200-101 Q&As

Interconnecting Cisco Networking Devices Part 2 (ICND2)

Pass Cisco 200-101 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/200-101.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

What are three reasons to collect Netflow data on a company network? (Choose three.)

A. To identify applications causing congestion

B. To authorize user network access

C. To report and alert link up / down instances

D. To diagnose slow network performance, bandwidth hogs, and bandwidth utilization

E. To detect suboptimal routing in the network

F. To confirm the appropriate amount of bandwidth that has been allocated to each Class of Service

Correct Answer: ADF

QUESTION 2

Refer to the exhibit.

Which WAN protocol is being used?

A. ATM

B. HDLC

C. Frame Relay

D. PPP

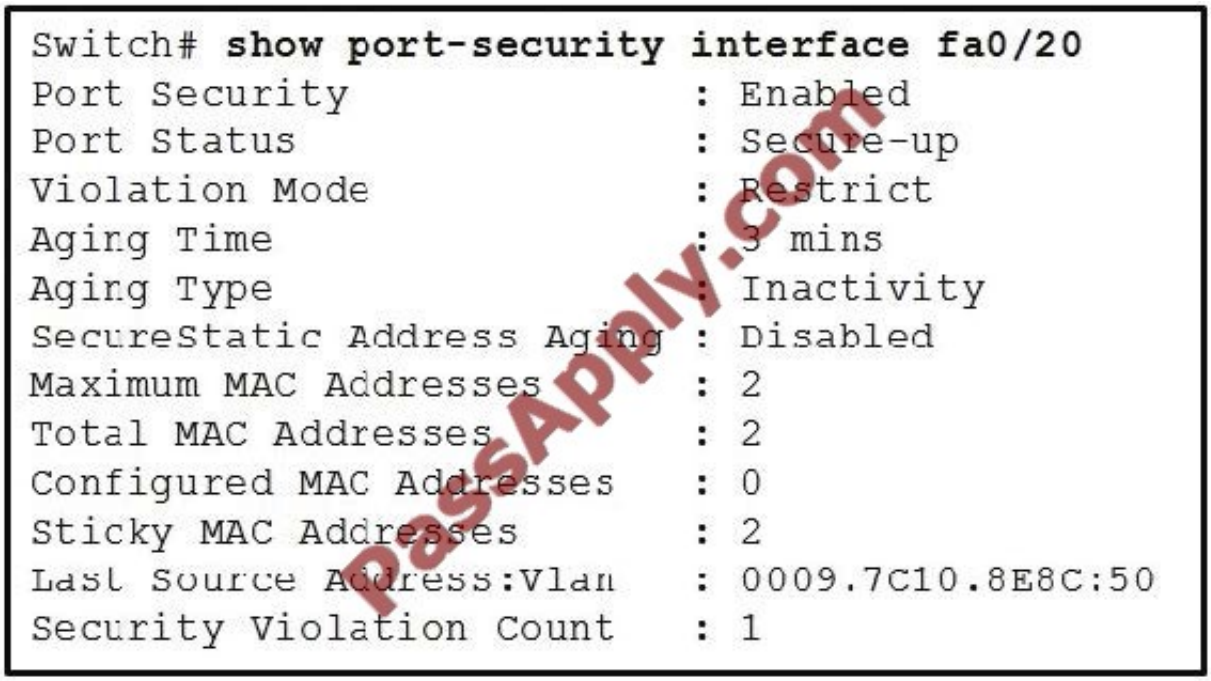
Correct Answer: C

"Show interface pos8/0/0" command showing LMI enq sent which show frame-relay encapsulation enabled on this

interface. Cisco supports three different Local Management Interface (LMI) types for Frame Relay: Cisco, ANSI Annex D, and Q933-A Annex A http://www.ciscopress.com/articles/article.asp? p=170741andseqNum=3

QUESTION 3

Refer to the exhibit.



What three actions will the switch take when a frame with an unknown source MAC address arrives at the interface? (Select three.)

A. Send an SNMP trap.

B. Send a syslog message.

C. Increment the Security Violation counter.

D. Forward the traffic.

E. Write the MAC address to the startup-config.

F. Shut down the port.

Correct Answer: ABC

Switchport Security Concepts and Configuration

http://www.ciscopress.com/articles/article.asp?p=1722561

Switchport Security Violations

The second piece of switchport port-security that must be understood is a security violation including what it is what causes it and what the different violation modes that exist. A switchport violation occurs in one of two situations:

When the maximum number of secure MAC addresses has been reached (by default, the maximum number of secure MAC addresses per switchport is limited to

1) An address learned or configured on one secure interface is seen on another secure interface in the same VLAN The action that the device takes when one of these violations occurs can be configured:

Protect--This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured with this mode, no notification action

is taken when traffic is dropped. Restrict--This mode permits traffic from known MAC addresses to continue to be forwarded while dropping traffic from unknown MAC addresses when over the allowed MAC address limit. When configured

with this mode, a syslog message is logged, a Simple Network Management Protocol (SNMP) trap is sent, and a violation counter is incremented when traffic is dropped.

Shutdown--This mode is the default violation mode; when in this mode, the switch will automatically force the switchport into an error disabled (err-disable) state when a violation occurs. While in this state, the switchport forwards no traffic.

The switchport can be brought out of this error disabled state by issuing the errdisable recovery cause CLI command or by disabling and re-enabling the switchport. Shutdown VLAN--This mode mimics the behavior of the shutdown mode but

limits the error disabled state the specific violating VLAN.

QUESTION 4

At which layer of the OSI model is RSTP used to prevent loops?

A. physical

B. data link

C. network

D. transport

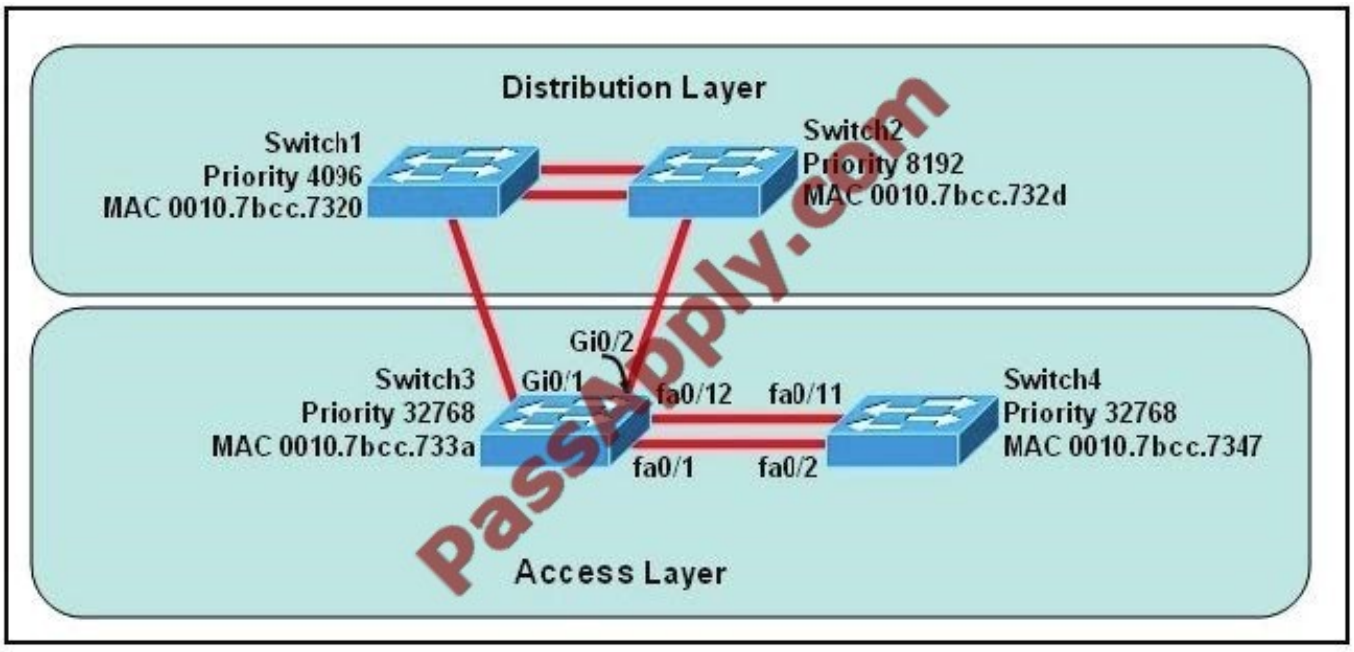
Correct Answer: B

RSTP and STP operate on switches and are based on the exchange of Bridge Protocol Data Units (BPDUs) between switches. One of the most important fields in BPDUs is the Bridge Priority in which the MAC address is used to elect the Root Bridge , RSTP operates at Layer 2.
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_white_paper09186a0080094cfa.shtml

---

QUESTION 5

Refer to the exhibit.



At the end of an RSTP election process, which access layer switch port will assume the discarding role?

A. Switch3, port fa0/1

B. Switch3, port fa0/12

C. Switch4, port fa0/11

D. Switch4, port fa0/2

E. Switch3, port Gi0/1

F. Switch3, port Gi0/2

Correct Answer: C

In this question, we only care about the Access Layer switches (Switch3 and 4). Switch 3 has a lower bridge ID than Switch 4 (because the MAC of Switch3 is smaller than that of Switch4) so both ports of Switch3 will be in forwarding state. The alternative port will surely belong to Switch4. Switch4 will need to block one of its ports to avoid a bridging loop between the two switches. But how does Switch4 select its blocked port? Well, the answer is based on the BPDUs it receives from Switch3. A BPDU is superior than another if it has:

1.

A lower Root Bridge ID

2.

A lower path cost to the Root

3.

A lower Sending Bridge ID

4.

A lower Sending Port ID

These four parameters are examined in order. In this specific case, all the BPDUs sent by Switch3 have the same Root Bridge ID, the same path cost to the Root and the same Sending Bridge ID. The only parameter left to select the best one is the Sending Port ID (Port ID = port priority + port index). In this case the port priorities are equal because they use the default value, so Switch4 will compare port index values, which are unique to each port on the switch, and because Fa0/12 is inferior to Fa0/1, Switch4 will select the port connected with Fa0/1 (of Switch3) as its root port and block the other port -> Port fa0/11 of Switch4 will be blocked (discarding role)