NAS Identifier (IP address) that the RADIUS servers expect the Array to use—this is normally the IP address of the Array's Gigabit1 port.

c. **Accounting**: If you would like the Array to send RADIUS Start, Stop, and Interim records to a RADIUS accounting server, click the **On** button and click **Apply**. The account settings appear, and must be configured.

4. **Accounting Settings**:

a. **Accounting Interval (seconds)**: Specify how often Interim records are to be sent to the server. The default is 300 seconds.

b. **Primary Server Address**: Enter the IP address or domain name of the primary RADIUS accounting server that you intend to use.

c. **Primary Port Number**: Enter the port number of the primary RADIUS accounting server. The default is 1813.

d. **Primary Shared Secret / Verify Secret**: Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.

e. **Secondary Server Address** (optional): If desired, enter an IP address or domain name for an alternative RADIUS accounting server. If the primary server becomes unreachable, the Array will "failover" to this secondary server (defined here).

f. **Secondary Port Number**: If using a secondary accounting server, enter its port number. The default is 1813.

g. **Secondary Shared Secret / Verify Secret**: If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.

5. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Admin Management

Global Settings (IAP)
Internal Radius
Access Control List
Management Control
Security
Understanding Groups

Internal Radius

This window allows you to define the parameters for the Array's internal RADIUS server for user authentication. However, the internal RADIUS server will only authenticate wireless clients that want to associate to the Array. This can be useful if an external RADIUS server is not available. To set up the internal RADIUS server, you must choose **Internal** as the RADIUS server mode in Global Settings. Refer to "Global Settings" on page 225.
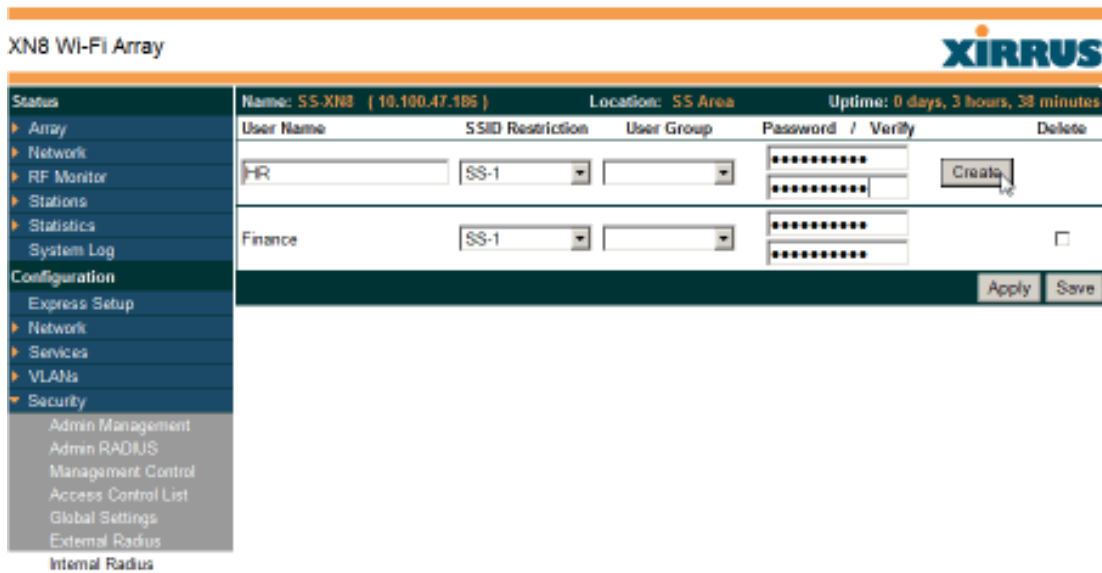
Figure 129. Internal RADIUS Server

Procedure for Creating a New User

1. **User Name:** Enter the name of the user that you want to authenticate to the internal RADIUS server.

2. **SSID Restriction**: (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the pull-down list.

3. **User Group**: (Optional) If you want to make this user a member of a previously defined user group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 247.

4. **Password**: (Optional) Enter a password for the user.

5. **Verify**: (Optional) Retype the user password to verify that you typed it correctly.

6. Click on the **Create** button to add the new user to the list.

Procedure for Managing Existing Users

1. **SSID Restriction:** (Optional) If you want to restrict a user to associating to a particular SSID, choose an SSID from its pull-down list.

2. **User Group**: (Optional) If you want to change the user's group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 247.

3. **Password**: (Optional) Enter a new password for the selected user.

4. **Verify Password**: (Optional) Retype the user password to verify that you typed it correctly.

5. If you want to delete one or more users, check their **Delete** check boxes, then click **Apply** or **Save**.

6. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Admin Management

External Radius

Global Settings (IAP)
Access Control List
Management Control
Security
Understanding Groups

Rogue Control List

This window allows you to set up a control list for rogue APs, based on a type that you define. You may classify rogue APs as blocked, so that the Array will take steps to prevent stations from associating with the blocked AP. See "About Blocking Rogue APs" on page 276. The Array can keep up to 5000 entries in this list. When finished, click on the **Save** button to save your changes.

> ✍ *The **RF Monitor > Intrusion Detection** window provides an alternate method for classifying rogues. You can list all Unknown stations and select all the rogues that you'd like to set to Known or Approved, rather than entering the SSID/BSSID as described below. See "Intrusion Detection" on page 148.*
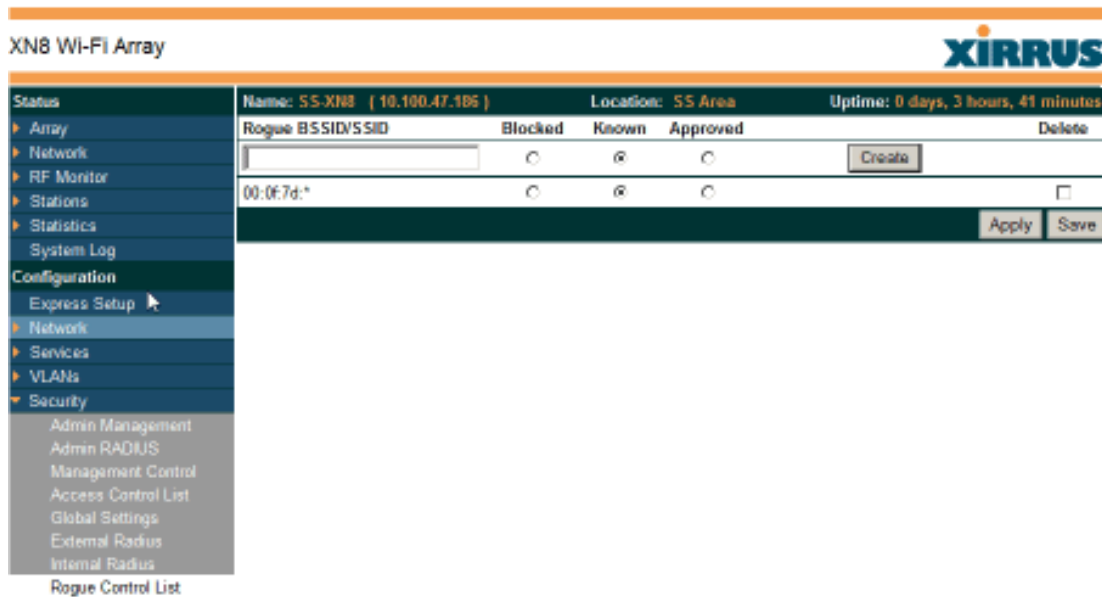
Figure 130. Rogue Control List

Procedure for Establishing Rogue AP Control

1. **Rogue BSSID/SSID:** Enter the BSSID or SSID for the new rogue AP. You may use the "*" character as a wildcard to match any string at this position. For example, **00:0f:7d:*** matches any string that starts with **00:0f:7d:**. Since Xirrus Arrays start with **00:0f:7d:**, this applies the Rogue Control Type to all Xirrus Arrays.

2. **Rogue Control Type**: Define a type for the new rogue AP, either **Blocked**, **Known** or **Approved**.

3. Click **Create** to add this rogue AP to the Rogue Control List.

4. **Rogue Control List**: If you want to edit the control type for a rogue AP, just click the radio button for the new type for the entry: **Blocked**, **Known** or **Approved**, then click **Apply** or **Save** to apply your change.

5. To delete rogue APs from the list, click their **Delete** checkboxes, then click **Apply** or **Save**.

6. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also
Network Map
Intrusion Detection
SSIDs
SSID Management

SSIDs

This is a status-only window that allows you to review SSID (Service Set IDentifier) assignments. It includes the SSID name, whether or not an SSID is visible on the network, any security and QoS parameters defined for each SSID, associated VLAN IDs, radio availability, and DHCP pools defined per SSID. You may click on an SSID's name to jump to the edit page for the SSID. There are no configuration options available on this page, but if you are experiencing problems or reviewing SSID management parameters, you may want to print this page for your records.

> *For a complete discussion of implementing Voice over Wi-Fi on the Array, see the* **Xirrus Voice over Wi-Fi Application Note** *in the* **Xirrus Library**.

For information to help you understand SSIDs and how multiple SSIDs are managed by the Wi-Fi Array, go to "Understanding SSIDs" on page 236 and the Multiple SSIDs section of "Frequently Asked Questions" on page 398. For a description of how QoS operates on the Array, see "Understanding QoS Priority on the Wi-Fi Array" on page 237.

Figure 131. SSIDs

The read-only Limits section of the SSIDs window allows you to review any limitations associated with your defined SSIDs. For example, this window shows the current state of an SSID (enabled or not), how much SSID and station traffic is

allowed, time on and time off, days on and off, and whether each SSID is currently active or inactive.

Understanding SSIDs

The SSID (Service Set Identifier) is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. SSIDs are case-sensitive and can contain up to 32 alphanumeric characters (do not include spaces when defining SSIDs).

Multiple SSIDs

A BSSID (Basic SSID) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS. A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS via a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or "wireless network name") identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. Wi-Fi Arrays support the ability to define and use multiple SSIDs simultaneously.

Using SSIDs

The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- The wireless security mode needed to join this SSID.
- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another SSID named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest Quality of Service (QoS) definition. This SSID might also forward traffic to specific VLANs on the wired network.

See Also

SSID Management

SSIDs

Understanding SSIDs

Understanding QoS Priority on the Wi-Fi Array

> *For a complete discussion of implementing Voice over Wi-Fi on the Array, see the **Xirrus Voice over Wi-Fi Application Note** in the **Xirrus Library**.*

The Wi-Fi Array's Quality of Service Priority feature (QoS) allows traffic to be prioritized according to your requirements. For example, you typically assign the highest priority to voice traffic, since this type of traffic requires delay to be under 10 ms. The Array has four separate queues for handling wireless traffic at different priorities, and thus it supports four traffic classes (QoS levels).
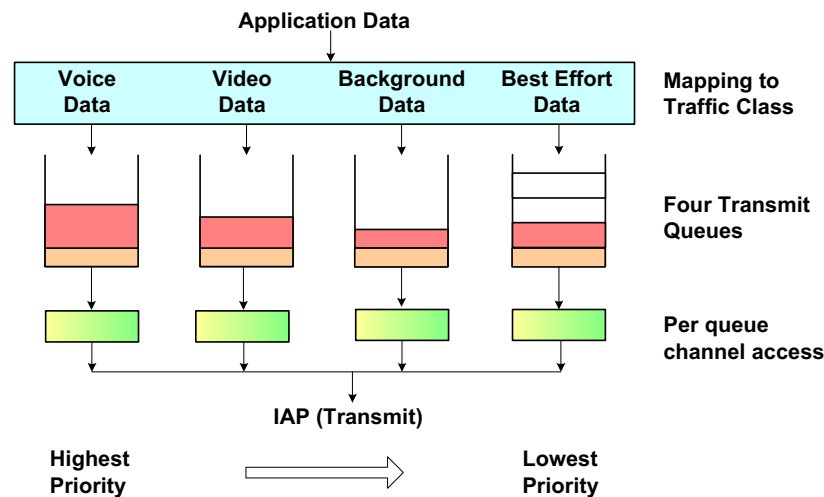
Figure 132. Four Traffic Classes

IEEE802.1p defines eight priority levels for wired networks. Each data packet may be tagged with a priority level, i.e., a **user priority** tag. Since there are eight

possible user priority levels and the Array implements four wireless QoS levels, user priorities are mapped to QoS as described below.

End-to-End QoS Handling

● Wired QoS - Ethernet Port:

Ingress: Incoming wired packets are assigned QoS priority based on their SSID and 802.1p tag (if any), as shown in the table below. This table follows the mapping recommended by IEEE802.11e.

FROM Priority Tag 802.1p (Wired)	TO Array QoS (Wireless)	Typical Use
0 (Default)	0 (Lowest priority)	Best Effort
1	1	Background—explicitly designated as low-priority and non-delay sensitive
2	1	Spare
3	0	Excellent Effort
4	2	Controlled Load
5	2	Video
6	3	Voice - requires delay <10ms
7 (Highest priority)	3 (Highest priority)	Network control

- Egress: Outgoing wired packets are IEEE 802.1p tagged at the Ethernet port for upstream traffic, thus enabling QoS at the edge of the network.

FROM Array QoS (Wireless)	TO Priority Tag 802.1p (Wired)
0 (Lowest priority)	0 (Default)
1	1
2	5
3 (Highest priority)	6

Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 0 is the default. See "SSID Management" on page 240. If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.

- The Array supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.

- How QoS is set for a packet in case of conflicting values:

    a. If an SSID has a QoS setting, and an incoming wired packet's user priority tag is mapped to a higher QoS value, then the higher QoS value is used.

    b. If a group or filter has a QoS setting, this overrides the QoS value above. See "Groups" on page 247, and "Filters" on page 289.

    c. Voice packets have the highest priority, as described below (Voice Support).

Packet Filtering QoS classification

- Filter rules can be used to redefine the QoS priority level to override defaults. See "Filter Management" on page 291. This allows the QoS priority level to be assigned based on protocol, source, or destination.

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 Wi-Fi 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**—802.11a(n), **2.4 GHz**—802.11bg(n) 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 205). 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 Wi-Fi Array" on page 237. 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 203.

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 289.

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 Wi-Fi 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 Wi-Fi network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the Wi-Fi 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 225). For an overview of the security options, see "Security Planning" on page 70 and "Understanding Security" on page 210.

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 225). 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 encryption settings are described in "Procedure for Configuring Network Security" on page 226. 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 229). Note that external RADIUS servers may be specified using IP addresses or domain names.

13. **L3**: For this SSID, Check the checkbox to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3, or clear the checkbox to allow roaming at Layer 2 only. 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 254.

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 244 for details of WPR usage and configuration.

SSID Limits

See "Group Limits" on page 251 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.

15. **Stations**: Enter the maximum number of stations allowed on this SSID. The default is 1024. 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.

16. **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.

17. **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 to force a traffic restriction.

18. **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.

19. **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.

20. To delete SSIDs, click their **Delete** checkboxes, then click **Apply** or **Save**.

21. Click **Apply** to apply the changes to the selected SSID, or click **Save** to apply your changes and make them permanent.

See Also
DHCP Server
External Radius
Global Settings (IAP)
Internal Radius
Security Planning
SSIDs
Understanding QoS Priority on the Wi-Fi Array

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

For an in-depth discussion, please see the *Xirrus Web Page Redirect Application Note* in the Xirrus Library.

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.
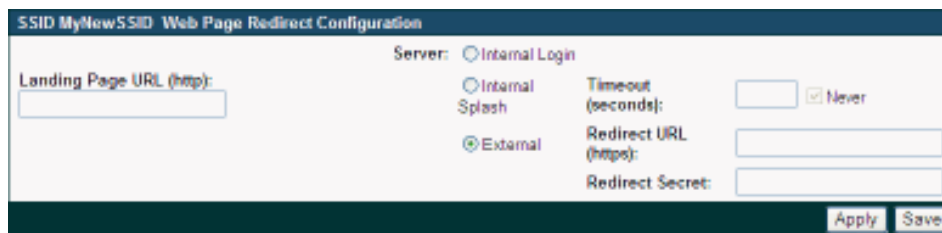
Figure 134. WPR Internal Splash Page Fields (SSID Management)

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

- 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 300 for more information.

  To set up use of a 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**.

- Internal Login page

  This option displays a login page (residing on the Array) instead of the first user-requested URL. Note that there is an upload function that

allows you to replace the default login page, if you wish. Please see "Web Page Redirect" on page 300 for more information.

To set up internal login, set **Server** to **Internal Login**.

The user name and password are obtained by the login page, and authentication occurs according to your configured authentication information (starting with Step 10 above). These parameters are configured as described in "Procedure for Configuring Network Security" on page 226.

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.

● 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 226. 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**. Enter the URL of the external web server in **Redirect URL**, and enter that server's shared secret in **Redirect Password**.

Groups

This is a status-only window that allows you to review user Group assignments. It includes the group name, Radius 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 Library.

Figure 135. Groups

Understanding Groups

User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. 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.

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 Wi-Fi 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. When finished, click the **Save** button to save your changes.
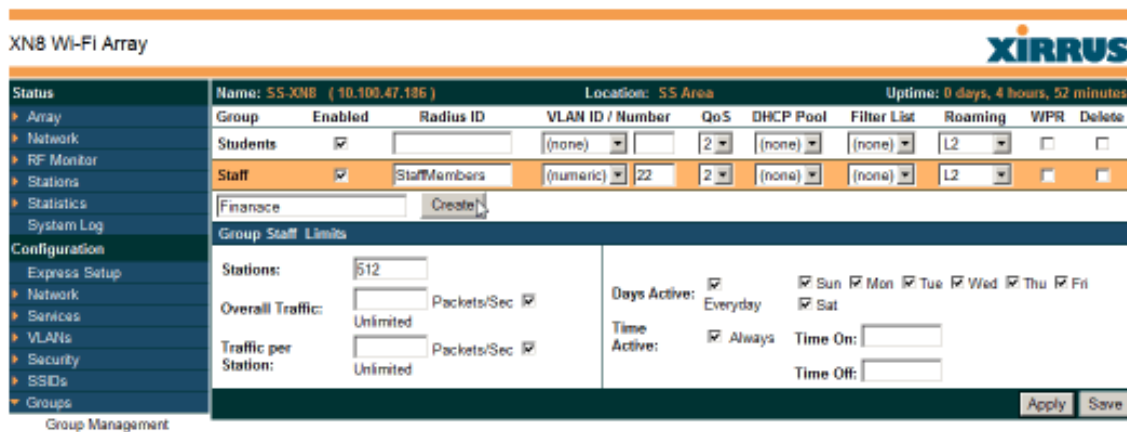

Figure 136. Group Management

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. **On**: 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. **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 205). **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.

6. **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 Wi-Fi Array" on page 237. The default value for this field is 2.

7. **Internal DHCP Pool Assigned**: (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 203.

8. **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 289.

9. **L3**: (Optional) For this group, check this box to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3. If the box is not checked, 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). See "Understanding Fast Roaming" on page 254.

10. **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 244 for details of WPR usage and configuration. Note that the Group Management window only allows you to set up an Internal Splash page. 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.

11. **Stations**: Enter the maximum number of stations allowed on this group. The default is 1024.

12. **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.

13. **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 field and make sure that the Unlimited box is unchecked to force a traffic restriction.

14. **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.

15. **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.

16. Click on the **Apply** button to apply the changes to the selected group, or click **Save** to apply your changes and make them permanent.

17. To delete an entry, check its **Delete** checkbox, then click the Save button to permanently remove the entry.

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 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 137. IAPs

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.

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 254

IAPs are configured using the following windows:

● "IAP Settings" on page 255

● "Global Settings (IAP)" on page 260

● "Global Settings .11a" on page 267

● "Global Settings .11bg" on page 269

- "Global Settings .11n" on page 273
- "Advanced RF Settings" on page 275
- "LED Settings" on page 283

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 Wi-Fi 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 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 17 to Step 19 in "Global Settings (IAP)" on page 260. To choose which of the enabled options are used by an SSID or Group, see "Procedure for Managing SSIDs" on page 240 (Step 13) or "Procedure for Managing Groups" on page 249.

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 on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent. To see a diagram of the layout and naming of IAPs, go to Figure 7 on page 16.

Figure 138. 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 123.

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 275.
- For all 802.11a settings, go to "Global Settings .11a" on page 267.

- For all 802.11bg settings, go to "Global Settings .11bg" on page 269.

- For all 802.11n settings, go to "Global Settings .11n" on page 273.

Procedure for Manually Configuring IAPs

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

2. In the **Band** column for 802.11abg(n) radios, select the wireless band for this IAP from the choices available in the pull-down menu, either **2.4GHz** or **5 GHz**. If the mode displayed is **Auto**, the mode has been set by the auto-channel feature based on the Channel selected. Note that IAP **abg(n)2** has an additional option—**monitor** mode. IAP **abg(n)2** should normally be set to monitor mode to enable Spectrum Analyzer and Radio Assurance (loopback testing) features.

   The XN16, XS16, and XS-3900 allow up to 12 IAPs to operate as 5 GHz — 802.11a(n) radios concurrently. Do not set Mode to 5 GHz for more than 12 IAPs. If you need additional 5 GHz radios, please contact Xirrus Customer Support. See "Contact Information" on page 417.

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.

   Select **Auto** to have the Array dynamically select a channel automatically, based on changes in the Wi-Fi environment. See "Allocating Channels" on page 54. After you click **Apply**, this window and the IAPs window will show the channel that was assigned, rather than Auto.

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 24 channels are available to 802.11a(n) radios.

If you have enabled **Public Safety** in the Advanced RF Settings window (Step 19), then the public safety band channels (191 and 195) in the 4.9GHz spectrum range will be listed. Operating these channels **requires a license**—using these channels without a license violates FCC rules. Warning notices are displayed when you select these channels.

*As mandated by FCC law, Array channels 100 - 140 are restricted to **indoor** use only.*

As mandated by FCC law, Arrays continually scan for signatures of military radar. If such a signature is detected, the Array will switch operation from conflicting channels to new ones.

4. The **Bonding** column only appears for XN Array models. It works together with the **Auto Channel Bonding** and **Dynamic/Static** options selected on the Global Settings .11n page. Also see the discussion of 802.11n bonding in "Channel Bonding" on page 63.

- **Off**—This channel is not bonded to another channel.
- **On**—This channel is bonded to an adjacent channel. The bonded channel is selected automatically by the Array based on current conditions. The choice of banded channel may be dynamic, changing as needed; or it may be static—fixed once the selection is made.
- **+1**—This channel is bonded to the next higher channel number. Auto Channel bonding does not apply.
- **-1**—This channel is bonded to the next lower channel number. Auto Channel bonding does not apply.

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

6. In the **Cell Size** column, select **Auto** to allow the optimal cell size to be automatically computed (see also, Step 8 on page 279). 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**.

   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 50.

7. 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 wireless mode you selected for the IAP.

8. If desired, enter a description for this IAP in the **Description** field.

9. 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.

10. Buttons at the bottom of the list allow you to **Enable All IAPs** or **Disable All IAPs**.

11. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Coverage and Capacity Planning
Global Settings (IAP)
Global Settings .11a
Global Settings .11bg
Global Settings .11n
IAPs
IAP Statistics Summary
LED Settings

Global Settings (IAP)

This window allows you to establish global IAP settings. Global IAP settings include enabling or disabling all IAPs (regardless of their operating mode), enabling or disabling the Beacon World Mode, specifying the short and long retry limits, and defining the beacon interval and DTIM period. Changes you make on this page are applied to all IAPs, without exception.

Figure 139. Global Settings (IAPs)

XIRRUS

Procedure for Configuring Global IAP Settings

1. **Country**: If no country is set, you may choose from the pull-down list. Once a country has been chosen, it may not be changed. You are responsible for choosing the correct country and conforming to the regulatory laws for wireless transmissions within your country. Please contact Xirrus Customer Support if you need to change the operating country after a country has already been set (see "Contact Information" on page 417).

   The channels that are available for assignment to an IAP will differ, depending on the country of operation. If you set **Country** to **United States**, then 24 channels are available to 802.11a(n) radios.

   Until you have chosen a country, 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 Status**: 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 Retry Limit**: This attribute indicates 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 Retry Limit**: This attribute indicates 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.

Beacon Configuration

5. **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. The value you enter here is applied to all IAPs.

6. **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.

7. **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.

Station Management

8. **Station Re-Authentication Period**: This option allows you to specify a time (in seconds) for the duration of station reauthentications.

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

10. **Max Station Association per IAP**: This option allows you to define how many station associations are allowed per IAP (up to 64 stations per IAP). Note that the SSIDs —SSID Management window also has a station limit option— **Station Limit** (page 243). 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.

11. **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.

12. **Block Intra-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).

13. **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

14. **Broadcast Rates**: This option 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, thus 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 (one that has -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. This means that 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.

15. **Load Balancing:**

The Xirrus Wi-Fi Array supports an automatic load balancing feature designed to distribute Wi-Fi stations across multiple radios rather than having stations associate to the closest radios with the strongest signal strength, as they normally would. In Wi-Fi 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 Library.

Choose **On** to enable Standard Load Balancing. If the Array decides that an IAP is overloaded, that IAP will not respond immediately to a client's Probe request. After a few seconds, if the client has still not associated the IAP will respond, assuming that this client is determined to associate to the overloaded IAP. Overloaded IAPs will always respond to Association and Authentication requests.

If you select **Aggressive** Load Balancing and an IAP is overloaded, that IAP will never respond to Probe, Association, or Authentication requests. This mode is useful because it 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.

16. **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 the following options for handling ARP requests:

• **Off**: ARP filtering is disabled. ARP requests are broadcast to stations. This is the default value.

- **Pass-thru**: The Array forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it.

- **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.

17. **Fast 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 18), 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 254 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 19). 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).

18. **Fast 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.

19. **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. **Fast 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**.

20. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also
Coverage and Capacity Planning
Global Settings .11a
Global Settings .11bg
Global Settings .11n
Advanced RF Settings
IAPs
IAP Statistics Summary
LED Settings
IAP Settings

Global Settings .11a

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 802.11a IAPs, auto-configuration of channel allocations for all 802.11a IAPs, and specifying the fragmentation and RTS thresholds for all 802.11a IAPs.
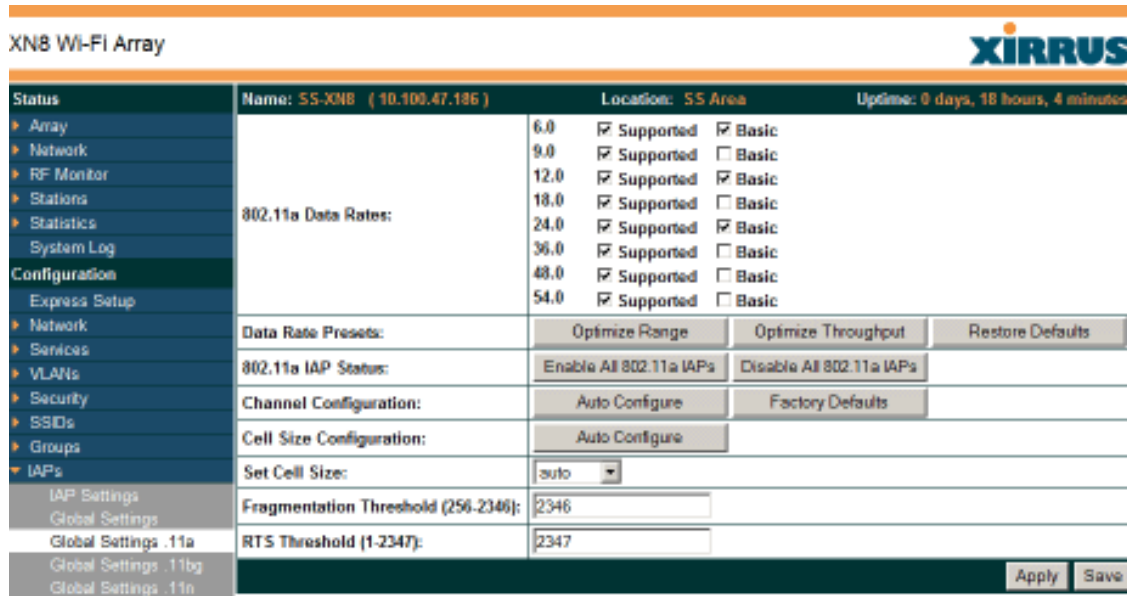

Figure 140. Global Settings .11a

Procedure for Configuring Global 802.11a IAP Settings

1. **802.11a Data Rates:** The Array allows you to define which data rates are supported for all 802.11a 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**—the Array uses this data rate to transmit to clients.

2. **Data Rate Presets**: The Wi-Fi 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 Status**: Click **Enable 802.11a IAPs** to enable all 802.11a IAPs for this Array, or click **Disable 802.11a IAPs** to disable all 802.11a IAPs.

4. **Channel Configuration**: Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11a IAP and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11a channel allocation. Use **Factory Defaults** to take you back to the factory default channel settings.

5. **Cell Size Configuration**: Click **Auto Configure** to instruct the Array to determine and set the best cell size for each enabled 802.11a IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP Settings window, each enabled 802.11a IAP will have its cell size set to **auto**.

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

7. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11a 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.

8. **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.

9. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Coverage and Capacity Planning
Global Settings (IAP)

Global Settings .11bg
Global Settings .11n
IAPs
IAP Statistics Summary
Advanced RF Settings
IAP Settings

Global Settings .11bg

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 141. Global Settings .11bg

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 rate 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 Wi-Fi 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 Status**: 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 802.11b/g channel allocations. **Factory Defaults** will take you back to the factory default channel settings.

6. **Cell Size Configuration**: Click **Auto Configure** to instruct the Array to determine and set the best cell size for each enabled 802.11b/g IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP Settings window, the cell size of each enabled 802.11b/g IAP will be set to **auto**.

7. **Set Cell Size:** The Cell Size may be set globally for all 802.11bg IAPs to **auto**, **large**, **medium**, **small**, or **max** using the drop down menu.

8. **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.

9. **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.

10. **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.

11. **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**.

12. **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.

13. **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.

14. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

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

Global Settings .11n

This window is displayed only for XN Array models. It 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 59.
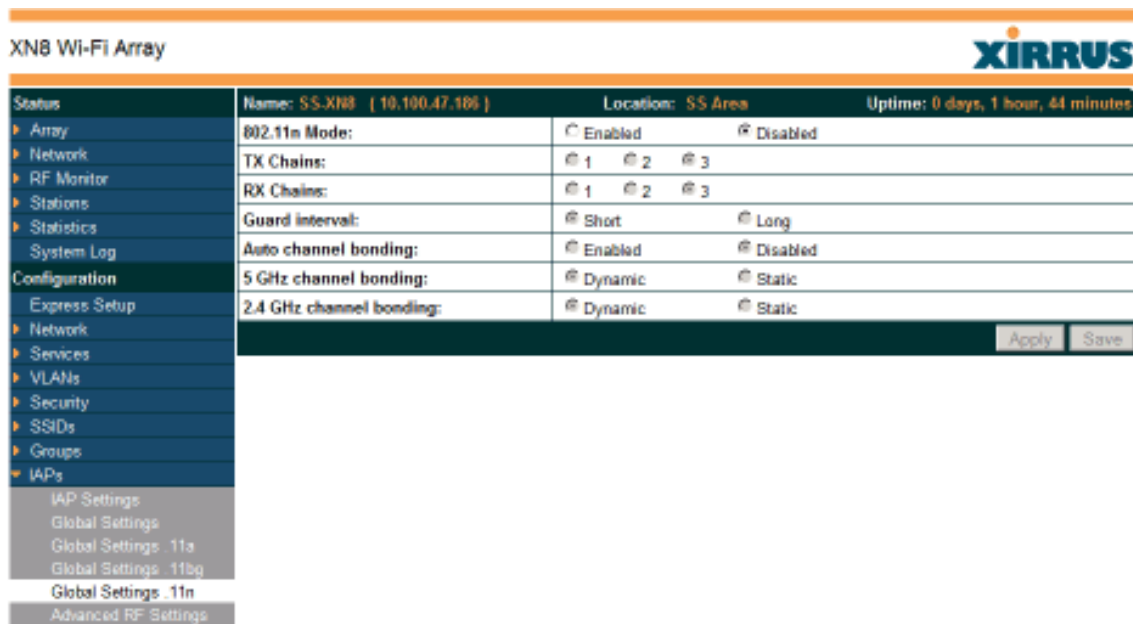
Figure 142. Global Settings .11n

Procedure for Configuring Global 802.11n IAP Settings

1. **802.11n Mode**: Select **Enabled** to operate in 802.11n mode, with four 802.11b/g/n mode ports and the remaining IAPs operating in 802.11a/n 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 135 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. IAPs abgn1 though abgn4 will behave in the same way as IAPs abg1 to abg4 on the XS Arrays; the 802.11a/n IAPs will operate in 802.11a mode.

2. **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 62.

3. **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 62.

4. **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 64.

5. **Auto-configure Channel Bonding**: Select **Enabled** to use Channel Bonding and automatically select the best channels for bonding. The default is **Disabled**. See "Channel Bonding" on page 63.

6. **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-Configure Channel Bonding is enabled. The default is **Dynamic**. See "Channel Bonding" on page 63.

7. **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 Dynamic option is only available when Auto-Configure Channel Bonding is enabled, and the default is **Dynamic**. See "Channel Bonding" on page 63.

Advanced RF Settings

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

Figure 143. 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 67.

About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see "Rogue Control List" on page 233), then the Array will take measures to prevent stations from staying associated to the rogue. When the monitor radio abg(n)2 is scanning, any time it hears a beacon from a blocked rogue abg(n)2 sends out a broadcast "deauth" signal using the rogue's BSSID and source address.   This has the effect of tossing off 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.

Procedure for Configuring Advanced RF Settings

RF Intrusion Detection

1. **Intrusion Detection:** This option allows you to establish the intrusion detection method, either Standard or Advanced, or you can choose **Off** to disable this feature. See "Array Monitor and Radio Assurance Capabilities" on page 406 for more information.

   - **Standard**—enables the abg(n)2 radio as a monitor which collects Rogue AP information.

   - **Advanced**—this option works in conjunction with the Xirrus Defense Module intrusion detection software (XDM). In this mode, the built-in monitor radio (IAP abg(n)2) functions as an RF threat sensor. Self-monitoring is not enabled.

   - **Off**—IAP abg(n)2 does not function as a monitor.

2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see "About Blocking Rogue APs" on page 276). Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block to **On**, and click **Apply**. 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.

RF Resilience

5. **Radio Assurance Mode**: When this mode is enabled, IAP abg(n)2 performs loopback tests on the Array. This mode requires Intrusion Detection to be set to Standard (Step 1) to enable abg(n)2's self-monitoring functions. It also requires abg(n)2 to be set to monitoring mode (see "Enabling Monitoring on the Array" on page 406).

   Operation of Radio Assurance mode is described in detail in "Array Monitor and Radio Assurance Capabilities" on page 406.

   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.

6. **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 275.

7. **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 52 and "Fine Tuning Cell Sizes" on page 53.

> ✎ *To use the Auto Cell feature, the following additional settings are required:*
>
> *The abg(n)2 radio 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 256.*
>
> *The **Intrusion Detection Mode** must **not** be set to **Advanced**. See "RF Intrusion Detection" on page 277.*

8. **Cell Size Configuration**: Click on the **Auto Configure** button to instruct the Array to determine and set the best cell size for each enabled IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP settings window, each enabled IAP will have its cell size set to **Auto**.

9. **Auto Cell Size Period**: 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).

10. **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.

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

12. **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 53.

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

13. **Channel Configuration**: Automatic channel configuration is the recommended method for channel allocation. When the Array performs auto channel configuration, it first negotiates 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.

Click **Auto Negotiate & Configure** to instruct the Array to determine the best channel allocation settings for each IAP and select the channel automatically, based on changes in the environment. The Array will first negotiate with other nearby Arrays to see if the start time needs to be staggered slightly.

Click **Auto Configure** to perform auto channel configuration immediately, without first negotiating with any nearby Arrays. This option is faster than Auto Negotiate and Configure. This allows you to manually perform auto channel without waiting, and may be used when you know that no other nearby Arrays are configuring their channels. If multiple Arrays are configuring channels at the same time, use the Auto Negotiate option to be ensure that multiple Arrays don't select the same channels.

Click **Factory Defaults** to instruct the Array to return all IAPs to their factory preset channels, as shown in the table below.

Factory Preset Channels (US) for both XN and XS models				
IAP	16-Radio Models	12-Radio Models	8-Radio Models	4-Radio Models
abg(n)1	1	1	1	1
abg(n)2	mon	mon	mon	mon
abg(n)3	11	11	11	11
abg(n)4	6	6	6	6
a(n)1	36	36	40	-
a(n)2	52	52	56	-
a(n)3	149	40	48	-
a(n)4	40	56	64	-
a(n)5	56	44	-	-
a(n)6	157	60	-	-
a(n)7	44	48	-	-
a(n)8	60	64	-	-
a(n)9	153	-	-	-
a(n)10	48	-	-	-
a(n)11	64	-	-	-
a(n)12	161	-	-	-

14. **Channel 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.

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 (in hours and minutes, using the format: hh:mm). Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated.

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.

*As mandated by FCC law, Array channels 100 - 140 are restricted to **indoor** use only.*

19. **Public Safety:** This option adds two additional channels (191 and 195) in the 4.9GHz spectrum range for public safety usage by qualified organizations. Operating these channels **requires a license**, and so they are not for general purpose use. Using these channels without a license violates FCC rules. Warning notices are displayed when you enable this feature and select these channels. All 802.11a(n) and 802.11a/b/g(/n) radios may be set to these channels.

20. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Coverage and Capacity Planning
Global Settings .11a

Global Settings .11bg

Global Settings .11n

IAPs

IAP Statistics Summary

IAP Settings

LED Settings

This window assigns behavior preferences for the Array's IAP LEDs.
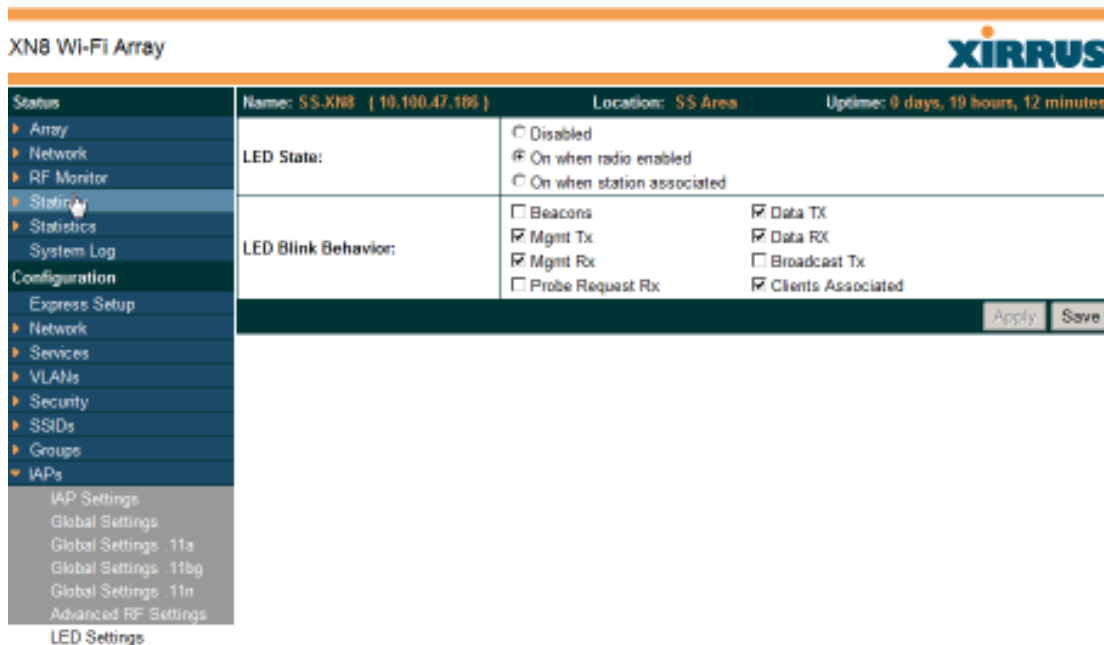
Figure 144. LED Settings

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.

   See also, "Array LED Operating Sequences" on page 108.

3. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Global Settings (IAP)
Global Settings .11a
Global Settings .11bg
IAPs
LED Boot Sequence

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 76 for an overview.

Figure 145. WDS

About Configuring WDS Links

A WDS link connects a client Array and a host Array (see Figure 146 on page 286). 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 76 for more illustrations.

The configuration for WDS is performed on the client Array only, as described in "WDS Client Links" on page 287. No WDS configuration is performed on the host Array. First you will set up a client link, defining the target (host) Array and SSID, and the maximum number of IAPs in the link. Then you will select the IAPs to be used in the link. When the client link is created, each member IAP will associate to an IAP on the host Array.
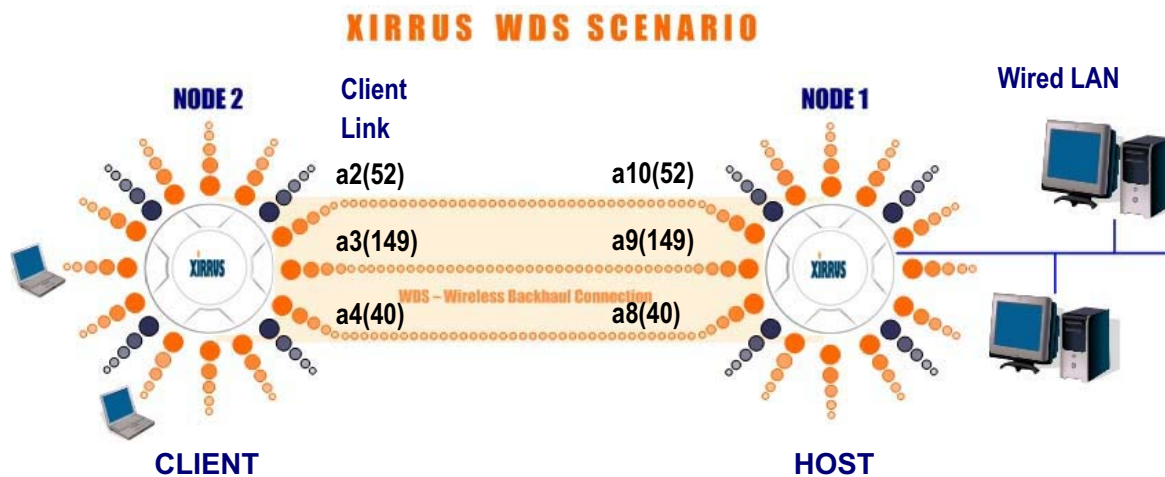
Figure 146. .Configuring a WDS Link

✎ *Once an IAP has been selected to act as a WDS client link, you will not be allowed to use auto-configured cell sizing on that IAP (since the cell must extend all the way to the other Array).*

See Also
SSID Management
WDS Client Link IAP Assignments:
WDS Client Links
WDS Statistics

WDS Client Links

This window allows you to set up a maximum of four WDS client links.

Figure 147. WDS Client Links

Procedure for Setting Up WDS Client Links

WDS Client Link Settings:

1. **Client Link:** Shows the ID (1 to 4) of each of the four possible WDS links.

2. **Enabled**: Check this box if you want to enable this WDS link, or uncheck the box to disable the link.

3. **Max IAPs Allowed (1-3)**: Enter the maximum number of IAPs for this link, between 1 and 3.

4. **Target Array Base MAC Address**: Enter the base MAC address of the target Array (the host Array at the other side of this link). To find this MAC address, open the **WDS** window on the *target* Array, and use **This Array Address** located on the right under the Summary of WDS Host Links.

5. **Target SSID**: Enter the SSID that the target Array is using.

6. **Username**: Enter a username for this WDS link. A username and password is required if the SSID is using PEAP for WDS authentication from the internal RADIUS server.

7. **Password**: Enter a password for this WDS link.

8. **Clear Settings**: Click on the **Clear** button to reset all of the fields on this line.

9. Click on the **Apply** button to apply your changes to this session, or click **Save** to apply your changes and make them permanent.

WDS Client Link IAP Assignments:

10. For each desired client link, select the IAPs that are part of that link.

> *Once an IAP has been selected to act as a WDS client link, no other association will be allowed on that IAP. However, wireless associations will be allowed on the WDS host side of the WDS session.*

11. **Auto Configure**: Click this button to instruct the Array to automatically determine the best channel allocation settings for each IAP that participates in a WDS link, based on changes in the environment. These changes are executed immediately, and are automatically applied.

12. **Reset All Links**: this command tears down all links configured on the Array and sets them back to their factory defaults, effective immediately.

See Also
SSID Management
WDS Planning
WDS
WDS Statistics

Filters

The Wi-Fi Array's integrated firewall uses stateful inspection to speed the decision of whether to allow or deny traffic. Filters are used to define the rules used for blocking or passing traffic. Filters can also set the VLAN and QoS level for selected traffic.

User connections managed by the firewall are maintained statefully—once a user flow is established through the Array, it is recognized and passed through without application of all defined filtering rules. Stateful inspection runs automatically on the Array. The rest of this section describes how to view and manage filters.

Filters are organized in groups, called Filter Lists. A filter list allows you to apply a uniform set of filters to SSIDs or Groups very easily.

The read-only Filters window provides you with an overview of all filter lists that have been defined for this Array, and the filters that have been created in each list. Filters are listed in the left side column by name under the filter list to which they belong. Each filter entry includes information about the type of filter, the protocol it is filtering, which port it applies to, source and destination addresses, and QoS and VLAN assignments.

Figure 148. Filters

Filter Lists

This window allows you to create filter lists. The Array comes with one predefined list, named **Global**, which cannot be deleted. Filter lists (including Global) may be applied to SSIDs or to Groups. Only one filter list at a time may be applied to a group or SSID (although the filter list may contain a number of filters). All filters are created within filter lists.

Figure 149. Filter Lists

Procedure for Managing Filter Lists

1. **New Filter List Name:** Enter a name for the new filter list in this field, then click on the Create button to create the list. All new filters are disabled when they are created. The new filter list is added to the Filter List table in the window. Click on the filter list name, and you will be taken to the Filter Management window for that filter list.

2. **On**: Check this box to enable this filter list, or leave it blank to disable the list. If the list is disabled, you may still add filters to it or modify it, but none of the filters will be applied to data traffic.

3. **Filters**: This read-only field displays the number of filters that belong to this filter list.

4. **SSIDs**: This read-only field lists the SSIDs that use this filter list.

5. **User Groups**: This read-only field lists the Groups that use this filter list.

6. **Delete**: Click this checkbox and then click the **Apply** or **Save** button to delete this filter list.

7. Click on the **Apply** button to apply your changes to the selected filter, or click **Save** to apply your changes and make them permanent.

8. Click a filter list to go to the Filter Management window to create and manage the filters that belong to this list.

Filter Management

This window allows you to create and manage filters that belong to a selected filter list, based on the filter criteria you specify.
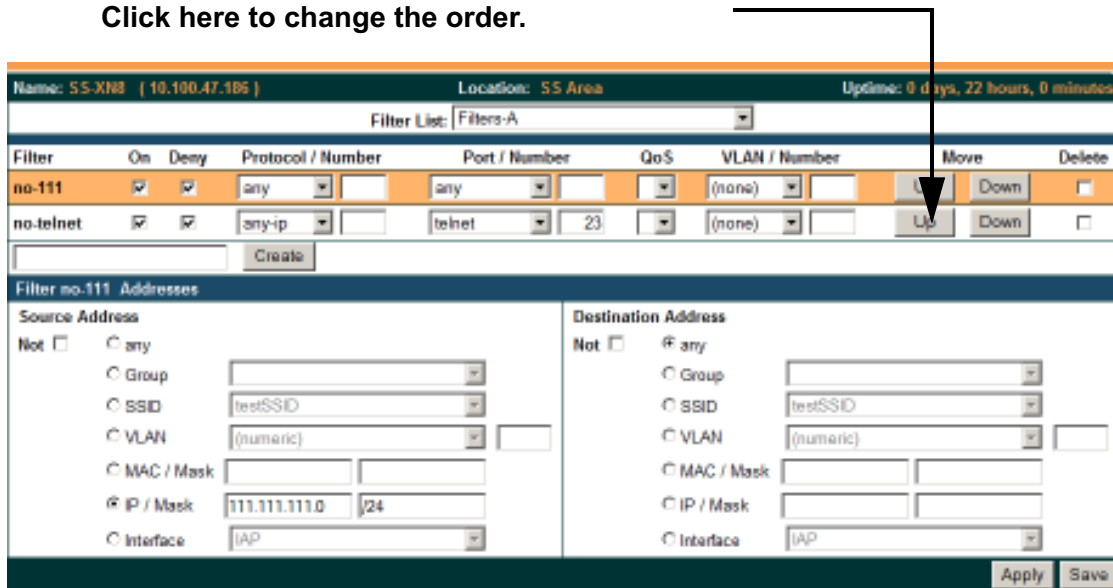
Figure 150. Filter Management

Note that filtering is secondary to the stateful inspection performed by the integrated firewall. Traffic for established connections is passed through without the application of these filtering rules.

Procedure for Managing Filters

1. **Filter List:** Select the filter list to display and manage on this window. All of the filters already defined for this list are shown, and you may create additional filters for this list.

2. **New Filter Name**: Enter a name for the new filter in the field next to the **Create** button, then click on the **Create** button to create the filter. All new filters are added to the table of filters at the top of the window. The filter name must be unique within the list, but it may have the same name as a filter in a different filter list. Two filters with the same name in different filter lists will be completely unrelated to each other—they may be defined with different parameter values.

3. **Filter**: Choose a filter entry to modify from the list at the top of the window.

4. **On**: Use this field to enable or disable this filter.

5. **Deny**: Choose whether this filter will be an **Allow** filter or a **Deny** filter. If you define the filter as an Allow filter, then any associations that meet the filter criteria will be allowed. If you define the filter as a Deny filter, any associations that meet the filter criteria will be denied.

6. **Protocol**: Choose a specific filter protocol from the pull-down list, or choose **numeric** and enter a **Number**, or choose **any** to instruct the Array to use the best filter. This is a match criterion.

7. **Port**: From the pull-down list, choose the type of port on which you want this filter to be active, or choose **1-65534** and enter a **Number**, or choose **any** to instruct the Array to apply the filter to any port. This is a match criterion.

8. **QoS**: (Optional) Set packets that match the filter criteria to this QoS level (0 to 3) from the pull-down list. Level 0 has the lowest priority; level 3 has the highest priority. By default, this field is blank and the filter does not modify QoS level. See "Understanding QoS Priority on the Wi-Fi Array" on page 237.

9. **VLAN ID**: (Optional) Set packets that match the filter criteria to this VLAN. Select a VLAN from the pull-down list, or select **numeric** and enter the number of a previously defined VLAN (see "VLANs" on page 205).

10. **Move Up/Down**: The filters are applied in the order in which they are displayed in the list, with filters on the top applied first. To change an entry's position in the list, just click its **Up** or **Down** button.

11. **Source Address**: Define a source address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.

12. **Destination Address**: Define a destination address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.

13. To delete a filter, check its **Delete** checkbox, then click the **Apply** or **Save** button.

14. Click on the **Apply** button to apply your changes to the selected filter, or click **Save** to apply your changes and make them permanent.

See Also
Filters
Filter Statistics
Understanding QoS Priority on the Wi-Fi Array
VLANs

Using Tools on the Wi-Fi Array

These WMI windows allow you to perform administrative tasks on your Array, such as upgrading software, rebooting, uploading and downloading configuration files, and other utility tasks. Tools are described in the following sections:

- **"System Tools" on page 296**
- **"CLI" on page 303**
- **"Logout" on page 305**

This section does not discuss using status or configuration windows. For information on those windows, please see:

- **"Viewing Status on the Wi-Fi Array" on page 127**
- **"Configuring the Wi-Fi Array" on page 175**

System Tools

This window allows you to manage files for software images, configuration, and Web Page Redirect (WPR), manage the system's configuration parameters, reboot the system, and use diagnostic tools.

Figure 151. System Tools

Procedure for Configuring System Tools

These tools are broken down into the following sections:

- System
- Configuration
- Diagnostics

- Web Page Redirect
- Tools
- Progress and Status Frames

System

1. **Save & Reboot** or **Reboot**: Use **Save & Reboot** to save the current configuration and then reboot the Array. The LEDs on the Array indicate the progress of the reboot, as described in "Powering Up the Wi-Fi Array" on page 107. Alternatively, use the **Reboot** button to discard any configuration changes which have not been saved since the last reboot.

2. **Software Upgrade**: This feature upgrades the ArrayOS to a newer version provided by Xirrus. Enter the filename and directory location (or click on the **Browse** button to locate the software upgrade file), then click on the **Upgrade** button to upload the new file to the Array. Progress of the operation will be displayed below, in the **Progress** section. Completion status of the operation is shown in the **Status** section.

   This operation does not run the new software or change any configured values. The existing software continues to run on the Array until you reboot, at which time the uploaded software will be used.

   ✎ *If you have difficulty upgrading the Array using the WMI, see "Upgrading the Array via CLI" on page 409 for a lower-level procedure you may use.*

   *Software Upgrade always uploads the file in binary mode. If you transfer any image file to your computer to have it available for the Software Upgrade command, it is **critical** to remember to transfer it (ftp, tftp) in **binary** mode!*

3. **License Key**: If Xirrus Customer Support provides you with a new license key for your Array, use this field to enter it. A valid license is required for Array operation, and it controls the features available on the Array. If you upgrade your Array for additional features, you will be provided with a license key to activate those capabilities.

   If you attempt to enter an invalid key, you will receive an error message and the current key will not be replaced.

Configuration

4. **Update from Remote File**: This field allows you to define the path to a configuration file (one that you previously saved—see Step 6 below). Click on the **Browse** button if you need to browse for the location of the file, then click **Update** to update your configuration settings.

5. **Update from Local File**: This field updates Array settings from a local configuration file on the Array. Select one of the following files from the drop-down list:

   • **factory.conf**: The factory default settings

   • **lastboot.conf**: The setting values from just before the last reboot

   • **saved.conf**: The last settings that were explicitly saved

   Click **Update** to update your configuration settings.

6. **Download Current Configuration:** Click on the link titled **xs_current.conf** to download the Array's current configuration settings to a file (that you can upload back to the Array at a later date). The system will prompt you for a destination for the file. The file will contain the Array's current configuration values.

   Important! When you have initially configured your Array, or have made significant changes to its configuration, we strongly recommend that you save the configuration to a file in order to have a safe backup of your working configuration.

7. **Reset to Factory Defaults**: Click on the **Reset/Preserve IP Settings** button to reset the system's current configuration settings to the factory default values, *except for the Array's management IP address which is left unchanged*. This function allows you to maintain management connectivity to the Array even after the reset. This will retain the Gigabit Ethernet port's IP address (see "Network Interfaces" on page 183), or if you have configured management over a VLAN it will maintain the management VLAN's IP address (see "VLAN Management" on page 207). *All other previous configuration settings will be lost*.

Click **Reset** to reset all of the system's current configuration settings to the factory default values, including the management IP address—*all previous configuration settings will be lost*. The Array's Gigabit Ethernet ports default to using DHCP to obtain an IP address.

✎ *If the IP settings change, the connection to the WMI may be lost.*

Diagnostics

8. **Diagnostic Log**: Click the **Create** button to save a snapshot of Array information for use by Xirrus Customer Support personnel. The Progress and Status Frames show the progress of this operation. When the process is complete, the filename `xs_diagnostic.log` will be displayed in blue and provides a link to the newly created log file. Click the link to download this file to the `C:\` folder on your local computer. (Figure 152)

Click Update to create log

Diagnostics

Diagnostic Log: xs_diagnostic.log   Create

**Then click this link to save
log file to local computer**
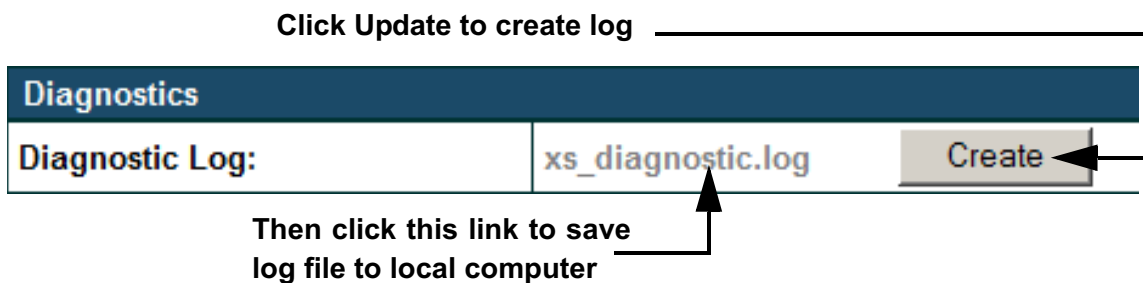
Figure 152. Saving the Diagnostic Log

This feature is only used at the request of Customer Support. It saves all of the information regarding your Array, including status, configuration, statistics, log files, and recently performed actions.

The diagnostic log is always saved as a file named `xs_diagnostic.log` on your `C:\` drive, so you should immediately rename the file to save it. This way, it will not be lost the next time you save a diagnostic log. Often, Customer Support will instruct you to save two diagnostic logs about ten minutes apart so that they can examine the difference in statistics

between the two snapshots (for example, to see traffic and error statistics for the interval). Thus, you must rename the first diagnostic log file.

All passwords are stored on the array in an encrypted form and will not be exposed in the diagnostic log.

Web Page Redirect

The Array uses a Perl script and a cascading style sheet to define the default splash/login Web page that the Array delivers for WPR. You may replace these files with files for one or more custom pages of your own. See Step 11 below to view the default files. See Step 14 on page 243 for more information about WPR and how the splash/login page is used.

Each SSID that has WPR enabled may have its own page. Custom files for a specific SSID **must** be named based on the SSID name. For example, if the SSID is named **Public**, the default `wpr.pl` and `hs.css` files should be modified as desired and renamed to `wpr-Public.pl` and `hs-Public.css` before uploading to the Array. If you modify and upload files named `wpr.pl` and `hs.css`, they will replace the factory default files and will be used for any SSID that does not have its own custom files, per the naming convention just described. Be careful not to replace the default files unintentionally.
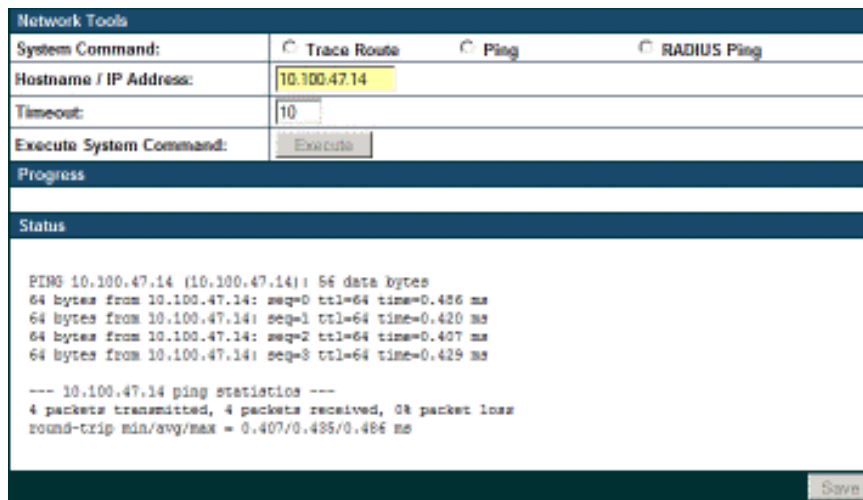
Figure 153. Managing WPR Splash/Login page files

9. **Upload File**: Use this to install files for your own custom WPR splash/ login page (as described above) on the Array. Note that uploaded files are not immediately used - you must reboot the Array first. At that time, the Array looks for and uses these files, if found.

Enter the filename and directory location (or click **Browse** to locate the splash/login page files), then click on the **Upload** button to upload the new files to the Array. You must reboot to make your changes take effect.

10. **Remove File**: Enter the name of the WPR file you want to remove, then click on the **Delete** button. You can use the **List Files** button to show you a list of files that have been saved on the Array for WPR. The list is displayed in the **Status** section at the bottom of the WMI window. You must reboot to make your changes take effect.

11. **Download Sample Files**: Click on a link to access the corresponding sample WPR files:

   • **wpr.pl**—a sample Perl script.

   • **hs.css**—a sample cascading style sheet.

Tools

Figure 154. System Command (Ping)

12. **System Command**: Choose **Trace Route**, **Ping**., or **RADIUS Ping**. For Trace Route and Ping, fill in **IP Address** and **Timeout**. Then click the **Execute** button to run the command.

   The RADIUS Ping command is a simple utility that tests connectivity to a RADIUS server by attempting to log in with the specified Username and

Password. When using a RADIUS server, this command allows you to verify that the server configuration is correct and whether a particular Username and Password are set up properly. If a client is having trouble accessing the network, you can quickly determine if there is a basic RADIUS problem by using the RADIUS Ping tool. For example, in Figure 155 (A), RADIUS Ping is unable to contact the server. In Figure 155 (B), RADIUS Ping verifies that the host information and secret for a RADIUS server are correct, but that the user account information is not.

Select RADIUS allows you to select a RADIUS server that you have already configured (External Radius, Internal Radius, or a server specified for a particular SSID), or select **Other Server** to specify another server by entering its **Host** name or IP address, **Port**, and shared **Secret**. Enter the **RADIUS Credentials**: **Username** and **Password**, then click the **Execute** button to run the command. The message **Testing RADIUS connection** appears. Click **OK** to proceed.

A — Windows Internet Explorer: Testing RADIUS connection ... server is not responding. Host is down, RADIUS secret is incorrect, or authentication failed. [OK]

B — The page at https://adrians-3900 says: Testing RADIUS connection ... host and secret are correct. Testing username and password ... authentication or authorization failed. [OK]
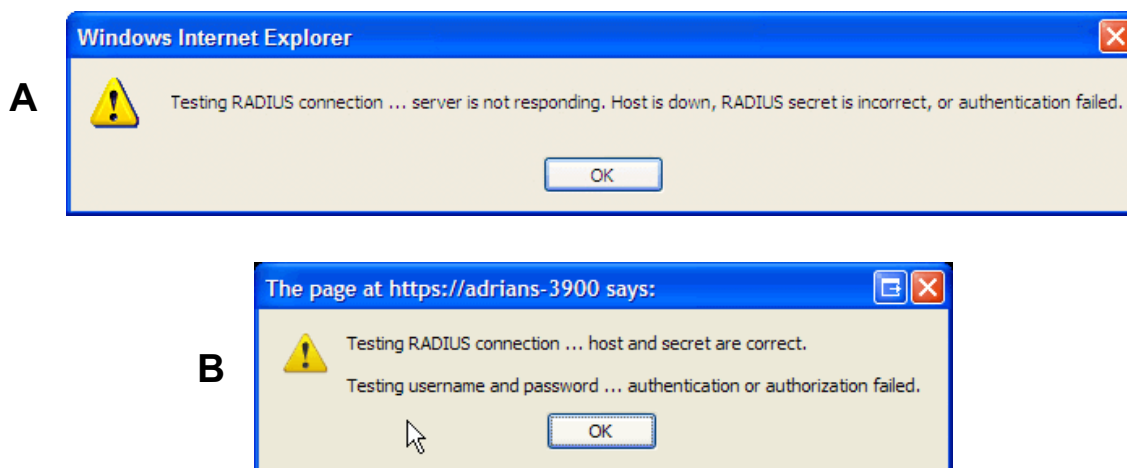
Figure 155. Radius Ping Output

13. **IP Address**: For Ping or Trace Route, enter the IP address of the target device.

14. **Timeout**: For Ping or Trace Route, enter a value (in seconds) before the action times out.

15. **Execute System Command**: Click **Execute** to start the specified command. Progress of command execution is displayed in the **Progress** frame. Results are displayed in the **Status** frame.

Progress and Status Frames

The **Progress** frame displays a progress bar for commands such as Software Upgrade and Ping. The **Status** frame presents the output from system commands (Ping and Trace Route), as well as other information, such as the results of software upgrade.

16. If you want to save the parameters you established in this window for future sessions, click on the **Save** button.

CLI

The WMI provides this window to allow you to use the Array's Command Line Interface (CLI). You can enter commands to configure the Array, or display information using show commands. You will not need to log in - you already logged in to the Array when you started the WMI.
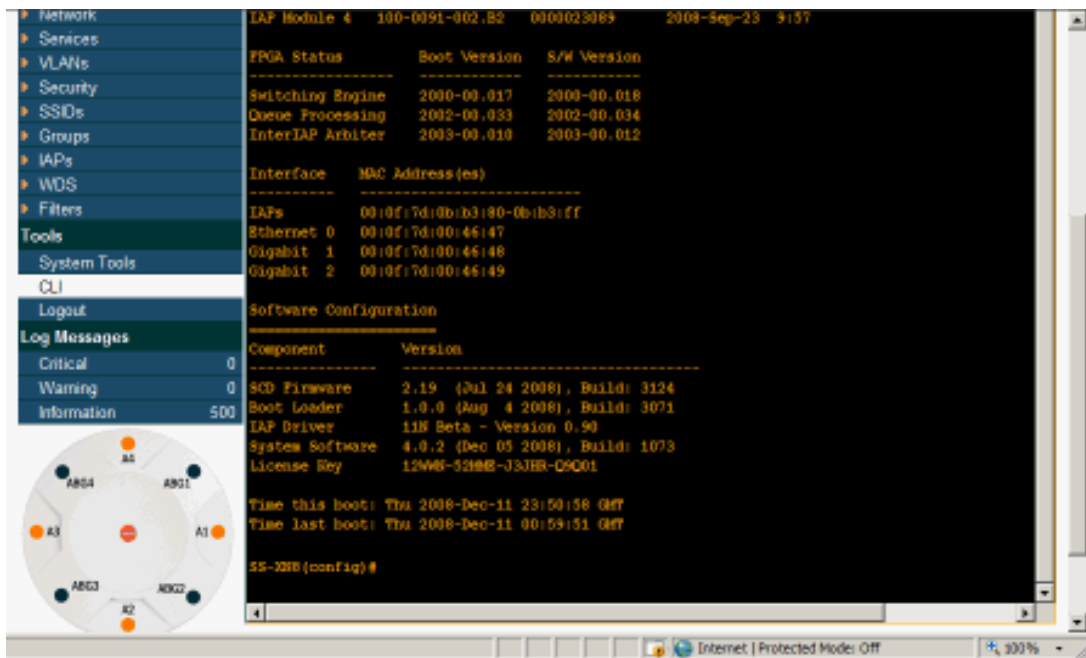
Figure 156. CLI Window

To enter a command, simply type it in. The command is echoed and output is shown in the normal way—that is, the same way it would be if you were using the CLI directly. You may use the extra scroll bar inside the right edge of the window to scroll through your output.

This window has some minor differences, compared to direct use of the CLI via the console or an SSH connection:

● The CLI starts in **config** mode. All configuration and show commands are available in this mode. You can "drill down" the mode further in the usual way. For example, you can type **interface iap** to change the mode to **config-iap**. The prompt will indicate the current command mode, for example:
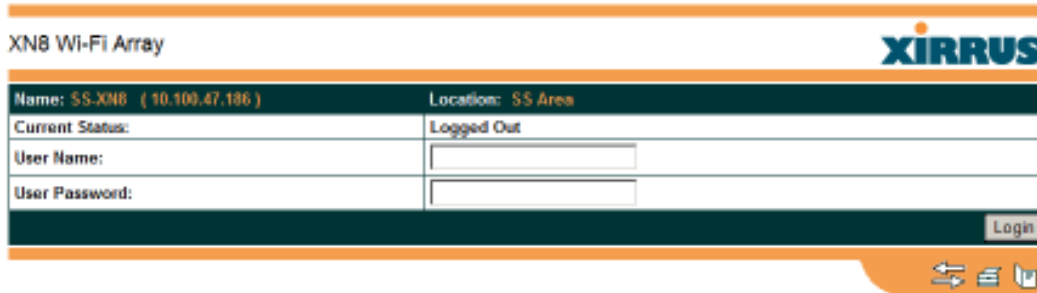
```
My-Array(config-iap) #
```

● You can abbreviate a command and it will be executed if you have typed enough of the command to be unambiguous. The command will not auto-complete, however. Only the abbreviated command that you actually typed will be shown. You can type a partial command and press Tab to have the command auto-complete. If the partial command is ambiguous a list of legal endings is displayed.

● Entering **quit** will return you to the previously viewed WMI page.

● Most, but not all, CLI commands can be run in this window. Specifically the **run-test** menu of commands is **not** available in this window. To use the run-test command, please connect using SSH and use CLI directly, or use the System Tools described in this chapter, such as Trace Route, Ping, and RADIUS Ping.

Help commands (the **?** character) are available, either at the prompt or after you have typed part of a command.

Logout

Click on the Logout button to terminate your session. When the session is terminated, you are presented with the Array's login window.

Figure 157. Login Window

The Command Line Interface

This section covers the commands and the command structure used by the Wi-Fi Array's Command Line Interface (CLI), and provides a procedure for establishing a Telnet connection to the Array. Topics discussed include:

- **"Establishing a Secure Shell (SSH) Connection" on page 307**.
- **"Getting Started with the CLI" on page 309**.
- **"Top Level Commands" on page 311**.
- **"Configuration Commands" on page 320**.
- **"Sample Configuration Tasks" on page 355**.

See Also
Establishing Communication with the Array
Network Map
System Tools
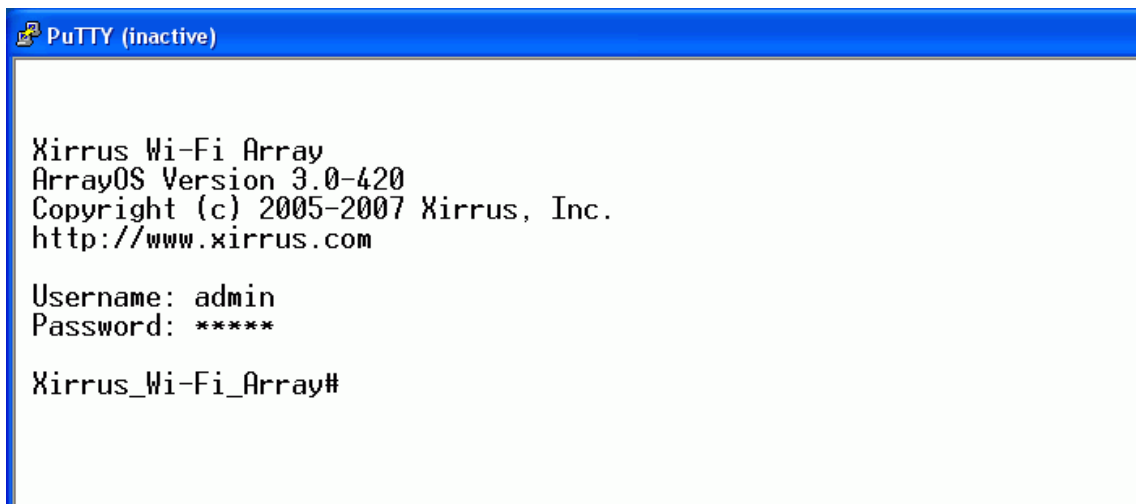
Establishing a Secure Shell (SSH) Connection

Use this procedure to initialize the system and log in to the Command Line Interface (CLI) via a Secure Shell (SSH) utility, such as PuTTY. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. Make sure that your SSH utility is set up to use SSH-2.

1. Start your SSH session and communicate with the Array via its IP address.

   - If the Array is connected to a network that uses DHCP, use the address assigned by DHCP. We recommend that you have the network administrator assign a reserved address to the Array for ease of access in the future.

   - If the network does not use DHCP, use the factory default address 10.0.2.1 to access either the Gigabit 1 or Gigabit 2 Ethernet port. You may need to change the IP address of the port on your computer that

---

is connected to the Array—change that port's IP address so that it is on the same 10.0.2.xx subnet as the Array port.

- If your Array is an 8-, 12-, or 16-port model, it has a 10/100Mb Ethernet port called Ethernet0. This management port has a default IP address of 10.0.1.1. You may connect your computer directly to this port, but you will need to set the IP address of the connected port on your computer to the 10.0.1.xx subnet.

2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the Array's Command Line Interface.

```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array#
```

Figure 158. Logging In

Getting Started with the CLI

The root command prompt (**Root Command Prompt**) is the first prompt you see after logging in to the CLI. If you are at a level other than the root command prompt you can return to this prompt at any time by using the **exit** command to step back through each command prompt level. The root command prompt you see in the CLI window is determined by the host name you assigned to your Array. The prompt **Xirrus_Wi-Fi_Array** is displayed throughout this document simply because this is the host name assigned to the Array used for development. To terminate your session at any time, use the **quit** command.

Note: If you terminate your session, with either the quit or exit command, your WMI session will also be terminated.

Inputting Commands

When inputting commands you need only type as many characters as the system requires before it recognizes your input. For example, you can type the abbreviated term **config** to access the configure prompt.

Getting Help

The CLI offers the following two levels of assistance:

● **help Command**

The **help** command is only available at the root command prompt. Initiating this command generates a window that provides information about the types of help that are available with the CLI.

Figure 159. Help Window
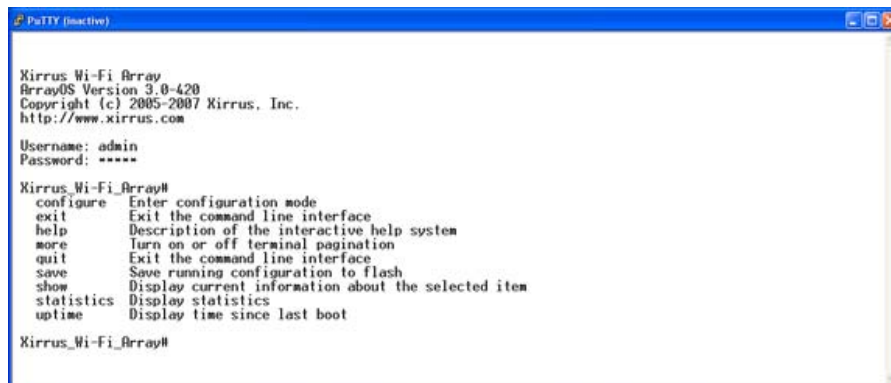
- **? Command**

  This command is available at any prompt and provides either FULL or PARTIAL help. Using the **?** (question mark) command when you are ready to enter an argument will display all the possible arguments (full help). Partial help is provided when you enter an abbreviated argument and you want to know what arguments will match your input.

Figure 160. Full Help

Figure 161 shows an example of how the Help system can provide the argument and format when specifying the time zone under the **date-time** command.

Figure 161. Partial Help

Top Level Commands

This section offers an at-a-glance view of all top level commands—organized alphabetically. Top level commands are defined here as commands that are directly accessible from the root command prompt (**Xirrus_Wi-Fi_Array#**). The root command prompt is based on the host name assigned to your Array. When inputting commands, be aware that all commands are **case-sensitive**.

All other commands are considered second level configuration commands—these are the commands you use to configure specific elements of the Array's features and functionality. For a listing of these commands with examples of command formats and structure, go to "Configuration Commands" on page 320.

Root Command Prompt

The following table shows the top level commands that are available from the root command prompt [**Xirrus_Wi-Fi_Array**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
configure	Enter the configuration mode. See "Configuration Commands" on page 320.
exit	Exit the CLI and terminate your session—if this command is used at any level other than the root command prompt you will simply exit the current level (step back) and return to the previous level.
help	Show a description of the interactive help system. See also, "Getting Help" on page 309.
history	List history of commands that have been executed.
more	Turn terminal pagination ON or OFF.
quit	Exit the Command Line Interface (from any level).
search	Search for pattern in show command output.

Command	Description
show	Display information about the selected item. See "show Commands" on page 315.
statistics	Display statistical data about the Array. See "statistics Commands" on page 318.
uptime	Display the elapsed time since the last boot.

configure Commands

The following table shows the second level commands that are available with the top level **configure** command [**Xirrus_Wi-Fi_Array(config)#**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
acl	Configure the Access Control List.
admin	Define administrator access parameters.
cdp	Configure Cisco Discovery Protocol settings.
clear	Remove/clear the requested elements.
contact-info	Contact information for assistance on this Array.
date-time	Configure date and time settings.
dhcp-server	Configure the DHCP Server.
dns	Configure the DNS settings.
end	Exit the configuration mode.
exit	Go UP one mode level.
file	Manage the file system.
filter	Define protocol filter parameters.
fips	Enable/disable FIPS 140-2, Level 2 Security.

Command	Description
group	Define user groups with parameter settings
help	Description of the interactive Help system.
history	List history of commands that have been executed.
hostname	Host name for this Array.
https	Enable/disable HTTPS.
interface	Select the interface to configure.
license	Enter a license key.
load	Load running configuration from flash
location	Location name for this Array.
management	Configure array management parameters
more	Turn ON or OFF terminal pagination.
netflow	Configure NetFlow data collector.
no	Disable (if enabled) or set to default value.
pci-audit	PCI DSS security monitoring.
quit	Exit the Command Line Interface.
radius-server	Configure the RADIUS server parameters.
reboot	Reboot the Array.
reset	Reset all settings to their factory default values and reboot.
run-tests	Run selective tests.
save	Save the running configuration to FLASH.
search	Search for pattern in show command output.
security	Set the security parameters for the Array.

Command	Description
show	Display current information about the selected item.
snmp	Enable, disable or configure SNMP.
ssh	Enable/disable SSH.
ssid	Configure the SSID parameters.
standby	Configure the standby parameters.
statistics	Display statistics.
syslog	Enable, disable or configure the Syslog Server.
telnet	Enable/disable Telnet.
uptime	Display time since the last boot.
vlan	Configure VLAN parameters.

show Commands

The following table shows the second level commands that are available with the top level **show** command [**Xirrus_Wi-Fi_Array# show**].

Command	Description
acl	Display the Access Control List.
admin	Display the administrator list or login information.
array-info	Display system information.
associated-stations	Display stations that have associated to the Array.
boot-env	Display Boot loader environment variables.
capabilities	Display detailed station capabilities.
cdp	Display Cisco Discovery Protocol settings.
channel-list	Display list of Array's 802.11a(n) and bg(n) channels.
clear-text	Display and enter passwords and secrets in the clear.
conntrack	Display the Connection Tracking table.
console	Display terminal settings.
contact-info	Display contact information.
country-list	Display countries that the Array can be set to support.
date-time	Display date and time settings summary.
dhcp-leases	Display IP addresses (leases) assigned to stations by the DHCP server.
dhcp-pool	Display internal DHCP server settings summary information.

Command	Description
diff	Display the difference between configurations.
dns	Display DNS summary information.
env-ctrl	Display the environmental controller status for the outdoor enclosure.
error-numbers	Display the detailed error number in error messages.
ethernet	Display Ethernet interface summary information.
external-radius	Display summary information for the external RADIUS server settings.
factory-config	Display the Array factory configuration information.
filters	Display filter information.
iap	Display IAP configuration information.
internal-radius	Display the users defined for the embedded RADIUS server.
lastboot-config	Display Array configuration at the time of the last boot-up.
management	Display settings for managing the Array, plus Standby, FIPS, and other information.
network-map	Display network map information.
realtime-monitor	Display realtime statistics for all IAPs.
rogue-ap	Display rogue AP information.
route	Display the routing table.
rssi-map	Display RSSI map by IAP for station.
running-config	Display configuration information for the Array currently running.

Command	Description
saved-config	Display the last saved Array configuration.
security	Display security settings summary information.
self-test	Display self test results.
snmp	Display SNMP summary information.
spanning-tree	Display spanning tree information.
spectrum-analyzer	Display spectrum analyzer measurements.
ssid	Display SSID summary information.
stations	Display station information.
statistics	Display statistics.
syslog	Display the system log.
syslog-settings	Display the system log (Syslog) settings.
temperature	Display the current board temperatures.
unassociated-stations	Display unassociated station information.
vlan	Display VLAN information.
wds	Display WDS information.
<cr>	Display configuration or status information.

statistics Commands

The following table shows the second level commands that are available with the top level **statistics** command [**Xirrus_Wi-Fi_Array# statistics**].

Command	Description
ethernet	Display statistical data for all Ethernet interfaces.
Ethernet Name **eth0**, **gig1**, **gig2**	Display statistical data for the defined Ethernet interface (either eth0, gig1 or gig2). FORMAT: **statistics gig1**
filter	Display statistics for defined filters (if any). FORMAT: **statistics filter [detail]**
filter-list	Display statistics for defined filter list (if any). FORMAT: **statistics filter <filter-list>**
iap	Display statistical data for the defined IAP. FORMAT: **statistics iap abgn4**
station	Display statistical data about associated stations. FORMAT: **statistics station billw**
vlan	Display statistical data for the defined VLAN. You must use the VLAN number (not its name) when defining a VLAN. FORMAT: **statistics vlan 1**
wds	Display statistical data for the defined active WDS (Wireless Distribution System) links. FORMAT: **statistics wds 1**

Command	Description
<cr>	Display configuration or status information.

Configuration Commands

All configuration commands are accessed by using the **configure** command at the root command prompt (**Xirrus_Wi-Fi_Array#**). This section provides a brief description of each command and presents sample formats where deemed necessary. The commands are organized alphabetically. When inputting commands, be aware that all commands are **case-sensitive**.

To see examples of some of the key configuration tasks and their associated commands, go to "Sample Configuration Tasks" on page 355.

acl

The **acl** command [**Xirrus_Wi-Fi_Array(config)# acl**] is used to configure the Access Control List.

Command	Description
add	Add a MAC address to the list. FORMAT: **acl add AA:BB:CC:DD:EE:FF**
del	Delete a MAC address from the list. FORMAT: **acl del AA:BB:CC:DD:EE:FF**
disable	Disable the Access Control List FORMAT: **acl disable**
enable	Enable the Access Control List FORMAT: **acl enable**
reset	Delete all MAC addresses from the list. FORMAT: **acl reset**

admin

The **admin** command [**Xirrus_Wi-Fi_Array(config-admin)#**] is used to configure the Administrator List.

Command	Description
add	Add a user to the Administrator List. FORMAT: **admin add [userID]**
del	Delete a user to the Administrator List. FORMAT: **admin del [userID]**
edit	Modify user in the Administrator List. FORMAT: **admin edit [userID]**
radius	Define a RADIUS server to be used for authenticating administrators. FORMAT: **admin radius [disable | enable | off | on | timeout <seconds> | auth-type [PAP | CHAP]]** **admin radius [primary |secondary]** **port <portid> server [<ip-addr> | <host>]** **secret <shared-secret>**
reset	Delete all users and restore the default user. FORMAT: **admin reset**

cdp

The **cdp** command [**Xirrus_Wi-Fi_Array(config)# cdp**] is used to configure the Cisco Discovery Protocol.

Command	Description
disable	Disable the Cisco Discovery Protocol FORMAT: **cdp disable**
enable	Enable the Cisco Discovery Protocol FORMAT: **cdp enable**
hold-time	Select CDP message hold time before messages received from neighbors expire. FORMAT: **cdp hold-time [# seconds]**
interval	The Array sends out CDP announcements at this interval. FORMAT: **cdp interval [# seconds]**
off	Disable the Cisco Discovery Protocol FORMAT: **cdp off**
on	Enable the Cisco Discovery Protocol FORMAT: **cdp on**

The Command Line Interface

clear

The **clear** command [**Xirrus_Wi-Fi_Array(config)# clear**] is used to clear requested elements.

Command	Description
authentication	Deauthenticate a station. FORMAT: **clear station [authenticated station]**
history	Clear the history of CLI commands executed. FORMAT: **clear history**
screen	Clear the screen where you're viewing CLI output. FORMAT: **clear syslog**
statistics	Clear the statistics for a requested interface. FORMAT: **clear statistics [eth0]**
syslog	Clear all Syslog messages, but continue to log new messages. FORMAT: **clear syslog**

contact-info

The **contact-info** command [**Xirrus_Wi-Fi_Array(config)# contact-info**] is used for managing administrator contact information.

Command	Description
email	Add an email address for the contact (must be in quotation marks). FORMAT: **contact-info email ["contact@mail.com"]**
name	Add a contact name (must be in quotation marks). FORMAT: **contact-info name ["Contact Name"]**
phone	Add a telephone number for the contact (must be in quotation marks). FORMAT: **contact-info phone ["8185550101"]**

date-time

The **date-time** command [**Xirrus_Wi-Fi_Array(config-date-time)#**] is used to configure the date and time parameters. Your Array supports the Network Time Protocol (NTP) in order to ensure that the Array's internal time is accurate. NTP is set to UTC time by default; however, you can set the time zone so that your Array will display local time. This is done by defining an offset from the UTC value. For example, Pacific Standard Time is 8 hours behind UTC time, so the offset from UTC time would be -8.

Command	Description
dst_adjust	Enable adjustment for daylight savings. FORMAT: **date-time dst_adjust**
no	Disable daylight savings adjustment. FORMAT: **date-time no dst_adjust**
ntp	Enable the NTP server. FORMAT: **date-time ntp on** (or **off** to disable)
offset	Set an offset from Greenwich Mean Time. FORMAT: **date-time no dst_adjust**
set	Set the date and time for the Array. FORMAT: **date-time set [10:24 10/23/2007]**
timezone	Configure the time zone. FORMAT: **date-time timezone [-8]**

dhcp-server

The **dhcp-server** command [**Xirrus_Wi-Fi_Array(config-dhcp-server**)#] is used to add, delete and modify DHCP pools.

Command	Description
add	Add a DHCP pool. FORMAT: **dhcp-server add [dhcp pool]**
del	Delete a DHCP pool. FORMAT: **dhcp-server del [dhcp pool]**
edit	Edit a DHCP pool FORMAT: **dhcp-server edit [dhcp pool]**
reset	Delete all DHCP pools. FORMAT: **dhcp-server reset**

dns

The **dns** command [**Xirrus_Wi-Fi_Array(config-dns)#**] is used to configure your DNS parameters.

Command	Description
domain	Enter your domain name. FORMAT: **dns domain [www.mydomain.com]**
server1	Enter the IP address of the primary DNS server. FORMAT: **dns server1 [1.2.3.4]**
server2	Enter the IP address of the secondary DNS server. FORMAT: **dns server1 [2.3.4.5]**
server3	Enter the IP address of the tertiary DNS server. FORMAT: **dns server1 [3.4.5.6]**

file

The **file** command [**Xirrus_Wi-Fi_Array(config-file)#**] is used to manage files.

Command	Description
active-image	Validate and commit a new array software image.
backup-image	Validate and commit a new backup software image.
check-image	Validate a new array software image.
chkdsk	Check flash file system.
copy	Copy a file to another file. FORMAT: **file copy [sourcefile destinationfile]**
dir	List the contents of a directory. FORMAT: **file dir [directory]**
erase	Delete a file from the FLASH file system. FORMAT: **file erase [filename]**
format	Format flash file system.
ftp	Open an FTP connection with a remote server. Files will be transferred in binary mode. FORMAT: **file ftp host {<hostname> |<ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the Array, it **must** be transferred in binary mode, or the file may be corrupted.
list	List the contents of a file. FORMAT: **file list [filename]**

Command	Description
remote-config	When the Array boots up, it fetches the specified configuration file from the TFTP server defined in the **file remote-server** command, and uses this configuration. This must be an Array configuration file with a **.conf** extension. A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your Arrays but don't want to have the same IP address for each Array, you may remove the **ipaddr** line from the file. You can then load the file on each array and the local IP addresses will not change. FORMAT: **file remote-config <config-file.conf>** **Note:** If you enter **file remote-config ?**, the help response suggests possibilities by listing all of the configuration files that are currently in the Array's flash.
remote-image	When the Array boots up, it fetches the named image file from the TFTP server defined in the **file remote-server** command, and upgrades to this file before booting. This must be an Array image file with a **.bin** extension. FORMAT: **file remote-image <image-file.bin>** **Note**: This will happen every time that the Array reboots. If you only want to fetch the remote-image one time be sure to turn off the remote image option after the initial download.
remote-server	Sets up a TFTP server to be used for automated remote update of software image and configuration files when rebooting. FORMAT: **file remote-server A.B.C.D**
rename	Rename a file.
scp	Copy a file to or from a remote system.

Command	Description
tftp	Open a TFTP connection with a remote server. FORMAT: **file tftp host {<hostname>	<ip>} [port <port_#>] [user {anonymous	<username> password <passwd> }] { put <source_file> [<dest_file>]	get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the Array, it **must** be transferred in binary mode, or the file may be corrupted.

filter

The **filter** command [**Xirrus_Wi-Fi_Array(config-filter)#**] is used to manage protocol filters and filter lists.

Command	Description
add	Add a filter. FORMAT: **filter add [name]**
add-list	Add a filter list. FORMAT: **filter add-list [name]**
del	Delete a filter. FORMAT: **filter del [name]**
del-list	Delete a filter list. FORMAT: **filter del-list [name]**
edit	Edit a filter. FORMAT: **filter edit [name type]**
edit-list	Edit a filter list FORMAT: **filter edit-list [name type]**
enable	Enable a filter list. FORMAT: **filter enable**
move	Change a filter priority. FORMAT: **filter move [name priority]**

Command	Description
off	Disable a filter list. FORMAT: **filter off**
on	Enable a filter list. FORMAT: **filter on**
reset	Delete all protocol filters and filter lists. FORMAT: **filter reset**

fips

The **fips** command [**Xirrus_Wi-Fi_Array(config)# fips**] is used to set the parameter values required for FIPS 140-2, Level 2 security. For more information, see Appendix E: Implementing FIPS Security.

Command	Description
disable	Reverts FIPS settings to the values they had before performing a fips on command. FORMAT: **fips disable**
enable	Set FIPS security on the Array. Remembers the values of parameters prior to setting them. FORMAT: **fips enable**
off	Reverts FIPS settings to the values they had before performing a fips on command. FORMAT: **fips off**
on	Set FIPS security on the Array. Remembers the values of parameters prior to setting them. FORMAT: **fips on**

group

The **group** command [**Xirrus_Wi-Fi_Array(config)# group**] is used to create and configure user groups. User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs. For more information, see "Groups" on page 247.

Command	Description
add	Create a new user group. FORMAT: **group add [group-name]**
del	Delete a user group. FORMAT: **group del [group-name]**
edit	Set parameters values for a group. FORMAT: **group edit [group-name]**
reset	Reset the group. FORMAT: **group reset**

hostname

The **hostname** command [**Xirrus_Wi-Fi_Array(config)# hostname**] is used to change the hostname used by the Array.

Command	Description
hostname	Change the hostname of the Array. FORMAT: **hostname [name]**

https

The **https** command [**Xirrus_Wi-Fi_Array(config)# https**] is used to enable or disable the Web Management Interface (https), which is enabled by default. It also allows you to establish a timeout for your Web management session.

Command	Description
disable	Disable the https feature. FORMAT: **https disable**
enable	Enable the https feature. FORMAT: **https enable**
off	Disable the https feature. FORMAT: **https off**
on	Enable the https feature. FORMAT: **https on**
timeout	Define an elapsed period (in seconds) after which the Web Management Interface will time out. FORMAT: **https timeout 5000**

interface

The **interface** command [**Xirrus_Wi-Fi_Array(config)# interface**] is used to select the interface that you want to configure. To see a listing of the commands that are available for each interface, use the **?** command at the selected interface prompt. For example, using the **?** command at the **Xirrus_Wi-Fi_Array(config-gig1}#** prompt displays a listing of all commands for the **gig1** interface.

Command	Description
console	Select the console interface. The console interface is used for management purposes only. FORMAT: **interface console**
eth0	Select the Fast Ethernet interface. The Fast Ethernet interface is used for management purposes only. FORMAT: **interface eth0** Note: To configure a static route for management traffic, next enter: **static-route addr [ip-addr]** **static-route mask [subnet-mask]**
gig1	Select the Gigabit 1 interface. FORMAT: **interface gig1**
gig2	Select the Gigabit 2 interface. FORMAT: **interface gig2**
iap	Select an IAP. FORMAT: **interface iap**

license

The **license** command [**Xirrus_Wi-Fi_Array(config)# license**] is used to set the license key for the Array. A valid license is required for Array operation, and it controls the features available on the Array.

Command	Description
<cr>	Set the license for the Array. FORMAT: **license <license-key>** When you enter the new key obtained from Xirrus, simply hit the Enter key **<cr>** to apply it.

load

The **load** command [**Xirrus_Wi-Fi_Array(config)# load**] loads a configuration file.

Command	Description
factory.conf	Load the factory settings configuration file. FORMAT: **load [factory.conf]**
lastboot.conf	Load the configuration file from the last boot-up. FORMAT: **load [lastboot.conf]**
[myfile].conf	If you have saved a configuration, enter its name to load it. FORMAT: **load [myfile.conf]**
saved.conf	Load the configuration file with the last saved settings. FORMAT: **load [saved.conf]**

location

The **location** command [**Xirrus_Wi-Fi_Array(config)# location**] is used to set the location for the Array.

Command	Description
<cr>	Set the location for the Array. FORMAT: **location [newlocation]**

management

The **management** command [**Xirrus_Wi-Fi_Array(config)# management**] enters management mode, where you may configure console management parameters.

Command	Description
<cr>	Enter management mode. FORMAT: **management <cr>**

more

The **more** command [**Xirrus_Wi-Fi_Array(config)# more**] is used to turn terminal pagination ON or OFF.

Command	Description
off	Turn OFF terminal pagination. FORMAT: **more off**
on	Turn ON terminal pagination. FORMAT: **more on**

netflow

The **netflow** command [**Xirrus_Wi-Fi_Array(config-netflow)#**] is used to enable or disable, or configure sending IP flow information (traffic statistics) to the collector you specify.

Command	Description
disable	Disable netflow. FORMAT: **netflow disable**
enable	Enable netflow. FORMAT: **netflow enable**
off	Disable netflow. FORMAT: **netflow off**
on	Enable netflow. FORMAT: **netflow on**
collector	Set the netflow collector IP address or fully qualified domain name (host.domain). Only one collector may be set. If port is not specified, the default is 2055. FORMAT: **netflow collector host {<ip-addr> | <domain>} [port <port#>]**

no

The **no** command [**Xirrus_Wi-Fi_Array(config)# no**] is used to disable a selected element or set the element to its default value.

Command	Description
acl	Disable the Access Control List. FORMAT: **no acl**
dot11a	Disable all 802.11a(n) IAPs (radios). FORMAT: **no dot11a**
dot11bg	Disable all 802.11bg(n) IAPs (radios). FORMAT: **no dot11bg**
https	Disable https access. FORMAT: **no https**
intrude-detect	Disable intrusion detection. FORMAT: **no intrude-detect**
management	Disable management on all Ethernet interfaces. FORMAT: **no management**
more	Disable terminal pagination. FORMAT: **no more**
ntp	Disable the NTP server. FORMAT: **no ntp**

Command	Description
snmp	Disable SNMP features. FORMAT: **no snmp**
ssh	Disable ssh access. FORMAT: **no ssh**
syslog	Disable the Syslog services. FORMAT: **no syslog**
telnet	Disable Telnet access. FORMAT: **no telnet**
ETH-NAME	Disable the selected Ethernet interface (eth0, gig1 or gig2). You cannot disable the console interface. with this command. FORMAT: **no eth0** (gig1 or gig2)

pci-audit

The **pci-audit** command [**Xirrus_Wi-Fi_Array(config)# pci-audit**] checks the configuration of the Array for conformance with PCI DSS standards. When you enter the pci-audit command, it lists any settings that violate PCI DSS requirements. In addition, if pci-audit is on (enabled), the Array will warn you if you change any parameters in a way that violates PCI DSS requirements. For example, if you enable pci-audit and then set encryption to **none** on an SSID (in the CLI or the WMI), a warning will be displayed and a Syslog message will be issued. For more information, see Appendix D: Implementing PCI DSS.

Command	Description
disable	The Array will not check configuration changes for PCI DSS violations. FORMAT: **pci-audit disable**
enable	The Array reports any current settings that violate PCI DSS, and will warn you and issue a Syslog message if you attempt to save configuration changes that violate PCI DSS. FORMAT: **pci-audit enable**
off	The Array will not check configuration changes for PCI DSS violations. FORMAT: **pci-audit off**
on	The Array reports any current settings that violate PCI DSS, and will warn you and issue a Syslog message if you make configuration changes that that violate PCI DSS. FORMAT: **pci-audit on**

quit

The **quit** command [**Xirrus_Wi-Fi_Array(config)# quit**] is used to exit the Command Line Interface.

Command	Description
<cr>	Exit the Command Line Interface. FORMAT: **quit** If you have made any configuration changes and your changes have not been saved, you are prompted to save your changes to Flash. At the prompt, answer **Yes** to save your changes, or answer **No** to discard your changes.

radius-server

The **radius-server** command [**Xirrus_Wi-Fi_Array(config-radius-server)#**] is used to configure the external and internal RADIUS server parameters.

Command	Description
external	Configure an external RADIUS server. FORMAT: **radius-server external** To configure a RADIUS server (primary, secondary, or accounting server, by IP address or host name), and the reporting interval use: **radius-server external accounting**
internal	Configure the external RADIUS server. FORMAT: **radius-server internal**
use	Choose the active RADIUS server (either external or internal). FORMAT: **use external** (or internal)

reboot

The **reboot** command [**Xirrus_Wi-Fi_Array(config)# reboot**] is used to reboot the Array. If you have unsaved changes, the command will notify you and give you a chance to cancel the reboot.

Command	Description
<cr>	Reboot the Array. FORMAT: **reboot**
delay	Reboot the Array after a delay of 1 to 60 seconds. FORMAT: **reboot delay [n]**

reset

The **reset** command [**Xirrus_Wi-Fi_Array(config)# reset**] is used to reset all settings to their default values then reboot the Array.

Command	Description
<cr>	Reset all configuration parameters to their factory default values. FORMAT: **reset** The Array is rebooted automatically.
preserve-ip-settings	Preserve all ethernet and VLAN settings and reset all other configuration parameters to their factory default values. FORMAT: **reset preserve-ip-settings** The Array is rebooted automatically.

run-tests

The **run-tests** command [**Xirrus_Wi-Fi_Array(run-tests)#**] is used to enter run-tests mode, which allows you to perform a range of tests on the Array.

Command	Description
<cr>	Enter run-tests mode. FORMAT: **run-tests**
iperf	Execute iperf utility. FORMAT: **run-tests iperf**
kill-beacons	Turn off beacons for selected single IAP. FORMAT: **run-tests kill-beacons [off | iap-name]**
kill-probe-responses	Turn off probe responses for selected single IAP. FORMAT: **run-tests kill-probe-responses [off | iap-name]**
led	LED test. FORMAT: **run-tests led [flash | rotate]**
memtest	Execute memory tests. FORMAT: **run-tests memtest**
ping	Execute ping utility. FORMAT: **run-tests ping [host-name | ip-addr]**

Command	Description
radius-ping	Special ping utility to test the connection to a RADIUS server. FORMAT: **run-tests radius-ping [external | ssid <ssidnum>] [primary | secondary] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** **run-tests radius-ping [internal | server <radserver> port <radport> secret <radsecret>] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** You may select a RADIUS server that you have already configured (**ssid** or **external** or **internal**) or specify another server (**server**).
rlb	Run manufacturing radio loopback test. FORMAT: **run-tests rlb {optional command line switches}**
self-test	Execute self-test. FORMAT: **run-tests self-test {logfile-name (optional)]**
site-survey	Enable or disable site survey mode. FORMAT: **run-tests site-survey [on | off | enable | disable]**
ssh	Execute ssh utility. FORMAT: **run-tests ssh [hostname | ip-addr]** **[command-line-switches (optional)]**
tcpdump	Execute tcpdump utility to dump traffic for selected interface or VLAN. FORMAT: **run-tests tcpdump**

Command	Description
telnet	Execute telnet utility. FORMAT: **run-tests telnet [hostname | ip-addr] [command-line-switches (optional)]**
traceroute	Execute traceroute utility. FORMAT: **run-tests traceroute [host-name | ip-addr]**

security

The **security** command [**Xirrus_Wi-Fi_Array(config-security)#**] is used to establish the security parameters for the Array.

Command	Description
wep	Set the WEP encryption parameters. FORMAT: **security wep**
wpa	Set the WEP encryption parameters. FORMAT: **security wpa**

snmp

The **snmp** command [**Xirrus_Wi-Fi_Array(config-snmp)#**] is used to enable, disable, or configure SNMP.

Command	Description
v2	Enable SNMP v2. FORMAT: **snmp v2**
v3	Enable SNMP v3. FORMAT: **snmp v3**
trap	Configure traps for SNMP. Up to four trap destinations may be configured, and you may specify whether to send traps for authentication failure. FORMAT: **snmp trap**

ssh

The **ssh** command [**Xirrus_Wi-Fi_Array(config)# ssh**] is used to enable or disable the SSH feature. The Array only allows SSH-2 connections, so be sure that your SSH client is configured to use SSH-2.

Command	Description
disable	Disable SSH. FORMAT: **ssh disable**
enable	Enable SSH. FORMAT: **ssh enable**

Command	Description
off	Disable SSH. FORMAT: **ssh off**
on	Enable SSH. FORMAT: **ssh on**
timeout	Set the SSH inactivity timeout. FORMAT: **ssh timeout 300** (in seconds)

ssid

The **ssid** command [**Xirrus_Wi-Fi_Array(config-ssid)#**] is used to establish your SSID parameters.

Command	Description
add	Add an SSID. FORMAT: **ssid add [newssid]**
del	Delete an SSID. FORMAT: **ssid del [oldssid]**
edit	Edit an existing SSID. FORMAT: **ssid edit [existingssid]**
reset	Delete all SSIDs and restore the default SSID. FORMAT: **ssid reset**

standby

The **standby** command [**Xirrus_Wi-Fi_Array(config-ssid)#**] sets this Array to function as a standby unit for another Array.

Command	Description
mode	Enable or disable standby mode on this Array. FORMAT: **standby mode [disable | enable | off | on]**
target	Specify the MAC address of the target Array to be monitored for failure. FORMAT: **standby target [AA:BB:CC:DD:EE:FF]**

syslog

The **syslog** command [**Xirrus_Wi-Fi_Array(config-syslog)#**] is used to enable, disable, or configure the Syslog server.

Command	Description
console	Enable or disable the display of Syslog messages on the console, and set the level to be displayed. All messages at this level and lower (i.e., more severe) will be displayed. FORMAT: **syslog console [on/off] level [0-7]**
disable	Disable the Syslog server. FORMAT: **syslog disable**
email	Disable the Syslog server. FORMAT: **syslog email from [email-from-address] level [0-7] password [email-acct-password] server [email-server-IPaddr] test [test-msg-text] to-list [recipient-email-addresses] user [email-acct-username]**
enable	Enable the Syslog server. FORMAT: **syslog enable**
local-file	Set the size and/or severity level (all messages at this level and lower will be logged). FORMAT: **syslog local-file size [1-500] level [0-7]**
no	Disable the selected feature. FORMAT: **syslog no [feature]**

Command	Description
off	Disable the Syslog server. FORMAT: **syslog off**
on	Enable the Syslog server. FORMAT: **syslog on**
primary	Set the IP address of the primary Syslog server and/or the severity level of messages to be logged. FORMAT: **syslog primary [1.2.3.4] level [0-7]**
secondary	Set the IP address of the secondary (backup) Syslog server and/or the severity level of messages to be logged. FORMAT: **syslog primary [1.2.3.4] level [0-7]**

telnet

The **telnet** command [**Xirrus_Wi-Fi_Array(config)# telnet**] is used to enable or disable Telnet.

Command	Description
disable	Disable Telnet. FORMAT: **telnet disable**
enable	Enable Telnet. FORMAT: **telnet enable**
off	Disable Telnet. FORMAT: **telnet off**
on	Enable Telnet. FORMAT: **telnet on**
timeout	Set the Telnet inactivity timeout. FORMAT: **telnet timeout 300** (in seconds)

uptime

The **uptime** command [**Xirrus_Wi-Fi_Array(config)# uptime**] is used to display the elapsed time since you last rebooted the Array.

Command	Description
<cr>	Display time since last reboot. FORMAT: **uptime**

vlan

The **vlan** command [**Xirrus_Wi-Fi_Array(config-vlan)#**] is used to establish your VLAN parameters.

Command	Description
add	Add a VLAN. FORMAT: **vlan add [newvlan]**
default-route	Assign a VLAN for the default route (for outbound management traffic). FORMAT: **vlan default-route [defaultroute]**
delete	Delete a VLAN. FORMAT: **vlan delete [oldvlan]**
edit	Modify an existing VLAN. FORMAT: **vlan edit [existingvlan]**
native-vlan	Assign a native VLAN (traffic is untagged). FORMAT: **vlan native-vlan [nativevlan]**
no	Disable the selected feature. FORMAT: **vlan no [feature]**
reset	Delete all existing VLANs. FORMAT: **vlan reset**

Sample Configuration Tasks

This section provides examples of some of the common configuration tasks used with the Wi-Fi Array, including:

- **"Configuring a Simple Open Global SSID" on page 356.**
- **"Configuring a Global SSID using WPA-PEAP" on page 357.**
- **"Configuring an SSID-Specific SSID using WPA-PEAP" on page 358.**
- **"Enabling Global IAPs" on page 359.**
- **"Disabling Global IAPs" on page 360.**
- **"Enabling a Specific IAP" on page 361.**
- **"Disabling a Specific IAP" on page 362.**
- **"Setting Cell Size Auto-Configuration for All IAPs" on page 363**
- **"Setting the Cell Size for All IAPs" on page 364.**
- **"Setting the Cell Size for a Specific IAP" on page 365.**
- **"Configuring VLANs on an Open SSID" on page 366.**
- **"Configuring Radio Assurance Mode (Loopback Tests)" on page 367.**

To facilitate the accurate and timely management of revisions to this section, the examples shown here are presented as screen images taken from a Secure Shell (SSH) session (in this case, PuTTY). Depending on the application you are using to access the Command Line Interface, and how your session is set up (for example, font and screen size), the images presented on your screen may be different than the images shown in this section. However, the data displayed will be the same.

Some of the screen images shown in this section have been modified for clarity. For example, the image may have been "elongated" to show all data without the need for additional images or scrolling. We recommend that you use the Adobe PDF version of this User's Guide when reviewing these examples—a hard copy document may be difficult to read.

As mentioned previously, the root command prompt is determined by the host name assigned to your Array.

Configuring a Simple Open Global SSID

This example shows you how to configure a simple open global SSID.

```
PuTTY (inactive)


Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption none broadcast
 Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
================================================
State              Enabled
Active             Yes
Encryption         Global Open
VLAN Name
VLAN Number        -
QoS Level          2
Active Band        802.11a & 802.11bg
Broadcast          On
DHCP Pool          none
Traffic Limit      Unlimited
Traffic/Station    Unlimited
Time on            Always
Time off           Never
Days on            All
Web Page Redirect  Disabled
```

Figure 162. Configuring a Simple Open Global SSID

Configuring a Global SSID using WPA-PEAP

This example shows you how to configure a global SSID using WPA-PEAP encryption in conjunction with the Array's Internal RADIUS server.

```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption wpa broadcast
 Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
=================================================
State              Disabled
Active             No
Encryption         Global WPA
VLAN Name
VLAN Number        -
QoS Level          2
Active Band        802.11a & 802.11bg
Broadcast          On
DHCP Pool          none
Traffic Limit      Unlimited
Traffic/Station    Unlimited
Time on            Always
Time off           Never
Days on            All
Web Page Redirect  Disabled

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# top
Xirrus_Wi-Fi_Array(config)# radius-server use internal
 Xirrus_Wi-Fi_Array(config)# radius-server internal add Mike password Jones ssid Companyx
 Xirrus_Wi-Fi_Array(config)# radius-server internal
Xirrus_Wi-Fi_Array(config-radius-internal)# show

Username                               SSID
---------                              -----
Mike                                   Companyx

Xirrus_Wi-Fi_Array(config-radius-internal)# save
 Xirrus_Wi-Fi_Array(config-radius-internal)# top
Xirrus_Wi-Fi_Array(config)# security wpa
Xirrus_Wi-Fi_Array(config-security-wpa)# show

Global Security Settings Summary
--------------------------------
WEP:  key 1 size : not set (default)
      key 2 size : not set
      key 3 size : not set
      key 4 size : not set

WPA:  cipher     : TKIP  on, AES off
      key mgmt   : EAP   on, PSK off
      rekey time : disabled
      passphrase : not set


Xirrus_Wi-Fi_Array(config-security-wpa)#
```

Figure 163. Configuring a Global SSID using WPA-PEAP

Configuring an SSID-Specific SSID using WPA-PEAP

This example shows you how to configure an SSID-specific SSID using WPA-PEAP encryption in conjunction with the Array's Internal RADIUS server.

```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption wpa ssid_specific broadcast
 Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# radius-server use internal
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# radius-server internal add Mike password Jones
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
 sXirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
=================================================
State               Enabled
Active              Yes
Encryption          SSID specific WPA
VLAN Name
VLAN Number         -
QoS Level           2
Active Band         802.11a & 802.11bg
Broadcast           On
DHCP Pool           none
Traffic Limit       Unlimited
Traffic/Station     Unlimited
Time on             Always
Time off            Never
Days on             All
Web Page Redirect   Disabled

SSID Specific WPA Security Settings
-----------------------------------
Key Management      EAP   on, PSK   off
PSK Passphrase      not set
Radius Server       internal

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# top
Xirrus_Wi-Fi_Array(config)# radius-server internal
Xirrus_Wi-Fi_Array(config-radius-internal)# show

Username                                    SSID
---------                                   -----
Mike                                        Companyx

Xirrus_Wi-Fi_Array(config-radius-internal)# save
 Xirrus_Wi-Fi_Array(config-radius-internal)#
```

Figure 164. Configuring an SSID-Specific SSID using WPA-PEAP

Enabling Global IAPs

This example shows you how to enable all IAPs (radios), regardless of the wireless technology they use.

Figure 165. Enabling Global IAPs

Disabling Global IAPs

This example shows you how to disable all IAPs (radios), regardless of the wireless technology they use.

Figure 166. Disabling Global IAPs

Enabling a Specific IAP

This example shows you how to enable a specific IAP (radio). In this example, the IAP that is being enabled is **a1** (the first IAP in the summary list).


```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a1 up
Xirrus_Wi-Fi_Array(config-iap)# save
 Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                            Cell    TX      RX
IAP State Channel Antenna   Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- -------- ---------------------- -------- --- -------------------- ----------------------
-------------------
 a1   up     64   int-dir  max     20dBm  -90dBm      0     C-1 00:0f:7d:03:5e:10-11
 a2 down     48   int-dir  max     20dBm  -90dBm      0     C-2 00:0f:7d:03:5e:30-31
 a3 down    157   int-dir  max     20dBm  -90dBm      0     C-3 00:0f:7d:03:5e:40-41
 a4 down     60   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5e:50-51
 a5 down     44   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5e:70-71
 a6 down    153   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:80-81
 a7 down     56   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:90-91
 a8 down     40   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:b0-b1
 a9 down    149   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:c0-c1
a10 down     52   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:d0-d1
a11 down     36   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:f0-f1
a12 down    161   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5e:00-01
abg1 down    11   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5e:20-21
abg2 down monitor int-omni manual  20dBm  -95dBm      0         00:0f:7d:03:5e:60-61
abg3 down     6   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:a0-a1
abg4 down     1   int-dir  max     20dBm  -90dBm      0         00:0f:7d:03:5d:e0-e1

Xirrus_Wi-Fi_Array(config-iap)#
```

Figure 167. Enabling a Specific IAP

Disabling a Specific IAP

This example shows you how to disable a specific IAP (radio). In this example, the IAP that is being disabled is **a2** (the second IAP in the summary list).

Figure 168. Disabling a Specific IAP

Setting Cell Size Auto-Configuration for All IAPs

This example shows how to set the cell size for all enabled IAPs to be auto-configured (**auto**). (See "Fine Tuning Cell Sizes" on page 53.) The **auto_cell** option may be used with **global_settings**, **global_a_settings**, or **global_bg_settings**. It sets the cell size of the specified IAPs to **auto**, and it launches an auto-configuration to adjust the sizes. Be aware that if the **intrude-detect** feature is enabled on **abg(n)2,** its cell size is unaffected by this command. Also, any IAPs used in WDS links are unaffected.

Auto-configuration may be set to run periodically at intervals specified by **auto_cell period** (in seconds) if **period** is non-zero. The percentage of overlap allowed between cells in the cell size computation is specified by **auto_cell overlap** (0 to 100). This example sets auto-configuration to run every 1200 seconds with an allowed overlap of 5%. It sets the cell size of all IAPs to **auto**, and runs a cell size auto-configure operation which completes successfully.

```
192.168.39.125 - PuTTY
Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# auto_cell overlap 5
Xirrus-WiFi-Array(config-iap-global)# auto_cell period 1200
Xirrus-WiFi-Array(config-iap-global)# auto_cell
Auto cell size configuration completed successfully.

Xirrus-WiFi-Array(config-iap-global)# save
Xirrus-WiFi-Array(config-iap-global)# exit
Xirrus-WiFi-Array(config-iap)# show

IAP Summary Table
                         Cell   TX      RX
IAP State Channel Antenna Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- ------- ----  ----- --------- -------- --- -------------------- ----------------
   a1 down    36   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:10
   a2  up     36   int-dir  auto  -10dBm  -65dBm      0       00:0f:7d:03:c3:30
   a3  up    157   int-dir  auto  -10dBm  -65dBm      0       00:0f:7d:03:c3:40
   a4  up     56   int-dir  auto  -10dBm  -65dBm      0       00:0f:7d:03:c3:50
   a5 down    56   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:70
   a6 down   157   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:80
   a7 down    44   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:90
   a8 down    60   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:b0
   a9  up    153   int-dir  auto  -10dBm  -65dBm      0       00:0f:7d:03:c3:c0
  a10 down    48   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:d0
  a11 down    64   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:f0
  a12 down   161   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:00
 abg1 down     1   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:20
 abg2  up monitor int-omni manual 20dBm  -95dBm      0       00:0f:7d:03:c3:60
 abg3 down    11   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:a0
 abg4 down     6   int-dir  max    20dBm  -90dBm      0       00:0f:7d:03:c3:e0

Xirrus-WiFi-Array(config-iap)#
```

Figure 169. Setting the Cell Size for All IAPs

Setting the Cell Size for All IAPs

This example shows you how to establish the cell size for all IAPs (radios), regardless of the wireless technology they use. Be aware that if the **intrude-detect** feature is enabled on **abg(n)2** the cell size cannot be set globally—you must first disable the intrude-detect feature on **abg(n)2**.

In this example, the cell size is being set to **small** for all IAPs. You have the option of setting IAP cell sizes to small, medium, large, or max. See also, "Fine Tuning Cell Sizes" on page 53.

```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# cellsize small
 Xirrus_Wi-Fi_Array(config-iap-global)# save
 Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                          Cell    TX       RX
IAP State Channel Antenna  Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- -------- ---------------------- -------- --- -------------------- ----------------------
------------------
  a1  up      64   int-dir  small   5dBm  -75dBm      0    C-1 00:0f:7d:03:5e:10-11
  a2  up      48   int-dir  small   5dBm  -75dBm      0    C-2 00:0f:7d:03:5e:30-31
  a3  up     157   int-dir  small   5dBm  -75dBm      0    C-3 00:0f:7d:03:5e:40-41
  a4  up      60   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5e:50-51
  a5  up      44   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5e:70-71
  a6  up     153   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:80-81
  a7  up      56   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:90-91
  a8  up      40   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:b0-b1
  a9  up     149   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:c0-c1
 a10  up      52   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:d0-d1
 a11  up      36   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:f0-f1
 a12  up     161   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5e:00-01
abg1  up      11   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5e:20-21
abg2 down      1   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5e:60-61
abg3  up       6   int-dir  small   5dBm  -75dBm      0        00:0f:7d:03:5d:a0-a1
```

Figure 170. Setting the Cell Size for All IAPs

Setting the Cell Size for a Specific IAP

This example shows you how to establish the cell size for a specific IAP (radio). In this example, the cell size for **a2** is being set to **medium**. You have the option of setting IAP cell sizes to small, medium, large, or max (the default is max). See also, "Fine Tuning Cell Sizes" on page 53.

```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Running configuration has not been saved.

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a2
 Xirrus_Wi-Fi_Array(config-iap-a2)# cellsize medium
 Xirrus_Wi-Fi_Array(config-iap-a2)# save
 Xirrus_Wi-Fi_Array(config-iap-a2)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
                            Cell   TX      RX

IAP State Channel Antenna   Size  Power Threshold Stations WDS MAC address / BSSID  Description
--------- ------- -------- --------------------- -------- --- ------------------- -----------------------
-------------------
  a1  up     64   int-dir  max      20dBm  -90dBm      0   C-1 00:0f:7d:03:5e:10-11

  a2  up     48   int-dir  medium   11dBm  -81dBm      0   C-2 00:0f:7d:03:5e:30-31

  a3  up    157   int-dir  max      20dBm  -90dBm      0   C-3 00:0f:7d:03:5e:40-41

  a4  up     60   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5e:50-51

  a5  up     44   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5e:70-71

  a6  up    153   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:80-81

  a7  up     56   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:90-91

  a8  up     40   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:b0-b1

  a9  up    149   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:c0-c1

 a10  up     52   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:d0-d1

 a11  up     36   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:f0-f1

 a12  up    161   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5e:00-01

abg1  up     11   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5e:20-21

abg2 down     1   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5e:60-61

abg3  up      6   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:a0-a1

abg4  up      1   int-dir  max      20dBm  -90dBm      0       00:0f:7d:03:5d:e0-e1


Xirrus_Wi-Fi_Array(config-iap)# _
```

Figure 171. Setting the Cell Size for a Specific IAP

Configuring VLANs on an Open SSID

This example shows you how to configure VLANs on an Open SSID.

```
Xirrus Wi-Fi Array

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# vlan
Xirrus_Wi-Fi_Array(config-vlan)# add VLAN2301 number 2301 ip addr 192.168.39.100 mask 255.255.255.0 gateway
 Changing IP address to 192.168.39.100.
Do you want to proceed? [yes/no]: y
 Xirrus_Wi-Fi_Array(config-vlan)# show

VLAN Summary Table

VLAN Name                Number  Management   DHCP      IP Address      IP Mask         IP Gateway
--------------------------  ----------  --------  --------------  ---------------  ---------------
VLAN2301                   2301  disallowed  disabled  192.168.39.100  255.255.255.0    192.168.39.1

Default Route     VLAN: none
Native (untagged) VLAN: none

Xirrus_Wi-Fi_Array(config-vlan)# default-route 2301
 Xirrus_Wi-Fi_Array(config-vlan)# show

VLAN Summary Table

VLAN Name                Number  Management   DHCP      IP Address      IP Mask         IP Gateway
--------------------------  ----------  --------  --------------  ---------------  ---------------
VLAN2301                   2301  disallowed  disabled  192.168.39.100  255.255.255.0    192.168.39.1

Default Route     VLAN: "VLAN2301" / 2301
Native (untagged) VLAN: none

Xirrus_Wi-Fi_Array(config-vlan)# exit
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption none broadcast
 Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# vlan 2301
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
=================================================
State           Enabled
Active          Yes
Encryption      Global Open
VLAN Name       VLAN2301
VLAN Number     2301
QoS Level       2
Active Band     802.11a & 802.11bg
Broadcast       On
DHCP Pool       none
Traffic Limit   Unlimited
Traffic/Station Unlimited
Time on         Always
Time off        Never
Days on         All
Web Page Redirect   Disabled

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# save
 Xirrus_Wi-Fi_Array(config-ssid-Companyx)#
```

✎ *Setting the default route enables the Array to send management traffic, such as Syslog messages and SNMP information to a destination behind a router.*

Figure 172. Configuring VLANs on an Open SSID

Configuring Radio Assurance Mode (Loopback Tests)

The Array uses the built-in monitor radio, IAP abg(n)2, to monitor other radios in the Array. Tests include sending probes on all channels and checking for a response, and checking whether beacons are received from the other radio. If a problem is detected, corrective actions are taken to recover. Loopback mode operation is described in detail in "Array Monitor and Radio Assurance Capabilities" on page 406.

The following actions may be configured:

- **alert-only**—the Array will issue an alert in the Syslog.

- **repair-without-reboot**—the Array will issue an alert and reset radios at the Physical Layer (Layer 1) and possibly at the MAC layer. The reset should not be noticed by users, and they will not need to reassociate.

- **reboot-allowed**—the Array will issue an alert, reset the radios, and schedule the Array to reboot at midnight (per local Array time) if necessary. All stations will need to reassociate to the Array.

- **off**—Disable IAP loopback tests (no self-monitoring occurs). Radio Assurance mode is off by default.

This is a global IAPs setting—abg(n)2 will monitor all other radios according to the settings above, and it cannot be set up to monitor particular radios. Radio assurance mode requires Intrusion Detection to be set to Standard.

The following example shows you how to configure a loopback test.

```
192.168.39.125 - PuTTY

Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# intrude-detect standard
Interface IAP abg2 state changed to down
Interface IAP abg2 band changed to monitor
Interface IAP abg2 channel changed to monitor
Interface IAP abg2 antenna changed to internal omni
Interface IAP abg2 tx-power changed to 20
Interface IAP abg2 rx-threshold changed to -95
Interface IAP abg2 state changed to up

Xirrus-WiFi-Array(config-iap-global)# loopback-test
  alert-only              Enable  IAP loopback tests with failure alerts only
  off                     Disable IAP loopback tests
  reboot-allowed          Enable  IAP loopback tests with alerts & repairs & reboots if n
  repair-without-reboot   Enable  IAP loopback tests with alerts & repairs, but no reboots
  <cr>                    Set global IAP parameters

Xirrus-WiFi-Array(config-iap-global)# loopback-test repair-without-reboot
Xirrus-WiFi-Array(config-iap-global)#
Xirrus-WiFi-Array(config-iap-global)# show

Global IAP Settings Summary
---------------------------
Country code        not set (defaults to US: United States)
Beacon interval     100 Kusec
Broadcast rates     standard
DTIM period         1 beacon
Short retries       7
Long  retries       4
Total IAPs          16
Max stations/IAP    64
Max phones  /IAP    16
Station timeout     1000 sec
Station reauth time 5 sec
Management          disallowed
Station to station  forward
Load balancing      off
Intrusion detection standard
Auto chan power up  off
Auto chan schedule  none
Auto cell period    1200 sec
Auto cell overlap   5%
Xirrus Fast Roaming via tunnels to arrays in-range or targeted
Sharp cell TX power off
Public Safety Band  disabled
802.11h support     on
Loopback test mode  repair w/o reboot
LED activity        on when IAP up
                    blink on data frame transmitted
                    blink on data frame received
                    blink on management frame transmitted
                    blink on management frame received
                    blink heartbeat on station associated

Xirrus-WiFi-Array(config-iap-global)#
Do you want to save changes to flash [yes/no]: █
```

Figure 173. Configuring Radio Assurance Mode (Loopback Testing)

Appendices

Page is intentionally blank

Appendix A: Servicing the Wi-Fi Array

This appendix contains procedures for servicing the Xirrus Wi-Fi Array, including the removal and reinstallation of major hardware components. Topics include:

- **"Removing the Access Panel" on page 373**.
- **"Reinstalling the Access Panel" on page 376**.
- **"Replacing the FLASH Memory Module" on page 378**.
- **"Replacing the Main System Memory" on page 380**.
- **"Replacing the Integrated Access Point Radio Module" on page 382**.
- **"Replacing the Power Supply Module" on page 385**.

! *Always disconnect the power source from the Array before attempting to remove or replace components. Never work on the unit with the power connected.*

! *You must be grounded and the work surface must be static-free.*

! *Caution! The Array contains a battery which is not to be replaced by the customer. Danger of Explosion exists if the battery is incorrectly replaced.*

Power switch

AC power cord receptacle
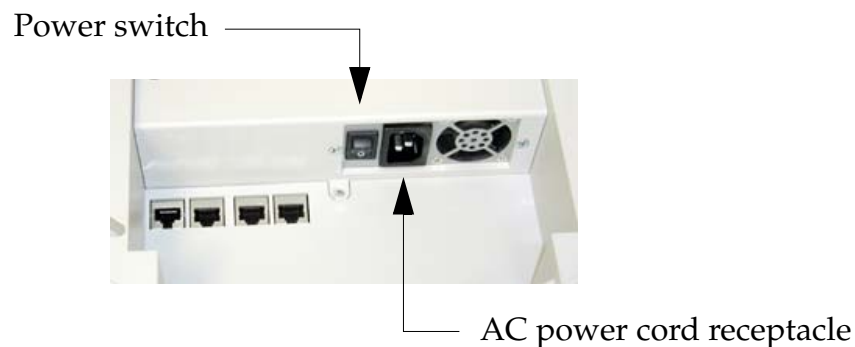
Figure 174. Disconnecting Power from the Array

✎ *Most service activities are performed with the Array placed face-down on a flat work surface. To avoid damaging the finished enclosure, we recommend using a protective material between the work surface and the unit (a clean sheet of paper will do the trick).*

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Removing the Access Panel

Use this procedure when you want to remove the system's access panel. You must remove this panel whenever you need to service the internal components of the Array.

1. Turn OFF the Array's main power switch (XS-3900 and XS-3700 only).

2. Disconnect the AC power cord or Ethernet cable supplying power from the Array.

3. Place the Array face-down on a flat surface. Avoid moving the unit to reduce the risk of damage (scratching) to the finished enclosure.

4. Remove the screws (3 places) that secure the access panel to the main body of the Array.
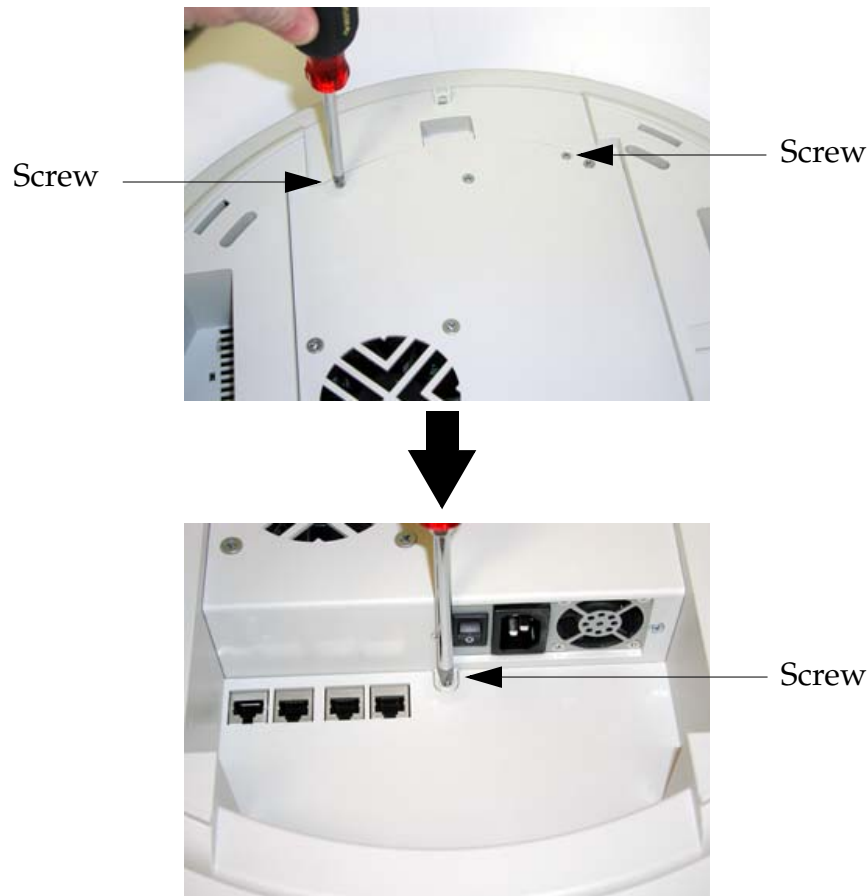
Figure 175. Removing the Access Panel Screws

5. Lift up the access panel to reveal the main system board.

Lift up the access panel

Figure 176. Removing the Access Panel

6. Disconnect the connectors to the power supply and the fan.

Fan connector   Power supply connector

Figure 177. Disconnecting the Power Supply and Fan

7. The access panel can now be safely removed.

See Also

Reinstalling the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Reinstalling the Access Panel

Use this procedure when you need to reinstall the access panel after servicing the Array's internal components.

1. Reconnect the fan and power supply.
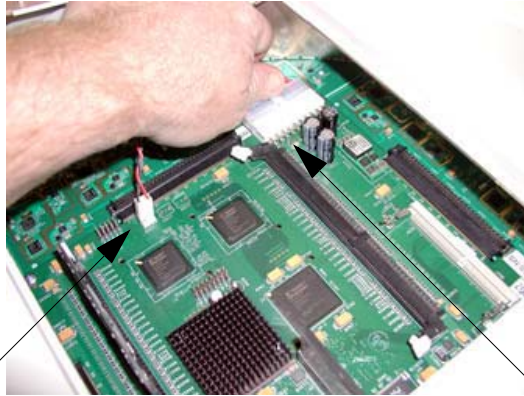
Fan connector   Power supply connector

Figure 178. Reconnecting the Fan and Power Supply

2. Reinstall the access panel and secure the panel with the three screws.

Screw
! Do not
   overtighten

Screw
! Do not
   overtighten

Screw
! Do not
   overtighten

Figure 179. Reinstalling the Access Panel

3. Reconnect the power source and turn ON the main power switch (if applicable).

See Also

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the FLASH Memory Module

Use this procedure when you want to replace the system's FLASH memory module.

1. Remove the system's access panel. Refer to "Removing the Access Panel" on page 373.

2. Remove the FLASH memory module, taking care not to "wiggle" the module and risk damaging the connection points.

FLASH memory module
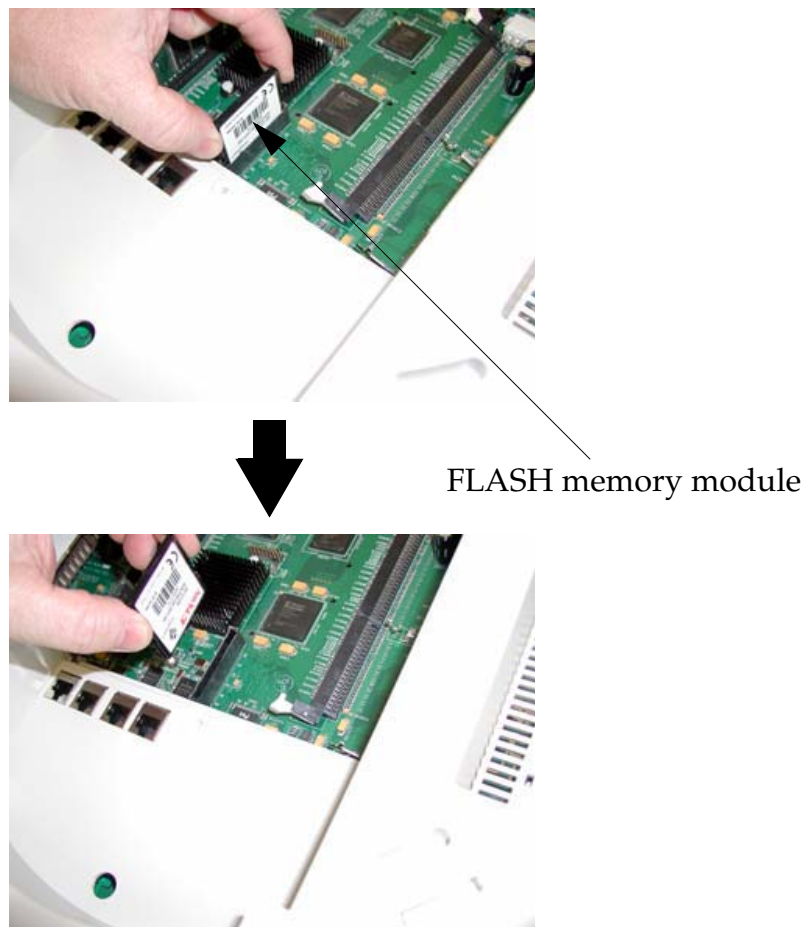
Figure 180. Removing the FLASH Memory Module

3. The removal procedure is complete. You can now reinstall the FLASH memory module (or install a new module).

4. Reinstall the access panel (refer to "Reinstalling the Access Panel" on page 376).

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the Main System Memory

Use this procedure when you want to replace the main system memory.

1. Remove the access panel (refer to "Removing the Access Panel" on page 373).

2. Remove the DIMM memory module, taking care not to "wiggle" the module and risk damaging the connection points.

DIMM memory module

Push down on the two locking tabs to release the DIMM memory module
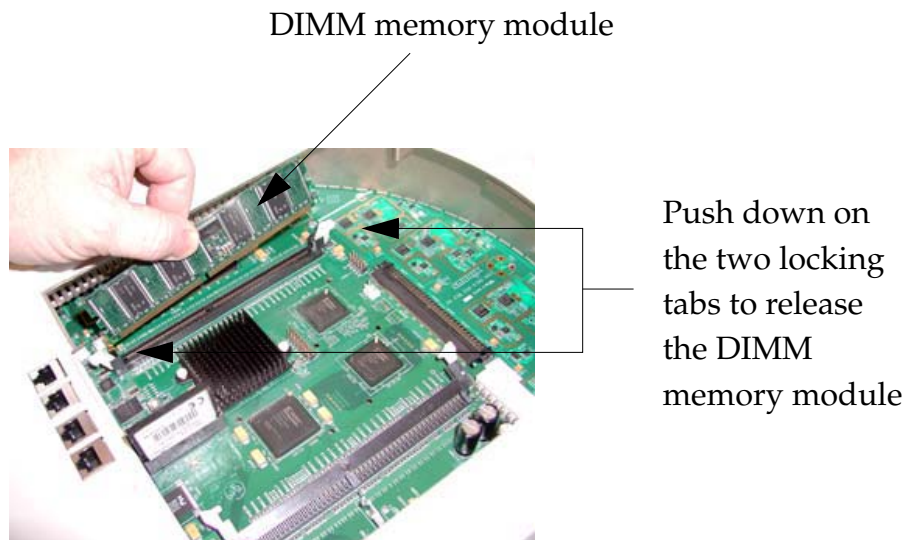
Figure 181. Removing the DIMM Memory Module

3. The removal procedure is complete. You can now reinstall the DIMM memory module (or install a new module). Ensure that the DIMM memory module is seated evenly and the locking tabs are in the upright position. The DIMM memory module is keyed to fit in its socket in one direction only.

4. Reinstall the access panel (refer to "Reinstalling the Access Panel" on page 376).

See Also

Reinstalling the Access Panel
Removing the Access Panel
Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the Integrated Access Point Radio Module

Use this procedure when you want to replace the integrated access point radio module.

1. Remove the access panel (refer to "Removing the Access Panel" on page 373).

2. Remove the locking screws (8 places) that secure the chassis cover to the main body of the Wi-Fi Array.

Screws (8 places)

Figure 182. Removing the Chassis Cover Screws

3. Lift and remove the chassis cover.
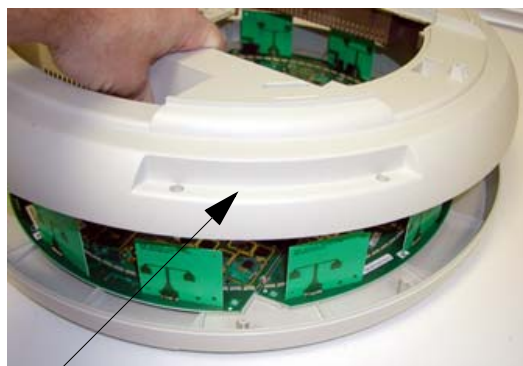
Remove the chassis cover

Figure 183. Removing the Chassis Cover

4. Lift the edge of the integrated access point module.
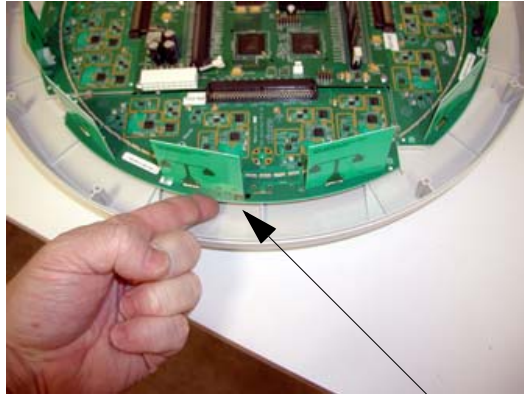
Lift here (do not force)

Figure 184. Lifting the Integrated Access Point Module

5. Slide the integrated access point module away from the unit to disconnect it from the main system board.
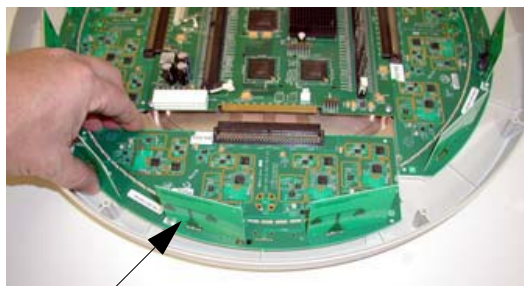
Disconnect the module

Figure 185. Disconnect the Integrated Access Point Module

6. The removal procedure is complete. You can now reinstall the integrated access point module (or install a new module).

7. Reinstall the chassis cover (see warnings).

> **!** *When reinstalling the chassis cover, take care to align the cover correctly to avoid damaging the antenna modules. Do not force the chassis cover onto the body of the unit.*

> **!** *Do not overtighten the locking screws.*

8. Reinstall the locking screws (8 places) to secure the chassis cover in place—do not overtighten.

9. Reinstall the access panel (refer to "Reinstalling the Access Panel" on page 376).

See Also

Reinstalling the Access Panel
Removing the Access Panel
Replacing the FLASH Memory Module
Replacing the Main System Memory
Replacing the Power Supply Module
Appendix A: Servicing the Wi-Fi Array

Replacing the Power Supply Module

Use this procedure when you want to replace the power supply module.

1. Remove the access panel (refer to "Removing the Access Panel" on page 373).

2. Because the power supply unit is molded into the access panel, you must install a new access panel assembly (with the power supply attached). Refer to "Reinstalling the Access Panel" on page 376.

Access panel (with power supply and fan)

Figure 186. Installing a New Access Panel (with Power Supply)

See Also

Reinstalling the Access Panel
Removing the Access Panel
Replacing the FLASH Memory Module
Replacing the Integrated Access Point Radio Module
Replacing the Main System Memory
Appendix A: Servicing the Wi-Fi Array

Use this Space for Your Notes

Appendix A: Servicing the Wi-Fi Array

Appendix B: Quick Reference Guide

This section contains product reference information. Use this section to locate the information you need quickly and efficiently. Topics include:

- **"Factory Default Settings" on page 387**.
- **"Keyboard Shortcuts" on page 394**.

Factory Default Settings

The following tables show the Wi-Fi Array's factory default settings.

Host Name

Setting	Default Value
Host name	Xirrus-WiFi-Array

Network Interfaces

Serial

Setting	Default Value
Baud Rate	115200
Word Size	8 bits
Stop Bits	1
Parity	No parity
Time Out	10 seconds

Gigabit 1 and Gigabit 2

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.2.1
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1504
Management Enabled	Yes

Fast Ethernet

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.1.1
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	100 Mbps

Setting	Default Value
MTU Size	1500
Management Enabled	Yes

Integrated Access Points (IAPs)

Setting	Default Value
IAP abg2 Defaults	Enabled Mode = Monitor Channel = Monitor Cell Size = Manual Antenna = Internal-Omni
Enabled (Radio State)	No
Mode ● XS16, XS-3900	802.11a for a1 to a12 802.11bg for abg1 to abg4
● XS12	802.11a for a1 to a8 802.11bg for abg1 to abg4
● XS8, XS-3700	802.11a for a1 to a4 802.11bg for abg1 to abg4
● XS4, XS-3500	802.11bg for abg1 to abg4
Channel	Auto
Cell Size	Max
Maximum Transmit Power	20
Antenna Selected	Internal

Server Settings

NTP

Setting	Default Value
Enabled	No
Primary	time.nist.gov
Secondary	pool.ntp.org

Syslog

Setting	Default Value
Enabled	Yes
Local Syslog Level	Information
Maximum Internal Records	500
Primary Server	None
Primary Syslog Level	Information
Secondary Server	None
Secondary Syslog Level	Information

SNMP

Setting	Default Value
Enabled	Yes
Read-Only Community String	xirrus_read_only
Read-Write Community String	xirrus
Trap Host	null (no setting)

Setting	Default Value
Trap Port	162
Authorization Fail Port	On

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes
IP Start Range	192.168.1.2
IP End Range	192.168.1.254
NAT	Disabled
IP Gateway	None
DNS Domain	None
DNS Server (1 to 3)	None

Default SSID

Setting	Default Value
ID	xirrus
VLAN	None
Encryption	Off
Encryption Type	None
QoS	2
Enabled	Yes

Setting	Default Value
Broadcast	On

Security

Global Settings - Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)
WEP Key Length	null (all 4 keys)
Default Key ID	1
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	Yes
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	Disabled

External RADIUS (Global)

Setting	Default Value
Enabled	Yes
Primary Server	None
Primary Port	1812

Setting	Default Value
Primary Secret	xirrus
Secondary Server	null (no IP address)
Secondary Port	1812
Secondary Secret	null (no secret)
Time Out (before primary server is retired)	600 seconds
Accounting	Disabled
Interval	300 seconds
Primary Server	None
Primary Port	1813
Primary Secret	xirrus
Secondary Server	None
Secondary Port	1813
Secondary Secret	null (no secret)

Internal RADIUS

Setting	Default Value
Enabled	No
The user database is cleared upon reset to the factory defaults. For the Internal RADIUS Server you have a maximum of 1,000 entries.	

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
SSH	On
SSH timeout	300 seconds
Telnet	Off
Telnet timeout	300 seconds
Serial	On
Serial timeout	300 seconds
Management over IAPs	Off
http timeout	300 seconds

Keyboard Shortcuts

The following table shows the most common keyboard shortcuts used by the Command Line Interface.

Action	Shortcut
Cut selected data and place it on the clipboard.	**Ctrl + X**
Copy selected data to the clipboard.	**Ctrl + C**

Action	Shortcut
Paste data from the clipboard into a document (at the insertion point).	**Ctrl + V**
Go to top of screen.	**Ctrl + Z**
Copy the active window to the clipboard.	**Alt + Print Screen**
Copy the entire desktop image to the clipboard.	**Print Screen**
Abort an action at any time.	**Esc**
Go back to the previous screen.	**b**
Access the Help screen.	**?**

See Also

An Overview

Use this Space for Your Notes

Appendix C: Technical Support

This appendix provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all topics below and try to determine if your problem resides with the Wi-Fi Array or your network infrastructure. Topics include:

- **"General Hints and Tips" on page 397**
- **"Frequently Asked Questions" on page 398**
- **"Array Monitor and Radio Assurance Capabilities" on page 406**
- **"Upgrading the Array via CLI" on page 409**
- **"Power over Gigabit Ethernet Compatibility Matrix" on page 414**
- **"Contact Information" on page 417**

General Hints and Tips

This section provides some useful tips that will optimize the reliability and performance of your Wi-Fi Arrays.

- The Wi-Fi Array requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.

- If using multiple Arrays in the same area, maintain a distance of at least 100 feet (30m) between Arrays if there is direct line-of-sight between the units, or at least 50 feet (15 m) if a wall or other barrier exists between the units.

- Keep the Wi-Fi Array away from electrical devices or appliances that generate RF noise. Because the Array is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).

- If using AC power, each Wi-Fi Array requires its own dedicated AC power outlet. Do not attempt to "piggy-back" AC power to multiple units. To avoid needing to run separate power cables to one or more Arrays, consider using Power over Gigabit Ethernet.

- If you are deploying multiple units, the Array should be oriented so that the **abg(n)2** radio is oriented in the direction of the least required coverage, because when in monitor mode the abg(n)2 radio does not function as an AP servicing stations.

- The Wi-Fi Array should only be used with Wi-Fi certified client devices.

See Also

Contact Information
Multiple SSIDs
Security
VLAN Support

Frequently Asked Questions

This section answers some of the most frequently asked questions, organized by functional area.

Multiple SSIDs

Q. **What Are BSSIDs and SSIDs?**

A. BSSID (Basic Service Set Identifier) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS.

A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS by way of a backbone that interconnects each access point.

The Extended Service Set (ESS) refers to the group of BSSIDs that are grouped together to form one ESS. The ESSID (often referred to as SSID or "wireless network name") identifies the Extended Service Set. Clients must associate to a single ESS at any given time. Clients ignore traffic from other Extended Service Sets that do not have the same SSID.

Legacy access points typically support one SSID per access point. Xirrus Wi-Fi Arrays support the ability for multiple SSIDs to be defined and used simultaneously.

Q. What would I use SSIDs for?

A. The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:

- Minimum security required to join this SSID.

- The wireless Quality of Service (QoS) desired for this SSID.

- The wired VLAN associated with this SSID.

As an example, one SSID named **accounting** might require the highest level of security, while another SSID named **guests** might have low security requirements.

Another example may define an SSID named **voice** that supports voice over Wireless LAN phones with the highest possible Quality of Service (QoS) definition. This type of SSID might also forward traffic to specific VLANs on the wired network.

Q. How do I set up SSIDs?

A. Use the following procedure as a guideline. For more detailed information, go to "SSIDs" on page 235.

1. From the Web Management Interface, go to the SSID Management page.

2. Select **Yes** to make the SSID visible to all clients on the network. Although the Wi-Fi 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.

3. Select the minimum security that will be required by users for this SSID.

4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.

5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.

6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.

7. Click on the **Apply** button to apply your changes to this session.

8. Click on the **Save** button to save your changes.

9. If you need to edit any of the SSID settings, you can do so from the SSID Management page.

See Also

Contact Information
General Hints and Tips
Security
SSIDs
SSID Management
VLAN Support

Security

Q. **How do I ensure that an Array meets FIPS requirements?**

A. To meet the Level 2 security requirements of FIPS 140-2, follow the instructions in Appendix E: Implementing FIPS Security.

Q. **How do I ensure that an Array meets PCI DSS requirements?**

A. To meet PCI DSS requirements, follow the instructions in Appendix D: Implementing PCI DSS.

Q. **How do I know my management session is secure?**

A. Follow these guidelines:

● Administrator passwords
Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.

● SSH versus Telnet

Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY. The Array only allows SSH-2 connections, so your SSH utility must be set up to use SSH-2.

- Configuration auditing

  Do not change approved configuration settings. The optional Xirrus Management System (XMS) offers powerful management features for small or large Wi-Fi Array deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.

Q. **Which wireless data encryption method should I use?**

A. Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The Wi-Fi Array allows you to establish the following data encryption configuration options:

- Open

  This option offers no data encryption and is **not recommended**, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.

- WEP (Wired Equivalent Privacy)

  This option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.

- WPA (Wi-Fi Protected Access)

  This is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

TKIP solves security issues with WEP. It also allows you to establish encryption keys on a per-user-basis, with key rotation for added security. In addition, TKIP provides Message Integrity Check (MIC) functionality and prevents active attacks on the wireless network.

AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, it is highly recommended for Enterprise networks.

Any of the above encryption modes can be used (and can be used at the same time).

Q. **Which user authentication method should I use?**

A. User authentication ensures that users are who they say they are. For example, the most obvious example of authentication is logging in with a user name and password. The Wi-Fi Array allows you to choose between the following user authentication methods:

- Pre-Shared Key
  Users must manually enter a key (pass phrase) on the client side of the wireless network that matches the key stored by the administrator in your Wi-Fi Arrays.

- RADIUS 802.1x with EAP
  802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal (provided by the Wi-Fi Array) or external. An external RADIUS server offers more functionality and is **recommended** for large Enterprise deployments.

  When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

- <u>MAC Address ACLs (Access Control Lists)</u>
  MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC addresses of each user in the **Allow** list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the **Deny** list.

Q. **Why do I need to authenticate my Wi-Fi Array units?**

A. When deploying multiple Wi-Fi Arrays, you may need to define which units are part of which wireless network (for example, if you are establishing more than one network). In this case, you need to employ the Xirrus Management System (XMS) which can authenticate your Arrays automatically and ensure that only authorized units are associated with the defined wireless network.

Q. **What is rogue AP (Access Point) detection?**

A. The Wi-Fi Array has a dedicated radio, IAP abg(n)2, which constantly scans the local wireless environment for rogue APs (non-Xirrus devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

See Also
Contact Information
General Hints and Tips
Multiple SSIDs
VLAN Support

VLAN Support

Q. **What Are VLANs?**

A. VLANs (Virtual Local Area Networks) are a logical grouping of network devices that share a common network broadcast domain. Members of a

particular VLAN can be on any segment of the physical network but logically only members of a particular VLAN can see each other.

VLANs are defined and implemented using the wired network switches that are VLAN capable. Packets are tagged for transmission on a particular VLAN according to the IEEE 802.1Q standard, with VLAN switches processing packets according to the tag.

Q. What would I use VLANs for?

A. Logically separating different types of users, systems, applications, or other logical division aids in performance and management of different network devices. Different VLANs can also be assigned with different packet priorities to prioritize packets from one VLAN over packets from another VLAN.

VLANs are managed by software settings—instead of physically plugging in and moving network cables and users—which helps to ease network management tasks.

Q. What are Wireless VLANs?

A. Wireless VLANs allow similar functionality to the wired VLAN definitions and extend the operation of wired VLANs to the wireless side of the network.

Wireless VLANs can be mapped to wireless SSIDs so that traffic from wired VLANs can be sent to wireless users of a particular SSID. The reverse is also true, where wireless traffic originating from a particular SSID can be tagged for transmission on a particular wired VLAN.

Sixteen SSIDs can be defined on your Wi-Fi Array, allowing a total of sixteen VLANs to be accessed (one per SSID).

As an example, to provide guest user access an SSID of **guest** might be created. This SSID could be mapped to a wired VLAN that segregates unknown users from the rest of the wired network and restricts them to Internet access only. Wireless users could then associate to the wireless network via the **guest** SSID and obtain access to the Internet through the

selected VLAN, but would be able to access other privileged network resources.

See Also

Contact Information
General Hints and Tips
Multiple SSIDs
Security

Array Monitor and Radio Assurance Capabilities

All models of the Wi-Fi Array have a monitor radio, **abg(n)2,** that checks that the Array's radios are functioning correctly, and acts as a dedicated threat sensor to detect and prevent intrusion from rogue access points.

Enabling Monitoring on the Array

IAP abg(n)2 may be set to monitor the Array or to be a normal IAP radio. In order to enable the functions required for intrusion detection and for monitoring the other Array radios, you **must** configure abg(n)2 on the IAP Settings window as follows:

- Check the **Enabled** checkbox.
- Set **Mode** to **Monitor**.
- Set **Channel** to **Monitor**.

The settings above will automatically set the **Antenna** selection to **Internal-Omni**., also required for monitoring. See the "IAP Settings" on page 255 for more details. The values above are the factory default settings for the Array.

How Monitoring Works

When the monitor radio abg(n)2 has been configured as just described, it performs these steps continuously (24/7) to check the other radios on the Array and detect possible intrusions:

1. The monitor radio scans all channels with a 200ms dwell time, hitting all channels about once every 10 seconds.

2. Each time it tunes to a new channel it sends out a probe request in an attempt to smoke out rogues.

3. It then listens for all probe responses and beacons to detect any rogues within earshot.

4. Array radios respond to that probe request with a probe response.

Intrusion Detection is enabled or disabled separately from monitoring. See Step 1 in "Advanced RF Settings" on page 275. Note that the **Advanced** setting is only used with the optional Xirrus Defense Module (XDM) software package.

XIRRUS®

Radio Assurance

The Array is capable of performing continuous, comprehensive tests on its radios to assure that they are operating properly. Testing is enabled using the **Radio Assurance Mode** setting on the Advanced RF Settings window (Step 5 in "Advanced RF Settings" on page 275). When this mode is enabled, IAP abg(n)2 performs loopback tests on the Array. Radio Assurance Mode requires **Intrusion Detection** to be set to **Standard** (See Step 1 in "Advanced RF Settings" on page 275).

When **Radio Assurance Mode** is enabled:

1. The Array keeps track of whether or not it hears beacons and probe responses from the Array's radios.

2. After 10 minutes (roughly 60 passes on a particular channel by the monitor radio), if it has not heard beacons or probe responses from one of the Array's radios it issues an alert in the Syslog. If repair is allowed (see "Radio Assurance Options" on page 408), the Array will reset and reprogram that particular radio at the Physical Layer (PHY—Layer 1). This action takes under 100ms and stations are not deauthenticated, thus users should not be impacted.

3. After another 10 minutes (roughly another 60 passes), if the monitor still has not heard beacons or probe responses from the malfunctioning radio it will again issue an alert in the Syslog. If repair is allowed, the Array will reset and reprogram the MAC (the lower sublayer of the Data Link Layer) and then all of the PHYs. This is a global action that affects all radios. This action takes roughly 300ms and stations are not deauthenticated, thus users should not be impacted.

4. After another 10 minutes, if the monitor still has not heard beacons or probe responses from that radio, it will again syslog the issue. If reboot is allowed (see "Radio Assurance Options" on page 408), the Array will schedule a reboot. This reboot will occur at one of the following times, whichever occurs first:

   • When no stations are associated to the Array

   • Midnight

Radio Assurance Options

If the monitor detects a problem with an Array radio as described above, it will take action according to the preference that you have specified in the **Radio Assurance Mode** setting on the Advanced RF Settings window (see Step 5 page 278):

- **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 the PHY and MAC as described above.

- **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets of the PHY and MAC, and schedule reboots as described above.

- **Disabled**—Disable IAP loopback tests (no self-monitoring occurs). Loopback tests are disabled by default.

Upgrading the Array via CLI

If you are experiencing difficulties communicating with the Array using the Web Management Interface, the Array provides lower-level facilities that may be used to accomplish an upgrade via the CLI and the Xirrus Boot Loader (XBL).

1. Download the latest software update from the Xirrus FTP site using your Enhanced Care FTP username and password. If you do not have an FTP username and password, contact Xirrus Customer Service for assistance (support@xirrus.com). The software update is provided as a zip file. Unzip the contents to a local temp directory. Take note of the extracted file name in case you need it later on—you may also need to copy this file elsewhere on the network depending on your situation.

2. Install a TFTP server software package if you don't have one running. It may be installed on any PC on your network, including your desktop or laptop. The Solar Winds version is freeware and works well.

   http://support.solarwinds.net/updates/New-customerFree.cfm?ProdId=52

   The TFTP install process creates the **TFTP-Root** directory on your C: drive, which is the default target for sending and receiving files. This may be changed if desired. This directory is where you will place the extracted Xirrus software update file(s). If you install the TFTP server on the same computer to which you extracted the file, you may change the TFTP directory to C:\xirrus if desired.

   You must make the following change to the default configuration of the Solar Winds TFTP server. In the **File/Configure** menu, select **Security**, then select **Transmit onl**y and click **OK**.

3. Determine the IP address of the computer hosting the TFTP server. (To display the IP address, open a command prompt and type **ipconfig**)

4. Connect your Array to the computer running TFTP using a serial cable, and open a terminal program if you haven't already. Attach a network cable to the Array's GIG1 port, if it is not already part of your network.

Boot your Array and watch the progress messages. When **Press space bar to exit to bootloader:** is displayed, press the space bar. The rest of this procedure is performed using the bootloader.

The following steps assume that you are running DHCP on your local network.

5. Type **dhcp** and hit return. This instructs the Array to obtain a DHCP address and use it during this boot in the bootloader environment.

6. Type **dir** and hit return to see what's currently in the compact flash.

7. Type **del** and hit return to delete the contents of the compact flash.

8. Type **update server <TFTP-server-ip-addr> xs-3.x-xxxx.bin** (the actual Xirrus file name will vary depending on Array model number and software version—use the file name from your software update) and hit return. The software update will be transferred to the Array's memory and will be written to the it's compact flash card. (See output below.)

9. Type **reset** and hit return. Your Array will reboot, running your new version of software.

Sample Output for the Upgrade Procedure:

The user actions are highlighted in the output below, for clarity.

> Username: **admin**
> Password: *****
>
> Xirrus-WiFi-Array# **configure**
> Xirrus-WiFi-Array(config)# **reboot**
> Are you sure you want to reboot? [yes/no]: **yes**
> Array is being rebooted.
>
>
> Xirrus Boot Loader 1.0.0 (Oct 17 2006 - 13:11:42), Build: 2725
>
> Processor | Motorola PowerPC, PVR=80200020 SVR=80300020
> Board | Xirrus MPC8540 CPU Board
> Clocks | CPU : 825 MHz   DDR : 330 MHz   Local Bus: 41 MHz

```
L1 cache   | Data: 32 KB   Inst: 32 KB   Status  : Enabled
Watchdog   | Enabled (5 secs)
I2C Bus    | 400 KHz
DTT        | CPU:34C  RF0:34C  RF1:34C  RF2:27C  RF3:29C
RTC        | Wed 2007-Nov-05  6:43:14 GMT
System DDR | 256 MB, Unbuffered Non-ECC (2T)
L2 cache   | 256 KB, Enabled
FLASH      |   4 MB, CRC: OK
FPGA       |   2 Devices programmed
Packet DDR | 256 MB, Unbuffered Non-ECC, Enabled
Network    | Mot FEC   Mot TSEC1 [Primary]  Mot TSEC2
IDE Bus 0  | OK
CFCard     | 122 MB, Model: Hitachi XXM2.3.0
Environment|   4 KB, Initialized


In:    serial
Out:   serial
Err:   serial
```

Press space bar to exit to bootloader:

```
XBL>dhcp
[DHCP  ] Device  : Mot TSEC1 1000BT Full Duplex
[DHCP  ] IP Addr : 192.168.39.195
XBL>dir


[CFCard] Directory of /

   Date      Time     Size     File or Directory name
----------- -------- --------  ---------------------------
2007-Nov-05  6:01:56       29   lastboot
2007-Apr-05 15:47:46  28210390   xs-3.1-0433.bak
2007-Mar-01 16:39:42            storage/
2007-Apr-05 15:56:38  28210430   xs-3.1-0440.bin
2007-Mar-03  0:56:28            wpr/


3 file(s), 2 dir(s)
```

XBL>**del** *

 [CFCard] Delete : 2 file(s) deleted

XBL>**update server 192.168.39.102 xs-3.0-0425.bin**

[TFTP] Device : Mot TSEC1 1000BT Full Duplex
[TFTP] Client : 192.168.39.195
[TFTP] Server : 192.168.39.102
[TFTP] File   : xs-3.0-0425.bin
[TFTP] Address : 0x1000000
[TFTP] Loading : ##
[TFTP] Loading : ##
[TFTP] Loading : ###### done
[TFTP] Complete: 12.9 sec, 2.1 MB/sec
[TFTP] Bytes   : 27752465 (1a77811 hex)
[CFCard] File   : xs-3.0-0425.bin
[CFCard] Address : 0x1000000
[CFCard] Saving : ### done
[CFCard] Complete: 137.4 sec, 197.2 KB/sec
[CFCard] Bytes   : 27752465 (1a77811 hex)

XBL>**reset**
[RESET]

Xirrus Boot Loader 1.0.0 (Oct 17 2006 - 13:11:42), Build: 2725

Processor | Motorola PowerPC, PVR=80200020 SVR=80300020
Board | Xirrus MPC8540 CPU Board
Clocks | CPU : 825 MHz   DDR : 330 MHz   Local Bus: 41 MHz
L1 cache | Data: 32 KB   Inst: 32 KB   Status : Enabled
Watchdog | Enabled (5 secs)
I2C Bus | 400 KHz
DTT | CPU:33C RF0:32C RF1:31C RF2:26C RF3:27C
RTC | Wed 2007-Nov-05 6:48:44 GMT
System DDR | 256 MB, Unbuffered Non-ECC (2T)

```
L2 cache   | 256 KB, Enabled
FLASH      |   4 MB, CRC: OK
FPGA       |   2 Devices programmed
Packet DDR | 256 MB, Unbuffered Non-ECC, Enabled
Network    | Mot FEC    Mot TSEC1 [Primary]  Mot TSEC2
IDE Bus 0  | OK
CFCard     | 122 MB, Model: Hitachi XXM2.3.0
Environment|   4 KB, Initialized


In:    serial
Out:   serial
Err:   serial


Press space bar to exit to bootloader:


[CFCard] File    : xs*.bin
[CFCard] Address : 0x1000000
[CFCard] Loading : ############################################### done
[CFCard] Complete: 26.9 sec, 1.0 MB/sec
[CFCard] Bytes   : 27752465 (1a77811 hex)
[Boot  ] Address : 0x01000000
[Boot  ] Image   : Verifying checksum .... OK
[Boot  ] Unzip   : Multi-File Image   .... OK
[Boot  ] Initrd  : Loading RAMDisk Image
[Boot  ] Initrd  : Verifying checksum .... OK
[Boot  ] Execute : Transferring control to OS


Initializing hardware ....................................... OK



Xirrus Wi-Fi Array
ArrayOS Version 3.0-425
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com


Username:
```

Power over Gigabit Ethernet Compatibility Matrix

The Xirrus Power over Gigabit Ethernet (PoGE) solution includes different modules to be used with particular Array models. The following two tables indicate the proper PoGE injector/splitters to use with each Array. **X** indicates products are INCOMPATIBLE. NA=Not Applicable.

Table 1: Current PoGE Injectors/Splitters

Array Model	Compatible Xirrus Injector/Splitter	XP1-MSI-X Injector	XP8-MSI Injector	XP1-MSI Injector	XP1-SPL Splitter
XS4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS8, XN4	Works with any PoGE injector, no splitter required	✓	✓	✓	NA
XN16/XN12/ XN8/XN4, XS16/XS12	Works with two injector options, no splitter required	✓	✓ [1]	X	NA
XS-3500-4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS-3700-8, DC (modified)[2]	Works only with legacy injector/splitter models, see Table 2.	X	X	X	X
XS-3900-16, DC (modified)[2]		X	X	X	X
XS-3700-8, DC (unmodified)	**DO NOT** connect unmodified XS-3700/3900 with -H or -HX injectors or splitter.	X	✓	✓	✓
XS-3900-16, DC (unmodified)		X	✓ [1]	✓	✓

1. The 8-port XP8-MSI-H and XP8-MSI injectors each power up to eight 4-port or 8-port Arrays; or four 16-port Arrays.
2. To see whether an Array is modified, see Figure 188 on page 416.

✍ *IMPORTANT NOTE: Only use -H versions of injectors/splitters together, and use non-H versions of injectors/splitters together - do not mix or match the two types.*

Table 2: Legacy PoGE Models

Array Model	Compatible Xirrus Injector/Splitter	XP1-MSI-H Injector	XP1-MSI-HX Injector	XP8-MSI-H Injector	XP1-SPL-H Splitter
XS4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS8	Works with any PoGE injector, no splitter required	✓	✓	✓	NA
XS16/XS12	Works with two injector options, no splitter required	X	✓	✓ [1]	NA
XS-3500-4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS-3700-8, DC (modified)[2]	Works only with -H version injector/splitters	✓	✓	✓	✓
XS-3900-16, DC (modified)[2]	Works only with -HX or XP8 version injector/splitters	X	✓	✓ [1]	✓
XS-3700-8, DC (unmodified)	**DO NOT** connect unmodified XS-3700/3900 with -H or -HX injectors or splitter.	X	X	X	X
XS-3900-16, DC (unmodified)		X	X	X	X

1. The 8-port XP8-MSI-H and XP8-MSI injectors each power up to eight 4-port or 8-port Arrays; or four 16-port Arrays.
2. To see whether an Array is modified, see Figure 188 on page 416.

Determining If an XS-3700 or XS-3900 is Modified for PoGE

The following pictures show how different Array power supply types look. On the XS-3700/XS-3900 Arrays, it is VERY important to note the yellow sticker (Figure 188 on page 416) that differentiates between modified and unmodified DC power versions.

**Connect Data OUT
to Gig1 or Gig2 port
with short cable**

**Connect Cat 5e
(from PoGE Injector)
to IN port**
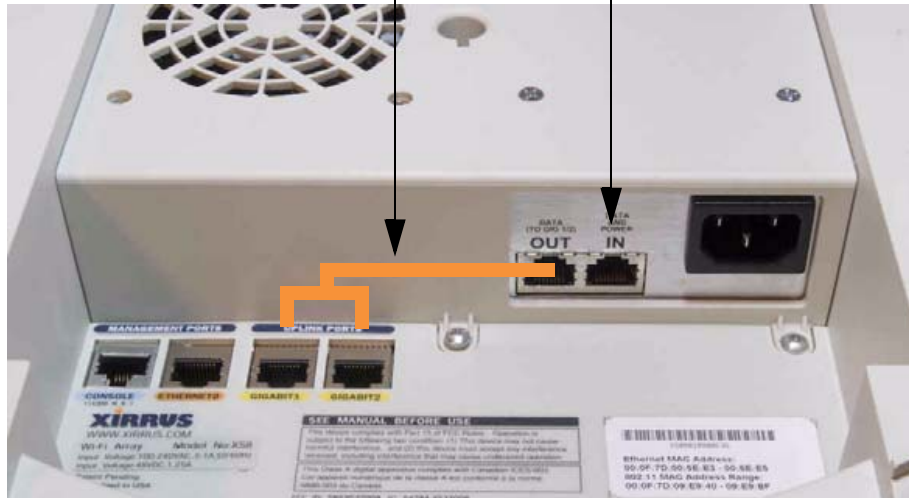
Figure 187. XN8/XN12/XN16/XS8/XS12/XS16: Integrated Splitter

Modified **XS-3700/XS-3900
(DC Version)
Accepts XP1-SPL-H splitter output
Must have *yellow label***

Unmodified **XS-3700/XS-3900
(DC Version)
Accepts XP1-SPL splitter output
Has no yellow label**

Figure 188. Determining if XS-37000/3900 is modified

Contact Information

Xirrus, Inc. is located in Thousand Oaks, California, just 55 minutes northwest of downtown Los Angeles and 40 minutes southeast of Santa Barbara.

Xirrus, Inc.
2101 Corporate Center Drive
Thousand Oaks, CA 91320
USA

Tel: 1.805.262.1600
        1.800.947.7871 Toll Free in the US
Fax: 1.866.462.3980

www.xirrus.com
support.xirrus.com

Appendix D: Implementing PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by major credit card companies to help those that process credit card transactions (or cardholder information) in order to secure cardholder information and protect it from unauthorized access, fraud and other security issues. The major contributors to the standard are VISA, MasterCard, American Express, JCB, and Discover. The standard also helps consolidate various individual standards that were developed by each of the listed card companies. Merchants or others who process credit card transactions are required to comply with the standard and to prove their compliance by way of an audit from a Qualified Security Assessor.

PCI DSS lays out a set of requirements that must be met in order to provide adequate security for sensitive data.

Payment Card Industry Data Security Standard Overview

The PCI Data Security Standard (PCI DSS) has 12 main requirements that are grouped into six *control objectives*. The following table lists each control objective and the specific requirements for each objective. For the latest updates to this list, check the PCI Security Standards Web site: www.pcisecuritystandards.org.

PCI DSS Control Objectives and Associated Requirements
Objective: Build and Maintain a Secure Network
● Requirement 1: Install and maintain a firewall configuration to protect cardholder data. ● Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
Objective: Protect Cardholder Data
● Requirement 3: Protect stored cardholder data. ● Requirement 4: Encrypt transmission of cardholder data across open, public networks.

PCI DSS Control Objectives and Associated Requirements
Objective: Maintain a Vulnerability Management Program   ● Requirement 5: Use and regularly update anti-virus software.   ● Requirement 6: Develop and maintain secure systems and applications.
Objective: Implement Strong Access Control Measures   ● Requirement 7: Restrict access to cardholder data by business need-to-know.   ● Requirement 8: Assign a unique ID to each person with computer access.   ● Requirement 9: Restrict physical access to cardholder data.
Objective: Regularly Monitor and Test Networks   ● Requirement 10: Track and monitor all access to network resources and cardholder data.   ● Requirement 11: Regularly test security systems and processes.
Objective: Maintain an Information Security Policy   ● Requirement 12: Maintain a policy that addresses information security.

PCI DSS and Wireless

The Xirrus Wi-Fi Array provides numerous security features that allow it to be a component of a PCI DSS-compliant network. The following sections indicate the specific features that allow the Xirrus Wi-Fi Array to operate in a PCI DSS mode.

The Xirrus Array PCI Compliance Configuration

The check list below is designed to help ensure that Xirrus Wi-Fi Arrays are configured in a manner that is supportive of PCI Data Security Standards. Detailed configuration steps for each item are found in the referenced section of the User's Guide.

✔	Xirrus Wi-Fi Array Configuration for PCI DSS	See...
( ) ( )	Register at the Xirrus Support Site to ensure notification and access to software updates. Confirm that the latest version of the Array OS is being used by checking the Xirrus web site.	support.xirrus.com
( )	Enable PCI Mode after configuring the Array in a PCI compliant state to ensure configuration changes cannot be saved that would invalidate a PCI compliant configuration. This item is covered on the following pages.	The pci-audit Command, p. 422
( )	Allow only necessary protocols and networks to be accessed by configuring your corporate firewall or using the internal Array firewall.	Filters, p. 289
( ) ( ) ( ) ( ) ( ) ( )	Change the default Admin account password. Remove any unnecessary admin or user accounts. Change the SNMP community string from the default password. Use WPA2 and 802.1x authentication. Change default SSID from Xirrus to a user-defined SSID. Disable SSID broadcast for all PCI compliant SSIDs.	Express Setup, p. 176 Admin Management, p. 215 SNMP, p. 200 SSIDs, p. 235 and Global Settings, p. 225 SSIDs, p. 235 SSIDs, p. 235
( ) ( ) ( )	Enable Secure Shell (ssh) for CLI (command line) access. Confirm telnet access is disabled (done by default). Confirm management over the wireless network is disabled.	Management Control, p. 219 Global Settings (IAP), p. 260

✓	Xirrus Wi-Fi Array Configuration for PCI DSS	See...
( ) ( )	Check that external RADIUS servers have been configured for use with 802.1x and WPA/WPA2 wireless security. Ensure that Array Administration Accounts are being validated by External RADIUS servers.	SSIDs, p. 235 and Global Settings, p. 225 Admin RADIUS, p. 216
( )	Ensure that each Xirrus Array is physically inaccessible such that console ports and management ports are not accessible.	Securing the Array, p. 94 See Indoor Enclosure
( ) ( )	Enable syslog messaging and define a syslog server on the wired network to receive syslog messages. Enable NTP and define an NTP server (optional).	System Log, p. 197 Time Settings (NTP), p. 194
( )	Enable the RF Monitor radio in the Xirrus Array. Categorize known or approved devices as such. Respond to any alert of unknown or unapproved wireless devices discovered by the RF Monitor.	IAP Settings, p. 255 Rogue Control List, p. 233 Intrusion Detection, p. 148

Additional information regarding implementation of PCI DSS on the Wi-Fi Array is described in the Xirrus White Paper, PCI Data Security Standard, available on the Xirrus web site.

The pci-audit Command

The Array provides a CLI command, pci-audit, that checks whether the Array's configuration satisfies PCI DSS wireless requirements. This command does not change any parameters, but will inform you of any violations that exist. Furthermore, the command **pci-audit enable** will put the Array in PCI Mode and monitor changes that you make to the Array's configuration in CLI or the WMI. PCI Mode will warn you (and issue a Syslog message) if the change violates PCI DSS requirements. A warning is issued when a non-compliant change is first applied to the Array, and also if you attempt to save a configuration that is non-compliant. Use this command in conjunction with The Xirrus Array PCI

Compliance Configuration above to ensure that you are using the Array in accordance with the PCI DSS requirements.

The pci-audit command checks items such as:

- Telnet is disabled.

- Admin RADIUS is enabled (admin login authentication is via RADIUS server).

- An external Syslog server is in use.

- All SSIDs must set encryption to WPA or better (which also enforces 802.1x authentication)

Sample output from this command is shown below.

```
SS-Array(config)# pci-audit
PCI audit failure: telnet enabled.
PCI audit failure: admin RADIUS authentication disabled.
PCI audit failure: SSID ssid2 encryption too weak.
PCI audit failure: SSID ssid3 encryption too weak.
PCI audit failure: SSID ssid4 encryption too weak.
PCI audit failure: SSID ssid5 encryption too weak.
PCI audit failure: SSID ssid6 encryption too weak.
```

Figure 189. Sample output of pci-audit command

Additional Resources

- PCI Security Standards Web site: www.pcisecuritystandards.org

- List of Qualified PCI Security Assessors: www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

- For the latest version of the Xirrus White Paper, PCI Data Security Standard, and the latest versions of Xirrus software, please check www.xirrus.com

Appendix E: Implementing FIPS Security

Wi-Fi Arrays may be configured to satisfy the requirements for Level 2 of Federal Information Processing Standard (FIPS) Publication 140-2. The procedure in this section lists simple steps that must be followed exactly to implement FIPS 140-2, Level 2. The procedure includes physical actions, and parameters that must be set in Web Management Interface (WMI) windows in the Security section and in other sections.

The following topics are discussed:

- "To implement FIPS 140-2, Level 2 using WMI" on page 425.
- "To check if an Array is in FIPS mode:" on page 431
- "To implement FIPS 140-2, Level 2 using CLI:" on page 431

To implement FIPS 140-2, Level 2 using WMI

1. Apply the supplied tamper-evident seals to the unit as indicated in the figures below. The procedure is slightly different, depending on the model.

   - Before you apply the tamper-evident seal, clean the area of any grease, dirt, or oil. We recommend using alcohol-based cleaning pads for this.

   - Each seal must be applied to straddle both sides of an opening so that it will show if an attempt has been made to open the Array.

- XS16, XS12, XS8, XS-3900, or XS-3700—Apply two seals, one on either side of the Array about 180° apart from each other, as shown. Apply a third seal to the access panel opening, as shown. **IMPORTANT: Make sure that each seal straddles a seam.**
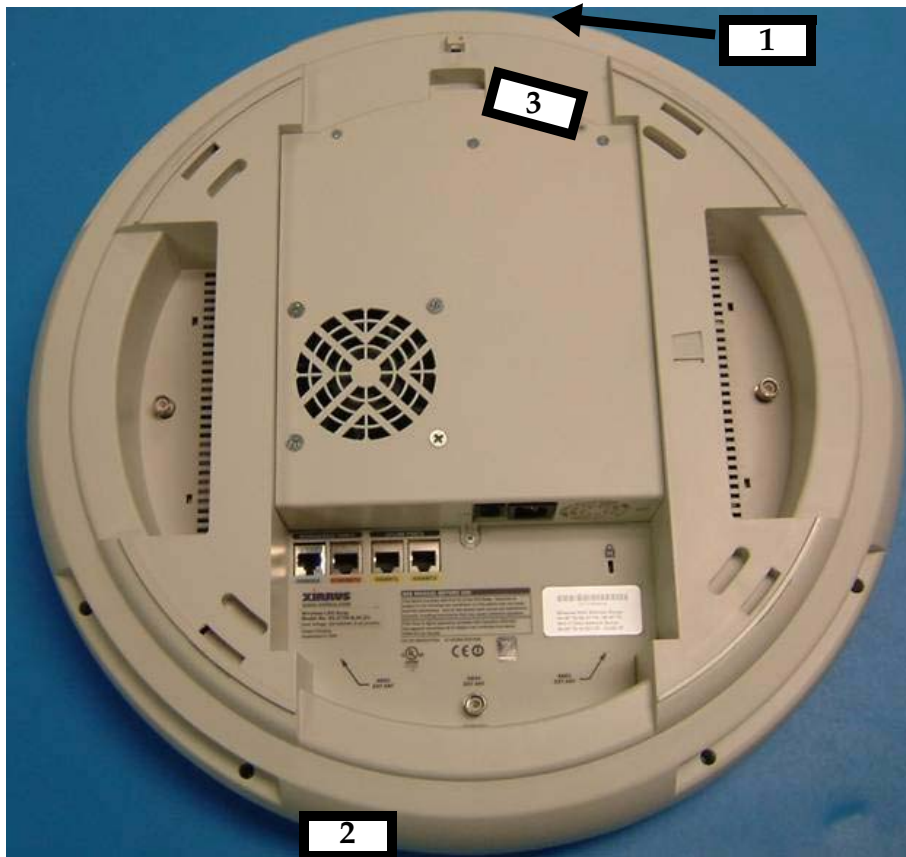
Figure 190. Applying Three Seals to XS16/XS12/XS8 or XS-3900/XS-3700

- XS4 or XS-3500—Apply two seals, one on either side of the Array about 180° apart from each other, as shown. **IMPORTANT: Make sure that each seal straddles a seam.**
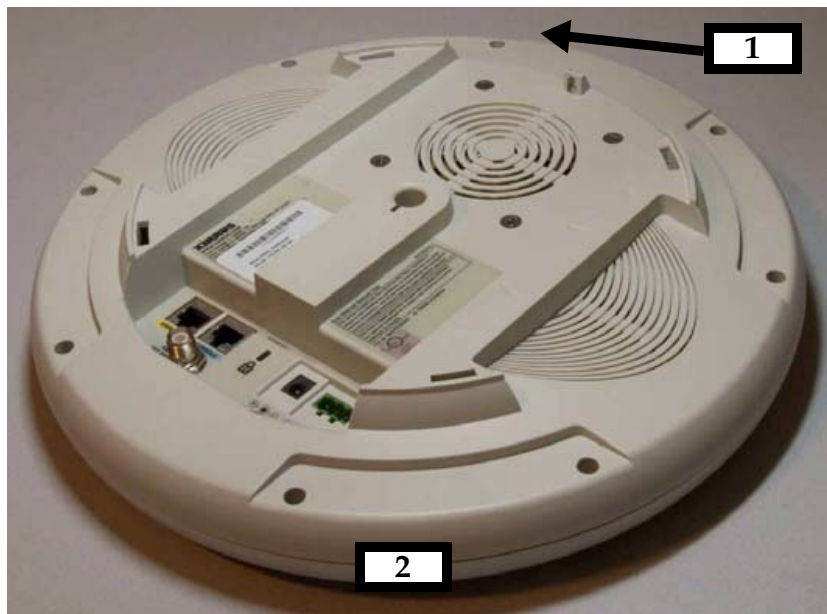
Figure 191. Applying Two Tamper-evident seals to the XS4 or XS-3500

2. Enable HTTPS using the CLI if it is not already enabled, using the following command:

   Xirrus_Wi-Fi_Array(config)# https on

This allows the Web Management Interface to be used for the rest of this procedure. HTTPS is enabled on Arrays by default.

3. Select the SSIDs/SSID Management window. Set **Encryption Type** to **WPA2** (Figure 192). Click **Modify**, then **Save**. Make sure that this is set for **each** SSID.

Figure 192. SSID Management Window

4. In the Security/Global Settings window, select **No** for **TKIP Enabled** and **Yes** for **AES Enabled**. Click **Apply**, then **Save**.
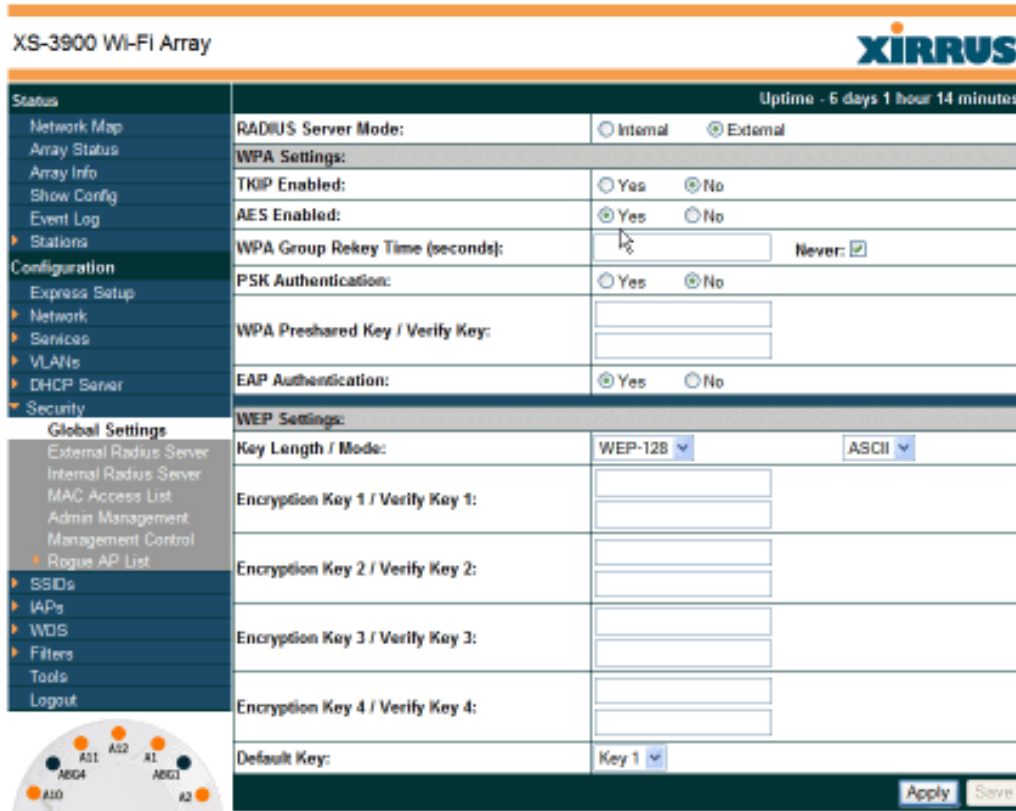
Figure 193. Security/Global Settings Window

5. In the Security/Management Control window, select **Yes** for **Enable Management over SSH**. Select **No** for **Enable Management over Telnet** and for **Enable Management over IAPs**. Click **Apply**, then **Save**.
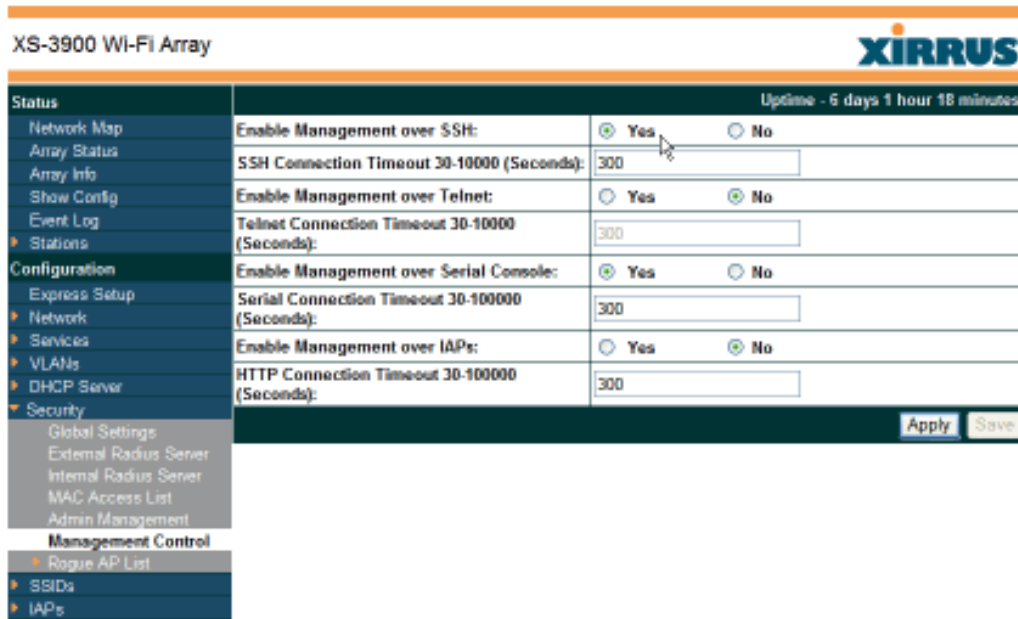
Figure 194. Security/Management Control Window

6. In the Services/SNMP window, select **No** for **Enable SNMP**. Click **Apply**, then **Save**.
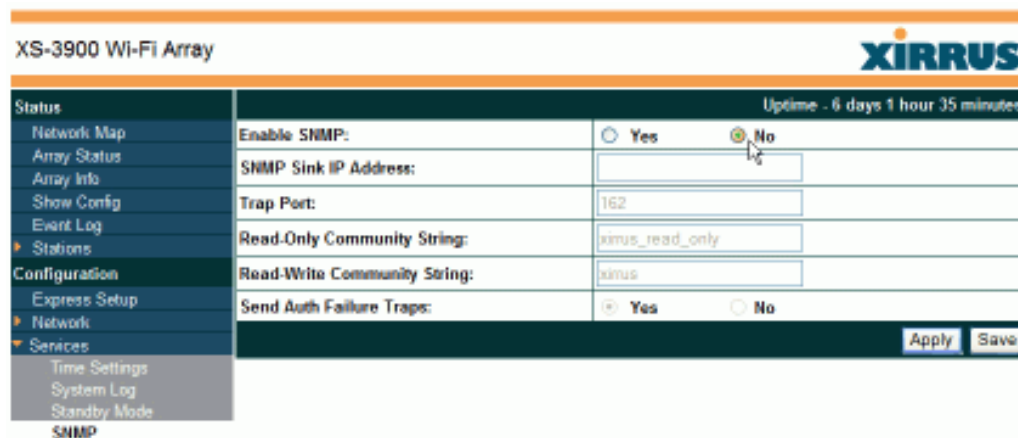
Figure 195. Services/SNMP Window

7. In the IAPs/Global Settings window, select **Off** for **Fast Roaming**. Click **Apply**, then **Save**.
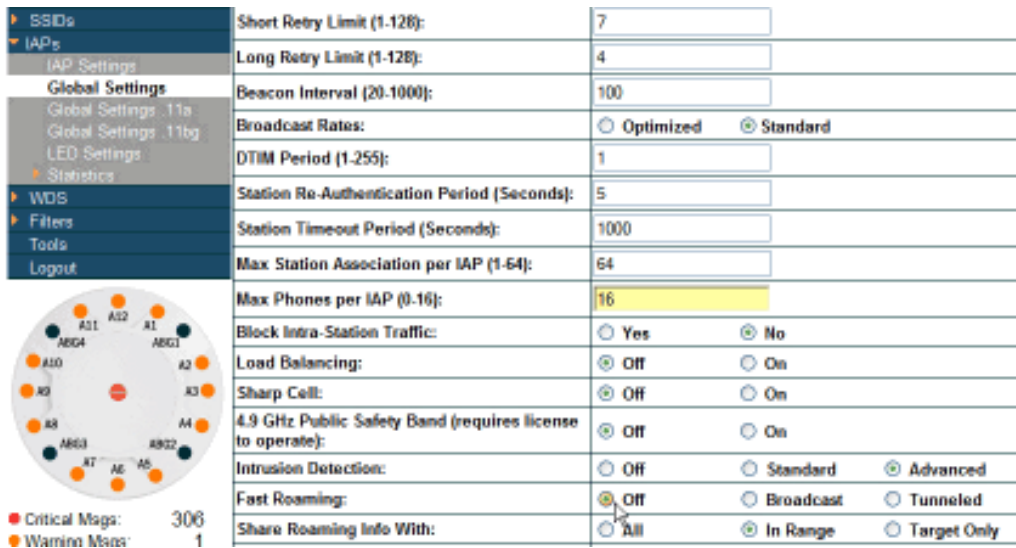
Figure 196. IAPs/Global Settings Screen

To check if an Array is in FIPS mode:

You may determine whether or not the Array is running in FIPS mode by verifying that the settings described in the previous procedure are in effect.

To implement FIPS 140-2, Level 2 using CLI:

1. The following CLI command will perform all of the settings required to put the Array in FIPS mode:.

   Xirrus_Wi-Fi_Array(config}# fips on

   This command remembers your previous settings for FIPS-related attributes. They will be restored if you use the **fips off** command.

   Use the **save** command to save these changes to flash memory.

2. Use the **fips off** command if you would like to revert the FIPS settings back to the values they had before you entered the **fips on** command.

   Xirrus_Wi-Fi_Array(config}# fips off

   Use the **save** command to save these changes to flash memory.

See Also

The Web Management Interface

The Command Line Interface

Appendix F: Notices

This appendix contains the following information:

Notices

FCC Notice

This device complies with Part 15 of the FCC Rules, with operation subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause unwanted operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate RF energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following safety measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Consult the dealer or an experienced wireless technician for help.

Use of a shielded twisted pair (STP) cable must be used for all Ethernet connections in order to comply with EMC requirements.

RF Radiation Hazard Warning

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location where the antennas of the device will have a minimum distance of at least 25 cm (9.84 inches) from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Non-Modification Statement

Unauthorized changes or modifications to the device are not permitted. Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Modifications to the device will void the warranty and may violate FCC regulations. Please go to the Xirrus Web site for a list of all approved antennas.

Indoor Use

This product has been designed for indoor use. Operation of channels in the 5150MHz to 5250MHz band and in the 5470MHz to 5725MHz band is permitted indoors only to reduce the potential for harmful interference to co-channel mobile satellite systems.

Cable Runs for Power over Gigabit Ethernet (PoGE)

If using PoGE, the Array must be connected to PoGE networks without routing cabling to the outside plant—this ensures that cabling is not exposed to lightning strikes or possible cross over from high voltage.

Use of RP-TNC External Antenna Connectors

External RP-TNC antenna connectors are not for outside plant connection.

Battery Warning

Caution! The Array contains a battery which is not to be replaced by the customer. Danger of Explosion exists if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Power Cord

If you will be using the Array with a power cord, you must use a UL-Approved cord (supplied with the unit). Order new power cords from the Xirrus product list—Xirrus supplies only UL-approved power cords.

Maximum Antenna Gain

Currently, the maximum antenna gain for external antennas is limited to 5.2dBi for operation in the 2400MHz to 2483.5MHz, 5150MHz to 5250MHz and 5725MHz to 5825MHz bands. The antenna gains must not exceed maximum EIRP limits set by the FCC / Industry Canada.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5150MHz to 5250MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LELAN devices used in Canada.

Industry Canada Notice and Marking

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

The term "IC:" before the radio certification number only signifies that Industry Canada technical specifications were met.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

EU Directive 1999/5/EC Compliance Information

This section contains compliance information for the Xirrus Wi-Fi Array family of products, which includes the XN16, XN12, XN8, XN4, XS16, XS12, XS8, XS4, XS-3900, XS-3700 and XS-3500. The compliance information contained in this section is relevant to the European Union and other countries that have implemented the EU Directive 1999/5/EC.

Declaration of Conformity

Cesky [Czech]	Toto zahzeni je v souladu se základnimi požadavky a ostatnimi odpovidajcimi ustano veni mi Směrnice 1999/5/EC.
Dansk [Danish]	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]	Dieses Gerat entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtinie 1999/5/EU.
Eesti [Estonian]	See seande vastab direktiivi 1999/5/EU olulistele nöuetele ja teistele as jakohastele sätetele.
English	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spain]	Este equipo cump le con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνυκη [Greek]	Αυτός ο εξοπλτσμός είναι σε συμμόρφωση με τις ουσιώδειζ απαιτήσειζ και ύλλες σχετικέζ διατάξειζ της Οδηγιαζ 1999/5/EC.
Français [French]	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.

XIRRUS®

Íslenska [Icelandic]	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajā prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šis įrenginys tenkina 1995/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
Nederlands [Dutch]	Dit apparant voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1995/5/EC.
Malti [Maltese]	Dan l-apparant huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]	Ez a készülék teljesiti az alapvetö követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]	Urządzenie jest zgodne z ogólnymi wymaganiami oraz sczególnymi mi warunkami określony mi Dyrektywą. UE:1999/5/EC.
Portuguès [Portuguese]	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi popoji Direktive 1999/5/EC.

Slovensky [Slovak]	Toto zariadenie je v zhode so základnými požadavkami a inými prislušnými nariadeniami direktiv: 1999/5/EC.
Suomi [Finnish]	Tämä laite täyttää direktiivin 1999/5//EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Assessment Criteria

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 301 893 and EN 300 328 (if applicable)
- EMC: EN 301 489-1 and EN 301 489-17
- Safety: EN 50371 to EN 50385 and EN 60601

CE Marking

For the Xirrus Wi-Fi Array (XN16, XN12, XN8, XN4, XS16, XS12, XS8, XS4, XS-3900, XS-3700 and XS-3500), the CE mark and Class-2 identifier opposite are affixed to the equipment and its packaging:

$$\mathsf{C} \mathsf{E} \quad \textcircled{!}$$

WEEE Compliance

Waste
Electrical and
Electronic
Equipment
(WEEE)

- Natural resources were used in the production of this equipment.

- This equipment may contain hazardous substances that could impact the health of the environment.

- In order to avoid harm to the environment and consumption of natural resources, we encourage you to use appropriate take-back systems when disposing of this equipment.

- The appropriate take-back systems will reuse or recycle most of the materials of this equipment in a way that will not harm the environment.

- The crossed-out wheeled bin symbol (in accordance with European Standard EN 50419) invites you to use those take-back systems and advises you not to combine the material with refuse destined for a land fill.

- If you need more information on collection, re-use and recycling systems, please contact your local or regional waste administration.

- Please contact Xirrus for specific information on the environmental performance of our

National Restrictions

In the majority of the EU and other European countries, the 2.4 GHz and 5 GHz bands have been made available for the use of Wireless LANs. The following table provides an overview of the regulatory requirements in general that are applicable for the 2.4 GHz and 5 GHz bands.

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor	Outdoor
2400–2483.5	100	X	X**
5150–5350*	200	X	N/A
5470–5725*	1000	X	X

Dynamic frequency selection and Transmit Power Control is required in these frequency bands.

**France is indoor use only in the upper end of the band.*

The requirements for any country may change at any time. Xirrus recommends that you check with local authorities for the current status of their national regulations for both 2.4 GHz and 5 GHz wireless LANs.

The following countries have additional requirements or restrictions than those listed in the above table:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Xirrus recommends checking at www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie www.bipt.be voor meer gegevens.

Les liasons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mèters doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez www.bipt.be pour de plus amples détails.

Greece

A license from EETT is required for the outdoor operation in the 5470 MHz to 5725 MHz band. Xirrus recommends checking www.eett.gr for more details.

Η δη ιουργβάικτ ωνεξωτεpικο pουστη ζ νησυ νοτ των 5470–5725 MHz ε ιτp ετάιωνο ετάά όάδειά της ΕΕΤΤ, ου οpηγεβτάι στεpά ά ό σ φωνη γν η του ΓΕΕΘΑ. εpισσότεpες λε τομ pειεωστο www.eett.gr

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check with www.communicazioni.it/it/ for more details.

Questo prodotto é conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti wireless LAN richiede una "autorizzazione Generale." Consultare www.communicazioni.it/it/ per maggiori dettagli.

Norway, Switzerland and Liechtenstein

Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

Calculating the Maximum Output Power

The regulatory limits for maximum output power are specified in EIRP (radiated power). The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Antennas

The Xirrus Wi-Fi Array employs integrated antennas that cannot be removed and which are not user accessible. Nevertheless, as regulatory limits are not the same throughout the EU, users may need to adjust the conducted power setting for the radio to meet the EIRP limits applicable in their country or region. Adjustments can be made from the product's management interface—either Web Management Interface (WMI) or Command Line Interface (CLI).

Operating Frequency

The operating frequency in a wireless LAN is determined by the access point. As such, it is important that the access point is correctly configured to meet the local regulations. See National Restrictions in this section for more information.

If you still have questions regarding the compliance of Xirrus products or you cannot find the information you are looking for, please contact us at:

Xirrus, Inc.
2101 Corporate Center Drive
Thousand Oaks, CA 91320
USA

Tel: 1.805.262.1600
          1.800.947.7871 Toll Free in the US
Fax: 1.866.462.3980

www.xirrus.com

Safety Warnings

! **Safety Warnings**

Read all user documentation before powering this device. All Xirrus interconnected equipment should be contained indoors. This product is not suitable for outdoor operation. Please verify the integrity of the system ground prior to installing Xirrus equipment. Additionally, verify that the ambient operating temperature does not exceed 50°C.

! **Explosive Device Proximity Warning**

Do not operate the XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/ XS-3900/XS-3700/XS-3500 unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

! **Lightning Activity Warning**

Do not work on the XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/ XS-3900/XS-3700/XS-3500 or connect or disconnect cables during periods of lightning activity.

! **Circuit Breaker Warning**

The XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/ XS-3500 relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.

Translated safety warnings appear on the following page.

Translated Safety Warnings

Avertissements de Sécurité

! **Sécurité**

Lisez l'ensemble de la documentation utilisateur avant de mettre cet appareil sous tension. Tous les équipements Xirrus interconnectés doivent être installés en intérieur. Ce produit n'est pas conçu pour être utilisé en extérieur. Veuillez vérifier l'intégrité de la terre du système avant d'installer des équipements Xirrus. Vérifiez également que la température de fonctionnement ambiante n'excède pas 50°C.

! **Proximité d'appareils explosifs**

N'utilisez pas l'unité XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/ XS-3900/XS-3700/XS-3500 à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.

! **Foudre**

N'utilisez pas l'unité XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/ XS-3900/XS-3700/XS-3500 et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.

! **Disjoncteur**

L'unité XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Software Warranty and License Agreement

THIS SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT") IS A LEGAL AGREEMENT BETWEEN YOU ("CUSTOMER") AND LICENSOR (AS DEFINED BELOW) AND GOVERNS THE USE OF THE SOFTWARE INSTALLED ON THE PRODUCT (AS DEFINED BELOW). IF YOU ARE AN EMPLOYEEbo OR AGENT OF CUSTOMER, YOU HEREBY REPRESENT AND WARRANT TO LICENSOR THAT YOU HAVE THE POWER AND AUTHORITY TO ACCEPT AND TO BIND CUSTOMER TO THE TERMS AND CONDITIONS OF THIS AGREEMENT (INCLUDING ANY THIRD PARTY TERMS SET FORTH HEREIN). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT RETURN THE PRODUCT AND ALL ACCOMPANYING MATERIALS (INCLUDING ALL DOCUMENTATION) TO THE RELEVANT VENDOR FOR A FULL REFUND OF THE PURCHASE PRICE THEREFOR.

CUSTOMER UNDERSTANDS AND AGREES THAT USE OF THE SOFTWARE SHALL BE DEEMED AN AGREEMENT TO THE TERMS AND CONDITIONS GOVERNING SUCH SOFTWARE AND THAT CUSTOMER IS BOUND BY AND BECOMES A PARTY TO THIS AGREEMENT.

1. Definitions

1.1 "Documentation" means the user manuals and all other all documentation, instructions or other similar materials accompanying the Software covering the installation, application, and use thereof.

1.2 "Licensor" means XIRRUS and its suppliers.

1.3 "Product" means a multi-radio access point containing four or more distinct radios capable of simultaneous operation on four or more non-overlapping channels.

1.4 "Software" means, collectively, each of the application and embedded software programs delivered to Customer in connection with this Agreement. For purposes of this Agreement, the term Software shall be deemed to include any and all Documentation and Updates provided with or for the Software.

1.5 "Updates" means any bug-fix, maintenance or version release to the Software that may be provided to Customer from Licensor pursuant to this Agreement or pursuant to any separate maintenance and support agreement entered into by and between Licensor and Customer.

2. Grant of Rights

2.1 **Software**. Subject to the terms and conditions of this Agreement, Licensor hereby grants to Customer a perpetual, non-exclusive, non-sublicenseable, non-transferable right and license to use the Software solely as installed on the Product in accordance with the accompanying Documentation and for no other purpose.

2.2 **Ownership**. The license granted under Sections 2.1 above with respect to the Software does not constitute a transfer or sale of Licensor's or its suppliers' ownership interest in or to the Software, which is solely licensed to Customer. The Software is protected by both national and international intellectual property laws and treaties. Except for the express licenses granted to the Software, Licensor and its suppliers retain all rights, title and interest in and to the Software, including (i) any and all trade secrets, copyrights, patents and other proprietary rights therein or thereto or (ii) any Marks (as defined in Section 2.3 below) used in connection therewith. In no event shall Customer remove, efface or otherwise obscure any Marks contained on or in the Software. All rights not expressly granted herein are reserved by Licensor.

2.3 **Copies**. Customer shall not make any copies of the Software but shall be permitted to make a reasonable number of copies of the related Documentation. Whenever Customer copies or reproduces all or any part of the Documentation, Customer shall reproduce all and not efface any titles, trademark symbols, copyright symbols and legends, and other proprietary markings or similar indicia of origin ("Marks") on or in the Documentation.

2.4 **Restrictions**. Customer shall not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) sell, rent, lease, license or sublicense, assign or otherwise transfer the Software, or any of Customer's rights and obligations under this Agreement except as expressly permitted herein; (ii) decompile, disassemble, or reverse engineer the Software, in whole or in part, provided that in those jurisdictions in which a total prohibition on any reverse engineering is prohibited as a matter of law and such prohibition is not cured by the fact that this Agreement is subject to the laws of the State of California, Licensor agrees to grant Customer, upon Customer's written request to Licensor, a limited reverse engineering license to permit interoperability of the Software with other software or code used by Customer; (iii) allow access to the Software by any user other than by Customer's employees and contractors who are bound in writing to confidentiality and non-use restrictions at least as protective as those set forth herein; (iv) except as expressly set forth herein, write or develop any derivative software or any other software program based upon the Software; or (v) use any

computer software or hardware which is designated to defeat any copy protection or other use limiting device, including any device intended to limit the number of users or devices accessing the Product.

3. Limited Warranty and Limitation of Liability

3.1 **Limited Warranty & Exclusions**. Licensor warrants that the Software will perform in substantial accordance with the specifications therefor set forth in the Documentation for a period of ninety [90] days after Customer's acceptance of the terms of this Agreement with respect to the Software ("Warranty Period"). If during the Warranty Period the Software does not perform as warranted, Licensor shall, at its option, correct the relevant Software giving rise to such breach of performance or replace such Software free of charge. THE FOREGOING ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE FOREGOING WARRANTY. THE WARRANTY SET FORTH ABOVE IS MADE TO AND FOR THE BENEFIT OF CUSTOMER ONLY. The warranty will apply only if (i) the Software has been used at all times and in accordance with the instructions for use set forth in the Documentation and this Agreement; (ii) no modification, alteration or addition has been made to the Software by persons other than Licensor or Licensor's authorized representative; and (iii) the Software or Product on which the Software is installed has not been subject to any unusual electrical charge.

3.2 **DISCLAIMER**. EXCEPT AS EXPRESSLY STATED IN THIS SECTION 3, ALL ADDITIONAL CONDITIONS, REPRESENTATIONS, AND WARRANTIES, WHETHER IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, ACCURACY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY DISCLAIMED BY LICENSOR AND ITS SUPPLIERS. THIS DISCLAIMER SHALL APPLY EVEN IF ANY EXPRESS WARRANTY AND LIMITED REMEDY OFFERED BY LICENSOR FAILS OF ITS ESSENTIAL PURPOSE. ALL WARRANTIES PROVIDED BY LICENSOR ARE SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN THIS AGREEMENT.

3.3 **HAZARDOUS APPLICATIONS**. THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF A NUCLEAR FACILITY, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROLS OR OTHER

DEVICES OR SYSTEMS IN WHICH A MALFUNCTION OF THE SOFTWARE WOULD RESULT IN FORESEEABLE RISK OF INJURY OR DEATH TO THE OPERATOR OF THE DEVICE OR SYSTEM OR TO OTHERS ("HAZARDOUS APPLICATIONS"). CUSTOMER ASSUMES ANY AND ALL RISKS, INJURIES, LOSSES, CLAIMS AND ANY OTHER LIABILITIES ARISING OUT OF THE USE OF THE SOFTWARE IN ANY HAZARDOUS APPLICATIONS.

3.4 **Limitation of Liability**.

(a) **TOTAL LIABILITY**. NOTWITHSTANDING ANYTHING ELSE HEREIN, ALL LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMER FOR THE RELEVANT SOFTWARE, OR PORTION THEREOF, THAT GAVE RISE TO SUCH LIABILITY OR ONE HUNDRED UNITED STATES DOLLARS (US$100), WHICHEVER IS GREATER. THE LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS SECTION SHALL BE CUMULATIVE AND NOT PER INCIDENT.

(b) **DAMAGES**. IN NO EVENT SHALL LICENSOR, ITS SUPPLIERS OR THEIR RELEVANT SUBCONTRACTORS BE LIABLE FOR (A) ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR LOST OR DAMAGED DATA, OR ANY INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE OR (B) ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES IN EACH CASE, EVEN IF LICENSOR OR ITS SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 **Exclusions**. SOME JURISDICTIONS DO NOT PERMIT THE LIMITATIONS OF LIABILITY AND LIMITED WARRANTIES SET FORTH UNDER THIS AGREEMENT. IN THE EVENT YOU ARE LOCATED IN ANY SUCH JURISDICTION, THE FOREGOING LIMITATIONS SHALL APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED IN SUCH JURISDICTIONS. IN NO EVENT SHALL THE FOREGOING EXCLUSIONS AND LIMITATIONS ON DAMAGES BE DEEMED TO APPLY TO ANY LIABILITY BASED ON FRAUD, WILLFUL MISCONDUCT, GROSS NEGLIGENCE OR PERSONAL INJURY OR DEATH.

4. Confidential Information

4.1 **Generally**. The Software (and its accompanying Documentation) constitutes Licensor's and its suppliers' proprietary and confidential information and contains valuable trade secrets of Licensor and its suppliers ("Confidential Information"). Customer shall protect the secrecy of the Confidential Information to the same extent it protects its other valuable, proprietary and confidential information of a similar nature but in no event shall Customer use less than reasonable care to maintain the secrecy of the Confidential Information. Customer shall not use the Confidential Information except to exercise its rights or perform its obligations as set forth under this Agreement. Customer shall not disclose such Confidential Information to any third party other than subject to non-use and non-disclosure obligations at least as protective of a party's right in such Confidential Information as those set forth herein.

4.2 **Return of Materials**. Customer agrees to (i) destroy all Confidential Information (including deleting any and all copies contained on any of Customer's Designated Hardware or the Product) within fifteen (15) days of the date of termination of this Agreement or (ii) if requested by Licensor, return, any Confidential Information to Licensor within thirty (30) days of Licensor's written request.

5. Term and Termination

5.1 **Term**. Subject to Section 5.2 below, this Agreement will take effect on the Effective Date and will remain in force until terminated in accordance with this Agreement.

5.2 **Termination Events**. This Agreement may be terminated immediately upon written notice by either party under any of the following conditions:

(a) If the other party has failed to cure a breach of any material term or condition under the Agreement within thirty (30) days after receipt of notice from the other party; or

(b) Either party ceases to carry on business as a going concern, either party becomes the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation, which proceeding is not dismissed within ninety (90) days, or a receiver is appointed with respect to a substantial part of its assets.

5.3 **Effect of Termination**.

(a) Upon termination of this Agreement, in whole or in part, Customer shall pay Licensor for all amounts owed up to the effective date of termination. Termination of this Agreement shall not constitute a waiver for any amounts due.

(b) The following Sections shall survive the termination of this Agreement for any reason: Sections 1, 2.2, 2.4, 3, 4, 5.3, and 6.

(c) No later than thirty (30) days after the date of termination of this Agreement by Licensor, Customer shall upon Licensor's instructions either return the Software and all copies thereof; all Documentation relating thereto in its possession that is in tangible form or destroy the same (including any copies thereof contained on Customer's Designated Hardware). Customer shall furnish Licensor with a certificate signed by an executive officer of Customer verifying that the same has been done.

6. Miscellaneous

If Customer is a corporation, partnership or similar entity, then the license to the Software and Documentation that is granted under this Agreement is expressly conditioned upon and Customer represents and warrants to Licensor that the person accepting the terms of this Agreement is authorized to bind such entity to the terms and conditions herein. If any provision of this Agreement is held to be invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect. During the course of use of the Software, Licensor may collect information on your use thereof; you hereby authorize Licensor to use such information to improve its products and services, and to disclose the same to third parties provided it does not contain any personally identifiable information. The express waiver by either party of any provision, condition or requirement of this Agreement does not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Customer and Licensor are independent parties. Customer may not export or re-export the Software or Documentation (or other materials) without appropriate United States, European Union and foreign government licenses or in violation of the United State's Export Administration Act or foreign equivalents and Customer shall comply with all national and international laws governing the Software. This Agreement will be governed by and construed under the laws of the State of California and the United States as applied to agreements entered into and to be performed entirely within California, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer

Information Transactions Act (as promulgated by any State) to this Agreement. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of, the state and federal courts located in Ventura County, California. Customer may not assign this Agreement by operation of law or otherwise, without the prior written consent of Licensor and any attempted assignment in violation of the foregoing shall be null and void. This Agreement cancels and supersedes all prior agreements between the parties. This Agreement may not be varied except through a document agreed to and signed by both parties. Any printed terms and conditions contained in any Customer purchase order or in any Licensor acknowledgment, invoice or other documentation relating to the Software shall be deemed deleted and of no force or effect and any additional typed and/or written terms and conditions contained shall be for administrative purposes only, i.e. to identify the types and quantities of Software to be supplied, line item prices and total price, delivery schedule, and other similar ordering data, all in accordance with the provisions of this Agreement.

Hardware Warranty Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

LIMITED WARRANTY. Xirrus warrants that for a period of one year from the date of purchase by the original purchaser ("Customer"): (i) the Xirrus Equipment ("Equipment") will be free of defects in materials and workmanship under normal use; and (ii) the Equipment substantially conforms to its published specifications. Except for the foregoing, the Equipment is provided AS IS. This limited warranty extends only to Customer as the original purchaser. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' option, repair, replacement, or refund of the Equipment if reported (or, upon request, returned) to the party supplying the Equipment to Customer. In no event does Xirrus warrant that the Equipment is error free or that Customer will be able to operate the Equipment without problems or interruptions.

This warranty does not apply if the Equipment (a) has been altered, except by Xirrus, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Xirrus, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra-hazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL XIRRUS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE EQUIPMENT EVEN IF XIRRUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Xirrus' or its suppliers' liability to Customer,

whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer.

The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any evaluation Equipment made available for testing or demonstration purposes. All such Equipment is provided AS IS without any warranty whatsoever.

Customer agrees the Equipment and related documentation shall not be used in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or cause or permit any third party to do any of the foregoing.

All information or feedback provided by Customer to Xirrus with respect to the Product shall be Xirrus' property and deemed confidential information of Xirrus.

Equipment including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Equipment.

This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this Warranty shall remain in full force and effect. This Warranty constitutes the entire agreement between the parties with respect to the use of the Equipment.

Manufacturer is Xirrus, Inc. 2101 Corporate Center Drive Thousand Oaks, CA 91320

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11d

A supplement to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It allows Access Points to communicate information on the permissible radio channels with acceptable power levels for user devices. Because the 802.11 standards cannot legally operate in some countries, 802.11d adds features and restrictions to allow WLANs to operate within the rules of these countries.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

802.1Q

An IEEE standard for MAC layer frame tagging (also known as encapsulation). Frame tagging uniquely assigns a user-defined ID to each frame. It also enables a switch to communicate VLAN membership information across multiple (and multi-vendor) devices by frame tagging.

AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

beacon interval

When a device in a wireless network sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. Network administrators can adjust the beacon interval—usually measured in milliseconds (ms) or its equivalent, kilo-microseconds (Kmsec).

bit rate

The transmission rate of binary symbols ('0' and '1'), equal to the total number of bits transmitted in one second.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a BSS network. See also, SSID.

CDP

(Cisco Discovery Protocol) CDP is a layer 2 network protocol which runs on most Cisco equipment and some other network equipment. It is used to share information with other directly connected network devices. Information such as the model, network capabilities, and IP address is shared. Wi-Fi Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors.

cell

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11). In the 5 GHz band, 802.11a uses 8 channels for indoor use and 4 for outdoor use, none of which overlap. In the U.S., additional channels are available, to bring the total to 24 channels.

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

default gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DHCP lease

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the "domain" address for Xirrus is: http://www.xirrus.com, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.

- **www** is a reference to the World Wide Web.

- **xirrus** refers to the company.

- **com** specifies that the domain belongs to a commercial enterprise.

DTIM

(Delivery Traffic Indication Message) A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

EAP

(Extensible Authentication Protocol) When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). However, LCP is somewhat inflexible because it has to specify an authentication device early in the process. EAP allows the system to gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP (for example, passwords and public keys).

EDCF

(Enhanced Distributed Coordinator Function) A QoS extension which uses the same contention-based access mechanism as current devices but adds "offset contention windows" that separate high priority packets from low priority packets (by assigning a larger random backoff window to lower priorities than to higher priorities). The result is "statistical priority," where high-priority packets usually are transmitted before low-priority packets.

encapsulation

A way of wrapping protocols such as TCP/IP, AppleTalk, and NetBEUI in Ethernet frames so they can traverse an Ethernet network and be unwrapped when they reach the destination computer.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

Fast Ethernet

A version of standard Ethernet that runs at 100 Mbps rather than 10 Mbps.

FCC

(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

FIPS

The Federal Information Processing Standard (FIPS) Publication 140-2 establishes a computer security standard used to accredit cryptographic modules. The standard is a joint effort by the U.S. and Canadian governments.

frame

A packet encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

Gigabit 1

The primary Gigabit Ethernet interface. See also, Gigabit Ethernet.

Gigabit 2

The secondary Gigabit Ethernet interface. See also, Gigabit Ethernet.

Gigabit Ethernet

The newest version of Ethernet, with data transfer rates of 1 Gigabit (1,000 Mbps).

Group

A user group, created to define a set of attributes (such as VLAN, traffic limits, and Web Page Redirect) and privileges (such as fast roaming) that apply to all users that are members of the group. This allows a uniform configuration to be easily applied to multiple user accounts. The attributes that can be configured for user groups are almost identical to those that can be configured for SSIDs.

host name

The unique name that identifies a computer on a network. On the Internet, the host name is in the form **comp.xyz.net**. If there is only one Internet site the host name is the same as the domain name. One computer can have more than one host name if it hosts more than one Internet site (for example, **home.xyz.net** and **comp.xyz.net)**. In this case, **comp** and **home** are the host names and **xyz.net** is the domain name.

IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs.

MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTU

(Maximum Transmission Unit) The largest physical packet size—measured in bytes—that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

PLCP

(Physical Layer Convergence Protocol) Defined by IEEE 802.6, a protocol specified within the Transmission Convergence layer that defines exactly how cells are formatted within a data stream for a particular type of transmission facility.

PoGE

This refers to the optional Xirrus XP1 Power over Gigabit Ethernet modules that provide DC power to Arrays. Power is supplied over the same Cat 5e or Cat 6 cable that supplies the data connection to your gigabit Ethernet switch, thus eliminating the need to run a power cable. See "Power over Gigabit Ethernet Compatibility Matrix" on page 414 for a list of Xirrus PoGE modules and the modules that are compatible with each Array.

preamble

Preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. PLCP has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

private key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

PSK

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

public key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider prioritizes or guarantees a service's performance.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SDMA

(Spatial Division Multiple Access) A wireless communications mode that optimizes the use of the radio spectrum and minimizes cost by taking advantage of the directional properties of antennas. The antennas are highly directional, allowing duplicate frequencies to be used for multiple zones.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSH

(Secure SHell) Developed by SSH Communications Security, Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. The Array only allows SSH-2 connections. SSH-2 provides strong authentication and secure communications over insecure channels. SSH-2 protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot "play back" the traffic or hijack the connection when encryption is enabled. When using SSH-2's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords. Be aware that your SSH utility must be set up to use SSH-2.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

TKIP

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven't been tampered with.

transmit power

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

User group

See Group.

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

VLAN tagging

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the 802.11n standard, traffic can be confined to VLANs that exist on

multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

1. That the packet has a tag.

2. Whether the packet should have priority over other packets.

3. Which VLAN it belongs to, so that the switch can forward or filter it correctly.

WDS (Wireless Distribution System)

WDS creates wireless backhauls between arrays. These links between arrays may be used rather than having to install data cabling to each array.

WEP

(Wired Equivalent Privacy) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

Wi-Fi Alliance

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

Wi-Fi Array

A high capacity Wi-Fi networking device consisting of multiple radios arranged in a circular array.

WPA

(Wi-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1x for authentication.

WPA2

(Wi-Fi Protected Access 2) WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.

Xirrus Management System (XMS)

A Xirrus product used for managing large Wi-Fi Array deployments from a centralized Web-based interface.

XP-3100

The Xirrus XP Power System (XP-3100) is a discontinued Xirrus product that provides distributed DC power to multiple XS-3900 units.

XP1 and XP8—Power over Gigabit Ethernet modules

See PoGE.

XPS—Xirrus Power System

A family of optional Xirrus products that provides power over Gigabit Ethernet. See PoGE.

Index

associated users 50
assurance (radio loopback testing) 275
authentication 18
    of admin via RADIUS 216
authority
    certificate 213, 221
auto negotiate 183
auto-blocking
    rogue APs 276
auto-configuration 112, 260, 267, 269
    channel and cell size 275

B

backhaul
    see WDS 76
backup unit
    see standby mode 275
band association 240
beacon interval 260
Beacon World Mode 260
beam distribution 17
benefits 16
blocking
    rogue APs 276
blocking rogue APs 275
boot 297
broadcast 265
    fast roaming 265
browser
    certificate error 213, 221
BSS 398
BSSID 148, 398
buttons 124

C

capacity
    of 802.11n 66
cascading style sheet
    sample for web page redirect 301
cdp 322

CDP (Cisco Discovery Protocol)
    settings 191
cdp CLI command 322
cell
    sharp cell 275
cell size 50, 255, 389
    auto-configuration 275
cell size configuration 275
certificate
    about 213, 221
    authority 213, 221
    error 213, 221
    install Xirrus authority 221
    X.509 213, 221
channel
    auto-configuration 275
    configuration 275
    list selection 275
    public safety 275
channels 50, 148, 255, 260, 267, 269,
        389
    factory default 280
    factory presets 281
    non-overlapping 18
Chassis Cover 382
chassis cover 382
Cisco Discovery Protocol
    see cdp 322
Cisco Discovery Protocol (CDP) 191
CLI 9, 79, 83, 110, 307
    executing from WMI 303
    using to upgrade software image
        409
CLI commands
    see commands 322
client
    web page redirect 300
Command Line Interface 9, 75, 83, 107,
        110, 307, 400
    configuration commands 320

XIRRUS

IEEE 802.1Q 403
image
  upgrade software image 297
implementing Voice over Wi-Fi 48, 205, 237
installation 45, 80, 86, 369
  installing the MCAP-3616 83
  mounting the unit 86
  requirements 45
  unpacking the unit 81
  workflow 80
installation workflow 80
Integrated Access Point Module 382
integrated radio module
  replacing 382
interfaces 176
  Web 119
Internet Explorer 46
intrusion detection 148, 277
  configuration 275
  setting as approved or known 148
IP Address 50, 112, 120, 126, 148, 176, 183, 190, 197, 200, 295, 390
IP Subnet Mask 112

K

key
  license, setting 337
  upgrade 297
key features 16
Keyboard Shortcuts 394
keyboard shortcuts 394
known
  setting rogues 148

L

lastboot.conf 298
Layer 3
  fast roaming 254
lease 390

Lease Time 390
leases, DHCP
  viewing 139
LEDs 107
  sequence 107
  settings 283
license Key
  upgrading 297
license key
  setting 337
limits
  group 251
  interactions 251
  station 251
  traffic 251
list, access control
  see access control list 223
list, MAC access
  see access control list 223
location information 112, 120, 176
log
  diagnostics, create file 299
log messages
  counters 124
log, system (event)
  viewing window 173
logging in 110, 126
Login 126
login
  via Console port 216
login page
  web page redirect 300
logout 305
long retry limit 260
loopback
  see radio assurance 367
loopback testing
  radio assurance mode 275

Q

R

traffic 251
RF
  intrusion detection 275
  spectrum management 275
RF configuration 275
RF management
  see channel 275
RF resilience 275
RFprotect, see XDM 277
roaming 19, 135, 265
roaming, fast 254
Rogue AP 9, 75, 148, 233, 400
rogue AP
  blocking 276
Rogue AP List 148
rogue APs
  blocking 275
Rogue Control List 233
rogue detection 17
rogues
  setting as known or approved 148
root command prompt 311
route
  trace route utility 301
routing table window 138
RSSI 148
RTS 267, 269
RTS threshold 267, 269

S

sample Perl and CSS files for 300
save
  with reboot 297
Save button 120
saved.conf 298
scalability 7
schedule
  auto channel configuration 275
Secondary Port 390
Secondary Server 390

secret 390
Secure Shell 46
secure Shell 45
Security
  FIPS 425
  PCI DSS 419
security 9, 18, 209, 398, 400
  certificate, see certificate 221
see group 247
self-monitoring 277
  radio assurance 367
  radio assurance options 278
self-test
  radio assurance mode 278
serial port 46, 110, 400
server, VTun
  see VTun 208
Service Set Identifier 112
Services 193, 373, 376, 398
servicing 371
servicing the unit 369
settings 176
setup, express 176
sharp cell 275
  setting in WMI 280
short retry limit 260
signal processing
  MIMO 61
SNMP 9, 14, 112, 176, 183, 193, 200, 390
  required for XMS 200, 201
software
  upgrade license key 297
software image
  upgrading via CLI 409
Software Upgrade 295
software upgrade 297
spatial multiplexing 62
specifications 20, 27, 34, 40
spectrum (RF) management 275

User's Guide

XiRRUS®

Wi-Fi Arrays