Cisco

400-351 Exam

Cisco CCIE Wireless Exam

Version: 18.0

Question: 1

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

Answer: B C D F

Question: 2

Refer to the exhibit.

Which option describes what this sequence of commands achievers on a Cisco Autonomus AP?

A. This example shows how to permit SNMP access to all objects with read-only permission to only those three specific IP addresses using the community string public. The access point also sends config traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string public is not sent with the traps because is the default community value.
B. This example shows how to permit SNMP access to all objects with read-only permission to only those three specific IP addresses using the community string public. The access point also sends config traps to the hosts 192.180.1.111 and 192.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string public is not sent with the traps.
C. This example shows how to permit any SNMP manager to access all objects with read-only permission using the community string public. The access point also sends config traps to the hosts 192.180.1.111 and 190.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string public is not sent with the traps as this is the default community value.
D. This example shows how to permit any SNMP manager to access to all objects with read-only

permission using the community string public. The access point also sends config traps to the hosts 192.180.1.111 and 190.180.1.33 using SNMPv1 and to the host 192.180.1.27 using SNMPv2C. The community string public is sent with the traps.

Answer: D

Explanation:

5. Use this command in order to enable the Read-only (RO) community string:

```
Router(config)#snmp-server community public RO
```

where "public" is the Read-only community string.

6. Use this command in order to enable the Read-write (RW) community string:

Router(config)#**snmp-server community private RW**

where "private" is the Read-write community string.

7. Exit out of the configuration mode and return to the main prompt:

```
Router(config)#exit
Router#
```

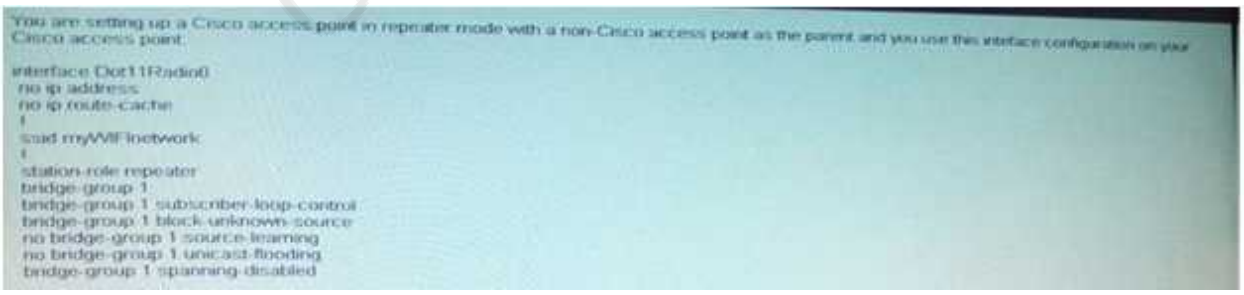
http://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7282-12

Confirmed: test in my demo switch, public default is ro

```
DEMO_SW(config)# snmp-server community public
DEMO_SW(config)#exi
DEMO_SW#sh run all | in public
snmp-server community publicv1default RO
```

Question: 3

Refer to the exhibit.



You are getting the following error message. Which reason for this issue true?
%DOT11-4-CANT_ASSOC Interface Dot 11 Radio0. Cannot associate NO Aironet Extension IE.

A. "dot11 extension " is missing under the interface Dot11Radio 0 interface.
B. When repeater mode is used, unicast-flooding must be enabled to allow Aironet IE communications.
C. The parent AP MAC address has not been defined.
D. Repeater mode only works between Cisco access point.

Answer: A

Explanation:

This example shows how to set up a repeater acess point with three potential parents:

```
AP# configure terminal
AP(config)# interface dot11radio 0
AP(config-if)# ssid chicago
AP(config-ssid)# infrastructure-ssid
AP(config-ssid)# exit
AP(config-if)# station-role repeater
AP(config-if)# dot11 extensions aironet
AP(config-if)# parent 1 0987.1234.h345 900
AP(config-if)# parent 2 7809.b123.c345 900
AP(config-if)# parent 3 6543.a456.7421 900
AP(config-if)# end
```

http://www.cisco.com/c/en/us/td/docs/wireless/access_point/12-2_11_JA/configuration/guide/b12211sc/s11rep

Question: 4

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.

Answer: BCE

Explanation:

AP Join

Before connecting your Access Points to the network, ensure licenses and the correct time is set on the controller.

Licenses

Licenses are based on the Right-To-Use license model (per AP license price for the CT5760 controller).

You must add the AP licenses you purchased and accept the EULA before connecting your APs. This is how you can do it:

WLC5760#license right-to-use activate apcount 510 slot 1 acceptEULA

Once you apply it, you can check the AP license information using the CLI:

WLC5760#show license right-to-use

Slot# License name Type Count Period left

---

1 apcount adder 510 Lifetime

You can also add evaluation licenses for testing purposes:

WLC5760#license right-to-use activate apcount evaluation acceptEULA

For additional license information, please refer to the Cisco Right to Use Licensing FAQ.

Enable Network Time Protocol (NTP) and Setup Time

NTP is very important for several features. It is mandatory to use NTP synchronization on controllers if you use any of these features—Location, SNMPv3, access point authentication, or MFP. The WLC supports synchronization with NTP using authentication.

You can setup NTP during the Initial Wizard configuration. To enable the NTP server use the following command:

WLC5760(config)#ntp server <ip_address>

Controller Time:

It is important to setup the correct time on the controller so that the AP can join the controller.

WLC5760#clock set hh:mm:ss day month year

Country Code settings:

Ensure that you have the correct Country Code set on your controller. To see the current Country Code configured on your controller, please issue the following CLI:

WLC5760(config)#show wireless country configured

Configured Country.....: US - United States

Question: 5

You are installing Converged Access controllers that run Cisco IOS-XE and you are ready to implement QoS. From the below, choose all the possible QoS target levels that would apply to downstream traffic (toward the client)?

A. Client, SSID, Radio, Port
B. Client, SSID, Radio
C. Client, Radio
D. Client, SSID

Answer: A

Explanation:

Restrictions for Wireless QoS

General Restrictions

- A target is an entity where a policy is applied. You can apply a policy to either a wired or wireless target. A wired target can be either a port, client, or VLAN. A wireless target can be either a port, SSID, client, or radio. Wireless QoS policies for port, SSID, client, and radio are applied in the downstream direction. That is, when traffic is flowing from the switch to wireless client. Only port, SSID, and client (using AAA and Cisco IOS command-line interface) policies are user-configurable. Radio policies are set by the wireless control module and are not user-configurable.
- Port and radio policies are applicable only in the downstream direction (traffic flowing from a wired source to a wireless target).
- SSID and client support non-queuing policies in the upstream direction. SSID and client targets can be configured with marking and policing policies.
- One policy per target per direction is supported.
- For marking rules for access points associated with the switch, the following rules apply:
  - Policing at the access point is not supported.
  - Client policies that are passed to the access points in the upstream direction are not supported.
  - The following rules apply for QoS at the SSID:
    - One table map is supported at the ingress policy.
    - Up to three table maps can be configured in the egress direction for SSID when a QoS-group is involved.

http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_010010

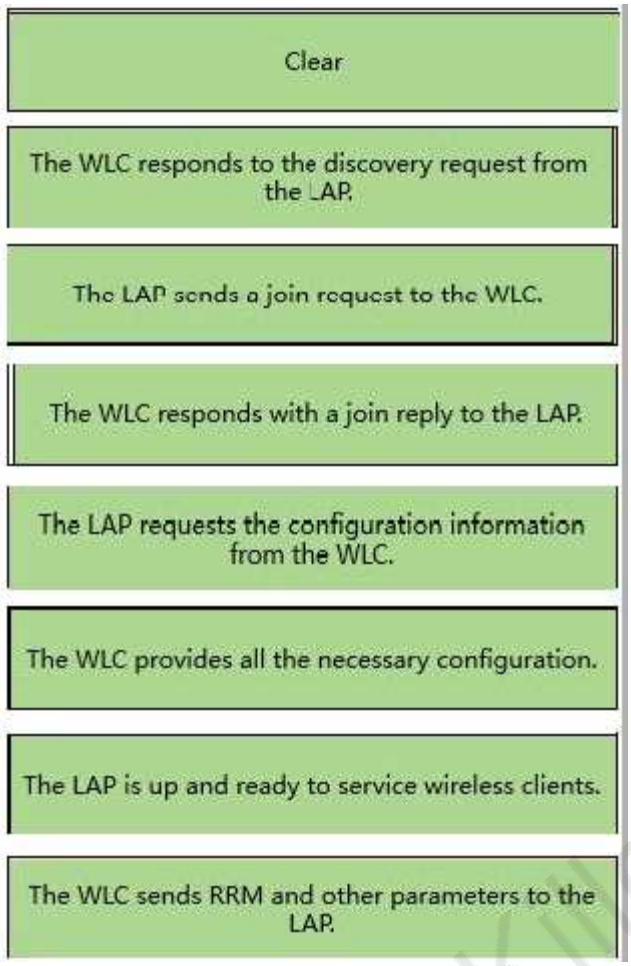
Question: 6

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

Answer:



Question: 7

Which memchanism incorporates the channel capacity into the CAC determination and gives a much more accurate assessment of the current call carrying capacity of the AP?

A. Static CAC
B. Reserved roaming bandwidth(%).
C. Expedited bandwidth.
D. Metrics collection.
E. Load-based AC
F. Max RF bandwidth (%).
G. Admission control.

Answer: E

Explanation:
AP Call Capacity
A key part of the planning process for a VoWLAN deployment is to plan the number of simultaneous voice streams per AP. When planning the voice stream capacity of the AP, consider the following points:

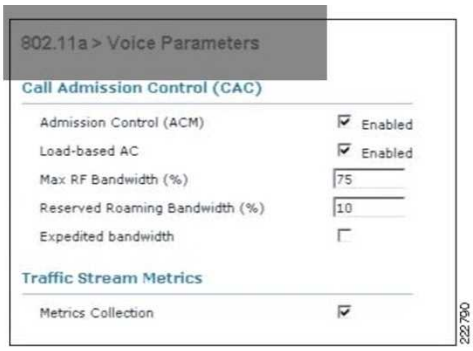
Note: A call between two phones associated to the same AP counts as two active voice streams.
The actual number of voice streams a channel can support is highly dependent on a number of issues, including environmental factors and client compliance to WMM and the Cisco Compatible Extension specifications. Figure 9-11 shows the Cisco Compatible Extension specifications that are most beneficial to call quality and channel capacity. Simulations indicate that a 5 GHz channel can support 14-18 calls. This means a coverage cell can include 20 APs, each operating on different channels, with each channel supporting 14 voice streams. The coverage cell can support 280 calls. The number of voice streams supported on a channel with 802.11b clients is 7; therefore, the coverage cell with three APs on the three non-overlapping channels supports 21 voice streams.
Figure 9-11 Cisco Compatible Extension VoWLAN Features

How Cisco Compatible Extensions Benefits VoWLAN Call Quality	
Feature	**Benefit**
CCKM Support for EAP-Types	Locally Cached Credentials Means Faster Roams
Unscheduled Automatic Power Save Delivery (U-APSD)	More Channel Capacity and Better Battery Life
TSPEC-Based Call Admission Control (CAC)	Managed Call Capacity for Roaming and Emergency Calls
Voice Metrics	Better and More Informed Troubleshooting
Neighbor List	Reduced Client Channel Scanning
Load Balancing	Calls Balanced Between APs
Dynamic Transmit Power Control (DTPC)	Clients Learn a Power to Transmit At
Assisted Roaming	Faster Layer 2 Roams

210352

Call Admission Control (CAC) also benefits call quality and can create bandwidth reservation for E911 and roaming calls.
The 802.11e, WMM, and Cisco Compatible Extension specifications help balance and prevent the overloading of a cell with voice streams. CAC determines whether there is enough channel capacity to start a call; if not, the phone may scan for another channel. The primary benefit of U-ASPD is the preservation of WLAN client power by allowing the transmission of frames from the WLAN client to trigger the forwarding of client data frames that are being buffered at the AP for power saving purposes. The Neighbor List option provides the phone with a list that includes channel numbers and channel capacity of neighboring APs. This is done to improve call quality, provide faster roams, and improve battery life.
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper/preface41
Understanding Static CAC
As mentioned previously, there are two types of Admissions Control. Static CAC is based on a percentage of the total Medium Times available and is measure in increments of 32 microseconds. In this section, we will cover how to configure Static and Load-Based CAC and also how to debug it.
http://www.cisco.com/c/en/us/td/docs/wireless/technology/vowlan/troubleshooting/vowlan_troubleshoot/5_Troubleshooting_CAC_Rev1-2
Load-Based CAC on the other hand is significantly more difficult to debug. LBCAC is dynamic with

regard to the algorithm used to decrement Medium Times from the total that is available. LBCAC takes into consideration different metrics, such as load, Co-channel interference, SNR, etc. and will therefore yield different results when tested. From our experience, it is very difficult to yield consistent results as RF fluctuates and changes within the given environment. Results tend to vary from one cell area to another and even in cell areas that yield the same signal strength.
http://www.cisco.com/c/en/us/td/docs/wireless/controller/4-1/configuration/guide/ccfig41/c41ccfg
o enable video CAC for this radio band, check the Admission Control (ACM) check box. The default value is disabled.
n the Reserved Roaming Bandwidth field, enter the percentage of maximum allocated bandwidth reserved for roaming video clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming video clients.
Range: 0 to 25%
Default: 0%
in the Reserved Roaming Bandwidth field, enter the percentage of maximum allocated bandwidth reserved for roaming voice clients. The controller reserves this much bandwidth from the maximum allocated bandwidth for roaming voice clients.
Range: 0 to 25%
Default: 6%
To enable expedited bandwidth requests, check the Expedited Bandwidth check box.
The default value is disabled.
To enable TSM, check the Metrics Collection check box. The default value is disabled.
Traffic stream metrics (TSM) can be used to monitor and report issues with voice quality.
In the Max RF Bandwidth field, enter the percentage of the maximum bandwidth allocated to clients for voice applications on this radio band. Once the client reaches the value specified, the access point rejects new calls on this radio band.
Range: 40 to 85%
Default: 75%



For best performance, the most accurate assessment of call capacity—*Load-based AC*—should be enabled. *Admission Control* enabled by itself uses the APs capacity to calculate the Call Admission Control (CAC). Load-based AC incorporates the channel capacity into the CAC determination and gives a much more accurate assessment of the current call-carrying capacity of the AP. Settings for the *Max RF bandwidth* and *Reserved Bandwidth* values depend on the VoWLAN handsets, the data rates used, and the other sources of the WLAN load. However, the Max RF Reservation should not be greater than 60 percent. At levels greater than 60 percent, the IEEE 802.11 protocol itself can start to be under stress with increases in retransmission. This can impact call quality even if WMM is being used, particularly if the is a number of voice calls are already in progress. Testing with the Cisco Unified IP Phone 7921G in both the 2.4 GHz and 5 GHz bands using the recommended signal levels and SNR suggests that the minimum value for the *Maximum Bandwidth Reservation* parameter of between 40 to 60 percent is also the best setting for this specific phone. Call quality starts to deteriorate when the *Max RF Bandwidth* is set at or below these levels.

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Mobility/vowlan/41dg/vowlan41dg-book/vowlan_ch8.pdf

Question: 8

On a Cisco 5760 WLC, which of the below is not part of the initial setup script?

A. Wireless management interface
B. Host name
C. HTTP server login account
D. SNMP Network Management
E. NTP server
F. Enable password
G. Default routing protocol

Answer: G

Explanation:
From:
CT5760 Controller and Catalyst3850 Switch Configuration Example - Cisco http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-vlan/116342-config-wlc-00
5760 WLC Initial Configuration
This section outlines the steps to succesfully configure the 5760 WLC in order to host wireless services.
Configure
Setup Script
--- System Configuration Dialog ---
Enable secret warning

In order to access the device manager, an enable secret is required
If you enter the initial configuration dialog, you will be prompted for the enable secret
If you choose not to enter the intial configuration dialog, or if you exit setup without setting the enable secret,
please set an enable secret using the following CLI in configuration mode- enable secret 0 <cleartext password>

Would you like to enter the initial configuration dialog? [yes/no]: yes
At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt. Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
Enter host name [Controller]: w-5760-1
The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after
entered, becomes encrypted in the configuration.
Enter enable secret: cisco
The enable password is used when you do not specify an
enable secret password, with some older software versions, and some boot images.
Enter enable password: cisco
The virtual terminal password is used to protect access to the router over a network interface.
Enter virtual terminal password: cisco
Configure a NTP server now? [yes]: Enter ntp server address : 192.168.1.200
Enter a polling interval between 16 and 131072 secs which is power of 2:16
Do you want to configure wireless network? [no]: no
Setup account for accessing HTTP server? [yes]: yes
Username [admin]: admin
Password [cisco]: cisco
Password is UNENCRYPTED.
Configure SNMP Network Management? [no]: no
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	NO	unset	up	up
GigabitEthernet0/0	unassigned	YES	unset	up	up
Te1/0/1	unassigned	YES	unset	up	up
Te1/0/2	unassigned	YES	unset	down	down
Te1/0/3	unassigned	YES	unset	down	down
Te1/0/4	unassigned	YES	unset	down	down
Te1/0/5	unassigned	YES	unset	down	down
Te1/0/6	unassigned	YES	unset	down	down

Enter interface name used to connect to the
management network from the above interface summary: vlan1
Configuring interface Vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: 192.168.1.20

Subnet mask for this interface [255.255.255.0] : 255.255.255.0
Class C network is 192.168.1.0, 24 subnet bits; mask is /24
Wireless management interface needs to be configured at startup
It needs to be mapped to an SVI that's not Vlan 1 (default)
Enter VLAN No for wireless management interface: 120
Enter IP address :192.168.120.94
Enter IP address mask: 255.255.255.0
The following configuration command script was created:
w-5760-1
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY^Q
enable password cisco line vty 0 15
password cisco
ntp server 192.168.1.200 maxpoll 4 minpoll 4 username admin privilege 15 password cisco
no snmp-server
!
no ip routing
!
interface Vlan1 no shutdown
ip address 192.168.1.20 255.255.255.0
!
interface GigabitEthernet0/0 shutdown
no ip address
!
interface TenGigabitEthernet1/0/1
!
interface TenGigabitEthernet1/0/2
!
interface TenGigabitEthernet1/0/3
!
interface TenGigabitEthernet1/0/4
!
interface TenGigabitEthernet1/0/5
!
interface TenGigabitEthernet1/0/6
vlan 120
interface vlan 120
ip addr 192.168.120.94 255.255.255.0 exit
wireless management interface Vlan120
!
end
[0] Go to the IOS command prompt without saving this config. [1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit. Enter your selection [2]: 2
Building configuration...
Compressed configuration from 2729 bytes to 1613 bytes[OK]
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started!

Question: 9

A Cisco Unified 7925G Wireless IP Phone is operating on the 5 GHz band and transmitting at a power level of 40 mW. Which configuration must be done on the controller to avoid one-way audio?

A. In DCA, enable UNH-1 channels only.
B. Set the maximum power level assignment to 26 dBm.
C. In DCA, enable UNII-II channels only.
D. Set the maximum power level assignment to 16 dBm.

Answer: D

Explanation:
https://www.cisco.com/c/en/us/support/docs/collaboration-endpoints/unified-wireless-ip-phone-7925g/200032-How-to-get-your-792x-wireless-phones-per

Question: 10

Which two effects does TSPEC-based admission control have as it relates to WMM clients?(Choose two.)

A. Deny clients access to the VLAN that do not support WMM.
B. Allow access only for VoWLAN traffic when interference is detected.
C. Enforce airtime entitilement for wireless voice applications.
D. Ensure that call quality does not degrade for existing VoWLAN calls.
E. Deny clients access to the WLAN if they do not comply with the TERP standard.

Answer: BE

Thank You for trying 400-351 PDF Demo

To Buy Latest 400-351 Full Version Download visit link below

https://www.certkillers.net/Exam/400-351

Start Your 400-351 Preparation