KillTest

質量更高　服務更好

練習題

https://www.killtest.net

一年免費更新服務

Exam : **200-105**

Title : Interconnecting Cisco Networking Devices Part 2 (ICND2 v3.0)

Version : DEMO

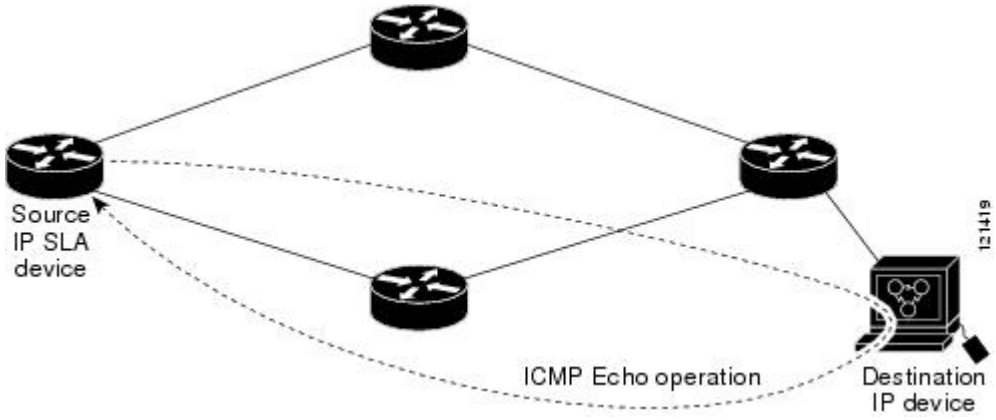
1. Topic 1, New Set Questions

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.

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.

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

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

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.