

WDS Statistics

The main WDS Statistics window provides statistical data for all WDS client and host links. To access data about a specific WDS client or host link, simply click on the desired link in the left frame to access the appropriate window. You may also choose to view a sum of the statistics for all client links, all host links, or all links (both client and host links).

| Status | Name: SS-XNB (10.100.47.186) | | Location: SS Area | | Uptime: 4 days, 4 hours, 4 minutes | | | | |
|--|---|-------|-------------------|--------|------------------------------------|-------|---------|--------|---------|
| <ul style="list-style-type: none"> ▶ Array ▶ Network ▶ RF Monitor ▶ Stations ▶ Statistics <ul style="list-style-type: none"> ▶ IAP ▶ Network ▶ VLAN ▼ WDS <ul style="list-style-type: none"> Client Link 1 Client Link 2 Client Link 3 Client Link 4 Host Link 1 Host Link 2 Host Link 3 | Receive Statistics | | | | Transmit Statistics | | | | |
| | Client Link | Bytes | Packets | Errors | Retries | Bytes | Packets | Errors | Retries |
| | 1 | | | | | | | | |
| | 2 | | | | | | | | |
| | 3 | | | | | | | | |
| | 4 | | | | | | | | |
| | Receive Statistics | | | | Transmit Statistics | | | | |
| | Host Link | Bytes | Packets | Errors | Retries | Bytes | Packets | Errors | Retries |
| | 1 | | | | | | | | |
| | 2 | | | | | | | | |
| | 3 | | | | | | | | |
| | 4 | | | | | | | | |
| | <input type="checkbox"/> Auto Refresh Refresh Clear | | | | | | | | |

Figure 81. WDS Statistics

See Also

- SSID Management
- WDS

Filter Statistics

The Filter Statistics window provides statistical data for all configured filters. The name, state (enabled—on or off), and type (allow or deny) of each filter is shown. For enabled filters, this window shows the number of packets and bytes that met the filter criteria. Click on a column header to sort the rows based on that column. Click on a filter name to edit the filter settings.

| Name | Type | State | Packets | Bytes |
|--------|---------|----------|---------|--------|
| Global | Filter1 | allow on | 1961 | 268436 |

Figure 82. Filter Statistics

See Also
Filters

Station Statistics

This status-only window provides an overview of statistical data for all stations. Stations are listed by MAC address, and Receive and Transmit statistics are summarized for each. For detailed statistics for a specific station, click the desired MAC address in the **Station** column and see “Per-Station Statistics” on page 133.

| Station | Receive Statistics by Station | | | | Transmit Statistics by Station | | | |
|-------------------|-------------------------------|-----------|--------|----------|--------------------------------|------------|--------|-----------|
| | Bytes | Packets | Errors | Retries | Bytes | Packets | Errors | Retries |
| 00:0E:3d:03:02:a8 | 693119 | 2043 | 0 | 223 | 2368 | 12 | 0 | 1 |
| 00:0E:b5:07:3c:79 | 51442645153 | 52791337 | 0 | 5371975 | 65480578303 | 65515091 | 26764 | 118569632 |
| 00:0e:35:45:d8:e0 | 1691913717 | 24210701 | 0 | 8748417 | 168562071943 | 164832863 | 112870 | 104185667 |
| 00:30:b4:01:69:c4 | 1004756270 | 10171896 | 0 | 0 | 265914094203 | 259348067 | 10303 | 48599772 |
| 00:0E:66:19:95:34 | 1550292533 | 5009662 | 0 | 1202533 | 36006965880 | 36032055 | 309651 | 41933995 |
| 00:03:76:b6:14:43 | 197116974748 | 195875363 | 0 | 32942200 | 277967033447 | 2668865001 | 45170 | 60729663 |
| 00:04:a2:8b:42:57 | 323018216404 | 312187936 | 0 | 29556244 | 507270199576 | 492647649 | 12040 | 39468662 |
| 00:10:18:91:0e:66 | 181652416042 | 177651569 | 0 | 18383672 | 264062154829 | 263394451 | 170454 | 36038464 |
| 00:40:96:a7:82:b2 | 249090923768 | 247980426 | 0 | 22610375 | 276050170214 | 270423992 | 18482 | 127696107 |

Figure 83. Station Statistics

Note that you can clear the data for an individual station (see *Per-Station Statistics*), but you cannot clear the data for all stations using this window.

You can **Refresh** the data (update the window with the latest information) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

See Also

Per-Station Statistics

Per-Station Statistics

This window provides detailed statistics for the selected station. This window is accessed from the [Station Statistics](#) window—click the MAC address of the desired entry in the **Station** column to display its Per-Station Statistics window.

Receive and Transmit statistics are listed by **Rate**—this is the data rate in Mbps. For a summary of statistics for all stations, see “[Station Statistics](#)” on page 132.

You can **Refresh** the data (update the window with the latest information) or **Clear** the data (reset all content to zero and begin counting again) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

Station Statistics for 00:0f:3d:03:02:e8

| Rate | Receive Statistics | | | | Transmit Statistics | | | | |
|--------------|--------------------|---------|--------|---------|---------------------|---------|--------|---------|---|
| | Bytes | Packets | Errors | Retries | Bytes | Packets | Errors | Retries | |
| 1 | 1015465 | 18726 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5.5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 3728543 | 77325 | 0 | 15 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 1710 | 5 | 0 | 3 | 0 | 0 | 0 | 0 | 0 |
| 18 | 1726 | 5 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| 24 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 36 | 5959 | 22 | 0 | 2 | 0 | 0 | 0 | 0 | 0 |
| 48 | 73724 | 228 | 0 | 29 | 0 | 0 | 0 | 0 | 0 |
| 54 | 693119 | 2043 | 0 | 223 | 2358 | 12 | 0 | 1 | 1 |
| Total | 6620246 | 98354 | 0 | 274 | 2358 | 12 | 0 | 1 | 1 |

Clear Auto Refresh Refresh

Figure 84. Individual Station Statistics Page

See Also

Station Statistics

System Log Window

This is a status only window that allows you to review the system log, where system alerts and messages are displayed. Although there are no configuration options available in this window, you do have the usual choice of deciding how the event messages are sorted by clicking in the column header for the desired field (Time Stamp, Priority, or Message).

- **Time Stamp**—sorts the list based on the time the event occurred.
- **Priority**—sorts the list based on the priority assigned to the message.
- **Message**—sorts the list based on the message category

The displayed messages may be filtered by using the **Filter Priority** option, which allows control of the minimum priority level displayed. For example, you may choose (under **Services >System Log**) to log messages at or above Debug level but use **Filter Priority** to display only those at Information level and above.

| Status | | Name: SS-X114 (192.168.1.74) | | Location: 12-125 | | Uptime: 2 days, 13 hours, 9 mins | |
|---------------|--|--------------------------------|------------------------------|---|---------------------------------------|----------------------------------|--|
| ▶ Array | | Clear All | Filter Priority: information | Highlight Priority: alert | <input type="checkbox"/> Auto Refresh | Refresh | |
| ▶ Network | | Time Stamp | Priority | Message | | | |
| ▶ RF Monitor | | Jul 10 04:11:24 | notification | Configuration saved by user shelly | | | |
| ▶ Stations | | Jul 10 04:11:18 | notification | Syslog local file level changed to 6 by user shelly | | | |
| ▶ Statistics | | Jul 10 03:30:49 | alert | Station e8:06:88:9a:35:7e, connectivity alarm: distance, 683 feet is greater than threshold of 500 feet | | | |
| System Log | | Jul 10 03:20:49 | alert | Station e8:06:88:9a:35:7e, connectivity alarm: data rate, 9Mbps is less than threshold of 10Mbps | | | |
| IDS Event Log | | Jul 10 02:10:49 | alert | Station e8:06:88:9a:35:7e, connectivity alarm: distance, 609 feet is greater than threshold of 500 feet | | | |
| Configuration | | Jul 10 00:39:50 | information | Station e8:06:88:9a:35:7e, IAP abgn3: associated, SSID: xirus42 | | | |
| Tools | | Jul 10 00:00:00 | alert | 143 days left on temporary license key. | | | |
| Log Messages | | Jul 9 14:38:25 | information | Station e8:06:88:9a:35:7e, IAP abgn3: disassociated, reason: Station has left BSS | | | |

Figure 85. System Log (Alert Level Highlighted)

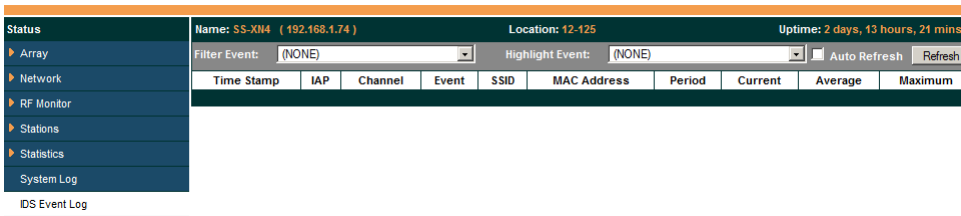
Use the **Highlight Priority** field if you wish to highlight messages at the selected priority level. Click on the **Refresh** button to refresh the message list, or click on the **Clear All** button at the upper left to delete all messages. You can also click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

Note that there is a shortcut way to view system log messages. If you click **Log Messages** near the bottom of the left hand frame, WMI displays counts of log messages at different severity levels. Click a count to display just those messages in the System Log window. See [Figure 38 on page 79](#) for more information.

IDS Event Log Window

This status only window displays the Intrusion Detection System (IDS) Event log, listing any detected attacks on your network. For descriptions of the types of attacks detected, as well as the settings to fine-tune IDS on the Array, please see “Intrusion Detection” on page 270.

The displayed messages may be filtered by using the **Filter Event** setting, which allows you to select just one type of intrusion to display. For example, you may choose to display only beacon flood attacks.



| Time Stamp | IAP | Channel | Event | SSID | MAC Address | Period | Current | Average | Maximum |
|------------|-----|---------|-------|------|-------------|--------|---------|---------|---------|
|------------|-----|---------|-------|------|-------------|--------|---------|---------|---------|

Figure 86. IDS Event Log

Use the **Highlight Event** field if you wish to highlight all events of one particular type in the list. Click on the **Refresh** button to refresh the message list, or click the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

Although there are no configuration options available in this window, you do have the usual choice of deciding how the event messages are sorted by clicking in the column header for the desired field.

- **Time Stamp**—the time that the event occurred.
- **IAP**—the affected radio.
- **Channel**—the affected channel.
- **Event**—the type of attack, as described in [Intrusion Detection](#).
- **SSID**—the SSID that was attacked.
- **MAC Address**—the MAC address of the attacker.
- **Period**—the length of the window used to determine whether the count of this type of event exceeded the threshold.

- **Current**—the count of this type of event for the current period.
- **Average**—the average count per period of this type of event.
- **Maximum**—the maximum count per period of this type of event.

Configuring the Wi-Fi Array

The following topics include procedures for configuring the Array using the product's embedded Web Management Interface (WMI). Procedures have been organized into functional areas that reflect the [flow and content](#) of the WMI.

The following WMI windows allow you to establish configuration parameters for your Array, and include:

- [“Express Setup” on page 139](#)
- [“Network” on page 146](#)
- [“Services” on page 156](#)
- [“VLANs” on page 171](#)
- [“Security” on page 175](#)
- [“SSIDs” on page 208](#)
- [“Groups” on page 228](#)
- [“IAPs” on page 234](#)
- [“WDS” on page 278](#)
- [“Filters” on page 283](#)
- [“Clusters” on page 289](#)

After making changes to the configuration settings of an Array you must click on the **Save changes to flash** button at the top of the configuration window, otherwise the changes you make will not be applied the next time the Array is rebooted.



*Some settings are only available if the Array's license includes appropriate Xirrus **Advanced Feature Sets**. If a setting is unavailable (grayed out), then your license does not support the feature. See [“About Licensing and Upgrades” on page 297](#).*

Note that the **Configuration** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See [Figure 39 on page 80](#).)

This chapter only discusses using the configuration windows on the Array. To view status or use system tools on the Array, please see:

- [“Viewing Status on the Wi-Fi Array” on page 85](#)
- [“Using Tools on the Wi-Fi Array” on page 295](#)

Express Setup

Use the Express Setup page to establish global configuration settings that enable basic Array functionality. Any changes you make in this window will affect all radios. When finished, click **Save changes to flash** if you wish to make your changes permanent.

| XR4820 Wi-Fi Array | | XIRRUS |
|--------------------------------------|---|--|
| Name: XR4012601C5B6 (10.100.54.55) | | Uptime: 5 days, 14 hours, 32 mins |
| Status | | |
| Array | Host Name: | XR4012601C5B6 |
| Network | Location Information: | |
| RF Monitor | Admin Contact: | |
| Stations | Admin Email: | |
| Statistics | Admin Phone: | |
| System Log | SNMPv2 Settings | |
| IDS Event Log | Enable SNMPv2: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Configuration | Read-Only Community String: | ***** |
| Express Setup | Read-Write Community String: | ***** |
| Network | Gigabit Ethernet 1 Settings | |
| Services | Enable Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| VLANs | Allow Management On Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Security | Configuration Server Protocol: | <input type="radio"/> DHCP <input checked="" type="radio"/> Static |
| SSIDs | IP Address: | 10.100.54.55 |
| Groups | IP Subnet Mask: | 255.255.255.0 |
| IAPs | Default Gateway: | 10.100.54.1 |
| WDS | Gigabit Ethernet 2 Settings | |
| Filters | Enable Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Clusters | Allow Management On Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Tools | Configuration Server Protocol: | <input type="radio"/> DHCP <input checked="" type="radio"/> Static |
| Help | IP Address: | 10.100.54.55 |
| System Tools | IP Subnet Mask: | 255.255.255.0 |
| CLI | Default Gateway: | 10.100.54.1 |
| Options | SSID Settings | |
| Logout | SSID (Wireless Network Name): | |
| Log Messages | Wireless Security: | Open |
| Critical 81 | <input type="button" value="Apply SSID Settings"/> | |
| Warning 81 | Admin Settings | |
| Information 242 | New Admin User (Replaces user "admin"): | |
| | New Admin Privilege Level: | 1 read-write |
| | New Admin Password: | |
| | Confirm Admin Password: | |
| | <input type="button" value="Apply Admin Settings"/> | |
| | Time and Date Settings | |
| | Current Array Date and Time: | Mon Aug 08 2011 11:21:19 |
| | Time Zone: | (GMT) Greenwich Mean Time: Dublin, Lisbon, London |
| | Auto Adjust Daylight Savings: | <input type="checkbox"/> |
| | Use Network Time Protocol: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| | Adjust Time (hrs:min:sec): | 11 : 20 : 48 AM <input type="button" value="Set Time"/> |
| | Adjust Date (month/day/year): | 08 / 08 / 2011 <input type="button" value="Set Date"/> |
| | IAP Settings | |
| | Enable/Configure All IAPs: | <input type="button" value="Execute"/> |

Figure 87. WMI: Express Setup

Procedure for Performing an Express Setup

1. **Host Name:** Specify a unique [host name](#) for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is Xirrus-WiFi-Array.
2. **Location Information:** Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
3. **Admin Contact:** Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
4. **Admin Email:** Enter the email address of the admin contact you entered in Step 3.
5. **Admin Phone:** Enter the telephone number of the admin contact you entered in Step 3.
6. **Configure SNMP:** Select whether to **Enable SNMPv2** on the Array, and set the SNMPv2 community strings. The factory default value for the **Read-Only Community String** is `xirrus_read_only`. The factory default value for the **Read-Write Community String** is `xirrus`. If you are using the Xirrus Management System (XMS), the read-write string must match the string used by XMS. XMS also uses the default value `xirrus`.
7. **Configure the Gigabit Ethernet 1 and Gigabit Ethernet 2 network interface settings.** Please see [“Network Interfaces” on page 147](#) for more information.

The fields for each of these interfaces are similar, and include:

- a. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.
- b. **Allow Management on Interface:** Choose **Yes** to allow management of the Array via this Gigabit interface, or choose **No** to deny all management privileges for this interface.

network. WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

- **WPA (Wi-Fi Protected Access)**—A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1x for authentication. WPA is the stronger of the two wireless security schemes.
- **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.
- **WPA-Both (WPA and WPA2)**—This option makes use of both WPA and WPA2.

For more information about security, including a full review of all security options and settings, go to [“Understanding Security”](#) on page 176.

- WEP Encryption Key/Passphrase:** Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase. This field and the one below only appear if you select a **Wireless Security** option other than **Open**.
- Confirm Encryption Key/Passphrase:** If you entered a WEP key or WPA passphrase, confirm it here.
- Click **Apply SSID Settings** when done.

9. **Admin Settings:** This section allows you to change the default admin username, password, and privileges for the Array. You may change the password and leave the user name as is, but we suggest that you change both to improve Array security.
 - a. **New Admin User (Replaces user “admin”):** Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the Array also offers the option of authenticating administrators using a RADIUS server (see [“Admin Management” on page 181](#))).
 - b. **New Admin Privilege Level:** By default, the new administrator will have read/write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see [“Admin Privileges” on page 183](#). Take care to make sure to leave yourself enough read/write privileges on at least one account to be able to administer the Array.
 - c. **New Admin Password:** Enter a new administration password for managing this Array. If you forget this password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
 - d. **Confirm Admin Password:** If you entered a new administration password, confirm the new password here.
 - e. Click **Apply Admin Settings** when done.
10. **Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you’re not using a server.
 - a. **Current Array Date and Time:** This read-only field shows the current time for your convenience.
 - b. **Time Zone:** Select your time zone from the choices available in the pull-down list.

- c. **Auto Adjust Daylight Savings:** If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
- d. **Use Network Time Protocol:** Check this box if you want to use an NTP server to synchronize the Array's clock. Use of NTP is mandatory for Arrays to be managed with XMS (the Xirrus Management System), and ensures that Syslog time-stamping is maintained across all units. Without using an NTP server (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies. If you select **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, select **No** (default) and set the system time on the Array manually.
- e. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
- f. **NTP Primary Authentication:** (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default). For more information on authenticated NTP, see "Time Settings (NTP)" on page 157.
- g. **NTP Primary Authentication Key ID:** Enter the key ID, which is a decimal integer.
- h. **NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- i. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.
- j. **Adjust Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes,

seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).

- k. Adjust Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, the date fields become active. Enter the revised date (month, day and year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).

11. IAP Settings:

Enable/Configure All IAPs: Click on the **Execute** button to enable and auto configure all IAPs (a message displays the countdown time—in seconds—to complete the auto-configuration task). When an IAP is enabled, its LED is switched on.

- 12. Click **Save changes to flash** to make your changes permanent, i.e., these settings will still be in effect after a reboot.

Network

This is a status-only window that provides a snapshot of the configuration settings currently established for the **Gigabit 1** and **Gigabit 2** interfaces. **DNS Settings** and **CDP Settings** (Cisco Discovery Protocol) are summarized as well. You must go to the appropriate configuration window to make changes to any of the settings displayed here (configuration changes cannot be made from this window). You can click on any item in the **Interface** column to “jump” to the associated configuration window.

| XR4820 Wi-Fi Array | | | | | | | | | | | | | | | |
|--|---------|------|----------|----------|------|--------|--------------|------------------------|-------------|-----------------------------|--------------|---------------|-------------|------------------------------------|--|
| Status | | | | | | | | | | Name: XR4820 (10.100.57.54) | | | | Uptime: 30 days, 17 hours, 10 mins | |
| Configuration | | | | | | | | | | | | | | | |
| Express Setup Save changes to flash | | | | | | | | | | | | | | | |
| Interface Settings Summary | | | | | | | | | | | | | | | |
| Interface | State | Mgmt | Auto Neg | LED | Link | Duplex | Speed (Mbps) | MTU Size | Port Mode | DHCP | IP Address | Subnet Mask | Gateway | | |
| gig1 | enabled | on | on | on | up | full | 1000 | 1500 | link-backup | enabled | 10.100.57.54 | 255.255.255.0 | 10.100.57.2 | | |
| gig2 | enabled | on | on | on | down | | | 1500 | link-backup | enabled | 10.100.57.54 | 255.255.255.0 | 10.100.57.2 | | |
| DNS Settings Summary | | | | | | | | | | | | | | | |
| Services | | | | Hostname | | Domain | | DNS Server 1 | | DNS Server 2 | | DNS Server 3 | | | |
| VLANs | | | | XR4820 | | | | pmrox.net 10.100.57.11 | | | | | | | |
| CDP Settings Summary | | | | | | | | | | | | | | | |
| Security | | | | State | | | | Interval | | | | Hold Time | | | |
| SSIDs | | | | Enabled | | | | 60 | | | | 180 | | | |
| Groups | | | | | | | | | | | | | | | |

Figure 88. Network Interfaces

WMI windows that allow you to change or view configuration settings associated with the network interfaces include:

- [“Network Interfaces” on page 147](#)
- [“DNS Settings” on page 153](#)
- [“CDP Settings” on page 154](#)

See Also

[DNS Settings](#)
[Network Interfaces](#)
[Network Status Windows](#)
[Spanning Tree Status](#)
[Network Statistics](#)

Network Interfaces

This window allows you to establish configuration settings for the Gigabit 1 and Gigabit 2 interfaces.

XR4820 Wi-Fi Array

| Status | Name: XR4820 (10.100.57.54) | Uptime: 30 days, 17 hours, 6 mins |
|-----------------------------|----------------------------------|---|
| Configuration | | |
| Save changes to flash | | |
| Express Setup | | |
| Gigabit Ethernet 1 Settings | | |
| Network | Enable Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Interfaces | LED Indicator: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| DNS | Allow Management On Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| CDP | Auto Negotiate: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Services | Duplex: | <input checked="" type="radio"/> Full <input type="radio"/> Half |
| VLANs | Maximum Transmission Unit (MTU): | 1500 |
| Security | Speed: | Gigabit |
| SSIDs | Port Mode: | Active backup (gig ports fail over to each other) |
| Groups | Configuration Server Protocol: | <input checked="" type="radio"/> DHCP <input type="radio"/> Static |
| IAPs | IP Address: | 10.100.57.54 |
| WDS | IP Subnet Mask: | 255.255.255.0 |
| Filters | Default Gateway: | 10.100.57.2 |
| Clusters | Gigabit Ethernet 2 Settings | |
| Tools | Enable Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Help | LED Indicator: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| System Tools | Allow Management On Interface: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| CLI | Auto Negotiate: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Options | Duplex: | <input checked="" type="radio"/> Full <input type="radio"/> Half |
| Logout | Maximum Transmission Unit (MTU): | 1500 |
| Log Messages | Speed: | 10 Megabit |
| Critical 156 | Port Mode: | Active backup (gig ports fail over to each other) |
| Warning 159 | Configuration Server Protocol: | <input checked="" type="radio"/> DHCP <input type="radio"/> Static |
| Information 362 | IP Address: | 10.100.57.54 |
| | IP Subnet Mask: | 255.255.255.0 |
| | Default Gateway: | 10.100.57.2 |

Figure 89. Network Settings

When finished making changes, click **Save changes to flash** if you wish to make your changes permanent. When the status of a port changes, a Syslog entry is created describing the change.

Procedure for Configuring the Network Interfaces

Configure the **Gigabit** network interfaces. The fields for each of these interfaces are the same, and include:

1. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.
2. **LED Indicator:** Choose **Enabled** to allow the LED for this interface to blink with traffic on the port, or choose **Disabled** to turn the LED off. The LED will still light during the boot sequence, then turn off. This option is only available for the Gigabit interfaces.
3. **Allow Management on Interface:** Choose **Yes** to allow management of this Array via the selected network interface, or choose **No** to deny all management privileges for this interface.
4. **Auto Negotiate:** This feature allows the Array to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available).
 - a. **Duplex:** Full-duplex mode transmits data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). Half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.!
 - b. **Speed:** If the Auto-Negotiate feature is disabled, you must manually choose the desired data transmission speed from the pull-down list. If configuring the Fast Ethernet interface the options are **10 Megabit** or **100 Megabit**. If configuring the Gigabit 1 or Gigabit 2 interfaces the options are **100 Megabit** or **Gigabit**.
5. **Port mode:** Select the desired behavior for the gigabit Ethernet ports from the following options. For a more detailed discussion of the use of the Gigabit ports and the options below, please see the *Xirrus Gigabit Ethernet Port Modes Application Note* in the [Xirrus Library](#).
 - a. **Active Backup (gig1/gig2 failover to each other)**—This mode provides fault tolerance and is the default mode. Gigabit 1 acts as the

primary link. Gigabit2 is the backup link and is passive. Gigabit2 assumes the IP properties of Gigabit1. If Gigabit 1 fails the Array automatically fails over to Gigabit2. When a failover occurs in this mode, Gigabit2 issues gratuitous ARPs to allow it to substitute for Gigabit1 at Layer 3 as well as Layer 2. See [Figure 90 \(a\)](#).

- b. Aggregate Traffic from gig1 & gig2 using 802.3ad**—The Array sends network traffic across both gigabit ports to increase link speed to the network. Both ports act as a single logical interface (trunk), using a load balancing algorithm to balance traffic across the ports. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. If the packet is a fragment or not TCP or UDP, the source and destination IP addresses are used to do the calculation. If the packet is TCP or UDP over IP then the source IP address, destination IP address, source port number and destination port number are all used to do the calculation. The network switch must also support 802.3ad. If a port fails, the trunk degrades gracefully—the other port still transmits. See [Figure 90 \(b\)](#).

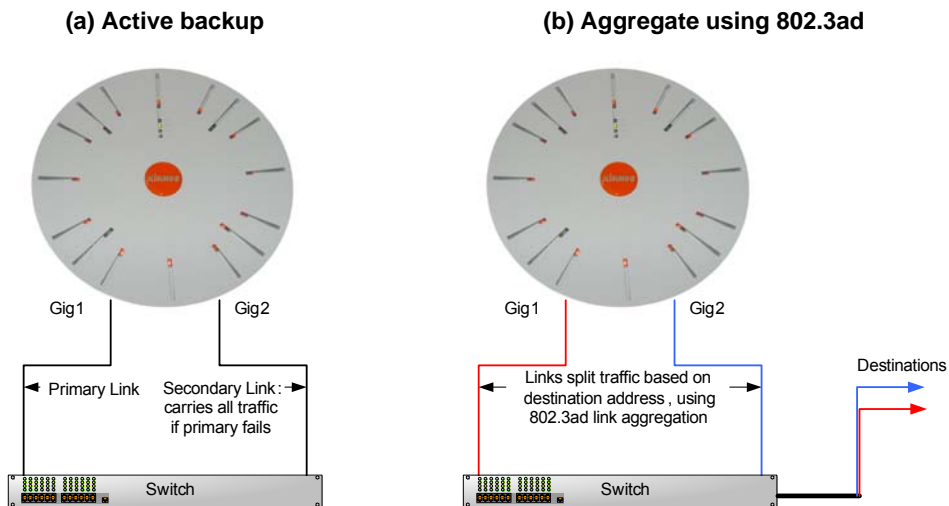


Figure 90. Port Modes (a-b)

- c. **Bridge traffic between gig1 & gig2**—Traffic received on Gigabit1 is transmitted by Gigabit2; similarly, traffic received on Gigabit2 is transmitted by Gigabit1. This allows the Array to act as a wired bridge and allows Arrays to be daisy-chained and still maintain wired connectivity. See Figure 91 (c).
- d. **Transmit Traffic on both gig1 & gig2**—Transmits incoming traffic on both Gigabit1 and Gigabit2. Any traffic received on Gigabit1 or Gigabit2 is sent to the onboard processor. This mode provides fault tolerance. See Figure 91 (d).

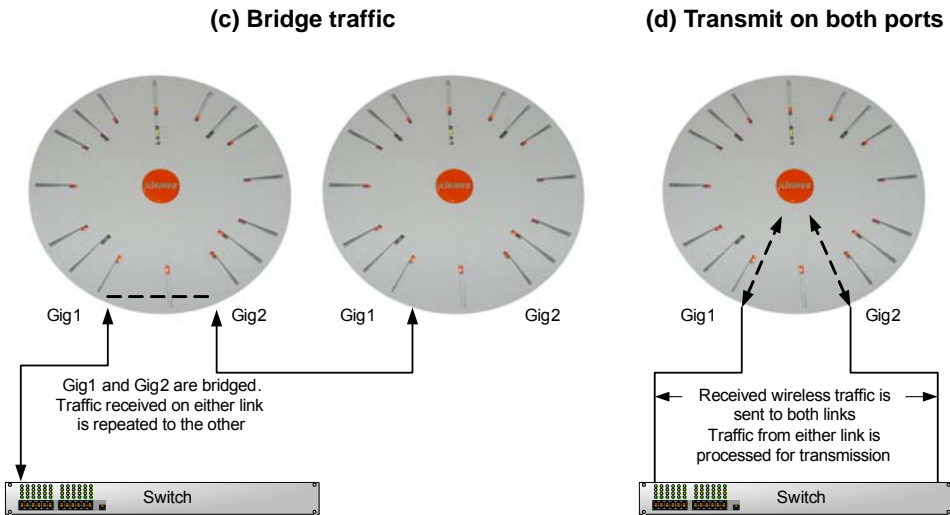
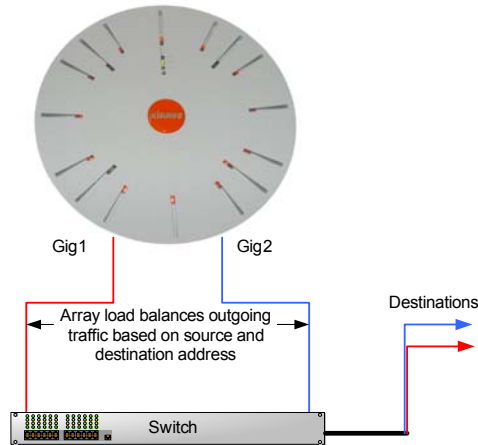


Figure 91. Port Modes (c-d)

- e. **Load balance traffic between gig1 & gig2**—This option provides trunking, similar to option (b)—**Aggregate Traffic from gig1 & gig2 using 802.3ad**, but it uses a different load balancing algorithm to determine the outgoing gigabit port. The outgoing port used is based on an exclusive OR of the source and destination MAC address. Like option (b), this mode also provides load balancing and fault tolerance. See Figure 92 (e).

(e) Load balance traffic



(f) Mirror traffic

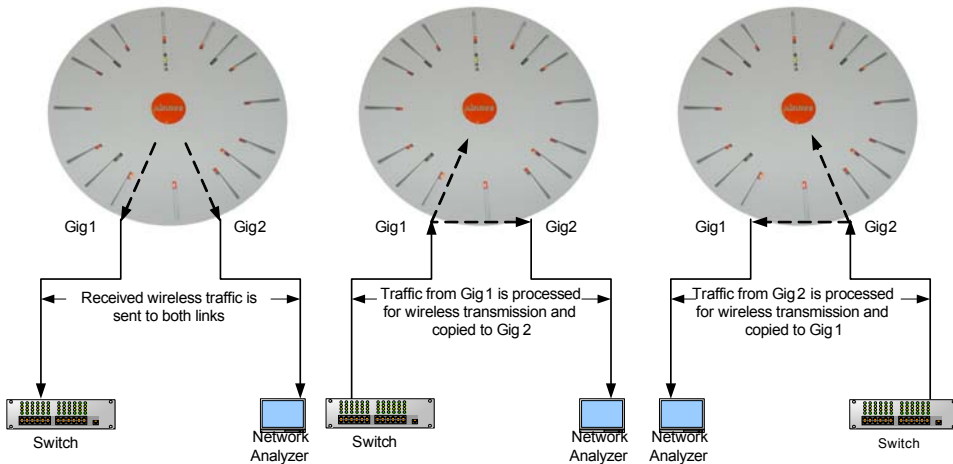


Figure 92. Port Modes (e-f)

- f. **Mirror traffic on both gig1 & gig2**—all traffic received on the Array is transmitted out both Gigabit1 and Gigabit2. All traffic received on Gigabit1 is passed on to the onboard processor as well as out Gigabit2. All traffic received on Gigabit2 is passed on to the onboard

processor as well as out Gigabit1. This allows a network analyzer to be plugged into one port to capture traffic for troubleshooting, while the other port provides network connectivity for data traffic. See Figure 92 (f).

6. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** when assigning IP addresses to the Array, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.
 - a. **IP Address:** If you selected the Static IP option, enter a valid IP address for the Array. To use any of the remote connections (Web, **SNMP**, or **SSH**), a valid IP address must be established.
 - b. **IP Subnet Mask:** If you selected the Static IP option, enter a valid IP address for the **subnet mask** (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
 - c. **Default Gateway:** If you selected the Static IP option, enter a valid IP address for the **default gateway**. This is the IP address of the router that the Array uses to transmit data to other networks.
7. When done configuring all interfaces as desired, click **Save changes to flash** if you wish to make your changes permanent.

See Also

[DNS Settings](#)

[Network](#)

[Network Statistics](#)

[Spanning Tree Status](#)

DNS Settings

This window allows you to establish your **DNS** (Domain Name System) settings. The Array uses these DNS servers to resolve host names into IP addresses. The Array also registers its own Host Name with these DNS servers, so that others may address the Array using its name rather than its IP address. An option allows you to specify that the Array's DNS servers will be assigned via a DHCP server on the wired network.

Note that the DNS servers defined here are not used by wireless clients—servers for stations associated to the Array are defined along with DHCP pools. See “[DHCP Server](#)” on page 168. At least one DNS server must be set up if you want to offer clients associating with the Array the ability to use meaningful host names instead of numerical IP addresses. When finished, click **Save changes to flash** if you wish to make your changes permanent.

| Status | Name: SS-XN0429091D207 | | Uptime: 5 days, 20 hours, 53 mins |
|----------------------|--|---|-----------------------------------|
| ▶ Array | DNS Hostname: | <input type="text" value="SS-XN0429091D207"/> | |
| ▶ Network | DNS Domain: | <input type="text" value="xirrus.com"/> | |
| ▶ RF Monitor | DNS Server 1: | <input type="text" value="10.100.1.10"/> | |
| ▶ Stations | DNS Server 2: | <input type="text" value="10.100.2.10"/> | |
| ▶ Statistics | DNS Server 3: | <input type="text"/> | |
| System Log | Use DNS settings assigned by DHCP | <input checked="" type="radio"/> On <input type="radio"/> Off | |
| Configuration | | | |
| Express Setup | <input type="button" value="Apply"/> <input type="button" value="Save"/> | | |
| ▶ Network | | | |
| Interlaces | | | |
| DNS | | | |

Figure 93. DNS Settings

Procedure for Configuring DNS Servers

1. **DNS Host Name:** Enter a valid DNS **host name**.
2. **DNS Domain:** Enter the DNS **domain** name.
3. **DNS Server 1:** Enter the IP address of the primary DNS server.
4. **DNS Server 2 and DNS Server 3:** Enter the IP address of the secondary and tertiary DNS servers (if required).

5. **Use DNS settings assigned by DHCP:** If you are using DHCP to assign the Array’s IP address, you may turn this option **On**. The Array will then obtain its DNS domain and server settings from the network DHCP server that assigns an IP address to the Array, rather than using the DNS Server fields above. You may also configure that DHCP server to assign a host name to the Array.
6. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

- DHCP Server
- Network
- Network Interfaces
- Network Statistics
- Spanning Tree Status

CDP Settings

CDP (Cisco Discovery Protocol) is a layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Wi-Fi Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors (see “CDP Neighbors” on page 100).

This window allows you to establish your CDP settings. When finished, **Save changes to flash** if you wish to make your changes permanent.

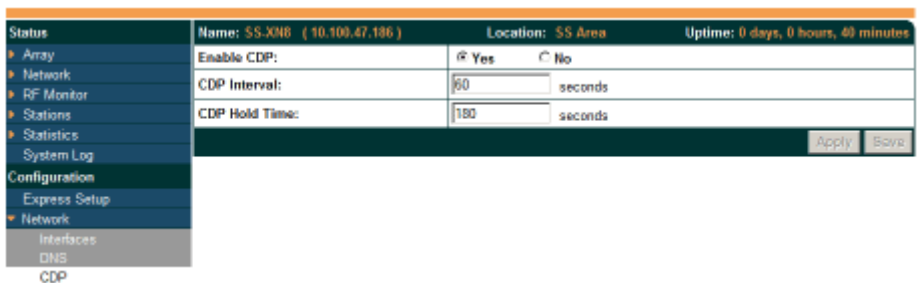


Figure 94. CDP Settings

Procedure for Configuring CDP Settings

1. **Enable CDP:** When CDP is enabled, the Array sends out CDP announcements of the Array's presence, and gathers CDP data sent by neighbors. When disabled, it does neither. CDP is enabled by default.
2. **CDP Interval:** The Array sends out CDP announcements advertising its presence at this interval. The default is 60 seconds.
3. **CDP Hold Time:** CDP information received from neighbors is retained for this period of time before aging out of the Array's neighbor list. Thus, if a neighbor stops sending announcements, it will no longer appear on the [CDP Neighbors](#) window after CDP Hold Time seconds from its last announcement. The default is 180 seconds.

See Also

[CDP Neighbors](#)

[Network](#)

[Network Interfaces](#)

[Network Statistics](#)

Services

This is a status-only window that allows you to review the current settings and status for services on the Array, including DHCP, SNMP, Syslog, and Network Time Protocol (NTP) services. For example, for the DHCP server, it shows each DHCP pool name, whether the pool is enabled, the IP address range, the gateway address, lease times, and the DNS domain being used. There are no configuration options available in this window, but if you are experiencing issues with network services, you may want to print this window for your records.

| Status | Name: XR4820 (10.100.57.54) | | | | | | | | | | Uptime: 30 days, 17 hours, 29 mins | | | |
|---------------|-----------------------------|---------|-------------|--------------------|----------------------|---------------|----------------|------------|----------------------|--------------|------------------------------------|----------|----------------|--|
| Configuration | Save changes to flash | | | | | | | | | | | | | |
| Express Setup | Time Settings Summary | | | | | | | | | | | | | |
| Network | NTP Server Status | | | | NTP Server 1 Address | | | | NTP Server 2 Address | | | | | |
| Services | Enabled | | | | | | | | | | | | | |
| Time | Netflow Summary | | | | | | | | | | | | | |
| Netflow | State | | | | Collector Host | | | | Collector Port | | | | | |
| WIFI Tag | Disabled | | | | | | | | | | | | | |
| System Log | System Log Settings Summary | | | | | | | | | | | | | |
| SNMP | Log Levels | | | | | | | | | | Log Servers | | | |
| DHCP Server | State | Console | Local Lines | Console | Local | 1st | 2nd | 3rd | Email | Primary | Secondary | Tertiary | Email | |
| | on | off | 2000 | 6 | 7 | 7 | 6 | 6 | 4 | 10.100.57.13 | | | | |
| VLANs | SNMP Settings Summary | | | | | | | | | | | | | |
| Security | SNMPv2 State | | | Trap Auth Failures | | | Trap Host IP 1 | | Trap Host IP 2 | | Trap Host IP 3 | | Trap Host IP 4 | |
| SSIDs | Enabled | | | Enabled | | | Xirus-XMS | | | | | | | |
| Groups | SNMPv3 State | | | SNMPv3 Security | | | Trap Port 1 | | Trap Port 2 | | Trap Port 3 | | Trap Port 4 | |
| IAPs | Disabled | | | sha / aes | | | 162 | | 162 | | 162 | | 162 | |
| WDS | DHCP Server Settings | | | | | | | | | | | | | |
| Filters | DHCP Name | State | NAT | IP Range/Mask | IP Gateway | Default Lease | Maximum Lease | DNS Domain | | | | | | |
| Clusters | WIFI Tag Summary | | | | | | | | | | | | | |
| Tools | State | | | | UDP Port | | | | Tag Channel BG | | | | | |
| | Disabled | | | | 1144 | | | | 0 | | | | | |

Figure 95. Services

The following sections discuss configuring services on the Array:

- “Time Settings (NTP)” on page 157
- “NetFlow” on page 159
- “Wi-Fi Tag” on page 161
- “System Log” on page 162
- “SNMP” on page 165
- “DHCP Server” on page 168

Time Settings (NTP)

This window allows you to manage the Array's time settings, including synchronizing the Array's clock with a universal clock from an NTP (Network Time Protocol) server. We recommend that you use NTP for proper operation of SNMP in XMS (the Xirrus Management System), since a lack of synchronization will cause errors to be detected. Synchronizing the Array's clock with an NTP server also ensures that Syslog time-stamping is maintained across all units.

It is possible to use authentication with NTP to ensure that you are receiving synchronization from a known source. For example, the instructions for requesting a key for the NIST Authenticated NTP server are available at http://www.nist.gov/pml/div688/grp00/upload/ntp_instructions.pdf.

The Array allows you to enter optional authentication information.

| Status | Name: SS-XN0429091D207 (10.100.47.16) Uptime: 2 days, 7 hours, 51 mins | |
|---------------|--|---|
| Array | Current Array Date and Time: | Sat Mar 13 2010 02:30:29 |
| Network | TimeZone: | [(GMT) Greenwich Mean Time: Dublin, Lisbon, London] |
| RF Monitor | Auto Adjust Daylight Savings: | <input type="checkbox"/> |
| Stations | Use Network Time Protocol: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Statistics | Adjust Time (hrs:min:sec): | <input type="checkbox"/> 2 : 22 : 17 AM |
| System Log | Adjust Date (month/day/year): | <input type="checkbox"/> 3 / 13 / 2010 |
| Configuration | Apply Save | |
| Express Setup | | |
| Network | | |
| Services | | |
| Time | | |

Figure 96. Time Settings (Manual Time)

Procedure for Managing the Time Settings

- 1. Current Array Date and Time:** Shows the current time for your convenience.
- 2. Time Zone:** Select the time zone you want to use (normally your local time zone) from the pull-down list.
- 3. Auto Adjust Daylight Savings:** Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).

4. **Use Network Time Protocol:** select whether to set time manually or use NTP to manage system time.
5. **Setting Time Manually**
 - a. **Adjust Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, you may enter a revised time (hours, minutes, seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).
 - b. **Adjust Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, you may enter a revised date (month, day and year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).
6. **Using an NTP Server**
 - a. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.

| Status | Name: SS-XH4 (192.168.1.74) | | Location: 12-125 | Uptime: 1 days, 0 hours, 5 mins |
|----------------------|--------------------------------------|---|--------------------------|---------------------------------|
| Configuration | Save changes to flash | | | |
| Express Setup | Current Array Date and Time: | | Fri Jul 08 2011 15:13:41 | |
| ▶ Network | Time Zone: | (GMT + 08:00) Beijing, Chongqing, Hong Kong | | |
| ▼ Services | Auto Adjust Daylight Savings: | <input checked="" type="checkbox"/> | | |
| Time | Use Network Time Protocol: | <input checked="" type="radio"/> Yes <input type="radio"/> No | | |
| Netflow | NTP Primary Server: | ntp.xirus.com | | |
| WiFi Tag | NTP Primary Authentication: | None | | |
| System Log | NTP Primary Authentication Key ID: | 1 | | |
| SNMP | NTP Primary Authentication Key: | | | |
| DHCP Server | NTP Secondary Server: | | | |
| ▶ VLANs | NTP Secondary Authentication: | None | | |
| ▶ Security | NTP Secondary Authentication Key ID: | 2 | | |
| ▶ SSIDs | NTP Secondary Authentication Key: | | | |

Figure 97. Time Settings (NTP Time Enabled)

- b. **NTP Primary Authentication:** (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default).

- c. **NTP Primary Authentication Key ID:** Enter the key ID, which is a decimal integer.
- d. **NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- e. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

See Also

[Express Setup](#)

[Services](#)

[SNMP](#)

[System Log](#)

NetFlow

This window allows you to enable or disable the sending of NetFlow information to a designated collector. NetFlow is a proprietary but open network protocol developed by Cisco Systems for collecting IP traffic information. When NetFlow is enabled, the Array will send IP flow information (traffic statistics) to the designated collector.

NetFlow sends per-flow network traffic information from the Array. Network managers can use a NetFlow collector to view the statistics on a per-flow basis and use this information to make key decisions. Knowing how many packets and bytes are sent to and from certain IP addresses or across specific network interfaces allows administrators to track usage by various areas. Traffic flow information may be used to engineer networks for better performance.

| Status | Name: SS-XN0429091D207 (10.100.47.16) | | Uptime: 0 days, 2 hours, 43 mins |
|----------------------|--|--|----------------------------------|
| ▶ Array | Enable Netflow: | <input checked="" type="radio"/> Yes | <input type="radio"/> No |
| ▶ Network | Netflow Collector Host: | <input type="text" value="100.100.100.100"/> | |
| ▶ RF Monitor | Netflow Collector Port: | <input type="text" value="2055"/> | |
| ▶ Stations | <input type="button" value="Apply"/> <input type="button" value="Save"/> | | |
| ▶ Statistics | | | |
| System Log | | | |
| Configuration | | | |
| Express Setup | | | |
| ▶ Network | | | |
| ▼ Services | | | |
| Time | | | |
| Netflow | | | |
| WiFi Tag | | | |

Figure 98. NetFlow



Some features, such as Netflow, are only available if the Array's license includes the *Xirrus Advanced RF Analysis Manager (RAM)*. If a setting is unavailable (grayed out), then your license does not support the feature. See *"About Licensing and Upgrades"* on page 297.

Procedure for Configuring NetFlow

1. **Enable NetFlow:** Choose **Yes** to enable NetFlow functionality, or choose **No** to disable this feature.
2. **NetFlow Collector Host (Domain or IP):** If you enabled NetFlow, enter the domain name or IP address of the collector.
3. **NetFlow Collector Port:** If you enabled NetFlow, enter the port on the collector host to which to send data.

Wi-Fi Tag

This window allows you to enable or disable Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channel. These tags are transmitted by specialized tag devices (for example, AeroScout Tags). A Wi-Fi tagging server (such as AeroScout) then queries the Array for a report on the tags that it has received. The Wi-Fi tagging server uses proprietary algorithms to determine locations for devices sending tag signals.

| Status | Name: SS-XM4 (10.100.47.16) | Location: map5 | Uptime: 7 days, 5 hours, 13 mins |
|------------|-------------------------------|-----------------------------------|--|
| Array | Enable WiFi Tag Support: | <input type="radio"/> Yes | <input checked="" type="radio"/> No |
| Network | WiFi Tag UDP Port: | <input type="text" value="1144"/> | |
| RF Monitor | WiFi Tag Channel BG: | <input type="text" value="0"/> | |
| Stations | | | <input type="button" value="Apply"/> <input type="button" value="Save"/> |

Figure 99. Wi-Fi Tag

Procedure for Configuring Wi-Fi Tag

- 1. Enable Wi-Fi Tag:** Choose **Yes** to enable Wi-Fi tag functionality, or choose **No** to disable this feature.
- 2. Wi-Fi Tag UDP Port:** If you enabled Wi-Fi tagging, enter the port on the Array which the Wi-Fi tagging server will use to query the Array for tagging data. When queried, the Array will send back information on the tags it has observed. For each, the Array sends information such as the MAC address of the tag transmitting device, and the RSSI and noise floor observed.
- 3. Wi-Fi Tag Channel:** If you enabled Wi-Fi tagging, enter the 802.11 channel on which the Array will listen for tags. The tag devices must be set up to transmit on this channel. Only one channel may be configured, and it must be an 802.11b/g channel in the range of Channel 1 to 11.

System Log

This window allows you to enable or disable the Syslog server, define primary, secondary, and tertiary servers, set up email notification, and set the level for Syslog reporting for each of the servers and for email notification—the Syslog service will send Syslog messages that are at the selected severity or above to the defined Syslog servers and email address.

| Status | Name: SS-XN0429091D207 (10.100.47.16) | | Uptime: 0 days, 2 hours, 51 mins |
|----------------------|--|--------------------------------------|-------------------------------------|
| Array | Enable Syslog Server: | <input checked="" type="radio"/> Yes | <input type="radio"/> No |
| Network | Console Logging: | <input type="radio"/> Yes | <input checked="" type="radio"/> No |
| RF Monitor | Local File Size (1-500): | <input type="text" value="500"/> | |
| Stations | Primary Server Address (Domain or IP): | <input type="text"/> | |
| Statistics | Secondary Server Address (Domain or IP): | <input type="text"/> | |
| System Log | Tertiary Server Address (Domain or IP): | <input type="text"/> | |
| Configuration | Email SMTP Address (Domain or IP): | <input type="text"/> | |
| Express Setup | Email SMTP User: | <input type="text"/> | |
| Network | Email SMTP Password: | <input type="text"/> | |
| Services | Email SMTP From: | <input type="text"/> | |
| Time | Email SMTP To: | <input type="text"/> | |
| Netflow | Syslog Levels | | |
| WiFi Tag | Console Logging: | information and more serious ▾ | |
| System Log | Local File: | information and more serious ▾ | |
| SNMP | Primary Server: | information and more serious ▾ | |
| DHCP Server | Secondary Server: | information and more serious ▾ | |
| VLANs | Tertiary Server: | information and more serious ▾ | |
| Security | Email SMTP Server: | warning and more serious ▾ | |
| SSIDs | <input type="button" value="Apply"/> <input type="button" value="Save"/> | | |
| Groups | | | |
| WPs | | | |

Figure 100. System Log

Procedure for Configuring Syslog

- 1. Enable Syslog Server:** Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.
- 2. Console Logging:** If you enabled Syslog, select whether or not to echo Syslog messages to the console as they occur. If you enable console logging, be sure to set the Console Logging level (see [Step 7](#) below).
- 3. Local File Size (1-500):** Enter a value in this field to define how many Syslog records are retained locally on the Array’s internal Syslog file. The default is 500.

4. **Primary Server Address (Domain or IP):** If you enabled Syslog, enter the domain name or IP address of the primary Syslog server.
5. **Secondary/Tertiary Server Address (Domain or IP):** If you enabled Syslog, you may enter the domain name or IP address of one or two additional Syslog servers to which messages will also be sent. (Optional)
6. **Email Notification:** The following parameters allow you to send an email to a designated address each time a Syslog message is generated. The email will include the text of the Syslog message.
 - a. **Email SMTP Address (Domain or IP):** The domain name or the IP address of the SMTP server to be used for sending the email. Note that this specifies the mail server, **not** the email recipient.
 - b. **Email SMTP User/Email SMTP Password:** Specify a user name and password for logging in to an account on the mail server designated in [Step a](#).
 - c. **Email SMTP From:** Specify the “From” email address to be displayed in the email.
 - d. **Email SMTP To:** Specify the entire email address of the recipient of the email notification.
7. **Syslog Levels:** For each of the Syslog destinations, choose your preferred level of Syslog reporting from the pull-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.
 - a. **Console Logging:** For messages to be echoed to the console, the default level is **Critical and more serious**. This prevents large numbers of non-critical messages from being displayed on the console. If you set this level too low, the volume of messages may make it very difficult to work with the CLI or view other output on the console.
 - b. **Local File:** For records to be stored on the Array’s internal Syslog file, choose your preferred level of Syslog reporting from the pull-down list. The default level is **Debugging and more serious**.

- c. **Primary Server:** Choose the preferred level of Syslog reporting for the primary server. The default level is **Debugging and more serious**.
 - d. **Secondary/Tertiary Server:** Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Information and more serious**. (Optional)
 - e. **Email SMTP Server:** Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.
8. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

System Log Window

Services

SNMP

Time Settings (NTP)

SNMP

This window allows you to enable or disable SNMP v2 and SNMP v3 and define the SNMP parameters. SNMP allows remote management of the Array by the Xirrus Management System (XMS) and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, neither, or both.

Complete SNMP details for the Array, including trap descriptions, are found in the Xirrus MIB, available at support.xirrus.com, in the **Downloads** section (login is required to download the MIB).

NOTE: If you are managing your Arrays with XMS (the Xirrus Management System), it is very important to make sure that your SNMP settings match those that you have configured for XMS. XMS uses both SNMP v2 and v3, with v3 given preference.

| | | |
|----------------------|--|---|
| Status | Name: SS-XN0429091D207 (10.100.47.16) Uptime: 0 days, 3 hours, 0 mins | |
| Array | SNMPv2 Settings | |
| Network | Enable SNMPv2: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| RF Monitor | Read-Write Community String: | •••••• |
| Stations | Read-Only Community String: | •••••••••••••••• |
| Statistics | SNMPv3 Settings | |
| System Log | Enable SNMPv3: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Configuration | Authentication: | <input checked="" type="radio"/> SHA <input type="radio"/> MD5 |
| Express Setup | Privacy: | <input checked="" type="radio"/> AES <input type="radio"/> DES |
| Network | Context Engine ID: | 8000521503000f7d14cb80 |
| Services | Read-Write Username: | xirrus-rw |
| Time | Read-Write Authentication Password: | •••••••• |
| Netflow | Read-Write Privacy Password: | •••••••• |
| WiFi Tag | Read-Only Username: | xirrus-ro |
| System Log | Read-Only Authentication Password: | •••••••• |
| SNMP | Read-Only Privacy Password: | •••••••• |
| DHCP Server | SNMP Trap Settings | |
| VLANs | Trap Host 1 IP Address: | Xirrus-XMS Port: 162 |
| Security | Trap Host 2 IP Address: | <input type="text"/> Port: 162 |
| SSIDs | Trap Host 3 IP Address: | <input type="text"/> Port: 162 |
| Groups | Trap Host 4 IP Address: | <input type="text"/> Port: 162 |
| IAPs | Send Auth Failure Traps: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| WDS | Keepalive Trap Interval: | 1 |
| Filters | <input type="button" value="Apply"/> <input type="button" value="Save"/> | |
| Clusters | | |

Figure 101. SNMP

Procedure for Configuring SNMP

SNMPv2 Settings

1. **Enable SNMPv2:** Choose **Yes** to enable SNMP v2 functionality, or choose **No** to disable this feature. When used in conjunction with the Xirrus Management System, SNMP v2 (**not** SNMP v3) must be enabled on each Array to be managed with XMS. The default for this feature is **Yes** (enabled).
2. **SNMP Read-Write Community String:** Enter the read-write community string. The default is **xirrus**.
3. **SNMP Read-Only Community String:** Enter the read-only community string. The default is **xirrus_read_only**.

SNMPv3 Settings

4. **Enable SNMPv3:** Choose **Yes** to enable SNMP v3 functionality, or choose **No** to disable this feature. The default for this feature is **Yes** (enabled).
5. **Authentication:** Select the desired method for authenticating SNMPv3 packets: **SHA** (Secure Hash Algorithm) or **MD5** (Message Digest Algorithm 5).
6. **Privacy:** Select the desired method for encrypting data: **DES** (Data Encryption Standard) or the stronger **AES** (Advanced Encryption Standard).
7. **Context Engine ID:** The unique identifier for this SNMP server. We recommend that you do not change this value. The Context Engine ID must be set if data collection is to be done via a proxy agent. This ID helps the proxy agent to identify the target agent from which data is to be collected.
8. **SNMP Read-Write Username:** Enter the read-write user name. This username and password allow configuration changes to be made on the Array. The default is **xirrus-rw**.
9. **SNMP Read-Write Authentication Password:** Enter the read-write password for authentication (i.e., logging in). The default is **xirrus-rw**.

10. **SNMP Read-Write Privacy Password:** Enter the read-write password for privacy (i.e., a key for encryption). The default is **xirrus-rw**.
11. **SNMP Read-Only Username:** Enter the read-only user name. This username and password do not allow configuration changes to be made on the Array. The default is **xirrus-ro**.
12. **SNMP Read-Only Authentication Password:** Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.
13. **SNMP Read-Only Privacy Password:** Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.

SNMP Trap Settings

14. **SNMP Trap Host IP Address:** Enter the **IP Address** or domain name, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. Note that by default, **Trap Host 1** sends traps to **Xirrus-XMS**. Thus, the Array will automatically communicate its presence to XMS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

For a definition of the traps sent by Xirrus Wi-Fi Arrays, you may download the Xirrus MIB from support.xirrus.com (login required). Search for the string **TRAP** in the MIB file.

15. **Send Auth Failure Traps:** Choose **Yes** to log authentication failure traps or **No** to disable this feature.
16. **Keepalive Trap Interval** (minutes): Traps are sent out at this interval to indicate the presence of the Array on the network. Keepalive traps are required for proper operation with XMS. To disable keepalive traps, set the value to **0**.
17. Click **Save changes to flash** if you wish to make your changes permanent.

See Also
Services

System Log
Time Settings (NTP)

DHCP Server

This window allows you to create, enable, modify and delete **DHCP** (Dynamic Host Configuration Protocol) address pools. DHCP allows the Array to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network. If you do not use the DHCP server on the Array, then your wired network must be configured to supply DHCP addresses and gateway and DNS server addresses to wireless clients.

When you create a DHCP pool, you must define the **DHCP lease time** (default and maximum), the IP address ranges (pools) that the DHCP server can assign, and the gateway address and DNS servers to be used by clients.

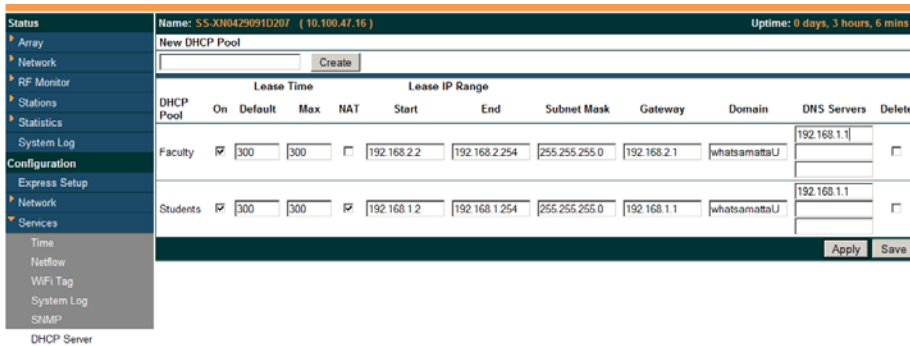


Figure 102. DHCP Management

DHCP usage is determined in several windows—see **SSID Management**, **Group Management**, and **VLAN Management**.

Procedure for Configuring the DHCP Server

1. **New Internal DHCP Pool:** Enter a name for the new DHCP pool, then click on the **Create** button. The new pool ID is added to the list of available DHCP pools.
2. **On:** Click this checkbox to make this pool of addresses available, or clear it to disable the pool.
3. **Lease Time—Default:** This field defines the default **DHCP lease** time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
4. **Lease Time—Max:** Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.
5. **Network Address Translation (NAT):** Check this box to enable the Network Address Translation feature.
6. **Lease IP Range—Start:** Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End:** Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask:** Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway:** If necessary, enter the IP address of the gateway.
10. **Domain:** Enter the DNS domain name. See “[DNS Settings](#)” on page 153.
11. **DNS Servers (1 to 3):** Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the assigned IP address. Note that if you leave these blank, no DNS information is sent to the stations. DHCP will **not** default to sending the DNS servers that are configured in DNS Settings. See also, “[DNS Settings](#)” on page 153.

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

See Also

DHCP Leases

DNS Settings

Network Map

VLANS

This is a status-only window that allows you to review the current status of assigned VLANs. A VLAN (Virtual LAN) is comprised of 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.

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN ([Step 1 page 173](#)).

| Status | | Name: SS-XNB (10.100.47.186) | | Location: SS Area | | Uptime: 0 days, 2 hours, 10 minutes | | | | | |
|-----------------|---------------------|------------------------------|--------|-------------------|----------|-------------------------------------|---------------|------------|---------------|------|-------|
| Array | Default Route VLAN: | | | | | | | | | | |
| Network | Native (Untagged): | | | | | | | | | | |
| RF Monitor | | | | | | | | | | | |
| Statistics | | | | | | | | | | | |
| System Log | | | | | | | | | | | |
| Configuration | | VLAN Name | Number | Management | DHCP | IP Address | Subnet Mask | Gateway | Tunnel Server | Port | State |
| Express Setup | VoIP | | 12 | disallowed | disabled | 10.10.10.10 | 255.255.255.0 | 10.10.10.1 | 10.10.10.8 | 0 | down |
| Network | Finance | | 5 | disallowed | enabled | | | | | | |
| Services | | | | | | | | | | | |
| VLANS | | | | | | | | | | | |
| VLAN Management | | | | | | | | | | | |

Figure 103. VLANs



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](#).

Understanding Virtual Tunnels

Xirrus Arrays support Layer 2 tunneling with Virtual Tunnels. This allows an Array to use tunnels to transport traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 core network.

The Array has low overhead and latency for virtual tunnel connections, with high resilience. The Array performs all encryption and decryption in hardware, maintaining wire-rate encryption performance on the tunnel.

Virtual Tunnel Server (VTS)

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from vtun.sourceforge.net. To enable the Array to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in [Step 10](#) on [page 174](#).

VTun may be configured for a number of different tunnel types, protocols, and encryption types. For use with Arrays, we recommend the following configuration choices:

- Tunnel Type: Ether (Ethernet tunnel)
- Protocol: UDP
- Encryption Type: select one of the encryption types supported by VTun (AES and Blowfish options are available)
- Keepalive: yes

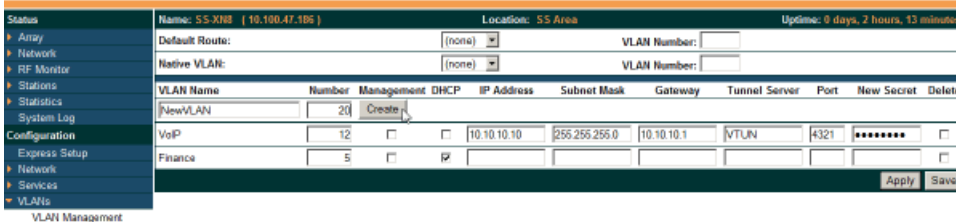
Client-Server Interaction

The Array is a client of the Virtual Tunnel Server. When you specify a VTS for an active VLAN-SSID pair, the Array contacts the VTS. The server then creates a tunnel session to the Array. VTun encapsulated packets will cross the Layer 3 network from the Array to the VTS. When packets arrive at the VTS, they will be de-encapsulated and the resultant packets will be passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction.

We recommend that you enable the VTun keep-alive option. This will send a keep-alive packet once per second to ensure that the tunnel remains active. Tunnels can be configured to come up on demand but this is a poor choice for Wi-Fi, since tunnel setup can take roughly 5-20 seconds and present a problem for authentication.

VLAN Management

This window allows you to assign and configure VLANs. After creating a new VLAN (added to the list of VLANs), you can modify the configuration parameters of an existing VLAN or delete a selected VLAN. You may create up to 32 VLANs.



| VLAN Name | Number | Management | DHCP | IP Address | Subnet Mask | Gateway | Tunnel Server | Port | New Secret | Delete |
|-----------|--------|--------------------------|-------------------------------------|-------------|---------------|------------|---------------|------|------------|--------------------------|
| NewVLAN | 20 | <input type="checkbox"/> | <input type="checkbox"/> | | | | | | | |
| VoIP | 12 | <input type="checkbox"/> | <input type="checkbox"/> | 10.10.10.10 | 255.255.255.0 | 10.10.10.1 | VLAN | 4321 | ***** | <input type="checkbox"/> |
| Finance | 5 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | | | | | | | <input type="checkbox"/> |

Figure 104. VLAN Management



The Wi-Fi Array supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Array dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Array (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (Figure 65 on page 112)

It is critical to configure all VLANs to be used on the Array, even those that will be dynamically assigned.

Procedure for Managing VLANs

1. **Default route:** This option allows you to choose a default VLAN route from the pull-down list. The VLAN you chose will appear in the corresponding VLAN Number field. The IP Gateway must be established for this function to work.
2. **Native VLAN:** This option allows you to choose the Native VLAN from the pull-down list. The VLAN you chose will appear in the corresponding VLAN Number field.

3. **New VLAN Name/Number:** Enter a name and number for the new VLAN in this field, then click on the **Create** button. The new VLAN is added to the list.
4. **VLAN Number:** Enter a number for this VLAN (1-4094).
5. **Management:** Check this box to allow management over this VLAN.
6. **DHCP:** Check this box if you want the DHCP server to assign the IP address, subnet mask and gateway address to the VLAN automatically, otherwise you must go to the next step and assign these parameters manually.
7. **IP Address:** If the DHCP option is disabled, enter a valid IP address for this VLAN association.
8. **Subnet Mask:** If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.
9. **Gateway:** If the DHCP option is disabled, enter the IP gateway address for this VLAN association.
10. **Tunnel Server:** If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see [“Understanding Virtual Tunnels”](#) on page 171.
11. **Port:** If this VLAN is to be tunneled, enter the port number of the tunnel server.
12. **New Secret:** Enter the password expected by the tunnel server.
13. **Delete:** To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.
14. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

VLAN Statistics
VLANs

Security

This status-only window allows you to review the Array’s security parameters. It includes the assigned network administration accounts, Access Control List (ACL) values, management settings, encryption and authentication protocol settings, and RADIUS configuration settings. There are no configuration options available in this window, but if you are experiencing issues with security, you may want to print this window for your records.

| Status | Name: XN0429091D207 (10.100.47.12) | Location: SS Desk | Uptime: 13 days, 5 hours, 55 mins |
|---------------------|--------------------------------------|-------------------------|-----------------------------------|
| Array | Administration | | |
| Network | Accounts | Level 0 | Level 1 |
| RF Monitor | 1 | 0 | 1 |
| Stations | Level 2 | Level 3 | Level 4 |
| Statistics | 0 | 0 | 0 |
| System Log | Level 5 | Level 6 | Level 7 |
| Configuration | 0 | 0 | 0 |
| Express Setup | Access Control List | | |
| Network | Enabled | Entries | List Type |
| Services | Yes | 2 | deny |
| VLANs | Management Control | | |
| Security | SSH Enabled | Telnet Enabled | HTTPS Enabled |
| Admin Management | Yes | No | Yes |
| Admin Privileges | Global Security | | |
| Admin RADIUS | TKIP Enabled | AES Enabled | PSK Enabled |
| Management Control | No | Yes | Yes |
| Access Control List | EAP Enabled | | |
| Global Settings | No | Yes | No |
| External Radius | RADIUS | | |
| Internal Radius | Server In Use | External Primary Server | External Primary Port |
| Rogue Control List | external | | 1812 |
| | | | Internal Radius Users |
| | | | 0 |

Figure 105. Security

For additional information about wireless network security, refer to:

- “Security Planning” on page 45
- “Understanding Security” on page 176
- The Security section of “Frequently Asked Questions” on page 404.

For information about secure use of the WMI, refer to:

- “Certificates and Connecting Securely to the WMI” on page 179
- “Using the Array’s Default Certificate” on page 180

- “Using an External Certificate Authority” on page 181
- “About Creating Admin Accounts on the RADIUS Server” on page 185
- “About Creating User Accounts on the RADIUS Server” on page 201

Security settings are configured with the following windows:

- “Admin Management” on page 181
- “Admin Privileges” on page 183
- “Admin RADIUS” on page 185
- “Management Control” on page 188
- “Access Control List” on page 195
- “Global Settings” on page 197
- “External Radius” on page 200
- “Internal Radius” on page 204
- “Rogue Control List” on page 206

Understanding Security

The Xirrus Wi-Fi Array incorporates many configurable security features. After initially installing an Array, always change the default administrator password (the default is admin), and choose a strong replacement password (containing letters, numbers and special characters). When appropriate, issue read-only administrator accounts.

Other security considerations include:

- **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 version 2 (SSH-2) utility. SSH-2 provides stronger security than SSH-1. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing:** The optional Xirrus Management System (XMS) offers powerful management features for small or large Xirrus Wi-Fi deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.

- **Choosing an encryption method:** Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The 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) and WPA2**—these are much stronger encryption modes than WEP, using TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) to encrypt data.

WPA 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, WPA2 with AES is highly recommended for Enterprise networks.

Any of the above encryption methods can be used and an Array can support multiple encryption methods simultaneously, but only one method may be selected per SSID (except that selecting **WPA-Both** allows WPA and WPA2 to be used at the same time on the same SSID).

Otherwise, if multiple security methods are needed, you must define multiple SSIDs.

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see “[SSID Management](#)” on page 213). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security>Global Settings** window under **WPA Settings** (see “[Global Settings](#)” on page 197).

- **Choosing an authentication method:** User authentication ensures that users are who they say they are. For this purpose, the Array allows you to choose between the following user authentication methods:
 - **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the Array.

This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.
 - **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, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the Wi-Fi Array) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.
 - **MAC Address ACLs (Access Control Lists)**—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 address 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.

The Wi-Fi Array will accept up to 1,000 ACL entries.

- **PCI DSS or FIPS 140-2 Security**—to implement the requirements of these security standards on the Wi-Fi Array, please see [Appendix D: Implementing PCI DSS](#) or [Appendix E: Implementing FIPS Security](#).

Certificates and Connecting Securely to the WMI

When you point your browser to the Array to connect to the WMI, the Array presents an X.509 security certificate to the browser to establish a secure channel. One significant piece of information in the certificate is the Array's host name. This ties the certificate to a particular Array and ensures the client that it is connecting to that host.

Certificate Authorities (CAs) are entities that digitally sign certificates, using their own certificates (for example, VeriSign is a well-known CA). When the Array presents its certificate to the client's browser, the browser looks up the CA that signed the certificate to decide whether to trust it. Browsers ship with a small set of trusted CAs already installed. If the browser trusts the certificate's CA, it checks to ensure the host name (and IP address) match those on the certificate. If any of these checks fail, you get a security warning when connecting to the WMI.

The Array ships with a default certificate that is signed by the Xirrus CA. You may choose to use this certificate, or to use a certificate issued by the CA of your choice, as described in the following sections:

- [Using the Array's Default Certificate](#)
- [Using an External Certificate Authority](#)

Using the Array's Default Certificate

| | | |
|---------------------|---|--|
| Security | Enable Management: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Admin Management | Connection Timeout 30-100000 (Seconds): | 30000 |
| Admin RADIUS | | |
| Management Control | HTTPS | |
| Access Control List | Connection Timeout 30-100000 (Seconds): | 30000 |
| Global Settings | Port: | 443 |
| External Radius | Import Xirrus Authority Into Browser: | xirrus-ca.crt |
| Internal Radius | HTTPS [X.509] Certificate Signed By | Xirrus |
| Rogue Control List | External Certification Authority | |
| SSIDs | Download Certificate Signing Request | 55-Array.csr |
| Groups | Upload Signed Certificate: | <input type="text"/> <input type="button" value="Browse"/> <input type="button" value="Upload"/> |
| IPs | | |
| WDS | | |

Figure 106. Import Xirrus Certificate Authority

The Array's certificate is signed by a Xirrus CA that is customized for your Array and its current host name. By default, browsers will not trust the Array's certificate. You may import the Xirrus certificate to instruct the browser to trust the Xirrus CA on all future connections to Arrays. The certificate for the Xirrus CA is available on the Array, so that you can import it into your browser's cache of trusted CAs (right alongside VeriSign, for example). On the [Management Control](#) window of the WMI you will see the `xirrus-ca.crt` file. (Figure 106)

By clicking and opening this file, you can follow your browser's instructions and import the Xirrus CA into your CA cache (see [page 192](#) for more information). This instructs your browser to trust any of the certificates signed by the Xirrus CA, so that when you connect to any of our Arrays you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the Array. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for 'hostname'.

Since an Array's certificate is based on the Array's host name, any time you change the host name the Array's CA will regenerate and sign a new certificate. This happens automatically the next time you reboot after changing the host name. If you have already installed the Xirrus CA on a browser, this new Array certificate should automatically be trusted.

When you install the Xirrus CA in your browser, it will trust a certificate signed by any Xirrus Array, as long as you connect using the Array's host name.

Using an External Certificate Authority

If you prefer, you may install a certificate on your Array signed by an outside CA.

Why use a certificate from an external CA? The Array’s certificate is used for security when stations attempt to associate to an SSID that has Web Page Redirect enabled. In this case, it is preferable for the Array to present a certificate from an external CA that is likely to be trusted by most browsers. When a WPR login page is presented, the user will not see a security error if the Array’s certificate was obtained from an external CA that is already trusted by the user’s browser.

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the Array after you obtain it from the CA. This certificate will be tied to the Array’s host name and private key. See “External Certification Authority” on page 193 for more details.

Admin Management

This window allows you to manage network administrator accounts (create, modify and delete). It also allows you to limit account access to a read only status. When finished, click on the **Save changes to flash** if you wish to make your changes permanent.

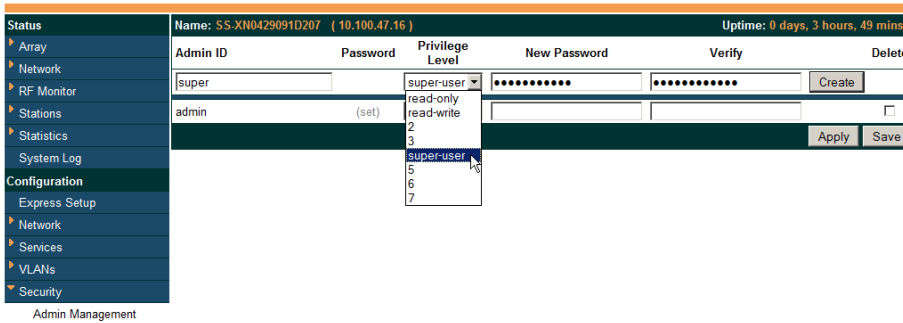


Figure 107. Admin Management

Procedure for Creating or Modifying Network Administrator Accounts

1. **Admin ID:** Enter the login name for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive.
2. **Read/Write:** Choose **Read/Write** if you want to give this administrator ID full read/write privileges, or choose **Read** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations.
3. **User Password:** Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive.
4. **Verify Password:** Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).
5. Click on the **Create** button to add this administrator ID to the list.
6. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

[Admin Privileges](#)

[External Radius](#)

[Global Settings \(IAP\)](#)

[Internal Radius](#)

[Management Control](#)

Admin Privileges

This window provides a detailed level of control over the privileges of Array administrators. Administrators may be assigned one of eight **Privilege Levels**. You may define the privilege level of each major feature (**Configuration Section**) that may be configured on the Array. For example, say that you set the privilege level to 4 for Reboot Array, Security, Radius Server, and SNMP, and you leave all other configuration sections at the default privilege level of 1. In this case, any administrator with a privilege level of 4 or higher may perform any operation on the Array, while an administrator with a privilege level lower than 4 but at least 1 may perform any operation except those whose level was set to 4. An error message will be displayed if an operation is attempted without a sufficient privilege level.

| Status | | Name: SS-XN0429091D207 (10.100.47.16) | | Uptime: 0 days, 3 hours, 33 mins | | | | | | | |
|---------------------|-------------------------|---|----------------------------------|----------------------------------|-----------------------|----------------------------------|-----------------------|-----------------------|-----------------------|--|--|
| Array | Privilege Level Names | | | | | | | | | | |
| Network | Privilege Level | Name | | | | | | | | | |
| RF Monitor | Level 0 | read-only | | | | | | | | | |
| Stations | Level 1 | read-write | | | | | | | | | |
| Statistics | Level 2 | 2 | | | | | | | | | |
| System Log | Level 3 | 3 | | | | | | | | | |
| Configuration | Level 4 | super-user | | | | | | | | | |
| Express Setup | Level 5 | 5 | | | | | | | | | |
| Network | Level 6 | 6 | | | | | | | | | |
| Services | Level 7 | 7 | | | | | | | | | |
| VLANs | Privilege Levels | | | | | | | | | | |
| Security | Minimum Privilege Level | | | | | | | | | | |
| Admin Management | Configuration Section | read-only 0 | read-write 1 | 2 | 3 | 4 | 5 | 6 | 7 | | |
| Admin Privileges | Access Control List | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| Admin RADIUS | Administrator | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| Management Control | Boot Environment | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| Access Control List | CDP | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| Global Settings | Cluster | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| External Radius | Console Interface | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| Internal Radius | Contact Information | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| Rogue Control List | Date and Time | <input type="radio"/> | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |
| SSIDs | | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | | |

Figure 108. Admin Privileges

Privilege level 0 is **read-only**. As a minimum, all administrators have permission for read access to all areas of Array configuration. Higher privilege levels may be used to define additional privileges for specific configuration sections.

If you are using an [Admin RADIUS](#) server to define administrator accounts, please see “[RADIUS Vendor Specific Attributes \(VSAs\) for Xirrus](#)” on page 415 to set the privilege level for each administrator.

Procedure for Configuring Admin Privileges

1. **Privilege Level Names** (optional): You may assign a **Name** to each Privilege Level. The name may be used to describe the access granted by this level. By default, levels **0** and **1** are named **read-only** and **read-write**, respectively, and levels **2** through **7** have the same name as their level number.
2. **Privilege Levels**: Use this section to assign a **Minimum Privilege Level** to selected **Configuration Sections** as desired. By default, all sections are assigned level 1. When you select a higher privilege level for a configuration section, then only administrators who have at least that privilege level will be able to make configuration changes to that section.
3. You may click ^ at the bottom of any row to toggle the values in the entire column to either on or off.
4. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

[External Radius](#)

[Groups](#)

[Admin Management](#)

[Admin RADIUS](#)

[Security](#)

Admin RADIUS

This window allows you to set up authentication of network administrators via RADIUS. Using RADIUS to control administrator accounts for logging in to Arrays has these benefits:

- Centralized control of administrator accounts.
- Less effort—you don't have to set up user names and passwords on each Array; just enter them once on the RADIUS server and then all of the Arrays can pull from the RADIUS server.
- Enforced policies—you may set password rules (e.g., passwords must contain at least one number and be at least 12 characters in length), and you may set expiration times for passwords.

Admin RADIUS settings override any local administrator accounts configured on the [Admin Management](#) window. If you have Admin RADIUS enabled, all administrator authentication is done via the configured RADIUS servers. The only exception to this is when you are connected via the Console port (using CLI). If you are using the Console port, the Array will authenticate administrators using accounts configured on the [Admin Management](#) window first, and then use the RADIUS servers. This provides a safety net to be ensure that you are not completely locked out of an Array if the RADIUS server is down.

About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Xirrus-Admin-Role** attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its Xirrus-Admin-Role attribute to the desired **Privilege Level Name** string, as defined in “[Admin Privileges](#)” on page 183. For more information about the RADIUS VSAs used by Xirrus, see “[RADIUS Vendor Specific Attributes \(VSAs\) for Xirrus](#)” on page 415.

When configuring administrator accounts on the RADIUS server, you must observe the same restrictions for length and legal characters as when creating these accounts on the Array using the [Admin Management](#) window: the user name and password must be between 5 and 50 characters, inclusive.

| | | | |
|----------------------|--|--|-------------------------------------|
| Status | Name: Bruce-XN8-Array (10.100.47.10) Location: Office Uptime: 5 days, 2 hours, 37 mins | | |
| ▶ Array | Admin RADIUS Settings | | |
| ▶ Network | Enable Admin RADIUS: | <input type="radio"/> Yes | <input checked="" type="radio"/> No |
| ▶ RF Monitor | Authentication Type: | <input checked="" type="radio"/> CHAP | <input type="radio"/> PAP |
| ▶ Stations | Timeout (seconds): | <input type="text" value="600"/> | |
| ▶ Statistics | Admin RADIUS Primary Server | | |
| System Log | Host Name / IP Address: | <input type="text" value="100.100.100.100"/> | |
| Configuration | Port Number: | <input type="text" value="1812"/> | |
| Express Setup | Shared Secret / Verify Secret: | <input type="text" value="*****"/> | <input type="text" value="*****"/> |
| ▶ Network | Admin RADIUS Secondary Server | | |
| ▶ Services | Host Name / IP Address: | <input type="text" value="100.99.100.100"/> | |
| ▶ VLANs | Port Number: | <input type="text" value="1812"/> | |
| ▶ Security | Shared Secret / Verify Secret: | <input type="text" value="*****"/> | <input type="text" value="*****"/> |
| Admin Management | | | |
| Admin RADIUS | <input type="button" value="Apply"/> <input type="button" value="Save"/> | | |

Figure 109. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable administrator authentication via RADIUS, and to set up primary and secondary servers to use for authentication of administrators attempting to log in to the Array.

1. Admin RADIUS Settings:

- a. **Enable Admin RADIUS:** Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.
- b. **Authentication Type:** Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).
 - PAP (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network “in the clear” (unencrypted) and is therefore considered insecure.
 - CHAP (Challenge-Handshake Authentication Protocol) is a more secure protocol. The login request is sent using a one-way hash function.
- c. **Timeout (seconds):** Define the maximum idle time (in seconds) before the RADIUS server’s session times out. The default is 600 seconds.

2. **Admin RADIUS Primary Server:** This is the RADIUS server that you intend to use as your primary server.
 - a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
 - b. **Port Number:** Enter the port number of this RADIUS server. The default is 1812.
 - c. **Shared Secret / Verify Secret:** Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.



The shared secret that you define must match the secret used by the RADIUS server.

3. **Admin RADIUS Secondary Server (optional):** If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will “failover” to the secondary RADIUS server (defined here).
 - a. **Host Name / IP Address:** Enter the IP address or domain name of this RADIUS server.
 - b. **Port Number:** Enter the port number of this RADIUS server. The default is 1812.
 - c. **Shared Secret / Verify Secret:** Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

Management Control

This window allows you to enable or disable the Array management interfaces and set their inactivity time-outs. The supported range is 300 (default) to 100,000 seconds.

| Status | Name: SS-XM4 (192.168.1.74) | | Location: 12-125 | | Uptime: 3 days, 22 hours, 35 mins | |
|---------------------------|--|---|---|--------------------------|------------------------------------|-----|
| Configuration | Save changes to flash | | | | | |
| Express Setup | Management Settings | | | | | |
| ▶ Network | Maximum login attempts allowed (1 - 255): | | 3 | | <input type="checkbox"/> Unlimited | |
| ▶ Services | Failed login retry period (0 - 65535 seconds): | | 0 | | | |
| ▶ VLANs | Pre-login Banner: | | Password is case-sensitive | | | |
| ▼ Security | | | Submit | | | |
| Admin Management | Post-login Banner: | | Welcome to Xirrus! | | | |
| Admin Privileges | | | Submit | | | |
| Admin RADIUS | | | | | | |
| Management Control | Management Transports | | | | | |
| Access Control List | | | Timeout (30-100000 seconds) | | Port | |
| Global Settings | SSH: | <input checked="" type="radio"/> On <input type="radio"/> Off | 100000 | | | 22 |
| External Radius | Telnet: | <input type="radio"/> On <input checked="" type="radio"/> Off | 300 | | | 23 |
| Internal Radius | Serial: | <input checked="" type="radio"/> On <input type="radio"/> Off | 300 | | | |
| Rogue Control List | HTTPS: | | 100000 | | | 443 |
| ▶ SSIDs | Management Modes | | | | | |
| ▶ Groups | Network Assurance: | | <input checked="" type="radio"/> On <input type="radio"/> Off | Period (60-900 seconds): | | 300 |
| ▶ IAPs | PCI Audit Mode: | | <input type="radio"/> On <input checked="" type="radio"/> Off | | | |
| ▶ WDS | FIPS 140-2, Level 2 Security: | | <input type="radio"/> On <input checked="" type="radio"/> Off | | | |
| ▶ Filters | HTTPS (X.509) Certificate | | | | | |
| ▶ Clusters | Import Xirrus Authority Into Browser: | | xirrus-ca.crt | | | |
| Tools | Certificate Signed By | | Xirrus | | | |
| Help | External Certification Authority | | | | | |
| System Tools | Download Certificate Signing Request | | SS-XM4.csr | | | |
| CLI | Upload Signed Certificate: | | Browse... Upload | | | |
| Options | Common Name: | | | | | |
| Logout | Organization Name: | | | | | |
| Log Messages | Organizational Unit Name: | | | | | |
| | Locality (City): | | | | | |
| | State or Province: | | | | | |
| | Country Name (2 Letter Code): | | | | | |
| | Email Address: | | | | | |
| | Create New Certificate Signing Request | | Create | | | |

Figure 110. Management Control

Procedure for Configuring Management Control

1. Management Settings:

- a. Maximum login attempts allowed (1-255):** After this number of consecutive failing administrator login attempts via ssh or telnet, the **Failed login retry period** is enforced. The default is 3.
- b. Failed login retry period (0-65535 seconds):** After the maximum number (defined above) of consecutive failing administrator login attempts via ssh or telnet, the administrator’s IP address is denied access to the array for the specified period of time (in seconds). The default is 0.
- c. Pre-login Banner:** Text that you enter here will be displayed above the WMI login prompt. (Figure 111)

| | | |
|---|---------------------------------------|--------------------------|
| Name: XN0429091D207 (10.100.47.12) | | Location: SS Desk |
| Current Status: | Logged Out | |
| | Password is case-sensitive. | |
| User Name: | <input type="text" value="admin"/> | |
| User Password: | <input type="password" value="••••"/> | |

Figure 111. Pre-login Banner

- d. Post-login Banner:** Text that you enter here will be displayed in a message box after a user logs in to the WMI.
- 2. SSH:**
- a. On/Off:** Choose **On** to enable management of the Array over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the Array. SSH clients used for connecting to the Array must be configured to use SSH-2.
 - b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

- c. **Port:** Enter a value in this field to define the port used by SSH. The default port is 22.
- 3. **Telnet:**
 - a. **On/Off:** Choose **On** to enable Array management over a Telnet connection, or **Off** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.
 - b. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
 - c. **Port:** Enter a value in this field to define the port used by Telnet. The default port is 23.
- 4. **Serial**
 - a. **On/Off:** Choose **On** to enable management of the Array via a serial connection, or choose **Off** to disable this feature.
 - b. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
- 5. **HTTPS**
 - a. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.
 - b. **Port:** Enter a value in this field to define the port used by SSH. The default port is 443.

6. Management Modes

- a. **Network Assurance:** Click the **On** button to enable this mode. Network assurance checks network connectivity to each server that you configure, such as the NTP server, RADIUS servers, SNMP trap hosts, etc. By proactively identifying network resources that are unavailable, the network manager can be alerted of problems potentially before end-users notice an issue. The distributed intelligence of Arrays provides this monitoring at multiple points across the network, adding to the ability to isolate the problem and expedite the resolution

Connectivity is checked when you configure a server. If a newly configured server is unreachable, you will be notified directly and a Syslog entry is created. Also, the Array cycles through all configured servers on an ongoing basis, checking one per second, so that each server is checked approximately every four or five minutes. Servers are checked regardless of whether they are configured as IP addresses or host names.

If a server becomes unreachable, a Syslog message is generated. When the server again becomes reachable, another Syslog message is generated.

To view the status of all configured servers checked by this feature, please see [“Network Assurance” on page 101](#).

- b. **PCI Audit Mode:** Click the **On** button to enable this mode. In PCI Audit Mode, the Array checks whether its configuration satisfies PCI DSS wireless requirements. This mode does not change any other settings, but will inform you of any violations that exist. Furthermore, the Array will monitor changes that you make to its 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” on page 427](#) to ensure that you are using

the Array in accordance with the PCI DSS requirements. For more information, see “[Appendix D: Implementing PCI DSS](#)” on page 425.

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)
- c. **FIPS 140-2, Level 2 Security:** Please see “[Appendix E: Implementing FIPS Security](#)” on page 431 for more information, including step-by-step instructions for proceeding to implement FIPS Level 2 Security requirements on an Array.

Click the **On** button to enable FIPS. This will perform all of the setting changes required to make the Array comply with FIPS requirements. A message is displayed showing the changes that were performed. The Array continues to enforce FIPS requirements by preventing you from making non-compliant configuration changes. Click the **Off** button to stop enforcing FIPS requirements.

Note that when you enable FIPS, the Array does *not* save your previous settings, and it will not restore them if you click the **Off** button. If you think you may wish to disable FIPS and restore your previous configuration at some later time, use **Set Restore Point** to save a copy of your configuration before enabling FIPS (see [Step 9 on page 301](#)).

7. HTTPS (X.509) Certificate

- a. **Import Xirrus Authority into Browser:** This feature imports the Xirrus Certificate Authority (CA) into your browser (for a discussion, please see “[Certificates and Connecting Securely to the WMI](#)” on [page 179](#)). Click the link (`xirrus-ca.crt`), and then click **Open** to view or install the current Xirrus CA certificate. Click **Install Certificate** to

start your browser's Certificate Install Wizard. We recommend that you use this process to install Xirrus as a root authority in your browser.

When you assign a **Host Name** to your Array using the [Express Setup](#) window, then the next time you reboot the Array it automatically creates a security certificate for that host name. That certificate uses Xirrus as the signing authority. Thus, in order to avoid having certificate errors on your browser when using WMI:

- You must have assigned a host name to the Array and rebooted at some time after that.
- Use **Import Xirrus Authority into Browser**
- Access WMI by using the host name of the Array rather than its IP address.

b. HTTPS (X.509) Certificate Signed By: This read-only field shows the signing authority for the current certificate.

8. External Certification Authority

This Step and [Step 9](#) allow you to obtain a certificate from an external authority and install it on an Array. "[Using an External Certificate Authority](#)" on [page 181](#) discusses reasons for using an external CA.

For example, to obtain and install a certificate from VeriSign on the Array, follow these steps:

- If you don't already have the certificate from the external (non-Xirrus) Certificate Authority, see [Step 9](#) to create a request for a certificate.
- Use [Step 8a](#) to review the request and copy its text to send to VeriSign.
- When you receive the new certificate from VeriSign, upload it to the Array using [Step 8b](#).

External Certification Authority has the following fields:

- a. **Download Certificate Signing Request:** After creating a certificate signing request (.csr file—[Step 9](#)), click the **View** button to review it. If it is satisfactory, click the name of the .csr file to display the text of the request. You can then copy this text and use it as required by the CA. You may also click on the filename of the .csr file to download it to your local computer.
 - b. **Upload Signed Certificate:** To use a custom certificate signed by an authority other than Xirrus, use the **Browse** button to locate the certificate file, then click **Upload** to copy it to the Array. The Array's web server will be restarted and will pick up the new certificate. This will terminate any current web sessions, and you will need to reconnect and re-login to the Array.
9. **To create a Certificate Signing Request**
 - a. Fill in the fields in this section: **Common Name, Organization Name, Organizational Unit Name, Locality (City), State or Province, Country Name, and Email Address.** Spaces may be used in any of the fields, except for Common Name, Country Name, or Email Address. Click the **Create** button to create the certificate signing request. See [Step 8](#) above to use this request.
10. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

[Network Interfaces](#) - to enable/disable management over an Ethernet interface

[Global Settings \(IAP\)](#) - to enable/disable management over IAPs

[Admin Management](#)

[External Radius](#)

[Global Settings \(IAP\)](#)

[Internal Radius](#)

[Access Control List](#)

[Security](#)

Access Control List

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

There is only one global ACL, and you may select whether its type is an Allow List or a Deny List, or whether use of the list is disabled.

There is also a per-SSID ACL (see “Per-SSID Access Control List” on page 226). If the same MAC address is listed in both the global ACL and in an SSID’s ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

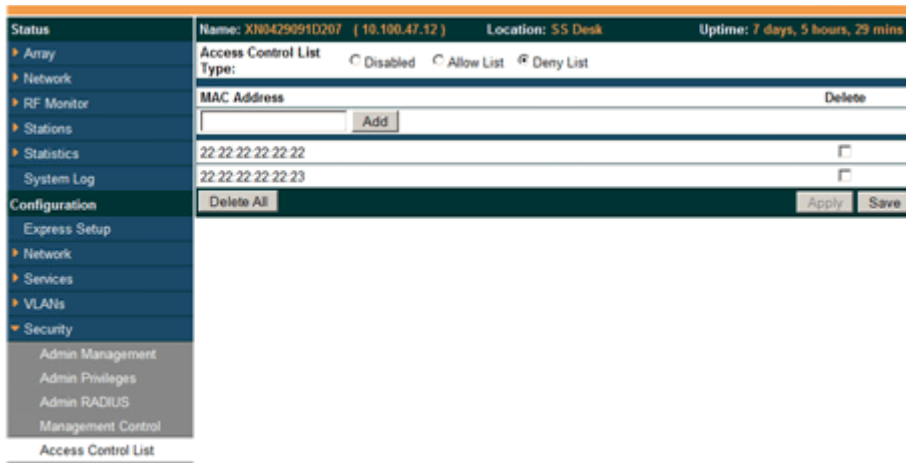


Figure 112. Access Control List

Procedure for Configuring Access Control Lists

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

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



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

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

See Also

External Radius

Global Settings (IAP)

Internal Radius

Management Control

Security

Station Status Windows (list of stations that have been detected by the Array)

Global Settings

This window allows you to establish the security parameters for your wireless network, including WEP, WPA, WPA2 and RADIUS authentication. When finished, click **Save changes to flash** if you wish to make your changes permanent.

For additional information about wireless network security, refer to “Security Planning” on page 45 and “Understanding Security” on page 176.

| Status | Name: SS-XNB (10.109.47.186) | Location: SS Area | Uptime: 0 days, 3 hours, 25 minutes |
|---------------------|---|-------------------|--|
| Array | RADIUS Server Mode: <input type="radio"/> Internal <input checked="" type="radio"/> External | | |
| Network | WPA Settings: | | |
| RF Monitor | TKIP Enabled: <input checked="" type="radio"/> Yes <input type="radio"/> No | | |
| Stations | AES Enabled: <input checked="" type="radio"/> Yes <input type="radio"/> No | | |
| Statistics | WPA Group Rekey Time (seconds): <input type="text"/> Never: <input checked="" type="checkbox"/> | | |
| System Log | PSK Authentication: <input type="radio"/> Yes <input checked="" type="radio"/> No | | |
| Configuration | WPA Preshared Key / Verify Key: <input type="text"/> <input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal | | |
| Express Setup | EAP Authentication: <input checked="" type="radio"/> Yes <input type="radio"/> No | | |
| Network | WEP Settings: | | |
| Services | Encryption Key 1 / Verify Key 1: <input type="text"/> <input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal <input checked="" type="radio"/> 40 bit (WEP-64) <input type="radio"/> 104 bit (WEP-128) | | |
| VLANs | Encryption Key 2 / Verify Key 2: <input type="text"/> <input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal <input type="radio"/> 40 bit (WEP-64) <input checked="" type="radio"/> 104 bit (WEP-128) | | |
| Security | Encryption Key 3 / Verify Key 3: <input type="text"/> <input type="radio"/> ASCII <input type="radio"/> Hexadecimal <input type="radio"/> 40 bit (WEP-64) <input type="radio"/> 104 bit (WEP-128) | | |
| Admin Management | Encryption Key 4 / Verify Key 4: <input type="text"/> <input type="radio"/> ASCII <input type="radio"/> Hexadecimal <input type="radio"/> 40 bit (WEP-64) <input type="radio"/> 104 bit (WEP-128) | | |
| Admin RADIUS | Default Key: <input type="text" value="Key 2"/> | | |
| Management Control | | | |
| Access Control List | | | |
| Global Settings | | | |
| External Radius | | | |
| Internal Radius | | | |
| Rogue Control List | | | |
| SSIDs | | | |
| Groups | | | |
| IAPs | | | |
| WDS | | | |
| Filters | | | |
| Tools | | | |
| | | | <input type="button" value="Apply"/> <input type="button" value="Save"/> |

Figure 113. Global Settings (Security)

Procedure for Configuring Network Security

1. **RADIUS Server Mode:** Choose the RADIUS server mode you want to use, either Internal or External. Parameters for these modes are configured in “External Radius” on page 200 and “Internal Radius” on page 204.

WPA Settings

These settings are used if the WPA or WPA2 encryption type is selected on the **SSIDs > SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

2. **TKIP Enabled:** Choose **Yes** to enable **TKIP** (Temporal Key Integrity Protocol), or choose **No** to disable TKIP.



*TKIP encryption does not support high throughput rates (see **Improved MAC Throughput**), per the IEEE 802.11n specification.*

TKIP should never be used for WDS links on XR arrays.

3. **AES Enabled:** Choose **Yes** to enable **AES** (Advanced Encryption Standard), or choose **No** to disable AES. If both AES and TKIP are enabled, the station determines which will be used.
4. **WPA Group Rekey Time (seconds):** Enter a value to specify the group rekey time (in seconds). The default is **Never**.
5. **PSK Authentication:** Choose **Yes** to enable PSK (Pre-Shared Key) authentication, or choose **No** to disable PSK.
6. **WPA Preshared Key / Verify Key:** If you enabled PSK, enter a passphrase here, then re-enter the passphrase to verify that you typed it correctly.
7. **EAP Authentication:** Choose **Yes** to enable **EAP** (Extensible Authentication Protocol) or choose **No** to disable EAP.

WEP Settings

These settings are used if the **WEP** encryption type is selected on the **SSIDs > SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).



*WEP encryption does not support high throughput rates or features like frame aggregation or block acknowledgements (see **Improved MAC Throughput**), per the IEEE 802.11n specification.*

WEP should never be used for WDS links on XN arrays.

- 8. Key Mode / Length:** If you enabled WEP, choose the mode (either ASCII or Hex) and the desired key length (either 40 or 104) from the pull-down lists.

Encryption Key 1 / Verify Key 1: Enter an encryption key of the length and type selected (to the right of the key fields):

- 10 hex/5 ASCII characters for 40 bits (WEP-64)
- 26 hex/13 ASCII characters for 104 bits (WEP-128)

Re-enter the key to verify that you typed it correctly. Hexadecimal characters are defined as ABCDEF and 0-9. For ASCII mode, you may include special characters, except for the double quote symbol (“”).

- 9. Encryption Key 2 to 4/ Verify Key 2 to 4/ Key Mode/Length** (optional): If desired, enter up to four encryption keys, in the same way that you entered the first key.
- 10. Default Key:** Choose which key you want to assign as the default key. Make your selection from the pull-down list.
- 11. Click **Save changes to flash**** if you wish to make your changes permanent.



After configuring network security, the configuration must be applied to an SSID for the new functionality to take effect.

See Also

- Admin Management
- External Radius
- Internal Radius
- Access Control List
- Management Control
- Security
- Security Planning
- SSID Management

External Radius

This window allows you to define the parameters of an external RADIUS server for user authentication. To set up an external RADIUS server, you must choose **External** as the RADIUS server mode in Global Settings. Refer to “Global Settings” on page 197.

| Status | Name: SS-XNB (10.109.47.186) | Location: SS Area | Uptime: 0 days, 3 hours, 30 minutes |
|--|---|---|-------------------------------------|
| <ul style="list-style-type: none"> ▶ Array ▶ Network ▶ RF Monitor ▶ Stations ▶ Statistics ▶ System Log Configuration <ul style="list-style-type: none"> Express Setup ▶ Network ▶ Services ▶ VLANs ▶ Security <ul style="list-style-type: none"> Admin Management Admin RADIUS Management Control Access Control List Global Settings External Radius Internal Radius Rogue Control List ▶ SSIDs ▶ Groups ▶ IAPs ▶ WDS ▶ Filters Tools <ul style="list-style-type: none"> System Tools CLI Logout | Primary Server Host Name / IP Address: <input type="text" value="radius1"/> Port Number: <input type="text" value="1812"/> Shared Secret / Verify Secret: <input type="password" value="*****"/> <input type="password" value="*****"/> | Secondary Server Host Name / IP Address: <input type="text"/> Port Number: <input type="text" value="1812"/> Shared Secret / Verify Secret: <input type="password"/> <input type="password"/> | |
| | Settings Timeout (seconds): <input type="text" value="600"/> NAS Identifier: <input type="text"/> Accounting: <input type="radio"/> Off <input checked="" type="radio"/> On | | |
| | Accounting Accounting Interval (seconds): <input type="text" value="300"/> | | |
| | Primary Server Host Name / IP Address: <input type="text" value="radius1"/> Primary Server Port Number: <input type="text" value="1813"/> Primary Server Shared Secret / Verify Secret: <input type="password" value="*****"/> <input type="password" value="*****"/> | Secondary Server Host Name / IP Address: <input type="text"/> Secondary Server Port Number: <input type="text" value="1813"/> Secondary Server Shared Secret / Verify Secret: <input type="password"/> <input type="password"/> | |
| | <input type="button" value="Apply"/> <input type="button" value="Save"/> | | |

Figure 114. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see “Understanding Groups” on page 228. User groups allow you to easily apply a uniform configuration to a user on the Array.

About Creating User Accounts on the RADIUS Server

A number of attributes of user (Wi-Fi client) accounts are controlled by RADIUS Vendor Specific Attributes (VSAs) defined by Xirrus. For example, you would use the VSA named **Xirrus-User-VLAN** if you wish to set the VLAN for a user account in RADIUS. For more information about the RADIUS VSAs used by Xirrus, see “RADIUS Vendor Specific Attributes (VSAs) for Xirrus” on page 415.

Procedure for Configuring an External RADIUS Server

1. **Primary Server:** This is the external RADIUS server that you intend to use as your primary server.
 - a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
 - b. **Port Number:** Enter the port number of this external RADIUS server. The default is 1812.
 - c. **Shared Secret / Verify Secret:** Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.



The shared secret that you define must match the secret used by the external RADIUS server.

2. **Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will “failover” to the secondary RADIUS server (defined here).
 - a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
 - b. **Port Number:** Enter the port number of this external RADIUS server. The default is 1812.

- c. **Shared Secret / Verify Secret:** Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.
- 3. **Settings:** Define the session timeout, the NAS Identifier, and whether accounting will be used.
 - a. **Timeout (seconds):** Define the maximum idle time (in seconds) before the external RADIUS server's session times out. The default is 600 seconds.
 - b. **NAS Identifier:** From the point of view of a RADIUS server, the Array is a client, also called a network access server (NAS). Enter the 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. The account settings appear, and must be configured.
- 4. **Accounting Settings:**

Note that RADIUS accounting start packets sent by the Array will include the client station's Framed-IP-Address attribute.

- a. **Accounting Interval (seconds):** Specify how often Interim records are to be sent to the server. The default is 300 seconds.
- b. **Primary Server Host Name / IP 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 Host Name / IP 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 **Save changes to flash**** if you wish to make your changes permanent.

See Also

Admin Management

Global Settings (IAP)

Internal Radius

Access Control List

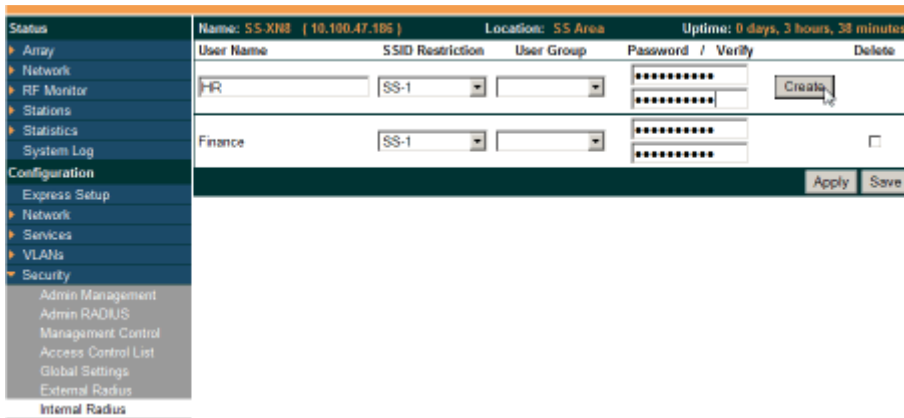
Management Control

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 197.



| Name: SS XNR (10.100.47.106) | Location: SS Area | Uptime: 0 days, 3 hours, 38 minutes | | |
|--------------------------------|-------------------|-------------------------------------|-------------------|--------------------------|
| User Name | SSID Restriction | User Group | Password / Verify | Delete |
| HR | SS-1 | | ***** ***** | Create |
| Finance | SS-1 | | ***** ***** | <input type="checkbox"/> |

Figure 115. Internal RADIUS Server



*Clients using PEAP may have difficulty authenticating to the Array using the Internal RADIUS server due to invalid security certificate errors. To prevent this problem, the user may disable the **Validate Server Certificate** option on the station. Do this by displaying the station's wireless devices and then displaying the properties of the desired wireless interface. In the security properties, disable **Validate server certificate**. In some systems, this may be found by setting the authentication method to PEAP and changing the associated settings.*

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 228](#).
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 228](#).
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, click their **Delete** buttons.
6. Click **Save changes to flash** if you wish to make your changes 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 273. The Array can keep up to 5000 entries in this list.



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 107.

| Rogue BSSID/SSID | Blocked | Known | Approved | Match Only: | BSSID | Manufacturer | SSID | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------|
| <input type="text"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | Create |
| 00:0E:7d:* | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | Delete |

Apply Save

Figure 116. Rogue Control List

Procedure for Establishing Rogue AP Control

- 1. Rogue BSSID/SSID:** Enter the BSSID, SSID, or manufacturer string to match for the new rogue control entry. The **Match Only** radio buttons specify what to match (e.g., the MAC address, SSID, or manufacturer).

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 Classification:** Enter the classification for the specified rogue AP(s), either **Blocked**, **Known** or **Approved**.
- 3. Match Only:** Select the match criterion to compare the **Rogue BSSID/SSID** string against: **BSSID**, **Manufacturer**, or **SSID**. The BSSID field contains the MAC address.
- 4.** Click **Create** to add this rogue AP to the Rogue Control List.
- 5. 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**.
- 6.** To delete rogue APs from the list, click their **Delete** buttons.
- 7.** Click **Save changes to flash** if you wish to make your changes permanent.

See Also

[Network Map](#)

[Intrusion Detection](#)

[SSIDs](#)

[SSID Management](#)

SSIDs

This status-only window 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. 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](#).

| Status | Name: SS-XM4 (192.168.1.74) | | Location: 12-125 | | Uptime: 3 days, 22 hours, 14 mins | | | | | | | | |
|---------------------|-----------------------------|-------------------|------------------|-----------------|-----------------------------------|----------|---------|----------------|-----------|-----------|-----|-----|----------|
| Configuration | Save changes to flash | | | | | | | | | | | | |
| Express Setup | | | | | | | | | | | | | |
| Network | | | | | | | | | | | | | |
| Services | | | | | | | | | | | | | |
| VLANs | | | | | | | | | | | | | |
| Security | | | | | | | | | | | | | |
| SSIDs | | | | | | | | | | | | | |
| SSID Management | | | | | | | | | | | | | |
| Active IAPs | | | | | | | | | | | | | |
| Access Control List | | | | | | | | | | | | | |
| SSID | Authentication & Encryption | Security Settings | Filter List | VLAN | Num | QoS | Band | Xirrus Roaming | Broadcast | DHCP Pool | WPR | ACL | Fallback |
| xirrus | open | none | global-settings | none | 0 | 2 | Both | off | off | none | off | off | None |
| xirrus42 | 802-1x | wpa | unique-settings | none | 0 | 2 | Both | off | on | xir-1.240 | off | off | Disable |
| Limits | | | | | | | | | | | | | |
| SSID | Enabled | Station Limit | SSID Traffic | Station Traffic | Time On | Time Off | Days On | Active | | | | | |
| xirrus | no | 1536 | unlimited | unlimited | always | never | all | no | | | | | |
| xirrus42 | yes | 1536 | unlimited | unlimited | always | never | all | yes | | | | | |

Figure 117. 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.

For information to help you understand SSIDs and how multiple SSIDs are managed by the Wi-Fi Array, go to “[Understanding SSIDs](#)” on page 209 and the [Multiple SSIDs](#) section of “[Frequently Asked Questions](#)” on page 404. For a description of how QoS operates on the Array, see “[Understanding QoS Priority on the Wi-Fi Array](#)” on page 210.

SSIDs are managed with the following windows:

- “SSID Management” on page 213
- “Active IAPs” on page 225

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 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).

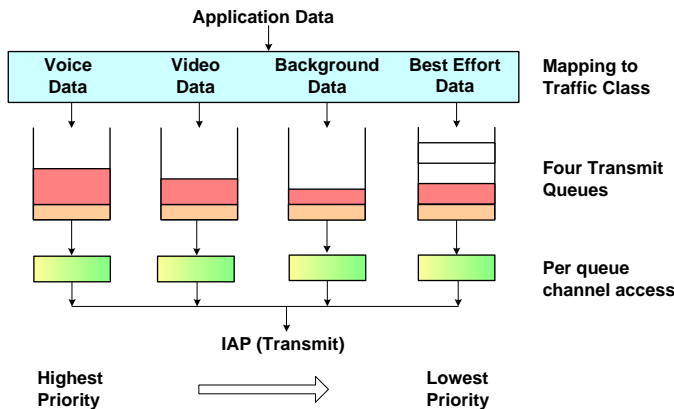


Figure 118. Four Traffic Classes

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 | 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 |
| 1 | 1 |
| 2 (Default) | 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 2 is the default. See [“SSID Management” on page 213](#). 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 228](#), and [“Filters” on page 283](#).
 - 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 286](#). This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

- The QoS priority implementation on the Array supports voice applications.

SSID Management

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

The screenshot shows the SSID Management configuration page for a device named 'SS-XN0429091D207'. At the top, there is a table listing SSIDs. The 'xirrus' SSID is selected and highlighted in orange. Below the table, there are several configuration sections:

- SSID xirrus Limits:** Includes fields for Stations (1920), Overall Traffic, Traffic per Station, Days Active (Everyday, Sun, Mon, Tue, Wed, Thu, Fri, Sat), and Time Active (Always).
- SSID xirrus Web Page Redirect Configuration:** Includes Landing Page URL, Background Image (page_bg.jpg), Logo Image (xirrus_logo.gif), Header Text File, Footer Text File, Server selection (Internal Login, Internal Splash, External), HTTPS Timeout (0-never), Redirect URL, Redirect Secret, and RADIUS Authentication Type (PAP, CHAP).
- SSID xirrus RADIUS Configuration:** Includes Radio Server selection (Internal, External), Accounting checkbox, and two RADIUS server entries with fields for Host/IP Address, Port, Shared Secret, and Verify Secret.

- Create new SSID
- Configure parameters
- Set traffic limits / usage schedule
- Configure WPR
- Configure RADIUS server

Figure 119. SSID Management

Procedure for Managing SSIDs

1. **New SSID Name:** To create a new SSID, enter a new SSID name to the left of the Create button (Figure 119), then click Create. The SSID name may only consist of the characters A-Z, a-z, 0-9, dash, and underscore. You may create up to 16 SSIDs.


SSID List (top of page)

2. **SSID:** Shows all currently assigned SSIDs. When you create a new SSID, the SSID name appears in this table. Click any SSID in this list to select it.
3. **On:** Check this box to activate this SSID or clear it to deactivate it.
4. **Brdcast:** Check this box to make the selected SSID visible to all clients on the network. Although the 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 beaconsed 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 171). 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 210. 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 168.
9. **Filter List:** If you wish to apply a set of filters to this SSID’s traffic, select the desired Filter List. See [“Filters”](#) on page 283.
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.*

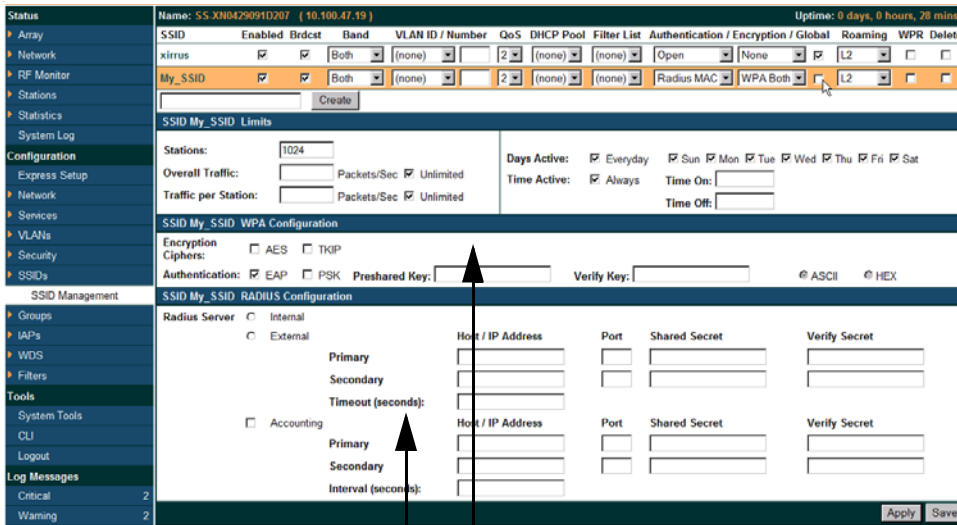
 - **802.1x:** Authenticates stations onto the Wi-Fi network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the Wi-Fi Array) or external.
11. **Encryption:** From the pull-down list, choose the encryption that will be required—specific to this SSID—either None, 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 197). For an overview of the security options, see “Security Planning” on page 45 and “Understanding Security” on page 176.



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

- 12. Global:** Check the checkbox if you want this SSID to use the security settings established at the global level (refer to “Global Settings” on page 197). Clear the checkbox if you want the settings established here to take precedence. Additional sections will be displayed to allow you to configure encryption, RADIUS, and RADIUS accounting settings. The **WPA Configuration** encryption settings have the same parameters as those described in “Procedure for Configuring Network Security” on page 198. 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 201). Note that external RADIUS servers may be specified using IP addresses or domain names.



Set Encryption
 Configure Radius, Accounting

Figure 120. SSID Management

13. **Roaming:** For this SSID, select whether to enable fast roaming between IAPs or Arrays at **L2&L3** (Layer 2 and Layer 3), at **L2** (Layer 2 only), or disable roaming (**Off**). You may only select fast roaming at Layers 2 and 3 if this has been selected in **Global Settings (IAP)**. See “Understanding Fast Roaming” on page 235.
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 219 for details of WPR usage and configuration.



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

- 15. Fallback:** Network Assurance checks network connectivity for the Array. When Network Assurance detects a failure, perhaps due to a bad link or WDS failure, if Fallback is set to **Disable** the Array will automatically disable this SSID. This will disassociate current clients, and prevent new clients from associating. Since the Array’s network connectivity has failed, this gives clients a chance to connect to other, operational parts of the Wi-Fi network. No changes are made to WDS configuration. See [Step a on page 191](#) for more information on Network Assurance.

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

- “SSID Limits” on page 218
- “Web Page Redirect Configuration Settings” on page 219
- “WPA Configuration Settings” on page 223
- “RADIUS Configuration Settings” on page 224

SSID Limits

See “Group Limits” on page 232 for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

- 16. Stations:** Enter the maximum number of stations allowed on this SSID. The default is 1536. This step is optional. Note that the IAPs - Global Settings window also has a station limit option—**Max Station Association per IAP**. If both station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.

17. **Overall Traffic:** Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.
18. **Traffic per Station:** Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.
19. **Days Active:** Choose **Everyday** if you want this SSID to be active every day of the week, or select only the specific days that you want this SSID to be active. Days that are not checked are considered to be the inactive days.
20. **Time Active:** Choose **Always** if you want this SSID active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that this SSID is active.
21. To delete SSIDs, click their **Delete** buttons.
22. Click **Save changes to flash** if you wish to make your changes permanent.

Web Page Redirect Configuration Settings

If you enable WPR, the SSID Management window displays additional fields that must be configured. For example configurations and complete examples, please see the *Xirrus Web Page Redirect Application Note* in the [Xirrus 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. The landing page may be specified for a user group as well. See "[Group Management](#)" on page 230. Note that if you change the management HTTPS port, WPR uses that port, too. See "[HTTPS](#)" on page 190.

| SSID Xirrus-ss Web Page Redirect Configuration | | | |
|--|--|--|--|
| Landing Page URL (http): | <input type="text"/> | Server: | <input type="radio"/> Internal Login <input type="radio"/> External Login |
| Background Image: | <input type="text" value="page_bg.jpg"/> | <input checked="" type="radio"/> Internal Splash <input type="radio"/> External Splash | HTTPS <input checked="" type="radio"/> On <input type="radio"/> Off RADIUS Authentication Type: <input type="radio"/> PAP <input checked="" type="radio"/> CHAP |
| Logo Image: | <input type="text" value="xirrus_logo.gif"/> | <input type="radio"/> External Login <input type="radio"/> External Splash | Timeout (seconds): <input type="text"/> <input checked="" type="checkbox"/> Never |
| Header Text File: | <input type="text"/> | <input type="radio"/> Landing Page Only | Redirect URL (https): <input type="text"/> |
| Footer Text File: | <input type="text"/> | | Redirect Secret: <input type="text"/> |

Figure 121. WPR Internal Splash Page Fields (SSID Management)

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

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

- Internal Login page

This option displays a login page (residing on the Array) instead of the first user-requested URL. There is an upload function that allows you to replace the default login page, if you wish. Please see “[Web Page Redirect](#)” on page 304 for more information.

To set up internal login, set **Server** to **Internal Login**. Set **HTTPS** to **On** for a secure login, or select **Off** to use HTTP. You may also customize the login page with logo and background images and header and footer text. See “[Customizing an Internal Login or Splash page](#)” on page 222.

The user name and password are obtained by the login page, and authentication occurs according to your configured authentication information (starting with [Step 10 on page 215](#) above). These authentication parameters are configured as described in “[Procedure for Configuring Network Security](#)” on page 198.

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



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

- **Internal Splash page**

This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Array. Note that there is an upload function that allows you to replace the default splash page, if you wish. Please see [“Web Page Redirect” on page 304](#) for more information. You may also customize the splash page with logo and background images and header and footer text. See [“Customizing an Internal Login or Splash page” on page 222](#).

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

- **External Login page**

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

Authentication occurs according to your configured RADIUS information. These parameters are configured as described in [“Procedure for Configuring Network Security” on page 198](#), except that the **RADIUS Authentication Type** is selected here, as described below. After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

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

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

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

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

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

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

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

Customizing an Internal Login or Splash page

You may customize these pages with a logo and/or background image, and header and/or footer text, as shown below in [Figure 122](#).

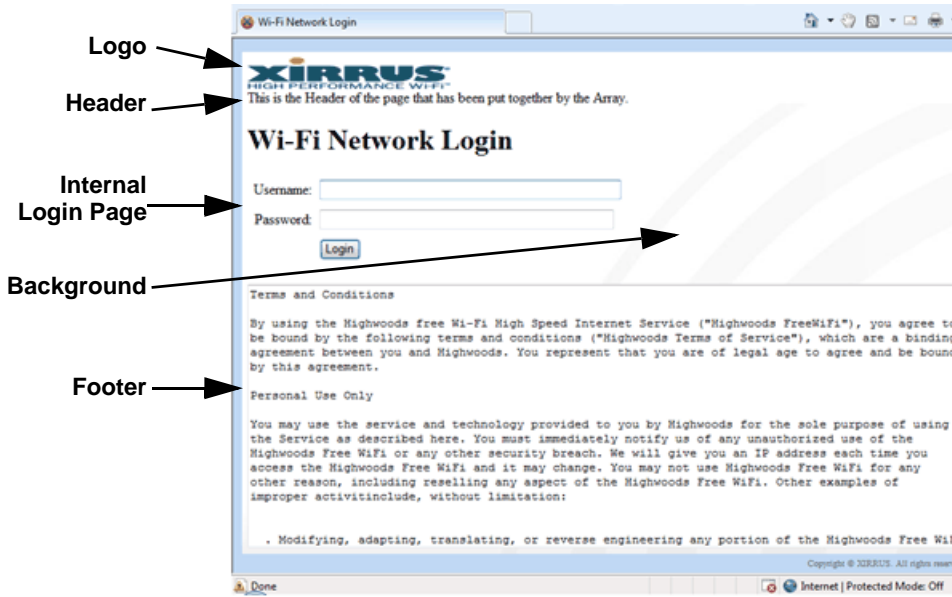


Figure 122. Customizing an Internal Login or Splash Page

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

WPA Configuration Settings

If you set **Encryption** for this SSID to one of the WPA selections ([Step 11 on page 215](#)) and you did not check the **Global** checkbox ([Step 12](#)), this section will be displayed. The **WPA Configuration** encryption settings have the same

parameters as those described in “Procedure for Configuring Network Security” on page 198

RADIUS Configuration Settings

The RADIUS settings section will be displayed if you set **Authentication** (Step 10 on page 215) to **RADIUS MAC** and you did not check the **Global** checkbox (Step 12). This means that you wish to set up a RADIUS server to be used for this particular SSID. If **Global** is checked, then the security settings (including the RADIUS server, if any) established at the global level are used instead (see “Global Settings” on page 197).

The RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see “Procedure for Configuring an External RADIUS Server” on page 201).

See Also

DHCP Server

External Radius

Global Settings (IAP)

Internal Radius

Security Planning

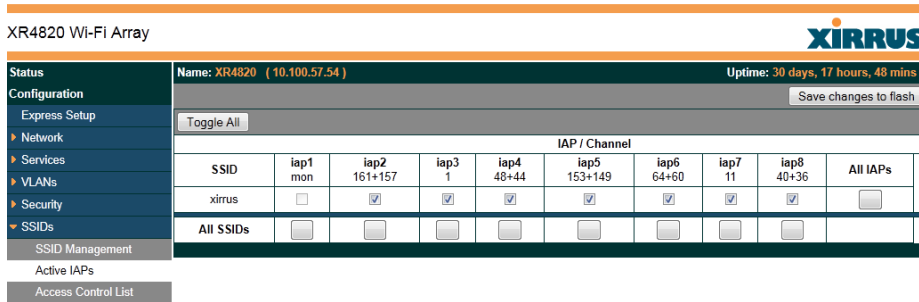
SSIDs

Understanding QoS Priority on the Wi-Fi Array

Active IAPs

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

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



XR4820 Wi-Fi Array **XIRRUS**

Status: Name: XR4820 (10.100.57.54) Uptime: 30 days, 17 hours, 48 mins

Configuration: Express Setup Save changes to flash

Toggle All

| SSID | IAP / Channel | | | | | | | | All IAPs |
|-----------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|
| | iap1 mon | iap2 161+157 | iap3 1 | iap4 48+44 | iap5 153+149 | iap6 64+60 | iap7 11 | iap8 40+36 | |
| xirrus | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| All SSIDs | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

Figure 123. Setting Active IAPs per SSID

Procedure for Specifying Active IAPs

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

Per-SSID Access Control List

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

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

There is also a global ACL (see “Access Control List” on page 195). If the same MAC address is listed in both the global ACL and in an SSID’s ACL, and if either ACL would deny that station access to that SSID, then access will be denied.

| | | | | | |
|--|--|-------------------|--|--|--|
| Name: XN0429091D207 (10.100.47.12) | | Location: SS Desk | | Uptime: 7 days, 3 hours, 23 mins | |
| SSID: Xirrus-ss | | | | | |
| Access Control List Type: <input checked="" type="radio"/> Disabled <input type="radio"/> Allow List <input type="radio"/> Deny List | | | | | |
| MAC Address | | | | Delete | |
| <input type="text"/> | | | | <input type="button" value="Add"/> | |
| <input type="button" value="Delete All"/> | | | | <input type="button" value="Apply"/> <input type="button" value="Save"/> | |

Figure 124. Per-SSID Access Control List

Procedure for Configuring Access Control Lists

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



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

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

Groups

This is a status-only window that allows you to review user (i.e., wireless client) **Group** assignments. It includes the group name, Radius ID, **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](#).

| Status | | Name: SS-XNB (10.100.47.106) | | Location: SS Area | | Uptime: 0 days, 4 hours, 57 minutes | | | |
|----------------------|---------------|--------------------------------|---------------|-------------------|-----------------|-------------------------------------|---------------|---------------------|--------|
| ▶ Array | Group Name | Radius ID | Filter List | VLAN | Num | QoS | Roaming Layer | DHCP Pool | WPR |
| ▶ Network | Students | | none | | | 2 | 2-only | | On |
| ▶ RF Monitor | Staff | StaffMembers | none | | 22 | 2 | 2-only | | |
| ▶ Stations | Limits | | | | | | | | |
| ▶ Statistics | Group Name | Enabled | Station Limit | SSID Traffic | Station Traffic | Time On | Time Off | Days On | Active |
| System Log | Students | Enabled | 512 | 1000000 | 100000 | 7:00 | 18:00 | Mon Tue Wed Thu Fri | Yes |
| Configuration | Staff | Enabled | 512 | Unlimited | Unlimited | Always | Never | All | Yes |
| Express Setup | | | | | | | | | |
| ▶ Network | | | | | | | | | |
| ▶ Services | | | | | | | | | |
| ▶ VLANs | | | | | | | | | |
| ▶ Security | | | | | | | | | |
| ▶ SSIDs | | | | | | | | | |
| ▼ Groups | | | | | | | | | |
| Group Management | | | | | | | | | |

Figure 125. Groups

Understanding Groups

User groups allow administrators to assign specific network parameters to users (wireless clients) through RADIUS privileges rather than having to map users to 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](#)

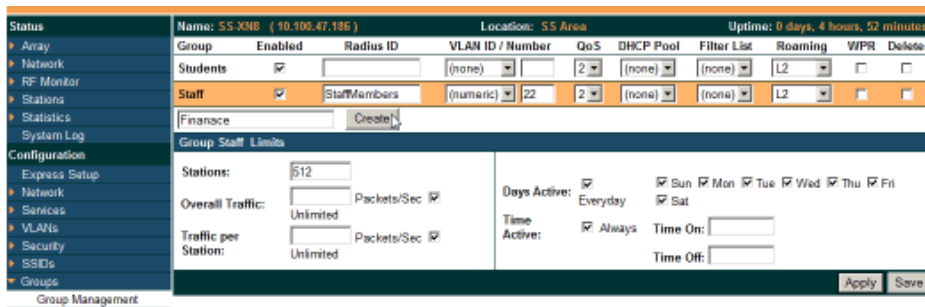
[Internal Radius](#)

[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.



| Group | Enabled | Radius ID | VLAN ID / Number | QoS | DHCP Pool | Filter List | Roaming | WPR | Delete |
|----------|-------------------------------------|--------------|------------------|-----|-----------|-------------|---------|--------------------------|--------------------------|
| Students | <input checked="" type="checkbox"/> | | (none) | 2 | (none) | (none) | L2 | <input type="checkbox"/> | <input type="checkbox"/> |
| Staff | <input checked="" type="checkbox"/> | StaffMembers | (numeric) 22 | 2 | (none) | (none) | L2 | <input type="checkbox"/> | <input type="checkbox"/> |
| Finance | <input type="checkbox"/> | | | | | | | | |

Configuration for selected group:

Stations: 512

Overall Traffic: Unlimited Packets/Sec

Traffic per Station: Unlimited Packets/Sec

Days Active: Everyday Sat

Time Active: Always Time On: Time Off:

Figure 126. 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 171](#)). **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 210](#). 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 168](#).
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 283](#).

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 235.
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 219 for details of WPR usage and configuration. Note that the Group Management window only allows you to set up an **Internal Splash** page and a **Landing Page URL**. The authentication options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the Array by a Radius server, this means the user has already been authenticated.

Group Limits

The Limits section allows you to limit the traffic or connection times allowed for this user group. Note that the IAPs—Global Settings window and the SSID management windows also have options to limit the number of stations, limit traffic, and/or limit connection times. If limits are set in more than one place, all limits will be enforced:

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

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

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

11. **Stations:** Enter the maximum number of stations allowed on this group. The default is 1536.
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. To delete an entry, click its **Delete** button.
17. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

DHCP Server

External Radius

Internal Radius

Security Planning

SSIDs

IAPs

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

XR4820 Wi-Fi Array

Name: XR4820 (10.100.57.54) Uptime: 30 days, 18 hours, 3 mins

Configuration Save changes to flash

- Express Setup
- Network
- Services
- VLANs
- Security
- SSIDs
- Groups
- IAPs**
 - IAP Settings
 - Global Settings
 - Global Settings .11a
 - Global Settings .11bg
 - Global Settings .11n
 - Advanced RF Settings
 - Intrusion Detection
 - LED Settings

| IAP | State | Channel | WiFi Mode | Antenna | Cell Size | TX Power | RX Threshold | Stations | WDS Link / Distance | MAC Address / BSSID | Description |
|------|-------|-------------|-----------|----------------------|-----------|----------|--------------|----------|---------------------|---------------------|-------------|
| iap1 | up | mon default | abgn | internal directional | monitor | 20 | -95 | 0 | | 00:0f:7d:43:bb:00 | |
| iap2 | up | 161 manual | an | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:10 | |
| iap3 | up | 1 manual | bgn | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:20 | |
| iap4 | up | 48 manual | an | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:30 | |
| iap5 | up | 153 manual | an | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:40 | |
| iap6 | up | 64 manual | an | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:50 | |
| iap7 | up | 11 manual | bgn | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:60 | |
| iap8 | up | 40 manual | an | internal directional | max | 20 | -90 | 0 | | 00:0f:7d:43:bb:70 | |

Figure 127. IAPs

The **Channel** column displays some status information that is not found elsewhere: the source of a channel setting. (Figure 128) If you set a channel manually (via [IAP Settings](#)), it will be labeled as **manual** next to the channel number (Figure 128). If an autochannel operation changed a channel, then it is labeled as **auto**. If the channel is set to the current factory default setting, the source will be **default**. This column also shows whether the channel selection is **locked**, or whether the IAP was automatically switched to this channel because the Array detected the signature of military **radar** in operation on a conflicting channel.

| IAP | State | Channel | WiFi Mode |
|-------|-------|---------|-----------|
| abgn1 | up | 44 | default |
| abgn2 | up | mon | default |
| abgn3 | up | 36 | default |
| abgn4 | up | 8 | manual |

Figure 128. Source of Channel Setting

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 235](#)

IAPs are configured using the following windows:

- [“IAP Settings” on page 237](#)
- [“Global Settings \(IAP\)” on page 243](#)
- [“Global Settings .11a” on page 250](#)
- [“Global Settings .11bg” on page 254](#)
- [“Global Settings .11n” on page 259](#)
- [“Advanced RF Settings” on page 262](#)
- [“LED Settings” on page 276](#)

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 user may be associated to any of the VLANs defined on the Array. The Layer 3 session is maintained by establishing a tunnel back to the originating Array. You should decide whether or not to use Layer 3 roaming based on your wired network design. Layer 3 roaming incurs extra overhead and may result in additional traffic delays.

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your Array, see [Step 21 to Step 23](#) in “[Global Settings \(IAP\)](#)” on page 243. To choose which of the enabled options are used by an SSID or Group, see “[Procedure for Managing SSIDs](#)” on page 214 (Step 13) or “[Procedure for Managing Groups](#)” on page 230.

IAP Settings

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

XR4820 Wi-Fi Array **XIRRUS** Uptime: 0 days, 0 hours, 8 mins

Configuration Save changes to flash

Express Setup Enable All IAPs Disable All IAPs Reset Channels

| IAP | Enabled | Band | WiFi Mode | Channel | Bond | Lock | Cell Size | Tx dBm | Rx dBm | WDS Dist. (miles) | Antenna Select | Description |
|------|-------------------------------------|---------|-----------|---------|------|--------------------------|-----------|--------|--------|-------------------|----------------|-------------|
| iap1 | <input checked="" type="checkbox"/> | monitor | abgn | mon | off | <input type="checkbox"/> | monitor | 20 | -95 | | Internal-Dir | |
| iap2 | <input checked="" type="checkbox"/> | 5 GHz | an | 56 | 52 | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |
| iap3 | <input checked="" type="checkbox"/> | 2.4 GHz | bgn | 1 | off | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |
| iap4 | <input checked="" type="checkbox"/> | 5 GHz | an | 48 | 44 | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |
| iap5 | <input checked="" type="checkbox"/> | 5 GHz | an | 153 | 149 | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |
| iap6 | <input checked="" type="checkbox"/> | 5 GHz | an | 64 | 60 | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |
| iap7 | <input checked="" type="checkbox"/> | 2.4 GHz | bgn | 11 | off | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |
| iap8 | <input checked="" type="checkbox"/> | 5 GHz | an | 40 | 36 | <input type="checkbox"/> | max | 20 | -90 | | Internal-Dir | |

Figure 129. 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 79.

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 262.
- For all 802.11a settings, go to “Global Settings .11a” on page 250.
- For all 802.11b settings, go to “Global Settings .11bg” on page 254.

- For all 802.11n settings, go to “Global Settings .11n” on page 259.

Procedure for Manually Configuring IAPs

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

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

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

2. In the **WiFi Mode** column, select the IEEE 802.11 wireless mode (or combination) that you want to allow on this IAP. When you select a WiFi Mode for an IAP, your selection in the **Channel** column will be checked to ensure that it is a valid choice for that WiFi Mode.

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

3. In the **Channel** column, select the [channel](#) you want this IAP to use from the channels available in the pull-down list. The list shows the channels available for the IAP selected (depending on which band the IAP is using). Channels that are shown in color indicate conditions that you need to keep in mind:
 - RED—Usage is not recommended, for example, because of overlap with neighboring radios.

- **YELLOW**—The channel has less than optimum separation (some degree of overlap with neighboring radios).
- **GRAY**—The channel is already in use.

The channels that are available for assignment to an IAP will differ, depending on the country of operation. If **Country** is set to **United States** in the [Global Settings \(IAP\)](#) window, then 24 channels are available to 802.11a(n) radios.

If you have enabled **Public Safety** in the [Advanced RF Settings](#) window ([Step 14](#)), 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. The Array will switch back to the original channel after 30 minutes if the channel is clear. If a radio was turned off because there were no available channels not affected by radar, the Array will now bring that radio back up after 30 minutes if that channel is clear. The 30 minute time frame complies with FCC regulations.

4. The **Bond** column only appears for XN Array models. It works together with the channel bonding options selected on the [Global Settings .11n](#) page. Also see the discussion of 802.11n bonding in “[Channel Bonding](#)” on page 38.
 - **Channel number**—If a channel number appears, then this channel is already bonded to the listed channel.
 - **Off**—Do not bond this channel to another channel.
 - **On**—Bond this channel to an adjacent channel. The bonded channel is selected automatically by the Array based on the **Channel** ([Step 3](#)).

The choice of banded channel is static—fixed once the selection is made.

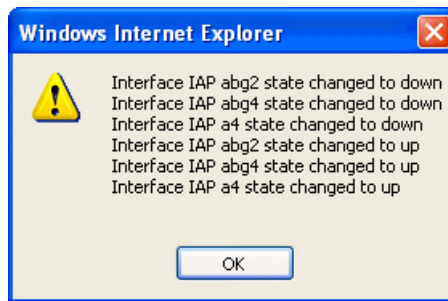
- **+1**—Bond this channel to the next higher channel number. Auto Channel bonding does not apply. This option is only available for some of the channels.
 - **-1**—Bond this channel to the next lower channel number. Auto Channel bonding does not apply. This option is only available for some of the channels.
5. Click the **Lock** check box if you want to lock in your channel selection so that 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 5 on page 265](#)). To set the cell size yourself, choose either **small**, **medium**, **large**, or **max** to use the desired pre-configured **cell size**, or choose **manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx dBm** (transmit) and **Rx dBm** (receive) fields. The default is **max**. If you select a value other than **auto**, the cell size will not be affected by cell size auto configuration.

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 24.

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



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

See Also

Coverage and Capacity Planning
Global Settings (IAP)

- Global Settings .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), and changing settings for beacons, station management, and advanced traffic optimization—including multicast processing, load balancing, and roaming. Changes you make on this page are applied to all IAPs, without exception.

| | | |
|-----------------------|---|---|
| Status | Name: XN8-1 (10.100.57.52) Uptime: 0 days, 14 hours, 53 mins | |
| ▶ Array | Country: | United States |
| ▶ Network | IAP Control: | <input type="button" value="Enable All IAPs"/> <input type="button" value="Disable All IAPs"/> |
| ▶ RF Monitor | Short Retries (1-128): | 7 |
| ▶ Stations | Long Retries (1-128): | 4 |
| ▶ Statistics | WiFi Alliance Mode: | <input checked="" type="radio"/> Off <input type="radio"/> On |
| System Log | Beacon Configuration | |
| IDS Event Log | Beacon Interval (20-1000 Kusec): | 100 |
| Configuration | DTIM Period (1-255 beacons): | 1 |
| Express Setup | 802.11h Beacon Support: | <input checked="" type="radio"/> Off <input type="radio"/> On |
| ▶ Network | WMM Power Save: | <input checked="" type="radio"/> Off <input type="radio"/> On |
| ▶ Services | Station Management | |
| ▶ VLANs | Station Re-Authentication Period (Seconds): | 0 |
| ▶ Security | Station Timeout Period (Seconds): | 300 |
| ▶ SSIDs | Max Station Association per Array (1-1536): | 1536 |
| ▶ Groups | Max Station Association per IAP (1-96): | 96 |
| ▼ IAPs | Max Phones per IAP (0-16): | 16 |
| IAP Settings | Block Inter-Station Traffic: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Global Settings | Allow Over Air Management: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Global Settings .11a | Advanced Traffic Optimization | |
| Global Settings .11bg | Multicast Processing: | Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription) |
| Global Settings .11n | Broadcast Rates: | <input checked="" type="radio"/> Optimized <input type="radio"/> Standard |
| Advanced RF Settings | Load Balancing: | <input type="radio"/> Off <input checked="" type="radio"/> On |
| Intrusion Detection | ARP Filtering: | <input type="radio"/> Off <input checked="" type="radio"/> Pass-thru <input type="radio"/> Proxy |
| LED Settings | Xirrus Roaming Layer: | <input type="radio"/> 2 and 3 <input checked="" type="radio"/> 2 only |
| ▶ WDS | Xirrus Roaming Mode: | <input type="radio"/> Off <input type="radio"/> Broadcast <input checked="" type="radio"/> Tunneled |
| ▶ Filters | Share Roaming Info With: | <input type="radio"/> All <input checked="" type="radio"/> In Range <input type="radio"/> Target Only |
| ▶ Clusters | | <input type="text"/> <input type="button" value="Add"/> |
| Tools | Xirrus Roaming Targets: | <input type="text"/> <input type="button" value="Delete"/> |
| Help | | |
| System Tools | | |

Figure 130. Global Settings (IAPs)

Procedure for Configuring Global IAP Settings



Some of the features below, such as Load Balancing, are only available if the Array's license includes the Xirrus Advanced RF Performance Manager (RPM). If a setting is unavailable (grayed out), then your license does not support the feature. See "About Licensing and Upgrades" on page 297.

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 423).

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 for 802.11a/n.

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 Control:** Click on the **Enable All IAPs** button to enable all IAPs for this Array, or click on the **Disable All IAPs** button to disable all IAPs.
3. **Short Retries:** This sets the maximum number of transmission attempts for a **frame**, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value (1 to 128) in the **Short Retry Limit** field if you want to increase or decrease this attribute.
4. **Long Retries:** This sets the maximum number of transmission attempts for a **frame**, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value (1 to 128) in the **Long Retry Limit** field if you want to increase or decrease this attribute.

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

Beacon Configuration

6. **Beacon Interval:** When the Array sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000 Kusecs. A Kusec is 1000 microseconds = 1 millisecond. The value you enter here is applied to all IAPs.
7. **DTIM Period:** A DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by the Array to a client device in sleep mode, alerting the device to broadcast traffic awaiting delivery. The **DTIM Period** is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all IAPs.
8. **802.11h Beacon Support:** This option enables beacons on all of the Array's radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.
9. **WMM Power Save:** Click **On** to enable Wi-Fi Multimedia Power Save support, as defined in IEEE802.11e. This option saves power and increases battery life by allowing the client device to doze between packets to save power, while the Array buffers downlink frames.

Station Management

10. **Station Re-Authentication Period:** This specifies an interval (in seconds) for station reauthentications. This is the minimum time period between station authentication attempts, enforced by the Array. This feature is part of the [Xirrus Advanced RF Security Manager \(RSM\)](#).
11. **Station Timeout Period:** Specify a time (in seconds) in this field to define the timeout period for station associations.

12. **Max Station Association per Array:** This option allows you to define how many station associations are allowed per Array (up to 1920 stations per Array). Note that the **Max Station Association per IAP** limit (below) may not be exceeded. If you have an unlicensed Array, this value is set to 1, which simply allows you to test the ability to connect to the Array.
13. **Max Station Association per IAP:** This defines how many station associations are allowed per IAP (up to 96 stations per IAP). Note that the SSIDs—SSID Management window also has a station limit option—**Station Limit** (page 218). 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.
14. **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.

15. **Block Inter-Station Traffic:** This option allows you to block or allow traffic between wireless clients that are associated to the Array. Choose either **Yes** (to block traffic) or **No** (to allow traffic).
16. **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

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

Select one of the following options:

- **Send multicasts unmodified.**
 - **Convert to unicast and send unicast packets to all stations.**
 - **Convert to unicast, snoop IGMP, and only send to stations subscribed (send as multicast if no subscription).**
 - **Convert to unicast, snoop IGMP, and only send to stations subscribed (don't send packet if no subscription).**
- 18. Broadcast Rates:** This changes the rates of broadcast traffic sent by the Array (including beacons). When set to **Optimized**, each broadcast or multicast packet that is transmitted on each radio is sent at the lowest transmit rate used by any client associated to that radio at that time. This results in each IAP broadcasting at the highest Array TX data rate that can be heard by all associated stations, improving system performance. The rate is determined dynamically to ensure the best broadcast/multicast performance possible. The benefit is dramatic. Consider a properly designed network (having -70db or better everywhere), where virtually every client should have a 54Mbps connection. In this case, broadcasts and multicasts will all go out at 54Mbps vs. the standard rate. Thus, with broadcast rate optimization on, broadcasts and multicasts use between 2% and 10% of the bandwidth that they would in Standard mode.

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

- 19. 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](#).

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

Choose **Off** to disable load balancing.

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

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

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

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

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

22. Xirrus Roaming Mode: This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3 (as specified in [Step 23](#)), 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 235 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 23](#)). 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).

23. 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.

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

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

See Also

Coverage and Capacity Planning

Global Settings .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.

| Status | | Name: XNB-1 (10.100.57.52) | | Uptime: 0 days, 14 hours, 56 m |
|----------------------|-------------------------------------|--|---|---|
| ▶ Array | | 6.0 | <input checked="" type="checkbox"/> Supported | <input checked="" type="checkbox"/> Basic |
| ▶ Network | | 9.0 | <input checked="" type="checkbox"/> Supported | <input type="checkbox"/> Basic |
| ▶ RF Monitor | | 12.0 | <input checked="" type="checkbox"/> Supported | <input checked="" type="checkbox"/> Basic |
| ▶ Stations | | 18.0 | <input checked="" type="checkbox"/> Supported | <input type="checkbox"/> Basic |
| ▶ Statistics | | 24.0 | <input checked="" type="checkbox"/> Supported | <input checked="" type="checkbox"/> Basic |
| System Log | | 36.0 | <input checked="" type="checkbox"/> Supported | <input type="checkbox"/> Basic |
| IDS Event Log | | 48.0 | <input checked="" type="checkbox"/> Supported | <input type="checkbox"/> Basic |
| | | 54.0 | <input checked="" type="checkbox"/> Supported | <input type="checkbox"/> Basic |
| Configuration | | | | |
| Express Setup | | | | |
| ▶ Network | | | | |
| ▶ Services | | | | |
| ▶ VLANs | | | | |
| ▶ Security | | | | |
| ▶ SSIDs | | | | |
| ▶ Groups | | | | |
| ▶ IAPs | | | | |
| IAP Settings | | | | |
| Global Settings | | | | |
| Global Settings .11a | | | | |
| | 802.11a Data Rates: | | | |
| | Data Rate Presets: | <input type="button" value="Optimize Range"/> <input type="button" value="Optimize Throughput"/> <input type="button" value="Restore Defaults"/> | | |
| | 802.11a IAP Control: | <input type="button" value="Enable All 802.11a IAPs"/> <input type="button" value="Disable All 802.11a IAPs"/> | | |
| | Channel Configuration: | <input type="button" value="Auto Configure"/> <input type="button" value="Factory Defaults"/> | | |
| | Set Cell Size: | <input type="text"/> <input type="button" value="Auto Configure"/> | | |
| | Auto Cell Period (seconds): | <input type="text"/> <input checked="" type="checkbox"/> None | | |
| | Auto Cell Size Overlap (%): | <input type="text" value="50"/> | | |
| | Auto Cell Min Tx Power (dBm): | <input type="text" value="10"/> <input type="button" value="Set Default"/> | | |
| | Fragmentation Threshold (256-2346): | <input type="text" value="2346"/> | | |
| | RTS Threshold (1-2347): | <input type="text" value="2347"/> | | |

Figure 131. Global Settings .11a

Procedure for Configuring Global 802.11a IAP Settings



Some of the features below, such as Auto Configure for Cell Size and Channel Configuration, are only available if the Array's license includes the Xirrus Advanced RF Performance Manager (RPM). If a setting is unavailable (grayed out), then your license does not support the feature. Please see "About Licensing and Upgrades" on page 297.

- 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**—data rates that can be used 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 Control:** 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.



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

RF Monitor Mode must be turned **On**. See “RF Monitor” on page 263

One of the radios must be in **monitor** mode with the default **RxdBm** setting of **-95**, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See “Procedure for Manually Configuring IAPs” on page 238.

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

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

For an overview of RF power and cell size settings, please see “Capacity and Cell Sizes” on page 27 and “Fine Tuning Cell Sizes” on page 28.

6. **Auto Cell Period (seconds):** You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.
7. **Auto Cell Size Overlap (%):** Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

8. **Auto Cell Min Tx Power (dBm):** Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.
9. **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.
10. **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.
11. Click **Save changes to flash** if you wish to make your changes 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.

| Status | Name: XIR8-1 (10.100.57.52) | | Uptime: 0 days, 45 hours, 0 mins |
|---|--|--|----------------------------------|
| <ul style="list-style-type: none"> Array Network RF Monitor Stations Statistics System Log IDS Event Log | 802.11g Data Rates: | 6.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 9.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 12.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 18.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 24.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 36.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 48.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 54.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic | |
| Configuration <ul style="list-style-type: none"> Express Setup Network Services VLANs Security SSIDs Groups IAPs <ul style="list-style-type: none"> IAP Settings Global Settings Global Settings .11a Global Settings .11bg Global Settings .11n Advanced RF Settings Intrusion Detection LED Settings | 802.11b Data Rates: | 1.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 2.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 5.5 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 11.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic | |
| | Data Rate Presets: | <input type="button" value="Optimize Range"/> <input type="button" value="Optimize Throughput"/> <input type="button" value="Restore Defaults"/> | |
| | 802.11bg IAP Control: | <input type="button" value="Enable All 802.11b/g IAPs"/> <input type="button" value="Disable All 802.11b/g IAPs"/> | |
| | Channel Configuration: | <input type="button" value="Auto Configure"/> <input type="button" value="Factory Defaults"/> | |
| | Set Cell Size: | <input type="text" value=""/> <input type="button" value="Auto Configure"/> | |
| | Auto Cell Period (seconds): | <input type="text" value=""/> <input checked="" type="checkbox"/> None | |
| | Auto Cell Size Overlap (%): | <input type="text" value="50"/> | |
| | Auto Cell Min Tx Power (dBm): | <input type="text" value="10"/> <input type="button" value="Set Default"/> | |
| | 802.11g Only: | <input type="radio"/> On <input checked="" type="radio"/> Off | |
| | 802.11g Protection: | <input checked="" type="radio"/> Auto CTS <input type="radio"/> Auto RTS <input type="radio"/> Off | |
| | 802.11g Slot: | <input checked="" type="radio"/> Auto <input type="radio"/> Short Only | |
| | 802.11b Preamble: | <input checked="" type="radio"/> Auto <input type="radio"/> Long Only | |
| | Fragmentation Threshold (256-2346): | <input type="text" value="2346"/> | |
| | RTS Threshold (1-2347): | <input type="text" value="2347"/> | |

Figure 132. Global Settings .11bg



Some of the features below, such as *Auto Configure for Cell Size* and *Channel Configuration*, are only available if the Array's license includes the *Xirrus Advanced RF Performance Manager (RPM)*. If a setting is unavailable (grayed out), then your license does not support the feature. Please see "About Licensing and Upgrades" on page 297.

Procedure for Configuring Global 802.11b/g IAP Settings

1. **802.11g Data Rates:** The Array allows you to define which data rates are supported for all 802.11g radios. Select (or deselect) 11g data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
 - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
 - **Supported Rate**—data rates that can be used to transmit to clients.
2. **802.11b Data Rates:** This task is similar to Step 1, but these data rates apply only to 802.11b IAPs.
3. **Data Rate Presets:** The 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.



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

RF Monitor Mode must be turned **On**. See “RF Monitor” on page 263

One of the radios must be in **monitor** mode with the default **RxdBm** setting of **-95**, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See “Procedure for Manually Configuring IAPs” on page 238.

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

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

For an overview of RF power and cell size settings, please see “Capacity and Cell Sizes” on page 27 and “Fine Tuning Cell Sizes” on page 28.

7. **Auto Cell Period (seconds):** You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient). The default value is **None**.
8. **Auto Cell Size Overlap (%):** Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB. The default value is **50%**.

9. **Auto Cell Min Tx Power (dBm):** Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes. The default value is **10**.
10. **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.
11. **802.11g Protection:** You should select **Auto CTS** or **Auto RTS** to provide automatic protection for all 802.11g radios in mixed networks (802.11b 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.

12. **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.
13. **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**.

14. **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.
15. **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.
16. Click **Save changes to flash** if you wish to make your changes 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 34.

| Status | | Name: XN8-1 (10.100.57.52) | | Uptime: 0 days, 15 hours, 4 mins | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|----------------------------|------------------------------|--|----------------------------------|-------------------------------------|--------------------------|-------------|----------------------|-----------|-------|---|------|-----|------|------|-------------------------------------|--------------------------|------|------|------|------|-------------------------------------|--------------------------|------|------|------|------|-------------------------------------|--------------------------|------|------|------|------|-------------------------------------|--------------------------|------|------|------|------|-------------------------------------|--------------------------|------|------|-------|-------|-------------------------------------|--------------------------|------|------|-------|-------|-------------------------------------|--------------------------|---|------|------|-------|-------|-------------------------------------|--------------------------|------|------|------|------|-------------------------------------|--------------------------|------|------|------|------|-------------------------------------|--------------------------|-------|------|------|------|-------------------------------------|--------------------------|-------|------|-------|-------|-------------------------------------|--------------------------|-------|------|-------|-------|-------------------------------------|--------------------------|-------|-------|-------|-------|-------------------------------------|--------------------------|-------|-------|-------|-------|-------------------------------------|--------------------------|-------|-------|-------|-------|-------------------------------------|--------------------------|--|--|--|--|--|--|--|--|---|--|---|--|---|--|---|--|
| <ul style="list-style-type: none"> ▶ Array ▶ Network ▶ RF Monitor ▶ Stations ▶ Statistics System Log IDS Event Log Configuration Express Setup ▶ Network ▶ Services ▶ VLANs ▶ Security ▶ SSIDs ▶ Groups ▼ IAPs <ul style="list-style-type: none"> IAP Settings Global Settings Global Settings .11a Global Settings .11bg Global Settings .11n Advanced RF Settings Intrusion Detection LED Settings ▶ WDS | 802.11n Data Rates: | | <table border="1"> <thead> <tr> <th>Spatial Streams</th> <th>Modulation & Coding</th> <th>Standard Rate</th> <th>Bonded Rate</th> <th>Bonded short GI Rate</th> <th>Supported</th> <th>Basic</th> </tr> </thead> <tbody> <tr> <td rowspan="7">1</td> <td>MCS0</td> <td>6.5</td> <td>13.5</td> <td>15.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS1</td> <td>13.0</td> <td>27.0</td> <td>30.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS2</td> <td>19.5</td> <td>40.5</td> <td>45.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS3</td> <td>26.0</td> <td>54.0</td> <td>60.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS4</td> <td>39.0</td> <td>81.0</td> <td>90.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS5</td> <td>52.0</td> <td>108.0</td> <td>120.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS6</td> <td>58.5</td> <td>121.5</td> <td>135.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td rowspan="9">2</td> <td>MCS7</td> <td>65.0</td> <td>135.0</td> <td>150.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS8</td> <td>13.0</td> <td>27.0</td> <td>30.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS9</td> <td>26.0</td> <td>54.0</td> <td>60.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS10</td> <td>39.0</td> <td>81.0</td> <td>90.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS11</td> <td>52.0</td> <td>108.0</td> <td>120.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS12</td> <td>78.0</td> <td>162.0</td> <td>180.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS13</td> <td>104.0</td> <td>216.0</td> <td>240.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS14</td> <td>117.0</td> <td>243.0</td> <td>270.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>MCS15</td> <td>130.0</td> <td>270.0</td> <td>300.0</td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> | Spatial Streams | Modulation & Coding | Standard Rate | Bonded Rate | Bonded short GI Rate | Supported | Basic | 1 | MCS0 | 6.5 | 13.5 | 15.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS1 | 13.0 | 27.0 | 30.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS2 | 19.5 | 40.5 | 45.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS3 | 26.0 | 54.0 | 60.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS4 | 39.0 | 81.0 | 90.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS5 | 52.0 | 108.0 | 120.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS6 | 58.5 | 121.5 | 135.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 2 | MCS7 | 65.0 | 135.0 | 150.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS8 | 13.0 | 27.0 | 30.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS9 | 26.0 | 54.0 | 60.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS10 | 39.0 | 81.0 | 90.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS11 | 52.0 | 108.0 | 120.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS12 | 78.0 | 162.0 | 180.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS13 | 104.0 | 216.0 | 240.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS14 | 117.0 | 243.0 | 270.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | MCS15 | 130.0 | 270.0 | 300.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 802.11n Mode: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | | TX Chains: <input type="radio"/> 1 <input type="radio"/> 2 <input checked="" type="radio"/> 3 | | RX Chains: <input type="radio"/> 1 <input type="radio"/> 2 <input checked="" type="radio"/> 3 | | Guard interval: <input checked="" type="radio"/> Short <input type="radio"/> Long | | Auto bond 5GHz channels: <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled | | 5 GHz channel bonding: <input checked="" type="radio"/> Dynamic <input type="radio"/> Static | | 2.4 GHz channel bonding: <input checked="" type="radio"/> Dynamic <input type="radio"/> Static | | Global channel bonding: <input type="button" value="Enable bonding on all IAPs"/> <input type="button" value="Disable bonding on all IAPs"/> | |
| Spatial Streams | Modulation & Coding | Standard Rate | Bonded Rate | Bonded short GI Rate | Supported | Basic | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | MCS0 | 6.5 | 13.5 | 15.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS1 | 13.0 | 27.0 | 30.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS2 | 19.5 | 40.5 | 45.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS3 | 26.0 | 54.0 | 60.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS4 | 39.0 | 81.0 | 90.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS5 | 52.0 | 108.0 | 120.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS6 | 58.5 | 121.5 | 135.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | MCS7 | 65.0 | 135.0 | 150.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS8 | 13.0 | 27.0 | 30.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS9 | 26.0 | 54.0 | 60.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS10 | 39.0 | 81.0 | 90.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS11 | 52.0 | 108.0 | 120.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS12 | 78.0 | 162.0 | 180.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS13 | 104.0 | 216.0 | 240.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS14 | 117.0 | 243.0 | 270.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | MCS15 | 130.0 | 270.0 | 300.0 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figure 133. Global Settings .11n

Procedure for Configuring Global 802.11n IAP Settings



802.11n operation is allowed only if the Array's license includes this feature. Please see "About Licensing and Upgrades" on page 297.

- 802.11n Data Rates:** The Array allows you to define which data rates are supported for all 802.11n radios. Select (or deselect) 11n data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
 - Basic Rate**—a wireless station (client) must support this rate in order to associate.
 - Supported Rate**—data rates that can be used to transmit to clients.
- 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 95 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.
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 37.
- 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 37.
- 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 39.

6. **Auto bond 5 GHz channels:** Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**. See [“Channel Bonding” on page 38](#).
7. **5 GHz channel bonding:** Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**. See [“Channel Bonding” on page 38](#).
8. **2.4 GHz channel bonding:** Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The default is **Dynamic**. See [“Channel Bonding” on page 38](#).
9. **Global channel bonding:** These buttons allow you to turn channel bonding on or off for all IAPs in one step. The effect of using one of these buttons will be shown if you go to the **IAP Settings** window and look at the **Bond** column. Clicking **Enable bonding on all IAPs** causes all IAPs to be bonded to their auto-bonding channel immediately, if appropriate. For example, an IAP will not be bonded if it is set to monitor mode, and 2.4 GHz radios will not be bonded. Click **Disable bonding on all IAPs** to turn off bonding on all IAPs immediately. See [“Channel Bonding” on page 38](#). Settings in [Step 7](#) and [Step 8](#) are independent of global channel bonding.

Advanced RF Settings

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

| Status | Name: Robin-XNB (10.100.54.245) | Location: Test Lab-123 | Uptime: 0 days, 16 hours, 37 m |
|-----------------------|--|---|--------------------------------|
| Array | RF Monitor | | |
| Network | RF Monitor Mode: | <input type="radio"/> Off <input checked="" type="radio"/> On | |
| RF Monitor | RF Resilience | | |
| Stations | Radio Assurance Mode: | Failure alerts & repairs, but no reboots | |
| Statistics | Enable Standby Mode: | <input type="radio"/> Yes <input checked="" type="radio"/> No | |
| System Log | Standby Target Address: | <input type="text"/> | |
| IDS Event Log | RF Power & Sensitivity | | |
| Configuration | Cell Size Configuration: | Auto Configure | |
| Express Setup | Sharp Cell: | <input checked="" type="radio"/> Off <input type="radio"/> On | |
| Network | RF Spectrum Management | | |
| Services | Configuration Status: | idle | |
| VLANs | Band Configuration: | Auto Configure | |
| Security | Channel Configuration: | Auto Configure Auto Negotiate & Configure Factory Defaults | |
| SSIDs | Auto Channel Configuration Mode: | <input type="radio"/> On Array PowerUp <input checked="" type="radio"/> Disabled | |
| Groups | Auto Channel Configure on Time (none or [day] hh:mm[am pm] ...): | <input type="text"/> | |
| IAPs | Channel List Selection: | <input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 40 <input checked="" type="checkbox"/> 44 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 52 <input checked="" type="checkbox"/> 56 <input checked="" type="checkbox"/> 60 <input checked="" type="checkbox"/> 64 <input type="checkbox"/> 100 <input type="checkbox"/> 104 <input type="checkbox"/> 108 <input type="checkbox"/> <input type="checkbox"/> 116 <input type="checkbox"/> 120 <input type="checkbox"/> 124 <input type="checkbox"/> 128 <input type="checkbox"/> 132 <input type="checkbox"/> 136 <input type="checkbox"/> 140 <input checked="" type="checkbox"/> 149 <input checked="" type="checkbox"/> 153 <input checked="" type="checkbox"/> 157 <input checked="" type="checkbox"/> 161 <input type="checkbox"/> | |
| IAP Settings | Auto Channel List: | Use Defaults Use All Channels | |
| Global Settings | Public Safety: | <input checked="" type="radio"/> Off <input type="radio"/> On | |
| Global Settings .11a | Station Assurance | | |
| Global Settings .11bg | Enable Station Assurance: | <input checked="" type="radio"/> Yes <input type="radio"/> No | |
| Global Settings .11n | Period: | 60 seconds | |
| Advanced RF Settings | Min Average Associated Time: | 30 seconds | |
| Intrusion Detection | Max Authentication Failures: | 3 | |
| LED Settings | Max Packet Error Rate: | 25 % | |
| WDS | Max Packet Retry Rate: | 25 % | |
| Filters | Min Packet Data Rate: | 10 Mbps | |
| Clusters | Min Received Signal Strength: | -85 dB | |
| Tools | Min Signal to Noise Ratio: | 10 dB | |
| Help | Max Distance from Array: | 1500 feet | |
| System Tools | | | |

Figure 134. Advanced RF Settings

About Standby Mode

Standby Mode supports the Array-to-Array fail-over capability. When you enable Standby Mode, the Array functions as a backup unit, and it enables its radios if it detects that its designated target Array has failed. The use of redundant Arrays to provide this fail-over capability allows Arrays to be used in mission-critical

applications. In Standby Mode, an Array monitors beacons from the target Array. When the target has not been heard from for 40 seconds, the standby Array enables its radios until it detects that the target Array has come back online. Standby Mode is off by default. Note that you must ensure that the configuration of the standby Array is correct. This window allows you to enable or disable Standby Mode and specify the primary Array that is the target of the backup unit. See also, “Failover Planning” on page 42.

Procedure for Configuring Advanced RF Settings



Some of the features below, such as Auto Configure for Cell Size and Channel Configuration, are only available if the Array’s license includes the Xirrus Advanced RF Performance Manager (RPM). If a setting is unavailable (grayed out), then your license does not support the feature. Please see “About Licensing and Upgrades” on page 297.

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

RF Monitor

1. **RF Monitor Mode:** Turning this mode **On** enables RF monitoring functionality, permitting the operation of features like intrusion detection.

RF Resilience

2. **Radio Assurance Mode:** When this mode is enabled, the monitor radio performs loopback tests on the Array. This mode requires RF Monitor Mode to be enabled (Step 1) to enable self-monitoring functions. It also requires a radio to be set to monitoring mode (see “Enabling Monitoring on the Array” on page 412).

Operation of Radio Assurance mode is described in detail in “Array Monitor and Radio Assurance Capabilities” on page 412.

The Radio Assurance mode scans and sends out probe requests on each channel, in turn. It listens for all probe responses and beacons. These tests

are performed continuously (24/7). If no beacons or probe responses are observed from a radio for a predetermined period, Radio Assurance mode will take action according to the preference that you have specified:

- **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
 - **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of one or all of the radios if needed.
 - **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets, and schedule reboots if needed.
 - **Disabled**—Disable IAP radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.
3. **Enable Standby Mode:** Choose **Yes** to enable this Array to function as a backup unit for the target Array, or choose **No** to disable this feature. See “About Standby Mode” on page 262.
 4. **Standby Target Address:** If you enabled the Standby Mode, enter the MAC address of the target Array (i.e., the address of the primary Array that is being monitored and backed up by this Array). To find this MAC address, open the Array Info window on the target Array, and use the Gigabit1 MAC Address.

RF Power & Sensitivity

For an overview of RF power and cell size settings, please see “Capacity and Cell Sizes” on page 27 and “Fine Tuning Cell Sizes” on page 28.



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

*RF Monitor Mode must be turned **On**. See “RF Monitor” on page 263*

*One of the radios must be in **monitor** mode, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See “Procedure for Manually Configuring IAPs” on page 238.*

5. **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**.
6. **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 28.

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

7. **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.
8. **Band Configuration:** Automatic band configuration is the recommended method for assigning bands to the abg(n) IAPs. It runs only on command, assigning IAPs to the 2.4GHz or 5GHz band when you click the **Auto Configure** button. The Array uses its radios to listen for other APs on the same channel, and it assigns bands based on where it finds the least interference. Auto band always assigns at least one radio to the 2.4GHz band. Auto band runs separately from auto channel configuration. If the band is changed for an IAP, associated stations will be disconnected and will then reconnect.
9. **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 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 **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 **Factory Defaults** to instruct the Array to return all IAPs to their factory preset channels.

10. **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.
11. **Auto Channel Configure on Time:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here. Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated. Time is specified in hours and minutes, using the format: **[day]hh:mm [am | pm]**. If you omit the optional **day** specification, channel configuration will run daily at the specified time. If you do not specify am or pm, time is interpreted in 24-hour military time. For example, Sat 11:00 pm and Saturday 23:00 are both acceptable and specify the same time.

12. **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.
13. **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.

14. **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.

Station Assurance

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

When a connection is experiencing problems and reaches one of these thresholds in the specified period of time, the Array responds with several actions: an event is triggered, a trap is generated, and a Syslog message is logged. For example, if a client falls below the threshold for **Min Average Associated Time**, this “bouncing” behavior might indicate roaming problems with the network’s RF design, causing the client to bounce between multiple arrays and not stay connected longer than the time to re-associate and then jump again. This can be corrected with RF adjustments. Station assurance alerts you to the fact that this station is encountering problems.

| Station Assurance | |
|-------------------------------|---|
| Enable Station Assurance: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Period: | <input type="text" value="60"/> seconds |
| Min Average Associated Time: | <input type="text" value="30"/> seconds |
| Max Authentication Failures: | <input type="text" value="3"/> |
| Max Packet Error Rate: | <input type="text" value="25"/> % |
| Max Packet Retry Rate: | <input type="text" value="25"/> % |
| Min Packet Data Rate: | <input type="text" value="10"/> Mbps |
| Min Received Signal Strength: | <input type="text" value="-85"/> dB |
| Min Signal to Noise Ratio: | <input type="text" value="10"/> dB |
| Max Distance from Array: | <input type="text" value="500"/> feet |

Figure 135. Station Assurance (Advanced RF Settings)

15. **Enable Station Assurance:** This is enabled by default. Click No if you wish to disable it, and click Yes to re-enable it. When station assurance is enabled, the Array will monitor connection quality indicators listed below and will display associated information on the [Station Assurance Status](#) page. When a threshold is reached, an event is triggered, a trap is generated, and a Syslog message is logged.
16. **Period:** In seconds, the period of time for a threshold to be reached. For example, the Array will check whether Max Authentication Failures has been reached in this number of seconds. The default value is 60 seconds.
17. **Min Average Associated Time:** (seconds) Station assurance detects whether the average length of station associations falls below this threshold during a period. The default value is 30 seconds.
18. **Max Authentication Failures:** Station assurance detects whether the number of failed login attempts reaches this threshold during a period. The default value is 3 failures.
19. **Max Packet Error Rate:** (%) Station assurance detects whether the packet error rate percentage reaches this threshold during a period. The default value is 25%.

20. **Max Packet Retry Rate:** (%) Station assurance detects whether the packet retry rate percentage reaches this threshold during a period. The default value is 25%.
21. **Min Packet Data Rate:** (Mbps) Station assurance detects whether the packet data rate falls below this threshold during a period. The default value is 10 Mbps.
22. **Min Received Signal Strength:** (dB) Station assurance detects whether the strength of the signal received from the station falls below this threshold during a period. The default value is -85 dB.
23. **Min Signal to Noise Ratio:** (dB) Station assurance detects whether the ratio of signal to noise received from the station falls below this threshold during a period. The default value is 10 dB.
24. **Max Distance from Array: Min Received Signal Strength:** (feet) Station assurance detects whether the distance of the station from the Array reaches this threshold during a period. The default value is 500 feet.

See Also

Coverage and Capacity Planning

Global Settings .11a

Global Settings .11bg

Global Settings .11n

IAPs

IAP Settings

Intrusion Detection

The Xirrus Array employs a number of IDS/IPS (Intrusion Detection System/Intrusion Prevention System) strategies to detect and prevent malicious attacks on the Wi-Fi network. This window allows you to adjust intrusion detection settings.

| Status | | Name: XNB-1 (10.100.57.52) | | Uptime: 2 days, 20 hours, 39 mins | | |
|----------------------|----------------------------------|--|---|---|--|-----------------------|
| Array | | | | | | Save changes to flash |
| Network | Intrusion Detection Mode: | <input type="radio"/> Off | <input checked="" type="radio"/> Standard | | | |
| RF Monitor | Auto Block Unknown Rogue APs: | <input checked="" type="radio"/> Off | <input type="radio"/> On | | | |
| Stations | Auto Block RSSI: | 50 | | | | |
| Statistics | Auto Block Level: | Automatically block unknown rogue APs with no encryption | | | | |
| System Log | Auto Block Network Types: | <input checked="" type="radio"/> All | <input type="radio"/> IBSS/Ad-hoc only | <input type="radio"/> ESS/Infrastructure only | | |
| IDS Event Log | DoS Attack Detection Settings | | | | | |
| Configuration | Attack/Event | Mode | Threshold (packets) | Period (seconds) | | |
| Express Setup | Beacon Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 20000 | 60 | | |
| Network | Probe Request Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 1000 | 60 | | |
| Services | Authentication Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 100 | 60 | | |
| VLANs | Association Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 100 | 60 | | |
| Security | Disassociation Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 100 | 60 | | |
| SSIDs | Deauthentication Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 100 | 60 | | |
| Groups | EAP Handshake Flood: | <input type="radio"/> Off <input type="radio"/> Auto <input checked="" type="radio"/> Manual | 100 | 60 | | |
| IAPs | Null Probe Response: | <input type="radio"/> Off <input checked="" type="radio"/> On | 2 | 60 | | |
| IAP Settings | MIC Error Attack: | <input type="radio"/> Off <input checked="" type="radio"/> On | 2 | 60 | | |
| Global Settings | Disassociation Attack: | <input type="radio"/> Off <input checked="" type="radio"/> On | 1 | 60 | | |
| Global Settings .11a | Deauthentication Attack: | <input type="radio"/> Off <input checked="" type="radio"/> On | 1 | 60 | | |
| Global Settings .11b | Duration Attack: | <input type="radio"/> Off <input checked="" type="radio"/> On | 10 | 2 | | |
| Global Settings .11n | Duration Attack NAV: | 5000 ms | | | | |
| Advanced RF Settings | Impersonation Detection Settings | | | | | |
| Intrusion Detection | Attack/Event | Mode | Threshold (packets) | Period (seconds) | | |
| LED Settings | AP impersonation | <input type="radio"/> Off <input checked="" type="radio"/> On | 1 | 60 | | |
| WDS | Station impersonation | <input type="radio"/> Off <input checked="" type="radio"/> On | 2 | 600 | | |
| Filters | Evil twin attack | <input type="radio"/> Off <input checked="" type="radio"/> On | | | | |
| | Sequence number anomaly | <input type="radio"/> Off <input type="radio"/> Data <input checked="" type="radio"/> Management | | | | |

Figure 136. Intrusion Detection Settings

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

- **Rogue Access Point Detection and Blocking**

Unknown access points are detected, and may be automatically blocked based on a number of criteria. See “About Blocking Rogue APs” on page 273.

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

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

- **Impersonation Detection**

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

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

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

About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see “Rogue Control List” on page 206), then the Array will take measures to prevent stations from staying associated to the rogue. When the monitor radio is scanning, any time it hears a beacon from a blocked rogue it sends out a broadcast “deauth” signal using the rogue’s BSSID and source address. This has the effect of disconnecting all of a rogue AP’s clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

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

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

Procedure for Configuring Intrusion Detection

RF Intrusion Detection and Auto Block Mode

1. **Intrusion Detection Mode:** This option allows you to choose the **Standard** intrusion detection method, or you can choose **Off** to disable this feature. See “Array Monitor and Radio Assurance Capabilities” on page 412 for more information.
 - **Standard**—enables the monitor radio to collect Rogue AP information.
 - **Off**—intrusion detection is disabled.

2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see “About Blocking Rogue APs” on page 273). Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block Unknown Rogue APs to **On**. Then the remaining Auto Block fields will be active.
3. **Auto Block RSSI:** Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.
4. **Auto Block Level:** Select rogue APs to block based on the level of encryption that they are using. The choices are:
 - Automatically block unknown rogue APs regardless of encryption.
 - Automatically block unknown rogue APs with no encryption.
 - Automatically block unknown rogue APs with WEP or no encryption.
5. **Auto Block Network Types:** Select rogues to automatically block by applying the criteria above only to networks of the type specified below. The choices are:
 - **All**—the unknown rogues may be part of any wireless network.
 - **IBSS/AD Hoc only**—only consider auto blocking rogues if they belong to an ad hoc wireless network (a network of client devices without a controlling Access Point, also called an Independent Basic Service Set—IBSS).
 - **ESS/Infrastructure only**—only consider auto blocking rogue APs if they are in infrastructure mode rather than ad hoc mode.

DoS Attack Detection Settings

6. **Attack/Event:** The types of DoS attack that you may detect are described in the [Type of Attack Table](#) on page 271. Detection of each attack type may be separately enabled or disabled. For each attack, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in

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

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

- **Manual** mode—threshold and period settings are used to detect a flood. Packets received are simply counted for the specified time period and compared against the flood threshold. The default for all of the floods is **Manual** mode.
 - **Auto** mode—the Array analyzes current traffic for packets of a given type versus traffic over the past hour to determine whether a packet flood should be detected. In this mode, threshold and period settings are ignored. This mode is useful for floods like beacon or probe floods, where the numbers of such packets detected in the air can vary greatly from installation to installation.
7. **Duration Attack NAV (ms)**: For the duration attack, you may also modify the default duration value that is used to determine whether a packet may be part of an attack. If the number of packets having at least this duration value exceeds the **Threshold** number in the specified **Period**, an attack is detected.

Impersonation Detection Settings

8. **Attack/Event**: The types of impersonation attack that you may detect are described in [Impersonation Attacks](#) on [page 272](#). Detection of each attack type may be turned **On** or **Off** separately. For **AP** or **Station Impersonation** attacks, a default **Threshold** and **Period (seconds)** are specified. If the number of occurrences of the type of packet being detected exceeds the threshold in the specified number of seconds, then the Array declares that an attack has been detected. You may modify the **Threshold** and **Period**.
9. **Sequence number anomaly**: You may specify whether to detect this type of attack in **Data** traffic or in **Management** traffic, or turn **Off** this type of detection.

LED Settings

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

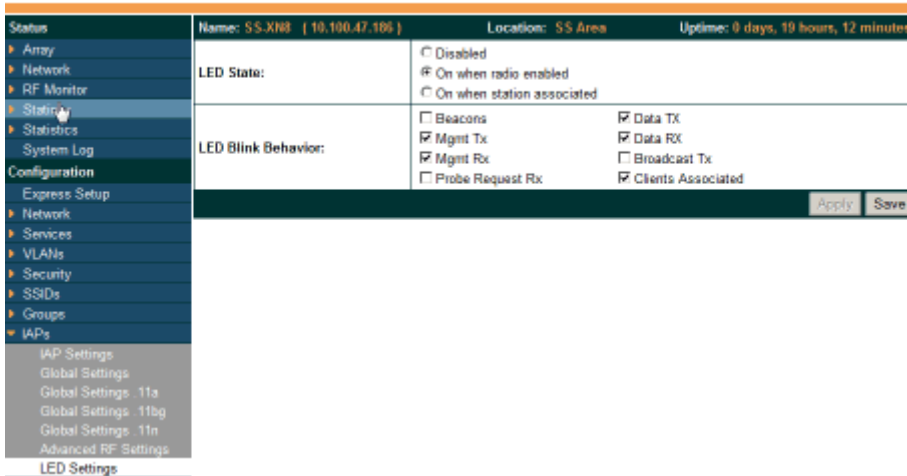


Figure 137. LED Settings

Procedure for Configuring the IAP LEDs

1. **LED State:** This option determines which event triggers the LEDs, either when an IAP is enabled or when an IAP first associates with the network. Choose **On Radio Enabled** or **On First Association**, as desired. You may also choose **Disabled** to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.
2. **LED Blink Behavior:** This option allows you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink. For default behavior, see “Array LED Operating Sequences” on page 63.
3. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Global Settings (IAP)

Global Settings .11a

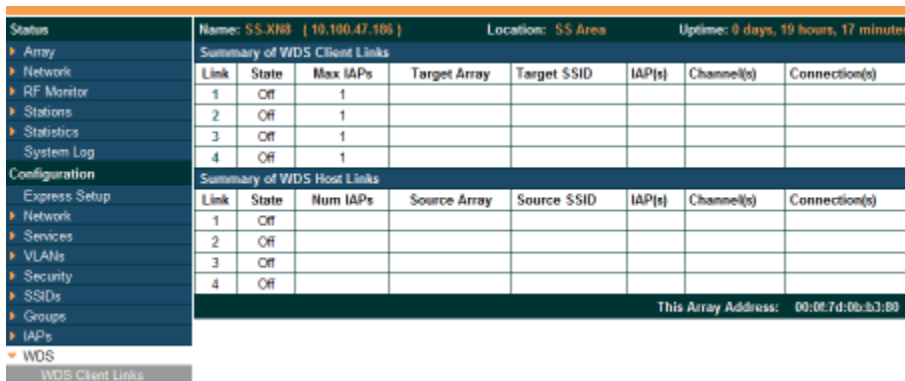
Global Settings .11bg

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 52 for an overview.



| Status | Name: SS-XNB (10.100.47.106) | | Location: SS Area | | Uptime: 0 days, 19 hours, 17 minutes | | | |
|------------------|--------------------------------|-------|-------------------|--------------|--------------------------------------|--------|------------|---------------------------------------|
| Array | Summary of WDS Client Links | | | | | | | |
| Network | Link | State | Max IAPs | Target Array | Target SSID | IAP(s) | Channel(s) | Connection(s) |
| RF Monitor | 1 | Off | 1 | | | | | |
| Stations | 2 | Off | 1 | | | | | |
| Statistics | 3 | Off | 1 | | | | | |
| System Log | 4 | Off | 1 | | | | | |
| Configuration | Summary of WDS Host Links | | | | | | | |
| Express Setup | Link | State | Num IAPs | Source Array | Source SSID | IAP(s) | Channel(s) | Connection(s) |
| Network | 1 | Off | | | | | | |
| Services | 2 | Off | | | | | | |
| VLANs | 3 | Off | | | | | | |
| Security | 4 | Off | | | | | | |
| SSIDs | | | | | | | | This Array Address: 00:0f:7d:0b:b3:80 |
| Groups | | | | | | | | |
| IAPs | | | | | | | | |
| WDS | | | | | | | | |
| WDS Client Links | | | | | | | | |

Figure 138. WDS

About Configuring WDS Links

A WDS link connects a client Array and a host Array (see [Figure 139 on page 279](#)). 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 52 for more illustrations.

The configuration for WDS is performed on the client Array only, as described in “WDS Client Links” on page 280. 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.

You may wish to consider configuring the WDS link IAPs so that only the WDS link SSIDs are active on them. See “Active IAPs” on page 225.

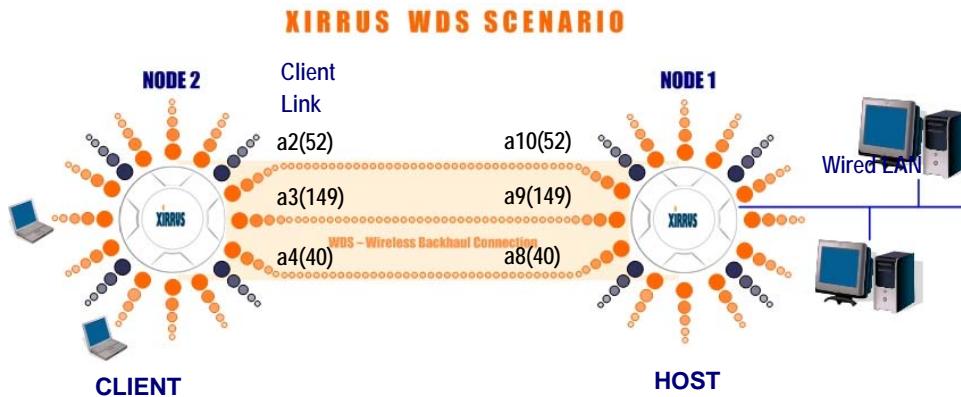


Figure 139. .Configuring a WDS Link



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).



When configuring WDS, if you use WPA-PSK (Pre-Shared Key) as a security mechanism, ensure that EAP is disabled. Communication between two Arrays in WDS mode will not succeed if the client Array has both PSK and EAP enabled on the SSID used by WDS. See **SSID Management**.



TKIP encryption does not support high throughput rates, per IEEE 802.11n. TKIP should *never* be used for WDS links on XR arrays.

Long Distance Links

If you are using WDS with an external antenna to provide backhaul over an extended distance, use the **WDS Dist. (Miles)** setting to prevent timeout

problems associated with long transmission times. (See “IAP Settings” on page 237) Set the approximate distance in miles between this IAP and the connected Array in the **WDS Dist. (Miles)** column. This will increase the wait time for frame transmission accordingly.

See Also

- SSID Management
- Active IAPs
- 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.

| Client Link | Enable | Max IAPs Allowed | Target Array Base MAC Address | Target SSID | Username | Password | Clear Settings |
|-------------|-------------------------------------|------------------|-------------------------------|-------------|----------|----------|----------------|
| 1 | <input checked="" type="checkbox"/> | 2 | 00:0f:7d:fa:00:80 | X-AW | wds | ***** | Clear |
| 2 | <input type="checkbox"/> | 1 | | | | | Clear |
| 3 | <input type="checkbox"/> | 1 | | | | | Clear |
| 4 | <input type="checkbox"/> | 1 | | | | | Clear |

| WDS Link | IAP/ Channel | | | | | | | |
|---------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|----------------------------------|
| | abgn1 11 | abgn2 monitor | abgn3 40+36 | abgn4 155 | an1 112+108 | an2 140 | an3 100+104 | an4 56+52 |
| Client Link 1 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Client Link 2 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Client Link 3 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Client Link 4 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| None | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> | <input checked="" type="radio"/> |

IAP Channel Assignment:

Figure 140. 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 **Save changes to flash** if you wish to make your changes permanent.

WDS Client Link IAP Assignments:

10. For each desired client link, select the IAPs that are part of that link. The IAP channel assignments are shown in the column headers.



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. **IAP Channel Assignment:** Click **Auto Configure** 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. **Allow Concurrent Stations:** Click **Yes** to instruct the Array to allow stations to associate to IAPs on a host Array that participate in a WDS link. The WDS host IAP will send beacons announcing its availability to wireless clients.
13. **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



This feature is only available if the Array's license includes the Xirrus Advanced RF Security Manager (RSM). If a setting is unavailable (grayed out), then your license does not support the feature. Please see "About Licensing and Upgrades" on page 297.

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.

| Name | Type | Protocol | Port | Source | Destination | Set QoS | Set VLAN | Enabled |
|-----------|-------|----------|------|------------------|-------------|---------|----------|---------|
| Global | | | | | | | | |
| new | allow | any | any | any | any | | | Yes |
| no-telnet | allow | any | any | any | any | | | Yes |
| Filters-A | | | | | | | | |
| -111 | deny | any | any | 111.111.111.0/24 | any | | | Yes |
| no-telnet | allow | any | any | any | any | | | Yes |

Orange arrow expands/collapses display

Figure 141. Filters

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.

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.

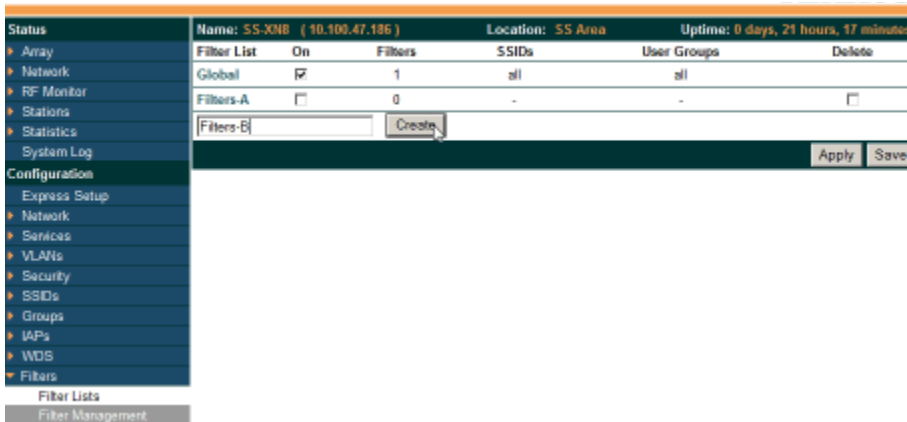


Figure 142. Filter Lists

Procedure for Managing Filter Lists

1. **Stateful Filtering:** Stateful operation of the integrated firewall can be **Enabled** or **Disabled**. If you have a large number of filters and you don't want to apply them in a stateful manner, you may use this option to turn the firewall off.

2. **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.
3. **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.
4. **Filters:** This read-only field displays the number of filters that belong to this filter list.
5. **SSIDs:** This read-only field lists the [SSIDs](#) that use this filter list.
6. **User Groups:** This read-only field lists the [Groups](#) that use this filter list.
7. **Delete:** Click this button to delete this filter list.
8. Click **Save changes to flash** if you wish to make your changes permanent.
9. 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.

Filters are applied in order, from top to bottom.
Click here to change the order.

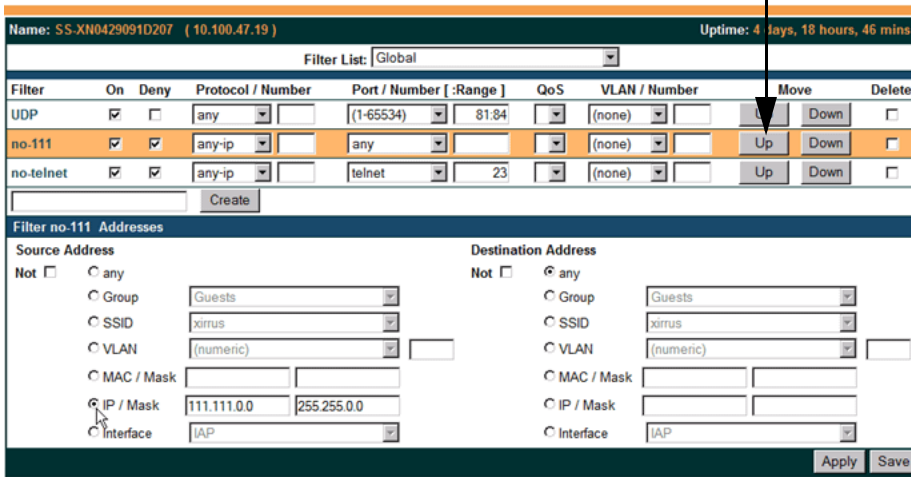


Figure 143. Filter Management

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:** This is a match criterion. From the pull-down list, choose the target port type for this filter. Choose **any** to instruct the Array to apply the filter to any port, or choose **1-65534** and enter a **Number**.

To enter a **Range** of port numbers, separate the start and end numbers with a colon as shown: **Start # : End #**.

| Port / Number [:Range] | |
|--------------------------|-------|
| (1-65534) | 81:84 |

8. **QoS:** (Optional) Set packets that match the filter criteria to this QoS level (0 to 3), selected 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 210.
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 171).
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, click its **Delete** button.
14. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Filters

Filter Statistics

Understanding QoS Priority on the Wi-Fi Array

VLANs

Clusters

Clusters allow you to configure multiple Arrays at the same time. Using WMI (or CLI), you may define a set of Arrays that are members of the cluster. Then you may enter Cluster mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member Arrays. When you exit cluster mode, configuration commands revert to applying only to the Array to which you are connected.

The read-only Clusters window provides you with an overview of all clusters that have been defined for this Array, and the Arrays that have been added to each. Arrays are listed in the left hand column by name under the cluster to which they belong. Each Array entry displays its IP Address, Username, and Password.

| Name: SS-XN0429091D207 (10.100.47.16) | | Uptime: 2 days, 0 hours, 37 mins | | |
|---|--------------|----------------------------------|----------|--------|
| Name | IP Address | Username | Password | Arrays |
| ▼ WestCluster | | | | 2 |
| BrianXN12 | 10.100.47.23 | admin | ••••• | |
| SS-XN0429091D207 | 10.100.47.16 | admin | ••••• | |

Figure 144. Clusters

Clusters are discussed in the following topics:

- Cluster Definition
- Cluster Management
- Cluster Operation

Cluster Definition

This window allows you to create clusters. All existing clusters are shown, along with the number of Arrays currently in each. Up to 16 clusters may be created, with up to 50 Arrays in each.

| Name: SS-XN0429091D207 (10.100.47.16) | | Uptime: 2 days, 0 hours, 41 mins |
|--|------------------|---------------------------------------|
| Cluster Name | Number of Arrays | |
| WestCluster | 2 | <input type="button" value="Delete"/> |
| <input type="text" value="EastCluster"/> | | <input type="button" value="Create"/> |
| | | <input type="button" value="Save"/> |

Figure 145. Cluster Definition

Procedure for Managing Cluster Definition

1. **New Cluster Name:** Enter a name for the new cluster in the field to the left of the **Create** button, then click **Create** to add this entry. The new cluster is added to the list in the window. Click on the cluster name, and you will be taken to the [Cluster Management](#) window for that cluster.
2. **Delete:** To delete a cluster, click its **Delete** button.
3. Click **Save changes to flash** if you wish to make your changes permanent.
4. Click a cluster to go to the [Cluster Management](#) window to add or remove Arrays in the cluster.

Cluster Management

This window allows you to add Arrays to or delete them from a selected cluster. A cluster may include a maximum of 50 Arrays.

Note that the Array on which you are currently running WMI is not automatically a member of the cluster. If you would like it to be a member, you must add it explicitly.

| Name: XN0429091D207 (10.100.47.12) | | Location: SS Desk | | Uptime |
|--------------------------------------|----------|-------------------|--|--------|
| Edit Cluster: WestCluster | | | | |
| Array | Username | Password | | |
| XN0429091D207 | admin | ••••• | | |
| Adrians-XN8 | admin | ••••• | | |

Figure 146. Cluster Management

Procedure for Managing Clusters

1. **Edit Cluster:** Select the cluster to display and manage on this window. All of the Arrays already defined for this cluster are shown, and you may add additional Arrays to this list.
2. **Array:** Enter the hostname or IP address of the Array that you wish to add to this cluster.
3. **Username/Password:** In these columns, enter the administrator name and password for access to the Array.
4. Click the **Add Array** button to enter the Array.
5. To delete an Array, click its **Delete** button.
6. Click **Save changes to flash** if you wish to make your changes permanent.

Cluster Operation

This window puts WMI into Cluster Mode. In this mode, all configuration operations that you execute in WMI or CLI are performed on the members of the cluster. They are **not** performed on the Array where you are running WMI, unless it is a member of the cluster.

You must use the **Save changes to flash** button at the top of configuration windows to permanently save your changes in Cluster Mode, just as you would in normal operation. When you are done configuring Arrays in the cluster, return to this window and click the **Exit** button to leave Cluster Mode.

| Name: SS-XN0429091D207 (10.100.47.16) | | Uptime: 2 days, 0 hours, 47 mins |
|---|------------------|----------------------------------|
| Cluster Name | Number of Arrays | |
| EastCluster | 0 | Operate |
| WestCluster | 2 | Operate |

Figure 147. Cluster Mode Operation

Procedure for Operating in Cluster Mode

1. **Operate:** Click the **Operate** button to the right of the desired cluster. A message informs you that you are operating in cluster mode. Click **OK**. The **Operate** button is replaced with an **Exit** button.

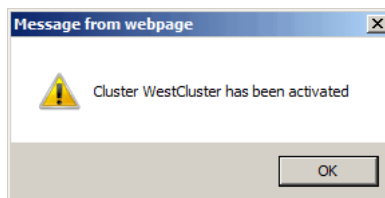


Figure 148. Cluster Mode Activation

2. Select a WMI window for settings that you wish to configure for the cluster, and proceed to make the desired changes.
3. Proceed to any additional pages where you wish to make changes.

4. Some Status and Statistics windows will present information for all Arrays in the cluster.
5. Click the **Save** button when done if you wish to save changes on the cluster member Arrays.
6. **Exit:** Click the **Exit** button to the right of the operating cluster to terminate Cluster Mode. The WMI returns to normal operation—managing only the Array to which it is connected.

Status and Statistics Windows in Cluster Mode

In Cluster Mode, many of the Status and Statistics windows will display information for all of the members of the cluster. You can tell whether a window displays cluster information—if so, it will display the Cluster Name near the top, as shown in [Figure 149](#).

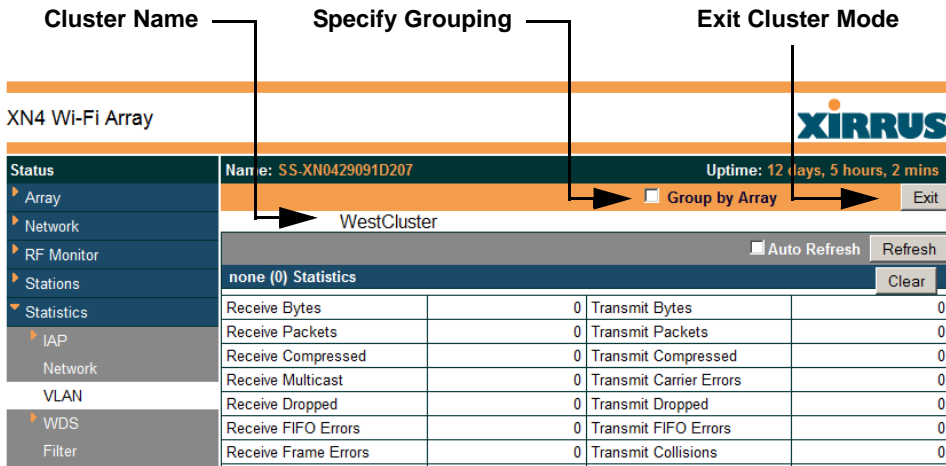


Figure 149. Viewing Statistics in Cluster Mode

You have the option to show aggregate information for the cluster members, or click the **Group by Array** check box to separate it out for each Array.

You may terminate cluster mode operation by clicking the **Exit** button to the right of the **Group by Array** check box.

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 308](#)
- [“Options” on page 309](#)
- [“Logout” on page 312](#)

Note that the **Tools** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See [Figure 39](#) on page 80)

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 85](#)
- [“Configuring the Wi-Fi Array” on page 137](#)

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.

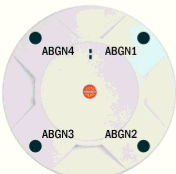
| | | |
|---|---|---|
| Status | Name: SS-XN0429091D207 (10.100.47.16) | Uptime: 8 days, 2 hours, 49 mins |
| Array | System | |
| Network | Reboot: | <input type="button" value="Save & Reboot"/> <input type="button" value="Reboot"/> |
| RF Monitor | Software Upgrade: | <input type="button" value="Browse..."/> <input type="button" value="Upgrade"/> |
| Stations | License Key: | 19XLUY-PTKCY-K2WEF-MGGV7 <input type="button" value="Upgrade"/> |
| Statistics | Remote TFTP Server: | <input type="text"/> |
| System Log | Remote Boot Image: | <input type="text"/> |
| Configuration | Remote Configuration: | <input type="text"/> |
| Express Setup | Configuration | |
| Network | Update From Remote File: | <input type="button" value="Browse..."/> <input type="button" value="Update"/> |
| Services | Update From Local File: | <input type="text"/> <input type="button" value="Update"/> |
| VLANs | Save To Local File: | <input type="text"/> <input type="button" value="Save"/> <input type="button" value="Set Restore Point"/> |
| Security | Download Current Configuration: | xs_current.conf |
| SSIDs | Reset to Factory Defaults: | <input type="button" value="Reset"/> <input type="button" value="Reset/ Preserve IP Settings"/> |
| Groups | Diagnostics | |
| IAPs | Diagnostic Log: | xs_diagnostic.log <input type="button" value="Create"/> |
| WDS | Web Page Redirect | |
| Filters | Upload File: | <input type="button" value="Browse..."/> <input type="button" value="Upload"/> |
| Clusters | Remove File: | <input type="text"/> <input type="button" value="Delete"/> <input type="button" value="List Files"/> |
| Tools | Download Sample Files: | wpr.pl hs.css |
| System Tools | Network Tools | |
| CLI | System Command: | <input type="radio"/> Trace Route <input type="radio"/> Ping <input type="radio"/> RADIUS Ping |
| Options | Hostname / IP Address: | 10.100.47.16 |
| Logout | Timeout: | 10 |
| Log Messages | Execute System Command: | <input type="button" value="Execute"/> |
| Critical 4 | Progress | |
| Warning 4 | Status | |
| Information 500 | Configuration file OK | |
|  | Status is shown here | Progress is shown here |
| | <input type="button" value="Save"/> | |

Figure 150. System Tools



Some tools, such as Network Tools and Diagnostics, are only available if the Array's license includes the Xirrus Advanced RF Analysis Manager (RAM). If a tool is unavailable (grayed out), then your license does not support the feature. See "About Licensing and Upgrades" on page 297.

About Licensing and Upgrades

The Array's license determines many of the features that are available on the Array. For example, automatic cell sizing and channel allocation require a license that includes the [Xirrus Advanced RF Performance Manager \(RPM\)](#). Also, IEEE 802.11n operation on XN model Arrays is a licensed feature. To check the features supported by your license, see "Array Information" on page 90.

If you are upgrading the Array to add new features that are not supported by your existing license, **you must enter the new license key that includes the upgrade's features before upgrading.**

Similarly, if you are upgrading the Array for a new release, you must enter the new license key that enables the operation of that release before upgrading. If you do not enter the new license first, the Array will display a message and revert to the previous software image, rather than trying to run new software for which it is not licensed. Major releases will need a new license key, but minor releases will not. For example, to upgrade from ArrayOS Release 5.0.5 to Release 5.1, you must enter a new license key. To upgrade from ArrayOS Release 5.0.5 to Release 5.0.6, use your existing license key.

If you will be entering license keys and performing upgrades on many Arrays, the effort will be streamlined by using the Xirrus Management System (XMS).

Procedure for Configuring System Tools

These tools are broken down into the following sections:

- System
- Configuration
- Diagnostics
- Web Page Redirect

- Network 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 62](#). 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. **Please note that you typically will need to enter a new license key to cover the upgrade’s features before clicking the Upgrade button.** See “[About Licensing and Upgrades](#)” on [page 297](#) for details.

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 418](#) 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 provides you with a new license key for your Array, use this field to enter it, then click the **Upgrade** button to the right. 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.

Automatic Updates from Remote Image or Configuration File

The Array software image or configuration file can be downloaded from an external server. In large deployments, all Arrays can be pointed to one TFTP server instead of explicitly initiating software image uploads to all Arrays. When the Array boots, the Array will download the software image from the specified TFTP server. Similarly, if you decide to change a setting in the Arrays, you can simply modify a single configuration file. After the Arrays are rebooted, they will automatically download the new configuration file from a single location on the specified TFTP server.

- 4. Remote TFTP Server:** This field defines the path to a TFTP server to be used for automated remote update of software image and configuration files when rebooting. You may specify the server using an IP address or host name.
- 5. Remote Boot Image:** When the Array boots up, it fetches the software image file specified here from the TFTP server defined above, and upgrades to this image before booting. This must be an Array image file with a **.bin** extension.

Make sure to place the file on the TFTP server. If you disable the remote boot image (by blanking out this field) or if the image can't be transferred, the Array will fall back to booting whatever image is on the compact flash.



The Remote Boot Image or Configuration update happens every time that the Array reboots. If you only want to fetch the remote image or configuration file one time, be sure to turn off the remote option (blank out the field on the System Tools page) after the initial download. When a remote boot image is used, the image is transferred directly into memory and is never written to the compact flash.

- 6. Remote Configuration:** When the Array boots up, it fetches the specified configuration file from the TFTP server defined above, and applies this configuration **after** the local configuration is applied. The remote configuration must be an Array configuration file with a **.conf** extension. Make sure to place the file on the TFTP server.

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.

A remote configuration is never saved to the compact flash unless you issue a Save command.

Configuration

- 7. Update from Remote File:** This field allows you to define the path to a configuration file (one that you previously saved—see [Step 9](#) and [Step 10](#) 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.
- 8. 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 using the **Save changes to flash** button at the top of each window.

- **history/saved-yyyyymmdd-pre-update.conf:**
history/saved-yyyyymmdd-post-update.conf:
Two files are saved for an upgrade: the setting values from just before an upgrade was performed, and the initial values afterward. The filename includes the upgrade date.
- **history/saved-yyyyymmdd-auto.conf:** Each time you use the **Save changes to flash** button, an “auto” file is saved with the settings current at that time.
- **history/saved-yyyyymmdd-pre-reset.conf:**
history/saved-yyyyymmdd-post-reset.conf:
Each time you use one of the **Reset to Factory Default** buttons, two files are saved: the setting values from just before the reset, and the initial values afterward. The filename includes the reset date.
- **history/saved-yyyyymmdd-hhmm.conf:** The setting values that were explicitly saved using the **Set Restore Point** button (see [Step 9](#) below).

Click **Update** to update your configuration settings. Note that the History folder allows a maximum of 16 files. The oldest file is automatically deleted to make room for each new file.

9. **Save to Local File:** There are a few options for explicitly requesting the Array to save your current configuration to a file on the Array:
 - To view the list of configuration files currently on the Array, click the down arrow to the right of this field. If you wish to replace one of these files (i.e., save the current configuration under an existing file name), select the file, then click **Save**. Note that you cannot save to the file names **factory.conf**, **lastboot.conf**, and **saved.conf** - these files are write-protected.
 - You may enter the desired file name, then click **Save**.
 - Click **Set Restore Point** to save a copy of the current configuration, basing the file name on the current date and time. For example:

history/saved-20100318-1842.conf

Note that the configuration is automatically saved to a file in a few situations, as described in [Step 8](#) above.



***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.*

- 10. 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.
- 11. 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 147), or if you have configured management over a VLAN it will maintain the management VLAN's IP address (see "[VLAN Management](#)" on page 173). *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

- 12. 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 151)

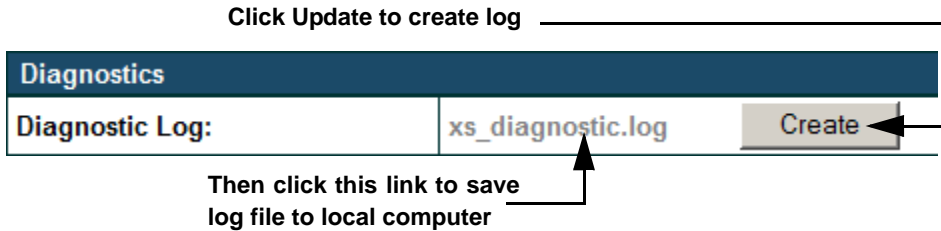


Figure 151. Saving the Diagnostic Log

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 15](#) below to view the default files. See [Step 14 on page 217](#) 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.

| Web Page Redirect | |
|------------------------|--|
| Upload File: | <input type="text" value="downloads\wpr-New.pl"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/> |
| Remove File: | <input type="text"/> <input type="button" value="Delete"/> <input type="button" value="List Files"/> |
| Download Sample Files: | wpr.pl hs.css |

Figure 152. Managing WPR Splash/Login page files

- 13. 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.

14. **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.
15. **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.

Network Tools

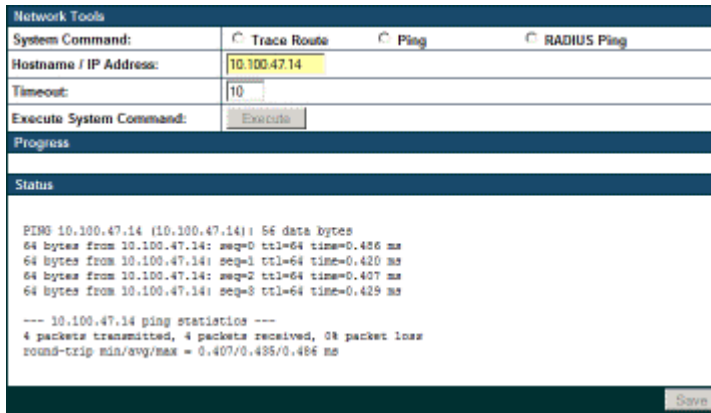


Figure 153. System Command (Ping)

16. **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.

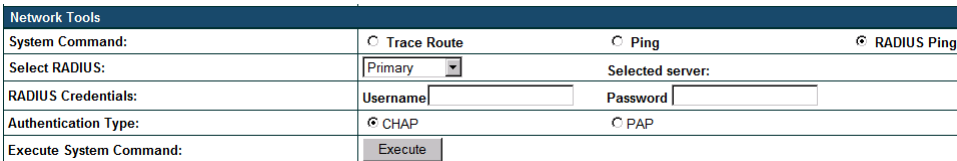


Figure 154. Radius Ping Command

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. When you make a choice in this field, additional fields will be displayed. Set **Select RADIUS** to **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**. Select the **Authentication Type**, **PAP** or **CHAP**. Click the **Execute** button to run the command. The message **Testing RADIUS connection** appears. Click **OK** to proceed.

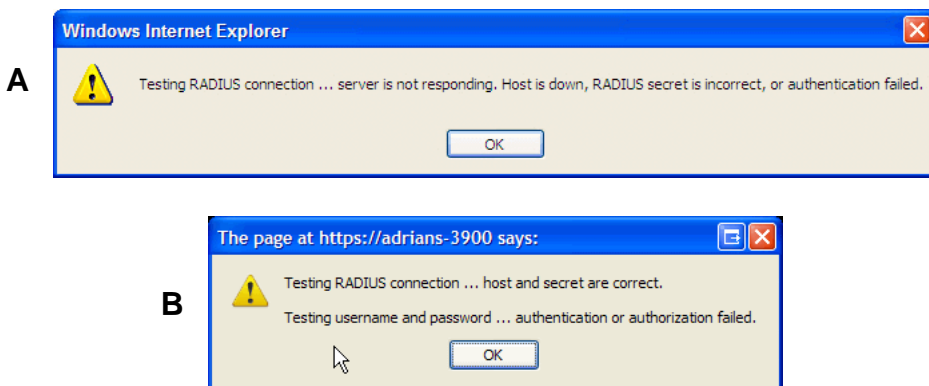


Figure 155. Radius Ping Output

17. **IP Address:** For Ping or Trace Route, enter the IP address of the target device.
18. **Timeout:** For Ping or Trace Route, enter a value (in seconds) before the action times out.
19. **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.

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

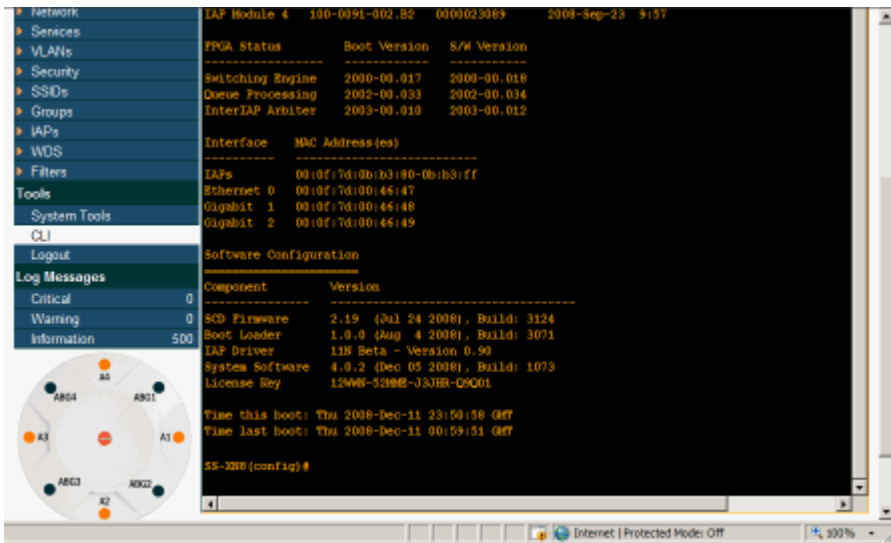


Figure 156. CLI Window

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.

Options

This window allows you to customize the behavior and appearance of the WMI.

| Status | Name: SS_XN0429091D207 (10.100.47.16) | Uptime: 2 days, 23 hours, 28 mins |
|--------------|---|-----------------------------------|
| ▸ Array | Style: <input type="text" value="Classic"/> <input type="button" value="Apply"/> | |
| ▸ Network | Refresh interval in seconds: <input type="text"/> <input type="button" value="Apply"/> | |
| ▸ RF Monitor | Close menu section when deselected: <input type="radio"/> Yes <input checked="" type="radio"/> No | |
| ▸ Stations | Clear screen when loading new page: <input checked="" type="radio"/> Yes <input type="radio"/> No | |
| ▸ Statistics | | |
| System Log | | |

Figure 157. WMI Display Options

Procedure for Configuring Options

1. **Style:** This option allows you to change the appearance and operation of the user interface. Select one of the available styles from the drop-down list. Click the **Apply** button to view the WMI with the selected style.

Note that some styles just change the display appearance (the skin) of WMI, in much the same way as changing the display theme used in Windows 7. Other styles include more extensive changes to the interface.



Figure 158. iPhone Style Option

For example, the **iPhone** style option (Figure 158) has a more compact display, suitable for use on smart phones. It shows the main menu in the orange bar at the top, rather than as a tree in its own frame on the left. Clicking one of the menu choices at the top in Figure 158 will display a drop-down menu with the options for that menu choice. Menus may be toggled on and off by clicking on the headers (Status, Configuration, etc.).

2. **Refresh Interval in Seconds:** Many of the windows in the Status section of the WMI have an Auto Refresh option. You may use this setting to change how often a status or statistics window is refreshed, if its auto refresh option is enabled. Enter the desired number of seconds between refreshes. The default refresh interval is 30 seconds.
3. **Close Menu Section when Deselected:** When you click a main section such as **SSIDs** in the left frame of the WMI (the navigation tree), the section is expanded to show submenu choices. Click **Yes** to automatically close any open submenus when you select a different section. If you click **No**, all menu sections will remain expanded once opened. **No** is the default. Note that if you enable this feature and you expand a section by clicking its orange arrow, the section will stay open as you select windows in other menu sections.
4. **Clear Screen When Loading New Page:** When this option is enabled and you click on a page that takes a long time to load for any reason, the main area of the screen is blanked out and displays a **Loading...** message. If this option is disabled, WMI simply shows the page you were viewing until the new page loads.

Logout

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

| | |
|------------------------------|--------------------------|
| Name: SS-XMR (10.100.47.186) | Location: SS Area |
| Current Status: | Logged Out |
| User Name: | <input type="text"/> |
| User Password: | <input type="password"/> |

Login

Figure 159. 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 an SSH connection to the Array. Topics discussed include:

- [“Establishing a Secure Shell \(SSH\) Connection” on page 313.](#)
- [“Getting Started with the CLI” on page 315.](#)
- [“Top Level Commands” on page 317.](#)
- [“Configuration Commands” on page 326.](#)
- [“Sample Configuration Tasks” on page 360.](#)



*Some commands are only available if the Array's license includes appropriate Xirrus **Advanced Feature Sets**. If a command is unavailable, an error message will notify you that your license does not support the feature. See [“About Licensing and Upgrades” on page 297.](#)*

See Also

[Establishing Communication with the Array](#)
[Network Map](#)
[System Tools](#)

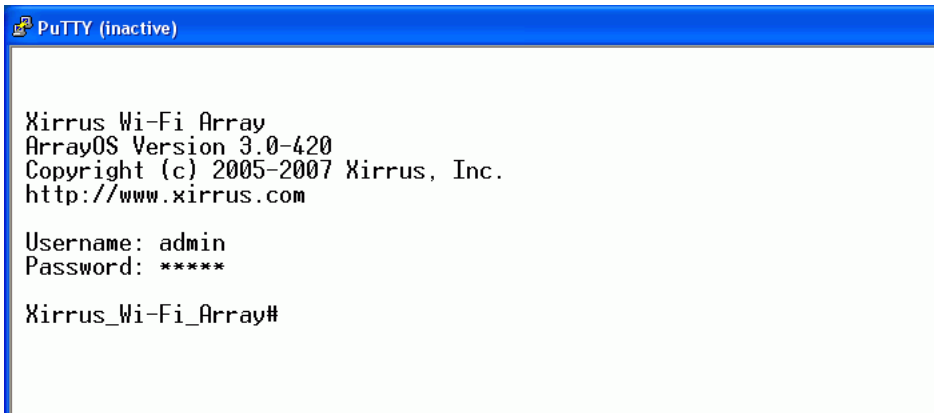
Establishing a Secure Shell (SSH) Connection

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.
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.



```
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#
```

Figure 160. 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.

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.



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

Username: admin
Password: ****

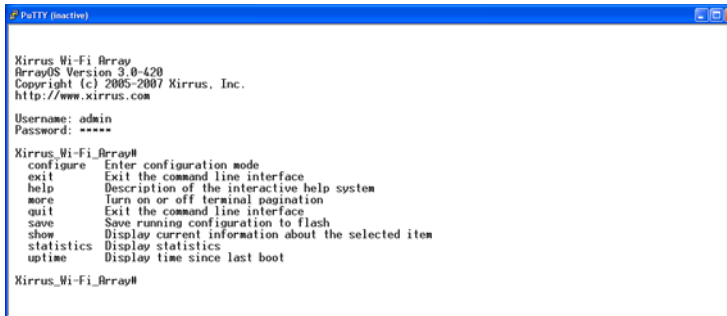
Xirrus_Wi-Fi_Array# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?').
Xirrus_Wi-Fi_Array#
```

Figure 161. 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.



```

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

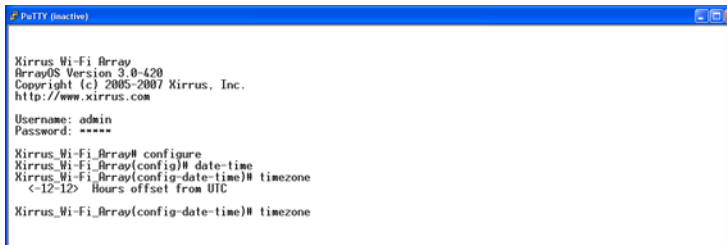
Username: admin
Password: *****

Xirrus_Wi-Fi_Array#
configure  Enter configuration mode
exit      Exit the command line interface
help     Description of the interactive help system
more     Turn on or off terminal pagination
quit     Exit the command line interface
save     Save running configuration to flash
show     Display current information about the selected item
statistics Display statistics
uptime   Display time since last boot

Xirrus_Wi-Fi_Array#
    
```

Figure 162. Full Help

Figure 163 shows an example of how the Help system can provide the argument and format when specifying the time zone under the **date-time** command.



```

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)# date-time
Xirrus_Wi-Fi_Array(config-date-time)# timezone
<-12-12> Hours offset from UTC

Xirrus_Wi-Fi_Array(config-date-time)# timezone
    
```

Figure 163. 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 326](#).

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 326 . |
| 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 315 . |
| 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 321. |
| statistics | Display statistical data about the Array. See “statistics Commands” on page 324. |
| 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. |
| cluster | Make configuration changes to multiple Arrays. |
| 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. |

| Command | Description |
|----------------------|--|
| filter | Define protocol filter parameters. |
| 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. |
| interface | Select the interface to configure. |
| 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. |
| 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. |
| restore | 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. |
| ssid | Configure the SSID parameters. |
| statistics | Display statistics. |
| syslog | Enable, disable or configure the Syslog Server. |
| uptime | Display time since the last boot. |
| vlan | Configure VLAN parameters. |
| wifi-tag | 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. |
| rss-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 iap2 |
| 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 |

| Command | Description |
|------------|---|
| wds | Display statistical data for the defined active WDS (Wireless Distribution System) links. FORMAT: statistics wds 1 |
| <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 360.

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 |

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 |

cluster

The **cluster** command [**Xirrus_Wi-Fi_Array(config)# cluster**] is used to create and operate clusters. Clusters allow you to configure multiple Arrays at the same time. Using CLI (or WMI), you may define a set of Arrays that are members of the cluster. Then you may switch the Array to Cluster operating mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member Arrays. When you exit cluster mode, configuration commands revert to applying only to the Array to which you are connected.

For more information, see “Clusters” on page 289.

| Command | Description |
|-------------|--|
| add | Create a new Array cluster. Enters edit mode for that cluster to allow you to specify the Arrays that belong to the cluster. FORMAT: cluster add [cluster-name] |
| del | Delete an Array cluster. Type del ? to list the existing clusters. FORMAT: cluster del [cluster-name] |
| edit | Enter edit mode for selected cluster to add or delete Arrays that belong to the cluster. FORMAT: cluster edit [cluster-name] |
| end | Exit Cluster configuration mode. Configuration returns to normal operation, affecting this Array only. FORMAT: cluster end |

| Command | Description |
|----------------|--|
| operate | Enter Cluster operation mode. All configuration commands are applied to all of the selected cluster's member Arrays until you give the end command (see above). FORMAT: cluster operate [cluster-name] |
| reset | Delete all clusters. FORMAT: cluster reset |

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 cp | 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 | <p>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.</p> <p>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.</p> <p>FORMAT: file remote-config <config-file.conf></p> <p>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.</p> |
| remote-image | <p>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.</p> <p>FORMAT: file remote-image <image-file.bin></p> <p>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.</p> |
| remote-server | <p>Sets up a TFTP server to be used for automated remote update of software image and configuration files when rebooting.</p> <p>FORMAT: file remote-server A.B.C.D</p> |
| rename | <p>Rename a file.</p> |

| Command | Description |
|-------------|---|
| scp | Copy a file to or from a remote system. You may specify the port to use. |
| 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 |
| stateful | Enable or disable stateful filtering (firewall). FORMAT: Stateful [enable disable on off] |

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 228.

| 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] |

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 |

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 management parameters.

| Command | Description |
|-------------------------|---|
| <code><cr></code> | Enter management mode. FORMAT: management <cr> |

The following types of settings may be configured in management mode:

- console Configure console management parameters
- fips Enable/disable FIPS 140-2, Level 2 Security.
See [Appendix E: Implementing FIPS Security](#)
- https Enable/disable HTTPS access
- license Set array software license key
- load Load running configuration from flash
- network-assurance Enable/disable network assurance
- pci-audit Enable/disable PCI (Payment Card Industry) audit mode.
See [“The pci-audit Command” on page 428.](#)
- restore Restore to previous saved config
- save Save running configuration to flash
- ssh Enable/disable SSH access
- standby Configure standby parameters
- telnet Enable/disable telnet access

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) |

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. |

restore

The **restore** command [**Xirrus_Wi-Fi_Array(config)# restore**] is used to restore configuration to a version that was previously saved locally.

| Command | Description |
|-------------------------|--|
| ? | Use this to display the list of available config files. FORMAT: restore ? |
| <filename> | Enter the name of the locally saved configuration to restore. FORMAT: restore <config-filename> |

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 | <p>Special ping utility to test the connection to a RADIUS server.</p> <p>FORMAT:</p> <p>run-tests radius-ping [external ssid <ssidnum>] [primary secondary] user <raduser> password <radpasswd> auth-type [CHAP PAP]</p> <p>run-tests radius-ping [internal server <radserver> port <radport> secret <radsecret>] user <raduser> password <radpasswd> auth-type [CHAP PAP]</p> <p>You may select a RADIUS server that you have already configured (ssid or external or internal) or specify another server.</p> |
| rlb | <p>Run manufacturing radio loopback test.</p> <p>FORMAT:</p> <p>run-tests rlb {optional command line switches}</p> |
| self-test | <p>Execute self-test.</p> <p>FORMAT:</p> <p>run-tests self-test {logfile-name (optional)}</p> |
| site-survey | <p>Enable or disable site survey mode.</p> <p>FORMAT:</p> <p>run-tests site-survey [on off enable disable]</p> |
| ssh | <p>Execute ssh utility.</p> <p>FORMAT:</p> <p>run-tests ssh [hostname ip-addr] [command-line-switches (optional)]</p> |
| tcpdump | <p>Execute tcpdump utility to dump traffic for selected interface or VLAN. Supports 802.11 headers.</p> <p>FORMAT:</p> <p>run-tests tcpdump</p> |

| 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 |

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 |

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] |

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 |

wifi-tag

The **wifi-tag** command [**Xirrus_Wi-Fi_Array(config-wifi-tag)#**] is used to enable or disable Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channels. See also “Wi-Fi Tag” on page 161.

| Command | Description |
|-----------------------|--|
| disable | Disable wifi-tag. FORMAT: wifi-tag disable |
| enable | Enable wifi-tag. FORMAT: wifi-tag enable |
| off | Disable wifi-tag. FORMAT: wifi-tag off |
| on | Enable wifi-tag. FORMAT: wifi-tag on |
| tag-channel-bg | Set an 802.11b or g channel for listening for tags. FORMAT: wifi-tag tag-channel-bg <1-255> |
| udp-port | Set the UDP port which a tagging server will use to query the Array for tagging information. FORMAT: wifi-tag udp-port <1025-65535> |

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 361.](#)
- [“Configuring a Global SSID using WPA-PEAP” on page 362.](#)
- [“Configuring an SSID-Specific SSID using WPA-PEAP” on page 363.](#)
- [“Enabling Global IAPs” on page 364.](#)
- [“Disabling Global IAPs” on page 365.](#)
- [“Enabling a Specific IAP” on page 366.](#)
- [“Disabling a Specific IAP” on page 367.](#)
- [“Setting Cell Size Auto-Configuration for All IAPs” on page 368](#)
- [“Setting the Cell Size for All IAPs” on page 369.](#)
- [“Setting the Cell Size for a Specific IAP” on page 370.](#)
- [“Configuring VLANs on an Open SSID” on page 371.](#)
- [“Configuring Radio Assurance Mode \(Loopback Tests\)” on page 372.](#)

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 164. 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
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 & 802.11g
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 165. 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
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 166. 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.

```
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)# all_up
Interface IAP a1 state changed to up
Interface IAP a3 state changed to up
Interface IAP a4 state changed to up
Interface IAP a5 state changed to up
Interface IAP a6 state changed to up
Interface IAP a7 state changed to up
Interface IAP a8 state changed to up
Interface IAP a9 state changed to up
Interface IAP a10 state changed to up
Interface IAP a11 state changed to up
Interface IAP a12 state changed to up
Interface IAP abg2 state changed to up
Interface IAP abg3 state changed to up
Interface IAP abg4 state changed to up

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
```

| IAP | State | Channel | Antenna | Cell | TX | RX | 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 | max | 20dBm | -90dBm | 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 | up | monitor | int-omni | manual | 20dBm | -95dBm | 0 | | 00:0f:7d:03:5e:60-61 | | | | |

Figure 167. Enabling Global IAPs

Disabling Global IAPs

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

```
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)# all_down
  Interface IAP a1 state changed to down
  Interface IAP a2 state changed to down
  Interface IAP a3 state changed to down
  Interface IAP a4 state changed to down
  Interface IAP a5 state changed to down
  Interface IAP a6 state changed to down
  Interface IAP a7 state changed to down
  Interface IAP a8 state changed to down
  Interface IAP a9 state changed to down
  Interface IAP a10 state changed to down
  Interface IAP a11 state changed to down
  Interface IAP a12 state changed to down
  Interface IAP abg1 state changed to down
  Interface IAP abg2 state changed to down
  Interface IAP abg3 state changed to down
  Interface IAP abg4 state changed to down

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 down   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
```

Figure 168. 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 169. 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).

```
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)# a2 down
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 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 up   monitor int-omni manual 20dBm -95dBm    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 170. 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 28.) 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 the **monitor** radio, 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
-----
IAP State Channel Antenna Cell Size TX Power RX 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 171. 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 the monitor radio the cell size cannot be set globally—you must first disable the intrude-detect feature on the monitor radio.

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 28.

```
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

| IAP | State | Channel | Antenna | Cell Size | TX Power | RX 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 172. 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 28.

```
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

| IAP | State | Channel | Antenna | Cell Size | TX Power | RX 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:90-31 | |
| 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 173. 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 & 802.11g
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 174. Configuring VLANs on an Open SSID

Configuring Radio Assurance Mode (Loopback Tests)

The Array uses its built-in monitor radio 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 412.

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—the monitor radio 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 reboot:
<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 175. 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 379.
- “Reinstalling the Access Panel” on page 382.
- “Replacing the FLASH Memory Module” on page 384.
- “Replacing the Main System Memory” on page 386.
- “Replacing the Integrated Access Point Radio Module” on page 388.
- “Replacing the Power Supply Module” on page 391.

! *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.*

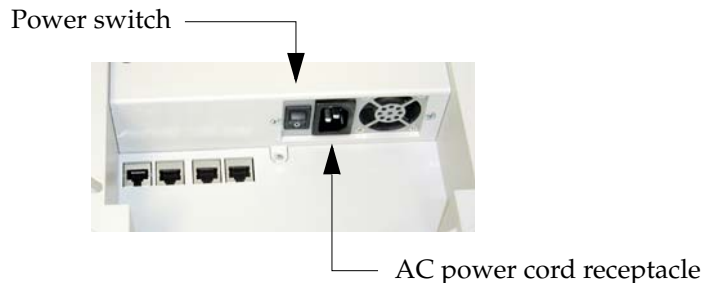


Figure 176. Disconnecting Power from the Array



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. Disconnect the AC power cord or Ethernet cable supplying power from the Array.
2. Place the Array face-down on a flat surface. Avoid moving the unit to reduce the risk of damage (scratching) to the finished enclosure.
3. Remove the screws (3 places) that secure the access panel to the main body of the Array.

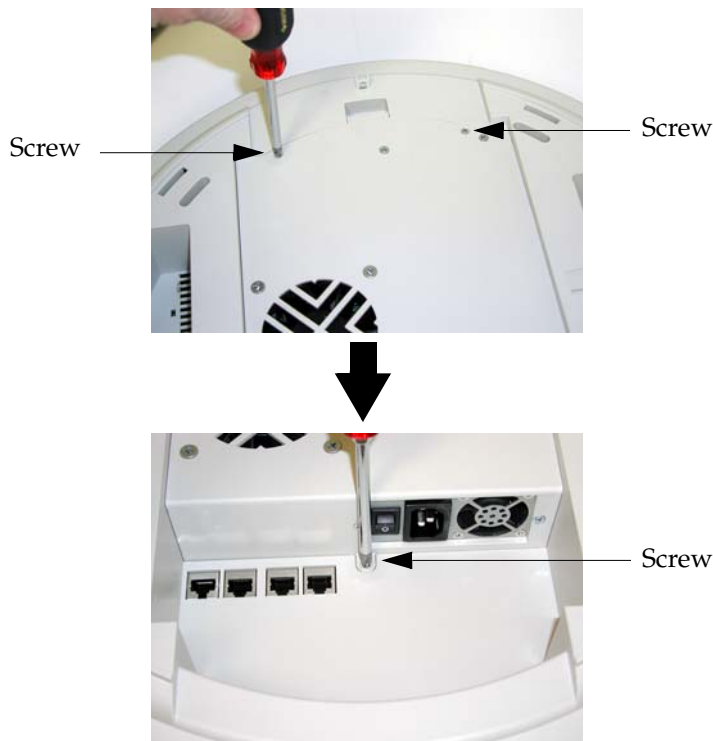


Figure 177. Removing the Access Panel Screws

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



Lift up the access panel

Figure 178. Removing the Access Panel

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



Fan connector

Power supply connector

Figure 179. Disconnecting the Power Supply and Fan

6. The access panel can now be safely removed.

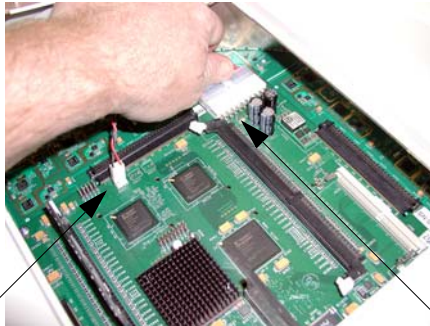
See Also

- 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 180. Reconnecting the Fan and Power Supply

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



Figure 181. 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 379.
2. Remove the FLASH memory module, taking care not to "wiggle" the module and risk damaging the connection points.

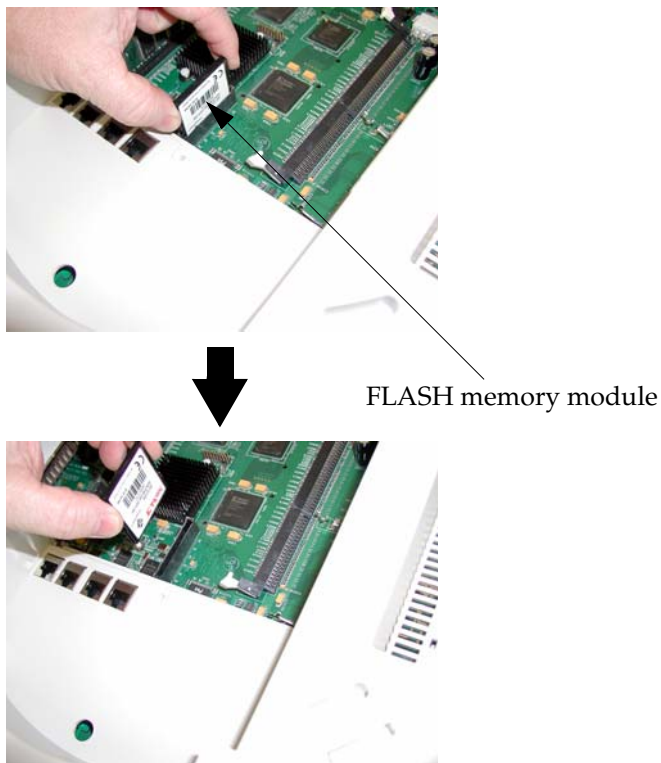


Figure 182. Removing the FLASH Memory Module

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 382).

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 379).
2. Remove the DIMM memory module, taking care not to “wiggle” the module and risk damaging the connection points.

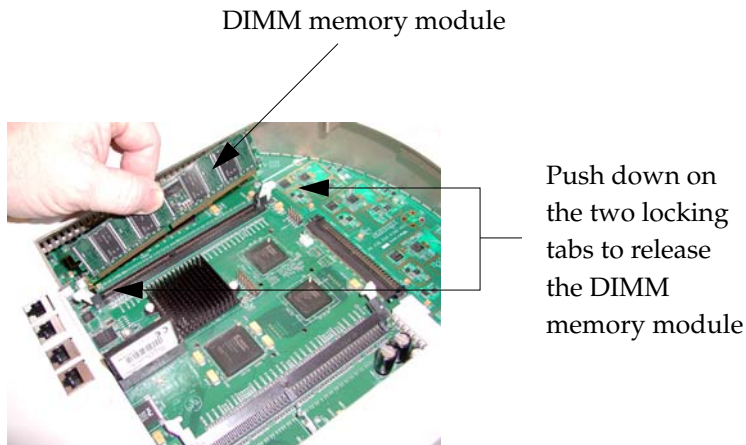


Figure 183. Removing the DIMM Memory Module

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 382).

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.

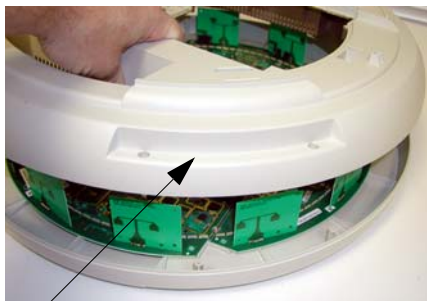
1. Remove the access panel (refer to “Removing the Access Panel” on page 379).
2. Remove the locking screws (8 places) that secure the chassis cover to the main body of the Wi-Fi Array.



Screws (8 places)

Figure 184. Removing the Chassis Cover Screws

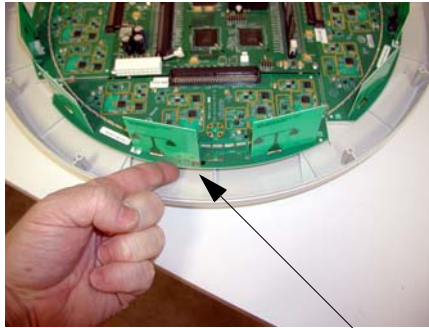
3. Lift and remove the chassis cover.



Remove the chassis cover

Figure 185. Removing the Chassis Cover

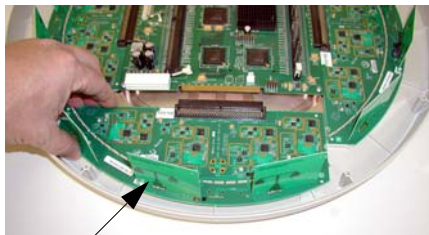
4. Lift the edge of the integrated access point module.



Lift here (do not force)

Figure 186. 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 187. 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 382).

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 379).
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 382.



Access panel (with power supply and fan)

Figure 188. 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 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 393.
- “Keyboard Shortcuts” on page 399.

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 |

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) |
| 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 |
| 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 |

| Setting | Default Value |
|-------------|---------------|
| Group Rekey | Disabled |

External RADIUS (Global)

| Setting | Default Value |
|---|----------------------|
| Enabled | Yes |
| Primary Server | None |
| Primary Port | 1812 |
| 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 |
| 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 403](#)
- [“Frequently Asked Questions” on page 404](#)
- [“Array Monitor and Radio Assurance Capabilities” on page 412](#)
- [“RADIUS Vendor Specific Attributes \(VSAs\) for Xirrus” on page 415](#)
- [“Upgrading the Array via CLI” on page 418](#)
- [“Contact Information” on page 423](#)

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 monitor radio is oriented in the direction of the least required coverage, because when in monitor mode the 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 208.
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 **Save changes to flash** if you wish to make your changes permanent.
8. 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).



TKIP encryption does not support high throughput rates, per the IEEE 802.11n.

TKIP should never be used for WDS links on XN arrays.

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.

- MAC Address ACLs (Access Control Lists)
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 integrated monitor capabilities, which can constantly scan 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 unable 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 integrated monitoring capabilities to check that the Array's radios are functioning correctly, and act as a threat sensor to detect and prevent intrusion from rogue access points.

Enabling Monitoring on the Array

Any radio 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 one monitor radio 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 237](#) for more details. The values above are the factory default settings for the Array.

How Monitoring Works

When the monitor radio 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 262](#).

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 2 in “[Advanced RF Settings](#)” on page 262). When this mode is enabled, the monitor radio 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 262).

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 414), 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 414), 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 2](#) page 263):

- **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.

RADIUS Vendor Specific Attributes (VSAs) for Xirrus

A number of RADIUS VSAs are defined for Xirrus Arrays. These control administrator privileges and a number of settings for user accounts, such as QoS, roaming, VLAN, etc.

The RADIUS VSAs are used by Arrays to define selected attributes for the following account types:

- **Array administrators**—the **Xirrus-Admin-Role** attribute sets the privilege level for this account. Set the value to the string defined in **Privilege Level Name** as described in “[About Creating Admin Accounts on the RADIUS Server](#)” on page 185.
- **Array users**—all of the VSAs whose names start with **Xirrus-User** set attributes of WiFi client accounts. As you can see in the **dictionary.xirrus** file listed below, attribute types may be integer or string. For integer -type attributes, the possible integer values that you may set are listed and described in **dictionary.xirrus**. For string-type attributes, set the value to an entry name that you have configured on the Array. For example, set **Xirrus-User-VLAN** to a VLAN Name that you created in “[VLAN Management](#)” on page 173. Most of the **Xirrus-User** attributes are described in “[Group Management](#)” on page 230.

The following Xirrus RADIUS VSA dictionary is provided here as a sample for your convenience. These definitions may be updated from time to time. **Always check the Xirrus Customer Support website for the latest version: support.xirrus.com.**

| | | | |
|--------------|-------------------------|-------|---------|
| VENDOR | Xirrus | 21013 | |
| BEGIN-VENDOR | Xirrus | | |
| ATTRIBUTE | Xirrus-Admin-Role | 1 | string |
| ATTRIBUTE | Xirrus-User-VLAN | 2 | string |
| ATTRIBUTE | Xirrus-User-Qos-WiFi | 3 | integer |
| ATTRIBUTE | Xirrus-User-Qos-L2 | 4 | integer |
| ATTRIBUTE | Xirrus-User-Qos-L3-TOS | 5 | integer |
| ATTRIBUTE | Xirrus-User-Qos-L3-DSCP | 6 | integer |

| | | | |
|-----------|---------------------------|----------------------|---------|
| ATTRIBUTE | Xirrus-User-Roaming-Layer | 7 | integer |
| ATTRIBUTE | Xirrus-User-Traffic-Limit | 8 | integer |
| ATTRIBUTE | Xirrus-User-DHCP-Pool | 9 | string |
| ATTRIBUTE | Xirrus-User-Filter-List | 10 | string |
| ATTRIBUTE | Xirrus-User-Group | 11 | string |
| ATTRIBUTE | Xirrus-User-Interface | 12 | string |
| ATTRIBUTE | Xirrus-User-Location | 13 | string |
| VALUE | Xirrus-User-Qos-Wifi | Best-Effort | 0 |
| VALUE | Xirrus-User-Qos-Wifi | Background | 1 |
| VALUE | Xirrus-User-Qos-Wifi | Video | 2 |
| VALUE | Xirrus-User-Qos-Wifi | Voice | 3 |
| VALUE | Xirrus-User-Qos-L2 | Best-Effort | 0 |
| VALUE | Xirrus-User-Qos-L2 | Background | 1 |
| VALUE | Xirrus-User-Qos-L2 | Standard | 2 |
| VALUE | Xirrus-User-Qos-L2 | Excellent-Effort | 3 |
| VALUE | Xirrus-User-Qos-L2 | Controlled | 4 |
| VALUE | Xirrus-User-Qos-L2 | Video | 5 |
| VALUE | Xirrus-User-Qos-L2 | Voice | 6 |
| VALUE | Xirrus-User-Qos-L2 | Network-Control | 7 |
| VALUE | Xirrus-User-Qos-L3-TOS | Routine | 0 |
| VALUE | Xirrus-User-Qos-L3-TOS | Priority | 1 |
| VALUE | Xirrus-User-Qos-L3-TOS | Immediate | 2 |
| VALUE | Xirrus-User-Qos-L3-TOS | Flash | 3 |
| VALUE | Xirrus-User-Qos-L3-TOS | Flash-Override | 4 |
| VALUE | Xirrus-User-Qos-L3-TOS | Critical-ECP | 5 |
| VALUE | Xirrus-User-Qos-L3-TOS | Internetwork-Control | 6 |
| VALUE | Xirrus-User-Qos-L3-TOS | Network-Control | 7 |
| VALUE | Xirrus-User-Qos-L3-TOS | Low-Delay. | 8 |
| VALUE | Xirrus-User-Qos-L3-TOS | High-Throughput | 16 |
| VALUE | Xirrus-User-Qos-L3-TOS | High-Reliability | 32 |
| VALUE | Xirrus-User-Roaming-Layer | L2-only | 0 |
| VALUE | Xirrus-User-Roaming-Layer | L2-and-L3 | 1 |

Wi-Fi Array



| | | | |
|------------|---------------------------|------|---|
| VALUE | Xirrus-User-Roaming-Layer | None | 3 |
| END-VENDOR | Xirrus | | |

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 only** 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-5.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 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:

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 |
|---|
| <p>Objective: Build and Maintain a Secure Network</p> <ul style="list-style-type: none"> ● 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. |
| <p>Objective: Protect Cardholder Data</p> <ul style="list-style-type: none"> ● 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... |
|--|---|---|
| <ul style="list-style-type: none"> () () | <p>Register at the Xirrus Support Site to ensure notification and access to software updates.</p> <p>Confirm that the latest version of the Array OS is being used by checking the Xirrus web site.</p> | <p>support.xirrus.com</p> |
| <ul style="list-style-type: none"> () | <p>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.</p> | <p>The pci-audit Command, p. 428</p> |
| <ul style="list-style-type: none"> () | <p>Allow only necessary protocols and networks to be accessed by configuring your corporate firewall or using the internal Array firewall.</p> | <p>Filters, p. 283</p> |
| <ul style="list-style-type: none"> () () () () () () | <p>Change the default Admin account password.</p> <p>Remove any unnecessary admin or user accounts.</p> <p>Change the SNMP community string from the default password.</p> <p>Use WPA2 and 802.1x authentication.</p> <p>Change default SSID from Xirrus to a user-defined SSID.</p> <p>Disable SSID broadcast for all PCI compliant SSIDs.</p> | <p>Express Setup, p. 139</p> <p>Admin Management, p. 181</p> <p>SNMP, p. 165</p> <p>SSIDs, p. 208 and Global Settings, p. 197</p> <p>SSIDs, p. 208</p> <p>SSIDs, p. 208</p> |
| <ul style="list-style-type: none"> () () () | <p>Enable Secure Shell (ssh) for CLI (command line) access.</p> <p>Confirm telnet access is disabled (done by default).</p> <p>Confirm management over the wireless network is disabled.</p> | <p>Management Control, p. 188</p> <p>Global Settings (IAP), p. 243</p> |

| ✓ | 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. | SSIDs , p. 208 and Global Settings , p. 197 |
| () | Ensure that Array Administration Accounts are being validated by External RADIUS servers. | Admin RADIUS , p. 185 |
| () | Ensure that each Xirrus Array is physically inaccessible such that console ports and management ports are not accessible. | Dismounting the Array , p. 61 See Indoor Enclosure |
| () | Enable Syslog messaging and define a Syslog server on the wired network to receive Syslog messages. | System Log , p. 162 |
| () | Enable NTP and define an NTP server (optional). | Time Settings (NTP) , p. 157 |
| () | 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. 237 Rogue Control List , p. 206 Intrusion Detection , p. 107 |

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` (part of the `management` command), 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*. This appendix lists simple steps that must be followed exactly to implement FIPS 140-2, Level 2. The procedures include physical actions, and parameters that must be set in the Web Management Interface (WMI) in the Security page and in other pages.

To satisfy FIPS 140-2, Level 2, perform the following procedures:

- “Securing the Array Physically” on page 431
- “To implement FIPS 140-2, Level 2 using WMI” on page 434
- - or - “To implement FIPS 140-2, Level 2 using CLI:” on page 436
- “To check if an Array is in FIPS mode:” on page 436

Securing the Array Physically

Operator Required Actions

1. The Cryptographic Officer is required to configure and periodically inspect the cryptographic module. Tamper evident seals and security straps shall be in control of the Cryptographic Officer at all times.
2. Apply supplied tamper-evident seals to the Array as indicated in the figures below. The procedure is slightly different, depending on the model.

IMPORTANT:

- **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 or seam so that it will show if an attempt has been made to open or tamper with the Array.**
- For 4-radio Arrays (XN4)—See [Step 3](#).
- For Arrays with 8 or more radios (XN8, XN12, XN16)—see [Step 4](#).



XN4, XN8, XN12, XN16 - seam location



XN8, XN12, XN16 Mounting plate openings

Figure 190. Tamper-evident seal appearance

3. For the XN4: Apply two seals, one on either side of the Array about 180° apart from each other, as shown in [Figure 191](#). **IMPORTANT: Make sure that each seal straddles a seam.**

Continue to [Step 5](#).

Tamper seal locations on seam:
Two (2) seals, placed straddling seam on opposite sides.
Locations indicated by arrows and colored blocks.



Figure 191. Tamper-evident seal locations for XN4 indicated by arrows

4. For the XN8, XN12, XN16: Apply a total of eight (8) seals, as follows.

- Apply two (2) seals, one on either side of the Array about 180° apart from each other, as shown in [Figure 192](#). **IMPORTANT: Make sure that each seal straddles a seam.**
- Apply tamper seals to the two (2) mounting plate openings, prior to mounting the Array body on the plate. Place three (3) seals across each opening as shown in [Figure 193](#).

Continue to [Step 5](#).

Tamper seal locations on seam:
Two (2) seals, placed straddling seam on opposite sides.

Locations indicated by arrows and colored blocks.



Figure 192. Two tamper-evident seals on seam of XN8/12/16

Tamper seal location covering two (2) mounting plate openings.
Six (6) seals placed - three (3) across each opening. Place labels on mounting plate prior to mounting Array body. Locations indicated by arrows and colored blocks.

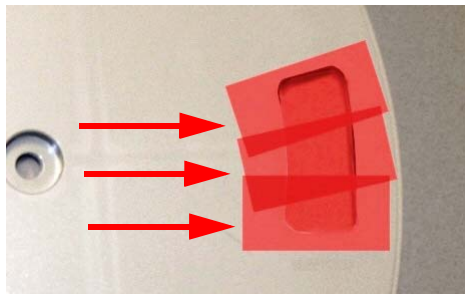


Figure 193. Six tamper-evident seals on mounting plate - XN8/12/16

5. Apply the supplied tamper-evident security strap to the unit as indicated in Figure 194. Each mounting plate and Array contains a single locking tab. The Array is mounted to the mounting plate and rotated until the mounting plate clicks into place and the locking tabs are aligned. Thread the security strap through the aligned locking tabs and then pull it through the strap lock until firmly affixed. The security strap should be pulled tight to prevent the mounting plate from turning. Tamper evidence may be indicated by a broken strap or cracked locking tab.

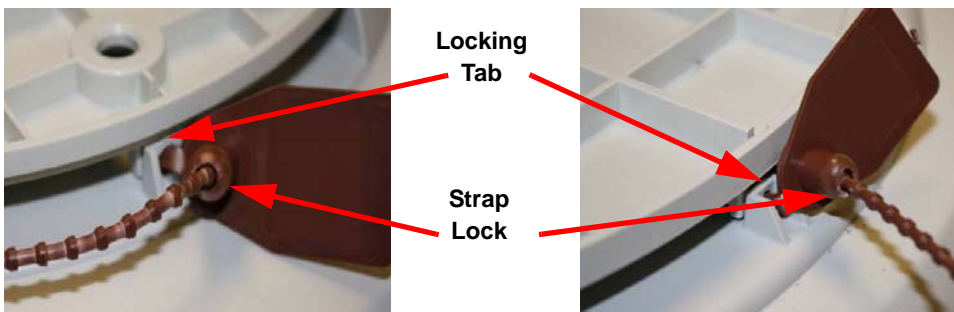


Figure 194. Apply the security strap through locking tab as shown

To implement FIPS 140-2, Level 2 using WMI

You must enable FIPS 140-2, Level 2 Security on the Array. To do this using the Web Management Interface (WMI - ArrayOS Rel. 5.0 and higher), follow the steps below. (To do this using the CLI, please see “To implement FIPS 140-2, Level 2 using CLI:” on page 436.)

1. 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.



The following steps must be performed in the order shown—you must enable FIPS 140-2 before you create SSIDs. Otherwise, FIPS mode will change the PSK keys of SSIDs, and you will not know what the keys are.

- Click **Security** in the menu on the left of the WMI window. Then click **Management Control**. In the **Management Modes** section, set **FIPS 140-2, Level 2 Security** to **On**. (Figure 195) The WMI will display a message showing the settings that it is changing to implement FIPS security. Click **Save**, then **OK**.

The screenshot shows the XIRRUS Management Control interface. On the left is a navigation menu with categories like Array, Network, Stations, Statistics, System Log, Configuration, Express Setup, Network, Services, VLANs, and Security. The Security section is expanded, showing sub-items: Admin Management, Admin Privileges, Admin RADIUS, and Management Control. The main panel displays 'Management Settings' for device XN0429091D207 (10.100.47.12) at location SS Desk, with an uptime of 12 days, 2 hours. Under 'Management Transports', SSH, Telnet, and Serial are set to 'On', while HTTPS is 'Off'. Under 'Management Modes', Network Assurance and PCI Audit Mode are 'On', and FIPS 140-2, Level 2 Security is set to 'On'. A 'Message from webpage' dialog box is overlaid on the screen, displaying a warning icon and the following text: 'Global WPA TKIP support changed to off', 'Global WPA passphrase changed', 'Cannot enable both EAP and PSK', 'Global WPA EAP support changed to off', 'Global WPA PSK support changed to on', 'SNMPv2 state changed to off', 'Interface IAP global fast roaming mode changed to off', 'SSID xirrus none TKIP support changed to off', 'SSID xirrus none passphrase changed', 'Cannot enable both EAP and PSK', 'SSID xirrus none EAP support changed to off', 'SSID xirrus none PSK support changed to on', 'SSID xirrus authentication changed to 802-1x', and 'SSID xirrus encryption changed to wpa2'. An 'OK' button is at the bottom of the dialog.

Figure 195. Security - Management Control Window

3. You may now proceed to define SSIDs, as described in “SSIDs” on page 208.

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 (ArrayOS 4.1 and higher versions).

```
Xirrus_Wi-Fi_Array(config)# management
Xirrus_Wi-Fi_Array(config-mgmt)# 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 wish to stop enforcing FIPS security requirements on the Array.

```
Xirrus_Wi-Fi_Array(config-mgmt)# fips off
```

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

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 procedures are in effect.

See Also

[The Web Management Interface](#)

[The Command Line Interface](#)

Appendix F: Notices

This appendix contains the following information:

- “Notices” on page 437
- “EU Directive 1999/5/EC Compliance Information” on page 440
- “Compliance Information (Non-EU)” on page 447
- “Safety Warnings” on page 448
- “Translated Safety Warnings” on page 449
- “Software License and Product Warranty Agreement” on page 450
- “Hardware Warranty Agreement” on page 456

Notices

Wi-Fi Alliance Certification



www.wi-fi.org

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, XS8 and XS4. 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 zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními 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 Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
- Eesti [Estonian]** See seande vastab direktiivi 1999/5/EU olulistele nõuetele ja teistele asjakohastele sätetele.
- English** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
- Español [Spain]** Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
- Ελληνική [Greek]** Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
- Français [French]** Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.

- 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 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
- Nederlands [Dutch]** Dit apparant voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
- Malti [Maltese]** Dan l-apparant huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
- Magyar [Hungarian]** Ez a készülék teljesíti az alapvető 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 szczególnymi mi warunkami określony mi Dyrektywą. UE:1999/5/EC.
- Português [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 požiadavkami a inými príslušnými nariadeniami direktív: 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, XS8 and XS4), the CE mark and Class-2 identifier opposite are affixed to the equipment and its packaging:



WEEE Compliance



- 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 liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres 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 ωνεξωτερικο ρουστη ζ νησυ νοτ των 5470–5725 MHz ε ιτρ ετάιωνο ετάά όάδειά της EETT, ου ορηγεβτάι στερά ά ό σ φωνη γν η του ΓΕΕΘΑ. επισσότερες λε τομ ρειεωστο 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.comunicazioni.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.comunicazioni.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

Compliance Information (Non-EU)

This section contains compliance information for the Xirrus Wi-Fi Array family of products, which includes the XN16, XN12, XN8, and XN4. The compliance information contained in this section is relevant to the listed countries (outside of the European Union and other countries that have implemented the EU Directive 1999/5/EC).

Declaration of Conformity

Mexico XN16: Cofetel Cert #: RCPXIXN10-1052
XN12: Cofetel Cert #: RCPXIXN10-1052-A1
XN8: Cofetel Cert #: RCPXIXN10-1052-A2
XN4: Cofetel Cert #: RCPXIXN10-1052-A3

Thailand This telecommunication equipment conforms to NTC technical requirement.

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/XS8/XS4 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/XS8/XS4 or connect or disconnect cables during periods of lightning activity.

- ! **Circuit Breaker Warning**
 - The XN16/XN12/XN8/XN4/XS16/XS8/XS4 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/XS8/XS4 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/XS8/XS4 et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.

- ! **Disjoncteur**

L'unité XN16/XN12/XN8/XN4/XS16/XS8/XS4 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 License and Product Warranty 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 EMPLOYEE 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 THEREFORE.

CUSTOMER UNDERSTANDS AND AGREES THAT USE OF THE PRODUCT AND 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.

1.0 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.

2.0 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; (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; (vi) disclose information about the performance or operation of the Product or Software to any third party without the prior written consent of Licensor; or (vii) engage a third party to perform benchmark or functionality testing of the Product or Software.

3.0 LIMITED WARRANTY AND LIMITATION OF LIABILITY

- 3.1 Limited Warranty & Exclusions. Licensor warrants that the Software will perform in substantial accordance with the specifications therefore 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 or Product does not perform as warranted, Licensor shall, at its option, correct the relevant Product and/or Software giving rise to such breach of performance or replace such Product and/or 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 FORSEEABLE 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.

4.0 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.

5.0 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.

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.

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

Numerics

11n
 see IEEE 802.11n 34
 4.9 GHz Public Safety Band 267
 802.11a 6, 7, 237, 250
 802.11a/b/g 22
 802.11a/b/g/n 12
 802.11a/n 12, 62, 213
 802.11b 6, 7, 254
 802.11b/g 237, 254
 802.11b/g/n 12, 62, 213
 802.11e 14
 802.11g 6, 7, 254
 802.11i 7, 68, 139
 802.11n 7
 see IEEE 802.11n 34
 WMI page 259
 802.11p 14
 802.11q 14
 802.1x 7, 45, 55, 68, 139, 406

A

abg(n)
 nomenclature 3

abg(n)2
 intrusion detection 273
 self-monitoring
 radio assurance (loopback mode) 263

AC power 44, 58, 379, 382

Access Control List 175

Access Control Lists 406

access control lists (ACLs) 195, 226

Access Panel 379, 382, 391

access panel
 reinstalling 382

removing 379

ACLs 45, 175, 406

active IAPs
 per SSID 225

Address Resolution Protocol
 window 98

Address Resolution Protocol (ARP)
 248

Admin 406

Admin ID 181

admin ID
 authentication via RADIUS 185

Admin Management 181

admin privileges
 setting in admin RADIUS account 185

admin RADIUS account
 if using Console port 185

admin RADIUS authentication 185

administration 68, 139, 175

Administrator Account 399

Advanced Encryption Standard 45, 406

Advanced RF Analysis Manager
 see RAM 16

Advanced RF Performance Manager
 see RPM 14

Advanced RF Security Manager
 see RSM 15

AeroScout
 see WiFi tag 161

AES 7, 13, 45, 55, 68, 139, 397, 406

allow traffic
 see filters 283

Analysis Manager
 see RAM 16

appearance
 WMI options 309
 WMI, changing 309

approved

- setting rogues 108
 - APs 55, 107, 206, 406
 - rogues, blocking 273
 - APs, rogue
 - see rogue APs 262, 273
 - ARP filtering 248
 - ARP table window 98
 - Array 24, 61, 62, 76, 139, 147
 - connecting 61
 - dismounting 61
 - management 295
 - mounting 61
 - powering up 62
 - securing 61
 - Web Management Interface 76
 - ArrayOS
 - upgrade 298
 - Arrays
 - managing in clusters 289
 - associated users 24
 - assurance
 - network server connectivity 101, 191
 - assurance (radio loopback testing) 262
 - assurance, station
 - see station assurance 267
 - attack (DoS)
 - see DoS attack 274
 - attack (impersonation)
 - see impersonation attack 275
 - authentication 13
 - of admin via RADIUS 185
 - authority
 - certificate 179, 192
 - auto block
 - rogue APs, settings 273
 - auto negotiate 147
 - auto-blocking
 - rogue APs 273
 - auto-configuration 68, 243, 250, 254
 - channel and cell size 262
 - automatic refresh
 - setting interval 311
 - automatic update from remote server
 - configuration files, boot image 299
- B**
- backhaul
 - see WDS 52
 - backup unit
 - see standby mode 262
 - band association 213
 - beacon interval 243
 - Beacon World Mode 243
 - beam distribution 12
 - benefits 12
 - block
 - rogue APs, settings 270
 - block (rogue APs)
 - see auto block 273
 - blocking
 - rogue APs 273
 - blocking rogue APs 262
 - boot 298
 - broadcast 248
 - fast roaming 249
 - browser
 - certificate error 179, 192
 - BSS 404
 - BSSID 107, 404
 - buttons 81
- C**
- capacity
 - of 802.11n 41
 - cascading style sheet
 - sample for web page redirect 305
 - cdp 328
 - CDP (Cisco Discovery Protocol)
 - settings 154

- cdp CLI command 328
- CDP neighbors 100
- cell
 - sharp cell 262
- cell size 24, 237
 - auto-configuration 262
- cell size configuration 262
- certificate
 - about 179, 192
 - authority 179, 192
 - error 179, 192
 - install Xirrus authority 192
 - X.509 179, 192
- channel
 - auto-configuration 262
 - configuration 262
 - list selection 262
 - public safety 262
- channels 24, 107, 237, 243, 250, 254
 - non-overlapping 13
- CHAP (Challenge-Handshake Authentication Protocol)
 - Admin RADIUS settings 186
 - web page redirect 222
- CHAP Challenge Handshake Authentication Protocol)
 - RADIUS ping 306
- character restrictions 84
- Chassis Cover 388
- chassis cover 388
- Cisco Discovery Protocol
 - see cdp 328
- Cisco Discovery Protocol (CDP) 154
- CLI 7, 55, 58, 65, 313
 - executing from WMI 308
 - using to upgrade software image 418
- CLI commands
 - see commands 328
- client
 - web page redirect 304
- cluster
 - CLI command 330
- clusters 289
 - defining 290
 - management 291
 - operating in cluster mode 292
- command
 - wifi-tag 359
- Command Line Interface 7, 51, 58, 62, 65, 313, 406
 - configuration commands 326
 - getting help 315
 - getting started 315
 - inputting commands 315
 - sample configuration tasks 360
 - SSH 313
 - top level commands 317
- command, utilities
 - ping, traceroute, RADIUS ping 305
- commands
 - acl 326
 - admin 327
 - cdp 328
 - clear 329
 - cluster 330
 - configure 318
 - contact-info 331
 - date-time 332
 - dhcp-server 333
 - dns 334
 - file 335
 - filter 338
 - group 330, 340
 - hostname 340
 - interface 341
 - load 342
 - location 342
 - management 343
 - more 344

- netflow 345
 - no 346
 - quit 348
 - radius-server 348
 - reboot 349, 357
 - reset 349
 - restore 350
 - run-tests 351
 - security 353
 - show 321
 - snmp 354
 - ssid 355
 - statistics 324
 - syslog 356
 - vlan 358
 - Community String 396
 - configuration 137, 406
 - express setup 139
 - reset to factory defaults 302
 - configuration changes
 - applying 83
 - configuration files
 - automatic update from remote server 299
 - download 300
 - update from local file 300
 - update from remote file 300
 - connection
 - tracking window 99
 - connectivity
 - servers, see network assurance 101, 191
 - Console port
 - login via 185
 - Contact Information 423
 - contact information 423
 - coverage 24, 58
 - extended 12
 - coverage patterns 7
 - critical messages 79
 - CTS/RTS 250, 254
- D**
- data rate 250, 254
 - data rates
 - increased by 802.11n 40
 - date/time restrictions
 - and interactions 232
 - DC power 44, 58
 - default gateway 68, 147
 - default settings 393
 - Default Value 397
 - DHCP 396
 - defaults
 - reset configuration to factory defaults 302
 - Delivery Traffic Indication Message 243
 - denial of service
 - see DoS attack 274
 - deny traffic
 - see filters 283
 - deployment 22, 32, 51, 55, 58, 406
 - ease of 13
 - examples 32
 - scenarios 32
 - detection
 - intrusion 273
 - see DoS attack 274
 - see impersonation attack 275
 - see impersonation detection 274
 - see intrusion detection 274, 275
 - DHCP 24, 65, 68, 139, 147, 395
 - default settings 396
 - leases window 99
 - DHCP Server 156
 - diagnostics
 - log, create file 302
 - DIMM 386
 - DIMM Memory Module 386

- DIMM module
 - replacing 386
 - display
 - WMI options 309
 - DNS 68, 139, 153
 - DNS domain 153
 - DNS server 153
 - Domain Name System 153
 - DoS attack detection
 - settings 274
 - DTIM 243
 - DTIM period 243
 - duplex 147
 - dynamic VLAN
 - overridden by group 231
- E**
- EAP 397, 406
 - EAP-MDS 13
 - EAP-PEAP 406
 - EAP-TLS 13, 45, 406
 - EAP-TTLS 13, 45, 406
 - EDCF 243
 - Encryption 397, 406
 - encryption 13
 - encryption method
 - recommended (WPA2 with AES) 177
 - setting 178
 - support of multiple methods 177
 - encryption method (encryption mode)
 - Open, WEP, WPA, WPA2, WPA-Both 177
 - encryption standard
 - AES, TKIP, both 177
 - setting 178
 - Enterprise 1, 6, 406
 - WLAN 6
 - Enterprise Class Management 7
 - Enterprise Class Security 7
 - ESS 404
 - ESSID 404
 - Ethernet 58, 61, 62, 65, 68, 139
 - event log
 - IDS (intrusion detection) 135
 - see system log 134
 - event messages 79
 - Express Setup 61, 68, 139
 - express setup 68, 139
 - Extended Service Set 404
 - Extensible Authentication Protocol 406
 - external RADIUS server 802.1x 21
- F**
- factory default settings 393
 - factory defaults 395, 396, 397, 399
 - DHCP 396
 - reset configuration to 300
 - factory.conf 300
 - fail-over
 - standby mode 262
 - failover 42, 55
 - Fan 379, 382
 - FAQs 404
 - Fast Ethernet 58, 65, 139, 147, 393
 - fast roaming 13, 95, 249
 - about 235
 - and VLANs 236
 - features 12, 51, 147, 159, 162, 243, 406
 - and license key 299
 - Federal Information Processing Standard (FIPS)
 - see FIPS 431
 - feedback 81
 - filter list 284
 - filter name 286
 - filters 283, 284, 286
 - stateful filtering, disabling 284
 - statistics 132
 - FIPS 140-2 Security 431

firewall 283
 and port usage 48
 stateful filtering, disabling 284
FLASH 384
FLASH memory
 replacing 384
FLASH Memory Module 384
fragmentation threshold 250, 254
frequently asked questions 404
FTP 406
FTP server 21

G

General Hints 403
getting started
 express setup 139
Gigabit 58, 65, 68, 139, 147, 393
global settings 243, 250, 254
glossary of terms 459
Group
 management 230
group 228
 CLI command 330, 340
 VLAN overrides dynamic VLAN 231
group limits and interactions 232
Group Rekey 397
guard interval
 short, for IEEE 802.11n 39
GUI
 see WMI 309

H

help
 button, bottom of page 82
 button, left frame 79
Help button 76
help button 81
host name 68, 76, 139, 153
hs.css 305

HTTPS
 certificate, see certificate 192
HTTPS port
 web page redirect 219, 223, 224
HyperTerminal 20, 58

I

IAP 24, 62, 68, 139, 237, 250, 254, 276
 active SSIDs 225
 fast roaming 235
 Intrusion Detection (IDS/IPS) 270
 naming 3
 settings 237
IAP LED 62, 276
IAP LED settings 276
IAPs
 auto block rogues 273
 intrusion detection 273
IDS
 see Intrusion Detection 270
IDS event log
 viewing window 135
IEEE 6, 68, 139
IEEE 802.11n
 capacity, increased 41
 deployment considerations 34
 guard interval, short 39
 improved MAC throughput 39
 increased data rates 40
 MIMO 35
 multiple data streams 37
 spatial multiplexing 37
 WMI page 259
IEEE 802.1Q 410
image
 upgrade software image 298
impersonation attack detection
 settings 275
implementing Voice over Wi-Fi 22,
 171, 210

- installation 19, 56, 61, 375
 - installing the MCAP-3616 58
 - mounting the unit 61
 - requirements 19
 - workflow 56
- installation workflow 56
- Integrated Access Point Module 388
- integrated radio module
 - replacing 388
- interfaces 139
 - Web 75
- internal login page
 - web page redirect 220
 - web page redirect, customize 222
- internal splash page
 - web page redirect 221
 - web page redirect, customize 222
- Internet Explorer 20
- interval
 - automatic WMI refresh 311
- intrusion detection 107, 273
 - and auto block settings 273
 - configuration 262
 - setting as approved or known 108
- intrusion detection (IDS)
 - viewing event log 135
- Intrusion Detection (IDS/IPS) 270
- IP Address 24, 68, 76, 83, 107, 139, 147, 153, 162, 165, 295, 395
- IP Subnet Mask 68
- IPS
 - see Intrusion Detection 270

K

- key
 - upgrade 299
- key features 12
- Keyboard Shortcuts 399
- keyboard shortcuts 399
- known

- setting rogues 108

L

- lastboot.conf 300
- Layer 3
 - fast roaming 235
- lease 395
- Lease Time 395
- leases, DHCP
 - viewing 99
- LEDs 62
 - sequence 62
 - settings 276
- license Key
 - upgrading 299
- limits
 - group 232
 - interactions 232
 - station 232
 - traffic 232
- list, access control
 - see access control list 195, 226
- list, MAC access
 - see access control list 195
- list, SSID access
 - see access control list 226
- location information 68, 76, 139
- log
 - diagnostics, create file 302
- log messages
 - counters 80
- log, IDS(intrusion detection)
 - viewing window 135
- log, system (event)
 - viewing window 134
- logging in 65, 83
- Login 83
- login
 - via Console port 185
- login page

- web page redirect 220, 304
- web page redirect, customize 222

logout 312

long retry limit 243

loopback

- see radio assurance 372

loopback testing

- radio assurance mode 262

M

MAC 45, 65, 404, 406

MAC Access Control Lists 45

MAC Access List 195

MAC address 195, 404, 406

MAC throughput

- improved by IEEE 802.11n 39

Main System Memory 386

Management 399, 406

management 85, 137, 295

- Array clusters 289
- of Arrays 295
- Web Management Interface (WMI) 75

maximum lease 395

Maximum Lease Time 395

Megabit 68

menu behavior

- WMI 311

Message Integrity Check 406

messages

- syslog counters 80

MIC 13, 406

MIMO (Multiple-In Multiple-Out) 35

mode

- cluster operating mode 292

monitoring

- intrusion detection 107
- see intrusion detection 273

mounting 61

mounting plate 61

mounting the unit 61

MTU 147

- size 147

multiple data streams 37

N

NAT

- table - see connection tracking 99

neighbors, CDP 100

Netflow 159

netflow

- CLI command 345

Netscape Navigator 19, 20

network

- interfaces 146
- settings 147

network assurance 101, 191

network connections 58, 83, 406

network installation 19, 375

network interface ports 65

network interfaces 147, 393

network status

- ARP table window 98
- connection

 - tracking window 99

- routing table window 98
- viewing leases 99

Network Time Protocol 68, 139, 157

network tools

- ping, traceroute, RADIUS ping 305

nomenclature 3

non-overlapping channels 13

NTP 68, 139, 157, 395

NTP Server 157

O

Open (encryption method) 177

optimization, VLAN 248

options

- WMI 309

overview 7

P

page loading

WMI 311

PAP (Password Authentication Protocol)

Admin RADIUS settings 186

RADIUS ping 306

web page redirect 222

passphrase 45, 68, 139

Password 399, 406

password 83

Payment Card Industry Data Security Standard

see PCI DSS 425

PCI DSS 425

PEAP 13, 280

performance 12

Performance Manager

see RPM 14

Ping 295

ping 305

planning 42, 44, 45, 51

failover 42

network management 51

port failover 42

power 44

security 45

switch failover 42

WDS 52

PoGE 19

see Power over Gigabit Ethernet 10

PoGE Power Injectors 1

port failover 42

port requirements 48

power cord 379

power outlet 19

Power over Gigabit Ethernet 3, 19, 44, 59

Power over Gigabit Ethernet (PoGE) 10

power planning 44

Power Supply 379, 382, 391

power supply

replacing 391

pre-shared key 45, 55, 406

Print button 76

print button 81

probe

see Netflow 159

product installation 19, 375

product overview 7

PSK 55, 397

public safety band 267

public safety channels 262

PuTTY 19, 51, 68, 139, 406

PuTTY 20

Q

QoS 14, 213, 397, 404, 466

conflicting values 212

levels defined 214, 231

priority 213

SSID 209, 214

about setting QoS 405

default QoS 397

user group 231

quality

of user experience 267

Quality of Service 14

see QoS 214, 231

quick reference guide 393

quick start

express setup 139

R

radio

assurance (self-test) 263

radio assurance (loopback testing) 262

radio assurance (loopback) mode 263

- radio distribution 12
 - radios
 - naming 3
 - RADIUS 7, 19, 45, 55, 175, 195, 226, 395, 406
 - admin authentication 185
 - setting admin privileges 185
 - setting user VSAs 201
 - Vendor Specific Attributes (VSAs) 415
 - RADIUS ping
 - CHAP Challenge Handshake Authentication Protocol) 306
 - PAP (Password Authentication Protocol) 306
 - RADIUS Ping command 306
 - RADIUS Server 395
 - RADIUS server 21
 - RADIUS settings
 - web page redirect 222
 - RAM (RF Analysis Manager) 16
 - reauthentication 243
 - reboot 298
 - redirect (WPR) 304
 - refresh interval
 - WMI 311
 - remote boot image
 - automatic update from remote TFTP server 299
 - remote configuration
 - automatic update from remote server 299
 - remote TFTP server
 - automatic update of boot image, configuration 299
 - Reset 295, 395
 - reset configuration
 - to factory defaults 302
 - restore command 350
 - restrictions
 - date/time 232
 - stations 232
 - traffic 232
 - RF
 - intrusion detection 262
 - spectrum management 262
 - RF Analysis Manager
 - see RAM 16
 - RF configuration 262
 - RF management
 - see channel 262
 - RF Performance Manager
 - see RPM 14
 - RF resilience 262
 - RF Security Manager
 - see RSM 15
- roaming 13, 95, 249
 - see fast roaming 235
 - Rogue AP 7, 51, 107, 206, 406
 - rogue AP
 - blocking 273
 - settings for blocking 270
 - Rogue AP List 107
 - rogue APs
 - auto block settings 273
 - blocking 262
 - Rogue Control List 206
 - rogue detection 12
 - rogues
 - setting as known or approved 108
 - root command prompt 317
 - route
 - trace route utility 305
 - routing table window 98
 - RPM (RF Performance Manager) 14
 - RSM (RF Security Manager) 15
 - RSSI 107
 - RTS 250, 254
 - RTS threshold 250, 254

S

- sample Perl and CSS files for 304
- save
 - with reboot 298
- Save button 76
- saved.conf 300
- scalability 6
- schedule
 - auto channel configuration 262
- Secondary Port 395
- Secondary Server 395
- secret 395
- Secure Shell 20
- secure Shell 19
- Security
 - FIPS 431
 - PCI DSS 425
- security 7, 13, 175, 404, 406
 - certificate, see certificate 192
- Security Manager
 - see RSM 15
- see group 228
- self-monitoring 273
 - radio assurance 372
 - radio assurance options 263
- self-test
 - radio assurance mode 263
- serial port 20, 65, 406
- server, VTun
 - see VTun 174
- servers
 - connectivity, see network assurance 101, 191
- Service Set Identifier 68
- Services 156, 379, 382, 404
- servicing 377
- servicing the unit 375
- settings 139
- setup, express 139
- sharp cell 262
 - setting in WMI 265
- short retry limit 243
- signal processing
 - MIMO 36
- skin
 - changing WMI appearance 309
- SNMP 7, 10, 68, 139, 147, 156, 165, 396
 - required for XMS 165, 166
- software
 - upgrade license key 299
- software image
 - upgrading via CLI 418
- Software Upgrade 295
- software upgrade 298
- spatial multiplexing 37
- spectrum (RF) management 262
- speed 6, 65, 147
 - 11 Mbps 6
 - 54 Mbps 6
- splash page
 - web page redirect 221, 304
 - web page redirect, customize 222
- SSH 19, 20, 51, 68, 139, 147, 176, 399, 406
- SSH-2 176
- SSID 7, 68, 76, 107, 139, 206, 213, 397, 404, 410
 - about usage 405
 - active IAPs 225
 - QoS 209, 214
 - about using 405
 - QoS, about usage 405
 - web page redirect settings 217
 - web page redirect settings, about 219, 223, 224
- SSID Access List 226
- SSID address 226
- SSID Management 213, 397, 404
- standby mode 262
- stateful filtering

- disabling 284
 - static IP 68, 139, 147
 - station
 - assurance 267
 - station assurance 267
 - station timeout period 243
 - Stations 404
 - stations
 - limits and interactions 232
 - rogues 108
 - statistics 132
 - statistics per station 133
 - statistics 139
 - filters 132
 - netflow 159
 - per-station 133
 - stations 132
 - WDS 131
 - status bar 76, 81
 - style
 - WMI appearance 309
 - submitting comments 81
 - subnet 19, 42, 68, 147
 - switch failover 42
 - synchronize 68, 139, 157
 - Syslog 68, 76, 139, 156, 162, 395
 - time-stamping 68
 - syslog messages
 - counters 80
 - Syslog reporting 162
 - Syslog Server 162
 - system commands
 - ping, trace route, RADIUS ping 305
 - System Configuration Reset 295
 - System Log 162
 - system log
 - viewing window 134
 - system memory
 - replacing 386
 - System Reboot 295
 - System Tools 295
 - system tools 296
- ## T
- tag, WiFi 161
 - T-bar 61
 - T-bar clips 61
 - TCP
 - port requirements 48
 - technical support
 - contact information 423
 - frequently asked questions 404
 - Telnet 176, 399, 406
 - Temporal Key Integrity Protocol 406
 - TFTP server
 - automatic update of boot image, configuration 299
 - Time Out 395
 - time zone 68, 139, 157
 - timeout 243, 295
 - Tips 403
 - TKIP 13, 45, 55, 68, 139, 397, 406
 - TKIP encryption
 - and XN Arrays 198
 - tool
 - ping, trace route, RADIUS ping 305
 - Tools 295, 406
 - tools, network 305
 - tools, system 296
 - trace route utility 305
 - traffic
 - filtering 283
 - limits and interactions 232
 - transmit power 24
 - Trap Host 396
 - trap port 165, 396
 - tunneled
 - fast roaming 249

tunnels
see VTun 171, 174

U

UDP

port requirements 48

Unit 61

attaching 61

mounting 61

unknown

setting rogues 108

upgrade

license key 299

software image 298

upgrading software image

via CLI 418

UPS 19, 55

user accounts

setting RADIUS VSAs 201

user group 228

QoS 231

user group limits and interactions 232

user interface 75

utilities

ping, trace route, RADIUS ping
305

utility buttons 81

V

Vendor Specific Attributes (VSAs)

RADIUS, for Xirrus 415

virtual tunnels

see VTun 174

VLAN 7, 55, 213, 397, 404, 410

broadcast optimization 248

dynamic

overridden by group 231

group (vs. dynamic VLAN) 231

vlan

CLI command 358

VLAN ID 213

VLANs 171

and fast roaming 236

voice

fast roaming 235

implementing on Array 22, 171,
210

Voice-over IP 254

VoIP 254

VoWLAN 14

VPN 68, 139, 406

VTs

Virtual Tunnel Server 171, 174

VTun

specifying tunnel server 171, 174

understanding 171

W

wall thickness considerations 22

warning messages 79

WDS 278, 280

about 52

long distance 241, 279

planning 52

statistics 131

timeouts 241, 279

WDS Client Links 280

Web interface

structure and navigation 79

web interface 75

Web Management Interface 51, 61, 62, 65, 83, 404

Web Management Interface (WMI) 75

web page redirect 304

also called WPR 304

CHAP (Challenge-Handshake Au-
thentication Protocol) 222

customize internal login/splash
page 222

HTTPS port 219, 223, 224

- install files for 304
 - internal login page 220
 - internal splash page 221
 - PAP, CHAP 222
 - RADIUS settings 222
 - remove files for 305
 - sample WPR files 305
 - SSID settings 217
 - SSID settings, about 219, 223, 224
 - WEP 13, 45, 68, 139, 175, 213, 397, 406
 - WEP (Wired Equivalent Privacy)
 - encryption method 177
 - WEP encryption
 - and XN Arrays 199
 - Wi-Fi Protected Access 7, 45, 68, 139, 406
 - WiFi tag 161
 - wifi-tag
 - CLI command 359
 - window loading
 - WMI 311
 - Wired Equivalent Privacy 68, 406
 - Wireless Distribution System 278
 - wireless LAN 6
 - wireless security 139
 - WLAN 139
 - WMI 7, 51, 55, 65, 75, 237
 - appearance options 309
 - appearance, changing 309
 - certificate error 179, 192
 - executing CLI commands 308
 - menu behavior 311
 - options 309
 - page loading 311
 - refresh interval 311
 - workflow 56
 - WPA 7, 55, 68, 139, 175, 213, 397, 406
 - WPA (Wi-Fi Protected Access) and WPA2
 - encryption method 177
 - WPA2 7
 - WPR
 - see web page redirect 304
 - wpr.pl 304, 305
- X**
- X.509
 - certificate 179, 192
 - XA-3300 1, 7
 - Xirrus
 - certificate authority 192
 - Xirrus Advanced RF Analysis Manager
 - see RAM 16
 - Xirrus Advanced RF Performance Manager
 - see RPM 14
 - Xirrus Advanced RF Security Manager
 - see RSM 15
 - Xirrus Management System 8, 10, 13, 21
 - SNMP required 165, 166
 - Xirrus Management System (XMS) 1
 - Xirrus PoGE Power Injectors 1
 - Xirrus Power over Gigabit Ethernet 19
 - Xirrus Remote DC Power System 19, 58
 - Xirrus Roaming Protocol 13, 95, 249
 - Xirrus Wireless Management System 19, 51, 406
 - XM-3300 1, 7, 19, 51, 55, 165, 406
 - XMS 8, 10, 13, 21
 - port requirements 48
 - setting IP address of 165
 - SNMP required 165, 166
 - XN Arrays
 - see also IEEE 802.11n 34
 - XN12 1, 7
 - XN16 1, 7
 - management 295

XN4 1, 7
XN8 1, 7
XP PoGE Power Injectors 1
XP1, XP8
 see Power over Gigabit Ethernet 10
XP-3100 19, 55, 58
XPS 19
XRP 13, 95, 249
xs_current.conf 300
xs_diagnostic.log 303
XS16 1, 7
 management 137, 295
XS4 1, 7
XS8 1, 7

User's Guide



Wi-Fi Arrays