

- **Description:** The description (if any) that you set for this IAP.

### Array Information

This is a status only window that shows you the current firmware versions utilized by the Array, the serial numbers assigned to each module, and MAC addresses.

You cannot make [configuration changes](#) in this window, but if you are experiencing issues with network services, you may want to print the content of this window for your records.

XN8 Wi-Fi Array				
Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 0 hours, 48 minutes	
Array	Hardware Configuration			
Summary	Model	XN8, 1.0GB (1.0GHz)		
Information	Component	Part Number	Serial Number	Date
Configuration	Array	180-0036-001	XN0839081AD18	2008-Sep-23 21:08
Admin History	Controller	100-0030-012 G1	0000017991	2008-Sep-16 0:50
Network	IAP Module 1	100-0091-002 B2	0000022947	2008-Sep-16 11:00
RF Monitor	IAP Module 2	100-0091-002 B2	0000022933	2008-Sep-16 11:14
Stations	IAP Module 3	100-0091-002 B2	0000022932	2008-Sep-16 12:37
Statistics	IAP Module 4	100-0091-002 B2	0000023089	2008-Sep-23 9:57
System Log	FPGA Status	Boot Version	SW Version	
Configuration	Switching Engine	2000-00.017	2000-00.018	
Express Setup	Queue Processing	2002-00.033	2002-00.034	
Network	InterIAP Arbitrator	2003-00.010	2003-00.011	
Services	Interface	MAC Address(es)		
VLANs	IAPs	00:0f:7d:0b:b3:80-0b:b3:f		
Security	Ethernet 0	00:0f:7d:00:46:47		
SSIDs	Gigabit 1	00:0f:7d:00:46:48		
Groups	Gigabit 2	00:0f:7d:00:46:49		
IAPs	Software Configuration			
WDS	Component	Version		
Filters	SCD Firmware	2.19 (Jul 24 2008), Build: 3124		
Tools	Boot Loader	1.0.0 (Aug 4 2008), Build: 3071		
System Tools	IAP Driver	11N Beta - Version 0.90		
CLI	System Software	4.0.2 (Dec 03 2008), Build: 1072		
Logout	License Key	12W/WN-52NWE-JJHR-Q9C01		
Log Messages	Time This Boot	Fri 2008-Dec-05 22:05:08 GMT		
Critical 0	Time Last Boot	Wed 2008-Dec-03 19:19:45 GMT		
Warning 0				
Information 500				

Figure 68. Array Information

## Array Configuration

This is a status only window that allows you to display the configuration settings assigned to the Array, based on the following filter options:

- **Running**—displays the current configuration (the one running now).
- **Saved**—displays the saved configuration from this session.
- **Lastboot**—displays the configuration as it was after the last reboot.
- **Factory**—displays the configuration established at the factory.

The screenshot shows the XIRRUS XNB Wi-Fi Array configuration interface. The top header displays 'XNB Wi-Fi Array' and the XIRRUS logo. Below the header, the status bar shows 'Name: SS-XNB (10.100.47.186)', 'Location: SS Area', and 'Uptime: 0 days, 2 hours, 2 minutes'. The main content area is divided into a left sidebar with navigation options and a main configuration display area. The 'Configuration' section is selected, and the 'Show Configuration' output is displayed. The output shows the current configuration for the array, including hostname, location, contact information, and hardware details.

```

!
configure
!
description
hostname SS-XNB
location "SS Area"
exit
!
contact-info
name "J Smith"
phone "805-555-1212"
email "jsw@xyzcorp.com"
exit
!
array-info
! hardware-configuration
! =====
! model: XNB, 1.0GB (1.0GHz)
!
! component      part number      serial number     date
! -----
! array          180-0036-001     XM0839081AD18    2008-Sep-23 21:08
! controller    100-0030-012.G1  0000017991       2008-Sep-16 0:50
! iap module 1  100-0091-002.B2  0000022947       2008-Sep-16 11:00
! iap module 2  100-0091-002.B2  0000022933       2008-Sep-16 11:14
! iap module 3  100-0091-002.B2  0000022932       2008-Sep-16 12:37
! iap module 4  100-0091-002.B2  0000023089       2008-Sep-23 9:57
!
! #pga status      boot version      s/w version
! -----
    
```

Figure 69. Show Configuration

If you want to see just the differences between the Running, Saved, Lastboot, and Factory configurations, you can do this by choosing a configuration option from the **Select Config** pull-down menu then selecting an alternative configuration option from the **Select Diff** pull-down menu.

To also include the default configuration settings in the output, choose your configuration then click in the **Include Defaults** check box. If **Include Defaults** is disabled, then only the changes from the default configuration are shown.

### Admin History

It is useful to know who else is currently logged in to an array while you're configuring it. It's also nice to see who has logged in since the array booted. This status-only window shows you all administrator logins to the Array that have occurred since the last reboot. To determine who is currently logged in, check which entries say **active** in the **Logout Time** column.

Status		Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area		Uptime: 4 days, 0 hours, 58 minutes			
Array		User	IP Address	Interface	Via	Login Time	Logout Time	Session Time D:MM
Summary Information		admin	10.100.21.55	WMI	https	Dec-09 12:59	active	0:02:05
Configuration		admin	10.100.21.55	WMI	https	Dec-09 11:54	active	0:03:10
Admin History		admin	10.100.21.55	WMI	https	Dec-09 10:16	active	0:04:48
Network		admin	10.100.21.55	WMI	https	Dec-08 10:16	Dec-09 10:16	
RF Monitor		admin	10.100.21.55	WMI	https	Dec-05 14:41	Dec-08 10:16	
Stations		admin	10.100.21.55	WMI	https	Dec-05 14:12	active	4:00:52
Statistics								
System Log								
Configuration								
Express Setup								
Network								
Services								
VLANs								

Figure 70. Admin Login History

### Network Status Windows

The following Network Status windows are available:

- **Network Map**—displays information about this Array and neighboring Arrays that have been detected.
- **Spanning Tree Status**—displays the spanning tree status of network links on this Array.
- **Routing Table**—displays information about routing on this Array.
- **ARP Table**—displays information about Address Resolution Protocol on this Array.
- **DHCP Leases**—displays information about IP addresses (leases) that the Array has allocated to client stations.
- **Connection Tracking/NAT**—lists connections that have been established for client stations.

- **CDP Neighbors**—lists neighboring network devices using Cisco Discovery Protocol.

## Network Map

This window offers detailed information about this Array and all neighboring Arrays, including how the Arrays have been set up within your network.

Status		Name: SS-XN8 [ 10.100.47.106 ]		Location: SS Area		Uptime: 0 days, 0 hours, 1 minute					
Array	Array Name	IP Address	Location	Array OS	IAP	Up	SSID	On	In Range	Fast Roam	Uptime D:H:M
Network	SS-XN8	10.100.47.106	SS Area	XS-4.0.2-1075	8	2	2	2	yes	yes	0:00:01
Network Map	XS0837081AAEE	10.100.49.137		XS-3.5-0694	8	1	16	16			1:21:24
Spanning Tree Status	XS0837081AA05	10.100.49.124		XS-3.5-0694	8	1	16	16			1:21:37
Routing Table	XS4	10.100.48.17		XS-4.0.2-1075	4	4	1	1			0:05:48
ARP Table	XS16170819B92	10.100.48.11		XS-4.0.2-1075	16	16	1	1			0:05:51
DHCP Leases	XS0838081AC21	10.100.49.106		XS-3.5-0694	8	1	16	16			1:21:24
Connection Tracking	XS1444081B4D8	10.100.49.155		XS-3.5-0694	4	1	1	1			1:21:34
CDP Neighbors	XS1370606002B1	10.100.48.14		XS-4.0.2-1075	8	8	1	1			0:05:51
RF Monitor	XN0850081BA86	10.100.49.181		XS-4.0.2-1074	8	1	1	1			0:22:51
Stations	XN0850081BA88	10.100.49.191		XS-4.0.2-1074	8	1	1	1			1:23:52
Statistics	XN0849081BA9F	10.100.49.151		XS-4.0.2-1075	8	1	1	1			0:00:11
System Log	XN0850081BA73	10.100.49.182		XS-4.0.2-1074	8	1	1	1			2:00:09
Configuration	XS0838081AC42	10.100.49.144		XS-3.5-0694	8	1	16	16			1:21:38
Express Setup	X1355207104ED	10.100.48.19		XS-4.0.2-1075	4	4	1	1			0:05:47
Network											
Services											

Figure 71. Network Map

The Network Map has a number of options at the bottom of the page that allow you to customize your output by selecting from a variety of information that may be displayed. You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the Array to refresh this window automatically.

## Content of the Network Map Window

By default, the network map shows the following status information for each Array:

- **Array Name:** The host name assigned to the Array. To establish the host name, go to “Express Setup” on page 176.
- **Location:** The location assigned to the Array. To establish the location information, go to “Express Setup” on page 176.
- **Array OS:** The software version running on the Array.

- **IP Address:** The Array's IP address. If DHCP is enabled, the Array's IP address is assigned by the DHCP server. If DHCP is disabled, you must assign a static IP address. To enable DHCP or to assign a static IP address for the Array, go to ["Express Setup" on page 176](#).
- **IAP:** The number of IAPs on the Array.
- **IAPs Up:** Informs you how many IAPs are currently up and running. To enable or disable all IAPs, go to ["Express Setup" on page 176](#). To enable or disable individual IAPs, go to ["IAP Settings" on page 255](#).
- **SSIDs:** Informs you how many SSIDs have been assigned for the Array. To assign an SSID, go to ["SSID Management" on page 240](#).
- **SSID On:** Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to ["SSID Management" on page 240](#).
- **In Range:** Informs you whether the Array is within wireless range of another Wi-Fi Array.
- **Fast Roam:** Informs you whether or not the Xirrus fast roaming feature is enabled. This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at both Layer 2 and Layer 3. To enable or disable fast roaming, go to ["Global Settings \(IAP\)" on page 260](#).
- **Uptime (D:H:M):** Informs you how long the Array has been up and running (in Days, Hours and Minutes).

To see additional information, select from the following checkboxes at the bottom of the page. This will show the columns described below.

#### *Hardware*

- **Model:** The model number of each Array (XN16, XS-4, etc.), plus the amount of RAM memory and the speed of the processor.
- **Serial:** Displays the serial number of each Array.

#### *License*

- **License Key:** The license key of each Array.
- **Licensed Features:** Lists the optional features enabled by the key, if any.

### *Software (enabled by default)*

- Enable/disable display of the Array OS column.

### *Firmware*

- **Boot Loader:** The software version number of the boot loader on each Array.
- **SCD Firmware:** The software version number of the SCD firmware on each Array.

### *IAP Info (enabled by default)*

- Enable/disable display of the IAP/Up columns.

### *Stations*

- **Stations:** Tells you how many stations are currently associated to each Array. To deauthenticate a station, go to [“Stations” on page 151](#).

The columns to the right (**H**, **D**, **W**, and **M**) show the highest number of stations that have been associated over various periods of time: the previous hour, day, week, and month.

### *Default*

- Sets the columns displayed to the default settings. By default, only Software and IAP Info are selected.

## **Spanning Tree Status**

Multiple active paths between stations can cause loops in the network. If a loop exists in the network topology, the potential exists for the duplication of messages. The spanning tree protocol is a link management protocol that provides path redundancy while preventing undesirable loops. For a wireless network to function properly, only one active path can exist between two stations.

To facilitate path redundancy, the spanning tree protocol defines a tree that spans all stations in the network and forces certain redundant data paths into a standby (blocked) state. If one segment in the spanning tree becomes unreachable, the spanning tree algorithm reconfigures the network topology and reestablishes the

link by activating the standby path. The spanning tree function is transparent to client stations.

Name: SS.XN8 ( 10.100.47.106 )		Location: SS Area		Uptime: 4 days, 1 hour, 38 minutes							
				WDS Client Links				WDS Host Links			
VLAN Name	Number	Gigabit	Gigabit2	1	2	3	4	1	2	3	4
(none)	-	forwarding	forwarding								
VoIP	12	forwarding	forwarding								
Finance	5	forwarding	forwarding								

Figure 72. Spanning Tree Status

This window shows the spanning tree status (forwarding or blocked) for path segments that terminate on the gigabit ports and WDS links of this Array. You may sort the rows based on the **VLAN Name** or **Number** columns by clicking the column header. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the Array to refresh this window automatically.

*See Also*

- Network
- Network Interfaces
- Network Status Windows
- VLANs
- WDS

## Routing Table

This status-only window lists the entries in the Array's routing table. The table provides the Array with instructions for sending each packet to its next hop on its route across the network.

XN8 Wi-Fi Array					
Status		Name: SS-XN8 ( 10.100.47.106 )		Location: SS Area	Uptime: 4 days, 1 hour, 42 minutes
Array	Destination	Mask	Gateway	Interface	
Network	255.255.255.255	255.255.255.255	0.0.0.0	eth0	
Network Map	10.100.47.0	255.255.255.0	0.0.0.0	gig1/2	
Spanning Tree Status	10.100.47.0	255.255.255.0	0.0.0.0	eth0	
Routing Table	10.10.10.0	255.255.255.0	0.0.0.0	vlan12	
ARP Table	0.0.0.0	0.0.0.0	10.100.47.1	gig1/2	
DHCP Leases					<input type="checkbox"/> Auto Refresh
Connection Tracking					Refresh
CDP Neighbors					

Figure 73. Routing Table

### See Also

#### VLANs

#### Configuring VLANs on an Open SSID

## ARP Table

This status-only window lists the entries in the Array's ARP table. For a device with a given IP address, this table lists the device's MAC address. It also shows the Array interface through which this device may be reached. The table typically includes devices that are on the same local area network segment as the Array.

XN8 Wi-Fi Array					
Status		Name: SS-XN8 ( 10.100.47.106 )		Location: SS Area	Uptime: 4 days, 1 hour, 42 minutes
Array	IP Address	MAC Address	Interface		
Network	10.100.47.1	00:10:DB:FF:20:A0	gig1/2		
Network Map	10.100.47.10	00:0F:7D:00:45:FA	gig1/2		
Spanning Tree Status	10.100.47.21	00:0F:7D:00:43:89	gig1/2		
Routing Table	10.100.47.14	00:0F:7D:00:34:17	gig1/2		
ARP Table					<input type="checkbox"/> Auto Refresh
DHCP Leases					Refresh
Connection Tracking					
CDP Neighbors					

Figure 74. ARP Table



*See Also*

Routing Table

ARP Filtering

### DHCP Leases

This status-only window lists the IP addresses (leases) that the Array has allocated to client stations. For each, it shows the IP address assigned from one of the defined DHCP pools, and the MAC address and host name of the client station. The start and end time of the lease show how long the allocation is valid. The same IP address is normally renewed at the expiration of the current lease.

XN8 Wi-Fi Array						
Status	Name: SS-XN8 [ 10.100.47.100 ]		Location: SS Area		Uptime: 4 days, 1 hour, 46 minutes	
Array	IP Address	MAC Address	Start Time	End Time	Time Left	Host Name
Network	192.168.1.254	00:21:00:5e:ab:8b	Dec-09 15:50:11	Dec-09 15:55:11	0 days 0:03:20	Shelly-PC

Figure 75. DHCP Leases

*See Also*

DHCP Server

## Connection Tracking/NAT

This status-only window lists the session connections that have been created on behalf of clients. This table may also be used to view information about current NAT sessions.

XNB Wi-Fi Array

Status Name: SS-XNB (10.100.47.186) Location: SS Area Uptime: 4 days, 1 hour, 49 minutes

		Outbound Traffic							Return Traffic						
type	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	Use
Network Map															
Spanning Tree Status	udp	192.168.1.254	224.0.0.252	54994	5355	1	51	Unreplied	224.0.0.252	192.168.1.254	5355	54994	0	0	1
Routing Table	udp	192.168.1.254	224.0.0.252	59697	5355	1	55	Unreplied	224.0.0.252	192.168.1.254	5355	59697	0	0	1
ARP Table	udp	10.100.47.14	255.255.255.255	32770	22610	1	95	Unreplied	255.255.255.255	10.100.47.14	22610	32770	0	0	1
DHCP Leases	udp	10.100.49.143	10.100.47.186	32769	22610	2	306	Unreplied	10.100.47.186	10.100.49.143	22610	32769	0	0	1
Connection Tracking	udp	10.100.47.186	10.100.23.58	37848	22610	1	157	Unreplied	10.100.23.58	10.100.47.186	22610	37848	0	0	1
CDP Neighbors	udp	10.100.49.109	10.100.47.186	32771	22610	2	306	Unreplied	10.100.47.186	10.100.49.109	22610	32771	0	0	1
RF Monitor															

Figure 76. Connection Tracking

Click the **Show Netbios** checkbox at the bottom of the page to display NetBIOS name information for the source and destination location of the connection. The Netbios columns will replace traffic statistics columns.

You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the Array to refresh this window automatically.

*See Also*  
Filters

### CDP Neighbors

This status-only window lists devices on the Array’s network that support the Cisco Discovery Protocol (CDP). The Array performs discovery on the network on an ongoing basis. This list shows the devices that have been discovered—Cisco devices and other devices on the network that have CDP running. For each, it shows the device’s host name, IP address, manufacturer and model name, the device interface that is connected to the network (i.e., the port that was discovered), and the network capabilities of the device (switch, router, supported protocols, etc.).

The screenshot shows the 'CDP Neighbors' section of the XNB Wi-Fi Array interface. The table lists discovered devices with columns for Hostname, IP Address, Model, Interface, Native VLAN, Capabilities, and Software. The interface includes a sidebar with navigation options like 'Array', 'Network', 'RF Monitor', 'Statistics', and 'Configuration'. The table data is as follows:

Status		Name: SS_XNB (10.100.47.186)		Location: SS Area		Uptime: 0 days, 1 hour, 29 minutes	
Hostname	IP Address	Model	Interface	Native VLAN	Capabilities	Software	
SS-XNB	10.100.47.186	Ximus XNB, 1.0GB (1.0GHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 4.0.2 (Dec 18 2008), Build: 1075	
adrians-3900	10.100.47.18	Ximus XS-3900, 612MB (825MHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 3.5 (Nov 26 2008), Build: 0691	
BriansXS	10.100.47.27	Ximus XS8, 1.0GB (1.0GHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 3.5 (Dec 18 2008), Build: 0695	
XS16	10.100.47.21	Ximus XS16, 612MB (825MHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 3.5 (Dec 18 2008), Build: 0695	
Bruces-Array	10.100.47.32	Ximus XS-3900, 512MB (825MHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 3.5 (Nov 07 2008), Build: 0690	
Bruces-11n-Array	10.100.47.34	Ximus XNB, 1.0GB (1.0GHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 4.0.2 (Nov 06 2008), Build: 1070	
XS4	10.100.47.14	Ximus XS4, 512MB (825MHz)	Gig1	none	L2SW[switch]	Ximus ArrayOS Version 3.4 (Jun 03 2008), Build: 0632	
BrianXN	10.100.47.10	Ximus XNB, 1.0GB (1.0GHz)	Gig1/2	none	L2SW[switch]	Ximus ArrayOS Version 4.0.2 (Dec 15 2008), Build: 1074	

Figure 77. CDP Neighbors

CDP must be enabled on the Array in order to gather and display this information. See “CDP Settings” on page 191.

## RF Monitor Windows

Every Wi-Fi Array includes an integrated RF spectrum analyzer as a standard feature. The spectrum analyzer allows you to characterize the RF environment by monitoring throughput, signal, noise, errors, and interference levels continually per channel. This capability uses the built-in threat-sensor radio **abg(n)2**. The associated software is part of the ArrayOS.

The following RF Status windows are available:

- **IAPs**—displays current statistics and RF measurements for each of the Array's IAPs.
- **Spectrum Analyzer**—displays current statistics and RF measurements for each of the Array's channels.
- **Intrusion Detection**—displays rogue APs that have been detected by the Array.

### IAPs

The RF Monitor—IAPs window displays traffic statistics and RF readings observed by each Array IAP (radio). Note that the data is an instantaneous snapshot for the IAP—it is not an average or a cumulative total.

Status		Uptime - 5 days, 23 hours, 24 minutes																		
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> </ul>		IAP	Channel	Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate								
IAPs				0	0K 0	0K	0%	100%	0%	100%	0	-20	-65	-70	0%	100%	65	-20	1M	50M
Spectrum Analyzer		abg1	1																	
Intrusion Detection		abg2	-																	
Stations		abg3	11																	
Statistics		abg4	6																	
Event Log		a1	36																	
Configuration		a2	52																	
Express Setup		a3	149																	
Network		a4	40																	

Figure 78. RF Monitor—IAPs

Figure 78 presents the data as a graphical display, enabled by selecting the **Graph** checkbox on the lower left. If this option is not selected, data is presented as a numerical table. You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the Array to refresh this window automatically.

## Spectrum Analyzer



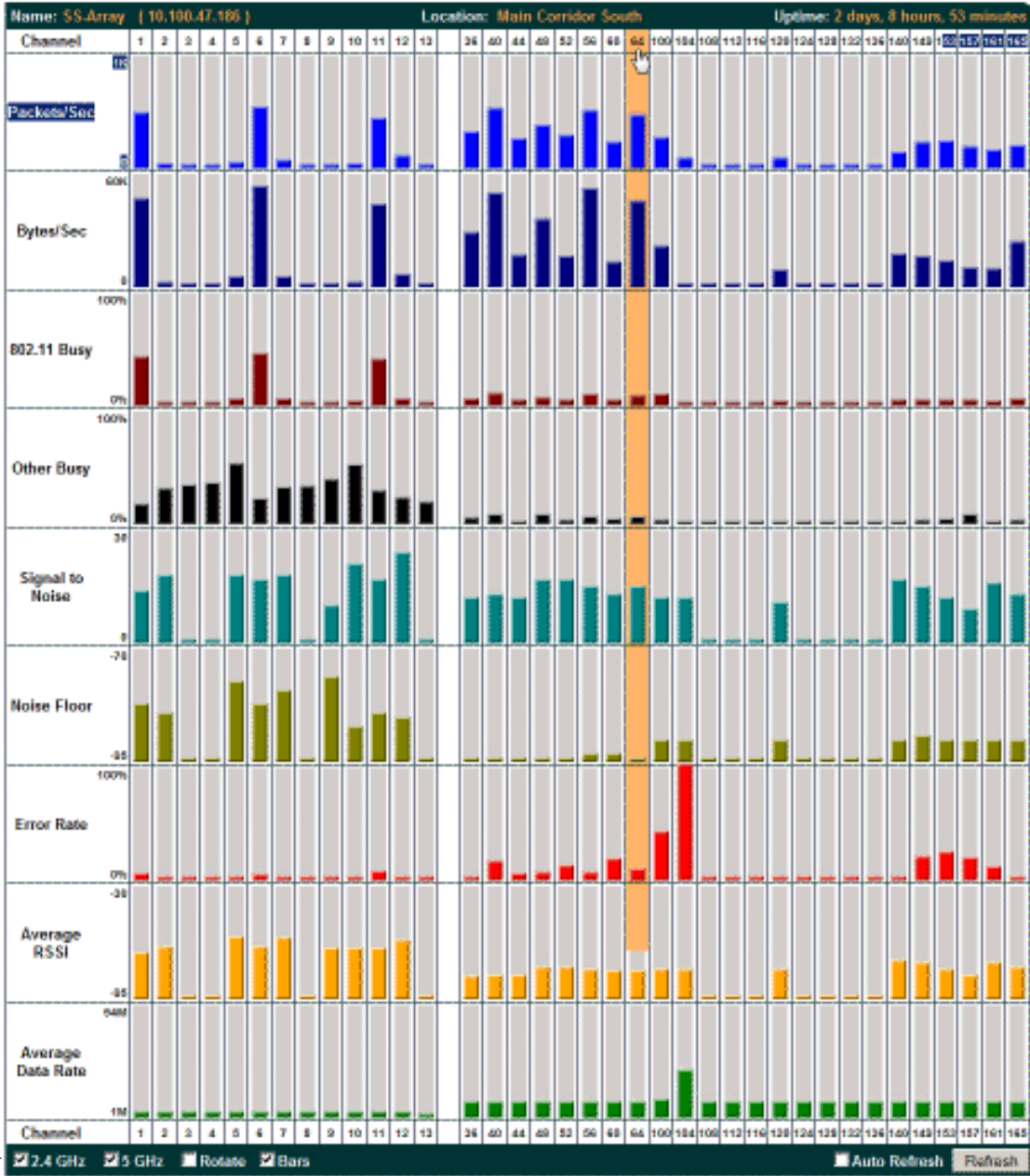
*The RF measurements for this feature are obtained by IAP **abg(n)2**, which **must** be set to **monitor** mode for any data to be available. See “IAP Settings” on page 255.*

Spectrum analysis on Wi-Fi Arrays is a distributed capability that automatically covers the entire Wi-Fi network, since a sensor is present in every unit. Arrays monitor the network 24/7 and analyze interference anywhere in the network from your desk. There’s no need to walk around with a device as with traditional spectrum analyzers, thus you don’t have to be in the right place to find outside sources that may cause network problems or pose a security threat. The Array monitors all 802.11 radio bands (a/b/g/n), not just those currently used for data transmission.

The RF Spectrum Analyzer window displays instantaneous traffic statistics and RF readings for all channels, as measured by the Array’s **abg(n)2** radio. This differs from the RF Monitor-IAPs window, which displays values measured by each IAP radio for its current assigned channel. For the spectrum analyzer, the **abg(n)2** radio is in a listen-only mode, scanning across all Wi-Fi channels. Each channel is scanned in sequence, for a 250 millisecond interval per channel. The spectrum analyzer window presents the data as a graphical display of vertical bar graphs for each statistic as shown in [Figure 79](#) (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in “[Spectrum Analyzer Measurements](#)” on page 146.

As an aid to viewing data for a particular channel, click the channel number. The channel will be highlighted down the page (or across the page for a rotated view, in both text and graph modes). Click additional channels to highlight them for easy comparison. To remove the highlighting from a channel, click the channel number again. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the Array to refresh this window automatically.


Click Channel number to highlight



Select Display Options

Figure 79. RF Spectrum Analyzer

The Spectrum Analyzer offers several display options:

- To display horizontal bar graphs, click the **Rotate** checkbox at the bottom of the data window.
- In the rotated view, if you wish to view data as a numerical table, click the **Text** checkbox. Click again to return to a graphical display. The text option is only available in the rotated view.
- When viewing a graphical display, click **Bars** to have the bar graphs displayed against a gray background—you may find this easier on the eyes. This operation is not available when Text is selected.
- You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Sorting is only available in the rotated view.
- At the bottom left of the frame, you may select whether to display only 2.4 GHz channels, 5 GHz channels, or both (both is the default). Note that the data is an instantaneous snapshot—it is not an average or a cumulative total.

### *Spectrum Analyzer Measurements*

The spectrum analyzer displays the following information:

- **Packets/Sec:** Total number of Wi-Fi packets per second on the channel, both valid and errored packets.
- **Bytes/Sec:** Total number of Wi-Fi bytes per second on the channel, valid packets only.
- **802.11 Busy:** Percentage of time that 802.11 activity is seen on the channel.
- **Other Busy:** Percentage of time that the channel is unavailable due to non-802.11 activity.

The total busy time (802.11 Busy plus Other Busy) will never total more than 100%. The remaining time (100% minus total busy time) is quiet time—the time that no activity was seen on the channel.



- **Signal to Noise:** Average SNR (signal to noise ratio) seen on the channel, calculated from the signal seen on valid 802.11 packets less the noise floor level. A dash value “-” means no SNR data was available for the interval.
- **Noise Floor:** Average noise floor reading seen on the channel (ambient noise). A dash value “-” means no noise data was available for the interval.
- **Error Rate:** Percentage of the total number of Wi-Fi packets seen on the channel that have CRC errors. The Error rate percentage may be high on some channels since the monitor radio is set to receive at a very sensitive level, enabling it to hear packets from devices at far distances.
- **Average RSSI:** Average RSSI level seen on 802.11 packets received on the channel. A dash value “-” means no RSSI data was available for the interval.
- **Average Data Rate:** Average data rate over time (per byte, not per packet) seen on 802.11 packets received on the channel. A dash value “-” means no data rate information was available for the interval. A higher data rate (above 6 Mbps) typically indicates user data traffic on the channel. Otherwise, the data rate reflects control packets at the lower basic rates.

### Intrusion Detection

This window displays all detected access points, according to the category you select from the drop-down list at the top—either Unknown, Known or Approved. This includes ad hoc access points (station-to-station connections). You can sort the results based on the following parameters by clicking the desired column header:

- SSID
- BSSID
- Manufacturer
- Channel
- RSSI
- Security
- Type
- Discovered
- Last Active

XN8 Wi-Fi Array **XIRRUS**

---

Name: SS-XN8 ( 10.100.47.186 )
Location: SS Area
Uptime: 4 days, 2 hours, 40 minutes

Select List Unknown

Select	BSSID	SSID	Manufacturer	Channel	RSSI	Security	Type	Discovered	Last Active
<input type="checkbox"/>	00:0b:6b:e0:00:f7	wlan-ng	Wistron Neweb	6	-51	none	ESS	Dec-05 14:06	active
<input type="checkbox"/>	00:0f:34:c0:46:30	tsunami	Cisco	11	-63	none	ESS	Dec-05 14:06	active
<input type="checkbox"/>	00:19:33:00:18:98	Giuseppe	Strix	165	-76	TKIP+PSK	ESS	Dec-05 14:06	active
<input type="checkbox"/>	00:0e:84:e4:19:9e	tsunami	Cisco	56	-87	none	ESS	Dec-05 14:06	active
<input type="checkbox"/>	00:11:20:ee:dc:83	LinkFloor3	Cisco	60	-61	none	ESS	Dec-08 16:13	active

Set Approved
Set Known
Set Blocked
 Auto Refresh
Refresh
Save

**Select the type of AP to display**

Figure 80. Intrusion Detection/Rogue AP List

The Intrusion Detection window provides the easiest method for designating rogue APs as Known, Approved, or Unknown. Choose one or more APs using the checkbox in the **Select** column, then set whether they are Approved, Known, or Unknown using the buttons on the lower left.

You can refresh the list at any time by clicking on the **Refresh** button, or click in the **Auto Refresh** check box to instruct the Array to refresh the list automatically.

### *See Also*

[Network Map](#)

[Rogue Control List](#)

[SSIDs](#)

[SSID Management](#)

## Station Status Windows

The following Station Status windows are available:

- **Stations**—this list describes all stations associated to the Array.
- **Location Map**—displays a map showing the approximate locations of all stations associated to the array.
- **RSSI**—for each associated station, this displays the Received Signal Strength Indicator at each of the Array’s IAPs.
- **Signal-to-Noise Ratio (SNR)**—for each associated station, this displays the SNR at each of the Array’s IAPs.
- **Noise Floor**—for each associated station, this displays the ambient noise (silence) value at each of the Array’s IAPs.
- **Max by IAP**—for each IAP, this shows the historical maximum number of stations that have been associated to it over various periods of time.

### Stations

This status-only window shows client stations currently visible to the Array. You may choose to view only stations that have associated to the Array, or only stations that are not associated, or both, by selecting the appropriate checkboxes above the list. The list shows the MAC address of each station, its NetBIOS name, its IP address, its manufacturer, the SSID used for the association, the **Group** (if any) that this station belongs to, its VLAN, its QoS, the IAP used for the association, transmit and receive rates, the **RSSI** for each station, and how long each association has been active (up time).

You may click the **Detail** checkbox at the bottom of the window to show a number of additional columns, including security settings used by the connection, the channel and band used, and additional RF measurements.

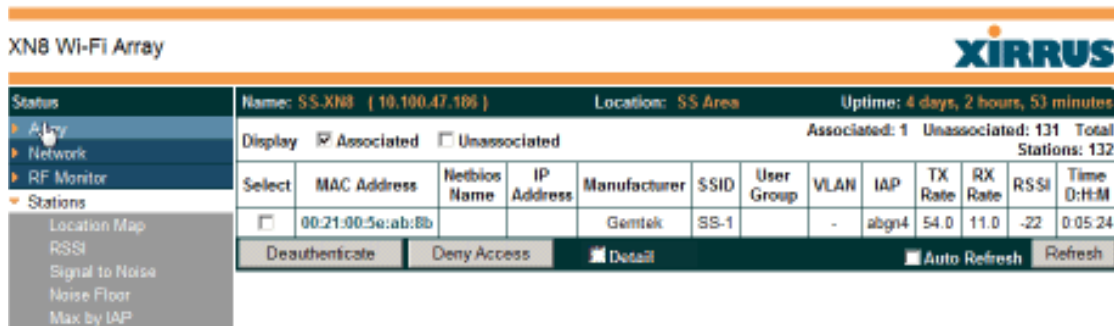


Figure 81. Stations

You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click again to reverse the sort order. You may select a specific station and perform one of the following actions by clicking the associated button:

- **Deny Access:** Sends a de-authentication frame to the selected station and explicitly denies it access by adding its MAC address to the Deny List in the Access Control List window. To permit access again, go to [“Access Control List” on page 223](#) and delete the station from the **Deny** list.
- **Deauthenticate:** Sends a de-authentication frame to the selected station. The station may re-authenticate.

Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

*See Also*

[Access Control List](#)

[Station Status Windows](#)

### Location Map

The Location Map shows the approximate locations of stations relative to this Array. You may display stations associated to this Array, unassociated stations (shown in gray), or both. The station count is shown on the left, above the map. You may also choose to display 5 GHz stations (shown in orange) or 2.4 GHz stations (shown in green), or both.

The map and Array are shown as if you were looking down on the Array from above, say from a skylight on the roof. Thus the positions of the radios **abg(n)1** to **abg(n)4** are a mirror image of the way they are typically drawn when looking at the face of the Array. Radios **abg(n)1** to **abg(n)4** are marked (1 to 4) on the map to show the orientation of the Array.

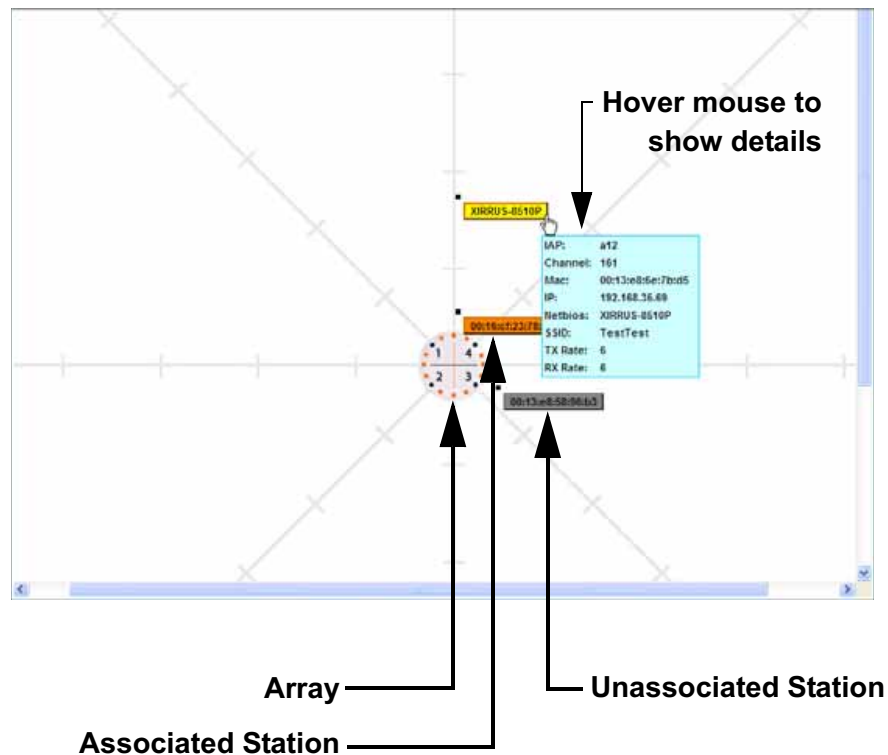


Figure 82. Location Map

A station is identified by its NetBIOS name if known, or else by its IP or MAC address. Hover the mouse over a station to show detailed information. If multiple stations are near each other, they will be displayed slightly offset so that one station does not completely obscure another. You may minimize a station that is not of interest by clicking it. Click it again for normal display. There is also a **Minimize All** button.

You may replace the range-finder background image above with your own custom image of the floorplan of the area served by the Array.

*Controls and items displayed on the Location Map window*



The controls for the Location Map are all at the bottom of the window and take up a fair amount of width. If some of the controls shown in Figure 83 are not visible, resize your browser window to be wider until all of the controls appear.

Also, the Location Map has its own scroll bars in addition to the browser's scroll bars. If you narrow the browser window, the map's scroll bar may be hidden. Use the browser's bottom scroll bar if you need to move it into view.

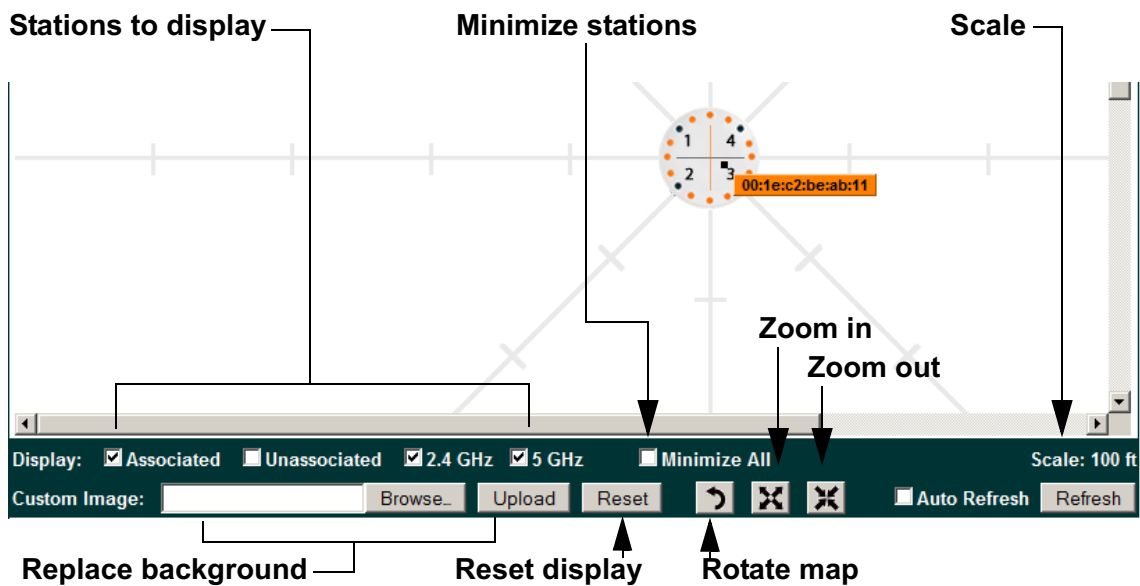


Figure 83. Controls for Location Map

- **Display Associated/Unassociated:** Select whether to display stations that are associated to the Array, stations that are not associated, or both.
- **Display 2.4 GHz/5 GHz:** Select whether to display 802.11bg(n) stations, or 802.11a(n) stations, or both.
- **Minimize All:** All stations are shown by default with their NetBIOS name or IP or MAC address. If the map is too cluttered, you can reduce the display for each station to a small rectangle. You may still display



detailed information for the station by hovering over it. To enlarge all rectangles, clear the Minimize All checkbox.

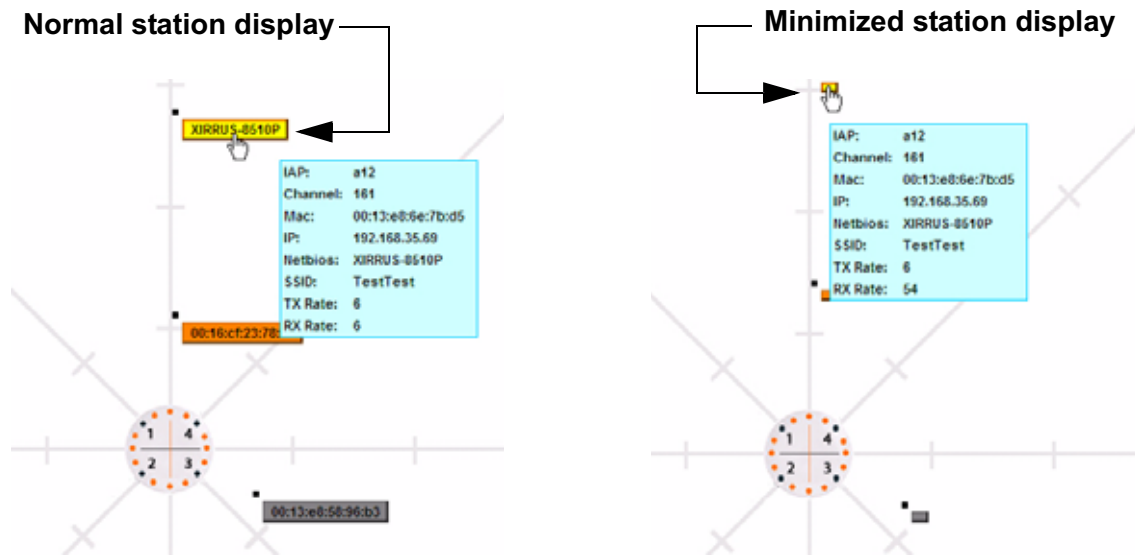





Figure 84. Minimizing stations

- **Scale:** This view-only value shows the approximate distance represented by each hashmark on the default map background. Scale is the rightmost of the items displayed in the control area - you may need to scroll to the right edge to see it.
- **Custom Image:** Use this feature to replace the default background image with your own image of the floor plan of your location. Click the **Browse** button and browse to the desired file on your computer. This may be a .gif, .jpg, .jpeg., .png, .htm, or .html file. The scale of the file should be 100 feet per inch. Then click **Upload** (see below). For more information on using the custom, image, see [“Working with the Custom Image”](#) on page 156.
- **Upload:** After browsing to the desired custom image, click the **Upload** button to install it. The map will be redisplayed with your new background. No hash marks are added to the image display.
- **Reset:** Click this button to restore the map display to the factory settings. All attributes are restored—including the stations selected for display, the scale, the rotation, and the background map.

-  ● **Rotate:** Click this button to rotate the orientation of the entire map. It rotates the map 45° counter-clockwise.
-  ● **Enlarge:** Click this button to enlarge (zoom in on) the map. The displayed **Scale** on the bottom right is updated with the new scale for the map.
-  ● **Reduce:** Click this button to reduce (zoom out on) the map. The displayed **Scale** on the bottom right is updated with the new scale for the map
- **Auto Refresh:** Instructs the Array to refresh this window automatically.
- **Refresh:** Updates the stations displayed.


### *See Also*

[Access Control List](#)

[Station Status Windows](#)

### *Working with the Custom Image*

After you have uploaded a custom image (see **Custom Image** and **Upload** in “[Controls and items displayed on the Location Map window](#)” on page 154), you should move the display of the Array on your map to correspond with its actual location at your site. The Location Map window provides a special set of controls for moving the location of the Array. These controls are displayed on the upper right corner of the map ([Figure 85](#)). The location controls only appear when you are using a custom image for your background. You will not see them if you are using the default map background.

To move the Array on the map in a particular direction, click an arrow for the desired direction on the location controls. The inner arrows move the Array by small steps; the outer arrows move it by larger steps. The arrows only work when you position the mouse directly over them—make sure you see the hand icon . If you need to return the Array to the center of the map, click the center of the location controls. When you are done, click the **Apply** button to save the new Array location, as well as the enlarge/reduce/rotate settings. These location settings will persist for the duration of the current WMI session, but not after a reboot (but the custom image will still be used after rebooting—whether or not you click **Apply**).

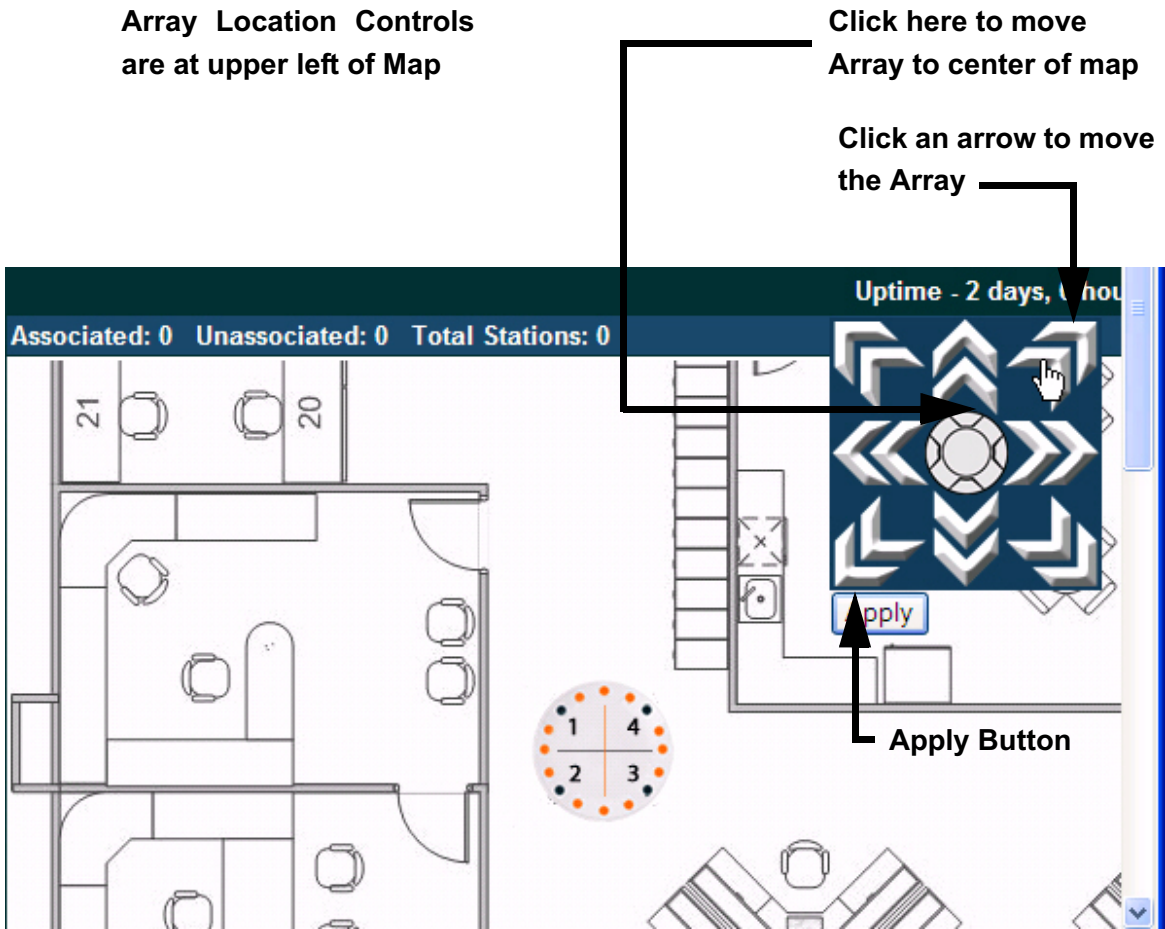


Figure 85. Setting Array location on a Custom Image

## RSSI

For each station that is associated to the Array, the RSSI (Received Signal Strength Indicator) window shows the station's RSSI value as measured by each IAP. In other words, the window shows the strength of the station's signal at each radio. You may choose to display **Unassociated Stations** as well with a checkbox at the bottom of the window.

RSSI Intensity (-95 to -30)																		
MAC Address	Netbios Name	IP Address	abg1	abg2	abg3	abg4	a1	a2	a3	a4	a5	a6	a7	a8	a9	a10	a11	a12
00:0f:3d:03:02:e8	TEST-PC-13	10.10.10.108										■						
00:0f:b5:97:3c:79	TEST-PC-4	10.10.10.134	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■
00:0e:35:45:dd:c0	TEST-PC-10	10.10.10.127																
00:30:b4:01:69:c4	TEST-PC-3	10.10.10.105																
00:0f:66:19:95:34	TEST-PC-8	10.10.10.109																
00:03:7f:bf:14:43	TEST-PC-7	10.10.10.103	■		■	■	■	■	■	■	■	■	■	■	■	■	■	■
00:04:e2:8b:42:57	TEST-PC-16	10.10.10.136																
00:10:18:91:0b:68	TEST-PC-11	10.10.10.122	■		■	■												
00:40:96:a7:d2:b2	TEST-PC-14	10.10.10.124																

Figure 86. Station RSSI Values

By default, the RSSI is displayed numerically. You may display the relative strength using color if you select **Colorize Intensity**, with the strongest signals indicated by the most intense color. (Figure 86) If you select **Graph**, then the RSSI is shown on a representation of the Array, either colorized or numerically based on your selection. (Figure 87) The stations are listed to the left of the Array—click on a station to show its RSSI values on the Array.

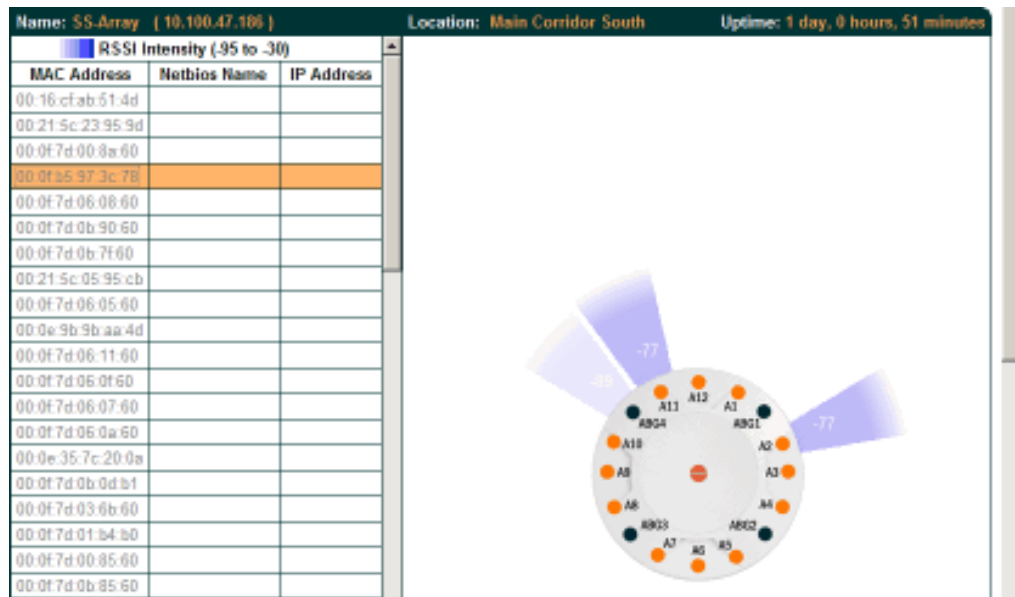


Figure 87. Station RSSI Values—Colorized Graphical View

In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

*See Also*

- Station Status Windows
- RF Monitor Windows

### Signal-to-Noise Ratio (SNR)

For each station that is associated to the Array, the Signal-to-Noise Ratio (SNR) window shows the station's SNR value as measured by each IAP. In other words, the window shows the SNR of the station's signal at each IAP radio. The signal-to-noise ratio can be very useful for determining the cause of poor performance at a station. A low value means that action may need to be taken to reduce sources of noise in the environment and/or improve the signal from the station.

The screenshot shows the XN8 Wi-Fi Array interface. On the left is a navigation menu with options: Status, Array, Network, RF Monitor, Stations, Location Map, RSSI, Signal to Noise (selected), Noise Floor, and Max by IAP. The main content area displays the following information:

Name: SS-X108 ( 10.100.47.186 )		Location: SS Area		Uptime: 4 days, 3 hours, 11 minutes							
MAC Address	Netbios Name	IP Address	abgn1	abgn2	abgn3	abgn4	an1	an2	an3	an4	
00:21:00:5e:ca:b8b			-	-	-	61	-	-	-	-	

Figure 88. Station Signal-to-Noise Ratio Values

You may choose to display **Unassociated Stations** as well with a checkbox at the bottom of the window.

By default, the SNR is displayed numerically. (Figure 88) You may display the relative value using color if you select **Colorize Intensity**, with the highest SNR indicated by the most intense color. (Figure 89) If you select **Graph**, then the SNR is shown on a representation of the Array, either colored or numerically based on your selection. The stations are listed to the left of the Array—click on a station to show its SNR values on the Array.

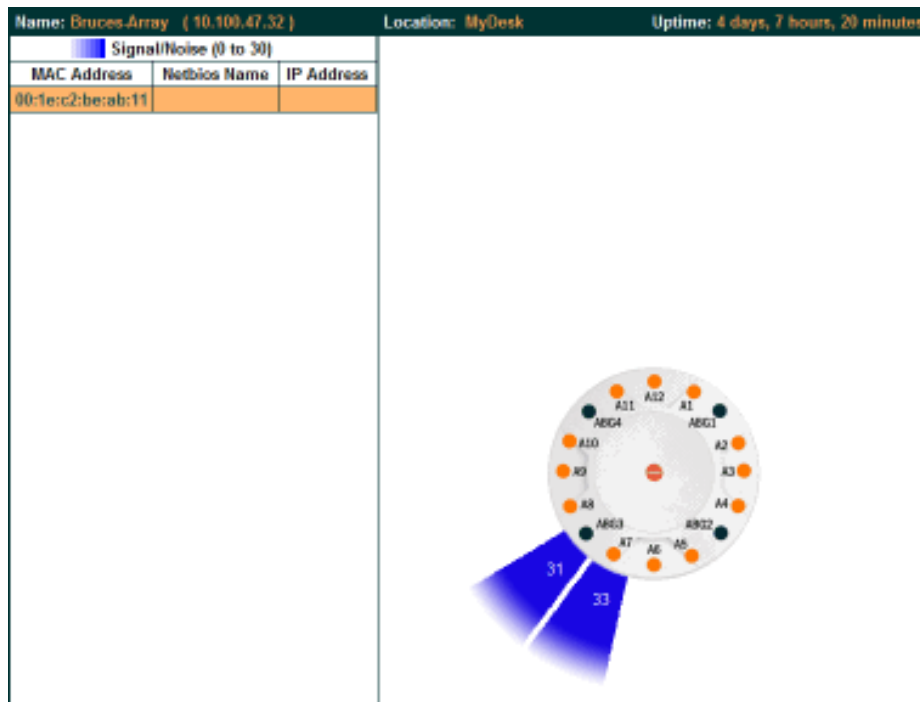


Figure 89. Station SNR Values—Colorized Graphical View

In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

*See Also*

Station Status Windows

RF Monitor Windows

## Noise Floor

For each station that is associated to the Array, the Noise Floor window shows the ambient noise affecting a station’s signal as measured by each IAP. The noise floor is the RSSI value when the station is not transmitting, sometimes called a Silence value. In other words, the window shows the noise floor of the station’s signal at each IAP radio. The noise floor value can be very useful for characterizing the environment of a station to determine the cause of poor performance. A relatively high value means that action may need to be taken to reduce sources of noise in the environment.

The screenshot shows the XN8 Wi-Fi Array interface. On the left is a navigation menu with options: Status, Array, Network, RF Monitor, Stations, Location Map, RSSI, Signal to Noise, Noise Floor (selected), and Max by IAP. The main content area displays details for a station named 'SS-XN8 (10.100.47.106)' located in 'SS Area' with an uptime of '4 days, 3 hours, 22 minutes'. Below this, a table shows noise floor values for various IAPs.

MAC Address	Netbios Name	IP Address	abgn1	abgn2	abgn3	abgn4	an1	an2	an3	an4
00:21:00:5e:ac:8b			-96	-	-	-96	-	-	-	-

Figure 90. Station Noise Floor Values

You may choose to display **Unassociated Stations** as well with a checkbox at the bottom of the window.

By default, the noise floor is displayed numerically. (Figure 90) You may display the relative value using color if you select **Colorize Intensity**, with the highest noise indicated by the most intense color. If you select **Graph**, then the ambient noise is shown on a representation of the Array, either colored or numerically based on your selection.(Figure 91) The stations are listed to the left of the Array—click on a station to show its values on the Array.



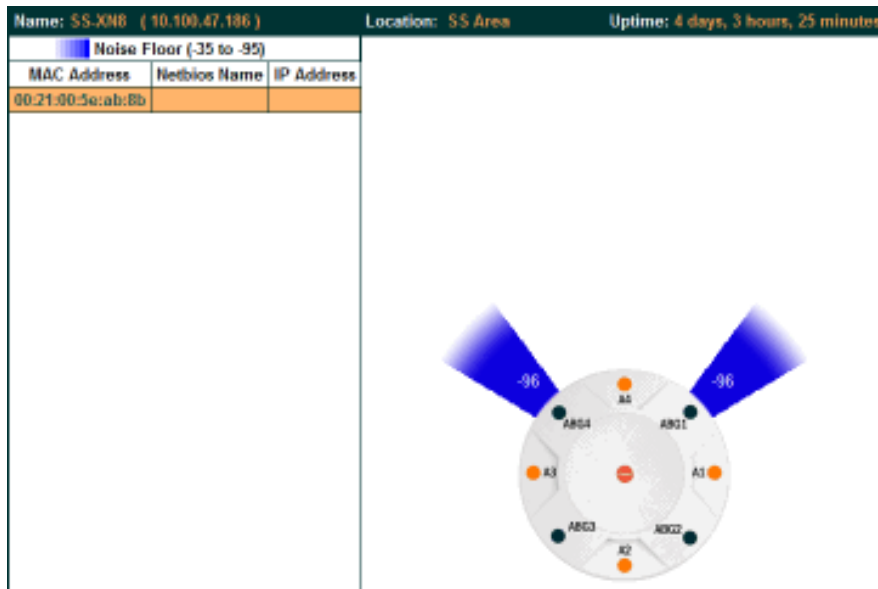


Figure 91. Station Noise Floor Values—Colorized Graphical View

In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

*See Also*

- Station Status Windows
- RF Monitor Windows

## Max by IAP

This status-only window shows the maximum number of client stations that have historically been associated to the Array. For each IAP, the list shows the IAP's state and channel number, the current number of stations associated, and the highest number of stations that have been associated over various periods of time: hour, day, week, month, and year. In other words, the Max Station Count shows the “high water mark” over the selected period of time—the maximum count of stations for the selected period, rather than a cumulative count of all stations that have associated. This information aids in network administration and in planning for additional capacity.

Status		Name: XSR8-CMU (172.16.1.8)		Uptime: 0 days, 1 hour, 29 minutes						
		Max station count								
	IAP	State	Channel	Current Stations	Hour	Day	Week	Month	Year	
▸ Array	abg1	up	1 manual	0	0	0	0	0	0	
▸ Network	abg2	up	monitor	0	0	0	0	0	0	
▸ RF Monitor	abg3	up	11 manual	2	3	3	3	3	3	
▾ Stations	abg4	up	6 manual	0	1	2	2	2	2	
Location Map	a1	up	36 manual	0	2	2	2	2	2	
RSSI	a2	up	153 manual	2	4	4	4	4	4	
Signal to Noise	a3	up	56 manual	0	0	0	0	0	0	
Noise Floor	a4	up	165 manual	1	1	1	1	1	1	
Max by IAP										
▸ Statistics										
System Log										

Figure 92. Max by IAP

You may click an IAP to go to the [IAP Settings](#) window. Click on the **Refresh** button to refresh the station list, or click **Auto Refresh** to instruct the Array to refresh this window automatically.

*See Also*

[IAPs](#)

[Station Status Windows](#)

## Statistics Windows

The following Array Statistics windows are available:

- **IAP Statistics Summary**—provides an overview of the statistical data associated with all IAPs. Expands to show links for displaying detailed statistics for individual IAPs.
- **Per-IAP Statistics**—provides detailed statistics for an individual IAP.
- **Network Statistics**—displays statistical data associated with each network (Ethernet) interface.
- **VLAN Statistics**—provides statistical data associated with your assigned VLANs.
- **WDS Statistics**—provides statistical data for all WDS client and host links.
- **Filter Statistics**—provides statistical data for all configured filters.
- **Station Statistics**—provides statistical data associated with each station.

### IAP Statistics Summary

This is a status only window that provides an overview of the statistical data associated with all IAPs. It also shows the channel used by each IAP. For detailed statistics for a specific IAP, see “Per-IAP Statistics” on page 166. Click the **Unicast Stats Only** checkbox on the lower left to filter the results, or clear the checkbox to show statistics for all wireless traffic.

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

XN8 Wi-Fi Array

Status Name: SS-XN8 ( 10.100.47.186 ) Location: SS Area Uptime: 4 days, 3 hours, 34 minutes

- ▶ Array
- ▶ Network
- ▶ RF Monitor
- ▶ Stations
- ▶ Statistics
  - ▼ IAP
    - IAP abgn1
    - IAP abgn2
    - IAP abgn3
    - IAP abgn4
    - IAP an1
    - IAP an2
    - IAP an3
    - IAP an4

Statistics for IAP All									
Receive Statistics by IAP						Transmit Statistics by IAP			
IAP	Channel	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
abgn1	1	5216920126	197823478	6327909	6597613	1785545569	6479993	17015352	0
abgn2	monitor	5514057421	110730414	2084140	46805	52598262	0	31587	0
abgn3	11	2525483	59570	2122	2298	722066	2242	3958	0
abgn4	6	8841010558	197057914	3711009	5814195	1974668688	7027414	14003973	0
an1	40	449765044	10002740	52483	5488440	2031371868	6487438	0	0
an2	56	1227961769	8591220	215648	3993583	2189924337	6489420	0	0
an3	48	433997191	9498186	55132	4554583	2055255364	6487917	0	0
an4	64	531168	2609	113	1494	722957	2259	0	0

Unicast Stats Only
  Auto Refresh

Figure 93. IAP Statistics Summary Page

### See Also

- System Log Window
- Global Settings (IAP)
- Global Settings .11a
- Global Settings .11bg
- IAPs

### Per-IAP Statistics

This is a status only window that provides detailed statistics for the selected IAP. If you click the link for **IAP All** in the left frame, each detailed statistic field will show the sum of that statistic for all IAPs. For a summary of statistics for all IAPs, see “[IAP Statistics Summary](#)” on page 165. Use the **Display Percentages** checkbox at the lower left to select the output format—check this option to express each statistic as a percentage of the total at the top of the column, or leave it blank to display raw numbers.

A quick way to display the statistics for a particular IAP is by clicking the Array graphic at the bottom left of the WMI window. Click the desired IAP, and the selected statistics will be displayed. See “[User Interface](#)” on page 123.

Name: SS-XM8 [ 10.100.47.186 ]		Location: SS Area		Uptime: 4 days, 3 hours, 39 minutes	
Statistics for IAP abg4					
Receive Statistics			Transmit Statistics		
Total Bytes	8848640898	Total Bytes	1976503120		
Total Packets	197226805	Total Packets	7034604		
Unicasts	25841	Unicasts	106		
Multicasts	0	Multicasts	15180		
Broadcasts	102409705	Broadcasts	42755		
Mgmt Packets	0	Mgmt Packets	7226222		
Beacons	94791259	Beacons	6976663		
Fragments	0	Fragments	0		
RTS Count	0	RTS Count	0		
CTS Count	0	CTS Count	0		
Receive Errors & Retries			Transmit Errors & Retries		
Total Errors	9533147	Total Errors	14015458		
Total Retries	5820027	Total Retries	0		
Dropped Packets	24	Dropped	8212136		
Unassociated	0	Unassociated	0		
CRC	3711363	ACK Failures	6803322		
Fragment Errors	0	RTS Failures	0		
Encryption Errors	1484	RTS Retries	0		
Duplicates	249	Single Retries	0		
Overruns	0	Multiple Retries	6804862		
<input type="checkbox"/> Display Percentages		<input type="checkbox"/> Auto Refresh		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>

Figure 94. Individual IAP Statistics Page (for IAP abg(n)1)

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

*See Also*

- System Log Window
- Global Settings (IAP)
- Global Settings .11a
- Global Settings .11bg
- IAPs

## Network Statistics

This is a status only window that allows you to review statistical data associated with each network (Ethernet) interface and its activity. You can **Refresh** the data (update the window with the latest information) or **Clear** the data (reset all content to zero and begin counting again) at any time by clicking on the appropriate button. You can also click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically. If you are experiencing problems on the Array, you may also want to print this window for your records.

Status	Name: SS-XM8 ( 10.100.47.186 )	Location: SS Area	Uptime: 4 days, 3 hours, 53 minutes	
▶ Array	Fast Ethernet Statistics enabled, link down, 100Mbps, full duplex			
▶ Network	Receive Bytes	0	Transmit Bytes	0
▶ RF Monitor	Receive Packets	0	Transmit Packets	0
▶ Stations	Receive Compressed	0	Transmit Compressed	0
▶ Statistics	Receive Multicast	0	Transmit Carrier Errors	0
▶ IAP	Receive Dropped	0	Transmit Dropped	0
▶ Network	Receive FIFO Errors	0	Transmit FIFO Errors	0
▶ VLAN	Receive Frame Errors	0	Transmit Collisions	0
▶ WDS	Receive Total Errors	0	Transmit Total Errors	0
▶ Filter	Gigabit 1 Statistics enabled, link up, 1000Mbps, full duplex			
▶ Stations	Receive Bytes	246021597	Transmit Bytes	202395823
System Log	Receive Packets	1745005	Transmit Packets	859020
Configuration	Receive Compressed	0	Transmit Compressed	0
Express Setup	Receive Multicast	0	Transmit Carrier Errors	0
▶ Network	Receive Dropped	0	Transmit Dropped	0
▶ Services	Receive FIFO Errors	0	Transmit FIFO Errors	0
▶ VLANs	Receive Frame Errors	0	Transmit Collisions	0
▶ Security	Receive Total Errors	0	Transmit Total Errors	0
▶ SSIDs	Gigabit 2 Statistics enabled, link down, 100Mbps, half duplex			
▶ Groups	Receive Bytes	0	Transmit Bytes	0
▶ IAPs	Receive Packets	0	Transmit Packets	0
▶ WDS	Receive Compressed	0	Transmit Compressed	0
▶ Filters	Receive Multicast	0	Transmit Carrier Errors	0
Tools	Receive Dropped	0	Transmit Dropped	0
System Tools	Receive FIFO Errors	0	Transmit FIFO Errors	0
CLI	Receive Frame Errors	0	Transmit Collisions	0
Logout	Receive Total Errors	0	Transmit Total Errors	0
Log Messages	<input checked="" type="checkbox"/> Auto Refresh   Refresh   Clear			
Critical	0			
Warning	0			

Figure 95. Network Statistics

### See Also

DHCP Server

DNS Settings

Network

Network Interfaces

### VLAN Statistics

This is a status only window that allows you to review statistical data associated with your assigned VLANs. You can refresh the information that is displayed on this page at any time by clicking on the **Refresh** button, or select the **Auto Refresh** option for this window to refresh automatically. The **Clear All** button at the lower left allows you to clear (zero out) all VLAN statistics.

**XN8 Wi-Fi Array** **XIRRUS**

Name: SS-XN8 ( 10.100.47.186 )      Location: SS Area      Uptime: 4 days, 3 hours, 59 minutes

VoIP (12) Statistics <span style="float: right;">Clear</span>				
Receive Bytes	0	Transmit Bytes		0
Receive Packets	0	Transmit Packets		0
Receive Compressed	0	Transmit Compressed		0
Receive Multicast	0	Transmit Carrier Errors		0
Receive Dropped	0	Transmit Dropped		0
Receive FIFO Errors	0	Transmit FIFO Errors		0
Receive Frame Errors	0	Transmit Collisions		0
Receive Total Errors	0	Transmit Total Errors		0
Finance (5) Statistics <span style="float: right;">Clear</span>				
Receive Bytes	0	Transmit Bytes		3313440
Receive Packets	0	Transmit Packets		5616
Receive Compressed	0	Transmit Compressed		0
Receive Multicast	0	Transmit Carrier Errors		0
Receive Dropped	0	Transmit Dropped		0
Receive FIFO Errors	0	Transmit FIFO Errors		0
Receive Frame Errors	0	Transmit Collisions		0
Receive Total Errors	0	Transmit Total Errors		0

Clear All       Auto Refresh      Refresh

Figure 96. VLAN Statistics

*See Also*

VLAN Management

VLANs

### WDS Statistics

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

Status		Name: SS-XNB ( 10.100.47.136 )	Location: SS Area	Uptime: 4 days, 4 hours, 4 minutes																																																					
<ul style="list-style-type: none"> <li>Array</li> <li>Network</li> <li>RF Monitor</li> <li>Stations</li> <li>Statistics                             <ul style="list-style-type: none"> <li>IAP</li> <li>Network</li> <li>VLAN</li> <li>WDS                                     <ul style="list-style-type: none"> <li>Client Link 1</li> <li>Client Link 2</li> <li>Client Link 3</li> <li>Client Link 4</li> <li>Host Link 1</li> <li>Host Link 2</li> <li>Host Link 3</li> </ul> </li> </ul> </li> </ul>		<table border="1"> <thead> <tr> <th colspan="4">Receive Statistics</th> <th colspan="4">Transmit Statistics</th> </tr> <tr> <th>Client Link</th> <th>Bytes</th> <th>Packets</th> <th>Errors</th> <th>Retries</th> <th>Bytes</th> <th>Packets</th> <th>Errors</th> <th>Retries</th> </tr> </thead> <tbody> <tr><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table>			Receive Statistics				Transmit Statistics				Client Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries	1									2									3									4								
Receive Statistics				Transmit Statistics																																																					
Client Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries																																																	
1																																																									
2																																																									
3																																																									
4																																																									
		<table border="1"> <thead> <tr> <th colspan="4">Receive Statistics</th> <th colspan="4">Transmit Statistics</th> </tr> <tr> <th>Host Link</th> <th>Bytes</th> <th>Packets</th> <th>Errors</th> <th>Retries</th> <th>Bytes</th> <th>Packets</th> <th>Errors</th> <th>Retries</th> </tr> </thead> <tbody> <tr><td>1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>2</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </tbody> </table>			Receive Statistics				Transmit Statistics				Host Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries	1									2									3									4								
Receive Statistics				Transmit Statistics																																																					
Host Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries																																																	
1																																																									
2																																																									
3																																																									
4																																																									
		<input type="checkbox"/> Auto Refresh   Refresh   Clear																																																							

Figure 97. WDS Statistics

*See Also*

SSID Management

WDS



### Filter Statistics

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

Name	Type	State	Packets	Bytes
Filter1	allow	on	1961	268436

Figure 98. Filter Statistics

*See Also*  
Filters

### Station Statistics

This status-only window provides an overview of statistical data for all stations. Stations are listed by MAC address, and Receive and Transmit statistics are summarized for each. For detailed statistics for a specific station, click the desired MAC address in the **Station** column and see “Per-Station Statistics” on page 172.

	Receive Statistics by Station				Transmit Statistics by Station			
	Station	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors
00:0e:3d:03:02:a8	693119	2043	0	223	2358	12	0	1
00:0e:b5:97:3c:79	51442645153	52791337	0	5371975	65480578303	65615091	26764	118569632
00:0e:35:45:dd:c0	1691913717	24210701	0	8748417	168562071943	164832863	112870	104185567
00:30:b4:01:69:c4	1004756270	10171896	0	0	265914094203	259348067	10303	48599772
00:0e:66:19:95:c4	1550292533	5009662	0	1202533	36006985880	36032055	309661	41993995
00:03:7f:bf:14:43	197116974748	195875363	0	32942200	277967033447	266885001	45170	60729663
00:04:a2:9b:42:57	323018216404	312187836	0	29556244	507270199576	492647649	12040	39468662
00:10:18:91:06:68	161652416042	177651569	0	18383672	264862154829	263394451	170454	36038464
00:40:96:a7:d2:b2	249090923768	247980426	0	22610375	276050170214	270423992	18482	127696107

Figure 99. Station Statistics

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

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

*See Also*

Per-Station Statistics

### Per-Station Statistics

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

Receive and Transmit statistics are listed by **Rate**—this is the data rate in Mbps. For a summary of statistics for all stations, see [“Station Statistics”](#) on page 171.

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

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

Rate	Receive Statistics				Transmit Statistics			
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
1	1015465	18726	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
5.5	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
6	3728543	77325	0	15	0	0	0	0
9	0	0	0	0	0	0	0	0
12	1710	5	0	3	0	0	0	0
18	1725	5	0	2	0	0	0	0
24	0	0	0	0	0	0	0	0
36	5959	22	0	2	0	0	0	0
48	73724	226	0	29	0	0	0	0
54	693119	2043	0	223	2358	12	0	1
<b>Total</b>	<b>5520246</b>	<b>98354</b>	<b>0</b>	<b>274</b>	<b>2358</b>	<b>12</b>	<b>0</b>	<b>1</b>

Clear  Auto Refresh Refresh

Figure 100. Individual Station Statistics Page

*See Also*

Station Statistics

## System Log Window

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

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

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

Status			
Name: SS-Array [ 10.100.47.185 ]		Location: Main Corridor South	
Uptime: 3 days, 1 hour, 8 minutes		Filter Priority: Notification	
Highlight Priority: Notification			
Time Stamp	Priority	Message	
Oct 21 17:24:38	Notification	Admin user admin logged into web management interface from 10.100.21.73	
Oct 21 17:24:33	Notification	Admin user admin was logged out of web management interface due to timeout.	
Oct 21 17:04:34	Alert	Rogue AP detected. SSID: SQA-WPR-Custom, BSSID: 00:0f:7d:06:cc:f0, Manufacturer: Ximus, Channel: 64, RSSI: -94, Security: none	
Oct 21 17:02:56	Alert	Rogue AP detected. SSID: zoroopen1, BSSID: 00:0f:7d:09:ef:50, Manufacturer: Ximus, Channel: 60, RSSI: -93, Security: none	
Oct 21 16:57:12	Alert	Rogue AP detected. SSID: public, BSSID: 00:0f:7d:04:f2:03, Manufacturer: Ximus, Channel: 161, RSSI: -90, Security: none	
Oct 21 16:55:01	Alert	Rogue AP detected. SSID: SQA-WPR-Custom, BSSID: 00:0f:7d:06:cd:50, Manufacturer: Ximus, Channel: 40, RSSI: -90, Security: none	
Oct 21 16:52:47	Alert	Rogue AP detected. SSID: SQA-WPR-Login-Int, BSSID: 00:0f:7d:0a:3f:51, Manufacturer: Ximus, Channel: 40, RSSI: -86, Security: none	
Oct 21 16:49:45	Alert	Rogue AP detected. SSID: fredigit, BSSID: 00:0f:7d:00:8d:56, Manufacturer: Ximus, Channel: 40, RSSI: -76, Security: none	

Figure 101. System Log

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



# Configuring the Wi-Fi Array

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

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

- [“Express Setup” on page 176](#)
- [“Network” on page 182](#)
- [“Services” on page 193](#)
- [“VLANs” on page 205](#)
- [“Security” on page 209](#)
- [“SSIDs” on page 235](#)
- [“Groups” on page 247](#)
- [“IAPs” on page 253](#)
- [“WDS” on page 285](#)
- [“Filters” on page 289](#)

After making changes to the configuration settings of an Array you must click on the **Save** button at the bottom of the configuration window, otherwise the changes you make will not be applied the next time the Array is rebooted. Click the **Apply** button if you want the changes applied to the current configuration, without making them permanent.

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

- [“Viewing Status on the Wi-Fi Array” on page 127](#)
- [“Using Tools on the Wi-Fi Array” on page 295](#)

## Express Setup

The Express Setup procedure allows you to establish global configuration settings that will enable basic Array functionality. Any changes you make in this window will affect all radios. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 1 day, 23 hours, 19 minutes
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>System Log</li> <li>Configuration</li> <li>Express Setup</li> <li>▶ Network</li> <li>▶ Services</li> <li>▶ VLANs</li> <li>▶ Security</li> <li>▶ SSIDs</li> <li>▶ Groups</li> <li>▶ IAPs</li> <li>▶ WDS</li> <li>▶ Filters</li> <li>Tools</li> <li>System Tools</li> <li>CLI</li> <li>Logout</li> <li>Log Messages</li> <li>Critical 6</li> <li>Warning 6</li> <li>Information 500</li> </ul>	Host Name: <input type="text" value="SS-XN8"/>	Location Information: <input type="text" value="SS Area"/>	Admin Contact: <input type="text" value="J Smith"/>
	Admin Email: <input type="text" value="jsa@xyzcorp.com"/>	Admin Phone: <input type="text" value="805-555-1212"/>	SNMPv2 Settings
	Enable SNMPv2: <input checked="" type="radio"/> Yes <input type="radio"/> No	Read-Only Community String: <input type="text" value="*****"/>	Read-Write Community String: <input type="text" value="*****"/>
	10/100 Ethernet 0 Settings	Enable Interface: <input checked="" type="radio"/> Yes <input type="radio"/> No	Configuration Server Protocol: <input type="radio"/> DHCP <input checked="" type="radio"/> Static
	IP Address: <input type="text" value="10.10.10.21"/>	IP Subnet Mask: <input type="text" value="255.255.255.0"/>	Default Gateway: <input type="text" value="10.10.10.1"/>
	Gigabit Ethernet 1 Settings	Enable Interface: <input checked="" type="radio"/> Yes <input type="radio"/> No	Allow Management On Interface: <input checked="" type="radio"/> Yes <input type="radio"/> No
	Configuration Server Protocol: <input type="radio"/> DHCP <input checked="" type="radio"/> Static	IP Address: <input type="text" value="10.10.10.186"/>	IP Subnet Mask: <input type="text" value="255.255.255.0"/>
	Default Gateway: <input type="text" value="10.10.10.1"/>	SSID Settings	SSID (Wireless Network Name): <input type="text"/>
	Wireless Security: <input type="text" value="Open"/>	Admin Settings	New Admin User (Replaces user "admin"): <input type="text" value="private"/>
	New Admin Password: <input type="text" value="*****"/>	Confirm Admin Password: <input type="text" value="*****"/>	Time and Date Settings
	TimeZone: <input type="text" value="(GMT - 08:00) Pacific Time (US &amp; Canada): Tijuana"/>	Auto Adjust Daylight Savings: <input checked="" type="checkbox"/>	Use Network Time Protocol: <input checked="" type="radio"/> Yes <input type="radio"/> No
	NTP Primary Server: <input type="text" value="time.nist.gov"/>	NTP Secondary Server: <input type="text" value="pool.ntp.org"/>	IAP Settings
	Enable/Configure All IAPs: <input type="button" value="Execute"/>	<input type="button" value="Apply"/> <input type="button" value="Save"/>	

Figure 102. WMI: Express Setup

### *Procedure for Performing an Express Setup*

1. **Host Name:** Specify a unique [host name](#) for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is Xirrus-WiFi-Array.
2. **Location Information:** Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
3. **Admin Contact:** Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
4. **Admin Email:** Enter the email address of the admin contact you entered in Step 3.
5. **Admin Phone:** Enter the telephone number of the admin contact you entered in Step 3.
6. **Configure SNMP:** Select whether to **Enable** SNMP on the Array, and set the SNMP community strings. The factory default value for the **SNMP Read-Only Community String** is `xirrus_read_only`. The factory default value for the **SNMP Read-Write Community String** is `xirrus`. If you are using the Xirrus Management System (XMS), the read-write string must match the string used by XMS. XMS also uses the default value `xirrus`.
7. **Configure the 10/100 Ethernet 0 (10/100 Mb) and Gigabit Ethernet 1 network interface settings.** Note that the and Gigabit Ethernet 2 port is not configured on this page. If you need to make changes to Gigabit 2, please see [“Network Interfaces” on page 183](#).

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

- a. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.
- b. **Allow Management on Interface:** This option is available only on the Gigabit 1 and Gigabit 2 interfaces—the 10/100 Ethernet port is also known as the Management Port, and management is **always** enabled

on this port. Choose **Yes** to allow management of the Array via this Gigabit interface, or choose **No** to deny all management privileges for this interface.

- c. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** to assign IP addresses to the Array's Ethernet interfaces, or choose **Static** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following information:
  - **IP Address:** Enter a valid IP address for this Array. To use a remote connection (Web, **SNMP**, or **SSH**), a valid IP address must be used.
  - **IP Subnet Mask:** Enter a valid IP address for the **subnet mask** (the default is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
  - **Default Gateway:** Enter a valid IP address for the **default gateway**. This is the IP address of the router that the Array uses to forward data to other networks.

8. **SSID Settings:** This section specifies the wireless network name and security settings.

- a. The **SSID (Wireless Network Name)** is a unique name that identifies a wireless network (SSID stands for Service Set Identifier). All devices attempting to connect to a specific WLAN must use the same SSID. The default SSID is **xirrus**. Entering a value in this field will replace the default SSID with the new name.

For additional information about SSIDs, go to the **Multiple SSIDs** section of "Frequently Asked Questions" on page 398.

- b. **Wireless Security:** Select the desired wireless security scheme (Open, **WEP** or **WPA**). Make your selection from the choices available in the pull-down list.
  - **Open**—This option offers no data encryption and is not recommended, though you might choose this option if clients are





write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). The default **admin** user is deleted. Note that the Array also offers the option of authenticating administrators using a RADIUS server (see “Admin Management” on page 215)).

- b. New Admin Password:** If desired, enter a new administration password for managing this Array. Choose a password that is not obvious, and one that you can remember. If you forget your password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
    - c. Confirm Admin Password:** If you entered a new administration password, confirm the new password here.
- 10. Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you’re not using a server.
  - a. Time Zone:** Select your time zone from the choices available in the pull-down list.
  - b. Auto Adjust Daylight Savings:** If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
  - c. Use Network Time Protocol:** Check this box if you want to use an NTP server to synchronize the Array’s clock. This ensures that Syslog time-stamping is maintained across all units. Without an NTP server assigned (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies. If you check **Yes**, the NTP server fields are displayed. If you don’t want to use an NTP server, leave this box unchecked (default) and set the system time on the Array manually.
  - d. NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.

- e. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server.
- f. **Set Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes, seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).
- g. **Set Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, the date fields become active. Enter the revised date (month, day and year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).

#### 11. IAP Settings:

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

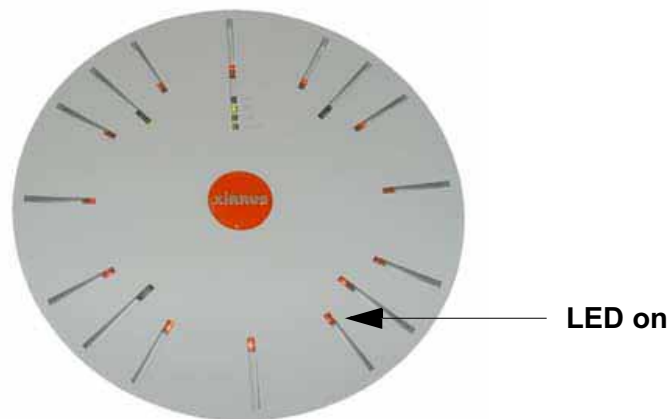


Figure 103. LEDs are Switched On

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

## Network

This is a status-only window that provides a snapshot of the configuration settings currently established for the 10/100 Ethernet 0 interface and the Gigabit 1 and Gigabit 2 interfaces. DNS Settings and CDP Settings (Cisco Discovery Protocol) are summarized as well. You must go to the appropriate configuration window to make changes to any of the settings displayed here (configuration changes cannot be made from this window). You can click on any item in the **Interface** column to “jump” to the associated configuration window.

XN8 Wi-Fi Array								
Name: SS-XN8 ( 10.100.47.186 )		Location: SS Area			Uptime: 0 days, 0 hours, 23 minutes			
<b>Interface Settings Summary</b>								
Interface	Status	Link	Port Mode	DHCP	IP Address	Subnet Mask	Gateway	
10/100 Ethernet 0	Enabled	down		Disabled	10.100.47.21	255.255.255.0	10.100.47.1	
Gigabit Ethernet 1	Enabled	up	link-backup	Disabled	10.100.47.186	255.255.255.0	10.100.47.1	
Gigabit Ethernet 2	Enabled	down	link-backup	Disabled	10.100.47.186	255.255.255.0	10.100.47.1	
<b>DNS Settings Summary</b>								
Hostname		Domain	DNS Server 1		DNS Server 2		DNS Server 3	
SS-XN8		ximus.com	10.100.1.10		10.100.2.10			
<b>CDP Settings Summary</b>								
State			Interval			Hold Time		
Enabled			60			180		

Figure 104. Network Interfaces

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

- [“Network Interfaces” on page 183](#)
- [“DNS Settings” on page 190](#)
- [“CDP Settings” on page 191](#)

### See Also

[DNS Settings](#)

[Network Interfaces](#)

[Network Status Windows](#)

[Spanning Tree Status](#)

[Network Statistics](#)

### Network Interfaces

This window allows you to establish configuration settings for the 10/100 Fast Ethernet interface and the Gigabit 1 and Gigabit 2 interfaces.

Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 0 hours, 26 minutes
Array	10/100 Ethernet 0 Settings		
Network	Enable Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
RF Monitor	Auto Negotiate:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Stations	Duplex:	<input checked="" type="radio"/> Full	<input type="radio"/> Half
Statistics	Speed:	100 Megabit	
System Log	Configuration Server Protocol:	<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
Configuration	IP Address:	10.100.100.21	
Express Setup	IP Subnet Mask:	255.255.255.0	
Network	Default Gateway:	10.100.100.1	
Interfaces	Static route (IP Address/Mask):		
DNS	Gigabit Ethernet 1 Settings		
CDP	Enable Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Services	LED Indicator:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
VLANs	Allow Management On Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Security	Auto Negotiate:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
SSIDs	Duplex:	<input checked="" type="radio"/> Full	<input type="radio"/> Half
Groups	Speed:	Gigabit	
IAPs	Port Mode:	Active backup (gig1/2 fail over to each other)	
WDS	Configuration Server Protocol:	<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
Filters	IP Address:	10.100.100.186	
Tools	IP Subnet Mask:	255.255.255.0	
System Tools	Default Gateway:	10.100.100.1	
CLI	Gigabit Ethernet 2 Settings		
Logout	Enable Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Log Messages	LED Indicator:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
Critical 6	Allow Management On Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Warning 6	Auto Negotiate:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Information 500	Duplex:	<input checked="" type="radio"/> Full	<input type="radio"/> Half
	Speed:	Gigabit	
	Port Mode:	Active backup (gig1/2 fail over to each other)	
	Configuration Server Protocol:	<input checked="" type="radio"/> DHCP	<input checked="" type="radio"/> Static
	IP Address:	10.100.100.186	
	IP Subnet Mask:	255.255.255.0	
	Default Gateway:	10.100.100.1	
			Apply Save

Figure 105. Network Settings



*Gigabit 2 settings will “mirror” Gigabit 1 settings (except for MAC addresses) and cannot be configured separately.*

When finished making changes, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent. When the status of an Ethernet or Gigabit port changes, a Syslog entry is created describing the change.

### Network Interface Ports

The following diagram shows the location of each network interface port on the underside of the Array.

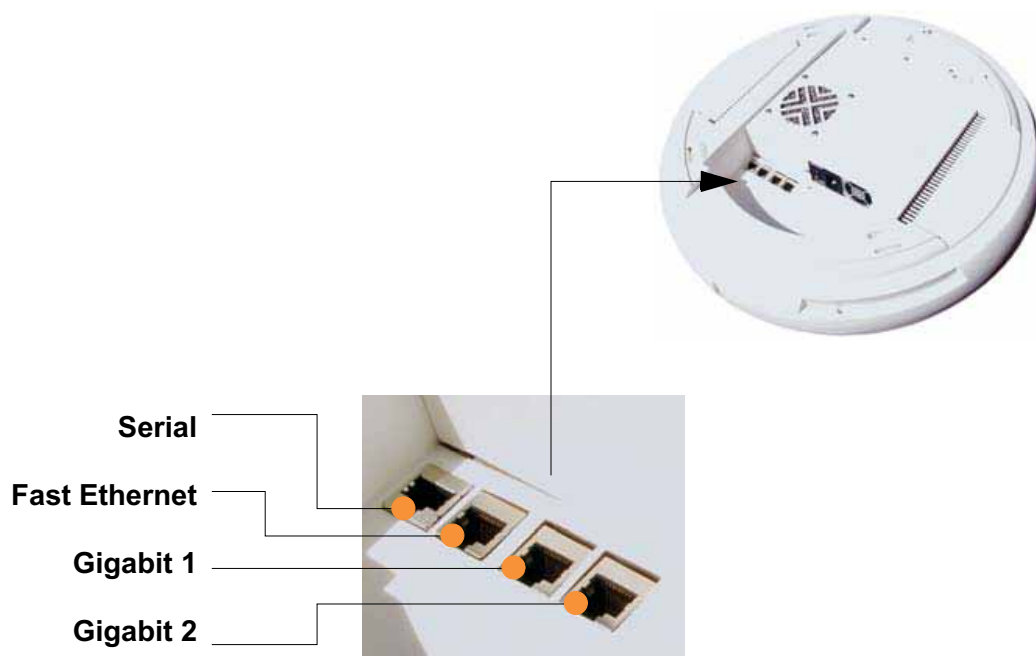


Figure 106. Network Interface Ports

### *Procedure for Configuring the Network Interfaces*

Configure the **Fast Ethernet** and **Gigabit 1** network interfaces (some **Gigabit 2** settings cannot be configured separately and will mirror **Gigabit 1**). The fields for each of these interfaces are the same, and include:

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

- a. **Active Backup (gig1/gig2 failover to each other)**—This mode provides fault tolerance and is the default mode. Gigabit 1 acts as the primary link. Gigabit2 is the backup link and is passive. Gigabit2 assumes the IP properties of Gigabit1. If Gigabit 1 fails the Array automatically fails over to Gigabit2. When a failover occurs in this mode, Gigabit2 issues gratuitous ARPs to allow it to substitute for Gigabit1 at Layer 3 as well as Layer 2. See [Figure 107 \(a\)](#).
- b. **Aggregate Traffic from gig1 & gig2 using 802.3ad**—The Array sends network traffic across both gigabit ports to increase link speed to the network. Both ports act as a single logical interface (trunk), using a load balancing algorithm to balance traffic across the ports. The destination IP address of a packet is used to determine its outgoing adapter. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. The network switch must also support 802.3ad. If a port fails, the trunk degrades gracefully—the other port still transmits. See [Figure 107 \(b\)](#).

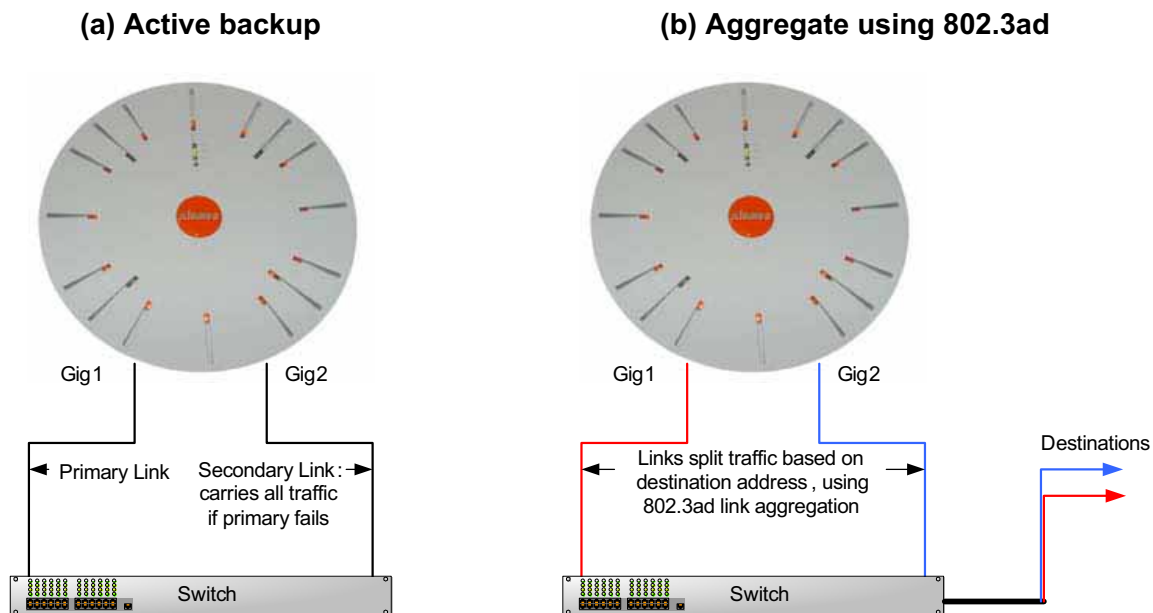


Figure 107. Port Modes (a-b)



- c. **Bridge traffic between gig1 & gig2**—Traffic received on Gigabit1 is transmitted by Gigabit2; similarly, traffic received on Gigabit2 is transmitted by Gigabit1. This allows the Array to act as a wired bridge and allows Arrays to be daisy-chained and still maintain wired connectivity. See [Figure 108 \(c\)](#).
- d. **Transmit Traffic on both gig1 & gig2**—Transmits incoming traffic on both Gigabit1 and Gigabit2. Any traffic received on Gigabit1 or Gigabit2 is sent to the onboard processor. This mode provides fault tolerance. See [Figure 108 \(d\)](#).

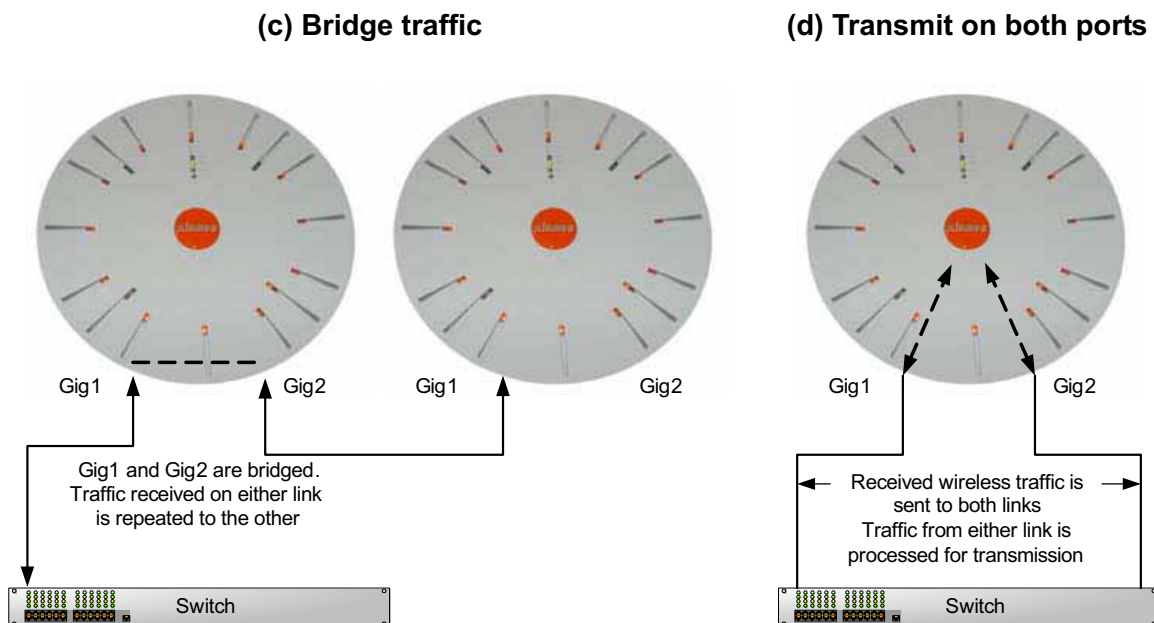
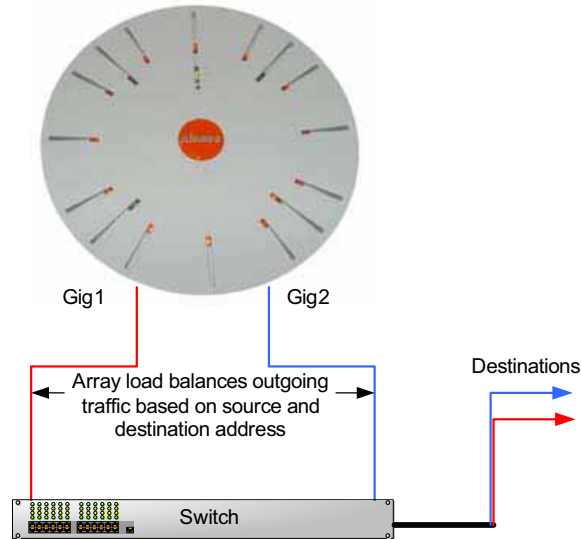


Figure 108. Port Modes (c-d)

- e. **Load balance traffic between gig1 & gig2**—This option provides trunking, similar to option (b)—**Aggregate Traffic from gig1 & gig2 using 802.3ad**, but it uses a different load balancing algorithm to determine the outgoing gigabit port. The outgoing port used is based on an exclusive OR of the source and destination MAC address. Like option (b), this mode also provides load balancing and fault tolerance. See [Figure 109 \(e\)](#).

**(e) Load balance traffic**



**(f) Mirror traffic**

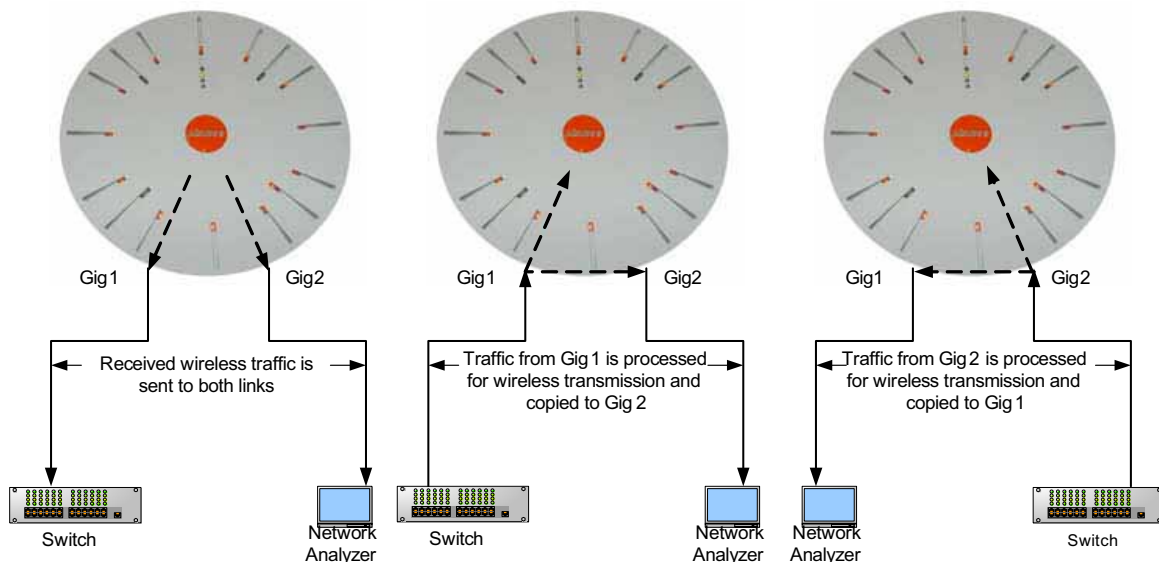


Figure 109. Port Modes (e-f)

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

processor as well as out Gigabit1. This allows a network analyzer to be plugged into one port to capture traffic for troubleshooting, while the other port provides network connectivity for data traffic. See [Figure 109 \(f\)](#).

6. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** when assigning IP addresses to the Array, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.
  - a. **IP Address:** If you selected the Static IP option, enter a valid IP address for the Array. To use any of the remote connections (Web, **SNMP**, or SSH), a valid IP address must be established.
  - b. **IP Subnet Mask:** If you selected the Static IP option, enter a valid IP address for the **subnet mask** (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
  - c. **Default Gateway:** If you selected the Static IP option, enter a valid IP address for the **default gateway**. This is the IP address of the router that the Array uses to transmit data to other networks.
7. **Static Route (IP Address/Mask):** (Fast Ethernet port only) The 10/100 Ethernet Port may be used for managing the Array out of band from the Gigabit Ethernet ports. The 10/100 port will route only management traffic, using a static route that may be configured using this field.
8. When done configuring all interfaces as desired, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

[DNS Settings](#)

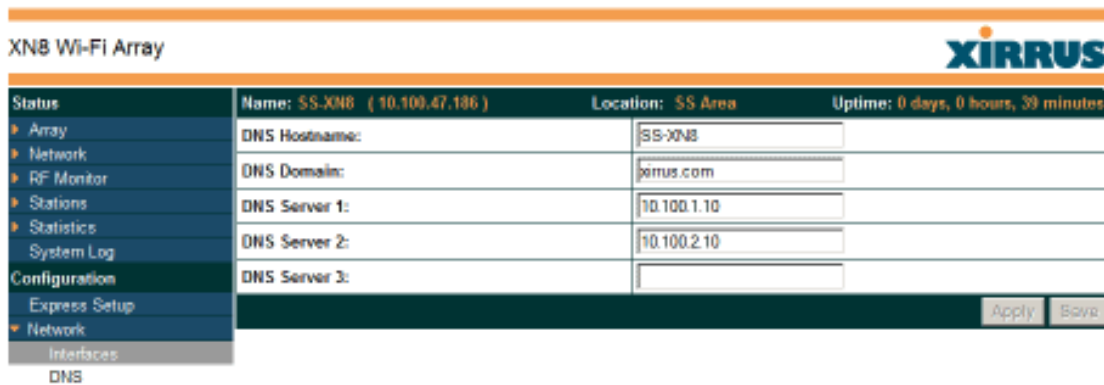
[Network](#)

[Network Statistics](#)

[Spanning Tree Status](#)

## DNS Settings

This window allows you to establish your [DNS](#) (Domain Name System) settings. At least one DNS server must be set up if you want to offer clients associating with the Array the ability to use meaningful host names instead of numerical IP addresses. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.



Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 0 days, 0 hours, 39 minutes
Array	DNS Hostname:	<input type="text" value="SS-XNB"/>	
Network	DNS Domain:	<input type="text" value="xirus.com"/>	
RF Monitor	DNS Server 1:	<input type="text" value="10.100.1.10"/>	
Stations	DNS Server 2:	<input type="text" value="10.100.2.10"/>	
Statistics	DNS Server 3:	<input type="text"/>	
System Log	<input type="button" value="Apply"/> <input type="button" value="Save"/>		
Configuration			
Express Setup			
Network			
Interfaces			
DNS			

Figure 110. DNS Settings

### *Procedure for Configuring DNS Servers*

1. **DNS Host Name:** Enter a valid DNS [host name](#).
2. **DNS Domain:** Enter the DNS [domain](#) name.
3. **DNS Server 1:** Enter the IP address of the primary DNS server.
4. **DNS Server 2 and DNS Server 3:** Enter the IP address of the secondary and tertiary DNS servers (if required).
5. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

[Network](#)

[Network Interfaces](#)

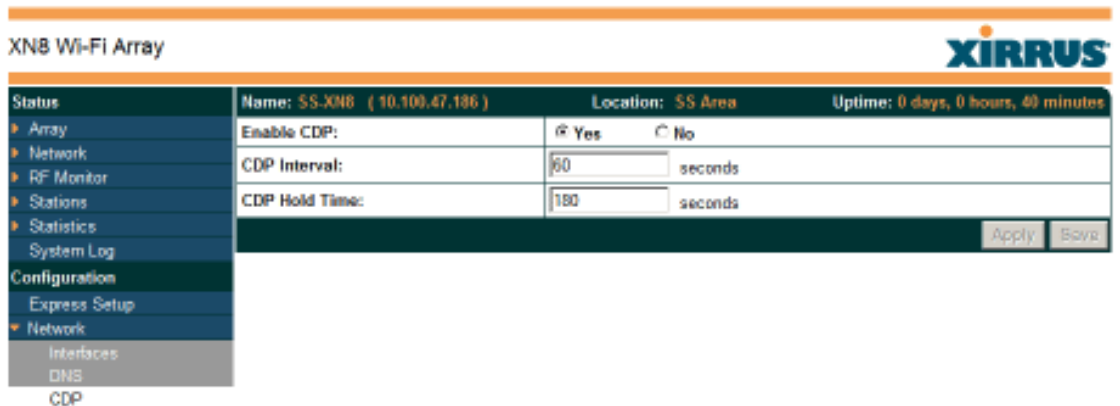
[Network Statistics](#)

[Spanning Tree Status](#)

## CDP Settings

CDP (Cisco Discovery Protocol) is a layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Wi-Fi Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors (see “CDP Neighbors” on page 141).

This window allows you to establish your CDP settings. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.



Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 0 hours, 49 minutes
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>System Log</li> <li>Configuration</li> <li>Express Setup</li> <li>▶ Network</li> <li>Interfaces</li> <li>DNS</li> <li>CDP</li> </ul>	Enable CDP: <input checked="" type="radio"/> Yes <input type="radio"/> No		
	CDP Interval:	<input type="text" value="60"/> seconds	
	CDP Hold Time:	<input type="text" value="180"/> seconds	
			<input type="button" value="Apply"/> <input type="button" value="Save"/>

Figure 111. CDP Settings

### Procedure for Configuring CDP Settings

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

*See Also*

CDP Neighbors

Network

Network Interfaces

Network Statistics

## Services

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

XN8 Wi-Fi Array							XIRRUS				
<b>Status</b>	Name: SS-XN8 ( 10.100.47.186 )		Location: SS Area		Uptime: 0 days, 0 hours, 42 minutes						
▶ Array	Time Settings Summary										
▶ Network	NTP Server Status		NTP Server 1 Address		NTP Server 2 Address						
▶ RF Monitor	Enabled		time.nist.gov		pool.ntp.org						
▶ Stations	Netflow Summary										
▶ Statistics	State		Collector Host		Collector Port						
▶ System Log	Disabled				2055						
<b>Configuration</b>	System Log Settings Summary										
▶ Express Setup	Syslog Server Status		Enabled								
▶ Network	Console Logging		Disabled		Level 6 and lower (Information and more serious)						
▶ Services	Local File		500 lines		Level 6 and lower (Information and more serious)						
▶ Time	Primary Server		10.100.47.17		Level 7 and lower (Debugging and more serious)						
▶ Netflow	Secondary Server		0.0.0.0		Level 6 and lower (Information and more serious)						
▶ System Log	Tertiary Server				Level 6 and lower (Information and more serious)						
▶ SNMP	Email SMTP Server				Level 4 and lower (Warning and more serious)						
▶ DHCP Server	SNMP Settings Summary										
▶ VLANs	SNMPv2 State		Trap Auth Failures		Trap Host IP 1		Trap Host IP 2		Trap Host IP 3		
▶ Security	Enabled		Enabled				0.0.0.0		0.0.0.0		
▶ SSIDs	SNMPv3 State		SNMPv3 Security		Trap Port 1		Trap Port 2		Trap Port 3		
▶ Groups	Enabled		SHA / AES		162		162		162		
▶ IAPs	DHCP Server Settings										
▶ WDS	DHCP Name		State		NAT		IP Range/Mask		IP Gateway		
▶ Filters	192		on		off		192.168.1.2 - 192.168.1.254 /255.255.255.0		192.168.1.1		
<b>Tools</b>	Default Lease		Maximum Lease		DNS Domain						
▶ System Tools	300		300								
▶ CLI											
▶ Logout											

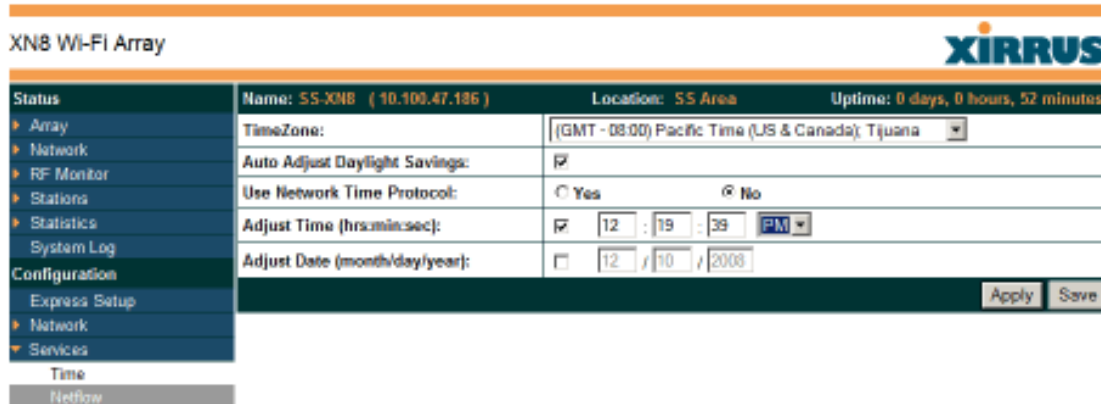
Figure 112. Services

The following sections discuss configuring services on the Array:

- “Time Settings (NTP)” on page 194
- “NetFlow” on page 196
- “System Log” on page 197
- “SNMP” on page 200
- “DHCP Server” on page 203

## Time Settings (NTP)

This window allows you to manage the Array's time settings, including synchronizing the Array's clock with a universal clock from an NTP (Network Time Protocol) server. Synchronizing the Array's clock with an NTP server ensures that Syslog time-stamping is maintained across all units.



Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 0 days, 0 hours, 52 minutes
Array	TimeZone:	[(GMT - 08:00) Pacific Time (US & Canada), Tijuana]	
Network	Auto Adjust Daylight Savings:	<input checked="" type="checkbox"/>	
RF Monitor	Use Network Time Protocol:	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Stations	Adjust Time (hrs:min:sec):	<input checked="" type="checkbox"/> 12 : 19 : 39 PM	
Statistics	Adjust Date (month/day/year):	<input type="checkbox"/> 12 / 10 / 2008	
System Log	Apply Save		
Configuration			
Express Setup			
Network			
Services			
Time			
Refresh			

Figure 113. Time Settings (Manual Time)

### Procedure for Managing the Time Settings

1. **Time Zone:** Select the time zone you want to use (normally your local time zone) from the pull-down list.
2. **Auto Adjust Daylight Savings:** Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
3. **Use Network Time Protocol:** select whether to set time manually or use NTP to manage system time.
4. **Setting Time Manually**
  - a. **Adjust Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes, seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).

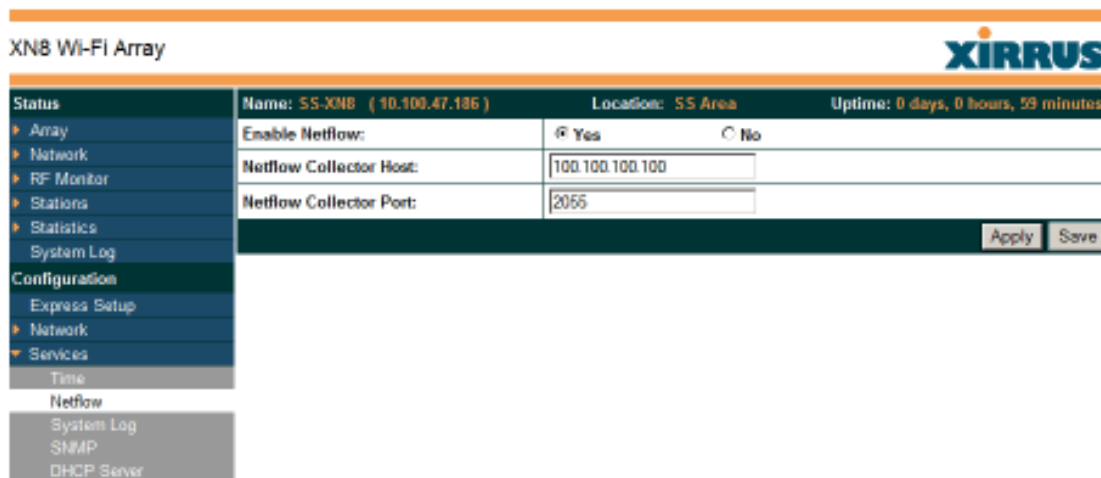




## NetFlow

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

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



XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS-XNB ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 0 hours, 59 minutes
Array	Enable Netflow:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Network	Netflow Collector Host:	<input type="text" value="100.100.100.100"/>	
RF Monitor	Netflow Collector Port:	<input type="text" value="2055"/>	
Stations	<input type="button" value="Apply"/> <input type="button" value="Save"/>		
Statistics			
System Log			
Configuration			
Express Setup			
Network			
Services			
Time			
Netflow			
System Log			
SNMP			
DHCP Server			

Figure 115. NetFlow

### *Procedure for Configuring NetFlow*

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

### System Log

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

Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 1 hour, 1 minute
Array	Enable Syslog Server:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Network	Console Logging:	<input type="radio"/> Yes	<input checked="" type="radio"/> No
RF Monitor	Local File Size (1-500):	<input type="text" value="500"/>	
Stations	Primary Server Address (Domain or IP):	<input type="text" value="10.100.100.117"/>	
Statistics	Secondary Server Address (Domain or IP):	<input type="text" value="10.100.101.117"/>	
System Log	Tertiary Server Address (Domain or IP):	<input type="text"/>	
Configuration	Email SMTP Address (Domain or IP):	<input type="text" value="mail.lyzcorp.com"/>	
Express Setup	Email SMTP User:	<input type="text" value="networkAdmin"/>	
Network	Email SMTP Password:	<input type="password" value="*****"/>	
Services	Email SMTP From:	<input type="text" value="Array12345"/>	
Time	Email SMTP To:	<input type="text" value="networkAdmin"/>	
Netflow	Syslog Levels		
System Log	Console Logging:	<input type="text" value="Information and more serious"/>	
SNMP	Local File:	<input type="text" value="Information and more serious"/>	
DHCP Server	Primary Server:	<input type="text" value="Information and more serious"/>	
VLANs	Secondary Server:	<input type="text" value="Information and more serious"/>	
Security	Tertiary Server:	<input type="text" value="Information and more serious"/>	
SSIDs	Email SMTP Server:	<input type="text" value="Warning and more serious"/>	
Groups		<input type="button" value="Apply"/> <input type="button" value="Save"/>	
IAPs			
WDS			
Filters			
Tools			
System Tools			
CLI			
Logout			

Figure 116. System Log

### Procedure for Configuring Syslog

- 1. Enable Syslog Server:** Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.
- 2. Console Logging:** If you enabled Syslog, select whether or not to echo Syslog messages to the console as they occur. If you enable console logging, be sure to set the Console Logging level (see [Step 7](#) below).

3. **Local File Size (1-500):** Enter a value in this field to define how many Syslog records are retained locally on the Array's internal Syslog file. The default is 500.
4. **Primary Server Address (Domain or IP):** If you enabled Syslog, enter the domain name or IP address of the primary Syslog server.
5. **Secondary/Tertiary Server Address (Domain or IP):** If you enabled Syslog, you may enter the domain name or IP address of one or two additional Syslog servers to which messages will also be sent. (Optional)
6. **Email Notification:** The following parameters allow you to send an email to a designated address each time a Syslog message is generated. The email will include the text of the Syslog message.
  - a. **Email SMTP Address (Domain or IP):** The domain name or the IP address of the SMTP server to be used for sending the email. Note that this specifies the mail server, **not** the email recipient.
  - b. **Email SMTP User/Email SMTP Password:** Specify a user name and password for logging in to an account on the mail server designated in [Step a](#).
  - c. **Email SMTP From:** Specify the "From" email address to be displayed in the email.
  - d. **Email SMTP To:** Specify the entire email address of the recipient of the email notification.
7. **Syslog Levels:** For each of the Syslog destinations, choose your preferred level of Syslog reporting from the pull-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.
  - a. **Console Logging:** For messages to be echoed to the console, the default level is **Critical and more serious**. This prevents large numbers of non-critical messages from being displayed on the console. If you set this level too low, the volume of messages may make it very difficult to work with the CLI or view other output on the console.



## SNMP

This window allows you to enable or disable SNMP v2 and SNMP v3 and define the SNMP parameters. SNMP v2 allows remote management of the Array by the Xirrus Management System (XMS) and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, neither, or both. If you enable both, be aware that data and keys are not encrypted when SNMPv2 is used.

***NOTE:** If you are managing your Arrays with XMS (the Xirrus Management System), it is very important to use SNMP v2 and the correct **Read-Write Community String** for proper operation of XMS with the Array. Both XMS and the Array must have the same value for this string.*

XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS-XN8 [ 10.100.47.188 ]	Location: SS Area	Uptime: 0 days, 1 hour, 6 minutes
Array	SNMPv2 Settings		
Network	Enable SNMPv2:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
RF Monitor	Read-Write Community String:	*****	
Stations	Read-Only Community String:	*****	
Statistics	SNMPv3 Settings		
System Log	Enable SNMPv3:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Configuration	Authentication:	<input checked="" type="radio"/> SHA	<input type="radio"/> MD5
Express Setup	Privacy:	<input checked="" type="radio"/> AES	<input type="radio"/> DES
Network	Context Engine ID:	80005215030007d0bb380	
Services	Read-Write Username:	xirrus-rw	
Time	Read-Write Authentication Password:	*****	
Netflow	Read-Write Privacy Password:	*****	
System Log	Read-Only Username:	xirrus-ro	
SNMP	Read-Only Authentication Password:	*****	
DHCP Server	Read-Only Privacy Password:	*****	
VLANs	SNMP Trap Settings		
Security	Trap Host 1 IP Address:	100.100.100.10	Port: 162
SSIDs	Trap Host 2 IP Address:	0.0.0.0	Port: 162
Groups	Trap Host 3 IP Address:	0.0.0.0	Port: 162
IAPs	Trap Host 4 IP Address:	0.0.0.0	Port: 162
WDS	Send Auth Failure Traps:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Filters	Apply Save		
Tools			
System Tools			
CU			
Logout			
Log Messages			
Critical			
Warning			

Figure 117. SNMP

### *Procedure for Configuring SNMP*

1. **Enable SNMPv2:** Choose **Yes** to enable SNMP v2 functionality, or choose **No** to disable this feature. When used in conjunction with the Xirrus Management System, SNMP v2 (**not** SNMP v3) must be enabled on each Array to be managed with XMS. The default for this feature is **Yes** (enabled).
2. **SNMP Read-Write Community String:** Enter the read-write community string. The default is **xirrus**.
3. **SNMP Read-Only Community String:** Enter the read-only community string. The default is **xirrus\_read\_only**.
4. **Enable SNMPv3:** Choose **Yes** to enable SNMP v3 functionality, or choose **No** to disable this feature. The default for this feature is **Yes** (enabled).
5. **Authentication:** Select the desired method for authenticating SNMPv3 packets: **SHA** (Secure Hash Algorithm) or **MD5** (Message Digest Algorithm 5).
6. **Privacy:** Select the desired method for encrypting data: **DES** (Data Encryption Standard) or the stronger **AES** (Advanced Encryption Standard).
7. **Context Engine ID:** The unique identifier for this SNMP server. We recommend that you do not change this value. The Context Engine ID must be set if data collection is to be done via a proxy agent. This ID helps the proxy agent to identify the target agent from which data is to be collected.
8. **SNMP Read-Write Username:** Enter the read-write user name. This username and password allow configuration changes to be made on the Array. The default is **xirrus-rw**.
9. **SNMP Read-Write Authentication Password:** Enter the read-write password for authentication (i.e., logging in). The default is **xirrus-rw**.
10. **SNMP Read-Write Privacy Password:** Enter the read-write password for privacy (i.e., a key for encryption). The default is **xirrus-rw**.

11. **SNMP Read-Only Username:** Enter the read-only user name. This username and password do not allow configuration changes to be made on the Array. The default is **xirrus-ro**.
12. **SNMP Read-Only Authentication Password:** Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.
13. **SNMP Read-Only Privacy Password:** Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.
14. **SNMP Trap Host IP Address:** Enter the **IP Address** or domain name, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps.
15. **Send Auth Failure Traps:** Choose **Yes** to log authentication failure traps or **No** to disable this feature.
16. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

Services

System Log

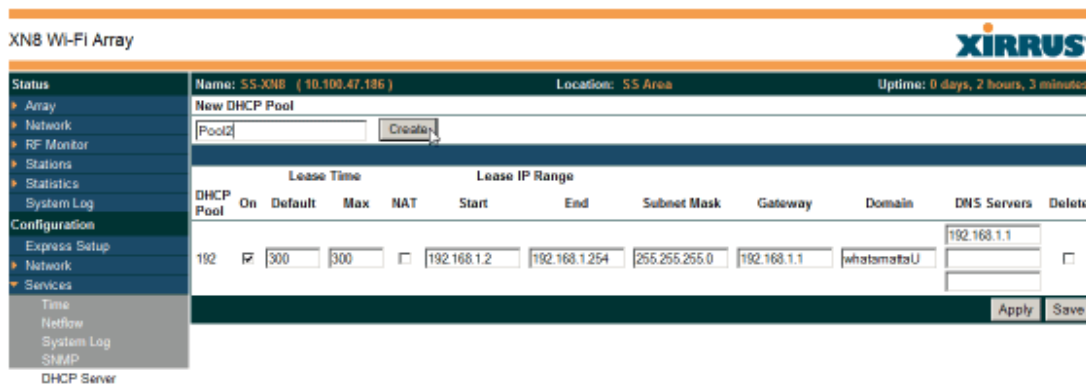
Time Settings (NTP)



## DHCP Server

This window allows you to create, modify and delete DHCP (Dynamic Host Configuration Protocol) pools and enable or disable DHCP server functionality. DHCP allows the Array to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network.

If you enable the DHCP server, you need to define the DHCP lease time (default and maximum) and establish the IP address range that the DHCP server can use.



The screenshot shows the DHCP Management interface for an XN8 Wi-Fi Array. The interface includes a navigation menu on the left with options like Array, Network, RF Monitor, Stations, Statistics, System Log, Configuration, Express Setup, Network, Services, Time, Netflow, System Log, SNMP, and DHCP Server. The main content area displays the 'New DHCP Pool' form and a table of existing DHCP pools.

DHCP Pool	On	Default	Max	NAT	Start	End	Subnet Mask	Gateway	Domain	DNS Servers	Delete
102	<input checked="" type="checkbox"/>	300	300	<input type="checkbox"/>	192.168.1.2	192.168.1.254	255.255.255.0	192.168.1.1	whatamattaU	192.168.1.1	<input type="checkbox"/>

Figure 118. DHCP Management

### Procedure for Configuring the DHCP Server

- 1. New Internal DHCP Pool:** Enter a name for the new DHCP pool, then click on the **Create** button. The new pool ID is added to the list of available DHCP pools.
- 2. On:** Click this checkbox to make this pool of addresses available, or clear it to disable the pool.
- 3. Lease Time—Default:** This field defines the default DHCP lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
- 4. Lease Time—Max:** Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.

5. **Network Address Translation (NAT):** Check this box to enable the Network Address Translation feature.
6. **Lease IP Range—Start:** Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End:** Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask:** Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway:** If necessary, enter the IP address of the gateway.
10. **Domain:** Enter the DNS domain name. See also, [“DNS Settings” on page 190](#).
11. **DNS Servers (1 to 3):** Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. See also, [“DNS Settings” on page 190](#).
12. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

[DHCP Leases](#)

[DNS Settings](#)

[Network Map](#)

## VLANs

This is a status-only window that allows you to review the current status of assigned VLANs. A VLAN (Virtual LAN) is comprised of a group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN ([Step 1 page 207](#)).

XN8 Wi-Fi Array										
Status		Name: SS-XN8 ( 10.100.47.186 )			Location: SS Area			Uptime: 0 days, 2 hours, 10 minutes		
Default Route VLAN:										
Native (Untagged):										
VLAN Name	Number	Management	DHCP	IP Address	Subnet Mask	Gateway	Tunnel Server	Port	State	
VoIP	12	disabled	disabled	10.10.10.10	255.255.255.0	10.10.10.1	10.10.10.8	0	down	
Finance	5	disabled	enabled							

Figure 119. VLANs



*For a complete discussion of implementing Voice over Wi-Fi on the Array, see the [Xirrus Voice over Wi-Fi Application Note](#) in the [Xirrus Library](#).*

## Understanding Virtual Tunnels

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

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

### *Virtual Tunnel Server (VTS)*

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from [vtun.sourceforge.net](http://vtun.sourceforge.net). To enable the Array to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in [Step 10](#) on [page 208](#).

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

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

### *Client-Server Interaction*

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

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

## VLAN Management

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

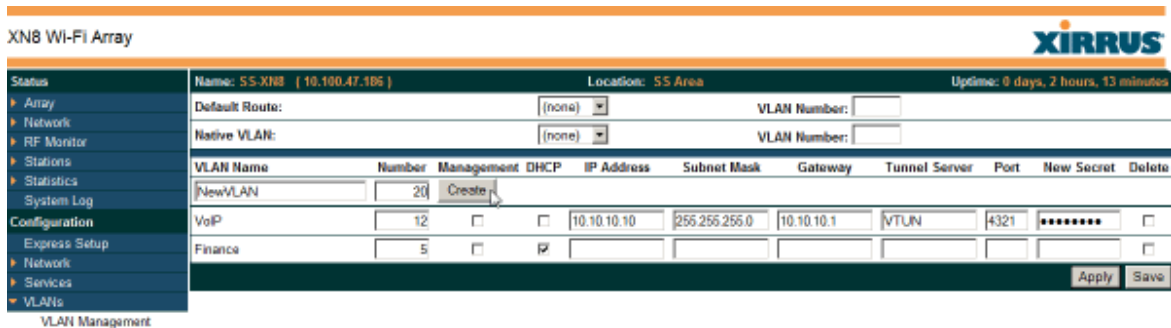


Figure 120. VLAN Management



*The Wi-Fi Array supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Array dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Array (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (Figure 81 on page 151)*

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

### Procedure for Managing VLANs

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

3. **New VLAN Name/Number:** Enter a name and number for the new VLAN in this field, then click on the **Create** button. The new VLAN is added to the list.
4. **VLAN Number:** Enter a number for this VLAN (1-4094).
5. **Management:** Check this box to allow management over this VLAN.
6. **DHCP:** Check this box if you want the DHCP server to assign the IP address, subnet mask and gateway address to the VLAN automatically, otherwise you must go to the next step and assign these parameters manually.
7. **IP Address:** If the DHCP option is disabled, enter a valid IP address for this VLAN association.
8. **Subnet Mask:** If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.
9. **Gateway:** If the DHCP option is disabled, enter the IP gateway address for this VLAN association.
10. **Tunnel Server:** If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see [“Understanding Virtual Tunnels”](#) on page 205.
11. **Port:** If this VLAN is to be tunneled, enter the port number of the tunnel server.
12. **New Secret:** Enter the password expected by the tunnel server.
13. **Delete:** To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.
14. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

VLAN Statistics  
VLANs

## Security

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

XN8 Wi-Fi Array			
Status	Name: SS-XN8 ( 10.100.47.106 )	Location: SS Area	Uptime: 0 days, 2 hours, 38 minutes
Administration	Accounts	Full Access	Read Only
Network	1	1	0
RF Monitor	Access Control List		
Stations	Enabled	Entries	List Type
Statistics	No	0	N/A
System Log	Management Control		
Configuration	SSH Enabled	Telnet Enabled	HTTPS Enabled
Express Setup	Yes	No	Yes
Network	Global Security		
Services	TKIP Enabled	AES Enabled	PSK Enabled
VLANs	Yes	Yes	No
Security	Radius		
Admin Management	Server In Use	External Primary Server	External Primary Port
Admin RADIUS	external	radius1	1812
Management Control	Internal Radius Users		
Access Control List	0		
Global Settings			
External Radius			
Internal Radius			
Rogue Control List			

Figure 121. Security

For additional information about wireless network security, refer to:

- “Security Planning” on page 70
- “Understanding Security” on page 210
- The Security section of “Frequently Asked Questions” on page 398.

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

- “Certificates and Connecting Securely to the WMI” on page 213

Security settings are configured with the following windows:

- “Admin Management” on page 215

- “Admin RADIUS” on page 216
- “Management Control” on page 219
- “Access Control List” on page 223
- “Global Settings” on page 225
- “External Radius” on page 228
- “Internal Radius” on page 231
- “Rogue Control List” on page 233

### Understanding Security

The Xirrus Wi-Fi Array incorporates many configurable security features. After initially installing an Array, always change the default administrator password (the default is admin), and choose a strong replacement password (containing letters, numbers and special characters). See also, “[See Also](#)” on page 126. When appropriate, issue read only administrator accounts.

Other security considerations include:

- **SSH versus Telnet:** Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit’s Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. SSH-2 provides stronger security than SSH-1. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing:** The optional Xirrus Management System (XMS) offers powerful management features for small or large Xirrus Wi-Fi deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.
- **Choosing an encryption method:** Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The Array allows you to establish the following data encryption configuration options:
  - **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are



required to use a VPN connection through a secure SSH utility, like PuTTY.

- **WEP (Wired Equivalent Privacy)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
- **WPA (Wi-Fi Protected Access) and WPA2**—these are much stronger encryption modes than WEP, using TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) to encrypt data.

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

AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, WPA2 with AES is highly recommended for Enterprise networks.

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

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see “[SSID Management](#)” on page 240). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security >Global Settings** window under **WPA Settings** (see “[Global Settings](#)” on page 225).

- **Choosing an authentication method:** User authentication ensures that users are who they say they are. For this purpose, the Array allows you to choose between the following user authentication methods:

- **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the Array.

This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.

- **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the Wi-Fi Array) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

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

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

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

## Certificates and Connecting Securely to the WMI

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

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

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

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

### Using the Array's Default Certificate

The Array's certificate is signed by a Xirrus CA that is customized for your Array and its current host name. By default, browsers will not trust the Array's certificate. You may import the Xirrus certificate to instruct the browser to trust the Xirrus CA on all future connections to Arrays. The certificate for the Xirrus CA is available on the Array, so that you can import it into your browser's cache of trusted CAs (right alongside VeriSign, for example). On the [Management Control](#) window of the WMI you will see the `xirrus-ca.crt` file. (Figure 122)

<ul style="list-style-type: none"> <li>Security</li> <li>Admin Management</li> <li>Admin RADIUS</li> <li>Management Control</li> <li>Access Control List</li> <li>Global Settings</li> <li>External Radius</li> <li>Internal Radius</li> <li>Rogue Control List</li> <li>SSIDs</li> <li>Groups</li> <li>IAPs</li> <li>WDS</li> </ul>	Enable Management:	<input checked="" type="radio"/> Yes <input type="radio"/> No
	Connection Timeout 30-100000 (Seconds):	<input type="text" value="30000"/>
	<b>HTTPS</b>	
	Connection Timeout 30-100000 (Seconds):	<input type="text" value="30000"/>
	Port:	<input type="text" value="443"/>
	Import Xirrus Authority Into Browser:	<input type="text" value="xirrus-ca.crt"/>
	HTTPS (X.509) Certificate Signed By	Xirrus
	<b>External Certification Authority</b>	
	Download Certificate Signing Request	SS-Array.csr
	Upload Signed Certificate:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>

Figure 122. Import Xirrus Certificate Authority

By clicking and opening this file, you can follow your browser's instructions and import the Xirrus CA into your CA cache (see [page 221](#) for more information). This instructs your browser to trust any of the certificates signed by the Xirrus CA, so that when you connect to any of our Arrays you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the Array. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for 'hostname'.

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

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

### Using an External Certificate Authority

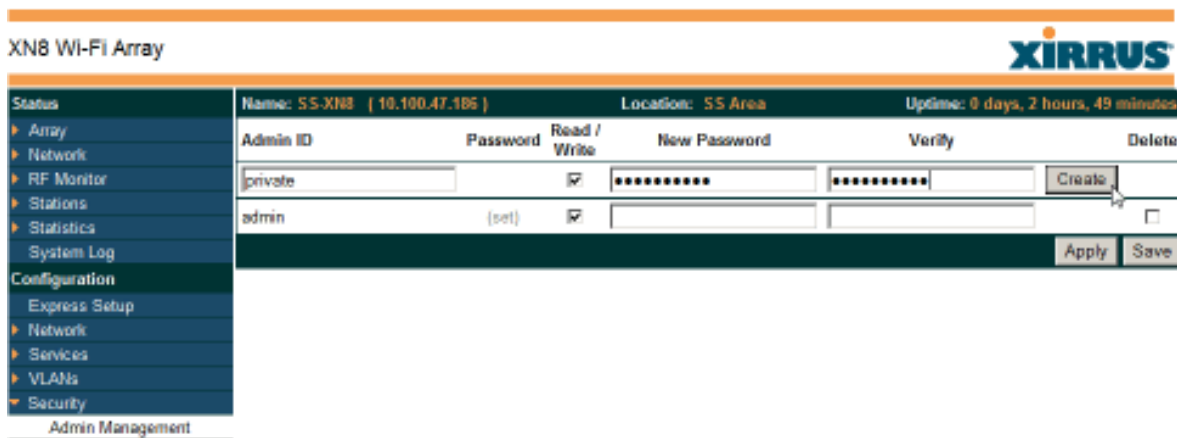
If you prefer, you may install a certificate on your Array signed by an outside CA.

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

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the Array after you obtain it from the CA. This certificate will be tied to the Array's host name and private key. See [“External Certification Authority”](#) on page 222 for more details.

## Admin Management

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



Admin ID	Password	Read / Write	New Password	Verify	Delete
private		<input checked="" type="checkbox"/>	*****	*****	<input type="checkbox"/>
admin	(set)	<input checked="" type="checkbox"/>			<input type="checkbox"/>

Figure 123. Admin Management

### *Procedure for Creating or Modifying Network Administrator Accounts*

1. **Admin ID:** Enter the login name for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive. For special characters that may be used, see [“See Also”](#) on page 126.
2. **Read/Write:** Choose **Read/Write** if you want to give this administrator ID full read/write privileges, or choose **Read** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations.
3. **User Password:** Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive. For special characters that may be used, see [“See Also”](#) on page 126.

4. **Verify Password:** Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).
5. Click on the **Create** button to add this administrator ID to the list.
6. Click **Apply** to apply modified settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

[External Radius](#)

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

[Internal Radius](#)

[Management Control](#)

[Security](#)

## **Admin RADIUS**

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

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

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

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Service-Type** attribute. To grant read-write permission, configure the RADIUS server to send back the Service-Type attribute with a value of **Administrative**. To grant read-only permission, the RADIUS server should send the Service-Type attribute with a value of **NAS Prompt**.

When configuring administrator accounts on the RADIUS server, you must observe the same restrictions for length and legal characters as when creating these accounts on the Array using the [Admin Management](#) window: the user name and password must be between 5 and 50 characters, inclusive. For special characters that may be used, see [“See Also” on page 126](#).

Use this window to enable/disable administrator authentication via RADIUS, and to set up primary and secondary servers to use for authentication of administrators attempting to log in to the Array. When finished, click on the **Save** button to save your changes.


XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 0 days, 2 hours, 59 minutes
Array	Admin RADIUS Settings		
Network	Enable Admin RADIUS:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
RF Monitor	Timeout (seconds):	<input type="text" value="600"/>	
Stations	Admin RADIUS Primary Server		
Statistics	Host Name / IP Address:	<input type="text" value="100.100.100.100"/>	
System Log	Port Number:	<input type="text" value="1812"/>	
Configuration	Shared Secret / Verify Secret:	<input type="password" value="*****"/> <input type="password" value="*****"/>	
Express Setup	Admin RADIUS Secondary Server		
Network	Host Name / IP Address:	<input type="text"/>	
Services	Port Number:	<input type="text" value="1812"/>	
VLANs	Shared Secret / Verify Secret:	<input type="password"/> <input type="password"/>	
Security			
Admin Management			
Admin RADIUS			
Management Control			
Access Control List			
			<input type="button" value="Apply"/> <input type="button" value="Save"/>

Figure 124. Admin RADIUS

---

### *Procedure for Configuring Admin RADIUS*

1. **Admin RADIUS Settings:**
  - a. **Enable Admin RADIUS:** Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.
  - b. **Timeout (seconds):** Define the maximum idle time (in seconds) before the RADIUS server's session times out. The default is 600 seconds.
2. **Admin RADIUS Primary Server:** This is the RADIUS server that you intend to use as your primary server.
  - a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
  - b. **Port Number:** Enter the port number of this RADIUS server. The default is 1812.
  - c. **Shared Secret / Verify Secret:** Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.

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



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

### Management Control

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

XNB Wi-Fi Array		XIRRUS	
Status	Name: SS-XNB ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 3 hours, 1 minute
Array	SSH	Enable Management:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Network	Connection Timeout 30-100000 (Seconds):		<input type="text" value="300"/>
RF Monitor	Port:		<input type="text" value="22"/>
Stations	Telnet	Enable Management:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Statistics	Connection Timeout 30-100000 (Seconds):		<input type="text" value="300"/>
System Log	Port:		<input type="text" value="23"/>
Configuration	Serial	Enable Management:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Express Setup	Connection Timeout 30-100000 (Seconds):		<input type="text" value="300"/>
Network	Port:		<input type="text" value="300"/>
Services	HTTPS	Connection Timeout 30-100000 (Seconds):	<input type="text" value="300"/>
WLANs	Port:		<input type="text" value="443"/>
Security	Import Xirrus Authority Into Browser:		<input type="text" value="xirrus-ca.crt"/>
Admin Management	HTTPS (X.509) Certificate Signed By		<input type="text" value="Xirrus"/>
Admin RADIUS	External Certification Authority		
Management Control	Download Certificate Signing Request		<input type="text" value="SS-XNB.csr"/>
Access Control List	Upload Signed Certificate:		<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Global Settings	Common Name:		<input type="text" value="SS-XNB"/>
External Radius	Organization Name:		<input type="text"/>
Internal Radius	Organizational Unit Name:		<input type="text"/>
Radius Control List	Locality (City):		<input type="text"/>
SSIDs	State or Province:		<input type="text"/>
Groups	Country Name (2 Letter Code):		<input type="text"/>
IAPs	Email Address:		<input type="text"/>
WDS	Create New Certificate Signing Request		<input type="button" value="Create"/>
Filters			<input type="button" value="Apply"/> <input type="button" value="Save"/>
Tools			
System Tools			
CLI			
Logout			
Log Messages			
Critical			
Warning			
Information			

Figure 125. Management Control

---

*Procedure for Configuring Management Control***1. SSH:**

- a. Enable Management:** Choose **Yes** to enable management of the Array over a Secure Shell (SSH-2) connection, or **No** to disable this feature. Be aware that only SSH-2 connections are supported by the Array. SSH clients used for connecting to the Array must be configured to use SSH-2.
- b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
- c. Port:** Enter a value in this field to define the port used by SSH. The default port is 22.

**2. Telnet:**

- a. Enable Management:** Choose **Yes** to enable Array management over a Telnet connection, or **No** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.
- b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
- c. Port:** Enter a value in this field to define the port used by Telnet. The default port is 23.

**3. Serial**

- a. Enable Management:** Choose **Yes** to enable management of the Array via a serial connection, or choose **No** to disable this feature.
- b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

#### 4. HTTPS

- a. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.
- b. **Port:** Enter a value in this field to define the port used by SSH. The default port is 443.
- c. **Import Xirrus Authority into Browser:** This feature imports the Xirrus Certificate Authority (CA) into your browser (for a discussion, please see [“Certificates and Connecting Securely to the WMI”](#) on page 213). Click the link ([xirrus-ca.crt](#)), and then click **Open** to view or install the current Xirrus CA certificate. Click **Install Certificate** to start your browser’s Certificate Install Wizard. We recommend that you use this process to install Xirrus as a root authority in your browser.

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

- You must have assigned a host name to the Array and rebooted at some time after that.
  - Use **Import Xirrus Authority into Browser**
  - Access WMI by using the host name of the Array rather than its IP address.
- d. **HTTPS (X.509) Certificate Signed By:** This read-only field shows the signing authority for the current certificate.

## 5. External Certification Authority

This Step and [Step 6](#) allow you to obtain a certificate from an external authority and install it on an Array. “[Using an External Certificate Authority](#)” on [page 214](#) discusses reasons for using an external CA.

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

- If you don't already have the certificate from the external (non-Xirrus) Certificate Authority, see [Step 6](#) to create a request for a certificate.
- Use [Step 5a](#) to review the request and copy its text to send to VeriSign.
- When you receive the new certificate from VeriSign, upload it to the Array using [Step 5b](#).

External Certification Authority has the following fields:

- a. Download Certificate Signing Request:** After creating a certificate signing request (.csr file—[Step 6](#)), click the **View** button to review it. If it is satisfactory, click the name of the .csr file to display the text of the request. You can then copy this text and use it as required by the CA. You may also click on the filename of the .csr file to download it to your local computer.
  - b. Upload Signed Certificate:** To use a custom certificate signed by an authority other than Xirrus, use the **Browse** button to locate the certificate file, then click **Upload** to copy it to the Array. The Array's web server will be restarted and will pick up the new certificate. This will terminate any current web sessions, and you will need to reconnect and re-login to the Array.
- 6. To create a Certificate Signing Request**
- a.** Fill in the fields in this section: **Common Name, Organization Name, Organizational Unit Name, Locality (City), State or Province, Country Name, and Email Address.** Spaces may be used in any of the fields, except for Common Name, Country Name, or Email

Address. Click the **Create** button to create the certificate signing request. See [Step 5](#) above to use this request.

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

*See Also*

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

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

[Admin Management](#)

[External Radius](#)

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

[Internal Radius](#)

[Access Control List](#)

[Security](#)

### Access Control List

This window allows you to create new station access lists, delete existing lists, and add/remove MAC addresses. When finished, click on the **Save** button to save your changes.

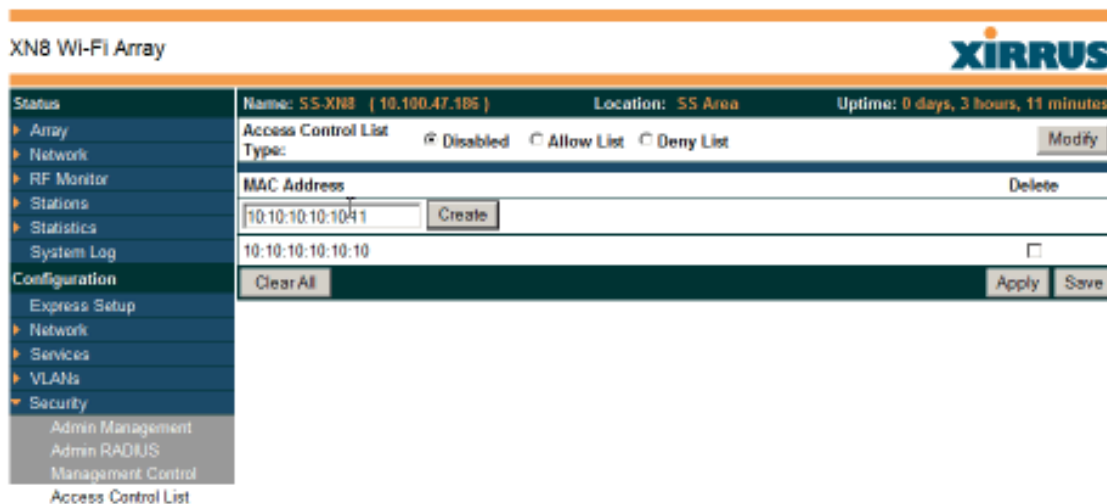


Figure 126. Access Control List

### *Procedure for Configuring Access Control Lists*

1. **Access Control List Type:** Select **Disabled** to disable the Access Control List, or select the Access Control List type—either **Allow List** or **Deny List**. Then click **Apply** to apply your changes.
  - **Allow List:** Only allows these MAC addresses to associate to the Array.
  - **Deny List:** Allows all MAC addresses except the addresses defined in this list.



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

2. **MAC Address:** If you want to add a MAC address to the ACL, enter the new MAC address here, then click on the **Create** button. The MAC address is added to the ACL.
3. **Delete:** You can delete selected MAC addresses from this list by checking their **Delete** buttons, then clicking **Apply** or **Save**.
4. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

External Radius

Global Settings (IAP)

Internal Radius

Management Control

Security

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

### Global Settings

This window allows you to establish the security parameters for your wireless network, including WEP, WPA, WPA2 and RADIUS authentication. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

For additional information about wireless network security, refer to “Security Planning” on page 70 and “Understanding Security” on page 210.

**XN8 Wi-Fi Array** **XIRRUS**

Name: SS-XN8 ( 10.100.47.186 )      Location: SS Area      Uptime: 0 days, 3 hours, 25 minutes

<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>System Log</li> <li><b>Configuration</b></li> <li>  Express Setup</li> <li>  ▶ Network</li> <li>  ▶ Services</li> <li>  ▶ VLANs</li> <li>  ▶ Security</li> <li>    Admin Management</li> <li>    Admin RADIUS</li> <li>    Management Control</li> <li>    Access Control List</li> <li>    <b>Global Settings</b></li> <li>    External Radius</li> <li>    Internal Radius</li> <li>    Rogue Control List</li> <li>  ▶ SSIDs</li> <li>  ▶ Groups</li> <li>  ▶ IAPs</li> <li>  ▶ WDS</li> <li>  ▶ Filters</li> <li>Tools</li> </ul>	RADIUS Server Mode:	<input type="radio"/> Internal <input checked="" type="radio"/> External		
	<b>WPA Settings:</b>			
	TKIP Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
	AES Enabled:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
	WPA Group Rekey Time (seconds):	<input type="text"/> Never: <input checked="" type="checkbox"/>		
	PSK Authentication:	<input type="radio"/> Yes <input checked="" type="radio"/> No		
	WPA Preshared Key / Verify Key:	<input type="text"/> <input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal		
	EAP Authentication:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
	<b>WEP Settings:</b>			
	Encryption Key 1 / Verify Key 1:	<input type="text"/> <input checked="" type="radio"/> ASCII <input checked="" type="radio"/> 40 bit (WEP-64) <input type="text"/> <input type="radio"/> Hexadecimal <input type="radio"/> 104 bit (WEP-128)		
	Encryption Key 2 / Verify Key 2:	<input type="text"/> <input checked="" type="radio"/> ASCII <input type="radio"/> 40 bit (WEP-64) <input type="text"/> <input type="radio"/> Hexadecimal <input checked="" type="radio"/> 104 bit (WEP-128)		
	Encryption Key 3 / Verify Key 3:	<input type="text"/> <input type="radio"/> ASCII <input type="radio"/> 40 bit (WEP-64) <input type="text"/> <input type="radio"/> Hexadecimal <input type="radio"/> 104 bit (WEP-128)		
	Encryption Key 4 / Verify Key 4:	<input type="text"/> <input type="radio"/> ASCII <input type="radio"/> 40 bit (WEP-64) <input type="text"/> <input type="radio"/> Hexadecimal <input type="radio"/> 104 bit (WEP-128)		
	Default Key:	<input type="text" value="Key 2"/>		
<input type="button" value="Apply"/> <input type="button" value="Save"/>				

Figure 127. Global Settings (Security)

### *Procedure for Configuring Network Security*

1. **RADIUS Server Mode:** Choose the RADIUS server mode you want to use, either Internal or External. Parameters for these modes are configured in “External Radius” on page 228 and “Internal Radius” on page 231.

#### **WPA Settings**

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

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



## WEP Settings

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

- 8. Key Mode / Length:** If you enabled WEP, choose the mode (either ASCII or Hex) and the desired key length (either 40 or 128) from the pull-down lists.

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

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

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

- 9. Encryption Key 2 to 4/ Verify Key 2 to 4/ Key Mode/Length** (optional): If desired, enter up to four encryption keys, in the same way that you entered the first key.
- 10. Default Key:** Choose which key you want to assign as the default key. Make your selection from the pull-down list.
- 11.** Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.



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

### See Also

Admin Management

External Radius

Internal Radius

Access Control List

Management Control

Security

Security Planning  
SSID Management

**External Radius**

This window allows you to define the parameters of an external RADIUS server for user authentication. To set up an external RADIUS server, you must choose **External** as the RADIUS server mode in Global Settings. Refer to “Global Settings” on page 225.


Status	Name: SS-XNB ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 3 hours, 30 minutes
<ul style="list-style-type: none"> <li>Array</li> <li>Network</li> <li>RF Monitor</li> <li>Stations</li> <li>Statistics</li> <li>System Log</li> <li><b>Configuration</b> <ul style="list-style-type: none"> <li>Express Setup</li> <li>Network</li> <li>Services</li> <li>VLANs</li> <li>Security                             <ul style="list-style-type: none"> <li>Admin Management</li> <li>Admin RADIUS</li> <li>Management Control</li> <li>Access Control List</li> <li>Global Settings</li> <li><b>External Radius</b></li> <li>Internal Radius</li> <li>Rogue Control List</li> </ul> </li> <li>SSIDs</li> <li>Groups</li> <li>IAPs</li> <li>WDS</li> <li>Filters</li> <li><b>Tools</b> <ul style="list-style-type: none"> <li>System Tools</li> <li>CLI</li> <li>Logout</li> </ul> </li> </ul> </li> </ul>	<p><b>Primary Server</b></p> <p>Host Name / IP Address: <input type="text" value="radius1"/></p> <p>Port Number: <input type="text" value="1812"/></p> <p>Shared Secret / Verify Secret: <input type="password" value="*****"/> <input type="password" value="*****"/></p> <p><b>Secondary Server</b></p> <p>Host Name / IP Address: <input type="text"/></p> <p>Port Number: <input type="text" value="1812"/></p> <p>Shared Secret / Verify Secret: <input type="text"/> <input type="text"/></p> <p><b>Settings</b></p> <p>Timeout (seconds): <input type="text" value="600"/></p> <p>NAS Identifier: <input type="text"/></p> <p>Accounting: <input type="radio"/> Off <input checked="" type="radio"/> On</p> <p><b>Accounting</b></p> <p>Accounting Interval (seconds): <input type="text" value="300"/></p> <p>Primary Server Host Name / IP Address: <input type="text" value="radius1"/></p> <p>Primary Server Port Number: <input type="text" value="1813"/></p> <p>Primary Server Shared Secret / Verify Secret: <input type="password" value="*****"/> <input type="password" value="*****"/></p> <p>Secondary Server Host Name / IP Address: <input type="text"/></p> <p>Secondary Server Port Number: <input type="text" value="1813"/></p> <p>Secondary Server Shared Secret / Verify Secret: <input type="text"/> <input type="text"/></p> <p style="text-align: right;"><input type="button" value="Apply"/> <input type="button" value="Save"/></p>		

Figure 128. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see “Understanding Groups” on page 247. User groups allow you to easily apply a uniform configuration to a user on the Array.

### *Procedure for Configuring an External RADIUS Server*

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

 *The shared secret that you define must match the secret used by the external RADIUS server.*
  
2. **Secondary Server (optional):** If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will “failover” to the secondary RADIUS server (defined here).
  - a. **Address:** Enter the IP address or domain name of this external RADIUS server.
  - b. **Port Number:** Enter the port number of this external RADIUS server. The default is 1812.
  - c. **Shared Secret / Verify Secret:** Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.
  
3. **Settings:** Define the session timeout, the NAS Identifier, and whether accounting will be used.
  - a. **Timeout (seconds):** Define the maximum idle time (in seconds) before the external RADIUS server’s session times out. The default is 600 seconds.
  - b. **NAS Identifier:** From the point of view of a RADIUS server, the Array is a client, also called a network access server (NAS). Enter the



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

### Internal Radius

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

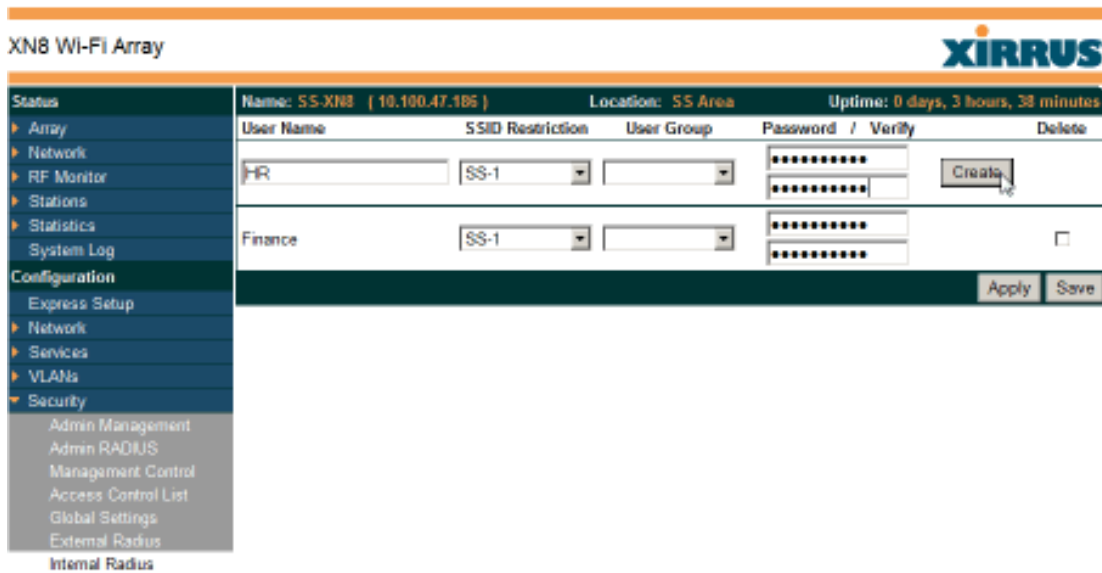


Figure 129. Internal RADIUS Server

### *Procedure for Creating a New User*

1. **User Name:** Enter the name of the user that you want to authenticate to the internal RADIUS server.
2. **SSID Restriction:** (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the pull-down list.
3. **User Group:** (Optional) If you want to make this user a member of a previously defined user group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See [“Understanding Groups” on page 247](#).
4. **Password:** (Optional) Enter a password for the user.
5. **Verify:** (Optional) Retype the user password to verify that you typed it correctly.
6. Click on the **Create** button to add the new user to the list.

### *Procedure for Managing Existing Users*

1. **SSID Restriction:** (Optional) If you want to restrict a user to associating to a particular SSID, choose an SSID from its pull-down list.
2. **User Group:** (Optional) If you want to change the user's group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See [“Understanding Groups” on page 247](#).
3. **Password:** (Optional) Enter a new password for the selected user.
4. **Verify Password:** (Optional) Retype the user password to verify that you typed it correctly.
5. If you want to delete one or more users, check their **Delete** check boxes, then click **Apply** or **Save**.
6. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

[Admin Management](#)  
[External Radius](#)

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

### Rogue Control List

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



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

The screenshot shows the 'Rogue Control List' configuration window in the XN8 Wi-Fi Array interface. The window title is 'XN8 Wi-Fi Array' and the XIRRUS logo is in the top right. The interface includes a navigation menu on the left with options like Array, Network, RF Monitor, and Security. The main area displays a table for adding rogue entries.

Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 3 hours, 41 minutes		
Array	Rogue BSSID/SSID	Blocked	Known	Approved	Delete
Network	<input type="text"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="button" value="Create"/>
RF Monitor	00:0F:7d:*	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Stations					<input type="button" value="Apply"/> <input type="button" value="Save"/>
Statistics					
System Log					
Configuration					
Express Setup					
Network					
Services					
VLANs					
Security					
Admin Management					
Admin RADIUS					
Management Control					
Access Control List					
Global Settings					
External Radius					
Internal Radius					
Rogue Control List					

Figure 130. Rogue Control List

### *Procedure for Establishing Rogue AP Control*

1. **Rogue BSSID/SSID:** Enter the BSSID or SSID for the new rogue AP. You may use the "\*" character as a wildcard to match any string at this position. For example, **00:0f:7d:\*** matches any string that starts with **00:0f:7d:**. Since Xirrus Arrays start with **00:0f:7d:**, this applies the Rogue Control Type to all Xirrus Arrays.
2. **Rogue Control Type:** Define a type for the new rogue AP, either **Blocked**, **Known** or **Approved**.
3. Click **Create** to add this rogue AP to the Rogue Control List.
4. **Rogue Control List:** If you want to edit the control type for a rogue AP, just click the radio button for the new type for the entry: **Blocked**, **Known** or **Approved**, then click **Apply** or **Save** to apply your change.
5. To delete rogue APs from the list, click their **Delete** checkboxes, then click **Apply** or **Save**.
6. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

#### *See Also*

Network Map

Intrusion Detection

SSIDs

SSID Management



## SSIDs

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



*For a complete discussion of implementing Voice over Wi-Fi on the Array, see the [Xirrus Voice over Wi-Fi Application Note](#) in the [Xirrus Library](#).*

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

XN8 Wi-Fi Array													
Status		Name: SS-XNB ( 10.100.47.186 )				Location: SS Area		Uptime: 0 days, 4 hours, 10 minutes					
▶ Array	▶ Network	SSID	Authentication & Encryption	Security Settings	Filter List	VLAN	Num	QoS	Band	Roaming Layer	DHCP Pool	WPR	
▶ RF Monitor	▶ Stations	testSSID	B02 1x WPA	Unique	none			2	Both	2-only	Off	none	Off
▶ Statistics	▶ System Log	SS-1	Open	None	Global	none		2	Both	2-only	On	192	Off
Configuration	Express Setup	Limits											
▶ Network	▶ Services	SSID	Enabled	Station Limit	SSID Traffic	Station Traffic	Time On	Time Off	Days On	Active			
▶ VLANs	▶ Security	testSSID	Yes	1024	Unlimited	Unlimited	Always	Never	All	Yes			
▶ SSIDs	SSID Management	SS-1	Yes	512	Unlimited	Unlimited	Always	Never	All	Yes			

Figure 131. SSIDs

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

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

### Understanding SSIDs

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

### *Multiple SSIDs*

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

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

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

### *Using SSIDs*

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

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

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

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

*See Also*

- SSID Management
- SSIDs
- Understanding SSIDs

### Understanding QoS Priority on the Wi-Fi Array



*For a complete discussion of implementing Voice over Wi-Fi on the Array, see the [Xirrus Voice over Wi-Fi Application Note](#) in the [Xirrus Library](#).*

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

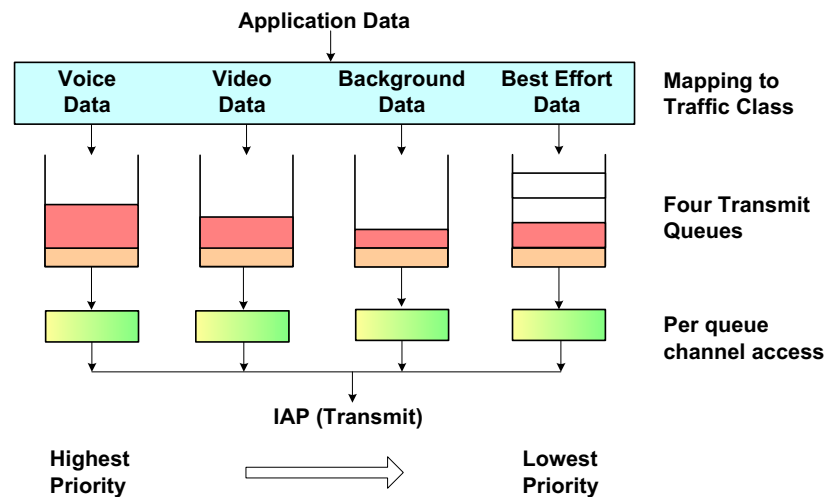


Figure 132. Four Traffic Classes

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

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

### *End-to-End QoS Handling*

- Wired QoS - Ethernet Port:

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

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

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

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

#### Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 0 is the default. See [“SSID Management” on page 240](#). If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.
- The Array supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.
- How QoS is set for a packet in case of conflicting values:
  - a. If an SSID has a QoS setting, and an incoming wired packet’s user priority tag is mapped to a higher QoS value, then the higher QoS value is used.
  - b. If a group or filter has a QoS setting, this overrides the QoS value above. See [“Groups” on page 247](#), and [“Filters” on page 289](#).
  - c. Voice packets have the highest priority, as described below ([Voice Support](#)).

#### Packet Filtering QoS classification

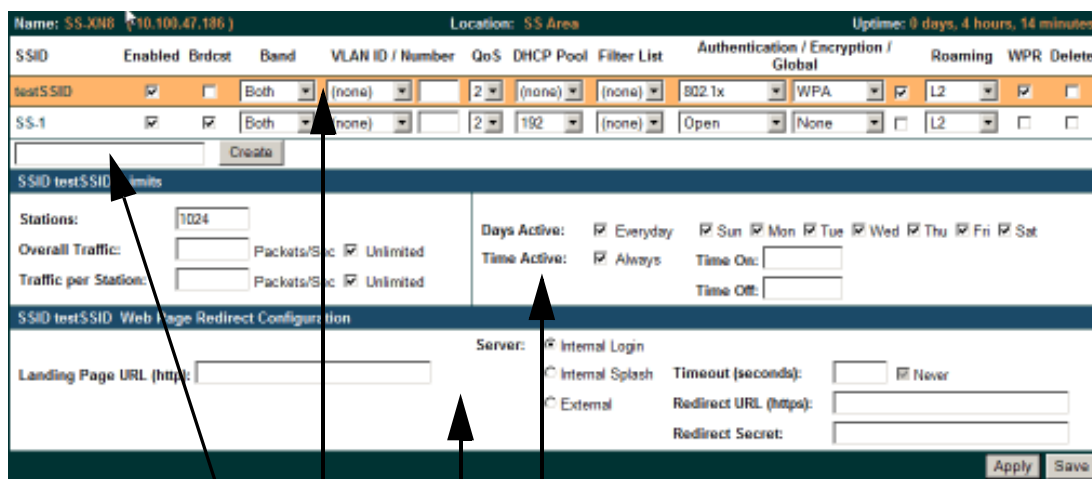
- Filter rules can be used to redefine the QoS priority level to override defaults. See [“Filter Management” on page 291](#). This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

- The QoS priority implementation on the Array supports voice applications. In particular, Spectralink voice packets are automatically classified and set to the highest priority level. **??Leave this in??**

**SSID Management**

This window allows you to manage SSIDs (create, edit and delete), assign security parameters and VLANs on a per SSID basis, and configure the Web Page Redirect functionality. When finished, click on the **Save** button to save your changes.



**Create new SSID**  
**Configure parameters**  
**Set traffic limits / usage schedule**  
**Configure WPR**

Figure 133. SSID Management

*Procedure for Managing SSIDs*

1. **New SSID Name:** To create a new SSID, enter a new SSID name to the left of the Create button (Figure 133), then click Create. You may create up to 16 SSIDs.

**SSID List (top of page)**


2. **SSID:** Shows all currently assigned SSIDs. When you create a new SSID, the SSID name appears in this table. Click any SSID in this list to select it.

3. **On:** Check this box to activate this SSID or clear it to deactivate it.
4. **Brdcast:** Check this box to make the selected SSID visible to all clients on the network. Although the Wi-Fi Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Clear this box if you do not want this SSID to be visible on the network.
5. **Band:** Choose which wireless band the SSID will be beaconsed on. Select either **5 GHz—802.11a(n)**, **2.4 GHz—802.11bg(n)** or **Both**.
6. **VLAN ID / Number:** From the pull-down list, select a VLAN that you want this traffic to be forwarded to on the wired network. Select **numeric** to enter the number of a previously defined VLAN in the **Number** field (see “VLANs” on page 205). This step is optional.
7. **QoS:** (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:
  - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
  - 1—Medium, with QoS prioritization aggregated across all traffic types.
  - 2—High, normally used to give priority to video traffic.
  - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID traffic, as described in “Understanding QoS Priority on the Wi-Fi Array” on page 237. The default value for this field is 2.

8. **DHCP Pool:** If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull--down list. An internal DHCP pool must be created before it can be assigned. To create an internal DHCP pool, go to “DHCP Server” on page 203.

9. **Filter List:** If you wish to apply a set of filters to this SSID's traffic, select the desired Filter List. See [“Filters” on page 289](#).
10. **Authentication:** The following authentication options are available:
  - **Open:** This option provides no authentication and is not recommended.
  - **RADIUS MAC:** Uses an external RADIUS server to authenticate stations onto the Wi-Fi network, based on the user's MAC address. Accounting for these stations is performed according to the accounting options that you have configured specifically for this SSID or globally (see [Step 12](#) below).

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

  - **802.1x:** Authenticates stations onto the Wi-Fi network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the Wi-Fi Array) or external.
11. **Encryption:** From the pull-down list, choose the encryption that will be required—specific to this SSID—either None, WEP, WPA, WPA2 or WPA-Both. The None option provides no security and is not recommended; WPA2 provides the best practice Wi-Fi security.

Each SSID supports only one encryption type at a time (except that WPA and WPA2 are both supported on an SSID if you select WPA-Both). If you need to support other encryption types, you must define additional SSIDs. The encryption standard used with WPA or WPA2 is selected in the Security>Global Settings window ([page 225](#)). For an overview of the security options, see [“Security Planning” on page 70](#) and [“Understanding Security” on page 210](#).

12. **Global:** Check the checkbox if you want this SSID to use the security settings established at the global level (refer to [“Global Settings” on page 225](#)). Clear the checkbox if you want the settings established here to take precedence. Additional sections will be displayed to allow you to



configure encryption, RADIUS, and RADIUS accounting settings. The encryption settings are described in [“Procedure for Configuring Network Security”](#) on page 226. The external RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see [“Procedure for Configuring an External RADIUS Server”](#) on page 229). Note that external RADIUS servers may be specified using IP addresses or domain names.

13. **L3:** For this SSID, Check the checkbox to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3, or clear the checkbox to allow roaming at Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in [Global Settings \(IAP\)](#). See [“Understanding Fast Roaming”](#) on page 254.
14. **WPR (Web Page Redirect):** Check the checkbox to enable the Web Page Redirect functionality, or clear it to disable this option. If enabled, WPR configuration fields will be displayed under the SSID Limits section. This feature may be used to provide an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. For example, some wireless devices and users may not have a correctly configured 802.1x (RADIUS) supplicant. Utilizing WPR’s Web-based login, users may be authenticated without using an 802.1x supplicant. See [“Web Page Redirect Configuration Settings”](#) on page 244 for details of WPR usage and configuration.

### SSID Limits

See [“Group Limits”](#) on page 251 for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

15. **Stations:** Enter the maximum number of stations allowed on this SSID. The default is 1024. This step is optional. Note that the IAPs - Global Settings window also has a station limit option—**Max Station**

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

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

### *See Also*

[DHCP Server](#)

[External Radius](#)

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

[Internal Radius](#)

[Security Planning](#)

[SSIDs](#)

[Understanding QoS Priority on the Wi-Fi Array](#)

### **Web Page Redirect Configuration Settings**

If you enable WPR, the SSID Management window displays additional fields that must be configured. For example configurations and complete examples, please

For an in-depth discussion, please see the *Xirrus Web Page Redirect Application Note* in the [Xirrus Library](#).

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

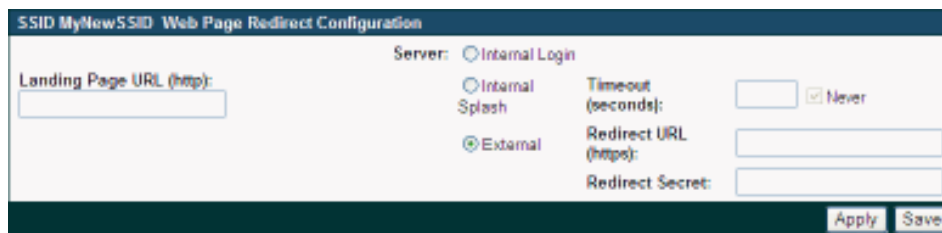


Figure 134. WPR Internal Splash Page Fields (SSID Management)

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

- Internal Splash page

This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Array. Note that there is an upload function that allows you to replace the default splash page, if you wish. Please see “[Web Page Redirect](#)” on page 300 for more information.

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

- Internal Login page

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

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

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

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

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



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

- External Login page

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

Authentication occurs according to your configured RADIUS information. These parameters are configured as described in “[Procedure for Configuring Network Security](#)” on page 226. After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

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

## Groups

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

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

For information to help you understand groups, see [Understanding Groups](#) below. For an in-depth discussion, please see the *Xirrus User Groups Application Note* in the [Xirrus Library](#).

Status		Name: SS-XN8 ( 10.100.47.186 )		Location: SS Area		Uptime: 0 days, 4 hours, 57 minutes			
Group Name	Radius ID	Filter List	VLAN	Num	QoS	Roaming Layer	DHCP Pool	WPR	
Students		none			2	2-only		On	
Staff	StaffMembers	none		22	2	2-only			
Limits									
Group Name	Enabled	Station Limit	SSID Traffic	Station Traffic	Time On	Time Off	Days On	Active	
Students	Enabled	512	1000000	100000	7:00	18:00	Mon Tue Wed Thu Fri	Yes	
Staff	Enabled	512	Unlimited	Unlimited	Always	Never	All	Yes	

Figure 135. Groups

## Understanding Groups

User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs.

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

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

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

### Using Groups

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

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

#### *See Also*

[External Radius](#)

[Internal Radius](#)

[SSIDs](#)

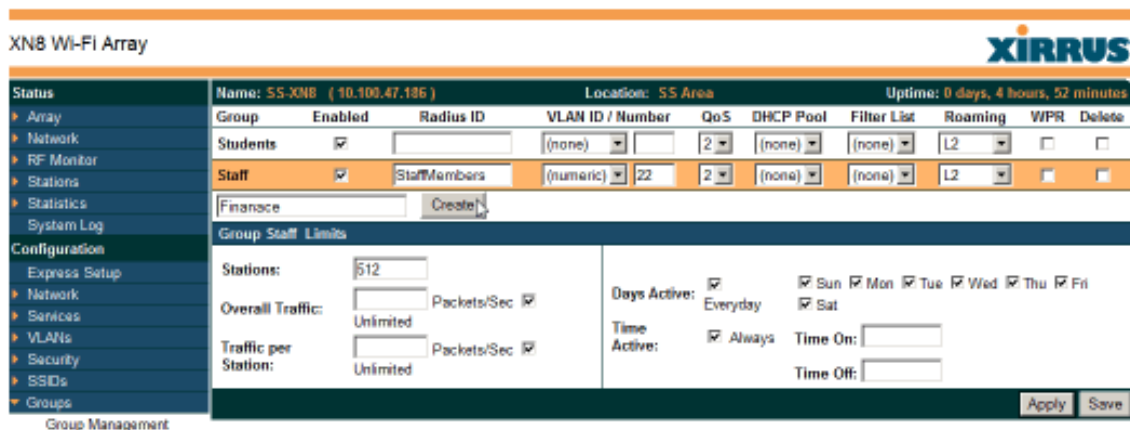
Understanding QoS Priority on the Wi-Fi Array

Web Page Redirect Configuration Settings

Understanding Fast Roaming

## Group Management

This window allows you to manage groups (create, edit and delete), assign usage limits and other parameters on a per group basis, and configure the Web Page Redirect functionality. When finished, click the **Save** button to save your changes.



The screenshot displays the 'Group Management' page for an XN8 Wi-Fi Array. The page title is 'XN8 Wi-Fi Array' and the XIRRUS logo is in the top right. The main content area is divided into a 'Status' section and a 'Configuration' section. The 'Status' section shows a table of groups with the following columns: Group, Enabled, Radius ID, VLAN ID / Number, QoS, DHCP Pool, Filter List, Roaming, WPR, and Delete. The 'Staff' group is highlighted in orange. Below the table, there is a 'Create' button and a text input field containing 'Finance'. The 'Configuration' section is titled 'Group Staff Limits' and contains several settings: 'Stations' (512), 'Overall Traffic' (Unlimited), 'Traffic per Station' (Unlimited), 'Days Active' (Everyday), and 'Time Active' (Always). There are also checkboxes for 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. At the bottom right of the configuration section are 'Apply' and 'Save' buttons.

Figure 136. Group Management

### Procedure for Managing Groups

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

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

2. **Group:** This column lists currently defined groups. When you create a new group, the group name appears in this list. Click on any group to select it, and then proceed to modify it as desired.
3. **On:** Check this box to enable this group or leave it blank to disable it. When a group is disabled, users that are members of the group will behave as if the group did not exist. In other words, the options configured for the SSID will apply to the users, rather than the options configured for the group.

4. **Radius ID:** Enter a unique Radius ID for the group, to be used on an external Radius server. When adding a user account to the external server, this Radius ID value should be entered for the user. When the user is authenticated, Radius sends this value to the Array. This tells the Array that the user is a member of the group having this Radius ID.
5. **VLAN ID:** (Optional) From the pull-down list, select a VLAN for this user's traffic to use. Select **numeric** and enter the number of a previously defined VLAN (see [“VLANs” on page 205](#)). **This user group's VLAN settings supersede Dynamic VLAN settings** (which are passed to the Array by the Radius server). To avoid confusion, we recommend that you avoid specifying the VLAN for a user in two places.
6. **QoS Priority:** (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:
  - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
  - 1—Medium; QoS prioritization is aggregated across all traffic types.
  - 2—High, normally used to give priority to video traffic.
  - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

The QoS setting you define here will prioritize wireless traffic for this group versus other traffic, as described in [“Understanding QoS Priority on the Wi-Fi Array” on page 237](#). The default value for this field is 2.

7. **Internal DHCP Pool Assigned:** (Optional) To associate an internal DHCP pool to this group, select it from the pull--down list. Only one pool may be assigned. An internal DHCP pool must be created before it can be assigned. To create a DHCP pool, go to [“DHCP Server” on page 203](#).
8. **Filter List:** (Optional) If you wish to apply a set a filters to this user group's traffic, select the desired Filter List. See [“Filters” on page 289](#).



9. **L3:** (Optional) For this group, check this box to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3. If the box is not checked, then roaming uses Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in [Global Settings \(IAP\)](#). See [“Understanding Fast Roaming”](#) on page 254.
10. **WPR (Web Page Redirect):** (Optional) Check this box if you wish to enable the Web Page Redirect functionality. This will open a **Web Page Redirect** details section in the window, where your WPR parameters may be entered. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. See [“Web Page Redirect Configuration Settings”](#) on page 244 for details of WPR usage and configuration. Note that the Group Management window only allows you to set up and Internal Splash page. The authentication options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the Array by a Radius server, this means the user has already been authenticated.

### Group Limits

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

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

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

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

11. **Stations:** Enter the maximum number of stations allowed on this group. The default is 1024.
12. **Overall Traffic:** Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic for this group, or enter a value in the Packets/Sec field and make sure that the Unlimited box is unchecked to force a traffic restriction.
13. **Traffic per Station:** Check the **Unlimited** checkbox if you do not want to place a restriction on the traffic per station for this group, or enter a value in the Packets/Sec field and make sure that the Unlimited box is unchecked to force a traffic restriction.
14. **Days Active:** Choose **Everyday** if you want this group to be active every day of the week, or select only the specific days that you want this group to be active. Days that are not checked are considered to be the inactive days.
15. **Time Active:** Choose **Always** if you want this group active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that group members may associate.
16. Click on the **Apply** button to apply the changes to the selected group, or click **Save** to apply your changes and make them permanent.
17. To delete an entry, check its **Delete** checkbox, then click the Save button to permanently remove the entry.

*See Also*

DHCP Server

External Radius

Internal Radius

Security Planning

SSIDs

## IAPs

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

Status		Name: SS-XNB ( 10.100.47.186 )		Location: SS Area		Uptime: 0 days, 5 hours, 3 minutes					
	IAP	State	Channel	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link	MAC Address / BSSID	Description
▶ Array	albn1	down	1	int-dir	max	20	-90	0		00:0f:7d:0b:b3:90-91	
▶ Network	albn2	up	monitor	int-omni	monitor	20	-95	0		00:0f:7d:0b:b3:b0-b1	
▶ RF Monitor	albn3	down	11	int-dir	max	20	-90	0		00:0f:7d:0b:b3:d0-d1	
▶ Stations	albn4	up	6	int-dir	medium	12	-81	1		00:0f:7d:0b:b3:f0-f1	
▶ Statistics	an1	down	40	int-dir	medium	12	-81	0		00:0f:7d:0b:b3:a0-a1	
▶ System Log	an2	down	56	int-dir	max	20	-90	0		00:0f:7d:0b:b3:c0-c1	
Configuration	an3	down	48	int-dir	max	20	-90	0		00:0f:7d:0b:b3:e0-e1	
▶ Express Setup	an4	down	64	int-dir	max	20	-90	0		00:0f:7d:0b:b3:80-81	
▶ Network											
▶ Services											
▶ VLANs											
▶ Security											
▶ SSIDs											
▶ Groups											
▼ IAPs											
▶ IAP Settings											

Figure 137. IAPs

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

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

- [“Understanding Fast Roaming”](#) on page 254

IAPs are configured using the following windows:

- [“IAP Settings”](#) on page 255
- [“Global Settings \(IAP\)”](#) on page 260
- [“Global Settings .11a”](#) on page 267
- [“Global Settings .11bg”](#) on page 269

- [“Global Settings .11n” on page 273](#)
- [“Advanced RF Settings” on page 275](#)
- [“LED Settings” on page 283](#)

### *See Also*

[IAP Statistics Summary](#)

### **Understanding Fast Roaming**

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

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

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your Array, see [Step 17 to Step 19](#) in [“Global Settings \(IAP\)” on page 260](#). To choose which of the enabled options are used by an SSID or Group, see [“Procedure for Managing SSIDs” on page 240 \(Step 13\)](#) or [“Procedure for Managing Groups” on page 249](#).

### IAP Settings

This window allows you to enable/disable IAPs, define the wireless mode for each IAP, specify the channel to be used and the cell size for each IAP, lock the channel selection, establish transmit/receive parameters, select antennas, and reset channels. Buttons at the bottom of the list allow you to **Reset Channels**, **Enable All IAPs**, or **Disable All IAPs**. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent. To see a diagram of the layout and naming of IAPs, go to Figure 7 on page 16.

The screenshot shows the 'XN8 Wi-Fi Array' configuration page. At the top right is the XIRRUS logo. Below it, the array name is 'SS-XNB (10.100.47.186)' and the location is 'SS Area'. The uptime is '0 days, 5 hours, 15 minutes'. A left-hand navigation menu includes options like Array, Network, RF Monitor, Stations, Statistics, System Log, Configuration, Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, and IAPs. The main area contains a table of IAP settings:

IAP	Enabled	Band	Channel	Bond	Lock	Cell Size	Tx dBm	Rx dBm	Antenna Select	Description
abgn1	<input checked="" type="checkbox"/>	2.4 GHz	1	off	<input type="checkbox"/>	max	20	-90	Internal-Dir	
abgn2	<input checked="" type="checkbox"/>	monitor	mon	off	<input type="checkbox"/>	monitor	20	-95	Internal-Omni	
abgn3	<input checked="" type="checkbox"/>	2.4 GHz	11	off	<input type="checkbox"/>	max	20	-90	Internal-Dir	
abgn4	<input checked="" type="checkbox"/>	2.4 GHz	6	off	<input type="checkbox"/>	medium	12	-81	Internal-Dir	
an1	<input checked="" type="checkbox"/>	5 GHz	40	36	<input type="checkbox"/>	medium	12	-81	Internal 5GHz	
an2	<input checked="" type="checkbox"/>	5 GHz	56	52	<input type="checkbox"/>	max	20	-90	Internal 5GHz	
an3	<input checked="" type="checkbox"/>	5 GHz	48	44	<input type="checkbox"/>	max	20	-90	Internal 5GHz	
an4	<input type="checkbox"/>	5 GHz	64	60	<input type="checkbox"/>	max	20	-90	Internal 5GHz	

At the bottom of the table are buttons for 'Enable All IAPs', 'Disable All IAPs', 'Reset Channels', 'Apply', and 'Save'.

Figure 138. IAP Settings

You may also access this window by clicking on the Array image at the lower left of the WMI window—click the orange Xirrus logo in the center of the Array. See “User Interface” on page 123.

#### Procedure for Auto Configuring IAPs

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

- For all radios, go to “Advanced RF Settings” on page 275.
- For all 802.11a settings, go to “Global Settings .11a” on page 267.

- For all 802.11bg settings, go to “Global Settings .11bg” on page 269.
- For all 802.11n settings, go to “Global Settings .11n” on page 273.

### *Procedure for Manually Configuring IAPs*

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



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

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

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

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

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



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

4. The **Bonding** column only appears for XN Array models. It works together with the **Auto Channel Bonding** and **Dynamic/Static** options selected on the **Global Settings .11n** page. Also see the discussion of 802.11n bonding in “**Channel Bonding**” on page 63. [Please check carefully??](#)
  - **Off**—This channel is not bonded to another channel.
  - **On**—This channel is bonded to an adjacent channel. The bonded channel is selected automatically by the Array based on current conditions. The choice of banded channel may be dynamic, changing as needed; or it may be static—fixed once the selection is made.
  - **+1**—This channel is bonded to the next higher channel number. Auto Channel bonding does not apply.
  - **-1**—This channel is bonded to the next lower channel number. Auto Channel bonding does not apply.
5. Click the **Lock** check box if you want to lock in your channel selection so that the autochannel operation (see **Advanced RF Settings**) cannot change it.

6. In the **Cell Size** column, select **Auto** to allow the optimal cell size to be automatically computed (see also, [Step 8 on page 279](#)). To set the cell size yourself, choose either **Small**, **Medium**, **Large**, or **Max** to use the desired pre-configured cell size, or choose **Manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx dBm** (transmit) and **Rx dBm** (receive) fields. The default is **Max**.

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

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

For additional information about cell sizes, go to "[Coverage and Capacity Planning](#)" on page 50.

7. In the **Antenna Select** column, choose the antenna you want this radio to use from the pull-down list. The list of available antennas will be different (or no choices will be available), depending on the wireless mode you selected for the IAP.
8. If desired, enter a description for this IAP in the **Description** field.



9. You may reset all of the enabled IAPs by clicking the **Reset Channels** button at the bottom of the list. A message will inform you that all enabled radios have been taken down and brought back up.



10. Buttons at the bottom of the list allow you to **Enable All IAPs** or **Disable All IAPs**.
11. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

Coverage and Capacity Planning

Global Settings (IAP)

Global Settings .11a

Global Settings .11bg

Global Settings .11n

IAPs

IAP Statistics Summary

LED Settings

## Global Settings (IAP)

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

**XN8 Wi-Fi Array** **XIRRUS**

Name: SS-XN8 ( 10.100.47.186 )      Location: SS Area      Uptime: 0 days, 18 hours, 0 minutes

<b>Status</b>	Country: United States	
▶ Array	IAP Status: <input type="button" value="Enable All IAPs"/> <input type="button" value="Disable All IAPs"/>	
▶ Network	Short Retry Limit (1-128): 7	
▶ RF Monitor	Long Retry Limit (1-128): 4	
▶ Stations	<b>Beacon Configuration</b>	
▶ Statistics	Beacon Interval (20-1000): 100	
System Log	DTIM Period (1-255): 1	
<b>Configuration</b>	802.11h Beacon Support: <input checked="" type="radio"/> OFF <input type="radio"/> ON	
Expressa Setup	<b>Station Management</b>	
▶ Network	Station Re-Authentication Period (Seconds): 5	
▶ Services	Station Timeout Period (Seconds): 1000	
▶ VLANs	Max Station Association per IAP (1-64): 64	
▶ Security	Max Phones per IAP (0-16): 16	
▶ SSIDs	Block Intra-Station Traffic: <input checked="" type="radio"/> Yes <input type="radio"/> No	
▶ Groups	Allow Over Air Management: <input type="radio"/> Yes <input checked="" type="radio"/> No	
▶ IAPs	<b>Advanced Traffic Optimization</b>	
IAP Settings	Broadcast Rates: <input checked="" type="radio"/> Optimized <input type="radio"/> Standard	
Global Settings	Load Balancing: <input type="radio"/> OFF <input checked="" type="radio"/> On <input type="radio"/> Aggressive	
Global Settings: 11a	ARP Filtering: <input type="radio"/> OFF <input checked="" type="radio"/> Pass-thru <input type="radio"/> Proxy	
Global Settings: 11bg	Fast Roaming Mode: <input type="radio"/> OFF <input type="radio"/> Broadcast <input checked="" type="radio"/> Tunneled	
Global Settings: 11n	Fast Roaming Layer: <input checked="" type="radio"/> 2 and 3 <input type="radio"/> 2 only	
Advanced RF Settings	Share Roaming Info With: <input type="radio"/> All <input checked="" type="radio"/> In Range <input type="radio"/> Target Only	
LED Settings	Fast Roaming Targets:	
▶ WDS	<input type="text" value="00:0f:7d:22:34:00"/> <input type="button" value="Add"/>	
▶ Filters	<input type="text" value="00:0f:7d:22:33:00"/> <input type="button" value="Delete"/>	
Tools	Name: no info Location: no info IP Address: no info	
System Tools	<input type="button" value="Apply"/> <input type="button" value="Save"/>	
CLI		
Logout		
Log Messages		
Critical 0		
Warning 0		
Information 500		

Figure 139. Global Settings (IAPs)

### *Procedure for Configuring Global IAP Settings*

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

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

Until you have chosen a country, the channel set defaults to channels and power levels that are legal worldwide—this set only includes the lower eight 5 GHz channels.

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

### Beacon Configuration

5. **Beacon Interval:** When the Array sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000. The value you enter here is applied to all IAPs.
6. **DTIM Period:** A DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by the Array to a client device in sleep mode, alerting the device to broadcast traffic awaiting delivery. The **DTIM Period** is a multiple of the **Beacon Interval**, and it determines how often DTIMs are sent out. By default, the DTIM period is 1, which means that it is the same as the beacon interval. Enter the desired multiple, between 1 and 255. The value you enter here is applied to all IAPs.
7. **802.11h Beacon Support:** This option enables beacons on all of the Array's radios to conform to 802.11h requirements, supporting dynamic frequency selection (DFS) and transmit power control (TPC) to satisfy regulatory requirements for operation in Europe.

### Station Management

8. **Station Re-Authentication Period:** This option allows you to specify a time (in seconds) for the duration of station reauthentications.
9. **Station Timeout Period:** Specify a time (in seconds) in this field to define the timeout period for station associations.
10. **Max Station Association per IAP:** This option allows you to define how many station associations are allowed per IAP (up to 64 stations per IAP). Note that the SSIDs —SSID Management window also has a station limit option— **Station Limit** (page 243). If both station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.

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



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

- 12. Block Intra-Station Traffic:** This option allows you to block or allow traffic between wireless clients that are associated to the Array. Choose either **Yes** (to block traffic) or **No** (to allow traffic).
- 13. Allow Over Air Management:** Choose **Yes** to enable management of the Array via the IAPs, or choose **No** (recommended) to disable this feature.

### Advanced Traffic Optimization

- 14. Broadcast Rates:** This option changes the rates of broadcast traffic sent by the Array (including beacons). When set to **Optimized**, each broadcast or multicast packet that is transmitted on each radio is sent at the lowest transmit rate used by any client associated to that radio at that time. This results in each IAP broadcasting at the highest Array TX data rate that can be heard by all associated stations, thus improving system performance. The rate is determined dynamically to ensure the best broadcast/multicast performance possible. The benefit is dramatic. Consider a properly designed network (one that has -70db or better everywhere), where virtually every client should have a 54Mbps connection. In this case, broadcasts and multicasts will all go out at 54Mbps vs. the standard rate. This means that with broadcast rate optimization on, broadcasts and multicasts use between 2% and 10% of the bandwidth that they would in Standard mode.

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

### 15. Load Balancing:

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

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

If you select **Aggressive** Load Balancing and an IAP is overloaded, that IAP will never respond to Probe, Association, or Authentication requests. This mode is useful because it prevents determined clients from forcing their way onto overloaded IAPs. Note that some clients are so determined to associate to a particular IAP that they will not try to associate to another IAP, and thus they never get on the network.

Choose **Off** to disable load balancing.

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

You may select the following options for handling ARP requests:

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

- **Pass-thru:** The Array forwards the ARP request. It passes along only ARP messages that target the stations that are associated to it.
- **Proxy:** The Array replies on behalf of the stations that are associated to it. The ARP request is not broadcast to the stations.

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

17. **Fast Roaming Mode:** This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3 (as specified in [Step 18](#)), while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see “[Understanding Fast Roaming](#)” on [page 254](#) for a discussion of this feature). XRP uses a discovery process to identify other Xirrus Arrays as fast roaming targets. This process has two modes:

- **Broadcast**—the Array uses a broadcast technique to discover other Arrays that may be targets for fast roaming.
- **Tunneled**—in this Layer 3 technique, fast roaming target Arrays must be explicitly specified.

To enable fast roaming, choose **Broadcast** or **Tunneled**, and set additional fast roaming attributes ([Step 19](#)). To disable fast roaming, choose **Off**. If you enable Fast Roaming, the following ports **cannot** be blocked:

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

18. **Fast Roaming Layer:** Select whether to enable roaming capabilities between IAPs or Arrays at Layer **2 and 3**, or at Layer **2 only**. Depending on your wired network, you may wish to allow fast roaming at Layer 3. This may result in delayed traffic.
19. **Share Roaming Info With:** Three options allow your Array to share roaming information with all Arrays; just with those that are within range; or with specifically targeted Arrays. Choose either **All**, **In Range** or **Target Only**, respectively.
  - a. **Fast Roaming Targets:** If you chose **Target Only**, use this option to add target MAC addresses. Enter the MAC address of each target Array, then click on **Add** (add as many targets as you like). To find a target's MAC address, open the **Array Info** window on the target Array and look for **IAP MAC Range**, then use the starting address of this range.

To delete a target, select it from the list, then click **Delete**.
20. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

Coverage and Capacity Planning

Global Settings .11a

Global Settings .11bg

Global Settings .11n

Advanced RF Settings

IAPs

IAP Statistics Summary

LED Settings

IAP Settings



### Global Settings .11a

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

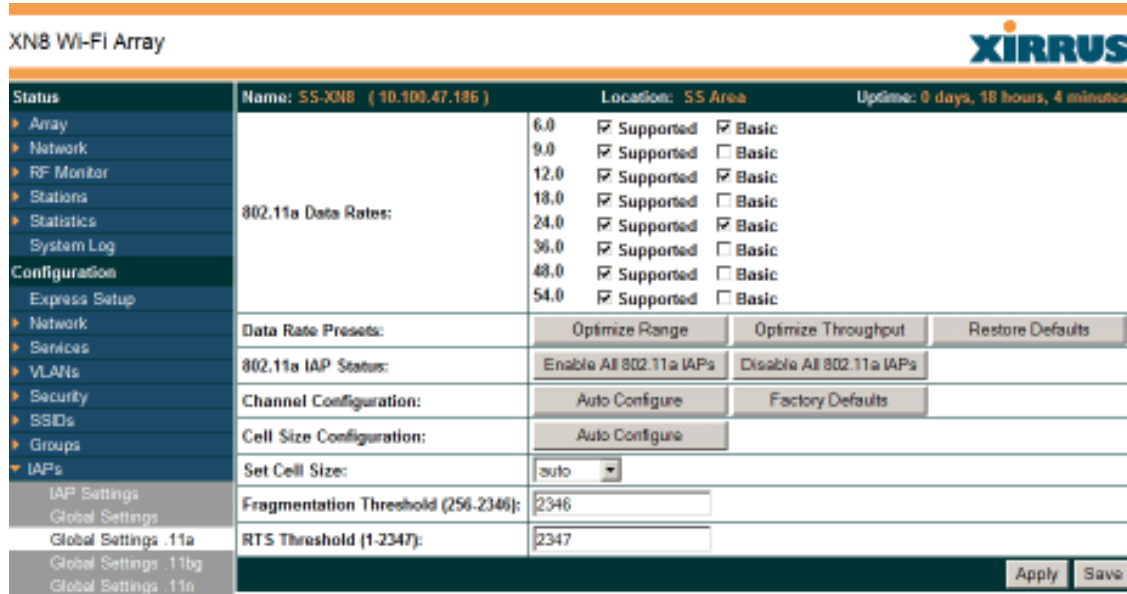


Figure 140. Global Settings .11a

#### Procedure for Configuring Global 802.11a IAP Settings

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

optimize data rates based on throughput. The **Restore Defaults** button will take you back to the factory default rate settings.

3. **802.11a IAP Status:** Click **Enable 802.11a IAPs** to enable all 802.11a IAPs for this Array, or click **Disable 802.11a IAPs** to disable all 802.11a IAPs.
4. **Channel Configuration:** Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11a IAP and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11a channel allocation. Use **Factory Defaults** to take you back to the factory default channel settings.
5. **Cell Size Configuration:** Click **Auto Configure** to instruct the Array to determine and set the best cell size for each enabled 802.11a IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP Settings window, each enabled 802.11a IAP will have its cell size set to **auto**.
6. **Set Cell Size:** The Cell Size may be set globally for all 802.11a IAPs to **auto**, **large**, **medium**, **small**, or **max** using the drop down menu.
7. **Fragmentation Threshold:** This is the maximum size for directed data **packets** transmitted over the 802.11a radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Smaller fragmentation numbers can help to “squeeze” packets through in noisy environments. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346.
8. **RTS Threshold:** The RTS (Request To Send) Threshold specifies the **packet** size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.
9. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

Coverage and Capacity Planning  
Global Settings (IAP)

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

### Global Settings .11bg

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

XNB Wi-Fi Array		XIRRUS	
Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 0 days, 18 hours, 11 minutes
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>System Log</li> <li><b>Configuration</b></li> <li>Express Setup</li> <li>▶ Network</li> <li>▶ Services</li> <li>▶ VLANs</li> <li>▶ Security</li> <li>▶ SSIDs</li> <li>▶ Groups</li> <li>▶ IAPs</li> <li>IAP Settings</li> <li>Global Settings</li> <li>Global Settings .11a</li> <li><b>Global Settings .11bg</b></li> <li>Global Settings .11n</li> <li>Advanced RF Settings</li> <li>LED Settings</li> <li>▶ WDS</li> <li>▶ Filters</li> <li><b>Tools</b></li> <li>System Tools</li> <li>CLI</li> <li>Logout</li> <li><b>Log Messages</b></li> <li>Critical 0</li> </ul>	<b>802.11g Data Rates:</b> 6.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 9.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 12.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 18.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 24.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 36.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 48.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 54.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic		
	<b>802.11b Data Rates:</b> 1.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 2.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 5.5 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 11.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic		
	Data Rate Presets:	Optimize Range	Optimize Throughput
	802.11b/g IAP Status:	Enable All 802.11b/g IAPs	Disable All 802.11b/g IAPs
	Channel Configuration:	Auto Configure	Factory Defaults
	Cell Size Configuration:	Auto Configure	
	Set Cell Size:	auto	
	802.11g Only:	<input type="radio"/> On	<input checked="" type="radio"/> OFF
	802.11g Protection:	<input checked="" type="radio"/> Auto CTS	<input type="radio"/> OFF
		<input type="radio"/> Auto RTS	
	802.11g Slot:	<input checked="" type="radio"/> Auto	<input type="radio"/> Short Only
	802.11b Preamble:	<input checked="" type="radio"/> Auto	<input type="radio"/> Long Only
	Fragmentation Threshold (256-2346):	2346	
	RTS Threshold (1-2347):	2347	
			Apply Save

Figure 141. Global Settings .11bg

### *Procedure for Configuring Global 802.11b/g IAP Settings*

- 1. 802.11g Data Rates:** The Array allows you to define which data rates are supported for all 802.11g radios. Select (or deselect) 11g data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
  - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
  - **Supported Rate**—data rate used to transmit to clients.
- 2. 802.11b Data Rates:** This task is similar to Step 1, but these data rates apply only to 802.11b IAPs.
- 3. Data Rate Presets:** The Wi-Fi Array can optimize your 802.11b/g data rates automatically, based on range or throughput. Click **Optimize Range** button to optimize data rates based on range, or click on the **Optimize Throughput** to optimize data rates based on throughput. **Restore Defaults** will take you back to the factory default rate settings.
- 4. 802.11b/g IAP Status:** Click **Enable All 802.11b/g IAPs** to enable all 802.11b/g IAPs for this Array, or click **Disable All 802.11b/g IAPs** to disable them.
- 5. Channel Configuration:** Click **Auto Configure** to instruct the Array to determine the best channel allocation settings for each 802.11b/g IAP and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11b/g channel allocations. **Factory Defaults** will take you back to the factory default channel settings.
- 6. Cell Size Configuration:** Click **Auto Configure** to instruct the Array to determine and set the best cell size for each enabled 802.11b/g IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP Settings window, the cell size of each enabled 802.11b/g IAP will be set to **auto**.
- 7. Set Cell Size:** The Cell Size may be set globally for all 802.11b/g IAPs to **auto**, **large**, **medium**, **small**, or **max** using the drop down menu.

8. **802.11g Only:** Choose **On** to restrict use to 802.11g mode only. In this mode, no 802.11b rates are transmitted. Stations that only support 802.11b will not be able to associate.
9. **802.11g Protection:** You should select **Auto CTS** or **Auto RTS** to provide automatic protection for all 802.11g radios in mixed networks (802.11b and g). You may select **Off** to disable this feature, but this is not recommended. Protection allows 802.11g stations to share an IAP with older, slower 802.11b stations. Protection avoids collisions by preventing 802.11b and 802.11g stations from transmitting simultaneously. When **Auto CTS** or **Auto RTS** is enabled and any 802.11b station is associated to the IAP, additional frames are sent to gain access to the wireless network.
  - Auto CTS requires 802.11g stations to send a slow Clear To Send frame that locks out other stations. Automatic protection reduces 802.11g throughput when 802.11b stations are present—Auto CTS adds less overhead than Auto RTS. The default value is Auto CTS.
  - With Auto RTS, 802.11g stations reserve the wireless media using a Request To Send/Clear To Send cycle. This mode is useful when you have dispersed nodes. It was originally used in 802.11b only networks to avoid collisions from “hidden nodes”—nodes that are so widely dispersed that they can hear the Array, but not each other.

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

10. **802.11g Slot:** Choose **Auto** to instruct the Array to manage the 802.11g slot times automatically, or choose **Short Only**. Xirrus recommends using **Auto** for this setting, especially if 802.11b devices are present.
11. **802.11b Preamble:** The **preamble** contains information that the Array and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble. A short preamble improves the efficiency of a network's throughput when transmitting

special data, such as voice, VoIP (Voice-over IP) and streaming video. Select **Auto** to instruct the Array to manage the preamble (long and short) automatically, or choose **Long Only**.

12. **Fragmentation Threshold:** This is the maximum size for directed data [packets](#) transmitted over the 802.11b/g IAP. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value, between 256 and 2346.
13. **RTS Threshold:** The RTS (Request To Send) Threshold specifies the [packet](#) size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.
14. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

### *See Also*

[Coverage and Capacity Planning](#)

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

[Global Settings .11a](#)

[Global Settings .11n](#)

[Advanced RF Settings](#)

[LED Settings](#)

[IAP Settings](#)

[IAP Statistics Summary](#)

### Global Settings .11n

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

Before changing your settings for 802.11n, please read the discussion in “IEEE 802.11n Deployment Considerations” on page 59.

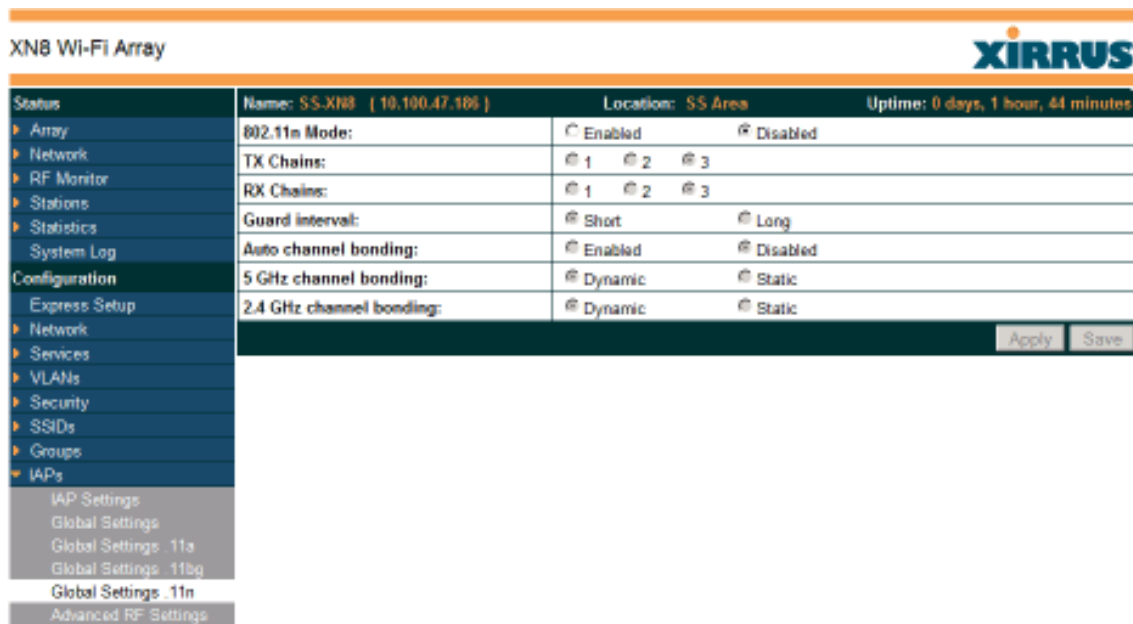


Figure 142. Global Settings .11n

#### Procedure for Configuring Global 802.11n IAP Settings

1. **802.11n Mode:** Select **Enabled** to operate in 802.11n mode, with four 802.11b/g/n mode ports and the remaining IAPs operating in 802.11a/n mode. Use of this mode is controlled by the Array’s license key. The key must include 802.11n capability, or you will not be able to enable this mode. See “License” on page 135 to view the features supported by your license key. Contact Xirrus Customer support for questions about your license.

If you select **Disabled**, then 802.11n operation is disabled on the Array. IAPs abgn1 through abgn4 will behave in the same way as IAPs abg1 to abg4 on the XS Arrays; the 802.11a/n IAPs will operate in 802.11a mode.

2. **TX Chains:** Select the number of separate data streams transmitted by the antennas of each IAP. The default is 3. See [“Multiple Data Streams—Spatial Multiplexing”](#) on page 62.
3. **RX Chains:** Select the number of separate data streams received by the antennas of each IAP. This number should be greater than or equal to **TX Chains**. The default is 3. See [“Multiple Data Streams—Spatial Multiplexing”](#) on page 62.
4. **Guard Interval:** Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short. See [“Short Guard Interval”](#) on page 64.
5. **Auto-configure Channel Bonding:** Select **Enabled** to use Channel Bonding and automatically select the best channels for bonding. The default is **Disabled**. See [“Channel Bonding”](#) on page 63.
6. **5 GHz Channel Bonding:** Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when Auto-Configure Channel Bonding is enabled. The default is **Dynamic**. See [“Channel Bonding”](#) on page 63.
7. **2.4 GHz Channel Bonding:** Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when Auto-Configure Channel Bonding is enabled, and the default is **Dynamic**. See [“Channel Bonding”](#) on page 63.



### Advanced RF Settings

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

Name: SS-XN8 ( 10.100.47.188 )		Location: SS Area		Uptime: 0 days, 18 hours, 35 minutes	
<b>RF Intrusion Detection</b>					
Intrusion Detection Mode:	<input type="radio"/> Off	<input checked="" type="radio"/> Standard	<input type="radio"/> Advanced		
Auto Block Unknown Rogue APs:	<input type="radio"/> Off	<input checked="" type="radio"/> On			
Auto Block RSSI:	<input type="text" value="-50"/>				
Auto Block Level:	Automatically block unknown rogue APs with no encryption				
<b>RF Resilience</b>					
Radio Assurance Mode:	Disabled				
Enable Standby Mode:	<input type="radio"/> Yes	<input checked="" type="radio"/> No			
Standby Target Address:	<input type="text"/>				
<b>RF Power &amp; Sensitivity</b>					
Cell Size Configuration:	Auto Configure				
Auto Cell Size Period (seconds):	<input type="text"/>	<input checked="" type="checkbox"/> None			
Auto Cell Size Overlap (%):	<input type="text" value="0"/>				
Auto Cell Min Tx Power (dBm):	<input type="text" value="10"/>	<input type="checkbox"/> Default			
Sharp Cell:	<input checked="" type="radio"/> Off	<input type="radio"/> On			
<b>RF Spectrum Management</b>					
Channel Configuration:	Factory Defaults	Auto Configure	Auto Negotiate & Configure		
Channel Configuration Status:	Idle				
Auto Channel Configuration Mode:	<input type="radio"/> On Array PowerUp	<input checked="" type="radio"/> Disabled			
Auto Channel Configure on Time (hh:mm):	<input type="text"/>				
Channel List Selection:	<input checked="" type="checkbox"/> 1 <input type="checkbox"/> 2 <input type="checkbox"/> 3 <input type="checkbox"/> 4 <input type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input type="checkbox"/> 7 <input type="checkbox"/> 8 <input type="checkbox"/> 9 <input type="checkbox"/> 10 <input checked="" type="checkbox"/> 11 <input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 40 <input checked="" type="checkbox"/> 44 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 52 <input checked="" type="checkbox"/> 56 <input checked="" type="checkbox"/> 60 <input checked="" type="checkbox"/> 64 <input type="checkbox"/> 100 <input type="checkbox"/> 104 <input type="checkbox"/> 108 <input type="checkbox"/> 112 <input type="checkbox"/> 116 <input type="checkbox"/> 120 <input type="checkbox"/> 124 <input type="checkbox"/> 128 <input type="checkbox"/> 132 <input type="checkbox"/> 136 <input type="checkbox"/> 140 <input checked="" type="checkbox"/> 149 <input checked="" type="checkbox"/> 153 <input checked="" type="checkbox"/> 157 <input checked="" type="checkbox"/> 161 <input checked="" type="checkbox"/> 165				
Auto Channel List:	Use Defaults	Use All Channels			
Public Safety:	<input checked="" type="radio"/> Off	<input type="radio"/> On			
					Apply Save

Figure 143. Advanced RF Settings

### About Standby Mode

Standby Mode supports the Array-to-Array fail-over capability. When you enable Standby Mode, the Array functions as a backup unit, and it enables its radios if it detects that its designated target Array has failed. The use of redundant Arrays to provide this fail-over capability allows Arrays to be used in mission-critical applications. In Standby Mode, an Array monitors beacons from the target Array. When the target has not been heard from for 40 seconds, the standby Array

enables its radios until it detects that the target Array has come back online. Standby Mode is off by default. Note that you must ensure that the configuration of the standby Array is correct. This window allows you to enable or disable Standby Mode and specify the primary Array that is the target of the backup unit. See also, [“Failover Planning” on page 67](#).

### About Blocking Rogue APs

If you classify a rogue AP as **blocked** (see [“Rogue Control List” on page 233](#)), then the Array will take measures to prevent stations from staying associated to the rogue. When the monitor radio abg(n)2 is scanning, any time it hears a beacon from a blocked rogue abg(n)2 sends out a broadcast “death” signal using the rogue’s BSSID and source address. This has the effect of tossing off all of a rogue AP’s clients approximately every 5 to 10 seconds, which is enough to make the rogue frustratingly unusable.

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

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

---

*Procedure for Configuring Advanced RF Settings***RF Intrusion Detection**

1. **Intrusion Detection:** This option allows you to establish the intrusion detection method, either Standard or Advanced, or you can choose **Off** to disable this feature. See [“Array Monitor and Radio Assurance Capabilities” on page 406](#) for more information.
  - **Standard**—enables the abg(n)2 radio as a monitor which collects Rogue AP information.
  - **Advanced**—this option works in conjunction with the Xirrus Defense Module intrusion detection software (XDM). In this mode, the built-in monitor radio (IAP abg(n)2) functions as an RF threat sensor. Self-monitoring is not enabled.
  - **Off**—IAP abg(n)2 does not function as a monitor.
2. **Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see [“About Blocking Rogue APs” on page 276](#)). Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block to **On**, and click **Apply**. Then the remaining Auto Block fields will be active.
3. **Auto Block RSSI:** Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.
4. **Auto Block Level:** Select rogue APs to block based on the level of encryption that they are using. The choices are:
  - Automatically block unknown rogue APs regardless of encryption.
  - Automatically block unknown rogue APs with no encryption.
  - Automatically block unknown rogue APs with WEP or no encryption.

## RF Resilience

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

Operation of Radio Assurance mode is described in detail in [“Array Monitor and Radio Assurance Capabilities”](#) on page 406.

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

- **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
  - **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of one or all of the radios if needed.
  - **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets, and schedule reboots if needed.
  - **Disabled**—Disable IAP radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.
6. **Enable Standby Mode:** Choose **Yes** to enable this Array to function as a backup unit for the target Array, or choose **No** to disable this feature. See [“About Standby Mode”](#) on page 275.
  7. **Standby Target Address:** If you enabled the Standby Mode, enter the MAC address of the target Array (i.e., the address of the primary Array that is being monitored and backed up by this Array). To find this MAC address, open the Array Info window on the target Array, and use the Gigabit1 MAC Address.

## RF Power & Sensitivity

For an overview of RF power and cell size settings, please see “Capacity and Cell Sizes” on page 52 and “Fine Tuning Cell Sizes” on page 53.



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

*The abg(n)2 radio must be in **monitor** mode, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See “Procedure for Manually Configuring IAPs” on page 256.*

*The **Intrusion Detection Mode** must **not** be set to **Advanced**. See “RF Intrusion Detection” on page 277.*

8. **Cell Size Configuration:** Click on the **Auto Configure** button to instruct the Array to determine and set the best cell size for each enabled IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP settings window, each enabled IAP will have its cell size set to **Auto**.
9. **Auto Cell Size Period:** You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient).
10. **Auto Cell Size Overlap (%):** Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB.
11. **Auto Cell Min Tx Power (dBm):** Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes.

- 12. Sharp Cell:** This feature reduces interference between neighboring Arrays or other Access Points by limiting to a defined boundary (cell size) the trailing edge bleed of RF energy. Choose **On** to enable the Sharp Cell functionality, or choose **Off** to disable this feature. See also, “[Fine Tuning Cell Sizes](#)” on page 53.

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

## RF Spectrum Management

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

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

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

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

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

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

15. **Auto Channel Configuration Mode:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP when the Array is powered up. Choose **On Array PowerUp** to enable this feature, or choose **Disabled** to disable this feature.
16. **Auto Channel Configure on Time:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here (in hours and minutes, using the format: hh:mm). Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated.
17. **Channel List Selection:** This list selects which channels are available to the auto channel algorithm. Channels that are not checked are left out of the auto channel selection process. Note that channels that have been locked by the user are also not available to the auto channel algorithm.
18. **Auto Channel List: Use All Channels** selects all available channels (this does not include locked channels). **Use Defaults** sets the auto channel list back to the defaults. This omits newer channels (100-140) because many wireless NICs don't support these channels.
19. **Public Safety:** This option adds two additional channels (191 and 195) in the 4.9GHz spectrum range for public safety usage by qualified organizations. Operating these channels **requires a license**, and so they are not for general purpose use. Using these channels without a license violates FCC rules. Warning notices are displayed when you enable this feature and select these channels. All 802.11a(n) and 802.11a/b/g(/n) radios may be set to these channels.
20. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

Coverage and Capacity Planning

Global Settings .11a

Global Settings .11bg

Global Settings .11n



IAPs

IAP Statistics Summary

IAP Settings

### LED Settings

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

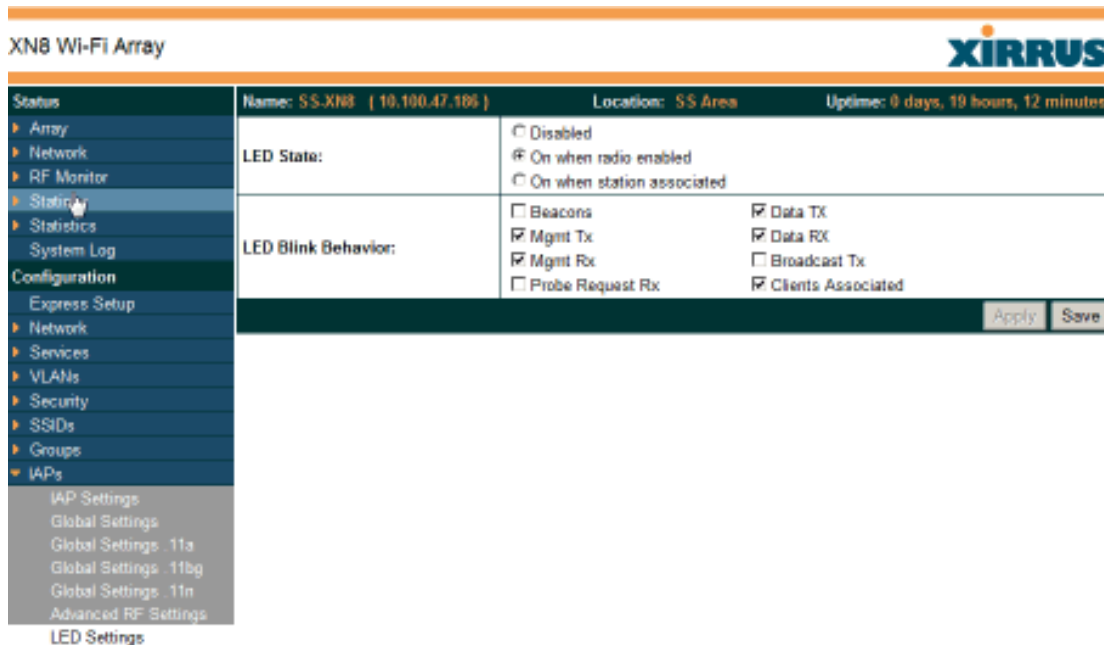


Figure 144. LED Settings

#### *Procedure for Configuring the IAP LEDs*

1. **LED State:** This option determines which event triggers the LEDs, either when an IAP is enabled or when an IAP first associates with the network. Choose **On Radio Enabled** or **On First Association**, as desired. You may also choose Disabled to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.
2. **LED Blink Behavior:** This option allows you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink.

See also, “Array LED Operating Sequences” on page 108.

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

*See Also*

Global Settings (IAP)

Global Settings .11a

Global Settings .11bg

IAPs

LED Boot Sequence

## WDS

This is a status-only window that provides an overview of all WDS links that have been defined. WDS (Wireless Distribution System) is a system that enables the interconnection of access points wirelessly, allowing your wireless network to be expanded using multiple access points without the need for a wired backbone to link them. The **Summary of WDS Client Links** shows the WDS links that you have defined on this Array and identifies the target Array for each by its base MAC address. The **Summary of WDS Host Links** shows the WDS links that have been established on this Array as a result of client Arrays associating to this Array (i.e., the client Arrays have this Array as their target). The summary identifies the source (client) Array for each link. Both summaries identify the IAPs that are part of the link and whether the connection for each is up or down. See “WDS Planning” on page 76 for an overview.

The screenshot shows the 'XN8 Wi-Fi Array' configuration page. The left sidebar contains a navigation menu with 'WDS' expanded to show 'WDS Client Links'. The main content area displays two summary tables. The top table, 'Summary of WDS Client Links', has columns for Link, State, Max IAPs, Target Array, Target SSID, IAP(s), Channel(s), and Connection(s). It lists four links, all with a state of 'Off' and 1 Max IAP. The bottom table, 'Summary of WDS Host Links', has columns for Link, State, Num IAPs, Source Array, Source SSID, IAP(s), Channel(s), and Connection(s). It also lists four links, all with a state of 'Off'. At the bottom right of the table area, it says 'This Array Address: 00:0f:7d:0b:b3:b0'.

Summary of WDS Client Links							
Link	State	Max IAPs	Target Array	Target SSID	IAP(s)	Channel(s)	Connection(s)
1	Off	1					
2	Off	1					
3	Off	1					
4	Off	1					

Summary of WDS Host Links							
Link	State	Num IAPs	Source Array	Source SSID	IAP(s)	Channel(s)	Connection(s)
1	Off						
2	Off						
3	Off						
4	Off						

This Array Address: 00:0f:7d:0b:b3:b0

Figure 145. WDS

### About Configuring WDS Links

A WDS link connects a client Array and a host Array (see Figure 146 on page 286). The host must be the Array that has a wired connection to the LAN. Client links from one or more Arrays may be connected to the host, and the host may also have client links. See “WDS Planning” on page 76 for more illustrations.

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

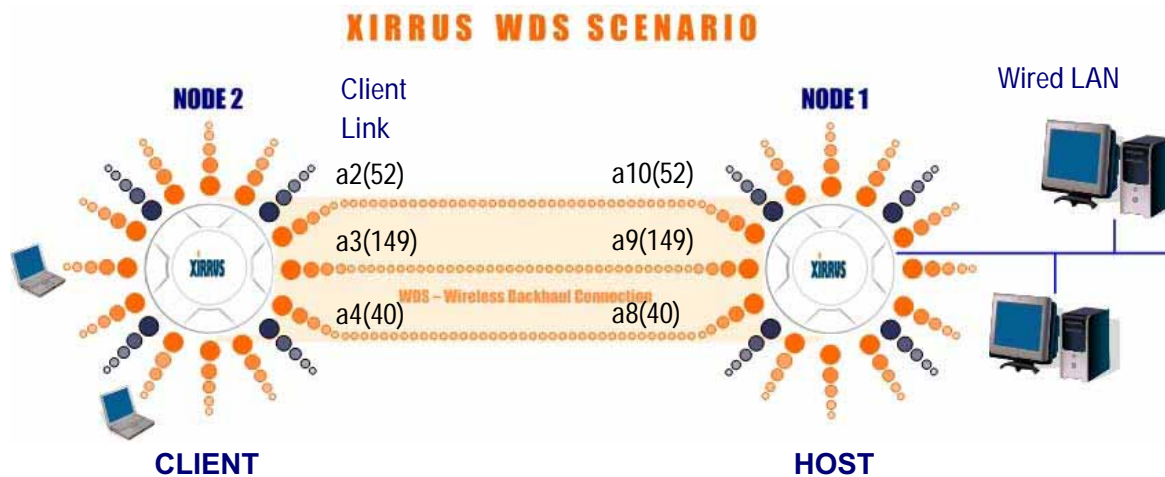


Figure 146. .Configuring a WDS Link



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

### See Also

[SSID Management](#)  
[WDS Client Link IAP Assignments:](#)  
[WDS Client Links](#)  
[WDS Statistics](#)

## WDS Client Links

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

Figure 147. WDS Client Links

### Procedure for Setting Up WDS Client Links

#### WDS Client Link Settings:

1. **Client Link:** Shows the ID (1 to 4) of each of the four possible WDS links.
2. **Enabled:** Check this box if you want to enable this WDS link, or uncheck the box to disable the link.
3. **Max IAPs Allowed (1-3):** Enter the maximum number of IAPs for this link, between 1 and 3.
4. **Target Array Base MAC Address:** Enter the base MAC address of the target Array (the host Array at the other side of this link). To find this MAC address, open the **WDS** window on the *target* Array, and use **This Array Address** located on the right under the Summary of WDS Host Links.

5. **Target SSID:** Enter the SSID that the target Array is using.
6. **Username:** Enter a username for this WDS link. A username and password is required if the SSID is using PEAP for WDS authentication from the internal RADIUS server.
7. **Password:** Enter a password for this WDS link.
8. **Clear Settings:** Click on the **Clear** button to reset all of the fields on this line.
9. Click on the **Apply** button to apply your changes to this session, or click **Save** to apply your changes and make them permanent.

#### WDS Client Link IAP Assignments:

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



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

11. **Auto Configure:** Click this button to instruct the Array to automatically determine the best channel allocation settings for each IAP that participates in a WDS link, based on changes in the environment. These changes are executed immediately, and are automatically applied.
12. **Reset All Links:** this command tears down all links configured on the Array and sets them back to their factory defaults, effective immediately.

#### See Also

[SSID Management](#)

[WDS Planning](#)

[WDS](#)

[WDS Statistics](#)

## Filters

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

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

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

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

**XNB Wi-Fi Array**

Status	Name: SS-XNB (10.100.47.186)		Location: SS Area		Uptime: 0 days, 22 hours, 5 minutes				
	Name	Type	Protocol	Port	Source	Destination	Set QoS	Set VLAN	Enabled
▶ Array	▼ Global								
▶ Network	new	allow	any	any	any	any			Yes
▶ RF Monitor	no-telnet	allow	any	any	any	any			Yes
▶ Stations	▼ Filters-A								
▶ Statistics	no-111	deny	any	any	111.111.111.0/24	any			Yes
▶ System Log	no-telnet	allow	any	any	any	any			Yes
Configuration									
▶ Express Setup									
▶ Network									
▶ Services									
▶ VLANs									
▶ Security									
▶ SSIDs									
▶ Groups									
▶ IAPs									
▶ WDS									
▼ Filters									
	Filter Lists								
	Filter Management								

**Orange arrow expands/collapses display**

Figure 148. Filters

## Filter Lists

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

The screenshot shows the 'XN8 Wi-Fi Array' configuration page. The top right corner features the XIRRUS logo. Below the title bar, there are fields for 'Name: SS-XN8 ( 10.100.47.186 )', 'Location: SS Area', and 'Uptime: 0 days, 21 hours, 17 minutes'. The main content area contains a table with the following data:

Filter List	On	Filters	SSIDs	User Groups	Delete
Global	<input checked="" type="checkbox"/>	1	all	all	
Filters-A	<input type="checkbox"/>	0	-	-	<input type="checkbox"/>
Filters-B	<input type="checkbox"/>				

Below the table, there is a 'Create' button and an 'Apply' button. The sidebar on the left includes sections for 'Status' (Array, Network, RF Monitor, Stations, Statistics, System Log) and 'Configuration' (Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, IAPs, WDS, Filters). The 'Filters' section is expanded to show 'Filter Lists' and 'Filter Management'.

Figure 149. Filter Lists

### *Procedure for Managing Filter Lists*

1. **New Filter List Name:** Enter a name for the new filter list in this field, then click on the Create button to create the list. All new filters are disabled when they are created. The new filter list is added to the Filter List table in the window. Click on the filter list name, and you will be taken to the **Filter Management** window for that filter list.
2. **On:** Check this box to enable this filter list, or leave it blank to disable the list. If the list is disabled, you may still add filters to it or modify it, but none of the filters will be applied to data traffic.
3. **Filters:** This read-only field displays the number of filters that belong to this filter list.



4. **SSIDs:** This read-only field lists the **SSIDs** that use this filter list.
5. **User Groups:** This read-only field lists the **Groups** that use this filter list.
6. **Delete:** Click this checkbox and then click the **Apply** or **Save** button to delete this filter list.
7. Click on the **Apply** button to apply your changes to the selected filter, or click **Save** to apply your changes and make them permanent.
8. Click a filter list to go to the **Filter Management** window to create and manage the filters that belong to this list.

### Filter Management

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

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

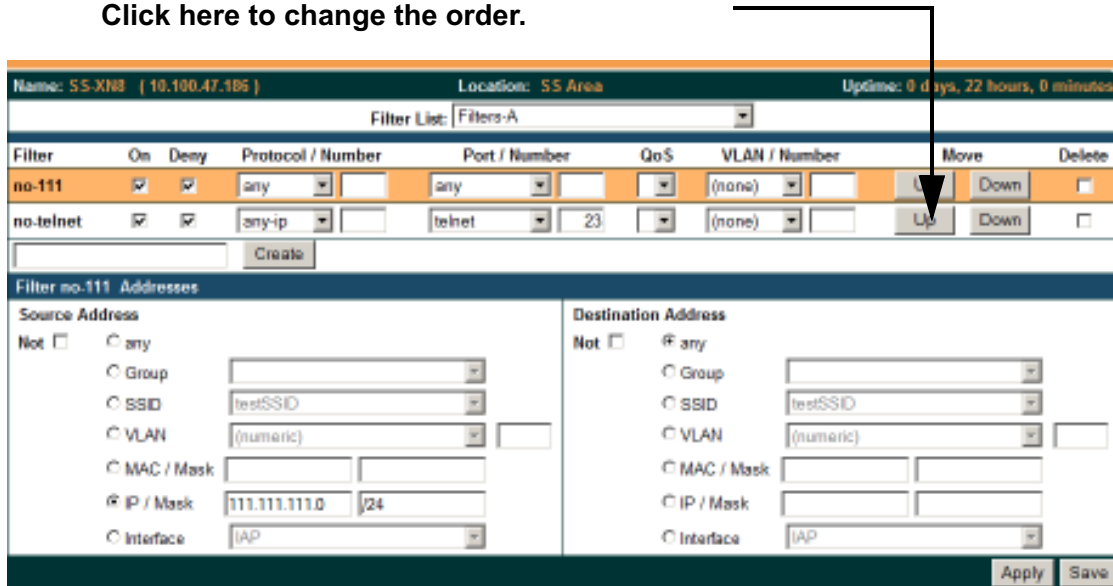


Figure 150. Filter Management

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

### *Procedure for Managing Filters*

1. **Filter List:** Select the filter list to display and manage on this window. All of the filters already defined for this list are shown, and you may create additional filters for this list.
2. **New Filter Name:** Enter a name for the new filter in the field next to the **Create** button, then click on the **Create** button to create the filter. All new filters are added to the table of filters at the top of the window. The filter name must be unique within the list, but it may have the same name as a filter in a different filter list. Two filters with the same name in different filter lists will be completely unrelated to each other—they may be defined with different parameter values.
3. **Filter:** Choose a filter entry to modify from the list at the top of the window.
4. **On:** Use this field to enable or disable this filter.
5. **Deny:** Choose whether this filter will be an **Allow** filter or a **Deny** filter. If you define the filter as an Allow filter, then any associations that meet the filter criteria will be allowed. If you define the filter as a Deny filter, any associations that meet the filter criteria will be denied.
6. **Protocol:** Choose a specific filter protocol from the pull-down list, or choose **numeric** and enter a **Number**, or choose **any** to instruct the Array to use the best filter. This is a match criterion.
7. **Port:** From the pull-down list, choose the type of port on which you want this filter to be active, or choose **1-65534** and enter a **Number**, or choose **any** to instruct the Array to apply the filter to any port. This is a match criterion.
8. **QoS:** (Optional) Set packets that match the filter criteria to this QoS level (0 to 3) from the pull-down list. Level 0 has the lowest priority; level 3 has the highest priority. By default, this field is blank and the filter does not modify QoS level. See [“Understanding QoS Priority on the Wi-Fi Array” on page 237](#).

9. **VLAN ID:** (Optional) Set packets that match the filter criteria to this VLAN. Select a VLAN from the pull-down list, or select **numeric** and enter the number of a previously defined VLAN (see “VLANs” on page 205).
10. **Move Up/Down:** The filters are applied in the order in which they are displayed in the list, with filters on the top applied first. To change an entry’s position in the list, just click its **Up** or **Down** button.
11. **Source Address:** Define a source address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.
12. **Destination Address:** Define a destination address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.
13. To delete a filter, check its **Delete** checkbox, then click the **Apply** or **Save** button.
14. Click on the **Apply** button to apply your changes to the selected filter, or click **Save** to apply your changes and make them permanent.

### *See Also*

[Filters](#)

[Filter Statistics](#)

[Understanding QoS Priority on the Wi-Fi Array](#)

[VLANs](#)



---

# Using Tools on the Wi-Fi Array

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

- **“System Tools” on page 296**
- **“CLI” on page 303**
- **“Logout” on page 305**

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

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

## System Tools

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

The screenshot displays the 'System Tools' interface for an XN8 Wi-Fi Array. The top header shows 'XN8 Wi-Fi Array' and the XIRRUS logo. The main content area is organized into several sections:

- System:** Includes 'Reboot' (Save & Reboot, Reboot), 'Software Upgrade' (Browse, Upgrade), and 'License Key' (12WWN-XXXXX-XXXXX-XXXXX, Upgrade).
- Configuration:** Includes 'Update From Remote File' (Browse, Update), 'Update From Local File' (dropdown, Update), and 'Download Current Configuration' (xs\_current.conf).
- Diagnostics:** Includes 'Diagnostic Log' (xs\_diagnostic.log, Create).
- Web Page Redirect:** Includes 'Upload File' (Browse, Upload) and 'Remove File' (Delete, List Files).
- Tools:** Includes 'System Command' (Trace Route, Ping, RADIUS Ping), 'Hostname / IP Address' (0.0.0.0), 'Timeout' (10), and 'Execute System Command' (Execute).
- Progress:** A section with a 'Status' indicator and a 'Progress' indicator, both highlighted with arrows and text annotations.

A sidebar on the left contains navigation options: Status, Array, Network, RF Monitor, Stations, Statistics, System Log, Configuration, Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, IAPs, WDS, Filters, and Tools. The Tools section is expanded to show System Tools, CLI, Logout, Log Messages, and a network diagram with nodes A1 through A4.

Figure 151. System Tools

### Procedure for Configuring System Tools

These tools are broken down into the following sections:

- System
- Configuration
- Diagnostics

- Web Page Redirect
- Tools
- Progress and Status Frames

## System

1. **Save & Reboot** or **Reboot**: Use **Save & Reboot** to save the current configuration and then reboot the Array. The LEDs on the Array indicate the progress of the reboot, as described in “Powering Up the Wi-Fi Array” on page 107. Alternatively, use the **Reboot** button to discard any configuration changes which have not been saved since the last reboot.
2. **Software Upgrade**: This feature upgrades the ArrayOS to a newer version provided by Xirrus. Enter the filename and directory location (or click on the **Browse** button to locate the software upgrade file), then click on the **Upgrade** button to upload the new file to the Array. Progress of the operation will be displayed below, in the **Progress** section. Completion status of the operation is shown in the **Status** section.

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



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

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

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

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

## Configuration

4. **Update from Remote File:** This field allows you to define the path to a configuration file (one that you previously saved—see [Step 6](#) below). Click on the **Browse** button if you need to browse for the location of the file, then click **Update** to update your configuration settings.
5. **Update from Local File:** This field updates Array settings from a local configuration file on the Array. Select one of the following files from the drop-down list:
  - **factory.conf:** The factory default settings
  - **lastboot.conf:** The setting values from just before the last reboot
  - **saved.conf:** The last settings that were explicitly saved

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

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



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

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



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



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

## Diagnostics

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

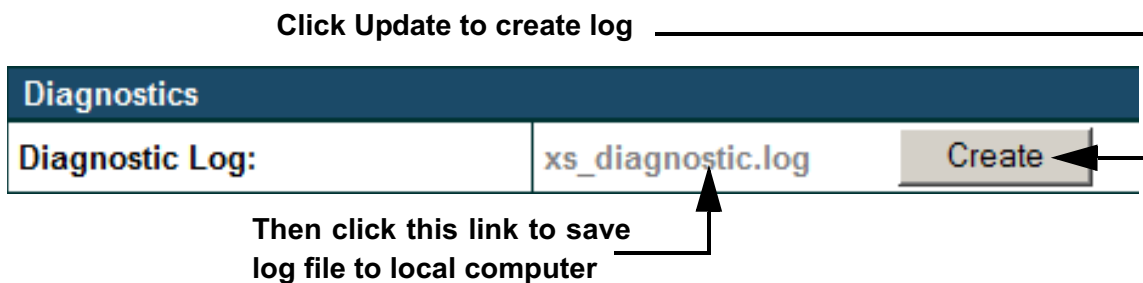


Figure 152. Saving the Diagnostic Log

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

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

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



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

### Web Page Redirect

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

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

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

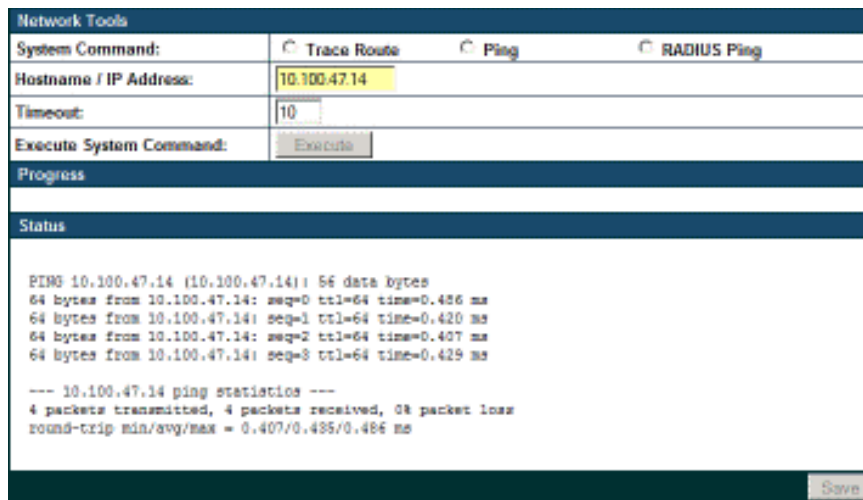
Figure 153. Managing WPR Splash/Login page files

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

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

10. **Remove File:** Enter the name of the WPR file you want to remove, then click on the **Delete** button. You can use the **List Files** button to show you a list of files that have been saved on the Array for WPR. The list is displayed in the **Status** section at the bottom of the WMI window. You must reboot to make your changes take effect.
11. **Download Sample Files:** Click on a link to access the corresponding sample WPR files:
  - **wpr.pl**—a sample Perl script.
  - **hs.css**—a sample cascading style sheet.

## Tools



Network Tools	
System Command:	<input type="radio"/> Trace Route <input checked="" type="radio"/> Ping <input type="radio"/> RADIUS Ping
Hostname / IP Address:	10.100.47.14
Timeout:	10
Execute System Command:	<input type="button" value="Execute"/>
Progress	
Status	
<pre> PING 10.100.47.14 (10.100.47.14): 56 data bytes 64 bytes from 10.100.47.14: seq=0 ttl=64 time=0.486 ms 64 bytes from 10.100.47.14: seq=1 ttl=64 time=0.420 ms 64 bytes from 10.100.47.14: seq=2 ttl=64 time=0.407 ms 64 bytes from 10.100.47.14: seq=3 ttl=64 time=0.429 ms  --- 10.100.47.14 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.407/0.485/0.486 ms           </pre>	
<input type="button" value="Save"/>	

Figure 154. System Command (Ping)

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

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

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

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

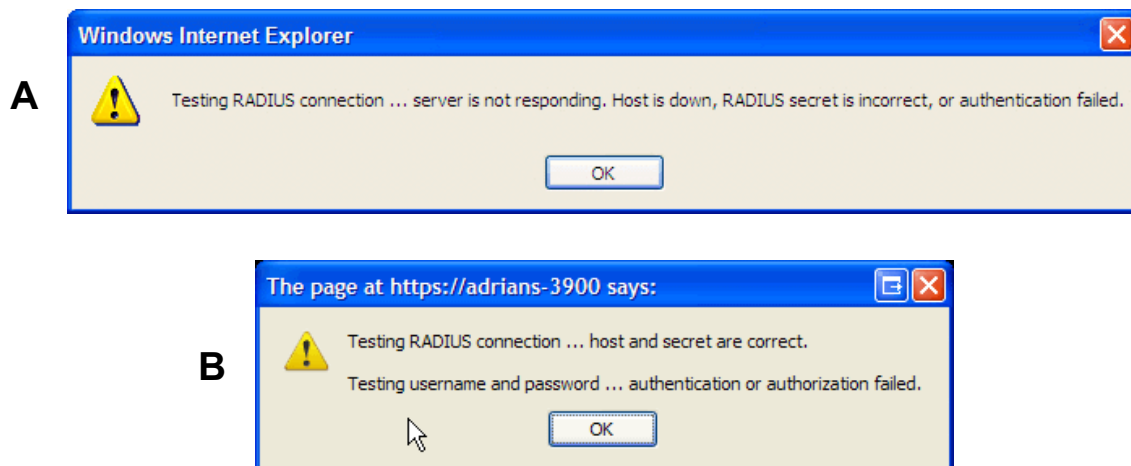


Figure 155. Radius Ping Output

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

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

### Progress and Status Frames

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

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

### CLI

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

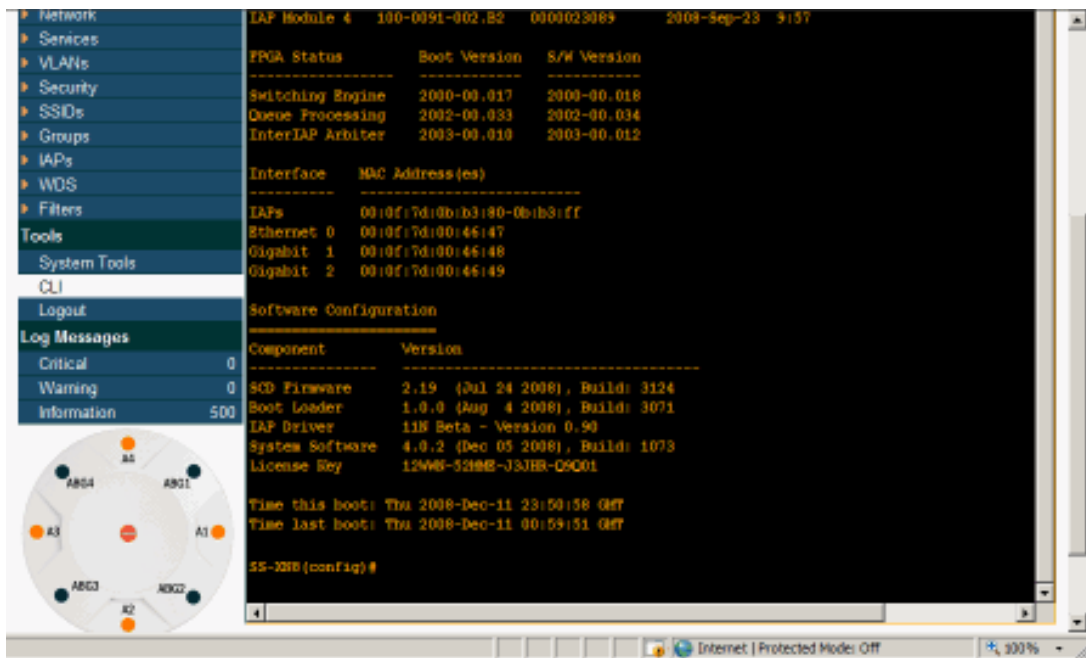


Figure 156. CLI Window

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

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

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

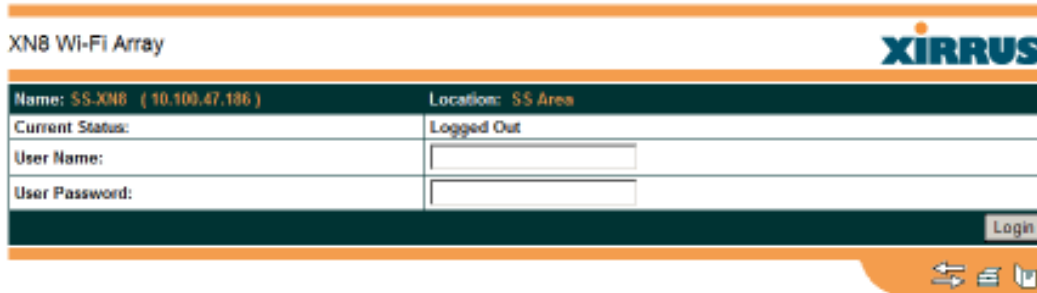
```
My-Array(config-iap) #
```

- You can abbreviate a command and it will be executed if you have typed enough of the command to be unambiguous. The command will not auto-complete, however. Only the abbreviated command that you actually typed will be shown. You can type a partial command and press Tab to have the command auto-complete. If the partial command is ambiguous a list of legal endings is displayed.
- Entering **quit** will return you to the previously viewed WMI page.
- Most, but not all, CLI commands can be run in this window. Specifically the **run-test** menu of commands is **not** available in this window. To use the run-test command, please connect using SSH and use CLI directly, or use the [System Tools](#) described in this chapter, such as Trace Route, Ping, and RADIUS Ping.

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

## Logout

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



XNB Wi-Fi Array	
Name: SS-XNB ( 10.100.47.186 )	Location: SS Area
Current Status:	Logged Out
User Name:	<input type="text"/>
User Password:	<input type="password"/>
<input type="button" value="Login"/>	

Figure 157. Login Window





---

# The Command Line Interface

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

- **"Establishing a Secure Shell (SSH) Connection" on page 308.**
- **"Getting Started with the CLI" on page 309.**
- **"Top Level Commands" on page 311.**
- **"Configuration Commands" on page 320.**
- **"Sample Configuration Tasks" on page 355.**

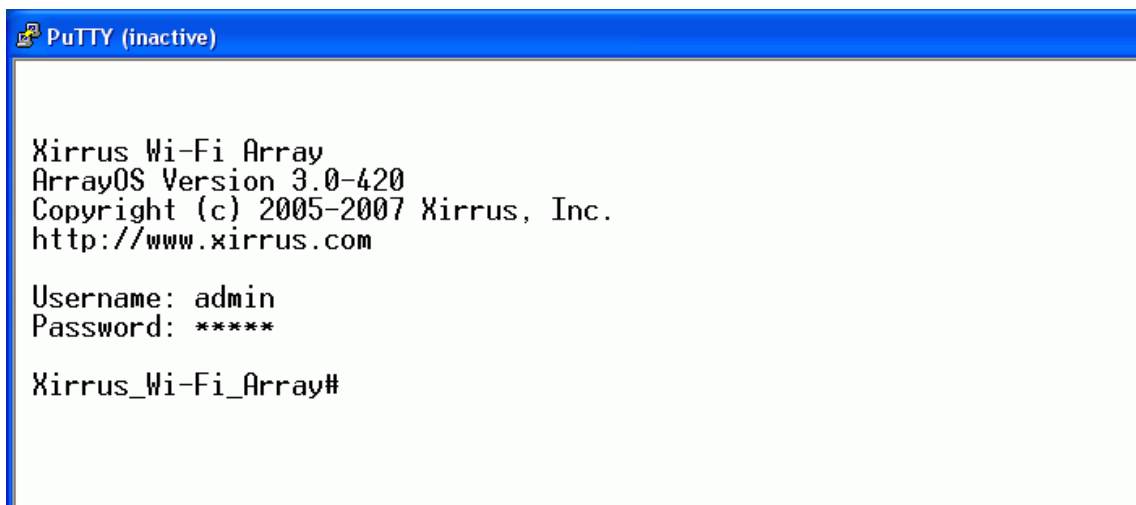
## *See Also*

Establishing Communication with the Array  
Network Map  
System Tools

## Establishing a Secure Shell (SSH) Connection

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

1. Start your SSH session and communicate with the Array via its default IP address (10.0.2.1 for both the Gigabit 1 and Gigabit 2 Ethernet ports).
2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the Array's Command Line Interface.



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

Username: admin
Password: *****

Xirrus_Wi-Fi_Array#
```

Figure 158. Logging In

## Getting Started with the CLI

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

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

## Inputting Commands

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

## Getting Help

The CLI offers the following two levels of assistance:

- **help Command**

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



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

Username: admin
Password: *****

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

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

Figure 159. Help Window

- **? Command**

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



```

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

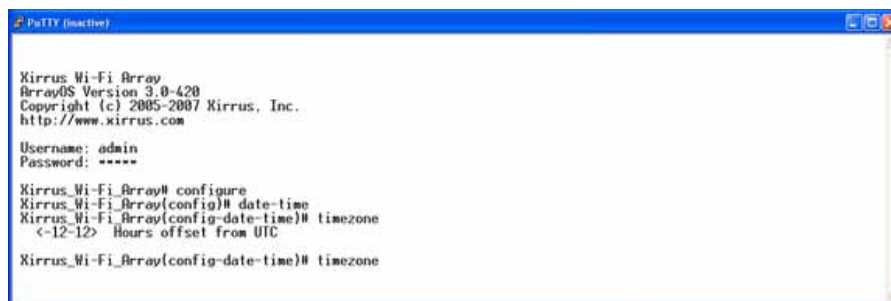
Username: admin
Password: ****

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

Xirrus_Wi-Fi_Array#
    
```

Figure 160. Full Help

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



```

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

Username: admin
Password: ****

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

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

Figure 161. Partial Help

## Top Level Commands

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

All other commands are considered second level configuration commands—these are the commands you use to configure specific elements of the Array’s features and functionality. For a listing of these commands with examples of command formats and structure, go to [“Configuration Commands” on page 320](#).

### Root Command Prompt

The following table shows the top level commands that are available from the root command prompt [**Xirrus\_Wi-Fi\_Array**].

Command	Description
<b>@</b>	Type <b>@n</b> to execute command <b>n</b> (as shown by the <a href="#">history</a> command).
<b>configure</b>	Enter the configuration mode. See <a href="#">“Configuration Commands” on page 320</a> .
<b>exit</b>	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.
<b>help</b>	Show a description of the interactive help system. See also, <a href="#">“Getting Help” on page 309</a> .
<b>history</b>	List history of commands that have been executed.
<b>more</b>	Turn terminal pagination ON or OFF.
<b>quit</b>	Exit the Command Line Interface (from any level).
<b>search</b>	Search for pattern in show command output.

Command	Description
<b>show</b>	Display information about the selected item. See “ <a href="#">show Commands</a> ” on page 315.
<b>statistics</b>	Display statistical data about the Array. See “ <a href="#">statistics Commands</a> ” on page 318.
<b>uptime</b>	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
<b>@</b>	Type <b>@n</b> to execute command <b>n</b> (as shown by the <a href="#">history</a> command).
<b>acl</b>	Configure the Access Control List.
<b>admin</b>	Define administrator access parameters.
<b>cdp</b>	Configure Cisco Discovery Protocol settings.
<b>clear</b>	Remove/clear the requested elements.
<b>contact-info</b>	Contact information for assistance on this Array.
<b>date-time</b>	Configure date and time settings.
<b>dhcp-server</b>	Configure the DHCP Server.
<b>dns</b>	Configure the DNS settings.
<b>end</b>	Exit the configuration mode.
<b>exit</b>	Go UP one mode level.
<b>file</b>	Manage the file system.
<b>filter</b>	Define protocol filter parameters.
<b>fips</b>	Enable/disable FIPS 140-2, Level 2 Security.

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

Command	Description
<b>show</b>	Display current information about the selected item.
<b>snmp</b>	Enable, disable or configure SNMP.
<b>ssh</b>	Enable/disable SSH.
<b>ssid</b>	Configure the SSID parameters.
<b>standby</b>	Configure the standby parameters.
<b>statistics</b>	Display statistics.
<b>syslog</b>	Enable, disable or configure the Syslog Server.
<b>telnet</b>	Enable/disable Telnet.
<b>uptime</b>	Display time since the last boot.
<b>vlan</b>	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
<b>acl</b>	Display the Access Control List.
<b>admin</b>	Display the administrator list or login information.
<b>array-info</b>	Display system information.
<b>associated-stations</b>	Display stations that have associated to the Array.
<b>boot-env</b>	Display Boot loader environment variables.
<b>capabilities</b>	Display detailed station capabilities.
<b>cdp</b>	Display Cisco Discovery Protocol settings.
<b>channel-list</b>	Display list of Array's 802.11a(n) and bg(n) channels.
<b>clear-text</b>	Display and enter passwords and secrets in the clear.
<b>conntrack</b>	Display the Connection Tracking table.
<b>console</b>	Display terminal settings.
<b>contact-info</b>	Display contact information.
<b>country-list</b>	Display countries that the Array can be set to support.
<b>date-time</b>	Display date and time settings summary.
<b>dhcp-leases</b>	Display IP addresses (leases) assigned to stations by the DHCP server.
<b>dhcp-pool</b>	Display internal DHCP server settings summary information.

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

Command	Description
<b>saved-config</b>	Display the last saved Array configuration.
<b>security</b>	Display security settings summary information.
<b>self-test</b>	Display self test results.
<b>snmp</b>	Display SNMP summary information.
<b>spanning-tree</b>	Display spanning tree information.
<b>spectrum-analyzer</b>	Display spectrum analyzer measurements.
<b>ssid</b>	Display SSID summary information.
<b>stations</b>	Display station information.
<b>statistics</b>	Display statistics.
<b>syslog</b>	Display the system log.
<b>syslog-settings</b>	Display the system log (Syslog) settings.
<b>temperature</b>	Display the current board temperatures.
<b>unassociated-stations</b>	Display unassociated station information.
<b>vlan</b>	Display VLAN information.
<b>wds</b>	Display WDS information.
<b>&lt;cr&gt;</b>	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
<b>ethernet</b>	Display statistical data for all Ethernet interfaces.
Ethernet Name <b>eth0, gig1, gig2</b>	Display statistical data for the defined Ethernet interface (either eth0, gig1 or gig2). FORMAT: <b>statistics gig1</b>
<b>filter</b>	Display statistics for defined filters (if any). FORMAT: <b>statistics filter [detail]</b>
<b>filter-list</b>	Display statistics for defined filter list (if any). FORMAT: <b>statistics filter &lt;filter-list&gt;</b>
<b>iap</b>	Display statistical data for the defined IAP. FORMAT: <b>statistics iap abgn4</b>
<b>station</b>	Display statistical data about associated stations. FORMAT: <b>statistics station billw</b>
<b>vlan</b>	Display statistical data for the defined VLAN. You must use the VLAN number (not its name) when defining a VLAN. FORMAT: <b>statistics vlan 1</b>
<b>wds</b>	Display statistical data for the defined active WDS (Wireless Distribution System) links. FORMAT: <b>statistics wds 1</b>

---

Command	Description
<cr>	Display configuration or status information.

## Configuration Commands

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

To see examples of some of the key configuration tasks and their associated commands, go to [“Sample Configuration Tasks”](#) on page 355.

### acl

The **acl** command [**Xirrus\_Wi-Fi\_Array(config)# acl**] is used to configure the Access Control List.

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

## admin

The **admin** command [Xirrus\_Wi-Fi\_Array(config-admin)#] is used to configure the Administrator List.

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

## cdp

The **cdp** command [Xirrus\_Wi-Fi\_Array(config)# **cdp**] is used to configure the Cisco Discovery Protocol.

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



**clear**

The **clear** command [Xirrus\_Wi-Fi\_Array(config)# **clear**] is used to clear requested elements.

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

### contact-info

The **contact-info** command [Xirrus\_Wi-Fi\_Array(config)# **contact-info**] is used for managing administrator contact information.

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

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

### dhcp-server

The **dhcp-server** command [**Xirrus\_Wi-Fi\_Array(config-dhcp-server)#**] is used to add, delete and modify DHCP pools.

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

## dns

The **dns** command [**Xirrus\_Wi-Fi\_Array(config-dns)#**] is used to configure your DNS parameters.

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

**file**

The **file** command [Xirrus\_Wi-Fi\_Array(config-file)#] is used to manage files.

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

Command	Description
<b>remote-config</b>	<p>When the Array boots up, it fetches the specified configuration file from the TFTP server defined in the <b>file remote-server</b> command, and uses this configuration. This must be an Array configuration file with a <b>.conf</b> 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 <b>ipaddr</b> line from the file. You can then load the file on each array and the local IP addresses will not change.</p> <p>FORMAT:  <b>file remote-config &lt;config-file.conf&gt;</b></p> <p><b>Note:</b> If you enter <b>file remote-config ?</b>, the help response suggests possibilities by listing all of the configuration files that are currently in the Array's flash.</p>
<b>remote-image</b>	<p>When the Array boots up, it fetches the named image file from the TFTP server defined in the <b>file remote-server</b> command, and upgrades to this file before booting. This must be an Array image file with a <b>.bin</b> extension.</p> <p>FORMAT:  <b>file remote-image &lt;image-file.bin&gt;</b></p> <p><b>Note:</b> 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>
<b>remote-server</b>	<p>Sets up a TFTP server to be used for automated remote update of software image and configuration files when rebooting.</p> <p>FORMAT:  <b>file remote-server A.B.C.D</b></p>
<b>rename</b>	Rename a file.
<b>scp</b>	Copy a file to or from a remote system.

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