300-115.exam.85q

Number: 300-115
Passing Score: 800
Time Limit: 120 min

300-115

Implementing Cisco IP Switched Networks

Sections

1. Layer 2 Technologies
2. Infrastructure Security
3. Infrastructure Services

4. Mix Questions

Exam A

QUESTION 1
An access switch has been configured with an EtherChannel port. After configuring SPAN to monitor this port, the network administrator notices that not all traffic is being replicated to the management server. What is a cause for this issue?

A. VLAN filters are required to ensure traffic mirrors effectively.
B. SPAN encapsulation replication must be enabled to capture EtherChannel destination traffic.
C. The port channel can be used as a SPAN source, but not a destination.
D. RSPAN must be used to capture EtherChannel bidirectional traffic.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
A source port or EtherChannel is a port or EtherChannel monitored for traffic analysis. You can configure both Layer 2 and Layer 3 ports and EtherChannels as SPAN sources. SPAN can monitor one or more source ports or EtherChannels in a single SPAN session. You can configure ports or EtherChannels in any VLAN as SPAN sources. Trunk ports or EtherChannels can be configured as sources and mixed with nontrunk sources. A port-channel interface (an EtherChannel) can be a SPAN source, but not a destination.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.html#wp1040905

QUESTION 2
A network engineer tries to configure storm control on an EtherChannel bundle. What is the result of the configuration?

A. The storm control settings will appear on the EtherChannel, but not on the associated physical ports.
B. The configuration will be rejected because storm control is not supported for EtherChannel.
C. The storm control configuration will be accepted, but will only be present on the physical interfaces.
D. The settings will be applied to the EtherChannel bundle and all associated physical interfaces.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
After you configure an EtherChannel, any configuration that you apply to the port-channel interface affects the EtherChannel; any configuration that you apply to the physical interfaces affects only the interface where you apply the configuration.
Storm Control is an exception to this rule. For example, you cannot configure Storm Control on some of the members of an EtherChannel; Storm Control must be configured on all or none of the ports. If you configure Storm Control on only some of the ports, those ports will be dropped from the EtherChannel interface (put in suspended state). Therefore, you should configure Storm Control at the EtherChannel Interface level, and not at the physical interface level.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/channel.html

QUESTION 3
What is the function of NSF?

A. forward traffic simultaneously using both supervisors
B. forward traffic based on Cisco Express Forwarding
C. provide automatic failover to back up supervisor in VSS mode
D. provide nonstop forwarding in the event of failure of one of the member supervisors

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VSS is network system virtualization technology that pools multiple Cisco Catalyst 6500 Series Switches into one virtual switch, increasing operational efficiency, boosting nonstop communications, and scaling system bandwidth capacity to 1.4 Tbps. Switches would operate as a single logical virtual switch called a virtual switching system 1440 (VSS1440). VSS formed by two Cisco Catalyst 6500 Series Switches with the Virtual Switching Supervisor 720-10GE.
In a VSS, the data plane and switch fabric with capacity of 720 Gbps of supervisor engine in each chassis are active at the same time on both chassis, combining for an active 1400-Gbps switching capacity per VSS. Only one of the virtual switch members has the active control plane. Both chassis are kept in sync with the

inter-chassis Stateful Switchover (SSO) mechanism along with Nonstop Forwarding (NSF) to provide nonstop communication even in the event of failure of one of the member supervisor engines or chassis.

Reference: http://ciscorouterswitch.over-blog.com/article-cisco-catalyst-6500-series-vss-1440-124536783.html

QUESTION 4
After UDLD is implemented, a Network Administrator noticed that one port stops receiving UDLD packets. This port continues to reestablish until after eight failed retries. The port then transitions into the errdisable state. Which option describes what causes the port to go into the errdisable state?

A. Normal UDLD operations that prevent traffic loops.
B. UDLD port is configured in aggressive mode.
C. UDLD is enabled globally.
D. UDLD timers are inconsistent.

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/udld.html

QUESTION 5
After reviewing UDLD status on switch ports, an engineer notices that the switch LEDs are green. Which statement describes what this indicates about the status of the port?

A. The port is fully operational and no known issues are detected.
B. The bidirectional status of “unknown” indicates that the port will go into the disabled state because it stopped receiving UDLD packets from its neighbor.
C. UDLD moved into aggressive mode after inconsistent acknowledgements were detected.
D. The UDLD port is placed in the “unknown” state for 5 seconds until the next UDLD packet is received on the interface.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:

Explanation:
By default, UDLD is disabled on all interfaces. We can enable UDLD globally on the device, or individually on specific interfaces with the command udld port. This enables UDLD in normal mode.
It would be prohibitively difficult to coordinate the configuration of UDLD on both ends of a link at the same time, so when UDLD is first enabled and does not detect a neighbor the link state is considered unknown, which is not necessarily an error condition. The port will remain operational during this time. When UDLD is finally enabled on the other end, the status will transition to bidirectional.

References: http://packetlife.net/blog/2011/mar/7/udld/

QUESTION 6
Pilot testing of the new switching infrastructure finds that when the root port is lost, STP immediately replaces the root port with an alternative root port. Which spanning-tree technology is used to accomplish backup root port selection?

A. PVST+
B. PortFast
C. BackboneFast
D. UplinkFast
E. Loop Guard
F. UDLD

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
I f a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanningtree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.
UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 interfaces (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swstpopt.html

QUESTION 7
A network engineer must set the load balance method on an existing port channel. Which action must be done to apply a new load balancing method?

A. Configure the new load balancing method using port-channel load-balance.
B. Adjust the switch SDM back to “default”.
C. Ensure that IP CEF is enabled globally to support all load balancing methods.
D. Upgrade the PFC to support the latest load balancing methods.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Example:
EtherChannel balances the traffic load across the links in a channel through the reduction of part of the binary pattern that the addresses in the frame form to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The mode applies to all EtherChannels that are configured on the switch. You configure the load balancing and forwarding method with use of the **port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}** global configuration command.

Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html

QUESTION 8
What does the command vlan dot1q tag native accomplish when configured under global configuration?

A. All frames within the native VLAN are tagged, except when the native VLAN is set to 1.
B. It allows control traffic to pass using the non-default VLAN.
C. It removes the 4-byte dot1q tag from every frame that traverses the trunk interface(s).
D. Control traffic is tagged.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The “vlan dot1q tag native” will tag all untagged frames, including control traffic, with the defined native VLAN.

QUESTION 9
A network engineer has just deployed a non-Cisco device in the network and wants to get information about it from a connected device. Cisco Discovery Protocol is not supported, so the open standard protocol must be configured. Which protocol does the network engineer configure on both devices to accomplish this?

A. IRDP
B. LLDP
C. NDP
D. LLTD

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol (CDP).

Reference: http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol

QUESTION 10
A manager tells the network engineer to permit only certain VLANs across a specific trunk interface. Which option can be configured to accomplish this?

A. allowed VLAN list
B. VTP pruning
C. VACL
D. L2P tunneling

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
When a trunk link is established, all of the configured VLANs are allowed to send and receive traffic across the link. VLANs 1 through 1005 are allowed on each trunk by default. However, VLAN traffic can be removed from the allowed list. This keeps traffic from the VLANs from passing over the trunk link.
Note: The allowed VLAN list on both the ends of the trunk link should be the same.
For Integrated Cisco IOS Software based switches, perform these steps:
1. To restrict the traffic that a trInk carries, issue the switchport trunk vlan-list interface configuration command.
This removes specific VLANs from the allowed list.

Reference: https://supportforums.cisco.com/document/11836/how-define-vlans-allowed-trunk-link

QUESTION 11
For client server failover purposes, the application server team has indicated that they must not have the standard 30 second delay before their switchport enters a forwarding state. For their disaster recovery feature to operate successfully, they require the switchport to enter a forwarding state immediately. Which spanningtree feature satisfies this requirement?

A. Rapid Spanning-Tree
B. Spanning-Tree Timers C. Spanning-Tree FastPort
D. Spanning-Tree PortFast
E. Spanning-Tree Fast Forward

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In order to allow immediate transition of the port into forwarding state, enable the STP PortFast feature. PortFast immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.
Example configuration:
Switch-C# configure terminal
Switch-C(config)# interface range fa0/3 - 24
Switch-C(config-if-range)# sp–nning-tree portfast

Reference: http://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=36

QUESTION 12
Which command does a network engineer use to verify the spanning-tree status for VLAN 10?

A. switch# show spanning-tree vlan 10
B. switch# show spanning-tree bridge
C. switch# show spanning-tree brief
D. switch# show spanning-tree summary
E. switch# show spanning-tree vlan 10 brief

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

Command	Description
show spanning-tree	Displays information about the spanning-tree state.

Example output:
SW2#show spanning-tree vlan 10


```
VLAN0010
  Spanning tree enabled protocol rstp
  Root ID     Priority    24586
              Address     0014.f2d2.4180
              Cost        9
              Port        216 (Port-channel21)
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    32778  (priority 32768 sys-id-ext 10)
              Address     001c.57d8.9000
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  300 sec

Interface           Role Sts Cost      Prio.Nbr Type
------------------- ---- --- --------- -------- --------------------------
Po21                Root FWD 9         128.216  P2p
Po23                Altn BLK 9         128.232  P2p
```

Reference: http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_s2.html

QUESTION 13
A new network that consists of several switches has been connected together via trunking interfaces. If all switches currently have the default VTP domain name "null", which statement describes what happens when“a do”ain name is configured on one of the switches?

A. The switch with the non-default domain name restores back to "null" upon reboot.
B. Switches with higher revisio“ num”ers does not accept the new domain name.
C. VTP summary advertisements are sent out of all ports with the new domain name.
D. All other switches with the default domain name become VTP clients.

Correct Answer: C
Section: Layer 2 Technologies
Explanation
Explanation/Reference:
Explanation:
By default, a switch will have a domain name of NULL and no password. If the switch hears a VTP advertisement it will automatically learn the VTP domain name, VLANs, and the configuration revision number.
Summary advertisements – sent out every 300 seconds and every time a change occurs on the VLAN database. Contained in a summary advertisement: ▪ VTP version
▪ **Domain name**
▪ Configuration revision number
▪ Time stamp
▪ MD5 encryption hash code

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html

QUESTION 14
A network engineer is setting up a new switched network. The network is expected to grow and add many new VLANs in the future. Which Spanning Tree Protocol should be used to reduce switch resources and managerial burdens that are associated with multiple spanning-tree instances?

A. RSTP
B. PVST
C. MST
D. PVST+
E. RPVST+

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Multiple Spanning Tree (MST) extends the IEEE 802.1w RST algorithm to multiple spanning trees. The main purpose of MST is to reduce the total number of spanning-tree instances to match the physical topology of the network and thus reduce the CPU cycles of a switch. PVRST+ runs STP instances for each VLAN and does not take into consideration the physical topology that might not require many different STP topologies. MST, on the other hand, uses a minimum number of STP instances to match the number of physical topologies present.
Figure 3-15 shows a common network design, featuring an access Switch A, connected to two Building Distribution submodule Switches D1 and D2. In this setup, there are 1000 VLANs, and the network administrator typically seeks to achieve load balancing on the access switch uplinks based on even or odd VLANs—or any other scheme deemed appropriate.

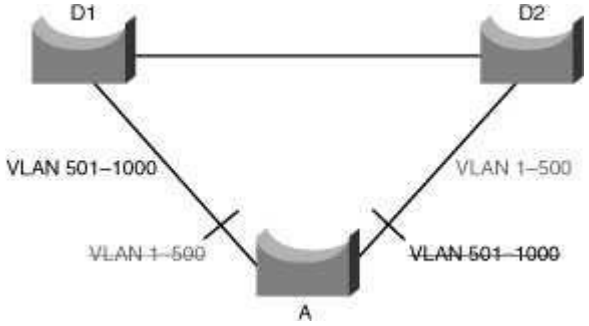


Figure 3-15: VLAN Load Balancing
Figure 3-15 illustrates two links and 1000 VLANs. The 1000 VLANs map to two MST instances. Rather than maintaining 1000 spanning trees, each switch needs to maintain only two spanning trees, reducing the need for switch resources.

Reference: http://ciscodocuments.blogspot.com/2011/05/chapter-03-implementing-spanning-tree_19.html

QUESTION 15
Which statement about the use of SDM templates in a Cisco switch is true?

A. SDM templates are used to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network.
B. SDM templates are used to create Layer 3 interfaces (switch virtual interfaces) to permit hosts in one VLAN to communicate with hosts in another VLAN.
C. SDM templates are used to configure ACLs that protect networks and specific hosts from unnecessary or unwanted traffic.
D. SDM templates are used to configure a set of ACLs that allows the users to manage the flow of traffic handled by the route processor.
E. SDM templates are configured by accessing the switch using the web interface.

Correct Answer: A

Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
You can use SDM templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system usage for some functions; for example, use the default template to balance resources, and use access template to obtain maximum ACL usage. To allocate hardware resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 16
Which SDM template disables routing and supports the maximum number of unicast MAC addresses?

A. VLAN
B. access
C. default
D. routing

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:

- Access — The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default — The default template gives balance to all functions.
- Routing — The routing template maximizes system resources for Ipv4 unicast routing, typically required for a router or aggregator in the center of a network.
- **VLANs — The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.**

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 17
Which SDM template is the most appropriate for a Layer 2 switch that provides connectivity to a large number of clients?

A. VLAN
B. default
C. access
D. routing

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:
▪ Access—The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs. ▪ Default—The default template gives balance to all functions.
▪ Routing—The routing template maximizes system resources for Ipv4 unicast routing, typically required for a router or aggregator in the center of a network. ▪ **VLANs—The VLAN template disables routing and supports the maximum number of unicast MAC addresses (clients). It would typically be selected for a Layer 2 switch.**

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 18
In a Cisco switch, what is the default period of time after which a MAC address ages out and is discarded?

A. 100 seconds
B. 180 seconds
C. 300 seconds
D. 600 seconds

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
To configure the aging time for all MAC addresses, perform this task:

	Command	Purpose
Step 1	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	Specifies the time before an entry ages out and is discarded from the MAC address table. The range is from 0 to 1000000; **the default is 300 seconds**. Entering the value 0 disables the MAC aging. If a VLAN is not specified, the aging specification applies to all VLANs.

Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/MACAddress.html

QUESTION 19
If a network engineer applies the command mac-address-table notification mac-move on a Cisco switch port, when is a syslog message generated?
A. A MAC address or host moves between different switch ports.
B. A new MAC address is added to the content-addressable memory.
C. A new MAC address is removed from the content-addressable memory.
D. More than 64 MAC addresses are added to the content-addressable memory.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
mac-address-table notification mac-move
To enable MAC-move notification, use the **mac-address-table notification mac-move** command in global configuration mode. To disable MAC-move notification, use the **no** form of this command.
Mac-address-table notification mac-move [**counter** [**syslog**]] **no**
mac-address-table notification mac-move [**counter** [**syslog**]]
Syntax Description

counter	(Optional) Specifies the MAC-move counter feature.
Syslog	(Optional) Specifies the syslogging facility when the MAC-move notification detects the first instance of the MAC move.

Usage Guidelines
MAC-move notification generates a syslog message whenever a MAC address or host moves between different switch ports.

Reference: http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html

QUESTION 20
Which option is a possible cause for an errdisabled interface?

A. routing loop
B. cable unpluggedC. STP loop guard
D. security violation

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
There are various reasons for the interface to go into errdisable. The reason can be:
- Duplex mismatch
- Port channel misconfiguration
- BPDU guard violation
- UniDirectional Link Detection (UDLD) condition
- Late-collision detection
- Link-flap detection
- **Security violation**
- Port Aggregation Protocol (PAgP) flap
- Layer 2 Tunneling Protocol (L2TP) guard
- DHCP snooping rate-limit
- Incorrect GBIC / Small Form-Factor Pluggable (SFP) module or cable
- Address Resolution Protocol (ARP) inspection ▪

Inline power

Reference: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00806cd87b.shtml

QUESTION 21
What is the default value for the errdisable recovery interval in a Cisco switch?

A. 30 seconds
B. 100 seconds
C. 300 seconds
D. 600 seconds

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
After you fix the root problem, the ports are still disabled if you have not configured errdisable recovery on the switch. In this case, you must reenable the ports manually. Issue the **shutdown** command and then the **no shutdown** interface mode command on the associated interface in order to manually reenable the ports. The **errdisable recovery** command allows you to choose the type of errors that automatically reenable the ports after a specified amount of time. The **show errdisable recovery** command shows the default error-disable recovery state for all the possible conditions.
cat6knative#**show errdisable recovery**
ErrDisable Reason Timer Status
---------- ----------udld
Disabled bpduguard
Disabled security-violatio
Disabled channel-misconfig
Disabled pagp-flap
Disabled dtp-flap
Disabled link-flap
Disabled l2ptguard
Disabled psecure-violation
Disabled gbic-invalid

Disabled dhcp-rate-limit
Disabled mac-limit
Disabled unicast-flood
Disabled arp-inspection
Disabled

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:
Note: The default timeout interval is 300 seconds and, by default, the timeout feature is disabled.

Reference: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00806cd87b.shtml

QUESTION 22
Which statement about LLDP-MED is true?

A. LLDP-MED is an extension to LLDP that operates between endpoint devices and network devices.
B. LLDP-MED is an extension to LLDP that operates only between network devices.
C. LLDP-MED is an extension to LLDP that operates only between endpoint devices.
D. LLDP-MED is an extension to LLDP that operates between routers that run BGP.

Correct Answer: A
Section: Layer 2 Technologies
Explanation
Explanation/Reference:
Explanation:
LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, and inventory management.

Reference: http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2_58_se/configuration/guide/swlldp.pdf

QUESTION 23
Which statement about Cisco devices learning about each other through Cisco Discovery Protocol is true?

A. Each device sends periodic advertisements to multicast address 01:00:0C:CC:CC:CC.
B. Each device broadcasts periodic advertisements to all of its neighbors.
C. Each device sends periodic advertisements to a central device that builds the network topology.
D. Each device sends periodic advertisements to all IP addresses in its ARP table.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Cisco devices send periodic CDP announcements to the multicast destination address 01-00-0c-cc-cc-cc, out each connected network interface. These multicast packets may be received by Cisco switches and other networking devices that support CDP into their connected network interface.

Reference: https://www.cisco.com/c/en/us/support/docs/network-management/discovery-protocol-cdp/118736-technote-cdp-00.html

QUESTION 24
Which option lists the information that is contained in a Cisco Discovery Protocol advertisement?

A. native VLAN IDs, port-duplex, hardware platform
B. native VLAN IDs, port-duplex, memory errors
C. native VLAN IDs, memory errors, hardware platform
D. port-duplex, hardware platform, memory errors

Correct Answer: A
Section: Layer 2 Technologies
Explanation
Explanation/Reference:
Explanation:
Type-Length-Value fields (TLVs) are blocks of information embedded in CDP advertisements. Table 21 summarizes the TLV definitions for CDP advertisements.

Table 21 **Type-Length-Value Definitions for CDPv2**

TLV	Definition
Device-ID TLV	Identifies the device name in the form of a character string.
Address TLV	Contains a list of network addresses of both receiving and sending devices.
Port-ID TLV	Identifies the port on which the CDP packet is sent.
Capabilities TLV	Describes the functional capability for the device in the form of a device type, for example, a switch.
Version TLV	Contains information about the software release version on which the device is running.
Platform TLV	Describes the hardware platform name of the device, for example, Cisco 4500.
IP Network Prefix TLV	Contains a list of network prefixes to which the sending device can forward IP packets. This information is in the form of the interface protocol and port number, for example, Eth 1/0.
VTP Management Domain TLV	Advertises the system's configured VTP management domain name-string. Used by network operators to verify VTP domain configuration in adjacent network nodes.
Native VLAN TLV	Indicates, per interface, the assumed VLAN for untagged packets on the interface. CDP learns the native VLAN for an interface. This feature is implemented only for interfaces that support the IEEE 802.1Q protocol.
Full/Half Duplex TLV	Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements.

Reference: http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf015.html

QUESTION 25
Which option describes a limitation of LLDP?

A. LLDP cannot provide information about VTP.
B. LLDP does not support TLVs.
C. LLDP can discover only Windows servers.
D. LLDP can discover up to two devices per port.

Correct Answer: A
Section: Layer 2 Technologies
Explanation
Explanation/Reference:
Explanation:
LLDP Versus Cisco Discovery Protocol TLV Comparison

Function Description	LLDP TLV	Cisco Discovery Protocol TLV
IP network prefix support-Used to send the network prefix and used for ODR	No	*IP Network Prefix TLV*
Hello piggybacking-Can be used to piggy back hello messages from other protocols	No	*Protocol Hello TLV*
Maximum-transmission-unit (MTU) support-Specifies the size of the MTU	No	*MTU TLV*
External port support-Used to identify the card terminating the fiber in the case of wavelength-division multiplexing (WDM)	No	*External Port-ID TLV*
VTP management support	**No**	***VTP Management Domain TLV***
Port unidirectional mode-Used in fiber, where the connection may be unidirectional	No	*Port UniDirectional Mode TLV*
Management address	*Management Address TLV*	*Management-AddressTLV*
Allows for organizational unique TLVs	*Yes*	*No*

Reference: http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html

QUESTION 26
Which statement about the UDLD protocol is true?

A. UDLD is a Cisco-proprietary Layer 2 protocol that enables devices to monitor the physical status of links and detect unidirectional failures.
B. UDLD is a Cisco-proprietary Layer 2 protocol that enables devices to advertise their identity, capabilities, and neighbors on a local area network.
C. UDLD is a standardized Layer 2 protocol that enables devices to monitor the physical status of links and detect unidirectional failures.
D. UDLD is a standardized Layer 2 protocol that enables devices to advertise their identity, capabilities, and neighbors on a local area network.

Correct Answer: A
Section: Layer 2 Technologies

Explanation

Explanation/Reference:
Explanation:
The Cisco-proprietary UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links. When a unidirectional link is detected, UDLD puts the affected port into the errdisabled state and alerts the user.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html

QUESTION 27
Which option lists the modes that are available for configuring UDLD on a Cisco switch?

A. normal and aggressive
B. active and aggressive
C. normal and active
D. normal and passive
E. normal and standby

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The Cisco-proprietary UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links. When a unidirectional link is detected, UDLD puts the affected port into the errdisabled state and alerts the user. **UDLD can operate in either normal or aggressive mode.**

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html

QUESTION 28
What is the default interval at which Cisco devices send Cisco Discovery Protocol advertisements?

A. 30 seconds
B. 60 seconds
C. 120 seconds
D. 300 seconds

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices. Cisco Discovery Protocol is enabled by default. Each device configured for Cisco Discovery Protocol advertises at least one address at which the device can receive messages and sends periodic advertisements (messages) to the well-known multicast address 01:00:0C:CC:CC:CC. Devices discover each other by listening at that address. They also listen to messages to learn when interfaces on other devices are up or go down.
Advertisements contain time-to-live information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it. **Advertisements supported and configured in Cisco software are sent, by default, every 60 seconds.**

Reference: http://www.cisco.com/en/US/docs/ios-xml/ios/cdp/configuration/15-mt/nm-cdp-discover.html

QUESTION 29
Which statement about Cisco Discovery Protocol configuration on a Cisco switch is true?

A. CDP is enabled by default and can be disabled globally with the command no cdp run.
B. CDP is disabled by default and can be enabled globally with the command cdp enable.
C. CDP is enabled by default and can be disabled globally with the command no cdp enable.
D. CDP is disabled by default and can be enabled globally with the command cdp run.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
CDP is enabled on your router by default, which means the Cisco IOS software will receive CDP information. CDP also is enabled on supported interfaces by default. To disable CDP on an interface, use the “no cdp enable interface” configuration command. To disable it globally, use the “no cdp run” command.

Reference: http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf015.html#wp1017573

QUESTION 30
Which VTP mode is needed to configure an extended VLAN, when a switch is configured to use VTP versions 1 or 2?
A. transparent
B. client

C. server
D. Extended VLANs are only supported in version 3 and not in versions 1 or 2.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP version 1 and version 2 support VLANs 1 to 1000 only. Extended-range VLANs are supported only in VTP version 3. If converting from VTP version 3 to VTP version 2, VLANs in the range 1006 to 4094 are removed from VTP control.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vtp.html

QUESTION 31
What is the size of the VLAN field inside an 802.1q frame?

A. 8-bit
B. 12-bit
C. 16-bit
D. 32-bit

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The VLAN field is a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs

Reference: http://en.wikipedia.org/wiki/IEEE_802.1Q

QUESTION 32
What is the maximum number of VLANs that can be assigned to an access switchport without a voice VLAN?

A. 0
B. 1

C. 2
D. 1024

Correct Answer: B
Section: Layer 2 Technologies
Explanation

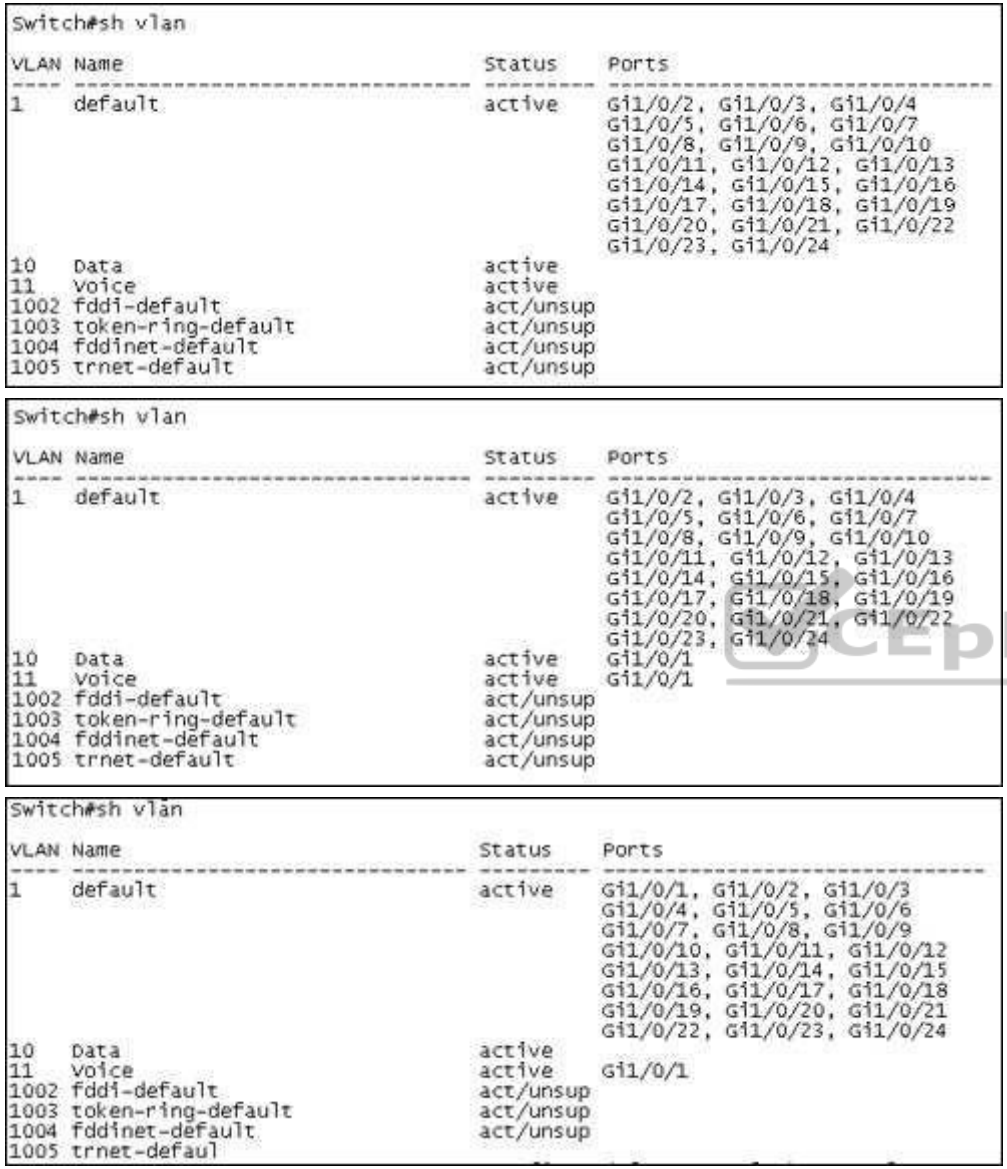
Explanation/Reference:
Explanation:
A standard (non-voice VLAN port) access switch port can belong to only a single VLAN. If more than one VLAN is needed, the port should be configured as a trunk port.

QUESTION 33
Refer to the exhibit.

```
Interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport voice vlan 11
 spanning-tree portfast
!
```


Which option shows the expected result if a show vlan command is issued?

A.



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
10   Data                             active
11   Voice                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
10   Data                             active    Gi1/0/1
11   Voice                            active    Gi1/0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
10   Data                             active
11   Voice                            active    Gi1/0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-defaul
```

B. C.

D.

```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
10   Data                             active    Gi1/0/1
11   voice                            active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```


Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In this case, the port has been configured both as a trunk and as a switchport in data vlan 10. Obviously, a port can not be both, so even though Cisco IOS will accept both, the port will actually be used as a trunk, ignoring the switchport access VLAN 10 command.

QUESTION 34
Which feature is automatically enabled when a voice VLAN is configured, but not automatically disabled when a voice VLAN is removed?

A. portfast

B. port-security
C. spanning tree
D. storm control

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Voice VLAN Configuration Guidelines
- You should configure voice VLAN on switch access ports.
- The voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the voice VLAN. Use the show vlan privileged EXEC command to see if the VLAN is present (listed in the display).
- The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvoip.html

QUESTION 35
Which VLAN range is eligible to be pruned when a network engineer enables VTP pruning on a switch?

A. VLANs 1-1001
B. VLANs 1-4094
C. VLANs 2-1001
D. VLANs 2-4094

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP pruning should only be enabled on VTP servers, all the clients in the VTP domain will automatically enable VTP pruning. By default, VLANs 2 – 1001 are pruning eligible, but VLAN 1 can't be pruned because it's an administrative VLAN. Both VTP versions 1 and 2 supports pruning. Reference: http://www.orbit-computer-solutions.com/vtp-pruning/

QUESTION 36
Which feature must be enabled to eliminate the broadcasting of all unknown traffic to switches that are not participating in the specific VLAN?

A. VTP pruning
B. port-security
C. storm control
D. bpdguard

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
VTP ensures that all switches in the VTP domain are aware of all VLANs. However, there are occasions when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is a feature that you use in order to eliminate or prune this unnecessary traffic.

Reference: http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html#vtp_pruning

QUESTION 37
Refer to the exhibit.

```
Switch1 (config)#vlan 10
VTP vlan configuration not allowed when device is in CLIENT mode.
Switch1#show interfaces trunk
Switch1#
```

The users in an engineering department that connect to the same access switch cannot access the network. The network engineer found that the engineering VLAN is missing from the database. Which action resolves this problem?

A. Disable VTP pruning and disable 802.1q.
B. Update the VTP revision number.
C. Change VTP mode to server and enable 802.1q.
D. Enable VTP pruning and disable 802.1q.

Correct Answer: C

Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Only VTP servers can add new VLANs to the switched network, so to enable vlan 10 on this switch you will first need to change the VTP mode from client to server. Then, you will need to enable 802.1Q trunking to pass this new VLAN along to the other switches.

QUESTION 38
A network engineer must implement Ethernet links that are capable of transporting frames and IP traffic for different broadcast domains that are mutually isolated. Consider that this is a multivendor environment. Which Cisco IOS switching feature can be used to achieve the task?

A. PPP encapsulation with a virtual template
B. Link Aggregation Protocol at the access layer
C. dot1q VLAN trunking
D. Inter-Switch Link

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Here the question asks for transporting “frames and IP traffic for different broadcast domains that are mutually isolated” which is basically a long way of saying VLANs so trunking is needed to carry VLAN information. There are 2 different methods for trunking, 802.1Q and ISL. Of these, only 802.1Q is supported by multiple vendors since ISL is a Cisco proprietary protocol.

QUESTION 39
Which statement about using native VLANs to carry untagged frames is true?

A. Cisco Discovery Protocol version 2 carries native VLAN information, but version 1 does not.
B. Cisco Discovery Protocol version 1 carries native VLAN information, but version 2 does not.
C. Cisco Discovery Protocol version 1 and version 2 carry native VLAN information.
D. Cisco Discovery Protocol version 3 carries native VLAN information, but versions 1 and 2 do not.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Cisco Discovery Protocol (CDP) version 2 passes native VLAN information between Cisco switches. If you have a native VLAN mismatch, you will see CDP error messages on the console output.

Reference: http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3

QUESTION 40
A network engineer must improve bandwidth and resource utilization on the switches by stopping the inefficient flooding of frames on trunk ports where the frames are not needed. Which Cisco IOS feature can be used to achieve this task?

A. VTP pruning
B. access list
C. switchport trunk allowed VLAN
D. VLAN access-map **Correct Answer:** A **Section: Layer 2 Technologies Explanation**

Explanation/Reference:
Explanation:
Cisco advocates the benefits of pruning VLANs in order to reduce unnecessary frame flooding. The “vtp pruning” command prunes VLANs automatically, which stops the inefficient flooding of frames where they are not needed.

Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/24330-185.html

QUESTION 41
Which action allows a network engineer to limit a default VLAN from being propagated across all trunks?

A. Upgrade to VTP version 3 for advanced feature set support.

B. Enable VTP pruning on the VTP server.
C. Manually prune default VLAN with switchport trunk allowed vlans remove.
D. Use trunk pruning vlan 1.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Manaully pruning the default VLAN (1) can only be done with the “switchport trunk allowed vlans remove” command. VLAN 1 is not VTP pruning eligible so it cannot be done via VTP pruning. The “trunk pruning vlan 1” option is not a valid command.

QUESTION 42
What is required for a LAN switch to support 802.1q Q-in-Q encapsulation?

A. Support less than 1500 MTU
B. Support 1504 MTU or higher
C. Support 1522 layer 3 IP and IPX packet
D. Support 1547 MTU only

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The default system MTU for traffic on Catalyst switches is 1500 bytes. Because the 802.1Q tunneling (Q-in-Q) feature increases the frame size by 4 bytes when the extra tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch system MTU size to at least 1504 bytes.

Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/tunnel.html

QUESTION 43
Refer to the exhibit.

```
3512xl(config)#int fastEthernet 0/1
3512xl(config-if)#switchport mode trunk
3512xl(config-if)#switchport trunk encapsulation dot1q
```

How many bytes are added to each frame as a result of the configuration?

A. 4-bytes except the native VLAN
B. 8-bytes except the native VLAN
C. 4-bytes including native VLAN
D. 8-bytes including native VLAN

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN. A VLAN tag adds 4 bytes to the frame. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI).

QUESTION 44
A network engineer configured a fault-tolerance link on Gigabit Ethernet links G0/1, G0/2, G0/3, and G0/4 between two switches using Ethernet port-channel. Which action allows interface G0/1 to always actively forward traffic in the port-channel?

A. Configure G0/1 as half duplex and G0/2 as full duplex.
B. Configure LACP port-priority on G0/1 to 1.
C. Configure LACP port-priority on G0/1 to 65535.
D. LACP traffic goes through G0/4 because it is the highest interface ID.

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:

A LACP port priority is configured on each port using LACP. The port priority can be configured automatically or through the CLI. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating. The higher the number, the lower the priority. The valid range is from 1 to 65535. The default is 32768.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html#wp1081491

QUESTION 45
Which statement about the use of PagP link aggregation on a Cisco switch that is running Cisco IOS Software is true?

A. PagP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on allow the formation of a channel.
B. PagP modes are active, desirable, and on. Only the combinations active-desirable, desirable-desirable, and on-on allow the formation of a channel.
C. PagP modes are active, desirable, and on. Only the combinations active-active, desirable-desirable, and on-on allow the formation of a channel.
D. PagP modes are off, active, desirable, and on. Only the combinations auto-auto, desirable-desirable, and on-on allow the formation of a channel.

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
PagP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on will allow a channel to be formed.
The PagP modes are explained below.
1. on: PagP will not run. The channel is forced to come up.
2. off: PagP will not run. The channel is forced to remain down.
3. auto: PagP is running passively. The formation of a channel is desired; however, it is not initiated.
4. desirable: PagP is running actively. The formation of a channel is desired and initiated.

Only the combinations of auto-desirable, desirable-desirable, and on-on will allow a channel to be formed. If a device on one side of the channel does not support PagP, such as a router, the device on the other side must have PagP set to on.

Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2900-xl-series-switches/21041-131.html

QUESTION 46
Which statement describes what happens when a port configured with root guard receives a superior BPDU?

A. The port goes into errdisabled state and stops forwarding traffic.
B. The port goes into BPDU-inconsistent state and stops forwarding traffic.
C. The port goes into loop-inconsistent state and stops forwarding traffic.
D. The port goes into root-inconsistent state and stops forwarding traffic.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The root guard ensures that the port on which root guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forlarded across this port. In this way, the root guard enforces the position of the root bridge.

Reference: http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml

QUESTION 47
Which statement about restrictions for multichassis LACP is true?

A. It is available only on a Cisco Catalyst 6500 Series chassis.
B. It does not support 1Gb links.
C. Converting a port channel to mLACP can cause a service disruption.
D. It is not available in VSS.

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
When configuring mLACP for Server Access, follow these guidelines and restrictions:
▪ PFC3A mode does not support the mLACP for server access feature.
▪ VSS mode does not support the mLACP for server access feature. ▪ No more than 100 VLANs can be active on a switch configured as a PoA. ▪ mLACP does not support half-duplex links. ▪ mLACP does not support multiple neighbors.
▪ **Converting a port channel to mLACP can cause a service disruption**.
▪ The DHD system priority must be lower (higher numerically) than the PoA system priority.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mlacp_server_support.html

QUESTION 48

What is the maximum number of 10 Gigabit Ethernet connections that can be utilized in an EtherChannel for the virtual switch link?

A. 4
B. 6
C. 8
D. 12

Correct Answer: C
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
The VSS is made up of the following:
▪ Virtual switch members: Cisco Catalyst 6500 Series Switches (up to two switches with initial release) deployed with the Virtual Switching Supervisor 720 10GE ▪ **Virtual switch link (VSL): 10 Gigabit Ethernet connections (up to eight using EtherChannel) between the virtual switch members.**

Reference: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_qas0900aecd806ed74b.html

QUESTION 49
Which statement describes what happens if all VSL connections between the virtual switch members are lost?

A. Both virtual switch members cease to forward traffic.
B. The VSS transitions to the dual active recovery mode, and both virtual switch members continue to forward traffic independently.
C. The virtual switch members reload.
D. The VSS transitions to the dual active recovery mode, and only the new active virtual switch continues to forward traffic.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Q. What happens if all VSL connections between the virtual switch members are lost?
A. VSLs can be configured with up to eight links between the two switches across any combination of line cards or supervisor ports to provide a high level of redundancy. If for some rare reason all VSL connections are lost between the virtual switch members leaving both the virtual switch members up, the VSS will transition to the dual active recovery mode.
The dual active state is detected rapidly (subsecond) by any of the following three methods:
▪ Enhancement to PagP used in MEC with connecting Cisco switches

- L3 Bidirectional Forwarding Detection (BFD) configuration on a directly connected link (besides VSL) between virtual switch members or through an L2 link through an access layer switch
- L2 Fast-Hello Dual-Active Detection configuration on a directly connected link (besides VSL) between virtual switch members (supported with 12.2(33)SXI)

In the dual active recovery mode, all interfaces except the VSL interfaces are in an operationally shut down state in the formerly active virtual switch member. The new active virtual switch continues to forward traffic on all links.

Reference: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_qas0900aecd806ed74b.html

QUESTION 50
Refer to the exhibit. Which two statements about the network environment of the device that generated this output are true? (Choose two.)

```
FastEthernet1/0/47 - Group 1 (version 2)
      State is Standby
            7 state changes, last state change 00:00:02
      Virtual IP address is 10.1.1.1
      Active virtual MAC address is 0000.0c9f.f001 (v2 default)
            Local virtual MAC address is 0000.0c9f.f001 (v2 default)
      Hello time 3 sec, hold time 10 sec
            Next hello sent in 0.375 secs
      Authentication MD5, key-string "cisco"
      Preemption enabled, delay min 5 secs
      Active router is 10.1.1.2, priority 255 (expires in 9.396 sec)
      Standby router is local
      Priority 100 (default 100)
      IP redundancy name is "hsrp-Fa1/0/47-1" (default)
```

A. The virtual IP address of the HSRP group is 10.1.1.1
B. If a router with a higher IP address and same HSRP priority as the active router becomes available, that router becomes the new active router 5 seconds later
C. The local device has a higher priority setting than the active router
D. The hello and hold timers are set to custom values
E. If the local device fails to receive a hello from the active router for more than 5 seconds, it can become the active router

Correct Answer: AB

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 51
If StormControl is enabled on a port and the traffic reaches the configured level, which two actions can be configured to occur? (Choose two.)

A. trap
B. log
C. notify admin
D. redirect traffic
E. shut down

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 52
In which two ways can a port respond to a port-security violation? (Choose two.)

A. The port enters the err-disabled state
B. The port enters the shutdown state
C. The port triggers an EEM script to notify support staff and continues to forward traffic normally
D. The SecurityViolation counter is incremented and the port sends an SNMP trap
E. The SecurityViolation counter is incremented and the port sends a critical syslog message to the console
F. The port immediately begins to drop all traffic

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

protect - The PFC drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
restrict - The PFC drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the security violation counter to increment. shutdown - Puts the interface into the error-disabled state immediately and sends an SNMP trap notification. Restrict increments the counter and sends an SNMP trap. And shutdown puts the interface in err-disabled state.

QUESTION 53
Which statement is correct about 802.1Q trunking?

A. Both switches must be in the same VTP domain.
B. The encapsulation type of both ends of the trunk does not have to match.
C. The native VLAN on both ends of the trunk must be VLAN 1.
D. 802.1Q trunking can only be configured on a Layer 2 port.
E. In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN.

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 54
Which of the following commands can be issued without interfering with the operation of loop guard?

A. Switch(config-if)#spanning-tree guard root
B. Switch(config-if)#spanning-tree portfast
C. Switch(config-if)#switchport mode trunk
D. Switch(config-if)#switchport mode access

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 55

The following command was issued on a router that is being configured as the active HSRP router.
standby ip 10.2.1.1
Which statement is true about this command?

A. This command will not work because the HSRP group information is missing
B. The HSRP MAC address will be 0000 0c07 ac00
C. The HSRP MAC address will be 0000 0c07 ac01.
D. The HSRP MAC address will be 0000.070c ad01.
E. This command will not work because the active parameter is missing

Correct Answer: B
Section: Mix Questions
Explanation
Explanation/Reference:

QUESTION 56
Routers R1 and R2 are configured for HSRP as shown below:

Router R1:
interface ethernet 0
ip address 20.6.2.1 255.255.255.0
standby 35 ip 20.6.2.21 standby 35
priority 100 interface ethernet 1 ip
address 20.6.1.1.2 255.255.255.0
standby 34 ip 20.6.1.21

Router R2:
interface ethernet 0
ip address 20.6.2.2 255.255.255.0
standby 35 ip 20.6.2.21

interface ethernet 1 ip address
20.6.1.1.1 255.255.255.0 standby
34 ip 20.6.1.21 standby 34 priority
100

You have configured the routers R1 & R2 with HSRP. While debugging router R2 you notice very frequent HSRP group state transitions. What is the most likely cause of this?

A. physical layer issues
B. no spanning tree loops
C. use of non-default HSRP timers
D. failure to set the command standby 35 preempt

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 57
Which two statements about the HSRP priority are true? (Choose two.)

A. To assign the HSRP router priority in a standby group, the standby group-number priority priority-value global configuration command must be used.
B. The default priority of a router is zero (0).
C. The no standby priority command assigns a priority of 100 to the router.
D. Assuming that preempting has also been configured, the router with the lowest priority in an HSRP group would become the active router.
E. When two routers in an HSRP standby group are configured with identical priorities, the router with the highest configured IP address will become the active router.

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 58
Which three statements are true of a default HSRP configuration? (Choose three.)

A. The Standby hello time is 2 seconds.
B. Two HSRP groups are configured.
C. The Standby track interface priority decrement is 10. D. The Standby hold time is 10 seconds
E. The Standby priority is 100.
F. The Standby delay is 3 seconds.

Correct Answer: CDE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 59
Refer to the exhibit. What is the result of setting GLBP weighting at 105 with lower threshold 90 and upper threshold 100 on this router?

```
Router# show glbp FastEthernet0/1 1

FastEthernet0/1 - Group 1

State is Listen
  64 state changes, last state change 00:00:54
Virtual IP address is 10.1.0.7
Hello time 50 msec, hold time 200 msec
  Next hello sent in 0.030 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication text "authword"
Preemption enabled, min delay 0 sec
Active is 10.1.0.2, priority 105 (expires in 0.184 sec)
Standby is 10.1.0.3, priority 100 (expires in 0.176 sec)
Priority 96 (configured)
Weighting 105 (configured 105), thresholds: lower 90, upper 100
  Track object 1 state Up decrement 10
  Track object 2 state Up decrement 10
Load balancing: round-robin
IP redundancy name is "glbp1"
  Group members:
    0004.4d83.4801 (10.0.0.0)
    0010.7b5a.fa41 (10.0.0.1)
    00d0.bbd3.bc21 (10.0.0.2) local
```

A. Only if both tracked objects are up will this router will be available as an AVF for group 1.
B. Only if the state of both tracked objects goes down will this router release its status as an AVF for group 1.
C. If both tracked objects go down and then one comes up, but the other remains down, this router will be available as an AVF for group 1.
D. This configuration is incorrect and will not have any effect on GLBP operation.
E. If the state of one tracked object goes down, then this router will release its status as an AVF for group 1.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 60
Which describes the default load balancing scheme used by the Gateway Load Balancing Protocol (GLBP)?

A. Per host using a strict priority scheme
B. Per session using a round-robin scheme
C. Per session using a strict priority scheme
D. Per GLBP group using a strict priority scheme
E. Per host basis using a round robin-scheme
F. Per GLBP group using a round-robin scheme

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 61
Which two statements about default FHRP behavior are true? (Choose two.)

A. A backup GLBP active virtual gateway can become active only if the current active virtual gateway fails.
B. Preemption is enabled by default.
C. Unless specifically Configured, the priority of an HSRP router is 200.
D. A standby HSRP router becomes active if it has a higher priority than the priority of the current active router.
E. A VRRP backup virtual router becomes the master router if its priority is higher than the priority of the current master router.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 62
To provide security, a service provider configures various private VLANs in its backbone network infrastructure to prevent certain VLANs from communicating to each other. Which version of VTP supports the use of private VLANs?

A. Version 1
B. Version 3
C. VTP does not support private VLANs
D. Version 2

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 63
Which statement about HSRP, GLBP, and VRRP is true?

A. VRRP group members communicate using multicast address 224.0.0.102.
B. MAC address 0000.0c07.acOc indicates that default gateway redundancy is provided through GLBP.
C. HSRP group members communicate using multicast address 224.0.0.18.
D. GLBP uses UDP port 3222 (source and destination) for hello messages.
E. MAC address 0c07.A698.8904 indicates that default gateway redundancy is provided through HSRP.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 64
What action should a network administrator take to enable VTP pruning on an entire management domain?

A. Enable VTP pruning on any client switch in the domain.
B. Enable VTP pruning on every switch in the domain.
C. Enable VTP pruning on any switch in the management domain.
D. Enable VTP pruning on a VTP server in the management domain.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 65
What is the effect of configuring the following command on a switch?

Switch(config) # spanning-tree portfast bpdufilter default

A. If BPDUs are received by a port configured for PortFast, then PortFast is disabled and the BPDUs are processed normally.
B. If BPDUs are received by a port configured for PortFast, they are ignored and none are sent.
C. If BPDUs are received by a port configured for PortFast, the port transitions to the forwarding state.
D. The command enables BPDU filtering on all ports regardless of whether they are configured for BPDU filtering at the interface level.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 66
Which protocol will enable a group of routers to form a single virtual router and will use the real IP address of a router as the gateway address?

A. Proxy ARP

B. HSRPC. IRDP
D. VRRP
E. GLBP

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
QUESTION 67
Which two statements are true about recommended practices that are to be used in a local VLAN solution design where layer 2 traffic is to be kept to a minimum? (Choose two.)

A. Routing should occur at the access layer if voice VLANs are utilized. Otherwise, routing should occur at the distribution layer.
B. Routing may be performed at all layers but is most commonly done at the core and distribution layers.
C. Routing should not be performed between VLANs located on separate switches.
D. VLANs should be local to a switch.
E. VLANs should be localized to a single switch unless voice VLANs are being utilized.

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 68
What two things occur when an RSTP edge port receives a BPDU? (Choose two.)

A. The port immediately transitions to the forwarding state.
B. The switch generates a Topology Change Notification BPDU.
C. The port immediately transitions to the err-disable state.
D. The port becomes a normal STP switch port.

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 69
How does VTP pruning enhance network bandwidth?

A. by restricting unicast traffic across VTP domains
B. by reducing unnecessary flooding of traffic to inactive VLANs
C. by limiting the spreading of VLAN information
D. by disabling periodic VTP updates

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 70
In the hardware address 0000.0c07.ac0a, what does 07.ac represent?

A. vendor code
B. HSRP group number
C. HSRP router number
D. HSRP well-known physical MAC address
E. HSRP well-known virtual MAC address

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 71
Which statement is true about RSTP topology changes?

A. Any change in the state of the port generates a TC BPDU.

B. Only nonedge ports moving to the forwarding state generate a TC BPDU.
C. If either an edge port or a nonedge 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.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
QUESTION 72
In a switch stack where is the SDM template stored?

A. All switches in stack
B. Master switch
C. Flash memory

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 73
Refer to exhibit, which two statements correctly indicate when an SNMP trap is set to the switch? (Choose two.)

```
Switch(config)# snamp-server enable traps mac-notification
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold limit 60
Switch(config)# mac address-table notification mac-move
```

A. When a new workstation connects to port Fa0/1
B. When 61 MAC address are in the switch table
C. When 61 percent of the MAC address table capacity is used

D. When the switch loses power and reboots
E. When the phone previously on Fa0/2 is now connect to Fa0/5

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:
QUESTION 74
Which two secondary VLAN types of Private VLANs (PVLANs)? (Choose two)

A. community
B. isolated
C. promiscuous
D. host

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Secondary VLANs provide Layer 2 isolation between ports within the same private VLAN domain.
There are two types of secondary VLANs:

- Isolated VLANs - Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs - Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level

QUESTION 75
What types of SDM templates you can use in switch? (Choose all that apply.)

A. Access
B. Default
C. Routing
D. VLANs

Correct Answer: ABCD

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
- Access - The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default - The default template gives balance to all functions.
- Routing - The routing template maximizes system resources for IPv4 unicast routing, typically required for a router or aggregator in the center of a network.
- VLANs - The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.

QUESTION 76
What is the process to configure EtherChannel?

A. shutdown both interface ports
B. shutdown the interface on one side only

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 77
What is the default spanning tree port priority?

A. 128
B. 129
C. 1
D. 64

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 78

How do you configure Spanning-tree EtherChannel guard?

A. (config)#spanning-tree etherchannel guard misconfig
B. (config-if)#spanning-tree etherchannel guard misconfig C. (config)#spanning-tree etherchannel misconfig guard
D. (config-if)#spanning-tree etherchannel misconfig guard

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 79
Which option is the value of the Tag Protocol Identifier 802.1Q tagged frame?

A. 0x0806
B. 0x888E
C. 0x0800
D. 0x8100

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
16-bit field set to 0x8100 in order to identify the frame as 802.1q tagged frame.

QUESTION 80
How do you configure loop guard?

A. (config)#spanning-tree loop guard default
B. (config-if)#spanning-tree loop
C. (config)#spanning-tree loop-guard default
D. (config-if)#spanning-tree guard loop

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 81
A dynamic access port is member of which VLAN by default?
A. VLAN 1 is the default VLAN
B. Same as the native VLAN
C. none until the port VLAN is determined
D. VLAN 4096

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 82
What happens if a switch with dhcp snooping and ip source guard enabled globally, what does the switch do when it receives a packet with option 82?

A. Drop
B. Remove 82 and forward
C. Proxy
D. NA

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 83
Which type of packet does DHCP snooping continuously check in a production network?

A. DHCP Snooping
B. DHCP Relay
C. DHCP Request
D. DHCP Acknowledge
E. DHCP Reply
F. DHCP Allow

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 84
Which three functions does Dynamic ARP Inspection perform with invalid IP-to MAC address bindings? (Choose three.)

A. deletes
B. logs
C. accepts
D. intercepts
E. discards
F. bypasses

Correct Answer: BDE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 85
Which statement about the configuration of MST on an IOS switch is true?

A. When MST is enabled, RSTP is automatically enabled and MST will use BPDU version 4, maximum of 16 instances of MST can exist.
B. When MST is enabled, RSTP is automatically disabled and MST will use BPDU version 4, maximum of 16 instances of MST can exist.
C. When MST is enabled, RSTP is automatically disabled and MST will use BPDU version 2, maximum of 16 instances of MST can exist.
D. When MST is enabled, RSTP is automatically enabled and MST will use BPDU version 2, maximum of 16 instances of MST can exist.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference: