cm (one half inch) of untwisted wire is between the end of the cable jacket and the channels on the jack.

Step 4

Snap the jack into its faceplate by pushing it in from the back side. Make sure when this is done, that the jack is right-side up so the clip faces down when the wall plate is mounted.

Step 5

Use the screws to attach the faceplate to either the box or to the bracket. If there is a surface-mounted box, keep in mind that it might hold 30 - 60 cm (1 - 2 feet) of excess cable. Then it will be necessary to either slide the cable through its tie-wraps or pull back the raceway that covers it in order to push the rest of the excess cable back into the wall. If there is a flush-mounted jack, all that is needed is to push the excess cable back into the wall.

Category 5 T568B Jack Wiring Color Scheme

Hold the jack with the 8-pin jack receptacle, which is the part that the RJ-45 connector goes into, facing up or away from the body while looking at the wire channels or slots. There should be four wire channels on each side. Match the wiring colors to the codes on the jack.



Single Wire punch tool



8-pin receptacle	
White Green	White Blue
Green	Blue
White Brown	White Orange
Brown	Orange



Lab 5.1.7 Hub and NIC Purchase

Objective

- Introduce the variety and prices of network components in the market
- Gather pricing information for hubs and Ethernet NICs for a small network

Background / Preparation

A friend has asked for help putting together a price list for a small LAN to be set up in a very small business. Rapid growth is not really a concern. The business has computers, but it has not networked the computers together. They are getting a DSL connection, so that they can access the Internet. They have been told that all they need is a small hub and connections to each computer to complete the project. Each machine is running a version of Windows that will work on a peer-to-peer network. The lab will use the Web site www.cdw.com, but any local source, catalog, or Web site can be used. The requirements include the following:

- 1 – Ethernet Hub
- 2 – Ethernet NICs for existing laptop PCs
- 3 – Ethernet NICs for existing desktop PCs
- 4 – Ethernet Cat 5e jumper cables – length 6.1 meters (20 feet)

Step 1 Research equipment pricing

Use at least three other sources for technologies and pricing. For Web searches, try www.cdw.com, www.google.com, or any other search engines that are preferred. Look at the prices for small hubs and how much more would it cost to use a small switch. Compare the cost to a wireless implementation.

Step 2 Compile one page summary of the results

Use Microsoft Excel, Word, or any comparable products to compile a one page summary of the results. A comparison table should show the choices and the features or factors that were compared, such as number of ports, features, price, performance, and so on.

Lab 5.1.10 Purchasing LAN Switches



Objective

- Introduce the variety and prices of network components in the market
- Gather pricing information for Ethernet switches and NICs for a network

Background / Preparation

Put together a proposal for replacing hubs with switches at a branch office. Research at least two different solutions and develop a proposal. The project details are the following:

- The company has a branch location still using an Ethernet hub network. Congestion issues are getting to be a serious problem as more and more services are being added to the network. Currently each of the four floors has one or more hubs in a wiring closet supporting 30-35 computers except the ground floor, which has 65 computers.
- The four floors plug into an 8-port 10-Mbps switch that was added earlier to reduce the congestion problems. While that solution was a major improvement it cannot keep up all of the time anymore. The two servers and router to the Internet also connect to the 8-port switch.
- The branch cabling is relatively new and certified to Category 5 standards. The company is not interested in any major cabling changes at this time.
- At least 75% of the 160 current workstations have NICs with 10/100, full duplex capabilities. All laptop computers have the newer NICs. All new machines include similar NICs.
- Consider what should be done with the existing switch. Are there higher bandwidth options for connecting the two servers?

The requirements include the following:

- Replace all hubs with switches.
- Replace the 10 Mbps NICs for existing desktop PCs.
- Each host connection should be 10/100 Mbps minimum.

Step 1 Research equipment pricing

Start by going to www.cisco.com and selecting “Products & Solutions” and following the links to “Switches” to gather basic information. Look specifically at the Catalyst 29xx and 35xx models.

Use at least three other sources for technologies and pricing. When doing Web searches, try www.cdw.com, www.google.com, or any other preferred search engines.

Step 2 Compile a table of your results

Use Microsoft Excel, Word, or any comparable products to compile a table of the results.

The first page is The Executive Summary where the recommended choice of products and the total cost is written. Include a short 8-15 line reason why this implementation was selected.

The second page is a comparison table showing the choices that were looked at and the features or factors that were compared such as price, performance, and so on.

The third page explains any security concerns discovered in the research. Summarize them as a bulleted list. Summarize whether the concerns are serious and if they can be overcome.

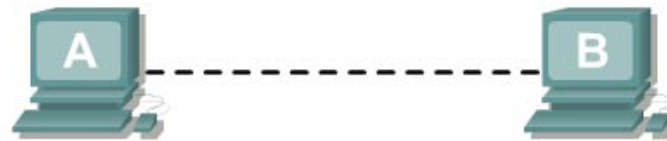
Optional Step 2 Create a 4-8 slide PowerPoint presentation




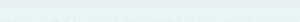
Instead of creating the above Excel or Word documents, create a four to eight slide PowerPoint presentation covering the same requirements.

Assume that there will be a presentation of the material.

If time allows, do both of these. That would often be the norm.

Lab 5.1.12 Building a Peer-to-Peer Network



Straight-through cable	
Serial cable	
Rollover (console)	
Crossover cable	

Objective

- Create a simple peer-to-peer network between two PCs
- Identify the proper cable to connect the two PCs
- Configure workstation IP address information
- Test connectivity using the `ping` command.

Background / Preparation

This lab focuses on the ability to connect two PCs to create a simple peer-to-peer Ethernet LAN between two workstations. The workstations will be directly connected to each other without using a hub or switch. In addition to the Layer 1 physical and Layer 2 data link connections, the computers must also be configured with the correct IP network settings, which is Layer 3, so that they can communicate. A basic Category 5/5e UTP crossover cable is all that is needed. A crossover cable is the same type that would be used as backbone or vertical cabling to connect switches together. Connecting the PCs in this manner can be very useful for transferring files at high speed and for troubleshooting interconnecting devices between PCs. If the two PCs can be connected with a single cable and are able to communicate, then any networking problems are not with the PCs themselves. Start this lab with the equipment turned off and with cabling disconnected. Work in teams of two with one person per PC. The following resources will be required:

- Two workstations with an Ethernet 10/100 NIC installed
- Several Ethernet cables, which are both straight-through and crossover, to choose from for connecting the two workstations

Step 1 Identify the proper Ethernet cable and connect the two PCs

- a. The connection between the two PCs will be accomplished using a Category 5 or 5e crossover cable. Locate a cable that is long enough to reach from one PC to the other, and attach one end

to the NIC in each of the PCs. Be sure to examine the cable ends carefully and select only a crossover cable.

- b. What kind of cable is required to connect from NIC to NIC? _____
- c. What is the category rating of the cable? _____
- d. What is the AWG wire size designation of the cable? _____

Step 2 Verify the physical connection

- a. Plug in and turn on the computers. To verify the computer connections, insure that the link lights on both NICs are lit. Are both link lights lit? _____

Step 3 Access the IP settings window

Note: Be sure to write down the existing IP settings, so that they can be restored at the end of the lab. These include IP address, subnet mask, default gateway, and DNS servers. If the workstation is a DHCP client, it is not necessary to record this information.

Windows 95 / 98 / Me/ users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC and click on **Properties**.
- Click on the **IP Address** tab and the **Gateway** tab.

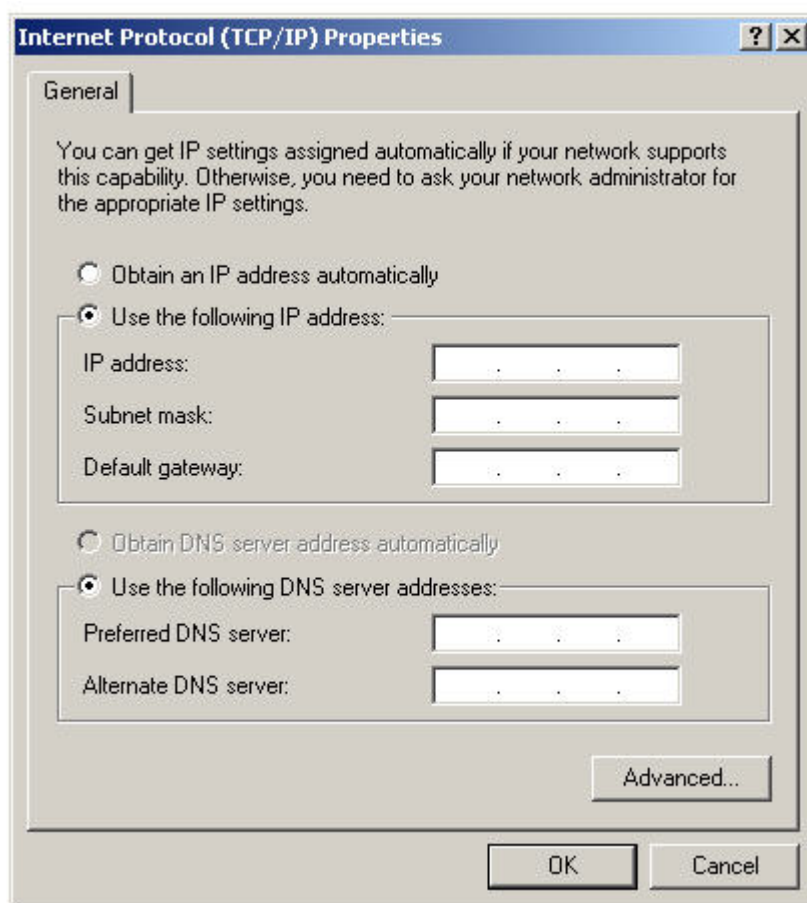
Windows NT / 2000 users should do the following:

- Click on **Start > Settings > Control Panel** and then open the **Network and Dial-up Connections** folder.
- Click and open the **Local Area Connection** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

Windows XP users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network Connection** icon.
- Select the **Local Area Network Connection** and click on **Change settings of this connection**.
- Select the **TCP/IP protocol** icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

See the example below:



Step 4 Configure TCP/IP settings for the two PCs

- Set the IP address information for each PC according to the information in the table.
- Note that the default gateway IP address is not required, since these computers are directly connected. The default gateway is only required on local area networks that are connected to a router.

Computer	IP Address	Subnet mask	Default Gateway
PC – A	192.168.1.1	255.255.255.0	Not Required
PC – B	192.168.1.2	255.255.255.0	Not Required

Step 5 Access the Command or MS-DOS prompt

- Use the Start menu to open the Command Prompt (MS-DOS-like) window:

Windows 95 / 98 / Me users should do the following:

Start > Programs > MS-DOS Prompt

Windows NT / 2000 users should do the following:

Start > Programs > Accessories > Command Prompt

Windows XP users should do the following:

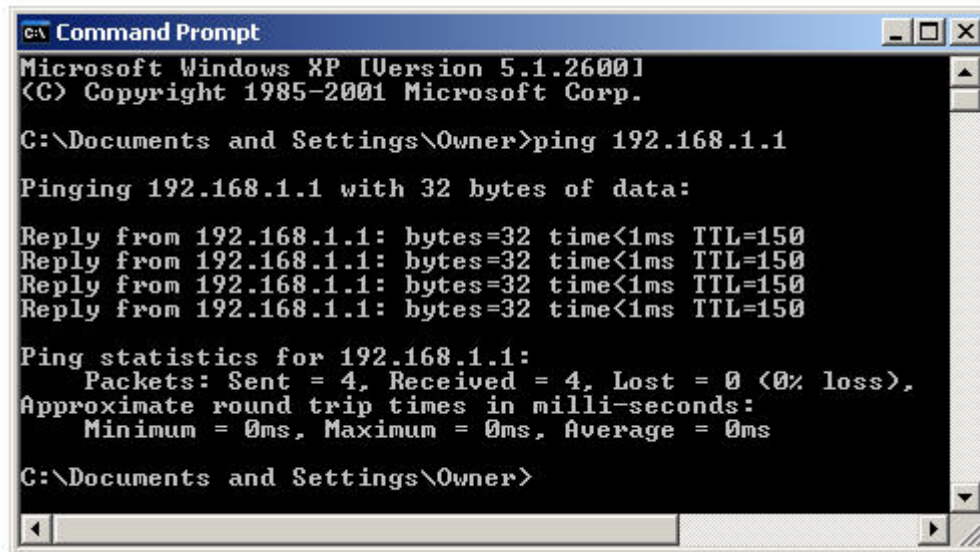
Start > Programs > Accessories > Command Prompt

Step 6 Verify that the PCs can communicate

- Test connectivity from one PC to the other by pinging the IP address of the opposite computer. Use the following command at the command prompt.

```
C:>ping 192.168.1.1 (or 192.168.1.2)
```

- Look for results similar to those shown below. If not, check the PC connections and TCP/IP settings for both PCs. What was the ping result?



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

Step 7 Confirm the TCP/IP network settings

Windows 95 / 98 / Me users should do the following:

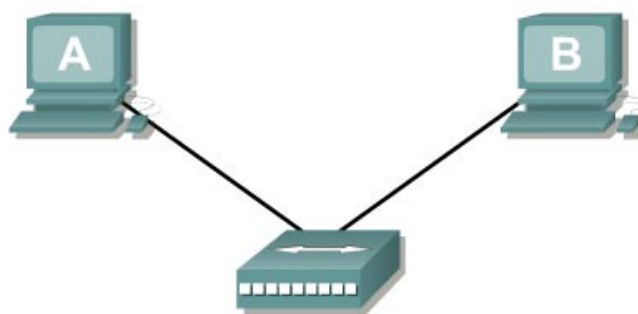
- Type the `winipcfg` command from the MS-DOS Prompt. Record the results:

Windows NT / 2000 / XP users should do the following:

- Type the `ipconfig` command from the Command Prompt. Record the results:

Step 8 Restore the PCs to their original IP settings, disconnect the equipment, and store the cables

Lab 5.1.13a Building a Hub-based Network



Straight-through cable	—————
Serial cable	————— ⚡
Rollover (console)
Crossover cable	- - - - -

Objective

- Create a simple network with two PCs using a hub
- Identify the proper cable to connect the PCs to the hub
- Configure workstation IP address information
- Test connectivity using the `ping` command

Background / Preparation

This lab focuses on the ability to connect two PCs to create a simple hub-based Ethernet LAN using two workstations. A hub is a networking concentration device sometimes referred to as a multiport repeater. Hubs are inexpensive and easy to install, but they permit collisions to occur. They are appropriate for a small LAN with light traffic.

In addition to the physical and data link connections, which are Layers 1 and 2, the computers must also be configured with the correct IP network settings, which is Layer 3, so that they can communicate. Since this lab uses a hub, a basic Category 5/5e UTP straight-through cable is needed to connect each PC to the hub. This is referred to as a patch cable or horizontal cabling, which is used to connect workstations and a typical LAN. Start this lab with the equipment turned off and with cabling disconnected. Work in teams of two with one person per PC. The following resources will be required:

- Two workstations with an Ethernet 10/100 NIC installed
- Ethernet 10BaseT or Fast Ethernet hub

- Several Ethernet cables, which are straight-through and crossover, to choose from for connecting the two workstations

Step 1 Identify the proper Ethernet cable and connect the two PCs to the hub

- The connection between the two PCs and the hub will be accomplished using a Category 5 or 5e straight-through patch cable. Locate two cables that are long enough to reach from each PC to the hub. Attach one end to the NIC and the other end to a port on the hub. Be sure to examine the cable ends carefully and select only a straight-through cable.
- What kind of cable is required to connect from NIC to hub? _____
- What is the category rating of the cable? _____
- What is the AWG wire size designation of the cable? _____

Step 2 Verify the physical connection

- Plug in and turn on the computers. To verify the computer connections, insure that the link lights on the both PC NICs and the hub interfaces are lit. Are all link lights lit? _____

Step 3 Access the IP settings window

Note: Be sure to write down the existing IP settings, so that they can be restored at the end of the lab. These include IP address, subnet mask, default gateway, and DNS servers. If the workstation is a DHCP client, it is not necessary to record this information.

Windows 95/98/Me users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC and click on **Properties**.
- Click on the **IP Address** tab and the **Gateway** tab.

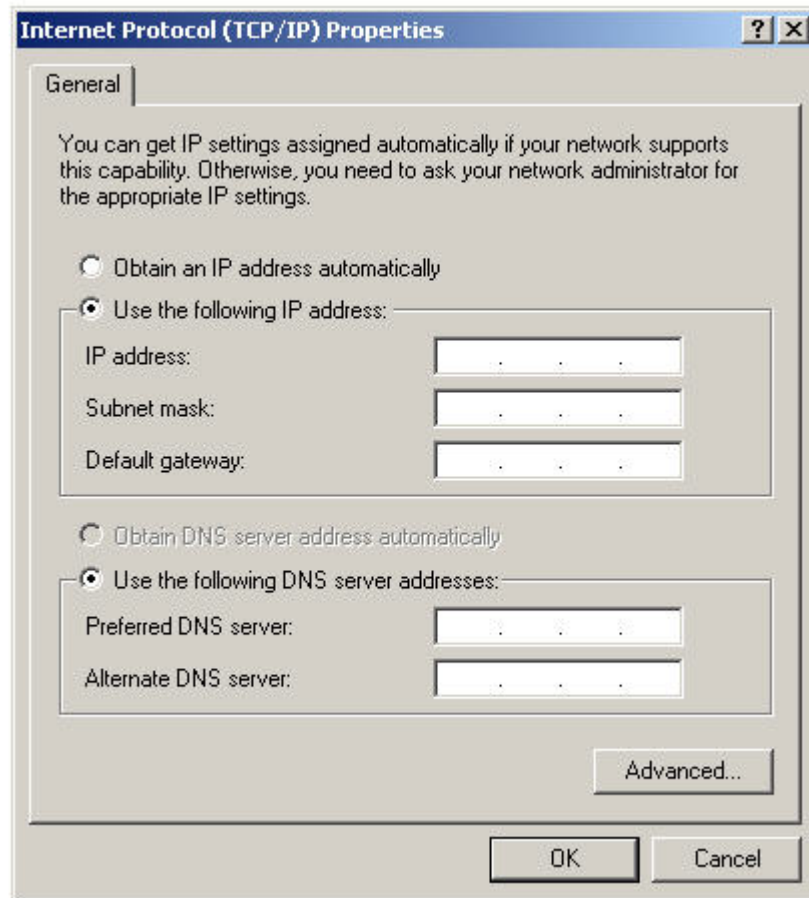
Windows NT/2000 users should do the following:

- Click on **Start > Settings > Control Panel** and then open the **Network and Dial-up Connections** folder.
- Click and open the **Local Area Connection** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

Windows XP users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network Connection** icon.
- Select the Local Area Network Connection and click on **Change settings of this connection**.
- Select the **TCP/IP protocol** icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

See the example below:



Step 4 Configure TCP/IP settings for the two PCs

- Set the IP address information for each PC according to the information in the table.
- Note that the default gateway IP address is not required, since these computers are directly connected. The default gateway is only required on local area networks that are connected to a router.

Computer	IP Address	Subnet mask	Default Gateway
PC – A	192.168.1.1	255.255.255.0	Not Required
PC – B	192.168.1.2	255.255.255.0	Not Required

Step 5 Access the Command or MS-DOS prompt

- Use the Start menu to open the Command Prompt (MS-DOS-like) window:

Windows 95/98/Me users should do the following:

Start > Programs > MS-DOS Prompt

Windows NT/2000 users should do the following:

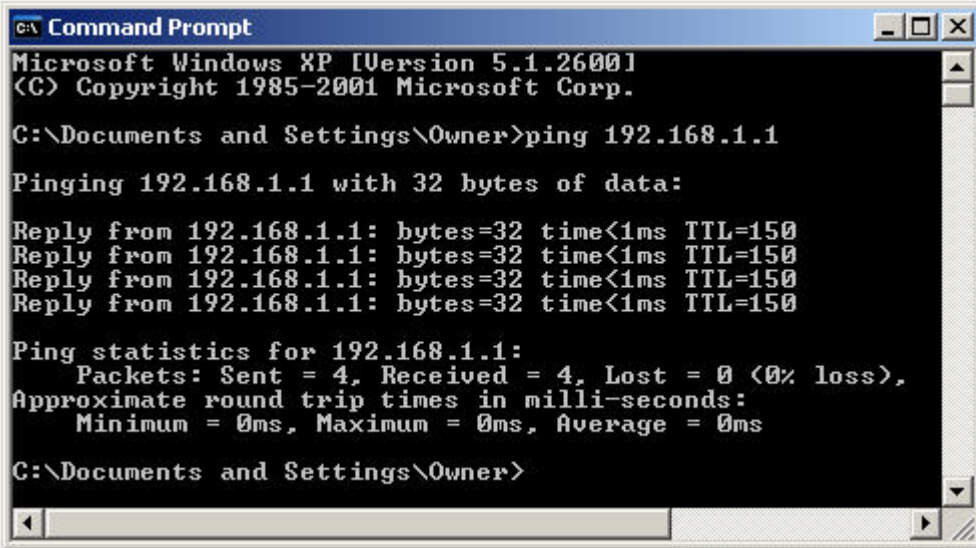
Start > Programs > Accessories > Command Prompt

Windows XP users should do the following:

Start > Programs > Accessories > Command Prompt

Step 6 Verify that the PCs can communicate

- a. Test connectivity from one PC to the other through the hub by pinging the IP address of the opposite computer. Use the following command at the command prompt.
`C:>ping 192.168.1.1 (or 192.168.1.2)`
- b. Look for results similar to those shown below. If not, check the PC connections and TCP/IP settings for both PCs. What was the ping result?



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600.1
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

Step 7 Confirm the TCP/IP network settings

Windows 95 / 98 / Me users should do the following:

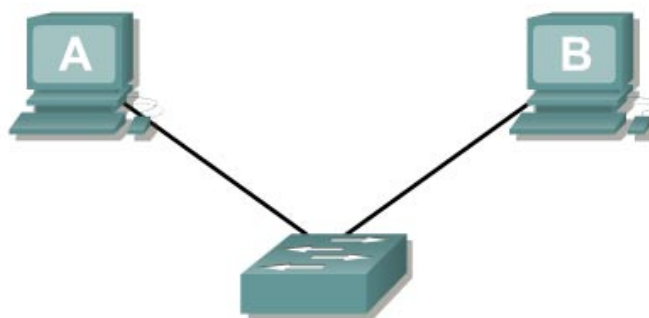
- a. Type the `winipcfg` command from the MS-DOS Prompt. Record the results.


Windows NT / 2000 / XP users should do the following:

- b. Type the `ipconfig` command from the Command Prompt. Record the results.

Step 8 Restore the PCs to their original IP settings, disconnect the equipment, and store the cables

Lab 5.1.13b Building a Switch-based Network



Straight-through cable	—————
Serial cable	———  ———
Rollover (console)
Crossover cable	- - - - -

Objective

- Create a simple network with two PCs using a switch
- Identify the proper cable to connect the PCs to the switch
- Configure workstation IP address information
- Test connectivity using the `ping` command

Background / Preparation

This lab focuses on the ability to connect two PCs to create a simple switch-based Ethernet LAN using two workstations. A switch is a networking concentration device sometimes referred to as a multiport bridge. Switches are relatively inexpensive and easy to install. When operating in full-duplex mode, they provide dedicated bandwidth to workstations. Switches eliminate collisions by creating microsegments between ports to which the two workstations are attached. They are appropriate for small to large LANs with moderate to heavy traffic.

In addition to the physical and data link connections, which are Layers 1 and 2, the computers must also be configured with the correct IP network settings, which is Layer 3, so that they can communicate. Since this lab uses a switch, a basic Category 5/5e UTP straight-through cable is needed to connect each PC to the switch. This is referred to as a patch cable or horizontal cabling, which is used to connect workstations and a typical LAN. Start this lab with the equipment turned off and with cabling disconnected. Work in teams of two with one person per PC. The following resources will be required:

- Two workstations with an Ethernet 10/100 NIC installed
- Ethernet 10BaseT or Fast Ethernet switch
- Several Ethernet cables, which are straight-through and crossover, to choose from for connecting the two workstations

Step 1 Identify the proper Ethernet cable and connect the two PCs to the switch

- The connection between the two PCs and the switch will be accomplished using a Category 5 or 5e straight-through patch cable. Locate two cables that are long enough to reach from each PC to the switch. Attach one end to the NIC and the other end to a port on the switch. Be sure to examine the cable ends carefully and select only a straight-through cable.
- What kind of cable is required to connect from NIC to switch? _____
- What is the category rating of the cable? _____
- What is the AWG wire size designation of the cable? _____

Step 2 Verify the physical connection

- Plug in and turn on the computers. To verify the computer connections, insure that the link lights on the both PC NICs and the switch interfaces are lit. Are all link lights lit? _____

Step 3 Access the IP settings window

Note: Be sure to write down the existing IP settings, so that they can be restored at the end of the lab. These include IP address, subnet mask, default gateway, and DNS servers. If the workstation is a DHCP client, it is not necessary to record this information.

Windows 95 / 98 / Me/ users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC and click on **Properties**.
- Click on the **IP Address** tab and the **Gateway** tab.

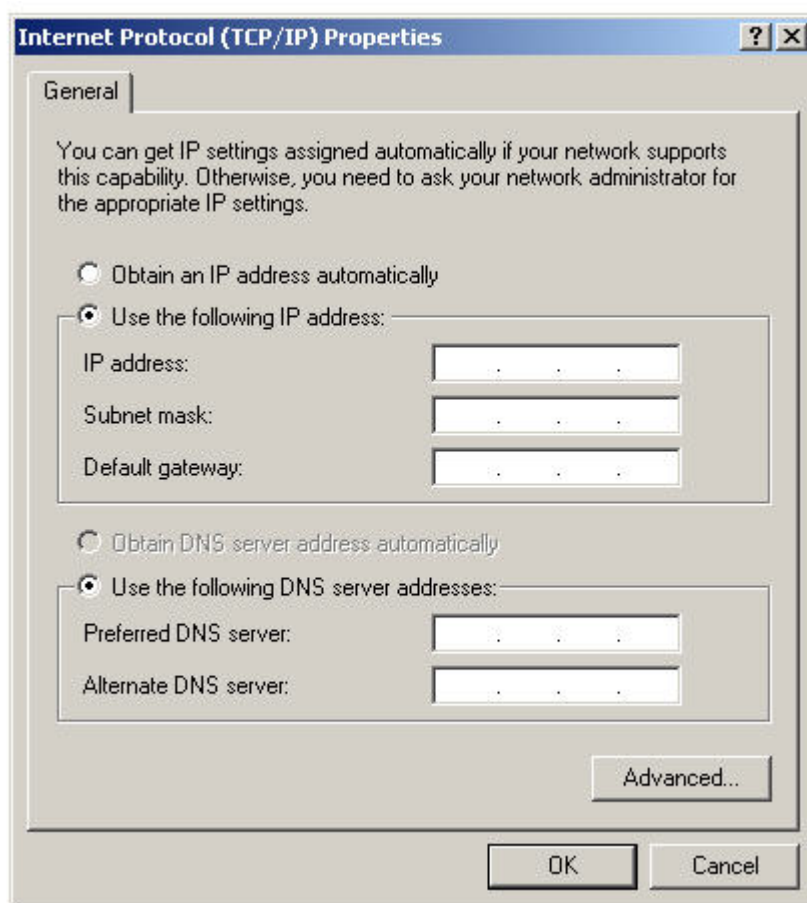
Windows NT / 2000 users should do the following:

- Click on **Start > Settings > Control Panel** and then open the **Network and Dial-up Connections** folder.
- Click and open the **Local Area Connection** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

Windows XP users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network Connection** icon.
- Select the Local Area Network Connection and click on **Change settings of this connection**.
- Select the **TCP/IP protocol** icon that is associated with the NIC on this PC.
- Click on **Properties** and click on **Use the following IP address**.

See the example below:



Step 4 Configure TCP/IP settings for the two PCs

- Set the IP address information for each PC according to the information in the table.
- Note that the default gateway IP address is not required, since these computers are directly connected. The default gateway is only required on local area networks that are connected to a router.

Computer	IP Address	Subnet mask	Default Gateway
PC – A	192.168.1.1	255.255.255.0	Not Required
PC – B	192.168.1.2	255.255.255.0	Not Required

Step 5 Access the Command or MS-DOS prompt

- Use the Start menu to open the Command Prompt (MS-DOS-like) window:

Windows 95 / 98 / Me users should do the following:

Start > Programs > MS-DOS Prompt

Windows NT / 2000 users should do the following:

Start > Programs > Accessories > Command Prompt

Windows XP users should do the following:

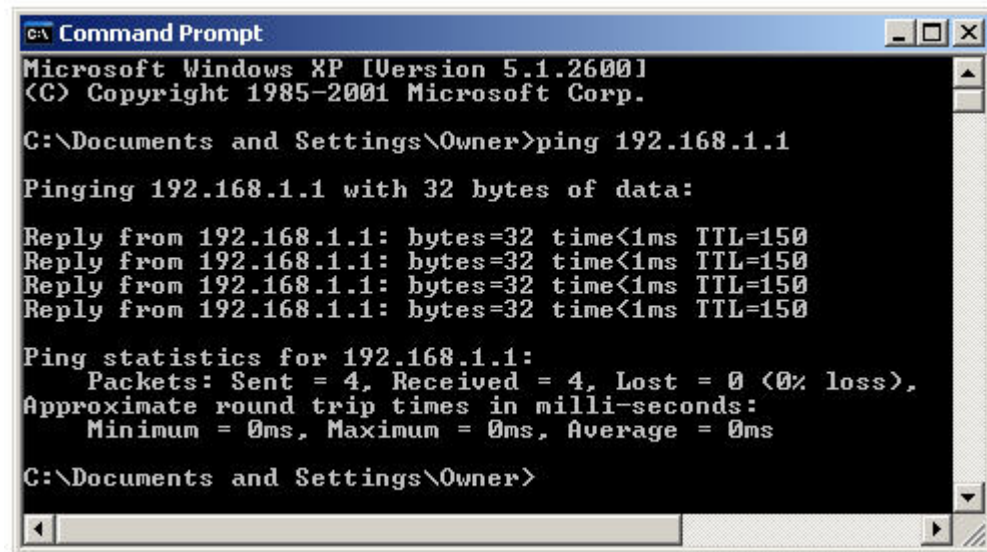
Start > Programs > Accessories > Command Prompt

Step 6 Verify that the PCs can communicate

- a. Test connectivity from one PC to the other through the switch by pinging the IP address of the opposite computer. Use the following command at the command prompt.

```
C:>ping 192.168.1.1 (or 192.168.1.2)
```

- b. Look for results similar to those shown below. If not, check the PC connections and TCP/IP settings for both PCs. What was the ping result?



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150
Reply from 192.168.1.1: bytes=32 time<1ms TTL=150

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

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

Step 7 Confirm the TCP/IP network settings

Windows 95 / 98 / Me users should do the following:

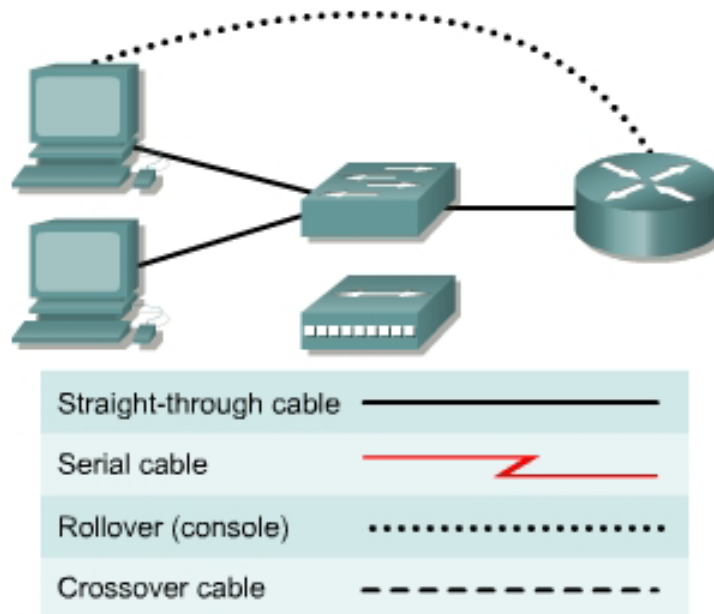
- a. Type the `winipcfg` command from the MS-DOS Prompt. Record the results.

Windows NT / 2000 / XP users should do the following:

- b. Type the `ipconfig` command from the Command Prompt. Record the results.

Step 8 Restore the PCs to their original IP settings, disconnect the equipment, and store the cables

Lab 5.2.3a Connecting Router LAN Interfaces



Objective

- Identify the Ethernet or Fast Ethernet interfaces on the router
- Identify and locate the proper cables to connect the router and PC to a hub or switch
- Use the cables to connect the router and PC to the hub or switch

Background / Preparation

This lab focuses on the ability to connect the physical cabling between Ethernet LAN devices such as hubs and switches and the appropriate Ethernet interface on a router. The computer(s) and router should be preconfigured with the correct IP network settings. Start this lab with the computer(s), router, and the hub or switch all turned off and unplugged. The following resources will be required:

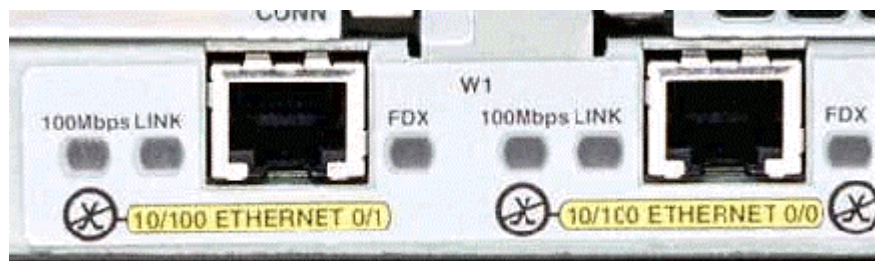
- At least one workstation with an Ethernet 10/100 NIC installed
- One Ethernet switch or hub
- One router with an RJ-45 Ethernet or Fast Ethernet interface or an AUI interface
- 10BASE-T AUI transceiver (DB-15 to RJ-45) for a router with an AUI Ethernet interface (2500 Series)
- Several Ethernet cables, which are straight-through and crossover, to choose from for connecting the workstation and router to the hub or switch.

Step 1 Identify the Ethernet or Fast Ethernet interfaces on the router

- Examine the router.

What is the model number of the router? _____

- Locate one or more RJ-45 connectors on the router labeled “Ethernet0” or “Ethernet1”. This identifier may vary depending on the type of router used; a 2600 series router is shown. A 2500 series router will have an AUI DB-15 Ethernet port labeled AUI 0. These will require a 10BASE-T transceiver to connect to the RJ-45 cable.



- Identify the Ethernet ports shown that could be used for connecting the routers. Record the information below. Record the AUI port numbers if a Cisco 2500 series router is being used.

Router	Port	Port

Step 2 Identify the proper cables and connect router

- The connection between the router and the hub or switch will be accomplished using a Category 5 straight-through patch cable. Locate a patch cable that is long enough to reach from the router to the hub. Be sure to examine the cable ends carefully and select only straight-through cables.
- Use a cable to connect the Ethernet interface that uses zero designation on the router to a port on the hub or switch. This identifier may vary depending on the type of router used; a 2600 series router is shown.

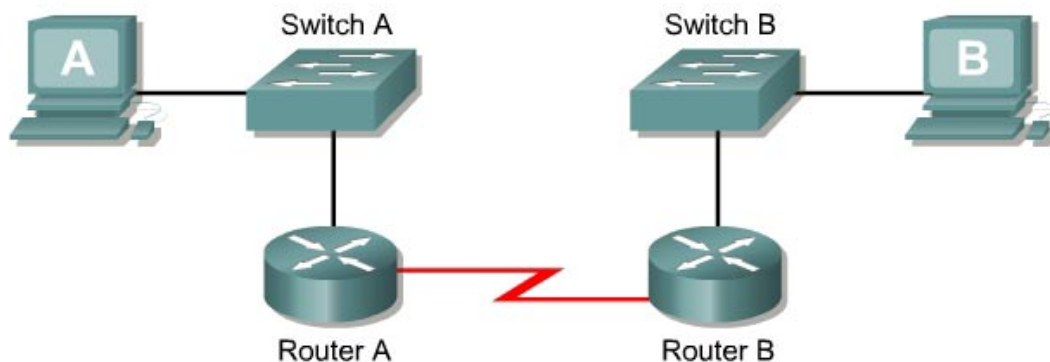
Step 3 Connect the workstation Ethernet cabling


- The computer(s) will also connect to the hub using a straight-through patch cable. Run Category 5 patch cables from each PC to where the switch or hub is located. Connect one end of these cables to the RJ-45 connector on the computer NIC and connect the other end to a port on the hub or switch. Be sure to examine the cable ends carefully and select only straight-through cables.

Step 4 Verifying the connection

- Plug in and turn on the routers, computers, and hub or switch.
- To verify the router connections, insure that the link light on the router interface and the hub or switch interface are both lit.
- To verify the computer connections, insure that the link light on the NIC and the hub or switch interface are both lit.

Lab 5.2.3b Building a Basic Routed WAN



Straight-through cable	—————
Serial cable	———  ———
Rollover (console)
Crossover cable	- - - - -

Objective

- Create a simple routed wide-area network (WAN) with two PCs, two switches or hubs, and two routers
- Identify the proper cables to connect a PC and router to each switch
- Identify the proper cables to connect the routers to form a WAN link
- Configure workstation IP address information
- Test connectivity using the `ping` command

Background / Preparation

This lab focuses on the ability to connect two simple LANs, each consisting of a workstation and a switch or hub, to form a basic router-to-router WAN. A router is a networking device that can be used to interconnect LANs which routes packets between different networks using Layer 3 IP addressing. Routers are typically used to connect the Internet.

In addition to the physical and data link connections, which are Layers 1 and 2, the computers and routers must also be configured with the correct IP network settings, which is Layer 3, so that they can communicate. Straight-through patch cables are used to connect each PC and router to its switch or hub. Two special V.35 cables are used to create the simulated WAN link between the routers.

Note: The two routers need to be preconfigured by the instructor or lab assistant to have the correct IP addresses on their LAN and WAN interfaces. Router A will provide the clocking signal as DCE.

Start this lab with the equipment turned off and with cabling disconnected. Work in teams of two with one person per LAN. The following resources will be required:

- Two workstations with an Ethernet 10/100 NIC installed
- Two Ethernet 10BaseT or Fast Ethernet switches or two hubs
- Two routers with an RJ-45 Ethernet or Fast Ethernet interface (or an AUI interface) and at least one serial interface.
- 10BASE-T AUI transceiver (DB-15 to RJ-45) for a router with an AUI Ethernet interface, which is a 2500 Series
- Four Ethernet straight-through cables for connecting the workstations and routers to the hub or switch
- One female (DCE) and one male (DTE) V.35 cable for interconnecting the routers

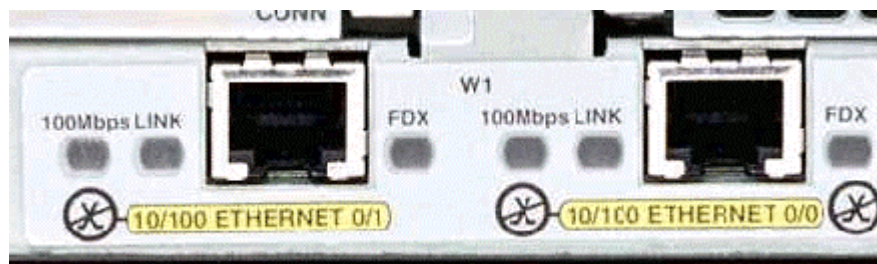
Step 1 Identify and connect the proper Ethernet cable from the PC to the switch

- The connection between the PC and the switch will be accomplished using a Category 5 or 5e straight-through patch cable. Attach one end to the NIC and the other end to a port on the switch or hub. Be sure to examine the cable ends carefully and select only a straight-through cable.
- Examine the switch or hub.

What is the model number of the switch or hub? _____

Step 2 Identify the Ethernet or Fast Ethernet interfaces on the routers

- Examine the routers.
- What is the model number of the Router A? _____
- What is the model number of the Router B? _____
- Locate one or more RJ-45 connectors on each router labeled "10/100 Ethernet" as shown below. The identifier may vary depending on the type of router used; a 2600 series router is shown. A 2500 series router will have an AUI DB-15 Ethernet port labeled "AUI 0". These will require a 10Base-T transceiver to connect to the RJ-45 cable.



- e. Identify the Ethernet ports that could be used for connecting the routers. Record the information below. Record the AUI port numbers when working with a Cisco 2500 series router.

Router	Port	Port

Step 3 Cable the router LAN links

- a. Router configuration

The routers should be preconfigured by the instructor or lab assistant so that the Ethernet 0 interface on each router has the proper IP address and subnet mask as indicated in the table below. This will allow the routers to route packets between local-area networks 192.168.1.0 and 192.168.2.0.

Router	E0 Interface IP Address	Subnet mask
Router – A	192.168.1.1	255.255.255.0
Router – B	192.168.2.1	255.255.255.0

- b. Connecting the cables

The connection between the router and the hub or switch will be accomplished using a Category 5 straight-through patch cable. Locate a patch cable that is long enough to reach from the router to the hub. Be sure to examine the cable ends carefully and select only straight-through cables. Connect the Ethernet interface that uses the 0 (zero) designation on the router to a port on the hub or switch. If connecting to 2500 series routers, use the 10BASE-T AUI transceiver.

Step 4 Verify the physical Ethernet connections

- a. Plug in and turn on the computers, switches/hubs and routers. To verify the connections, insure that the link lights on the both PC NICs, both switch/hub interfaces and router Ethernet interfaces are lit. Are all link lights lit? _____ If not, check connections and cable types.

Step 5 Identify the serial interfaces on the router

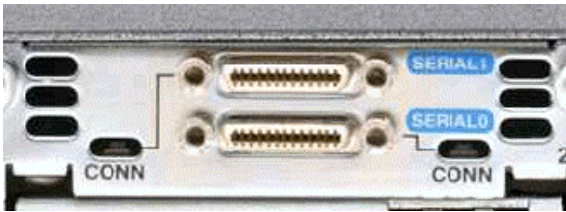

- a. Examine the routers.
- b. Identify the serial ports on each router that could be used for connecting the routers to simulate a WAN link. Record the information below. If there is more than one serial interface, use Interface 0 on each router.

Router Name	Router Serial Port	Router Serial Port
Router A		
Router B		

Step 6 Identify and locate the proper V.35 cables

- Next, inspect the serial cables available in the lab. Depending on the type of router and/or serial card, the router may have different connectors.
- Router serial port characteristics

The two most common types are the DB-60 connector and the smart serial. Using the table below indicate which type routers that are being used.

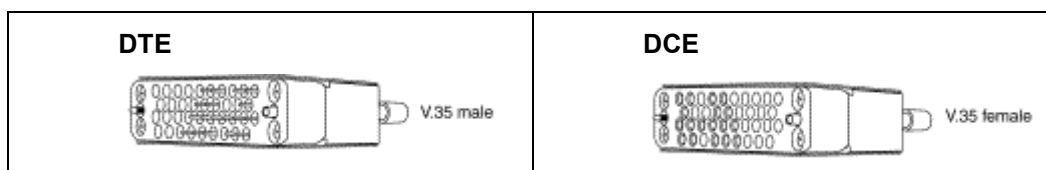
Router	Smart Serial	DB60
		
RTR A	<input type="checkbox"/>	<input type="checkbox"/>
RTR B	<input type="checkbox"/>	<input type="checkbox"/>

- Simulating the WAN link - DCE / DTE and Clocking

Since this will not be through a live lease line, one of the routers will need to provide the clocking for the circuit. This is normally provided to each of the routers by a DCE device such as a CSU/DSU. To provide this clocking signal, one of the routers will need a DCE cable instead of the normal DTE that is used on the other router. Therefore, the connection between routers needs to be done using one DCE cable and one DTE cable between routers. A V.35 DCE cable and a V.35 DTE cable will be used to simulate the WAN connection.

- V. 35 cable characteristics

The V.35 DCE connector is a large female V.35 (34-pin) connector. The DTE cable has a large male V.35 connector. The cables are also labeled as DCE or DTE on the router end of the cable. Use the DCE cable on Router A since it will be providing the clock signal.



Step 7 Cable the router WAN link

a. Router configuration

Router A should be preconfigured by the instructor or lab assistant to provide the DCE clock signal on the Serial 0 interface. The Serial 0 interface on each router should have the proper IP address and subnet mask as indicated in the table below. The network interconnecting the router serial interfaces is 192.168.3.0.

Router	Clocking	S0 Interface IP Address	Subnet mask
Router – A	DCE	192.168.3.1	255.255.255.0
Router – B	DTE	192.168.3.2	255.255.255.0

b. Connecting the cables

The DCE cable will attach to the Serial 0 interface on Router A. The DTE cable should be attached to the Serial 0 interface on Router B. First make the connection between the two V.35 cables. There is only one proper way for the cables to fit together. Align the pins on the male cable with the sockets on the female cables and gently couple them. When they are joined, turn the thumbscrews clockwise to secure the connectors.

Make the connection to each of the routers. Holding the connector in one hand, properly orient the cable connector and the router connector so that the tapers match. Push the cable connector partially into the router connector and tighten the thumb screws to fully insert the cable into the connector.

Step 8 Configure Workstation IP settings

Note: Be sure to write down the existing IP settings so that they can be restored at the end of the lab. These include IP address, subnet mask, default gateway, and DNS servers. If the workstation is a DHCP client, it is not necessary to record this information.

Access the IP Settings window.

Windows 95 / 98 / ME/ users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network** icon.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC and click on **Properties**.
- Click on the **IP Address** tab and the **Gateway** tab.

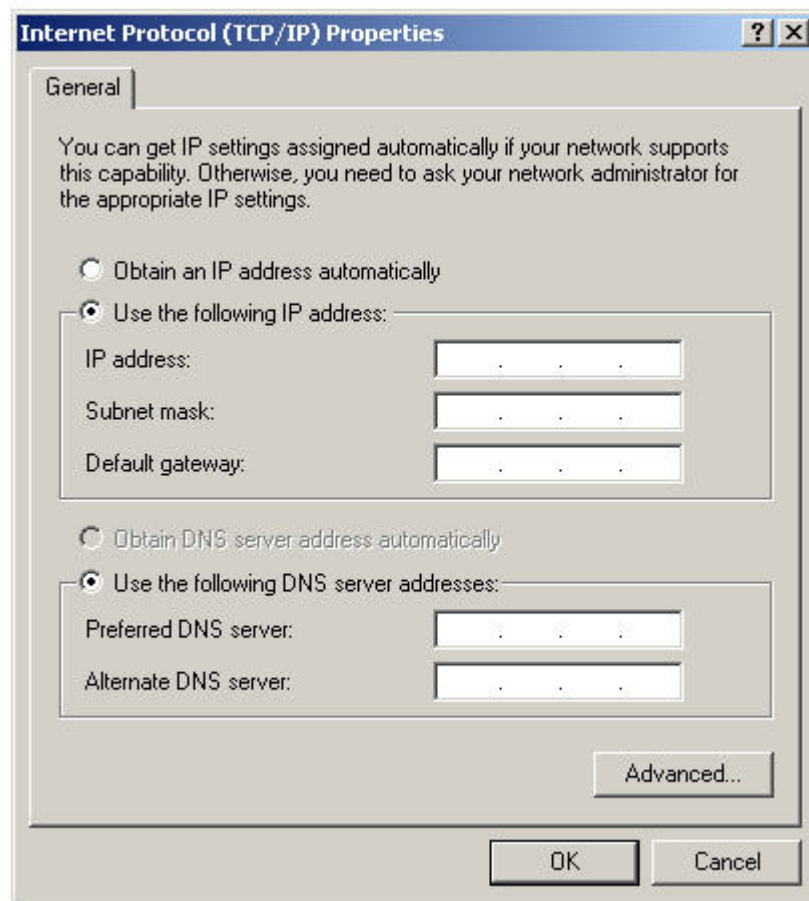
Windows NT / 2000 users should do the following:

- Click on **Start > Settings > Control Panel** and then open the **Network and Dial-up Connections** folder.
- Click and open the **Local Area Connection** icon.
- Select the **TCP/IP protocol** icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

Windows XP users should do the following:

- Click on **Start > Settings > Control Panel** and then click the **Network Connection** icon.
- Select the **Local Area Network Connection** and click on **Change settings of this connection**.
- Select the TCP/IP protocol icon that is associated with the NIC in this PC.
- Click on **Properties** and click on **Use the following IP address**.

See the example below.



Set the IP address information for each PC according to the information in the table.

Note that the IP address of each PC is on the same network as the default gateway, which is the Ethernet interface of the connected router. The default gateway is required on local area networks that are connected to a router.

Computer	IP Address	Subnet mask	Default Gateway
PC – A	192.168.1.2	255.255.255.0	192.168.1.1
PC – B	192.168.2.2	255.255.255.0	192.168.2.1

Step 9 Verify that PCs can communicate across the WAN

- Access the Command Prompt (MS-DOS-like):

Windows 95 / 98 / Me users should do the following:

Start > Programs > MS-DOS Prompt

Windows NT / 2000 users should do the following:

Start > Programs > Accessories > Command Prompt

Windows XP users should do the following:

Start > Programs > Accessories > Command Prompt

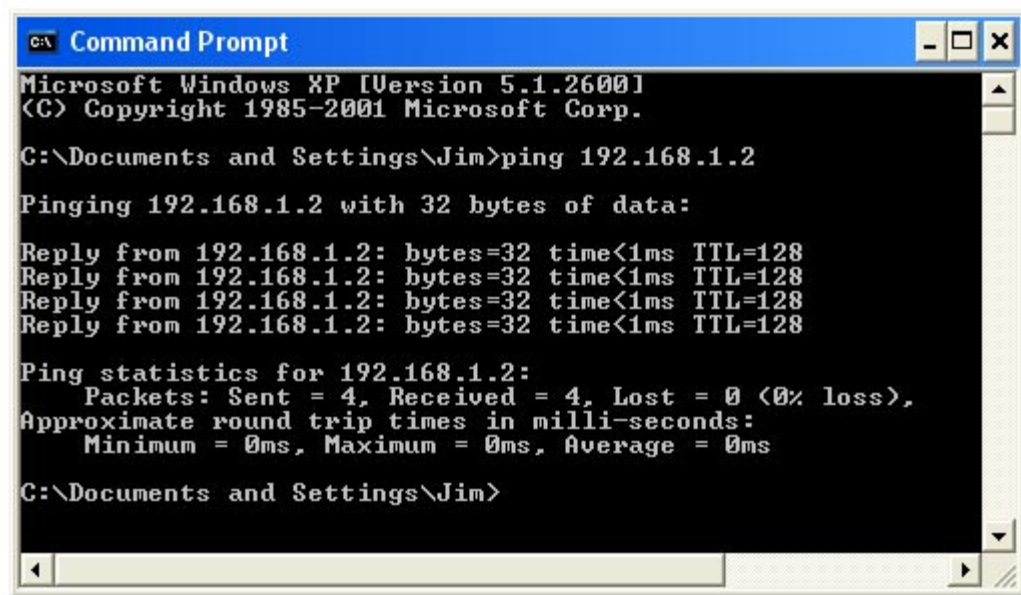
- b. Test connectivity

Ping the IP address of the computer on the other LAN. Enter the following command at the command prompt.

```
C:>ping 192.168.1.2
```

This will test IP connectivity from one workstation through its switch and router across the WAN link and through the other router and switch to the other PC.

- c. Look for results similar to those shown below. If not, check the PC connections and TCP/IP settings for both PCs. What was the ping result?



```
C:\ Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jim>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

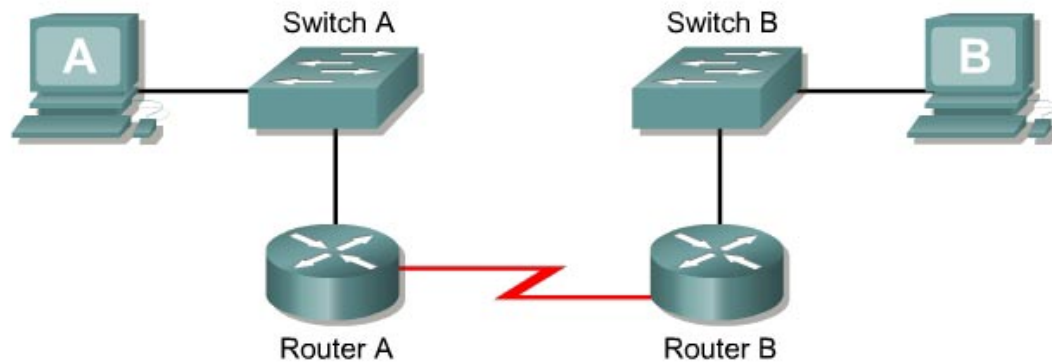
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128
Reply from 192.168.1.2: bytes=32 time<1ms TTL=128


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

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

Step 10 Restore the PCs to their original IP settings, disconnect the equipment, and store the cables

Lab 5.2.3c Troubleshooting Interconnected Devices



Straight-through cable	—————
Serial cable	———  ———
Rollover (console)
Crossover cable	- - - - -

Objective

- Create a simple routed wide-area network (WAN) with two PCs, two switches or hubs, and two routers
- Configure workstation IP address information
- Identify and correct networking problems related to cabling issues
- Identify and correct networking problems workstation IP addressing issues

Background / Preparation

This lab focuses on configuring a basic router-to-router WAN and then troubleshooting Layer 1 cabling problems and workstation Layer 3 IP addressing problems.

Note: The two routers need to be preconfigured by the instructor or lab assistant to have the correct IP addresses on their LAN and WAN interfaces. Router A will provide the clocking signal as DCE.

Use the prior lab “Basic Routed WAN” to set up this lab prior to starting the troubleshooting. As the configuration shown is being set up, problems with cabling and workstation IP addressing should be introduced into the setup of the network. By working in teams of two, one person can set up the

configuration and introduce some errors, and the other person can troubleshoot the setup to determine the problems.

The equipment needed in this lab is the following:

- Two Ethernet 10BASE-T or Fast Ethernet switches or two hubs
- Two routers with an RJ-45 Ethernet or Fast Ethernet interface (or an AUI interface) and at least one serial interface.
- 10BASE-T AUI transceiver (DB-15 to RJ-45) for a router with an AUI Ethernet interface, which is a 2500 Series
- Several straight-through, crossover, and improperly wired or bad cables for connecting the workstations and routers to the hub or switch
- One female (DCE) and one male (DTE) V.35 cable for interconnecting the routers

Step 1 Set up the lab configuration for Team member A by doing the following:

- Set up the lab according to prior lab “Building a Basic Routed WAN”.
- As the components are being connected, use a variety of Category 5 cables including at least one crossover cable and a cable that is improperly wired.
- When configuring the workstations, introduce at least one misconfiguration of IP address information per PC.
- Record the problems introduced in the table below. Space is provided for up to three cabling problems and three IP problems. If it is a cabling problem, indicate the location of the problem, such as PC-A to Switch-A. If it is an IP related problem, indicate which PC the problem is with. In the third column, describe the problem introduced, such as crossover cable used, wrong IP address or wrong default gateway.

Type of problem	Location of problem	Problem introduced
Cabling related		
Cabling related		
Cabling related		
IP related		
IP related		
IP related		

Step 2 Troubleshoot the lab configuration for Team member B

- Check workstation to workstation connectivity.
Ping from the command prompt on workstation A to the IP address of workstation B. If problems have been introduced, the ping attempt should fail.
- Check physical layer integrity.
Start with Layer 1 issues and check the cabling between the PCs and the switch. Check for the proper type of cable as well as good connections. Check the cabling between the routers and the switches for connections. Replace cables and insure good connections as necessary.
- Check network layer integrity.

Check for Layer 3 configuration problems with the workstations. Note that the router should be preconfigured and should not have the problems that are introduced. Use the command prompt and the command `winipcfg` (Windows 95/98/ME) or `ipconfig` (Windows NT/2000) to check the IP configuration of each workstation. Control panel network application may also be used to check IP settings. Verify the IP address subnet mask and default gateway for each workstation.

Step 3 Record problems found in the table below. This should be done by Team member B.





Type of problem	Location of problem	Corrective Action Taken
Cabling related		
Cabling related		
Cabling related		
IP related		
IP related		
IP related		

Step 4 Team members A and B switch roles and repeat the lab

Step 5 Restore the PCs to their original IP settings, disconnect the equipment, and store the cables

Lab 5.2.7 Establishing a Console Connection to a Router or Switch



Straight-through cable	
Serial cable	
Rollover (console)	
Crossover cable	

Objective

- Create a console connection from a PC to a router and switch using the proper cable
- Configure HyperTerminal on the PC
- Observe the router and switch user interface

Background / Preparation

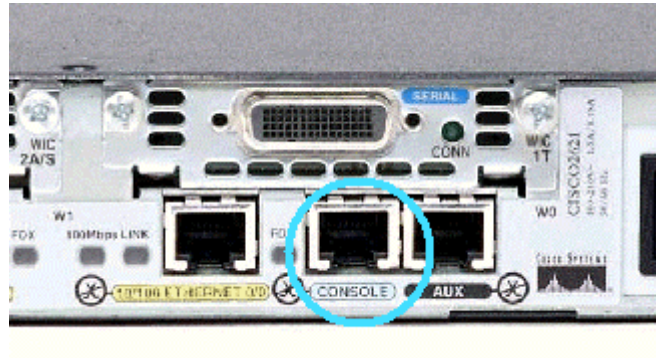
This lab will focus on the ability to connect a PC to a router or a switch in order to establish a console session and observe the user interface. A console session allows the user to check or change the configuration of the switch or router and is the simplest method of connecting to one of these devices.

This lab should be performed twice, once with a router and once with a switch to see the differences between the user interfaces. Start this lab with the equipment turned off and with cabling disconnected. Work in teams of two with one for the router and one for the switch. The following resources will be required:

- Workstation with a serial interface and HyperTerminal installed
- Ethernet 10BASE-T or Fast Ethernet switch
- Cisco Router
- Rollover or console cable for connecting the workstation to the router or switch

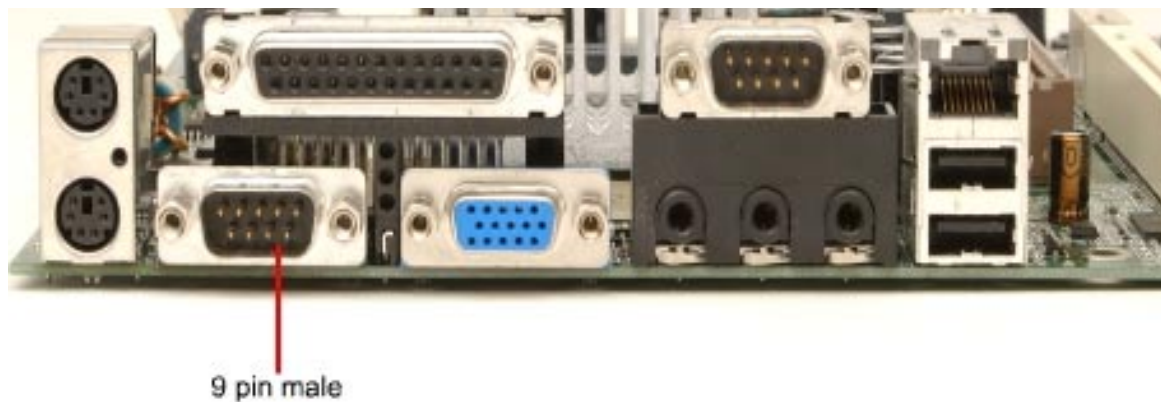
Step 1 Identify the Router/Switch console connectors

- a. Examine the router or switch and locate the RJ-45 connector labeled "Console".



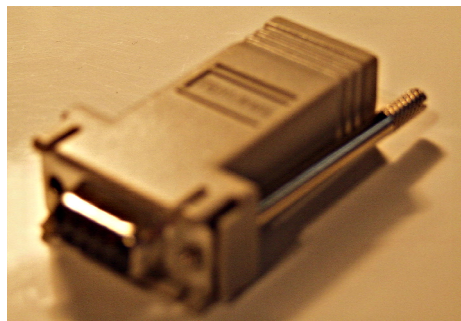
Step 2 Identify the computer serial interface, which is COM 1 or 2

- a. It should be a 9 or 25-pin male connector labeled serial or COM1. It may or may not be identified.



Step 3 Locate the RJ-45 to DB-9 adapter

One side of the adapter connects to the PC's serial interface and the other to the RJ-45 rollover cable connector. If the serial interface on the PC or dumb terminal is a DB-25, an RJ-45 to DB-25 adapter will be needed. Both of these adapters typically come with a Cisco router or switch.

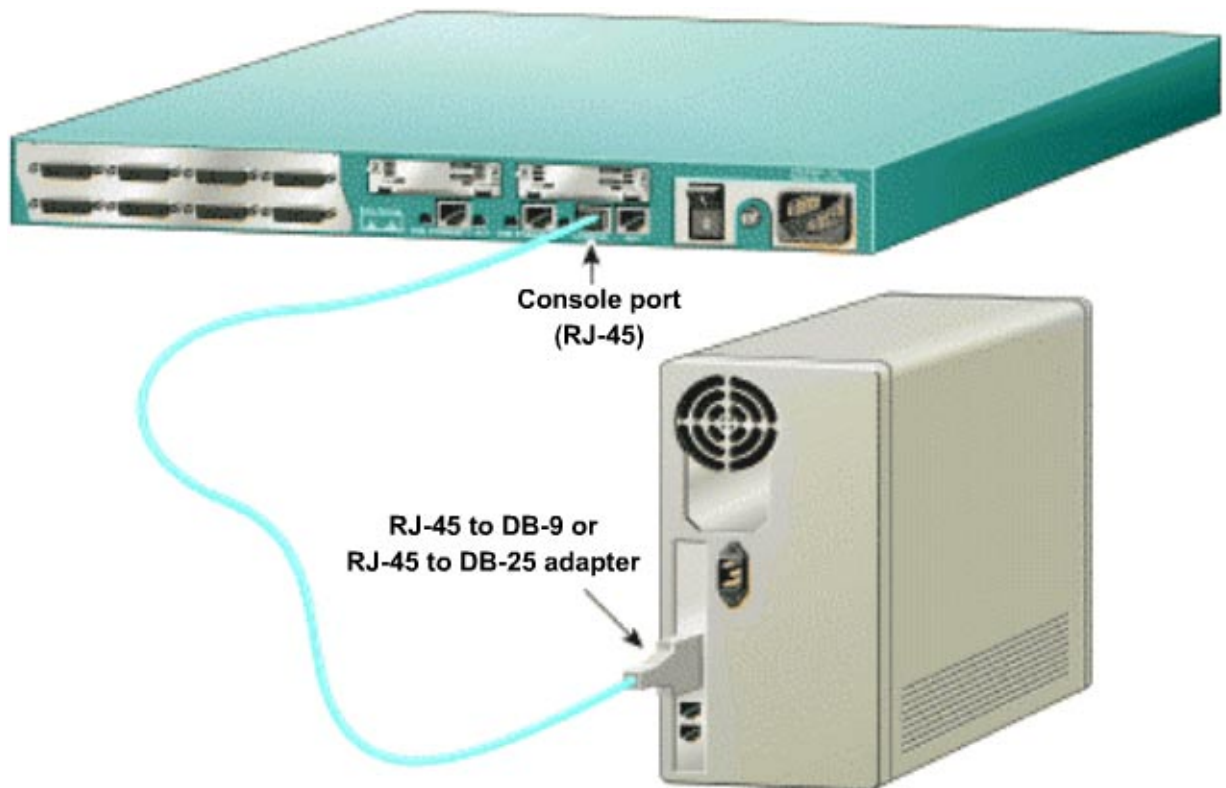


Step 4 Locate or build a rollover cable

Use a rollover cable. If necessary, make one of adequate length to connect the router or switch to a workstation.

Step 5 Connect the cabling components

Connect the rollover cable to the router or switch console port RJ-45 connector. Next, connect the other end of the rollover cable to the RJ-45 to DB-9 or DB-25 adapter. Finally, attach the adapter to a PC serial port, either DB-9 or DB-25, depending on the computer.



Step 6 Start the PC HyperTerminal program

- a. Turn on the computer
- b. From the Windows taskbar, locate the **HyperTerminal** program:
Start > Programs > Accessories > Communications > Hyper Terminal

Step 7 Name the HyperTerminal Session

At the "Connection Description" popup enter a name in the connection Name field and select **OK**.



Step 8 Specify the computer connecting interface

At the “Connect To” popup, use the drop down arrow in the Connect using: field to select **COM1** and select **OK**.

Note: Depending on which serial port was used on the PC, it may be necessary to set this to **COM2**.



Step 9 Specify the interface connection properties

- a. At the “COM1 Properties” popup use the drop down arrows to select the following:

Bits per second = **9600**

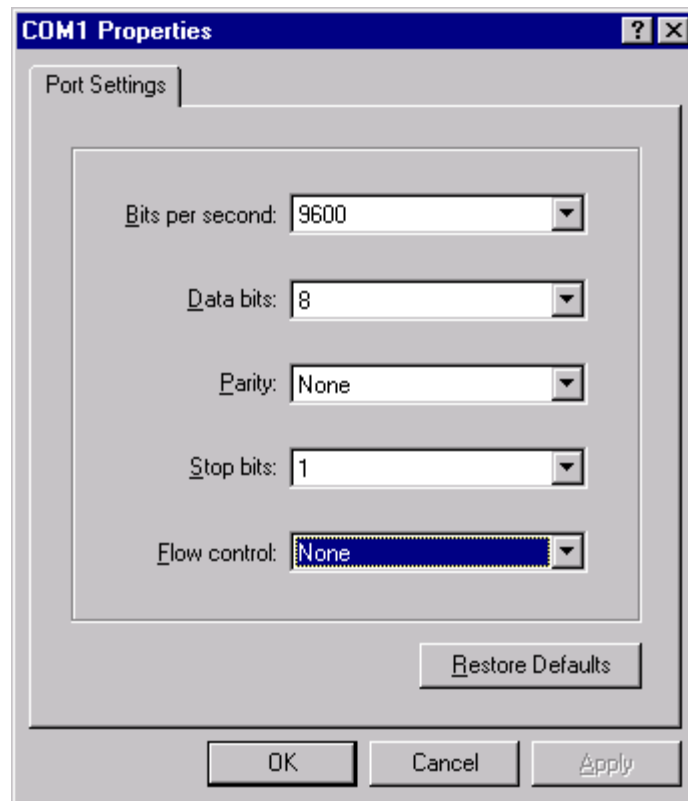
Data bits = **8**

Parity = **None**

Stop bits = **1**

Flow control = **None**

- b. Then select **OK**.



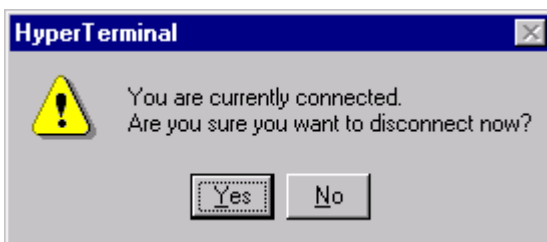
- c. When the HyperTerminal session window comes up, turn on the router or switch. If the router or switch is already on, press the **Enter** key. There should be a response from the router or switch. If there is, then the connection has been successfully completed.

Step 10 Observe the router or switch user interface

- Observe the user interface.
- If this is a router, what is the prompt? _____
- If this is a switch, what is the prompt? _____

Step 11 Close the Session

- To end the console session from a HyperTerminal session, select the following:
File > Exit
- When the HyperTerminal disconnect warning popup appears, select **Yes**.



- c. The computer will then ask if the session is to be saved. Select **No**.

Step 12 Shut down the router or switch and store the cables



Lab 7.1.2 Waveform Decoding

Objective

The purpose of this lab is to integrate knowledge of networking media, OSI Layers 1, 2, and 3, and Ethernet, by taking a digital waveform of an Ethernet frame and decoding it. Specifically, students will do the following:

- Review numbering systems, OSI concepts, and encoding methods as background from Module 1.
- Learn to decode the waveform back into binary, reorder the binary, and identify Ethernet field boundaries from Module 2.
- Decode the Ethernet Length/Type field, locate and read RFCs, and decode Layer 3 of the waveform from Module 3.
- Use a Protocol Analyzer from Module 4.

Background / Preparation

As a student of networking, there are many new concepts to learn:

- The OSI model
- Networking media and signals
- Ethernet
- The TCP/IP protocols

Network administrators, technicians, and engineers study and troubleshoot a network using Protocol Analysis software. Protocol Analysis software allows the capture and interpretation of frame-level data, which is crucial for understanding what is happening on a live and perhaps troublesome network. Hand-decoding the signal gives more insight into what the software is doing automatically. Therefore, this lab provides an important foundation for future learning of network troubleshooting.

A Digital Oscilloscope was attached to an Ethernet 10BASE2 coaxial cable to capture actual Ethernet waveforms. Although it is possible to capture waveforms on 10BASE-T and 100BASE-TX twisted pair media, the coaxial cable gives the cleanest and most readable waveform data. This data is available from the instructor. Decoding the waveform is a crucial step in understanding how networks operate.

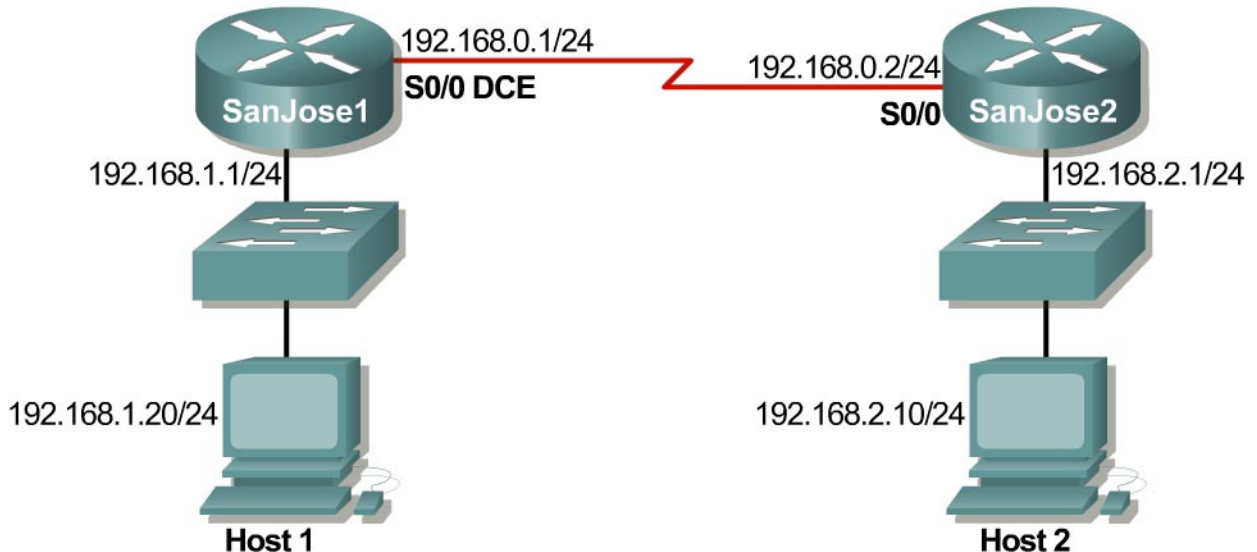
For the first part of the lab, all that is needed is this lab printout and the printout of the waveform for students to write on as they decode. The last task of the lab involves the use of a Protocol Analyzer, which is Fluke Protocol Inspector or the equivalent.

Note: This lab is over 20 pages long and includes excellent supplemental sections on the following:

- Numbering systems, which include binary, decimal, and hex
- The OSI 7-Layer model with real-world examples
- Signaling and Encoding methods of Ethernet Waveform and Manchester

The lab can be downloaded from the local Academy server at the institution with Version 3.0 of the curriculum or from the Cisco Academy Connection website. The Ethernet waveform for decoding will also need to be downloaded. Check with the instructor for help in obtaining the lab and waveform.

Lab 7.1.9a Introduction to Fluke Network Inspector



Objective

This lab is a tutorial demonstrating how to use the Fluke Networks Network Inspector (NI) to discover and analyze network devices within a broadcast domain. This lab will demonstrate the key features of the tool that can be incorporated into various troubleshooting efforts in the remaining labs.

Background / Preparation

The Network Inspector software can distinguish workstations, servers, network printers, switches, and managed hubs, if they have been assigned a network address.

Options for conducting this lab.

- 1) Use Network Inspector in a small controlled LAN that is configured by the instructor in a closed lab environment as shown above. The minimum equipment should include a workstation, a switch, and a router.
- 2) Perform the steps in a larger environment such as the classroom or the school network to see more variety. Before attempting to run NI on the school LAN, check with the instructor and the network administrator.

The following is a list of points to consider:

1. Network Inspector detects the devices within a network subnet or VLAN. It does not search beyond a router. It will not inventory the entire network of the school unless it is all on one subnet.
2. Network Inspector is not a Cisco product nor is it limited to detecting just Cisco devices.

3. Network Inspector is a detection tool, but it is not a configuration tool. It cannot be used to reconfigure any devices.

The output in this lab is representative only, and output will vary depending on the number of devices, device MAC addresses, device hostnames, and which LAN is joined.

This lab introduces the Fluke Networks Network Inspector software, which may be useful in later troubleshooting labs and in the field. While the Network Inspector software is a valuable part of the Academy program, it is also representative of features available on other products in the market.

At least one host must have the Network Inspector software installed. If the lab is done in pairs, having the software installed on both machines means that each person can run the lab steps. Be sure to select both the Network Inspector and the Network Inspector Agent during installation.

The Console can be anywhere that has a valid IP path and security to allow the connection to an Agent. In fact, it might be an interesting exercise to have the Console reach across the serial link to load the database from the other Agent. The student can have the Console reading from a different database than the one that is currently in use by the Agent on the same PC.

Step 1 Configure the lab or attach the workstation to the school LAN

Option 1. If the closed lab environment is selected, cable the equipment as shown above and load the configuration files into the appropriate routers. These files might already be preloaded. If not, obtain them from the instructor. These files should support the IP addressing scheme as shown in the figure above and the table below.

Configure the workstation according to the specifications in the table below.

Host #1	Host #2
IP Address: 192.168.1.20	IP Address: 192.168.2.10
Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

Since the software discovers devices on the network, the more devices the better the demonstration. If available, add additional hosts to both LANs.

Option 2. If option 2, connect to school LAN, is selected, simply connect the workstation, with Network Inspector or Protocol Expert installed, directly to a classroom switch or to a data jack connected to the school LAN.

Step 2 Start Network Inspector and the Agent

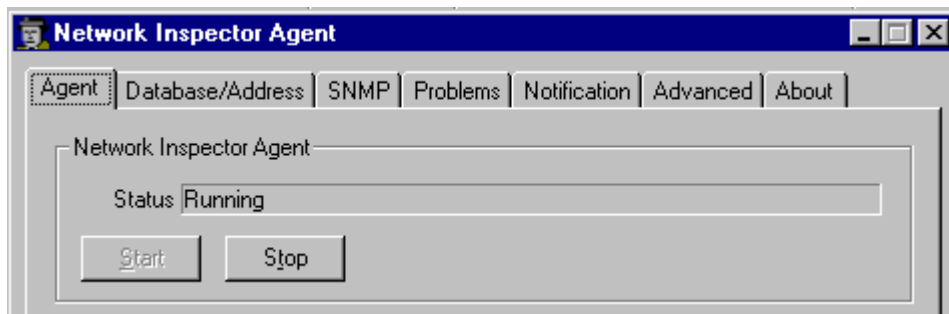
From the Start menu, launch the Network Inspector Console.

Click on the **Agent** button at the left end of the toolbar so that the Agent can be started.



If necessary, select the **Agent** tab in the window, then click on the **Start** button and watch the **Status** box until it shows that the Agent is running as in the figure below. This process may take several minutes to start.

Notice the Agent status on the bottom of the Console window. Look closely and notice that the Agent has been running since 9:57 PM in the second graphic captured below that is in Step 3.

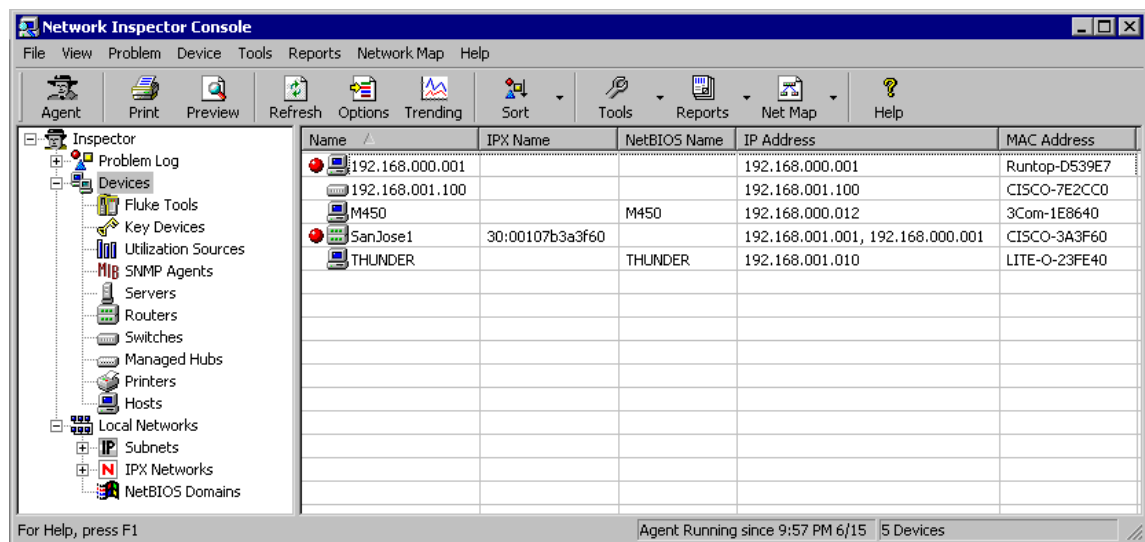


Use the **Close** button in the lower-right corner of the Agent window to send the Agent away. In some versions, this may be a **Hide** button. Do not use the **Stop** button or the discovery process will cease.

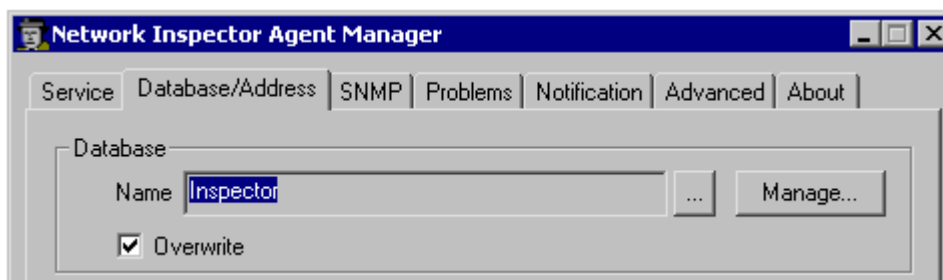
Step 3 Allow network discovery to occur

The Network Inspector software is designed to quietly, both passively and actively, collect network data. As such it takes time for devices to appear. This small network should be discovered in a minute or two. Active collection of statistical data is delayed for the first 10 minutes. An actual production network might take 30 minutes or more before most data is discovered.

After a few minutes, the Console window should start showing information about the network. In the following example, two additional workstations were added.



Note: Entries from previous sessions may be seen. It will take a few minutes for the entries to match the network. In the Agent window, under the **Database/Address** tab, there is a checkbox for **Overwrite**. If that box is checked, the current database content is discarded and a fresh data set is loaded as it is discovered when the Agent starts. Otherwise, any new data is integrated with the existing database as it is discovered.

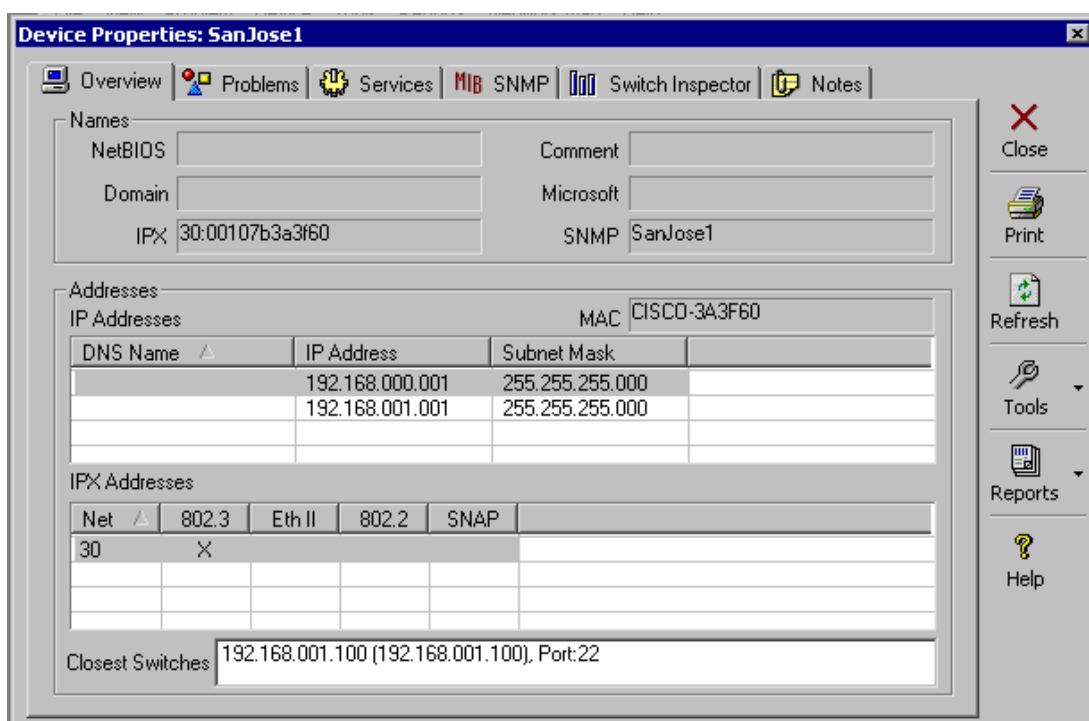


Notice the hostnames, which are M450, SanJose1 and Thunder, in the example above. PC hostnames will be different in student output. Also notice the IP addresses and MAC addresses for each discovered device. It should be obvious that both SanJose1 and SanJose2 have two IP addresses assigned to the LAN interface.

Notice that NI does not investigate beyond the router interface. It collects information only on the devices that share the same broadcast domain as the computer NIC.

Step 4 Investigate device properties

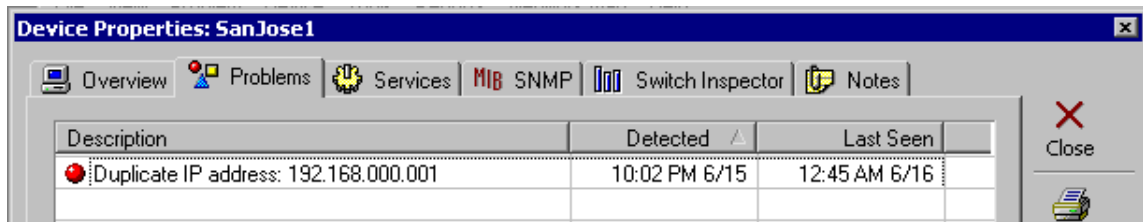
Double click on the router device name and look over the available Device Properties. Remember that results will depend on the devices included in the LANs subnet.



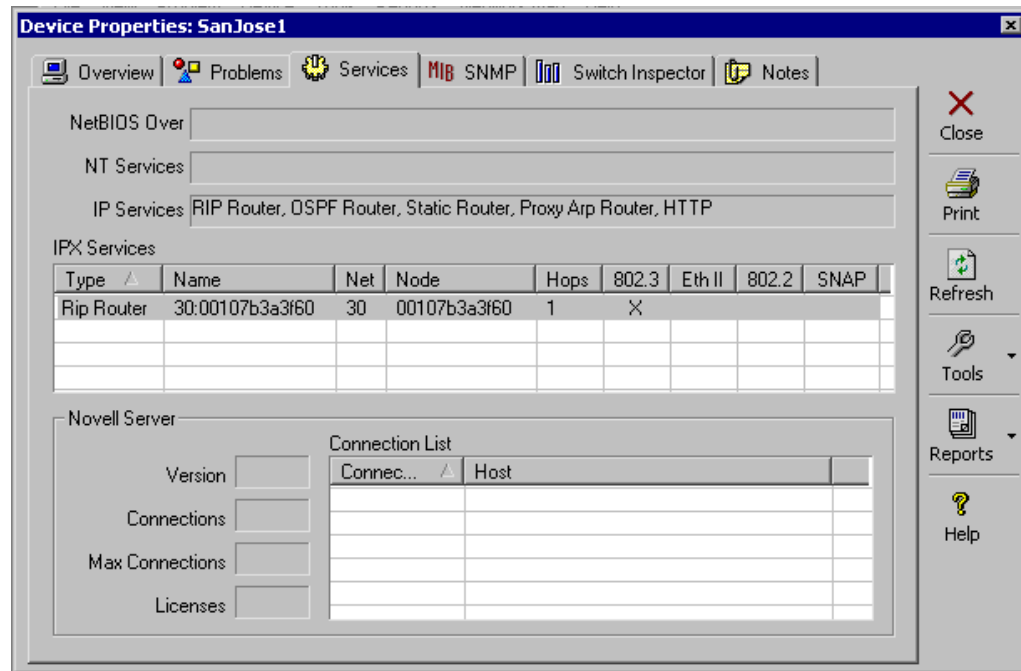
The **Overview** tab in the above graphic shows IP addresses, the IPX address, the IPX networks attached, the IPX data frame used (802.3 above), and the MAC address. Notice that the OUI has been converted to identify the manufacturer in the above example.

The closest switches will only appear if Network Inspector has been provided with a valid SNMP Community String for them.

The **Problems** tab reveals one of the IP addresses is duplicated within the network. This occurs if the student configured an optional host as defined in Step 1. The red ball to the left of the Description indicates a problem.



The **Services** tab reveals the IP and IPX Services running on the routers.

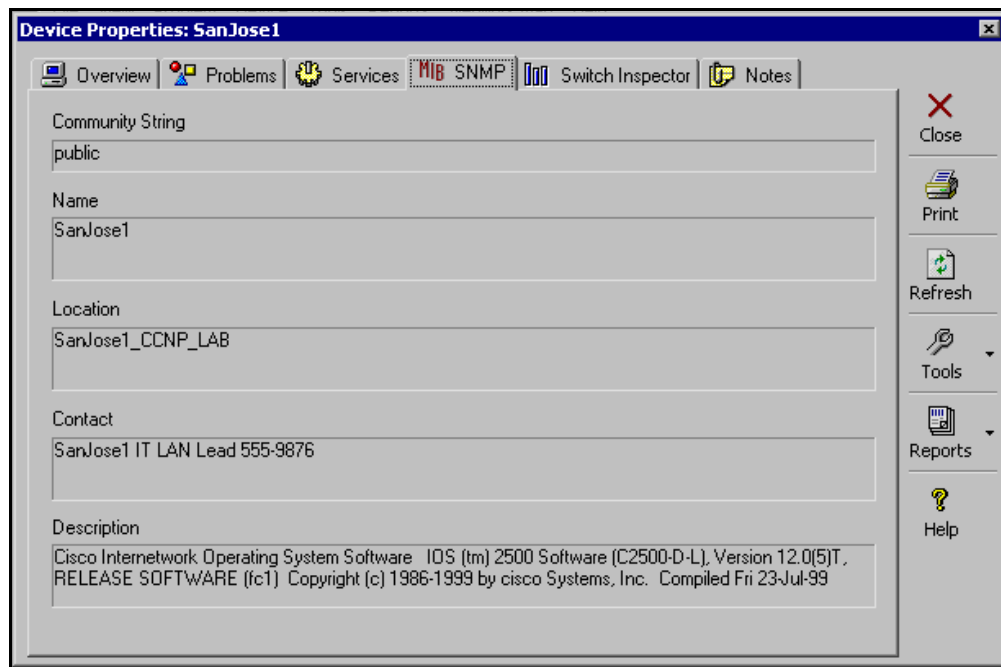


The IP Services example in the graphic above reveals that the **IP HTTP Server** service has been turned on. This means the router can be accessed via a Web browser.

The IPX Services shows the IPX Network ID (30), the Node address (MAC), the frame type, and the fact that IPX RIP is running.

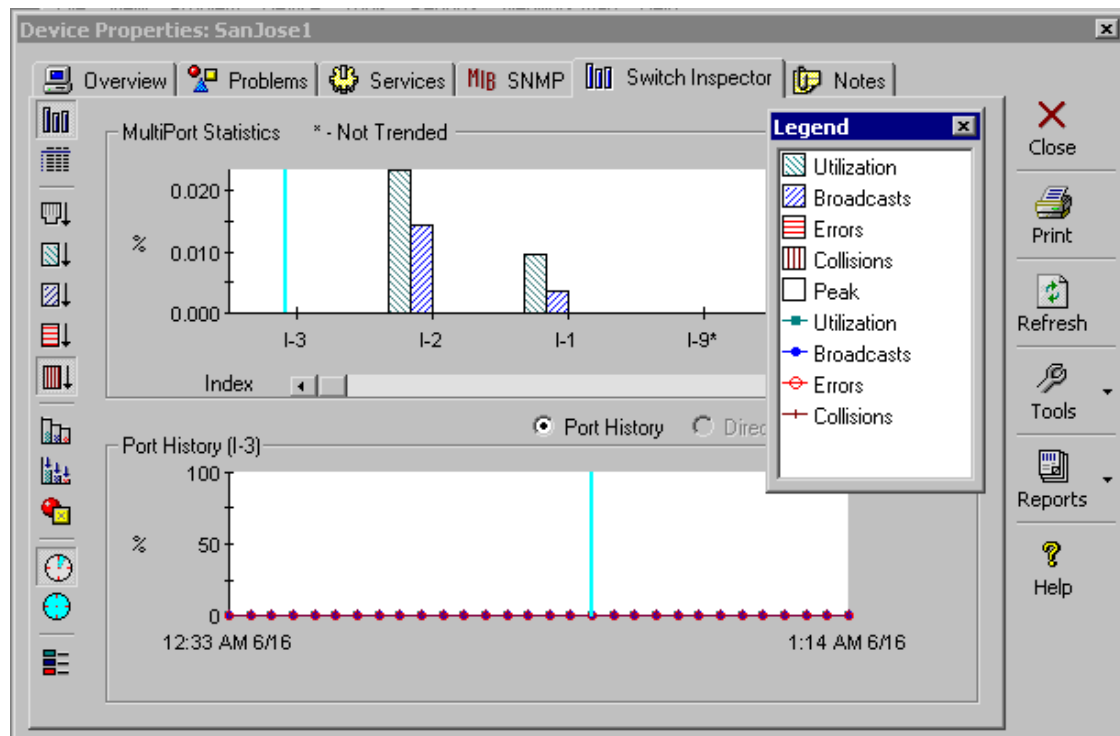
The bottom third of the window shows the information that would have been revealed if the device had been a Novell Server. A multi-homed server, which is one with more than one NIC (connection) in separate networks, is working as a router or bridge.


The **MIB SNMP** tab reveals SNMP information as well as the router IOS information.

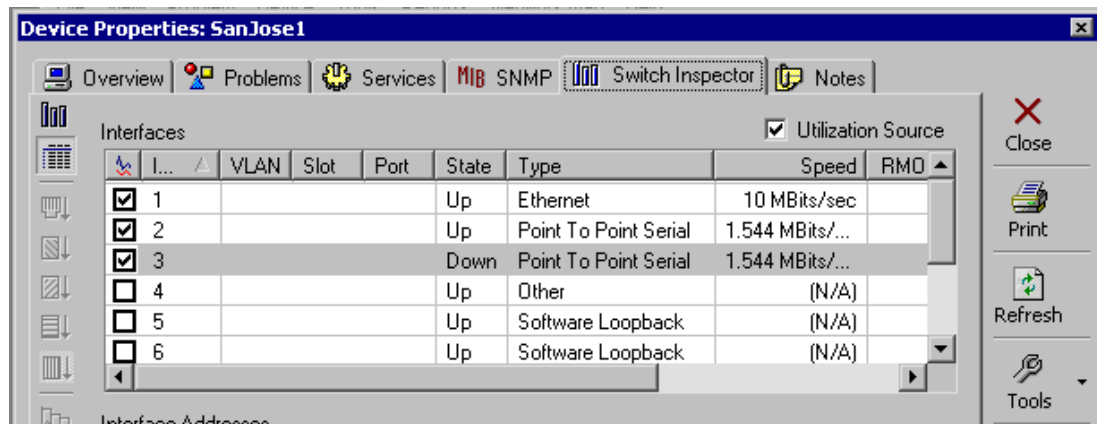


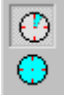
The **Switch Inspector** tab creates a variety of charts of the switch interface data for the selected device. This data is not collected during the initial 10-minute period. The Switch Inspector test provides basic utilization graphs for any SNMP enabled device. The level of information offered by this test depends on which MIBs are supported by the selected device. For example, since SanJose1 is a router, the student cannot display the address of any directly connected devices for a highlighted port. The buttons on the left side of the window change the chart format. The **Graph**

Legend  button at the bottom-left corner displays the floating legend seen below.



The second button is the **TabularView** , and selecting it details each interface on the selected device including whether the interface is up or down. The check box at the left of each line determines whether statistics are gathered for trending on that interface. Scrolling to the right reveals MTU and Description (FastEthernet0/0 or Token-Ring 0/1) details.

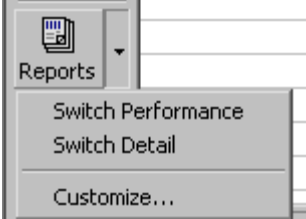




The two clock-like buttons switch between a one-hour or 24-hour history, which can create an interesting comparison if the NI has been running for an extended time. The results will be the same in this short exercise.

While in the Switch Inspector, the **Reports** button on the right side of the screen will expand to show two options. Select the **Switch Performance** choice and a multi-page report with various charts will appear on the screen. Look over the results.

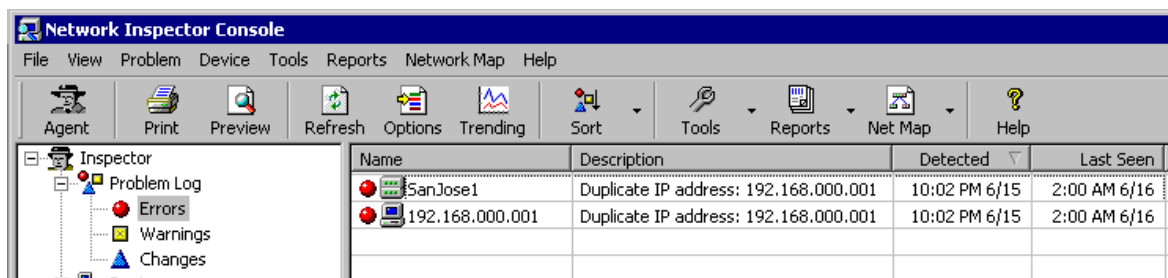
The **Switch Detail** option only works with a switch.



After looking over the Device Properties window, click on the **Close** button in the upper right corner to return to the Network Inspector Console.

Step 5 Explore the left panel options

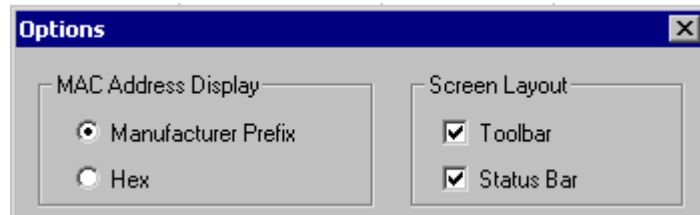
At the Network Inspector Console, experiment with expanding and contracting the choices in the left-side pane. As with the Explorer, if an item on the left side is selected, the right side will show the details. In the following example, expanding the Problems Log and selecting **Errors** shows the devices on the right side with errors. This makes it easy to spot the duplicate IP address device.



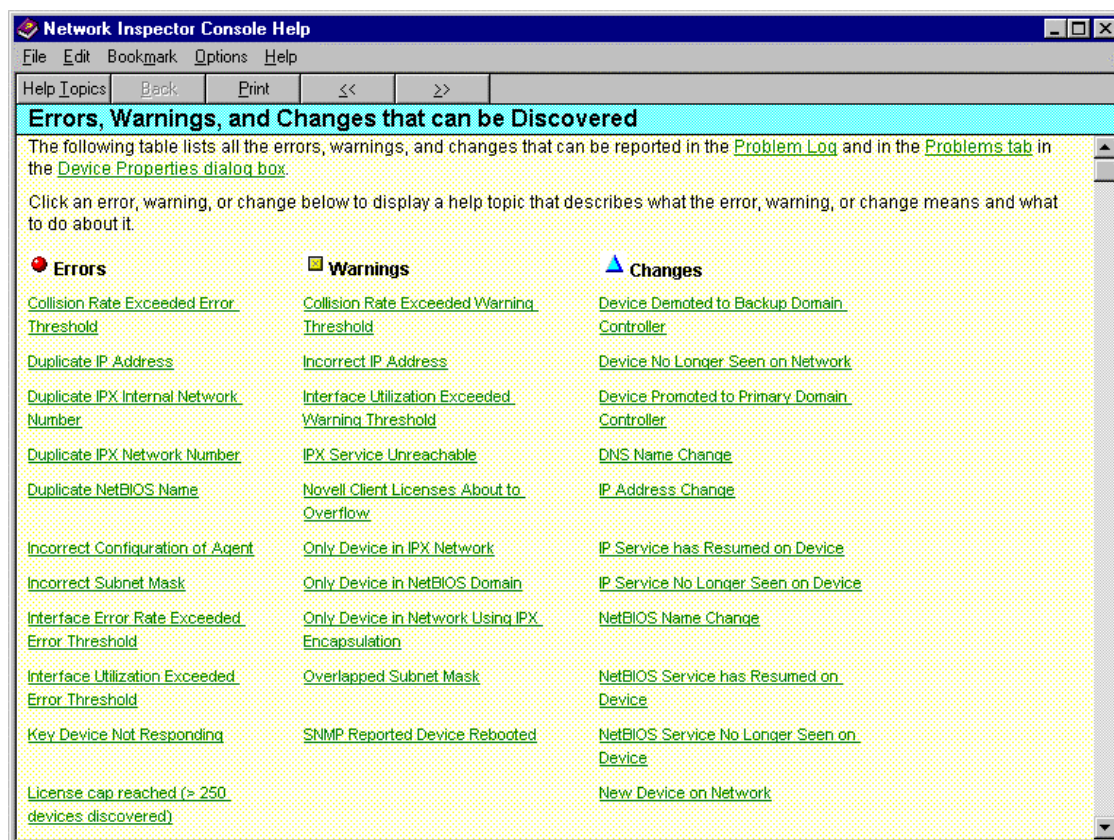
Try different options on the left pane and note the result in the right pane. Due to the limited number of devices, some will be empty. Try it later with a larger sample.

In the left pane, select **Devices** to show all devices in the right pane. Note the format of the MAC address.

Click on the **Options** button in the toolbar (or View > Options) and note that the student can choose between **Manufacturer Prefix** and **Hex**. Select the one that is not chosen, look over the other options, and then click on OK. Note the result.



Getting Help. In the Console main screen, check that the **Problem Log** is selected, and that a device shown in the detail window has been highlighted. Press F1, which is the Help function key, to show a list of problems by category.



As an example, one of the problems created by the current Lab configuration in the above graphic is a duplicate IP address. To learn about duplicate IP addresses, what the symptoms are, and what can be done about them, select the hyperlink listing for **Duplicate IP Address** from the list. There is a wealth of information in the Help for this software.

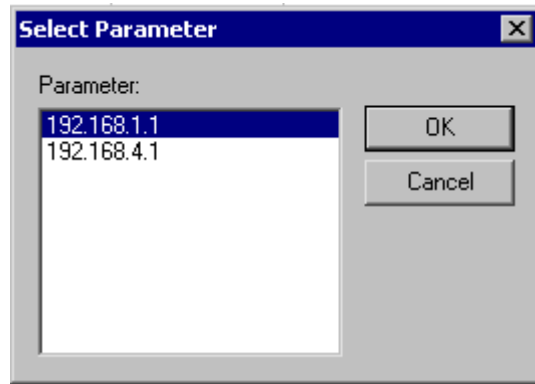
Take a minute and experiment with the **Preview**, **Sort**, and **Reports** buttons in the toolbar. The features should be obvious. Look particularly at the troubleshooting and documentation possibilities of the reports.

Select a host and then open the **Tools** button in the toolbar and pick **Ping**.

The Select Parameter box will include the LAN IP addresses that the student can ping. Select one and click on OK.

A command (MSDOS) window will appear to show the results.

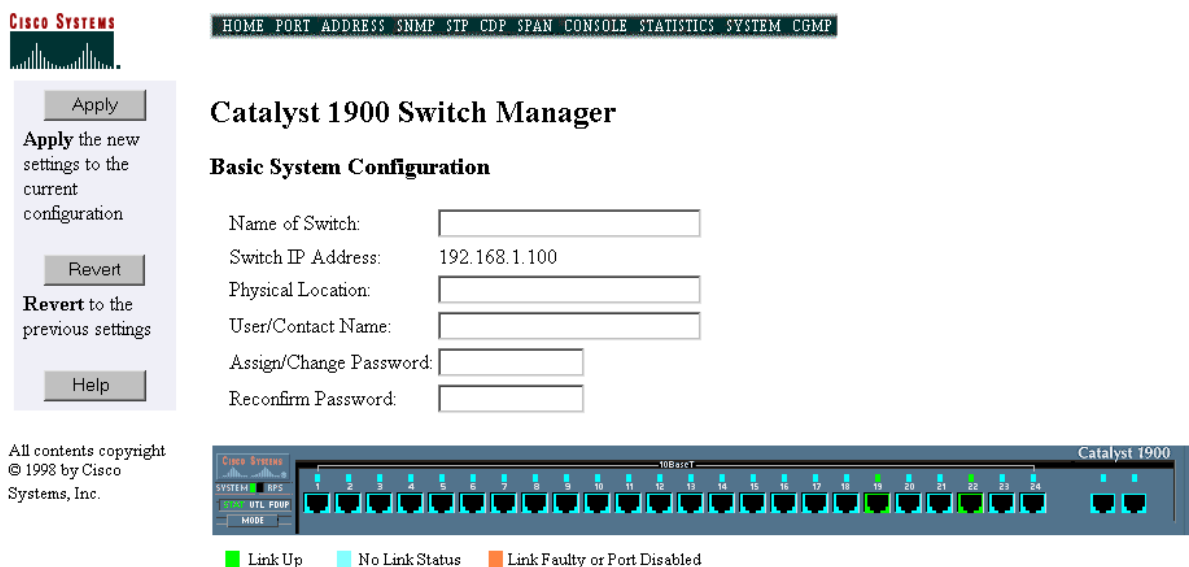
Type **exit** to close the new window when finished.



Try using the **Telnet** and **Traceroute** options. Select a router or switch in the Console display and then choose Tools | Telnet and a window with a Telnet session open will appear. Trace works the same way.

The **Web** option on the **Tools** button will open a Web session with a device if the IP HTTP Server feature is turned on. If trying this, the username is the hostname, which is SanJose1 or SanJose2, and the password is cisco.

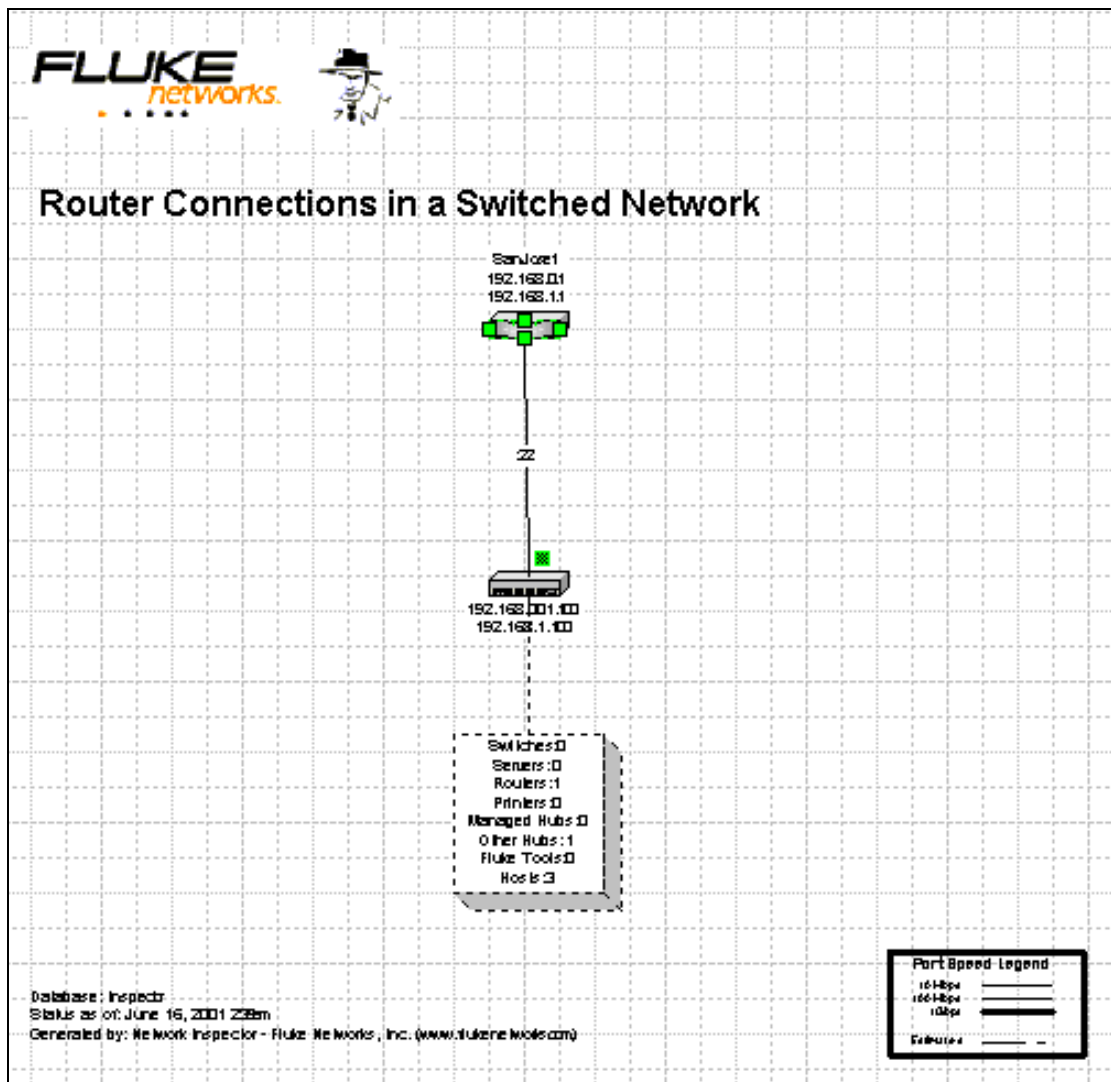
In the sample lab above, the switch is a Catalyst 1924 with an IP address assigned. Therefore, the following appears if the **Web** choice is selected while the switch is highlighted:



Experiment with the above toolbar options until comfortable with the features.

Step 6 Use Net Map and Visio to diagram the network

If Visio is installed on the workstation, the **Net Map** button on the toolbar will activate Visio and create a network map of the broadcast domain. The following example uses the “Router Connections in a Switched Network” on the Net Map button. It will draw the network whether or not a switch is included.



The Visio is fully integrated into NI. This means that double clicking one of the devices in the drawing will call up the Device Properties window that was used in Step 4.

Step 7 Document router information.

Using the skills covered earlier, select the router and document the following information where available:

- What is the name of the device? _____
- What IP services is the device running? _____
- What IPX services is the device running? _____
- What is the SNMP community string? _____
- What is the location? _____
- Who is the contact? _____
- Which interfaces are available? _____
- Which interfaces are up? _____

- i. List below any problem(s) that the software has discovered.

Step 8 Observe device discovery

If possible, connect the two switches with a crossover cable and watch the NI output as new devices are discovered. If a crossover cable is unavailable, remove one of the switches and plug the host(s) and router into the second switch. While this would not usually be done in a production environment, do it now just to see how NI responds.

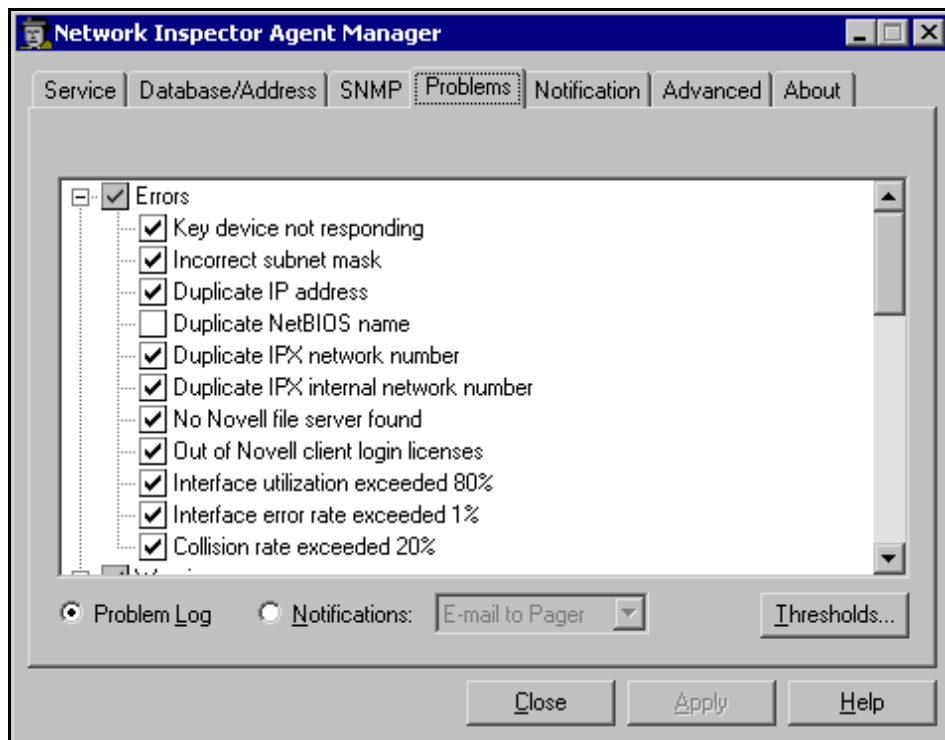
New devices should show up initially with blue triangles indicating they are newly discovered. Many should eventually get a yellow warning rectangle indicating a potential problem. Remember that this process could take 10 or more minutes.

Eventually, the other subnets and the second router should be seen.

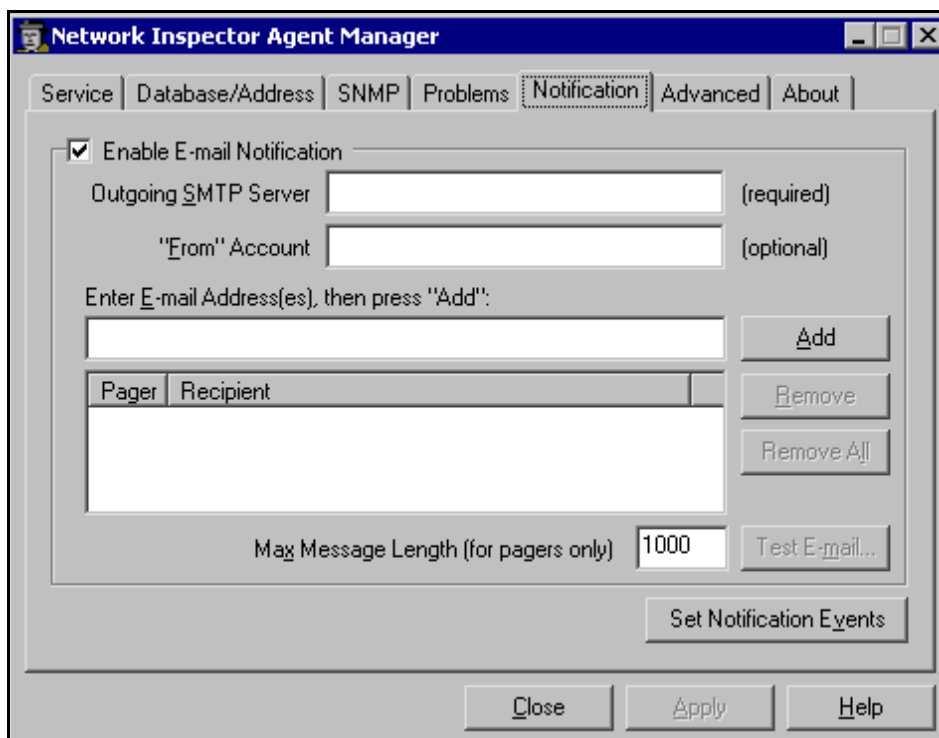
Step 9 Stop the capture and access the Problems and Notification tabs

Click on the **Agent** button in the toolbar. The Agent has been collecting data all this time. Click on the **Stop** button and then confirm intentions when prompted.

Look over the tabs to see the database options that can be set. Note the **Problems** tab and the choices for focusing the investigation.



On the **Notification**, notice that e-mail notifications can be sent out. To use this feature, the student would need the same information as that required to set up an Internet e-mail account or Outlook e-mail account.



If the student starts the Agent again, it may take a few minutes to detect any changes that occurred while the agent was off.

Step 10 Experiment with NI

Experiment with the NI tool by looking at the different devices.

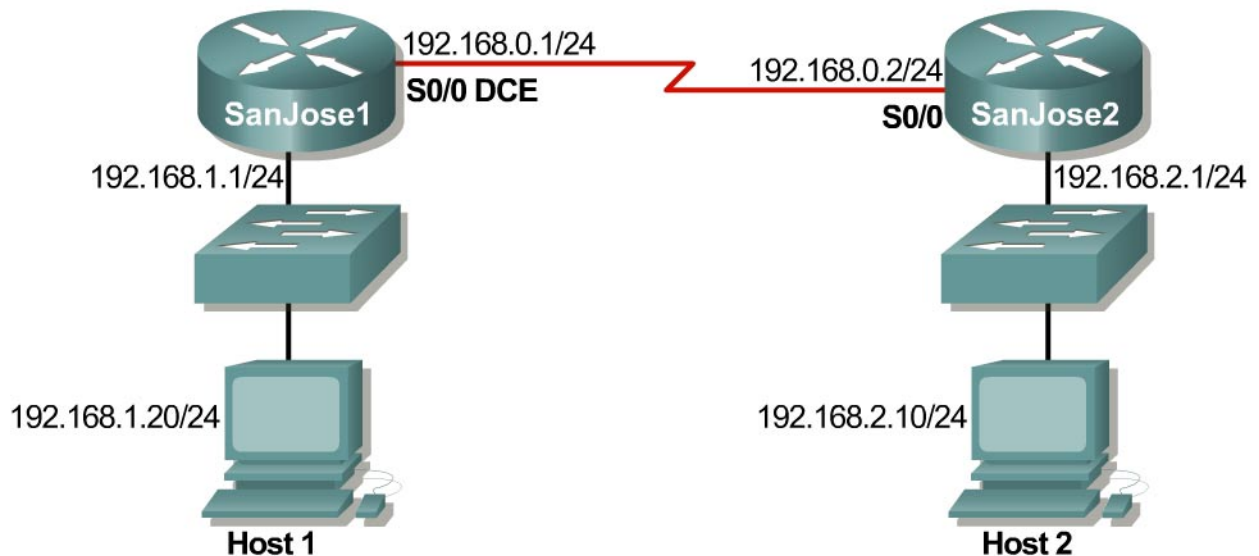
If NI is installed on the classroom computers, investigate the devices on that larger network.

Reflection

How might this information be used in troubleshooting?

What advantages over HyperTerminal might it have for troubleshooting documentation?

Lab 7.1.9b Introduction to Fluke Protocol Inspector



Objective

This lab is a tutorial demonstrating how to use the Fluke Networks Protocol Inspector to analyze network traffic and data frames. This lab will demonstrate key features of the tool that can be incorporated into various troubleshooting efforts in the remaining labs.

Background / Preparation

The output in this lab is representative only. Output will vary depending on the number of devices added, device MAC addresses, device hostnames, which LAN is joined, and so on.

This lab introducing Protocol Inspector will be useful in later troubleshooting labs as well as in the field. While the Protocol Inspector (PI) software is a valuable part of the Academy program, it is also representative of features available on other products in the market.

Options for conducting this lab.

- 1) Use Protocol Inspector or Protocol Expert in a small controlled LAN that is configured by the instructor in a closed lab environment as shown in the figure above. The minimum equipment should include a workstation, a switch, and a router.
- 2) Perform the steps in a larger environment such as the classroom or the school network to see more variety. Before attempting to run PI or PE on the school LAN, check with the instructor and the network administrator.

At least one of the hosts must have the Protocol Inspector software installed. If the lab is done in pairs, having the software installed on both machines means that each person can run the lab steps. However, each host may display slightly different results.

Step 1 Configure the lab or attach a workstation to the school LAN

Option 1. If the closed lab environment is selected, cable the equipment as shown above and load the configuration files into the appropriate routers. These files might be preloaded. If not, obtain them from the instructor. These files should support the IP addressing scheme as shown in the figure above and the table below.

Configure the workstations according to the specifications as in the figure shown above and table below.

Host #1	Host #2
IP Address: 192.168.1.20	IP Address: 192.168.2.10
Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0
Default Gateway: 192.168.1.1	Default Gateway: 192.168.2.1

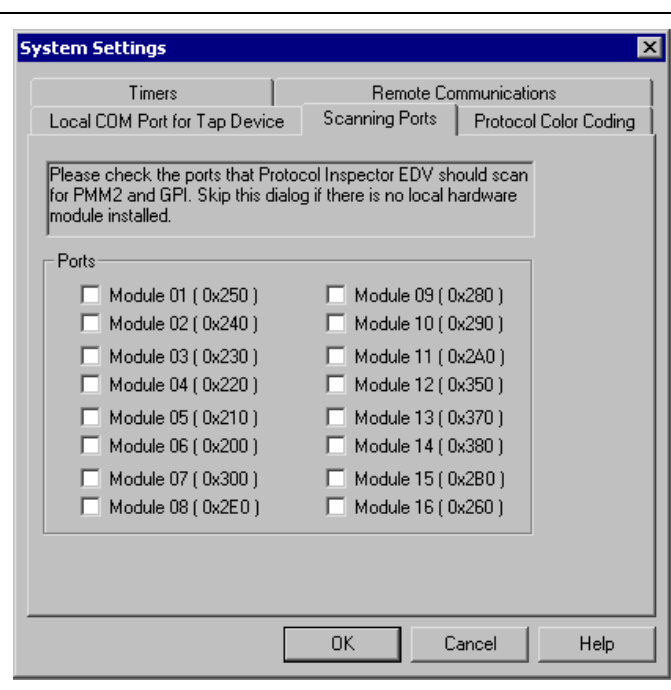
Option 2. If option 2, connect to school LAN, is selected, simply connect the workstation, with PI or PE installed, directly to a classroom switch or to a data jack connected to the school LAN.

Step 2 Start Protocol Inspector EDV program

From the Start menu, launch the Fluke Protocol Inspector EDV program.

Note: The first time the program is run, a message will appear that asks, “Do you have any Fluke analyzer cards or Fluke taps in your local system?”

If using the educational version, click on **No**. If answering yes or if the following screen appears, just click on **OK** without selecting any ports.



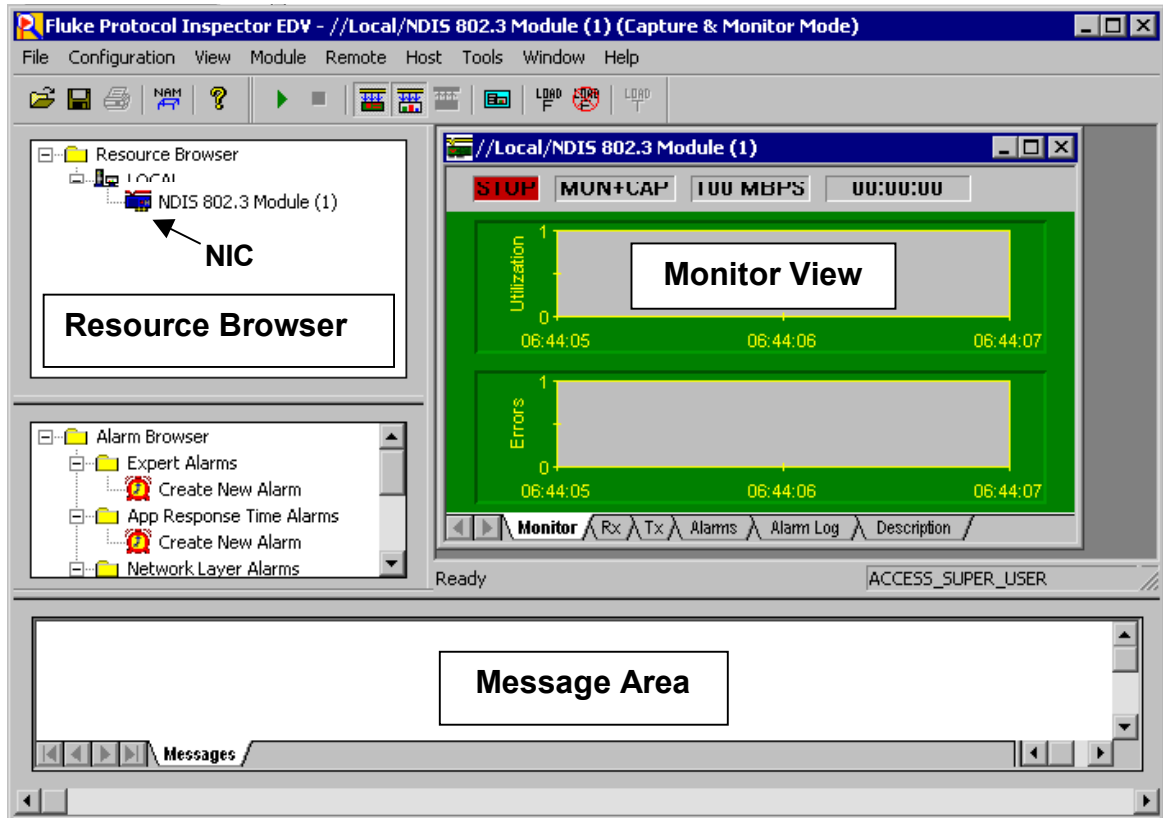
There are four main Protocol Inspector views, which include the following:

- Summary View
- Detail View
- Capture View of Capture Buffers
- Capture View of Capture Files


The program opens in the **Summary View**. This view shows several windows used by the tool. The **Resource Browser** window in the upper left corner shows the only monitoring device that is

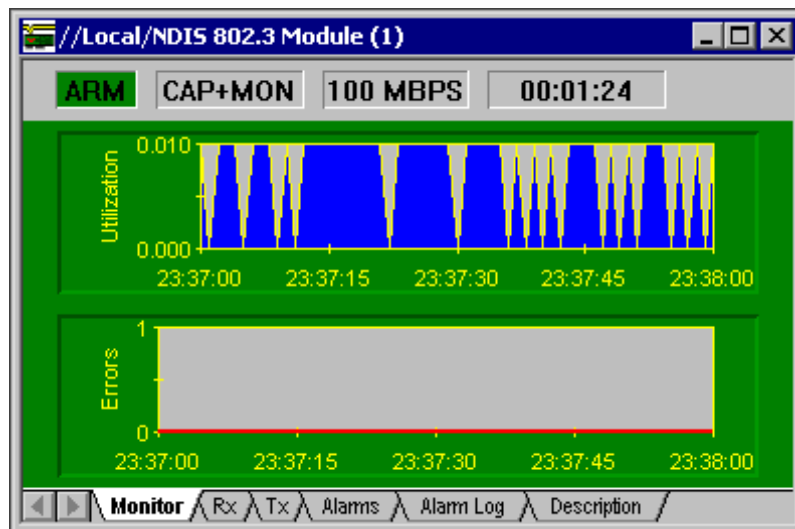
available, which is the NDIS 802.3 Module (NIC) of the host. If there were Protocol Media Monitors, they would be displayed with the associated host devices. The **Alarm Browser** on the left side and **Message Area** at the bottom will be covered later.

The **Monitor View**, which is in the main window on the upper right, monitors one resource per window in a variety of viewing options. The example below and probably the startup screen show no information in the Monitor View window. The **Stop** in the upper-left corner of the Monitor View window confirms that no monitoring is occurring.



Step 3 Start the Monitor / Capture process

To start the monitoring/capturing process, use the Start  button or Module | Start from the menu system. The Utilization chart should start showing activity like the graphic below:



The word **Arm** should appear where **Stop** had been before. If opening the **Module** menu, notice that **Stop** is now an option while **Start** is muted. Do not stop the process yet. Restart it again if it is stopped.

The tabs at the bottom of the window show the resulting data in a variety of forms. Click on each and note the result. **Transmit (Tx)**, **Alarms**, and **Alarm Log** will be blank. The following is the **Received (Rx)** frames, which indicates that **Broadcast** and **Multicast** frames are being received, but they may not show any **Unicasts**.

The screenshot shows the same window as before, but with the "Rx" tab selected. The "ARM" button is still highlighted. The timer now shows "00:08:27". The main area displays a table with two sections: "MAC Counters" and "Errors".

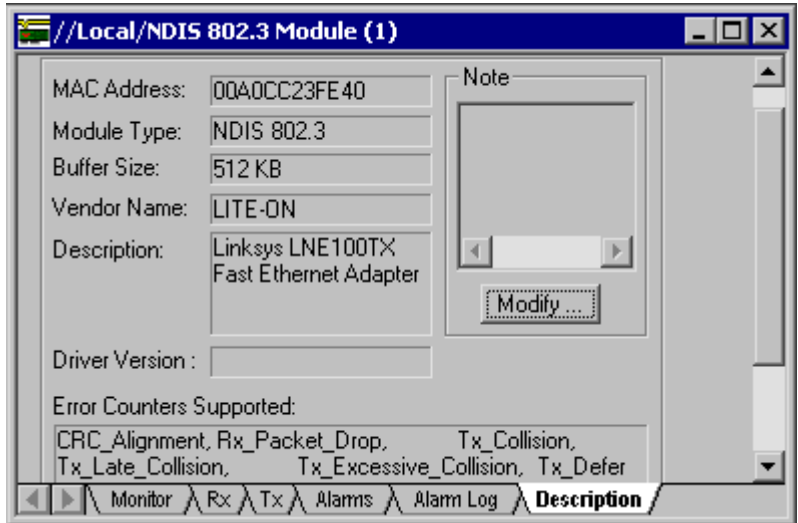
MAC Counters	Value	Errors	Value
Frames Captured	463	CRC Alignment	0
Frames Received	463	Undersize	N/A
Broadcast	100	Oversize	N/A
Multicast	363	Fragments	N/A
Unicast	0	Jabbers	N/A
Frames/Second	2	Collision Indication	N/A
Bytes Received	31,400	Packet Dropped	0
Utilization	0	Errors	0

At the bottom, the tabs are "Monitor", "Rx" (selected), "Tx", "Alarms", "Alarm Log", and "Description".


Using the console connection to the router, ping the monitoring host (192.168.1.10 or 192.168.2.10), and notice that **Unicast** frames appear. Unfortunately, the errors shown in the third column will not appear in the lab exercise unless a traffic generator like the Fluke Networks OptiView product has been added.

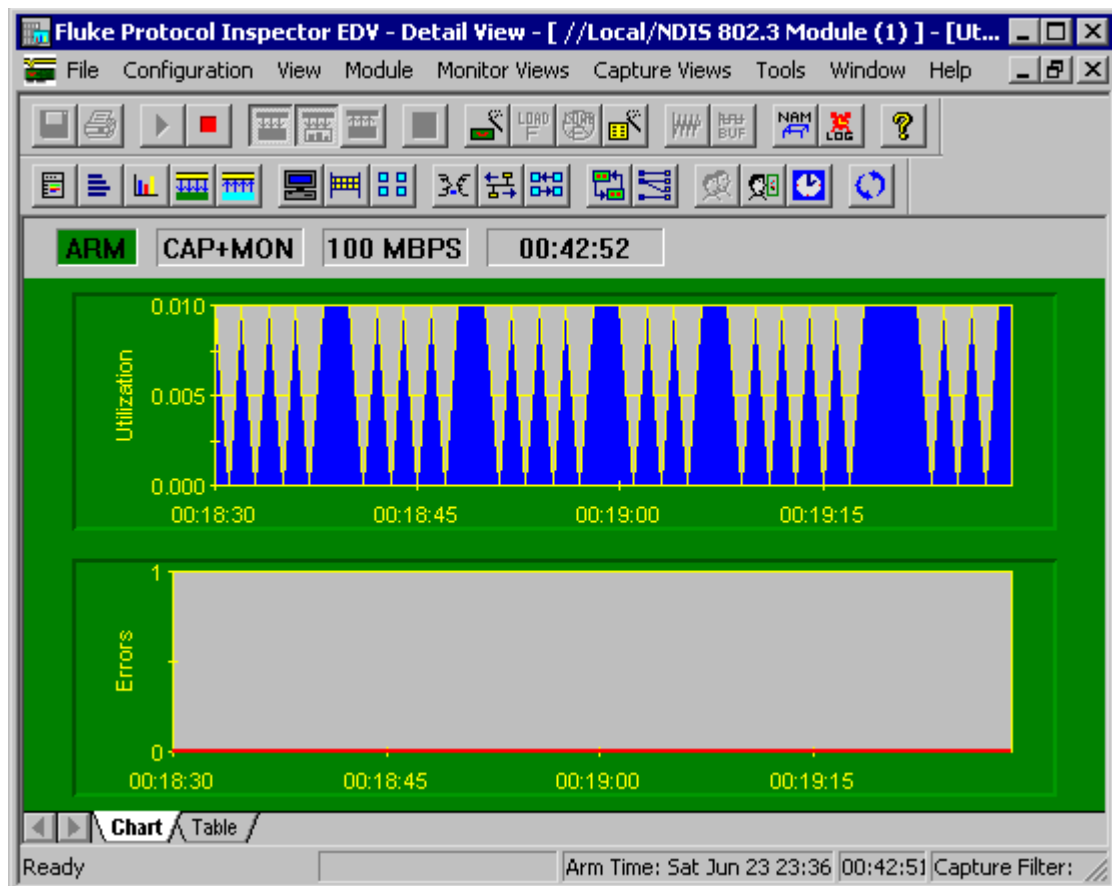
The **Description** tab reveals the MAC address, manufacturer, and model of the NIC. It also shows which Error Counters are on.

Take a few minutes to become familiar with the tabs and the scroll features of the window.



Step 4 View Details

To go to the **Detail View** window click on the **Detail View**  button in the toolbar or double click anywhere on the Monitor View chart. This will open a second window that should look something like the following, after maximizing the **Utilization / Errors Strip Chart (RX)** window.





Note: If necessary, activate all toolbars on the View menu.

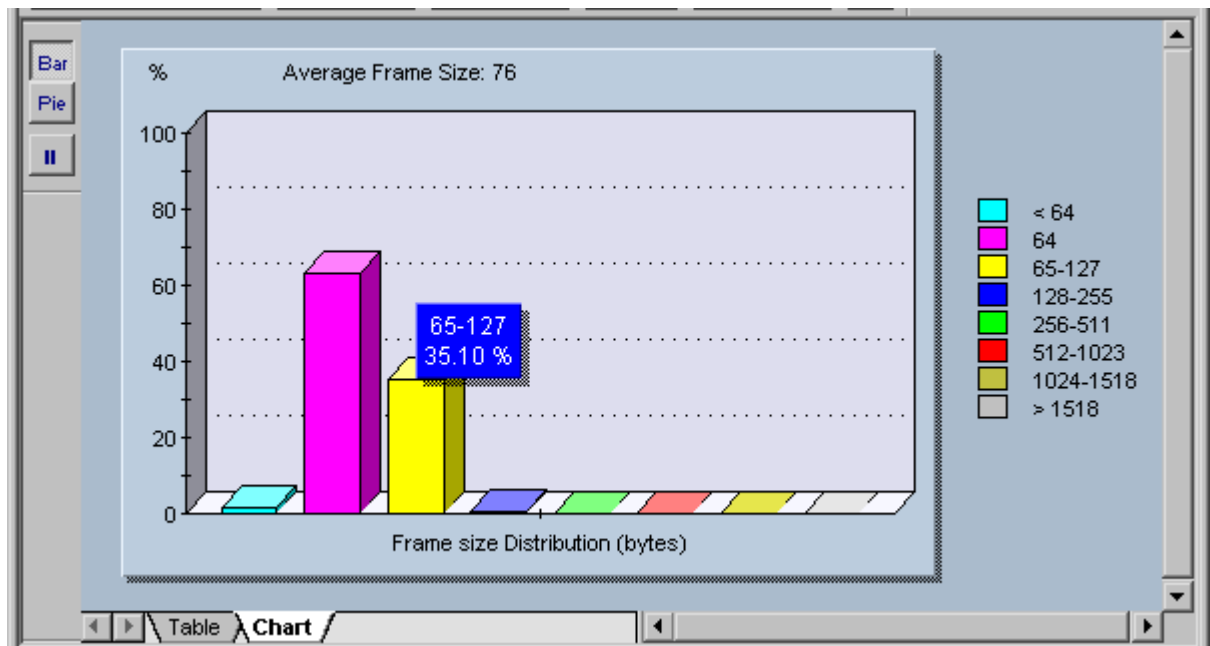
Initially, the chart output is the same as before. However, there are many more toolbar and menu options than in the Summary View. Before looking at these features, confirm that the **Chart** and **Table** tabs show the same information that was seen earlier.


Like all Windows compliant programs, placing the mouse over a button brings up a screen tip briefly identifying the purpose of the button. As the mouse moves over the buttons, notice that some are muted. This means that the feature is not appropriate under the current circumstances. In some cases, it is not supported in the educational version.

Note: There is a complete display of the toolbars and what they do in the Appendix at the end of this lab.

Click on the **Mac Statistics**  button to see the Rx frame table data displayed in another format. The result should be obvious. Maximize the resulting window. The one piece of new information is the **Speed**, which shows the NIC transmission rate.


Click on the **Frame Size Distribution**  button to see a distribution of the size frames being received by the NIC. Placing the mouse over any bar will display a small summary like the one shown below. Maximize the resulting window.

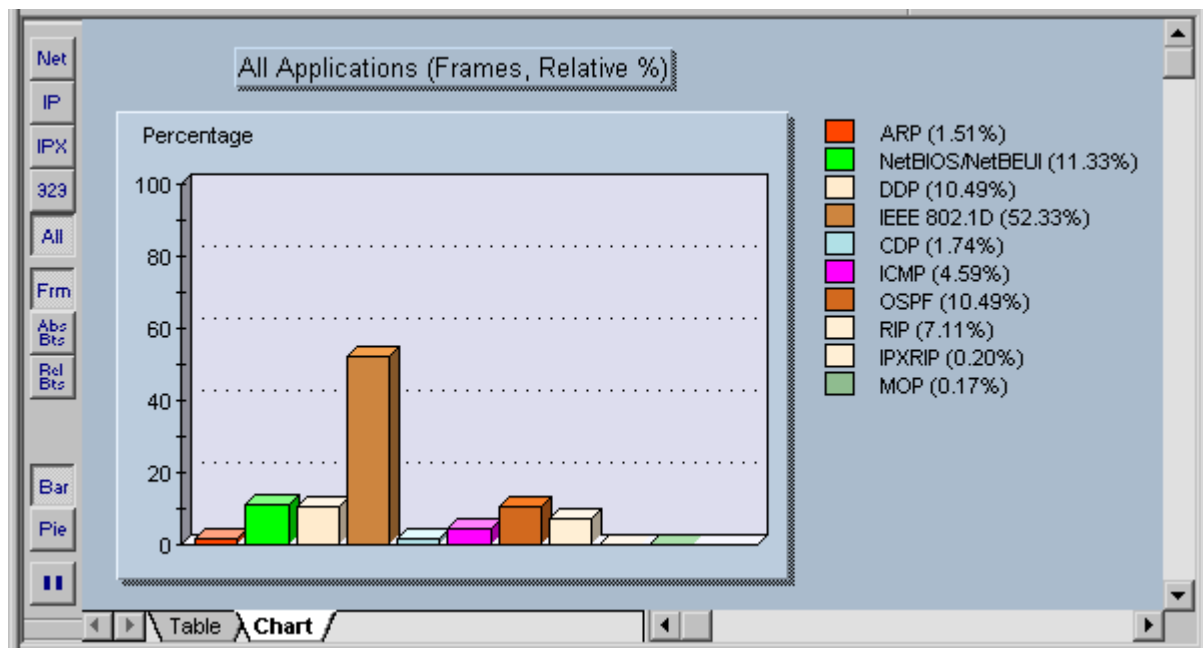


Try the **Pie**, **Bar**, and **Pause**  buttons in the upper-left corner. Note that the **Pause** stops the capture, so click on it again to resume the capture. Look at both the **Table** and **Chart** tab displays as well.


With the sample configurations, the student should be getting mainly small frames, because the only thing happening is routing updates. Try using the extended Ping feature from the router Console connection, and specify 100 pings with a larger packet size.

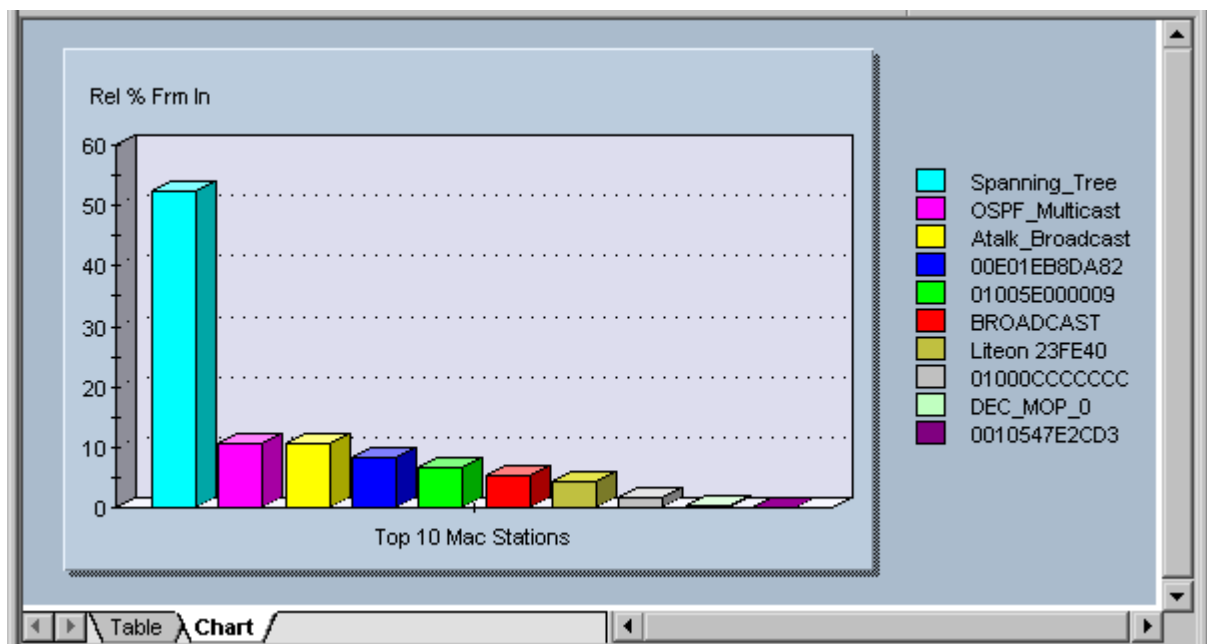
If maximizing each new display, return to any previous view by using the Window menu. The student can also **Tile** the windows. Experiment with the Window menu features and then close any unwanted views.

Click on the **Protocol Distribution**  button to see a distribution of the protocols being received by the NIC. Placing the mouse over any bar will display a small summary panel. Maximize the resulting window.



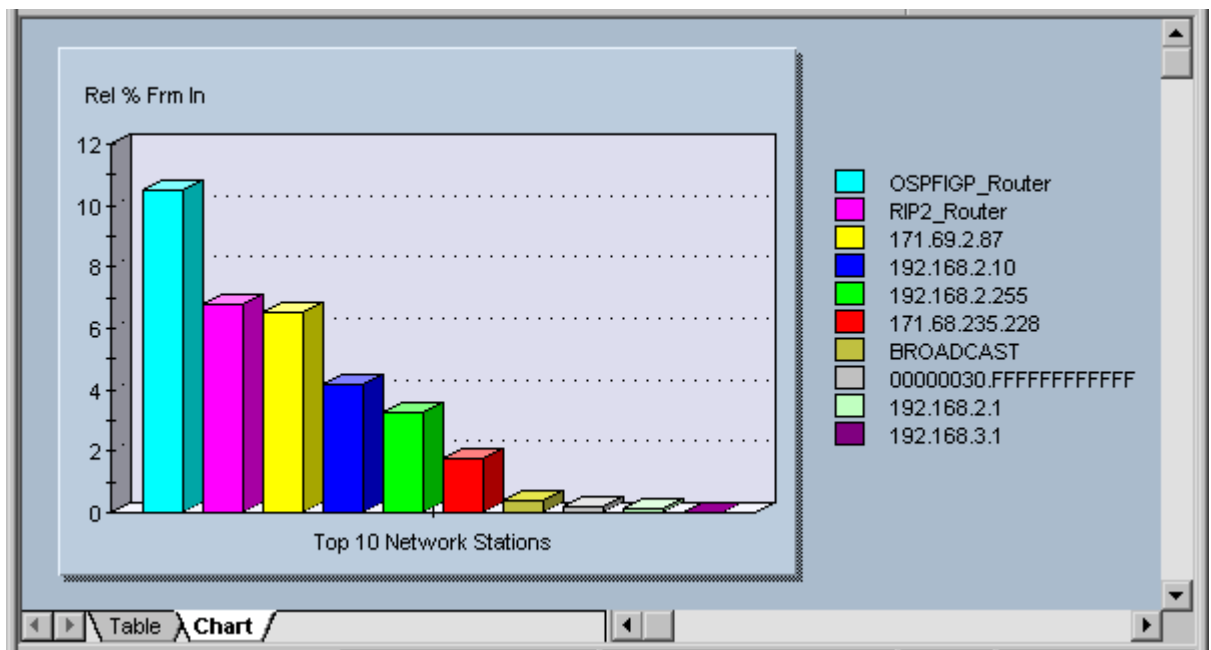
Try each of the buttons and tabs to see the results. The **Net** button shows only network protocols. The **323** button refers to the H323 Voiceover IP protocols. Depending on the version of Protocol Expert or Inspector that is being used, this button may be called VoIP. Look at the **Frm** (frame) and the **Abs Bts** (absolute bytes) and **Rel Bts** (relative bytes) to see the results. Remember that the **Pause** button stops the capture.

Click on the **Host Table**  button to see the MAC stations and related traffic.




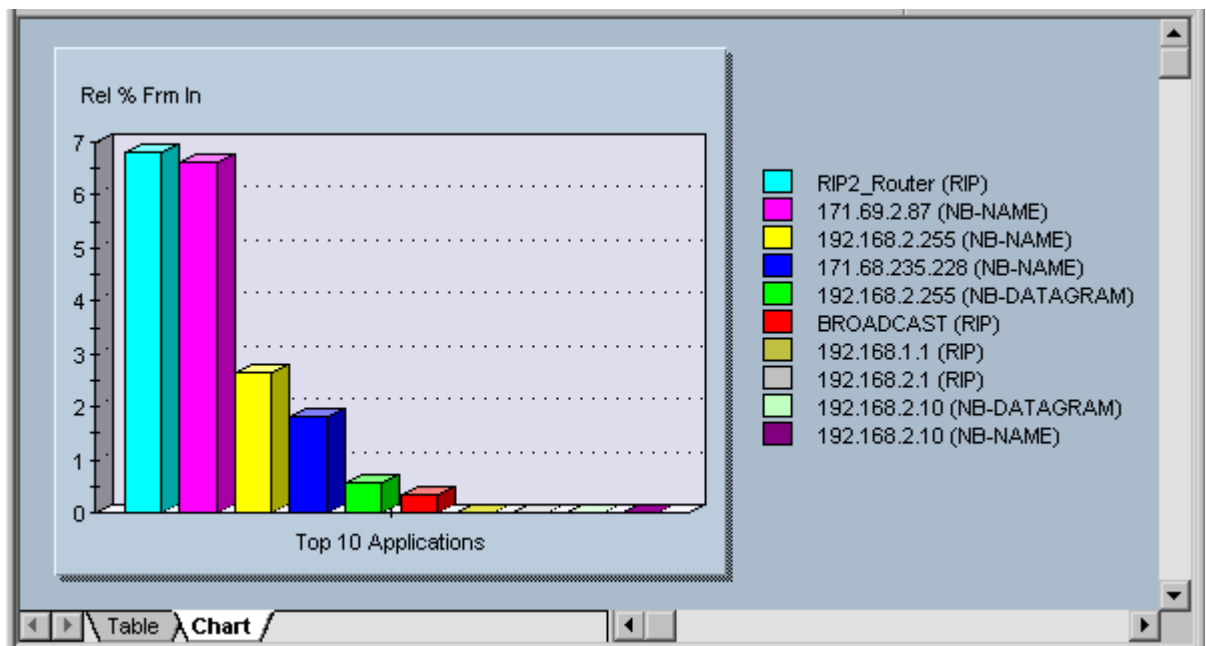
Notice the Spanning Tree, AppleTalk, and OSPF traffic. Be sure to look at the **Table** tab to see the actual values.

Click on the **Network Layer Host Table**  button to see the network (IP/IPX) stations and related traffic.

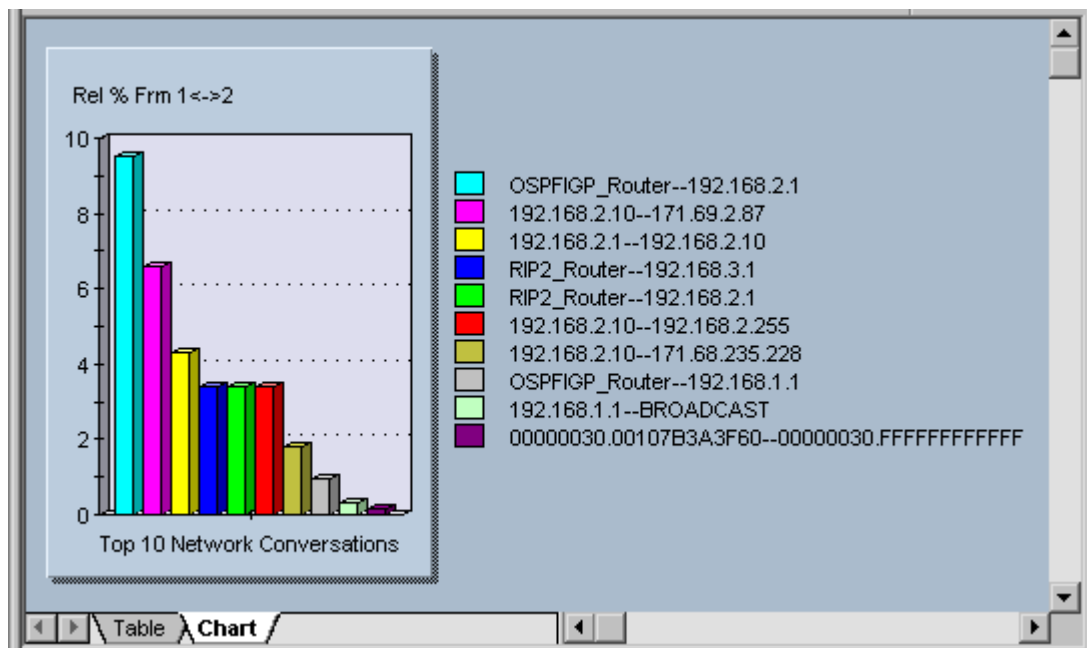


Any pings and any additional hosts that might have added to the configuration will impact the actual addresses that appear on the right.

Click on the **Application Layer Host Table**  button to see the network station traffic by application.



Experiment with the next three  buttons. They create host-to-host matrices for MAC, Network, and Application layer conversations. The following is an example of the Network Layer (IP/IPX) conversations.



Of the next two buttons, the first is the **VLAN** button that shows network traffic on VLANs. This sample does not use VLANs. Remember this button when troubleshooting VLANs later.

The second button creates a matrix comparing MAC and Network station addresses to names. In the following example the second row is a Novell station.

MAC Station Name	MAC Station Address	Network Station Name	Network Station Address
00107B3A3F60	00107B3A3F60	192.168.1.1	192.168.1.1
00107B3A3F60	00107B3A3F60	00000030.00107B3A3F60	00000030.00107B3A3F60
Liteon 23FE40	00A0CC23FE40	192.168.2.10	192.168.2.10
00E01EB8DA82	00E01EB8DA82	192.168.2.1	192.168.2.1
00E01EB8DA82	00E01EB8DA82	192.168.3.1	192.168.3.1



The **Name Table** button opens the current name table for viewing or editing.


NameTable Entries		
Protocol	Name	Address
MAC	HP_Probe	090009000001
MAC	OSPF_Multicast	01005E000005
IP	IP_Station1	206.132.32.2
IP	BROADCAST	255.255.255.255
IP	IP_Multicast	224.0.0.0
IP	DVMRP_Router	224.0.0.4
IP	OSPF_IGP_Router	224.0.0.5
IP	OSPF_IGP_Router_0	224.0.0.6




The **Expert View** button shows the expert symptoms discovered. These statistics are how the PIs try to point out potential problems. The underlined options bring up additional detail windows if there are any values recorded. The sample for this lab will not show much, but it will look over the options for debugging ISL, HSRP, and other types of problems that will be seen in later labs.

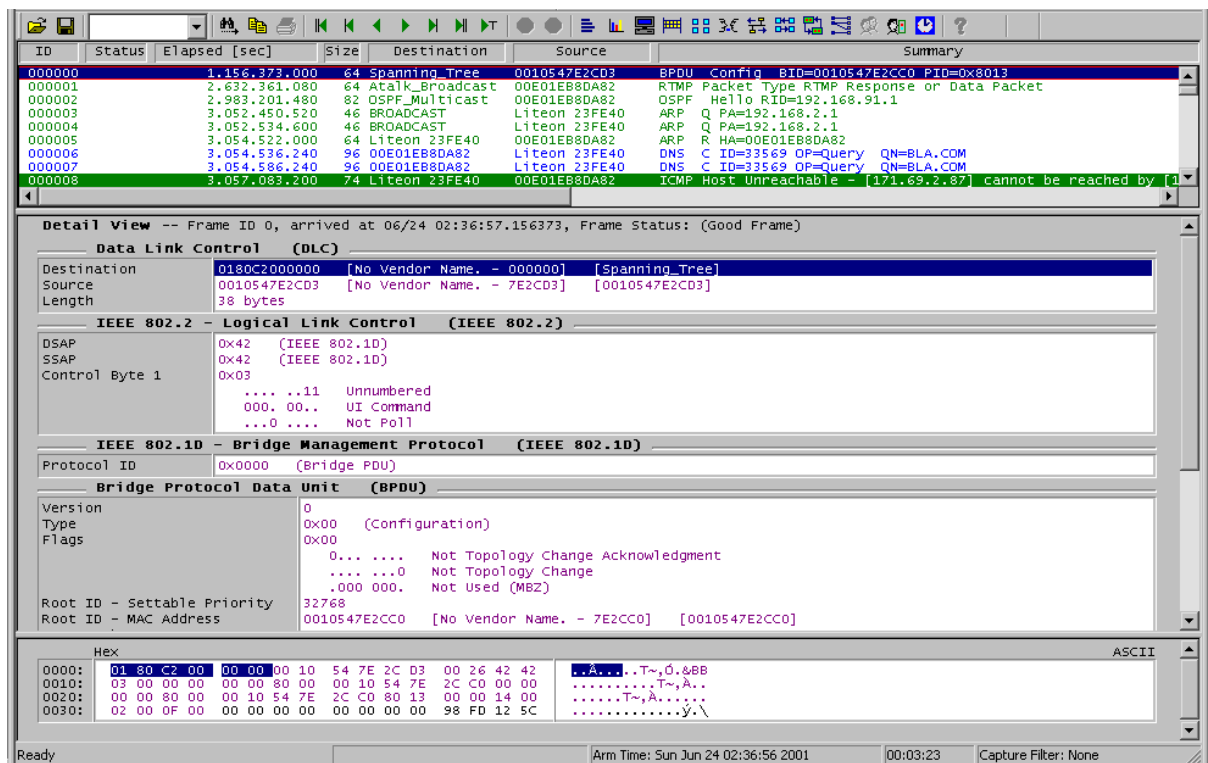
Expert Category	Value	Expert Category	Value
ICMP All Errors	368	Duplicate Network Address	0
ICMP Destination Unreachable	368	Unstable MST	0
ICMP Redirects	0	SAP Broadcast	0
Excessive Bootp	0	OSPF Broadcast	923
Excessive ARP	0	RIP Broadcast	25
NFS Retransmissions	0	ISL Illegal VLAN ID	0
TCP/M SYN Attack	0	ISL BPDU/CDP Packets	0
TCP/M RST Packets	0	IP Time to Live Expiring	0
TCP/M Retransmissions	0	IP Checksum Errors	0
TCP/M Zero Window	0	Illegal Network Source Address	0
TCP/M Long Acks	0	Illegal MAC Source Address	0
TCP/M Frozen Window	0	Total MAC Stations	11
Network Overload	0	Broadcast/Multicast Storm	0
Non Responsive Stations	0	Physical Errors	0
		HSRP Errors	0
		TCP Checksum Errors	0

Step 5 Stop the capture process

To stop the frame capture to look at individual frames use the **Stop**  button or Module | Stop from the menu.

Once the capture has been stopped, click on the **Capture View**  button. With the education version, a message box appears announcing that the capture is limited to 250 packets. Just click OK.

The resulting window can be a little overwhelming at first. Maximize the window to hide any other windows open in the background.



The screenshot shows the Wireshark network protocol analyzer interface. The top pane displays a list of captured packets. The middle pane shows the 'Detail View' for the selected packet (Frame 0), which is an ICMP Host Unreachable message. The bottom pane shows the raw packet data in hexadecimal and ASCII.

ID	Status	Elapsed [sec]	Size	Destination	Source	Summary
000000		1.156.373.000	64	Spanning_Tree	0010547E2CD3	BPDU Config BID=0010547E2CC0 PID=0x8013
000001		2.632.361.080	64	Atalk_Broadcast	00E01EB8DA82	RTMP Packet Type RTMP Response or Data Packet
000002		2.983.201.480	82	OSPF_Multicast	00E01EB8DA82	OSPF Hello RID=192.168.91.1
000003		3.052.450.520	46	BROADCAST	Liteon 23FE40	ARP Q PA=192.168.2.1
000004		3.052.534.600	46	BROADCAST	Liteon 23FE40	ARP Q PA=192.168.2.1
000005		3.054.522.000	64	Liteon 23FE40	00E01EB8DA82	R HA=00E01EB8DA82
000006		3.054.536.240	96	00E01EB8DA82	Liteon 23FE40	DNS C ID=33569 OP=Query QN=BLA.COM
000007		3.054.586.240	96	00E01EB8DA82	Liteon 23FE40	DNS C ID=33569 OP=Query QN=BLA.COM
000008		3.057.083.200	74	Liteon 23FE40	00E01EB8DA82	ICMP Host Unreachable - [171.69.2.87] cannot be reached by [1

Detail View -- Frame ID 0, arrived at 06/24 02:36:57.156373, Frame Status: (Good Frame)

Data Link Control (DLC)

Destination: 0180C2000000 [No Vendor Name. - 000000] [Spanning_Tree]
Source: 0010547E2CD3 [No Vendor Name. - 7E2CD3] [0010547E2CD3]
Length: 38 bytes

IEEE 802.2 - Logical Link Control (IEEE 802.2)

DSAP: 0x42 (IEEE 802.1D)
SSAP: 0x42 (IEEE 802.1D)
Control Byte 1: 0x03
... ..11 Unnumbered
000. 00.. UI Command
...0 Not Poll

IEEE 802.1D - Bridge Management Protocol (IEEE 802.1D)

Protocol ID: 0x0000 (Bridge PDU)

Bridge Protocol Data Unit (BPDU)

Version: 0
Type: 0x00 (Configuration)
Flags: 0x00
... .. Not Topology Change Acknowledgment
... ..0 Not Topology Change
...000 000. Not Used (MBZ)
Root ID - Settable Priority: 32768
Root ID - MAC Address: 0010547E2CC0 [No Vendor Name. - 7E2CC0] [0010547E2CC0]

Hex

```

0000: 01 80 C2 00 00 00 00 10 54 7E 2C D3 00 26 42 42 ..A...T~.d.&BB
0010: 03 00 00 00 00 00 80 00 00 10 54 7E 2C C0 00 00 .....T~.A....
0020: 00 10 54 7E 2C C0 80 13 00 00 14 00 .....T~.A....
0030: 02 00 0F 00 00 00 00 00 00 00 00 00 98 FD 12 5C .....y.\

```

ASCII

```

..A...T~.d.&BB
.....T~.A....
.....T~.A....
.....y.\

```

Ready | Arm Time: Sun Jun 24 02:36:56 2001 | 00:03:23 | Capture Filter: None

In looking over the results, note that there are actually three horizontal windows open. The top window lists the captured packets. The middle window shows the detail of the selected packet in the top window, and the bottom window shows the HEX values for the packet.

By positioning the mouse over the borders among the three windows, a line mover or two-headed arrow will appear. This allows the distribution of space for each window to be changed. It may be advantageous to make the middle window as large as possible and leave five to six rows in each of the other two, as shown above.

Look over the packets listed in the top window. DNS, ARP, RTMP, and other types of packets should be found. If using a switch, there should be CDP and Spanning Tree packets. Notice that as rows are selected in the top window, the contents of the other two windows change.

Select information in the middle window, and notice that the HEX display in the bottom window changes to show where that specific information is stored. In the following example, selecting the Source Address (IP) shows HEX values from the packet.

Checksum	0xA777 (Correct)
Source Address	192.168.2.10
Destination Address	171.69.2.87
	[58 bytes of data]

Hex	
0000:	00 E0 1E B8 DA 82 00 A0 CC 23 FE 40 08 00 45 00 .à.Ú..i#p@..E.
0010:	00 4E 22 D9 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Û....\$wA..«E
0020:	02 57 00 89 00 89 00 3A 99 97 83 21 01 00 00 01 .W.....!....

Note also the color coding makes it easier to locate information from the middle window in the HEX window. In the following example with a DNS packet, the data in the Data Link Control (DLC) section of middle window is purple, while the Internet Protocol (IP) section is green. The corresponding HEX values are the same colors.

000005	3.054.522.000	64 Liteon 23FE40	00E01EB8DA82	ARP R HA=0C
000006	3.054.536.240	96 00E01EB8DA82	Liteon 23FE40	DNS C ID=33
000007	3.054.586.240	96 00E01EB8DA82	Liteon 23FE40	DNS C ID=33

Data Link Control (DLC)	
Destination	00E01EB8DA82 [No Vendor Name. - B8DA82] [00E01EB8DA82]
Source	00A0CC23FE40 [LITE-ON COMMUNICATIONS, INC. - 23FE40] [Liteon
EtherType	0x0800 (Internet Protocol (IP))

Internet Protocol (IP)	
Version/Header Length	0x45 0100 Version 4 0101 20 bytes - Header Length
Type of Service	0x00

Hex	
0000:	00 E0 1E B8 DA 82 00 A0 CC 23 FE 40 08 00 45 00 .à.Ú..i#p@..E.
0010:	00 4E 22 D9 00 00 80 11 A7 77 C0 A8 02 0A AB 45 .N"Û....\$wA..«E
0020:	02 57 00 89 00 89 00 3A 99 97 83 21 01 00 00 01 .W.....!....
0030:	00 00 00 00 00 00 20 45 43 45 40 45 42 43 4F 45ECMEBCOE
0040:	44 45 50 45 4E 43 41 43 41 43 41 43 41 43 41 43 DEPENCACACACAC
0050:	41 43 41 43 41 41 41 00 00 20 00 01 67 87 47 13 ACACAAA...g.G.

Notice in the above example the **EtherType** is **0x0800**. This indicates that it is an IP packet. Notice the MAC addresses for both the Destination and Source hosts as well as where that data is stored in the HEX display.

In the same example, the next section in the middle window is the **User Datagram Protocol (UDP)** information, which includes the UDP port numbers.

User Datagram Protocol (UDP)	
Source Port	137 (NETBIOS Name Service)
Destination Port	137 (NETBIOS Name Service)
Length	58 bytes
Checksum	0x9997 (Correct)
	[50 bytes of data]

The structure of the middle window changes for each type of packet.

Take a few minutes to select different packet types in the top window, and then look over the resulting display in the other two windows. Pay particular attention to the EtherType, any port numbers, as well as source and destination addresses, which include both MAC and network layer. There should be RIP, OSPF, and RTMP or AppleTalk packets in the capture. Make sure that the important data can be loaded and interpreted. In the following RIP capture, notice that this is a RIP version 2 packet. The multicast destination address is 224.0.0.9, and that the actual route table entries can be seen. What would the multicast destination address be in version 1? _____

Source Address	192.168.3.1
Destination Address	224.0.0.9 [RIP2_Router] [72 bytes of data]
User Datagram Protocol (UDP)	
Source Port	520 (Routing Information Protocol)
Destination Port	520 (Routing Information Protocol)
Length	72 bytes
Checksum	0x6192 (Correct)
	[64 bytes of data]
Routing Information Protocol	
Command	2 (Routing Response)
Version	2 (RIP2)
Unused	0 0
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.0.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.90.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1
Routing Info	Addr Family: 2 (IP), Route Tag: 0, Addr:192.168.91.0, Subnet Mask:255.255.255.0, Next Hop:0.0.0.0, Metric:1

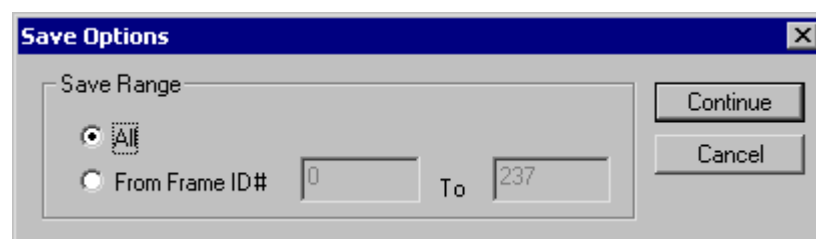
If there are any CDP packets, figure out the platform. The following is from a Catalyst 1900 switch.

Variable Type	0x0006 (Platform)
Variable Length	14
Platform	cisco 1900
0020:	31 30 33 34 37 43 32 43 43 30 00 00 02 00 11 00 10547 EEE0.....
0030:	00 00 01 01 01 CC 00 04 C0 A8 01 64 00 03 00 06i..A..d....
0040:	31 39 00 04 00 08 00 00 00 0A 00 05 00 09 56 38 19.....V8
0050:	2E 30 30 00 06 00 0E 63 69 73 63 6F 20 31 39 30 .00....Cisco 190
0060:	30 8A 88 60 39 0..9

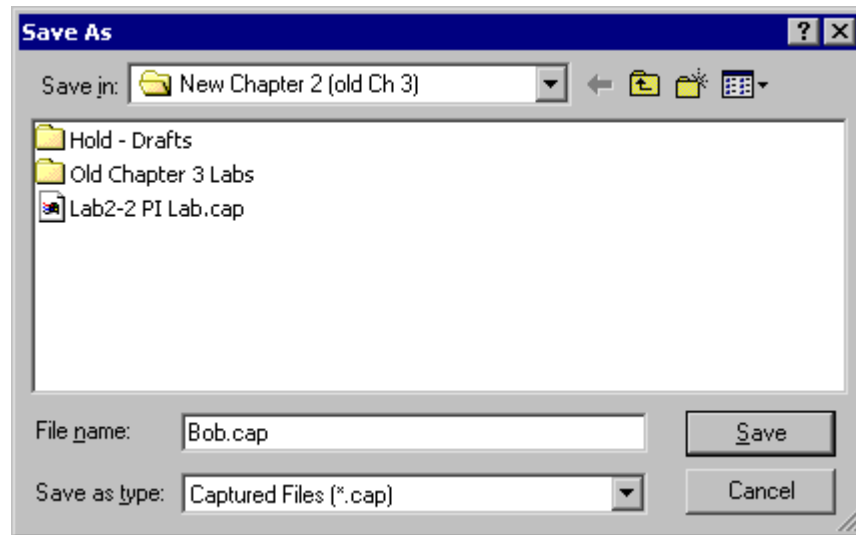
Experiment until comfortable with the tools.


Step 6 Save the captured data

To save captured data, use the **Save Capture**  button or choose File | Save Capture from the menu system. Depending on the version of Protocol Expert or Inspector that is being used, the File menu may offer "Save Current Section" instead of "Save Capture". Accept the **All** option by using the **Continue** button. The student can save just a range of captured frames with this window.




Use a proper file name and store the file on the appropriate disk. If the CAP extension is showing when this window opens, make sure it remains after typing the name.




Use the **Open Capture File**  button and open the file called Lab3-2 PI Lab.cap. If it is not available, then open the file that was just saved.

The student is now using the **Capture View of Capture Files**. There is no difference in tools, but the title bar at the top of the screen indicates that a file is being viewed rather than a capture in memory.

Step 7 Examine frames

Select a frame in the top window and try the  buttons. The arrows by themselves move up or down one frame. The arrow with single line is top or bottom of the current window, while the arrow with two arrows is the top or bottom of the entire list. The arrow with the T also moves to the top of the list.

Use the **Search**  buttons to perform searches. Type text like OSPF in the list box. Then click on the binoculars, and it will move from one OSPF entry to the next.

Experiment until comfortable with the tools.

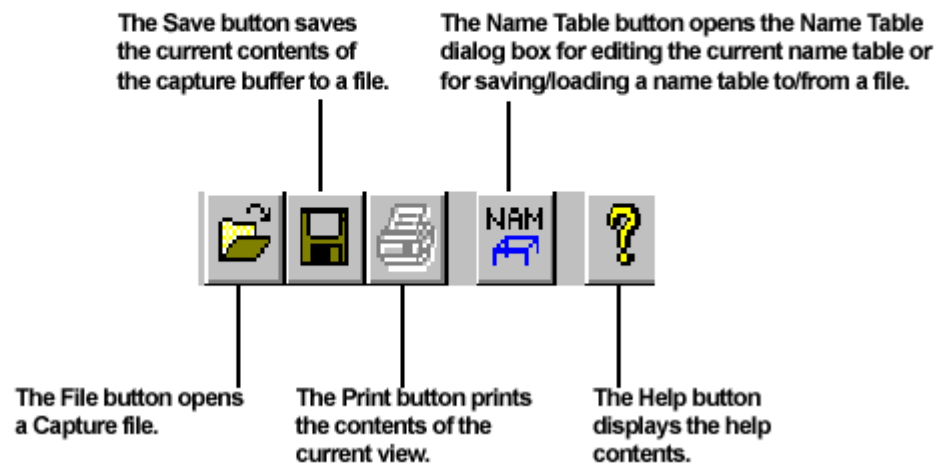
Reflection

- How might this tool be used in troubleshooting?

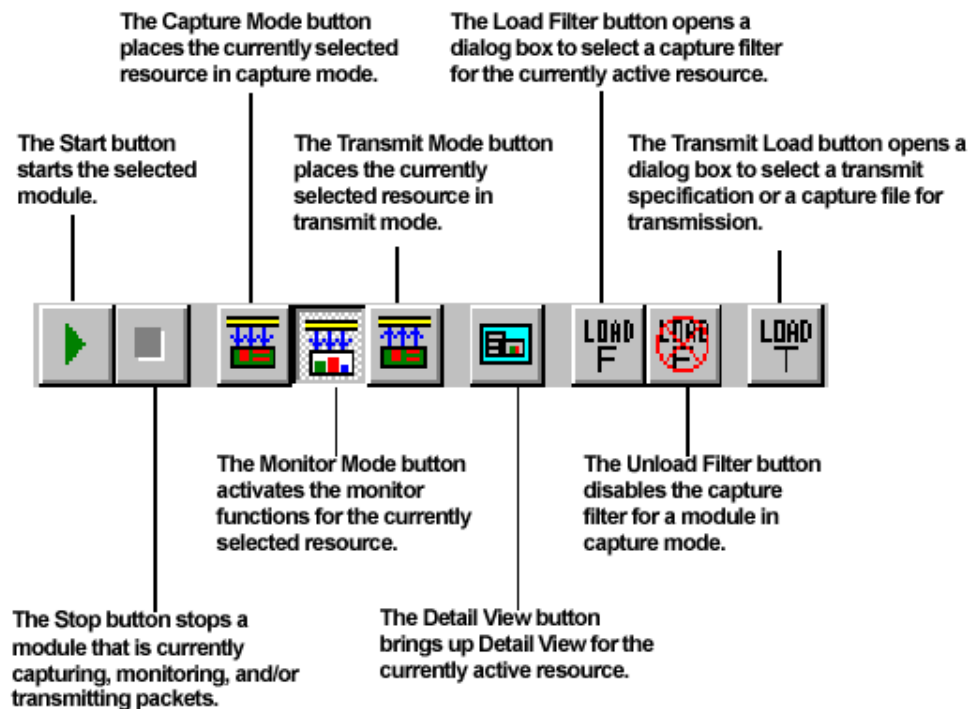
- Is all of the data on the network being analyzed?

- What is the impact of being connected to a switch?

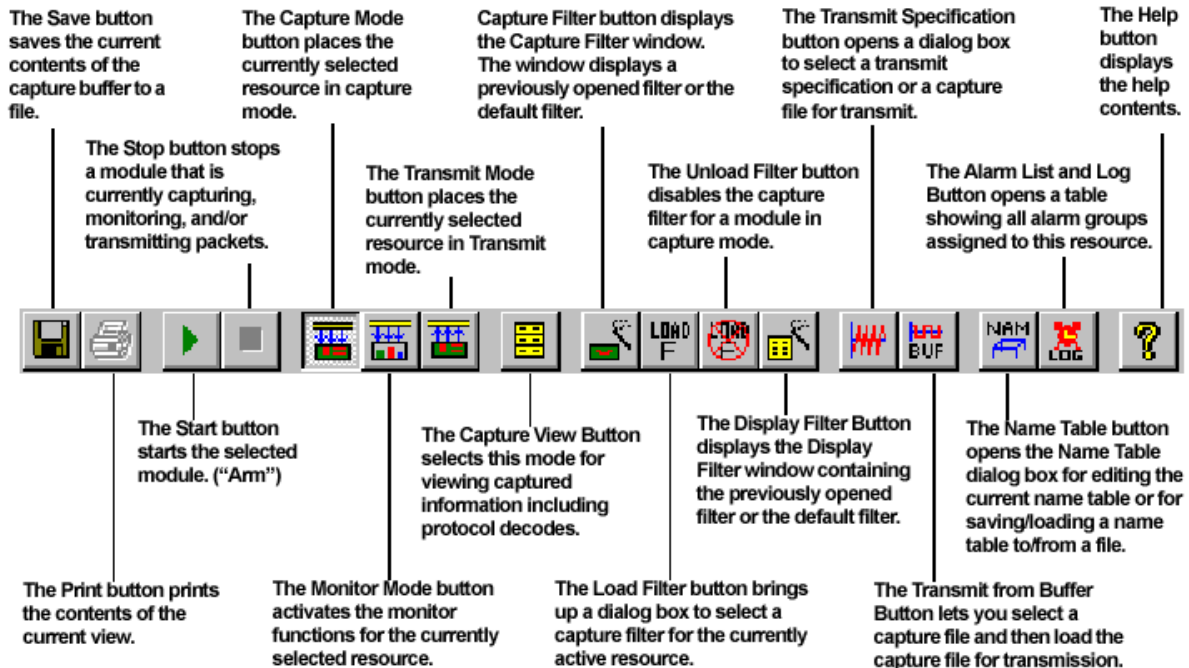
Protocol Inspector Toolbar



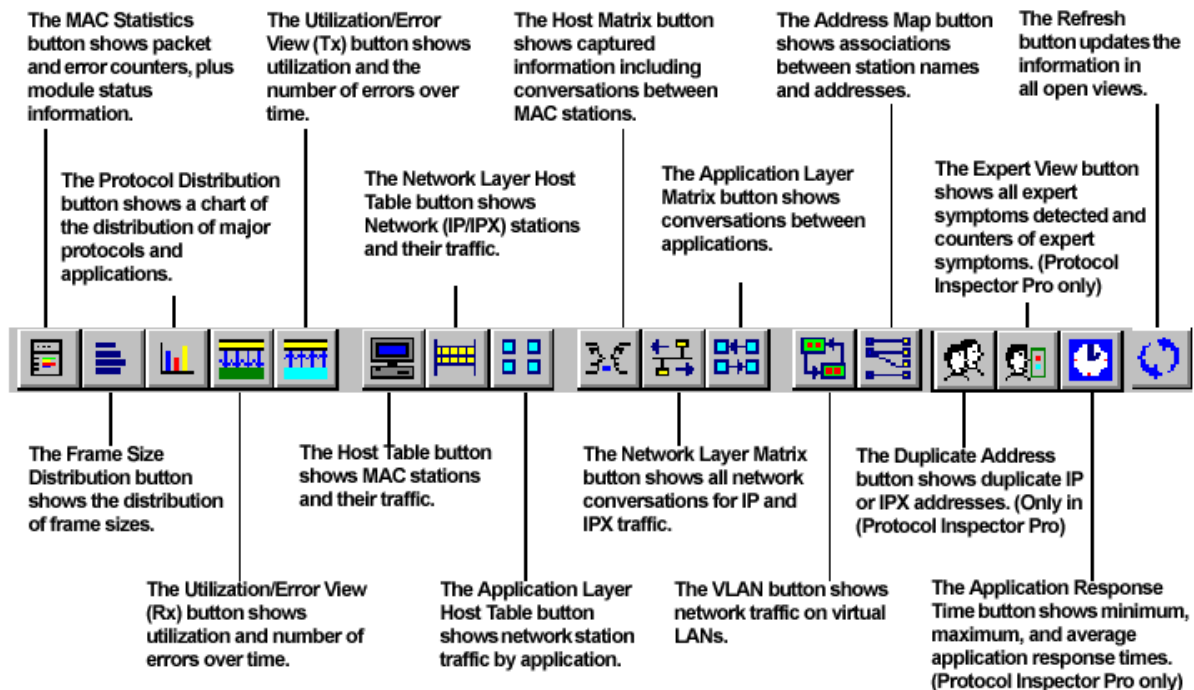
Module Toolbar (Summary View)



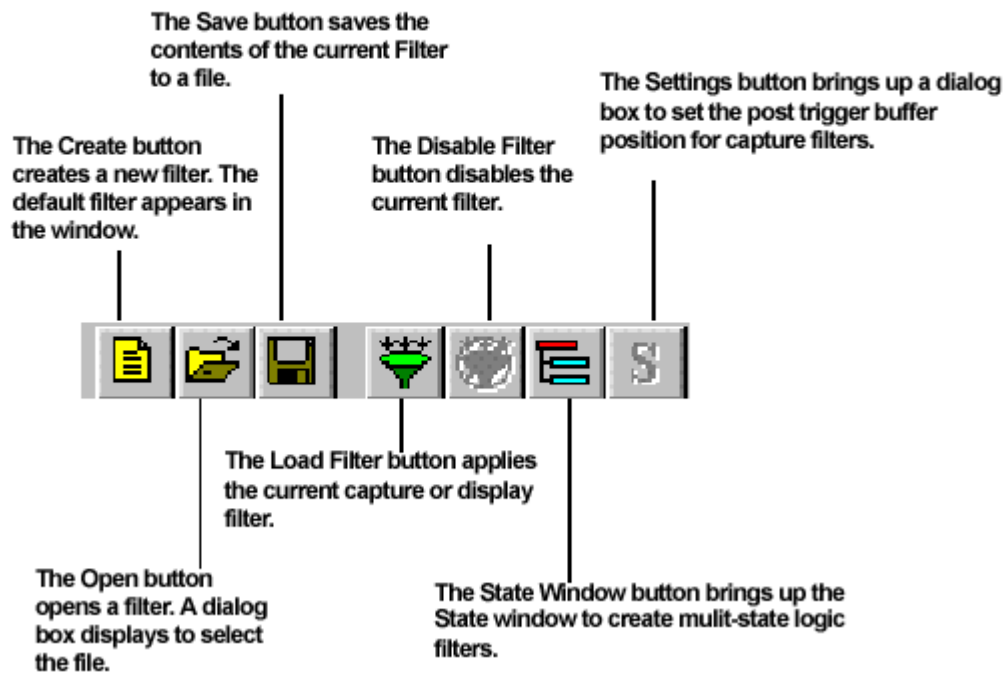
Detail View Toolbar



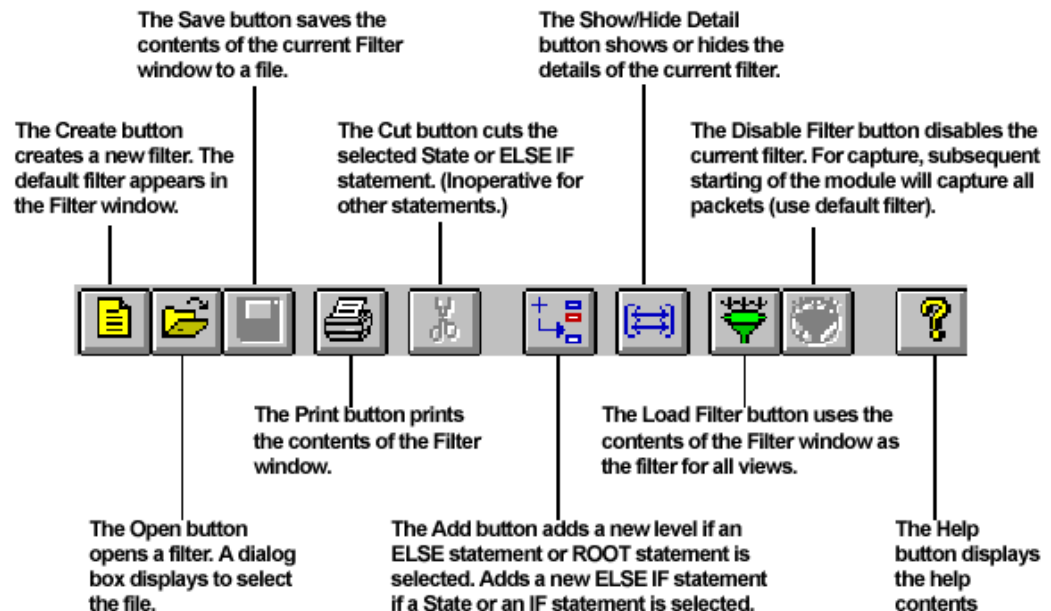
Data Views Toolbar (Note: Only some of these views are available with GMM cards)



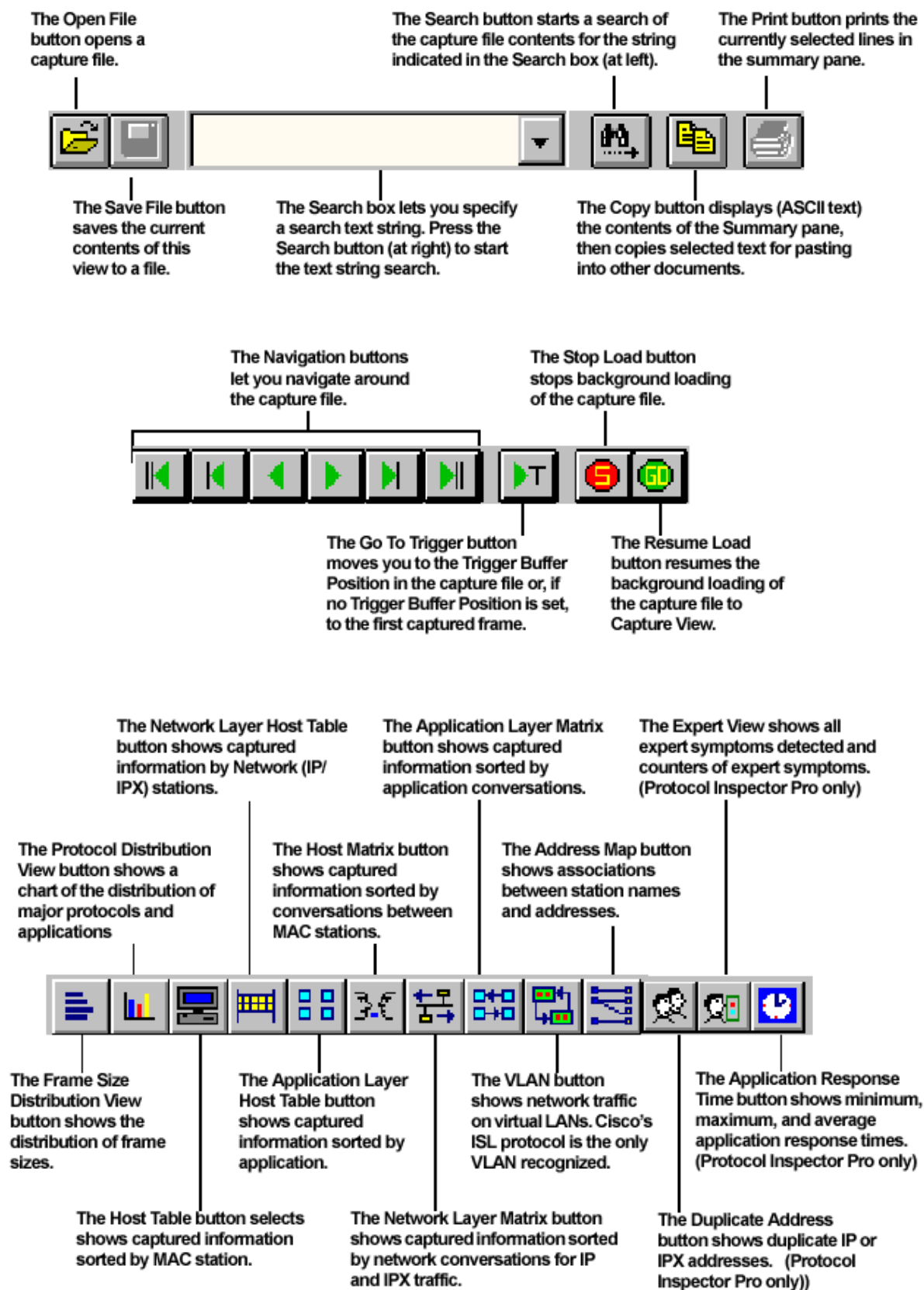
Create/Modify Filter Toolbar



State Toolbar



Capture View Toolbar



Function Keys

Function keys perform different operations within different Protocol Inspector views.

Function Key	Summary View	Detail View
F1	Help	Help
F2	System Settings	Capture View Display Options
F3	Module Settings	Module Settings
F4	Module Monitor View Preferences	Create Display Filter
F5	Connect to Remote	Create Capture Filter
F6	Load Capture Filter	Load Capture Filter
F7	Open Capture File	Expert Summary View
F8	Save Capture	Save Capture
F9	Go to Detail View	Capture View
F10	Start/Stop	Start/Stop
F11	N/A	N/A
F12	N/A	N/A

Other Keyboard Shortcuts...

Key Combination	Action
Alt + F4	Close Window
Ctrl + O	Open
Ctrl + S	Save
Ctrl + T	Start Module
Ctrl + P	Stop Module



Lab 9.2.7 IP Addressing Basics

Objective

- Name the five different classes of IP addresses
- Describe the characteristics and use of the different IP address classes
- Identify the class of an IP address based on the network number
- Determine which part, or octet, of an IP address is the network ID and which part is the host ID
- Identify valid and invalid IP host addresses based on the rules of IP addressing
- Define the range of addresses and default subnet mask for each class

Background / Preparation

This lab exercise helps develop an understanding of IP addresses and how TCP/IP networks operate. It is primarily a written lab exercise. However, it would be worthwhile to review some real network IP addresses using the command line utilities `ipconfig` for Windows NT/2000/XP or `wingipcfg` for Windows 9x/ME. IP addresses are used to uniquely identify individual TCP/IP networks and hosts, such as computers and printers, on those networks in order for devices to communicate. Workstations and servers on a TCP/IP network are called hosts and each has a unique IP address. This address is referred to as its host address. TCP/IP is the most widely used protocol in the world. The Internet or World Wide Web only uses IP addressing. In order for a host to access the Internet, it must have an IP address.

In its basic form, the IP address has two parts:

- A network address
- A host address

The network portion of the IP address is assigned to a company or organization by the Internet Network Information Center (InterNIC). Routers use the IP address to move data packets between networks. IP addresses are 32 bits long according to the current version IPv4 and are divided into 4 octets of 8 bits each. They operate at the network layer (Layer 3) of the Open System Interconnection (OSI) model, which is the Internet layer of the TCP/IP model. IP addresses are assigned in the following ways:

- Statically – manually, by a network administrator
- Dynamically – automatically, by a Dynamic Host Configuration Protocol (DHCP) server

The IP address of a workstation, or host is a logical address, meaning it can be changed. The Media Access Control (MAC) address of the workstation is a 48-bit physical address. This address is burned into the network interface card (NIC) and cannot change unless the NIC is replaced. The combination of the logical IP address and the physical MAC address helps route packets to their proper destination.

There are five different classes of IP addresses, and depending on the class, the network and host part of the address will use a different number of bits. In this lab, different classes of IP addresses will be worked with and to help become familiar with the characteristics of each. The understanding of IP addresses is critical to the understanding of TCP/IP and internetworks in general. The following resources are required:

- PC workstation with Windows 9x/NT/2000/XP installed
- Access to the Windows Calculator

Step 1 Review IP address classes and their characteristics

Address classes

There are five classes of IP addresses, A through E. Only the first three classes are used commercially. A Class A network address is discussed in the table to get started. The first column is the class of IP address. The second column is the first octet, which must fall within the range shown for a given class of addresses. The Class A address must start with a number between 1 and 126. The first bit of a Class A address is always a zero, meaning the High Order Bit (HOB) or the 128 bit cannot be used. 127 is reserved for loopback testing. The first octet alone defines the network ID for a Class A network address.

Default subnet mask

The default subnet mask uses all binary ones, decimal 255, to mask the first 8 bits of the Class A address. The default subnet mask helps routers and hosts determine if the destination host is on this network or another one. Because there are only 126 Class A networks, the remaining 24 bits, or 3 octets, can be used for hosts. Each Class A network can have 2^{24} , or over 16 million hosts. It is common to subdivide the network into smaller groupings called subnets by using a custom subnet mask, which is discussed in the next lab.

Network and host address

The network or host portion of the address cannot be all ones or all zeros. As an example, the Class A address of 118.0.0.5 is a valid IP address. The network portion, or first 8 bits, which are equal to 118, is not all zeros and the host portion, or last 24 bits, is not all zeros or all ones. If the host portion were all zeros, it would be the network address itself. If the host portion were all ones, it would be a broadcast for the network address. The value of any octet can never be greater than decimal 255 or binary 11111111.

Class	1 st Octet Decimal Range	1 st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126 *	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	11110	Experimental; used for research			

Note: Class A address 127 cannot be used and is reserved for loopback and diagnostic functions.

Step 2 Determine basic IP addressing

Use the IP address chart and your knowledge of IP address classes to answer the following questions:

1. What is the decimal and binary range of the first octet of all possible Class B IP addresses?

Decimal: From: _____ To: _____

Binary: From: _____ To: _____

2. Which octet(s) represent the network portion of a Class C IP address? _____
3. Which octet(s) represent the host portion of a Class A IP address? _____
4. What is the maximum number of useable hosts with a Class C network address? _____
5. How many Class B networks are there? _____
6. How many hosts can each Class B network have? _____
7. How many octets are there in an IP address? _____ How many bits per octet? _____

Step 3 Determine the host and network portions of the IP address

With the following IP host addresses, indicate the following:

- Class of each address
- Network address or ID
- Host portion
- Broadcast address for this network
- Default subnet mask

The host portion will be all zeros for the network ID. Enter just the octets that make up the host. The host portion will be all ones for a broadcast. The network portion of the address will be all ones for the subnet mask. Fill in the following table:

Host IP Address	Address Class	Network Address	Host Address	Network Broadcast Address	Default Subnet Mask
216.14.55.137					
123.1.1.15					
150.127.221.244					
194.125.35.199					
175.12.239.244					

Step 4 Given an IP address of 142.226.0.15 and a subnet mask of 255.255.255.0, answer the following questions:

What is the binary equivalent of the second octet? _____

What is the class of the address? _____

What is the network address of this IP address? _____

Is this a valid IP host address (Y/N)? _____

Why or why not?

Step 5 Determine which IP host addresses are valid for commercial networks

For the following IP host addresses, determine which are valid for commercial networks and indicate why or why not. Valid means it could be assigned to any of the following:

- Workstation
- Server
- Printer
- Router interface
- Any other compatible device

Fill in the following table:

IP Host Address	Valid Address? (Yes/No)	Why or Why Not
150.100.255.255		
175.100.255.18		
195.234.253.0		
100.0.0.23		
188.258.221.176		
127.34.25.189		
224.156.217.73		



Lab 9.3.5 DHCP Client Setup

Objective

The purpose of this lab is to introduce Dynamic Host Configuration Protocol (DHCP) and the process for setting up a network computer as a DHCP client to use DHCP services.

Background / Preparation

DHCP provides a mechanism for dynamically assigning IP addresses and other information. A DHCP server device located on the LAN or at the ISP can respond to a host request and furnish all of the following required information:

- IP address
- Subnet mask
- Default gateway
- Domain Name System (DNS) server
- Other resource addresses

Without DHCP all of the above information would have to be manually configured on each host individually.

The DHCP device is typically a network server.

In small networks, DHCP services can be provided by a small router. This includes many home networks with DSL, cable, or wireless connections. Cisco and many other manufacturers offer small routers that include the following features:

- An Internet or WAN connection
- A small built-in hub or switch
- A DHCP server service

This lab will focus on setting up a computer to use the DHCP services provided.

This lab assumes the PC is running any version of Windows. Ideally, this lab will be done in a classroom or other LAN connected to the Internet. It can also be done from a single remote connection via a modem or DSL-type connection.

Note: If the network that the computer is connected to is using static addressing, follow the lab and view the various screens. **Do not** try to change settings on these machines. The static settings will be lost and would require reconfiguration.

Step 1 Establish a network connection

If the connection to the Internet is dialup, connect to the ISP to ensure that the computer has an IP address. In a TCP/IP LAN with a DHCP server it should not be necessary to do this step.

Step 2 Access a command prompt

Windows NT, 2000, and XP users will use the **Start** menu to open the **Command Prompt** window. The Command Prompt window is like the MS-DOS Prompt window for other Windows versions:

Start > Programs > Accessories > Command Prompt or **Start > Programs > Command Prompt**

To open the MS-DOS Prompt window, Windows 95, 98, and ME users will use the Start menu:

Start > Programs > Accessories > MS-DOS Prompt or **Start > Programs > MS-DOS Prompt**

Step 3 Display IP settings to determine if the network is using DHCP

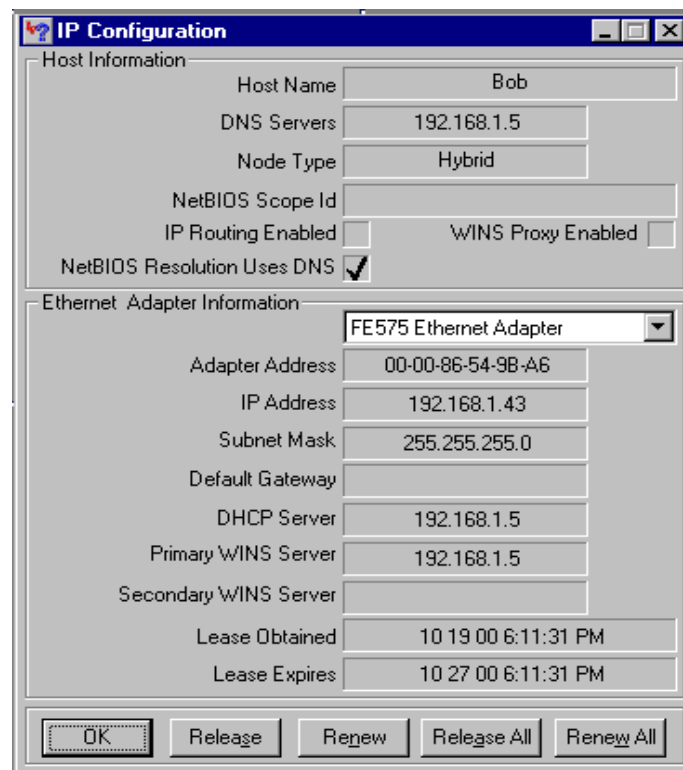
Windows 95/98/ME users:

Type `winipcfg` and press **Enter**, then click the **More Info** button.

The example below indicates that DHCP is in fact being used by the entries in the following boxes:

- **DHCP Server IP address**
- **Lease Obtained**
- **Lease Expires**

These entries would be blank in a statically configured device. DHCP also supplied the DHCP and WINS server addresses. The missing default gateway indicates a proxy server.



Windows NT / 2000 / XP users:

Type `ipconfig/all` and press **Enter**.

The following Windows NT, 2000, and XP example indicates that DHCP is in fact being used by the **DHCP enabled** entry. The entries for the **DHCP Server**, **Lease Obtained**, and **Lease Expires** confirm this fact. These last three entries would not exist in a statically configured device and **DHCP enabled** would say **No**.

```
C:\>ipconfig /all

Windows 2000 IP Configuration

Host Name . . . . . : thunder
Primary DNS Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description . . . . . : LNE100TX Fast Ethernet Adapter Version 1.0
Physical Address. . . . . : 00-A0-CC-23-FE-40
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IP Address. . . . . : 192.168.1.10
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DNS Servers . . . . . : 24.0.224.33
                        24.0.224.34
Lease Obtained. . . . . : Tuesday, January 09, 2001 10:56:19 AM
Lease Expires . . . . . : Monday, January 15, 2001 10:56:19 AM

C:\>
```

Is DHCP running on the network? _____

Ask the instructor or lab assistant for help if it is hard to tell whether or not the DHCP is actually running.

What is the length of the DHCP lease? _____

DHCP servers provide IP addresses for a limited time, usually several days. However, the actual length of time can be configured by the network administrator. If a lease expires, the IP address is returned to the pool to be used by others. This allows DHCP to recapture inactive IP addresses without humans having to update the records. An organization that lacks enough IP addresses for every user may use very short lease durations, so that they are reused even during brief periods of inactivity.

When a computer stays connected to the network and remains powered on, it will automatically request that the lease be extended. This helps a computer avoid an expired lease as long as it is used regularly.

Sometimes a computer is moved from one network to another where the network portion of the IP address is different. When this happens, the computer may still retain its settings from the old network and be unable to connect to the new network. One solution is to release and renew the lease. Statically configured computers can do this, but there will be no change. Computers connected directly to an ISP may lose connection and have to replace their call, but no permanent changes will occur. Follow these steps to release and renew the DHCP lease:

Windows NT/2000/XP users:

Type **ipconfig/release** and press **Enter**. Look over the results and then type **ipconfig /renew**.

Since the machine did not actually change locations as described above, the same settings as before will probably appear. If the machine had been moved as described above, a new settings would appear.

Windows 95/98/ME users:

Click on the **Release All** button. Look over the results and then click on the **Renew All** button.

Since the machine did not actually change locations as described above, the same settings as before will probably appear. If the machine had been moved as described above, new settings would appear.

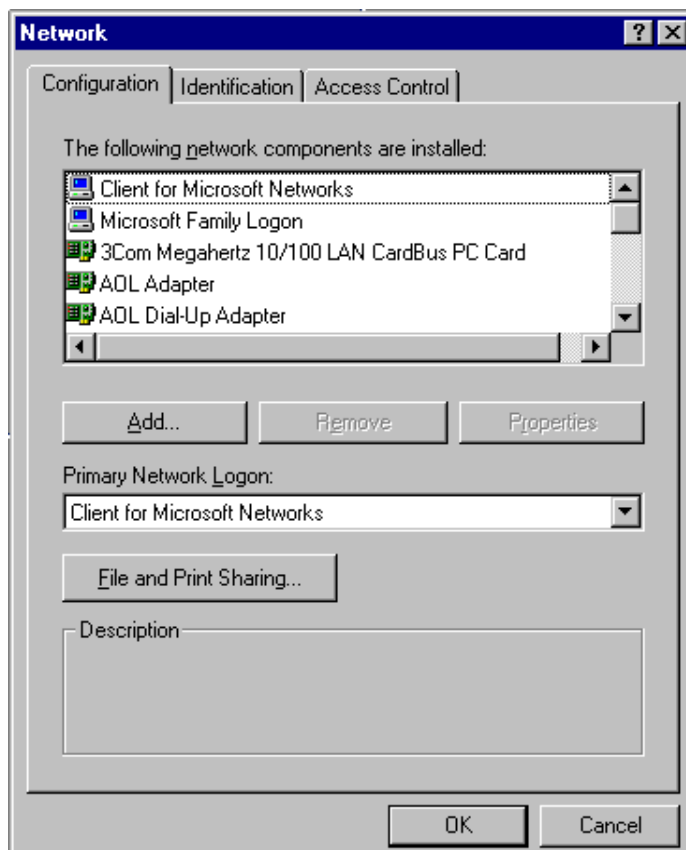
Step 4 Accessing the network configuration window

On the desktop, right click on the **Network Neighborhood** or **My Network Places** icon and choose **properties**. If neither icon on the machine, try using the Start button:

Start > Settings > Control Panel

Then double click on the **Network** icon.

Some users will see a screen like the Network properties box shown below:



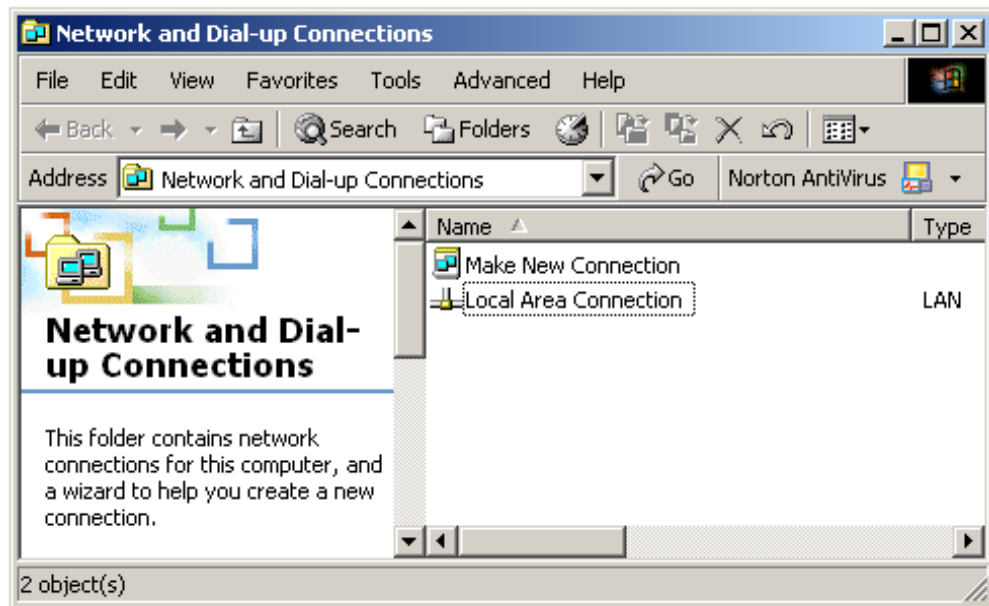
Different versions of Windows will have slightly different tabs and the current configuration of the computer will determine the items included in the Network Components box. However, the box should still look similar to the one above.

Most Windows 95, 98, and ME systems should see the Network Properties at this point. So, if a Network window similar to the one above is shown, skip to the next numbered step.

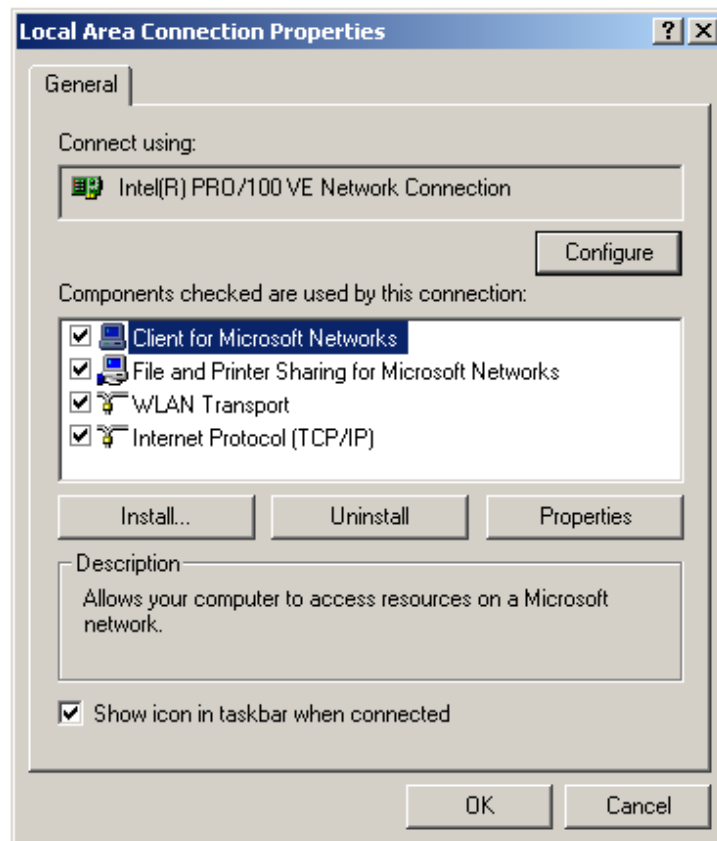
Windows 2000 and XP users need to do two more things.

In the window, double-click on **Local Area Connection**.

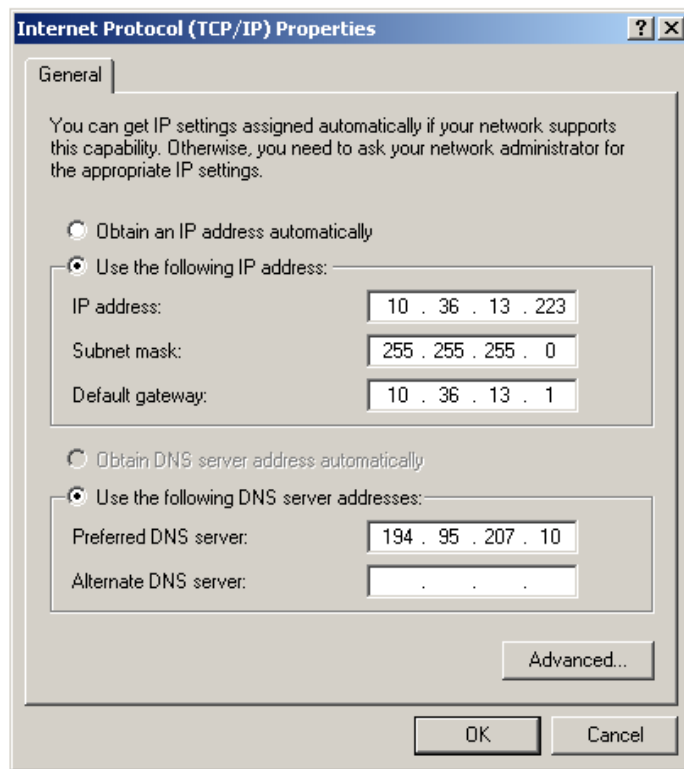
When the **Local Area Connection Status** window appears, click on the **Properties** button. That will bring up a **Local Area Connection Properties** similar to the one shown in the next step.



In the network properties window scroll through the listed components and find a listing for TCP/IP. If there is more than one listing, find the one for the current network connection, such as NIC or modem. In Windows 2000 and XP it will look like the following:



Select the appropriate TCP/IP entry and click on the **Properties** button or double-click directly on the TCP/IP entry. The screen that will appear next depends again on the version of Windows being used, but the process and concepts are the same. The screen below should look very similar to what Windows 2000 and XP users are seeing. First thing that should be noted on the example computer is that it is configured for Static addressing.



Step 5 Enable DHCP

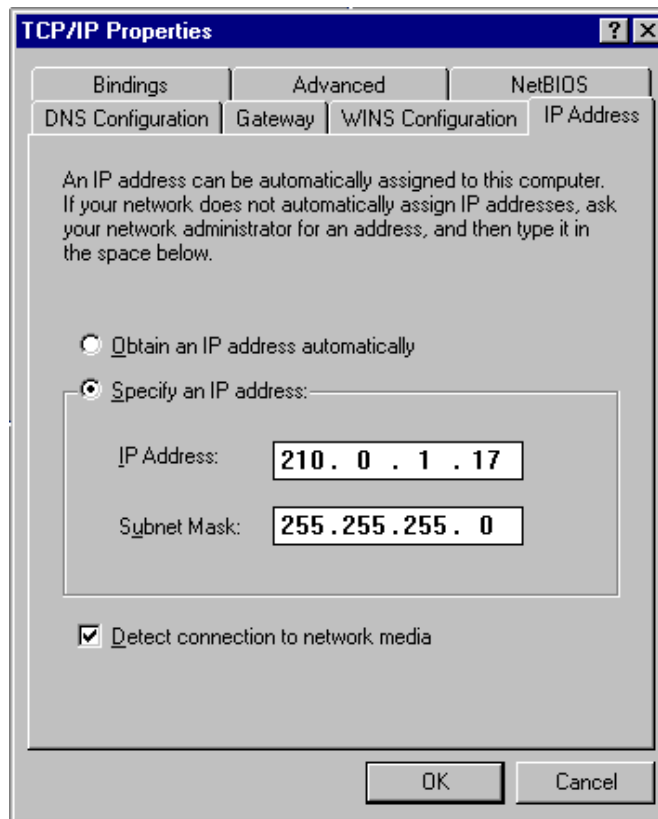
To enable DHCP, select **Obtain an IP address automatically** and typically select **Obtain DNS server address automatically**. The various settings will blank out as these options are selected. If the computer had Static addressing and it needs to be restored, click on the **Cancel** button. To keep the changed settings click **OK**.

Older versions of Windows have multiple tabs and require selecting **Obtain an IP address automatically** on this tab and then going to the **DNS Configuration** tab to select **Obtain DNS server address automatically**.

If this computer was really being converted from static to DHCP, any entries in the **Gateway** and **WINS Configuration** tabs would need to be removed.

If the computer had Static addressing and it needs to be restored, click on the **Cancel** button.

To keep these settings click **OK**.



Older versions of Windows will say that it is necessary to restart the computer. Windows 2000 and XP typically do not require a restart.

Windows 95 might even ask for the installation CD-ROM to complete the process.

If the computer was really being changed over to DHCP, Step 3 would be repeated to confirm the valid set of configurations.

Reflection

Why might a network administrator prefer that various network profiles be used to hide the above options and screens, thereby preventing users from making any changes?

As a network administrator what would be some of the potential benefits of using a DHCP server within a network?

Note: Many small routers that are supplied for cable, DSL, or ISDN connections have DHCP configured by default. This allows additional computers to share the network connection through the use of a hub or switch. Each computer would need to be configured like in the lab. Typically, DHCP will assign addresses using one of the private networks, such as 192.168.1.0, that are set-aside for this purpose. While it is common to allow these settings to be changed, read and understand the instruction manual first. Learn where the **Reset Defaults** button is located.



Lab 9.3.7 Workstation ARP

Objective

- Introduce Address Resolution Protocol (ARP) and the `arp -a` workstation command.
- Explore the `arp` command help feature using the `-?` option.

Background / Preparation

ARP is used as a tool for confirming that a computer is successfully resolving network Layer 3 addresses to Media Access Control (MAC) Layer 2 addresses. The TCP/IP network protocol relies on IP addresses like 192.168.14.211 to identify individual devices and to assist in navigating data packets between networks. While the IP address is essential to move data from one LAN to another, it cannot deliver the data in the destination LAN by itself. Local network protocols, like Ethernet or Token Ring, use the MAC, or Layer 2, address to identify local devices and deliver all data. A computer MAC address has been seen in prior labs.

This is an example of a MAC address:

- **00-02-A5-9A-63-5C**

A MAC address is a 48-bit address displayed in Hexadecimal (HEX) format as six sets of two HEX characters separated by dashes. In this format each hex symbol represents 4 bits. With some devices, the 12 hex characters may be displayed as three sets of four characters separated by periods or colons (0002.A59A.635C).

ARP maintains a table in the computer of IP and MAC address combinations. In other words, it keeps track of which MAC address is associated with an IP address. If ARP does not know the MAC address of a local device, it issues a broadcast using the IP address. This broadcast searches for the MAC address that corresponds to the IP address. If the IP address is active on the LAN, it will send a reply from which ARP will extract the MAC address. ARP will then add the address combination to the local ARP table of the requesting computer.

MAC addresses and therefore ARP are only used within the LAN. When a computer prepares a packet for transmission, it checks the destination IP address to see if it is part of the local network. It does this by checking to see if the network portion of the IP address is the same as the local network. If it is, the ARP process is consulted to get the MAC address of the destination device using the IP address. The MAC address is then applied to the data packet and used for delivery.

If the destination IP address is not local, the computer will need the MAC address of the default gateway. The default gateway is the router interface that the local network is connected to in order to provide connectivity with other networks. The gateway MAC address is used because the packet will be delivered there and the router will then forward it to the network it is intended for.

If the computer does not receive any packets from an IP address after a few minutes, it will drop the MAC/IP entry from the ARP table assuming the device has logged off. Later attempts to access that IP address will cause ARP to do another broadcast and update the table.

This lab assumes the use of any version of Windows. This is a non-destructive lab and can be performed with a home machine without concern of changing the system configuration. Ideally, this lab will be done in a classroom or other LAN connected to the Internet. It can be done from a single remote connection via a modem or DSL-type connection.

Step 1 Establish a network connection

If the connection to the Internet is dial-up, connect to the ISP to ensure that the computer has an IP address. In a TCP/IP LAN with a Dynamic Host Configuration Protocol (DHCP) server it should not be necessary to do this step.

Step 2 Access a command prompt

Windows NT / 2000 / XP users:

Use the Start menu to open the Command Prompt window. This window is similar to the MS-DOS window on older Windows versions:

Start > Programs > Accessories > Command Prompt or Start > Programs > Command Prompt

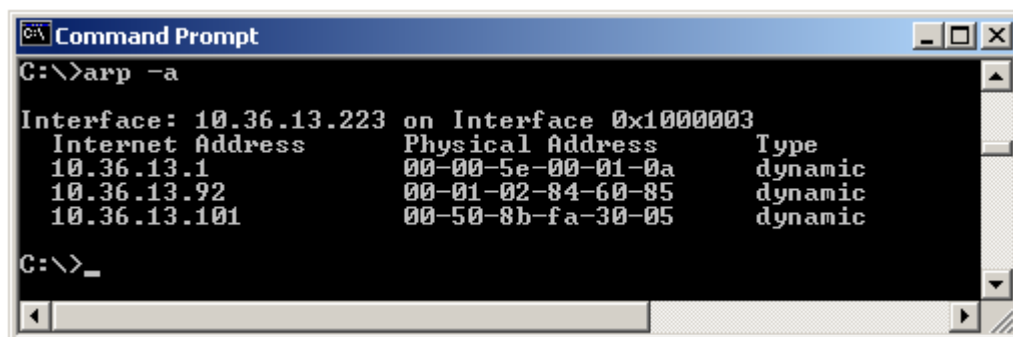
Windows 95 / 98 / ME users:

Use the Start menu to open the MS-DOS Prompt window:

Start > Programs > Accessories > MS-DOS Prompt or Start > Programs > MS-DOS Prompt

Step 3 Display the ARP table

- In the window type `arp -a` and press **Enter**. Do not be surprised if there are no entries. The message displayed will probably be, 'No ARP Entries Found'. Windows computers remove any addresses that are unused after a couple minutes.
- Try pinging a couple local addresses and a website URL. Then re-run the command. The figure below shows a possible result of the `arp -a` command. The MAC address for the website will be listed because it is not local, but that will cause the default gateway to be listed. In the example below 10.36.13.1 is the default gateway while the 10.36.13.92 and 10.36.13.101 are other network computers. Notice that for each IP address there is a physical address, or MAC, and type, indicating how the address was learned.
- From the figure below, it might be logically concluded that the network is 10.36.13.0 and the host computers are represented by 22, 1, 92, and 101.



Step 4 Ping several URLs

- Ping the following URLs and note the IP address of each. Also select one additional URL to ping and record it below:

www.cisco.com: _____

www.msn.de: _____

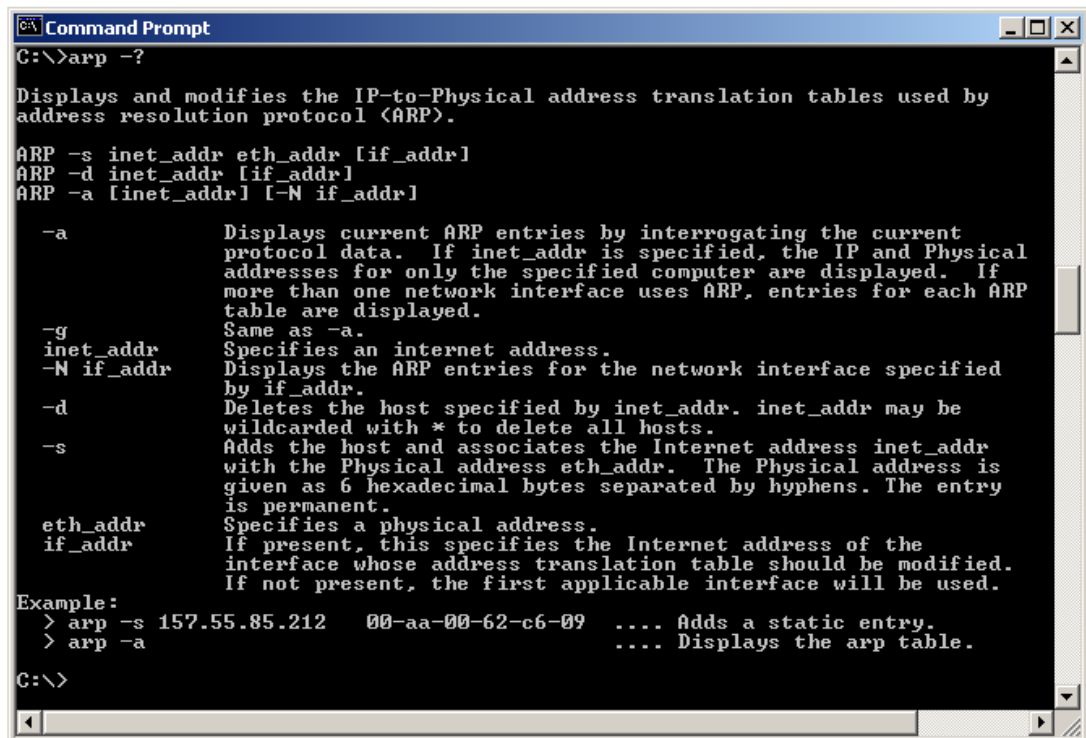
_____: _____

- Now run the `arp -a` command again and record the MAC addresses for each of the above next to their IP addresses. Can it be done? _____
- Why or why not? _____

- d. What MAC address was used in delivering each of the pings to the URLs? _____
_____ Why? _____

Step 4 Use the ARP help feature

Try the command `arp -?` to see the help feature and look over the options.



```
C:\>arp -?

Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a          Displays current ARP entries by interrogating the current
            protocol data. If inet_addr is specified, the IP and Physical
            addresses for only the specified computer are displayed. If
            more than one network interface uses ARP, entries for each ARP
            table are displayed.
-g          Same as -a.
            Specifies an internet address.
-N if_addr  Displays the ARP entries for the network interface specified
            by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
            wildcarded with * to delete all hosts.
-s          Adds the host and associates the Internet address inet_addr
            with the Physical address eth_addr. The Physical address is
            given as 6 hexadecimal bytes separated by hyphens. The entry
            is permanent.
eth_addr    Specifies a physical address.
if_addr     If present, this specifies the Internet address of the
            interface whose address translation table should be modified.
            If not present, the first applicable interface will be used.

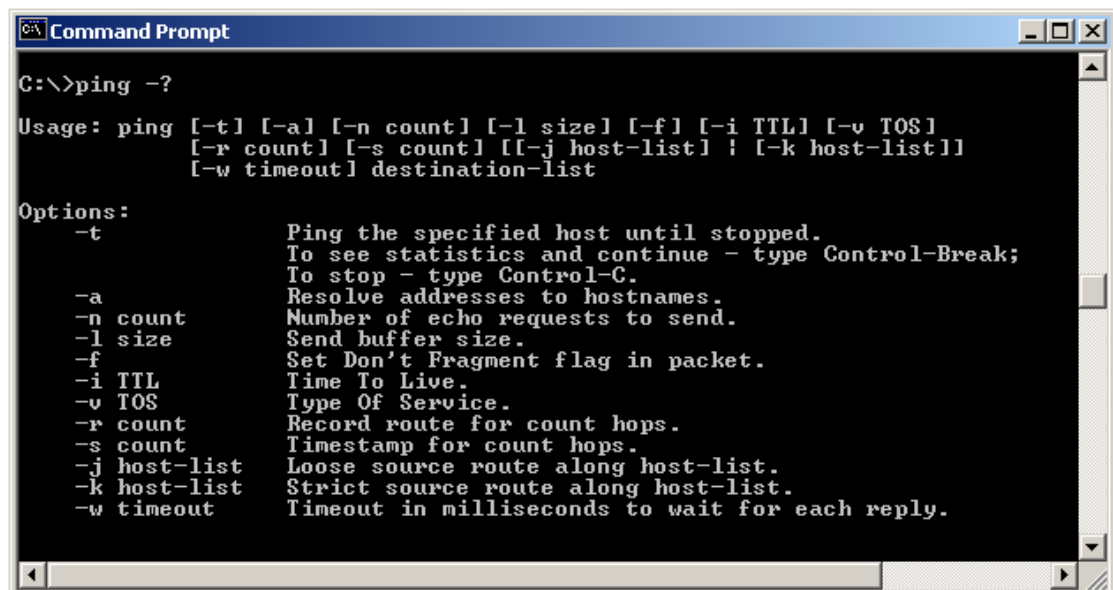
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a                                     .... Displays the arp table.

C:\>
```

The purpose of this step is not so much the ARP command options but to demonstrate using the `?` to access help, if available. Help is not always implemented uniformly. Some commands use `/?` instead of `-?`.

Step 5 Use help with tracert and ping

Try `tracert -?` and then `ping -?` to see the options available for the commands used previously.



```
C:\>ping -?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
           [-r count] [-s count] [[-j host-list] ! [-k host-list]]
           [-w timeout] destination-list

Options:
-t          Ping the specified host until stopped.
            To see statistics and continue - type Control-Break;
            To stop - type Control-C.
-a          Resolve addresses to hostnames.
-n count    Number of echo requests to send.
-l size     Send buffer size.
-f          Set Don't Fragment flag in packet.
-i TTL      Time To Live.
-v TOS      Type Of Service.
-r count    Record route for count hops.
-s count    Timestamp for count hops.
-j host-list Loose source route along host-list.
-k host-list Strict source route along host-list.
-w timeout  Timeout in milliseconds to wait for each reply.
```

In looking at the help for ping, notice the `-t` option, which will send continuous pings, not just four. More importantly, notice the two commands to stop it:

- **Control-Break**
- **Control-C**

These two-key commands are common for stopping runaway activities. Try pinging a neighboring computer with the `-t` option and then try the Control-Break and Control-C features. An example in the above network would be `ping 10.36.13.101 -t` and then press **Enter**.

Be sure to use the `Control-C` command to stop the pings.

Reflection

Based on observations made today, what could be deduced about the following results?

Computer 1

IP Address: 192.168.12.113

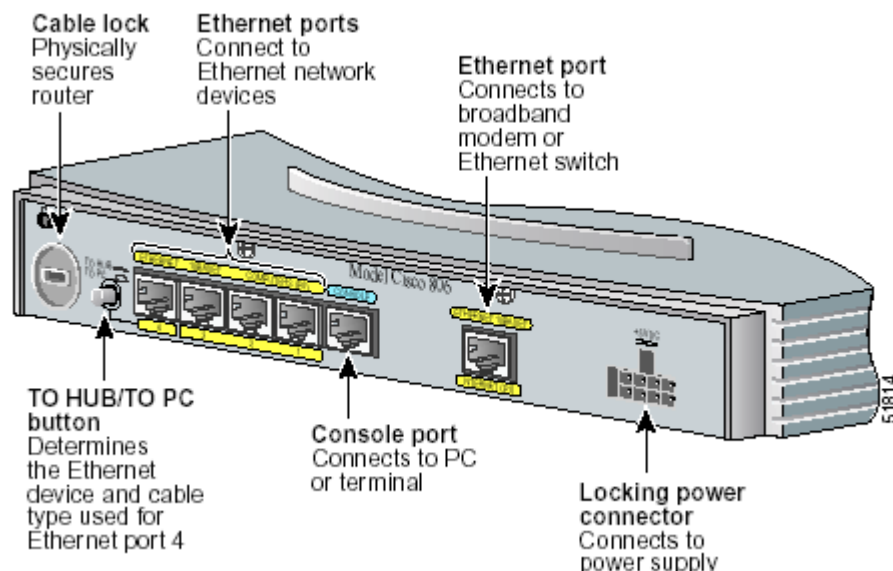
Subnet Mask: 255.255.255.0

Default Gateway: 192.168.12.1

Pings and tracert to 207.46.28.116 were both successful.

What will be the ARP table entry associated with this address and why?

Lab 10.2.9 Small Router Purchase



Objective

The purpose of this lab is to introduce the variety and prices of network components in the market. This lab will look specifically at small routers used by telecommuters when working from home. The lab will use the web site <http://www.cisco.com> but any local source, catalog, or website can be used.

Background / Preparation

Some company executives want more secure connections when working with cable and DSL connections from their homes. They have requested a proposal for purchasing small routers for this purpose. The assignment is to research at least two different solutions and develop a proposal. The project details are as follows:

- The company IT department is interested in reliability.
- There is concern about working with and supporting too many models of devices.
- The company uses Cisco routers throughout the corporate network.
- The company would like to be able to extend Cisco IOS features like Virtual Private Network (VPN) and firewall out to these remote users.

In talking to the executives and support personnel, it has become apparent that some of the personnel live in areas that do not support DSL or cable service. Models that might also support Integrated Services Digital Network (ISDN) connections must now also be looked into.

The requirements for the proposal include the following:

- 12 routers supporting DSL or cable connections
- 3 routers supporting ISDN connections
- All devices are to support the Cisco IOS features

Assume the service provider will supply any required modem device and that the router will connect to it via an Ethernet interface.

Several executives expressed an interest in being able to connect 2 or 3 computers to the same link. It is safe to assume this request will be made by most users.

Step 1 Research equipment pricing

Start by going to <http://www.cisco.com> and selecting **Products & Services** and following the links to **Routers** to gather basic information. Look specifically at the 700, 800, and small office, home office (SOHO) models.

Look at the Overview option, particularly any white papers, presentations, and brochures. These may provide useful data and graphics for the final presentation.

Use at least three other sources for technologies and pricing. If using Web searches, try <http://www.cdw.com>, <http://www.google.com>, or any other preferred search engine.

Step 2 Compile a one-page summary of your results

Use Microsoft Excel, Word, or any comparable products to compile a summary of the results. Include a short 8-15 line reason why this implementation was selected. Include a simple diagram showing the following:

- Router
- PCs
- Power cord
- Cable or DSL modem

Optional Step 2

Instead of creating the above Excel or Word documents, create a 4 to 8 slide PowerPoint presentation covering the same requirements.

Assume that the material will need to be presented.

If time allows, complete both step 2 and the optional presentation. This is a likely requirement for many jobs.



Lab 10.3.5a Basic Subnetting

Objective

- How to identify reasons to use a subnet mask
- How to distinguish between a default subnet mask and a custom subnet mask
- What given requirements determine the subnet mask, number of subnets, and hosts per subnet
- What needs to be understood about useable subnets and useable numbers of hosts
- How to use the ANDing process to determine if a destination IP address is local or remote
- How to identify valid and invalid IP host addresses based on a network number and subnet mask

Background / Preparation

This lab exercise focuses on the basics of IP subnet masks and their use with TCP/IP networks. The subnet mask can be used to split up an existing network into subnetworks, or subnets. Some of the primary reasons for subnetting are the following:

- Reduce the size of the broadcast domains, which creates smaller networks with less traffic
- Allow LANs in different geographical locations to communicate through routers
- Provide improved security by separating one LAN from another

Routers separate subnets, and determine when a packet can go from one subnet to another. Each router a packet goes through is considered a hop. Subnet masks help workstations, servers, and routers in an IP network determine if the destination host for the packet they want to send is on their own network or another network. This lab reviews the default subnet mask and then focuses on custom subnet masks. Custom subnet masks use more bits than the default subnet masks by borrowing these bits from the host portion of the IP address. This creates a three-part address:

- The original network address
- The subnet address made up of the bits borrowed
- The host address made up of the bits left after borrowing some for subnets

Step 1 Review the structure of IP addresses

If an organization has a Class A IP network address, the first octet, or 8 bits, is assigned and does not change. The organization can use the remaining 24 bits to define up to 16,777,214 hosts on its network. This is a lot of hosts. It is not possible to put all of these hosts on one physical network without separating them with routers and subnets.

It is common for a workstation to be on one network or subnet and a server to be on another. When the workstation needs to retrieve a file from the server it will need to use its subnet mask to determine the network or subnet that the server is on. The purpose of a subnet mask is to help hosts and routers determine the network location where a destination host can be found. Refer to the table below to review the following information:

- The IP address classes
- The default subnet masks

- The number of networks that can be created with each class of network address
- The number of hosts that can be created with each class of network address

Address Class	1 st Octet Decimal Range	1 st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126 *	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	11110	Experimental; used for research			

* Class A address 127 cannot be used and is reserved for loopback and diagnostic functions.

Step 2 Review the ANDing process

Hosts and routers use the ANDing process to determine if a destination host is on the same network or not. The ANDing process is done each time a host wants to send a packet to another host on an IP network. In order to connect to a server, the IP address of the server or the host name, such as, <http://www.cisco.com>, must be known. If the host name is used a Domain Name Server (DNS) will convert it to an IP address.

First, the source host will compare, or AND, its own IP address to its own subnet mask. The result of the ANDing is to identify the network where the source host resides. It will then compare the destination IP address to its own subnet mask. The result of the 2nd ANDing will be the network that the destination host is on. If the source network address and the destination network address are the same, they can communicate directly. If the results are different, they are on different networks or subnets. If this is the case, the source host and the destination host will need to communicate through routers or might not be able to communicate at all.

ANDing depends on the subnet mask. The subnet mask always uses all ones to represent the network, or network + subnet, portion of the IP address. A default subnet mask for a Class C network is 255.255.255.0 or 11111111.11111111.11111111.00000000. This is compared to the source IP address bit for bit. The first bit of the IP address is compared to the first bit of the subnet mask, the second bit to the second, and so on. If the two bits are both ones, the ANDing result is a one. If the two bits are a zero and a one, or two zeros, the ANDing result is a zero. Basically, this means that a combination of 2 ones results in a one, anything else is a zero. The result of the ANDing process is the identification of the network or subnet number that the source or destination address is on.

Step 3 Two Class C networks using the default subnet mask

This example shows how a Class C default subnet mask can be used to determine which network a host is on. A default subnet mask does not break an address into subnets. If the default subnet mask is used, the network is not being subnetted. Host X, the source on network 200.1.1.0 has an IP address of 200.1.1.5. It wants to send a packet to Host Z, the destination on network 200.1.2.0 and has an IP address of 200.1.2.8. All hosts on each network are connected to hubs or switches and

then to a router. Remember that with a Class C network address, the first 3 octets, or 24 bits, are assigned as the network address. So, these are two different Class C networks. This leaves one octet, or 8 bits for hosts, so each Class C network could have up to 254 hosts:

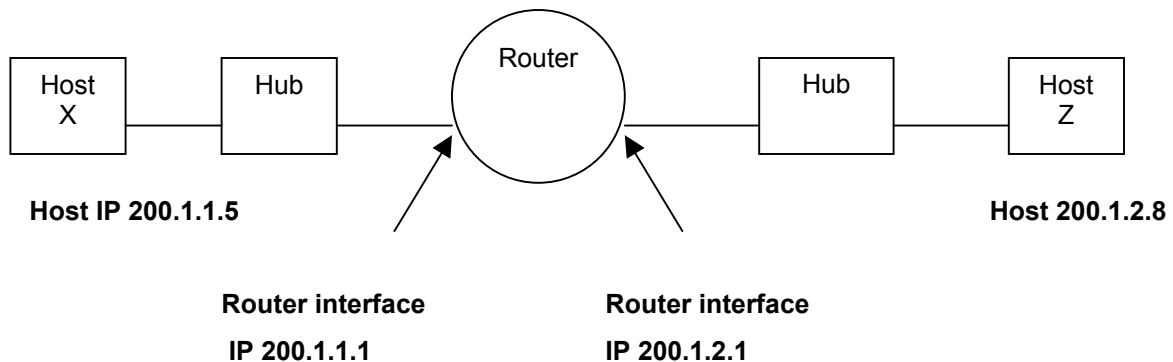
- $2^8 = 256 - 2 = 254$

Source net: 200.1.1.0

Destination net: 200.1.2.0

Subnet mask: 255.255.255.0

Subnet mask: 255.255.255.0



The ANDing process helps the packet get from Host 200.1.1.5 on network 200.1.1.0 to Host 200.1.2.8 on network 200.1.2.0 by using the following steps:

1. Host X compares its own IP address to its own subnet mask using the ANDing process.

Host X IP address 200.1.1.5	11001000.00000001.00000001.00000101
Subnet Mask 255.255.255.0	11111111.11111111.11111111.00000000
ANDing Result (200.1.1.0)	11001000.00000001.00000001.00000000

Note: The result of the ANDing process is the network address of Host X, which is 200.1.1.0.

2. Next, Host X compares the IP address of the Host Z destination to its own subnet mask using the ANDing process.

Host Z IP address 200.1.2.8	11001000.00000001.00000010.00001000
Subnet Mask 255.255.255.0	11111111.11111111.11111111.00000000
ANDing Result (200.1.2.0)	11001000.00000001.00000010.00000000

Note: The result of the ANDing process is the network address of Host Z, which is 200.1.2.0.

Host X compares the ANDing results from Step 1 and the ANDing results from Step 2, and notes they are different. Host X now knows that Host Z is not in its local-area network (LAN). Therefore, it must send the packet to its default gateway, which is the IP address of the router interface of 200.1.1.1 on network 200.1.1.0. The router then repeats the ANDing process to determine which router interface to send the packet out to.

Step 4 One Class C network with subnets using a custom subnet mask

This example uses a single Class C network address (200.1.1.0) and shows how a Class C custom subnet mask can be used to determine which subnetwork (or subnet) a host is on and to route packets from one subnetwork to another. Remember that with a Class C network address, the first 3 octets, or 24 bits are assigned as the network address. This leaves one octet, or 8 bits, for hosts. So, each Class C network could have up to 254 hosts:

- $2^8 = 256 - 2 = 254$

Perhaps less than 254 hosts, workstations and servers combined, are desired on one network. This could be for security reasons or to reduce traffic. It can be done by creating two subnetworks and separating them with a router. This will create smaller independent broadcast domains and can improve network performance and increase security. This is possible because these subnetworks will be separated by one or more router. Assume at least two subnetworks will be needed and that there will be at least 50 hosts per subnetwork. Because there is only one Class C network address, only 8 bits in the fourth octet are available for a total of 254 possible hosts. Therefore, a custom subnet mask must be created. The custom subnet mask will be used to borrow bits from the host portion of the address. The following steps help accomplish this:

1. The first step to subnetting is to determine how many subnets are needed. In this case, its two subnetworks. To see how many bits should be borrowed from the host portion of the network address, add the bit values from right to left until the total is equal to or greater than the number of subnets needed. Because two subnets are needed, add the one bit and the two bit, which equals three. This is greater than the number of subnets needed. To remedy this, borrow at least two bits from the host address starting from the left side of the octet that contains the host address.

Network address: 200.1.1.0

4th octet Host address bits:	1	1	1	1	1	1	1	1
Host address bit values (from right)	128	64	32	16	8	4	<u>2</u>	<u>1</u>

Add bits starting from the right side, the 1 and the 2, until the sum is greater than the number of subnets needed.

Note: An alternate way to calculate the number bits to be borrowed for subnets is to take the number of bits borrowed to the power of 2. The result must be greater than the number of subnets needed. As an example if 2 bits are borrowed the calculation is two to the second power, which equals four. Since the number of subnets needed is two this should be adequate.

2. After we know how many bits to borrow, we take them from the left side of the of the host address, the 4th octet. Every bit borrowed from the host address bit leaves fewer bits for the hosts. Even though the number of subnets is increased, the number of hosts per subnet is decreased. Because two bits need to be borrowed from the left side, that new value must be shown in the subnet mask. The existing default subnet mask was 255.255.255.0 and the new custom subnet mask is 255.255.255.192. The 192 results from adding the first two bits from the left, $128 + 64 = 192$. These bits now become 1s and are part of the overall subnet mask. This leaves 6 bits for host IP addresses or $2^6 = 64$ hosts per subnet.

4th Octet borrowed bits for subnet:	<u>1</u>	<u>1</u>	0	0	0	0	0	0
Subnet bit values: (from left side)	<u>128</u>	<u>64</u>	32	16	8	4	2	1

With this information, the following table can be built. The first two bits are the subnet binary value.

The last 6 bits are the host bits. By borrowing 2 bits from the 8 bits of the host address 4 subnets, 2^2 , with 64 hosts each, can be created. The 4 networks created are as follows:

- The 200.1.1.0 network
- The 200.1.1.64 network
- The 200.1.1.128 network
- The 200.1.1.192 network

The 200.1.1.0 network is considered unusable, unless the networking device supports the IOS command `ip subnet-zero`, which allows using the first subnet.

Subnet No.	Subnet Bits Borrowed Binary Value	Subnet Bits Decimal Value	Host Bits Possible Binary Values (Range) (6 Bits)	Subnet/Host Decimal Range	Useable?
0 Subnet	00	0	000000–111111	0–63	No
1 st Subnet	01	64	000000–111111	64–127	Yes
2 nd Subnet	10	128	000000–111111	128–191	Yes
3 rd Subnet	11	192	000000–111111	192–254	No

Notice that the first subnet always starts at 0 and, in this case, increases by 64, which is the number of hosts on each subnet. One way to determine the number of hosts on each subnet or the start of each subnet is to take the remaining host bits to the power of 2. Because we borrowed two of the 8 bits for subnets and have 6 bits left, the number of hosts per subnet is 2^6 or 64. Another way to figure the number of hosts per subnet or the increment from one subnet to the next is to subtract the subnet mask value in decimal, 192 in the fourth octet, from 256, which is the maximum number of possible combinations of 8 bits. This equals 64. This means start at 0 for the first network and add 64 for each additional subnetwork. For example, if the second subnet is used, the 200.1.1.64 network cannot be used for a host ID since the network ID of the 64 subnet has all zeros in the host portion.

Another common way to represent a subnet mask, is the use of the “slash/number” (/#) where the # following the slash is the number of bits used in the mask (network and subnet combined). As an example, a Class C network address such as 200.1.1.0 with a standard subnet mask (255.255.255.0) would be written as 200.1.1.0 /24, indicating that 24 bits are used for the mask. The same network, when subnetted by using two host bits for subnets, would be written as 200.1.1.0 /26. This indicates that 24 bits are used for the network and 2 bits for the subnet. This would represent a custom subnet mask of 255.255.255.192 in dotted decimal format.

A Class A network of 10.0.0.0 with a standard mask (255.0.0.0) would be written as 10.0.0.0 /8. If 8 bits (the next octet) were being used for subnets it would be written as 10.0.0.0 /16. This would represent a custom subnet mask of 255.255.0.0 in dotted decimal format. The “slash” number after the network number is an abbreviated method of indicating the subnet mask being used.

Step 5 Use the following information and the previous examples to answer the following subnet-related questions

A company has applied for and received a Class C network address of 197.15.22.0. The physical network is to be divided into 4 subnets, which will be interconnected by routers. At least 25 hosts will be needed per subnet. A Class C custom subnet mask needs to be used and a router is needed between the subnets to route packets from one subnet to another. Determine the number of bits that need to be borrowed from the host portion of the network address and the number of bits that will be left for host addresses.

Note: There will be 8 possible subnets, of which 6 can be used.

Fill in the following table and answer the following questions:

Subnet No.	Subnet Bits Borrowed Binary Value	Subnet Bits Decimal and Subnet No.	Host Bits Possible Binary Values (Range) (5 Bits)	Subnet/Host Decimal Range	Use?
0 Subnet					
1 st Subnet					
2 nd Subnet					
3 rd Subnet					
4 th Subnet					
5 th Subnet					
6 th Subnet					
7 th Subnet					

NOTES:

Use the table just developed to help answer the following questions:

- Which octet(s) represent the network portion of a Class C IP address? _____
- Which octet(s) represent the host portion of a Class C IP address? _____
- What is the binary equivalent of the Class C network address in the scenario? **197.15.22.0**
 Decimal network address: _____
 Binary network address: _____
- How many high-order bits were borrowed from the host bits in the fourth octet? _____
- What subnet mask must be used? Show the subnet mask in decimal and binary.
 Decimal subnet mask: _____
 Binary subnet mask: _____
- What is the maximum number of subnets that can be created with this subnet mask? _____
- What is the maximum number of useable subnets that can be created with this mask? _____
- How many bits were left in the fourth octet for host IDs? _____

9. How many hosts per subnet can be defined with this subnet mask? _____
10. What is the maximum number of hosts that can be defined for all subnets with this scenario?
Assume the lowest and highest subnet numbers and the lowest and highest host ID on each
subnet cannot be used. _____
11. Is 197.15.22.63 a valid host IP address with this scenario? _____
12. Why or why not? _____
13. Is 197.15.22.160 a valid host IP address with this scenario? _____
14. Why or why not? _____
15. Host A has an IP address of 197.15.22.126. Host B has an IP address of 197.15.22.129. Are
these hosts on the same subnet? _____ Why?



Lab 10.3.5b Subnetting a Class A Network

Objective

Analyze a Class A network address with the number of network bits specified in order to determine the following:

- Subnet mask
- Number of subnets
- Hosts per subnet
- Information about specific subnets

Background / Preparation

This is a written exercise and is to be performed without the aid of an electronic calculator.

Step 1 Given a Class A network address of 10.0.0.0 / 24 answer the following questions

How many bits were borrowed from the host portion of this address? _____

What is the subnet mask for this network?

1. Dotted decimal _____

2. Binary _____

How many usable subnetworks are there? _____

How many usable hosts are there per subnet? _____

What is the host range for usable subnet sixteen? _____

What is the network address for usable subnet sixteen? _____

What is the broadcast address for usable subnet sixteen? _____

What is the broadcast address for the last usable subnet? _____

What is the broadcast address for the major network? _____



Lab 10.3.5c Subnetting a Class B Network

Objective

The objective of this lab is to provide a subnetting scheme using a Class B network

Background / Preparation

This is a written lab and is to be performed without the aid of an electronic calculator.

ABC Manufacturing has acquired a Class B address, 172.16.0.0. The company needs to create a subnetting scheme to provide the following:

- 36 subnets with at least 100 hosts
- 24 subnets with at least 255 hosts
- 10 subnets with at least 50 hosts

It is not necessary to supply an address for the WAN connection since it is supplied by the Internet service provider.

Step 1 Given this Class B network address and these requirements answer the following questions

How many subnets are needed for this network? _____

What is the minimum number of bits that can be borrowed? _____

What is the subnet mask for this network? _____

1. Dotted decimal _____

2. Binary _____

3. Slash format _____

How many usable subnetworks are there? _____

How many usable hosts are there per subnet? _____

Step 2 Complete the following chart listing the first three subnets and the last 4 subnets

Subnetwork #	Subnetwork ID	Host Range	Broadcast ID

What is the host range for subnet two? _____

What is the broadcast address for the 126th subnet? _____

What is the broadcast address for the major network? _____



Lab 10.3.5d Subnetting a Class C Network

Objective

The objective of this lab is to provide a subnetting scheme using a Class C network.

Background / Preparation

This is a written exercise and is to be performed without the aid of an electronic calculator.

The Classical Academy has acquired a Class C address, 192.168.1.0. The academy needs to create subnets to provide low level security and broadcast control on the LAN. It is not necessary to supply an address for the WAN connection. It is supplied by the Internet service provider.

The LAN consists of the following, each of which will require its own subnet:

- Classroom #1 28 nodes
- Classroom #2 22 nodes
- Computer lab 30 nodes
- Instructors 12 nodes
- Administration 8 nodes

Step 1 Given this Class C network address and these requirements answer the following questions

How many subnets are needed for this network? _____

What is the subnet mask for this network?

1. Dotted decimal _____
2. Binary _____
3. Slash format _____

How many usable hosts are there per subnet? _____

Step 2 Complete the following chart

Subnetwork #	Subnetwork IP	Host Range	Broadcast ID

What is the host range for subnet six? _____

What is the broadcast address for the 3rd subnet? _____

What is the broadcast address for the major network? _____



Lab 11.2.4 Protocol Inspector, TCP, and HTTP

Objective

The objective of this lab is to use Protocol Inspector, or equivalent software, to view dynamic Transmission Control Protocol (TCP) operations. The operation that will be specifically looked at is HTTP during web page access.

Background / Preparation

Protocol analysis software has a feature called **capture**. This feature allows all frames through an interface to be captured for analysis. With this feature, it is possible to see how the TCP moves segments filled with user data across the network. TCP may seem to be a bit abstract, but the protocol analyzer shows just how important TCP is to network processes such as e-mail and web browsing.

At least one of the hosts must have the Protocol Inspector software installed. If the lab is done in pairs, having the software installed on both machines means that each person can run the lab steps. However, each host may display slightly different results.

Step 1 Start Protocol Inspector and your browser

Step 2 Go to detail view

Step 3 Start a capture

Step 4 Request a Web Page

Step 5 Watch the monitor view while the web page is requested and delivered

Step 6 Stop the capture

Step 7 Study the TCP frames, HTTP frames, and statistics using various views, especially the detail view

Step 8 Using the detail view, explain what evidence it provides about the following:

- TCP handshakes
- TCP acknowledgments
- TCP segmentation and segment size
- TCP sequence numbers
- TCP sliding windows
- HTTP protocol

Reflection

How did this lab help to visualize the TCP protocol in action?
