Vendor: Cisco

Exam Code: 300-135

Exam Name: Troubleshooting and Maintaining Cisco IP Networks (TSHOOT v2.0)

Version: DEMO

QUESTION 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 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:

```
LevelLevel NameDescription
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 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: BD
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 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
```

D.
```
ntp server 10.1.1.1 fallback
ntp server 10.1.1.2
```

Answer: C
Explanation:
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 5
A network administrator is troubleshooting an EIGRP connection between RouterA, IP address 10.1.2.1, and RouterB, IP address 10.1.2.2. Given the debug output on RouterA, which two statements are true? (Choose two.)

```
RouterA# debug eigrp packets
...
01:39:13:  EIGRP: Received HELLO on Serial0/0 nbr 10.1.2.2
01:39:13: AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0 peerQ un/rely 0/0
01:39:13:           K-value mismatch
```

A. RouterA received a hello packet with mismatched autonomous system numbers.
B. RouterA received a hello packet with mismatched hello timers.
C. RouterA received a hello packet with mismatched authentication parameters.
D. RouterA received a hello packet with mismatched metric-calculation mechanisms.
E. RouterA will form an adjacency with RouterB.
F. RouterA will not form an adjacency with RouterB.

Answer: DF

QUESTION 6
Refer to the exhibit. How would you confirm on R1 that load balancing is actually occurring on the default- network (0.0.0.0)?

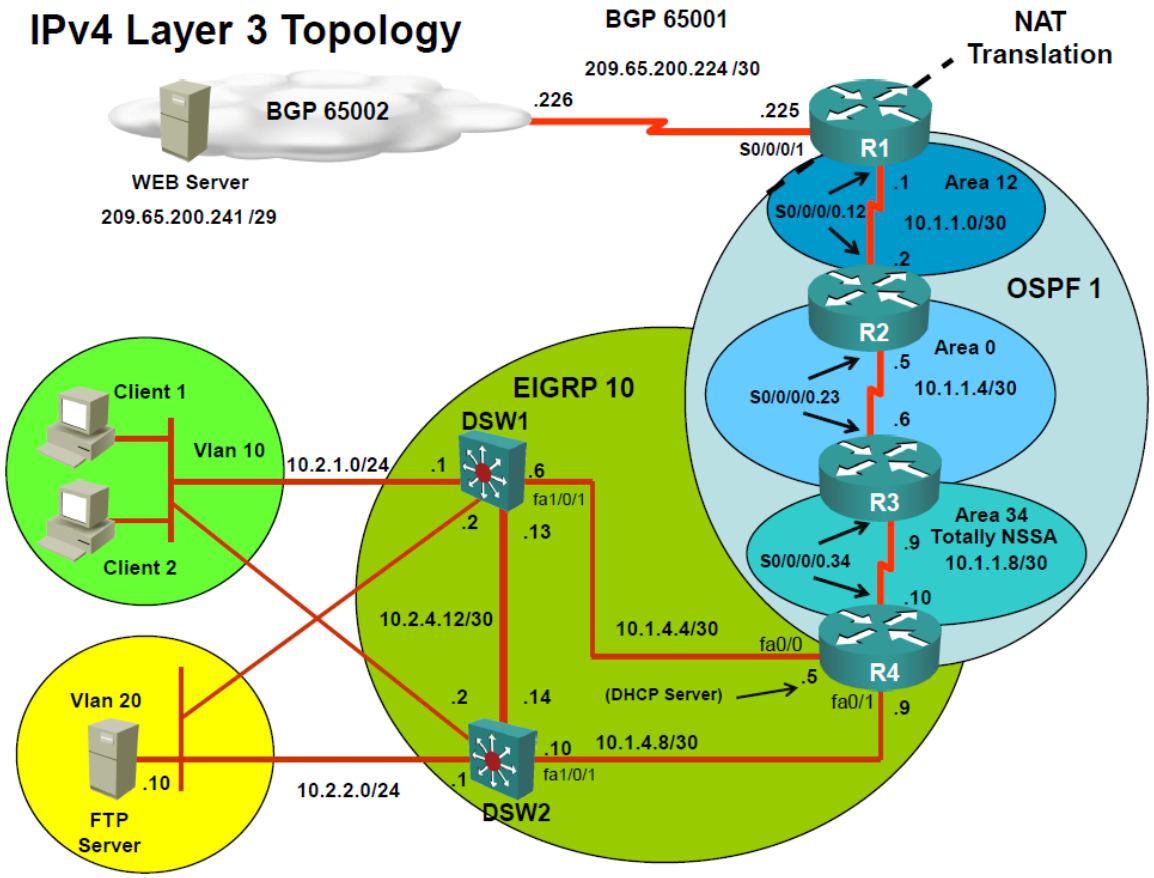
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 212.50.185.126 to network 0.0.0.0

D    212.50.167.0/24 [90/160000] via 212.50.185.82, 00:05:55, Ethernet1/0
     212.50.166.0/24 is variably subnetted, 4 subnets, 2 masks
D       212.50.166.0/24 is a summary, 00:05:55, Null0
C       212.50.166.1/32 is directly connected, Loopback1
C       212.50.166.2/32 is directly connected, Loopback2
C       212.50.166.20/32 is directly connected, Loopback20
     212.50.185.0/27 is subnetted, 3 subnets
C       212.50.185.64 is directly connected, Ethernet1/0
C       212.50.185.96 is directly connected, Ethernet0/0
C       212.50.185.32 is directly connected, Ethernet2/0
D*EX 0.0.0.0/0 [170/2174976] via 212.50.185.126, 00:05:55, Ethernet0/0
               [170/2174976] via 212.50.185.125, 00:05:55, Ethernet0/0
!
```

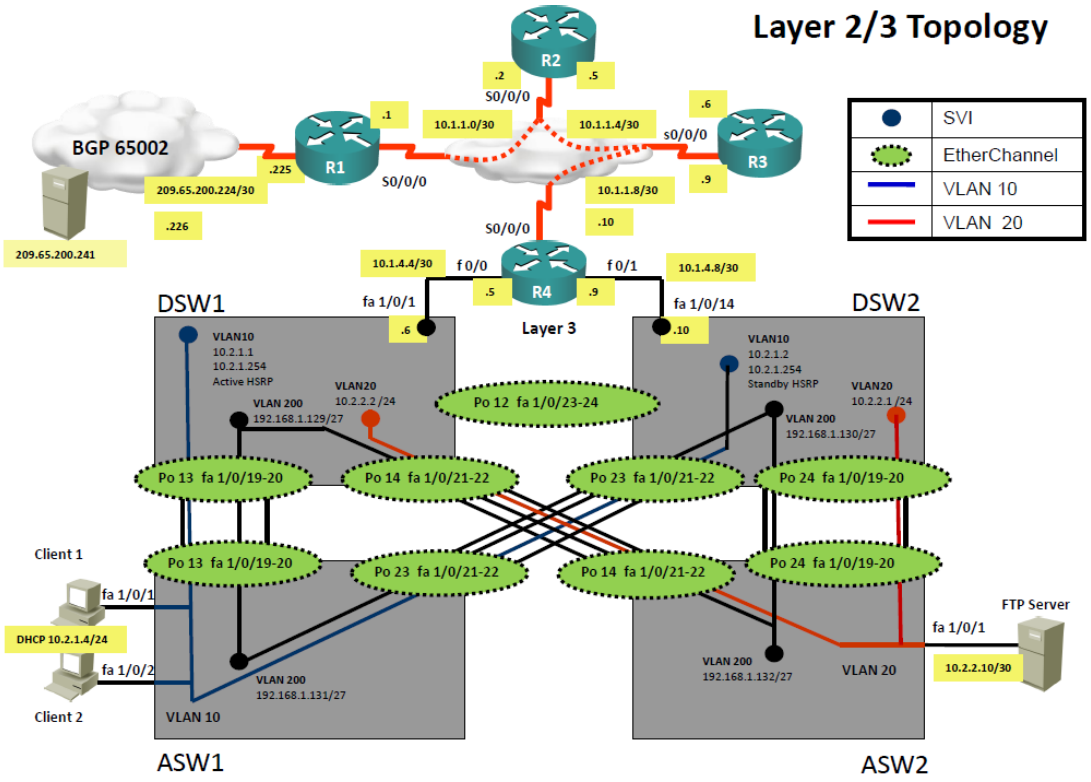
A. Use ping and the show ip route command to confirm the timers for each default network resets to 0.
B. Load balancing does not occur over default networks; the second route will only be used for failover.
C. Use an extended ping along with repeated show ip route commands to confirm the gateway of last resort address toggles back and forth.
D. Use the traceroute command to an address that is not explicitly in the routing table.

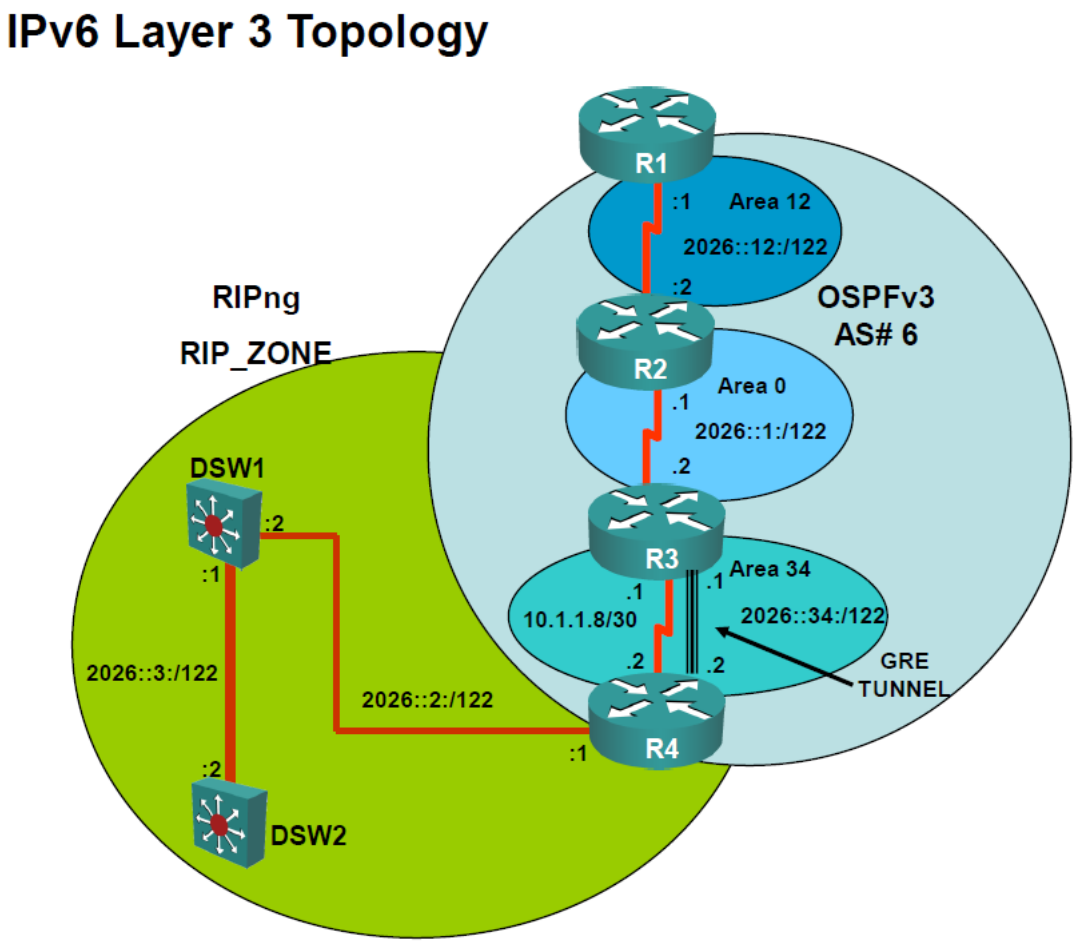
Answer: D

Trouble Ticket (16 TT Questions and Answers)

See the Topology, complete those 16 TT questions.


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


Layer 2/3 Topology
R2
.2
.5
S0/0/0
BGP 65002
.1
10.1.1.0/30
10.1.1.4/30
.6
S0/0/0
R1
R3
.225
S0/0/0
.9
209.65.200.224/30
10.1.1.8/30
.226
.10
S0/0/0
209.65.200.241
10.1.4.4/30
f 0/0
R4
f 0/1
10.1.4.8/30
.5
.9
DSW1
fa 1/0/1
.6
Layer 3
fa 1/0/14
.10
DSW2
VLAN10
10.2.1.1
10.2.1.254
Active HSRP
VLAN20
10.2.2.2 /24
VLAN 200
192.168.1.129/27
Po 12 fa 1/0/23-24
VLAN10
10.2.1.2
10.2.1.254
Standby HSRP
VLAN20
10.2.2.1/24
VLAN 200
192.168.1.130/27
Po 13 fa 1/0/19-20
Po 14 fa 1/0/21-22
Po 23 fa 1/0/21-22
Po 24 fa 1/0/19-20
Client 1
Po 13 fa 1/0/19-20
Po 23 fa 1/0/21-22
Po 14 fa 1/0/21-22
Po 24 fa 1/0/19-20
FTP Server
fa 1/0/1
DHCP 10.2.1.4/24
fa 1/0/2
VLAN 200
192.168.1.131/27
VLAN 200
192.168.1.132/27
VLAN 20
10.2.2.10/30
Client 2
VLAN 10
ASW1
ASW2
SVI
EtherChannel
VLAN 10
VLAN 20



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

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

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

```
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for
solution
```

Client is unable to ping IP 209.65.200.241

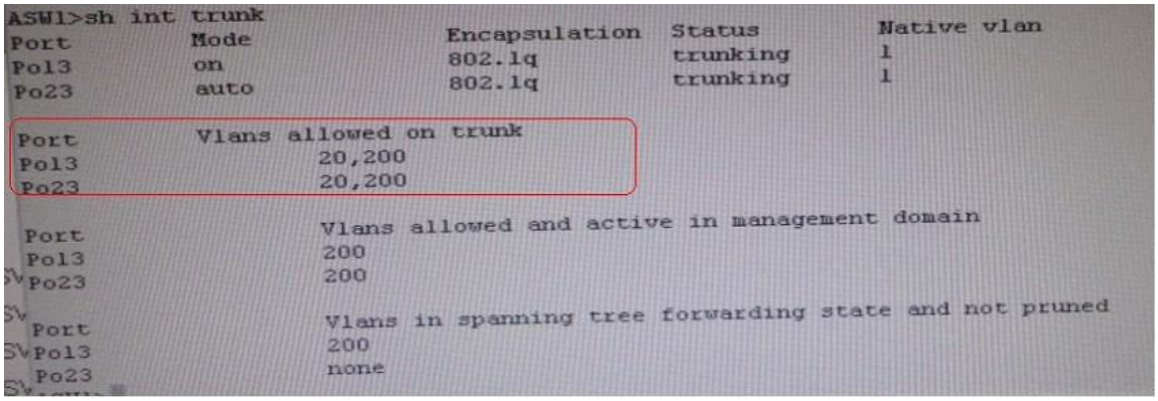
Solution:
Steps need to follow as below:

- When we check on client 1 & Client 2 desktop we are not receiving DHCP address from R4 Ipconfig ----- Client will be getting 169.X.X.X

- On ASW1 port Fa1/0/ 1 & Fa1/0/2 access port VLAN 10 was assigned which is using IP address 10.2.1.0/24
Sh run ------- & check for running config of int fa1/0/1 & fa1/0/2

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



- 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 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 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 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.