- A. It requires multiple links between core switches
- B. It generates one spanning-tree instance for each VLAN
- C. It maps multiple VLANs into the same spanning-tree instance
- D. It uses multiple active paths between end stations.

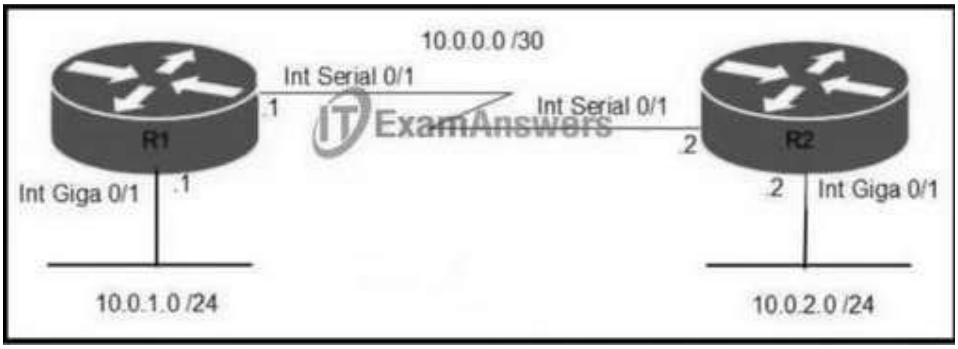
Correct Answer: B

555. Which WLC management connection type is vulnerable to man-in-the-middle attacks?

- A. SSH
- B. HTTPS
- C. Telnet
- D. console

Correct Answer: C

556. Refer to the exhibit. Which command configures OSPF on the point-to-point link between routers R1 and R2?



- A. router-id 10.0.0.15
- B. neighbor 10.1.2.0 cost 180
- C. ipospf priority 100
- D. network 10.0.0.0 0.0.0.3 area 0

Correct Answer: D

557. A network engineer must implement an IPv6 configuration on the vlan 2000 interface to create a routable locally-unique unicast address that is blocked from being advertised to the internet. Which configuration must the engineer apply?

A.
```
interface vlan 2000
ipv6 address ffc0:0000:aaaa::1234:2343/64
```

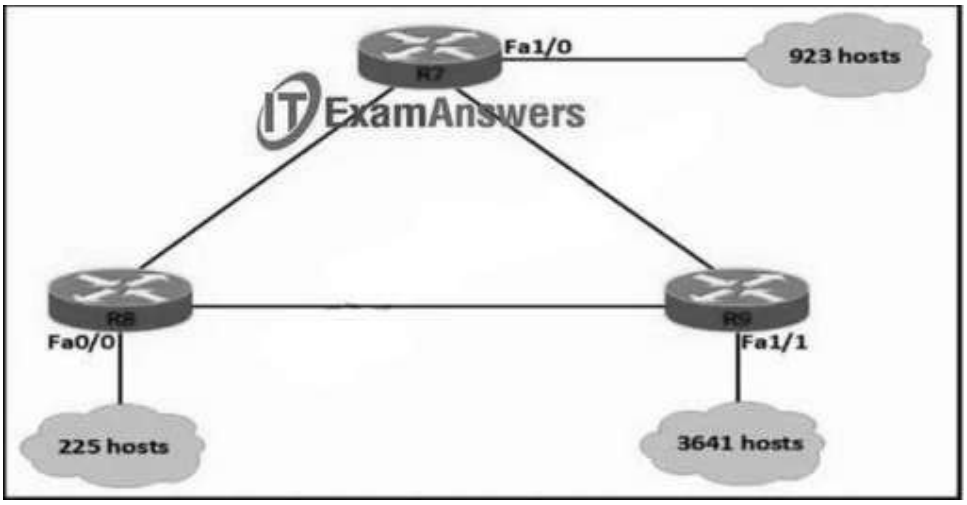
B.
interface vlan 2000
Ipv6 address fc00:0000:aaaa:a15d:1234:2343:8aca/64

C.
interface vlan 2000
ipv6 address fe80;0000:aaaa::1234:2343/64

D.
interface vlan 2000
ipv6 address fd00::1234:2343/64

Correct Answer: D

558. Refer to the exhibit. An IP subnet must be configured on each router that provides enough addresses for the number of assigned hosts and anticipates no more than 10% growth for now hosts. Which configuration script must be used?



A.
R7#
configure terminal
interface Fa 1/0
ip address 10.1.56.1
255.255.252.0
no shutdownR8#
configure terminal
interface Fa0/0
ip address 10.9.32.1
255.255.255.0
no shutdown

B.
R7#
configure terminal
interface Fa1/0
ip address 10.1.56.1
255.255.248.0
no shutdownR8#
configure terminal
interface Fa0/0
ip address 10.9.32.1
255.255.254.0
no shutdown

R9#
configure terminal
interface Fa 1/1
ip address 10.23.96.1
255.255.240.0
no shutdown

C.
R7#
configure terminal
interface Fa 1/0
ip address 10.1.56.1
255.255.240.0
no shutdownR8#
configure terminal
interface Fa0/0
ip address 10.9.32.1
255.255.224.0
no shutdown

R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1
255.255.192.0
no shutdown

R9#
configure terminal
interface Fa1/1
ip address 10.23.96.1
255.255.248.0
no shutdown

D.
R7# configure terminal
interface Fa1/0
ip address 10.1.56.1
255.255.192.0
no shutdownR8#
configure terminal
interface Fa0/0
ip address 10.9.32.1
255.255.224.0
no shutdown

R9#
configure terminal
interface Fa 1/1
ip address 10.23.96.1
255.255.128.0
no shutdown

Correct Answer: A

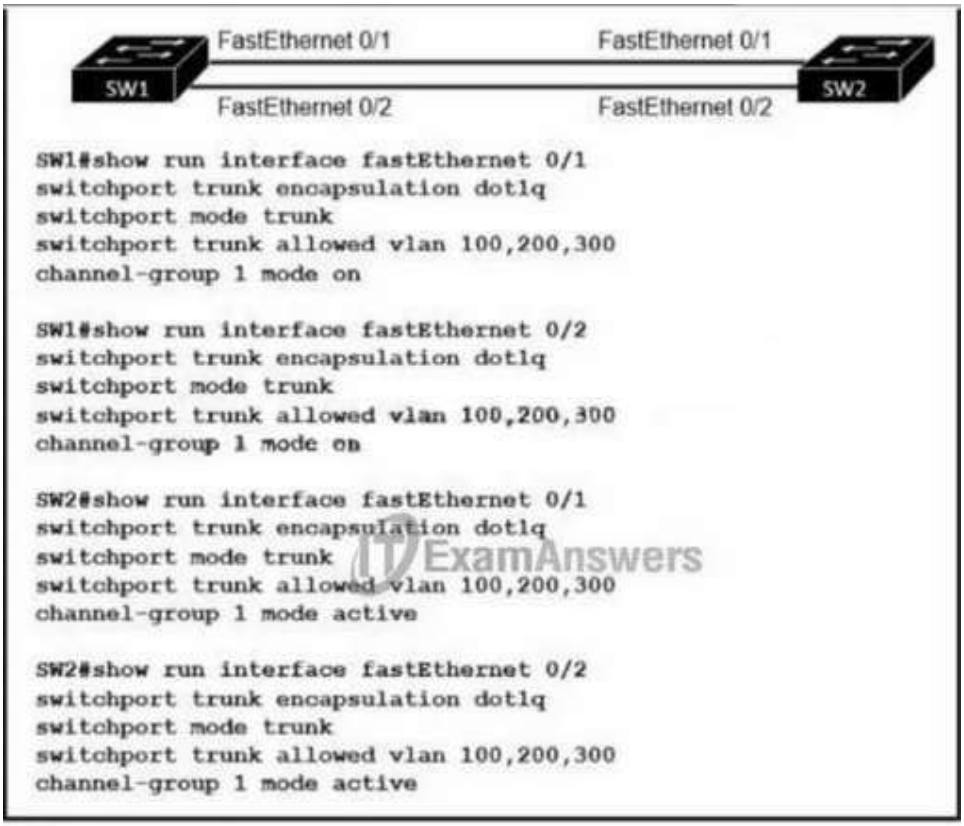
559. Which characteristic differentiates the concept of authentication from authorization and accounting?

- A. user-activity logging
- B. service limitations
- C. consumption-based billing
- **D. identity verification**

Correct Answer: D

560. Refer to the exhibit. An engineer built a new L2 LACP EtherChannel between SW1 and SW2 and executed these show commands to verify the work. Which additional task allows the two switches to

establish an LACP port channel?



- A. Change the channel-group mode on SW2 to auto
- B. Change the channel-group mode on SW1 to desirable.
- C. Configure the interface port-channel 1 command on both switches.
- D. Change the channel-group mode on SW1 to active or passive.

Correct Answer: D

561. Refer to the exhibit. Traffic that is flowing over interface TenGigabitEthernet0/0 experiences slow transfer speeds. What is the

reason for the issue?

```
TenGigabitEthernet0/0/0 is up, line protocol is up
  Hardware is BUILT-IN-2T+6X1GE, address is 74a0.2f7a.0123 (bia 74a0.2f7a.0123)
  Description: Uplink
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 10000Mbps, link type is force-up, media type is unknown media type
  output flow-control is on, input flow-control is on
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:05:40, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 6160000 bits/sec, 1113 packets/sec
  5 minute output rate 11213000 bits/sec, 1553 packets/sec
     12662416065 packets input, 12607032232894 bytes, 0 no buffer
     Received 14117163 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 26271385 multicast, 0 pause input
     7907779058 packets output, 5073750426832 bytes, 0 underruns
     0 output errors, 8662416065 collisions, 1 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
     1 carrier transitions
```

- A. heavy traffic congestion
- B. a duplex incompatibility
- C. a speed conflict
- D. queuing drops

Correct Answer: B

562. Which type of network attack overwhelms the target server by sending multiple packets to a port until the half-open TCP resources of the target are exhausted?

- A. SYN flood
- B. reflection
- C. teardrop
- D. amplification

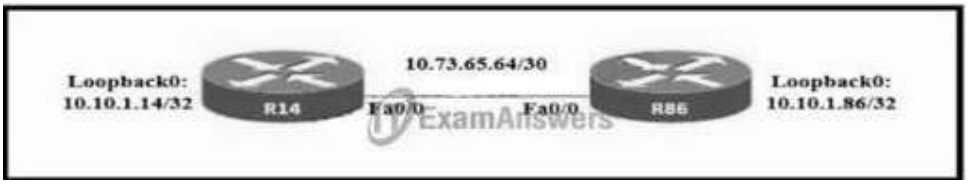
Correct Answer: A

563. Which interface mode must be configured to connect the lightweight APs in a centralized architecture?

- A. WLAN dynamic
- B. management
- C. trunk
- D. access

Correct Answer: D

564. Refer to the exhibit. Which configuration allows routers R14 and R86 to form an OSPFv2 adjacency while acting as a central point for exchanging OSPF information between routers?



A.

```
R14#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf network broadcast
ip ospf 10 area 0
ip mtu 1500

router ospf 10
ip ospf priority 255
router-id 10.10.1.14

R86#
interface Loopback0
ip ospf 10 area 0

interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip ospf network broadcast
ip ospf 10 area 0
ip mtu 1500
```

B.

```
R14#
interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf network broadcast
ip ospf priority 255
ip mtu 1500

router ospf 10
router-id 10.10.1.14
network 10.10.1.14 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
R86#
interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip ospf network broadcast
ip mtu 1500

router ospf 10
router-id 10.10.1.86
network 10.10.1.86 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
```

C.

```
R14#
interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip ospf network broadcast
ip ospf priority 0
ip mtu 1400

router ospf 10
router-id 10.10.1.14
network 10.10.1.14 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
R86#
interface Loopback0
ip address 10.10.1.86 255.255.255.255
```

D.

```
R14#
interface FastEthernet0/0
ip address 10.73.65.65 255.255.255.252
ip cspf network broadcast
ip ospf priority 255
ip mtu 1500

router ospf 10
router-id 10.10.1.14
network 10.10.1.14 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
R86#
interface FastEthernet0/0
ip address 10.73.65.66 255.255.255.252
ip ospf network broadcast
ip mtu 1400

router ospf 10
router-id 10.10.1.86
network 10.10.1.86 0.0.0.0 area 0
network 10.73.65.64 0.0.0.3 area 0
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: B

565. Which two components comprise part of a PKI? (Choose two.)

- A. preshared key that authenticates connections
- B. RSA token
- C. CA that grants certificates
- D. clear-text password that authenticates connections
- E. one or more CRLs

Correct Answer: B,C

566. Which two network actions occur within the data plane? (Choose two.)

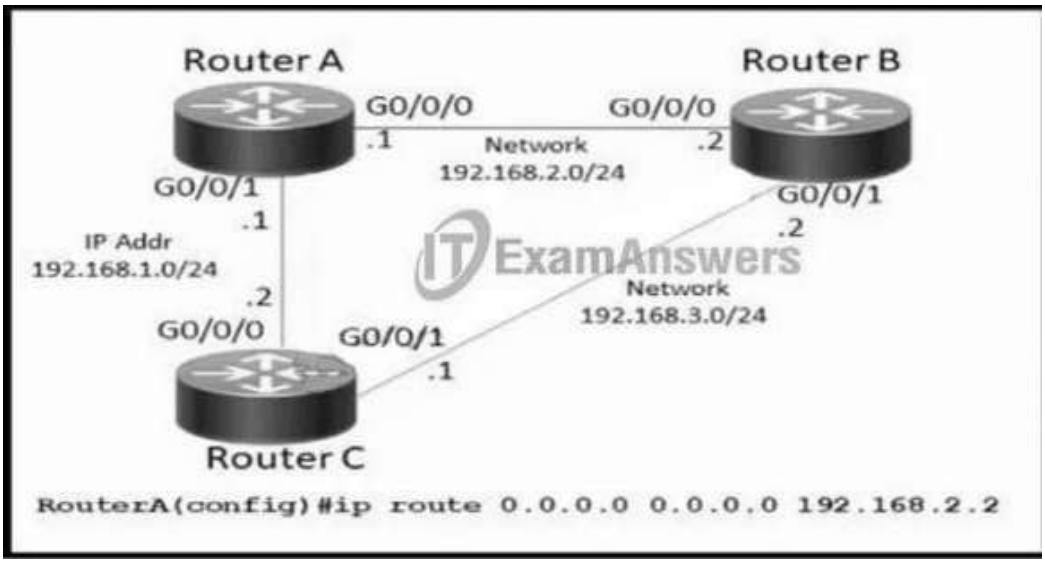
- A. Add or remove an 802.1Q trunking header.
- B. Make a configuration change from an incoming NETCONF RPC.
- C. Run routing protocols.
- D. Match the destination MAC address to the MAC address table.
- E. Reply to an incoming ICMP echo request.

Correct Answer: A,D

Explanation: Actions DATA PLANE:

- De-encapsulating and re-encapsulating a packet in a data-link frame (routers, Layer 3 switches)
- Adding or removing an 802.1Q trunking header (routers and switches)
- Matching an Ethernet frame's destination Media Access Control (MAC) address to the MAC address table (Layer 2 switches)
- Matching an IP packet's destination IP address to the IP routing table (routers, Layer 3 switches)
- Encrypting the data and adding a new IP header (for virtual private network [VPN] processing)
- Changing the source or destination IP address (for Network Address Translation [NAT] processing)
- Discarding a message due to a filter (access control lists [ACLs], port security

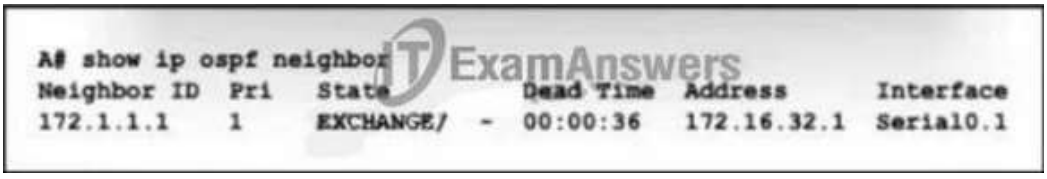
567. Refer to the exhibit. Which command must be issued lo enable a floating static default route on router A?



- A. ip route 0.0.0.0 0.0.0.0 192.168.1.2
- B. ip default-gateway 192.168.2.1
- C. ip route 0.0.0.0 0.0.0.0 192.168.2.1 10
- D. ip route 0.0.0.0 0.0.0.0 192.168.1.2 10

Correct Answer: D

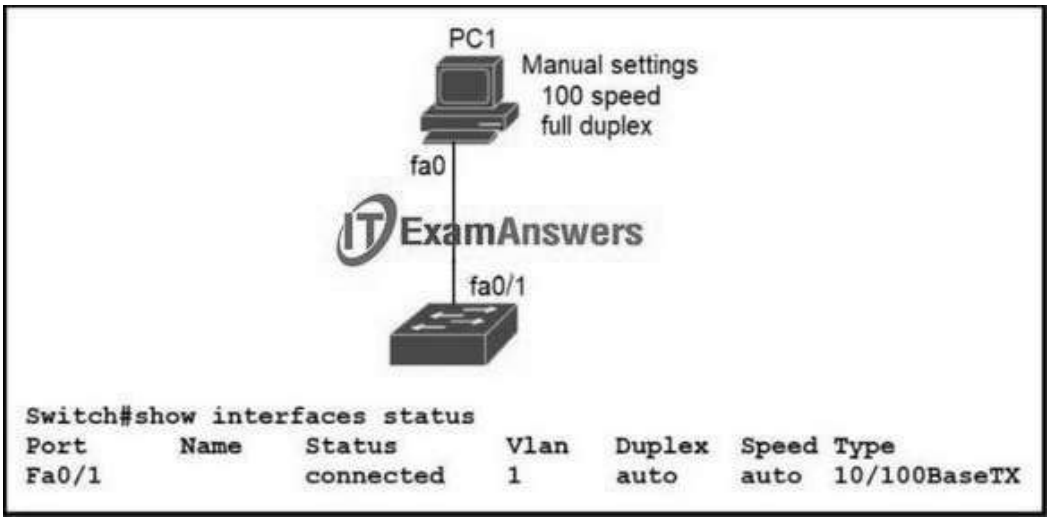
568. Refer to the exhibit. An engineer assumes a configuration task from a peer Router A must establish an OSPF neighbor relationship with neighbor 172 1 1 1 The output displays the status of the adjacency after 2 hours. What is the next step in the configuration process for the routers to establish an adjacency?



- A. Configure router A to use the same MTU size as router B.
- B. Set the router B OSPF ID to a nonhost address.
- C. Configure a point-to-point link between router A and router B.
- D. Set the router B OSPF ID to the same value as its IP address

Correct Answer: A

569. Refer to the exhibit. The link between PC1 and the switch is up. but it is performing poorly. Which interface condition is causing the performance problem?

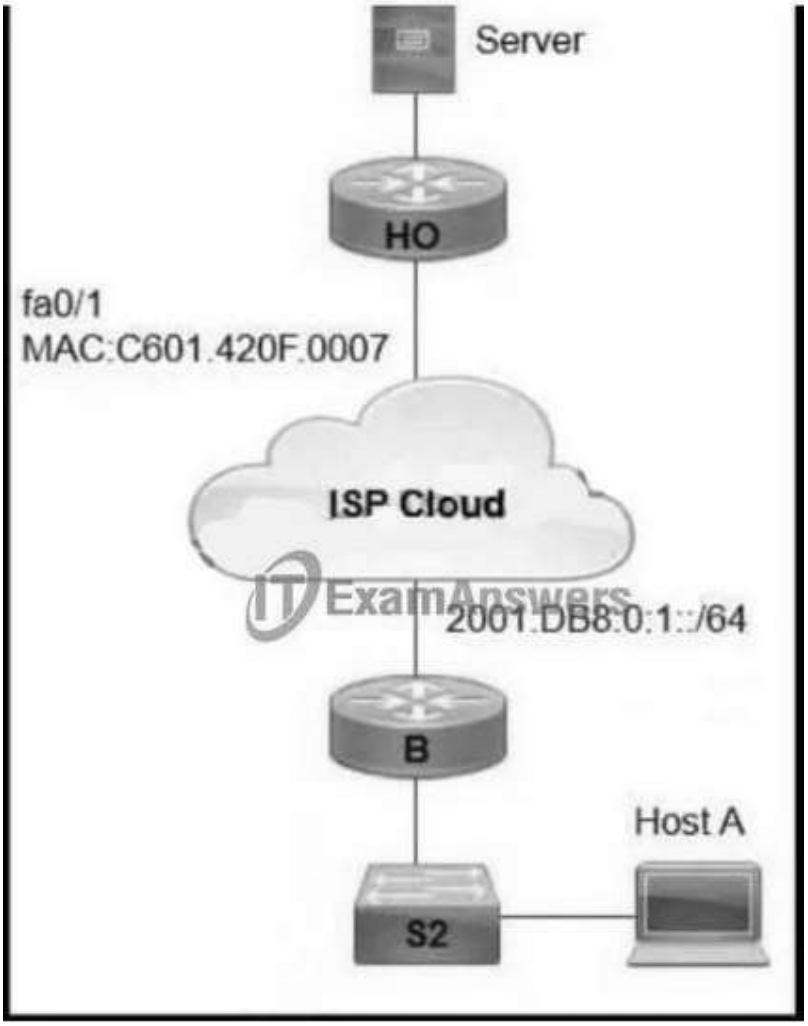


- A. There is a duplex mismatch on the interface
- B. There is an issue with the fiber on the switch interface.
- C. There is a speed mismatch on the interface.
- D. There is an interface type mismatch

Correct Answer: A

570. Refer to the exhibit. An engineer is configuring the HO router. Which IPv6 address configuration must be applied to the router fa0/1 interface for the router to assign a unique 64-bit IPv6 address to

Itself?

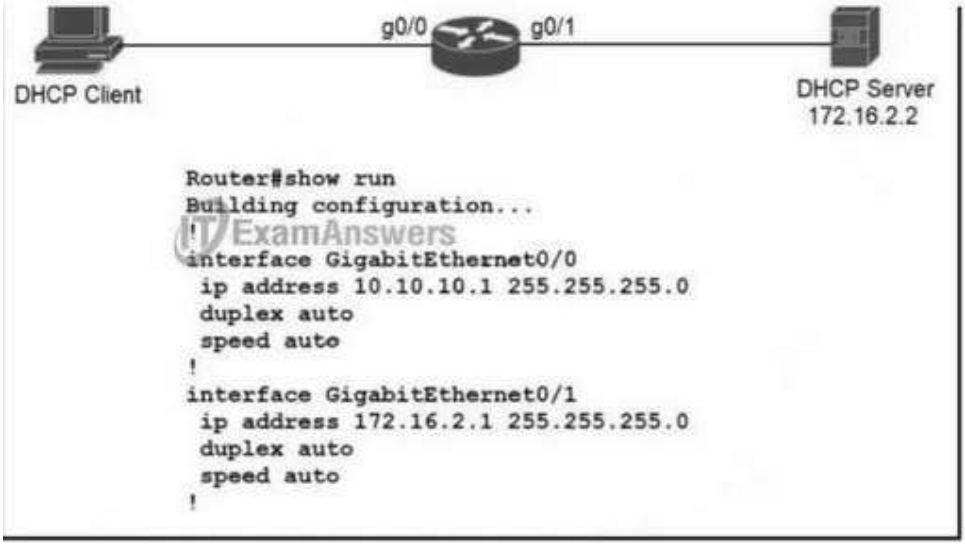


- A. ipv6 address 2001:DB8:0:1:C601:42FF:FE0F:7/64
- B. ipv6 address 2001:DB8:0:1:C601:42FE:800F:7/64
- C. ipv6 address 2001 :DB8:0:1:FFFF:C601:420F:7/64
- D. ipv6 address 2001 :DB8:0:1:FE80:C601:420F:7/64

Correct Answer: B

571. Refer to the exhibit. An engineer is configuring a new router on the network and applied this configuration. Which additional configuration allows the PC to obtain its IP address from a DHCP

server?



- A. Configure the ip dhcp relay information command under interface Gi0/1.
- B. Configure the ip dhcp smart-relay command globally on the router
- C. Configure the ip helper-address 172.16.2.2 command under interface Gi0/0
- D. Configure the ip address dhcp command under interface Gi0/0

Correct Answer: C

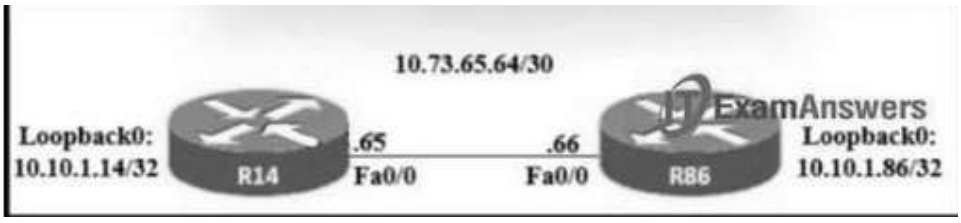
572. A network administrator is setting up a new IPv6 network using the 64-bit address 2001 0EB8 00C1 2200:0001 0000 0000 0331/64 To simplify the configuration the administrator has decided to compress the address Which IP address must the administrator configure?

- A. ipv6 address 21:EB8:C1:2200:1::331/64
- B. ipv6 address 2001:EB8:C1:22:1::331/64
- C. ipv6 address 2001 :EB8:C 1:2200.1 ::331-64
- D. ipv6 address 2001:EB8:C1:2200:1:0000:331/64

Correct Answer: C

573. Refer to the exhibit. A static route must be configured on R14 to forward traffic for the 172 21 34 0/25 network that resides on

R86 Which command must be used to fulfill the request?



- A. ip route 172.21.34.0 255.255.255.192 10.73.65.65
- B. ip route 172.21.34.0 255.255.255.0 10.73.65.65
- C. ip route 172.21.34.0 255.255.128.0 10.73.65.64
- D. ip route 172.21.34.0 255.255.255.128 10.73.65.66

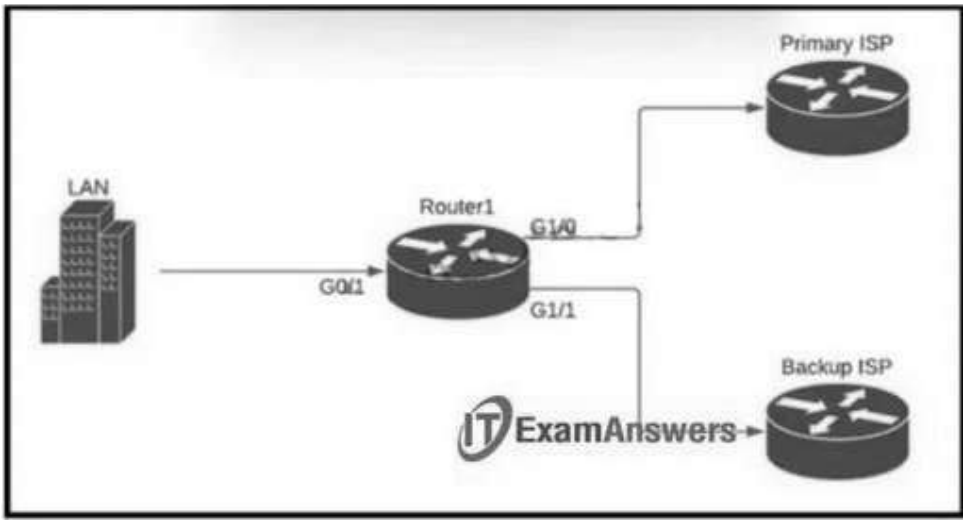
Correct Answer: D

574. What is a function of Opportunistic Wireless Encryption in an environment?

- A. offer compression
- B. increase security by using a WEP connection
- C. provide authentication
- D. protect traffic on open networks

Correct Answer: D

575. Refer to the exhibit. A company is configuring a failover plan and must implement the default routes in such a way that a floating static route will assume traffic forwarding when the primary link goes down. Which primary route configuration must be used?



- A. ip route 0.0.0.0 0.0.0.0 192.168.0.2 GigabitEthernet1/0

- B. ip route 0.0.0.0 0.0.0.0 192.168.0.2 tracked
- C. ip route 0.0.0.0 0.0.0.0 192.168.0.2 floating
- **D. ip route 0.0.0.0 0.0.0.0 192.168.0.2**

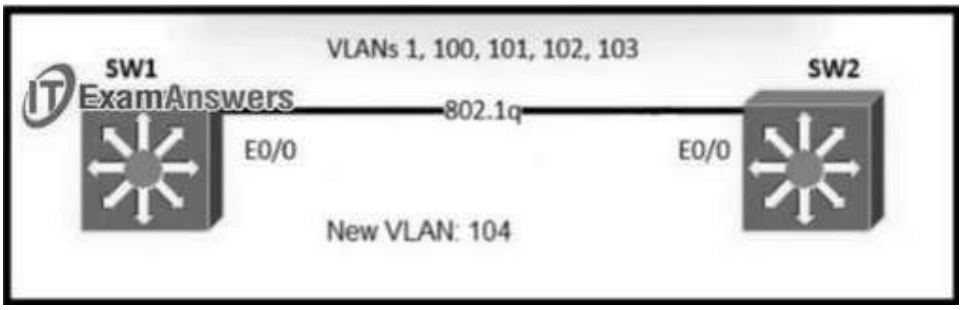
Correct Answer: D

576. Which action implements physical access control as part of the security program of an organization?

- A. configuring a password for the console port
- B. backing up syslogs at a remote location
- C. configuring enable passwords on network devices
- **D. setting up IP cameras to monitor key infrastructure**

Correct Answer: D

577. Refer to the exhibit. An engineer is asked to insert the new VLAN into the existing trunk without modifying anything previously configured Which command accomplishes this task?



- A. switchport trunk allowed vlan 100-104
- **B. switchport trunk allowed vlan add 104**
- C. switchport trunk allowed vlan all
- D. switchport trunk allowed vlan 104

Correct Answer: B

578. Refer to the exhibit. What is a reason for poor performance on the network interface?

```
Hardware is ISR4331-3x1GE, address is 5486.bc25.1f70 (bia 5486.bc25.1f70)
Description: << WAN Link >>
Internet address is 192.0.2.2/30
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
   reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive not supported
Full Duplex, 1000Mbps, link type is auto, media type is RJ45
output flow-control is off, input flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:00, output 00:00:11, output hang never
Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 7000 bits/sec, 4 packets/sec
5 minute output rate 4000 bits/sec, 4 packets/sec
   22579370 packets input, 8825545968 bytes, 0 no buffer
   Received 67 broadcasts (0 IP multicasts)
   0 runts, 0 giants, 0 throttles
   3612699 input errors, 3612699 CRC, 0 frame, 0 overrun, 0 ignored
   0 watchdog, 10747057 multicast, 0 pause input
   12072167 packets output, 1697953637 bytes, 0 underruns
   0 output errors, 0 collisions, 1 interface resets
   6 unknown protocol drops
   0 babbles, 0 late collision, 0 deferred
   5 lost carrier, 0 no carrier, 0 pause output
   0 output buffer failures, 0 output buffers swapped out
```


- A. The interface is receiving excessive broadcast traffic.
- B. The cable connection between the two devices is faulty.
- C. The interface is operating at a different speed than the connected device.
- D. The bandwidth setting of the interface is misconfigured

Correct Answer: B

579. Refer to the exhibit. The following must be considered:
* SW1 is fully configured for all traffic
* The SW4 and SW9 links to SW1 have been configured
* The SW4 interface Gi0/1 and Gi0/0 on SW9 have been configured
* The remaining switches have had all VLANs added to their VLAN database.

Which configuration establishes a successful ping from PC2 to PC7

without interruption to traffic flow between other PCs?

A)

```
SW4#
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14,108

SW11#
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14,108
!
interface Gi0/1
switchport mode trunk
switchport trunk allowed vlan 14,108

SW9#
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14
```

B)

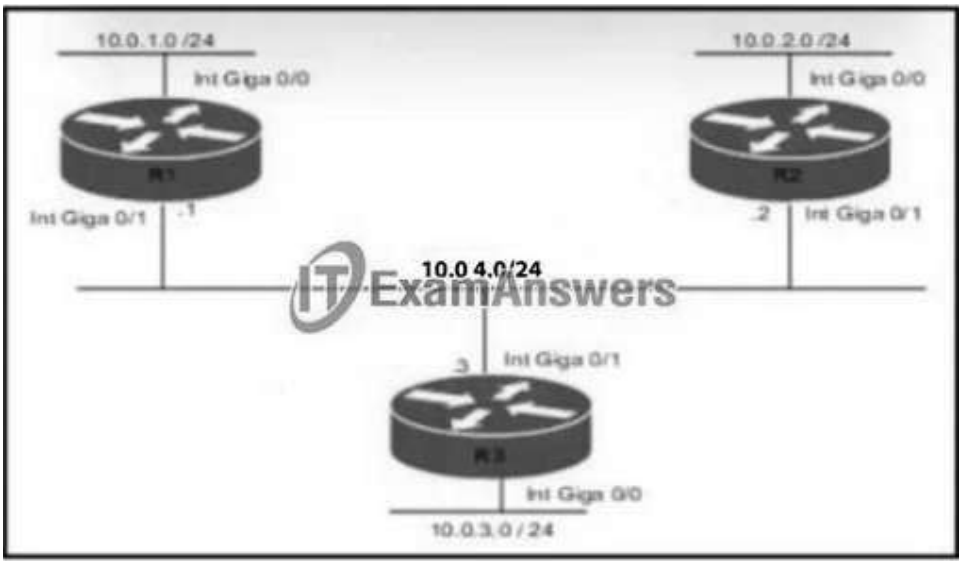
```
SW4#
interface Gi0/2
switchport mode trunk
switchport trunk allowed vlan 14

SW11#
```

- A. Option A
- B. Option B

Correct Answer: A

580. Refer to the exhibit. Routers R1 and R3 have the default configuration The router R2 priority is set to 99 Which commands on

R3 configure it as the DR in the 10.0 4.0/24 network?



- A. R3(config)#interface Gig0/1 R3(config-if)#ip ospf priority 100
- B. R3(config)#interface Gig0/0 R3(config-if)#ip ospf priority 100
- C. R3(config)#interface Gig0/0 R3(config-if)i=ip ospf priority 1
- D. R3(config)#interface Gig0/1 R3(config-if)#ip ospf priority 0

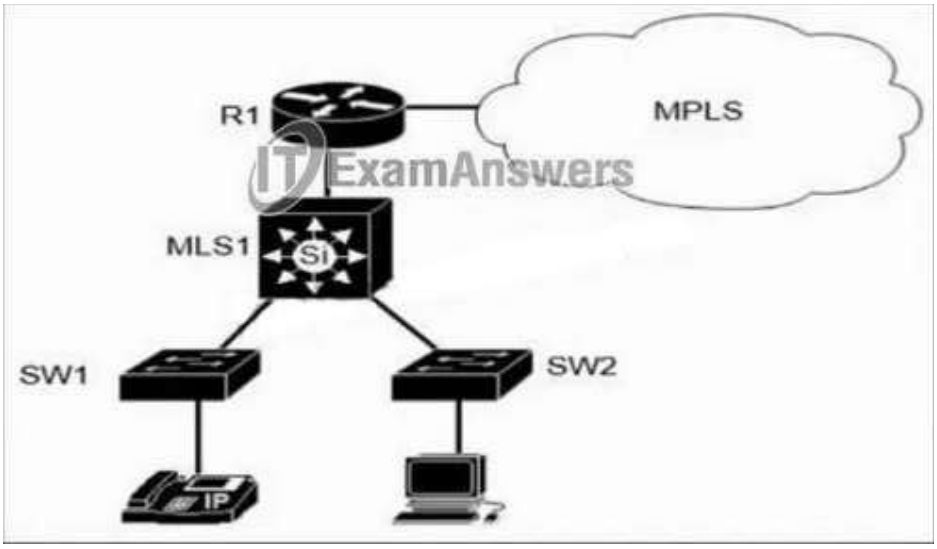
Correct Answer: A

581. Which QoS per-hop behavior changes the value of the ToS field in the IPv4 packet header?

- A. shaping
- B. classification
- C. policing
- D. marking

Correct Answer: D

582. Refer to the exhibit. Which plan must be Implemented to ensure optimal QoS marking practices on this network?

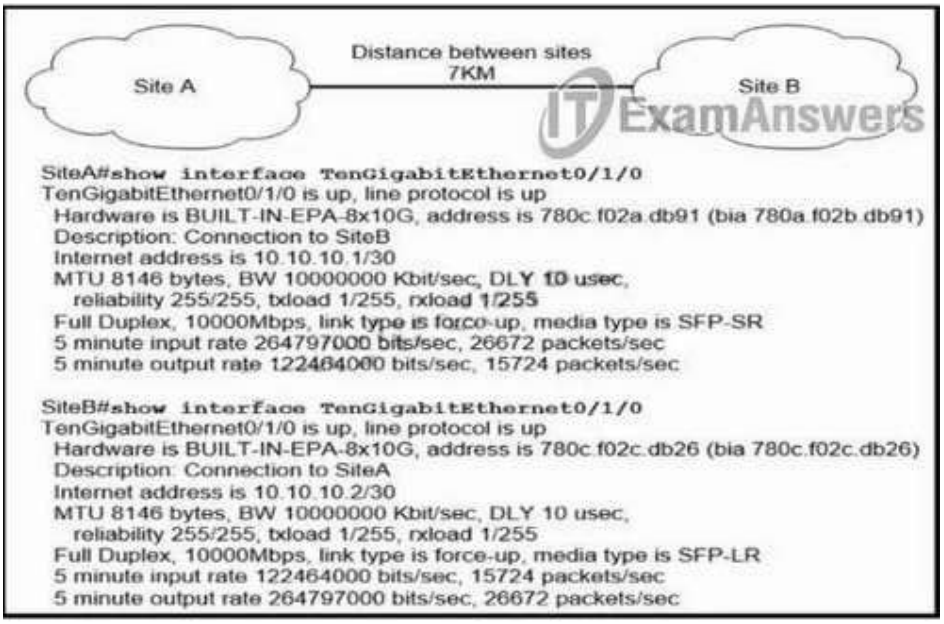


- A. As traffic traverses MLS1 remark the traffic, but trust all markings at the access layer.
- B. Trust the IP phone markings on SW1 and mark traffic entering SW2 at SW2.
- C. Remark traffic as it traverses R1 and trust all markings at the access layer.
- D. As traffic enters from the access layer on SW1 and SW2. trust all traffic markings.

Correct Answer: B

583. Refer to the exhibit. Site A was recently connected to site B over a new single-mode fiber path. Users at site A report Intermittent connectivity Issues with applications hosted at site B.

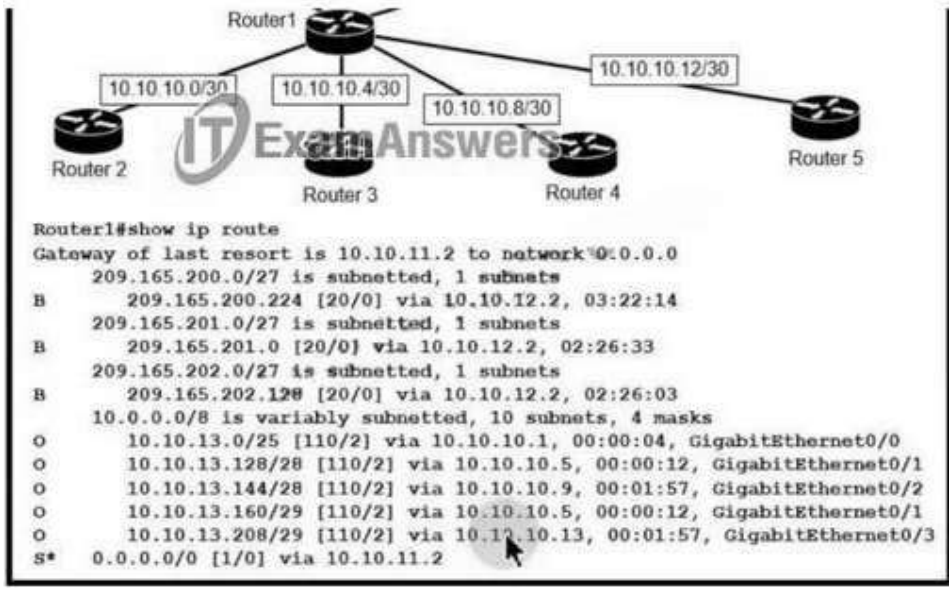
What is the reason for the problem?



- A. Heavy usage is causing high latency.
- B. An incorrect type of transceiver has been inserted into a device on the link.
- C. physical network errors are being transmitted between the two sites.
- D. The wrong cable type was used to make the connection.

Correct Answer: B

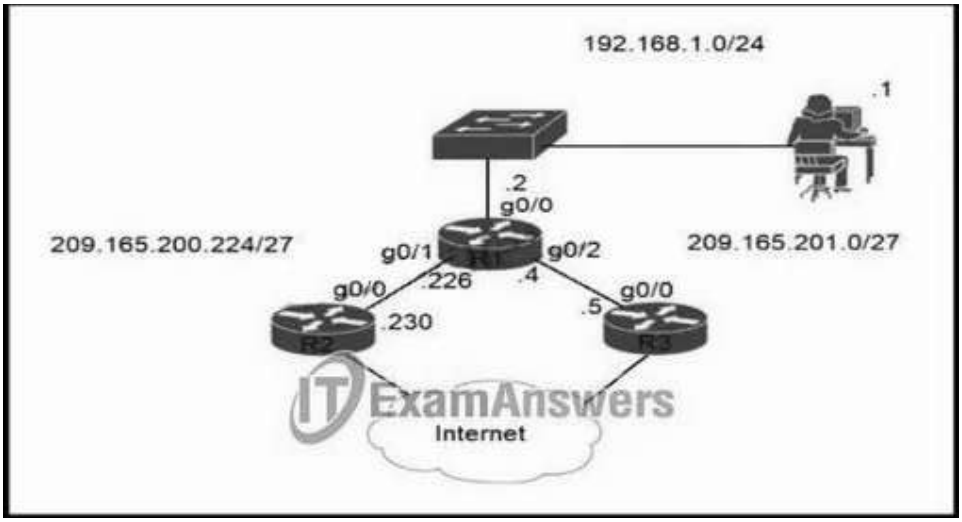
584. Refer to the exhibit. Which next-hop IP address does Routed use for packets destined to host 10.10.13.158?



- A. 10.10.10.5
- B. 10.10.11.2
- C. 10.10.12.2
- D. 10.10.10.9

Correct Answer: D

585. Refer to the exhibit. Router R1 currently is configured to use R3 as the primary route to the Internet, and the route uses the default administrative distance settings. A network engineer must configure R1 so that it uses R2 as a backup, but only if R3 goes down. Which command must the engineer configure on R1 so that it correctly uses R2 as a backup route, without changing the administrative distance configuration on the link to R3?



- A. ip route 0.0.0.0 0.0.0.0 g0/1 1
- B. ip route 0.0.0.0 0.0.0.0 209.165.201.5 10
- C. ip route 0.0.0.0 0.0.0.0 209.165.200.226 1
- D. ip route 0,0.0.0 0.0.0.0 g0/1 6

Correct Answer: D

586. A network engineer is installing an IPv6-only capable device. The client has requested that the device IP address be reachable only from the internal network. Which type of IPv6 address must the engineer assign?

- A. unique local address
- B. link-local address
- C. aggregatable global address
- D. IPv4-compatible IPv6 address

Correct Answer: A

587. A network engineer must configure two new subnets using the address block 10.70.128.0/19 to meet these requirements:
* The first subnet must support 24 hosts
* The second subnet must support 472 hosts
* Both subnets must use the longest subnet mask possible from the address block.
Which two configurations must be used to configure the new subnets and meet a requirement to use the first available address in each subnet for the router interfaces? (Choose two)

A.
```
interface vlan 1234
ip address 10.70.159.1 255.255.254.0
```

B.
```
interface vlan 1148
ip address 10.70.148.1 255.255.254.0
```

C.
```
interface vlan 4722
ip address 10.70.133.17 255.255.255.192
```

D.
```
interface vlan 3002
ip address 10.70.147.17 255.255.255.224
```

E.
```
interface vlan 155
ip address 10.70.155.65 255.255.255.224
```

Correct Answer: B,E

588. What is one reason to implement LAG on a Cisco WLC?

- A. to increase security and encrypt management frames
- **B. to provide link redundancy and load balancing**
- C. to allow for stateful and link-state failover
- D. to enable connected switch ports to failover and use different VLANs

Correct Answer: B

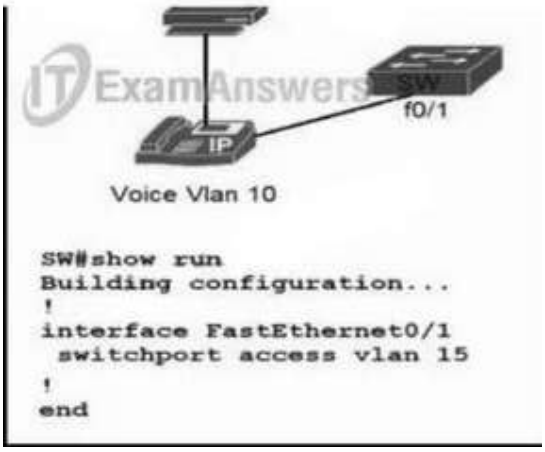
589. Refer to the exhibit. Web traffic is coming in from the WAN interface. Which route takes precedence when the router is processing traffic destined for the LAN network at 10.0.10.0/24?

```
R1# show ip route
     Codes:
     C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP, D -
     EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA
     external type 1, N2 - OSPF NSSA external type 2, E1 - OSPF external type
     1, E2 - OSPF external type 2, E - EGP
     i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default,
     U - per-user static route, o - ODR
Gateway of last resort is not set
C    10.0.0.0/8 is directly connected, Loopback0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
O    10.0.1.3/32 [110/100] via 10.0.1.100, 00:39:08, Serial0
C    10.0.1.0/24 is directly connected, Serial0
O    10.0.1.5/32 [110/5] via 10.0.1.50, 00:39:08, Serial0
O    10.0.10.0/24 [110/10] via 10.0.1.4, 00:39:08, Gigabit Ethernet 0/0
D    10.0.10.0/24 [90/10] via 10.0.1.5, 00:39:08, Gigabit Ethernet 0/1
```

- A. via next-hop 10.0.1.5
- B. via next-hop 10 0 1.4
- C. via next-hop 10.0 1.50
- D. via next-hop 10.0 1 100

Correct Answer: A

590. Refer to the exhibit. All VLANs are present in the VLAN database. Which command sequence must be applied to complete the configuration?




```
SW#show run
Building configuration...
!
interface FastEthernet0/1
 switchport access vlan 15
!
end
```

- A. Interface FastEthernet0/1 switchport trunk native vlan 10 switchport trunk allowed vlan 10,15
- B. Interface FastEthernet0/1 switchport mode trunk switchport trunk allowed vlan 10,15
- C. interface FastEthernet0/1 switchport mode access switchport voice vlan 10
- D. Interface FastEthernet0/1 switchport trunk allowed vlan add 10 vlan 10 private-vlan isolated

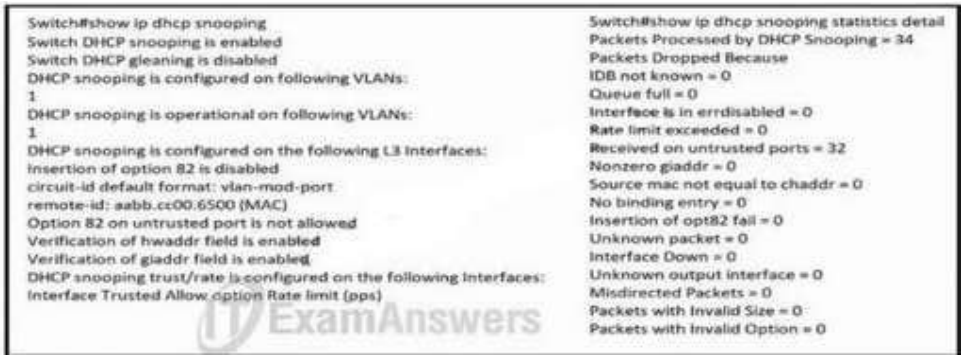
Correct Answer: C

591. Refer to the exhibit. An engineer is updating the R1 configuration to connect a new server to the management network. The PCs on the management network must be blocked from pinging the default gateway of the new server. Which command must be configured on R1 to complete the task?

- A. R1(config)#ip route 172.16.2.2 255.255.255.248 gi0/1
- B. R1(config)#ip route 172.16.2.2 255.255.255.255 gi0/0
- C. R1(conflg)#ip route 172.16.2.0 255.255.255.0 192.168.1.15
- D. R1(conflg)#ip route 172.16.2.0 255.255.255.0 192.168.1.5

Correct Answer: B

592. Refer to the exhibit. The DHCP server and clients are connected to the same switch. What is the next step to complete the DHCP configuration to allow clients on VLAN 1 to receive addresses from the DHCP server?



- A. Configure the ip dhcp snooping trust command on the interlace that is connected to the DHCP client.
- B. Configure the ip dhcp relay information option command on the interface that is connected to the DHCP client.
- C. Configure the ip dhcp snooping trust command on the interface that is connected to the DHCP server.
- D. Configure the Ip dhcp relay information option command on the interface that is connected to the DHCP server.

Correct Answer: C

593. An engineer is configuring remote access to a router from IP subnet 10.139.58.0/28. The domain name, crypto keys, and SSH have been configured. Which configuration enables the traffic on the destination router?

A)
```
interface FastEthernet0/0
 ip address 10.122.49.1 255.255.255.240
 access-group 120 in

ip access-list extended 120
 permit tcp 10.139.58.0 255.255.255.248 any eq 22
```
B)
```
interface FastEthernet0/0
 ip address 10.122.49.1 255.255.255.252
 ip access-group 110 in

ip access-list extended 110
 permit tcp 10.139.58.0 0.0.0.15 host 10.122.49.1 eq 22
```
C)
```
interface FastEthernet0/0
 ip address 10.122.49.1 255.255.255.248
 ip access-group 10 in

ip access-list standard 10
 permit udp 10.139.58.0 0.0.0.7 host 10.122.49.1 eq 22
```
D)
```
interface FastEthernet0/0
 ip address 10.122.49.1 255.255.255.252
 ip access-group 105 in

ip access-list standard 105
 permit tcp 10.139.58.0 0.0.0.7 eq 22 host 10.122.49.1
```

- A. Option A
- B. Option B
- C. Option C
- D. Option D

Correct Answer: B

594. Which PoE mode enables powered-device detection and guarantees power when the device is detected?

- A. dynamic
- B. static
- C. active
- D. auto

Correct Answer: B

595. A Cisco engineer must configure a single switch interface to meet these requirements

- accept untagged frames and place them in VLAN 20
- accept tagged frames in VLAN 30 when CDP detects a Cisco IP phone

Which command set must the engineer apply?

A.
```
switchport mode dynamic desirable
switchport access vlan 20
switchport trunk allowed vlan 30
switchport voice vlan 30
```

B.
```
switchport mode dynamic auto
switchport trunk native vlan 20
switchport trunk allowed vlan 30
switchport voice vlan 30
```

C.
```
switchport mode access
switchport access vlan 20
switchport voice vlan 30
```

D.
```
switchport mode trunk
switchport access vlan 20
switchport voice vlan 30
```

Correct Answer: C

596. Refer to the exhibit. Which minimum configuration items are needed to enable Secure Shell version 2 access to R15?

A.

```
Router(config)#hostname R15
R15(config)#crypto key generate rsa general-keys modulus 1024
R15(config-line #line vty 0 15
R15(config-line)#transport input ssh
R15(config)#ip ssh source-interface Fa0/0
R15(config)#ip ssh stricthostkeycheck
```

B.

```
Router(config)#crypto key generate rsa general-keys modulus 1024
Router(config)#ip ssh version 2
Router(config-line #line vty 0 15
Router(config-line)#transport input ssh
Router(config)#ip ssh logging events
R15(config)#ip ssh stricthostkeycheck
```

C.

```
Router(config)#ip domain-name cisco.com
Router(config)#crypto key generate rsa general-keys modulus 1024
Router(config)#ip ssh version 2
Router(config-line)#line vty 0 15
Router(config-line)#transport input all
Router(config)#ip ssh logging events
```

D.

```
Router(config)#hostname R15
```

```
R15(config)#ip domain-name cisco.com
R15(config)#crypto key generate rsa general-keys modulus 1024
R15(config)#ip ssh version 2
R15(config-line)#line vty 0 15
R15(config-line)#transport input ssh
```

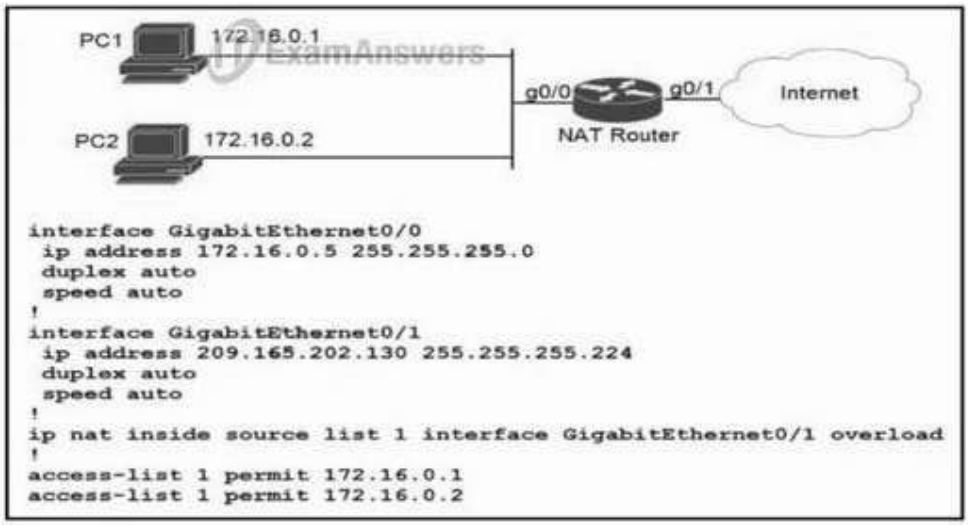
Correct Answer: D

597. Refer to the exhibit. Users need to connect to the wireless network with IEEE 802. 11r-compatible devices. The connection must be maintained as users travel between floors or to other areas in the building. What must be the configuration of the connection?

- A. Select the WPA Policy option with the CCKM option.
- B. Disable AES encryption.
- C. Enable Fast Transition and select the FT 802.1x option.
- D. Enable Fast Transition and select the FT PSK option.

Correct Answer: D

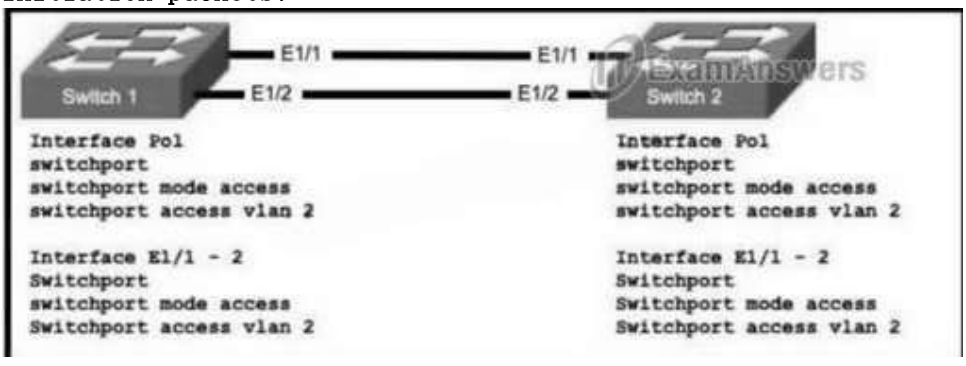
598. Refer to the exhibit. How should the configuration be updated to allow PC1 and PC2 access to the Internet?



- A. Modify the configured number of the second access list.
- B. Add either the ip nat {inside|outside} command under both interfaces.
- C. Remove the overload keyword from the ip nat inside source command.
- D. Change the ip nat inside source command to use interface GigabitEthernet0/0.

Correct Answer: B

599. Refer to the exhibit. An engineer is configuring an EtherChannel using LACP between Switches 1 and 2. Which configuration must be applied so that only Switch 1 sends LACP initiation packets?



A.
Switch 1 (config-if)#channel-group 1 mode on
Swrtch2(config-if)#channel-group 1 mode passive

B.

```
Switch1(config-if)#channel-group 1 mode passive
Switch2(config-if)#channel-group 1 mode active
```

C.

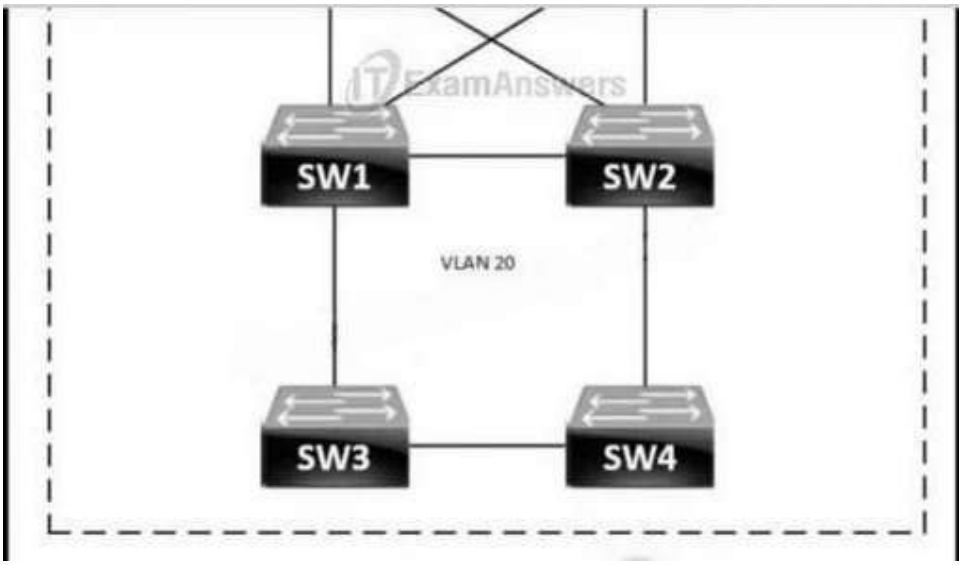
```
Switch1{config-if)#channel-group 1 mode active
Switch2(config-if)#channel-group 1 mode passive
```

D.

```
Switch1(config-if)#channel-group 1 mode on
Switch2(config-if)#channel-group 1 mode active
```

Correct Answer: C

600. Refer to the exhibit. Which switch becomes the root of a spanning tree for VLAN 20 if all links are of equal speed?



- A. SW1 = 24596 0018.184e.3c00
- B. SW2 = 28692 004a.14e5.4077
- C. SW3 = 32788 0022.55cf.dd00
- D. SW4 = 64000 0041.454d.407f

Correct Answer: A

601. Refer to the exhibit. Packets received by the router from BGP enter via a serial interface at 209 165 201 1 Each route is present within the routing table Which interface is used to forward traffic

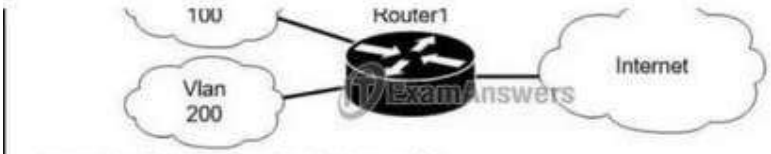
with a destination IP of 10.1.1.19?

```
RIP     10.1.1.16/28[120/5]  via  F0/0
OSPF    10.1.1.0/24[110/30]  via  F0/1
OSPF    10.1.1.0/24[110/40]  via  F0/2
EIGRP   10.1.0.0/26[90/20]   via  F0/3
EIGRP   10.0.0.0/8 [90/133]  via  F0/4
```

- A. F0/4
- B. F0/0
- C. F0/1
- D. F0/3

Correct Answer: B

602. Refer to the exhibit. Users on existing VLAN 100 can reach sites on the Internet. Which action must the administrator take to establish connectivity to the Internet for users in VLAN 200?



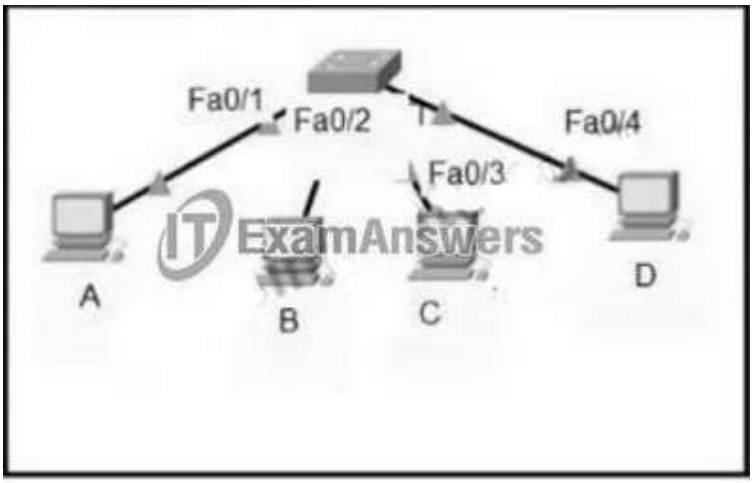

```
Router1(config)#interface GigabitEthernet0/0
Router1(config-if)#ip address 209.165.200.225 255.255.255.224
Router1(config-if)#ip nat outside
Router1(config)#interface GigabitEthernet0/1
Router1(config-if)#ip nat inside
Router1(config)#interface GigabitEthernet0/1.100
Router1(config-if)#encapsulation dot1Q 100
Router1(config-if)#ip address 10.10.10.1 255.255.255.0
Router1(config)#interface GigabitEthernet0/1.200
Router1(config-if)#encapsulation dot1Q 200
Router1(config-if)#ip address 10.10.20.1 255.255.255.0
Router1(config)#ip access-list standard NAT_INSIDE_RANGES
Router1(config-std-nacl)#permit 10.10.10.0 0.0.0.255
Router1(config)#ip nat inside source list NAT_INSIDE_RANGES interface GigabitEthernet0/0 overload
```

- A. Define a NAT pool on the router.
- B. Configure static NAT translations for VLAN 200.
- C. Configure the ip nat outside command on another interface for VLAN 200.
- D. Update the NAT_INSIDE_RANGES ACL

Correct Answer: D

603. Refer to the exhibit. Host A sent a data frame destined for host D What does the switch do when it receives the frame from host

A?



SwitchA#show mac-address table
Mac Address Table

Vlan	Mac Address	Type	Ports
2	000c.859c.bb7b	DYNAMIC	Fa0/1
2	0010.11dc.3e91	DYNAMIC	Fa0/2
2	0041.45d7.c451	DYNAMIC	Fa0/3

SwitchA#

- A. It drops the frame from the switch CAM table.
- B. It floods the frame out of all ports except port Fa0/1.
- C. It shuts down the port Fa0/1 and places it in err-disable mode.
- D. It experiences a broadcast storm.

Correct Answer: B

604. Which protocol uses the SSL?

- A. HTTP
- B. SSH
- C. HTTPS
- D. Telnet

Correct Answer: C

605. Which value is the unique identifier that an access point uses to establish and maintain wireless connectivity to wireless network devices?

- A. VLANID
- B. SSID

- C. RFID
- D. WLANID

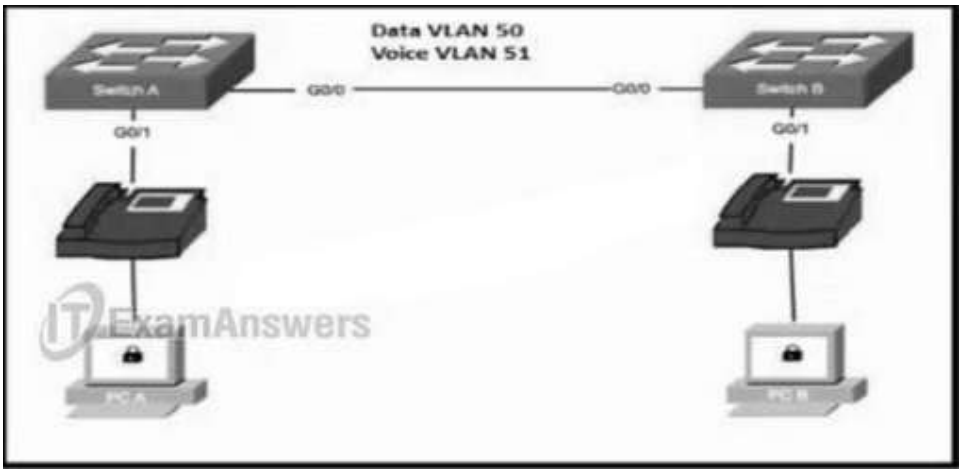
Correct Answer: B

606. A network engineer is configuring a switch so that it is remotely reachable via SSH. The engineer has already configured the host name on the router. Which additional command must the engineer configure before entering the command to generate the RSA key?

- A. password password
- B. crypto key generate rsa modulus 1024
- C. ip domain-name domain
- D. ip ssh authentication-retries 2

Correct Answer: C

607. Refer to the exhibit. Switch A is newly configured. All VLANs are present in the VLAN database. The IP phone and PC A on Gi0/1 must be configured for the appropriate VLANs to establish connectivity between the PCs. Which command set fulfills the requirement?



A.

```
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vian 50
SwitchA(config-if)#switchport voice vlan 51
```

B.

```
SwitchA(config-if)#switchport mode access
SwitchA(config-if)#switchport access vlan 50
SwitchA(config-if)#switchport voice vlan untagged
```

C.
```
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan add 50, 51
SwitchA(config-if)#switchport voice vlan dot1p
```

D.
```
SwitchA(config-if)#switchport mode trunk
SwitchA(config-if)#switchport trunk allowed vlan 50, 51
SwitchA(config-if)#mls qos trust cos
```

Correct Answer: A

608. Which QoS traffic handling technique retains excess packets in a queue and reschedules these packets for later transmission when the configured maximum bandwidth has been surpassed?

- A. weighted random early detection
- B. traffic policing
- **C. traffic shaping**
- D. traffic prioritization

Correct Answer: C

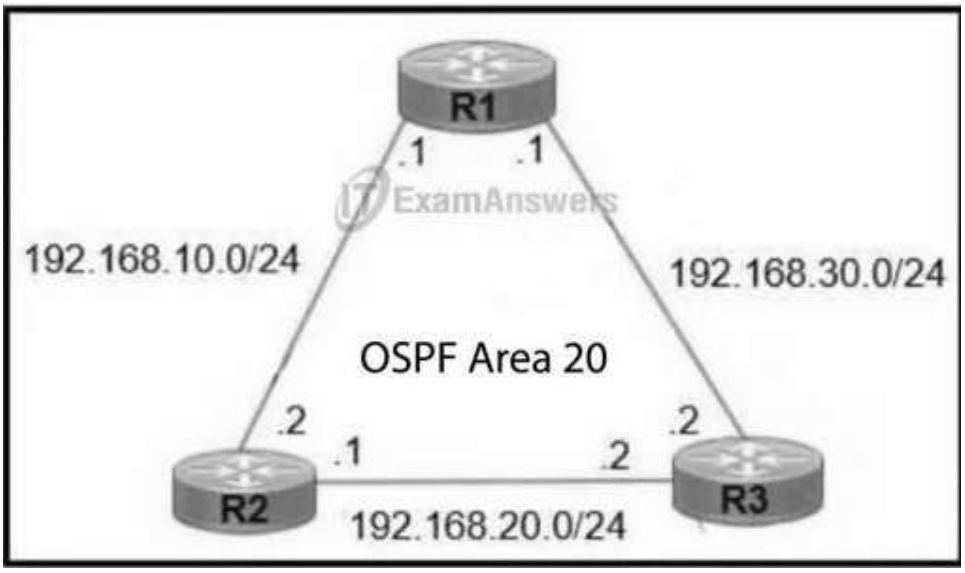
609. What is the function of the controller in a software-defined network?

- A. multicast replication at the hardware level
- B. fragmenting and reassembling packets
- **C. making routing decisions**
- D. forwarding packets

Correct Answer: C

610. Refer to the exhibit. R1 learns all routes via OSPF Which command configures a backup static route on R1 to reach the

192.168.20.0/24 network via R3?



- A. R1(config)#ip route 192.168.20.0 255.255.0.0 192.168.30.2
- B. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 90
- C. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2 111
- D. R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.30.2

Correct Answer: C

611. Which wireless security protocol relies on Perfect Forward Secrecy?

- A. WPA3
- B. WPA
- C. WEP
- D. WPA2

Correct Answer: A

612. Refer to the exhibit. Router R1 resides in OSPF Area 0. After updating the R1 configuration to influence the paths that it will use to direct traffic, an engineer verified that each of the four Gigabit interfaces has the same route to 10.10.0.0/16. Which

interface will R1 choose to send traffic to reach the route?

- A. GigabitEthernet0/0
- B. GigabltEthornet0/1
- C. GigabitEthernet0/2
- D. GigabitEthernet0/3

Correct Answer: C

613. Which two spanning-tree states are bypassed on an interface running PortFast? (Choose two.)

- A. disabled
- B. listening
- C. forwarding
- D. learning
- E. blocking

Correct Answer: B,D

614. Which Layer 2 switch function encapsulates packets for different VLANs so that the packets traverse the same port and maintain traffic separation between the VLANs?

- A. VLAN numbering
- B. VLAN DSCP
- C. VLAN tagging
- D. VLAN marking

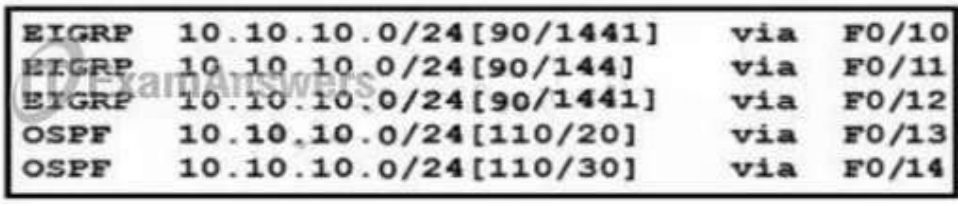
Correct Answer: C

615. What is an expected outcome when network management automation is deployed?

- A. A distributed management plane must be used.
- B. Software upgrades are performed from a central controller
- C. Complexity increases when new device configurations are added
- D. Custom applications are needed to configure network devices

Correct Answer: B

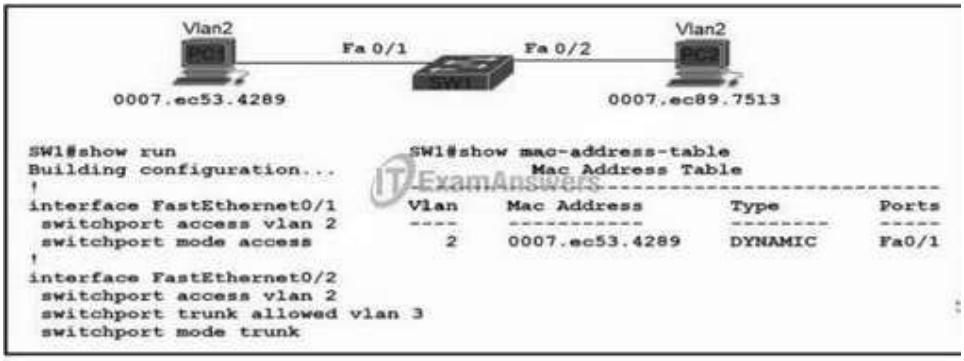
616. Refer to the exhibit. Packets received by the router from BGP enter via a serial interface at 209.165.201.10. Each route is present within the routing table. Which interface is used to forward traffic with a destination IP of 10.10.10.24?



- A. F0/10
- B. F0/11
- C. F0/12
- D. F0/13

Correct Answer: B

617. Refer to the exhibit. An engineer has started to configure replacement switch SW1. To verify part of the configuration, the engineer issued the commands as shown and noticed that the entry for PC2 is missing. Which change must be applied to SW1 so that PC1 and PC2 communicate normally?



A.

SW1(config)#interface fa0/2
SW1(config-if)#no switchport mode trunk
SW1(config-if)#no switchport trunk allowed vlan 3
SW1(config-if)#switchport mode access

B.

SW1(config)#interface fa0/1
SW1(config-if)#no switchport access vlan 2
SW1(config-if)#switchport trunk native vlan 2
SW1(config-if)#switchport trunk allowed vlan 3

C.

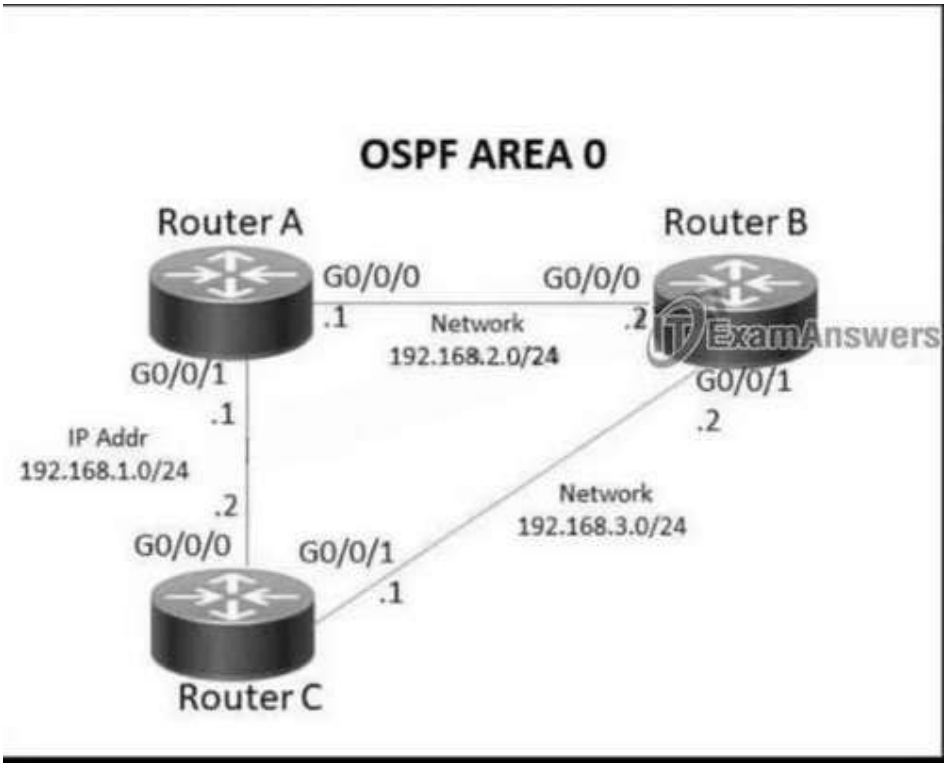
SW1(config)#interface fa0/1
SW1(config-if)#no switchport access vlan 2
SW1(config-if)#switchport access vlan 3
SW1(config-if)#switchport trunk allowed vlan 2

D.

SW1(config)#interface fa0/2
SW1(config-if)#no switchport access vlan 2
SW1(config-if)#no switchport trunk allowed vlan 3
SW1(config-if)#switchport trunk allowed vlan 2

Correct Answer: A

618. Refer to the exhibit. Which action must be taken to ensure that router A is elected as the DR for OSPF area 0?



- A. Configure the OSPF priority on router A with the lowest value between the three routers.
- B. Configure router B and router C as OSPF neighbors of router A.
- C. Configure the router A interfaces with the highest OSPF priority value within the area.
- D. Configure router A with a fixed OSPF router ID

Correct Answer: C

619. An engineer is installing a new wireless printer with a static IP address on the Wi-Fi network. Which feature must be enabled and configured to prevent connection issues with the printer?

- A. passive client
- B. client exclusion
- C. DHCP address assignment
- D. static IP tunneling

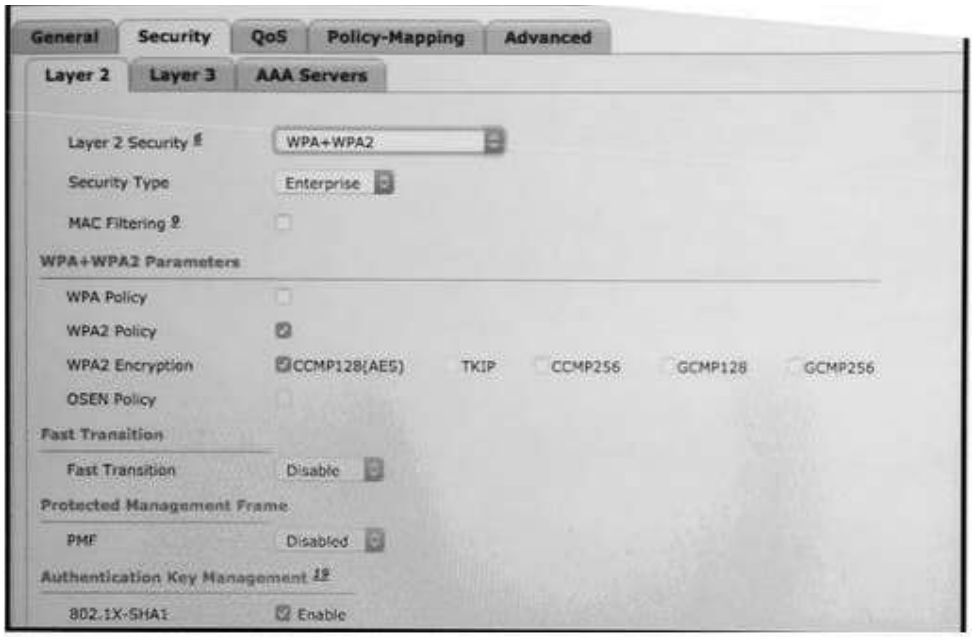
Correct Answer: B

620. An engineer is configuring router R1 with an IPv6 static route for prefix 2019:C15C:0CAF:E001::/64. The next hop must be 2019:C15C:0CAF:E002::1 The route must be reachable via the R1 Gigabit 0/0 interface. Which command configures the designated route?

- A. R1(config)#ipv6 route 2019:C15C:0CAF:E001::/64 2019:C15C:0CAF:E002::1
- B. R1(config-if)#ipv6 route 2019:C15C:0CAF:E001::/64 2019:C15C:0CAF:E002::1
- C. R1(config-if)#ip route 2019:C15C:0CAF:E001::/64 GigabitEthernet0/0
- D. R1(config)#ip route 2019:C15C:0CAF:E001::/64 GigabitEthernet0/0

Correct Answer: A

621. Refer to the exhibit. What must be configured to enable 802.11w on the WLAN?



- A. Set PMF to Required.
- B. Enable MAC Filtering.
- C. Enable WPA Policy.
- D. Set Fast Transition to Enabled

Correct Answer: A

622.Which QoS queuing method discards or marks packets that exceed the desired bit rate of traffic flow?

- A. shaping
- B. policing
- C. CBWFQ
- D. LLQ

Correct Answer: B

623. What is the role of disaggregation in controller-based networking?

- A. It divides the control-plane and data-plane functions.
- B. It summarizes the routes between the core and distribution layers of the network topology.
- C. It enables a network topology to quickly adjust from a ring network to a star network
- D. It streamlines traffic handling by assigning individual devices to perform either Layer 2 or Layer 3 functions.

Correct Answer: A

624. Refer to the exhibit. All traffic enters the CPE router from interface Serial0/3 with an IP address of 192.168.50.1. Web traffic from the WAN is destined for a LAN network where servers are load balanced. An IP packet with a destination address of the HTTP virtual IP of 192.168.1.250 must be forwarded. Which routing table entry does the router use?

```
CPE# show ip route
     192.168.1.0/24 is variably subnetted, 3 subnets, 3 masks
B    192.168.1.0/24 [20/1] via 192.168.12.2, 00:00:06
R    192.168.1.128/25 [120/5] via 192.168.13.3, 00:02:35, Ethernet0/1
O    192.168.1.192/26 [110/11] via 192.168.14.4, 00:02:23, Ethernet0/2
D    192.168.1.224/27 [90/1024640] via 192.168.15.5, 00:01:40, Ethernet0/3
```

- A. 192.168.1.0/24 via 192.168.12.2
- B. 192.168.1.128/25 via 192.168.13.3
- C. 192.168.1.192/26 via 192.168.14.4
- D. 192.168.1.224/27 via 192.168.15.5

Correct Answer: B

625. What is a zero-day exploit?

- A. It is when a new network vulnerability is discovered before a fix is available
- B. It is when the perpetrator inserts itself in a conversation between two parties and captures or alters data.
- C. It is when the network is saturated with malicious traffic that overloads resources and bandwidth
- D. It is when an attacker inserts malicious code into a SQL server.

Correct Answer: A

626. A network engineer is replacing the switches that belong to a managed-services client with new Cisco Catalyst switches. The new switches will be configured for updated security standards, including replacing Telnet services with encrypted connections and doubling the modulus size from 1024. Which two commands must the engineer configure on the new switches? (Choose two.)

- A. crypto key generate rsa general-keys modulus 1024
- B. transport input all
- C. crypto key generate rsa usage-keys
- D. crypto key generate rsa modulus 2048
- E. transport Input ssh

Correct Answer: A,E

627. An engineer has configured the domain name, user name, and password on the local router. What is the next step to complete the configuration tor a Secure Shell access RSA key?

- A. crypto key Import rsa pem
- B. crypto key pubkey-chain rsa
- C. crypto key generate rsa
- D. crypto key zeroize rsa

Correct Answer: C

628. Refer to the exhibit. What is the next hop for traffic entering R1 with a destination of 10.1.2.126?

```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set
      10.0.0.0/24 is subnetted, 5 subnets
D     10.1.2.0/24 [90/2170112] via 10.165.20.226, 00:01:30, Serial0/0
D     10.1.3.0/24 [90/2170112] via 10.165.20.226, 00:01:30, Serial0/0
D     10.1.2.0/25 [90/2170112] via 10.165.20.126, 00:01:30, Serial0/0
D     10.1.3.0/25 [90/2170112] via 10.165.20.146, 00:01:30, Serial0/0
D     10.1.4.0/25 [90/2170112] via 10.165.20.156, 00:01:30, Serial0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.18.10.0/24 is directly connected, GigabitEthernet0/0
      192.168.21.0/24 is variably subnetted, 2 subnets, 2 masks
C     192.168.11.0/24 is directly connected, GigabitEthernet0/1
     10.165.20.0/24 is variably subnetted, 2 subnets, 2 masks
C    10.165.20.224/24 is directly connected, Serial0/0
S     10.1.2.112/28 [1/0] via 10.165.20.166
```

- A. 10.165 20.126
- B. 10.165.20.146
- C. 10.165.20.166
- D. 10.165 20.226

Correct Answer: D

629. After a recent security breach and a RADIUS failure, an engineer must secure the console port of each enterprise router with a local username and password. Which configuration must the engineer apply to accomplish this task?

A.

```
aaa new-model line
con 0
password plaintextpassword
privilege level 15
```

B.

```
username localuser secret plaintextpassword
line con 0
login authentication default
privilege level 15
```

C.

```
username localuser secret plaintextpassword
line con 0
```

```
no login local
privilege level 15
```

D.

```
aaa new-model
aaa authorization exec default local aaa
authentication login default radius
username localuser privilege 15 secret plaintextpassword
```

Correct Answer: B

630. An engineer is configuring SSH version 2 exclusively on the R1 router. What is the minimum configuration required to permit remote management using the cryptographic protocol?

A.

```
hostname R1
ip domain name cisco
crypto key generate rsa general-keys modulus 1024
username cisco privilege 15 password 0 cisco123 ip
ssh version 2
line vty 0 15
transport input ssh
login local
```

B.

```
hostname R1
crypto key generate rsa general-keys modulus 1024
username cisco privilege 15 password 0 cisco123 ip
ssh version 2
line vty 0 15
transport input all
login local
```

C.

```
hostname R1
service password-encryption
crypto key generate rsa general-keys modulus 1024
username cisco privilege 15 password 0  cisco123
ip ssh version 2
line vty 0 15
transport input ssh
login local
```

D.
hostname R1
ip domain name cisco
crypto key generate rsa general-keys modulus 1024
username cisco privilege 15 password 0 cisco123 ip
ssh version 2
line vty 0 15
transport input all
login local

Correct Answer: C

631. Why would VRRP be implemented when configuring a new subnet in a multivendor environment?

- A. when a gateway protocol is required that support more than two Cisco devices for redundancy
- B. to enable normal operations to continue after a member failure without requiring a change In a host ARP cache
- C. to ensure that the spanning-tree forwarding path to the gateway is loop-free
- D. to interoperate normally with all vendors and provide additional security features for Cisco devices

Correct Answer: A

632. What provides centralized control of authentication and roaming In an enterprise network?

- A. a lightweight access point
- B. a firewall
- C. a wireless LAN controller
- D. a LAN switch

Correct Answer: C

633. Refer to the exhibit. The given Windows PC is requesting the IP address of the host at www.cisco.com. To which IP address is the

request sent?

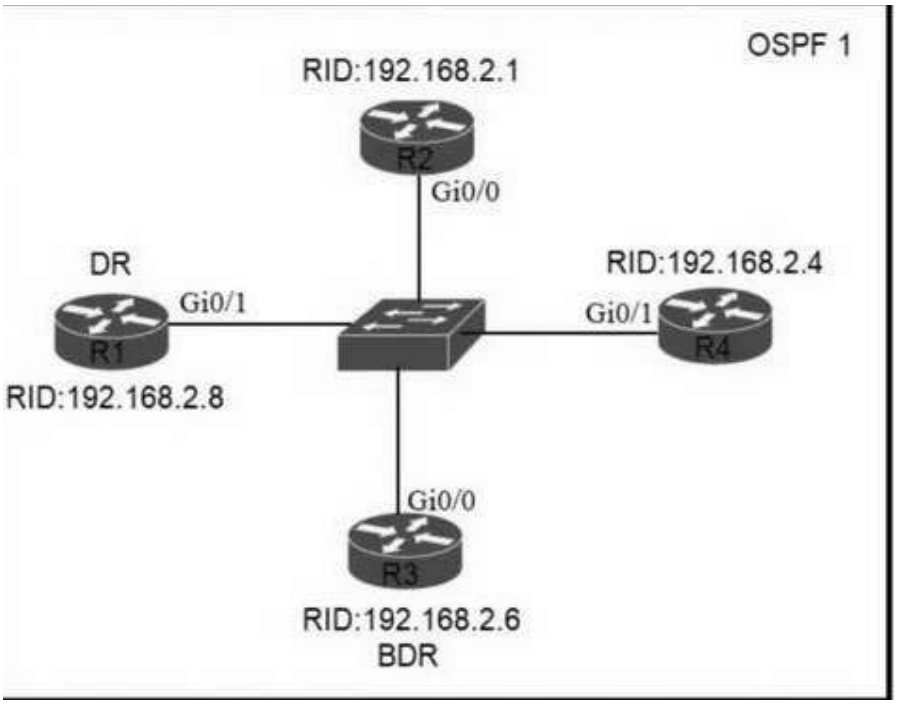
```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family
Controller
   Physical Address. . . . . . . . . : 3C-52-82-33-F3-8F
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi:
   Connection-specific DNS Suffix  : arcep.se
   Description . . . . . . . . . . . : Intel(R) Dual Band
Wireless-AC 7265
   Physical Address. . . . . . . . . : C8-21-58-B4-F3-EF
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::45a1:b3fa:2f37:bf37%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.226(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : October 3, 2019 12:28:08 PM
   Lease Expires . . . . . . . . . . : October 3, 2019 7:18:37 PM
   Default Gateway . . . . . . . . . : 192.168.1.100
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DHCPv6 IAID . . . . . . . . . . . : 46670168
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-FF-05-55-3C-52-82-33-D3-84
   DNS Servers . . . . . . . . . . . : 192.168.1.253
   NetBIOS over Tcpip. . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       arcep.se
```

- A. 192.168.1.226
- B. 192.168.1.100
- C. 192.168.1.254
- D. 192.168.1.253

Correct Answer: D

634. Refer to the exhibit. All routers in the network are configured. R2 must be the DR. After the engineer connected the devices, R1 was elected as the DR. Which command sequence must be

configured on R2 to be elected as the DR in the network?



A.
R2(config)#router ospf 1
R2(config-router)#router-id 10.100.100.100

B.
R2(config)#router ospf 1
R2(config-router)#router-id 192.168.2.7

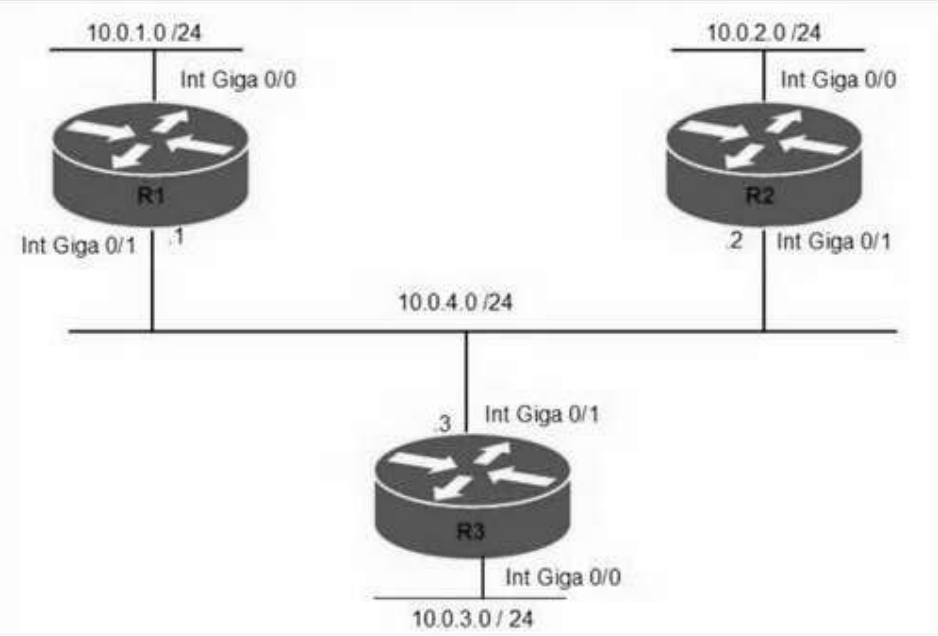
C.
R2(config)#interface gi0/0
R2(config-if)#ip ospf priority 100

D.
R2(config)#interface gi0/0
R2(config-if)#ip ospf priority 1

Correct Answer: C

635. Refer to the exhibit. Router R1 must be configured to reach the 10.0.3.0/24 network from the 10.0.1.0/24 segment. Which command must

be used to configure the route?



- A. route add 10.0.3.0 mask 255.255.255.0 10.0.4.3
- B. route add 10.0.3.0 0.255.255.255 10.0.4.2
- C. ip route 10.0.3.0 255.255.255.0 10.0.4.3
- D. ip route 10.0.3.0 0.255.255.255 10.0.4.2

Correct Answer: C

636. What is the collapsed layer in collapsed core architectures?

- A. core and distribution
- B. distribution and access
- C. core and WAN
- D. access and WAN

Correct Answer: A

637. What is the purpose of the Cisco DNA Center controller?

- A. to securely manage and deploy network devices
- B. to provide Layer 3 services to autonomous access points
- C. to secure physical access to a data center
- D. to scan a network and generate a Layer 2 network diagram

Correct Answer: A

638. How does authentication differ from authorization?

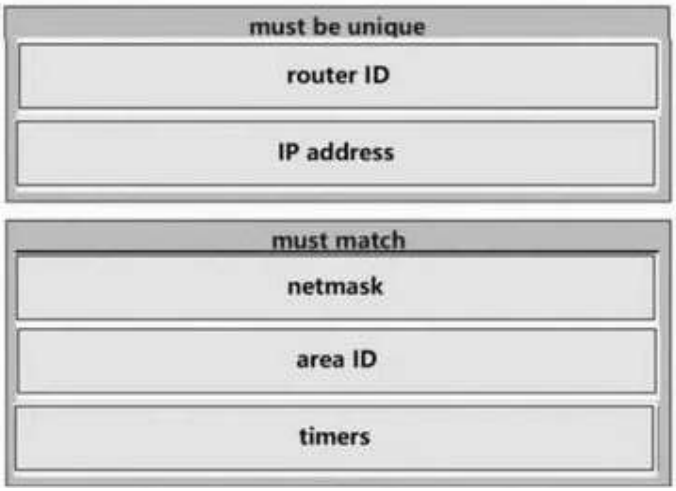
- A. Authentication is used to verify a person's identity, and authorization is used to create syslog messages for logins.
- B. Authentication is used to determine what resources a user is allowed to access, and authorization is used to track what equipment is allowed access to the network.
- C. Authentication verifies the identity of a person accessing a network, and authorization determines what resource a user can access.
- D. Authentication is used to record what resource a user accesses, and authorization is used to determine what resources a user can access.

Correct Answer: C

Drag & Drop Questions

1. A network engineer is configuring an OSPFv2 neighbor adjacency. Drag and drop the parameters from the left onto their required categories on the right. No all parameters are used.

Correct Answer:



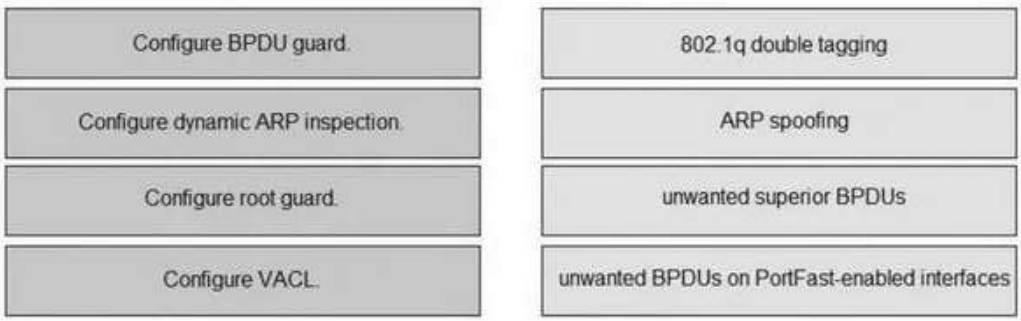
Must be unique:
- router ID
- IP address

Must match:
- netmask
- area ID
- timers

Section: IP Connectivity

2. Drag and drop the threat-mitigation techniques from the left onto the types of threat or attack they mitigate on the right.

Select and Place:



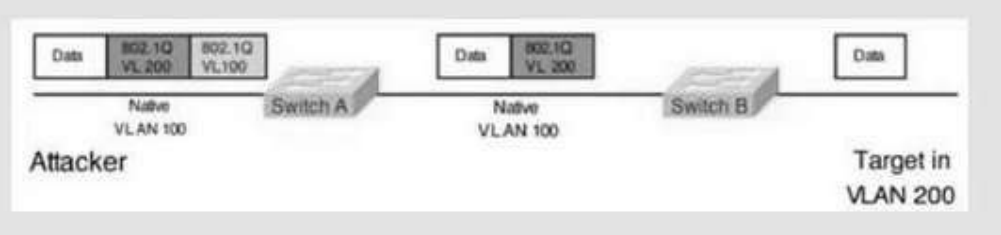
Correct Answer:

Configure BPDU guard.	Configure VACL.
Configure dynamic ARP inspection.	Configure dynamic ARP inspection.
Configure root guard.	Configure root guard.
Configure VACL.	Configure BPDU guard.

Section: Security Fundamentals

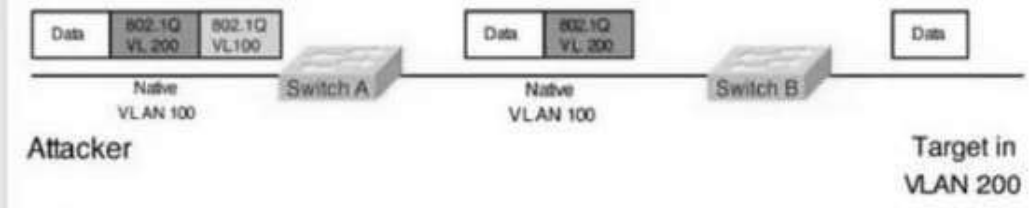
Configure VACL. -> 802.1q double tagging Configure dynamic ARP inspection. -> ARP spoofing Configure root guard. -> unwanted superior BPDUs
Configure BPDU guard. -> unwanted BPDUs on PortFast-enabled interfaces

Explanation/Reference:
Double-Tagging attack:



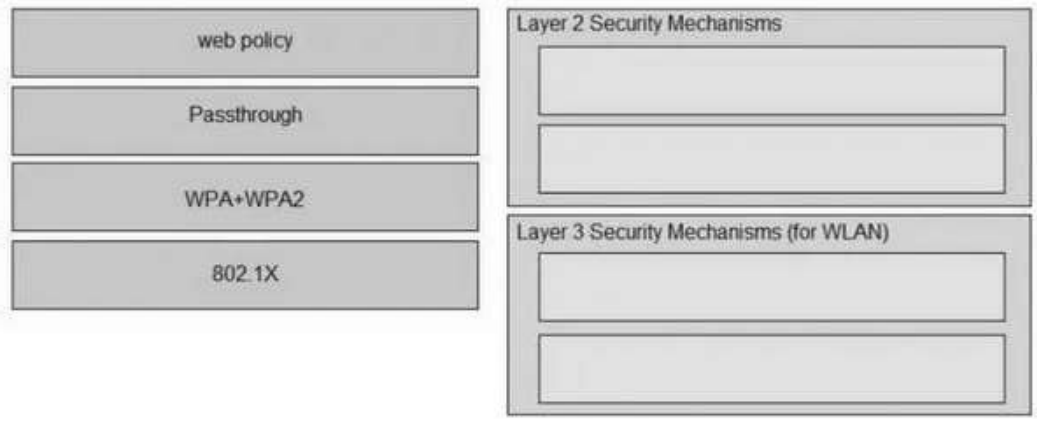
In this attack, the attacking computer generates frames with two 802.1Q tags. The first tag matches the native VLAN of the trunk port (VLAN 10 in this case), and the second matches the VLAN of a host it wants to attack (VLAN 20).
When the packet from the attacker reaches Switch A, Switch A only sees the first VLAN 10 and it matches with its native VLAN 10 so this VLAN tag is removed. Switch A forwards the frame out all links with the same native VLAN 10. Switch B receives the frame with an tag of VLAN 20 so it removes this tag and forwards out to the Victim computer.
Note: This attack only works if the trunk (between two switches) has the same native VLAN as the attacker.
To mitigate this type of attack, you can use VLAN access control lists (VACLs, which applies to all traffic within a VLAN. We can use VACL to drop attacker traffic to specific victims/servers) or implement Private VLANs.
ARP attack (like ARP poisoning/spoofing) is a type of attack in which a malicious actor sends falsified ARP messages over a local area

network as ARP allows a gratuitous reply from a host even if an ARP request was not received. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. This is an attack based on ARP which is at Layer 2.
Dynamic ARP inspection (DAI) is a security feature that validates ARP packets in a network which can be used to mitigate this type of attack.

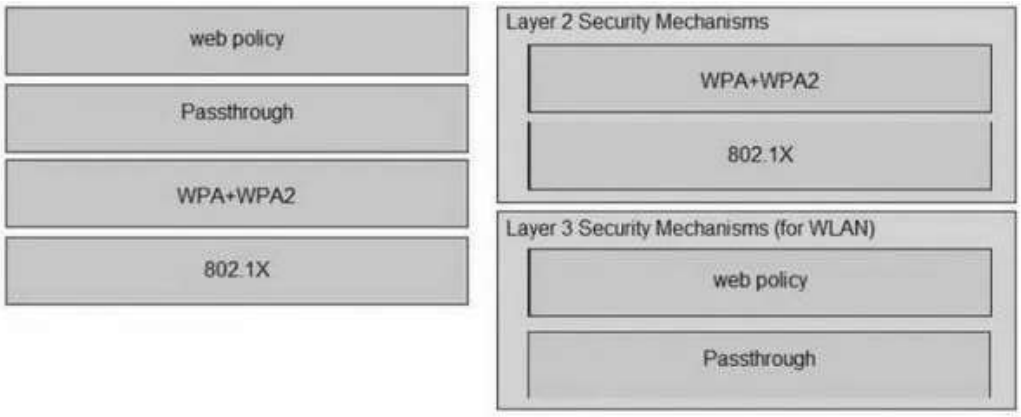


3. Drag and drop the Cisco Wireless LAN Controller security settings from the left onto the correct security mechanism categories on the right

Select and Place:



Correct Answer:



Layer 2 Security Mechanisms:
- WPA+WPA2
- 802.1X

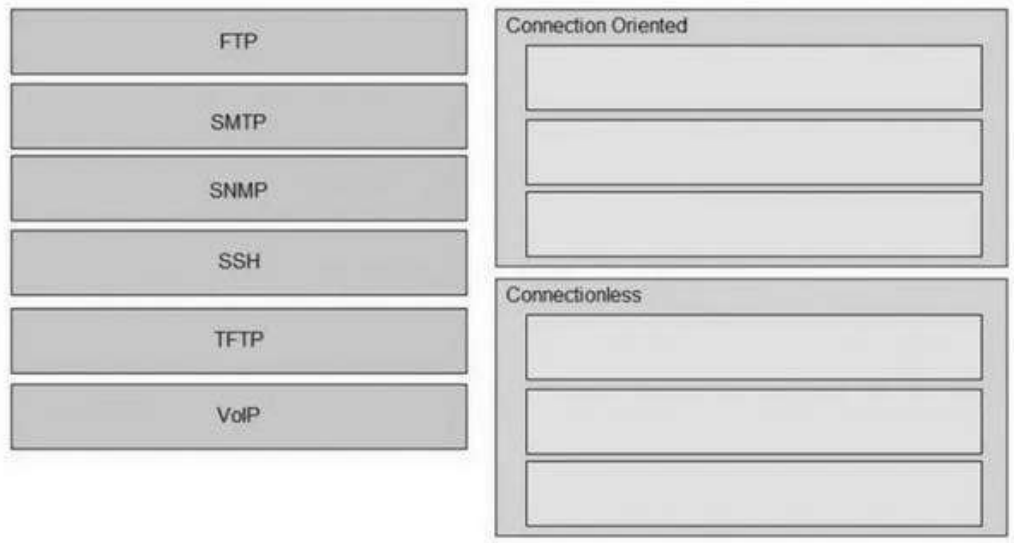
Layer 3 Security Mechanisms (for WLAN):
- web policy
- Passthrough

Section: Security Fundamentals

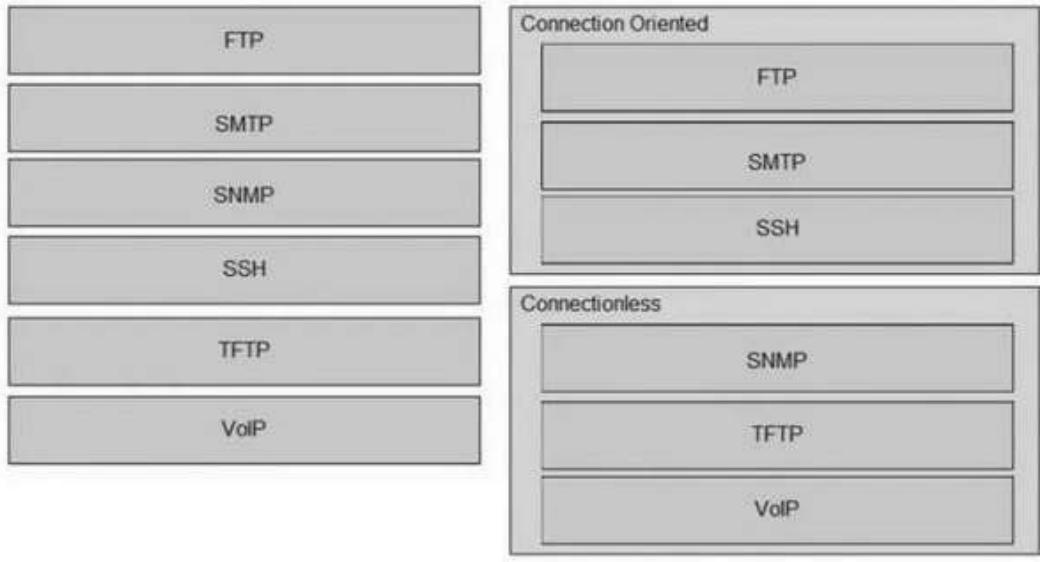
Explanation/Reference: Layer 2 Security Mechanism includes WPA+WPA2, 802.1X, Static WEP, CKIP while Layer 3 Security Mechanisms (for WLAN) includes IPSec, VPN Pass-Through, Web Passthrough …
Reference: Click here

4. Drag and drop the network protocols from the left onto the correct transport services on the right.

Select and Place:



Correct Answer:



Connection Oriented:
- FTP
- SMTP
- SSH

Connectionless:
- SNMP
- VoIP
- TFTP

Section: IP Services

Explanation/Reference: SSH uses TCP port 22 while SNMP uses UDP port 161 and 162.

5. Refer to the exhibit.

```
[root#HostTime =]# ip route
default via 192.168.1.193 dev eth1 proto static
192.168.1.0/26 dev sth1 proto kernel scope link src 192.168.1.200 metric 1

[root#HostTime =]# ip addr show eth1
eth1:mtu 1500 qdisc pfifo_fast qlan 1000
   link/ether 00:0C:22:83:79:A3 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.200/26 hrd 192.168.1.255 scope global eth1
   inet6 fe80::20c::29ff:fe89:79b3/64 scope link
   valid_lft forever preferred_lft forever
```

Drag and drop the networking parameters from the left onto the correct values on the right.

Select and Place:

default gateway	00:0C:22
host IP address	00:0C:22:83:79:A3
NIC MAC address	192.168.1.193
NIC vendor OUI	192.168.1.200
subnet mask	255.255.255.192

Correct Answer:

default gateway	NIC vendor OUI
host IP address	NIC MAC address
NIC MAC address	default gateway
NIC vendor OUI	host IP address
subnet mask	subnet mask

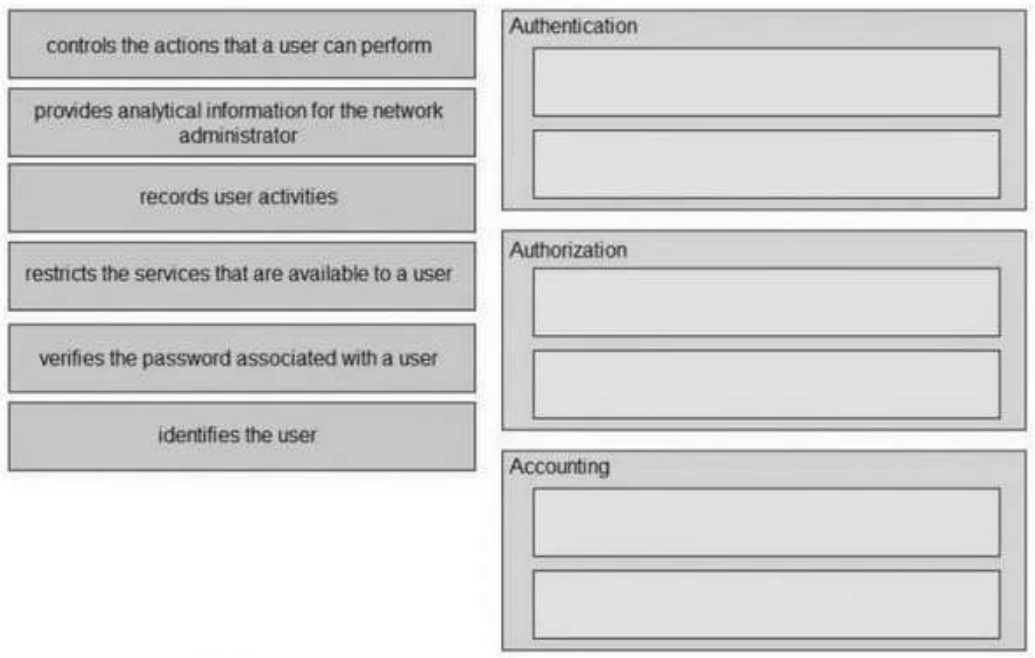
NIC vendor OUI -> 00:0C:22
NIC MAC address -> 00:0C:22:83:79:A3
default gateway -> 192.168.1.193 host
IP address -> 192.168.1.200 subnet
mask -> 255.255.255.192

Section: Network Fundamentals

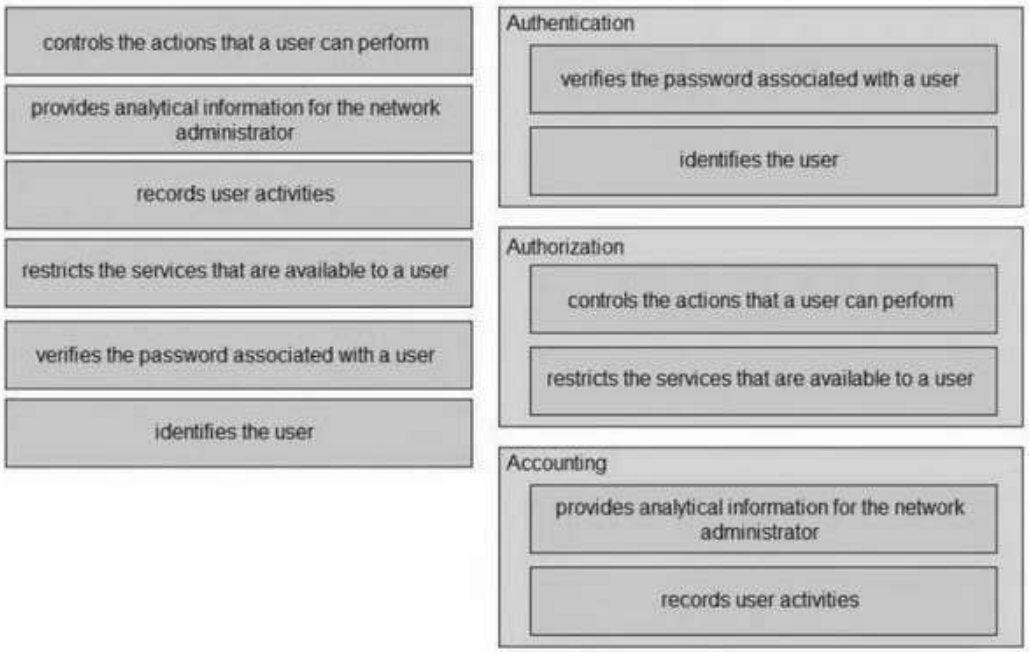
Explanation/Reference: The "ip route" and "ip addr show eth1" are Linux commands.
+ "ip route": display the routing table
+ "ip addr show eth1": get depth information (only on eth1 interface) about your network interfaces like IP Address, MAC Address information

6. Drag and drop the AAA functions from the left onto the correct AAA services on the right.

Select and Place:



Correct Answer:



Authentication:
- verifies the password associated with a user
- identifies the user

Authorization:
- controls the actions that a user can perform
- restricts the services that are available to a user

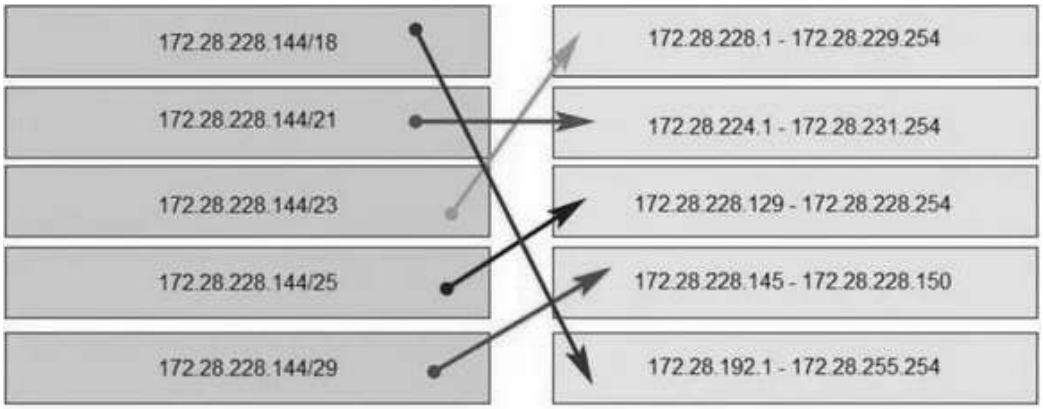
Accounting:
- provides analytical Information for the network administrator
- records user activities

Section: Security Fundamentals

7. Drag and drop the IPv4 network subnets from the left onto the correct usable host ranges on the right.

Select and Place:

Correct Answer:



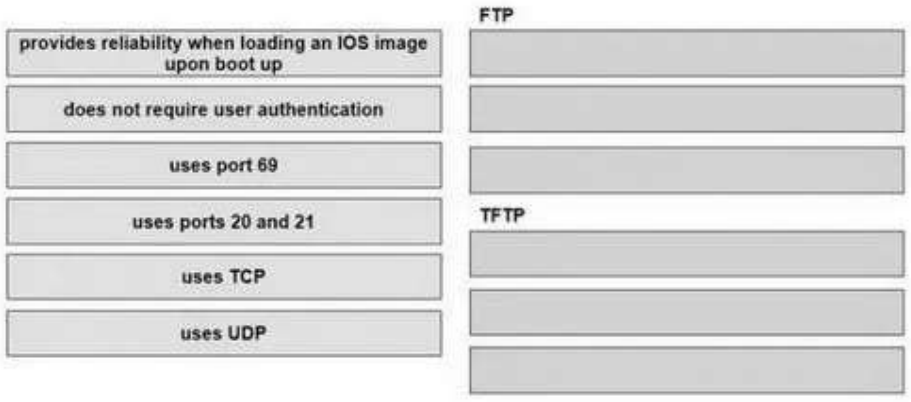
172.28.228.144/21 -> 172.28.224.1 - 172.28.231.254
172.28.228.144/29 -> 172.28.228.145 - 172.28.228.150
172.28.228.144/23 -> 172.28.228.1 - 172.28.229.254
172.28.228.144/25 -> 172.28.228.129 - 172.28.228.254
172.28.228.144/18 -> 172.28.192.1 - 172.28.255.254

Explanation/Reference: This subnet question requires us to grasp how to subnet very well. To quickly find out the subnet range, we have to find out the increment and the network address of each subnet. Let's take an example with the subnet 172.28.228.144/18:
From the /18 (= 1100 0000 in the 3rd octet), we find out the increment is 64. Therefore the network address of this subnet must be the greatest multiple of the increment but not greater than the value in the 3rd octet (228). We can find out the 3rd octet of the network address is 192 (because 192 = 64 * 3 and 192 < 228) -> The network address is 172.28.192.0. So the first usable host should be 172.28.192.1 and it matches with the 5th answer on the right. In this case we don't need to calculate the broadcast address because we found the correct answer.

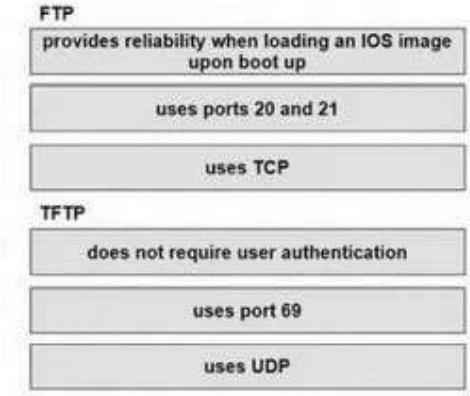
Let’s take another example with subnet 172.28.228.144/23 -> The increment is 2 (as /23 = 1111 1110 in 3rd octet) -> The 3rd octet of the network address is 228 (because 228 is the multiply of 2 and equal to the 3rd octet) -> The network address is 172.28.228.0 -> The first usable host is 172.28.228.1. It is not necessary but if we want to find out the broadcast address of this subnet, we can find out the next network address, which is 172.28.(228 + the increment number).0 or 172.28.230.0 then reduce 1 bit -> 172.28.229.255 is the broadcast address of our subnet.
Therefore the last usable host is 172.28.229.254.

8. Drag and drop the descriptions of file transfer protocols from the left onto the correct protocols on the right.

Select and Place:



Correct Answer:



FTP:
- provides reliability when loading an IOS image upon boot up

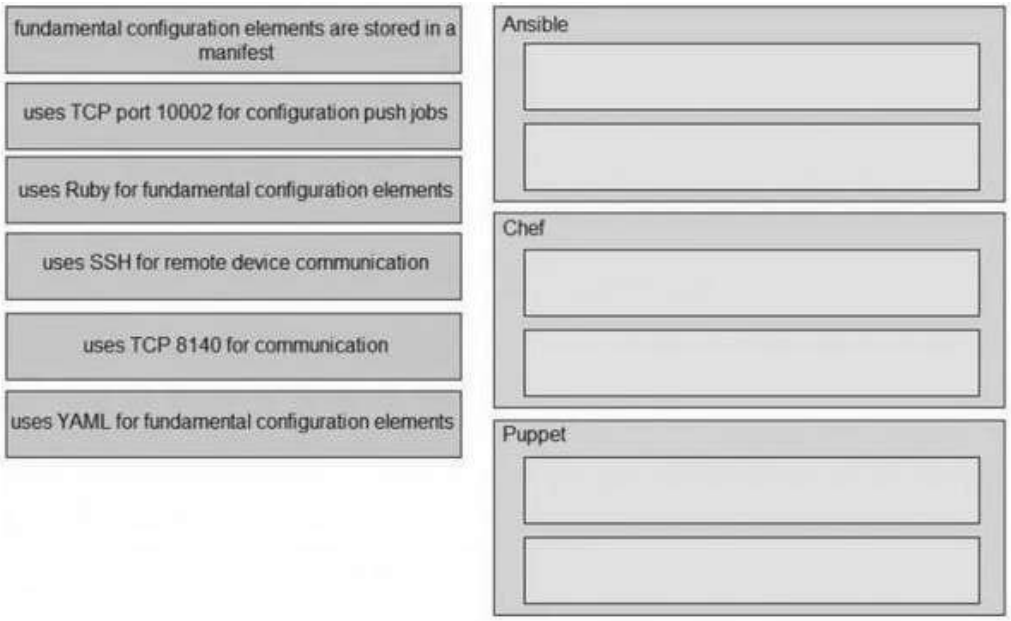
- uses ports 20 and 21
- uses TCP

TFTP:
- does not require user authentication
- uses port 69
- uses UDP

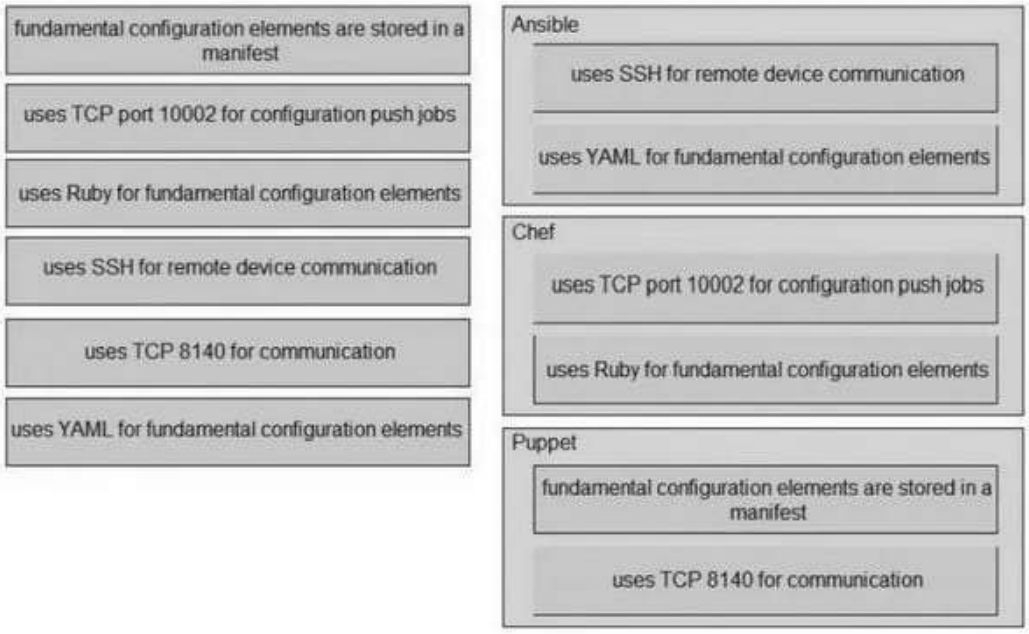
Section: Network Fundamentals

9. Drag drop the descriptions from the left on to the correct configuration-management technologies on the right.

Select and Place:



Correct Answer:



Ansible:
- uses SSH for remote device communication
- uses YAML for fundamental configuration elements

Chef:
- uses TCP port 10002 for configuration push jobs
- uses Ruby for fundamental configuration elements

Puppet:
- fundamental configuration elements are stored in a manifest
- uses TCP 8140 for communication

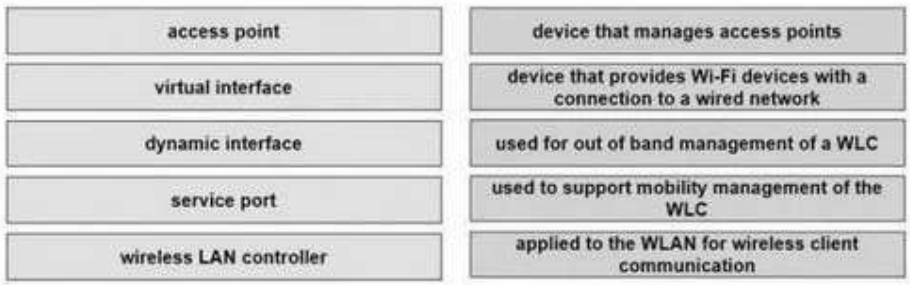
Section: Automation and Programmability

Explanation/Reference: The focus of Ansible is to be streamlined and fast, and to require no node agent installation.
Thus, Ansible performs all functions over SSH. Ansible is built on Python, in contrast to the Ruby foundation of Puppet and Chef.
TCP port 10002 is the command port. It may be configured in the Chef Push Jobs configuration file .
This port allows Chef Push Jobs clients to communicate with the Chef Push Jobs server.
Puppet is an open-source configuration management solution, which is built with Ruby and offers custom Domain Specific Language (DSL) and Embedded Ruby (ERB) templates to create custom Puppet language files, offering a declarative-paradigm programming approach.

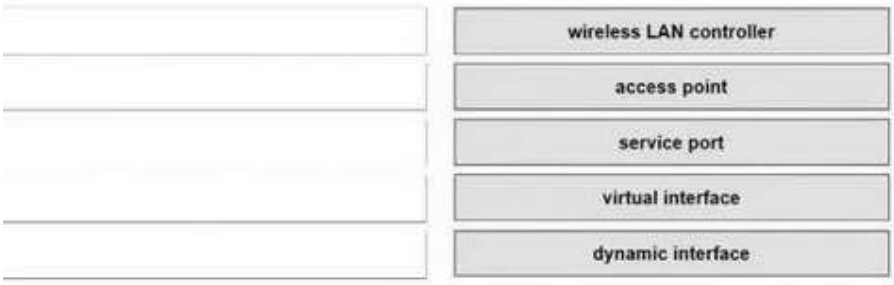
A Puppet piece of code is called a manifest, and is a file with .pp extension.

10. Drag and drop the WLAN components from the left onto the correct descriptions on the right.

Select and Place:



Correct Answer:



Section: Network Access

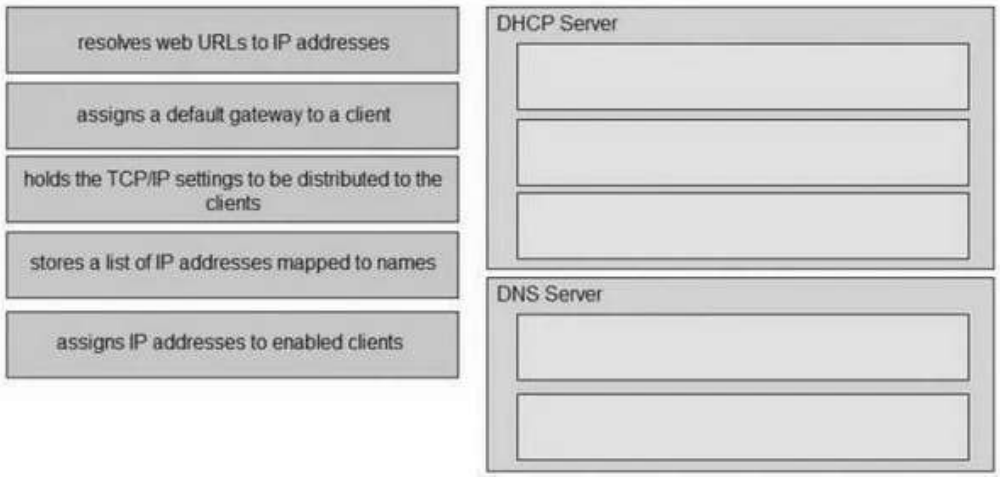
wireless LAN controller -> device that manages access points
access point -> device that provides Wi-Fi devices with a connection to a wired network
service port -> used for out of band management of a WLC
virtual interface -> used to support mobility management of the WLC
dynamic interface -> applied to the WLAN for wireless client communication

Explanation/Reference:
The service port can be used management purposes, primarily for out-of-band management.
However, AP management traffic is not possible across the service port. In most cases, the service port is used as a "last resort" means of accessing the controller GUI for management purposes. For example, in the case where the system distribution ports on the

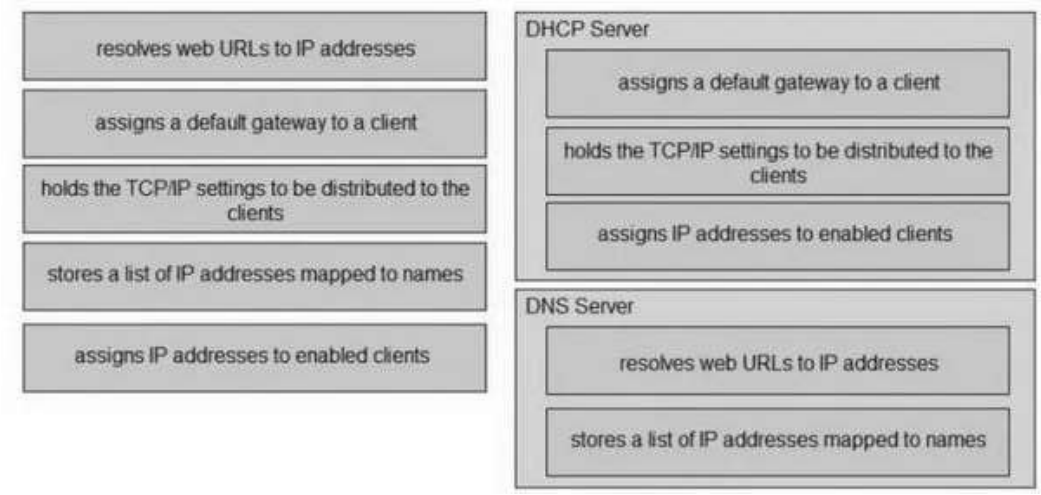
controller are down or their communication to the wired network is otherwise degraded.
A dynamic interface with the Dynamic AP Management option enabled is used as the tunnel source for packets from the controller to the access point and as the destination for CAPWAP packets from the access point to the controller.
The virtual interface is used to support mobility management, Dynamic Host Configuration Protocol (DHCP) relay, and embedded Layer 3 security such as guest web authentication. It also maintains the DNS gateway host name used by Layer 3 security and mobility managers to verify the source of certificates when Layer 3 web authorization is enabled.

11. Drag and drop the functions from the left onto the correct network components on the right.

Select and Place:



Correct Answer:

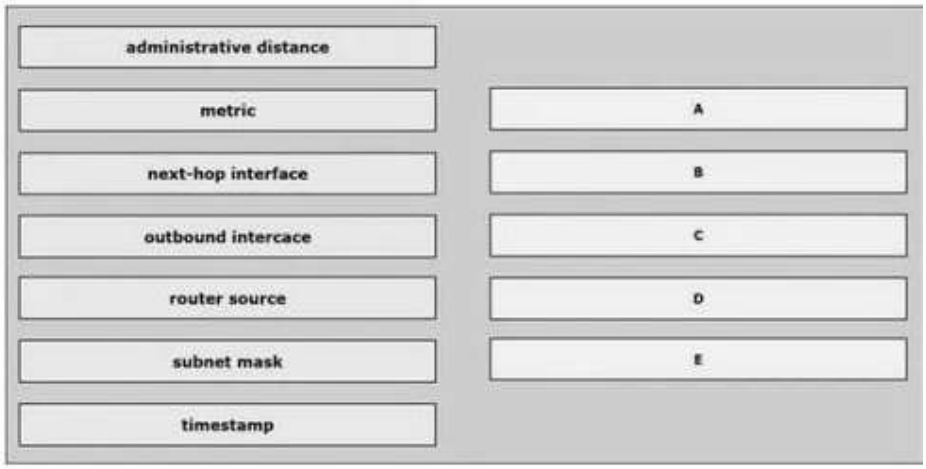


DHCP Server:
- assigns a default gateway to a client
- holds the TCP/IP settings to be distributed to the clients
- assigns IP addresses to enabled clients

DNS Server:
- resolves web URLs to IP addresses
- stores a list of IP addresses mapped to names

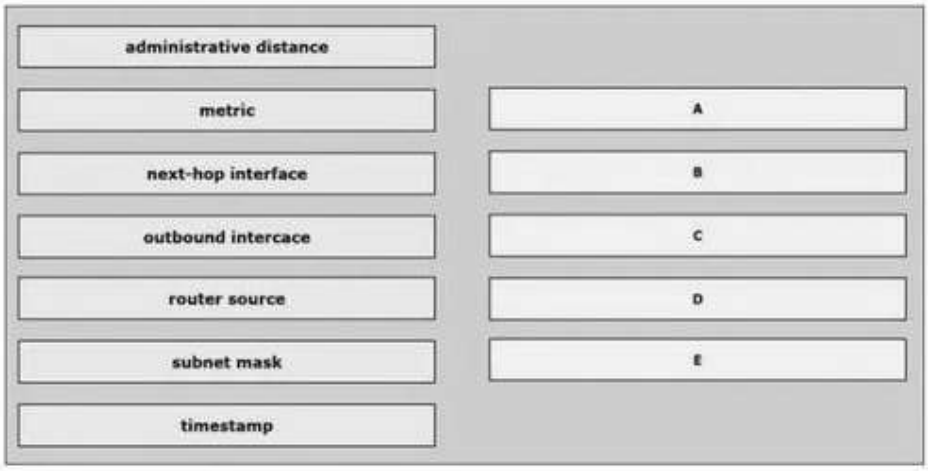
Section: IP Services

12. Refer to the exhibit

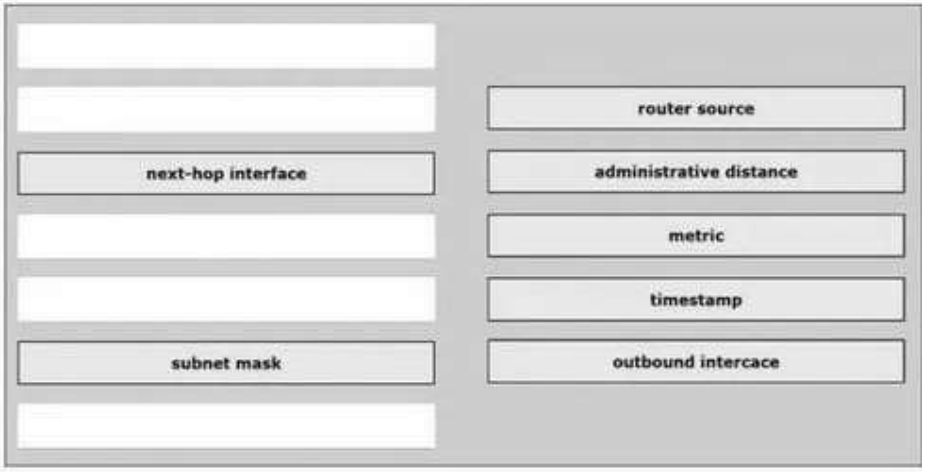


Drag and drop the routing table components on the left onto the corresponding letter from the exhibit on the right not all options are used.

Select and Place:



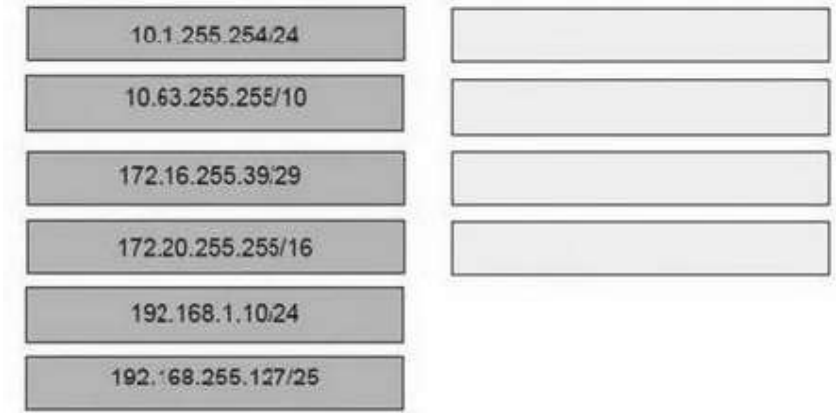
Correct Answer:



A: router source
B: administrative distance
C: metric
D: timestamp
E: outbound intercace

13. Drag and drop each broadcast IP address on the left to the Broadcast Address column on the right Not all options are used.

Select and Place:



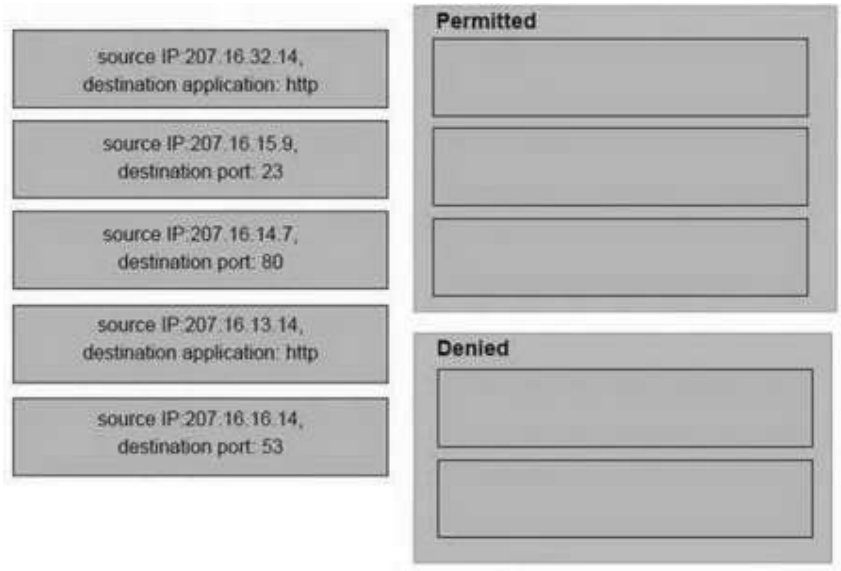
Correct Answer:

14. An interface has been configured with the access list that is shown below.

access-list 107 deny tcp 207.16.12.0.0.0.3.255 any eq http
access-list 107 permit ip any any

On the basis of that access list, drag each information packet on the left to the appropriate category on the right.

Select and Place:



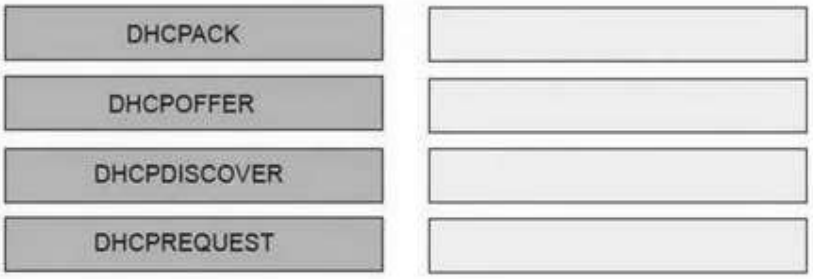
Correct Answer:

Permitted:
- source IP:207.16.32.14, destination application: http
- source IP:207.16.15.9, destination port: 23
- source IP:207.16.16.14, destination port: 53

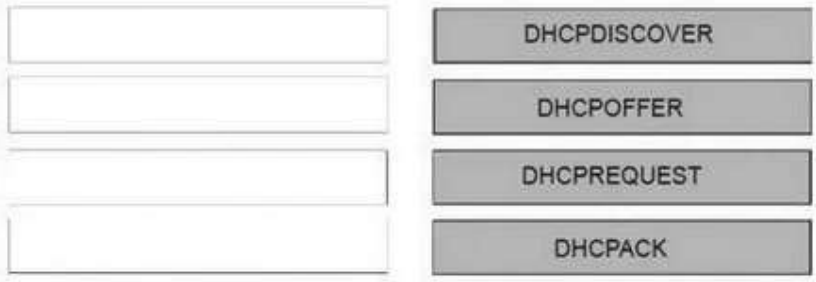
Denied:
- source IP:207.16.14.7, destination port: 80
- source IP:207.16.13.14, destination application: http

15. Order the DHCP message types as they would occur between a DHCP client and a DHCP server.

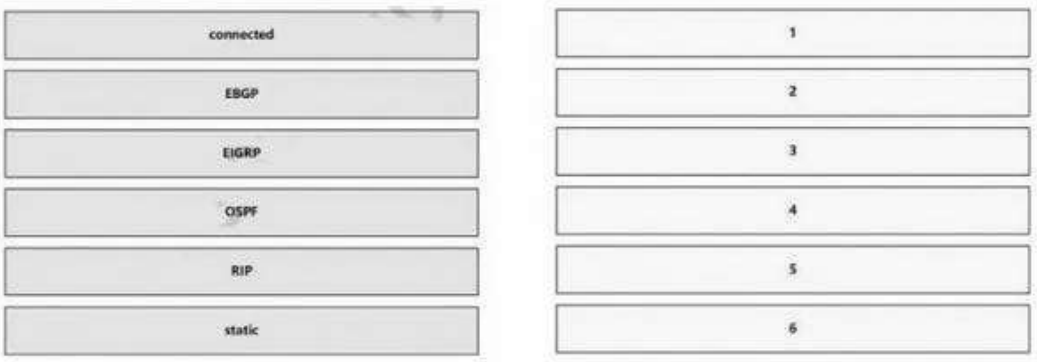
Select and Place:



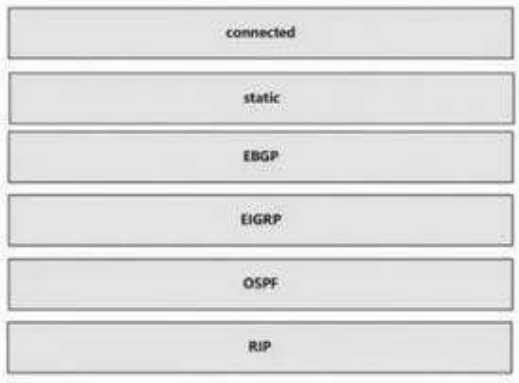
Correct Answer:



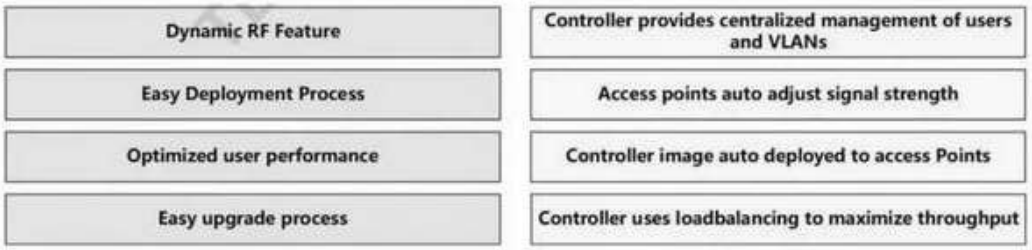
16. Drag each route source from the left to the numbers on the right. Beginning with the lowest and ending with the highest administrative distance.



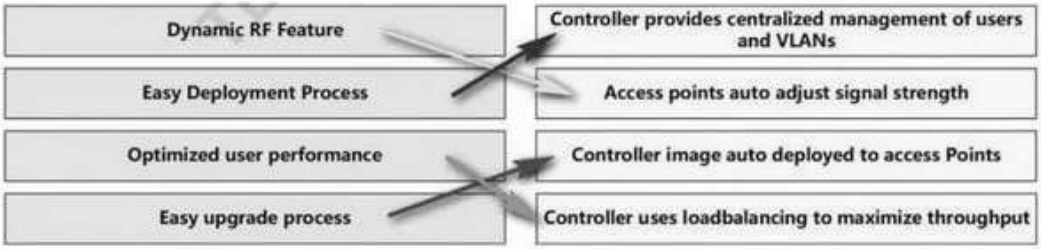
Answer:



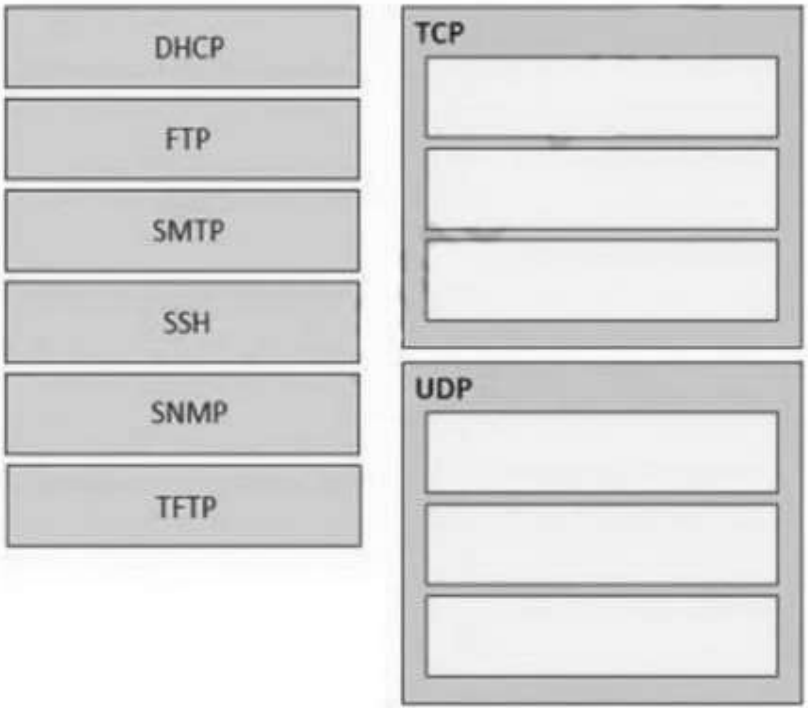
17. Drag and drop the benefits of a cisco wireless Lan controller from the left onto the correct examples on the right.



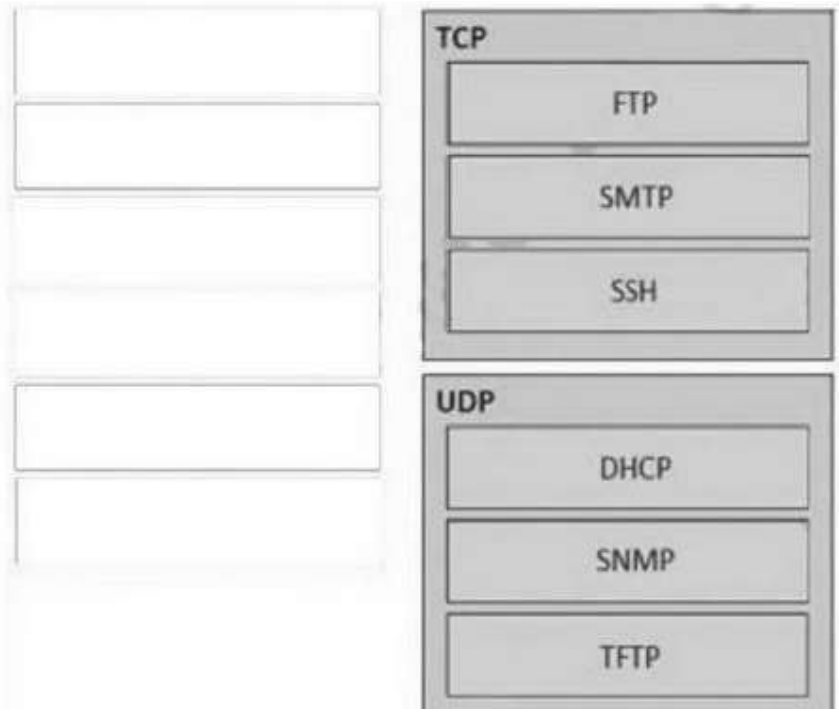
Answer:



18. Drag and drop the application protocols from the left onto the transport protocols that is uses on the right.



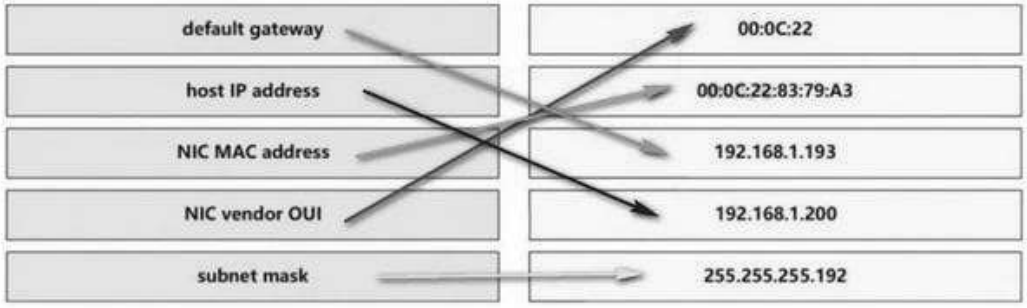
Answer:



19. Refer to the exhibit. Drag and drop the networking parameters from the left on to the correct values on the right.

```
[root#HostTime ~]# ip route
default via 192.168.1.193 dev eth1 proto static
192.168.1.0/26 dev sth1 proto kernel scope link src 192.168.1.200 metric 1

[root#HostTime ~]# ip addr show eth1
eth1:mtu 1500 qdisc pfifo_fast qlan 1000
   link/ether 00:0C:22:83:79:A3 brd ff:ff:ff:ff:ff:ff
   inet 192.168.1.200/26 hrd 192.168.1.255 scope global eth1
   inet6 fe80::20c::29ff:fe89:79b3/64 scope link
   valid_lft forever preferred_lft forever
```

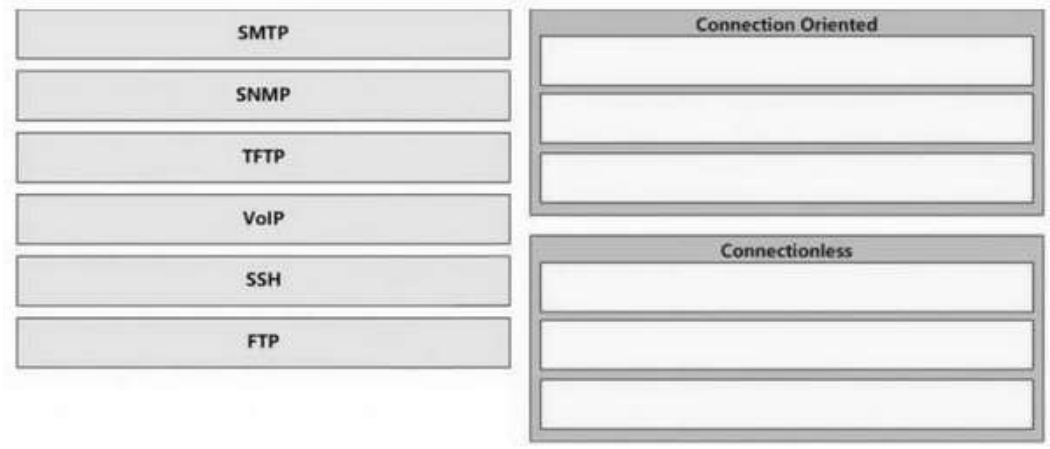
Answer:



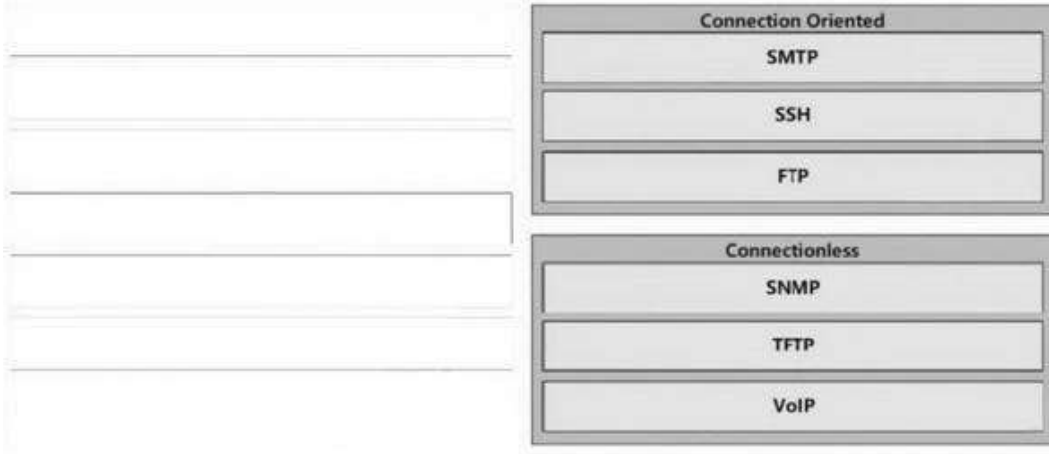
Explanation/Reference: The “ip route” and “ip addr show eth1” are Linux commands.

+ “ip route”: display the routing table
+ “ip addr show eth1”: get depth information (only on eth1 interface) about your network interfaces like IP Address, MAC Address information

20. Drag and drop the networking parameters from the left on to the correct values on the right.

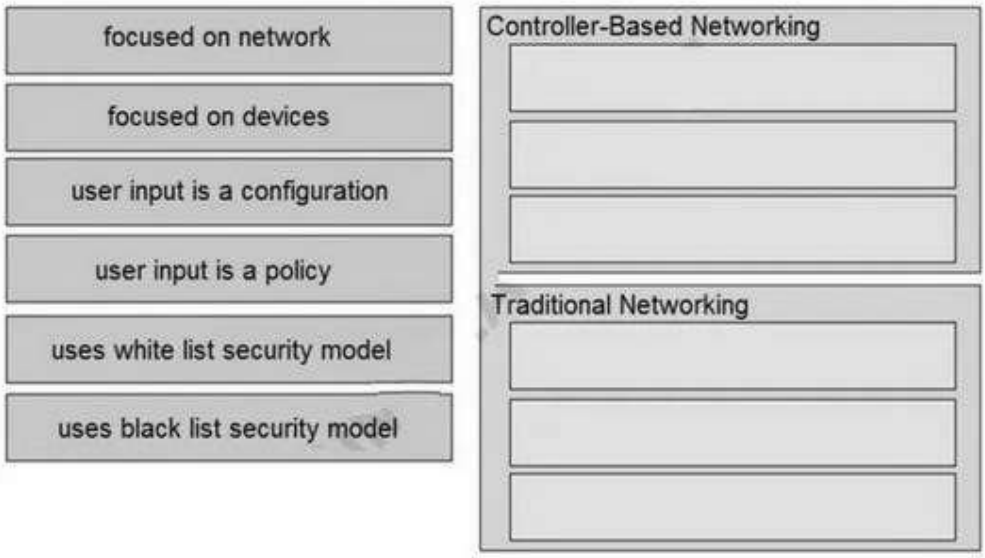


Answer:

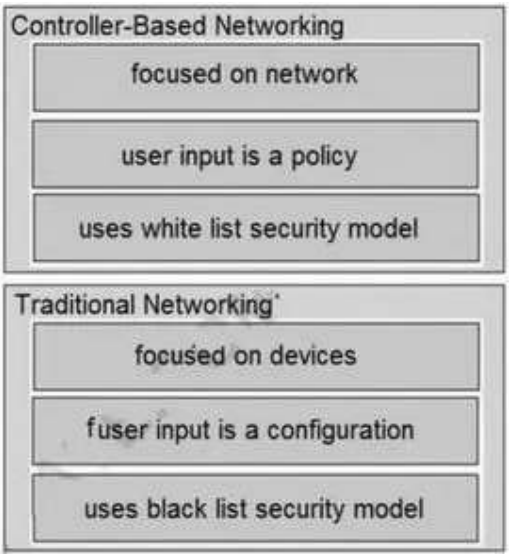


Explanation/Reference: SSH uses TCP port 22 while SNMP uses UDP port 161 and 162.

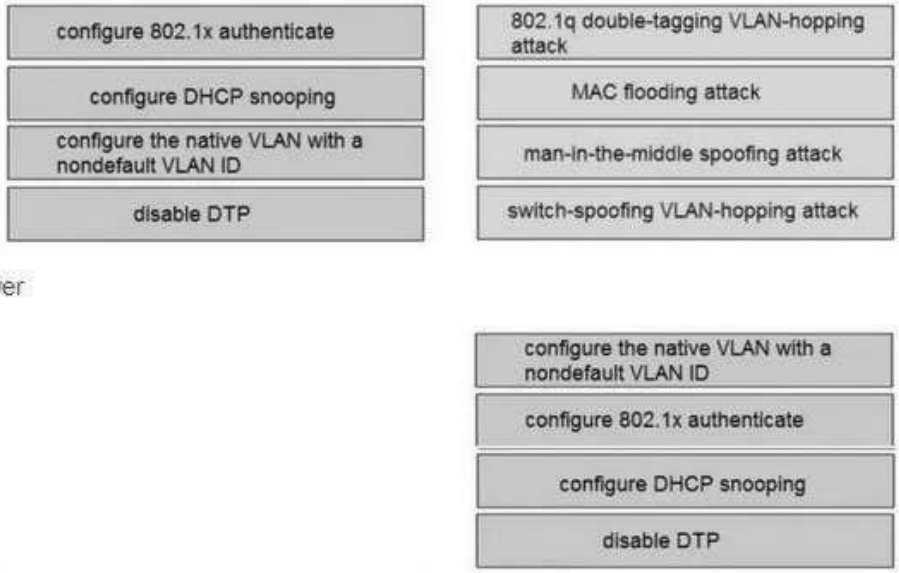
21. Drag and drop the characteristics of networking from the left onto the correct networking types on the right



Answer



22. Drag and drop the attack-mitigation techniques from the left onto the Types of attack that they mitigate on the right.

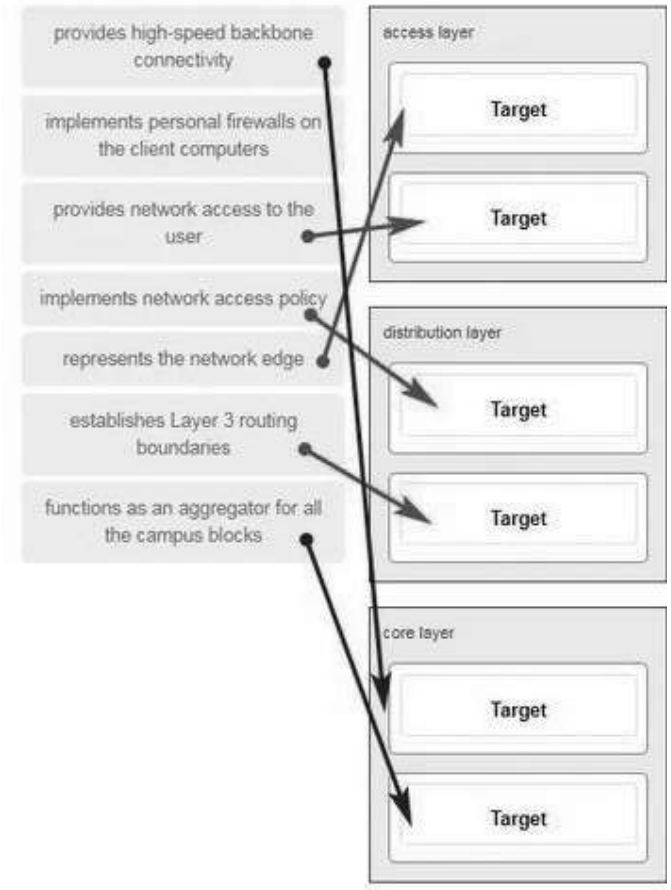


- **802.1q double-tagging VLAN-hopping attack**: configure the native VLAN with a nondefault VLAN ID
- **MAC flooding attack**: configure 802.1x authenticate
- **man-in-the-middle spoofing attack**: configure DHCP snooping
- **switch-spoofing VLAN-hopping attack**: disable DTP

23. Match the functions to the corresponding layers. (Not all options are used.)


provides high-speed backbone connectivity
implements personal firewalls on the client computers
provides network access to the user
implements network access policy
represents the network edge
establishes Layer 3 routing boundaries
functions as an aggregator for all the campus blocks
access layer
Target
Target
distribution layer
Target
Target
core layer
Target
Target

Answer



access layer

- provides network access to the user
- represents the network edge

distribution layer

- implements network access policy
- establishes Layer 3 routing boundaries

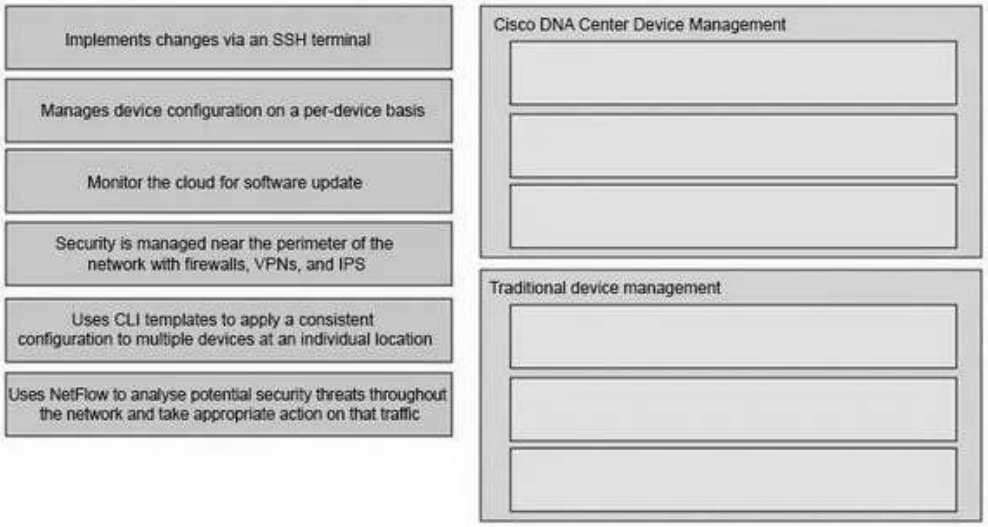
core layer

- provides high-speed backbone connectivity
- functions as an aggregator for all the campus blocks

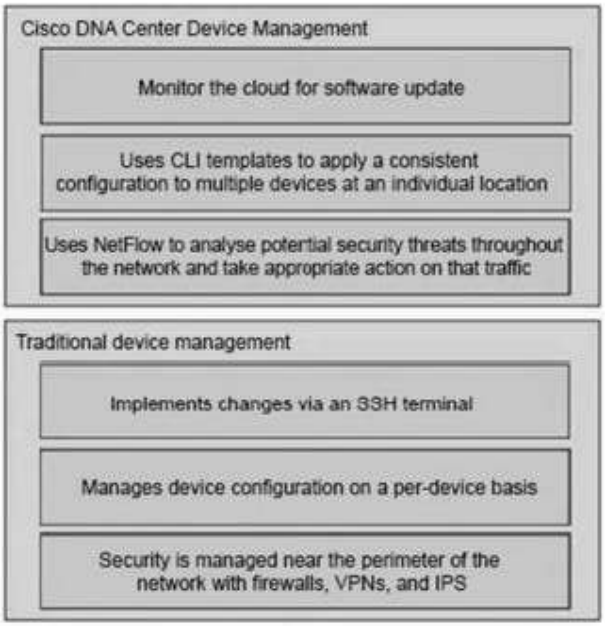
Not use:

- implements personal firewalls on the client computers

24. Drag the descriptions of device management from the left onto the types of device management on the right



Answer



Cisco DNA Center Device Management

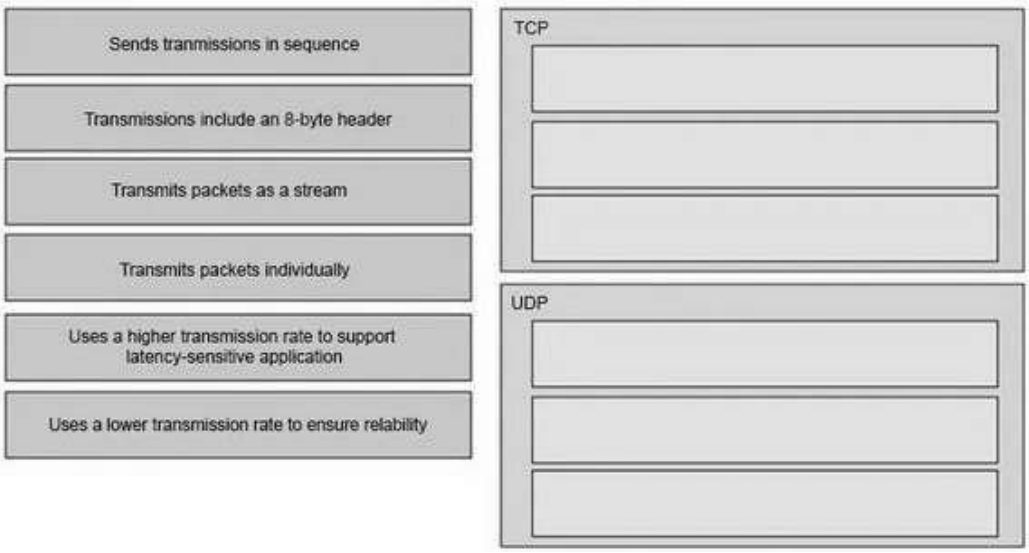
- 3. Monitor the cloud for software update
- 5. Uses CLI templates to apply a consistent configuration to multiple devices at an individual location

- 6. Uses NetFlow to analyse potential security threats throughout the network and take appropriate action on that traffic

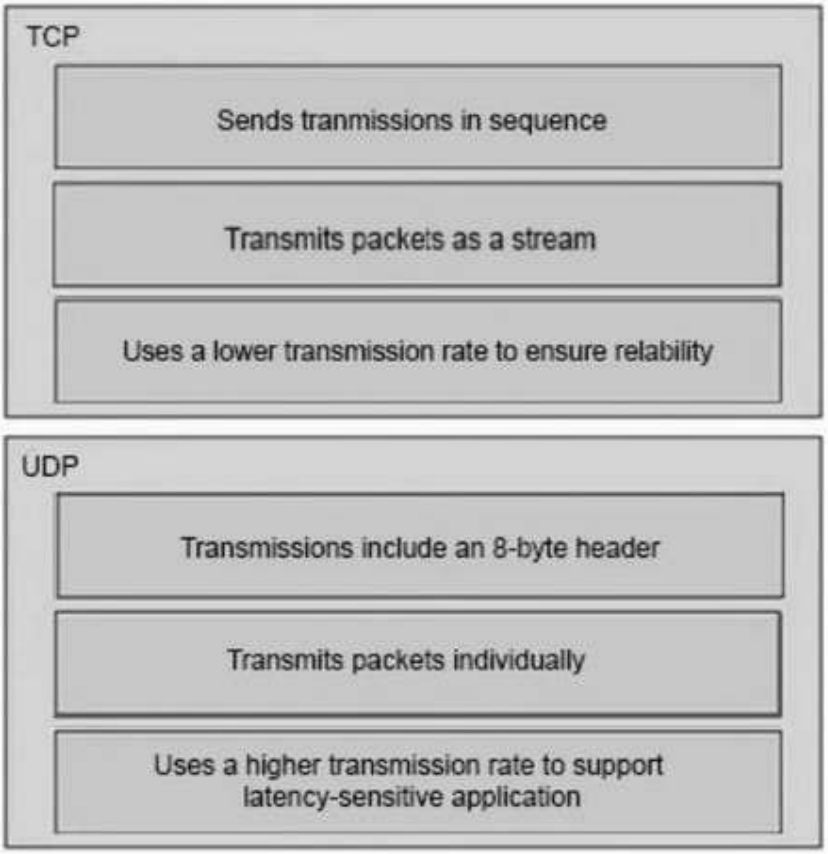
Traditional device management

- 1. Implements changes via an SSH terminal
- 2. Manages device configuration on a per-device basis
- 4. Security is managed near the perimeter of the network with firewalls, VPNs, and IPS

25. Drag the descriptions of IP protocol transmissions from the left onto the IP traffic types on the right.



Answer



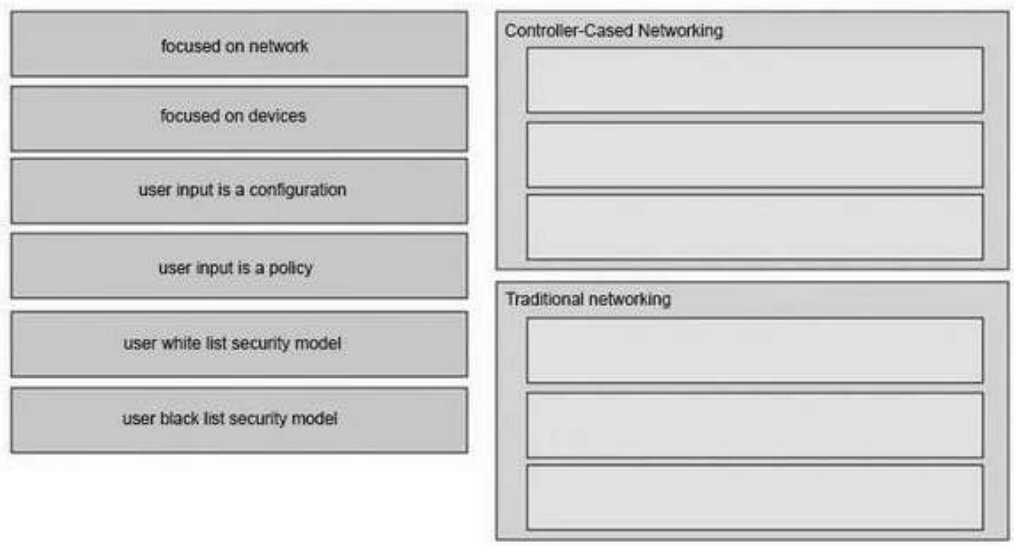
TCP

- 1. Sends tranmissions in sequence
- 3. Transmits packets as a stream
- 6. Uses a lower transmission rate to ensure relability

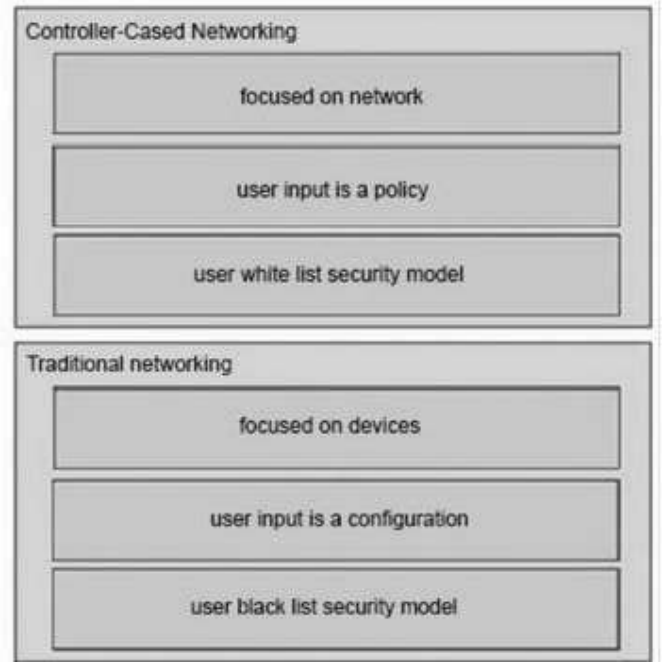
UDP

- 2. Transmissions include an 8-byte header
- 4. Transmits packets individually
- 5. Uses a higher transmission rate to support latency-sensitive application

26. Drag and drop to the characteristics of networking from the left onto the correct networking types on the right.

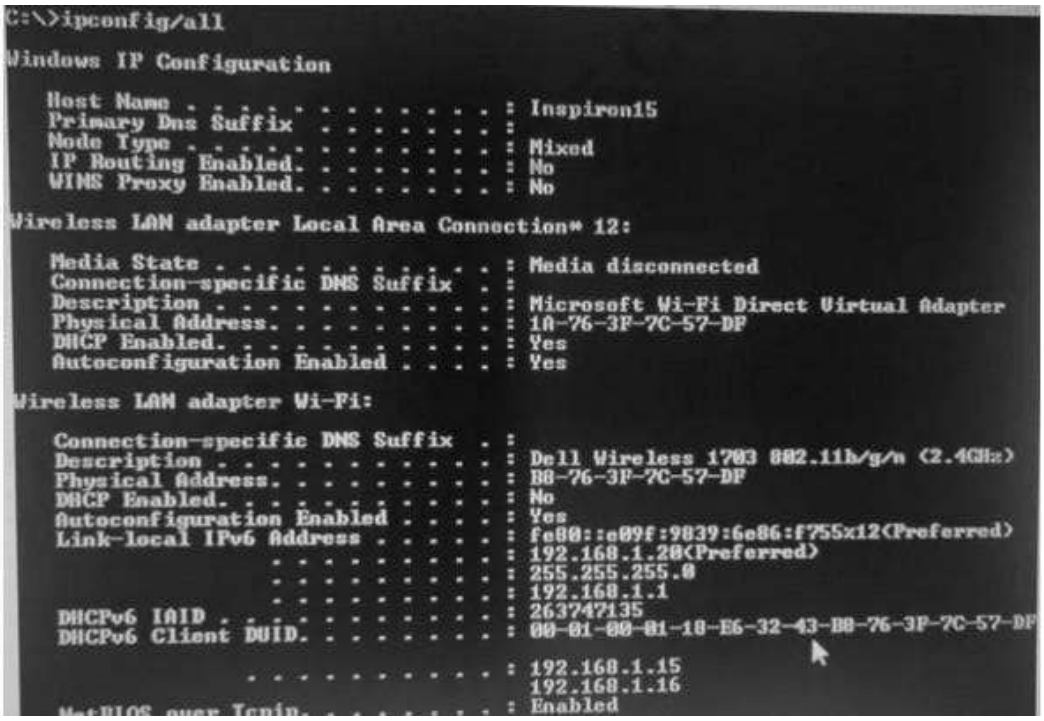


Answers:

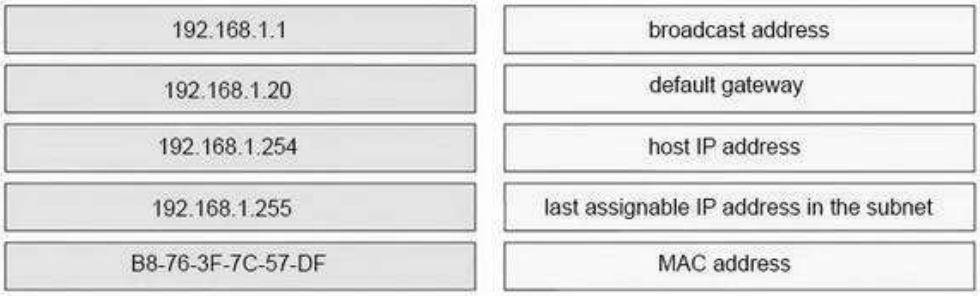


27. Refer to the exhibit.

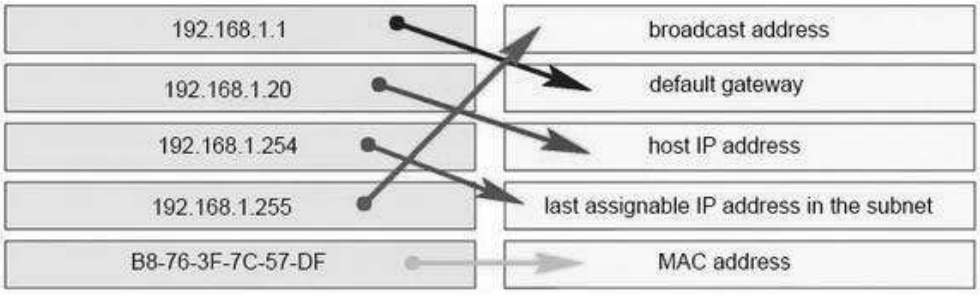
An engineer is tasked with verifying network configuration parameters on a client workstation to report back to the team lead. Drag and drop the node identifiers from the left onto the network parameters on the right.


C:\>ipconfig/all
Windows IP Configuration
Host Name . . . . . : Inspiron15
Primary Dns Suffix . . . . . :
Node Type . . . . . : Mixed
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
Wireless LAN adapter Local Area Connection* 12:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft Wi-Fi Direct Virtual Adapter
Physical Address. . . . . : 1A-76-3P-7C-57-DP
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . :
Description . . . . . : Dell Wireless 1703 802.11b/g/n (2.4GHz)
Physical Address. . . . . : B8-76-3P-7C-57-DP
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::e09f:9839:6e86:f755x12(Preferred)
. . . . . : 192.168.1.20(Preferred)
. . . . . : 255.255.255.0
. . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 263747135
DHCPv6 Client DUID. . . . . : 00-01-00-01-18-E6-32-43-B8-76-3P-7C-57-DP
. . . . . : 192.168.1.15
192.168.1.16
NetBIOS over Tcpip. . . . . : Enabled

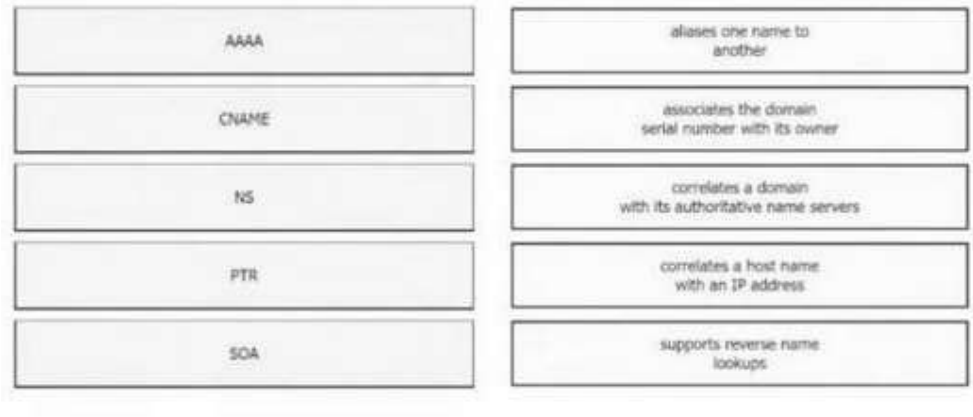
An engineer is tasked with verifying network configuration parameters on a client workstation to report back to the team lead. Drag and drop the node identifiers from the left onto the network parameters on the right.



Answer:

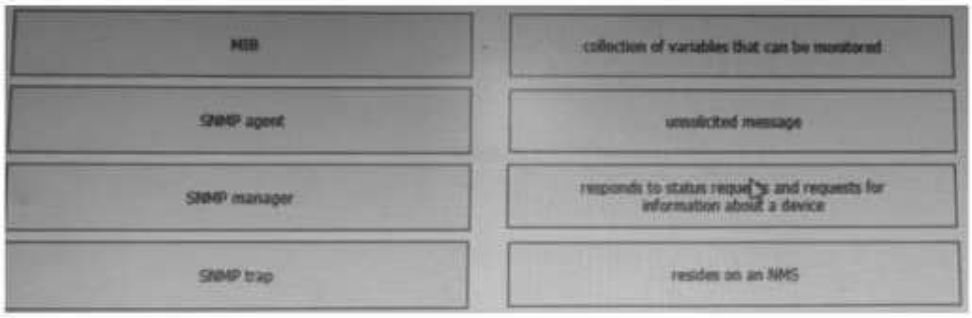


28. Drag the IPv6 DNS record types from the left onto the description on the right.

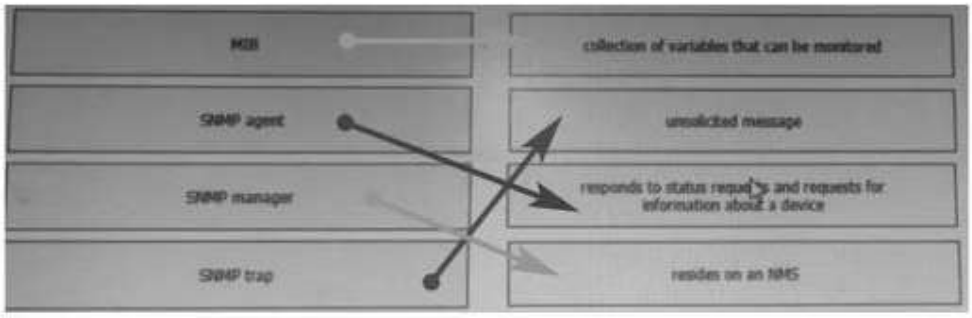


Answer:

29. Drag and drop the SNMP components from the left onto the descriptions on the right.

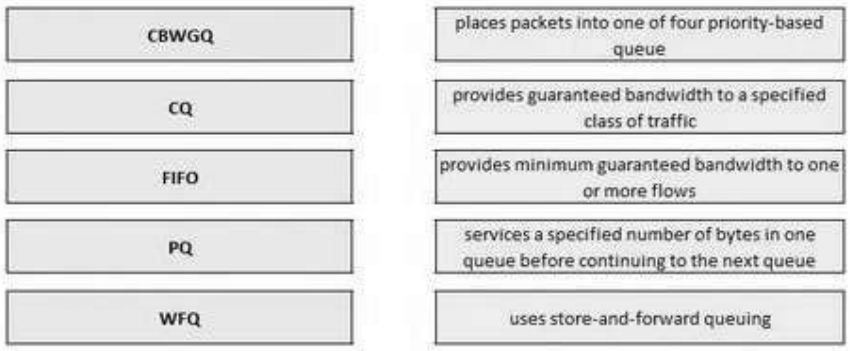


Answer:

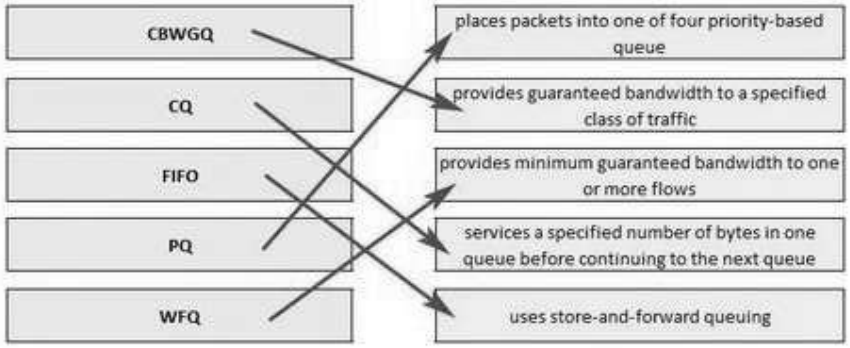


Explanation: MIB: collection of variables that can be monitored SNMP agent: responds to status requests and requests for information about a device
SNMP manager: The SNMP manager is part of an NMS
SNMP trap: unsolicited messages that are sent by the SNMP agent and alert the NMS to a condition on the network

30. Drag and drop the QoS congestion management terms from the left onto the description on the right.

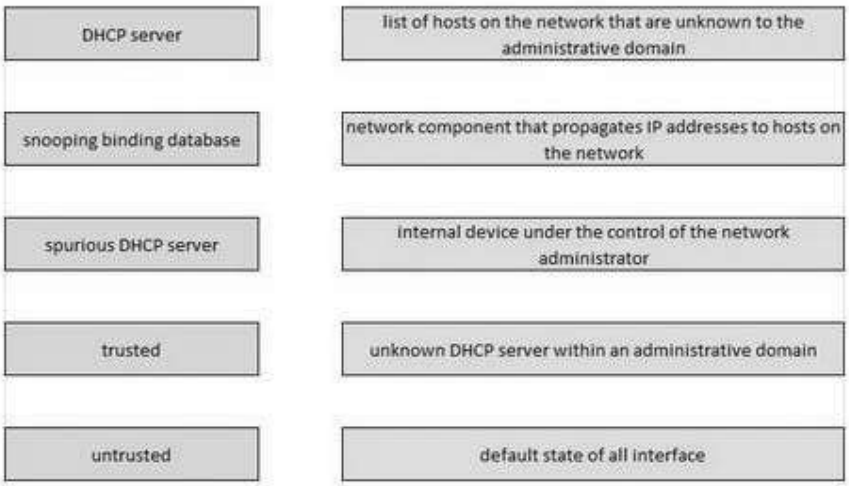


Answer:

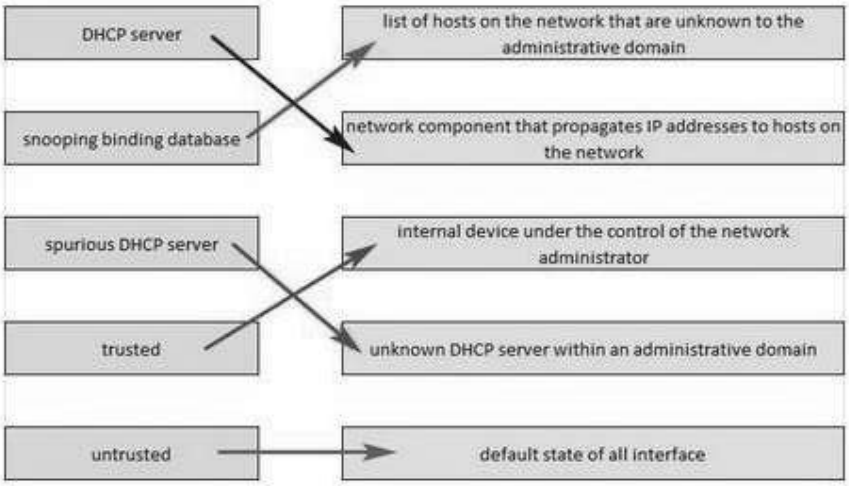


- **CBWGQ** : provides guaranteed bandwidth to a specified class of traffic
- **CQ** : services a specified number of bytes in one queue before continuing to the next queue
- **FIFO** : uses store-and-forward queuing
- **PQ** : places packets into one of four priority-based queues
- **WFQ** : provides minimum guaranteed bandwidth to one or more flows

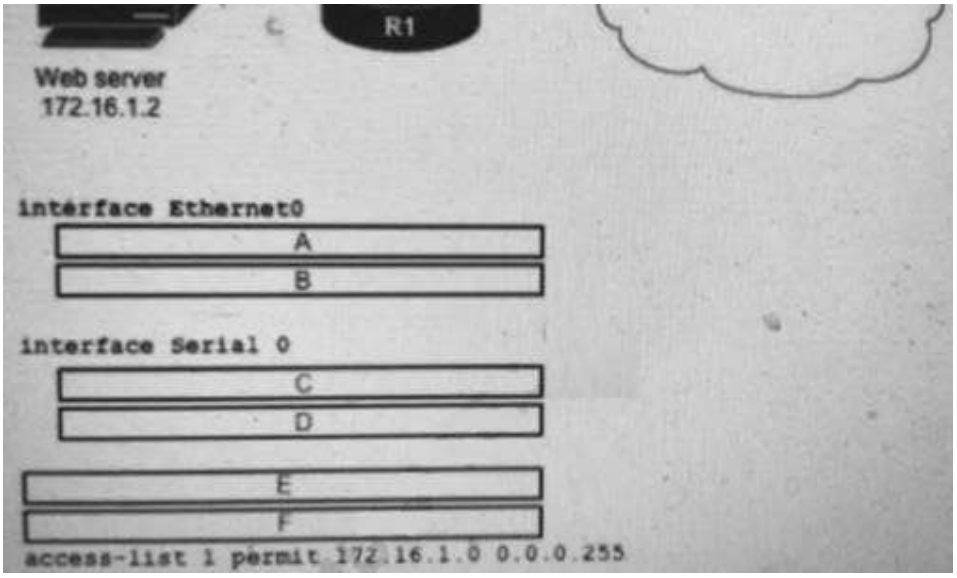
31. Drag and drop the DHCP snooping terms from the left onto the descriptions on the right.


DHCP server
list of hosts on the network that are unknown to the administrative domain
snooping binding database
network component that propagates IP addresses to hosts on the network
spurious DHCP server
internal device under the control of the network administrator
trusted
unknown DHCP server within an administrative domain
untrusted
default state of all interface

Answer:

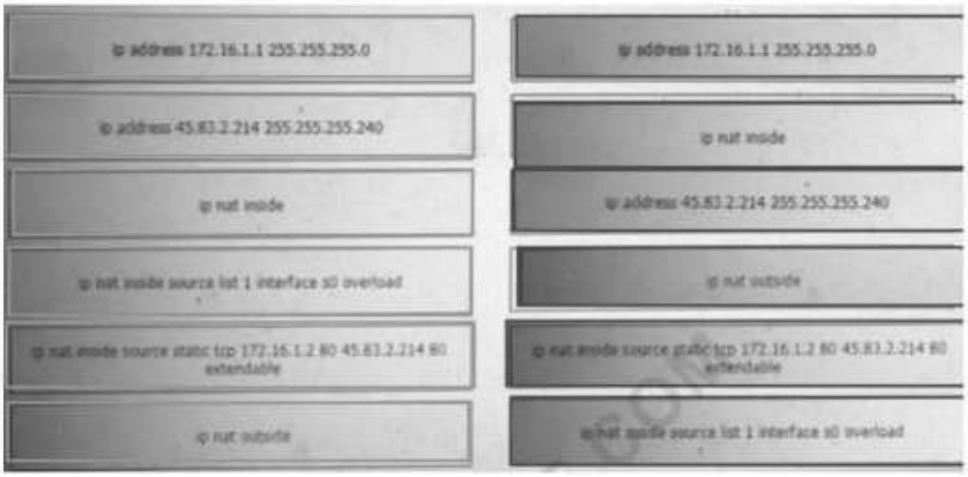

DHCP server
list of hosts on the network that are unknown to the administrative domain
snooping binding database
network component that propagates IP addresses to hosts on the network
spurious DHCP server
internal device under the control of the network administrator
trusted
unknown DHCP server within an administrative domain
untrusted
default state of all interface

32. Refer to the exhibit.

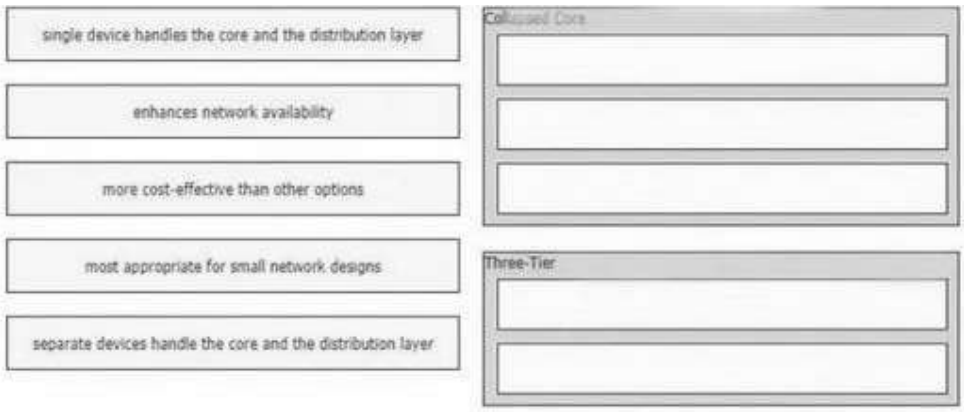


An engineer is configuring the router to provide static NAT for the webserver Drag and drop the configuration commands from the left onto the letters that correspond to its position in the configuration on the right.

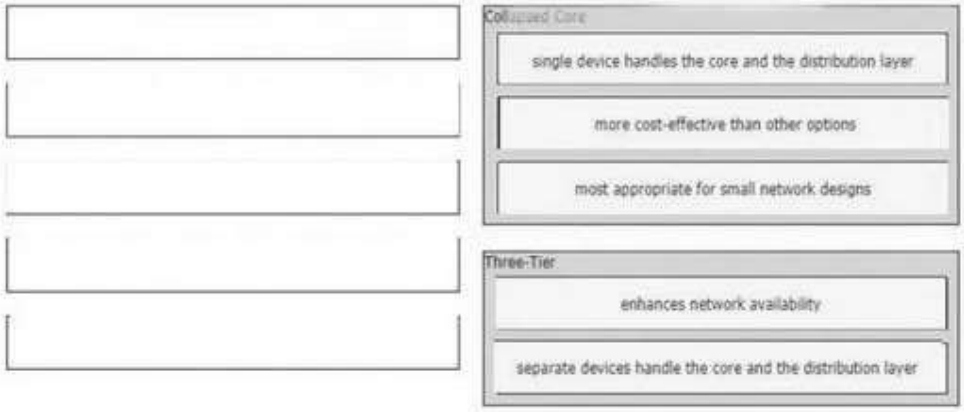
Answer:



33. Drag and drop the characteristics of network architectures from the left onto the type of architecture on the right.

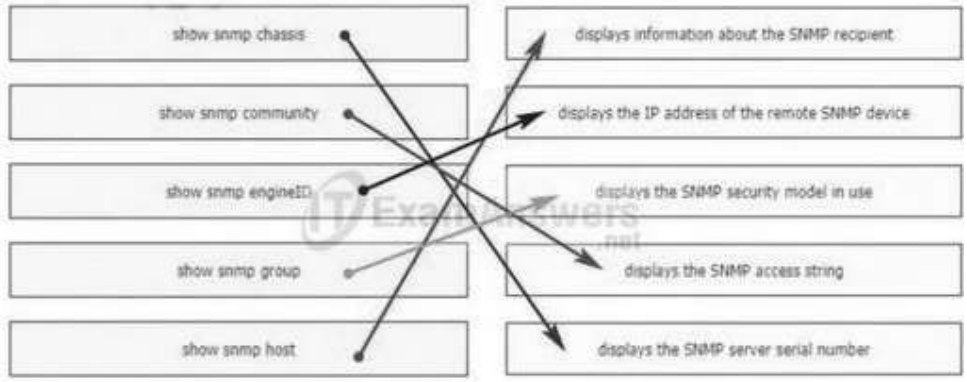


Answers

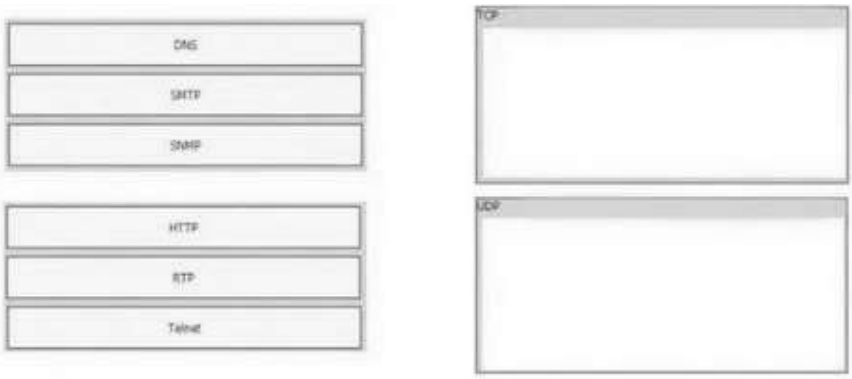


34. Drag and drop the SNMP manager and agent identifier commands from the left onto the functions on the right

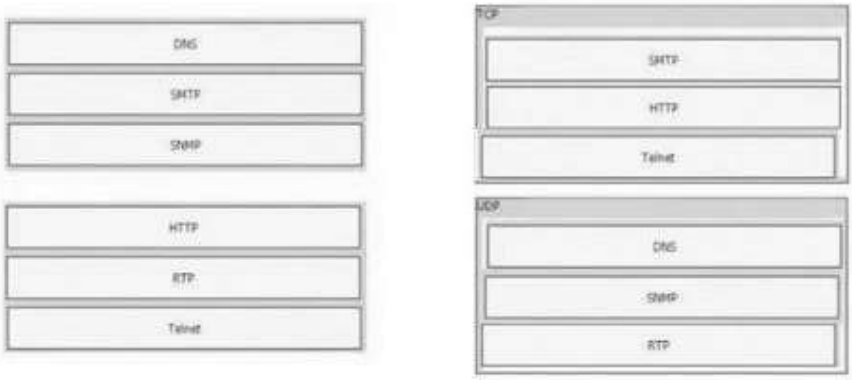
Answers



35. Drag and drop the TCP/IP protocols from the left onto the transmission protocols on the right

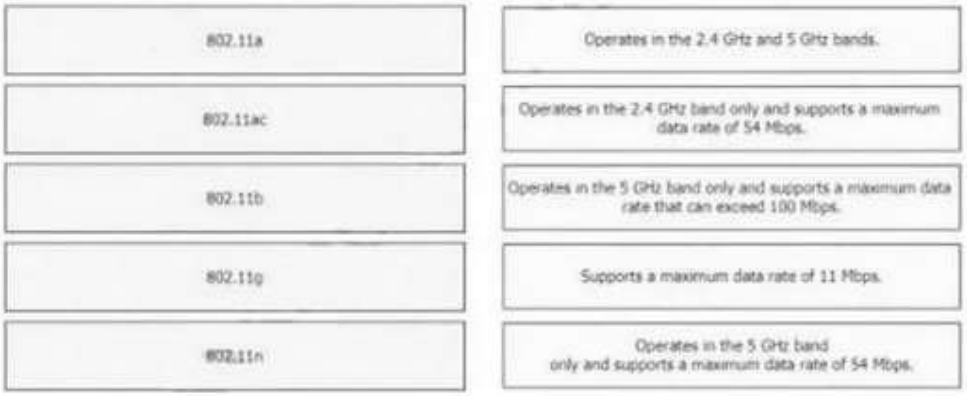


Correct Answer:



36.

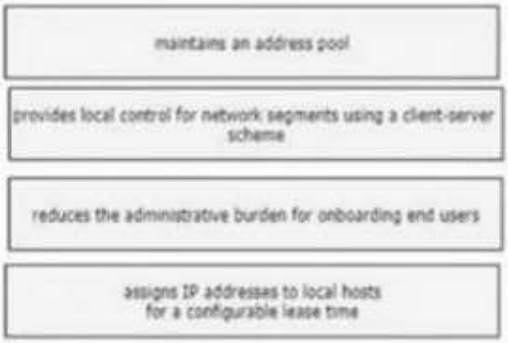
Drag and drop the 802.11 wireless standards from the left onto the matching statements on the right



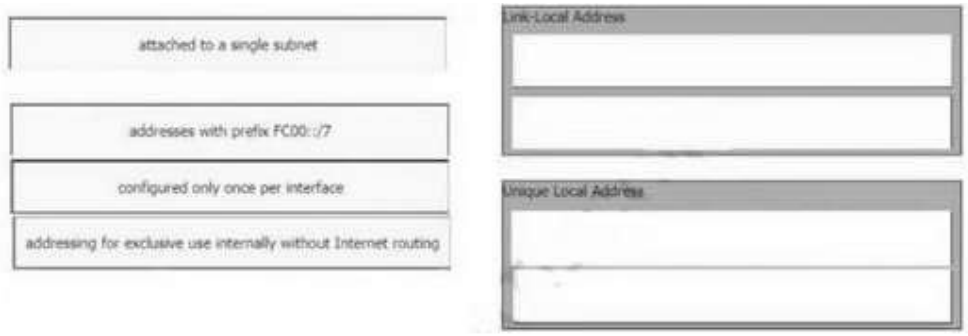
Answer:

37. Drag and drop the functions of DHCP from the left onto any of the positions on the right (Not all functions are used)

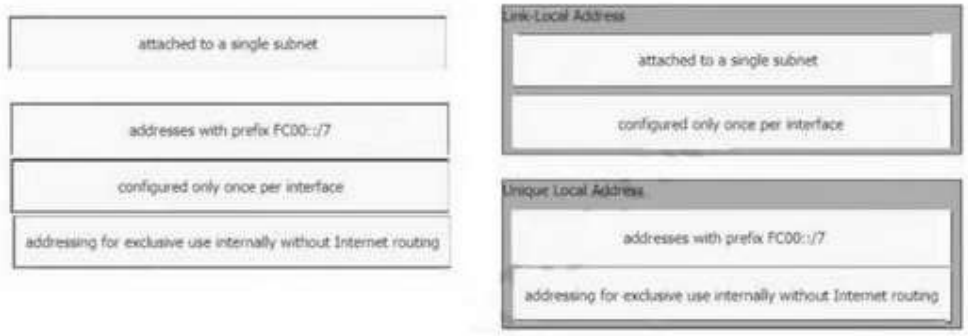
Answer:



38. Drag and drop the IPv6 address type characteristics from the left to the right



Answer:

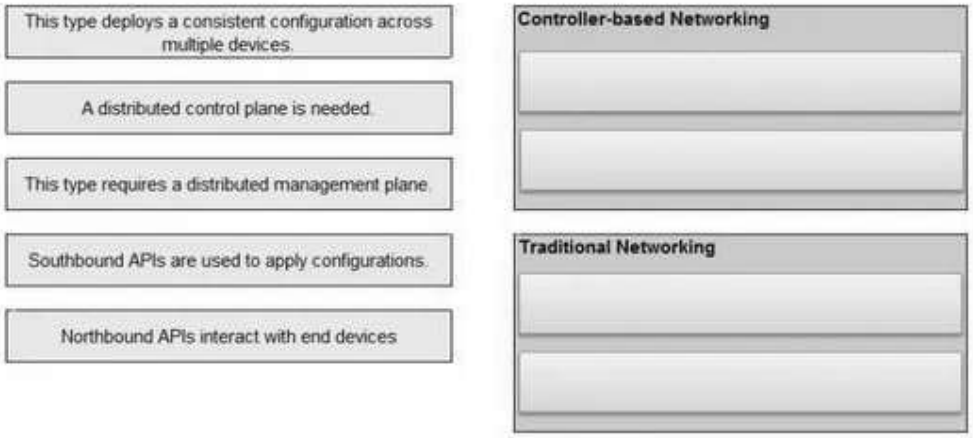


Explanation/Reference: "A link-local address is a unicast address that is confined to a single link, a single subnet."
"There can be only one link-local address per interface."
"ULA addresses are for devices that never need access to the Internet and never need to be accessible from the Internet."
Reference: Click here

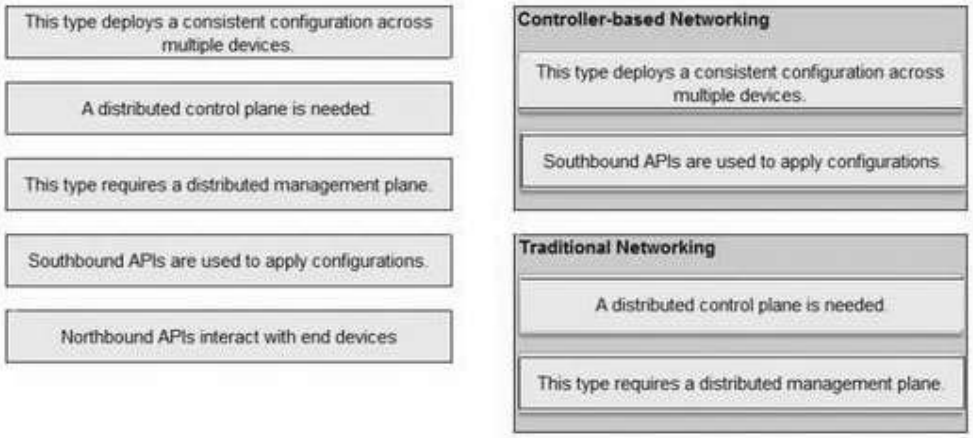
39. An engineer is configuring an encrypted password for the enable command on a router where the local user database has already been configured. Drag and drop the configuration commands from the left into the correct sequence on the right (Not all commands are used)

Answer:

40. Drag and drop the statement about networking from the left into the Corresponding networking types on the right. Not all statements are used.



Answer:



Controller-based Networking :

- This type deploys a consistent configuration across multiple devices.
- Southbound APIs are used to apply configurations.

Traditional Networking :

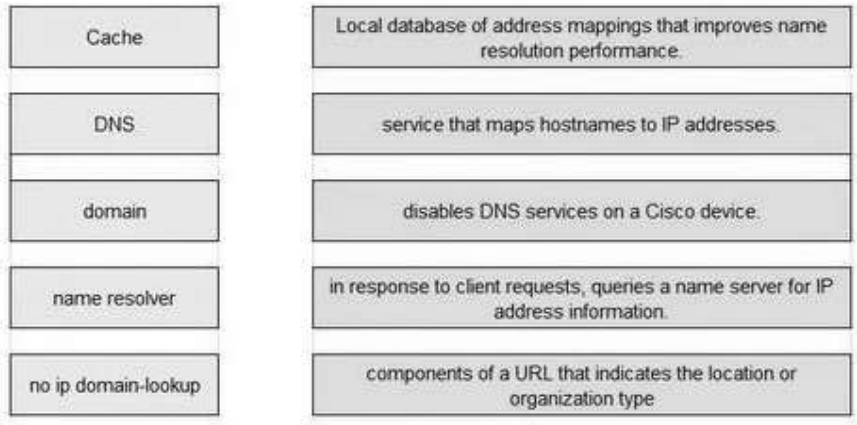
- A distributed control plane is needed.
- This type requires a distributed management plane.

Explanation: On a SND network the control plane is centralized on the the SND controller not distributed on the networking devices.

Northbound APIs do not interact with end devices. They allow the SND controller to interact with applications on the application plane.

On a SND network the management plane is not centralized, it is distributed. Network management protocols, such as Telnet, SSH, SNMP, and Syslog operate in the management plane on both traditional network and controller-based network.

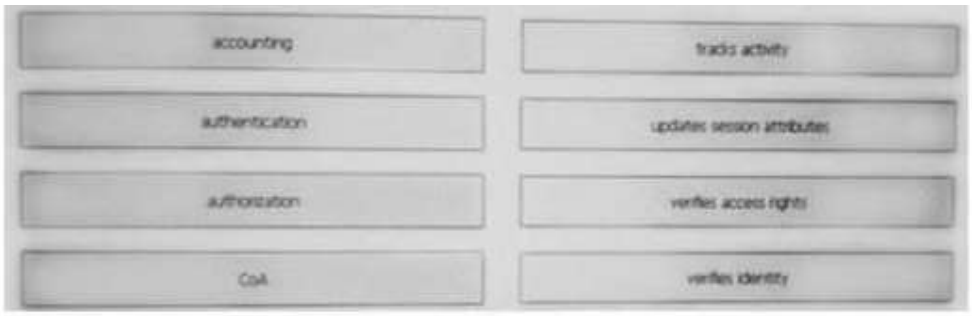
41. Drag and drop the DNS lookup components from the left onto the functions on the right.



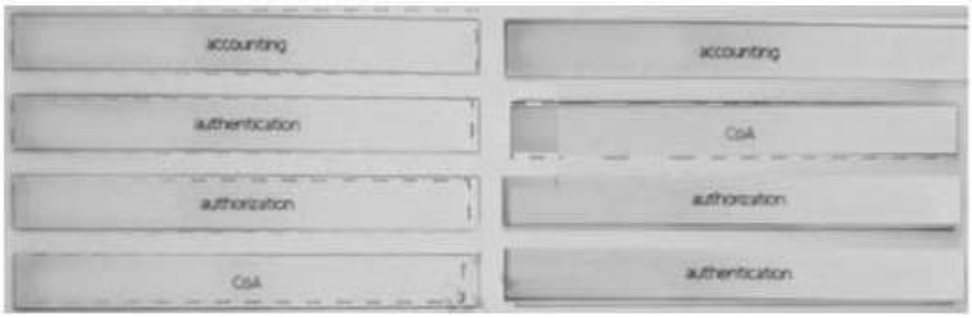
Answers

- **Cache** –> Local database of address mappings that improves name resolution performance.
- **DNS** –> service that maps hostnames to IP addresses.
- **no ip domain-lookup** –> disables DNS services on a Cisco device.
- **name resolver** –> in response to client requests, queries a name server for IP address information.
- **domain** –> components of a URL that indicates the location or organization type

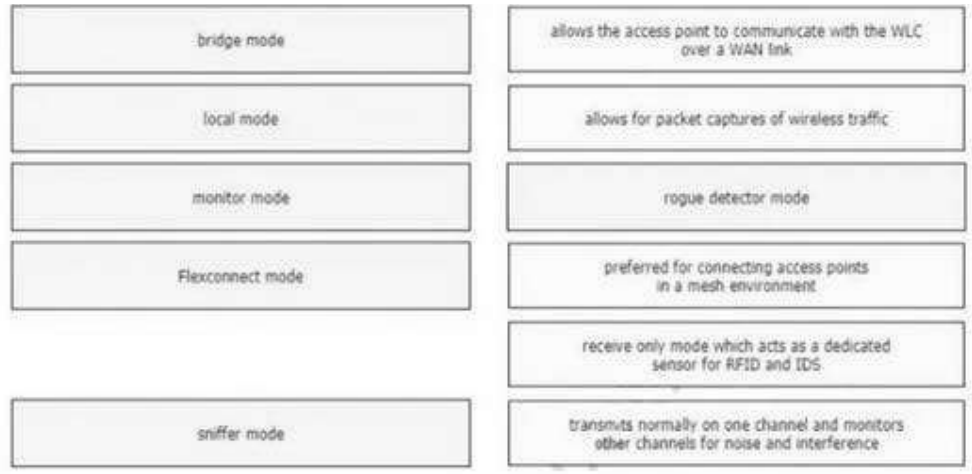
42. Drag and drop the AAA terms from the left onto the description on the right.



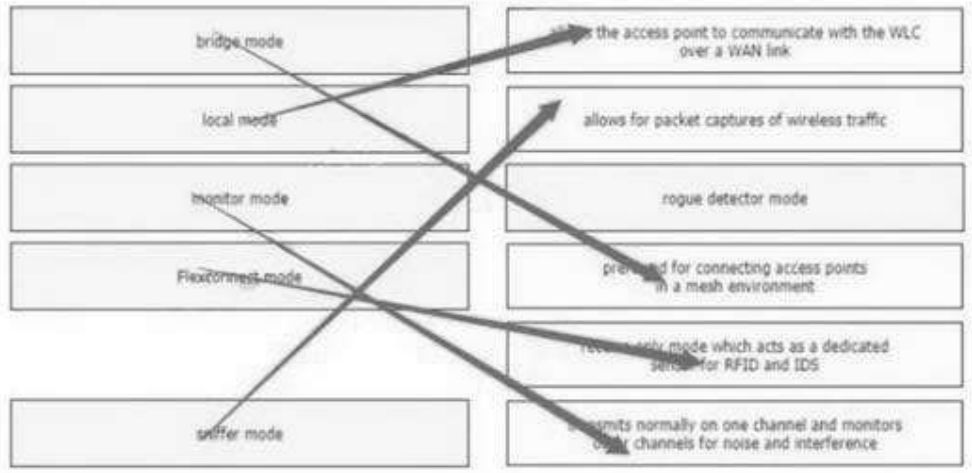
Answer:



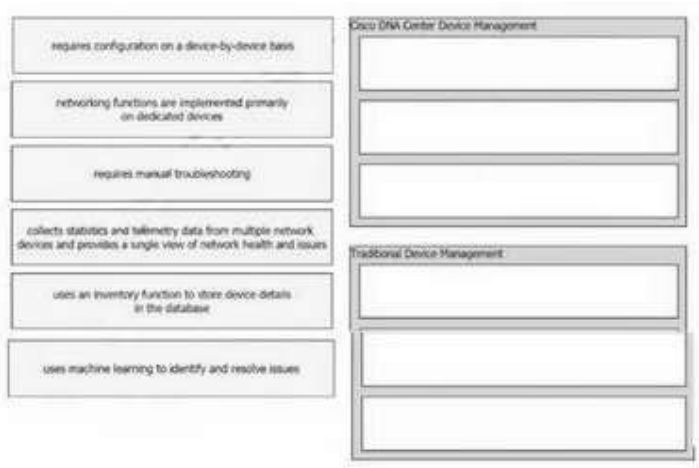
43. Drag and drop the lightweight access point operation modes from the left onto the descriptions on the right



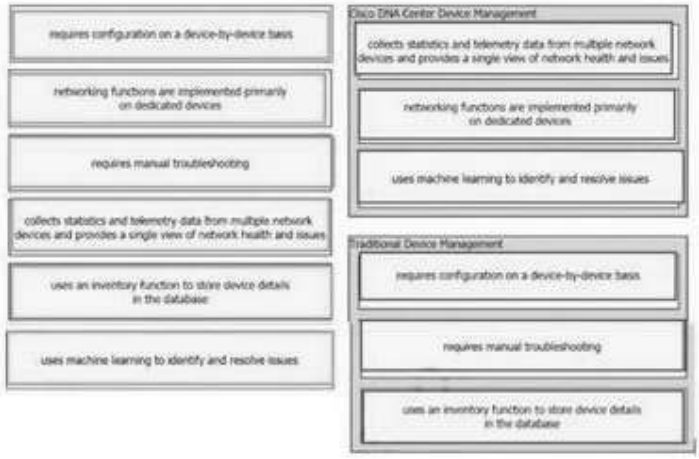
Answer:



44. Drag the descriptions of device management from the left onto the types of device management on the right.

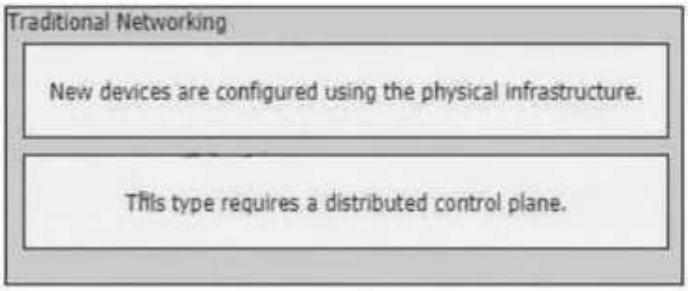


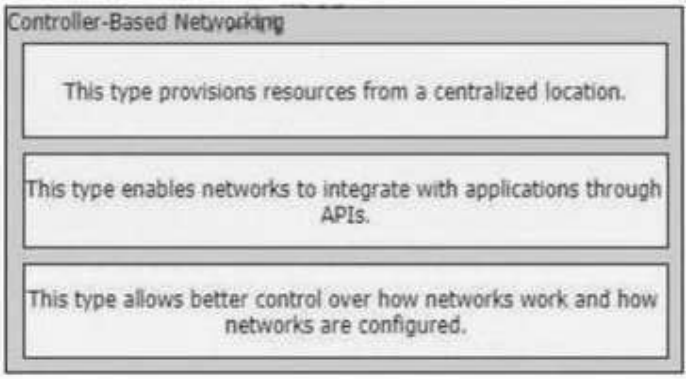
Answer:



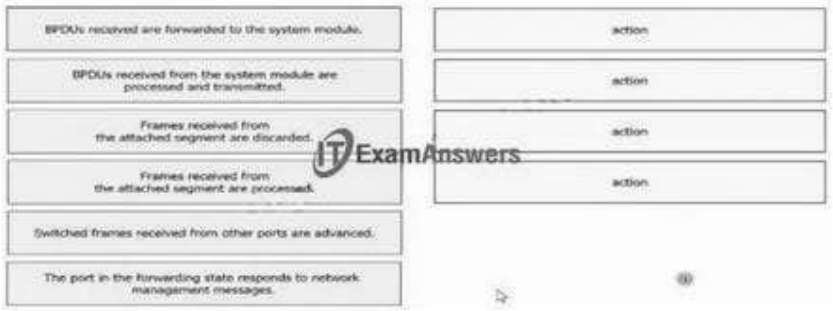
45. Drag and drop the statements about networking from the left onto the corresponding networking types on the right.

Answer:

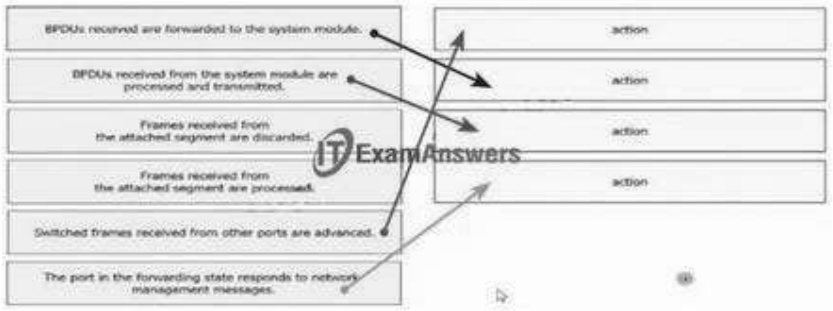




46. Drag and drop the Rapid PVST+ forwarding slate actions from the loft to the right. Not all actions are used.

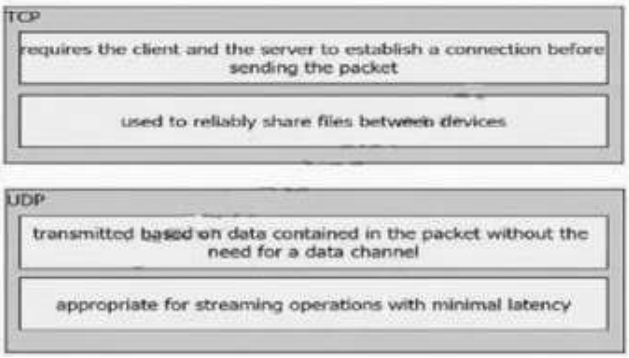


Answer:



47. Drag and drop the TCP or UDP details from the left onto their corresponding protocols on the right.

Answer:



48. Drag and drop the facts about wireless architectures from the left onto the types of access point on the right. Not all options are used.

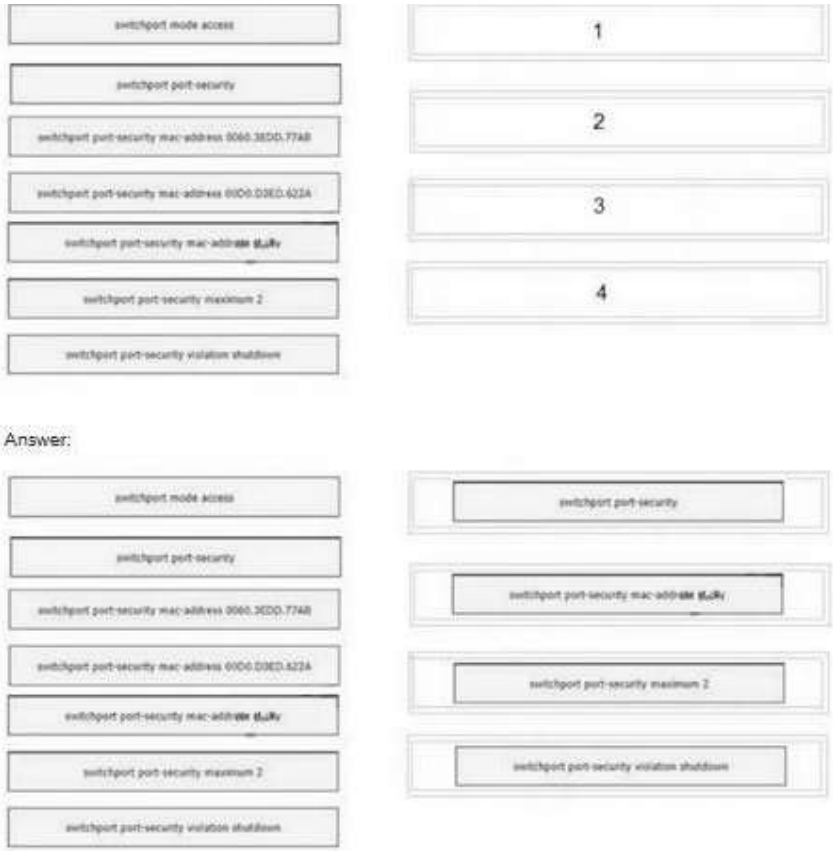
Answer:

49. Refer to the exhibit. Drag and drop the prefix lengths from the left onto the corresponding prefixes on the right Not all prefixes are used see the answer below.

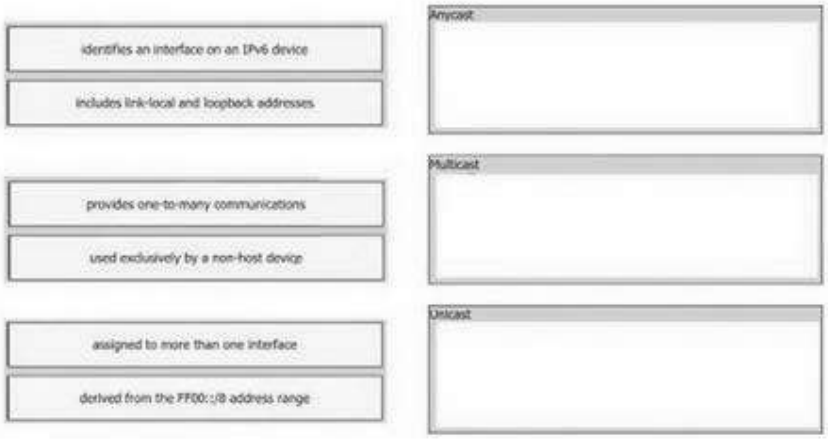
```
      209.165.201.0/27 is subnetted, 1 subnets
B        209.165.201.0 [20/0] via 10.10.12.2, 02:26:33
      209.165.202.0/27 is subnetted, 1 subnets
B        209.165.202.128 [20/0] via 10.10.12.2, 02:26:03
      10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
C        10.10.10.0/28 is directly connected, GigabitEthernet0/0
C        10.10.11.0/30 is directly connected, FastEthernet2/0
C        10.10.12.0/30 is directly connected, GigabitEthernet0/1
O        10.10.13.0/25 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.128/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.144/28 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.160/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
O        10.10.13.208/29 [110/2] via 10.10.10.1, 00:00:04, GigabitEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.10.11.2
```

Answer:

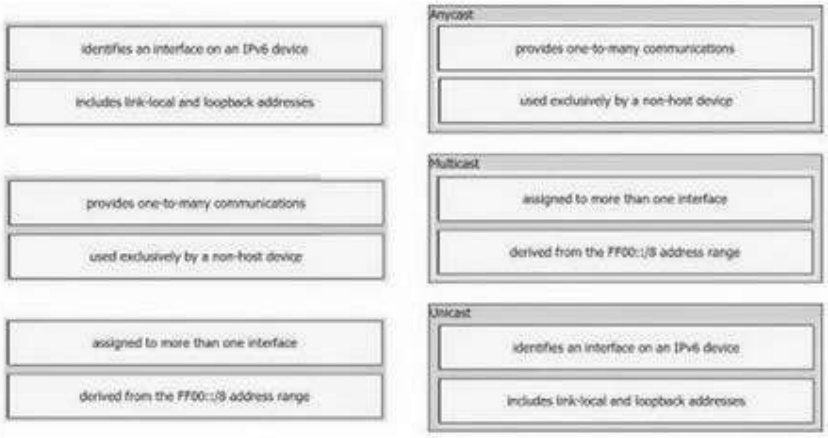
50. An engineer is tasked to configure a switch with port security to ensure devices that forward unicasts multicasts and broadcasts are unable to flood the port The port must be configured to permit only two random MAC addresses at a time Drag and drop the required configuration commands from the left onto the sequence on the right Not all commands are used.



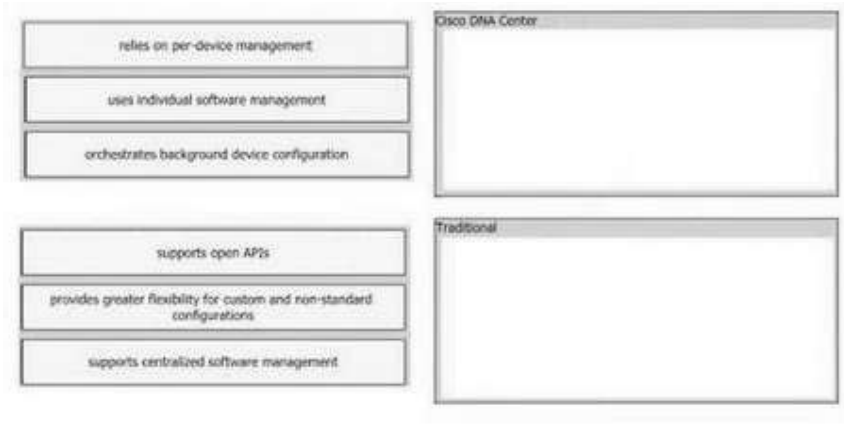
51. Drag and drop the IPv6 address details from the left onto the corresponding types on the right.



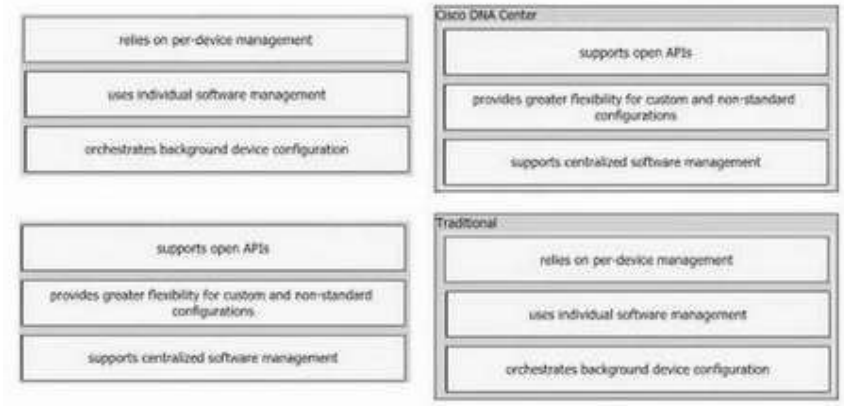
Answer:



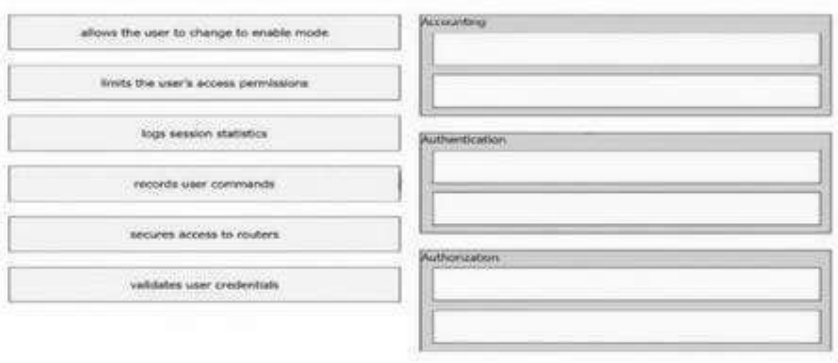
52. Drag and drop each characteristic of device-management technologies from the left onto the deployment type on the right.



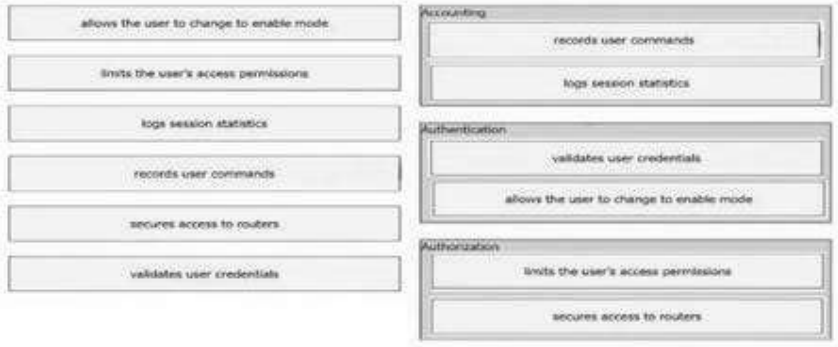
Answer:



53. Drag and drop the descriptions of AAA services from the left onto the corresponding services on the right.

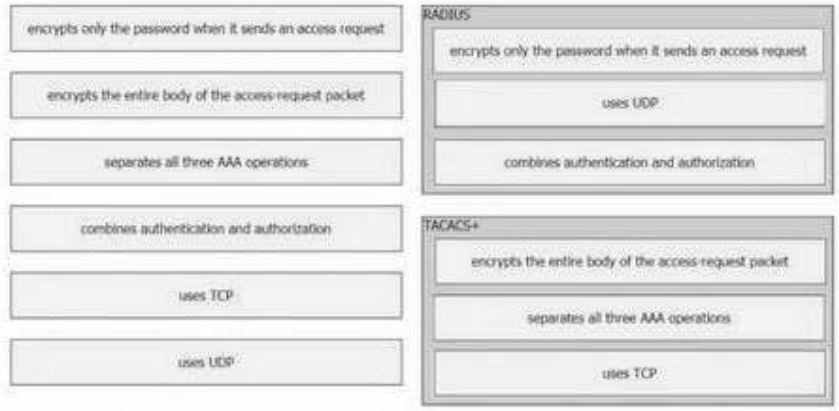


Answer:

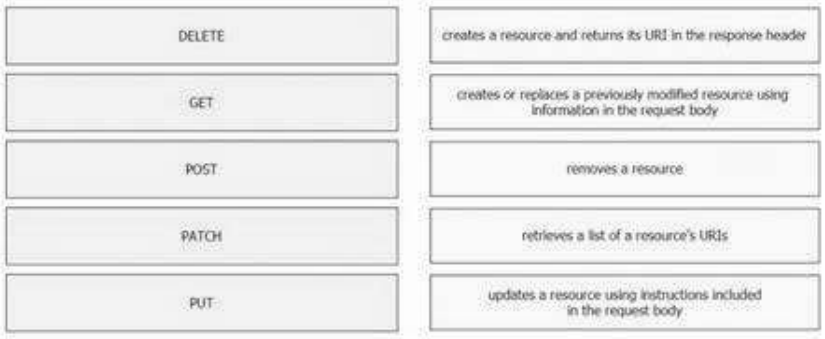


54. Drag and drop the functions of AAA supporting protocols from the left onto the protocols on the right.

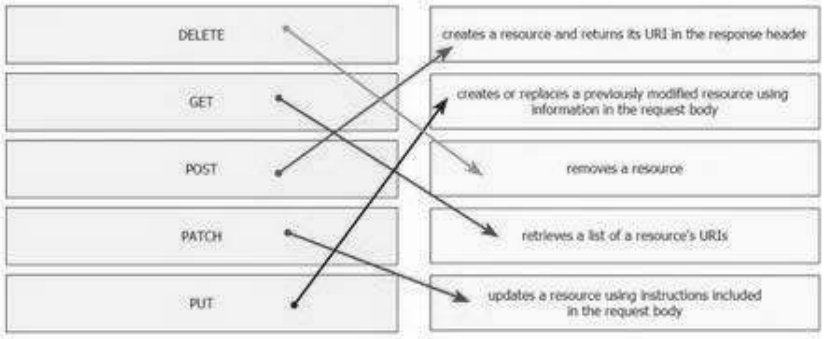
Answer:



55. Drag and drop the HTTP methods used with REST-based APIs from the left onto the descriptions on the right.


DELETE
GET
POST
PATCH
PUT
creates a resource and returns its URI in the response header
creates or replaces a previously modified resource using information in the request body
removes a resource
retrieves a list of a resource's URIs
updates a resource using instructions included in the request body

Answer:


DELETE
GET
POST
PATCH
PUT
creates a resource and returns its URI in the response header
creates or replaces a previously modified resource using information in the request body
removes a resource
retrieves a list of a resource's URIs
updates a resource using instructions included in the request body