[Updated Constantly]

HERE

CCNA 4 (v5.0.3 + v6.0) Chapter 5 Exam Answers Full

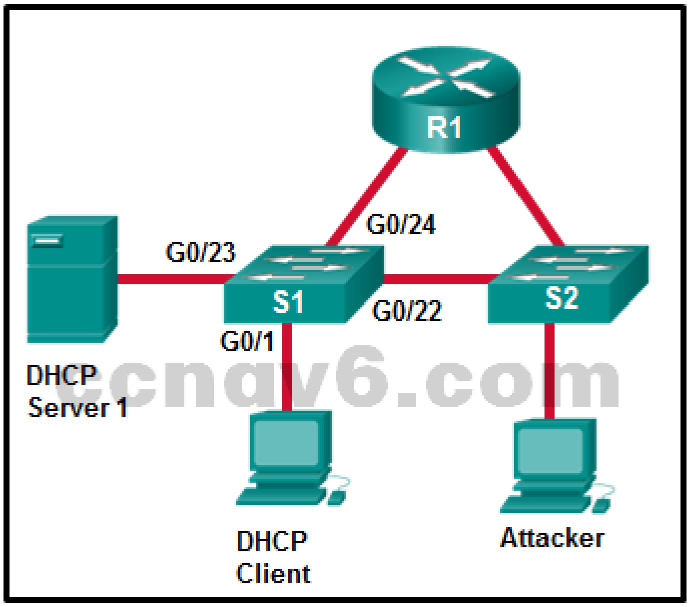
1. **What is the behavior of a switch as a result of a successful CAM table attack?**
   - The switch will drop all received frames.
   - The switch interfaces will transition to the error-disabled state.
   - **The switch will forward all received frames to all other ports.***
   - The switch will shut down.

   As a result of a CAM table attack, a switch can run out of memory resources to store MAC addresses. When this happens, no new MAC addresses can be added to the CAM table and the switch will forward all received frames to all other ports. This would allow an attacker to capture all traffic that is flooded by the switch.

2. **What network attack seeks to create a DoS for clients by preventing them from being able to obtain a DHCP lease?**
   - **DHCP starvation***
   - CAM table attack
   - IP address spoofing
   - DHCP spoofing

   DCHP starvation attacks are launched by an attacker with the intent to create a DoS for DHCP clients. To accomplish this goal, the attacker uses a tool that sends many DHCPDISCOVER messages in order to lease the entire pool of available IP addresses, thus denying them to legitimate hosts.

3. **The exhibit shows a network consisting of a router, two switches, a DHCP client host, an attacker host, and a DHCP server. Switch S1 shows four interface connections: G0/1 to the DHCP client, G0/22 to switch S2, G0/24 to router R1, and G0/23 to the DHCP server. The attacker host is connected to switch S2.Refer to the exhibit. Which interface on switch S1 should be configured as a DHCP snooping trusted port to help mitigate DHCP spoofing attacks?**



- G0/1
- G0/24
- G0/22
- **G0/23***

When DHCP snooping is configured, the interface that connects to the DHCP server is configured as a trusted port. Trusted ports can source DHCP requests and acknowledgments. All ports not specifically configured as trusted are considered untrusted by the switch and can only source DHCP requests.

4. **When using 802.1X authentication, what device controls physical access to the network, based on the authentication status of the client?**
- **the switch that the client is connected to***
- the router that is serving as the default gateway
- the authentication server
- the supplicant

The devices involved in the 802.1X authentication process are as follows:
The supplicant, which is the client that is requesting network access
The authenticator, which is the switch that the client is connecting and that is actually controlling physical network access
The authentication server, which performs the actual authentication

5. **What device is considered a supplicant during the 802.1X authentication process?**
- the router that is serving as the default gateway
- **the client that is requesting authentication***
- the authentication server that is performing client authentication
- the switch that is controlling network access

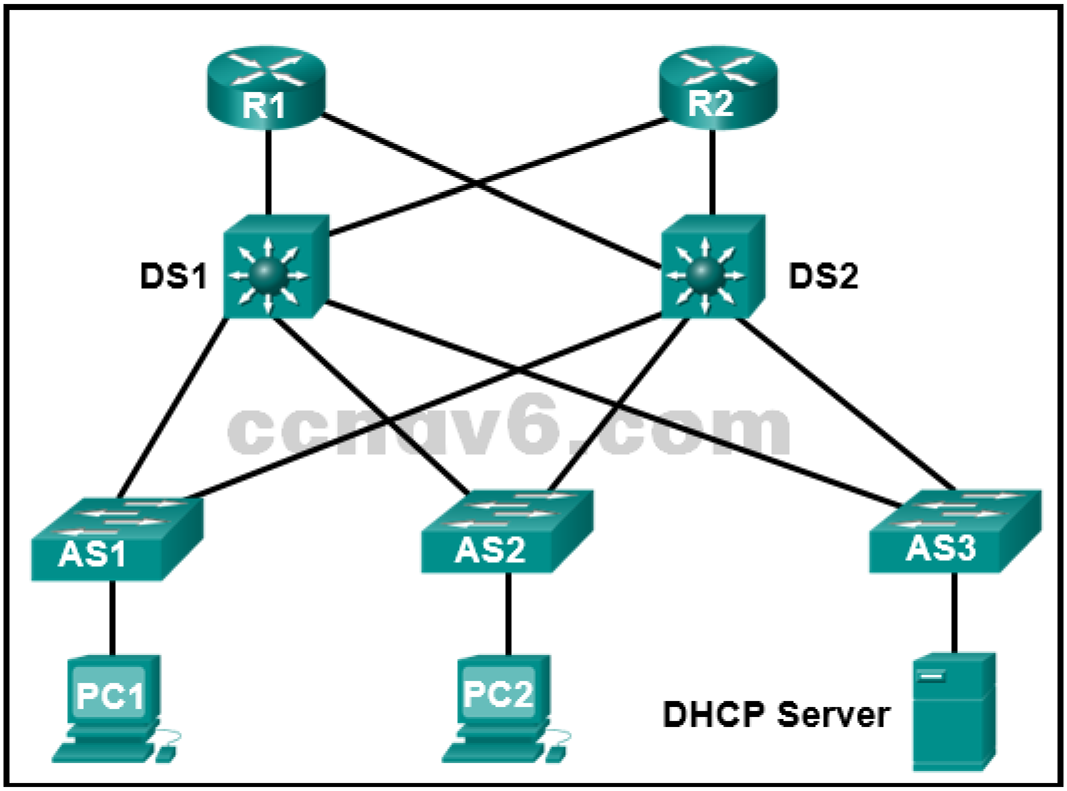
The devices involved in the 802.1X authentication process are as follows:
The supplicant, which is the client that is requesting network access
The authenticator, which is the switch that the client is connecting to and that is actually

controlling physical network access
The authentication server, which performs the actual authentication

6. **What is a drawback of the local database method of securing device access that can be solved by using AAA with centralized servers?**
   - There is no ability to provide accountability.
   - **User accounts must be configured locally on each device, which is an unscalable authentication solution.***
   - It is very susceptible to brute-force attacks because there is no username.
   - The passwords can only be stored in plain text in the running configuration.

The local database method of securing device access utilizes usernames and passwords that are configured locally on the router. This allows administrators to keep track of who logged in to the device and when. The passwords can also be encrypted in the configuration. However, the account information must be configured on each device where that account should have access, making this solution very difficult to scale.

7. **The exhibit shows a network topology. On the top, there are two routers, labeled R1 and R2. Under the two routers, there are two Layer 3 switches, labeled DS1 and DS2, . Under DS1 and DS2, there are three Layer 2 switches, labeled AS1, AS2, and AS3. Both R1 and R2 have two connections, one to DS1 and another to DS2. DS1 and DS2 each has three connections, one to AS1, one to AS2, and one to AS3. PC1 is connected on switch AS1 and PC2 is connected to switch AS2. There is a DHCP server connected on switch AS3.Refer to the exhibit. PC1 and PC2 should be able to obtain IP address assignments from the DHCP server. How many ports among switches should be assigned as trusted ports as part of the DHCP snooping configuration?**



- 1

- 3
- 5
- **7***

The DHCP snooping configuration includes building the DHCP Snooping Binding Database and assigning necessary trusted ports on switches. A trusted port points to the legitimate DHCP servers. In this network design, because the DHCP server is attached to AS3, seven switch ports should be assigned as trusted ports, one on AS3 toward the DHCP server, one on DS1 toward AS3, one on DS2 toward AS3, and two connections on both AS1 and AS2 (toward DS1 and DS2), for a total of seven.

8. **What protocol is used to encapsulate the EAP data between the authenticator and authentication server performing 802.1X authentication?**

- TACACS+
- SSH
- **RADIUS***
- MD5

Encapsulation of EAP data between the authenticator and the authentication server is performed using RADIUS.

9. **Which two protocols are used to provide server-based AAA authentication? (Choose two.)**

- SNMP
- **RADIUS***
- SSH
- 802.1x
- **TACACS+***

Server-based AAA authentication uses an external TACACS or RADIUS authentication server to maintain a username and password database. When a client establishes a connection with an AAA enabled device, the device authenticates the client by querying the authentication servers.

10. **Which protocol defines port-based authentication to restrict unauthorized hosts from connecting to the LAN through publicly accessible switch ports?**

- RADIUS
- TACACS+
- **802.1x***
- SSH

802.1x is an IEEE standard that defines port-based access control. By authenticating each client that attempts to connect to the LAN, 802.1x provides protection from unauthorized clients.

11. **What are three techniques for mitigating VLAN attacks? (Choose three.)**

- Use private VLANs.
- Enable BPDU guard.
- **Enable trunking manually.***
- Enable Source Guard.
- **Disable DTP.***
- **Set the native VLAN to an unused VLAN.***

Mitigating a VLAN attack can be done by disabling Dynamic Trunking Protocol (DTP), manually setting ports to trunking mode, and by setting the native VLAN of trunk links to VLANs not in use.

12. **Which statement describes SNMP operation?**
    - **A set request is used by the NMS to change configuration variables in the agent device.***
    - An NMS periodically polls the SNMP agents that are residing on managed devices by using traps to query the devices for data.
    - A get request is used by the SNMP agent to query the device for data.
    - An SNMP agent that resides on a managed device collects information about the device and stores that information remotely in the MIB that is located on the NMS.

An SNMP agent that resides on a managed device collects and stores information about the device and its operation. This information is stored by the agent locally in the MIB. An NMS periodically polls the SNMP agents that are residing on managed devices by using the get request to query the devices for data.

13. **A network administrator is analyzing the features supported by the multiple versions of SNMP. What are two features that are supported by SNMPv3 but not by SNMPv1 or SNMPv2c? (Choose two.)**
    - **message encryption***
    - community-based security
    - SNMP trap mechanism
    - **message source validation***
    - bulk retrieval of MIB information

SNMPv3 provides message integrity to ensure that a packet was not tampered with and authentication to determine if the message is from a valid source. SNMPv3 also supports message encryption. SNMPv1 and SNMPv2 do not support message encryption, but do support community strings. SNMPv2c supports bulk retrieval operation. All SNMP versions support the SNMP trap mechanism.

14. **Which protocol or service can be configured to send unsolicited messages to alert the network administrator about a network event such as an extremely high CPU utilization on a router?**
    - NetFlow
    - syslog
    - NTP
    - **SNMP***

SNMP can be used to collect and store information such as device CPU utilization. Syslog is used to access and store system messages. Cisco developed NetFlow for the purpose of gathering statistics on packets that are flowing through Cisco routers and multilayer switches. NTP is used to allow network devices to synchronize time settings.

15. **What is the function of the MIB element as part of a network management system?**
    - to collect data from SNMP agents
    - to change configurations on SNMP agents
    - to send and retrieve network management information
    - **to store data about a device***

The Management Information Base (MIB) resides on a networking device and stores operational data about the device. The SNMP manager can collect information from SNMP agents. The SNMP agent provides access to the information.

16. **Which SNMP version uses weak community string-based access control and supports bulk retrieval?**
    - SNMPv3
    - SNMPv2Classic
    - **SNMPv2c***
    - SNMPv1

    Both SNMPv1 and SNMPv2c use a community-based form of security, and community strings are plaintext passwords. Plaintext passwords are not considered a strong security mechanism. Version 1 is a legacy solution and not often encountered in networks today.

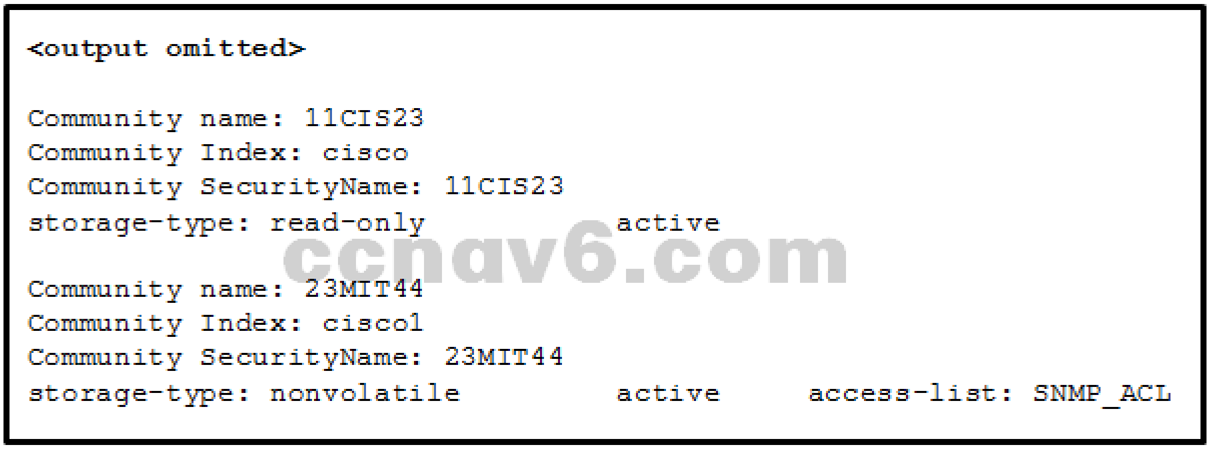
17. **What are SNMP trap messages?**
    - **unsolicited messages that are sent by the SNMP agent and alert the NMS to a condition on the network***
    - messages that are used by the NMS to change configuration variables in the agent device
    - messages that are sent periodically by the NMS to the SNMP agents that reside on managed devices to query the device for data
    - messages that are used by the NMS to query the device for data

    A GET request is a message that is used by the NMS to query the device for data. A SET request is a message that is used by the NMS to change configuration variables in the agent device. An NMS periodically polls the SNMP agents residing on managed devices, by querying the device for data by using the GET request.

18. **A network administrator issues two commands on a router:**
    R1(config)# snmp-server host 10.10.50.25 version 2c campus
    R1(config)# snmp-server enable trapsWhat can be concluded after the commands are entered?
    - No traps are sent, because the notification-types argument was not specified yet.
    - Traps are sent with the source IP address as 10.10.50.25.
    - **If an interface comes up, a trap is sent to the server.***
    - The snmp-server enable traps command needs to be used repeatedly if a particular subset of trap types is desired.

    The snmp-server enable traps command enables SNMP to send trap messages to the NMS at 10.10.50.25. This notification-types argument can be used to specify what specific type of trap is sent. If this argument is not used, then all trap types are sent. If the notification-types argument is used, then repeated use of this command is required if another subset of trap types is desired.

19. **Refer to the exhibit. What can be concluded from the produced output?**

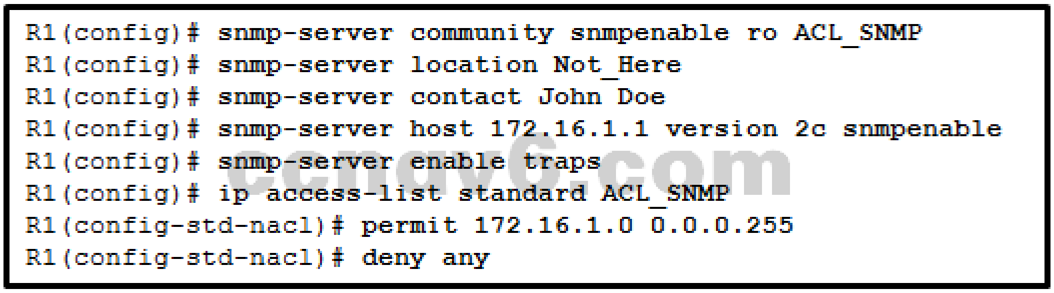


```
<output omitted>

Community name: 11CIS23
Community Index: cisco
Community SecurityName: 11CIS23
storage-type: read-only            active

Community name: 23MIT44
Community Index: cisco1
Community SecurityName: 23MIT44
storage-type: nonvolatile          active      access-list: SNMP_ACL
```

- The system contact was not configured with the snmp-server contact command.
- The location of the device was not configured with the snmp-server location command.
- This is the output of the show snmp command without any parameters.
- **An ACL was configured to restrict SNMP access to an SNMP manager.***

The output is produced in response to the show snmp community command. It displays the community string and any ACLs that may be configured. The show snmp command without any keyword does not display information relating to the SNMP community string or, if applicable, the associated ACL. Because the show snmp community command does not display the contact or location information, whether they are configured or not cannot be concluded.

20. **Refer to the exhibit. A SNMP manager has IP address 172.16.1.120. The SNMP manager is unable to change configuration variables on the R1 SNMP agent. What could be the problem?**

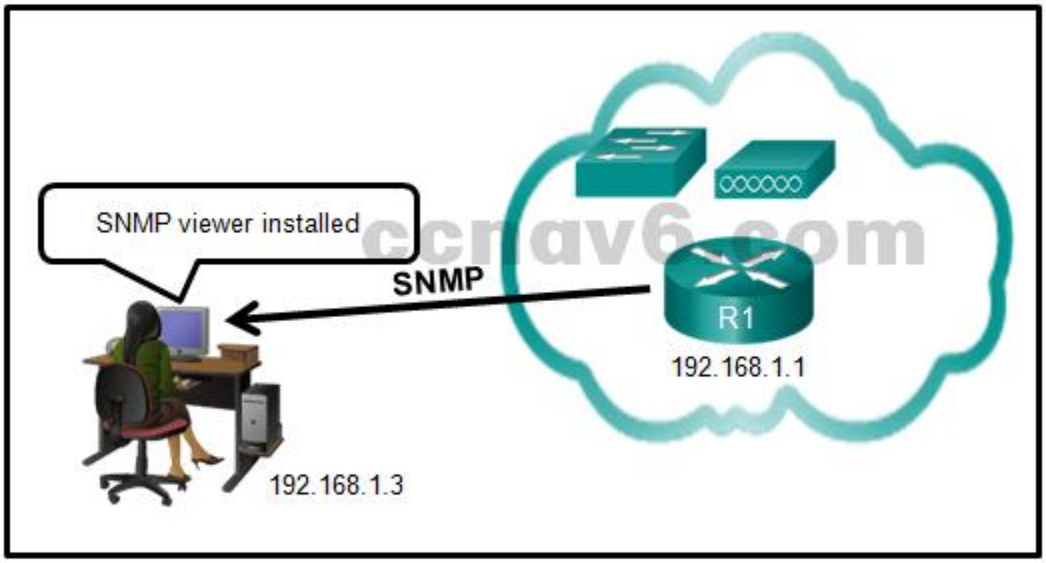


```
R1(config)# snmp-server community snmpenable ro ACL_SNMP
R1(config)# snmp-server location Not_Here
R1(config)# snmp-server contact John Doe
R1(config)# snmp-server host 172.16.1.1 version 2c snmpenable
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard ACL_SNMP
R1(config-std-nacl)# permit 172.16.1.0 0.0.0.255
R1(config-std-nacl)# deny any
```

- The ACL of ACL_SNMP has not been implemented on an interface yet.
- The SNMP agent should have traps disabled.
- The IP address of the SNMP manager must be 172.16.1.1.
- **The SNMP agent is not configured for write access.***

Because the SNMP manager is able to access the SNMP agent, the problem is not related to the ACL configuration. The SNMP agent configuration should have an access level configured of rw to support the SNMP manager set requests. The SNMP manager cannot change configuration variables on the SNMP agent R1 with only ro access. The IP address of the SNMP manager does not have to be 172.16.1.1 to make changes to the SNMP agent. The SNMP agent does not have to have traps disabled.

21. **Refer to the exhibit. Router R1 was configured by a network administrator to use SNMP version 2. The following commands were issued:**



R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.10.3

Why is the administrator not able to get any information from R1?

- The snmp-server enable traps command is missing.
- **There is a problem with the ACL configuration.***
- The snmp-server community command needs to include the rw keyword.
- The snmp-server location command is missing.

The permit statement with the incorrect IP address is the reason why the administrator is not able to access router R1. The correct statement should be permit 192.168.1.3. The snmp-server location and snmp-server enable traps commands are optional commands and have no relation to the access restriction to router R1. The rw keyword does not need to be included in this case because the administrator just wants to obtain information, not change any configuration.

22. **A network administrator has issued the snmp-server user admin1 admin v3 encrypted auth md5 abc789 priv des 256 key99 command. What are two features of this command? (Choose two.)**

- It restricts SNMP access to defined SNMP managers.
- It allows a network administrator to configure a secret encrypted password on the SNMP server.
- **It uses the MD5 authentication of the SNMP messages.***
- **It adds a new user to the SNMP group.***
- It forces the network manager to log into the agent to retrieve the SNMP messages.

The command snmp-server user admin1 admin v3 encrypted auth md5 abc789 priv des 256 key99 creates a new user and configures authentication with MD5. The command does not use a secret encrypted password on the server. The command snmp-server community string access-list-number-or-name restricts SNMP access to defined SNMP managers.

23. **Which statement describes the RSPAN VLAN?**

- The RSPAN VLAN can be used to carry secure traffic between switches.
- **The RSPAN VLAN must be the same on both the source and destination switch.***
- The RSPAN VLAN must be the same as the native VLAN.
- The RSPAN VLAN can be used for remote management of network switches.

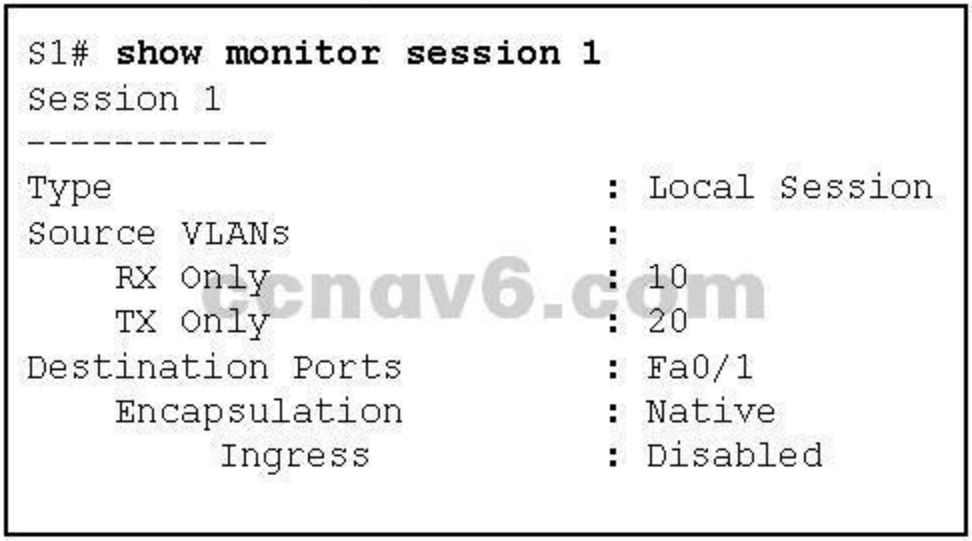
Remote SPAN (RSPAN) allows source and destination ports to be in different switches. RSPAN uses two sessions. One session is used as the source and one session is used to copy or receive the traffic from a VLAN. The traffic for each RSPAN session is carried over trunk links in a user-specified RSPAN VLAN that is dedicated (for that RSPAN session) in all participating switches.

24. **Which statement describes the function of the SPAN tool used in a Cisco switch?**

- It is a secure channel for a switch to send logging to a syslog server.
- It supports the SNMP trap operation on a switch.
- It provides interconnection between VLANs over multiple switches.
- **It copies the traffic from one switch port and sends it to another switch port that is connected to a monitoring device.***

To analyze network traffic passing through a switch, switched port analyzer (SPAN) can be used. SPAN can send a copy of traffic from one port to another port on the same switch where a network analyzer or monitoring device is connected. SPAN is not required for syslog or SNMP. SPAN is used to mirror traffic, while syslog and SNMP are configured to send data directly to the appropriate server.

25. **Refer to the exhibit. Based on the output generated by the show monitor session 1 command, how will SPAN operate on the switch?**



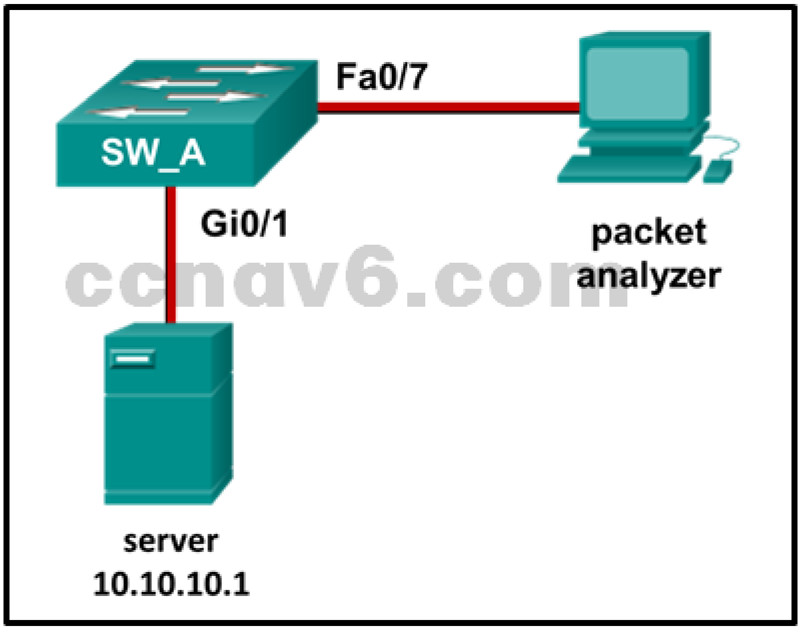
```
S1# show monitor session 1
Session 1
-----------
Type                          : Local Session
Source VLANs                  :
    RX Only                   : 10
    TX Only                   : 20
Destination Ports             : Fa0/1
    Encapsulation             : Native
         Ingress              : Disabled
```

- **All traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.***
- All traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic transmitted from VLAN 10 or received on VLAN 20 is forwarded to FastEthernet 0/1.
- Native VLAN traffic received on VLAN 10 or transmitted from VLAN 20 is forwarded to FastEthernet 0/1.

- The show monitor session command is used to verify how SPAN is configured (what ports are involved in the traffic mirroring).

A server (10.10.10.1) connects to Gi0/1 on switch SW_A. A packet analyzer is connected to port Fa0/7 of SW_A.

26. **Refer to the exhibit. Which command or set of commands will configure SW_A to copy all traffic for the server to the packet analyzer?**



- Sw_A(config)# monitor session 1 destination interface gi0/1
  Sw_A(config)# monitor session 1 source interface fa0/1
- **Sw_A(config)# monitor session 5 source interface gi0/1**
  Sw_A(config)# monitor session 5 destination interface fa0/7*
- Sw_A(config)# monitor session 1 destination interface fa0/7
  Sw_A(config)# monitor session 1 source interface fa0/7
- Sw_A(config)# monitor session 5 source interface gi0/1
  Sw_A(config)# monitor session 6 destination interface fa0/7

The local SPAN configuration requires two statements to identify the source and destination ports for the mirrored traffic. The statements must use the same session number. In this example, the source port is the port connected to the server (Gi0/1) and the destination port is the port attached to the packet analyzer (Fa0/7).