Vendor: Cisco

Exam Code:200-120

Exam Name: Cisco Certified Network Associate Exam

Version: Demo

QUESTION 1

At which layer of the OSI model is RSTP used to prevent loops?

A. physical

B. data link

C. network

D. transport

Correct Answer: B

RSTP and STP operate on switches and are based on the exchange of Bridge Protocol Data Units (BPDUs) between switches. One of the most important fields in BPDUs is the Bridge Priority in which the MAC address is used to elect the Root Bridge -> RSTP operates at Layer 2 ?Data Link layer >;.

QUESTION 2

A switch is configured with all ports assigned to VLAN 2 with full duplex FastEthernet to segment existing departmental traffic. What is the effect of adding switch ports to a new VLAN on the switch?

A. More collision domains will be created.

B. IP address utilization will be more efficient.

C. More bandwidth will be required than was needed previously.

D. An additional broadcast domain will be created.

Correct Answer: D

Each VLAN creates its own broadcast domain. Since this is a full duplex switch, each port is a separate collision domain.

QUESTION 3

A network administrator is trying to add a new router into an established OSPF network. The networks attached to the new router do not appear in the routing tables of the other OSPF routers. Given the information in the partial configuration shown below, what configuration error is causing this problem?

Router(config)# router ospf 1 Router(config-router)# network 10.0.0.0 255.0.0.0 area 0

A. The process id is configured improperly.

B. The OSPF area is configured improperly.

C. The network wildcard mask is configured improperly.

D. The network number is configured improperly.

E. The AS is configured improperly.

F. The network subnet mask is configured improperly.

Correct Answer: C

When configuring OSPF, the mask used for the network statement is a wildcard mask similar to an access list. In this specific example, the correct syntax would have been "network 10.0.0.0 0.0.0.255 area 0."

QUESTION 4

Syslog was configured with a level 3 trap. Which 3 types of logs would be generated (choose four)

A. Emergencies

B. Alerts

C. Critical

D. Errors

E. Warnings

Correct Answer: ABCD

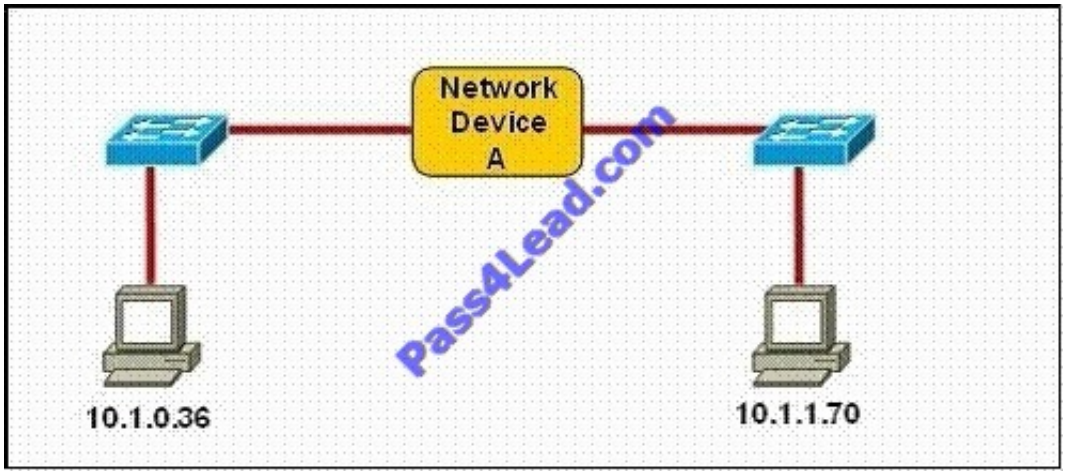
The Message Logging is divided into 8 levels as listed below:

Level Keyword Description 0 emergencies System is unusable 1 alerts Immediate action is needed 2 critical Critical conditions exist 3 errors Error conditions exist 4 warnings Warning conditions exist 5 notification Normal, but significant, conditions exist 6 informational Informational messages 7 debugging Debugging messages

The highest level is level 0 (emergencies). The lowest level is level 7. If you specify a level with the "logging console level" command, that level and all the higher levels will be displayed. For example, by using the "logging console warnings" command, all the logging of emergencies, alerts, critical, errors, warnings will be displayed.

QUESTION 5

Refer to the exhibit.



Which three statements correctly describe Network Device A? (Choose three.)

A. With a network wide mask of 255.255.255.128, each interface does not require an IP address.

B. With a network wide mask of 255.255.255.128, each interface does require an IP address on a unique IP subnet.

C. With a network wide mask of 255.255.255.0, must be a Layer 2 device for the PCs to communicate with each other.

D. With a network wide mask of 255.255.255.0, must be a Layer 3 device for the PCs to communicate with each other.

E. With a network wide mask of 255.255.254.0, each interface does not require an IP address.

Correct Answer: BDE

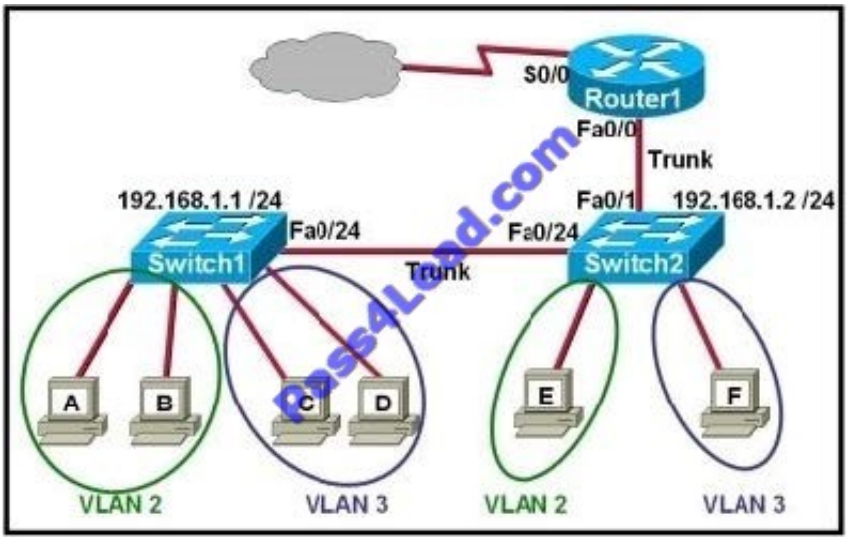
If Subnet Mask is 255.255.255.128 the hosts vary from x.x.x.0 - x.x.x.127 and x.x.x.128- x.x.x.255, so the IP Addresses of 2 hosts fall in different subnets so each interface needs an IP an address so that they can communicate each other.

If Subnet Mask is 255.255.255.0 the 2 specified hosts fall in different subnets so they need a Layer 3 device to communicate.

If Subnet Mask is 255.255.254.0 the 2 specified hosts are in same subnet so are in network address and can be accommodated in same Layer 2 domain and can communicate with each other directly using the Layer 2 address.

QUESTION 6

Refer to the exhibit.



Which two statements are true about interVLAN routing in the topology that is shown in the exhibit? (Choose two.)

A. Host E and host F use the same IP gateway address.

B. Router1 and Switch2 should be connected via a crossover cable.

C. Router1 will not play a role in communications between host A and host D.

D. The FastEthernet 0/0 interface on Router1 must be configured with subinterfaces.

E. Router1 needs more LAN interfaces to accommodate the VLANs that are shown in the exhibit.

F. The FastEthernet 0/0 interface on Router1 and the FastEthernet 0/1 interface on Switch2 trunk ports must be configured using the same encapsulation type.

Correct Answer: DF

In order for multiple VLANs to connect to a single physical interface on a Cisco router, subinterfaces must be used, one for each VLAN. This is known as the router on a stick configuration. Also, for any trunk to be formed, both ends of the trunk must agree on the encapsulation type, so each one must be configured for 802.1q or ISL.

QUESTION 7

Which three statements accurately describe Layer 2 Ethernet switches? (Choose three.)

A. Spanning Tree Protocol allows switches to automatically share VLAN information.

B. Establishing VLANs increases the number of broadcast domains.

C. Switches that are configured with VLANs make forwarding decisions based on both Layer 2 and Layer 3 address information.

D. Microsegmentation decreases the number of collisions on the network.

E. In a properly functioning network with redundant switched paths, each switched segment will contain one root bridge with all its ports in the forwarding state. All other switches in that broadcast domain will have only one root port.

F. If a switch receives a frame for an unknown destination, it uses ARP to resolve the address.

Correct Answer: BDE

Microsegmentation is a network design (functionality) where each workstation or device on a network gets its own dedicated segment (collision domain) to the switch. Each network device gets the full bandwidth of the segment and does not

have to share the segment with other devices. Microsegmentation reduces and can even eliminate collisions because each segment is its own collision domain ->.

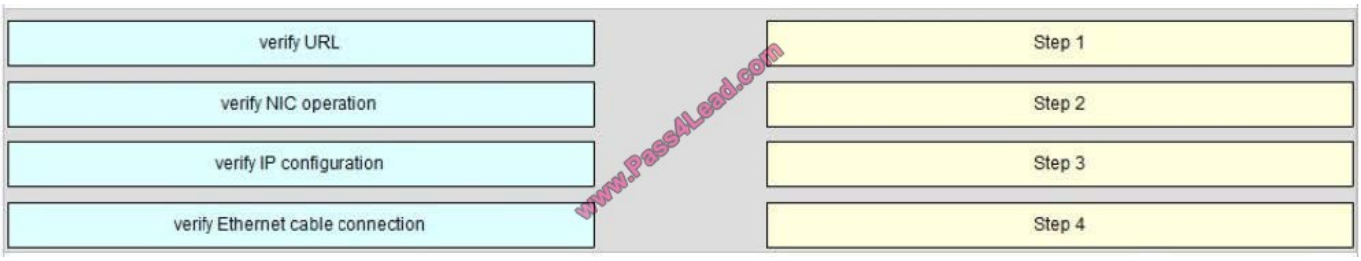
Note: Microsegmentation decreases the number of collisions but it increases the number of collision domains.

QUESTION 8

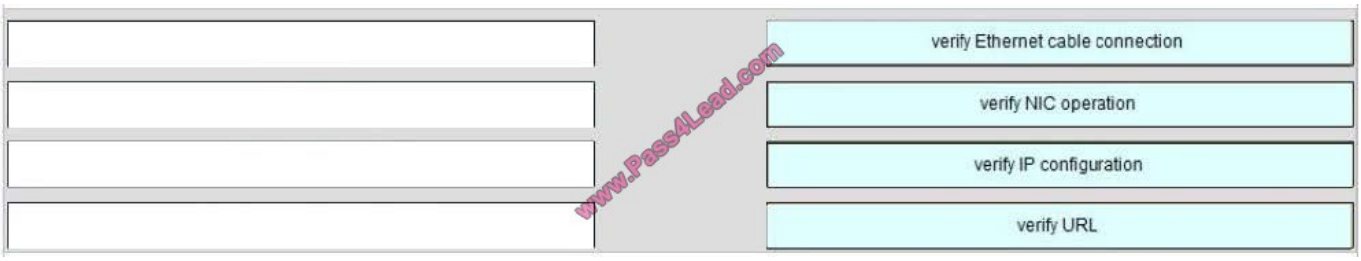
DRAG DROP

A user is unable to connect to the Internet. Based on the layered approach to troubleshooting and beginning with the lowest layer, drag each procedure on the left to its proper category on the right.

Select and Place:



Correct Answer:



The question asks us to “begin with the lowest layer” so we have to begin with Layer 1: verify physical connection; in this case an Ethernet cable connection. For your information, “verify Ethernet cable connection” means that we check if the

type of connection (crossover, straight-through, rollover…) is correct, the RJ45 headers are plugged in, the signal on the cable is acceptable…

Next we “verify NIC operation”. We do this by simply making a ping to the loopback interface 127.0.0.1. If it works then the NIC card (layer 1, 2) and TCP/IP stack (layer 3) are working properly.

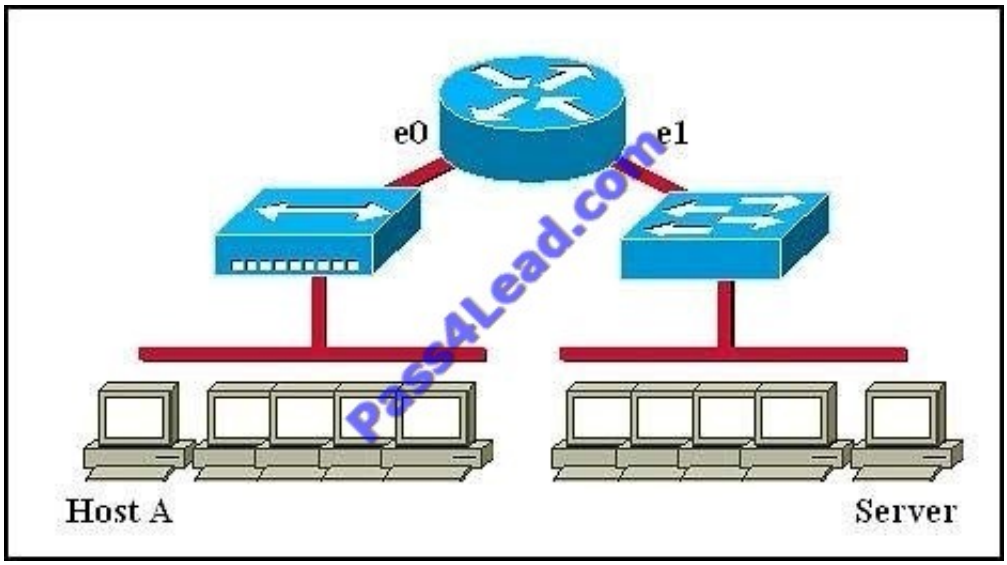
Verify IP configuration belongs to layer 3. For example, checking if the IP can be assignable for host, the PC’s IP is in the same network with the gateway…

Verifying the URL by typing in your browser some popular websites like google.com, microsoft.com to assure that the far end server is not down (it sometimes make we think we can't access to the Internet). We are using a URL so this step

belongs to layer 7 of the OSI model.

QUESTION 9

Refer to the graphic.



Host A is communicating with the server. What will be the source MAC address of the frames received by Host A from the server?

A. the MAC address of router interface e0

B. the MAC address of router interface e1

C. the MAC address of the server network interface

D. the MAC address of host A

Correct Answer: A

Whereas switches can only examine and forward packets based on the contents of the MAC header, routers can look further into the packet to discover the network for which a packet is destined. Routers make forwarding decisions based on the packet\\'s network-layer header (such as an IPX header or IP header). These network-layer headers contain source and destination network addresses. Local devices address packets to the router\\'s MAC address in the MAC header. After receiving the packets, the router must perform the following steps:

1.

Check the incoming packet for corruption, and remove the MAC header. The router checks the packet for MAC-layer errors. The router then strips off the MAC header and examines the network-layer header to determine what to do with the packet.

2.

Examine the age of the packet. The router must ensure that the packet has not come too far to be forwarded. For example, IPX headers contain a hop count. By default, 15 hops is the maximum number of hops (or routers) that a packet can cross. If a packet has a hop count of 15, the router discards the packet. IP headers contain a Time to Live (TTL) value. Unlike the IPX hop count, which increments as the packet is forwarded through each router, the IP TTL value decrements as the IP packet is forwarded through each router. If an IP packet has a TTL value of 1, the router discards the packet. A router cannot decrement the TTL value to 1 and then forward the packet.

3.

Determine the route to the destination. Routers maintain a routing table that lists available networks, the direction to the desired network (the outgoing interface number), and the distance to those networks. After determining which direction to forward the packet, the router must build a new header. (If you want to read the IP routing tables on a Windows 95/98 workstation, type ROUTE PRINT in the DOS box.)

4.

Build the new MAC header and forward the packet. Finally, the router builds a new MAC header for the packet. The MAC header includes the router\\'s MAC address and the final destination\\'s MAC address or the MAC address of the next router in the path.

QUESTION 10

What is the danger of the permit any entry in a NAT access list?

A. It can lead to overloaded resources on the router.

B. It can cause too many addresses to be assigned to the same interface.

C. It can disable the overload command.

D. It prevents the correct translation of IP addresses on the inside network.

Correct Answer: A

QUESTION 11

Which two are features of IPv6? (Choose two.)

A. anycast

B. broadcast

C. multicast

D. podcast

E. allcast

Correct Answer: AC

IPv6 addresses are classified by the primary addressing and routing methodologies common in networking: unicast addressing, anycast addressing, and multicast addressing. A unicast address identifies a single network interface. The Internet Protocol delivers packets sent to a unicast address to that specific interface.

An anycast address is assigned to a group of interfaces, usually belonging to different nodes. A packet sent to an anycast address is delivered to just one of the member interfaces, typically the nearest host, according to the routing

protocol\\'s definition of distance. Anycast addresses cannot be identified easily, they have the same format as unicast addresses, and differ only by their presence in the network at multiple points. Almost any unicast address can be employed as an anycast address. A multicast address is also used by multiple hosts, which acquire the multicast address destination by participating in the multicast distribution protocol among the network routers. A packet that is sent to a multicast address is delivered to

all interfaces that have joined the corresponding multicast group.

QUESTION 12

What are two benefits of using NAT? (Choose two.)

A. NAT facilitates end-to-end communication when IPsec is enabled.

B. NAT eliminates the need to re-address all hosts that require external access.

C. NAT conserves addresses through host MAC-level multiplexing.

D. Dynamic NAT facilitates connections from the outside of the network.

E. NAT accelerates the routing process because no modifications are made on the packets.

F. NAT protects network security because private networks are not advertised.

Correct Answer: BF

By not revealing the internal IP addresses, NAT adds some security to the inside network -> F is correct.

NAT has to modify the source IP addresses in the packets -> E is not correct.

Connection from the outside of the network through a "NAT" network is more difficult than a more network because IP addresses of inside hosts are hidden -> C is not correct.

In order for IPsec to work with NAT we need to allow additional protocols, including Internet Key Exchange (IKE), Encapsulating Security Payload (ESP) and Authentication Header (AH) -> more complex -> A is not correct.

By allocating specific public IP addresses to inside hosts, NAT eliminates the need to re-address the inside hosts -> B is correct.

NAT does conserve addresses but not through host MAC-level multiplexing. It conserves addresses by allowing many private IP addresses to use the same public IP address to go to the Internet -> C is not correct.

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: