ISLEVER

642-813

Implementing cisco switched networks

DEMO

https://www.islever.com/642-813.html

https://www.islever.com/cisco.html

Topic 1, Implement VLAN based solution, given a network design and a set of requirements

QUESTION NO: 1

Which statement is true about RSTP topology changes?

A. Any change in the state of the port generates a TC BPDU.
B. Only non-edge ports moving to the forwarding state generate a TC BPDU.
C. If either an edge port or a non-edge port moves to a block state, then a TC BPDU is generated.
D. Only edge ports moving to the blocking state generate a TC BPDU.
E. Any loss of connectivity generates a TC BPDU.

Answer: B
Explanation:
The IEEE 802.1D Spanning Tree Protocol was designed to keep a switched or bridged network loop free, with adjustments made to the network topology dynamically. A topology change typically takes 30 seconds, where a port moves from the Blocking state to the Forwarding state after two intervals of the Forward Delay timer. As technology has improved, 30 seconds has become an unbearable length of time to wait for a production network to failover or "heal" itself during a problem.

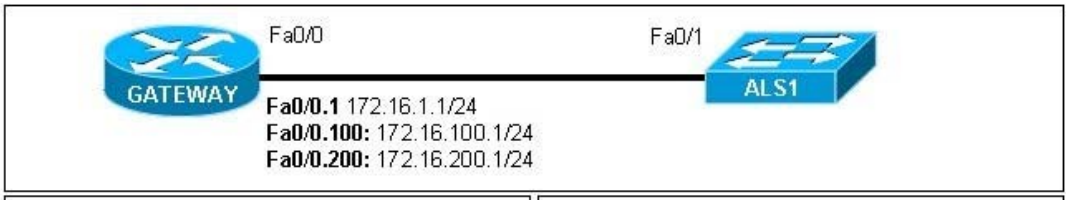
Topology Changes and RSTP
Recall that when an 802.1D switch detects a port state change (either up or down), it signals the Root Bridge by sending topology change notification (TCN) BPDUs. The Root Bridge must then signal a topology change by sending out a TCN message that is relayed to all switches in the STP domain. RSTP detects a topology change only when a non-edge port transitions to the Forwarding state. This might seem odd because a link failure is not used as a trigger. RSTP uses all of its rapid convergence mechanisms to prevent bridging loops from forming. Therefore, topology changes are detected only so that bridging tables can be updated and corrected as hosts appear first on a failed port and then on a different functioning port. When a topology change is detected, a switch must propagate news of the change to other switches in the network so they can correct their bridging tables, too. This process is similar to the convergence and synchronization mechanism-topology change (TC) messages propagate through the network in an ever-expanding wave.

Reference:

CCNP BCMSN Official Exam Certification Guide, Fourth Edition, Chapter 11: Advanced Spanning Tree Protocol, Rapid Spanning Tree Protocol, Topology Changes and RSTP, p. 269

QUESTION NO: 2

Refer to the exhibit.




```
hostname GATEWAY
!
interface FastEthernet0/0
no shutdown
!
interface FastEthernet0/0.1
description Management VLAN
encapsulation dot1Q 1 native
ip address 172.16.1.1 255.255.255.0
!
interface FastEthernet0/0.100
description Finance VLAN
encapsulation dot1Q 100
ip address 172.16.100.1 255.255.255.0
!
interface FastEthernet0/0.200
description Engineering VLAN
encapsulation dot1Q 200
ip address 172.16.200.1 255.255.255.0
```

```
hostname ALS1
!
enable secret cisco
!
interface FastEthernet0/1
!
interface FastEthernet0/6
switchport access vlan 100
switchport mode access
!
interface FastEthernet0/11
switchport access vlan 200
switchport mode access
!
interface Vlan1
ip address 172.16.1.101 255.255.255.0
!
ip default-gateway 172.16.1.1
```

Why are users from VLAN 100 unable to ping users on VLAN 200?

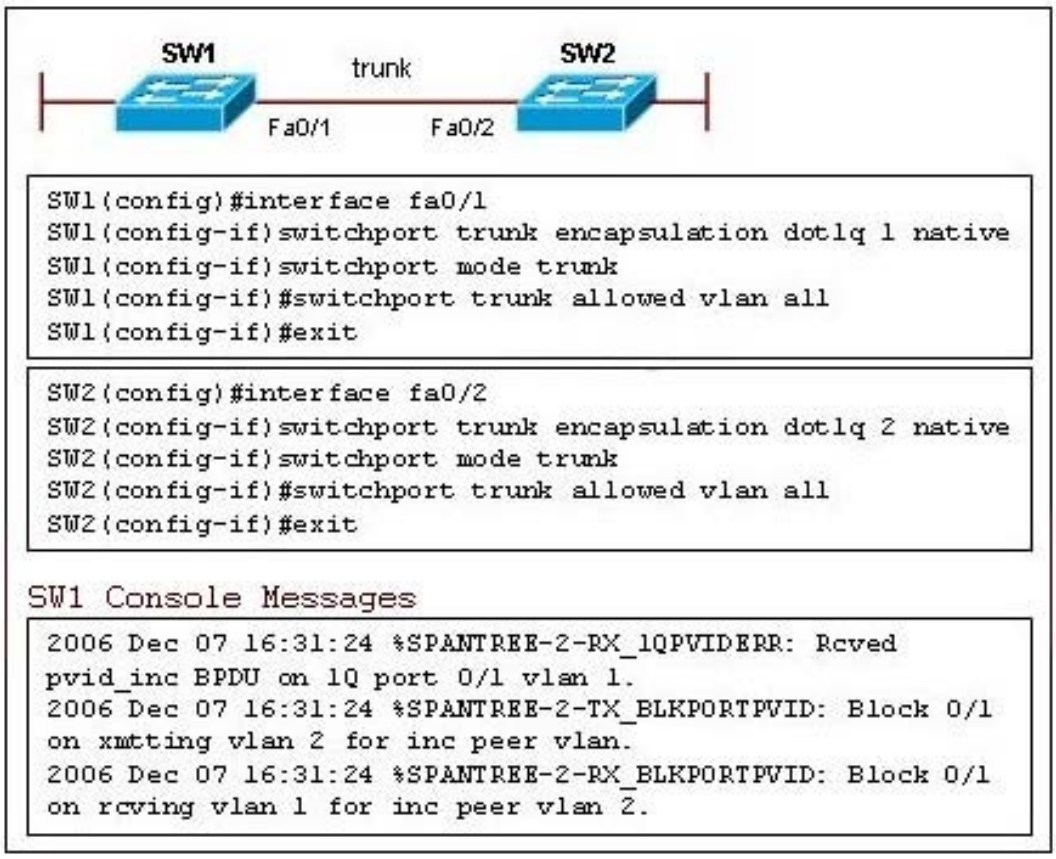
A. Encapsulation on the switch is wrong.
B. Trunking must be enabled on Fa0/1.
C. The native VLAN is wrong.
D. VLAN 1 needs the no shutdown command.
E. IP routing must be enabled on the switch.

Answer: B
Explanation:
Switch supports multiple VLAN but have no Layer3 capability to route packets between those VLANs, the switch must be connected to router external to the switch. This setup is most efficiently accomplished by providing a single trunk link between the switch and the router that can carry the traffic of multiple VLANs, which can in turn be routed by the router. For that trunk require between Router & Switch. So trunking need to be enable on Fa0/1.

http://www.cisco.com/en/US/tech/tk389/tk815/tk857/tsd_technology_support_sub-protocol_home.html

QUESTION NO: 3

Refer to the exhibit.



The link between switch SW1 and switch SW2 is configured as a trunk, but the trunk failed to establish connectivity between the switches. Based on the configurations and the error messages received on the console of SW1, what is the cause of the problem?

A. The two ends of the trunk have different duplex settings.
B. The two ends of the trunk have different EtherChannel configurations.
C. The two ends of the trunk have different native VLAN configurations.
D. The two ends of the trunk allow different VLANs on the trunk.

Answer: C
Explanation:
The native VLAN, if not explicitly configured, will default to the default VLAN, (VLAN1). The Native VLAN is configured for an 802.1Q Trunk port. 802.1Q trunks carry traffic from multiple VLANs by tagging the traffic with VLAN identifiers (Tagged Traffic) which identifies which packets are associated with which VLANs, and they can also carry non VLAN traffic from legacy switches or non 802.1Q compliant switches (Untagged Traffic). The switch will place untagged traffic on the