Use the honeypot feature carefully as it could interfere with legitimate SSIDs and prevent clients from associating to another available network.

SSID Management

This window allows you to manage SSIDs (create, edit and delete), assign security parameters and VLANs on a per SSID basis, and configure the Web Page Redirect functionality.

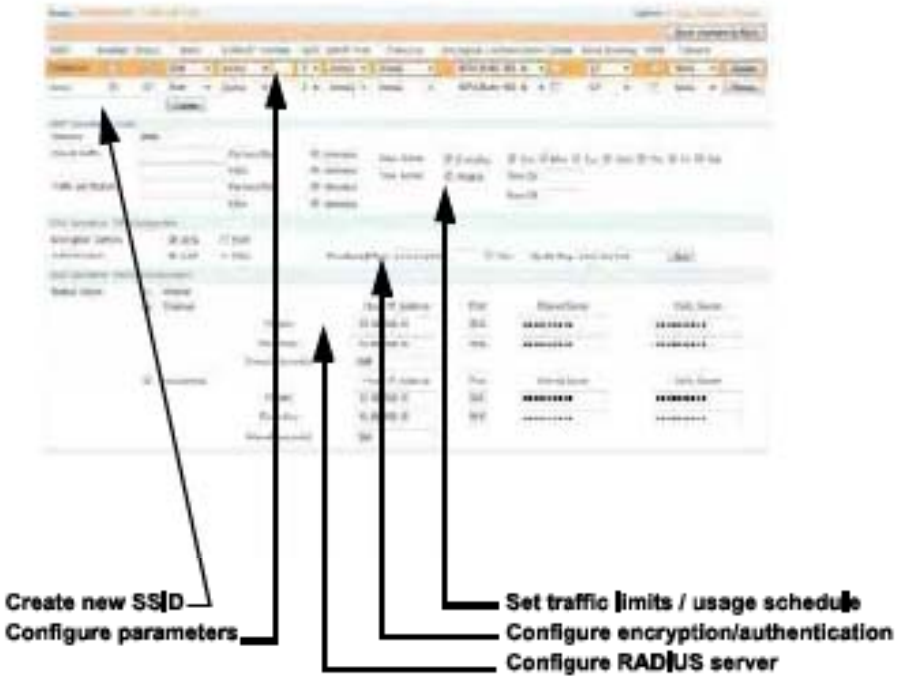

Figure 137. SSID Management

Procedure for Managing SSIDs

1. **New SSID Name:** To create a new SSID, enter a new SSID name to the left of the Create button (Figure 137), then click Create. The SSID name may only consist of the characters A-Z, a-z, 0-9, dash, and underscore. You may create up to 16 SSIDs.

SSID List (top of page)

2. **SSID**: Shows all currently assigned SSIDs. When you create a new SSID, the SSID name appears in this table. Click any SSID in this list to select it.
3. **On**: Check this box to activate this SSID or clear it to deactivate it.
4. **Brdcast**: Check this box to make the selected SSID visible to all clients on the network. Although the Wireless Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Clear this box if you do not want this SSID to be visible on the network.
5. **Band**: Choose which wireless band the SSID will be beaconed on. Select either **5 GHz**—802.11an, **2.4 GHz**—802.11bgn or **Both**.
6. **VLAN ID / Number**: From the pull-down list, select a VLAN that you want this traffic to be forwarded to on the wired network. Select **numeric** to enter the number of a previously defined VLAN in the **Number** field (see "VLANs" on page 199). This step is optional.
7. **QoS**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:
   - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
   - 1—Medium, with QoS prioritization aggregated across all traffic types.
   - 2—High, normally used to give priority to video traffic.

- 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic, as described in "Understanding QoS Priority on the Wireless Array" on page 244. The default value for this field is 2.

8. **DHCP Pool**: If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull–down list. An internal DHCP pool must be created before it can be assigned. To create an internal DHCP pool, go to "DHCP Server" on page 197.

9. **Filter List**: If you wish to apply a set a filters to this SSID's traffic, select the desired Filter List. See "Filters" on page 344.

10. **Authentication**: The following authentication options are available:

    - **Open**: This option provides no authentication and is not recommended.
    - **RADIUS MAC**: Uses an external RADIUS server to authenticate stations onto the wireless network, based on the user's MAC address. Accounting for these stations is performed according to the accounting options that you have configured specifically for this SSID or globally (see Step 12 below).

    If this SSID is on a VLAN, the VLAN must have management turned on in order to pass CHAP authentication challenges from the client station to the RADIUS server.

    - **802.1x**: Authenticates stations onto the wireless network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the Wireless Array) or external.

11. **Encryption**: From the pull-down list, choose the encryption that will be required—specific to this SSID—either None, WEP, WPA, WPA2 or WPA-Both. The None option provides no security and is not recommended; WPA2 provides the best practice Wi-Fi security.

Each SSID supports only one encryption type at a time (except that WPA and WPA2 are both supported on an SSID if you select WPA-Both). If you need to support other encryption types, you must define additional SSIDs. The encryption standard used with WPA or WPA2 is selected in the Security>Global Settings window (page 230). For an overview of the security options, see "Security Planning" on page 46 and "Understanding Security" on page 209.

*XN model Arrays cannot use the SSID-specific WEP keys specified in this step. They can only use the global WEP keys specified in the **Global Settings** window.*

12. **Global**: Check the checkbox if you want this SSID to use the security settings established at the global level (refer to "Global Settings" on page 230). Clear the checkbox if you want the settings established here to take precedence. Additional sections will be displayed to allow you to configure encryption, RADIUS, and RADIUS accounting settings. The **WPA Configuration** encryption settings have the same parameters as those described in "Procedure for Configuring Network Security" on page 231. The external RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see "Procedure for Configuring an External RADIUS Server" on page 235). Note that external RADIUS servers may be specified using IP addresses or domain names.

Figure 138. SSID Management

13. **Roaming**: For this SSID, select whether to enable fast roaming between IAPs or Arrays at **L2&L3** (Layer 2 and Layer 3), at **L2** (Layer 2 only), or disable roaming (**Off**). You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings (IAP). See "Understanding Fast Roaming" on page 273.

14. **WPR (Web Page Redirect)**: Check the checkbox to enable the Web Page Redirect functionality, or clear it to disable this option. If enabled, WPR configuration fields will be displayed under the SSID Limits section. This feature may be used to provide an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate

URL. For example, some wireless devices and users may not have a correctly configured 802.1x (RADIUS) supplicant. Utilizing WPR's Web-based login, users may be authenticated without using an 802.1x supplicant. See "Web Page Redirect Configuration Settings" on page 255 for details of WPR usage and configuration.

When using WPR, it is particularly important to adhere to the SSID naming restrictions detailed in ***Step 1****.*

15. **Fallback**: Network Assurance checks network connectivity for the Array. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the Array will automatically disable this SSID. This will disassociate current clients, and prevent new clients from associating. Since the Array's network connectivity has failed, this gives clients a chance to connect to other, operational parts of the wireless network. No changes are made to WDS configuration. See Step a on page 225 for more information on Network Assurance.

The lower part of the window contains a few sections of additional settings to configure for the currently selected SSID, depending on the values chosen for the settings described above.

- **"SSID Limits" on page 254**
- **"Web Page Redirect Configuration Settings" on page 255**
- **"WPA Configuration Settings" on page 259**
- **"RADIUS Configuration Settings" on page 260**

SSID Limits

See "Group Limits" on page 268 for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

16. **Stations**: Enter the maximum number of stations allowed on this SSID. This step is optional. Note that the IAPs - Global Settings window also has a station limit option—**Max Station Association per IAP**. If both

station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.

17. **Overall Traffic**: Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.

18. **Traffic per Station**: Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Packets/Sec** field or the **Kbps** field to force a traffic restriction. If you set both values, the Array will enforce the limit it reaches first.

19. **Days Active**: Choose **Everyday** if you want this SSID to be active every day of the week, or select only the specific days that you want this SSID to be active. Days that are not checked are considered to be the inactive days.

20. **Time Active**: Choose **Always** if you want this SSID active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that this SSID is active.

21. To delete SSIDs, click their **Delete** buttons.

22. Click **Save changes to flash** if you wish to make your changes permanent.

Web Page Redirect Configuration Settings

If you enable WPR, the SSID Management window displays additional fields that must be configured. For example configurations and complete examples, please see the *Xirrus Web Page Redirect Application Note* in the *Xirrus Resource Center*.

If enabled, WPR displays a splash or login page when a user associates to the wireless network and opens a browser to any URL (provided the URL does not point to a resource directly on the user's machine). The user-requested URL is captured, the user's browser is redirected to the splash or login page, and then the browser is redirected either to your specified landing page, if any, or else back to the captured URL. The landing page may be specified for a user group as well.

See "Group Management" on page 266. Note that if you change the management HTTPS port, WPR uses that port, too. See "HTTPS" on page 224.

Figure 139. WPR Internal Splash Page Fields (SSID Management)

Note that when users roam between Arrays, their WPR Authentication will follow them so that re-authentication is not required.

You may select among five different modes for use of the Web Page Redirect feature, each displaying a different set of parameters that must be entered:

- Internal Login page

  This option displays a login page (residing on the Array) instead of the first user-requested URL. There is an upload function that allows you to replace the default login page, if you wish. Please see "Web Page Redirect" on page 368 for more information.

  To set up internal login, set **Server** to **Internal Login**. Set **HTTPS** to **On** for a secure login, or select **Off** to use HTTP. You may also customize the login page with logo and background images and header and footer text. See "Customizing an Internal Login or Splash page" on page 258.

  The user name and password are obtained by the login page, and authentication occurs according to your configured authentication information (starting with Step 10 on page 251 above). These authentication parameters are configured as described in "Procedure for Configuring Network Security" on page 231.

After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

Both the Internal Login and External Login options of WPR perform authentication using your configured RADIUS servers.

- Internal Splash page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Array. Note that there is an upload function that allows you to replace the default splash page, if you wish. Please see "Web Page Redirect" on page 368 for more information. You may also customize the splash page with logo and background images and header and footer text. See "Customizing an Internal Login or Splash page" on page 258.

  To use an internal splash page, set **Server** to **Internal Splash**. Enter a value in the **Timeout** field to define how many seconds the splash screen is displayed before timing out, or select **Never** to prevent the page from timing out automatically. After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

- External Login page

  This option redirects the user to a login page on an external web server for authentication, instead of the first user-requested URL. Login information (user name and password) must be obtained by that page, and returned to the Array for authentication.

  Authentication occurs according to your configured RADIUS information. These parameters are configured as described in "Procedure for Configuring Network Security" on page 231, except that the **RADIUS Authentication Type** is selected here, as described below. After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

To set up external login page usage, set **Server** to **External Login**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

Select the **RADIUS Authentication Type**. This is the protocol used for authentication of users, **CHAP** or **PAP** (the default).

- **PAP** (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network "in the clear" (unencrypted) and is therefore considered insecure.
- **CHAP** (Challenge-Handshake Authentication Protocol) is a more secure Protocol. The login request is sent using a one-way hash function.

- External Splash page

  This option displays a splash page instead of the first user-requested URL. The splash page files reside on an external web server.

  To set up external splash page usage, set **Server** to **External Splash**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Secret**.

  After the splash page, the user is redirected to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

- Landing Page Only

  This option redirects the user to a specific landing page. If you select this option, enter the desired address in **Landing Page URL**.

Customizing an Internal Login or Splash page

You may customize these pages with a logo and/or background image, and header and/or footer text, as shown below in Figure 140.

Figure 140. Customizing an Internal Login or Splash Page

- **Background Image**—specify an optional jpg, gif, or png file to display in the background of the page. Other customizations (logo, header, footer) will overlay the background, so that it will not be visible in those areas.
- **Logo Image**—specify an optional jpg, gif, or png file to display at the top of the page.
- **Header Text File**—specify an optional .txt file to display at the top of the page (beneath the logo, if any).
- **Footer Text File**—specify an optional .txt file to display at the bottom of the page.

WPA Configuration Settings

If you set **Encryption** for this SSID to one of the WPA selections (Step 11 on page 251) and you did not check the **Global** checkbox (Step 12), this section will be displayed. The **WPA Configuration** encryption settings have the same

parameters as those described in "Procedure for Configuring Network Security" on page 231

RADIUS Configuration Settings

The RADIUS settings section will be displayed if you set **Authentication** (Step 10 on page 251) to **RADIUS MAC** and you did not check the **Global** checkbox (Step 12). This means that you wish to set up a RADIUS server to be used for this particular SSID. If **Global** is checked, then the security settings (including the RADIUS server, if any) established at the global level are used instead (see "Global Settings" on page 230).

The RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see "Procedure for Configuring an External RADIUS Server" on page 235).

See Also

DHCP Server
External Radius
Global Settings (IAP)
Internal Radius
Security Planning
SSIDs
Understanding QoS Priority on the Wireless Array

Active IAPs

By default, when a new SSID is created, that SSID is active on all IAPs. This window allows you to specify which IAPs will offer that SSID. Put differently, you can specify which SSIDs are active on each IAP.

This feature is useful in conjunction with WDS. You may use this window to configure the WDS link IAPs so that only the WDS link SSIDs are active on them.

Figure 141. Setting Active IAPs per SSID

Procedure for Specifying Active IAPs

1. **SSID**: For a given SSID row, check off the IAPs on which that SSID is to be active. Uncheck any IAPs which should not offer that SSID.
2. **All IAPs**: This button, in the last column, may be used to deny this SSID on all IAPs. Click again to activate the SSID on all IAPs.
3. **All SSIDs**: This button, in the bottom row, may be used to activate all SSIDs on this IAP. Click again to deny all SSIDs on this IAP.
4. **Toggle All**: This button, on the lower left, may be used to deny all SSIDs on all IAPs. Click again to activate all SSIDs on all IAPs.
5. Click **Save changes to flash** if you wish to make your changes permanent.

Per-SSID Access Control List

This window allows you to enable or disable the use of the per-SSID Access Control List (ACL), which controls whether a station with a particular MAC address may associate to this SSID. You may create access control list entries and delete existing entries, and control the type of list.

There is one ACL per SSID, and you may select whether its type is an Allow List or a Deny List, or whether use of this list is disabled. You may create up to 1000 entries per SSID.

There is also a global ACL (see "Access Control List" on page 227). If the same MAC address is listed in both the global ACL and in an SSID's ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

Figure 142. Per-SSID Access Control List

Procedure for Configuring Access Control Lists

1. **SSID**: Select the SSID whose ACL you wish to manage.
2. **Access Control List Type**: Select Disabled to disable use of the Access Control List for this SSID, or select the ACL type—either Allow List or Deny List.
    - **Allow List**: Only allows the listed MAC addresses to associate to the Array. All others are denied.

- **Deny List**: Denies the listed MAC addresses permission to associate to the Array. All others are allowed.

In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.

3. **MAC Address**: If you want to add a MAC address to the ACL, enter the new MAC address here, then click the **Add** button. The MAC address is added to the ACL. You may use a wildcard (*) for one or more digits to match a range of addresses. **Delete**: You may delete selected MAC addresses from this list by clicking their **Delete** buttons.
4. **Delete All**: This button, on the upper left, may be used to delete all the MAC entries in an ACL.
5. Click **Save changes to flash** if you wish to make your changes permanent.

Groups

This is a status-only window that allows you to review user (i.e., wireless client) Group assignments. It includes the group name, Radius ID, Device ID, VLAN IDs and QoS parameters and roaming layer defined for each group, and DHCP pools and web page redirect information defined for the group. You may click on a group's name to jump to the edit page for the group. There are no configuration options available on this page, but if you are experiencing problems or reviewing group management parameters, you may want to print this page for your records.

The **Limits** section of this window shows any limitations configured for your defined groups. For example, this window shows the current state of a group (enabled or disabled), how much group and per-station traffic is allowed, time on and time off, and days on and off.

For information to help you understand groups, see Understanding Groups below. For an in-depth discussion, please see the *Xirrus User Groups Application Note* in the *Xirrus Resource Center*.

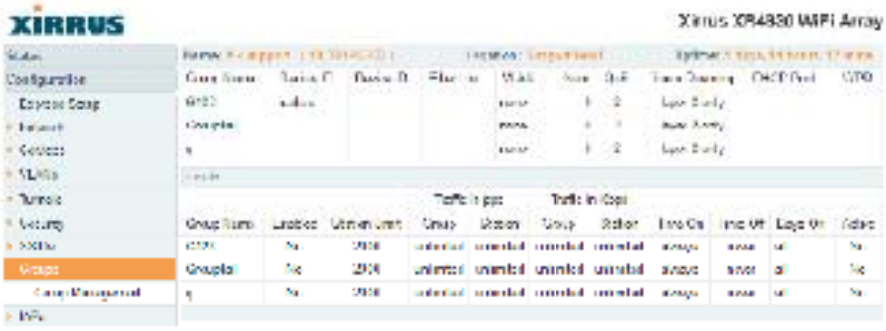

Figure 143. Groups

Understanding Groups

User groups allow administrators to assign specific network parameters to users (wireless clients) through RADIUS privileges rather than having to map users to an SSID tailored for that set of privileges. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs.

A group allows you to define a set of parameter values to be applied to selected users. For example, you might define the user group **Students**, and set its VLAN, security parameters, web page redirect (WPR), and traffic limits. When a new user is created, you can apply all of these settings just by making the user a member of the group. The group allows you to apply a uniform configuration to a set of users in one step.

In addition, you can restrict the group so that it only applies its settings to group members who are connecting using a specific device type, such as iPad or phone. Thus, you could define a group named **Student-Phone** with **Device ID** set to **Phone**, and set the group's **VLAN Number** to 100. This group's settings will only be applied to group members who connect using a phone, and they will all use VLAN 100. Note that settings for the group in the RADIUS server will override any settings on this WMI page.

Almost all of the parameters that can be set for a group are the same as SSID parameters. This allows you to configure features at the user group level, rather than for an entire SSID. If you set parameter values for an SSID, and then enter different values for the same parameters for a user group, the **user group values have priority** (i.e., group settings will override SSID settings).

Group names are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining Groups).

Using Groups

User accounts are used to authenticate wireless clients that want to associate to the Array. These accounts are established in one of two ways, using the **Security> Internal Radius** window or the **Security> External Radius** window. In either case, you may select a user group for the user, and that user group's settings will apply to the user:

- Internal Radius—when you add or modify a user entry, select a user group to which the user will belong.
- External Radius—when you add or modify a user account, specify the **Radius ID** for the user group to which the user will belong. This must be the same Radius ID that was entered in the Group Management window. When the user is authenticated, the external Radius server will send the

Radius ID to the Array. This will allow the Array to identify the group to which the user belongs.

See Also

External Radius
Internal Radius
SSIDs
Understanding QoS Priority on the Wireless Array
Web Page Redirect Configuration Settings
Understanding Fast Roaming

Group Management

This window allows you to manage groups (create, edit and delete), assign usage limits and other parameters on a per group basis, and configure the Web Page Redirect functionality.

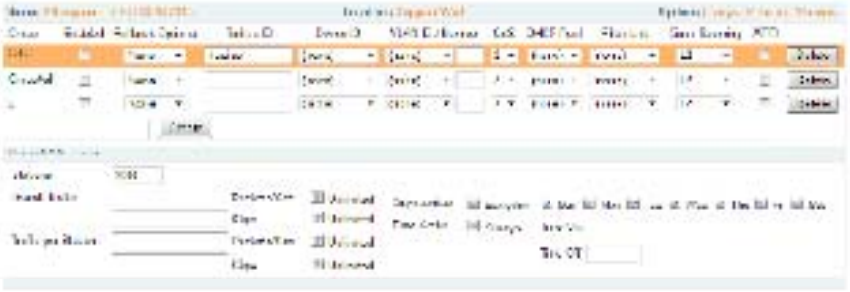

Figure 144. Group Management

Procedure for Managing Groups

1. **New Group Name:** To create a new group, enter a new group name next to the Create button, then click **Create**. You may create up to 16 groups.

   To configure and enable this group, proceed with the following steps.

2. **Group**: This column lists currently defined groups. When you create a new group, the group name appears in this list. Click on any group to select it, and then proceed to modify it as desired.

3. **Enabled**: Check this box to enable this group or leave it blank to disable it. When a group is disabled, users that are members of the group will behave as if the group did not exist. In other words, the options configured for the SSID will apply to the users, rather than the options configured for the group.

4. **Radius ID**: Enter a unique Radius ID for the group, to be used on an external Radius server. When adding a user account to the external server, this Radius ID value should be entered for the user. When the user is authenticated, Radius sends this value to the Array. This tells the Array that the user is a member of the group having this Radius ID.

5. **Device ID**: You may select a device type from this drop-down list, for example, **Notebook**, **phone**, **iPhone**, or **Android**. This allows you to apply the group settings only if a station authenticates as a user that is a member of the group and the station's device type matches **Device ID**. **Select none** if you do not want to consider the device type. If you have a Radius ID you should not enter a Device ID.

6. **VLAN ID**: (Optional) From the pull-down list, select a VLAN for this user's traffic to use. Select **numeric** and enter the number of a previously defined VLAN (see "VLANs" on page 199). This user group's VLAN settings supersede Dynamic VLAN settings (which are passed to the Array by the Radius server). To avoid confusion, we recommend that you avoid specifying the VLAN for a user in two places.

7. **QoS Priority**: (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:

   - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
   - 1—Medium; QoS prioritization is aggregated across all traffic types.
   - 2—High, normally used to give priority to video traffic.
   - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this group versus other traffic, as described in "Understanding QoS Priority on the Wireless Array" on page 244. The default value for this field is 2.

8. **DHCP Pool**: (Optional) To associate an internal DHCP pool to this group, select it from the pull--down list. Only one pool may be assigned. An internal DHCP pool must be created before it can be assigned. To create a DHCP pool, go to "DHCP Server" on page 197.

9. **Filter List**: (Optional) If you wish to apply a set of filters to this user group's traffic, select the desired Filter List. See "Filters" on page 344.

10. **Xirrus Roaming**: (Optional) For this group, select roaming behavior. Select **L2&L3** to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3. If you select **L2**, then roaming uses Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in Global Settings (IAP). You may select **Off** to disable fast roaming. See "Understanding Fast Roaming" on page 273.

11. **WPR (Web Page Redirect)**: (Optional) Check this box if you wish to enable the Web Page Redirect functionality. This will open a **Web Page Redirect** details section in the window, where your WPR parameters may be entered. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. See "Web Page Redirect Configuration Settings" on page 255 for details of WPR usage and configuration. Note that the Group Management window only allows you to set up an **Internal Splash** page and a **Landing Page URL**. The authentication options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the Array by a Radius server, this means the user has already been authenticated.

Group Limits

The Limits section allows you to limit the traffic or connection times allowed for this user group. Note that the IAPs—Global Settings window and the SSID management windows also have options to limit the number of stations, limit

traffic, and/or limit connection times. If limits are set in more than one place, all limits will be enforced:

- As soon as any station limit is reached, no new stations can associate until some other station has terminated its association.
- As soon as any traffic limit is reached, it is enforced.
- If any connection date/time restriction applies, it is enforced.

You can picture this as a logical AND of all restrictions. For example, suppose that a station's SSID is available MTWTF between 8:00am and 5:00pm, and the User Group is available MWF between 6:00am and 8:00pm, then the station will be allowed on MWF between 8:00am and 5:00pm.

To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

12. **Stations**: Enter the maximum number of stations allowed on this group. The default is 1536.
13. **Overall Traffic**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic for this group, or enter a value in the Packets/Sec field and make sure that the Unlimited box is unchecked to force a traffic restriction.
14. **Traffic per Station**: Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic per station for this group, or enter a value in the **Packets/Sec** or **Kbps** field and make sure that the Unlimited box is unchecked to force a traffic restriction.
15. **Days Active**: Choose **Everyday** if you want this group to be active every day of the week, or select only the specific days that you want this group to be active. Days that are not checked are considered to be the inactive days.
16. **Time Active**: Choose **Always** if you want this group active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that group members may associate.
17. To delete an entry, click its **Delete** button.

18. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

DHCP Server
External Radius
Internal Radius
Security Planning
SSIDs

IAPs

This status-only window summarizes the status of the Integrated Access Points (radios). For each IAP, it shows whether it is up or down, the channel and wireless mode, the antenna that it is currently using, its cell size and transmit and receive power, how many users (stations) are currently associated to it, whether it is part of a WDS link, and its MAC address.

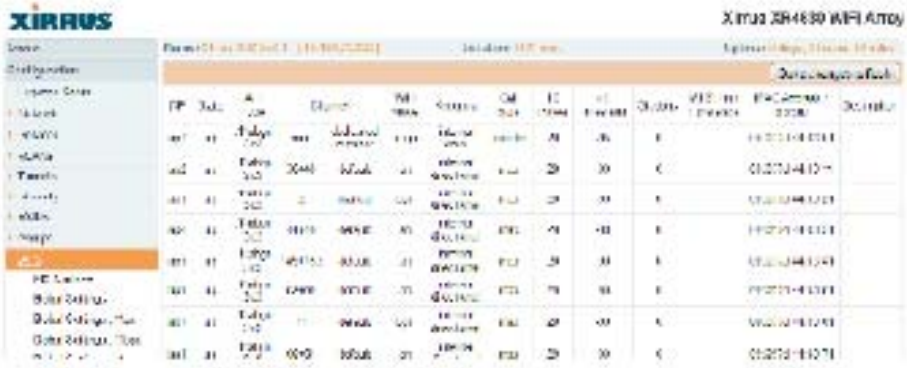

Figure 145. IAPs

The **Channel** column displays some status information that is not found elsewhere: the source of a channel setting. (Figure 146) If you set a channel manually (via IAP Settings), it will be labeled as **manual** next to the channel number (Figure 146). If an autochannel operation changed a channel, then it is labeled as **auto**. If the channel is set to the current factory default setting, the source will be **default**. This column also shows whether the channel selection is **locked**, or whether the IAP was automatically switched to this channel because the Array detected the signature of **radar** in operation on a conflicting channel (see also, Step 8 on page 282).

There are no configuration options in this window, but if you are experiencing problems or simply reviewing the IAP assignments, you may print this window for your records. Click any **IAP** name to open the associated configuration page.

IAP	State	AP Type	Channel		WiFi Mode	Antenna	Cell Size
iap1	up	11abgn 3x3	mon	dedicated monitor	abgn	internal omni	monitor
iap2	up	11abgn 3x3	36+40	default	an	internal directional	max
iap3	up	11abgn 3x3	2	manual	bgn	internal directional	max
iap4	up	11abgn 3x3	44+48	default	an	internal directional	max

Figure 146. Source of Channel Setting

Arrays have a fast roaming feature, allowing them to maintain sessions for applications such as voice, even while users cross boundaries between Arrays. Fast roaming is set up in the Global Settings (IAP) window and is discussed in:

- **"Understanding Fast Roaming" on page 273**

IAPs are configured using the following windows:

- **"IAP Settings" on page 274**
- **"Global Settings (IAP)" on page 280**
- **"Global Settings .11an" on page 293**
- **"Global Settings .11bgn" on page 298**
- **"Global Settings .11n" on page 304**
- **"Advanced RF Settings" on page 313**
- **"LED Settings" on page 334**
- **"DSCP Mappings" on page 335**
- **"Roaming Assist" on page 336**

See Also

IAP Statistics Summary

Understanding Fast Roaming

To maintain sessions for real-time data traffic, such as voice and video, users must be able to maintain the same IP address through the entire session. With traditional networks, if a user crosses VLAN or subnet boundaries (i.e., roaming between domains), a new IP address must be obtained.

Mobile wireless users are likely to cross multiple roaming domains during a single session (especially wireless users of VoIP phones). **Layer 3 roaming** allows a user to maintain the same IP address through an entire real-time data session. The user may be associated to any of the VLANs defined on the Array. The Layer 3 session is maintained by establishing a tunnel back to the originating Array. You should decide whether or not to use Layer 3 roaming based on your wired network design. Layer 3 roaming incurs extra overhead and may result in additional traffic delays.

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your Array, see Step 28 to Step 30 in "Global Settings (IAP)" on page 280. To choose which of the enabled options are used by an SSID or Group, see "Procedure for Managing SSIDs" on page 250 (Step 13) or "Procedure for Managing Groups" on page 266.

IAP Settings

This window allows you to enable/disable IAPs, define the wireless mode for each IAP, specify the channel to be used and the cell size for each IAP, lock the channel selection, establish transmit/receive parameters, select antennas, and reset channels. Buttons at the bottom of the list allow you to **Reset Channels**, **Enable All IAPs, or Disable All IAPs**. When finished, click **Save changes to flash** if you wish to make your changes permanent.

Figure 147. IAP Settings

You may also access this window by clicking on the Array image at the lower left of the WMI window—click the orange Xirrus logo in the center of the Array. See "User Interface" on page 88.

Procedure for Auto Configuring IAPs

You can auto-configure channel and cell size of radios by clicking on the **Auto Configure** buttons on the relevant WMI page (auto configuration only applies to enabled radios):

- For all radios, go to "Advanced RF Settings" on page 313.
- For all 802.11a settings, go to "Global Settings .11an" on page 293.
- For all 802.11bg settings, go to "Global Settings .11bgn" on page 298.
- For all 802.11n settings, go to "Global Settings .11n" on page 304.

Procedure for Manually Configuring IAPs

1. In the **Enabled** column, check the box for an IAP to enable it, or uncheck the box if you want to disable the IAP.

   In the **Band** column, select the wireless band for this IAP from the choices available in the pull-down menu, either **2.4GHz** or **5 GHz**. Choosing the **5GHz** band will automatically select an adjacent channel for bonding. If the band displayed is **auto**, the **Band** is about to be changed based on a new **Channel** selection that you made that requires the change.

   One of the IAPs must be set to **monitor** mode to support Spectrum Analyzer, Radio Assurance (**loop**back testing), and Intrusion Detection features.

   For XN16 Arrays only—
   The XN16 allows up to 12 IAPs to operate as 5 GHz—802.11an radios concurrently using internal antennas. Do not set Mode to 5 GHz for more than 12 IAPs unless you are using external antennas. Please contact Xirrus Customer Support for details.

2. In the **WiFi Mode** column, select the IEEE 802.11 wireless mode (or combination) that you want to allow on this IAP. The drop-down list will only display the appropriate choices for the selected **Band**. For example, the 5 GHz band allows you to select **an**, **a-only**, or **n-only**, while 2.4GHz also includes 802.11b and 802.11g choices. When you select a WiFi Mode for an IAP, your selection in the **Channel** column will be checked to ensure that it is a valid choice for that WiFi Mode.

   By selecting appropriate WiFi Modes for the radios on your Arrays, you can greatly improve wireless network performance. For example, if you have 802.11b and 802.11n stations using the same IAP, throughput on that radio is reduced greatly for the 802.11n stations. By supporting 802.11b stations only on selected radios in your network, the rest of your 802.11a or 11n radios will have greatly improved performance. Take care to ensure that your network provides adequate coverage for the types of stations that you need to support.

3. In the **Channel** column, select the channel you want this IAP to use from the channels available in the pull-down list. The list shows the channels available for the IAP selected (depending on which band the IAP is using). Channels that are shown in color indicate conditions that you need to keep in mind:

   - RED—Usage is not recommended, for example, because of overlap with neighboring radios.
   - YELLOW—The channel has less than optimum separation (some degree of overlap with neighboring radios).
   - GRAY—The channel is already in use.

   The channels that are available for assignment to an IAP will differ, depending on the country of operation. If **Country** is set to **United States** in the Global Settings (IAP) window, then 21 channels are available to 802.11an radios.

   As mandated by FCC/IC law, Arrays continually scan for signatures of radar. If such a signature is detected, the Array will switch operation from conflicting channels to new ones. The Array will switch back to the original channel after 30 minutes if the channel is clear. If a radio was turned off because there were no available channels not affected by radar, the Array will now bring that radio back up after 30 minutes if that channel is clear. The 30 minute time frame complies with FCC/IC regulations.

4. The **Bond** column works together with the channel bonding options selected on the Global Settings .11n page. Also see the discussion of 802.11n bonding in "Channel Bonding" on page 39.

   - **Channel number**—If a channel number appears, then this channel is already bonded to the listed channel.
   - **Off**—Do not bond his channel to another channel.
   - **On**—Bond this channel to an adjacent channel. The bonded channel is selected automatically by the Array based on the **Channel** (Step 3). The choice of banded channel is static—fixed once the selection is made.

- **+1**—Bond this channel to the next higher channel number. Auto Channel bonding does not apply. This option is only available for some of the channels.
- **-1**—Bond this channel to the next lower channel number. Auto Channel bonding does not apply. This option is only available for some of the channels.

5. Click the **Lock** check box if you want to lock in your channel selection so that an autochannel operation (see Advanced RF Settings) can't change it.

6. In the **Cell Size** column, select **auto** to allow the optimal cell size to be automatically computed (see also, "RF Power & Sensitivity" on page 316). To set the cell size yourself, choose either **small**, **medium**, **large**, or **max** to use the desired pre-configured cell size, or choose **manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx dBm** (transmit) and **Rx dBm** (receive) fields. The default is **max**. If you select a value other than **auto**, the cell size will not be affected by cell size auto configuration. Note that ultra low power **Tx dBm** settings are possible. Values from -15dB to 5dB are provided specifically to help in high density 2.4 GHz environments.

   When other Arrays are within listening range of this one, setting cell sizes to **Auto** allows the Array to change cell sizes so that coverage between cells is maintained. Each cell size is optimized to limit interference between sectors of other Arrays on the same channel. This eliminates the need for a network administrator to manually tune the size of each cell when installing multiple Arrays. In the event that an Array or a radio goes offline, an adjacent Array can increase its cell size to help compensate.

   The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the Array's cell diameter. In a large office, or if multiple Arrays are in use, you may choose **Small** cells to achieve a higher data rate, since walls and other objects will not define the cells naturally.

For additional information about cell sizes, go to "Coverage and Capacity Planning" on page 28.

7. If you are using WDS to provide backhaul over an extended distance, use **WDS Dist. (Miles)** to prevent timeout problems associated with long transmission times. Set the approximate distance in miles between this IAP and the connected Array in this column. This increases the wait time for frame transmission accordingly.
8. In the **Antenna Select** column, choose the antenna you want this radio to use from the pull-down list. The list of available antennas will be different (or no choices will be available), depending on the Array model and on the wireless mode you selected for the IAP.
9. If desired, enter a description for this IAP in the **Description** field.
10. You may reset all of the enabled IAPs by clicking the **Reset Channels** button at the bottom of the list. A message will inform you that all enabled radios have been taken down and brought back up.

11. Buttons at the bottom of the list allow you to **Enable All IAPs** or **Disable All IAPs**.
12. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11an

Global Settings .11bgn
Global Settings .11n
IAPs
IAP Statistics Summary
LED Settings

Global Settings (IAP)

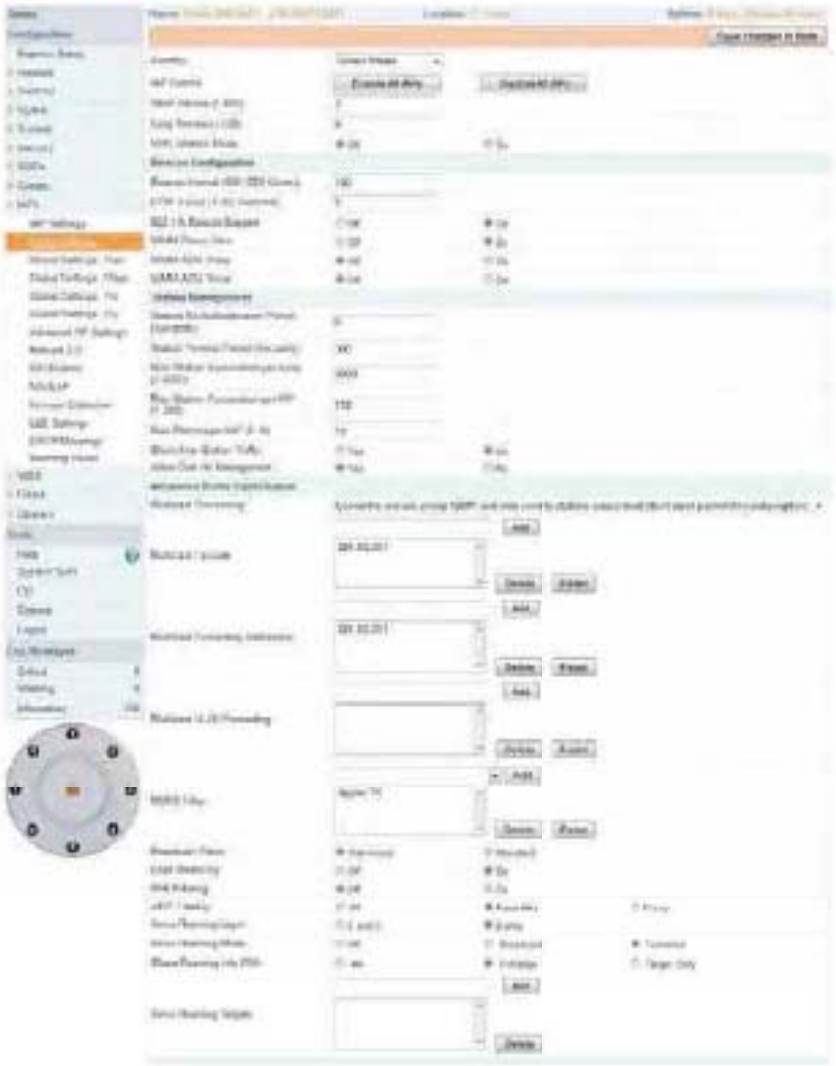

Figure 148. Global Settings (IAP's)

This window allows you to establish global IAP settings. Global IAP settings include enabling or disabling all IAPs (regardless of their operating mode), and changing settings for beacons, station management, and advanced traffic optimization—including multicast processing, load balancing, and roaming. Changes you make on this page are applied to all IAPs, without exception.

Procedure for Configuring Global IAP Settings

Some of the features below, such as Load Balancing, are only available if the Array's license includes the ***Xirrus Advanced RF Performance Manager (RPM)****. If a setting is unavailable (grayed out), then your license does not support the feature. See* ***"About Licensing and Upgrades" on page 361.***

1. **Country**: This is a display-only value. Once a country has been set, it may not be changed.

   The channels that are available for assignment to an IAP will differ, depending on the country of operation. If **Country** is set to **United States**, then 21 channels are available for 802.11a/n.

   If no country is displayed, the channel set defaults to channels and power levels that are legal worldwide—this set only includes the lower eight 5 GHz channels.

2. **IAP Control**: Click on the **Enable All IAPs** button to enable all IAPs for this Array, or click on the **Disable All IAPs** button to disable all IAPs.

3. **Short Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value (1 to 128) in the **Short Retry Limit** field if you want to increase or decrease this attribute.

4. **Long Retries**: This sets the maximum number of transmission attempts for a frame, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value (1 to 128) in the **Long Retry Limit** field if you want to increase or decrease this attribute.

5. **Wi-Fi Alliance Mode**: Set this **On** if you need Array behavior to conform completely to Wi-Fi Alliance standards. This mode is normally set to **Off**.

Beacon Configuration

6. **Beacon Interval**: When the Array sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000 Kusecs. A Kusec is 1000 microseconds = 1 millisecond. The value you enter here is applied to all IAPs.

7. **DTIM Period**: A DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by the Array to a client device in sleep mode, alerting the device to broadcast traffic awaiting delivery. The **DTIM Period** is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all IAPs.

8. **802.11h Beacon Support**: This option enables beacons on all of the Array's radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.

9. **WMM Power Save**: Click **On** to enable Wireless Multimedia Power Save support, as defined in IEEE802.11e. This option saves power and increases battery life by allowing the client device to doze between packets to save power, while the Array buffers downlink frames. The default setting is **On**.

10. **WMM ACM Video**: Click **On** to enable Wireless Multimedia Admission Control for video traffic. When admission control for video is enabled, the Array evaluates a video request from a client device against the network load and channel conditions. If the network is not congested, it accepts the request and grants the client the medium time for its traffic stream. Otherwise, it rejects the request. Some clients contain sufficient

intelligence to decide to either delay the traffic stream, associate with a different AP, or establish a best-effort traffic stream outside the operation of WMM-Admission Control. The default setting is **Off**.

11. **WMM ACM Voice**: Click **On** to enable Wireless Multimedia Admission Control for voice calls. When admission control for voice is enabled, the Array evaluates a voice request from a client device against the network load and channel conditions. If the network is not congested, it accepts the request and grants the client the medium time for its call. Otherwise, it rejects the request. Some clients contain sufficient intelligence to decide to either delay the traffic stream, associate with a different AP, or establish a best-effort traffic stream outside the operation of WMM-Admission Control. The default setting is **Off**.

Station Management

12. **Station Re-Authentication Period**: This specifies an interval (in seconds) for station reauthentications. This is the minimum time period between station authentication attempts, enforced by the Array. This feature is part of the Xirrus Advanced RF Security Manager (RSM).

13. **Station Timeout Period**: Specify a time (in seconds) in this field to define the timeout period for station associations.

14. **Max Station Association per Array**: This option allows you to define how many station associations are allowed per Array (up to 1280 stations per Array). Note that the **Max Station Association per IAP** limit (below) may not be exceeded. If you have an unlicensed Array, this value is set to 1, which simply allows you to test the ability to connect to the Array.

15. **Max Station Association per IAP**: This defines how many station associations are allowed per IAP. Note that the SSIDs—SSID Management window also has a station limit option—**Station Limit** (page 254). If both station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.

16. **Max Phones per IAP**: This option allows you to control the maximum number of phones that are allowed per IAP. The default is set to a maximum of 16 but you can reduce this number, as desired. Enter a value in this field between 0 (no phones allowed) and 16.

This admission control feature applies only to Spectralink phones. It does not apply to all VoIP phones in general.

17. **Block Inter-Station Traffic**: This option allows you to block or allow traffic between wireless clients that are associated to the Array. Choose either **Yes** (to block traffic) or **No** (to allow traffic).

18. **Allow Over Air Management**: Choose **Yes** to enable management of the Array via the IAPs, or choose **No** (recommended) to disable this feature.

Advanced Traffic Optimization

19. **Multicast Processing**: This sets how multicast traffic is handled. Multicast traffic can be received by a number of subscribing stations at the same time, thus saving a great deal of bandwidth. In some of the options below, the Array uses IGMP snooping to determine the stations that are subscribed to the multicast traffic. IGMP (Internet Group Management Protocol) is used to establish and manage the membership of multicast groups.

    Multicast handling options are only applicable to traffic transmitted from the Array to wireless stations. Select one of the following options:

    - **Send multicasts unmodified**. This is useful when multicast is not needed because no video or audio streaming is required or when it is used only for discovering services in the network. Some situations where you might use this option are:
        - for compatibility with ordinary operation, i.e., there is no optimization or modification of multicast traffic.
        - if you have an application where many subscribers need to see the multicast—a large enough number that it would be less efficient to convert to unicast and better just to send out multicast

even though it must be sent out at the speed of the slowest connected station.

An example of a situation that might benefit from the use of this mode is ghosting all the laptops in a classroom using multicast. One multicast stream at, say, 6 Mbps is probably more efficient than thirty unicast streams.

The next three options convert multicast to unicast. Packets are sent directly to the stations at the best possible data rates. This approach significantly improves the quality of the voice and video multicast streams.

- **Convert to unicast and send unicast packets to all stations**. This may be useful in link-local multicast situations.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (send as multicast if no subscription)**. This option is useful when you need to stream voice or video multicast traffic to all stations, but some stations are capable of subscribing to multicast groups while other stations are not. The stations that do not subscribe will not benefit from conversion to unicast; their video or voice quality may be compromised.
- **Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription)**. This option is useful in well controlled environments when you need to stream voice or video multicast traffic only to stations that are capable of subscribing to multicast groups and there is no need for the rest of the stations to receive the data stream.

20. **Multicast Exclude:** This is a list of multicast IP addresses that will not be subject to multicast-to-unicast conversion. This list is useful on networks where applications such as those using multicast Domain Name System (mDNS) are in use. For example, Apple Bonjour finds local network devices such as printers or other computers using mDNS. By default, the list contains the IPv4 multicast address for Apple Bonjour mDNS: 224.0.0.251.

To add a new IP address to the list, type it in the top field and click the **Add** button to its right. You may only enter IP addresses—host names are not allowed. This is because mDNS is a link local multicast address, and does not require IGMP to the gateway.

To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

21. **Multicast Forwarding**

Multicast Forwarding is a Xirrus feature that forwards selected multicast traffic between wired VLANs and wireless SSIDs. For example, Apple devices use mDNS to advertise and find services, using local network multicasts that are not routed. This creates an issue when you are using Apple devices on the Wireless LAN, and have other devices that provide services connected on the wired infrastructure in a different VLAN, for example, printers and AppleTV devices. One way to address this issue is to set up multicast forwarding between the wireless SSID and the wired VLAN. This requires the wired VLAN to be trunked to the Array. Once configured correctly, mDNS traffic will be forwarded from the specified wireless network(s) to the specified wired VLANs and vice-versa, subject to any mDNS service filtering defined (Step 23).

Use multicast forwarding together with multicast VLAN forwarding (Step 22) and mDNS filtering (Step 23) to make services available across VLANs as follows:

- In **Multicast Forwarding Addresses**, enter a list of multicast addresses that you want forwarded, for example, 224.0.0.251 (the multicast address for Bonjour).
- In **Multicast VLAN Forwarding**, enter a list of VLANs that participate in the multicast forwarding.
- In **MDNS Filter**, specify the mDNS service types that are allowed to be forwarded.
  - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed.*

- If you enter service types, then this acts as an allow filter, and *mDNS packets are passed only for the listed service types.*

Note that mDNS filtering may be used to filter the mDNS packet types that are forwarded within the same VLAN. Also, in conjunction with multicast forwarding, it may be used to filter the mDNS packet types that are forwarded across configured VLANs.

After you have entered these settings, when multicast packets arrive from the wired network from one of the **Multicast Forwarding Addresses** on any VLAN specified in **Multicast VLAN Forwarding**, they are forwarded to the corresponding wireless SSID for that VLAN. .

Multicast packets coming in from the wireless network on an SSID tied to one of the specified VLANs and matching one of the **Multicast Forwarding Addresses** are forwarded to the specified VLANs on the wired network.

No modifications are made to the forwarded packets – they are just forwarded between specified VLANs and associated SSIDs.

Xirrus strongly recommends the use of MDNS Filters (Step 23) when using multicast forwarding. Only allow required services to be forwarded.

Carefully monitor results, as forwarding may flood your network with multicast traffic. Experience has shown Bonjour devices to be very chatty. Also note that since this is link local multicast traffic, it will be sent to every wired port in the VLAN, as IGMP snooping does not work with link local multicast addresses.

To specify **Multicast Forwarding Addresses:** enter each IP address in the top field and click the **Add** button to its right. You may only enter IPv4 multicast addresses - host names are not allowed. To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

22. **Multicast VLAN Forwarding:** This is a list of VLANs that participate in the multicast forwarding. Please see the description of multicast forwarding in Step 21 above.

The VLANs you enter must be explicitly defined (see "VLANs" on page 199) in order to participate in multicast forwarding. In fact, the Array discards packets from undefined VLANs.

To add a new VLAN to the list, enter its number or name in the top field and click the **Add** button to its right. You may enter multiple VLANs at once, separated by a space. To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

These VLANs must be trunked to the Array from the LAN switch, and be defined on the Array. See "VLAN Management" on page 201 and "SSID Management" on page 249.

Note that Multicast Forwarding and mDNS Filtering capabilities also work if both devices are wireless. For example, let's say that AppleTV is using wireless to connect to an SSID that is associated with VLAN 56, and the wireless client is on an SSID that is associated with VLAN 58. Normally the wireless client would not be able to use Bonjour to discover the AppleTV because they are on separate VLANs. But if you add 224.0.0.251 to the ***Multicast Forwarding Addresses****, then add VLANs 56 and 58 to the* ***Multicast VLAN Forwarding*** *list, then the wireless client will be able to discover the AppleTV. In this same scenario you could add AppleTV to the* ***MDNS Filter*** *list so that only MDNS packets for the AppleTV service type would be forwarded between VLANs 56 and 58.*

Note that all the VLANs that you add to this list do not have to be associated with SSIDs. As an example, say that AppleTV is on the wired network on VLAN 56, while the wireless device is connected to an SSID that is associated to VLAN 58. In this case, VLAN 56 and 58 need to be defined on the Array but only VLAN 58 needs to be associated to a SSID.

23. **MDNS Filter**: There are many different types of services that may be specified in multicast query and response packets. The mDNS filters let you restrict forwarding, so that multicast packets are forwarded only for the services that you explicitly specify. This list may be used to restrict the amount of Apple Bonjour multicast traffic forwarding. For example, you may restrict forwarding to just AppleTV and printing services. Please see the description of multicast forwarding in Step 21 above.

    The **MDNS Filter** operates as follows:

    - If you leave this field blank, then there is ***no*** filter, and *mDNS packets for all service types are passed.*
    - If you enter service types, then this acts as an allow filter, and *mDNS packets are passed only for the listed service types.*

    To add an mDNS packet type to the list of packets that may be forwarded, select it from the drop-down list in the top field and click the **Add** button to its right. The drop-down list offers packet types such as **AirTunes**, **Apple-TV**, **iChat**, **iPhoto**, **iTunes**, **iTunes-Home-Sharing**, **Internet-Printing**, **Mobile-Device-Sync**, and **Secure-Telnet**.

    For example, to allow mirroring of an iPad on an Apple-TV, select **Apple-TV**.

    You may define your own type if you do not see the service you want in the drop-down list. Simply enter the mDNS service name that you would like to allow through. Custom mDNS packet types must be prefixed with an underscore, e.g., **_airvideoserver**.

    To remove an entry, select it in the list and click **Delete**. To remove *all* entries from the list, click **Reset**.

24. **Broadcast Rates**: This changes the rates of broadcast traffic sent by the Array (including beacons). When set to **Optimized**, each broadcast or multicast packet that is transmitted on each radio is sent at the lowest transmit rate used by any client associated to that radio at that time. This results in each IAP broadcasting at the highest Array TX data rate that can be heard by all associated stations, improving system performance. The rate is determined dynamically to ensure the best broadcast/multicast

performance possible. The benefit is dramatic. Consider a properly designed network (having -70db or better everywhere), where virtually every client should have a 54Mbps connection. In this case, broadcasts and multicasts will all go out at 54Mbps vs. the standard rate. Thus, with broadcast rate optimization on, broadcasts and multicasts use between 2% and 10% of the bandwidth that they would in Standard mode.

When set to **Standard** (the default), broadcasts are sent out at the lowest basic rate only—6 Mbps for 5GHz clients, or 1 Mbps for 2.4GHz clients. The option you select here is applied to all IAPs.

25. **Load Balancing:** The Xirrus Wireless Array supports an automatic load balancing feature designed to distribute wireless stations across multiple radios rather than having stations associate to the closest radios with the strongest signal strength, as they normally would. In wireless networks, the station decides to which radio it will associate. The Array cannot actually force load balancing, however the Array can "encourage" stations to associate in a more uniform fashion across all of the radios of the Array. This option enables or disables active load balancing between the Array IAPs. For an in-depth discussion, see the *Xirrus Station Load Balancing Application Note* in the *Xirrus Resource Center*.

    If you select **On** and an IAP is overloaded, that IAP will send an "AP Full" message in response to Probe, Association, or Authentication requests. This prevents determined clients from forcing their way onto overloaded IAPs. Note that some clients are so determined to associate to a particular IAP that they will not try to associate to another IAP, and thus they never get on the network.

    Choose **Off** to disable load balancing.

26. **ARP Filtering:** Address Resolution Protocol finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. ARP filtering allows you to reduce the proliferation of ARP messages by restricting how they are forwarded across the network.

    You may select from the following options for handling ARP requests:

- **Off**: ARP filtering is disabled. ARP requests are broadcast to radios that have stations associated to them.
- **Pass-thru**: The Array forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it. This is the default value.
- **Proxy**: The Array replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

Note that the Array has a broadcast optimization feature that is always on (it is not configurable). Broadcast optimization restricts all broadcast packets (not just ARP broadcasts) to only those radios that need to forward them. For instance, if a broadcast comes in from VLAN 10, and there are no VLAN 10 users on a radio, then that radio will not send out that broadcast. This increases available air time for other traffic.

27. **IPv6 Filtering**: this setting allows blocking of IPv6 traffic which may be a concern for IT managers. The Xirrus Array currently bridges IPv6 traffic. Set IPv6 filtering **On** if you wish to prevent the forwarding of IPv6 packets through the Array in both directions—wired network to wireless and wireless network to wired. The default is **Off**.

28. **Xirrus Roaming Layer**: Select whether to enable roaming capabilities between IAPs or Arrays at Layer **2 and 3**, or at Layer **2 only**. Depending on your wired network, you may wish to allow fast roaming at Layer 3. This may result in delayed traffic.

29. **Xirrus Roaming Mode**: This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3 (as specified in Step 30), while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see "Understanding Fast Roaming" on page 273 for a discussion of this feature). XRP uses a discovery process to identify other Xirrus Arrays as fast roaming targets. This process has two modes:

    - **Broadcast**—the Array uses a broadcast technique to discover other Arrays that may be targets for fast roaming.

- **Tunneled**—in this Layer 3 technique, fast roaming target Arrays must be explicitly specified.

To enable fast roaming, choose **Broadcast** or **Tunneled**, and set additional fast roaming attributes (Step 30). To disable fast roaming, choose **Off**. If you enable Fast Roaming, the following ports **cannot** be blocked:

- **Port 22610**—reserved for Layer 2 roaming using UDP to share PMK information between Arrays.
- **Ports 15000 to 17999**—reserved for Layer 3 roaming (tunneling between subnets).

30. **Share Roaming Info With:** Three options allow your Array to share roaming information with all Arrays; just with those that are within range; or with specifically targeted Arrays. Choose either **All**, **In Range** or **Target Only**, respectively.

    a. **Xirrus Roaming Targets:** If you chose **Target Only**, use this option to add target MAC addresses. Enter the MAC address of each target Array, then click on **Add** (add as many targets as you like). To find a target's MAC address, open the **Array Info** window on the target Array and look for **IAP MAC Range**, then use the starting address of this range.

    To delete a target, select it from the list, then click **Delete**.

See Also

Coverage and Capacity Planning
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
Advanced RF Settings
IAPs
IAP Statistics Summary
LED Settings
IAP Settings

Global Settings .11an

This window allows you to establish global 802.11a IAP settings. These settings include defining which 802.11a data rates are supported, enabling or disabling all 802.11an IAPs, auto-configuration of channel allocations for all 802.11an IAPs, and specifying the fragmentation and RTS thresholds for all 802.11an IAPs.

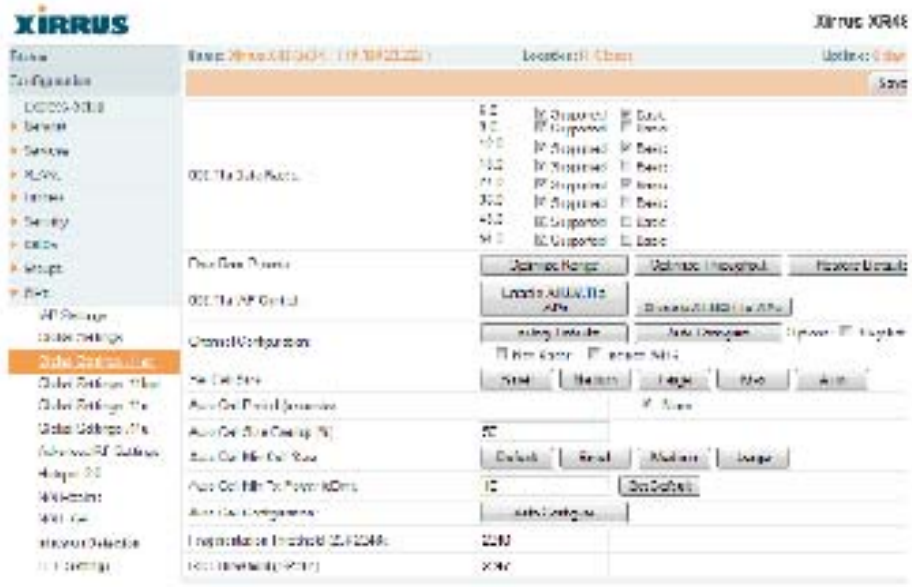

Figure 149. Global Settings .11an

Procedure for Configuring Global 802.11an IAP Settings

1. **802.11a Data Rates:** The Array allows you to define which data rates are supported for all 802.11an radios. Select (or deselect) data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.
2. **Data Rate Presets**: The Wireless Array can optimize your 802.11a data rates automatically, based on range or throughput. Click **Optimize Range**

to optimize data rates based on range, or click **Optimize Throughput** to optimize data rates based on throughput. The **Restore Defaults** button will take you back to the factory default rate settings.

3. **802.11a IAP Control**: Click **Enable 802.11a IAPs** to enable all 802.11an IAPs for this Array, or click **Disable 802.11a IAPs** to disable all 802.11an IAPs.

*Some of the features below, such as Auto Configure for Cell Size and Channel Configuration, are only available if the Array's license includes the **Xirrus Advanced RF Performance Manager (RPM)**. If a setting is unavailable (grayed out), then your license does not support the feature. Please see "About Licensing and Upgrades" on page 361.*

4. **Channel Configuration**: Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11an IAP and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11a channel allocation (see "RF Spectrum Management" on page 318).

   Click **Factory Defaults** if you wish to instruct the Array to return all IAPs to their factory preset channels. As of release 6.3, Arrays no longer all use the same factory preset values for channel assignments. Instead, if the Array has been deployed for a while and already has data from the spectrum analyzer and Xirrus Roaming Protocol about channel usage on neighboring arrays, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the Array has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On the XR-500 and XR-1000 Series Arrays, the **Factory Defaults** button will not restore iap1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **Timeshare Mode** again - see "RF Monitor" on page 314.*

The following options may be selected for auto configuration:

- **Non-Radar**: give preference to channels that are not required to use dynamic frequency selection (DFS) to avoid communicating in the same frequency range as some radar (also see Step 8 on page 282).

Channels Required to Use DFS Radar Avoidance in USA			
36+40	Non-radar	116+120	DFS required
44+48	Non-radar	124+128	DFS required
52+56	DFS required	132+136	DFS required
60+64	DFS required	149+153	Non-radar
100+104	DFS required	157+161	Non-radar
108+112	DFS required		

- **Negotiate**: negotiate air-time with other Arrays before performing a full scan.
- **Full Scan**: perform a full traffic scan on all channels on all IAPs to determine the best channel allocation.
- **Include WDS**: automatically assign 5GHz to WDS client links.

To use the Auto Cell Size feature, the following additional settings are required:

*RF Monitor Mode must be turned **On**. See **"RF Monitor" on page 314***

*One of the radios must be in **monitor** mode with the default **RxdBm** setting of **-95**, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See **"Procedure for Manually Configuring IAPs" on page 275**.*

5. **Set Cell Size**: Cell Size may be set globally for all 802.11an IAPs to **Auto**, **Large**, **Medium**, **Small**, or **Max** using the buttons.

For an overview of RF power and cell size settings, please see "RF Power & Sensitivity" on page 316, "Capacity and Cell Sizes" on page 30, and "Fine Tuning Cell Sizes" on page 31.

6. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

7. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

8. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large**, **Medium**, or **Small**.

9. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

10. **Auto Cell Configuration**: Click this button to instruct the Array to determine and set the best cell size for each 802.11an IAP whose **Cell Size** is **auto** on the IAP Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the IAP Settings window to view the cell size settings that were applied.

11. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11an radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here.

Smaller fragmentation numbers can help to "squeeze" packets through in noisy environments. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346.

12. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11bgn
Global Settings .11n
IAPs
IAP Statistics Summary
Advanced RF Settings
IAP Settings

Global Settings .11bgn

This window allows you to establish global 802.11b/g IAP settings. These settings include defining which 802.11b and 802.11g data rates are supported, enabling or disabling all 802.11b/g IAPs, auto-configuring 802.11b/g IAP channel allocations, and specifying the fragmentation and RTS thresholds for all 802.11b/g IAPs.

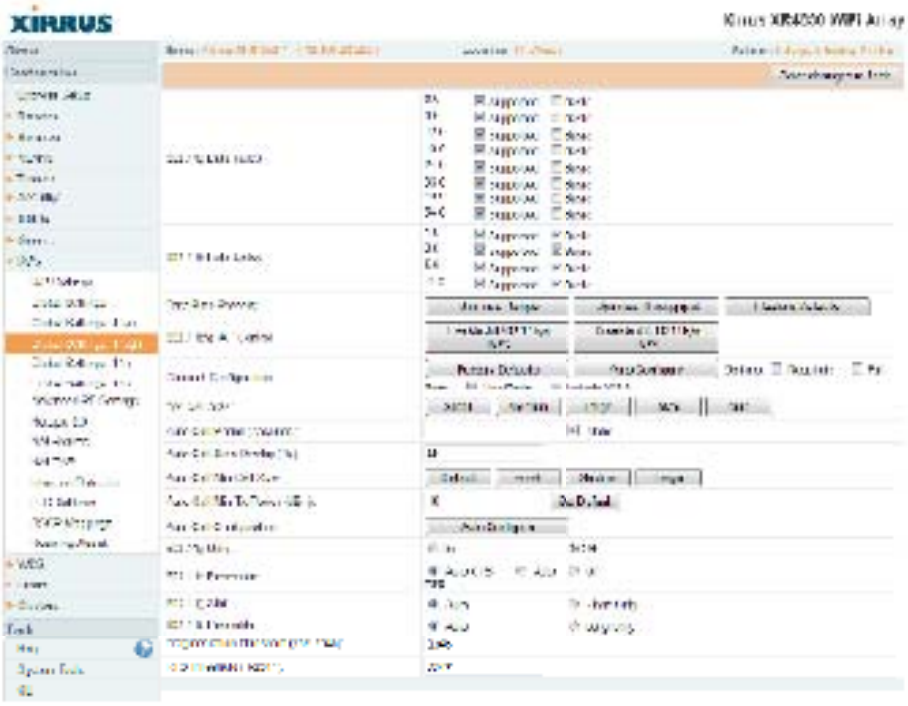

Figure 150. Global Settings .11bgn

Some of the features below, such as Auto Configure for Cell Size and Channel Configuration, are only available if the Array's license includes the ***Xirrus Advanced RF Performance Manager (RPM)****. If a setting is unavailable (grayed out), then your license does not support the feature. Please see* ***"About Licensing and Upgrades" on page 361.***

Procedure for Configuring Global 802.11b/g IAP Settings

1. **802.11g Data Rates:** The Array allows you to define which data rates are supported for all 802.11g radios. Select (or deselect) 11g data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
   - **Basic Rate—**a wireless station (client) must support this rate in order to associate.
   - **Supported Rate—**data rates that can be used to transmit to clients.
2. **802.11b Data Rates**: This task is similar to Step 1, but these data rates apply only to 802.11b IAPs.
3. **Data Rate Presets**: The Wireless Array can optimize your 802.11b/g data rates automatically, based on range or throughput. Click **Optimize Range** button to optimize data rates based on range, or click on the **Optimize Throughput** to optimize data rates based on throughput. **Restore Defaults** will take you back to the factory default rate settings.
4. **802.11b/g IAP Control**: Click **Enable All 802.11b/g IAPs** to enable all 802.11b/g IAPs for this Array, or click **Disable All 802.11b/g IAPs** to disable them.
5. **Channel Configuration**: Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11b/g IAP and select the channel automatically, based on changes in the environment. This is the recommended method for channel allocation (see "RF Spectrum Management" on page 318).

   Click **Factory Defaults** if you wish to instruct the Array to return all IAPs to their factory preset channels. As of release 6.3, Arrays no longer all use the same factory preset values for channel assignments. Instead, if the Array has been deployed for a while and already has data from the spectrum analyzer and Xirrus Roaming Protocol about channel usage on neighboring arrays, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the Array has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior

data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On the XR-500 and XR-1000 Series Arrays, the **Factory Defaults** button will not restore iap1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **Timeshare Mode** again - see "RF Monitor" on page 314.*

The following options may be selected for auto configuration:

- **Negotiate**: negotiate air-time with other Arrays before performing a full scan.
- **Full Scan**: perform a full traffic scan on all channels on all IAPs to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in "Procedure for Configuring Global 802.11an IAP Settings" on page 293.
- **Include WDS**: automatically assign 5GHz to WDS client links.

To use the Auto Cell Size feature, the following additional settings are required:

*RF Monitor Mode must be turned **On**. See **"RF Monitor" on page 314***

*One of the radios must be in **monitor** mode with the default **RxdBm** setting of **-95**, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See **"Procedure for Manually Configuring IAPs" on page 275**.*

6. **Set Cell Size/ Autoconfigure**: Cell Size may be set globally for all 802.11b/g IAPs to **auto, large, medium, small,** or **max** using the drop down menu.

   For an overview of RF power and cell size settings, please see "RF Power & Sensitivity" on page 316, "Capacity and Cell Sizes" on page 30, and "Fine Tuning Cell Sizes" on page 31.

7. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

8. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

9. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large**, **Medium**, or **Small**.

10. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

11. **Auto Cell Configuration**: Click **Auto Configure** to instruct the Array to determine and set the best cell size for each enabled 802.11b/g IAP whose **Cell Size** is **auto** on the IAP Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the IAP Settings window to view the cell size settings that were applied.

12. **802.11g Only**: Choose **On** to restrict use to 802.11g mode only. In this mode, no 802.11b rates are transmitted. Stations that only support 802.11b will not be able to associate.

13. **802.11g Protection**: You should select **Auto CTS** or **Auto RTS** to provide automatic protection for all 802.11g radios in mixed networks (802.11 b and g). You may select **Off** to disable this feature, but this is not recommended. Protection allows 802.11g stations to share an IAP with

older, slower 802.11b stations. Protection avoids collisions by preventing 802.11b and 802.11g stations from transmitting simultaneously. When **Auto CTS** or **Auto RTS** is enabled and any 802.11b station is associated to the IAP, additional frames are sent to gain access to the wireless network.

- Auto CTS requires 802.11g stations to send a slow Clear To Send frame that locks out other stations. Automatic protection reduces 802.11g throughput when 802.11b stations are present—Auto CTS adds less overhead than Auto RTS. The default value is Auto CTS.
- With Auto RTS, 802.11g stations reserve the wireless media using a Request To Send/Clear To Send cycle. This mode is useful when you have dispersed nodes. It was originally used in 802.11b only networks to avoid collisions from "hidden nodes"—nodes that are so widely dispersed that they can hear the Array, but not each other.

When there are no 11b stations associated and an auto-protection mode is enabled, the Array will not send the extra frames, thus avoiding unnecessary overhead.

14. **802.11g Slot**: Choose **Auto** to instruct the Array to manage the 802.11g slot times automatically, or choose **Short Only**. Xirrus recommends using **Auto** for this setting, especially if 802.11b devices are present.
15. **802.11b Preamble**: The preamble contains information that the Array and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble. A short preamble improves the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video. Select **Auto** to instruct the Array to manage the preamble (long and short) automatically, or choose **Long Only**.
16. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11b/g IAP. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value, between 256 and 2346.

17. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11an
Global Settings .11n
Advanced RF Settings
LED Settings
IAP Settings
IAP Statistics Summary

Global Settings .11n

This window allows you to establish global 802.11n IAP settings. These settings include enabling or disabling 802.11n mode for the entire Array, specifying the number of transmit and receive chains (data stream) used for spatial multiplexing, setting a short or standard guard interval, auto-configuring channel bonding, and specifying whether auto-configured channel bonding will be static or dynamic.

Before changing your settings for 802.11n, please read the discussion in "IEEE 802.11n Deployment Considerations" on page 35.

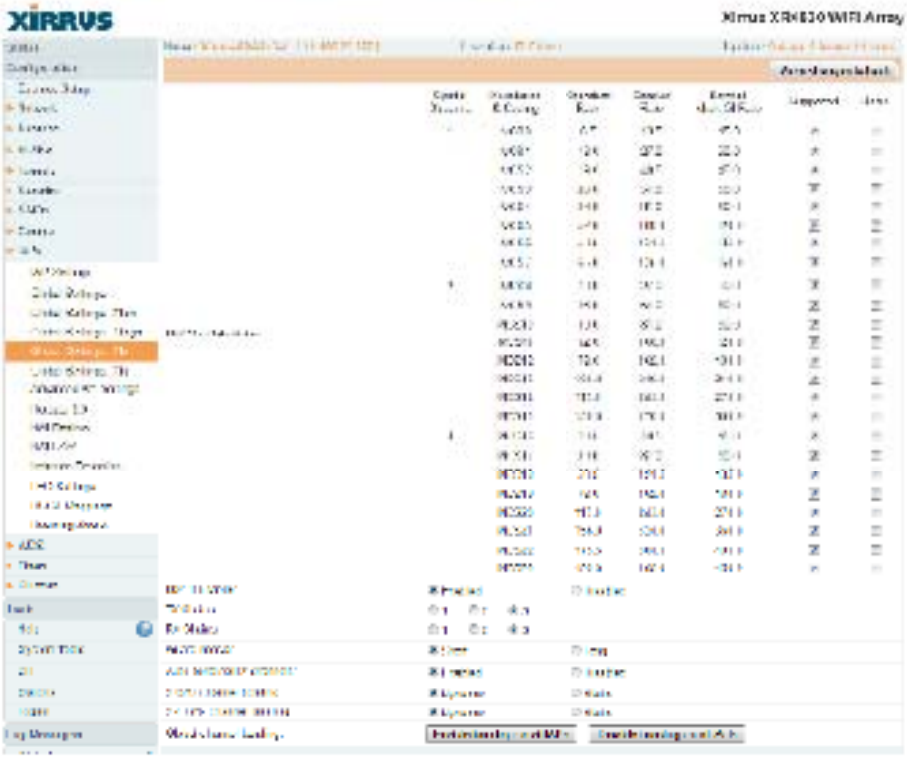

Figure 151. Global Settings .11n

Procedure for Configuring Global 802.11n IAP Settings

802.11n operation is allowed only if the Array's license includes this feature. Please see "About Licensing and Upgrades" on page 361.

1. **802.11n Data Rates**: The Array allows you to define which data rates are supported for all 802.11n radios. Select (or deselect) 11n data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
   - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
   - **Supported Rate**—data rates that can be used to transmit to clients.
2. **802.11n Mode**: Select **Enabled** to allow the Array to operate in 802.11n mode. Use of this mode is controlled by the Array's license key. The key must include 802.11n capability, or you will not be able to enable this mode. See "License" on page 107 to view the features supported by your license key. Contact Xirrus Customer support for questions about your license.

   If you select **Disabled**, then 802.11n operation is disabled on the Array. For XN Arrays, IAPs abgn1 though abgn4 will operate in 802.11abg mode; the 802.11a/n IAPs will operate in 802.11a mode.
3. **TX Chains**: Select the number of separate data streams transmitted by the antennas of each IAP. The default is 3. See "Multiple Data Streams—Spatial Multiplexing" on page 38.
4. **RX Chains**: Select the number of separate data streams received by the antennas of each IAP. This number should be greater than or equal to **TX Chains**. The default is 3. See "Multiple Data Streams—Spatial Multiplexing" on page 38.
5. **Guard interval**: Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short. See "Short Guard Interval" on page 40.

6. **Auto bond 5 GHz channels**: Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**. See "Channel Bonding" on page 39.

7. **5 GHz channel bonding**: Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**. See "Channel Bonding" on page 39.

8. **2.4 GHz channel bonding**: Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The default is **Dynamic**. See "Channel Bonding" on page 39.

9. **Global channel bonding**: These buttons allow you to turn channel bonding on or off for all IAPs in one step. The effect of using one of these buttons will be shown if you go to the **IAP Settings** window and look at the **Bond** column. Clicking **Enable bonding on all IAPs** causes all IAPs to be bonded to their auto-bonding channel immediately, if appropriate. For example, an IAP will not be bonded if it is set to monitor mode, and 2.4 GHz radios will not be bonded. Click **Disable bonding on all IAPs** to turn off bonding on all IAPs immediately. See "Channel Bonding" on page 39. Settings in Step 7 and Step 8 are independent of global channel bonding.

Understanding 802.11u

As the number of access points available in public venues increases, mobile devices users have a harder time distinguishing usable SSIDs from the tens, if not hundreds of access points visible. Using the 802.11u protocol, access points may broadcast information about the services and access that they offer and to respond to queries for additional information related to the facilities that the downstream service network provides.

The type of information broadcast or available from 802.11u-compliant access points includes:

- **Access Network Type**. Indicates the type of network available. For example: public or private, free or charged, etc.
- **Internet Connectivity**. Indicates whether the network provides Internet connectivity.
- **Authentication**. Indicates whether additional authentication steps will be required to use the network as well as the network authentication types that are in use.
- **Venue Information**. The type and name of the location where the access point is found.
- **Identification**. A globally unique identification for the access point.
- **IPv4/IPv6 Addressing.** Indicate the type of IP addressing (IPv4 and/or IPv6) and NATing that is performed by the network.
- **Roaming Consortium**. The service network may be connected to one or more roaming providers, called consortia, that allow access points from multiple service providers to be used transparently through a single paid service. The access point may advertise multiple consortia to mobile devices.
- **Domain Names.** A list of domain names to which the mobile user may end up belonging based on authentication credentials used.

- **Cellular Networks**. The service network may have arrangements with one or more cellular service providers who can transparently provide wireless and Internet connectivity.

Figure 152. 802.11u Global Settings

Procedure for Configuring 802.11u Settings

Use this window to establish the 802.11u configuration.

1. **802.11u Internetworking.** Click **On** to enable 802.11u protocol operation.
2. **Access Network Type**: This indicates the type of network supported by the access point. The choices are:

a. **Chargeable public network**

b. **Emergency services only network**

c. **Free public network**

d. **Personal device network**

e. **Private network with guest access**

f. **Test or experimental network**

g. **Wildcard**

3. **Internet Connectivity.** Click **Provided** if Internet connectivity is available through the access point from the back end provider to which the mobile user ends up belonging. Click **Unspecified** otherwise—for example, depending on the SLAs (service level agreements) of the mobile user, Internet access may or may not be provided.

4. **Additional Step Required for Access.** Click **Disabled** if no additional authentication steps will be required to complete the connection and **Enabled** otherwise. The available authentication techniques are described in the **Network Authentication Types** field (Step 13).

5. **Venue Group**. Select the general type of venue that the access point is located in. Various choices are available, including **Business, Residential,** and **Outdoor.** For each **Venue Group,** a further set of sub-choices are available in the **Venue Type** field below. The particular name of the venue is specified in the **Venue Names** field (Step 14).

6. **Venue Type**. For each of the **Venue Group** choices, a further set of sub-choices are available. For example, if you set **Venue Group** to **Assembly,** the choices include **Amphitheater, Area, Library,** and **Theatre.**

7. **HESSID**. Enter the globally unique homogeneous ESS ID. This SSID is marked as being HotSpot 2.0 capable. This SSID attribute is global—if 802.11u is enabled and HotSpot 2.0 is enabled, then all SSIDs will have HotSpot 2.0 capability.

8. **IPv4 Availability.** Select the type of IPv4 addressing that will be assigned by the network upon connection. NATed addresses are IP addresses that have been changed by mapping the IP address and port number to IP addresses and new port numbers routable by other networks. **Double NATed** addresses go through two levels of NATing. **Port restricted IPv4 addresses** refer to specific UDP and TCP port numbers associated with standard Internet services; for example, port 80 for web pages. The choices for this field are:
   a. **Double NATed private IPv4 address available**
   b. **IPv4 address not available**
   c. **IPv4 address availability not known**
   d. **Port-restricted IPv4 address available**
   e. **Port-restricted IPv4 address and double NATed IPv4 address available**
   f. **Port-restricted IPv4 address and single NATed IPv4 address available**
   g. **Public IPv4 address available**
   h. **Single NATed private IPv4 address available**
9. **IPv6 Availability.** Select the type of IPv6 addressing that is available from the network upon connection.
   a. **IPv6 address not available**
   b. **IPv6 address availability not known**
   c. **IPv6 address available**
10. **Roaming Consortium.** Each of the roaming consortia has an organizational identifier (OI) obtained from IEEE that unique identifies the organization. This is similar to the OUI part of a MAC address. Use this control to build up a list of OIs for the consortia available. Enter the OI as a hexadecimal string of between 6 and 30 characters in the **Add** field

and click **Add**. The OI will appear in the list. An OI may be deleted by selecting it in the list and clicking **Delete**. All OIs may be deleted by clicking **Reset**.

11. **Domain Names**. Use this control to build up a list of domain names. Enter the name in the **Add** field and click **Add**, and it will appear in the list. A name may be deleted by selecting it in the list and clicking **Delete**. All names may be deleted by clicking **Reset**.

12. **Cell Network**. Each of the cell networks is identified by a mobile country code (MCC) and mobile network code (MNC). Use this control to build up a list of cell networks. Enter the MCC as a three digit number and the MNC as a two or three digit number and click **Add**. The cell network will appear in the list. A cell network may be deleted by selecting it in the list and clicking **Delete**. All networks may be deleted by clicking **Reset**.

13. **Network Authentication Types**. Each network authentication that is in use on the network should be specified in this list. The choices are:

    a. **Acceptance of terms and conditions**. This choice displays a web page asking for the user's acceptance of terms and conditions of use. The URL should be specified in the URL field before clicking **Add**.

    b. **DNS redirection**.

    c. **HTTP/HTTPS redirection**. This choice causes the user's first web page reference to be redirected to a different URL for login or other information. The URL should be specified in the URL field before clicking **Add**.

    d. **On-line enrollment supported**. This choice indicates that the user may sign up for network access as part of the authentication process.

    When **Add** is clicked the authentication type and optional URL will appear in the list. An authentication type may be deleted by selecting it in the list and clicking **Delete**. All authentication types may be deleted by clicking **Reset**.

14. **Venue Names.** The list of names associated with the venue are specified here. A venue name may be added to the list in English or Chinese. Enter the name in the appropriate field and click **Add**. The name will appear in the list. A name may be deleted by selecting it in the list and clicking **Delete**. All names may be deleted by clicking **Reset**.

Advanced RF Settings

This window allows you to establish RF settings, including automatically configuring channel allocation and cell size, and configuring radio assurance and standby modes. Changes you make on this page are applied to all IAPs, without exception.

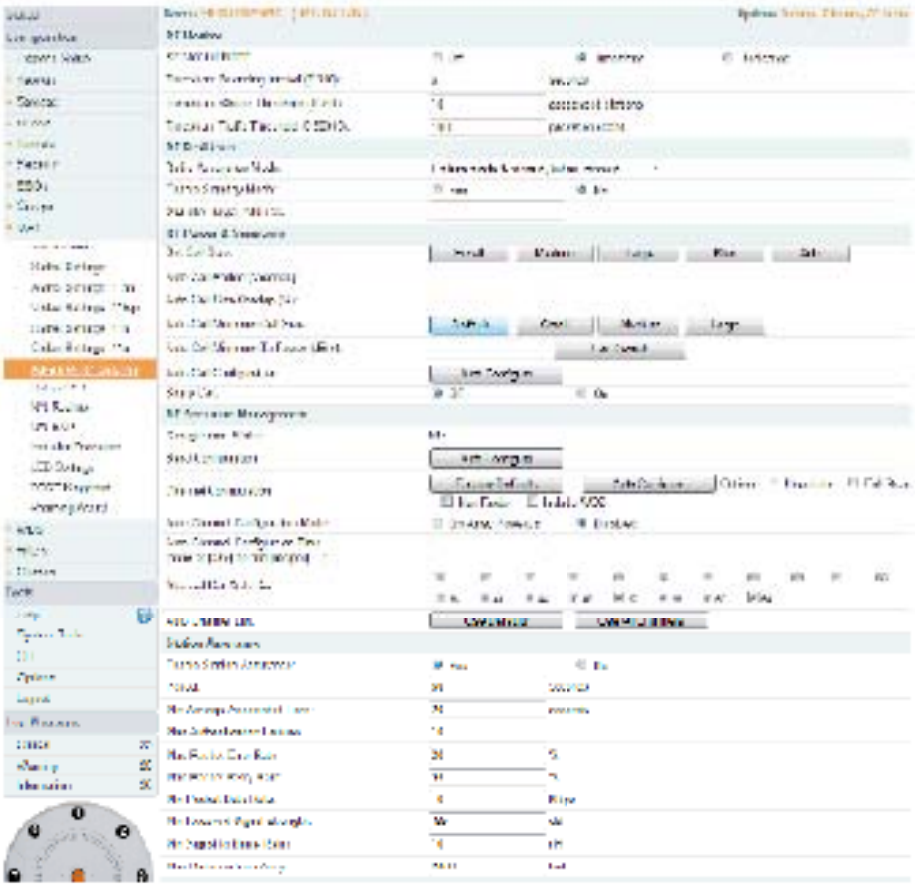

Figure 153. Advanced RF Settings

About Standby Mode

Standby Mode supports the Array-to-Array fail-over capability. When you enable Standby Mode, the Array functions as a backup unit, and it enables its radios if it detects that its designated target Array has failed. The use of redundant Arrays to provide this fail-over capability allows Arrays to be used in mission-critical applications. In Standby Mode, an Array monitors beacons from the target Array. When the target has not been heard from for 40 seconds, the standby Array enables its radios until it detects that the target Array has come back online. Standby Mode is off by default. Note that you must ensure that the configuration of the standby Array is correct. This window allows you to enable or disable Standby Mode and specify the primary Array that is the target of the backup unit. See also, "Failover Planning" on page 42.

Procedure for Configuring Advanced RF Settings

Some of the features below, such as Auto Configure for Cell Size and Channel Configuration, are only available if the Array's license includes the ***Xirrus Advanced RF Performance Manager (RPM)****. If a setting is unavailable (grayed out), then your license does not support the feature. Please see* ***"About Licensing and Upgrades" on page 361****.*

Other features below, such as RF Intrusion Detection, are only available if the Array's license includes the ***Xirrus Advanced RF Security Manager (RSM)****.*

RF Monitor

1. **RF Monitor Mode**: RF monitoring permits the operation of features like intrusion detection. The monitor may operate in **Dedicated** mode, or in **Timeshare** mode which allows the radio to divide its time between monitoring and acting as a standard radio that allows stations to associate to it. **Timeshare** mode is especially useful for small Arrays with two IAPs, such as the XR-500 and XR-1000 Series, allowing one IAP to be shared between monitoring the airwaves for problems and providing services to stations. Settings allow you to give priority to monitoring or wireless services, depending on your needs.

If **Timeshare** mode is selected, you may adjust the following settings:

- **Timeshare Scanning Interval (6-600)**: number of seconds between monitor (off-channel) scans.
- **Timeshare Station Threshold (0-240)**: when the number of stations associated to the monitor radio exceeds this threshold, scanning is halted.
- **Timeshare Traffic Threshold (0-50000)**: when the number of packets per second handled by the monitor radio exceeds this threshold, scanning is halted.

RF Resilience

2. **Radio Assurance Mode**: When this mode is enabled, the monitor radio performs loopback tests on the Array. This mode requires RF Monitor Mode to be enabled (Step 1) to enable self-monitoring functions. It also requires a radio to be set to monitoring mode (see "Enabling Monitoring on the Array" on page 460).

   Operation of Radio Assurance mode is described in detail in "Array Monitor and Radio Assurance Capabilities" on page 460.

   The Radio Assurance mode scans and sends out probe requests on each channel, in turn. It listens for all probe responses and beacons. These tests are performed continuously (24/7). If no beacons or probe responses are observed from a radio for a predetermined period, Radio Assurance mode will take action according to the preference that you have specified:

   - **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
   - **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of one or all of the radios if needed.
   - **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets, and schedule reboots if needed.
   - **Disabled**—Disable IAP radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.

3. **Enable Standby Mode**: Choose **Yes** to enable this Array to function as a backup unit for the target Array, or choose **No** to disable this feature. See "About Standby Mode" on page 314.

4. **Standby Target Address**: If you enabled the Standby Mode, enter the MAC address of the target Array (i.e., the address of the primary Array that is being monitored and backed up by this Array). To find this MAC address, open the Array Info window on the target Array, and use the Gigabit1 MAC Address.

RF Power & Sensitivity

For an overview of RF power and cell size settings, please see "Capacity and Cell Sizes" on page 30 and "Fine Tuning Cell Sizes" on page 31.

To use the Auto Cell Size feature, the following additional settings are required:

*RF Monitor Mode must be turned **On**. See **"RF Monitor" on page 314**.*

*One of the radios must be in **monitor** mode, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See **"Procedure for Manually Configuring IAPs" on page 275**.*

5. **Set Cell Size**: Cell Size may be set globally for all enabled IAPs to **Auto, Large, Medium, Small,** or **Max** using the buttons.

6. **Auto Cell Period (seconds)**: You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.

7. **Auto Cell Size Overlap (%)**: Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

8. **Auto Cell Min Cell Size**: Use this setting if you wish to set the minimum cell size that Auto Cell may assign. The values are **Default**, **Large**, **Medium**, or **Small**.

9. **Auto Cell Min Tx Power (dBm)**: Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.

10. **Auto Cell Configuration**: Click this button to instruct the Array to determine and set the best cell size for each enabled IAP whose **Cell Size** is **auto** on the IAP Settings window, based on changes in the environment. This is the recommended method for setting cell size. You may look at the Tx and Rx values on the IAP Settings window to view the cell size settings that were applied.

11. **Sharp Cell**: This feature reduces interference between neighboring Arrays or other Access Points by limiting to a defined boundary (cell size) the trailing edge bleed of RF energy. Choose **On** to enable the Sharp Cell functionality, or choose **Off** to disable this feature. See also, "Fine Tuning Cell Sizes" on page 31.

    The Sharp Cell feature only works when the cell size is Small, Medium, or Large (or Auto)—but not Max. If an IAP cell size is set to Max, the Sharp Cell feature will be disabled for that radio.

RF Spectrum Management

12. **Configuration Status**: Shows the status of auto channel configuration. If an operation is in progress, the approximate time remaining until completion is displayed; otherwise **Idle** is displayed.

13. **Band Configuration**: Automatic band configuration is the recommended method for assigning bands to the abgn IAPs. It runs only on command, assigning IAPs to the 2.4GHz or 5GHz band when you click the **Auto Configure** button. The Array uses its radios to listen for other APs on the same channel, and it assigns bands based on where it finds the least interference.

    Auto band assigns as many IAPs to the 5 GHz band as possible when there are other Arrays within earshot. It does this by determining how many Arrays are in range and then picking the number of radios to place in the 2.4 GHz band. Note that for another Array to be considered to be in range, the other Array must be visible via both the wireless and wired networks—the Array must be listed in the Network Map table, its entry must have **In Range** set to **Yes**, and it must have at least one active IAP with an SSID that has broadcast enabled.

    Auto band runs separately from auto channel configuration. If the band is changed for an IAP, associated stations will be disconnected and will then reconnect.

14. **Channel Configuration**: Automatic channel configuration is the recommended method for channel allocation. When the Array performs auto channel configuration, you may optionally instruct it to first negotiate with any other nearby Arrays that have been detected, to determine whether to stagger the start time for the procedure slightly. Thus, nearby Arrays will not run auto channel at the same time. This prevents Arrays from interfering with each other's channel assignments.

    The **Configuration Status** field displays whether an Auto Configure cycle is currently running on this Array or not.

    Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each enabled IAP and select the channel

automatically, based on changes in the environment. This is the recommended method for channel allocation (see "RF Spectrum Management" on page 318). The following options may be selected for auto configuration:

- **Negotiate**: negotiate air-time with other Arrays before performing a full scan. Negotiating is slower, but if multiple Arrays are configuring channels at the same time the Negotiate option ensures that multiple Arrays don't select the same channels. Turning off the Negotiate option allows the **Auto Configure** button to manually perform auto channel without waiting, and may be used when you know that no other nearby Arrays are configuring their channels.
- **Full Scan**: perform a full traffic scan on all channels on all IAPs to determine the best channel allocation.
- **Non-Radar**: give preference to channels without radar-detect. See table in "Procedure for Configuring Global 802.11an IAP Settings" on page 293.
- **Include WDS**: automatically assign 5GHz to WDS client links.

Click **Factory Defaults** if you wish to instruct the Array to return all IAPs to their factory preset channels. As of release 6.3, Arrays no longer all use the same factory preset values for channel assignments. Instead, if the Array has been deployed for a while and already has data from the spectrum analyzer and Xirrus Roaming Protocol about channel usage on neighboring arrays, it performs a quick auto channel using that information (without doing a full RF scan) to make an intelligent choice of channel assignments. If the Array has been rebooted and has no saved configuration or is just being deployed for the first time, it has no prior data about its RF environment. In this case, it will pick a set of compatible channel assignments at random.

*On the XR-1000 Series Arrays, the **Factory Defaults** button will not restore iap1 to monitor mode. You will need to restore this setting manually. Also, you may need to set **RF Monitor Mode** to **Timeshare Mode** again - see "RF Monitor" on page 314.*

15. **Auto Channel Configuration Mode**: This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP when the Array is powered up. Choose **On Array PowerUp** to enable this feature, or choose **Disabled** to disable this feature.

16. **Auto Channel Configure on Time**: This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here. Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated. Time is specified in hours and minutes, using the format: **[day]hh:mm [am|pm]**. If you omit the optional **day** specification, channel configuration will run daily at the specified time. If you do not specify am or pm, time is interpreted in 24-hour military time. For example, Sat 11:00 pm and Saturday 23:00 are both acceptable and specify the same time.

17. **Channel List Selection**: This list selects which channels are available to the auto channel algorithm. Channels that are not checked are left out of the auto channel selection process. Note that channels that have been locked by the user are also not available to the auto channel algorithm.

18. **Auto Channel List**: **Use All Channels** selects all available channels (this does not include locked channels). **Use Defaults** sets the auto channel list back to the defaults. This omits newer channels (100-140)—many wireless NICs don't support these channels.

Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the wireless network. You can quickly detect stations that are having problems and take steps to correct them. Use these settings to establish threshold values for errors and other problems. Station assurance is enabled by default, with a set of useful default thresholds that you may adjust as desired.

When a connection is experiencing problems and reaches one of these thresholds in the specified period of time, the Array responds with several actions: an event is triggered, a trap is generated, and a Syslog message is logged. For example, if a client falls below the threshold for **Min Average Associated Time**, this "bouncing" behavior might indicate roaming problems with the network's RF

design, causing the client to bounce between multiple arrays and not stay connected longer than the time to re-associate and then jump again. This can be corrected with RF adjustments. Station assurance alerts you to the fact that this station is encountering problems.

Figure 154. Station Assurance (Advanced RF Settings)

19. **Enable Station Assurance**: This is enabled by default. Click No if you wish to disable it, and click Yes to re-enable it. When station assurance is enabled, the Array will monitor connection quality indicators listed below and will display associated information on the Station Assurance Status page. When a threshold is reached, an event is triggered, a trap is generated, and a Syslog message is logged.
20. **Period**: In seconds, the period of time for a threshold to be reached. For example, the Array will check whether Max Authentication Failures has been reached in this number of seconds.
21. **Min Average Associated Time**: (seconds) Station assurance detects whether the average length of station associations falls below this threshold during a period.
22. **Max Authentication Failures**: Station assurance detects whether the number of failed login attempts reaches this threshold during a period.
23. **Max Packet Error Rate**: (%) Station assurance detects whether the packet error rate percentage reaches this threshold during a period.

24. **Max Packet Retry Rate**: (%) Station assurance detects whether the packet retry rate percentage reaches this threshold during a period.
25. **Min Packet Data Rate**: (Mbps) Station assurance detects whether the packet data rate falls below this threshold during a period.
26. **Min Received Signal Strength**: (dB) Station assurance detects whether the strength of the signal received from the station falls below this threshold during a period.
27. **Min Signal to Noise Ratio**: (dB) Station assurance detects whether the ratio of signal to noise received from the station falls below this threshold during a period.
28. **Max Distance from Array**: **Min Received Signal Strength**: (feet) Station assurance detects whether the distance of the station from the Array reaches this threshold during a period.

See Also

Coverage and Capacity Planning
Global Settings .11an
Global Settings .11bgn
Global Settings .11n
IAPs
IAP Settings
Radio Assurance

Hotspot 2.0

Understanding Hotspot 2.0

Hotspot 2.0 is a part of the Wi-Fi Alliance's Passpoint certification program. It specifies additional information above and beyond that found in 802.11u, which allows mobile clients to automatically discover, select, and connect to networks based on preferences and network optimization. Mobile clients that support Hotspot 2.0 are informed of an access point's support via its beacon message.

Hotspot 2.0 messages forward several types of information to clients, including:

- **Uplink and Downlink Speeds**
- **Link Status**
- **Friendly Name**
- **Connection Capabilities** The access point will restrict the protocols that can be used by a specification of protocol and port numbers.

Procedure for Hotspot 2.0 Settings

Use this window to establish the Hotspot 2.0 configuration.

1. **Hotspot 2.0.** Click **Enabled to** enable Hotspot 2.0 operation.
2. **Downstream Group-addressed Forwarding.** Click **Enabled** to allow the access point to forward group-addressed traffic (broadcast and multicast) to all connected devices. Click **Disabled** to cause the access point to convert group-addressed traffic to unicast messages.
3. **WAN Downlink Speed.** Enter the WAN downlink speed in kbps into the field.
4. **WAN Uplink Speed.** Enter the WAN uplink speed in kbps into the field.

Figure 155. Hotspot 2.0 Settings

5. **English/Chinese Operator Friendly Name.** Enter an English or Chinese name into one of the fields. An incorrectly entered name can be deleted by clicking the corresponding **Delete.**

6. **Connection Capabilities.** A Hotspot 2.0 access point limits the particular protocols that clients may use. The set of default protocols is shown initially. This table specifies the protocols in terms of:

   a. A common **Name**, such as FTP or HTTP.

   b. A **Protocol** number. For example 1 for ICMP, 6 for TCP, 17 for UDP, and 50 for Encapsulated Security Protocol in IPsec VPN connections.

   c. **Port** number for UDP/TCP connection.

d. **Status**: one of **open, closed** or **unknown.**

Any of the entries may be deleted by clicking the corresponding **Delete** button. New entries may be created by entering the name of the protocol in the box beside the **Create** button, and then clicking **Create.** The new protocol will be added to the list with zeros in the protocol fields and **unknown** for the status. Enter the appropriate **Protocol** and **Port** values before setting the **Status** field to **open.**

NAI Realms

Understanding NAI Realm Authentication

A network access identifier (NAI) is a specification of a particular user. A NAI takes the general form of e-mail addresses. Examples of NAIs are:

```
joe@example.com
fred@foo-9.example.com
jack@3rd.depts.example.com
fred.smith@example.com
```

Figure 156. NAI Realms

The **NAI Realm** is the part of the NAI following the @ sign. In the examples above, the realms are: **example.com, 3rd.depts.example.com,** and **foo-9.example.com.** Use the **NAI Realms** page, in conjunction with the **NAI EAP** page, to specify the authentication techniques to be used to access that realm with appropriate parameters.

Procedure for NAI Realms Settings

Use this window to establish the names of the supported realms.

1. **Enter the realm name.** Enter the name of a realm in the box to the left of the **Create** button and click **Create**. The realm will be added to the **NAI Realms** list. Any of the realms may be deleted by clicking the corresponding **Delete** button.
2. **Enter Authentication Information.** The NAI EAP page is used to specify authentication for a realm. Click on the name of a realm to go to the NAI EAP page for that realm. **See "NAI EAP" on page 326.**

NAI EAP

This window allows specification of the authentication techniques for a realm.

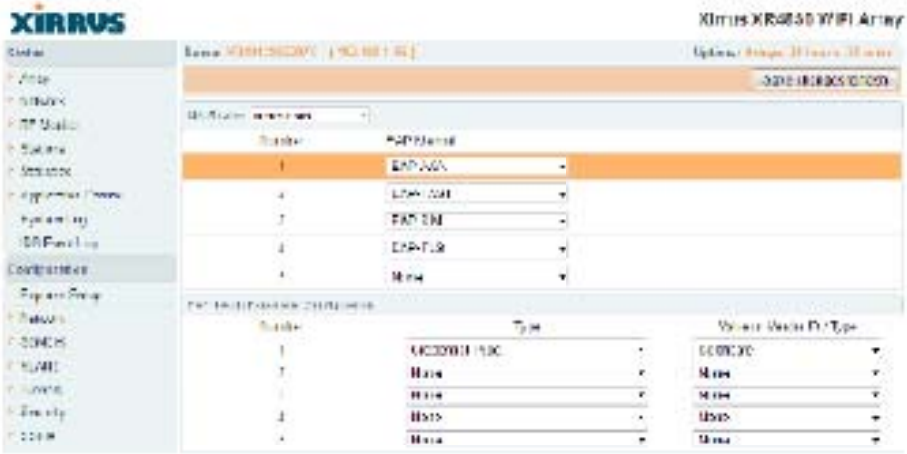

Figure 157. NAI EAP

Procedure for NAI Realms Settings

1. Select the realm to be configured in the **NAI Realm** drop down.
2. Select **EAP Methods**. Each realm may support up to five EAP authentication methods. Beside each of the five numbers (1, 2, 3, 4, 5) select the method from the drop down. The choices are:
   - **EAP-AKA**
   - **EAP-AKA' (EAP-AKA prime)**

- **EAP-FAST**
- **EAP-MSCHAP-V2**
- **EAP-SIM**
- **EAP-TLS**
- **EAP-TTLS**
- **GTC**
- **MD5-Challenge**
- **None**
- **PEAP**

3. **Specify Authentication Parameters.** Each of the authentication methods may specify up to five authentication parameters. To specify the parameters click on the number corresponding to the authentication method; i.e. **1**, **2**, **3**, **4**, or **5**. This displays the **EAP n Auth Parameter Configuration** below the list of **EAP Methods**. For up to five of the parameters, select the **Type** and **Value or Vendor ID / Type**. The choices for the **Type** are:

   - **Credential Type**
   - **Expanded EAP Method**
   - **Expanded Inner EAP Method**
   - **Inner Authentication EAP Method Type**
   - **Non-EAP Inner Authentication Type**
   - **None**
   - **Tunneled EAP Method Credential Type**

   For each type, a value or a vendor ID and type must be specified, as applicable.

Intrusion Detection

The Xirrus Array employs a number of IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) strategies to detect and prevent malicious attacks on the wireless network. Use this window to adjust intrusion detection settings.

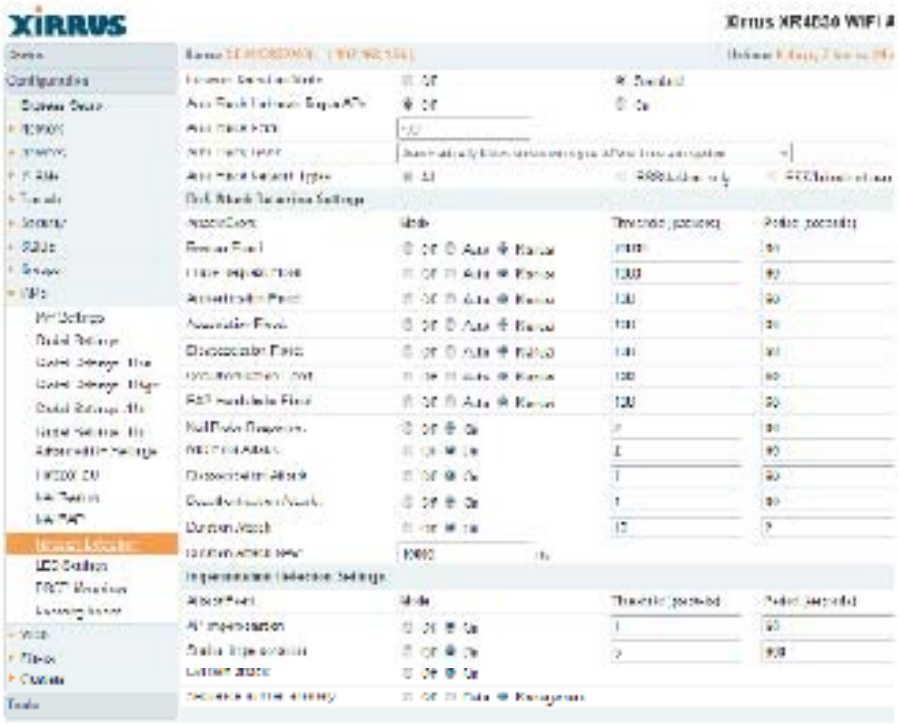

Figure 158. Intrusion Detection Settings

The Array provides a suite of intrusion detection and prevention options to improve network security. You can separately enable detection of the following types of problems:

- **Rogue Access Point Detection and Blocking**

  Unknown APs are detected, and may be automatically blocked based on a number of criteria. See "About Blocking Rogue APs" on page 331.

- **Denial of Service (DoS) or Availability Attack Detection**

  A DoS attack attempts to flood an Array with communications requests so that it cannot respond to legitimate traffic, or responds so slowly that it becomes effectively unavailable. The Array can detect a number of types of DoS attacks, as described in the table below.

- **Impersonation Detection**

  These malicious attacks use various techniques to impersonate a legitimate AP or station, often in order to eavesdrop on wireless communications. The Array detects a number of types of impersonation attacks, as described in the table below.

Type of Attack	Description
DoS Attacks	
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.
Probe Request Flood	Generating thousands of counterfeit 802.11 probe requests to overburden the Array.
Authentication Flood	Sending forged Authenticates from random MAC addresses to fill the Array's association table.
Association Flood	Sending forged Associates from random MAC addresses to fill the Array's association table.
Disassociation Flood	Flooding the Array with forged Disassociation packets.
Deauthentication Flood	Flooding the Array with forged Deauthenticates.
EAP Handshake Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.
Null Probe Response	Answering a station probe-request frame with a null SSID. Many types of popular NIC cards cannot handle this situation, and will freeze up.

Type of Attack	Description
MIC Error Attack	Generating invalid TKIP data to exceed the Array's MIC error threshold, suspending WLAN service.
Disassociation Attack (Omerta)	Sending forged disassociation frames to all stations on a channel in response to data frames.
Deauthentication Attack	Sending forged deauthentication frames to all stations on a channel in response to data frames.
Duration Attack (Duration Field Spoofing)	Injecting packets into the WLAN with huge duration values. This forces the other nodes in the WLAN to keep quiet, since they cannot send any packet until this value counts down to zero. If the attacker sends such frames continuously it silences other nodes in the WLAN for long periods, thereby disrupting the entire wireless service.
Impersonation Attacks	
AP impersonation	Reconfiguring an attacker's MAC address to pose as an authorized AP. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Station impersonation	Reconfiguring an attacker's MAC address to pose as an authorized station. Administrators should take immediate steps to prevent the attacker from entering the WLAN.
Evil twin attack	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.
Sequence number anomaly	A sender may use an Add Block Address request (ADDBA - part of the Block ACK mechanism) to specify a sequence number range for packets that the receiver can accept. An attacker spoofs an ADDBA request, asking the receiver to reset its sequence number window to a new range. This causes the receiver to drop legitimate frames, since their sequence numbers will not fall in that range.

About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see "Rogue Control List" on page 240), then the Array will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue it sends out a broadcast "deauth" signal using the rogue's BSSID and source address. This has the effect of disconnecting all of a rogue AP's clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

The Advanced RF Settings window allows you to set up **Auto Block** parameters so that unknown APs get the same treatment as explicitly blocked APs. This is basically a "shoot first and ask questions later" mode. By default, auto blocking is turned off. Auto blocking provides two parameters for qualifying blocking so that APs must meet certain criteria before being blocked. This keeps the Array from blocking every AP that it detects. You may:

- Set a minimum RSSI value for the AP—for example, if an AP has an RSSI value of -90, it is probably a harmless AP belonging to a neighbor and not in your building.
- Block based on encryption level.
- Block based on whether the AP is part of an ad hoc network or infrastructure network.

Procedure for Configuring Intrusion Detection

RF Intrusion Detection and Auto Block Mode

1. **Intrusion Detection Mode**: This option allows you to choose the **Standard** intrusion detection method, or you can choose **Off** to disable this feature. See "Array Monitor and Radio Assurance Capabilities" on page 460 for more information.
    - **Standard**—enables the monitor radio to collect Rogue AP information.
    - **Off**—intrusion detection is disabled.

2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see "About Blocking Rogue APs" on page 331). Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block Unknown Rogue APs to **On**. Then the remaining Auto Block fields will be active.
3. **Auto Block RSSI**: Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.
4. **Auto Block Level**: Select rogue APs to block based on the level of encryption that they are using. The choices are:
   - Automatically block unknown rogue APs regardless of encryption.
   - Automatically block unknown rogue APs with no encryption.
   - Automatically block unknown rogue APs with WEP or no encryption.
5. **Auto Block Network Types**: Select rogues to automatically block by applying the criteria above only to networks of the type specified below. The choices are:
   - **All**—the unknown rogues may be part of any wireless network.
   - **IBSS/AD Hoc only**—only consider auto blocking rogues if they belong to an ad hoc wireless network (a network of client devices without a controlling Access Point, also called an Independent Basic Service Set—IBSS).
   - **ESS/Infrastructure only**—only consider auto blocking rogue APs if they are in infrastructure mode rather than ad hoc mode.

DoS Attack Detection Settings

6. **Attack/Event**: The types of DoS attack that you may detect are described in the Type of Attack Table on page 329. Detection of each attack type may be separately enabled or disabled. For each attack, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in

the specified number of seconds, then the Array declares that an attack has been detected. You may modify the **Threshold** and **Period**.

For the Flood attack settings, you also have a choice of **Auto** or **Manual**.

- **Manual** mode—threshold and period settings are used to detect a flood. Packets received are simply counted for the specified time period and compared against the flood threshold. The default for all of the floods is **Manual** mode.
- **Auto** mode—the Array analyzes current traffic for packets of a given type versus traffic over the past hour to determine whether a packet flood should be detected. In this mode, threshold and period settings are ignored. This mode is useful for floods like beacon or probe floods, where the numbers of such packets detected in the air can vary greatly from installation to installation.

7. **Duration Attack NAV (ms)**: For the duration attack, you may also modify the default duration value that is used to determine whether a packet may be part of an attack. If the number of packets having at least this duration value exceeds the **Threshold** number in the specified **Period**, an attack is detected.

Impersonation Detection Settings

8. **Attack/Event**: The types of impersonation attack that you may detect are described in Impersonation Attacks on page 330. Detection of each attack type may be turned **On** or **Off** separately. For **AP** or **Station Impersonation** attacks, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the Array declares that an attack has been detected. You may modify the **Threshold** and **Period**.

9. **Sequence number anomaly**: You may specify whether to detect this type of attack in **Data** traffic or in **Management** traffic, or turn **Off** this type of detection.

LED Settings

This window assigns behavior preferences for the Array's IAP LEDs.

Figure 159. LED Settings

Procedure for Configuring the IAP LEDs

1. **LED State:** This option determines which event triggers the LEDs, either when an IAP is enabled or when an IAP first associates with the network. Choose **On Radio Enabled** or **On First Association**, as desired. You may also choose Disabled to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.
2. **LED Blink Behavior:** This option allows you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink. For default behavior, see "Array LED Operating Sequences" on page 64.
3. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Global Settings (IAP)
Global Settings .11an
Global Settings .11bgn
IAPs
LED Boot Sequence

DSCP Mappings

DSCP is the 6-bit Differentiated Services Code Point (DiffServ) field in the IPv4 or IPv6 packet header, defined in RFC2474 and RFC2475. The DSCP value classifies the packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

The DSCP Mappings page shows the default mapping of each of the 64 DSCP values to one of the Array's four QoS levels, and allows you to change these mappings.

For a detailed discussion of the operation of QoS and DSCP mappings on the Array, please see "Understanding QoS Priority on the Wireless Array" on page 244.

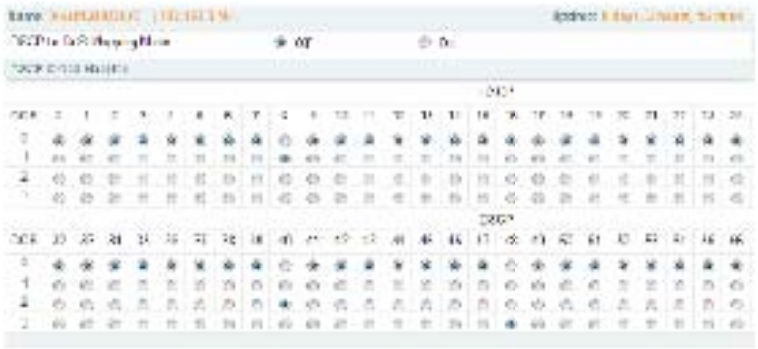

Figure 160. DSCP Mappings

Procedure for Configuring DSCP Mappings

1. **DSCP to QoS Mapping Mode**: Use the **On** and **Off** buttons to enable or disable the use of the DSCP mapping table to determine the QoS level applied to each packet.
2. **DSCP to QoS Mapping**: The radio buttons in this table show all DSCP values (0 to 63), and the QoS level to which each is mapped. To change the QoS level applied to a DSCP value, click the desired QoS level (0 to 3) underneath it.

Roaming Assist

Roaming assist is a Xirrus feature that helps clients roam to Arrays that will give them high quality connections. Some smart phones and tablets will stay connected to a radio with poor signal quality, even when there's a radio with better signal strength within range. When roaming assist is enabled, the Array "assists" the device by deauthenticating it when certain parameters are met. This encourages a client with a high roaming threshold (i.e., a device that may not roam until signal quality has seriously dropped) to move to an Array that gives it a better signal. The deauthentication is meant to cause the client to choose a different radio. You can specify the device types that will be assisted in roaming.

The roaming threshold is the difference in signal strength between radios that will trigger a deauthentication. If the client's signal is lower than the sum of the threshold and the stronger neighbor radio's RSSI, then we "assist" the client. For example:

Threshold = -5
RSSI of neighbor Array = -65
RSSI of client = -75
-75 < (-5 + -65) : Client will roam

Another example:

Threshold = -15
RSSI of neighbor array = -60
RSSI of station = -70
-70 > (-15 + -60) : Client will not roam

Procedure for Configuring Roaming Assist

1. **Enable Roaming Assist**: Use the **Yes** and **No** buttons to enable or disable this feature.
2. **Backoff Period**: After deauthenticating a station, it may re-associate to the same radio. To prevent the Array from repeatedly deauthenticating the station when it comes back, there is a backoff period. This is the number of seconds the station is allowed to stay connected before another deauthentication.

3. **Roaming Threshold**: This is the difference in signal strength between radios that will trigger a deauthentication, as described in the discussion above. In most cases, this will be a negative number.

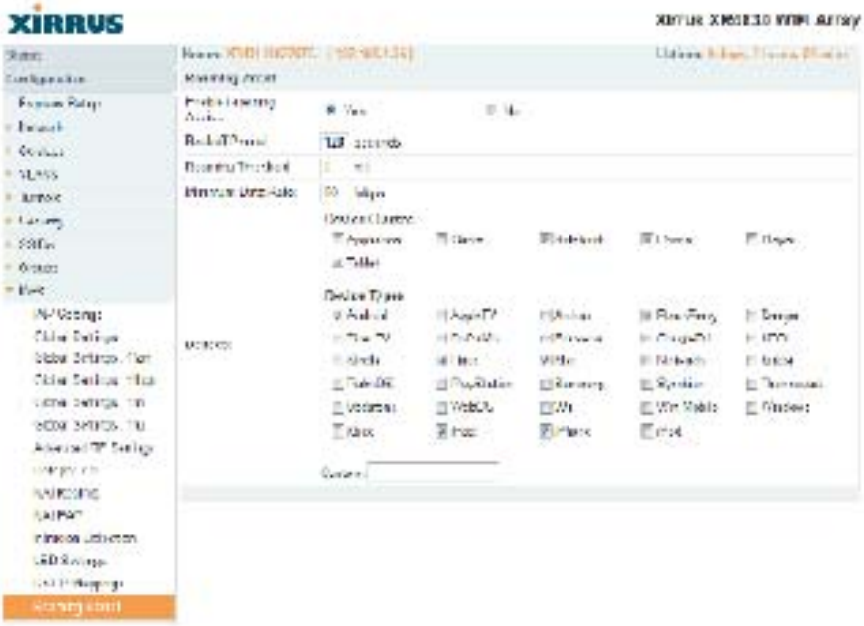

Figure 161. Roaming Assist

4. **Minimum Data Rate**: If the station's data rate (either Tx or Rx) falls below this rate, it will trigger a deauthentication.

5. **Device Classes and Device Types**: You can configure the device classes or types that will be assisted in roaming. Many small, embedded devices (such as the default device types: phones, tablets, music players) are sticky—they have high roaming thresholds that tend to keep them attached to the same radio despite the presence of radios with better signal strength. You may check off one or more entries, but use care since roaming assist may cause poor results in some cases.

WDS

This is a status-only window that provides an overview of all WDS links that have been defined. WDS (Wireless Distribution System) is a system that enables the interconnection of access points wirelessly, allowing your wireless network to be expanded using multiple access points without the need for a wired backbone to link them. The **Summary of WDS Client Links** shows the WDS links that you have defined on this Array and identifies the target Array for each by its base MAC address. The **Summary of WDS Host Links** shows the WDS links that have been established on this Array as a result of client Arrays associating to this Array (i.e., the client Arrays have this Array as their target). The summary identifies the source (client) Array for each link. Both summaries identify the IAPs that are part of the link and whether the connection for each is up or down. See "WDS Planning" on page 53 for an overview.

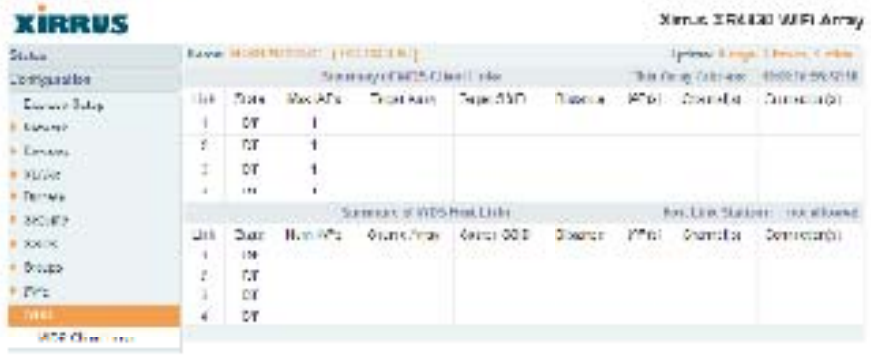

Figure 162. WDS

About Configuring WDS Links

A WDS link connects a client Array and a host Array (see Figure 163 on page 339). The host must be the Array that has a wired connection to the LAN. Client links from one or more Arrays may be connected to the host, and the host may also have client links. See "WDS Planning" on page 53 for more illustrations.

The configuration for WDS is performed on the client Array only, as described in "WDS Client Links" on page 340. No WDS configuration is performed on the host Array. First you will set up a client link, defining the target (host) Array and SSID,