Cisco

Exam 300-135

Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Version: Demo

[Total Questions: 10]

Topic break down

Topic	No. of Questions
Topic 1: Mix Questions	2
Topic 2: Troubleshooting VTP	1
Topic 7: Ticket 2 : ACCESS VLAN	1
Topic 13: Ticket 8 : Redistribution of EIGRP to OSPF	1
Topic 20: Ticket 15: IPv6 Routing Issue 2	2
Topic 23: Mix Questions Set 2	3

Topic 1, Mix Questions

Question No : 1 - (Topic 1)

For which two reasons might a GRE Tunnel interface enter an up/down state? (Choose two)

A. The tunnel source is using a loopback interface.
B. The tunnel mode is defined as transport.
C. Keepalives are disabled on the interfaces
D. The route to the destination is through the tunnel itself.
E. The tunnel source interface is down.

Answer: D,E

Question No : 2 - (Topic 1)

Which two statements about GRE tunnel keepalives are true? (Choose two)

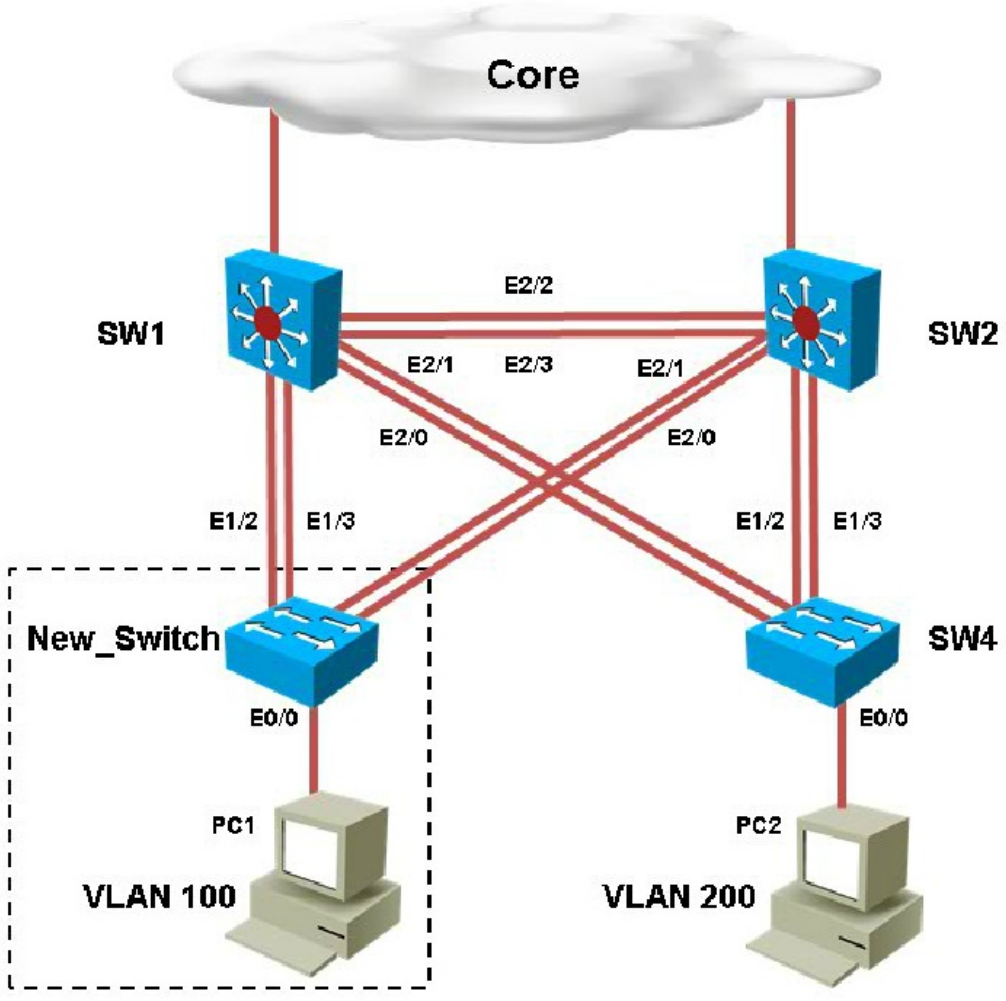
A. They are supported in point-to-point GRE tunnels.
B. They are supported in multipoint GRE tunnels.
C. They are supported in VRFs only if the fVRF and iVRF match.
D. They are supported with IPsec tunnel protection.
E. They are enabled by default.

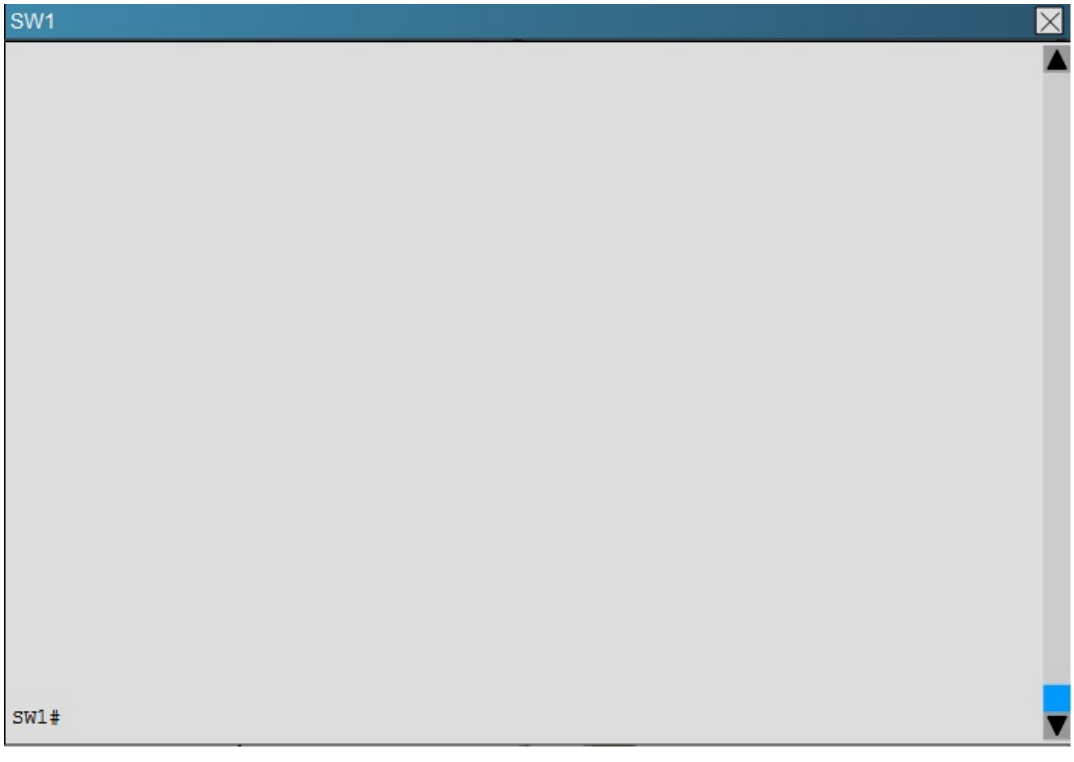
Answer: A,D

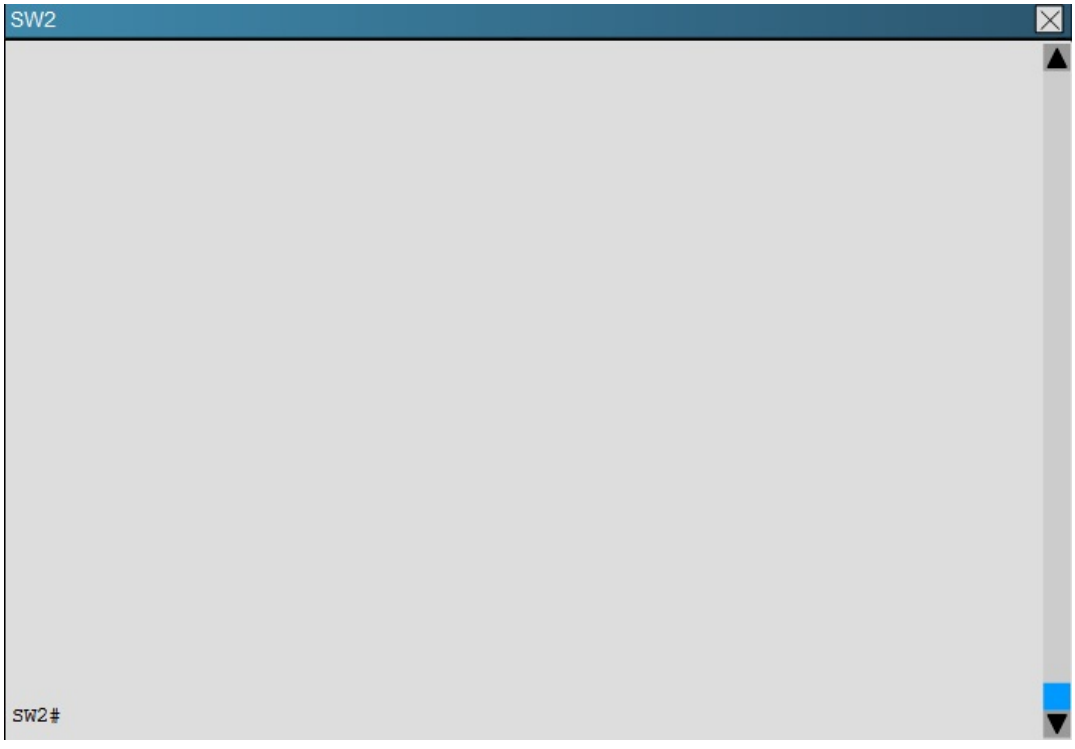
Topic 2, Troubleshooting VTP

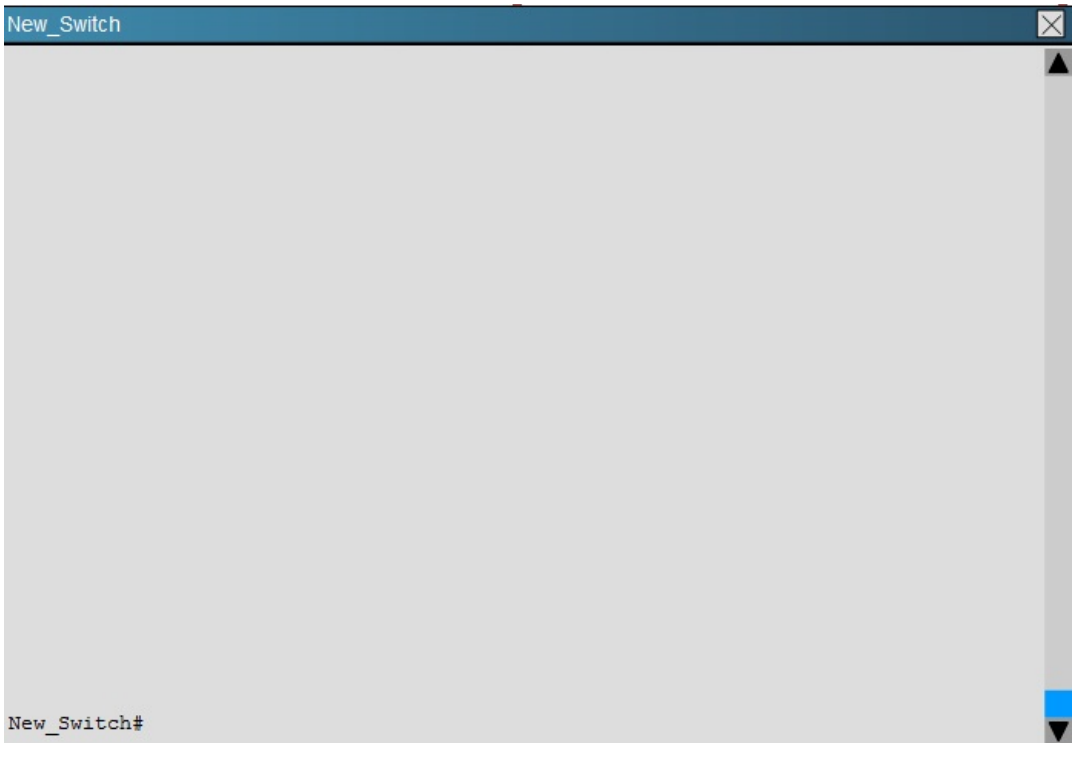
Question No : 3 - (Topic 2)

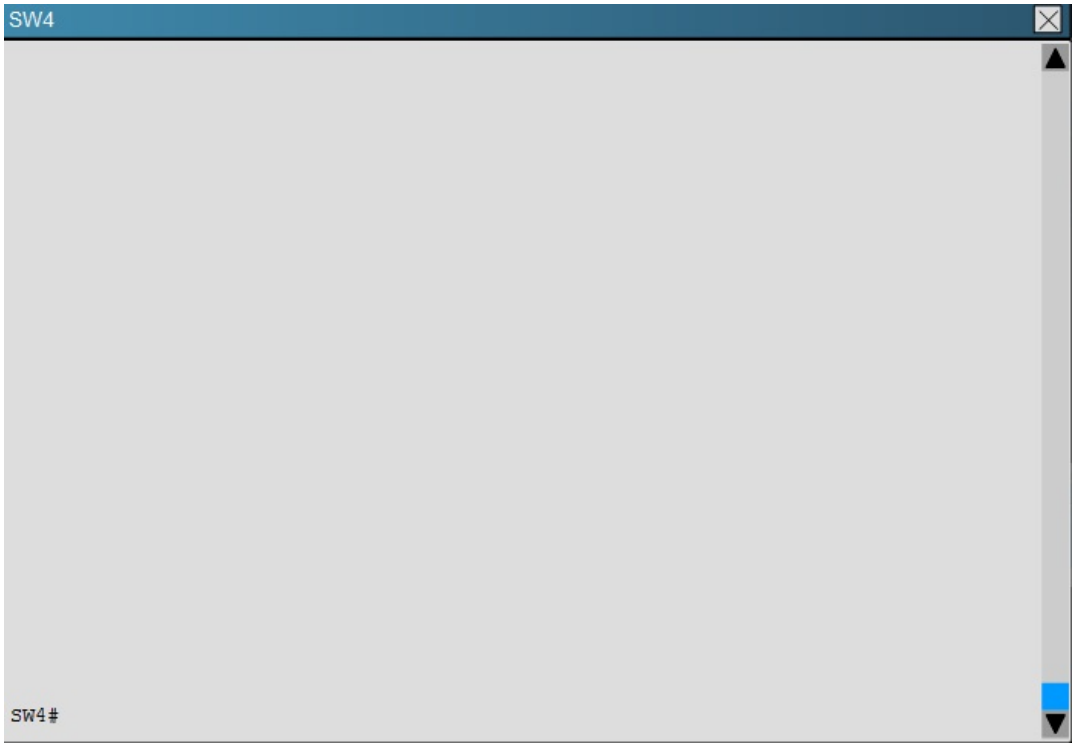
A customer network engineer has made configuration changes that have resulted in some loss of connectivity. You have been called in to evaluate a switch network and suggest resolutions to the problems.


Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200


SW1
SW1#


SW2
SW2#


New_Switch
New_Switch#



Which of statement is true regarding STP issue identified with switches in the given topology?

A. Loopguard configured on the New_Switch places the ports in loop inconsistent state
B. Rootguard configured on SW1 places the ports in root inconsistent state
C. Bpduguard configured on the New_Switch places the access ports in error-disable
D. Rootguard configured on SW2 places the ports in root inconsistent state

Answer: A

Explanation:

On the new switch, we see that loopguard has been configured with the “spanning-tree guard loop” command.

New_Switch

```
!
interface Ethernet2/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 duplex auto
 spanning-tree bpdufilter enable
 spanning-tree guard loop
!
```

The loop guard feature makes additional checks. If BPDUs are not received on a non-

designated port, and loop guard is enabled, that port is moved into the STP loop-inconsistent blocking state, instead of the listening / learning / forwarding state. Without the loop guard feature, the port assumes the designated port role. The port moves to the STP forwarding state and creates a loop.

Topic 7, Ticket 2 : ACCESS VLAN

Topology Overview (Actual Troubleshooting lab design is for below network design)

- Client Should have IP 10.2.1.3
- EIGRP 100 is running between switch DSW1 & DSW2
- OSPF (Process ID 1) is running between R1, R2, R3, R4
- Network of OSPF is redistributed in EIGRP
- BGP 65001 is configured on R1 with Webserver cloud AS 65002
- HSRP is running between DSW1 & DSW2 Switches

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.

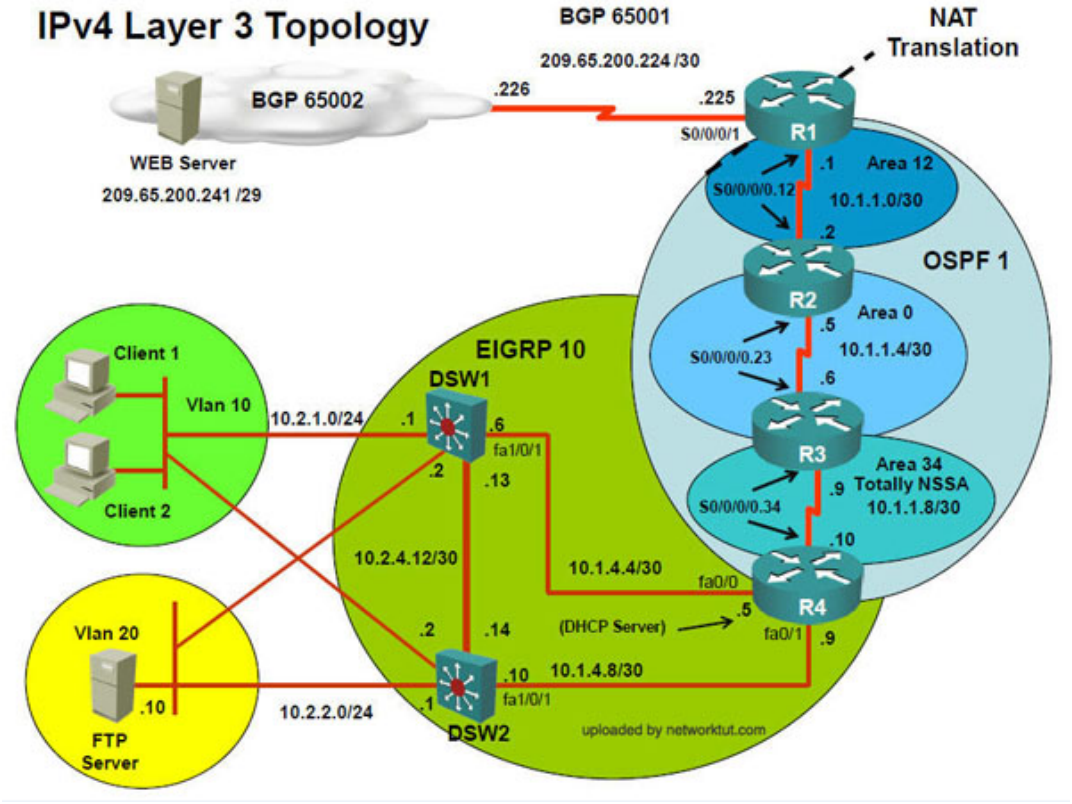
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range. R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

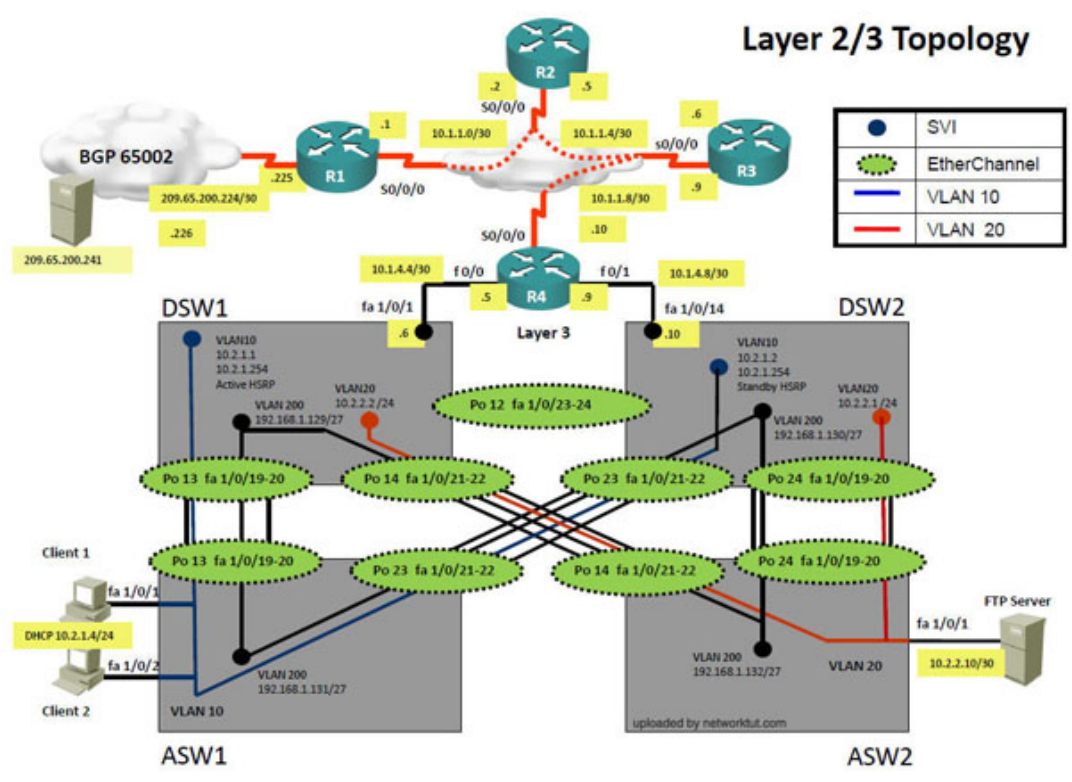
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution





Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

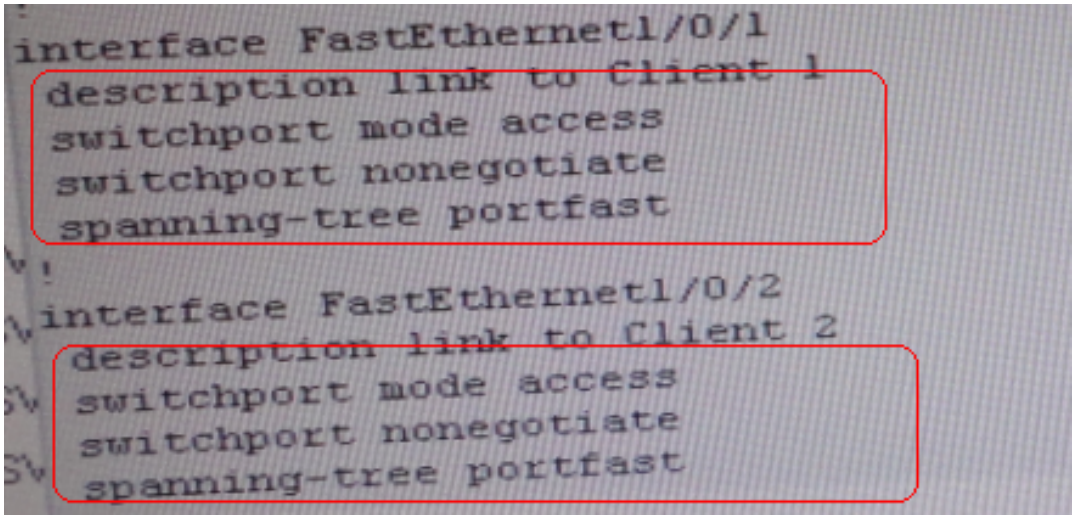
- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4

Ipconfig ----- Client will be getting 169.X.X.X

- On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24

Sh run ------- & check for running config of int fa1/0/1 & fa1/0/2

==========



==========

- Here we are not able to see access Vlan10 configured for Port Fa1/0/1 & Fa1/0/2
- Change required: On ASW1, for configuring Access Vlan under interface fa1/0/1 & 1/0/2 we have to enable command switchport access vlan 10

Question No : 4 - (Topic 7)

The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to isolated the cause of this fault and answer the following questions.

What is the solution to the fault condition?

A. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport mode access vlan 10 command.
B. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport access mode vlan 10 command.
C. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport vlan 10 access command.
D. In Configuration mode, using the interface range Fastethernet 1/0/1 – 2, then switchport access vlan 10 command.

Answer: D

Explanation:

The problem here is that VLAN 10 is not configured on the proper interfaces on switch ASW1.

Topic 13, Ticket 8 : Redistribution of EIGRP to OSPF

Topology Overview (Actual Troubleshooting lab design is for below network design)

- Client Should have IP 10.2.1.3
- EIGRP 100 is running between switch DSW1 & DSW2
- OSPF (Process ID 1) is running between R1, R2, R3, R4
- Network of OSPF is redistributed in EIGRP
- BGP 65001 is configured on R1 with Webserver cloud AS 65002
- HSRP is running between DSW1 & DSW2 Switches

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range. R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP

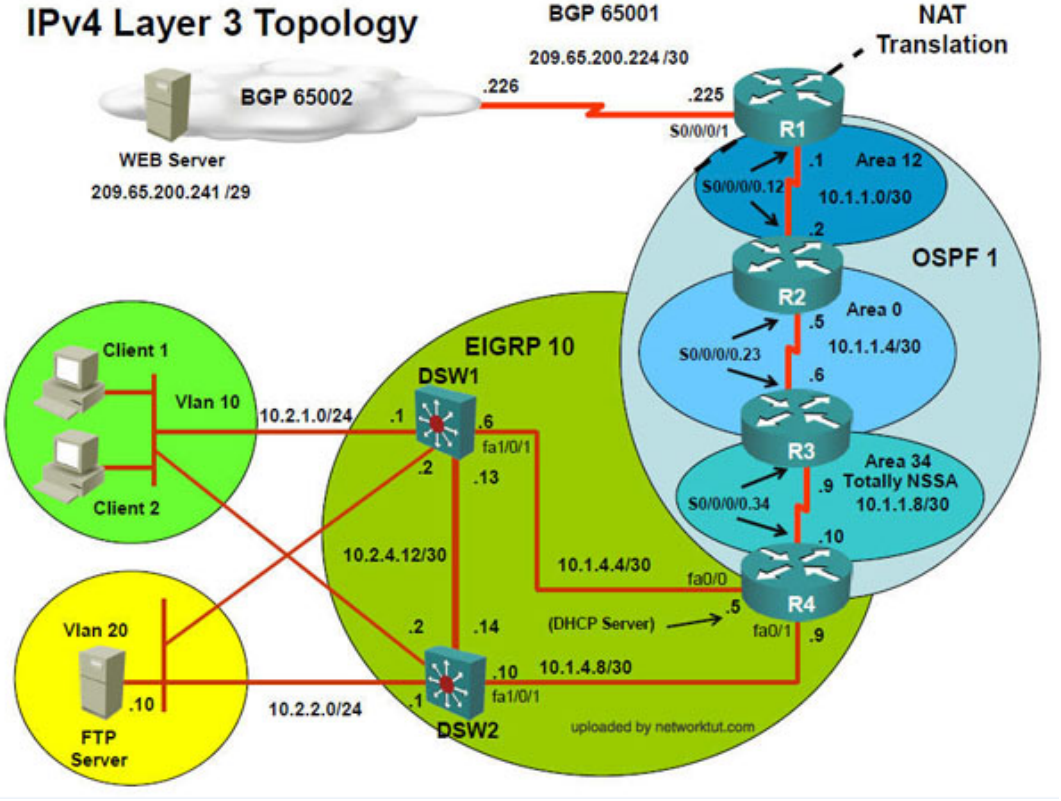
server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

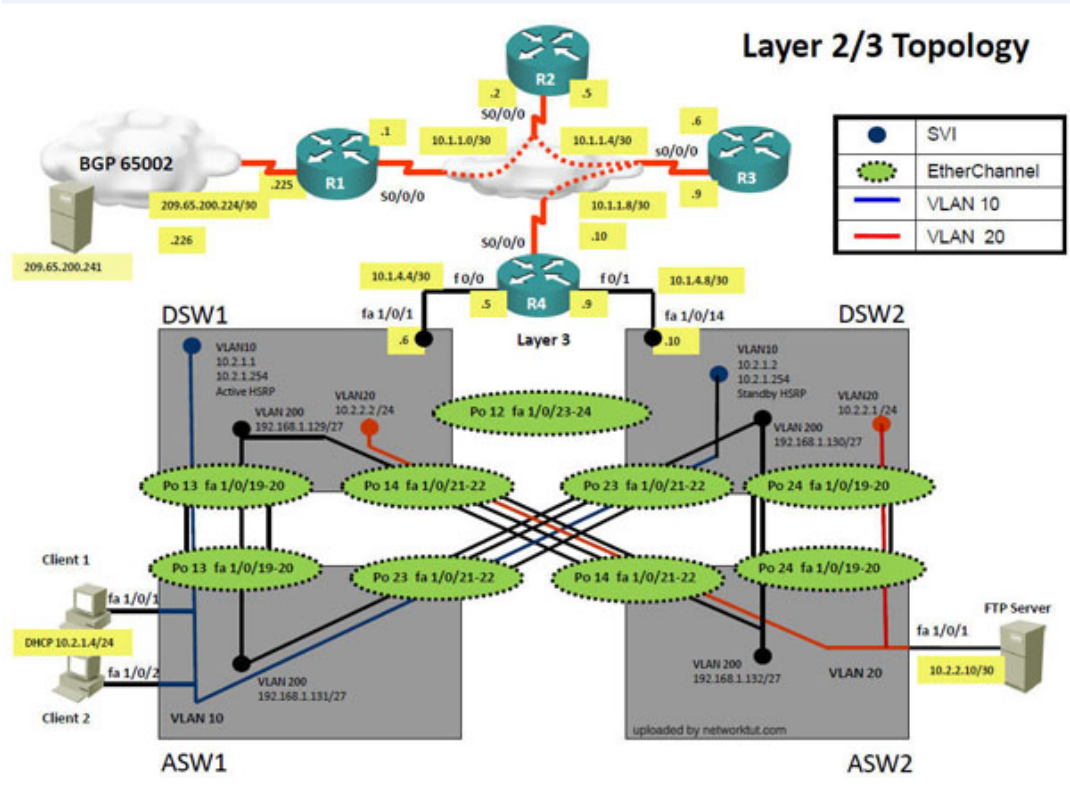
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========





Client is unable to ping IP 209.65.200.241

Solution

Steps need to follow as below:-

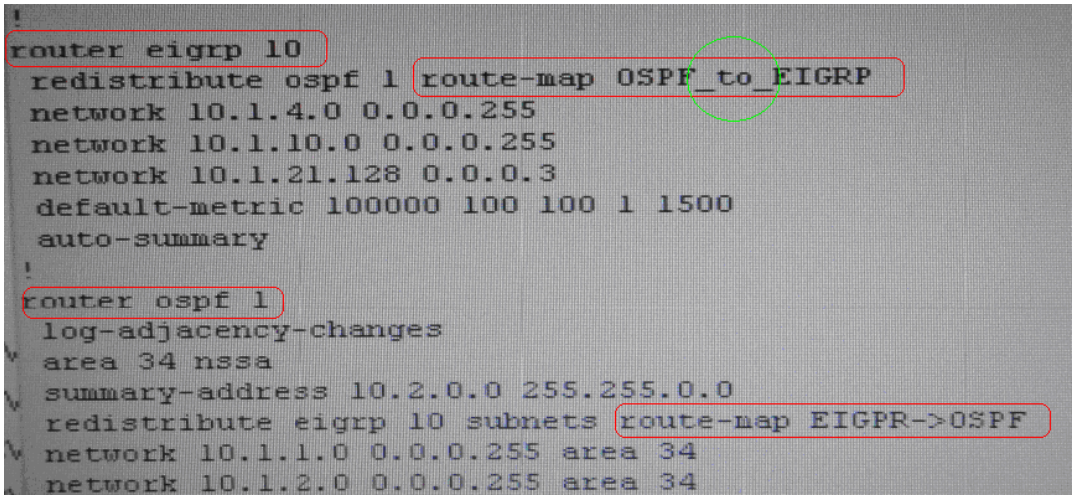
- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4

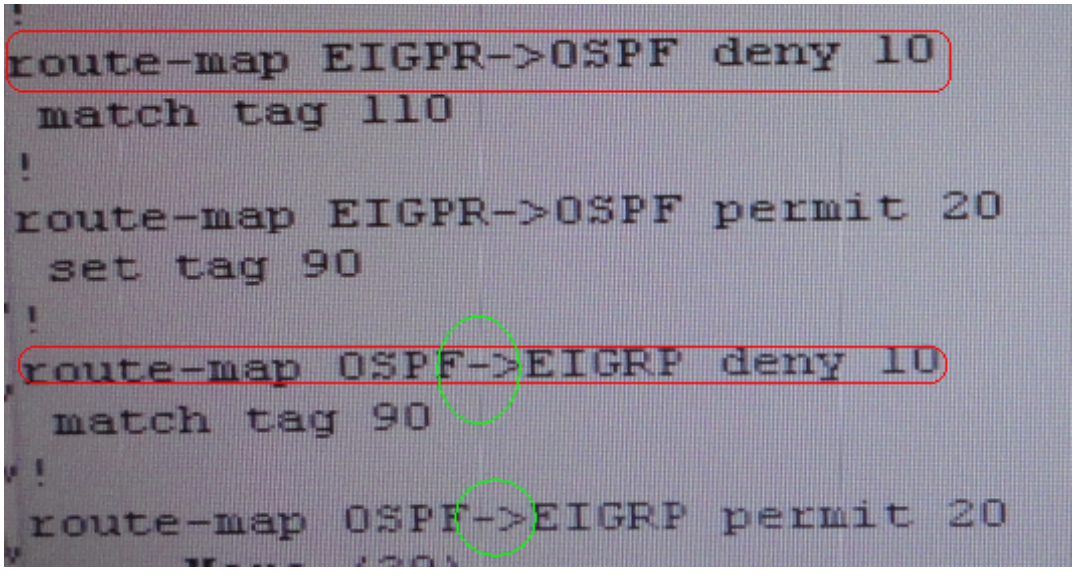
ipconfig ----- Client will be receiving IP address 10.2.1.3

- IP 10.2.1.3 will be able to ping from R4 , but cannot ping from R3, R2, R1

- This clearly shows problem at R4 since EIGRP is between DSW1, DSW2 & R4 and OSPF protocol is running between R4, R3, R2, R1 so routes from R4 are not propagated to R3, R2, R1

- Since R4 is able to ping 10.2.1.3 it means that routes are received in EIGRP & same needs to be advertised in OSPF to ping from R3, R2, R1.
- Need to check the routes are being advertised properly or not in OSPF & EIGRP vice-versa.





- From above snap shot it clearly indicates that redistribution done in EIGRP is having problem & by default all routes are denied from ospf to EIGRP… so need to change route-map name.
- Change required: On R4, in the redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue. It references route-map OSPF_to_EIGRP but the actual route map is called OSPF->EIGRP.

Question No : 5 - (Topic 13)

The implementations group has been using the test bed to do a 'proof-of-concept' that requires both Client 1 and Client 2 to access the WEB Server at 209.65.200.241. After several changes to the network addressing, routing scheme, DHCP services,

NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating that Client 1 cannot ping the 209.65.200.241 address.

Use the supported commands to isolated the cause of this fault and answer the following questions.

The fault condition is related to which technology?

A. NTP
B. IP DHCP Server
C. IPv4 OSPF Routing
D. IPv4 EIGRP Routing
E. IPv4 Route Redistribution
F. IPv6 RIP Routing
G. IPv6 OSPF Routing
H. IPv4 and IPv6 Interoperability
I. IPv4 layer 3 security

Answer: E

Explanation:
On R4, in the redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue. It references route-map OSPF_to_EIGRP but the actual route map is called OSPF->EIGRP.

Topic 20, Ticket 15: IPv6 Routing Issue 2

Topology Overview (Actual Troubleshooting lab design is for below network design)

- Client Should have IP 10.2.1.3
- EIGRP 100 is running between switch DSW1 & DSW2
- OSPF (Process ID 1) is running between R1, R2, R3, R4
- Network of OSPF is redistributed in EIGRP
- BGP 65001 is configured on R1 with Webserver cloud AS 65002
- HSRP is running between DSW1 & DSW2 Switches

The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.

In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1.
DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary.

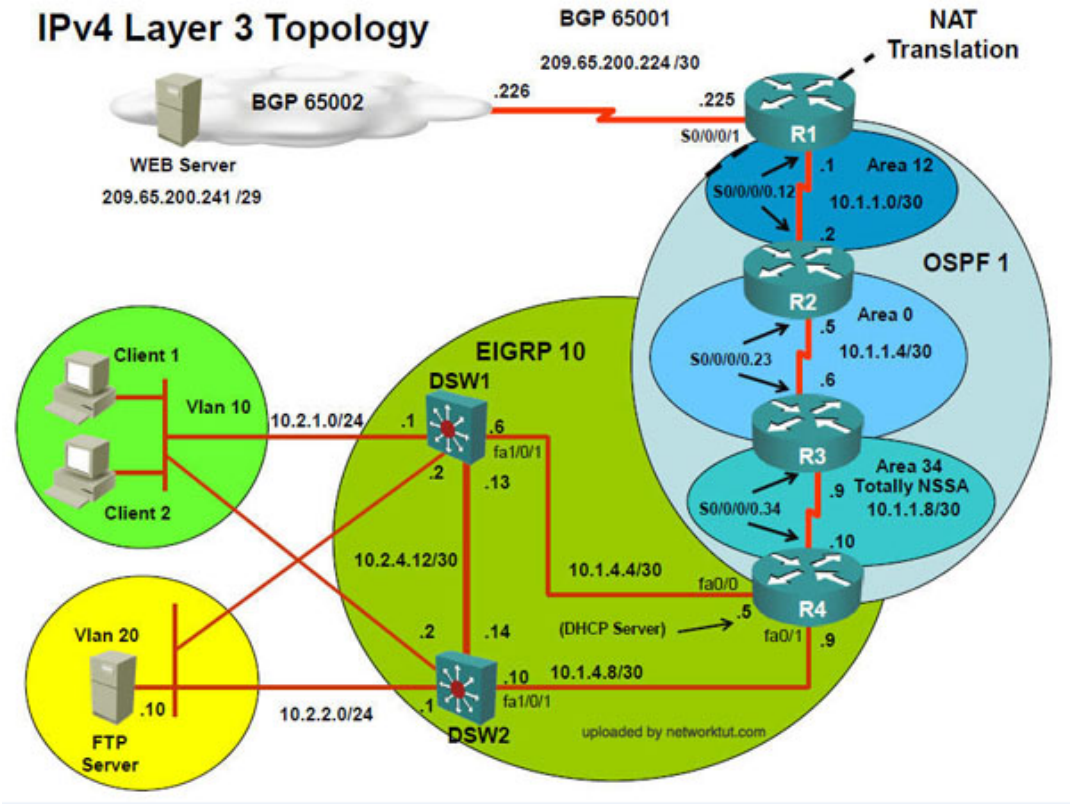
R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. Because the company's address space is in the private range. R1 is also providing NAT translations between the inside (10.1.0.0/16 & 10.2.0.0/16) networks and outside (209.65.0.0/24) network.
ASW1 and ASW2 are layer 2 switches.
NTP is enabled on all devices with 209.65.200.226 serving as the master clock source.
The client workstations receive their IP address and default gateway via R4's DHCP server.
The default gateway address of 10.2.1.254 is the IP address of HSRP group 10 which is running on DSW1 and DSW2.

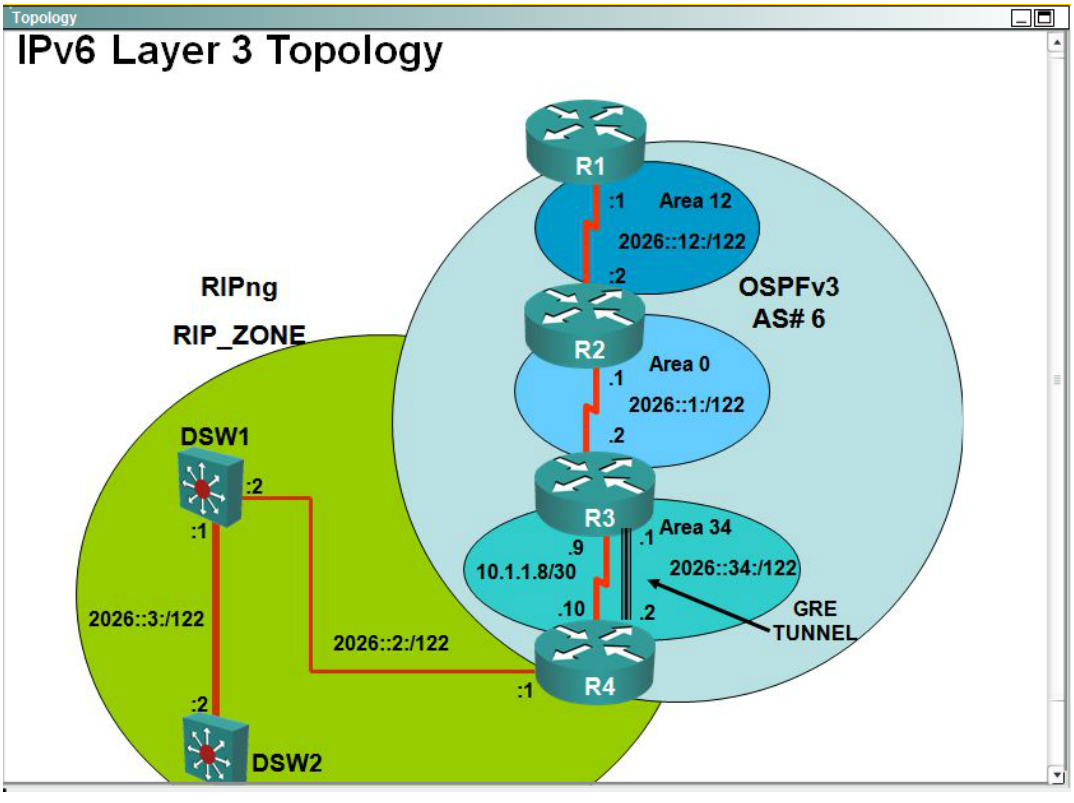
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6.
DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE.
The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where necessary.

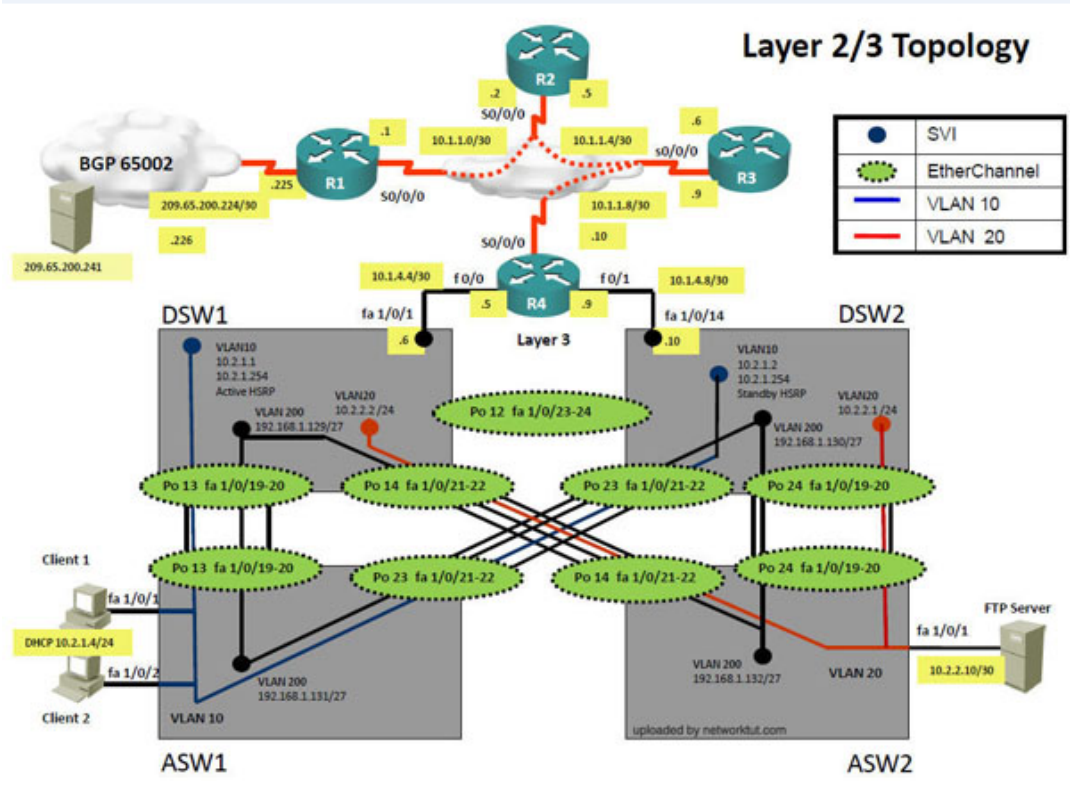
Recently the implementation group has been using the test bed to do a 'proof-of-concept' on several implementations. This involved changing the configuration on one or more of the devices. You will be presented with a series of trouble tickets related to issues introduced during these configurations.

Note: Although trouble tickets have many similar fault indications, each ticket has its own issue and solution.

Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
==========


IPv4 Layer 3 Topology
BGP 65001
NAT Translation
209.65.200.224 /30
BGP 65002
.226
.225
S0/0/0/1
R1
WEB Server
209.65.200.241 /29
.1
Area 12
S0/0/0/0.12
10.1.1.0/30
.2
OSPF 1
R2
.5
Area 0
10.1.1.4/30
S0/0/0/0.23
.6
Client 1
EIGRP 10
DSW1
Vlan 10
10.2.1.0/24
.1
.6
fa1/0/1
.2
.13
R3
Area 34
Totally NSSA
10.1.1.8/30
S0/0/0/0.34
.9
.10
Client 2
10.2.4.12/30
10.1.4.4/30
fa0/0
R4
.5
.2
.14
(DHCP Server)
fa0/1
.9
Vlan 20
.10
10.1.4.8/30
10.2.2.0/24
.1
fa1/0/1
.10
FTP Server
DSW2
uploaded by networktut.com


Topology
IPv6 Layer 3 Topology
R1
:1
Area 12
2026::12:/122
:2
RIPng
RIP_ZONE
OSPFv3
AS# 6
R2
Area 0
.1
2026::1:/122
.2
DSW1
R3
:2
:1
.9
.1
Area 34
10.1.1.8/30
2026::34:/122
2026::3:/122
.10
.2
GRE
TUNNEL
2026::2:/122
R4
:1
:2
DSW2



Questions

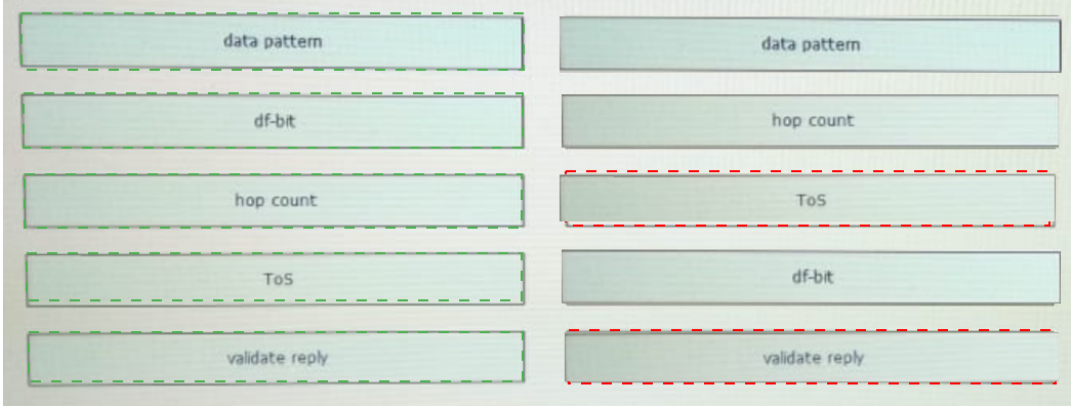
The implementation group has been using the test bed to do an IPv6 'proof-of-concept'. After several changes to the network addressing and routing schemes, a trouble ticket has been opened indicating that the loopback address on R1 (2026::111:1) is not able to ping the loopback address on DSW2 (2026::102:1).

Using the supported commands to isolate the cause of this fault and answer the following questions.

Question No : 6 DRAG DROP - (Topic 20)

Drag and drop the extended ping options from the left onto the troubleshooting functions they perform on the right.

Answer:



Explanation: Data pattern = detects framing errors
Df-bit = Verify routing metrics
Hop count = prevents packet segmentation when set
ToS = Troubleshoots QoS issues
Validate Reply = verify that a packet was received

Question No : 7 DRAG DROP - (Topic 20)

Drag and drop the extended traceroute options from the left onto the troubleshooting they perform on the right.

max ttl	limits the number of hops a packet travels.
port number	limits the number of traceroute packets sent to a single destination.
probe count	troubleshoots connections geenrated from a specific interface.
source address	troubleshoots QoS issues
type of service	troubleshoots TCP and UDP port states

Answer:

Explanation: Max TTL —> limits the number of hops a packet travel
Port number –> troubleshoot connections generated from specific interface
Probe count –> limits the number of traceroute
Source address–> troubleshoot TCP and UDP port
Type of service –> troubleshoot QoS issues

Topic 23, Mix Questions Set 2

Question No : 8 - (Topic 23)

Which of the following is an unlikely reason for the ARP process to fail?

A. CEF switching is disabled on the switch
B. The source device and destination device are in different VLANs
C. The VLAN is excluded from the trunk
D. The host is connected to the switch through an IP phone
E. A faulty cable from host to switch or between switches
F. The trunking encapsulation type is inconsistent on the two ends of the link

Answer: A,D

Question No : 9 - (Topic 23)

You have 2 NTP servers in your network - 10.1.1.1 and 10.1.1.2. You want to configure a Cisco router to use 10.1.1.2 as its NTP server before falling back to 10.1.1.1. Which commands will you use to configure the router?

A. ntp server 10.1.1.1
ntp server 10.1.1.2
B. ntp server 10.1.1.1
ntp server 10.1.1.2 primary
C. ntp server 10.1.1.1
ntp server 10.1.1.2 prefer
D. ntp server 10.1.1.1 fallback
ntp server 10.1.1.2

Answer: C

Explanation:

Preferred server

A router can be configured to prefer an NTP source over another. A preferred server's responses are discarded only if they vary dramatically from the other time sources. Otherwise, the preferred server is used for synchronization without consideration of the other time sources. Preferred servers are usually specified when they are known to be extremely accurate. To specify a preferred server, use the *prefer* keyword appended to the *ntp server* command. The following example tells the router to prefer *TimeServerOne* over *TimeServerTwo*:

Router#*config terminal*
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#*ntp server TimeServerOne prefer*
Router(config)#*ntp server TimeServerTwo*
Router(config)#^*Z*

Reference: Hardening Cisco Routers By Thomas Akin February 2002 0-596-00166-5, Chapter 10, NTP.

Question No : 10 - (Topic 23)

Which of the following is not a valid reason for a packet to be punted?

A. The TCAM has reached capacity
B. An unknown destination MAC address
C. A packet being discarded due to a security violation
D. A Telnet packet from a session being initiated with the switch
E. Routing protocols sending broadcast traffic
F. A packet belonging to a GRE tunnel

Answer: C

Reference: CCNP TSHOOT Certification Guide: Advanced Cisco CatalystSwitch Troubleshooting