Lab 2: Wireless and Enterprise Routers

CNIT34400-006
Group 30
Abbie Docter
William Park
Submitted To: Royden Butterfield
Date Submitted: 3/10/2022
Date Due: 3/10/2022

TABLE OF CONTENTS

PROCEDURES 2
Set up Phase I architecture 2
Created new users in VyOS 3
Configured WAN Ethernet interface on VyOS 3
Configured WLAN interface on VyOS 4
Configured DHCP for wireless network 4
Configured NAT for wireless network 5
Configured VLANs on VyOS 6
Configured DHCP for VLANs on VyOS 9
Configured DNS for VLANs on VyOS 11
Configured NAT for VLANs on VyOS 12
Configured SSH access on VyOS 13
Configured SSH access on Cisco switches 14
Configured SSH access on HP/Aruba switch 15
Configured IIS website with port forwarding 15
Disabled wireless access point 16
Set up Phase II architecture 16
Configured WAN Ethernet interface on Cisco router 17
Configured sub-interfaces on Cisco router 17
Configured DHCP for VLANs on Cisco router 18
Configured NAT for VLANs on Cisco router 19
Configured SSH access on Cisco router 20
Analyzed VLAN traffic using Wireshark 20

RESULTS 22

BIBLIOGRAPHY 26

APPENDIX A: ANSWERS TO LAB QUESTIONS 28
Traffic monitoring 28
802.1Q frame tags 28

APPENDIX B: CONFIGURATION FILES 30
Cisco switches 30
HP/Aruba switch 39
VyOS router 41
Cisco router 48

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 underlined and menu navigation is notated by the pipe symbol (|).

Set up Phase I architecture

The Phase I architecture included three switches, three PC's, and a VyOS router.

1. Connected VyOS port 0 to CIT network via gray uplink cable
2. Connected VyOS port 1 to top Cisco switch port 37
3. Connected top Cisco switch port 40 to bottom Cisco switch port 40
4. Connected top Cisco switch port 42 to HP switch port 22
5. Connected top Cisco switch port 1 to Patch Panel 1 port 7
6. Connected bottom Cisco switch port 1 to Patch Panel 1 port 8
7. Connected HP switch port 1 to Patch Panel 1 port 9
8. Connected VyOS console port to Patch Panel 2 port 7
9. Connected top Cisco switch console port to Patch Panel 2 port 8
10. Connected HP switch console port to Patch Panel 2 port 9
11. Connected PC1 to Patch Panel 1 port 7
12. Connected PC2 to Patch Panel 1 port 8
13. Connected PC3 to Patch Panel 1 port 9

Created new users in VyOS

New usernames and passwords were created in VyOS to allow for access control and SSH access.

1. Pressed **Windows** key and typed in PuTTY to open application
2. Entered a speed of 115200 and clicked **Open** to connect to VyOS device
3. Logged into VyOS device using default username of vyos and default password of CNIT344-240
4. Utilized the adduser [username] command to add new users
    a. Created two users: adocter and park
5. Typed configure to enter configuration mode
6. Entered the following command to set passwords, once for each user:
    a. set system login user [username] authentication plaintext-password [password]
7. Typed commit and save commands to save configuration

Configured WAN Ethernet interface on VyOS

The uplink port was configured as a WAN interface to connect to the cit.lcl network.

1. Typed configure to enter configuration mode
2. Typed set interfaces ethernet eth0 address 10.25.30.254/24 to set IP and subnet
3. Typed set protocols static route 0.0.0.0/0 next-hop 10.25.30.1 to set default gateway
4. Entered commit and save commands to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured WLAN interface on VyOS

A WLAN interface was configured to host a wireless network.

1. Typed configure to enter configuration mode
2. Entered set interfaces wireless wlan0 address 172.16.30.1/24 to set IP and subnet
3. Entered set interfaces wireless wlan0 description 'Group 30 Wireless Network' to set description
4. Entered set interfaces wireless wlan0 channel 1 to specify a 2.4Ghz channel
5. Entered set interfaces wireless wlan0 mode g to specify a protocol/mode
6. Entered set interfaces wireless wlan0 type access-point to set interface as a wireless access point
7. Entered set interfaces wireless wlan0 ssid 'c240-344g30' to set the ID/name
8. Entered set interfaces wireless wlan0 security wpa mode wpa2 to set the security protocol
9. Entered set interfaces wireless wlan0 wpa passphrase [password] to set the password
10. Entered set interfaces wireless wlan0 country-code us to set the country code
11. Issued commit and save commands to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured DHCP for wireless network

DHCP was configured to automatically assign IP addresses to any devices that connect to the wireless network.

1. Typed configure to enter configuration mode
2. Entered set service dhcp-server shared-network-name YOLO subnet 172.16.30.0/24 default-router 172.16.30.1 to set default gateway

3. Entered set service dhcp-server shared-network-name YOLO subnet 172.16.30.0/24 name-server 10.2.1.11 to set DNS server
4. Entered set service dhcp-server shared-network-name YOLO subnet 172.16.30.0/24 range 0 start 172.16.30.100 to set the start of the range of acceptable addresses
5. Entered set service dhcp-server shared-network-name YOLO subnet 172.16.30.0/24 range 0 stop 172.16.30.200 to set the end of the range of acceptable addresses
6. Entered set service dns forwarding listen-address 172.16.30.1 to set address to listen for DNS requests
7. Entered set service dns forwarding allow-from 172.16.30.0/24 to specify addresses to allow DNS requests from
8. Entered set service dns forwarding dhcp wlan0 to specify WLAN interface to apply DNS settings to
9. Entered commit and save commands to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured NAT for wireless network

NAT was configured to allow the devices connected to the wireless network to connect to the Internet. This would be impossible without NAT due to 172.16.0.0/16 addresses being reserved for private IP addressing. The addresses needed to be translated in order to be allowed to connect to the Internet.

1. Typed configure to enter configuration mode
2. Typed set nat source rule 10 source address 172.16.30.0/24 to set the range of addresses to translate

Wireless and Enterprise Routers

3. Typed set nat source rule 10 outbound-interface eth0 to specify which interface the traffic would leave from
4. Typed set nat source rule 10 translation address ‘masquerade’ to allow the router to choose what IP addresses to translate to
5. Entered commit and save commands to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured VLANs on VyOS

VLANs were configured on the VyOS device to create further segmentation of the network, allowing for more granular management of the network while still letting devices in different VLANs communicate with each other.

1. Typed configure to enter configuration mode
2. Entered set interfaces ethernet eth1 vif 30 description ‘VLAN 30’ to create VLAN 30 and set its description
3. Entered set interfaces ethernet eth1 vif 30 address 192.168.30.1/24 to set the address for VLAN 30
4. Entered set interfaces ethernet eth1 vif 130 description ‘VLAN 130’ to create VLAN 130 and set its description
5. Entered set interfaces ethernet eth1 vif 130 address 192.168.130.1/24 to set the address for VLAN 130
6. Entered set interfaces ethernet eth1 vif 230 description ‘VLAN 230’ to create VLAN 230 and set its description

Wireless and Enterprise Routers

7. Entered set interfaces ethernet eth1 vif 230 address 192.168.230.1/24 to set the address for VLAN 230
8. Entered commit and save commands to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured VLANs on Cisco switches

VLANs were configured on both Cisco switches to allow VLANs to be assigned to specific ports. With DHCP enabled, this allowed for dynamic IP addressing based upon VLAN.

1. Typed configure to enter configuration mode
2. Typed in the following commands to create VLAN 30 and add it to port 11:
    a. Entered vlan 30 to create VLAN 30
    b. Entered exit to leave VLAN configuration mode
    c. Entered int Gi1/0/11 to enter interface configuration mode for port 11
    d. Entered switchport mode access to set the port to access mode
    e. Entered switchport access vlan 30 to assign VLAN 30 to the port
    f. Entered exit to leave interface configuration mode
3. Typed in the following commands to create VLAN 130 and add it to port 12:
    a. Entered vlan 130 to create VLAN 130
    b. Entered exit to leave VLAN configuration mode
    c. Entered int Gi1/0/12 to enter interface configuration mode for port 12
    d. Entered switchport mode access to set the port to access mode
    e. Entered switchport access vlan 130 to assign VLAN 130 to the port
    f. Entered exit to leave interface configuration mode

4. Typed in the following commands to create VLAN 230 and add it to port 13:
    a. Entered vlan 230 to create VLAN 230
    b. Entered exit to leave VLAN configuration mode
    c. Entered int Gi1/0/13 to enter interface configuration mode for port 13
    d. Entered switchport mode access to set the port to access mode
    e. Entered switchport access vlan 230 to assign VLAN 230 to the port
    f. Entered exit to leave interface configuration mode
5. Repeated steps 2 through 4 for second Cisco switch
6. Typed in the following commands to trunk port 40 on bottom Cisco switch:
    a. Entered int Gi1/0/40 to enter interface configuration mode
    b. Entered switchport trunk encapsulation dot1q to set protocol to VLANs
    c. Entered switchport mode trunk to set the port to trunk mode
    d. Entered switchport trunk allowed vlan add 30 to add VLAN 30 to the port
    e. Entered switchport trunk allowed vlan add 130 to add VLAN 130 to the port
    f. Entered switchport trunk allowed vlan add 230 to add VLAN 230 to the port
    g. Entered exit to leave interface configuration mode
7. Repeated steps 6a-6g for interfaces Gi1/0/37, Gi1/0/40, and Gi1/0/42 on top Cisco switch
8. Entered copy run start command to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured VLANs on HP/Aruba switch

VLANs were configured on the HP switch to allow VLANs to be assigned to specific ports. With DHCP enabled, this allowed for dynamic IP addressing based upon VLAN.

Wireless and Enterprise Routers

1. Typed configure to enter configuration mode
2. Entered vlan 30 to create VLAN 30, then issued exit command to leave interface configuration mode
3. Entered vlan 130 to create VLAN 130, then issued exit command to leave interface configuration mode
4. Entered vlan 230 to create VLAN 230, then issued exit command to leave interface configuration mode
5. Entered interface 11 untagged vlan 30 to assign VLAN 30 to port 11 as an access port
6. Entered interface 12 untagged vlan 130 to assign VLAN 130 to port 12 as an access port
7. Entered interface 13 untagged vlan 230 to assign VLAN 230 to port 13 as an access port
8. Entered interface 22 tagged vlan 30 to assign VLAN 30 to port 22 as a trunked port
9. Entered interface 22 tagged vlan 130 to assign VLAN 130 to port 22 as a trunked port
10. Entered interface 22 tagged vlan 230 to assign VLAN 230 to port 22 as a trunked port
11. Typed write memory to save running configuration into startup configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured DHCP for VLANs on VyOS

DHCP was configured for each VLAN on the VyOS device to dynamically allocate IP addresses based upon which VLAN a device was connected to.

1. Entered configuration mode by typing configure
2. Entered set service dhcp-server shared-network-name DHCP30 subnet 192.168.30.0/24 default-router 192.168.30.1 to set the default gateway for VLAN 30

3. Entered set service dhcp-server shared-network-name DHCP30 subnet 192.168.30.0/24 name-server 10.2.1.11 to set the default DNS server
4. Entered set service dhcp-server shared-network-name DHCP30 subnet 192.168.30.0/24 range 0 start 192.168.30.100 to set the start of the DHCP pool for VLAN 30
5. Entered set service dhcp-server shared-network-name DHCP30 subnet 192.168.30.0/24 range 0 stop 192.168.30.200 to set the end of the DHCP pool for VLAN 30
6. Entered set service dhcp-server shared-network-name DHCP130 subnet 192.168.130.0/24 default-router 192.168.130.1 to set the default gateway for VLAN 130
7. Entered set service dhcp-server shared-network-name DHCP130 subnet 192.168.130.0/24 name-server 10.2.1.11 to set the default DNS server
8. Entered set service dhcp-server shared-network-name DHCP130 subnet 192.168.130.0/24 range 0 start 192.168.130.100 to set the start of the DHCP pool for VLAN 130
9. Entered set service dhcp-server shared-network-name DHCP130 subnet 192.168.130.0/24 range 0 stop 192.168.130.200 to set the end of the DHCP pool for VLAN 130
10. Entered set service dhcp-server shared-network-name DHCP230 subnet 192.168.230.0/24 default-router 192.168.230.1 to set the default gateway for VLAN 230
11. Entered set service dhcp-server shared-network-name DHCP230 subnet 192.168.230.0/24 name-server 10.2.1.11 to set the default DNS server
12. Entered set service dhcp-server shared-network-name DHCP230 subnet 192.168.230.0/24 range 0 start 192.168.230.100 to set the start of the DHCP pool for VLAN 230

13. Entered set service dhcp-server shared-network-name DHCP230 subnet 192.168.230.0/24 range 0 stop 192.168.230.200 to set the end of the DHCP pool for VLAN 230
14. Typed commit and save commands to save the configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured DNS for VLANs on VyOS

DNS was specified for each VLAN on the VyOS to forward DNS queries to the correct server on the cit.lcl network.

1. Entered set service dns forwarding listen-address 192.168.30.1 to specify the IP address to listen for DNS requests for VLAN 30
2. Entered set service dns forwarding allow-from 192.168.30.0/24 to specify the network to forward DNS requests from for VLAN 30
3. Entered set service dns forwarding dhcp eth1.30 to specify the interface the DNS requests would come from for VLAN 30
4. Entered set service dns forwarding listen-address 192.168.130.1 to specify the IP address to listen for DNS requests for VLAN 130
5. Entered set service dns forwarding allow-from 192.168.130.0/24 to specify the network to forward DNS requests from for VLAN 130
6. Entered set service dns forwarding dhcp eth1.130 to specify the interface the DNS requests would come from for VLAN 130
7. Entered set service dns forwarding listen-address 192.168.230.1 to specify the IP address to listen for DNS requests for VLAN 230

8. Entered set service dns forwarding allow-from 192.168.230.0/24 to specify the network to forward DNS requests from for VLAN 230
9. Entered set service dns forwarding dhcp eth1.230 to specify the interface the DNS requests would come from for VLAN 230
10. Typed commit and save commands to save the configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured NAT for VLANs on VyOS

NAT was configured to translate VLAN-based internal addresses to addresses appropriate for the cit.lcl network, allowing for connection to the Internet through cit.lcl.

1. Typed configure to enter configuration mode
2. Typed set nat source rule 30 source address 192.168.30.0/24 to set the range of addresses to translate for VLAN 30
3. Typed set nat source rule 30 outbound-interface eth0 to specify which interface the traffic would leave from for VLAN 30
4. Typed set nat source rule 30 translation address masquerade to allow the router to choose what IP addresses to translate to for VLAN 30
5. Typed set nat source rule 130 source address 192.168.130.0/24 to set the range of addresses to translate for VLAN 130
6. Typed set nat source rule 130 outbound-interface eth0 to specify which interface the traffic would leave from for VLAN 130
7. Typed set nat source rule 130 translation address masquerade to allow the router to choose what IP addresses to translate to for VLAN 130

8. Typed set nat source rule 230 source address 192.168.230.0/24 to set the range of addresses to translate for VLAN 230
9. Typed set nat source rule 230 outbound-interface eth0 to specify which interface the traffic would leave from for VLAN 230
10. Typed set nat source rule 230 translation address masquerade to allow the router to choose what IP addresses to translate to for VLAN 230
11. Typed commit and save to save the configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured SSH access on VyOS

SSH was configured on the VyOS router to allow for remote connection to the device without requiring the use of a serial cable.

1. Typed configure to enter configuration mode
2. Typed set service ssh port 22 to specify which TCP port should allow SSH traffic
3. Typed set service ssh access-control allow user adocter to allow the *adocter* user to SSH into the device
4. Typed set service ssh access-control allow user park to allow the *park* user to SSH into the device
5. Typed set service ssh listen-address 10.25.30.254 to specify the IP address that should listen for SSH connections
6. Typed commit and save to save configuration
7. Searched for command prompt on personal Windows laptop

Wireless and Enterprise Routers

8. Typed ssh adocter@10.25.30.254 into command prompt and logged into VyOS device to confirm SSH settings were correct

Configured SSH access on Cisco switches

SSH was configured on the Cisco switches to allow for remote connection to the device without requiring the use of a serial cable.

1. Typed configure terminal to enter configuration mode
2. Entered ip default-gateway 192.168.30.1 to set default gateway for the switch
3. Entered interface vlan 30 to enter interface configuration mode
4. Entered ip address 192.168.30.* 255.255.255.0 to set the IP address for VLAN 30
    a. * = 2 for the top Cisco switch
    b. * = 3 for the bottom Cisco switch
5. Entered exit to leave interface configuration
6. Entered ip domain-name docterpark.com to set domain name for RSA key generation
7. Entered crypto key generate rsa to generate an RSA key pair
8. Inputted bit value of 1024 to ensure security of RSA key
9. Entered ip ssh version 2 to set the SSH version to 2
10. Entered line vty 0 4 to enter line configuration mode
11. Entered transport input ssh to set the line to listen for SSH connections
12. Entered login local to specify the login type
13. Entered exit to exit line configuration mode
14. Entered username park password [password] to create new user for SSH purposes
15. Entered copy run start to save configuration

Configured SSH access on HP/Aruba switch

SSH was configured on the HP switch to allow for remote connection to the device without requiring the use of a serial cable.

1. Typed configure to enter configuration mode
2. Entered crypto key generate ssh rsa bits 1024 to generate 1024-bit RSA key pair
3. Entered aaa authentication ssh login local to specify local login mode for SSH
4. Entered aaa authentication ssh enable local to enable SSH connections
5. Entered write memory to save configuration

Configured IIS website with port forwarding

Port forwarding was configured alongside an IIS website in order for the website to be visible to any device within the cit.lcl network.

1. Searched for IIS manager on Windows PC to open application
2. Opened server on left panel and opened **Sites**
3. Right-clicked on default website and selected **Edit bindings**
4. Clicked **Add**
5. Filled in the IP of host as 192.168.130.100 and clicked **OK**
6. Swapped over to VyOS terminal
7. Entered configuration mode by typing configure
8. Entered set nat destination rule 99 destination port 80 to set TCP port 80 (HTTP) as forwarding port

Wireless and Enterprise Routers

9. Entered set nat destination rule 99 inbound-interface eth0 to set interface traffic would come from
10. Entered set nat destination rule 99 protocol tcp to set protocol to TCP
11. Entered set nat destination rule 99 translation address 192.168.130.100 to direct the HTTP traffic to the IIS server
12. Typed commit and save to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Disabled wireless access point

The wireless interface was disabled to reduce wireless network interference.

1. Typed configure to enter configuration mode
2. Typed set interfaces wireless wlan0 disable to disable WLAN interface
3. Typed commit and save to save configuration

Set up Phase II architecture

The devices for Phase II consisted of a Cisco 2811 router, two Cisco switches, an HP switch, two Windows 10 PCs, and one Ubuntu PC.

1. Connected Cisco router port 0 to CIT network via gray uplink cable
2. Connected Cisco router port 1 to top Cisco switch port 37
3. Connected top Cisco switch port 40 to bottom Cisco switch port 40
4. Connected top Cisco switch port 42 to HP switch port 22
5. Connected top Cisco switch port 1 to Patch Panel 1 port 7
6. Connected bottom Cisco switch port 1 to Patch Panel 1 port 8

Wireless and Enterprise Routers

7. Connected HP switch port 1 to Patch Panel 1 port 9
8. Connected Cisco router console port to Patch Panel 2 port 7
9. Connected top Cisco switch console port to Patch Panel 2 port 8
10. Connected HP switch console port to Patch Panel 2 port 9
11. Connected PC1 to Patch Panel 1 port 7
12. Connected PC2 to Patch Panel 1 port 8
13. Connected PC3 to Patch Panel 1 port 9

Configured WAN Ethernet interface on Cisco router

The interface hosting the uplink connection was configured as a WAN interface to communicate with the cit.lcl network.

1. Typed configure terminal to enter configuration mode
2. Entered interface FastEthernet 0/0 to enter interface configuration mode
3. Entered ip address 10.25.30.254 255.255.255.0 to set IP address and subnet mask on the interface
4. Entered no shutdown to enable the interface
5. Entered exit to leave interface configuration mode
6. Entered copy run start to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured sub-interfaces on Cisco router

Sub-interfaces were configured within the LAN interface to handle the VLANs configured on the Cisco switches. Cisco routers technically do not have VLANs in the same

sense that the VyOS router did; the VLANs' information instead gets configured into sub-interfaces.

1. Typed configure terminal to enter configuration mode
2. Entered interface FastEthernet 0/1.30 to enter interface configuration mode
3. Entered encapsulation dot1Q 30 to set the sub-interface as the VLAN 30 interface
4. Entered ip address 192.168.30.1 255.255.255.0 to set the IP and subnet mask
5. Entered no shutdown to enable the sub-interface
6. Entered exit to leave interface configuration mode
7. Repeated steps 2 through 6 for sub-interfaces 0/1.130 and 0/1.230
8. Entered copy run start to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured DHCP for VLANs on Cisco router

DHCP allowed for dynamic allocation of IP addresses based on VLAN.

1. Typed configure terminal to enter configuration mode
2. Entered ip dhcp excluded-address 192.168.30.1 to exclude the gateway address from the pool of available addresses
3. Entered ip dhcp pool DHCP30 to enter DHCP pool configuration mode
4. Entered network 192.168.30.0 255.255.255.0 to specify network address and subnet mask
5. Entered default-router 192.168.30.1 to set the default gateway for this network
6. Entered dns-server 10.2.1.11 to specify the DNS server
7. Entered exit to leave DHCP pool configuration mode
8. Repeated steps 2 through 7 for VLANs 130 and 230

Wireless and Enterprise Routers

9. Entered copy run start to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured NAT for VLANs on Cisco router

NAT was configured to translate local addresses to addresses appropriate for the cit.lcl network, allowing for connection to the Internet through cit.lcl.

1. Entered into configuration mode by typing configure terminal
2. Entered interface fa0/1.30 to enter interface configuration mode for .30 sub-interface
3. Entered ip nat inside to set sub-interface as inside for NAT purposes
4. Entered exit to leave interface configuration mode
5. Repeated steps 2 through 4 for interfaces fa0/1.130 and fa0/1.230
6. Entered interface fa0/0 to enter interface configuration mode for eth0 interface
7. Entered ip nat outside to set interface as outside for NAT purposes
8. Entered exit to interface configuration mode
9. Entered access-list 30 permit 192.168.30.0 0.0.0.255 to add .30 network to allowed addresses for NAT
10. Entered access-list 30 permit 192.168.130.0 0.0.0.255 to add .130 network to allowed addresses for NAT
11. Entered access-list 30 permit 192.168.230.0 0.0.0.255 to add .230 network to allowed addresses for NAT
12. Entered ip nat pool outsideconnet 10.25.30.254 10.25.30.254 netmask 255.255.255.0 to create NAT pool for outside IP addresses
13. Enabled ip nat inside source list 30 interface fa0/0 overload to enable dynamic NAT

Wireless and Enterprise Routers

14. Entered ip route 0.0.0.0 0.0.0.0 10.25.30.1 to set IP default route
15. Entered copy run start to save configuration
    a. Full configuration can be viewed in Appendix B: Configuration Files

Configured SSH access on Cisco router

SSH access was configured on the Cisco router to allow for remote connection into the router without the need for a serial cable connection.

1. Entered configuration mode by typing configuration terminal
2. Entered ip domain-name doctorpark.com to set domain name for RSA key generation
3. Entered crypto key generate rsa to generate an RSA key pair
4. Inputted bit value of 2048 to ensure security of RSA key
5. Entered ip ssh version 2 to set the SSH version to 2
6. Entered line vty 0 4 to enter line configuration mode
7. Entered transport input ssh to set the line to listen for SSH connections
8. Entered login local to specify the login type
9. Entered exit to exit line configuration mode
10. Entered username park password [password] to create new user for SSH purposes

Analyzed VLAN traffic using Wireshark

SPAN was utilized to forward traffic from a trunked port to the Ubuntu PC in order to view 802.1Q tags within frames. Wireshark was utilized to capture the frames.

1. Connected PC2 to top Cisco switch port 10 temporarily
2. Initiated serial connection to top Cisco switch via console port

Wireless and Enterprise Routers

3. Searched for PuTTY application and clicked **Open**
4. Logged into top Cisco switch
5. Entered configuration mode by typing configure terminal
6. Entered monitor session 1 source interface Gi1/0/37 to set trunked port 37 as the source port for SPAN
7. Entered monitor session 1 destination interface Gi1/0/10 to set port 10 as the destination port for SPAN
8. Opened application menu on PC2 and searched for terminal
9. Typed sudo wireshark into the terminal to open administrator-level Wireshark
10. Clicked the **blue shark fin button** to start capturing packets
11. Generated traffic through trunked port by searching for and opening Microsoft Edge on a Windows PC and typing google.com into the address bar
12. Filtered packets by using the vlan display filter
13. Clicked the **red stop button** to stop capturing packets
14. Analyzed packets for 802.1Q tags
    a. Analysis can be found in Appendix A: Answers to Lab Questions

RESULTS

This section includes end-of-lab physical and logical diagrams for Phases I and II.

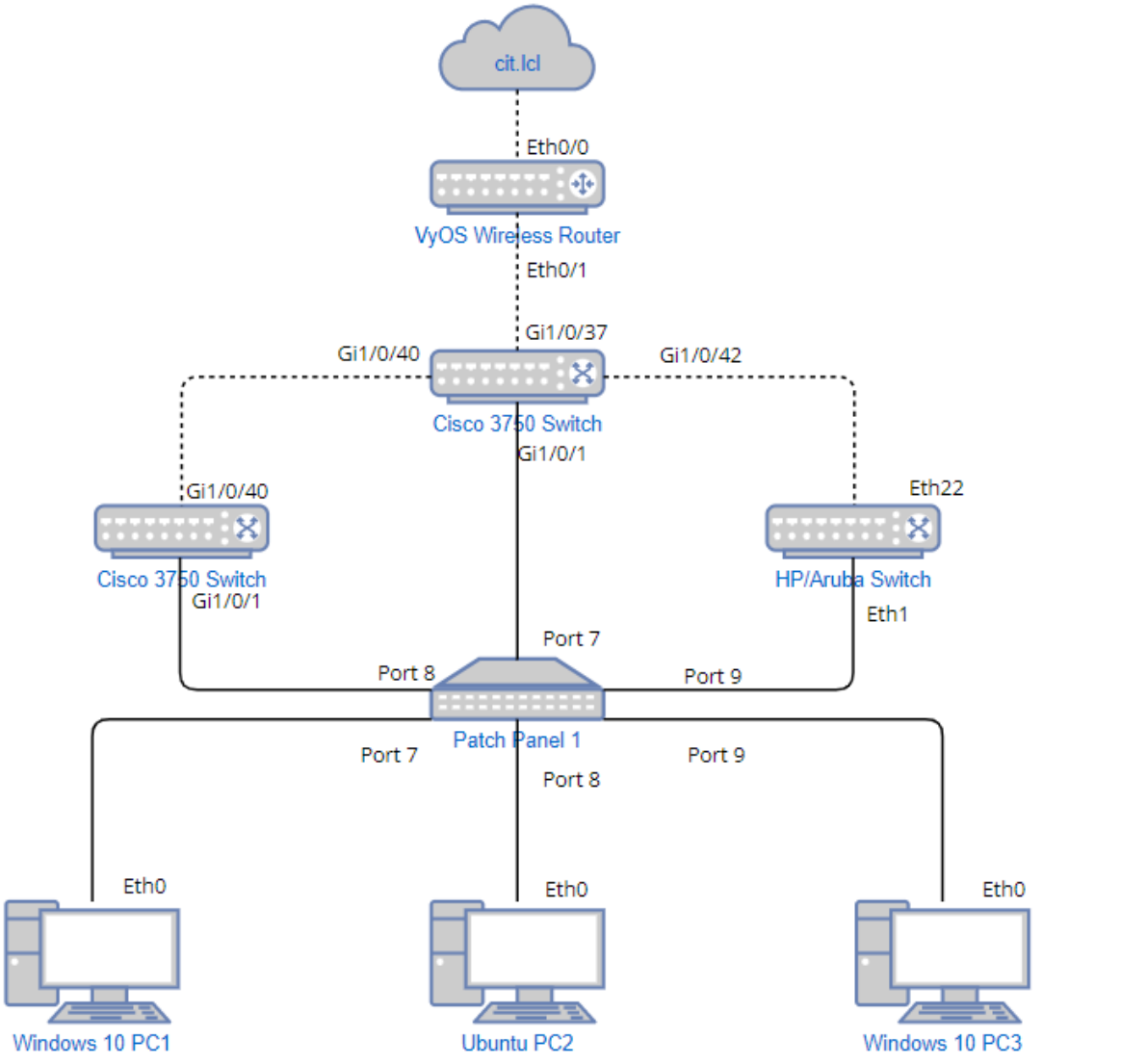

Figure 1: Phase I Physical Diagram

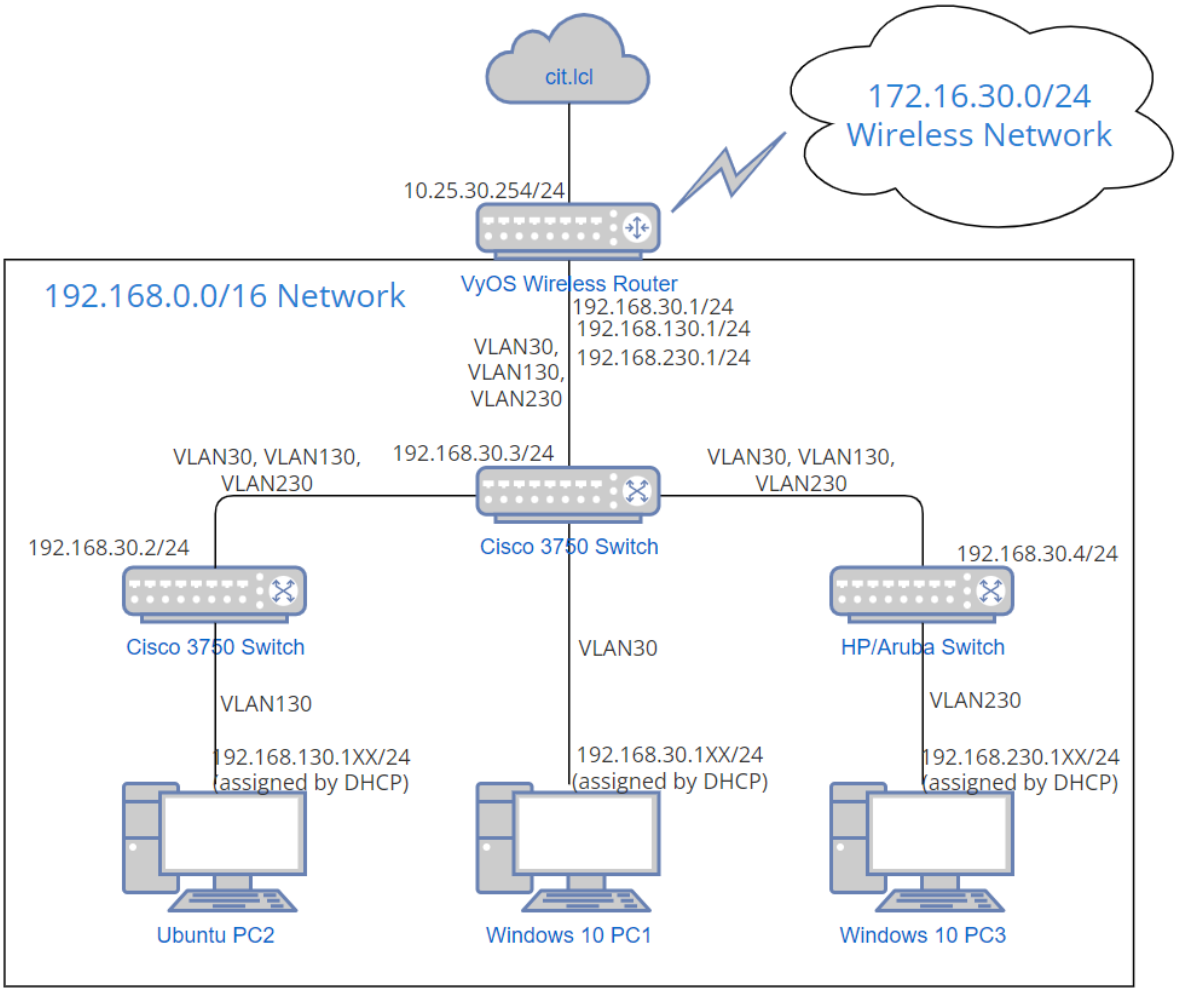

Figure 2: Phase I Logical Diagram

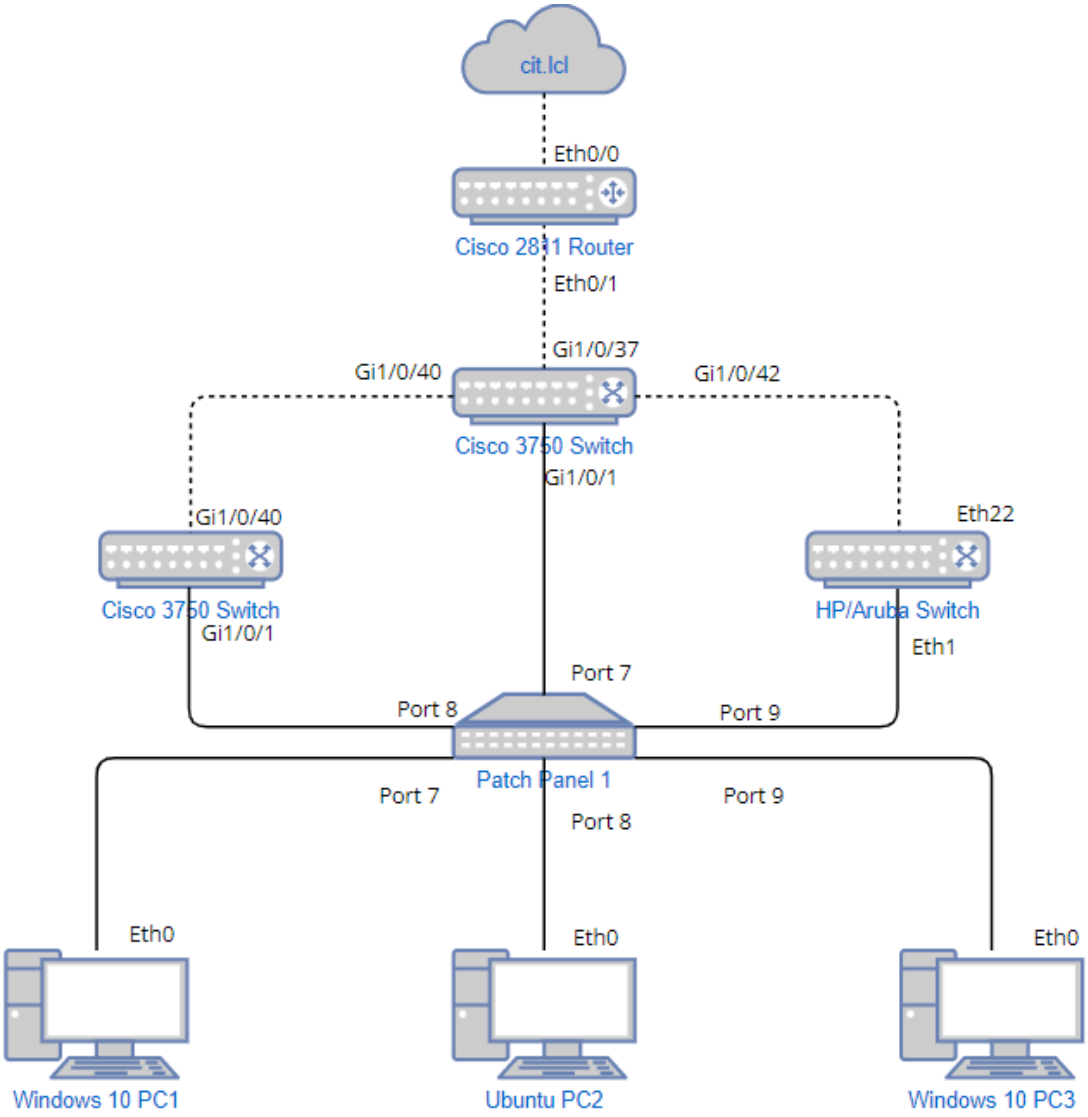

Figure 3: Phase II Physical Diagram

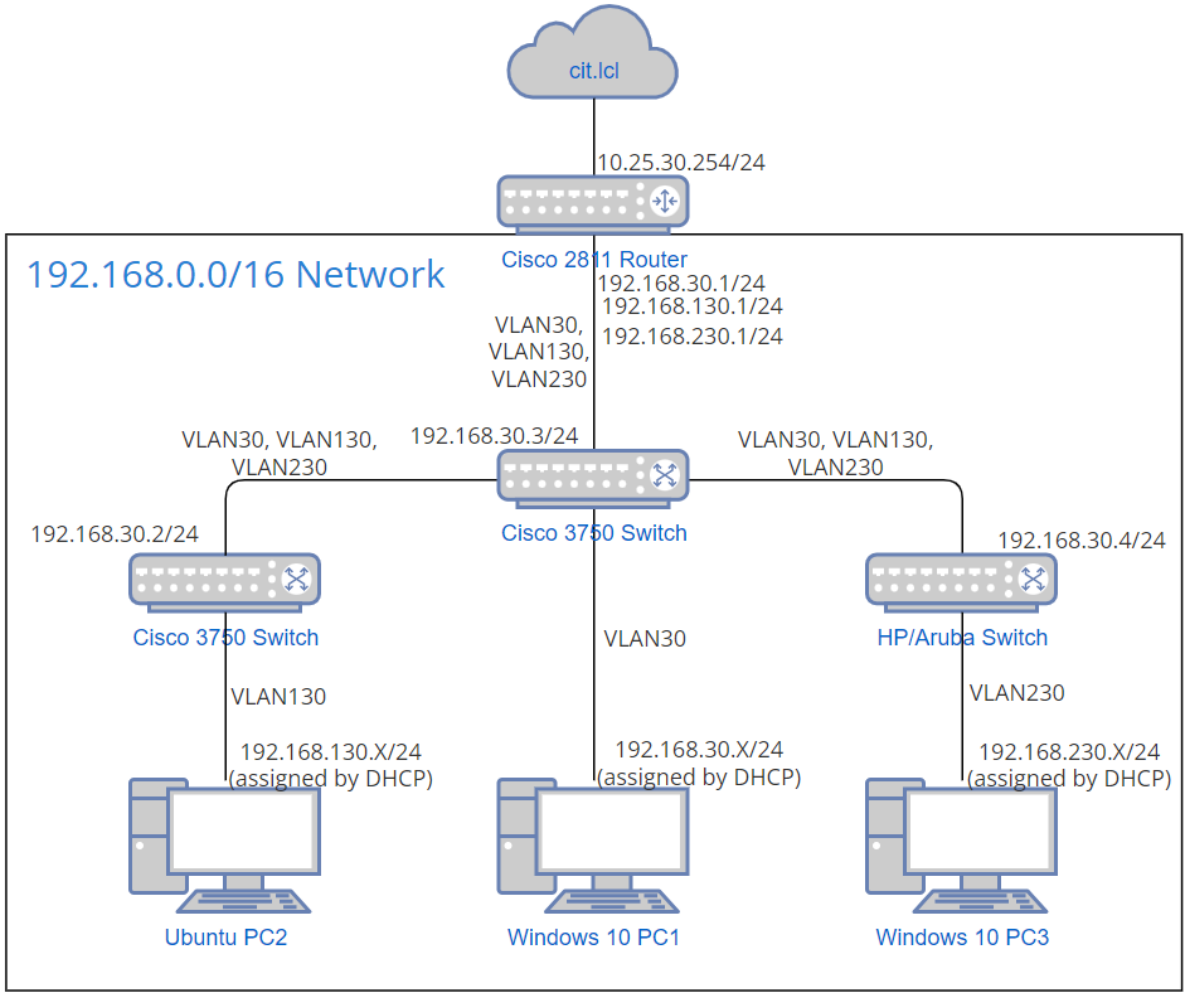

Figure 4: Phase II Logical Diagram

BIBLIOGRAPHY

Andamasov, Y. (2018). *Adding users*. VyOS. Retrieved March 10, 2022, from https://support.vyos.io/en/kb/articles/adding-users-2

Andamasov, Y. (2021). *Nat principles*. VyOS. Retrieved March 10, 2022, from https://support.vyos.io/en/kb/articles/nat-principles

Butterfield, R. (personal communication, March 9,2022)

Canonical (2022), Ubuntu

Ciena Inc. (2022). VyOS

Cisco Systems (2022), Cisco 3750

Cisco Systems (2022), Cisco 2811

CIT-NET Lab Information. Lab Report Template. (2022). Retrieved March 10, 2022, from https://purdue.brightspace.com/d2l/le/content/171363/viewContent/3726799/View

Configure Cisco Router as DHCP Server. Study CCNA. (2021, June 24). Retrieved March 10, 2022, from https://study-ccna.com/configure-cisco-router-as-dhcp-server/

Deadman, R. (2022). Spring 2022 CNIT240-007/CNIT344-006 LAB. Lab 2 Assignment and Report Submission. Retrieved March 10, 2022, from https://purdue.brightspace.com/d2l/lms/dropbox/user/folder_submit_files.d2l?ou=458824&db=531240&grpid=538115

Deadman, R. (personal communication, March 9,2022)

DHCP server. DHCP Server - VyOS 1.4.x (sagitta) documentation. (2022). Retrieved March 10, 2022, from https://docs.vyos.io/en/latest/configuration/service/dhcp-server.html

Eshenko, D. (2019). *Set/change the password of a user*. VyOS. Retrieved March 10, 2022, from https://support.vyos.io/en/kb/articles/set-change-the-password-of-a-user

Ethernet. Ethernet - VyOS 1.4.x (sagitta) documentation. (n.d.). Retrieved March 10, 2022, from https://docs.vyos.io/en/latest/configuration/interfaces/ethernet.html

Hewlett Packard Enterprise (2022), HP/Aruba

Group 24 (personal communication, March 4,2022)

How to configure lan and WAN interface on Vyos Router. TechnologyRSS. (2020, May 24). Retrieved March 10, 2022, from https://technologyrss.com/configure-lan-and-wan-interface-vyos-router/

Wireless and Enterprise Routers

How to configure SSH on Cisco Ios. NetworkLessons.com. (2022, January 12). Retrieved March 10, 2022, from https://networklessons.com/cisco/ccna-200-301/configure-ssh-cisco-ios

How to configure Vlans on the catalyst switches. Cisco Community. (2020, August 16). Retrieved March 10, 2022, from https://community.cisco.com/t5/networking-documents/how-to-configure-vlans-on-the-catalyst-switches/ta-p/3131780

Kaplan, M., Circonflexe, T., & Morriss, J. (2022). *WireShark*. VLAN. Retrieved March 10, 2022, from https://wiki.wireshark.org/VLAN

khan, hamid. (2019, March 5). *VLAN configuration on router*. Home - Cisco Community. Retrieved March 10, 2022, from https://community.cisco.com/t5/routing/vlan-configuration-on-router/td-p/2588774

Microsoft Windows (2022), Windows 10

Natarajan, R. (2013, August 19). *How to enable SSH on Cisco Switch, Router and asa*. The Geek Stuff. Retrieved March 10, 2022, from https://www.thegeekstuff.com/2013/08/enable-ssh-cisco/

Packard, H. (n.d.). *Support center*. Document Display | HPE Support Center. Retrieved March 10, 2022, from https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c03182828

Quick start. Quick Start - VyOS 1.4.x (sagitta) documentation. (n.d.). Retrieved March 10, 2022, from https://docs.vyos.io/en/sagitta/quick-start.html

rebortg, & c-po. (2021). *Default Gateway/Route*. Default Gateway/Route - VyOS 1.4.x (sagitta) documentation. Retrieved March 10, 2022, from https://docs.vyos.io/en/latest/configuration/system/default-route.html

System. (2015, March 12). *How to set a subnet and gateway to an ethernet interface*. VyOS Platform Community Forums. Retrieved March 10, 2022, from https://forum.vyos.io/t/how-to-set-a-subnet-and-gateway-to-an-ethernet-interface/411

techhub. Configuring the switch for SSH operation. (n.d.). Retrieved March 10, 2022, from

https://techhub.hpe.com/eginfolib/networking/docs/switches/RA/15-18/5998-

8151_ra_2620_asg/content/ch08s06.html

APPENDIX A: ANSWERS TO LAB QUESTIONS

This section answers questions asked throughout the lab assignment.

Traffic monitoring

Compare and contrast the per VLAN statistics with the overall statistics of traffic traversing a particular interface (the uplink to the router, for instance).

- There are less frames going into each VLAN statistics compared to the uplink to the router. Router receives all the information from all the VLANs while the PC receives traffic only from VLANs.

Compare the number of ingress and egress frames. Explain.

- To compare the number of ingress and egress frames, IP source and IP destination filter was used to get the number of frames. Within the same amount of time, IP source, ingress, seemed to receive a few more frames compared to IP destination, egress.

What is the correlation between octets and frames?

- Frames are divisible by octets. Frames are 1,512 bits - or 64 octets - long. Because octets are units of 8 bits, any frames larger than 1512 bits (e.g. frames with VLAN tags) are splitted.

802.1Q frame tags

Describe each fields' purpose and function.

- The priority field describes how high of a priority the packet is so switches can prioritize it accordingly. The drop eligible indicator (DEI) field, formerly known as the CFI field, tells the switch whether or not the packet is eligible to be dropped if there is a lot of traffic congestion. The ID field denotes the ID number of the VLAN associated with the packet.

Compare and contrast with a frame that does not contain an 802.1Q tag from the same host to the same external location.

- The frame with the 802.1Q tag includes a section within the frame that describes the tag. This section includes the fields mentioned above. The frame without the 802.1Q tag does not have this section.

APPENDIX B: CONFIGURATION FILES

This section includes configuration files for the various switches and routers referenced in this report.

Cisco switches

```
Current configuration : 3399 bytes
!
! Last configuration change at 00:44:57 UTC Wed May 18 2011
! NVRAM config last updated at 00:45:01 UTC Wed May 18 2011
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname top_cisco_switch
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zS83$5nkbkQI4lwSzJJlPq.ctf.
enable password 7 0222015A0F280A351F1A5D
!
```

username park password 7 095C4F1B12

no aaa new-model

switch 1 provision ws-c3750e-48pd

system mtu routing 1500

!

!

ip domain-name docterpark.com

!

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

!

!

!

!

!

!

!

!

vlan internal allocation policy ascending

!

```
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1/0/1
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface GigabitEthernet1/0/4
!
interface GigabitEthernet1/0/5
```

```
!
interface GigabitEthernet1/0/6
!
interface GigabitEthernet1/0/7
!
interface GigabitEthernet1/0/8
!
interface GigabitEthernet1/0/9
!
interface GigabitEthernet1/0/10
!
interface GigabitEthernet1/0/11
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet1/0/12
 switchport access vlan 130
 switchport mode access
!
interface GigabitEthernet1/0/13
 switchport access vlan 230
 switchport mode access
!
```

```
interface GigabitEthernet1/0/14
!
interface GigabitEthernet1/0/15
!
interface GigabitEthernet1/0/16
!
interface GigabitEthernet1/0/17
!
interface GigabitEthernet1/0/18
!
interface GigabitEthernet1/0/19
!
interface GigabitEthernet1/0/20
!
interface GigabitEthernet1/0/21
!
interface GigabitEthernet1/0/22
!
interface GigabitEthernet1/0/23
!
interface GigabitEthernet1/0/24
!
interface GigabitEthernet1/0/25
```

```
!
interface GigabitEthernet1/0/26
!
interface GigabitEthernet1/0/27
!
interface GigabitEthernet1/0/28
!
interface GigabitEthernet1/0/29
!
interface GigabitEthernet1/0/30
!
interface GigabitEthernet1/0/31
!
interface GigabitEthernet1/0/32
!
interface GigabitEthernet1/0/33
!
interface GigabitEthernet1/0/34
!
interface GigabitEthernet1/0/35
!
interface GigabitEthernet1/0/36
!
```

```
interface GigabitEthernet1/0/37
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/38
!
interface GigabitEthernet1/0/39
!
interface GigabitEthernet1/0/40
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/41
!
interface GigabitEthernet1/0/42
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet1/0/43
!
interface GigabitEthernet1/0/44
!
interface GigabitEthernet1/0/45
```

```
!
interface GigabitEthernet1/0/46
!
interface GigabitEthernet1/0/47
!
interface GigabitEthernet1/0/48
!
interface GigabitEthernet1/0/49
!
interface GigabitEthernet1/0/50
!
interface GigabitEthernet1/0/51
!
interface GigabitEthernet1/0/52
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface Vlan1
 no ip address
!
interface Vlan30
```

```
 ip address 192.168.30.3 255.255.255.0
!
ip default-gateway 192.168.30.1
ip http server
ip http secure-server
!
!
!
snmp-server community exit RO
!
!
line con 0
 password 7 05080806351F1A5D1E1718071B5F54
 login
line vty 0
 password 7 140E1718
 login
line vty 1
 password 7 1511050510797F702F213A37035446
 login local
 transport input ssh
line vty 2 4
 password 7 0716245F
```

```
 login
line vty 5 15
 password 7 0716245F
 login
!
end
```

HP/Aruba switch

```
hostname "hp-aruba-switch"
module 1 type jl259a
snmp-server community "public" unrestricted
vlan 1
   name "DEFAULT_VLAN"
   no untagged 11-13
   untagged 1-10,14-28
   ip address dhcp-bootp
   ipv6 enable
   ipv6 address dhcp full
   exit
vlan 30
   name "VLAN30"
   untagged 11
   tagged 22
```

```
  no ip address
  exit
vlan 130
  name "VLAN130"
  untagged 12
  tagged 22
  no ip address
  exit
vlan 230
  name "VLAN230"
  untagged 13
  tagged 22
  no ip address
  exit
no tftp server
no autorun
no dhcp config-file-update
no dhcp image-file-update
no dhcp tr69-acs-url
password manager
password operator
```

VyOS router

show interfaces

```
 ethernet eth0 {
     address 10.25.30.254/24
     hw-id 00:e0:4c:68:2f:bb
 }
 ethernet eth1 {
     hw-id 00:e0:4c:68:2f:bc
     vif 30 {
         address 192.168.30.1/24
         description "VLAN 30"
     }
     vif 130 {
         address 192.168.130.1/24
         description "VLAN 130"
     }
     vif 230 {
         address 192.168.230.1/24
         description "VLAN 230"
     }
 }
 ethernet eth2 {
     hw-id 00:e0:4c:68:2f:bd
```

```
}
ethernet eth3 {
    hw-id 00:e0:4c:68:2f:be
}
ethernet eth4 {
    hw-id 00:e0:4c:68:2f:bf
}
ethernet eth5 {
    hw-id 00:e0:4c:68:2f:c0
}
loopback lo {
}
wireless wlan0 {
    address 172.16.30.1/24
    channel 1
    country-code us
    description "Group 30 Wireless Network"
    disable
    hw-id 60:6c:66:33:a4:cd
    mode g
    physical-device phy0
    security {
        wpa {
```

```
            mode wpa2
            passphrase docterpark
        }
    }
    ssid c240-344g30
    type access-point
}
```

show nat

```
destination {
    rule 99 {
        destination {
            port 80
        }
        inbound-interface eth0
        protocol tcp
        translation {
            address 192.168.130.100
        }
    }
}
source {
    rule 10 {
```

```
        outbound-interface eth0
        source {
            address 172.16.30.0/24
        }
        translation {
            address masquerade
        }
    }
    rule 30 {
        outbound-interface eth0
        source {
            address 192.168.30.0/24
        }
        translation {
            address masquerade
        }
    }
    rule 130 {
        outbound-interface eth0
        source {
            address 192.168.130.0/24
        }
        translation {
```

```
            address masquerade
        }
    }
    rule 230 {
        outbound-interface eth0
        source {
            address 192.168.230.0/24
        }
        translation {
            address masquerade
        }
    }
}
```

show service dhcp-server

```
 shared-network-name DHCP30 {
    subnet 192.168.30.0/24 {
        default-router 192.168.30.1
        name-server 10.2.1.11
        range 0 {
            start 192.168.30.100
            stop 192.168.30.200
        }
```

```
    }
}
shared-network-name DHCP130 {
    subnet 192.168.130.0/24 {
        default-router 192.168.130.1
        name-server 10.2.1.11
        range 0 {
            start 192.168.130.100
            stop 192.168.130.200
        }
    }
}
shared-network-name DHCP230 {
    subnet 192.168.230.0/24 {
        default-router 192.168.230.1
        name-server 10.2.1.11
        range 0 {
            start 192.168.230.100
            stop 192.168.230.200
        }
    }
}
shared-network-name YOLO {
```

```
    subnet 172.16.30.0/24 {
        default-router 172.16.30.1
        name-server 10.2.1.11
        range 0 {
            start 172.16.30.100
            stop 172.16.30.200
        }
        static-mapping something {
        }
    }
}
```

show service dns

```
 forwarding {
    allow-from 172.16.30.0/24
    allow-from 192.168.30.0/24
    allow-from 192.168.130.0/24
    allow-from 192.168.230.0/24
    dhcp wlan0
    dhcp eth1.30
    dhcp eth1.130
    dhcp eth1.230
    listen-address 172.16.30.1
```

```
    listen-address 192.168.30.1
    listen-address 192.168.130.1
    listen-address 192.168.230.1
 }
```

Cisco router

```
Current configuration : 2401 bytes
!
! Last configuration change at 17:47:06 UTC Wed Mar 9 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname cisco_router
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
```

```
!
dot11 syslog
ip source-route
!
!
ip cef
ip dhcp excluded-address 192.168.30.1
ip dhcp excluded-address 192.168.130.1
ip dhcp excluded-address 192.168.230.1
!
ip dhcp pool DCHP30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 10.2.1.11
!
ip dhcp pool DHCP130
 network 192.168.130.0 255.255.255.0
 default-router 192.168.130.1
 dns-server 10.2.1.11
!
ip dhcp pool DHCP230
 network 192.168.230.0 255.255.255.0
 default-router 192.168.230.1
```

```
 dns-server 10.2.1.11
!
!
!
ip domain name doctorpark
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
!
!
voice-card 0
!
crypto pki token default removal timeout 0
!
```

```
!
!
!
license udi pid CISCO2811 sn FTX1131A2AZ
username park password 7 051B071D2A
!
redundancy
!
!
ip ssh version 2
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.25.30.254 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
```

```
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface FastEthernet0/1.130
 encapsulation dot1Q 130
 ip address 192.168.130.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface FastEthernet0/1.230
 encapsulation dot1Q 230
 ip address 192.168.230.1 255.255.255.0
 ip nat inside
```

```
 ip virtual-reassembly in
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip nat pool outsideconnet 10.25.30.254 10.25.30.254 netmask 255.255.255.0
ip nat inside source list 30 interface FastEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 10.25.30.1
!
access-list 30 permit 192.168.30.0 0.0.0.255
access-list 30 permit 192.168.130.0 0.0.0.255
```

```
access-list 30 permit 192.168.230.0 0.0.0.255
!
!
!
!
!
!
control-plane
!
!
!
!
mgcp profile default
!
!
!
!
!
!
line con 0
 password 7 110A170C03415F58
 login
line aux 0
```

```
line vty 0 4
 login local
 transport input ssh
!
scheduler allocate 20000 1000
end
```