Cisco

100-105

Cisco Interconnecting Cisco Networking Devices Part 1 (ICND1 v3.0)

Question: 1

By default, how many MAC addresses are permitted to be learned on a switch port with port security enabled?

A. 8
B. 2
C. 1
D. 0

Answer: C

Question: 2

Which dynamic routing protocol uses only the hop count to determine the best path to a destination?

A. IGRP
B. RIP
C. EIGRP
D. OSPF

Answer: B

Question: 3

Which feature allows a device to use a switch port that is configured for half-duplex to access the network?

A. CSMA/CD
B. IGMP
C. port security
D. split horizon

Answer: A

Explanation:
Ethernet began as a local area network technology that provided a half-duplex shared channel for stations connected to coaxial cable segments linked with signal repeaters. In this appendix, we take a detailed look at the half-duplex shared-channel mode of operation, and at the CSMA/CD mechanism that makes it work.

In the original half-duplex mode, the CSMA/CD protocol allows a set of stations to compete for access to a shared Ethernet channel in a fair and equitable manner. The protocol's rules determine the behavior of Ethernet stations, including when they are allowed to transmit a frame onto a shared Ethernet channel, and what to do when a collision occurs.
Today, virtually all devices are connected to Ethernet switch ports over full-duplex media, such as twisted-pair cables. On this type of connection, assuming that both devices can support the full-duplex mode of operation and that Auto-Negotiation (AN) is enabled, the AN protocol will automatically select the highest-performance mode of operation supported by the devices at each end of the link. That will result in full-duplex mode for the vast majority of Ethernet connections with modern interfaces that support full duplex and AN.

Question: 4

Which component of a routing table entry represents the subnet mask?

A. routing protocol code
B. prefix
C. metric
D. network mask

Answer: D

Explanation:
IP Routing Table Entry Types
An entry in the IP routing table contains the following information in the order presented:
Network ID. The network ID or destination corresponding to the route. The network ID can be class-based, subnet, or supernet network ID, or an IP address for a host route.
Network Mask. The mask that is used to match a destination IP address to the network ID.
Next Hop. The IP address of the next hop.
Interface. An indication of which network interface is used to forward the IP packet.
Metric. A number used to indicate the cost of the route so the best route among possible multiple routes to the same destination can be selected. A common use of the metric is to indicate the number of hops (routers crossed) to the network ID.
Routing table entries can be used to store the following types of routes:
Directly Attached Network IDs. Routes for network IDs that are directly attached. For directly attached networks, the Next Hop field can be blank or contain the IP address of the interface on that network.
Remote Network IDs. Routes for network IDs that are not directly attached but are available across other routers. For remote networks, the Next Hop field is the IP address of a local router in between the forwarding node and the remote network.
Host Routes. A route to a specific IP address. Host routes allow routing to occur on a per-IP address basis. For host routes, the network ID is the IP address of the specified host and the network mask is 255.255.255.255.
Default Route. The default route is designed to be used when a more specific network ID or host route is not found. The default route network ID is 0.0.0.0 with the network mask of 0.0.0.0.

Question: 5

Which technology supports the stateless assignment of IPv6 addresses?

A. DNS
B. DHCPv6
C. DHCP
D. autoconfiguration

Answer: B

Explanation:
DHCPv6 Technology Overview
IPv6 Internet Address Assignment Overview
IPv6 has been developed with Internet Address assignment dynamics in mind. Being aware that IPv6 Internet addresses are 128 bits in length and written in hexadecimals makes automation of address-assignment an important aspect within network design. These attributes make it inconvenient for a user to manually assign IPv6 addresses, as the format is not naturally intuitive to the human eye. To facilitate address assignment with little or no human intervention, several methods and technologies have been developed to automate the process of address and configuration parameter assignment to IPv6 hosts.
The various IPv6 address assignment methods are as follows:
1. Manual Assignment
An IPv6 address can be statically configured by a human operator. However, manual assignment is quite open to errors and operational overhead due to the 128 bit length and hexadecimal attributes of the addresses, although for router interfaces and static network elements and resources this can be an appropriate solution.
2. Stateless Address Autoconfiguration (RFC2462)
Stateless Address Autoconfiguration (SLAAC) is one of the most convenient methods to assign Internet addresses to IPv6 nodes. This method does not require any human intervention at all from an IPv6 user. If one wants to use IPv6 SLAAC on an IPv6 node, it is important that this IPv6 node is connected to a network with at least one IPv6 router connected. This router is configured by the network administrator and sends out Router Advertisement announcements onto the link. These announcements can allow the on-link connected IPv6 nodes to configure themselves with IPv6 address and routing parameters, as specified in RFC2462, without further human intervention.
3. Stateful DHCPv6
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) has been standardized by the IETF through RFC3315. DHCPv6 enables DHCP servers to pass configuration parameters, such as IPv6 network addresses, to IPv6 nodes. It offers the capability of automatic allocation of reusable network addresses and additional configuration flexibility. This protocol is a stateful counterpart to "IPv6 Stateless Address Autoconfiguration" (RFC 2462), and can be used separately, or in addition to the stateless autoconfiguration to obtain configuration parameters.
4. DHCPv6-PD
DHCPv6 Prefix Delegation (DHCPv6-PD) is an extension to DHCPv6, and is specified in RFC3633. Classical DHCPv6 is typically focused upon parameter assignment from a DHCPv6 server to an IPv6 host running a DHCPv6 protocol stack. A practical example would be the stateful address assignment of "2001:db8::1" from a DHCPv6 server to a DHCPv6 client. DHCPv6-PD however is aimed at assigning complete subnets and other network and interface parameters from a DHCPv6-PD server to a DHCPv6-PD client. This means that instead of a single address assignment, DHCPv6-PD will

assign a set of IPv6 "subnets". An example could be the assignment of "2001:db8::/60" from a DHCPv6-PD server to a DHCPv6-PD client. This will allow the DHCPv6-PD client (often a CPE device) to segment the received address IPv6 address space, and assign it dynamically to its IPv6 enabled interfaces.
5. Stateless DHCPv6
Stateless DHCPv6 is a combination of "stateless Address Autoconfiguration" and "Dynamic Host Configuration Protocol for IPv6" and is specified by RFC3736. When using stateless-DHCPv6, a device will use Stateless Address Auto-Configuration (SLAAC) to assign one or more IPv6 addresses to an interface, while it utilizes DHCPv6 to receive "additional parameters" which may not be available through SLAAC. For example, additional parameters could include information such as DNS or NTP server addresses, and are provided in a stateless manner by DHCPv6. Using stateless DHCPv6 means that the DHCPv6 server does not need to keep track of any state of assigned IPv6 addresses, and there is no need for state refreshment as result. On network media supporting a large number of hosts associated to a single DHCPv6 server, this could mean a significant reduction in DHCPv6 messages due to the reduced need for address state refreshments. From Cisco IOS 12.4(15)T onwards the client can also receive timing information, in addition to the "additional parameters" through DHCPv6. This timing information provides an indication to a host when it should refresh its DHCPv6 configuration data. This behavior (RFC4242) is particularly useful in unstable environments where changes are likely to occur.

Question: 6

When enabled, which feature prevents routing protocols from sending hello messages on an interface'?

A. virtual links
B. passive-interface
C. directed neighbors
D. OSPF areas

Answer: B

Explanation:
You can use the passive-interfacecommand in order to control the advertisement of routing information. The command enables the suppression of routing updates over some interfaces while it allows updates to be exchanged normally over other interfaces.
With most routing protocols, the passive-interface command restricts outgoing advertisements only. But, when used with Enhanced Interior Gateway Routing Protocol (EIGRP), the effect is slightly different. This document demonstrates that use of the passive-interface command in EIGRP suppresses the exchange of hello packets between two routers, which results in the loss of their neighbor relationship. This stops not only routing updates from being advertised, but it also suppresses incoming routing updates. This document also discusses the configuration required in order to allow the suppression of outgoing routing updates, while it also allows incoming routing updates to be learned normally from the neighbor.

Question: 7

Configuration of which option is required on a Cisco switch for the Cisco IP phone to work?

A. PortFast on the interface
B. the interface as an access port to allow the voice VLAN ID
C. a voice VLAN ID in interface and global configuration mode
D. Cisco Discovery Protocol in global configuration mode

Answer: B

Explanation:
When you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link.
In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi-VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.
The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. You can configure a voice VLAN with the "switchport voice vlan …" command under interface mode. The full configuration is shown below:

```
Switch(config)#interface fastethernet0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#switchport voice vlan 20
```

Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-4500-series-switches/69632-configuring-cat-ip-phone.html
Configure the Switch Port to Carry Both Voice and Data Traffic
When you connect an IP phone to a switch using a trunk link, it can cause high CPU utilization in the switches. As all the VLANs for a particular interface are trunked to the phone, it increases the number of STP instances the switch has to manage. This increases the CPU utilization. Trunking also causes unnecessary broadcast / multicast / unknown unicast traffic to hit the phone link.
In order to avoid this, remove the trunk configuration and keep the voice and access VLAN configured along with Quality of Service (QoS). Technically, it is still a trunk, but it is called a Multi-VLAN Access Port (MVAP). Because voice and data traffic can travel through the same port, you should specify a different VLAN for each type of traffic. You can configure a switch port to forward voice and data traffic on different VLANs. Configure IP phone ports with a voice VLAN configuration. This configuration creates a pseudo trunk, but does not require you to manually prune the unnecessary VLANs.
The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone. The voice VLAN feature is disabled by default. The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

Question: 8

Which statement about the inside interface configuration in a NAT deployment is true?

A. It is defined globally
B. It identifies the location of source addresses for outgoing packets to be translated using access or route maps.
C. It must be configured if static NAT is used
D. It identifies the public IP address that traffic will use to reach the internet.

Answer: B

Explanation:
This module describes how to configure Network Address Translation (NAT) for IP address conservation and how to configure inside and outside source addresses. This module also provides information about the benefits of configuring NAT for IP address conservation.
NAT enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address.
NAT is also used at the enterprise edge to allow internal users access to the Internet and to allow Internet access to internal devices such as mail servers.

Question: 9

Which of the following commands enables a network administrator to verify the application layer connectivity between source and destination?

A. ping
B. telnet
C. traceroute
D. verify
E. trace

Answer: B

Question: 10

WAN data link encapsulation types include which of the following? (Choose two.)

A. T1
B. Frame Relay
C. DSL

D. PPP
E. ISDN

Answer: B, D

Question: 11

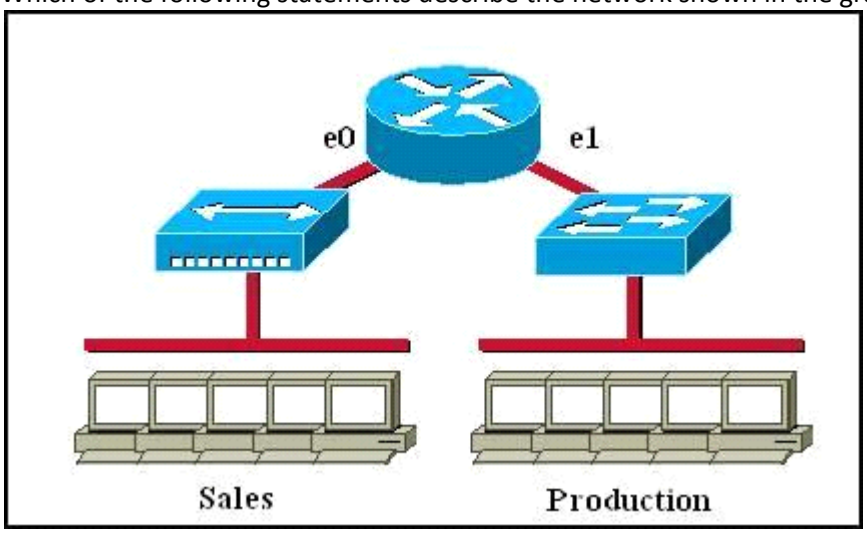
Which Layer 1 devices can be used to enlarge the area covered by a single LAN segment? (Choose two.)

A. switch
B. router
C. NIC
D. hub
E. repeater
F. RJ-45 transceiver

Answer: D, E

Question: 12

Which of the following statements describe the network shown in the graphic? (Choose two.)



A. There are two broadcast domains in the network.
B. There are four broadcast domains in the network.
C. There are six broadcast domains in the network.
D. There are four collision domains in the network.
E. There are five collision domains in the network.
F. There are seven collision domains in the network.

Answer: A, F

Question: 13

Assuming a subnet mask of 255.255.248.0, three of the following addresses are valid host addresses. Which are these addresses? (Choose three.)

A. 172.16.9.0
B. 172.16.8.0
C. 172.16.31.0
D. 172.16.20.0

Answer: A, C, D

Question: 14

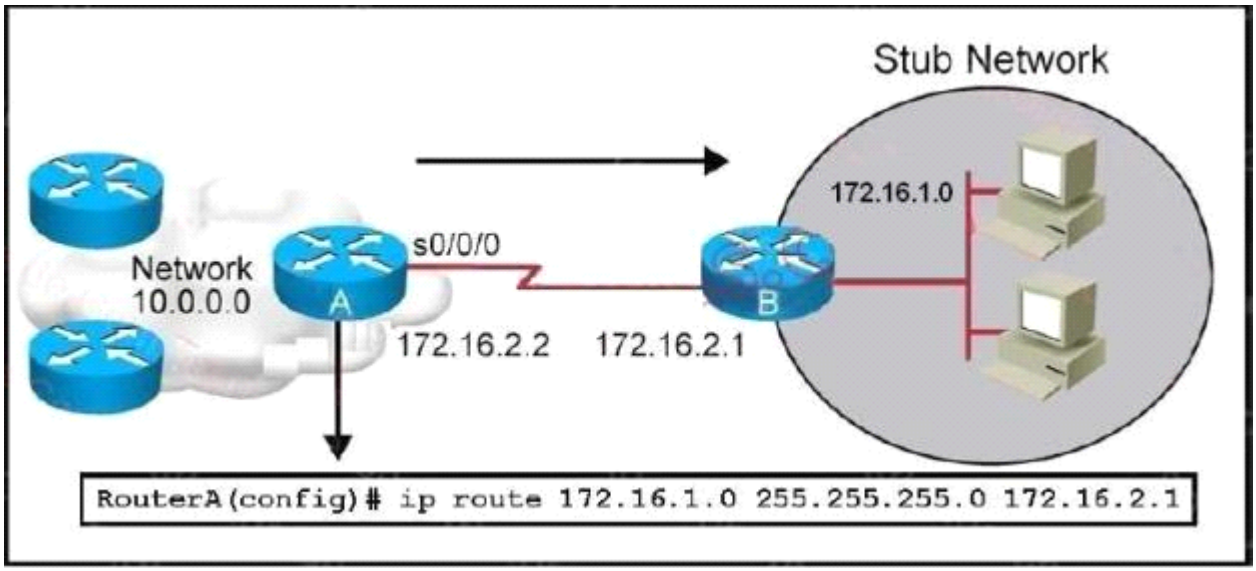
An administrator previously changed the encapsulation on a synchronous serial line and saved the configuration. Now the administrator wants to restore the encapsulation back to the default. What action can the administrator do to return the interface back to its default encapsulation?

A. Change the encapsulation to ARPA.
B. Configure the interface for HDLC encapsulation.
C. Reboot the router and allow it to reload the configuration.
D. Issue the shutdown then no shutdown commands to reset the encapsulation on the interface.
E. Remove the cable and plug it back in to allow the router to autonegotiate encapsulation settings.

Answer: B

Question: 15

Refer to the exhibit. Which statement is correct regarding the configuration shown?



A. This will not work as the subnet mask on serial interfaces must be /30.
B. What is shown as being configured would be considered a default route.
C. This configuration creates a bidirectional path between RouterA and RouterB.
D. The command ip route 172.16.1.0 255.255.255.0 s0/0/0 would provide similar routing functionality.

Answer: D

Question: 16

Refer to the exhibit. Which statement is correct regarding the results shown for the show interface s0/0/0 command?

```
RouterA# show interface s0/0/0
Serial0/0/0 is administratively down, line protocol is down
  Hardware is GT96K Serial
  Internet address is 10.12.12.1/28
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive set (10 sec)
  Last input never, output 00:00:14, output hang never
  Last clearing of "show interface" counters 5d15h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 81071
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     145 packets output, 5084 bytes, 0 underruns
     0 output errors, 0 collisions, 4 interface resets
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=down  DSR=up  DTR=down  RTS=down  CTS=down
```

A. The subnet mask for this interface is 255.255.255.248.
B. The subnet mask for this interface is 255.255.255.252.
C. The IP address that is configured on s0/0/0 is a public address.
D. This interface can be enabled by issuing a no shutdown command.
E. The default encapsulation protocol for a Cisco serial interface is PPP.

Answer: D

Question: 17

When troubleshooting a LAN interface operating in full duplex mode, which error condition can be immediately ruled out?

A. giants
B. no buffers
C. collisions
D. ignored
E. dribble condition

Answer: C

Question: 18

Which transport layer protocol is best suited for the transport of VoIP data?

A. RIP
B. UDP
C. TCP
D. OSPF
E. HTTP

Answer: B

Question: 19

Which statement describes the effect of the exec-timeout 30 command?

A. The router maintains a user session indefinitely after it is active for 30 seconds.
B. The router disconnects the user session if it is inactive for 30 minutes.
C. The router maintains a user session indefinitely after it is active for 30 minutes.
D. The router disconnects a user session if it is inactive for 30 seconds.

Answer: B

Question: 20

Which statement about the default switch configuration for remote access managements is true?

A. The system name is set to Cisco.
B. The Telnet password is set to cisco.
C. No default gateway is defined.
D. One IP address is preconfigured.

Answer: C

Thank You for Trying Our Product

For More Information – Visit link below:

20% Discount Coupon Code:
20off2018

https://www.examsboost.com/

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer