***Lab 4: Routing, NAT, and ACL***

CNIT34400-007  
Group 11  
Keegan Long  
Ethan Hammond  
Cade Sturm  
Submitted To: Waleed Nasr  
Date Submitted: 12/11/22  
Date Due: 12/11/22

TABLE OF CONTENTS

[EXECUTIVE SUMMARY](#_zhv8cg2l3ndv)……………………………………………………………………….. 5

[BUSINESS SCENARIO](#_2d58lusxew17)………………………………………………………………………….. 4

[PROCEDURES](#_k83df4s7vmej)…………………………………………………………………………………... 5

[Removing STP and Setting VLANs from the Switches](#_l30d1s6xt9ia)……………………………………… 5

[Point to Point Protocol Configuration on Router 1 & 2 (Cisco 2901 DTE, Cisco 1921 DCE)](#_ekolfnfbm2kz). 6

[RIP Configurations on Routers](#_qh9822avylv0)……………………………………………………………….. 6

[VyOS RIP Configurations](#_xv5hlphrfmud)…………………………………………………………………….. 7

[VLAN Reconfigurations](#_vv4x4jub4mzm)……………………………………………………………………… 9

[DHCP Configurations on Router 2](#_wck23k9egxi3)………………………………………………………….. 10

[NAT/PAT Configurations on Router 1 for ACLs](#_no9k5zrcuy9j)……………………………………………. 12

[TFTP Server Setup](#_g39bma6biqxm)…………………………………………………………………………... 13

[RESULTS](#_blxyvnksl32i)………………………………………………………………………………………... 15

REFERENCES………………………………………………………………………………….. 18

[APPENDIX A: ROUTER AND SWITCH CONFIGURATIONS](#_yfkkxnmmg7xg)……………………………… 20

# EXECUTIVE SUMMARY

This lab included the purging of MSTP from all switches on the network, removal of one of the switches, addition of a DCE DTE connection between two Cisco routers, and implementation of a distance vector routing protocol. The wired connection of a DCE DTE serial cable between the two Cisco routers required the configuration of Point to Point Protocol to choose a clock speed for the DCE connection to simulate a WLAN connection between the two routers. The network topology was set up with the Cisco switch, VyOS access point, and Router 1 on the left side of the network, and the Router 2 and HP switch on the right side of the network.

The next phase of the lab was to get the connections to work between all of the devices, implement Router Information Protocol (RIP), and add Access Control Lists (ACL) to permit and deny access of all network functionalities to the end devices. RIP was configured on Router 1 with entries for all 172.30.x.x networks as well as 192.169.x.x networks. Router 2 needed to have entries for all 192.168.x.x networks and 172.30.x.x networks to be able to update its routing table for VyOS and 168 networks to be transferred across routers.

This lab report includes a business scenario to explain the purpose of the lab, a procedures section to show how every task was carried out, a results section to explain the outcome of the lab, a references section for all sources that were used in the making of the lab, as well as an appendix for all networking devices’ configuration pages with Appendix A.

# BUSINESS SCENARIO

Patch cables and building wiring from KNOY 203 and KNOY 206 were used to rearrange all of the network architecture. Terminal programs like PuTTY and SecureCRT were used for all configurations of all networking devices. Configurations were modified for all Cisco routers, Cisco switches, VyOS routers, and HP switches. Patch cables in KNOY 203 were used to make connections between all of the devices to allow for network connectivity as well as SSH. Physical cables were also responsible for the layer 1 connection between the two Cisco routers with a DTE DCE connection. Console commands were used to configure the routers for Point-To-Point Protocol encapsulation for the DTE DCE connection to simulate a WLAN connection between the two routers. Console commands were used to set up PPP encapsulation, configure all VLANs, configure switch and router interfaces, implement Routing Information Protocol, as well as set up a VyOS router as an access point for wireless devices. New devices and network topologies in enterprise environments will always be changing and it is useful to know how to configure them.

RIP was configured through PuTTY on all 3 routers to allow Router 1 to know of all Router 2 networks, as well as both routers to know of all 172 VLAN networks from the VyOS wireless access point. This is useful in companies because wireless networks will always be used, and multiple routers allow for more traffic to be able to be routed efficiently across the network topology. Companies must use dynamic routing protocols to gain the benefits of not having to use static routing.

It was also necessary to configure the routers with ACLs to enhance the security measures on the network. Blocking ports from specific IPs in the network would be used by all enterprise IT environments to ensure all workers can use what they need to use and cannot use what they do not need to use. Large companies contain security risks and firewall rules are a way of blocking users’ access to services like HTTP that could pose a security risk to the integrity of a company’s data.

# PROCEDURES

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, folder navigation, and repetitive commands are shown with the pipe symbol and are *italicized*: *Start | Programs | MS Office | Word*.

## Removing STP and Setting VLANs from the Switches

As MSTP was configured in Lab 3, it must be taken off of the network to add the second router with a simulated WLAN connection with a PPP connection. In addition, adding the VyOS router as an access point will work easiest without MSTP configured on the switches.

1. Used no followed by all MSTP commands for the Aruba switch configurations to turn off STP.
2. Typed no followed by all MSTP commands for the Cisco switch 1 to turn off STP.
3. Typed no followed by all MSTP commands for the Cisco switch 2 to turn off STP.
4. Used interface g0/48 switchport access vlan 172to set the port to accept 172 VLAN traffic.
5. Entered interface g0/48 switchport mode access to switch the mode on the switches to allow VLAN 172 traffic.

## Point to Point Protocol Configuration on Router 1 and 2 (Cisco 2901 DTE, Cisco 1921 DCE)

Point to Point Protocol (PPP) needed to be configured on Router 1 and 2 after a physical connection was created with a DTE to DCE cable on Serial 0/0/0 with a specified clockrate on both routers. This was to simulate a WLAN connection between the two routers to work together.

1. Used int serial0/0/0 to get into the serial interface.
2. Entered encapsulation ppp to set the protocol encapsulation for the router.
3. Typed ip address 192.168.61.1 255.255.255.252 to set the IP address on 192.168.61.0/30 subnet.
4. Used int serial0/0/0 to get into the serial interface.
5. Entered encapsulation ppp to set the protocol encapsulation for the router.
6. Used clock rate 64000 to set the DCE serial interface clock rate.
7. Typed ip address 192.168.61.2 255.255.255.252 to set the IP address on 192.168.61.0/30.

## RIP Configurations on Routers

With multiple routers, switches, and a router acting as an access point, setting static routing tables for all devices was not practical. Therefore, a distance vector routing protocol was implemented called RIP to dynamically set routing tables to converge in the network.

Router 1 Configurations

1. Used router ripto enter the rip configuration.
2. Typed network 10.0.0.0 | network 192.168.61.0 | network 192.168.11.0 | network 192.168.111.0 | network 192.168.211.0 to establish all networks to be used by RIP.
3. Used no auto-summary to disable the auto summary feature.
4. Entered default-information originate to inform RIP of the default route.
5. Typed version 2 to change the RIP version to 2.
6. Used no validate-update-source to disable auto updates and not confuse RIP.

Router 2 Configurations

1. Used router ripto enter the rip configuration.
2. Typednetwork 192.169.61.0 | network 192.169.11.0 | network 192.169.111.0 | network 192.169.211.0 to establish all networks to be used by RIP.
3. Used no auto-summary to disable the auto summary feature.
4. Typed version 2 to change the RIP version to 2.
5. Used int gigabitethernet 0/1.11 ip address 192.169.11.0 | int gigabitethernet 0/1.111 ip address 192.169.111.0 | int gigabitethernet 0/1.211 ip address 192.169.211.0 to change all VLANs for RIP.

## VyOS RIP Configurations

RIP needed to be set not only on the routers, but all routers and access points if the access point was to be used as a WLAN. All routers needed to have the same RIP table configurations so they knew all of the networks.

1. Used set interfaces ethernet eth1 address 172.30.1.2/25 to set the virtual interface address.
2. Used Set protocols rip network 172.30.1.0/25 | 172.30.1.128/25 | 172.30.0.0/16 to set the network address on RIP.
3. Typed set protocols static router 172.30.1.0/25 next hop 172.30.1.1/25 to set the next router over.
4. Used set interfaces wireless wlan0 address 172.30.1.129/25 to set the address of the wireless network.
5. Entered set service dhcp-server shared-network-name WLAN subnet 172.30.1.128/25to set the ip for DHCP.
6. Used set service dhcp-server shared-network-name WLAN subnet 172.30.1.128/25 default-router 172.30.1.129 to set the default route.
7. Entered set service dhcp-server shared-network-name WLAN subnet 172.30.1.128/25 name-server 10.2.1.11 | 10.2.1.12 to set the DHCP DNS servers.
8. Typed set service dhcp-server shared-network-name WLAN subnet 172.30.1.128/25 range 0 start 172.30.1.130 | stop 172.30.1.230 to set the range of leasing addresses.

## VLAN Reconfigurations

VLANs needed to be reconfigured on all networking devices after RIP was configured to allow the 172 IPs to flow through the network wirelessly through the VyOS AP. This was done through both routers and a switch of adding interfaces.

Router 1

1. Added the VyOS VLAN to the router with Interface GigabitEthernet0/1.172.
2. Used encapsulation dot1Q 172 to set the VLAN to be accessed.
3. Added the IP for the interface with ip address 172.30.1.1 255.255.255.0.
4. Permitted NAT on the VLAN with ip nat inside.

Router 2

1. Added the VyOS VLAN to the router with Interface GigabitEthernet0/1.172.
2. Used encapsulation dot1Q 172 to set the VLAN to be accessed.
3. Added the IP for the interface with ip address 172.30.1.1 255.255.255.0.
4. Permitted NAT on the VLAN with ip nat inside.

Cisco Switch

1. Added the VyOS VLAN to trunking ports on the Cisco switch with interface GigabitEthernet1/0/47 switchport access vlan 172 | switchport mode access.

HP Switch

1. Added the VyOS VLAN to trunking ports by navigating to the *menu* | *VLAN Configurations* and changing *VLAN 172* to *tagged*.

## DHCP Configurations on Router 2

DHCP had to be updated after RIP implementation to ensure that the 192.168.x.x and 192.169.x.x networks were set dynamically. Router 2 needed to be set to all 169 networks so that RIP can add them in the RIP routing table to be dynamically populated to the other routers.

1. Entered ip dhcp excluded-address 192.169.11.1 192.169.11.99 to start DHCP pool at 100 for 11 VLAN.
2. Used ip dhcp excluded-address 192.169.11.201 192.169.11.254 to end DHCP pool at 254 for 11 VLAN.
3. Typed ip dhcp excluded-address 192.169.111.1 192.169.111.99 to start DHCP pool at 100 for 111 VLAN.
4. Used ip dhcp excluded-address 192.169.211.1 192.169.211.99 to start DHCP pool at 100 for 211 VLAN.
5. Typed ip dhcp excluded-address 192.169.111.201 192.169.111.254 to end DHCP pool at 254 for 111 VLAN.
6. Used ip dhcp excluded-address 192.169.211.201 192.169.211.254 to end DHCP pool at 254 for 211 VLAN.
7. Entered ip dhcp pool VLAN11 followed by:
   1. network 192.169.11.0 255.255.255.0 to set the network address for VLAN 11.
   2. default-router 192.169.11.1 255.255.255.0 to set the default route for VLAN 11.
8. Entered ip dhcp pool VLAN111 followed by:
   1. network 192.169.111.0 255.255.255.0 to set the network address for VLAN 111.
   2. default-router 192.169.111.1 255.255.255.0 to set the default route for VLAN 111.
9. Entered ip dhcp pool VLAN211 followed by:
   1. network 192.169.211.0 255.255.255.0 to set the network address for VLAN 211.
   2. default-router 192.169.211.1 255.255.255.0 to set the default route for VLAN 211.
10. Modified subinterface for VLAN 11 by changing the ip address from 192.168.11.1 to 192.169.11.1 withinterface GigabitEthernet0/1.11 ip address 192.169.11.1 255.255.255.0.
11. Modified subinterface for VLAN 111 by changing the ip address from 192.168.111.1 to 192.169.111.1 withinterface GigabitEthernet0/1.111 ip address 192.169.111.1 255.255.255.0.
12. Modified subinterface for VLAN 211 by changing the ip address from 192.168.211.1 to 192.169.211.1 withinterface GigabitEthernet0/1.211 ip address 192.169.211.1 255.255.255.0.

## NAT/PAT Configurations on Router 1 for ACLs

Router 1 was the only router that required ACLs on it as it was the edge router before being sent to CIT-NET on the uplink port. ACLs were implemented such that users on the 111 VLAN were not able to access webpages, but the 11 and 211 VLANs were. Also, 172 users were to be the only users to be able to use TFTP with PC2.

1. Used access-list 100 permit tcp 192.168.11.0 0.0.0.255 any eq www to allow all HTTP connection for 168 networks.
2. Typed access-list 100 permit tcp 192.168.11.0 0.0.0.255 any eq 443 to allow all HTTPS connections for 168 networks.
3. Entered access-list 100 permit tcp 192.168.211.0 0.0.0.255 any eq www to allow 168 VLAN 211 to connect to HTTP.
4. Used access-list 100 permit tcp 192.168.211.0 0.0.0.255 any eq 443 to allow 168 VLAN 211 to connect to HTTPS.
5. Entered access-list 100 deny tcp any any eq 443 to deny all HTTPS access for everything else.
6. Entered access-list 100 deny tcp any any eq www to deny all HTTP access for everything else.
7. Used access-list 100 permit ip any any to allow all IP functionalities for internet.
8. Typed ip nat inside source list 100 interface GigabitEthernet0/0 overload to allow NAT to access outside the network.
9. Used ip nat pool NATPOOL 10.25.11.254 10.25.11.254 netmask 255.255.255.0 to set the pool of addresses for NAT.
10. Entered ip nat inside source list 100 pool NATPOOL overload to set NAT to masquerade.

Router 2 NAT/PAT Configurations

1. Entered access-list 101 permit udp 172.30.1.0 0.0.0.255 any eq tftp to allow 172 networks to use TFTP.
2. Used access-list 101 deny udp 192.168.0.0 0.0.255.255 any eq tftp to deny all other access to TFTP for 168 networks.
3. Entered access-list 101 permit ip any any to allow all other network access.
4. Used access-list 101 deny udp 192.169.0.0 0.0.255.255 any eq tftp to deny 169 networks TFTP access.
5. Typed ip access-group 101 out (**ON** interface Serial0/0/0) to assign NAT to an access group for ACLs.

## TFTP Server Setup

A TFTP server had to be set up on the Linux machine (PC2) to demonstrate ACL propagation from the networking devices. TFTP was set up using a CLI by installing TFTP and creating a directory for the filesystem. The Windows machine also had to install TFTP client to be able to interact with the Linux server.

PC2 (Ubuntu Machine)

1. Opened up a terminal window in Linux and typed sudo apt install tftpd-hpa to install TFTP server.
2. Used sudo nano /etc/default/tftpd-hpa to edit the config file of the TFTP server.
3. Modified the TFTP\_DIRECTORY variable path to /var/lib/tftpboot.
4. Created the /var/lib/tftpboot directory with sudo mkdir /var/lib/tftpboot.
5. Changed ownership of the directory with sudo chown echammon:echammon /var/lib/tftpboot.
6. Allowed all access to the directory with sudo chmod 777 /var/lib/tftpboot.
7. Added a test file in the directory using touch test.txt > /var/lib/tftpboot.

PC1 (Windows Machine)

1. Opened a Windows search bar and typed ‘Add or Remove Programs’ and selected *TFTP Client* from the selection and installed it.
2. Opened a CMD Window and typed TFTP -i [IP OF LINUX MACHINE] GET test.txt to test the TFTP server.

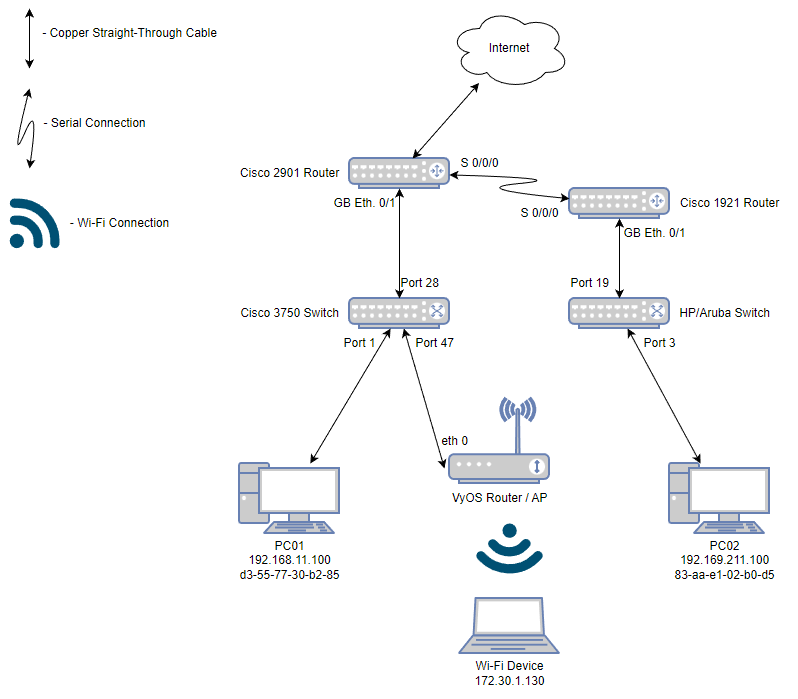
# 

# RESULTS

The outcome of this lab’s work results in two mirror networks (192.168.0.0/16 and 192.169.0.0/16) from each respective Cisco router, as well as the access point network 172.30.1.128/25. The RIPv2 protocol is used to route between the networks on each router, advertising each respective VLAN network for the RIPv2 instance, and advertising the point-to-point connection between the routers. Each Cisco router provides DHCP addresses to clients on each respective VLAN for the mirrored networks, and the VyOS device acting as the access point provides DHCP addresses to the clients on its /25 network.

The physical architecture of this network is straightforward and a mirrored design with an access point, although the logical access each VLAN has on the network are controlled from the router's access control lists. The ACL’s restrict Trivial File Transfer Protocol access to only originate from clients on the access point, as well as restrict web traffic to only 192.168.11.0/24 and 192.168.211.0/24 networks. These practices can encourage security policies and implement access control between networks. The remaining IP traffic on this network will be translated with NAT/PAT and will be accessible to the rest of the CIT domain.

Figure 1 illustrates the physical layout of the network, while figure 2 shows the logical layout.

Figure 1: Physical Network Topology

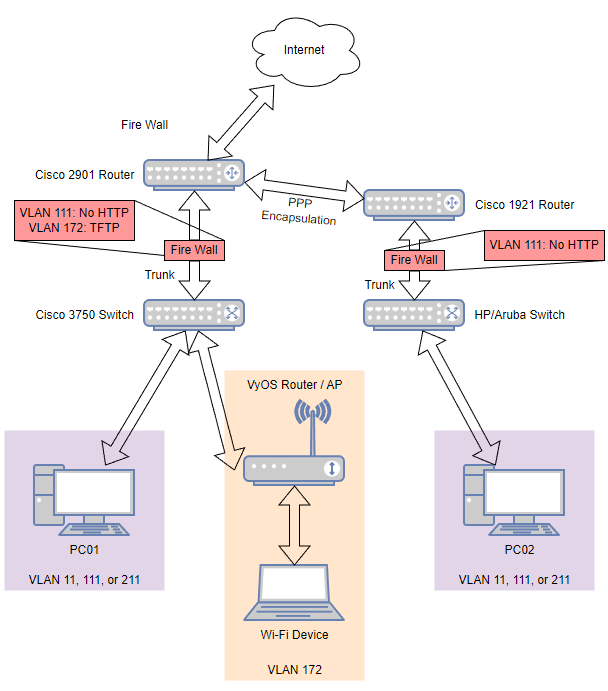


Figure 2: Logical Network Topology

# References

Deadman, R. (2022, December 11). Lab 4: Routing, NAT, and ACL [Lab Manual]. D2L Brightspace. https://purdue.brightspace.com/d2l/le/dropbox/598194/641332/DownloadAttachment?fid=21501172

Cisco. (2015, November 18). *IP routing: Rip Configuration Guide, Cisco Ios Release 15M&T - Configuring Routing Information protocol [cisco IOS 15.4M&T]*. Cisco. Retrieved December 11, 2022, from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\_rip/configuration/15-mt/irr-15-mt-book/irr-cfg-info-prot.html

Cisco. (2017, November 13). *Point-to-point protocol (PPP)*. Cisco. Retrieved December 11, 2022, from https://www.cisco.com/c/en/us/tech/wan/point-to-point-protocol-ppp/index.html

Cisco. (2022, October 7). *Configure and filter IP access lists*. Cisco. Retrieved December 11, 2022, from https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

J. Bennett (Personal communication, November 29, 2022)

*RIPv2 (routing information protocol)*. Cisco Community. (2019, March 1). Retrieved December 11, 2022, from https://community.cisco.com/t5/networking-knowledge-base/ripv2-routing-information-protocol/ta-p/3117425

*RIP*. RIP - VyOS 1.3.x (equuleus) documentation. (n.d.). Retrieved December 11, 2022, from https://docs.vyos.io/en/equuleus/configuration/protocols/rip.html

Stack Exchange (1966, January 1). *What's the difference between serial DCE and serial DTE Link?* Network Engineering Stack Exchange. Retrieved December 11, 2022, from https://networkengineering.stackexchange.com/questions/55017/whats-the-difference-between-serial-dce-and-serial-dte-link

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

Upravnik. (2022, August 13). *Configuring ripv2*. Study CCNA. Retrieved December 11, 2022, from https://study-ccna.com/configuring-ripv2/

W. Nasr (Personal communication, December 1, 2022).

# 

# 

# APPENDIX A: ROUTER AND SWITCH CONFIGURATIONS

-- g11rtr1 --

version 15.7

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname g11rtr1

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

description "CIT-Uplink"

ip address 10.25.11.254 255.255.255.0

ip nat outside

ip virtual-reassembly in

duplex auto

speed auto

interface GigabitEthernet0/1

description "Downstream"

no ip address

ip access-group 100 in

ip nat inside

ip virtual-reassembly in

duplex auto

speed auto

interface GigabitEthernet0/1.11

description "VLAN 11 Subinterface"

encapsulation dot1Q 11

ip address 192.168.11.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/1.111

description "VLAN 111 Subinterface"

encapsulation dot1Q 111

ip address 192.168.111.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/1.172

description "VLAN 172 Subinterface"

encapsulation dot1Q 172

ip address 172.30.1.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface GigabitEthernet0/1.211

description "VLAN 211 Subinterface"

encapsulation dot1Q 211

ip address 192.168.211.1 255.255.255.0

ip nat inside

ip virtual-reassembly in

interface Serial0/0/0

ip address 192.168.61.1 255.255.255.252

encapsulation ppp

clock rate 2000000

router rip

version 2

no validate-update-source

network 10.0.0.0

network 172.30.0.0

network 192.168.11.0

network 192.168.61.0

network 192.168.111.0

network 192.168.211.0

default-information originate

no auto-summary

ip forward-protocol nd

no ip http server

no ip http secure-server

ip nat pool NATPOOL 10.25.11.254 10.25.11.254 netmask 255.255.255.0

ip nat inside source list 100 pool NATPOOL overload

ip route 0.0.0.0 0.0.0.0 10.25.11.1

access-list 100 permit tcp 192.168.11.0 0.0.0.255 any eq www

access-list 100 permit tcp 192.168.11.0 0.0.0.255 any eq 443

access-list 100 permit tcp 192.168.211.0 0.0.0.255 any eq www

access-list 100 permit tcp 192.168.211.0 0.0.0.255 any eq 443

access-list 100 deny tcp any any eq 443

access-list 100 deny tcp any any eq www

access-list 100 permit ip any any

access-list 100 permit tcp 172.30.1.0 0.0.0.255 any eq 69

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

-- g11rtr2 --

version 15.7

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

hostname g11rtr2

boot-start-marker

boot-end-marker

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

no aaa new-model

ip dhcp excluded-address 192.169.11.1 192.169.11.99

ip dhcp excluded-address 192.169.11.201 192.169.11.254

ip dhcp excluded-address 192.169.111.1 192.169.111.99

ip dhcp excluded-address 192.169.211.1 192.169.211.99

ip dhcp excluded-address 192.169.111.201 192.169.111.254

ip dhcp excluded-address 192.169.211.201 192.169.211.254

ip dhcp pool VLAN11

network 192.169.11.0 255.255.255.0

default-router 192.169.11.1 255.255.255.0

dns-server 10.2.1.11 10.2.1.12

ip dhcp pool VLAN111

network 192.169.111.0 255.255.255.0

default-router 192.169.111.1 255.255.255.0

dns-server 10.2.1.11 10.2.1.12

ip dhcp pool VLAN211

network 192.169.211.0 255.255.255.0

default-router 192.169.211.1 255.255.255.0

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

no ip address

shutdown

interface GigabitEthernet0/1

description "Downstream"

no ip address

ip access-group 101 in

ip virtual-reassembly in

duplex auto

speed auto

interface GigabitEthernet0/1.11

description "VLAN 11 Subinterface"

encapsulation dot1Q 11

ip address 192.169.11.1 255.255.255.0

ip virtual-reassembly in

interface GigabitEthernet0/1.111

description "VLAN 111 Subinterface"

encapsulation dot1Q 111

ip address 192.169.111.1 255.255.255.0

ip virtual-reassembly in

interface GigabitEthernet0/1.211

description "VLAN 211 Subinterface"

encapsulation dot1Q 211

ip address 192.169.211.1 255.255.255.0

ip virtual-reassembly in

interface Serial0/0/0

ip address 192.169.61.2 255.255.255.252

encapsulation ppp

ip access-group 101 out

router rip

version 2

no validate-update-source

network 192.169.11.0

network 192.169.61.0

network 192.169.111.0

network 192.169.211.0

default-information originate

no auto-summary

ip forward-protocol nd

no ip http server

no ip http secure-server

ip route 0.0.0.0 0.0.0.0 192.169.61.1

access-list 101 permit tcp 172.30.1.0 0.0.0.255 any eq tftp

access-list 101 deny tcp 192.169.0.0 0.0.255.255 any eq tftp

access-list 101 permit ip any any

access-list 101 deny tcp 192.169.0.0 0.0.255.255 any eq tftp

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

-- vyos --

interfaces

ethernet eth0

address 172.30.1.2/25

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

ethernet eth1

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

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 172.16.30.129/25

channel 2

country-code us

description "Group 11 Wireless Network"

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

mode g

physical-device phy0

security

wpa

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

ssid c240-344g11

type access-point

protocols

static

route 172.30.1.0/25

next-hop 172.30.1.1

service

dhcp-server

shared-network-name WLAN

subnet 172.30.1.128/25

default-router 172.30.129.1

name-server 10.2.1.11

range 0

start 172.30.1.130

stop 172.30.1.230

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 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

-- g11sw1 --

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

description "VLAN 11 Access"

switchport access vlan 11

switchport mode access

interface GigabitEthernet1/0/2

shutdown

interface GigabitEthernet1/0/3

shutdown

interface GigabitEthernet1/0/4

shutdown

interface GigabitEthernet1/0/5

shutdown

interface GigabitEthernet1/0/6

shutdown

interface GigabitEthernet1/0/7

shutdown

interface GigabitEthernet1/0/8

shutdown

interface GigabitEthernet1/0/9

shutdown

interface GigabitEthernet1/0/10

shutdown

interface GigabitEthernet1/0/11

description "VLAN 111 Access"

switchport access vlan 111

switchport mode access

interface GigabitEthernet1/0/12

shutdown

interface GigabitEthernet1/0/13

shutdown

interface GigabitEthernet1/0/14

shutdown

interface GigabitEthernet1/0/15

shutdown

interface GigabitEthernet1/0/16

shutdown

interface GigabitEthernet1/0/17

shutdown

interface GigabitEthernet1/0/18

shutdown

interface GigabitEthernet1/0/19

shutdown

interface GigabitEthernet1/0/20

shutdown

interface GigabitEthernet1/0/21

description "VLAN 211 Access"

switchport access vlan 211

switchport mode access

interface GigabitEthernet1/0/22

shutdown

interface GigabitEthernet1/0/23

shutdown

interface GigabitEthernet1/0/24

shutdown

interface GigabitEthernet1/0/25

shutdown

interface GigabitEthernet1/0/26

shutdown

interface GigabitEthernet1/0/27

shutdown

interface GigabitEthernet1/0/28

description "CIT Uplink"

switchport trunk encapsulation dot1q

switchport mode trunk

interface GigabitEthernet1/0/29

shutdown

interface GigabitEthernet1/0/30

shutdown

interface GigabitEthernet1/0/31

shutdown

interface GigabitEthernet1/0/32

shutdown

interface GigabitEthernet1/0/33

shutdown

interface GigabitEthernet1/0/34

shutdown

interface GigabitEthernet1/0/35

shutdown

interface GigabitEthernet1/0/36

shutdown

interface GigabitEthernet1/0/37

shutdown

interface GigabitEthernet1/0/38

shutdown

interface GigabitEthernet1/0/39

shutdown

interface GigabitEthernet1/0/40

shutdown

interface GigabitEthernet1/0/41

shutdown

interface GigabitEthernet1/0/42

shutdown

interface GigabitEthernet1/0/43

shutdown

interface GigabitEthernet1/0/44

shutdown

interface GigabitEthernet1/0/45

shutdown

interface GigabitEthernet1/0/46

shutdown

interface GigabitEthernet1/0/47

description "VyOS Access Point"

switchport access vlan 172

switchport mode access

interface GigabitEthernet1/0/48

shutdown

interface GigabitEthernet1/0/49

shutdown

interface GigabitEthernet1/0/50

shutdown

interface GigabitEthernet1/0/51

shutdown

interface GigabitEthernet1/0/52

shutdown

interface TenGigabitEthernet1/0/1

shutdown

interface TenGigabitEthernet1/0/2

shutdown

interface Vlan1

no ip address

shutdown

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

-- g11sw2 --

hostname "s2"

interface 19

lacp Passive

exit

snmp-server community "public" Unrestricted

vlan 1

name "DEFAULT\_VLAN"

untagged 2-10,12-18,20-22,24

ip address dhcp-bootp

no untagged 1,11,21,19

exit

vlan 11

name "vlan 11"

untagged 1

ip address 192.169.11.10 255.255.255.0

tagged 19

exit

vlan 111

name "vlan 111"

untagged 11

ip address 192.169.111.10 255.255.255.0

tagged 19

exit

vlan 211

name "vlan 211"

untagged 21

ip address 192.169.211.10 255.255.255.0

tagged 19

exit

ip ssh

password manager

password operator