4

Wireless Local Area Networks (WLANs)

Contents

Overview

A wireless LAN (WLAN) is a LAN that uses a wireless medium; typically it provides wireless stations a connection to a private LAN, the Internet, or both. The WLAN might include multiple radio ports (RPs), each of which is identified by an individual basic service set identifier (BSSID), but supports the same service set identifier (SSID). Stations associated to one RP can roam to another RP that provides access to the same WLAN (shares the same SSID).

By default, all RP radios adopted by a ProCurve Wireless Edge Services xl Module support all WLANs that you enable on that module. In “Configuration Options: Normal Versus Advanced Mode” on page 4-4, you will learn about how the module assigns these WLANs to BSSIDs on each RP radio. (This process may affect which WLANs operate in open and which in closed system.) Mastering these concepts will help you better design your network, and is particularly important when you plan to configure more than four WLANs.

The WLAN defines settings that control the wireless communications. These range from the method that wireless stations must use to authenticate themselves to the encryption algorithms that protect data to the parameters by which stations compete for access to the wireless medium. When you configure the WLAN, you must choose these settings, as described in “Configuring a WLAN” on page 4-26 and “Traffic Management (QoS)” on page 4-90.

Because all RPs in a WLAN must agree upon settings, the Wireless Edge Services xl Module, as a single wireless controller, greatly simplifies configuration. After you configure and enable a WLAN on the module, the module can automatically configure these settings on all adopted RPs.

The RPs send and receive traffic in these WLANs. The traffic that they receive from wireless stations, they forward (via Radio Port virtual LANs [VLANs]) to the Wireless Edge Services xl Module, which assigns this traffic to a VLAN. The module can:

- assign all traffic from a WLAN to the same VLAN (manual VLAN assignment)
- assign traffic to different VLANs depending on the identity of the user that sent the traffic (dynamic VLAN assignment)

You will learn about both of these options in “VLAN Assignment” on page 4-81.

Note that, instead of assigning traffic to a VLAN, the module can forward it over a Generic Routing Encapsulation (GRE) tunnel.

Configuration Options: Normal Versus Advanced Mode

When the Wireless Edge Services xl Module deploys a WLAN's configuration to an RP, it assigns the SSID associated with that WLAN to a BSSID on the RP's radio (or radios). You can configure the module to assign WLANs to RPs in one of two modes: normal or advanced. In normal configuration mode, the Wireless Edge Services xl Module handles mapping WLANs to BSSIDs on all RP radios. In advanced mode, you must manually assign WLANs to radios and to BSSIDs.

Normal configuration is the generally recommended option. However, you can use advanced configuration to restrict certain WLANs to certain areas, to select which WLANs the RPs announce, or to increase the number of WLANs supported by your network.

The following sections describe how to use normal mode and advanced mode configuration. The instructions assume that you have already configured all of the WLANs for your network and that you are ready to enable them.

Normal Mode Configuration

You almost always use normal mode configuration. In this mode, the Wireless Edge Services xl Module OS automatically adds enabled WLANs to the default configuration for adopted radios, matching each WLAN's SSID to a particular BSSID. Whenever the module adopts an RP, it deploys this configuration to the RP.

In normal mode configuration, a Wireless Edge Services xl Module (and its RPs) can support up to 16 WLANs.

Why Use Normal Mode

Normal mode configuration is simple to use and suitable for most environments. The deployment is entirely transparent: you simply enable WLANs, and as soon as an RP is adopted by the module, that RP begins to support those WLANs.

Unless you need more than 16 WLANs or have a pressing reason to force certain RPs to support certain WLANs only, you should not deviate from normal mode.

Enabling WLANs Using Normal Mode

In normal mode, to configure and activate WLANs, you complete these steps:

1. Configure the SSID, VLAN, and other options for each WLAN that you want to include in your network. See "Configuring a WLAN" on page 4-26 for instructions on how to do so.
2. On the **Network Setup** > **Radio Setup** screen, select the WLANs and click **Enable**.

The Wireless Edge Services xl Module then automatically implements this process:

1. It assigns the SSID for WLAN 1 to the *first* BSSID on every radio on every adopted RP.
2. It assigns the SSID for WLAN 2 to the *second* BSSID on every RP radio. In our example, it assigns SSID B to BSSID 2.
3. This process continues for up to *four* WLANs.

The figures below illustrate this process.

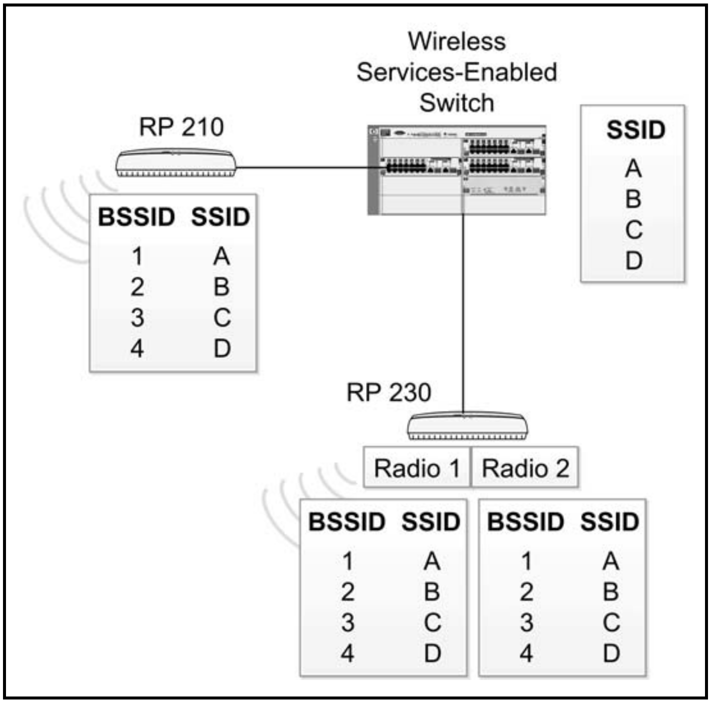
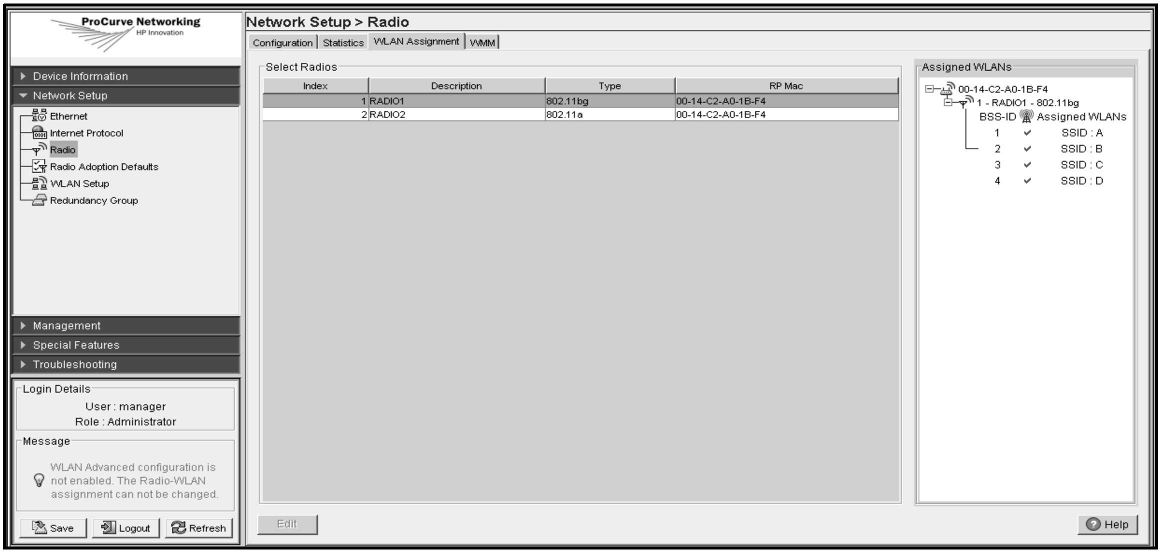


Figure 4-1. Assigning WLANs (Normal)

Figure 4-2 shows the screen in which you can verify that radios have received the WLAN assignment.



Network Setup > Radio

Login Details
User : manager
Role : Administrator

Message
WLAN Advanced configuration is not enabled. The Radio-WLAN assignment can not be changed.

Select Radios

Index	Description	Type	RP Mac
1	RADIO1	802.11bg	00-14-C2-A0-1B-F4
2	RADIO2	802.11a	00-14-C2-A0-1B-F4

Assigned WLANs

00-14-C2-A0-1B-F4
1 - RADIO1 - 802.11bg

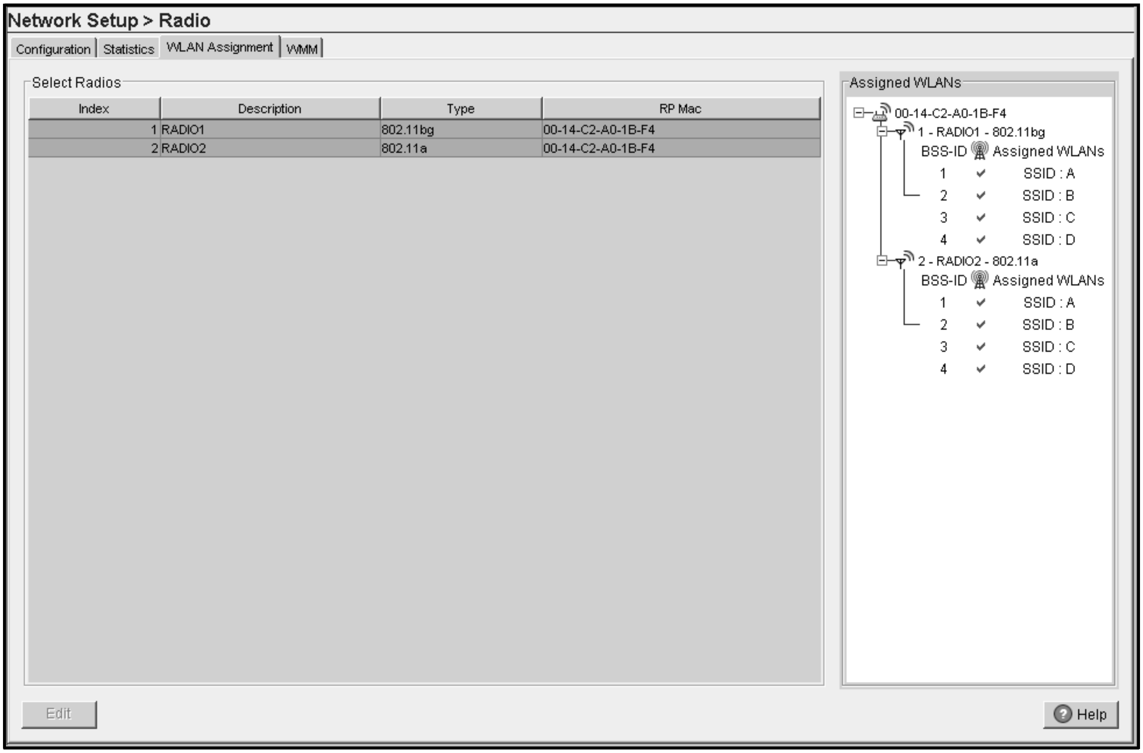
BSS-ID		Assigned WLANs
1	✓	SSID : A
2	✓	SSID : B
3	✓	SSID : C
4	✓	SSID : D

Figure 4-2. Assigning WLANs to a Radio (Normal)

To view the screen in Figure 4-2, select **Network Setup** > **Radio** and click the **WLAN Assignment** tab. Select a radio, and information is displayed in the area in the right of the screen, called **Assigned WLANs**.

The **Assigned WLANs** area lists the four BSSIDs on the radio and the SSID (or SSIDs) assigned to each BSSID. View this screen whenever you want to see exactly which WLANs each RP radio in your wireless network supports.

Note that if the RP includes two radios, each WLAN is matched to corresponding BSSIDs on each radio, as shown on the RP 230 in Figure 4-1. Figure 4-3 shows the screen in the Web browser interface in which you can verify that radio 2 has also received the WLAN configuration. (To view the SSID for both radios at the same time, hold down the **Shift** key and select the two.)



Index	Description	Type	RP Mac
1	RADIO1	802.11bg	00-14-C2-A0-1B-F4
2	RADIO2	802.11a	00-14-C2-A0-1B-F4

```
00-14-C2-A0-1B-F4
  1 - RADIO1 - 802.11bg
    BSS-ID  Assigned WLANs
    1   ✓   SSID : A
    2   ✓   SSID : B
    3   ✓   SSID : C
    4   ✓   SSID : D
  2 - RADIO2 - 802.11a
    BSS-ID  Assigned WLANs
    1   ✓   SSID : A
    2   ✓   SSID : B
    3   ✓   SSID : C
    4   ✓   SSID : D
```

Figure 4-3. Assigning WLANs to the Second Radio (Normal)

You must understand that these assignments are constant: WLAN 2 is always assigned to BSSID 2, even if you have not enabled WLAN 1.

Enabling More Than Four WLANs Using Normal Mode

Using normal mode, you can configure and enable up to 16 WLANs, which all adopted RP radios will support. However, because the RPs only support four BSSIDs per radio, the process of assigning WLANs changes slightly when you enable more than four WLANs.

For the four WLANs with the lowest index numbers, the Wireless Edge Services xl Module uses the process described above.

WLANs subsequent to WLAN 4 share the BSSID that the first four WLANs use. For example, in Figure 4-4, SSID E (that for WLAN 5) is mapped to all radios' BSSID 1 along with SSID A (for WLAN 1). SSID F (that for WLAN 6), as well as SSID B, is assigned to the second BSSID, and so on.

As always, if the RP includes two radios, every WLAN is assigned to a BSSID on each.

This process is illustrated in the figures below.

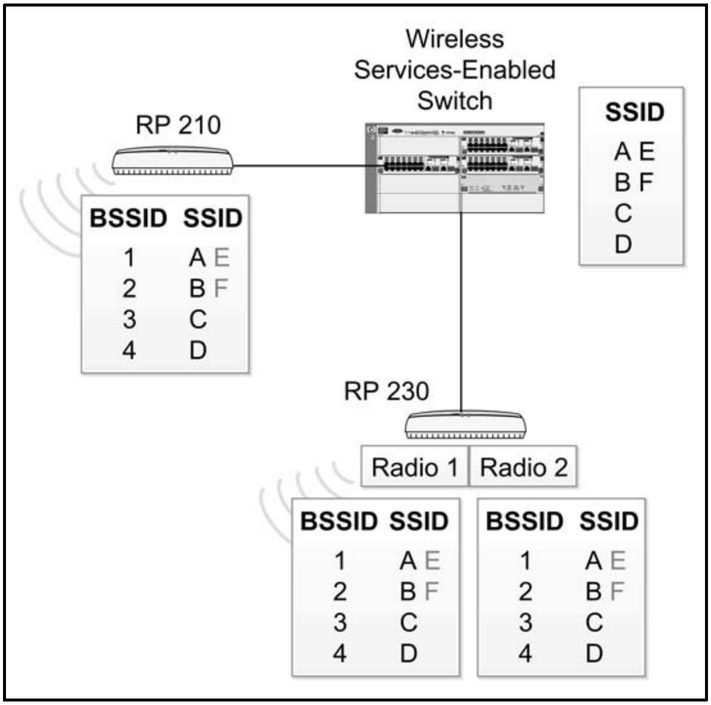
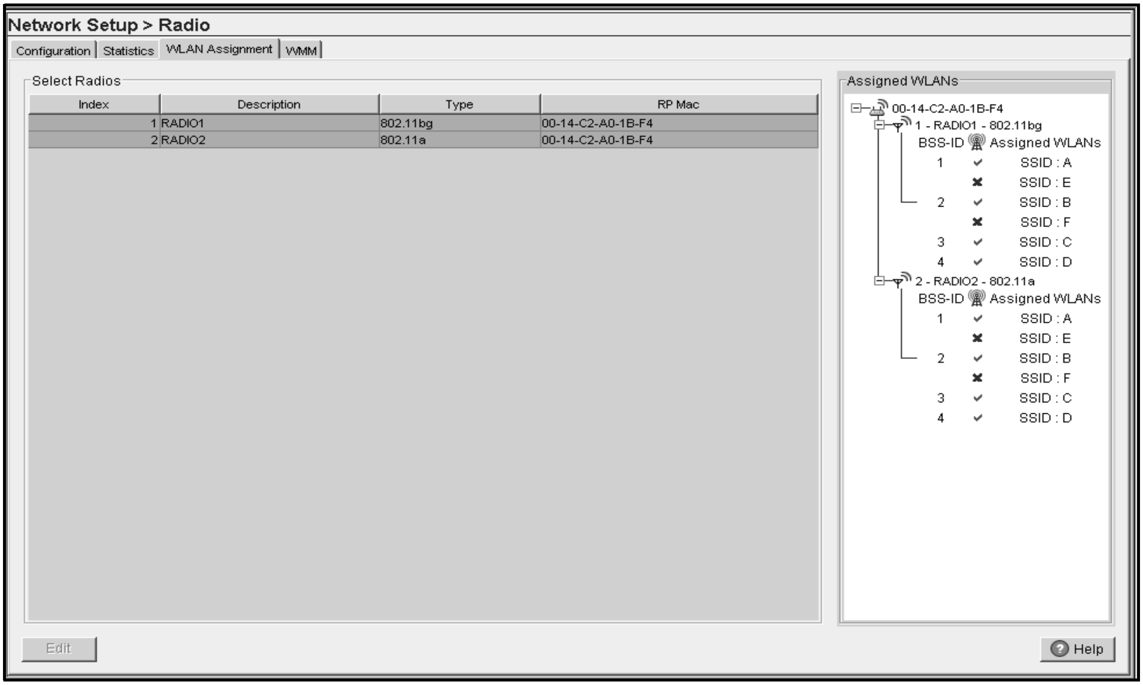


Figure 4-4. Assigning Six WLANs to a Radio (Normal)



Network Setup > Radio

Index	Description	Type	RP Mac
1	RADIO1	802.11bg	00-14-C2-A0-1B-F4
2	RADIO2	802.11a	00-14-C2-A0-1B-F4

```
00-14-C2-A0-1B-F4
  1 - RADIO1 - 802.11bg
    BSS-ID   Assigned WLANs
    1    ✓   SSID : A
         ✗   SSID : E
    2    ✓   SSID : B
         ✗   SSID : F
    3    ✓   SSID : C
    4    ✓   SSID : D
  2 - RADIO2 - 802.11a
    BSS-ID   Assigned WLANs
    1    ✓   SSID : A
         ✗   SSID : E
    2    ✓   SSID : B
         ✗   SSID : F
    3    ✓   SSID : C
    4    ✓   SSID : D
```

Figure 4-5. Viewing Six WLANs Assigned to a Radio (Normal)

RP radios send beacon frames to announce the WLANs that they support. The source of a beacon frame is a BSSID, and each beacon can include only one SSID. Therefore, if you enable more than four WLANs, RPs support all of them, but only announce the first four. The WLAN that each BSSID announces is the primary WLAN—in normal mode, always the WLAN with the lowest index number on that BSSID.

On the **Network Setup** > **Radio** > **WLAN Assignment** screen, a green check mark under the beacon icon indicates the SSID that the RP announces. For example, in Figure 4-5, the RP uses BSSID 1 to send beacons for SSID A, but not for SSID E.

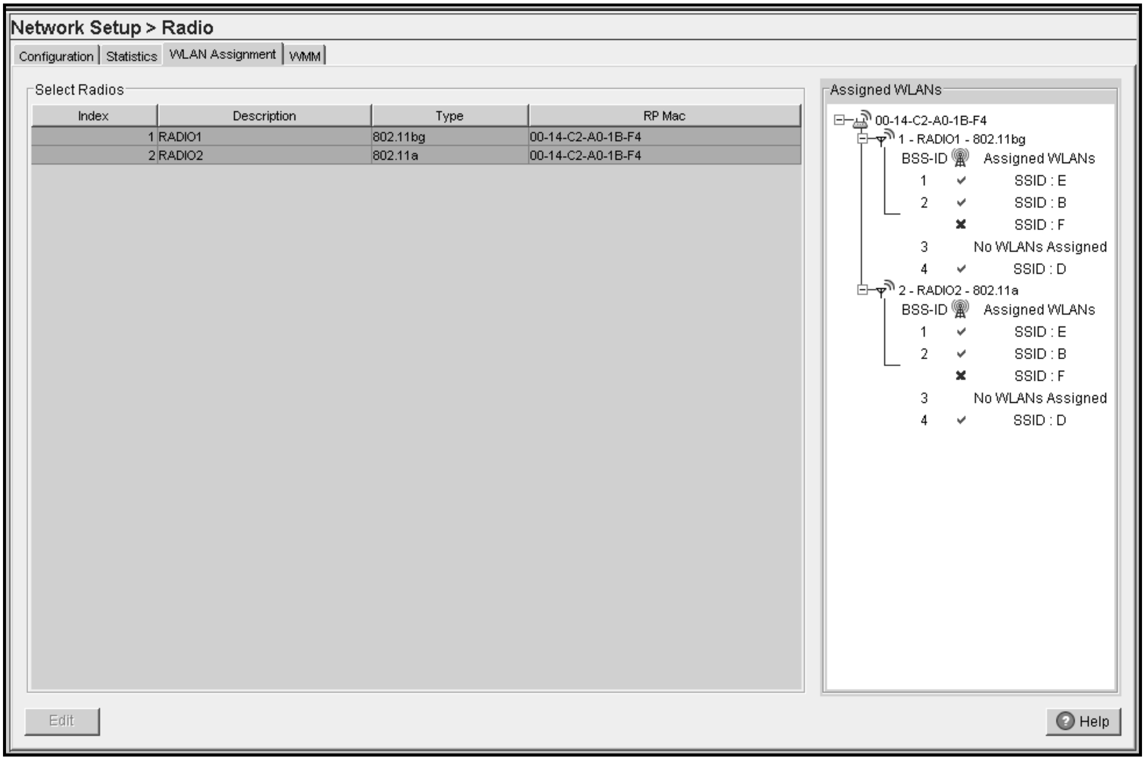
While RPs do not beacon non-primary WLANs, they do respond to probes for them, so wireless stations can connect these WLANs. Some wireless clients require the user to manually input the correct SSID; others automatically send out probes and discover the SSID.

You can configure WLANs 1 through 4 to operate in closed system. In this case, the RP does not announce *any* SSID in beacons from that BSSID. (It does *not* announce the SSID for another WLAN sharing that BSSID.)

In other words, with normal configuration, WLANs 5 through 16 *always* operate in partially closed system. If you want these WLANs to operate in completely closed system, you should disable responses to probe requests. You cannot disable closed system.

See “Enabling Closed System Operations” on page 4-66 to learn more about configuring this features described above.

Finally, again, note that the WLAN assignments are constant. If, for whatever reason, you configure and enable WLANs 2, 4, 5, and 6 instead of 1, 2, 3, and 4, SSID B (WLAN 2) is assigned to BSSID 2, not BSSID 1. SSID F (WLAN 6) is also assigned to BSSID 2, and no SSID is assigned to BSSID 3. (See Figure 4-6.) For this reason, you should generally configure WLANs in order, beginning at index 1.



Network Setup > Radio

Select Radios

Index	Description	Type	RP Mac
1	RADIO1	802.11bg	00-14-C2-A0-1B-F4
2	RADIO2	802.11a	00-14-C2-A0-1B-F4

Assigned WLANs

```
00-14-C2-A0-1B-F4
  1 - RADIO1 - 802.11bg
    BSS-ID    Assigned WLANs
    1    ✓    SSID : E
    2    ✓    SSID : B
         ✗    SSID : F
    3         No WLANs Assigned
    4    ✓    SSID : D
  2 - RADIO2 - 802.11a
    BSS-ID    Assigned WLANs
    1    ✓    SSID : E
    2    ✓    SSID : B
         ✗    SSID : F
    3         No WLANs Assigned
    4    ✓    SSID : D
```

Figure 4-6. Enabling Out of Sequence WLANs

Table 4-1 shows the BSSID to which all 16 WLANs available in normal mode are always assigned.

Table 4-1. WLAN Assignment to BSSID

SSIDs for WLANs	BSSID
1, 5, 9, 13	1
2, 6, 10, 14	2
3, 7, 11, 15	3
4, 8, 12, 16	4

When deciding which WLAN index number to use for a WLAN, keep in mind that this number determines on which BSSID RPs carry that WLAN's traffic. You should generally avoid mixing bulk data and time-sensitive data such as voice on the same BSSID. For example, if stations connect to WLAN 1 to download files from your network's FTP server, you should not configure WLAN 5 for VoWLAN devices.

Advanced Mode Configuration

In advanced mode, you manually control which RP radios support which WLANs. You can even control to which BSSID a WLAN's SSID is assigned, and which of multiple SSIDs that share a BSSID is present in beacons. However, because such precise control adds unnecessary complexity in most environments, this mode is not generally recommended.

In advanced mode configuration, the Wireless Edge Services xl Module supports up to 32 WLANs.

Note

Remember that advanced mode can lead to configuration errors that cut off network access for some users to some WLANs.

Whenever you prevent certain RPs or radios from supporting a WLAN, whether deliberately or not, you open the possibility that roaming wireless stations lose their connection to the network—which can be frustrating.

In addition, because you must manually assign WLANs to radios, advanced mode configuration can be tedious.

Why Use Advanced Mode

Reasons that you might use advanced mode include:

- You want to restrict access to a WLAN to a certain area.

  For example, if a WLAN allows wireless users to access sensitive financial information, you might not want your network to support that WLAN, even protected by encryption, in a public lobby. Advanced mode allows you to assign a WLAN to certain RPs only, so you control where the WLAN exists.

  For example, in Figure 4-7, the administrator has assigned SSID A to the RP in Building 2, and SSIDs B, C, and D to other RPs.

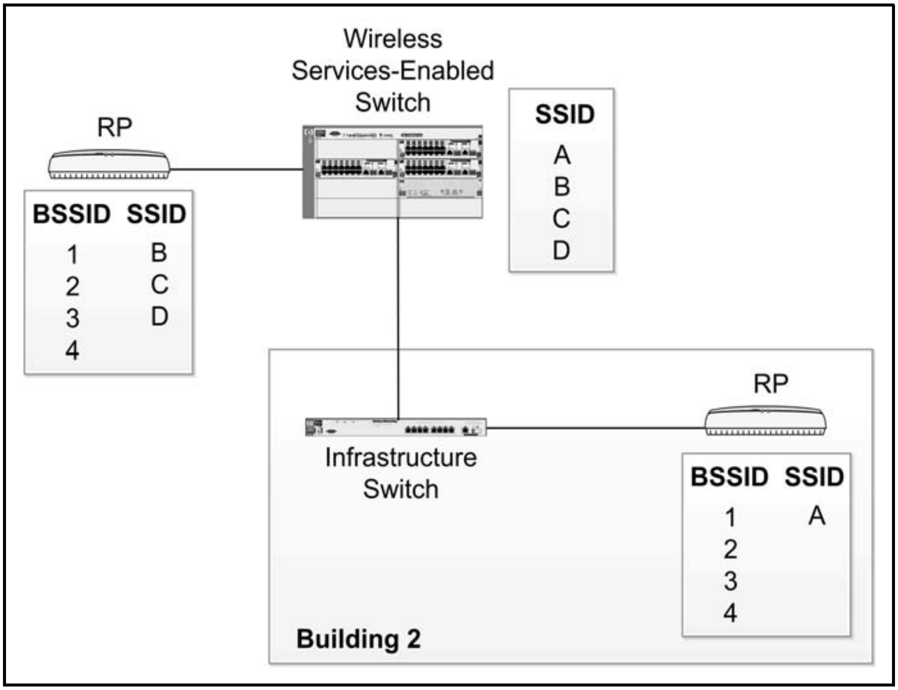


Figure 4-7. Restricting a WLAN to an Area

- Your network includes more than four WLANs, and you want beacons to include one of the WLANs with a higher index number.

  In this case, you should assign the WLAN that you want RPs to beacon as the primary WLAN on a specific BSSID.

- You want your RPs to announce more than four SSIDs.

  While a single RP radio can only beacon four SSIDs, it is possible to customize WLAN assignments so that different RP radios beacon different SSIDs. That is, you can configure certain WLANs as the primary WLANs on some of your organization's RPs, and other WLANs as primary on others. However, such a configuration would mean that certain WLANs are beaconed only in certain areas, which may not be ideal.

- You want more than 16 WLANs in your network.

  With advanced mode configuration, you can configure up to 32 WLANs on the Wireless Edge Services xl Module. However, you cannot assign every WLAN to every RP radio.

  Each RP radio has 4 BSSIDs, and each BSSID supports at most 4 WLANs. So each RP radio can support up to 16 WLANs. If your network includes dual-radio RPs, you can expand the number of WLANs on a single RP from 16 to 32: enable half of the WLANs on one radio and half on the other.

  To provide coverage for different WLANs in different areas, simply assign the WLANs to the correct RPs.

  Providing coverage for more than 16 WLANs in one area is more complicated. You can enable some WLANs on one RP and some on another, and then place the RPs close together. (Remember to set the RPs to non-overlapping channels.) For dual-radio RPs, you can also enable some WLANs on radios operating in 802.11bg and some WLANs on radios operating in 802.11a.

  However, either method could cause connectivity problems and uneven support for WLANs throughout your wireless network. For example, if you use the second method, certain WLANs are supported only by radios operating in 802.11a mode and others only by radios operating in 802.11bg mode. Users might well have difficulty connecting to the desired WLAN.

Enabling WLANs Using Advanced Mode Configuration

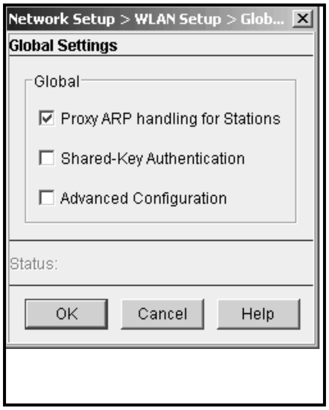
To activate WLANs with advanced mode configuration, complete these steps:

1. Configure WLANs just as you would in normal mode. (Instructions on this process are provided in "Configuring a WLAN" on page 4-26.)

2. Enable advanced configuration:

   a. Select **Network Setup** > **WLAN Setup**.

   b. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed. (See Figure 4-8.)


Network Setup > WLAN Setup > Glob...

Global Settings

Global

☑ Proxy ARP handling for Stations

□ Shared-Key Authentication

□ Advanced Configuration

Status:

Figure 4-8. Global WLAN Settings Screen

   c. Check the **Advanced Configuration** box, and then click the **OK** button.

3. Enable the WLANs.

4. You must now manually assign the WLANs to RP radios. You can do this in two ways:

   - You can manually assign WLANs as a part of a default configuration to be sent to any newly adopted RP.

     In this case, the Wireless Edge Services xl Module deploys the WLAN configuration to all RP radios when they are adopted, as it would in normal mode. However, instead of automatically assigning WLAN 1 to BSSID 1, and so on, the module allows you to select which WLANs are assigned to which BSSIDs.

   - You can manually assign WLANs to specific BSSIDs on specific RP radios.

     In this case, only the specified radios support the WLANs.

You can use both types of advanced configuration in conjunction. For example, you can create a radio adoption default configuration, but then override that configuration for specific RP radios after they are adopted.

For more security, you could leave the radio adoption default configuration empty so that newly adopted RP radios do not immediately support your network's WLANs. After you decide that an RP is authorized, you can manually configure the WLAN assignment on its radio or radios.

The following sections supply more information about these two methods.

Manually Assigning WLANs to the Radio Adoption Default Configuration. Configure the radio adoption default configuration to customize the WLANs that the Wireless Edge Services xl Module sends to all newly adopted radios. This configuration actually divides into two parts—one for 802.11a radios and one for 802.11bg radios.

Note

If you decide to use advanced mode configuration after the module has already adopted RPs, any WLAN assignments established in the radio adoption default configurations will *not* apply to these RPs. You must instead assign the WLANs to specific radios, as explained in "Manually Assigning WLANs to a Specific Radio" on page 4-18.

You should configure the radio adoption default configurations when you want all RPs in your network to support the same WLANs (as they would with normal mode configuration), but for some reason the normal WLAN assignment is inadequate.

For example:

- You have added several WLANs to your network. You now want RP beacons to include one of the new WLANs in preference to one of the old, but the new WLAN has an index number higher than 4.
- You have temporarily disabled several WLANs and you want to spread the others more evenly over the BSSIDs.
- You want to enable more than 16 WLANs, or more than four open system WLANs, on a single RP, so you assign some of the WLANs to 802.11a radios and some to 802.11bg radios.
- You want to configure different WLAN settings for stations that use different 802.11 types.

If you are using advanced mode to restrict one WLAN to a certain area, then you can create WLAN assignments in the radio adoption default configurations for all other, non-restricted WLANs.

For example, to restrict WLAN 1 to one building, you will explicitly assigned that WLAN to RPs in that building, as described in "Manually Assigning WLANs to a Specific Radio" on page 4-18. All other RPs in the wireless network should support WLANs 2 through 5. You create a default configuration for both types of radios (802.11a and 802.11bg), in which you assign these WLANs.

Figure 4-9 displays an environment such as this. This figure also shows the option of enabling SSID A (WLAN 1) on the default configuration, but having SSID E (WLAN 5) be the primary WLAN. (Stations in WLAN 1 can then roam into areas in which WLAN 1 operates in closed system.) In this example, WLAN 1 is less a restricted WLAN than a WLAN that is primarily used by employees in one area.

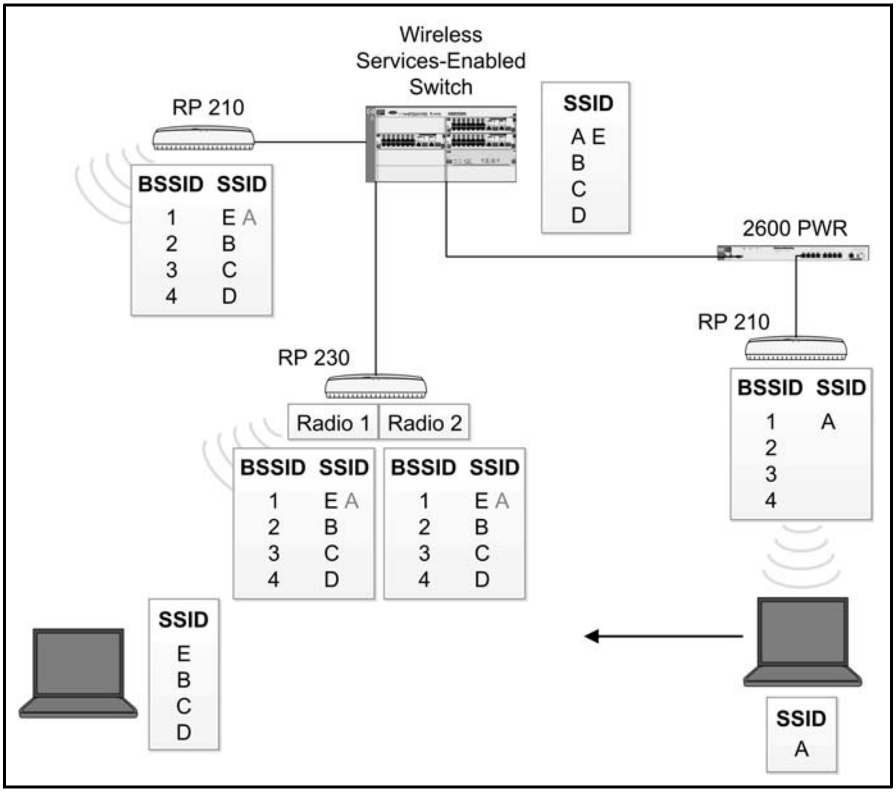


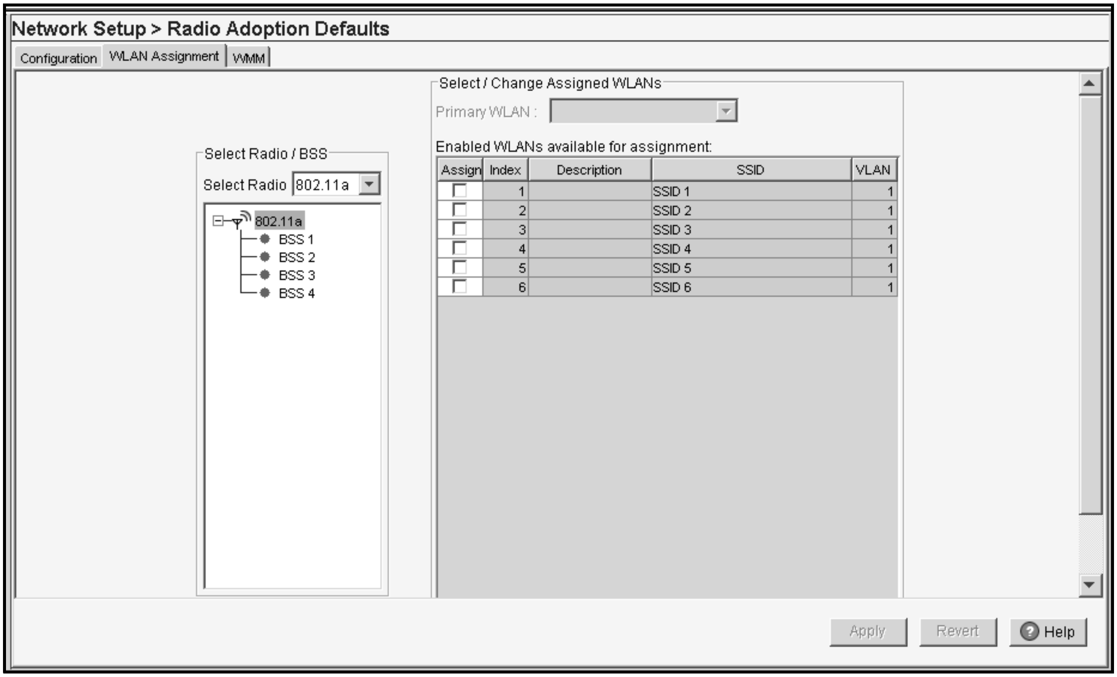
Figure 4-9. Configuring an Area-Specific WLAN

Note

Depending on whether you enable WLANs or advanced mode configuration first, the radio adoption configuration begins with either the normal WLAN assignment or an empty WLAN assignment. Leaving the WLAN assignment in the default configurations empty is not necessarily undesirable: it can increase security. However, you should be aware that in this case newly adopted radios will not support WLANs until you manually configure them to do so.

To modify the default configuration using advanced mode, complete these steps:

1. Select **Network Setup** > **Radio Adoption Defaults** and click the **WLAN Assignment** tab.



Network Setup > Radio Adoption Defaults

Primary WLAN :

Select Radio 802.11a

Enabled WLANs available for assignment:

Assign	Index	Description	SSID	VLAN
□	1		SSID 1	1
□	2		SSID 2	1
□	3		SSID 3	1
□	4		SSID 4	1
□	5		SSID 5	1
□	6		SSID 6	1

Figure 4-10. Customizing WLAN Assignment for the Radio Adoption Default (Advanced Mode)

2. Choose the radio type from the **Select Radio** drop-down menu.

Note

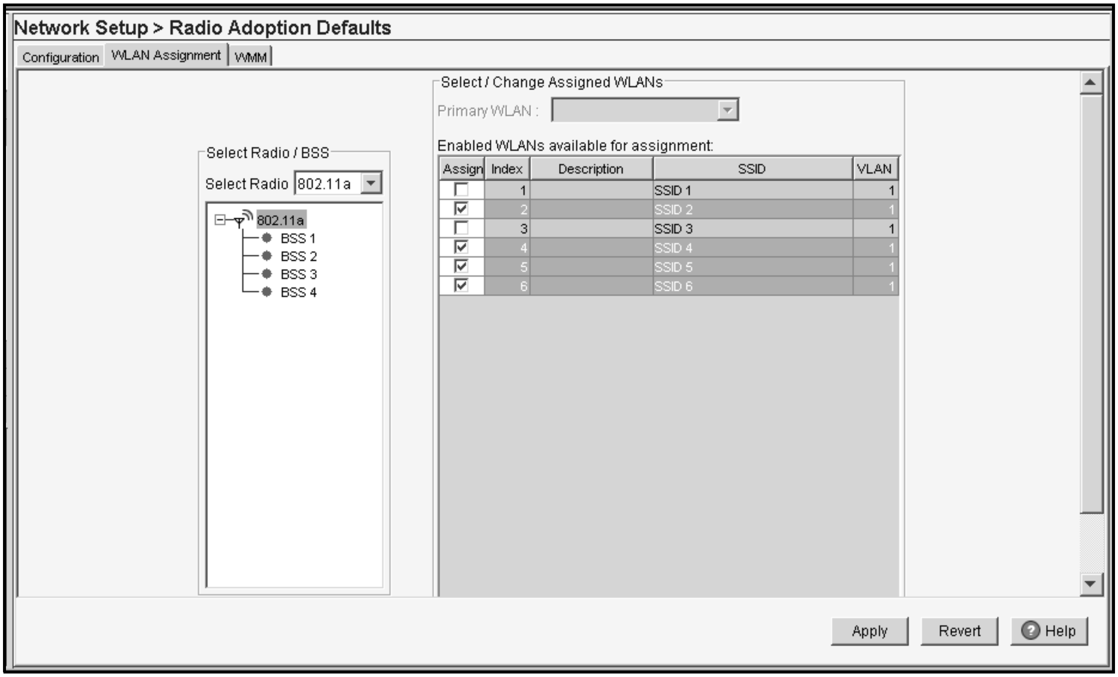
If your network includes radios of both types, you should remember to configure a default WLAN assignment for each. Typically, these assignments should match.

You can assign WLANs to the radio as a whole or to individual BSSIDs.

3. Check the **Assign** box for each WLAN that you want to assign to the radio, and then click the **Apply** button.

4. If you want to assign a specific WLAN to a specific BSSID number, or if you want to choose the primary WLAN, complete steps 5 through 8.

5. Select a BSSID from one of the four listed under the radio. Check the **Assign** box for each WLAN that you want to assign to this BSSID. (You can choose up to four. Generally, but not always, you should fill all four BSSIDs before you assign multiple WLANs to a BSSID.)


Network Setup > Radio Adoption Defaults

Select Radio: 802.11a

Primary WLAN :

Enabled WLANs available for assignment:

Assign	Index	Description	SSID	VLAN
☐	1		SSID 1	1
☑	2		SSID 2	1
☐	3		SSID 3	1
☑	4		SSID 4	1
☑	5		SSID 5	1
☑	6		SSID 6	1

Figure 4-11. Assigning WLANs to a BSSID in the Default Configuration

6. In the **Primary WLAN** drop-down menu, choose the WLAN for which the radio should beacon the SSID.

7. If you want to assign more WLANs to the radio, select another BSSID and repeat steps 5 and 6.

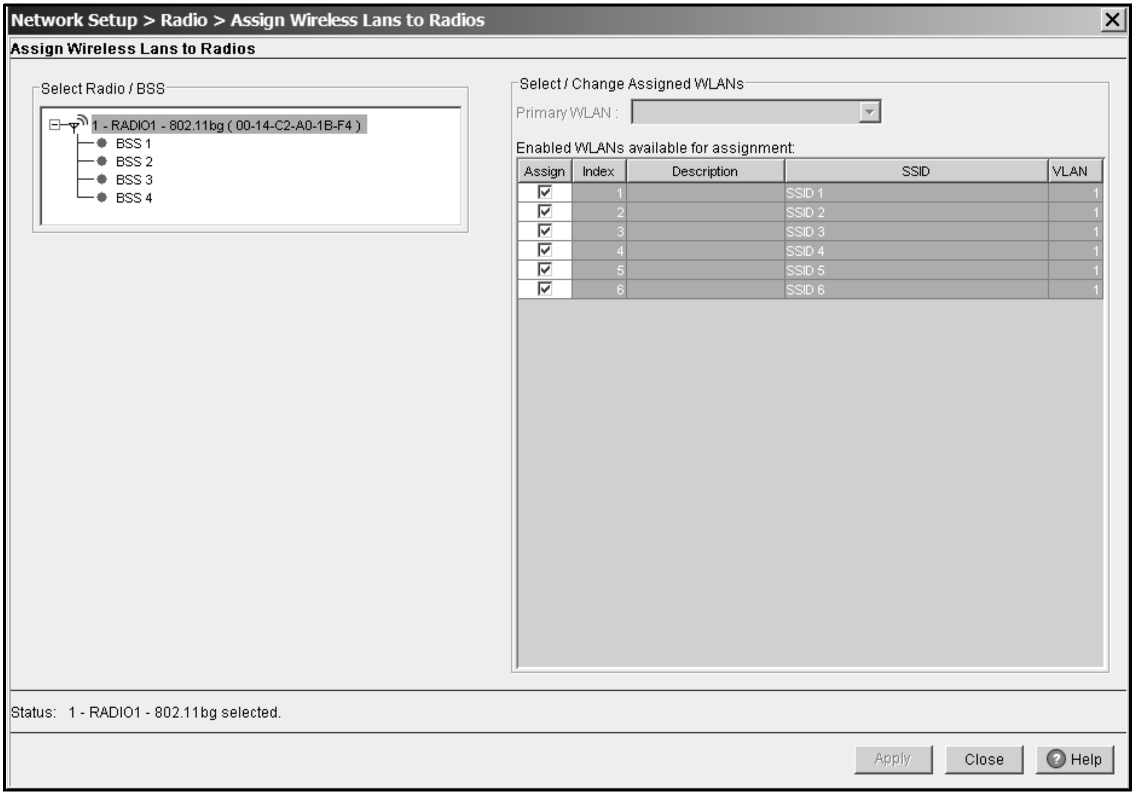
8. Click the **Apply** button.

Manually Assigning WLANs to a Specific Radio. Select this option to alter the WLAN assignment on a specific radio. By assigning different WLANs to different RP radios, you can:

- establish different WLANs in different areas of the network
- establish more than 16 WLANs in your network
- have different RP radios beacon different SSIDs

To manually assign WLANs, complete these steps:

1. Select **Network Setup** > **Radio** and click the radio that you want to configure.
2. Click the **WLAN Assignment** tab.
3. Click the **Edit** button. The **Network Setup** > **Radio** > **Assign Wireless Lans to Radios** screen is displayed. (See Figure 4-12.)



Network Setup > Radio > Assign Wireless Lans to Radios

Assign Wireless Lans to Radios

Select Radio / BSS

- 1 - RADIO1 - 802.11bg (00-14-C2-A0-1B-F4)
  - BSS 1
  - BSS 2
  - BSS 3
  - BSS 4

Select / Change Assigned WLANs

Primary WLAN :

Enabled WLANs available for assignment:

Assign	Index	Description	SSID	VLAN
☑	1		SSID 1	1
☑	2		SSID 2	1
☑	3		SSID 3	1
☑	4		SSID 4	1
☑	5		SSID 5	1
☑	6		SSID 6	1

Status: 1 - RADIO1 - 802.11bg selected.

Figure 4-12. Assigning WLANs to a Specific RP Radio

4. You can assign SSIDs either to the radio as a whole or to a specific BSSID. For example, you could assign SSIDs to the radio if:
   - you are assigning four or fewer WLANs to the radio
   - you are assigning more than four WLANs, but you want the radio to advertise the four with the lowest index numbers

   Complete step 5 to assign SSIDs to the radio as a whole. Complete step 6 to assign SSIDs to a specific BSSID.

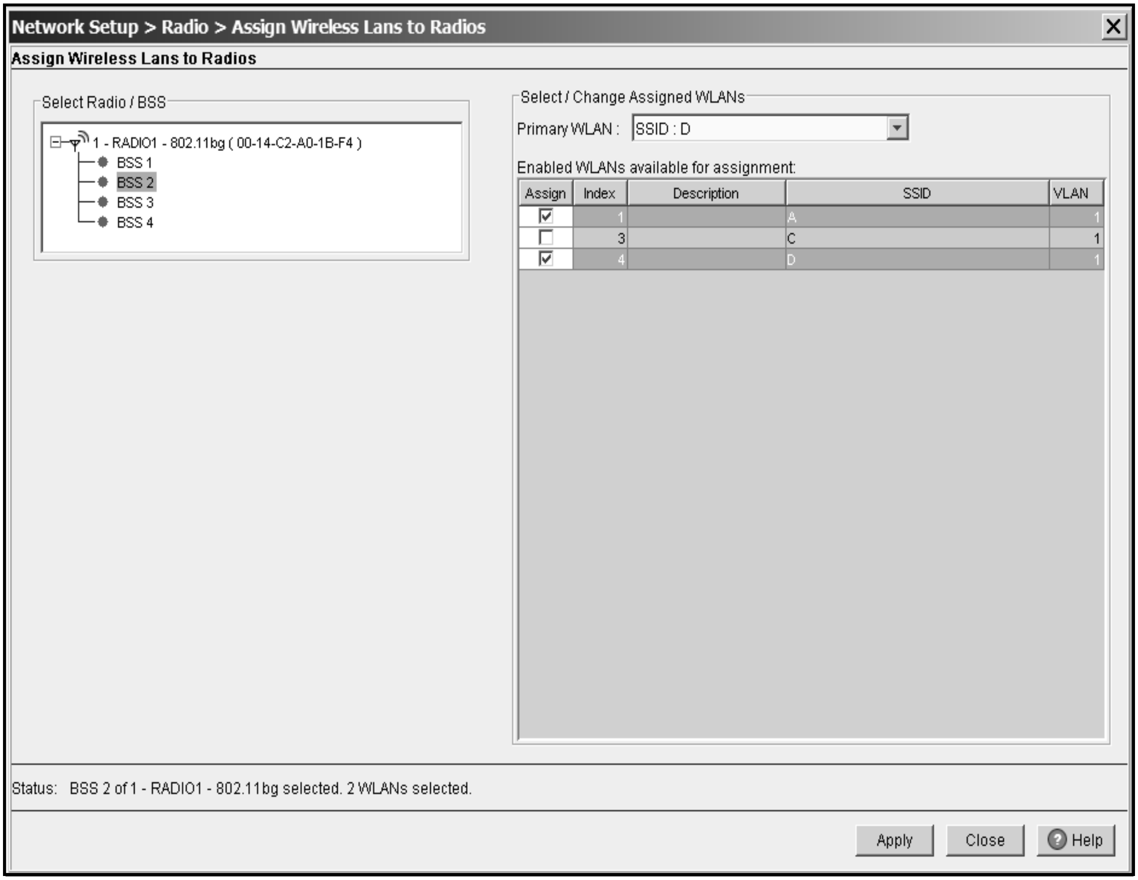
5. As shown in Figure 4-13, check the **Assign** box for each WLAN that you want the radio (or radios) to support. You can select up to 16 WLANs, but, as in normal mode, the RP radio only beacons SSIDs for the four WLANs with the lowest index numbers.

   Click the **Apply** button.

6. Alternatively, you can assign a WLAN to a specific BSSID on the radio:

   a. In the left area, **Select Radio/BSS**, select that BSSID.

   b. Check the **Assign** box for each WLAN that you want to assign to the BSSID. You can select up to four WLANs, but as always, the beacons only include one.


Network Setup > Radio > Assign Wireless Lans to Radios
Assign Wireless Lans to Radios
Select Radio / BSS
1 - RADIO1 - 802.11bg (00-14-C2-A0-1B-F4)
BSS 1
BSS 2
BSS 3
BSS 4
Select / Change Assigned WLANs
Apply
Close
Help

Primary WLAN : SSID : D

Enabled WLANs available for assignment:

Assign	Index	Description	SSID	VLAN
☑	1		A	1
□	3		C	1
☑	4		D	1

Status: BSS 2 of 1 - RADIO1 - 802.11bg selected. 2 WLANs selected.

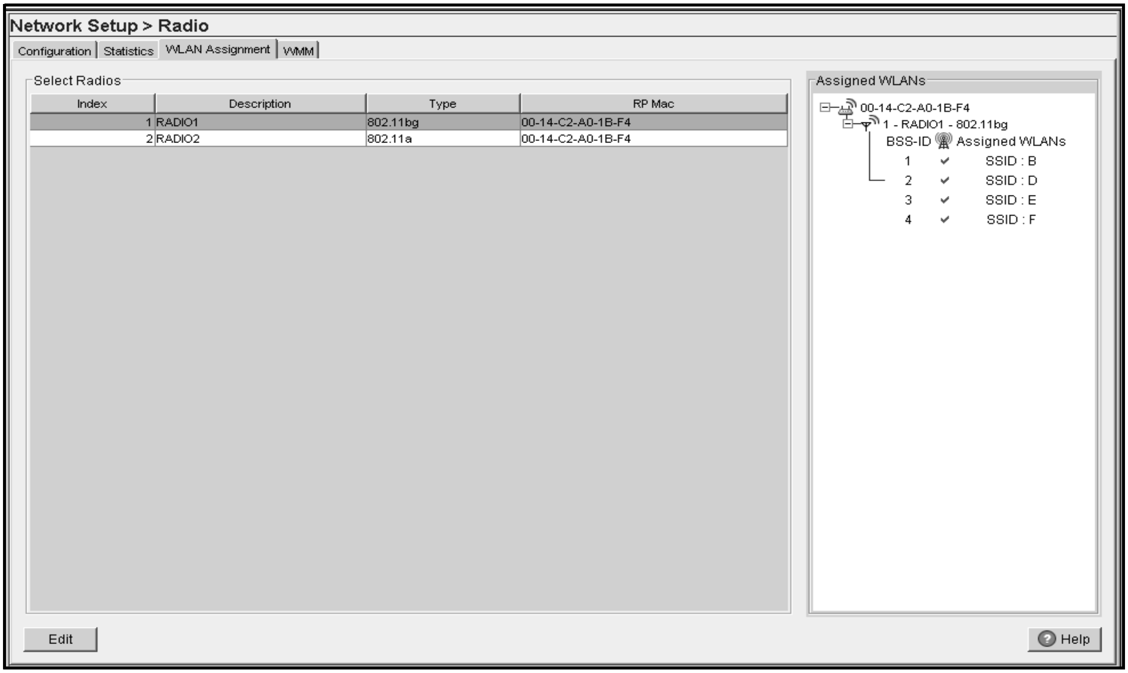
Figure 4-13. Assigning WLANs to a BSSID on a Radio

c. You can select which SSID RPs include in beacons by selecting a WLAN from the **Primary WLAN** drop-down menu.

d. Repeat this step for the other BSSIDs until you have assigned all the WLANs that you want this radio to support. Generally, you should assign at least one WLAN to each BSSID before you add multiple WLANs to a BSSID. This maximizes the number of SSIDs that RPs can beacon to wireless stations.

7. Click the **Apply** button, and then click the **Close** button.

The screen such as that in Figure 4-14 is displayed; you can check your configuration in the **Assigned WLAN** area.



Network Setup > Radio

Index	Description	Type	RP Mac
1	RADIO1	802.11bg	00-14-C2-A0-1B-F4
2	RADIO2	802.11a	00-14-C2-A0-1B-F4

00-14-C2-A0-1B-F4
1 - RADIO1 - 802.11bg

BSS-ID		Assigned WLANs
1	✓	SSID : B
2	✓	SSID : D
3	✓	SSID : E
4	✓	SSID : F

Figure 4-14. Selected WLANs Assigned to Radio 1 (Using Advanced Mode)

When you assign WLANs to the radio as a whole, as opposed to the BSSID, the Wireless Edge Services xl Module allocates SSIDs to the radio's four BSSIDs much as it does in normal mode. However, only the SSIDs of the WLANs that you selected are part of the process. Instead of always assigning WLAN 1 to BSSID 1 and WLAN 2 to BSSID 2, the module assigns the SSID for the enabled WLAN with the lowest index number to BSSID 1, and so on.

For example, you use advanced mode configuration to assign WLANs 2, 4, 5, and 6 to a particular RP radio. The Wireless Edge Services xl Module assigns SSID B (for WLAN 2) to BSSID 1, SSID D (for WLAN 4) to BSSID 2, and so on.

Figure 4-15 illustrates this configuration.

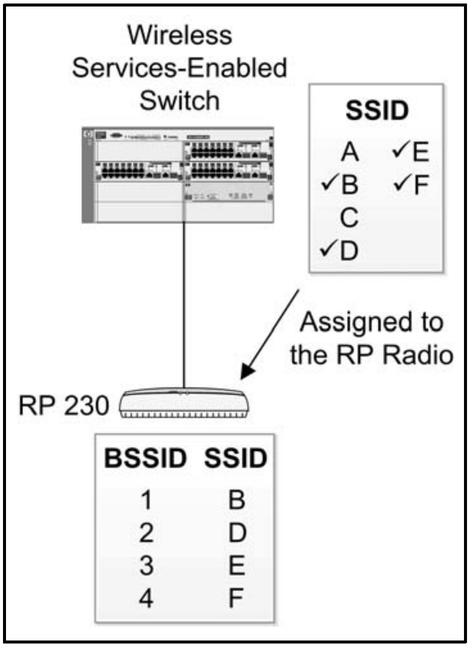


Figure 4-15. Manually Assigning WLANs to an RP Radio

Figure 4-14 shows the **Network Setup** > **Radio** screen in which you would check this configuration.

If you had assigned a fifth WLAN to the radio, then two SSIDs would be assigned to BSSID 1, and beacons would advertise only one of these SSIDs.

If you want the beacons to include the WLAN with the higher index number, then you should select the BSSID for the WLAN on the **Network Setup** > **Radio** > **WLAN Assignment** screen. Then select the higher WLAN from the **Primary WLAN** drop-down menu, as shown in Figure 4-13.

Using Normal and Advanced Mode Together

Rather than using advanced mode alone, it is often a good idea to first enable WLANs in normal mode, producing a template WLAN assignment that you can then alter with advanced mode configuration.

To use normal and advanced mode together, complete these steps:

1. Select **Network Setup** > **WLAN Setup**.
2. Configure the WLANs, as described in "Configuring a WLAN" on page 4-26.
3. On the **Network Setup** > **WLAN Setup** screen, select the WLANs, and then click **Enable**.
4. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed.
5. Check the **Advanced Configuration** box, and then click the **OK** button.
6. If necessary, tailor the radio adoption default configurations:
   a. Select **Network Setup** > **Radio Adoption Defaults** and click the **WLAN Assignment** tab.
   b. Edit the WLAN assignment, as described in "Manually Assigning WLANs to the Radio Adoption Default Configuration" on page 4-15. For example, you might select a different WLAN from the **Primary WLAN** drop-down menu.
7. If necessary, tailor a specific radio's configuration:
   a. Select **Network Setup** > **Radio** and click the **WLAN Assignment** tab.
   b. Select the radio and click the **Edit** button.
   c. Edit the WLAN assignment, as described in "Manually Assigning WLANs to a Specific Radio" on page 4-18. For example, you can prevent an RP in a public space from supporting a WLAN by unchecking the **Assign** box for that WLAN's SSID.

Changing from Advanced Mode to Normal Mode Configuration

Before disabling advanced mode configuration, you must verify that all WLAN assignments are compatible with normal mode. Check that:

- WLANs 1, 5, 9, and 13 (if enabled) are assigned to BSSID 1
- WLANs 2, 6, 10, and 14 (if enabled) are assigned to BSSID 2
- WLANs 3, 7, 11, and 15 (if enabled) are assigned to BSSID 3
- WLANs 4, 8, 12, and 16 (if enabled) are assigned to BSSID 4

If necessary, reconfigure the WLAN assignments as described in “Enabling WLANs Using Advanced Mode Configuration” on page 4-13. You must also remove all WLANs with indexes 17 and higher from the BSSIDs.

Note

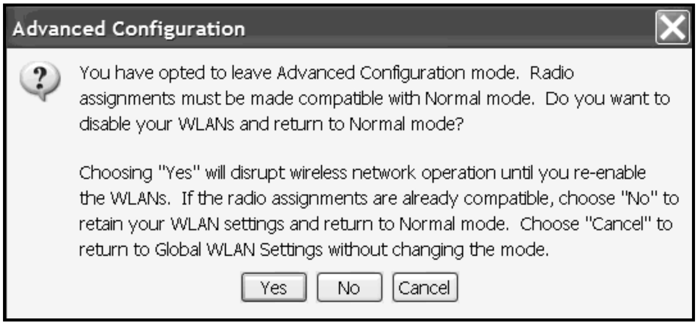
WLANs 17 through 32 are not available in normal mode. If you want the Wireless Edge Services xl Module to continue supporting one of these WLANs, then you must configure the corresponding SSID and settings on a WLAN with an index number from 1 through 16.

You must check the WLAN assignment for all of the following configurations:

- the radio adoption default configuration for 802.11a radios
- the radio adoption default configuration for 802.11bg radios
- the configuration for every RP radio adopted by your module

To disable advanced mode configuration, complete these steps:

1. Click **Network Setup** > **WLAN Setup**.
2. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed.
3. Uncheck the **Advanced Configuration** box, and then click the **OK** button. The screen shown in Figure 4-16 is displayed.



Advanced Configuration

You have opted to leave Advanced Configuration mode. Radio assignments must be made compatible with Normal mode. Do you want to disable your WLANs and return to Normal mode?

Choosing "Yes" will disrupt wireless network operation until you re-enable the WLANs. If the radio assignments are already compatible, choose "No" to retain your WLAN settings and return to Normal mode. Choose "Cancel" to return to Global WLAN Settings without changing the mode.

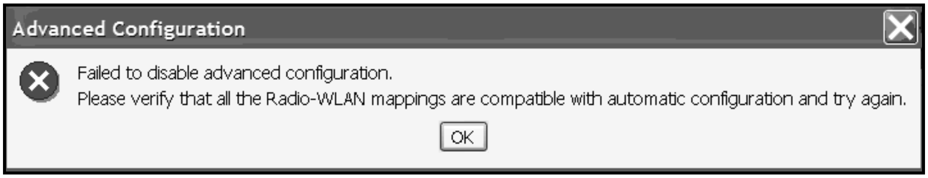
Figure 4-16. Disabling Advanced Configuration

4. Click the **No** button if you have verified that the WLAN assignment is compatible with normal mode. This option disables advanced mode, but leaves currently enabled WLANs active.

Caution

Take care when selecting the button. Clicking the **Yes** button and clicking the **No** button will both disable advanced mode. However, clicking the **Yes** button also disables all WLANs.

If you click the **No** button but the WLAN assignment is incorrect, the screen shown in Figure 4-17 is displayed.



Advanced Configuration

Failed to disable advanced configuration.
Please verify that all the Radio-WLAN mappings are compatible with automatic configuration and try again.

Figure 4-17. Failing to Disable Advanced Configuration

Click the **OK** button. You can now either:

- check the WLAN assignments on all radios and default configurations, reassigning SSIDs to BSSIDs as described at the beginning of this section
- execute a forced disable by clicking the **Yes** button

Click the **Yes** button to force advanced mode to disable. This option disables advanced mode configuration as well as *all* WLANs, even those that are compatible with normal mode. Take care when selecting this option because it disassociates wireless stations and can disrupt network activity.

After you click the **Yes** button, you should move to the **Network Setup** > **WLAN Setup** screen and re-enable the WLANs. The Wireless Edge Services xl Module then assigns the SSIDs to the correct BSSIDs.

Click the **Cancel** button to continue using advanced mode configuration.

Configuring a WLAN

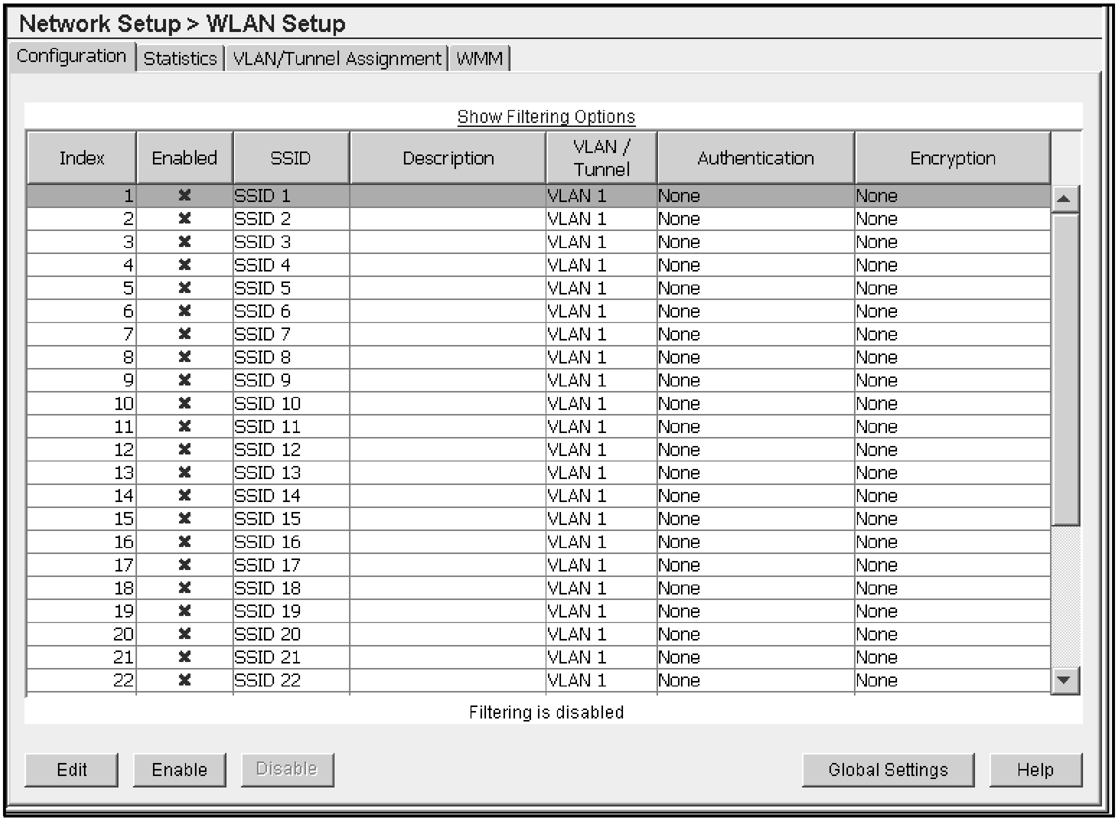
To configure a WLAN, you must set:

- the SSID
- the VLAN (or tunnel) in which traffic will be forwarded
- security options, which include:
  - authentication method
  - encryption option

Optionally, you can configure:

- advanced settings for individual WLANs, which include:
  - inter-station blocking
  - closed system operations
  - inactivity timeouts
- global settings for all WLANs, which include:
  - proxy Address Resolution Protocol (ARP)
  - shared-key authentication

The following sections will guide you through the process of configuring these settings. The first step is accessing the **Network Setup** > **WLAN Setup** > **Configuration** screen.



Network Setup > WLAN Setup

Index	Enabled	SSID	Description	VLAN / Tunnel	Authentication	Encryption
1	✖	SSID 1		VLAN 1	None	None
2	✖	SSID 2		VLAN 1	None	None
3	✖	SSID 3		VLAN 1	None	None
4	✖	SSID 4		VLAN 1	None	None
5	✖	SSID 5		VLAN 1	None	None
6	✖	SSID 6		VLAN 1	None	None
7	✖	SSID 7		VLAN 1	None	None
8	✖	SSID 8		VLAN 1	None	None
9	✖	SSID 9		VLAN 1	None	None
10	✖	SSID 10		VLAN 1	None	None
11	✖	SSID 11		VLAN 1	None	None
12	✖	SSID 12		VLAN 1	None	None
13	✖	SSID 13		VLAN 1	None	None
14	✖	SSID 14		VLAN 1	None	None
15	✖	SSID 15		VLAN 1	None	None
16	✖	SSID 16		VLAN 1	None	None
17	✖	SSID 17		VLAN 1	None	None
18	✖	SSID 18		VLAN 1	None	None
19	✖	SSID 19		VLAN 1	None	None
20	✖	SSID 20		VLAN 1	None	None
21	✖	SSID 21		VLAN 1	None	None
22	✖	SSID 22		VLAN 1	None	None

Filtering is disabled

Figure 4-18. Network Setup > WLAN Setup > Configuration Screen

As you can see in Figure 4-18, this screen displays the 32 WLANs that are available for configuration. Remember that in normal configuration mode, you can only configure WLANs 1 through 16.

On the Wireless Edge Services xl Module, you do not *create* WLANs as such. The module has already created them; you configure options for and enable the WLANs. The default configuration for each WLAN is displayed in seven columns:

- **Index**—Lists the WLANs by index number. Although you will create your own name for the WLAN, this index number is important because it determines which WLAN is the primary WLAN on a BSSID, if you enable more than four WLANs. (By default, the WLAN on the BSSID with the lowest number is the primary WLAN.)

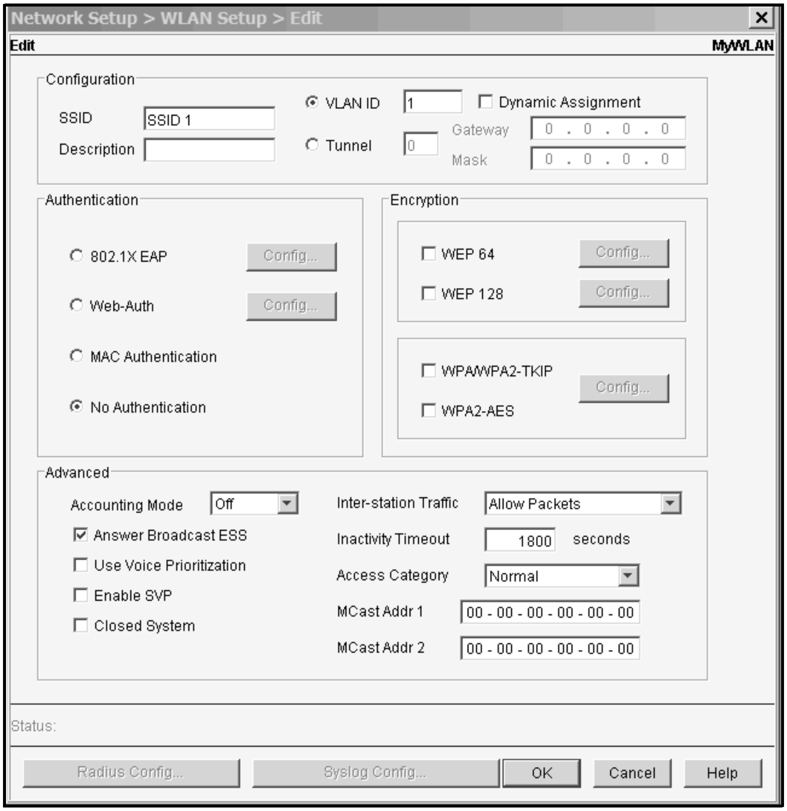
- **Enabled**—Indicates whether the WLAN has been enabled. The Wireless Edge Services xl Module does not deploy a WLAN configuration to RPs until you enable the WLAN. By default, all WLANs are disabled.
- **SSID**—Displays the WLAN's SSID. By default, this SSID simply indicates the WLAN's index number. You will change this to a network name when you configure the WLAN.
- **Description**—Describes the WLAN so that you can quickly see its purpose. For example, it might read "Internet access for guests."
- **VLAN/Tunnel**—Displays the interface in which traffic received from this WLAN is forwarded. Typically, this is a VLAN interface, but the Wireless Edge Services xl Module can also forward WLAN traffic over a GRE tunnel. Initially, all WLANs are assigned to the default VLAN, VLAN 1. You will learn more about VLAN assignment in "Setting Basic Configuration Options: SSID and Interface" on page 4-30 and "VLAN Assignment" on page 4-81.
- **Authentication** and **Encryption**—Display the security options implemented on the WLAN.

When you want to establish a new WLAN in your network (or to alter settings of an existing WLAN), select a WLAN and click the **Edit** button at the bottom of the screen.

Note

You must select a WLAN with index number 1 to 16 unless you enable advanced mode configuration. See "Advanced Mode Configuration" on page 4-11.

The screen illustrated in Figure 4-19 is displayed: this is the **Edit** screen for the selected WLAN. On this screen, you configure settings for your WLAN.



Network Setup > WLAN Setup > Edit ✕

Edit MyWLAN

Configuration

SSID: SSID 1
Description:
● VLAN ID: 1 □ Dynamic Assignment
○ Tunnel: 0 Gateway: 0 . 0 . 0 . 0
Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP [Config...]
○ Web-Auth [Config...]
○ MAC Authentication
● No Authentication

Encryption

□ WEP 64 [Config...]
□ WEP 128 [Config...]
□ WPA/WPA2-TKIP [Config...]
□ WPA2-AES

Advanced

Accounting Mode: Off
☑ Answer Broadcast ESS
□ Use Voice Prioritization
□ Enable SVP
□ Closed System
Inter-station Traffic: Allow Packets
Inactivity Timeout: 1800 seconds
Access Category: Normal
MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

[Radius Config...] [Syslog Config...] [OK] [Cancel] [Help]

Figure 4-19. Editing a WLAN

In the **Configuration** section, you create the WLAN's basic settings.

Configure security standards in the **Authentication** and **Encryption** sections. If you choose an authentication option that requires a RADIUS server, the **RADIUS Config...** button is enabled, and you can configure RADIUS settings.

Optionally, you can configure advanced options in the **Advanced** section.

The following sections explain in more detail how to configure these settings. However, the advanced options that deal specifically with quality of service (QoS) are described in "Traffic Management (QoS)" on page 4-90.

Setting Basic Configuration Options: SSID and Interface

You must set the following options in the **Configuration** section of a WLAN's **Edit** screen:

- the SSID

  The SSID identifies the WLAN; stations associated to the same SSID are in the same WLAN regardless of the RP radio to which they have associated. The SSID is sometimes called the network name; it is the name that users see when they search for wireless networks to which to connect (as long as the WLAN operates in open system).

  Because SSIDs distinguish WLANs from each other, each WLAN must have a unique SSID.

- the interface associated with the WLAN

  It is the Wireless Edge Services xl Module's role to ready traffic received from RPs for transmission into the Ethernet network. The module removes the 802.11 header and adds an Ethernet header. This header includes a 802.1Q tag for a particular VLAN. In other words, the module assigns stations in the WLAN to a VLAN.

  By default, the module places all wireless traffic in VLAN 1. If your network only uses one subnetwork, this configuration is adequate. Many networks, however, include multiple subnetworks, of which VLAN 1 is sometimes the management VLAN. Because of security, as well as other, concerns, you should often assign the WLAN a new VLAN ID.

  You can tag wireless traffic for one of your network's user VLANs, or you can create a separate VLAN entirely dedicated to wireless stations. If you choose the second option, of course, you must ensure traffic can reach its destination. For example, configure the Wireless Edge Services xl Module to route traffic. You might also need to configure Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) services on the VLAN. See "Reserving VLANs for Wireless Users" on page 1-18 of *Chapter 1: Introduction* for more explanation.

  Instead of mapping the WLAN to a VLAN, you can map it to a tunnel interface. See *Chapter 12: Configuring Tunnels with Generic Routing Encapsulation* for more information on this topic.

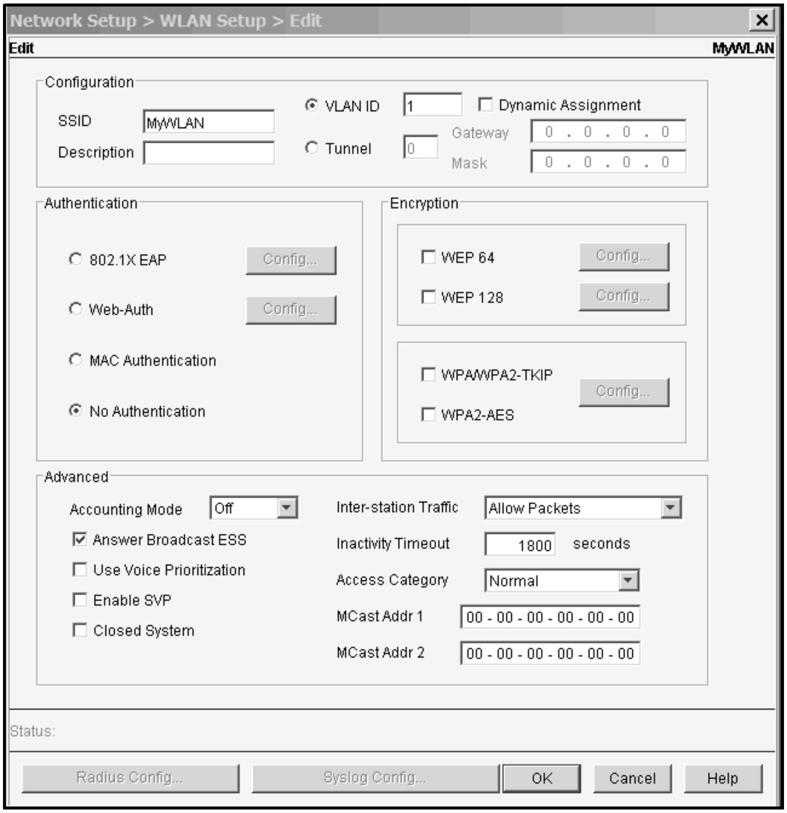
  Finally, your network might include a RADIUS server that assigns users to VLANs based on their identities. Enable dynamic VLANs to allow the module to enforce these assignments. (The VLAN ID that you configure manually remains the default for users not assigned to a dynamic VLAN.)

You can also enter a description, but this setting is optional.

To configure these options, follow these steps:

1. Access the **Edit** screen for the WLAN, as described in “Configuring a WLAN” on page 4-26.

2. Under **Configuration**, in the **SSID** field, enter the SSID that you have selected for this WLAN.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID: MyWLAN
Description:
● VLAN ID: 1 □ Dynamic Assignment
○ Tunnel: 0 Gateway: 0 . 0 . 0 . 0 Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP
○ Web-Auth
○ MAC Authentication
● No Authentication

Encryption

□ WEP 64
□ WEP 128
□ WPA/WPA2-TKIP
□ WPA2-AES

Advanced

Accounting Mode: Off
☑ Answer Broadcast ESS
□ Use Voice Prioritization
□ Enable SVP
□ Closed System
Inter-station Traffic: Allow Packets
Inactivity Timeout: 1800 seconds
Access Category: Normal
MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-20. Configuring the SSID

When you enable the WLAN, the Wireless Edge Services xl Module automatically configures this SSID on all adopted RP radios (as long as you are using normal mode). For more information on how the module does this, see “Normal Mode Configuration” on page 4-4.

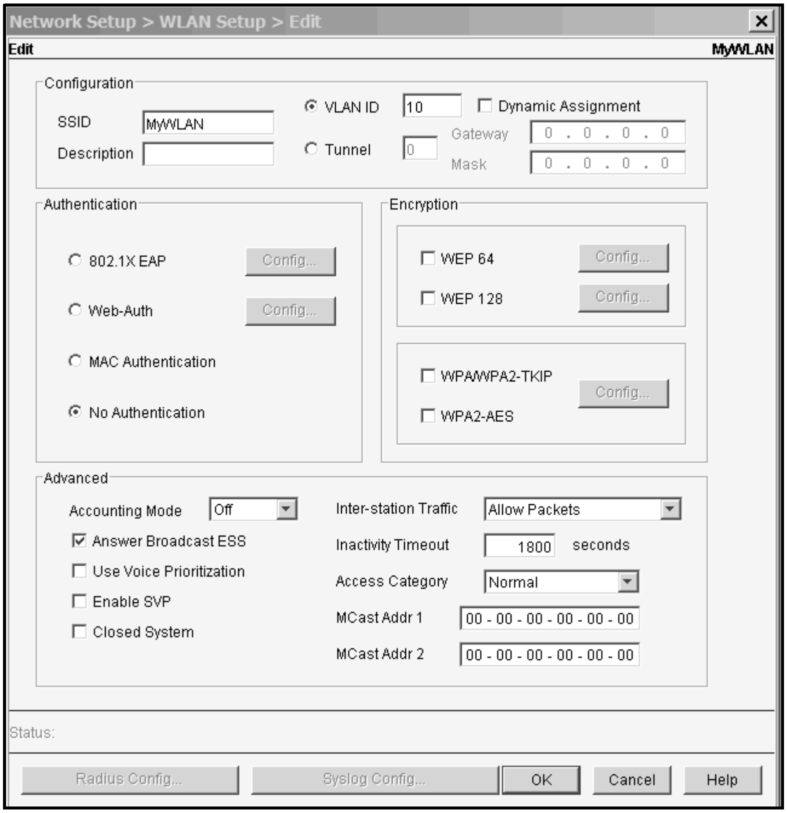
3. In the **Description** field, enter information about this WLAN to remind you and other administrators of its purpose.

For example, if this WLAN provides network access for sales representatives in conference rooms, you could enter "Sales/Conference Rooms." (This information is for reference only and is not sent to the RPs nor broadcast to wireless stations.)

4. Select the interface to which the module maps wireless traffic. Choose one of the following:
   - Select **VLAN ID** and enter a value in the corresponding field to map the WLAN to a particular VLAN.

     This is the typical configuration. The Wireless Edge Services xl Module tags traffic that arrives on the WLAN for the VLAN you specify. The VLAN ID can be a value from 1 to 4096.
   - Select **Tunnel** and enter the index number for a previously configured tunnel interface.

     Choose this option to configure the module to tunnel all of this WLAN's traffic to a remote device, such as a WAN router that connects to the Internet. In the **Gateway** and **Mask** fields, enter the remote device's IP address on the tunnel subnetwork. See *Chapter 12: Configuring Tunnels with Generic Routing Encapsulation* for more information.



Network Setup > WLAN Setup > Edit

Edit — MyWLAN

Configuration
- SSID: MyWLAN
- Description:
- ● VLAN ID: 10 — □ Dynamic Assignment
- ○ Tunnel: 0
- Gateway: 0 . 0 . 0 . 0
- Mask: 0 . 0 . 0 . 0

Authentication
- ○ 802.1X EAP
- ○ Web-Auth
- ○ MAC Authentication
- ● No Authentication

Encryption
- □ WEP 64
- □ WEP 128
- □ WPA/WPA2-TKIP
- □ WPA2-AES

Advanced
- Accounting Mode: Off
- ☑ Answer Broadcast ESS
- □ Use Voice Prioritization
- □ Enable SVP
- □ Closed System
- Inter-station Traffic: Allow Packets
- Inactivity Timeout: 1800 seconds
- Access Category: Normal
- MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
- MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-21. Setting the VLAN ID

5. Check the **Dynamic Assignment** box to enable the Wireless Edge Services xl Module to apply dynamic (or user-based) VLAN assignments received from a RADIUS server.

   Do not use dynamic VLAN assignment when the WLAN requires Layer 3 mobility.

   If the WLAN uses Web-Auth set the DHCP lease for the WLAN’s static VLAN very low. This allows the station to request a new IP address in the dynamic VLAN after the user authenticates.

6. Continue configuring the WLAN. See “Configuring Security Options” on page 4-34. (Or click **OK** to apply the settings and close the **Edit** screen.)

Necessary Configurations on the Wireless Services-Enabled Switch

The VLAN for which the Wireless Edge Services xl Module tags WLAN traffic is called an uplink VLAN. If you decide to have your Ethernet infrastructure devices route traffic from the wireless stations, you must tag the module's uplink port for the stations' VLAN. You make this configuration from the wireless services-enabled switch. (See the Wireless Edge Services xl MOdule Supplement to the *ProCurve 6400cl/5300xl/3400cl Management and Configuration Guide*.)

Alternatively, you can have the Wireless Edge Services xl Module route wireless traffic and perform other necessary services for the wireless stations' VLAN. In this case, no further configuration on the wireless services-enabled switch is necessary.

Configuring Security Options

From the **Network Setup** > **WLAN Setup** > **Edit** screen, you can also configure authentication and encryption options.

The security provided by a WLAN is one of its most important functions. All RPs in a WLAN must use the same security options and, for some security options, static keys. Therefore, the Wireless Edge Services xl Module, which automatically deploys the same WLAN configuration to all adopted RPs, simplifies establishing a WLAN throughout a wireless network. Remember, however, that if your network includes more than one Wireless Edge Services xl Module, you must configure exactly the same security options for identical WLANs on different modules.

Configuring Authentication

For the best security, you should enable some form of authentication on every WLAN. Authentication protects your network resources from unauthorized access; it can also protect wireless stations from connecting to a rogue access point (AP).

The Wireless Edge Services xl Module supports three types of authentication:

- 802.1X Extensible Authentication Protocol (EAP)
- Web authentication (Web-Auth)
- Media Access Control (MAC) authentication

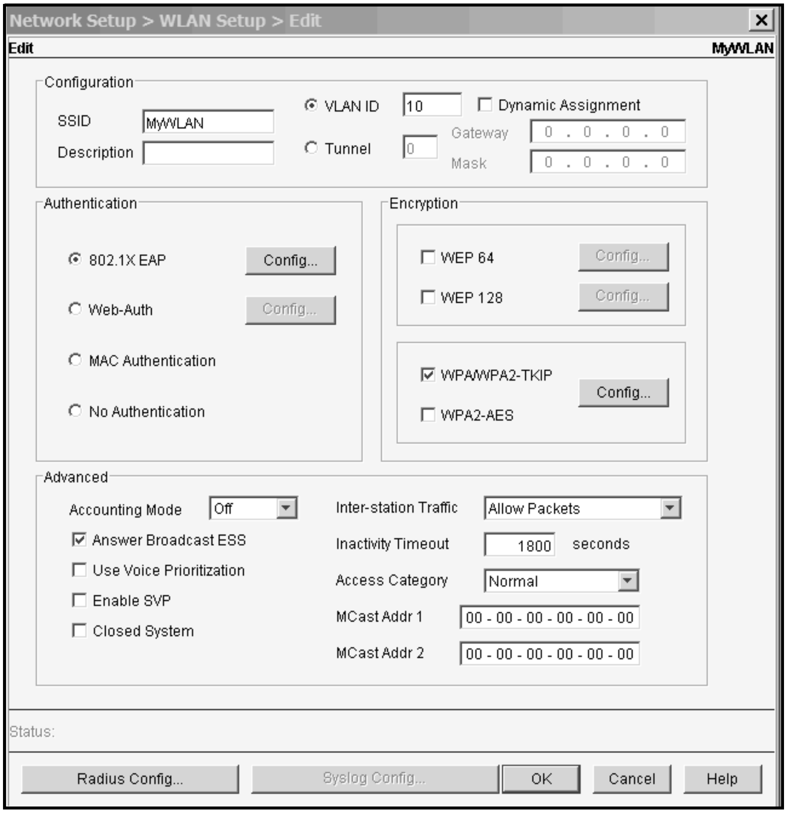
You configure authentication methods as part of each individual WLAN's settings, and, as far as that WLAN is concerned, they are mutually exclusive. For example, a WLAN can require stations to authenticate using 802.1X or using Web-Auth, but not both. However, one WLAN can require 802.1X and a different WLAN, Web-Auth.

The MAC authentication configured on a WLAN is MAC authentication to a *RADIUS server*. That is, the module forwards stations' MAC addresses to be checked against accounts stored on a network server.

The Wireless Edge Services xl Module can also enforce de facto local MAC authentication, using globally configured filters, or MAC standard access control lists (ACLs), that are applied to the WLAN. You can combine these filters with another type of authentication: first, the MAC ACLs filter association requests; then the WLAN's specific authentication method initiates. See *Chapter 13: Wireless Network Management* to learn how to configure MAC standard ACLs.

802.1X EAP. 802.1X is the IEEE standard for wireless authentication. When a station attempts to connect to a WLAN that uses this standard, the Wireless Edge Services xl Module places the association in closed status, dropping all traffic except EAP messages. The module forwards these messages to an authentication server (RADIUS server), and the station and server verify each other's identities. During the authentication process, the station and module also receive dynamic keys for encryption.

As an alternative to a network RADIUS server, you can use the Wireless Edge Services xl Module's internal RADIUS capabilities. See *Chapter 11: RADIUS Server* for more information.



Network Setup > WLAN Setup > Edit

Edit — MyWLAN

Configuration
- SSID: MyWLAN
- Description:
- ● VLAN ID: 10 — □ Dynamic Assignment
- ○ Tunnel: 0 — Gateway: 0 . 0 . 0 . 0 — Mask: 0 . 0 . 0 . 0

Authentication
- ● 802.1X EAP — Config...
- ○ Web-Auth — Config...
- ○ MAC Authentication
- ○ No Authentication

Encryption
- □ WEP 64 — Config...
- □ WEP 128 — Config...
- ☑ WPA/WPA2-TKIP — Config...
- □ WPA2-AES

Advanced
- Accounting Mode: Off
- ☑ Answer Broadcast ESS
- □ Use Voice Prioritization
- □ Enable SVP
- □ Closed System
- Inter-station Traffic: Allow Packets
- Inactivity Timeout: 1800 seconds
- Access Category: Normal
- MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
- MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

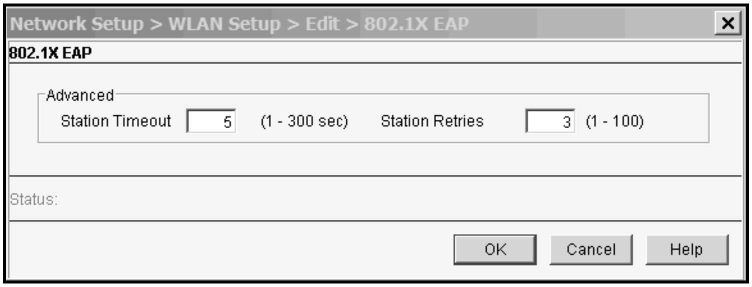
Radius Config... | Syslog Config... | OK | Cancel | Help

Figure 4-22. Enabling 802.1X Authentication

To configure 802.1X authentication for a WLAN, complete these steps:

1. Click **Network Setup** > **WLAN Setup**.
2. Select the WLAN and click the **Edit** button.
3. Under **Authentication**, select **802.1X EAP**.

4. Optionally, click the **Config** button next to **802.1X EAP** to configure some advanced settings for the station:



Network Setup > WLAN Setup > Edit > 802.1X EAP

802.1X EAP

Advanced

Station Timeout 5 (1 - 300 sec) Station Retries 3 (1 - 100)

Status:

Figure 4-23. Specifying 802.1X EAP Settings

   a. Enter a value in the **Station Timeout** field to control how long the module will wait for a station to authenticate itself.

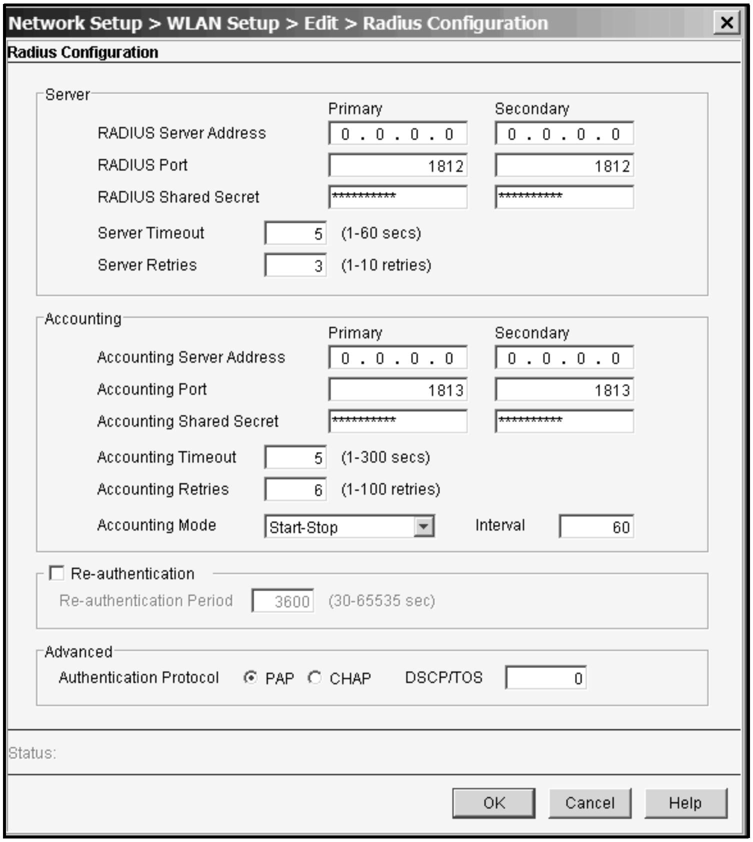
      The **Station Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   b. Enter a value in the **Station Retries** field to control how many times the module will reissue a challenge to the station.

      The setting for **Station Retries** can be from 1 to 10; the default setting is 3.

   c. Click the **OK** button. You return to the WLAN's **Edit** screen.

5. 802.1X requires a RADIUS server to act as the authentication server. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.



Network Setup > WLAN Setup > Edit > Radius Configuration

Radius Configuration

Server

	Primary	Secondary
RADIUS Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
RADIUS Port	1812	1812
RADIUS Shared Secret	**********	**********

Server Timeout 5 (1-60 secs)
Server Retries 3 (1-10 retries)

Accounting

	Primary	Secondary
Accounting Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
Accounting Port	1813	1813
Accounting Shared Secret	**********	**********

Accounting Timeout 5 (1-300 secs)
Accounting Retries 6 (1-100 retries)
Accounting Mode Start-Stop Interval 60

☐ Re-authentication
Re-authentication Period 3600 (30-65535 sec)

Advanced
Authentication Protocol ● PAP ○ CHAP DSCP/TOS 0

Status:

Figure 4-24. Radius Configuration Screen

6. In the **Radius Configuration** screen, under **Server**, specify settings for your network's RADIUS servers.

   Enter settings for your primary server in the fields in the **Primary** column:

   a. In the **RADIUS Server Address** field, specify the IP address of your network's primary RADIUS server.

      To use the module's internal server, enter 127.0.0.1.

   b. Leave the **RADIUS Port** field at the default value unless you know that your server uses a different port.

      The default value is 1812.

c. In the **RADIUS Shared Secret** field, enter a character string up to 127 characters.

The RADIUS server uses the secret to identify the Wireless Edge Services xl Module as a legitimate client. You must match the secret configured for the module in your RADIUS server's configuration.

If you are using the module's internal server, do not enter a shared secret.

d. Optionally, enter settings for a secondary RADIUS server in the fields in the **Secondary** column.

7. Optionally, alter other RADIUS server settings:

   - Enter a value in the **Server Timeout** to control how long the Wireless Edge Services xl Module will wait for a reply from the RADIUS server.

     The **Server Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   - Enter a value in the **Server Retries** fields to control how many times the module will reattempt to contact a server that does not reply.

     The setting for **Server Retries** can be from 1 to 10. By default, the value is 3; Wireless Edge Services xl Module attempts to contact the server up to four times (one initial try and three subsequent tries).

8. Check the **Re-authentication** box if you want to force stations to periodically re-authenticate to the network. Specify how often (in seconds) stations must re-authenticate in the **Re-authentication Period** field.

   Re-authentication occurs in the background. By default, re-authentication is disabled, but if you enable it, the default period is one hour (3600 seconds). The valid range is 30 to 65535 seconds.

9. Optionally, enter a value in the DSCP/TOS field to prioritize traffic to the RADIUS server.

   Valid values range from 0 through 63.

   a. Leave the other settings at their defaults and click the **OK** button. You will return to the WLAN's **Edit** screen.

10. You must now configure the encryption option. See "Configuring Encryption" on page 4-48.

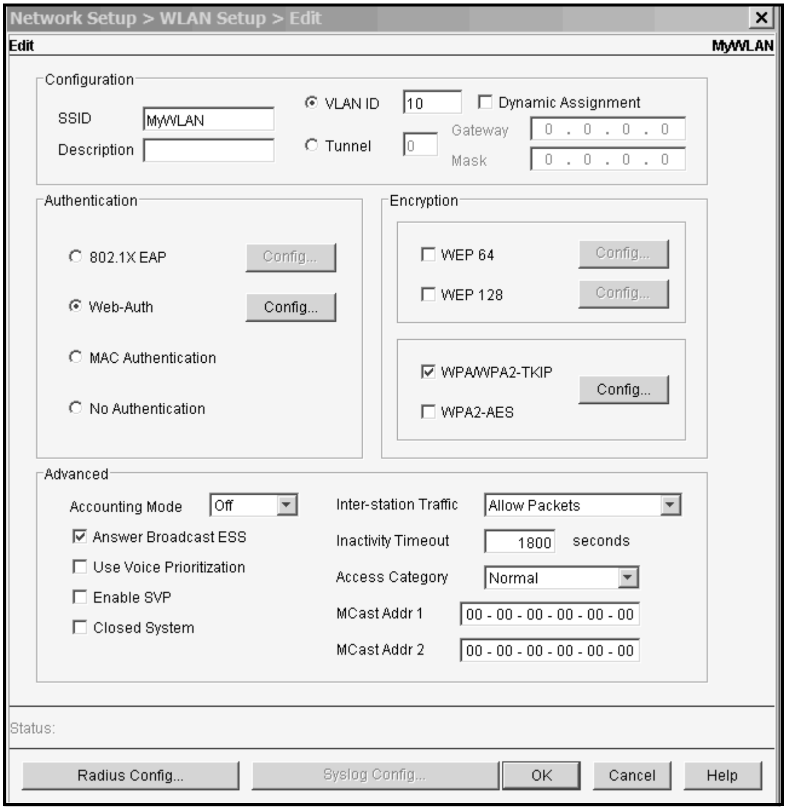
Web-Auth. Web-Auth allows wireless stations that do not support 802.1X to authenticate to a RADIUS server. Web-Auth is an easy-to-use option that is often selected for wireless networks that provide Internet or limited network access to a broad range of users. The instructions below simply guide you through the most basic Web-Auth settings. You should refer to *Chapter 5: Web Authentication for Mobile Users* to learn how to configure more advanced options and customize Web pages.

Note

You can configure MAC authentication for more security in a WLAN using Web-Auth. (See *Chapter 13: Wireless Network Management*.)

To enable Web-Auth on a WLAN, complete these steps:

1. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
2. Select the WLAN that you want to use Web-Auth, and then click the **Edit** button. The **Edit** screen is displayed.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 10 □ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP Config...

● Web-Auth Config...

○ MAC Authentication

○ No Authentication

Encryption

□ WEP 64 Config...

□ WEP 128 Config...

☑ WPA/WPA2-TKIP Config...

□ WPA2-AES

Advanced

Accounting Mode Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic Allow Packets

Inactivity Timeout 1800 seconds

Access Category Normal

MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

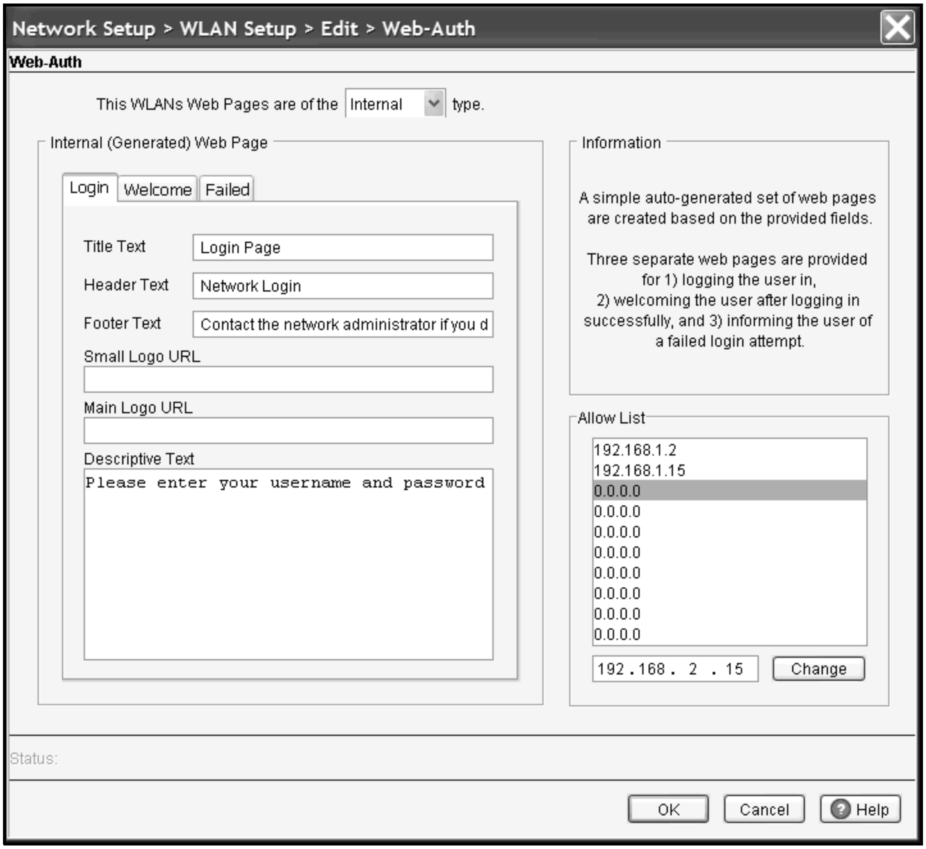
Figure 4-25. Enabling Web-Auth

3. Under **Authentication**, select **Web-Auth**.

Note

On the configuration screens that appear in this procedure, you can quickly get the WLAN running by completing these minimal steps. (Learn more about the process in *Chapter 5: Web Authentication for Mobile Users*.)

4. Click the **Config** button next to **Web-Auth**. The **Web-Auth** screen is displayed.



Network Setup > WLAN Setup > Edit > Web-Auth

Web-Auth

This WLANs Web Pages are of the Internal type.

Internal (Generated) Web Page

Title Text: Login Page

Header Text: Network Login

Footer Text: Contact the network administrator if you d

Small Logo URL:

Main Logo URL:

Descriptive Text: Please enter your username and password

Information

A simple auto-generated set of web pages are created based on the provided fields.

Three separate web pages are provided for 1) logging the user in, 2) welcoming the user after logging in successfully, and 3) informing the user of a failed login attempt.

Allow List

192.168.1.2
192.168.1.15
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0
0.0.0.0

192 . 168 . 2 . 15

Status:

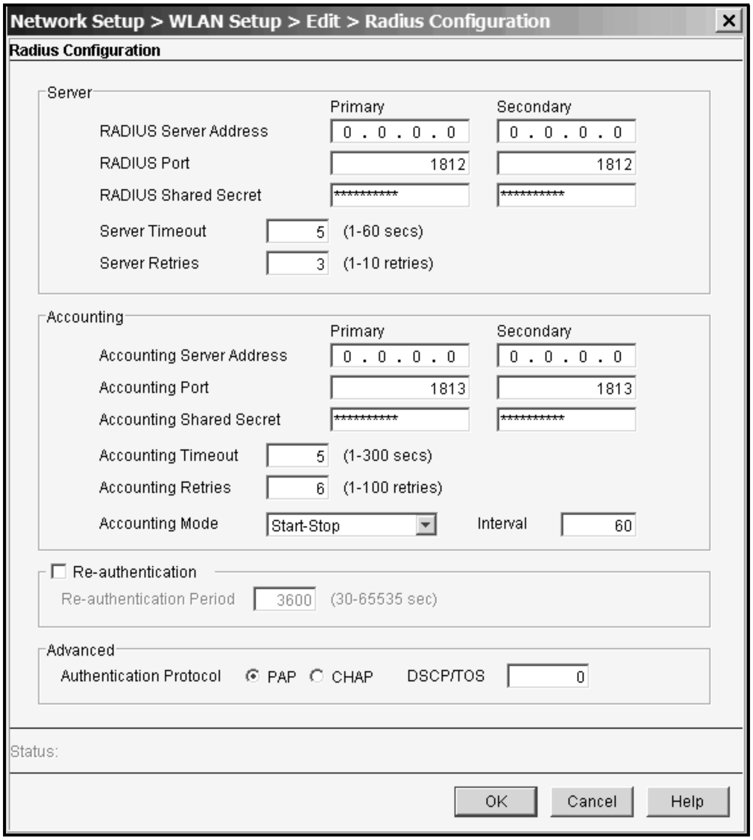
Figure 4-26. Configuring the Allow

5. On the **Web-Auth** screen, under **Allow List**, add the IP addresses that *unauthorized* stations are allowed to access.

The Wireless Edge Services xl Module automatically handles traffic such as DHCP and Domain Name System (DNS) requests. In this basic configuration, you are using Web-Auth pages stored on the module, so you are not required to add any IP addresses to the Allow list. For more advanced options, see *Chapter 5: Web Authentication for Mobile Users*.

6. Leave other settings at their defaults and click the **OK** button.

7. Web-Auth requires a RADIUS server to act as the authentication server. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.



Network Setup > WLAN Setup > Edit > Radius Configuration

Radius Configuration

Server

	Primary	Secondary
RADIUS Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
RADIUS Port	1812	1812
RADIUS Shared Secret	***********	***********

Server Timeout 5 (1-60 secs)
Server Retries 3 (1-10 retries)

Accounting

	Primary	Secondary
Accounting Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
Accounting Port	1813	1813
Accounting Shared Secret	***********	***********

Accounting Timeout 5 (1-300 secs)
Accounting Retries 6 (1-100 retries)
Accounting Mode Start-Stop Interval 60

□ Re-authentication
Re-authentication Period 3600 (30-65535 sec)

Advanced
Authentication Protocol ● PAP ○ CHAP DSCP/TOS 0

Status:

Figure 4-27. Radius Configuration Screen

8. In the **Radius Configuration** screen, under **Server**, specify settings for your network's RADIUS servers.

   Enter settings for your primary server in the fields in the **Primary** column:

   a. In the **RADIUS Server Address** field, specify the IP address of your network's primary RADIUS server.

      To use the module's internal server, enter 127.0.0.1.

   b. Leave the **RADIUS Port** field at the default value unless you know that your server uses a different port.

      The default value is 1812.

   c. In the **RADIUS Shared Secret** field, enter a character string up to 127 characters.

      The RADIUS server uses the secret to identify the Wireless Edge Services xl Module as a legitimate client. You must match the secret configured for the module in your RADIUS server's configuration.

      If you are using the module's internal server, you do not need to enter a shared secret.

   d. Optionally, enter settings for a secondary RADIUS server in the fields in the **Secondary** column.

9. Optionally, alter other RADIUS server settings:

   - Enter a value in the **Server Timeout** to control how long the Wireless Edge Services xl Module will wait for a reply from the RADIUS server.

     The **Server Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   - Enter a value in the **Server Retries** fields to control how many times the module will reattempt to contact a server that does not reply.

     The setting for **Server Retries** can be from 1 to 10. By default, the value is 3; Wireless Edge Services xl Module attempts to contact the server up to four times (one initial try and three subsequent tries).

10. Check the **Re-authentication** box if you want to force stations to periodically re-authenticate to the network. Specify how often (in seconds) stations must re-authenticate in the **Re-authentication Period** field.

    Re-authentication occurs in the background. By default, re-authentication is disabled, but if you enable it, the default period is one hour (3600 seconds). The valid range is 30 to 65535 seconds.

11. Choose the protocol in which the Wireless Edge Services xl Module packages users' credentials. Select **PAP** (the default) or **CHAP** for the **Authentication Protocol**.

12. Optionally, enter a value in the DSCP/TOS field to prioritize traffic to the RADIUS server.

    Valid values range from 0 through 63.

13. Leave the other settings at their defaults and click the **OK** button.

14. You should now configure the encryption options. See "Configuring Encryption" on page 4-48.

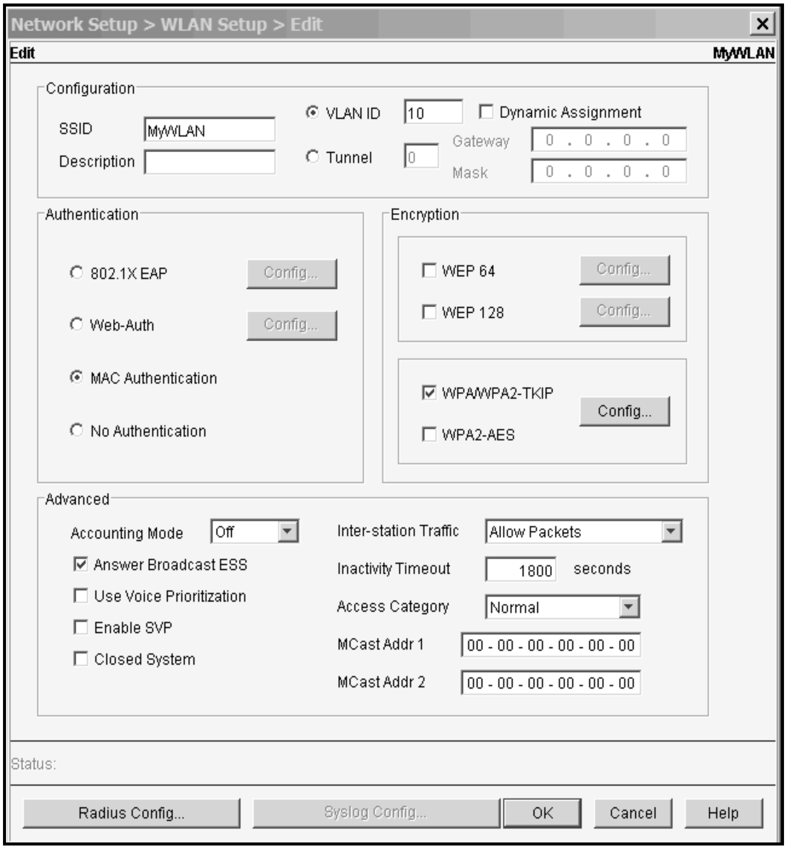
MAC Authentication. The **MAC Authentication** option refers to RADIUS MAC authentication. When a station attempts to associate with the WLAN, the Wireless Edge Services xl Module forwards the station's MAC address in a request to a RADIUS server. The RADIUS server decides whether the station can associate.

To configure MAC authentication, complete these steps:

1. Access the **Edit** screen for the WLAN:

   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.

   b. Select the WLAN that should use MAC authentication and click the **Edit** button.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 10 □ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

● MAC Authentication

○ No Authentication

Encryption

□ WEP 64

□ WEP 128

☑ WPA/WPA2-TKIP

□ WPA2-AES

Advanced

Accounting Mode Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic Allow Packets

Inactivity Timeout 1800 seconds

Access Category Normal

MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

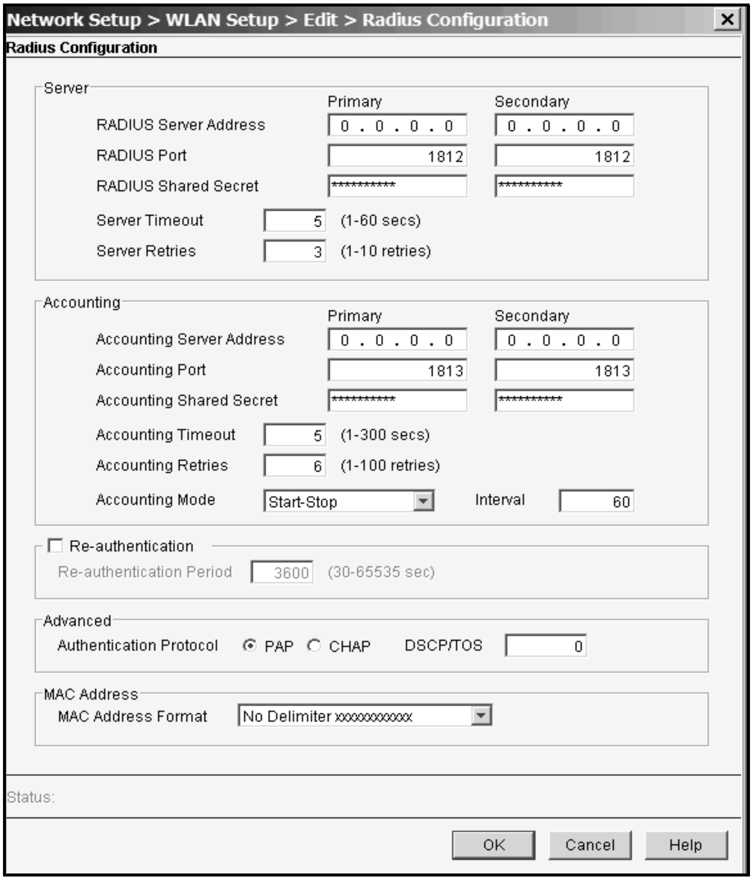
MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-28. Enabling MAC Authentication

2. Under **Authentication**, select **MAC Authentication**.

3. This authentication option requires a RADIUS server to act as the authentication server. Click the **Radius Config** button at the bottom of the screen. The **Radius Configuration** screen is displayed.



Network Setup > WLAN Setup > Edit > Radius Configuration

Radius Configuration

Server

	Primary	Secondary
RADIUS Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
RADIUS Port	1812	1812
RADIUS Shared Secret	***********	***********

Server Timeout 5 (1-60 secs)

Server Retries 3 (1-10 retries)

Accounting

	Primary	Secondary
Accounting Server Address	0 . 0 . 0 . 0	0 . 0 . 0 . 0
Accounting Port	1813	1813
Accounting Shared Secret	***********	***********

Accounting Timeout 5 (1-300 secs)

Accounting Retries 6 (1-100 retries)

Accounting Mode Start-Stop Interval 60

□ Re-authentication

Re-authentication Period 3600 (30-65535 sec)

Advanced

Authentication Protocol ● PAP ○ CHAP DSCP/TOS 0

MAC Address

MAC Address Format No Delimiter xxxxxxxxxxxx

Status:

Figure 4-29. Radius Configuration Screen for MAC Authentication

4. In the **Radius Configuration** screen, under **Server**, specify settings for your network's RADIUS servers.

   Enter settings for your primary server in the fields in the **Primary** column:

   a. In the **RADIUS Server Address** field, specify the IP address of your network's primary RADIUS server.

      To use the module's internal server, enter 127.0.0.1.

   b. Leave the **RADIUS Port** field at the default value unless you know that your server uses a different port.

      The default value is 1812.

c. In the **RADIUS Shared Secret** field, enter a character string up to 127 characters.

The RADIUS server uses the secret to identify the Wireless Edge Services xl Module as a legitimate client. You must match the secret configured for the module in your RADIUS server's configuration.

If you are using the module's internal server, you do not need to enter a shared secret.

d. Optionally, enter settings for a secondary RADIUS server in the fields in the **Secondary** column.

5. Optionally, alter other RADIUS server settings:

   - Enter a value in the **Server Timeout** to control how long the Wireless Edge Services xl Module will wait for a reply from the RADIUS server.

     The **Server Timeout** can be from 1 to 60 seconds, and the default setting is 5 seconds.

   - Enter a value in the **Server Retries** fields to control how many times the module will reattempt to contact a server that does not reply.

     The setting for **Server Retries** can be from 1 to 10. By default, the value is 3; Wireless Edge Services xl Module attempts to contact the server up to four times (one initial try and three subsequent tries).

6. Check the **Re-authentication** box if you want to force stations to periodically re-authenticate to the network. Specify how often (in seconds) stations must re-authenticate in the **Re-authentication Period** field.

   Re-authentication occurs in the background. By default, re-authentication is disabled, but if you enable it, the default period is one hour (3600 seconds). The valid range is 30 to 65535 seconds.

7. Choose the RADIUS protocol in which the Wireless Edge Services xl Module packages the MAC address. Select **PAP** (the default) or **CHAP** for the **Authentication Protocol**.

8. Optionally, enter a value in the DSCP/TOS field to prioritize traffic to the RADIUS server.

   Valid values range from 0 through 63.

9. In the **MAC Address** section, choose the format in which the Wireless Edge Services xl Module forwards the MAC address.

   The module sends the station's MAC address as the username and the password in the RADIUS request. The username and password must match exactly those in the account against which the RADIUS server checks them. For example, if the account uses delimiters in the MAC address, the module must use delimiters in the same places.

   Choose from among five options for the format:

   - **No Delimiter (xxxxxxxxxxxx)**
   - **Multi Colon (xx:xx:xx:xx:xx:xx)**
   - **Multi Dash (xx-xx-xx-xx-xx-xx)**
   - **Quad Dot (xxxx.xxxx.xxxx)**
   - **Single Dash (xxxxxx-xxxxxx)**

10. Click the **OK** button.

11. If you want to use encryption, you should now configure the encryption option. See "Configuring Encryption" on page 4-48.

Configuring Encryption

Encryption ensures the privacy of data sent through the wireless medium. Even if hackers intercept packets, they cannot decrypt them without the correct key.

The WLANs controlled by the Wireless Edge Services xl Module can support any of these encryption standards, listed from least secure to most secure:

- Wired Equivalent Privacy (WEP) with a 64-bit
- WEP with a 128-bit key
- Wi-Fi Protected Access (WPA)/WPA2 with Temporal Key Integrity Protocol (TKIP)
- WPA2 with Advanced Encryption Standard (AES)

No matter which type of authentication you select, you can select any type of encryption. You can select both WPA/WPA2-TKIP and WPA2-AES at the same time. However, all other encryption options are mutually exclusive.

If your WLAN does not use authentication, the encryption option enforces a de facto authentication: the user must enter the correct encryption key in order to connect to the WLAN. However, this form of authentication is less secure, particularly when used with WEP.

Table 4-2 displays the names that this management and configuration guide uses for combinations of authentication and encryption options.

Table 4-2. Encryption and Authentication Options

Authentication	Encryption	Called
None	WEP (64-bit or 128-bit)	Static WEP
	WPA/WPA2 TKIP	WPA/WPA2 with preshared keys (PSK)
	WPA2 AES	WPA2-PSK
MAC authentication	None	RADIUS MAC authentication
	WEP (64-bit or 128-bit)	RADIUS MAC authentication and static WEP
	WPA/WPA2 TKIP	RADIUS MAC authentication and WPA/WPA2-PSK
	WPA2 AES	RADIUS MAC authentication and WPA2-PSK
802.1X	WEP (64-bit or 128-bit)	Dynamic WEP
	WPA/WPA2 TKIP	WPA/WPA2 with 802.1X
	WPA2 AES	WPA2 with 802.1X (802.11i standard)
Web-Auth	None	Web-Auth
	WEP (64-bit or 128-bit)	Web-Auth and static WEP
	WPA/WPA2 TKIP	Web-Auth and WPA/WPA2-PSK
	WPA2 AES	Web-Auth

Configuring Static WEP Encryption (No Authentication). If you enable WEP encryption without authentication, WEP keys both encrypt wireless traffic and provide rudimentary authentication. You set the WEP key manually; wireless users must enter the same key before they can connect to the WLAN. This security option is sometimes called static WEP because you set the key manually.

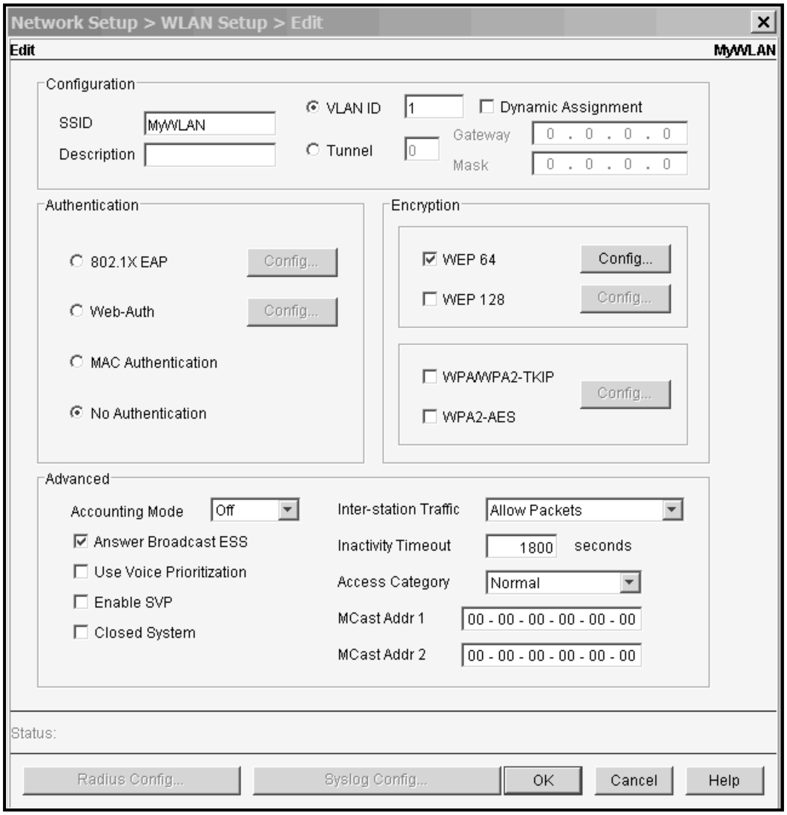
Note

By default, all WLANs use open-key authentication for WEP, which means that all stations can associate. However, the Wireless Edge Services xl Module quietly drops any incorrectly encrypted frames, ensuring that only stations that have the correct key can forward data and truly connect to the WLAN.

An alternative to open-key authentication, shared-key authentication, has been denigrated because it leaks information about the WEP key. You should only use this option if required by your stations. See “Configuring Global WLAN Settings” on page 4-76 for information on enabling shared-key authentication.

To configure static WEP, complete these steps:

1. Access the **Edit** screen for the WLAN that is to use static WEP:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed. (See Figure 4-30.)



Network Setup > WLAN Setup > Edit

Edit — MyWLAN

Configuration

SSID: MyWLAN

Description:

● VLAN ID: 1 □ Dynamic Assignment

○ Tunnel: 0 Gateway: 0 . 0 . 0 . 0 Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

○ MAC Authentication

● No Authentication

Encryption

☑ WEP 64

□ WEP 128

□ WPA/WPA2-TKIP

□ WPA2-AES

Advanced

Accounting Mode: Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic: Allow Packets

Inactivity Timeout: 1800 seconds

Access Category: Normal

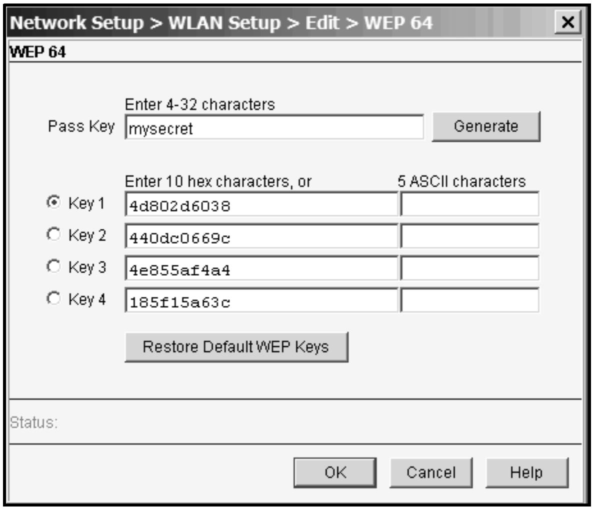
MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-30. Configuring WEP Encryption with No Authentication

2. Under **Authentication**, select **No Authentication**.
3. Under **Encryption**, check either the **WEP 64** or **WEP 128** box.
4. Click the corresponding **Config** button. The **WEP 64** or **WEP 128** screen is displayed.



Network Setup > WLAN Setup > Edit > WEP 64

WEP 64

Enter 4-32 characters

Pass Key mysecret

Enter 10 hex characters, or 5 ASCII characters

● Key 1 4d802d6038

○ Key 2 440dc0669c

○ Key 3 4e855af4a4

○ Key 4 185f15a63c

Status:

Figure 4-31. Configuring a Static WEP Key

5. Specify the static key.

   The Wireless Edge Services xl Module provides several options for configuring static keys:

   - It can automatically generate four hex keys from a manually entered pass key.

     Enter a string from 4 to 32 characters in the **Pass Key** field and click the **Generate** button.

     As shown in Figure 4-31, the Wireless Edge Services xl Module then creates four different keys, which automatically appear in the **Key** fields. Note that these keys are in hexadecimal. Wireless users can enter the keys in this form, or you can convert the hex number to an ASCII string and tell users that string.

   - You can manually enter up to four hex keys.
   - You can manually enter up to four ASCII keys.

     If you want to set one or more of the four keys yourself, simply move your cursor to the field for that key and enter the key. You can enter the key in hexadecimal (the first field) or in ASCII (the second field). If you want, you can specify some keys in hexadecimal and others in ASCII. You can also generate four keys from a pass key, and then change one or more of the keys.

The number of characters for the key depends on the WEP key length and on the format in which you enter the key. Table 4-3 summarizes these requirements.

Table 4-3. Key Length for Static WEP Keys

Key Length	Format	Characters
64-bit	Hexadecimal	10
	ASCII	5
128-bit	Hexadecimal	26
	ASCII	13

The key next to the selected circle (**Key 1** in Figure 4-31) is the key that currently encrypts and decrypts data. For greater security, remember to periodically change which key is in use.

Note

The more often an encryption key is used, the more vulnerable it is to hackers. Even when administrators diligently rotate and change WEP keys, this form of WEP is significantly less secure than WEP with 802.1X authentication or WPA/WPA2.

6. If you want to return this WLAN to the default static WEP keys, click the **Restore Default WEP Keys** button.

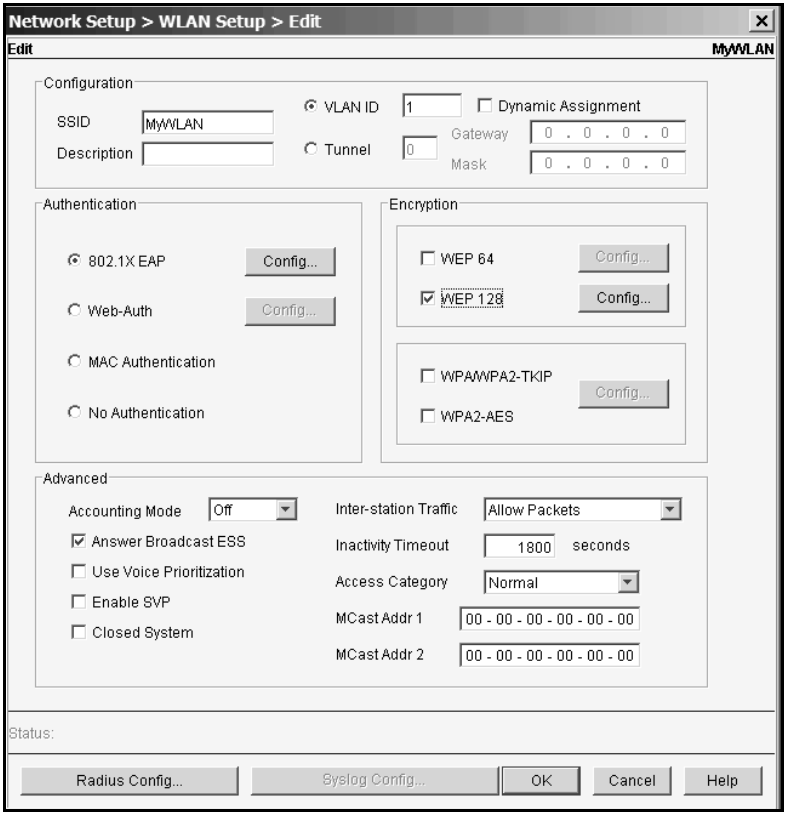
   Another screen is displayed, asking you to confirm the return to the default keys. If you are sure, click **Yes**. You still have one more chance to change your mind. The keys do not return to the defaults until you click the **OK** button and close the screen. You can view the default values for WEP keys through the CLI by entering this command: **show running-config include-factory**.

7. After you set the key, click the **OK** button. Then click the **OK** button on the WLAN's **Edit** screen to apply the settings.

Configuring WEP Encryption with 802.1X Authentication (Dynamic WEP). WEP with 802.1X authentication is also called dynamic WEP because 802.1X helps to distribute encryption keys automatically. The Wireless Edge Services xl Module and stations encrypt and decrypt data with WEP keys; however, instead of every station using the same key, stations first identify themselves to a network authentication server. When a station passes the authentication test, the station and the authentication server generate a unique WEP key for that session alone, which the server passes to the module.

To configure this type of security for a WLAN, complete these steps:

1. Access the **Edit** screen for the WLAN that is to use dynamic WEP:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed. (See Figure 4-30.)
2. Enable 802.1X authentication and specify the RADIUS server. (See "802.1X EAP" on page 4-35.)
3. On the WLAN's **Edit** screen, under **Encryption**, check either the **WEP 64** or **WEP 128** box, as shown in Figure 4-32.



Network Setup > WLAN Setup > Edit

Edit — MyWLAN

Configuration
- SSID: MyWLAN
- Description:
- ● VLAN ID: 1
- □ Dynamic Assignment
- ○ Tunnel: 0
- Gateway: 0 . 0 . 0 . 0
- Mask: 0 . 0 . 0 . 0

Authentication
- ● 802.1X EAP
- ○ Web-Auth
- ○ MAC Authentication
- ○ No Authentication

Encryption
- □ WEP 64
- ☑ WEP 128
- □ WPA/WPA2-TKIP
- □ WPA2-AES

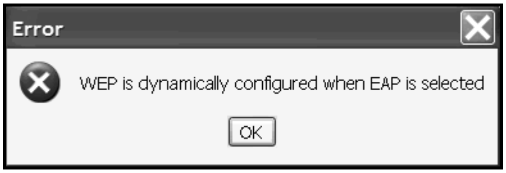
Advanced
- Accounting Mode: Off
- ☑ Answer Broadcast ESS
- □ Use Voice Prioritization
- □ Enable SVP
- □ Closed System
- Inter-station Traffic: Allow Packets
- Inactivity Timeout: 1800 seconds
- Access Category: Normal
- MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
- MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-32. Specifying WEP Encryption with 802.1X Authentication (Dynamic WEP)

Do *not* select the **Config** button to configure the WEP key; the RADIUS server automatically generates and sends the dynamic WEP keys to successfully authenticated users.

If you click the **Config** button, the message in Figure 4-33 is displayed. The message does not indicate a problem: it simply informs you that you have completed all necessary steps for configuring encryption on this WLAN.



Error

WEP is dynamically configured when EAP is selected

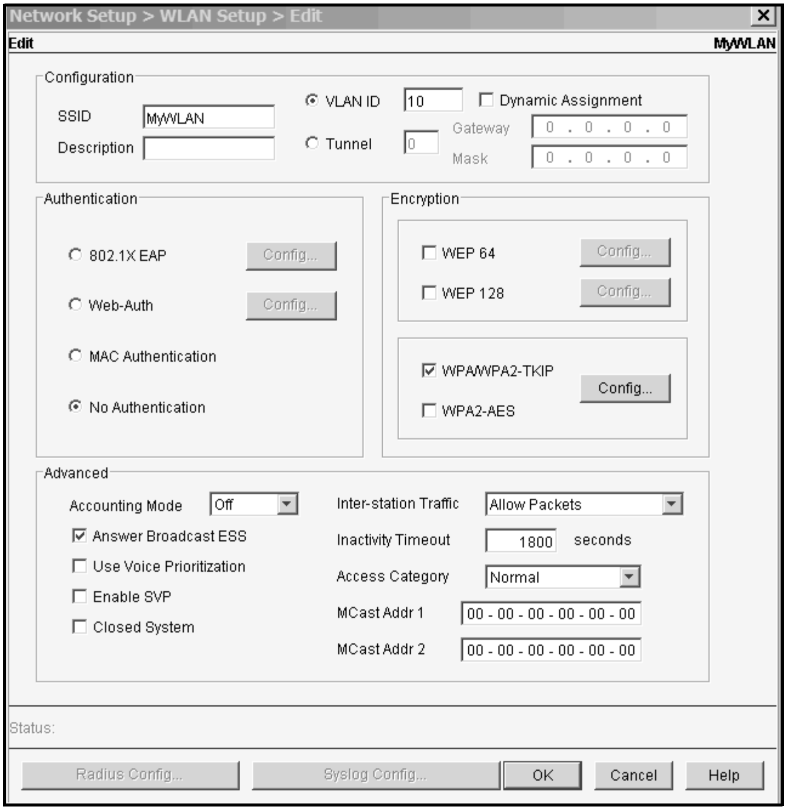
Figure 4-33. No Need to Configure WEP Keys When the WLAN Uses 802.1X

Configuring WPA/WPA2 with 802.1X. WPA and WPA2 are similar standards, both of which provide more robust encryption than WEP and rely on 802.1X authentication. Both standards generate hierarchies (or sets) of encryption keys. In the key hierarchy, each station has its own pairwise key, which the Wireless Edge Services xl Module also knows. All stations in the same WLAN use the same group key for multicast and broadcast traffic. WPA uses TKIP for the key hierarchy and WPA2 uses CCMP with AES encryption.

To configure WPA/WPA2, you must select the protocol: TKIP, AES, or both. AES is the most secure form of encryption and the one specified by WPA2 and 802.11i. However, not all stations support AES encryption.

In the **Edit** screen for a WLAN, as shown in Figure 4-34, the two options for WPA/WPA2 encryption are listed as:

- WPA/WPA2-TKIP
- WPA2-AES



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 10 □ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP Config...

○ Web-Auth Config...

○ MAC Authentication

● No Authentication

Encryption

□ WEP 64 Config...

□ WEP 128 Config...

☑ WPA/WPA2-TKIP Config...

□ WPA2-AES

Advanced

Accounting Mode Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic Allow Packets

Inactivity Timeout 1800 seconds

Access Category Normal

MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-34. Configuring WPA/WPA2 Encryption

Table 4-4 displays the types of stations supported by each option. It also lists which protocols each option uses to generate group (multicast and broadcast) keys and to generate pairwise (per-session) keys.

Table 4-4. Options for WPA/WPA2

Encryption Option	Multicast and Broadcast Keys	Per-Session Keys	Supported Stations
WPA/WPA2 TKIP	TKIP	TKIP	• WPA-enabled stations • WPA2-enabled stations
WPA2 AES	AES	AES	• WPA-enabled stations with support for AES • WPA2-enabled stations
WPA/WPA2 TKIP and WPA2 AES	TKIP	TKIP or AES	• WPA-enabled stations • WPA2-enabled stations

Note that WPA2-enabled stations can connect to a WLAN that uses any of these options. By default, WPA2 stations can use TKIP to associate to a WLAN. You can turn off this option in the CLI, but typically should not.

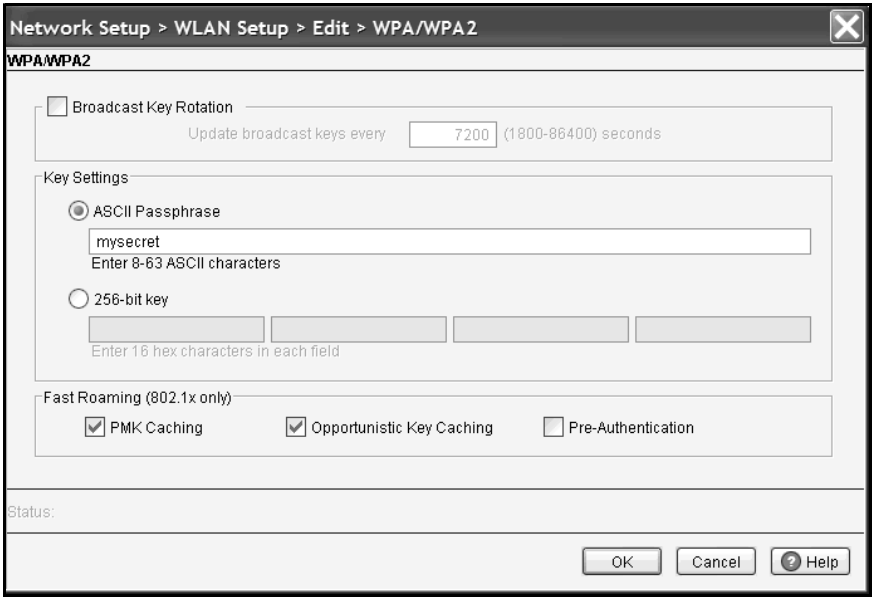
WPA-enabled stations can only connect to a WPA2 AES WLAN if they have software to support AES encryption.

To configure WPA/WPA2 encryption, complete these steps:

1. Access the **Edit** screen for the WLAN that is to use WPA/WPA2 with 802.1X:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed. (See Figure 4-30.)
2. Under **Authentication**, select **802.1X EAP**.
3. Under **Encryption**, select your encryption protocol:
   - To use TKIP, check the **WPA/WPA2-TKIP** box.

     The Wireless Edge Services xl Module and wireless stations will use TKIP for all encryption. Note that both WPA and WPA2 stations can connect, but WPA2 stations will use TKIP.
   - To use AES, check the **WPA2-AES** box.

     This option forces all wireless stations to use AES, the most secure algorithm used for wireless encryption.
   - To allow both protocols (mixed-mode), check both boxes.
4. If you want, you can also configure advanced options.
   a. Click the **Config** button in the WPA section of the **Edit** screen. The **WPA/WPA2** screen is displayed.



Network Setup > WLAN Setup > Edit > WPA/WPA2

WPA/WPA2

□ Broadcast Key Rotation

Update broadcast keys every 7200 (1800-86400) seconds

Key Settings

● ASCII Passphrase

mysecret

Enter 8-63 ASCII characters

○ 256-bit key

Enter 16 hex characters in each field

Fast Roaming (802.1x only)

☑ PMK Caching ☑ Opportunistic Key Caching □ Pre-Authentication

Status:

Figure 4-35. Advanced Options for WPA/WPA2

b. If you want, check the **Broadcast Key Rotation** box.

Because all stations must use the same broadcast key, this key is clearly more vulnerable to hackers than the per-session keys. Periodically changing the broadcast key helps to protect your WLAN.

By default, the Wireless Edge Services xl Module does not rotate the broadcast key. However, if you enable the feature, the default rotation period is every 7,200 seconds (two hours).

In the **Update broadcast keys every** field, you can enter any value from 60 seconds (one minute) through 86,400 seconds (one day). The shorter the rotation period, the more secure, but also the more overhead added by the key redistribution.

c. You can also enable fast roaming features (to speed roaming with 802.1X).

A station might roam back and forth between several RPs. Ideally, such roaming is hidden from the wireless user, who need not know when he or she connects to a new RP, but only that the wireless connection remains good.

Fast roaming speeds authentication to a new RP, which can be the most time-consuming phase of the roam, so it only applies to WLANs that use 802.1X authentication.

Check these boxes to enable the Wireless Edge Services xl Module's fast roaming capabilities:

- **PMK Caching**—The RP and the wireless station agree on a PMK identifier for their session, which each stores even after the station disassociates. If the wireless station roams back to the RP, the two can quickly exchange the PMK identifier and renegotiate necessary keys, instead of completing the entire authentication process.
- **Opportunistic Key Caching**—This capability further speeds roaming between RPs that are connected to the same module. The wireless station can use the same PMK to associate to any RP that connects to the module.
- **Pre-Authentication**—Pre-authentication speeds roaming for stations that move from an RP on a *different* Wireless Edge Services to an RP on *this* module.

  The station must also support pre-authentication. It listens for beacons from other RPs that support its SSID and authenticates to them before it roams. The station sends its EAP messages through its current RP, and that RP's module broadcasts the EAP messages throughout the wired network. Pre-authentication allows your module to listen for and respond to EAP messages destined to its RPs. The module must be on the same subnetwork as the original module to receive the EAP messages.

d. After you have configured all the advanced options that you desire, click the **OK** button.

5. Click the **OK** button.

Configuring WPA/WPA2-PSK. As noted above, WPA/WPA2 typically requires 802.1X authentication. However, for networks that do not have a RADIUS server, you can set a password, or preshared key, instead of enforcing 802.1X. All users must enter this same preshared key to connect to the WLAN.

Although a preshared key is less secure than 802.1X authentication, the WPA/WPA2 encryption is still quite strong. WPA/WPA2-PSK is a far better option than static WEP for small to medium networks.

For more information on WPA/WPA2 encryption, see the introduction to "Configuring WPA/WPA2 with 802.1X" on page 4-55. To configure WPA/WPA-PSK on a WLAN complete these steps:

1. Access the **Edit** screen for the WLAN that is to use WPA/WPA2-PSK:

   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.

   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed. (See Figure 4-30.)

2. Under **Authentication**, select **No Authentication**.

3. Under **Encryption**, select your encryption protocol:

   - To use TKIP, check the **WPA/WPA2-TKIP** box.

     The Wireless Edge Services xl Module and wireless stations will use TKIP for all encryption. Note that both WPA and WPA2 stations can connect, but WPA2 stations will use TKIP.

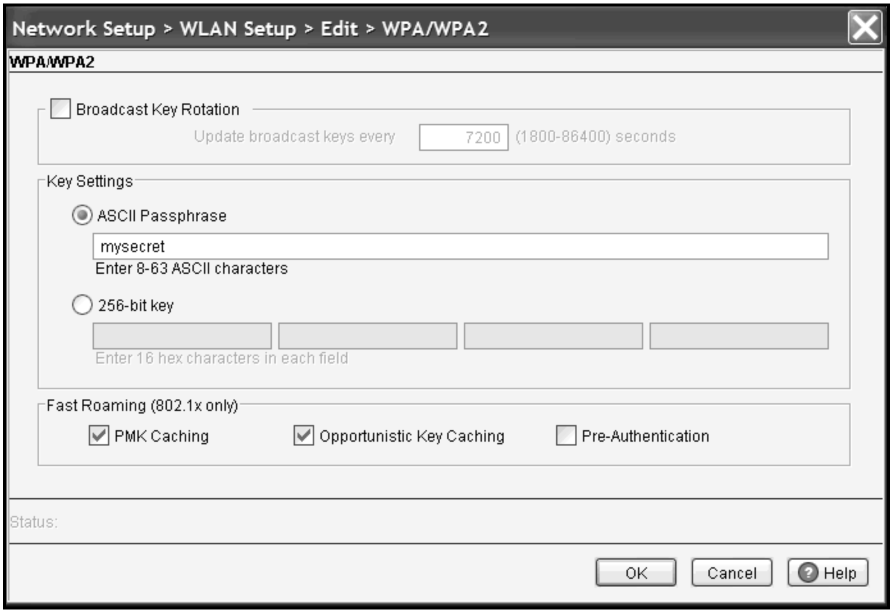
   - To use AES, check the **WPA2-AES** box.

     This option forces all wireless stations to use AES, the most secure algorithm used for wireless encryption.

   - To allow both protocols (mixed-mode), check both boxes.

4. Specify the preshared key that users must enter to connect to the WLAN.

   a. Click the **Config** button next to the WPA encryption options. The **WPA/WPA2** screen is displayed.



Network Setup > WLAN Setup > Edit > WPA/WPA2

WPA/WPA2

□ Broadcast Key Rotation

Update broadcast keys every 7200 (1800-86400) seconds

Key Settings

● ASCII Passphrase

mysecret

Enter 8-63 ASCII characters

○ 256-bit key

Enter 16 hex characters in each field

Fast Roaming (802.1x only)

☑ PMK Caching ☑ Opportunistic Key Caching □ Pre-Authentication

Status:

Figure 4-36. Configuring a Key for WPA/WPA2 Encryption with No Authentication

b. Enter the preshared key.

As always, you should select a key that conforms to the highest security standards. The longer the key and the more special characters it contains, the more secure it is. (The key must be at least 22 characters to withstand a brute force attack.)

You can enter the key in one of two ways:

– Select **ASCII Passphrase**, and then enter a password of from 8 to 63 characters. Users must enter the same characters to access the WLAN.

– Select **256-bit key**, and then enter the key manually in hexadecimal. Enter 16 characters in each of the four fields.

5. If you want, check the **Broadcast Key Rotation** box.

   Because all stations must use the same broadcast key, this key is clearly more vulnerable to hackers than the per-session keys. Periodically changing the broadcast key helps to protect your WLAN.

   By default, the Wireless Edge Services xl Module does not rotate the broadcast key. However, if you enable the feature, the default rotation period is every 7,200 seconds (two hours).

   In the **Update broadcast keys every** field, you can enter any value from 60 seconds (one minute) through 86,400 seconds (one day). The shorter the rotation period, the more secure, but also the more overhead added by the key redistribution.

6. Click the **OK** button to apply your settings and close the **WPA/WPA2** screen.

7. Click the **OK** button in the WLAN's **Edit** screen to apply your settings.

Configuring Encryption for a WLAN that Uses MAC Authentication. A WLAN that enforces MAC authentication to a network server can also provide wireless encryption. In this case, a wireless user must pass two tests to connect to the WLAN: the user's station must pass MAC authentication, and the user must enter the correct WEP or WPA/WPA2 key.

This section explains how to add encryption to a WLAN already configured for RADIUS MAC authentication. See "MAC Authentication" on page 4-44 for instructions on configuring the authentication.

After selecting **MAC Authentication** in a WLAN's **Edit** screen, you have several choices for which boxes in the **Encryption** section to check. Table 4-5 summarizes these options and refers you to section that explains how to configure the second security option.

Table 4-5. Encryption Options for RADIUS MAC Authentication

Encryption Option	Security Option	Reference
WEP 64	static WEP	"Configuring Static WEP Encryption (No Authentication)" on page 4-49
WEP 128	static WEP	"Configuring Static WEP Encryption (No Authentication)" on page 4-49
WPA/WPA2-TKIP	WPA/WPA2-PSK	"Configuring WPA/WPA2-PSK" on page 4-59
WPA2-AES	WPA2-PSK	"Configuring WPA/WPA2-PSK" on page 4-59
WPA/WPA2-TKIP and WPA2-AES	WPA/WPA2-PSK	"Configuring WPA/WPA2-PSK" on page 4-59

Configuring Encryption for a WLAN that Uses Web-Auth. Web-Auth occurs after a station connects to the WLAN and, by itself, provides no encryption.

To protect the users' data within the wireless network, you can add WEP or WPA/WPA2 encryption. In this case, users must first enter a WEP or WPA key to connect to the WLAN. Then, when they attempt to access a Web site, they must submit their username and password for Web-Auth.

See "Web-Auth" on page 4-40 or *Chapter 5: Web Authentication for Mobile Users* for instructions on configuring the authentication. After selecting **Web-Auth** in a WLAN's **Edit** screen, you have several choices for which boxes in the **Encryption** section to check. Table 4-6 summarizes these options and refers you to section that explains how to configure the second security option.

Table 4-6. Encryption Options for Web-Auth

Encryption Option	Security Option	Reference
WEP 64	static WEP	"Configuring Static WEP Encryption (No Authentication)" on page 4-49
WEP 128	static WEP	"Configuring Static WEP Encryption (No Authentication)" on page 4-49
WPA/WPA2-TKIP	WPA/WPA2-PSK	"Configuring WPA/WPA2-PSK" on page 4-59
WPA2-AES	WPA2-PSK	"Configuring WPA/WPA2-PSK" on page 4-59
WPA/WPA2-TKIP and WPA2-AES	WPA/WPA2-PSK	"Configuring WPA/WPA2-PSK" on page 4-59

Configuring Advanced WLAN Settings

In the **Advanced** section of a WLAN's **Edit** screen, you can establish more specialized settings for a WLAN.

This section will explain how to configure:

- control over inter-station traffic
- closed system operations
- inactivity timeouts

You will learn how to configure other advanced settings, which deal with QoS capabilities, in "Traffic Management (QoS)" on page 4-90.

Controlling Inter-Station Traffic

Often, a wireless network serves simply to connect mobile users to your Ethernet network or to the Internet. In this case, wireless stations primarily need to communicate with the Wireless Edge Services xl Module and servers in the wired network; they do not need to communicate with other wireless stations. However, by default they are allowed to do so (albeit through their RPs since infrastructure mode requires that wireless stations send all traffic to the RP).

For increased security, you can prevent two wireless stations in a particular WLAN from communicating with each other. You have three options for controlling wireless station-to-station traffic in a particular WLAN:

- allow all inter-station traffic

  When a wireless station attempts to communicate with another station in the WLAN, the Wireless Edge Services xl Module forwards the packet toward the second station's RP.

- drop all inter-station traffic

  When a wireless station attempts to communicate with another station in the WLAN, the Wireless Edge Services xl Module drops the packet.

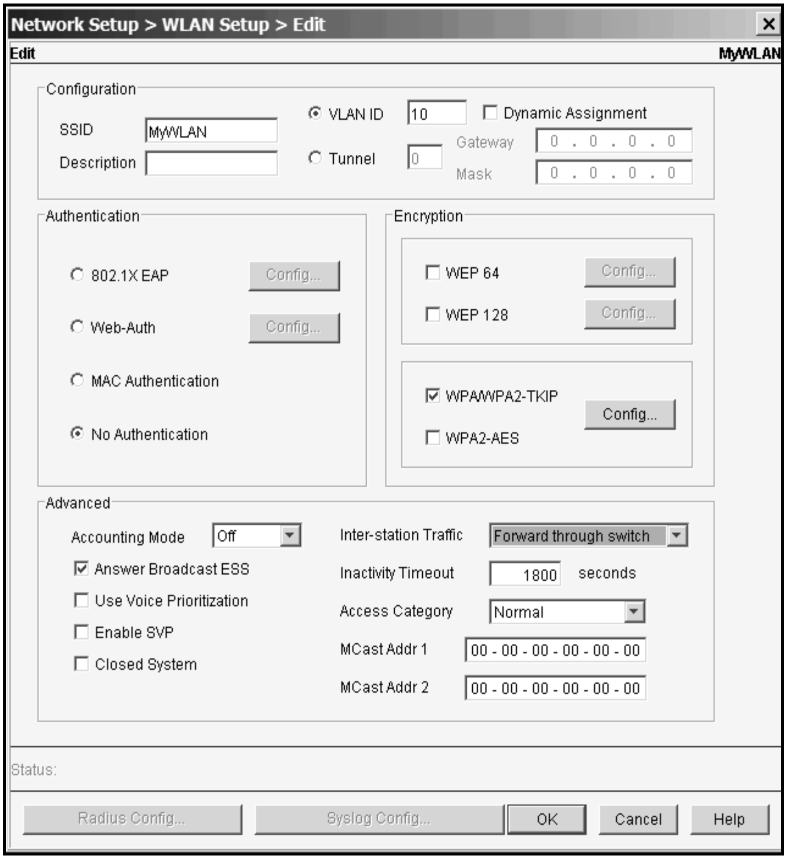
- forward inter-station traffic through the switch

  This option allows inter-station traffic but ensures that it complies with your network policies. When a wireless station attempts to communicate with another station in the WLAN, the Wireless Edge Services xl Module forwards the traffic into the wired network in the VLAN configured for that WLAN (or in the user's dynamic VLAN). The wireless services-enabled switch enforces any applicable access controls and sends the packet back to the module to be forwarded to toward the second station's RP.

To enable inter-station blocking on a WLAN, complete these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
2. In the **Inter-station Traffic** drop-down menu under **Advanced**, choose how the module treats inter-station traffic:
   - **Drop packets**
   - **Allow Packets**
   - **Forward through switch**

   The default setting is to allow inter-station traffic.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 10 □ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

○ MAC Authentication

● No Authentication

Encryption

□ WEP 64

□ WEP 128

☑ WPA/WPA2-TKIP

□ WPA2-AES

Advanced

Accounting Mode Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic Forward through switch

Inactivity Timeout 1800 seconds

Access Category Normal

MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-37. Controlling Inter-Station Traffic

3. Click the **OK** button.

Remember that this setting applies to a WLAN; it does not apply to an RP as a whole, which might associate with stations in several WLANs. If you want to prevent the Wireless Edge Services xl Module from forwarding traffic between wireless stations in different WLANs, you must configure this option for both WLANs.

Note

Remember to consider whether a RPs must forward traffic between devices such as Voice-over-WLAN (VoWLAN) phones.

Enabling Closed System Operations

Wireless stations have two ways that they can discover the SSID for a WLAN:

- RPs send beacons that include the SSID for the WLAN. All wireless stations listen for beacons.
- RPs answer probes from stations requesting the RP to send all SSIDs that it supports.

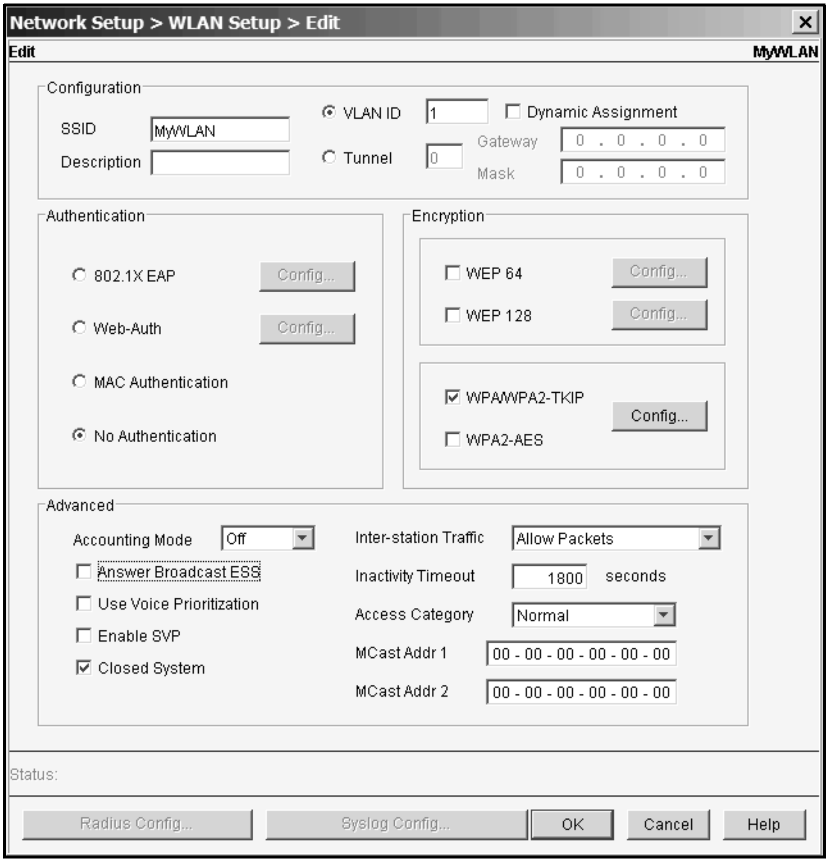
  RPs can only beacon the SSIDs for the four primary WLANs (with normal configuration, WLANs 1 through 4). This second option allows some wireless stations to automatically discover the SSID for the other WLANs as well.

To configure a WLAN to operate truly in closed system—that is prevent wireless stations from discovering the WLAN's SSID—you must disable both of the functions described above.

In the past, organizations have used closed system as a rudimentary security measure. However, widely available wireless sniffer software can detect SSIDs in management frames with already associated stations. Therefore, closed system deters only the most casual of unauthorized users. For true security, enable authentication and encryption as described in "Configuring Security Options" on page 4-34.

To configure a WLAN to operate in closed system, complete these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 1 □ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

○ MAC Authentication

● No Authentication

Encryption

□ WEP 64

□ WEP 128

☑ WPA/WPA2-TKIP

□ WPA2-AES

Advanced

Accounting Mode Off

□ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

☑ Closed System

Inter-station Traffic Allow Packets

Inactivity Timeout 1800 seconds

Access Category Normal

MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-38. Enabling Closed System

2. In the **Advanced** section, check the **Closed System** box.

3. Uncheck the **Answer Broadcast ESS** box to prevent RPs from telling wireless stations the SSID in response to probes.

4. Click the **OK** button.

Configuring the Inactivity Timeout

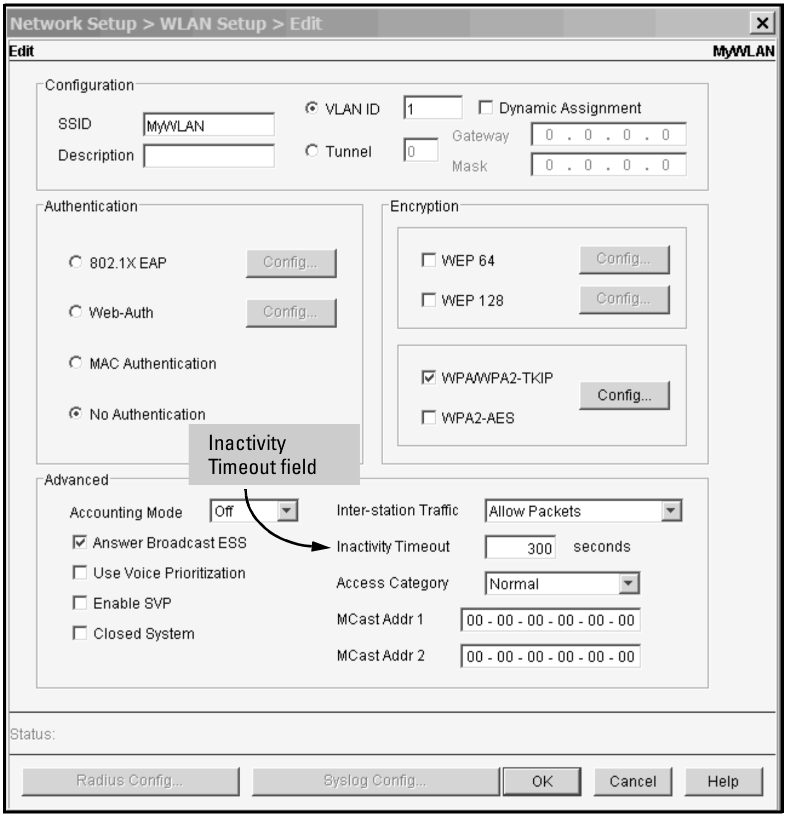
Users do not always bother to disconnect from wireless connections when they turn off or leave their stations. Although the user is no longer truly connected, the Wireless Edge Services xl Module continues to store the station's association. On an RP nearing its maximum number of stations, an unterminated association can prevent a new station from connecting to the wireless network. The unterminated association can also be a security risk, as an unauthorized user may access the station, and through it, the authorized user's connection.

The Wireless Edge Services xl Module forces stations that have been idle for a certain period of time to reassociate.

Note Stations handle the reassociation in the background; users may not even notice the process.

The inactivity timeout, which is the time that a station can be idle before reassociating, is configured for all stations on a particular WLAN. To set this time, complete these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.



Network Setup > WLAN Setup > Edit

Edit — MyWLAN

Configuration

SSID: MyWLAN

Description:

● VLAN ID: 1 □ Dynamic Assignment

○ Tunnel: 0 Gateway: 0 . 0 . 0 . 0 Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

○ MAC Authentication

● No Authentication

Encryption

□ WEP 64

□ WEP 128

☑ WPA/WPA2-TKIP

□ WPA2-AES

Advanced

Accounting Mode: Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic: Allow Packets

Inactivity Timeout: 300 seconds

Access Category: Normal

MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Inactivity Timeout field

Figure 4-39. Setting the Inactivity Timeout

2. Under **Advanced**, in the **Inactivity Timeout** field, enter a value from 60 seconds (one hour) through 86400 seconds (one day).

   The default timeout is 1800 seconds (30 minutes).

   In Figure 4-39, the administrator has lowered the timeout to 300 seconds (five minutes).

3. Click the **OK** button.

Configuring Accounting on a WLAN

The Wireless Edge Services xl Module can implement accounting on a WLAN—that is, track users' activity and consumption of network resources. Your company might analyze logs for security auditing and traffic management. Or your company might submit the reports to a billing server in order to charge users for wireless access.

You can configure the module to use these types of accounting:

- **syslog**—The Wireless Edge Services xl Module forwards logs about stations in this WLAN to a syslog server.
- **RADIUS**—The Wireless Edge Services xl Module sends messages to a RADIUS accounting server when a station connects or disconnects and, optionally, at universally throughout the connection. The messages include information such as the station's MAC address, the duration of the connection, and the network resources consumed.

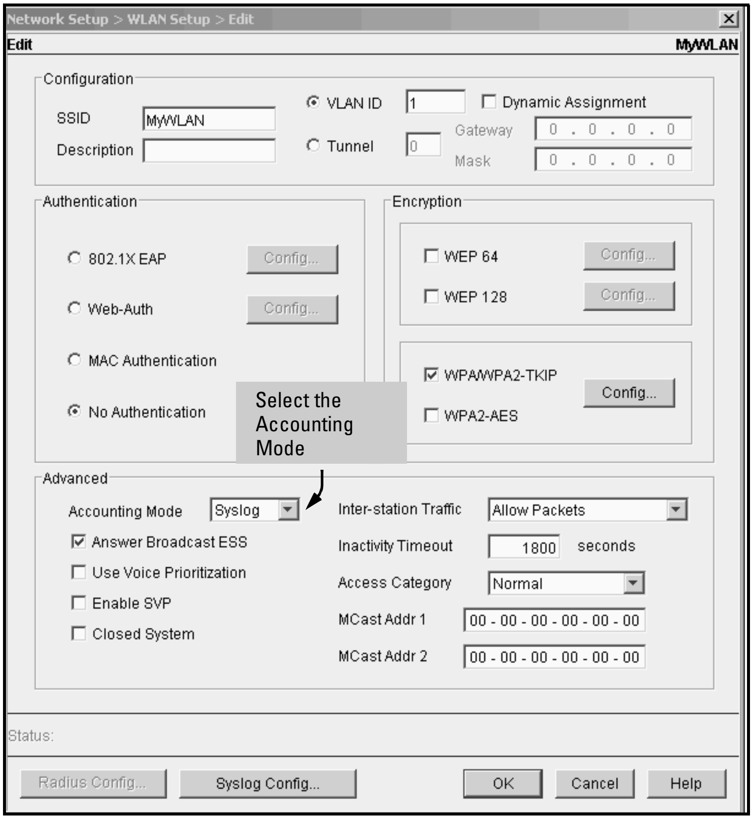
  The RADIUS accounting server can be an external server or the Wireless Edge Services xl Module's own internal RADIUS server. See *Chapter 11: RADIUS Server* for more information about this server.

  The WLAN on which you enable RADIUS accounting must also enforce authentication to a RADIUS server.

Enabling Logging to a Syslog Server on a WLAN

Follow these steps to enable the Wireless Edge Services xl Module to log WLAN activity to a syslog server:

1. Select **Network Setup** > **WLAN Setup** > **Configuration**.
2. Select the WLAN from the list and click the **Edit** button. The **Edit** screen for the WLAN is displayed.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 1

□ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

○ MAC Authentication

● No Authentication

Encryption

□ WEP 64

□ WEP 128

☑ WPA/WPA2-TKIP

□ WPA2-AES

Select the Accounting Mode

Advanced

Accounting Mode Syslog

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic Allow Packets

Inactivity Timeout 1800 seconds

Access Category Normal

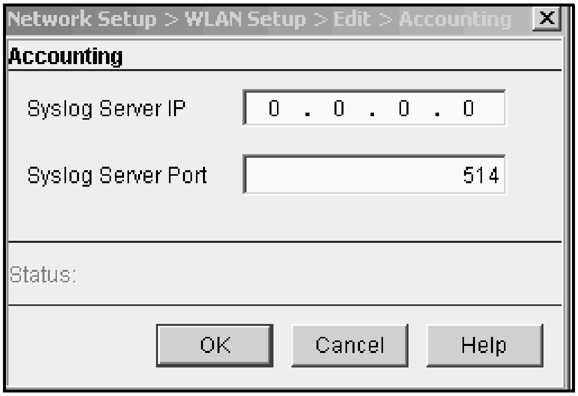
MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-40. Enabling Syslog Accounting on a WLAN

3. In the **Advanced** section, in the **Accounting Mode** field, use the drop-down menu to select **Syslog**.
4. Click the **Syslog Config** button. The **Accounting** screen is displayed.



Network Setup > WLAN Setup > Edit > Accounting

Accounting

Syslog Server IP: 0 . 0 . 0 . 0

Syslog Server Port: 514

Status:

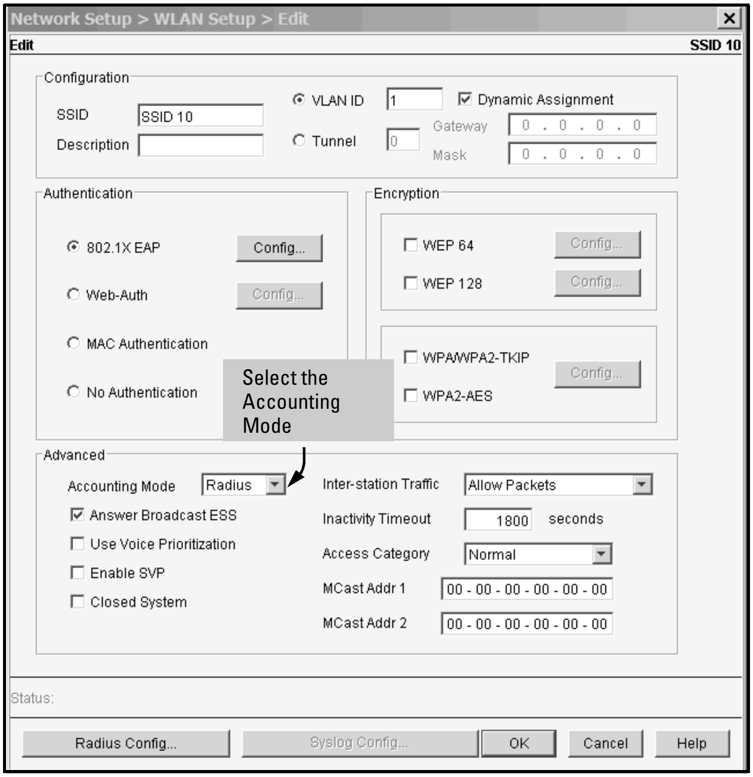
Figure 4-41. Specifying the Syslog Server

5. In the **Syslog Server IP** field, specify the Syslog server's IP address.
6. In the **Syslog Server Port** field, enter your server's UDP port or keep the default 514.
7. Click the **OK** button.
8. In the WLAN's **Edit** screen, click the **OK** button.
9. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Enabling RADIUS Accounting on a WLAN

To activate RADIUS accounting on a WLAN, follow these steps:

1. Select **Network Setup** > **WLAN Setup** > **Configuration**.
2. Select the WLAN from the list and click the **Edit** button. The **Edit** screen for the WLAN is displayed.



Network Setup > WLAN Setup > Edit

Edit — SSID 10

Configuration

SSID: SSID 10
Description:
● VLAN ID: 1
☑ Dynamic Assignment
○ Tunnel: 0
Gateway: 0 . 0 . 0 . 0
Mask: 0 . 0 . 0 . 0

Authentication

● 802.1X EAP
○ Web-Auth
○ MAC Authentication
○ No Authentication

Encryption

□ WEP 64
□ WEP 128
□ WPA/WPA2-TKIP
□ WPA2-AES

Advanced

Accounting Mode: Radius
☑ Answer Broadcast ESS
□ Use Voice Prioritization
□ Enable SVP
□ Closed System
Inter-station Traffic: Allow Packets
Inactivity Timeout: 1800 seconds
Access Category: Normal
MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

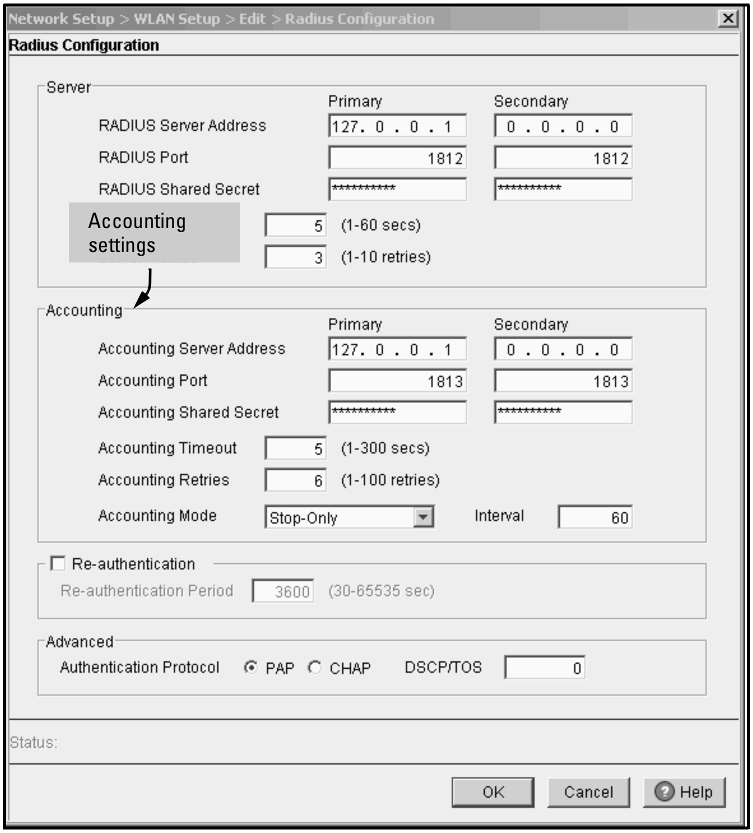
Select the Accounting Mode

Figure 4-42. Enabling RADIUS Accounting for a WLAN

3. In the **Advanced** section, in the **Accounting Mode** field, use the drop-down menu to select **Radius**.

   Users must authenticate to a RADIUS server for RADIUS accounting to function. Select **802.1X EAP**, **Web-Auth**, or **MAC Authentication** for the authentication method.

4. Click the **Radius Config** button. The **Radius Configuration** screen is displayed.



Network Setup > WLAN Setup > Edit > Radius Configuration

Radius Configuration

Server

	Primary	Secondary
RADIUS Server Address	127. 0 . 0 . 1	0 . 0 . 0 . 0
RADIUS Port	1812	1812
RADIUS Shared Secret	**********	**********

5 (1-60 secs)

3 (1-10 retries)

Accounting settings

Accounting

	Primary	Secondary
Accounting Server Address	127. 0 . 0 . 1	0 . 0 . 0 . 0
Accounting Port	1813	1813
Accounting Shared Secret	**********	**********

Accounting Timeout 5 (1-300 secs)

Accounting Retries 6 (1-100 retries)

Accounting Mode Stop-Only Interval 60

□ Re-authentication

Re-authentication Period 3600 (30-65535 sec)

Advanced

Authentication Protocol ● PAP ○ CHAP DSCP/TOS 0

Status:

Figure 4-43. Specifying the Accounting Server in the Radius Configuration Screen

To enforce RADIUS accounting, the WLAN must use 802.1X authentication, Web-Auth, or MAC authentication for the **Authentication** mode.

5. Configure settings for the primary accounting server in the **Primary** column of the **Accounting** section.

   a. Specify the server's IP address in the **Accounting Server Address** field.

      To use the Wireless Edge Services xl Module's internal server for accounting, enter 127.0.0.1.

   b. Enter your RADIUS accounting server's port in the **Accounting Port** field.

      Typically, leave the default port: 1813.

c. In the **Accounting Shared Secret** field, enter a string up to 127 characters long. (The string can include alphanumeric and special characters.)

   The accounting server uses the shared secret to verify that reports are from a legitimate source. The key you specify must match the key configured for the module in the accounting server's client configurations.

   If you are using the module's internal server, you don't need to specify a key.

6. Optionally, configure settings for a secondary server by completing the fields in the **Secondary** column of the **Accounting** section.

7. Optionally, alter the value in the **Accounting Timeout** field.

   This setting determines the length of time in seconds that the Wireless Edge Services xl Module waits for an acknowledgement from the accounting server. The default is five seconds, and the valid range is from 1 to 300 seconds. Raise the timeout if your network or accounting server is frequently busy.

8. Optionally, alter the value in the **Accounting Retries** field.

   If the module does not receive an acknowledgement from the accounting server, it resends the report. The default number of retries is 6, and the valid range is from 1 to 100.

   Re-sending reports ensures that users' activity is logged correctly—particularly important if your company charges for wireless service.

9. From the **Accounting Mode** drop-down menu, choose when the Wireless Edge Services xl Module sends a report:

   - **Start-Stop**—when a station connects to this WLAN and when it disconnects
   - **Stop-Only**—only when a station disconnects
   - **Start-Interim-Stop**—when a station connects to this WLAN, periodically for as long as the connection persists, and when the station closes the connection

10. If you have selected **Start-Interim-Stop** for the **Accounting Mode**, enter a value in the **Interval** field.

    This setting determines how often, in seconds, the module sends periodic reports on user activities. (It applies *only* when you select **Start-Interim-Stop**.) The default value is 60 seconds, and the valid range is from 60 to 3600 seconds (1 hour).

11. Click the **OK** button.
12. In the WLAN's **Edit** screen, click the **OK** button.
13. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

Configuring Global WLAN Settings

The ProCurve Wireless Edge Services xl Module also supports these features:

- **Proxy ARP**—With this feature enabled, the Wireless Edge Services xl Module responds to ARP requests on behalf of its wireless stations, reducing overhead in the wireless network. Proxy ARP is also necessary when you map a WLAN to a tunnel because a tunnel does not carry ARP traffic (see *Chapter 12: Configuring Tunnels with Generic Routing Encapsulation*).
- **Shared-key authentication**—Open and shared-key authentication apply to WLANs that use WEP encryption.

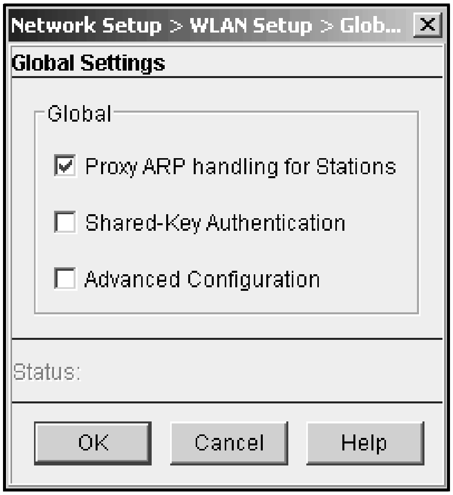
  Open-key authentication, which is the default for all WLANs on the module, allows stations to immediately associate to the RP. (However, they still must have the correct WEP key to properly send and receive data.)

  Shared-key authentication is an obsolete form of authentication requiring stations to prove that they have the WEP key before associating to the RP. This option is *not* recommended because it leaks information about the key.

You enable and disable these features for *all* WLANs on the Wireless Edge Services xl Module.

To configure global WLAN settings, complete these steps:

1. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
2. Click the **Global Settings** button. The **Global WLAN Settings** screen is displayed.



Network Setup > WLAN Setup > Glob...

Global Settings

Global

☑ Proxy ARP handling for Stations

□ Shared-Key Authentication

□ Advanced Configuration

Status:

Figure 4-44. Global WLAN Settings Screen

3. Check the boxes for the features that you want to enable.

Note The **Advanced Configuration** selection refers to how SSIDs are assigned to RP radios; see "Advanced Mode Configuration" on page 4-11.

4. Click the **OK** button.

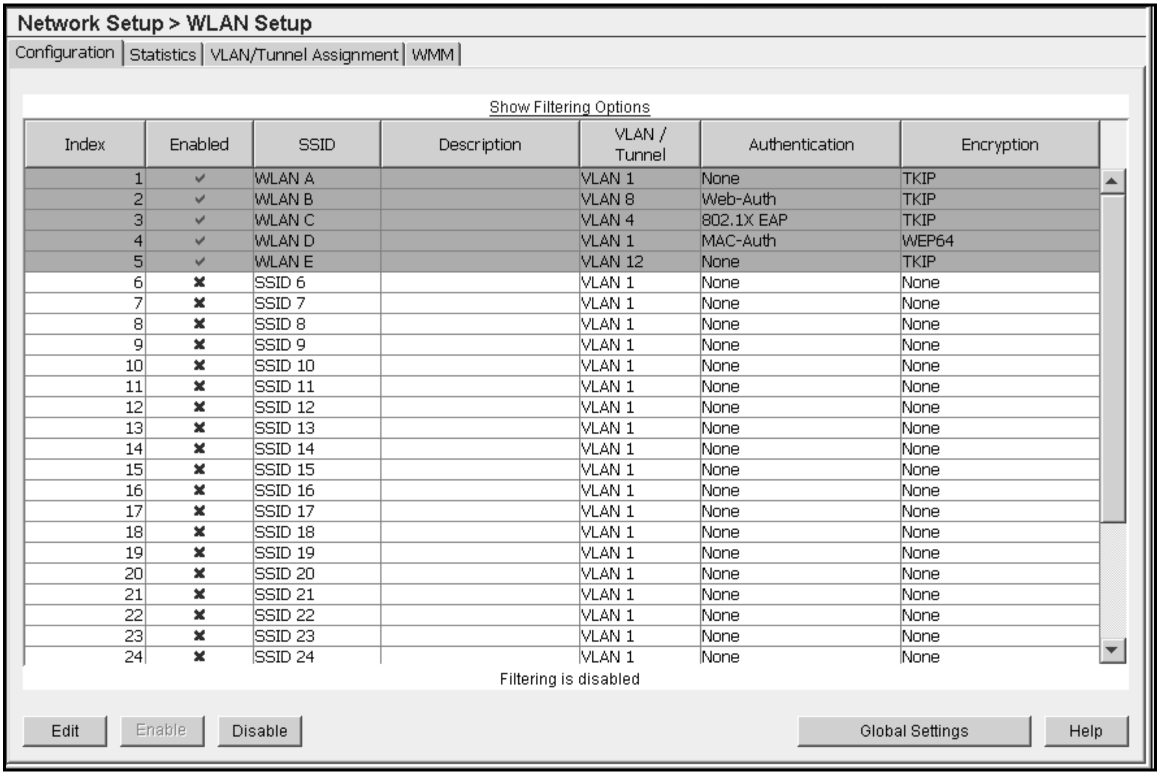
Enabling the WLAN

RPs in your wireless network will not support the WLAN until you enable it.

To enable the WLAN, complete these steps:

1. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
2. Select the WLAN that you want to enable. You can use the **<Ctrl>** key to select multiple WLANs.
3. Click the **Enable** button.

   The icon in the **Enabled** column should change from a red X to a green check mark, as shown in Figure 4-45.



Index	Enabled	SSID	Description	VLAN / Tunnel	Authentication	Encryption
1	✓	WLAN A		VLAN 1	None	TKIP
2	✓	WLAN B		VLAN 8	Web-Auth	TKIP
3	✓	WLAN C		VLAN 4	802.1X EAP	TKIP
4	✓	WLAN D		VLAN 1	MAC-Auth	WEP64
5	✓	WLAN E		VLAN 12	None	TKIP
6	✗	SSID 6		VLAN 1	None	None
7	✗	SSID 7		VLAN 1	None	None
8	✗	SSID 8		VLAN 1	None	None
9	✗	SSID 9		VLAN 1	None	None
10	✗	SSID 10		VLAN 1	None	None
11	✗	SSID 11		VLAN 1	None	None
12	✗	SSID 12		VLAN 1	None	None
13	✗	SSID 13		VLAN 1	None	None
14	✗	SSID 14		VLAN 1	None	None
15	✗	SSID 15		VLAN 1	None	None
16	✗	SSID 16		VLAN 1	None	None
17	✗	SSID 17		VLAN 1	None	None
18	✗	SSID 18		VLAN 1	None	None
19	✗	SSID 19		VLAN 1	None	None
20	✗	SSID 20		VLAN 1	None	None
21	✗	SSID 21		VLAN 1	None	None
22	✗	SSID 22		VLAN 1	None	None
23	✗	SSID 23		VLAN 1	None	None
24	✗	SSID 24		VLAN 1	None	None

Filtering is disabled

Figure 4-45. Enabling a WLAN

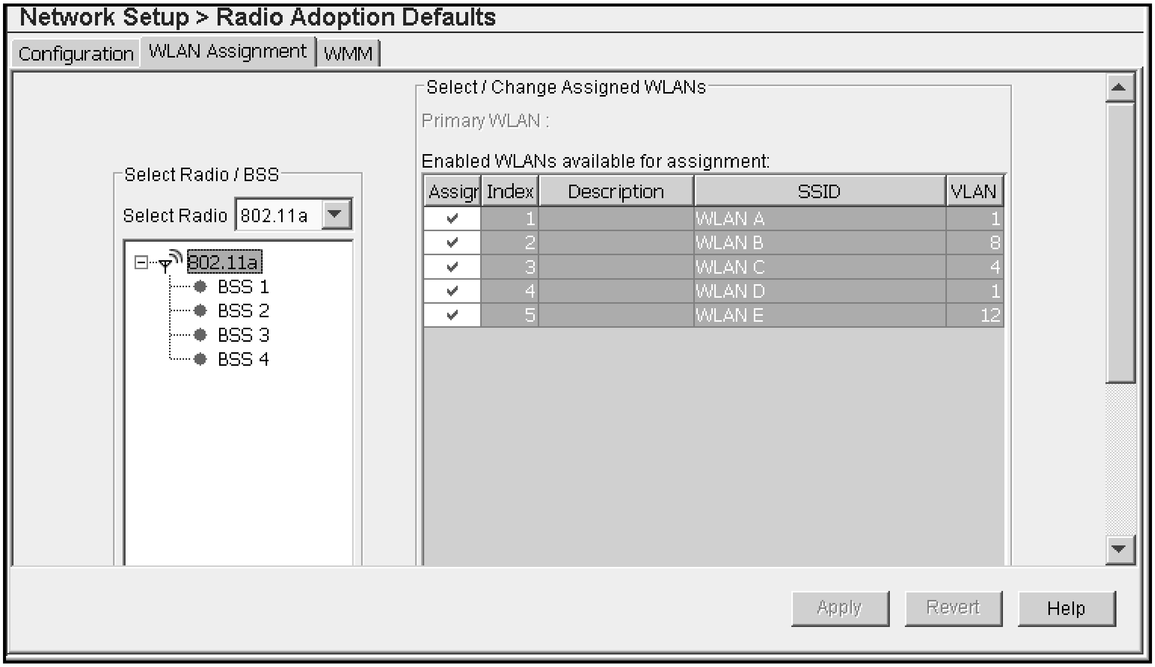
4. Click the **OK** button.

As long as you are operating in normal mode, all radios on all RPs that the Wireless Edge Services xl Module has adopted or will adopt support the enabled WLANs.

You can confirm that RPs are actually supporting the enabled WLANs by selecting **Network Setup** > **Radio** and checking the **WLAN Assignment** tab. Select an RP radio to view which SSIDs are mapped to that radio's BSSIDs.

The radio also adds the enabled WLANs to the WLAN assignment for default radio adoption configurations, which you can view by selecting **Network Setup** > **Radio Adoption Defaults** and clicking the **WLAN Assignment** tab.

For example, Figure 4-46 shows the default configuration after you enable the five WLANs shown in Figure 4-45.



Network Setup > Radio Adoption Defaults

Select Radio / BSS

Select Radio 802.11a

Select / Change Assigned WLANs

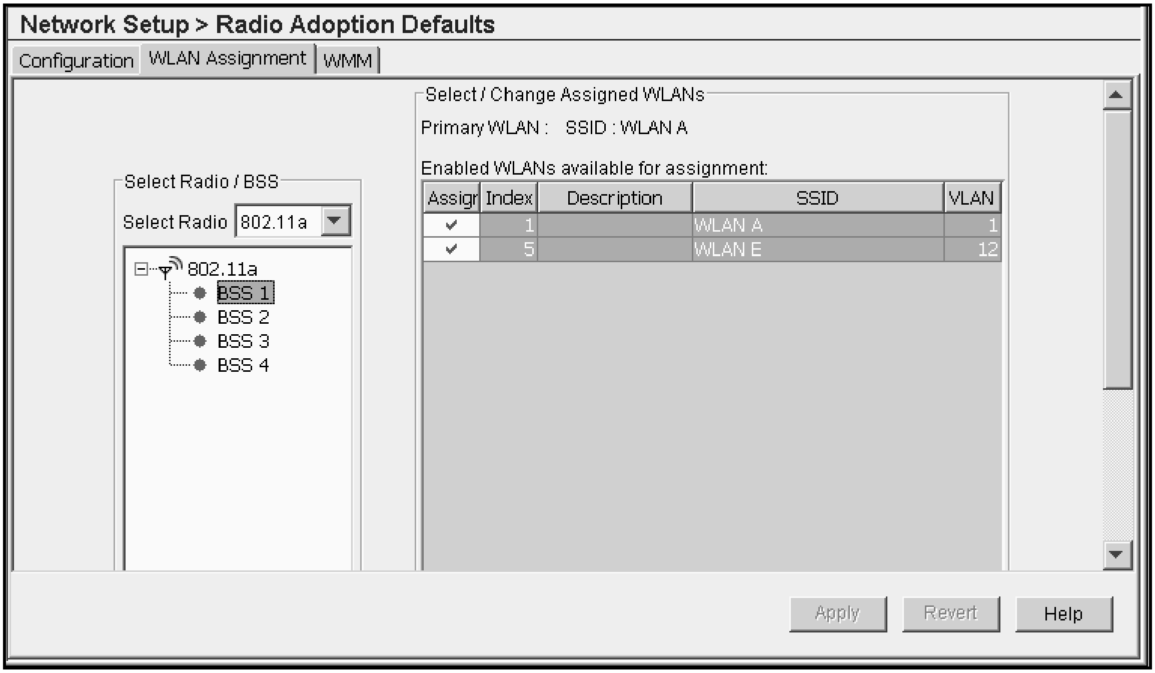
Primary WLAN :

Enabled WLANs available for assignment:

Assign	Index	Description	SSID	VLAN
✓	1		WLAN A	1
✓	2		WLAN B	8
✓	3		WLAN C	4
✓	4		WLAN D	1
✓	5		WLAN E	12

Figure 4-46. Viewing the WLANs Assigned to Radios in the Default Configuration

The radio supports all five WLANs. However, some of the WLANs share a BSSID. For example, when BSS 1 is selected in the section on the left, the section on the right shows the two WLANs that share this BSSID. See Figure 4-47.



Network Setup > Radio Adoption Defaults

Select Radio: 802.11a

Primary WLAN : SSID : WLAN A

Enabled WLANs available for assignment:

Assign	Index	Description	SSID	VLAN
✓	1		WLAN A	1
✓	5		WLAN E	12

Figure 4-47. Viewing the WLANs Assigned to a BSSID in the Default Configuration

To review how the Wireless Edge Services xl Module assigns WLANs to RP radios, see “Normal Mode Configuration” on page 4-4.

VLAN Assignment

The instructions for configuring a WLAN include the basic mechanics for assigning all traffic from a WLAN to a VLAN.

This section will explain in more depth when and why you would assign one WLAN to one VLAN and another WLAN to another VLAN. You will also learn about the ability of the Wireless Edge Services xl Module to assign individual wireless *users* to VLANs—an ability that provides a high degree of flexibility and control at the edge of the network.

To understand the importance of the VLAN assignment, consider role of the Wireless Edge Services xl Module as the guard between the wireless and wired portions of your network. RPs encapsulate wireless traffic with Ethernet headers so wireless users can access the wired network, but the module *controls* this traffic so that wireless users receive the *appropriate* network access.

In a traditional Ethernet network, one of the primary ways in which administrators control network rights is by assigning users to various subnetworks, or VLANs. Traditionally, administrators used hardware-based rules to enforce these assignments: they plugged a user's workstation into a switch port configured to carry traffic on the appropriate VLAN. However, you cannot control mobile users in a wireless network in this way, because wireless users do not connect through a set port. Instead:

- Users may connect through different ports at different times.
- Traffic from many different users may arrive on the same port.

When you configure VLAN assignment on a Wireless Edge Services xl Module, you enable the module to take over, for wireless stations, the role of assigning users to the correct VLANs. In other words, you establish the foundation for control over mobile users' network rights. The module acts as an *intelligent* door to your network, opening on the correct subnetwork for each wireless user.

You have a choice about how to treat the VLANs to which the module assigns wireless traffic. If you want your *wired* infrastructure devices to handle this traffic, make sure that on the wireless-services enabled switch you tag the module's internal uplink port for these VLANs. If you want the Wireless Edge Services xl Module to route the wireless traffic into VLANs used on the wired network, you *should not* tag the internal uplink port for the VLANs for *wireless* users. On the other hand, you *might* tag the port for the *wired* VLANs (depending on whether the module has VLAN interfaces for those VLANs or simply knows routes to them).

The Wireless Edge Services xl Module determines the VLAN to which to assign incoming wireless traffic based on one of two criteria:

- the wireless user's identity
- the wireless station's WLAN

You configure WLAN-based VLAN assignments manually. (See "Setting Basic Configuration Options: SSID and Interface" on page 4-30.)

Identity or user-based VLAN assignments are dynamic and received from an authentication server. This server can be either the Wireless Edge Services xl Module's internal RADIUS server on an external RADIUS server. You must activate dynamic VLANs on a WLAN in order for the module to enforce dynamic VLAN assignments. (See "Setting Basic Configuration Options: SSID and Interface" on page 4-30.)

Note that the Wireless Edge Services xl Module can use both kinds of assignment on the same WLAN, but dynamic settings always take precedence when dynamic VLANs are enabled. For example, you manually assign WLAN 1 to VLAN 10. Users A, B, and C connect to WLAN 1; however, the RADIUS database only includes a VLAN assignment for users A and B. When user C connects to the WLAN, the module forwards its traffic in VLAN 10. When user A connects to the WLAN, the authentication server sends users' VLAN assignment, and the module forwards user A's traffic in VLAN 20. (See Figure 4-48.)

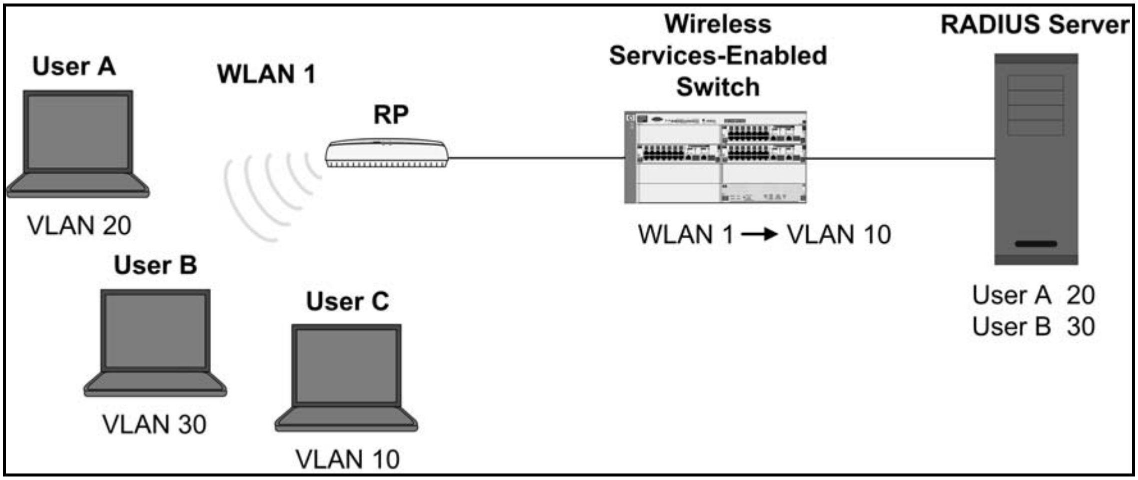
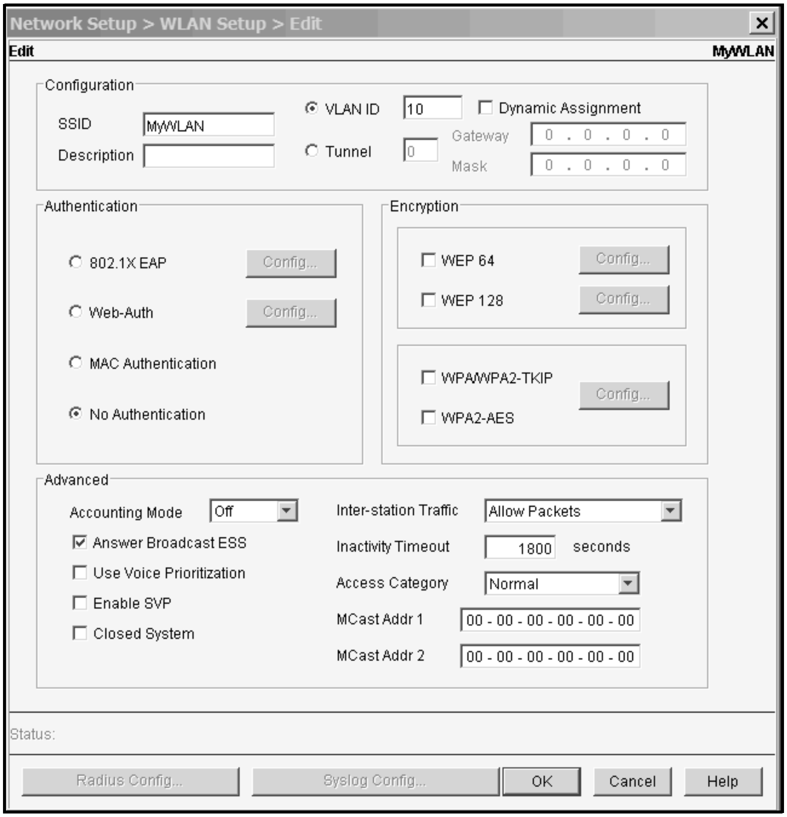


Figure 4-48. WLAN Versus Identity-Based VLAN Assignment

WLAN-Based VLAN Assignment

You configure WLAN-based VLAN assignment by manually assigning the WLAN to a VLAN.

Typically, you complete this step at the same time that you configure the SSID and security settings, as described in "Setting Basic Configuration Options: SSID and Interface" on page 4-30 and as shown in Figure 4-49.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID: MyWLAN
Description:
● VLAN ID: 10 □ Dynamic Assignment
○ Tunnel: 0
Gateway: 0 . 0 . 0 . 0
Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP Config...
○ Web-Auth Config...
○ MAC Authentication
● No Authentication

Encryption

□ WEP 64 Config...
□ WEP 128 Config...
□ WPA/WPA2-TKIP
□ WPA2-AES Config...

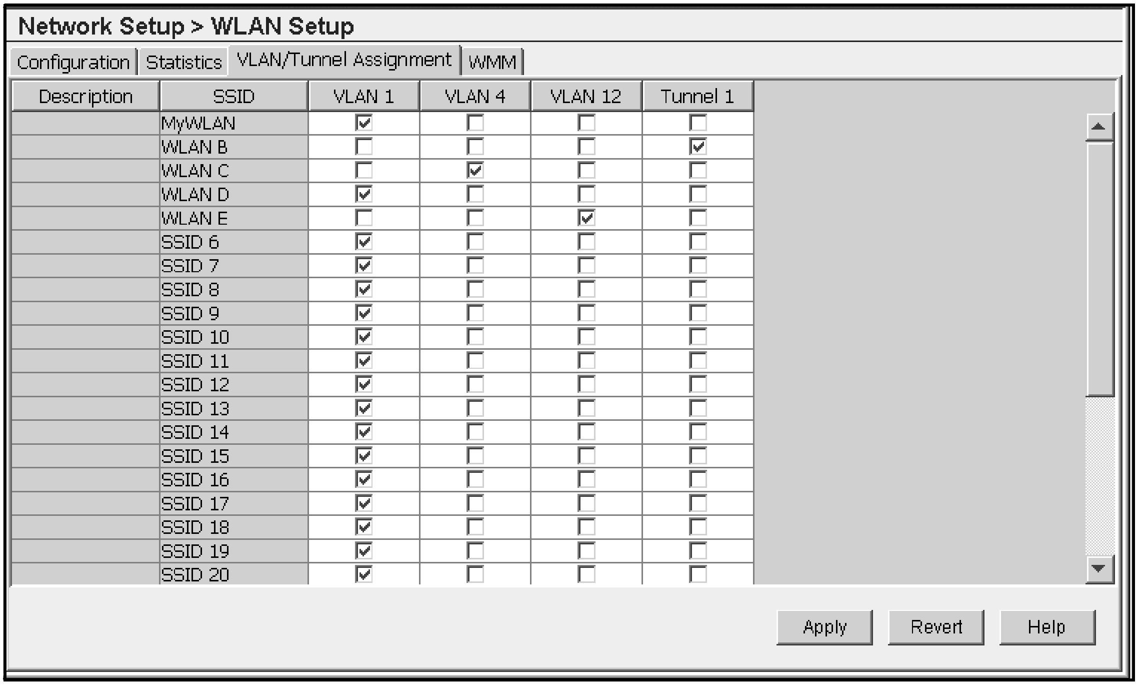
Advanced

Accounting Mode: Off
☑ Answer Broadcast ESS
□ Use Voice Prioritization
□ Enable SVP
□ Closed System
Inter-station Traffic: Allow Packets
Inactivity Timeout: 1800 seconds
Access Category: Normal
MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00
MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-49. Configuring WLAN-Based VLAN Assignment

You can quickly change the interface assignment for multiple WLANs by selecting the **VLAN/Tunnel Assignment** tab on the **Network Setup** > **WLAN Setup** screen, as shown in Figure 4-50.



Description	SSID	VLAN 1	VLAN 4	VLAN 12	Tunnel 1
	MyWLAN	☑	□	□	□
	WLAN B	□	□	□	☑
	WLAN C	□	☑	□	□
	WLAN D	☑	□	□	□
	WLAN E	□	□	☑	□
	SSID 6	☑	□	□	□
	SSID 7	☑	□	□	□
	SSID 8	☑	□	□	□
	SSID 9	☑	□	□	□
	SSID 10	☑	□	□	□
	SSID 11	☑	□	□	□
	SSID 12	☑	□	□	□
	SSID 13	☑	□	□	□
	SSID 14	☑	□	□	□
	SSID 15	☑	□	□	□
	SSID 16	☑	□	□	□
	SSID 17	☑	□	□	□
	SSID 18	☑	□	□	□
	SSID 19	☑	□	□	□
	SSID 20	☑	□	□	□

Figure 4-50. Network Setup > WLAN Setup > VLAN/Tunnel Assignment Screen

In the first two columns, the **Network Setup** > **WLAN Setup** > **VLAN Assignment** screen shows this information for each WLAN:

- **Description** (if configured)
- **SSID**

All the VLANs to which at least one WLAN has been assigned compose the subsequent columns. If you have configured a WLAN to forward traffic over a tunnel, the tunnel interface is also displayed, as shown in Figure 4-50.

The check mark indicates to which interface the WLAN has been assigned.

For example, Figure 4-50 shows the **Network Setup** > **WLAN Setup** > **VLAN/ Tunnel Assignment** screen for a Wireless Edge Services xl Module on which five WLANs have been configured and enabled. These WLANs have been assigned to a variety of VLAN interfaces and to one tunnel interface. You can change the VLAN assignment for any of the WLANs simply by checking the box in the new column. Note that because a WLAN can only be *manually* assigned to a single VLAN, the check mark in the previous column automatically disappears.

See “Identity-Based, or Dynamic, VLAN Assignment” on page 4-88 for an explanation of how the Wireless Edge Services xl Module can dynamically match WLAN traffic to multiple VLANs.

Considerations for WLAN-Based VLAN Assignment

By default, all WLANs are mapped to VLAN 1. In some networks that use multiple VLANs, this VLAN is reserved for the management VLAN. Just as you might prevent a switch port from carrying traffic in VLAN 1 before connecting a user to this port, you might want to remove a WLAN from VLAN 1 and place it in a different VLAN.

In addition, just as you might create several VLANs to isolate users from each other and direct them toward the appropriate resources, you might create several WLANs and assign different VLANs to these WLANs to control wireless users’ network rights.

When determining how many WLANs to create and which VLANs to assign to these WLANs, consider these issues:

- What type of network access will users connecting to the wireless network require?

  For example, if the users need the wireless connection exclusively for Internet access, then they probably will not need to be part of any specific subnetwork. You could create a single WLAN and map that WLAN to any user VLAN in your network. Remember, however, that the wireless users will then receive the same sort of network rights as users in that VLAN, which is not ideal in many cases. It might be a better idea to create a new VLAN, such as VLAN 100, that is exclusively for wireless users; network administrators could limit traffic in that VLAN to such applications as DHCP, DNS, and HTTP.

  You can then either:

  - Add that VLAN to the Ethernet network—completing all necessary steps such as tagging switch ports for the VLAN and configuring a DHCP server to provide addresses in the appropriate subnetwork range.
  - Terminate that VLAN on the Wireless Edge Services xl Module and configure the module to route traffic, act as a DHCP server, and perform NAT.

  For more information on these options, see “Determining the Layer 3 Services Your Wireless Edge Services xl Module Should Provide” on page 1-17 of *Chapter 1: Introduction.*

- Who will be connecting to this WLAN?
  - **Guests**—In this case as well, you could assign the WLAN to a VLAN reserved for wireless users. Network administrators could then control traffic from that VLAN appropriately—for example, limiting wireless users to Internet access or to certain network servers.
  - **Employees who will use the wireless connection exclusively**—You can use the same policies to assign new employees to a VLAN that you would use if the employees used traditional, wired connections. Then simply assign the WLAN to that VLAN.

    If you want to assign different employees to different VLANs, then you must configure a separate WLAN for each employee category and ensure that the employees connect to the correct WLAN. Dynamic VLAN assignment offers a more elegant solution and will be discussed later in "Identity-Based, or Dynamic, VLAN Assignment" on page 4-88.
  - **Employees who will use the wireless connection as well as a traditional connection**—In this case particularly, you should focus on the type of network access that the employees will require. If, for example, the employees only need to check their email and access the Internet, then you could group them all together in a WLAN and VLAN that has been configured to allow such limited access.

    If, on the other hand, the employees need access equivalent to wired connections, then you must configure the Wireless Edge Services xl Module to place each employee in the VLAN in which that employee operates in the Ethernet network. In a network with a single user VLAN, the process is straightforward enough: simply create a WLAN and assign it to that VLAN.

    However, to replicate, for wireless users, wired access to a network with multiple VLANs, you must:

    i. Determine the user VLANs to which mobile employees belong.
    ii. Create one WLAN for each user VLAN, mapping each WLAN to a different VLAN.
    iii. Configure security on each WLAN such that only the employees that should be placed in the corresponding VLAN can connect to the WLAN.

    Dynamic VLAN assignment, described in "Identity-Based, or Dynamic, VLAN Assignment" on page 4-88, greatly simplifies this process, while providing finer control.

Note

When the Wireless Edge Services xl module places traffic in a VLAN, it tags it for that VLAN. You must remember to tag the module's uplink port for each VLAN to which you manually assign a WLAN. (For more on configuring the wireless services-enabled switch, see the *Wireless Edge Services xl MOdule Supplement to the ProCurve 6400cl/5300xl/3400cl Management and Configuration Guide.*)

Figure 4-51 illustrates how a station connects a WLAN and receives an address in the appropriate subnetwork from the network's DHCP server.

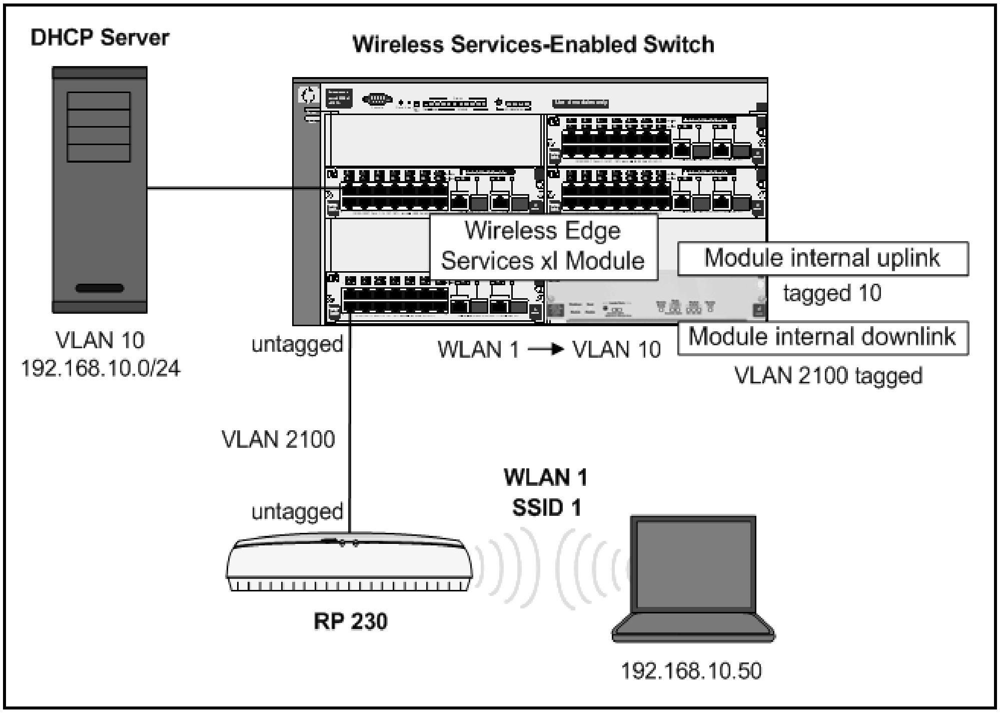


Figure 4-51. Assigning a Wireless Station to a VLAN

Identity-Based, or Dynamic, VLAN Assignment

The Wireless Edge Services xl Module can also divide traffic from wireless users into VLANs based on those users' identities. This capability (variously called user-based VLANs or identity-based VLANs, as well as dynamic VLAN assignment) allows you to:

- configure one WLAN for your wireless network with a single SSID and unified wireless security policy
- simultaneously retain granular control over the network rights of each wireless user

In order for your Wireless Edge Services xl Module to implement dynamic VLAN assignment in a WLAN, stations must authenticate to a RADIUS server. This server can be either the module's internal server or an external network server.

You must also manually enable dynamic VLAN assignment on the WLAN.

You should not use dynamic VLANs in certain circumstances:

- You must place the WLAN in a Layer 3 mobility domain—Dynamic VLANs disable Layer 3 mobility on the WLAN. See *Chapter 9: Fast Layer 2 Roaming and Layer 3 Mobility* for guidelines on when a network requires Layer 3 mobility.
- The WLAN requires Web-Auth—Dynamic VLANs can cause complications because the Web-Auth station receives an IP address before it authenticates. However, if you must, you can enabled dynamic VLAN assignment. Take care to set the DHCP lease for the static VLAN very low.

On the Wireless Edge Services xl Module, to enable dynamic VLAN assignment on a WLAN, complete these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
2. Verify that the WLAN uses 802.1X EAP, Web-Auth, or MAC authentication.
3. Check the **Dynamic Assignment** box.
4. Click the **OK** button.
5. On the RADIUS server, configure users' VLAN assignments.
   a. See "Creating a Group" on page 11-12 in *Chapter 11: RADIUS Server* to learn how to configure VLAN assignments on the Wireless Edge Services xl Module's internal RADIUS server.

b. One of the easiest ways to configure the assignment on an *external* server itself is via an Identity Driven Manager (IDM) agent installed on the server. In this case, you would configure the assignment through ProCurve IDM and its Policy Manager. You would:

   - Configure communities that include the wireless users.
   - Create policies that match these communities to the appropriate VLANs.
   - Deploy the policies to the RADIUS server that the Wireless Edge Services xl Module uses to authenticate wireless users.

In either case, when a user connects to a WLAN and authenticates to the RADIUS server, the RADIUS server sends the VLAN assignment configured for that user's community to the Wireless Edge Services xl Module. The module then tags all traffic from that user for that VLAN.

6. On the wireless services-enabled switch, you might need to tag the module's uplink port for the user-based VLANs just as you might if you had configured the VLAN assignment manually.

   Whether you tag to VLAN on the uplink port depends on whether you want the Ethernet infrastructure to route the traffic or the module to do so. See "Determining the Layer 3 Services Your Wireless Edge Services xl Module Should Provide" on page 1-17 of *Chapter 1: Introduction* for more guidance in this decision.

   See the *Wireless Edge Services xl Module Supplement to the 6400cl/5300xl/3400cl Management and Configuration Guide* for instructions on tagging the uplink port.

Note

Remember that the Wireless Edge Services xl Module can receive other identity-based settings from an external RADIUS server, including:

- access control lists (ACLs)
- a rate limit on traffic from the wireless station

If you are using IDM, simply configure these settings in the IDM Policy Manager at the same time that you configure the VLAN assignment. Refer to the *ProCurve Identity Driven Manager User's Guide* for more detailed instructions on how to configure identity-based settings. (You can download this guide from **http://www.procurve.com**.)

Traffic Management (QoS)

Contemporary users demand more from wireless connections—more bandwidth and more multimedia applications—but they also demand less jitter and fewer dropped calls.

The ProCurve Wireless Edge Services xl Module helps RPs to deliver a high QoS for voice, video, and other high-priority or time-sensitive traffic.

The Wireless Edge Services xl Module and adopted RPs support protocols designed to improve QoS over the radio medium:

- SpectraLink Voice Priority (SVP)
- Wireless Multimedia (WMM)

In addition, the Wireless Edge Services xl Module can use voice prioritization to mark traffic destined to VoWLAN devices for priority handling in both the Ethernet and wireless network.

Using WLAN prioritization and weighted fair queuing (WFQ), the Wireless Edge Services xl Module queues traffic outbound to RPs according to the WLAN to which it is destined. The module allocates relatively more bandwidth to the queues for WLANs with a higher priority.

Figure 4-52 displays where these various QoS mechanisms affect traffic.

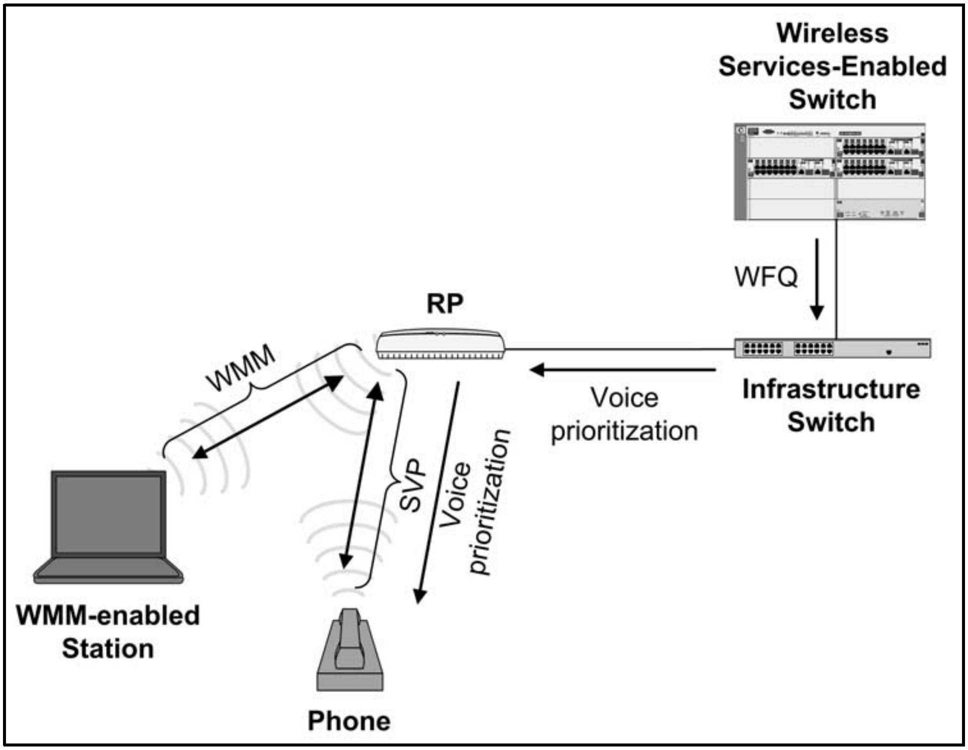


Figure 4-52. QoS Mechanisms Supported by the Wireless Edge Services xl Module

SVP

SVP maintains a high QoS specifically for VoWLAN devices that are SVP-capable. SVP is implemented in wireless phones, wireless APs, and SpectraLink servers. This IEEE 802.11-compliant mechanism minimizes latency for voice traffic by providing priority queues reserved for voice packets and by increasing the probability that all voice packets are transmitted in a predictable and timely manner.

SVP devices access the medium without waiting the default 802.11 interframe spacing (IFS) interval. In addition, SVP-enabled RPs and phones transmit voice packets in a coordinated fashion, thereby eliminating the need for a random backoff time and the attendant delays.

The Wireless Edge Services xl Module can configure RPs to support SVP—that is, to recognize SVP frames, place them in priority queues, and transmit them with a zero backoff time. If your network includes a SpectraLink server and SVP-capable phones, you should enable this support in the WLAN that includes these phones.

To enable SVP support, complete these steps:

1. Access the **Edit** screen for the WLAN that includes voice devices:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
2. Under **Advanced**, check the **Enable SVP** box.
3. Click the **OK** button.

Note

Remember that you are enabling SVP support on the *WLAN*, not on a particular RP. Because an RP may carry traffic for several WLANs, it might support SVP for some stations and not for others.

In other words, all ProCurve RPs *can* support SVP, but they actually do so only on the WLANs for which you have enabled such support.

WMM

A wireless network uses a shared medium (a radio). To avoid collisions, 802.11 specifies that all stations and RPs use distributed coordination function (DCF), which is similar to Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

When a wireless device wants to transmit, it selects a random backoff time and then listens for contention. After the medium has been free for an entire IFS interval (3 ms in DCF), the device counts down its backoff timer and transmits. Because all devices compete for the medium on the same footing, the QoS for time-sensitive applications can be seriously degraded.

WMM is a Wi-Fi protocol that prioritizes wireless traffic, ensuring that the most important and the most time-sensitive traffic receives a high QoS. WMM is similar to Enhanced Distributed Channel Access (EDCA), which is the prioritization method specified in the IEEE 802.11e standard.

Support for WMM is particularly important when mobile users use VoWLAN applications. It will become increasingly crucial as users demand for a wide array of applications the same quality of network access that they receive over Ethernet connections.

Prioritization with WMM

WMM improves QoS by dividing traffic into priority queues, one for each of four access categories (ACs). The higher the AC, the higher the QoS the traffic requires.

The Wireless Edge Services xl Module can use WMM to prioritize the following traffic:

- traffic sent from RP radios to wireless stations
- traffic sent from wireless stations to RP radios

Priority Queuing and ACs. Table 4-7 shows the ACs into which RPs and wireless stations can divide traffic.

Table 4-7. WMM ACs

Queue Number	AC
1	Background
2	Best Effort
3	Video
4	Voice

Each AC queue is defined by different parameters, which include:

- the IFS—now called the arbitration IFS number (AIFSN)
- the minimum contention window (CW Min)—the maximum value for the initial random backoff time
- the maximum contention window (CW Max)—the maximum value for the random backoff time in a network experiencing collisions
- the transmit opportunity (Transmit Ops)—the continuous time during which a device that has won control of the radio can retain control

When devices use different parameters to transmit different types of traffic, the most time-sensitive traffic can receive the QoS that it needs. For example, the queue for voice traffic uses a smaller contention window, so VoWLAN devices on average choose smaller backoff times and win control of the medium more quickly.

When you enable WMM, traffic is assigned to an AC (and WMM queue) according to its QoS mark. Table 4-8 shows how QoS marks map to ACs, by default. You can customize these mappings for traffic transmitted by RP radios. (See "Customizing How QoS Marks Map to ACs" on page 4-106.)

Table 4-8. Priority Values for WMM ACs

Queue Number	AC	802.1p Priority	DSCP
1	Background	1, 2	8-23
2	Best Effort	0, 3	0-7. 24-31
3	Video	4, 5	32-47
4	Voice	6, 7	48-63

By default, the module uses 802.1p priority to place traffic in a queue. You can choose DSCP instead; see "Customizing Station WMM Parameters" on page 4-101.

Priority Queuing on Traffic Transmitted from RPs to Wireless Stations. Remember that all traffic on a radio shares the same medium. So an RP radio may queue traffic for multiple WLANs together. By default, RPs queue traffic according to the classification of the WLAN to which it belongs. Because, by default, this classification is normal for all WLANs, all traffic receives the same handling.

One way to configure RPs to prioritize the traffic they transmit is to assign different classifications to traffic in different WLANs. See "Manually Classifying a WLAN's Traffic" on page 4-109.

For more precise prioritization, you can enable WMM on a WLAN. WMM allows RPs to queue traffic destined the WLAN according to each frame's QoS mark. In other words, the RP uses an 802.1p or DSCP value to assign traffic to an AC. The RP creates one queue for each AC on each of its radios. The radio then transmits traffic in that queue using the RP WMM parameters (such as AIFSN) for that AC. (For more information about the RP WMM parameters for wired to wireless traffic, see "Viewing and Customizing RP WMM Parameters" on page 4-104.)

In this way, traffic with a higher priority receives more bandwidth, as shown in Figure 4-53. The RP radio continues to provide all wired to wireless traffic belonging to non-WMM WLANs with normal QoS.

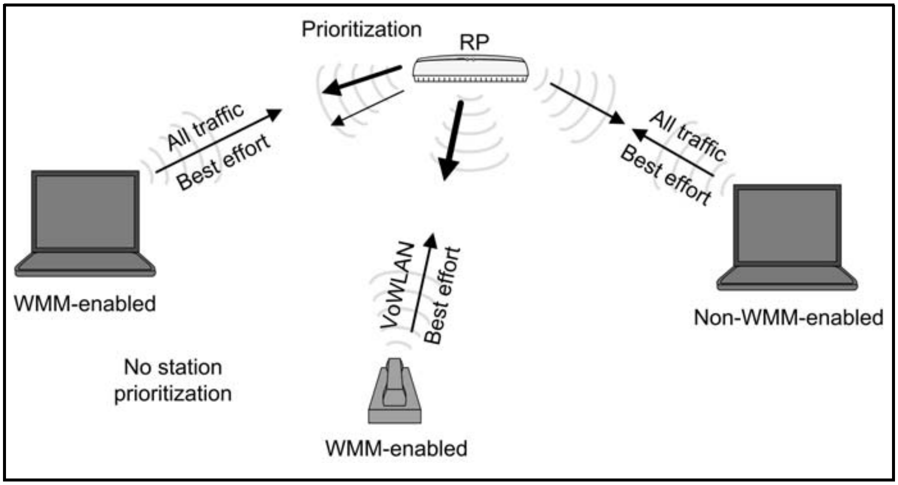


Figure 4-53. Using WMM to Prioritize Traffic Transmitted from RPs to Wireless Stations

Priority Queuing on Traffic Transmitted from Wireless Stations to RPs. Only when you enable WMM on a WLAN, WMM-enabled stations also implement priority queuing on traffic they transmit.

RPs broadcast station WMM parameters throughout the WLAN. WMM-enabled stations queue traffic according to 802.1p or DSCP value, using the WMM parameters to determine how to handle traffic in each queue. (Non-WMM stations continue to handle all traffic normally.) Figure 4-54 illustrates the affect of WMM on wireless station to RP traffic.

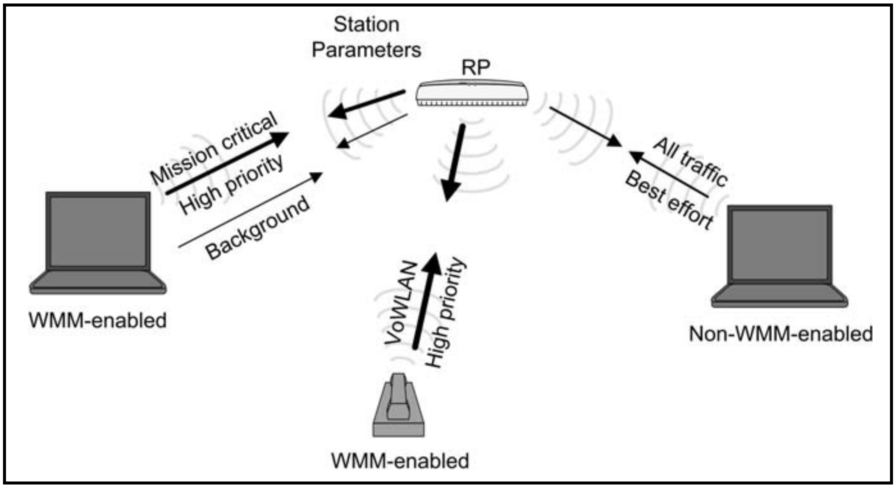


Figure 4-54. Using WMM to Prioritize Traffic Transmitted From Wireless Stations to RPs

Note that the station WMM parameters can differ from the RP WMM parameters.

Enabling WMM on a WLAN

Enabling WMM on a WLAN, enables the following:

- RP radios use QoS marks (802.1p, by default) to queue traffic destined to stations in this WLAN

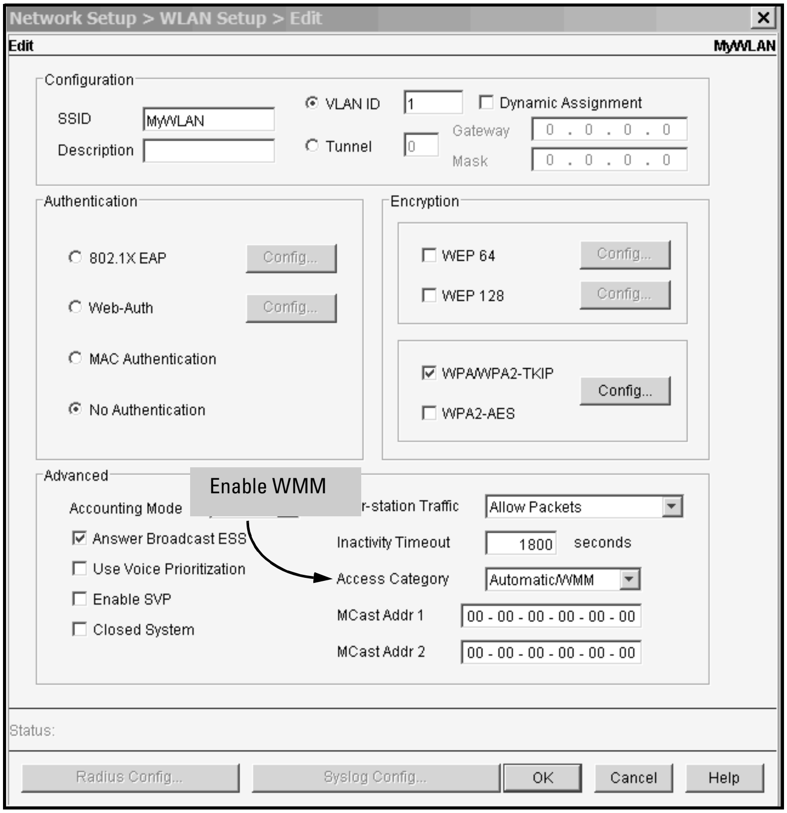
  Radios grant better QoS to high priority queues by using different parameters to transmit traffic in those queues.

- WMM-enabled stations in the WLAN use QoS marks to queue traffic destined to their RPs

  Adopted RP radios broadcast WMM parameters for the four ACs. Wireless stations that are WMM-enabled queue and transmit traffic accordingly. Non-WMM-enabled stations continue to use standard settings for all traffic, which match those for the Best Effort AC (queue 1).

To enable WMM prioritization, complete these steps:

1. Access the **Edit** screen for the WLAN that includes voice devices:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.


Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID: MyWLAN

Description:

● VLAN ID: 1 □ Dynamic Assignment

○ Tunnel: 0 Gateway: 0 . 0 . 0 . 0 Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

○ MAC Authentication

● No Authentication

Encryption

□ WEP 64

□ WEP 128

☑ WPA/WPA2-TKIP

□ WPA2-AES

Advanced

Accounting Mode

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic: Allow Packets

Inactivity Timeout: 1800 seconds

Access Category: Automatic/WMM

MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Enable WMM

Figure 4-55. Enabling WMM on a WLAN

2. Under **Advanced**, in the **Access Category** drop-down menu, select **Automatic/WMM**.

3. Click the **OK** button.

The next section explains how to make some advanced configurations for WMM.

Changing the Protocol that Prioritizes Traffic and Enabling Admission Control

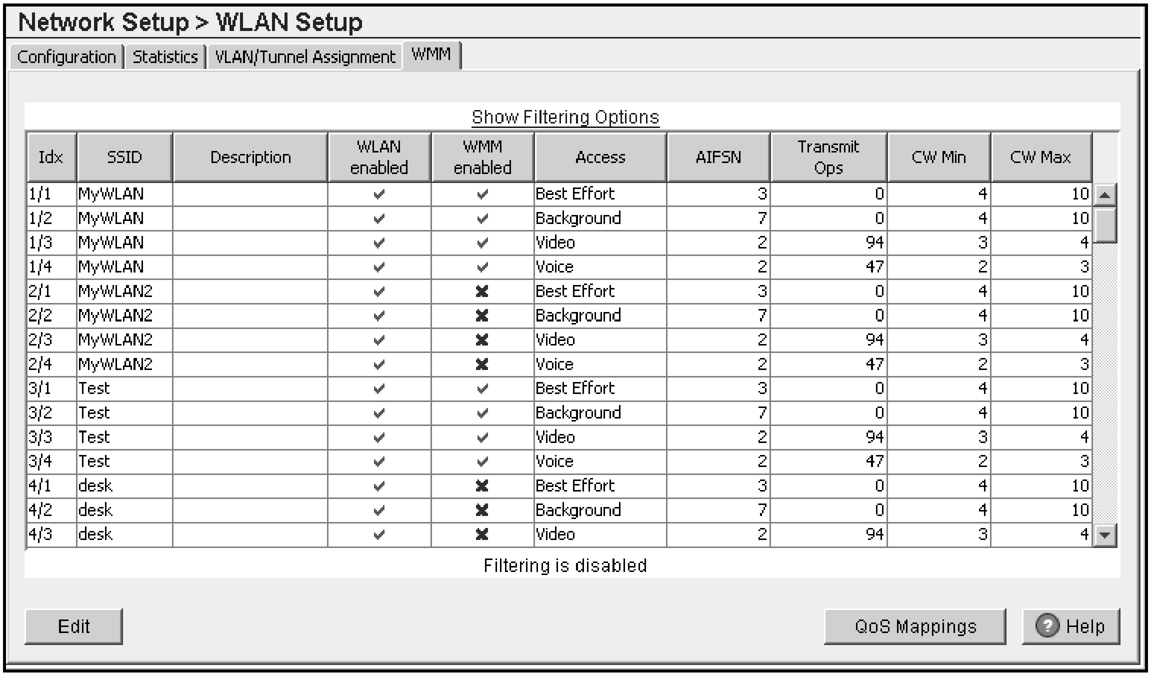
As discussed earlier, when you enable WMM, wireless devices queue frames according to QoS marks. The default protocol for the QoS mark is 802.1p. However, you can change the protocol to DSCP by accessing advanced WMM parameters.

Another advanced WMM parameter is admission control, a feature available for Video and Voice queues. The more stations that use high priority settings, the less effect those settings have. Admission control restricts the number of stations in a wireless cell that can use the high priority settings by forcing stations to check with the RP first.

To configure these advanced options, follow these steps:

1. Select **Network Setup** > **WLAN Setup** and click the **WMM** tab.

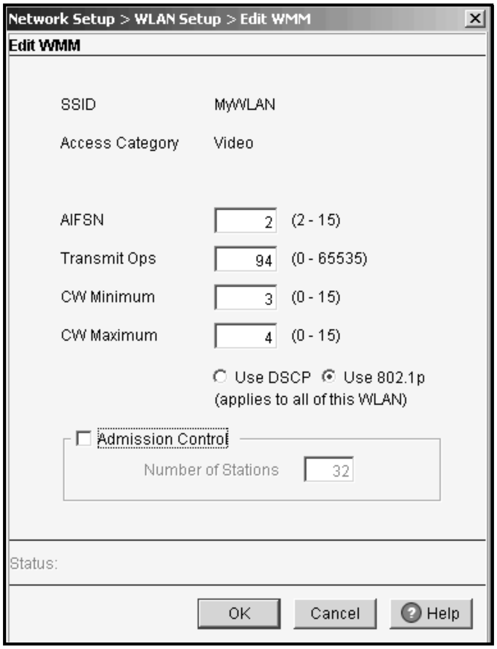
   As you can see in Figure 4-56, the WMM enabled column displays the WLANs for which you have set the **Access Category** to **Automatic/WMM**.



Idx	SSID	Description	WLAN enabled	WMM enabled	Access	AIFSN	Transmit Ops	CW Min	CW Max
1/1	MyWLAN		✓	✓	Best Effort	3	0	4	10
1/2	MyWLAN		✓	✓	Background	7	0	4	10
1/3	MyWLAN		✓	✓	Video	2	94	3	4
1/4	MyWLAN		✓	✓	Voice	2	47	2	3
2/1	MyWLAN2		✓	✗	Best Effort	3	0	4	10
2/2	MyWLAN2		✓	✗	Background	7	0	4	10
2/3	MyWLAN2		✓	✗	Video	2	94	3	4
2/4	MyWLAN2		✓	✗	Voice	2	47	2	3
3/1	Test		✓	✓	Best Effort	3	0	4	10
3/2	Test		✓	✓	Background	7	0	4	10
3/3	Test		✓	✓	Video	2	94	3	4
3/4	Test		✓	✓	Voice	2	47	2	3
4/1	desk		✓	✗	Best Effort	3	0	4	10
4/2	desk		✓	✗	Background	7	0	4	10
4/3	desk		✓	✗	Video	2	94	3	4

Figure 4-56. Station EDCA (WMM) Parameters

2. Select the queue for which you want to alter the settings, and then click the **Edit** button. The **Edit WMM** screen is displayed.



Network Setup > WLAN Setup > Edit WMM

Edit WMM

SSID MyWLAN

Access Category Video

AIFSN 2 (2 - 15)

Transmit Ops 94 (0 - 65535)

CW Minimum 3 (0 - 15)

CW Maximum 4 (0 - 15)

○ Use DSCP ● Use 802.1p
(applies to all of this WLAN)

□ Admission Control

Number of Stations 32

Status:

Figure 4-57. Editing Station EDCA (WMM) Parameters

3. Select the prioritization protocol used by your wireless stations:
   - 802.1p is a Layer 2 protocol that marks traffic in the VLAN tag for one of eight priorities.
   - DSCP is a Layer 3 protocol that marks traffic in the IP header for one of 64 priorities.

   Wireless devices queue frames according to the priority marked by the selected protocol. For example, if you select 802.1p, a wireless devices transmits a frame with priority value of 5 in its VLAN tag, using the parameters for the Video AC. A frame with a DSCP value in the IP header, but no 802.1p value, is transmitted according to the Best Effort AC.

   Refer to Table 4-8 on page 4-94 to review to which ACs various priority values map. See "Customizing How QoS Marks Map to ACs" on page 4-106 to change which values map to which ACs.

Note

If you change the protocol for one queue, the setting automatically changes in the other three queues for the WLAN; in other words, the setting applies to the WLAN as a whole. (It does not make sense to use 802.1p to queue some traffic, but queue other traffic according to DSCP.)

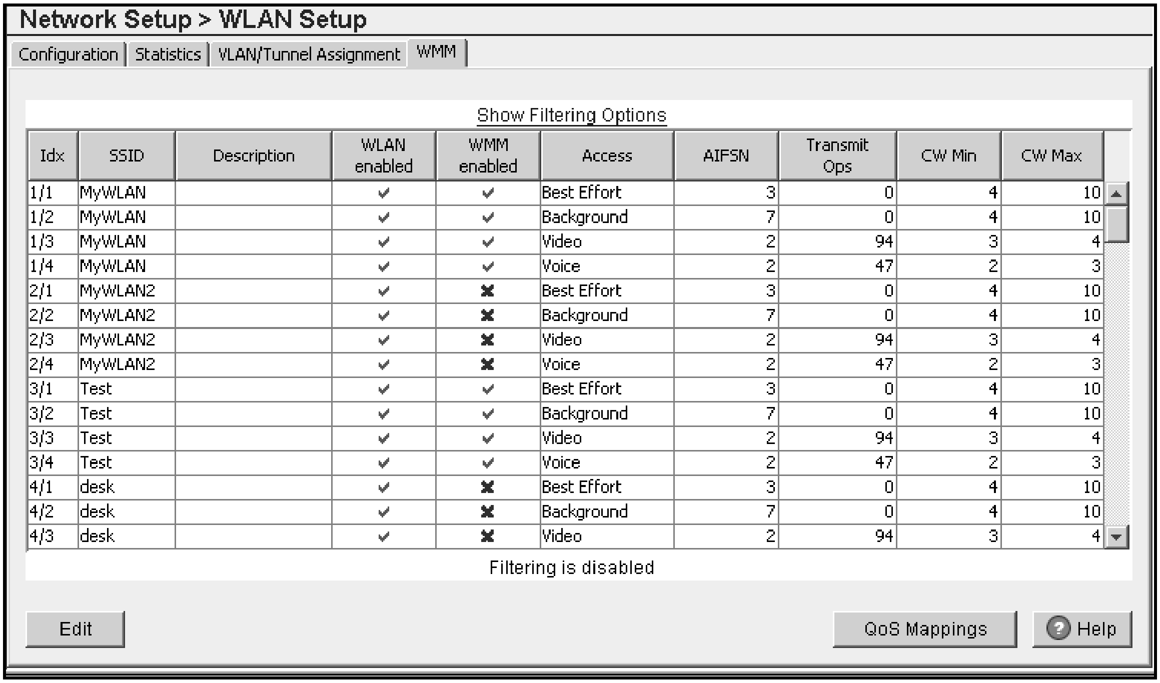
4. To restrict the number of stations allowed to use the settings for this queue, check the **Admission Control** box and enter a value from 1 to 255.

   This option is only available for the Voice and Video ACs.

5. Click the **OK** button.

Viewing Station WMM Parameters

From the **Network Setup** > **WLAN Setup** > **WMM**, you can also view the station WMM parameters, which determine how WMM-enabled stations in a WMM-enabled WLAN handle traffic placed in various ACs.



Idx	SSID	Description	WLAN enabled	WMM enabled	Access	AIFSN	Transmit Ops	CW Min	CW Max
1/1	MyWLAN		✓	✓	Best Effort	3	0	4	10
1/2	MyWLAN		✓	✓	Background	7	0	4	10
1/3	MyWLAN		✓	✓	Video	2	94	3	4
1/4	MyWLAN		✓	✓	Voice	2	47	2	3
2/1	MyWLAN2		✓	✗	Best Effort	3	0	4	10
2/2	MyWLAN2		✓	✗	Background	7	0	4	10
2/3	MyWLAN2		✓	✗	Video	2	94	3	4
2/4	MyWLAN2		✓	✗	Voice	2	47	2	3
3/1	Test		✓	✓	Best Effort	3	0	4	10
3/2	Test		✓	✓	Background	7	0	4	10
3/3	Test		✓	✓	Video	2	94	3	4
3/4	Test		✓	✓	Voice	2	47	2	3
4/1	desk		✓	✗	Best Effort	3	0	4	10
4/2	desk		✓	✗	Background	7	0	4	10
4/3	desk		✓	✗	Video	2	94	3	4

Filtering is disabled

Figure 4-58. Station WMM Settings

Figure 4-58 shows the default settings for WMM queues. As you can see, each WLAN has its own four queues. This is because RPs broadcast one set of station parameters to all stations in a WLAN. They can broadcast another set of station parameters to all stations in another WLAN (if that WLAN uses WMM).

The **Idx** column lists the WLAN and the queue number. For example, the first row displays the settings for queue 1 on WLAN 1. To see the AC for this queue, look at the **Access** column. For example, queue 1 is the Background queue.

The **SSID** and **Description** columns further identify the WLAN in question.

A green check mark in the **WLAN Enabled** column indicates that RPs in your network currently support this WLAN; a green check mark in the **WMM Enabled** column indicates that RPs are allowed to send the WMM parameters to stations (**Access Category** is **Automatic/WMM**.) In Figure 4-58, four WLANs are active and enabled. However, only two (MyWLAN and Test) implement WMM prioritization on wireless station to RP traffic.

The final four columns list the station WMM parameters for the queue in this row. The default settings grant lower latency for the queues with higher numbers.

Typically, no further configuration is necessary. You only need to know that by accepting these settings from the RPs, wireless stations can improve QoS for certain types of traffic.

For example, if a wireless station is transmitting a voice frame, the station will compete for the radio using the advantageous settings that the RP has specified for such frames. However, the station must meet these requirements for the prioritization to take effect:

- The station must support WMM.
- The traffic must be marked by an application on the wireless station for the higher AC.

Customizing Station WMM Parameters

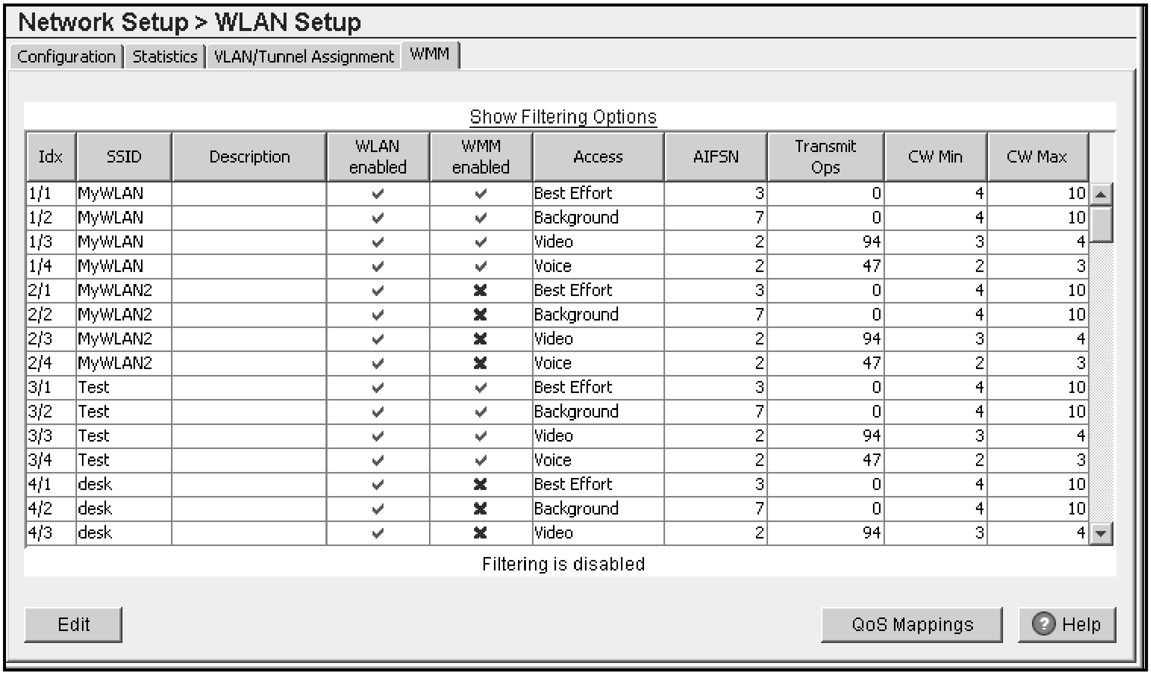
If you have a great deal of experience working with WMM and other QoS protocols, you can customize the queue settings to the needs of your environment.

Note

Because the Wireless Edge Services xl Module automatically defines settings such that traffic in a higher-priority queue receives lower latency, the default station WMM parameters settings are usually adequate. Also, because incorrect settings can adversely affect network performance, ProCurve Networking generally recommends that you do *not* change these parameters.

To customize station WMM parameters, complete these steps:

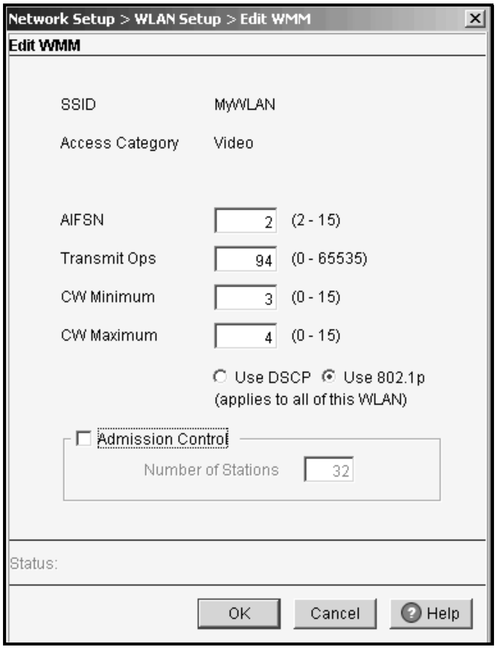
1. Select **Network Setup** > **WLAN Setup** and click the **WMM** tab.



Idx	SSID	Description	WLAN enabled	WMM enabled	Access	AIFSN	Transmit Ops	CW Min	CW Max
1/1	MyWLAN		✓	✓	Best Effort	3	0	4	10
1/2	MyWLAN		✓	✓	Background	7	0	4	10
1/3	MyWLAN		✓	✓	Video	2	94	3	4
1/4	MyWLAN		✓	✓	Voice	2	47	2	3
2/1	MyWLAN2		✓	✗	Best Effort	3	0	4	10
2/2	MyWLAN2		✓	✗	Background	7	0	4	10
2/3	MyWLAN2		✓	✗	Video	2	94	3	4
2/4	MyWLAN2		✓	✗	Voice	2	47	2	3
3/1	Test		✓	✓	Best Effort	3	0	4	10
3/2	Test		✓	✓	Background	7	0	4	10
3/3	Test		✓	✓	Video	2	94	3	4
3/4	Test		✓	✓	Voice	2	47	2	3
4/1	desk		✓	✗	Best Effort	3	0	4	10
4/2	desk		✓	✗	Background	7	0	4	10
4/3	desk		✓	✗	Video	2	94	3	4

Figure 4-59. Station WMM Parameters

2. Select the queue for which you want to alter the settings, and then click the **Edit** button. The **Edit WMM** screen is displayed.



Network Setup > WLAN Setup > Edit WMM

Edit WMM

SSID MyWLAN

Access Category Video

AIFSN 2 (2 - 15)

Transmit Ops 94 (0 - 65535)

CW Minimum 3 (0 - 15)

CW Maximum 4 (0 - 15)

○ Use DSCP ● Use 802.1p
(applies to all of this WLAN)

□ Admission Control

Number of Stations 32

Status:

Figure 4-60. Editing Station EDCA (WMM) Parameters

3. View the **SSID** and **Access Category** settings to verify that you are configuring the correct queue. In Figure 4-60, the Best Effort queue (queue 1) in MyWLAN is being customized.

4. Enter the desired values in the **AIFSN**, **Transmit Ops**, **CW Minimum**, and **CW Maximum** fields.

   The values for the **AIFSN** and **Transmit Ops** are in ms. The CW Min and CW Max values are determined by raising 2 to the power of the value in the corresponding field and subtracting one. For example, if you enter 4 in the **CW Minimum** field, the CW Min value is 15. (Setting the CW Min and CW Max values in this way forces you to specify values allowed by WMM.)

   Again, take great care in establishing these settings. ProCurve Networking cannot guarantee any behavior. However, you can keep these tips in mind:

   - The lower the AIFSN and the CW minimum values, the lower the latency for traffic in the queue, and in a congested network, the higher the throughput. In a congested network, raising the AIFSN or the CW minimum of low-priority queues can improve QoS for high-priority. Raising the AIFSN value a certain amount sometimes has a more dramatic effect than raising the CW value the same amount. However, raising either value too high can starve out low-priority traffic.

- By default, high-priority queues on the RP use an AIFSN value of 1 ms; high-priority queues on stations use an AIFSN value of 2 ms. You might want to reserve the 1-ms AIFSN for RPs.
- When you grant a queue a Transmit Ops, you allow a station that wins access to the radio continued access to the medium for that length of time. If you set this value excessively high, then lower-priority traffic, and even other high-priority traffic, may be unacceptably delayed. Although the Web browser interface lists the maximum value as 65,535, generally the Transmit Ops is set in terms of tens, or at the most, hundreds of milliseconds—not thousands. In several seconds, applications can time out, frustrating users throughout your network.
- In a network with many users and high congestion, increasing CW Maximum values can decrease the number of collisions.
- The CW Maximum value must always be higher than the CW Minimum value.

Viewing and Customizing RP WMM Parameters

As discussed earlier, RPs handle traffic as dictated by the WMM parameters (AISFN and so forth) for the traffic's AC. Also as discussed earlier, the Wireless Edge Services xl Module assigns traffic to an AC according to the WLAN setting or, if the AC is set to automatic/WMM, according to priority value.

The ProCurve 210, 220, and 230 RPs use default parameters that work for nearly all applications. (For example, the parameters are such that voice frames more quickly and more often win access to the medium.)

Note

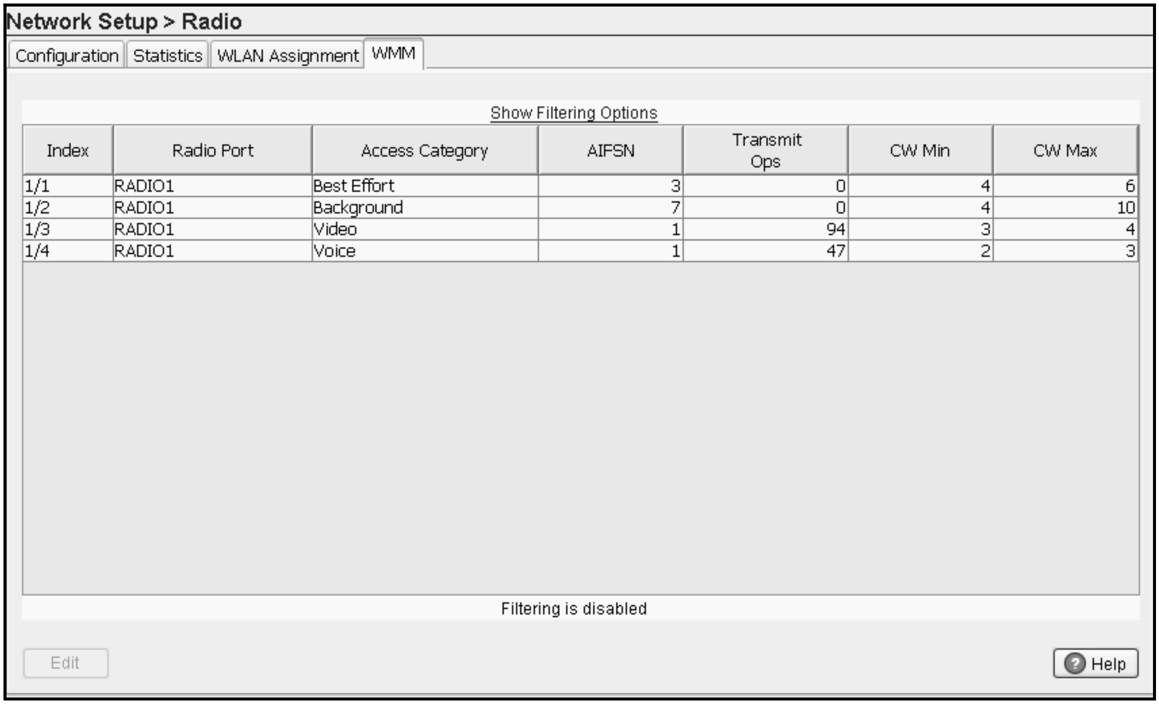
Because the Wireless Edge Services xl Module automatically defines settings such that traffic in a higher-priority queue receives lower latency, the default radio WMM settings are usually adequate. Incorrect settings can adversely affect network performance; ProCurve Networking strongly recommends that you do not change these parameters.

Like other radio settings, you can alter:

- the WMM queue parameters that the Wireless Edge Services xl Module sends to newly adopted radios
- the WMM queue parameters used by particular radios

To customize the RP WMM parameters, complete these steps:

1. Choose whether you are configuring parameters for any newly adopted radio or for a particular radio:
   - To configure settings for any newly adopted radio, select **Network Setup** > **Radio Adoption Defaults**.
   - To configure settings for particular radios, select **Network Setup** > **Radio**.
2. Click the **WMM** tab. On the screen that is displayed (see Figure 4-62), queues are listed depending on the configuration type:
   - For the radio adoption default configurations, queues are listed on the screen by radio type and access category—for example, **802.11a** and **Background**.
   - If you are configuring WMM settings for particular radios, queues are indexed according to radio number and queue number. For example, in Figure 4-62, the **Voice** queue for radio 1 would be indexed 1/4.



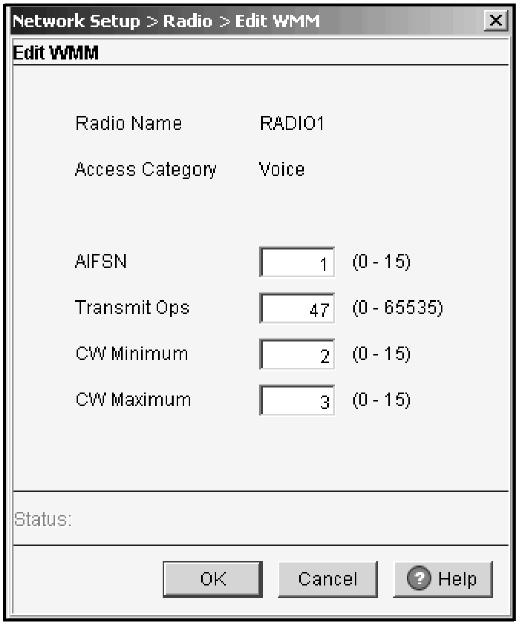
Network Setup > Radio

Index	Radio Port	Access Category	AIFSN	Transmit Ops	CW Min	CW Max
1/1	RADIO1	Best Effort	3	0	4	6
1/2	RADIO1	Background	7	0	4	10
1/3	RADIO1	Video	1	94	3	4
1/4	RADIO1	Voice	1	47	2	3

Filtering is disabled

Figure 4-61. Network Setup > Radio > WMM Screen

3. To change the parameters for a particular queue, select the queue and click the **Edit** button. The **Edit WMM** screen is displayed.



Network Setup > Radio > Edit WMM

Edit WMM

Radio Name RADIO1

Access Category Voice

AIFSN 1 (0 - 15)

Transmit Ops 47 (0 - 65535)

CW Minimum 2 (0 - 15)

CW Maximum 3 (0 - 15)

Status:

Figure 4-62. Edit WMM Screen for Radio 1's Voice AC

4. To change the AIFSN value, enter a new value between 0 and 15 in the **AIFSN** field. This value is in ms.
5. To change the Transmit Ops value, enter a new value between 0 and 65,535 in the **Transmit Ops** field. This value is in ms.
6. To change the CW Min, enter a new value between 0 and 15 in the **CW Minimum** field. The CW Min is 2 to the power of this value, minus 1, in ms. For example, if you enter 3, then the CW Min is 7 ms.
7. To change the CW Max, enter a new value between 0 and 15 in the **CW Maximum** field. The CW Max is 2 to the power of this value, minus 1, in ms.
8. Click the **OK** button.

Customizing How QoS Marks Map to ACs

As discussed earlier, enabling WMM on a WLAN allows wireless devices to queue traffic according to either an 802.1p or DSCP. Table 4-9 shows the default mapping of values to priority queues.

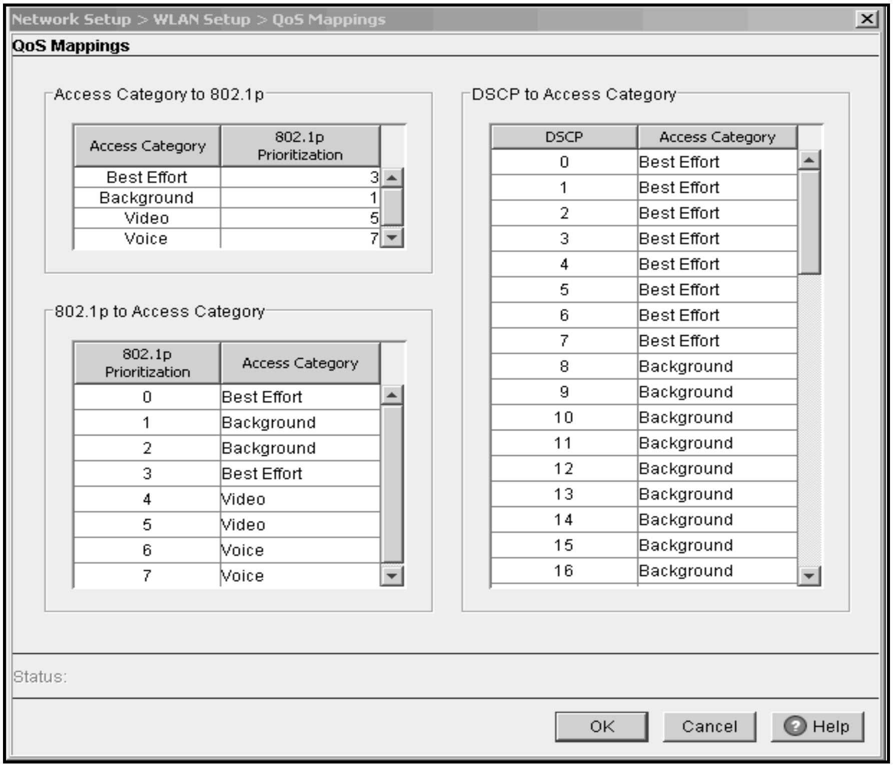
Table 4-9. Priority Values for WMM ACs

Queue Number	AC	802.1p Priority	DSCP
1	Background	1, 2	8-23
2	Best effort	0, 3	0-7. 24-31
3	Video	4, 5	32-47
4	Voice	6, 7	48-63

The mapping of priority value to AC occurs as traffic is prepared for transmission in a WLAN. For traffic traveling the opposite direction—from the WLAN to the Ethernet—the Wireless Edge Services xl Module reverses the operation, marking traffic that arrives in a particular AC with a priority value.

You can change the mapping to customize your network's queues. Follow these steps:

1. Select **Network Setup** > **WLAN Setup** and click the **WMM** tab.
2. Click the **QoS Mappings** button. The **QoS Mappings** screen is displayed.



QoS Mappings

Access Category to 802.1p

Access Category	802.1p Prioritization
Best Effort	3
Background	1
Video	5
Voice	7

802.1p to Access Category

802.1p Prioritization	Access Category
0	Best Effort
1	Background
2	Background
3	Best Effort
4	Video
5	Video
6	Voice
7	Voice

DSCP to Access Category

DSCP	Access Category
0	Best Effort
1	Best Effort
2	Best Effort
3	Best Effort
4	Best Effort
5	Best Effort
6	Best Effort
7	Best Effort
8	Background
9	Background
10	Background
11	Background
12	Background
13	Background
14	Background
15	Background
16	Background

Status:

Figure 4-63. Customizing QoS Mappings

3. Use the **Access Category to 802.1p** section to configure the Wireless Edge Services xl Module, to mark incoming wireless traffic with a QoS value for priority handling in the wired network.

   Click a field in the **802.1p Prioritization** column. Then enter a value between 0 and 7. The module marks traffic that arrives in this AC with this 802.1p value.

4. If you are using 802.1p to prioritize traffic in at least one WLAN, configure the QoS mappings in the **802.1p to Access Category** section.

   To select the AC to which a particular 802.1p value maps, click the **Access Category** column in the row for that value. Then choose **Best Effort**, **Background**, **Video**, or **Voice** from the drop-down menu.

5. If you are using DSCP to prioritize traffic in at least one WLAN, configure the QoS mappings in the **DSCP to Access Category** section.

   To select the AC to which a particular DSCP maps, click the **Access Category** column in the row for that value. Then choose **Best Effort**, **Background**, **Video**, or **Voice** from the drop-down menu.

6. Click the **OK** button.

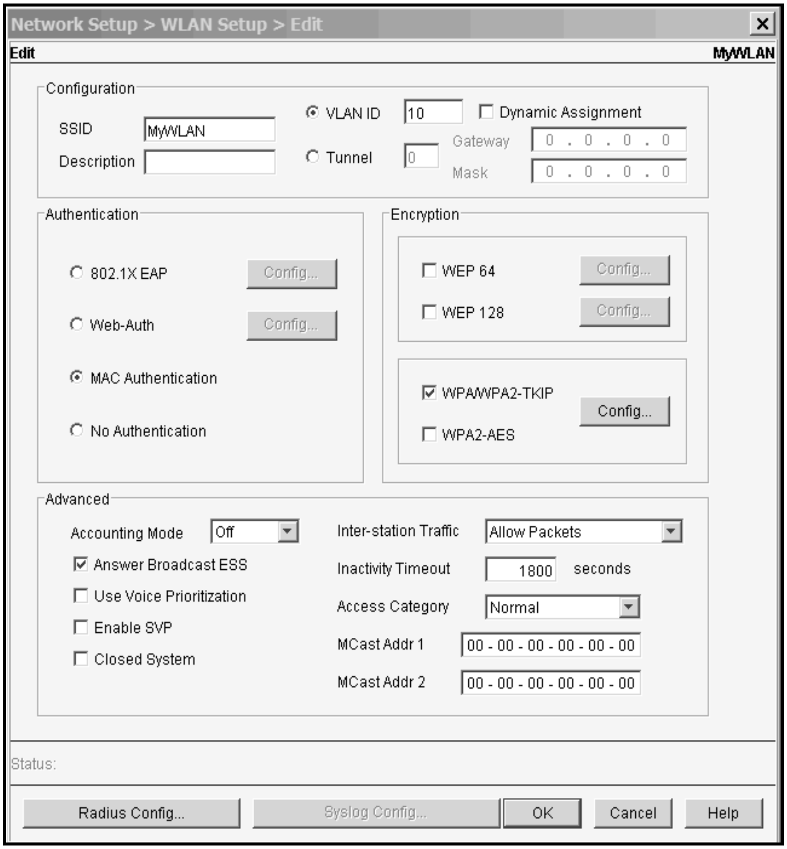
Manually Classifying a WLAN's Traffic

By default, the Wireless Edge Services xl Module and RPs treat traffic destined to stations in any WLAN equally. However, you can manually assign all traffic in a particular WLAN to a specific AC. Traffic then receives QoS according to the relative priority of that AC. For example, you could configure a WLAN for traditional data traffic and a WLAN for voice traffic. To prioritize traffic sent to the voice wireless devices, you would manually set the entire voice WLAN to the Voice AC.

Note With WMM, RPs *automatically* prioritize different types of traffic. Enabling WMM on a WLAN also allows WMM-capable stations to prioritize traffic automatically according to QoS values. See "WMM" on page 4-92 and "Enabling WMM on a WLAN" on page 4-96.

To set a WLAN's AC manually, follow these steps:

1. Access the **Edit** screen for the WLAN:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID MyWLAN

Description

● VLAN ID 10 ☐ Dynamic Assignment

○ Tunnel 0

Gateway 0 . 0 . 0 . 0

Mask 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP

○ Web-Auth

● MAC Authentication

○ No Authentication

Encryption

☐ WEP 64

☐ WEP 128

☑ WPA/WPA2-TKIP

☐ WPA2-AES

Advanced

Accounting Mode Off

☑ Answer Broadcast ESS

☐ Use Voice Prioritization

☐ Enable SVP

☐ Closed System

Inter-station Traffic Allow Packets

Inactivity Timeout 1800 seconds

Access Category Normal

MCast Addr 1 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2 00 - 00 - 00 - 00 - 00 - 00

Status:

Figure 4-64. Setting a WLAN's AC

2. Choose the name of an AC from the **Access Category** drop-down menu in the **Advanced** section.

   By default, RPs handle traffic as follows, from traffic that receives the highest priority to traffic that receives the lowest:

   - **Voice**
   - **Video**
   - **Normal**
   - **Low**

Enabling Prioritization of Voice Traffic

Voice prioritization improves the QoS for traffic destined *to* VoWLAN devices. The Wireless Edge Services xl Module configures RPs to monitor all packets from stations in a WLAN; if the IP type in a packet's header indicates that it is a voice packet, the module marks all traffic destined to the packet's source as high-priority voice packets.

Traffic destined to the VoWLAN device thus receives priority handling both in the Ethernet network (from the wireless services-enabled switch to the RP) and in the wireless network (from the RP to the VoWLAN device). The wireless services-enabled switch forwards the traffic in its high-priority queue, and the RP uses its Voice queue settings.

Voice prioritization thus helps to maintain QoS for VoWLAN devices that do not support WMM on their own.

To enable the Wireless Edge Services xl Module to prioritize traffic to voice stations in a particular WLAN, complete these steps:

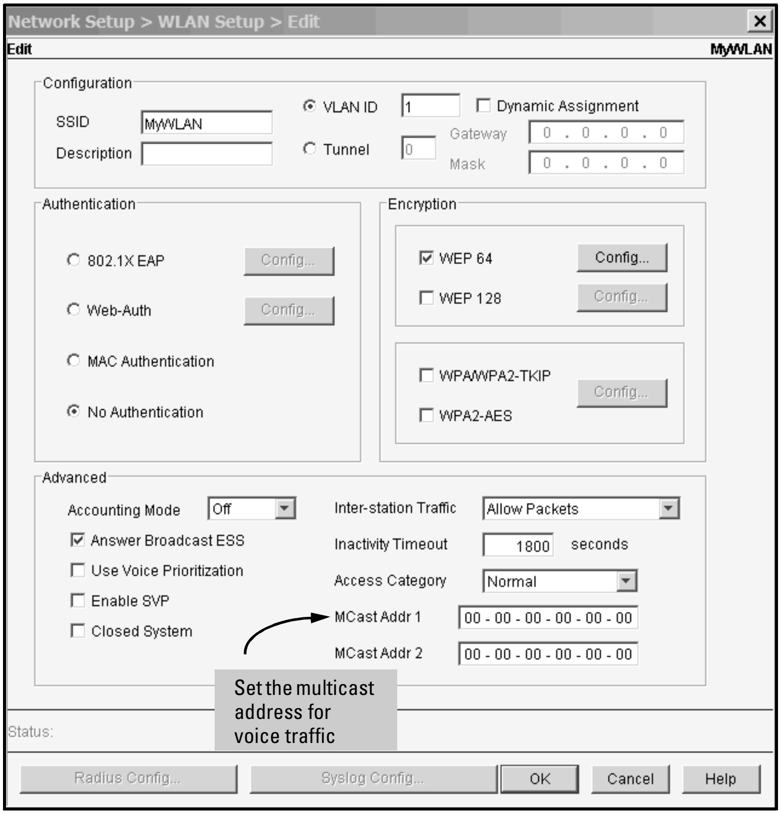
1. Access the **Edit** screen for the WLAN that includes voice devices:
   a. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
   b. Select the WLAN and click the **Edit** button. The **Edit** screen is displayed.
2. Under **Advanced**, check the **Use Voice Prioritization** box.
3. Click the **OK** button.

Specifying Multicast Addresses for Voice Traffic

VoWLAN devices often send and listen for traffic on a specific multicast address. When you specify this address in a WLAN's settings, the Wireless Edge Services xl Module prioritizes this traffic.

To specify multicast addresses for voice traffic, complete these steps:

1. Select **Network Setup** > **WLAN Setup** and click the **Configuration** tab.
2. Select the WLAN that includes voice devices, and then click the **Edit** button. The **Edit** screen is displayed.



Network Setup > WLAN Setup > Edit

Edit MyWLAN

Configuration

SSID: MyWLAN

Description:

● VLAN ID: 1 □ Dynamic Assignment

○ Tunnel: 0

Gateway: 0 . 0 . 0 . 0

Mask: 0 . 0 . 0 . 0

Authentication

○ 802.1X EAP Config...

○ Web-Auth Config...

○ MAC Authentication

● No Authentication

Encryption

☑ WEP 64 Config...

□ WEP 128 Config...

□ WPA/WPA2-TKIP Config...

□ WPA2-AES

Advanced

Accounting Mode: Off

☑ Answer Broadcast ESS

□ Use Voice Prioritization

□ Enable SVP

□ Closed System

Inter-station Traffic: Allow Packets

Inactivity Timeout: 1800 seconds

Access Category: Normal

MCast Addr 1: 00 - 00 - 00 - 00 - 00 - 00

MCast Addr 2: 00 - 00 - 00 - 00 - 00 - 00

Status:

Set the multicast address for voice traffic

Figure 4-65. Setting the Multicast Address

3. Under **Advanced**, in the **MCast Addr 1** field, enter the address for voice traffic.
4. If you want, enter a second address in the **MCast Addr 2** field.
5. Click the **OK** button.