IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

http://www.itrenzheng.com

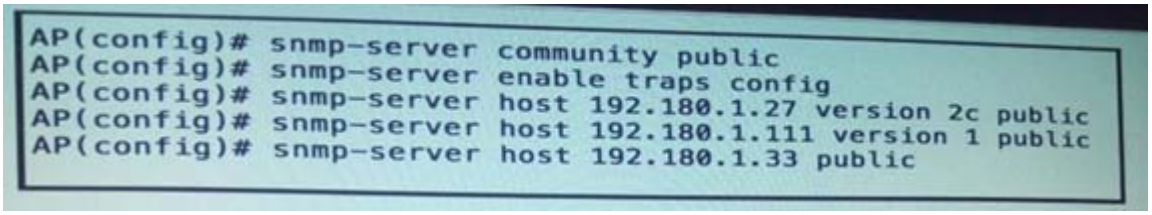
Exam : **400-351**

Title : CCIE Wireless Written Exam

Version : DEMO

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

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.html

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
```

3.

```
You are setting up a Cisco access point in repeater mode with a non-Cisco access point as the parent and you use this interface configuration on your
Cisco access point.

interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid myWifinetwork
 !
 station-role repeater
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
```

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.html

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

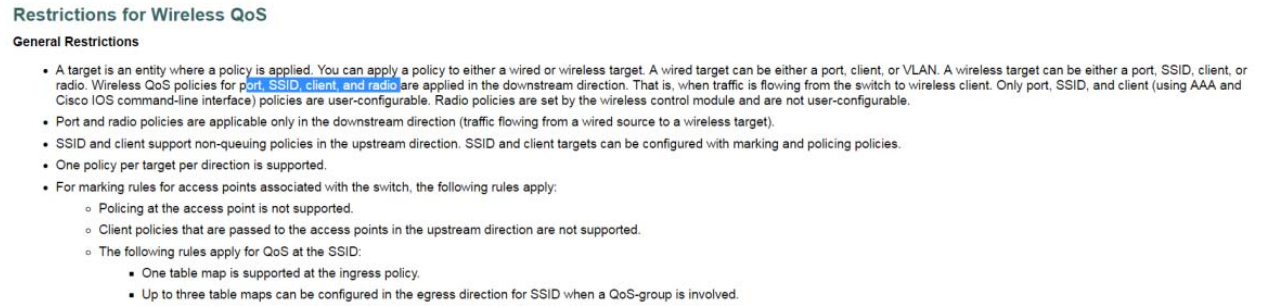
5.You are installing Converged Access controllers that run Cisco IOS-XE and you are ready to implement QoS. From the below, choose all the possible QoS target levels that would apply to downstream traffic (toward the client)?A. Client, SSID, Radio, Port
B. Client, SSID, Radio

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.html