

# **Advanced Troubleshooting CCIE Routing & Switching v5.0**

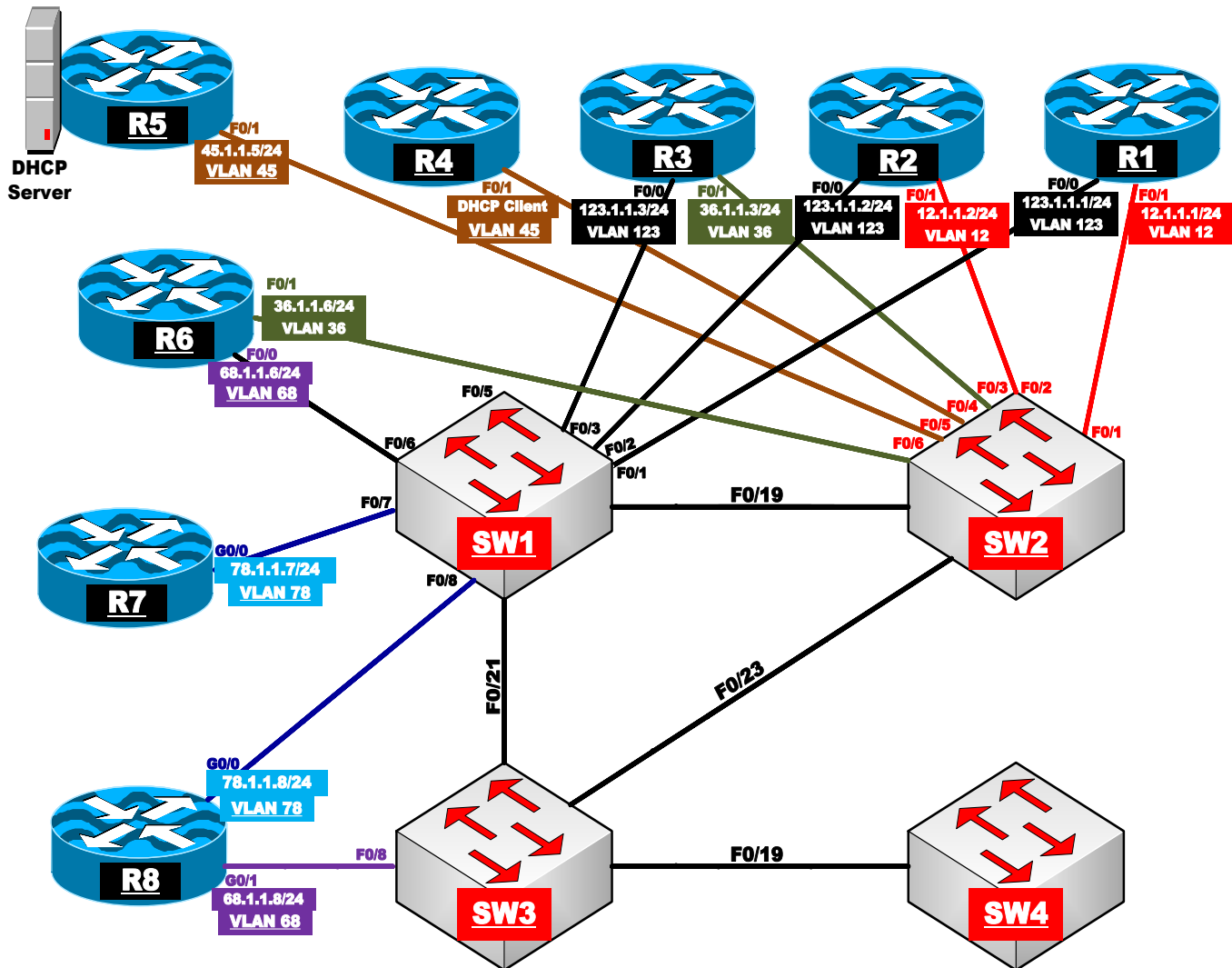
[www.MicronicsTraining.com](http://www.MicronicsTraining.com)

**Narbik Kocharians  
CCSI, CCIE #12410  
R&S, Security, SP**

## **Switching-II Questions & Answers**

# Troubleshooting Switching

## Scenario 2



### Lab Setup:

To copy and paste the initial configurations, go to “CCIE-TS-Initial-configurations” folder → “Switching” → “TS-Switching-Initial-Lab-2”.

## Rules:

- **DO NOT** configure or change the VTP domain on any of the four switches.
- **DO NOT** change VLAN assignments

## Ticket 1

R6 and R8 can establish an Eigrp neighbor adjacency but they don't have reachability. DO NOT change the VLAN assignment, or remove a command by negating it to fix this problem.

**Let's verify the problem:**

### On R6:

```
R6#Show ip eigrp neighbors
```

```
EIGRP-IPv4 Neighbors for AS(1)
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
0	68.1.1.8	Fa0/0	14	00:04:31	2	200	0	6

**It looks like the two routers have established a neighbor adjacency. Let's ping 68.1.1.8 to verify reachability.**

```
R6#Ping 68.1.1.8
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 68.1.1.8, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

**Are these two routers on the same VLAN? Let's check SW1 and SW3:**

### On SW1:

```
SW1#Show Vlan br | Exc unsp
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/9, Fa0/10 Fa0/11, Fa0/18, Fa0/20, Fa0/22

```

Fa0/23, Fa0/24, Gi0/1, Gi0/2
68 VLAN0068 active Fa0/6
212 VLAN0212 active Fa0/12
213 VLAN0213 active Fa0/13
214 VLAN0214 active Fa0/14
215 VLAN0215 active Fa0/15
216 VLAN0216 active Fa0/16
217 VLAN0217 active Fa0/17

```

### On SW3:

SW3#**Show vlan brief | Exc unSUP**

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/9 Fa0/10, Fa0/11, Fa0/18, Fa0/22 Fa0/24, Gi0/1, Gi0/2
<b>68 VLAN0068</b>	<b>active</b>	<b>Fa0/8</b>
212 VLAN0212	active	Fa0/12
213 VLAN0213	active	Fa0/13
214 VLAN0214	active	Fa0/14
215 VLAN0215	active	Fa0/15
216 VLAN0216	active	Fa0/16
217 VLAN0217	active	Fa0/17

**R6 and R8 are in VLAN 68, let's check the trunk and see if the trunk is allowing the traffic for this VLAN to traverse through:**

### On SW1:

SW1#**Show interface trunk**

Port	Mode	Encapsulation	Status	Native vlan
Fa0/19	on	802.1q	trunking	1
Fa0/21	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/19	1-4094
Fa0/21	1-4094

Port	Vlans allowed and active in management domain
Fa0/19	1, <b>68</b> , 212-217
Fa0/21	1, <b>68</b> , 212-217

Port	Vlans in spanning tree forwarding state and not pruned
------	--

```
Fa0/19      1, 68, 212-217
Fa0/21      1, 68, 212-217
```

### **On SW3:**

```
SW3#Show interface trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Fa0/19	desirable	n-802.1q	trunking	1
Fa0/20	desirable	n-isl	trunking	1
Fa0/21	on	802.1q	trunking	1
Fa0/23	on	802.1q	trunking	1

Port	Vlans allowed on trunk
Fa0/19	1-4094
Fa0/20	1-4094
Fa0/21	1-4094
Fa0/23	1-4094

Port	Vlans allowed and active in management domain
Fa0/19	1, 68, 212-217
Fa0/20	1, 68, 212-217
Fa0/21	1, 68, 212-217
Fa0/23	1, 68, 212-217

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/19	1, 68, 212-217
Fa0/20	68
Fa0/21	1, 68, 212-217

Port	Vlans in spanning tree forwarding state and not pruned
Fa0/23	1, 68, 212-217

**So far so good, let's verify the path from SW1 to SW3:**

### **On SW1:**

```
SW1#Show spanning-tree vlan 68
```

```
VLAN0068
Spanning tree enabled protocol ieee
Root ID      Priority    24644
             Address    000c.858b.7a00
```

**Cost 38**

Port 21 (FastEthernet0/19)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32836 (priority 32768 sys-id-ext 68)  
Address 0012.7f40.9380  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/6	Desg	FWD	19	128.8	P2p
<b>Fa0/19</b>	<b>Root</b>	<b>FWD</b>	<b>19</b>	<b>128.21</b>	<b>P2p</b>
Fa0/21	Desg	FWD	19	128.23	P2p

The Fa0/6 interface of SW1 connects to R6, and from SW1's perspective, both F0/19 and F0/21 are in forwarding state, but F0/19 is the root port, and the local switch has a cost of 38, which means that it has to traverse two 100M links (The default cost of a Fast Ethernet interface is 19), this means that SW3 is the root. Let's verify this by repeating the same show command on SW2:

### On SW2:

SW2#**Show spanning-tree vlan 68**

VLAN0068

Spanning tree enabled protocol ieee

Root ID Priority 24644  
Address 000c.858b.7a00

**Cost 19**

Port 25 (FastEthernet0/23)  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32836 (priority 32768 sys-id-ext 68)  
Address 001d.e5d6.0000  
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec  
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
<b>Fa0/19</b>	<b>Desg</b>	<b>FWD</b>	<b>19</b>	<b>128.21</b>	<b>P2p</b>
<b>Fa0/23</b>	<b>Root</b>	<b>FWD</b>	<b>19</b>	<b>128.25</b>	<b>P2p</b>

Let's verify this information on SW3:

### On SW3:

```
SW3#Show spanning-tree Vlan 68
```

```
VLAN0068
```

```
Spanning tree enabled protocol ieee
```

```
Root ID      Priority      24644  
Address      000c.858b.7a00
```

```
This bridge is the root
```

```
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID    Priority      24644 (priority 24576 sys-id-ext 68)  
Address      000c.858b.7a00
```

```
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec  
Aging Time  300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
<b>Fa0/8</b>	<b>Desg</b>	<b>FWD</b>	<b>19</b>	<b>128.8</b>	<b>P2p</b>
Fa0/19	Desg	FWD	19	128.19	P2p
Fa0/20	Desg	FWD	19	128.20	P2p
Fa0/21	Desg	FWD	19	128.21	P2p
Fa0/23	Desg	FWD	19	128.23	P2p

**Why is SW1 going through SW2 to get to SW3, when the link (The F0/21) between SW1 and SW3 are trunking and in "FWD" state? This can mean that we have a spanning-tree loop. Let's check the F0/21 interfaces of SW1 and SW3:**

### **On SW1:**

```
SW1#Show run int f0/21 | B interface
```

```
interface FastEthernet0/21  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
end
```

### **On SW3:**

```
SW3#Show run int f0/21 | B interface
```

```
interface FastEthernet0/21  
  switchport trunk encapsulation dot1q  
  switchport mode trunk  
spanning-tree bpdupfilter enable  
end
```

We can see the problem, BPDUFilter is configured on the F0/21 interface of SW3, this does mean that we have a spanning-tree loop. Let's check the CPU utilization on SW3:

```
SW3#Show processes cpu | Inc five
```

```
CPU utilization for five seconds: 99%/93%; one minute: 99%; five minutes:92%
```

let's remove this and verify this configuration; once the BPDUFilter is removed, SW1 should use its F0/21 interface as its root port and either SW1 or SW2 will transition their F0/19 interface into "BLK" state for this VLAN:

### On SW3:

```
SW3(config)#Int f0/21
```

```
SW3(config-if)#spanning-tree bpdufilter disable
```

### On SW1:

```
SW1#Show spanning-tree vlan 68 | B Interface
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/6	Desg	FWD	19	128.8	P2p
Fa0/19	Desg	FWD	19	128.21	P2p
<b>Fa0/21</b>	<b>Root</b>	<b>FWD</b>	<b>19</b>	<b>128.23</b>	<b>P2p</b>

Let's check SW2, it has probably transitioned its F0/19 interface to blocking:

### On SW2:

```
SW2#Show spanning-tree vlan 68 | B Interface
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
<b>Fa0/19</b>	<b>Altn</b>	<b>BLK</b>	<b>19</b>	<b>128.21</b>	<b>P2p</b>
Fa0/23	Root	FWD	19	128.25	P2p

Let's check R6 and see if has established an Eigrp neighbor adjacency:

### On R6:

```
R6#Show ip eigrp neighbors
```

```
IP-EIGRP neighbors for process 1
```



```

H   Address                Interface      Hold Uptime    SRTT   RTO   Q   Seq
   68.1.1.8                Fa0/0         12 00:04:49    3      200  0   15

```

R6#**Ping 68.1.1.8**

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 68.1.1.8, timeout is 2 seconds:

**!!!!**

**Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms**

### On SW3:

SW3#**Show processes cpu | Inc five**

CPU utilization for **five seconds: 0%/0%; one minute: 0%; five minutes: 8%**

## Ticket 2

### SHUT and NO Shut the F0/1 interface on R4 before proceeding.

In VLAN 45, R5 is configured as a DHCP server, and R4 as a DHCP client. R4 can not acquire an IP address from this DHCP server. Fix this problem without removing any commands.

**Let's verify the problem:**

### On R4:

R4#**Show ip int brief**

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
Serial0/0	unassigned	YES	unset	administratively down	down
<b>FastEthernet0/1</b>	<b>unassigned</b>	<b>YES</b>	<b>DHCP</b>	<b>up</b>	up
Serial0/1	unassigned	YES	unset	administratively down	down

**Let's verify the configuration on the F0/1 interface:**

R4#**Show run int f0/1 | B interface**

```
interface FastEthernet0/1
 ip address dhcp
 duplex auto
 speed auto
 end
```

The F0/1 interface of R4 is configured correctly, let's verify the configuration of the DHCP server (R5):

### On R5:

```
R5#Show run | S dhcp pool
```

```
ip dhcp pool tst
 network 45.1.1.0 255.255.255.0
```

```
R5#Show run | Inc dhcp
```

```
ip dhcp excluded-address 45.1.1.5
 ip dhcp pool tst
```

```
R5#Show ip int br | Exc unass
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	45.1.1.5	YES	manual	up	up

It seems like the configuration was performed correctly. Let's verify the VLAN configuration on SW2:

### On SW2:

```
SW2#Show vlan br | Exc unass
```

VLAN Name	Status	Ports
1 default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/14, Fa0/15, Fa0/16 Fa0/18, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gi0/1, Gi0/2
12 VLAN0012	active	Fa0/1, Fa0/2
36 VLAN0036	active	Fa0/3, Fa0/6
<b>45 VLAN0045</b>	<b>active</b>	<b>Fa0/4, Fa0/5</b>
68 VLAN0068	active	
212 VLAN0212	active	Fa0/12
213 VLAN0213	active	Fa0/13
214 VLAN0214	active	
215 VLAN0215	active	
216 VLAN0216	active	

```
217 VLAN0217 active Fa0/17
```

The VLAN is configured properly, the routers are configured properly, could there be a Vlan access-map or an access-list blocking this traffic?

Let's verify:

```
SW2#Show vlan access-map
SW2#
```

```
SW2#Show access-list
SW2#
```

Let's check for any configuration that has 45 in it:

```
SW2#Show run | Inc 45
```

```
ip dhcp snooping vlan 45
switchport access vlan 45
switchport access vlan 45
```

WOW...DHCP Snooping is enabled for VLAN 45, let's verify DHCP Snooping configuration:

```
SW2#Show ip dhcp snooping
```

```
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
45
```

```
Insertion of option 82 is enabled
circuit-id format: vlan-mod-port
remote-id format: MAC
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
```

Interface	Trusted	Rate limit (pps)
-----	-----	-----

The output of the above command reveals that DHCP snooping is enabled globally, and it's applied to VLAN 45, and option 82 is also enabled. If option 82 is enabled, the host's DHCP Discover message will include the "circuit-id" which is the MAC address of SW2, and the "port-id" which is the port to which the router is connected to, since these added information is NOT understood by the DHCP server, it ignores the discover messages received by R4. Let's disable option 82:

```
SW2(config)#No ip dhcp snooping information option
```

Let's verify this configuration on R4:

### On R4:

```
R4#Show ip int br
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	up	up
Serial0/0	unassigned	YES	unset	administratively down	down
<b>FastEthernet0/1</b>	<b>unassigned</b>	<b>YES</b>	<b>DHCP</b>	<b>up</b>	<b>up</b>
Serial0/1	unassigned	YES	unset	administratively down	down

Let's enable "Debug ip packet det" on R4:

```
R4#Debug ip packet detail
```

```
IP packet debugging is on (detailed)
```

```
IP: s=0.0.0.0 (local), d=255.255.255.255 (FastEthernet0/1), len 604,  
sending broad/multicast  
UDP src=68, dst=67
```

```
IP: s=0.0.0.0 (local), d=255.255.255.255 (FastEthernet0/1), len 604,  
sending broad/multicast  
UDP src=68, dst=67
```

```
IP: s=0.0.0.0 (local), d=255.255.255.255 (FastEthernet0/1), len 604,  
sending broad/multicast  
UDP src=68, dst=67
```

We can see that the local router is sending the DHCP discover messages but it's NOT receiving any offers.

Let's go through what we have verified so far:

R4 is configured as a DHCP client

R5 is configured as a DHCP Server

SW2 has these two routers in VLAN 45

SW2 is configured with "IP DHCP Snooping" and "IP dhcp snooping vlan 45".

Option 82 is also disabled

Since the dhcp snooping option is enabled and applied to VLAN 45, all ports in VLAN 45 will transition into untrusted state. When a port is in untrusted state, the switch will discard the DHCP messages like Offer, ACK, NACK coming from all ports, this includes the port that R5 is connected to. This is designed that way to mitigate rogue DHCP servers. Let's see if this port is trusted:

## On SW2:

```
SW2#Show run int f0/5 | B interface
```

```
interface FastEthernet0/5
  switchport access vlan 45
  switchport mode access
  spanning-tree portfast
end
```

**OK.....we can see the problem. Let's trust this port:**

```
SW2 (config)#int f0/5
SW2 (config-if)#ip dhcp snooping trust
```

## To verify the configuration:

## On R4:

```
R4 (config)#int f0/1
R4 (config-if)#Shut
R4 (config-if)#No shut
```

**You should see the following debug output:**

```
IP: s=0.0.0.0 (local), d=255.255.255.255 (FastEthernet0/1), len 604,
sending broad/multicast
  UDP src=68, dst=67
```

```
IP: s=45.1.1.5 (FastEthernet0/1), d=255.255.255.255, len 328, rcvd 2
  UDP src=67, dst=68
```

```
IP: s=0.0.0.0 (local), d=255.255.255.255 (FastEthernet0/1), len 604,
sending broad/multicast
  UDP src=68, dst=67
```

```
IP: s=45.1.1.5 (FastEthernet0/1), d=255.255.255.255, len 328, rcvd 2
  UDP src=67, dst=68
```

```
%DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/1 assigned DHCP address
45.1.1.1, mask 255.255.255.0, hostname R4
```

**You may get a different IP address from the same range.**

```
R4#Show ip int br | Exc unass
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/1	45.1.1.1	YES	DHCP	up	up

**Let's disable the debug:**

```
R4#Undebug all
```

All possible debugging has been turned off

### Ticket 3

VLAN 123 is configured with static IP Source Guard but it is not working. Use Ping to test.

**By looking at the diagram, we can see that the F0/0 interfaces of R1, R2 and R3 are configured in VLAN 123. Let's verify:**

#### On SW1:

```
SW1#Show vlan brief | Exc unass
```

VLAN Name	Status	Ports
1 default	active	Fa0/4, Fa0/5, Fa0/9, Fa0/10 Fa0/11, Fa0/18, Fa0/20, Fa0/22 Fa0/23, Fa0/24, Gi0/1, Gi0/2
12 VLAN0012	active	
36 VLAN0036	active	
45 VLAN0045	active	
68 VLAN0068	active	Fa0/6
114 VLAN0114	active	
121 VLAN0121	active	
<b>123 VLAN0123</b>	<b>active</b>	<b>Fa0/1, Fa0/2, Fa0/3</b>
212 VLAN0212	active	Fa0/12
213 VLAN0213	active	Fa0/13
214 VLAN0214	active	Fa0/14
215 VLAN0215	active	Fa0/15
216 VLAN0216	active	Fa0/16
217 VLAN0217	active	Fa0/17
232 VLAN0232	active	

**Let's verify the IP Source Guard configuration on SW1:**

**On SW1:**

```
SW1#Show run int f0/1 | B interface
```

```
interface FastEthernet0/1
  switchport access vlan 123
  switchport mode access
  spanning-tree portfast
  ip verify source
end
```

```
SW1#Show run int f0/2 | B interface
```

```
interface FastEthernet0/2
  switchport access vlan 123
  switchport mode access
  spanning-tree portfast
  ip verify source
end
```

```
SW1#Show run int f0/3 | B interface
```

```
interface FastEthernet0/3
  switchport access vlan 123
  switchport mode access
  spanning-tree portfast
  ip verify source
end
```

**Let's verify the source binding table, we should see three bindings, one for R1, one for R2, and another for R3 :**

**On SW1:**

```
SW1#Show ip source binding | Inc 123.1.1
```

00:00:22:22:22:22	123.1.1.2	infinite	static	123	FastEthernet0/2
00:00:11:11:11:11	123.1.1.1	infinite	static	123	FastEthernet0/1
00:00:33:33:33:33	123.1.1.3	infinite	static	123	FastEthernet0/3

**The table looked correct, let's check the configuration of the F0/0 interfaces of R1, R2 and R3:**

### On R1:

```
R1#Show int f0/0 | Inc bia|address
```

```
Hardware is Gt96k FE, address is 0000.1111.1111 (bia 0016.c898.c6e0)
Internet address is 123.1.1.1/24
```

### On R2:

```
R2#Show int f0/0 | Inc bia|address
```

```
Hardware is Gt96k FE, address is 0000.2222.2222 (bia 0011.9279.1f70)
Internet address is 123.1.1.2/24
```

### On R3:

```
R3#Show int f0/0 | Inc bia|address
```

```
Hardware is Gt96k FE, address is 0000.3333.3333 (bia 0012.d927.d710)
Internet address is 123.1.1.3/24
```

**This is configured correctly. Let's verify DHCP Snooping configuration:**

### On SW1:

```
SW1#Show ip dhcp snooping
```

```
Switch DHCP snooping is disabled
```

```
DHCP snooping is configured on following VLANs:
```

```
123
```

```
Insertion of option 82 is enabled
  circuit-id format: vlan-mod-port
  remote-id format: MAC
```

```
Option 82 on untrusted port is not allowed
```

```
Verification of hwaddr field is enabled
```

Interface	Trusted	Rate limit (pps)
-----	-----	-----

**The output of the above show command reveals that the DHCP Snooping feature is NOT enabled, let's verify this by looking at the running configuration:**

### On SW1:

```
SW1#Show run | Inc ip dhcp snooping
```



```
ip dhcp snooping vlan 123
```

Yes, we can see that it is applied to VLAN 123, but it is NOT enabled globally, let's enable DHCP Snooping globally:

### On SW1:

```
SW1(config)#IP Dhcp snooping
```

### To verify the configuration:

### On SW1

```
SW1#Show ip dhcp snooping
```

```
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
123
```

```
Insertion of option 82 is enabled
  circuit-id format: vlan-mod-port
  remote-id format: MAC
Option 82 on untrusted port is not allowed
```

```
Verification of hwaddr field is enabled
Interface           Trusted           Rate limit (pps)
-----
```

Perfect....let's test the configuration by changing the IP address of R1 to 123.1.1.10 or any IP address that is not configured in the source binding table and test the configuration:

### On R1:

```
R1(config)#int f0/0
R1(config-if)#ip addr 123.1.1.10 255.255.255.0
```

```
R1#Ping 123.1.1.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 123.1.1.2, timeout is 2 seconds:
```

```
.....
Success rate is 0 percent (0/5)
```

Let's change the IP address of R1 back to 123.1.1.1/24 and test again:

## On R1

```
R1(config)#int f0/0
R1(config-if)#ip addr 123.1.1.1 255.255.255.0
```

```
R1#Ping 123.1.1.2
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 123.1.1.2, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

## On SW1:

```
SW1#Sh ip source binding static
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:00:22:22:22:22	123.1.1.2	infinite	static	123	FastEthernet0/2
00:00:11:11:11:11	123.1.1.1	infinite	static	123	FastEthernet0/1
00:00:33:33:33:33	123.1.1.3	infinite	static	123	FastEthernet0/3

```
Total number of bindings: 3
```

## Ticket 4

The F0/19 interface of SW4 is configured as a trunk link. The user has setup port security on this interface and set the maximum number of MAC addresses to 2, but for some reason this is NOT working.

**Let's verify the configuration on SW4:**

## On SW4:

```
SW4#Show run int f0/19 | B interface
```

```
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport port-security maximum 2
```

```
switchport port-security aging time 5
switchport port-security aging type inactivity
```

We can see that the maximum number of MAC addresses allowed is 2, and the aging type and aging time are also set. But the port security is NOT enabled. Let's verify this information:

```
SW4#Show port-security interface F0/19
```

```
Port Security : Disabled
Port Status : Secure-down
Violation Mode : Shutdown
Aging Time : 5 mins
Aging Type : Inactivity
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
```

Let's enable port-security:

```
SW4(config)#int f0/19
SW4(config-if)#Switchport port-security
```

Once the port-security is enabled, you should see the following console messages:

```
%PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/19, putting
Fa0/19 in err-disable state
```

```
%PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused
by MAC address 000a.f402.6d93 on port FastEthernet0/19.
```

We can clearly see that port security is working, once the feature was enabled, the interface transitioned into err-disable state. To verify this information:

```
SW4#Show interface f0/19 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/19		err-disabled	1	auto	auto	10/100BaseTX

## Ticket 5

In VLAN 12, R1 can NOT ping R2's F0/1 interface. You can break one of the rules.

**Let's verify the problem:**

### On R1:

```
R1#Ping 12.1.1.2
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
```

```
.....
```

```
Success rate is 0 percent (0/5)
```

```
R1#Show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	12.1.1.1	-	0000.2121.2121	ARPA	FastEthernet0/1
<b>Internet</b>	<b>12.1.1.2</b>	<b>0</b>	<b>Incomplete</b>	<b>ARPA</b>	
Internet	123.1.1.1	-	0000.1111.1111	ARPA	FastEthernet0/0
Internet	123.1.1.2	11	0000.2222.2222	ARPA	FastEthernet0/0

**We can see that ARP was "incomplete", this can mean that we have a layer 2 problem, before checking layer 2, let's see the configuration of the F0/1 interfaces of R1 and R2:**

### On R1:

```
R1#Show run int f0/1 | B interface
```

```
interface FastEthernet0/1
  mac-address 0000.2121.2121
  ip address 12.1.1.1 255.255.255.0
  duplex auto
  speed auto
end
```

### On R2:

```
R2#Show run int f0/1 | B interface
```

```
interface FastEthernet0/1
  mac-address 0000.1212.1212
  ip address 12.1.1.2 255.255.255.0
```

```

duplex auto
speed auto
end

```

**Well.....the interfaces are configured correctly, let's verify the switch configuration:**

**On SW2:**

```
SW2#Show vlan br | Exc unsp
```

VLAN Name	Status	Ports
1 default	active	Fa0/7, Fa0/8, Fa0/9, Fa0/10 Fa0/11, Fa0/14, Fa0/15, Fa0/16 Fa0/18, Fa0/20, Fa0/21, Fa0/22 Fa0/24, Gi0/1, Gi0/2
<b>12 VLAN0012</b>	<b>active</b>	<b>Fa0/1, Fa0/2</b>
36 VLAN0036	active	Fa0/3, Fa0/6
45 VLAN0045	active	Fa0/4, Fa0/5
68 VLAN0068	active	
114 VLAN0114	active	
121 VLAN0121	active	
123 VLAN0123	active	
212 VLAN0212	active	Fa0/12
213 VLAN0213	active	Fa0/13
214 VLAN0214	active	
215 VLAN0215	active	
216 VLAN0216	active	
217 VLAN0217	active	Fa0/17
232 VLAN0232	active	

**Let's check the VLAN:**

```
SW2#Show vlan id 12
```

VLAN Name	Status	Ports
<b>12 VLAN0012</b>	<b>active</b>	<b>Fa0/1, Fa0/2, Fa0/19, Fa0/23</b>

VLAN Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
<b>12 enet</b>	100012	1500	-	-	-	-	-	0	0

Remote SPAN VLAN  
-----  
Disabled

```
Primary Secondary Type                Ports
-----
```

**This is also correct, let's verify the interface configuration, maybe an access-list is configured to block the communication between the two routers:**

```
SW2#Show run int f0/1 | B interface
```

```
interface FastEthernet0/1
  switchport access vlan 12
  switchport mode access
  spanning-tree portfast
```

```
SW2#Show run int f0/2 | B interface
```

```
interface FastEthernet0/2
  switchport access vlan 12
  switchport mode access
  spanning-tree portfast
```

**Let's verify the MAC address of these two routers on the switch:**

```
SW2#Show mac address-table dynamic interface f0/1 vlan 12
```

```
Mac Address Table
```

```
-----
Vlan    Mac Address      Type      Ports
-----
 12     0000.2121.2121  DYNAMIC   Fa0/1
```

```
Total Mac Addresses for this criterion: 1
```

```
SW2#Show mac address-table dynamic interface f0/2 vlan 12
```

```
Mac Address Table
```

```
-----
Vlan    Mac Address      Type      Ports
-----
```

**The switch does not see R2, this could be that R2 did not see the ping generated by R1, let's ping from R2 and verify the result:**

**On R2:**

```
R2#Ping 12.1.1.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 12.1.1.1, timeout is 2 seconds:
```

```
.....  
Success rate is 0 percent (0/5)
```

### On SW2:

```
SW2#Show mac address-table dynamic interface f0/2 vlan 12
```

```
Mac Address Table
```

```
-----  
Vlan      Mac Address      Type      Ports  
----      -
```

**WOW...may be something is filtering/blocking the MAC address of R2, let's verify:**

```
SW2#Show run | Inc 0000.1212.1212
```

```
mac-address-table static 0000.1212.1212 vlan 12 drop
```

**We can clearly see the problem, this is called Unicast MAC address filtering. When this feature is enabled, the switch drops packets with the configured MAC address as source or destination.**

**The switch is configured to drop any traffic sourcing or destined to "0000.1212.1212" MAC address in VLAN 12. Let's remove this filter and try again:**

```
SW2 (config)#No mac address-table static 0000.1212.1212 vlan 12 drop
```

### To verify the configuration:

### On R1:

```
R1#Ping 12.1.1.2
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 12.1.1.2, timeout is 2 seconds:
```

```
.!!!!  
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

### On SW2:

```
SW2#Show mac address-table dynamic interface f0/2 vlan 12
```

```
Mac Address Table
```

```
-----  
Vlan      Mac Address      Type      Ports  
-----  
12       0000.1212.1212  DYNAMIC  Fa0/2
```

```
Total Mac Addresses for this criterion: 1
```

## Ticket 6

In VLAN 36, R6 can not ping R3. You are allowed to break one of the rules.

**Let's verify the problem:**

### On R3:

```
R3#Ping 36.1.1.6
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 36.1.1.6, timeout is 2 seconds:
```

```
.....  
Success rate is 0 percent (0/5)
```

```
R3#Show arp
```

```
Protocol  Address      Age (min)  Hardware Addr  Type   Interface  
Internet  36.1.1.3     -          0000.3636.3636 ARPA   FastEthernet0/1  
Internet  36.1.1.6     0          Incomplete     ARPA   FastEthernet0/0  
Internet  123.1.1.3    -          0000.3333.3333 ARPA   FastEthernet0/0
```

**It looks like the problem is with SW2, let's verify SW2's configuration:**

### On SW2:

```
SW2#Show vlan br | exc unshp
```

```
VLAN Name      Status      Ports  
-----  
-----
```



```

1    default                                active    Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                           Fa0/11, Fa0/14, Fa0/15, Fa0/16
                                           Fa0/18, Fa0/20, Fa0/21, Fa0/22
                                           Fa0/24, Gi0/1, Gi0/2
12   VLAN0012                              active    Fa0/1, Fa0/2
36  VLAN0036                              active    Fa0/3, Fa0/6
45   VLAN0045                              active    Fa0/4, Fa0/5
68   VLAN0068                              active
114  VLAN0114                              active
121  VLAN0121                              active
123  VLAN0123                              active
212  VLAN0212                              active    Fa0/12
213  VLAN0213                              active    Fa0/13
214  VLAN0214                              active
215  VLAN0215                              active
216  VLAN0216                              active
217  VLAN0217                              active    Fa0/17
232  VLAN0232                              active

```

SW2#**Show mac address-table dynamic interface F0/3 vlan 36**

Mac Address Table

```

-----
Vlan    Mac Address      Type      Ports
----    -
36     0000.3636.3636  DYNAMIC   Fa0/3

```

Total Mac Addresses for this criterion: 1

SW2#**Show mac address-table dynamic interface F0/6 vlan 36**

Mac Address Table

```

-----
Vlan    Mac Address      Type      Ports
----    -

```

**The switch does not see the MAC address of R6, let's check the configuration of the F0/3, and F0/6 interfaces on the switch, and then check for a unicast Mac address filtering:**

SW2#**Show run int f0/3 | B inter**

```

interface FastEthernet0/3
 switchport access vlan 36
 switchport mode access
 spanning-tree portfast

```

```
SW2#Show run int f0/6 | B inter
```

```
interface FastEthernet0/6
 switchport access vlan 36
 switchport mode access
 spanning-tree portfast
```

**Let's find out the MAC address of R6:**

### **On R6:**

```
R6#Show int f0/1 | inc bia
```

```
Hardware is MV96340 Ethernet, address is 0000.6363.6363 (bia 0017.5aad.52ab)
```

```
SW2#Show run | Inc 0000.6363.6363
```

```
SW2#
```

**What else could be the problem? May be some type of filtering is configured based on the interface? Let's verify:**

### **On SW2**

```
SW2#Show run | Inc Fa0/6
```

```
monitor session 1 destination interface Fa0/6
```

**It looks like SPAN was configured on SW2 and the destination port or the monitor port was configured to be F0/6 interface. When a port is configured as monitor port, the port does not transmit any traffic except that required for the SPAN session and incoming traffic is never learned or forwarded on a destination port.**

**The second way to find out the problem:**

```
SW2#Show interface f0/3 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/3		connected	36	a-full	a-100	10/100BaseTX

```
SW2#Show interface f0/6 status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/6		monitoring	36	a-full	a-100	10/100BaseTX

**Let's remove the command and verify the communication:**

```
SW2 (config) #No monitor session 1 destination interface Fa0/6
```

### On R3

```
R3#Ping 36.1.1.6
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 36.1.1.6, timeout is 2 seconds:

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/4 ms
```

## Ticket 7

In VLAN 78, R7 can NOT ping R8's F0/0 interface.

**Let's verify the problem:**

### On R7:

```
R7#Ping 78.1.1.8
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 78.1.1.8, timeout is 2 seconds:

```
.....
```

```
Success rate is 0 percent (0/5)
```

```
R7#Show arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	78.1.1.7	-	0000.7777.7777	ARPA	GigabitEthernet0/0
<b>Internet</b>	<b>78.1.1.8</b>	<b>0</b>	<b>Incomplete</b>	<b>ARPA</b>	

**We should not waste time, we should go right to the SW1 and check its configuration:**

### On SW1:

**WOW.....you should see the following console messages on SW1:**

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/7, vlan  
78. ([0000.7777.7777/78.1.1.7/0000.0000.0000/78.1.1.8/02:24:37 UTC Mon Mar
```

1 1993])

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/7, vlan
78. ([0000.7777.7777/78.1.1.7/0000.0000.0000/78.1.1.8/02:24:37 UTC Mon Mar
1 1993])
```

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/7, vlan
78. ([0000.7777.7777/78.1.1.7/0000.0000.0000/78.1.1.8/02:24:37 UTC Mon Mar
1 1993])
```

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/7, vlan
78. ([0000.7777.7777/78.1.1.7/0000.0000.0000/78.1.1.8/02:24:37 UTC Mon Mar
1 1993])
```

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/7, vlan
78. ([0000.7777.7777/78.1.1.7/0000.0000.0000/78.1.1.8/02:24:37 UTC Mon Mar
1 1993])
```

From the above console messages we can see that we have a problem with DAI (Dynamic Arp Inspection).

The above console message states the following:

The Switch (SW1) received an invalid ARP request (Req) on Fa0/7 in VLAN 78.

The ARP request was from a host with a MAC address of 0000.7777.7777 and an IP address of 78.1.1.7 for 78.1.1.8 (R8).

This means that R7 is NOT allowed to send ARP request and this is why we are getting this error message. Let's verify the configuration of DAI.

### On SW1:

```
SW1#Show run | Inc ip arp
```

```
ip arp inspection vlan 78
```

We can see that the "IP ARP inspection" command is NOT referencing an ARP access-list, and obviously "IP DHCP Snooping" is also enabled, or else Dynamic ARP Inspection would not have worked. Let's verify the entries in the DHCP Snooping DB:

```
SW1#Show ip dhcp snooping binding
```

MacAddress	IpAddress	Lease (sec)	Type	VLAN	Interface
00:00:88:88:88:88	78.1.1.8	9217	dhcp-snooping	78	FastEthernet0/8

Total number of bindings: 1

We can clearly see the problem, when the F0/7 interface of SW1 receives the ARP request from R7, it consults the DHCP snooping DB for an entry for R7, and since it does not find one, it drops the packets and sends a console message. Let's add an entry for R7 in the Snooping DB and try pinging again. Let's find out the MAC address of R8:

### On R7:

```
R7#Show int g0/0 | Inc bia
```

```
Hardware is CN Gigabit Ethernet, address is 0000.7777.7777 (bia 24e9.b3ab.4b20)
```

### On SW1:

```
SW1#IP Dhcp snooping bindin 0000.7777.7777 vlan 78 78.1.1.7 int F0/7 exp 1000
```

### To verify the configuration:

### On R7:

```
R7#Ping 78.1.1.8
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 78.1.1.8, timeout is 2 seconds:
```

```
.!!!!
```

```
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

## Ticket 8

Your client is complaining that he can not save the running configuration on SW4 by using "Wr" and everytime he tries to save using the "WR" command he gets the following console error message:

```
Error reading config file "flash:/startup-config file open failed (Not enough space)
```

```
OR
```

```
startup-config file open failed (Not enough space)
```

Let's verify the problem:

### On SW4:

```
SW4#wr
```

**startup-config file open failed (Not enough space)**

**WOW...what can cause that? Let's verify the boot parameters:**

```
SW4#Show boot
```

```
BOOT path-list:      c3550-ipservicesk9-mz.122-25.SEE4.bin
Config file:      flash:/
Private Config file: flash:/private-config.text
Enable Break:       no
Manual Boot:        no
HELPER path-list:
NVRAM/Config file
  buffer size:      393216
```

**We can see the problem, the "Config file" is instructed to be saved in the flash, but a file name has not been specified. Let's fix this problem:**

```
SW4 (config) #Boot config-file flash:/config.text
```

**You must reload the switch for this change to be implemented:**

**To verify the solution:**

**On SW4**

```
SW4#reload
```

**Let's try to save the running configuration when the switch comes up:**

```
SW4>en
SW4#wr
Building configuration...
[OK]
```

## **Ticket 9**

Erase the startup configuration and the "vlan.dat" and reload the devices before proceeding to the next scenario.