Lab 4: Routing, Network Address Translation, and Access Control Lists

CNIT34400-006
Group 30
Abbie Docter
William Park
Submitted To: Royden Butterfield
Date Submitted: 5/1/2022
Date Due: 5/1/2022

TABLE OF CONTENTS

Table of Contents

EXECUTIVE SUMMARY

The project outlined in this report was focused around implementing the Routing Information Protocol (RIP) to improve communication between routers, adding another set of Local Area Networks (LANs) along with a wireless network, and utilizing Access Control Lists (ACLs) on the routers to implement business security protocols. Some previously configured interfaces and protocols also had to be either reconfigured or removed in order for this project to be completed successfully.

The Business Scenario section of this report depicts the network architecture before the project was implemented. The Procedures section details the steps taken to implement the project. The Results section explains the network architecture after the project was completed. The Conclusions and Recommendations section analyzes how well the project went and makes recommendations on how to complete the project if something similar must be done again in the future. The Bibliography section contains the materials referenced to complete the project. Appendix A of this report contains problems that were encountered and potential solutions to those problems. Appendix B includes the finalized configuration files of all routers and switches utilized in the project.

Routing, NAT, and ACL

BUSINESS SCENARIO

Craft-A-Palooza, a small business focused on helping niche artists market their art, was looking to add new networks to their architecture in the 192.169.0.0/16 addressing space. They were also looking to add a wireless network with the use of a VyOS wireless router. This setup required that the Multiple Spanning Tree Protocol (MSTP) was removed from their switches and a routing protocol was installed onto their routers. They also requested that certain security protocols be put in place, to be implemented with the use of Access Control Lists (ACLs). The applications used in this project were Windows 10, VyOS, Cisco IOS, HPE ArubaOS, PuTTY, Windows Command Prompt, and SolarWinds. The beginning network architecture, including IP addressing, can be viewed in Figures 1 and 2 below.

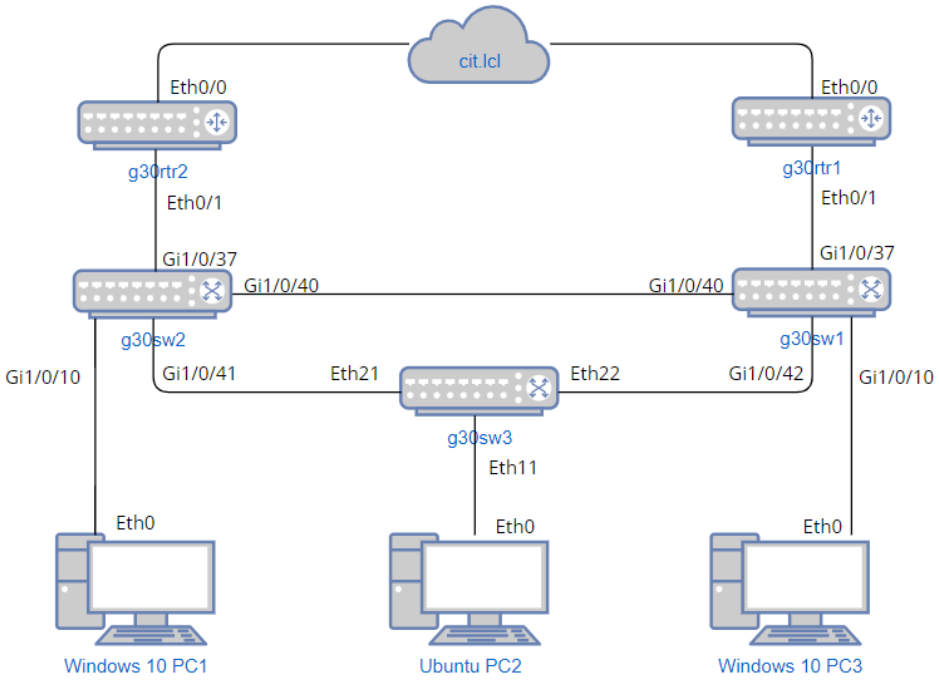

Figure 1: Beginning Physical Diagram

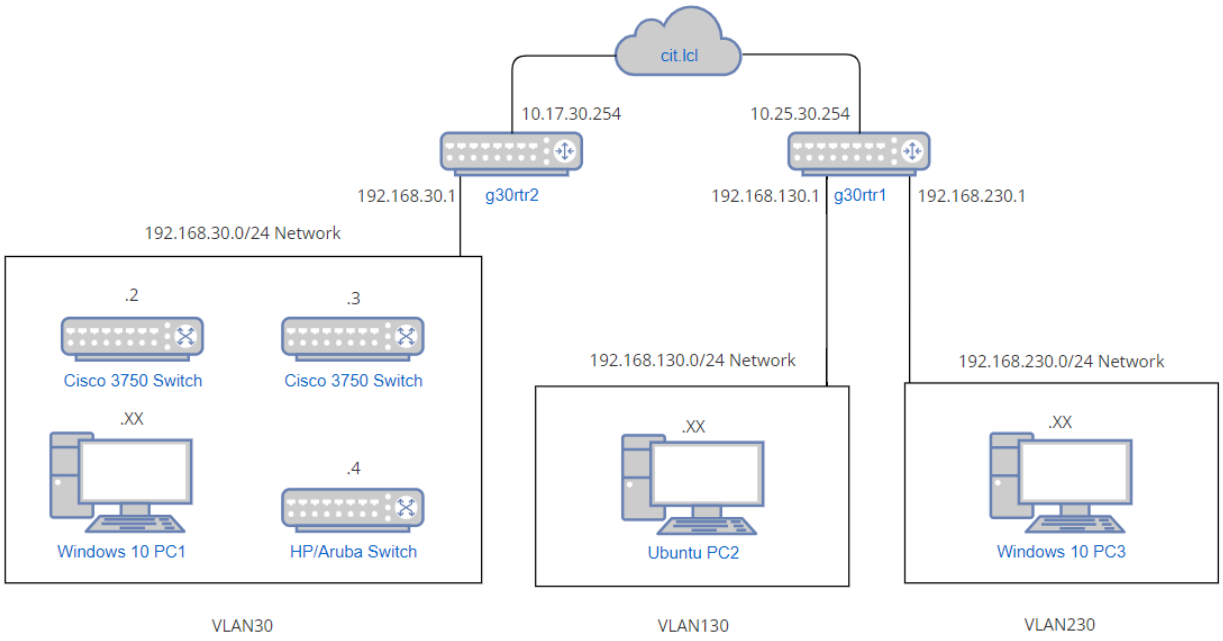

Figure 2: Beginning Logical Diagram

PROCEDURES

This section includes steps to recreate what was achieved in the previous few weeks. In this report, **buttons** are bolded, *options* are italicized, <u>text entered the computer</u> is underlined and menu navigation is notated by the pipe symbol (|).

Set up network architecture

The following steps are required to set up a network architecture that is needed to set up VLANs, NAT/PAT, distance vector routing protocols such as RIP version 2 and ACLs.

1. Connected Cisco 2811 router port 0 to CIT 10.25.0.0/16 network via gray uplink cable
2. Connected Cisco 2811 router port 1 to Cisco switch port 37
3. Connected Cisco 2811 router serial port 0 to Cisco 1921 router serial port 0
4. Connected Cisco 1921 router port 1 to HP switch port 22
5. Connected Cisco switch port 35 to VyOS port 1
6. Connected Cisco switch port 11 to Rack 16 Patch Panel 1 port 7
7. Connected HP switch switch port 12 to Rack 16 Patch Panel 1 port 8
8. Connected Cisco router console port to Rack 16 Patch Panel 2 port 7
9. Connected Cisco 1921 router console port to Rack 16 Patch Panel 2 port 8
10. Connected PC1 to Rack 16 Patch Panel 1 port 7
11. Connected PC2 to Rack 16 Patch Panel 1 port 8

Removed MSTP from switches

The following removes MSTP instances from Cisco and HP switches. After doing so, the priority is set for each switch depending on the VLANs.

1. Navigated to Putty installed on windows computer
2. Selected **serial** for connection type and clicked connect
3. Entered login ID and password
4. For Cisco switches:
    a. configure terminal
    b. spanning-tree mst configuration to enter spanning tree configuration mode
    c. no instance 1 vlan 30 to create new MSTP instance for vlans 30
    d. no instance 2 vlan 130,230 to create new MSTP instance for vlans 130 & 230
    e. no name MSTPLeft to specify MSTP
    f. no revision 2 to specify revision number
    g. exit to leave spanning tree configuration mode
    h. no spanning-tree mst 2 priority 0 to set high priority for vlans 130 & 230
    i. no spanning-tree mst 2 root primary to set high priority for vlans 130 & 230
    j. no spanning-tree mode mst to swap switch to use to MSTP
    k. copy run start to save configuration
5. For HP switch:
    a. configure
    b. no spanning-tree instance 1 vlan 30 to create MSTP instance for vlan 30

c. no spanning-tree instance 2 vlan 130 230 to create MSTP instance for vlans 130 & 230
d. no spanning-tree instance 1 priority 3 to set low priority for vlan 30
e. no spanning-tree instance 2 priority 3 to set low priority for vlans 130 & 230
f. no spanning-tree config-name MSTPLeft to name MSTP
g. no spanning-tree config-revision 2 to set revision number
h. no spanning-tree mode mstp to swap switch to use MSTP
i. write memory to save configuration

Removed WAN uplink port configuration from g30rtr2

The following removes CIT uplink from Cisco 1921 router by navigating to the interface and disabling IP address, NAT, NAT on each sub-interface, and IP route.

1. Typed configure terminal to enter configuration mode
2. Entered the following command:
    a. interface Gi 0/0 to enter interface configuration mode
    b. no ip address to remove IP address and subnet mask on the interface
    c. no ip nat outside to remove NAT on the interface
    d. exit to leave interface configuration mode
    e. removed ip nat inside on sub-interfaces gi0/1.30, 1.130, 1.230
    f. no access-list 12 to further remove NAT
    g. no ip route 0.0.0.0 10.17.30.1 to remove route
    h. copy run start to save configuration

Configured serial ports on routers

Connected ports and created /30 IP address range?

1. For g30rtr1:
2. Typed following into the configure terminal
    a. interface serial0/0/0
    b. IP address 192.168.80.2 255.255.255.252
    c. clock rate 2000000
    d. bandwidth 64
    e. no shutdown
    f. encapsulation ppp
    g. end
    h. copy run start
3. For g30rtr2:
4. Typed following into the configure terminal
    a. interface serial0/0/0
    b. IP address 192.168.80.1 255.255.255.252
    c. no shutdown
    d. encapsulation ppp
    e. end
    f. copy run start

Configured sub-interfaces on g30rtr1 and g30rtr2

The following configures VLAN 172 on Cisco routers and set up ip address, sub-interfaces, and subnet masks. Because the procedure for both router is slightly different in IP address, the procedure is written at once and have inputted .2 for router 1 and .3 for router 2.

1. Typed configure terminal to enter configuration mode
2. Entered the following commands on 2811 and 1921:
    a. interface GigabitEthernet 0/1.172 to enter interface configuration mode
    b. encapsulation dot1Q 172 to set the sub-interface as the VLAN 172 interface
    c. ip address 172.30.1[.2 or .3] 255.255.255.128 to set the IP and subnet mask
    d. no shutdown to enable the sub-interface
    e. exit to leave interface configuration mode
3. Entered copy run start to save configuration

Configured VLAN 172 on g30sw1

The following configures VLAN 172 on Cisco switch. The following puts the name, description, and switchport mode access command to sets the port as an access port.

1. Typed configure terminal to enter configuration mode
2. Entered vlan 172 to enter vlan configuration mode
    a. name VLAN172
3. Entered int vlan 172 to enter vlan (interface) configuration moe
    a. description ‘Vlan 172 wireless network’
    b. no shutdown

4. Entered int gi1/0/35 to enter interface configuration mode
    a. no shutdown
    b. switchport mode access
    c. switchport access vlan 172
    d. end
    e. copy run start

Configured VLAN 172 on g30sw3

The following configures VLAN 172 on HP switch to add trunked port.

1. Typed configure to enter configuration mode
2. Entered vlan 172 to enter VLAN configuration mode
3. Typed the following commands:
    a. name VLAN172
    b. tagged 22
    c. end
    d. write memory

Removed VLANs from VyOS

The following removes VLANs 30, 130, 230 which existed from previous configuration.

1. Typed configure to enter configuration mode
2. Entered delete interfaces ethernet eth1 vif 30 to remove VLAN 30
3. Entered delete interfaces ethernet eth1 vif 130 to remove VLAN 130

4. Entered delete interfaces ethernet eth1 vif 230 to remove VLAN 230
5. Entered commit and save commands to save configuration

Configured interfaces on VyOS

The following set up VyOS device as an access point: 172.30.1.128/25 network.

1. Typed configure to enter configuration mode
2. Entered delete interfaces wireless wlan0 address 172.16.30.1/24 to delete old IP and subnet
3. Entered set interfaces wireless wlan0 address 172.30.1.129/25 to set new IP and subnet
4. The rest of the wireless is already set up from lab 2
5. Entered delete interfaces wireless wlan0 disable to enable WLAN interface
6. set interfaces ethernet eth1 address 172.30.1.1/25
7. Issued commit and save commands to save configuration

Reconfigured addresses in 1921

The following reconfigures addresses to be changed from 192.168 to 192.169. 192,168 configurations existed previously, which is why it needs reconfiguration rather than making new ones.

1. Typed the following in the configure terminal to enter configuration mode
2. Typed the following into the terminal to change the ip addresses:
    a. interface gigabitEthernet 0/1.30
    b. ip address 192.169.30.1 255.255.255.0

c. exit

d. interface gigabitEthernet 0/1.130

e. ip address 192.169.130.12 255.255.255.0

f. exit

g. interface gigabitEthernet 0/1.230

h. ip address 192.169.230.12 255.255.255.0

i. ip route 0.0.0.0 0.0.0.0 10.25.30.1

j. **ctr+ z** to get out of config mode

k. typed copy run start

Configured DHCP for VLANs on 1921

The following configures DHCP on Cisco 1921 for 192.169.[30, 130, 230].0/24 addressing.

1. Typed the following in the configure terminal to enter configuration mode
    a. ip dhcp excluded-address 192.169.30.1 to exclude the gateway address from the pool of available addresses
    b. ip dhcp pool DHCP30 to enter DHCP pool configuration mode
    c. network 192.169.30.0 255.255.255.0 to specify network address and subnet mask
    d. default-router 192.169.30.1 to set the default gateway for this network
    e. dns-server 10.2.1.11 to specify the DNS server
    f. exit to leave DHCP pool configuration mode

g. ip dhcp excluded-address 192.169.130.1 to exclude the gateway address from the pool of available addresses
h. ip dhcp pool DHCP130 to enter DHCP pool configuration mode
i. network 192.169.130.0 255.255.255.0 to specify network address and subnet mask
j. default-router 192.169.130.1 to set the default gateway for this network
k. dns-server 10.2.1.11 to specify the DNS server
l. exit to leave DHCP pool configuration mode
m. ip dhcp excluded-address 192.169.230.1 to exclude the gateway address from the pool of available addresses
n. ip dhcp pool DHCP230 to enter DHCP pool configuration mode
o. network 192.169.230.0 255.255.255.0 to specify network address and subnet mask
p. default-router 192.169.230.1 to set the default gateway for this network
q. dns-server 10.2.1.11 to specify the DNS server
r. exit to leave DHCP pool configuration mode

2. Entered exit to exit the config t mode.
3. Entered copy run start to save configuration

Configure Access-list and remove old access list

The following configures access list to enable new IPs and remove previous access list.

1. Typed configure to enter configuration mode

Routing, NAT, and ACL

2. Entered the following to diable and enable new access list
    a. access-list 12 permit 192.169.30.0 0.0.0.255
    b. access-list 12 permit 192.169.130.0 0.0.0.255
    c. access-list 12 permit 192.169.230.0 0.0.0.255
    d. no access-list 12 permit 192.168.30.0 0.0.0.255
    e. no access-list 12 permit 192.168.130.0 0.0.0.255
    f. no access-list 12 permit 192.168.230.0 0.0.0.255
    g. exit | exit
    h. write mem

Disabled old DHCP for wireless network

The following disable DHCP on VyOS for 192.168.0.0/16 and 172.16.30.0/24 addressing which exists on DHCP share network name: DHCP 30, DHCP 130, DHCP 230, and YOLO.

1. Typed configure to enter configuration mode
2. Entered delete service dhcp-server shared-network-name DHCP30
3. Entered delete service dhcp-server shared-network-name DHCP130
4. Entered delete service dhcp-server shared-network-name DHCP230
5. Entered delete service dhcp-server shared-network-name YOLO

Disabled old DNS Forwarding for wireless network

The following disables DNS forwarding for wireless network.

1. delete service dns forwarding allow-from 172.16.30.0/24

2. delete service dns forwarding allow-from 192.168.30.0/24
3. delete service dns forwarding allow-from 192.168.130.0/24
4. delete service dns forwarding allow-from 192.168.230.0/24
5. delete service dns forwarding dhcp eth1.30
6. delete service dns forwarding dhcp eth1.130
7. delete service dns forwarding dhcp eth1.230
8. delete service dns forwarding listen-address 172.16.30.1
9. delete service dns forwarding listen-address 192.168.30.1
10. delete service dns forwarding listen-address 192.168.130.1
11. delete service dns forwarding listen-address 192.168.230.1
12. Entered commit and save commands to save configuration

Configured new DHCP for wireless network

The following configure DHCP on VyOS for 172.30.1.128/25 addressing, some amount of addresses

1. Typed configure to enter configuration mode
2. Entered set service dhcp-server shared-network-name DHCPW subnet 172.30.1.128/25 default-router 172.30.1.129 to set default gateway
3. Entered set service dhcp-server shared-network-name DHCPW subnet 172.30.1.128/25 name-server 10.2.1.11 to set DNS server
4. Entered set service dhcp-server shared-network-name DHCPW subnet 172.30.1.128/25 range 0 start 172.30.1.150 to set the start of the range of acceptable addresses

5. Entered set service dhcp-server shared-network-name DHCPW subnet 172.30.1.128/25 range 0 stop 172.30.1.250 to set the end of the range of acceptable addresses
6. Entered set service dns forwarding listen-address 172.30.1.129 to set address to listen for DNS requests
7. Entered set service dns forwarding allow-from 172.30.1.0/25 to specify addresses to allow DNS requests from
8. Entered set service dns forwarding allow-from 172.30.1.128/25 to specify addresses to allow DNS requests from
9. Entered commit and save commands to save configuration

Configured NAT on g30rtr1 for new wireless and local networks

The following configure NAT on 2811 (172.30.1.0/25 -> 10.25.30.0 and 192.169.[30, 130, 230].0/24 -> 10.25.30.0).

1. Typed configure terminal to enter configuration mode
2. Commands:
    a. access-list 30 permit 192.169.30.0 0.0.0.255
    b. access-list 30 permit 192.169.130.0 0.0.0.255
    c. access-list 30 permit 192.169.230.0 0.0.0.255
    d. access-list 30 permit 172.30.1.0 0.0.0.127
    e. access-list 30 permit 172.30.1.128 0.0.0.127
    f. access-list 30 permit 192.168.80.0 0.0.0.3
    g. interface fastethernet 0/1.172 | ip nat inside

Configured NAT on VyOS

The following disables old NAT configuration and configurs new NAT on VyOS from 172.30.1.128/25 -> 172.30.1.0/25

1. Entered configure
2. Typed delete nat source rule 10 to delete previous NAT rule
    a. repeated for rules 30, 130, 230, and 99
3. Typed set nat source rule 172 source address 172.30.1.128/25 to set the range of addresses to translate
4. Typed set nat source rule 172 outbound-interface eth1 to specify which interface the traffic would leave from
5. Typed set nat source rule 172 translation address masquerade to allow the router to choose what IP addresses to translate to
6. Entered commit and save commands to save configuration

Configured RIP for g30rtr1

The following shows the setup of RIP version 2 on the g30rtr1.

1. Typed configure terminal to enter configuration mode
2. router rip
3. no auto-summary
4. version 2
5. network 192.168.30.0

6. network 192.168.130.0
7. network 192.168.230.0
8. network 192.168.80.0
9. network 10.25.30.0
10. network 172.30.1.0
11. end
12. copy run start

Configured RIP for g30rtr2

The following shows the setup of RIP version 2 on the g30rtr2.

1. Typed configure terminal to enter configuration mode
2. router rip
3. version 2
4. no auto-summary
5. network 192.169.30.0
6. network 192.169.130.0
7. network 192.169.230.0
8. network 192.168.80.0

Configured RIP for VyOS

The following shows the setup of RIP version 2 on the VyoS Router.

1. Typed configure to enter configuration mode

Routing, NAT, and ACL

2. Typed the following commands in the terminal:
    a. set protocols rip network 172.30.1.0/25
    b. set protocols rip network 172.30.1.128/25
    c. set protocols rip interface eth1

Set up TFTP server

The following includes the steps to set up TFTP server on windows 10 on PC2.

1. Unpacked zip drive downloaded from SolarWinds TFTP server
2. Ran **solarWinds TFTP wizard**
3. Clicked **Next** for Destination Location
4. Clicked **Finish** for TFTP Server Setup
5. Navigated to **File** | **Configure** | **Security**
6. Checked **only all IP addresses to send/receive files**
7. Clicked **OK** to exit

Configured ACL rules for accessing TFTP

The following includes the configuration of router Cisco 1921 to allow 172.30.1.0/24 network to allow port 69.

1. Typed configure to enter configuration mode
2. Typed the following into the terminal:
    a. access-list 111 permit udp 172.30.1.0 0.0.0.255 any eq 69
    b. access-list 111 deny udp 192.0.0.0 0.255.255.255 any eq 69

c. access-list 111 permit ip any any
d. interface g0/1.30
e. ip access-group 111 out
f. exit
g. interface g0/1.130
h. ip access-group 111 out
i. exit
j. interface g0/1.230
k. ip access-group 111 out
l. end
m. write mem

Configured ACL rules for accessing web browser

The following includes configuration of Cisco 2811; Only allows 192.168/9.30.0/24 and 192.168/9.230.0/24 networks to access ports 80 & 443.

1. Typed configure to enter configuration mode
2. Commands:
    a. access-list 180 deny tcp 192.168.130.0 0.0.0.255 any eq 80
    b. access-list 180 deny tcp 192.169.130.0 0.0.0.255 any eq 80
    c. access-list 180 deny tcp 192.168.130.0 0.0.0.255 any eq 443
    d. access-list 180 deny tcp 192.169.130.0 0.0.0.255 any eq 443
    e. access-list 180 permit ip any any

f. interface fa0/1 .30, .130, .230

    i. ip access-group 180 in

g. interface serial0/0/0

    i. ip access-group 180 in

RESULTS

In this project, new networks were added in the 192.169.0.0/16 and 172.30.1.0/24 addressing spaces. Multiple configurations had to be altered or removed in order for the project to be completed. In addition, ACLs were configured to implement security rules. Figure 3 below shows the physical configuration of routers and switches. Figure 4 below shows the logical configuration of the network with VLANs and IP addresses.

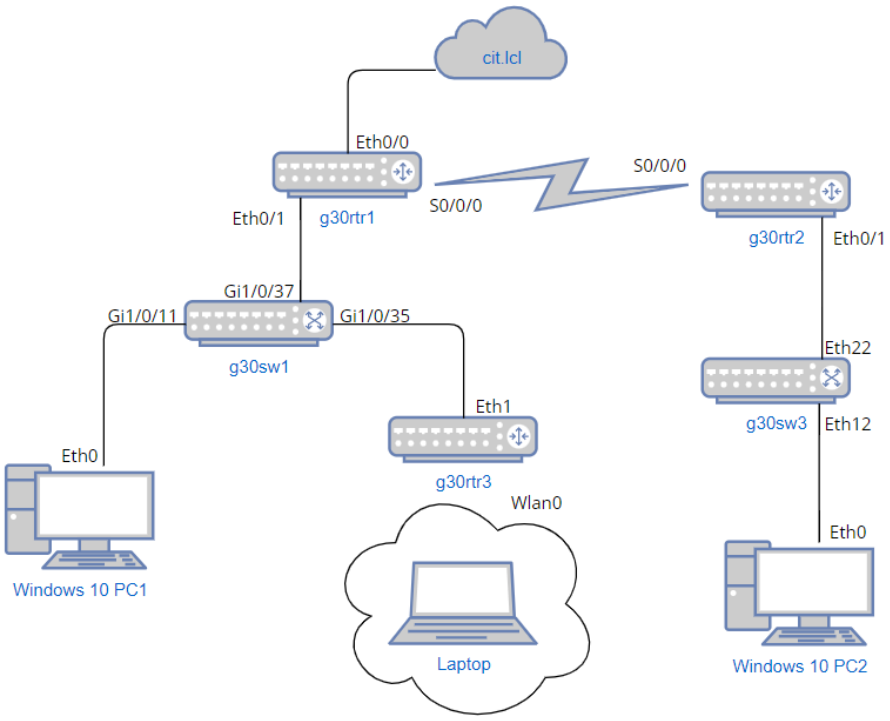

Figure 3: Ending Physical Diagram

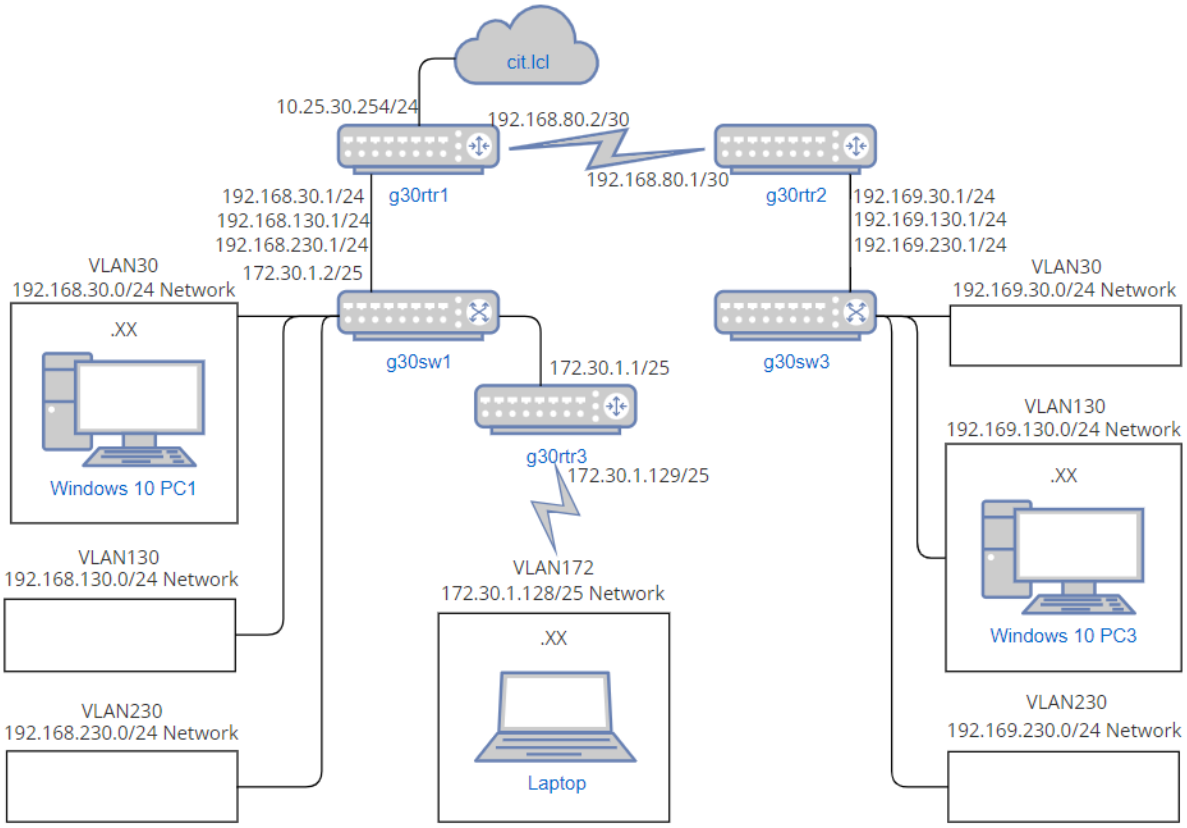

Figure 4: Ending Logical Diagram

CONCLUSIONS AND RECOMMENDATIONS

The project described in this report was a success. All project requirements were implemented and functional, including the network architecture adjustments, the Routing Information Protocol (RIP) implementation, the creation of new Local Area Networks (LANs) and Wireless LAN (WLAN), and the Access Control List (ACL) rules.

Recommendations

The following are recommendations for completing the projects outlined in this report.

Recommendation 1: The recommended order for completing the projects would be to adjust the network architecture first, remove configurations that are no longer needed, adjust interface configurations and Virtual LANs (VLANs), set up new DHCP and NAT, configure RIP, and finally configure the ACL rules.

Recommendation 2: Since so many changes were being made concurrently during the project, it was helpful to document throughout the course of the project to help keep track of what had been done and what still needed to be done. In addition, documenting interface numbers was useful for configuring them later.

Recommendation 3: It is highly recommended to test the network configurations during the project's implementation and not leave all of the testing for the end. Otherwise, it may be difficult to discern exactly what is causing issues since connectivity problems could be attributed to multiple different things.

BIBLIOGRAPHY

Butterfield, R. (personal communication, March 29,2022)

Canonical (2022), Ubuntu

Cisco. (2002). *IP Access List Security for CCNA Exam #640-607*. Configuring RIP Between R1 and R2 > IP Access List Security for CCNA Exam #640-607 | Cisco Press. Retrieved May 1, 2022, from https://www.ciscopress.com/articles/article.asp?p=26421&seqNum=3

Cisco Systems (2022), Cisco 1921

Cisco Systems (2022), Cisco 2811

Cisco Systems (2022), Cisco 3750

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

Deadman, R. (2022). Spring 2022 CNIT240-007/CNIT344-006 LAB. Lab 3 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 28,2022)

Doelger, S. (2011). *How to configure a Cisco with TFTP - UNAVCO*. UNAVCO. Retrieved May 2, 2022, from https://kb.unavco.org/kb/article/how-to-configure-a-cisco-with-tftp-707.html

Hewlett Packard Enterprise (2022), HP/Aruba

Microsoft Windows (2022), Windows 10

Park, W., & Docter, A. (2022). Lab 2: Wireless and Enterprise Routers. *Wireless and Enterprise Routers.*

Park, W., & Docter, A. (2022). Lab 3: Spanning Tree Protocol and Physical Security. *Spanning Tree Protocol and Physical Security.*

RIP. RIP - VyOS 1.3.x (equuleus) documentation. (n.d.). Retrieved May 1, 2022, from https://docs.vyos.io/en/equuleus/configuration/protocols/rip.html

Solarwinds (2022), Soarwinds TFTP Server

Tech, R. S. (2012). *Routerswitch Tech.* Router Switch Blog. Retrieved May 1, 2022, from https://blog.router-switch.com/2012/04/how-to-configure-ppp-on-cisco-router%EF%BC%9F/

TFTP¶. TFTP - VyOS 1.2.x (crux) documentation. (n.d.). Retrieved May 1, 2022, from https://docs.vyos.io/en/crux/configuration/service/tftp-server.html

APPENDIX A: PROBLEM SOLVING

This section describes several issues faced throughout this project. Each problem is broken down by giving a *Problem Description*; listing *Possible Solutions*, each of which are generated through a brain-storming exercise, accompanied by the reasoning for it; *Solutions Attempted*, which simply list which options from the *Possible Solutions* list that were attempted; and finally, a detailed description of the *Final Solution* and why it solved the problem.

Problem 1: ACL Rules

Problem Description: To allow specific TFTP from VyOS only, access list needs to be configured and set in order for block of the connection to other network. While the access list was set up accordingly, it did not seem to work since the file was transferred from non-able network to TFTP server but the content was missing.

Possible Solutions: Reset up of access list, could possibly solve the error from the previous configuration; write memory, might be possibly because of not saved configuration.

Solutions Attempted: Looked at the access-list configuration set up for TFTP and tried to reorganized the configuration

Final Solution: The problem was the out of the three access-list command, “access-list ### permit ip any any” was configured at the first or second rather than last command. Because the order of the access-list matters, after reordering the commands, the problem was solved.

Problem 2 Title

Problem Description: While DHCP for VLANS were configured accordingly, the PCs did not seem to have internet connection

Possible Solutions: Looking over previous DHCP configuration from lab 2 to see the difference from the current configuration; Ask for assistance, look at “show run” command configuration

Solutions Attempted: The group tried all of them and after looking at the configurations, we were able to discover default-router and/or DNS-server wasn’t set up.

Final Solution: The final solution was simple. The DNS-server and/or default-router commands needed to be entered with following required information on DHCP pool configuration for the internet connection to work.

APPENDIX B: CONFIGURATION FILES

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

g30rtr1

```
Current configuration : 3653 bytes
! Last configuration change at 23:10:23 UTC Wed Apr 27 2022
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname g30rtr1
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 excluded-address 192.168.30.2
ip dhcp excluded-address 192.168.30.3
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 dhcp pool DHCP30
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 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
 description 'WAN Uplink to CIT-NET'
 ip address 10.25.30.254 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
interface FastEthernet0/1
 description 'LAN Link'
 no ip address
 duplex auto
 speed auto
interface FastEthernet0/1.30
 description 'Subinterface for VLAN 30'
 encapsulation dot1Q 30
 ip address 192.168.30.1 255.255.255.0
 ip access-group 180 in
 ip nat inside
 ip virtual-reassembly in
interface FastEthernet0/1.130
 description 'Subinterface for VLAN 130'
 encapsulation dot1Q 130
 ip address 192.168.130.1 255.255.255.0
 ip access-group 180 in
 ip nat inside
 ip virtual-reassembly in
interface FastEthernet0/1.172
 encapsulation dot1Q 172
 ip address 172.30.1.2 255.255.255.128
 ip nat inside
 ip virtual-reassembly in
interface FastEthernet0/1.230
 description 'Subinterface for VLAN 230'
 encapsulation dot1Q 230
 ip address 192.168.230.1 255.255.255.0
 ip access-group 180 in
 ip nat inside
 ip virtual-reassembly in
interface Serial0/0/0
 bandwidth 64
 ip address 192.168.80.2 255.255.255.252
 ip access-group 180 in
```

```
 ip nat inside
 ip virtual-reassembly in
 encapsulation ppp
 clock rate 2000000
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
router rip
 version 2
 network 10.0.0.0
 network 172.30.0.0
 network 192.168.30.0
 network 192.168.80.0
 network 192.168.130.0
 network 192.168.230.0
 no auto-summary
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
access-list 30 permit 192.169.30.0 0.0.0.255
access-list 30 permit 192.169.130.0 0.0.0.255
access-list 30 permit 192.169.230.0 0.0.0.255
access-list 30 permit 172.30.1.0 0.0.0.127
access-list 30 permit 192.168.80.0 0.0.0.3
access-list 180 deny   tcp 192.168.130.0 0.0.0.255 any eq www
access-list 180 deny   tcp 192.169.130.0 0.0.0.255 any eq www
access-list 180 deny   tcp 192.168.130.0 0.0.0.255 any eq 443
access-list 180 deny   tcp 192.169.130.0 0.0.0.255 any eq 443
access-list 180 permit ip any any
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
```

g30rtr2

```
Current configuration : 2564 bytes
Last configuration change at 21:26:30 UTC Wed Apr 27 2022
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname g30rtr2
boot-start-marker
boot-end-marker
no aaa new-model
ethernet lmi ce
ip dhcp excluded-address 192.169.30.1
ip dhcp excluded-address 192.169.130.1
ip dhcp excluded-address 192.169.230.1
ip dhcp pool DHCPs
 network 192.169.30.0 255.255.255.0
 default-router 192.169.30.1
 dns-server 10.2.1.11
ip dhcp pool DHCP130
 network 192.169.130.0 255.255.255.0
 default-router 192.169.130.1
 dns-server 10.2.1.11
ip dhcp pool DHCP230
 network 192.169.230.0 255.255.255.0
 default-router 192.169.230.1
 dns-server 10.2.1.11
ip cef
no ipv6 cef
multilink bundle-name authenticated
license udi pid CISCO1921/K9 sn FTX182485NW
redundancy
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
interface GigabitEthernet0/0
 description 'WAN Uplink to CIT-NET'
 no ip address
 ip virtual-reassembly in
 duplex auto
```

```
 speed auto
interface GigabitEthernet0/1
 description 'LAN Link'
 no ip address
 ip access-group 111 out
 duplex auto
 speed auto
interface GigabitEthernet0/1.30
 description 'VLAN 30 Network'
 encapsulation dot1Q 30
 ip address 192.169.30.1 255.255.255.0
 ip access-group 111 out
 ip virtual-reassembly in
interface GigabitEthernet0/1.130
 description 'VLAN 130 Network'
 encapsulation dot1Q 130
 ip address 192.169.130.1 255.255.255.0
 ip access-group 111 out
 ip virtual-reassembly in
interface GigabitEthernet0/1.230
 description 'VLAN 230 Network'
 encapsulation dot1Q 230
 ip address 192.169.230.1 255.255.255.0
 ip access-group 111 out
 ip virtual-reassembly in
interface Serial0/0/0
 ip address 192.168.80.1 255.255.255.252
 encapsulation ppp
router rip
 version 2
 network 192.168.80.0
 network 192.169.30.0
 network 192.169.130.0
 network 192.169.230.0
 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 10.25.30.1!
access-list 111 permit udp 172.30.1.0 0.0.0.255 any eq tftp
access-list 111 deny   udp 192.0.0.0 0.255.255.255 any eq tftp
access-list 111 permit ip any any!
control-plane
 vstack
```

```
line con 0
 password 7 094F40000D564346
 login
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
 transport input none
scheduler allocate 20000 1000
end
```

g30rtr3

```
interfaces {
    ethernet eth0 {
        address 10.25.30.254/24
        hw-id 00:e0:4c:68:2f:bb
    }
    ethernet eth1 {
        address 172.30.1.1/25
        hw-id 00:e0:4c:68:2f:bc
    }
    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 172.30.1.129/25
        channel 1
        country-code us
```

```
        description "Group 30 Wireless Network"
        hw-id 60:6c:66:33:a4:cd
        mode g
        physical-device phy0
        security {
            wpa {
                mode wpa2
                passphrase **********
            }
        }
        ssid c240-344g30
        type access-point
    }
}
nat {
    destination {
    }
    source {
        rule 172 {
            outbound-interface eth1
            source {
                address 172.30.1.128/25
            }
            translation {
                address masquerade
            }
        }
    }
}
protocols {
    rip {
        interface eth1 {
        }
        network 172.30.1.0/25
        network 172.30.1.128/25
    }
    static {
        route 0.0.0.0/0 {
            next-hop 10.25.30.1 {
            }
        }
    }
}
service {
```

```
    dhcp-server {
        shared-network-name DHCPW {
            subnet 172.30.1.128/25 {
                default-router 172.30.1.129
                name-server 10.2.1.11
                range 0 {
                    start 172.30.1.150
                    stop 172.30.1.250
                }
            }
        }
    }
    dns {
        forwarding {
            allow-from 172.30.1.0/25
            allow-from 172.30.1.128/25
            dhcp wlan0
            listen-address 172.30.1.129
        }
    }
    ssh {
        access-control {
            allow {
                user adocter
                user park
            }
        }
        listen-address 10.25.30.254
        port 22
    }
}
system {
    config-management {
        commit-revisions 100
    }
    conntrack {
        modules {
            ftp
            h323
            nfs
            pptp
            sip
            sqlnet
            tftp
```

```
        }
    }
    console {
        device ttyS0 {
            speed 115200
        }
    }
    host-name g30rtr3
    login {
        user adocter {
            authentication {
                encrypted-password **********
            }
        }
        user park {
            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
            }
        }
    }
}
```

g30sw1

```
Current configuration : 5716 bytes
! Last configuration change at 00:34:19 UTC Wed Apr 6 2011
! NVRAM config last updated at 00:34:46 UTC Wed Apr 6 2011
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname g30sw1
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
crypto pki trustpoint TP-self-signed-201839104
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-201839104
 revocation-check none
 rsakeypair TP-self-signed-201839104
crypto pki certificate chain TP-self-signed-201839104
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 32303138 33393130 34301E17 0D313130 33333030 31323931
  325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3230 31383339
  31303430 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  B5814665 F211A20A B7E21DE0 669543CB 93EEF9BB 495F887A 4A1EAAC1 29D0F42F
  472F83F0 D9330607 082E039E B5FF2C6B 4B31C0C1 803FD53A 4C108371 4A13F16C
  A1E18CE2 3A915DAC 68707578 51E11D0A 5C8C55B0 52467E69 46ADC6A3 1A0B37EC
  1315C822 B40CFF04 A2BEECC3 F3B23AA8 2FC57D73 00FE9FCE F79533B5 5A7B9E0B
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 1680142D 22148C84 2A710276 FF38BC1A 1E9B92EA BBE7DB30 1D060355
  1D0E0416 04142D22 148C842A 710276FF 38BC1A1E 9B92EABB E7DB300D 06092A86
  4886F70D 01010505 00038181 00842F20 559FBE74 3D97B42F 223452BF D58EEF34
  971FE601 05027F6B 4BF34D78 9658476F 794A7519 2A5620AF 7722DC83 4B5A810A
  2A44BB30 527E3ACB 4439A417 4D49EE8D 814BBD59 8041910E 5FB477AB C8FE7E95
  B7456607 14548686 6C065DA8 95DB2097 90F4D5B7 10144A56 990CED44 EED1020D
  59D90132 B1090C60 50240F03 B1
```

```
        quit
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
 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
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
 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
 shutdown
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
 shutdown
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
 switchport access vlan 172
 switchport mode access
interface GigabitEthernet1/0/36
 shutdown
interface GigabitEthernet1/0/37
 description TrunkToG30rtr1
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface GigabitEthernet1/0/38
 shutdown
interface GigabitEthernet1/0/39
 shutdown
interface GigabitEthernet1/0/40
```

```
 description TrunkToG30sw2
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface GigabitEthernet1/0/41
 shutdown
interface GigabitEthernet1/0/42
 description TrunkToG30sw3
 switchport trunk encapsulation dot1q
 switchport mode trunk
interface GigabitEthernet1/0/43
 shutdown
interface GigabitEthernet1/0/44
 shutdown
interface GigabitEthernet1/0/45
 shutdown
interface GigabitEthernet1/0/46
 shutdown
interface GigabitEthernet1/0/47
 shutdown
interface GigabitEthernet1/0/48
 shutdown
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
 description 'VLAN 30 Network'
 ip address 192.168.30.3 255.255.255.0
interface Vlan130
 description 'VLAN 130 Network'
 no ip address
interface Vlan172
 description 'Vlan 172 wireless network'
 no ip address
interface Vlan230
 description 'VLAN 230 Network'
 no ip address
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
```

g30sw3

```
; JL259A Configuration Editor; Created on release #WC.16.08.0001
; Ver #14:07.6f.f8.1d.9b.3f.bf.bb.ef.7c.59.fc.6b.fb.9f.fc.ff.ff.37.ef:24
hostname "g30sw3"
module 1 type jl259a
interface 4
   disable
   exit
interface 5
   disable
   exit
interface 6
   disable
   exit
interface 7
   disable
   exit
interface 8
   disable
   exit
interface 9
   disable
   exit
interface 10
   disable
```

```
  exit
interface 14
  disable
  exit
interface 15
  disable
  exit
interface 16
  disable
  exit
interface 17
  disable
  exit
interface 18
  disable
  exit
interface 19
  disable
  exit
interface 20
  disable
  exit
interface 23
  disable
  exit
interface 24
  disable
  exit
interface 25
  disable
  exit
interface 26
  disable
  exit
interface 27
  disable
  exit
interface 28
  disable
  exit
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 172
   name "VLAN172"
   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
```