Vendor: Cisco

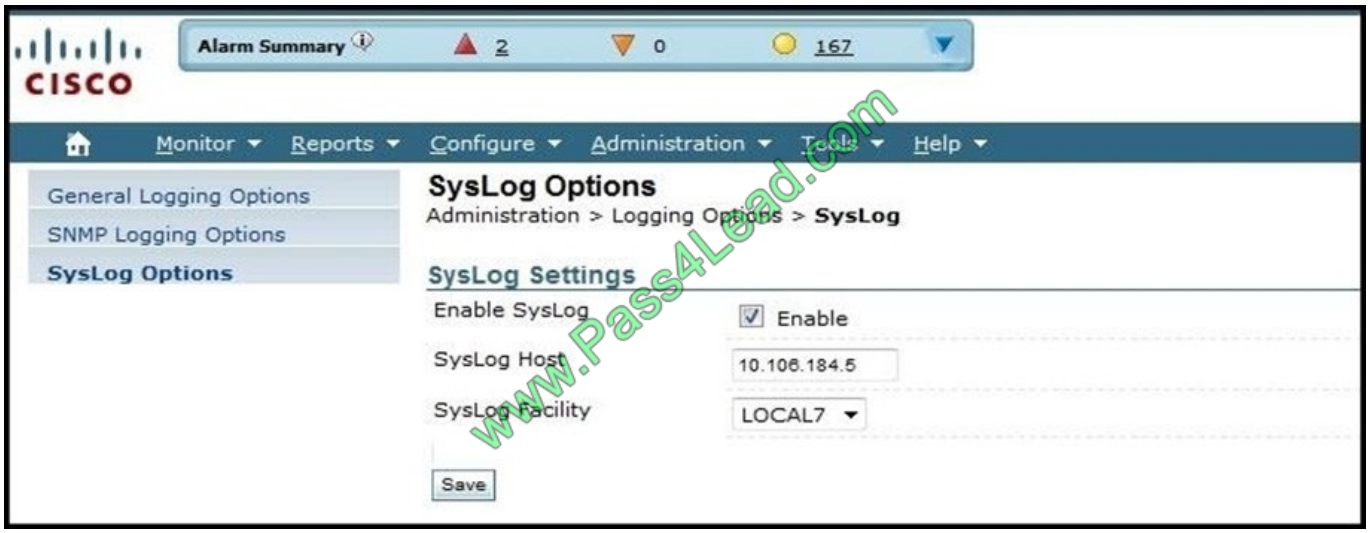
Exam Code:200-355

Exam Name: Implementing Cisco Wireless Network Fundamentals

Version: Demo

QUESTION 1

Refer to the exhibit.



Which syslog facility option is shown?

A. an information field, which is added to every message that comes from the WLC

B. a security feature, which is set on the syslog server

C. the type of syslog server

D. the Cisco WLC identifier for this syslog server

Correct Answer: A

A facility level is used to specify what type of program is logging a message. This lets the configuration file specify that messages from different facilities will be handled differently. Local7 maps to Facility level 23, which is local so the WLC will add this information to syslog messages when sending to the syslog server.

QUESTION 2

What are four features of WPA? (Choose four.)

A. a larger initialization vector, increased to 48 bits

B. a message integrity check protocol to prevent forgeries

C. authenticated key management using 802.1X

D. support for a key caching mechanism

E. unicast and broadcast key management

F. requires AES-CCMP

Correct Answer: ABCE

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function that combines the secret root key with the initialization vector before passing it to the RC4 initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP related key attacks. Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit Message Integrity Check (MIC). To be able to run on legacy WEP hardware with minor upgrades, TKIP uses RC4 as its cipher. TKIP also provides a rekeying mechanism. TKIP ensures that every data packet is sent with a unique encryption key. Key mixing increases the complexity of decoding the keys by giving an attacker substantially less data that has been encrypted using any one key. WPA2 also implements a new message integrity code, MIC. The message integrity check prevents forged packets from being accepted. Under WEP it was possible to alter a packet whose content was known even if it had not been decrypted. http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol
http://documentation.netgear.com/reference/fra/wireless/WirelessNetworkingBasics-3-14.html

---

QUESTION 3

Which wireless client attempts to authenticate by using 802.1X?

A. supplicant

B. authenticator

C. EAP

D. RADIUS

Correct Answer: A

802.1x is an Institute of Electrical and Electronics Engineers (IEEE) standard that provides an authentication framework for WLANs. 802.1x uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. The authentication protocols that operate inside the 802.1x framework that are suitable for wireless networks include EAP-Transport Layer Security (EAP-TLS), Protected EAP (PEAP), and EAP-Tunneled TLS (EAP-TTLS). These protocols allow the network to authenticate the client while also allowing the client to authenticate the network. 802.1x authentication consists of three components:
http://www.arubanetworks.com/techdocs/ArubaOS_60/UserGuide/802.1x.php

---

QUESTION 4

In a network with a deployed Cisco WLC, which two entities must be configured with the shared secret key for 802.1X authentication? (Choose two.)

A. RADIUS server

B. wireless client

C. AP

D. WLC

E. supplicant

Correct Answer: AD

The WLC needs to be configured in order to forward the user credentials to an external RADIUS server. The external RADIUS server then validates the user credentials and provides access to the wireless clients.
http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wlan-security/69730-eap-auth-wlc.html

---

QUESTION 5

A WLAN deployment uses a combination of Cisco Aironet 1260 APs and multiple Cisco 5500 Wireless LAN Controllers to provide wireless LAN access to end- users. The network administrator has decided to use DHCP Option 43 to enable the APs to discover the wireless LAN controllers. When configuring the DHCP scope, which format should be used for the Cisco WLC addresses?

A. a comma-separated ASCII string of Cisco WLC AP-manager addresses

B. a comma-separated ASCII string of Cisco WLC management addresses

C. a comma-separated ASCII string of Cisco WLC virtual IP addresses

D. a hexadecimal string of Cisco WLC AP-manager addresses

E. a hexadecimal string of Cisco WLC management addresses

F. a hexadecimal string of Cisco WLC virtual IP addresses

Correct Answer: E

Complete these steps in order to configure DHCP Option 43, in the embedded Cisco IOS DHCP server, for all Cisco Aironet APs that run Cisco IOS. This includes all APs except for the VxWorks 1000 Series (see the next section) and the 600

Series OEAP which does not use Option 43. ip dhcp pool

network

default-router

dns-server

option 43 hex

The hexadecimal string in step 3 is assembled as a sequence of the TLV values for the Option 43 suboption: Type + Length + Value. Type is always the suboption code 0xf1. Length is the number of controller management IP addresses times

4 in hex. Value is the IP address of the controller listed sequentially in hex.

http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html

---

QUESTION 6

When calculating the link budget for a wireless point-to-point bridge, the engineer notices that one antenna has its gain marked as 2.85 dBd. With a 20-mW access point and 3-dBi loss for the cable, what is the approximate EIRP?

A. 15 dBm

B. 18 dBm

C. 22 dBm

D. 25 dBm

Correct Answer: A

QUESTION 7

Which CLI command is used on a Cisco WLC to troubleshoot mobility, rogue detection, and load- balancing events?

A. debug dot11

B. debug capwap all

C. show dot11 details

D. show capwap details

Correct Answer: A

http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-3/command/reference/cr73/b_cr_7-3_chapter_010.html#wp3619872221

QUESTION 8

Which information on the Monitoring page of a Cisco WLC verifies that the wireless network is operational?

A. In the Access Point Summary section, the All APs number in the Up column is the same as in the Total column.

B. In the Client Summary section, the Current Clients number is positive.

C. In the Controller Summary section, the 802.11b/g Network State is shown as Enabled.

D. In the Controller Summary section, the CPU Usage number is positive.

Correct Answer: A

The output from the access point summary section of the Cisco WLC can be seen at the reference link below:
http://www.cisco.com/c/en/us/td/docs/wireless/wcs/6-0/configuration/guide/WCS60cg/6_0mon.html

---

QUESTION 9

Which purpose does a spectrum analyzer serve during a site survey?

A. Detect and measure RF energy on a frequency.

B. Identify and monitor rogue APs in the environment

C. Capture and save RF traffic to analyze it offline.

D. Generate a list of interference reports.

Correct Answer: A

QUESTION 10

An engineer has been noticing the power settings on several of the office APs change from day to day ever since two more APs were installed. After logging into the WLC, the engineer verifies that the power levels on 4 of the 802.11n radios are fluctuating up and down. What is the reason for this?

A. The controller has the APs in H-REAP mode and are on a Layer 2 connection instead of Layer 3.

B. The RRM has revealed a bad survey and is attempting to power down some of the radios to make up for it.

C. The WLC has created temporary coverage holes while stepping through power levels for some of the APs.

D. Several APs have high levels of overlapping coverage in the same area and the WLC is using RRM to correct the cell sizes AP coverage.

Correct Answer: D

QUESTION 11

Which protocol helps the administrator to determine whether a detected rogue AP is in the network of the organization?

A. RLDP

B. RCP

C. RDP

D. RAPP

Correct Answer: A

RLDP is an active approach, which is used when rogue AP has no authentication (Open Authentication) configured. This mode, which is disabled by default, instructs an active AP to move to the rogue channel and connect to the rogue as a client. During this time, the active AP sends deauthentication messages to all connected clients and then shuts down the radio interface. Then, it will associate to the rogue AP as a client.

The AP then tries to obtain an IP address from the rogue AP and forwards a User Datagram Protocol (UDP) packet (port 6352) that contains the local AP and rogue connection information to the controller through the rogue AP. If the controller receives this packet, the alarm is set to notify the network administrator that a rogue AP was discovered on the wired network with the RLDP feature. https://supportforums.cisco.com/discussion/10941011/rd-rogue-detector-or-rldp-rogue-location-discovery-protocol

---

QUESTION 12

A customer is reviewing Cisco Prime Infrastructure to identify malicious rogue access points that are operating within

the customer environment. Which dashboard in Cisco Prime Infrastructure displays this information by default?

A. Context Aware

B. CleanAir

C. Security

D. General

Correct Answer: C

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: