[Updated Constantly]

HERE

CCNA 2 (v5.1 + v6.0) Chapter 5 Exam Answers Full

How to find: Press “Ctrl + F” in the browser and fill in whatever wording is in the question to find that question/answer.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. **Which statement describes the port speed LED on the Cisco Catalyst 2960 switch?**
   - **If the LED is green, the port is operating at 100 Mb/s.***
   - If the LED is off, the port is not operating.
   - If the LED is blinking green, the port is operating at 10 Mb/s.
   - If the LED is amber, the port is operating at 1000 Mb/s.

   The port speed LED indicates that the port speed mode is selected. When selected, the port LEDs will display colors with different meanings. If the LED is off, the port is operating at 10 Mb/s. If the LED is green, the port is operating at 100 Mb/s. If the LED is blinking green, the port is operating at 1000 Mb/s.
2. **Which command is used to set the BOOT environment variable that defines where to find the IOS image file on a switch?**
   - config-register
   - **boot system***
   - boot loader
   - confreg

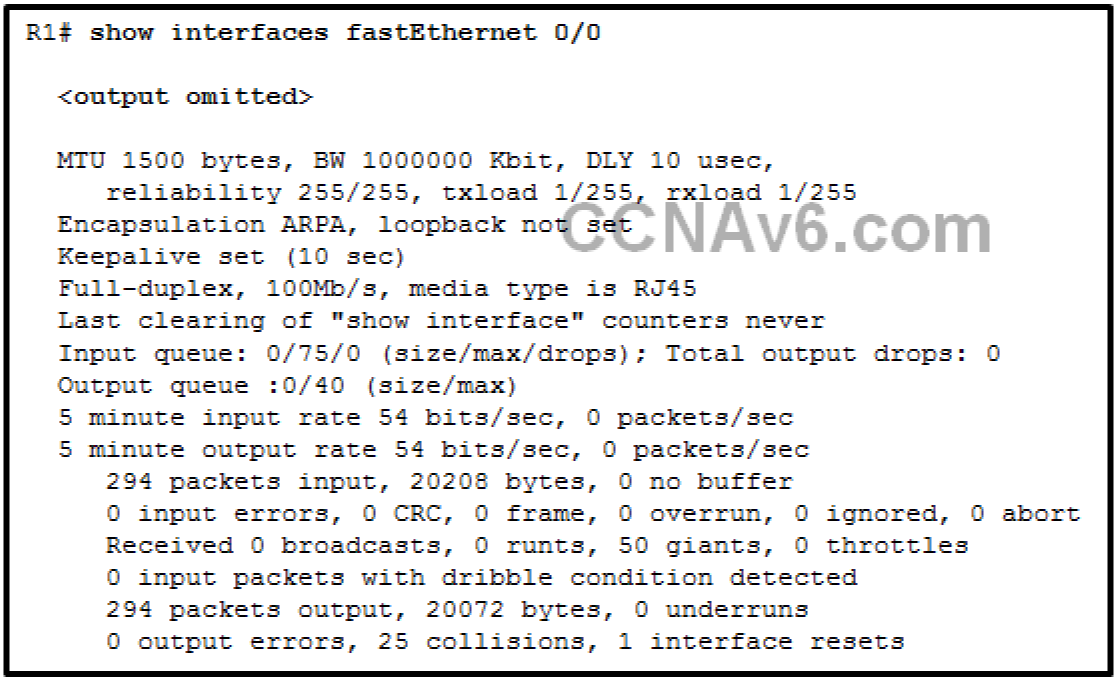
   The boot system command is used to set the BOOT environment variable. The config-register and confreg commands are used to set the configuration register. The boot loader command supports commands to format the flash file system, reinstall the operating system software, and recover from a lost or forgotten password.
3. **What is a function of the switch boot loader?**
   - to speed up the boot process
   - to provide security for the vulnerable state when the switch is booting
   - to control how much RAM is available to the switch during the boot process
   - **to provide an environment to operate in when the switch operating system cannot be found***

   The switch boot loader environment is presented when the switch cannot locate a valid operating system. The boot loader environment provides a few basic commands that allows a network administrator to reload the operating system or provide an alternate location of the operating system.
4. **Which interface is the default location that would contain the IP address used to manage a 24-port Ethernet switch?**
   - **VLAN 1***
   - Fa0/0
   - Fa0/1

- interface connected to the default gateway
- VLAN 99

5. **A production switch is reloaded and finishes with a Switch> prompt. What two facts can be determined? (Choose two.)**
   - **POST occurred normally.***
   - The boot process was interrupted.
   - There is not enough RAM or flash on this router.
   - **A full version of the Cisco IOS was located and loaded.***
   - The switch did not locate the Cisco IOS in flash, so it defaulted to ROM.
6. **Which two statements are true about using full-duplex Fast Ethernet? (Choose two.)**
   - **Performance is improved with bidirectional data flow.***
   - Latency is reduced because the NIC processes frames faster.
   - Nodes operate in full-duplex with unidirectional data flow.
   - Performance is improved because the NIC is able to detect collisions.
   - **Full-duplex Fast Ethernet offers 100 percent efficiency in both directions.***
7. **In which situation would a technician use the show interfaces switch command?**
   - to determine if remote access is enabled
   - **when packets are being dropped from a particular directly attached host***
   - when an end device can reach local devices, but not remote devices
   - to determine the MAC address of a directly attached network device on a particular interface

   The show interfaces command is useful to detect media errors, to see if packets are being sent and received, and to determine if any runts, giants, CRCs, interface resets, or other errors have occurred. Problems with reachability to a remote network would likely be caused by a misconfigured default gateway or other routing issue, not a switch issue. The show mac address-table command shows the MAC address of a directly attached device.
8. **Refer to the exhibit. A network technician is troubleshooting connectivity issues in an Ethernet network with the command show interfaces fastEthernet 0/0. What conclusion can be drawn based on the partial output in the exhibit?**

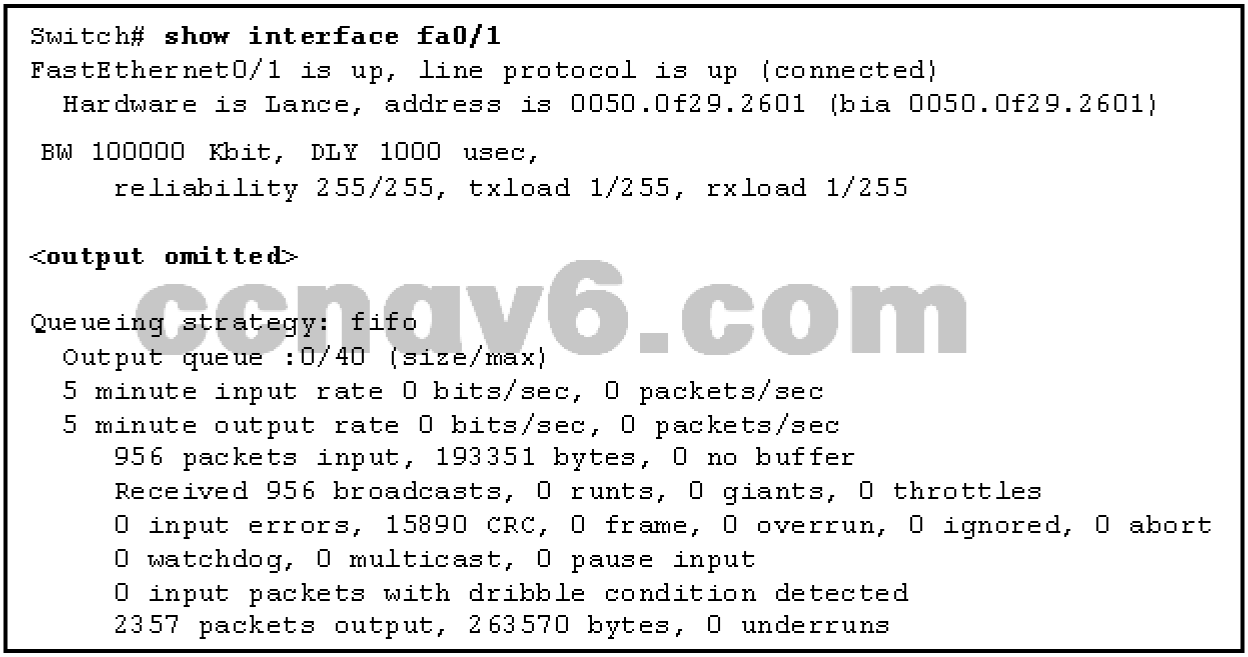


```
R1# show interfaces fastEthernet 0/0

  <output omitted>

  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is RJ45
  Last clearing of "show interface" counters never
  Input queue: 0/75/0 (size/max/drops); Total output drops: 0
  Output queue :0/40 (size/max)
  5 minute input rate 54 bits/sec, 0 packets/sec
  5 minute output rate 54 bits/sec, 0 packets/sec
     294 packets input, 20208 bytes, 0 no buffer
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     Received 0 broadcasts, 0 runts, 50 giants, 0 throttles
     0 input packets with dribble condition detected
     294 packets output, 20072 bytes, 0 underruns
     0 output errors, 25 collisions, 1 interface resets
```

- All hosts on this network communicate in full-duplex mode.
- Some workstations might use an incorrect cabling type to connect to the network.
- There are collisions in the network that cause frames to occur that are less than 64 bytes in length.
- **A malfunctioning NIC can cause frames to be transmitted that are longer than the allowed maximum length.***

The partial output shows that there are 50 giants (frames longer than the allowed maximum) that were injected into the network, possibly by a malfunctioning NIC. This conclusion can be drawn because there are only 25 collisions, so not all the 50 giants are the result of a collision. Also, because there 25 collisions, it is most likely that not all hosts are using full-duplex mode (otherwise there would not be any collisions). There should be no cabling issues since the CRC error value is 0. There are 0 runts, so the collisions have not caused malformed frames to occur that are shorter than 64 bytes in length .

9. **Refer to the exhibit. What media issue might exist on the link connected to Fa0/1 based on the show interface command?**



```
Switch# show interface fa0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Lance, address is 0050.0f29.2601 (bia 0050.0f29.2601)
 BW 100000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255

<output omitted>

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
     956 packets input, 193351 bytes, 0 no buffer
     Received 956 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 15890 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     2357 packets output, 263570 bytes, 0 underruns
```

- The bandwidth parameter on the interface might be too high.
- There could be an issue with a faulty NIC.
- **There could be too much electrical interference and noise on the link.***
- The cable attaching the host to port Fa0/1 might be too long.
- The interface might be configured as half-duplex.

Escalating CRC errors usually means that the data is being modified during transmission from the host to the switch. This is often caused by high levels of electromagnetic interference on the link.

10. **If one end of an Ethernet connection is configured for full duplex and the other end of the connection is configured for half duplex, where would late collisions be observed?**

- on both ends of the connection
- on the full-duplex end of the connection
- only on serial interfaces
- span style="color: red;">**on the half-duplex end of the connection***

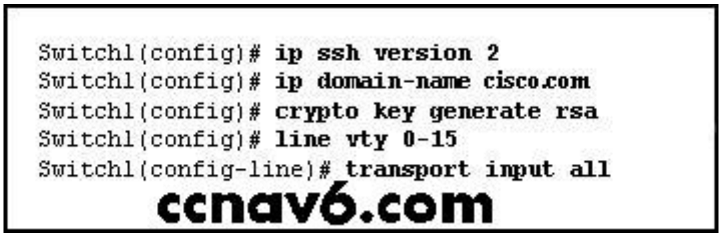
Full-duplex communications do not produce collisions. However, collisions often occur in half-duplex operations. When a connection has two different duplex configurations, the half-duplex end will experience late collisions. Collisions are found on Ethernet networks. Serial interfaces use technologies other than Ethernet.

11. **What is one difference between using Telnet or SSH to connect to a network device for management purposes?**

- Telnet uses UDP as the transport protocol whereas SSH uses TCP.
- Telnet does not provide authentication whereas SSH provides authentication.
- Telnet supports a host GUI whereas SSH only supports a host CLI.
- **Telnet sends a username and password in plain text, whereas SSH encrypts the username and password.***

SSH provides security for remote management connections to a network device. SSH does so through encryption for session authentication (username and password) as well as for data transmission. Telnet sends a username and password in plain text, which can be targeted to obtain the username and password through data capture. Both Telnet and SSH use TCP, support authentication, and connect to hosts in CLI.

12. **Refer to the exhibit. The network administrator wants to configure Switch1 to allow SSH connections and prohibit Telnet connections. How should the network administrator change the displayed configuration to satisfy the requirement?**



```
Switch1(config)# ip ssh version 2
Switch1(config)# ip domain-name cisco.com
Switch1(config)# crypto key generate rsa
Switch1(config)# line vty 0-15
Switch1(config-line)# transport input all
```

- Use SSH version 1.
- Reconfigure the RSA key.
- Configure SSH on a different line.
- **Modify the transport input command.***

13. **What is the effect of using the switchport port-security command?**

- **enables port security on an interface***
- enables port security globally on the switch
- automatically shuts an interface down if applied to a trunk port
- detects the first MAC address in a frame that comes into a port and places that MAC address in the MAC address table

Port security cannot be enabled globally. All active switch ports should be manually secured using the switchport port-security command, which allows the administrator to control the number of valid MAC addresses allowed to access the port. This command does not specify what action will be taken if a violation occurs, nor does it change the process of populating the MAC address table.

14. **Where are dynamically learned MAC addresses stored when sticky learning is enabled with the switchport port-security mac-address sticky command?**

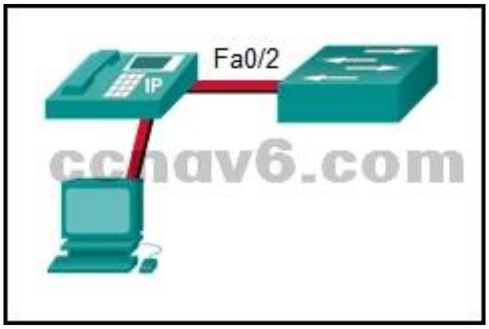
- ROM
- **RAM***
- NVRAM
- flash

When MAC addresses are automatically learned by using the sticky command option, the learned MAC addresses are added to the running configuration, which is stored in RAM.

15. **A network administrator configures the port security feature on a switch. The security policy specifies that each access port should allow up to two MAC addresses. When the maximum number of MAC addresses is reached, a frame with the unknown source MAC address is dropped and a notification is sent to the syslog server. Which security violation mode should be configured for each access port?**
    - **restrict***
    - protect
    - warning
    - shutdown

    In port security implementation, an interface can be configured for one of three violation modes:
    Protect – a port security violation causes the interface to drop packets with unknown source addresses and no notification is sent that a security violation has occurred.
    Restrict – a port security violation causes the interface to drop packets with unknown source addresses and to send a notification that a security violation has occurred.
    Shutdown – a port security violation causes the interface to immediately become error-disabled and turns off the port LED. No notification is sent that a security violation has occurred.
16. **Which two statements are true regarding switch port security? (Choose two.)**
    - The three configurable violation modes all log violations via SNMP.
    - **Dynamically learned secure MAC addresses are lost when the switch reboots.***
    - The three configurable violation modes all require user intervention to re-enable ports.
    - After entering the sticky parameter, only MAC addresses subsequently learned are converted to secure MAC addresses.
    - **If fewer than the maximum number of MAC addresses for a port are configured statically, dynamically learned addresses are added to CAM until the maximum number is reached.***
17. **Which action will bring an error-disabled switch port back to an operational state?**
    - Remove and reconfigure port security on the interface.
    - Issue the switchport mode access command on the interface.
    - Clear the MAC address table on the switch.
    - **Issue the shutdown and then no shutdown interface commands.***

    When a violation occurs on a switch port that is configured for port security with the shutdown violation action, it is put into the err-disabled state. It can be brought back up by shutting down the interface and then issuing the no shutdown command.
18. **Refer to the exhibit. Port Fa0/2 has already been configured appropriately. The IP phone and PC work properly. Which switch configuration would be most appropriate for port Fa0/2 if the network administrator has the following goals?**



No one is allowed to disconnect the IP phone or the PC and connect some other wired device.
If a different device is connected, port Fa0/2 is shut down.
The switch should automatically detect the MAC address of the IP phone and the PC and add those addresses to the running configuration.

- SWA(config-if)# switchport port-security
  SWA(config-if)# switchport port-security mac-address sticky
- SWA(config-if)# switchport port-security mac-address sticky
  SWA(config-if)# switchport port-security maximum 2
- **SWA(config-if)# switchport port-security**
  SWA(config-if)# switchport port-security maximum 2
  SWA(config-if)# switchport port-security mac-address sticky*
- SWA(config-if)# switchport port-security
  SWA(config-if)# switchport port-security maximum 2
  SWA(config-if)# switchport port-security mac-address sticky
  SWA(config-if)# switchport port-security violation restrict

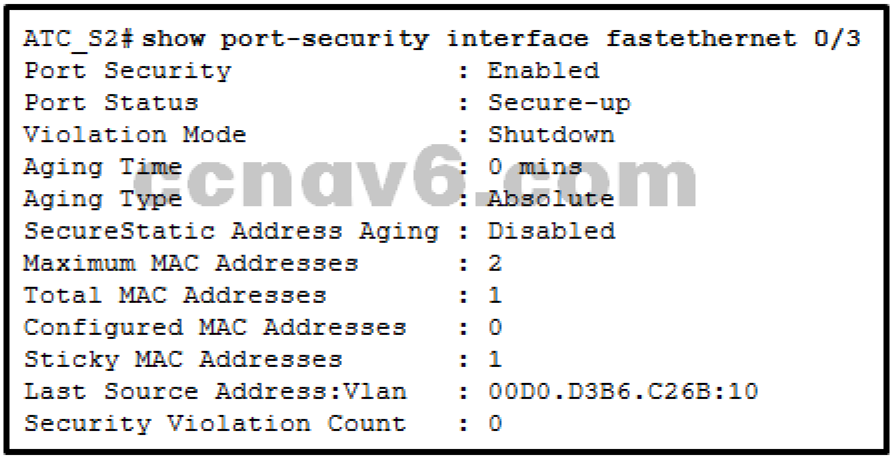
The default mode for a port security violation is to shut down the port so the switchport port-security violation command is not necessary. The switchport port-security command must be entered with no additional options to enable port security for the port. Then, additional port security options can be added.

19. **The following words are displayed:**

ATC_S2# show port-security interface fastethernet 0/3
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 2
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 00D0.D3B6.C26B:10
Security Violation Count : 0

Refer to the exhibit. What can be determined about port security from the information

that is shown?

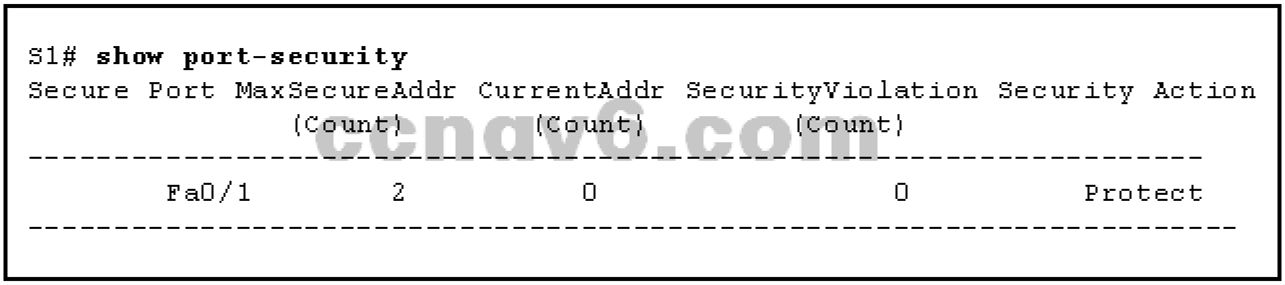


```
ATC_S2# show port-security interface fastethernet 0/3
Port Security               : Enabled
Port Status                 : Secure-up
Violation Mode              : Shutdown
Aging Time                  : 0 mins
Aging Type                  : Absolute
SecureStatic Address Aging  : Disabled
Maximum MAC Addresses       : 2
Total MAC Addresses         : 1
Configured MAC Addresses    : 0
Sticky MAC Addresses        : 1
Last Source Address:Vlan    : 00D0.D3B6.C26B:10
Security Violation Count    : 0
```

- The port has been shut down.
- The port has two attached devices.
- **The port violation mode is the default for any port that has port security enabled.***
- The port has the maximum number of MAC addresses that is supported by a Layer 2 switch port which is configured for port security.

The Port Security line simply shows a state of Enabled if the switchport port-security command (with no options) has been entered for a particular switch port. If a port security violation had occurred, a different error message appears such as Secure-shutdown. The maximum number of MAC addresses supported is 50. The Maximum MAC Addresses line is used to show how many MAC addresses can be learned (2 in this case). The Sticky MAC Addresses line shows that only one device has been attached and learned automatically by the switch. This configuration could be used when a port is shared by two cubicle-sharing personnel who bring in separate laptops.

20. **Refer to the exhibit. Which event will take place if there is a port security violation on switch S1 interface Fa0/1?**



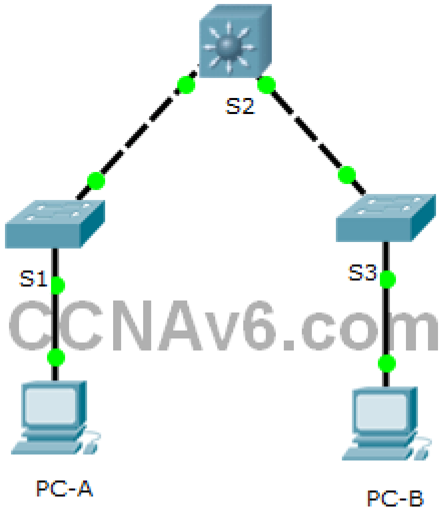
```
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)          (Count)
------------------------------------------------------------------------
       Fa0/1          2          0                0            Protect
--------------------------------------------------------------------------
```

- A notification is sent.
- A syslog message is logged.
- **Packets with unknown source addresses will be dropped.***
- The interface will go into error-disabled state.

Interface FastEthernet 0/1 is configured with the violation mode of protect. If there is a violation, interface FastEthernet 0/1 will drop packets with unknown MAC addresses.

21. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**
Which event will take place if there is a port security violation on switch S1 interface

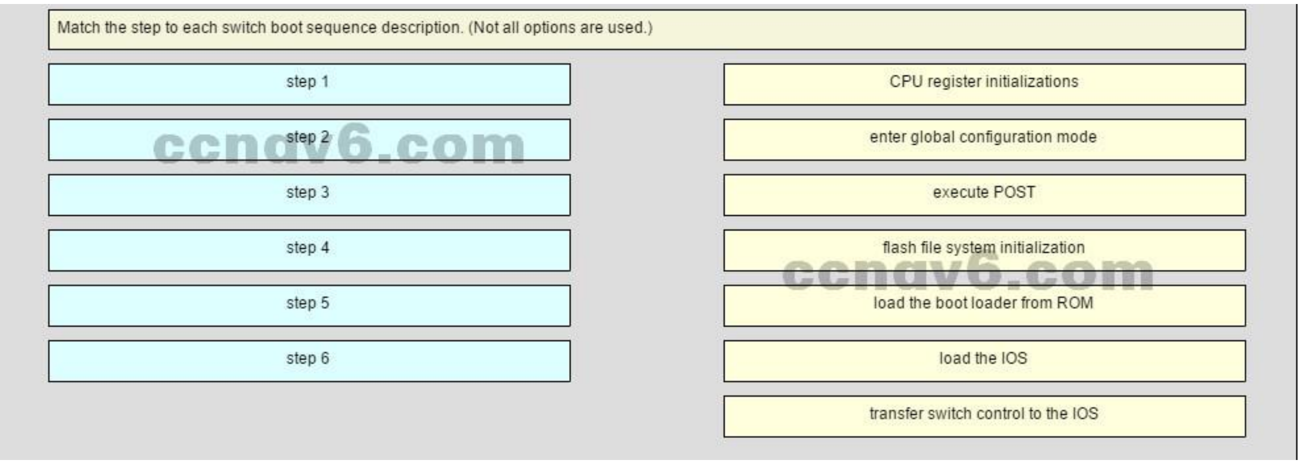
Fa0/1?



- **Packets with unknown source addresses will be dropped.**
- A syslog message is logged.
- The interface will go into error-disabled state.
- A notification is sent.

The violation mode can be viewed by issuing the show port-security interface command. Interface FastEthernet 0/1 is configured with the violation mode of protect. If there is a violation, interface FastEthernet 0/1 will drop packets with unknown MAC addresses.

22. **Fill in the blank.**
    Do not use abbreviations.What is the missing command on S1? “ **ip address 192.168.99.2 255.255.255.0** ”
23. **Match the step to each switch boot sequence description. (Not all options are used.)**


Match the step to each switch boot sequence description. (Not all options are used.)

step 1
step 2
step 3
step 4
step 5
step 6

CPU register initializations
enter global configuration mode
execute POST
flash file system initialization
load the boot loader from ROM
load the IOS
transfer switch control to the IOS

Place the options in the following order:

step 3

– not scored –

step 1

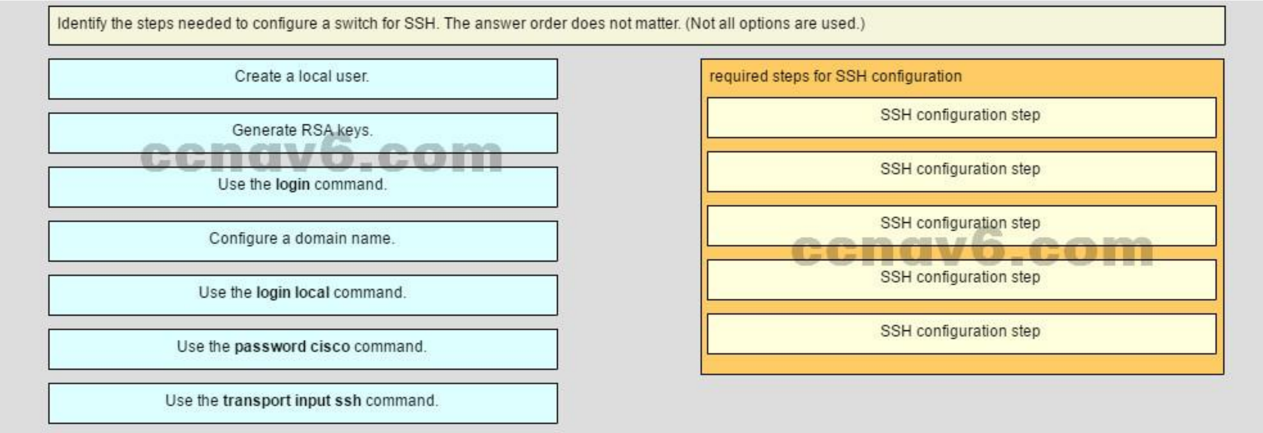
step 4

step 2

step 5
step 6

The steps are:
1. execute POST
2. load the boot loader from ROM
3. CPU register initializations
4. flash file system initialization
5. load the IOS
6. transfer switch control to the IOS

24. **Identify the steps needed to configure a switch for SSH. The answer order does not matter. (Not all options are used.)**



Identify the steps needed to configure a switch for SSH. The answer order does not matter. (Not all options are used.)

Create a local user.

Generate RSA keys.

Use the **login** command.

Configure a domain name.

Use the **login local** command.

Use the **password cisco** command.

Use the **transport input ssh** command.

required steps for SSH configuration

SSH configuration step

SSH configuration step

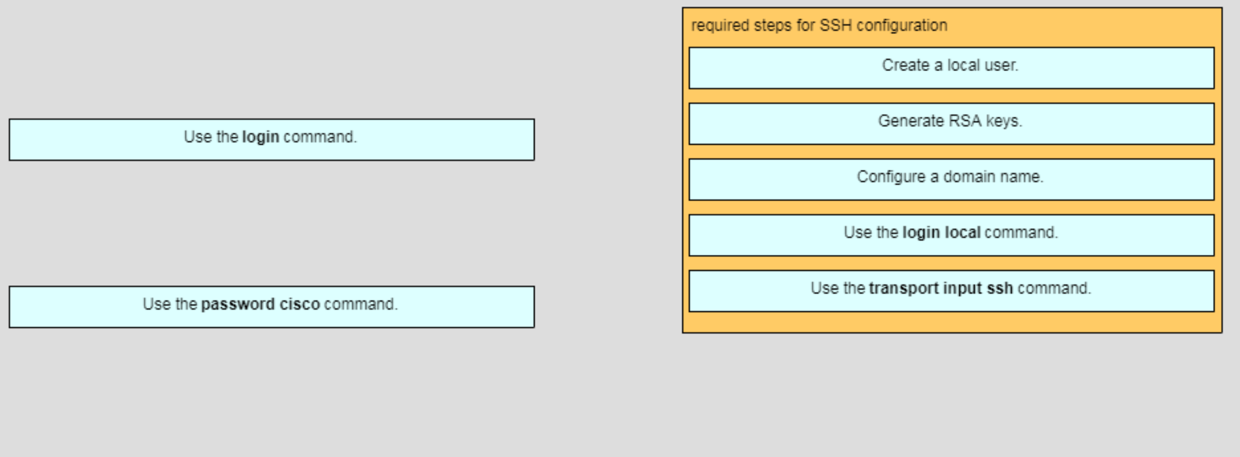
SSH configuration step

SSH configuration step

SSH configuration step

Place the options in the following order:

[+] Create a local user.
[+] Generate RSA keys.
[+] Configure a domain name.
[+] Use the login local command.
[+] Use the transport input ssh command.
[+] Order does not matter within this group.



Use the **login** command.

Use the **password cisco** command.

required steps for SSH configuration

Create a local user.

Generate RSA keys.

Configure a domain name.

Use the **login local** command.

Use the **transport input ssh** command.

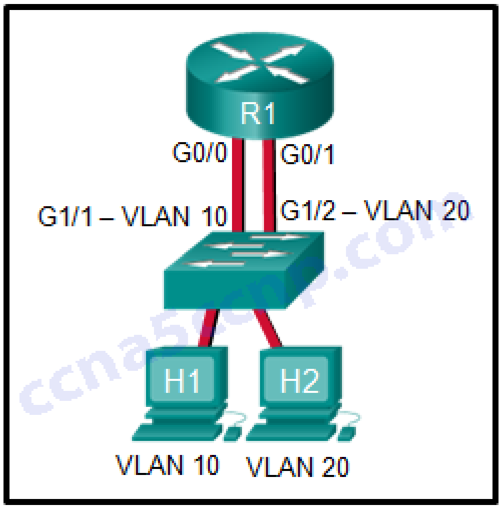
The login and password cisco commands are used with Telnet switch configuration, not SSH configuration.

Old Version: CCNA 2 Chapter 5 Exam Answers v6.0

1. **What is a disadvantage of using router-on-a-stick inter-VLAN routing?**

- does not support VLAN-tagged packets
- requires the use of more physical interfaces than legacy inter-VLAN routing
- **does not scale well beyond 50 VLANs***
- requires the use of multiple router interfaces configured to operate as access links

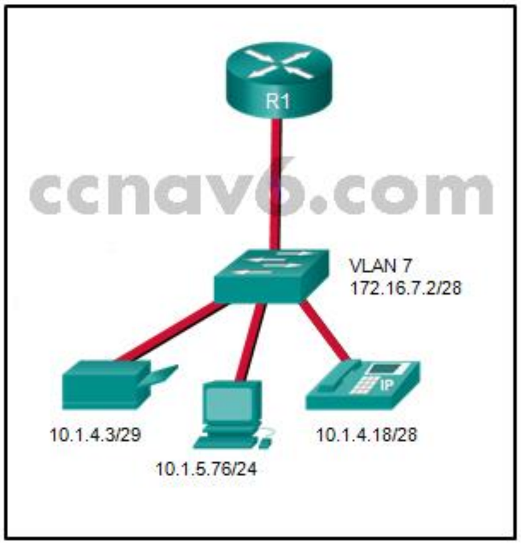
2. **How is traffic routed between multiple VLANs on a multilayer switch?**
   - Traffic is routed via physical interfaces.
   - **Traffic is routed via internal VLAN interfaces. ***
   - Traffic is broadcast out all physical interfaces.
   - Traffic is routed via subinterfaces.
3. **Refer to the exhibit. In this network design, which connection or connections if any, add the VLAN ID number if host H1 sends information to host H2?**



CCNA2 Chapter 5 v5.03 006

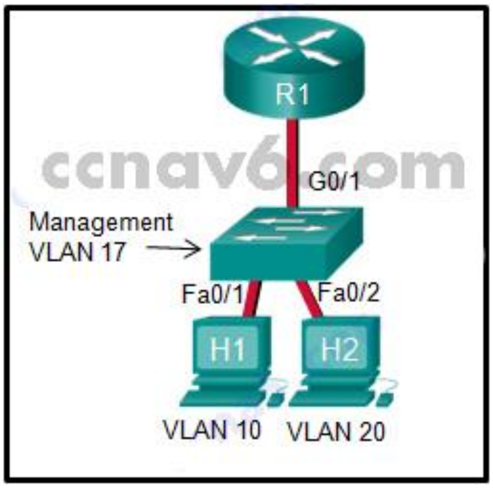
   - **no link***
   - from H1 to the switch
   - from the switch to G0/0 on the router
   - from G0/1 on the router to G1/2 on the switch
   - from the switch to H2
4. **What is a characteristic of legacy inter-VLAN routing?**
   - Only one VLAN can be used in the topology.
   - **The router requires one Ethernet link for each VLAN.***
   - The user VLAN must be the same ID number as the management VLAN.
   - Inter-VLAN routing must be performed on a switch instead of a router.
5. **Refer to the exhibit. A network administrator needs to configure router-on-a-stick for the networks that are shown. How many subinterfaces will have to be created on the router if each VLAN that is shown is to be routed and each VLAN has its own**

subinterface?



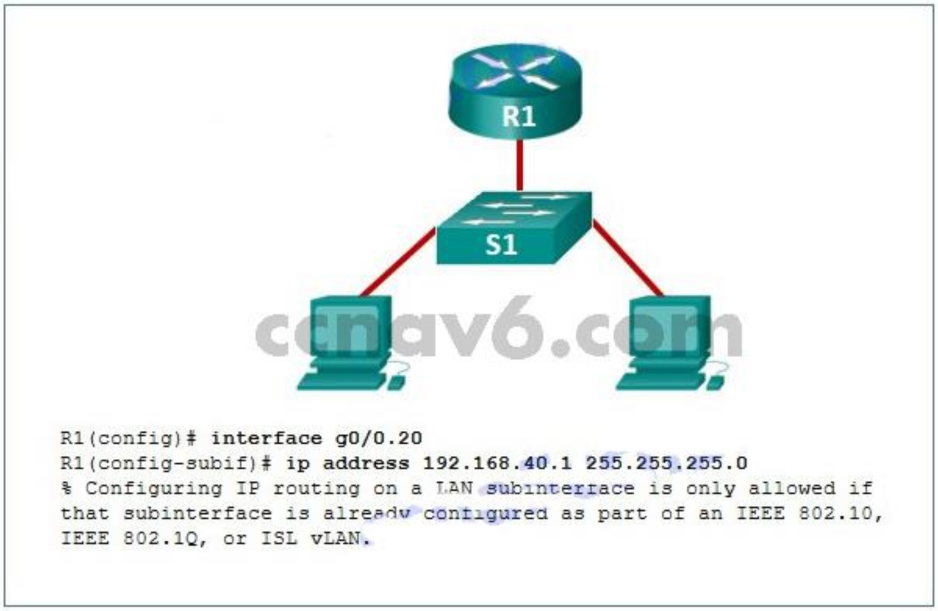
- 1
- 2
- 3
- **4***
- 5

6. **Refer to the exhibit. In what switch mode should port G0/1 be assigned if Cisco best practices are being used?**



- access
- **trunk***
- native
- auto

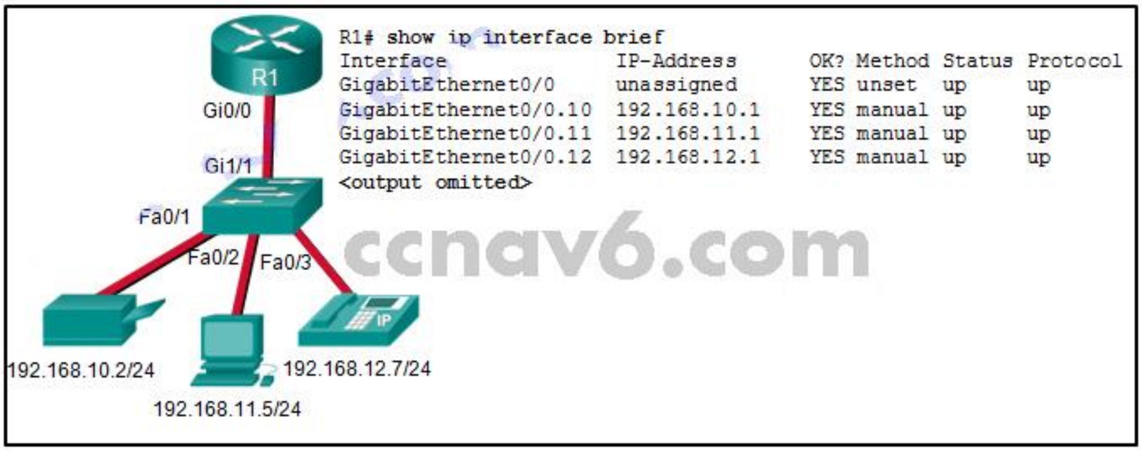
7. **Refer to the exhibit. What is the problem with this configuration, based on the output of the router?**



```
R1(config)# interface g0/0.20
R1(config-subif)# ip address 192.168.40.1 255.255.255.0
% Configuring IP routing on a LAN subinterface is only allowed if
that subinterface is already configured as part of an IEEE 802.10,
IEEE 802.1Q, or ISL vLAN.
```

- The subnet mask is wrong.
- There is no subinterface for the administrative VLAN.
- The subinterface number does not match the third octet in the IPv4 address.
- **The encapsulation has not been configured on the subinterface.***

8. **Refer to the exhibit. Communication between the VLANs is not occurring. What could be the issue?**

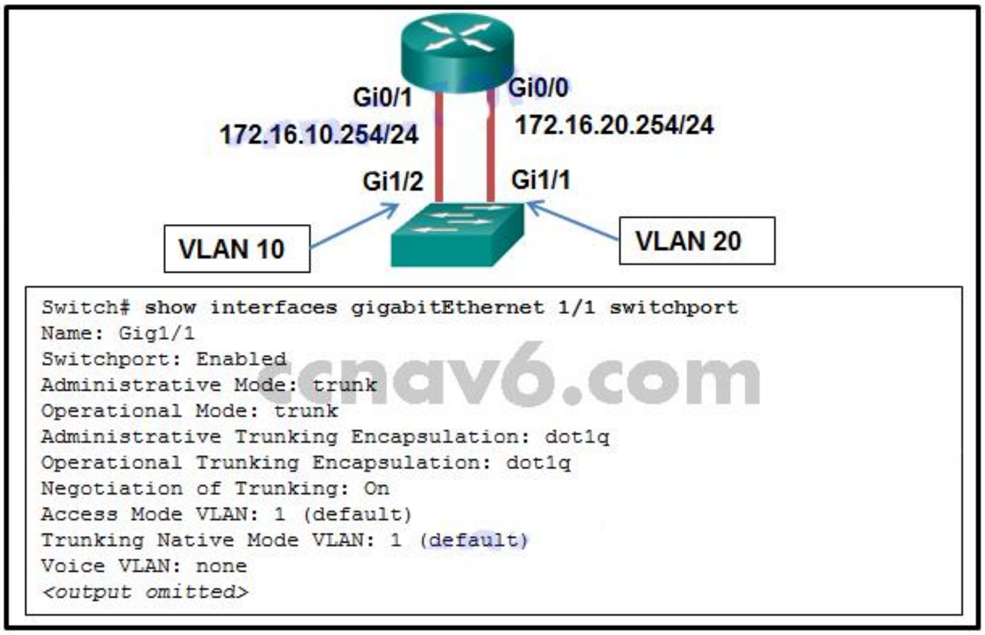


```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status Protocol
GigabitEthernet0/0     unassigned      YES unset  up     up
GigabitEthernet0/0.10  192.168.10.1    YES manual up     up
GigabitEthernet0/0.11  192.168.11.1    YES manual up     up
GigabitEthernet0/0.12  192.168.12.1    YES manual up     up
<output omitted>
```

- The wrong port on the router has been used.
- **The Gi1/1 switch port is not in trunking mode.***
- A duplex issue exists between the switch and the router.
- Default gateways have not been configured for each VLAN.

9. **Refer to the exhibit. A network administrator is verifying the configuration of inter-VLAN routing. Users complain that PCs on different VLANs cannot communicate. Based on the output, what are two configuration errors on switch interface Gi1/1?**

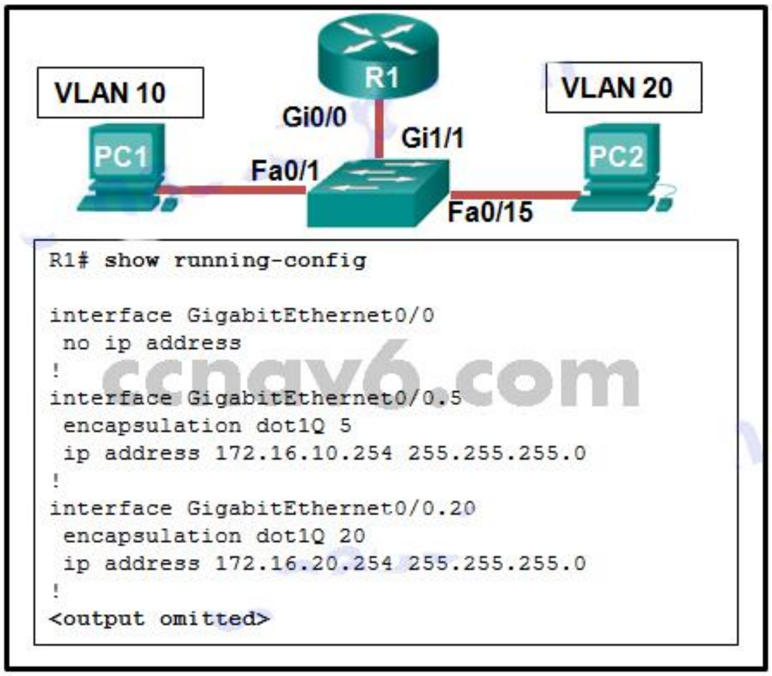
(Choose two.)



```
Switch# show interfaces gigabitEthernet 1/1 switchport
Name: Gig1/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
<output omitted>
```

- **Gi1/1 is in the default VLAN.***
- Voice VLAN is not assigned to Gi1/1.
- **Gi1/1 is configured as trunk mode.***
- Negotiation of trunking is turned on on Gi1/1.
- The trunking encapsulation protocol is configured wrong.

10. **Refer to the exhibit. A network administrator is verifying the configuration of inter-VLAN routing. Users complain that PC2 cannot communicate with PC1. Based on the output, what is the possible cause of the problem?**

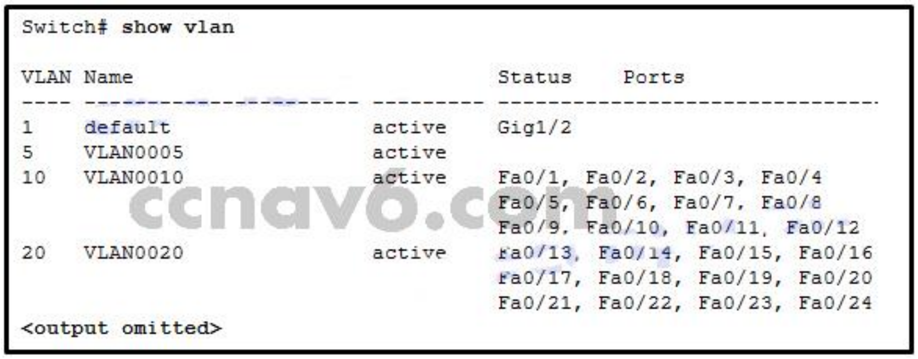


```
R1# show running-config

interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.5
 encapsulation dot1Q 5
 ip address 172.16.10.254 255.255.255.0
!
interface GigabitEthernet0/0.20
 encapsulation dot1Q 20
 ip address 172.16.20.254 255.255.255.0
!
<output omitted>
```

- Gi0/0 is not configured as a trunk port.
- The command interface GigabitEthernet0/0.5 was entered incorrectly.
- There is no IP address configured on the interface Gi0/0.

- The no shutdown command is not entered on subinterfaces.
- **The encapsulation dot1Q 5 command contains the wrong VLAN. ***

11. **Refer to the exhibit. A network administrator is verifying the configuration of inter-VLAN routing. Based on the partial output that is displayed by the use of the show vlan command, which conclusion can be drawn for the Gi1/1 interface?**



```
Switch# show vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/2
5    VLAN0005                         active
10   VLAN0010                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
20   VLAN0020                         active    Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24

<output omitted>
```

- It is shut down.
- It belongs to the default VLAN.
- **It is configured as trunk mode.***
- It is not connected to any device.

12. **Inter-VLAN communication is not occurring in a particular building of a school. Which two commands could the network administrator use to verify that inter-VLAN communication was working properly between a router and a Layer 2 switch when the router-on-a-stick design method is implemented? (Choose two.)**
    - **From the router, issue the show ip route command.***
    - From the router, issue the show interfaces trunk command.
    - From the router, issue the show interfaces interface command.
    - **From the switch, issue the show interfaces trunk command.***
    - From the switch, issue the show interfaces interface command.
13. **How are IP addressing designs affected by VLAN implementations?**
    - VLANs do not support VLSM.
    - VLANs do not use a broadcast address.
    - **Each VLAN must have a different network number.***
    - Each VLAN must have a different subnet mask.
14. **While configuring inter-VLAN routing on a multilayer switch, a network administrator issues the no switchport command on an interface that is connected to another switch. What is the purpose of this command?**
    - **to create a routed port for a single network***
    - to provide a static trunk link
    - to create a switched virtual interface
    - to provide an access link that tags VLAN traffic
15. **What is a disadvantage of using multilayer switches for inter-VLAN routing?**
    - Multilayer switches have higher latency for Layer 3 routing.
    - **Multilayer switches are more expensive than router-on-a-stick implementations.***
    - Spanning tree must be disabled in order to implement routing on a multilayer switch.
    - Multilayer switches are limited to using trunk links for Layer 3 routing.
16. **What is a characteristic of a routed port on a Layer 3 switch?**
    - It supports trunking.

- **It is not assigned to a VLAN.***
- It is commonly used as a WAN link.
- It cannot have an IP address assigned to it.

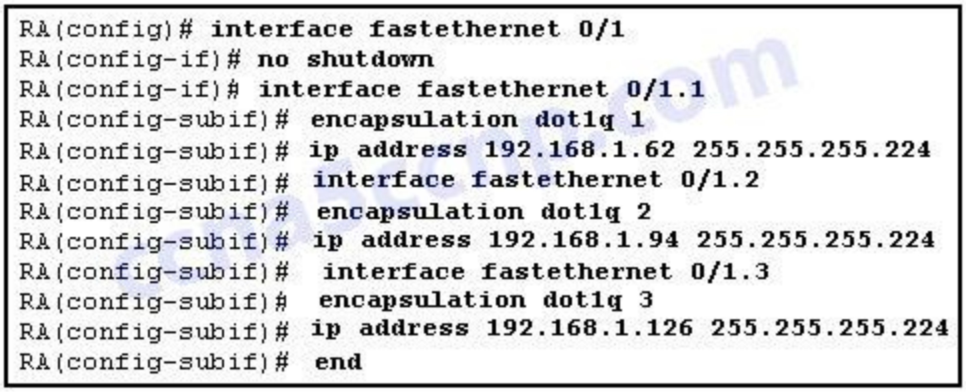
17. **An administrator is attempting to configure a static route on a Cisco 2960 series switch. After the administrator types the command ip route 0.0.0.0 0.0.0.0 10.1.1.1, an error message appears stating that the command is not recognized. What must the administrator do so that this command is accepted?**

- Enter the command no switchport.
- Enter the command ipv6 unicast-routing.
- Enter the command ip route 0.0.0.0 0.0.0.0. vlan 10.
- **Enter the command sdm prefer lanbase-routing and reload.***

18. **Which statement describes a disadvantage of using router subinterfaces for inter-VLAN routing?**

- It is more expensive than using individual router interfaces.
- **Routed traffic must contend for bandwidth on a single router interface.***
- Trunking cannot be used to connect the router to the switch.
- All untagged traffic is dropped.

19. **Refer to the exhibit. Router RA receives a packet with a source address of 192.168.1.35 and a destination address of 192.168.1.85. What will the router do with this packet?**



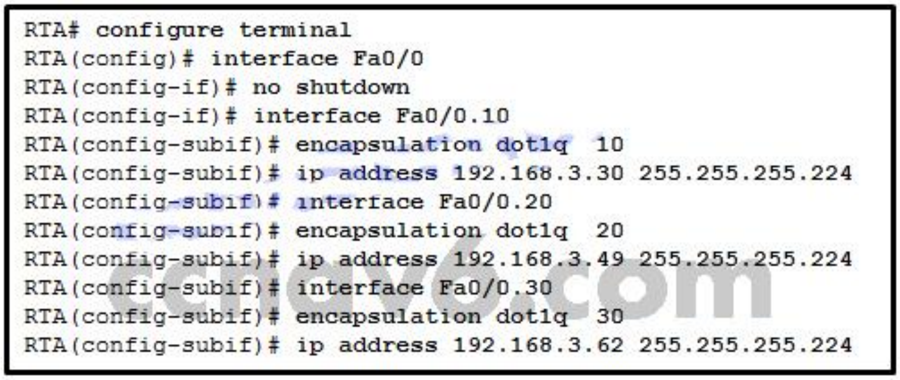
```
RA(config)# interface fastethernet 0/1
RA(config-if)# no shutdown
RA(config-if)# interface fastethernet 0/1.1
RA(config-subif)# encapsulation dot1q 1
RA(config-subif)# ip address 192.168.1.62 255.255.255.224
RA(config-subif)# interface fastethernet 0/1.2
RA(config-subif)# encapsulation dot1q 2
RA(config-subif)# ip address 192.168.1.94 255.255.255.224
RA(config-subif)# interface fastethernet 0/1.3
RA(config-subif)# encapsulation dot1q 3
RA(config-subif)# ip address 192.168.1.126 255.255.255.224
RA(config-subif)# end
```

CCNA2 Chapter 5 v5.03 004

- The router will drop the packet.
- The router will forward the packet out interface FastEthernet 0/1.1.
- **The router will forward the packet out interface FastEthernet 0/1.2.***
- The router will forward the packet out interface FastEthernet 0/1.3.
- The router will forward the packet out interface FastEthernet 0/1.2 and interface FastEthernet 0/1.3.

20. **Refer to the exhibit. After attempting to enter the configuration that is shown in router RTA, an administrator receives an error and users on VLAN 20 report that they are**

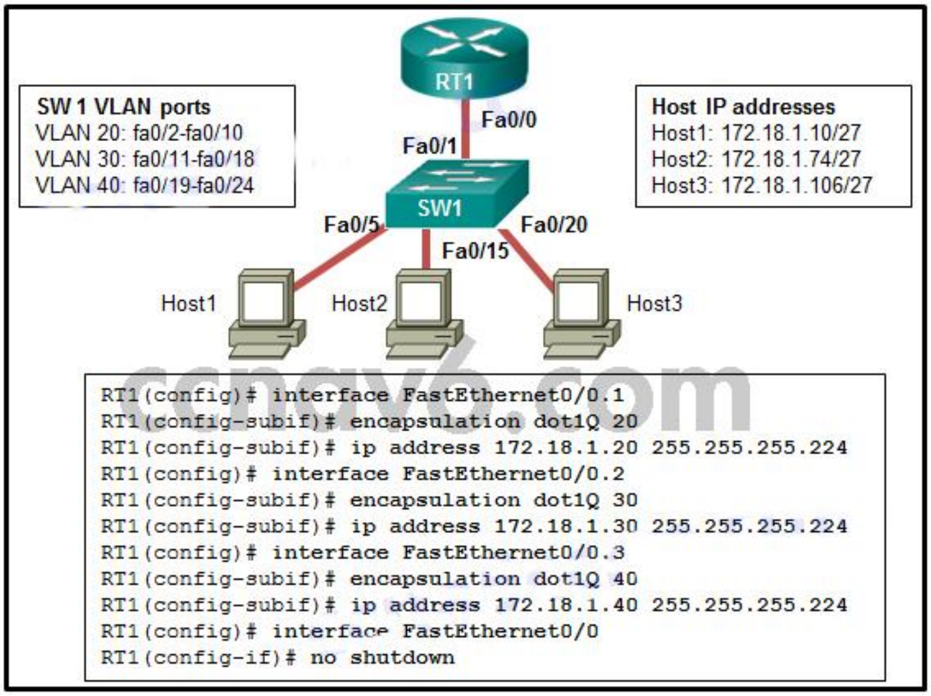
unable to reach users on VLAN 30. What is causing the problem?



```
RTA# configure terminal
RTA(config)# interface Fa0/0
RTA(config-if)# no shutdown
RTA(config-if)# interface Fa0/0.10
RTA(config-subif)# encapsulation dot1q  10
RTA(config-subif)# ip address 192.168.3.30 255.255.255.224
RTA(config-subif)# interface Fa0/0.20
RTA(config-subif)# encapsulation dot1q  20
RTA(config-subif)# ip address 192.168.3.49 255.255.255.224
RTA(config-subif)# interface Fa0/0.30
RTA(config-subif)# encapsulation dot1q  30
RTA(config-subif)# ip address 192.168.3.62 255.255.255.224
```

- Dot1q does not support subinterfaces.
- There is no address on Fa0/0 to use as a default gateway.
- **RTA is using the same subnet for VLAN 20 and VLAN 30.***
- The no shutdown command should have been issued on Fa0/0.20 and Fa0/0.30.

21. **Refer to the exhibit. A network administrator is configuring RT1 for inter-VLAN routing. The switch is configured correctly and is functional. Host1, Host2, and Host3 cannot communicate with each other. Based on the router configuration, what is causing the problem?**



SW 1 VLAN ports
VLAN 20: fa0/2-fa0/10
VLAN 30: fa0/11-fa0/18
VLAN 40: fa0/19-fa0/24

Host IP addresses
Host1: 172.18.1.10/27
Host2: 172.18.1.74/27
Host3: 172.18.1.106/27

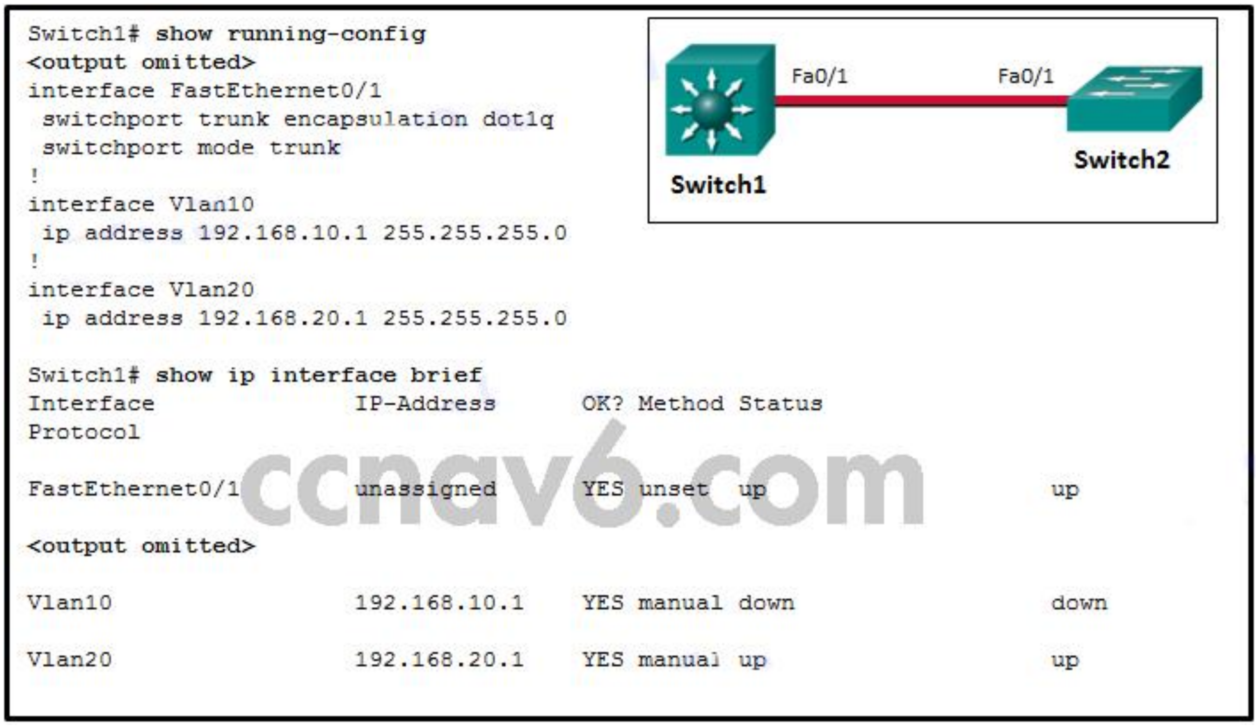
```
RT1(config)# interface FastEthernet0/0.1
RT1(config-subif)# encapsulation dot1Q 20
RT1(config-subif)# ip address 172.18.1.20 255.255.255.224
RT1(config)# interface FastEthernet0/0.2
RT1(config-subif)# encapsulation dot1Q 30
RT1(config-subif)# ip address 172.18.1.30 255.255.255.224
RT1(config)# interface FastEthernet0/0.3
RT1(config-subif)# encapsulation dot1Q 40
RT1(config-subif)# ip address 172.18.1.40 255.255.255.224
RT1(config)# interface FastEthernet0/0
RT1(config-if)# no shutdown
```

- Interface Fa0/0 is missing IP address configuration information.
- **IP addresses on the subinterfaces are incorrectly matched to the VLANs.***
- Each subinterface of Fa0/0 needs separate no shutdown commands.
- Routers do not support 802.1Q encapsulation on subinterfaces.

22. **What condition is required to enable Layer 3 switching?**

- **The Layer 3 switch must have IP routing enabled.***
- All participating switches must have unique VLAN numbers.
- All routed subnets must be on the same VLAN.
- Inter-VLAN portions of Layer 3 switching must use router-on-a-stick.

23. **Refer to the exhibit. Which command can the administrator issue to change the VLAN10 status to up?**



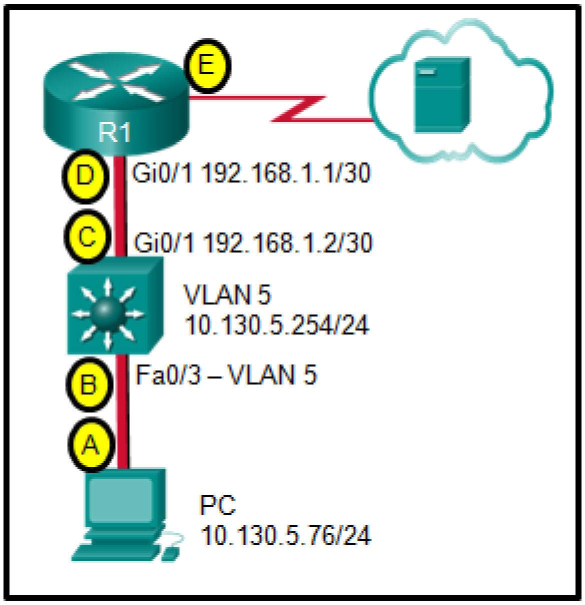
```
Switch1# show running-config
<output omitted>
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Vlan10
 ip address 192.168.10.1 255.255.255.0
!
interface Vlan20
 ip address 192.168.20.1 255.255.255.0

Switch1# show ip interface brief
Interface               IP-Address      OK? Method Status
Protocol

FastEthernet0/1         unassigned      YES unset  up                   up

<output omitted>

Vlan10                  192.168.10.1    YES manual down                 down

Vlan20                  192.168.20.1    YES manual up                   up
```

- Switch1(config)# interface vlan 10
  Switch1(config-if)# no shutdown
- Switch1(config)# interface vlan 10
  Switch1(config-if)# ip address 192.168.10.1 255.255.255.0
- Switch1(config)# interface vlan 10
  Switch1(config-if)# ip address 192.168.10.1 255.255.255.0
  Switch1(config-if)# no shutdown
- **Switch1(config)# vlan 10**
  Switch1(config-vlan)# exit*

24. **Fill in the blank. Do not use abbreviations.**
A network engineer is troubleshooting the configuration of new VLANs on a network. Which command is used to display the list of VLANs that exists on the switch? **show vlan**

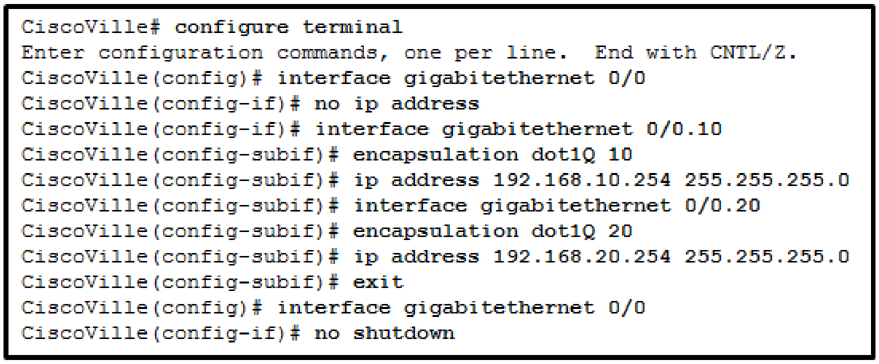
25. **Refer to the exhibit. The switch does the routing for the hosts that connect to VLAN 5. If the PC accesses a web server from the Internet, at what point will a VLAN number be**

added to the frame?



- point A
- point B
- point C
- point D
- point E
- **No VLAN number is added to the frame in this design.***

26. **Which type of inter-VLAN communication design requires the configuration of multiple subinterfaces?**
    - **router on a stick***
    - routing via a multilayer switch
    - routing for the management VLAN
    - legacy inter-VLAN routing
27. **A small college uses VLAN 10 for the classroom network and VLAN 20 for the office network. What is needed to enable communication between these two VLANs while using legacy inter-VLAN routing?**
    - **A router with at least two LAN interfaces should be used.***
    - Two groups of switches are needed, each with ports that are configured for one VLAN.
    - A router with one VLAN interface is needed to connect to the SVI on a switch.
    - A switch with a port that is configured as trunk is needed to connect to a router.
28. **Refer to the exhibit. A network administrator has configured router CiscoVille with the above commands to provide inter-VLAN routing. What command will be required on a switch that is connected to the Gi0/0 interface on router CiscoVille to allow inter-VLAN routing??**

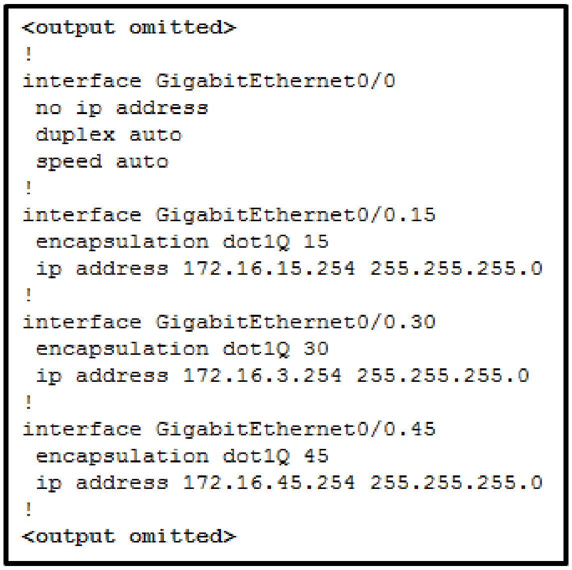


```
CiscoVille# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no ip address
CiscoVille(config-if)# interface gigabitethernet 0/0.10
CiscoVille(config-subif)# encapsulation dot1Q 10
CiscoVille(config-subif)# ip address 192.168.10.254 255.255.255.0
CiscoVille(config-subif)# interface gigabitethernet 0/0.20
CiscoVille(config-subif)# encapsulation dot1Q 20
CiscoVille(config-subif)# ip address 192.168.20.254 255.255.255.0
CiscoVille(config-subif)# exit
CiscoVille(config)# interface gigabitethernet 0/0
CiscoVille(config-if)# no shutdown
```

CCNA Chapter 5 Exam Answer 003 (v5.02, 2015)

- switchport mode access
- no switchport
- **switchport mode trunk***
- switchport mode dynamic desirable

29. **Refer to the exhibit. A router-on-a-stick configuration was implemented for VLANs 15, 30, and 45, according to the show running-config command output. PCs on VLAN 45 that are using the 172.16.45.0 /24 network are having trouble connecting to PCs on VLAN 30 in the 172.16.30.0 /24 network. Which error is most likely causing this problem??**

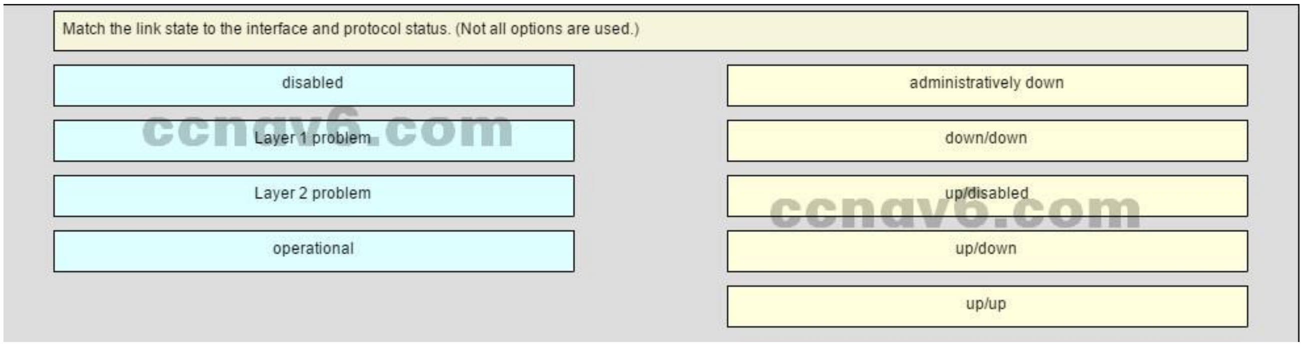


```
<output omitted>
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.15
 encapsulation dot1Q 15
 ip address 172.16.15.254 255.255.255.0
!
interface GigabitEthernet0/0.30
 encapsulation dot1Q 30
 ip address 172.16.3.254 255.255.255.0
!
interface GigabitEthernet0/0.45
 encapsulation dot1Q 45
 ip address 172.16.45.254 255.255.255.0
!
<output omitted>
```

CCNA Chapter 5 Exam Answer 009 (v5.02, 2015)

- The wrong VLAN has been configured on GigabitEthernet 0/0.45.
- The command no shutdown is missing on GigabitEthernet 0/0.30.
- The GigabitEthernet 0/0 interface is missing an IP address.
- **There is an incorrect IP address configured on GigabitEthernet 0/0.30.***

30. **Match the link state to the interface and protocol status. (Not all options are used.)**



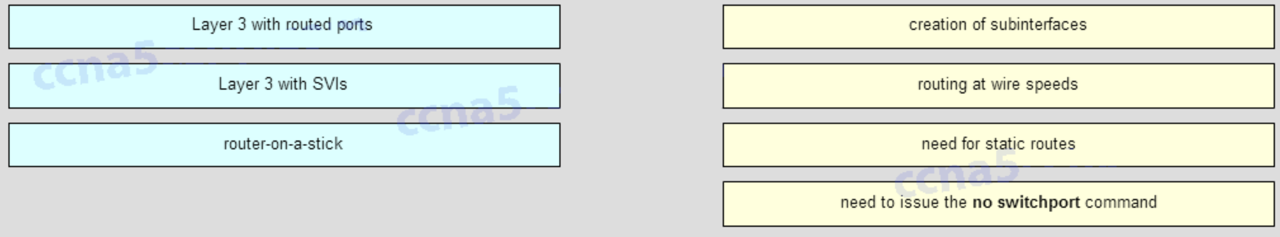
Match the link state to the interface and protocol status. (Not all options are used.)

disabled
Layer 1 problem
Layer 2 problem
operational

administratively down
down/down
up/disabled
up/down
up/up

Place the options in the following order:
disable -> administratively down
Layer 1 problem -> down/down
– not scored –
Layer 2 problem -> up/down
operational -> up/up

31. **Match the inter-VLAN routing method to the corresponding characteristic (not all options are used).**



Layer 3 with routed ports
Layer 3 with SVIs
router-on-a-stick

creation of subinterfaces
routing at wire speeds
need for static routes
need to issue the **no switchport** command

Place the options in the following order:
router-on-a-stick -> creation of subinterfaces
Layer 3 with SVIs -> routing at wire speeds
– not scored –
Layer 3 with routed ports -> need to issue the no switchport command