any cable that is not yellow is straight through
- yellow is straight through

CST8182 – NETWORKING FUNDAMENTALS 03-Lab

Learning Outcomes – At the end of this lab, you need to <u>understand:</u>

- ☐ Cable types and when/where to use them
- ☐ Creating a very small network (Peer-to-peer)
- ☐ Connecting to the internal & college networks
- ☐ Setting a static & DHCP IP address
- ☐ Releasing, renewing and verifying the IP address on the correct NIC
- ☐ Testing connectivity
- ☐ Capturing with Wireshark
- ☐ Reading a basic Wireshark capture

Lab connectivity information

Patch panel connections

- Blue (1st Jack): From PCs "Blue" add-on network card. This is the <u>NIC</u> you will use this semester.
- Green (2nd Jack): From PCs serial port. This is your console connection.
- ~~Black (3rd Jack): Unused in semester 1.~~

Cable types:

- You will be using 3 types of cables in the lab; **straight through, crossover, and console**.
- A straight through cable is used for connecting different types of devices (eg. PC to switch) (Often referred to as a patch cord)
- A crossover cable is used for connecting "like" devices (eg. PC to PC or PC to Router)
- A console cable is used to connect from a serial port on your PC to the console port of the router.

READ THE ENTIRE LAB BEFORE YOU START.

(Get the big picture)

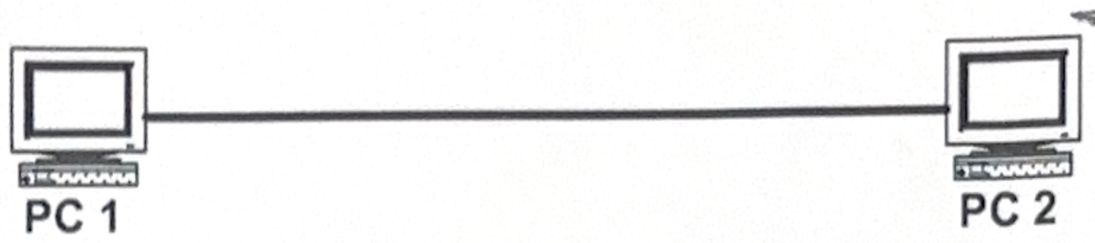
Task 0: Allow ICMP echo requests through the firewall.

- Referring to the "ICMP Firewall Rule.PDF" file, you can allow the ICMP packets be received by your lab PC or you can simply disable the Firewall (ask your lab prof to help you with this in case you need help).

go to windows defender and turn off firewall

Task 1: Create a peer-to-peer network of two PCs using static addressing

1.1 Working with your lab partner, use the correct cable to directly connect your PC to your partner's PC **at the patch panel**. Use the blue jacks. This is the smallest possible network; 2 PCs directly connected to each other.



Connect the disconnect the blue straight through cable from the switch connect the PC port on the patch panel to the partner pc port using yellow crossover

1.2 Assign a static IP address to each PC:

PC 1: 192.168.1.x (X= your workstation number) **PC 2**: 192.168.1.x (X= your workstation number)
Use a subnet mask of 255.255.255.0.
Do you need a default gateway this time? (No... Why not?)

Example: If PC 1 was station number T113-**09**, the IP address would be 192.168.1.**9**.
If PC 2 was station number T113-**10**, the IP address would be 192.168.1.**10**.

1.3 Test connectivity by using the **ping** command from a CMD prompt. Ping your partner's PC. (**ping 192.168.1.__**). Although testing from **both** directions is not truly necessary to prove connectivity, BOTH partners should ping the other.

Normal with regular permissions

NOTE: You should be able to successfully ping your partner. If you get a negative response, each partner should double-check the **other partner's settings**. If you don't find any problems with your partner's settings, try disabling the firewall (this is okay with the lab computers).

A successful ping will look **similar to** this, but the replies should be from your partner's IP address. Always pay attention to the "from" address.

Pinging 192.168.1.25 with 32 bytes of data:
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255
Reply from 192.168.1.25: bytes=32 time<1ms TTL=255

any cable that is not yellow is straight through
– yellow is straight through

CST8182 – NETWORKING FUNDAMENTALS 03-Lab

Learning Outcomes – At the end of this lab, you need to understand:

- ☐ Cable types and when/where to use them
- ☐ Creating a very small network (Peer-to-peer)
- ☐ Connecting to the internal & college networks
- ☐ Setting a static & DHCP IP address
- ☐ Releasing, renewing and verifying the IP address on the correct NIC
- ☐ Testing connectivity
- ☐ Capturing with Wireshark
- ☐ Reading a basic Wireshark capture

Lab connectivity information

Patch panel connections

- Blue (1st Jack): From PCs "Blue" add-on network card. This is the NIC you will use this semester.
- Green (2nd Jack): From PCs serial port. This is your console connection.
- ~~Black (3rd Jack): Unused in semester 1.~~

Cable types:

- You will be using 3 types of cables in the lab; **straight through, crossover, and console**.
- A straight through cable is used for connecting different types of devices (eg. PC to switch) (Often referred to as a patch cord)
- A crossover cable is used for connecting "like" devices (eg. PC to PC or PC to Router)
- A console cable is used to connect from a serial port on your PC to the console port of the router.

READ THE ENTIRE LAB BEFORE YOU START.

(Get the big picture)

Task 0: Allow ICMP echo requests through the firewall.

- Referring to the "ICMP Firewall Rule.PDF" file, you can allow the ICMP packets be received by your lab PC or you can simply disable the Firewall (ask your lab prof to help you with this in case you need help).

go to windows defender and turn off firewall

Collecting Results 1

Open **a word pad** application from your desktop and save it as "**03-Lab-{your username}.rtf**". Write "CHECKPOINT 1" and then copy the following screen capture under the CHECKPOINT 1 title:

☐ **SC1-** Take a screen capture of the output of the ping command.

Task 2: Use Wireshark to view network activity

2.1 **Start Wireshark and set it to capture packets from the "Blue" network interface card**. This is the card that is connected to the blue (left) jack in the patch panel.

NOTE: This is the proper sequence of events to get the capture:

1. Start the capture in Wireshark (On both PCs)
2. Ping your partner from the command prompt (Both partners) 3. Stop the capture in Wireshark when the ping is complete.

2.2 **On BOTH PCs**: Ping each other and then **stop the captures on both PCs when the ping is complete.** (EACH partner should have captured all the pings from both PCs)

2.2.1 Filter your capture for **icmp** and examine the output, noting the three windows, each one with increasing amounts of detail. (Note that Filters can be applied before, during, or after a Wireshark capture.)

2.2.2 Find **your** ping **in your Wireshark capture** and compare the output to the results of your ping in your Command (CMD) window. It should make sense!

NOTE: **Your** ping is the one where your IP address is in the Source column and your partner's IP is in the destination column.

2.2.3 Compare the output of your capture with the output of your partner's capture. Do you see any differences? (Look at the source and destination IP addresses)

2.2.4 What other traffic, if any, was captured by Wireshark? (Remove the filter and explore.) ARP Broadcast – WHO HAS 1250.13.1

2.2.5 Save the Wireshark capture to the desktop as "**03-Lab Task 2.2 ping.pcapng**".

any cable that is not yellow is straight through
- yellow is straight through

CST8182 – NETWORKING FUNDAMENTALS

03-Lab

Learning Outcomes – At the end of this lab, you need to <u>understand:</u>

- ☐ Cable types and when/where to use them
- ☐ Creating a very small network (Peer-to-peer)
- ☐ Connecting to the internal & college networks
- ☐ Setting a static & DHCP IP address
- ☐ Releasing, renewing and verifying the IP address on the correct NIC
- ☐ Testing connectivity
- ☐ Capturing with Wireshark
- ☐ Reading a basic Wireshark capture

Lab connectivity information

Patch panel connections

- Blue (1st Jack): From PCs "Blue" add-on network card. This is the <u>NIC</u> you will use this semester.
- Green (2nd Jack): From PCs serial port. This is your console connection.
- ~~Black (3rd Jack): Unused in semester 1.~~

Cable types:

- You will be using 3 types of cables in the lab; **straight through, crossover, and console**.
- A straight through cable is used for connecting different types of devices (eg. PC to switch) (Often referred to as a patch cord)
- A crossover cable is used for connecting "like" devices (eg. PC to PC or PC to Router)
- A console cable is used to connect from a serial port on your PC to the console port of the router.

READ THE ENTIRE LAB BEFORE YOU START.

(Get the big picture)

Task 0: Allow ICMP echo requests through the firewall.

- Referring to the "ICMP Firewall Rule.PDF" file, you can allow the ICMP packets be received by your lab PC or you can simply disable the Firewall (ask your lab prof to help you with this in case you need help).

go to windows defender and turn off firewall

NOTE: To open the Wireshark captures on your own laptop, you need to install Wireshark.
https://www.wireshark.org/download.html (**Accept all defaults when installing**)

Collecting Results 2

Into your "**03-Lab-{your username}.rtf**"file, write "CHECKPOINT 2" and then copy the following screen capture under the CHECKPOINT 2 title:

☐ **SC2-** Take a screen capture of ICMP echo request and replies and highlight the source and destination IP addresses.

Be prepared to identify and **EXPLAIN**:

The sending and receiving hosts. ○ **Your** ICMP echo request ○ The reply to **your** request

Based on the capture, who initiated the connectivity test? (**Who is the source of the request?)**

(Before you explain it to the professor, Practice by explaining this to your partner!)

Task 3: Connect to the Internal Lab Network using DHCP

3.1 Connect your PC using the correct cable type to the "S1-Central" switch. S1-Central should be connected to the Internal lab (yellow) network. What type of cable should you use? Is there an exception to this? straight through

Reminder: *You will not have connectivity while the link light is orange… You have a chance of connectivity when it turns green. This process can take as long as 50 seconds.*

3.2 Configure your PC to use DHCP (Dynamic Host Configuration Protocol). DNS should be set to DHCP as well. Be patient while attempting to obtain an address.

3.3 Confirm you have an IP address by opening a CMD prompt and typing **ipconfig**. (Have you written this in your lab journal yet?) Locate **the correct NIC** (Network Interface Card) to determine which network you are connected to. You can tell based on the IP address you receive form a DHCP server;

In T113, the college network (Red):

10.50.13.x College services, Internet access, lab printer access
red internet access

In T113, the "Internal" network (Yellow):

Collecting Results 1

Open a word pad application from your desktop and save it as "03-Lab-{your username}.rtf". Write "CHECKPOINT 1" and then copy the following screen capture under the CHECKPOINT 1 title:

☐ SC1- Take a screen capture of the output of the ping command.

Task 2: Use Wireshark to view network activity

2.1 **Start Wireshark and set it to capture packets from the "Blue" network interface card.** This is the card that is connected to the blue (left) jack in the patch panel.

NOTE: This is the proper sequence of events to get the capture:

1. Start the capture in Wireshark (On both PCs)
2. Ping your partner from the command prompt (Both partners) 3. Stop the capture in Wireshark when the ping is complete.

2.2 **On BOTH PCs:** Ping each other and then **stop the captures on both PCs when the ping is complete.** (EACH partner should have captured all the pings from both PCs)

2.2.1 Filter your capture for **icmp** and examine the output, noting the three windows, each one with increasing amounts of detail. (Note that Filters can be applied before, during, or after a Wireshark capture.)

2.2.2 Find **your** ping **in your Wireshark capture** and compare the output to the results of your ping in your Command (CMD) window. It should make sense!

NOTE: **Your** ping is the one where your IP address is in the Source column and your partner's IP is in the destination column.

2.2.3 Compare the output of your capture with the output of your partner's capture. Do you see any differences? (Look at the source and destination IP addresses)

2.2.4 What other traffic, if any, was captured by Wireshark? (Remove the filter and explore.) ARP Broadcast – Who has 10.50.13.1

2.2.5 Save the Wireshark capture to the desktop as "**03-Lab Task 2.2 ping.pcapng**".

172.16.254.x Internal lab network only

No DHCP server responding: 169.x.x.x Nowhere! (Check your connections)

3.3.1 To be sure you are on the correct network, use the following series of commands:

ipconfig /release	(This clears your DHCP IP address)
ipconfig /renew	(This requests an new IP address from the DHCP server)
ipconfig	To re-verify your IP address (ALWAYS VERIFY!!!)

Once you have verified that you are indeed connected to the internal network, move on to 3.4.

NOTE: You should verify that you have reachability to the Eagle-server by pinging it: "ping eagle-server.example.com".

3.4 **Start a new Wireshark capture.**

DO NOT open the webpage before starting the next capture.

Not even to test the link.

You **MUST** start the capture **before** opening the web page.

3.4.1 **With your Wireshark capture running,** open the Chrome web browser and connect to http://eagle-server.example.com . Leave your Wireshark capture running for at least 75 seconds and then stop the capture.

Suggestion: Type the URL in notepad. Check it for typos and then copy/paste.

3.5 Examine the output. How many different protocols can you identify? What are their names? Do **all** protocols use an IP address?

3.6 Save your Wireshark capture as "**03-Lab Task 3.4.pcapng**".

3.7 As you did for ICMP earlier, you can use a filter to help isolate certain packets. The basic protocol used by web browsers is usually HTTP, so use **http** as your filter this time.

172.16.254.x Internal lab network only

No DHCP server responding: 169.x.x.x Nowhere! (Check your connections)

3.3.1 To be sure you are on the correct network, use the following series of commands:

ipconfig /release	(This clears your DHCP IP address)
ipconfig /renew	(This requests an new IP address from the DHCP server)
ipconfig	To re-verify your IP address (ALWAYS VERIFY!!!)

Once you have verified that you are indeed connected to the internal network, move on to 3.4.

NOTE: You should verify that you have reachability to the Eagle-server by pinging it:
"ping eagle-server.example.com".

3.4 **Start a new Wireshark capture.**

DO NOT open the webpage before starting the next capture.

Not even to test the link.

You **MUST** start the capture **before** opening the web page.

3.4.1 **With your Wireshark capture running**, open the Chrome web browser and connect to http://eagle-server.example.com . Leave your Wireshark capture running for at least 75 seconds and then stop the capture.

Suggestion: Type the URL in notepad. Check it for typos and then copy/paste.

3.5 Examine the output. How many different protocols can you identify? What are their names? Do **all** protocols use an IP address?

3.6 Save your Wireshark capture as "**03-Lab Task 3.4.pcapng**".

3.7 As you did for ICMP earlier, you can use a filter to help isolate certain packets. The basic protocol used by web browsers is usually HTTP, so use **http** as your filter this time.

Collecting Results 3

Into your "**03-Lab-{your username}.rtf**", write "CHECKPOINT 3" and then copy the following screen capture under the CHECKPOINT 3 title:

☐ **SC3-**Take a screen capture of your wireshark capture, highlighting **1.** your initial connection to the Eagle server. Hint: Filter for http and look at the info column. You are trying to **GET** a web page. 2. Your IP address 3. Eagle-Server's IP address in the Wireshark capture

Talk to your partner before your demo! Explain it to each other before trying to explain it to the professor.

DEMO your three screen captures to your lab instructor

At this step you must have three screen captures inserted into your word file as well as two wireshark captures. If you are confident everything is correct, demo it to your lab instructor. Not demoing your files will result in Mark 0.

Clean up and Post-lab

- You should always save all your results. At the end of the semester, you should have saved all the work that you did throughout the semester.

- Reboot your computer. The PCs in the lab are running DeepFreeze. All of your information, settings, logins, etc. are deleted when you reboot the PC.

- Make sure that the network wiring for your station (and your partner's station) is back to its default configuration. The short blue patch cord (aka. straight through cable) should be connected from your stations blue patch panel connector to the S1 Central switch. The S1 Central switch should be connected to the college (red) network. Put borrowed cables neatly back in the cabinet.

- Leave your workstation clean and organized. That includes pushing in the chair. In other words, leave it the way that you would like to find it.