Vendor: Cisco

Exam Code: 642-832

Exam Name: Troubleshooting and maintaing cisco ip networks

Version: Demo

Question Set 1

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

Correct Answer: D
Explanation

Explanation/Reference:
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

Correct Answer: D
Explanation

Explanation/Reference:
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

Correct Answer: BD
Explanation

Explanation/Reference:
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

References:

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 10.1.1.1ntp server 10.1.1.2
B. ntp server 10.1.1.1ntp server 10.1.1.2 primary
C. ntp server 10.1.1.1ntp server 10.1.1.2 prefer
D. ntp server 10.1.1.1 fallbackntp server 10.1.1.2

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

Preferred server
A router can be configured to prefer an NTP source over another. A preferred server's responses are discarded only if they vary dramatically from the other time sources. Otherwise,
the preferred server is used for synchronization without consideration of the other time sources. Preferred servers are usually specified when they are known to be extremely accurate.
To specify a preferred server, use the prefer keyword appended to the ntp server command. The following example tells the router to prefer TimeServerOne over TimeServerTwo:
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ntp server TimeServerOne prefer
Router(config)#ntp server TimeServerTwo
Router(config)#^Z

QUESTION 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

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

Cisco routers 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, 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 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

Correct Answer: BD

Explanation

Explanation/Reference:
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.
References:

QUESTION 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 a 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

Correct Answer: D
Explanation

Explanation/Reference:
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.
References:

QUESTION 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

Correct Answer: ACE
Explanation

Explanation/Reference:
Explanation:

The FCAPS maintenance model consists of the following:
FCAPS Maintenance Tasks:

QUESTION 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

Correct Answer: ABD
Explanation

Explanation/Reference:
Explanation:

QUESTION 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.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

QUESTION 11
Refer to the shown below.

%LINK-3-UPDOWN: Interface Serial0/0, changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up

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.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

QUESTION 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.

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:

QUESTION 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.

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

QUESTION 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

Correct Answer: B
Explanation

Explanation/Reference:
Explanation:

QUESTION 15
What are two approaches to maintaining a network?(Choose two.)

A. PPDIOO
B. structured
C. bottoms up
D. interrupt-driven

Correct Answer: BD
Explanation

Explanation/Reference:

Explanation:

QUESTION 16
Refer to the graphic above.

```
ip ftp username backup
ip ftp password san-fran
```

Which command sequences, shown below, would accomplish the same task as that shown in the graphic?

A)

```
ip http client username backup
ip http client password 0 san-fran
```

B)

```
ip tftp username backup
ip tftp password san-fran
```

C)

```
ip scp username backup
ip scp password san-fran
```

D)

```
ip stp username backup
ip stp password san-fran
```

A. Exhibit A
B. Exhibit B
C. Exhibit C
D. Exhibit D

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

QUESTION 17
Which two statements about the Cisco Aironet Desktop Utility (ADU) are true? (Select two)

A. The Aironet Desktop Utility (ADU) profile manager feature can create and manage only one profile for the wireless client adapter.
B. The Aironet Desktop Utility (ADU) can support only one wireless client adapter installed and used at a time.
C. The Aironet Desktop Utility (ADU) can be used to establish the association between the client adapter and the access point, manage authentication to the wireless network, and enable encryption.

D. The Aironet Desktop Utility (ADU) and the Microsoft Wireless Configuration Manager can be used at the same time to configure the wireless client adapter.

Correct Answer: BC
Explanation

Explanation/Reference:
Explanation:

You can configure your Cisco Aironet Wireless LAN Client Adapter through the Cisco ADU or a third-party tool, such as the Microsoft Wireless Configuration Manager. Because third-party tools may not provide all the functionality available in ADU, Cisco recommends that you use ADU. The Aironet Desktop Utility (ADU) can support only one wireless client adapter as well as Aironet Desktop Utility establish the association between the client adapter and Access Point, allows to authenticate wireless client, allows to configure encryption by setting static WEP, WPA/WPA2 passphrase.

QUESTION 18
At which layer of the OSI model does the Spanning Tree Protocol (STP) operate at?

A. Layer 5
B. Layer 4
C. Layer 3
D. Layer 2
E. Layer 1

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

Spanning-Tree Protocol (STP) is a Layer 2 (L2) protocol designed to run on bridges and switches. The specification for STP is called 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. Loops are deadly to a network.

QUESTION 19
In computer networking a multicast address is an identifier for a group of hosts that have joined a multicast group. Multicast addressing can be used in the Link Layer (OSI Layer 2), such as Ethernet Multicast, as well as at the Internet Layer (OSI Layer 3) as IPv4 or IPv6 Multicast. Which two descriptions are correct regarding multicast addressing?

A. The first 23 bits of the multicast MAC address are 0x01-00-5E. This is a reserved value that indicates a multicast application.
B. The last 3 bytes (24 bits) of the multicast MAC address are 0x01-00-5E. This is a reserved value that indicates a multicast application.
C. To calculate the Layer 2 multicast address, the host maps the last 23 bits of the IP address into the last 24 bits of the MAC address. The high-order bit is set to 0.
D. The first 3 bytes (24 bits) of the multicast MAC address are 0x01-00-5E. This is a reserved value that indicates a multicast application.

Correct Answer: CD
Explanation

Explanation/Reference:
Explanation:
The point of this question is the form of multicast MAC address, and the conversion between the multicast MAC address and IP address.

The multicast MAC address is 6 bytes(48 bits), the first 3 bytes (24 bits) of the multicast MAC address are 0x01-00-5E, the last 3 bytes(24 bits) of the multicast MAC address =0 + 23 bit(the last 23 bit of the IP

address). "0x01-00-5E" is a reserved value that indicates a multicast application.

QUESTION 20
EIGRP is being used as the routing protocol on the Company network. While troubleshooting some network connectivity issues, you notice a large number of EIGRP SIA (Stuck in Active) messages. What causes these SIA routes? (Select two)

A. The neighboring router stops receiving ACK packets from this router.
B. The neighboring router starts receiving route updates from this router.
C. The neighboring router is too busy to answer the query (generally caused by high CPU utilization).
D. The neighboring router is having memory problems and cannot allocate the memory to process the query or build the reply packet.

Correct Answer: CD
Explanation

Explanation/Reference:
Explanation:

SIA routes are due to the fact that reply packets are not received. This could be caused by a router which is unable to send reply packets. The router could have reached the limit of its capacity, or it could be malfunctioning.
Incorrect Answers
A:Missing replies, not missing ACKs, cause SIA.
B:Routes updates do not cause SIA.
Notes: If a router does not receive a reply to all outstanding queries within 3 minutes, the route goes to the stuck in active (SIA) state. The router then resets the neighbors that fail to reply by going active on all routes known through that neighbor, and it re-advertises all routes to that neighbor.
References:

QUESTION 21
You want to enhance the security within the Company LAN and prevent VLAN hopping. What two steps can be taken to help prevent this? (Select two)

A. Enable BPD guard
B. Disable CDP on ports where it is not necessary
C. Place unused ports in a common unrouted VLAN
D. Prevent automatic trunk configuration
E. Implement port security

Correct Answer: CD
Explanation

Explanation/Reference:
Explanation:

To prevent VLAN hoping you should disable unused ports and put them in an unused VLAN, or a separate unrouted VLAN. By not granting connectivity or by placing a device into a VLAN not in use, unauthorized access can be thwarted through fundamental physical and logical barriers. Another method used to prevent VLAN hopping is to prevent automatic trunk configuration. Hackers used 802.1Q and ISL tagging attacks, which are malicious schemes that allow a user on a VLAN to get unauthorized access to another VLAN. For example, if a switch port were configured as DTP auto and were to receive a fake DTP packet, it might become a trunk port and it might start accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port.
References:

QUESTION 22
The Company network is being flooded with invalid Layer 2 addresses, causing switch CAM tables to be filled and forcing unicast traffic to be transmitted out all switch ports. Which type of Layer 2 attack is being used here?

A. MAC spoofing
B. VLAN hopping
C. MAC address flooding
D. DHCP flooding
E. Session hijacking

Correct Answer: C
Explanation

Explanation/Reference:
Explanation:
Port security is especially useful in the face of MAC address flooding attacks. In these attacks, an attacker tries to fill up a switch's CAM tables by sending a large number of frames to it with source MAC addresses that the switch is unaware of at that time. The switch learns about these MAC addresses and puts them in its CAM table, thinking that these MAC addresses actually exist on the port on which it is receiving them. In reality, this port is under the attacker's control and a machine connected to this port is being used to send frames with spoofed MAC addresses to the switch. If the attacker keeps sending these frames in a large-enough quantity, and the switch continues to learn of them, eventually the switch's CAM table becomes filled with entries for these bogus MAC addresses mapped to the compromised port.
Under normal operations, when a machine receiving a frame responds to it, the switch learns that the MAC address associated with that machine sits on the port on which it has received the response frame. It puts this mapping in its CAM table, allowing it to send any future frames destined for this MAC address directly to this port rather than flood all the ports on the VLAN. However, in a situation where the CAM table is filled up, the switch is unable to create this CAM entry. At this point, when the switch receives a legitimate frame for which it does not know which port to forward the frame to, the switch floods all the connected ports belonging to the VLAN on which it has received the frame. The switch continues to flood the frames with destination addresses that do not have an entry in the CAM tables to all the ports on the VLAN associated with the port it is receiving the frame on.
References:

QUESTION 23
A MAC address flood attack is occurring on the Company LAN. During this attack, numerous frames are forwarded to a switch which causes the CAM table to fill to capacity. How does this action benefit the attacker?

A. All traffic is tagged with a specific VLAN ID from the VLAN of the attacker and is now viewable.
B. Clients will forward packets to the attacking device, which will in turn send them to the desired destination but not before recording the traffic patterns.
C. All traffic is redirected to the VLAN that the attacker used to flood the CAM table.
D. All traffic is flooded out all ports and an attacker is able to capture all data.
E. None of the other alternatives apply

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

MAC flooding basically involves bombarding the switch with spoofed ARP requests in the hope of making the switch "fail open". This, in essence, makes the switch display the characteristics of a hub, where it sends packets to all ports. A MAC flooding attack looks like traffic from thousands or computers moving into one port, but it's actually the attacker spoofing the MAC address of thousands of non-existent hosts. The goal is to flood the switches CAM (content addressable memory) table, or port/MAC table with these bogus requests, and once flooded, the switch will broadcast openly onto a LAN, allowing the attacker to start sniffing. The success of this attack is almost completely dependant on the model and manufacturer of the switch.
References:

QUESTION 24
Which of the following characteristics describe the BPDU Guard feature? (Choose all that apply.)

A. A BPDU Guard port should only be configured on ports with PortFast enabled.
B. BPDU Guard and PortFast should not be enabled on the same port.
C. BPDU Guard is used to ensure that superior BPDUs are not received on a switch port.
D. A BPDU Guard port receiving a BPDU will go into err-disable state.
E. A BPDU Guard port receiving a BPDU will be disabled.
F. BPDU Guard can be enabled on any switch port.

Correct Answer: AE
Explanation

Explanation/Reference:
Explanation:

QUESTION 25
Which of the following are valid modes of accessing the data plane? (Choose all that apply.)

A. Serial connection
B. Secure Shell
C. RADIUS
D. Simple Network Management Protocol
E. HTTP
F. Telnet

Correct Answer: ABDEF
Explanation

Explanation/Reference:
Explanation:

QUESTION 26
Which of the following is not an essential prerequisite for AutoQoS to be correctly applied to an interface? (Choose all that apply.)

A. The interface must be configured as a Multilink PPP interface.
B. The correct bandwidth should be configured on the interface.
C. A QoS policy must not be currently attached to the interface.
D. CEF must be enabled.
E. AutoQoS must be enabled globally before it can be enabled on the interface.
F. An IP address must be configured on the interface if its speed is equal to or less than 768 kbps.

Correct Answer: AE
Explanation

Explanation/Reference:
Explanation:

QUESTION 27
Which of the following topology situations would be a qood candidate for configuring DMVPN?

A. Extranet VPN
B. Managed overlay VPN topology
C. Hub-and-spoke VPN topology
D. Central-site VPN topology
E. Full mesh VPN topology
F. Remote-access VPN topology

Correct Answer: E

Explanation

Explanation/Reference:
Explanation:

QUESTION 28
Which of the following is not considered a common approach to narrow the field of potential problem causes? (Choose the best answer.)

A. Following the traffic path
B. Top-down
C. Comparing configurations
D. Bottom-up
E. Divide and conquer
F. Examine SLAs

Correct Answer: F
Explanation

Explanation/Reference:
Explanation:

QUESTION 29
Which of the following best describes the following command: ip flow-export destination 192.168.1.50 1500?

A. it is not a valid NetFlow command.
B. it is an SNMP command that exports 1500-byte packets to IP address 192.168.1.50.
C. it is a NetFlov/ command that v/ill export 1500-byte packets to IP address 192.168.1.50.
D. it is a NetFlov/ command that allows IP address 192.168.1.50 to send traffic to port 1500.
E. It is a NetFlov/ command that v/ill specify that the NetFlov/ collector's IP address is 192.168.1.50 over UDP port 1500.
F. It is an SNMP command that exports flows to destination address 1Q2.168.1.50 for packets up to an MTU of 1500.

Correct Answer: E
Explanation

Explanation/Reference:
Explanation:

QUESTION 30
Which of the following are valid methods of providing a router with information concerning the location of the RP? (Choose all that apply.)

A. Statically defined RP
B. Bootstrap Router
C. Auto-RP
D. RP Discovery Protocol (RDP)
E. RP Helios
F. RPARP(RARP)

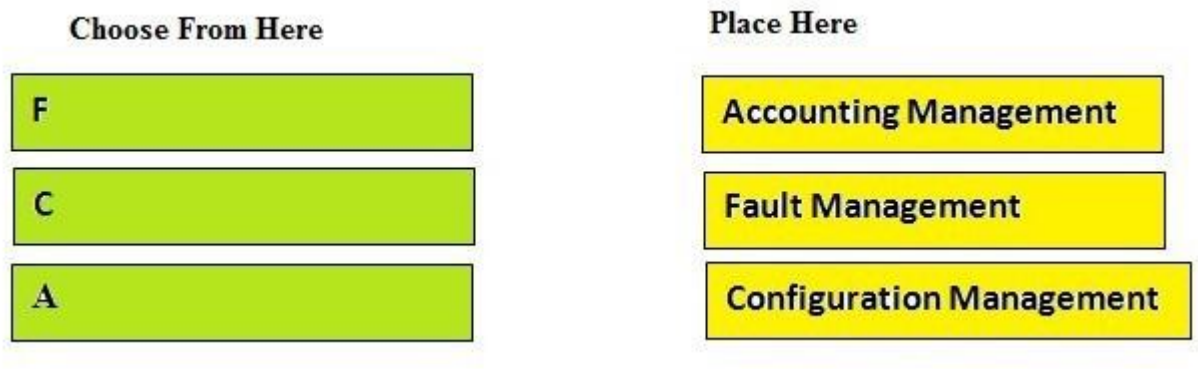
Correct Answer: ABC
Explanation

Explanation/Reference:
Explanation:

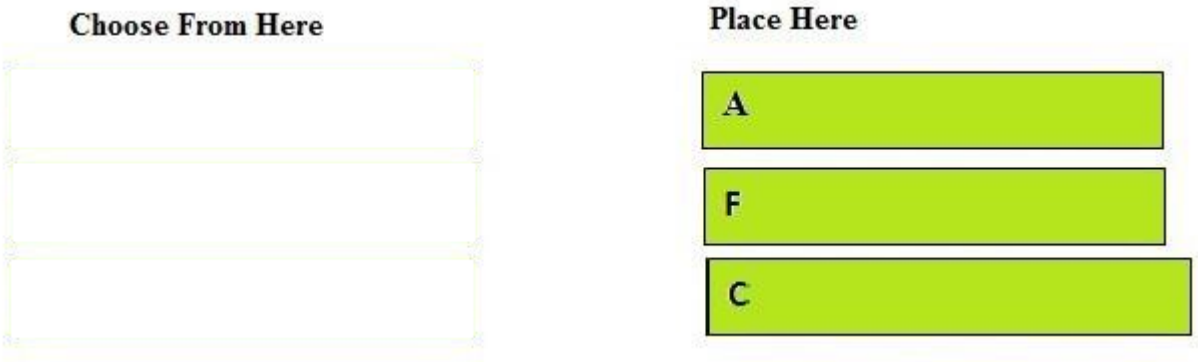
Question Set 1

QUESTION 1
FCAPS is a network maintenance model defined by ISO. FCAPS stands for:

Select and Place:



Correct Answer:



Explanation

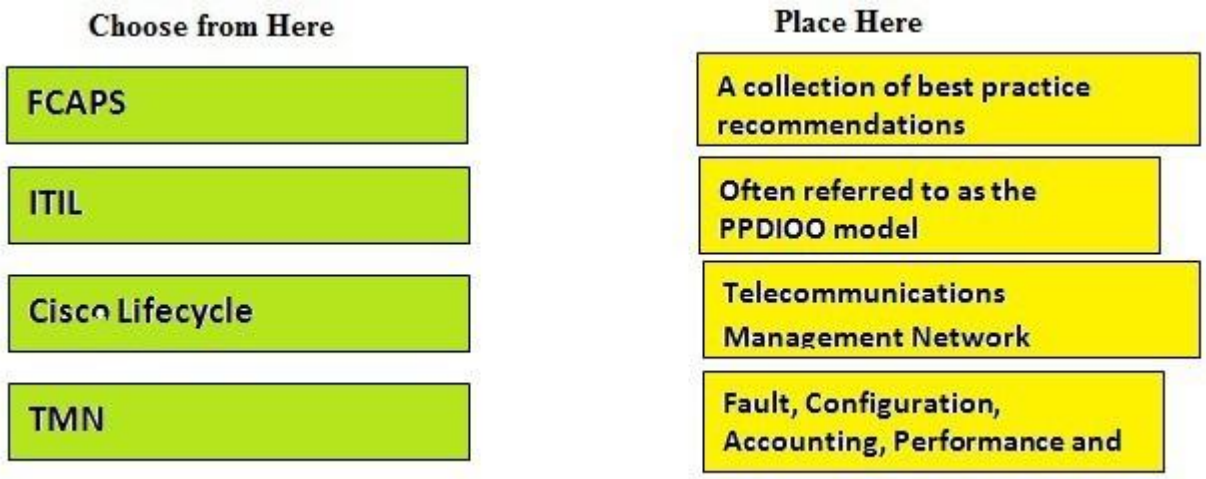
Explanation/Reference:
Explanation:

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

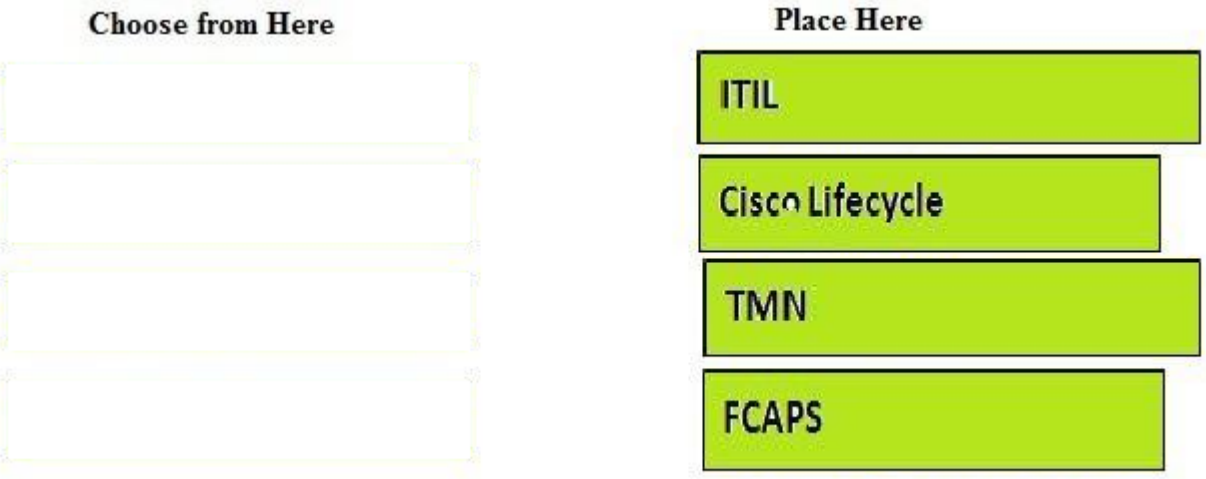
The FCAPS maintenance model consists of the following:
FCAPS Maintenance Tasks:

QUESTION 2
There are many Network Maintenance models. Match the model names on the left to the options on the right:

Select and Place:



Correct Answer:



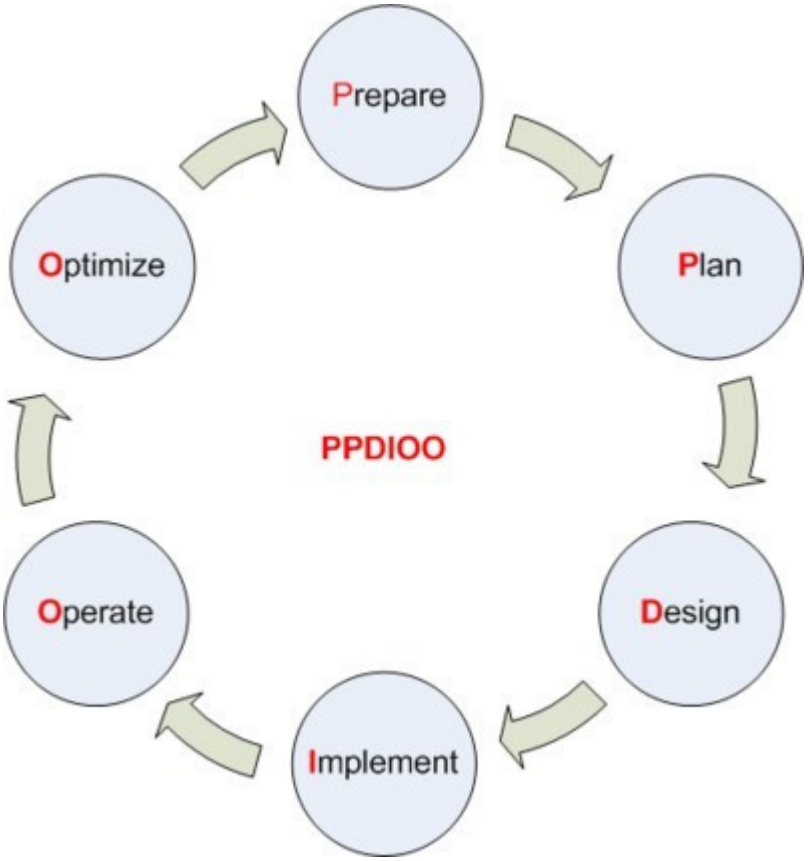
Explanation

Explanation/Reference:
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

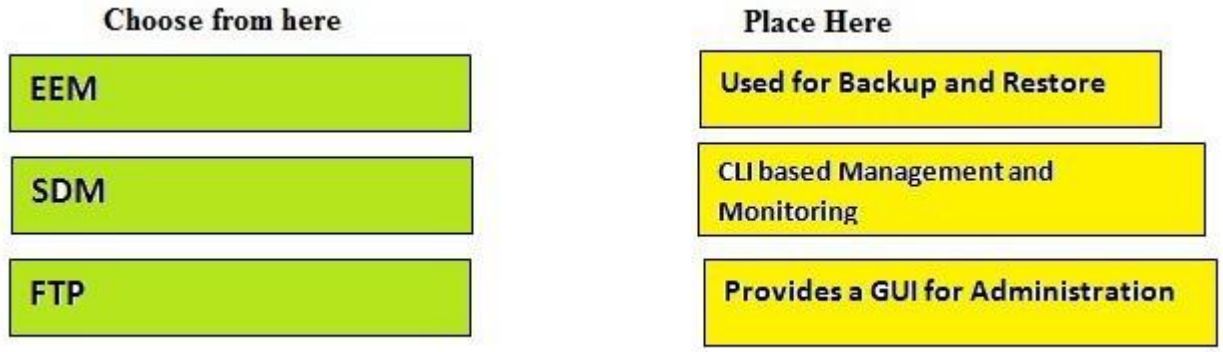
Explanation
FCAPS
Fault-, Configuration-, Accounting-, Performance- and Security management defined by ISO
ITIL
IT Infrastructure Library
Defines a collection of best-practice recommendations that work together to meet business goals.
TMN
Telecommunications Management Network
ITU-T variation of FCAPS - See above - specially targeted towards Tele Communication Networks
PPDIOO
Also called Cisco Lifecycle Services (See drawing below)



PPDIOO Life Cycle
References:

QUESTION 3
Match the items on the left to their purpose on the right

Select and Place:



Correct Answer:

Explanation

Explanation/Reference:
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-confg]?
Writing R1-confg !!!
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 minuttes. 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-confg-4 Archive # Name
1 ftp://192.168.2.33/R1-confg-1
2 ftp://192.168.2.33/R1-confg-2
3 ftp://192.168.2.33/R1-confg-3 <- Most Recent

Testlet 1

Topic 3, Ticket 1 : Switch Port Trunk

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

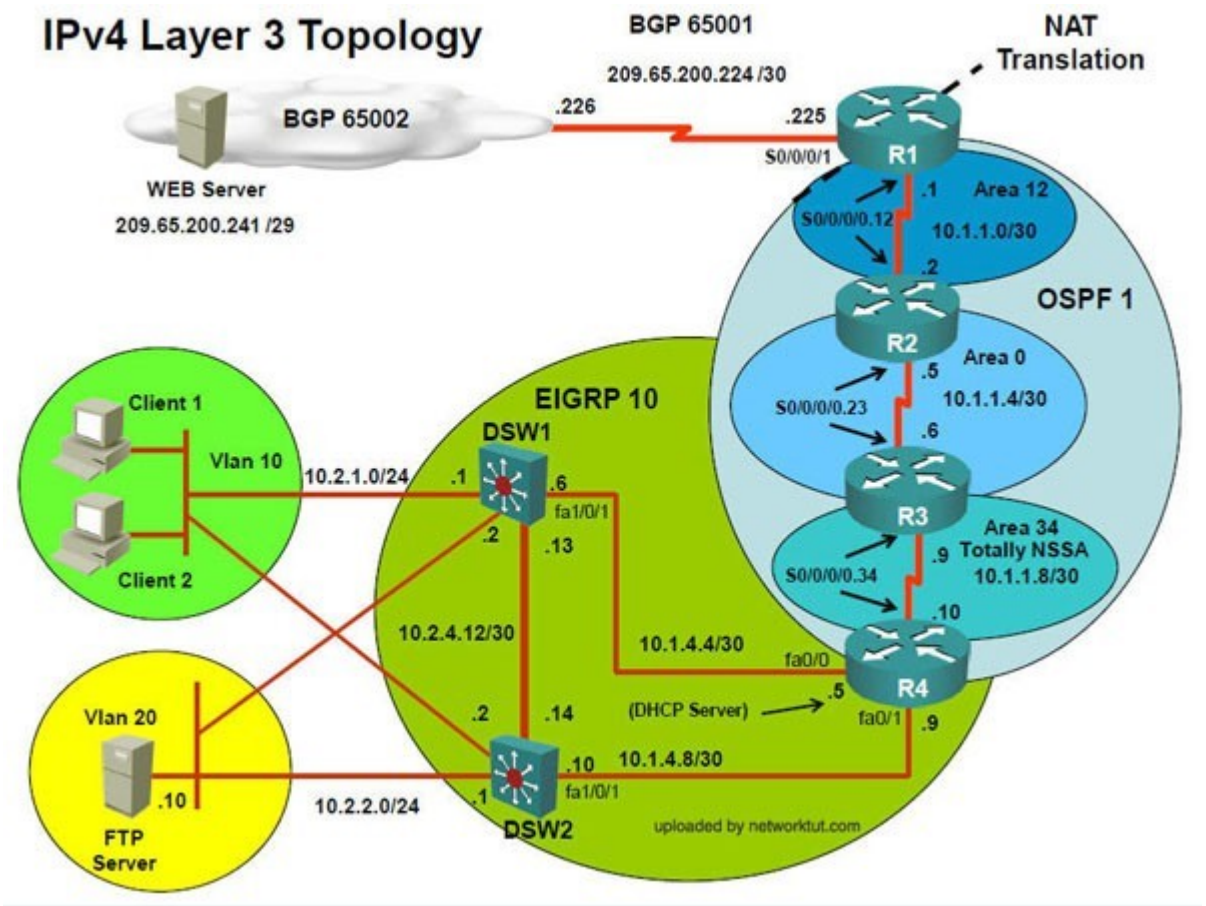
The company has created the test bed shown in the layer 2 and layer 3 topology exhibits. This network consists of four routers, two layer 3 switches and two layer 2 switches.

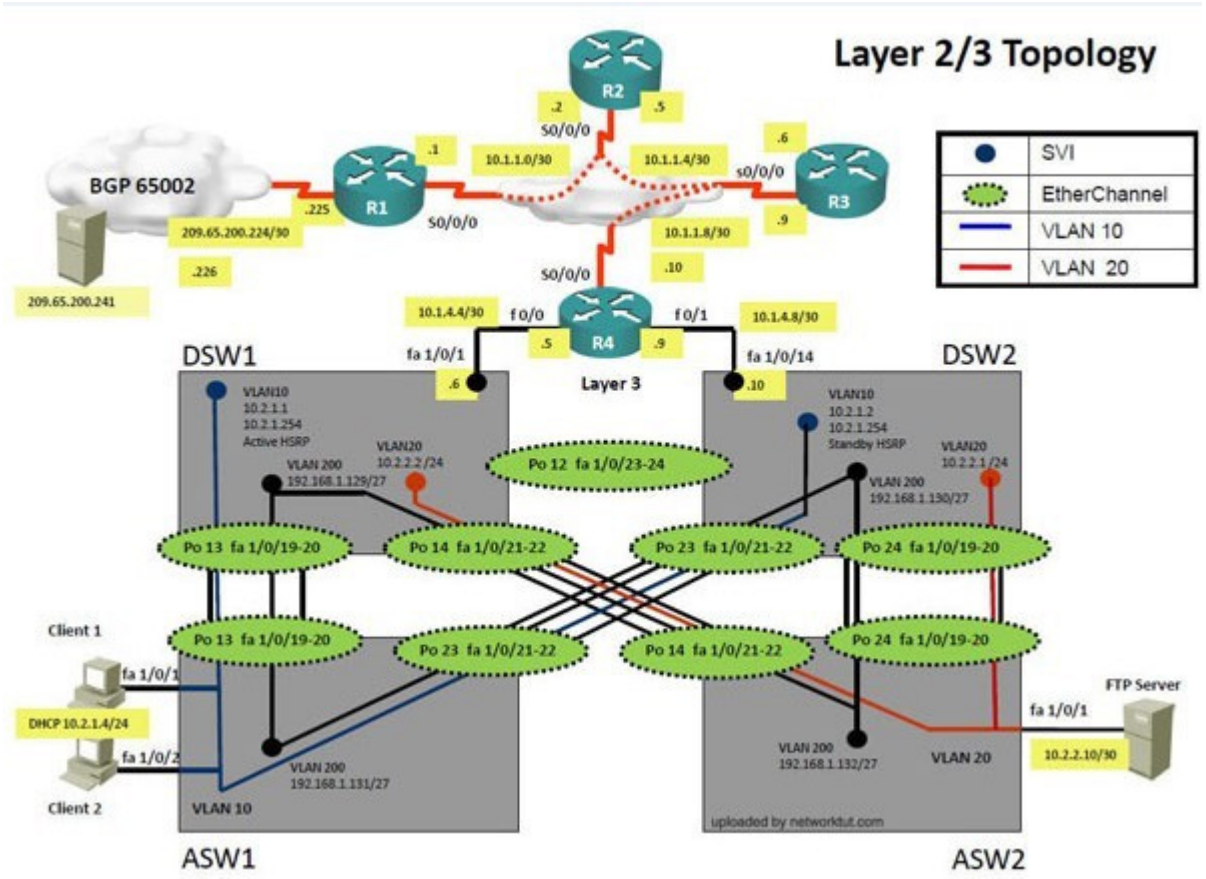
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. 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
========== ======

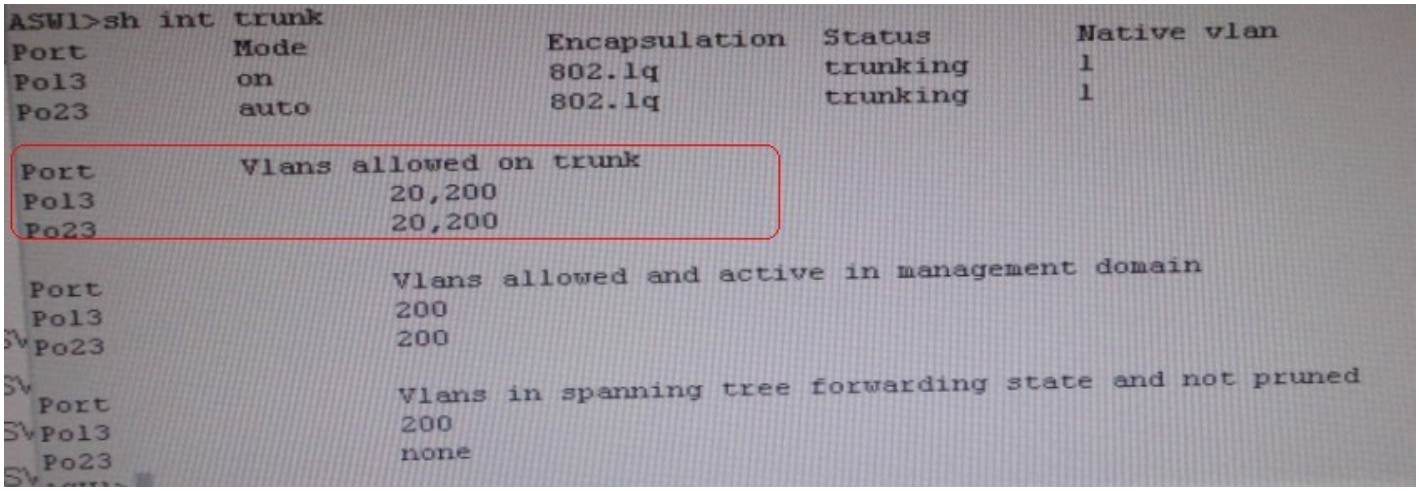




Client is unable to ping IP 209.65.200.241

Solution
Steps need to follow as below:-
Ipconfig ----- Client will be getting 169.X.X.X

Sh run ------- & check for running config of int fa1/0/1 & fa1/0/2
==========
interface FastEthernet1/0/1switchport mode accessswitchport access vlan 10interface FastEthernet1/0/2switchport mode accessswitchport access vlan 10
==========



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 1
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

Correct Answer: G
Explanation

Explanation/Reference:
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 2
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

Correct Answer: B
Explanation

Explanation/Reference:
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 3
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.

Correct Answer: B
Explanation

Explanation/Reference:
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.

========== =====

Testlet 1

Topic 4, Ticket 2 : ACCESS VLAN

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

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.

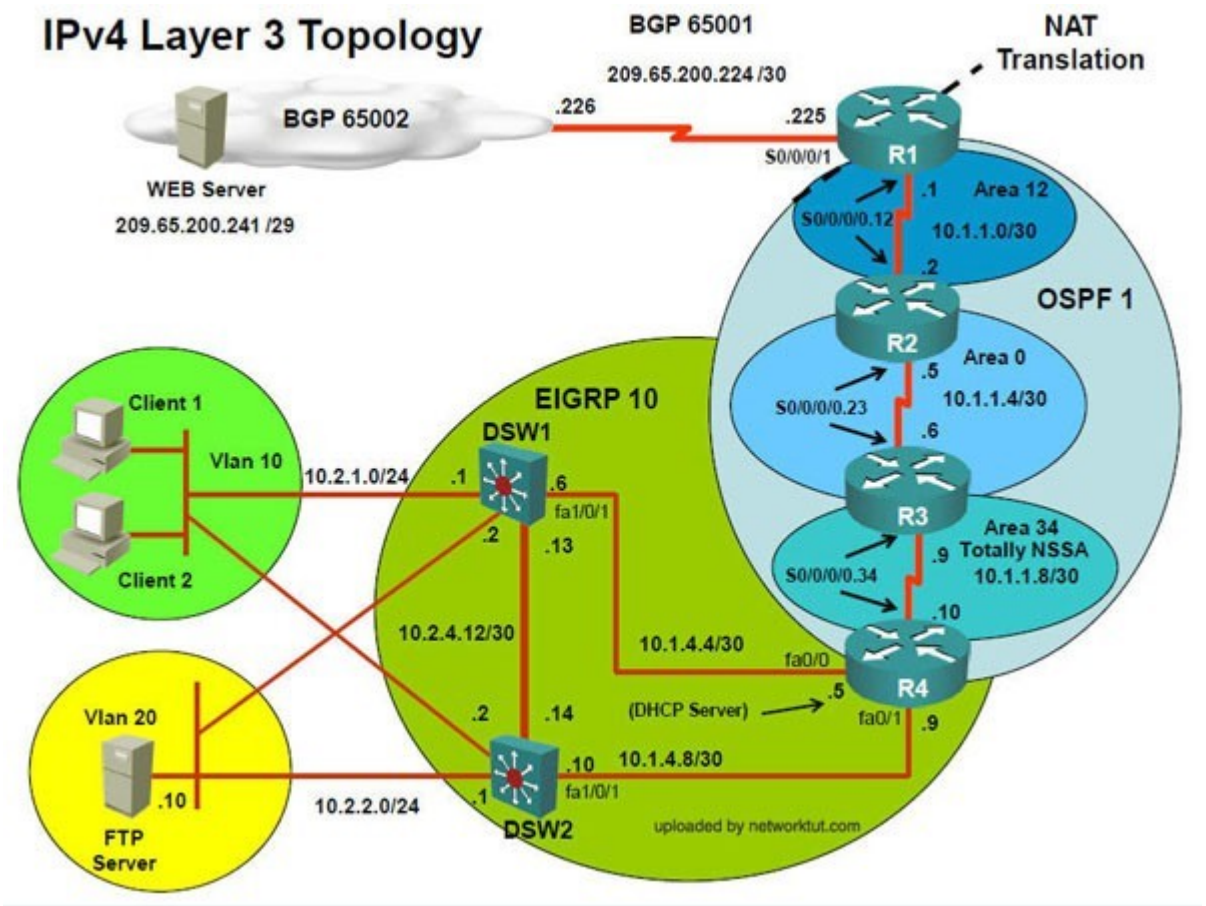
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. 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.

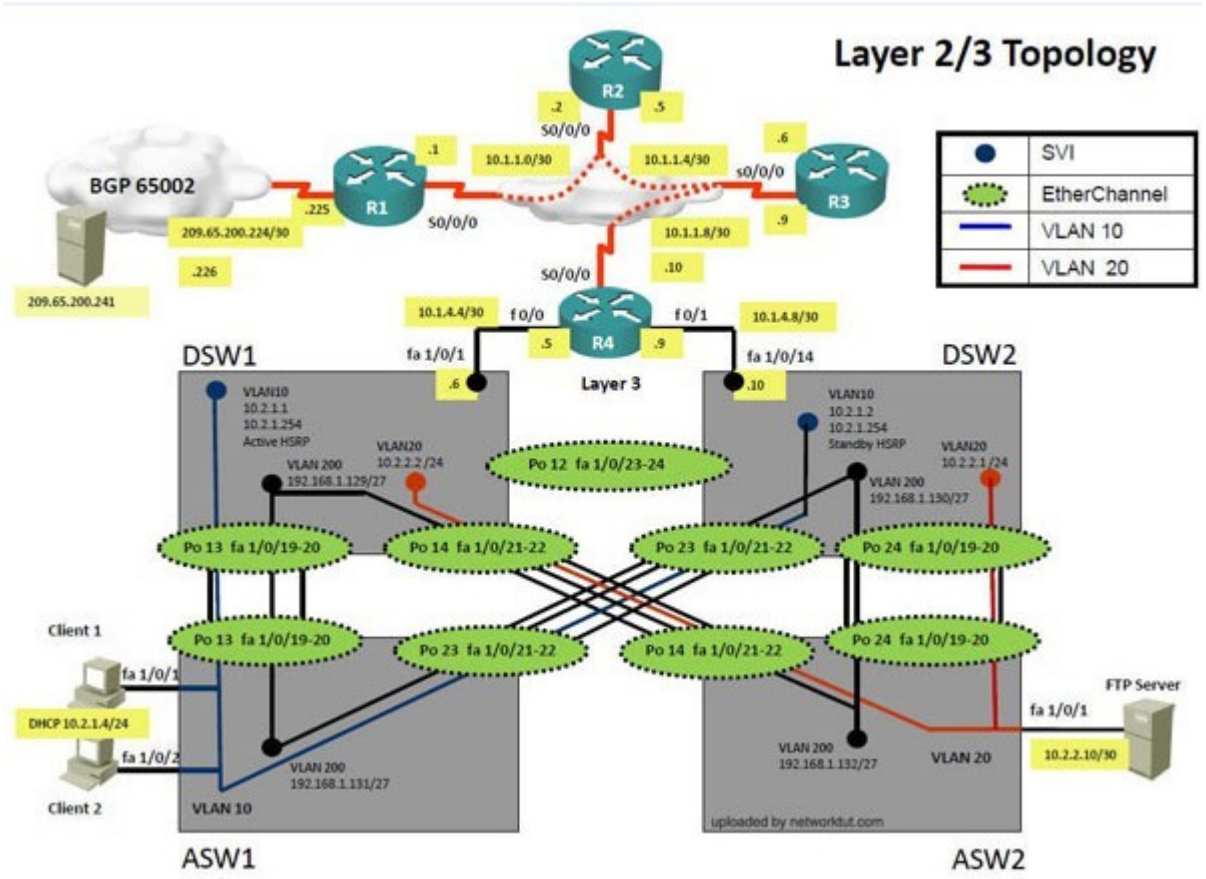
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where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

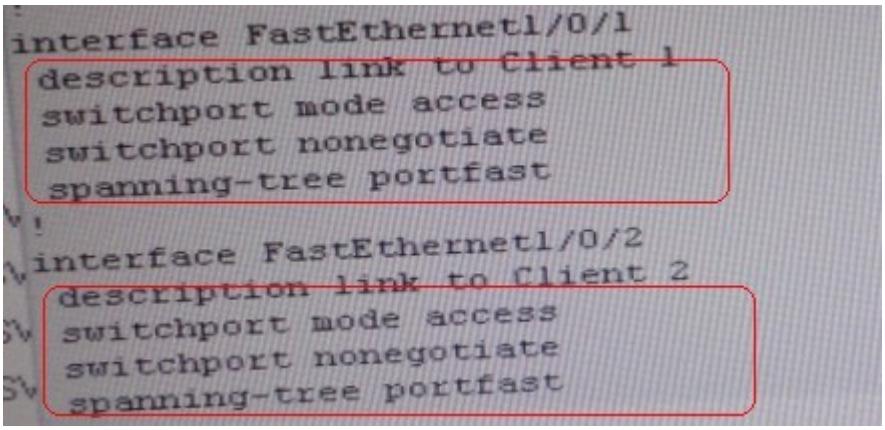




Client is unable to ping IP 209.65.200.241

Solution
Steps need to follow as below:-
Ipconfig ----- Client will be getting 169.X.X.X

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



==========

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

QUESTION 1
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

Correct Answer: G
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
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

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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.

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

========== ======

Testlet 1

Topic 5, Ticket 3 : OSPF Authentication

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

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.

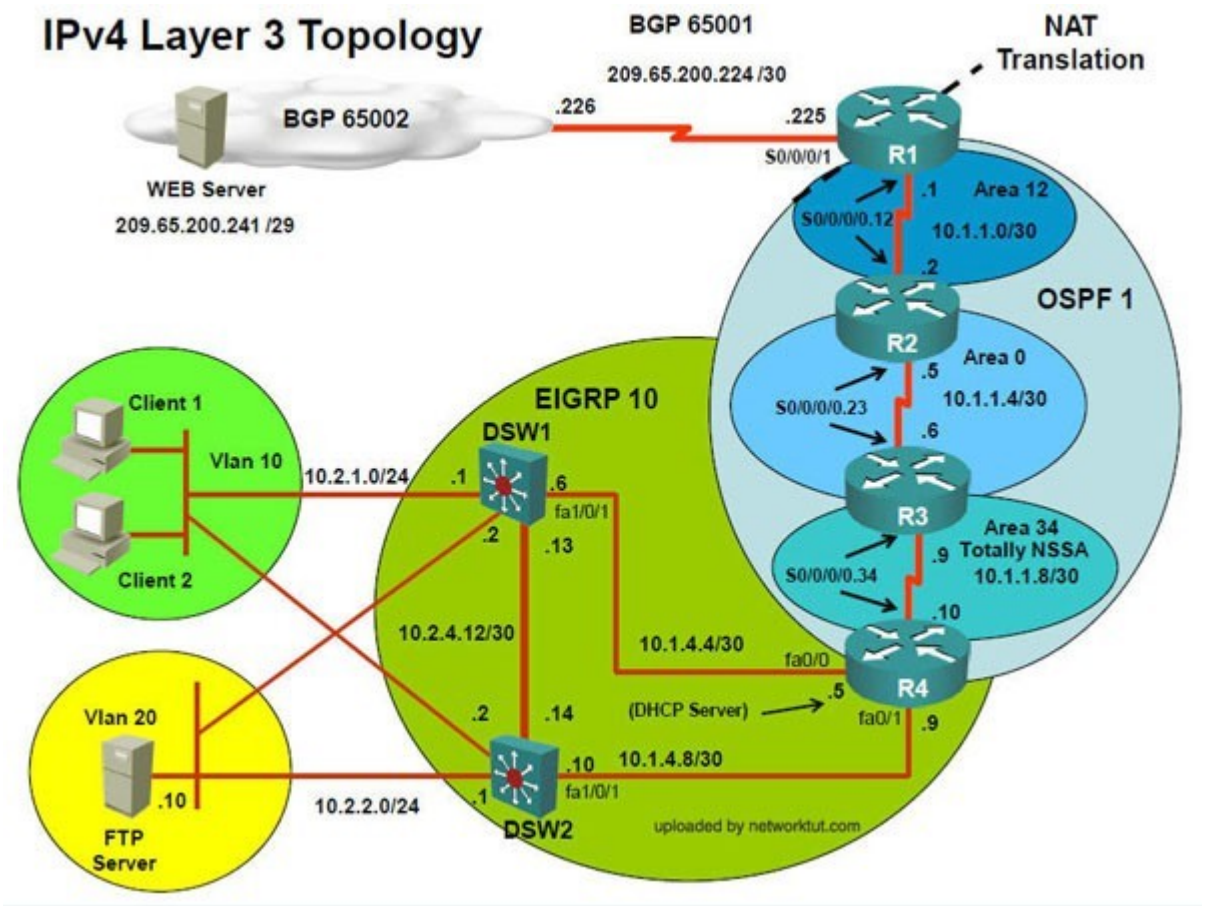
In the IPv4 layer 3 topology, R1, R2, R3, and R4 are running OSPF with an OSPF process number 1. DSW1, DSW2 and R4 are running EIGRP with an AS of 10. Redistribution is enabled where necessary. R1 is running a BGP AS with a number of 65001. This AS has an eBGP connection to AS 65002 in the ISP's network. 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.

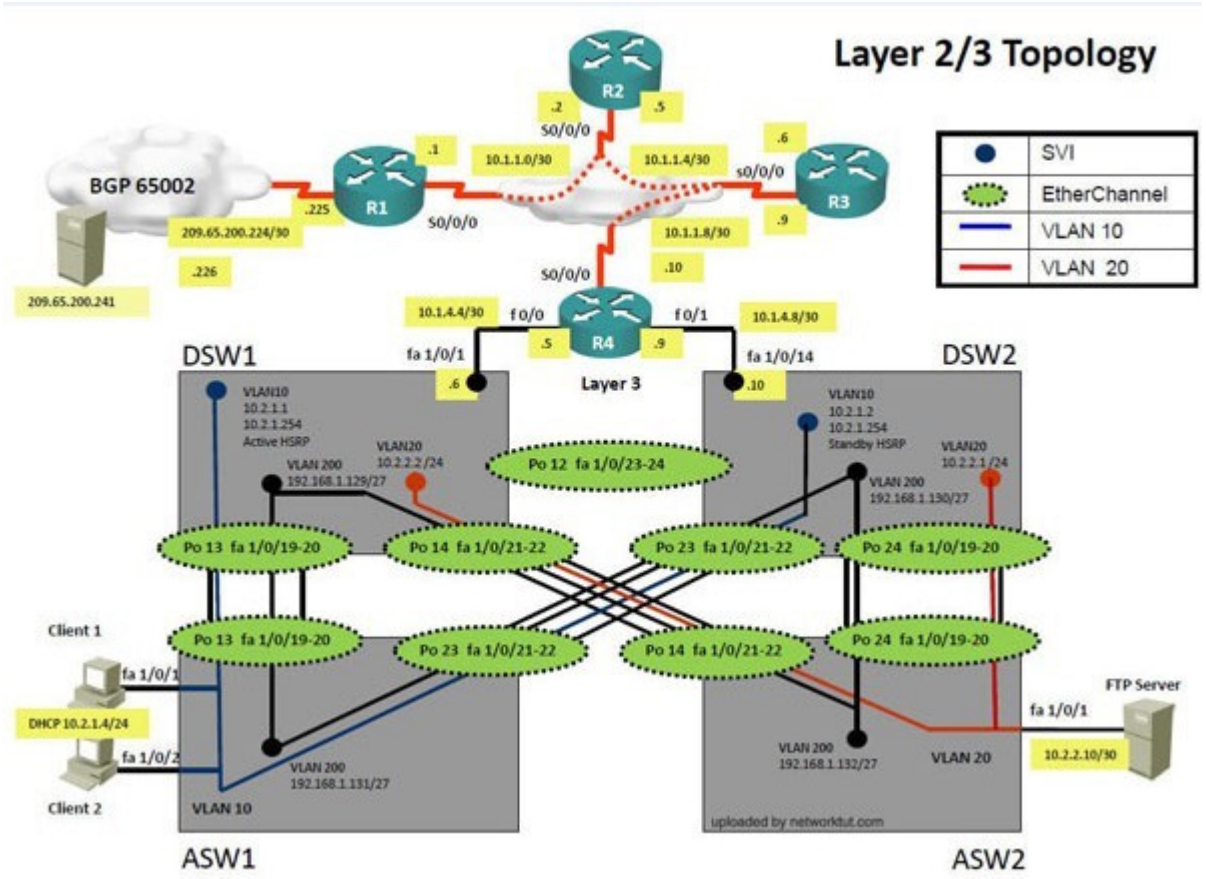
In the IPv6 layer 3 topology R1, R2, and R3 are running OSPFv3 with an OSPF process number 6. DSW1, DSW2 and R4 are running RIPng process name RIP_ZONE. The two IPv6 routing domains, OSPF 6 and RIPng are connected via GRE tunnel running over the underlying IPv4 OSPF domain. Redistrution is enabled where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

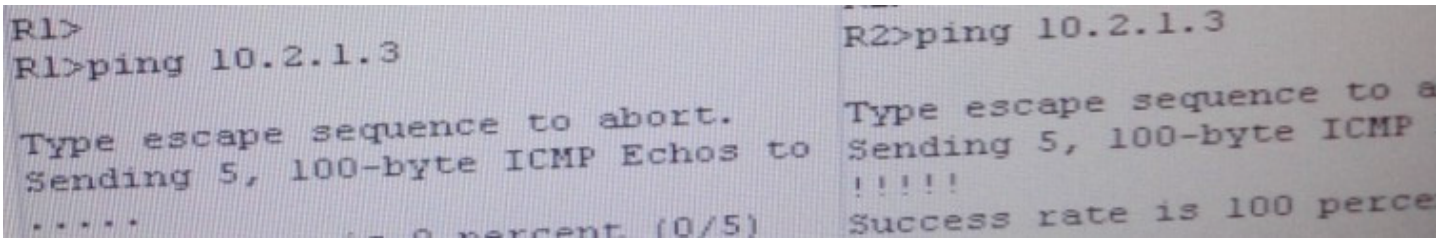
Each ticket has 3 sub questions that need to be answered & topology remains same.
Question-1 Fault is found on which device,
Question-2 Fault condition is related to,
Question-3 What exact problem is seen & what needs to be done for solution
========== ======



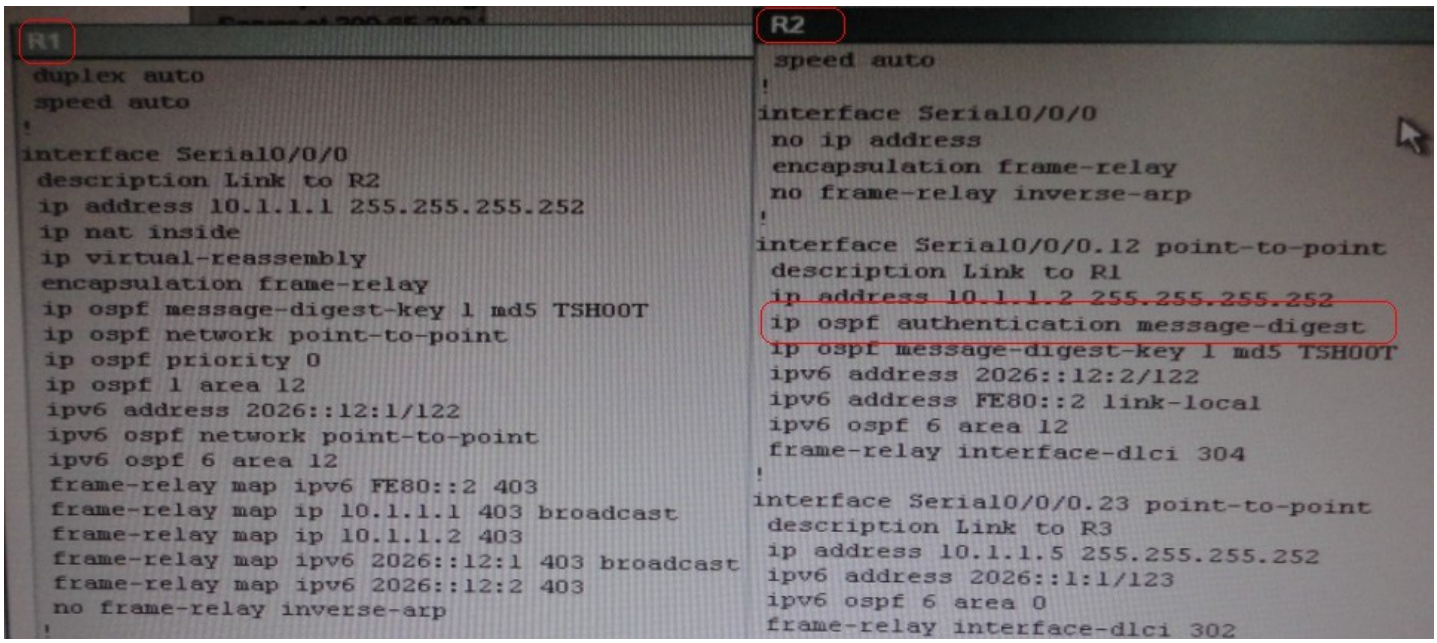


Client is unable to ping IP 209.65.200.241

Solution
Steps need to follow as below:-
Ipconfig ----- Client will be receiving IP address 10.2.1.3



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
Sh run ------------------------- Interface Serial0/0/0/0.12 on R2



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

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

QUESTION 1
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

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

QUESTION 2
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

Correct Answer: D
Explanation

Explanation/Reference:
Explanation:

QUESTION 3
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.

Correct Answer: A
Explanation

Explanation/Reference:
Explanation:

========== ======

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

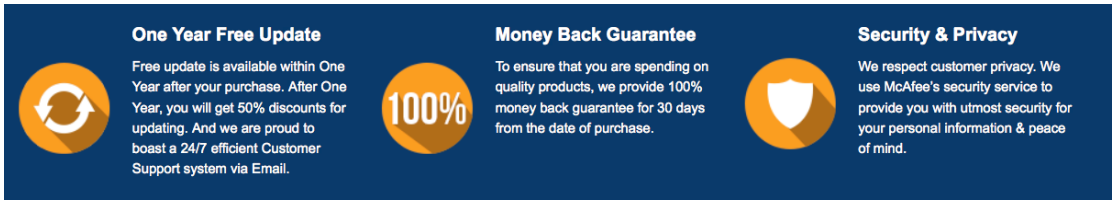
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions