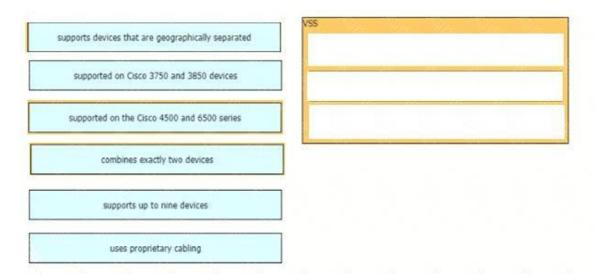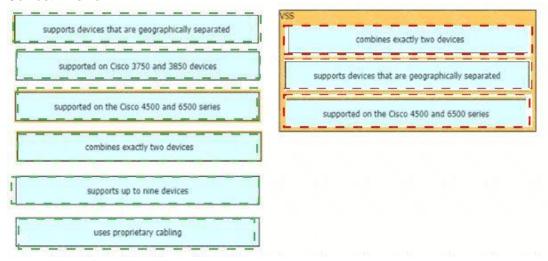**QUESTION 288**
DRAG DROP
Drag and drop the descriptions of the VSS technology from the left to the right. Not all options are used.

supports devices that are geographically separated	VSS
supported on Cisco 3750 and 3850 devices	
supported on the Cisco 4500 and 6500 series	
combines exactly two devices	
supports up to nine devices	
uses proprietary cabling	

Correct Answer:

supports devices that are geographically separated	VSS
supported on Cisco 3750 and 3850 devices	combines exactly two devices
supported on the Cisco 4500 and 6500 series	supports devices that are geographically separated
combines exactly two devices	supported on the Cisco 4500 and 6500 series
supports up to nine devices	
uses proprietary cabling	

QUESTION 289
How do stratum levels relate to the distance from a time source?

A. Stratum 1 devices are connected directly to an authoritative time source.
B. Stratum 15 devices are connected directly to an authoritative time source
C. Stratum 0 devices are connected directly to an authoritative time source.
D. Stratum 15 devices are an authoritative time source.

Correct Answer: C

QUESTION 290
The login method is configured on the VTY lines of a router with these parameters:

■The first method for authentication is TACACS
■If TACACS is unavailable, login is allowed without any provided credentials

Which configuration accomplishes this task?

A. R1#sh run | include aaa
    aaa new-model
    aaa authentication login VTY group tacacs+ none
    aaa session-id common
    R1#sh run | section vty
    line vty 0 4
    password 7 0202039485748
    R1#sh run | include username
    R1#
B. R1#sh run | include aaa
    aaa new-model
    aaa authentication login telnet group tacacs+ none
    aaa session-id common
    R1#sh run | section vty
    line vty 0 4
    R1#sh run | include username
    R1#
C. R1#sh run | include aaa
    aaa new-model
    aaa authentication login default group tacacs+ none
    aaa session-id common
    R1#sh run | section vty
    line vty 0 4
    password 7 0202039485748
D. R1#sh run | include aaa
    aaa new-model
    aaa authentication login default group tacacs+
    aaa session-id common
    R1#sh run | section vty
    line vty 0 4
    transport input none
    R1#

Correct Answer: C
Explanation:
According to the requirements (first use TACACS+, then allow login with no authentication), we have to use "aaa authentication login ... group tacacs+ none" for AAA command.

The next thing to check is the if the "aaa authentication login default" or "aaa authentication login list-name " is used. The `default' keyword means we want to apply for all login connections (such as tty, vty, console and aux). If we use this keyword, we don't need to configure anything else under tty, vty and aux lines. If we don't use this keyword then we have to specify which line(s) we want to apply the authentication feature.

From above information, we can find out answer

R1#sh run | include aaa
aaa new-model

aaa authentication login default group tacacs+ none

aaa session-id common

R1#sh run | section vty

line vty 0 4

password 7 0202039485748

If you want to learn more about AAA configuration, please read our AAA TACACS+ and RADIUS

Tutorial - Part 2.

For your information, answer 'R1#sh run | include aaa

aaa new-model

aaa authentication login telnet group tacacs+ none

aaa session-id common

R1#sh run | section vty

line vty 0 4

R1#sh run | include username

R1#' would be correct if we add the following command under vty line ("line vty 0 4"): "login
authentication telnet" ("telnet" is the name of the AAA list above)

QUESTION 291
Which line must be added in the Python function to return the JSON object {"cat_9k":
"FXS193202SE")?

```
Import json
def get_data():
    test_json = """
    {
        "response": [{
        "managementIpAddress": "10.10.2.253",
        "memorySize": "3398345152",
        "serialNumber": "FXS1932Q2SE",
        "softwareVersion": "16.3.2",
        "hostname": "cat_9k"
    }],
        "version": "1.0"
    }
    """
```

A. return (json.dumps({d['hostname']: d['serialNumber'] for d in json.loads(test_json)['response']}))

B. return (json.dumps({for d in json.loads(test_json)['response']: d['hostname']: d['serialNumber']}))

C. return (json.loads({d['hostname']: d['serialNumber'] for d in json.dumps(test_json)['response']}))

D. return (json.loads({for d in json.dumps(test_json)['response']: d['hostname']: d['serialNumber']}))

Correct Answer: D

QUESTION 292
Refer to the exhibit. Which command must be applied to Router 1 to bring the GRE tunnel to an up/up state?

```
Router1#
Router1#show run int tunnel 0
Building configuration...

Current configuration : 95 bytes
!
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel destination 192.168.10.2
end


Router1#show ip int br
Interface            IP-Address      OK? Method Status                 Protocol
GigabitEthernet0/0   192.168.1.1     YES manual up                     up
GigabitEthernet0/1   unassigned      YES unset  administratively down  down
GigabitEthernet0/2   unassigned      YES unset  administratively down  down
GigabitEthernet0/3   unassigned      YES unset  administratively down  down
Loopback0            192.168.10.1    YES manual up                     up
Tunnel0              172.16.1.1      YES manual up                     down
Router1#
```

A. Router1(config-if)#tunnel mode gre multipoint
B. Router1(config-if)#tunnel source Loopback0
C. Router1(config-if)#tunnel source GigabitEthernet0/1
D. Router1(config)#interface tunnel0

Correct Answer: B

QUESTION 293
A network engineer is enabling HTTPS access to the core switch, which requires a certificate to be installed on the switch signed by the corporate certificate authority. Which configuration commands are required to issue a certificate signing request from the core switch?

A. Core-Switch(config)#**crypto pki enroll Core-Switch**
    Core-Switch(config)#**ip http secure-trustpoint Core-Switch**

B. Core-Switch(config)#**crypto pki trustpoint Core-Switch**
    Core-Switch(ca-trustpoint)#**enrollment terminal**
    Core-Switch(config)#**crypto pki enroll Core-Switch**

C. Core-Switch(config)#**crypto pki trustpoint Core-Switch**
    Core-Switch(ca-trustpoint)#**enrollment terminal**
    Core-Switch(config)#**ip http secure-trustpoint Core-Switch**

D. Core-Switch(config)#**ip http secure-trustpoint Core-Switch**
    Core-Switch(config)#**crypto pki enroll Core-Switch**

Correct Answer: B

QUESTION 294
A vulnerability assessment highlighted that remote access to the switches is permitted using unsecure and unencrypted protocols. Which configuration must be applied to allow only secure and reliable remote access for device administration?

A. line vty 0 15
    login local
    transport input none
B. line vty 0 15
    login local
    transport input telnet ssh
C. line vty 0 15
    login local
    transport input ssh
D. line vty 0 15
    login local
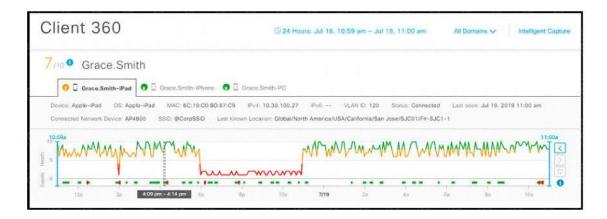   transport input all

Correct Answer: C

QUESTION 295
How do the RIB and the FIB differ?

A. FIB contains routes learned through a dynamic routing protocol, and the RIB contains routes that are static or directly connected.
B. RIB contains the interface for a destination, and the FIB contains the next hop information.
C. FIB is derived from the control plane, and the RIB is derived from the data plane.
D. RIB is derived from the control plane, and the FIB is derived from the RIB.

Correct Answer: D

QUESTION 296
Refer to the exhibit. Cisco DNA Center has obtained the username of the client and the multiple devices that the client is using on the network. How is Cisco DNA Center getting these context details?

A. The administrator had to assign the username to the IP address manually in the user database tool on Cisco DNA Center.
B. Those details are provided to Cisco DNA Center by the Identity Services Engine
C. Cisco DNA Center pulled those details directly from the edge node where the user connected.
D. User entered those details in the Assurance app available on iOS and Android devices