
# Vendor: Cisco

# Exam Code: 400-351

# Exam Name: CCIE Wireless Written Exam

# Version: Demo

**QUESTION 1**
Which three statements about the high availability configuration on the Cisco 5760 WLCs are true? (Choose three.)

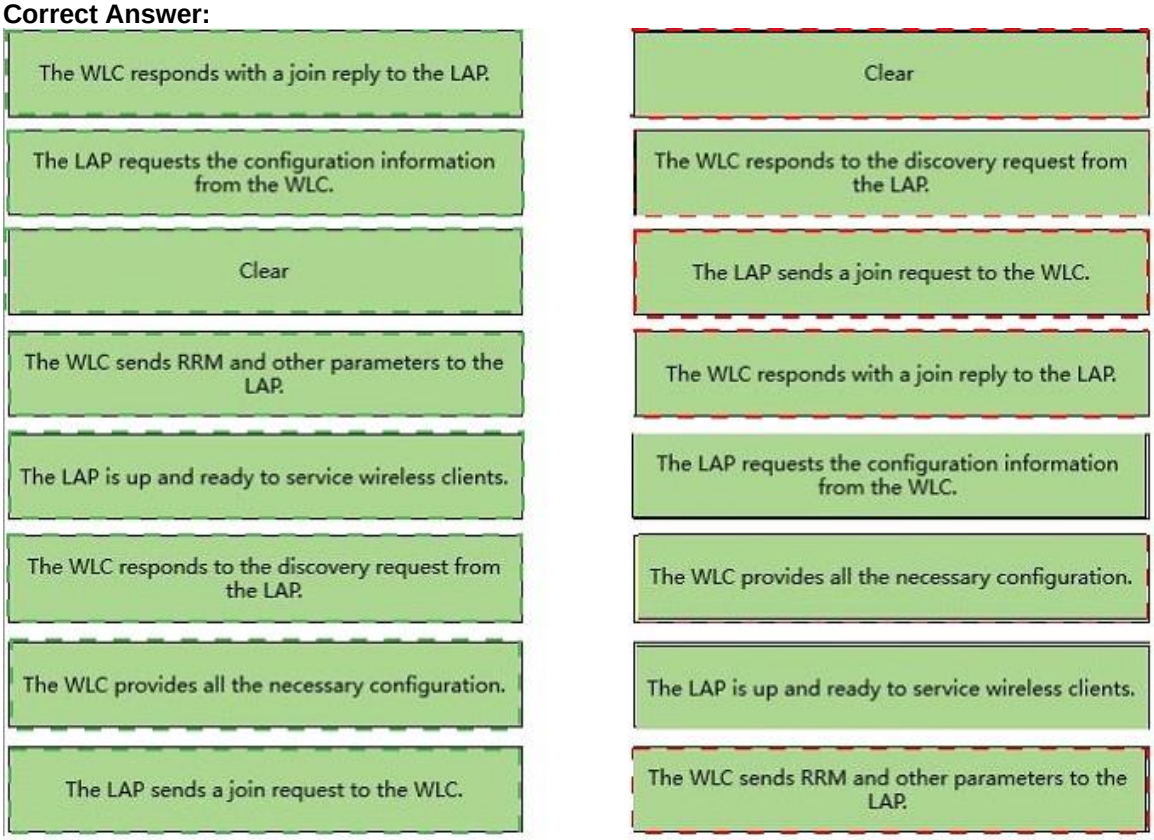
A. Cisco WLC with more reboots is elected as active when the default stack priority is in use.
B. EtherChannel bundles all ports on both active and standby Cisco WLC on a logical port.
C. Cisco 5760 WLC uses a dedicated high availability port for high availability and configuration synchronization.
D. High availability switchover is triggered when one of the ports on the active Cisco WLC EtherChannel bundle fails.
E. Active Cisco WLCs in a pair can be identified using LED state without issuing any command on the Cisco WLC console.
F. Cisco WLC with the highest priority in a stack are elected as the active Cisco WLC during the election process.
G. All configuration including certificates are automatically synced between active and standby Cisco WLC.

**Correct Answer:** BEF
**Explanation:**
http://www.cisco.com/c/en/us/td/docs/wireless/technology/5760_deploy/CT5760_Controller_Deployment_Guide/High_Availability.html

**QUESTION 2**
DRAG DROP
Drag and drop the CAPWAP event on the left into the order in which they occur on the right during the WLC discovery and join processes.

| | |
|---|---|
| The WLC responds with a join reply to the LAP. | Target 1 |
| The LAP requests the configuration information from the WLC. | Target 2 |
| Clear | Target 3 |
| The WLC sends RRM and other parameters to the LAP. | Target 4 |
| The LAP is up and ready to service wireless clients. | Target 5 |
| The WLC responds to the discovery request from the LAP. | Target 6 |
| The WLC provides all the necessary configuration. | Target7 |
| The LAP sends a join request to the WLC. | Target 8 |

**Correct Answer:**




**QUESTION 3**
Which two statements about accessing the GUI and CLI of Cisco WLC are true? (Choose two.)

A. The feature "Management using Dynamic Interfaces" can be applied to one of the Dynamic Interfaces only.
B. Wireless management access is only possible through the default management WLAN "thazz"
C. The wireless clients can access the Cisco WLC only when the option " Enable Controller Management to be accessible from Wireless Clients" is checked.
D. The feature "Management using Dynamic Interfaces" can be configured in CLI only. Wireless management access is only possible through the default management WLAN - WLAN ID.
E. Wired clients |can have only CLI access with the dynamic interface of the Cisco WLC, while wireless clients have both CLI and GUI access with the dynamic interface when the feature "Management using Dynamic Interfaces" is enabled.

**Correct Answer:** AC

**QUESTION 4**
Which feature intersection of a Cisco 5760 Wireless LAN Controller with HA AP SSO is not true?

A. Switchover during AP preimage download causes the Aps to start image download all over again from the new active controller.
B. Upon guest anchor controller switchover, mobility tunnels stay active, Aps remain connected, clients rejoin at MA or MC, and clients are anchored on the new active controller.
C. WIPS information is synced to the standby unit. The standby unit does not have to relean wIPS

information upon switchover.

D. Roamed clients that have their data path going through the mobility tunnel endpoint "becomed Local" in case of Layer 2 with sticky anchoring and Layer 3 roam. Layer 2 roamed clients are not affected except when roaming occurs between Cisco Unified Wireless Network and CA controller.

**Correct Answer:** C
**Explanation:**
CT5760 High Availability AP SSO Deployment Guide, Cisco IOS XE Release 3.3 - Cisco

http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/5700/software/release/ios_xe_33/5760_HA_DG_iosXE33.html

This document introduces the Access Point Stateful Switch Over redundancy model for High Availability (HA) with CT5760 controllers using the StackWise-480 technology. HA in Cisco 5700 Series Wireless Controller is enabled using Cisco StackWise-480 technology.

Feature Intersection with AP SSO
Switchover during AP Pre-Image download causes the APs to start image download all over again from the new Active controller.
Rogue APs and clients are not synced to Standby and are re-learnt upon switchover.
Infra structure MFP key is not synced to the Standby controller and is re-learnt upon switchover.
New Active controller re-learns the shim list from IPS and other MCs. and redistributes it to the MAs.
wIPS information is not synced to the Standby unit and is re-learnt upon switchover.
Clean Air detected Interferer devices are re-learnt after switchover.
Net Flow records are cleared upon switchover and collection starts fresh on the new Active controller.
Mobility paths and tunnels to the MO and other peer MCs are not disrupted upon switchover. However the Client state is cleaned up on the MO under which the HA pair exists and is re-learnt from the new Active controller when the client re-associates.
Roamed clients that have their data path going through the Mobility Tunnel Endpoint (MTE) "become Local"' in case of L2 with Sticky Anchoring and L3 Roam. L2 Roamed Clients are not affected except when roaming occurs between CUWN and CA controllers.
RRM related configurations and the AP neighbor list in the Leader HA pair is synced to the Standby controller.
Upon Guest Anchor controller switchover, mobility tunnels stay active. APs remain connected, clients rejoin at MA or MC. and are anchored on the new Active controller.

**QUESTION 5**
With the introduction of mDNS policies in AireOS release 8.0, the administrator can configure to identify who uses the Bonjour service instances and in which location. Based on user 802.1x authentication, a AAA server/ISE can be configured to return which two possible values in the form of a "CISCO-AV-PAIR"? (Choose two.)

A. Client-role
B. User-role
C. User-ID
D. Bonjour-profile
E. Client-location

**Correct Answer:** BD
**Explanation:**

## Information about Bonjour gateway based on access policy

From 7.4 release WLC supports Bonjour gateway functionality on WLC itself for which you need not even enable multicast on the controller. The WLC explores all Bonjour discovery packets and does not forward them on AIR or Infra network.

Bonjour is Apple's version of Zeroconf - it is Multicast Domain Name System (mDNS) with DNS-SD (Domain Name System-Service Discovery). Apple devices will advertise their services via IPv4 and IPv6 simultaneously (IPv6 link local and Globally Unique). To address this issue Cisco WLC acts as a Bonjour Gateway. The WLC listens for Bonjour services and by caching those Bonjour advertisements (AirPlay, AirPrint etc) from the source/host e.g. AppleTV and responds to Bonjour clients when they ask/request for a service.

Bonjour gateway has inadequate capabilities to filter cached wired or wireless service instances based on the credentials of the querying client and its location.

Currently the limitations are:

- Location-Specific Services (LSS) filters the wireless service instances only while responding to a query from wireless clients. The filtering is based on the radio neighborhood of the querying client.
- LSS cannot filter wired service instance because of no sense of location.
- LSS filtering is per service type and not per client. It means that all clients receive the location based filtered response if LSS is enabled for the service type and clients cannot override the behavior.
- There is no other filtering mechanism based on client role or user-id.

The requirement is to have configuration per service instance.

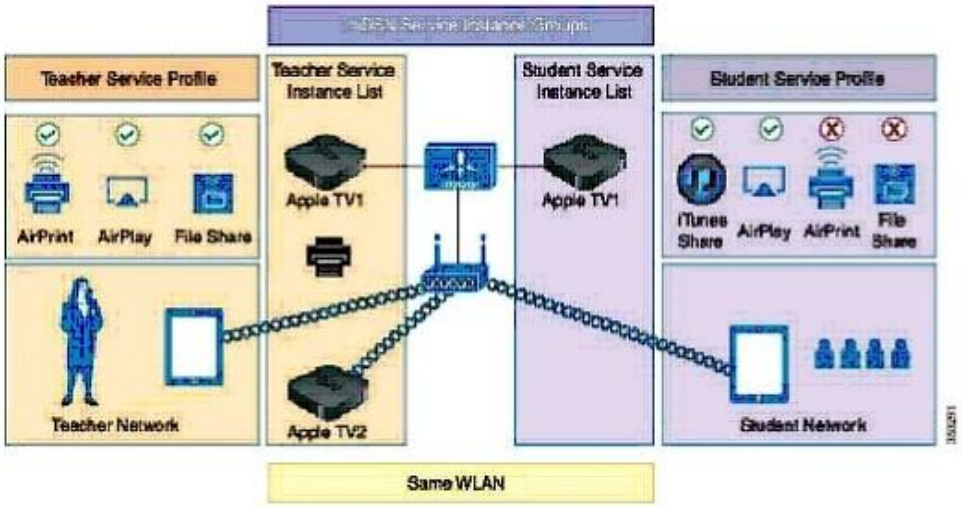
Following are the three criteria of the service instance sharing:

- User-id
- Client-role
- Client location

## Introduction to Bonjour Policies and New Requirements

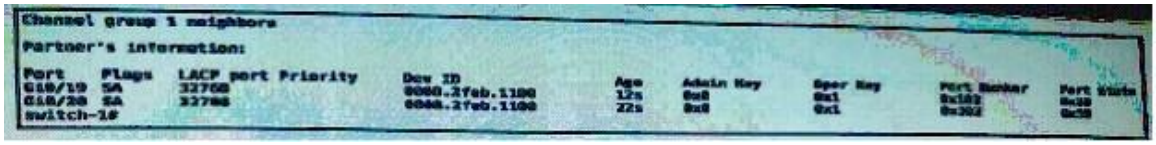
Enterprise credentials of Bonjour are poor and hence the advent of Bonjour gateway. Bonjour gateway snoops and caches Bonjour services across VLANs and periodically refreshes the same. WLC acts as a proxy for all Bonjour services published by wireless and wired devices. Bonjour gateway as of release prior to 8.0 had inadequate capabilities to filter cached wired / wireless service instances based on the credentials of the querying client and its location.

With introduction of the Bonjour policies in the release 8.0, the administrator can configure to identify who uses the Bonjour service instances and in what location (all this applies to the same WLAN). With introduction of the Bonjour policies, the administrator does not need to create multiple WLANs to select which services are allowed or should be used on specific WLAN. Based on user 802.1x authentication, the AAA server or ISE can be configured to return USER-ROLE or BONJOUR-PROFILE in the form of the "CISCO-AV-PAIR". This value gets plumbed into the policy created on the wireless controller. Based on the user authentication, a configured policy and profile are applied to a specific user on the same WLAN.




http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-0/WLAN-Bonjour-DG.html

**QUESTION 6**
Refer to the exhibit. A network administrator is installing a new converged access Cisco WLC. The uplink connection is to be a Gigabit port channel. Which characteristic is true?




A. The port channel mode is set to active and sends PDUs at 30 sec intervals.
B. The port channel mode is set to active and sends PDUs at 1 sec intervals.
C. The port channel uses a Cisco proprietary protocol.
D. The port-channel member interfaces must be set to trunk mode.
E. The port channel is currently down.

**Correct Answer:** A
**Explanation:**


Age Over 1 sec and flag as SA , Slow rate and in Active mode

**lacp rate**

To set the rate at which Link Aggregation Control Protocol (LACP) control packets are ingressed to an LACP-supported interface, use the lacp rate command in interface configuration mode. To return to the default settings, use the no form of this command.

lacp rate {normal | fast}

no lacp rate

syntax description

| | |
|---|---|
| normal | Specifies that LACP control packets are ingressed at the normal rate, every 30 seconds after the link is bundled. |
| fast | Specifies that LACP control packets are ingressed at the fast rate, once every 1 second. |

Command Default

The default ingressed rate for control packets is 30 seconds after the link is bundled.

**Examples**

**Information About LACP Neighbors for a Specific Port Example**

This example shows how to display the information about the LACP neighbors for a specific port channel:

```
Device# show lacp 1 neighbors

Flags:  S - Device sends PDUs at slow rate.     F - Device sends PDUs at fast rate.
        A - Device is in Active mode.           P - Device is in Passive mode.
Channel group 1 neighbors
          Partner                   Partner
Port      System ID                 Port Number     Age     Flags
Fa4/1     8000,00b0.c23e.d84e       0x81            29s     P
Fa4/2     8000,00b0.c23e.d84e       0x82            0s      P
Fa4/3     8000,00b0.c23e.d84e       0x83            0s      P
Fa4/4     8000,00b0.c23e.d84e       0x84            0s      P
          Port          Admin     Oper      Port
          Priority      Key       Key       State
Fa4/1     32768         200       200       0x81
Fa4/2     32768         200       200       0x81
Fa4/3     32768         200       200       0x81
Fa4/4     32768         200       200       0x81
Device#
```

The following table describes the significant fields shown in the display.

Table 4 show lacp neighbors Field Descriptions

| Field | Description |
|---|---|
| Port | Port on which link bundling is configured. |
| Partner System ID | Peer's LACP system identification (sys-id). It is a combination of the system priority and the MAC address of the peer device. |
| Partner Port Number | Port number on the peer device |
| Age | Number of seconds since the last LACP PDU was received on the port |
| Flags | Indicators of device activity. |
| Port Priority | Port priority setting. |
| Admin Key | Defines the ability of a port to aggregate with other ports. |
| Oper Key | Determines the aggregation capability of the link. |
| Port State | Activity state of the port.<br>See the Port State description in the show lacp internal Field Descriptions table for state variables. |

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cether/command/ce-xe-3se-3850-cr-book/ce-xe-3se-3850-cr-book_chapter_00.html

**QUESTION 7**

When configuration an autonoumous access point, which configuration broadcasts two SSIDs?

A. dot11 ssid data1
   vlan 10
   authentication open

authentication key-managerment wpa version 1
wpa-psk ascii cisco123
end
!
dot11 ssid data2
vlan 11
authentication open
authentication key-management wpa version 2
wps-psk accii Cisco12345
end

B. dot11 ssid data1
vlan 10
authentication open
authentication key-management wpa version 1
wpa-psk ascii cisco123
mbssid guest-mode
end
!
dot11 ssid data2
vlan 11
authentication open
authentication key-management wpa version 2
wpa-psk accii Cisco12345
mbssid guest-mode
end

C. mbssid
!
dot11 ssid data1
vlan 10
authentication open
authentication key-management wpa version 1
wpa-psk ascii cisco123
end
!
dot11 ssid data2
vlan 11
authentication open
authentication key-management wpa version 2
wpa-psk accii Cisco12345
end

D. dot11 ssid data1
vlan 10
authentication open
authentication key-management wpa version 1
wpa-psk ascii cisco123
guest-mode
end
!
dot11 ssid data2
vlan 11
authentication open
authentication key-management wpa version 2
wpa-psk ascii cisco12345
guest-mode
end

E. dot11 ssid data1
vlan 10
authentication open
authentication key-management wpa version 1
wpa-psk ascii cisco123
mbssid
end
!
dot11 ssid data2
vlan 11
authentication open
authentication key-management wpa version 2
wpa-psk accii Cisco12345
mbssid
end

**Correct Answer:** B
**Explanation:**

**CLI Configuration Example**

This example shows the CLI commands that you use to enable multiple BSSIDs on a radio interface, create an SSID called *visitor*, designate the SSID as a BSSID, specify that the BSSID is included in beacons, set a DTIM period for the BSSID, and assign the SSID *visitor* to the radio interface:

```
router(config)# interface dot11 0
router(config-if)# mbssid
router(config-if)# exit
router(config)# dot11 ssid visitor
router(config-ssid)# mbssid guest-mode
router(config-ssid)# exit
router(config)# interface dot11 0
router(config-if)# ssid visitor
```

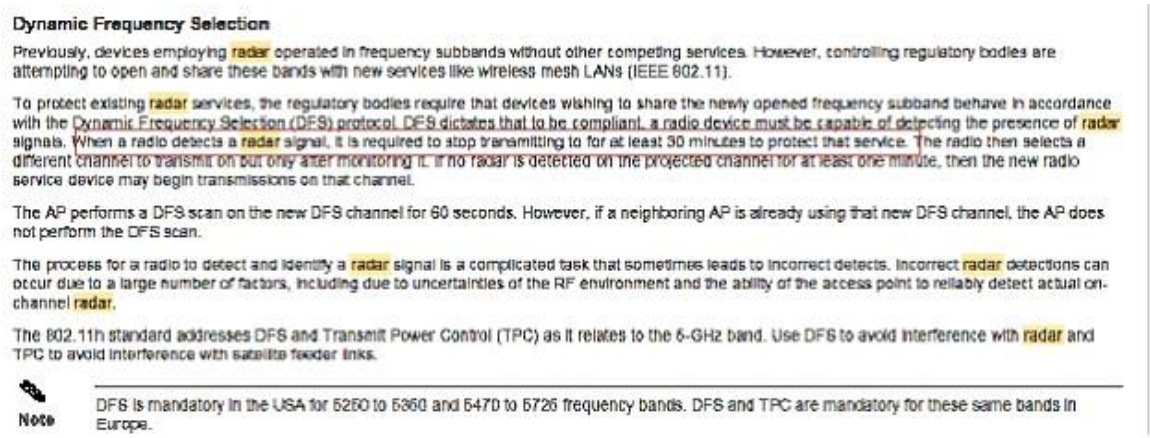
You can also use the **dot11 mbssid** global configuration command to simultaneously enable multiple BSSIDs on all radio interfaces that support multiple BSSIDs.

http://www.cisco.com/c/en/us/td/docs/routers/access/1800/wireless/configuration/guide/awg/s37ssid.pdf

**QUESTION 8**
Which statement about a Cisco Mesh Network when a radar event is detected by the MAP on a mesh tree when coordinated channel change is enabled is true?

A. The MAP immediately stops transmission of the current channel and joins the parent again after 30 minutes after the channel is marked as clean.
B. The MAP continues transmission of the beacons and probes for 10 seconds after the radar detection and suspends operation for the next 30 mins.
C. The MAP propagates radar event information to the RAP in the same BGN. Searchs for a different parent working on a nono-dfs channel and join there.
D. The MAP propagates the radar event information to the RAP and the whole sector moves to the new channel.

**Correct Answer:** B
**Explanation:**
http://www.cisco.com/c/en/us/td/docs/wireless/technology/mesh/8-3/b_mesh_83/Troubleshooting.html



**Dynamic Frequency Selection**

Previously, devices employing radar operated in frequency subbands without other competing services. However, controlling regulatory bodies are attempting to open and share these bands with new services like wireless mesh LANs (IEEE 802.11).

To protect existing radar services, the regulatory bodies require that devices wishing to share the newly opened frequency subband behave in accordance with the Dynamic Frequency Selection (DFS) protocol. DFS dictates that to be compliant, a radio device must be capable of detecting the presence of radar signals. When a radio detects a radar signal, it is required to stop transmitting to for at least 30 minutes to protect that service. The radio then selects a different channel to transmit on but only after monitoring it. If no radar is detected on the projected channel for at least one minute, then the new radio service device may begin transmissions on that channel.

The AP performs a DFS scan on the new DFS channel for 60 seconds. However, if a neighboring AP is already using that new DFS channel, the AP does not perform the DFS scan.

The process for a radio to detect and identify a radar signal is a complicated task that sometimes leads to incorrect detects. Incorrect radar detections can occur due to a large number of factors, including due to uncertainties of the RF environment and the ability of the access point to reliably detect actual on-channel radar.

The 802.11h standard addresses DFS and Transmit Power Control (TPC) as it relates to the 5-GHz band. Use DFS to avoid interference with radar and TPC to avoid interference with satellite feeder links.

Note

DFS is mandatory in the USA for 5250 to 5360 and 5470 to 5726 frequency bands. DFS and TPC are mandatory for these same bands in Europe.

**QUESTION 9**
You have received a new Cisco 5760 Controller and have gone through the initial startup wizard. You are now trying to add APs to the controller, but these are not joining. Which three checks should you do next? (Choose three.)

A. Check that the radios are not in a shutdown state.
B. Check the country code of the controller. The APs do not join the controller if the country code does not match.
C. Check that the correct time is set on the controller.
D. Check that option 53 has been set in the DHCP scope.
E. Check that the controller has enough AP licenses.
F. Check that the controller has been configured with the correct hostname. Otherwise, DNS resolution fails.

**Correct Answer:** BCE

**QUESTION 10**
You are the network administrator for ACME corporation. Your organization has deployed a single Cisco 5500 Series Wireless Controller with 100 Cisco Aironet 3500 Series Aps. A new IT member is worried that most of these Aps are working at a power level3 on the 5GHz radio specially. As this power level setting is causing issues in your wireless network. Which option describes the likely cause of this behavior?

A. The WLC has been recently rebooted, which causes the TPC algorithm to set power level 3 on all APs for 90 seconds.
B. The controller TPC algorithm seems to have a problem. It might have been set to work in TPCv2 mode instead of TPCvl.
C. The WLC is misconfigured because the static power of level 3 has been set for all the APs under TPC settings.
D. Cisco 7925 wireless IP Phones are in use and the DTPC feature is enabled on the 5 GHz radio.

**Correct Answer:** D
**Explanation:**
Tx Power
Num Of Supported Power Levels ..... 5
Tx Power Level 1 ..... 18 dBm
Tx Power Level 2 ..... 15 dBm

Tx Power Level 3..... 12 dBm
Tx Power Level 4 ..... 9 dBm
Tx Power Level 5 ..... 6 dBm

https://supportforums.cisco.com/discussion/11635606/power-level-wlc

**QUESTION 11**
Which two statements about AP Local Authentication by FlexConnect AP in standalone mode are true? (Choose two)

A. From AireOS release 8.0, Cisco Extended Keying Groups (CEKG) is a supported Local Authentication Protocol when deploying FlexConnect.
B. Only LEAP, EAP-FAST, PEAP, and EAP-TLS authentications are supported.
C. Cisco Wireless LAN Controller must generate a certificate signing request by itself for submitting to a certificate authority for signing.
D. Only the vendor Certificate Authority (CA) certificate has to be downloaded to the Cisco Wireless LAN Controller for EAP-TLS authentication.
E. When using EAP-TLS, a FlexConnect Group must be created so that the Cisco Wireless LAN Controller can push the certificates to the FlexConnect AP in the FlexConnect Group.

**Correct Answer:** BE

**QUESTION 12**
On a Cisco autonomous AP, the maximum number of attempts to send a packet (packet retries) is set to 32 by default. Which statement about the result when the AP has tried to send a packet for that number of attempts and no response is received from the client is true?

A. The access point drops the packet.
B. The client MAC address is excluded for 60 seconds.
C. The access point resets the radio interface.
D. The access point disassociates the client.

**Correct Answer:** A
**Explanation:**
Packet Retries & Max-Retries I mrn-cciew
https://mrncciew.com/2013/06/16/packet-retries-max-retries/
In Autonomous(IOS) AP, you can configure number of attempts the wireless device makes to send a packet before giving up & dropping the packet. There are two ways of configuring this feature. One method for best effort (priority value 0) traffic & another method for non- best effort (priority value 1-7)
1. Best-effort Traffic (packet retries command)
2. N on-Best-effort Traffic (packet max-retries command )

CLI default:
packet retries 32 drop-packet
channel width 40-above
channel dfs station-role
root rts retries 32

cfg:
http://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3-3/cg15-3-3-chap6-radio.html

Configuring the Maximum Data Packet Retries
The maximum data retries setting determines the number of attempts the makes to send a packet before giving up and dropping the packet. The default setting is 32. Beginning in privileged EXEC mode.

**QUESTION 13**
Prime Infrastructure will trigger alarms indicating that the Prime Infrastructure physical or virtual server is low on disk space. As the administrator, Which three actions can you take to increase disk space immediately upon receiving a Major alert ( 60 percent disk usage)? (Choose three.)

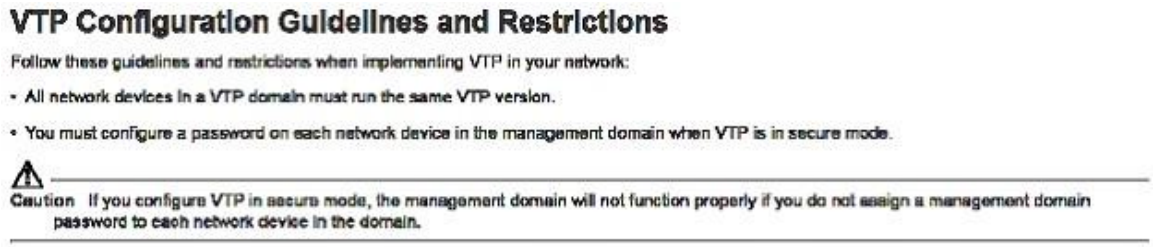
A. Enable cron job on ade for disk clean up using $du -sh.
B. Change the disk controller RAID.
C. Conpacting the PI database using the ncs database purge command.
D. Reduce the storage load on the local disk by setting up and using remote trackup reponitories.
E. Reduce the length of time you store client association data and related events.
F. Compacting the PI database using the ncs cleanup command.

**Correct Answer:** DEF

**QUESTION 14**
You have been hired to install new Cisco switches at ACME Corporation. The company has an existing Cisco network comprised of access layer switches that use multiple VLANs and VLAN trunking protocol to distribute the VLANs to the switches throughout the network. Which two methods are best to accomplish your task? (Choose two.)

A. Configure the VLAN Trunking Protocol pruning on the new switches because they may not need all of the VLANs.
B. Prior to installation, ensure that all switches are running the same Cisco IOS software version as the VTP server.
C. Ensure that all the new Cisco switches have their VTP domain name set to the default value of null
D. Configure one of the new switches as a VTP server to distribute the VLANs appropriately.
E. Ensure that all switches have the same VLAN Trunking Protocol password and encryption level.
F. Configure all new switches as VTP clients and relocated switches as VTP server because the already have all the VLANs in their database.
G. Ensure that all switches are running the same VTP version.

**Correct Answer:** EG
**Explanation:**



**VTP Configuration Guidelines and Restrictions**

Follow these guidelines and restrictions when implementing VTP in your network:

- All network devices in a VTP domain must run the same VTP version.
- You must configure a password on each network device in the management domain when VTP is in secure mode.

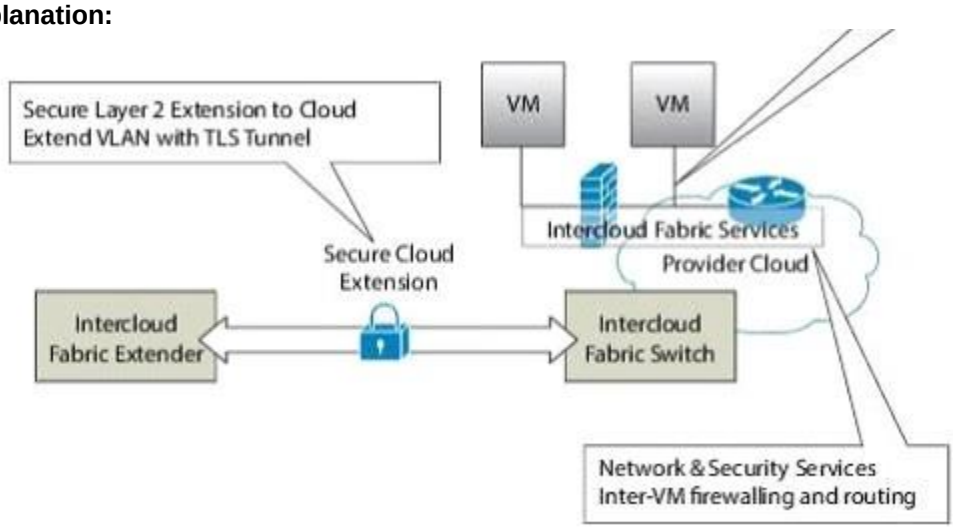
**Caution** If you configure VTP in secure mode, the management domain will not function properly if you do not assign a management domain password to each network device in the domain.

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vtp.html#wp1034490

**QUESTION 15**
Which option describes the function of the Intercloud Fabric Extender?

A. It provides the network overlay functionality between the used clouds or cloud models.
B. It establishes a secure site-to-site tunnel to the intercloud fabric agent in the private cloud.
C. It applies network policies and collects and reports VEM-related intercloud statistics.
D. It establishes a secure site-to-site tunnel to the intercloud fabric switch in the provider cloud.

**Correct Answer:** D
**Explanation:**




**Intercloud Fabric Extender**

The Intercloud Fabric Extender is a virtual machine that runs in the private cloud. It is responsible for establishing a secure tunnel for interconnecting the Intercloud Fabric components in the private cloud with the provider cloud. The main functions of the Intercloud Fabric Extender are as follows:

- Establishes a secure tunnel to interconnect all of the cloud resources.
- Interacts with the virtual switch, such as the Cisco Nexus 1000V, at the private cloud.

**Cisco Intercloud Fabric Agent**

The Cisco Intercloud Fabric Agent (ICA) provides a network overlay for the VMs in the cloud. It secures the guest VM traffic in the cloud and abstracts the cloud infrastructure. It is deployed in the provider cloud as a secure tunnel driver that runs within the cloud VM's operating system. It also redirects network traffic to the secure overlay network as follows:

- Establishes a secure tunnel to connect to an Intercloud Fabric Switch that allows VMs in the cloud to communicate with private cloud VMs and provider cloud VMs.
- Collects secure overlay-related statistics.

**Intercloud Fabric Switch**

The Intercloud Fabric Switch is a virtual machine that runs in the provider cloud. It is responsible for establishing secure tunnels for connecting VMs in the provider cloud to the private cloud VMs and other VMs in the cloud. The main functions of the Intercloud Fabric Switch are as follows:

- Runs the Virtual Ethernet Module (VEM) to provide the Cisco Nexus 1000V functions.
- Establishes a secure tunnel to connect the VEM with Intercloud Fabric Extender.
- Establishes secure tunnels to connect all of the cloud VMs.
- Monitors and reports statistics of VMs in the cloud.
- Monitors and reports any component failures in the cloud to Cisco Prime Network Services Controller (PNSC).

The VEM is embedded in the Intercloud Fabric Switch and is responsible for the following:

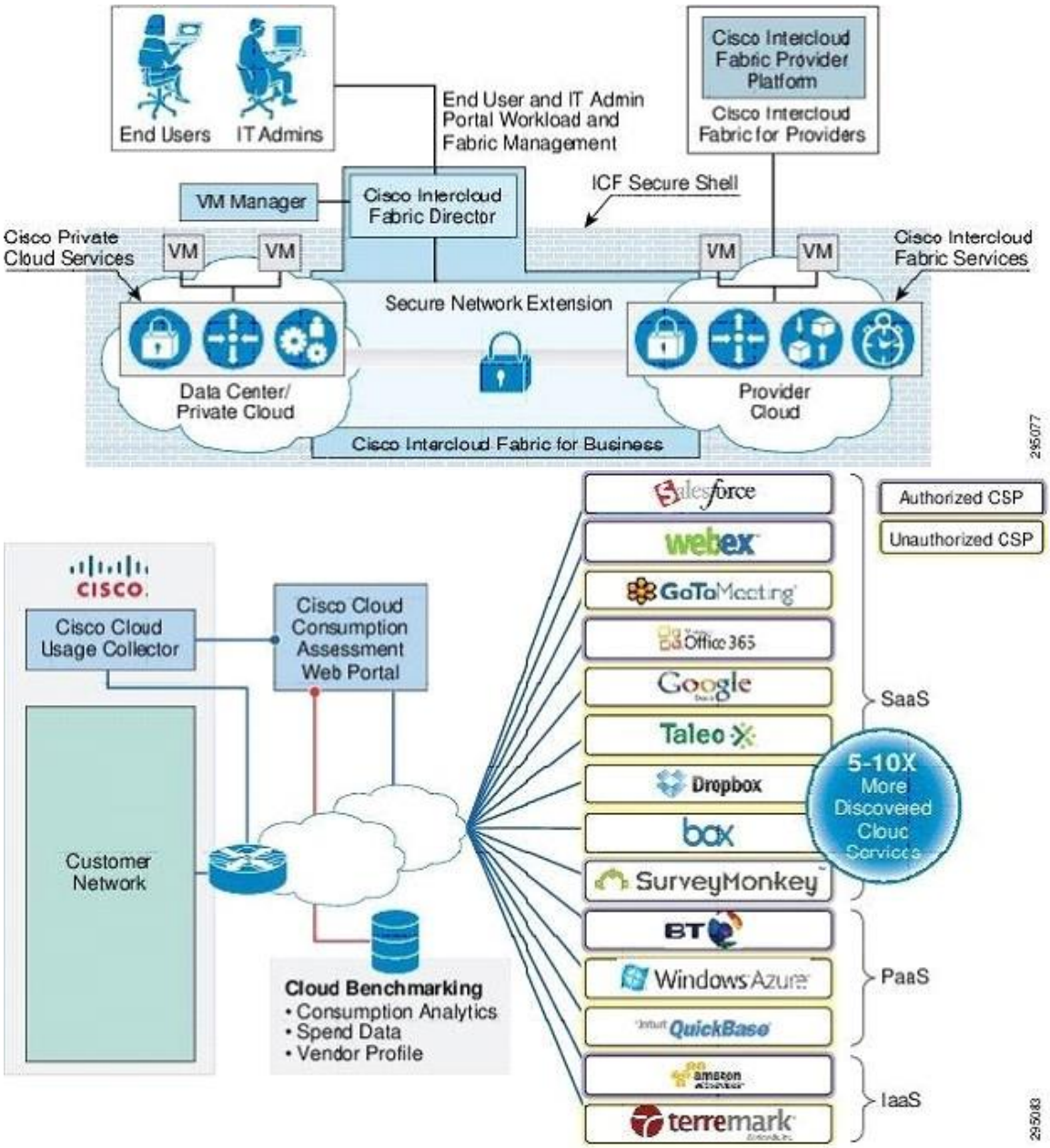
- Communicates with the Virtual Supervisor Module (VSM) function that runs at the private cloud for retrieving VM-specific network policies such as port profiles.
- Switches the network traffic between cloud VMs.
- Switches the network traffic between cloud VMs and the private cloud.
- Applies network policies to any switching network traffic.
- Collects and reports VEM-related statistics.

http://www.cisco.com/c/en/us/td/docs/cloud-systems-management/cisco-intercloud-fabric/cisco-intercloud-fabric-for-business/2-3-1/getting-started-guide/b_Cisco_Intercloud_Fabric_Getting_Started_Guide_Release_2_3_1/b_Cisco_Intercloud_Fabric_Getting_Started_Guide_Release_2_3_1_chapter_00.pdf

Cisco Inter cloud Fabric Architectural Overview - Cisco

http://www.cisco.com/c/en/us/td/docs/solutions/Hybrid_Cloud/Intercloud/Intercloud_Fabric/Intercloud_Fabric_2.html

Cisco Intercloud Fabric Secure Extension
All data in motion is cryptographically isolated and encrypted within the Cisco Intercloud Fabric Secure Extender. This data includes traffic exchanged between the private and public clouds (site to site) and the virtual machines running in the cloud (VM to VM). A Datagram Transport Layer Security (DTLS) tunnel is created between these endpoints to more securely transmit this data. DTLS is a User Datagram Protocol (UDP)-based highly secure transmission protocol. The Cisco Intercloud Fabric Extender always initiates the creation of a DTLS tunnel.
The encryption algorithm used is configurable, and different encryption strengths can be used depending on the level of security desired. The encryption algorithm used is configurable, and different encryption strengths can be used depending on the level of security desired.




**QUESTION 16**
Which two statements about VXLAN are true? (Choose two.)

A. VXLAN overcomes the 802.1Q virtual LAN address space limitation.
B. VXLAN is an encapsulation method used to create a Layer 3 overlay network
C. VXLAN uses the Spanning Tree Protocol for loop prevention.
D. VXLAN is a Cisco proprietary standard.
E. VXLAN can be used to enforce Layer 2 isolation in a multitenant infrastructure.

**Correct Answer:** AE
**Explanation:**
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-pap

er-c11-729383.html

**QUESTION 17**
When a Flex Connect AP is in the "local authentication, local switching" state, it handles client authentication and switches client data packets locally. This state is valid in standalone mode and connected mode. Which three statements about a FlexConnect AP are true? (Choose three).

A. In connected mode, the AP provides minimal information about the locally authenticated client to the controller. This information is not available on the controller policy type. Access VLAN. VLAN name, supported rates. Encryption ciphter.
B. In connected mode, the access point provides minimal information about the locally authenticated client to the controller. However, this information is available to the controller policy type., access VLAN, VLAN name, supported rates, encryption cipher.
C. Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 100 ms and the maximum transmission unit no smaller than 576 bytes.
D. Local authentication is useful where you cannot maintain a remote office setup of a minimum bandwidth of 128 kbps with the round-trip latency no greater than 150 ms and the maximum transmission unit no higher than 500 bytes.
E. Local authentication in connected mode does not require any WLAN configuration.
F. Local authentication can be enabled only on the WLAN of a FlexConnect AP that is in local switching mode.

**Correct Answer:** ACF
**Explanation:**
http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-2/configuration/guide/cg/cg_flexconnect.html

**QUESTION 18**
Which four options are the HTTP methods supported by a reset API?

A. RETRIEVE
B. GET
C. PUT
D. DELETE
E. COPY
F. POST
G. SET

**Correct Answer:** BCDF

**QUESTION 19**
Which three types of ACLs are supported by the Cisco 5760 WLC? (Choose three.)

A. Port ACLs.
B. VLAN ACLs(VLAN maps).
C. Router port ACLs.
D. AP Radio ACL Switch port ACLs.
E. Router ACLs.

**Correct Answer:** ABE
**Explanation:**
http://www.cisco.com/c/en/us/td/docs/wireless/controller/5700/software/release/3se/security/configuration_guide/b_sec_3se_5700_cg/b_sec_1501_3850_cg_chapter_01010.html#ID6

ACL Precedence
Port ACLs
Router ACLs
VLAN Maps

**QUESTION 20**
You are the network administrator of a Cisco Autonomous AP deployment. You want to stop a client with MAC address 5057.a89e.b1f7 and IP address 10.0.0.2 from associating to your APs. Which configuration do you use ?

A. access-list 700 permit 5057.a89e.b1f7 0000.0000.0000 !
dot11 association mac-list 700
B. ip access-list 25 deny host 10.0.0.2
!
interface Dot11Radio0
ip access-group 25 out
!
interface Dot11Radio1
ip access-group 25 out
C. ip access-list 25 deny host 10.0.0.2
!
interface Dot11Radio0
ip access-group 25 in
!
interface Dot11Radio1
ip access-group 25 in
D. access-list 700 deny 5057.a89e.b1f7 0000.0000.0000 !
dot11 association on mac-list 700

**Correct Answer:** D