




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 261.



Figure 163. 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 and XN arrays.

Long Distance Links

If you are using WDS 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 274) 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.

Figure 164. WDS Client Links

Procedure for Setting Up WDS Client Links

WDS Client Link Settings:

1. **Host Link Stations:** Check the **Allow** checkbox to instruct the Array to allow stations to associate to IAPs on a host Array that participates in a WDS link. The WDS host IAP will send beacons announcing its availability to wireless clients. This is disabled by default.



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.

2. **Spanning Tree Protocol (STP):** Check the **Enable** checkbox to instruct the Array to enforce the Spanning Tree Protocol on all WDS links. This is enabled by default. Use of STP is strongly recommended in most situations. However, in situations like the one in the next step, where WDS is used by an Array mounted on a high speed train, STP can add significant delay (often on the order of 30 to 60 seconds) while initially analyzing network topology. In such a situation, it may be desirable to disable STP.



Caution: If STP is disabled and a network connection is made on the WDS Client Array's Gigabit link that can reach the WDS Host Array, broadcast and multicast packets will not be blocked. A broadcast storm may cause a network outage.

3. **Roaming RSSI Threshold:** If an Array is deployed on a mobile site (on a train, for example), you can use WDS to implement a wireless backhaul that will roam between Arrays at fixed locations. When another candidate Array for WDS host target is found, the client link will roam to the new Array if its RSSI is stronger than the RSSI of the current host connection by at least the **Roaming RSSI Threshold**. The default is 6 dB.
4. **Roaming RSSI Averaging Weight:** This weight changes how much the latest RSSI reading influences the cumulative weighted RSSI value utilized in checking the threshold (above) to make a roaming decision.

The higher the weight, the lower the influence of a new RSSI reading. This is not exactly a percentage, but a factor in the formula for computing the current RSSI value based on new readings:

$$\text{StoredRSSI} = (\text{StoredRSSI} * \text{RoamingAvgWeight} + \text{NewRSSIReading} * (100 - \text{RoamingAvgWeight})) / 100$$

This prevents erroneous or out-of-line RSSI readings from causing the WDS link to jump to a new array. Such readings can result from temporary obstructions, external interference, etc.

5. Click **Save changes to flash** after you are finished making changes on this page if you wish to make your changes permanent.

WDS Client Link IAP Setting:

6. **Enable/Disable/Reset All Links:** Click the appropriate button to:
 - **Enable All Links**—this command activates all WDS links configured on the Array.
 - **Disable All Links**—this command deactivates all WDS links configured on the Array. It leaves all your settings unchanged, ready to re-enable.
 - **Reset All Links**—this command tears down all links configured on the Array and sets them back to their factory defaults, effective immediately.
7. **Client Link:** Shows the ID (1 to 4) of each of the four possible WDS links.
8. **Enabled:** Check this box if you want to enable this WDS link, or uncheck the box to disable the link.
9. **Max IAPs Allowed (1-3):** Enter the maximum number of IAPs for this link, between 1 and 3.
10. **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. To allow any Xirrus Array to be accepted as a WDS target, enter the Xirrus OUI: **00:0f:7d:00:00:00** (this is useful for roaming in a mobile deployment, as described in [Step 3 on page 341](#)).

- 11. Target SSID:** Enter the SSID that the target Array is using.
- 12. 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.
- 13. Password:** Enter a password for this WDS link.
- 14. Clear Settings:** Click on the **Clear** button to reset all of the fields on this line.

WDS Client Link IAP Assignments:

- 15.** For each desired client link, select the IAPs that are part of that link. The IAP channel assignments are shown in the column headers.
- 16. 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.

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 361.

The Wireless 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.



The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic. See "Air Cleaner" on page 403.

XIRRUS Xirrus XRM4

Base: FW401000000 (151.100.1.1)

Global Config: enabled

Applicat. Control: enabled

NAME	TYPE	LOG	ENABLE	ACT	FORWARD	SNATCH	EXTENSION	GROUP
Application								
Yankee	allow	3	any	any	allow	any	any	
Yankee	allow	3	any	any	any	any	any	
Global								
air-cleaner-Block-1	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-2	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-3	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-4	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-5	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-6	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-7	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-8	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-9	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-10	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-11	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-12	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-13	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-14	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-15	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-16	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-17	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-18	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-19	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-20	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-21	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-22	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-23	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-24	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-25	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-26	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-27	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-28	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-29	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-30	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-31	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-32	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-33	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-34	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-35	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-36	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-37	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-38	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-39	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-40	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-41	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-42	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-43	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-44	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-45	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-46	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-47	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-48	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-49	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-50	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-51	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-52	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-53	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-54	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-55	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-56	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-57	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-58	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-59	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-60	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-61	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-62	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-63	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-64	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-65	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-66	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-67	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-68	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-69	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-70	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-71	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-72	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-73	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-74	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-75	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-76	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-77	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-78	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-79	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-80	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-81	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-82	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-83	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-84	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-85	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-86	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-87	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-88	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-89	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-90	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-91	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-92	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-93	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-94	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-95	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-96	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-97	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-98	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-99	deny	7	any	any	any	any	any	10.10.10.0/10
air-cleaner-Block-100	deny	7	any	any	any	any	any	10.10.10.0/10

Orange arrow expands/collapses display

Figure 165. Filters

User connections managed by the firewall are maintained statefully—once a user flow is established through the Array, it is recognized and passed through

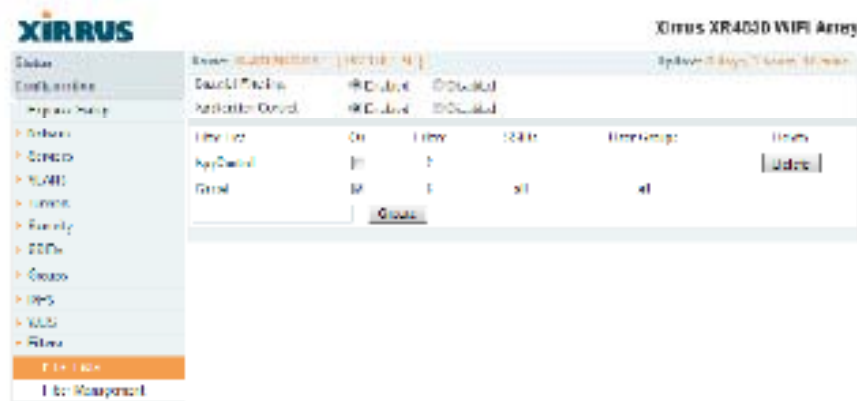
without application of all defined filtering rules. Stateful inspection runs automatically on the Array. The rest of this section describes how to view and manage filters.

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

The read-only Filters window provides you with an overview of all filter lists that have been defined for this Array, and the filters that have been created in each list. Filters are listed in the left side column by name under the filter list to which they belong. Each filter entry is a link that takes you to its **Filter Management** entry, and the list 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.



Filter List	Type	Protocol	Port	Source	Destination	QoS	VLAN
Global	M	T	all	all			

Figure 166. 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. **Application Control:** Operation of the Application Control feature may be **Enabled** or **Disabled**. See "Application Control Windows" on page 150.



The Application Control feature is only available if the Array license includes Application Control. If a setting is unavailable (grayed out), then your license does not support the feature. See "About Licensing and Upgrades" on page 361.

Application Control data is only available from XR Series Array models. It is not available on XN Arrays.

3. **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.
4. **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.
5. **Filters:** This read-only field displays the number of filters that belong to this filter list.
6. **SSIDs:** This read-only field lists the [SSIDs](#) that use this filter list.
7. **User Groups:** This read-only field lists the [Groups](#) that use this filter list.
8. **Delete:** Click this button to delete this filter list. The **Global** filter list may not be deleted.

9. Click **Save changes** to flash if you wish to make your changes permanent.
10. 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 an especially powerful feature when combined with the intelligence provided by the “Application Control Windows” on page 150.

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



The screenshot displays the Filter Management window. At the top, there is a header with the text "Filters are applied in order, from top to bottom, Click here to change the order." and an arrow pointing to a "Change Order" button in the top right corner of the table below. The table lists several filter rules with columns for ID, Name, Type, and various filter criteria. Below the table, there are two sections for defining filter criteria: "Filter Criteria" and "Application Filter". Each section has a list of criteria with checkboxes and input fields for values.

Figure 167. Filter Management

Based on Application Control's analysis of your wireless traffic, you can create filters to enhance wireless usage for your business needs:

- Usage of non-productive and risky applications like BitTorrent can be restricted.
- Traffic for mission-critical applications like VoIP and WebEx may be given higher priority (QoS).
- Non-critical traffic from applications like YouTube may be given lower priority (QoS).
- Traffic flows for specific applications may be controlled by sending them into VLANs that are designated for that type of traffic.

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. **Add Preset Filter:** A number of predefined "Air Cleaner" filters are available using these buttons. You can use these rules to eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. For more information, please see "Air Cleaner" on page 403.
3. **New Filter Name:** To add a new filter, enter its name in the field next to the **Create** button at the bottom of the list, then click **Create**. All new filters are added to the table of filters in 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.

Viewing or modifying existing filter entries:

4. **Filter:** Select a filter entry if you wish to modify it. Source and destination details are displayed below the bottom of the list.
5. **On:** Use this field to enable or disable this filter.
6. **Log:** Log usage of this filter to Syslog.
7. **Type:** 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.
8. **Layer:** Select network layer 2 or 3 for operation of this filter.
9. **Protocol/Number:** 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.
10. **Port/Number:** 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)	8184

11. **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 Wireless Array”](#) on page 244.
12. **VLAN/Number:** (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 199).

13. **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.
14. To delete a filter, click its **Delete** button.

Select an existing filter entry in the list to view or modify the following, shown below the list of filters:

15. **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.
16. **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.

Below the Source and Destination Addresses, you may enter a **Category** or an **Application** to be matched by the filter:

17. **Category:** If you wish this filter to apply to a particular category of application, such as **File-Transfer** or **Database**, select it from the listed options.



Figure 168. Filter Category or Application

18. **Applications:** If you wish this filter to apply to a specific application, such as **WebEx**, click the letter or number that it starts with. Then select the desired application. You may select a **Category** or an **Application**, but not both.
19. Click **Save changes to flash** if you wish to make your changes permanent.

See Also[Filters](#)[Filter Statistics](#)[Understanding QoS Priority on the Wireless Array](#)[VLANs](#)

Clusters



This feature is not available on XR-500 Series Arrays.

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.

Xirrus XR4930 WFI Array				
Base: 37141204300 (10.10.1.10)		Export: 37141204300 (10.10.1.10)		
Name	IP Address	Username	Password	Array
Cluster				
Cluster0001	10.10.1.10	admin	****	

Figure 169. 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.



Figure 170. 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.



Figure 171. 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.



An XR-1000 Series Array cannot act as the Cluster controller. It will operate correctly as a member of a 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.



Figure 172. 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.

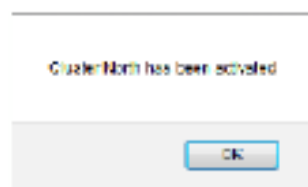


Figure 173. Cluster Mode Activation

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 174.

The screenshot shows the WMI interface in Cluster Mode. At the top, the 'Cluster Name' is 'Cluster: North'. Below this, there is a 'Specify Grouping' dropdown menu set to 'Group by Array'. To the right, there is an 'Exit Cluster Mode' button. The main content area displays a table of statistics for two WMI windows. Each window has a 'Close' button. The table has columns for 'Receive' and 'Transmit' counts for various error types.

WMI Window	Receive	Transmit
Receive Bytes	0	Transmit Bytes
Receive Compressed	0	Transmit Compressed
Receive Multicast	0	Transmit Multicast
Receive Dropped	0	Transmit Dropped
Receive 802.11 Error	0	Transmit 802.11 Error
Receive 802.11 Retries	0	Transmit 802.11 Retries
Receive Total Errors	0	Transmit Total Errors
Receive Collisions	0	Transmit Collisions
Receive Packets	0	Transmit Packets
Receive Packets Received	0	Transmit Packets Received

Figure 174. 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 Wireless 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 360](#)
- [“CLI” on page 371](#)
- [“Options” on page 373](#)
- [“Logout” on page 376](#)

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 43 on page 89](#))

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

- [“Viewing Status on the Wireless Array” on page 95](#)
- [“Configuring the Wireless Array” on page 159](#)

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.

The screenshot shows the 'System Tools' section of a web interface. It includes various configuration options and buttons for file management and diagnostics. At the bottom, there is a progress bar and a status area. Two black arrows point to these areas with the following labels:

- Progress is shown here**: Points to the progress bar.
- Status is shown here**: Points to the status area below the progress bar.

Figure 175. 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 361.

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 101.

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 Wireless Array” on page 63. Alternatively, use the **Reboot** button to discard any configuration changes which have not been saved since the last reboot. You may specify an optional **Delay** period in seconds to wait before the reboot starts.
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 361 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 WML, see “Upgrading the Array via CLI” on page 464 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!

- License Key:** If Xirrus provides you with a new license key for your Array, use this field to enter it, then click the **Apply** 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.

- 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.
- 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 171](#)), or if you have configured management over a VLAN it will maintain the management VLAN's IP address (see ["VLAN Management" on page 201](#)). *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 176)



Figure 176. 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 253](#) 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:

Remove File:

Download Sample Files: [wpr.pl](#) [hs.css](#)

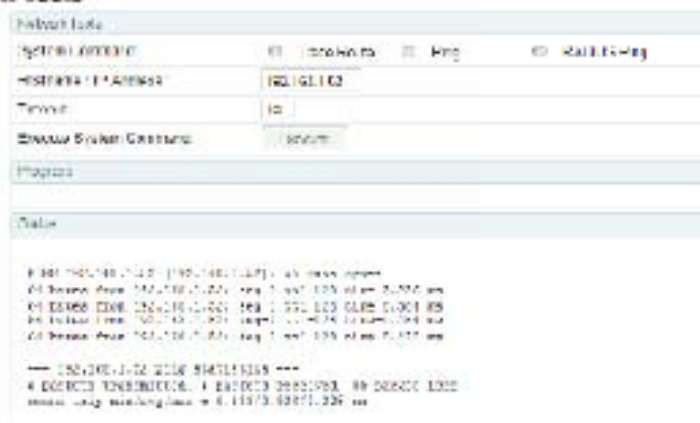
Figure 177. Managing WPR Splash/Login page files

- 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



```

System Command (Ping)
-----
Hostname/IP Address: 192.168.1.102
Timeout: 10
Execute System Command: Execute

Output:
-----
Pinging 192.168.1.102 [192.168.1.102]: 32 bytes of data:
64 bytes from 192.168.1.102: icmp_seq=1 ttl=64 time=0.200 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=64 time=0.201 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=64 time=0.201 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=64 time=0.201 ms

--- 192.168.1.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, 0%
time = 0.817s, ping times = 0.817s, 0.201 ms
  
```

Figure 178. 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.

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 179 (A), RADIUS Ping is unable to contact the server. In Figure 179 (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.

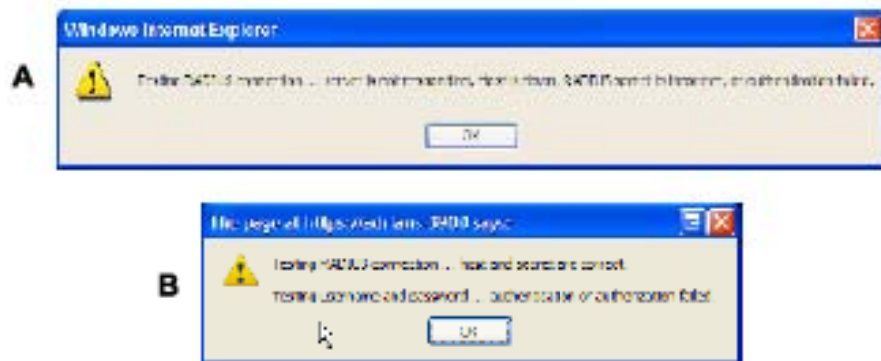


Figure 179. Radius Ping Output

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.

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. If output runs past the right edge of the screen, there is also a horizontal scroll bar at the bottom of the page.

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. By default, the Array uses the **New** style option, shown below.

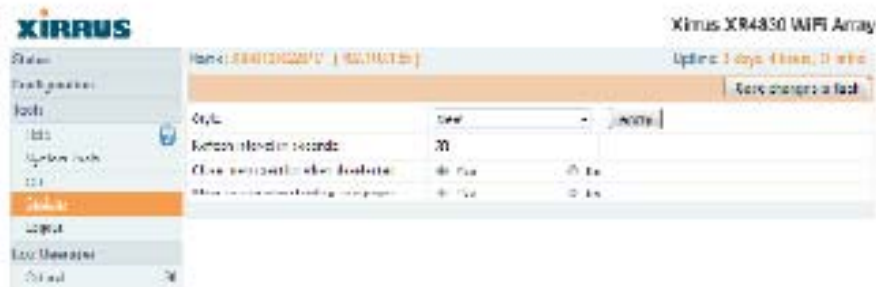


Figure 181. WMI Display Options

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 182. iPhone Style Option

For example, the **iPhone** style option (Figure 182) 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 182 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.).

- 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: XIRBUS@XIRBUS.COM (10.10.10.10)	
Current Status:	Logged Out
User Name:	admin
User Password:	****

Figure 183. Login Window

The Command Line Interface

This section covers the commands and the command structure used by the Wireless 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 377.
- "Getting Started with the CLI" on page 379.
- "Top Level Commands" on page 381.
- "Configuration Commands" on page 390.
- "Sample Configuration Tasks" on page 426.



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 361.

See Also

Establishing Communication with the Array
Network Map
System Tools

Establishing a Secure Shell (SSH) Connection

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

1. Start your SSH session and communicate with the Array via its IP address.
 - If the Array is connected to a network that uses DHCP, use the address assigned by DHCP. We recommend that you have the

network administrator assign a reserved address to the Array for ease of access in the future.

- If the network does not use DHCP, use the factory default address 10.0.2.1 to access either the Gigabit 1 or Gigabit 2 Ethernet port. You may need to change the IP address of the port on your computer that is connected to the Array—change that port's IP address so that it is on the same 10.0.2.xx subnet as the Array port.
 - If your Array is an 8-, 12-, or 16-port model, it has a 10/100Mb Ethernet port called Ethernet0. This management port has a default IP address of 10.0.1.1. You may connect your computer directly to this port, but you will need to set the IP address of the connected port on your computer to the 10.0.1.xx subnet.
2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the Array's Command Line Interface.



```
PUTTY (active)
Xirrus Hi-Fi Array
ArrayOS Version 9.0.423
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus Hi-Fi Array#
```

Figure 184. 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.



```

Xirrus_Wi-Fi_Array
Xirrus_Wi-Fi_Array
Copyright © 2005-2007 Xirrus, Inc.
All rights reserved.

Xirrus_Wi-Fi_Array
Password: *****

Xirrus_Wi-Fi_Array
Help for the command set are used to a command by entering
a keyword or part of a keyword matches. The help list will
be empty and you will receive only a blank line if the
keyword matches.

Two types of help are provided:
1) Full help is available when you are asked to enter a
command prompt. For example, type ? and you will receive
output.
2) Partial help is provided when an abbreviation of a command is entered
and you need to know that command's syntax. For example,
type ?config?
Xirrus_Wi-Fi_Array
  
```

Figure 185. Help Window

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 390.

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 390.
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 379.
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 385.
statistics	Display statistical data about the Array. See "statistics Commands" on page 388.
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 802.11an and bgn 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.
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.
diff	Display the difference between configurations.
dns	Display DNS summary information.

Command	Description
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.
rsi-map	Display RSSI map by IAP for station.
running-config	Display configuration information for the Array currently running.
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.

Command	Description
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 statistics iap abgn4
station	Display statistical data about associated stations. FORMAT: statistics station billw
vlan	Display statistical data for the defined VLAN. You must use the VLAN number (not its name) when defining a VLAN. FORMAT: statistics vlan 1

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 426.

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 352.

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	Rename a file.

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. Details about the air cleaner feature are after the end of this table. FORMAT: filter add [air-cleaner 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]

Air Cleaner

The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. You may select **all** of the air cleaner rules for the greatest effect, or only specific rules, such as **broadcast** or **multicast**, to eliminate only a particular source of traffic. The following options are offered:

```
MyArray(config)# filter add air-cleaner
all      All air cleaner filters
arp      Eliminate station to station ARPs over the air
broadcast Eliminate broadcast traffic from the air
dhcp     Eliminate stations serving DHCP addresses from the air
multicast Eliminate chatty multicast traffic from the air
netbios  Eliminate NetBIOS traffic from the air
```

If you select **all**, the rules shown in [Figure 188](#) are added to the predefined filter list named **Global**. These rules assume that you have station-to-station blocking enabled, that a DHCP server is on the Array's wired connection, and that you want to block most all multicast and all broadcast traffic not vital to normal

operation. If you find that there is a particular type of multicast or broadcast traffic that you want to allow, just add a specific allow filter for it before the deny filter in this list that would normally block it. Add or delete any of the Multicast rules as necessary for a specific site. Remember that the order of the rules is important.

Name	Type	Layer	Protocol	Port	Source	Destination	Action
Air-cleaner-Arp.1	deny	2	arp	any	1/any/any	1/any/any	on
Air-cleaner-Dhcp.1	deny	2	udp	6881	1/any/any	1/any/any	on
Air-cleaner-Dhcp.2	deny	2	udp	6881	1/any/any	1/any/any	on
Air-cleaner-Mcast.1	deny	2	udp	notidm	any	any	on
Air-cleaner-Mcast.2	deny	2	udp	notidm	any	any	on
Air-cleaner-Mcast.3	deny	2	udp	notidm	any	any	on
Air-cleaner-Mcast.4	deny	2	any	any	any	any	off
Air-cleaner-Mcast.5	deny	2	any	any	any	any	off
Air-cleaner-Mcast.6	deny	2	any	any	any	any	off
Air-cleaner-Mcast.7	deny	2	any	any	any	any	off
Air-cleaner-Mcast.8	deny	2	any	any	any	any	off
Air-cleaner-Mcast.9	deny	2	any	any	any	any	off
Air-cleaner-Dhcp.3	allow	2	udp	6881	any	any	on
Air-cleaner-Dhcp.4	allow	2	udp	6881	any	any	on
Air-cleaner-Dhcp.5	deny	2	any	any	any	any	on

Figure 188. Air Cleaner Filter Rules

Explanations of some sample rules are below.

- **Air-cleaner-Arp.1** blocks ARPs from one client from being transmitted to clients via all of the radios. The station to station block setting doesn't block this traffic, so this filter eliminates this unnecessary traffic.
- **Air-cleaner-Dhcp.1** drops all DHCP client traffic coming in from the gigabit interface. This traffic doesn't need to be transmitted by the radios since there shouldn't be any DHCP server associated to the radios and offering DHCP addresses. For large subnets the DHCP discover/request broadcast traffic can be significant.
- **Air-cleaner-Dhcp.2** drops all DHCP server traffic coming in from the radio interfaces. There should not be any DHCP server associated to the radios. These rogue DHCP servers are blocked from doing any damage with this filter. There have been quite a few cases in public venues like schools and conventions where such traffic is seen.

- **Air-cleaner-Mcast.1** drops all multicast traffic with a destination MAC address starting with 01. This filters out a lot of IP multicast traffic that starts with 224.
- **Air-cleaner-Mcast.2** drops all multicast traffic with a destination MAC address starting with 33. A lot of IPv6 traffic and other multicast traffic is blocked by this filter.
- **Air-cleaner-Mcast.3** drops all multicast traffic with a destination MAC address starting with 09. A lot of Appletalk traffic and other multicast traffic is blocked by this filter. Note that for OSX 10.6,* Snow Leopard no longer supports Appletalk.
- **Air-cleaner-Bcast.1** allows all ARP traffic (other than the traffic that was denied by **Air-cleaner-Arp.1**). This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.4** allows all XRP traffic from Arrays to be received from the wire. This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.5** drops all other broadcast traffic that hasn't previously been explicitly allowed. This filter will catch all UDP broadcast traffic as well as all other known and unknown protocol broadcast traffic.



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 264.

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

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: <code>management <cr></code>

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

- **banner** Configure login banner messages
- **console** Configure console management parameters
- **https** Enable/disable HTTPS access
- **license** Set array software license key
- **load** Load running configuration from flash
- **max-auth-attempts** Maximum number of authentication (login) attempts (0 means unlimited)
- **network-assurance** Enable/disable network assurance
- **reauth-period** Time between failed CLI login attempts
- **restore** Restore to previous saved config
- **revert** Revert to saved configuration after delay if configuration not saved
- **save** Save running configuration to flash
- **ssh** Enable/disable SSH access
- **standby** Configure standby parameters
- **telnet** Enable/disable telnet access
- **uptime** Display time since last boot
- **xircon** Enable/disable xircon access. See *Xircon User's Guide* for more information. Not available for XN Arrays.

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 IAPs (radios). FORMAT: no dot11a
dot11b	Disable all 802.11b IAPs (radios). FORMAT: no dot11b
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
<code><cr></code>	Enter run-tests mode. FORMAT: <code>run-tests</code>
<code>iperf</code>	Execute iperf utility. FORMAT: <code>run-tests iperf</code>
<code>kill-beacons</code>	Turn off beacons for selected single IAP. FORMAT: <code>run-tests kill-beacons [off iap-name]</code>
<code>kill-probe-responses</code>	Turn off probe responses for selected single IAP. FORMAT: <code>run-tests kill-probe-responses [off iap-name]</code>
<code>led</code>	LED test. FORMAT: <code>run-tests led [flash rotate]</code>
<code>memtest</code>	Execute memory tests. FORMAT: <code>run-tests memtest</code>
<code>ping</code>	Execute ping utility. FORMAT: <code>run-tests ping [host-name ip-addr]</code>

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

Command	Description
telnet	Execute telnet utility. FORMAT: run-tests telnet [hostname ip-addr] [command-line-switches (optional)]
tracert	Execute traceroute utility. FORMAT: run-tests tracert [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: <code>vlan add [newvlan]</code>
default-route	Assign a VLAN for the default route (for outbound management traffic). FORMAT: <code>vlan default-route [defaultroute]</code>
delete	Delete a VLAN. FORMAT: <code>vlan delete [oldvlan]</code>
edit	Modify an existing VLAN. FORMAT: <code>vlan edit [existingvlan]</code>
native-vlan	Assign a native VLAN (traffic is untagged). FORMAT: <code>vlan native-vlan [nativevlan]</code>
no	Disable the selected feature. FORMAT: <code>vlan no [feature]</code>
reset	Delete all existing VLANs. FORMAT: <code>vlan reset</code>

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 188.

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 Wireless Array, including:

- “Configuring a Simple Open Global SSID” on page 427.
- “Configuring a Global SSID using WPA-PEAP” on page 428.
- “Configuring an SSID-Specific SSID using WPA-PEAP” on page 429.
- “Enabling Global IAPs” on page 430.
- “Disabling Global IAPs” on page 431.
- “Enabling a Specific IAP” on page 432.
- “Disabling a Specific IAP” on page 433.
- “Setting Cell Size Auto-Configuration for All IAPs” on page 434
- “Setting the Cell Size for All IAPs” on page 435.
- “Setting the Cell Size for a Specific IAP” on page 436.
- “Configuring VLANs on an Open SSID” on page 437.
- “Configuring Radio Assurance Mode (Loopback Tests)” on page 438.

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.

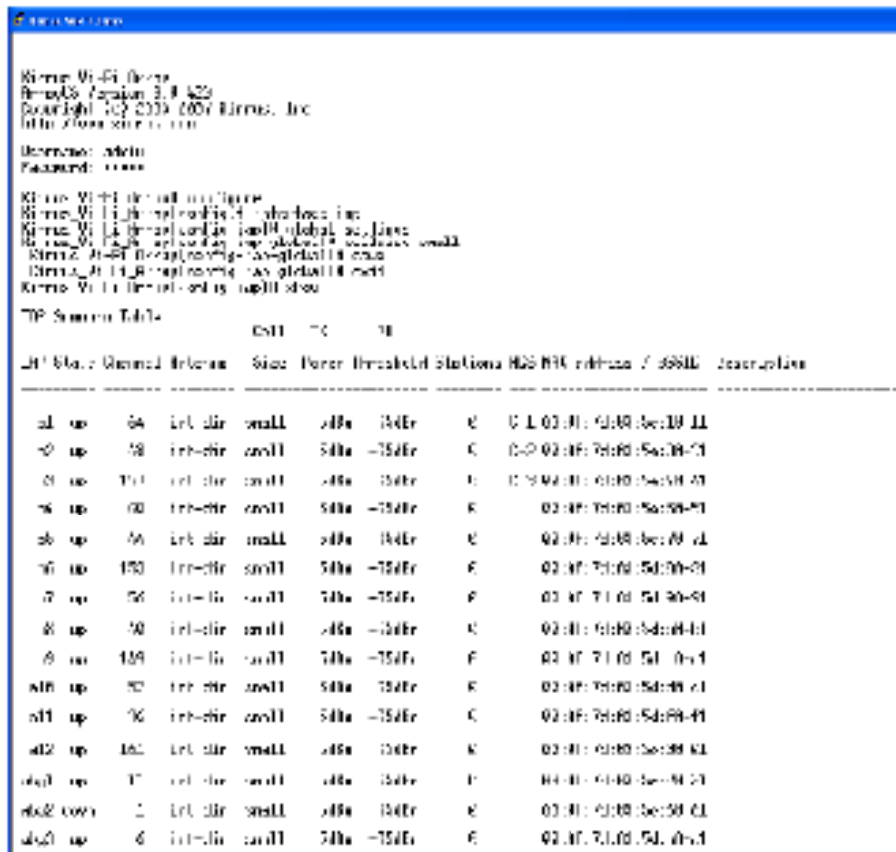
Some of the screen images shown in this section have been modified for clarity. For example, the image may have been “elongated” to show all data without the need for additional images or scrolling. We recommend that you use the Adobe PDF version of this User’s Guide when reviewing these examples—a hard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

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

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 31.



```

Xirrus Wi-Fi Group
Xirrus Version 3.4.429
Copyright (C) 2019 (2007) Xirrus, Inc.
All rights reserved.

Username: admin
Password: admin

Xirrus Wi-Fi Controller Settings
Xirrus Wi-Fi Controller Radio 1 - auto-tune on
Xirrus Wi-Fi Controller Radio 2 - global cell size
Xirrus Wi-Fi Controller Radio 3 - global cell size small
Xirrus Wi-Fi Controller Radio 4 - global cell size
Xirrus Wi-Fi Controller Radio 5 - global cell size
Xirrus Wi-Fi Controller Radio 6 - global cell size
Xirrus Wi-Fi Controller Radio 7 - global cell size
Xirrus Wi-Fi Controller Radio 8 - global cell size
Xirrus Wi-Fi Controller Radio 9 - global cell size
Xirrus Wi-Fi Controller Radio 10 - global cell size
Xirrus Wi-Fi Controller Radio 11 - global cell size
Xirrus Wi-Fi Controller Radio 12 - global cell size
Xirrus Wi-Fi Controller Radio 13 - global cell size
Xirrus Wi-Fi Controller Radio 14 - global cell size
Xirrus Wi-Fi Controller Radio 15 - global cell size
Xirrus Wi-Fi Controller Radio 16 - global cell size
Xirrus Wi-Fi Controller Radio 17 - global cell size
Xirrus Wi-Fi Controller Radio 18 - global cell size
Xirrus Wi-Fi Controller Radio 19 - global cell size
Xirrus Wi-Fi Controller Radio 20 - global cell size
Xirrus Wi-Fi Controller Radio 21 - global cell size
Xirrus Wi-Fi Controller Radio 22 - global cell size
Xirrus Wi-Fi Controller Radio 23 - global cell size
Xirrus Wi-Fi Controller Radio 24 - global cell size
Xirrus Wi-Fi Controller Radio 25 - global cell size
Xirrus Wi-Fi Controller Radio 26 - global cell size
Xirrus Wi-Fi Controller Radio 27 - global cell size
Xirrus Wi-Fi Controller Radio 28 - global cell size
Xirrus Wi-Fi Controller Radio 29 - global cell size
Xirrus Wi-Fi Controller Radio 30 - global cell size
Xirrus Wi-Fi Controller Radio 31 - global cell size
Xirrus Wi-Fi Controller Radio 32 - global cell size
Xirrus Wi-Fi Controller Radio 33 - global cell size
Xirrus Wi-Fi Controller Radio 34 - global cell size
Xirrus Wi-Fi Controller Radio 35 - global cell size
Xirrus Wi-Fi Controller Radio 36 - global cell size
Xirrus Wi-Fi Controller Radio 37 - global cell size
Xirrus Wi-Fi Controller Radio 38 - global cell size
Xirrus Wi-Fi Controller Radio 39 - global cell size
Xirrus Wi-Fi Controller Radio 40 - global cell size
Xirrus Wi-Fi Controller Radio 41 - global cell size
Xirrus Wi-Fi Controller Radio 42 - global cell size
Xirrus Wi-Fi Controller Radio 43 - global cell size
Xirrus Wi-Fi Controller Radio 44 - global cell size
Xirrus Wi-Fi Controller Radio 45 - global cell size
Xirrus Wi-Fi Controller Radio 46 - global cell size
Xirrus Wi-Fi Controller Radio 47 - global cell size
Xirrus Wi-Fi Controller Radio 48 - global cell size
Xirrus Wi-Fi Controller Radio 49 - global cell size
Xirrus Wi-Fi Controller Radio 50 - global cell size
Xirrus Wi-Fi Controller Radio 51 - global cell size
Xirrus Wi-Fi Controller Radio 52 - global cell size
Xirrus Wi-Fi Controller Radio 53 - global cell size
Xirrus Wi-Fi Controller Radio 54 - global cell size
Xirrus Wi-Fi Controller Radio 55 - global cell size
Xirrus Wi-Fi Controller Radio 56 - global cell size
Xirrus Wi-Fi Controller Radio 57 - global cell size
Xirrus Wi-Fi Controller Radio 58 - global cell size
Xirrus Wi-Fi Controller Radio 59 - global cell size
Xirrus Wi-Fi Controller Radio 60 - global cell size
Xirrus Wi-Fi Controller Radio 61 - global cell size
Xirrus Wi-Fi Controller Radio 62 - global cell size
Xirrus Wi-Fi Controller Radio 63 - global cell size
Xirrus Wi-Fi Controller Radio 64 - global cell size
Xirrus Wi-Fi Controller Radio 65 - global cell size
Xirrus Wi-Fi Controller Radio 66 - global cell size
Xirrus Wi-Fi Controller Radio 67 - global cell size
Xirrus Wi-Fi Controller Radio 68 - global cell size
Xirrus Wi-Fi Controller Radio 69 - global cell size
Xirrus Wi-Fi Controller Radio 70 - global cell size
Xirrus Wi-Fi Controller Radio 71 - global cell size
Xirrus Wi-Fi Controller Radio 72 - global cell size
Xirrus Wi-Fi Controller Radio 73 - global cell size
Xirrus Wi-Fi Controller Radio 74 - global cell size
Xirrus Wi-Fi Controller Radio 75 - global cell size
Xirrus Wi-Fi Controller Radio 76 - global cell size
Xirrus Wi-Fi Controller Radio 77 - global cell size
Xirrus Wi-Fi Controller Radio 78 - global cell size
Xirrus Wi-Fi Controller Radio 79 - global cell size
Xirrus Wi-Fi Controller Radio 80 - global cell size
Xirrus Wi-Fi Controller Radio 81 - global cell size
Xirrus Wi-Fi Controller Radio 82 - global cell size
Xirrus Wi-Fi Controller Radio 83 - global cell size
Xirrus Wi-Fi Controller Radio 84 - global cell size
Xirrus Wi-Fi Controller Radio 85 - global cell size
Xirrus Wi-Fi Controller Radio 86 - global cell size
Xirrus Wi-Fi Controller Radio 87 - global cell size
Xirrus Wi-Fi Controller Radio 88 - global cell size
Xirrus Wi-Fi Controller Radio 89 - global cell size
Xirrus Wi-Fi Controller Radio 90 - global cell size
Xirrus Wi-Fi Controller Radio 91 - global cell size
Xirrus Wi-Fi Controller Radio 92 - global cell size
Xirrus Wi-Fi Controller Radio 93 - global cell size
Xirrus Wi-Fi Controller Radio 94 - global cell size
Xirrus Wi-Fi Controller Radio 95 - global cell size
Xirrus Wi-Fi Controller Radio 96 - global cell size
Xirrus Wi-Fi Controller Radio 97 - global cell size
Xirrus Wi-Fi Controller Radio 98 - global cell size
Xirrus Wi-Fi Controller Radio 99 - global cell size
Xirrus Wi-Fi Controller Radio 100 - global cell size
  
```

TP Station Table									
AP	Chan	Ref	Size	Power	Breakout	Stations	MSR	MSR address / 65536	Description
1	up	94	1st dir	small	40m	100m	0	0.1.0.1:0.0.0.0:0.0.0.0	11
2	up	18	1st dir	small	50m	150m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
3	up	114	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
4	up	60	1st dir	small	50m	150m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
5	up	56	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
6	up	170	1st dir	small	50m	150m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
7	up	56	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
8	up	50	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
9	up	108	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
10	up	92	1st dir	small	50m	150m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
11	up	96	1st dir	small	50m	150m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
12	up	162	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
13	up	17	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
14	up	2	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11
15	up	6	1st dir	small	40m	100m	0	0.0.0.0:0.0.0.0:0.0.0.0	11

Figure 197. 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 31.

```

Xirrus_Wi-Fi-Array
Xirrus_Wi-Fi-Array> show
Copyright (c) 2015-2020 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Warning: configure is not a valid command

Xirrus_Wi-Fi-Array> show
Xirrus_Wi-Fi-Array> show ip interface brief
Xirrus_Wi-Fi-Array> show ip interface brief
Xirrus_Wi-Fi-Array> show ip interface brief
Xirrus_Wi-Fi-Array> show ip interface brief
Xirrus_Wi-Fi-Array> show ip interface brief

IAP Summary Table
-----
IP Status (Up/Down) | Interface | Size | Power | IP Address | Station MAC | BSSID | Channel | Frequency | Description
-----
a1 up | 64 | ltr-dbr | max | 2400m | 3400r | C | 0.1 | 00:01:00:00:00:00 | 11
a2 up | 78 | ltr-dbr | medium | 1400m | 3100r | C | 0.2 | 00:00:7d:00:5d:00 | C1
a3 up | 151 | ltr-dbr | max | 2400m | 3400r | C | 0.3 | 00:01:00:00:00:00 | C1
a4 up | 68 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | C1
a5 up | 76 | ltr-dbr | max | 2400m | 3400r | C | 00:00:7d:00:5d:00 | F1
a6 up | 152 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | F1
a7 up | 50 | ltr-dbr | max | 2400m | 3400r | C | 00:00:7d:00:5d:00 | F1
a8 up | 20 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | F1
a9 up | 100 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | F1
a10 up | 50 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | C1
a11 up | 20 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | F1
a12 up | 100 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | F1
ap1 up | 1 | ltr-dbr | max | 2400m | 3400r | C | 00:00:7d:00:5d:00 | F1
ap2 down | - | ltr-dbr | max | 2400m | 3400r | C | 00:00:7d:00:5d:00 | C1
ap3 up | 4 | ltr-dbr | max | 2400m | 3400r | C | 00:01:00:00:00:00 | C1
ap4 up | 7 | ltr-dbr | max | 2400m | 3400r | C | 00:00:7d:00:5d:00 | F1

Xirrus_Wi-Fi-Array> configure ip interface _

```

Figure 198. Setting the Cell Size for a Specific IAP

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 460.

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.

```

192.168.39.128 -PuTTY
Xirrus-MIFI-Arroyo# conf t
Xirrus-MIFI-Arroyo(config)# int interface 1ap
Xirrus-MIFI-Arroyo(config-if)# ip global_settings
Xirrus-MIFI-Arroyo(config-if)# ip global# increase detect standard
Interface 1AP abg? state changed to down
Interface 1AP abg? band changed to monitor
Interface 1AP abg? channel changed to monitor
Interface 1AP abg? antenna changed to internal and
Interface 1AP abg? tx-power changed to 38
Interface 1AP abg? rx-threshold changed to -94
Interface 1AP abg? state changed to up

Xirrus-MIFI-Arroyo(config-if)# ip global# loopback test
loopback-only      Enable  1AP loopback tests with alerts & repairs only
off                Disable 1AP loopback tests
robust allowed     Enable  1AP loopback tests with alerts & repairs & reboots if no
repair-without-test Enable 1AP loopback tests with alerts & repairs, but no robust-
test
set global 1AP parameters

Xirrus-MIFI-Arroyo(config-if)# ip global# increase-test repair-without-reboot
Xirrus-MIFI-Arroyo(config-if)# ip global#
Xirrus-MIFI-Arroyo(config-if)# ip global# stop

Global 1AP Settings Summary
-----
Country code      not set (defaults to US United States)
Access interval   100 msec
Broadcast rates   standard
DTIM period       1 beacon
Short retention   7
Lang             0
Local 1APs        10
Max stations/1AP  64
Max plmns /1AP   10
Station timeout   1000 sec
Station refresh   0 sec
Management        disabled
Station to station Forward
Load balancing     off
Intrusion detection standard
Ratd class power  up
Ratd class schedule none
Ratd cell period  1200 sec
Ratd cell overlap 50
Steered Cell Handing with tunnels to change in-range or targeted
Steered cell TX power off
Radio Safety Mode disabled
802.11h support    on
Loopback test mode explicit w/o robust
L1h enabled by    on when 1AP up
                  Link on data frame transmitted
                  Link on data frame received
                  Link on management frame transmitted
                  Link on management frame received
                  Link heartbeat on station associated

Xirrus-MIFI-Arroyo(config-if)# ip global#
Do you want to save changes to flash (yes/no):

```

Figure 200. Configuring Radio Assurance Mode (Loopback Testing)



Appendices



Page is intentionally blank



Appendix A: 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 443.
- “Keyboard Shortcuts” on page 449.

Factory Default Settings

The following tables show the Wireless 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	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

Setting	Default Value
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

Setting	Default Value
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

Setting	Default Value
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	Yes
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	Disabled

External RADIUS (Global)

Setting	Default Value
Enabled	Yes
Primary Server	None
Primary Port	1812
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

Setting	Default Value
Primary Secret	null (no secret)
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

Setting	Default Value
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 B: 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 Wireless Array or your network infrastructure. Topics include:

- “General Hints and Tips” on page 451
- “Frequently Asked Questions” on page 452
- “Array Monitor and Radio Assurance Capabilities” on page 460
- “RADIUS Vendor Specific Attribute (VSA) for Xirrus” on page 463
- “Upgrading the Array via CLI” on page 464
- “Contact Information” on page 469

General Hints and Tips

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

- The Wireless 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 Wireless 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 you are deploying multiple units, the Array should be oriented so that the monitor **abgn2** 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 Wireless 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 Wireless 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 242](#).
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 Wireless Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
 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 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 Wireless 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 Wireless 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 Wireless 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 Wireless 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 Wireless 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 Wireless Array units?**
- A.** When deploying multiple Wireless 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 Wireless 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 Wireless 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 Wireless 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 IAP abgn2 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 274 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 313.

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 313). 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 313).

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 462), 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 462), 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 315](#)):

- **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 Attribute (VSA) for Xirrus

A RADIUS VSA is defined for Xirrus Arrays to control administrator privileges settings for user accounts. The RADIUS VSA is used by Arrays to define the following attribute for administrator accounts:

- **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 218.



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, FVR=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 XM2.3.0
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 XGM2.3.0
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 C: Notices

This appendix contains the following information:

- “Notices” on page 471
- “EU Directive 1999/5/EC Compliance Information” on page 475
- “Compliance Information (Non-EU)” on page 482
- “Safety Warnings” on page 483
- “Translated Safety Warnings” on page 484
- “Software License and Product Warranty Agreement” on page 485
- “Hardware Warranty Agreement” on page 491

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 B 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.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- 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.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to IEEE LAN devices.

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.

Cable Run 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.

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.*

UL Statement

Use only with listed ITE product.

Power Cord

If you will be using Xirrus equipment 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.

RF Radiation Hazard Warning

To ensure compliance with FCC and Industry Canada 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 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.

Installez l'appareil en veillant à conserver une distance d'au moins 25 cm entre les éléments rayonnants et les personnes. Cet avertissement de sécurité est conforme aux limites d'exposition définies par la norme CNR-102 relative aux fréquences radio.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is 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 undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes:

(1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution :

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

EU Directive 1999/5/EC Compliance Information

This section contains compliance information for the Xirrus Wireless Array family of products. 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]** Αυτό το εξοπλισμό είναι σε συμμόρφωση με τις ουσιώδεις 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 būtiskajām 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 apparaat 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 Wireless Array, 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 products.

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**
5250–5350*	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.ibpt.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 όη υπογράφει ενδοχώρα ποσση ζ νηου νοτ 5470–5725 MHz ε το ετάμνο ετάά δάδειά της EETT, ου ορηγεβράσ στερά ά ό σ φωνη γν η του ΓΕΕΘΑ. ερισσότερες λε τομ πρσιωστο 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 Wireless 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 Wireless Array family of products. 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 XR Series Wireless Array 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 XR Series Wireless Array or connect or disconnect cables during periods of lightning activity.
-  **Circuit Breaker Warning**
The XR Series Wireless Array 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 XR Wireless Array 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 XR Wireless Array et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.
-  **Disjoncteur**
L'unité XR Wireless Array 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 five years 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 identity 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 (Kμsec).

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. Wireless 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).

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 through 4

The Gigabit Ethernet interfaces on XR Series Arrays. XR-4000 Series Arrays have two gigabit interfaces, while XR-6000 Series and higher models have four gigabit interfaces. See also, [Gigabit Ethernet](#).

Gigabit Ethernet

A 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-supplied 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.

Wireless Array

A high capacity wireless 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 Wireless 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-supplied products that provides power over Gigabit Ethernet. See PoGE.



Index

Numerics

11n
 see IEEE 802.11n 35
 802.11a 3, 5, 274, 293
 802.11a/b/g 26
 802.11a/b/g/n 15
 802.11a/n 15, 63, 249
 802.11b 3, 5, 298
 802.11b/g 274, 298
 802.11b/g/n 15, 63, 249
 802.11e 16
 802.11g 3, 5, 298
 802.11i 5, 71, 161
 802.11n 5
 see IEEE 802.11n 35
 WMI page 304
 802.11p 16
 802.11q 16
 802.1x 5, 46, 56, 71, 161, 454

A

abg(n)
 nomenclature 2
 abg(n)2
 intrusion detection 331
 self-monitoring
 radio assurance (loopback mode) 314, 315
 Access Control List 208
 Access Control Lists 454
 access control lists (ACLs) 227, 262
 ACLs 46, 208, 454
 active IAPs
 per SSID 261
 Address Resolution Protocol
 window 109

Address Resolution Protocol (ARP)
 290
 Admin 454
 Admin ID 214
 admin ID
 authentication via RADIUS 218
 Admin Management 214
 admin privileges
 setting in admin RADIUS account
 218
 admin RADIUS account
 if using Console port 218
 admin RADIUS authentication 218
 administration 71, 161, 208
 Administrator Account 448
 Advanced Encryption Standard 46,
 454
 Advanced RF Analysis Manager
 see RAM 18
 Advanced RF Performance Manager
 see RPM 16
 Advanced RF Security Manager
 see RSM 17
 AeroScout
 see WiFi tag 188
 AES 5, 16, 46, 56, 71, 161, 446, 454
 allow traffic
 see filters 344
 Analysis Manager
 see RAM 18
 appearance
 WMI options 373
 WMI, changing 373
 approved
 setting rogues 120
 APs 56, 119, 240, 454
 rogues, blocking 331
 APs, rogue
 see rogue APs 313, 331
 ARP filtering 290

ARP table window 109
Array 28, 62, 63, 84, 161, 171
 connecting 62
 dismounting 62
 management 359
 mounting 62
 powering up 63
 securing 62
 Web Management Interface 84
ArrayOS
 upgrade 362
Arrays
 managing in clusters 352
associated users 28
assurance
 network server connectivity 112, 225
assurance (radio loopback testing) 313
assurance, station
 see station assurance 320
attack (DoS)
 see DoS attack 332
attack (impersonation)
 see impersonation attack 333
authentication 16
 of admin via RADIUS 218
authority
 certificate 212, 225
auto block
 rogue APs, settings 331
auto negotiate 171
auto-blocking
 rogue APs 331
auto-configuration 71, 280, 293, 298
 channel and cell size 313
automatic refresh
 setting interval 374
automatic update from remote server
 configuration files, boot image 363

B

backhaul
 see WDS 53
backup unit
 see standby mode 314
band association 249
beacon interval 280
Beacon World Mode 280
beam distribution 15
benefits 14
block
 rogue APs, settings 328
block (rogue APs)
 see auto block 331
blocking
 rogue APs 331
blocking rogue APs 313
boot 362
broadcast 291
 fast roaming 291
browser
 certificate error 212, 225
BSS 452
BSSID 119, 452
buttons 91

C

capacity
 of 802.11n 42
cascading style sheet
 sample for web page redirect 369
cdp 392
CDP (Cisco Discovery Protocol)
 settings 183
cdp CLI command 392
CDP neighbors 111
cell
 sharp cell 313
cell size 28, 274
 auto-configuration 313

- cell size configuration 313
- certificate
 - about 212, 225
 - authority 212, 225
 - error 212, 225
 - install Xirrus authority 225
 - X.509 212, 225
- channel
 - auto-configuration 313
 - configuration 313
 - list selection 313
- channels 28, 119, 274, 280, 293, 298
 - non-overlapping 15
- CHAP (Challenge-Handshake Authentication Protocol)
 - Admin RADIUS settings 219
 - web page redirect 258
- CHAP Challenge Handshake Authentication Protocol)
 - RADIUS ping 370
- character restrictions 93
- Chrome 24
- Cisco Discovery Protocol
 - see cdp 392
- Cisco Discovery Protocol (CDP) 183
- CLI 5, 56, 59, 66, 377
 - executing from WMI 371
 - using to upgrade software image 464
- CLI commands
 - see commands 392
- client
 - web page redirect 368
- cluster
 - CLI command 394
- clusters 352
 - defining 353
 - management 354
 - operating in cluster mode 355
- command
 - wifi-tag 425
- Command Line Interface 5, 52, 59, 63, 66, 377, 454
 - configuration commands 390
 - getting help 379
 - getting started 379
 - inputting commands 379
 - sample configuration tasks 426
 - SSH 377
 - top level commands 381
- command, utilities
 - ping, traceroute, RADIUS ping 369
- commands
 - acl 390
 - admin 391
 - cdp 392
 - clear 393
 - cluster 394
 - configure 382
 - contact-info 395
 - date-time 396
 - dhcp-server 397
 - dns 398
 - file 399
 - filter 402
 - group 394, 406
 - hostname 406
 - interface 407
 - load 408
 - location 408
 - management 409
 - more 410
 - netflow 411
 - no 412
 - quit 414
 - radius-server 414
 - reboot 415, 423
 - reset 415
 - restore 416
 - run-tests 417

- security 419
 - show 385
 - snmp 420
 - ssid 421
 - statistics 388
 - syslog 422
 - vlan 424
 - Community String 445
 - configuration 159, 454
 - express setup 161
 - reset to factory defaults 366
 - configuration changes
 - applying 92
 - configuration files
 - automatic update from remote server 363
 - download 364
 - update from local file 364
 - update from remote file 364
 - connection
 - tracking window 110
 - connectivity
 - servers, see network assurance 112, 225
 - Console port
 - login via 218
 - Contact Information 469
 - contact information 469
 - coverage 28, 59
 - extended 15
 - coverage patterns 5
 - critical messages 89
 - CTS/RTS 293, 298
- D**
- data rate 293, 298
 - data rates
 - increased by 802.11n 41
 - date/time restrictions
 - and interactions 268
 - default gateway 71, 171
 - default settings 443
 - Default Value 446
 - DHCP 445
 - defaults
 - reset configuration to factory defaults 366
 - Delivery Traffic Indication Message 280
 - denial of service
 - see DoS attack 332
 - deny traffic
 - see filters 344
 - deployment 26, 52, 56, 59, 454
 - case of 15
 - detection
 - intrusion 331
 - see DoS attack 332
 - see impersonation attack 333
 - see impersonation detection 332
 - see intrusion detection 332, 333
 - DHCP 28, 66, 71, 161, 171, 444
 - default settings 445
 - leases window 110
 - DHCP Server 184
 - diagnostics
 - log, create file 366
 - display
 - WMI options 373
 - DNS 71, 161, 181
 - DNS domain 181
 - DNS server 181
 - Domain Name System 181
 - DoS attack detection
 - settings 332
 - DTIM 280
 - DTIM period 280
 - duplex 171
 - dynamic VLAN
 - overridden by group 267

E

EAP 446, 454
 EAP-MDS 16
 EAP-PEAP 454
 EAP-TLS 16, 46, 454
 EAP-TTLS 16, 46, 454
 EDCF 280
 Encryption 446, 454
 encryption 16
 encryption method
 recommended (WPA2 with AES)
 210
 setting 211
 support of multiple methods 210
 encryption method (encryption mode)
 Open, WEP, WPA, WPA2, WPA-
 Both 209
 encryption standard
 AES, TKIP, both 210
 setting 211
 Enterprise 1, 3, 454
 WLAN 3
 Enterprise Class Management 5
 Enterprise Class Security 5
 ESS 452
 ESSID 452
 Ethernet 59, 62, 63, 66, 71, 161
 event log
 IDS (intrusion detection) 157
 see system log 150, 156
 event messages 89
 Express Setup 62, 71, 161
 express setup 71, 161
 Extended Service Set 452
 Extensible Authentication Protocol 454
 external RADIUS server 802.1x 25

F

factory default settings 443
 factory defaults 444, 445, 446, 448

DHCP 445
 reset configuration to 364
 factory.conf 364
 fail-over
 standby mode 314
 failover 42, 56
 FAQs 452
 Fast Ethernet 59, 66, 161, 171, 443
 fast roaming 15, 106, 291
 about 273
 and VLANs 273
 features 14, 52, 171, 187, 190, 280, 454
 and license key 363
 feedback 91
 filter list 345
 filter name 347
 filtering
 IPv6 291
 filters 344, 345, 347
 stateful filtering, disabling 346
 statistics 147
 Firefox 24
 firewall 344
 and port usage 48
 stateful filtering, disabling 346
 fragmentation threshold 293, 298
 frequently asked questions 452
 FTP 454
 FTP server 25

G

General Hints 451
 getting started
 express setup 161
 Gigabit 59, 66, 71, 161, 171, 443
 global settings 280, 293, 298
 glossary of terms 493
 Google Chrome 24
 Group
 management 266

- group 264
 - CLI command 394, 406
 - VLAN overrides dynamic VLAN 267
- group limits and interactions 268
- Group Rekey 446
- guard interval
 - short, for IEEE 802.11n 40
- GUI
 - see WMI 373
- H**
- help
 - button, bottom of page 91
 - button, left frame 88
- Help button 84
- help button 91
- host name 71, 84, 161, 181
- hs.css 369
- HTTPS
 - certificate, see certificate 225
- HTTPS port
 - web page redirect 255, 259, 260
- HyperTerminal 24, 59
- I**
- IAP 28, 63, 71, 161, 274, 293, 298, 334
 - active SSIDs 261
 - fast roaming 273
 - Intrusion Detection (IDS/IPS) 328
 - naming 2
 - settings 274
- IAP LED 63, 334
- IAP LED settings 334
- IAPs
 - auto block rogues 331
 - intrusion detection 331
- IDS
 - see Intrusion Detection 328
- IDS event log
 - viewing window 157
- IEEE 3, 71, 161
- IEEE 802.11n
 - capacity, increased 42
 - deployment considerations 35
 - guard interval, short 40
 - improved MAC throughput 40
 - increased data rates 41
 - MIMO 36
 - multiple data streams 38
 - spatial multiplexing 38
 - WMI page 304
- IEEE 802.1Q 457
- image
 - upgrade software image 362
- impersonation attack detection
 - settings 333
- implementing Voice over Wi-Fi 26, 199, 244
- installation 23, 57, 62, 441
 - installing the MCAP-3616 59
 - mounting the unit 62
 - requirements 23
 - workflow 57
- installation workflow 57
- interfaces 161
 - Web 83
- internal login page
 - web page redirect 256
 - web page redirect, customize 258
- internal splash page
 - web page redirect 257
 - web page redirect, customize 258
- Internet Explorer 24
- interval
 - automatic WMI refresh 374
- intrusion detection 119, 331
 - and auto block settings 331
 - configuration 313
 - setting as approved or known 120

- intrusion detection (IDS)
 - viewing event log 157
- Intrusion Detection (IDS/IPS) 328
- IP Address 28, 71, 84, 92, 119, 161, 171, 181, 190, 194, 359, 444
- IP Subnet Mask 71
- IPS
 - see Intrusion Detection 328
- IPv6
 - filtering 291
- K**
- key
 - upgrade 363
- key features 14
- Keyboard Shortcuts 449
- keyboard shortcuts 449
- known
 - setting rogues 120
- L**
- lastboot.conf 364
- Layer 3
 - fast roaming 273
- lease 444
- Lease Time 444
- leases, DHCP
 - viewing 110
- LEDs 63
 - sequence 63
 - settings 334
- license Key
 - upgrading 363
- limits
 - group 268
 - interactions 268
 - station 268
 - traffic 268
- list, access control
 - see access control list 227, 262
- list, MAC access
 - see access control list 227
- list, SSID access
 - see access control list 262
- location information 71, 84, 161
- log
 - diagnostics, create file 366
- log messages
 - counters 89
- log, IDS(intrusion detection)
 - viewing window 157
- log, system (event)
 - viewing window 150, 156
- logging in 66, 92
- Login 92
- login
 - via Console port 218
- login page
 - web page redirect 256, 368
 - web page redirect, customize 258
- logout 376
- long retry limit 280
- loopback
 - see radio assurance 438
- loopback testing
 - radio assurance mode 313
- M**
- MAC 46, 66, 452, 454
- MAC Access Control Lists 46
- MAC Access List 227
- MAC address 227, 452, 454
- MAC throughput
 - improved by IEEE 802.11n 40
- Management 448, 454
- management 95, 159, 359
 - Array clusters 352
 - of Arrays 359
 - Web Management Interface (WMI) 83

- maximum lease 444
 - Maximum Lease Time 444
 - Megabit 71
 - menu behavior
 - WMI 375
 - Message Integrity Check 454
 - messages
 - syslog counters 89
 - MIC 16, 454
 - MIMO (Multiple-In Multiple-Out) 36
 - mode
 - cluster operating mode 355
 - monitoring
 - intrusion detection 119
 - see intrusion detection 331
 - mounting 62
 - mounting plate 62
 - mounting the unit 62
 - MTU 171
 - size 171
 - multiple data streams 38
- N**
- NAT
 - table - see connection tracking 110
 - neighbors, CDP 111
 - Netflow 187
 - netflow
 - CLI command 411
 - network
 - interfaces 169
 - settings 171
 - network assurance 112, 225
 - network connections 59, 92, 454
 - network installation 23, 441
 - network interface ports 66
 - network interfaces 171, 443
 - network status
 - ARP table window 109
 - connection
 - tracking window 110
 - routing table window 109
 - viewing leases 110
 - Network Time Protocol 71, 161, 185
 - network tools
 - ping, traceroute, RADIUS ping 369
 - nomenclature 2
 - non-overlapping channels 15
 - NTP 71, 161, 185, 444
 - NTP Server 185
- O**
- Open (encryption method) 210
 - optimization, VLAN 291
 - options
 - WMI 373
 - overview 5
- P**
- page loading
 - WMI 375
 - PAP (Password Authentication Protocol)
 - Admin RADIUS settings 219
 - RADIUS ping 370
 - web page redirect 258
 - passphrase 46, 71, 161
 - Password 448, 454
 - password 92
 - PEAP 16, 340
 - performance 14
 - Performance Manager
 - see RPM 16
 - Ping 359
 - ping 369
 - planning 42, 45, 46, 52
 - failover 42
 - network management 52
 - port failover 42
 - power 45

- security 46
- switch failover 42
- WDS 53
- PoGE 23
 - see Power over Gigabit Ethernet 12
- PoGE Power Injectors 1
- port failover 42
- port requirements 48
- power outlet 23
- Power over Gigabit Ethernet 2, 23, 45, 59
- Power over Gigabit Ethernet (PoGE) 12
- power planning 45
- pre-shared key 46, 56, 454
- Print button 84
- print button 91
- probe
 - see Netflow 187
- product installation 23, 441
- product overview 5
- product specifications 22
- PSK 56, 446
- PuTTY 23, 52, 71, 161, 454
- PuTTY 24

Q

- QoS 16, 249, 446, 452, 500
 - conflicting values 247
 - levels defined 250, 267
 - priority 249
 - SSID 244, 250
 - about setting QoS 453
 - default QoS 446
 - user group 267
- quality
 - of user experience 320
- Quality of Service 16
 - see QoS 250, 267
- quick reference guide 443
- quick start

- express setup 161

R

- radio
 - assurance (self-test) 314, 315
 - radio assurance (loopback testing) 313
 - radio assurance (loopback) mode 314, 315
 - radio distribution 14
 - radios
 - naming 2
- RADIUS 5, 23, 46, 56, 208, 227, 262, 444, 454
 - admin authentication 218
 - setting admin privileges 218
 - setting user VSAs 234
 - Vendor Specific Attributes (VSAs) 463
- RADIUS ping
 - CHAP (Challenge Handshake Authentication Protocol) 370
 - PAP (Password Authentication Protocol) 370
- RADIUS Ping command 369
- RADIUS Server 444
- RADIUS server 25
- RADIUS settings
 - web page redirect 258
- RAM (RF Analysis Manager) 18
- reauthentication 280
- reboot 362
- redirect (WPR) 368
- refresh interval
 - WMI 374
- remote boot image
 - automatic update from remote TFTP server 363
- remote configuration
 - automatic update from remote server 363

- remote TFTP server
 - automatic update of boot image, configuration 363
 - Reset 359, 444
 - reset configuration
 - to factory defaults 366
 - restore command 416
 - restrictions
 - date/time 268
 - stations 268
 - traffic 268
 - RF
 - intrusion detection 313
 - spectrum management 313
 - RF Analysis Manager
 - see RAM 18
 - RF configuration 313
 - RF management
 - see channel 313
 - RF Performance Manager
 - see RPM 16
 - RF resilience 313
 - RF Security Manager
 - see RSM 17
 - roaming 15, 106, 291
 - see fast roaming 273
 - Rogue AP 5, 52, 119, 240, 454
 - rogue AP
 - blocking 331
 - settings for blocking 328
 - Rogue AP List 119
 - rogue APs
 - auto block settings 331
 - blocking 313
 - Rogue Control List 240
 - rogue detection 15
 - rogues
 - setting as known or approved 120
 - root command prompt 381
 - route
 - trace route utility 369
 - routing table window 109
 - RPM (RF Performance Manager) 16
 - RSM (RF Security Manager) 17
 - RSSI 119
 - RTS 293, 298
 - RTS threshold 293, 298
- ## S
- Safari 24
 - sample Perl and CSS files for 368
 - save
 - with reboot 362
 - Save button 84
 - saved.conf 364
 - scalability 3
 - schedule
 - auto channel configuration 313
 - Secondary Port 444
 - Secondary Server 444
 - secret 444
 - Secure Shell 24
 - secure Shell 23
 - security 5, 16, 208, 452, 454
 - certificate, see certificate 225
 - Security Manager
 - see RSM 17
 - see group 264
 - self-monitoring 331
 - radio assurance 438
 - radio assurance options 314, 315
 - self-test
 - radio assurance mode 314, 315
 - serial port 24, 66, 454
 - server, VTun
 - see VTun 203
 - servers
 - connectivity, see network assurance 112, 225
 - Service Set Identifier 71

- Services 184, 452
- servicing the unit 441
- settings 161
- setup, express 161
- sharp cell 313
 - setting in WMI 317
- short retry limit 280
- signal processing
 - MIMO 36
- skin
 - changing WMI appearance 373
- SNMP 5, 13, 71, 161, 171, 184, 194, 445
 - required for XMS 194, 195
- software
 - upgrade license key 363
- software image
 - upgrading via CLI 464
- Software Upgrade 359
- software upgrade 362
- spatial multiplexing 38
- specifications 22
- spectrum (RF) management 313
- speed 3, 66, 171
 - 11 Mbps 3
 - 54 Mbps 3
- splash page
 - web page redirect 257, 368
 - web page redirect, customize 258
- SSH 23, 24, 52, 71, 161, 171, 209, 448, 454
- SSH-2 209
- SSID 5, 71, 84, 119, 161, 240, 249, 446, 452, 457
 - about usage 452
 - active IAPs 261
 - QoS 244, 250
 - about using 453
 - QoS, about usage 452
 - web page redirect settings 253
 - web page redirect settings, about 255, 259, 260
- SSID Access List 262
- SSID address 262
- SSID Management 249, 446, 452
- standby mode 314
- stateful filtering
 - disabling 346
- static IP 71, 161, 171
- station
 - assurance 320
- station assurance 320
- station timeout period 280
- Stations 452
- stations
 - limits and interactions 268
 - rogues 120
 - statistics 148
 - statistics per station 149
- statistics 161
 - filters 147
 - netflow 187
 - per-station 149
 - stations 148
 - WDS 145
- status bar 84, 91
- style
 - WMI appearance 373
- submitting comments 91
- subnet 23, 42, 71, 171
- switch failover 42
- synchronize 71, 161, 185
- Syslog 71, 84, 161, 184, 190, 444
 - time-stamping 71
- syslog messages
 - counters 89
- Syslog reporting 190
- Syslog Server 190
- system commands
 - ping, trace route, RADIUS ping 369

System Configuration Reset 359

System Log 190

system log

viewing window 150, 156

System Reboot 359

System Tools 359

system tools 360

T

tag, WiFi 188

T-bar 62

T-bar clips 62

TCP

port requirements 48

technical support

contact information 469

frequently asked questions 452

Telnet 209, 448, 454

Temporal Key Integrity Protocol 454

TFTP server

automatic update of boot image,
configuration 363

Time Out 444

time zone 71, 161, 185

timeout 280, 359

Tips 451

TKIP 16, 46, 56, 71, 161, 446, 454

TKIP encryption

and XN Arrays 231

tool

ping, trace route, RADIUS ping
369

Tools 359, 454

tools, network 369

tools, system 360

trace route utility 369

traffic

filtering 344

limits and interactions 268

transmit power 28

Trap Host 445

trap port 194, 445

tunneled

fast roaming 291

Tunnels 204

tunnels

see VTun 199, 203

U

UDP

port requirements 48

Unit 62

attaching 62

mounting 62

unknown

setting rogues 120

upgrade

license key 363

software image 362

upgrading software image

via CLI 464

user accounts

setting RADIUS VSAs 234

user group 264

QoS 267

user group limits and interactions 268

user interface 83

utilities

ping, trace route, RADIUS ping
369

utility buttons 91

V

Vendor Specific Attributes (VSAs)

RADIUS, for Xirrus 463

virtual tunnels

see VTun 203

VLAN 5, 56, 249, 446, 452, 457

broadcast optimization 291

dynamic

- overridden by group 267
 - group (vs. dynamic VLAN) 267
 - vlan
 - CLI command 424
 - VLAN ID 249
 - VLANs 199
 - and fast roaming 273
 - voice
 - fast roaming 273
 - implementing on Array 26, 199, 244
 - Voice-over IP 298
 - VoIP 298
 - VoWLAN 16
 - VPN 71, 161, 454
 - VTS
 - Virtual Tunnel Server 199, 203
 - VTun
 - specifying tunnel server 199, 203
 - understanding 199
- W**
- wall thickness considerations 26
 - warning messages 89
 - WDS 338, 340
 - about 53
 - long distance 278, 339
 - planning 53
 - statistics 145
 - timeouts 278, 339
 - WDS Client Links 340
 - Web interface
 - structure and navigation 88
 - web interface 83
 - Web Management Interface 52, 62, 63, 66, 92, 452
 - Web Management Interface (WMI) 83
 - web page redirect 368
 - also called WPR 368
 - CHAP (Challenge-Handshake Au-
thentication Protocol) 258
 - customize internal login/splash
page 258
 - HTTPS port 255, 259, 260
 - install files for 368
 - internal login page 256
 - internal splash page 257
 - PAP, CHAP 258
 - RADIUS settings 258
 - remove files for 369
 - sample WPR files 369
 - SSID settings 253
 - SSID settings, about 255, 259, 260
 - WEP 16, 46, 71, 161, 208, 249, 446, 454
 - WEP (Wired Equivalent Privacy)
 - encryption method 210
 - WEP encryption
 - and XN Arrays 232
 - Wi-Fi Protected Access 5, 46, 71, 161, 454
 - WiFi tag 188
 - wifi-tag
 - CLI command 425
 - window loading
 - WMI 375
 - Wired Equivalent Privacy 71, 454
 - Wireless Distribution System 338
 - wireless LAN 3
 - wireless security 161
 - WLAN 161
 - WMI 5, 52, 56, 66, 83, 274
 - appearance options 373
 - appearance, changing 373
 - certificate error 212, 225
 - executing CLI commands 371
 - menu behavior 375
 - options 373
 - page loading 375
 - refresh interval 374
 - workflow 57

- WPA 5, 56, 71, 161, 208, 249, 446, 454
- WPA (Wi-Fi Protected Access) and WPA2
 - encryption method 210
- WPA2 5
- WPR
 - see web page redirect 368
- wpr.pl 368, 369
- X**
- X.509
 - certificate 212, 225
- Xirrus
 - certificate authority 225
- Xirrus Advanced RF Analysis Manager
 - see RAM 18
- Xirrus Advanced RF Performance Manager
 - see RPM 16
- Xirrus Advanced RF Security Manager
 - see RSM 17
- Xirrus Management System 5, 13, 15, 23, 25, 52, 454
 - SNMP required 194, 195
- Xirrus Management System (XMS) 1
- Xirrus PoGE Power Injectors 1
- Xirrus Power over Gigabit Ethernet 23
- Xirrus Roaming Protocol 15, 106, 291
- XMS 5, 13, 15, 25
 - port requirements 48
 - setting IP address of 194
 - SNMP required 194, 195
- XN Array
 - management 159, 359
- XN Arrays
 - see also IEEE 802.11n 35
- XN12 1, 5
- XN16 1, 5
 - management 359
- XN4 1, 5
- XN8 1, 5
- XP PoGE Power Injectors 1
- XP1, XP8
 - see Power over Gigabit Ethernet 12
- XPS 23
- XRP 15, 106, 291
- xs_current.conf 364
- xs_diagnostic.log 367



1.800.947.7871 Toll Free in the US
+1.805.262.1600 Sales
+1.805.262.1601 Fax
2101 Corporate Center Drive
Thousand Oaks, CA 91320, USA

To learn more visit
xirrus.com or
email info@xirrus.com