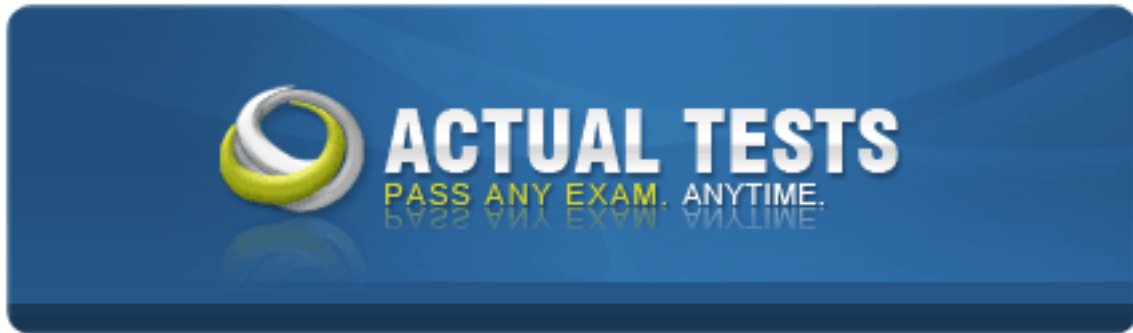


Cisco 642-832



**Troubleshooting and Maintaining Cisco IP Networks
(TSHOOT)
Version: 8.8**

Topic 1, Multiple Choice Questions

QUESTION NO: 1

The following commands are issued on a Cisco Router:

```
Router(configuration)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
```

```
Router(configuration)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
```

```
Router(configuration)#exit
```

```
Router#debug ip packet 199
```

What will the debug output on the console show?

- A. All IP packets passing through the router
- B. Only IP packets with the source address of 10.1.1.1
- C. All IP packets from 10.1.1.1 to 172.16.1.1
- D. All IP Packets between 10.1.1.1 and 172.16.1.1

Answer: D

Explanation:

In this example, the “debug ip packet” command is tied to access list 199, specifying which IP packets should be debugged. Access list 199 contains two lines, one going from the host with IP address 10.1.1.1 to 172.16.1.1 and the other specifying all TCP packets from host 172.16.1.1 to 10.1.1.1.

QUESTION NO: 2

What level of logging is enabled on a Router where the following logs are seen?

```
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
```

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

- A. alerts
- B. critical
- C. errors
- D. notifications

Answer: D

Explanation:

Cisco routers, switches, PIX and ASA firewalls prioritize log messages into 8 levels (0-7), as shown below:

Level	Level Name	Description
0	Emergencies	System is unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Informational messages
6	Informational	Normal but significant conditions
7	Debugging	Debugging messages

When you enable logging for a specific level, all logs of that severity and greater (numerically less) will be logged. In this case we can see that logging level of 3 (as seen by the 3 in “**LINK-3-UPDOWN**”) and level 5 (as seen by the 5 in “**LINEPROTO-5-UPDOWN**”) are shown, which means that logging level 5 must have been configured. As shown by the table, logging level 5 is Notifications.

QUESTION NO: 3

You have the followings commands on your Cisco Router:

ip ftp username admin

ip ftp password backup

You have been asked to switch from FTP to HTTP. Which two commands will you use to replace the existing commands?

- A. ip http username admin
- B. ip http client username admin
- C. ip http password backup
- D. ip http client password backup
- E. ip http server username admin
- F. ip http server password backup

Answer: B,D

Explanation:

Configuring the HTTP Client

Perform this task to enable the HTTP client and configure optional client characteristics.

The standard HTTP 1.1 client and the secure HTTP client are always enabled. No commands

exist to disable the HTTP client. For information about configuring optional characteristics for the HTTPS client, see the *HTTPS-HTTP Server and Client with SSL 3.0*, Release 12.2(15)T, feature module.

SUMMARY STEPS

1.

enable
2.

configure terminal
3.

ip http client cache {ager interval *minutes* | memory {file *file-size-limit* | pool *pool-size-limit*}
4.

ip http client connection {forceclose | idle timeout *seconds* | retry *count* | timeout *seconds*}
5.

ip http client password *password*
6.

ip http client proxy-server *proxy-name* proxy-port *port-number*
7.

ip http client response timeout *seconds*
8.

ip http client source-interface *type number*
9.

ip http client username *username*

Reference: HTTP 1.1 Web Server and Client

. http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_http_web.html

QUESTION NO: 4

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

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
```

QUESTION NO: 5

The following command is issued on a Cisco Router:

```
Router(configuration)#logging console warnings
```

Which alerts will be seen on the console?

- A. Warnings only
- B. debugging, informational, notifications, warnings
- C. warnings, errors, critical, alerts, emergencies
- D. notifications, warnings, errors
- E. warnings, errors, critical, alerts

Answer: C

Explanation:

Cisco routers prioritize log messages into 8 levels (0-7), as shown below:

Level	Level Name	Description
0	Emergencies	System is unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Informational messages
6	Informational	Normal but significant conditions
7	Debugging	Debugging messages

When you enable logging for a specific level, all logs of that severity and greater (numerically less)

will be logged. In this case, when you enable console logging of warning messages (level 4), it will log levels 0-4, making the correct answer warnings, errors, critical, alerts, and emergencies.

QUESTION NO: 6

Which two of the following options are categories of Network Maintenance tasks?

- A.** Firefighting
- B.** Interrupt-driven
- C.** Policy-based
- D.** Structured
- E.** Foundational

Answer: B,D

Explanation:

Proactive Versus Reactive Network Maintenance:

Network maintenance tasks can be categorized as one of the following:

Structured tasks: Performed as a predefined plan.

Interrupt-driven tasks: Involve resolving issues as they are reported.

Reference: CCNP TSHOOT Official Certification Guide, Kevin Wallace, Chapter 1, p.7

QUESTION NO: 7

You enabled CDP on two Cisco Routers which are connected to each other. The Line and Protocol status for the interfaces on both routers show as UP but the routers do not see each other as CDP neighbors. Which layer of the OSI model does the problem most likely exist?

- A.** Physical
- B.** Session
- C.** Application
- D.** Data-Link
- E.** Network

Answer: D

Explanation:

CDP is a protocol that runs over Layer 2 (the data link layer) on all Cisco routers, bridges, access servers, and switches. CDP allows network management applications to discover Cisco devices that are neighbors of already known devices, in particular, neighbors running lower-layer, transparent protocols. With CDP, network management applications can learn the device type and

the SNMP agent address of neighboring devices. This feature enables applications to send SNMP queries to neighboring devices. In this case, the line protocol is up which means that the physical layer is operational (layer 1) but the data link layer is not.

Reference: "Configuring CDP"

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.1E/native/configuration/guide/cdp.html>

QUESTION NO: 8

FCAPS is a network maintenance model defined by ISO. It stands for which of the following ?

- A. Fault Management
- B. Action Management
- C. Configuration Management
- D. Protocol Management
- E. Security Management

Answer: A,C,E

Explanation:

The FCAPS maintenance model consists of the following:

FCAPS Maintenance Tasks:

QUESTION NO: 9

Which three management categories are contained in the FCAPS network maintenance model? (Choose three.)

- A. Config
- B. Fault
- C. Storage
- D. Accounting
- E. Redundancy
- F. Telecommunications

Answer: A,B,D

Explanation:

QUESTION NO: 10

What is the result of configuring the logging console warning command?

- A. Messages with a severity level of 4 and higher will be logged to all available TTY lines.
- B. Only warning messages will be logged on the console.
- C. Warning, error, critical, and informational messages will be logged on the console.
- D. Warning, critical, alert, and emergency messages will be logged on the console.
- E. The logging console warning command needs to be followed in the configuration with logging buffered byte size to specify the message buffer size for the console.

Answer: D

Explanation:

QUESTION NO: 11

Refer to the shown below.

%PIX|ASA-3-105010: (Primary) Failover message block alloc failed

- %PIX|ASA-3-106010: Deny inbound protocol src interface_name:dest_address/dest_port dst interface_name:source_address/source_port
- %PIX|ASA-3-106011: Deny inbound (No xlate) string
- %PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)
- %PIX-3-107003: RIP: Attempted reference of stale data encountered in function, line: line_num
- %PIX|ASA-3-109010: Auth from inside_address/inside_port to outside_address/outside_port failed (too many pending auths) on interface interface_name.
- %PIX|ASA-3-109013: User must authenticate before using this service
- %PIX|ASA-3-109016: Can't find authorization ACL acl_ID for user 'user'
- %PIX|ASA-3-109018: Downloaded ACL acl_ID is empty
- %PIX|ASA-3-109019: Downloaded ACL acl_ID has parsing error; ACE string
- %PIX|ASA-3-109020: Downloaded ACL has config error; ACE
- %PIX|ASA-3-109023: User from source_address/source_port to dest_address/dest_port on interface outside_interface must authenticate before using this service.

What statement is correct regarding the output shown in the graphic?

- A.** These two log messages will not have a severity level. They are not errors but are just informational messages.
- B.** The first log message is categorized as a warning message.
- C.** These messages regarding interface status are normal output and will always be displayed when you exit config mode.
- D.** The first log message is an error message with a severity level of 3.
- E.** The second message would be shown if the logging console warning command had been issued.

Answer: D

Explanation:

QUESTION NO: 12

Refer to the configuration statements shown in the graphic above.

```
R1(config)#access-list 199 permit tcp host 10.1.1.1 host 172.16.1.1
```

```
R1(config)#access-list 199 permit tcp host 172.16.1.1 host 10.1.1.1
```

```
R1(config)#end
```

```
R1#debug ip packet 199 detail
```

Which statement reflects what the effect is of this configuration sequence?

- A.** These commands will generate an error message because you cannot use an access list with any debug commands.
- B.** These commands will have no effect at all. The debug ip packet command will work as normal and display info for all IP packets.
- C.** These commands turn on debug ip packet only for packets between hosts 10.1.1.1 and 172.16.1.1.
- D.** These commands will only work when you specify only one host rather than two.

Answer: C

Explanation:

QUESTION NO: 13

What is the result if you configure two devices with the ntp server command?

- A. Nothing will happen until one of the devices is configured with the prefer parameter.
- B. The NTP protocol will determine which server is most reliable and will synchronize to that server.
- C. The device with the highest priority will become the active server and the other device will become the backup server.
- D. The device with the lowest MAC address will become the active server and the other device will become the backup server.

Answer: B

Explanation:

QUESTION NO: 14

A technician is troubleshooting connectivity problems between two routers that are directly connected through a serial line. The technician notices that the serial line is up, but cannot see any neighbors displayed in the output of the show cdp neighbors command.

In which OSI layer is the problem most likely occurring?

- A. physical
- B. data link
- C. network
- D. transport
- E. application

Answer: B

Explanation:

QUESTION NO: 15

What are two approaches to maintaining a network?(Choose two.)

- A. PPDIOO
- B. structured

- C. bottoms up
- D. interrupt-driven

Answer: B,D

Explanation:

Topic 2, Drag Drop Questions

QUESTION NO: 16 DRAG DROP

FCAPS is a network maintenance model defined by ISO. FCAPS stands for:

Choose From Here	Place Here
F	Accounting Management
C	Fault Management
A	Configuration Management

Answer:

Choose From Here	Place Here
F	A
C	F
A	C

Explanation: F-> Fault Management
C-> Configuration Management
A -> Accounting Management

The FCAPS maintenance model consists of the following:

FCAPS Maintenance Tasks:

QUESTION NO: 17 DRAG DROP

There are many Network Maintenance models. Match the model names on the left to the options on the right:

Choose from Here	Place Here
FCAPS	A collection of best practice recommendations
ITIL	Often referred to as the PPDIOO model
Cisco Lifecycle	Telecommunications Management Network
TMN	Fault, Configuration, Accounting, Performance and

Answer:

Choose from Here	Place Here
FCAPS	ITIL
ITIL	Cisco Lifecycle
Cisco Lifecycle	TMN
TMN	FCAPS

Explanation:

FCAPS -> Fault, Configuration, Accounting, Performance and Security (ISO)

ITIL -> A collection of best practice recommendations

Cisco Lifecycle -> Often referred to as the PPDIOO model

TMN -> Telecommunications Management Network

Well Known Network Maintenance Models

Maintenance models

Model

Explanation

FCAPS

Fault-, Configuration-, Accounting-, Performance- and Security management

defined by ISO

ITIL

IT Infrastructure Library

Defines a collection of best-practice recommendations that work together to meet business goals.

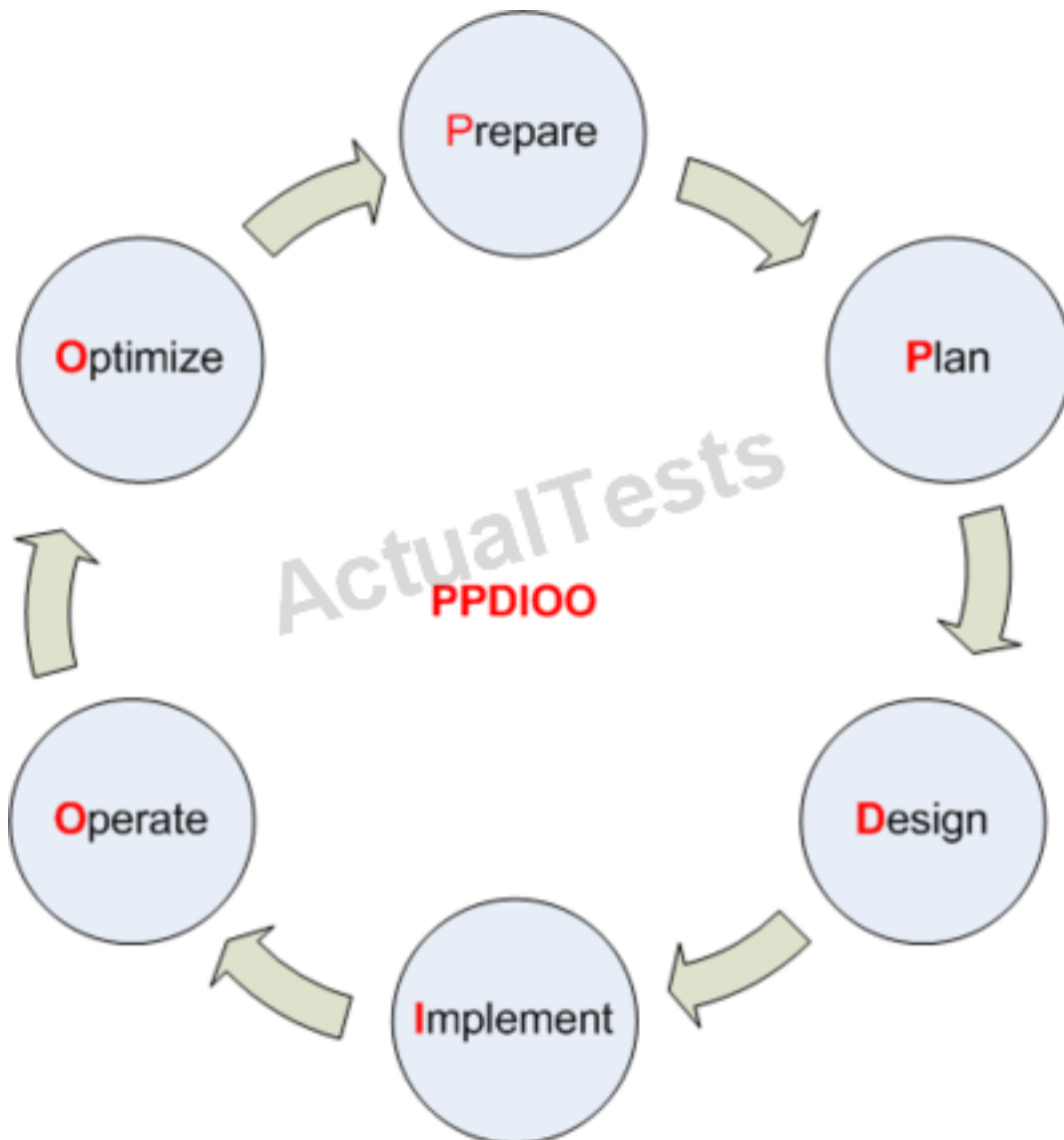
TMN

Telecommunications Management Network

ITU-T variation of FCAPS - See above - specially targeted towards Tele Communication Networks

PPDIOO

Also called Cisco Lifecycle Services (See drawing below)



PPDIOO Life Cycle

Reference: http://mars.tekkom.dk/mediawiki/index.php/CCNP_TSHOOT_642-832/Chapter_1

QUESTION NO: 18 DRAG DROP

Match the items on the left to their purpose on the right

Choose from here	Place Here
EEM	Used for Backup and Restore
SDM	CLI based Management and Monitoring
FTP	Provides a GUI for Administration

Answer:

Choose from here	Place Here
EEM	FTP
SDM	EEM
FTP	SDM

Explanation: EEM -> CLI based Management and Monitoring

SDM -> Provides a GUI for Administration

FTP -> Used for Backup and Restore

Cisco IOS Embedded Event Manager (EEM) is a powerful and flexible CLI based subsystem that provides real-time network event detection and onboard automation. It gives you the ability to adapt the behavior of your network devices to align with your business needs.

Cisco SDM is an intuitive, Web-based device-management tool for Cisco IOS® Software-based routers. The Cisco SDM simplifies router and security configuration through smart wizards, which help customers and Cisco partners quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the command-line interface (CLI). The Cisco SDM is supported on a wide range of Cisco routers and Cisco IOS Software releases.

Cisco devices can use FTP to backup and restore configuration files and IOS software. Some examples of this are shown below:

Example 1: Backing up manually

```
R1# copy startup-config ftp://kevin:dj7jS@192.168.22.33
```

```
Address or name of remote host [ 192.168.22.33]?
```

```
Destination file name [r1-config]?
```

Writing R1-config !!!

3458 bytes copied in 3.443 secs (1243 bytes/sec)

Example 2: Backing up automatically

The configuration below will make a backup:

```
write-memory Trigger backup when running-config is copied to nvram
time-period 1440 Trigger backup every 1440 minutes. 60*24=1440
!
ip ftp username kevin
ip ftp password dj7jS
!
archive
path ftp://192.168.2.33/R1-config
write-memory
time-period 1440Viewing
```

R1#show archive

The next archive file will be named ftp://192.168.2.33/R1-config-4

Archive # Name

0

1 ftp://192.168.2.33/R1-config-1

2 ftp://192.168.2.33/R1-config-2

3 ftp://192.168.2.33/R1-config-3 <- Most Recent

Topic 3, Ticket 1 : Switch Port Trunk

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. Redistribution 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.

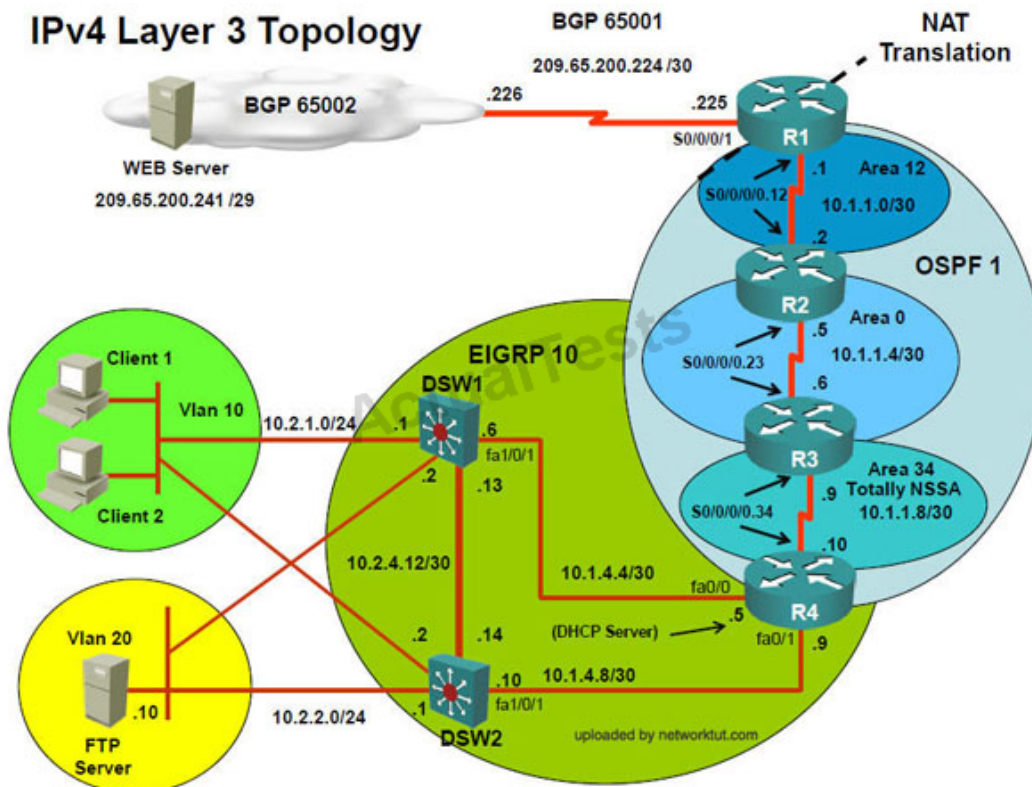
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

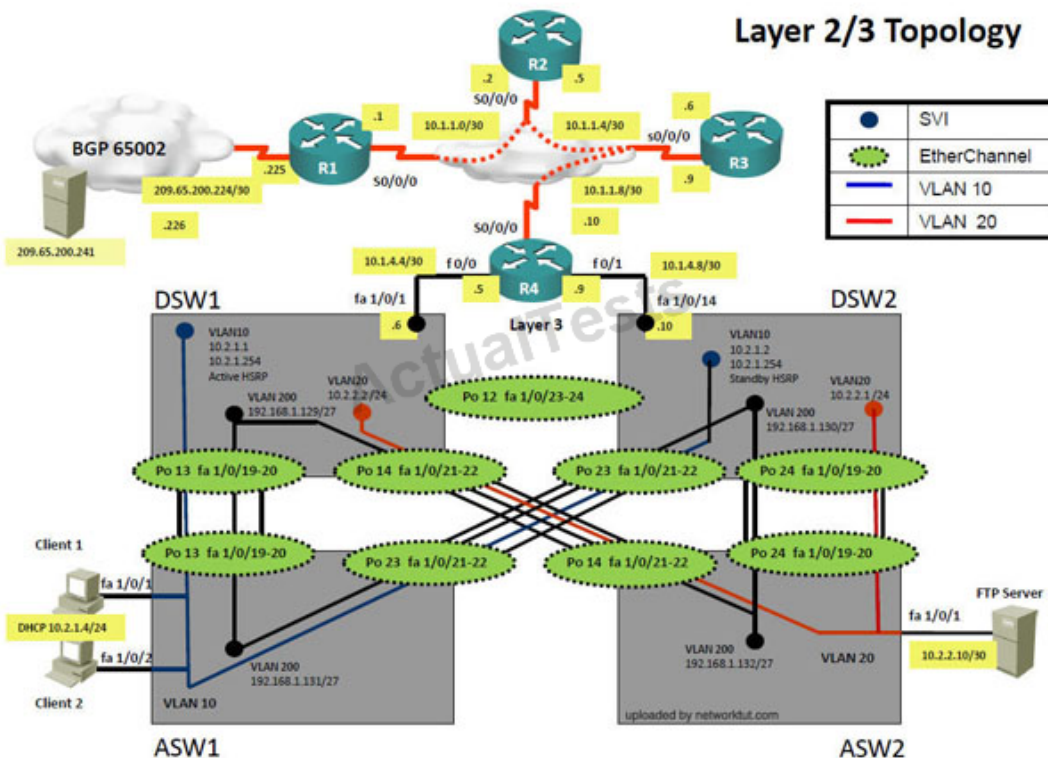
Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



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

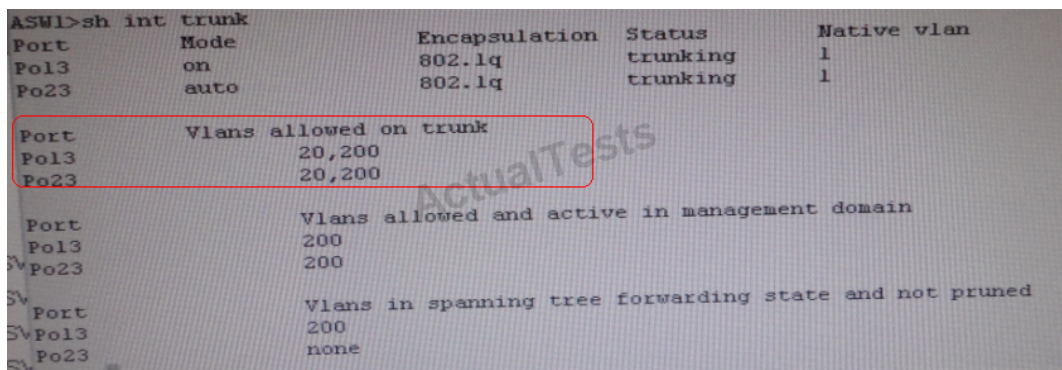
Sh run ----- & check for running config of int fa1/0/1 & fa1/0/2

=====

```
interface FastEthernet1/0/1switchport mode accessswitchport access vlan 10
interface FastEthernet1/0/2switchport mode accessswitchport access vlan 10
```

=====

- We need to check on ASW 1 trunk port the trunk Po13 & Po23 were receiving VLAN 20 & 200 but not VLAN 10 so that switch could not get DHCP IP address and was failing to reach IP address of Internet



Port	Mode	Encapsulation	Status	Native vlan
Po13	on	802.1q	trunking	1
Po23	auto	802.1q	trunking	1

Port	Vlans allowed on trunk
Po13	20,200
Po23	20,200

Port	Vlans allowed and active in management domain
Po13	200
Po23	200

Port	Vlans in spanning tree forwarding state and not pruned
Po13	200
Po23	none

- **Change required:** On ASW1 below change is required for switch-to-switch connectivity..
int range portchannel13,portchannel23 switchport trunk allowed vlan none switchport trunk allowed vlan 10,200

So in ticket Answer to the fault condition will be as :

QUESTION NO: 19

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, and FHRP services, a trouble ticket has been operated 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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: G

Explanation:

Since the Clients are getting an APIPA we know that DHCP is not working. However, upon closer examination of the ASW1 configuration we can see that the problem is not with DHCP, but the fact that the trunks on the port channels are only allowing VLANs 1-9, when the clients belong to VLAN 10. VLAN 10 is not traversing the trunk on ASW1, so the problem is with the trunk configuration on ASW1.

QUESTION NO: 20

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, and FHRP services, 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. Switch-to-Switch Connectivity
- C. Access Vlans
- D. Port Security
- E. VLAN ACL / Port ACL
- F. Switch Virtual Interface

Answer: B

Explanation:

Since the Clients are getting an APIPA we know that DHCP is not working. However, upon closer examination of the ASW1 configuration we can see that the problem is not with DHCP, but the fact

that the trunks on the port channels are only allowing VLANs 1-9, when the clients belong to VLAN 10. VLAN 10 is not traversing the trunk on ASW1, so the problem is with switch to switch connectivity, specifically the trunk configuration on ASW1.

QUESTION NO: 21

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, and FHRP services, 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 port-channel 13 command, then configure switchport trunk allowed vlan none followed by switchport trunk allowed vlan 20,200 commands.
- B.** In Configuration mode, using the interface port-channel 13, port-channel 23, then configure switchport trunk none allowed vlan none followed by switchport trunk allowed vlan 10,200 commands.
- C.** In Configuration mode, using the interface port-channel 23 command, then configure switchport trunk allowed vlan none followed by switchport trunk allowed vlan 20,200 commands.
- D.** In Configuration mode, using the interface port-channel 23, port-channel, then configure switchport trunk allowed vlan none followed by switchport trunk allowed vlan 10,20,200 commands.

Answer: B

Explanation:

We need to allow VLANs 10 and 200 on the trunks to restore full connectivity. This can be accomplished by issuing the "switchport trunk allowed vlan 10,200" command on the port channels used as trunks in DSW1.

=====

====

Topic 4, 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. Redistribution 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.

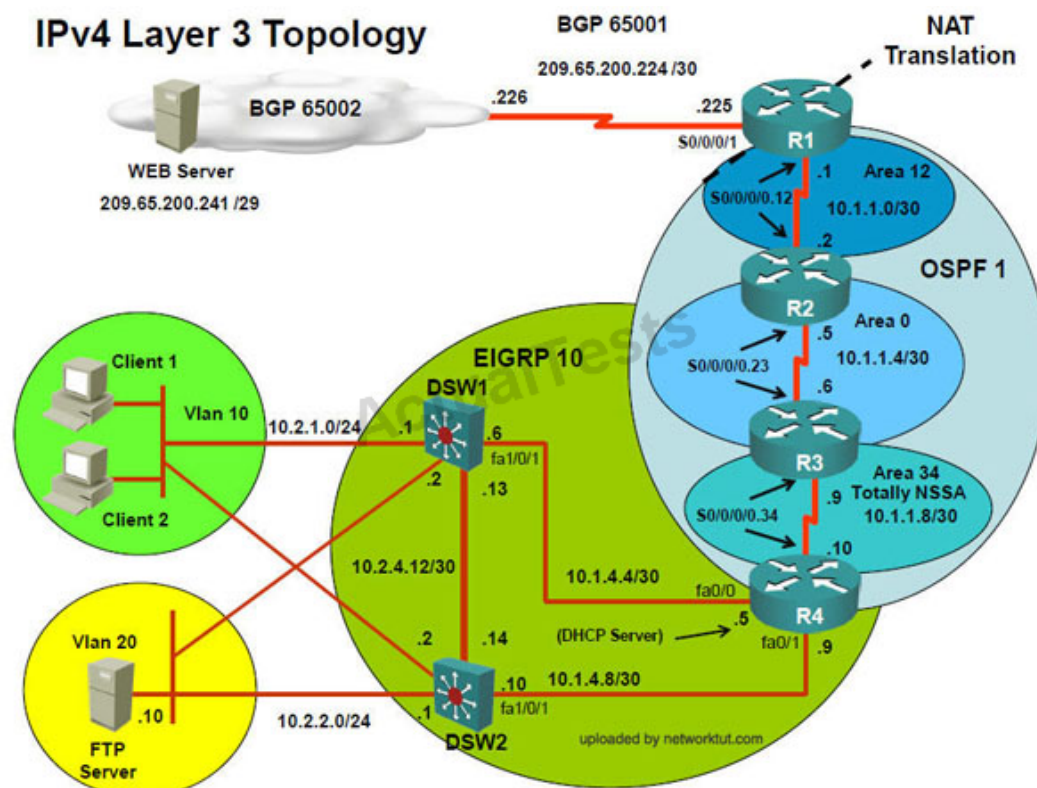
Question-1 Fault is found on which device,

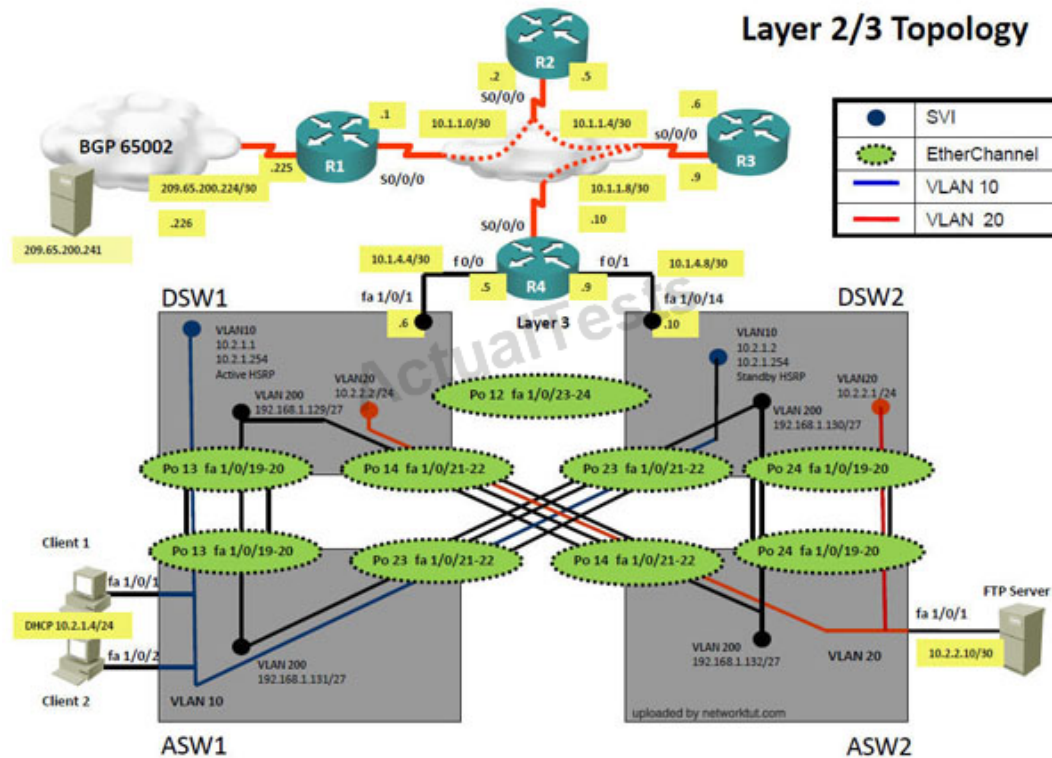
Question-2 Fault condition is related to,

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

=====

```
interface FastEthernet1/0/1
description link to Client 1
switchport mode access
switchport nonegotiate
spanning-tree portfast

interface FastEthernet1/0/2
description link to Client 2
switchport mode access
switchport nonegotiate
spanning-tree portfast
```

- =====
- 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
-

So in ticket Answer to the fault condition will be as:

QUESTION NO: 22

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. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: G

Explanation:

QUESTION NO: 23

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 switch technology?

- A. NTP
- B. Switch-to-Switch Connectivity
- C. Loop Prevention
- D. Access Vlans
- E. VLAN ACL Port ACL
- F. Switch Virtual Interface
- G. Port Security

Answer: D

Explanation:

QUESTION NO: 24

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:

=====

=====

Topic 5, Ticket 3 : OSPF Authentication

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. Redistribution 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.

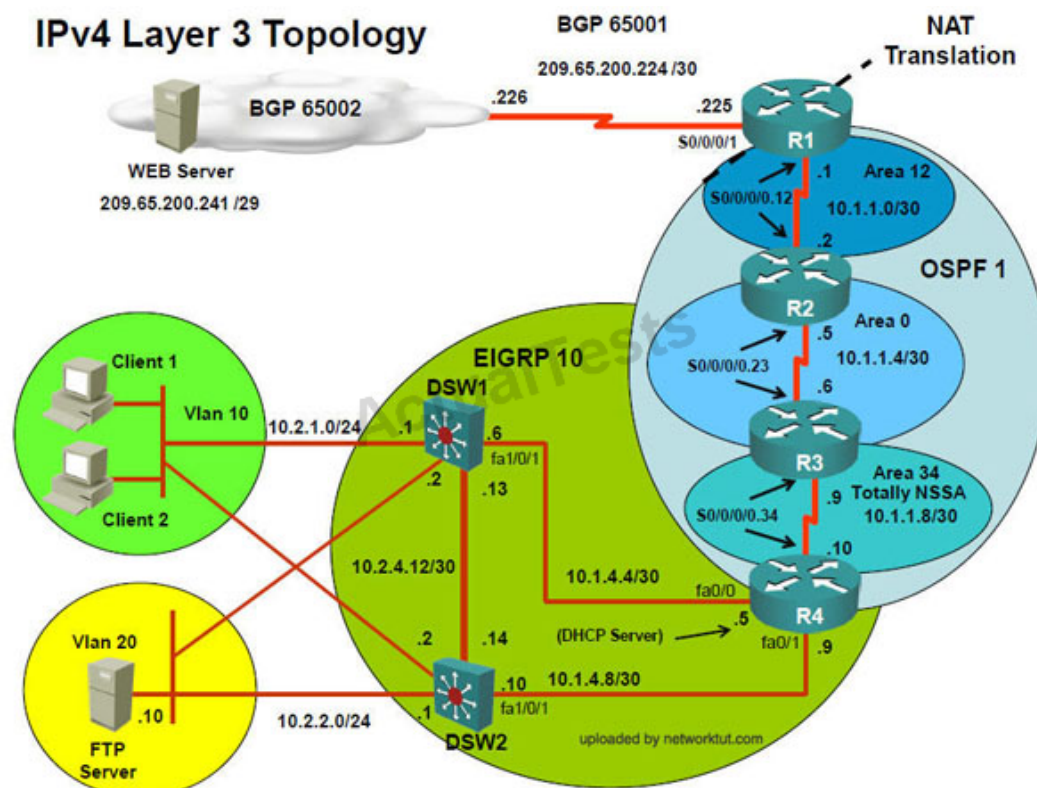
Question-1 Fault is found on which device,

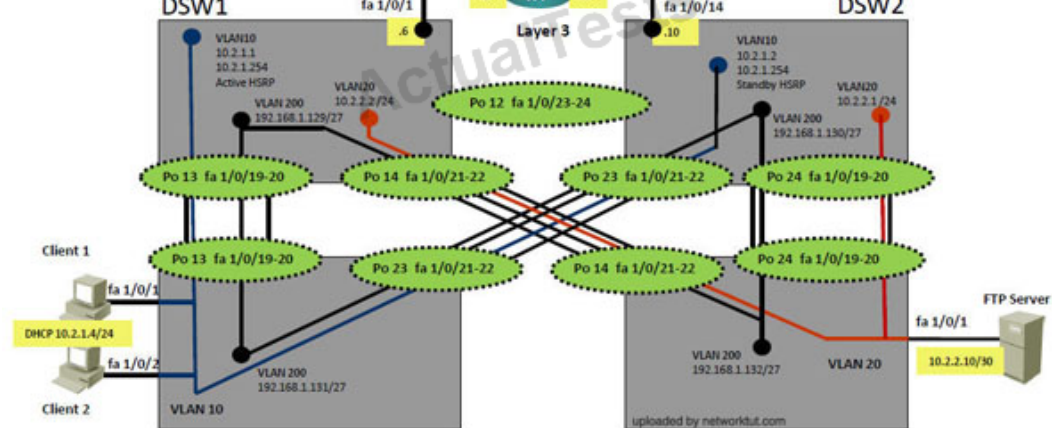
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

=====



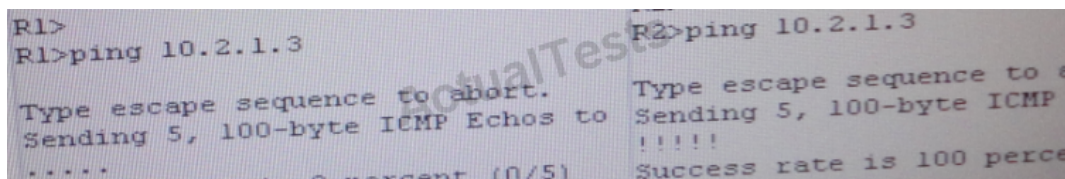


Client is unable to ping IP 209.65.200.241

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 , R3, R2 but not from R1



- Check for neighborship of ospf
sh ip ospf nei ----- Only one neighborship is forming with R2 & i.e. with R3

Since R2 is connected to R1 & R3 with routing protocol ospf than there should be 2 neighbors seen but only one is seen

- Need to check running config of R2 & R3 for interface Sh run ----- Interface Serial0/0/0/0.12 on R2

```

R1
duplex auto
speed auto
!
interface Serial0/0/0
description Link to R2
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly
encapsulation frame-relay
ip ospf message-digest-key 1 md5 TSHOOT
ip ospf network point-to-point
ip ospf priority 0
ip ospf 1 area 12
ipv6 address 2026::12:1/122
ipv6 ospf network point-to-point
ipv6 ospf 6 area 12
frame-relay map ipv6 FE80::2 403
frame-relay map ip 10.1.1.1 403 broadcast
frame-relay map ip 10.1.1.2 403
frame-relay map ipv6 2026::12:1 403 broadcast
frame-relay map ipv6 2026::12:2 403
no frame-relay inverse-arp

R2
speed auto
!
interface Serial0/0/0
no ip address
encapsulation frame-relay
no frame-relay inverse-arp
!
interface Serial0/0/0.12 point-to-point
description Link to R1
ip address 10.1.1.2 255.255.255.252
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 TSHOOT
ipv6 address 2026::12:2/122
ipv6 address FE80::2 link-local
ipv6 ospf 6 area 12
frame-relay interface-dlci 304
!
interface Serial0/0/0.23 point-to-point
description Link to R3
ip address 10.1.1.5 255.255.255.252
ipv6 address 2026::1:1/123
ipv6 ospf 6 area 0
frame-relay interface-dlci 302

```

Sh run ----- Interface Serial0/0/0/0 on R1

- **Change required:** On R1, for IPV4 authentication of OSPF command is missing and required to configure----- ip ospf authentication message-digest

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 25

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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: A

Explanation:

QUESTION NO: 26

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. BGP
- B. NTP
- C. IP NAT
- D. IPv4 OSPF Routing
- E. IPv4 OSPF Redistribution
- F. IPv6 OSPF Routing
- G. IPv4 layer 3 security

Answer: D

Explanation:

QUESTION NO: 27

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.** Enable OSPF authentication on the s0/0/0 interface using the ip ospf authentication message-digest command
- B.** Enable OSPF routing on the s0/0/0 interface using the network 10.1.1.0 0.0.0.255 area 12 command.
- C.** Enable OSPF routing on the s0/0/0 interface using the network 209.65.200.0 0.0.0.255 area 12 command.
- D.** Redistribute the BGP route into OSPF using the redistribute BGP 65001 subnet command.

Answer: A

Explanation:

=====

=====

Topic 6, Ticket 4 : BGP Neighbor

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. Redistribution 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.

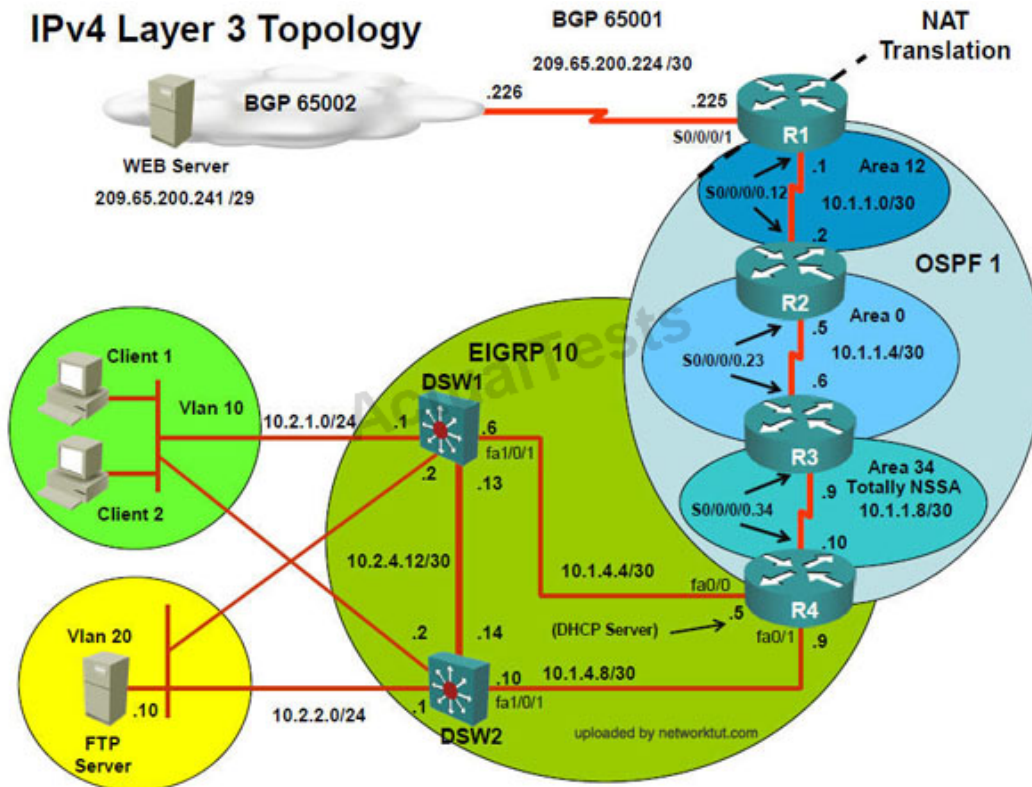
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

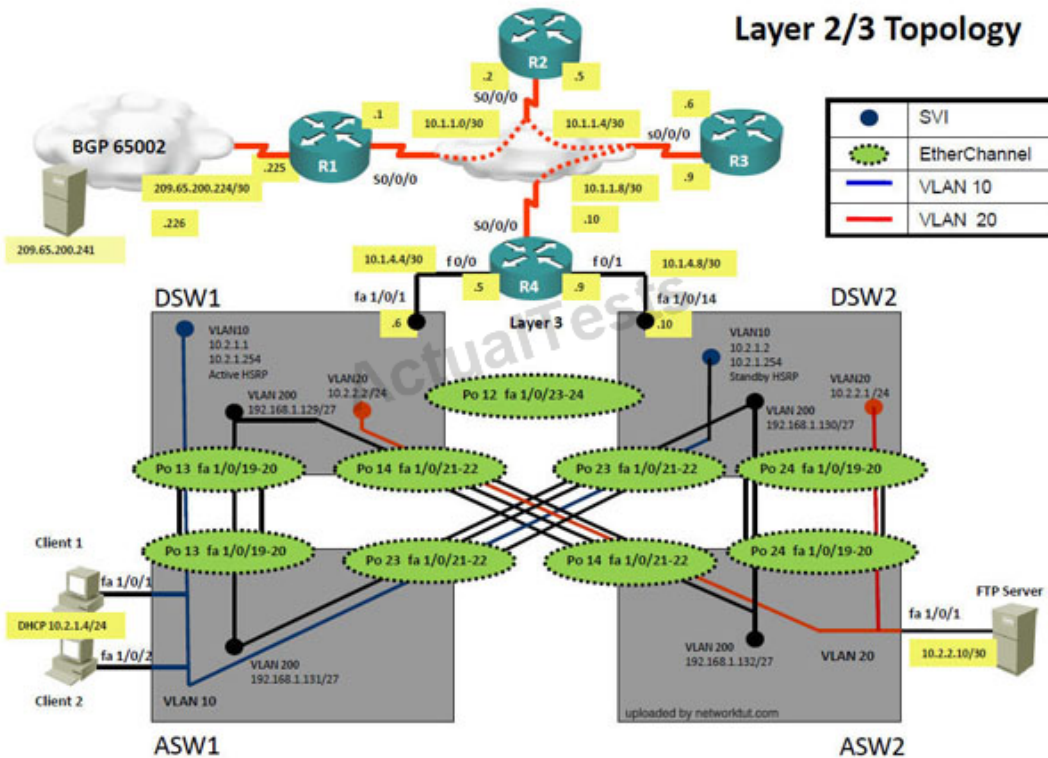
Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



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 , R3, R2, R1
- Look for BGP Neighbourship
Sh ip bgp summary ----- No O/P will be seen
- Check for interface IP & ping IP 209.65.200.225 ---- Reply will be received from Webserver interface
- Look for peering IP address via sh run on R1 interface serial 0/0/1

```
interface Serial0/0/1
description Link to ISP
ip address 209.65.200.225 255.255.255.252
ip nat outside
ip virtual-reassembly
ntp broadcast client
ntp broadcast key 1
```

```
router bgp 65001
no synchronization
bgp log-neighbor-changes
neighbor 209.56.200.226 remote-as 65002
no auto-summary
```

- Since we are receiving icmp packets from Webserver interface on R1 so peering IP address under router BGP is configured wrong IP but with correct AS nos.
- **Change required:** On R1 under router BGP Change neighbor 209.56.200.226 remote-as 65002 statement to neighbor 209.65.200.226 remote-as 65002

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 28

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 schemes, 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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1

Answer: A

Explanation:

QUESTION NO: 29

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. BGP
- B. NTP
- C. IP NAT
- D. IPv4 OSPF Routing
- E. IPv4 OSPF Redistribution
- F. IPv6 OSPF Routing
- G. IPv4 layer 3 security

Answer: A

Explanation:

QUESTION NO: 30

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. Under the BGP process, enter the `bgp redistribute-internal` command.
- B. Under the BGP process, `bgp confederation identifier 65001` command.
- C. Deleted the current BGP process and reenter all of the command using 65002 as the AS number.
- D. Under the BGP process, delete the `neighbor 209.56.200.226 remote-as 65002` command and enter the `neighbor 209.65.200.226 remote-as 65002` command.

Answer: D

Explanation:

=====

=====

Topic 7, Ticket 5 : NAT ACL

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. Redistribution 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.

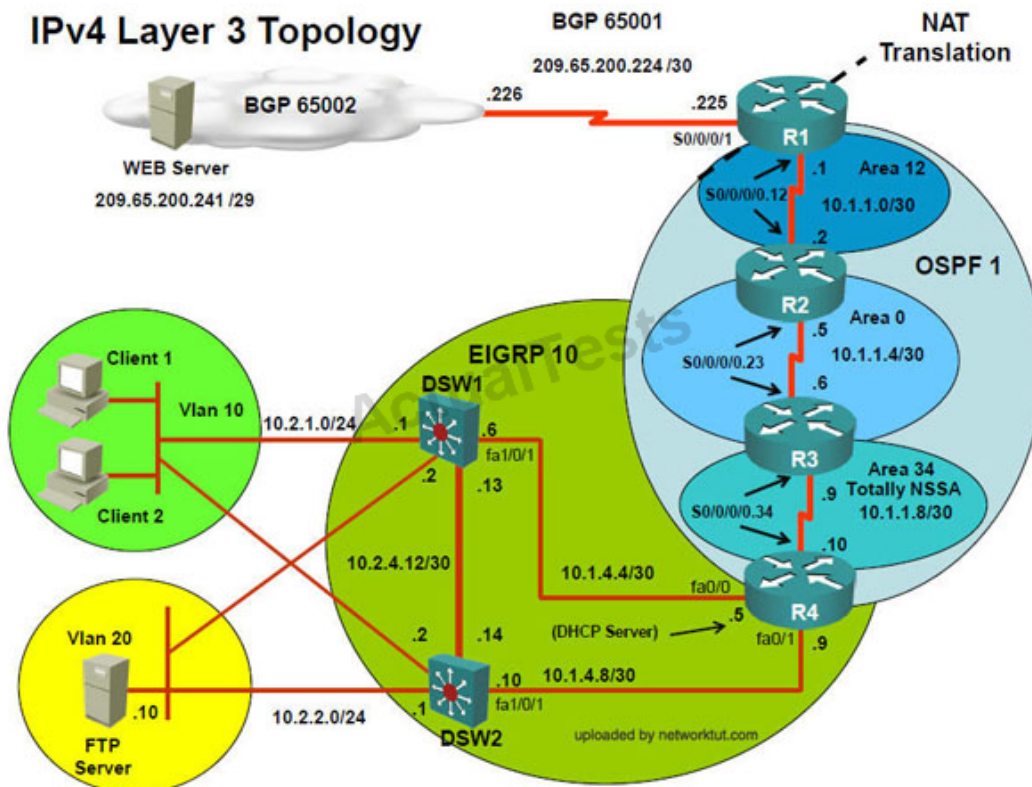
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

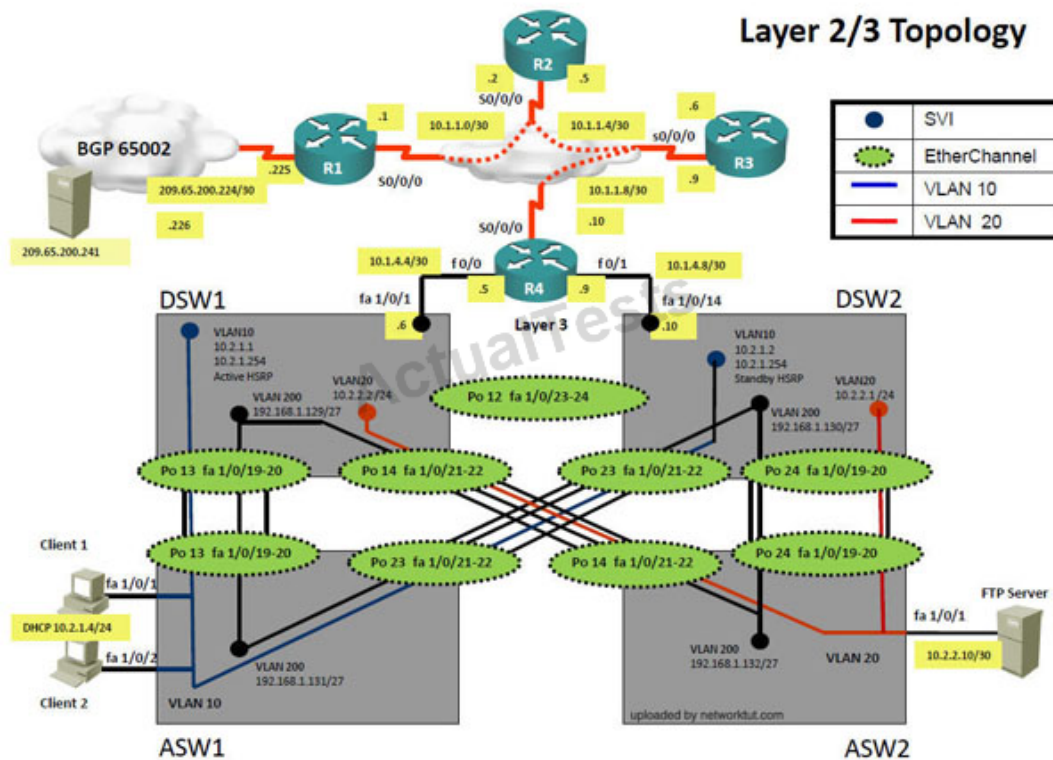
Question-3 What exact problem is seen & what needs to be done for solution

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



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 , R3, R2, R1
- Look for BGP Neighbourship
Sh ip bgp summary ----- State of BGP will be in established state & will be able to receive I prefix (209.65.200.241)
- As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of webserver & we are able to ping the same from R1. Further troubleshooting needs to be done on R1 on serial 0/0/1
- Check for running config. i.e sh run for interface serial 0/0/1..

```
interface Serial0/0/1
description Link to ISP
ip address 209.65.200.225 255.255.255.252
ip nat outside
ip virtual-reassembly
ntp broadcast client
ntp broadcast key 1
```

!

```
ip http server
no ip http secure-server
ip nat inside source list nat_traffic interface Serial0/0/1 overload
!
ip access-list standard nat_traffic
permit 10.1.0.0 0.0.255.255
!
ipv6 router ospf 6
log-adjacency-changes
```

!

From above snapshot we are able to see that IP needs to be PAT to serial 0/0/1 to reach web server IP

(209.65.200.241). But in access-list of NAT IP allowed IP is 10.1.0.0/16 is allowed & need 10.2.0.0/16 to

- As per troubleshooting we are able to ping ip 10.2.1.3 from R1 & BGP is also receiving prefix of web server & we are able to ping the same from R1. Its should be checked further for running config of interface for stopping
- **Change required:** On R1, In natting we need to add client IP address for reachability to server.

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 31

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 schemes, 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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1

Answer: A

Explanation:

QUESTION NO: 32

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. BGP
- B. NTP
- C. IP NAT
- D. IPv4 OSPF Routing
- E. IPv4 OSPF Redistribution
- F. IPv6 OSPF Routing
- G. IPv4 layer 3 security

Answer: C

Explanation:**QUESTION NO: 33**

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. Under the interface Serial0/0/0 configuration enter the ip nat inside command.
- B. Under the interface Serial0/0/0 configuration enter the ip nat outside command.
- C. Under the ip access-list standard nat_traffic configuration enter the permit 10.2.0.0 0.0.255.255 command.
- D. Under the ip access-list standard nat_traffic configuration enter the permit 209.65.200.0 0.0.0.255 command.

Answer: C

Explanation:

=====

=====

Topic 8, Ticket 6 : R1 ACL

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. Redistribution 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.

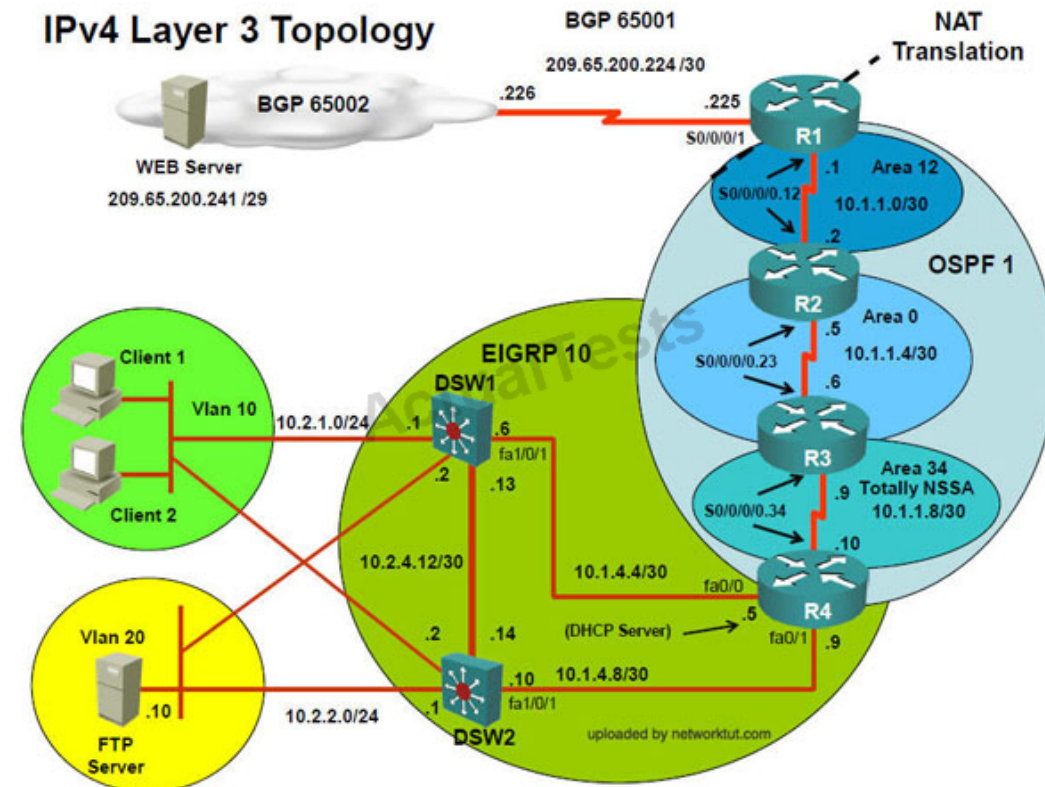
Each ticket has 3 sub questions that need to be answered & topology remains same.

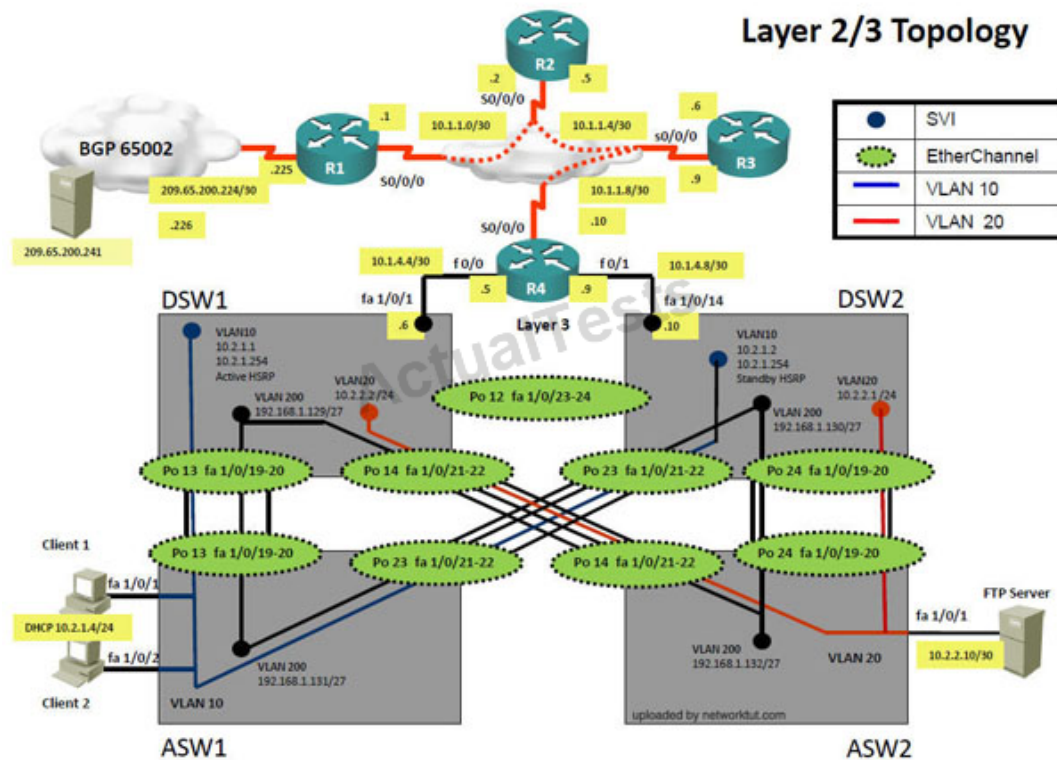
Question-1 Fault is found on which device,

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 , R3, R2, R1
- Look for BGP Neighbourship
- Sh ip bgp summary ----- State of BGP will be in active state. This means connectivity issue between serial
- Check for running config. i.e sh run --- over here check for access-list configured on interface as BGP is down (No need to check for NAT configuration as its configuration should be right as first need to bring BGP up)

```
interface Serial0/0/1
description Link to ISP
ip address 209.65.200.225 255.255.255.252
ip access-group edge_security in
ip nat outside
ip virtual-reassembly
ntp broadcast client
ntp broadcast key 1
no cdp enable
```

```
ip nat inside source list nat_traffic interface Serial0/0/1 overload
!
ip access-list standard nat_traffic
permit 10.1.0.0 0.0.255.255
permit 10.2.0.0 0.0.255.255
!
ip access-list extended edge_security
deny ip 10.0.0.0 0.255.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
permit ip host 209.65.200.241 any
!
```

- In above snapshot we can see that access-list of edge_security on R1 is not allowing wan IP network
 - **Change required:** On R1, we need to permit IP 209.65.200.222/30 under access list.
-

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 34

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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1

Answer: A

Explanation:

QUESTION NO: 35

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. BGP
- B. NTP
- C. IP NAT
- D. IPv4 OSPF Routing
- E. IPv4 OSPF Redistribution
- F. IPv6 OSPF Routing
- G. IPv4 layer 3 security

Answer: G

Explanation:

QUESTION NO: 36

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. Under the interface Serial0/0/1 enter the ip access-group edge_security out command.
- B. Under the ip access-list extended edge_security configuration add the permit ip 209.65.200.224 0.0.0.3 any command.
- C. Under the ip access-list extended edge_security configuration delete the deny ip 10.0.0.0 0.255.255.255 any command.
- D. Under the interface Serial0/0/0 configuration delete the ip access-group edge_security in command and enter the ip access-group edge_security out command.

Answer: B

Explanation:

=====

=====

Topic 9, Ticket 7 : Port Security

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. Redistribution 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.

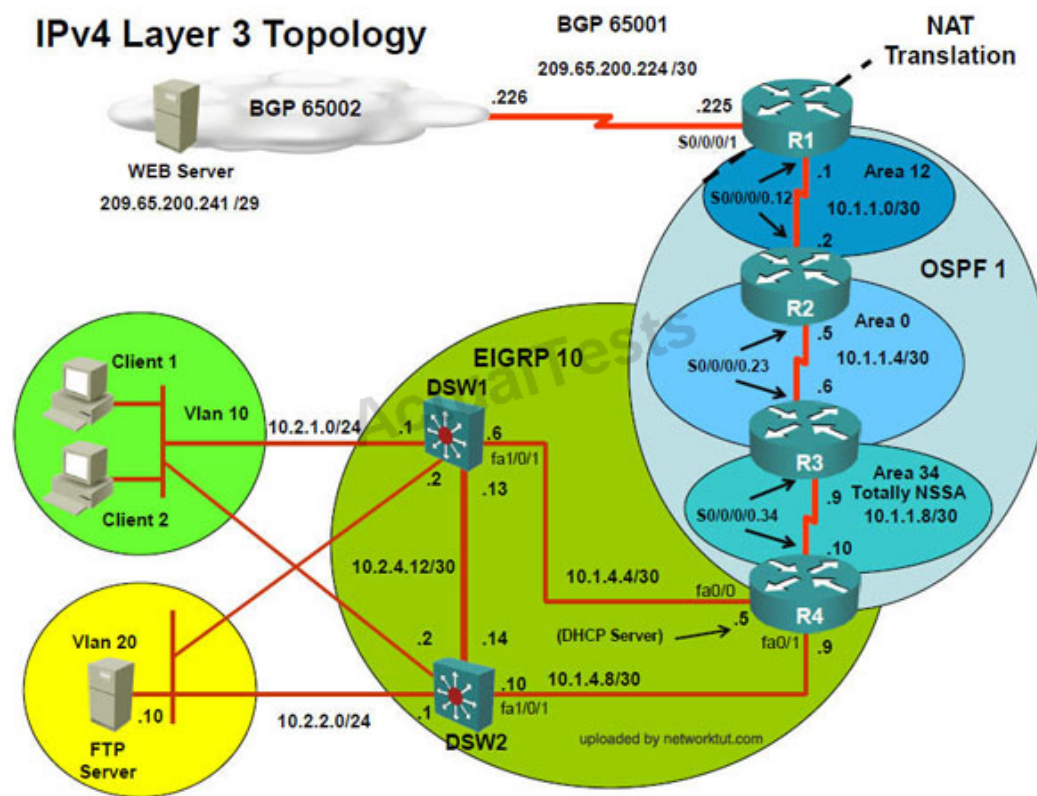
Question-1 Fault is found on which device,

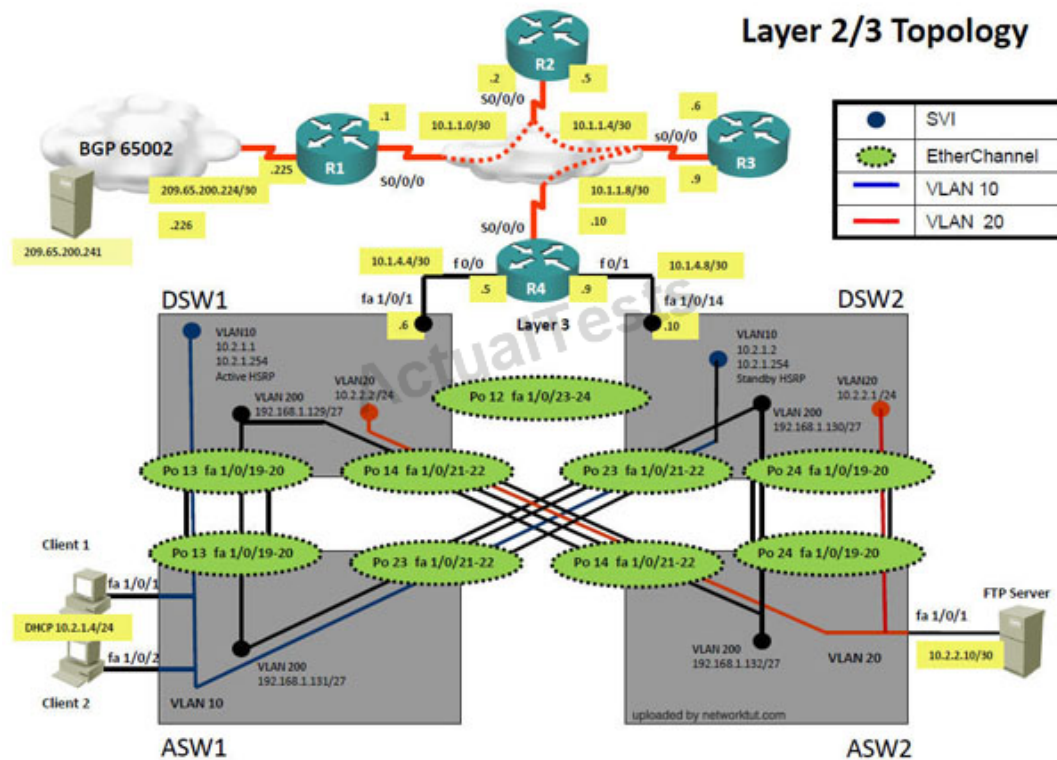
Question-2 Fault condition is related to,

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 but when we checked interface it was showing down
- Sh run ----- check for running config of int fa1/0/1 & fa1/0/2 (switchport access Vlan 10 will be there with switch port security command). Now check as below

Sh int fa1/0/1 & sh int fa1/0/2

```
ASW1
FastEthernet1/0/1 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 001b.90ab.bc83 (bia 001b.90ab.bc83)
Description: link to Client 1
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

```
ASW1
FastEthernet1/0/2 is down, line protocol is down (err-disabled)
Hardware is Fast Ethernet, address is 001b.90ab.bc84 (bia 001b.90ab.bc84)
Description: link to Client 2
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

- As seen on interface the port is in err-disable mode so need to clear port.
 - **Change required:** On ASW1, for port security need command to remove port-security under interface under interface fa1/0/1 & fa1/0/2.
-

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 37

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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: G

Explanation:

QUESTION NO: 38

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. Switch-to-Switch Connectivity
- C. Access Vlan
- D. Port Security
- E. VLAN ACL / Port ACL
- F. Switch Virtual Interface

Answer: D

Explanation:

QUESTION NO: 39

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 Fa 1/0/1 – 2, then no switchport port-security interface configuration commands. Then in exec mode clear errdisable interface fa 1/0/1 – 2 vlan 10 command
- B. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security, followed by shutdown, no shutdown interface configuration commands.
- C. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security interface configuration commands.
- D. In Configuration mode, using the interface range Fa 1/0/1 – 2, then no switchport port-security interface configuration commands. Then in exec mode clear errdisable interface fa 1/0/1, then clear errdisable interface fa 1/0/2 commands.

Answer: B

Explanation:

Reference:

http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00806cd87b.shtml

=====
=====

Topic 10, 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 RIPv3 process name RIPv3_ZONE.

The two IPv6 routing domains, OSPF 6 and RIPv3 are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistribution 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.

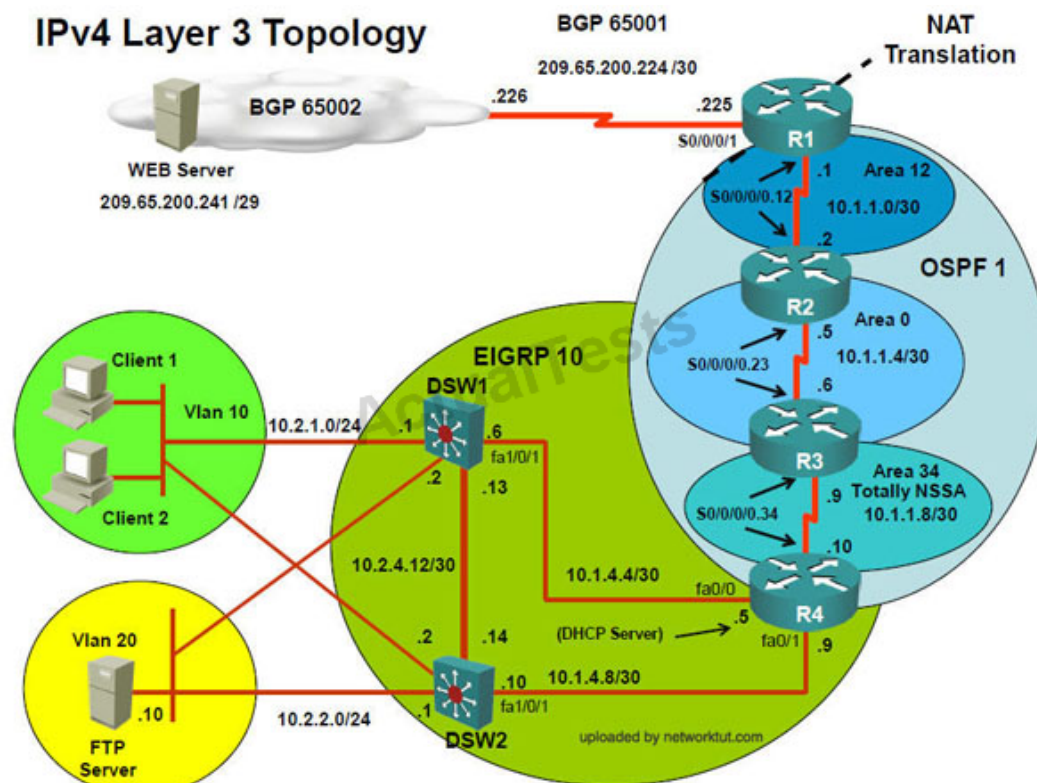
Question-1 Fault is found on which device,

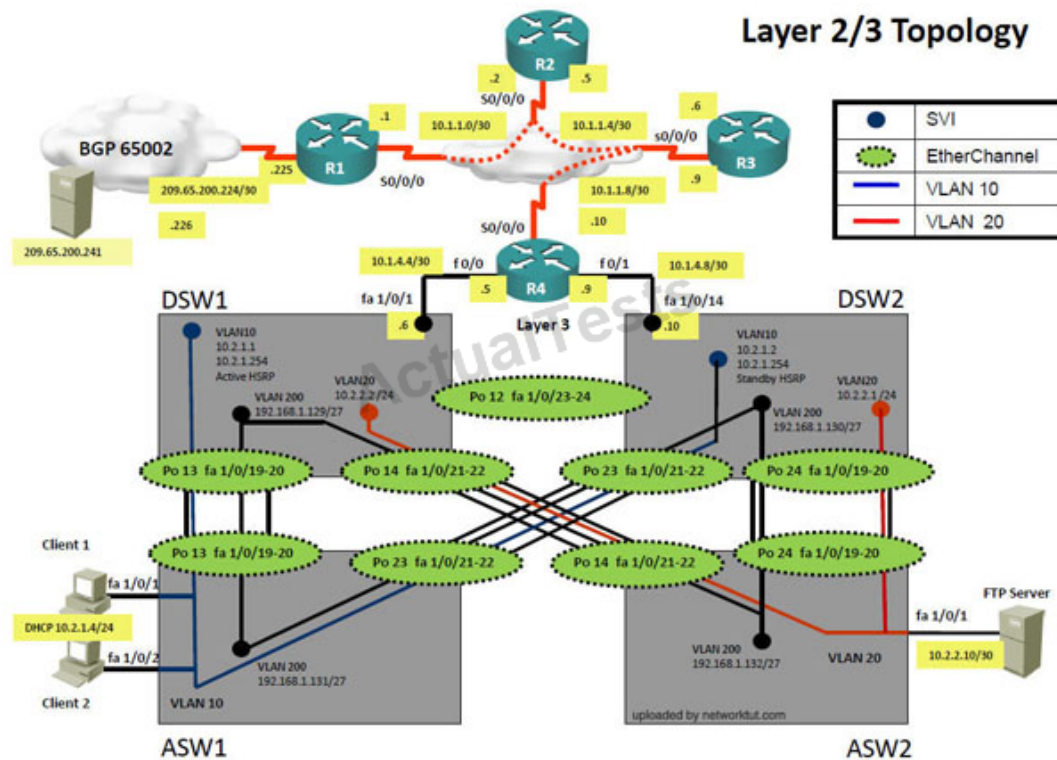
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

=====





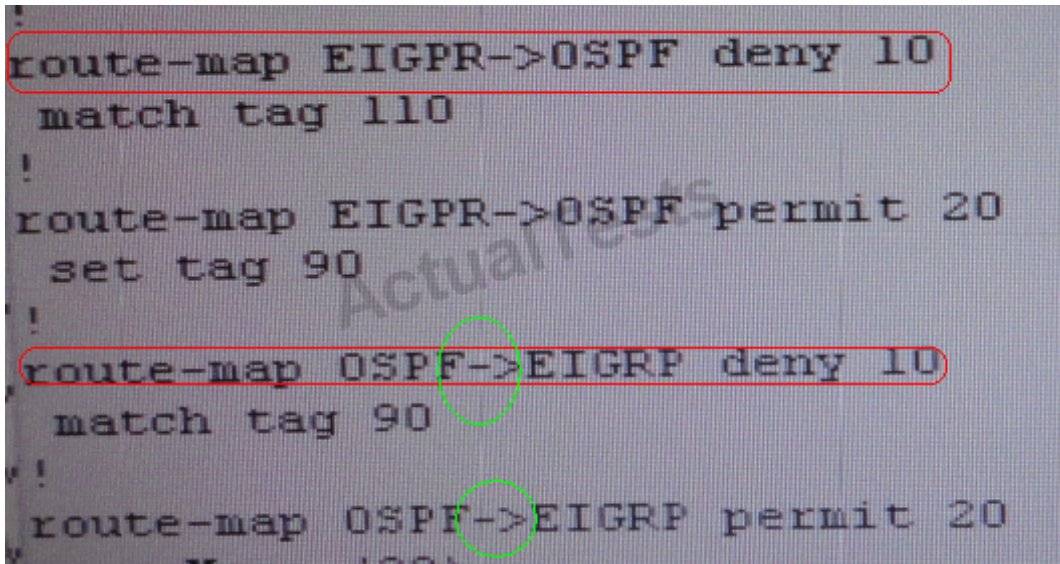
Client is unable to ping IP 209.65.200.241

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.

```
!
router eigrp 10
 redistribute ospf 1 route-map OSPF_to_EIGRP
 network 10.1.4.0 0.0.0.255
 network 10.1.10.0 0.0.0.255
 network 10.1.21.128 0.0.0.3
 default-metric 100000 100 100 1 1500
 auto-summary
!
router ospf 1
 log-adjacency-changes
 area 34 nssa
 summary-address 10.2.0.0 255.255.0.0
 redistribute eigrp 10 subnets route-map EIGRP->OSPF
 network 10.1.1.0 0.0.0.255 area 34
 network 10.1.2.0 0.0.0.255 area 34
```



```
!
route-map EIGRP->OSPF deny 10
  match tag 110
!
route-map EIGRP->OSPF permit 20
  set tag 90
!
route-map OSPF->EIGRP deny 10
  match tag 90
!
route-map OSPF->EIGRP permit 20
```

- 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 redistribution of EIGRP routing protocol, we need to change name of route-map to resolve the issue...
-

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 40

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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: D

Explanation:

QUESTION NO: 41

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:

QUESTION NO: 42

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.

Which is the solution to the fault condition?

- A.** Under the EIGRP process, delete the redistribute ospf 1 route-map OSPF_to_E IGRP command and enter the redistribute ospf 1 route-map OSPF -> E IGRP command.
- B.** Under the EIGRP process, delete the redistribute ospf 1 route-map OSPF_to_E IGRP command and enter the redistribute ospf 6 metric route-map OSPF -> E IGRP command.
- C.** Under the OSPF process, delete the redistribute eigrp10 subnets route-map EIGRP->OSPF command and enter the redistribute eigrp10 subnets route-map OSPF -> E IGRP command.
- D.** Under the OSPF process, delete the redistribute eigrp10 subnets route-map EIGRP->OSPF command and enter the redistribute eigrp10 subnets route-map EIGRP -> OSPF command.
- E.** Under the EIGRP process, delete the redistribute ospf 1 route-map OSPF_to_EIGRP command and enter redistribute ospf 1 metric 100000 100 100 1 15000 route_map OSPF_to_EIGRP command

Answer: A

Explanation:

=====

=====

Topic 11, Ticket 9 : EIGRP AS number

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. Redistribution 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.

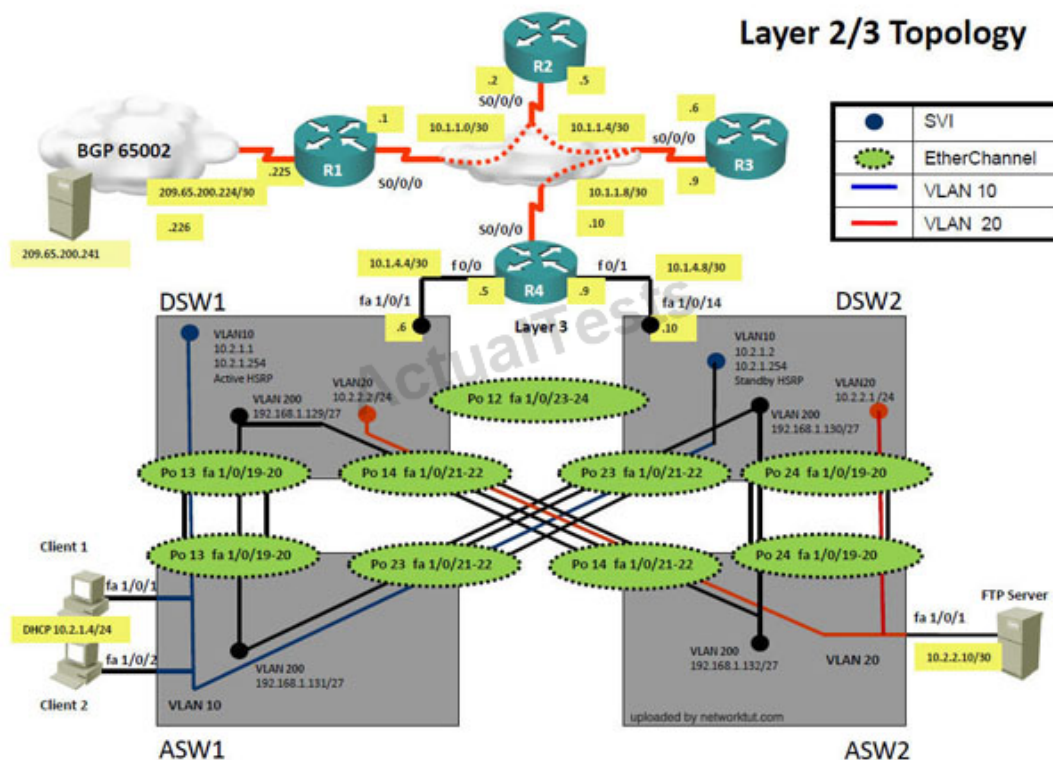
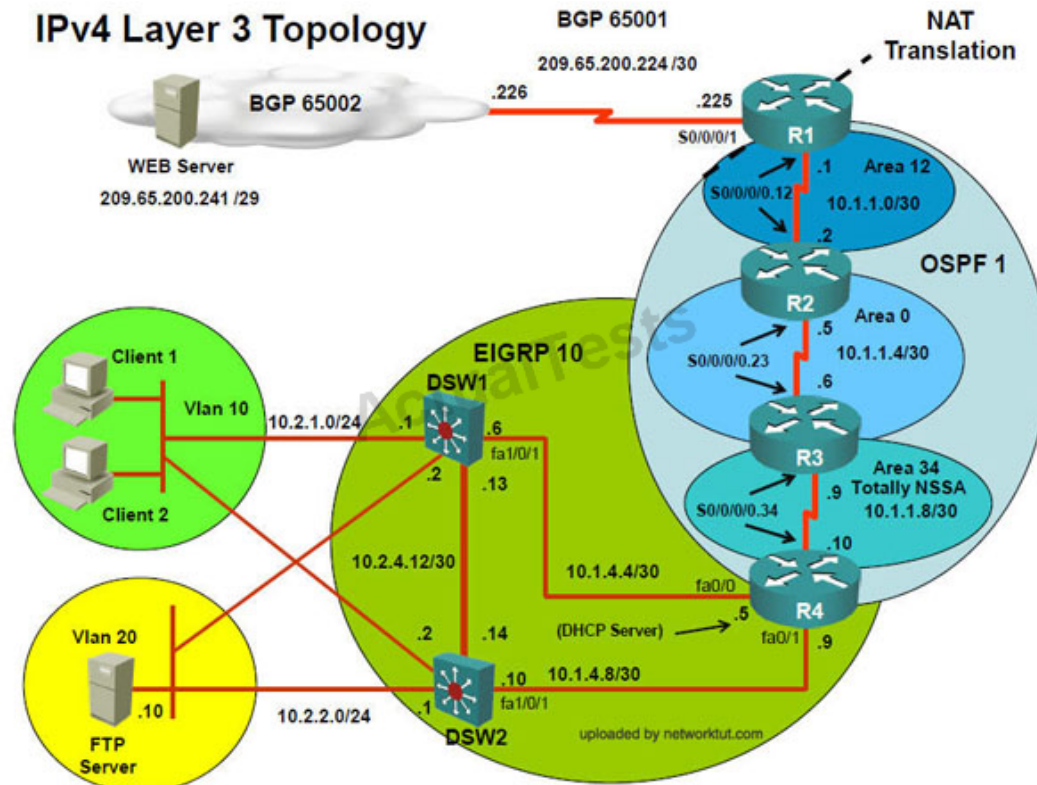
Question-1 Fault is found on which device,

Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====

=====



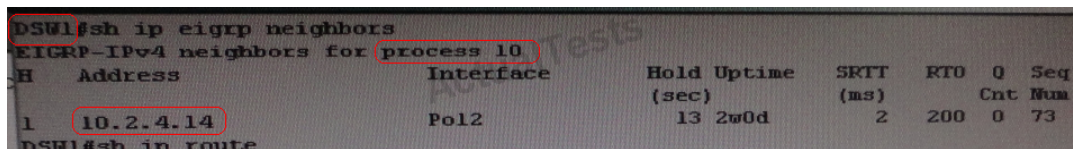
Client is unable to ping IP 209.65.200.241

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
- From Client PC we can ping 10.2.1.254
- But IP 10.2.1.3 is not able to ping from R4, R3, R2, R1
- This clearly shows problem at R4 Kindly check routes in EIGRP there are no routes of eigrp.
- Check the neighborship of EIGRP on R4; there are no neighbor seen from DSW1 & DSW2
check the running config of EIGRP protocol it shows EIGRP AS 1 process.... Now check on DSW1 & DSW2

On DSW1 only one Eigrp neighbour is there with DSW2 but its not with R4...



H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTT	Q	Seq Cnt	Num
1	10.2.4.14	Po12	13	2w0d	2	200	0	73	

- From above snapshot & since R4 has EIGRP AS number 1 due to which neighbour is not happening.
- **Change required:** On R4, IPV4 EIGRP Routing, need to change the EIGRP AS number from 1 to 10 since DSW1 & DSW2 is having EIGRP AS number 10

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 43

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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: D

Explanation:

QUESTION NO: 44

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: D

Explanation:

QUESTION NO: 45

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. Disable auto summary on the EIGRP process
- B. Enable EIGRP on the FastEthernet0/0 and FastEthernet0/1 interface using the no passive-interface command.
- C. Change the AS number on the EIGRP routing process from 1 to 10 to much the AS number used on DSW1 and DSW2.
- D. Under the EIGRP process, delete the network 10.1.4.0 0.0.0.255 command and enter the network 10.1.4.4 0.0.0.252 and 10.1.4.8 0.0.0.252 commands.

Answer: C

Explanation:

=====

=====

Topic 12, Ticket 10 : VLAN Access Map

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. Redistribution 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.

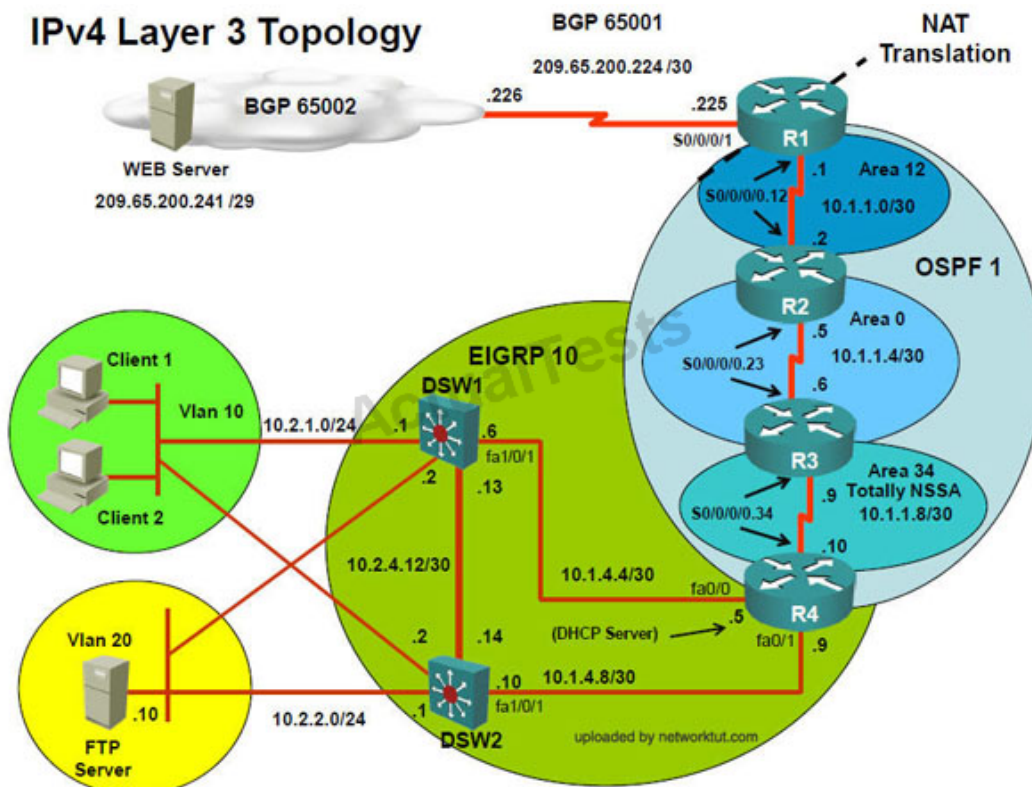
Each ticket has 3 sub questions that need to be answered & topology remains same.

Question-1 Fault is found on which device,

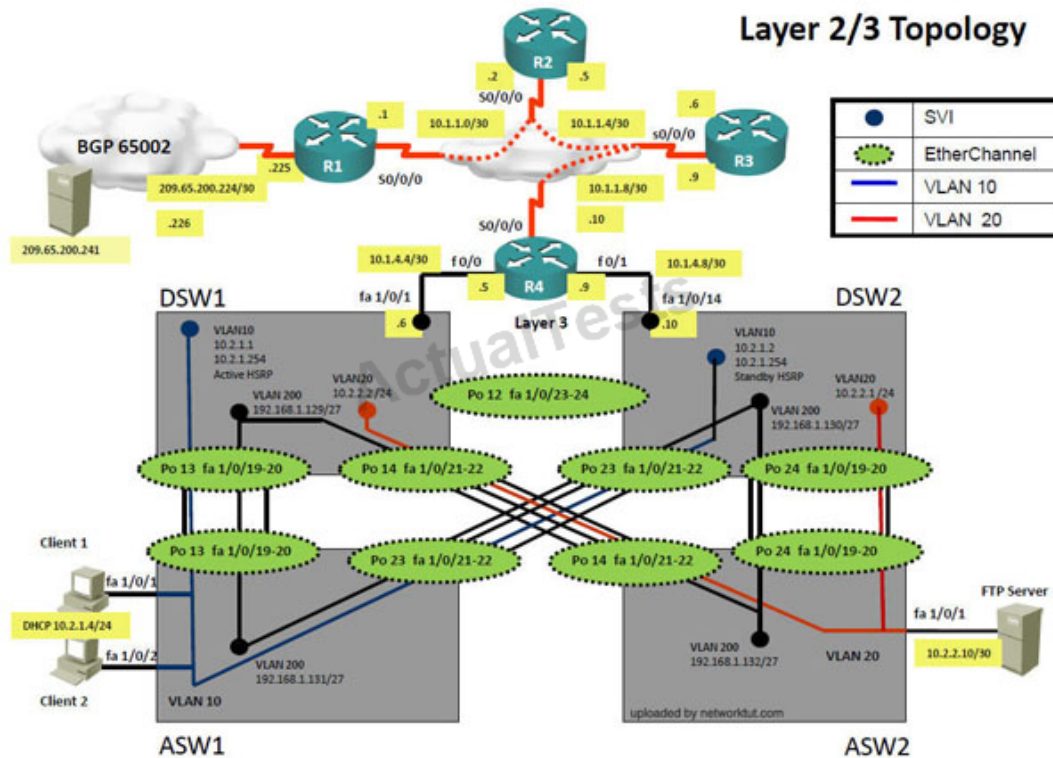
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

IPv4 Layer 3 Topology



Layer 2/3 Topology



Client 1 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
- From Client PC we can ping 10.2.1.254....
- But IP 10.2.1.3 is not able to ping from R4, R3, R2, R1

```
DSW1
vlan access-map test1 10
  action drop
  match ip address 10
vlan access-map test1 20
  action drop
  match ip address 20
vlan access-map test1 30
  action forward
  match ip address 30
vlan access-map test1 40
  action forward
!
vlan filter test1 vlan-list 10
vlan internal allocation policy ascending
```

```
!
access-list 10 permit 10.2.1.3
access-list 20 permit 10.2.1.4
access-list 30 permit 10.2.1.0 0.0.0.255
```

- **Change required:** On DSW1, VLAN ACL, Need to delete the VLAN access-map test1 whose action is to drop access-list 10 i.e 10.2.1.3

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 46

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.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: E

Explanation:

QUESTION NO: 47

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 Helper
- C. IPv4 EIGRP Routing
- D. IPv6 RIP Routing
- E. IPv4 layer 3 security
- F. Switch-to-Switch Connectivity
- G. Loop Prevention
- H. Access Vlan
- I. Port Security
- J. VLAN ACL / Port ACL
- K. Switch Virtual Interface

Answer: J

Explanation:

QUESTION NO: 48

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. Under the global configuration mode enter no access-list 10 command.
- B. Under the global configuration mode enter no access-map vlan 10 command.
- C. Under the global configuration mode enter no vlan access-map test1 10 command.
- D. Under the global configuration mode enter no vlan filter test1 vlan-list 10 command.

Answer: C

Explanation:

Topic 13, Ticket 11 : IPV6 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. Redistribution 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,

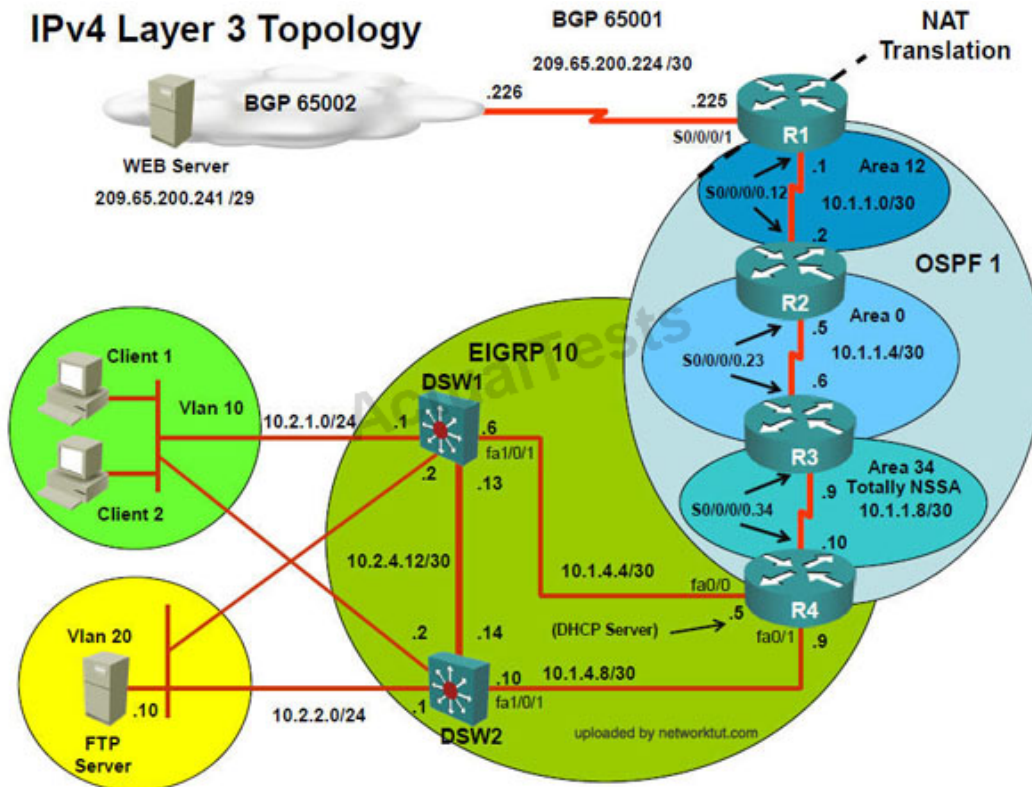
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

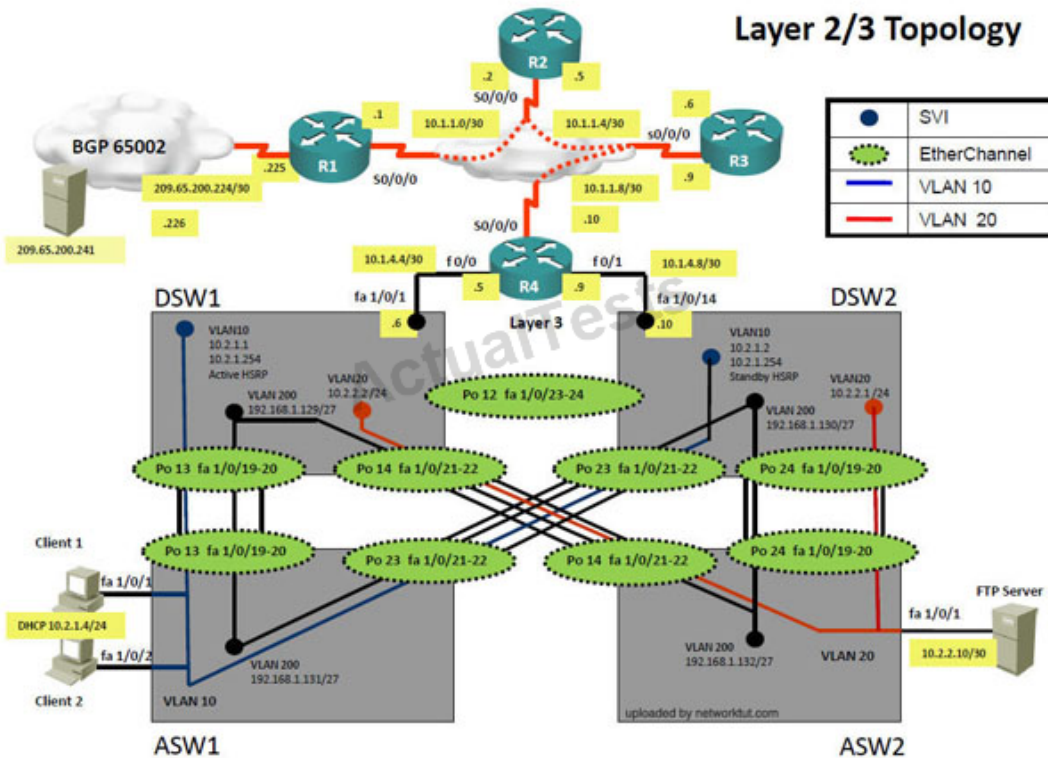
=====

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



Issues

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).

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
- From Client PC we can ping 10.2.1.254....
- But IP 10.2.1.3 is able to ping from R4, R3, R2, R1.
- Since the problem is R1 (2026::111:1) is not able to ping loopback of DSW1 (2026::102:1).
- Kindly check for neighbourship of routers as IPV6.... As per design below neighbourship should be present for IPV6
R1 ---R2 --- R3 --- R4--- DSW1 & DSW2 ----- Neighbourship between devices of IPV6

```
R2#sh ipv6 ospf nei
Neighbor ID      Pri   State   Dead Time   Interface ID  Interface
10.1.10.1        1    FULL/  -           00:00:32     6          Serial0/0/0.12
R2#
```

R2 IPV6 OSPF neighbourship is with R1

```
R3>sh ipv6 ospf ne
R3>sh ipv6 ospf neighbor
Neighbor ID      Pri   State   Dead Time   Interface ID  Interface
10.1.21.129      1    FULL/  -           00:00:31     15         Tunnel134
R3>
```

R3 IPV6 OSPF neighbourship is with R4

```
interface Serial0/0/0.23 point-to-point
description Link to R3
ip address 10.1.1.5 255.255.255.252
ipv6 address 2026::1:1/123
frame-relay interface-dlci 302
!
```

```
!
interface Serial0/0/0.23 point-to-point
ip address 10.1.1.6 255.255.255.252
ipv6 address 2026::1:2/122
ipv6 ospf 6 area 0
frame-relay interface-dlci 203
!
```

- As per above snapshot we cannot see IPV6 neighbourship between R2 & R3 when checked interface configuration ipv6 ospf area 0 is missing on R2 which is connected to R3
- **Change required:** On R2, IPV6 OSPF routing, Configuration is required ipv6 ospf 6 area 0 under interface

serial 0/0/0.23

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 49

The implementations group has been using the test bed to do a 'proof-of-concept'. After several changes to the network addressing, 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).

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

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: B

Explanation:

QUESTION NO: 50

The implementations group has been using the test bed to do a 'proof-of-concept'. After several changes to the network addressing, 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).

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. IPv4 OSPF Routing
- C. IPv6 OSPF Routing
- D. IPv4 layer 3 security

Answer: C

Explanation:

QUESTION NO: 51

The implementations group has been using the test bed to do a 'proof-of-concept'. After several changes to the network addressing, 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).

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

What is the solution to fault condition?

- A. Under the interface Serial 0/0/0.23 configuration enter the ipv6 ospf 6 area 0 command.
- B. Under the interface Serial0/0/0.12 configuration enter the ipv6 ospf 6 area 12 command.
- C. Under ipv6 router ospf 6 configuration enter the network 2026::1:/122 area 0 command.
- D. Under ipv6 router ospf 6 configuration enter no passive-interface default command.

Answer: A

Explanation:

=====

=====

Topic 14, Ticket 12 : HSRP Issue

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. Redistribution 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.

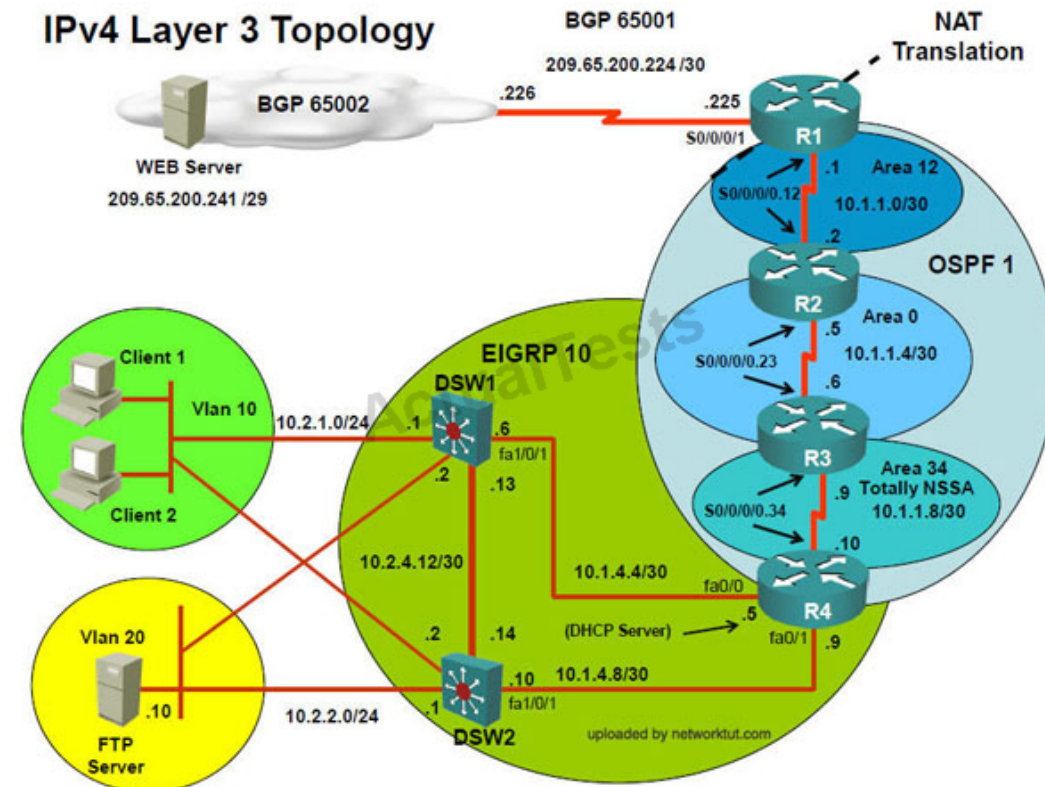
Each ticket has 3 sub questions that need to be answered & topology remains same.

Question-1 Fault is found on which device,

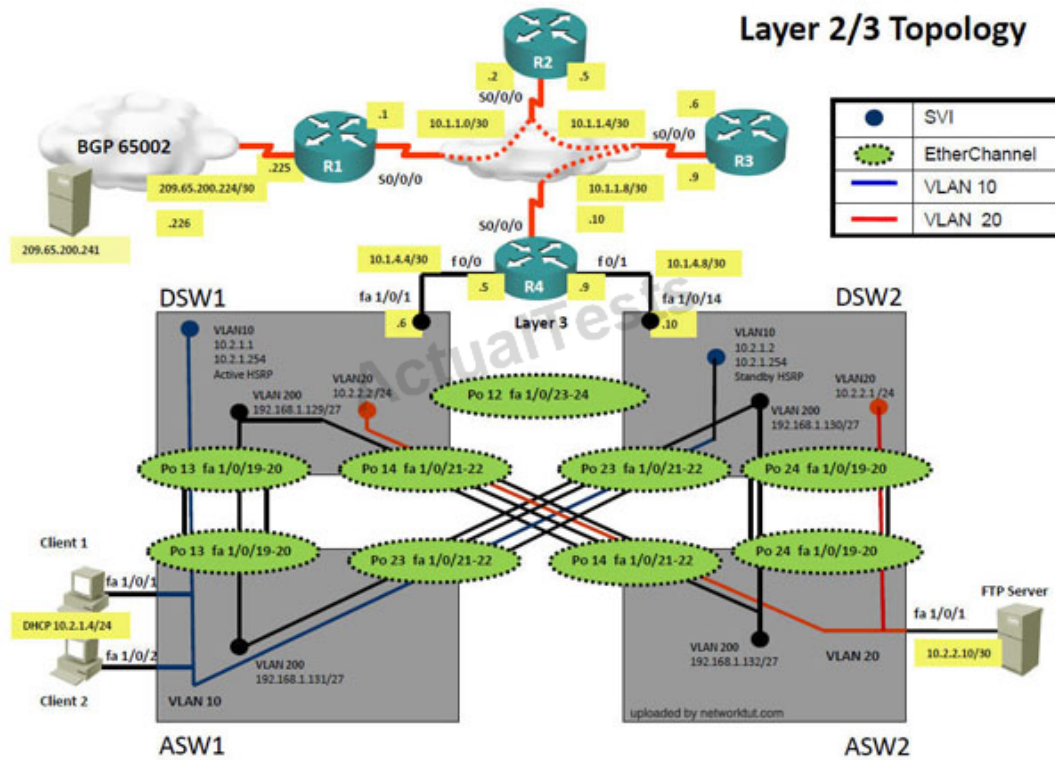
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

=====



Layer 2/3 Topology



The implementation 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 schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened indicating DSW1 will not become the active router for HSRP group 10.

Solution

Steps need to follow as below:-

- Since the problem is raised that DSW1 will not become active router for HSRP group 10
- we will check for the HSRP configuration...

DSW1

```
track 1 ip route 10.2.21.128 255.255.255.224 metric threshold
threshold metric up 1 down 2
track 10 ip route 10.1.21.128 255.255.255.224 metric threshold
threshold metric up 61 down 62
no ip subnet-zero
ip routing
```

```
!
interface Vlan10
 ip address 10.2.1.1 255.255.255.0
 ip helper-address 10.1.21.129
 standby 10 ip 10.2.1.254
 standby 10 priority 200
 standby 10 preempt
 standby 10 track 1 decrement 60
```

DSW2

```
!
interface Vlan10
 ip address 10.2.1.2 255.255.255.0
 ip helper-address 10.1.21.129
 standby 10 ip 10.2.1.254
 standby 10 priority 150
 standby 10 preempt
!
```

- From snapshot we see that the track command given needs to be changed under active VLAN10 router
- **Change Required:** On DSW1, related to HSRP, under vlan 10 change the given track 1 command. & use track 10 command.

So in ticket Answer to the fault condition will be as below for

QUESTION NO: 52

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 schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened DSW1 will not become the active router for HSRP group 10.

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

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: E

Explanation:

QUESTION NO: 53

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 schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened DSW1 will not become the active router for HSRP group 10.

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. HSRP
- C. IP DHCP Helper
- D. IPv4 EIGRP Routing
- E. IPv6 RIP Routing
- F. IPv4 layer 3 security
- G. Switch-to-Switch Connectivity
- H. Loop Prevention
- I. Access Vlans

Answer: B

Explanation:

QUESTION NO: 54

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 schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and device security, a trouble ticket has been opened DSW1 will not become the active router for HSRP group 10.

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.** Under the interface vlan 10 configuration enter standby 10 preempt command.
- B.** Under the track 1 object configuration delete the threshold metric up 1 down 2 command and enter the threshold metric up 61 down 62 command.
- C.** Under the track 10 object configuration delete the threshold metric up 61 down 62 command and enter the threshold metric up 1 down 2 command.
- D.** Under the interface vlan 10 configuration delete the standby 10 track1 decrement 60 command and enter the standby 10 track 10 decrement 60 command.

Answer: D

Explanation:

Topic 15, Ticket 13 : DHCP Issue
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. Redistribution 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,

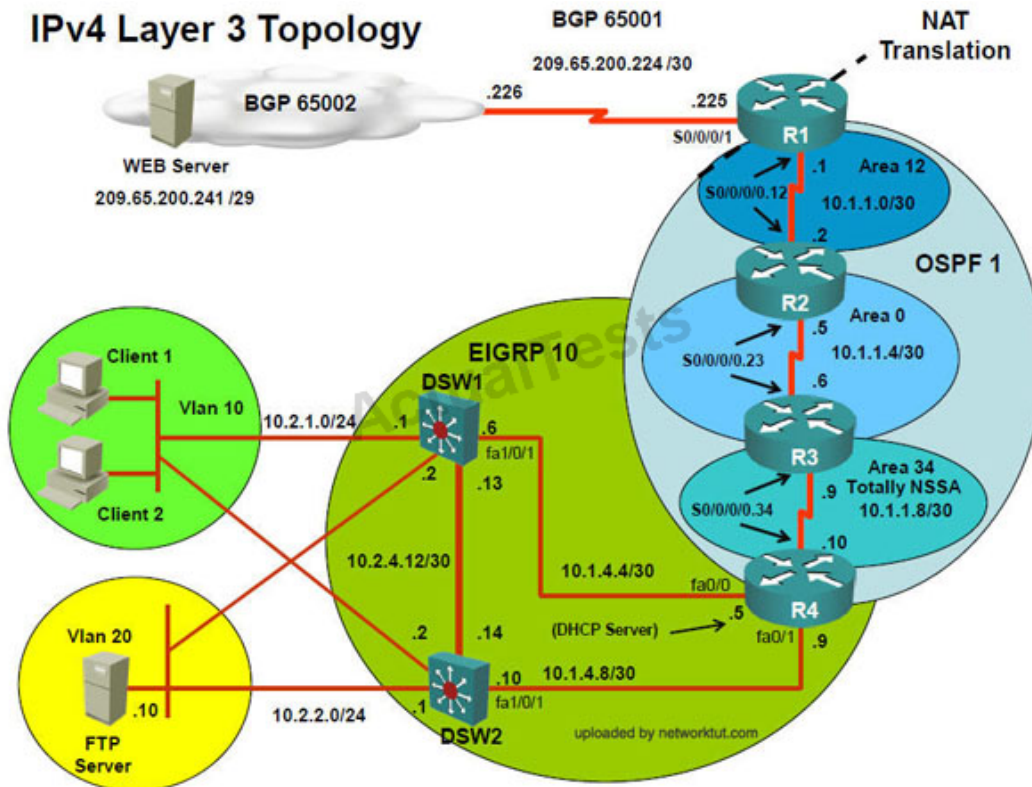
Question-2 Fault condition is related to,

Question-3 What exact problem is seen & what needs to be done for solution

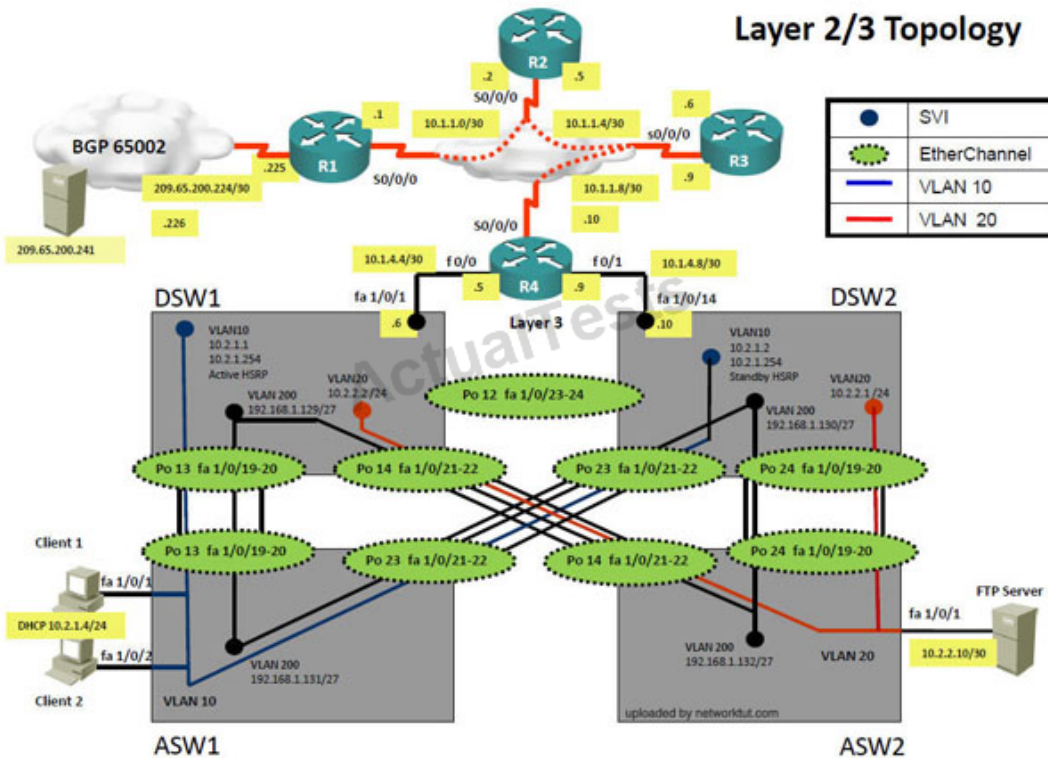
=====

=====

IPv4 Layer 3 Topology



Layer 2/3 Topology



The implementation 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 schemes, DHCP services, NTP services, layer 2 connectivity, FHRP services, and, device security, a trouble ticket has been opened indicating DSW1 will not become the active router for HSRP group 10.

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 Private IP address 169.254.X.X
- From ASW1 we can ping 10.2.1.254....
- On ASW1 VLAN10 is allowed in trunk & access command will is enabled on interface but DHCP IP address is not recd.

On R4 DHCP ip address is not allowed for network 10.2.1.0/24 which clearly shows the problem lies on R4 & the problem is of DHCP

QUESTION NO: 55

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 schemes, 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 isolate the cause of this fault and answer the following question.

On which device is the fault condition located?

- A. R1
- B. R2
- C. R3
- D. R4
- E. DSW1
- F. DSW2
- G. ASW1
- H. ASW2

Answer: D

Explanation:

QUESTION NO: 56

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 schemes, 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 isolate the cause of this fault and answer the following question.

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: B

Explanation:

QUESTION NO: 57

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 schemes, 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 isolate the cause of this fault and answer the following question.

What is the solution to the fault condition?

- A. Under the global configuration, delete the no ip dhcp use vrf connected command.
- B. Under the IP DHCP pool configuration, delete the default -router 10.2.1.254 command and enter the default-router 10.1.4.5 command.
- C. Under the IP DHCP pool configuration, delete the network 10.2.1.0 255.255.255.0 command and enter the network 10.1.4.0 255.255.255.0 command.
- D. Under the IP DHCP pool configuration, issue the no ip dhcp excluded-address 10.2.1.1 10.2.1.253 command and enter the ip dhcp excluded-address 10.2.1.1 10.2.1.2 command.

Answer: D

Explanation:

