Cisco

200-105 Exam

Cisco Interconnecting Cisco Networking Devices Part 2 Exam

Version: 9.1

Question: 1

Which protocol authenticates connected devices before allowing them to access the LAN?

A. 802.1d
B. 802.11
C. 802.1w
D. 802.1x

Answer: D

Explanation:
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.
The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

Question: 2

What is a difference between TACACS+ and RADIUS in AAA?

A. Only TACACS+ allows for separate authentication.
B. Only RADIUS encrypts the entire access-request packet.
C. Only RADIUS uses TCP.
D. Only TACACS+ couples authentication and authorization.

Answer: A

Explanation:
Authentication and Authorization
RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

Question: 3

Which statement about the IP SLAs ICMP Echo operation is true?

A. The frequency of the operation .s specified in milliseconds.
B. It is used to identify the best source interface from which to send traffic.
C. It is configured in enable mode.
D. It is used to determine the frequency of ICMP packets.

Answer: D

Explanation:
This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. ICMP Echo is useful for troubleshooting network connectivity issues. This module also demonstrates how the results of the ICMP Echo operation can be displayed and analyzed to determine how the network IP connections are performing.
ICMP Echo Operation
The ICMP Echo operation measures end-to-end response time between a Cisco router and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP Echo request message to the destination and receiving an ICMP Echo reply.
In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements.
Figure 1. ICMP Echo Operation
The IP SLAs ICMP Echo operation conforms to the same IETF specifications for ICMP ping testing and the two methods result in the same response times.
Configuring a Basic ICMP Echo Operation on the Source Device
SUMMARY STEPS

1. enable
2. configure terminal

3. ip sla operation-number
4. icmp-echo {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name]
5. frequency seconds
6. end

Question: 4

Which type of interface can negotiate an IP address for a PPPoE client?

A. Ethernet
B. dialer
C. serial
D. Frame Relay

Answer: B

Question: 5

Which option is a benefit of switch stacking?

A. It provides redundancy with no impact on resource usage.
B. It simplifies adding and removing hosts.
C. It supports better performance of high-needs applications.
D. It provides higher port density with better resource usage.

Answer: D

Explanation:
A stackable switch is a network switch that is fully functional operating standalone but which can also be set up to operate together with one or more other network switches, with this group of switches showing the characteristics of a single switch but having the port capacity of the sum of the combined switches.

Question: 6

What is the first step you perform to configure an SNMPv3 user?

A. Configure server traps.
B. Configure the server group.
C. Configure the server host.
D. Configure the remote engine ID.

Answer: B

Explanation:
The first task in configuring SNMPv3 is to define a view. To simplify things, we'll create a view that allows access to the entire internet subtree:

```
router(config)#snmp-server view readview internet included
```

This command creates a view called readview. If you want to limit the view to the system tree, for example, replace internet with system. The included keyword states that the specified tree should be included in the view; use excluded if you wanted to exclude a certain subtree.
Next, create a group that uses the new view. The following command creates a group called readonly ; v3 means that SNMPv3 should be used. The auth keyword specifies that the entity should authenticate packets without encrypting them; read readview says that the view named readview should be used whenever members of the readonly group access the router.

```
router(config)#snmp-server group readonly v3 auth read readview
```

Question: 7

Which spanning-tree feature places a port immediately into a forwarding stated?

A. BPDU guard
B. PortFast
C. loop guard
D. UDLD
E. Uplink Fast

Answer: B

Explanation:
PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch or trunk ports that are connected to a single workstation, switch, or server to allow those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state.

Question: 8

How can you disable DTP on a switch port?

A. Configure the switch port as a trunk.
B. Add an interface on the switch to a channel group.
C. Change the operational mode to static access.
D. Change the administrative mode to access.

Answer: D

Question: 9

If host Z needs to send data through router R1 to a storage server, which destination MAC address does host Z use to transmit packets?

A. the host Z MAC address
B. the MAC address of the interface on R1 that connects to the storage server
C. the MAC address of the interface on R1 that connects to host Z
D. the MAC address of the storage server interface

Answer: C

Question: 10

Which Cisco platform can verify ACLs?

A. Cisco Prime Infrastructure
B. Cisco Wireless LAN Controller
C. Cisco APIC-EM
D. Cisco IOS-XE

Answer: C

Question: 11

Which statement about QoS default behavior is true?

A. Ports are untrusted by default.
B. VoIP traffic is passed without being tagged.
C. Video traffic is passed with a well-known DSCP value of 46.
D. Packets are classified internally with an environment.
E. Packets that arrive with a tag are untagged at the edge of an administrative domain.

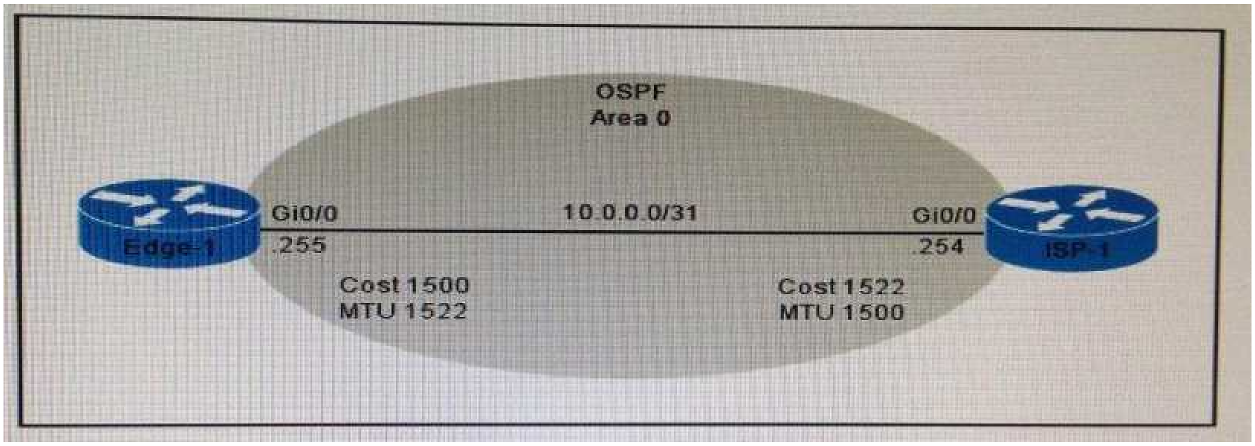
Answer: E

Explanation:
Frames received from users in the administratively-defined VLANs are classified or tagged for transmission to other devices. Based on rules that you define, a unique identifier (the tag) is inserted in each frame header before it is forwarded. The tag is examined and understood by each device before any broadcasts or transmissions to other switches, routers, or end stations. When the frame reaches the last switch or router, the tag is removed before the frame is sent to the target end station. VLANs that are

assigned on trunk or access ports without identification or a tag are called native or untagged frames. For IEEE 802.1Q frames with tag information, the priority value from the header frame is used. For native frames, the default priority of the input port is used.
Each port on the switch has a single receive queue buffer (the ingress port) for incoming traffic. When an untagged frame arrives, it is assigned the value of the port as its port default priority. You assign this value by using the CLI or CMS. A tagged frame continues to use its assigned CoS value when it passes through the ingress port.

Question: 12

Refer to the exhibit.



Router edge-1 is unable to establish OSPF neighbor adjacency with router ISP-1. Which two configuration changes can you make on edge-1 to allow the two routers to establish adjacency? (Choose two.)

A. Set the subnet mask on edge-1 to 255 255.255.252.
B. Reduce the MTU on edge-1 to 1514.
C. Set the OSPF cost on edge-1 to 1522.
D. Reduce the MTU on edge-1 to 1500.
E. Configure the ip ospf mtu-ignore command on the edge-1 Gi0/0 interface.

Answer: D, E

Explanation:
A situation can occur where the interface MTU is at a high value, for example 9000, while the real value of the size of packets that can be forwarded over this interface is 1500.
If there is a mismatch on MTU on both sides of the link where OSPF runs, then the OSPF adjacency will not form because the MTU value is carried in the Database Description (DBD) packets and checked on the other side.

Question: 13

Which statement about MPLS is true?

A. It operates in Layer 1.
B. It operates between Layer 2 and Layer 3.
C. It operates in Layer 3.
D. it operates in Layer 2.

Answer: B

Explanation:
MPLS belongs to the family of packet-switched networks. MPLS operates at a layer that is generally considered to lie between traditional definitions of OSI Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a layer 2.5 protocol.

Question: 14

Which statement about named ACLs is true?

A. They support standard and extended ACLs.
B. They are used to filter usernames and passwords for Telnet and SSH.
C. They are used to filter Layer 7 traffic.
D. They support standard ACLs only.
E. They are used to rate limit traffic destined to targeted networks.

Answer: A

Explanation:
Named Access Control Lists (ACLs) allows standard and extended ACLs to be given names instead of numbers. Unlike in numbered Access Control Lists (ACLs), we can edit Named Access Control Lists. Another benefit of using named access configuration mode is that you can add new statements to the access list, and insert them wherever you like. With the legacy syntax, you must delete the entire access list before reapplying it using the updated rules.

Question: 15

Which two switch states are valid for 802.1w? (Choose two.)

A. listening
B. backup
C. disabled
D. learning
E. discarding

Answer: D, E

Explanation:
Port States
There are only three port states left in RSTP that correspond to the three possible operational states. The

802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

Question: 16

Which option is the benefit of implementing an intelligent DNS for a cloud computing solution?

A. It reduces the need for a backup data center.
B. It can redirect user requests to locations that are using fewer network resources.
C. It enables the ISP to maintain DNS records automatically.
D. It eliminates the need for a GSS.

Answer: B

Question: 17

Which identification number is valid for an extended ACL?

A. 1
B. 64
C. 99
D. 100
E. 299
F. 1099

Answer: D

Question: 18

Which two pieces of information are provided by the show controllers serial 0 command? (Choose two.)

A. the type of cable that is connected to the interface.
B. The uptime of the interface
C. the status of the physical layer of the interface
D. the full configuration of the interface
E. the interface's duplex settings

Answer: A, C

Explanation:
The show controller command provides hardware-related information useful to troubleshoot and diagnose issues with Cisco router interfaces. The Cisco 12000 Series uses a distributed architecture with a central command-line interface (CLI) at the Gigabit Route Processor (GRP) and a local CLI at each line card.

Question: 19

Which three options are the HSRP states for a router? (Choose three.)

A. initialize
B. learn
C. secondary
D. listen
E. speak
F. primary

Answer: B, D, E

Explanation:
HSRP States

Question: 20

While you were troubleshooting a connection issue, a ping from one VLAN to another VLAN on the same switch failed. Which command verifies that IP routing is enabled on interfaces and the local VLANs are up?

A. show ip interface brief
B. show ip nat statistics
C. show ip statistics
D. show ip route

Answer: A

Explanation:
Initiate a ping from an end device in one VLAN to the interface VLAN on another VLAN in order to verify that the switch routes between VLANs. In this example, ping from VLAN 2 (10.1.2.1) to Interface VLAN 3 (10.1.3.1) or Interface VLAN 10 (10.1.10.1). If the ping fails, verify that IP routing is enabled and that the VLAN interfaces status is up with the show ip interface brief command.