CS 646 Network Protocols Security
Team Members: Rasheed Azeez, Murali Badiger, and Shivam Patel
April 3, 2018

Project 2: Network Design

<u>Task 1 – "The Basics"</u>

a) Create a VLAN for PCs and assign all associated ports to this VLAN.

The following virtual local area networks (VLAN) 30 and ports were assigned for personal computers (PC) at each location:

Location	Ports
Detroit, MI	25 - 40
San Jose, CA	25 - 40
New York, NY	25 - 40
Seattle, WA	13 - 20
Dallas, TX	13 - 20
Las Vegas, NV	13 - 20
Newark, NJ	13 - 20
Raleigh, NC	13 - 20
Boston, MA	13 - 20

b) Create a VLAN for Phones and assign all associated ports to this VLAN.

The following virtual local area networks (VLAN) 10 and ports were assigned for phones at each location:

Location	Ports
Detroit, MI	1 - 12
San Jose, CA	1 - 12
New York, NY	1 - 12
Seattle, WA	1 - 6
Dallas, TX	1 - 6
Las Vegas, NV	1 - 6
Newark, NJ	1 - 6
Raleigh, NC	1 - 6
Boston, MA	1 - 6

c) Create a VLAN for Printers and assign all associated ports to this VLAN.

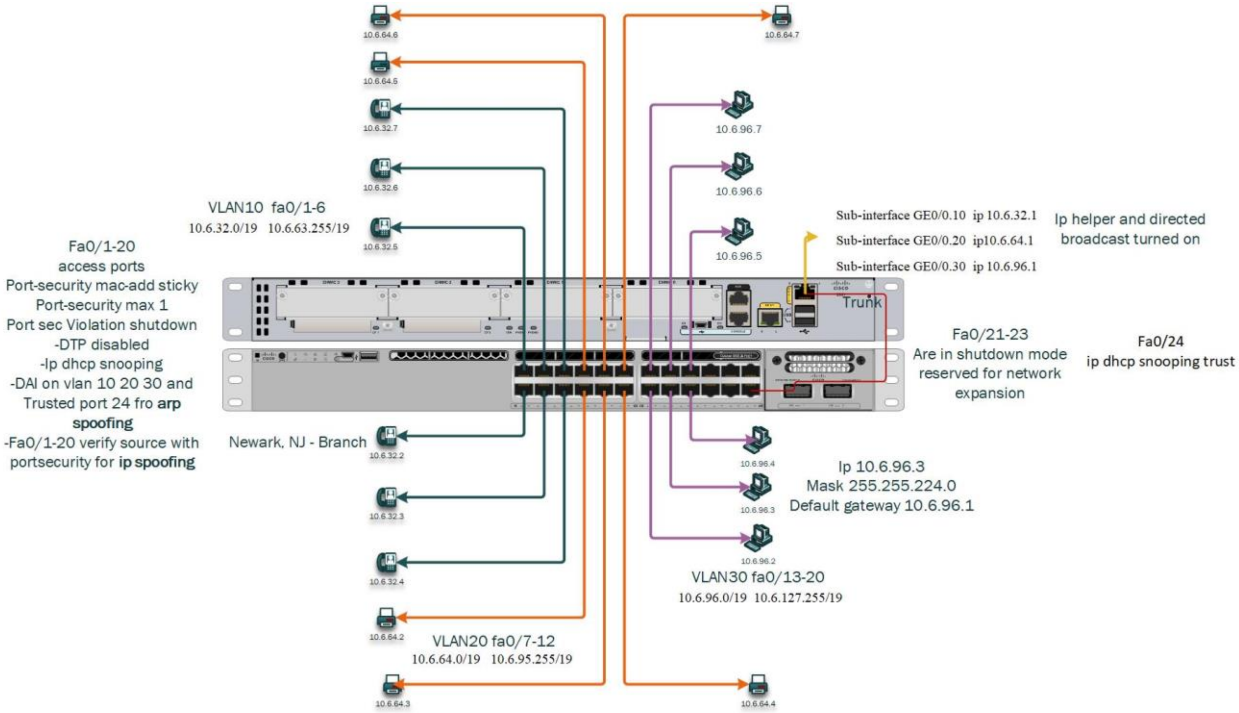
The following virtual local area networks (VLAN) 20 and ports were assigned for phones at each location:

Location	Ports
Detroit, MI	13 - 24
San Jose, CA	13 - 24
New York, NY	13 - 24
Seattle, WA	7 – 12
Dallas, TX	7 – 12
Las Vegas, NV	7 – 12
Newark, NJ	7 – 12
Raleigh, NC	7 – 12
Boston, MA	7 – 12

d) Indicate which ports are access ports and which are trunk ports.

Location	Trunk Port
Detroit, MI	48
San Jose, CA	48
New York, NY	48
Seattle, WA	24
Dallas, TX	24
Las Vegas, NV	24
Newark, NJ	24
Raleigh, NC	24
Boston, MA	24

These are the ports that will be used in the initial design and implemented of the network. The network is being designed in a way where additional trunk ports can be added for another switch if future capacity requires. All other ports will serve as access port for all VLANs. Other ports that are not being utilized with be placed in “shutoff” mode.



<u>Diagram 1</u>: Layout of layer 2 interfaces and sub interfaces.

e and f) Specify the router interfaces needed for each VLAN along with any other layer 3 interfaces. Use sub-interfaces in your design when trunks are configured.

For this network, the network engineers have decided to configure three sub-interfaces for each VLAN. The sub-interfaces are listed below:

- ✓ Sub-interface GE0/0.10 for VLAN 10 (Phones) IP 10.x.32.1 with Encapsulation dot1q 10
- ✓ Sub-interface GE0/0.20 for VLAN 20 (Printers) IP 10.x.64.1 with Encapsulation dot1q 20
- ✓ Sub-interface GE0/0.30 for VLAN 30 (PCs) IP 10.x.96.1 with Encapsulation dot1q 30

For example, PCs will have 10.x.96.1 as the default getaway. X will be replaced according to internet protocol (IP) scheme of the particular location. A detailed diagram is provided below:

g) Specify how forwarding of DHCP requests to the central DHCP server (recall that this is a layer-3 technology) will be handled.

For managing DHCP requests, **IP Helper** will be set on the all sub interface Ge0/0.10 , Ge0/0.20 and Ge0/0.30 on each router. Using this functionality will allow the interface to point to actual DHCP server, whose IP address is 10.100.1.50. This will take any incoming local DHCP request coming and forward them to the central DHCP server.

for example, for the **Newark,NJ** router,

```
interface ge0/0.10
ip helper-address 10.100.1.50
interface ge0/0.20
ip helper-address 10.100.1.50
interface ge0/0.30
ip helper-address 10.100.1.50
```

DHCP server will have all pools to serve different subnets.

Task 2- Basic Layer-2 Security

a) Your design should take into consideration the number of MAC addresses that can be learned on all connected ports (consider ports connected to PCs, printers, phones, etc.)

For this network, there is a set limit of 1 MAC address that can be learned by each port. The engineers have used the port security feature to set this limit. Limiting the number of secure MAC addresses and assigning a single address, the attached workstation is assured the full bandwidth of the port. If the maximum MAC addresses are reached on a secure port, violations will occur for any additional addresses attempting to access the port that differs from the identified secure MAC addresses.

The following command is used to configure the secure port:
switchport port-security maximum max-addr [vlan vlan-ID]
max-addr- Maximum number of secure MAC addresses for the interface; valid values are from 1 to 1025.
vlan-ID- Specifies the VLAN on which the MAC address should be secured.

b) Where should DHCP snooping be deployed?

DHCP snooping is a Layer 2 switch feature that mitigates the security risks posed by denial-of-service (DOS) from rogue DHCP servers. These rogue services have the ability to disrupt networks as they compete with authorized DHCP servers attempting to configure hosts on the network for communication. DHCP snooping is built on the concept of using one or more trusted ports that have been identified as having legitimate DHCP servers attached. As clients communicate on the network, the switch builds a "bindings table"—a database that lists the client MAC address, DHCP-assigned address, switch port, VLAN, and remaining DHCP lease time. The network switch filters any DHCP server messages from untrusted ports in order to protect the integrity of legitimate DHCP servers and their services. The feature is enabled on each VLAN; by default, all interfaces on these VLANs are untrusted. Any interface hosting a DHCP server must be explicitly defined as being "trusted". With this network DHCP snooping is enabled on the following VLANs and trusted ports: VLANS 10, VLAN 20 and VLAN30 and trusted ports 24 and 48 (connected to DHCP server).

The commands are as follows:

1.) ***To enable DHCP snooping on VLAN:***
Switch(config) #ip dhcp snoop VLAN_NAME

2.) ***We have to tell the switch, to which port the trusted dhcp server is connected, command***
Switch(config) #int PORT_NUMBER

DHCP snooping rate-limiting should be enabled to harden the switch against a resource exhaustion-based DoS attack.

c) Where should Dynamic ARP Inspection be deployed?

DAI ensures that only valid ARP requests and responses are relayed. DAI intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability safeguards the network from some man-in-the-middle (MITM) attacks. The switch performs these activities:

1.) Intercepts all ARP requests and responses on untrusted ports

2.) Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination

3.) Drops invalid ARP packets

DAI determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping feature enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. For packets received on untrusted interfaces, the switch performed the forwarding if the packet is checked and verified. ARP packets are validated against user-configured ARP access control lists (ACLs) for hosts configured with static IP addresses. The switch logs dropped packets.

For this network, DAI is enabled on VLAN 10, VLAN 20 and VLAN 30. Once DAI is enabled, all the associated ports on that VLAN are untrusted. All network the ports connecting to PCs, phones and printers are untrusted, whereas the ports connected to switches, i.e., trunk ports are configured as trusted. With this configuration, all ARP packets entering the network from any given switch will undergo a security check.

d) How will you protect all applicable ports from Yersenia DTP attacks?

By default, most ports are configured in dynamic mode. When a port is connected to another switch that supports the "Dynamic Trunking Protocol" (DTP), the port will auto-negotiate trunking parameters and become a trunk port. One attack vector that can be deployed by a malicious user is pretending to be a switch that supports DTP in an effort to become a member of all VLANs. To prevent such an attack, trunking should be disabled on the ports connecting to PCs, mobile devices, printers and any unused ports. Ports connecting to other switches should be hardcoded as trunks and negotiation should be disabled on those trunk ports. For this network, trunking and negotiation has been disabled on all the access ports and ports connecting to other switches are hardcoded as trunks and negotiation has been disabled on those ports..

e) How will you protect all applicable ports from Yersenia STP attacks?

1.) The ports connected to end user devices such as PCs, phones and printers have the PortFast feature enabled. This functionality reduces the amount of time required for the port to go into a forwarding state after being connected. The PortFast feature enabled a port that connects to an end-user device eliminates the potential to create a topology loop. With this, the port can become active more quickly by skipping the spanning tree protocol**'s (STP)** listening and learning states. Ports with PortFast feature enabled should never receive a bridge protocol data unit (BPDU). Attackers can send thousands of BPDUs using randomly generated MAC addresses. From the network's point of view, these appear to be new switches joining the network. The switches will be overwhelmed with all the new STP traffic and cause a DoS condition across the entire network.

    However, the above attack vector can be avoided by deploying BPDU guard. The BPDU guard is enabled on all the ports which have PortFast enabled on them i.e., the ports which are connected to end users. If these ports receive a BPDU, the BPDU guard will disable the port. Within this network, the BPDU guard has been established on all the ports which connect to PCs, mobiles and printers.

2.) There is one more possibility of an STP attack which is by introducing a switch with a lower priority and MAC address than that of real root. If this attack is successful, the attacker can seize the root role which leads to topology changes, which can bring instability to the network.

    This can be avoided by using Root Guard. Root guard allows the device to participate in STP as long as the device does not try to become the root. If root guard blocks the port, subsequent recovery is automatic.

    Root guard limits the switch ports out of which the root bridge may be negotiated. If a root-guard-enabled port receives BPDUs that are superior to those that the current root bridge is sending, then that port is moved to a blocking state. When there are no more superior BPDUs incoming to the port, the port will be activated again. This prevents attacker from seizing the root role. Root guard should be deployed towards ports that connect to switches which should not be the root bridge.

f) How will you handle VTP?

The VLAN Trunking Protocol (VTP) is designed to assist with network management by seamlessly propagating VLAN information throughout network switches. It involves a VTP server (effectively a switch) to be in charge of propagating all VLAN information. All switches, minus the VTP server switch, are configured as client switches that are responsible for listening for announcements regarding any VLAN changes made from the VTP server.

A potential VTP attack involves a station sending VTP messages through the network, advertising that there are no VLANs on the network. Thus, all client VTP switches erase their valid VLAN information databases. Such a scenario can also occur if a switch is plugged into the network that is configured as a VTP server and contains a VTP configuration version higher than the existing VTP server. In this case, all switches overwrite their valid information with that obtained by the 'new' VTP server.

One potential solution for this is either to avoid using VTP or use password based authentication for VTP messages. For the network, due to the scalability, it is not practical to implement VTP. Rather, MD5 authentication will be used for all VTP messages to ensure VTP messages are processed by the client switches if the password contained in the message is not correct.

g) How will you handle layer 2 discovery technologies such as a CDP and LLDP?

Link Layer Discovery Protocol (LLDP) is a neighbor discovery protocol that is used for network devices to advertise information about themselves to other devices on the network and learn about each other. LLDP runs over the data-link layer of the network. Cisco Discovery Protocol (CDP) is a variant of LLDP, but proprietary to Cisco based network devices. The protocol contain the following information on network devices: software version, IP address, platform, capabilities, and the native VLAN, etc.

However, these discovery messages used by these protocols are not encrypted, making critical network information easily available for malicious users to exploit. Attackers can generally use this information to identify vulnerable points within the network to launch attacks, typically in the form of a DoS.

CDP/LLDP is typically required for the ports connecting to IP phones. CDP/LLDP has been enabled on the network and disabled wherever it is not needed. For this network, Cisco devices are being used, so CDP is enabled on all the ports which connect to phones.

Task 3- Layer 3 Routing

a) Design a subnetting scheme and detail the associated routing table.

Being that there 9 main locations (3 headquarters and 6 branches), each location will operate on its own subnet. From the configurations set in Task 1 above, each subnet will be divided into three equal IP address spaces for VLAN 10, 20, and 30. In order to create enough subnets required for each location, 3 bits need to be borrowed from the host part of the network prefix. 3 bits are required from the host part because the first (all zeroes) and the last (all ones) subnets cannot be used as they are reserved as the network and broadcast addresses respectively. Using this knowledge, using these 3 bits would provide the following: $(2)^3 – 2= 6$ subnets.

Original IP Block Recommendation

Location	Router Name	IP Address
Detroit, MI	A	10.4.0.0/16
San Jose, CA	B	10.1.0.0/16
New York, NY	C	10.2.0.0/16
Seattle, WA	D	10.9.0.0/16
Dallas, TX	E	10.3.0.0/16
Las Vegas, NV	F	10.5.0.0/16
Newark, NJ	G	10.6.0.0/16
Raleigh, NC	H	10.7.0.0/16
Boston, MA	I	10.8.0.0/16

Revised IP Address Scheme

Location	Router	Outgoing Interface	Destination	Router	Incoming Interface
Detroit, MI	A	10.255.255.128/31	San Jose, CA	B	10.255.255.129/31
		10.255.255.192/31	New York, NY	C	10.255.255.193/31
San Jose, CA	B	10.255.255.224/31	Seattle, WA	D	10.255.255.225/31
		10.255.255.240/31	Dallas, TX	E	10.255.255.241/31
		10.255.255.248/31	Las Vegas, NV	F	10.255.255.249/31
New York, NY	C	10.255.255.252/31	Newark, NJ	G	10.255.255.253/31
		10.255.255.64/31	Raleigh, NC	H	10.255.255.65/31
		10.255.255.32/31	Boston, MA	I	10.255.255.33/31

Router A

Location	Network Address	Broadcast Address
Detroit, MI	10.4.0.0/19	10.4.31.255/19

Location	VLAN	Network Address	Broadcast Address
Detroit, MI	10	10.4.32.0/19	10.4.63.255/19
	20	10.4.64.0/19	10.4.95.255/19
	30	10.4.96.0/19	10.4.127.255/19

Routing Table for A

Route	Destination	Destination IP	NetMask	Interface	Metric	Next Hop	Next Hop IP Address
1	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/3	1	San Jose, CA	10.255.255.128/31
2	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/5	1	New York, NY	10.255.255.192/31
3	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/3	2	San Jose, CA	10.255.255.128/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/3	2	San Jose, CA	10.255.255.128/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/3	2	San Jose, CA	10.255.255.128/31
6	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/5	2	New York, NY	10.255.255.192/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/5	2	New York, NY	10.255.255.192/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/5	2	New York, NY	10.255.255.192/31

Router B

Location	Network Address	Broadcast Address
San Jose, CA	10.1.0.0/19	10.1.31.255/19

Location	VLAN	Network Address	Broadcast Address
San Jose, CA	10	10.1.32.0/19	10.1.63.255/19
	20	10.1.64.0/19	10.1.95.255/19
	30	10.1.96.0/19	10.1.127.255/19

Routing Table for B

Route	Destination	Destination IP	NetMask	Port	Metric	Next Hop	Next Hop IP Address
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/2	1	Detroit, MI	10.255.255.129/31
2	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/2	2	Detroit, MI	10.255.255.129/31
3	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/5	1	Seattle, WA	10.255.255.224/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/4	1	Dallas, TX	10.255.255.240/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/3	1	Las Vegas, NV	10.255.255.248/31
6	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/2	3	Detroit, MI	10.255.255.129/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/2	3	Detroit, MI	10.255.255.129/31

8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/2	3	Detroit, MI	10.255.255.129/31

Router C

Location	Network Address	Broadcast Address
New York, NY	10.2.0.0/19	10.2.31.255/19

Location	VLAN	Network Address	Broadcast Address
New York, NY	10	10.2.32.0/19	10.2.63.255/19
	20	10.2.64.0/19	10.2.95.255/19
	30	10.2.96.0/19	10.2.127.255/19

Routing Table for C

Route	Destination	Destination IP	NetMask	Port	Metric	Next Hop	Next Hop IP Address
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/2	1	Detroit, MI	10.255.255.193/31
2	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/2	2	Detroit, MI	10.255.255.193/31
3	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/2	3	Detroit, MI	10.255.255.193/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/2	3	Detroit, MI	10.255.255.193/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/2	3	Detroit, MI	10.255.255.193/31
6	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/3	1	Newark, NJ	10.255.255.252/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/4	1	Raleigh, NC	10.255.255.64/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/5	1	Boston, MA	10.255.255.32/31

Router D

Location	Network Address	Broadcast Address
Seattle, WA	10.9.0.0/19	10.9.31.255/19

Location	VLAN	Network Address	Broadcast Address
Seattle, WA	10	10.9.32.0/19	10.9.63.255/19
	20	10.9.64.0/19	10.9.95.255/19
	30	10.9.96.0/19	10.9.127.255/19

Routing Table for D

Route	Destination	Destination IP	NetMask	Port	Metric	Next Hop	Next Hop IP Address
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.225/31
2	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/1	3	San Jose, CA	10.255.255.225/31
3	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/1	1	San Jose, CA	10.255.255.225/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.225/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.225/31
6	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.225/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.225/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.225/31

Router E

Location	Network Address	Broadcast Address
Dallas, TX	10.3.0.0/19	10.3.31.255/19

Location	VLAN	Network Address	Broadcast Address
Dallas, TX	10	10.3.32.0/19	10.3.63.255/19
	20	10.3.64.0/19	10.3.95.255/19
	30	10.3.96.0/19	10.3.127.255/19

Routing Table for E

Route	Destination	Destination IP	NetMask	Port	Metric	Next Hop	Next Hop IP Address
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.241/31
2	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/1	3	San Jose, CA	10.255.255.241/31
3	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/1	1	San Jose, CA	10.255.255.241/31
4	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.241/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.241/31
6	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.241/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.241/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.241/31

Router F

Location	Network Address	Broadcast Address
Las Vegas, NV	10.5.0.0/19	10.5.31.255/19

Location	VLAN	Network Address	Broadcast Address
Las Vegas, NV	10	10.5.32.0/19	10.5.63.255/19
	20	10.5.64.0/19	10.5.95.255/19
	30	10.5.96.0/19	10.5.127.255/19

Routing Table for F

Route	Destination	Destination IP	NetMask	Port	Metric	Next Hop	Next Hop IP Address
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.249/31
2	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/1	3	San Jose, CA	10.255.255.249/31
3	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/1	1	San Jose, CA	10.255.255.249/31
4	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.249/31
5	Dallas TX	10.3.0.0/16	255.255.0.0	Gi0/1	2	San Jose, CA	10.255.255.249/31
6	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.249/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.249/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/1	4	San Jose, CA	10.255.255.249/31

Router G

Location	Network Address	Broadcast Address
Newark, NJ	10.6.0.0/19	10.6.31.255/19

Location	VLAN	Network Address	Broadcast Address
Newark, NJ	10	10.6.32.0/19	10.6.63.255/19
	20	10.6.64.0/19	10.6.95.255/19
	30	10.6.96.0/19	10.6.127.255/19

Routing Table for G

Route	**Destination**	**Destination IP**	**NetMask**	**Port**	**Metric**	**Next Hop**	**Next Hop IP Address**
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.253/31
2	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/1	3	New York, NY	10.255.255.253/31
3	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.253/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.253/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.253/31
6	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/1	1	New York, NY	10.255.255.253/31
7	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.253/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.253/31

Router H

Location	**Network Address**	**Broadcast Address**
Raleigh, NC	10.7.0.0/19	10.7.31.255/19

Location	**VLAN**	**Network Address**	**Broadcast Address**
Raleigh, NC	10	10.7.32.0/19	10.7.63.255/19
	20	10.7.64.0/19	10.7.95.255/19
	30	10.7.96.0/19	10.7.127.255/19

Routing Table for H

Route	**Destination**	**Destination IP**	**NetMask**	**Port**	**Metric**	**Next Hop**	**Next Hop IP Address**
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.65/31
2	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/1	3	New York, NY	10.255.255.65/31
3	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.65/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.65/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.65/31
6	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/1	1	New York, NY	10.255.255.65/31
7	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.65/31
8	Boston, MA	10.8.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.65/31

Router I

Location	Network Address	Broadcast Address
Boston, MA	10.8.0.0/19	10.8.31.255/19

Location	VLAN	Network Address	Broadcast Address
Boston, MA	10	10.8.32.0/19	10.8.63.255/19
	20	10.8.64.0/19	10.8.95.255/19
	30	10.8.96.0/19	10.8.127.255/19

Routing Table for I

Route	Destination	Destination IP	NetMask	Port	Metric	Next Hop	Next Hop IP Address
1	Detroit, MI	10.4.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.33/31
2	San Jose, CA	10.1.0.0/16	255.255.0.0	Gi0/1	3	New York, NY	10.255.255.33/31
3	Seattle, WA	10.9.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.33/31
4	Dallas, TX	10.3.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.33/31
5	Las Vegas, NV	10.5.0.0/16	255.255.0.0	Gi0/1	4	New York, NY	10.255.255.33/31
6	New York, NY	10.2.0.0/16	255.255.0.0	Gi0/1	1	New York, NY	10.255.255.33/31
7	Newark, NJ	10.6.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.33/31
8	Raleigh, NC	10.7.0.0/16	255.255.0.0	Gi0/1	2	New York, NY	10.255.255.33/31

Task 4 – Basic Layer-3 Security

a) The Update Server needs to be able to remotely power-on devices using wake-on-lan (WoL). Design your directed broadcasting security around this requirement. Research the WoL "magic packet" and design accordingly.

IP Helper is configured at the interface where the WoL server is connected, so any related requests will be forwarded to the router that is targeted for WoL (with directed broadcast address) and the within that router's network "magic packet" will be broadcasted. Secondly, directed broadcast is enabled on every router at GE0/0 interface with an ACL to allow only packets form the WoL server; by default, directed broadcast is disabled. Typically WoL utilizes port 9, but for this network the port was altered to increase security. GE0/0 is connected to local subnet in all routers, so that interface will allow directed broadcast from WoL server or otherwise it may drop "magic packets".

b) Protect against IP spoofing on all applicable switch ports.

Enable the following features of ports 24 and 48: DHCP snooping, Dynamic ARP Inspection, IP Source Guard, and DHCP snooping. Additionally, where a router is connected, IP Source Guard will use the DHCP snooping database to block spoofed traffic.

c) And D) Design an access list for the appropriate layer-3 ports to prevent spoofing (pay close attention to how you apply this access list, it may not be obvious to you what is ingress and what is egress). Ensure you don't break DHCP.

For WA,TX,NV,NJ,NC,MA Gi0/0 , MI Gi0/3,MI Gi0/5 ,

```
ip access-list extended INBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
deny ip host 0.0.0.0 any
```

```
ip access-list extended OUTBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any   (we can
permit only particular subnet(/27) in each interface if
we need more security)
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
permit ip host 0.0.0.0 any
```

For MI Gi0/4

```
ip access-list extended INBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.100.0.0   0.0.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
deny ip host 0.0.0.0 any
```

```
ip access-list extended OUTBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
permit ip host 0.0.0.0 any
```

For Gi0/3,4,5 of CA and NY

```
ip access-list extended INBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
permit ip host 0.0.0.0 any
```

```
ip access-list extended OUTBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
deny ip host 0.0.0.0 any
```

For CA ad NY Gi0/2

```
ip access-list extended INBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
deny ip host 0.0.0.0 any
```

```
ip access-list extended OUTBOUND
permit icmp any any echo
permit icmp any any echo-reply
permit icmp any any unreachable
deny icmp any any
permit ip 10.0.0.0   0.255.255.255 any
deny ip 172.16.0.0  0.15.255.255 any
deny ip 192.168.0.0   0.0.255.255 any
deny ip 127.0.0.0   0.255.255.255 any
permit ip host 0.0.0.0 any
```

and also should be directed broadcast from wol server so that should be allowed.