***Lab 2: Wireless Router/Enterprise Routers***

CNIT34400-007  
Group 11  
Keegan Long  
Ethan Hammond  
Cade Sturm  
Submitted To: Waleed Nasr  
Date Submitted: 10/20/22  
Date Due: 10/20/22

[**P**](#_oepeg6fn8xi3)**rocedures 3**

[Configuring the VyOS Wireless router users](#_bs8ikuqgdbs) 3

[Configuring the VyOS Wireless Router network](#_tzyocwslcq5x) 4

[Configuring DHCP on VyOS Router](#_8yhspmmln0iv) 5

[Configuring DNS on VyOS Router](#_k29on1stu6u9) 7

[VLAN and NAT Configs on Router](#_plqhmxa4asm3) 8

[Create username/password and VLAN Configuration on Cisco Switches](#_osdsbixipje8) 10

[Enabling SSH on the Cisco switches](#_irfmvbi7kl2e) 11

[Configuring VLAN interfaces for Cisco switches](#_dorgelrvulbx) 12

[Configure trunk for VLANs on Cisco switch 1 (s1)](#_bypt6oqddq9s) 12

[Configure trunk for VLANs on Cisco Switch 2 (s2)](#_mppxhfhq5mp4) 13

[HP Procurve Switch Configuration](#_201jyofe10hm) 14

[Windows 10 IIS Web Configuration](#_p00vra6a0vlz) 15`

[Cisco 2811/2901 Router Initial Configuration](#_92wkqwxd9d95) 16

[DNS/DHCP Configurations for Cisco Router](#_j8d2sf55oqzx) 17

[NAT, IP, and VLAN Configurations for Cisco Router](#_s6r3d4pthf4r) 19

[Creating SPAN session for Cisco router Wireshark captures](#_s7i8np43ihq2) 20

[Capturing an 802.1Q tag within a frame in transit outside the network](#_femjn2z308sx) 21

[**R**](#_cr357gljundh)**esults 22**

[**References**](#_xvq36tz2hsl7) **25**

[**Appendices**](#_1ze1xuduf37k) **28**

[Appendix A: Questions and Answers](#_89209c5moya0) 28

[Appendix B: Passwords and SSH Keys](#_q888ykkmhvh3) 29

[Appendix C: Router Configurations](#_yhb9m17ewaow) 30

[Appendix D: Switch Configurations](#_ey2tqs6aq4aj) 36

# 

# PROCEDURES

The procedure section covers how to configure a wireless router using VyOS. To do this, there needs to be IP, DNS, DHCP, NAT, and default route configurations. SSH was also configured for all devices including the router for remote access. Three VLANs were created within the network to break up broadcast domains for traffic management. Three switches were configured to take the traffic from the router and trunk it down between the switches to the PCs to allow for dynamic IP distribution. In an enterprise environment, static IPs may not be practical, and VLANs serve as a mediator to control the traffic and dynamically assign IP addresses. Lastly, a Cisco 2811 router was put in place of the VyOS router and managed by Cisco’s switch operating system. After every section, the commands commit and save were run to save the configuration to nonvolatile memory.

The formatting key of the following section will obey rules below: buttons are **bold**; options are *italicized*; text entered into the computer is in Courier New style; menu and folder navigation are shown with the pipe symbol and are *italicized*: *Start | Programs | MS Office | Word*.

## Configuring the VyOS Wireless router users

In order to secure a router from outsider access, password-protected users needed to be created to ensure that anyone attempting to login to the VyOS router had appropriate username and password credentials.

1. Opened *SecureCRT* and selected the serial port and selected 115200 as the speed to connect to the switch.
2. Entered the default username and password to begin configuring the switch.
3. Entered configure | set system login user ‘username’ authentication plaintext-password [INITIALS]cnit344 to create users and assign them a plaintext password.
4. Changed the default user password by entering the same command used to make a new user with the new password while logged into vyos@vyos.

## Configuring the VyOS Wireless Router network

The next step was to configure the VyOS router to enable its wireless network to allow devices to connect to it via Wi-Fi. After the wireless network was configured and confirmed to be functional, it was disabled to prevent needless interference in the KNOY building.

1. Entered set interfaces ethernet eth0 address 10.25.11.254/24 to enter the WLAN interface.
2. Used show interfaces to confirm that the IP configuration was saved.
3. Entered set protocols static route 0.0.0.0/24 next-hop 10.25.11.1 to set the next hop default gateway.
4. Typed set interfaces wireless wlan0 address 172.16.11.1/24 to set the WiFi IP.
5. Entered set interfaces wireless wlan0 description “Group 11 Wireless Network” to set a description.
6. Set the channel using set interfaces wireless wlan0 channel 2.
7. Set the wireless type with set interfaces wireless wlan0 type access-point.
8. Entered set interfaces wireless wlan0 mode g to set the mode of the WLAN.
9. Typed set interfaces wireless wlan0 ssid “c240-344g11” to set a Wi-Fi SSID.
10. Set the wireless security mode by entering set interfaces wireless wlan0 security wpa passphrase g11c240-344.
11. Set the country code with set interfaces wireless wlan0 country-code us.
12. Entered *set interfaces wireless wlan0 disable* to turn off the WIFI for less KNOY interference.

## Configuring DHCP on VyOS Router

DHCP would allow the VyOS router to automatically assign TCP/IP information to the three computers. With DHCP, the computers will not require their IP statuses to be set statically in order to receive a network connection.

1. Set the default router with set service dhcp-server shared-network-name WLAN subnet 172.16.11.0/24 default-router 172.16.11.1.
2. Set the DNS services with set service dhcp-server shared-network-name WLAN subnet 172.16.11.0/24 name-server 10.2.1.11.
3. Entered set service dhcp-server shared-network-name WLAN subnet 172.16.11.0/24 range 0 start 172.16.11.100 to start the DHCP value range.
4. Entered set service dhcp-server shared-network-name WLAN subnet 172.16.11.0/24 range 0 stop 172.16.11.200 to end the DHCP value range.
5. Entered set service dhcp-server shared-network-name VLAN11 to create the VLAN name in DHCP.
6. Entered set service dhcp-server shared-network-name VLAN11 subnet 192.168.11.0/24 to add the subnet for the VLAN.
7. Entered set service dhcp-server shared-network-name VLAN11 subnet 192.168.11.0/24 default router 192.168.11.1 to set the default route.
8. Entered set service dhcp-server shared-network-name VLAN11 subnet 192.168.11.0/24 name-server 192.168.11.1 to set the DNS server for the VLAN.
9. Repeated steps 5-8 for VLANs 111 and 211 to set up all VLANs together.

## Configuring DNS on VyOS Router

The Domain Name Service (DNS) also needed to be configured on the VyOS router to listen to requests from the VLANs and WLANs’ gateway addresses, as well as set the CIT DNS servers on each VLAN.

1. Typed set service dns forwarding listen-address 192.168.11.1 to set the DNS to listen for requests from that VLANs gateway address.
2. Typed set service dns forwarding listen-address 192.168.111.1 to set the DNS to listen for requests from that VLANs gateway address.
3. Typed set service dns forwarding listen-address 192.168.211.1 to set the DNS to listen for requests from that VLANs gateway address.
4. Typed set service dns forwarding listen-address 172.16.11.1 to set the DNS to listen for requests from the WLANs gateway address.
5. Typed set service dns forwarding allow-from 0.0.0.0/0 to allow DNS request from all ip ranges.
6. Set DNS name servers with set service dns forwarding name-server 10.2.1.11 and set service dns forwarding name-server 10.2.1.12.
7. Typed set service dhcp-server shared-network-name VLAN111 subnet 192.168.111.0/24 name-server 10.2.1.11 (and again with) 10.2.1.12 to set the CIT DNS servers on VLAN 111.
8. Typed set service dhcp-server shared-network-name VLAN11 subnet 192.168.11.0/24 name-server 10.2.1.11(and again with) 10.2.1.12 to set the CIT DNS servers on VLAN 11.
9. Typed set service dhcp-server shared-network-name VLAN211 subnet 192.168.211.0/24 name-server 10.2.1.11(and again with) 10.2.1.12.

## VLAN and NAT Configs on Router

Network Address Translation (NAT) allowed the VyOS router to send any data outside of the internal network as one IP address, despite the network containing multiple IP addresses across three VLANS. The proper NAT settings were configured and VLANS 11, 111, and 211 were defined.

1. Entered set nat source rule 10 outbound-interface eth0 to set the uplink to the router.
2. Entered set nat source rule 10 source address 172.16.11.0/24 to set the inside router address.
3. Typed set nat source rule 10 translation address masquerade to allow the router translate multiple addresses to one IP.

VLAN 11

1. Entered set interface ethernet eth1 vif 11 description ‘VLAN 11’ to set a description.
2. Entered set interface ethernet eth1 vif 11 address 192.168.11.1/24 to give an address to the virtual interface.
3. Entered set nat source rule 11 outbound-interface eth0 to set eth0 as the uplink.
4. Entered set nat source rule 11 source address 192.168.11.0/24 to set the source address.
5. Typed set nat source rule 11 translation address masquerade to allow the interface to translate multiple addresses to one IP.

VLAN 111

1. Entered set interface ethernet eth1 vif 111 description ‘VLAN111’to set a description.
2. Configured set interface ethernet eth1 vif 111 address 192.168.111.1/24 to give an address to the virtual interface.
3. Entered set nat source rule 111 outbound-interface eth0to set eth0 as the uplink.
4. Used set nat source rule 111 source address 192.168.111.0/24to set the source address.
5. Typed set nat source rule 111 translation address masquerade to allow the interface to translate multiple addresses to one IP.

VLAN 211

1. Entered set interface ethernet eth1 vif 211 description “VLAN211’to set a description.
2. Entered set interface ethernet eth1 vif 211 address 192.168.211.1/24to give an address to the virtual interface.
3. Entered set nat source rule 211 outbound-interface eth0to set eth0 as the uplink.
4. Entered set nat source rule 211 source address 192.168.211.0/24to set the source address.
5. Typed set nat source rule 211 translation address masquerade to allow the interface to translate multiple addresses to one IP.
6. Entered set service ssh port ‘22’ to enable SSH and set the default port on the VyOS device.

## Create username/password and VLAN Configuration on Cisco Switches

Similar to the creation of a user on the VyOS router, the Cisco switches also needed usernames and passwords to be implemented to protect them from unauthorized access. The passwords for the created user accounts were also made invisible, or “secret,” in the switches’ configuration files as well as encrypted.

1. Enter the configuration mode by entering the command conf t.
2. Set the username and password with the command username cisco password SWcnit344.
3. Set the secret password by entering enable secret SWcnit344.
4. Encrypt the passwords with the command service password-encryption.
5. Named the VLAN 11 with vlan 11 | name “vlan 11”.
6. Named the VLAN 111 with vlan 111 | name “vlan 111”.
7. Named the VLAN 211 with vlan 211 | name “vlan 211”.

## Enabling SSH on the Cisco switches

Secure Shell (SSH) Protocol was enabled on the Cisco switches to allow remote access to the switches without the need of a physical serial connection. A pair of RSA keys needed to be generated so that the SSH connection would be encrypted.

1. Enter the configuration mode on the switches by entering the command config t.
2. Set the hostname of the switches using the command hostname (s1, s2, & s3).
3. Set the domain name of the network with *ip domain-name cit.lcl.*
4. Generate the RSA keys with the command crypto key generate rsa.
5. Enter *1024* for the bits in the modulus of the RSA key.
6. Returned to previous configuration mode with the command *Exit.*
7. Entered the VTY configuration lines with *line vty 0 15.*
8. Set the input lines for ssh access with transport input ssh.
9. Set login access for the vty lines with login local.
10. Returned to previous configuration mode with the command Exit.
11. Configured the console with the command line console 0.
12. Enable logging for the console lines with logging synchronous.
13. Set login access for the console lines with login local.
14. Returned to privileged mode with the command End and save with wr.
15. Used ssh -oKeyAlgorithms=+diffie-hellman-group1-sha1 -c aes256-cbc cisco@192.168.11.[10,11, or 12 depending on the switch] on PuTTY to remotely log into the switch.

## Configuring VLAN interfaces for Cisco switches

The three VLANs also had to be defined on each of the Cisco switches.

1. Used int vlan 11 | ip address 192.168.11.11 255.255.255.0
2. Entered int vlan 111 | ip address 192.168.111.11 255.255.255.0
3. Typed int vlan 211 | ip address 192.168.211.11 255.255.255.0

(for Cisco Switch 2 [s2]) :

1. Used int vlan 11 | ip address 192.168.11.12 255.255.255.0
2. Entered int vlan 111 | ip address 192.168.111.12 255.255.255.0
3. Typed int vlan 211 | ip address 192.168.211.12 255.255.255.0

## Configure trunk for VLANs on Cisco switch 1 (s1)

In order for the devices in each VLAN to communicate with each other, the three switches required trunking to be enabled on set ports that connected each switch to other devices. The mode of the desired ports was set to ‘trunk’ and the encapsulation mode was set to ‘dot1q’.

1. Used en | conf t | interface gi 1/0/35 to enter port 35 configuration.
2. Typed switchport mode trunk to switch the port mode to trunk the VLANs.
3. Used switchport trunk encapsulation dot1q to change the encapsulation mode.
4. Entered switchport access vlan 211 to allow the VLAN to function as an access port.
5. Typed en | conf t | interface gi 1/0/47 to enter port 47 configuration (HP trunk).
6. Entered switchport mode trunkto switch the port mode to trunk the VLANs.
7. Used switchport trunk allowed vlan all to add all VLANs to the HP trunk.
8. Typed exit | interface gi 1/0/48 to enter port 48 configuration (Second Cisco trunk).
9. Typed switchport mode trunkto switch the port mode to trunk the VLANs.
10. Used switchport trunk encapsulation dot1q to change the encapsulation mode.
11. Typed switchport trunk allowed vlan all to add all VLANs to the Cisco trunk.
12. Used interface gi 1/0/25 | switchport access vlan 211 | switchport mode access to allow pc access to the VLAN.

## Configure trunk for VLANs on Cisco Switch 2 (s2)

The same methods of configuring trunking were used on the second Cisco switch as well.

1. Used en | conf t | interfaces gi 3/0/48 to enter port 48 configuration.
2. Typed switchport mode trunkto switch the port mode to trunk the VLANs.
3. Used switchport trunk encapsulation dot1q to change the encapsulation mode.
4. Typed switchport trunk allowed vlan all to add all VLANs to the Cisco trunk.
5. Used switchport mode accessto allow interface access.
6. Entered switchport access vlan 111 to allow PC1 to access VLAN 111.

## HP Procurve Switch Configuration

Now that both of the Cisco switches were set up correctly, the same configurations had to be made on the HP Procurve switch as well. Trunking, user passwords, SSH, and VLANs were configured for the third and final switch.

Trunking

1. Used menu to access the Aruba menu.
2. Navigated to *VLAN | Port assignment* and changed port 23 to *No | Tagged | Tagged | Tagged*.
3. Changed port 12 to *No | No | No | untagged.*
4. Saved and closed the menu.

Passwords and SSH

1. Entered Conf t | password manager to set a manager password.
2. Used password operator to set an operator password.
3. Used conf t | ip ssh to enable ssh.
4. Entered crypto key generate ssh to create an ssh encryption key for the connection.
5. Used sh ip host-public-key fingerprintto check the public key.

VLAN Configurations

1. Used vlan 11 | name “vlan 11” | ip address 192.168.11.10 255.255.255.0.
2. Used vlan 111 | name “vlan 111” | ip address 192.168.111.10 255.255.255.0
3. Entered vlan 211 | name “vlan 211” | ip address 192.168.211.10 255.255.255.0

## Windows 10 IIS Web Configuration

Using NAT protocol, the VyOS router would be able to allow access to a default website hosted on PC1 using Windows’ Internet Information Services (IIS). IIS needed to be installed on PC1 and proper destination rules needed to be set on the VyOS router to allow access to the website.

1. Navigated to *Control Panel* | *Turn Windows Features On or Off* and checked “Internet Information Services” and “Internet Information Services Hostable Web Core”.
2. Opened IIS by searching “IIS” In the Windows search bar.
3. Used set nat destination rule 100 destination port ‘80’on the VyOS router to set the DNAT port to port 80.
4. Entered set nat destination rule 100 protocol ‘tcp’ to set NAT for TCP.
5. Used set nat destination rule 100 inbound-interface any to add a label.
6. Set nat destination rule 100 translation address 192.168.111.100 to put all traffic from port 80 to that address.

## Cisco 2811/2901 Router Initial Configuration

To first allow access to the new Cisco router, the router needed to be reset before configuration could begin, which was done by putting the router in ‘rommon’ mode. Once reset, the router could be configured, including setting the router name and enabling SSH access.

1. Turned off the Cisco router and turned it back on and pressed ‘ctrl + break’ on a keyboard to enter *rommon* mode.
2. Entered confreg 0x2142 | reset to set the registrar to ignore the startup-config (NVRAM) on reboot and to reload the router.
3. Entered config-register 0x2102 to set the configuration register back to default after reboot
4. Used hostname r1in config terminal mode to change the name of the switch.
5. Set the domain name of the network with ip domain-name cit.lcl.
6. Generate the RSA keys with the command crypto key generate rsa.
7. Enter *1024* for the bits in the modulus of the RSA key.
8. Set the username password with the command username cisco password RTcnit344.
9. Configure the VTY lines with line vty 0 15*.*
10. Set the input for ssh access with transport input sshand login local to set it at login.
11. Returned to previous configuration mode with the command Exit*.*
12. Configured the console with the command line console 0*.*
13. Enable logging for the console lines with logging synchronous*.*
14. Set login access for the console lines with login local*.*
15. Returned to privileged mode with the command End and save with wr*.*

## DNS/DHCP Configurations for Cisco Router

Just like the VyOS router, DHCP and DNS needed to be configured to allow the devices to automatically be assigned IP information based on their VLANs.

1. Used ip dns server | ip dhcp pool VLAN11 to enable dns and create a DHCP pool named ‘VLAN11’.
2. Used default-router 192.168.11.1 255.255.255.0to set the default router.
3. Entered network 192.168.11.0 255.255.255.0 to set the network address.
4. Typed dns-server 10.2.1.11 | dns-server 10.2.1.12 to set the dns servers.
5. Entered ip dhcp excluded-address 192.168.11.1 192.168.11.99 | ip dhcp excluded-address 192.168.11.201 192.168.11.254 to exclude all unused IPs for the VLANs.
6. Used ip dns server | ip dhcp pool VLAN111 to enable dns and create a DHCP pool named ‘VLAN111’.
7. Used default-router 192.168.111.1 255.255.255.0to set the default router.
8. Entered network 192.168.111.0 255.255.255.0 to set the network address.
9. Typed dns-server 10.2.1.11 | dns-server 10.2.1.12 to set the dns servers.
10. Entered ip dhcp excluded-address 192.168.111.1 192.168.111.1 99 | ip dhcp excluded-address 192.168.111.201 192.168.111.254 to exclude all unused IPs for the VLANs.
11. Used ip dns server | ip dhcp pool VLAN211 to enable dns and create a DHCP pool named ‘VLAN211’.
12. Used default-router 192.168.211.1 255.255.255.0to set the default router.
13. Entered network 192.168.211.0 255.255.255.0 to set the network address.
14. Typed dns-server 10.2.1.11 | dns-server 10.2.1.12 to set the dns servers.
15. Entered ip dhcp excluded-address 192.168.211.1 192.168.211.1 99 | ip dhcp excluded-address 192.168.211.201 192.168.211.254 to exclude all unused IPs for the VLANs.

## NAT, IP, and VLAN Configurations for Cisco Router

NAT, IP, and VLANs would also need to be reconfigured on the Cisco router with the same parameters as the VyOs router.

1. Used Interface gigabitEthernet0/0 | ip nat outside to set the upstream.
2. Entered interface gigabitEthernet0/1 | ip nat inside to set the downstream.
3. Typed access-list 1 permit 192.168.11.0 0.0.0.255 to set the VLAN11 NAT.
4. Retyped step 3 for VLAN 111 and 211.
5. Used ip nat inside source list 1 interface gigabitEthernet0/0 overload*.*
6. Entered int gigabitEthernet 0.0 to enter the interface.
7. Used ip address 10.25.11.254 255.255.255.0 to set the IP for the router.
8. Typed exit to get out of the interface.
9. Usedint g0/1.11 | encapsulation dot1Q 11to create the vlan.
10. Entered ip address 192.168.11.1 255.255.255.0 to set the ip of the vlan.
11. Usedint g0/1.111 | encapsulation dot1Q 111to create the vlan.
12. Entered ip address 192.168.111.1 255.255.255.0 to set the ip of the vlan.
13. Usedint g0/1.211 | encapsulation dot1Q 211to create the vlan.
14. Entered ip address 192.168.211.1 255.255.255.0 to set the ip of the vlan.
15. Typed ip route 0.0.0.0 0.0.0.0 10.25.11.1to set the default route.

## Creating SPAN session for Cisco router Wireshark captures

A Switched Port Analyzer (SPAN) session was used to capture data being sent between VLANS. PC3 was used as the monitoring PC to relay information sent between the VLANS, while PC2 used Wireshark to capture the data echoed by PC3. Answers to questions about the traffic that Wireshark captured can be found in Appendix A.

1. Used monitor session 1 source interface Gi1/0/35 to configure a monitoring session for Switch 1 uplink to monitor all VLAN traffic.
2. Entered monitor session 1 destination interface Gi1/0/10 encapsulation dot1q to set the destination wireshark monitoring interface to include dot1q VLAN traffic in the SPAN session.
3. Captured dot1q traffic and monitored ingress/ egress packets in wireshark.
4. Used no monitor session 1 to clear the SPAN session
5. Used monitor session 1 source interface Gi1/0/11 to configure a monitoring session on Switch 1 to monitor traffic from VLAN 111 coming from PC1.
6. Entered monitor session 1 destination interface Gi1/0/10 encapsulation dot1q to set the destination wireshark monitoring interface to capture packets coming from PC 1 on VLAN 111.

## Capturing an 802.1Q tag within a frame in transit outside the network

To view the contents of a frame with an 802.1Q tag, traveling outside the network, one PC was required to access a public website in order to have the frame sent beyond the local network. PC3 accessed http://www.espn.com for this purpose. While the frame was sent, Wireshark was opened on PC2 and isolated a frame containing the desired tag. Answers to questions relating to the 802.1Q tag can be found in Appendix A.

# RESULTS

The outcome of the work for this lab resulted in a small scale example of a computer network in an enterprise environment. Different devices have been assigned to different VLANs to simulate groups of PCs in certain departments or locations having their own virtual networks for a more efficient system of information transfer. The switches connecting these VLANs have trunking enabled to allow data to be quickly sent between VLANs if the need arises. Enterprise environments also normally contain a large number of PCs requiring their own IP addresses, so DHCP services have been accurately enabled on the router to automatically assign TCP/IP settings to each computer.

The architecture of the network resembles a “router on a stick” configuration, with the router of the network connected to the main switch. In this specific instance, the main switch is also connected to two other switches, resulting in three total switches that connect to three PCs. Trunking has been enabled between the router and the main switch, as well as between each switch-to-switch connection.

The figures below show physical and logical network diagrams of the network. Note that the layouts of the networks are the same whether the VyOS or Cisco router were used.

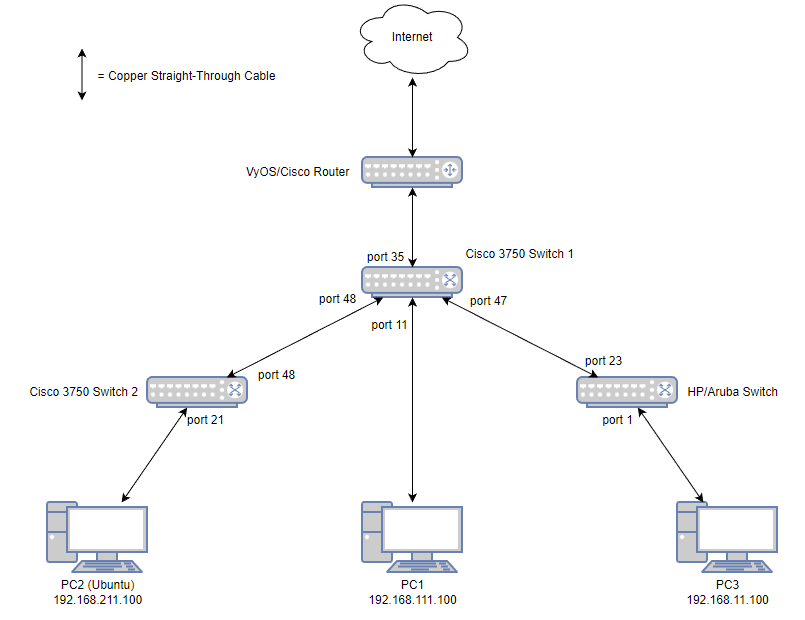


Figure 1: Physical Network Diagram. Note: Some port numbers differ from those mentioned in the Procedures section. The diagram represents the final port allocations for the network.

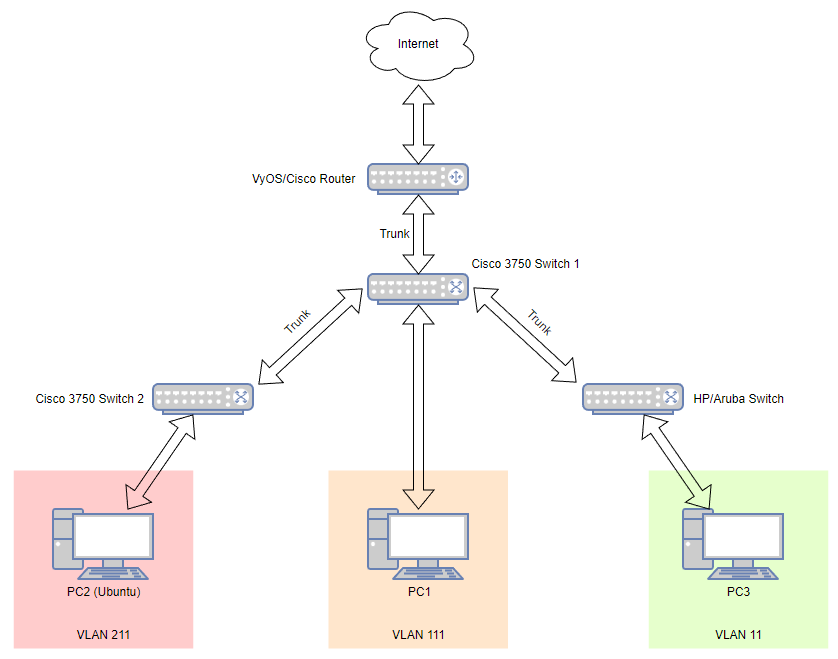


Figure 2: Logical Network Diagram

# References

*Bridge*. Bridge - VyOS 1.3.x (equuleus) documentation. (n.d.). Retrieved October 20, 2022, from https://docs.vyos.io/en/equuleus/configuration/interfaces/bridge.html

*Cisco Press*. DHCP and Easy IP > CCNP 1: Advanced IP Addressing Management | Cisco Press. (n.d.). Retrieved October 20, 2022, from https://www.ciscopress.com/articles/article.asp?p=330807&seqNum=8

*Cisco Router Setup Guide and TUTORIAL HOWTO with commands and examples*. rtt - IT Resource. (n.d.). Retrieved October 20, 2022, from http://realtechtalk.com/Cisco\_Router\_Setup\_Guide\_and\_Tutorial\_Howto\_With\_Commands\_and\_Examples-2171-articles

Cisco. (2021, September 23). *Password recovery for the 2900 Integrated Services Router*. Cisco. Retrieved October 20, 2022, from https://www.cisco.com/c/en/us/support/docs/routers/2800-series-integrated-services-routers/112033-c2900-password-recovery-00.html

Community.hpe.com. (n.d.). Retrieved October 20, 2022, from https://community.hpe.com/t5/switches-hubs-and-modems/remove-config-lines/td-p/4563667

*Configuring trunk ports on the HP Procurve*. Configuring Trunk Ports on the HP Procurve Comments. (n.d.). Retrieved October 20, 2022, from https://www.techieshelp.com/configuring-trunk-ports-on-the-hp-procurve/

Deadman, R. (2022, September 14). Lab 2 - Wireless Router/Enterprise Router [Lab Manual]. D2L Brightspace. https://purdue.brightspace.com/d2l/le/dropbox/598194/641311/DownloadAttachment?fid=21500970

Enterprise, H. P. (n.d.). *Support center*. Document Display | HPE Support Center. Retrieved October 20, 2022, from https://support.hpe.com/hpesc/public/docDisplay?docId=c02597101

*Login/user management*. Login/User Management - VyOS 1.4.x (sagitta) documentation. (n.d.). Retrieved October 20, 2022, from https://docs.vyos.io/en/latest/configuration/system/login.html

*Quick start*. Quick Start - VyOS 1.4.x (sagitta) documentation. (n.d.). Retrieved October 20, 2022, from https://docs.vyos.io/en/latest/quick-start.html

*Static*. Static - VyOS 1.3.x (equuleus) documentation. (n.d.). Retrieved October 20, 2022, from https://docs.vyos.io/en/equuleus/configuration/protocols/static.html#static-routing

Tatham, S (2022). PuTTY. https://www.putty.org/.

*VLAN - configuring Vlan Trunks [Cisco Catalyst 3850 series switches]*. Cisco. (2013, November 7). Retrieved October 20, 2022, from https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2\_0\_se/multibook/configuration\_guide/b\_consolidated\_config\_guide\_3850\_chapter\_0100010.html

*VLAN sub-interfaces (802.1Q)*. VyOS. (n.d.). Retrieved October 20, 2022, from https://support.vyos.io/en/kb/articles/vlan-sub-interfaces-802-1q-2

*Wireless Modes and Channels*. Wireless modes and channels. (n.d.). Retrieved October 20, 2022, from https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/wireless/ap\_about\_wireless\_modes\_c.html

*WLAN/WIFI - Wireless LAN*. WLAN/WIFI - Wireless LAN - VyOS 1.3.x (equuleus) documentation. (n.d.). Retrieved October 20, 2022, from https://docs.vyos.io/en/equuleus/configuration/interfaces/wireless.html

W. Nasr (Personal communication, October 10, 2022).

# APPENDICES

## Appendix A: Questions and Answers

Compare the number of ingress and egress frames. Explain.

Ingress frames are what come into the router or switch, while egress frames take the path out of the switch or router to go to its destination. Wireshark was used to capture each kind of frame by setting the filter to the source MAC address for the ingress packets and the destination MAC address for the egress packets. The number of ingress frames were about the same as egress frames, which makes sense as the frames that go into the switch/router, aside from headers stripped off, should be the same as frames going out of the devices.

What is the correlation between octets and frames?

An ethernet frame will have a maximum size limit it can transverse the network, which can be identified by combining the ethernet header, the payload, and the Frame Check Sequence field. This comes to a total of 1518 bytes, or 1518 octets of bits, which is the final form the file data takes before being put onto the wire. An octet is the smallest significant piece of information in regards to the network, before being put onto the wire.

Describe each fields’ purpose and function.

The different fields of the 802.1q tag within the frame are identified as the Tag Protocol Identifier, Priority, Canonical Format Indicator, and the VLAN ID. The Tag Protocol Identifier, or TPID, indicates the type of the frame. The Priority field is used by the switch to indicate fram priority in case congestion occurs. The Canonical Format Indicator, or CFI, indicates if the MAC address is encapsulated in canonical format, which is used to ensure compatibility between Ethernet and token ring networks. The final field in the 802.1q tag is the VLAN ID field used to tag different VLANs and is a range from 0 to 4095.

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

Egress frames are sent out with an 802.1Q tag when they are associated with a particular VLAN and can be sent across switches and routers. When the frame is sent to the correct recipient, the tag is stripped off and the data is fully transmitted to the host with the correct corresponding VLAN IP. Frames without an 802.1Q tag are captured in Wireshark when the tag has been stripped off and is seen as an ingress frame without a tag coming inwards. Once the frame gets on the path to the host that it needs, there is no longer a need for it to keep the tag.

## Appendix B: Passwords and SSH Keys

VyOS Router Login: [INITIALS]cnit344; g11c240-344  
Cisco Router Login: cisco; RTcnit344  
Cisco Switches Login: cisco: SWcnit344  
HP Switch Login: SWcnit344

SSH into the switches from VyOS router: ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c aes256-ctr cisco@192.168.11.[10(HP), 11(S1), or 12(S2)]

SSH into the switches from Cisco router: ssh -c 3des -l [cisco, manager] 192.168.11.[10(HP), 11(S1), or 12(S2)]

## 

## Appendix C: Router Configurations

VyOS Router

interfaces

ethernet eth0

address 10.25.11.254/24

hw-id 00:a7:3f:69:17:f4

ethernet eth1

hw-id 00:a7:3f:69:17:f5

vif 11

address 192.168.11.1/24

description "VLAN 11"

vif 111

address 192.168.111.1/24

Description “VLAN 111”

vif 211

address 192.168.211.1/24

description "VLAN 211"

ethernet eth2

hw-id 00:a7:3f:69:17:f6

ethernet eth3

hw-id 00:a7:3f:69:17:f7

ethernet eth4

hw-id 00:a7:3f:69:17:f8

ethernet eth5

hw-id 00:a7:3f:69:17:f9

loopback lo

wireless wlan0

address 172.16.11.1/24

channel 2

country-code us

description "Group 11 Wireless Network"

disable

hw-id 68:5d:43:61:db:b3

mode g

physical-device phy0

security

wpa

passphrase \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ssid c240-344g11

type access-point

nat

destination

rule 100

description "Port Forward Web Server"

destination

port 80

inbound-interface any

protocol tcp

translation

address 192.168.111.100

source

rule 10

outbound-interface eth0

source

address 172.16.11.0/24

translation

address masquerade

rule 11

outbound-interface eth0

source

address 192.168.11.0/24

translation

address masquerade

rule 111

outbound-interface eth0

source

address 192.168.111.0/24

translation

address masquerade

rule 211

outbound-interface eth0

source

address 192.168.211.0/24

translation

address masquerade

protocols

static

route 0.0.0.0/0

next-hop 10.25.11.1

service

dhcp-server

shared-network-name VLAN11

subnet 192.168.11.0/24

default-router 192.168.11.1

name-server 10.2.1.11

name-server 10.2.1.12

range 0

start 192.168.11.100

stop 192.168.11.200

shared-network-name VLAN111

subnet 192.168.111.0/24

default-router 192.168.111.1

name-server 10.2.1.11

name-server 10.2.1.12

range 0

start 192.168.111.100

stop 192.168.111.200

shared-network-name VLAN211

subnet 192.168.211.0/24

default-router 192.168.211.1

name-server 10.2.1.11

name-server 10.2.1.12

range 0

start 192.168.211.100

stop 192.168.211.200

shared-network-name WLAN

subnet 172.16.11.0/24

default-router 172.16.11.1

name-server 10.2.1.11

range 0

start 172.16.11.100

stop 172.16.11.200

dns

forwarding

allow-from 0.0.0.0/0

listen-address 172.16.11.1

listen-address 192.168.11.1

listen-address 192.168.111.1

listen-address 192.168.211.1

name-server 10.2.1.11

name-server 10.2.1.12

ssh

port 22

system

config-management

commit-revisions 100

conntrack

modules

ftp

h323

nfs

pptp

sip

sqlnet

tftp

console

device ttyS0

speed 115200

host-name vyos

login

user echammon

authentication

encrypted-password \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

user long325

authentication

encrypted-password \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

user sturmc

authentication

encrypted-password \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

user vyos

authentication

encrypted-password \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ntp

server time1.vyos.net

server time2.vyos.net

server time3.vyos.net

syslog

global

facility all

level info

facility protocols

level debug

Cisco 2901 Router

version 15.7

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname r1

boot-start-marker

boot-end-marker

enable secret 5 $1$5Zj0$T.oOhzVxxmqDhdb02ZBXx/

no aaa new-model

ip dhcp excluded-address 192.168.11.1 192.168.11.99

ip dhcp excluded-address 192.168.11.201 192.168.11.254

ip dhcp excluded-address 192.168.111.1 192.168.111.99

ip dhcp excluded-address 192.168.211.1 192.168.211.99

ip dhcp excluded-address 192.168.111.201 192.168.111.254

ip dhcp excluded-address 192.168.211.201 192.168.211.254

ip dhcp pool VLAN11

network 192.168.11.0 255.255.255.0

default-router 192.168.11.1 255.255.255.0

dns-server 10.2.1.11 10.2.1.12

ip dhcp pool VLAN111

network 192.168.111.0 255.255.255.0

default-router 192.168.111.1 255.255.255.0

dns-server 10.2.1.11 10.2.1.12

ip dhcp pool VLAN211

network 192.168.211.0 255.255.255.0

default-router 192.168.211.1 255.255.255.0

dns-server 10.2.1.11 10.2.1.12

ip domain name cit.lcl

ip name-server 10.2.1.11

ip name-server 10.2.1.12

ip cef

no ipv6 cef

multilink bundle-name authenticated

license udi pid CISCO2901/K9 sn FJC1905A316

username cisco password 7 122B31141C0218577E7F

redundancy

interface Embedded-Service-Engine0/0

no ip address

shutdown

interface GigabitEthernet0/0

ip address 10.25.11.254 255.255.255.0

ip nat outside

ip virtual-reassembly in

duplex auto

speed auto

interface GigabitEthernet0/1

no ip address

ip nat inside

ip virtual-reassembly in

duplex auto

speed auto

interface GigabitEthernet0/1.11

encapsulation dot1Q 11

ip address 192.168.11.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/1.111

encapsulation dot1Q 111

ip address 192.168.111.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/1.211

encapsulation dot1Q 211

ip address 192.168.211.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface Serial0/0/0

no ip address

shutdown

clock rate 2000000

ip forward-protocol nd

no ip http server

no ip http secure-server

ip nat inside source list 1 interface GigabitEthernet0/0 overload

ip nat inside source list 2 interface GigabitEthernet0/0 overload

ip nat inside source list 3 interface GigabitEthernet0/0 overload

ip route 0.0.0.0 0.0.0.0 10.25.11.1

ip ssh version 2

access-list 1 permit 192.168.11.0 0.0.0.255

access-list 2 permit 192.168.111.0 0.0.0.255

access-list 3 permit 192.168.211.0 0.0.0.255

control-plane

vstack

line con 0

logging synchronous

login local

line aux 0

line 2

no activation-character

no exec

transport preferred none

transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

stopbits 1

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

scheduler allocate 20000 1000

end

## 

## Appendix D: Switch Configurations

Switch 1

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname s1

boot-start-marker

boot-end-marker

enable secret 5 $1$6CST$5Ws2EJu.reI4AxshKRtKJ0

username cisco password 7 03376C080806351F1A5D

no aaa new-model

switch 1 provision ws-c3750e-48pd

system mtu routing 1500

ip domain-name cit.lcl

crypto pki trustpoint TP-self-signed-226055936

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-226055936

revocation-check none

rsakeypair TP-self-signed-226055936

crypto pki certificate chain TP-self-signed-226055936

certificate self-signed 01

30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 32323630 35353933 36301E17 0D313130 33333030 31323931

375A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F

532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3232 36303535

39333630 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100

F51AB902 F5A756D9 7703F3A7 E1C6AAFF E70391D3 C8414F32 F7B53035 7DEF420D

BA991260 A08468C5 4A239AF0 8EBADA0D 6480CF18 89636E0B 419866E4 6F82EEB9

24DC9F2C 2060BF37 18331BCC 421E1F8D D1B5F4B5 A17DBCE3 F04903B8 0DE8F6C9

8F611E5D FA542EE5 86603396 24D11CC0 7AAF6FF4 25FE8BE1 3B9F45BC 1073CF07

02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D

23041830 16801489 4788099D 6D696E95 B2C49BFD B3E3F73A ED5B5730 1D060355

1D0E0416 04148947 88099D6D 696E95B2 C49BFDB3 E3F73AED 5B57300D 06092A86

4886F70D 01010505 00038181 00686416 3C86C8C4 75D2E03A DE3B2F3E 076CB98D

0A2B5124 7D7D8E44 17B10203 854DBA01 66006C27 E096D2CF 5FD2075C 1DC7849E

C73CF3CB 6E786007 85E1AFF6 15853EE3 96CFD019 1FD8A2E1 727A359F 31228E4C

184599C1 F77F305F DF3F5FE8 0822AECB B90FFB35 752232F3 38DC7DB8 2B4B68D4

3C495B3B 1CD70BFF 45758584 FB

quit

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

interface FastEthernet0

no ip address

interface GigabitEthernet1/0/1

switchport access vlan 11

switchport mode access

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 111

switchport mode access

interface GigabitEthernet1/0/12

interface GigabitEthernet1/0/13

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

switchport access vlan 211

switchport mode access

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

description "CIT Uplink"

switchport trunk encapsulation dot1q

switchport mode trunk

interface GigabitEthernet1/0/36

interface GigabitEthernet1/0/37

interface GigabitEthernet1/0/38

interface GigabitEthernet1/0/39

interface GigabitEthernet1/0/40

interface GigabitEthernet1/0/41

interface GigabitEthernet1/0/42

interface GigabitEthernet1/0/43

interface GigabitEthernet1/0/44

interface GigabitEthernet1/0/45

interface GigabitEthernet1/0/46

interface GigabitEthernet1/0/47

switchport trunk encapsulation dot1q

switchport mode trunk

interface GigabitEthernet1/0/48

switchport trunk encapsulation dot1q

switchport mode trunk

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 Vlan11

ip address 192.168.11.11 255.255.255.0

interface Vlan111

ip address 192.168.111.11 255.255.255.0

interface Vlan211

ip address 192.168.211.11 255.255.255.0

ip http server

ip http secure-server

line con 0

login local

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

end

Switch 2

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname s2

boot-start-marker

boot-end-marker

enable secret 5 $1$z8iH$E3e6hXZBL0Be6TjyZF9.j/

username cisco password 7 012031075502125C7518

no aaa new-model

switch 2 provision ws-c3750e-48pd

system mtu routing 1500

ip domain-name cit.lcl

crypto pki trustpoint TP-self-signed-3397340800

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-3397340800

revocation-check none

rsakeypair TP-self-signed-3397340800

crypto pki certificate chain TP-self-signed-3397340800

certificate self-signed 01

3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 33333937 33343038 3030301E 170D3131 30333330 30313239

32315A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649

4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 33393733

34303830 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281

8100AAFD B9EEA1FE 84F81832 5BF1BF37 34131739 8C90F6A0 587C352D 6DBB0521

5EDC1929 C48FDA19 49D4883C 7ACBA271 57B20283 4AAD56EB C2D73094 CBAF0C28

0C565A38 37F1153A 3378FA1D A3041905 A2BF64D7 A5A6B107 7E6B30E0 2C7444AD

EF3B6EEE 44D801F6 08EE7462 268C0F4E 5F7886B7 4E5745D0 5D1D1FCD FEF6FAFA

C6BF0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603

551D2304 18301680 14049082 C374348E E1992303 8B7C31A4 C61EB274 97301D06

03551D0E 04160414 049082C3 74348EE1 9923038B 7C31A4C6 1EB27497 300D0609

2A864886 F70D0101 05050003 8181007F E8924808 D2324FD5 086D95D3 8572F5A5

97EA406A 0DB3451F E9B14401 F4A26914 BAF1EE92 04D40478 B85F8824 E919F5A8

4DAD7417 F7652156 80F80398 46E091F9 509AA713 EB06B3E7 6BA827A6 1448E00B

1EF71F0D D8C04EE2 F38C8ED1 CEE6D7F0 B176CB99 B62E1BB6 ECE96BF8 93579FD3

91CC135B 8FD25039 3BD93339 3E239C

quit

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

interface FastEthernet0

no ip address

interface GigabitEthernet2/0/1

switchport access vlan 11

switchport mode access

interface GigabitEthernet2/0/2

interface GigabitEthernet2/0/3

interface GigabitEthernet2/0/4

interface GigabitEthernet2/0/5

interface GigabitEthernet2/0/6

interface GigabitEthernet2/0/7

interface GigabitEthernet2/0/8

interface GigabitEthernet2/0/9

interface GigabitEthernet2/0/10

interface GigabitEthernet2/0/11

switchport access vlan 111

switchport mode access

interface GigabitEthernet2/0/12

interface GigabitEthernet2/0/13

interface GigabitEthernet2/0/14

interface GigabitEthernet2/0/15

interface GigabitEthernet2/0/16

interface GigabitEthernet2/0/17

interface GigabitEthernet2/0/18

interface GigabitEthernet2/0/19

interface GigabitEthernet2/0/20

interface GigabitEthernet2/0/21

switchport access vlan 211

switchport mode access

interface GigabitEthernet2/0/22

interface GigabitEthernet2/0/23

interface GigabitEthernet2/0/24

interface GigabitEthernet2/0/25

interface GigabitEthernet2/0/26

interface GigabitEthernet2/0/27

interface GigabitEthernet2/0/28

interface GigabitEthernet2/0/29

interface GigabitEthernet2/0/30

interface GigabitEthernet2/0/31

interface GigabitEthernet2/0/32

interface GigabitEthernet2/0/33

interface GigabitEthernet2/0/34

interface GigabitEthernet2/0/35

interface GigabitEthernet2/0/36

interface GigabitEthernet2/0/37

interface GigabitEthernet2/0/38

interface GigabitEthernet2/0/39

interface GigabitEthernet2/0/40

interface GigabitEthernet2/0/41

interface GigabitEthernet2/0/42

interface GigabitEthernet2/0/43

interface GigabitEthernet2/0/44

interface GigabitEthernet2/0/45

interface GigabitEthernet2/0/46

interface GigabitEthernet2/0/47

interface GigabitEthernet2/0/48

interface GigabitEthernet2/0/49

interface GigabitEthernet2/0/50

interface GigabitEthernet2/0/51

interface GigabitEthernet2/0/52

interface TenGigabitEthernet2/0/1

interface TenGigabitEthernet2/0/2

interface Vlan1

no ip address

interface Vlan11

ip address 192.168.11.12 255.255.255.0

interface Vlan111

ip address 192.168.111.12 255.255.255.0

interface Vlan211

ip address 192.168.211.12 255.255.255.0

ip http server

ip http secure-server

line con 0

login local

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

transport input ssh

end

Switch 3

hostname "s3"

interface 12

lacp Passive

exit

interface 23

lacp Passive

exit

snmp-server community "public" Unrestricted

vlan 1

name "DEFAULT\_VLAN"

untagged 2-10,12-20,22,24

ip address dhcp-bootp

no untagged 1,11,21,23

exit

vlan 11

name "vlan 11"

untagged 1

ip address 192.168.11.10 255.255.255.0

tagged 23

exit

vlan 111

name "vlan 111"

untagged 11

ip address 192.168.111.10 255.255.255.0

tagged 23

exit

vlan 211

name "vlan 211"

untagged 21

ip address 192.168.211.10 255.255.255.0

tagged 23

exit

ip ssh

password manager

password operator