[Updated Constantly]

HERE

CCNA 2 (v5.1 + v6.0) Chapter 3 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 dynamic routing protocol was developed to interconnect different Internet service providers?**
   - **BGP***
   - EIGRP
   - OSPF
   - RIP

   BGP is a protocol developed to interconnect different levels of ISPs as well as ISPs and some of their larger private clients.
2. **Which routing protocol is limited to smaller network implementations because it does not accommodate growth for larger networks?**
   - OSPF
   - **RIP***
   - EIGRP
   - IS-IS

   The RIP protocol was created with a metric that does not support larger networks. Other routing protocols, including OSPF, EIGRP, and IS-IS, scale well and accommodate growth and larger networks.
3. **What two tasks do dynamic routing protocols perform? (Choose two.)**
   - discover hosts
   - **update and maintain routing tables***
   - propagate host default gateways
   - **network discovery***
   - assign IP addressing
4. **When would it be more beneficial to use a dynamic routing protocol instead of static routing?**
   - in an organization with a smaller network that is not expected to grow in size
   - on a stub network that has a single exit point
   - in an organization where routers suffer from performance issues
   - **on a network where there is a lot of topology changes***

   Dynamic routing protocols consume more router resources, are suitable for larger networks, and are more useful on networks that are growing and changing.
5. **When would it be more beneficial to use static routing instead of dynamic routing protocols?**
   - **on a network where dynamic updates would pose a security risk***

- on a network that is expected to continually grow in size
- on a network that has a large amount of redundant paths
- on a network that commonly experiences link failures

Dynamic routing protocols are viewed as less secure than static routing because they commonly forward routing information on the same links that data traffic is crossing.

6. **What is a purpose of the network command when configuring RIPv2 as the routing protocol?**
   - **It identifies the interfaces that belong to a specified network.***
   - It specifies the remote network that can now be reached.
   - It immediately advertises the specified network to neighbor routers with a classful mask.
   - It populates the routing table with the network entry.

   The network command is used to advertise the directly connected networks of a router. It enables RIP on the interfaces that belong to the specified network.
7. **A network administrator configures a static route on the edge router of a network to assign a gateway of last resort. How would a network administrator configure the edge router to automatically share this route within RIP?**
   - Use the auto-summary command.
   - Use the passive-interface command.
   - Use the network command.
   - **Use the default-information originate command.***

   The default-information originate command instructs a router to propagate the static default route in RIP or OSPF.
8. **What is the purpose of the passive-interface command?**
   - allows a routing protocol to forward updates out an interface that is missing its IP address
   - allows a router to send routing updates on an interface but not receive updates via that interface
   - allows an interface to remain up without receiving keepalives
   - allows interfaces to share IP addresses
   - **allows a router to receive routing updates on an interface but not send updates via that interface***
9. **Which route would be automatically created when a router interface is activated and configured with an IP address?**
   - D 10.16.0.0/24 [90/3256] via 192.168.6.9
   - **C 192.168.0.0/24 is directly connected, FastEthernet 0/0***
   - S 192.168.1.0/24 is directly connected, FastEthernet 0/1
   - O 172.16.0.0/16 [110/65] via 192.168.5.1

   Directly connected networks are identified with a C and are automatically created whenever an interface is configured with an IP address and activated.

10. **Refer to the exhibit. Which two types of routes could be used to describe the 192.168.200.0/30 route? (Choose two.)**

```
R1# show ip route | begin Gateway
Gateway of last resort is not set

  192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.10.0/24 is directly connected, GigabitEthernet0/0.10
L     192.168.10.254/32 is directly connected, GigabitEthernet0/0.10
  192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.20.0/24 is directly connected, GigabitEthernet0/0.20
L     192.168.20.254/32 is directly connected, GigabitEthernet0/0.20
O     192.168.30.0/24 [110/2] via 192.168.200.2, 00:01:20,
GigabitEthernet0/1
  192.168.200.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.200.0/30 is directly connected, GigabitEthernet0/1
L     192.168.200.1/32 is directly connected, GigabitEthernet0/1
```

- **ultimate route***
- level 1 parent route
- level 1 network route
- **level 2 child route***
- supernet route

A level 2 child route is a route that has a network with a mask that is greater than the classful equivalent. An ultimate route is a route that uses a next-hop IP address or exit interface to forward traffic.

11. **What occurs next in the router lookup process after a router identifies a destination IP address and locates a matching level 1 parent route?**
    - **The level 2 child routes are examined.***
    - The level 1 supernet routes are examined.
    - The level 1 ultimate routes are examined.
    - The router drops the packet.

    When a router locates a parent route that matches the destination IP address of a packet, the router will then examine the level 2 child routes contained within it.
12. **Which route would be used to forward a packet with a source IP address of 192.168.10.1 and a destination IP address of 10.1.1.1?**
    - C 192.168.10.0/30 is directly connected, GigabitEthernet0/1
    - S 10.1.0.0/16 is directly connected, GigabitEthernet0/0
    - **O 10.1.1.0/24 [110/65] via 192.168.200.2, 00:01:20, Serial0/1/0***
    - S* 0.0.0.0/0 [1/0] via 172.16.1.1

    Even though OSPF has a higher administrative distance value (less trustworthy), the best match is the route in the routing table that has the most number of far left matching bits.
13. **Which two requirements are used to determine if a route can be considered as an ultimate route in a router's routing table? (Choose two.)**
    - contain subnets
    - be a default route
    - **contain an exit interface***
    - be a classful network entry
    - **contain a next-hop IP address***

An ultimate route is a routing table entry that contains either a next-hop IP address (another path) or an exit interface, or both. This means that directly connected and link-local routes are ultimate routes. A default route is a level 1 ultimate route, but not all ultimate routes are default routes. Routing table entries that are subnetted are level 1 parent routes but do not meet either of the two requirements to be ultimate routes. Ultimate routes do not have to be classful network entries.

14. **What is a disadvantage of using dynamic routing protocols?**
    - They are only suitable for simple topologies.
    - Their configuration complexity increases as the size of the network grows.
    - **They send messages about network status insecurely across networks by default.***
    - They require administrator intervention when the pathway of traffic changes.

    By default, dynamic routing protocols forward messages across a network without authenticating the receiver or originator of traffic. Static routes increase in configuration complexity as the network grows larger and are more suitable for smaller networks. Static routes also require manual intervention when a network topology changes or links become disabled.

15. **Which two statements are true regarding classless routing protocols? (Choose two.)**
    - **sends subnet mask information in routing updates***
    - sends complete routing table update to all neighbors
    - is supported by RIP version 1
    - **allows for use of both 192.168.1.0/30 and 192.168.1.16/28 subnets in the same topology***
    - reduces the amount of address space available in an organization

16. **Refer to the exhibit. Based on the partial output from the show ip route command, what two facts can be determined about the RIP routing protocol? (Choose two.)**

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 6 masks
C       10.0.0.0/25 is directly connected, GigabitEthernet0/1
L       10.0.0.1/32 is directly connected, GigabitEthernet0/1
C       10.0.0.128/26 is directly connected, GigabitEthernet0/0
L       10.0.0.129/32 is directly connected, GigabitEthernet0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
R       172.16.0.0/25 [120/1] via 192.168.1.1, 00:00:12, Serial0/1/0
R       172.16.0.128/25 [120/1] via 192.168.1.1, 00:00:12, Serial0/1/0
     192.168.1.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.1.0/30 is directly connected, Serial0/1/0
L       192.168.1.2/32 is directly connected, Serial0/1/0
```

    - **RIP version 2 is running on this router and its RIP neighbor.***
    - The metric to the network 172.16.0.0 is 120.
    - RIP version 1 is running on this router and its RIP neighbor.
    - **The command no auto-summary has been used on the RIP neighbor router.***
    - RIP will advertise two networks to its neighbor.

    The router learned, via RIP, that 172.16.0.0 is variably subnetted, and that there are two subnet and mask entries for that network. This means that RIP version 2 is running on both routers and that the command no auto-summary has been applied on the neighbor router. RIPv2 has an administrative distance of 120 and this router will advertise all connected networks to the neighbor via 192.168.1.1.

17. **While configuring RIPv2 on an enterprise network, an engineer enters the command network 192.168.10.0 into router configuration mode. What is the result of entering this command?**
    - The interface of the 192.168.10.0 network is sending version 1 and version 2 updates.
    - The interface of the 192.168.10.0 network is receiving version 1 and version 2 updates.
    - **The interface of the 192.168.10.0 network is sending only version 2 updates.***
    - The interface of the 192.168.10.0 network is sending RIP hello messages.

    The command being entered by the engineer will cause RIPv2 to activate on the interface for the 192.168.10.0 network. If RIPv1 is configured, the router will send only version 1 updates, but will listen for both version 1 and version 2 updates. If RIPv2 is configured, the router will send and listen to only version 2 updates.
18. **A destination route in the routing table is indicated with a code D. Which kind of route entry is this?**
    - a static route
    - a route used as the default gateway
    - a network directly connected to a router interface
    - **a route dynamically learned through the EIGRP routing protocol***

    Routes in a routing table are manually created or dynamically learned. Letter D indicates that the route was learned dynamically through the EIGRP routing protocol.
19. **Refer to the exhibit. Which interface will be the exit interface to forward a data packet with the destination IP address 172.16.0.66?**

```
R1# show ip route
<output omitted>

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 7 subnets, 3 masks
R       172.16.0.0/26 [120/1] via 192.168.1.1, 00:00:24, Serial0/0/0
D       172.16.0.64/26 [90/2170112] via 192.168.1.6, 00:05:56, Serial0/0/1
R       172.16.0.128/26 [120/1] via 192.168.1.1, 00:00:24, Serial0/0/0
C       172.16.0.192/27 is directly connected, GigabitEthernet0/0
L       172.16.0.193/32 is directly connected, GigabitEthernet0/0
C       172.16.0.224/27 is directly connected, GigabitEthernet0/1
L       172.16.0.225/32 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.0/30 is directly connected, Serial0/0/0
L       192.168.1.2/32 is directly connected, Serial0/0/0
C       192.168.1.4/30 is directly connected, Serial0/0/1
L       192.168.1.5/32 is directly connected, Serial0/0/1
     192.168.2.0/30 is subnetted, 1 subnets
R       192.168.2.0/30 [120/1] via 192.168.1.1, 00:00:24, Serial0/0/0
R1#
```

    - Serial0/0/0
    - **Serial0/0/1***
    - GigabitEthernet0/0
    - GigabitEthernet0/1

    The destination IP address 172.16.0.66 belongs to the network 172.16.0.64/26. In the routing table there is a route learned by EIGRP (identified with code “D”) with 192.168.1.6 as the next-hop address and Serial 0/0/1 as the exiting interface.
20. **Which type of route will require a router to perform a recursive lookup?**
    - **an ultimate route that is using a next hop IP address on a router that is not using CEF***

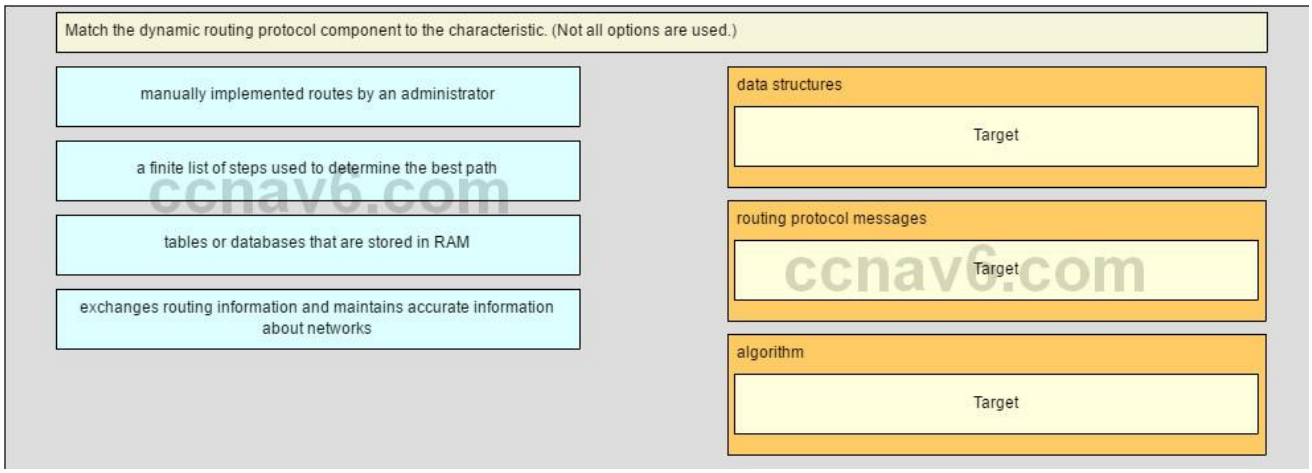
- a level 2 child route that is using an exit interface on a router that is not using CEF
- a level 1 network route that is using a next hop IP address on a router that is using CEF
- a parent route on a router that is using CEF

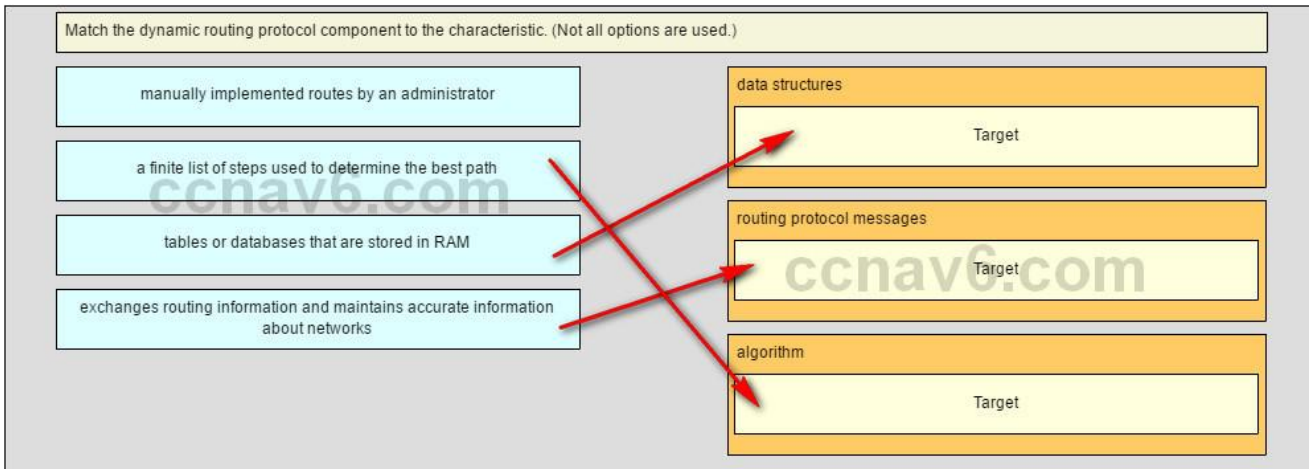
When Cisco Express Forwarding (CEF) is not being used on a router, a recursive lookup must be performed when a route using a next-hop IP address is selected as the best pathway to forward data.

21. **Which route is the best match for a packet entering a router with a destination address of 10.16.0.2?**
    - S 10.0.0.0/8 [1/0] via 192.168.0.2
    - **S 10.16.0.0/24 [1/0] via 192.168.0.9***
    - S 10.16.0.0/16 is directly connected, Ethernet 0/1
    - S 10.0.0.0/16 is directly connected, Ethernet 0/0

    Before the administrative distance of a route is compared, the route with the most specific best match is utilized. The 192.168.14.0/26 network contains the best match to the destination IP address of 192.168.14.20 and thus the 192.168.14.0/26 RIP route is utilized over the EIGRP and OSFP routes, regardless of administrative distance.
22. **A router is configured to participate in multiple routing protocol: RIP, EIGRP, and OSPF. The router must send a packet to network 192.168.14.0. Which route will be used to forward the traffic?**
    - **a 192.168.14.0/26 route that is learned via RIP***
    - a 192.168.14.0/24 route that is learned via EIGRP
    - a 192.168.14.0/25 route that is learned via OSPF
    - a 192.168.14.0/25 route that is learned via RIP
23. **What is different between IPv6 routing table entries compared to IPv4 routing table entries?**
    - IPv6 routing tables include local route entries which IPv4 routing tables do not.
    - **By design IPv6 is classless so all routes are effectively level 1 ultimate routes.***
    - The selection of IPv6 routes is based on the shortest matching prefix, unlike IPv4 route selection which is based on the longest matching prefix.
    - IPv6 does not use static routes to populate the routing table as used in IPv4.

    Routers running IOS release 15 have link local routing table entries for both IPv4 and IPv6. The selection of both IPv6 routes and IPv4 routes is based on the longest matching prefix. The routing tables of both IPv6 and IPv4 use directly connected interfaces, static routes, and dynamically learned routes.
24. **Match the dynamic routing protocol component to the characteristic. (Not all options are used.)**

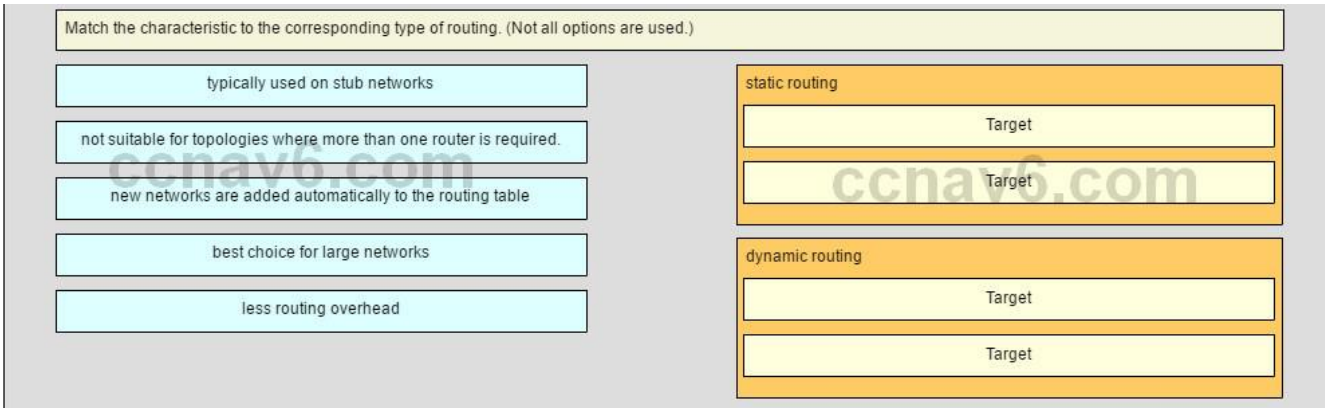


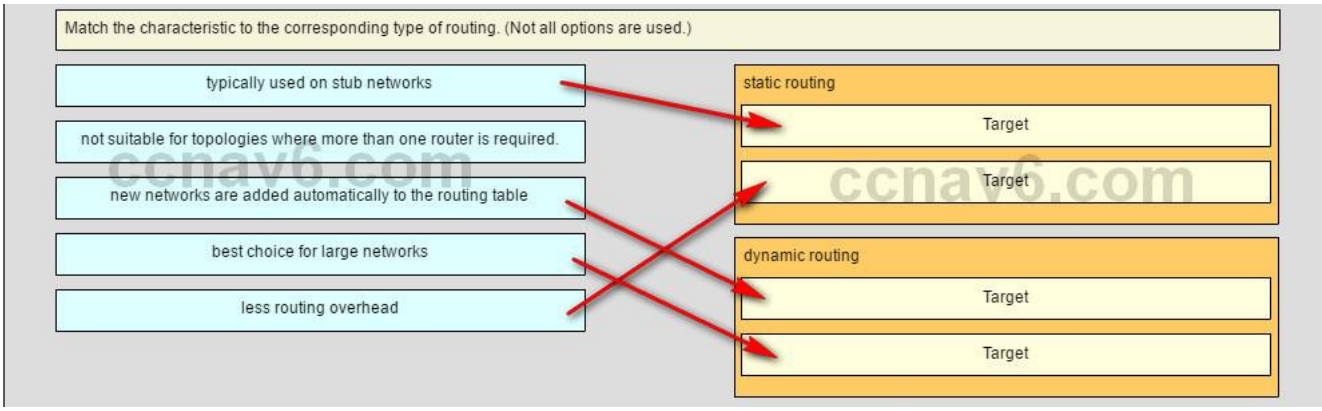


data structures
tables or databases that are stored in RAM*
routing protocol messages
exchanges routing information and maintains accurate information about networks*
algorithm
a finite list of steps used to determine the best path*

The three components of dynamic routing protocols include:
Data structures
Routing protocol messages
Algorithm

25. **Match the characteristic to the corresponding type of routing. (Not all options are used.)**





Place the options in the following order:

[+] typically used on stub networks *

[+] less routing overhead *

[#] new networks are added automatically to the routing table *

[#] best choice for large networks*

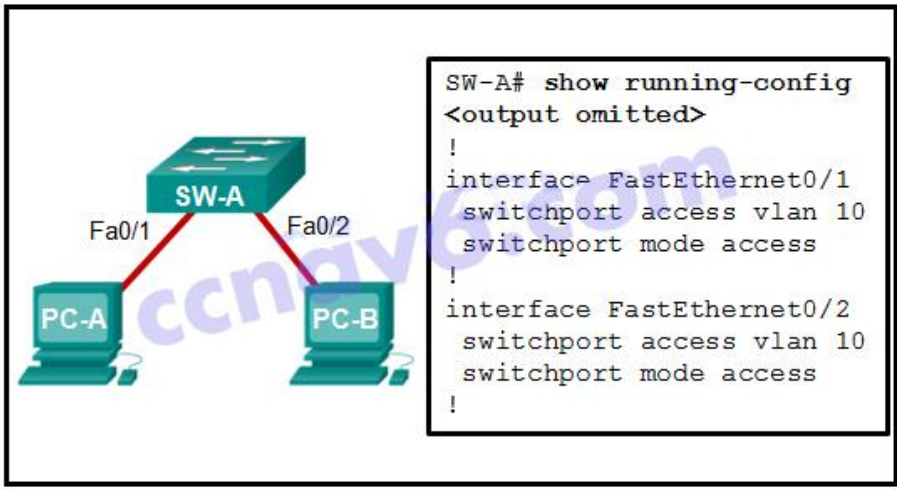
Both static and dynamic routing could be used when more than one router is involved. Dynamic routing is when a routing protocol is used. Static routing is when every remote route is entered manually by an administrator into every router in the network topology.

Older Version: CCNA 2 Chapter 3 Exam Answers v5.1

1. **Which three statements accurately describe VLAN types? (Choose three).**
   - **A management VLAN is any VLAN that is configured to access management features of the switch.***
   - A data VLAN is used to carry VLAN management data and user-generated traffic.
   - **After the initial boot of an unconfigured switch, all ports are members of the default VLAN. ***
   - **An 802.1Q trunk port, with a native VLAN assigned, supports both tagged and untagged traffic.***
   - Voice VLANs are used to support user phone and e-mail traffic on a network.
   - VLAN 1 is always used as the management VLAN.
2. **Which type of VLAN is used to designate which traffic is untagged when crossing a trunk port?**
   - data
   - default

- **native***
- management

3. **What are three primary benefits of using VLANs? (Choose three.)**
   - **security***
   - a reduction in the number of trunk links
   - **cost reduction ***
   - end user satisfaction
   - **improved IT staff efficiency***
   - no required configuration
4. **Refer to the exhibit. A frame is traveling between PC-A and PC-B through the switch. Which statement is true concerning VLAN tagging of the frame?**



   - A VLAN tag is added when the frame leaves PC-A.
   - A VLAN tag is added when the frame is accepted by the switch.
   - A VLAN tag is added when the frame is forwarded out the port to PC-B.
   - **No VLAN tag is added to the frame.***
5. **Which command displays the encapsulation type, the voice VLAN ID, and the access mode VLAN for the Fa0/1 interface?**
   - show vlan brief
   - **show interfaces Fa0/1 switchport***
   - show mac address-table interface Fa0/1
   - show interfaces trunk
6. **What must the network administrator do to remove Fast Ethernet port fa0/1 from VLAN 2 and assign it to VLAN 3?**
   - Enter the no vlan 2 and the vlan 3 commands in global configuration mode.
   - **Enter the switchport access vlan 3 command in interface configuration mode.***
   - Enter the switchport trunk native vlan 3 command in interface configuration mode.
   - Enter the no shutdown in interface configuration mode to return it to the default configuration and then configure the port for VLAN 3.
7. **A Cisco Catalyst switch has been added to support the use of multiple VLANs as part of an enterprise network. The network technician finds it necessary to clear all VLAN information from the switch in order to incorporate a new network design. What should the technician do to accomplish this task?**
   - Erase the startup configuration and reboot the switch.

- Erase the running configuration and reboot the switch.
- **Delete the startup configuration and the vlan.dat file in the flash memory of the switch and reboot the switch.***
- Delete the IP address that is assigned to the management VLAN and reboot the switch.

8. **Which two characteristics match extended range VLANs? (Choose two.)**
   - CDP can be used to learn and store these VLANs.
   - **VLAN IDs exist between 1006 to 4094. ***
   - **They are saved in the running-config file by default.***
   - VLANs are initialized from flash memory.
   - They are commonly used in small networks.
9. **What happens to switch ports after the VLAN to which they are assigned is deleted?**
   - The ports are disabled.
   - The ports are placed in trunk mode.
   - The ports are assigned to VLAN1, the default VLAN.
   - **The ports stop communicating with the attached devices.***
10. **A Cisco switch currently allows traffic tagged with VLANs 10 and 20 across trunk port Fa0/5. What is the effect of issuing a switchport trunk allowed vlan 30 command on Fa0/5?**
    - It allows VLANs 1 to 30 on Fa0/5.
    - It allows VLANs 10, 20, and 30 on Fa0/5.
    - **It allows only VLAN 30 on Fa0/5.***
    - It allows a native VLAN of 30 to be implemented on Fa0/5.
11. **What VLANs are allowed across a trunk when the range of allowed VLANs is set to the default value?**
    - **All VLANs will be allowed across the trunk.***
    - Only VLAN 1 will be allowed across the trunk.
    - Only the native VLAN will be allowed across the trunk.
    - The switches will negotiate via VTP which VLANs to allow across the trunk.
12. **Which command should the network administrator implement to prevent the transfer of DTP frames between a Cisco switch and a non-Cisco switch?**
    - S1(config-if)# switchport mode trunk
    - **S1(config-if)# switchport nonegotiate***
    - S1(config-if)# switchport mode dynamic desirable
    - S1(config-if)# switchport mode access
    - S1(config-if)# switchport trunk allowed vlan none
13. **Under which two occasions should an administrator disable DTP while managing a local area network? (Choose two.)**
    - **when connecting a Cisco switch to a non-Cisco switch***
    - when a neighbor switch uses a DTP mode of dynamic auto
    - when a neighbor switch uses a DTP mode of dynamic desirable
    - **on links that should not be trunking***
    - on links that should dynamically attempt trunking
14. **In a basic VLAN hopping attack, which switch feature do attackers take advantage of?**
    - an open Telnet connection
    - automatic encapsulation negotiation
    - forwarding of broadcasts

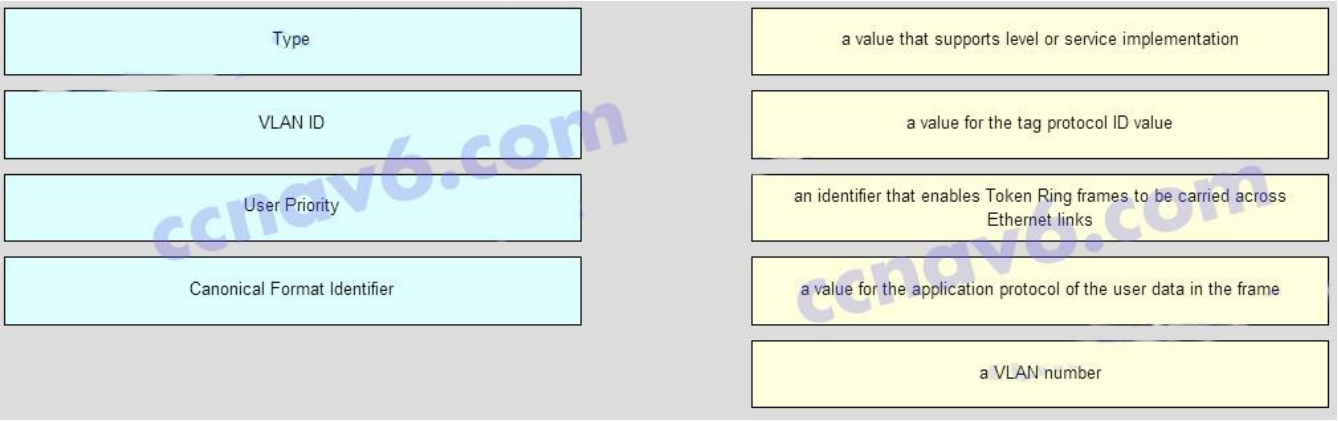
- **the default automatic trunking configuration***

15. **Which two Layer 2 security best practices would help prevent VLAN hopping attacks? (Choose two.)**
    - **Change the native VLAN number to one that is distinct from all user VLANs and is not VLAN 1.***
    - Change the management VLAN to a distinct VLAN that is not accessible by regular users.
    - Statically configure all ports that connect to end-user host devices to be in trunk mode.
    - **Disable DTP autonegotiation on end-user ports.***
    - Use SSH for all remote management access.
16. **Refer to the exhibit. Interface Fa0/1 is connected to a PC. Fa0/2 is a trunk link to another switch. All other ports are unused. Which security best practice did the administrator forget to configure?**

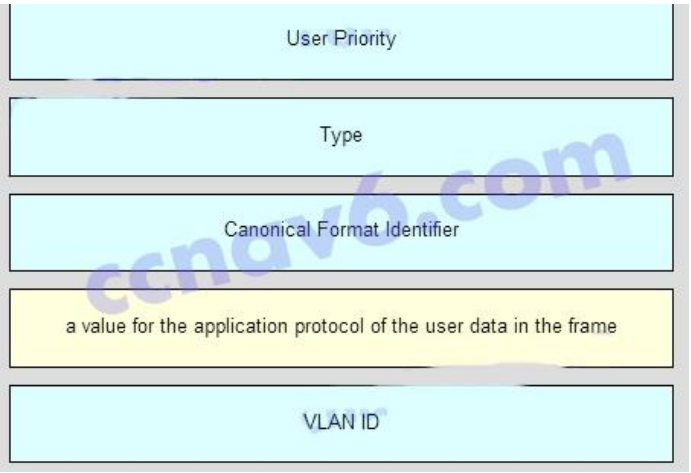
```
ALS1# show running-config
<output omitted>
interface FastEthernet0/1
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 switchport nonegotiate
!

ALS1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
<output omitted>
10   Users                            active
40   Native                           active
50   Management                       active
99   Unused                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
```


    - Disable autonegotiation and set ports to either static access or static trunk.
    - Change the native VLAN to a fixed VLAN that is distinct from all user VLANs and to a VLAN number that is not VLAN 1.
    - Configure all unused ports to a ‘black-hole’ VLAN that is not used for anything on the network.
    - **All user ports are associated with VLANs distinct from VLAN 1 and distinct from the ‘black-hole’ VLAN.***
17. **Match the IEEE 802.1Q standard VLAN tag field with the description. (Not all options are used.)**

- Question



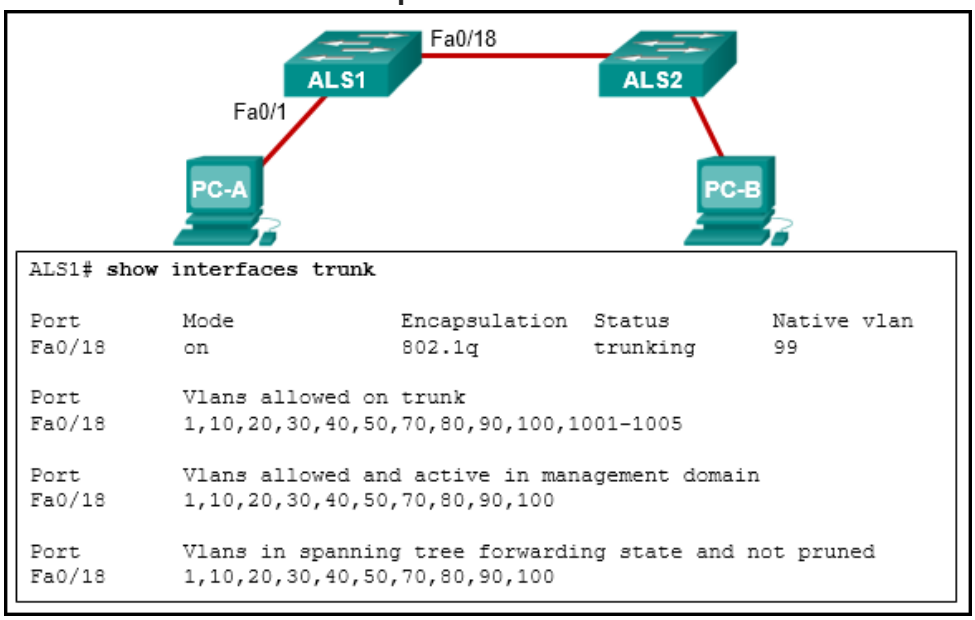
- Answer



18. **A network administrator is determining the best placement of VLAN trunk links. Which two types of point-to-point connections utilize VLAN trunking? (Choose two.)**
    - **between two switches that utilize multiple VLANs***
    - between a switch and a client PC
    - **between a switch and a server that has an 802.1Q NIC***
    - between a switch and a network printer
    - between two switches that share a common VLAN
19. **What is the effect of issuing a *switchport access vlan 20* command on the Fa0/18 port of a switch that does not have this VLAN in the VLAN database?**
    - The command will have no effect on the switch.
    - **VLAN 20 will be created automatically.***
    - An error stating that VLAN 20 does not exist will be displayed and VLAN 20 is not created.
    - Port Fa0/18 will be shut down.
20. **Port Fa0/11 on a switch is assigned to VLAN 30. If the command *no switchport access vlan 30* is entered on the Fa0/11 interface, what will happen?**
    - Port Fa0/11 will be shutdown.
    - An error message would be displayed.
    - **Port Fa0/11 will be returned to VLAN 1.***
    - VLAN 30 will be deleted.
21. **Which command is used to remove only VLAN 20 from a switch?**
    - delete vlan.dat

- delete flash:vlan.dat
- **no vlan 20 ***
- no switchport access vlan 20

22. **Refer to the exhibit. PC-A and PC-B are both in VLAN 60. PC-A is unable to communicate with PC-B. What is the problem?**



CCNA 2 Chapter 3 Exam Answer 002 (v5.02, 2015)

- The native VLAN should be VLAN 60.
- The native VLAN is being pruned from the link.
- The trunk has been configured with the switchport nonegotiate command.
- **The VLAN that is used by PC-A is not in the list of allowed VLANs on the trunk.***

23. **What happens to a port that is associated with VLAN 10 when the administrator deletes VLAN 10 from the switch?**

- **The port becomes inactive.***
- The port goes back to the default VLAN.
- The port automatically associates itself with the native VLAN.
- The port creates the VLAN again.

24. **In a basic VLAN hopping attack, which switch feature do attackers take advantage of?**

- an open Telnet connection
- automatic encapsulation negotiation
- forwarding of broadcasts
- **the default automatic trunking configuration***

25. **Which two Layer 2 security best practices would help prevent VLAN hopping attacks? (Choose two.)**

- **Change the native VLAN number to one that is distinct from all user VLANs and is not VLAN 1.***
- Change the management VLAN to a distinct VLAN that is not accessible by regular users.
- Statically configure all ports that connect to end-user host devices to be in trunk mode.
- **Disable DTP autonegotiation on end-user ports.***
- Use SSH for all remote management access.

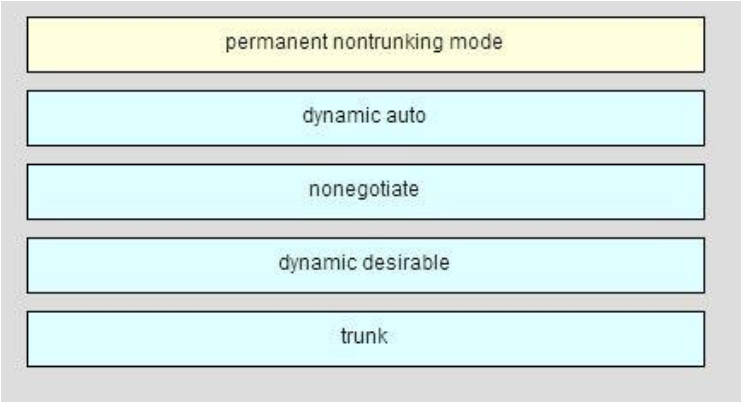
26. **Refer to the exhibit. Interface Fa0/1 is connected to a PC. Fa0/2 is a trunk link to another switch. All other ports are unused. Which security best practice did the**

administrator forget to configure?

```
ALS1# show running-config
<output omitted>
interface FastEthernet0/1
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 switchport nonegotiate
!

ALS1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
<output omitted>
10   Users                            active
40   Native                           active
50   Management                       active
99   Unused                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
```


- Disable autonegotiation and set ports to either static access or static trunk.
- Change the native VLAN to a fixed VLAN that is distinct from all user VLANs and to a VLAN number that is not VLAN 1.
- Configure all unused ports to a ‘black-hole’ VLAN that is not used for anything on the network.
- **All user ports are associated with VLANs distinct from VLAN 1 and distinct from the ‘black-hole’ VLAN.***

27. **Match the DTP mode with its function. (Not all options are used.)**



28. **A network administrator is determining the best placement of VLAN trunk links. Which two types of point-to-point connections utilize VLAN trunking? (Choose two.)**
    - between two switches that share a common VLAN
    - **between a switch and a server that has an 802.1Q NIC***
    - between a switch and a client PC

- between a switch and a network printer
- **between two switches that utilize multiple VLANs***

29. **What happens to a port that is associated with VLAN 10 when the administrator deletes VLAN 10 from the switch?**
    - The port automatically associates itself with the native VLAN.
    - The port creates the VLAN again.
    - The port goes back to the default VLAN.
    - **The port becomes inactive.***
30. **Refer to the exhibit. Interface Fa0/1 is connected to a PC. Fa0/2 is a trunk link to another switch. All other ports are unused. Which security best practice did the administrator forget to configure?**

```
ALS1# show running-config
<output omitted>
interface FastEthernet0/1
 switchport mode access
 switchport nonegotiate
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 40
 switchport mode trunk
 switchport nonegotiate
!

ALS1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
<output omitted>
10   Users                            active
40   Native                           active
50   Management                       active
99   Unused                           active    Fa0/3, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24, Gi0/1, Gi0/2
```


- Configure all unused ports to a ‘black-hole’ VLAN that is not used for anything on the network.
- Disable autonegotiation and set ports to either static access or static trunk.
- Change the native VLAN to a fixed VLAN that is distinct from all user VLANs and to a VLAN number that is not VLAN 1.
- **All user ports are associated with VLANs distinct from VLAN 1 and distinct from the ‘black-hole’ VLAN.***

31. **Which command is used to remove only VLAN 20 from a switch?**
    - no switchport access vlan 20
    - delete flash:vlan.dat
    - **no vlan 20***
    - delete vlan.dat

32. **What is the effect of issuing a switchport access vlan 20 command on the Fa0/18 port of a switch that does not have this VLAN in the VLAN database?**
    - **VLAN 20 will be created automatically.***
    - The command will have no effect on the switch.
    - Port Fa0/18 will be shut down.
    - An error stating that VLAN 20 does not exist will be displayed and VLAN 20 is not created.
33. **Place the options in the following order:**

– not scored –
dynamic auto
nonegotiate
dynamic desirable
trunk

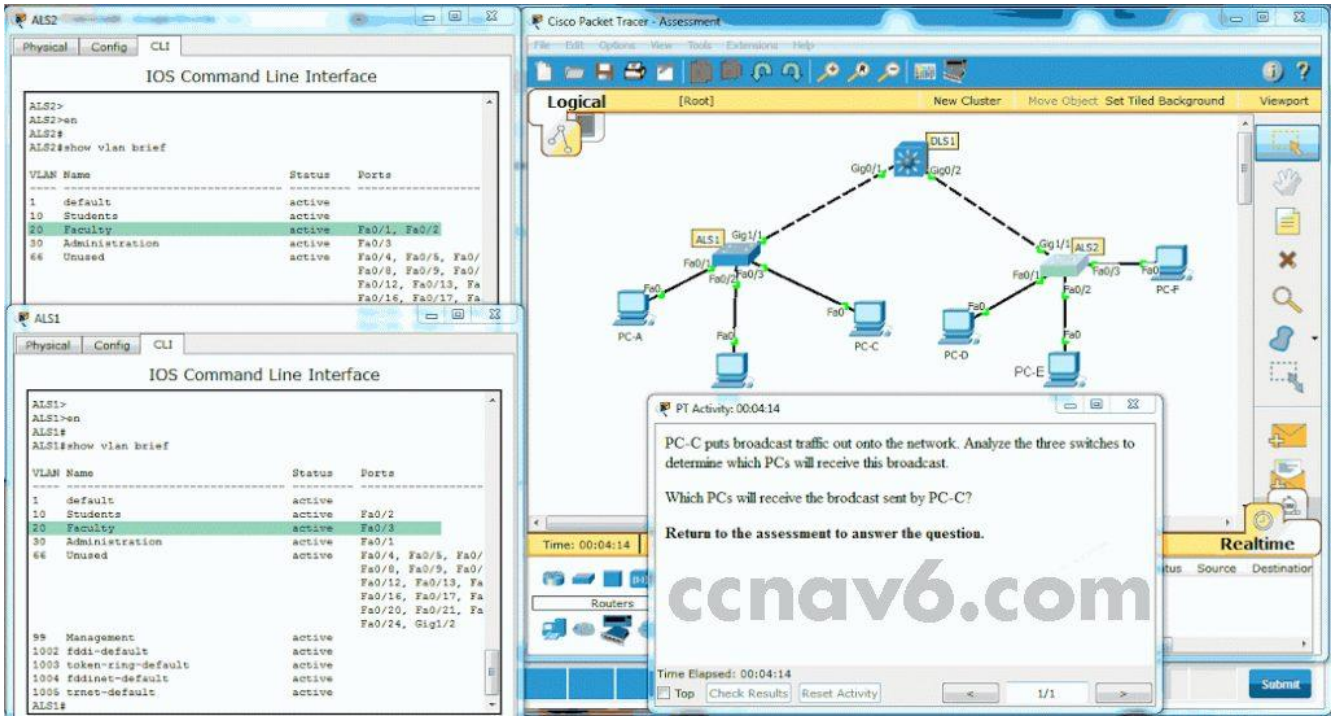
34. **Port Fa0/11 on a switch is assigned to VLAN 30. If the command no switchport access vlan 30 is entered on the Fa0/11 interface, what will happen?**
    - **Port Fa0/11 will be returned to VLAN 1.***
    - VLAN 30 will be deleted.
    - An error message would be displayed.
    - Port Fa0/11 will be shutdown.
35. **Which two Layer 2 security best practices would help prevent VLAN hopping attacks? (Choose two.)**
    - **Disable DTP autonegotiation on end-user ports.***
    - Change the management VLAN to a distinct VLAN that is not accessible by regular users.
    - Statically configure all ports that connect to end-user host devices to be in trunk mode.
    - **Change the native VLAN number to one that is distinct from all user VLANs and is not VLAN 1.***
    - Use SSH for all remote management access.
36. **In a basic VLAN hopping attack, which switch feature do attackers take advantage of?**
    - automatic encapsulation negotiation
    - **the default automatic trunking configuration***
    - an open Telnet connection
    - forwarding of broadcasts

37. **Refer to the exhibit. PC-A and PC-B are both in VLAN 60. PC-A is unable to communicate with PC-B. What is the problem?**


```
ALS1# show interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Fa0/18      on               802.1q         trunking      99

Port        Vlans allowed on trunk
Fa0/18      1,10,20,30,40,50,70,80,90,100,1001-1005

Port        Vlans allowed and active in management domain
Fa0/18      1,10,20,30,40,50,70,80,90,100

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/18      1,10,20,30,40,50,70,80,90,100
```

- The native VLAN is being pruned from the link.
- **The VLAN that is used by PC-A is not in the list of allowed VLANs on the trunk.***
- The trunk has been configured with the switchport nonegotiate command.
- The native VLAN should be VLAN 60.

38. **Under which two occasions should an administrator disable DTP while managing a local area network? (Choose two.)**
    - when a neighbor switch uses a DTP mode of dynamic desirable
    - on links that should dynamically attempt trunking
    - **when connecting a Cisco switch to a non-Cisco switch***
    - when a neighbor switch uses a DTP mode of dynamic auto
    - **on links that should not be trunking***
39. **Open the PT Activity. Perform the tasks in the activity instructions and then answer the question.**

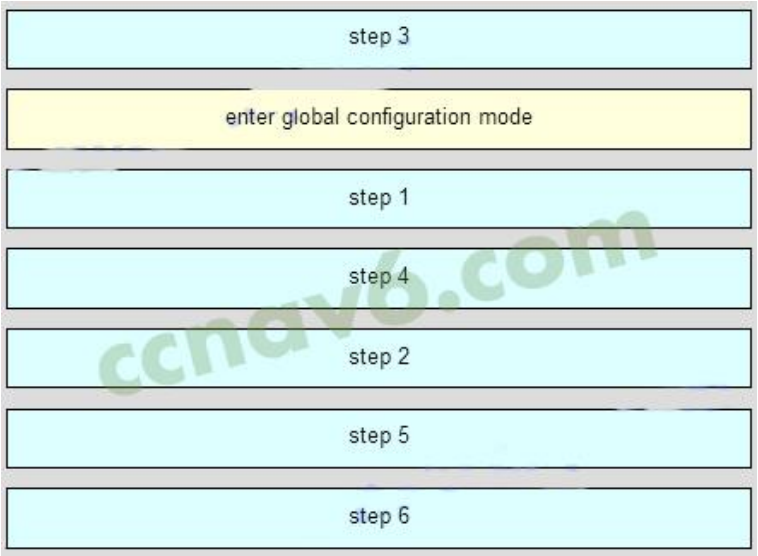


Which PCs will receive the broadcast sent by PC-C?

- **PC-D, PC-E***
- PC-A, PC-B, PC-D, PC-E
- PC-A, PC-B
- PC-A, PC-B, PC-D, PC-E, PC-F
- PC-A, PC-B, PC-E

40. **Which two statements are true about VLAN implementation? (Choose two.)**
    - The network load increases significantly because of added trunking information.
    - **Devices in one VLAN do not hear the broadcasts from devices in another VLAN.***
    - The size of the collision domain is reduced.
    - **VLANs logically group hosts, regardless of physical location.***
    - The number of required switches in a network decreases.
41. **Refer to the exhibit. DLS1 is connected to another switch, DLS2, via a trunk link. A host that is connected to DLS1 is not able to communicate to a host that is connected to DLS2, even though they are both in VLAN 99. Which command should be added to**

Fa0/1 on DLS1 to correct the problem?



- switchport trunk allowed vlan add 99
- **switchport trunk native vlan 66***
- switchport mode dynamic auto
- switchport nonegotiate

42. **Which switch feature ensures that no unicast, multicast, or broadcast traffic is passed between ports that are configured with this feature?**
    - switch port security
    - **PVLAN protected port***
    - ACL
    - VLAN
43. **Fill in the blank. Use the full command syntax.**
    The " **show vlan brief*** " command displays the VLAN assignment for all ports as well as the existing VLANs on the switch.
44. **Which combination of DTP modes set on adjacent Cisco switches will cause the link to become an access link instead of a trunk link?**
    - **dynamic auto – dynamic auto***
    - dynamic desirable – dynamic desirable
    - dynamic desirable – trunk
    - dynamic desirable – dynamic auto
45. **An administrator has determined that the traffic from a switch that corresponds to a VLAN is not being received on another switch over a trunk link. What could be the problem?**
    - trunk mode mismatch
    - **allowed VLANS on trunks***
    - native VLANS mismatch
    - dynamic desirable mode on one of the trunk links
46. **What is the default DTP mode on Cisco 2960 and 3560 switches?**
    - trunk
    - **dynamic auto***
    - access
    - dynamic desirable

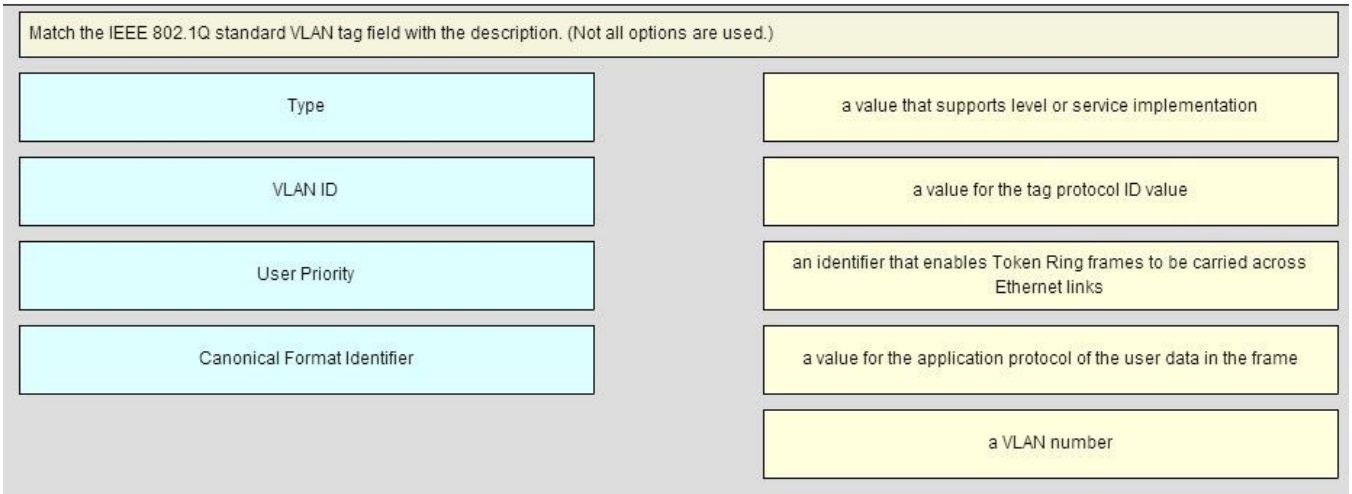
47. **Refer to the exhibit.**

```
ALS2# show interfaces fa0/1 switchport
<output omitted>

Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Access Mode VLAN: 20 (Faculty)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Protected: true
Appliance trust: none
```


What can be determined from the output that is shown?

- **Interface FastEthernet 0/1 is configured with the switchport protected command.***
- Interface FastEthernet 0/1 is configured with the nonegotiate keyword.
- Interface FastEthernet 0/1 is trunking and using Native VLAN 1.
- Interface FastEthernet 0/1 is configured as dynamic auto by the administrator.

48. **Match the IEEE 802.1Q standard VLAN tag field in the description. (not all options are used)**



Place the options in the following order:

User Priority – value that supports level or service implementation
Type – value for the tag protocol ID value
Canonical Format Identifier – identifier that enables Token Ring frames to be carried across Ethernet Links
– not scored – -value for the application protocol of the user data in a frame*
VLAN ID – VLAN number

49. **Which two modes does Cisco recommend when configuring a particular switch port? (Choose two.)**

- **trunk***
- IEEE 802.1Q
- **access***

- Gigabit Ethernet
- FastEthernet
- ISL