PassTest

Bessere Qualität , bessere Dienstleistungen!

Q&A

http://www.passtest.de

Einjährige kostenlose Aktualisierung

Exam : HP0-Y39

Title : Managing & Troubleshooting Enterprise Wireless Networks

Version : Demo

1.Click the Exhibit button and view both exhibits.

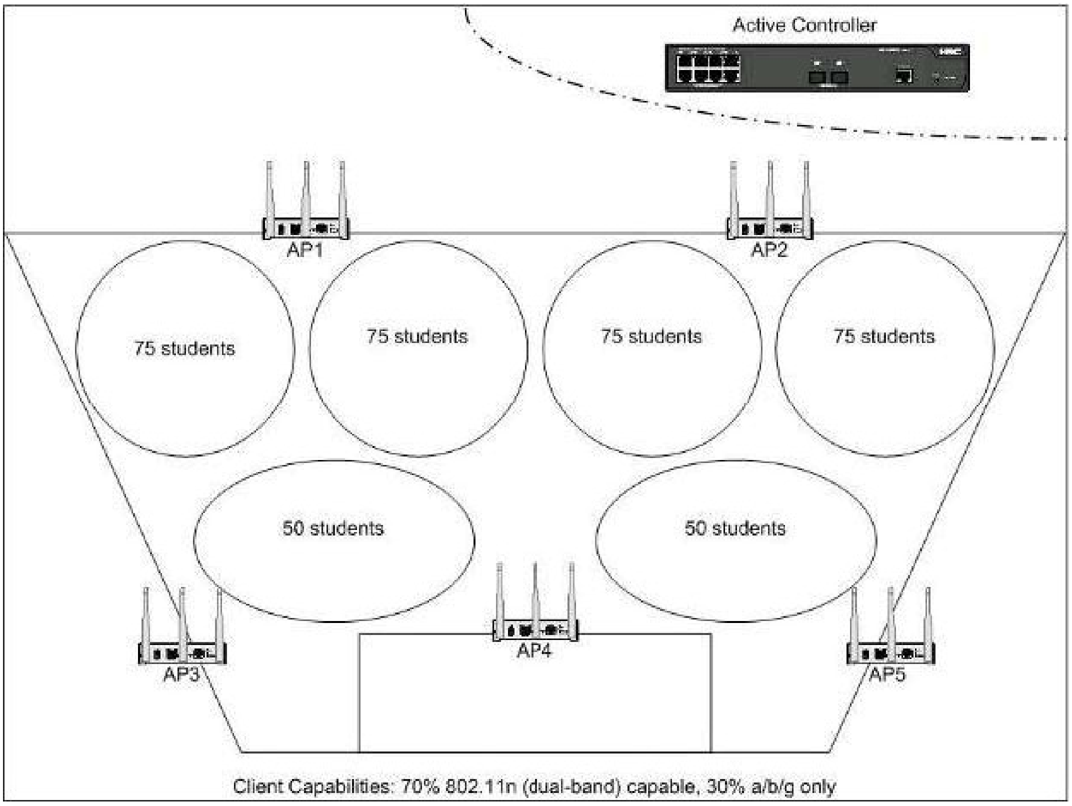
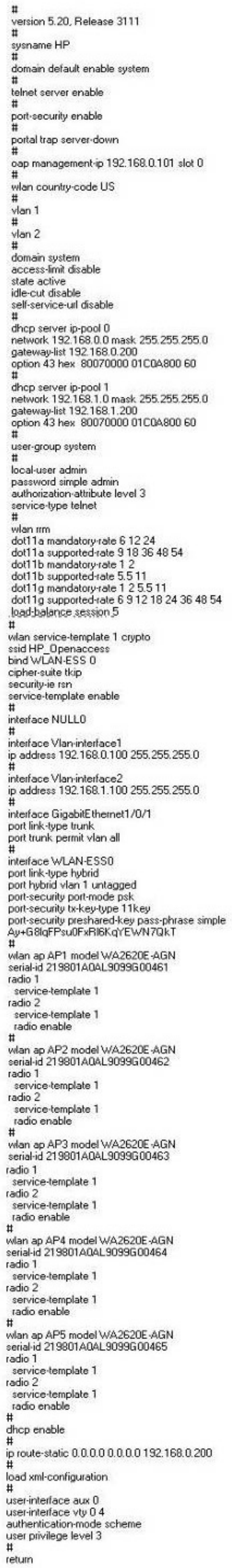


Exhibit 2: Active controller configuration



```
#
version 5.20, Release 3111
#
sysname HP
#
domain default enable system
#
telnet server enable
#
port-security enable
#
portal trap server-down
#
oap management-ip 192.168.0.101 slot 0
#
wlan country-code US
#
vlan 1
#
vlan 2
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
dhcp server ip-pool 0
network 192.168.0.0 mask 255.255.255.0
gateway-list 192.168.0.200
option 43 hex  80070000 01C0A800 60
#
dhcp server ip-pool 1
network 192.168.1.0 mask 255.255.255.0
gateway-list 192.168.1.200
option 43 hex  80070000 01C0A800 60
#
user-group system
#
local-user admin
password simple admin
authorization-attribute level 3
service-type telnet
#
wlan rrm
dot11a mandatory-rate 6 12 24
dot11a supported-rate 9 18 36 48 54
dot11b mandatory-rate 1 2
dot11b supported-rate 5.5 11
dot11g mandatory-rate 1 2 5.5 11
dot11g supported-rate 6 9 12 18 24 36 48 54
load-balance session 5
#
wlan service-template 1 crypto
ssid HP_Openaccess
bind WLAN-ESS 0
cipher-suite tkip
security-ie rsn
service-template enable
#
interface NULL0
#
interface Vlan-interface1
ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface2
ip address 192.168.1.100 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type trunk
port trunk permit vlan all
#
interface WLAN-ESS0
port link-type hybrid
port hybrid vlan 1 untagged
port-security port-mode psk
port-security tx-key-type 11key
port-security preshared-key pass-phrase simple
Ay+G8lqFPsu0FxRI6KqYEWN7QkT
#
wlan ap AP1 model WA2620E-AGN
serial-id 219801A0AL9099G00461
radio 1
  service-template 1
radio 2
  service-template 1
  radio enable
#
wlan ap AP2 model WA2620E-AGN
serial-id 219801A0AL9099G00462
radio 1
  service-template 1
radio 2
  service-template 1
  radio enable
#
wlan ap AP3 model WA2620E-AGN
serial-id 219801A0AL9099G00463
radio 1
  service-template 1
radio 2
  service-template 1
  radio enable
#
wlan ap AP4 model WA2620E-AGN
serial-id 219801A0AL9099G00464
radio 1
  service-template 1
radio 2
  service-template 1
  radio enable
#
wlan ap AP5 model WA2620E-AGN
serial-id 219801A0AL9099G00465
radio 1
  service-template 1
radio 2
  service-template 1
  radio enable
#
dhcp enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.0.200
#
load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
authentication-mode scheme
user privilege level 3
#
return
```

A university media course uses an auditorium that seats 400 students. Students are experiencing slow network performance, and some clients are having difficulty connecting to the wireless network. The IT staff installed wireless access points (APs) over a year ago. Previous classes, consisting of 200 students had no problems. Based on the exhibits, what is a solution to optimize performance for all students?

A. Enable radio 1 on all APs.

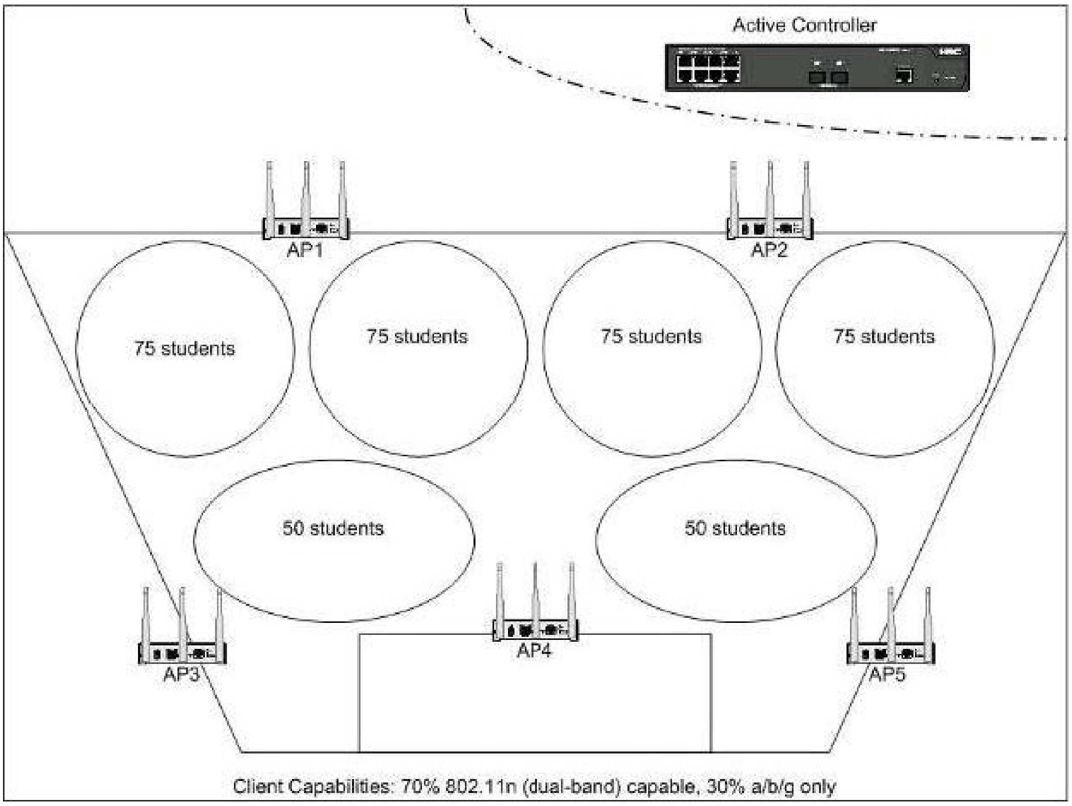
B. Add service-template1 to all 2.4Ghz radios.

C. Remove service-template1 from all 5Ghz radios.

D. Set cipher-suite to ccmp for service-template1.

Answer: A

2.Click the Exhibit button and view both exhibits.



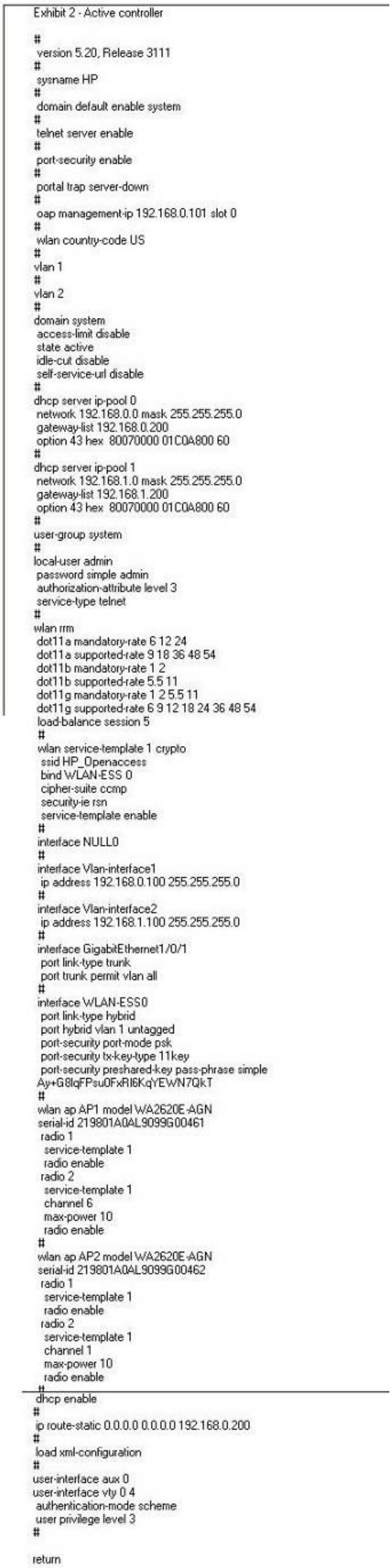


Exhibit 2 - Active controller

```
#
 version 5.20, Release 3111
#
 sysname HP
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 portal trap server-down
#
 oap management-ip 192.168.0.101 slot 0
#
 wlan country-code US
#
vlan 1
#
vlan 2
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool 0
 network 192.168.0.0 mask 255.255.255.0
 gateway-list 192.168.0.200
 option 43 hex  80070000 01C0A800 60
#
dhcp server ip-pool 1
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.200
 option 43 hex  80070000 01C0A800 60
#
user-group system
#
local-user admin
 password simple admin
 authorization-attribute level 3
 service-type telnet
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
 load-balance session 5
#
wlan service-template 1 crypto
 ssid HP_Openaccess
 bind WLAN-ESS 0
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface2
 ip address 192.168.1.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface WLAN-ESS0
 port link-type hybrid
 port hybrid vlan 1 untagged
 port-security port-mode psk
 port-security tx-key-type 11key
 port-security preshared-key pass-phrase simple
Ay+G8IqFPsu0FxRI6KqYEWN7QkT
#
wlan ap AP1 model WA2620E-AGN
serial-id 219801A0AL9099G00461
 radio 1
  service-template 1
  radio enable
 radio 2
  service-template 1
  channel 6
  max-power 10
  radio enable
#
wlan ap AP2 model WA2620E-AGN
serial-id 219801A0AL9099G00462
 radio 1
  service-template 1
  radio enable
 radio 2
  service-template 1
  channel 1
  max-power 10
  radio enable
#
dhcp enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.0.200
#
load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#

return
```

A university media course uses an auditorium that seats 400 students. Wireless access points (APs) are installed to provide access to the school's video servers. All clients show maximum signal strength, but some students are experiencing frequent interruptions of video playback. Based on the exhibits, what is a solution to optimize network throughput for all students.?

A. setting maximum power on radio 1 on all APs

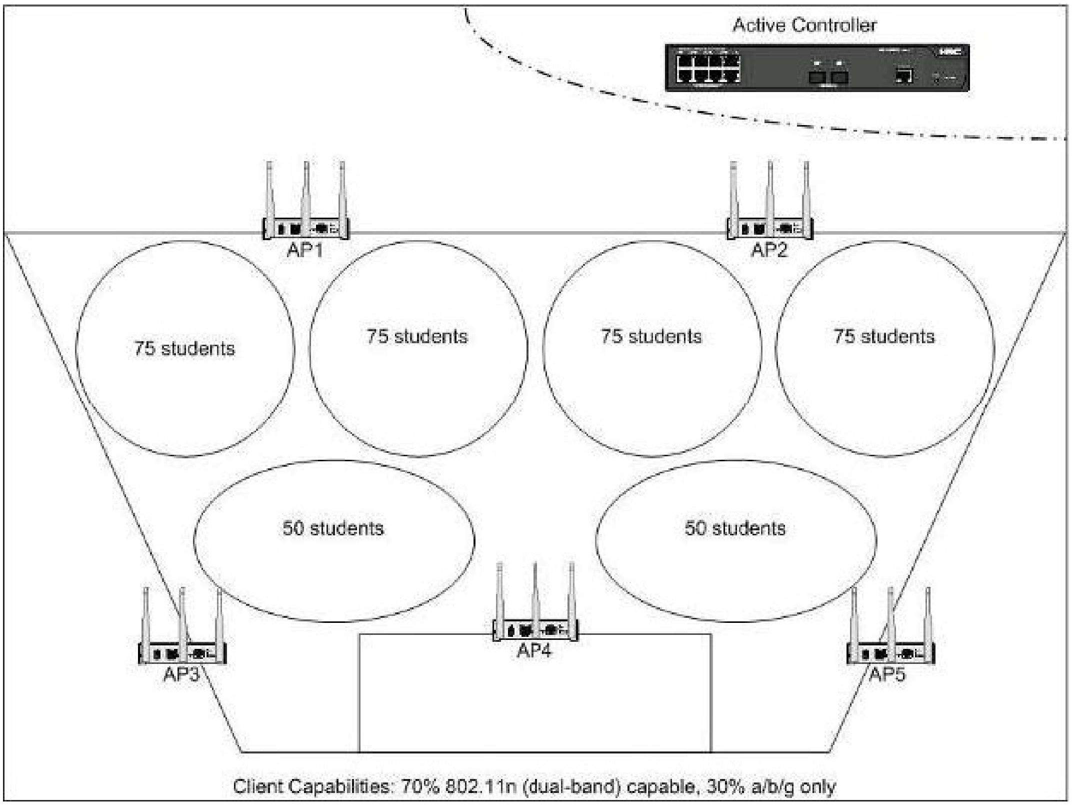
B. setting mandatory data rates for 802.11a to 12

C. changing the channel on radio 2 of AP5 to channel 6

D. lowering the RTS threshold on all radios

Answer: C

3.Click the Exhibit button and view both exhibits.



A university media course uses an auditorium that seats 400 students. Wireless access points (APs) are installed to provide access to the school's video servers. Some students are experiencing frequent interruptions to video playback while others have no issues. Based on the exhibits, what is a solution to optimize performance for all students?

A. Set all radios to maximum power.

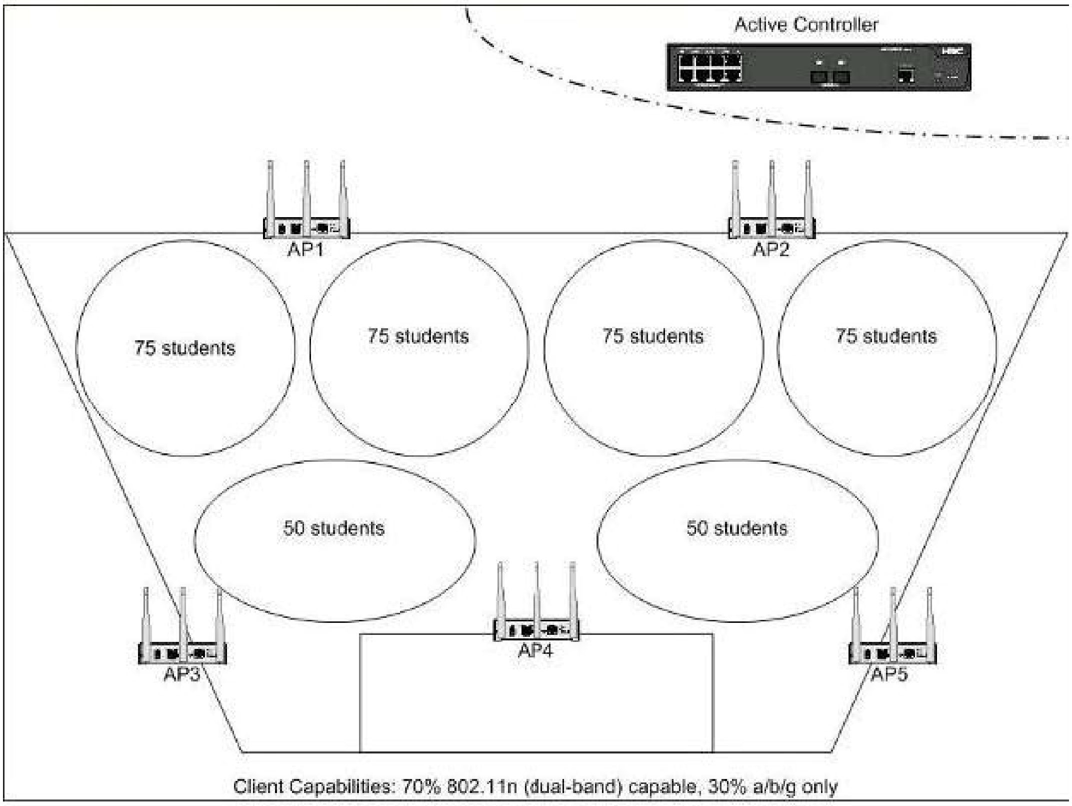
B. Set all APs to the same channel.

C. Enable load balancing of clients across APs.

D. Increase the beacon interval.

Answer: C

4.Click the Exhibit button and view both exhibits.


Active Controller
AP1
AP2
75 students
75 students
75 students
75 students
50 students
50 students
AP3
AP4
AP5
Client Capabilities: 70% 802.11n (dual-band) capable, 30% a/b/g only

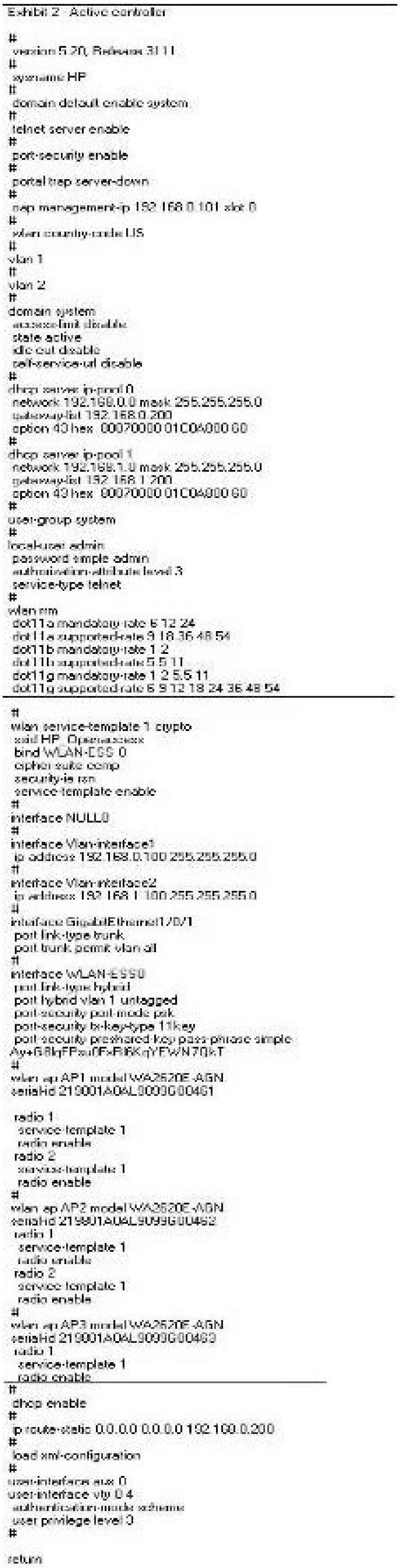


Exhibit 2 Active controller

```
#
 version 5.20, Release 3111
#
 sysname HP
#
 domain default enable system
#
 telnet server enable
#
 port-security enable
#
 portal trap server-down
#
 oap management-ip 192.168.0.101 slot 0
#
 wlan country-code US
#
vlan 1
#
vlan 2
#
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
dhcp server ip-pool 0
 network 192.168.0.0 mask 255.255.255.0
 gateway-list 192.168.0.200
 option 43 hex 80070000 01C0A800 60
#
dhcp server ip-pool 1
 network 192.168.1.0 mask 255.255.255.0
 gateway-list 192.168.1.200
 option 43 hex 80070000 01C0A800 60
#
user-group system
#
local-user admin
 password simple admin
 authorization-attribute level 3
 service-type telnet
#
wlan rrm
 dot11a mandatory-rate 6 12 24
 dot11a supported-rate 9 18 36 48 54
 dot11b mandatory-rate 1 2
 dot11b supported-rate 5.5 11
 dot11g mandatory-rate 1 2 5.5 11
 dot11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 1 crypto
 ssid HP_Openaccess
 bind WLAN-ESS 0
 cipher-suite ccmp
 security-ie rsn
 service-template enable
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.0.100 255.255.255.0
#
interface Vlan-interface2
 ip address 192.168.1.100 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk permit vlan all
#
interface WLAN-ESS0
 port link-type hybrid
 port hybrid vlan 1 untagged
 port-security port-mode psk
 port-security tx-key-type 11key
 port-security preshared-key pass-phrase simple
Ay+G8lqFPxu0FxRI6KqYEWN70kT
#
wlan ap AP1 model WA2620E-AGN
serial-id 219801A0AL9099G00461

 radio 1
  service-template 1
  radio enable
 radio 2
  service-template 1
  radio enable
#
wlan ap AP2 model WA2620E-AGN
serial-id 219801A0AL9099G00462
 radio 1
  service-template 1
  radio enable
 radio 2
  service-template 1
  radio enable
#
wlan ap AP3 model WA2620E-AGN
serial-id 219801A0AL9099G00463
 radio 1
  service-template 1
  radio enable
#
 dhcp enable
#
 ip route-static 0.0.0.0 0.0.0.0 192.168.0.200
#
 load xml-configuration
#
user-interface aux 0
user-interface vty 0 4
 authentication-mode scheme
 user privilege level 3
#

return
```

A university media course uses an auditorium that seats 400 students. Wireless access points (APs) are installed to provide access to the school's video servers. Students running 802.11n clients are not seeing optimal bandwidth connection data rates. Based on the exhibits, what is a solution to optimize 802.11n data rates?

A. Disable High Throughput (HT mode) on all radios.

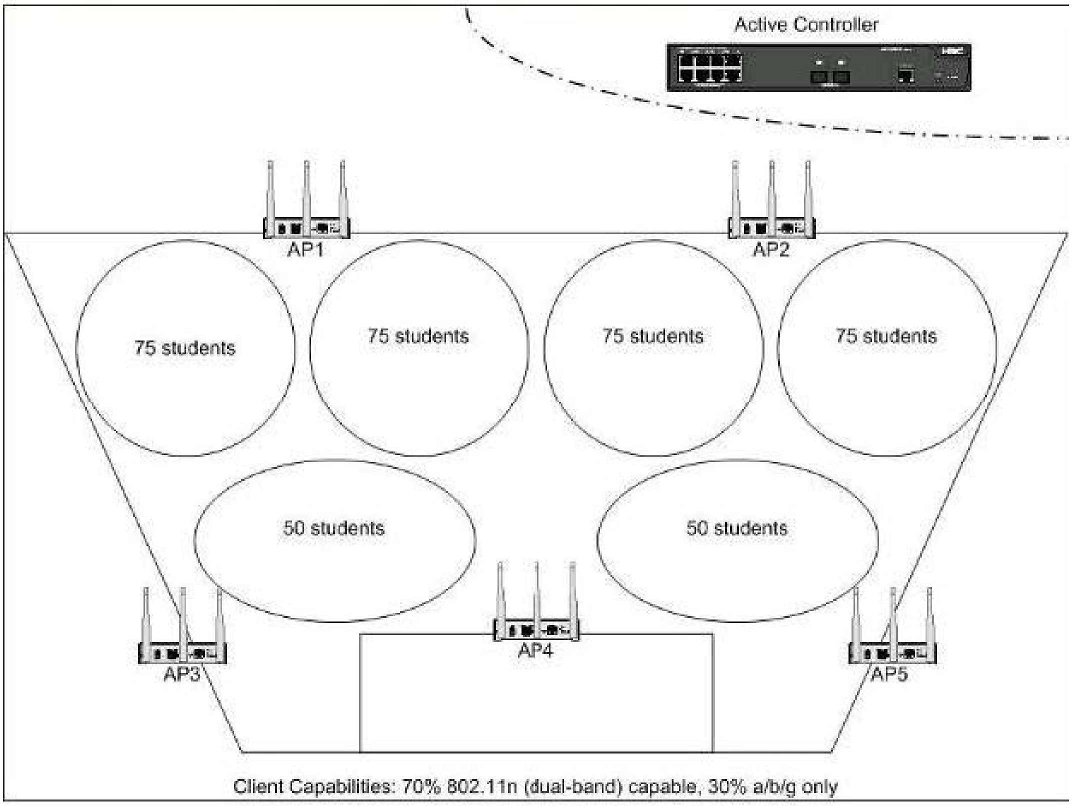
B. Disable RTS/CTS capability on non-802.11n client NICs.

C. Configure Band Steering mode on radio 1 on all APs and radio 2 on AP3 and AP5.

D. Configure Greenfield mode on radio1 on all APs and radio 2 on AP3 and AP5.

Answer: D

5.Click the Exhibit button.



A customer is experiencing network performance issues with their wireless network. The customer decides to take corrective actions on their wireless active controller. Based on the exhibit, what will happen on the wireless network if the customer sent a 1200 byte packet from a wireless client associated to essid HP_Openaccess? (Select two.)

A. The wireless packet will be fragmented.

B. The wireless packet will trigger RTS/CTS frames to be sent.

C. The wireless packet will not be fragmented.

D. The wireless packet will not trigger RTS/CTS frames to be sent.

E. The access point will send more Beacon frames than if the default configuration had been left unchanged.

Answer: A,B

6.RF Manager has determined that a Rogue access point (AP) must be quarantined. The only sensor within range is listed as busy. What happens?

A. RF Manager reclassifies the new Rogue AP as banned so that it cannot connect on the wired side.

B. RF Manager specifies that a quarantine is pending for the new Rogue AP until the sensor is no longer busy.

C. The sensor stops quarantining one of the currently quarantined devices and starts quarantining the new Rogue AP.

D. The sensor splits its time between blocking the currently quarantined devices and the new Rogue AP.

Answer: B

7.What is the risk of applying intrusion prevention to an access point (AP) listed as Indeterminate?

A. RF Manager cannot determine whether the AP follows your Authorized WLAN policy. You might quarantine your own AP, which could frustrate users.

B. RF Manager has classified the AP as Indeterminate because you authorized it manually, but it does not follow your Authorized WLAN policy.

Quarantining your own AP could frustrate users.

C. RF Manager has classified the AP as Indeterminate because its signal is so low. Sensors will make themselves busy in quarantining an AP that is probably too far away to be a risk.

D. RF Manager cannot determine whether the AP is connected to your system. You might quarantine another company's AP, which is illegal.

Answer: D

8.You set your country of operation and then apply the default Sensor Configuration Template settings to all sensors in RF Manager. How do your sensors handle channels that cannot be used legally in your country?

A. The sensors scan these channels and detect threats, but they do not take action against the threats.

B. The sensors scan these channels, detect threats, and take the action you have specified against any detected threats.

C. The sensors scan these channels and prevent any authorized access points or clients from operating on these channels.

D. The sensors do not scan these channels for threats.

Answer: A

9.Click the Exhibit button and view the three exhibits.

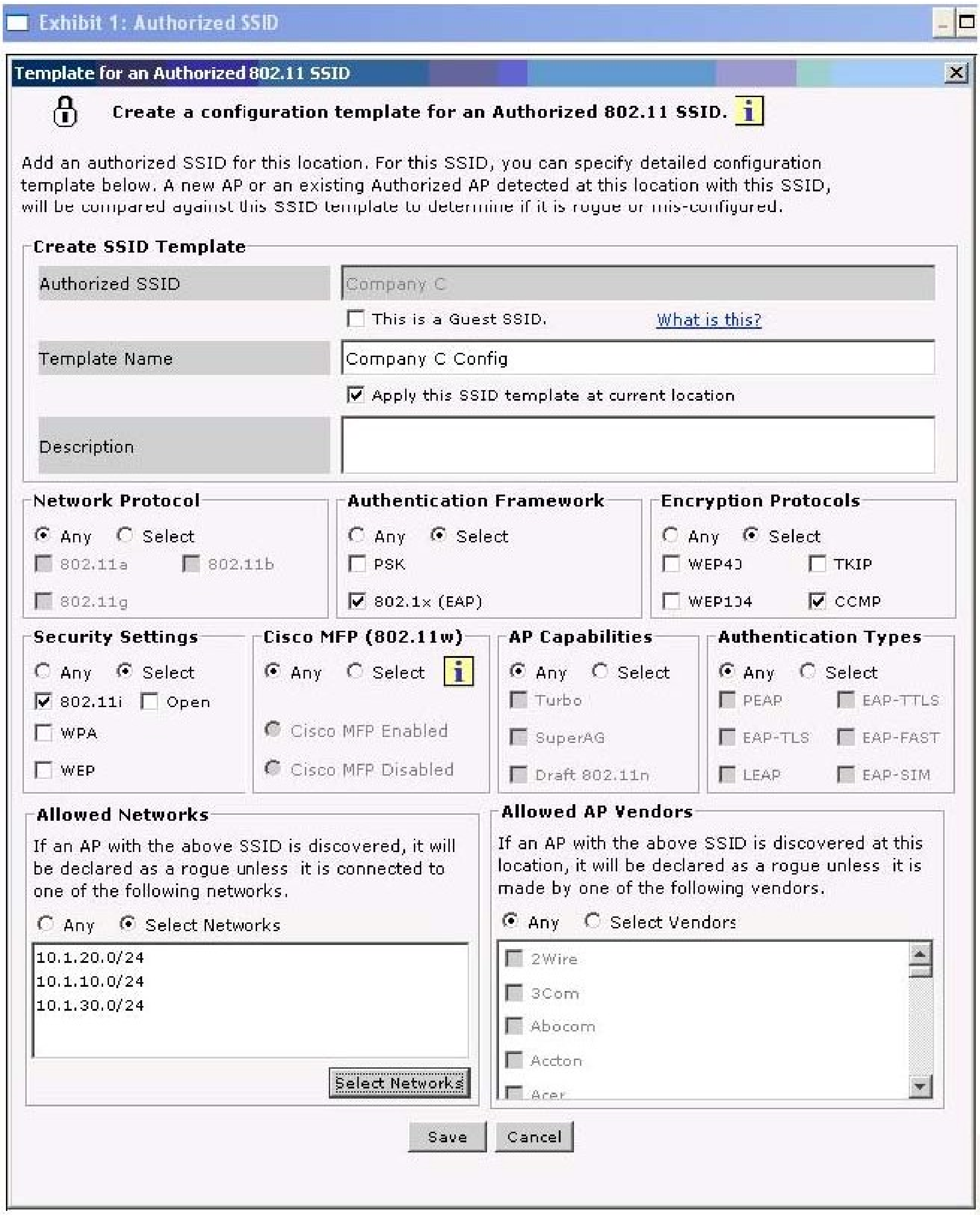


Exhibit 1: Authorized SSID

Template for an Authorized 802.11 SSID

Create a configuration template for an Authorized 802.11 SSID.

Add an authorized SSID for this location. For this SSID, you can specify detailed configuration template below. A new AP or an existing Authorized AP detected at this location with this SSID, will be compared against this SSID template to determine if it is rogue or mis-configured.

Create SSID Template

Authorized SSID	Company C
	☐ This is a Guest SSID. What is this?
Template Name	Company C Config
	☑ Apply this SSID template at current location
Description	

Network Protocol

● Any ○ Select

☐ 802.11a ☐ 802.11b

☐ 802.11g

Authentication Framework

○ Any ● Select

☐ PSK

☑ 802.1x (EAP)

Encryption Protocols

○ Any ● Select

☐ WEP40 ☐ TKIP

☐ WEP104 ☑ CCMP

Security Settings

○ Any ● Select

☑ 802.11i ☐ Open

☐ WPA

☐ WEP

Cisco MFP (802.11w)

● Any ○ Select

○ Cisco MFP Enabled

○ Cisco MFP Disabled

AP Capabilities

● Any ○ Select

☐ Turbo

☐ SuperAG

☐ Draft 802.11n

Authentication Types

● Any ○ Select

☐ PEAP ☐ EAP-TTLS

☐ EAP-TLS ☐ EAP-FAST

☐ LEAP ☐ EAP-SIM

Allowed Networks

If an AP with the above SSID is discovered, it will be declared as a rogue unless it is connected to one of the following networks.

○ Any ● Select Networks

10.1.20.0/24
10.1.10.0/24
10.1.30.0/24

Select Networks

Allowed AP Vendors

If an AP with the above SSID is discovered at this location, it will be declared as a rogue unless it is made by one of the following vendors.

● Any ○ Select Vendors

☐ 2Wire
☐ 3Com
☐ Abocom
☐ Accton
☐ Acer

Save Cancel

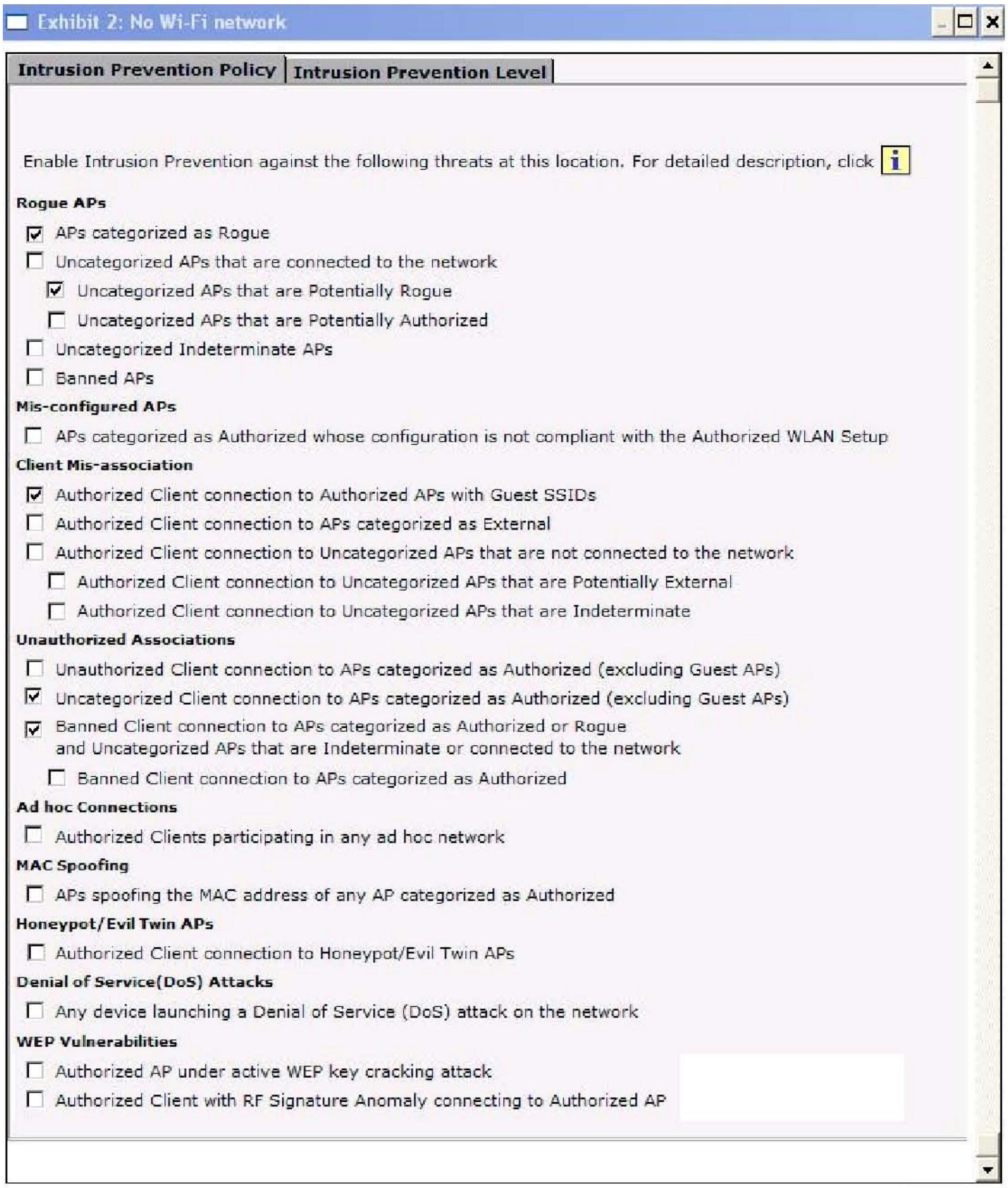


Exhibit 2: No Wi-Fi network
Intrusion Prevention Policy
Intrusion Prevention Level

Enable Intrusion Prevention against the following threats at this location. For detailed description, click

Rogue APs

☑ APs categorized as Rogue
□ Uncategorized APs that are connected to the network
☑ Uncategorized APs that are Potentially Rogue
□ Uncategorized APs that are Potentially Authorized
□ Uncategorized Indeterminate APs
□ Banned APs

Mis-configured APs

□ APs categorized as Authorized whose configuration is not compliant with the Authorized WLAN Setup

Client Mis-association

☑ Authorized Client connection to Authorized APs with Guest SSIDs
□ Authorized Client connection to APs categorized as External
□ Authorized Client connection to Uncategorized APs that are not connected to the network
□ Authorized Client connection to Uncategorized APs that are Potentially External
□ Authorized Client connection to Uncategorized APs that are Indeterminate

Unauthorized Associations

□ Unauthorized Client connection to APs categorized as Authorized (excluding Guest APs)
☑ Uncategorized Client connection to APs categorized as Authorized (excluding Guest APs)
☑ Banned Client connection to APs categorized as Authorized or Rogue
and Uncategorized APs that are Indeterminate or connected to the network
□ Banned Client connection to APs categorized as Authorized

Ad hoc Connections

□ Authorized Clients participating in any ad hoc network

MAC Spoofing

□ APs spoofing the MAC address of any AP categorized as Authorized

Honeypot/Evil Twin APs

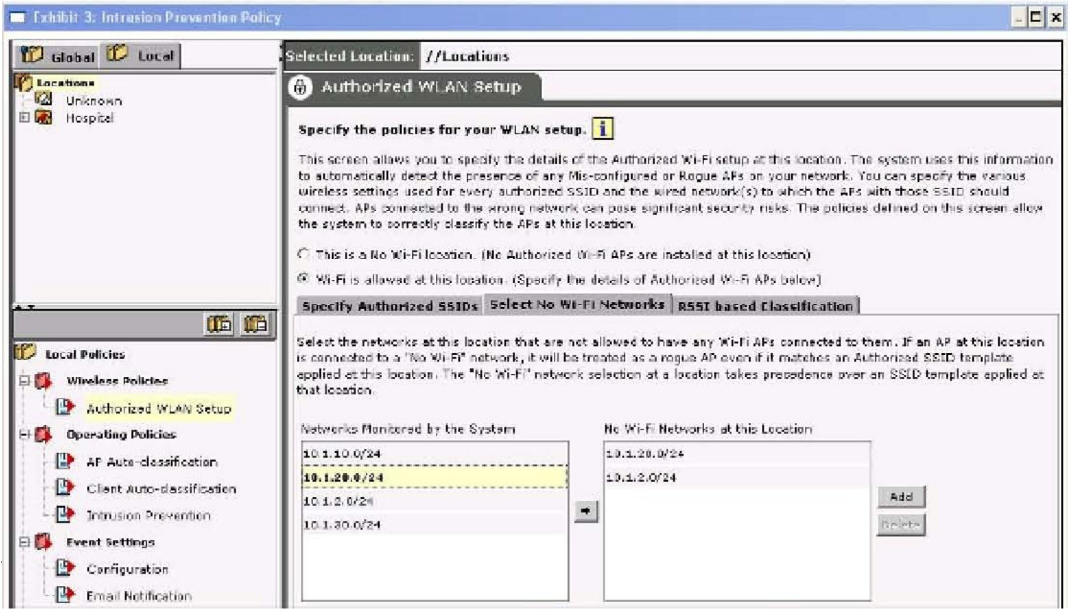
□ Authorized Client connection to Honeypot/Evil Twin APs

Denial of Service(DoS) Attacks

□ Any device launching a Denial of Service (DoS) attack on the network

WEP Vulnerabilities

□ Authorized AP under active WEP key cracking attack
□ Authorized Client with RF Signature Anomaly connecting to Authorized AP



Selected Location: //Locations

Specify the policies for your WLAN setup.

This screen allows you to specify the details of the Authorized Wi-Fi setup at this location. The system uses this information to automatically detect the presence of any Mis-configured or Rogue APs on your network. You can specify the various wireless settings used for every authorized SSID and the wired network(s) to which the APs with those SSID should connect. APs connected to the wrong network can pose significant security risks. The policies defined on this screen allow the system to correctly classify the APs at this location.

○ This is a No Wi-Fi location. (No Authorized Wi-Fi APs are installed at this location)
● Wi-Fi is allowed at this location. (Specify the details of Authorized Wi-Fi APs below)

Select the networks at this location that are not allowed to have any Wi-Fi APs connected to them. If an AP at this location is connected to a "No Wi-Fi" network, it will be treated as a rogue AP even if it matches an Authorized SSID template applied at this location. The "No Wi-Fi" network selection at a location takes precedence over an SSID template applied at that location.

Networks Monitored by the System
10.1.10.0/24
10.1.20.0/24
10.1.2.0/24
10.1.30.0/24

No Wi-Fi Networks at this Location
10.1.20.0/24
10.1.2.0/24

RF Manager and its sensors have detected an association between an Uncategorized Client and an access point (AP) that uses these settings:

SSID = Company C

Security = WPA2 with CCMP and 802.1X

The AP is detected while passing the client traffic on VLAN 20 (10.1.20.0/24). WiFi is permitted at this location. The exhibits show the Authorized SSID Template, other Authorized WLAN Policy settings, and the Intrusion Prevention Policy for the location.

What does RF Manager have its sensors do?

A. quarantine the AP only

B. quarantine the client only

C. take no action against either device

D. quarantine both the AP and the client

Answer: A

10.What are the requirements for deploying a sensor that is discovered by RF Manager with zero configuration? (Select two.)

A. The sensor must operate in network detector (ND) mode.

B. The sensor must be installed on the same VLAN as RF Manager.

C. The network must be set up to assign the sensor IP settings through DHCP.

D. The DNS server must map the WiFi-security-server to the RF Manager IP address.

E. RF Manager and the sensor must both be at their default IP settings.

Answer: C,D

11.What is a potential risk of enabling the RSSI-based classification feature in an Authorized WLAN policy?

A. RF Manager must rely exclusively on RSSI to detect the locations of harmful devices, instead of drawing on the findings of network detectors. This might make the prediction less accurate.

B. Sensors might decide that they should not take action against a potentially harmful device because its RSSI is low and the device might still be a risk.

C. RF Manager might classify your own access points (APs) as Rogue APs because their transmit power is too high and take action against them.

D. RF Manager might classify legitimate access points (APs) owned by nearby companies as Rogue APs and take action against them.

Answer: D

12.Which action does RF Manager take to quarantine a client?

A. It instructs the client's access point to place the client's traffic in a quarantine VLAN.

B. It instructs a sensor to send a forced disassociation message to the client's access point (AP) so that the AP forces the client to disconnect.

C. It instructs a sensor to send frames to interfere with the frames sent by the quarantined client.

D. It adds the client's MAC address to the access point's MAC lockout list, thereby blocking the client's traffic.

Answer: C

13.By default, which roles do the RF Manager and its sensors perform in detecting Rogue access points (APs)?
A. Sensors monitor wireless transmissions and RF Manager monitors wired transmissions. They combine the data to find APs that use your SSIDs but are not on your network.
B. Sensors monitor wireless transmissions and RF Manager monitors wired transmissions. They combine the data to find unauthorized APs on your network.
C. Sensors monitor wired and wireless transmissions so RF Manager can find unauthorized APs connected to your wired network.
D. Sensors detect APs that use your SSIDs but are not on your Authorized AP list.
Answer: C

14.In sensor only (SO) mode, what does an HP sensor monitor?
A. It monitors only one untagged VLAN as well as wireless signals.
B. It monitors wireless signals, but does not monitor VLANs.
C. It monitors multiple VLANs as well as wireless signals.
D. It monitors multiple VLANs, but does not monitor wireless signals.
Answer: A

15.A customer reports the performance of their HP A-WA2620E access point (AP) is inadequate. While investigating the report, you determine that the AP is functioning in MIMO 3x2 mode instead of MIMO 3x3 as desired. What is one possible cause of this problem?
A. The AP is powered using 802.3af PoE.
B. The AP is configured to use a 40Mhz channel bandwidth.
C. The AP is not implementing the local switching feature.
D. The AP is powered using 802.3at PoE.
Answer: A