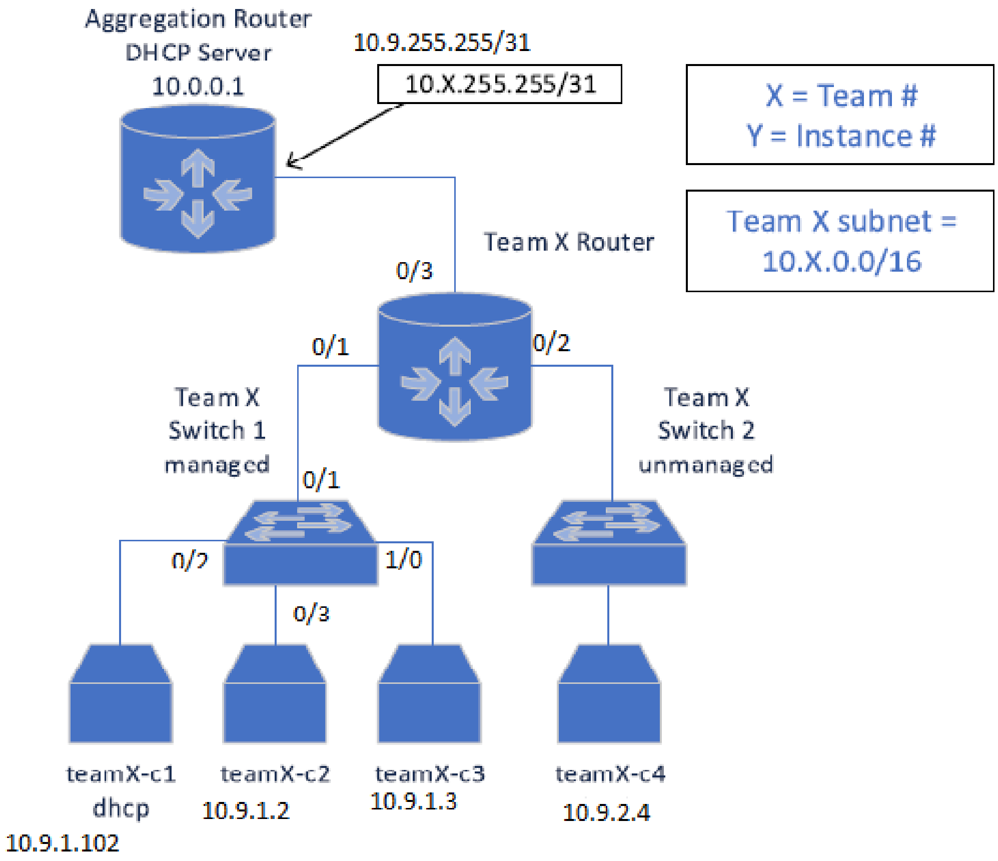
Team 9

Ronn Joseph – rj85

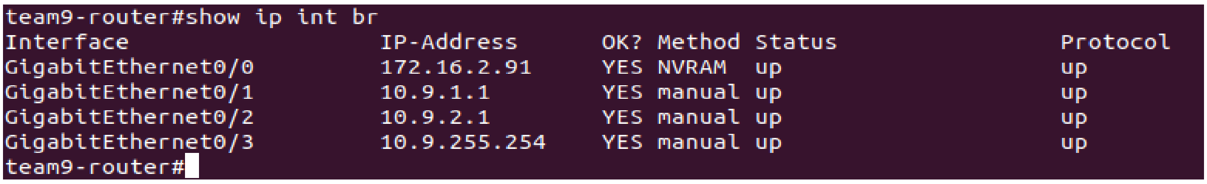
Akilnath Bodipudi – ab2348

CS646 – Project 2



Task 1:

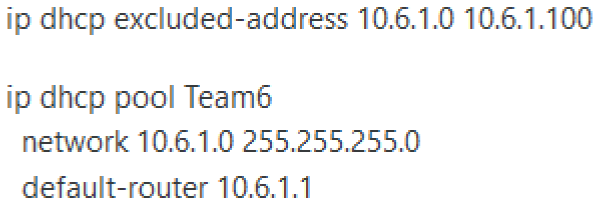
a. Initially, We established the connectivity across four clients nodes and aggregation router/ DHCP server, we were able to ping all the devices on network interfaces in addition to their management.



```
team9-router#show ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     172.16.2.91     YES NVRAM  up                    up
GigabitEthernet0/1     10.9.1.1        YES manual up                    up
GigabitEthernet0/2     10.9.2.1        YES manual up                    up
GigabitEthernet0/3     10.9.255.254    YES manual up                    up
team9-router#
```

There were no ip address assigned to interfaces of the switch expect management ip. We configured router to be DHCP relay agent between DHCP server and client 1. The client’s 2,3 and 4 are configured with static ip addresses where as client 1 is configured to be dhcp client.

On the router, we configured dhcp pool for ip 10.9.1.0 network as mentioned in forum:



```
ip dhcp excluded-address 10.6.1.0 10.6.1.100

ip dhcp pool Team6
 network 10.6.1.0 255.255.255.0
 default-router 10.6.1.1
```

In addition, we also included ip route in client 1, in order to establish connectivity to DHCP server:

Sudo route add – int 10.0.0.0 netmask 255.0.0.0 gw 10.9.1.1

b. For ssh, we configured client/server with the following for router/switch:

- ssh version 2
- authentication timeout 120 secs.
- Authentication retries 3.
- RSA Key size 1024 bits.

c. We created two accounts (Admin and User) with appropriate privilege levels. Where admin has full-access and user read-only access for both router and switch.

Username admin privilege 15 secret admin
Username user privilege 1 secret user

d. We backed up router/switch configuration to jump host using the commands mentioned in the forum. We enabled secure copy server on both router/switch and on jump host. We executed command:

Scp cisco@172.16.2.91 : running-config .   (router)
Scp cisco@172.16.2.92 : running-config .   (switch)

e. To protect the router/switch VTY’s from being accessed by clients we enable access-list on the VTY lines.

Access-list 4 deny 10.9.1.0 0.0.0.255
Access-list 4 deny 10.9.2.0 0.0.0.255
Access-list permit any
We enabled access-list in VTY line with command: **access-class for in vrf-also**

VTY connection is only permitted only after enable vrf -also.

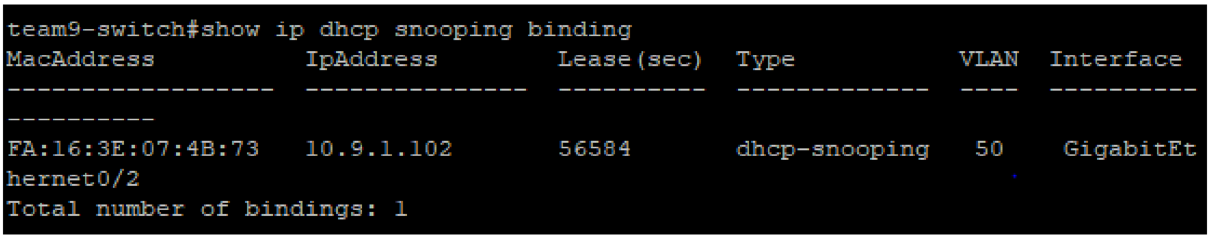
Task 2 :

a. To protect switch ports from mac address table overflow attack, we attempted to implement port-security to apply congestion control and prevent switch ports from learning more MAC address than necessary. Because of the way Private VLANs were configured, we implemented only on **interface giga 0/1** because interface 0/1 configured in promiscuous mode. Therefore, all communication between primary Vlan and rest of the network will communicate thru this "Gateway".

```
Switchport port-security
Switchport port-security maximum 10
Switchport port-security mac-address sticky
Switchport port-security mac-address fa16.3e07.4b73
Switchport port-security mac-address fa16.3e4d.1b7b
Switchport port-security mac-address fa16.3ea9.e316
Switchport port-security mac-address fa16.3eaf.bf4c
```

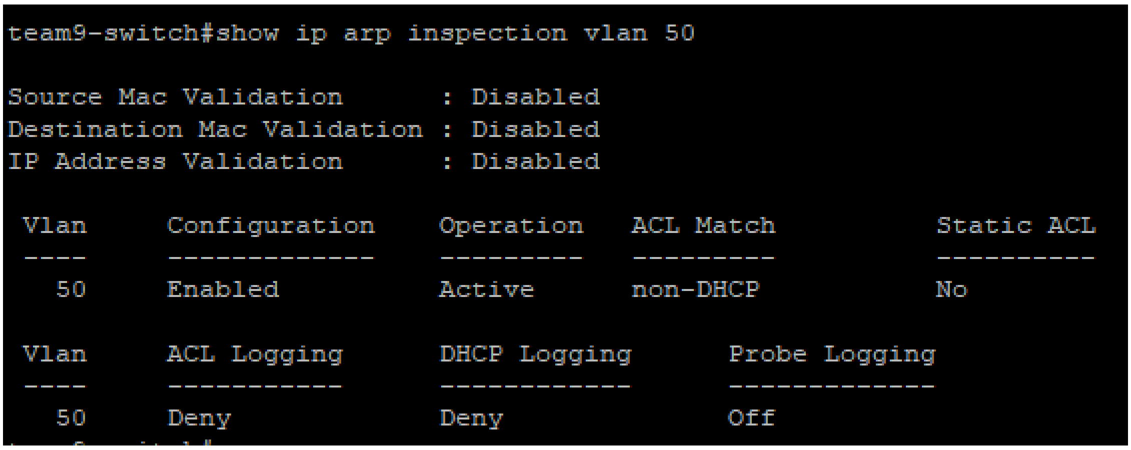
b. We protected our clients from arp cache poisoning attacks by implementing dynamic arp inspection. To implement dynamic arp inspection, we need to enable dhcp snooping: so that we can use dynamic binding table to make sure MAC address are trusted devices and filters out untrusted devices.

```
Switch DHCP snooping is enabled
Switch DHCP gleaning is disabled
DHCP snooping is configured on following VLANs:
50
DHCP snooping is operational on following VLANs:
50-52
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is disabled
   circuit-id default format: vlan-mod-port
   remote-id: 5e00.0023.0000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                  Trusted    Allow option    Rate limit (pps)
-----------------------    -------    ------------    ----------------
GigabitEthernet0/1           yes        yes             unlimited
  Custom circuit-ids:
```



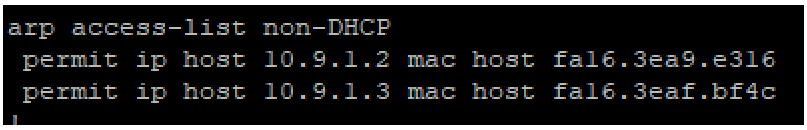
```
team9-switch#show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ----------
----------
FA:16:3E:07:4B:73   10.9.1.102       56584       dhcp-snooping   50    GigabitEt
hernet0/2
Total number of bindings: 1
```

We used dynamic arp inspection in vlan 50 to validate arp packets by intercepting them to verify their ip and MAC address that are binded to trusted client and allow the communication. Dynamic arp inspection uses dhcp snooping to verify arp packets in their dynamic IP address. Since we have a mixed environment of static and dynamic IP addresses, we will also implement an arp access-list to verify non-dhcp clients.



```
team9-switch#show ip arp inspection vlan 50

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
   50     Enabled          Active      non-DHCP           No

 Vlan     ACL Logging      DHCP Logging      Probe Logging
 ----     -----------      ------------      -------------
   50     Deny             Deny              Off
```

Below is the arp access-list(non-DHCP), also used to verify arp packets



```
arp access-list non-DHCP
 permit ip host 10.9.1.2 mac host fa16.3ea9.e316
 permit ip host 10.9.1.3 mac host fa16.3eaf.bf4c
```

c. To combat DTP attacks, we **disabled dynamic trunking** and changed all ports which does not require trucking ports to access ports and refrained from using vlan 1.

   In addition, we applied command: **switchport nonegotiate,** the device will not engage in negotiation protocol on interfaces gi 0/1-3 , 1/0 .
   These commands are applied to stop vlan hopping and attacks on 802.1q

d. To combat STP attacks, we **enabled root guard** and **bpdu guard.**
   Command: **spanning tree bpduguard enable , spanning tree guard root**
   The root guard is enabled in order to protect against yersinia attacks claiming root role, the root guard keeps on blocking port until a device stops attempting to become a root.

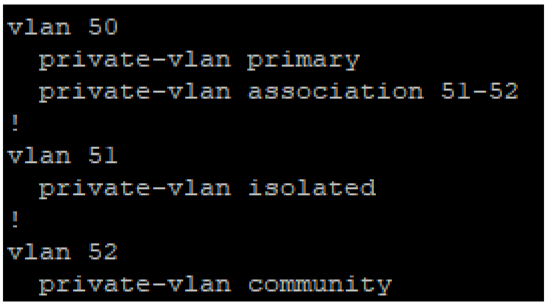
The bpdu guard protects from Yersinia attacks which is causes switchports to enter forwarding state of STP. These two mitigations are being implemented on interface gi 0/1-3, 1/0.

e. To counter the VTP attacks such as deleting VLAN and attacks that use VTP(VLAN Trunking Protocol) , we should use the command **VTP mode off,** but since we are configuring private VLANs, the next best mitigation would be is to apply **VTP mode transparent** globally.
f. To protect against attacks that uses CDP and LLDP, we used the commands **No CDP run, NO LLDP run, (**globally**).** The reason is that CDP/LLDP is not authenticated in anyway. And is prone to CDP table flooding attack.

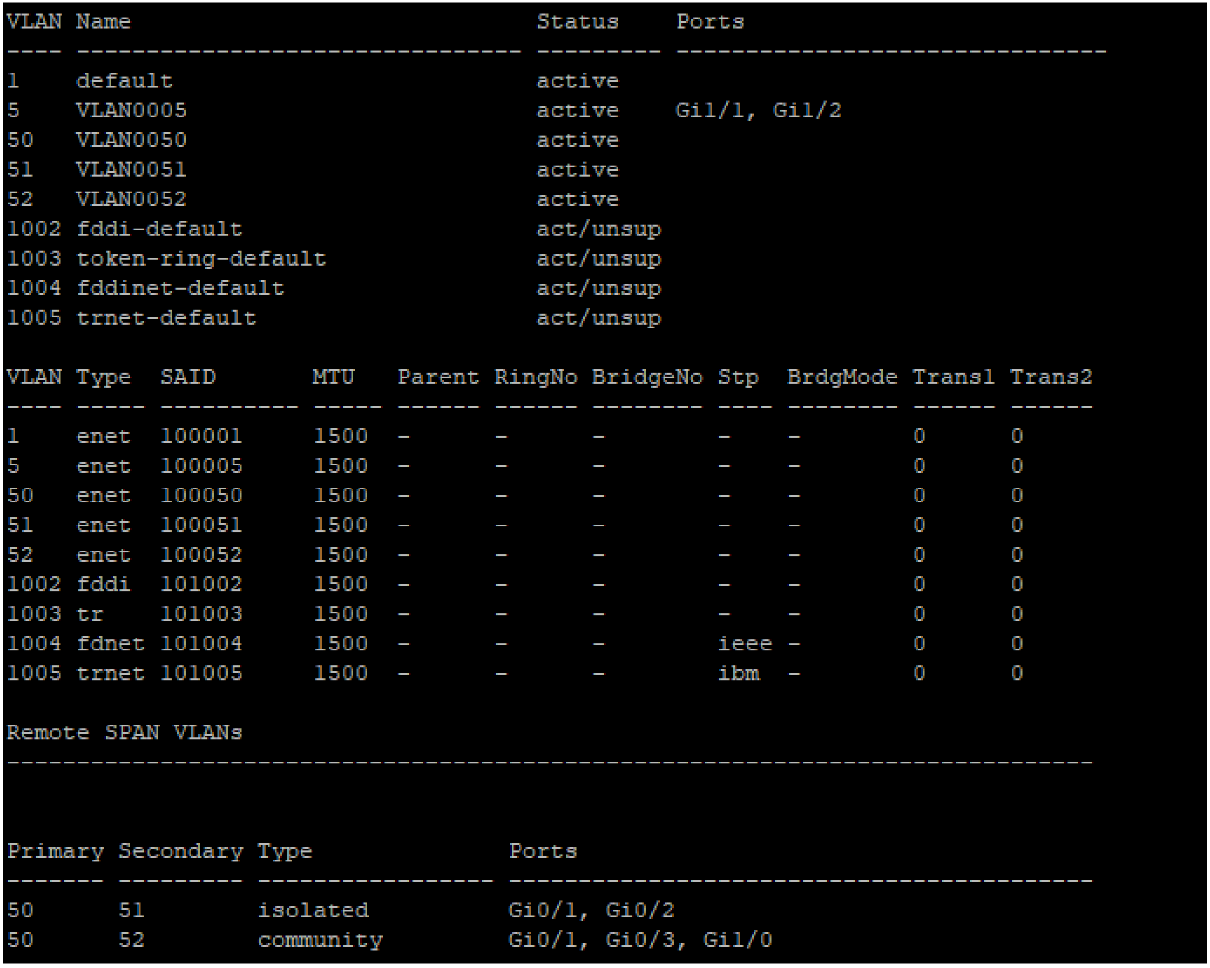
Refer to next page

g. We prevented client 1 from communicating with client 2 and 3 by implementing private VLAN and having client 1 encapsulated within isolated port.
   We appointed vlan 51 as isolated vlan that is connected through interface gi 0/2, which can only communicate with promiscuous port from the VLAN.

h. We prevented client 2 and 3 from communicating with client 1 by implementing private VLAN and having client 2 and 3 encapsulated within community ports.
   We appointed vlan 50 as primary vlan and vlan 52 as community vlan that connected through interface gi 0/3 and gi 1/0. In this way, clients 2and 3 communicate with each other and with promiscuous port. The promiscuous port is located on interface gi 0/1, which lets the member of private vlans communicate with rest of the networks(see references).



```
vlan 50
  private-vlan primary
  private-vlan association 51-52
!
vlan 51
  private-vlan isolated
!
vlan 52
  private-vlan community
```



```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
5    VLAN0005                         active    Gi1/1, Gi1/2
50   VLAN0050                         active
51   VLAN0051                         active
52   VLAN0052                         active
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
5    enet  100005     1500  -      -      -        -    -        0      0
50   enet  100050     1500  -      -      -        -    -        0      0
51   enet  100051     1500  -      -      -        -    -        0      0
52   enet  100052     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

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


Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
50      51        isolated          Gi0/1, Gi0/2
50      52        community         Gi0/1, Gi0/3, Gi1/0
```

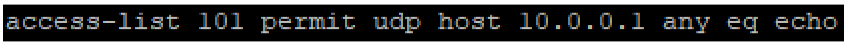
Task 3

a. The WOL(Wake On Lan) will be forwarding a magic packet which the packet must be sent to device. Where the device will wake up only on the information in WoL packet. This process called subnet directed broadcast.
We must configure the helper-address (10.0.0.1) on the interface 0/1 on router, we used port 7 for WOL. The reason is that port 7 which sends echo signal automatically to device.
Interface gi0/1
We configured router by making the magic packet to send to 10.9.2.0 network thru router(172.16.2.91) with help of helper address.
Ip forward-protocol udp 7

For each remote network, we need to add an ip helper-address on router interface, which is server gateway.
Interface gi0/3
Ip helper-address 10.9.1.255
Ip helper-address 10.9.2.255

This will allow us to forward WoL packets from server, the final step is to enable port 7 for remote clients
Access-list 101permit udp host 10.0.0.1 any eq 7
Interface gi0/1
Ip helper-address 10.0.0.1
Ip directed-broadcast 101

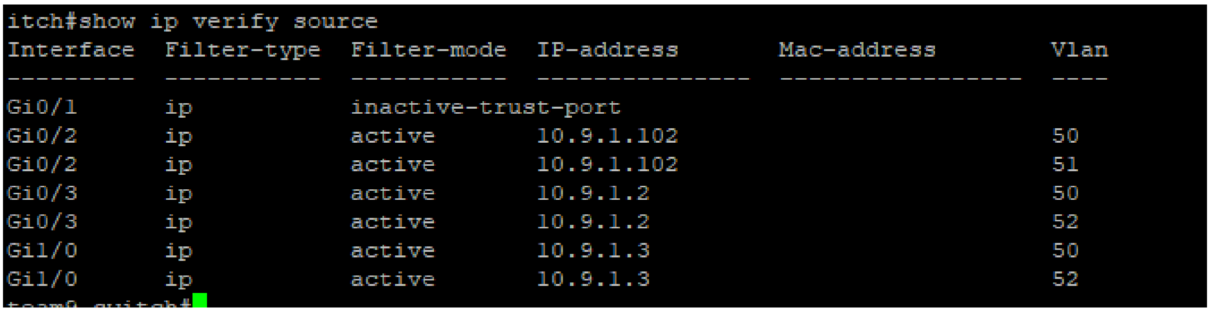
The below screenshot shows the output for WoL, where aggression server 10.0.0.1 send the magic packet via port 7 but in buldiing configuration it shows echo, the reason is that the configured by default as a proxy to relay Wake-on-LAN (WOL) magic packets from the Internet to hosts on the local network in order to wake them up remotely.



```
access-list 101 permit udp host 10.0.0.1 any eq echo
```

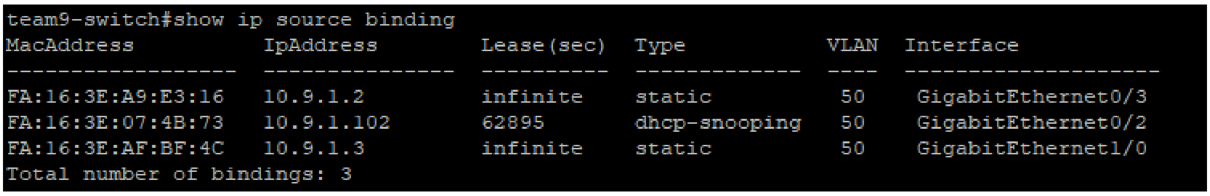
Refer to next page

b. The IP spoofing was protected against on all switch ports thru the utility of ip source guard. We enabled IP source guard by using DHCP snooping, which is enabled on an untrusted interface. After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. The IP source binding table is being binded that they are learned by DHCP snooping configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. We enabled ip source guard on interfaces 0/1-3, 1/0.



```
itch#show ip verify source
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----
Gi0/1      ip           inactive-trust-port
Gi0/2      ip           active       10.9.1.102                          50
Gi0/2      ip           active       10.9.1.102                          51
Gi0/3      ip           active       10.9.1.2                            50
Gi0/3      ip           active       10.9.1.2                            52
Gi1/0      ip           active       10.9.1.3                            50
Gi1/0      ip           active       10.9.1.3                            52
team9-switch#
```

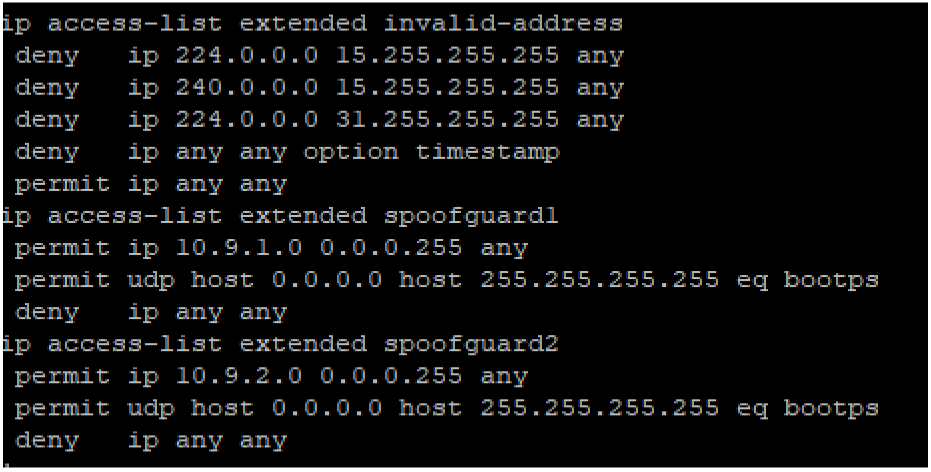
After the MAC address and IP address are binded to the respective clients, IP source guard will use the binding table to verify legitimate traffic on the mentioned interfaces.



```
team9-switch#show ip source binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
FA:16:3E:A9:E3:16   10.9.1.2         infinite    static          50    GigabitEthernet0/3
FA:16:3E:07:4B:73   10.9.1.102       62895       dhcp-snooping   50    GigabitEthernet0/2
FA:16:3E:AF:BF:4C   10.9.1.3         infinite    static          50    GigabitEthernet1/0
Total number of bindings: 3
```

c. The access-lists “spoofguard1” and “spoofguard2” contains rules to prevent ip-spoofing. These access-lists also allows possible new dhcp clients to discover dhcp server within the network(10.9.0.0/16). Spoofguard 1 is used to prevent possible incoming spoofing attacks from clients 1,2 or 3. Spoofguard 2 is used for same purpose against client 4. Spoofguard 1 and 2 are limited to only preventing spoofing attacks from different networks. The clients in that particular network could be still able to spoof within their network. Eg: client 2(10.9.1.2) and client 4(10.9.2.4) cannot spoof each other IPs, but client 2 could spoof client 3(10.9.1.3).

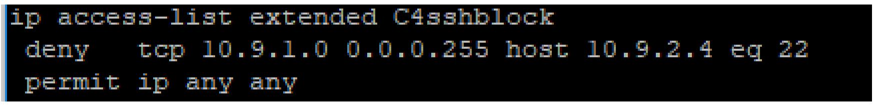
We used the following access lists for c and d:



```
ip access-list extended invalid-address
 deny   ip 224.0.0.0 15.255.255.255 any
 deny   ip 240.0.0.0 15.255.255.255 any
 deny   ip 224.0.0.0 31.255.255.255 any
 deny   ip any any option timestamp
 permit ip any any
ip access-list extended spoofguard1
 permit ip 10.9.1.0 0.0.0.255 any
 permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
 deny   ip any any
ip access-list extended spoofguard2
 permit ip 10.9.2.0 0.0.0.255 any
 permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
 deny   ip any any
```

d. This access-list “invalid-address” contains rules against blocking packets from invalid addresses and other circumstances, the list blocks the source addresses in their 224/4 and 240/4 block, the packets with timestamp ip option. The first three lines indented to deny the ip addresses, that are reserved for future and research purposes, they are also not for operations. The timestamp line is used to drop any packets with time stamp option enabled to avoid timebased attacks.

e. To prevent client 1, 2,3 from being able to ssh into client 4 via data network, we implemented a access-list(C4sshblock). We applied this list into interface gi0/1 inbound. In this way, client 4 can still able to communicate with other clients not have any communication disrupted.



```
ip access-list extended C4sshblock
 deny   tcp 10.9.1.0 0.0.0.255 host 10.9.2.4 eq 22
 permit ip any any
```

Running config(switch)

```
Building configuration...

Current configuration : 5642 bytes
!
! Last configuration change at 18:23:43 UTC Tue Apr 16 2019 by cisco
!
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service compress-config
!
hostname team9-switch
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable password cisco
!
username admin privilege 15 secret 5 $1$QITX$OScxraqz3KHVu.yAKgVrC0
username user secret 5 $1$w/aR$mKa3JM0qrihPFenqQMXAv1
username cisco privilege 15 secret 5 $1$gIoD$eJSPsCul5pwr.uSt.C88B1
no aaa new-model
!
!
!
!
!
vtp domain team9.cs646
vtp mode transparent
ip arp inspection vlan 50
ip arp inspection filter non-DHCP vlan  50
!
!
!
ip dhcp snooping vlan 50
no ip dhcp snooping information option
ip dhcp snooping
no ip domain-lookup
```

```
ip domain-name team9rout
ip cef
no ipv6 cef
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
vlan 5
!
vlan 50
  private-vlan primary
  private-vlan association 51-52
!
vlan 51
  private-vlan isolated
!
vlan 52
  private-vlan community
no cdp run
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface Loopback0
 description Loopback
 no ip address
!
interface GigabitEthernet0/0
 description OOB management
 no switchport
 vrf forwarding Mgmt-intf
 ip address 172.16.2.92 255.255.255.0
 negotiation auto
 no cdp enable
!
interface GigabitEthernet0/1
```

```
 description To router
 switchport access vlan 5
 switchport private-vlan mapping 50 51-52
 switchport mode private-vlan promiscuous
 switchport nonegotiate
 switchport port-security maximum 10
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky fa16.3e4d.1b7b
 switchport port-security
 ip arp inspection trust
 media-type rj45
 negotiation auto
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
 ip dhcp snooping trust
!
interface GigabitEthernet0/2
 description To client1
 switchport access vlan 5
 switchport private-vlan host-association 50 51
 switchport mode private-vlan host
 switchport nonegotiate
 media-type rj45
 negotiation auto
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
!
interface GigabitEthernet0/3
 description To client 2
 switchport access vlan 5
 switchport private-vlan host-association 50 52
 switchport mode private-vlan host
 switchport nonegotiate
 media-type rj45
 negotiation auto
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
!
interface GigabitEthernet1/0
 description To client 3
 switchport access vlan 5
 switchport private-vlan host-association 50 52
 switchport mode private-vlan host
 switchport nonegotiate
 media-type rj45
 negotiation auto
 spanning-tree bpduguard enable
 spanning-tree guard root
 ip verify source
!
interface GigabitEthernet1/1
 description GigabitEthernet1/1
 switchport access vlan 5
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/2
 description GigabitEthernet1/2
 switchport access vlan 5
 switchport mode access
 media-type rj45
 negotiation auto
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip ssh version 2
ip scp server enable
!
!
ip source binding FA16.3EA9.E316 vlan 50 10.9.1.2 interface Gi0/3
ip source binding FA16.3EAF.BF4C vlan 50 10.9.1.3 interface Gi1/0
access-list 4 deny   10.9.1.0 0.0.0.255
access-list 4 deny   10.9.2.0 0.0.0.255
access-list 4 permit any
!
arp access-list non-DHCP
 permit ip host 10.9.1.2 mac host fa16.3ea9.e316
 permit ip host 10.9.1.3 mac host fa16.3eaf.bf4c
!
!
!
control-plane
!
banner exec ^C
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************^
C
```

```
banner incoming ^C
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************^
C
banner login ^C
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************^
C
!
line con 0
 password cisco
line aux 0
line vty 0 4
 access-class 4 in vrf-also
 exec-timeout 720 0
 password cisco
 login local
 transport input ssh
!
!
end
```

Running config(router)

```
Building configuration...


Current configuration : 5179 bytes
!
! Last configuration change at 01:10:01 UTC Mon Apr 15 2019 by cisco
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname team9-router
!
boot-start-marker
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
enable secret 5 $1$T4CZ$/AP27mO/NvKkxmCQ.AUTw/
enable password cisco
!
no aaa new-model
!
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
!
!
!
!
!
no ip source-route
!
!
```

```
!
ip dhcp excluded-address 10.9.1.0 10.9.1.100
!
ip dhcp pool Team9
 network 10.9.1.0 255.255.255.0
 default-router 10.9.1.1
!
!
!
no ip domain lookup
ip domain name team9ssh
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
!
!
username cisco privilege 15 secret 5 $1$qmdz$YR9Z23GvqskEtnxTR.QqV0
username admin privilege 15 secret 5 $1$4b.G$kjOFFarvg88gZW7tEthla.
username user secret 5 $1$wycS$AFkaSImI7Ch6Tq7GTlkmj.
!
redundancy
!
lldp run
!
!
!
!
!
!
!
!
!
!
!
!
!
interface GigabitEthernet0/0
 description OOB Management
 vrf forwarding Mgmt-intf
 ip address 172.16.2.91 255.255.255.0
 duplex full
 speed auto
 media-type rj45
 no cdp enable
!
interface GigabitEthernet0/1
 description To switch1
 ip address 10.9.1.1 255.255.255.0
 ip access-group C4sshblock in
 ip helper-address 10.0.0.1
 ip directed-broadcast 101
 duplex full
 speed auto
 media-type rj45
!
interface GigabitEthernet0/2
 description To switch2
 ip address 10.9.2.1 255.255.255.0
 ip access-group spoofguard2 in
 ip helper-address 10.0.0.1
 ip directed-broadcast 101
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/3
 description To aggregation router
 ip address 10.9.255.254 255.255.255.254
 ip access-group invalid-address in
 ip helper-address 10.0.0.1
 ip helper-address 10.9.1.255
 ip helper-address 10.9.2.255
 duplex full
 speed auto
 media-type rj45
!
router ospf 1
 router-id 1.1.1.1
 network 10.0.0.0 0.255.255.255 area 0
!
router ospf 10
!
ip forward-protocol nd
ip forward-protocol udp echo
!
!
no ip http server
no ip http secure-server
```

```
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip scp server enable
!
ip access-list extended C4sshblock
 deny   tcp 10.9.1.0 0.0.0.255 host 10.9.2.4 eq 22
 permit ip any any
ip access-list extended invalid-address
 deny   ip 224.0.0.0 15.255.255.255 any
 deny   ip 240.0.0.0 15.255.255.255 any
 deny   ip 224.0.0.0 31.255.255.255 any
 deny   ip any any option timestamp
 permit ip any any
ip access-list extended spoofguard1
 permit ip 10.9.1.0 0.0.0.255 any
 permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
 deny   ip any any
ip access-list extended spoofguard2
 permit ip 10.9.2.0 0.0.0.255 any
 permit udp host 0.0.0.0 host 255.255.255.255 eq bootps
 deny   ip any any
!
ipv6 ioam timestamp
!
!
access-list 4 deny   10.9.1.0 0.0.0.255
access-list 4 deny   10.9.2.0 0.0.0.255
access-list 4 permit any
access-list 101 permit udp host 10.0.0.1 any eq echo
!
control-plane
!
banner exec ^C
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************^
C
banner incoming ^C
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************^
C
banner login ^C
**************************************************************************
* IOSv is strictly limited to use for evaluation, demonstration and IOS  *
* education. IOSv is provided as-is and is not supported by Cisco's      *
* Technical Advisory Center. Any use or disclosure, in whole or in part, *
* of the IOSv Software or Documentation to any third party for any       *
* purposes is expressly prohibited except as otherwise authorized by     *
* Cisco in writing.                                                      *
**************************************************************************^
C
!
line con 0
 password cisco
line aux 0
line vty 0 4
 access-class 4 in vrf-also
 exec-timeout 720 0
 password cisco
 login local
 transport input ssh
!
no scheduler allocate
!
end
```

REFERENCES

i). ftp://ftp.hp.com/%2F/pub/networking/software/Security-Oct2005-59906024-Chap09-Port_Security.pdf

ii). https://www.techrepublic.com/blog/it-security/lock-down-cisco-switch-port-security-88196/

iii). https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html

iv). https://www.routerfreak.com/configure-lldp-link-layer-discovery-protocol/

v). https://www.symantec.com/connect/articles/configuring-wol-deployment-solution-cisco-environment

vi). https://community.cisco.com/t5/security-analytics-and/how-to-stop-ip-spoofing-on-the-network/td-p/3394447

vii). https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html

viii). https://www.juniper.net/documentation/en_US/junos/topics/example/port-security-protect-from-spoofing-els.html

ix).https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcpsnoop.html

x). https://www.juniper.net/documentation/en_US/junos/topics/concept/port-security-ip-source-guard.html

xi). https://www.cnetsys.com/how-to-enable-wake-on-lan-wol-windows-7/

xii). https://en.wikipedia.org/wiki/Echo_Protocol

xiii). https://www.symantec.com/connect/articles/configuring-wol-deployment-solution-cisco-environment