KTest

更に上のクオリティ　更に上のサービス

問題集

http://www.ktest.jp

1年で無料進級することに提供する

Exam : **300-115**

Title : Implementing Cisco IP Switched Networks

Version : DEMO

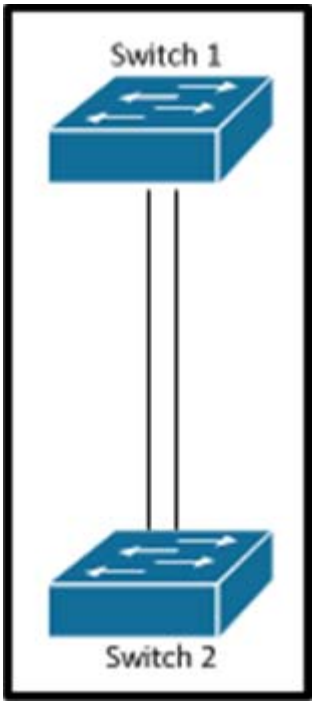
1.What is the maximum number of switches that can be stacked using Cisco StackWise?
A. 4
B. 5
C. 8
D. 9
E. 10
F. 13
Answer: D
Explanation:
Up to 9 Cisco Catalyst switches can be stacked together to build single logical StackWise switch since Cisco IOS XE Release 3.3.0SE. Prior to Cisco IOS XE Release3.3.0SE, up to 4 Cisco Catalyst switches could be stacked together.
Reference: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series- switches/qa_c67-722110.html

2.A network engineer wants to add a new switch to an existing switch stack.
Which configuration must be added to the new switch before it can be added to the switch stack?
A. No configuration must be added.
B. stack ID
C. IP address
D. VLAN information
E. VTP information
Answer: A

3.What percentage of bandwidth is reduced when a stack cable is broken?
A. 0
B. 25
C. 50
D. 75
E. 100
Answer: C
Explanation:
Physical Sequential Linkage
The switches are physically connected sequentially, as shown in Figure 3. A break in any one of the cables will result in the stack bandwidth being reduced to half of its full capacity. Subsecond timing mechanisms detect traffic problems and immediately institute failover. This mechanism restores dual path flow when the timing mechanisms detect renewed activity on the cable. Figure 3. Cisco StackWise Technology Resilient Cabling

Reference: http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series- switches/prod_white_paper09186a00801b096a.html

4.Refer to the exhibit.



Which set of configurations will result in all ports on both switches successfully bundling into an EtherChannel?

A. switch1 channel-group 1 mode active switch2 channel-group 1 mode auto

B. switch1 channel-group 1 mode desirable switch2 channel-group 1 mode passive

C. switch1 channel-group 1 mode on switch2 channel-group 1 mode auto

D. switch1 channel-group 1 mode desirable switch2 channel-group 1 mode auto

Answer: D

Explanation:

The different ether channel modes are described in the table below: Mode Description active Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending LACP packets.

Auto Places an interface into a passive negotiating state, in which the interface re- sponds to PAgP packets it receives but does not start PAgP packet negotia- tion. This setting minimizes the transmission of PAgP packets.

Desirable Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending PAgP packets.

On Forces the interface into an EtherChannel without PAgP or LACP. With the on mode, a usable EtherChannel exists only when an interface group in the on mode is connected to another interface group in the on mode.
Passive Places an interface into a passive negotiating state, in which the interface re- sponds to LACP packets that it receives, but does not start LACP packet ne-gotiation. This setting minimizes the transmission of LACP packets.
Both the auto and desirable PAgP modes allow interfaces to negotiate with partner interfaces to determine if they can form an EtherChannel based on criteria such as interface speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers. Interfaces can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:
An interface in the desirable mode can form an EtherChannel with another interface that is in the desirable or auto mode.
An interface in the auto mode can form an EtherChannel with another interface in the desirable mode. An interface in the auto mode cannot form an EtherChannel with another interface that is also in the auto mode because neither interface starts PAgP negotiation. An interface in the on mode that is added to a port channel is forced to have the same characteristics as the already existing on mode interfaces in the channel.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swethchl.html

5.Refer to the exhibit.

```
interface GigabitEthernet0/1
 switchport
 switchport mode trunk
 switchport trunk allowed vlan 1-100
!
interface GigabitEthernet0/48
 switchport
 switchport mode access
!
monitor session 1 source interface GigabitEthernet0/1
monitor session 1 destination interface GigabitEthernet0/48
```

How can the traffic that is mirrored out the GigabitEthernet0/48 port be limited to only traffic that is received or transmitted in VLAN 10 on the GigabitEthernet0/1 port?
A. Change the configuration for GigabitEthernet0/48 so that it is a member of VLAN 10.
B. Add an access list to GigabitEthernet0/48 to filter out traffic that is not in VLAN 10.
C. Apply the monitor session filter globally to allow only traffic from VLAN 10.
D. Change the monitor session source to VLAN 10 instead of the physical interface.
Answer: C
Explanation:
To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the monitor session filter global configuration command.
Usage Guidelines You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack. You can

monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [, | -] options.
If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (-). VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the monitor session session_number filter vlan vlan-id command to limit SPAN traffic on trunk source ports to only the specified VLANs. VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/network_management/command_reference/b_nm_3se_3850_cr/ b_nm_3se_3850_cr_chapter_010.html#wp3875419997