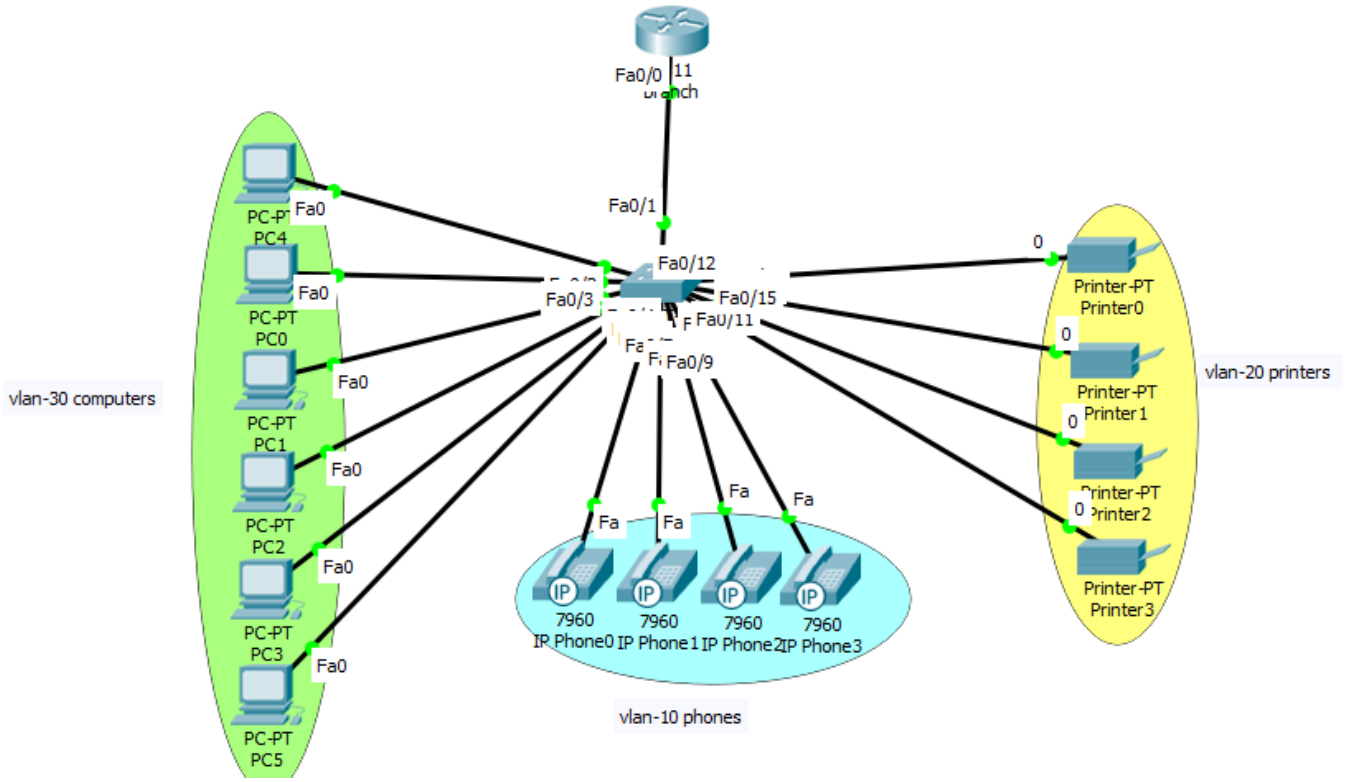
Ketaki Vitthal Kakade (kk524)
Adhithya Sivanesh (as3423)
Arman Gupta (ag986)

Network Protocol Security

PROJECT 2

Task 1: “The Basics”



(Figure 1)

A VLAN is a collection of one or more devices that belong to the same or different LAN’s and are able to communicate as if they were attached to the same wire, when in reality they could be located on a number of different LAN segments. Since VLAN’s are based on logical connections instead of physical connections, this makes them extremely flexible.

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

In our design, the computers in the LAN are connected on port number interfaces f0/2 to f0/7 on the switch. The assigning of PC’s to VLAN’s have been shown in Figure 2.

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

In our design, the phones in the LAN are connected on port number interfaces f0/8 to f0/11 on the switch. The assigning of PC's to VLAN's have been shown in Figure 2.

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

In our design, the printers in the LAN are connected on port number interfaces f0/12 to f0/15 on the switch. The assigning of PC's to VLAN's have been shown in Figure 2.

IOS Command Line Interface

```
Switch(config)#
Switch(config)#do show vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                                 Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                                 Fa0/24, Gig0/1, Gig0/2
10   Phones                            active    Fa0/8, Fa0/9, Fa0/10, Fa0/11
20   Printers                          active    Fa0/12, Fa0/13, Fa0/14, Fa0/15
30   Computers                         active    Fa0/2, Fa0/3, Fa0/4, Fa0/5
                                                 Fa0/6, Fa0/7
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
1005 trnet-default                     act/unsup

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
10   enet  100010     1500  -      -      -        -    -        0      0
20   enet  100020     1500  -      -      -        -    -        0      0
30   enet  100030     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005     1500  -      -      -        ibm  -        0      0

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
Switch(config)#
Switch(config)#
Switch(config)#
```

(Figure 2)

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

The access port are the ports that are connected to the end devices while the trunk ports are ports carrying traffic of different vlans. Thus, following are the assigned ports: -
Access ports: f0/2 to f0/15
Trunk port: f0/1
The below given diagram show the trunk ports according to our network design.

```
Switch(config)#
Switch(config)#
Switch(config)#show inter
Switch(config)#do show inter
Switch(config)#do show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/1       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/1       10,20,30

Port        Vlans allowed and active in management domain
Fa0/1       10,20,30

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/1       10,20,30
```

(Figure 3)

e) Specify the router interfaces needed for each VLAN along with any other layer 3 interfaces.

The router needs only one physical interface in order to be connected to all the vlan. Refer to the Figure 1. Interface f0/0 will be divided into three virtual interfaces each of these will act as layer 3 interfaces.

f) Use sub-interfaces in your design when trunks are configured.

Interface f0/0 is divided into sub- interfaces namely:
f0/0.10 for vlan 10
f0/0.20 for vlan 20
f0/0.30 for vlan 30.
These sub-interface are shown in figure 4.

IOS Command Line Interface

```
Router(config)#
Router(config)#
Router(config)#
Router(config)#
Router(config)#do show ip inter
Router(config)#do show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        unassigned      YES unset  up                    up
FastEthernet0/0.10     10.4.0.18       YES manual up                    up
FastEthernet0/0.20     10.4.0.27       YES manual up                    up
FastEthernet0/0.30     10.4.0.1        YES manual up                    up
FastEthernet0/1        unassigned      YES unset  up                    down
Vlan1                  unassigned      YES unset  administratively down down
Router(config)#do show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.4.0.0/28 is directly connected, FastEthernet0/0.30
C       10.4.0.16/29 is directly connected, FastEthernet0/0.10
C       10.4.0.24/29 is directly connected, FastEthernet0/0.20

Router(config)#
```

(Figure 4)

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

The given DHCP server resides on a remote subnet. To locate this DHCP server, the clients will make a broadcast request which the routers does not forward beyond their subnet. For this reason, we make use of ip-helper address command to relay the client's broadcast requests for this UDP service. The ip helper address will accept the broadcast request for

DHCP service and forward it as a unicast request to a specific IP address (10.100.1.150) which belongs to the DHCP server.
Host A broadcast for an ip address which will be relayed to the default gateway, that is the router of branch west/east coast headquarter having ip 10.x.x.x. The default router will have an ip helper address for DHCP service which will be the address of the DHCP server (10.100.1.150). The broadcast request will then be forwarded to the next hop router (headquarter router) as a unicast request. The next hop router will also have ip helper address due to which it is able to find its way to the DHCP server. The response is routed back to the user end router and then back to the client via MAC address.

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.).

Port security is a layer 2 traffic control feature which enables an administrator to configure individual switch ports to allow only a specific number of source MAC addresses which ingress the port. The primary use of port security is to prevent users from adding extra switches to the switch in order to extend the reach of the network so that two or more users can share a single access port. This feature can be used to restrict input to an interface by limiting and identifying the MAC addresses of the clients that can access the port. If Port security is configured, then it should be configured on all user facing interfaces. By default, port security limits the ingress MAC address count to 1. This count can be modified to accommodate a host or an ip phone and we could also modify the maximum MAC count for access and voice vlans independently.

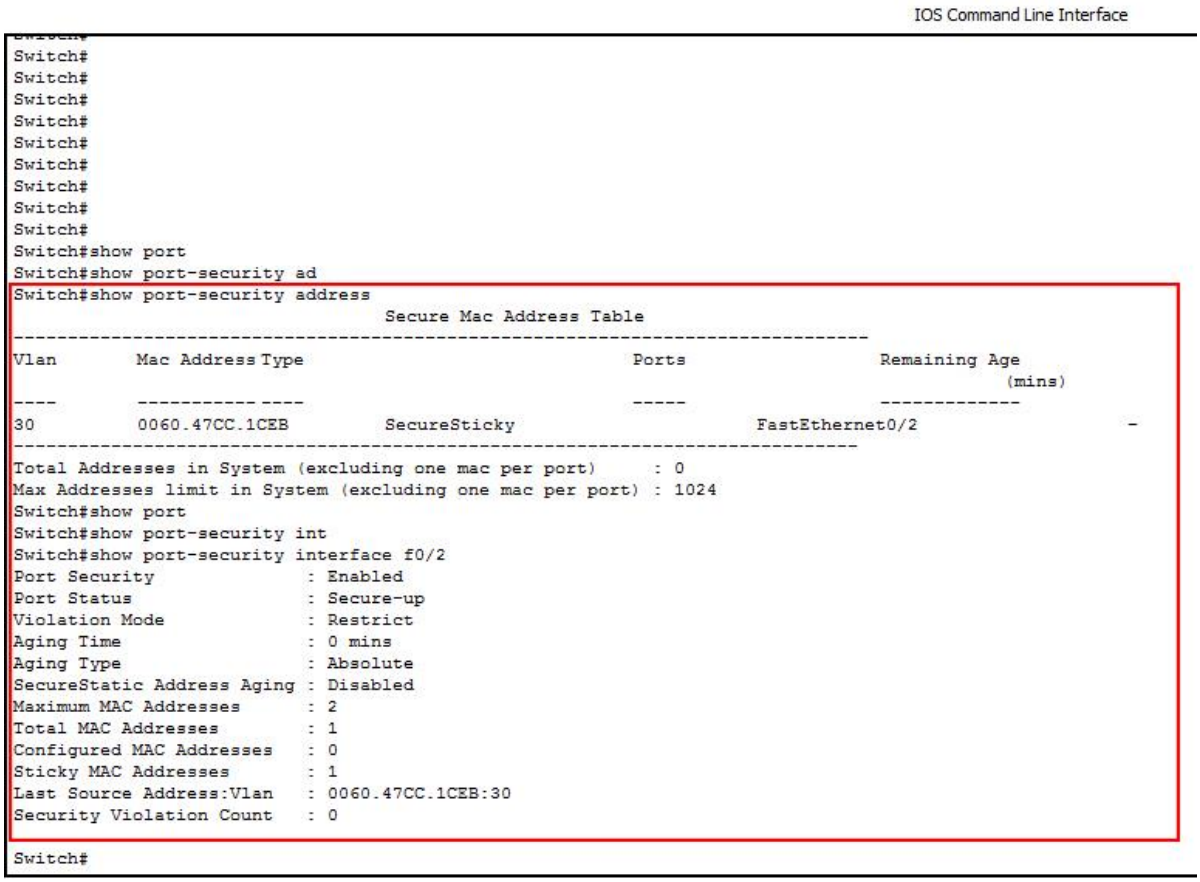
IOS Command Line Interface

```
%LINK-5-CHANGED: Interface FastEthernet0/15, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to up

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up


Switch>
Switch>
Switch>
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int
Switch(config)#interface range
Switch(config)#interface range f0/2
Switch(config-if-range)#swi
Switch(config-if-range)#switchport mode
Switch(config-if-range)#switchport mode acc
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#swi
Switch(config-if-range)#switchport po
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maxi
Switch(config-if-range)#switchport port-security maximum 2
Switch(config-if-range)#swi
Switch(config-if-range)#switchport port
Switch(config-if-range)#switchport port-security vio
Switch(config-if-range)#switchport port-security violation re
Switch(config-if-range)#switchport port-security violation restrict ?
  <cr>
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security mac
Switch(config-if-range)#switchport port-security mac-address st
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#
```

(Figure 5)

A security violation occurs when the maximum number of secure MAC addresses is reached, and if the MAC address of a client attempting to access the port is different from any of the identified secure MAC addresses.

In our design module, we make use of *RESTRICT* mode for security violation (Figure 5). In this mode, the frames for MAC addresses other than allowed addresses are dropped. Port numbers f0/2 to f0/15 are all user facing access ports with max limit of MAC learning to 2 and MAC addresses are configured to be sticky. These addresses are dynamically learned or manually configured, stored in the table and added to the running configuration. If these addresses are saved in the coding file, the interface does not need to dynamically relearn them when the switch restarts. Figure 6 shows the port-security addresses implemented in our design.



(Figure 6)

b) Where should DHCP Snooping be deployed?

DHCP snooping is an access layer security feature. Any switch containing access ports in a vlan serviced by DHCP is a potential candidate. In our design, it is the switch(switch0) that is connected to the router- i.e. deployed on vlans. DHCP snooping requires to differentiate between trusted and untrusted interfaces. Trusted interfaces are those which are connected to the DHCP server or another switch and trusted interface is configured to receive only messages from within the network, which in this case is the trunk port connected to the branch router (f0/1). Untrusted interfaces are those connected to the end user, that is configured to receive messages from outside the network or firewall i.e. interfaces f0/2 to f0/15. DHCP snooping provides security by maintaining DHCP snooping binding table - a database that lists client mac address, DHCP assigned address, switchport, vlan and remaining DHCP lease time. This table helps to filter all untrusted DHCP messages from a rogue DHCP server. To retain the bindings across switch reloads, we must use the DHCP snooping database agent without which the bindings established are lost upon switch reload. The Figure 7 shows the configuration of DHCP snooping and the trusted port.

```
Switch#ip dh
Switch#config
Configuring from terminal, memory, or network [terminal]? t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp
Switch(config)#ip dhcp ?
  excluded-address  Prevent DHCP from assigning certain addresses
  pool              Configure DHCP address pools
  relay             DHCP relay agent parameters
  snooping          DHCP Snooping
Switch(config)#ip dhcp snoo
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snoop vlan 10,20,30
Switch(config)#int f0/1
Switch(config-if)#ip dhcp snoop
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#show ip dhcp snoopi
Switch#show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10,20,30
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                  Trusted    Rate limit (pps)
------------------------   -------    ----------------
FastEthernet0/1            yes        unlimited
Switch#
```

(Figure 7)

c) Where should Dynamic ARP Inspection be deployed? Remember, DAI is configured per-port.

It is recommended to configure dynamic ARP inspection only on ports facing the end-user as untrusted ports. Port nos. f0/2 to f0/15.ports connecting network devices such as switches should be configured as trusted to avoid connectivity issues. DAI relies on DHCP snooping table information to perform ARP packets validation. DAI deployment involves identification of trusted and untrusted ports. DAI will trust and allow ARP packets on all trusted interfaces without inspection and will intercept all packets on untrusted interface. When DAI intercepts packets, it compares the source mac and ip address with the DHCP snooping binding table; if no valid entry is found then it will drop the ARP packet and the local ARP cache is not updated. Since DAI relies on DHCP snooping binding table, we must allow the binding table to be built before applying DAI, or else DAI will block all traffic.

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

To protect against DTP attacks the following things can be done:

a) **Disable auto-trunking mode i.e. Dynamic Desirable or Dynamic auto: Which means they negotiate to trunk port if the connecting device advertises itself as trunk on all trunk ports. i.e. f0/1 (trunk port) on switch0**

b) **Disable DTP Advertisements- All ports advertise and waits for DTP communications to switchport modes. We should disable this so that it will prevent any negotiations from occurring. This will result from either setting ports to access mode or setting trunking ports to non-negotiate.**

c) **Shut down ports- Ports with no devices connected to them should be shutdown administratively as all physical ports are enabled by default on a switch.**

d) **Assign to a non-existent vlan- Set all unused ports to a non-existent VLAN to prevent any leakage of data, just in case the ports become enabled accidentally i.e. f0/15 to f0/24 on switch0.**

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

In an STP attack, a rogue workstation could start generating superior configuration BPDU's in order to elect itself as the ROOT Bridge. The 2 best methods to protect against the STP attacks would be enabling either "BPDU GUARD" and "ROOT GUARD" feature.

a) **BPDU Guard: BPDU guard should be enabled on all end user facing ports i.e. port f0/2 to f0/15 on switch0. All access ports are put into portfast mode because the access port does not participate in the STP and does not need to go through listening and learning state. On a BPDU guard enabled interface, the first reception of any type of BPDU will force the port into an "Err-disabled" state and it remains in err-disabled state until manually turned on. BPDU guard can be enabled on all ports where portfast is enabled by using the command "spanning-tree portfast bpduguard default".**

b) **Root Guard: Root guard feature is also enabled on an interface by interface basis but will only stop data from being forwarded on an interface while it is receiving superior Configuration BPDU's. If a "Root Guard" enabled interface receives a superior BPDU, the port is placed in the "BLOCKING" state for being "ROOT-INCONSISTENT" and will not forward traffic as long as it continues to receive superior BPDU's. This feature should be enabled on all interfaces that will connect to other switches. In our design, root is not enabled as no switches are connected to each other.**

c) **All unused ports should be shut in order to prevent any unwanted new connections.**

f) How will you handle VTP?

On configuring a new VLAN on any of the VTP server, the VLAN gets distributed across all the switches in the domain. So, the need to configure the same VLAN everywhere is removed. Vtp uses a versioning system with a client sever architecture. Clients sync their configuration with Vtp server to maintain current VLAN database version. If VTP is not required, configure switches in transparent mode in which the switch does not advertise its vlan configuration and does not synchronise its vlan configuration based on received advertisements. For our design,

a. **We keep our switches in transparent mode and VTP password is set using MD5 encryption.**
b. **Non-participating switches should be configured in transparent mode.**
c. **Enable vtp pruning, which is used to eliminate unnecessary traffic- unnecessary unicasts and broadcasts in a vlan.**

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

Attacker can use the CDP and LLDP information to discover the entire topology of our network at layer 2 and layer 3 because of which most people choose to disable CDP throughout the network. This can be done on routers that connect to internet, but on the other hand, insider attacks are also possible. It is hard to decide whether we need to disable CDP or not. In such situations the decision depends upon how much we can trust our network users. Therefore, we disable CDP and LLDP, where we do not need it and implement only where it administratively necessary i.e. ports on which ip phones are connected.

Task 3: Layer-3 Routing

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

IP Schemes:

Las Vegas Branch (NV): 10.4.0.0/16

a) **VLAN 30 – PC: 10.4.0.0 – 10.4.0.15/28.**

Network address 10.4.0.0
Broadcast address 10.4.0.15
Default Gateway: 10.4.0.1

b) Vlan 10 – Phones: 10.4.0.16 – 10.4.0.23
Network address 10.4.0.16
Broadcast address 10.4.0.23
Default Gateway: 10.4.0.17

c) Vlan 20 – Printers: 10.4.0.24 – 10.4.0.31
Network address 10.4.0.24
Broadcast address 10.4.0.31
Default Gateway: 10.4.0.25

Similarly, we design IP schemes for LANs on every branch router as follows:

Seattle Branch (WA): 10.9.0.0/16

a) VLAN 30 – PC: 10.9.0.0 – 10.9.0.15/28.

b) Vlan 10 – Phones: 10.9.0.16 – 10.9.0.23

c) Vlan 20 – Printers: 10.9.0.24 – 10.9.0.31

Dallas Branch (TX): 10.3.0.0/16

a) VLAN 30 – PC: 10.3.0.0 – 10.3.0.15/28.

b) Vlan 10 – Phones: 10.3.0.16 – 10.3.0.23

c) Vlan 20 – Printers: 10.3.0.24 – 10.3.0.31

San Jose West Coast Headquarters (CA): 10.1.0.0/16

d) VLAN 30 – PC: 10.1.0.0 – 10.1.0.15/28.

e) Vlan 10 – Phones: 10.1.0.16 – 10.1.0.23

f) Vlan 20 – Printers: 10.1.0.24 – 10.1.0.31

Detroit Word Headquarters (MI): 10.5.0.0/16

d) **VLAN 30 – PC: 10.5.0.0 – 10.5.0.15/28.**

e) **Vlan 10 – Phones: 10.5.0.16 – 10.5.0.23**

f) **Vlan 20 – Printers: 10.5.0.24 – 10.5.0.31**

New York East Coast Headquarters (NY): 10.2.0.0/16

g) **VLAN 30 – PC: 10.2.0.0 – 10.2.0.15/28.**

h) **Vlan 10 – Phones: 10.2.0.16 – 10.2.0.23**

i) **Vlan 20 – Printers: 10.2.0.24 – 10.2.0.31**

Newark Branch (NJ): 10.6.0.0/16

g) **VLAN 30 – PC: 10.6.0.0 – 10.6.0.15/28.**

h) **Vlan 10 – Phones: 10.6.0.16 – 10.6.0.23**

i) **Vlan 20 – Printers: 10.6.0.24 – 10.6.0.31**

Raleigh Branch (NC): 10.7.0.0/16

j) **VLAN 30 – PC: 10.7.0.0 – 10.7.0.15/28.**

k) **Vlan 10 – Phones: 10.7.0.16 – 10.7.0.23**

l) **Vlan 20 – Printers: 10.7.0.24 – 10.7.0.31**

Boston Branch (MA): 10.8.0.0/16

j) **VLAN 30 – PC: 10.8.0.0 – 10.8.0.15/28.**

k) **Vlan 10 – Phones: 10.8.0.16 – 10.8.0.23**

l) **Vlan 20 – Printers: 10.8.0.24 – 10.8.0.31**

Ip addressing scheme between San Jose Branch router and Las Vegas Branch router are as follows:

a) Las Vegas – San Jose: 10.255.255.1 – 10.255.255.2/31.
b) San Jose – Detroit: 10.255.255.3 – 10.255.255.4/31.
c) Detroit – DHCP Server: 10.100.1.149 – 10.100.1.150/31.
d) Seattle – San Jose: 10.255.255.5 – 10.255.255.6/31.
e) Dallas – San Jose: 10.255.255.7 – 10.255.255.8/31.
f) Newark – New York: 10.255.255.9 – 10.255.255.10/31.
g) Raleigh – New York: 10.255.255.11 – 10.255.255.12/31.
h) Boston – New York: 10.255.255.13 – 10.255.255.14/31.

Routing table

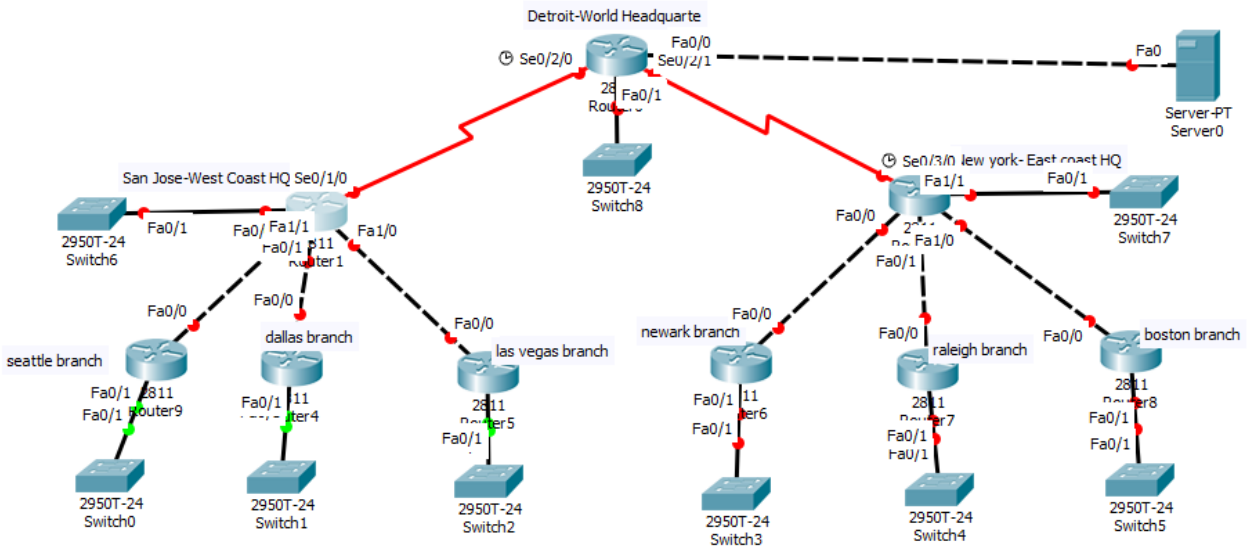
a) 10.4.0.0/28: Directly connected to fa0/1 – Sub interface fa0/1.30.
b) 10.4.0.16/29: Directly connected to fa0/1 - Sub interface fa0/1.10.
c) 10.4.0.24/29: Directly connected to fa0/1 - Sub interface fa0/1.20.
d) 10.255.255.1/31: Directly connected to fa0/0.
e) 10.255.255.2/31: Connected via 10.255.255.1/31.
f) 10.100.1.148/30: Connected via 10.255.255.1/31.

Task 4: Basic Layer-3 Security

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.

Wake on LAN is a technology that allows a network professional to remotely power on a computer or to wake it up from sleep mode. It is also a type of broadcast technology in which the packets are sent within the same network. Wake on LAN works by sending a wake-up frame or packet to a client machine from a server machine that has remote network management software installed. The Wake on LAN network adapter installed in the client

receives the wake-up frame and gets turned on. So as the update server is having an IP address "10.100.1.160" and all the PCs are not on the server's network, the server will then send a directed broadcast containing a magic packet for computer's NIC and for this the directed broadcast service must be allowed on every router. Magic packets are usually sent over the network and contain the subnet information, network broadcast address, and the MAC address of the target computer's network card, whether Ethernet or wireless. Now, we know that allowing directed broadcast will open the gates for Smurf Attack on the network. To avoid this, an ACL will be assigned to the ingress of router connected to the update server. As a WOL packet an ICMP request, it will target the UDP port 9 of the PCs and thus by assigning this ACL, the routers will accept packets only from the sources specified in ACL.



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

For protecting our network from ip spoofing on all applicable switch ports, we have enabled ip source guard which blocks all ip traffic received on the interface except for DHCP packets allowed by DHCP snooping. Ip source guard is supported on access port with ip source filtering or with source address filtering. It is enabled along with DHCP snooping on all untrusted ports i.e. f0/2 to f0/15 on switch0, since these ports have maximum chances of getting spoofed. The ip source binding table has bindings that are learned by DHCP snooping or are manually configured.
An entry in this table has ip address, its associated mac address, and its associated vlan number. Ip source guard uses the entries created by DHCP snooping to validate the hosts connected to a switch. Any traffic received from a host without valid DHCP binding entry is

dropped.

c) 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.

Router(config)# ip access-list ext ingress-antispoof
Router(config-ext-nacl)# deny ip 10.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# deny ip 172.16.0.0 0.15.255.255 any
Router(config-ext-nacl)# deny ip 192.168.0.0 0.0.255.255 any
Router(config-ext-nacl)# deny ip 127.0.0.0 0.255.255.255 any
Router(config-ext-nacl)# deny ip 224.0.0.0 31.255.255.255 any
Router(config-ext-nacl)# deny ip 169.254.0.0 0.0.255.255 any
Router(config-ext-nacl)# permit ip any any

d) Extra Credit: On the same layer-3 interfaces above, protect against incoming/outgoing packets with invalid addresses.

For outgoing packets:

access-list 130 permit ip 10.4.0.0 0.0.0.15 any
access-list 130 permit ip 10.4.0.16 0.0.0.7 any
access-list 130 permit ip 10.4.0.24 0.0.0.7 any
ip access 130 deny ip any any log

Interface f0/1
ip access group 130 out

For incoming packets from WAN, DHCP.
access list 111 permit ip 10.255.255.0 0.0.0.1 any

access list 111 permit ip 10.100.1.150 0.0.0.0 any

interface f0/0
ip access-group 111 in