Cisco

100-105 Exam

Interconnecting Cisco Networking Devices Part 1 (ICND)

Questions & Answers
Demo

Question No : 1

Which address type does a switch use to make selective forwarding decisions?

A. destination IP address
B. source MAC address
C. source IP address
D. source and destination IP address
E. destination MAC address

Answer: E

Explanation:
Switches analyze the destination MAC to make its forwarding decision since it is a layer 2 device.
Routers use the destination IP address to make forwarding decisions.

Question No : 2

In which two ways does TCP differ from UDP? (Choose two.)

A. TCP provides synchronized communication.
B. TCP segments are essentially datagrams.
C. TCP provides sequence numbering of packets.
D. TCP uses broadcast delivery.
E. TCP provides best effort delivery.

Answer: AC

Explanation:
TCP differs from UDP in the following ways: TCP provides best effort delivery.
TCP provides synchronized communication. TCP segments are essentially datagrams.
TCP provides sequence numbering of packets. TCP uses broadcast delivery.

Question No : 3

Under which circumstance should a network administrator implement one-way NAT?

A. when the network must route UDP traffic
B. when traffic that originates outside the network must be routed to internal hosts
C. when traffic that originates inside the network must be routed to internal hosts
D. when the network has few public IP addresses and many private IP addresses require outside access

Answer: D

Explanation:
NAT operation is typically transparent to both the internal and external hosts. Typically the internal host is aware of the true IP address and TCP or UDP port of the external host. Typically the NAT device may function as the default gateway for the internal host. However the external host is only aware of the public IP address for the

NAT device and the particular port being used to communicate on behalf of a specific internal host.
NAT and TCP/UDP

"Pure NAT", operating on IP alone, may or may not correctly parse protocols that are totally concerned with IP information, such as ICMP, depending on whether the payload is interpreted by a host on the "inside" or "outside" of translation. As soon as the protocol stack is traversed, even with such basic protocols as TCP and UDP, the protocols will break unless NAT takes action beyond the network layer. IP packets have a checksum in each packet header, which provides error detection only for the header. IP datagrams may become fragmented and it is necessary for a NAT to reassemble these fragments to allow correct recalculation of higher-level checksums and correct tracking of which packets belong to which connection. The major transport layer protocols, TCP and UDP, have a checksum that covers all the data they carry, as well as the TCP/UDP header, plus a "pseudo-header" that contains the source and destination IP addresses of the packet carrying the TCP/UDP header. For an originating NAT to pass TCP or UDP successfully, it must recompute the TCP/ UDP header checksum based on the translated IP addresses, not the original ones, and put that checksum into the TCP/UDP header of the first packet of the fragmented set of packets. The receiving NAT must recompute the IP checksum on every packet it passes to the destination host, and also recognize and recompute the TCP/ UDP header using the retranslated addresses and pseudo-header. This is not a completely solved problem.
One solution is for the receiving NAT to reassemble the entire segment and then recompute a checksum calculated across all packets.
The originating host may perform Maximum transmission unit (MTU) path discovery to determine the packet size that can be transmitted without fragmentation, and then set the don't fragment (DF) bit in the appropriate packet header field. Of course, this is only a one- way solution, because the responding host can send packets of any size, which may be fragmented before reaching the NAT.

Question No : 4

Which destination IP address can a host use to send one message to multiple devices across different subnets?

A. 172.20.1.0
B. 127.0.0.1
C. 192.168.0.119
D. 239.255.0.1

Answer: D

Explanation:
Multicast is a networking protocol where one host can send a message to a special multicast IP address and one or more network devices can listen for and receive those messages.
Multicast works by taking advantage of the existing IPv4 networking infrastructure, and it does so in something of a weird fashion. As you read, keep in mind that things are a little confusing because multicast was "shoe- horned" in to an existing technology. For the rest of this article, let's use the multicast IP address of 239.255.0.1.

Question No : 5

Which option must occur before a workstation can exchange HTTP packets with a web server?

A. An ICMP connection must be established between the workstation and the web server.
B. A UDP connection must be established between the workstation and its default gateway.
C. A TCP connection must be established between the workstation and its default gateway.
D. A UDP connection must be established between the workstation and the web server.
E. An ICMP connection must be established between the workstation and its default gateway.
F. A TCP connection must be established between the workstation and the web server.

Answer: F

Explanation:
HTTP uses TCP port 80.
http://pentestlab.wordpress.com/2012/03/05/common-tcpip-ports/

Question No : 6

Refer to the exhibit.

```
Router#configure terminal
Router(config) #vlan 10
Router(config-vlan) #do show vlan
```

Which statement describes the effect of this configuration?

A. The VLAN 10 VTP configuration is displayed.
B. The VLAN 10 spanning-tree output is displayed.
C. The VLAN 10 configuration is saved when the router exits VLAN configuration mode.
D. VLAN 10 is added to the VLAN database.

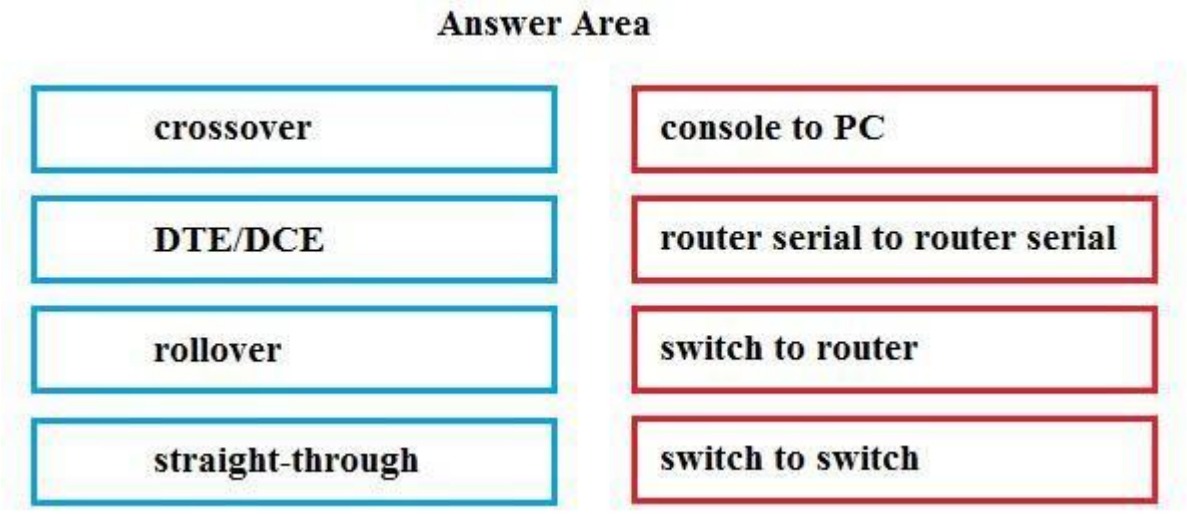
Answer: D

Explanation:
With the configuration above, when we type "do show vlan" we would not see VLAN 10 in the VLAN database because it has not been created yet. VLAN 10 is only created when we exits VLAN configuration mode (with "exit" command).

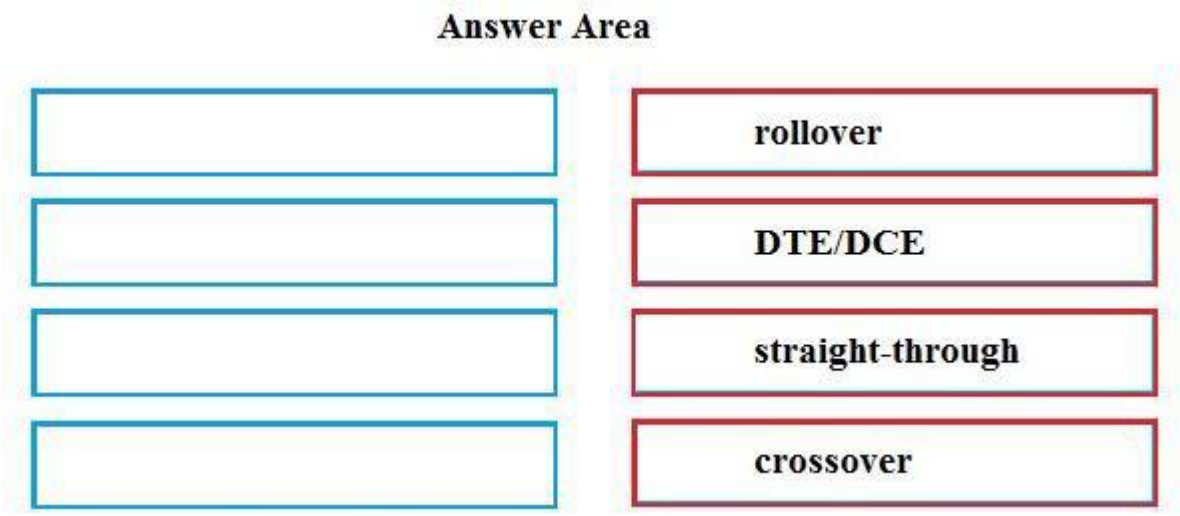
Question No : 7

DRAG DROP
Drag and drop each cable type from the left onto the type of connection for which it is best suited on the right.

Select and Place:



Correct Answer:



Question No : **8**

Which route source code represents the routing protocol with a default administrative distance of 90 in the routing table?

A. S
B. E
C. D
D. R
E. O

Answer: C

Explanation:
S Static
E EGP
D EIGRP
R RIP
O OSPF
Default Administrative distance of EIGRP protocol is 90 then answer is C.

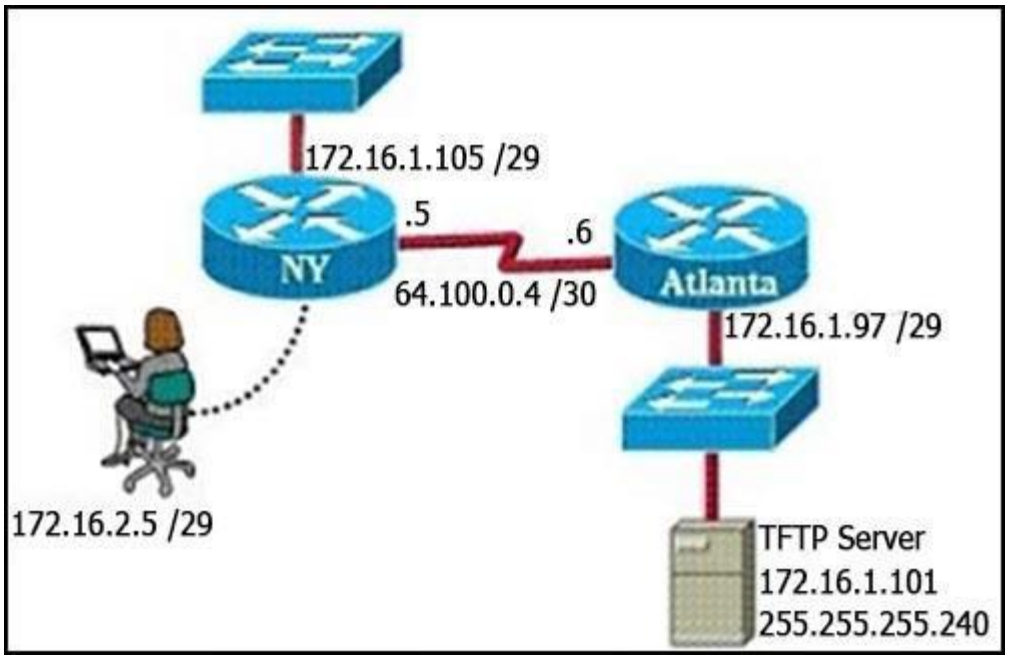
```
Router# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -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

Default Distance Value TableThis table lists the administrative distance default values of the protocols that Cisco supports:
Route Source
Default Distance Values
Connected interface
Static route

Enhanced Interior Gateway Routing Protocol (EIGRP) summary route External Border Gateway Protocol (BGP)
Internal EIGRP
IGRP
OSPF
Intermediate System-to-Intermediate System (IS-IS) Routing Information Protocol (RIP) Exterior Gateway Protocol (EGP)
On Demand Routing (ODR)
External EIGRP
Internal BGP
Unknown*

Question No : 9

Refer to the exhibit.



A TFTP server has recently been instated in the Atlanta office. The network administrator is located in the NY office and has made a console connection to the NY router. After establishing the connection they are unable to backup the configuration file and iOS of the NY router to the TFTP server. What is the cause of this problem?

A. The TFTP server has an incorrect subnet mask.
B. The TFTP server has an incorrect IP address.

C. The network administrator computer has an incorrect IP address.
D. The NY router has an incorrect subnet mask.

Answer: A

Explanation:
The subnet mask of the TFTP server needs to be in the same subnet as the default gateway.

Question No : 1 **0**

On a Cisco switch, which protocol determines if an attached VoIP phone is from Cisco or from another vendor?

A. CDP
B. RTP
C. UDP
D. TCP

Answer: A

Explanation:
The Cisco Unified IP Phone uses CDP to communicate information such as auxiliary VLAN ID, per port power management details, and Quality of Service (QoS) configuration information with the Cisco Catalyst switch.