SmartPath EMS VMA begins transferring the configuration to SmartPath AP3 and displays the Monitor > Access Points > SmartPath AP Update Results page where you can observe the progress and the result of the operation.

After SmartPath AP3 reboots to activate its new configuration, it tries to reconnect with SmartPath EMS VMA. However, it cannot do so because it is a mesh point that now belongs to the cluster1-test cluster while its portals—SmartPath AP1 and 2—are still using their original configurations in which they are members of cluster0. This loss of connectivity will continue until you update the portals, which you do next.

5. Repeat the previous steps to update SmartPath AP1 and SmartPath AP2.

After they reboot and activate their new configurations, check the status of their CAPWAP connections by looking at the CAPWAP column on the Monitor > Access Points > SmartPath APs page with the View mode set as Monitor. After a few minutes, all three SmartPath APs will reestablish their connections.

8.7 Example 7: Selective Multicast Forwarding through GRE Tunnels

SmartPath APs can selectively block or allow broadcast and multicast traffic through GRE tunnels to reduce traffic congestion. You can filter traffic either by using a blacklist to block all broadcast and multicast traffic (or to block all except to a few select destinations) or by using a whitelist to allow all broadcast and multicast traffic (or to allow all except to a few destinations).

Most IP cameras are designed to send video via an IP multicast protocol. When configuring a number of cameras to send video to a central monitoring facility through a GRE tunnel, the SmartPath AP terminating the tunnels at the monitoring facility automatically forwards the multicast traffic it receives back through all the other GRE tunnels to the cameras because they are all members of the same multicast group. Not only is this unnecessary, but it can also create a very large amount of traffic. This is particularly problematic because GRE does not have a mechanism for pruning traffic, and multicast traffic arriving at a GRE tunnel endpoint must be replicated on all outgoing tunnels.

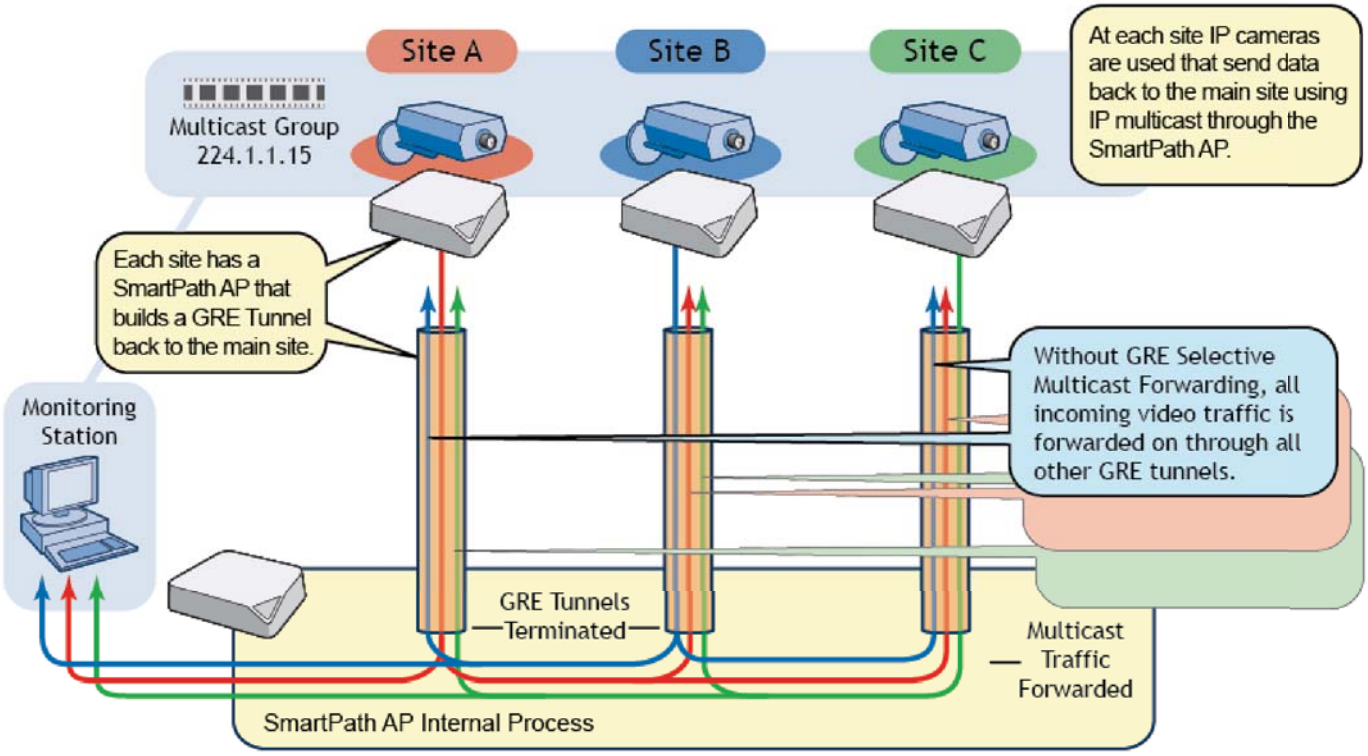


Figure 8-12. Selective multicast forwarding through GRE.

GRE selective multicast forwarding allows you to determine whether a specific multicast group or set of multicast groups can receive multicast packets, or whether the SmartPath AP blocks all or no multicast packets.

Filtering multicast packet occurs in two main ways: by blacklisting and whitelisting. You cannot use blacklists and whitelists together because their operations are mutually exclusive; however, you can modify each to suit your particular requirements. To set a blacklist or whitelist, you must first define a default rule to block or allow all, and then you can add exceptions as needed.

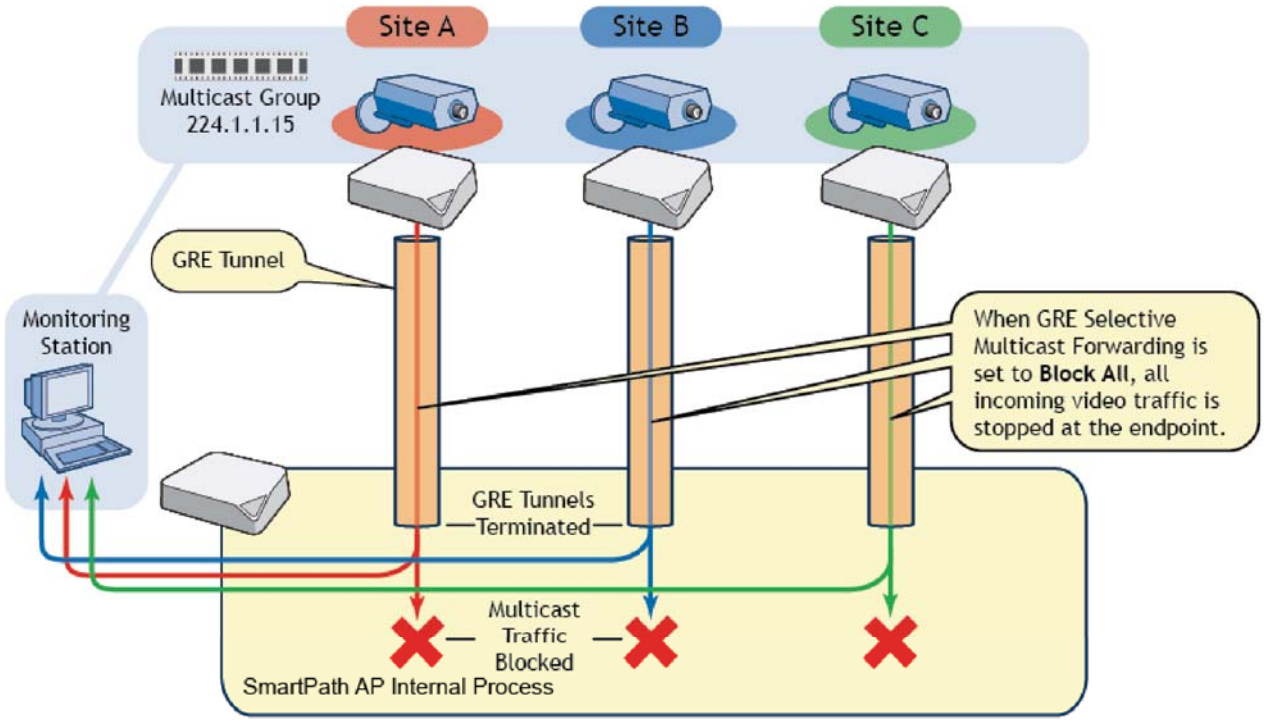


Figure 8-13. Filtering multicast packets.

By default, a SmartPath AP forwards all multicast packets. To customize IP multicast filtering, enter the following in SmartPath EMS VMA:

1. Click Configuration > Advanced Configuration > Management Services > Management Options, and then click New.
2. Enter a name for the new management options object in the Name text box. This name can be up to 32 characters long.
3. In the GRE Tunneling Selective Multicast Forwarding section, select whether you want to begin with an open filter by selecting Allow All, or a closed filter by selecting Block All.

NOTE: For most applications, you want to begin with a closed filter and then specify the multicast addresses you want to forward through the GRE tunnels. The steps that follow assume that this is the case, and that Block All is selected.

4. In the Exception IP List, enter the following, and then click "Apply:"

IP: Enter the IP address of the multicast address (for example, 224.1.1.10). You can also enter the network address of a multicast subnet (e.g., 224.1.1.0).

Netmask: If you entered a network address in the IP column above, then enter the subnet mask here that includes all the addresses of that network. For example, if you entered 224.1.1.0 in the IP column and wish to include 224.1.1.1 and 224.1.1.2, then enter 255.255.255.252 (a 30-bit mask). However, if you entered an IP address in the IP column, then enter 255.255.255.255.

5. If there are additional IP multicast addresses or ranges you want to add to the exception list, repeat Step 4 for each address or range. When done, click "Save."

You can also create these lists through the CLI. To create a whitelist for selective multicast forwarding through GRE tunnels except for a single IP address (for example, 224.1.1.10), make an SSH connection to the SmartPath AP where you want to create the whitelist, and then enter the following command:

```
forwarding-engine tunnel selective-multicast-forward block-all except 224.1.1.10
```

To create a whitelist for selective multicast forwarding except for a range of IP addresses (e.g., 224.1.1.0/24), enter the following command:

```
forwarding-engine tunnel selective-multicast-forward block-all except 224.1.1.0/30
```

8.8 Example 8: IP Multicast Enhancements

IP Multicast Enhancements: To minimize airtime consumption caused by multicast frame transmissions, SmartPath APs can convert multicast to unicast frames when channel utilization is high or multicast group membership is low. Furthermore, when SmartPath APs cannot detect any multicast group members among their active clients, they can automatically suppress multicast frame transmissions completely.

Video streaming typically makes use of multicasting as its transport. With multicasting, a data stream from a single source reaches multiple subscribers identified by their multicast group IP address. These subscribers notify their network routers and switches when they belong to a particular group and are interested in receiving data. When a router or switch receives such a notification, it then forwards any multicast stream for that group onto the network segment from which it received the notification. If there are no subscribers on a particular segment, the forwarding device stops transmitting the stream to conserve bandwidth.

On a wireless network, data transmitted by multiple stations on the same RF channel in an overlapping area must share the same physical transportation resource: the available airtime. When an access point transmits unicast traffic, it uses a rate-adaptation algorithm to determine the fastest data rate at which it can communicate with each station. When transmitting multicast traffic, the access point must choose the best data rate all the group members can support. If one group member has a slow connection, the access point must transmit at that speed to all group members. This not only slows down data transmissions to other members with stronger connections, it also uses up more airtime that otherwise would be available for use by other wireless stations in the area.

To reduce unnecessary airtime usage for multicast transmissions, a SmartPath AP can convert multicast frames to unicast frames under certain conditions or at all times, and it can also drop multicast frames when there are no group members present to receive them. In addition to reducing airtime usage, another benefit of using unicast traffic is the increased reliability of video delivery. If a wireless client does not receive a unicast frame and does not reply with an ACK, the access point will retransmit it. However, multicast traffic does not support wireless frame delivery confirmation as unicast traffic does.

When a SmartPath AP is enabled to convert multicast frames to unicast, it performs the conversion when the percent of channel usage exceeds a specified threshold or when the number of multicast group members drops below a specified threshold. By default, the channel utilization threshold is 60% and the membership count threshold is 10. You can change the channel utilization threshold from 1 to 100 % and the membership count threshold from 1 to 30 on a per-SSID basis. These settings are on the Configuration > SSIDs > New page in the IP Multicast subsection within the Advanced section.

Figure 8-14. IP multicast screen.

If you want the SmartPath AP to convert multicast frames to unicast when the channel utilization or membership count conditions are met, select "Auto." For the SmartPath AP to make the conversion unconditionally, select "Always." If you do not want the SmartPath AP to use the multicast-to-unicast conversion feature but instead follow the standard 802.11 behavior for sending multicast frames, select "Disable."

In addition to the conversion technique, SmartPath APs also perform Internet Group Management Protocol (IGMP) snooping to check if any multicast group members are associated; and when they are not, the SmartPath AP drops all multicast packets. Specifically, SmartPath APs snoop IGMP Report and Leave messages.

9. Common Configuration Examples

Through the use of examples, this chapter shows how to use SmartPath EMS VMA in Enterprise mode to configure several features that are somewhat more advanced than those covered in the previous chapter. The examples cover topics such as topological maps, IEEE 802.1X authentication, captive web portals, and the SmartPath EMS VMA concept of classifier tags, which is a method for
assigning the different definitions of a single network object to various managed SmartPath APs. By trying out these examples—or perhaps just reading them—you can better familiarize yourself with the SmartPath EMS VMA GUI and how to use it to manage and configure SmartPath APs.

The following examples in this chapter show how to use SmartPath EMS VMA to configure the following features:

- Secton 9.1, Example 1: Mapping Locations and Installing SmartPath APs—Upload image files of topology maps to SmartPath EMS VMA and use one of two ways to associate physical SmartPath APs with their corresponding icons on the maps.
- Section 9.2, Example 2: IEEE 802.1X with an External RADIUS Server—Configure an IEEE 802.1X SSID and enable SmartPath APs to act as RADIUS authenticators, forwarding authentication requests from their wireless clients to an external RADIUS authentication server.
- Section 9.3, Example 3: Providing Guest Access through a Captive Web Portal—Provide controlled and limited wireless network access for guests. This example includes the configuration of a captive web portal, QoS policy, IP firewall policy, user profile, and SSID.
- Section 9.4, Example 4: Private PSKs—Import a file of user names, e-mail addresses, and other data to create private PSK users. Assign the users to a private PSK SSID, and distribute the private PSK data to users through e-mail.
- Section 9.5: Example 5: Using SmartPath AP Classifiers—Define a single VLAN object with three different definitions, each definition marked with a classifier tag so that the SmartPath APs similarly tagged at different sites can apply the appropriate VLAN for their location.

9.1 Example 1: Mapping Locations and Installing SmartPath APs

SmartPath EMS VMA allows you to mark the location of SmartPath APs on maps so that you can track devices and monitor their status. First, you must upload the maps to SmartPath EMS VMA, and then name and arrange them in a structured hierarchy (see "Setting Up Topology Maps"). After that, you can follow one of two ways to install SmartPath APs so that you can later put their corresponding icons on the right maps (see Section 9.1.1).

In this example, you set up maps and install more than 70 SmartPath APs at three locations in a corporate network. After that, you can use SmartPath EMS VMA to create configurations for them, and then push the configurations to them over the network. The general design of the deployment is shown in Figure 9-1.

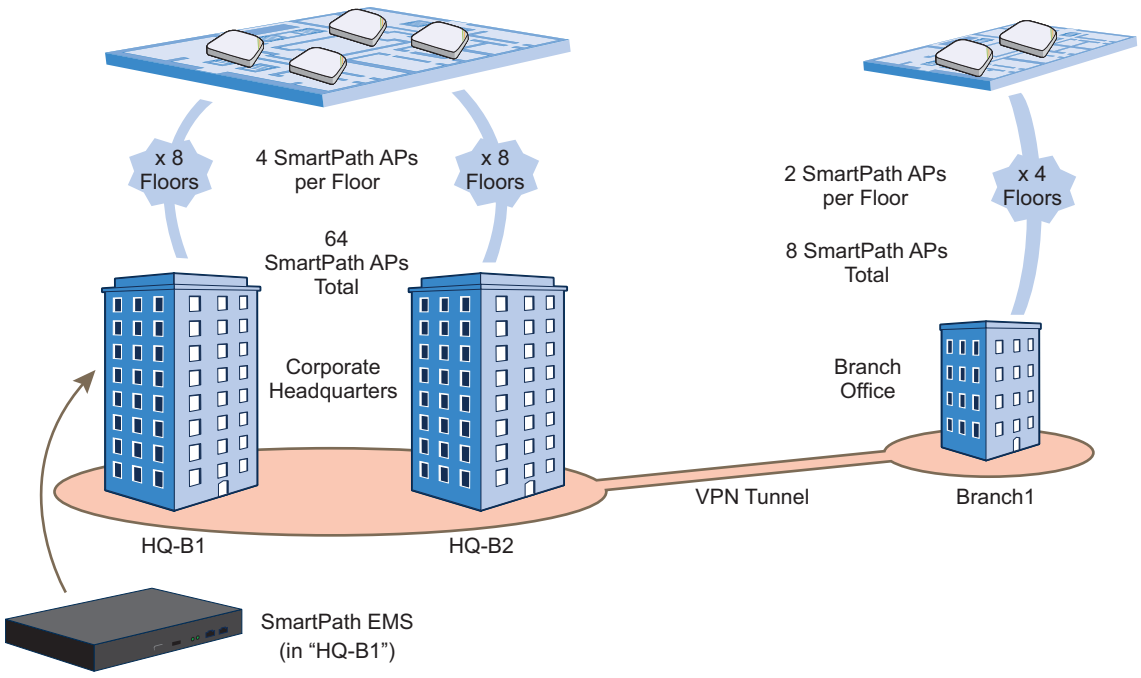


Figure 9-1. Deployment overview.

9.1.1 Setting Up Topology Maps

In this example, you upload maps to SmartPath EMS VMA showing floor plans for three office buildings and organize them in a hierarchical structure. You need to make .png of .jpg files of drawings or blueprints showing the layout of each floor. Also, as an easy means of organizing the maps in the SmartPath EMS VMA GUI, you create a file showing the three buildings HQ-B1, HQ-B2, and Branch-1. By using this drawing at the top topographical level, you can display icons for each floor of each building. You can then click an icon to link to its corresponding map. This is shown in Figure 9-2.

NOTE: Instead of using an illustration of buildings, you can also set the image of the root map as None and use the Add Wall tool to draw three simple rectangles. This option is useful when you have floor plans but not an illustration depicting the external buildings.

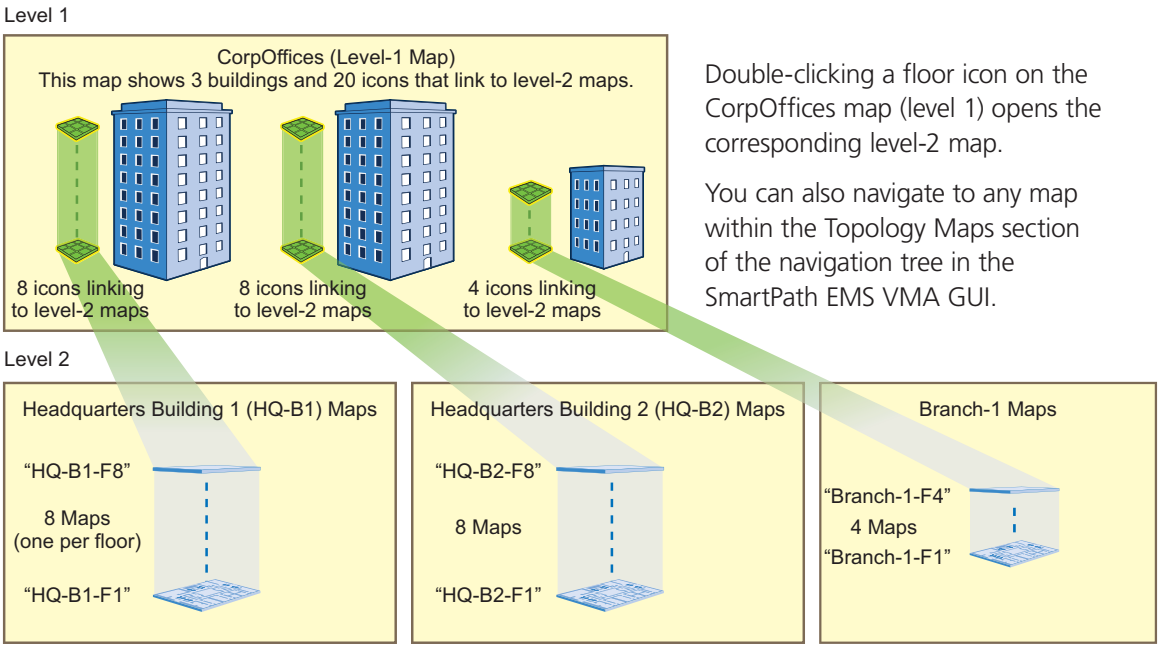


Figure 9-2. Organizational structure of level-1 and -2 maps.

Uploading Maps

NOTE: All image files that you upload to SmartPath EMS VMA must be in .png or .jpg format.

1. Log in to the SmartPath EMS VMA GUI as explained in Section 7.1.
2. To begin using maps, you must first set the root map, which will be at the top level of all the maps you add under it. Click Topology, enter the following, and then click Update:

   Root Map Name: CorpOffices (Note that spaces are not allowed in map level names. This will be the map at the top of a hierarchical structure of maps. After defining this map, you can then add other maps beneath it.)

   Operational Environment: Because the CorpOffices "map" does not contain any SmartPath AP icons—it is an illustration of three buildings that you use to organize the submaps of the floors in each building—the environment setting is irrelevant. Leave it at its default, Office.

   Background Image: Click Import > Upload, navigate to corp_offices.png and select it. Then choose corp_offices.png from the Background Image drop-down list.

   Map Size and SmartPath AP Installation Height: Because the corp_offices.png depicts buildings instead of a floor plan, it is not necessary to specify the size of the image or the SmartPath AP installation height.

3. To add maps below the root map, click Topology, right-click CorpOffices, and then choose Add/Delete Image from the pop-up menu that appears. In the Add/Delete Image window, click Upload, navigate to the directory containing the image files that you want to upload, select up to five of them, and then click Open.

The selected image files are transferred from your management system to SmartPath EMS VMA as shown in Figure 9-3.

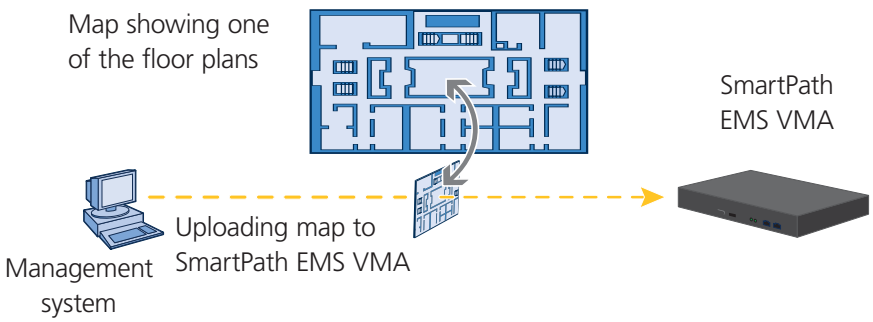


Figure 9-3. Uploading a map of a building floor plan.

4. Repeat this for all the image files that you need to load, and then close the dialog box when done. For this example, you load these 21 files:

- 8 maps for the eight floors in HQ-B1 (Headquarters Building 1)
- 8 maps for the eight floors in HQ-B2 (Headquarters Building 2)
- 4 maps for the four floors in Branch-1
- 1 file (named "corp_offices.png" in this example) that shows a picture of the three buildings

Naming and Arranging Maps within a Structure

1. Click Topology, right-click the top level map "CorpOffices", and then choose New from the pop-up menu that appears.
2. In the New Map (Submap for CorpOffices) dialog box, enter the following, and then click Create:

   Map Name: HQ-B1-F1

   Map Icon: Floor

   Environment: Because the environment is that of a typical office building, choose Office. The environment assists in the prediction of signal strength and attenuation shown in the heat maps.

   Background Image: Choose HQ-B1-F1.png from the drop-down list.

   Map Width (optional): 120 feet (SmartPath EMS VMA automatically calculates map height using the aspect ratio of the image.)

   SmartPath AP Installation Height: 13 feet; a fairly standard ceiling height in offices

   A floor icon ( ) labeled "HQ-B1-F1" appears on the CorpOffices image, and a new entry named "HQ-B1-F1" appears nested under "CorpOffices" in the navigation tree.
3. Select the icon, and drag it to the location you want.
4. Click Topology, right-click the top level map "CorpOffices", and then choose New from the pop-up menu that appears.
5. In the New Map (Submap for CorpOffices) dialog box, enter the following, and then click Create:

   Map Name: HQ-B1-F2

   Map Icon: Floor

   Environment: Office

   Background Image: Choose HQ-B1-F2.png from the drop-down list.

   Map Width (optional): 120 feet

   SmartPath AP Installation Height: 13 feet

A floor icon labeled "HQ-B1-F2" appears on the CorpOffices image, and a new entry named "HQ-B1-F2" appears nested under "CorpOffices" in the navigation tree.

6. Select the icon and drag it to the location you want.

After adding the CorpOffices "map" (really an illustration showing three buildings), two floor plans for the first and second floors of "HQ-B1", and dragging the floor icons into position, the display of the CorpOffices map looks similar to that in Figure 9-4.

The submaps in the navigation tree and the icons on this map link to other maps.

Click a submap or double-click an icon to open the map to which it links.

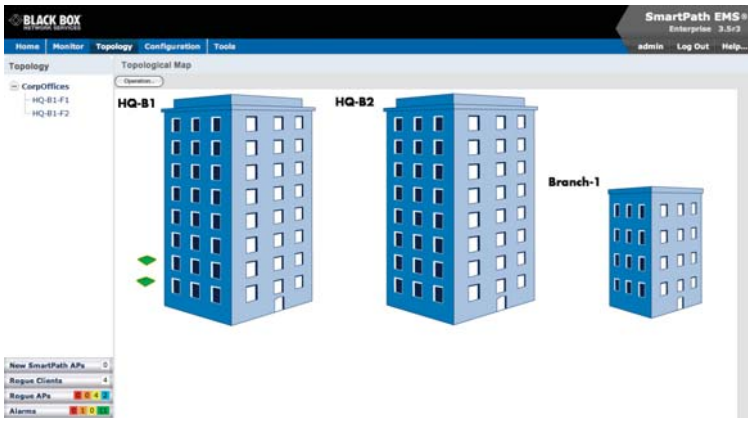


Figure 9-4. CorpOffice map (Level 1) with links to Level-2 maps HQ-B1-F1 and HQ-B1-F2.

7. Repeat this process until you have arranged all the maps and icons in place as shown in Figure 9-5.

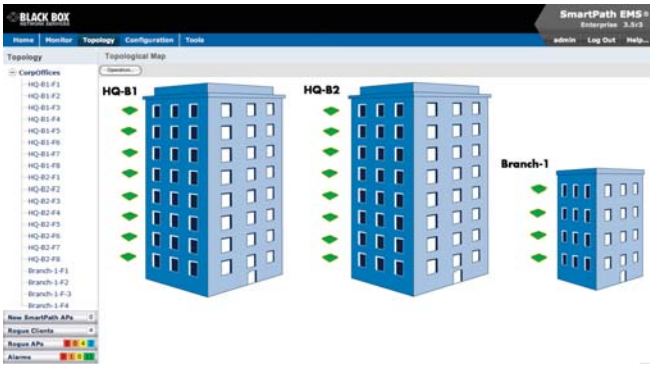


Figure 9-5. CorpOffice map with links to all Level-2 maps.

NOTE: You can add up to seven levels to the map hierarchy. You can also remove maps as long as they do not have any submaps or SmartPath AP icons on them. To remove a map from the hierarchy, right-click it in the Map Hierarchy list, select Remove from the short-cut menu that pops up, and then click "Yes."

9.1.2 Preparing the SmartPath APs

There are several approaches that you can take when mapping the location of installed SmartPath AP devices. Two possible approaches are presented below. The first approach ("Using MAC Addresses") allows you to install SmartPath APs without needing to do any extra configurations, but you later have to match each SmartPath AP with the right map in SmartPath EMS VMA manually. With the second approach ("Using SNMP"), SmartPath EMS VMA automatically assigns SmartPath APs to maps. This approach does require a small amount of configuration of each SmartPath AP up front, but after the SmartPath APs form a CAPWAP connection with SmartPath EMS VMA, the automatic assignment of SmartPath APs to their appropriate maps on SmartPath EMS VMA occurs without any further effort.

NOTE: For a summary of how SmartPath APs use CAPWAP to discover and connect to SmartPath EMS VMA, see "How SmartPath APs Connect to SmartPath EMS VMA" in Section 8.4, Connecting SmartPath APs to SmartPath EMS VMA.

Using MAC Addresses

With this approach, you write down the MAC address labelled on the underside of each SmartPath AP and its location while installing the SmartPath APs throughout the buildings. The MAC address on the label is for the mgt0 interface. Because the MAC addresses of all SmartPath APs begin with the MAC OUI 008C:10, you only need to record the last six numerals in the address. For example, if the MAC OUI is 008C:1000:0120, you only need to write "000120" to be able to distinguish it from other SmartPath APs later.

NOTE: 008C:10 is the Black Box MAC address portion. You need to change this.

1. Make copies of the maps uploaded to SmartPath EMS VMA, label them, and take them along when installing the SmartPath APs.

2. When you install a SmartPath AP, write the last six digits of its MAC address at its location on the map.

When SmartPath APs automatically connect with SmartPath EMS VMA, SmartPath EMS VMA displays them on the Monitor > Access Points > SmartPath APs page. You can differentiate them in the displayed list by MAC address (node ID), which allows you to match the SmartPath APs in the GUI with those you noted during installation so that you can properly assign each one to a map.

Using SNMP

This approach makes use of the Simple Network Management Protocol (SNMP) sysLocation Management Information Base (MIB) object, which you define on SmartPath APs. SmartPath EMS VMA can use this information to associate a SmartPath AP with a map and provide a description of where on the map each SmartPath AP belongs.

1. Make copies of the maps you uploaded to SmartPath EMS VMA, label them, and take them with you for reference when installing the SmartPath APs.

2. For each SmartPath AP that you install, do the following:

   2.1 Make a serial connection to the console port, and log in (see "Log in through the console port" in Section 11.1, Example 1: Deploying a Single SmartPath AP).

   2.2 Enter the following command, in which `string1` describes the location of the SmartPath AP on the map (in open format) and `string2` is the name of the map:

   ```
   snmp location string1@string2
   ```

   For example, if you install a SmartPath AP in the northwest corner on the first floor of Building 1, enter snmp location northwest_corner@HQ-B1-F1. If you want to use spaces in the description, surround the entire string with quotation marks: snmp location "northwest corner@HQ-B1-F1".

   If you want, you can include some or all of the map hierarchy in the SNMP location string. For example, if a map named "floor-1" is nested under a higher level map named "building-1", then enter the command as follows: snmp location northwest_corner@floor-1@building-1 . Similarly, if these two maps are nested under a higher level map named "campus-1", then include that next higher level in the SNMP location string: snmp location northwest_corner@floor-1@building-1@campus-1. Although including the map hierarchy is unnecessary to identify a map in SmartPath EMS VMA—all map names must be unique—including the map hierarchy in the SNMP location can provide a simple way to check that preconfigured SmartPath APs get distributed to
   various sites correctly before they are installed.

   2.3 Mount and cable the SmartPath AP to complete its installation. (For mounting instructions, see the mounting section in the chapter for the SmartPath AP platform that you are installing.)

When a SmartPath AP connects to SmartPath EMS VMA, SmartPath EMS VMA checks its SNMP location and automatically associates it with the map specified in its SNMP location description. You can then click the icon to see its location and drag it to the specified location on the map. Also, on the Monitor > Access Points > SmartPath APs page (view mode: Config), you can sort detected SmartPath APs by map name to assign them more easily to WLAN policies.

NOTE: The first approach—using MAC addresses—makes the deployment considerably easier for installers, whereas the second approach—using SNMP—makes new SmartPath AP management easier for the SmartPath EMS VMA administrator. You can decide which approach makes the most sense for your team.

9.1.3 NetConfig UI

The clusterUI—the GUI configuration interface for SmartPath APs—is no longer used in its previous form to configure SmartPath APs. As the WLAN management model evolved and new services and integration abilities became available, the role of the SmartPath AP as a WLAN management portal changed. Now only a fundamental set of configuration options is available through a new Web user interface called the NetConfig UI. Using the NetConfig UI, you can configure basic network and SmartPath EMS VMA connectivity settings and upload new SmartPath OS images to the SmartPath AP hosting the NetConfig UI.

Accessing the NetConfig UI

To log in to the NetConfig UI on a SmartPath AP, you must first know the IP address of its mgt0 interface. If the SmartPath AP joins a network that provides devices with network settings through DHCP, the SmartPath AP acts as a DHCP client and automatically receives its network settings from the DHCP server. To learn which IP address the server dynamically assigned the SmartPath AP, note the MAC address of the SmartPath AP (it is labeled on the bottom of its chassis) and then check the list of IP-to-MAC address assignments on the DHCP server. You can also configure the DHCP server to sign the SmartPath AP a static IP address.

If the SmartPath AP joins a network that does not use DHCP, the SmartPath AP—after attempting to reach a DHCP server for about two minutes—fails over to its default IP address, 192.168.1.1. To access the NetConfig UI, you have several options:

- Manually set the network settings on your management system to 192.168.1.2/24 and connect an Ethernet cable between eth0 on the SmartPath AP and the Ethernet port on your system. You can then open a browser and connect to the NetConfig UI at the default IP address. Configure appropriate network settings for the mgt0 interface so that the SmartPath AP can access the network when cabled to it as a portal or when deployed as a mesh point and connecting wirelessly to the network through another SmartPath AP functioning as a portal. Disconnect the Ethernet cable between the SmartPath AP and your system and then connect the SmartPath AP to the network.
- Use the virtual access console, which is a special SSID solely for administrative access to the CLI. Using your wireless client, scan for an SSID named "BB-<clusterap-hostname>_ac". (The default host name for a SmartPath AP consists of "BB-" plus the last six digits of its MAC address, so the SSID will be something similar to "BB-123456_ac".) Select it, and when prompted to enter a network key, type Black Box, and then click "Connect." Check the IP address of the default gateway that the DHCP server on the SmartPath AP assigned your client. For example, in Windows, open the command prompt and enter ipconfig. Then make an SSH or a Telnet connection to the SmartPath AP at the default gateway IP address. When prompted to log in, enter the default login name and password: admin, Black Box. Enter the following commands to set an appropriate IP address and netmask for its mgt0 interface, and set the default gateway for the network segment to which you connect the SmartPath AP:

```
interface mgt0 ip <ip _ addr> <netmask>
ip route default gateway <ip _ addr>
```

You can then connect your management system to the same network, open a browser, and connect to the NetConfig UI at the IP address that you set.

- For SmartPath APs with console ports (SmartPath AP 300 series), you can connect to the console port and set a static IP address through the CLI. The console settings are 9600 bits per second, 8 data bits, no parity, 1 stop bit, and no flow control. After you log in, enter the two commands shown above to define network settings that are appropriate for the SmartPath AP.

Configuring a SmartPath AP through the NetConfig UI

When you log in to the NetConfig UI, there are three pages that provide settings for an initial configuration:

Local Network Settings: Configure the SmartPath AP to be a DHCP client or use static network settings for the IP address and netmask of its mgt0 interface, its default gateway, and DNS server.

SmartPath EMS VMA Configuration: A SmartPath AP makes various attempts to contact a CAPWAP server automatically (see "Automatically Discovering the CAPWAP Server"). To allow the CAPWAP discovery process to discover the SmartPath EMS VMA—the CAPWAP server—automatically, do not configure the settings on this page. However, if you want to define the SmartPath EMS VMA network settings for the SmartPath AP to use, you can do so here.

Upgrade SmartPath OS Software: You can update the SmartPath OS firmware by uploading a SmartPath OS image file directly from your local computer or from a network server.

Local Network Settings

The Local Network Settings page is the initial page that appears when you log in to the NetConfig UI.

If you want the SmartPath AP to use a configuration supplied by a DHCP server, click "Local Network Settings," select "DHCP Client," and then click "Apply."

If you want to configure the network settings manually, click "Local Network Settings," select "Static Network Settings," enter the following, and then click "Apply:"

Interface IP Address: Type the IP address that you the SmartPath AP to use for its mgt0 interface.

Netmask: Enter an appropriate netmask for the subnet to which the mgt0 interface connects.

Gateway: Enter the IP address of the router through which the SmartPath AP sends traffic beyond its immediate subnet.

DNS Server: Type the IP address of the primary DNS server.

SmartPath EMS VMA Configuration

Although a SmartPath AP automatically attempts to discover a physical SmartPath EMS VMA appliance, SmartPath EMS VMA Virtual Appliance, or SmartPath EMS Online, you can also specify a particular SmartPath EMS VMA instance. To configure how the SmartPath AP communicates with SmartPath EMS VMA, click "SmartPath EMS VMA Configuration," enter the following, and then click "Apply:"

SmartPath EMS VMA IP Address or Host Name: Type the IP address of the SmartPath EMS VMA interface—MGT or LAN—to which the SmartPath AP forms a CAPWAP connection, or type a domain name that resolves to that address. The SmartPath AP acts as a CAPWAP client and SmartPath EMS VMA acts as a CAPWAP server for all SmartPath AP-SmartPath EMS VMA communications. The default CAPWAP server configured on a SmartPath AP is staging.blackbox.com, which the SmartPath AP uses if it cannot discover a CAPWAP server on the local network.

Port: Type the port number you want the SmartPath AP to use to communicate with SmartPath EMS VMA. The default is UDP Port 12222, but if the SmartPath AP cannot form a connection on that port, it tries on TCP Port 80 (HTTP).

Use HTTP for SmartPath AP communications with SmartPath EMS VMA: Selecting this checkbox forces the SmartPath AP to attempt to communicate with SmartPath EMS VMA solely on Port 80 (HTTP) without trying to establish a connection on Port 12222 first. Enabling this option when there is a firewall in front of the SmartPath AP that only permits outbound HTTP traffic can accelerate the CAPWAP connection process by bypassing the initial attempts to use UDP Port 12222.

Send SmartPath AP communications with SmartPath EMS VMA through an HTTP proxy server: If you configure the SmartPath AP to use Port 80 (HTTP) to communicate with SmartPath EMS VMA, you can also configure it to use an HTTP proxy server to make that connection. When you select this checkbox, the form expands to display the proxy configuration controls. To configure connection settings with an HTTP proxy, select this checkbox, and then enter the following:

IP Address or Domain Name: Type the IP address of the HTTP proxy server or a domain name that resolves to its IP address.

Port: Type the port number that the SmartPath AP uses to connect to the HTTP proxy server.

Authenticate the SmartPath AP on the HTTP proxy server: Select this checkbox if the HTTP proxy server requires connections to be authenticated. Selecting this checkbox activates the user name and password fields.

User Name: Enter the user name that the SmartPath AP submits to authenticate itself to the HTTP proxy server.

Password: Enter the password that the SmartPath AP submits to the HTTP proxy server along with its user name.

Upgrade SmartPath OS Firmware

You can use the NetConfig UI to update the SmartPath OS firmware running on the SmartPath AP. First, download the latest SmartPath OS image for your SmartPath AP from the Black Box Support site and save it to your local workstation. After that, log in to the NetConfig UI, click "Upgrade SmartPath OS Software," enter the following, and then click "Apply:"

Image File: Click "Browse," navigate to the image file, select it, and then click "Open."

If you want to activate the new image automatically, select "Activate after" and enter the number of seconds that you want the SmartPath AP to wait before rebooting. The default wait is 300 seconds (five minutes).

If you do not want the SmartPath AP to activate the firmware automatically, select "Activate at next reboot." If you select this option, the SmartPath AP loads the new firmware the next time it boots up.

9.2 Example 2: IEEE 802.1x with an External RADIUS Server

You can configure SmartPath APs to act as RADIUS authenticators, also known as RADIUS clients or network access server (NAS) devices. They forward IEEE 802.1X/EAP user authentication requests and responses between wireless supplicants and up to four RADIUS authentication servers (a primary and three backups). In this example, you configure two SmartPath APs to act as RADIUS authenticators. They provide network access to wireless clients/RADIUS supplicants and pass authentication requests between the supplicants and a RADIUS authentication server.

NOTE: This example makes several assumptions about the RADIUS authentication server: (1) user accounts are already stored on it; (2) it listens on UDP port 1812 for authentication requests; (3) it uses "t6bEdmNfot3vW9vVr6oAz48CNCsDtInd" as its shared secret; (4) it allows RADIUS authentication requests from NAS devices in the 10.1.1.0/24 subnet. For configuration details, consult the product documentation for your RADIUS server.

You also configure an SSID that makes use of IEEE 802.1X/EAP authentication on the SmartPath AP authenticators. Because an SSID using 802.1X/EAP authentication can support numerous user profiles, the example shows how two groups of users—employees and IT staff—can access the same SSID but be assigned to two different VLANs. See Figure 9-6.

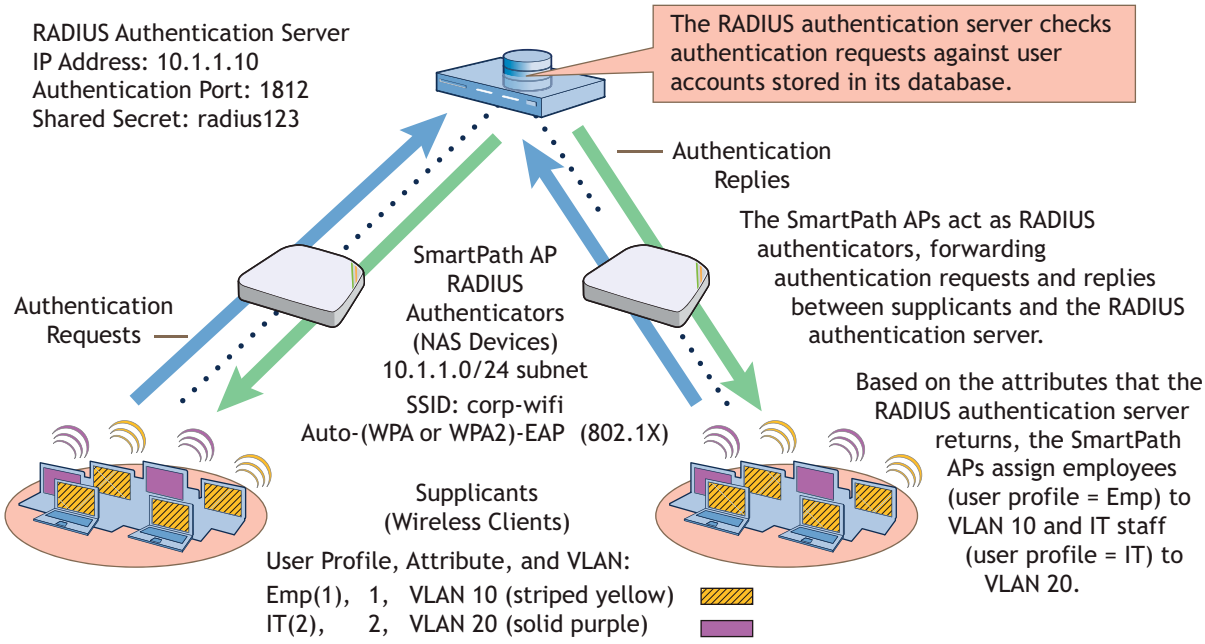


Figure 9-6. Authentication requests and replies for wireless clients on two SmartPath APs.

This example assumes that you have already accepted the SmartPath APs for SmartPath EMS VMA management, assigned them to a WLAN policy that includes a cluster and at least one SSID, and pushed that configuration to them. In other words, the SmartPath APs are already under SmartPath EMS VMA management by the time you begin the configuration in this example. If that is not yet the case, see Chapter 8 before continuing.

VLANs and User Profiles

To begin, you create two VLAN objects and then two user profiles, each of which references one of the VLANs. When you configure the SSID later, you reference both user profiles in the SSID configuration. With this approach, the SmartPath APs apply different VLANs to traffic from different users based on their corresponding user profiles.

1. To create a VLAN object for employee traffic, click "Configuration > Advanced Configuration > Network Objects > VLANs > New," and then enter the following in the VLANs dialog box:

   VLAN Name: VLAN-10

   Enter the following, and then click "Apply:"

   VLAN ID: 10

   Type: Global

   Setting the type as "Global" means that SmartPath EMS VMA applies the VLAN entry to all SmartPath APs that include the VLAN object in their configuration—unless you add another VLAN entry to this VLAN object and assign it a more specific classification type such as a classifier tag, map, or SmartPath AP. Then the SmartPath AP applies the other VLAN entry if it has the same classifier tag, is on the specified map, or is the specified SmartPath AP.

   Description: VLAN for employees

2. To save the configuration and close the VLANs dialog box, click "Save."

3. To create a VLAN object for IT staff traffic, select the check box for the newly created VLAN object "VLAN-10" in the list on the Configuration > Advanced Configuration > Network Objects > VLANs page, and then click Clone.

   The VLANs dialog box appears with the settings for VLAN-10.

4. For VLAN Name, enter VLAN-20; in the VLAN ID field, change 10 to 20; modify the Description field to VLAN for IT staff; and then click "Save."

   You can see the two newly created VLAN objects on the Configuration > Advanced Configuration > Network Objects > VLANs page.

5. To create a user profile for employees, click "Configuration > User Profiles > New," enter the following, leave the other settings as they are, and then click "Save:"

   Name: Emp(1)

   Including the attribute number "(1)" as part of the user profile name is helpful when troubleshooting and when configuring the RADIUS server. The name "Emp(1)" serves as reminder to use 1 as the Tunnel-Private-Group-ID attribute when configuring the RADIUS server. SmartPath APs use a combination of three RADIUS attributes to determine which user profile to assign to an authenticated user: Tunnel-Type = GRE (10), Tunnel-Medium-Type = IP (1), and Tunnel-Private-Group-ID = <number>. If a SmartPath AP receives all three attributes and the third one matches a user profile attribute, it then applies that user profile to traffic from the authenticated user. Including the attribute number in the user profile name makes configuring the RADIUS server a bit simpler.

   Attribute Number: 1

   Default VLAN: VLAN-10

   Description: For employees to use VLAN 10

6. To create a user profile for IT staff, select the check box of the user profile that you just created, "Emp(1)", and then click Clone.

   The User Profiles dialog box appears with the settings for Emp(1).

7. For Name, enter IT(2); for Attribute Number, enter 2; for Default VLAN, choose VLAN-20, modify the text in the Description field to For IT staff to use VLAN 20, and then click Save.

SmartPath APs as RADIUS Authenticators

SmartPath AP RADIUS authenticators provide network access to wireless clients and pass authentication requests between the wireless clients acting as RADIUS supplicants and a RADIUS authentication server. In this section, you configure the settings that control how the SmartPath APs communicate with the RADIUS authentication server.

Click Configuration > Advanced Configuration > Authentication > AAA Client Settings > New, and enter the following:

RADIUS Name: RADIUS-10.1.1.10

This is a name for the RADIUS configuration object on SmartPath EMS VMA. Provide it with a useful name that easily identifies it to you. The name can be up to 32 characters and cannot contain spaces.

Description: HQ RADIUS server with employee accounts

Enter a useful comment about the configuration. It can be up to 64 characters, including spaces.

In the RADIUS Servers section, enter the following to define the necessary network and security settings for making secure connections with the RADIUS authentication server:

Click the New icon to the right of the IP Address/Domain Name drop-down list, and define the IP address of the RADIUS authentication server in the IP Objects/Host Names dialog box that appears:

IP Address: (select; this setting automatically applies a netmask of 255.255.255.255)

Object Name: AuthServer-10.1.1.10

Enter the following, and then click Apply to add the IP address to the address configuration:

IP Entry: 10.1.1.10

Type: Global

Setting the type as "Global" means that SmartPath EMS VMA applies the IP entry to all SmartPath APs that include the IP address/host name object in their configuration.

Description: RADIUS auth server at 10.1.1.10

Click "Save" to save the address configuration and return to the AAA Client Settings page.

IP Address/Domain Name: AuthServer-10.1.1.10 (This is the address that you just created.)

Server Type: Authentication

You can define the service that the RADIUS server provides: authentication, accounting, or both (auth/acct). In this example, the server only authenticates users, so there is no need to enable accounting. When RADIUS accounting is enabled, the RADIUS authenticators report the status and cumulative length of RADIUS supplicant sessions to the RADIUS authentication server. Accounting is often used to track client activity so that users can be accurately charged for network use. It is also sometimes used to gather statistics about general network usage.

Shared Secret: t6bEdmNfot3vW9vVr6oAz48CNCsDtInd

Confirm Secret: t6bEdmNfot3vW9vVr6oAz48CNCsDtInd

The shared secret that you enter here must exactly match that on the RADIUS authentication server. Because the authentication server and authenticators use it to verify each other's identities when establishing a RADIUS session, it is important that the shared secret be fairly strong. Therefore, you use the longest string possible—32 alphanumeric characters—randomly arranged. To see the text strings that you enter, clear the Obscure Password checkbox.

Server Role: Primary

To provide server redundancy, you can configure up to four RADIUS servers, designating one as the primary server and the others as backup servers. The RADIUS authenticators only send RADIUS authentication requests to the backup servers when the primary server becomes unreachable. Because only one RADIUS server is configured in this example, it must be designated as the primary.

To add the RADIUS authentication server to the AAA client settings configuration, click Apply.

In the Advanced Settings section, you can change the RADIUS authentication port number, enable RADIUS accounting, and change the RADIUS accounting port number. For this example, keep their default values.

Authentication Port: 1812

UDP port 1812 is the default port number on which RADIUS servers listen for authentication requests. In this example, the RADIUS server is using the default port number. If your RADIUS server listens on a different port, make sure that you enter that port number here.

Accounting Port: 1813

UDP port 1813 is the default port number on which RADIUS accounting servers listen for accounting reports. In this example, accounting is not enabled, so this setting is irrelevant.

You can expand the Optional Settings section at the bottom of the page to modify additional settings pertaining to RADIUS; however, the default settings work well for this example and do not need to be changed.

Retry Interval: 600 seconds (the default setting)

This field is only relevant when both primary and backup RADIUS authentication servers are configured. The retry interval defines how long a SmartPath AP RADIUS authenticator waits before retrying a previously unresponsive primary RADIUS server, even if the current backup server is responding. When there is only a single RADIUS authentication server, as in this example, the retry interval does not matter.

Accounting Interim Update Interval: 20 seconds (the default setting)

This setting defines the interval for sending RADIUS accounting updates to report the status and cumulative length of RADIUS supplicant sessions. This setting is important when enforcing RADIUS accounting, which is not involved in the present example. Therefore, this setting is irrelevant here.

Permit Dynamic Change of Authorization Messages (RFC 3576): (clear; the default setting)

This option allows SmartPath AP RADIUS authenticators to accept unsolicited disconnect and Change of Authorization (CoA) messages from the RADIUS authentication server by enabling the dynamic authorization extension provided in RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS). "Disconnect" messages terminate a user's session immediately, and CoA messages modify session authorization attributes such as VLANs and user profile IDs. The ability for SmartPath AP RADIUS authenticators to accept these messages from the RADIUS authentication server is not required in this example, so it remains disabled.

To save the configuration as "RADIUS-10.1.1.10" and close the dialog box, click Save.

Defining an SSID with 802.1X/EAP Authentication

Define an SSID that supports 802.1X/EAP authentication and directs the SmartPath AP RADIUS authenticators to forward authentication requests from RADIUS supplicants to the RADIUS authentication server that you just defined.

Click "Configuration > SSIDs > New," enter the following, leave all other values at their default settings, and then click "Save:"

Profile Name: corp-wifi

SSID: corp-wifi

Description: Employee and IT WLAN access; 802.1X

SSID Access Security: WPA/WPA2 802.1X (Enterprise)

Use Default 802.1X Settings: (select)

By default, when a SmartPath AP hosts a WPA/WPA2 802.1X (Enterprise) SSID, it negotiations with clients over the use of WPA or WPA2 for key management and TKIP or CCMP (AES) for encryption, and uses whichever methods each client supports. The SmartPath AP and client use EAP (802.1X) for authentication through an external RADIUS server.

RADIUS Server: RADIUS-10.1.1.10

User profile assigned if no attribute is returned from RADIUS after successful authentication: Emp(1)

The SmartPath AP RADIUS authenticator applies the user profile "Emp(1)" to users if the RADIUS authentication server successfully authenticates them and returns a Tunnel-Private-Group-ID attribute that matches the attribute for this user profile (1). The SmartPath AP also applies this profile to users if the RADIUS authentication server does not return any attributes.

If the RADIUS server authenticates a user and returns attributes that do not match an existing user profile, the user profile lookup will fail and SmartPath AP will reject the client.

User profiles assigned via attributes returned from RADIUS after successful authentication: Click IT(2) in the Available User Profiles list, and then click the right arrow (>) to move it to the Selected User Profiles list.

The SmartPath AP RADIUS authenticator applies the "IT(2)" user profile only if the RADIUS authentication server returns a Tunnel-Private-Group-ID attribute matching the attribute for this user profile (2).

Only the selected user profiles can be assigned via RADIUS for use with this SSID: (clear)

When cleared, this setting allows access to authenticated users even when the Tunnel-Private-Group-ID attribute that the RADIUS authentication server returns matches another user profile configured on the SmartPath AP but not specified for this SSID. If you do not mind granting access to all valid user accounts on the RADIUS authentication server, disable this option by clearing the checkbox. This is the default setting.

On the other hand, if you want to restrict access to authenticated users only when the RADIUS authentication server returns attributes that match one of the specified user profiles for the SSID, enable this option by selecting the checkbox and then specifying the action that you want to the SmartPath AP to take: ban the client for a period of time, ban it indefinitely, or simply disconnect it. You might want to enable this if the RADIUS authentication server contains accounts for users other than employees and IT staff—perhaps there are accounts for contractors and guests. Even though the server would approve authentication requests from such users if they submitted a correct user name and password, you might not want them to use this SSID to access the WLAN.

SSID Broadcast Band: 2.4 GHz (11n/b/g)

Assigning an SSID to the 2.4-GHz radio in access mode allows SmartPath APs to use their second radio, which operates at 5 GHz, for wireless backhaul communications.

Applying the RADIUS and SSID Settings to SmartPath APs

1. Click Configuration > WLAN Policies > (select the name of a WLAN policy that has already been applied to the SmartPath APs) > Add/Remove SSID Profile, select corp-wifi in the Available SSID Profiles list, click the right arrow (>) to move it to the Selected SSID Profiles list, click Apply to add the SSID to the WLAN policy, and then click Save to save the modified policy and close its dialog box.
2. Click Monitor > Access Points > SmartPath APs > (checkboxes for the two SmartPath AP RADIUS authenticators) > Update > Upload and Activate Configuration, enter the following, and then click Upload:

   Upload and activate configuration: (select)

   Upload and activate CWP pages and Server key: (clear)

   Upload and activate certificate for RADIUS and VPN services: (clear)

   Upload and activate employee, guests, and contractor credentials: (clear)

   Check boxes for both SmartPath APs: (select)

Connecting Supplicants to the WLAN

The 802.1X authentication process is somewhat different depending on the operating system on which the RADIUS supplicant is running and whether the client uses the user's login credentials to authenticate itself on a domain. If the supplicant is on a PC running Windows Vista® and is on a domain, and the RADIUS server is configured with domain authentication:

1. View the available SSIDs in the area, and select corp-wifi.
2. Click Connect.

Because most PC-based supplicants use their Windows login credentials to authenticate the client with the domain, the 802.1X authentication process happens automatically.

NOTE: If the supplicant is on a PC running Windows XP, you must configure it to use PEAP for authentication. By default, a Windows XP wireless client uses Smart Card or other Certificate instead of PEAP.

If the supplicant is Windows based and you are not on a domain:

1. Configure the SSID on your client as follows:

   Network name (SSID): corp-wifi

   Network authentication: WPA2

Data encryption: AES

Enable IEEE 802.1X authentication for this network: (select)

EAP type: Protected EAP (PEAP)

Authenticate as computer when computer information is available: (clear)

Authenticate as guest when user or computer information is unavailable: (clear)

Validate server certificate: (clear)

Select Authentication Method: Secured password (EAP-MSCHAP v2)

Automatically use my WIndows logon name and password (and domain if any): (clear)

2. View the available SSIDs in the area and select corp-wifi.
3. Click "Connect."
4. When the prompt appears for you to select a certificate or enter other credentials to validate your identity, click the prompt, enter the user name and password stored on the RADIUS server, and then click "OK."

If the supplicant is on a Macintosh computer and is not on a domain, view the available SSIDs in the area, and select corp-wifi. Then click Join Network, and accept the certificate that the RADIUS server provides, assuming it is from a trustworthy source. After the RADIUS server validates your identity, the client connects to the WLAN.

9.3 Example 3: Providing Guest Access through a Captive Web Portal

A captive Web portal is a way to control network access by requiring users to authenticate their identity or complete a registration form before assigning them network and user profile settings that allow them network access beyond the SmartPath AP with which they associated. A captive web portal provides registered users with network access while containing unregistered users. Because the Black Box captive web portal feature is very flexible, you will have a number of choices to make when configuring it. Several of these are examined first—"Registration Types," "Providing Network Settings", and "Modifying Captive Web Portal Pages"—and then a complete configuration example is presented.

9.3.1 Registration Types

There are five types of registration (four are shown in Figure 9-7) that a captive Web portal can require of users:

Self-Registration: With this option, users must complete a registration form and accept a network use policy before being allowed to pass through the captive Web portal. This is a good choice when you cannot know in advance who will be attempting to make a network connection through the captive Web portal and simply want to keep a record of the users, or if user authentication is unimportant.

User Authentication: With this option, users must enter and submit a valid user name and password to log in. The SmartPath AP acts as a RADIUS authenticator or RADIUS client and forwards the submitted login credentials to a RADIUS server for authentication. The RADIUS authentication server can either be an internal server on a SmartPath AP or an external RADIUS server on the network. This is a good choice when you can set up a RADIUS authentication server with user accounts before the users attempt to access the network.

Both (Auth/Self-reg): This is a combination of the previous two registration types. Users can authenticate themselves by submitting a user name and password or complete and submit a registration form.

Private PSK Server: This option automatically assigns users with a private PSK after they either self-register or authenticate themselves.

Use Policy Acceptance: With this option, the user is presented with a network use policy, and only has to click Accept to gain network access.

External Authentication: SmartPath APs redirect unregistered users' HTTP and HTTPS traffic to a captive Web portal on an external server, such as the amigopod Visitor Management Appliance.

Self-Registration

The user self-registers by entering data that can then be saved to a syslog server for tracking and auditing.

Both (Auth/Self-reg)

Authentication at the top and self-registration at the bottom (the user submits one of them).

User Authentication

The user submits a name and password, which are sent to a RADIUS server for authentication.

Use Policy Acceptance

The user must accept a network use policy to gain network access.

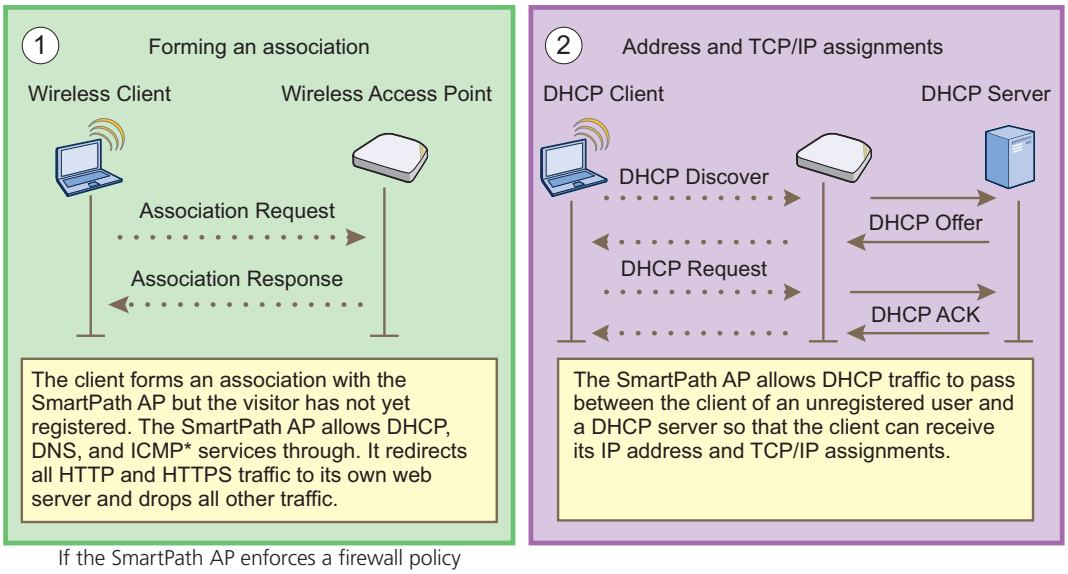
Figure 9-7. Four types of registration through a captive Web portal running on a SmartPath AP.

9.3.2 Providing Network Settings

In addition to various registration types, Black Box offers two approaches to providing captive Web portal clients with network settings. One approach uses external DHCP and DNS servers on the network, and the other uses internal DHCP and DNS servers on the SmartPath AP itself.

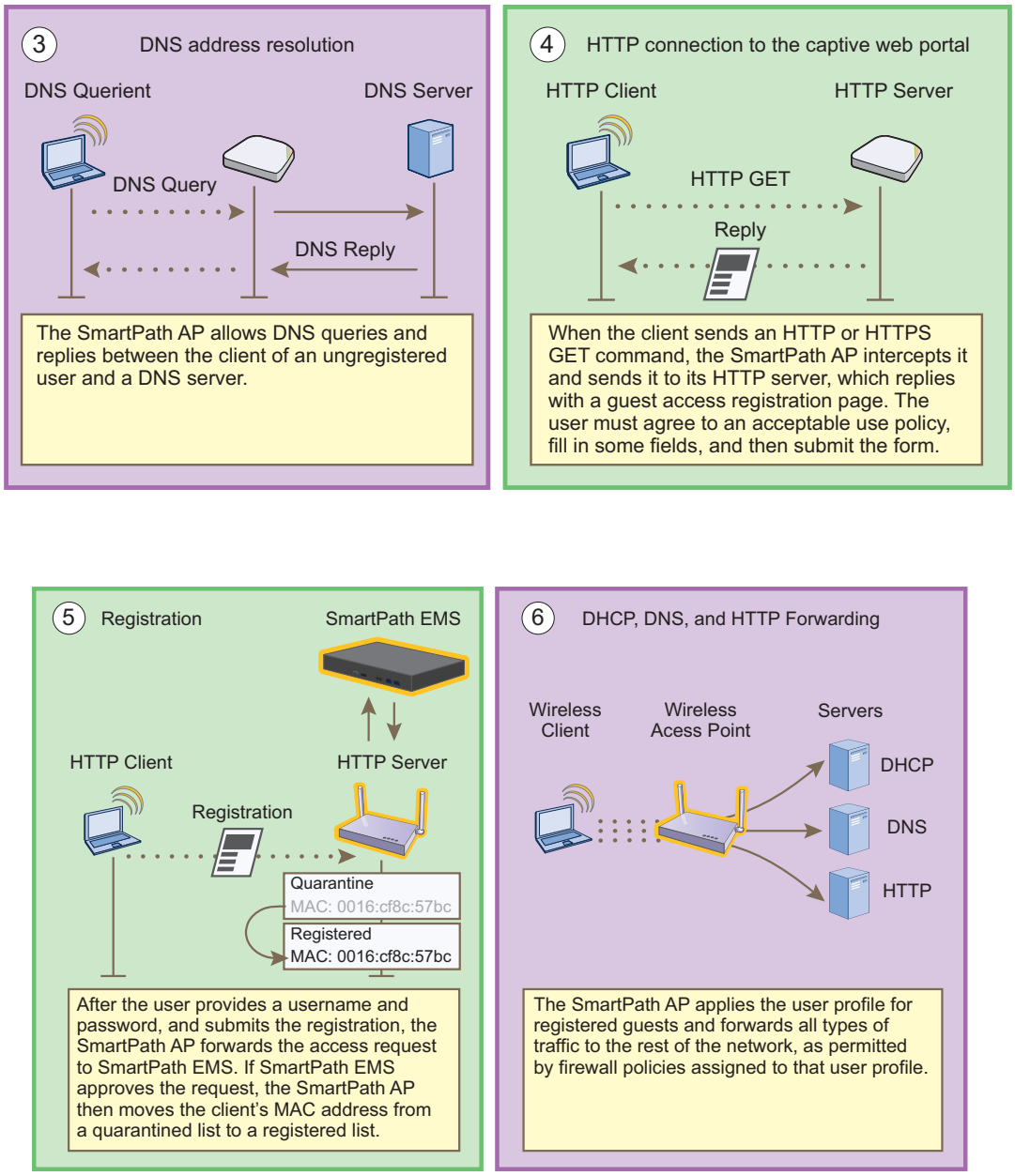
Captive Web Portal with External DHCP and DNS Servers

With this approach, when the client of a previously unregistered visitor first associates with the guest SSID, the SmartPath AP allows DHCP and DNS traffic to pass through so that the client can receive its address and TCP/IP assignments and resolve domain names to IP addresses. It also allows ICMP traffic for diagnostic purposes. However, the SmartPath AP intercepts all HTTP and HTTPS traffic from that client—and drops all other types of traffic—thereby limiting its network access to just the SmartPath AP with which it associated. No matter what website the visitor tries to reach, the SmartPath AP directs the visitor's browser to a registration page. After the visitor registers, the SmartPath AP stores the client's MAC address as a registered user, applies the appropriate user profile to the visitor, and stops keeping the client captive; that is, the SmartPath AP no longer intercepts HTTP and HTTPS traffic from that MAC address, but allows the client to access external web servers. The entire process is shown in Figure 9-8.



If the SmartPath AP enforces a firewall policy that blocks ICMP services from registered users, it will also block them from unregistered users. In contrast to ICMP, DHCP and DNS are essential services that must always be permitted by the SmartPath AP firewall.

Figure 9-8. Captive Web portal exchanges using external DHCP and DNS servers.

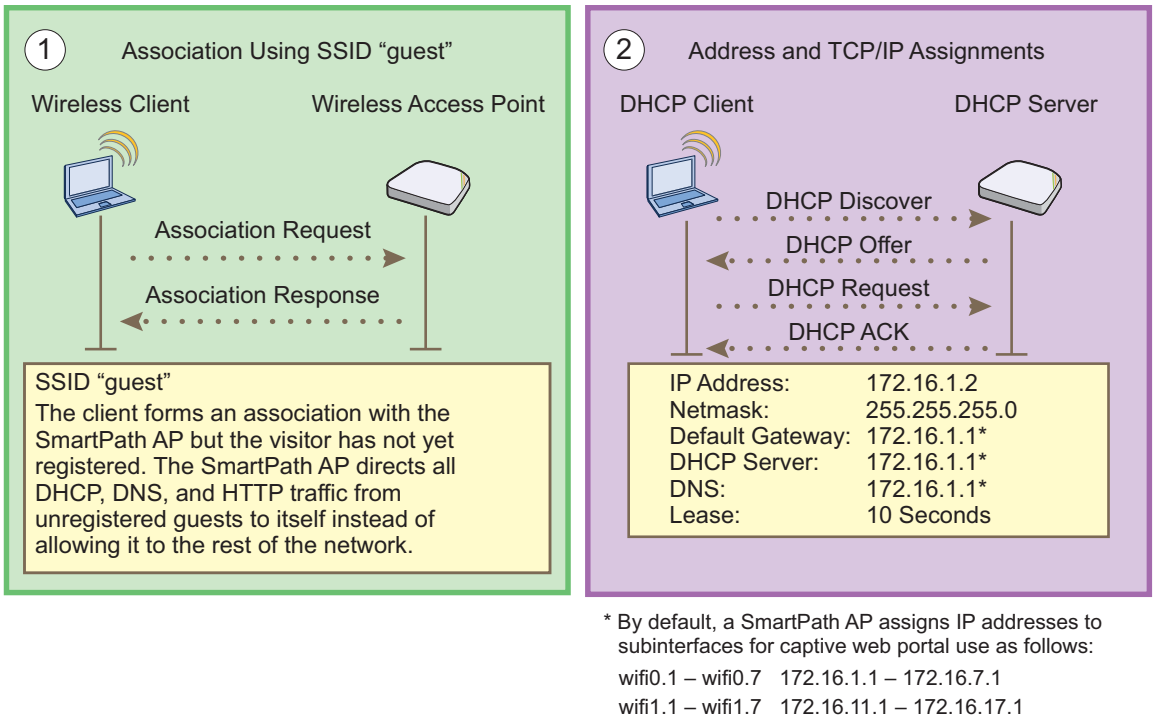


Figures 9-9 and 9-10. Captive Web portal exchanges using HTTP.

To enable the captive web portal to forward DHCP and DNS traffic from unregistered users to external servers on the network, click Configuration > Advanced Configuration > Authentication > Captive Web Portals > New, and select Use external DHCP and DNS servers on the network.

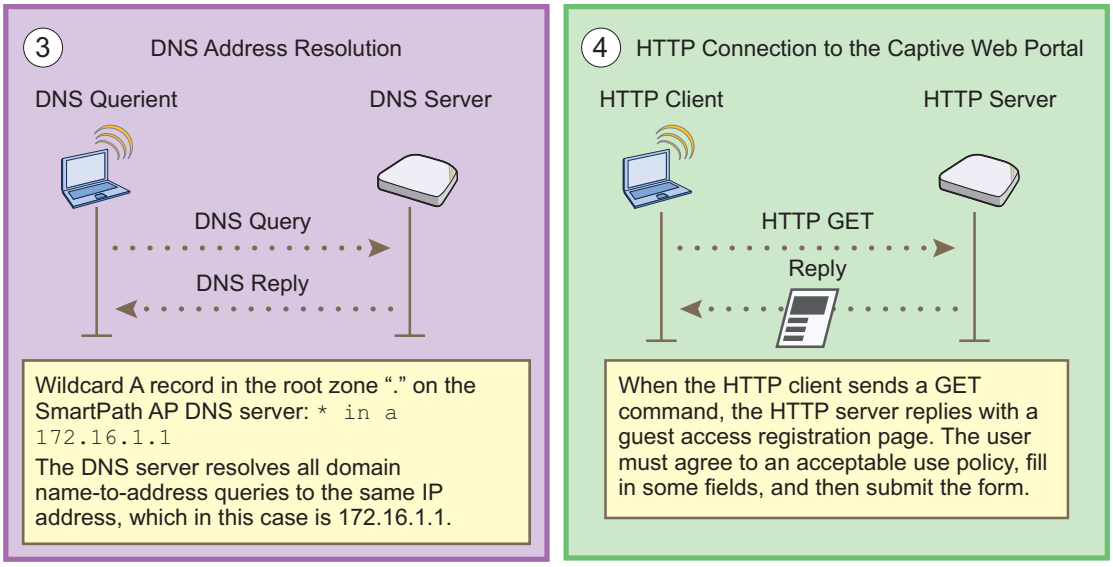
Captive Web Portal with Internal DHCP and DNS Servers

With this approach, when the client of an unregistered user first associates with the SmartPath AP, it acts as a DHCP, DNS, and Web server, limiting the client's network access to just the SmartPath AP with which it is associated. No matter what website the user tries to reach, the SmartPath AP directs the browser to a registration page. After the user registers, the SmartPath AP stores the client's MAC address as a registered user and stops keeping the station captive; that is, the SmartPath AP no longer acts as a DHCP, DNS, and web server for traffic from that MAC address, but allows the client to access external servers. The entire process is shown in Figures 9-11 and 9-12.



* By default, a SmartPath AP assigns IP addresses to subinterfaces for captive web portal use as follows:

wifi0.1 – wifi0.7 172.16.1.1 – 172.16.7.1
wifi1.1 – wifi1.7 172.16.11.1 – 172.16.17.1



Figures 9-11 and 9-12. Captive Web portal exchanges using internal servers, Steps 1–4.

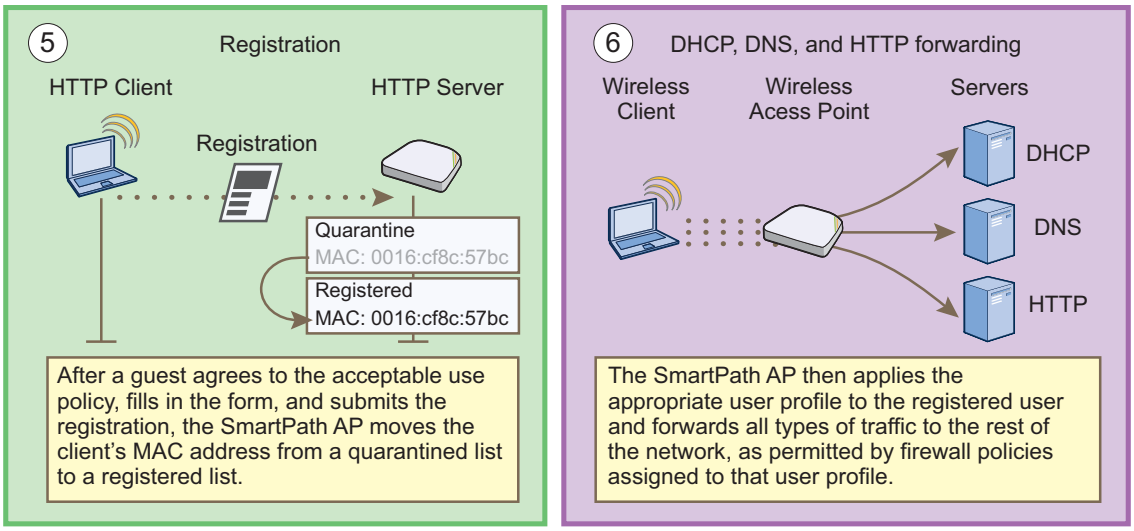


Figure 9-13. Captive Web portal exchanges using internal servers, Steps 5–6.

To enable the captive Web portal to forward DHCP and DNS traffic from unregistered users to its internal servers, click Configuration > Advanced Configuration > Authentication > Captive Web Portals > New, and select Use internal DHCP and DNS servers on the SmartPath AP. By default, the internal DHCP server issues leases with a ten-second lifetime, and if a client with a nonexistent lease requests a lease renewal, the SmartPath AP responds by broadcasting a DHCP NAK. You can change the SmartPath AP response so that it sends a unicast NAK or ignores the request completely (Keep Silent).

9.3.3 Modifying Captive Web Portal Pages

Black Box provides .html files and images for use on the captive Web portal server and a tool in the GUI to modify the supplied text, colors, and images to better suit the needs of your organization. The various file names and their purposes are as follows. An example of the default web page components is shown in Figure 9-14:

- registration.html (the main login page for self-registration)
- authentication.html (the main login page for user authentication)
- auth-reg.html (the main login page for either self-registration or user authentication)
- eula.html (the login page for the acceptable use policy)
- success.html (the page that appears after registering successfully)
- blackbox_3d.jpg (default main image on the web pages)
- failure.html (the page that appears after an unsuccessful registration attempt)
- blackbox_hex_light.jpg (optional background image)
- reg.php (a file that the SmartPath AP generates automatically and stores on its internal Web server)
- blackbox_hex_dark.jpg (optional background image)
- blackbox_spacer.png (a transparent image that provides space at the top of Web pages; size 200 x 103 px)
- blackbox_logo_reverse.png (Black Box logo with white text at the bottom of the Web pages; size 111 x 48 px)
- blackbox_3d_bg.png (an image that provides blue filler as background around the main image; size 5 x 5 px)
- blackbox_logo.png (Black Box logo with dark text; size 111 x 48 px)
- use-policy.html (the page that appears when you click the Acceptable Use Policy link on the registration.html or auth-reg.html pages)

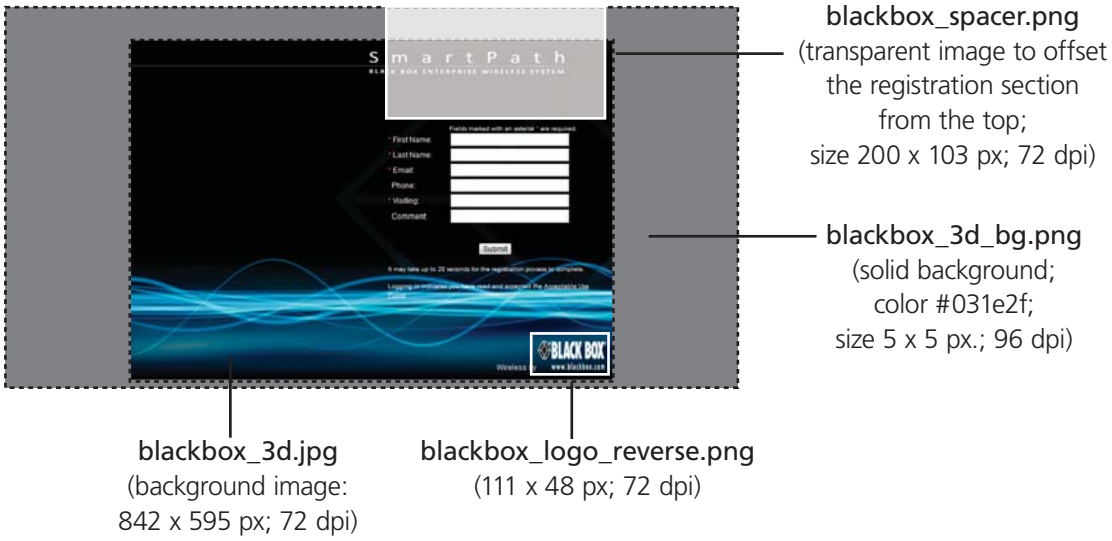


Figure 9-14. Components of the captive Web portal self-registration page.

Unregistered users' browsers are redirected to the login page of the captive Web portal for the SSID to which they associate. The login page might be registration.html, authentication.html, or auth-reg.html, depending on the registration method that you configure the portal to use. You can have a different registration page for each SSID.

To modify the default set of .html and image files for a captive Web portal, do the following:

1. Click Configuration > Advanced Configuration > Authentication > Captive Web Portals > New.
2. Enter a name for the captive Web portal configuration, and choose one of the following methods from the Registration Type drop-down list:

   User Authentication: Requires users to submit a valid user name and password to log in. The SmartPath AP then forwards the submitted login credentials to a RADIUS server for authentication.

   Self-registration: Requires users to enter data and accept a network use policy before being allowed to pass through the captive Web portal.

   Both (Auth/Self-reg): Requires users to submit either one of the two types of registration.

   Use Policy Acceptance: Requires users to accept a network usage policy before accessing the network.

   There is also a fifth option, External Authentication, which redirects unregistered users' HTTP and HTTPS traffic to a captive Web portal on an external server instead of redirecting it to an internal captive Web portal on a SmartPath AP. For information about configuring it, see the SmartPath EMS VMA on-line Help.)
3. To modify the login page, expand Captive Web Portal Login Page Settings, select Modify automatically generated Web pages, click Customize Login Page, modify any of the following settings to customize the look of the captive web portal pages, and then click Save:

   Background Image: You have three preloaded image files to use—blackbox_3d.jpg (default), blackbox_hex_dark.jpg, and blackbox_hex_light.jpg—and you can also import an image file of your choice.

   To import a background image, click Add/Remove to open the Add/Remove CWP Web Page Resources page. Click Browse, navigate to the image file and select it, and then click Upload.

   Whatever size the background image is, it eventually tiles. If you use an image that tiles seamlessly, the tiling cannot be noticed. See the two alternative background images with hexagons in the Background Image drop-down list for examples.

Foreground Color: The foreground color controls the color of the text that appears on the page. By default, it is white (RGB 255, 255, 255), which shows up clearly against the dark blue of the default background image smartpath_3d.jpg. If you change the background image to something with lighter colors, such as blackbox_hex_light.jpg, you can make the foreground color darker to provide greater contrast.

Header Image: This image file is empty and acts as a shim or spacer to offset the form from the top of the page. By default, the head image is smartpath_spacer.png, and it is 200 x 103 px at 72 dpi. If you want to increase or decrease the space above the form, you can replace this with a different .png file. The file format is Portable Network Graphics (PNG) because it supports transparency. You can also replace it with a file containing an image if you prefer.

Footer Image: By default, this is a graphic of the Black Box logo. The file name is blackbox_logo_reverse.png and its dimensions are 111 x 48 px at 72 dpi. If you replace this with a different image, make sure it has the same or nearly the same dimensions to avoid distortion.

Use Policy: This is a text file that states the company policy for network usage. A user can view the policy by clicking the "Acceptable Use Policy" link on the registration page during the captive web portal registration process. A generic policy is provided in the "use-policy.txt" file. You can export this file, edit it, and import the edited file, or replace it with a completely different file.

NOTE: You can check how your customizations affect page appearance by clicking Preview.

4. In a similar manner, you can also modify the automatically generated pages that appear after a successful login and after an unsuccessful one. These pages appear after a user successfully registers or fails to register. The file names are success.html and failure.html and are called by the internal script reg.php. The background image, foreground color, header image, and footer image function similarly to those on the Login page. You can specify the same images or different ones on the result pages, and you can use preloaded images or import others to use instead.

NOTICE: The main difference between the success page and the login page is the notice that is displayed to users. By default, the notice is "You are now connected to the wireless network." You can modify this to a different message as long as it has fewer than 256 characters. You can click inside the text box and edit the text on-screen or copy text from an external source and paste it into the text box.

NOTE: In addition to modifying the images and text for the preloaded HTML files and importing new image files, you can also import entire Web pages. In the sections for the login page, success page, and failure page, select Import custom Web pages, click Add/Remove, browse to the files that you want to import, and then click Upload.

You can also export the default captive Web portal HTML and image files from SmartPath EMS VMA and use them for reference when designing new ones. To do that, click the Export option at the top of the Configuration > Advanced Configuration > Authentication > Captive Web Portals > New page.

9.3.4 Configuring a Captive Web Portal

In this example, you configure a captive Web portal to provide guests with wireless network access. The configuration includes the following elements:

- Captive Web Portal—Define a captive Web portal that uses self-registration, the auto-generated Web pages provided in SmartPath EMS VMA, and external DHCP and DNS servers.
- QoS Rate Limiting—To preserve bandwidth for employees, reduce the rate limit for guests somewhat.
- Firewall Policy—To maintain security, restrict visitors to accessing just the public network.
- User Profile—Apply the QoS rate limiting and firewall policy to the user profile that the SmartPath AP applies to traffic from successfully registered users.
- SSID—Configure an SSID that secures wireless traffic with a preshared key and permits access to the public network only through the captive Web portal.
- WLAN Policy—Add the SSID to a WLAN policy.

• Files and Configuration Upload—Push the captive web portal files and the WLAN policy to the managed SmartPath APs.

Guests use a preshared key to secure wireless traffic between their wireless clients and SmartPath APs. After forming a secure association with a SmartPath AP, the SmartPath AP intercepts all outbound traffic—except DHCP, DNS, and ICMP traffic—and presents them with a self-registration page. The guests must complete a form and accept a network usage policy before being allowed to access the public network. Registered visitors' activity can be tracked and stored in historical logs on a syslog server for security and compliance auditing.

Captive Web Portal

To create a captive Web portal requiring users to self-register to gain network access, click Configuration > Advanced Configuration > Authentication > Captive Web Portals > New, enter the following, leave all the other values at their default settings, and then click Save:

Name: CWP-guest1

Registration Type: Self-registration

Description: Captive Web portal for guest registration

Leaving everything else at its default setting creates a captive Web portal configuration that uses all the predefined Web files and the default network settings. The DHCP, DNS, and ICMP traffic from the clients of unregistered users is allowed to pass through the SmartPath AP to external servers.

QoS Rate Limiting

To allot guests with enough bandwidth to satisfy basic network access but not enough to interfere with employee traffic, click Configuration > Advanced Configuration > QoS Policies > Rate Control & Queuing > New, enter the following, and then click Save:

Name: QoS-Guests

Per User Rate Limit: 2000 kbps for 802.11a/b/g; 2000 kbps for 802.11n

This is the maximum amount of bandwidth that a single user belonging to this profile can use. It is far less than the bandwidth you can reserve for other users such as employees, but it should be sufficient for basic Web access for visitors.

Description: QoS per guest

Per User Queue Management: Enter the following items in bold, and leave all other settings unchanged:

Table 9-1. QoS rate limiting parameters.

Class Number—Name	Scheduling Type	Scheduling Weight	Weight % (Read Only)	Policing Rate Limit (kbps) (8-2.11a/b/g)	Policing Rate Limit (kbps) (802.11n)
7—Network Control	Strict	0	0	0	0
6—Voice	Strict	0	0	0	0
5—Video	Weighted Round Robin	60	28	2000	2000
4—Controlled Load	Weighted Round Robin	50	23	2000	2000
3—Excellent Effort	Weighted Round Robin	40	19	2000	2000
2—Best Effort 1	Weighted Round Robin	30	14	2000	2000
1—Best Effort 2	Weighted Round Robin	20	9	2000	2000
0—Background	Weighted Round Robin	10	4	2000	2000

The rate limit for network control and voice is 0 kbps because guests are not permitted to run any applications that would generate network control traffic or use VoIP applications. In this example, guests are expected to use cell phones or other phones provided for them. (If you want to provide VoIP for guests, then you must enable the SIP ALG, add another rule to the firewall policy permitting SIP traffic, and set the rate limit for voice at 128 kbps.)

Firewall Policy

You create a firewall policy that permits outgoing HTTP and HTTPS traffic from within the corporate network to the public network but not to the corporate network itself. When applying the policy to a user profile, you apply a default action that denies all incoming traffic and all other unspecified types of outgoing traffic.

Address Objects

To make address objects for use in firewall rules to block traffic to private IP address space in the internal network, click Configuration > Advanced Configuration > Network Objects > IP Objects/Host Names > New, enter the following, and then click Apply:

Network: (select)

Object Name: 10.0.0.0/8

In the IP Entry field, enter 10.0.0.0 for the IP address, 255.0.0.0 for the netmask, choose Global for the type, enter a useful description such as Deny RFC 1918 (private addresses), and then click Apply.

To save the address and close the dialog box, click "Save."

Repeat the above to create two more address objects, one for 172.16.0.0/12 (IP address = 172.16.0.0; netmask = 255.240.0.0) and another for 192.168.0.0/16 (IP address = 192.168.0.0; netmask = 255.255.0.0).

Custom Service

To make a custom service for NAT-T (NAT Traversal) to permit IKE traffic when traversing a NAT device, click Configuration > Advanced Configuration > Network Objects > Network Services > New, enter the following, and then click Save:

Name: NAT-T

Description: NAT Traversal

IP Protocol: UDP (17)

Port Number: 4500

Service Idle Timeout: 1800

ALG Type: (leave blank)

Firewall Policy Rules

To create an IP firewall policy to control outgoing traffic, click Configuration > Advanced Configuration > Security Policies > IP Policies > New, and enter the following:

Policy Name: guest-IP-policy-from-access

Description: Allow guests to access the public network

To add rules to permit DHCP, DNS, HTTP, HTTPS, IKE, and NAT-T to the public network while denying any type of traffic to the internal network, enter the following (CTRL-click to select multiple services):

Table 9-2. CTRL-click to select multiple services.

(Action)	Source	Destination	Service‡	Action	Logging*	(Action)
	[-any]	[-any-]*	DHCP-Server, DNS†	Permit	Off	Click "Apply."
Click "New."	[-any-]	10.0.0.0/8	[-any-]	Deny	Dropped Packets	Click "Apply."
Click "New."	[-any-]	172.16.0.0/12	[-any-]	Deny	Dropped Packets	Click "Apply."
Click "New."	[-any-]	192.168.0.0/16	[-any-]	Deny	Dropped Packets	Click "Apply."
Click "New."	[-any-]	[-any-]	HTTP, HTTPS, IKE, NAT-T	Permit	Both	Click "Apply."
Click "New."	[-any-]	[-any-]	[-any-]	Deny	Dropped Packets	Click "Apply."

* You do not enable logging for DHCP and DNS services because they would generate too many log entries. You enable logging for packets that SmartPath EMS VMA drops because of the enforcement of rules that deny traffic (Dropped Packets) and the logging of
session initiation and termination (Both) for traffic permitted by policy rules.

†Because the source for DHCPDISCOVER and DHCPREQUEST messages does not yet have an IP address and the destination is 255.255.255.255 for broadcast traffic, both the source and destination IP addresses must be set as "[-any-]".

‡Press the SHIFT key while selecting multiple contiguous services, and the CTRL key while selecting multiple contiguous or non-contiguous services. When you click Apply, SmartPath EMS VMA generates a separate rule for each service.

SmartPath EMS VMA adds new rules to the bottom of the rule list, so that if you enter the rules in the order presented above, they will already be in the correct positions, as shown in Figure 9-15. The SmartPath AP firewall checks policy rules from top to bottom and applies the first match that it finds.

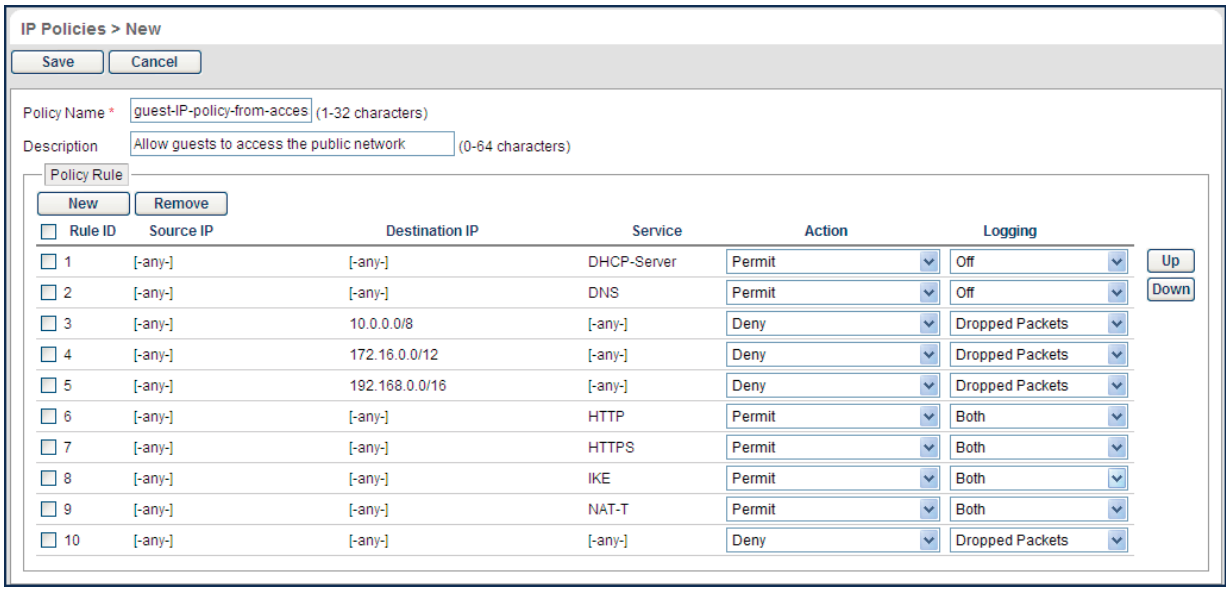


Figure 9-15. Firewall policy rules.

NOTE: If you need to rearrange a set of policy rules, select the checkbox to the left of a rule, and then click the Up and Down buttons on the right to move the selected rule to a new position.

The rules in this policy allow clients to access a DHCP and DNS server to get their network settings and resolve DNS queries so that they can access the captive web portal. They deny traffic to all private IP address spaces, thus blocking access to the internal network. Rules 7–9 allow HTTP and HTTPS traffic so that guests can browse the public network and they allow IKE and NAT-T traffic so that they can make VPN connections back to their corporate sites. Finally, Rule 10 logs all outgoing packets that SmartPath APs drop because the firewall blocked them.

To save the firewall policy and close the dialog box, click "Save."

NOTE: You do not have to create a policy to control incoming traffic because you will set the default action to deny all incoming and outgoing traffic not specified in any of the policy rules.

User Profile

A user profile contains the rate control and queuing QoS settings, VLAN, firewall policies, tunnel policy, and schedules that you want the SmartPath AP to apply to traffic from certain users. Because the SSID in this example uses a preshared key for user authentication, you can assign a single user profile to it.* The SmartPath AP then applies the various settings in the user profile to all traffic on this SSID.

*An SSID using a preshared key supports a single user profile. An SSID using 802.1X authentication can support multiple user profiles.

To define a user profile so that SmartPath APs can apply the appropriate QoS settings, VLAN, and firewall policies to all traffic on that SSID, click Configuration > User Profiles > New, enter the following, leave the other settings as they are, and then click Save:

Name: Self-reg-guests(3)

The number 3 is included as part of the user profile name so that you can easily know its attribute number when looking at the user profile name.

Attribute Number: 3

You must enter an attribute number that is unique for the WLAN policy to which the user profile is attached. Although you can define different user profiles with the same attribute number in SmartPath EMS VMA, the attribute number must be unique for each user profile that appears in the same WLAN policy. You can set an attribute number between 1 and 4095. (The default user profile "default-profile", which cannot be deleted, uses attribute 0.)

In this example, you only associate the user profile to an SSID that authenticates users with a preshared key, so the attribute number is not used here. It becomes important if you use a remote RADIUS authentication server for IEEE 802.1X authentication. When replying to a successful user authentication request, the server returns a set of attributes, and SmartPath APs use a combination of three of them to determine which user profile to assign to traffic from an authenticated user:

Tunnel-Type = GRE (10)

Tunnel-Medium-Type = IP (1)

Tunnel-Private-Group-ID = <number>

If a SmartPath AP receives all three attributes and the Tunnel-Private-Group-ID matches the attribute of a user profile, it then applies that user profile to traffic from the authenticated user. Regardless of its ultimate use in an SSID using a preshared key or 802.1X, the attribute number for a user profile is a required setting.

Default VLAN: 1

Description: Visiting guests

Manage users for this profile via User Manager: (clear)†

†Although not a component in this example, User Manager is an excellent option for guest management. Information about setting up and managing users through User Manager is available in the SmartPath EMS VMA on-line Help. You can perform a search for "User Manager," or navigate through the TOC to Home > Administration > User Manager.

Expand Firewalls, and enter the following in the IP Firewall Policy section:

From-Access: guest-IP-policy-from-access

This is the policy that you created in "Firewall Policy."

To-Access: (nothing)

Default Action: Deny

Expand QoS Settings, and enter the following:

Rate Control & Queuing Policy: QoS-Guests

This is the policy that you created in "QoS Rate Limiting." The SmartPath AP applies these rates and scheduling to users that belong to this user profile on an individual basis.

CAC Guaranteed Airtime: 0 (default)

Call Admission Control (CAC) monitors the SmartPath AP resource load and airwaves for congestion, and then determines whether to allow additional VoIP calls using Session Initiation Protocol (SIP) or Vocera services to initiate on that SmartPath AP. If the SmartPath AP and airwaves are already overused, then a new caller is not permitted to start a call. Because this user policy will not be applied to voice traffic, it is unnecessary to set this.

Policing Rate Limit a/b/g mode (0-54000 Kbps): 2000

Policing Rate Limit 11n mode (0-2000000 Kbps): 2000

The maximum traffic policing rate for the entire user profile is the same as that for an individual user. By keeping the two rates the same, a single on-line user is not restricted to a smaller rate than that of the profile to which he or she belongs. (These rates can be the same as or greater than the individual user rates.)

Setting a rate limit of 2000 kbps provides guests with a basic amount of available bandwidth without interfering with the bandwidth usage of other users, such as employees.

Scheduling Weight: 5

The weight defines a preference for forwarding traffic. It does not specify a percentage or an amount. Its value is relative to the weights of QoS schedules in other user profiles in the same WLAN policy.

Because wireless access for guests is mainly a convenience and not a necessity, you assign it a weight that is low in comparison to the weights of other user profiles to give guests the lowest priority. In this example, 5 is used. Because this setting is a relative weight, modify it as necessary based on the weights of the other user profiles present.

NOTE: Although SmartPath APs apply policing at all times, they only apply scheduling weights when usage is at maximum capacity.

SSID

You can provide visitors with secure but unregistered network access by issuing them a preshared key to use when associating with the guest SSID. A receptionist can provide visitors with the preshared key along with access instructions upon their arrival, as shown in Figure 9-16. This approach provides visitors with secured network access by using WPA or WPA2 with preshared keys and TKIP or CCMP (AES) encryption.

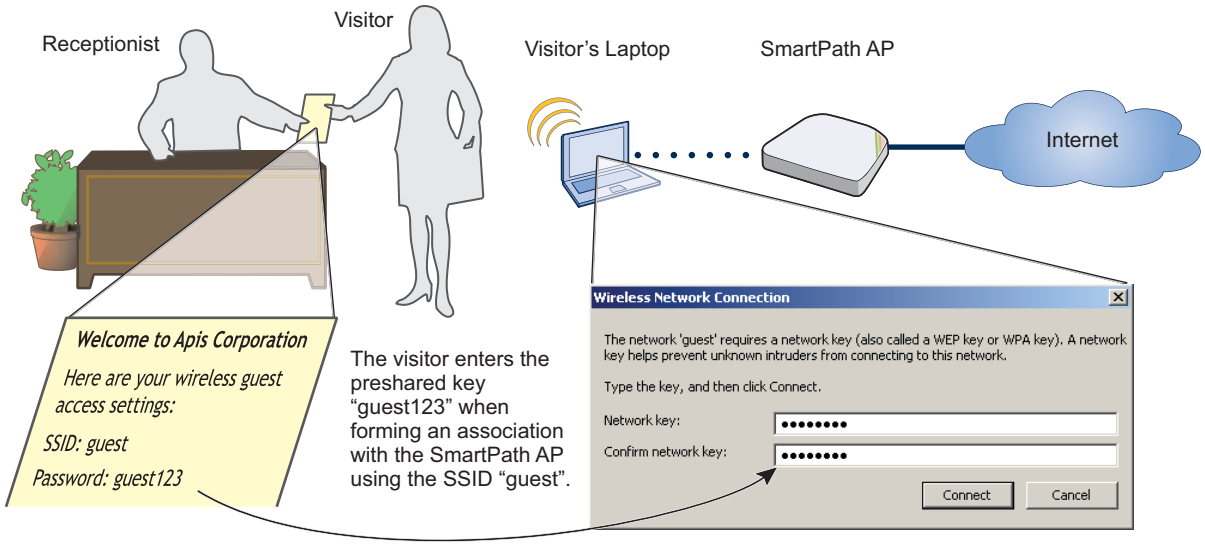


Figure 9-16. Guest access using a preshared key.

The guest SSID provides secure network access for visitors. Also, by linking visitors to the guest SSID, you can differentiate them from employees—who associate with other SSIDs—so that you can apply one group of settings for visitors and another for employees. In addition, by assigning employees and guests to different VLANs, you can separate their traffic.

To create an SSID for guest access, click "Configuration > SSIDs > New," enter the following, leave all other values at their default settings, and then click "Save:"

Profile Name: guest

SSID: guest

Description: SSID for registering company guests

SSID Access Security: WPA/WPA2 PSK (Personal)

Use Default WPA/WPA2 PSK Settings: (select)

Key Value and Confirm Value: guest123

Enable Captive Web Portal: (select); CWP-guest1

Self-Registration Access: User Profile: Self-reg-guests(3)

SSID Broadcast Band: 2.4 GHz (11n/b/g)

WLAN Policy

To add the SSID to an existing WLAN policy, click Configuration > WLAN Policies > wlan_policy, enter the following and then click Save:

In the SSID Profiles section, click Add/Remove SSID Profile, select guest in the Available SSID Profiles list, click the right arrow (>) to move the SSID profile to the Selected SSID Profiles list, and then click Apply.

Files and Configuration Upload

To push the files and configuration to the managed SmartPath APs on which you want to provide guest access, click Monitor > Access Points > SmartPath APs > (select SmartPath APs) > Update > Upload and Activate Configuration, enter the following, and then click Upload:

Upload and activate configuration: (select)

Upload and activate CWP pages and Server key: (select)

Upload and activate certificate for RADIUS and VPN services: (clear)

Upload and activate employee, guests, and contractor credentials: (clear)

List of all SmartPath APs selected on the Monitor > Access Points > SmartPath APs page: (select)

Because the WLAN policy for the selected SmartPath APs contains an SSID using captive Web portal files, upload and activate the files required for the captive Web portal to function and also the configuration. SmartPath EMS VMA uploads the captive web portal files first followed by the configuration.

The SmartPath AP Update Results page appears so that you can monitor the progress of the upload procedure. When complete, "100%" appears in the Upload Rate column and "Successful" appears in the Update Result column.

NOTE: If a managed SmartPath AP already has the maximum number of captive Web portal directories (8), you must remove at least one of them before you can add a new one. To see how many directories are already on a SmartPath AP and remove a directory if necessary, do the following:

1. *Click Monitor > Access Points > SmartPath APs > (select a SmartPath AP) > Update > Remove Captive Web Page Directory > Remove Specific Web Page Directory.*
2. *Select the checkbox of the directory that you want to remove, and then click Submit.*

To test the captive Web portal:

1. Take a wireless client near one of the SmartPath APs, and form an association with the guest SSID, entering guest123 when prompted for the preshared key.
2. After the client has formed an association, open a Web browser.

   The SmartPath AP intercepts the HTTP or HTTPS traffic from your browser to the URL of its home page and redirects it to the login page (registration.html) on the captive Web portal.
3. Complete the registration form, and then click Submit.

   After a successful registration, the "Login Successful" page appears.
4. Close the Web page and open a new browser window.

   The browser successfully opens to its home page, and you can visit other sites on the public network. If there is any Web server on the local network, try to browse to it and you will find that it is not possible. Similarly, if you try to ping the default gateway or a remote website (www.blackbox.com, for example), you will find that you do not receive any responses because the firewall does not permit ICMP traffic to either the internal or external network. On the other hand, if there is a remote IKE peer to which you can build a VPN tunnel, you will find that you will be able to do so.

9.3.5 IP Firewall Policy Support of Domain Names

IP firewall policies now support domain name as the source and destination in their rules.

9.3.6 VMware PCoIP and Citrix UCA

With both PCoIP (PC-over-IP) and CItrix ICA (Independent Computing Architecture) desktop virtualization protocols now predefined as services, you can quickly create firewall rules to allow or block these two services.

9.4 Example 4: Private PSKs

Private PSKs are unique preshared keys created for individual users on the same SSID.3 They offer unique keys per user and user profile flexibility (similar to 802.1X) with the simplicity of preshared keys. For this example, the steps for generating, applying, and distributing private PSK user data are as follows:

1. Define two user profiles.
2. Create two private PSK user groups. Each group includes an attribute that links it to one of the user profiles.
3. Import manually created private PSK users and assign them to one of the two private PSK user groups.
4. Create an SSID that references the private PSK groups and user profiles to which the PSK groups link.
5. Reference the SSID in a WLAN policy.
6. Push the configuration and user database to managed SmartPath APs.
7. E-mail private PSK user data to individuals to use when connecting to the network through the SSID.

NOTE: Before you can e-mail the private PSK user data, you must configure the SMTP server and From Email settings in the Update Email Service Settings section on the Home > Administration > SmartPath EMS VMA Services page.

An overview of the process is shown in Figure 9-17.

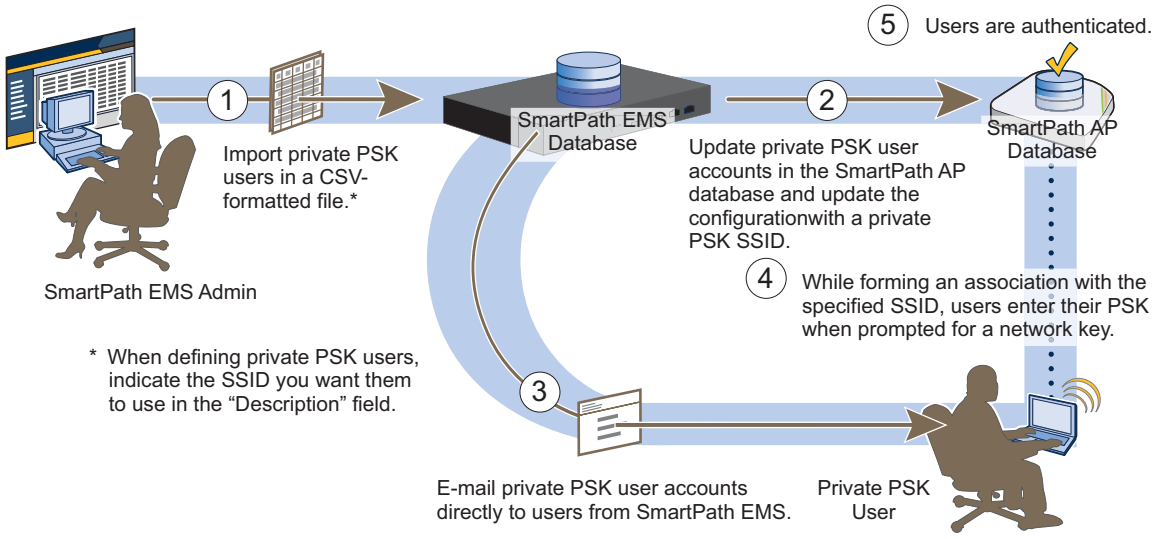


Figure 9-17. Private PSK configuration, application, distribution, and usage.

**NOTE: It is also possible for groups of users to use the same private PSK. For example, you might find it expedient to create a single private PSK user for visitors. You then e-mail the private PSK user data to the lobby ambassador to hand out to all visitors that arrive that week. If you set the validity period so that it recurs on a weekly basis, SmartPath EMS VMA and the SmartPath APs generate a new PSK for that private PSK user each week. With this approach, the SmartPath APs update the PSK automatically at the start of each new week, and you simply e-mail the new data from SmartPath EMS VMA to the lobby ambassador to distribute to that week's visitors. (It is important that the system clocks on SmartPath EMS VMA and the SmartPath APs be synchronized for this to work properly.)*

9.4.1 Private PSK Enhancements

You can set up a captive Web portal that allows users to self-register and receive their own, individual private PSKs (preshared keys). In addition, you can configure a SmartPath AP to generate sets of private PSK users with admin-defined validity periods, which is convenient for users such as contractors that require temporary network access for lengths of time longer than a day.

Private PSK Self-Registration

You can configure an SSID with a captive Web portal so that when users register, they receive their own private PSKs and the name of a second SSID with which to associate by entering their newly acquired PSK. To accomplish this, one or more SmartPath APs act as authenticators and one of them also acts as a private PSK server. Users associate with an authenticator on an open SSID referred to as the "registration SSID." When they open a Web browser and attempt to make an HTTP connection, the authenticator captures the HTTP traffic and redirects it to the captive Web portal on the private PSK server, which presents a registration page to the users. After they register, the private PSK server redirects them back to the captive Web portal on the authenticator with which they are associated. The authenticator then displays a "successful registration" page that contains the private PSK and name of the SSID with which the user must associate next. This procedure completely eliminates the need for an administrator or receptionist to distribute private PSKs to users. The users automatically get PSKs for themselves by registering on a captive Web portal.

NOTE: The configuration steps below assume that the private PSK authenticator and server are on different SmartPath APs to differentiate their roles clearly. However, a single SmartPath AP can act as both a private PSK authenticator and server.

Step 1: Make a Private PSK User Group

Create a user group for automatically generated private PSK users. All users added to this group automatically inherit the attributes that you set for the group.

Click "Configuration > Advanced Configuration > Authentication > Local User Groups > New," enter the following, and then click "Save:"

User Group Name: Type a unique name for the user group. Including the user profile attribute number in the name helps ensure that you later assign user groups and user profiles with the same attribute in the SSID.

Description: Type a useful note for later reference.

Automatically generated private PSK users:

User Profile Attribute: Type the attribute number for the user group. The SmartPath AP uses this to reference a user profile with the same number to members of this group.

VLAN ID: Type the VLAN ID that you want SmartPath APs to assign to traffic from users in this group. If you leave this empty, SmartPath APs assign traffic to the VLAN ID set in the user profile. If you specify a VLAN ID here, it supersedes the one defined in the user profile.

Reauthorization Time: Use the default setting of 1800 seconds (30 minutes) or set a new one from 600 to 86400 seconds (10 minutes to 24 hours). If you enter 0, clients do not have to reauthorize themselves.

User Name Prefix: Type a text string to be added to the beginning of all automatically generated private PSK users.

Private PSK Secret: Type a random string of up to 64 characters to be used as part of the PSK generation process.

Step 2: Add Users to the Group

Create a number of users and add them to the private PSK user group.

Click "Configuration > Advanced Configuration > Authentication > Local Users > Bulk," enter the following, and then click "Create:"

Create Users under Group: From the drop-down list, choose the name of the group configured in Step 1.

Number of New Users: Enter the number of private PSK users that you want to generate.

Description: Type a note about the private PSK. If you send the keys to users through e-mail, this description appears in the e-mail message, so you might want to enter the SSID that users access when connecting to the network.

E-mail Notification: If you were to send e-mail notices from SmartPath EMS VMA to the person or people coordinating distribution of the private PSKs, you would enter their e-mail addresses here, using semicolons to separate multiple e-mail addresses. However, because the goal of this configuration is for users to register themselves and obtain their own private PSKs, leave this field empty.

Step 3: Set a Static IP Address on the SmartPath AP Private PSK Server

The SmartPath AP that you use as the private PSK server must have manually defined network settings; that is, a static IP address, netmask, and default gateway.

Click "Monitor > Access Points > SmartPath APs," select the checkbox for the SmartPath AP that you want to set as the private PSK server, and then click "Modify." Expand the Interface and Network Settings section, enter the following, and then click "Save:"

DHCP Client Enabled: (clear)

IP Address: Enter a suitable IP address for the segment of the network to which the SmartPath AP is connected. This is the IP address of the mgt0 interface on the SmartPath AP.

Netmask: Enter an appropriate netmask for the subnet to which the mgt0 interface connects.

Default Gateway: Enter the IP address of the router through which the SmartPath AP sends traffic beyond its immediate subnet.

Step 4: Create an SSID Profile

Create an SSID profile that contains a private PSK SSID, a captive Web portal through which users can self-register, the private PSK user groups whose users you want to assign to people registering successfully, and the user profiles that you want to apply to their traffic. You also create a registration SSID, which is a companion to the private PSK SSID being configured. Users initially connect to the registration SSID to get their private PSKs. Then they can make a secure connection to the private PSK SSID by entering their keys.

Click "Configuration > Guided Configuration > SSIDs > New," enter the following, leave other settings at their default values, and then click "Save:"

Profile Name: Type the name of the SSID profile. This refers to the configuration object that contains the SSID and all its related settings.

SSID: Use the same name that you entered for the profile name, which automatically appears here after you enter it in the previous field, or type a different name for the SSID. (Note that although the SSID profile name cannot contain spaces, the SSID name can.) This is the SSID to which users connect after they register themselves through the captive Web portal. After a successful registration, they receive a private PSK and this SSID name. They can then form an association with the SmartPath AP on this SSID, authenticate themselves by entering their private PSK, and access the rest of the network.

Private PSK:

Private PSK User Groups: In the Available Private PSK User Groups column, select the user group created in Step 1, and then click the right arrow (>) to move it to the Selected Private PSK User Groups column.

Enable private PSK self-registration:

SmartPath AP Private PSK Server: Choose the IP address of the SmartPath AP that you configured in Step 3.

Captive Web Portal: Click the New icon (+) to open the New Captive Web Portal dialog box, enter the following, and then click "Save:"

Name: Enter a name for the captive Web portal, which you can then choose in the Captive Web Portal drop-down list.

Registration Type: Private PSK Server

Description: Add a note about the captive Web portal for future reference.

Captive Web Portal Login Page Settings

Private PSK Server Registration Type: Self-registration

There are two options: Authentication and Self-registration. When you select Self-registration, users must complete and submit a registration form to obtain their private PSKs. When you select Authentication, they must enter and submit a user name and password, which the SmartPath AP sends to a RADIUS server to validate before providing them with private PSKs. (When you set the registration type as Authentication, then you must also set a RADIUS server in the SSID configuration.)

Optional Advanced Settings

Enable HTTPS: Because the registration SSID uses open authentication, enabling HTTPS provides encryption for the traffic between the client and SmartPath AP.

HTTPS Certificate: Choose "Default-CWPCert" from the drop-down list.

NOTE: You can leave all other settings as they are or modify them to suit your network needs.

After you save the captive Web portal configuration, SmartPath EMS VMA automatically returns to the SSID dialog box. Choose the captive Web portal that you just created from the Captive Web Portal drop-down list.

Registration SSID: Enter a name for the SSID with which users first associate. This SSID uses open authentication, but user traffic is secured through HTTPS.

NOTE: This SSID name does not appear in the SSIDs list. It is only used in association with the SSID being configured.

User profiles assigned after successful private PSK authentication:

Check the attribute number that you included in the name of the private PSK user group when you configured it in Step 1 and remember it. Click the New icon (+) to open a section where you can create a user profile. Type a name that includes the same number as the attribute of the private PSK user group that you created, enter that number again in the Attribute Number field, and enter the VLAN ID that you want the SmartPath AP to assign to traffic from these users. If you want to configure other aspects of the user profile, click "More Settings." When you are finished, click "Apply."

In the Available User Profiles column, select the user profile that you just created, and then click the right arrow (>) to move it to the Selected User Profiles column.

Step 5: Add the SSID Profile to a WLAN Policy

Before pushing the configuration, private PSK users, and captive Web portal files to the SmartPath APs, you must first add the SSID profile to a WLAN policy.

Click "Configuration > Guided Configuration > WLAN Policies," click the name of the WLAN policy that applies to your SmartPath APs, enter the following, and then click "Save:"

Add/Remove SSID Profiles: (click)

Select the SSID that you created in Step 4 in the Available SSID Profiles column, click the right arrow (>) to move it to the Selected SSID Profiles column, and then click "Apply."

Step 6: Push the Configuration to All SmartPath APs

You must push the configuration and captive Web portal files to all the SmartPath APs. They all get the same Web directory with all the login, success, and failure HTML pages, but only the private PSK server shows the login page on its captive Web portal and only the authenticators show the success and failure pages on theirs. SmartPath EMS VMA detects which SmartPath AP is the private PSK server and only sends the private PSK users to it.

Click "Monitor > Access Points > SmartPath APs," select the SmartPath APs to be authenticators and the one to be a private PSK server, click "Update > Upload and Activate Configuration," select all the upload options, and then click "Upload."

The diagram below shows the flow of traffic between client, authenticator, and private PSK server.

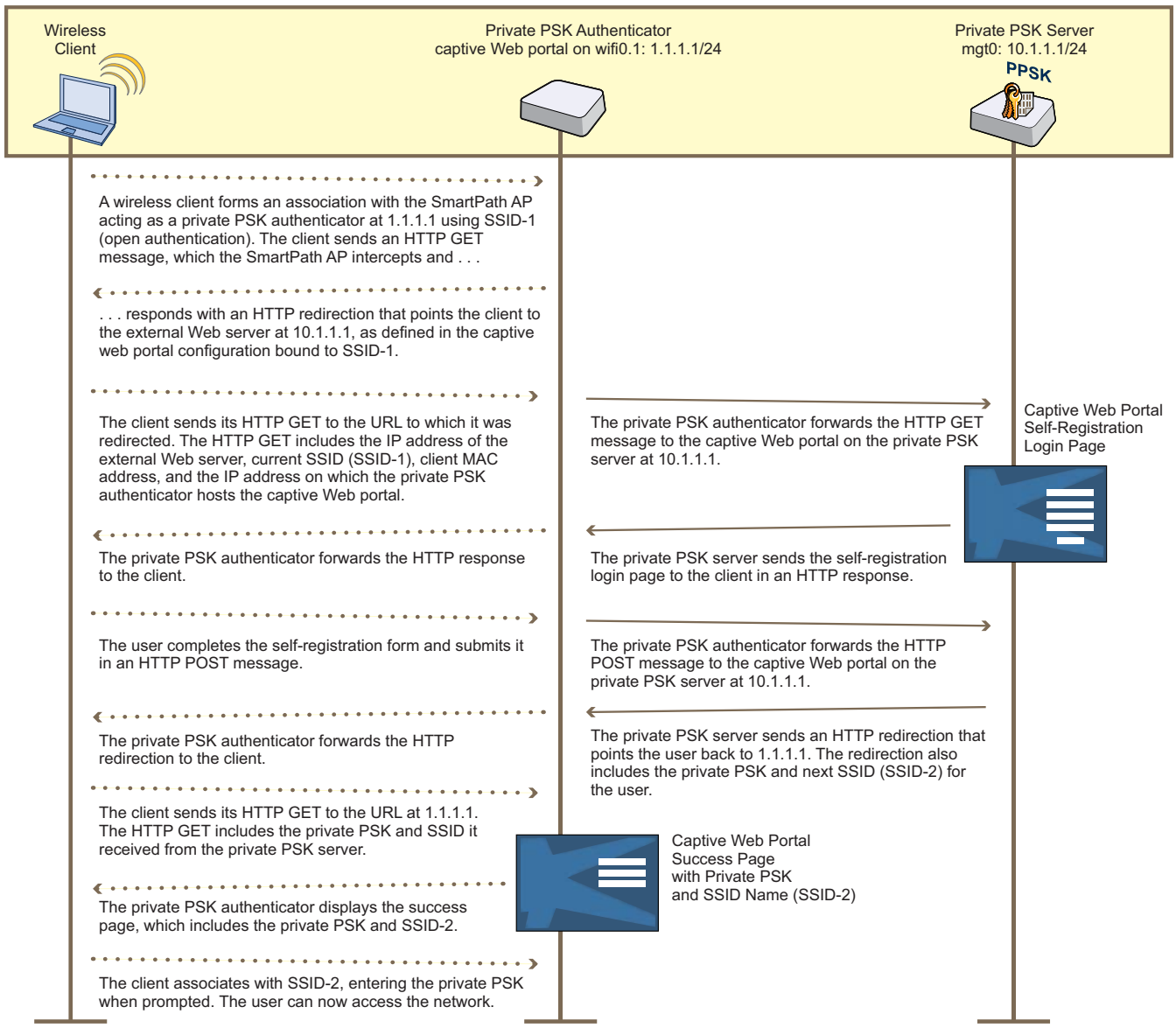


Figure 9-18. Private PSK authenticator.

NOTE: The private PSK that each user receives through the self-registration process is bound to the MAC address of the device in use while registering. For example, a user might get a private PSK while registering with a laptop. If the user later disconnects his laptop and tries to connect using the same private PSK with another device, such as an Apple® iPad® for example, the SmartPath AP would reject the connection attempt because the iPad MAC address would not match the one that the private PSK server previously bound to the user's key.

Recurring Automatic Generation of Private PSKs

For private PSK generation, the recurring option refreshes keys every day. This option satisfies the needs of guest access for daily visitors, but is less suitable for temporary users for longer stays, such as contractors who might need to access the wireless network for several days or several weeks. For such users, it is more convenient to have one key that they can use for longer periods of time rather than having to obtain a new key every day.

NOTE: Because the generation of private PSK users is time sensitive, make sure that the system clocks on both SmartPath EMS VMA and the SmartPath APs are accurate and synchronized.

To configure private PSK users for longer periods, click Configuration > Advanced Configuration > Authentication > Local User Groups > New, enter the following, leave the other settings with their default values, and then click Save:

User Group Name: Enter a name for the user group. Consider indicating how long the private PSK users are valid as part of the name, such as "3-day-keys", "1-week-keys", "2-week-keys". Also, consider including the attribute number in the user group name. By including this information in the user group name, you can make sure an SSID references the correct user group for a corresponding user profile.

Automatically generated private PSK users:

User Profile Attribute: Type the attribute number for the user group. The SmartPath AP uses this to assign a user profile with the same number to members of this group.

VLAN ID: Type the VLAN ID that you want SmartPath APs to assign to traffic from users in this group. If you leave this empty, SmartPath APs assign traffic to the VLAN ID set in the user profile. If you specify a VLAN ID here, it supersedes the one defined in the user profile.

Reauthorization Time: Use the default setting of 1800 seconds (30 minutes) or set a new one from 600 to 86400 seconds (10 minutes to 24 hours).

User Name Prefix: Type a text string to be added to the beginning of to all automatically generated private PSK users. You can also include the private PSK user validity period here, by entering a text string such as "2-day", "1-week", "3-week", and so on. If you include numbers and special characters, be sure to include them in the Character types used in generated PSKs and manually created passwords option in the Private PSK Advanced Options section.

Private PSK Secret: Type a random string of up to 64 characters to be used as part of the PSK generation process.

Expand the Private PSK Advanced Generation Options section, and enter the following:

PSK Validity Period: Recurring

Enable the automatic creation and rotation of private PSK users and their keys: This enables the creation of private PSK users and exposes the following controls to determine how many sets to generate, how many private PSK users to include in each set, and the amount of time between the generation of each new set.

NOTE: The validity period for subsequent private PSK user sets is calculated by adding the bulk interval to the starting and ending times. To see how the PSK validity period settings work with the bulk private PSK feature, refer to the following example.

Private PSK Start Time: Enter a start date and time for the generation of the first set of private PSK users. This is also the starting point when they become valid.

Private PSK Lifetime: Enter the length of time during which private PSK users are valid. You can set their lifetime to be as short as a few hours (set days as 0, and define the lifetime in just hours and minutes) or as long as a full year (set days as 365).

Private PSK Rotation Interval: Set the amount of time between the generation of each set of private PSK users. Enter the number of days (0-365), hours, and minutes. For example, if you want to generate a new set of private PSK users every day, set the number of days as 1.

Private PSK Rotations: Set the number of times to generate a set of private PSK users. Enter a number from 1 to 500. The default is 1, which means that SmartPath EMS VMA only generates one set of users.

Private PSK Users to Create per Rotation: Set the number of private PSK users to generate in each set. You can generate from 1 to 9999 users in each set. The default is 10, which means that each set will contain 10 private PSK users. (1–9999)

Example: To create a user group that generates 10 private PSK users at 8:00 A.M. every day for a year starting on 06/14/2011 and make each user valid for two days, enter the following:

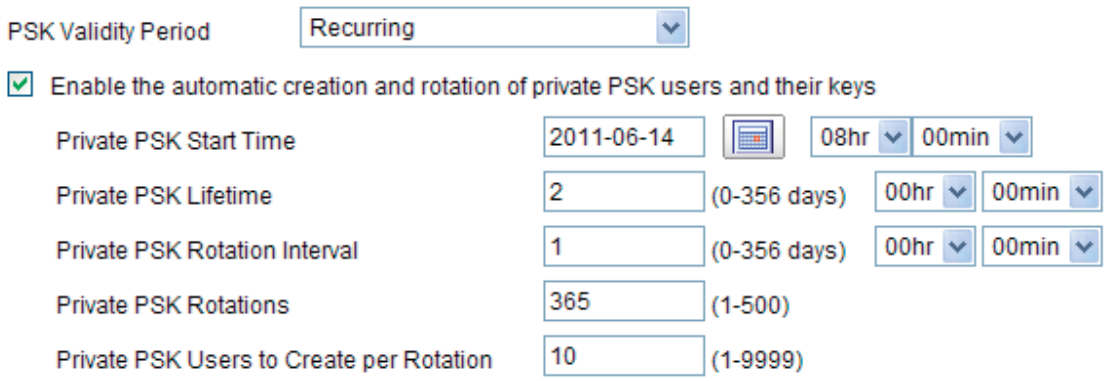


Figure 9-19. PSK validity period.

SmartPath EMS VMA generates a set of 20 private PSK users, consisting of two subsets:

- The first subset of 10 users is valid from 8:00 AM 2011-06-14 to 7:59 AM 2011-06-16.
- The second subset of 10 users is valid from 8:00 AM 2011-06-15 to 7:59 AM 2011-06-17.

The SmartPath AP calculates the validity periods for subsequent private PSK user sets by adding the private PSK interval to the private PSK start time. In this example, the generation of 10 more users occurs two days later after the first 10 users expire. Because the first 10 users are no longer valid, the new users are assigned the same key prefixes that the first 10 users had. Similarly, when the second set of 10 users expires, the next set of users gets their prefixes. After that, new sets of 10 users are generated every day for the rest of the year.

Automatically Binding a Private PSK to a Client MAC Address

When configuring a private PSK SSID, you have the option to bind a private PSK to the MAC address of the first client that uses it. This provides tighter control over which devices can use the private PSK to access the network. For example, there might be a policy permitting network connections for corporate-owned devices only, and you want to ensure that employees do not reuse their private PSKs to go on-line with other devices that they own privately. Enabling the binding of the private PSK to a single MAC address blocks access to all devices other than that of the first client that uses it. If an employee makes a network connection with a corporate device first, he cannot make another connection with a different device later. On the other hand, if he goes on-line with a privately owned device first, he will be unable to connect the company-issued device later, which will expose the policy breach when he has to report his inability to make a network connection.

To create an SSID with the automatic private PSK-to-client MAC address binding enabled, do the following:

Click "Configuration > SSIDs, New, type a name for the SSID profile," choose the broadcast band, enter the following, and then click "Save:"

Private PSK: (select)

Private PSK User Groups: Select an entry in the Available Private PSK User Groups column, and then click the right arrow (>) to move it to the Selected Private PSK User Groups column.

Automatically bind a private PSK to a MAC address:

SmartPath AP Private PSK Server: Choose the SmartPath AP that you want to use as the private PSK server from the drop-down list. This is the SmartPath AP that will store all the private PSK users and act as a server that the other SmartPath APs will contact when checking and requesting a binding of a user-submitted private PSK to the MAC address of the user's client.

User profiles assigned after successful private PSK authentication: In the Available User Profiles column, select an entry whose attribute number matches the attribute number of the selected private PSK user group, and then click the right arrow (>) to move it to the Selected User Profiles column.

9.4.2 User Profiles

Unlike a traditional PSK SSID, a private PSK SSID can support multiple user profiles. For this example, you create two user profiles, one for employees with full network access and another for contractors with limited access.

To define a user profile for employees, click Configuration > User Profiles > New, enter the following, leave the other settings as they are, and then click Save:

Name: Employees(30)

The number 30 is included as part of the user profile name so that you can easily know its attribute.

Attribute Number: 30

The SmartPath AP uses this attribute number to link the user profile to a user group with the same attribute. You can use any number between 1 and 4095.

Default VLAN: 1

Description: Corporate employees

To define a user profile for contractors with a firewall policy that allows basic network protocols to the public network while blocking access to the internal network, click Configuration > User Profiles > New, enter the following, leave the other settings as they are, and then click Save:

Name: Contractors(35)

Attribute Number: 35

Default VLAN: 1

Description: short-term contractors

Expand Firewalls, and enter the following in the IP Firewall Policy section:

From-Access: Click the New icon to open the IP Firewall Policy dialog box, and then enter the following:

Policy Name: contractors-outgoing-IP-policy

Description: Apply to contractor user profiles

Policy Rules:

To add rules permitting only DHCP, DNS, HTTP, and HTTPS to the public network while denying any type of traffic to the internal network, enter the following (use CTRL-click or SHIFT-click to select multiple services):

Table 9-3. CTRL-click or SHIFT-click to select multiple services.

(Click…)	Source	Destination*	Service	Action	Logging*	(Click)
	[-any]	[-any-]	DHCP-Server, DNS	Permit	Off	Apply
New	[-any-]	10.0.0.0/8	[-any-]	Deny	Dropped Packets	Apply
New	[-any-]	172.16.0.0/12	[-any-]	Deny	Dropped Packets	Click “Apply.”
New	[-any-]	192.168.0.0/16	[-any-]	Deny	Dropped Packets	Click “Apply.”
New	[-any-]	[-any-]	HTTP, HTTPS	Permit	Both	Apply

* The three addresses "10.0.0.0/8", "172.16.0.0/12", and "192.168.0.0/16" that define private network address space were created in a previous example. See “Address Objects” in Figure 9-15.

Click “Save” to save the IP firewall policy and return to the User Profile dialog box.

From-Access: contractors-outgoing-IP-policy (This is the firewall policy that you just created.)

To-Access: (nothing)

Default Action: DenyUser Profile Reassignment

9.4.3 User Profile Reassignment

SmartPath APs can reassign users to different user profiles based on the MAC addresses or OUIs, operating systems, and device domain names of their clients. This allows a SmartPath AP to assign different user profiles to a user going on the network with the same credentials but using different devices. For example, you might apply one set of firewall and QoS policies to employees using authorized company-issued equipment and a different set when they go on-line with unauthorized mobile devices.

To configure SmartPath APs to reassign user profiles based on client characteristics:

Step 1: Create MAC Objects

Click Configuration > Advanced Configuration > Network Objects > MAC Objects > New, enter the following, and then click Save:

MAC Address or MAC Address Range or MAC OUI: Select the one you want to use to distinguish a type of client device.

If you want to create a user profile reassignment policy rule for a single device, select MAC address.

or

If you want to make a policy rule that applies to devices with a range of MAC addresses (such as a shipment of company-purchased laptops), enter the MAC Address Range.

or

If you want to set a policy rule for all clients with the same OUI—and, therefore, the same device type—select MAC OUI.

NOTE: You can see a list of OUIs on the Home > Administration > Auxiliary Files > MAC OUI Dictionary page. You can also download the entire file for reference.

MAC Object Name: Type the name of the MAC object. This is the name that appears in the MAC Object drop-down list when you configure a client classification policy in the User Profile dialog box.

Based on whether you selected MAC Address, MAC Address Range, or MAC OUI, enter a 12-hexadecimal MAC address, the start and end MAC addresses of an address range, or a 6-hexadecimal MAC OUI, optionally include a description, and then click “Apply.”

To add another MAC entry, click “New,” and then make another MAC entry, include an optional description, and then click “Apply.” You can add up to 255 entries to a single MAC object, and there can be up to 128 MAC objects per SmartPath AP.

Step 2: Create OS Objects

There are several predefined OS objects for common operating systems and versions of those systems:

- Windows NT 5.1 (Windows XP), NT 5.2 (Windows 2003), NT 6.0 (Windows Vista and Windows 2008), and NT 6.1 (Windows 7)

- Mac® OS X
- iPad
- iPhone®
- Android™

If one or more of these predefined OS objects satisfies your needs, you can skip this step.

Click Configuration > Advanced Configuration > Network Objects > OS Objects > New, enter the following, and then click Save:

Object Name: Type the name of the OS object. This is the name that appears in the OS Object drop-down list when you configure a client classification policy in the User Profile dialog box.

To define the OS object, enter the following, and then click "Apply:"

OS Version: Choose one of the entries in the drop-down list, or click in the empty space at the top of the list and type the name of an OS version. Because SmartPath APs use HTTP snooping to learn clients' operating systems, the OS version string that you enter must match the version that appears in the user-agent field in HTTP request headers. Lists of user-agent strings for most OS versions are available on-line.

Description: (optional) Type a useful description for the OS version.

To add another OS version, click "New," either choose an existing OS version entry or create a new one, add an optional description, and then click "Apply." You can add up to 32 OS versions to a single OS object, and there can be up to 64 OS objects per SmartPath AP.

Step 3: Create Device Domain Objects

SmartPath APs can learn device domain names during 802.1X/EAP user authentication when clients first go on the wireless network. SmartPath APs learn the domain for users' devices from the domain name that users enter when logging in with their user name + domain name and password. SmartPath APs can discern the domain name when any of the following formats are used:

```
domain\user _ name

user _ name@domain

host/user _ name.domain
```

Based on the ability of SmartPath APs to detect a specific domain name or the presence of any domain name, SmartPath APs can classify client types and assign user profiles based on the result of that classification.

Click Configuration > Advanced Configuration > Network Objects > Device Domain Objects > New, enter the following, and then click "Save:"

Object Name: Type the name of the device domain object. This is the name that appears in the Domain Name Object drop-down list when you configure a client classification policy in the User Profile dialog box.

There are two predefined entries in the Domain Name drop-down list: Known and Unknown. When applied in a user profile reassignment policy rule, they have the following meanings:

Known: When a rule specifies Known as the device domain, SmartPath APs apply the rule if they detect a domain name during the 802.1X/EAP login process. The exact domain name is irrelevant.

Unknown: When a rule specifies Unknown as the device domain, SmartPath APs apply the rule if they do not detect any domain name, perhaps because a user authentication method other than 802.1X/EAP is used that does not require users to submit a domain name when logging in.

Choose one of the predefined entries in the drop-down list, or click the empty space at the top of the list and type the name of a specific device domain, and then click "Apply."

To add another domain name, click New, click the empty space at the top of the drop-down list and type a new domain name, add an optional description, and then click "Apply." You can create up to 32 entries for a single device domain object, and there can be up to 64 device domain objects per SmartPath AP.

Step 4: Set User Profile Reassignment Policy Rules

With the MAC, OS, and device domain objects defined, you can now create a policy to classify client types and assign user profiles based on how the clients are classified.

Click Configuration > Guided Configuration > User Profiles > user_profile, expand the Client Classification Policy section, enter the following to add a client classification policy, and then click "Save:"

Enable user profile reassignment based on client classification rules: (select)

Choose an entry from the MAC Object, OS Object, and Device Domain Object drop-down lists. If you do not see one that you need, click the New icon (+), and create it. Then choose the user profile from the Reassigned User Profile drop-down list that you want to apply to traffic from clients that match all three device classification objects.

NOTE: SmartPath APs apply policy rules to change user profile assignments based on three client characteristics: MAC address, OS version, and device domain membership. A rule that sets one of these classification types as "[-any-]" ignores that particular characteristic and bases user profile reassignments on the other two.

To add another rule, click "New," add the three client classification objects and the user profile reassignment, and then click "Apply."

The order of the rules within a policy is important. SmartPath APs look for a match to the individual rules starting from the top, and as soon as they find a match, that is the rule that is applied. To reorder the rules within a policy, select the checkbox to the left of the ID of the rule that you want to move, and then click the Up or Down buttons located on the right of the rules until you are satisfied with the order of the rules in the policy.

Step 5: Enable User Profile Reassignment in SSIDs

You can enable and disable user profile reassignments at the SSID level.

To enable it, click Configuration > Guided Configuration > SSIDs > ssid_name, select the Enable user profile reassignment based on client classification rules checkbox, and then click "Save." To disable it, clear the checkbox.

NOTE: The SSID must contain a user profile that is configured with a client classification policy.

To apply your settings, push the WLAN profile referencing the modified SSIDs and user profiles to the SmartPath APs.

9.4.4 Private PSK User Groups

You next create two private PSK user groups, one for employees and another for contractors.

To create a private PSK user group for employees, click Configuration > Advanced Configuration > Authentication > Local User Groups > New, enter the following, and then click Save:

User Group Name: Employees(30)

Including the attribute number in the private PSK user group name and in the user profile name makes it easier to match them when configuring the SSID.

Description: Corp employees

User Type: Manually created private PSK users

User Profile Attribute: 30

This must be the same number as the user profile "Employees(30)".

VLAN ID: 1

If you leave this field empty, the SmartPath AP applies the VLAN ID set in the Employees(30) user profile, which is already set as 1. If you set a different VLAN ID here than the one in the user profile, this setting takes precedence over the one in user profile.

Reauthorization Time: 1800 (default)

This setting is only used when private PSK user accounts are stored on a RADIUS server and a reauthorization interval is not set on the server for those users. If user accounts are stored on a RADIUS server that returns a reauthorization interval attribute, the SmartPath APs use that value instead of this one. If user accounts are stored locally on SmartPath APs, the SmartPath APs ignore this setting.

To create a private PSK user group for contractors, click Configuration > Advanced Configuration > Authentication > Local User Groups > New, enter the following, and then click Save:

User Group Name: Contractors(35)

Description: Contractors at corp

User Type: Manually created private PSK users

User Profile Attribute: 35

VLAN ID: 1

Reauthorization Time: 1800 (default)

NOTE: If you want to define advanced options, click + to expand the Private PSK Advanced Options section. You can modify the characteristics of keys that SmartPath EMS VMA generates, such as their length, the types of characters used in them, the method of their generation, and the period of time during which they are valid. This example uses the default settings, one of which is the requirement that the password in the imported .csv file must contain letters, digits, and special characters. This requirement has significance in Section 9.4.4.

9.4.5 Importing Private PSK Users

Create a list of private PSK users in a .csv file, assign them to the two private PSK user groups Employees(30) and Contractors(35), and import the file to SmartPath EMS VMA.

1. Define a set of private PSK users in a CSV-formatted file, and save it to your management system. The left-to-right order of columns in file must be as follows:

   User Name, User Type (3), User Group Name, Password, Email, Description, Virtual SmartPath EMS VMA Name

   The value 3 indicates that the user type is a manually defined private PSK user. When using the default settings, the password must contain letters, digits, and special characters.* Multiple e-mail addresses (up to 128 characters total) must be separated by semicolons without spaces before or after the semicolons. The text in the Description column is included in the e-mail sent to users, so you use it to identify the SSID. The last column is only required if there is at least one virtual SmartPath EMS VMA system and you are logged in to "All VSPMs" as an admin with superuser privileges. Otherwise, omit it.

* If you do not include a password string in the imported file, SmartPath EMS VMA automatically generates a random string during the import process. For example, if the first entry omits the password, it would be as follows (note the empty space between the commas): Bob Lai, 3, Employees(30), , hm-admin@apis.com;blai@apis.com, Use SSID star, home

The following is a sample of a few private PSK user definitions:

#User Name, User Type 3, User Group Name, Password, Email, Description, VHM

Bob Lai, 3, Employees(30), hon;VP#243, hm-admin@apis.com;blai@apis.com, Use SSID star, home

Jenny Lo, 3, Employees(30), loN#953d:)n, hm-admin@apis.com;jlo@apis.com, Use SSID star, home

Phil Wei, 3, Contractors(35), meX18ca1#!, hm-admin@apis.com;mgr@apis.com, Use SSID star, home

Bill Li, 3, Contractors(35), Cm$7)3bO1!, hm-admin@apis.com;mgr@apis.com, Use SSID star, home

Notice that the private PSK user definitions for employees are sent directly to the people who will use them, but those for contractors are sent to a department manager for dissemination. All definitions are also sent to the SmartPath EMS VMA administrator as a backup.

2. Click Configuration > Advanced Configuration > Authentication > Local Users > Import > Browse, navigate to the file containing the private PSK user definitions, select it, and then click Import.

9.4.6 Private PSK SSID

To configure an SSID for the private PSK users that you have created, click Configuration > SSIDs > New, enter the following, and then click Save:

Profile Name: star

SSID: star

The profile name is the name that you reference in the WLAN policy and contains the SSID and related configuration objects, such as user profiles and user groups. The SSID is the name that SmartPath APs broadcast. Although they can be different so that you can create different profiles for the same SSID for use at different locations, the two names are the same in this example.

Description: Use for both employees and contractors

SSID Access Security: Private PSK

Use Default Private PSK Settings: (select)

Private PSK User Groups: Select Employees(30) and Contractors(35) in the Available Private PSK User Groups list and then click the right arrow (>) to move them to the Selected Private PSK groups list.

User Profiles for Traffic Management: Select Employees(30) and Contractors(35) in the Available User Profiles list and then click the right arrow to move them to the Selected User Profiles list.

SSID Broadcast Band: 2.4 GHz (11n/b/g)

This is the broadcast band for the radio operating in access mode.

9.4.7 WLAN Policy

To add the SSID to a WLAN policy, click Configuration > WLAN Policies > wlan_policy_name > Add/Remove SSID Profile, select star in the Available SSID Profiles list, click the right arrow (>) to move it to the Selected SSID Profiles list, click Apply, and then click Save.

To push the private PSK user groups, users, and WLAN policy configuration to the SmartPath APs on which you want to provide guest access, click Monitor > Access Points > SmartPath APs > (select SmartPath APs) > Update > Upload and Activate Configuration, enter the following, and then click Upload:

Upload and activate configuration: (select)

Upload and activate CWP pages and Server key: (clear)

Upload and activate certificate for RADIUS and VPN services: (clear)

Upload and activate employee, guests, and contractor credentials: (select)

List of all SmartPath APs selected on the Monitor > Access Points > SmartPath APs page: (select)

Because the WLAN policy for the selected SmartPath APs contains an SSID using captive web portal files, upload and activate the files required for the captive Web portal to function and also the configuration. SmartPath EMS VMA uploads the captive Web portal files first followed by the configuration.

The SmartPath AP Update Results page appears so that you can monitor the progress of the upload procedure. When complete, "100%" appears in the Upload Rate column and "Successful" appears in the Update Result column.

9.4.8 E-mail Notification

To distribute the private PSK user definitions to the employees and the manager in charge of the contractors, click Configuration > Advanced Configuration > Authentication > Local Users, select the users, and then click Email PSK. The specified recipients receive a separate e-mail message for each private PSK user, with content like the following:

PSK: hon;VP#243

Description: Use SSID star

User Name: Bob Lai

Start Time:

End Time:

If you define a lifetime for a private PSK user (configurable in the Private PSK Advanced Options section in the Local User Group dialog box), start and end times are also listed here. This can be useful if you want to provide users—such as the contractors in this example perhaps—with WLAN connectivity for a fixed period of time.

Instead of sending the private PSK users through e-mail, you can also export them in a .csv file. To do that, select the users that you want to export, click the Export PSK button, and then save it to a directory of your choice. You can open the file using a spreadsheet program such as Microsoft Excel®.

9.5 Example 5: Using SmartPath AP Classifiers

In SmartPath EMS VMA, some network objects can support multiple definitions as long as each definition is uniquely classified by a map name, SmartPath AP name, or classifier tag—and one of the definitions is classified as global. The definition classified as global is what SmartPath EMS VMA applies when none of the other more specific classification types are applicable. When you then assign a WLAN policy that includes that one network object to various SmartPath APs, SmartPath EMS VMA applies the appropriate definition based on the location, name, or tag of each SmartPath AP. The network objects that support multiple definitions are IP addresses/host names, MAC addresses/OUIs, and VLANs.

In this example, there are four sites: a main office and three branch offices. You assign the same WLAN policy to the SmartPath APs at all branch offices. However, the network at each office uses a different VLAN for its wireless clients:

- Branch office 1: VLAN 10
- Branch office 2: VLAN 20
- Branch office 3: VLAN 30

To continue using a single WLAN policy for all branch offices while supporting their different VLANs, you use SmartPath AP classifiers. You do not classify SmartPath APs at Branch Office 1. As a result, they will use the VLAN definition classified as global. You classify the SmartPath APs at Branch Offices 2 and 3 as "branch2" and "branch3". You also classify two VLAN definitions as "branch2" and "branch3" so that SmartPath EMS VMA will apply them to the SmartPath APs with the same classifiers. The classification scheme is show in Figure 9-20.

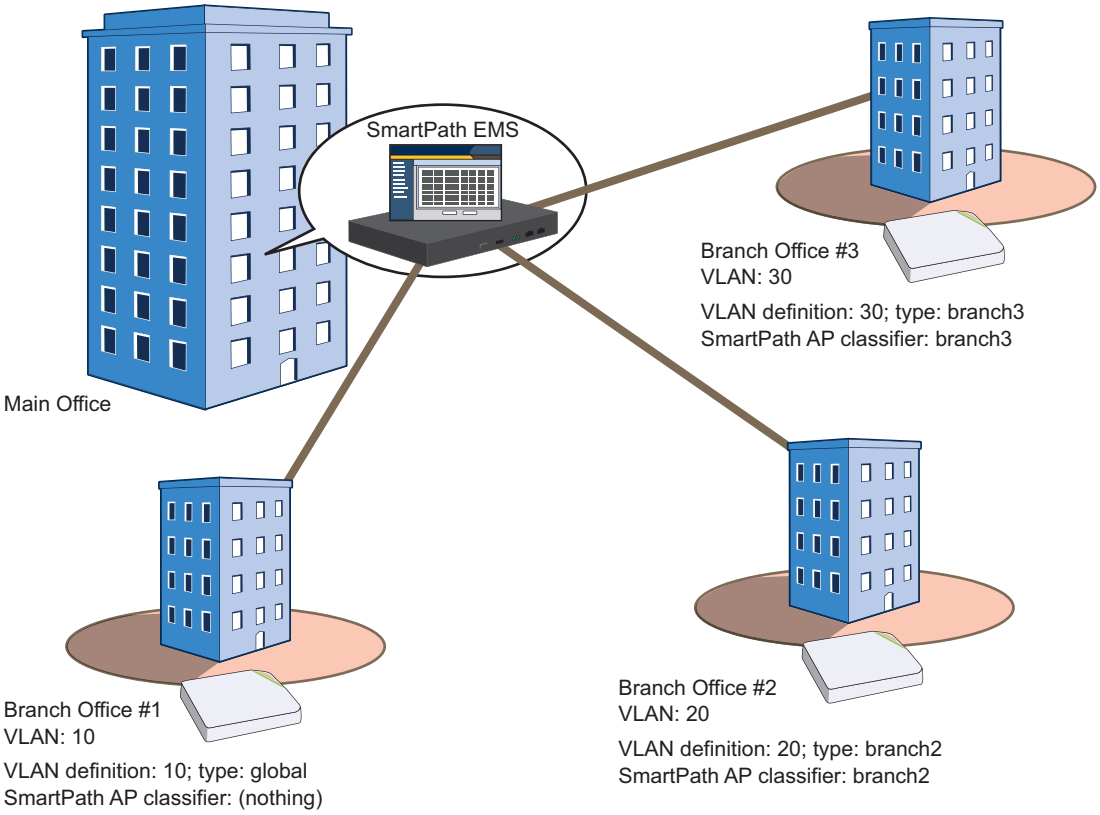


Figure 9-20. SmartPath AP classifiers and VLANs.

NOTE: It is assumed that the SmartPath APs have already been assigned to maps in the Topology section of the GUI.

The configuration steps are as follows:

1. Classify SmartPath APs at Branch Offices 2 and 3.
2. Create a VLAN object with three definitions for VLANs 10, 20, and 30.
3. Reference the VLAN object in a user profile that is used in an SSID that is part of the WLAN policy used by the SmartPath APs at each branch office.
4. Update all the SmartPath APs and note how the user profile at each site has the correct VLAN definition.

9.5.1 Set SmartPath AP Classifiers

Click Monitor > Access Points > SmartPath APs (view mode: Config), and then click the column heading Topology Map to group the managed SmartPath APs by the map to which they are assigned.

Multiselect the SmartPath APs belonging to all the maps at Branch Office 2,* click Modify, expand Advanced Settings, enter branch2 in the Tag1 field, and then click Save.

*To multiselect all the SmartPath APs on the same map, click the first SmartPath AP assigned to a map and then SHIFT-click the last one. This example assumes that you have used a naming convention that allows you to select SmartPath APs on multiple maps at the same site because all the maps at that site begin with the same word, such as "branch2-floor1", "branch2-floor2", and so on.

Multiselect the SmartPath APs belonging to all the maps at branch office 3, click Modify, expand Advanced Settings, enter branch3 in the Tag1 field, and then click Save.

9.5.2 Create a VLAN Object with Three Definitions

Click Configuration > Advanced Configuration > Network Objects > VLANs > New, enter the following, and then click Apply:

VLAN Name: branchVLAN-10-20-30

VLAN ID: 10

Type: Global

Description: VLAN at Branch Office #1

Click New, enter the following, and then click Apply:

VLAN ID: 20

Type: Classifier

Value: branch2

Description: VLAN at Branch Office #2

Click New, enter the following, and then click Apply:

VLAN ID: 30

Type: Classifier

Value: branch3

Description: VLAN at Branch Office #3

To save your settings and close the dialog box, click Save.

9.5.3 Reference the VLAN Object

To assign the VLAN object to a user profile that is used in an SSID that is part of the WLAN policy assigned to the SmartPath APs at all the branch offices:

Click Configuration > User Profiles > user_profile_name, choose branchVLAN-10-20-30 from the Default VLAN drop-down list, and then click Save.

The relationships among the objects from the SmartPath APs down to each VLAN definition are as follows:

SmartPath AP > WLAN policy > SSID > user profile > VLAN object > VLAN definition

— VLAN 10; Type: global

branch2 VLAN 20; Type: classifier = branch2

branch3 VLAN 30; Type: classifier = branch3

9.5.4 Update SmartPath APs

To apply the VLAN definitions to the SmartPath APs at all the branch offices, click Monitor > Access Points > SmartPath APs, multiselect the SmartPath APs at all branch offices, click Update > Upload and Activate Configuration, and then enter the following:

Upload and activate configuration: (select)

Upload and activate CWP pages and Server key: (clear)

Upload and activate certificate for RADIUS and VPN services: (clear)

Upload and activate employee, guests, and contractor credentials: (clear)

List of all SmartPath APs selected on the Monitor > Access Points > SmartPath APs page: (select)

The SmartPath AP Update Results page appears so that you can monitor the progress of the upload procedure. When complete, "100%" appears in the Upload Rate column and "Successful" appears in the Update Result column.

Check that the VLANs are being applied properly:

In the Upload and Activate Configuration dialog box, click the host name of a SmartPath AP at Branch Office 1, and then select View Configuration. Notice the VLAN ID that appears in the View Configuration-clusterap_name window that pops up:

```
user-profile name vlan-id 10
```

Close the Configuration Details window, and then click the host name of a SmartPath AP at Branch Office 2. The VLAN ID for the same user profile is 20:

```
user-profile name vlan-id 20
```

If you click the host name for a SmartPath AP at Branch Office 3, you can see that its VLAN ID is 30:

```
user-profile name vlan-id 30
```

Make sure that all the SmartPath APs in the list at the bottom of Upload and Activate Configuration page are selected, and then click Upload.

VMware PCoIP and CItrix ICA

With both PCoIP (PC-over-IP) and Citrix ICA (Independent Computing Architecture) desktop virtualization protocols now predefined as services, you can quickly create firewall rules to allow or block these two services.

9.6 Example 6: Multiple Default Routes

Multiple Default Routes: You can configure multiple Layer 2 routes based on the VLAN ID of a user so that the SmartPath AP can route Layer 2 traffic through different Ethernet interfaces as appropriate. This allows, for example, a guest user on a corporate network segment to access a more appropriate segment for routing to the Internet while the SmartPath AP forwards traffic from an employee on a different VLAN through a different Ethernet interface.

Multiple Default Routes

SmartPath APs with two Ethernet ports can now support multiple default routes based on the VLAN of the traffic. With this feature configured, you can easily tunnel guest traffic from a SmartPath AP on a private network to a SmartPath AP in the DMZ. The SmartPath AP in the DMZ terminates the tunnel and forwards it out eth1—properly tagged with the correct VLAN—to the public network. For corporate traffic, the SmartPath AP applies a different VLAN tag and forwards it out eth0 to the corporate network. To do this, the SmartPath AP that bridges the two subnets must meet the following requirements:

- The SmartPath AP must have two Ethernet ports.
- The SmartPath AP must have the eth1 port in backhaul mode.
- The Ethernet ports must not be set as an aggregate or redundant pair.

If your guest (public) network is on a separate subnet from your corporate (private) network, guests who connect through SmartPath APs on your corporate subnet can be easily redirected to the public network using a SmartPath AP as an intermediary to bridge the two disparate subnets. This intermediary SmartPath AP connects to your corporate subnet using its eth0 interface, and to your public subnet using its eth1 interface. You configure eth0 to use the corporate VLAN by default, and eth1 to use the public VLAN by default.

When a guest connects to a SmartPath AP on the corporate network, the SmartPath AP applies a guest user policy to the traffic, which assigns it to the public VLAN (20). The SmartPath AP tags the frame with the public VLAN, encapsulates it with a GRE wrapper, and forwards it to the eth0 port of the SmartPath AP in the DMZ. That SmartPath AP terminates the GRE tunnel, revealing the public VLAN ID and routes the frame out the eth1 port to the public network with the public VLAN tag (see Figure 9-21).

NOTE: You do not need to set a default Layer 2 route for VLAN 20 on the SmartPath AP in the trusted network. The user profile applied to guest traffic directs the SmartPath AP to forward all that traffic through an INXP tunnel, which uses eth0 as its egress interface and the SmartPath AP in the DMZ as its destination. On the other hand, the user profile for corporate users assigns their traffic to VLAN 1. The SmartPath AP forwards it out eth0, which is the egress interface in its default Layer 2 route.

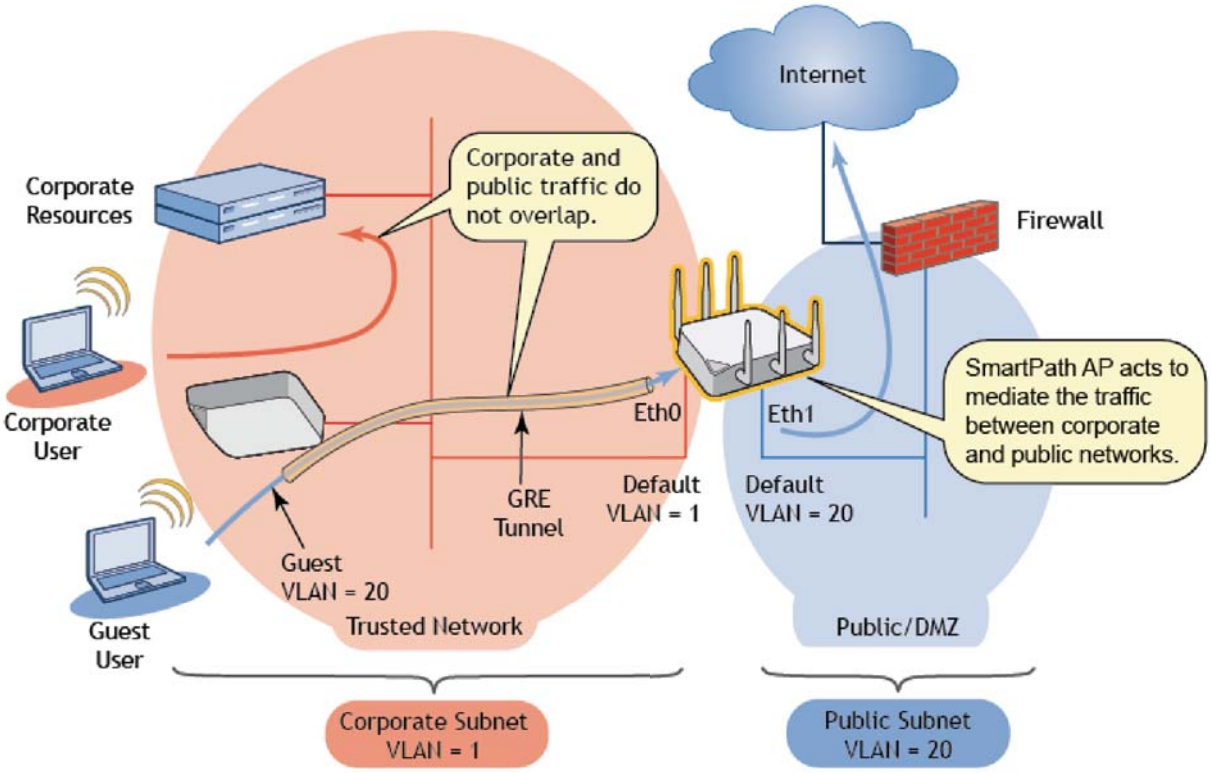


Figure 9-21. Multiple default routes.

There are two places that require configuration to forward traffic in this way. Steps 1–3 configure the Ethernet interfaces to accept tagged frames; Steps 4–6 configure the SmartPath AP to forward the internal traffic between interfaces.

Furthermore, the following process assumes that you have already configured the SSIDs, user policies, and WLAN policies on your WLAN, and that you have configured your network infrastructure to handle 802.1Q or similar VLAN tagging where necessary. For more information on configuring the WLAN and other policies, see the SmartPath EMS VMA Help system. To configure multiple default routes based on VLAN ID, enter the following on SmartPath EMS VMA:

1. Click Monitor > Access Points > SmartPath APs, select the SmartPath APs that you want to configure to mediate traffic between the trusted network and the public network/DMZ, and then click "Modify."
2. In the SmartPath AP settings dialog box that appears, expand the Interface and Network Settings section, and then choose Backhaul from the Eth1 Operation Mode drop-down list.

3. Expand the Advanced Ethernet Settings section, enter the default VLAN ID for your public network in the Eth1 row in the Native VLAN column, and then enter the VLAN IDs you want to allow on the public network in the Allowed VLAN column.

NOTE: You do not have to enter a value in the Allowed VLAN column if the only VLAN ID allowed is entered in the Native VLAN column. This is because entering a value in the Native VLAN column implicitly allows that VLAN ID on that interface. If you have additional VLAN IDs you want to add, you can enter a single VLAN ID (for example, 20), a range of VLAN IDs (for example, 11–30), a non-contiguous list of VLAN IDs separated by commas (for example, 15,20,25), or a combination of these formats (for example, 11–15,20,25-30). Be careful to avoid permitting access to the VLAN of your corporate network on an interface permitting access to the VLAN of your public network as this might expose your corporate data to guests and other non-corporate users.

4. Expand the Routing section, and then in the Multiple Network Default Routing subsection, click "New."

5. Enter the VLAN ID whose default route you want the SmartPath AP to forward out the eth1 interface, and then click "Apply." By default, the egress interface for default Layer 2 routes is eth0. However, the VLAN IDs you enter here use eth1 as the egress interface in their default routes.

6. If you want to forward multiple VLAN IDs, you can add more VLAN IDs, but you can only enter one VLAN ID per line.

10. SmartPath Operating System (OS)

You can deploy a single SmartPath AP and it will provide wireless access as an autonomous AP. However, if you deploy two or more SmartPath APs in a cluster, you can provide superior wireless access with many benefits. A cluster is a set of SmartPath APs that exchanges information with each other to form a collaborative whole (see Figure 10-1). Through coordinated actions based on shared information, cluster members can provide the following services that autonomous APs cannot:

- Consistent QoS policy enforcement across all cluster members
- Coordinated and predictive wireless access control that provides fast roaming to clients moving from one cluster member to another
- Best-path routing for optimized data forwarding
- Automatic radio frequency and power selection

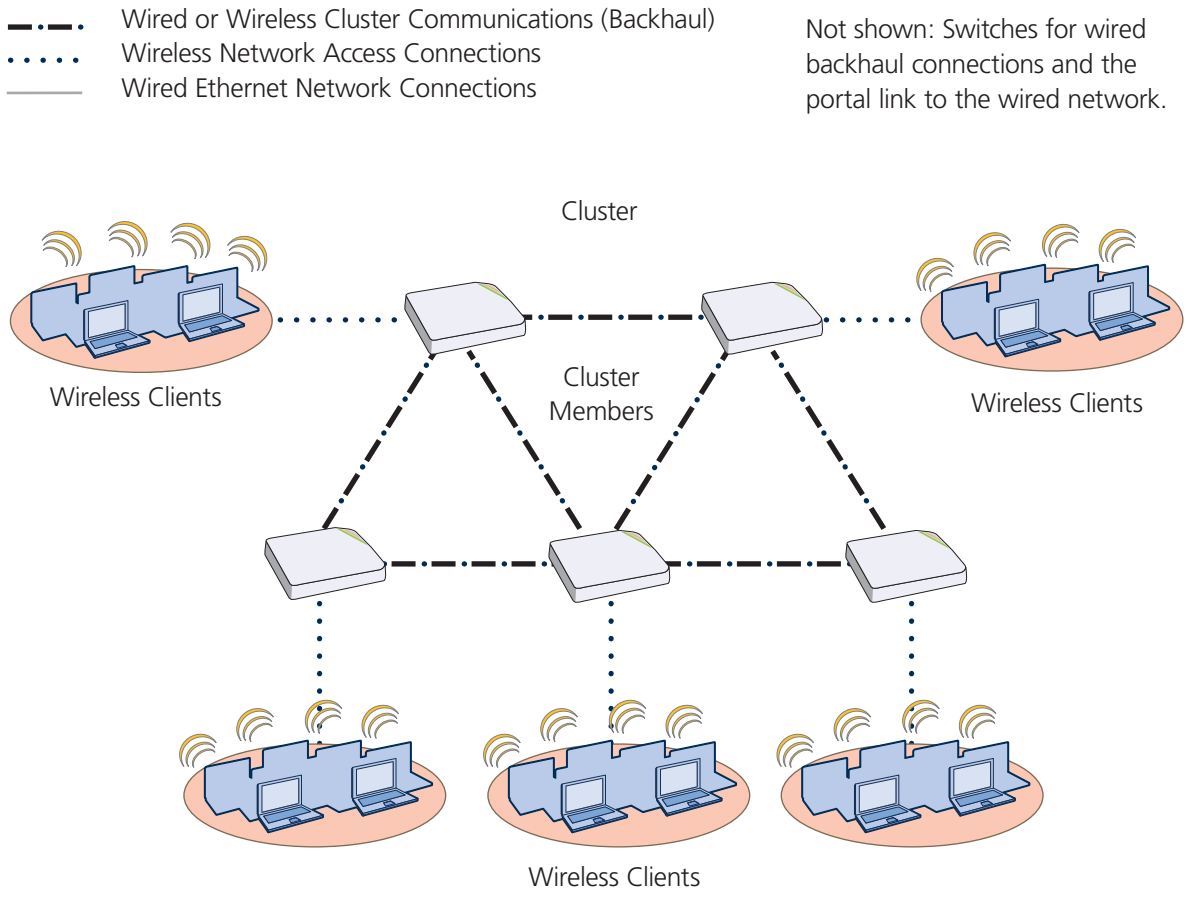


Figure 10-1. SmartPath APs in a cluster.

SmartPathOS is the operating system that runs on SmartPath APs.

10.1 Common Default Settings and Commands

Many major components of SmartPathOS are automated and typically require no further configuration. For example, radio power and frequency selection occurs automatically, as does route learning. Also, after defining a cluster and a password that cluster members use to secure communications, all SmartPath APs belonging to that cluster automatically initiate and maintain communications with each other.

Additionally, there are many default settings that simplify the setup of a SmartPath AP because these are the typical settings for many of the most common deployments. The following are some important default settings and the commands necessary to change them if you need to do so.

Table 10-1. Common default settings and commands.

	Default Settings	Commands
mgt0 interface	DHCP client = enabled	To disable the DHCP client: `no interface mgt0 dhcp client` To set an IP address: `interface mgt0 ip` *`ip_addr netmask`*
	VLAN ID = 1	To set the native (untagged) VLAN that the switch infrastructure in the surrounding wired and wireless backhaul network uses: `interface mgt0 native-vlan` *`number`*
	VLAN ID = 1	To set the VLAN for administrative access to the SmartPath AP, management traffic between SmartPath APs and SmartPath EMS VMA, and control traffic among cluster members: `interface mgt0 vlan` *`number`*
wifi0 and wifi1 interfaces	wifi0 mode = access wifi1 mode = backhaul	To change the mode of the wifi0 or wifi1 interface: `interface { wifi0 | wifi1 } mode { access | backhaul }`
	wifi0 radio profile = radio_g0 wifi1 radio profile = radio_a0	To change the radio profile of the wifi0 or wifi1 interface to a different, previously defined profile: `interface { wifi0 | wifi1 } radio profile` *`string`*

	antenna = internal	To have the wifi0 interface use an external antenna:
		`interface { wifi0 | wifi1 } radio antenna`
		`external`

	channel = automatic selection	To set a specific radio channel: `interface { wifi0 | wifi1 } radio channel` *`number`*
	power = automatic selection	To set a specific transmission power level (in dBms): `interface { wifi0 | wifi1 } radi0 power` *`number`*
User profile	default-profile: group ID = 0 policy name = def-user-qos VLAN ID = 1	You cannot change the group ID or QoS policy name for the default user profile. To change its VLAN ID: `user-profile default-profile vlan-id` *`number`*

10.2 Configuration Overview

The amount of configuration depends on the complexity of your deployment. As you can see in "Deployment Examples (CLI)" in Chapter 11, you can enter a minimum of three commands to deploy a single SmartPath AP, and just a few more to deploy a cluster.

However, for cases when you need to fine tune access control for more complex environments, SmartPathOS offers a rich set of CLI commands. The configuration of SmartPath APs falls into two main areas: Device-Level Configurations (Section 10.2.1) and Policy-Level Configurations (Section 10.2.2). Consider your deployment plans and then refer to the following sections for guidance on the commands you need to configure them.

NOTE: To find all commands using a particular character or string of characters, you can do a search using the following command: `show cmds | { include | exclude } string`

10.2.1 Device-Level Configurations

Device-level configurations refer to the management of a SmartPath AP and its connectivity to wireless clients, the wired network, and other cluster members. The following list contains some key areas of device-level configurations and relevant commands.

• Management

• Administrators, admin authentication method, login parameters, and admin privileges

`admin { auth | manager-ip | min-password-length | read-only | read-write |`

`root-admin } ...`

• Logging settings

`log { buffered | console | debug | facility | flash | server | trap } ...`

• Connectivity settings

- Interfaces

`interface { eth0 | wifi0 | wifi1 } ...`

• Layer 2 and Layer 3 forwarding routes

`route mac_addr ...`

`ip route { default | host | net } ip_addr ...`

• VLAN assignments

For users:

`user-profile string qos-policy string vlan-id number attribute number`

For the mgt0 interface (the native VLAN in the surrounding network, and the VLAN for administrative access, management traffic, and control traffic among cluster members):

`interface mgt0 native-vlan number`

`interface mgt0 vlan number`

• Radio settings

`radio profile string ...`

10.2.2 Policy-Level Configurations

Policies control how wireless clients access the network. The following list contains some key areas of policy-level configurations and relevant commands.

• QoS settings

```
qos { classifier-map | classifier-profile | marker-map | marker-profile | policy } …
```

- User profiles

```
user-profile string …
```

- SSIDs

```
ssid string …
```

- AAA (authentication, authorization, and accounting) settings for IEEE 802.1X authentication

```
aaa radius-server …
```

Although the configuration of most SmartPathOS features involves one or more related commands, to define and apply a QoS policy to a group of users, you must configure several different but related features: a QoS policy, a user profile, and—if you do not authenticate users with a RADIUS server—an SSID that references the user profile, and an interface to which you assign the SSID. The configuration steps are shown in Figure 10-2.

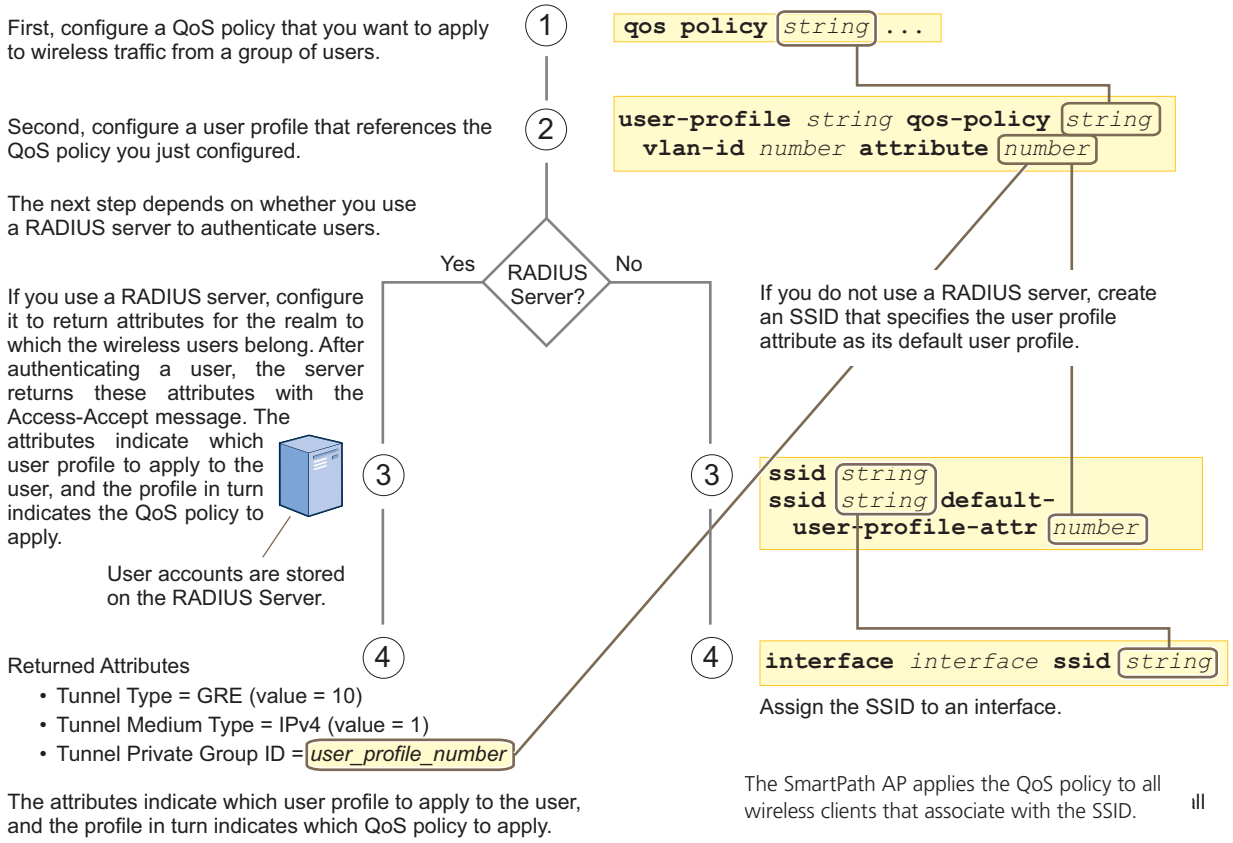


Figure 10-2. Steps for configuring and applying QoS.

10.3 SmartPathOS Configuration File Types

SmartPathOS supports several types of configuration files: running, current, backup, bootstrap, default, and failed.

The running configuration (config) is the configuration that is actively running in DRAM. During the bootup process, a SmartPath AP loads the running config from one of up to four config files stored in flash memory:

- current: a flash file containing a combination of default and admin-defined settings. During the bootup process, this is the first config that the SmartPath AP attempts to load as the running config. This is also the file to which you typically save commands from the running config (you can also save them to the bootstrap config). See Figure 10-3.

- backup: a flash file that the SmartPath AP attempts to load during the reboot process if there is a newly uploaded current config file or if it cannot load the current config file. See Figures 10-4 and 10-5.
- bootstrap: a flash file containing a second config composed of a combination of default and admin-defined settings. The SmartPath AP fails over to this config when you enter the reset config command or if both the current and backup config files fail to load. See Figure 10-6.
- default: a flash file containing only default settings. If there is no bootstrap config, the SmartPath AP reverts to this config when you enter the reset config command or if both the current and backup config files fail to load. See Figure 10-6.

NOTE: There is also a failed config file, which holds any backup config that fails to load. See Figure 10-5.

When using the CLI, the two most frequently accessed config types are the running config and current config. When you enter a command in the running config, the SmartPath AP performs it immediately. However, because the running config is stored in volatile memory (DRAM), the commands are not yet permanent and will be lost when the SmartPath AP next reboots. For your configuration settings to persist after rebooting, enter the save config command. This command saves the running config to the current config, which is a file stored in nonvolatile (flash) memory. See Figure 10-3.

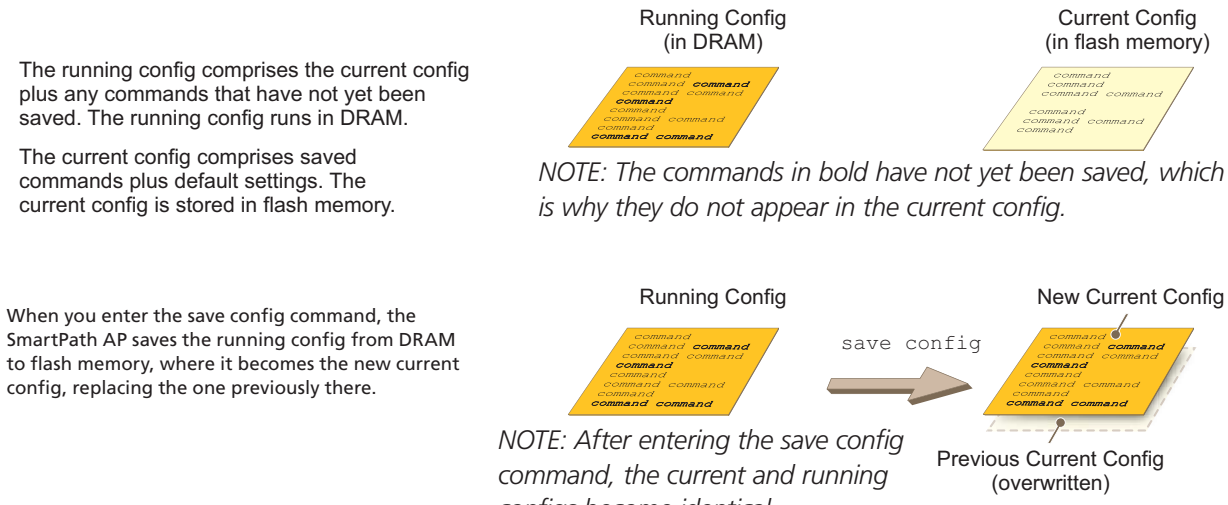


Figure 10-3. Relationship between running and current config files.

When you upload a configuration file from SmartPath EMS VMA or from a TFTP or SCP server, the SmartPath AP stores the uploaded file in the backup config partition in flash memory, where it remains until the SmartPath AP reboots. If there is a backup config file already stored in flash, the newly uploaded file overwrites it. See Figure 10-4.

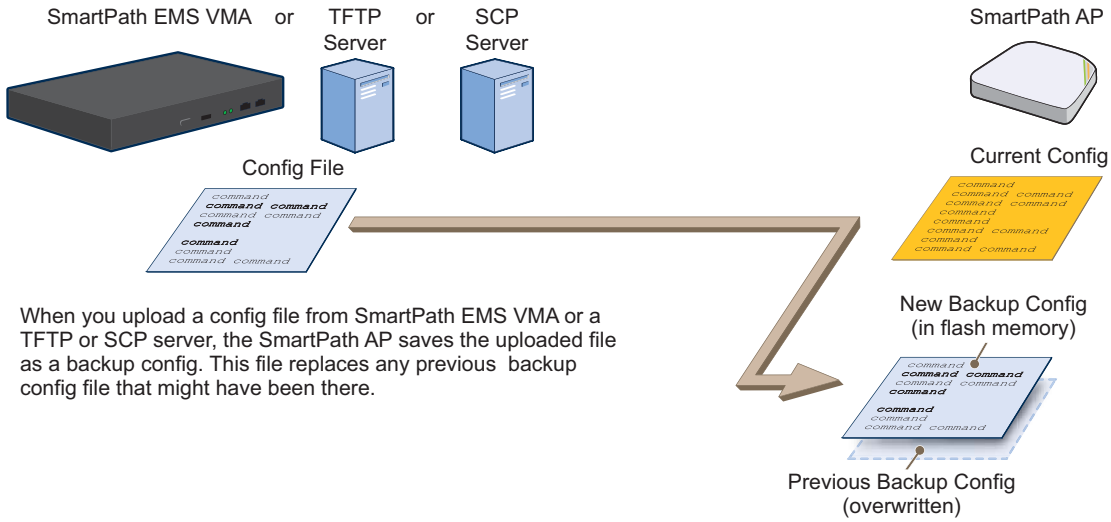


Figure 10-4. Relationship between current and backup config files during a file upload.

When the SmartPath AP reboots, it attempts to load the the newly uploaded config file. If the file loads successfully, the SmartPath AP makes that file the new current config and makes the previous current config the new backup config. If the file does not load successfully, the SmartPath AP reboots again and loads the previous current config file. The SmartPath AP saves the file it was unable to load as a failed config for diagnostics. See Figure 10-5.

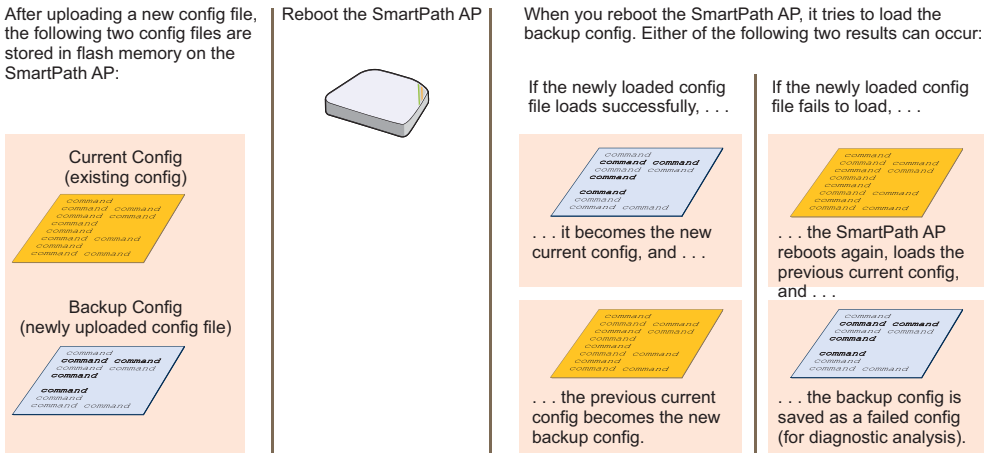


Figure 10-5. Relationship between current and backup config files while rebooting a SmartPath AP.

NOTE: To upload and activate a config file from SmartPath EMS VMA , see "Uploading SmartPath AP Configurations." To upload and activate a config file from a TFTP or SCP server using the CLI, use the following commands:

```
save config tftp://ip _ addr:filename current { hh:mm:ss | now | offset hh:mm:ss }
save config scp://username@ip _ addr:filename current { hh:mm:ss |now |offset hh:mm:ss }
```

When a SmartPath AP ships from the factory, it is loaded with a default config file, which acts initially as the running and current configs. If you enter and save any commands, the SmartPath AP then stores a separate config file as the current config, combining the default settings with the commands you entered and saved. If you want to return to the default settings, you can press the reset button or enter the reset config command. A SmartPath AP might also return to the default config if both the current and backup configs fail to load, which might happen if you update the SmartPathOS firmware to an image that cannot work with either config.

NOTE: You can disable the ability of the reset button to reset the configuration by entering this command:

```
no reset-button reset-config-enable
```

Reverting to the default config can be very useful, especially in the early stages when you are still learning about SmartPathOS and are likely to be experimenting with different settings. However, retaining the ability of a SmartPath AP to revert to its default settings after its deployment can present a problem if it is a mesh point in a cluster. If the SmartPath AP reverts to the default config, it will not be able to rejoin its cluster. Consequently, it will not be able to get an IP address through DHCP nor be able to communicate with SmartPath EMS VMA (assuming that you are managing it through SmartPath EMS VMA). In this case, you would have to make a serial connection to the console port on the SmartPath AP and reconfigure its cluster settings through the CLI.

To avoid the above situation, you can use a bootstrap config. A bootstrap config is typically a small config file that comes last in the boot order (current – backup – bootstrap) and that replaces the default config as the one a SmartPath AP loads when you reset the configuration. See Figure 10-6.

NOTE: Be careful to remember the login name and password defined in the bootstrap config file. If they become lost or forgotten, you must obtain a one-time login key from Black Box technical support. To get the key, you must already have had a support contract in place

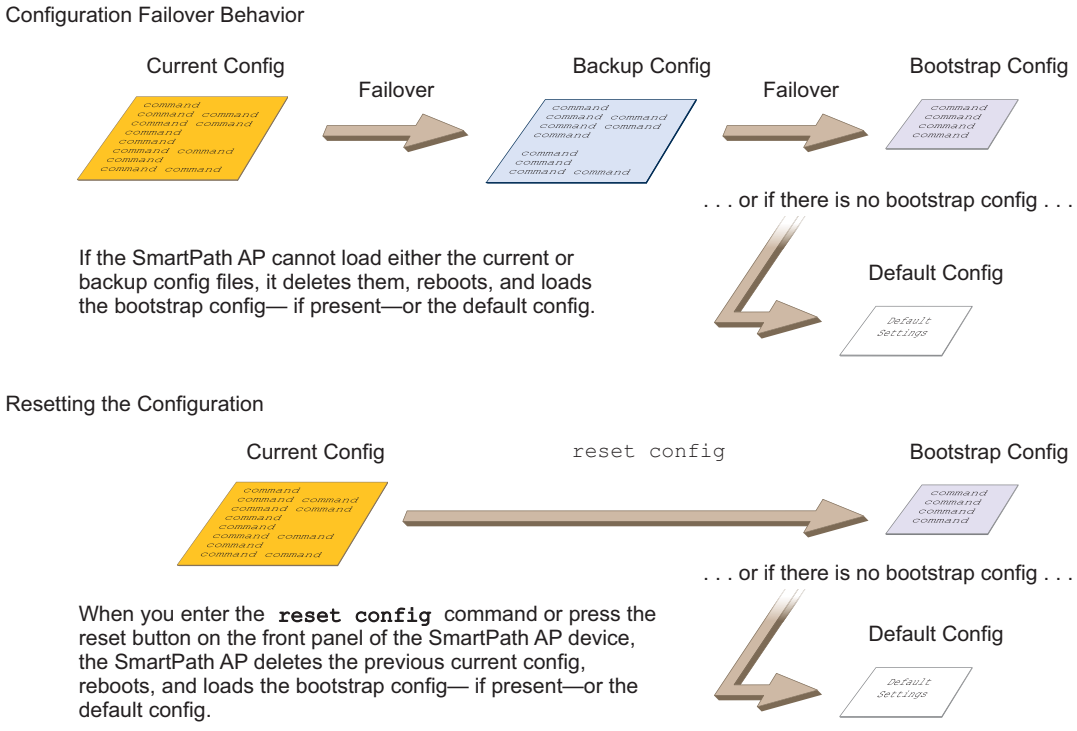


Figure 10-6. Relationship of current, backup, bootstrap, and default config files.

To create and load a bootstrap config, make a text file containing a set of commands that you want the SmartPath AP to load as its bootstrap configuration (for an example, see Section 11.5). Save the file locally and then load it with one of the following commands:

`save config tftp://ip _ addr:filename bootstrap`

`save config scp://username@ip _ addr:filename bootstrap`

NOTE: Similar to the way that a current config consists of the commands you added on top of the default config, a bootstrap config consists of default definitions and settings plus whatever other settings you configure.

After it is loaded, you can enter the following command to view the bootstrap file: `show config bootstrap`

If you want to run the bootstrap config, enter the following commands:

`load config bootstrap`

`reboot`

When the bootstrap config loads, enter the login parameters you defined for that configuration. To return to your previous current config file, enter the following commands:

`load config backup`

`reboot`

11. Deployment Examples CLI

This chapter presents several deployment examples to introduce the primary tasks involved in configuring SmartPath APs through the SmartPathOS CLI.

In Deploying a Single SmartPath AP in Section 11.1, you deploy one SmartPath AP as an autonomous access point. This is the simplest configuration: You only need to enter and save three commands.

In Deploying a Cluster in Section 11.2, you add two more SmartPath APs to the one deployed in the first example to form a cluster with three members. The user authentication method in this and the previous example is very simple: A preshared key is defined and stored locally on each SmartPath AP and on each wireless client.

In Using IEEE 802.1X Authentication in Section 11.3, you change the user authentication method. Taking advantage of existing Microsoft Active Directory (AD) user accounts, the SmartPath APs use IEEE 802.1X Extensible Authentication Protocol (EAP) to forward authentication requests to a RADIUS server whose database is linked to that of the AD server.

In Applying QoS in Section 11.4, you apply QoS (Quality of Service) filters to user traffic so that delay-sensitive voice traffic receives higher priority than other more delay-resistant traffic.

NOTE: To focus attention on the key concepts of an SSID (first example), cluster (second example), and IEEE 802.1X authentication (third example), QoS was intentionally omitted from these examples. However, the QoS settings you define in the last example can apply equally well to the configurations in the others.

In Loading a Bootstrap Configuration in Section 11.5, you load a bootstrap config file on the SmartPath APs. When a bootstrap config is present, it loads instead of the default config whenever SmartPathOS is reset or if the current and backup configs do not load. This example shows how using a bootstrap config can help minimize theft and increase convenience.

Because each example builds on the previous one, it is recommended to read them sequentially. Doing so will help build an understanding of the fundamentals involved in configuring SmartPath APs.

If you want to view just the CLI commands used in the examples, see "CLI Commands for Examples" in Section 11.6. Having the commands in blocks by themselves makes it easy to copy-and-paste them at the command prompt.

The following are the equipment and network requirements for these examples:

• Equipment

- Management system (computer) capable of creating a serial connection to the SmartPath AP

- VT100 emulator on the management system

- Serial cable (also called a “null-modem cable”) that ships as an optional accessory (AH-ACC-Serial-DB9). You use this to connect your management system to the SmartPath AP.

NOTE: You can also access the CLI by using Telnet or Secure Shell (SSH). After connecting a SmartPath AP to the network, make either a Telnet or SSH connection to the IP address that the DHCP server assigns the mgt0 interface. (Telnet is disabled by default.)

• Network

- Layer 2 switch through which you connect the SmartPath AP to the wired network

- Ethernet cable—either straight-through or cross-over

- Network access to a DHCP server

- For the third and fourth examples, network access to an AD server and RADIUS server

11.1 Example 1: Deploying a Single SmartPath AP

In this example, you deploy one SmartPath AP (SmartPath AP-1) to provide network access to a small office with 15–20 wireless clients. You only need to define the following SSID parameters on the SmartPath AP and clients:

- SSID name: employee
- Security protocol suite: WPA-auto-psk

- WPA—Uses Wi-Fi Protected Access, which provides dynamic key encryption and mutual authentication of the client and SmartPath AP
- Auto—Automatically negotiates WPA or WPA2 and the encryption protocol: Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP)
- PSK—Derives encryption keys from a preshared key that the client and SmartPath AP both already have

- Preshared key: N38bu7Adr0n3

After defining SSID "employee" on SmartPath AP-1, you then bind it to the wifi0 interface, which is in access mode by default. The wifi0 interface links to radio 1, which operates at 2.4 GHz (in accordance with the IEEE 802.11b, g, and n standards). This example assumes that the clients also support 802.11b, g, or n.

NOTE: By default, the wifi1 interface is in backhaul mode and links to the 5-GHz radio, supporting IEEE 802.11a and 802.11n. To put wifi1 in access mode so that both interfaces provide access—wifi0 at 2.4 GHz and wifi1 at 5 GHz—enter this command: interface wifi1 mode access. Then, in addition to binding SSID "employee" to wifi0 (as explained in Step 2), also bind it to wifi1.

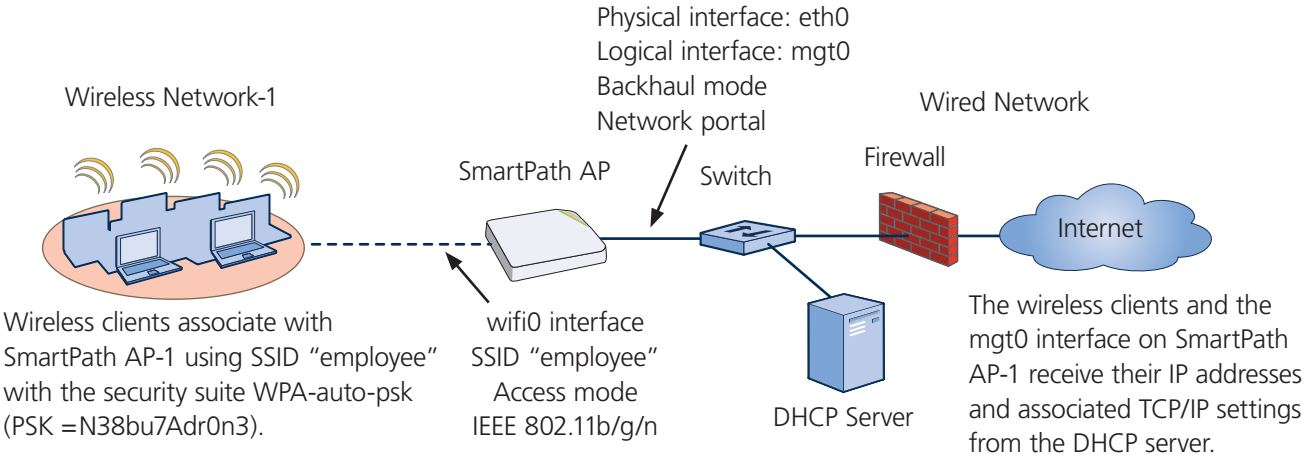


Figure 11-1. Single SmartPath AP for a small wireless network.

Step 1: Log in through the console port.

1. Connect the power cable from the DC power connector on the SmartPath AP to the AC/DC power adapter that ships with the device as an option, and connect that to a 100–240-volt power source.

NOTE: If the switch supports PoE, the SmartPath AP can receive its power that way instead.

The Power LED glows steady amber during the bootup process. After the bootup process completes, it then glows steady green to indicate that the firmware is loaded and running.

2. Connect one end of an RS-232 serial (or “null modem”) cable to the serial port (or Com port) on your management system.
3. Connect the other end of the cable to the male DB9 or RJ-45 console port on the SmartPath AP.

4. On your management system, run a VT100 terminal emulation program, such as Tera Term Pro (a free terminal emulator) or Hilgraeve Hyperterminal (provided with Windows operating systems). Use the following settings:
    - Bits per second (baud rate): 9600
    - Data bits: 8
    - Parity: none
    - Stop bits: 1
    - Flow control: none

    For SmartPath APs set with "FCC" as the region code, the Initial CLI Configuration Wizard appears. For SmartPath APs set with "world" as the region code, a prompt appears to set the country code for the location where you intend to deploy the SmartPath AP. To set the country code, enter the boot-param country-code number command, in which number is the appropriate country code number. For a list of country codes, see Appendix: Country Codes.
5. Because you do not need to configure all the settings presented in the wizard, press N to cancel it.

    The login prompt appears.
6. Log in using the default user name admin and password blackbox.

Step 2: Configure the SmartPath AP.

1. Create an SSID and assign it to an interface.

```
ssid employee
ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
```

    You first create an SSID named "employee" and then define its protocol suite and preshared key (N38bu7Adr0n3) in standard ASCII (American Standard Code for Information Interchange) text.

```
interface wifi0 ssid employee
```

    You assign the SSID to the wifi0 interface, which is in access mode by default. When you make this assignment, the SmartPath AP automatically creates subinterface wifi0.1 and uses that for the SSID. The SmartPath AP (LWN602HA) supports up to eight per interface for a possible maximum total of 16. A SmartPath AP can use one or two Wi-Fi interfaces in access mode to communicate with wireless clients accessing the network, and a Wi-Fi interface in backhaul mode to communicate wirelessly with other SmartPath APs when in a cluster (see subsequent examples).
2. (Optional) Change the name and password of the root admin.

```
admin root-admin mwebster password 3fF8ha
```

    As a safety precaution, you change the default root admin name and password to mwebster and 3fF8ha. The next time you log in, use these instead of the default definitions.
3. (Optional) Change the host name of the SmartPath AP.

```
hostname SmartPath AP-1
```

4. Save your changes to the currently running configuration, and then log out of the serial session.

```
save config
exit
```

The SmartPath AP configuration is complete.

NOTE: By default, the minimum password length is 5 characters. You can change the minimum length by entering the following command: admin min-password-length <number> (The minimum password length can be between 5 and 32 characters.)

Step 3: Configure the wireless clients.

Define the "employee" SSID on all the wireless clients. Specify WPA-PSK for network authentication, AES or TKIP for data encryption, and the preshared key N38bu7Adr0n3.

Step 4: Position and power on the SmartPath AP.

1. Place the SmartPath AP within range of the wireless clients and, optionally, mount it as explained in the mounting section in the chapter about the SmartPath AP model that you are using.
2. Connect an Ethernet cable from the PoE In port to the network switch.
3. If you have powered off the SmartPath AP, power it back on by reconnecting it to a power source.

   When you power on the SmartPath AP, the mgt0 interface, which connects to the wired network through the eth0 port, automatically receives its IP address through DHCP.

Step 5: Check that clients can form associations and access the network.

1. To check that a client can associate with the SmartPath AP and access the network, open a wireless client application and connect to the "employee" SSID. Then contact a network resource, such as a web server.
2. Log in to the SmartPath AP CLI, and check that you can see the MAC address of the associated client and an indication that the correct SSID is in use by entering the following command:

```
show ssid employee station
```

```
show ssid employee station

Chan=channel number; Pow=Power in dbm;

A-Mode=Authentication mode; Cipher=Encryption mode;

A-Time=Associated time; Auth=Authenticated;

UPID=User profile Identifier; Phymode=Physical mode;

Mac Addr       IP Addr    Chan  Rate  Pow  A-Mode    Cipher   A-Time    VLAN  Auth  UPID  Phymode
-------------- ---------  ----  ----  ---  --------  -------  --------  ----  ----  ----  -------
0016:cf8c:57bc 10.1.1.35 11    54M   -38  wpa2-psk  aes ccm  00:00:56  1     Yes   0     11g
```

Check that the MAC address in the table matches that of the wireless client .

Check that the authentication and encryption modes match those in the SSID security protocol suite.

Figure 11-2. Show SSID employee station.

NOTE: You can also enter the following commands to check the association status of a wireless client: show auth, show roaming cache, and show roaming cache mac <mac_addr>.

The setup of a single SmartPath AP is complete. Wireless clients can now associate with the SmartPath AP using SSID "employee" and access the network.

11.2 Example 2: Deploying a Cluster

Building on "Deploying a Single SmartPath AP" in Section 11.1, the office network has expanded and requires more SmartPath APs to provide greater coverage. In addition to the basic configuration covered in the previous example, you configure all three SmartPath APs to form a cluster within the same Layer 2 switched network. The following are the configuration details for the cluster:

- Cluster name: cluster1
- Preshared key for cluster1 communications: s1r70ckH07m3s

NOTE: The security protocol suite for cluster communications is WPA-AES-psk.

SmartPath AP-1 and -2 are cabled to a switch and use the native ("untagged") VLAN for wired backhaul communications. They communicate with each other over both wired and wireless backhaul links, the wired link taking precedence. However, SmartPath AP-3 only communicates with SmartPath AP-1 and -2 over a wireless link (see Figure 2). Because SmartPath AP-1 and -2 connect to the wired network, they act as portals. In contrast, SmartPath AP-3 is a mesh point.

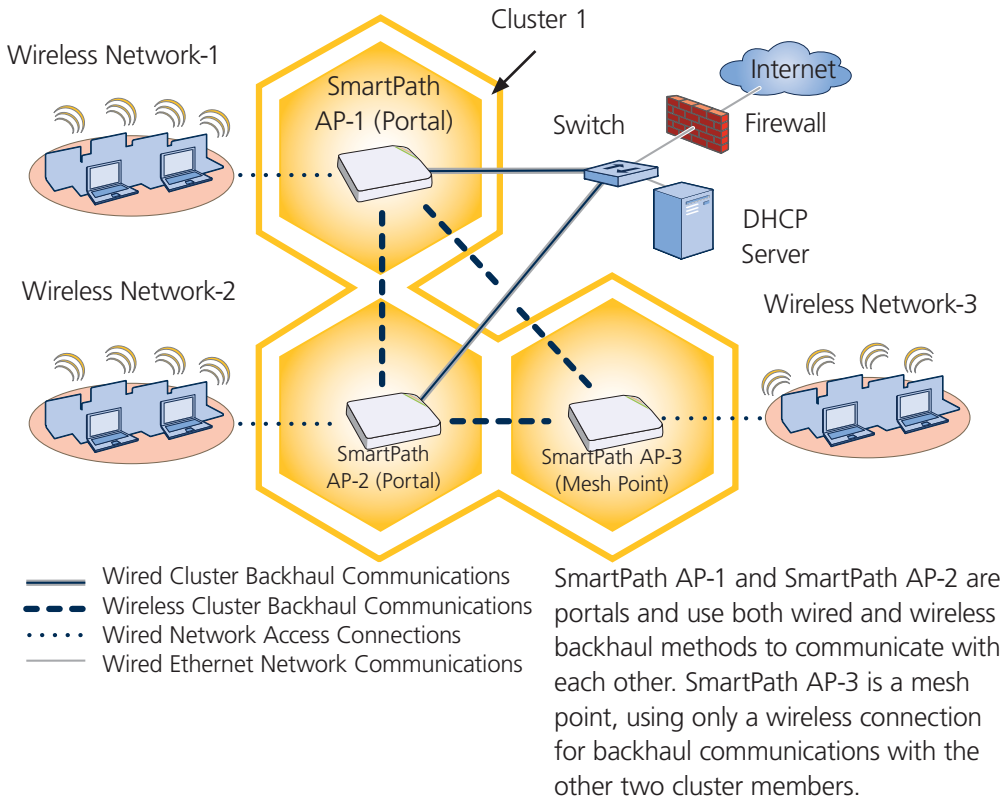


Figure 11-3. Three SmartPath APs in a cluster.

NOTE: If all cluster members can communicate over wired backhaul links, you can then use both radios for access. The wifi0 interface is already in access mode by default. To put wifi1 in access mode, enter this command: interface wifi1 mode access. In this example, however, a wireless backhaul link is required.

Step 1: Configure SmartPath AP-1

1. Using the connection settings described in the first example, log in to SmartPath AP-1.

2. Configure SmartPath AP-1 as a member of "cluster1" and set the security protocol suite.

```
cluster cluster1
```

You create a cluster, which is a set of SmartPath APs that collectively distribute data and coordinate activities among themselves, such as client association data for fast roaming, route data for making optimal data-path forwarding decisions, and policy enforcement for QoS and security.

```
cluster cluster1 password s1r70ckH07m3s
```

You define the password that cluster members use to derive the preshared key for securing backhaul communications with each other. The password must be the same on all cluster members.

```
interface mgt0 cluster cluster1
```

By setting "cluster1" on the mgt0 interface, you join SmartPath AP-1 to the cluster.

```
save config
```

3. Before closing the console session, check the radio channel that SmartPath AP-1 uses on its backhaul interface, which by default is wifi1:

```
show interface

State=Operational state; Chan=Channel;

Radio=Radio profile; U=up; D=down;

Name      MAC addr         Mode       State Chan  VLAN  Radio      Cluster     SSID

-------   --------------   --------   ----- ----  ----  --------   --------    --------

Mgt0      0019:7700:0020     -        U     -     1       -        cluster1      -

Eth0      0019:7700:0020   backhaul   U     -     1       -        cluster1      -

Wifi0     0019:7700:0024   access     U     11    -     radio_ng0    -           -

Wifi0.1   0019:7700:0024   access     U     11    -     radio_ng0  cluster1    employee

Wifi1     0019:7700:0028   backhaul   U     149   -     radio_na0    -           -

Wifi1.1   0019:7700:0028   backhaul   U     149   1     radio_na0  cluster1      -
```

The wifi1 interface and the wifi1.1 subinterface are in backhaul mode and are using channel 149. Both wifi1 and wifi1.1 use the default radio profile radio_na0. (Depending on the SmartPath AP model, the default profile might be radio_a0.) This is a profile for radio2, which operates in the 5 GHz frequency range as specified in the IEEE 802.11a and n standards.

Figure 11-4. Show interface.

SmartPath AP-1 is set to use wireless interface wifi1 and its subinterface wifi1.1 for backhaul communications.

Write down the radio channel for future reference (in this example, it is 149). When configuring SmartPath AP-2 and -3, make sure that they also use this channel for backhaul communications.

```
exit
```

Step 2: Configure SmartPath AP-2 and SmartPath AP-3.

1. Power on SmartPath AP-2 and log in through its console port.
2. Configure SmartPath AP-2 with the same commands that you used for SmartPath AP-1:

```
ssid employee

ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
```

```
interface wifi0 ssid employee
cluster cluster1
cluster cluster1 password s1r70ckH07m3s
interface mgt0 cluster cluster1
```

3. (Optional) Change the name and password of the superuser.

```
admin superuser mwebster password 3fF8ha
```

4. Check that the channel ID for wifi1 and wifi1.1 is now 149.

```
show interface
```

If the channel ID for wifi1 and wifi1.1 is not 149, set it to 149 so that SmartPath AP-2 uses the same channel as SmartPath AP-1 for backhaul communications.

```
interface wifi1 radio channel 149
```

Setting the channel for the parent interface (wifi1) sets it for all its subinterfaces. An interface in backhaul mode only needs one subinterface, which by default is wifi1.1.

```
save config
exit
```

5. Repeat the above steps for SmartPath AP-3.

Step 3: Connect SmartPath AP-2 and SmartPath AP-3 to the network.

1. Place SmartPath AP-2 within range of its clients and within range of SmartPath AP-1. This allows SmartPath AP-1 and -2 to send backhaul communications to each other wirelessly as a backup path in case either member loses its wired connection to the network.
2. Connect an Ethernet cable from the PoE In port on SmartPath AP-2 to the network switch.
3. Power on SmartPath AP-2 by connecting it to a power source.

After SmartPath AP-2 finishes booting up (indicated when the Power LED changes from steady amber to steady green), it automatically discovers another member of cluster1 (SmartPath AP-1). The two members use a preshared key based on their shared secret (s1r70ckH07m3s) to authenticate each other and AES to encrypt wired backhaul communications and AES-CCMP to encrypt wireless backhaul communications between themselves. You can tell when they have formed a cluster because the Mesh LED changes its blinking pattern from a fast to slow.

4. Place SmartPath AP-3 within range of its wireless clients and one or both of the other cluster members.
5. Power on SmartPath AP-3 by connecting it to a power source.

After SmartPath AP-3 boots up, it discovers the two other members of cluster1 over a wireless backhaul link. The members authenticate themselves and establish a security association for encrypting backhaul communications among themselves. SmartPath AP-3 then learns its default route to the wired network from the other cluster members. If the other members send routes with equal costs—which is what happens in this example—SmartPath AP-3 uses the first route it receives. When it learns this route, it can communicate with the DHCP server to get an IP address for its mgt0 interface.

6. Check that SmartPath AP-3 has associated with the other members at the wireless level.

Log in to SmartPath AP-3 and enter this command to see its neighbors in cluster1:

Log in to SmartPath AP-3 and enter this command to see its neighbors in SmartPath AP-1:

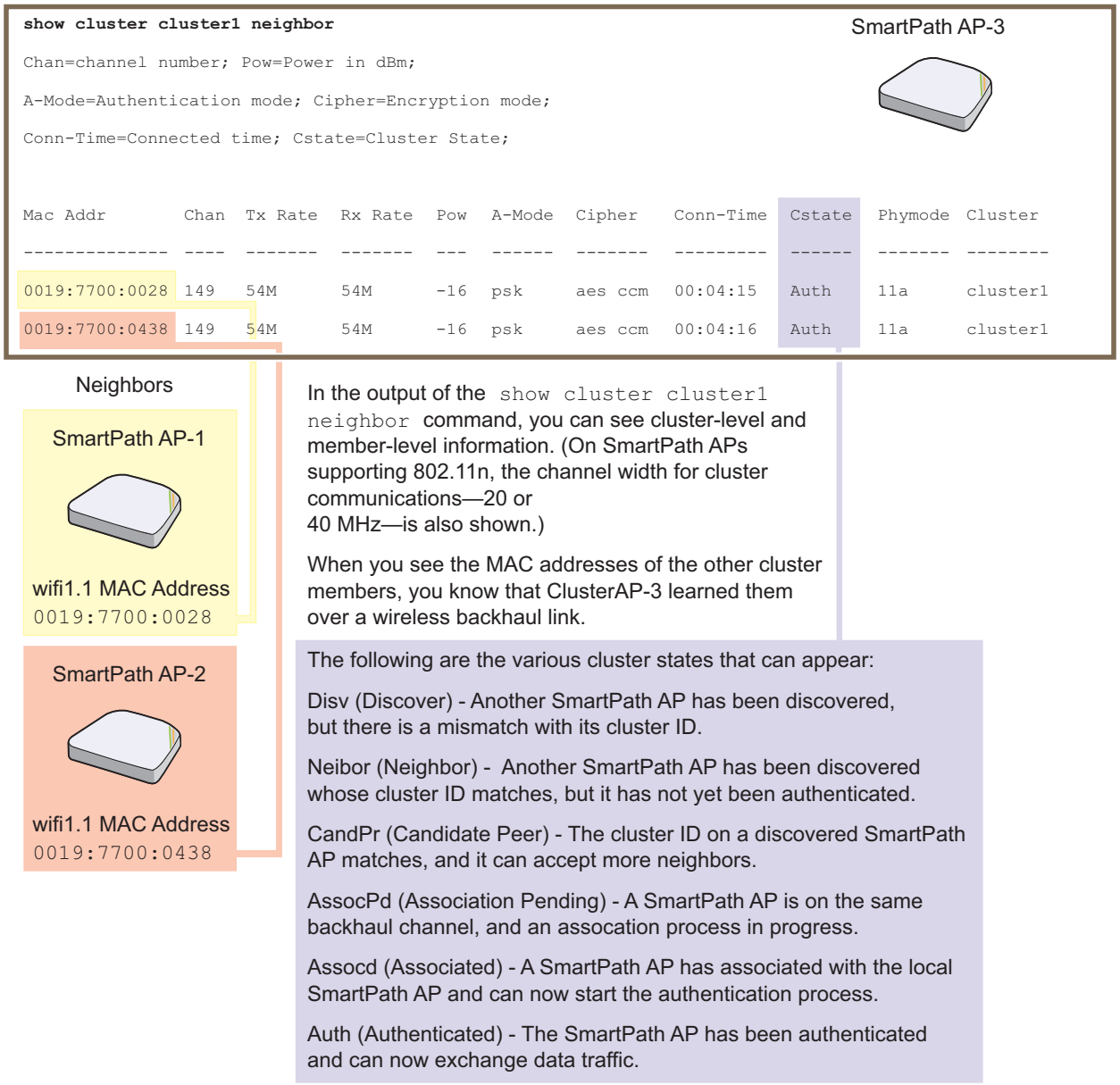


Figure 11-5. Neighbors in Cluster 1.

7. To check that the cluster members have full data connectivity with each other, associate a client in wireless network-1 with SmartPath AP-1 (the SSID "employee" is already defined on clients in wireless network-1; see Section 11.1). Then check if SmartPath AP-1 forwards the client's MAC address to the others to store in their roaming caches.

After associating a wireless client with SmartPath AP-1, log in to SmartPath AP-1 and enter this command:

```
show ssid employee station
```

After associating a wireless client with SmartPath AP-1, log in to SmartPath AP-1 and enter this command:

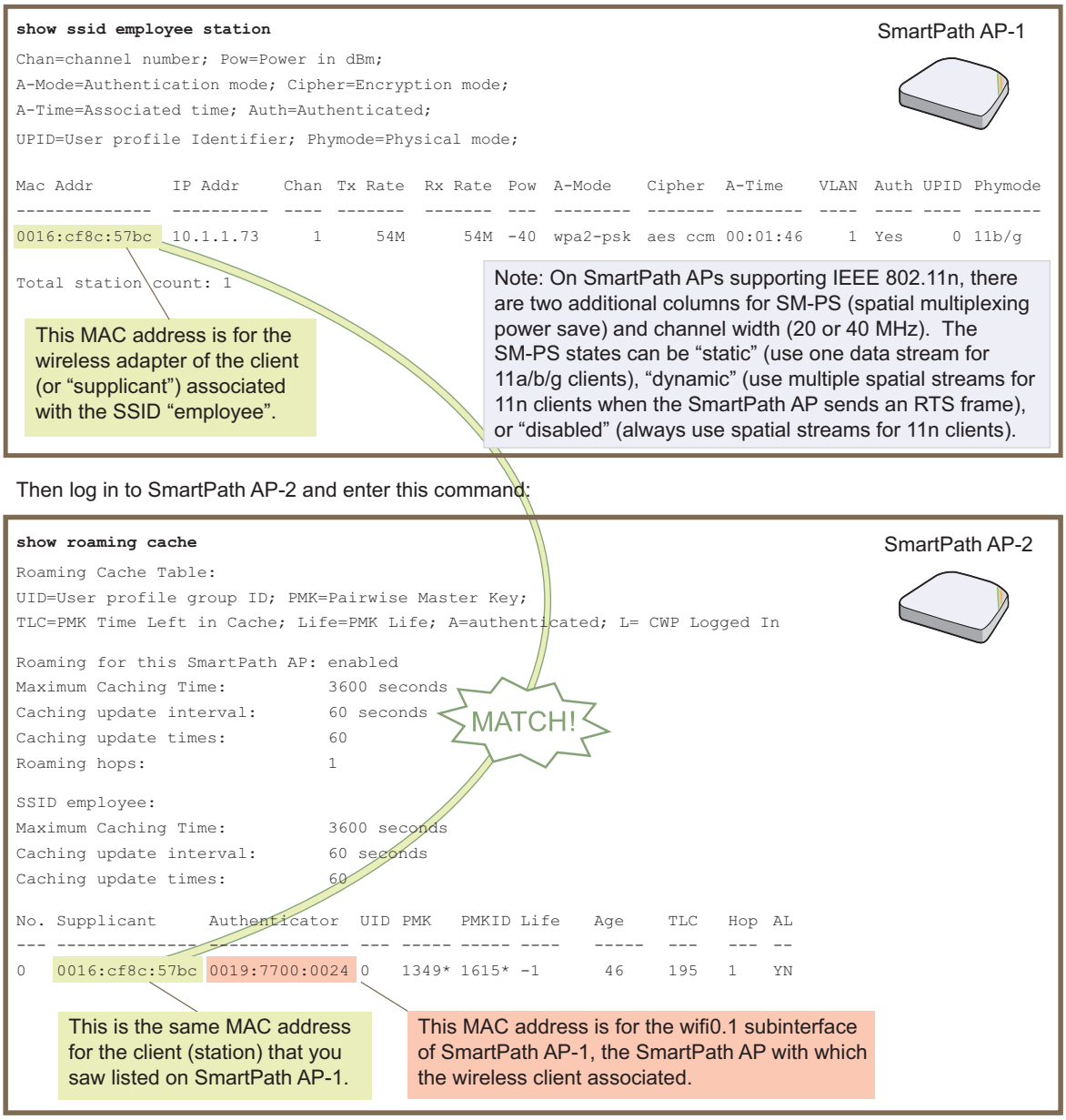


Figure 11-6. Show SSID employee station.

When you see ther MAC address of the wireless client that is associated with SmartPath AP-1 in the roaming cache of SmartPath AP-2, you know that SmartPath AP-1 and -2 are successfully sending data over the backhaul link.

Repeat this to confirm that SmartPath AP-3 also has a backhaul connection with the other members.

Step 4: Configure wireless clients.

Define the "employee" SSID on all the wireless clients in wireless network-2 and -3. Specify WPA-PSK for network authentication, AES or TKIP for data encryption, and the preshared key N38bu7Adr0n3.

The setup of cluster1 is complete. Wireless clients can now associate with the SmartPath APs using SSID "employee" and access the network. The SmartPath APs communicate with each other to share client associations (to support fast roaming) and routing data (to select optimal data paths).

11.3 Example 3: Using IEEE 802.1x Authentication

In this example, you use a Microsoft AD (Active Directory) server and a RADIUS server to authenticate wireless network users. To accomplish this, you make the following modifications to the cluster set up in "Deploying a Cluster:"

- Configure settings for the RADIUS server on the SmartPath APs
- Change the SSID parameters on the SmartPath APs and wireless clients to use IEEE 802.1X.

The basic network design is shown in Figure 11-7.

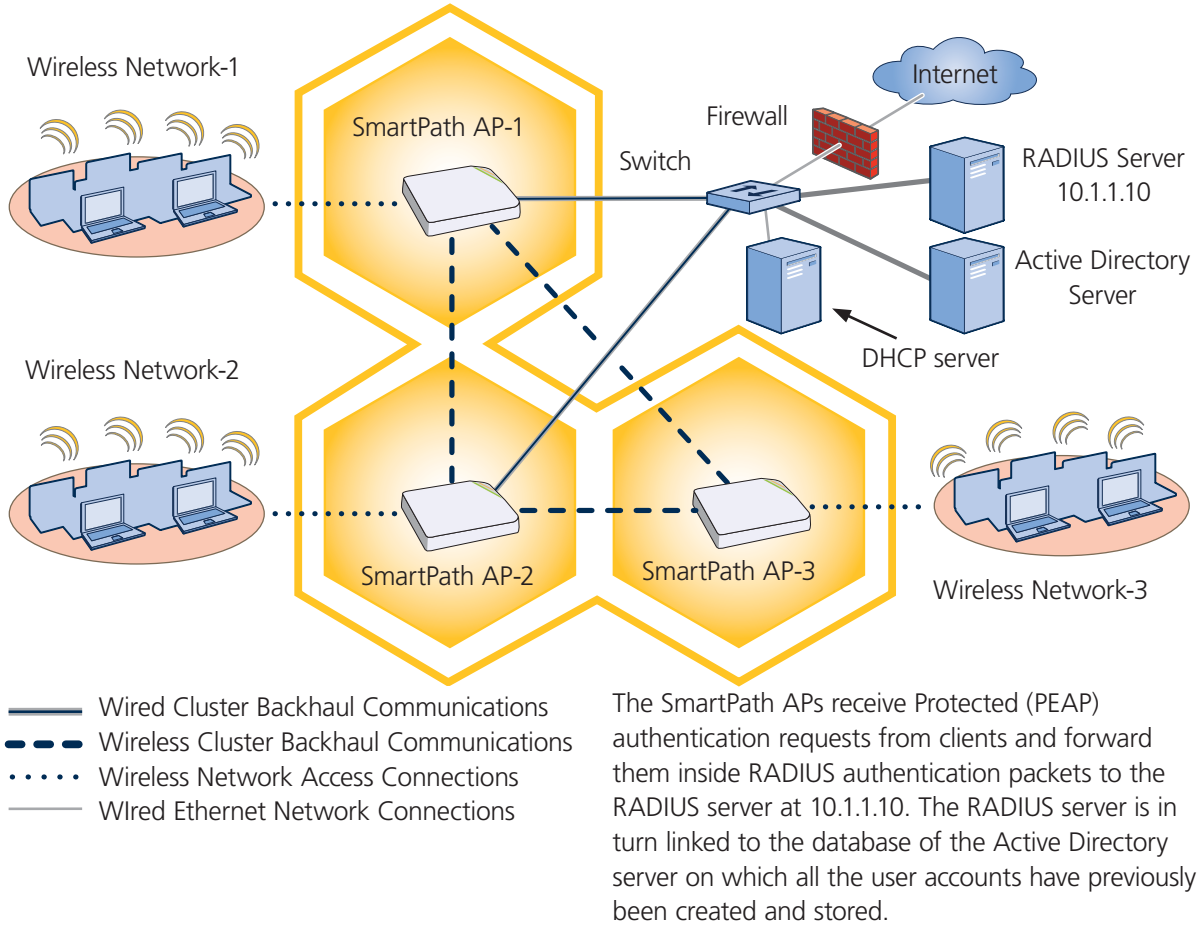


Figure 11-7. Cluster and 802.1X authentication.

NOTE: This example assumes that the RADIUS and AD servers were previously configured and populated with user accounts that have been in use on a wired network (not shown). The only additional configuration on these servers is to enable the RADIUS server to accept authentication requests from the SmartPath APs.

Step 1: Define the RADIUS server on the SmartPath AP-1.

Configure the settings for the RADIUS server (IP address and shared secret) on SmartPath AP-1.

```
aaa radius-server first 10.1.1.10 shared-secret s3cr3741n4bl0X
```

The IP address of the RADIUS server is 10.1.1.10, and the shared secret that SmartPath AP-1 and the RADIUS server use to authenticate each other is "s3cr3741n4b10X". You must also enter the same shared secret on the RADIUS server when you define the SmartPath APs as access devices (see Step 4).

Step 2: Change the SSID on SmartPath AP-1.

1. Change the authentication method in the SSID.

```
ssid employee security protocol-suite wpa-auto-8021x
save config
```

The protocol suite requires Wi-Fi Protected Access (WPA) or WPA2 security protocol for authentication and key management, AES or TKIP encryption, and user authentication through IEEE 802.1X.

2. Enter the `show interface mgt0` command and note the dynamically assigned IP address of the mgt0 interface. You need to know this address to define SmartPath AP-1 as an access device on the RADIUS server in Step 4.

```
exit
```

Step 3: Configure SmartPath AP-2 and SmartPath AP-3.

1. Log in to SmartPath AP-2 through its console port.

2. Configure SmartPath AP-2 with the same commands that you used for SmartPath AP-1:

```
aaa radius-server first 10.1.1.10 shared-secret s3cr3741n4bl0X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

NOTE: Although all SmartPath APs in this example use the same shared secret, they can also use different secrets.

3. Enter the show interface mgt0 command to learn its IP address. You need this address for Step 4.

```
exit
```

4. Log in to SmartPath AP-3 and enter the same commands.

Step 4: Configure the RADIUS Server to accept authentication requests from the SmartPath APs.

Log in to the RADIUS server and define the three SmartPath APs as access devices. Enter their individual mgt0 IP addresses or the subnet containing the IP addresses of all their mgt0 interfaces and the shared secret:

```
s3cr3741n4bl0X
```

Step 5: Modify the SSID on the wireless clients.

Modify the "employee" SSID on all the wireless clients in wireless network-2 and -3. Specify WPA or WPA2 for network authentication, AES or TKIP for data encryption, and Protected EAP (PEAP) for user authentication.

If the supplicant is on a PC running Windows Vista and is on a domain, and the RADIUS server is configured with domain authentication:

1. View the available SSIDs in the area, and select employee.

2. Click Connect.

Because most PC-based supplicants use their Windows login credentials to authenticate the client with the domain, the 802.1X authentication process happens automatically.

NOTE: If the supplicant is on a PC running Windows XP, you must configure it to use PEAP for authentication. By default, a Windows XP wireless client uses Smart Card or other Certificate instead of PEAP.

If the supplicant is Windows based and you are not on a domain.

1. Configure the SSID on your client as follows:

   Network name (SSID): employee

   Network authentication: WPA2

   Data encryption: AES

   Enable IEEE 802.1X authentication for this network: (select)

   EAP type: Protected EAP (PEAP)

   Authenticate as computer when computer information is available: (clear)

   Authenticate as guest when user or computer information is unavailable: (clear)

   Validate server certificate: (clear)

   Select Authentication Method: Secured password (EAP-MSCHAP v2)

   Automatically use my WIndows logon name and password (and domain if any): (clear)

2. View the available SSIDs in the area and select employee.
3. Click Connect.
4. When the prompt appears for you to select a certificate or enter other credentials to validate your identity, click the prompt, enter the user name and password that are stored on the RADIUS authentication server, and then click OK.

If the supplicant is on a Macintosh computer and is not on a domain:

1. View the available SSIDs in the area, and select employee.
2. Click Join Network.
3. Accept the certificate that the RADIUS server provides, assuming it is from a trustworthy source. After the RADIUS authentication server validates your identity, the client connects to the WLAN.

Step 6: Check that clients can form associations and access the network.

1. To check that a client can associate with a SmartPath AP and access the network, open a wireless client application and connect to the "employee" SSID. Then contact a network resource, such as a Web server.
2. Log in to the SmartPath AP CLI, and check that you can see the MAC address or the associated client and an indication that the correct SSID is in use by entering the following command:

```
show ssid employee station
```

```
show ssid employee station

Chan=channel number; Pow=Power in dbm;

A-Mode=Authentication mode; Cipher=Encryption mode;

A-Time=Associated time; Auth=Authenticated;

UPID=User profile Identifier; Phymode=Physical mode;

Mac Addr          IP Addr    Chan  Rate  Pow   A-Mode    Cipher    A-Time    VLAN  Auth  UPID  Phymode
--------------    ---------  ----  ----  ----  --------  -------   --------  ----  ----  ----  -------
0016:cf8c:57bc    10.1.1.35  11    54M   -38   wpa2-psk  aes ccm   00:00:56  1     Yes   0     11g
```

Check that the MAC address in the table matches that of the wireless client .

Check that the authentication and encryption modes match those in the SSID security protocol suite.

Figure 11-8. Checking the MAC address and authentication and encryption types.

Check that the MAC and IP addresses in the table match those of the wireless client.

Check that the authentication and encryption modes match those in the SSID security protocol suite.

NOTE: You can also enter the following commands to check the association status of a wireless client: show auth, show roaming cache, and show roaming cache mac <mac_addr>.

The setup for using IEEE 802.1X is complete. Wireless clients can now associate with the SmartPath AP using SSID "employee," authenticate themselves through IEEE 802.1X to a RADIUS server, and access the network.

11.4 Active Directory Integration Improvement

There are two significant improvements in Active Directory integration. The first simplifies the integration process between SmartPath AP RADIUS servers and Active Directory servers (domain controllers). The second makes it possible to configure SmartPath AP RADIUS servers to work with Active Directory servers when SmartPath EMS VMA is running in Express mode. The following section explains the simplified integration process.

Step 1: Configure Active Directory Settings for SmartPath AP RADIUS Servers

Define a SmartPath AP as a RADIUS server and configure it to work with an Active Directory server. The following steps explain the process when running SmartPath EMS VMA in Enterprise mode:

Click "Configuration > Advanced Configuration > Authentication > AAA User Directory Settings > New," and configure the following Active Directory settings:

Name: Type a name for this configuration. It can be up to 32 characters long and cannot contain spaces.

Description: Type a note about the configuration for later reference. It can be up to 64 characters long, including spaces.

Active Directory: (select)

SmartPath AP RADIUS Server: From the drop-down list, choose a SmartPath AP that you intend to make a RADIUS server.

Because other SmartPath APs acting as RADIUS authenticators must be able to send user authentication requests to the SmartPath AP RADIUS server, it cannot have a dynamically assigned IP address. Therefore, it cannot be a DHCP client; it must have a manually defined IP address, netmask, default gateway, and DNS server IP address. When you choose a SmartPath AP, its IP address, netmask, default gateway, and DNS server settings appear in the fields. In addition, if the SmartPath AP that you choose is a DHCP client, SmartPath EMS VMA prompts you to enter static network and DNS settings for it and then click "Apply." After you save this Active Directory configuration, SmartPath EMS VMA applies the new network and DNS settings to the SmartPath AP. The next time you push a configuration to that SmartPath AP, it will receive these new settings.

Default Domain

Domain: Type the DNS domain name to which the SmartPath AP RADIUS server and Active Directory server belong; for example, blackbox.com.

Active Directory Server: Choose a previously defined IP object/host name for the Active Directory server from the drop-down list. If you do not see the one that you need, click the New icon (+) and define it, or select the blank space at the top of the drop-down list and type the IP address or host name of the server. When you do so, SmartPath EMS VMA automatically creates a corresponding IP object/host name.

BaseDN: (read-only) After you configure this section and click "Retrieve Directory Information," SmartPath EMS VMA displays the BaseDN, which is the point in the LDAP tree structure under which the server stores user accounts in its database.

Computer OU: Set the OU (organizational unit) where the SmartPath AP RADIUS server has privileges to add itself as a computer in the domain or leave it blank. The default is the Computers OU, but you can configure this field to point to any container, based on your facility security policy. Enter this in the form ou/sub-ou/sub-ou, using only forward slashes. If any containers in the path contain spaces, enclose the entire string in quotation marks.

NOTE: The host name of a SmartPath AP RADIUS server stored in the computer OU on the Active Directory server has the following limitations: Its name cannot be longer than 256 characters and cannot contain underscores.

TLS Encryption: Select the checkbox to enable TLS (Transport Layer Security) to encrypt the user lookup requests that the SmartPath AP RADIUS server sends to the Active Directory server. Clear the checkbox to disable TLS encryption and send the lookup requests in plain text.

NOTE: The link that the SmartPath AP RADIUS server makes when it joins the Active Directory domain and logs in to the Active Directory server with its domain admin name and password is encrypted using Kerberos v5.

Click "Retrieve Directory Information." SmartPath EMS VMA attempts to retrieve the Active Directory server BaseDN. If the SmartPath AP succeeds in retrieving this information, it displays it along with the following message: "The Active Directory server IP address and the BaseDN were successfully retrieved." It also displays the following options and shows the Domain Admin Credentials to Join Domain section:

Domain Admin Credentials to Join Domain

Domain Admin: Enter the name that the SmartPath AP RADIUS server uses to log in to the Active Directory server and add itself as a computer in the domain, or as a computer in an organizational unit in the domain. The name must be for a domain user and have rights to create a computer in the domain, or create a computer in an organizational unit in the domain. It can be up to 64 characters long.

Password: Enter the password that the SmartPath AP RADIUS authentication server submits when joining an Active Directory domain. The password must exactly match the password entered for the user account defined on the Active Directory server for the SmartPath AP RADIUS authentication server. It can be up to 64 characters long. To ensure accuracy, enter the password again in the Confirm Password field. To see the text string that you type, clear the Obscure Password checkbox.

After you enter the appropriate domain administrator credentials, click "Join and Save" or "Join and Discard." The first option saves the domain admin credentials on SmartPath EMS VMA after successfully joining the domain; the second clears them. Choose the option that best satisfies your security policy. When you click one of the two Join options, the SmartPath AP RADIUS server attempts to add itself to the domain. If it is successful, the following message appears: "The SmartPath AP RADIUS server successfully joined the Active Directory domain." In addition, the Domain Users Credentials for User Auth section appears.

Domain Users Credentials for User Auth

Domain User: Enter the name that the SmartPath AP RADIUS server provides to authenticate itself to the Active Directory server when initiating a connection to request a user account lookup. The domain user name can be in either user principal format (user@domain.com) or DN format (cn=administrator,cn=users,dc=domain,dc=com).

Password: Enter the password that the SmartPath AP RADIUS server supplies when requesting a user account lookup on the Active Directory server. The password must exactly match the password entered for the user account defined on the Active Directory server for the SmartPath AP RADIUS server. It can be up to 64 characters long. To ensure accuracy, enter the password again in the Confirm Password field. To see the text string that you type, clear the Obscure Password checkbox.

After you enter the appropriate domain user credentials, click "Test Authentication." SmartPath EMS VMA submits its domain user name and password to authenticate itself. If successful, the following message appears: "The user was successfully authenticated." In addition, the Multiple Domain Info section appears. You can define up to eight Active Directory domains in one or more forests in which SmartPath AP RADIUS servers can perform user lookups. The domain you define first—before adding others—is the default domain and indeed is identified as such by the section heading, Default Domain.

Multiple Domain Info

A SmartPath AP RADIUS server can support authentication lookups of users in up to eight Active Directory domains in one or more forests. To add a domain, click "New," enter the following, and then click "Apply:"

Domain: Enter the Windows domain name to which the SmartPath AP RADIUS authentication server and Active Directory server both belong. This must not include any parent domains, such as .com, .net, .org, and so on. The domain name can be up to 64 characters long.

Full Name: Enter the complete Windows DNS domain name, including parent domains. For example, if the domain is "blackbox" and it is a child domain of "com", then enter "blackbox.com" here. The full domain name can be up to 64 characters long.

Active Directory Server: Enter the IP address or resolvable domain name of the Active Directory server that contains the user accounts you want the SmartPath AP RADIUS authentication server to authenticate. The server domain name can be up to 64 characters long.

Domain User: Enter the name that the SmartPath AP RADIUS server provides to authenticate itself to the Active Directory server when initiating a connection to request a user account lookup. The form of the name must match the form that appears as an entry on the Active Directory server. For example, the entry name might be "clusterap1" and be located in the LDAP directory structure at "cn=clusterap1,cn=admins,cn=users,dc=blackboxblackboxblackboxblackbox,dc=com". It might also be in e-mail format, such as "jsmith@apis.com," for example. It can be up to 256 characters long.

Password: Enter the password that the SmartPath AP RADIUS server supplies when requesting a user account lookup on the Active Directory server. The password must exactly match the password entered for the user account defined on the Active Directory server for the SmartPath AP RADIUS server. It can be up to 64 characters long. To ensure accuracy, enter the password again in the Confirm Password field. To see the text string that you type, clear the Obscure Password checkbox.

Step 2: Configure SmartPath AP RADIUS Server Settings that Reference the Active Directory Settings

Click "Configuration > Advanced Configuration > Authentication > SmartPath AP AAA Server Settings > New," enter the following, and then click "Save:"

Name: Type a name for this configuration. It can be up to 32 characters long and cannot contain spaces.

Description: Type a note about the configuration for later reference. It can be up to 64 characters long, including spaces.

Expand the Database Access Settings section, and select Active Directory. From the Active Directory drop-down list, choose the name of the Active Directory settings that you created on the AAA User Directory Settings page above. From the Server Role drop-down list, choose Primary. Then click "Apply."

Select LDAP server attribute mapping. A new section expands. You have the option of manually mapping LDAP user groups to local user profiles or automatically mapping LDAP user groups to user profiles through the use of matching attributes.

Manually map LDAP user groups to user profiles: Select this option to display the Active Directory domain and LDAP directory structure retrieved from the server so that you can make a direct, static map of LDAP user groups (or OUs) on the Active Directory server to user profiles on SmartPath AP RADIUS authenticators.

LDAP User Group Attribute: Enter the attribute name defined on the Active Directory server that you want to use to link users to user profiles on SmartPath AP authenticators. The default LDAP user group attribute name on Active

Directory is "memberOf". (The attribute type set on the Active Directory server must be "string".) The LDAP user group attribute string can be up to 32 characters long.

SmartPath AP for communication: Choose the name of the SmartPath AP to use as a medium for communicating with the Active Directory server. The usual choice is the SmartPath AP RADIUS server specified in the Active Directory profile.

Select an OU from the directory that has the same attribute name as that defined in the LDAP User Group Attribute field. The default is "memberOf". Then, from the User Profile drop-down list, choose the user profile that you want to apply to users in the selected OU, and click "Apply."

NOTE: If you select Global Catalog near the top of the page, then you also have the choice to type the user group name instead of selecting an OU in the directory tree.

The mappings of OU to user profile are then shown in the order in which SmartPath AP authenticators will apply them, starting from the top. If you want to rearrange the order of the mappings, select the checkbox of one of the OU-to-user profile mapping, and then click the Up or Down arrow on the far right to move it to its new position.

Automatically map LDAP user groups to user profiles by matching attributes: Select this option to display the attribute names that the Active Directory is using for user profiles, VLANs, and reauthorization time so that you can use them to make a dynamic mapping of LDAP user groups (or OUs) on the Active Directory server to user profiles on SmartPath AP RADIUS authenticators.

User Profile Attribute: Enter the attribute name defined on the Active Directory server that you want to map to the user profile attribute defined on SmartPath AP RADIUS authenticators. By default, the SmartPath AP RADIUS server maps the msRADIUSCallbackNumber attribute in Active Directory to the user profile attribute defined on SmartPath AP RADIUS authenticators. The attribute type set on the Active Directory server must be "string" and can be up to 32 characters long.

VLAN ID: Enter the attribute name defined on the Active Directory server whose VLAN ID setting you want to apply to the authenticated user. By default, the SmartPath AP RADIUS server maps the msRASSavedCallbackNumber attribute in Active Directory to the VLAN ID and forwards this to SmartPath AP RADIUS authenticators. The attribute type set on the Active Directory server must be "string" and can be up to 32 characters long.

Reauthorization Time: Enter the attribute name defined on the Active Directory server whose reauthorization time setting you want to apply to the authenticated user. By default, the SmartPath AP RADIUS server maps the msRADIUSServiceType attribute in Active Directory to the reauth time and forwards this to SmartPath AP RADIUS authenticators. The attribute type set on the Active Directory server must be "integer" and can be up to 32 characters long.

Step 3: Assign the RADIUS Server Settings to SmartPath APs

Click "Monitor > Access Points > SmartPath APs," select Config at the top of the main window, select the checkbox next to a SmartPath AP with a static IP address that you want to make a RADIUS server, and then click "Modify." Expand the Service Settings section, choose the SmartPath AP AAA Server Settings name from the SmartPath AP RADIUS Service drop-down list, and then click "Save."

Repeat the above step for any other SmartPath APs that you want to make RADIUS servers with access to the same Active Directory server. When done, push the configuration to all the SmartPath APs.

11.5 RADIUS Authentication for VHM Administrators

In previous SmartPath EMS VMA versions, it was only possible to use RADIUS authentication for home system administrators when no VHMs were present. Now both home system administrators and VHM administrators can be authenticated through an external RADIUS server.

To configure SmartPath EMS VMA to authenticate administrators whose login accounts are stored on an external RADIUS server:

1. Log in to the home system as an admin with super-user privileges. Either note the name and attribute number of one of the predefined admin groups or create a new one. To create a new admin group, click "Home > Administration > Administrators > Admin Groups > New," enter the following, and then click "Save:"

Name: Type a name for the group.

Attribute: Assign an unused attribute number to the group. You can see which attributes are already in use on the Home > Administration > Administrators > Admin Groups page. (To see the admin group attribute numbers for the home system and all VHMs, log in to All VHMs by clicking "Log Out > Switch Virtual HM > All VHMs.")

Select read and write privileges for the features and maps that you want to enable for members of this group.

2. Either log in to the VHM with VHM admin credentials or log in to the home system with super-user privileges and then switch to the VHM by clicking Log Out > Switch Virtual HM > vhm_name. If one of the predefined admin groups suits your needs, note its name and attribute number. If not, create a new admin group by clicking "Home > Administration > Administrators > Admin Groups > New," entering the following, and then clicking "Save:"

Name: Type a name for the group.

Attribute: Assign an unused attribute number to the group.

NOTE: You can see which attributes are already in use on the home system and all VHMs on the Home > Administration > Administrators > Admin Groups page when you are logged in to All VHMs. If you are a VHM admin logged in to your VHM, you can only see the attributes for those groups in your VHM.

Select read and write privileges for the features and maps that you want to enable for members of this group.

3. To configure SmartPath EMS VMA to communicate with the RADIUS server, click "Home > Administration > SmartPath EMS VMA Services," select HM Admin Authentication, enter the following, and then click "Update:"

HM Admin Authentication: To enable SmartPath EMS VMA admin accounts stored on SmartPath EMS VMA and on a RADIUS server, choose "Both" from the drop-down list.

Authentication Type: Choose either PAP or CHAP or MS CHAP V2. See the SmartPath EMS Online Help for more information about these options.

RADIUS Server: Choose the RADIUS server configuration from the drop-down list. If you do not see the one you need, click the New icon (+) and create it.

4. Click "Home > Administration > Auxiliary Files > RADIUS Dictionary," and download the RADIUS dictionary file from SmartPath EMS VMA to your management system. Using a text editor, add the names and attributes of the predefined VHM admin groups as well as any other admin-defined groups to the file. It is the attribute number that links an admin on the RADIUS server to the correct admin group—and correct VHM—on SmartPath EMS VMA.

5. Import the RADIUS dictionary file into the RADIUS server, and configure the RADIUS server to communicate with SmartPath EMS VMA as a network access server (NAS).

11.6 Example 4: Applying QoS

In this example, you want the cluster members to prioritize voice, streaming media, and e-mail traffic. First, you map distinguishing elements of these traffic types to three SmartPath QoS classes:

Class 6: voice traffic from VoIP phones with MAC OUI 00:12:3b (the OUI for all phones in the network)

Voice traffic is very sensitive to delay and cannot tolerate packet loss without loss of voice quality. When other traffic is competing with voice traffic for bandwidth, it becomes essential to prevent that traffic from interfering with voice traffic. Because voice traffic for a single call requires very little bandwidth—typically from 8 to 64 kbps depending on the voice codec used—a good approach for setting its rate is to calculate the bandwidth necessary for a voice call plus related telephony traffic from a single user's computer, softphone, or handset and then multiply that by the potential number of concurrent VoIP users.

Class 5: streaming media using the Microsoft Media Server (MMS) protocol on TCP Port 1755

Although streaming media is also time sensitive, streaming media software for both clients and servers offers limited buffering to prevent choppy sounds and pixelated video when network congestion occurs. Because congestion for more than a few seconds can adversely effect streaming media, it is important to assign this type of traffic a higher priority than other types, but its priority should be lower than that for voice, which is even more sensitive to delay.

Class 3: data traffic for e-mail using the following protocols:

SMTP (Simple Mail Transfer Protocol) on TCP Port 25

POP3 (Post Office Protocol version 3) on TCP Port 110

Then you create classifier profiles that reference these traffic-to-class mappings. You bind the profiles to the wifi0.1 and eth0 interfaces so that cluster members map the traffic matching these profiles that arrives at these interfaces to the proper SmartPath classes.

You next define a QoS policy that defines how the cluster members prioritize and process the traffic mapped to Classes 6, 5, and 3. The QoS policy (named "voice") is shown in Figure 11-9 and has these settings:

Class 6 (voice)

Forwarding: strict (Cluster members forward traffic mapped to this class immediately without queuing it.)

Maximum rate for all Class 6 traffic: 512 kbps, which supports an 8- to 64-kbps VoIP call (depending on the compression that the codec provides) plus other telephony traffic such as DHCP, DNS, HTTP, and TFTP.

Class 5 (streaming media)

Forwarding: WRR (weighted round robin) with a weight of 90

By assigning class 5 a higher weight (90) than Class 3 and 2 weights (Class 3 = 60, Class 2 = 30), you give streaming media roughly a 3:2 priority over Class 3 traffic and a 3:1 priority over Class 2 traffic.

Maximum traffic rate for all Class 5 traffic: 20,000 kbps

You change the bandwidth available for streaming media when there is no competition for it (the default rate for Class 5 is 10,000 kbps on SmartPath APs that do not support the IEEE 802.11n standard and 50,000 kbps on SmartPath APs that do. However, you do not set the maximum rate (54,000 or 1,000,000 kbps, depending on the SmartPath AP model that you are configuring) to ensure that streaming media does not consume all available bandwidth even if it is available.

Class 3 (e-mail)

Forwarding: WRR with a weight of 60

To help ensure that e-mail traffic remains flowing even when other types of data traffic compete with it for available bandwidth, you elevate its priority by mapping SMTP and POP3 traffic to Class 3 and giving that class a higher weight (60) than the weight for Class 2 traffic (30).

Maximum traffic rate for all Class 3 traffic: 54,000 or 1,000,000 kbps (the default, depending on the SmartPath AP)

NOTE: The SmartPath AP assigns all traffic that you do not specifically map to a class to Class 2, which by default uses WRR with a weight of 30 and a rate of 54,000 or 1,000,000 kbps, depending on the SmartPath AP.

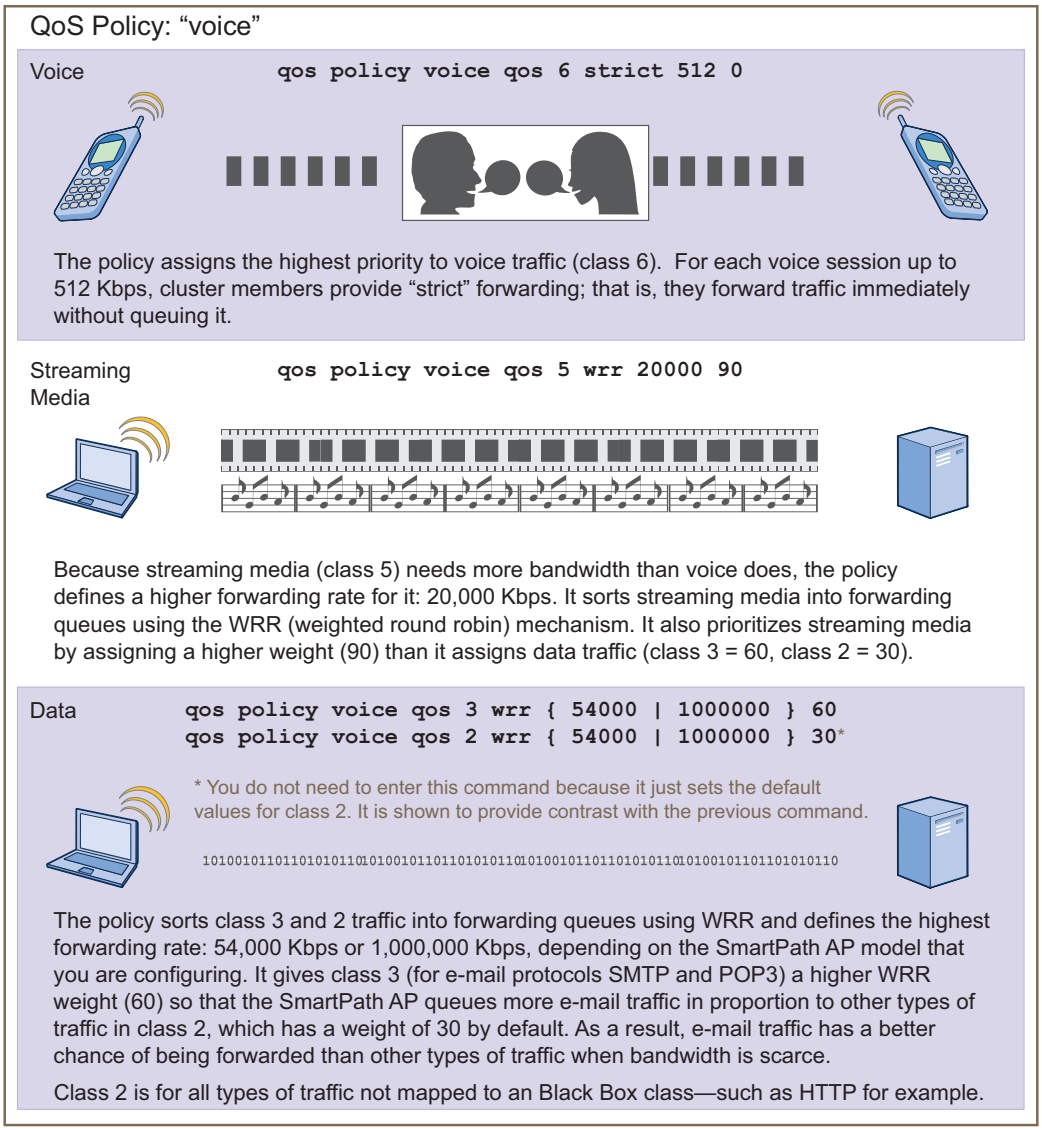


Figure 11-9. QoS policy “voice” for voice, streaming media, and data.

NOTE: This example assumes that the RADIUS and AD servers were previously configured and populated with user accounts and have been serving a wired network (not shown). The only additional configuration is to enable the RADIUS server to accept authentication requests from the SmartPath APs.

Finally, you create a user profile “employee-net” and apply the QoS policy “voice” to the user profile on each cluster member. You also configure the RADIUS server to return attributes in its authentication responses to indicate the user group to which the cluster members then assign users.

Step 1: Map traffic types to QoS classes on SmartPath AP-1.

1. Map the MAC organizational unit identifier (OUI) of network users’ VoIP phones to Class 6.

```
qos classifier-map oui 00:12:3b qos 6
```

In this example, all network users use VoIP phones from the same vendor whose OUI (that is, the MAC address prefix) is 00:12:3b. When SmartPath AP-1 receives traffic from a client whose source MAC address contains this OUI, it assigns it to Class 6.

2. Define the custom services that you need.

```
service mms tcp 1755

service smtp tcp 25

service pop3 tcp 110
```

The Microsoft Media Server (MMS) protocol can use several transports (UDP, TCP, and HTTP). However, for a SmartPath AP to be able to map a service to a SmartPath QoS class, it must be able to identify that service by a unique characteristic such as a static destination port number or a nonstandard protocol number. Unlike MMS/UDP and MMS/HTTP, both of which use a range of destination ports, MMS/TCP uses the static destination Port 1755, which a SmartPath AP can use to map the service to a class.

Therefore, you define a custom service for MMS using TCP Port 1755. You also define custom services for SMTP and POP3 so that you can map them to SmartPath Class 3. By doing so, you can prioritize e-mail traffic above other types of traffic that the SmartPath AP assigns to Class 2 by default.

3. Map services to classes.

```
qos classifier-map service mms qos 5

qos classifier-map service smtp qos 3

qos classifier-map service pop3 qos 3
```

Unless you map a specific service to a QoS class, a SmartPath AP maps all traffic to Class 2. In this example, you prioritize voice, media, and e-mail traffic by assigning them to higher QoS classes than Class 2, and then by defining the forwarding and weighting mechanisms for each class (see Step 3).

Step 2: Create profiles to check traffic arriving at interfaces on SmartPath AP-1.

1. Define two classifier profiles for the traffic types “mac” and “service.”

```
qos classifier-profile employee-voice mac

qos classifier-profile employee-voice service

qos classifier-profile eth0-voice mac

qos classifier-profile eth0-voice service
```

Classifier profiles define which components of incoming traffic SmartPath AP-1 checks. Because you specify "mac" and "service", it checks the MAC address in the Ethernet frame header and the service type (by protocol number in the IP packet header and port number in the transport packet header). If it detects traffic matching a classifier-map, it maps it to the appropriate class. However, before this can happen, you must first associate the profiles with the interfaces that will be receiving the traffic that you want checked. This you do with the next two commands.

2. Associate the classifier profiles with the employee SSID and the eth0 interface so that SmartPath AP-1 can classify incoming traffic arriving at these two interfaces.

```
ssid employee qos-classifier employee-voice

interface eth0 qos-classifier eth0-voice
```

By creating two QoS classifiers and associating them with the employee SSID and eth0 interface, SmartPath AP-1 can classify traffic flowing in both directions for subsequent QoS processing; that is, it can classify traffic flowing from the wireless LAN to the wired LAN, and from the wired LAN to the wireless LAN.

NOTE: If the surrounding network uses the IEEE 802.1p QoS classification system (for wired network traffic) or 802.11e (for wireless network traffic), you can ensure that SmartPath AP-1 checks for them by entering these commands:

```
qos classifier-profile eth0-voice 8021p

qos classifier-profile employee-voice 80211e
```

Step 3: Apply QoS on SmartPath AP-1.

1. Create a QoS policy.

For SmartPath APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For SmartPath APs supporting IEEE 802.11a/b/g/n:

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
```

By default, a newly created QoS policy attempts to forward traffic mapped to Classes 6 and 7 immediately upon receipt. This immediate forwarding of received traffic is called "strict" forwarding. To assign strict forwarding to VoIP traffic from phones whose MAC OUI is mapped to Class 6, you simply retain the default settings for Class 6 traffic on SmartPath APs supporting 802.11a/b/g data rates. For SmartPath APs supporting 802.11n data rates, the default user profile rate is 20,000 kbps for Class 6 traffic, so you change it to 512 kbps.

For Classes 5 and 3, you limit the rate of traffic and set WRR weights so that the SmartPath AP can control how to put the rate-limited traffic into forwarding queues. You use the default settings for Class 2 traffic.

When you enter any one of the above commands, the SmartPath AP automatically sets the maximum bandwidth for all members of the user group to which you later apply this policy and the bandwidth for any individual group member. You leave the maximum traffic rate at the default 54,000 or 1,000,000 kbps—depending on the SmartPath AP model that you are configuring—for the user group. You also leave the maximum bandwidth for a single user at 54,000 or 1,000,000 kbps, so that if a single user needs all the bandwidth and there is no competition for it, that user can use it all.

Also by default, the traffic rate for this policy has a weight of 10. At this point, because this is the only QoS policy, the weight is inconsequential. If there were other QoS policies, then their weights would help determine how the SmartPath AP would allocate the available bandwidth.

The QoS policy that you define is shown in Figure 11-10. Although you did not configure settings for QoS Classes 0, 1, 2, 4, and 7, the policy applies default settings to them. The SmartPath AP assigns all traffic that you do not specifically map to a class to Class 2, which uses WRR with a weight of 30 and a default rate of 54,000 or 1,000,000 kbps. Because nothing is mapped to Classes 0, 1, 4, and 7, their settings are irrelevant.

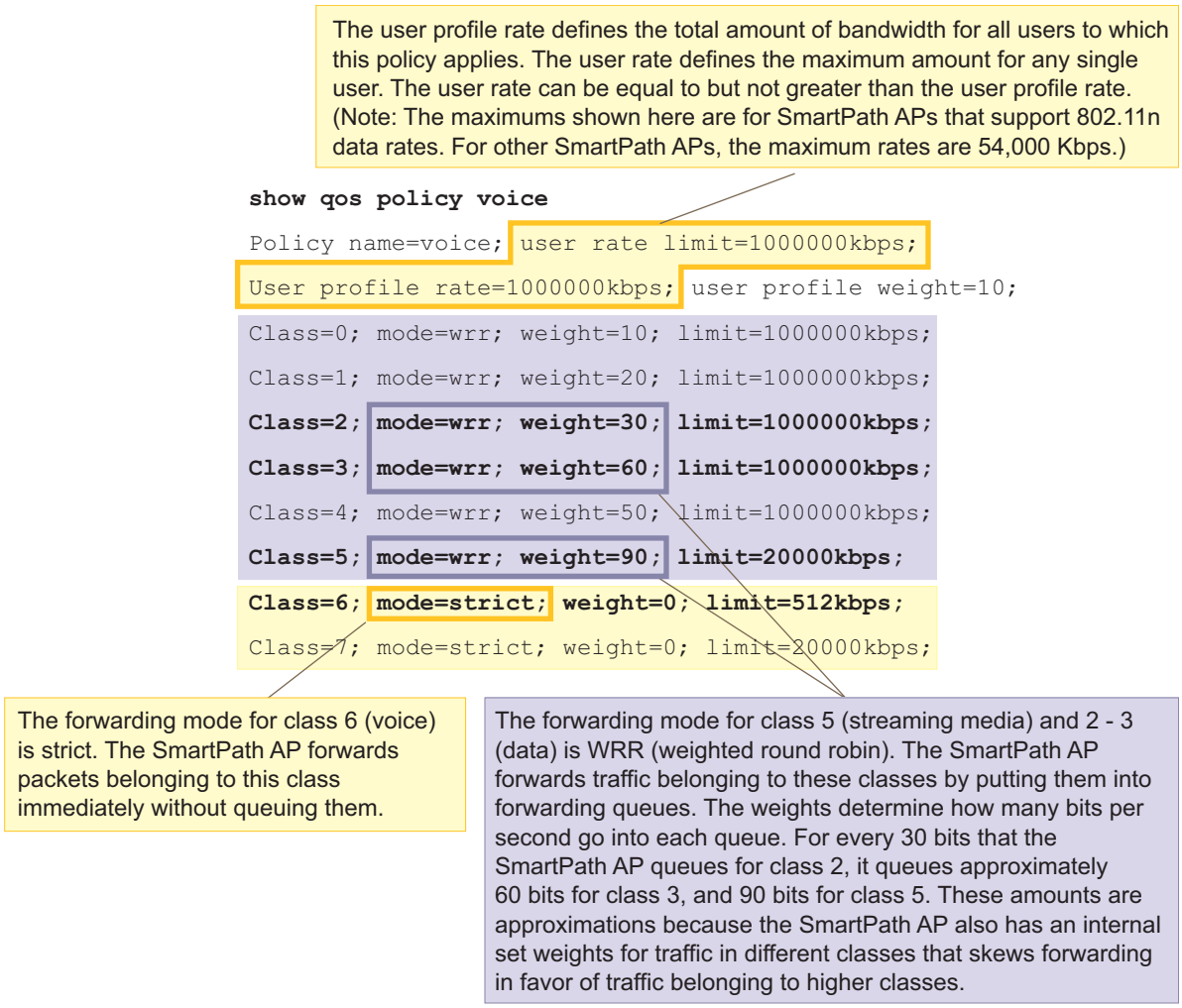


Figure 11-10. QoS policy "voice."

2. Create a user profile and apply the QoS policy to it.

```
user-profile employee-net qos-policy voice attribute 2
```

You apply the QoS policy "voice" to all users belonging to the user-profile "employee-net" with attribute 2. On the RADIUS server, you must configure Attribute 2 as one of the RADIUS attributes that the RADIUS server returns when authenticating users (see Step 5 on the next page).

NOTE: When SmartPath AP-1 does not use RADIUS for user authentication, you must assign the user profile to an SSID. To do that, use the following command: `ssid employee default-user-profile-attr 2`

```
save config
exit
```

Step 4: Configure SmartPath AP-2 and SmartPath AP-3.

1. Log in to SmartPath AP-2 through its console port.

2. Configure SmartPath AP-2 with the same commands that you used for SmartPath AP-1:

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For SmartPath APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For SmartPath APs supporting IEEE 802.11a/b/g/n:

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 1000000 60
user-profile employee-net qos-policy voice attribute 2
save config
exit
```

3. Log in to SmartPath AP-3 and enter the same commands.

Step 5: Configure RADIUS server attributes.

1. Log in to the RADIUS server and define the three SmartPath APs as RADIUS clients.

2. Configure the following attributes for the realm to which the wireless user accounts in network-1, -2, and -3 belong:

- Tunnel Type = GRE (value = 10)
- Tunnel Medium Type = IP (value = 1)
- Tunnel Private Group ID = 2

The RADIUS server returns the above attributes for all wireless users it authenticates from network-1, -2, and -3. The SmartPath AP uses the combination of returned RADIUS attributes to assign users to the user group 2 ("employee-net"). It does not use them to create a GRE tunnel, which the tunnel type attribute might lead you to think.

When there is more traffic than available bandwidth, the SmartPath AP applies the "voice" policy. It performs strict forwarding for voice and uses a WRR scheduling discipline for directing streaming media and data traffic to queues to await forwarding. The QoS configuration is complete.

11.7 Loading a Bootstrap Configuration

As explained in Section 10.3, SmartPathOS Configuration File Types, a bootstrap config file is typically a small set of commands to which a SmartPath AP can revert when the configuration is reset or if the SmartPath AP cannot load its current and backup configs. If you do not define and load a bootstrap config, the SmartPath AP reverts to the default config in these situations, which can lead to two potential problems:

- If both the current and backup configs fail to load on a SmartPath AP acting as a mesh point in a hard-to-reach location—such as a ceiling crawlspace—the SmartPath AP would revert to the default config. Because a mesh point needs to join a cluster before it can access the network and the default config does not contain the cluster settings that the mesh point needs to join the cluster, an administrator would need to crawl to the device to make a console connection to reconfigure the SmartPath AP.
- If the location of a SmartPath AP is publicly accessible, someone could press the reset button on the front panel of the device to return the configuration to its default settings, log in using the default login name and password (admin, blackbox), and thereby gain complete admin access.

NOTE: You can disable the ability of the reset button to reset the configuration by entering this command:

```
no reset-button reset-config-enable
```

A bootstrap configuration can help in both of these situations. For the first case, a bootstrap config with the necessary cluster membership settings can allow the SmartPath AP to connect to the network and thereby become accessible over the network for further configuring. For the second case, a bootstrap config with a number of obstacles such as a hard-to-guess login name and password and a disabled access subinterface can make the firmware inaccessible and the device unusable.

SmartPath AP-1 and -2 are in locations that are not completely secure. SmartPath AP-3 is a mesh point in a fairly inaccessible location. To counter theft of the first two SmartPath APs and to avoid the nuisance of physically accessing the third SmartPath AP, you define a bootstrap config file that addresses both concerns and load it on the SmartPath APs.

Step 1: Define the bootstrap config on SmartPath AP-1.

1. Make a serial connection to the console port on SmartPath AP-1, log in, and load the default config.

```
load config default
```

```
reboot
```

You do not want the bootstrap config to contain any of your previously defined settings from the current config. Therefore, you load the default config, which has only default settings. When you begin with the default config and enter the commands that define the bootstrap config, the bootstrap config will have just those commands and the default config settings.

2. Confirm the reboot command, and then, when you are asked if you want to use the Black Box Initial Configuration Wizard, enter no.

3. Log in using the default user name admin and password blackbox.

4. Define admin login parameters for the bootstrap config that are difficult to guess.

```
admin root-admin Cwb12o11siNIm8vhD2hs password 8wDamKC1Lo53Ku71
```

You use the maximum number of alphanumeric characters for the login name (20 characters) and password (32 characters). By mixing uppercase and lowercase letters with numbers in strings that do not spell words or phrases, you make the login much harder to guess.

5. Leave the various interfaces in their default up or down states.

By default, the wifi0 and wifi0.1 interfaces are down, but the mgt0, eth0, wifi1, and wifi1.1 subinterfaces are up. The cluster members need to use wifi1.1, which is in backhaul mode, so that SmartPath AP-3 can rejoin cluster1 and, through cluster1, access DHCP and DNS servers to regain network connectivity. (By default, mgt0 is a DHCP client.) You leave the eth0 interface up so that Cluster-1 and Cluster-2 can retain an open path to the wired network. However, with the two interfaces in access mode—wifi0 and wifi0.1— in the down state, none of the SmartPath APs will be able provide network access to any wireless clients. Wireless clients cannot form associations through wifi1.1 nor can a computer attach through the eth0 interface—because it is also in backhaul mode—and obtain network access through the mesh.

6. Define the cluster settings so that any of the three SmartPath APs using the bootstrap config can rejoin the grid.

```
cluster cluster1
```

```
cluster cluster1 password s1r70ckH07m3s
```

```
interface mgt0 cluster cluster1
```

When a SmartPath AP boots up using the bootstrap config, it can rejoin cluster1 because the configuration includes the cluster name and password and binds the mgt0 interface to the cluster. This is particularly useful for SmartPath AP-3 because it is a mesh point and can only access the wired network after it has joined the cluster. It can then reach the wired network through either of the portals, SmartPath AP-1 or SmartPath AP-2.

7. Save the configuration as a bootstrap config.

```
save config running bootstrap
```

If anyone resets the current configuration, the SmartPath AP will load this bootstrap config and thwart any thief from accessing the configuration and any wireless client from accessing the network.

NOTE: Be careful to remember the login name and password defined in a bootstrap config file. If they become lost or forgotten, you must obtain a one-time login key from Black Box technical support. To get the key, you must already have had a support contract in place. The first one-time login key is free. After that, there is a small handling fee for each additional key.

Step 2: Save the bootstrap config to a TFTP server.

1. Check the configurations to make sure the settings are accurate.

```
show config bootstrap
```

Check that the settings are those you entered in the previous step for the bootstrap config.

```
show config backup
```

NOTE: The backup config is the previous current config. This is the configuration that has all your previously defined settings.

2. Return to the previous current config.

```
load config backup
```

```
reboot
```

3. When SmartPath AP-1 finishes rebooting, log back in using the login parameters you set in Section 11.1 (mwebster, 3fF8ha).

4. Check that the current config is the same as your previous current config.

```
show config current
```

5. Save the file as bootstrap-cluster1.txt to the root directory of your TFTP server running on your management system at 10.1.1.31, an address received by the same DHCP server and in the same subnet as the SmartPath AP addresses.

```
save config bootstrap tftp://10.1.1.31:bootstrap-cluster1.txt
```

Step 3: Load the bootstrap config file on SmartPath AP-2 and SmartPath AP-3.

1. Make a serial connection to the console port on SmartPath AP-2 and log in.

2. Upload the bootstrap-cluster1.txt config file from the TFTP server to SmartPath AP-2 as a bootstrap config.

```
save config tftp://10.1.1.31:bootstrap-cluster1.txt bootstrap
```

3. Check that the uploaded config file is now the bootstrap config.

```
show config bootstrap
```

4. Repeat the procedure to load the bootstrap config on SmartPath AP-3. The bootstrap configs are now in place on all three SmartPath APs.

11.8 Command Line Interface (CLI) Commands for Examples

This section includes all the CLI commands for configuring the SmartPath APs in the previous examples. The CLI configurations are presented in their entirety (without explanations) as a convenient reference, and—if you are reading this guide as a PDF—as an easy way to copy and paste the commands. Simply copy the blocks of text for configuring the SmartPath APs in each example and paste them at the command prompt.

NOTE: The following sections omit optional commands, such as changing the login name and password, and commands used to check a configuration.

11.8.1 Commands for Example 1

Enter the following commands to configure the SSID "employee" on the single SmartPath AP in Example 1 in Section 11.1:

```
ssid employee

ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3

interface wifi0.1 ssid employee

save config
```

11.8.2 Commands for Example 2

Enter the following commands to configure three SmartPath APs as members of "cluster1" in Example 2 in Section 11.2:

SmartPath AP-1:

```
cluster cluster1

cluster cluster1 password s1r70ckH07m3s

interface mgt0 cluster cluster1

save config
```

SmartPath AP-2:

```
ssid employee

ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3

interface wifi0.1 ssid employee

cluster cluster1

cluster cluster1 password s1r70ckH07m3s

interface mgt0 cluster cluster1

save config
```

SmartPath AP-3:

```
ssid employee
ssid employee security protocol-suite wpa-auto-psk ascii-key N38bu7Adr0n3
interface wifi0.1 ssid employee
cluster cluster1
cluster cluster1 password s1r70ckH07m3s
interface mgt0 cluster cluster1
save config
```

11.8.3 Commands for Example 3

Enter the following commands to configure the cluster members to support IEEE 802.1X authentication in Example 3 in Section 11.3:

SmartPath AP-1:

```
aaa radius-server first 10.1.1.10 shared-secret s3cr3741n4bl0X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

SmartPath AP-2:

```
aaa radius-server first 10.1.1.10 shared-secret s3cr3741n4bl0X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

SmartPath AP-3:

```
aaa radius-server 10.1.1.10 shared-secret s3cr3741n4bl0X
ssid employee security protocol-suite wpa-auto-8021x
save config
```

11.8.4 Commands for Example 4

Enter the following commands to configure the cluster members to apply QoS to voice, streaming media, and data traffic in Example 4 in Section 11.4:

SmartPath AP-1:

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
```

```
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For SmartPath APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For SmartPath APs supporting IEEE 802.11a/b/g/n:

```
      qos policy voice qos 6 strict 512 0
      qos policy voice qos 5 wrr 20000 90
      qos policy voice qos 3 wrr 1000000 60
user-profile employee-net qos-policy voice attribute 2
save config
```

SmartPath AP-2:

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For SmartPath APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For SmartPath APs supporting IEEE 802.11a/b/g/n:

```
qos policy voice qos 6 strict 512 0
qos policy voice qos 5 wrr 20000 90
```

```
qos policy voice qos 3 wrr 1000000 60
user-profile employee-net qos-policy voice attribute 2
save config
```

SmartPath AP-3:

```
qos classifier-map oui 00:12:3b qos 6
service mms tcp 1755
service smtp tcp 25
service pop3 tcp 110
qos classifier-map service mms qos 5
qos classifier-map service smtp qos 3
qos classifier-map service pop3 qos 3
qos classifier-profile employee-voice mac
qos classifier-profile employee-voice service
qos classifier-profile eth0-voice mac
qos classifier-profile eth0-voice service
ssid employee qos-classifier employee-voice
interface eth0 qos-classifier eth0-voice
```

For SmartPath APs supporting IEEE 802.11a/b/g:

```
qos policy voice qos 5 wrr 20000 90
qos policy voice qos 3 wrr 54000 60
```

For SmartPath APs supporting IEEE 802.11a/b/g/n:

```
qos policy voice qos 6 strict 512 0
      qos policy voice qos 5 wrr 20000 90
      qos policy voice qos 3 wrr 1000000 60
user-profile employee-net qos-policy voice attribute 2
save config
```

11.8.5 Commands for Example 5

Enter the following commands to create bootstrap config files and load them on the cluster members in Example 5 in Section 11.5:

bootstrap-security.txt

```
admin root-admin Cwb12o11siNIm8vhD2hs password 8wDamKC1Lo53Ku71
cluster cluster1
cluster cluster1 password s1r70ckH07m3s
interface mgt0 cluster cluster1
```

SmartPath AP-1

```
save config tftp://10.1.1.31:bootstrap-security.txt bootstrap
```

```
        show config bootstrap
```

SmartPath AP-2

```
        save config tftp://10.1.1.31:bootstrap-security.txt bootstrap
        show config bootstrap
```

SmartPath AP-3

```
        save config tftp://10.1.1.31:bootstrap-meshpoint.txt bootstrap
        show config bootstrap
```

12. Traffic Types

This is a list of all the types of traffic that might be involved with a SmartPath AP and SmartPath EMS VMA deployment. If a firewall lies between any of the sources and destinations listed below, make sure that it allows these traffic types.

Table 12-1. Traffic supporting network access for wireless clients.

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
Active Directory	SmartPath AP RADIUS server mgt0 interface	Active Directory domain controller or global catalog server	6 TCP	1024-65535	139, and 445 or 3268	Required for a SmartPath AP RADIUS server to contact a domain controller on Port 445 or a global catalog server on Port 3268
			17 UDP	1024-65535	389	
DHCP	Unregistered wireless client	SmartPath AP Wi-Fi subinterface in access mode	17 UDP	68	67	Required for captive Web portal functionality
DNS	Unregistered wireless client	SmartPath AP Wi-Fi subinterface in access mode	17 UDP	53, or 1024–65535	53	Required for captive Web portal functionality
GRE	SmartPath AP mgt0 interface	SmartPath AP mgt0 interface	47 GRE	N.A.	N.A.	Required to support DNX* and Layer 3 roaming between members of different clusters
HTTP	Unregistered wireless client	SmartPath AP Wi-Fi subinterface in access mode	6 TCP	1024–65535	80	Required for captive Web portal functionality
HTTPS	Unregistered wireless client	SmartPath AP Wi-Fi subinterface in access mode	6 TCP	1024–65535	443	Required for captive Web portal functionality using a server key
IKE	SmartPath AP VPN client mgt0 interface	SmartPath AP VPN server mgt0 interface	17 UDP	500 and 4500 for NAT—Traversal	500 and 4500 for NAT—Traversal	Required for SmartPath AP VPN clients to connect to SmartPath AP VPN servers
IPsec ESP	SmartPath AP VPN client or server mgt0 interface	SmartPath AP VPN server or client mgt0 interface	50 ESP	N.A.	N.A.	Required for IPsec VPN traffic to flow between SmartPath AP VPN clients and servers
IPsec ESP with NAT—Traversal enabled	SmartPath AP VPN client or server mgt0 interface	SmartPath AP VPN server or client mgt0 interface	17 UDP	4500	4500	Required for VPN traffic to flow when a NAT device is detected in-line
LDAP	SmartPath AP RADIUS server mgt0 interface	OpenLDAP server	6 TCP	1024–65535	389	Required for a SmartPath AP RADIUS server to contact an OpenLDAP server
LDAPS	SmartPath AP RADIUS server mgt0 interface	OpenLDAP server	6 TCP	1024–65535	636	Required for a SmartPath AP RADIUS server to make an encrypted connection to an OpenLDAP server
RADIUS accounting	SmartPath AP mgt0 interface	RADIUS server	17 UDP	1024–65535	1813†	Required to support RADIUS accounting
RADIUS authentication	SmartPath AP mgt0 interface	RADIUS		1024–65535	1812†	Required for 802.1x authentication of users

*DNX = dynamic network extensions

†This is the default destination port number. You can change it to a different port number from 1 to 65535.

Table 12-2. Traffic supporting management of SmartPath APs.

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
CAPWAP*	SmartPath AP mgt0 interface	SmartPath EMS VMA	17 UDP	12222	12222	Required for SmartPath APs to | discover SmartPath EMS VMA and send it alarms, events, reports, traps, and SSH keys; used by SmartPath EMS VMA to upload delta configs to SmartPath APs
Distributed SmartPathOS image download	SmartPath AP mgt0 interface	SmartPath AP mgt0 interface	6 TCP	1024–65535	3007	Required for distributing a SmartPathOS image downloaded to one SmartPath AP from SmartPath EMS VMA and from there to all other
HTTP	Management system	SmartPath EMS VMA MGT port	6 TCP	1024–65535	80	Redirected to HTTPS when accessing the SmartPath EMS VMA and SmartPath EMS Online GUI; used for uploading image files for maps to SmartPath EMS Online
	SmartPath AP mgt0 interface	SmartPath EMS VMA MGT port	6 TCP	1024–65535	80	Used as CAPWAP transport by SmartPath APs connecting to SmartPath EMS VMA and SmartPath EMS Online through HTTP proxy servers; used by SmartPath EMS VMA and SmartPath EMS Online to monitor SmartPath APs and push delta configs
HTTPS	Management system	SmartPath EMS VMA MGT port	6 TCP	1024–65535	443	Required for accessing the SmartPath EMS VMA and SmartPath EMS Online GUI
	SmartPath AP mgt0 interface	SmartPath EMS VMA MGT port	6 TCP	1024–65535	443	Used to upload files—SmartPathOS images, full configs, captive Web portals pages, certificates—from SmartPath EMS VMA and SmartPath EMS Online to SmartPath APs; used for uploading packet captures from SmartPath APs to SmartPath EMS VMA and SmartPath EMS Online
Iperf	mgt0 interface on Iperf client	mgt0 interface on Iperf server	6 TCP	1024–65535	5001†	Required for performing diagnostic testing of network performance
NTP	SmartPath AP mgt0 interface	SmartPath EMS VMA	17 UDP	1024–65535	123	Required for SmartPath AP time synchronization with SmartPath EMS VMA
Remote Sniffer	Admin workstation	SmartPath AP mgt0 interface	6 TCP	1024–65535	2002†	Used when capturing packets on SmartPath AP interfaces
SNMP	SNMP managers	SmartPath AP mgt0 interface	17 UDP	1024–65535	161	Required for SNMP managers to contact SmartPath APs
SNMP traps	SmartPath AP mgt0 interface	SNMP managers	17 UDP	1024–65535	162	Required for sending SNMP traps to configured SNMP managers

*Control and provisioning of wireless access points.

†This is the default destination port number. You can change it to a different port number from 1 to 65535.

Table 12-2 (continued). Traffic supporting management of SmartPath APs.

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
SSHv2	SmartPath AP mgt0 interface	SmartPath EMS VMA	6 TCP	1024–65535	22	Required for a SmartPath EMS VMA to upload files—SmartPath OS images, full configs, captive web portals pages, certificate—to SmartPath APs
TFTP	SmartPath AP mgt0 interface	SmartPath EMS VMA	17 UDP	1024–65535	69	Used for uploading packet capture files from SmartPath APs to SmartPath EMS VMA and for loading SmartPath OS image files from SmartPath EMS VMA to SmartPath

*Control and provisioning of wireless access points.

†This is the default destination port number. You can change it to a different port number from 1 to 65535.

Table 12-3. Traffic supporting device operations.

Service	Source	Destination	Protocol	SRC Port	DST Port	Notes
SmartPath Cooperative Control Messages	SmartPath AP mgt0 interface	SmartPath AP mgt0 interface	17 UDP	3000*	3000*	Required for cluster communications and operates at Layer 3
SmartPath Cooperative Control Messages	SmartPath AP wifi1.1 or eth0 interface	SmartPath AP wifi1.1 or eth0 interface	N.A.	N.A.	N.A.	Required for cluster communications and operates at the Logical Link Control (LLC) sublayer of Layer 2
AeroScout Reports	AeroScout engine	SmartPath AP mgt0 interface	17 UDP	1024–65535	1144	Required to report tracked devices to an AeroScout engine
DHCP	SmartPath AP mgt0 interface	DHCP server	17 UDP	68	67	By default, a SmartPath AP gets its IP address through DHCP.
Ekahau	Ekahau Positioning Engine (EPE)	SmartPath AP mgt0 interface	17 UDP	1024–65535	8552, 8553, 8554	Required for SmartPath APs to communicate with EPE
NTP	SmartPath AP mgt0 interface or SmartPath EMS VMA MGT port	NTP server	6 TCP	1024–65535	123	Required for time synchronization with an NTP server
SMTP	SmartPath EMS VMA MGT port	SMTP server	6 TCP	1024–65535	25*	Required for the SmartPath EMS VMA to send e-mail alerts to administrators
SSHv2	Management system	SmartPath AP mgt0 interface or SmartPath EMS VMA MGT port	6 TCP	1024–65535	22	Used for secure network access to the SmartPath AP or SmartPath EMS VMA CLI, and (SCP) for uploading files to and downloading files from SmartPath APs
syslog	SmartPath AP mgt0 interface	syslog server	17 UDP	1024–65535	514	Required for remote logging to a syslog server
Telnet	Management system	SmartPath AP mgt0 interface	6 TCP, 17 UDP	1024–65535	23	Used for unsecured network access to the SmartPath AP CLI
TFTP	TFTP server or mgt0	SmartPath AP mgt0 or TFTP server	17 UDP	1024–65535	69	Used for uploading files to SmartPath APs and downloading files from them

* This is the default port number. You can change it to a different port number from 1024 to 65535.

Appendix. Country Codes

When the region code on a SmartPath AP is preset as "world," you must set a country code for the location where you intend to deploy the SmartPath AP. This code determines the radio channels and power settings that the SmartPath AP can use when deployed in that country. For SmartPath APs intended for use in the United States, the region code is preset as

"FCC"—for "Federal Communications Commission"—and the country code is preset for the United States. You can see the region code in the output of the show boot-param command.

To set a country code when the region is "world", enter the following command, in which number is the appropriate country code number: boot-param country-code number.

NOTE: Be sure to enter the correct country code. An incorrect entry might result in illegal radio operation and cause harmful interference to other systems.

To apply radio settings for the updated country code, reboot the SmartPath AP by entering the reboot command.

To see a list of the available channels available for the country code that you have set on the SmartPath AP, enter the following command: show interface { wifi0 | wifi1 } channel. For example, the output for the show interface wifi0 channel command on a SmartPath AP whose region code is FCC and country code is 840 (United States) shows that Channels 1 through 11 are available. If a channel does not appear in this list, you cannot configure the radio to use it.

The following list of country codes is provided for your convenience.

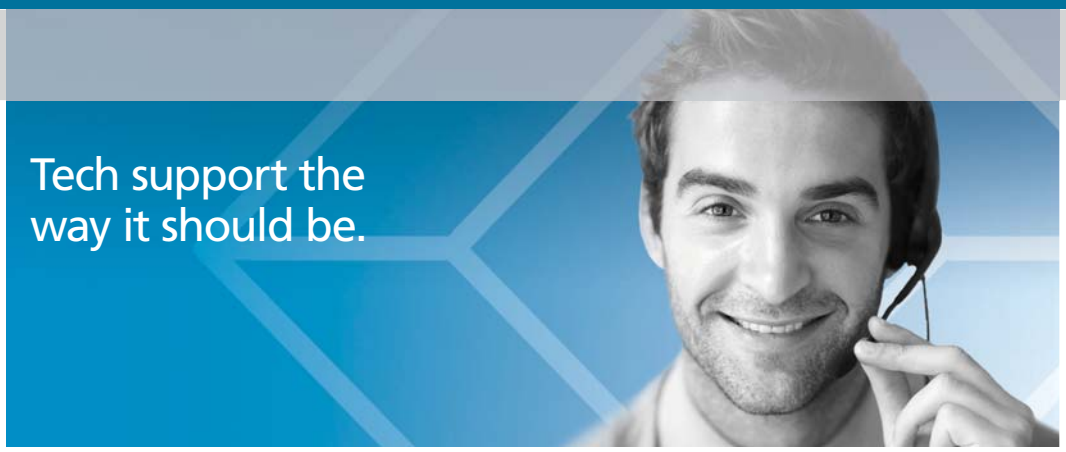
Table A-1. Countries and country codes.

Country	Country Code	Country	Country Codes	Country	Country Code	Country	Country Code
Albania	8	Algeria	12	Argentina	32	Armenia	51
Australia	36	Austria	40	Azerbaijan	31	Bahrain	48
Belarus	112	Belgium	56	Belize	84	Bolivia	68
Bosnia and Herzergovina	70	Brazil	76	Brunei Darussalem	96	Bulgaria	100
Canada	124	Chile	152	China	156	Colombia	170
Costa Rica	188	Croatia	191	Cyprus	196	Czech Republic	203
Denmark	208	Dominican Republic	214	Ecuador	218	Egypt	818
El Salvador	222	Estonia	233	Faroe Islands	234	Finland	246
France	250	Georgia	268	Germany	276	Greece	300
Guatemela	320	Honduras	340	Hong Kong	344	Hungary	348
Iceland	352	India	356	Indonesia	360	Iran	364
Iraq	`368	Ireland	372	Israel	376	Italy	380
Jamaica	388	Japan	392	Japan 1 (JP1)	393	Japan2 (JP0)	394
Japan3 (JP1-1)	395	Japan4 (JE1)	396	Japan5 (JE2)	397	Japan6 (JP6)	399
Japan7 (J7)	4007	Japan8 (J8)	4008	Japan9 (J9)	4009	Japan10 (J10)	4010

Table A-1 (continued). Countries and country codes.

Country	Country Code	Country	Country Codes	Country	Country Code	Country	Country Code
Japan 11 (J11)	4011	Japan12 (J12)	4012	Japan13 (J13)	4013	Japan14 (J14)	4014
Japan 15 (J15)	4015	Japan16 (J16)	4016	Japan17 (J17)	4017	Japan17 (J17)	4017
Japan 18 J18)	4018	Japan19 (J19)	4019	Japan20 (J20)	4020	Japan21 (J21)	4021
Japan22 (J22)	4022	Japan23 (J23)	4023	Japan24 (J24)	4024	Jordan	400
Kazakhstan	398	Kenya	404	Korea (North Korea)	408	Korea (South Korea, ROC)	410
Korea (South Korea, ROC2)	411	Korea (South Korea, ROC3)	412	Kuwait	414	Latvia	428
Lebanon	422	Libya	434	Liechtenstein	438	Lithuania	440
Luxembourg	442	Macau	446	Macedonia the former Yugoslav Republic of Macedonia)	807	Malaysia	458
Malta	470	Mauritius	480	Mexico	484	Monaco (Principality of Monaco)	492
Morocco	504	Netherlands	528	New Zealand	554	Nicaragua	558
Norway	578	Oman	512	Pakistan (Islamic Republic of Pakistan)	586	Panama	591
Paraguay	600	Peru	604	Phillippines (Republic of the Phillippines)	608	Poland	616
Portugal	620	Puerto Rico	630	Qatar	634	Romania	642
Russia	643	Saudi Arabia	682	Singapore	702	Slovakia (Slovak Republic)	703
Slovenia	705	South Africa	710	Spain	724	Sri Lanka	144
Sweden	752	Switzerland	756	Syria	760	Taiwan	158
Thailand	764	Trinidad and Tobago	780	Tunisia	788	Turkey	792
U.A.E.	784	Ukraine	804	United Kingdom	826	United States	840
United States (Public Safety: FCC49)	842	Uruguay	858	Uzbekistan	860	Vietnam	704
Yemen	887	Zimbabwe	716	—	—	—	—

Black Box Tech Support: FREE! Live. 24/7.



Great tech support is just 30 seconds away at 724-746-5500 or blackbox.com.

BLACK BOX®
NETWORK SERVICES

About Black Box

Black Box Network Services is your source for an extensive range of networking and infrastructure products. You'll find everything from cabinets and racks and power and surge protection products to media converters and Ethernet switches all supported by free, live 24/7 Tech support available in 30 seconds or less.

LWN602A, rev. 4