

➤ **Vendor: Cisco**

➤ **Exam Code: 200-125**

➤ **Exam Name: Cisco Certified Network Associate  
(v3.0)**

➤ **Question 251 – Question 300**

[Visit PassLeader and Download Full Version 200-125 Exam Dumps](#)

**QUESTION 251**

Drag and Drop Question

Match the terms on the left with the appropriate OSI layer on the right. (Not all options are used.)	
frames	Network Layer <div></div> <div></div> <div></div>
packets	
UDP	
IP addresses	Transport Layer <div></div> <div></div> <div></div>
segments	
MAC addresses	
windowing	
routing	

**Answer:**

Match the terms on the left with the appropriate OSI layer on the right. (Not all options are used.)

frames	Network Layer
packets	packets
UDP	IP addresses
IP addresses	routing
segments	Transport Layer
MAC addresses	UDP
windowing	segments
routing	windowing

### QUESTION 252

#### Lab Simulation Question - ACL-1

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".

The Core connection uses an IP address of 198.18.196.65

The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254

Host A 192.168.33.1

Host B 192.168.33.2

Host C 192.168.33.3

Host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30

The Finance Web Server is assigned an IP address of 172.22.242.23.

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".

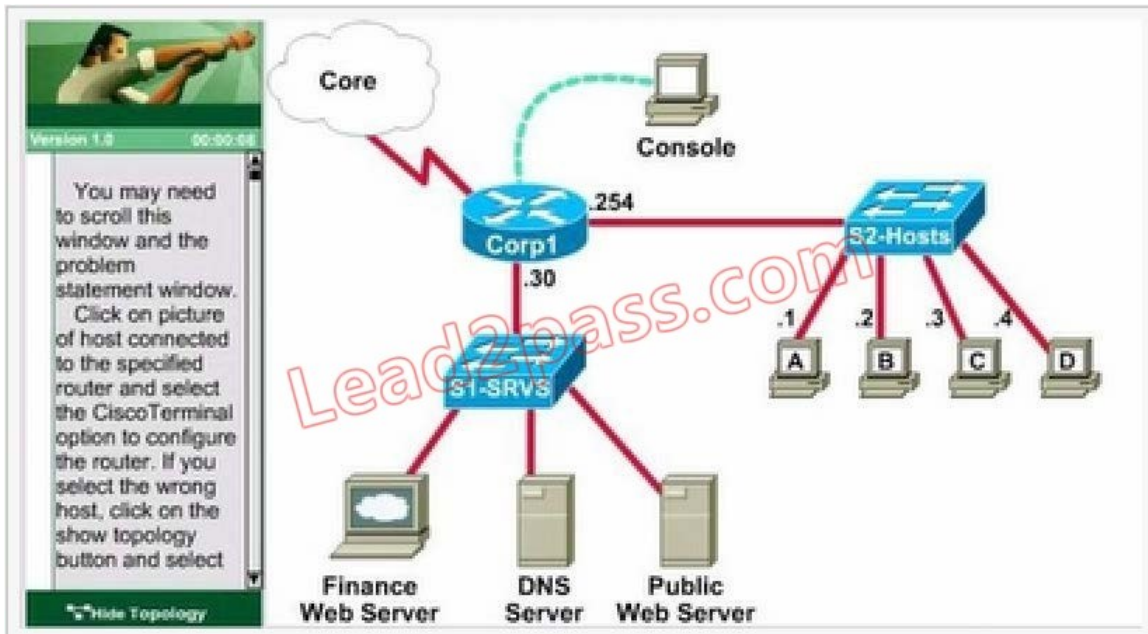
The Core connection uses an IP address of 198.18.196.65

The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254.

- ☐ host A 192.168.33.1
- ☐ host B 192.168.33.2
- ☐ host C 192.168.33.3
- ☐ host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30

The Finance Web Server is assigned an IP address of 172.22.242.23



**Answer:**

```
Corp1>enable
Password: cisco
```

We should create an access-list and apply it to the interface which is connected to the Servers LAN interface, because it can filter out traffic from both Sw-Hosts and Core networks. The Server LAN network has been assigned addresses of 172.22.242.17 – 172.22.242.30 so we can guess the interface connected to them has an IP address of 172.22.242.30 (.30 is the number shown in the figure). Use the “show ip interface brief” command to check which interface has the IP address of 172.22.242.30.

```
Corp1#show ip interface brief
Interface      IP-Address      OK? Method Status Protocol
FastEthernet0/0 192.168.33.254  YES manual up      up
FastEthernet0/1 172.22.242.30   YES manual up      up
Serial0/0       198.18.196.65   YES manual up      up
```

We learn that interface FastEthernet0/1 is the interface connected to Server LAN network. It is the interface we will apply our access-list (for outbound direction).

```
Corp1#configure terminal
```

Our access-list needs to allow host C – 192.168.33.3 to the Finance Web Server 172.22.242.23 via web (port 80)

```
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
```

Deny other hosts access to the Finance Web Server via web

```
Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80
```

All other traffic is permitted

```
Corp1(config)#access-list 100 permit ip any any
```

Apply this access-list to Fa0/1 interface (outbound direction)

```
Corp1(config)#interface fa0/1
```

```
Corp1(config-if)#ip access-group 100 out
```

Notice: We have to apply the access-list to Fa0/1 interface (not Fa0/0 interface) so that the access-list can filter traffic coming from both the LAN and the Core networks. If we apply access list to the inbound interface we can only filter traffic from the LAN network.

In the real exam, just click on host C and open its web browser. In the address box type `http://172.22.242.23` to check if you are allowed to access Finance Web Server or not. If your configuration is correct then you can access it.

Click on other hosts (A, B and D) and check to make sure you can't access Finance Web Server from these hosts.

Finally, save the configuration

```
Corp1(config-if)#end
```

```
Corp1#copy running-config startup-config
```

This configuration only prevents hosts from accessing Finance Web Server via web but if this server supports other traffic – like FTP, SMTP... then other hosts can access it, too.

Notice: In the real exam, you might be asked to allow other host (A, B or D) to access the Finance Web Server so please read the requirement carefully.

#### **Modification #1**

A network associate is adding security to the configuration of the Corp router. The user on host B should be able to access the Finance Web Server. Host B should be denied to access other server on S1-SRVS network. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host B access to the Finance Web Server. Deny host B from accessing the other servers. All other traffic is permitted.

```
access-list 100 permit ip host 192.168.33.2 host 172.22.242.23
access-list 100 deny ip host 192.168.33.2 172.22.242.16 0.0.0.15
access-list 100 permit ip any any
```

#### **Modification #2**

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to access the Finance Web Server. No other hosts from the LAN nor the Core should be able access this server. All other traffic should be allowed.

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host C access the Finance Web Server. No other hosts will have access to the Finance Web Server. All other traffic is permitted.

```
access-list 100 permit ip host 192.168.33.3 host 172.22.242.23
access-list 100 deny ip any host 172.22.242.23
access-list 100 permit ip any any
```

#### **Modification #3**

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. Other access from host C to Finance Web Server should be denied. No other hosts from the LAN nor the Core should be able to access the Finance Web Server. All other traffic should be allowed. The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. Also host C should be denied to access any other services of Finance Web Server. No other hosts will access to the Finance Web Server. All other traffic is permitted.

```
access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
access-list 100 deny ip any host 172.22.242.23
access-list 100 permit ip any any
```

#### **Modification #4**

A network associate is adding security to the configuration of the Corp1 router. The user on host D should be able to use a web browser to access financial information from the Finance Web Server. Other access from host C to Finance Web Server should be denied. No other hosts from the LAN nor the Core should be able to access the Finance Web Server. All hosts from the LAN nor the Core should be able to access public web server.

The task is to create and apply a numbered access-list with no more than three statements that will allow ONLY host D should be able to use a web browser(HTTP)to access the Finance Web Server. Other types of access from host D to the Finance Web Server should be blocked. All access from

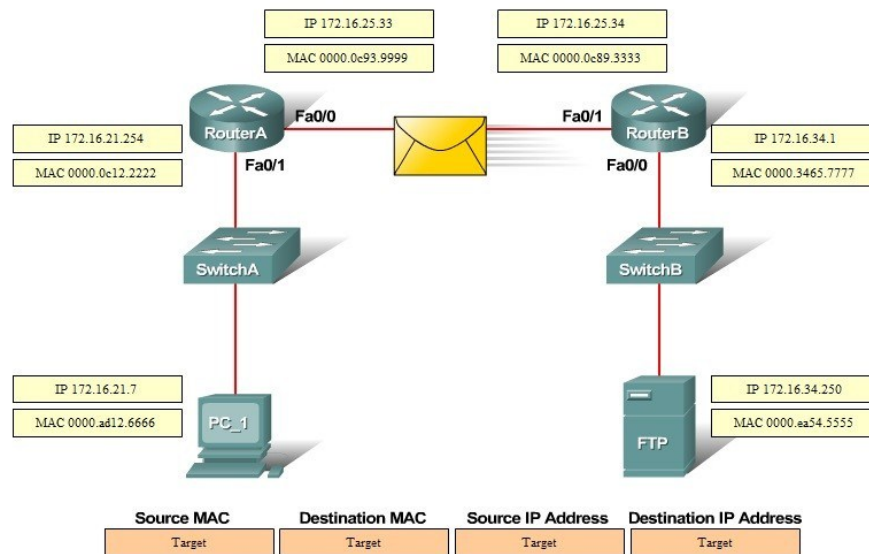
hosts in the Core or local LAN to the Finance Web Server should be blocked. All hosts in the Core and local LAN should be able to access the Public Web Server.

```
access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
access-list 100 deny ip any host 172.22.242.23
access-list 100 permit ip any any
```

### QUESTION 253

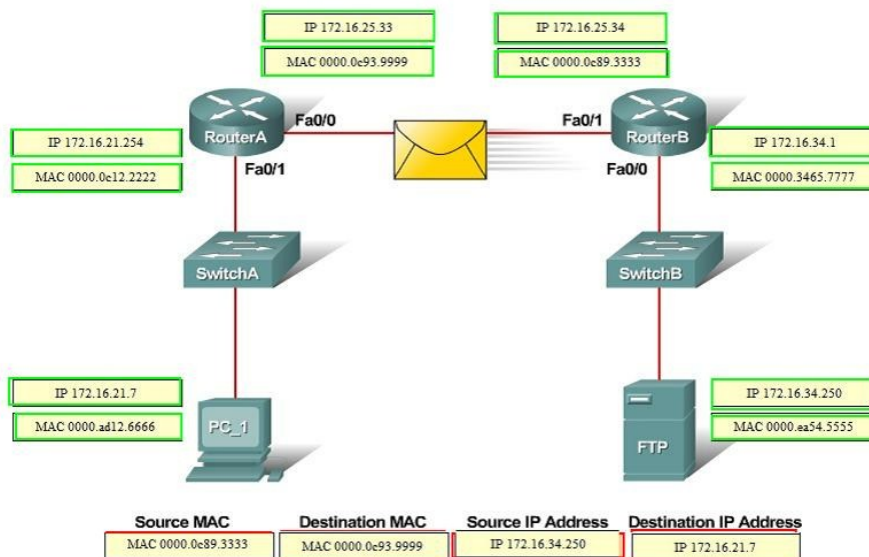
#### Drag and Drop Question

Refer to the exhibit. PC\_1 is exchanging packets with the FTP server. Consider the packets as they leave RouterB interface Fa0/1 towards RouterA. Drag the correct frame and packet addresses to their place in the table.



#### Answer:

Refer to the exhibit. PC\_1 is exchanging packets with the FTP server. Consider the packets as they leave RouterB interface Fa0/1 towards RouterA. Drag the correct frame and packet addresses to their place in the table.



### QUESTION 254

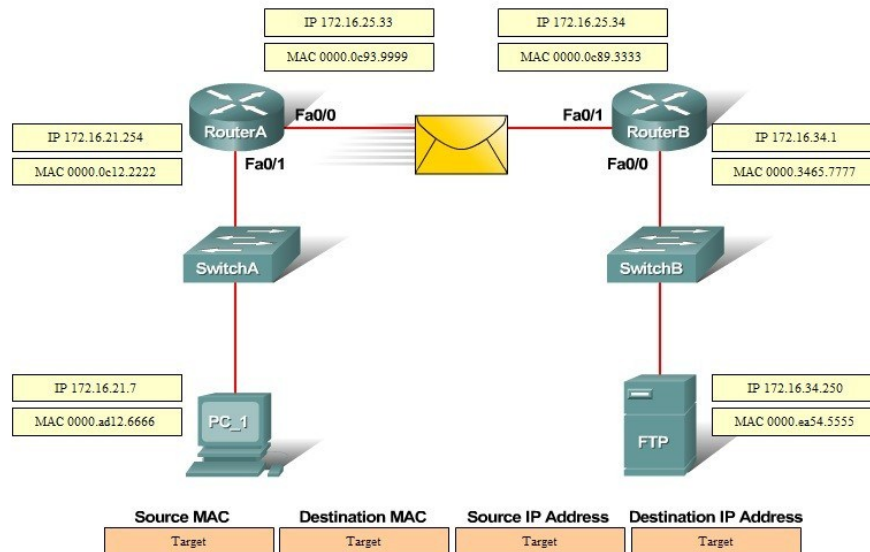
#### Drag and Drop Question

[200-125 Exam Dumps](#) [200-125 Exam Questions](#) [200-125 PDF Dumps](#) [200-125 VCE Dumps](#)

<http://www.passleader.com/200-125.html>

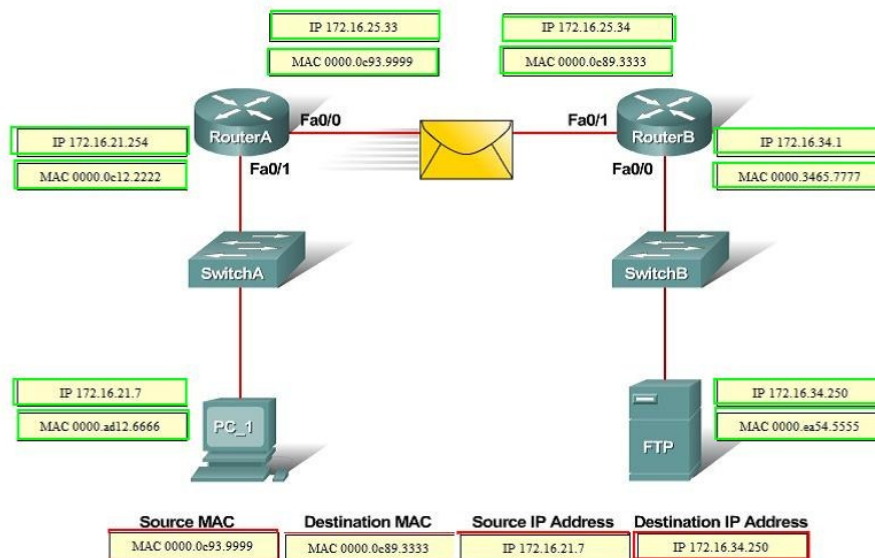


Refer to the exhibit. PC\_1 is sending packets to the FTP server. Consider the packets as they leave RouterA interface Fa0/0 towards RouterB. Drag the correct frame and packet address to their place in the table.



**Answer:**

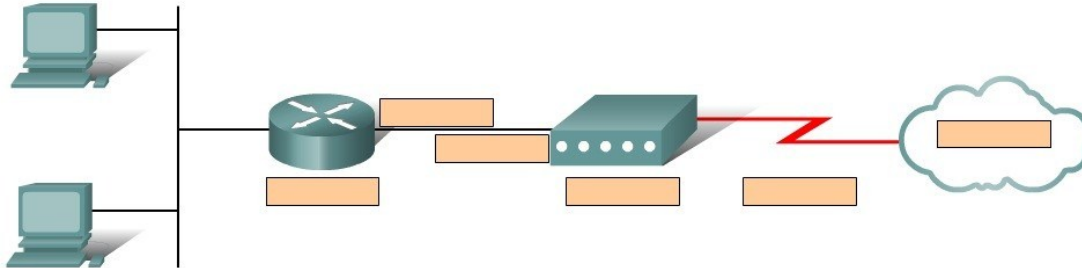
Refer to the exhibit. PC\_1 is sending packets to the FTP server. Consider the packets as they leave RouterA interface Fa0/0 towards RouterB. Drag the correct frame and packet address to their place in the table.



**QUESTION 255**

Drag and Drop Question

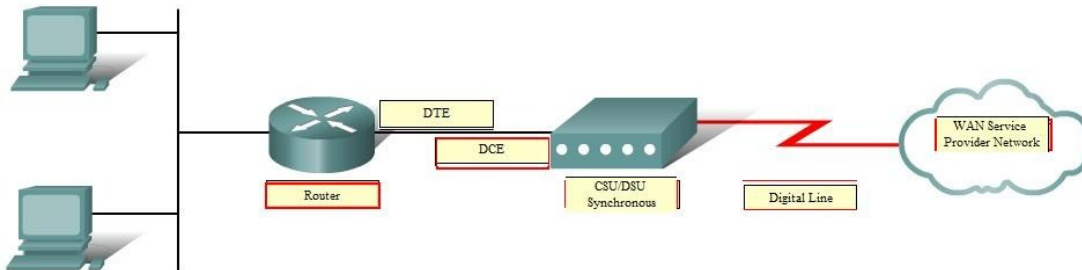
Refer to the exhibit. Complete this network diagram by dragging the correct device name or description to the correct location. Not all the names or descriptions will be used.



Digital Line
CSU/DSU Synchronous
Analog Modem Asynchronous
WAN Service Provider Network
Router
Switch
DTE
DCE

**Answer:**

Refer to the exhibit. Complete this network diagram by dragging the correct device name or description to the correct location. Not all the names or descriptions will be used.



Digital Line
CSU/DSU Synchronous
Analog Modem Asynchronous
WAN Service Provider Network
Router
Switch
DTE
DCE

**QUESTION 256**

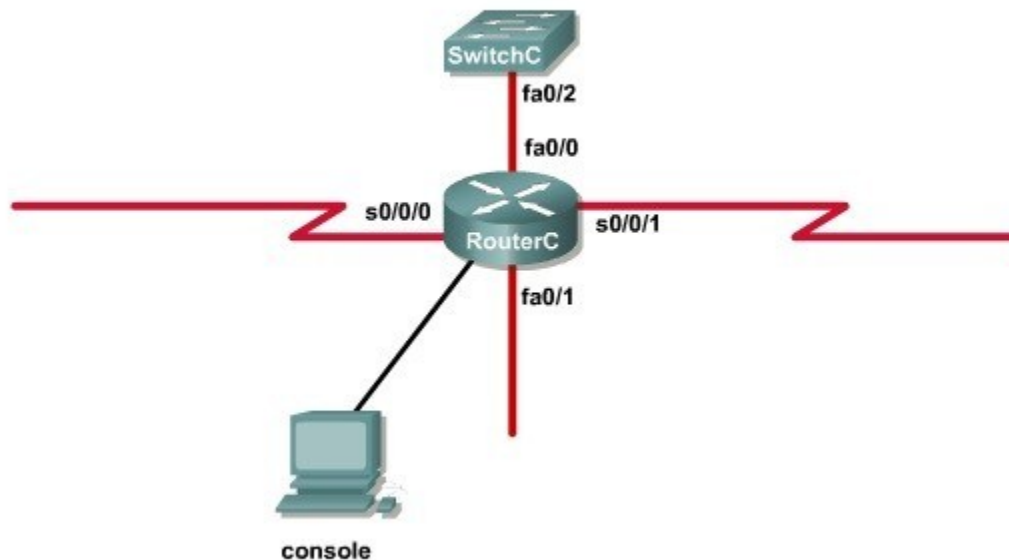
Hotspot Question

**Instructions**

An administrator is trying to ping and telnet from SwitchC to RouterC with the results shown below.

```
SwitchC>  
SwitchC> ping 10.4.4.3  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.4.4.3, timeout is 2 seconds:  
U.U.U  
Success rate is 0 percent (0/5)  
SwitchC>  
SwitchC> telnet 10.4.4.3  
Trying 10.4.4.3 ...  
% Destination unreachable; gateway or host down  
SwitchC>
```

Click the console connected to RouterC and issue the appropriate commands to answer the questions.

**Topology**





<output omitted>

```
interface Loopback1
 ip address 172.16.4.1 255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1 255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3 255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
```

[Dumps](#) [200-125 VCE Dumps](#)

```
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 not auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.4.4.3 0.0.0.0 area 0
 network 10.45.45.1 0.0.0.0 area 0
 network 10.140.3.2 0.0.0.0 area 0
 network 192.168.2.62 0.0.0.0 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any

access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any

access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply
access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any

access-list 114 permit ip 10.4.4.0.0.0.255 any

access-list 115 permit ip 0.0.0.0 255.255.255.0 any

access-list 122 deny tcp any any
access-list 122 deny imp any any echo-reply
access-list 122 permit ip any any
!
```

<output omitted>

Which will fix the issue and allow ONLY ping to work while keeping telnet disabled?

- A. Correctly assign an IP address to interface fa0/1.
- B. Change the ip access-group command on fa0/0 from "in\*" to "our."
- C. Remove access-group 106 in from interface fa0/0 and add access-group 115 in.
- D. Remove access-group 102 out from interface s0/0/0 and add access-group 114 in
- E. Remove access-group 106 in from interface fa0/0 and add access-group 104 in.

**Answer: E**

**Explanation:**

Let's have a look at the access list 104:

```
access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 permit icmp any any echo-reply
access-list 104 permit ip any any
```

The question does not ask about ftp traffic so we don't care about the two first lines. The 3rd line denies all telnet traffic and the 4th line allows icmp traffic to be sent (ping). Remember that the access list 104 is applied on the inbound direction so the 5th line "access-list 104 deny icmp any any echo-reply" will not affect our icmp traffic because the "echo-reply" message will be sent over the outbound direction.

### QUESTION 257

#### Hotspot Question

##### Instructions

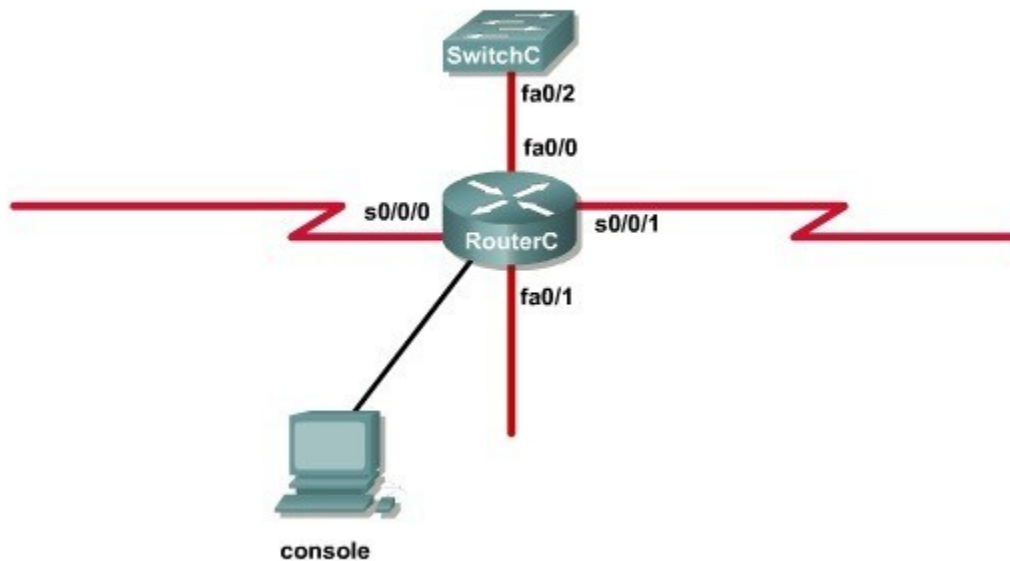
An administrator is trying to ping and telnet from SwitchC to RouterC with the results shown below.

```
SwitchC>
SwitchC> ping 10.4.4.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.4.4.3, timeout is 2 seconds:
U.U.U
Success rate is 0 percent (0/5)
SwitchC>
SwitchC> telnet 10.4.4.3
Trying 10.4.4.3 ...
% Destination unreachable; gateway or host down
SwitchC>
```

Click the console connected to RouterC and issue the appropriate commands to answer the questions.



Topology



RouterC

Press RETURN to get started!  
RouterC>

<output omitted>

```
interface Loopback1
 ip address 172.16.4.1 255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1 255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3 255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
```

[Dumps](#) [200-125 VCE Dumps](#)

```
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 not auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.4.4.3 0.0.0.0 area 0
 network 10.45.45.1 0.0.0.0 area 0
 network 10.140.3.2 0.0.0.0 area 0
 network 192.168.2.62 0.0.0.0 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any

access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any

access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply
access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any

access-list 114 permit ip 10.4.4.0.0.0.255 any

access-list 115 permit ip 0.0.0.0 255.255.255.0 any

access-list 122 deny tcp any any
access-list 122 deny imp any any echo-reply
access-list 122 permit ip any any
!
<output omitted>
```

What would be the effect of issuing the command ip access-group 114 in to the fa0/0 interface?

- A. Attempts to telnet to the router would fail.
- B. It would allow all traffic from the 10.4.4.0 network.
- C. IP traffic would be passed through the interface but TCP and UDP traffic would not.
- D. Routing protocol updates for the 10.4.4.0 network would not be accepted from the fa0/0 interface.

**Answer: B**

**Explanation:**

From the output of access-list 114: access-list 114 permit ip 10.4.4.0 0.0.0.255 any we can easily understand that this access list allows all traffic (ip) from 10.4.4.0/24 network

**QUESTION 258**

Hotspot Question

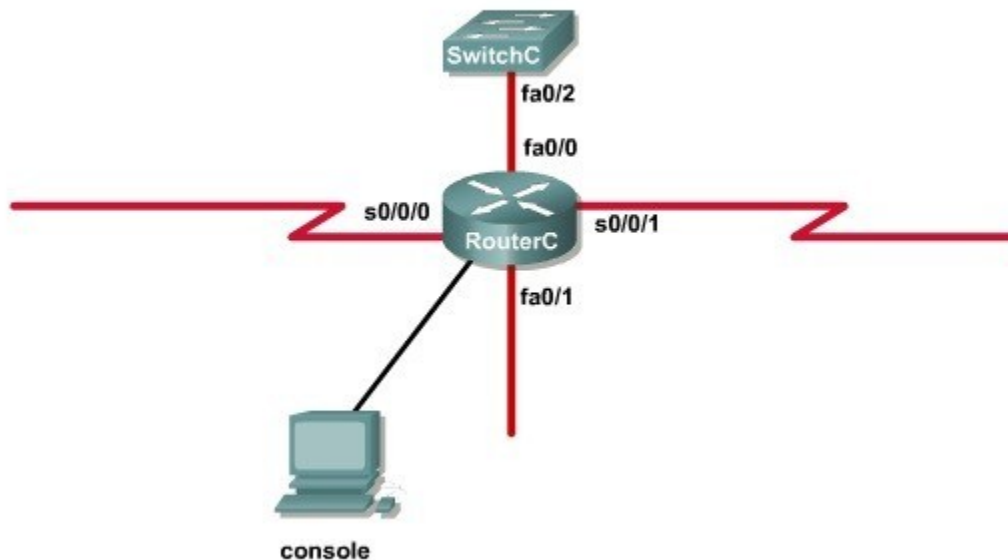
Instructions

An administrator is trying to ping and telnet from SwitchC to RouterC with the results shown below.

```
SwitchC>  
SwitchC> ping 10.4.4.3  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.4.4.3, timeout is 2 seconds:  
U.U.U  
Success rate is 0 percent (0/5)  
SwitchC>  
SwitchC> telnet 10.4.4.3  
Trying 10.4.4.3 ...  
% Destination unreachable; gateway or host down  
SwitchC>
```

Click the console connected to RouterC and issue the appropriate commands to answer the questions.

Topology







<output omitted>

```
interface Loopback1
 ip address 172.16.4.1 255.255.255.0
!
interface Loopback2
 ip address 10.145.145.1 255.255.255.0
 ipv6 address 2001:410:2:3::/64 eui-64
!
interface FastEthernet0/0
 ip address 10.4.4.3 255.255.255.0
 ip access-group 106 in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 bandwidth 64
 no ip address
 ip access-group 102 out
 encapsulation frame-relay
 ip ospf authentication
 ip ospf authentication
 ip ospf authentication-key san-fran
!
interface Serial0/0/0.1 point-to-point
 ip address 10.140.3.2 255.255.255.0
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 frame-relay interface-dlci 120
!
interface Serial0/0/1
 bandwidth 64
 ip address 10.45.45.1 255.255.255.0
 ip access-group 102 in
 ip authentication mode eigrp 100 md5
 ip authentication key-chain eigrp 100 icndchain
 ip ospf authentication
 ip ospf authentication-key san-fran
 ipv6 address 2001:410:2:10::/64 eui-64
!
```

[Dumps](#) [200-125 VCE Dumps](#)

```
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
 network 192.168.2.0
 not auto-summary
!
router ospf 100
 log-adjacency-changes
 network 10.4.4.3 0.0.0.0 area 0
 network 10.45.45.1 0.0.0.0 area 0
 network 10.140.3.2 0.0.0.0 area 0
 network 192.168.2.62 0.0.0.0 area 0
!
router rip
 version 2
 network 10.0.0.0
 network 172.16.0.0
!
ip default-gateway 10.1.1.2
!
!
ip http server
no ip http secure-server
!
```

```
access-list 102 permit tcp any any eq ftp
access-list 102 permit tcp any any eq ftp-data
access-list 102 deny tcp any any eq telnet
access-list 102 deny icmp any any echo-reply
access-list 102 permit ip any any

access-list 104 permit tcp any any eq ftp
access-list 104 permit tcp any any eq ftp-data
access-list 104 deny tcp any any eq telnet
access-list 104 permit icmp any any echo
access-list 104 deny icmp any any echo-reply
access-list 104 permit ip any any

access-list 106 permit tcp any any eq ftp
access-list 106 permit tcp any any ftp-data
access-list 106 deny tcp any any eq telnet
access-list 106 permit icmp any any echo-reply
access-list 110 permit udp any any eq domain
access-list 110 permit udp any eq domain any
access-list 110 permit tcp any any eq domain
access-list 110 permit tcp any eq domain any
access-list 110 permit tcp any any

access-list 114 permit ip 10.4.4.0.0.0.255 any

access-list 115 permit ip 0.0.0.0 255.255.255.0 any

access-list 122 deny tcp any any
access-list 122 deny imp any any echo-reply
access-list 122 permit ip any any
!
```

<output omitted>

What would be the effect of Issuing the command ip access-group 115 in on the s0/0/1 interface?

- A. No host could connect to RouterC through s0/0/1.
- B. Telnet and ping would work but routing updates would fail.
- C. FTP, FTP-DATA, echo, and www would work but telnet would fail.
- D. Only traffic from the 10.4.4.0 network would pass through the interface.

**Answer: A**

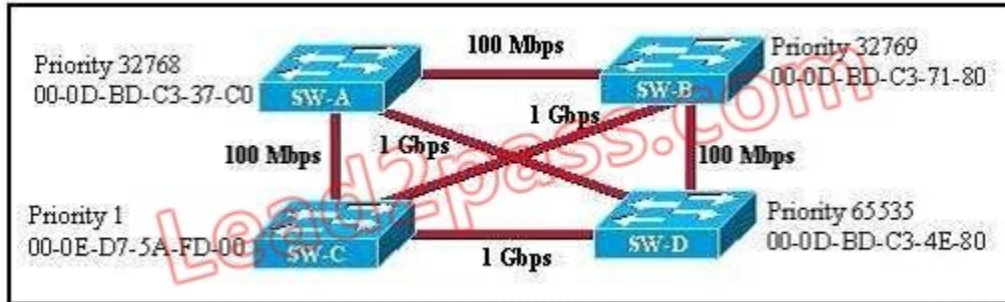
**Explanation:**

First let's see what was configured on interface S0/0/1:

```
interface Serial0/0/1
bandwidth 64
ip address 10.45.45.1 255.255.255.0
ip access-group 102 in
```

**QUESTION 259**

Refer to the exhibit. Based on the information given, which switch will be elected root bridge and why?



- A. Switch A, because it has the lowest MAC address
- B. Switch A, because it is the most centrally located switch
- C. Switch B, because it has the highest MAC address
- D. Switch C, because it is the most centrally located switch
- E. Switch C, because it has the lowest priority
- F. Switch D, because it has the highest priority

**Answer: E**

**QUESTION 260**

Lab

Simulation

Question

-

EIGRP



CCNA.com has a small network that is using EIGRP as its IGP. All routers should be running an EIGRP AS number of 12. Router MGT is also running static routing to the ISP.

CCNA.com has recently adding the ENG router. Currently, the ENG router does not have connectivity to the ISP router. All other interconnectivity and Internet access for the existing locations of the company are working properly.

**The task** is to identify the fault(s) and correct the router configuration(s) to provide full connectivity between the routers.

**Access to the router CLI can be gained by clicking on the appropriate host.**

All passwords on all routers are **cisco**.

IP addresses are listed in the chart below.

**MGT**

Fa0/0 - 192.168.77.33

S1/0 - 198.0.18.6

S0/0 - 192.168.27.9

S0/1 - 192.168.50.21

**ENG**

Fa0/0 - 192.168.77.34

Fa1/0 - 192.168.12.17

Fa0/1 - 192.168.12.1

**Parts1**

Fa0/0 - 192.168.12.33

Fa0/1 - 192.168.12.49

S0/0 - 192.168.27.10

**Parts2**

Fa0/0 - 192.168.12.65

Fa0/1 - 192.168.12.81

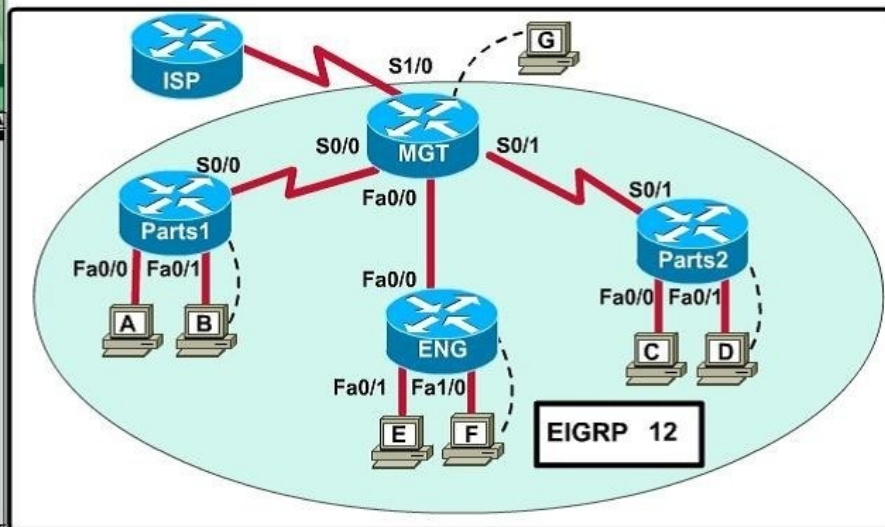
S0/1 - 192.168.50.22

Lead2pass.com



- You may need to scroll this window and the problem statement window.
- Click on picture of host connected to the specified router and select the CiscoTerminal option to configure the router. If you select the wrong host, click on the show topology

Hide Topology

**Answer:**

First we should check the configuration of the ENG Router.

Click the console PC "F" and enter the following commands.

```
ENG> enable
```

```
Password: cisco
```

```
ENG# show running-config
```

```
Building configuration...
```

```
Current configuration : 770 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname ENG
!
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
!
interface FastEthernet0/0
ip address 192.168.77.34 255.255.255.252
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.60.65 255.255.255.240
duplex auto
speed auto
!
interface FastEthernet1/0
ip address 192.168.60.81 255.255.255.240
duplex auto
speed auto
!
router eigrp 22
network 192.168.77.0
network 192.168.60.0
no auto-summary
!
ip classless
!
line con 0
line vty 0 4
login
!
end
ENG#
```

From the output above, we know that this router was wrongly configured with an autonomous number (AS) of 22. When the AS numbers among routers are mismatched, no adjacency is formed. (You should check the AS numbers on other routers for sure)

To solve this problem, we simply re-configure router ENG router with the following commands:

```
ENG# conf t
ENG(config)# no router eigrp 22
ENG(config)# router eigrp 12
ENG(config-router)# network 192.168.60.0
ENG(config-router)# network 192.168.77.0
ENG(config-router)# no auto-summary
ENG(config-router)# end
ENG# copy running-config startup-config
```

Second we should check the configuration of the MGT Router.

Click the console PC "G" and enter the following commands.

```
MGT> enable
Password: cisco
```

```
MGT# show running-config
Building configuration...
Current configuration : 1029 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname MGT
!
enable secret 5 $1$mERr$hX5rVt7rPNoS4wqbXKX7m0
!
interface FastEthernet0/0
ip address 192.168.77.33 255.255.255.252
duplex auto
speed auto
!
interface Serial0/0
ip address 192.168.36.13 255.255.255.252
clock rate 64000
!
interface Serial0/1
ip address 192.168.60.25 255.255.255.252
clock rate 64000
!
interface Serial1/0
ip address 198.0.18.6 255.255.255.252
!
interface Serial1/1
no ip address
shutdown
!
interface Serial1/2
no ip address
shutdown
!
interface Serial1/3
no ip address
shutdown
!
router eigrp 12
network 192.168.36.0
network 192.168.60.0
network 192.168.85.0
network 198.0.18.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 198.0.18.5
!
line con 0
line vty 0 4
login
!
```

end

MGT#

Notice that it is missing a definition to the network ENG. Therefore we have to add it so that it can recognize ENG router

MGT# conf t

MGT(config)# router eigrp 12

MGT(config-router)# network 192.168.77.0

MGT(config-router)# end

MGT# copy running-config startup-config

Now the whole network will work well. You should check again with ping command from router ENG to other routers!

In Short:

#### **ENG Router**

ENG>enable

Password: cisco ENG# conf t

ENG(config)# no router eigrp 22

ENG(config)# router eigrp 12

ENG(config-router)# network 192.168.60.0

ENG(config-router)# network 192.168.77.0

ENG(config-router)# no auto-summary

ENG(config-router)# end

ENG# copy running-config startup-config

#### **MGT Router**

MGT>enable

Password: cisco MGT# conf t

MGT(config)# router eigrp 12

MGT(config-router)# network 192.168.77.0

MGT(config-router)# end

MGT# copy running-config startup-config

#### **Some Modification in Question**

After adding ENG router, no routing updates are being exchanged between MGT and the new location. All other inter connectivity for the existing locations of the company are working properly. But Internet connection for existing location including Remote1 and Remote2 networks are not working.

Faults Identified:

1. Incorrect Autonomous System Number configured in ENG router.
2. MGT router does not advertise route to the new router ENG.
3. Internet Connection is not working all stations.

We need to correct the above two configuration mistakes to have full connectivity

Steps:

1. ENG Router: Change the Autonomous System Number of ENG
2. Perimeter Router: Add the network address of interface of Perimeter that link between MGT and ENG.
3. Perimeter Router: Add default route and default-network.

Check the IP Address of S1/0 interface of MGT Router using show running-config command. (The interface used to connect to the ISP)

!

interface Serial1/0

ip address 198.0.18.6 255.255.255.252

!

For Internet sharing we have create a default route, and add default-network configuration. The IP address is 198.0.18.6/30. Then the next hop IP will be 198.0.18.5.

#### **ENG Router**

ENG>enable

Password: cisco ENG# conf t

```
ENG(config)# no router eigrp 22
ENG(config)# router eigrp 12
ENG(config-router)# network 192.168.60.0
ENG(config-router)# network 192.168.77.0
ENG(config-router)# no auto-summary
ENG(config-router)# end
ENG# copy running-config startup-config

MGT Router
MGT>enable
Password: cisco MGT# conf t
MGT(config)# router eigrp 12
MGT(config-router)# network 192.168.77.0
MGT(config-router)# exit
MGT(config)# ip route 0.0.0.0 0.0.0.0 198.0.18.5
MGT(config)# ip default-network 198.0.18.0
MGT(config)# exit
MGT# copy running-config startup-config
```

**Important:**

If you refer the topology and IP chart, the MGT router uses Fa0/0 to connect ENG router, S0/0 used to connect Remote1, and S0/1 used to connect Remote2.

Refer to the command show running-config, the command #PASSIVE-INTERFACE <Interface Name> will deny EIGRP updates to specified interface. In that case we need to use #no passive-interface <Interface Name> to allow the routing updates to be passed to that interface. For example when used the #show run command and we see the output like below.

```
!
router eigrp 22
network 192.168.77.0
network 192.168.60.0
passive-interface FastEthernet 0/0
passive-interface Serial 1/0
no auto-summary
!
```

Then the command would be

```
MGT(config)#router eigrp 12
MGT(config-router)#no passive-interface Fa0/0
MGT(config-router)#end
```

Also MGT router connect to the ISP router using Serial 1/0. If you see passive-interface s1/0, then do not remove it using #no passive-interface s1/0 command.

**QUESTION 261**

Lab Simulation Question - CLI

Central Florida Widgets recently installed a new router in their office. Complete the network installation by performing the initial router configurations and configuring R1PV2 routing using the router command line interface (CLI) on the RC.

Configure the router per the following requirements:

- Name of the router is R2
- Enable.secret password is cisco
- The password to access user EXEC mode using the console is cisco2
- The password to allow telnet access to the router is cisco3

IPv4 addresses must be configured as follows:

- Ethernet network 209.165.201.0/27 - router has fourth assignable host address in subnet
- Serial network is 192.0.2.176/28 - router has last assignable host address in the subnet.

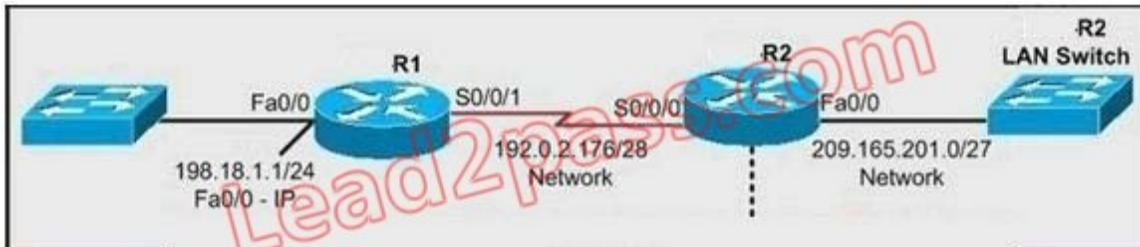


- Interfaces should be enabled.
- Router protocol is RIPv2

**Attention:**

In practical examinations, please note the following, the actual information will prevail.

1. Name of the router is xxx
2. EnableE. secret password is xxx
3. Password In access user EXEC mode using the console is xxx
4. The password to allow telnet access to the router is xxx
5. IP information



**Answer:**

**Step 1:**

Click on the console host, you will get a pop-up screen CLI of Router.

Router>

Configure the new router as per the requirements provided in Lab question

Requirement 1:

Name of the router is R2

**Step 2:**

To change the hostname of the router to R2 follow the below steps:

Router>

Router>enable

Router#configure terminal

Router(config)#hostname R2

R2(config)#

Requirement 2:

Enable-secret password is cisco1

**Step 3:**

To set the enable secret password to cisco1 use the following command

R2(config)#enable secret cisco1

Requirement 3:

The password to access user EXEC mode using the console is cisco2

**Step 4:**

We need to configure the line console 0 with the password cisco2

Also remember to type login command after setting up the password on line con 0 which allows router to accept logins via console.

R2(config)#line con 0

R2(config-line)#password cisco2

R2(config-line)#login

R2(config-line)#exit

R2(config)#

Requirement 4:

The password to allow telnet access to the router is cisco3

**Step 5:**

To allow telnet access we need to configure the vty lines 0 4 with the password cisco3

Also remember to type login command after setting up the password on line vty 0 4 which allows router to accept logins via telnet.

R2(config)#line vty 0 4

R2(config-line)#password cisco3

```
R2(config-line)#login
R2(config-line)#exit
R2(config)#
```

Requirement 5:

(5.1) Ethernet network 209.165.201.0 /27 - Router has the fourth assignable host address in subnet.

(5.2) Serial Network is 192.0.2.176 /28 - Router has the last assignable host address in subnet.

**Step 6:**

Ethernet network 209.165.201.0 /27 - Router has the fourth assignable host address in subnet.

Ethernet Interface on router R2 is Fast Ethernet 0/0 as per the exhibit

First we need to identify the subnet mask

Network: 209.165.201.0 /27

Subnet mask: /27: 27 bits = 8 + 8 + 8 + 3

=8(bits).8(bits).8(bits).11100000 (3bits)

=255.255.255.11100000

=11100000 = 128+64+32+0+0+0+0+0

= 224

Subnet mask: 255.255.255.224

Different subnet networks and their valid first and last assignable host address range for above subnet mask are

Subnet Networks :::: Valid Host address range :::: Broadcast address

209.165.201.0 :::: 209.165.201.1 - 209.165.201.30 :::: 209.165.201.31

209.165.201.32 :::: 209.165.201.33 - 209.165.201.62 :::: 209.165.201.63

209.165.201.64 :::: 209.165.201.65 - 209.165.201.94 :::: 209.165.201.95

209.165.201.96 :::: 209.165.201.97 - 209.165.201.126 :::: 209.165.201.127

209.165.201.128 :::: 209.165.201.129 - 209.165.201.158 :::: 209.165.201.159

209.165.201.160 :::: 209.165.201.161 - 209.165.201.190 :::: 209.165.201.191

209.165.201.192 :::: 209.165.201.193 - 209.165.201.222 :::: 209.165.201.223

209.165.201.224 :::: 209.165.201.225 - 209.165.201.254 :::: 209.165.201.255

Use above table information for network 209.165.201.0 /27 to identify

First assignable host address: 209.165.201.1

Last assignable host address: 209.165.201.30

Fourth assignable host address: 209.165.201.4

This IP address (209.165.201.4) which we need to configure on Fast Ethernet 0/0 of the router using the subnet mask 255.255.255.224

```
R2(config)#interface fa 0/0
```

```
R2(config-if)#ip address 209.165.201.4 255.255.255.224
```

Requirement 6:

To enable interfaces

Use no shutdown command to enable interfaces

```
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
```

**Step 7:**

Serial Network is 192.0.2.176 /28 - Router has the last assignable host address in subnet.

Serial Interface on R2 is Serial 0/0/0 as per the exhibit

First we need to identify the subnet mask

Network: 192.0.2.176 /28

Subnet mask: /28: 28bits = 8bits+8bits+8bits+4bits

=8(bits).8(bits).8(bits).11110000 (4bits)

=255.255.255.11110000

=11110000 = 128+64+32+16+0+0+0+0

= 240

Subnet mask: 255.255.255.240

Different subnet networks and their valid first and last assignable host address range for above subnet mask are

Subnet Networks :::: Valid Host address :::: Broadcast address

192.0.2.0 ::::: 192.0.2.1 - 192.0.2.14 ::::: 192.0.2.15  
192.0.2.16 ::::: 192.0.2.17 - 192.0.2.30 ::::: 192.0.2.31  
192.0.2.32 ::::: 192.0.2.33 - 192.0.2.46 ::::: 192.0.2.47  
192.0.2.48 ::::: 192.0.2.49 - 192.0.2.62 ::::: 192.0.2.64  
192.0.2.64 ::::: 192.0.2.65 - 192.0.2.78 ::::: 192.0.2.79  
192.0.2.80 ::::: 192.0.2.81 - 192.0.2.94 ::::: 192.0.2.95  
192.0.2.96 ::::: 192.0.2.97 - 192.0.2.110 ::::: 192.0.2.111  
192.0.2.112 ::::: 192.0.2.113 - 192.0.2.126 ::::: 192.0.2.127  
192.0.2.128 ::::: 192.0.2.129 - 192.0.2.142 ::::: 192.0.2.143  
192.0.2.144 ::::: 192.0.2.145 - 192.0.2.158 ::::: 192.0.2.159  
192.0.2.160 ::::: 192.0.2.161 - 192.0.2.174 ::::: 192.0.2.175  
192.0.2.176 ::::: 192.0.2.177 - 192.0.2.190 ::::: 192.0.2.191  
and so on ...

Use above table information for network 192.0.2.176 /28 to identify

First assignable host address: 192.0.2.177

Last assignable host address: 192.0.2.190

We need to configure Last assignable host address (192.0.2.190) on serial 0/0/0 using the subnet mask 255.255.255.240

```
R2(config)#interface serial 0/0/0
```

```
R2(config-if)#ip address 192.0.2.190 255.255.255.240
```

**Requirement 6:**

To enable interfaces

Use no shutdown command to enable interfaces

```
R2(config-if)#no shutdown
```

```
R2(config-if)#exit
```

**Requirement 7:**

Router protocol is RIPv2

**Step 8:**

Need to enable RIPv2 on router and advertise its directly connected networks

```
R2(config)#router rip
```

To enable RIP v2 routing protocol on router use the command version 2

```
R2(config-router)#version 2
```

Optional: no auto-summary (Since LAB networks do not have discontinuous networks)

RIP v2 is classless, and advertises routes including subnet masks, but it summarizes routes by default.

So the first things we need to do when configuring RIP v2 is turn off auto-summarization with the router command no auto-summary if you must perform routing between disconnected subnets.

```
R2 (config-router) # no auto-summary
```

Advertise the serial 0/0/0 and fast Ethernet 0/0 networks into RIP v2 using network command

```
R2(config-router)#network 192.0.2.176
```

```
R2(config-router)#network 209.165.201.0
```

```
R2(config-router)#end
```

**Step 9:**

Important please do not forget to save your running-config to startup-config

```
R2# copy running-config startup-config
```

## **QUESTION 262**

Lab Simulation Question - ACL-4

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

The task is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".

The Core connection uses an IP address of 198.18.196.65

The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254.

- o host A 192.168.33.1
- o host B 192.168.33.2
- o host C 192.168.33.3
- o host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30

The Finance Web Server is assigned an IP address of 172.22.242.23



**Answer:**

```
Corp1>enable
Corp1#configure terminal
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host
172.22.242.23 eq 80
Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80
Corp1(config)#access-list 100 permit ip any any
Corp1(config)#interface fa 0/1 sh ip int brief
Corp1(config-if)#ip access-group 100 out
Corp1(config-if)#end
Corp1#copy running-config startup-config
```

**Explanation:**

Select the console on Corp1 router

Configuring ACL

Corp1>enable

Corp1#configure terminal

Comment: To permit only Host C (192.168.33.3){source addr} to access finance server address

(172.22.242.23) {destination addr} on port number 80 (web)

```
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host  
172.22.242.23 eq 80
```

Comment: To deny any source to access finance server address (172.22.242.23) {destination addr} on port number 80 (web)

```
Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80
```

Comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.

```
Corp1(config)#access-list 100 permit ip any any
```

Applying the ACL on the Interface

Comment: Check show ip interface brief command to identify the interface type and number by checking the IP address configured.

```
Corp1(config)#interface fa 0/1
```

If the ip address configured already is incorrect as well as the subnet mask. this should be corrected in order ACL to work type this commands at interface mode :

no ip address 192.x.x.x 255.x.x.x (removes incorrect configured ipaddress and subnet mask)

Configure Correct IP Address and subnet mask:

```
ip address 172.22.242.30 255.255.255.240 ( range of address specified going to server is given as  
172.22.242.17 - 172.22.242.30 )
```

Comment: Place the ACL to check for packets going outside the interface towards the finance web server.

```
Corp1(config-if)#ip access-group 100 out
```

```
Corp1(config-if)#end
```

Important: To save your running config to startup before exit.

```
Corp1#copy running-config startup-config
```

Verifying the Configuration:

Step1: show ip interface brief command identifies the interface on which to apply access list. Step2: Click on each host A,B,C & D . Host opens a web browser page , Select address box of the web browser and type the ip address of finance web server(172.22.242.23) to test whether it permits /deny access to the finance web Server .

Step 3: Only Host C (192.168.33.3) has access to the server . If the other host can also access then maybe something went wrong in your configuration . check whether you configured correctly and in order.

Step 4: If only Host C (192.168.33.3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

### **QUESTION 263**

Lab Simulation Question - ACL-2



A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

**The task** is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.



Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".  
The Core connection uses an IP address of 198.18.247.65.  
The computers in the Hosts LAN have been assigned addresses of 192.168.240.1 - 192.168.240.254.

- o host A 192.168.240.1
- o host B 192.168.240.2
- o host C 192.168.240.3

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".  
The Core connection uses an IP address of 198.18.247.65.  
The computers in the Hosts LAN have been assigned addresses of 192.168.240.1 - 192.168.240.254.

- o host A 192.168.240.1
- o host B 192.168.240.2
- o host C 192.168.240.3

**Answer:**

```
Corp1#conf t
Corp1(config)# access-list 128 permit tcp host 192.168.240.1 host
172.22.141.26 eq www Corp1(config)# access-list 128 deny tcp any host
172.22.141.26 eq www
Corp1(config)# access-list 128 permit ip any any
Corp1(config)#int fa0/1
Corp1(config-if)#ip access-group 128 out
Corp1(config-if)#end
Corp1#copy run startup-config
```

**QUESTION 264**

Lab Simulation Question - ACL-3



A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

**The task** is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.

Access to the router CLI can be gained by clicking on the appropriate host.

All passwords have been temporarily set to "cisco".

The Core connection uses an IP address of 198.18.196.65

The computers in the Hosts LAN have been assigned addresses of 192.168.33.1 - 192.168.33.254.

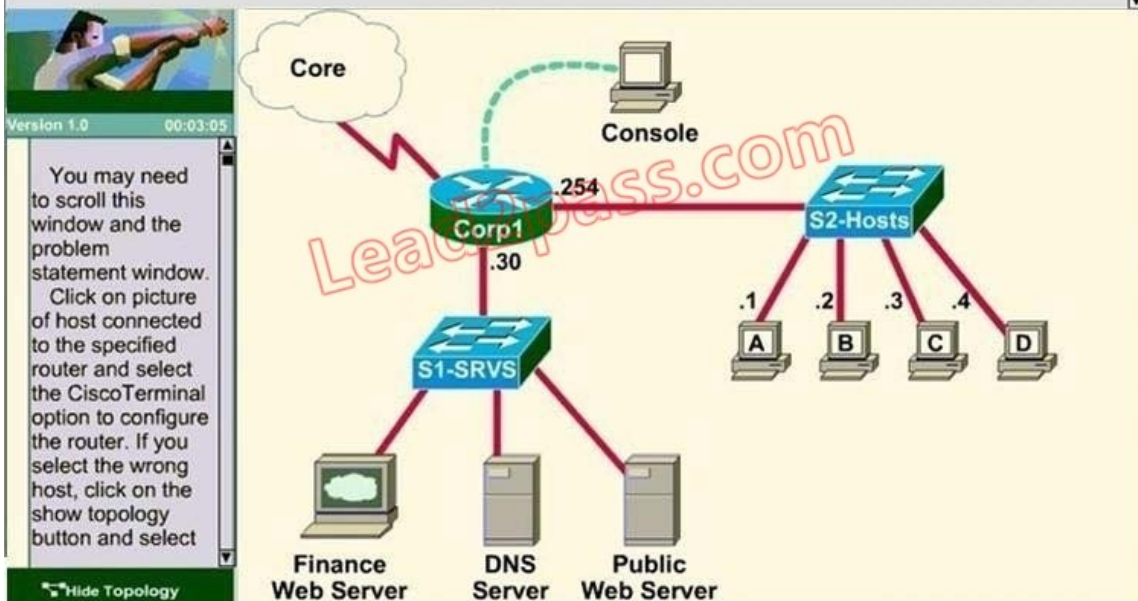
- o host A 192.168.33.1
- o host B 192.168.33.2
- o host C 192.168.33.3
- o host D 192.168.33.4

The servers in the Server LAN have been assigned addresses of 172.22.242.17 - 172.22.242.30

The Finance Web Server is assigned an IP address of 172.22.242.23

A network associate is adding security to the configuration of the Corp1 router. The user on host C should be able to use a web browser to access financial information from the Finance Web Server. No other hosts from the LAN nor the Core should be able to use a web browser to access this server. Since there are multiple resources for the corporation at this location including other resources on the Finance Web Server, all other traffic should be allowed.

**The task** is to create and apply an access-list with no more than three statements that will allow ONLY host C web access to the Finance Web Server. No other hosts will have web access to the Finance Web Server. All other traffic is permitted.



**Answer:**

```
Corp1>enable
Corp1#configure terminal
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host
172.22.242.23 eq 80
Corp1(config)#access-list 100 deny tcp 192.168.33.0 0.0.0.255 host
172.22.242.23 eq 80
Corp1(config)#access-list 100 permit ip any any
Corp1(config)#interface fa 0/1 sh ip int brief
Corp1(config-if)#ip access-group 100 out
Corp1(config-if)#end
Corp1#copy running-config startup-config
```

**Explanation:**

Select the console on Corp1 router

Configuring ACL

Corp1 >enable

Corp1#configure terminal

comment: To permit only Host C (192.168. 33. 3){source addr} to access finance server address (172.22. 242. 23){destination addr} on port number 80 (web)

```
Corp1(config)#access-list 100 permit tcp host 192.168.33.3 host 172.22.242.23 eq 80
```

Comment: To deny any source to access finance server address (172. 22. 242. 23) {destination addr} on port number 80 (web)

```
Corp1(config)#access-list 100 deny tcp any host 172.22.242.23 eq 80
```

Comment: To permit ip protocol from any source to access any destination because of the implicit deny any any statement at the end of ACL.

```
Corp1(config)#access-list 100 permit ip any any
```

Applying the ACL on the Interface

comment: Check show ip interface brief command to identify the interface type and number by checking the IP address configured.

```
Corp1(config)#interface fa 0/1
```

If the ip address configured already is incorrect as well as the subnet mask, this should be corrected in order ACL to work type this commands at interface mode :

no ip address 192. x. x. x 255. x. x. x (removes incorrect configured ip address and subnet mask)

Configure Correct IP Address and subnet mask:

ip address 172. 22. 242. 30 255. 255. 255. 240 (range of address specified going to server is given as 172. 22. 242. 17-172. 22. 242. 30 )

Comment: Place the ACL to check for packets going outside the interface towards the finance web server.

```
Corp1(config-if)#ip access-group 100 out
```

```
Corp1(config-if)#end
```

Important: To save your running config to startup before exit.

```
Corp1#copy running-config startup- config
```

Verifying the Configuration:

Step1: show ip interface brief command identifies the interface on which to apply access list. Step2: Click on each host A,B,C & D. Host opens a web browser page, Select address box of the web browser and type the ip address of finance web server(172. 22. 242. 23) to test whether it permits /deny access to the finance web Server.

Step 3: Only Host C (192.168. 33. 3) has access to the server. If the other host can also access then maybe something went wrong in your configuration check whether you configured correctly and in order.

Step 4: If only Host C (192.168. 33. 3) can access the Finance Web Server you can click on NEXT button to successfully submit the ACL SIM.

**QUESTION 265**

Lab Simulation Question - NAT-1

The following have already been configured on the router:

- The basic router configuration
- The appropriate interfaces have been configured for NAT inside and NAT outside.
- The appropriate static routes have also been configured (since the company will be a stub network, no routing protocol will be required)
- All passwords have been temporarily set to "cisco".

The task is to complete the NAT configuration using all IP addresses assigned by the ISP to provide Internet access for the hosts in the Weaver LAN. Functionality can be tested by clicking on the host provided for testing.

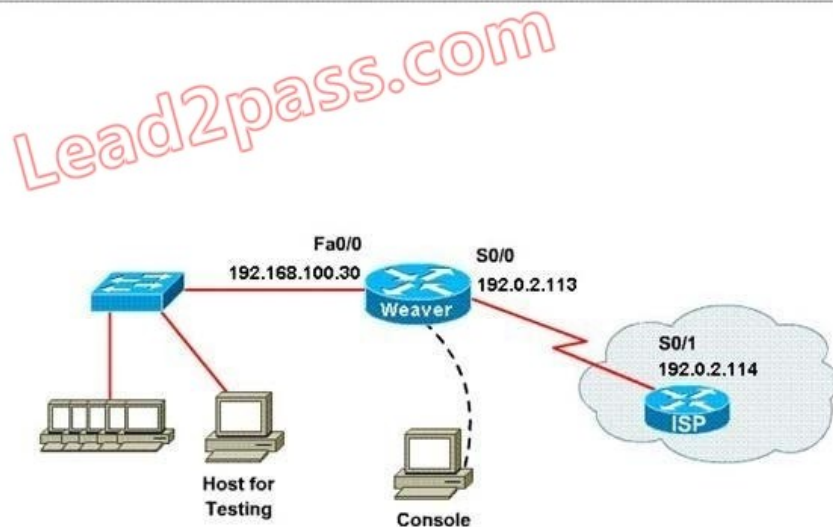
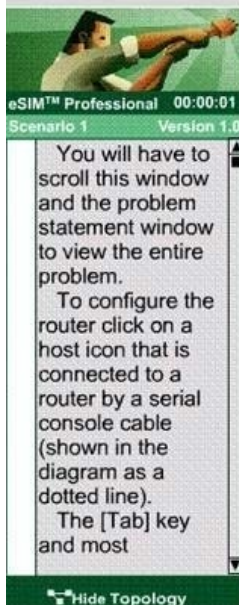
Configuration information

router name - Weaver

inside global addresses-198.18.184.105 198.18.184.110/29

inside local addresses - 192.168.100.17 - 192.168.100.30/28

number of inside hosts - 14



A network associate is configuring a router for the weaver company to provide internet access. The ISP has provided the company six public IP addresses of 198.18.184.105 198.18.184.110. The company has 14 hosts that need to access the internet simultaneously. The hosts in the company LAN have been assigned private space addresses in the range of 192.168.100.17 ?192.168.100.30.

**Answer:**

The company has 14 hosts that need to access the internet simultaneously but we just have 6 public IP addresses from 198.18.184.105 to 198.18.184.110/29.

Therefore we have to use NAT overload (or PAT)

Double click on the Weaver router to open it

```
Router>enable
```

```
Router#configure terminal
```

First you should change the router's name to Weaver

```
Router(config)#hostname Weaver
```

Create a NAT pool of global addresses to be allocated with their netmask.

```
Weaver(config)#ip nat pool mypool 198.18.184.105 198.18.184.110 netmask 255.255.255.248
```

Create a standard access control list that permits the addresses that are to be translated

```
Weaver(config)#access-list 1 permit 192.168.100.16 0.0.0.15
```

Establish dynamic source translation, specifying the access list that was defined in the prior step

```
Weaver(config)#ip nat inside source list 1 pool mypool overload
```

This command translates all source addresses that pass access list 1, which means a source address from 192.168.100.17 to 192.168.100.30, into an address from the pool named mypool (the pool contains addresses from 198.18.184.105 to 198.18.184.110)

Overload keyword allows to map multiple IP addresses to a single registered IP address (many-to-one) by using different ports

The question said that appropriate interfaces have been configured for NAT inside and NAT outside statements.

This is how to configure the NAT inside and NAT outside, just for your understanding:

```
Weaver(config)#interface fa0/0
Weaver(config-if)#ip nat inside
Weaver(config-if)#exit
Weaver(config)#interface s0/0
Weaver(config-if)#ip nat outside
Weaver(config-if)#end
```

Finally, we should save all your work with the following command:

```
Weaver#copy running-config startup-config
```

Check your configuration by going to "Host for testing" and type:

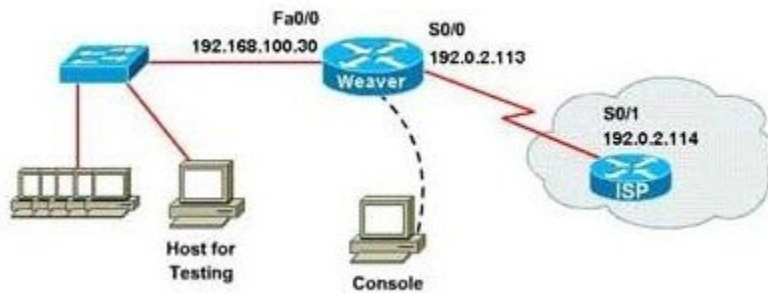
```
C:\>ping 192.0.2.114
```

The ping should work well and you will be replied from 192.0.2.114

### QUESTION 266

#### Lab Simulation Question - NAT-2

A network associate is configuring a router for the Weaver company to provide internet access. The ISP has provided the company six public IP addresses of 198.18.184.105 - 198.18.184.110. The company has 14 hosts that need to access the internet simultaneously. The hosts in the company LAN have been assigned private space addresses in the range of 192.168.100.17 - 192.168.100.30.



The following have already been configured on the router:

- The basic router configuration
- The appropriate interfaces have been configured for NAT inside and NAT outside
- The appropriate static routes have also been configured (since the company will be a stub network, no routing protocol will be required.)
- All passwords have been temporarily set to "cisco"

The task is to complete the NAT configuration using all IP addresses assigned by the ISP to provide internet access for the hosts in the weaver LAN. Functionality can be tested by clicking on the host provided for testing.

Configuration information:

```
Router name      - Weaver
Inside global addresses - 198.18.184.105 - 198.18.184.110 /29
Inside local addresses   - 192.168.100.17 - 192.168.100.30 /28
```



Number of inside hosts - 14

**Answer:**

**Step 1: Router Name**

```
Router>enable
Router#configure terminal
Router(config)#hostname Weaver
Weaver(config)#
```

**Step 2: NAT Configuration**

```
Weaver(config)#access-list 10 permit 192.168.100.16 0.0.0.15
Weaver(config)#ip nat pool mynatpool 198.18.184.105 198.18.184.110
netmask 255.255.255.248
Weaver(config)#ip nat inside source list 10 pool mynatpool overload
Weaver(config)#end
```

**Step 3: Save Configuration**

```
Weaver#copy run start
```

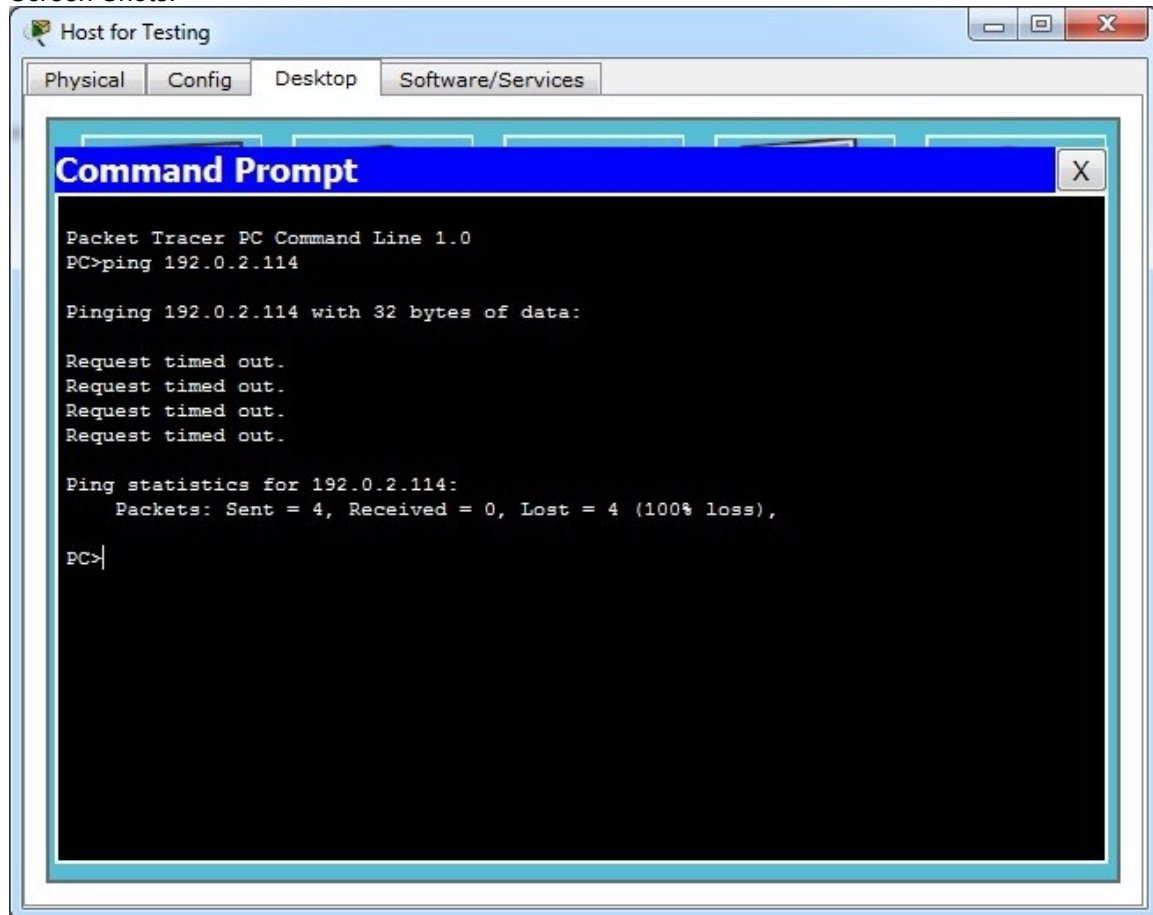
**Verification:**

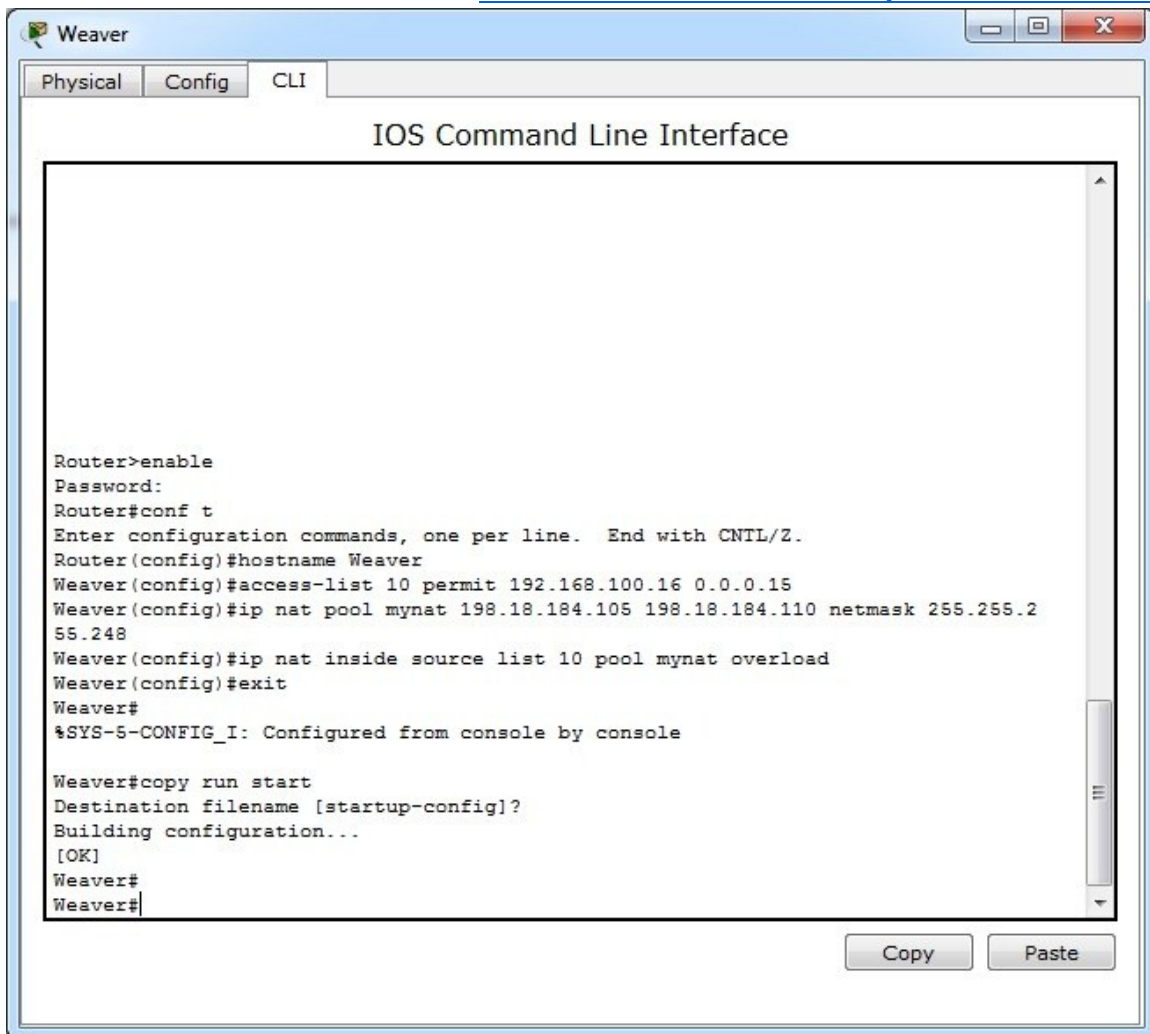
We can verify the answer by pinging the ISP IP Address (192.0.2.114) from Host for testing.

Click "Host for testing"

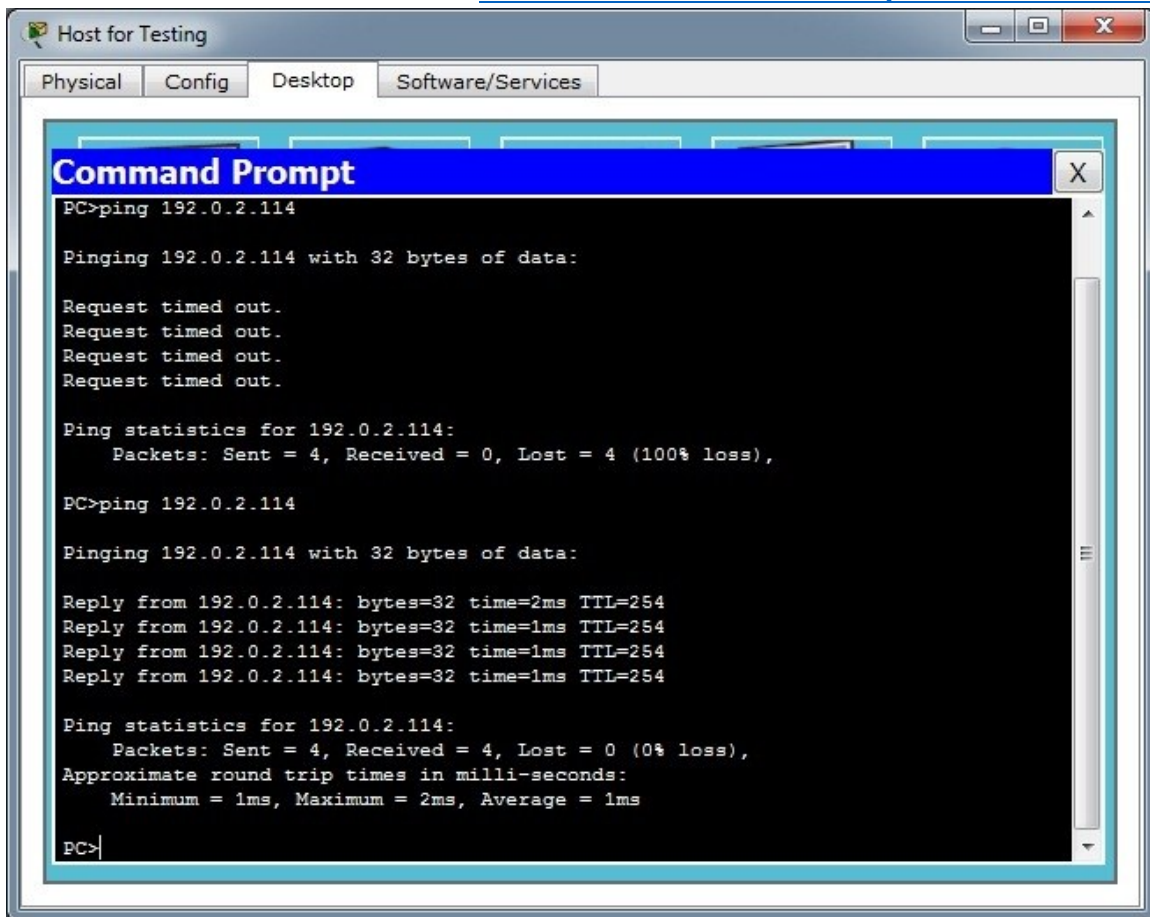
In command prompt, type "ping 192.0.2.114". If ping succeeded then the NAT is working properly.

Screen Shots:









```
Host for Testing
Physical Config Desktop Software/Services

Command Prompt
PC>ping 192.0.2.114

Pinging 192.0.2.114 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.0.2.114:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>ping 192.0.2.114

Pinging 192.0.2.114 with 32 bytes of data:

Reply from 192.0.2.114: bytes=32 time=2ms TTL=254
Reply from 192.0.2.114: bytes=32 time=1ms TTL=254
Reply from 192.0.2.114: bytes=32 time=1ms TTL=254
Reply from 192.0.2.114: bytes=32 time=1ms TTL=254

Ping statistics for 192.0.2.114:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms

PC>
```

**QUESTION 267**

In a switched environment, what does the IEEE 802.1Q standard describe?

- A. the operation of VTP
- B. a method of VLAN trunking
- C. an approach to wireless LAN communication
- D. the process for root bridge selection
- E. VLAN pruning

**Answer: B**

**Explanation:**

A broadcast domain must sometimes exist on more than one switch in the network. To accomplish this, one switch must send frames to another switch and indicate which VLAN a particular frame belongs to. On Cisco switches, a trunk link is created to accomplish this VLAN identification. ISL and IEEE 802.1Q are different methods of putting a VLAN identifier in a Layer 2 frame. The IEEE 802.1Q protocol interconnects VLANs between multiple switches, routers, and servers. With 802.1Q, a network administrator can define a VLAN topology to span multiple physical devices. Cisco switches support IEEE 802.1Q for FastEthernet and Gigabit Ethernet interfaces. An 802.1Q trunk link provides VLAN identification by adding a 4-byte tag to an Ethernet Frame as it leaves a trunk port.

**QUESTION 268**

What are three benefits of GLBP? (Choose three.)

- A. GLBP supports up to eight virtual forwarders per GLBP group.
- B. GLBP supports clear text and MD5 password authentication between GLBP group members.
- C. GLBP is an open source standardized protocol that can be used with multiple vendors.
- D. GLBP supports up to 1024 virtual routers.
- E. GLBP can load share traffic across a maximum of four routers.
- F. GLBP elects two AVGs and two standby AVGs for redundancy.

**Answer: BDE**

**QUESTION 269**

Which three statements about HSRP operation are true? (Choose three.)

- A. The virtual IP address and virtual MAC address are active on the HSRP Master router.
- B. The HSRP default timers are a 3 second hello interval and a 10 second dead interval.
- C. HSRP supports only clear-text authentication.
- D. The HSRP virtual IP address must be on a different subnet than the routers' interfaces on the same LAN.
- E. The HSRP virtual IP address must be the same as one of the router's interface addresses on the LAN.
- F. HSRP supports up to 255 groups per interface, enabling an administrative form of load balancing.

**Answer: ABF**

**Explanation:**

The virtual MAC address of HSRP version 1 is 0000.0C07.ACxx, where xx is the HSRP group number in hexadecimal based on the respective interface. For example, HSRP group 10 uses the HSRP virtual MAC address of 0000.0C07.AC0A. HSRP version 2 uses a virtual MAC address of 0000.0C9F.FXXX (XXX: HSRP group in hexadecimal)

**QUESTION 270**

Which three statements about Syslog utilization are true? (Choose three.)

- A. Utilizing Syslog improves network performance.
- B. The Syslog server automatically notifies the network administrator of network problems.
- C. A Syslog server provides the storage space necessary to store log files without using router disk space.
- D. There are more Syslog messages available within Cisco IOS than there are comparable SNMP trap messages.
- E. Enabling Syslog on a router automatically enables NTP for accurate time stamping.
- F. A Syslog server helps in aggregation of logs and alerts.

**Answer: CDF**

**QUESTION 271**

A network administrator enters the following command on a router: logging trap 3. What are three message types that will be sent to the Syslog server? (Choose three.)

- A. informational
- B. emergency
- C. warning
- D. critical
- E. debug
- F. error

**Answer: BDF**

**QUESTION 272**

What is the default Syslog facility level?

- A. local4
- B. local5
- C. local6
- D. local7

**Answer: D**

**QUESTION 273**

What command instructs the device to timestamp Syslog debug messages in milliseconds?

- A. service timestamps log datetime localtime
- B. service timestamps debug datetime msec
- C. service timestamps debug datetime localtime
- D. service timestamps log datetime msec

**Answer: B**

**Explanation:**

The "service timestamps debug" command configures the system to apply a time stamp to debugging messages. The time-stamp format for datetime is MMM DD HH:MM:SS, where MMM is the month, DD is the date, HH is the hour (in 24-hour notation), MM is the minute, and SS is the second. With the additional keyword msec, the system includes milliseconds in the time stamp, in the format HH:DD:MM:SS.mmm, where .mmm is milliseconds

**QUESTION 274**

Refer to the exhibit. What is the cause of the Syslog output messages?

```
*Mar 01, 00:37:57.3737: %SYS-5-CONFIG_I: Configured from console by console
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down
%DUAL-5-NBRCHANGE: IP-EIGRP 1: Neighbor 10.10.11.2 (FastEthernet0/1) is down: interface down
```

- A. The EIGRP neighbor on Fa0/1 went down due to a failed link.
- B. The EIGRP neighbor connected to Fa0/1 is participating in a different EIGRP process, causing the adjacency to go down.
- C. A shut command was executed on interface Fa0/1, causing the EIGRP adjacency to go down.
- D. Interface Fa0/1 has become error disabled, causing the EIGRP adjacency to go down.

**Answer: C**

**QUESTION 275**

What are three components that comprise the SNMP framework? (Choose three.)

- A. MIB
- B. agent
- C. set
- D. AES
- E. supervisor
- F. manager

**Answer: ABF**

**QUESTION 276**

What are three components that comprise the SNMP framework? (Choose three.)

- A. MIB
- B. agent
- C. set
- D. AES
- E. supervisor
- F. manager

**Answer: ABF**

**QUESTION 277**

What SNMP message alerts the manager to a condition on the network?

- A. response
- B. get
- C. trap
- D. capture

**Answer: C**

**QUESTION 278**

What authentication type is used by SNMPv2?

- A. HMAC-MD5
- B. HMAC-SHA
- C. CBC-DES
- D. community strings

**Answer: D**

**QUESTION 279**

Which three statements about the features of SNMPv2 and SNMPv3 are true? (Choose three.)

- A. SNMPv3 enhanced SNMPv2 security features.
- B. SNMPv3 added the Inform protocol message to SNMP.
- C. SNMPv2 added the Inform protocol message to SNMP.
- D. SNMPv3 added the GetBulk protocol messages to SNMP.
- E. SNMPv2 added the GetBulk protocol message to SNMP.
- F. SNMPv2 added the GetNext protocol message to SNMP.

**Answer: ACE**

**QUESTION 280**

What are three reasons to collect Netflow data on a company network? (Choose three.)

- A. To identify applications causing congestion.

- B. To authorize user network access.
- C. To report and alert link up / down instances.
- D. To diagnose slow network performance, bandwidth hogs, and bandwidth utilization.
- E. To detect suboptimal routing in the network.
- F. To confirm the appropriate amount of bandwidth that has been allocated to each Class of Service.

**Answer:** ADF

**QUESTION 281**

What Netflow component can be applied to an interface to track IPv4 traffic?

- A. flow monitor
- B. flow record
- C. flow sampler
- D. flow exporter

**Answer:** A

**Explanation:**

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the record, which is configured for the flow monitor and stored in the flow monitor cache.

For example, the following example creates a flow monitor named FLOW-MONITOR-1 and enters Flexible NetFlow flow monitor configuration mode:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)#
```

**QUESTION 282**

What Cisco IOS feature can be enabled to pinpoint an application that is causing slow network performance?

- A. SNMP
- B. Netflow
- C. WCCP
- D. IP SLA

**Answer:** B

**QUESTION 283**

What command visualizes the general NetFlow data on the command line?

- A. show ip flow export
- B. show ip flow top-talkers
- C. show ip cache flow
- D. show mls sampling
- E. show mls netflow ip

**Answer:** C

**Explanation:**

The "show ip cache flow" command displays a summary of the NetFlow

```
GATEWAY#show ip cache flow
IP packet size distribution (1149 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .134 .475 .100 .010 .006 .037 .043 .005 .001 .004 .001 .002 .001 .000

   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .003 .000 .001 .020 .147 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  13 active, 4083 inactive, 378 added
  7046 age polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  13 active, 1011 inactive, 378 added, 378 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
```

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-WMW	32	0.0	8	989	0.1	3.8	8.1
TCP-other	24	0.0	2	57	0.0	2.2	14.4
UDP-other	309	0.1	2	105	0.3	2.4	15.4
Total:	365	0.1	3	318	0.4	2.5	14.7

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Fa0/0	10.0.0.23	Null	10.255.255.255	11	0089	0089	9
Fa0/0	10.0.0.30	Null	10.255.255.255	11	008A	008A	1

#### QUESTION 284

What are three values that must be the same within a sequence of packets for Netflow to consider them a network flow? (Choose three.)

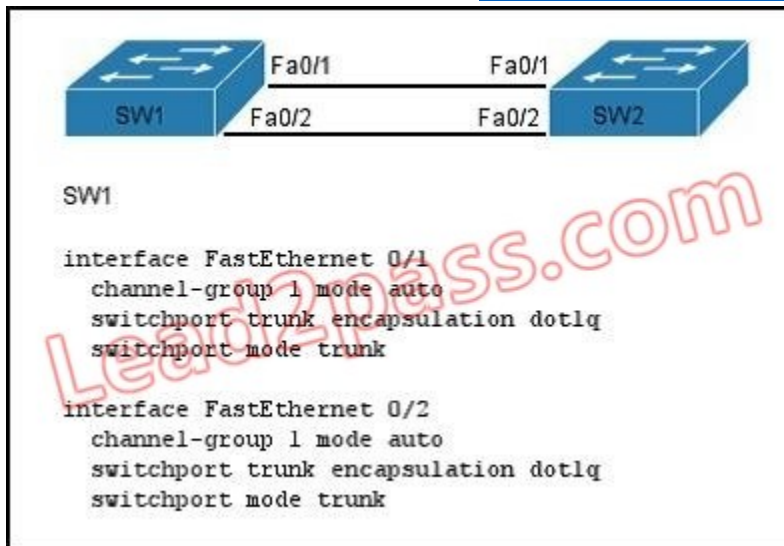
- A. source IP address
- B. source MAC address
- C. egress interface
- D. ingress interface
- E. destination IP address
- F. IP next-hop

**Answer:** ADE

#### QUESTION 285

Refer to the exhibit. A network administrator is configuring an EtherChannel between SW1 and SW2. The SW1 configuration is shown. What is the correct configuration for SW2?





- A. interface FastEthernet 0/1  
channel-group 1 mode active  
switchport trunk encapsulation dot1q  
switchport mode trunk  
interface FastEthernet 0/2  
channel-group 1 mode active  
switchport trunk encapsulation dot1q  
switchport mode trunk
- B. interface FastEthernet 0/1  
channel-group 2 mode auto  
switchport trunk encapsulation dot1q  
switchport mode trunk  
interface FastEthernet 0/2  
channel-group 2 mode auto  
switchport trunk encapsulation dot1q  
switchport mode trunk
- C. interface FastEthernet 0/1  
channel-group 1 mode desirable  
switchport trunk encapsulation dot1q  
switchport mode trunk  
interface FastEthernet 0/2  
channel-group 1 mode desirable  
switchport trunk encapsulation dot1q  
switchport mode trunk
- D. interface FastEthernet 0/1  
channel-group 1 mode passive  
switchport trunk encapsulation dot1q  
switchport mode trunk  
interface FastEthernet 0/2  
channel-group 1 mode passive  
switchport trunk encapsulation dot1q  
switchport mode trunk

**Answer: C**

**QUESTION 286**

What are three factors a network administrator must consider before implementing Netflow in the network? (Choose three.)

- A. CPU utilization
- B. where Netflow data will be sent
- C. number of devices exporting Netflow data
- D. port availability
- E. SNMP version
- F. WAN encapsulation

**Answer: ABC**

**QUESTION 287**

Which two statements about the OSPF Router ID are true? (Choose two.)

- A. It identifies the source of a Type 1 LSA.
- B. It should be the same on all routers in an OSPF routing instance.
- C. By default, the lowest IP address on the router becomes the OSPF Router ID.
- D. The router automatically chooses the IP address of a loopback as the OSPF Router ID.
- E. It is created using the MAC Address of the loopback interface.

**Answer: AD**

**QUESTION 288**

What parameter can be different on ports within an EtherChannel?

- A. speed
- B. DTP negotiation settings
- C. trunk encapsulation
- D. duplex

**Answer: B**

**QUESTION 289**

What are two benefits of using a single OSPF area network design? (Choose two.)

- A. It is less CPU intensive for routers in the single area.
- B. It reduces the types of LSAs that are generated.
- C. It removes the need for virtual links.
- D. It increases LSA response times.
- E. It reduces the number of required OSPF neighbor adjacencies.

**Answer: BC**

**QUESTION 290**

Refer to the exhibit. What set of commands was configured on interface Fa0/3 to produce the given output?

```
FastEthernet0/3:
Port state      = 1
Channel group   = 2          Mode = Passive      Gcchange = -
Port-channel    = Po2       GC      = -          Pseudo port-channel = Po2
Port index      = 0         Load = 0x00       Protocol  = LACP
```

- A. interface FastEthernet 0/3  
channel-group 1 mode desirable  
switchport trunk encapsulation dot1q  
switchport mode trunk
- B. interface FastEthernet 0/3  
channel-group 2 mode passive  
switchport trunk encapsulation dot1q  
switchport mode trunk
- C. interface FastEthernet 0/3  
channel-group 2 mode active  
switchport trunk encapsulation dot1q  
switchport mode trunk
- D. interface FastEthernet 0/3  
channel-group 2 mode on  
switchport trunk encapsulation dot1q  
switchport mode trunk

**Answer: B**

### QUESTION 291

Refer to the exhibit. If the devices produced the given output, what is the cause of the EtherChannel problem?

```
SW1#show etherchannel summary
Flags: D - down      P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3     S - Layer2
       U - in use     f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----
1      Po1(SU)         -           Fa0/2(P) Fa0/1(D)
```

```
SW1#show interface fa0/1
FastEthernet0/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 0060.5c11.9501
(bia 0060.5c11.9501)
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes);
    Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

```
SW2#show etherchannel summary
Flags: D - down      P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3     S - Layer2
       U - in use     f - failed to allocate aggregator
       u - unsuitable for bundling
       w - waiting to be aggregated
       d - default port

Number of channel-groups in use: 2
Number of aggregators:          2

Group  Port-channel  Protocol    Ports
-----
1      Po1(SU)         -           Fa0/2(P) Fa0/1(D)
```

```
SW2#show interface fa0/1
FastEthernet0/1 is down, line protocol is down (disabled)
Hardware is Lance, address is 00d0.97a7.7901
(bia 00d0.97a7.7901)
MTU 1500 bytes, BW 100000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:08, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes);
    Total output drops: 0
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
```

- A. SW1's Fa0/1 interface is administratively shut down.
- B. There is an encapsulation mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.
- C. There is an MTU mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.
- D. There is a speed mismatch between SW1's Fa0/1 and SW2's Fa0/1 interfaces.

**Answer: D**

**QUESTION 292**

What are two enhancements that OSPFv3 supports over OSPFv2? (Choose two.)

- A. It requires the use of ARP.
- B. It can support multiple IPv6 subnets on a single link.
- C. It supports up to 2 instances of OSPFv3 over a common link.
- D. It routes over links rather than over networks.

**Answer: BD**

**QUESTION 293**

When a router undergoes the exchange protocol within OSPF, in what order does it pass through each state?

- A. exstart state > loading state > exchange state > full state
- B. exstart state > exchange state > loading state > full state
- C. exstart state > full state > loading state > exchange state
- D. loading state > exchange state > full state > exstart state

**Answer: B**

**QUESTION 294**

A network administrator creates a layer 3 EtherChannel, bundling four interfaces into channel group

1. On what interface is the IP address configured?

- A. the port-channel 1 interface
- B. the highest number member interface
- C. all member interfaces
- D. the lowest number member interface

**Answer: A**

**QUESTION 295**

Refer to the exhibit. If the router Cisco returns the given output and has not had its router ID set manually, what value will OSPF use as its router ID?

```
Cisco#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet0/1	172.16.1.1	YES	manual	up	up
Loopback0	1.1.1.1	YES	manual	up	up
Loopback1	2.2.2.2	YES	manual	up	up
Vlan1	unassigned	YES	unset	administratively down	down

- A. 192.168.1.1
- B. 172.16.1.1
- C. 1.1.1.1
- D. 2.2.2.2

**Answer: D**

**QUESTION 296**

What command sequence will configure a router to run OSPF and add network 10.1.1.0/24 to area 0?

- A. router ospf area 0  
network 10.1.1.0 255.255.255.0 area 0
- B. router ospf  
network 10.1.1.0 0.0.0.255
- C. router ospf 1  
network 10.1.1.0 0.0.0.255 area 0
- D. router ospf area 0  
network 10.1.1.0 0.0.0.255 area 0
- E. router ospf  
network 10.1.1.0 255.255.255.0 area 0
- F. router ospf 1  
network 10.1.1.0 0.0.0.255

**Answer: C**

**QUESTION 297**

What OSPF command, when configured, will include all interfaces into area 0?

- A. network 0.0.0.0 255.255.255.255 area 0
- B. network 0.0.0.0 0.0.0.0 area 0
- C. network 255.255.255.255 0.0.0.0 area 0
- D. network all-interfaces area 0

**Answer: A**

**QUESTION 298**

Which statement describes the process ID that is used to run OSPF on a router?

- A. It is globally significant and is used to represent the AS number.
- B. It is locally significant and is used to identify an instance of the OSPF database.
- C. It is globally significant and is used to identify OSPF stub areas.
- D. It is locally significant and must be the same throughout an area.

**Answer: B**

**QUESTION 299**

Which three are the components of SNMP? (Choose three)

- A. MIB
- B. SNMP Manager
- C. SysLog Server
- D. SNMP Agent
- E. Set

**Answer: ABD**

**Explanation:**

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

The SNMP framework has three parts:

- + An SNMP manager
- + An SNMP agent
- + A Management Information Base (MIB)

The SNMP manager is the system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on such a device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

The SNMP agent is the software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a Cisco routing device, you must define the relationship between the manager and the agent.

The Management Information Base (MIB) is a virtual information storage area for network management information, which consists of collections of managed objects.

**QUESTION 300**

What are the Popular destinations for syslog messages to be saved?

- A. Flash
- B. The logging buffer .RAM
- C. The console terminal
- D. Other terminals
- E. Syslog server

**Answer: BCE**

**Explanation:**

By default, switches send the output from system messages and debug privileged EXEC commands to a logging process. The logging process controls the distribution of logging messages to various destinations, such as the logging buffer (on RAM), terminal lines (console terminal), or a



UNIX syslog server, depending on your configuration. The process also sends messages to the console.

Note: Syslog messages can be written to a file in Flash memory although it is not a popular place to use. We can configure this feature with the command logging file flash:filename.

[Visit PassLeader and Download Full Version 200-125 Exam Dumps](#)