Lab 1: Physical Layer and Ethernet Overview

CNIT34400-006
Group 30
Abbie Docter
William Park
Submitted To: Royden Butterfield
Date Submitted: 2/17/2022
Date Due: 2/17/2022

PROCEDURES

This section includes steps to recreate what was achieved in the previous few weeks. In this report, buttons are bolded, options are italicized, text entered into the computer is in the Courier New font, and menu navigation is notated by the pipe symbol.

Connected switches to workstations

The switches were factory reset to remove any previous configuration that had been done on them. Afterwards they were connected to the PC's via cabling.

1. Located **Mode** button on switch
2. Held down button until lights flashed green
3. Waited until switch booted up
4. Connected switch ports 1, 2, and 3 to patch panel 1 ports 7, 8, and 9 respectively
5. Connected patch panel 1 ports 7, 8, and 9 to the yellow connections for bench 18 on the cross connect
6. Connected switch console ports to patch panel 2 ports 7, 8, and 9
7. Connected patch panel 2 ports 7, 8, and 9 to the red connections for bench 18 on the cross connect

Configured IP & DNS settings on workstations

Manually setting the IP and DNS settings on the workstations was imperative for setting up a proper Local Area Network.

1. Opened Control Panel

2. Navigated to *Network and Internet* | *Network and Sharing Center*
3. Clicked on **Ethernet 2**
4. Set IP and DNS settings according to Table 1

Table 1: IP and DNS settings for workstations

IP	Subnet	Gateway	DNS
10.25.30.1*	255.255.255.0	10.25.30.1	10.2.1.11, 10.2.1.12

   a. *Different workstations had different digits

5. Clicked **OK**

Connected workstations to lab printer

The workstations were connected to the printer in order to facilitate printing while in lab.

1. Opened Control Panel
2. Navigated to *Hardware and Sound* | *Devices and Printers* | *Add a Printer*
3. Selected **The printer that I want isn't listed**
4. Toggled *Add a printer using a TCP/IP address or hostname*
5. Entered `10.3.1.206` for the printer IP address
6. Selected **Generic Printer** for printer categories
7. selected **Do not share printer**

Set up file sharing

A file share was created between the two Windows workstations to facilitate network testing.

1. Opened File Explorer on Windows 10

2. Created new folder to share
3. Right clicked the folder and selected **Properties**
4. Navigated to the *Sharing* tab and clicked **Share**
5. Entered *Everyone*, and then clicked **Add**
6. Set *Read/Write* for Permission Level on Everyone
7. Clicked **Share**
8. Confirmed the folder's network path
9. Clicked **Close**
10. Opened file explorer on second Windows 10 machine
11. Navigated to *This PC* | *Computer* | *Map Network Drive*
12. Entered the folder's network path into the Folder box and selected **Finish**

Configured switch passwords

The switches were configured to require passwords upon login and entering enabled mode.

1. Opened PuTTY on workstation
2. Changed option to *Serial* and clicked **OK**
3. Waited until switch responded
4. Typed in `enable` command and pressed **Enter** to enter enable mode
5. Typed in `configure terminal` and pressed **Enter** to enter configuration mode
6. Typed `enable secret` followed by desired enable password and pressed **Enter**
7. Issued `service password-encryption` command to turn on password encryption
8. Typed in `line console 0` to enter line console configuration and pressed **Enter**

9. Typed `password` followed by desired login password and pressed **Enter**
10. Typed `login` and pressed **Enter**
11. Exited out of line console configuration

Analyzed packets using Wireshark

Wireshark was utilized to determine the types of protocols used for file sharing services.

1. Opened Wireshark on workstation
2. Selected ethernet connection
3. Pressed the blue shark fin button to start capturing packets
4. Sent file through file share
5. Pressed the red button to stop capturing packets
6. Analyzed packets to determine protocols in use
    a. Analysis included in Appendix A

Configured SPAN

SPAN allowed for forwarding of traffic from one switch port to another. It essentially allowed one workstation to monitor network traffic from another workstation.

1. Opened PuTTY on Windows workstation
2. Changed option to *Serial* and clicked **OK**
3. Logged into switch and entered configuration mode
4. Typed `monitor session 1 source interface GigabitEthernet 1/0/1` and hit **Enter**

5. Typed `monitor session 1 destination interface GigabitEthernet 1/0/9` and hit **Enter**
6. Exited configuration mode
7. Typed `show monitor session 1` to confirm SPAN settings
8. Opened Wireshark on Ubuntu workstation and began monitoring traffic
9. Generated network traffic on Windows workstation
10. Verified traffic showed up in Wireshark on Ubuntu machine
11. Re-entered configuration mode on switch
12. Stopped SPAN session by typing `no monitor session 1`

Configured full network architecture

Once all of the switches and workstations had their basic configurations, the rest of the switches were added into the network topology.

1. Connected port 1 of the top Cisco switch to port 1 of the HP/Aruba switch
2. Connected port 2 the HP/Aruba switch to port 2 of the bottom Cisco switch
3. Connected patch panel 1 port 7 to port 3 of the top Cisco switch
4. Connected patch panel 1 port 8 to port 3 of the HP/Aruba switch
5. Connected patch panel 1 port 9 to port 3 of the bottom Cisco switch

Analyzed duplex settings

The duplex settings were tested and analyzed to determine which setting would be the most efficient for the network.

1. Opened command prompt on Windows workstation
2. Entered the following commands to create 1MB and 100MB files:
    a. `fsutil file createnew test1.txt 1000000`
    b. `fsutil file createnew test1.txt 100000000`
3. Opened Control Panel
4. Navigated to *Network and Internet* | *Network & Sharing Center*
5. Right clicked on **Ethernet**
6. Selected **Properties**
7. Selected **Configure** and navigated to *Advanced* tab
8. Navigated to *Speed & Duplex* from list
9. For each duplex option in the dropdown, performed the following:
    a. Moved the files to shared folder between Windows hosts
    b. Recorded the time it took for files to transmit into Table 2
    c. Uploaded the files to Google Drive
    d. Recorded the time it took for files to transmit into Table 3
    e. Deleted the files from the shared folder and Google Drive

Table 2: Transfer Times Between Two Hosts

	Calculated Time (100MB)	Actual Time (100MB) Wireshark	Calculated Time (1MB)	Actual Time (1MB) Wireshark	Explanation for the Difference
100 Mbps full-duplex	8 sec	9.83 sec	0.08 sec	0.02 sec	
100 Mbps half-duplex	16 sec	11 sec	0.16 sec	0.15 sec	

10 Mbps full-duplex	1 min 15 sec	1 min 29 sec	0.8 sec	1.09 sec	
10 Mbps half-duplex	2 min 30 sec	1 min 44 sec	1.6 sec	2.43 sec	

Table 3: Transfer Times Between a Host and an Internet Server

	Calculated Time (100MB)	Actual Time (100MB) Wireshark	Calculated Time (1MB)	Actual Time (1MB) Wireshark	Explanation for the Difference
100 Mbps full-duplex	8 sec	10 sec	0.08 sec	0.38 sec	
100 Mbps half-duplex	16 sec	10 sec	0.16 sec	0.32 sec	
10 Mbps full-duplex	1 min 20 sec	1 min 31 sec	0.8 sec	1.28 sec	
10 Mbps half-duplex	2 min 30 sec	1 min 51 sec	1.6 sec	1.68 sec	

Changed MAC address

The MAC address for one of the workstations was changed in order to see how such a change affected the network.

1. Opened registry editor
2. Navigated to

   Computer\HKEY_LOCAL_MACHINE\CurrentControlSet\Control\Class\{4d36e972-E325-1ce-bfc1-08002be10318}\0001
3. Right clicked in the main section and selected **New**

4. Set the data values to be a string
5. Named new data value `NetworkAddress`
6. Set the data to be `001122334455`

Analyzed ethernet frame transmission

Wireshark was utilized to analyze the rate of ethernet frame transmissions and how often frames had to be re-sent over the network.

1. Opened command prompt on Host A
2. Created large file by issuing `fsutil file createnew largefile.txt 804637000` command
3. Placed large file into file share
4. Opened Wireshark on Host B and started capturing frames
5. Downloaded large file onto Host B
6. Stopped capturing packets in Wireshark
7. Analyzed packets to determine number of frames sent over the network
    a. Analysis included in Appendix A

BIBLIOGRAPHY

Cisco. (2016, October 18). Catalyst 2960 and 2960-S Software Configuration Guide, 12.2(55)Se - configuring span and RSPAN [Cisco Catalyst 2960 series switches]. Cisco. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swspan.html#29138

Cisco. (2021, November 1). Access the CLI via putty using a console connection on 300 and 500 series managed switches. Cisco. Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb4984-access-the-cli-via-putty-using-a-console-connection-on-300-a.html

Configuring span on Cisco Catalyst Switches - Monitor and Capture Network Traffic/Packets. (n.d.). Retrieved from https://www.firewall.cx/cisco-technical-knowledgebase/cisco-switches/940-cisco-switches-span-monitoring.html

How to configure Cisco Switches - a step by Step Guide. Comparitech. (2021, April 7). Retrieved from https://www.comparitech.com/net-admin/configure-cisco-switches/

Jorgenson, Wyatt. (2019, March 5). Making a straight-through cable. Instructables. Retrieved from https://www.instructables.com/Making-a-Straight-Through-Cable/

MicroNugget: How to configure span and RSPAN on ... - youtube. (n.d.). Retrieved from https://www.youtube.com/watch?v=GyDpkVoix00

PittNet Wired: Configuring Windows 10 for Wired Publicly Accessible Network Ports | University of Pittsburgh. (2019, August 8). Retrieved from https://www.technology.pitt.edu/help-desk/how-to-documents/pittnetwired-configuring-windows-10-wired-publicly-accessible-network#:~:text=Right%2Dclick%20on%20Ethernet%20and,Duplex%20or%20just%20Speed%20%26%20Duplex

Rendek, L. (2021, November 11). *Ubuntu static IP configuration*. Linux Tutorials - Learn Linux Configuration. Retrieved from https://linuxconfig.org/how-to-configure-static-ip-address-on-ubuntu-18-10-cosmic-cuttlefish-linux#:~:text=Ubuntu%20Desktop,-The%20simplest%20approach&text=Click%20on%20the%20top%20right,netmask%2C%20gateway%20and%20DNS%20settings

Stanojevic, Milan. (2021, March 25). How to change your mac address in windows 10 [full guide]. Windows Report - Error-free Tech Life. Retrieved from https://windowsreport.com/mac-address-changer-windows-10/

Show mac address-table interface . Home - Cisco Community. (2020, July 20). Retrieved from https://community.cisco.com/t5/switching/show-mac-address-table-interface-lt-interface-range-gt/td-p/2955998

Other references:

The TA's, especially Royden and Sam

Professor Deadman

Windows 10

Ubuntu

Wireshark

PuTTY

Cisco switches

HP/Aruba switch

APPENDIX A: ANSWERS TO LAB QUESTIONS

This section answers questions asked throughout the lab assignment.

Switch console access

Table 4: MAC table for top Cisco switch

Vlan	Mac Address	Type	Ports
All	0100.0ccc.cccc	STATIC	CPU
All	0100.0ccc.cccd	STATIC	CPU
All	0180.c200.0000	STATIC	CPU
All	0180.c200.0001	STATIC	CPU
All	0180.c200.0002	STATIC	CPU
All	0180.c200.0003	STATIC	CPU
All	0180.c200.0004	STATIC	CPU
All	0180.c200.0005	STATIC	CPU
All	0180.c200.0006	STATIC	CPU
All	0180.c200.0007	STATIC	CPU
All	0180.c200.0008	STATIC	CPU
All	0180.c200.0009	STATIC	CPU
All	0180.c200.000a	STATIC	CPU
All	0180.c200.000b	STATIC	CPU
All	0180.c200.000c	STATIC	CPU
All	0180.c200.000d	STATIC	CPU
All	0180.c200.000e	STATIC	CPU
All	0180.c200.000f	STATIC	CPU
All	0180.c200.0010	STATIC	CPU

All	ffff.ffff.ffff	STATIC	CPU
1	0027.0c05.fe11	DYNAMIC	Gi1/0/48
1	d0d0.fdfe.537f	DYNAMIC	Gi1/0/48

Startup configuration is the configuration that a switch boots into. Running configuration is the current configuration of the switch.

Only 1 VLAN is configured and assigned.

Packet analysis

What layers of the OSI model are involved in file sharing across the network?

What protocols were involved during file sharing process in the LAN environment?

Use one packet as an example to explain the how TCP/IP layered architecture and the encapsulation processed

If someone were only given the captured packets, are they able to reassemble the file transmitted? Use the captured packets to support your answer.

Cable construction

What are the physical layer characteristics of the cables you have constructed?

Evaluate the physical layer characteristics and resulting data rates of each type of ISO/IEC 11801:2002 standards for “Category” cable.

What is the correct term for each of the cables you constructed? That is, why should the cables not be called “Ethernet cables”?

Cable applications

What kinds of connections typically use straight-through cables, crossover cables, and rollover cables?

- The straight-through cables would use same order of the T-568B. Crossover cables used T-568B on one side while using T-568A on other side. Rollover uses RS-232 connectors that are used on printer and computers.

Use a crossover cable that you construct to directly connect two PCs (no switches and do not unplug the wiring from the back of the computers – use the cross-connects in Knoy 203 to make the connection) and configure the lab computers such that files can be shared between computers. What IP addresses and network mask were used? Does a default gateway need to be configured?

Cable analysis & evaluation

Use a modular tester to troubleshoot a series of potentially "broken" cables

Assuming these are cables constructed using the TIA-568B standard, what must be done to repair each of these cables?

Assuming these are cables constructed using the ISOC standard, what must be done to repair each of these cables?

Why will a rollover cable not be sufficient for transmission of data over an Ethernet-based network?

Ethernet frame analysis

Calculate the number of Ethernet frames required to transfer of this file based on the standard payload size of Ethernet frames (assuming no errors occur in transmission)

Calculated was 804,637 KB * 1024 bytes/KB / 1518 bytes/frame = about 542,785 frames.

Is this the actual number of frames that were transmitted? Explain.

Wireshark showed 597,069 frames. Some got dropped during transmission.

Track the number of errored/retransmitted frames that occurred during this transfer. Explain the potential cause(s).