



## Wi-Fi Arrays

August 9, 2011  
Release 6.0





# Wi-Fi Array™

## XR Series

All rights reserved. This document may not be reproduced or disclosed in whole or in part by any means without the written consent of Xirrus, Inc.

**Part Number: 800-0022-001**  
(Revision A)



## Trademarks

**XIRRUS** is a registered trademark of Xirrus, Inc. All other trademarks and brand names are marks of their respective holders.

Please see Legal Notices, Warnings, Compliance Statements, and Warranty and License Agreements in “Appendix F: Notices” on page 437.

Xirrus, Inc.

2101 Corporate Center Drive

Thousand Oaks, CA 91320

USA

Tel: 1.805.262.1600

1.800.947.7871 Toll Free in the US

Fax: 1.866.462.3980

*[www.xirrus.com](http://www.xirrus.com)*

# Table of Contents

<b>List of Figures.....</b>	<b>xi</b>
<b>Introduction .....</b>	<b>1</b>
The Xirrus Family of Products .....	1
Nomenclature .....	3
About this User’s Guide .....	4
Organization .....	4
Notes and Cautions .....	6
Screen Images .....	6
Your User’s Guide as a PDF Document .....	6
Hyperlinks .....	6
Why Choose the Xirrus Wi-Fi Array? .....	6
Wi-Fi Array Product Overview .....	7
Enterprise Class Security .....	8
Deployment Flexibility .....	9
Power over Gigabit Ethernet (PoGE) .....	10
Enterprise Class Management .....	10
Key Features and Benefits .....	12
High Capacity and High Performance .....	12
Extended Coverage .....	12
Non-Overlapping Channels .....	13
SDMA Optimization .....	13
Fast Roaming .....	13
Easy Deployment .....	13
Secure Wireless Access .....	13
Applications Enablement .....	14
Advanced Feature Sets .....	14
Xirrus Advanced RF Performance Manager (RPM) .....	14
Xirrus Advanced RF Security Manager (RSM) .....	15
Xirrus Advanced RF Analysis Manager (RAM) .....	16
<b>Installing the Wi-Fi Array .....</b>	<b>19</b>
Installation Prerequisites .....	19

---

Optional Network Components .....	21
Client Requirements .....	21
Planning Your Installation .....	22
General Deployment Considerations .....	22
Coverage and Capacity Planning .....	24
Placement .....	24
RF Patterns .....	25
Capacity and Cell Sizes .....	27
Fine Tuning Cell Sizes .....	28
Roaming Considerations .....	29
Allocating Channels .....	29
Deployment Examples .....	32
IEEE 802.11n Deployment Considerations .....	34
MIMO (Multiple-In Multiple-Out) .....	35
Multiple Data Streams—Spatial Multiplexing .....	37
Channel Bonding .....	38
Improved MAC Throughput .....	39
Short Guard Interval .....	39
Obtaining Higher Data Rates .....	40
802.11n Capacity .....	41
Failover Planning .....	42
Port Failover Protection .....	42
Switch Failover Protection .....	43
Power Planning .....	44
Power over Gigabit Ethernet .....	44
Security Planning .....	45
Wireless Encryption .....	45
Authentication .....	45
Meeting PCI DSS Standards .....	46
Meeting FIPS Standards .....	46
Port Requirements .....	48
Network Management Planning .....	51
WDS Planning .....	52
Common Deployment Options .....	55
Installation Workflow .....	56
Installing Your Wi-Fi Array .....	58
Choosing a Location .....	58

---

Wiring Considerations .....	59
Mounting the Array .....	61
Dismounting the Array .....	61
Powering Up the Wi-Fi Array .....	62
Array LED Operating Sequences .....	63
LED Boot Sequence .....	63
LED Operation when Array is Running .....	64
Establishing Communication with the Array .....	65
Using the Serial Port .....	65
Using the Ethernet Ports .....	65
Starting the WMI .....	66
Logging In .....	66
Entering the License .....	66
Performing the Express Setup Procedure .....	68
Procedure for Performing an Express Setup .....	69
<b>The Web Management Interface .....</b>	<b>75</b>
An Overview .....	76
Structure of the WMI .....	77
User Interface .....	79
Utility Buttons .....	81
Logging In .....	83
Applying Configuration Changes .....	83
Character Restrictions .....	84
<b>Viewing Status on the Wi-Fi Array .....</b>	<b>85</b>
Array Status Windows .....	86
Array Summary .....	86
Content of the Array Summary Window .....	87
Array Information .....	90
Array Configuration .....	91
Admin History .....	92
Network Status Windows .....	92
Network .....	93
Network Map .....	94
Content of the Network Map Window .....	94
Spanning Tree Status .....	97

---

Routing Table .....	98
ARP Table .....	98
DHCP Leases .....	99
Connection Tracking/NAT .....	99
CDP Neighbors .....	100
Network Assurance .....	101
RF Monitor Windows .....	102
IAPs .....	103
Spectrum Analyzer .....	104
Intrusion Detection .....	107
Channel History .....	109
Station Status Windows .....	111
Stations .....	112
Location Map .....	113
RSSI .....	118
Signal-to-Noise Ratio (SNR) .....	120
Noise Floor .....	122
Max by IAP .....	124
Station Assurance .....	125
Statistics Windows .....	126
IAP Statistics Summary .....	126
Per-IAP Statistics .....	127
Network Statistics .....	129
VLAN Statistics .....	130
WDS Statistics .....	131
Filter Statistics .....	132
Station Statistics .....	132
Per-Station Statistics .....	133
System Log Window .....	134
IDS Event Log Window .....	135
<b>Configuring the Wi-Fi Array .....</b>	<b>137</b>
Express Setup .....	139
Network .....	146
Network Interfaces .....	147
DNS Settings .....	153
CDP Settings .....	154

---



---

Services .....	156
Time Settings (NTP) .....	157
NetFlow .....	159
Wi-Fi Tag .....	161
System Log .....	162
SNMP .....	165
DHCP Server .....	168
VLANs .....	171
Understanding Virtual Tunnels .....	171
VLAN Management .....	173
Security .....	175
Understanding Security .....	176
Certificates and Connecting Securely to the WMI .....	179
Using the Array’s Default Certificate .....	180
Using an External Certificate Authority .....	181
Admin Management .....	181
Admin Privileges .....	183
Admin RADIUS .....	185
About Creating Admin Accounts on the RADIUS Server .....	185
Management Control .....	188
Access Control List .....	195
Global Settings .....	197
External Radius .....	200
About Creating User Accounts on the RADIUS Server .....	201
Internal Radius .....	204
Rogue Control List .....	206
SSIDs .....	208
Understanding SSIDs .....	209
Understanding QoS Priority on the Wi-Fi Array .....	210
SSID Management .....	213
SSID List (top of page) .....	214
SSID Limits .....	218
Web Page Redirect Configuration Settings .....	219
WPA Configuration Settings .....	223
RADIUS Configuration Settings .....	224
Active IAPs .....	225
Per-SSID Access Control List .....	226

---

Groups .....	228
Understanding Groups .....	228
Using Groups .....	229
Group Management .....	230
Group Limits .....	232
IAPs .....	234
Understanding Fast Roaming .....	235
IAP Settings .....	237
Global Settings (IAP) .....	243
Beacon Configuration .....	245
Station Management .....	245
Advanced Traffic Optimization .....	246
Global Settings .11a .....	250
Global Settings .11bg .....	254
Global Settings .11n .....	259
Advanced RF Settings .....	262
About Standby Mode .....	262
RF Monitor .....	263
RF Resilience .....	263
RF Power & Sensitivity .....	264
RF Spectrum Management .....	265
Station Assurance .....	267
Intrusion Detection .....	270
DoS Attacks .....	271
Impersonation Attacks .....	272
About Blocking Rogue APs .....	273
RF Intrusion Detection and Auto Block Mode .....	273
DoS Attack Detection Settings .....	274
Impersonation Detection Settings .....	275
LED Settings .....	276
WDS .....	278
About Configuring WDS Links .....	278
Long Distance Links .....	279
WDS Client Links .....	280
Filters .....	283
Filter Lists .....	284
Filter Management .....	286

---

Clusters .....	289
Cluster Definition .....	290
Cluster Management .....	291
Cluster Operation .....	292
<b>Using Tools on the Wi-Fi Array .....</b>	<b>295</b>
System Tools .....	296
About Licensing and Upgrades .....	297
System .....	298
Automatic Updates from Remote Image or Configuration File ....	299
Configuration .....	300
Diagnostics .....	302
Web Page Redirect .....	304
Network Tools .....	305
Progress and Status Frames .....	307
CLI .....	308
Options .....	309
Logout .....	312
<b>The Command Line Interface .....</b>	<b>313</b>
Establishing a Secure Shell (SSH) Connection .....	313
Getting Started with the CLI .....	315
Inputting Commands .....	315
Getting Help .....	315
Top Level Commands .....	317
Root Command Prompt .....	317
configure Commands .....	318
show Commands .....	321
statistics Commands .....	324
Configuration Commands .....	326
acl .....	326
admin .....	327
cdp .....	328
clear .....	329
cluster .....	330
contact-info .....	331
date-time .....	332

---

dhcp-server .....	333
dns .....	334
file .....	335
filter .....	338
group .....	340
hostname .....	340
interface .....	341
load .....	342
location .....	342
management .....	343
more .....	344
netflow .....	345
no .....	346
quit .....	348
radius-server .....	348
reboot .....	349
reset .....	349
restore .....	350
run-tests .....	351
security .....	353
snmp .....	354
ssid .....	355
syslog .....	356
uptime .....	357
vlan .....	358
wifi-tag .....	359
Sample Configuration Tasks .....	360
Configuring a Simple Open Global SSID .....	361
Configuring a Global SSID using WPA-PEAP .....	362
Configuring an SSID-Specific SSID using WPA-PEAP .....	363
Enabling Global IAPs .....	364
Disabling Global IAPs .....	365
Enabling a Specific IAP .....	366
Disabling a Specific IAP .....	367
Setting Cell Size Auto-Configuration for All IAPs .....	368
Setting the Cell Size for All IAPs .....	369
Setting the Cell Size for a Specific IAP .....	370

---

Configuring VLANs on an Open SSID .....	371
Configuring Radio Assurance Mode (Loopback Tests) .....	372
<b>Appendices .....</b>	<b>375</b>
<b>Appendix A: Servicing the Wi-Fi Array .....</b>	<b>377</b>
Removing the Access Panel .....	379
Reinstalling the Access Panel .....	382
Replacing the FLASH Memory Module .....	384
Replacing the Main System Memory .....	386
Replacing the Integrated Access Point Radio Module .....	388
Replacing the Power Supply Module .....	391
<b>Appendix B: Quick Reference Guide .....</b>	<b>393</b>
Factory Default Settings .....	393
Host Name .....	393
Network Interfaces .....	393
Serial .....	393
Gigabit 1 and Gigabit 2 .....	394
Fast Ethernet .....	394
Server Settings .....	395
NTP .....	395
Syslog .....	395
SNMP .....	396
DHCP .....	396
Default SSID .....	397
Security .....	397
Global Settings - Encryption .....	397
External RADIUS (Global) .....	398
Internal RADIUS .....	399
Administrator Account and Password .....	399
Management .....	399
Keyboard Shortcuts .....	399
<b>Appendix C: Technical Support .....</b>	<b>403</b>
General Hints and Tips .....	403
Frequently Asked Questions .....	404
Multiple SSIDs .....	404
Security .....	406

---

VLAN Support .....	410
Array Monitor and Radio Assurance Capabilities .....	412
Enabling Monitoring on the Array .....	412
How Monitoring Works .....	412
Radio Assurance .....	413
Radio Assurance Options .....	414
RADIUS Vendor Specific Attributes (VSAs) for Xirrus .....	415
Upgrading the Array via CLI .....	418
Sample Output for the Upgrade Procedure: .....	419
Contact Information .....	423
<b>Appendix D: Implementing PCI DSS .....</b>	<b>425</b>
Payment Card Industry Data Security Standard Overview .....	425
PCI DSS and Wireless .....	426
The Xirrus Array PCI Compliance Configuration .....	427
The pci-audit Command .....	428
Additional Resources .....	429
<b>Appendix E: Implementing FIPS Security .....</b>	<b>431</b>
Securing the Array Physically .....	431
Operator Required Actions .....	431
To implement FIPS 140-2, Level 2 using WMI .....	434
To implement FIPS 140-2, Level 2 using CLI: .....	436
To check if an Array is in FIPS mode: .....	436
<b>Appendix F: Notices .....</b>	<b>437</b>
Notices .....	437
EU Directive 1999/5/EC Compliance Information .....	440
Compliance Information (Non-EU) .....	447
Safety Warnings .....	448
Translated Safety Warnings .....	449
Software License and Product Warranty Agreement .....	450
Hardware Warranty Agreement .....	456
<b>Glossary of Terms.....</b>	<b>459</b>
<b>Index.....</b>	<b>471</b>

# List of Figures

Figure 1.	Xirrus Arrays: XR Series (on left) and XN Series .....	1
Figure 2.	The Xirrus Management System .....	2
Figure 3.	Wi-Fi Array (XR Series) .....	8
Figure 4.	Wireless Coverage Patterns .....	9
Figure 5.	WMI: Array Status.....	11
Figure 6.	Layout of IAPs (XR4830) .....	12
Figure 7.	Wall Thickness Considerations .....	23
Figure 8.	Unit Placement.....	24
Figure 9.	Full (Normal) Coverage.....	25
Figure 10.	Adjusting RF Patterns .....	26
Figure 11.	Custom Coverage .....	26
Figure 12.	Connection Rate vs. Distance.....	27
Figure 13.	Transmit Power.....	28
Figure 14.	Overlapping Cells.....	29
Figure 15.	Allocating Channels Manually .....	31
Figure 16.	Deployment Scenario (54 Mbps)—Per Sector.....	32
Figure 17.	Deployment Scenario (36 Mbps)—Per Sector.....	32
Figure 18.	Deployment Scenario (18 Mbps)—Per Sector.....	33
Figure 19.	Classic 802.11 Signal Transmission .....	35
Figure 20.	MIMO Signal Processing .....	36
Figure 21.	Spatial Multiplexing .....	37
Figure 22.	Channel Bonding .....	38
Figure 23.	MAC Throughput Improvements.....	39
Figure 24.	Computing 802.11n Data Rates .....	40
Figure 25.	802.11n Increases Capacity .....	41
Figure 26.	Port Failover Protection .....	42
Figure 27.	Switch Failover Protection .....	43
Figure 28.	Port Requirements for XMS .....	48
Figure 29.	WDS Link.....	52
Figure 30.	A Multiple Hop WDS Connection .....	53
Figure 31.	WDS Failover Protection .....	53
Figure 32.	Installation Workflow .....	56
Figure 33.	Array Placement .....	58
Figure 34.	LED Locations .....	62

Figure 35.	Network Interface Ports.....	65
Figure 36.	Express Setup .....	68
Figure 37.	Web Management Interface .....	76
Figure 38.	WMI: Frames .....	79
Figure 39.	Major Menu Sections Collapsed (on left) .....	80
Figure 40.	WMI: Utility Buttons.....	81
Figure 41.	Feedback Form.....	82
Figure 42.	Logging In to the Wi-Fi Array .....	83
Figure 43.	Array Summary .....	86
Figure 44.	Disabled IAP (Partial View).....	88
Figure 45.	IAP Cells .....	89
Figure 46.	Array Information .....	90
Figure 47.	Show Configuration.....	91
Figure 48.	Admin Login History.....	92
Figure 49.	Network Settings .....	93
Figure 50.	Network Map .....	94
Figure 51.	Spanning Tree Status.....	97
Figure 52.	Routing Table .....	98
Figure 53.	ARP Table .....	98
Figure 54.	DHCP Leases.....	99
Figure 55.	Connection Tracking .....	99
Figure 56.	CDP Neighbors .....	100
Figure 57.	Network Assurance.....	101
Figure 58.	RF Monitor—IAPs .....	103
Figure 59.	RF Monitor—IAPs .....	103
Figure 60.	RF Spectrum Analyzer.....	105
Figure 61.	Intrusion Detection/Rogue AP List.....	107
Figure 62.	RF Monitor—Channel History.....	109
Figure 63.	RF Monitor—Channel History (Rotated) .....	110
Figure 64.	RF Monitor—Channel History (Text) .....	110
Figure 65.	Stations .....	112
Figure 66.	Location Map.....	113
Figure 67.	Controls for Location Map .....	115
Figure 68.	Minimizing stations.....	116
Figure 69.	Station RSSI Values .....	118
Figure 70.	Station RSSI Values—Colorized Graphical View .....	119
Figure 71.	Station Signal-to-Noise Ratio Values .....	120



---

Figure 72.	Station SNR Values—Colorized Graphical View .....	121
Figure 73.	Station Noise Floor Values .....	122
Figure 74.	Station Noise Floor Values—Colorized Graphical View .....	123
Figure 75.	Max by IAP .....	124
Figure 76.	Station Assurance .....	125
Figure 77.	IAP Statistics Summary Page.....	127
Figure 78.	Individual IAP Statistics Page .....	128
Figure 79.	Network Statistics.....	129
Figure 80.	VLAN Statistics.....	130
Figure 81.	WDS Statistics .....	131
Figure 82.	Filter Statistics .....	132
Figure 83.	Station Statistics .....	132
Figure 84.	Individual Station Statistics Page.....	133
Figure 85.	System Log (Alert Level Highlighted) .....	134
Figure 86.	IDS Event Log .....	135
Figure 87.	WMI: Express Setup .....	139
Figure 88.	Network Interfaces .....	146
Figure 89.	Network Settings .....	147
Figure 90.	Port Modes (a-b) .....	149
Figure 91.	Port Modes (c-d) .....	150
Figure 92.	Port Modes (e-f) .....	151
Figure 93.	DNS Settings.....	153
Figure 94.	CDP Settings.....	154
Figure 95.	Services.....	156
Figure 96.	Time Settings (Manual Time).....	157
Figure 97.	Time Settings (NTP Time Enabled).....	158
Figure 98.	NetFlow .....	160
Figure 99.	Wi-Fi Tag.....	161
Figure 100.	System Log .....	162
Figure 101.	SNMP .....	165
Figure 102.	DHCP Management .....	168
Figure 103.	VLANs.....	171
Figure 104.	VLAN Management .....	173
Figure 105.	Security.....	175
Figure 106.	Import Xirrus Certificate Authority .....	180
Figure 107.	Admin Management .....	181
Figure 108.	Admin Privileges .....	183

---

Figure 109. Admin RADIUS .....	186
Figure 110. Management Control .....	188
Figure 111. Pre-login Banner .....	189
Figure 112. Access Control List .....	195
Figure 113. Global Settings (Security) .....	197
Figure 114. External RADIUS Server .....	200
Figure 115. Internal RADIUS Server .....	204
Figure 116. Rogue Control List .....	206
Figure 117. SSIDs .....	208
Figure 118. Four Traffic Classes .....	210
Figure 119. SSID Management .....	213
Figure 120. SSID Management .....	217
Figure 121. WPR Internal Splash Page Fields (SSID Management).....	220
Figure 122. Customizing an Internal Login or Splash Page.....	223
Figure 123. Setting Active IAPs per SSID .....	225
Figure 124. Per-SSID Access Control List .....	226
Figure 125. Groups.....	228
Figure 126. Group Management .....	230
Figure 127. IAPs.....	234
Figure 128. Source of Channel Setting .....	235
Figure 129. IAP Settings .....	237
Figure 130. Global Settings (IAPs) .....	243
Figure 131. Global Settings .11a .....	250
Figure 132. Global Settings .11bg.....	254
Figure 133. Global Settings .11n .....	259
Figure 134. Advanced RF Settings.....	262
Figure 135. Station Assurance (Advanced RF Settings) .....	268
Figure 136. Intrusion Detection Settings.....	270
Figure 137. LED Settings .....	276
Figure 138. WDS.....	278
Figure 139. .Configuring a WDS Link.....	279
Figure 140. WDS Client Links .....	280
Figure 141. Filters .....	283
Figure 142. Filter Lists .....	284
Figure 143. Filter Management .....	286
Figure 144. Clusters .....	289
Figure 145. Cluster Definition .....	290

Figure 146. Cluster Management.....	291
Figure 147. Cluster Mode Operation.....	292
Figure 148. Cluster Mode Activation .....	292
Figure 149. Viewing Statistics in Cluster Mode.....	293
Figure 150. System Tools.....	296
Figure 151. Saving the Diagnostic Log.....	303
Figure 152. Managing WPR Splash/Login page files.....	304
Figure 153. System Command (Ping).....	305
Figure 154. Radius Ping Command.....	305
Figure 155. Radius Ping Output.....	306
Figure 156. CLI Window .....	308
Figure 157. WMI Display Options .....	309
Figure 158. iPhone Style Option.....	310
Figure 159. Login Window .....	312
Figure 160. Logging In.....	314
Figure 161. Help Window .....	315
Figure 162. Full Help .....	316
Figure 163. Partial Help.....	316
Figure 164. Configuring a Simple Open Global SSID.....	361
Figure 165. Configuring a Global SSID using WPA-PEAP.....	362
Figure 166. Configuring an SSID-Specific SSID using WPA-PEAP.....	363
Figure 167. Enabling Global IAPs.....	364
Figure 168. Disabling Global IAPs.....	365
Figure 169. Enabling a Specific IAP.....	366
Figure 170. Disabling a Specific IAP.....	367
Figure 171. Setting the Cell Size for All IAPs.....	368
Figure 172. Setting the Cell Size for All IAPs.....	369
Figure 173. Setting the Cell Size for a Specific IAP .....	370
Figure 174. Configuring VLANs on an Open SSID.....	371
Figure 175. Configuring Radio Assurance Mode (Loopback Testing).....	373
Figure 176. Disconnecting Power from the Array.....	377
Figure 177. Removing the Access Panel Screws.....	379
Figure 178. Removing the Access Panel .....	380
Figure 179. Disconnecting the Power Supply and Fan.....	380
Figure 180. Reconnecting the Fan and Power Supply .....	382
Figure 181. Reinstalling the Access Panel.....	382
Figure 182. Removing the FLASH Memory Module.....	384

Figure 183. Removing the DIMM Memory Module .....	386
Figure 184. Removing the Chassis Cover Screws.....	388
Figure 185. Removing the Chassis Cover .....	388
Figure 186. Lifting the Integrated Access Point Module .....	389
Figure 187. Disconnect the Integrated Access Point Module .....	389
Figure 188. Installing a New Access Panel (with Power Supply) .....	391
Figure 189. Sample output of pci-audit command.....	429
Figure 190. Tamper-evident seal appearance .....	432
Figure 191. Tamper-evident seal locations for XN4 indicated by arrows.....	432
Figure 192. Two tamper-evident seals on seam of XN8/12/16 .....	433
Figure 193. Six tamper-evident seals on mounting plate - XN8/12/16 .....	433
Figure 194. Apply the security strap through locking tab as shown.....	434
Figure 195. Security - Management Control Window .....	435

# Introduction

These topics introduce the Xirrus Wi-Fi Array, including an overview of its key features and benefits, and a detailed listing of the product's physical, environmental, technology and regulatory specifications.

- **"The Xirrus Family of Products" on page 1.**
- **"About this User's Guide" on page 4.**
- **"Why Choose the Xirrus Wi-Fi Array?" on page 6.**
- **"Wi-Fi Array Product Overview" on page 7.**
- **"Key Features and Benefits" on page 12.**
- **"Advanced Feature Sets" on page 14.**

## The Xirrus Family of Products



Figure 1. Xirrus Arrays: XR Series (on left) and XN Series

The Xirrus family of products includes the following:

- **The XR Series of Xirrus Wi-Fi Arrays**  
The newest Xirrus Wi-Fi Arrays have been completely redesigned with state of the art components to provide increased bandwidth per radio, additional radios, and integrated switching capacity of up to 10 Gbps. The radios support IEEE802.11 a, b, g, and n clients, and feature the capacity and performance needed to replace switched Ethernet to the desktop.

- **The XN Series of Xirrus Wi-Fi Arrays (XN16 / XN12 / XN8 / XN4)**  
The Xirrus Wi-Fi Arrays have the speed and reach of IEEE 802.11n technology. The XN Series of Arrays feature the capacity and performance needed to replace switched Ethernet to the desktop. The XN16 has 16 IAPs, the XN12 has 12 IAPs, the XN8 has 8 IAPs, and the XN4 has 4 IAPs. For detailed information on the features and usage of the XN Series, please see the *Xirrus Wi-Fi Array User's Guide*, Part Number: 800-0006-001.
- **Xirrus Management System (XMS)**  
XMS is used for managing large Array deployments from a centralized Web-based interface. The XMS server is available pre-installed on the Xirrus XM-33xx-CC Management Appliance series, or as a software package (XA-3300-CC) to be installed on your own server hardware.

Figure 2 illustrates the elements of the Xirrus Management System. Users start the XMS client simply by entering the URL of the XMS server on a web browser. The XMS server manages a number of Wi-Fi Arrays via SNMP.

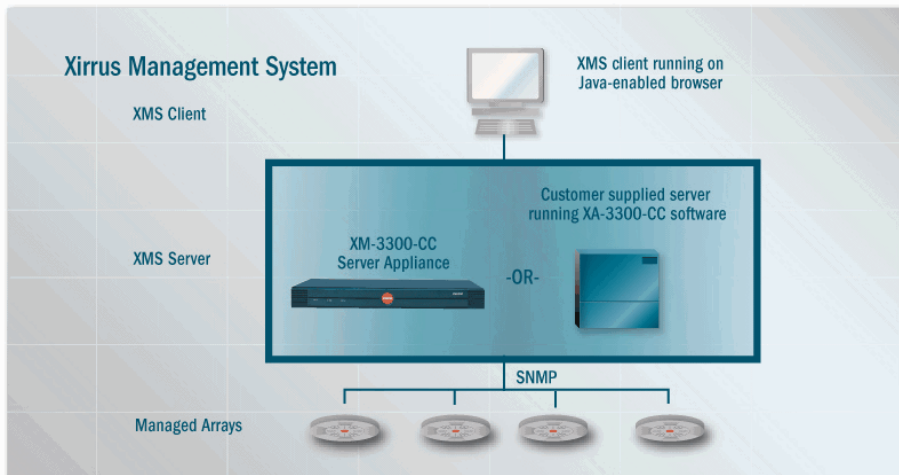


Figure 2. The Xirrus Management System

If you need detailed information about this product, refer to the XMS User's Guide, part number 800-0007-001.

- **Xirrus Power over Gigabit Ethernet (PoGE)**

The PoGE modules eliminate the need for running separate power cabling. Additionally, an available eight port module provides distributed power to multiple Arrays, facilitating backup power when connected via a UPS.

### **Nomenclature**

Throughout this User's Guide, the Xirrus Wi-Fi Array is also referred to as simply the **Array**. In some instances, the terms **product** and **unit** are also used. When discussing specific products from the Xirrus family, the product name is used (for example, XR4830). The Wi-Fi Array's operating system is referred to as the **ArrayOS**. The Web Management Interface for browser-based management of the Array is referred to as **WMI**.

The XR Series Arrays have very flexible radio capabilities—each of the radios may be independently configured to support IEEE802.11a, 11b, 11g, or 11n clients or a combination of client types. One radio is typically assigned as the RF **monitor** radio, supporting intrusion detection and prevention, self-monitoring, and other services. Radios support both 2.4GHz and 5 GHz, and are named **iap1**, **iap2**, ... **iapn**.

The Xirrus Management System is referred to as **XMS**. The Power over Gigabit Ethernet system may be referred to as **PoGE**.

## About this User's Guide

This User's Guide provides detailed information and procedures that will enable wireless network administrators to install, configure and manage the Wi-Fi Array so that end users can take full advantage of the product's features and functionality without technical assistance.

## Organization

Topics and procedures are organized by function under the following chapter headings:

- **Introduction**  
Provides a brief introduction to wireless technology, an overview of the product, including its key features and benefits, and presents the product specifications.
- **Installing the Wi-Fi Array**  
Defines prerequisites for deploying and installing the Array and provides instructions to help you plan and complete a successful installation.
- **The Web Management Interface**  
Offers an overview of the product's embedded Web Management Interface, including its content and structure. It emphasizes what you need to do to ensure that any configuration changes you make are applied, and provides a list of restricted characters. It also includes instructions for logging in to the Array with your Web browser.
- **Viewing Status on the Wi-Fi Array**  
Describes the status and statistics displays available on the Array using its embedded Web Management Interface.
- **Configuring the Wi-Fi Array**  
Contains procedures for configuring the Array using its embedded Web Management Interface.
- **Using Tools on the Wi-Fi Array**  
Contains procedures for using utility tools provided in the Web Management Interface. It includes procedures for upgrading the system



firmware, uploading and downloading configurations and other files, using diagnostic tools, and resetting the Array to its factory defaults.

- **The Command Line Interface**  
Includes 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. This chapter also includes some sample key configuration tasks using the CLI.
- **Appendix A: Servicing the Wi-Fi Array**  
Contains procedures for servicing the Array, including the removal and reinstallation of major hardware components.
- **Appendix B: Quick Reference Guide**  
Contains the product's factory default settings.
- **Appendix C: Technical Support**  
Offers guidance to resolve technical issues, including general hints and tips to enhance your product experience, and a procedure for isolating problems within an Array-enabled wireless network. Also includes Frequently Asked Questions (FAQs) and Xirrus contact information.
- **Appendix D: Implementing PCI DSS**  
Discusses meeting PCI DSS security standards with the Array.
- **Appendix E: Implementing FIPS Security**  
Discusses meeting FIPS security standards with the Array.
- **Appendix F: Notices**  
Contains the legal notices, licensing, and compliance statements for the Array. Please read this section carefully.
- **Glossary of Terms**  
Provides an explanation of terms directly related to Xirrus product technology, organized alphabetically.
- **Index**  
The index is a valuable information search tool. Use the index to locate specific topics discussed in this User's Guide. Simply click on any page number in the index to jump to the referenced topic.

## Notes and Cautions

The following symbols are used throughout this User's Guide:



*This symbol is used for general notes that provide useful supplemental information.*



*This symbol is used for cautions. Cautions provide critical information that may adversely affect the performance of the product.*

## Screen Images

Some screen images of the Web Management Interface have been modified for clarity. For example, an image may have been cropped to highlight a specific area of the screen, and/or sample data may be included in some fields.

## Your User's Guide as a PDF Document

This User's Guide is also made available as a secure PDF (Portable Document Format) file and can be viewed using the Adobe® Acrobat Reader® product. It cannot be edited or modified. If you don't have Acrobat Reader, you can download it free-of-charge from: <http://www.adobe.com>.

## Hyperlinks

If you click on body text that appears in the color **TEAL** (with the exception of headings or notes) the embedded hyperlink within the text will immediately take you to the referenced destination. All internal and external cross-references, including page numbers within the **List of Figures** and the **Index**, have associated hyperlinks. After "jumping" to a referenced topic, if you want to return to the previous page (reference source), simply click on Acrobat's **previous page** button.

## Why Choose the Xirrus Wi-Fi Array?

The deployment of Wi-Fi is becoming increasingly common as businesses strive for greater flexibility in the workplace and the need for employee mobility rises. The only requirements for an effective wireless deployment are a power source, a couple of screws, and a little imagination.

Wi-Fi is also fully compatible with standard Ethernet protocols, so connectivity with existing wired infrastructure is transparent to users—they can still access and use the same applications and network services that they use when plugged into the company’s wired LAN (it’s only the plug that no longer exists).

Wi-Fi has come a long way in the past few years and now offers the performance, reliability and security that Enterprise customers have come to expect from their networks. The technology is being driven by four major IEEE standards:

- **802.11a**  
Operates in the 5 GHz range with a maximum speed of 54 Mbps.
- **802.11b**  
Operates in the 2.4 GHz range with a maximum speed of 11 Mbps.
- **802.11g**  
Supports a higher transmission speed of 54 Mbps in the 2.4 GHz range and is backwards compatible with 802.11b.
- **802.11n**  
Uses multiple antennas per radio to boost transmission speed as high as 450Mbps, increasing throughput, range, and maximum number of users. 802.11n is backwards compatible with 802.11a/b/g.

Whether you have just a handful of users or thousands of users, wireless has the scalability and flexibility to serve your needs.

### Wi-Fi Array Product Overview

Part of the family of Xirrus products, the Wi-Fi Array is a high capacity, multi-mode device designed for the Enterprise market, with twice the range and much higher capacity than competitive wireless products.



Figure 3. Wi-Fi Array (XR Series)

The Wi-Fi Array (regardless of the product model) is Wi-Fi® compliant and simultaneously supports 802.11a, 802.11b, 802.11g, and 802.11n clients. Integrated switching and active enterprise class features such as [VLAN](#) support and multiple [SSID](#) capability enable robust network compatibility and a high level of scalability and system control. The optional Xirrus Management System (XMS) allows global management of hundreds of Arrays from a central location.

Multiple versions of the Array with different numbers of Integrated Access Points (IAPs) support a variety of deployment applications.

### **Enterprise Class Security**

The latest and most effective wireless encryption security standards, including WPA (Wi-Fi Protected Access) and WPA2 with 802.11i AES (Advanced Encryption Standard) are available on the Wi-Fi Array. In addition, the use of an embedded RADIUS server (or 802.1x with an external RADIUS server) ensures user authentication—multiple Arrays can authenticate to the optional XMS, ensuring only authorized Arrays become part of the wireless network. With the Xirrus [Advanced Feature Sets](#), intrusion detection and prevention, site monitoring, and RF spectrum analysis are performed in the background by the Array automatically.

## Deployment Flexibility

Xirrus' unique multi-radio architecture generates 360 degrees of sectored high-gain 802.11a/b/g/n coverage that provides extended range and the highest possible data rates for a large volume of clients. Each sector can be adjusted automatically or manually, creating a pattern of wireless coverage perfectly tailored to individual customer needs. For example:

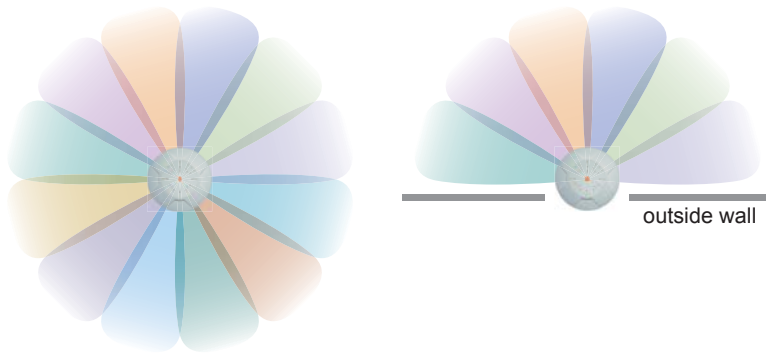


Figure 4. Wireless Coverage Patterns

Figure 4 depicts the following two scenarios:

- **Full pattern coverage**  
All radios are activated with coverage spanning 360 degrees. If within range, clients will always receive coverage regardless of their geographic position relative to the Array.
- **Partial pattern coverage**  
If desired, the Wi-Fi Array can be deployed close to an exterior wall. In this case, half of all available radios have been deactivated to prevent redundant signals from “bleeding” beyond the site’s perimeter wall. This configuration may also be used in those cases where you want to restrict wireless coverage to selected areas of the building’s interior.

### **Power over Gigabit Ethernet (PoGE)**

The Xirrus Power over Gigabit Ethernet modules provide power to your Arrays over the same Cat 5e or Cat 6 cable used for data, eliminating the need to run power cables and provide an AC power outlet in proximity to each unit. Managed modules provide the ability to control power using XMS.

### **Enterprise Class Management**

The Wi-Fi Array can be configured with its default RF settings, or the RF settings can be customized using the Array's embedded Web Management Interface (WMI). The WMI enables easy configuration and control from a graphical console, along with a full compliment of troubleshooting tools and statistics.

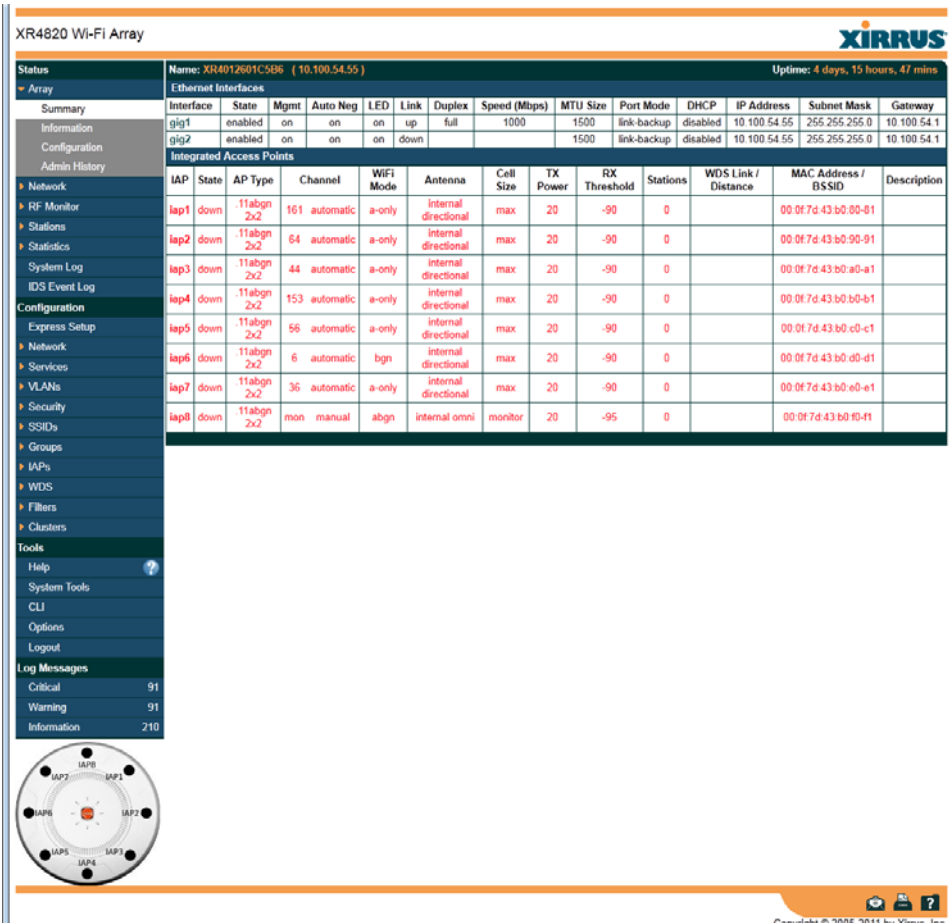


Figure 5. WMI: Array Status

In addition, a fully featured Command Line Interface (CLI) offers IT professionals a familiar management and control environment. SNMP (Simple Network Management Protocol) is also supported to allow management from an SNMP compliant management tool, such as the optional Xirrus Management System.



*For deployments of more than five Arrays, we recommend that you use the Xirrus Management System (XMS). The XMS offers a rich set of features for fine control over large deployments.*

## Key Features and Benefits

This section describes some of the key product features and the benefits you can expect when deploying the Wi-Fi Array (the XR4830 product is highlighted in this section).

### High Capacity and High Performance



Figure 6. Layout of IAPs (XR4830)

The XR4830 version of the Wi-Fi Array (Figure 6) easily handles time-sensitive traffic such as voice, and can enable wireless connectivity. This model includes two Gigabit uplink ports for connection to the wired network. Its eight IAPs (radios) provide a maximum wireless capacity of 3.6 Gbps, which offers ample reserves for the high demands of current and future applications. Of the eight IAPs, seven operate as radios which may be set up to serve your choice of client types—any or all of 802.11a/b/g/n (5 GHz or 2.4 GHz bands), providing backwards compatibility with 802.11b and 802.11g.

In the recommended configuration, one IAP is configured in RF monitoring and intrusion detection/prevention mode.

### Extended Coverage

One XR4830 solution enables you to replace eight access points (including one omnidirectional IAP for monitoring the network). Seven IAP radios with integrated directional antennas provide increased wireless range and enhanced



data rates in all directions. With a Wi-Fi Array deployed, far fewer access points are needed and wired-like resiliency is delivered throughout your wireless network. Your Wi-Fi Array deployment ensures:

- Continuous connectivity if an IAP (radio) fails.
- Continuous connectivity if an Array fails.
- Continuous connectivity if a WDS link or switch fails.
- Continuous connectivity if a Gigabit uplink or switch fails.

### **Non-Overlapping Channels**

Complete use of non-overlapping channels limits interference and delivers maximum capacity. On the XR4830, up to 8 non-overlapping channels are fully utilized across the 5GHz and 2.4GHz spectrums.

### **SDMA Optimization**

SDMA (Spatial Division Multiple Access) technology provides full 360° coverage while allowing independent channel and power output customization. Also supports fast inter-zone handoffs for time-sensitive applications and roaming.

### **Fast Roaming**

Utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at both Layer 2 and Layer 3.

### **Easy Deployment**

The Xirrus Management System (XMS) offers real time monitoring and management capabilities for the wireless network—ideal for the Enterprise market. It also allows you to import floor plans to help you plan your deployment. The Xirrus Wi-Fi Array chassis has a plenum rated, lockable and tamper resistant case.

### **Secure Wireless Access**

Multiple layers of authentication and encryption ensure secure data transmissions. The Wi-Fi Array is 802.11i compliant with line-rate encryption support for 40 and 128 bit WEP, WPA and WPA2 with TKIP and AES encryption.

Authentication is provided via 802.1x, including PEAP, EAP-TLS, EAP-TTLS, and LEAP (Lightweight Extensible Authentication Protocol) passthrough.

### **Applications Enablement**

The Wi-Fi Array's QoS (Quality of Service) functionality combined with true switch capabilities enable high density video and Voice over Wireless LAN deployments. Compliant with 802.1p and 802.1Q standards.

### **Advanced Feature Sets**

The Wi-Fi Array offers a family of powerful functionality packages, including the RF Performance Manager (RPM), RF Security Manager (RSM), and RF Analysis Manager (RAM). These packages are separately licensed for operation on your Array.

#### **Xirrus Advanced RF Performance Manager (RPM)**

The Xirrus RPM optimizes the bandwidth usage and station performance of 802.11n Wi-Fi networks. Leveraging the multiple integrated access point (multi-radio) design of the Xirrus Wi-Fi Array, RPM manages the allocation of wireless bandwidth to wireless stations across multiple RF channels. The result maximizes overall network performance with superior flexibility and capacity.

Today's wireless infrastructure is faced with ever increasing numbers and variations of Wi-Fi enabled clients, whether in the form of notebooks, netbooks, smart phones, IP phones, printers, projectors, cameras, RFID tags, etc. The advent of higher speed 802.11n Wi-Fi and its increased use of the 5GHz spectrum adds to the number of variables today's wireless networks must accommodate. Backwards compatibility with older clients is crucial, however their operation in a Wi-Fi network can significantly hinder the performance of faster clients. As an example, 802.11b Wi-Fi stations communicate more than 10 times slower than 802.11n stations.

With each of the Array's multiple radios operating on a different channel, RPM selects the ideal radio for each station. High-speed stations are grouped together on radios with other high speed stations, while lower speed stations are combined

with other lower speed stations. This ensures optimal performance for high-speed 802.11n stations without compromise.

The complete feature set of the RPM package includes:

- WDS (Wireless Distribution System) for point-to-point communication
- Wi-Fi Mode per IAP
- Sharp Cell technology
- Wireless Data Rate Optimization
- Wireless Traffic Shaping
- Wireless Voice Call Admission Control
- Fast Layer 2 and 3 Roaming
- Standby Mode

### **Xirrus Advanced RF Security Manager (RSM)**

The Xirrus RSM improves security and minimizes the risk in deploying 802.11n wireless networks. Leveraging an integrated 24/7 threat sensor and hardware-based encryption/decryption in each Array, RSM secures the Wi-Fi network from multiple types of threats. The result delivers uncompromised overall network security with superior flexibility and performance.

Today's Wi-Fi networks face a number of potential security threats in the form of rogue access points, ad-hoc clients, unauthorized clients, wireless-based attacks, eavesdropping, etc. As 802.11n is increasingly adopted in enterprise networks, defending against these threats becomes more critical. With the Array's dedicated threat sensor radio scanning all channels in the 2.4GHz and 5GHz spectrums, RSM searches for security threats and automatically mitigates them.

High performance encryption/decryption in the enterprise Wi-Fi network is a must. The Wi-Fi network needs to support each client using the highest level of encryption (WPA2 Enterprise/128 bit AES) and without degrading the overall performance of the network. Xirrus incorporates hardware-based encryption/decryption into each Array, delivering line-rate encryption at the edge of the network instead of at a choke point within a centralized controller.

The complete feature set of the RSM package includes:

- Wireless IDS/IPS (Intrusion Detection/Prevention System)
- Wireless stateful firewall
- User group policies
- Authenticated guest access gateway
- NAC integration
- PCI audit compliance enforcement

### **Xirrus Advanced RF Analysis Manager (RAM)**

The RF Advanced Analysis Manager (RAM) tests and troubleshoots 802.11n wireless networks. The deployment of 802.11n presents a set of unique challenges based on technology differences with legacy 802.11a/b/g networks, both on the wireless infrastructure and client side. Xirrus' RAM equips each Wi-Fi Array with a powerful set of tools and features to optimally tune and verify an 802.11n installation, as well as give IT administrators the ability to troubleshoot issues that may occur within the wireless environment.

The 802.11n standard will continue to evolve over the next several years with additional performance and optional functions, along with ongoing stream of IEEE 802.11 amendments. This changing wireless landscape mandates that appropriate tools are available to the user to analyze, optimize, and troubleshoot their changing environments.

The distributed architecture of the Array enables the execution of powerful wireless and networking analysis at the edge of the network where packets traverse the wireless-to-wired boundary. The Array includes an embedded Wi-Fi Controller with the necessary computing and memory resources to provide these functions securely at the network's edge.

The key elements of the RAM package include:

- RF Analysis – An embedded Spectrum Analyzer leverages the dedicated threat sensor radio in each Wi-Fi Array to provide a continual view of utilization, interference, and errors across all available Wi-Fi channels.

- Packet Analysis – Integrated packet capture provides filterable views of all traffic traversing on the wired and wireless interfaces of the Array.
- Performance Analysis – Embedded traffic generation enables the throughput of the Array’s wireless or wired interfaces to be analyzed.
- Failure Recovery – Radio Assurance provides an automatic self-test and self healing mechanism that ensures continuous system operation.
- Netflow Support
- Network Tools: ping, RADIUS ping, traceroute



# Installing the Wi-Fi Array

The instructions for completing a successful installation include the following topics:

- “Installation Prerequisites” on page 19.
- “Planning Your Installation” on page 22.
- “Installation Workflow” on page 56.
- “Installing Your Wi-Fi Array” on page 58.
- “Powering Up the Wi-Fi Array” on page 62.
- “Establishing Communication with the Array” on page 65.
- “Performing the Express Setup Procedure” on page 68.

## Installation Prerequisites

Your Wi-Fi Array deployment requires the presence of hardware and services in the host wired/wireless network, including:

- **Power Source**  
Most Arrays are powered via Xirrus Power over Gigabit Ethernet. PoGE supplies power over the same Cat 5e or Cat 6 cable used for data, thus reducing cabling and installation effort. PoGE power injector modules are available in 1-, 2-, and 8-port configurations and are typically placed near your Gigabit Ethernet switch. An AC outlet is required for each injector module. Current Array models have integrated splitters, so no separate splitter is required.
- **Ethernet port**  
You need at least one 100/1000 BaseT port to establish wired Gigabit Ethernet connectivity (via the product’s Gigabit 1 or Gigabit 2 port) and one 10/100 BaseT port (if desired) for product management.

! *The Array’s Ethernet ports should be connected to an Ethernet switch, not an Ethernet hub—if a hub is used, we recommend that you connect only one Ethernet port.*

! The Gigabit1 Ethernet interface is the primary port for both data and management traffic. If a single Ethernet connection is used, it must be connected to the Gigabit1 Ethernet interface. See also, “Port Failover Protection” on page 42.

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 for this interface. See “interface” on page 341.

- **Secure Shell (SSH) utility**

To establish secure remote command line access to the Array, you need a Secure Shell (SSH) utility, such as PuTTY. The utility **must** be configured to use SSH-2, since the Array will only allow SSH-2 connections.

- **Secure Web browser**

Either Internet Explorer (version 7.0 or higher), Mozilla Firefox (version 3.0 or higher), Chrome (version 3.0 or higher), or Safari (version 5.0 or higher). A secure Web browser is required for Web-based management of the Array. The browser must be on the same subnet as the Array, or you must set a static route for management as described in the warning above.

- **Serial connection capability**

To connect directly to the console port on the Array, your computer must be equipped with a male 9-pin serial port and terminal emulation software (for example, HyperTerminal). The Xirrus Array only supports serial cable lengths up to 25’ per the RS-232 specification.

Use the following settings when establishing a serial connection:

Bits per second	115,200
Data bits	8
Parity	None



Stop bits	1
Flow control	None

### Optional Network Components

The following network components are optional.

- **Xirrus Management System (XMS)**  
The optional XMS offers powerful management features for small or large Wi-Fi Array deployments.
- **External RADIUS server**  
Although your Array comes with an embedded [RADIUS](#) server, for 802.1x authentication in large deployments you may want to add an external RADIUS server.

### Client Requirements

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

#### *See Also*

[Coverage and Capacity Planning](#)  
[Deployment Examples](#)  
[Failover Planning](#)  
[Planning Your Installation](#)

## Planning Your Installation

This section provides guidelines and examples to help you plan your Xirrus Wi-Fi Array deployment to achieve the best overall coverage and performance. We recommend you conduct a site survey to determine the best location and settings for each Array you install.

The following topics are discussed:

- “General Deployment Considerations” on page 22
- “Coverage and Capacity Planning” on page 24
- “IEEE 802.11n Deployment Considerations” on page 34
- “Failover Planning” on page 42
- “Power Planning” on page 44
- “Security Planning” on page 45
- “Port Requirements” on page 48
- “Network Management Planning” on page 51
- “WDS Planning” on page 52
- “Common Deployment Options” on page 55



*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](#).*

## General Deployment Considerations

The Wi-Fi Array’s unique multi-radio architecture generates 360 degrees of sectorized high-gain 802.11a/b/g/n coverage that provides extended range. However, the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through may affect the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise at your location. To maximize wireless range, follow these basic guidelines:

1. Keep the number of walls and ceilings between the Array and your receiving devices to a minimum—each wall or ceiling can reduce the wireless range from between 3 and 90 feet (1 to 30 meters). Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between each device. For example, a wall that is 1.5 feet thick (half a meter) at  $90^\circ$  is actually almost 3 feet thick (or 1 meter) when viewed at a  $45^\circ$  angle. At an acute  $2^\circ$  degree angle the same wall is over 42 feet (or 14 meters) thick! For best reception, try to ensure that your wireless devices are positioned so that signals will travel straight through a wall or ceiling.

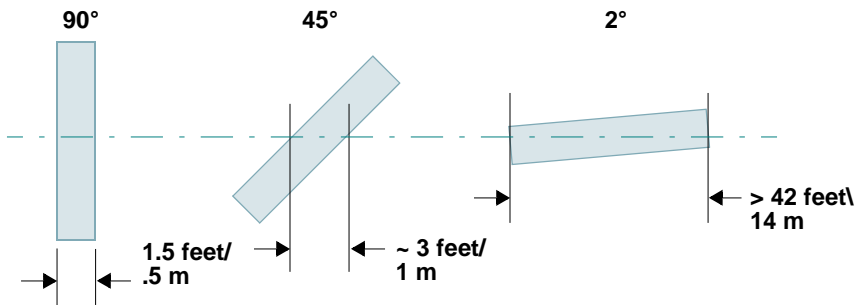


Figure 7. Wall Thickness Considerations

3. Try to position wireless client devices so that the signal passes through drywall (between studs) or open doorways and not other materials that can adversely affect the wireless signal.

### See Also

[Coverage and Capacity Planning](#)

[Deployment Examples](#)

[Common Deployment Options](#)

[Installation Prerequisites](#)

## Coverage and Capacity Planning

This section considers coverage and capacity for your deployment(s), including placement options, RF patterns and cell sizes, area calculations, roaming considerations, and channel allocations.



*Note that several advanced features in this section are part of the Xirrus Advanced RF Performance Manager (RPM). They require the license installed on the Array to include support for RPM. Please see “About Licensing and Upgrades” on page 297.*

## Placement

Use the following guidelines when considering placement options:

1. The best placement option for the Array is ceiling-mounted within an open plan environment (cubicles rather than fixed walls).
2. Keep the Array away from electrical devices or appliances that generate RF noise. Because the Array is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting)—we recommend maintaining a distance of at least 3 to 6 feet (1 to 2 meters).

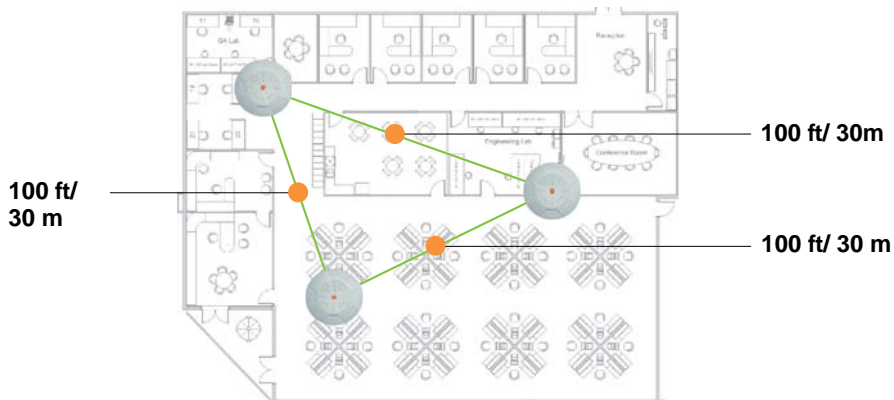


Figure 8. Unit Placement

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

### **RF Patterns**

The Wi-Fi Array allows you to control—automatically or manually—the pattern of wireless coverage that best suits your deployment needs. You can choose to operate with full coverage, half coverage, or custom coverage (by enabling or disabling individual sectors).

#### ***Full (Normal) Coverage***

In normal operation, the Array provides a full 360 degrees of coverage.

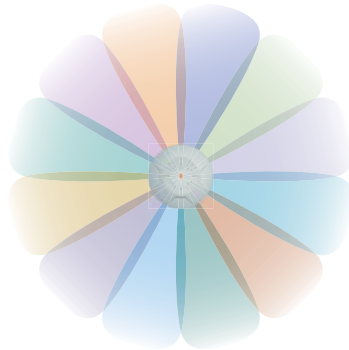


Figure 9. Full (Normal) Coverage

#### ***Half Coverage***

If installing a unit close to an exterior wall, you can deactivate half of the radios to prevent redundant signals from “bleeding” beyond the wall and extending

service into public areas. The same principle applies if you want to restrict service to an adjacent room within the site.

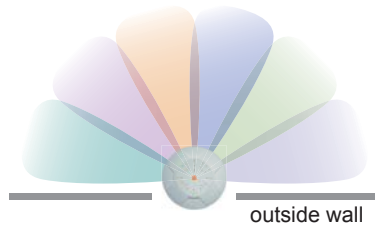


Figure 10. Adjusting RF Patterns

### *Custom Coverage*

Where there are highly reflective objects in proximity to the Array, you can turn off specific radios to avoid interference and feedback.

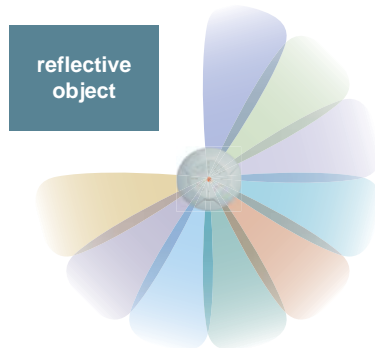


Figure 11. Custom Coverage

### Capacity and Cell Sizes

Cell sizes should be estimated based on the number of users, the applications being used (for example, data/video/voice), and the number of Arrays available at the location. The capacity of a cell is defined as the minimum data rate desired for each sector multiplied by the total number of sectors being used.

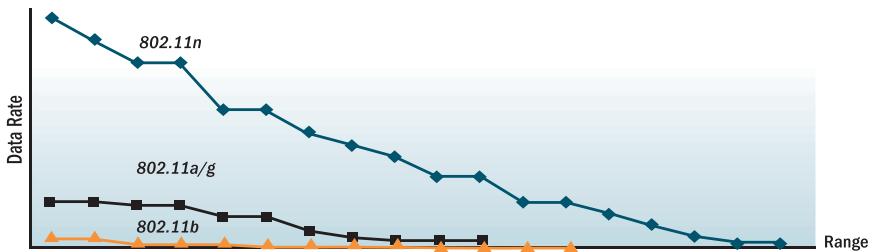


Figure 12. Connection Rate vs. Distance

Figure 12 shows relative connection rates for 802.11n vs. 802.11a/g and 802.11b, and the effect of distance on the connection rates. Wireless environments can vary greatly so the actual rates may be different depending on the specific network deployment.

### Fine Tuning Cell Sizes

Adjusting the [transmit power](#) allows you to fine tune cell sizes. There are four standard sizes—Small, Medium, Large, or Max (the default is **Max**). There is also an Auto setting that automatically determines the best cell size, and a Manual setting that allows you to choose your power settings directly.

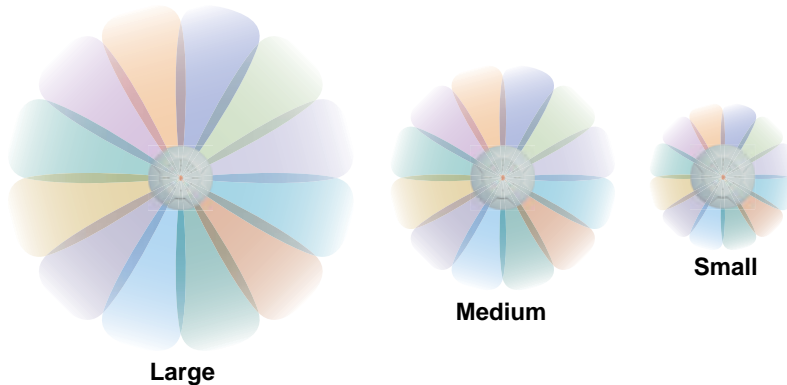


Figure 13. Transmit Power

Auto Cell Size is an automatic, self-tuning mechanism that balances cell size between Arrays to guarantee coverage while limiting the RF energy that could extend beyond the organizational boundary. Auto Cell uses communication between Arrays to dynamically set radio power so that complete coverage is provided to all areas, yet at the minimum power level required. This helps to minimize potential interference with neighboring networks. Additionally, Arrays running Auto Cell automatically detect and compensate for coverage gaps caused by system interruptions. To enable the Auto Cell Size feature, go to “[RF Power & Sensitivity](#)” on page 264. For a complete discussion of the Auto Cell size feature, see the *Xirrus Auto Cell Application Note* in the [Xirrus Library](#).

If you are installing many units in proximity to each other, we recommend that you use Auto Cell Size; otherwise, reduce the transmit power using manual settings to avoid excessive interference with other Arrays or installed APs. See also, “[Coverage and Capacity Planning](#)” on page 24.



### *Sharp Cell*

This patented Xirrus RF management option automatically creates more intelligently defined cells and improves performance by creating smaller, high-throughput cells. By dynamically limiting each cell to a defined boundary (cell size), the trailing edge bleed of RF energy is reduced, thus minimizing interference between neighboring Wi-Fi Arrays or other Access Points. To enable the Sharp Cell feature, go to “[RF Power & Sensitivity](#)” on page 264. For more information about this feature, see the *Xirrus Sharp Cell Application Note* in the [Xirrus Library](#).

### **Roaming Considerations**

Cells should overlap approximately 10 - 15% to accommodate client roaming.

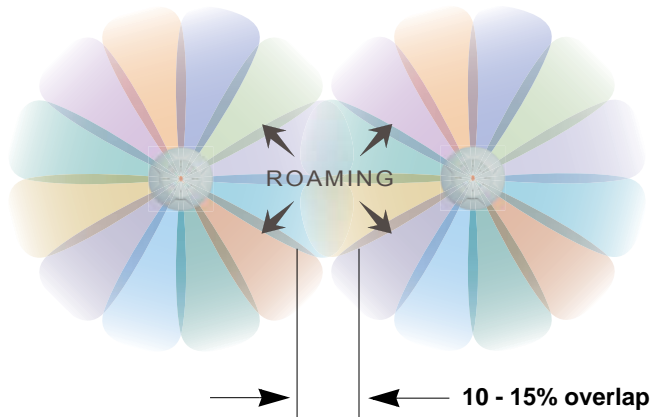


Figure 14. Overlapping Cells

### **Allocating Channels**

Because the Wi-Fi Array is a multi-channel device, allocating the best channels to radios is important if peak performance is to be maintained.

### *Automatic Channel Selection*

We recommend that you allow the Array to make intelligent channel allocation decisions automatically. In the automatic mode, channels are allocated dynamically, driven by changes in the environment. Auto Channel assignment is

performed by scanning the surrounding area for RF activity on all channels, then automatically selecting and setting channels on the Array to the best channels available. This function is typically executed when initially installing Arrays in a new location and may optionally be configured to execute periodically to account for changes in the RF environment over time. Auto Channel selection has significant advantages, including:

- Allows the Array to come up for the first time and not interfere with existing equipment that may be already running, thereby limiting co-channel interference.
- More accurately tunes the RF characteristics of a Wi-Fi installation than manual configuration since the radios themselves are scanning the environment from their physical location.
- May be configured to run periodically.

To set up the automatic channel selection feature, go to “[Advanced RF Settings](#)” on [page 262](#). For more information about this feature, see the *Xirrus Auto Channel Application Note* in the [Xirrus Library](#).

**Manual Channel Selection**

You can manually assign channels on a per radio basis, though manual selection is not recommended (and not necessary).



*To avoid co-channel interference, do not select adjacent channels for radios that are physically next to each other.*

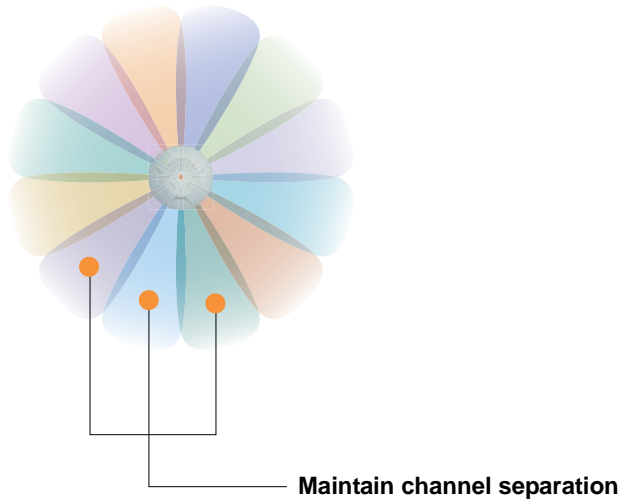


Figure 15. Allocating Channels Manually

**See Also**

- Deployment Examples
- Failover Planning
- Installation Prerequisites

### Deployment Examples

The following examples employ 802.11a cells, each offering minimum throughputs of 54 Mbps, 36 Mbps, and 18 Mbps per sector respectively, and assume a floor plan covering a total area of about 60,000 square feet (5574 sq m).

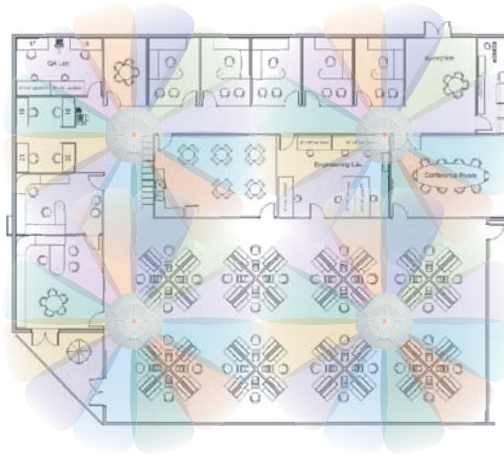


Figure 16. Deployment Scenario (54 Mbps)—Per Sector



Figure 17. Deployment Scenario (36 Mbps)—Per Sector



Figure 18. Deployment Scenario (18 Mbps)—Per Sector

*See Also*

Coverage and Capacity Planning

Failover Planning

Planning Your Installation

## IEEE 802.11n Deployment Considerations



*IEEE 802.11n features are supported only on XN Array models, and this section applies only to those Arrays. Note that the license installed on the Array must include support for 802.11n. Please see “About Licensing and Upgrades” on page 297.*

The Xirrus XN Arrays support IEEE 802.11n on all IAPs, in both 2.4 GHz and 5 GHz bands. Use of 802.11n offers significant benefits:

- Higher data rates
- Higher throughput
- Supports more users
- More robust connections
- Increased coverage area
- More secure connections—supports WPA2 (Wi-Fi Protected Access 2)

These benefits result in better support for a wide range of applications such as voice and video, intensive usage such as CAD/CAM and backups, dense user environments, and for manufacturing and warehousing environments.



*While 802.11n increases coverage area by almost doubling the reach, you must consider the legacy wireless devices in your network. Wireless stations connecting using 802.11a/b/g will still be subject to a reach of up to 100 feet, depending on the environment.*

The techniques that 802.11n uses to realize these performance improvements, and the results that can be expected are discussed in:

- “MIMO (Multiple-In Multiple-Out)” on page 35
- “Multiple Data Streams—Spatial Multiplexing” on page 37
- “Channel Bonding” on page 38
- “Improved MAC Throughput” on page 39
- “Short Guard Interval” on page 39
- “Obtaining Higher Data Rates” on page 40
- “802.11n Capacity” on page 41

Two very important techniques to consider are [Channel Bonding](#) and [Multiple Data Streams—Spatial Multiplexing](#) because they contribute a large portion of 802.11n’s speed improvements and because they are optional and configurable, as opposed to the parts of 802.11n that are fixed. While the settings for 802.11n IAPs come pre-configured on the Array for robust performance in typical usage, you should review the settings for your deployment, especially channel bonding. A global setting is provided to enable or disable 802.11n mode. See “[Global Settings .11n](#)” on page 259 to configure 802.11n operation.

### MIMO (Multiple-In Multiple-Out)

MIMO (Multiple-In Multiple-Out) signal processing is one of the core technologies of 802.11n. It mitigates interference and maintains broadband performance even with weak signals.

Prior to 802.11n, a data stream was transmitted via one antenna. At the receiving end, the antenna with the best signal was selected to receive data. ([Figure 19](#))

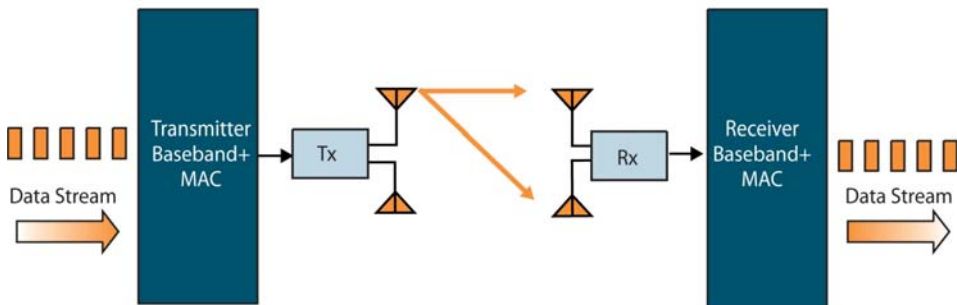


Figure 19. Classic 802.11 Signal Transmission

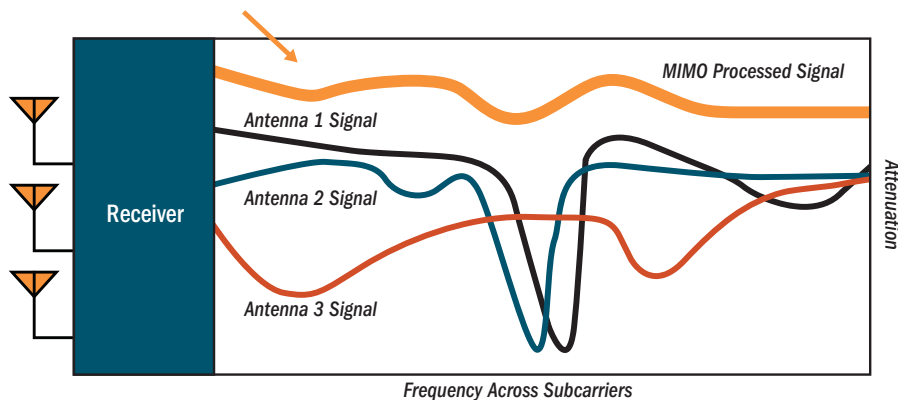


Figure 20. MIMO Signal Processing

MIMO signal processing uses multiple antennas to send and receive data. It takes advantage of multipath reflections to improve signal coherence and greatly increase receiver sensitivity (Figure 20). Multipath signals were considered to be interference by 802.11a/b/g radios, and degraded performance. In 802.11n, these signals are used to enhance performance. This extra sensitivity can be used for greater range or higher data rates. The enhanced signal is the processed sum of individual antennas. Signal processing eliminates nulls and fading that any one antenna would see. MIMO signal processing is sophisticated enough to discern multiple spatial streams (see [Multiple Data Streams—Spatial Multiplexing](#)). There are no settings to configure for MIMO.



### Multiple Data Streams—Spatial Multiplexing

Spatial Multiplexing transmits completely separate data streams on different antennas (in the same channel) that are recombined to produce new 802.11n data rates. Higher data rates are achieved by splitting the original data stream into separate data streams. Each separate stream is transmitted on a different antenna (using its own RF chain). MIMO signal processing at the receiver can detect and recover each stream. Streams are then recombined, yielding higher data rates.

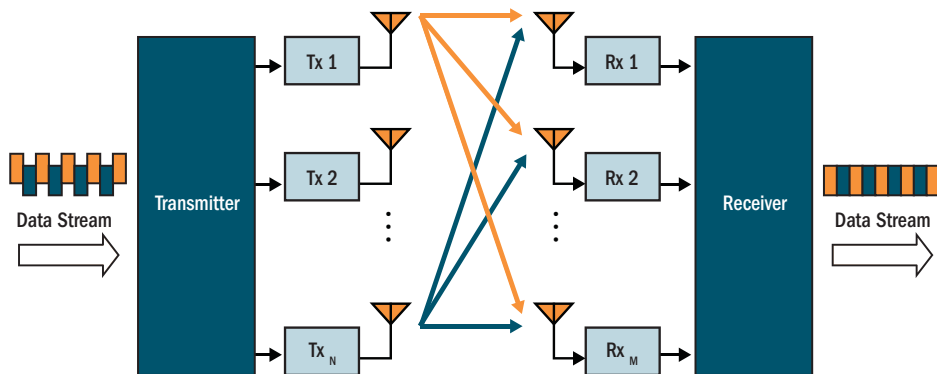


Figure 21. Spatial Multiplexing

Spatial multiplexing can double, triple, or quadruple the data rate, depending on the number of transmit antennas used. You can configure the number of chains (i.e., streams) separately for transmitting and receiving. By default, the Array uses three chains for transmitting and receiving (see “Global Settings .11n” on page 259).

## Channel Bonding

Channel bonding increases data rates by combining two adjacent 20 MHz channels into one 40 MHz channel. This increases the data rate to slightly more than double.

A bonded 40 MHz channel is specified in terms of the Primary channel and the adjacent channel to Bond. The Bond channel is represented by **+1** to use the channel above the Primary channel, or **-1** to use the channel below. In the example shown, Channel 40 is the Primary channel and it is bonded to Channel 36, the channel below it, by specifying **-1**. Be aware that Channel Bonding can make channel planning more difficult, since you are using two channels for an IAP. We recommend the use of the 5 GHz band, since it has many more channels than the 2.4 GHz band, and thus more channels are available for bonding.

The Array provides an Automatic Channel Bonding setting that will automatically select the best channel for bonding on each IAP. If you enable this option, you may select whether bonding will be dynamic (the bonded channel changes in response to environmental conditions) or static (the bonded channel will not be changed). See “Global Settings .11n” on page 259. To configure channel bonding manually, on a per-IAP basis, see “IAP Settings” on page 237.

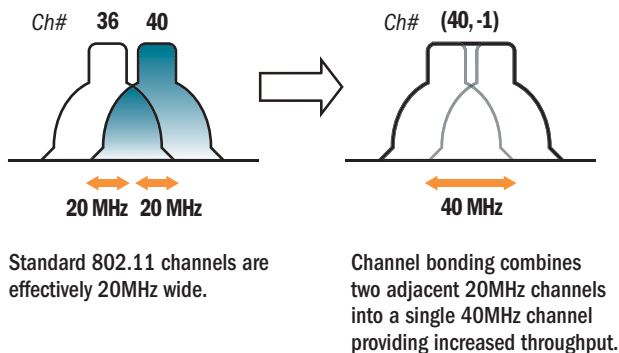


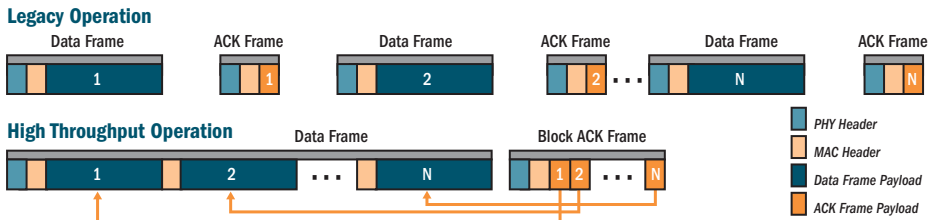
Figure 22. Channel Bonding

### Improved MAC Throughput

These changes make 802.11n transmission of MAC frames 40% more efficient than legacy transmission:

- MAC data frames are combined and given a single PHY header.
- Implicit Block ACK acknowledges all data frames within a combined frame.
- Spacing between frames is reduced.

#### Frame Aggregation



#### RIFS Usage (Reduced Inter-Frame Spacing)

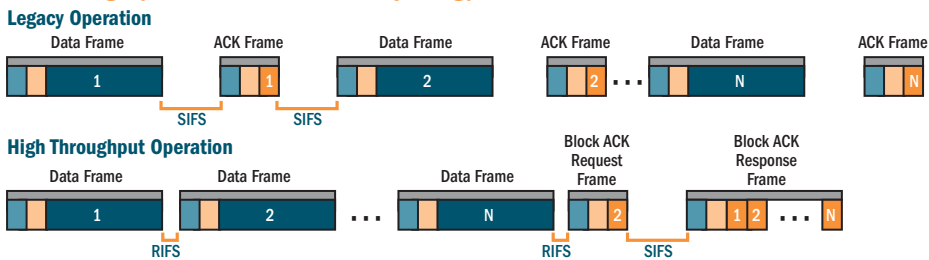


Figure 23. MAC Throughput Improvements

### Short Guard Interval

This option reduces the wait time between signals that are being sent out over the air. The guard interval provides immunity to propagation delays and reflections, and is normally 800 ns (long). By using a short guard interval (400 ns), the data rate is increased by approximately 11%. The short interval may be used in many environments (especially indoors). If the short guard interval is used in an

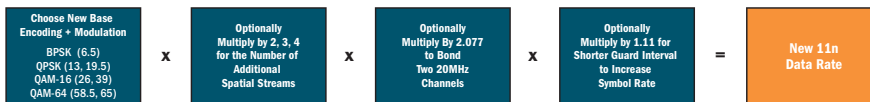
inappropriate environment, the signal quality will suffer and throughput will decrease. See “Global Settings .11n” on page 259 to configure the guard interval.

### Obtaining Higher Data Rates

The data rate increase obtained by using 802.11n on an Array is incremental, based on the technologies that are applied and the options that you select:

- Higher encoding rates (Mandatory in 802.11n)
- Spatial Streams (Mandatory, but multiplier varies directly with number of streams selected.)
- Channel Bonding (Mandatory in 802.11n, apply multiplier to IAP if it is bonded.)
- Short Guard Interval (Optional)

See Figure 24 to compute your 802.11n data rate increase for an IAP. Apply this increase to the 802.11 a, b or g data rates selected for the Array.



### Expected 802.11n Data Rates

802.11a 802.11g Rates	Expected First Generation Device Data Rates					
	11n Mandatory Data Rates	One Spatial Stream		Two Spatial Streams		
		With Channel Bonding (40MHz)	With Short Guard Interval		With Channel Bonding (40MHz)	With Short Guard Interval
6	6.5	13.5	15	13	27	30
9	13	27	30	26	54	60
12	19.5	40.5	45	39	81	90
18	26	54	60	52	108	120
24	39	81	90	78	162	180
36	52	108	120	104	216	240
48	58.5	121.5	135	117	243	270
54	65	135	150	130	270	300

Figure 24. Computing 802.11n Data Rates

### 802.11n Capacity

802.11n offers major increases in capacity over previous 802.11 standards, as shown in Figure 25. Note that this chart shows figures for 802.11n (with one spatial stream and channel bonding).

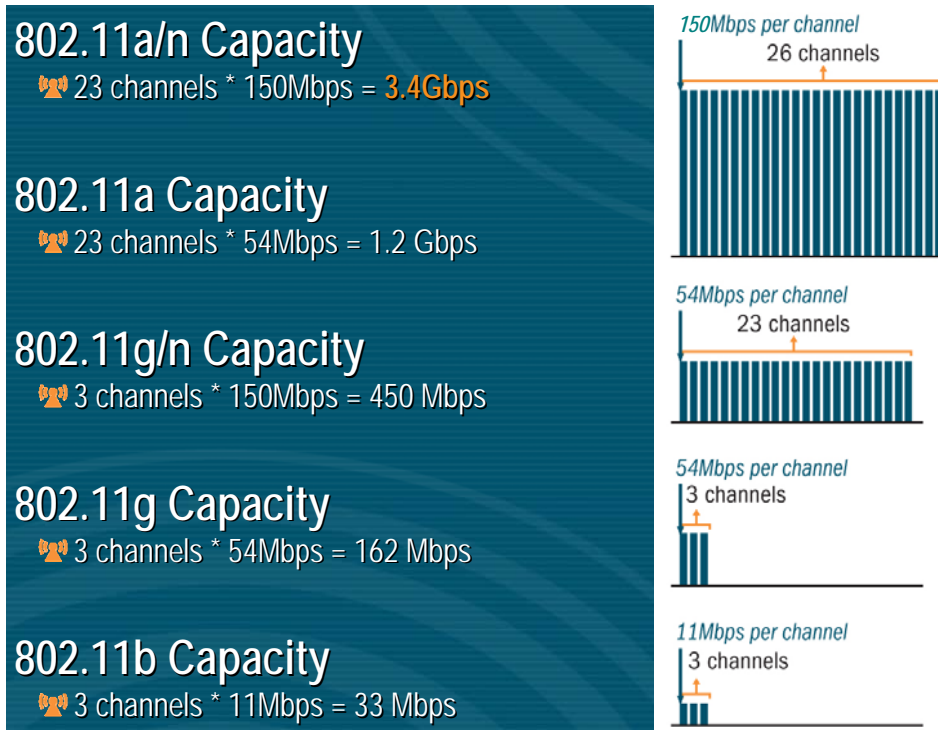


Figure 25. 802.11n Increases Capacity

**Failover Planning**

This section discusses failover protection at the unit and port levels.

**Port Failover Protection**

To ensure that service is continued in the event of a port failure, you can utilize the Gigabit 1 and Gigabit 2 Ethernet ports simultaneously.

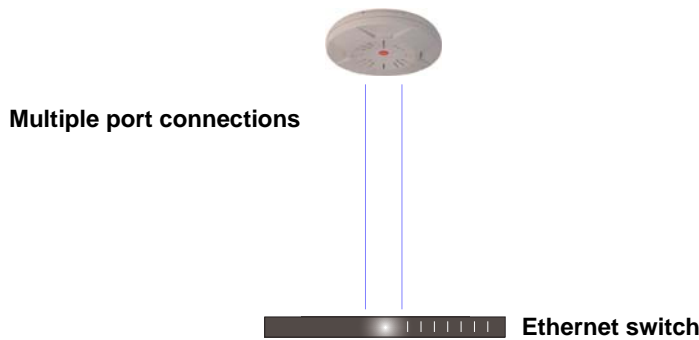


Figure 26. Port Failover Protection

In addition, the Array has full failover protection between the Gigabit 1 and Gigabit 2 ports (see following table).

Interface	Bridges Data?	Bridges Management Traffic?	Fails Over To:	IP address
Gigabit 1 (gig1)	Yes	Yes	Gigabit 2	DHCP or static
Gigabit 2 (gig2)	Yes	Yes	Gigabit 1	Assumes the IP address of Gigabit 1

The Wi-Fi Array Gigabit Ethernet ports actually support a number of modes:

- 802.3ad Link Aggregation
- Load Balancing

- Broadcast
- Link Backup
- Bridged
- Mirrored

### Switch Failover Protection

To ensure that service is continued in the event of a switch failure, you can connect Arrays to more than one Ethernet switch (not a hub).



Figure 27. Switch Failover Protection



*Gigabit Ethernet connections must be on the same subnet.*

### See Also

Coverage and Capacity Planning  
Deployment Examples  
Installation Prerequisites  
Network Management Planning  
Planning Your Installation  
Power Planning  
Security Planning

## Power Planning

All XR Series Array models support Power over Gigabit Ethernet (PoGE) with an integrated splitter.

### Power over Gigabit Ethernet

To deliver power to the Array, you must use Xirrus Power over Gigabit Ethernet (PoGE) modules. They provide power over Cat 5e or Cat 6 cables to the Array without running power cables.

Specific models of the Array are compatible with specific PoGE modules.



*When using Cat 5e or Cat 6 cable, power can be provided up to a distance of 100m.*

### See Also

Coverage and Capacity Planning

Deployment Examples

Failover Planning

Network Management Planning

Security Planning



## Security Planning

This section offers some useful guidelines for defining your preferred encryption and authentication method. For additional information, see “Understanding Security” on page 176 and the Security section of “Frequently Asked Questions” on page 404.



*Note that several advanced features in this section are part of the Xirrus Advanced RF Security Manager (RSM). They require the license installed on the Array to include support for RSM. Please see “About Licensing and Upgrades” on page 297.*

## Wireless Encryption

Encryption ensures that no user can decipher another user’s data transmitted over the airwaves. There are three encryption options available to you, including:

- **WEP-40bit or WEP-128bit**  
Because WEP is vulnerable to cracks, we recommend that you only use this for legacy devices that cannot support a stronger encryption type.
- **Wi-Fi Protected Access (WPA)**  
This is much more secure than WEP and uses TKIP for encryption.
- **Wi-Fi Protected Access (WPA2) with AES**  
This is government-grade encryption—available on most new client adapters—and uses the AES-CCM encryption mode (Advanced Encryption Standard-Counter Mode).

## Authentication

Authentication ensures users are who they say they are, and occurs when users attempt to join the wireless network and periodically thereafter. The following authentication methods are available with the Wi-Fi Array:

- **RADIUS 802.1x**  
802.1x uses a remote RADIUS server to authenticate large numbers of clients, and can handle different authentication methods (EAP-TLS, EAP-TTLS, EAP-PEAP, and EAP-LEAP Passthrough). Administrators may

also be authenticated via RADIUS when preferred, or to meet particular security standards.

- **Xirrus Internal RADIUS server**  
Recommended for smaller numbers of users (about 100 or less). Supports EAP-PEAP only
- **Pre-Shared Key**  
Uses a pass-phrase or key that is manually distributed to all authorized users. The same passphrase is given to client devices and entered into each Array.
- **MAC Access Control Lists (ACLs)**  
MAC access control lists provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network, and can be used in addition to any of the above authentication methods. ACLs are good for embedded devices, like printers and bar-code scanners (though MAC addresses can be spoofed). The Array supports 1,000 ACL entries.

### Meeting PCI DSS Standards

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by major credit card companies. It lays out a set of requirements that must be met in order to provide adequate security for sensitive data. The Wi-Fi Array may be configured to satisfy PCI DSS standards. For details, please see [Appendix D: Implementing PCI DSS](#). Note that the license installed on the Array must include the [Xirrus Advanced RF Security Manager \(RSM\)](#) to support PCI audit compliance enforcement. Please see “[About Licensing and Upgrades](#)” on [page 297](#).

### Meeting FIPS Standards

The Federal Information Processing Standard (FIPS) Publication 140-2 establishes a computer security standard used to accredit cryptographic modules. The standard is a joint effort by the U.S. and Canadian governments. To implement Level 2 security requirements of FIPS Level 2 on the Wi-Fi Array, see [Appendix E: Implementing FIPS Security](#).

*See Also*

Failover Planning

Network Management Planning

Power Planning

## Port Requirements

A number of ports are used by various Array features and by the Xirrus Management System (XMS). The [Port Requirements table on page 49](#) lists ports and the features that require them (XMS port requirements are included in the table for your convenience). If you are using a feature, please make sure that the ports that it requires are not blocked by firewalls or other policies, and that they do not conflict with any other port assignments.

As an example, XMS port requirements are illustrated in [Figure 28](#). XMS requires ports 161, 162, and 443 to be passed between Arrays and the XMS server. Similarly, ports 9090 and 9091 are required for communication between the XMS server and XMS clients, and port 25 is typically used by the XMS server to access an SMTP server to send email notifications.

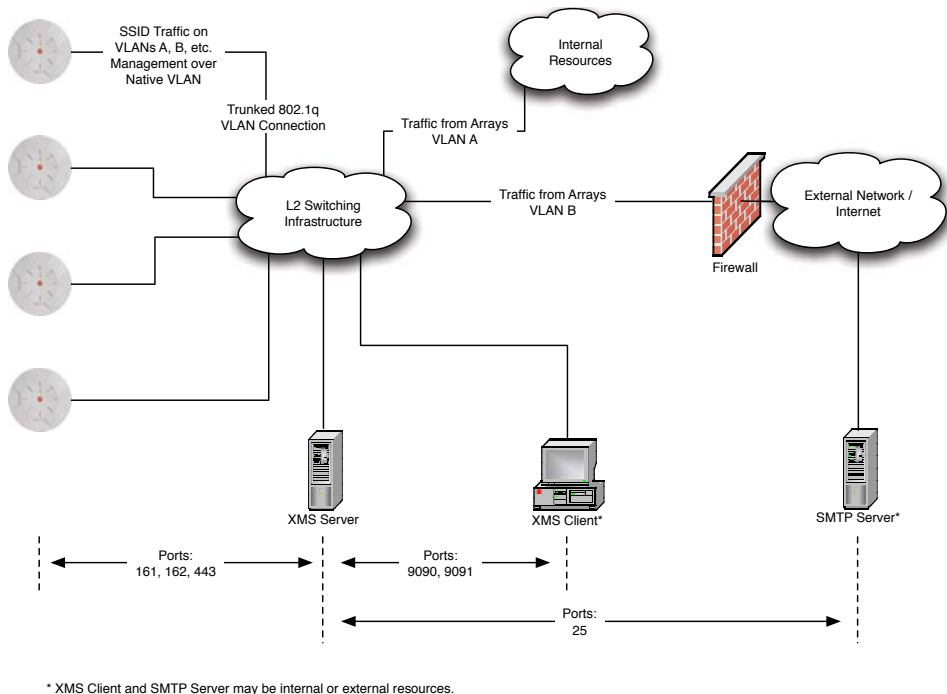


Figure 28. Port Requirements for XMS

The following table lists port requirements for the Array and for XMS, how they are used, and whether they may be changed.

Port	Application	Peer	Configurable
<b>Array</b>			
20 tcp 21 udp	FTP	Client	Yes
22 tcp	SSH	Client	Yes
23 tcp	Telnet	Client	Yes
25 tcp	SMTP	Mail Server	No
69 tcp	TFTP	TFTP Server	No
161 tcp/udp	SNMP	XMS Server	No
162 tcp/udp	SNMP Traphost Note - Up to four Traphosts may be configured.	XMS Server	Yes - but required by XMS
443 tcp	HTTPS (WMI,WPR)	Client	Yes
514 udp	Syslog	Syslog Server	No
1812, 1645 udp	RADIUS (some servers use 1645)	RADIUS Server	Yes
1813, 1646 udp	RADIUS Accounting (some servers still use 1646)	RADIUS Accounting Server	Yes
2055 udp	Netflow	Client	Yes
5000 tcp	Virtual Tunnel	VTUN Server	Yes

Port	Application	Peer	Configurable
<b>XMS</b>			
25 tcp	SMTP	Mail Server	Yes
161 udp	SNMP	Arrays	No
162 udp	SNMP Traphost 1	Arrays	Via XMS config file
443 tcp	HTTPS	Arrays	No
514 udp	Resident Syslog server	Internal*	Via XMS config file
1099 tcp	RMI Registry	Internal*	No
2000 tcp	XMS Back-end Server	Internal*	No
3306 tcp	MySQL Database	Internal*	No
8001 tcp	Status Viewer	Internal*	No
8007 tcp	Tomcat Shutdown	Internal*	During installation
8009 tcp	Web Container	Internal*	During installation
9090 tcp	XMS Webserver	XMS client	During installation
9091 tcp	XMS Client Server	XMS client	Via XMS config file
* Internal to XMS Server, no ports need to be unblocked on other network devices			

### See Also

Management Control

External Radius

Services

VLAN Management

## Network Management Planning

Network management can be performed using any of the following methods:

- Command Line Interface, using an SSH (Secure Shell) utility, like PuTTY. The utility **must** be set up to use SSH-2, since the Array will only allow SSH-2 connections.
- Web-based management, using the Array's embedded Web Management Interface (WMI). This method provides configuration and basic monitoring tools, and is good for small deployments (one or two units).
- Centralized Web-based management, using the optional Xirrus Management System (XMS), which can be run on a dedicated Xirrus appliance or your own server. The XMS is used for managing large Wi-Fi Array deployments from a centralized Web-based interface and offers the following features:
  - ◆ Globally manage large numbers of Arrays (up to 500)
  - ◆ Seamless view of the entire wireless network
  - ◆ Easily configure large numbers of Arrays
  - ◆ Rogue AP monitoring
  - ◆ Easily manage system-wide firmware updates
  - ◆ Monitor performance and trends
  - ◆ Aggregation of alerts and alarms

### *See Also*

[Failover Planning](#)

[Power Planning](#)

[Security Planning](#)

## WDS Planning

WDS (Wireless Distribution System) creates wireless backhauls between arrays, allowing your wireless network to be expanded using multiple Arrays without the need for a wired backbone to link them (see [Figure 29](#)). WDS features include:

- One to three IAPs may be used to form a single WDS link, yielding up to 1350 Mbps bandwidth per link. Up to three different WDS links may be created on a single Array.
- Automatic IAP Load Balancing
- If desired, you may allow clients to associate to a BSS on the same radio interface used for a WDS Host Link. This will take bandwidth from the WDS link.



Figure 29. WDS Link

- Multiple links per Array allow you to configure multi-hop connections.



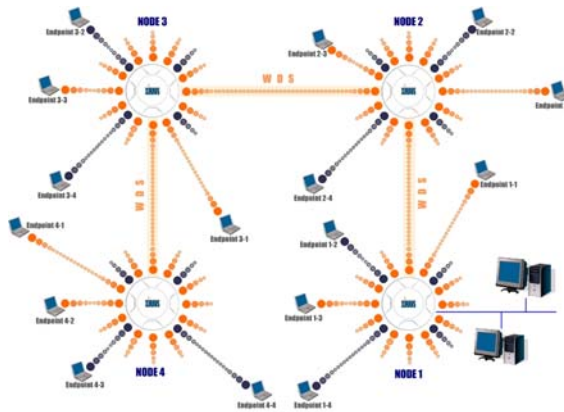


Figure 30. A Multiple Hop WDS Connection

- Multiple WDS links can provide link redundancy (failover capability - see Figure 31). A network protocol (Spanning Tree Protocol—STP) prevents Arrays from forming network loops.

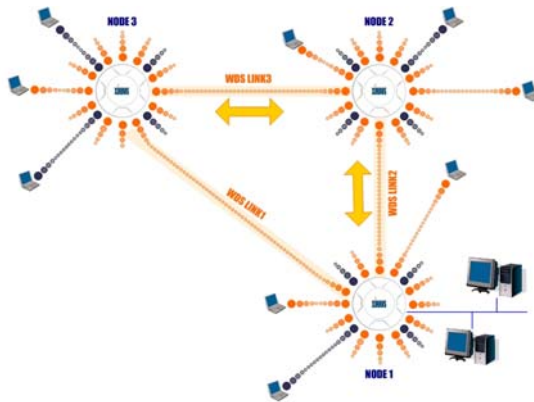


Figure 31. WDS Failover Protection

WDS links have a Host/Client relationship similar to the usual IAP/station pattern for Arrays:

- A *WDS Client Link* associates/authenticates to a host (target) Array in the same way that a station associates to an IAP. The client side of the link must be configured with the root MAC address of the target (host) Array.
- A *WDS Host Link* acts like an IAP by allowing one WDS Client Link to associate to it. An Array may have both client and host links.

WDS configuration is performed only on the client-side Array. See “WDS” on [page 278](#). Note that both Arrays must be configured with the same SSID name.

### Common Deployment Options

The following table lists some typical and recommended deployment options for a number of the features that have been discussed in this chapter.

Function	Number of Wi-Fi Arrays	
	One or Two	Three or More
Power	Power over Gigabit Ethernet	Power over Gigabit Ethernet UPS backup (recommended)
Failover	Recommended	Highly recommended
VLANs	Optional	Optional use, Can be used to put all APs on one VLAN or map to existing VLAN scheme
Encryption	WPA2 with AES (recommended) PSK or 802.1x	WPA2 with AES (recommended) 802.1x keying
Authentication	Internal RADIUS server EAP-PEAP Pre-Shared Key	External RADIUS server
Management	Internal WMI Internal CLI (via SSHv2)	XMS (SNMP)

#### *See Also*

Coverage and Capacity Planning

Deployment Examples

Network Management Planning

Planning Your Installation

Power Planning

Security Planning

## Installation Workflow

This workflow illustrates the steps that are required to install and configure your Wi-Fi Array successfully. Review this flowchart before attempting to install the unit on a customer's network.

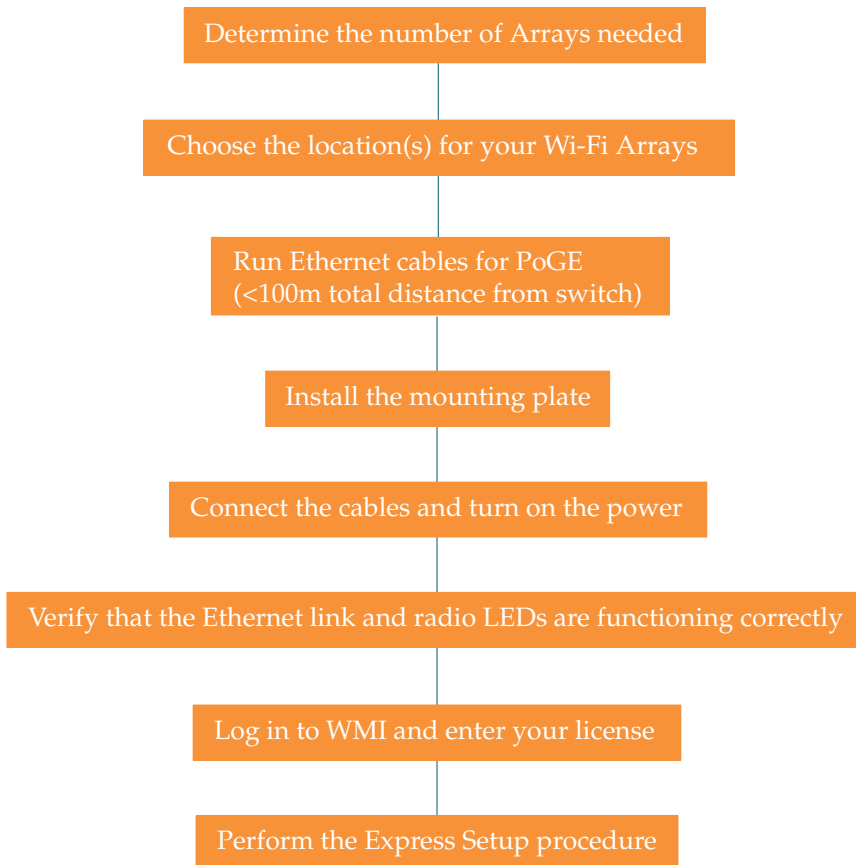


Figure 32. Installation Workflow

### *See Also*

Coverage and Capacity Planning  
Deployment Examples

---

Common Deployment Options

Failover Planning

Installation Prerequisites

Planning Your Installation

Power Planning

Wi-Fi Array Product Overview

Security Planning

## Installing Your Wi-Fi Array

This section provides instructions for completing a physical installation of your Xirrus Wi-Fi Array.

### Choosing a Location

Based on coverage, capacity and deployment examples previously discussed, choose a location for the Array that will provide the best results for your needs. The Wi-Fi Array was designed to be mounted on a ceiling where the unit is unobtrusive and wireless transmissions can travel unimpeded throughout open plan areas.

You also have the option of mounting the Array on a wall, using the optional wall mount assembly kit.

Choose a location that is central to your users (see the following diagram for correct placement).

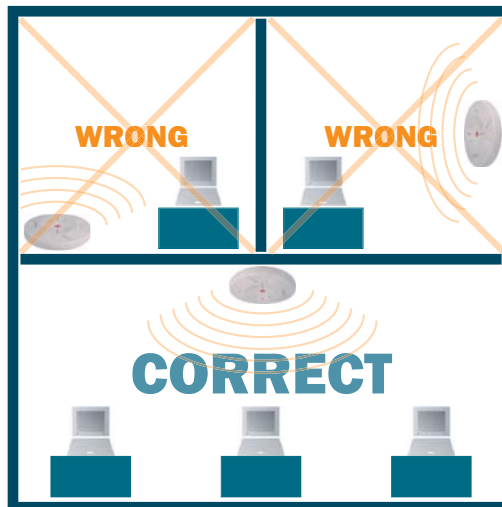


Figure 33. Array Placement

## Wiring Considerations

Before using the Xirrus Power over Gigabit Ethernet modules (PoGE) to distribute power, see “Power over Gigabit Ethernet (PoGE)” on page 10.

Once you have determined the best location for your Wi-Fi Array, you must run cables to the location for the following services:

### Power

- No power cable to the Array is required if using PoGE modules. The PoGE module requires a dedicated AC power outlet (100 - 240 VAC).

### Network

- Gigabit 1—the total of all Cat 5e or Cat 6 cable segments from the Gigabit Ethernet switch to the Array must be less than 100m long. The Array must be connected to PoGE networks without routing cabling to the outside plant, to ensure that cabling is not exposed to lightning strikes or possible high voltage crossover.
- Gigabit 2
- Serial cable (optional) — cable lengths up to 25’ per the RS-232 specification.

## Important Notes About Network Connections

Read the following notes before making any network connections.



*When the unit’s IP address is unknown or a network connection has not been established, the serial cable is used for connecting directly with the Command Line Interface (CLI) via HyperTerminal. When a network connection is established, the Array can be managed from any of the available network connections, either Gigabit 1 or Gigabit 2.*



*The Array’s Ethernet ports should be plugged into an Ethernet switch, not an Ethernet hub—if a hub is used, we recommend that you connect only one Ethernet port.*

! *The Gigabit1 Ethernet interface is the primary port for both data and management traffic. If a single Ethernet connection is used, it must be connected to the Gigabit1 Ethernet interface. See also, “Port Failover Protection” on page 42.*

*See Also*

Failover Planning  
Installation Prerequisites  
Installation Workflow  
Mounting the Array  
Power over Gigabit Ethernet (PoGE)



---

## Mounting the Array

A number of options are available for mounting Arrays:

- Ceiling mount
- Wall mount
- Secure mount in a locking indoor enclosure
- **Outdoor enclosure**
- I-Beam mount in a protective enclosure (gymnasium mount)
- Factory enclosure

A detailed Quick Installation Guide is provided with the mounting option that you selected when ordering your Array. Please follow the provided instructions carefully.

## Dismounting the Array

### *To dismount any other Array model*

For all Array models, push up on the Array (i.e., push it against the mounting plate). Then turn the Array to the left to remove it. This is similar to dismounting a smoke detector.

## Powering Up the Wi-Fi Array

When powering up, the Array follows a specific sequence of LED patterns showing the boot progress, and following a successful boot will provide extensive status information.

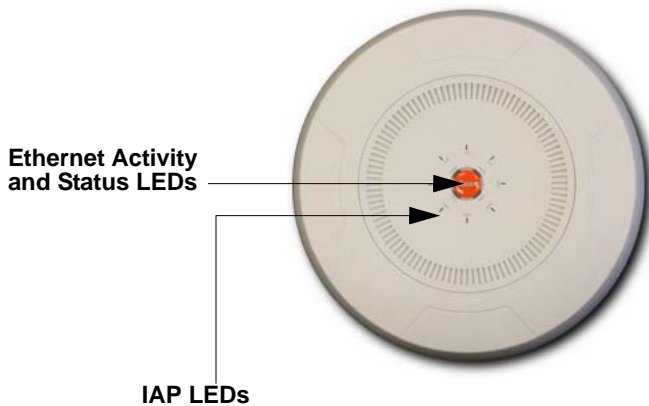


Figure 34. LED Locations

Array LED settings may be altered or disabled entirely for diagnostic purposes or for personal preference. Changes are made via the Array's Command Line Interface or the Web Management Interface—refer to “LED Settings” on page 276.

## Array LED Operating Sequences

Use the following tables to review the operating sequences of the Array's LEDs.

- "LED Boot Sequence" on page 63
- "LED Operation when Array is Running" on page 64

### LED Boot Sequence

The normal boot LED sequence is as follows:

Array Activity	Status LED	IAP LEDs
<b>Power ON</b>	Blinking GREEN	All OFF
<b>Boot loader power ON self-test</b>	Blinking GREEN	All ON
<b>Image load from compact FLASH</b>	Blinking GREEN	Spinning pattern (rotate all to ON, then all to OFF)
<b>Image load failure</b>	Blinking ORANGE	All OFF
<b>Hand off to ArrayOS</b>	Solid GREEN	All OFF
<b>System software initialization</b>	Solid GREEN	Walking pattern—(LED rotating one position per second)
<b>Up and running</b>	Solid GREEN	ON for IAPs that are up: OFF for IAPs that are down. Behavior may be changed using "LED Settings" on page 276.

### LED Operation when Array is Running

The normal LED operation when the Array is running is shown in the table below. Note that behavior may be modified using “LED Settings” on page 276 or via the CLI.

LED Status	Reason
<b>IAP LED is OFF</b>	IAP is down
<b>IAP LED is solid ON</b>	IAP is up, but no associations and no traffic
<b>IAP LED heartbeat</b>	IAP is up, with stations associated but no traffic
<b>IAP LED flashing</b> Flashing at 10 Hz Flashing at 5 Hz Flashing at 2.5 Hz	IAP is up, passing traffic Traffic > 1500 packets/sec Traffic > 150 packets/sec Traffic > 1 packet/sec
<b>IAP LED is GREEN</b>	IAP is operating in the 2.4 GHz band
<b>IAP LED is ORANGE</b>	IAP is operating in the 5 GHz band
<b>IAP LED flashing ORANGE to GREEN at 1 Hz</b>	The radio is in monitor mode (standard intrude detect)
Ethernet LEDs are dual color <b>Ethernet LED is ORANGE</b> <b>Ethernet LED is GREEN</b>	Transferring data at 1 Gbps Transferring data at 10/100 Mbps

#### See Also

[Installation Prerequisites](#)  
[Installation Workflow](#)  
[Installing Your Wi-Fi Array](#)  
[LED Settings](#)

## Establishing Communication with the Array

The Array can be configured through the Command Line Interface (CLI) using SSH, or on a browser via the graphical Web Management Interface (WMI). You can use the CLI via the serial management port, the Fast Ethernet port, or either of the Gigabit Ethernet ports. You can use the WMI via any of the Array's Ethernet ports.

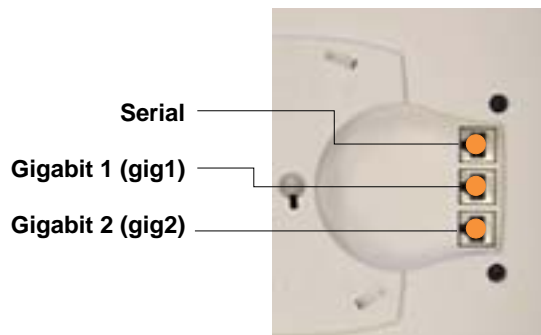


Figure 35. Network Interface Ports

### Using the Serial Port

If using the serial port to make your connection, use serial settings of 8 bits, no parity, no flow control, 1 stop bit (8N1) and a speed setting of 115200 baud. Use the communication package of your choice.

### Using the Ethernet Ports

By default, the Array's Ethernet interfaces use DHCP to obtain an IP address. If the Array is booted and does not receive DHCP addresses Gigabit Ethernet ports, both Gigabit Ethernet ports will default to 10.0.2.1.

If the Array is connected to a network that provides DHCP addresses, the IP address can be determined by the following three methods:

1. The simplest way to address the Array is using its default hostname which is the Array's serial number (for example, XR40123091CACD). If your network provides DHCP and DNS, then you can use this hostname.

2. Otherwise, examine the DHCP tables on the server and find the addresses assigned to the Array (Xirrus MAC addresses begin with 000F7D).
3. Alternatively, you may query the Array using the CLI via the serial port. Log in using the default user name **admin** and password **admin**. Use the **show ethernet** command to view the IP addresses assigned to each port.

## Starting the WMI

Use this procedure to log in to the WMI via your Web browser.

1. Establish a network connection and open your Web browser.
2. Connect to the Wi-Fi Array using its host name or IP address as described in the previous section.

## Logging In

When logging in to the Array, use the default user name and password—the default user name is **admin**, and the default password is **admin**.

### *See Also*

[Installation Workflow](#)

[Performing the Express Setup Procedure](#)

[Powering Up the Wi-Fi Array](#)

## Entering the License

A license is needed to operate the Wi-Fi Array at full functionality. Without a license, the Array may only be powered up and have a basic network configuration.

The Array's license determines many of the features that are available on the Array. For example, automatic cell sizing and channel allocation require a license supporting the RF Performance Manager (RPM). Also, IEEE 802.11n operation on XN model Arrays requires a license.

The Array's license is not installed at the factory. **You must enter your license before proceeding to the next step, [Performing the Express Setup Procedure](#).**

The procedure below describes entering the license key using the WMI. If you are using the Xirrus Management System (XMS), you may use it to easily manage and upgrade large numbers of licenses for the wireless network.

1. This procedure assumes that you have pointed a browser to the Array's IP address to start WMI, and that you have logged in with the default username and password above.
2. In the left hand frame, in the **Tools** section, click **System Tools**.
3. **License Key:** Enter the key that was provided for the Array. The key was provided to you in an email as an attachment in the form of an Excel file (.xls). Enter the key exactly as it appears in the file. Click the **Upgrade** button to apply the key.
4. Now you may verify the features provided by the key. In the **Status** section of the left hand frame, click **Array** and then click **Information**. Check the items listed in the **License Features** row.



*If you are installing a large number of licenses and do not have XMS, a Xirrus Licensing Tool may be acquired from Xirrus Support to help push licenses to large number of Arrays.*

## Performing the Express Setup Procedure

The Express Setup procedure establishes global configuration settings that enable basic Array functionality. Changes made in this window will affect all radios.

Status	Name: SS-XM4 (192.168.1.74)	Location: 12-125	Uptime: 0 days, 13 hours, 12 mins
Array	<a href="#">Save changes to flash</a>		
Network	Host Name:	SS-XM4	
RF Monitor	Location Information:	12-125	
Stations	Admin Contact:	jsmith	
Statistics	Admin Email:	jsmith@xyzcorp.com	
System Log	Admin Phone:	555-555-1212	
IDS Event Log	SNMPv2 Settings		
Configuration	Enable SNMPv2:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Express Setup	Read-Only Community String:	*****	
Network	Read-Write Community String:	*****	
Services	Gigabit Ethernet 1 Settings		
VLANs	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Security	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
SSIDs	Configuration Server Protocol:	<input checked="" type="radio"/> DHCP <input type="radio"/> Static	
Groups	IP Address:	192.168.1.74	
IAPs	IP Subnet Mask:	255.255.255.0	
WDS	Default Gateway:	192.168.1.254	
Filters	SSID Settings		
Clusters	SSID (Wireless Network Name):		
Tools	Wireless Security:	Open	
Help	<a href="#">Apply SSID Settings</a>		
System Tools	Admin Settings		
CLI	New Admin User (Replaces user "admin"):		
Options	New Admin Privilege Level:	1: read-write	
Logout	New Admin Password:		
Log Messages	Confirm Admin Password:		
Critical 12	<a href="#">Apply Admin Settings</a>		
Warning 12	Time and Date Settings		
Information 45	Current Array Date and Time:	Fri Jul 08 2011 12:27:30	
	Time Zone:	(GMT + 08:00) Beijing, Chongqing, Hong Kong	
	Auto Adjust Daylight Savings:	<input type="checkbox"/>	
	Use Network Time Protocol:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
	NTP Primary Server:	ntp.ximus.com	
	NTP Primary Authentication:	None	
	NTP Primary Authentication Key ID:	1	
	NTP Primary Authentication Key:		
	NTP Secondary Server:		
	NTP Secondary Authentication:	None	
	NTP Secondary Authentication Key ID:	2	
	NTP Secondary Authentication Key:		
	IAP Settings		
	Enable/Configure All IAPs:	<a href="#">Execute</a>	



Figure 36. 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 SNMPv2:** Select whether to **Enable** SNMPv2 on the Array, and change the **SNMP Community Strings** if desired. If you are using the Xirrus Management System (XMS), these strings must match the values used by XMS. The default values for the Array match the defaults in XMS. For more details, including SNMPv3, see “SNMP” on page 165.
7. **Configure the Gigabit 1 and Gigabit 2 network interfaces.** The fields for each of these interfaces are the same, and include:
  - a. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.
  - b. **Allow Management on Interface:** Choose **Yes** to allow management of the Array via this network 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 any of the remote connections (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. **SSID (Wireless Network Name):** The SSID (Service Set Identifier) is a unique name that identifies a wireless network. All devices attempting to connect to a specific WLAN must use the same SSID. The default for this field is “**xirrus**.”

For additional information about SSIDs, go to the [Multiple SSIDs](#) section of “[Frequently Asked Questions](#)” on page 404.

- b. **Wireless Security:** Select the desired wireless security scheme (Open, [WEP](#), [WPA](#), [WPA2](#), or WPA-Both). WPA2 is recommended for the best Wi-Fi security.
- **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)**—An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

- **WPA** (Wi-Fi Protected Access)—A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1x for authentication.
- **WPA2** (Wi-Fi Protected Access 2)—WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.
- **WPA-Both** (WPA and WPA2)—This option makes use of both WPA and WPA2.

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

- c. **WEP Encryption Key/Passphrase:** Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase. This field and the one below only appear if you select a **Wireless Security** option other than **Open**.
  - d. **Confirm Encryption Key/Passphrase:** If you entered a WEP key or WPA passphrase, confirm it here.
  - e. Click **Apply SSID Settings** when done.
9. **Admin Settings:** This section allows you to change the default admin username, password, and privileges for the Array. You may change the password and leave the user name as is, but we suggest that you change both to improve Array security.
  - a. **New Admin User (Replaces user “admin”):** Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the Array also offers the option of authenticating administrators using a RADIUS server (see [“Admin Management” on page 181](#)).

- b. New Admin Privilege Level:** By default, the new administrator will have read/write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see [“Admin Privileges” on page 183](#).
          - c. New Admin Password:** Enter a new administration password for managing this Array. If you forget this password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
          - d. Confirm Admin Password:** If you entered a new administration password, confirm the new password here.
          - e. Click Apply Admin Settings** when done.
- 10. Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you’re not using a server.
  - a. Current Array Date and Time:** This read-only field shows the current time for your convenience.
  - b. Time Zone:** Select your time zone from the choices available in the pull-down list.
  - c. Auto Adjust Daylight Savings:** If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
  - d. Use Network Time Protocol:** Check this box if you want to use an [NTP](#) server to synchronize the Array’s clock. Use of NTP is mandatory for Arrays to be managed with XMS (the Xirrus Management System), and ensures that Syslog time-stamping is maintained across all units. 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.

- e. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
- f. **NTP Primary Authentication:** If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default). For more information on authenticated NTP, see [“Time Settings \(NTP\)”](#) on page 157.
- g. **NTP Primary Authentication Key ID:** Enter the key ID, which is a decimal integer.
- h. **NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- i. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.
- j. **Adjust Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes, seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).
- k. **Adjust Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, the date fields become active. Enter the revised date (month, day and year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).

### 11. IAP Settings:

**Enable/Configure All IAPs:** Click on the **Execute** button to enable and auto configure all IAPs (a message displays the countdown time—in seconds—to complete the auto-configuration task). When an IAP is enabled, its LED is switched on. (see also “[Array LED Operating Sequences](#)” on page 63.)

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

This ends the Express Setup procedure.

#### *See Also*

[Establishing Communication with the Array](#)

[Installation Prerequisites](#)

[Installation Workflow](#)

[Logging In](#)

[Multiple SSIDs](#)

[Security](#)

---

# The Web Management Interface

This topic provides an overview of the Xirrus Wi-Fi Array's embedded Web Management Interface (WMI), used for establishing your network's configuration settings and wireless operating parameters. It also includes login instructions. The following topics are discussed:

- An Overview
- Structure of the WMI
- User Interface
- Logging In
- Applying Configuration Changes

## An Overview

The WMI is an easy-to-use graphical interface to your Wi-Fi Array. It allows you to configure the product to suit your individual requirements and ensure that the unit functions efficiently and effectively.

**XR4820 Wi-Fi Array** **XIRRUS**

Status: Name: XR4012601C.506 (10.100.54.55) Uptime: 5 days, 14 hours, 42 mins

Configuration: Enable All IAPs | Disable All IAPs | Reset Channels

IAP	Enabled	Band	WiFi Mode	Channel	Bond	Lock	Cell Size	Tx dBm	Rx dBm	WDS Dist. (miles)	Antenna Select	Description
lap1	<input type="checkbox"/>	5 GHz	a-only	161	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap2	<input type="checkbox"/>	5 GHz	a-only	64	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap3	<input type="checkbox"/>	5 GHz	a-only	44	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap4	<input type="checkbox"/>	5 GHz	a-only	153	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap5	<input type="checkbox"/>	5 GHz	a-only	56	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap6	<input type="checkbox"/>	2.4 GHz	bgn	6	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap7	<input type="checkbox"/>	5 GHz	a-only	36	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
lap0	<input type="checkbox"/>	monitor	abgn	mon	off	<input type="checkbox"/>	monitor	20	-95		Internal-Omni	

Navigation menu includes: Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, IAPs, IAP Settings, WDS, Filters, Clusters, Tools, Log Messages.

Copyright © 2005-2011 by Xirus, Inc.

Figure 37. Web Management Interface



## Structure of the WMI

The content of the WMI is organized by function and hierarchy, shown in the following table. Click on any item below to jump to the referenced destination.

<p><b>Status Windows</b></p> <ul style="list-style-type: none"> <li>Array Status Windows             <ul style="list-style-type: none"> <li>Array Summary</li> <li>Array Information</li> <li>Array Configuration</li> <li>Admin History</li> </ul> </li> <li>Network Status Windows             <ul style="list-style-type: none"> <li>Network Map</li> <li>Spanning Tree Status</li> <li>Routing Table</li> <li>ARP Table</li> <li>DHCP Leases</li> <li>Connection Tracking/NAT</li> <li>CDP Neighbors</li> <li>Network Assurance</li> </ul> </li> <li>RF Monitor Windows             <ul style="list-style-type: none"> <li>IAPs</li> <li>Spectrum Analyzer</li> <li>Intrusion Detection</li> <li>Channel History</li> </ul> </li> <li>Station Status Windows             <ul style="list-style-type: none"> <li>Stations</li> <li>Location Map</li> <li>RSSI</li> <li>Signal-to-Noise Ratio (SNR)</li> <li>Noise Floor</li> <li>Max by IAP</li> <li>Station Assurance</li> </ul> </li> </ul>	<p><b>Statistics Windows</b></p> <ul style="list-style-type: none"> <li>IAP Statistics Summary</li> <li>Per-IAP Statistics</li> <li>Network Statistics</li> <li>VLAN Statistics</li> <li>WDS Statistics</li> <li>Filter Statistics</li> <li>Station Statistics</li> <li>Per-Station Statistics</li> </ul> <p><b>System Log Window</b></p> <p><b>IDS Event Log Window</b></p>
--	--

<b>Configuration Windows</b>	<b>Configuration Windows (cont'd)</b>
Express Setup	IAPs
Network	IAP Settings
Network Interfaces	Global Settings (IAP)
DNS Settings	Global Settings .11a
CDP Settings	Global Settings .11b
Services	Global Settings .11n
Time Settings (NTP)	Advanced RF Settings
NetFlow	Intrusion Detection
Wi-Fi Tag	LED Settings
System Log	WDS
SNMP	WDS Client Links
DHCP Server	Filters
VLANs	Filter Lists
VLAN Management	Filter Management
Security	Clusters
Admin Management	Cluster Definition
Admin Privileges	Cluster Management
Admin RADIUS	Cluster Operation
Management Control	
Access Control List	<b>Tool Windows</b>
Global Settings	System Tools
External Radius	CLI
Internal Radius	Options
Rogue Control List	Logout
SSIDs	
SSID Management	
Active IAPs	
Per-SSID Access Control List	
Groups	
Group Management	

### User Interface

The WMI has been designed with simplicity in mind, making navigation quick and easy. In the following example, you'll see that windows are divided into left and right frames.

Left frame
Right frame
Array info

IAP	Enabled	Band	WiFi Mode	Channel	Bond	Lock	Cell Size	Tx dBm	Rx dBm	WDS Dist. (miles)	Antenna Select	Description
iap1	<input type="checkbox"/>	5 GHz	a-only	161	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap2	<input type="checkbox"/>	5 GHz	a-only	64	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap3	<input type="checkbox"/>	5 GHz	a-only	44	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap4	<input type="checkbox"/>	5 GHz	a-only	153	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap5	<input type="checkbox"/>	5 GHz	a-only	56	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap6	<input type="checkbox"/>	2.4 GHz	bgn	6	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap7	<input type="checkbox"/>	5 GHz	a-only	36	off	<input type="checkbox"/>	max	20	-90		Internal-Dir	
iap8	<input type="checkbox"/>	monitor	abgn	mon	off	<input type="checkbox"/>	monitor	20	-95		Internal-Omni	

Log Messages	Count
Critical	81
Warning	84
Information	244

Figure 38. WMI: Frames

The left frame contains three main elements:

- Menu organized by function (for example, Network, SSIDs, Security, etc.). Click a heading, such as **Network**, to display a summary of its current configuration, as well as an associated pull-down menu. The three major menu sections (**Status**, **Configuration**, **Tools**) may each be collapsed down to hide the headings under them. Click again to display the headings. (Figure 39)
- Three **Log Messages** counters are located at the bottom of the menu. They provide a running total of messages generated by the ArrayOS Syslog subsystem during your session—organized into **Critical**, **Warning**, and **General** messages. Click on a counter to display the associated Syslog messages. Messages at the selected level or higher will be shown. For more information, please see “System Log Window” on page 134.
- The Array representation contains shortcut links. Click a radio to view statistics for it. Click the center of the Array to display the **IAP Settings** window, which allows you to configure the Array’s radios.

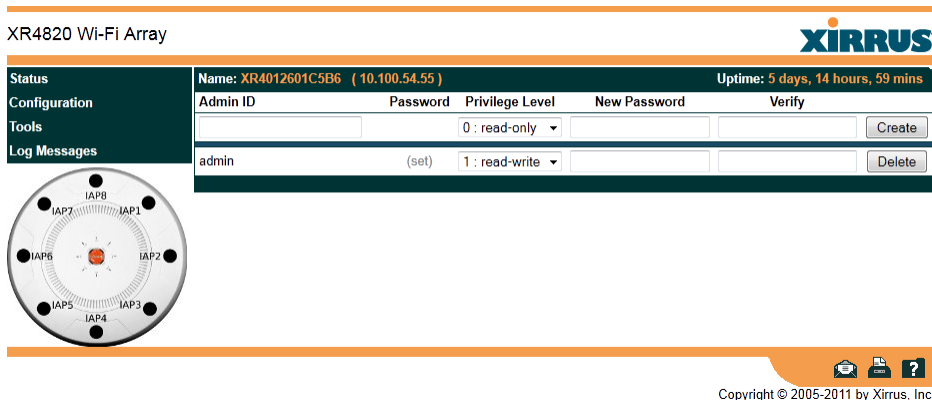


Figure 39. Major Menu Sections Collapsed (on left)

The right frame displays the status information or configuration parameters for the Wi-Fi Array. This is where you review the Array’s current status and activity or input data (if you want to make changes). The green Array information bar at the top of the frame describes the Array—the Name and IP address allow you to

quickly confirm that WMI is connected to the correct Array. The current Uptime since the last reboot is also shown.



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

Note that WMI provides options which allow you to change its appearance and behavior. You may change:

- **Style**—changes the colors and appearance of WMI (i.e., its “skin”).
- **Refresh Interval**—the refresh time when automatic refresh is selected.
- **Close menu section when deselected**—changes the behavior of the menu in the left frame.
- **Clear screen when loading new page.**

See “**Options**” on page 309 for more information.

### Utility Buttons

At the bottom of each window you will find a set of useful buttons—a **Feedback** button, a **Print** button and a **Help** button.

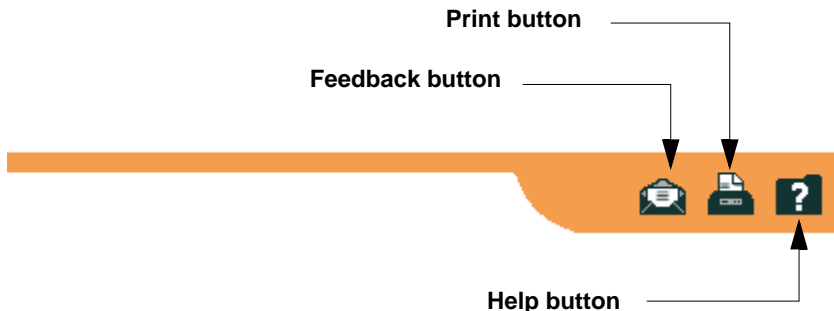


Figure 40. WMI: Utility Buttons

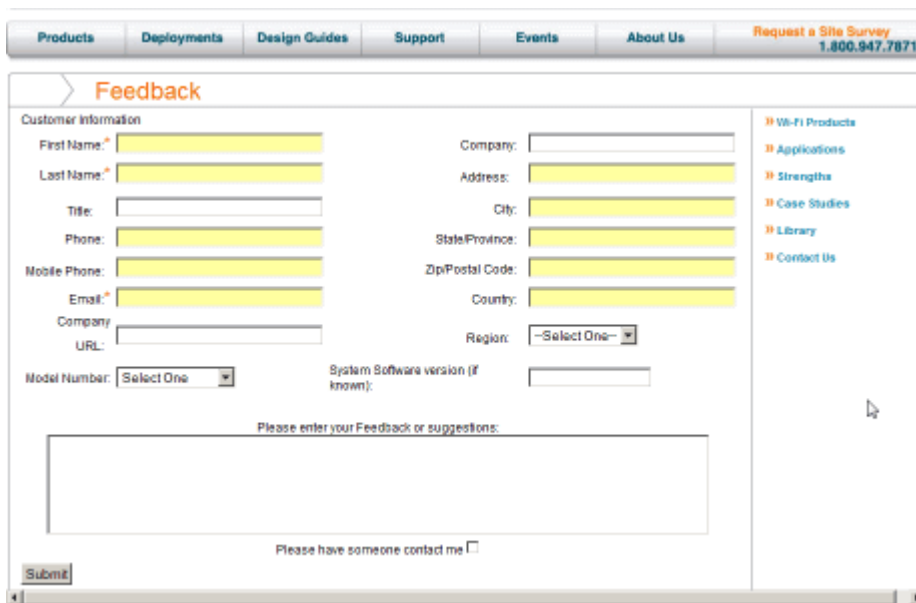
- Click on the **Feedback** button to generate a Web page that allows you to submit your comments to Xirrus, Inc. You can also access the feedback

page at <http://www.xirrus.com/public/feedback/>. Refer to Figure 41 on page 82 to see a sample of the feedback form.

- Click on the **Print** button to send a print file of the active window to your local printer.
- Click on the **Help** button to access the Array's online help system.

### Submitting Your Comments

When submitting comments via the Feedback button (Figure 41), ensure that you provide as much detail as possible, including your contact information, the product model number that the comment relates to, and the ArrayOS software version (if known). When finished, click on the **Submit** button to submit your comment.



The screenshot shows a web browser window displaying the Xirrus Feedback Form. At the top, there is a navigation bar with links for Products, Deployments, Design Guides, Support, Events, About Us, and a Request a Site Survey button with the phone number 1.800.947.7871. The main heading is "Feedback". Below this, the form is organized into sections. The "Customer Information" section includes fields for First Name, Last Name, Title, Phone, Mobile Phone, Email, Company, URL, Company, Address, City, State/Province, Zip/Postal Code, Country, and Region. There are also dropdown menus for Model Number and System Software version (if known). A large text area is provided for "Please enter your Feedback or suggestions:". At the bottom, there is a checkbox for "Please have someone contact me" and a "Submit" button. On the right side, there is a vertical menu with links for Wi-Fi Products, Applications, Strengths, Case Studies, Library, and Contact Us.

Figure 41. Feedback Form

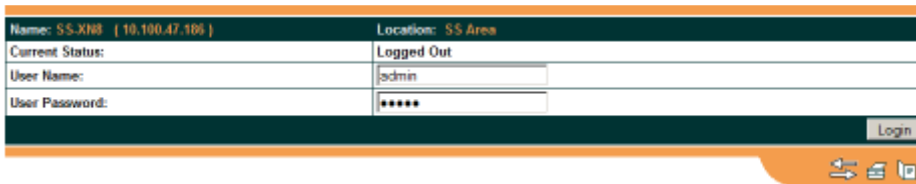
## Logging In

Use this procedure to log in to the WMI via your Web browser.

1. Establish a network connection and open your Web browser.
2. If your network supports DHCP and DNS, enter the Array's default host name in the browser's URL. The default host name is simply the Array's serial number (for example, XN0823091CACD).

Otherwise, enter the Array's IP address. This may be determined as described in "Using the Ethernet Ports" on page 65.

3. To log in to the Array's Web Management Interface, enter **admin** for both the user name and password.



The screenshot shows a web browser window displaying the login page for a Wi-Fi Array. The page has a dark blue header with orange accents. At the top left, it displays "Name: SS-X08 (10.100.47.108)" and "Location: SS Area". Below this is a table with two columns: "Current Status:" and "Logged Out". The "Current Status:" row shows "User Name:" with the value "admin" and "User Password:" with masked characters "\*\*\*\*\*". The "Logged Out" column is empty. A "Login" button is located at the bottom right of the form area. At the bottom of the browser window, navigation icons for back, forward, and home are visible.

Figure 42. Logging In to the Wi-Fi Array

## Applying Configuration Changes

In most of the WMI configuration windows, your changes to settings are applied to the Array as you make them. In most cases, there is no separate Apply button to click to make the changes take effect. There are a few exceptions to this rule. In these cases, a particular section of a page may have its own **Apply Settings** button right below the settings.

In both cases described above, the changes that you have made are not saved to the latest configuration file in the Array's flash memory, so they will not be restored after a reboot. Click the **Save changes to flash** button (located on the upper right of each page) in order to make sure that these changes will be applied after rebooting. This will save the entire current configuration, not only the changes on current WMI page.

### Character Restrictions

When inputting strings in the WMI (for example, assigning SSIDs, host name, password, etc.), use common alphanumeric characters. Some of the fields in the WMI will not accept special characters, so use of the following characters should typically be avoided:

&    <    >    '    "    /    \



---

# Viewing Status on the Wi-Fi Array

These windows provide status information and statistics for your Array using the product's embedded Web Management Interface (WMI). You cannot make [configuration changes](#) to your Array from these windows. The following topics have been organized into functional areas that reflect the [flow and content](#) of the Status section of the navigation tree in the left frame of the WMI.

- [“Array Status Windows” on page 86](#)
- [“Network Status Windows” on page 92](#)
- [“RF Monitor Windows” on page 102](#)
- [“Station Status Windows” on page 111](#)
- [“Statistics Windows” on page 126](#)
- [“System Log Window” on page 134](#)
- [“IDS Event Log Window” on page 135](#)

Configuration and Tools windows are not discussed here. For information on these windows, please see:

- [“Configuring the Wi-Fi Array” on page 137](#)
- [“Using Tools on the Wi-Fi Array” on page 295](#)

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

## Array Status Windows

The following Array Status windows are available:

- **Array Summary**—displays information on the configuration of all Array interfaces, including IAPs.
- **Array Information**—provides version/serial number information for all Array components.
- **Array Configuration**—shows all configuration information for the Array in text format.
- **Admin History**—shows all current and past logins since the last reboot.

### Array Summary

This is a status only window that provides a snapshot of the global configuration settings for all Wi-Fi Array network interfaces and IAPs. 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. Clicking on an interface or IAP will take you to the proper window for making configuration changes.

XR4820 Wi-Fi Array													XIRRUS			
Name: XR4012601C5B6 ( 10.100.54.55 )													Uptime: 5 days, 15 hours, 41 mins			
Ethernet Interfaces																
Interface	State	Mgmt	Auto Neg	LED	Link	Duplex	Speed (Mbps)	MTU Size	Port Mode	DHCP	IP Address	Subnet Mask	Gateway			
gig1	enabled	on	on	on	up	full	1000	1500	link-backup	disabled	10.100.54.55	255.255.255.0	10.100.54.1			
gig2	enabled	on	on	on	down			1500	link-backup	disabled	10.100.54.55	255.255.255.0	10.100.54.1			
Integrated Access Points																
IAP	State	AP Type	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link / Distance	MAC Address / BSSID	Description				
iap1	down	11abgn 2x2	161	automatic	a-only	internal directional	max	20	-90	0	00:0f:7d:43:b0:80-81					
iap2	down	11abgn 2x2	64	automatic	a-only	internal directional	max	20	-90	0	00:0f:7d:43:b0:90-91					
iap3	down	11abgn 2x2	44	automatic	a-only	internal directional	max	20	-90	0	00:0f:7d:43:b0:a0-a1					
iap4	down	11abgn 2x2	153	automatic	a-only	internal directional	max	20	-90	0	00:0f:7d:43:b0:b0-b1					
iap5	down	11abgn 2x2	56	automatic	a-only	internal directional	max	20	-90	0	00:0f:7d:43:b0:c0-c1					
iap6	down	11abgn 2x2	6	automatic	bgn	internal directional	max	20	-90	0	00:0f:7d:43:b0:d0-d1					
iap7	down	11abgn 2x2	36	automatic	a-only	internal directional	max	20	-90	0	00:0f:7d:43:b0:e0-e1					
iap8	down	11abgn 2x2		mon manual	abgn	internal omni	monitor	20	-95	0	00:0f:7d:43:b0:f0-f1					

Figure 43. Array Summary

## Content of the Array Summary Window

The Array Summary window is sub-divided into the **Ethernet Interfaces** section and the **Integrated Access Points** (radio) section, providing you with the following information:

- **Ethernet Interfaces Section**

This section provides information about network interface devices. To make configuration changes to these devices, go to [“Network Interfaces” on page 147](#).

- **Interface:** Lists the network interfaces that are available on the Array (Gigabit Ethernet 1 and Gigabit Ethernet 2).
- **Status:** Shows the current state of each interface, either enabled or disabled.
- **Link:** Shows whether the link on this interface is up or down.
- **DHCP:** Shows whether DHCP on this port is enabled or disabled.
- **IP Address:** Shows the current IP address assigned to each network interface device.
- **Subnet Mask:** Shows the subnet mask, which defines the number of IP addresses that are available on the routed subnet where the Array is located.
- **Gateway:** Shows the IP address of the router that the Array uses to transmit data to other networks.

- **Integrated Access Points Section**

This section provides information about the Integrated Access Points (IAPs) that are contained within the Array. How many IAPs are listed depends on which product model you are using. To make configuration changes to these IAPs, go to [“IAP Settings” on page 237](#).

- **IAP:** Lists the IAPs that are available on the Array.
- **State:** Shows the current state of each IAP, either up or down. IAPs that are down are shown in RED. [Figure 44](#) shows an example where IAP a3 is down.

- AP Type:** Shows the types of 802.11 clients supported by this IAP (11/a/b/g/n) and the number of separate data streams transmitted and received by the antennas of each IAP for 802.11n. For example, 3x3 means that the IAP supports three transmit chains and three receive chains. See [“Multiple Data Streams—Spatial Multiplexing”](#) on page 37.

Integrated Access Points											
IAP	State	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link / Distance	MAC Address / BSSID	Description
iap1	down										
iap2	up	36 manual	an	internal directional	max	20	-90	0		00:0f:7d:44:02:90	
iap3	down										
iap4	up	56 manual	an	internal directional	max	20	-90	0		00:0f:7d:44:02:b0	
iap5	down										
iap6	up	1 manual	bgn	internal directional	max	20	-90	0		00:0f:7d:44:02:d0	
iap7	down										
iap8	up	48 manual	an	internal directional	max	20	-90	0		00:0f:7d:44:02:f0	

Figure 44. Disabled IAP (Partial View)

- Channel:** Shows which channel each IAP is using, and the channel setting. To avoid co-channel interference, adjacent radios should not be using adjacent channels. To make channel selections for a specific IAP, go to [“IAP Settings”](#) on page 237.
- Antenna:** Shows which antenna is being used by each IAP.
- Wi-Fi Mode:** Shows the 802.11 client types that the IAP has been configured to support.
- Cell Size:** Indicates which cell size setting is currently active for each IAP—small, medium, large, max, automatic, or manually defined by you. The cell size of an IAP is a function of its transmit power and determines the IAP’s overall coverage. To define cell sizes, go to [“IAP Settings”](#) on page 237. For additional information about cell sizes and the importance of planning for and defining the optimum cell sizes for your Array, go to [“Coverage and Capacity Planning”](#) on page 24.

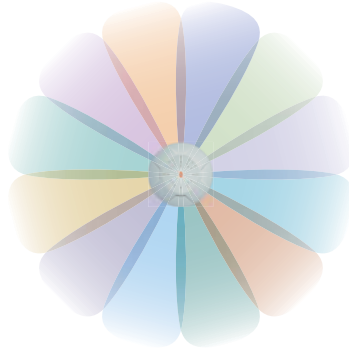


Figure 45. IAP Cells

- **Tx Power:** Shows the transmit power for each IAP.
- **Rx Threshold:** Shows the receive threshold for each IAP.
- **Stations:** Informs you how many client stations are currently associated with each IAP. XN Arrays can handle up to 96 concurrent users per individual IAP, thus 16-port XN models can handle 1536 users per Array.
- **WDS Link/Distance:** The WDS Link on this radio (if any), and whether the link has been set to support [Long Distance Links](#). See “WDS” on page 278.
- **MAC Address/BSSID:** Shows the MAC address for each IAP.
- **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, serial numbers assigned to each module, MAC addresses, licensing information, recent boot timestamps, and current internal temperatures.

Note that the **License Features** row lists the features that are supported by your Array's license. See "About Licensing and Upgrades" on page 297 and "Advanced Feature Sets" on page 14 for more information.

XR4820 Wi-Fi Array

Status	Name: XR4012601C5B6 ( 10.100.54.55 )			Uptime: 5 days, 16 hours, 12 mins
▼ Array	<b>Hardware Configuration</b>			
Summary	<b>Model</b>	XR4820, 1.0GB-ECC (700MHz)		
Information	<b>Component</b>	<b>Part Number</b>	<b>Serial Number</b>	<b>Date</b>
Configuration	System	XR4820	XR4012601C5B6	2011-Jun-29 15:49
Admin History	Controller	100-0114-001.7	0000116150	2011-Jan-12 18:59
▶ Network	IAP Module 1	100-0119-003.02	0200002203	2011-Jun-25 19:56
▶ RF Monitor	IAP Module 2	100-0119-003.02	0200002254	2011-Jun-26 17:02
▶ Stations	IAP Module 3	100-0119-003.02	0200002304	2011-Jun-27 14:51
▶ Statistics	IAP Module 4	100-0119-003.02	0200002177	2011-Jun-27 16:47
System Log	IAP Module 5	100-0119-003.02	0200002230	2011-Jun-28 5:10
IDS Event Log	IAP Module 6	100-0119-003.02	0200002201	2011-Jun-25 19:56
	IAP Module 7	100-0119-003.02	0200002199	2011-Jun-25 19:56
<b>Configuration</b>	<b>FPGA Status</b>	<b>Boot Version</b>	<b>S/W Version</b>	
Express Setup	Switching Engine	3000-00.004	3000-00.007	
▶ Network	<b>Interface</b>	<b>MAC Address(es)</b>		
▶ Services	IAPs	00:0f:7d:43:b0:80-43:b0:ff		
▶ VLANs	Gigabit 1	00:0f:7d:01:c5:b6		
▶ Security	Gigabit 2	00:0f:7d:01:c5:b7		
▶ SSIDs	<b>Software Configuration</b>			
▶ Groups	<b>Component</b>	<b>Version</b>		
▶ IAPs	SCD Firmware	3.08 (Jul 1 2011), Build: 4196		
▶ WDS	Boot Loader	6.0.0 (Jul 15 2011), Build: 6025		
▶ Filters	IAP Driver	1.5.0 (Jul 30 2011), Build: 1234		
▶ Clusters	System Software	6.0.1 (Jul 30 2011), Build: 3081		
<b>Tools</b>	License Key	1QVU1-D8J6F-1W1X5-2D0E6		
<b>Log Messages</b>	License Features	ArrayOS 6.0 for 8 2x2 IAPs + RF Performance Manager + RF Analysis Manager + RF Security Manager + Public Safety Band + 802.11n		
	<b>Operating Status</b>			
	Time This Boot	Tue 2011-Aug-02 20:49:03 GMT		
	Time Last Boot	Tue 2011-Aug-02 20:39:25 GMT		
	<b>Component</b>	<b>Temperature °C (F)</b>		
	Controller	54 ( 129.2 )		

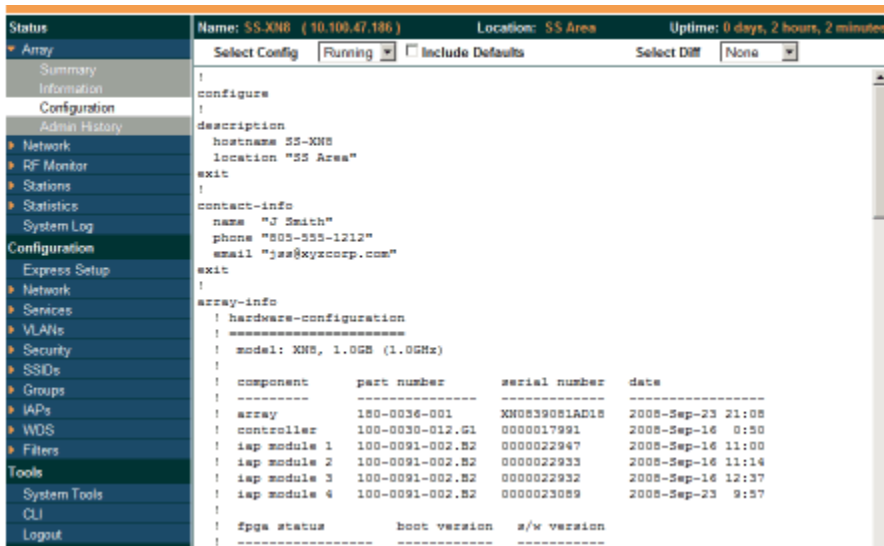
Figure 46. Array Information

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.

## 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.



```

Status
Name: SS-X08 ( 10.100.47.186 ) Location: SS Area Uptime: 0 days, 2 hours, 2 minutes
Array
Select Config [Running] [ ] Include Defaults Select Diff [None]
Summary
Information
Configuration
Admin History
Network
RF Monitor
Stations
Statistics
System Log
Configuration
Express Setup
Network
Services
VLANs
Security
SSIDs
Groups
IAPs
WDS
Filters
Tools
System Tools
CLI
Logout

!
configure
!
description
hostname SS-X08
location "SS Area"
exit
!
contact-info
name "J Smith"
phone "805-555-1212"
email "jss@xyzcorp.com"
exit
!
array-info
! hardware-configuration
! =====
! model: X08, 1.0GB (1.0GHz)
!
!
! component      part number      serial number     date
! -----
! array          100-0036-001     XH0839081AD18    2008-Sep-23 21:08
! controller    100-0030-012.G1  0000017991       2008-Sep-16  8:50
! 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
!
! fpga status      boot version     s/w version
! -----

```

Figure 47. 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: S5-X100 [ 10.100.47.100 ]	Location: S5 Area			Uptime: 4 days, 0 hours, 50 minutes		
<ul style="list-style-type: none"> <li>▼ Array</li> <li>Summary Information</li> <li>Configuration</li> <li>Admin History</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> </ul>	User	IP Address	Interface	Via	Login Time	Logout Time	Session Time D:H:M
	admin	10.100.21.55	WIFI	https	Dec-09 12:59	active	0:02:05
	admin	10.100.21.55	WIFI	https	Dec-09 11:54	active	0:03:10
	admin	10.100.21.55	WIFI	https	Dec-09 10:16	active	0:04:48
	admin	10.100.21.55	WIFI	https	Dec-08 10:15	Dec-09 10:15	
	admin	10.100.21.55	WIFI	https	Dec-05 14:41	Dec-08 10:16	
	admin	10.100.21.55	WIFI	https	Dec-05 14:12	active	4:00:52

Figure 48. Admin Login History

## Network Status Windows

The following Network Status windows are available:

- **Network**—displays a summary of network interface settings.
- **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 Assurance**—shows results of connectivity tests for network servers.

### Network

This window provides a snapshot of the configuration settings currently established for Array’s wired interfaces. This includes the Gigabit interfaces. **DNS Settings** are summarized as well. You can click on any item in the **Interface** column to go to the associated configuration window.

Interface	State	Mgmt	Auto Neg	LED	Link	Duplex	Speed (Mbps)	MTU Size	Port Mode	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	on	on	on	up	full	1000	1500	link-backup	disabled	10.100.54.55	255.255.255.0	10.100.54.1
gig2	enabled	on	on	on	down			1500	link-backup	disabled	10.100.54.55	255.255.255.0	10.100.54.1

DNS Settings Summary				
Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3
XR4012601C5B6				

Figure 49. Network Settings

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

- **“Network Interfaces” on page 147**
- **“DNS Settings” on page 153**
- **“CDP Settings” on page 154**

## 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: BrianXN16 ( 10.100.47.33 )			Uptime: 0 days, 0 hours, 29 mins
Array	<input type="checkbox"/> Hardware <input type="checkbox"/> License <input checked="" type="checkbox"/> Software <input type="checkbox"/> Firmware <input type="checkbox"/> IAP Info <input type="checkbox"/> Stations <input type="checkbox"/> Default <input type="checkbox"/> Auto Refresh <input type="button" value="Refresh"/>			
Network	Array Name	IP Address	Location	Array OS
Network Map	SS-XN0429091D207	10.100.47.16		XS-4.1.0-1269
Spanning Tree Status	BrianXN16	10.100.47.33		XS-4.1.0-1269
Routing Table	Adrians-XN8	10.100.47.12	Behind the hot water pipes, 3rd washroom on left	XS-4.0.8-1201
ARP Table	XN0820091C8A6	10.100.46.151		XS-4.0.7-1195
DHCP Leases	XN0823091CACD	10.100.46.66		XS-4.0.7-1192
Connection Tracking	XN0803091BF2E	10.100.46.152		XS-4.0.7-1192
CDP Neighbors	Sheyda-XN8	10.100.47.38		XS-4.0.7-1192
Network Assurance	Sams-X-N4	10.100.46.31		XS-4.0.7-1192
RF Monitor	Bruces-XN8-Array	10.100.47.10	Desk	XS-4.0.7-1192
Stations	Jose-XS16	10.100.46.223		XS-3.5-0724
Statistics	Bruces-XS3900-Array	10.100.47.13	Office	XS-3.5-0724
	adrians-3900	10.100.47.11		XS-3.5-0724

Figure 50. Network Map

The Network Map has a number of options at the top 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 139](#). You may click the host name to access WMI for this Array.
- **IP Address:** The Array’s IP address. You may click the address to access WMI for this Array. 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 139](#).

- **Location:** The location assigned to the Array. To establish the location information, go to [“Express Setup” on page 139](#).
- **Array OS:** The software version running on the Array.
- **IAP:** The number of IAPs on the Array.
- **(IAP) Up:** Informs you how many IAPs are currently up and running. To enable or disable all IAPs, go to [“Express Setup” on page 139](#). To enable or disable individual IAPs, go to [“IAP Settings” on page 237](#).
- **SSID:** Informs you how many SSIDs have been assigned for the Array. To assign an SSID, go to [“SSID Management” on page 213](#).
- **(SSID) On:** Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to [“SSID Management” on page 213](#).
- **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 243](#).
- **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, XS4, etc.), plus the amount of RAM memory and the speed of the processor.
- **Serial:** Displays the serial number of each Array.

#### *License*

- **License:** 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 112](#).

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.

	VLAN Name	Number	Gigabit 1	Gigabit 2	WDS Client Links				WDS Host Links					
					1	2	3	4	1	2	3	4		
Spanning Tree Status	none	0	forwarding	forwarding										

Figure 51. 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.

The screenshot shows the XN16 Wi-Fi Array interface. At the top, it displays the name 'BrianXN16 (10.100.47.33)' and the uptime '0 days, 0 hours, 31 mins'. Below this is a navigation menu with 'Array' and 'Network' options. The 'Network' section is expanded to show a table with the following data:

Destination	Mask	Gateway	Interface
255.255.255.255	255.255.255.255	0.0.0.0	eth0
10.100.47.0	255.255.255.0	0.0.0.0	gig1/2
10.0.1.0	255.255.255.0	0.0.0.0	eth0
0.0.0.0	0.0.0.0	10.100.47.1	gig1/2

Figure 52. 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.

The screenshot shows the XN16 Wi-Fi Array interface. At the top, it displays the name 'BrianXN16 (10.100.47.33)' and the uptime '0 days, 0 hours, 32 mins'. Below this is a navigation menu with 'Array' and 'Network' options. The 'Network' section is expanded to show a table with the following data:

IP Address	MAC Address	Interface
10.100.47.13	00:0F:7D:00:43:0A	gig1/2
10.100.47.1	00:10:DB:FF:20:A0	gig1/2
10.100.47.38	00:0F:7D:01:1C:1F	gig1/2
10.100.47.10	00:0F:7D:00:45:F1	gig1/2
10.100.47.16	00:0F:7D:00:B8:0D	gig1/2

Figure 53. 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.

IP Address	MAC Address	Start Time	End Time	Time Left	Host Name
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 54. 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.

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		
udp		10.100.47.10	255.255.255.255	39127	22610	1	220	Unreplied	255.255.255.255	10.100.47.10	22610	39127	0	0	1		
udp		10.100.47.16	10.100.40.137	60161	22610	1	214	Unreplied	10.100.40.137	10.100.47.16	22610	60161	0	0	1		
udp		10.100.47.16	10.100.47.33	15004	15003	995	87688	Assured	10.100.47.33	10.100.47.16	15003	15004	995	87688	1		
udp		10.100.46.16	10.100.47.16	41319	161	211873	74205993	Assured	10.100.47.16	10.100.46.16	161	41319	211873	87025111	1		
udp		10.100.47.16	10.110.37.8	60161	22610	1	214	Unreplied	10.110.37.8	10.100.47.16	22610	60161	0	0	1		
udp		10.100.47.16	10.100.1.13	48391	162	1	229	Unreplied	10.100.1.13	10.100.47.16	162	48391	0	0	1		
udp		10.100.47.16	255.255.255.255	60161	22610	1	214	Unreplied	255.255.255.255	10.100.47.16	22610	60161	0	0	1		

Figure 55. 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).

Status		Name: SS.XN0429091D207 ( 10.100.47.16 )						Uptime: 0 days, 23 hours, 51 mins	
<ul style="list-style-type: none"> <li>▸ Array</li> <li>▾ Network                             <ul style="list-style-type: none"> <li>Network Map</li> <li>Spanning Tree Status</li> <li>Routing Table</li> <li>ARP Table</li> <li>DHCP Leases</li> <li>Connection Tracking</li> <li>CDP Neighbors</li> <li>Network Assurance</li> </ul> </li> <li>▸ RF Monitor</li> <li>▸ Stations</li> <li>▸ Statistics</li> <li>System Log</li> </ul>		<input type="checkbox"/> Auto Refresh <input type="button" value="Refresh"/>							
Hostname	IP Address	Model	Interface	Native VLAN	Capabilities	Software			
Adrians-XN8	10.100.47.12	Xirrus XN8, 1.0GB-ECC (1.0GHz)	Gig1/2	none	L2SW (switch)	Xirrus ArrayOS Version 4.0.8 (Feb 17 2010), Build: 1201			
BrianXN16	10.100.47.33	Xirrus XN16, 1.0GB-ECC (1.0GHz)	Gig1/2	none	L2SW (switch)	Xirrus ArrayOS Version 4.1.0 (Mar 24 2010), Build: 1269			
Bruces-XN8-Array	10.100.47.10	Xirrus XN8, 1.0GB-ECC (1.0GHz)	Gig1/2	none	L2SW (switch)	Xirrus ArrayOS Version 4.0.7 (Dec 31 2009), Build: 1192			
Bruces-XS3900-Array	10.100.47.13	Xirrus XS-3900, 512MB (825MHz)	Gig1/2	none	L2SW (switch)	Xirrus ArrayOS Version 3.5 (May 20 2009), Build: 0724			
SS-XN0429091D207	10.100.47.16	Xirrus XN4, 512MB-ECC (825MHz)	Gig1	none	L2SW (switch)	Xirrus ArrayOS Version 4.1.0 (Mar 24 2010), Build: 1269			
Sheyda-XN8	10.100.47.38	Xirrus XN8, 1.0GB-ECC (1.0GHz)	Gig1/2	none	L2SW (switch)	Xirrus ArrayOS Version 4.0.7 (Dec 31 2009), Build: 1192			
adrians-3900	10.100.47.11	Xirrus XS-3900, 512MB (825MHz)	Gig1/2	none	L2SW (switch)	Xirrus ArrayOS Version 3.5 (May 20 2009), Build: 0724			

Figure 56. CDP Neighbors

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.).

CDP must be enabled on the Array in order to gather and display this information. See “CDP Settings” on page 154.



## Network Assurance

This status-only window shows the results of ongoing network assurance testing.

Status		Name: BrianXN16 ( 10.100.47.33 )		Uptime: 0 days, 0 hours, 29 mins	
▾ Array					
▾ Network	<input type="checkbox"/> Auto Refresh <input type="button" value="Refresh"/>				
Network Map	<b>Setting</b>	<b>Hostname</b>	<b>IP Address</b>	<b>Status</b>	
Spanning Tree Status	DNS server 1		10.100.1.10	Connectivity OK	
Routing Table	DNS server 2		10.100.2.10	Connectivity OK	
ARP Table	NTP primary server	ntp.xirrus.com	72.18.205.156	Connectivity OK	
DHCP Leases	SNMP trap host 1	Xirrus-XMS	10.100.1.13	Connectivity OK	
Connection Tracking	gig1 IP gateway		10.100.47.1	Connectivity OK	
CDP Neighbors	gig2 IP gateway		10.100.47.1	Connectivity OK	
Network Assurance					

Figure 57. Network Assurance

The Array checks connectivity to network servers that you have configured (for example, DNS and NTP servers) on an ongoing basis. For each server, this list shows the server’s host name (if any), IP address, and status.

Network assurance must be enabled on the Array in order to perform these connectivity tests and display this information. See [“Management Control” on page 188](#).

*See Also*

[Management Control](#)

## 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 assigned threat-sensor (monitor) radio. 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.
- **Channel History**—charts ongoing statistics and RF measurements for one selected channel over time.



*Some status information is only available if the Array’s license includes **Advanced Feature Sets**. For example, the Spectrum Analyzer requires the **Xirrus Advanced RF Analysis Manager (RAM)**. If a feature is unavailable, then your license does not support the feature and you will get an error message if you try to set the feature. See “**About Licensing and Upgrades**” on page 297.*

### 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. To graph these values over time for a particular channel, see “Channel History” on page 109. For detailed information on the measurements displayed, please see “Spectrum Analyzer Measurements” on page 106.

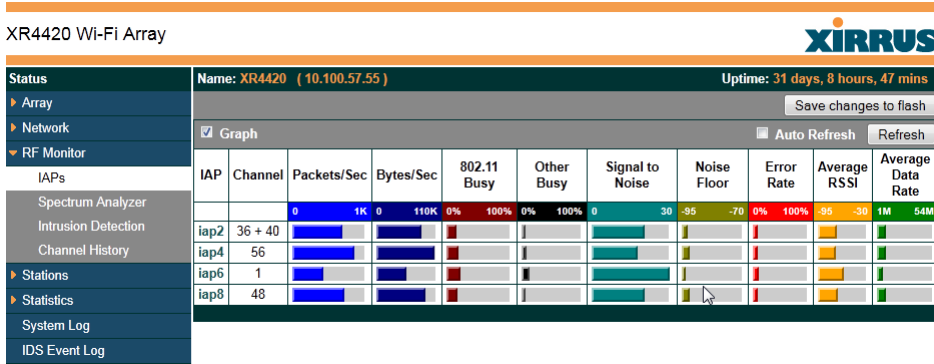


Figure 58. RF Monitor—IAPs

Figure 58 presents the data as a graphical display, enabled by selecting the **Graph** checkbox on the upper left. If this option is not selected, data is presented as a numerical table.

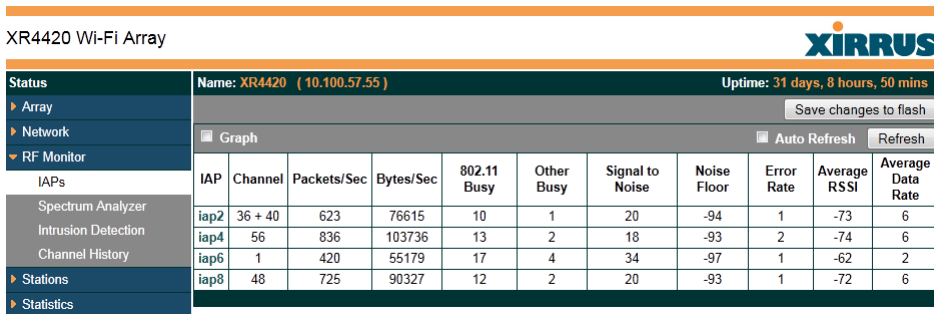



Figure 59. RF Monitor—IAPs

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 the monitor radio. You **must** have a radio set to **monitor** mode for any data to be available. See “IAP Settings” on page 237.*

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 monitor 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 monitor 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 60](#) (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in “[Spectrum Analyzer Measurements](#)” on page 106.

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.

Select Display Options      Click Channel number to highlight

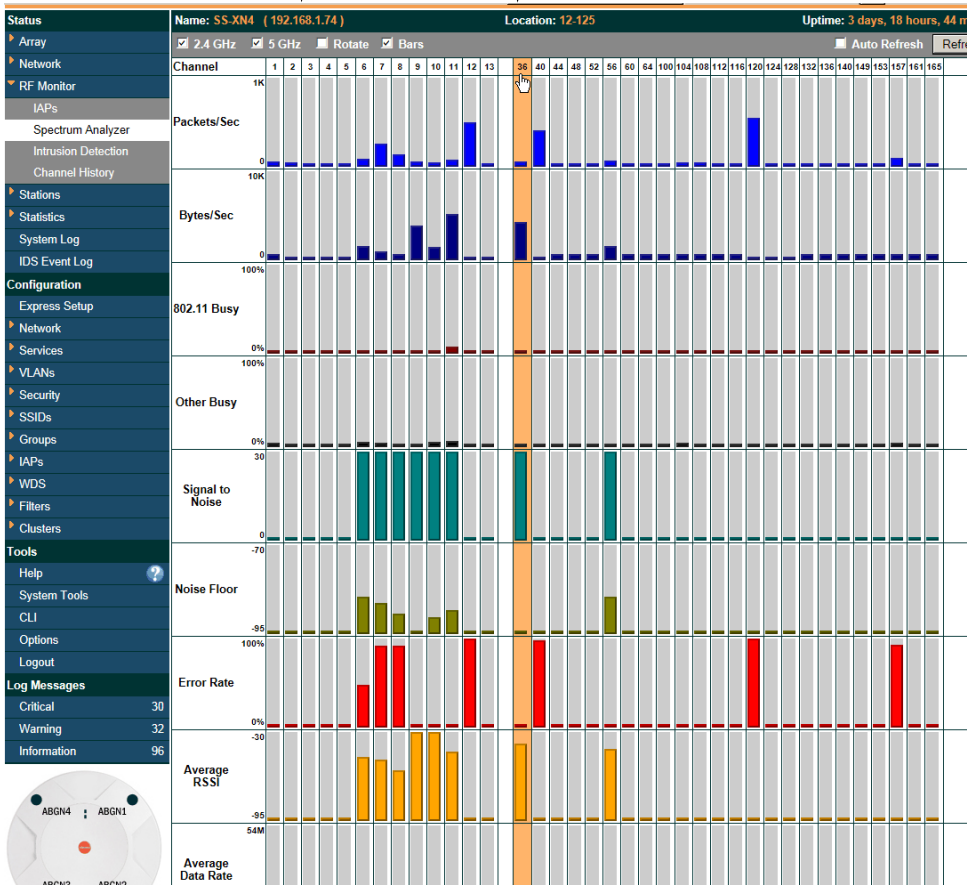



Figure 60. RF Spectrum Analyzer

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 (the default is both). 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 classifications you select from the checkboxes at the top—**Blocked**, **Unknown**, **Known**, or **Approved**. This includes ad hoc access points (station-to-station connections). For more information about intrusion detection, rogue APs, and blocking, please see “About Blocking Rogue APs” on page 273.

Classify APs 
Select APs to Display

Name: SS-XM4 ( 192.168.1.74 ) Location: 12-125 Uptime: 3 days, 19 hours, 43 mins										
<input type="checkbox"/> Select All <input type="checkbox"/> Approve <input type="checkbox"/> Set Known <input type="checkbox"/> Block <input type="checkbox"/> Set Unknown <input type="checkbox"/> Approved ( 0 ) <input type="checkbox"/> Known ( 0 ) <input type="checkbox"/> Blocked ( 0 ) <input checked="" type="checkbox"/> Unknown ( 12 ) <input type="checkbox"/> Auto Refresh <input type="button" value="Refresh"/>										
Select	BSSID	SSID	Manufacturer	Channel	RSSI	Security	Type	Status	Discovered	Last Active
<input type="checkbox"/>	00:13:10:23:53:84	MTSetup	Cisco-Linksys	6	-58	none	ESS	unknown	Jul-11 09:03	active
<input type="checkbox"/>	00:14:bf:de:3d:35	linksys	Cisco-Linksys	6	-67	none	ESS	unknown	Jul-11 09:22	Jul-11 09:30
<input type="checkbox"/>	00:1d:0f:d8:91:98	rascarcapac	TP-LINK	6	-61	WEP	ESS	unknown	Jul-11 09:03	active
<input type="checkbox"/>	00:1e:e5:90:79:28	linksys	Cisco-Linksys	6	-62	TKIP+PSK	ESS	unknown	Jul-11 09:04	active
<input type="checkbox"/>	00:22:a4:5c:e6:a9	2WIRE267	2wire	6	-48	WEP	ESS	unknown	Jul-11 09:03	active
<input type="checkbox"/>	34:ef:44:f2:97:9e	SINGTEL-0244	2wire	11	-24	AES+TKIP+PSK	ESS	unknown	Jul-11 09:03	active
<input type="checkbox"/>	64:b9:e8:4e:ad:a7	Free Public WiFi	Apple	1	-69	none	IBSS	unknown	Jul-11 09:20	Jul-11 09:20
<input type="checkbox"/>	74:ea:3a:ee:b9:b0	JustAnthony	TP-LINK	11	-57	AES+TKIP+PSK	ESS	unknown	Jul-11 09:03	active
<input type="checkbox"/>	90:84:0d:9c:1b:2b	Free Public WiFi	Apple	1	-72	none	IBSS	unknown	Jul-11 09:47	Jul-11 09:47
<input type="checkbox"/>	98:2c:be:11:51:7e	SINGTEL-2022	2wire	1	-72	AES+TKIP+PSK	ESS	unknown	Jul-11 09:04	active
<input type="checkbox"/>	98:2c:be:15:b3:2a	SINGTEL-8989	2wire	9	-73	AES+TKIP+PSK	ESS	unknown	Jul-11 09:04	active
<input type="checkbox"/>	cc:08:e0:da:e5:db	Free Public WiFi	Apple	1	-65	none	IBSS	unknown	Jul-11 09:13	Jul-11 09:13

Figure 61. Intrusion Detection/Rogue AP List

The Intrusion Detection window provides the easiest method for classifying rogue APs as Blocked, Known, Approved, or Unknown. Choose one or more APs using the checkbox in the **Select** column, then use the buttons on the upper left to classify them with the following actions: **Approve**, **Set Known**, **Block**, or **Set Unknown**.

You can sort the results based on the following parameters by clicking the desired column header:

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

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](#)



### Channel History

The RF Monitor—Channel History window focuses on traffic statistics and RF readings observed for just one channel that you select in the **Channel** field. A new set of readings is added every 10 seconds for a 5 GHz channel, or every 5 seconds for a 2.4 GHz channel. For descriptions of the measurements displayed, please see “Spectrum Analyzer Measurements” on page 106.

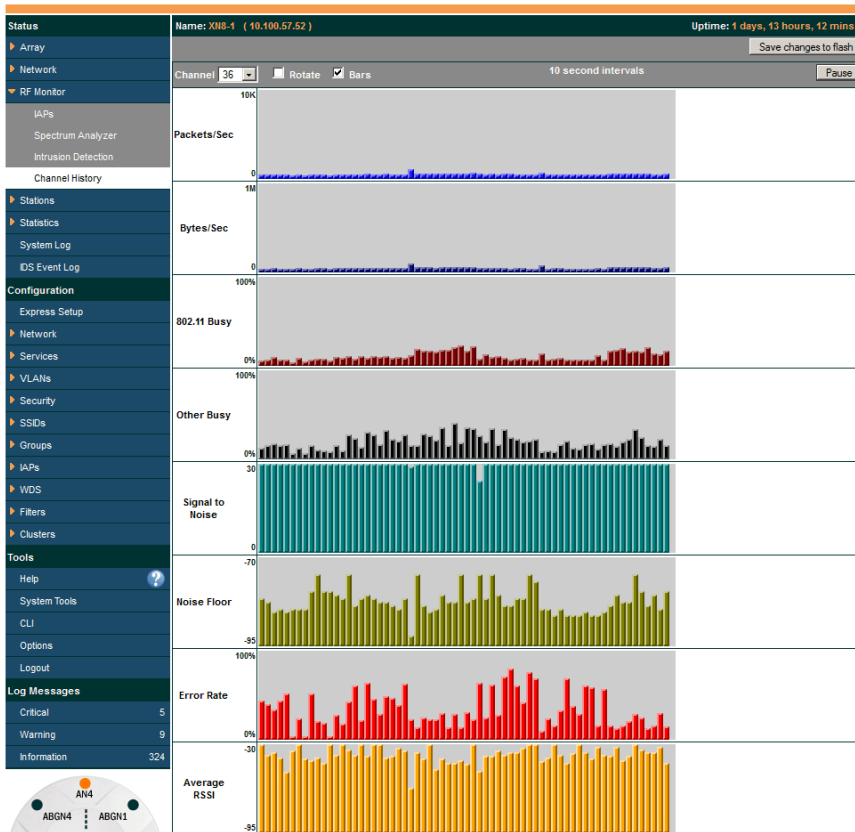


Figure 62. RF Monitor—Channel History

Figure 62 presents the data in graphical form. New data appears at the left, with older readings shifting to the right. To make the data appear as a barchart, click the **Bar** checkbox which will shade the background.

You also have the option of clicking the **Rotate** checkbox to give each statistic its own column. In other words, the graph for each statistic will grow down the page as new readings display at the top. (Figure 63)

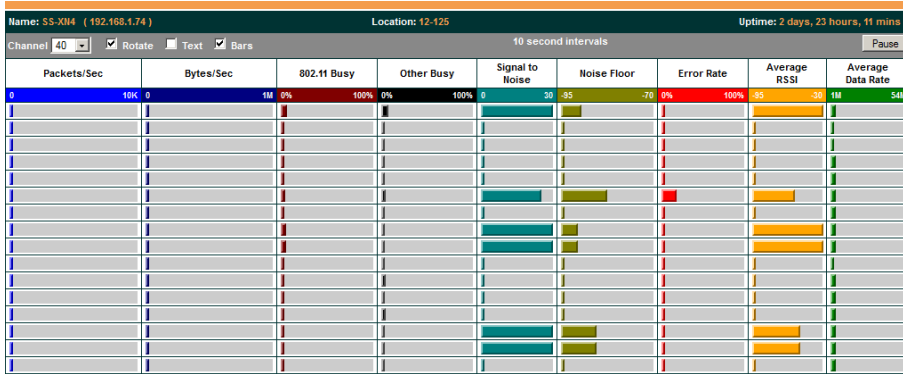


Figure 63. RF Monitor—Channel History (Rotated)

If you select **Rotate** and **Text** together, data is presented as a numerical table. (Figure 64)

Click **Pause** to stop collecting data, or **Resume** to continue.

Name: SS-X14 ( 192.168.1.74 )		Location: 12-125		Uptime: 2 days, 23 hours, 22 mins					
Channel: 40		<input checked="" type="checkbox"/> Rotate <input checked="" type="checkbox"/> Text <input type="checkbox"/> Bars		10 second intervals					Resume
Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate	
0	0	0	0	96	38	0	64	2	
0	0	0	0	96	19	0	52	2	
0	0	0	0	96	19	0	52	2	
0	0	2	0	96	15	0	96	2	
0	0	1	2	67	19	0	38	2	
0	0	0	0	96	23	0	56	2	
0	0	0	0	0	0	0	0	2	
0	0	0	0	96	38	0	68	2	
0	0	0	0	96	38	0	68	2	

Figure 64. RF Monitor—Channel History (Text)

## 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.
- **Station Assurance**— displays stations that are having connectivity problems.



*Some status information is only available if the Array’s license includes the Xirrus Advanced RF Analysis Manager (RAM). If a feature is unavailable, then your license does not support the feature and you will get an error message if you try to set the feature. See “About Licensing and Upgrades” on page 297.*

## 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 **Unassociated**, or both, by selecting the appropriate checkboxes above the list. The list always shows the MAC address of each station, its IP address, 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 other checkboxes above the list to show a number of additional columns:

- **Identification:** shows more identifying information for the station—its **User Name**, **Host Name**, **Manufacturer**, **Device Type**, and **Device Class** (for example, notebook, iPad, etc.).
- **Security:** includes security settings used by the connection—**Enc(ryption)** type, **Cipher** used, **Key Mgmt** used, and **Media** supported by the station.
- **Connection Info:** shows the **Band** (5GHz or 2.4 GHz) and **Channel(s)** used (plus bonded channel, if any, for 802.11n). Shows additional RF measurements that affect the quality of the connection: **SNR** (signal to noise ratio) and **Silence**—the ambient noise (floor) value.

Select	MAC Address	IP Address	User Name	Hostname	Manufacturer	Device Type	Device Class	SSID	Group	VLAN	QoS	IAP	TX Rate	RX Rate	RSSI	Time D:H:M
<input type="checkbox"/>	88:53:2e:0c:e7:16	192.168.1.129		Farkle	Intel	Windows	Notebook	xirus42		2		abgn3	300.0Mbps	300.0Mbps	-43	2:23:38

Figure 65. 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 195 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. The location of each station is computed based on the [RSSI](#) of its signal as received by the Array. The distance is adjusted based on the environment setting that you selected. You may display just the stations associated to this Array, unassociated stations (shown in gray), or both. The station count is shown on the right, above the map. You may also choose to display only 5 GHz stations (shown in orange) or 2.4 GHz stations (shown in green), or both.

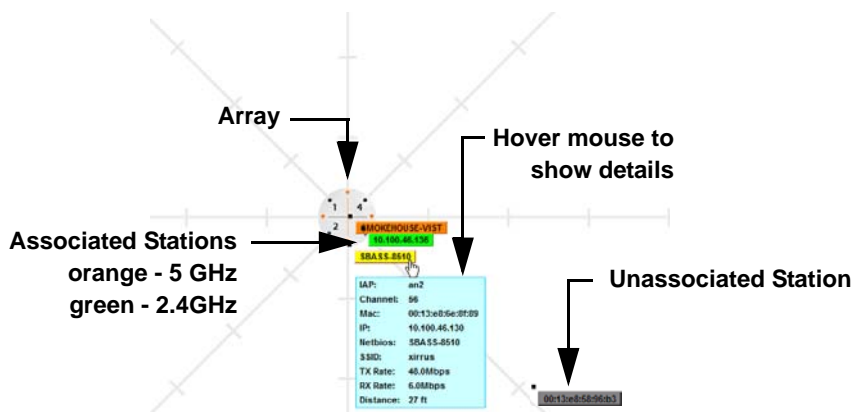


Figure 66. Location Map

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 are a mirror image of the way they are typically drawn when looking at the face of the Array. Radios are marked on the map to show the orientation of the Array.

A station is identified by the type of **Preferred Label** that you select: **Netbios Name**, **IP Address**, **MAC Address**, or **Manufacturer**. 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. 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—see [“Working with the Custom Image”](#) on page 117

Hover the mouse over a station to show detailed information. (Figure 66) For a station that is associated to this Array, the details include:

- The **IAP**, **Channel**, and **SSID** to which the station is associated.
- The **MAC** and **IP** address and **Netbios** name of the station.
- The **TX Rate** and **RX Rate** of this connection.
- The approximate **Distance** of this station from the Array. The distance is estimated using the received signal strength and your environment setting. The environment determines the typical signal attenuation due to walls and other construction that affect signal reception.

### Controls and items displayed on the Location Map window



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.

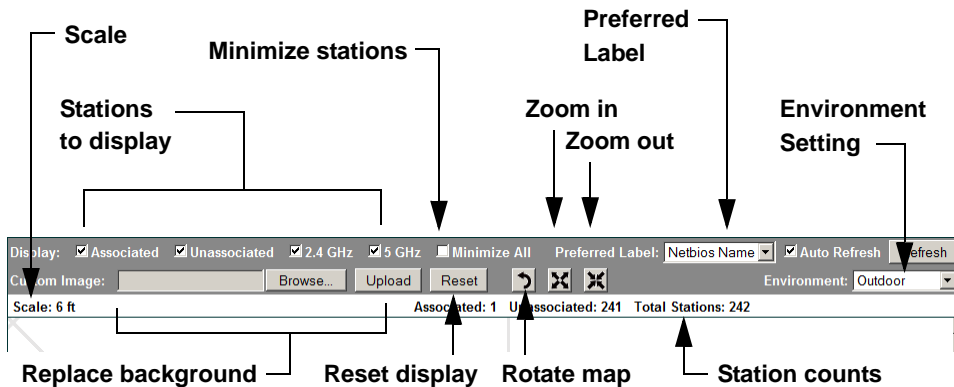


Figure 67. Controls for Location Map

- **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 802.11b(g)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. (Figure 68) You may still display detailed information for the station by hovering over it. To enlarge all rectangles, clear the Minimize All checkbox.
- **Preferred Label:** This field is located on the top of the window towards the right. It selects the type of label to be displayed for stations: **Netbios Name**, **IP Address**, **MAC Address**, or **Manufacturer**. If you select NetBIOS (this is the default), then that name, if known, will be used to label each Array. Else, its IP or MAC address will be used, in that order.
- **Auto Refresh:** Instructs the Array to refresh this window automatically.
- **Refresh:** Updates the stations displayed.

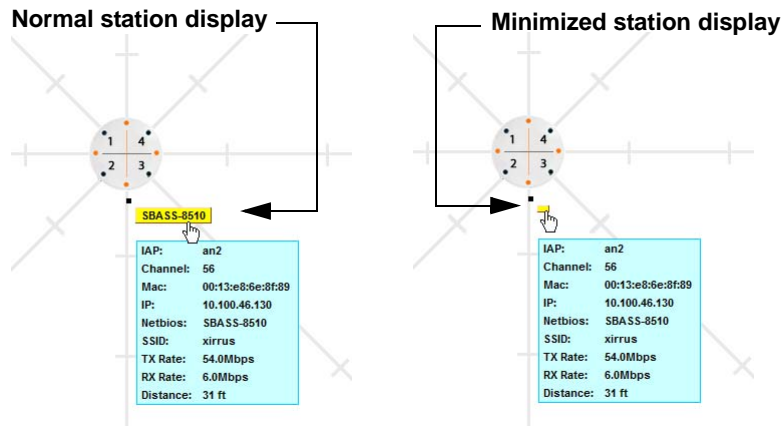





Figure 68. Minimizing stations

- **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 117.
- **Upload:** After browsing to the desired custom image, click the **Upload** button to install it. The map is redisplayed with your new background. No hash marks (for the map scale) 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** is updated with the new scale for the map.
-  **Reduce:** Click this button to reduce (zoom out on) the map. The displayed **Scale** is updated with the new scale for the map.



- **Environment:** This field is located on the top right of the window. Select the type of environment for this Array's deployment: **Outdoor**, **Indoor open** (few walls or obstructions), **Indoor walled** (typical wall or cubicle construction), or **Indoor dense** (many walls or obstructions, or unusually dense walls).
- **Scale:** This view-only value shows the approximate distance represented by each hashmark on the default map background.
- **Associated, Unassociated, Total Stations:** These view-only values show the station counts observed by the Array.

### *See Also*

#### 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 115), you should move the display of the Array on your map to correspond with its actual location at your site.

To move the Array on the map, simply click it, then drag and drop it to the desired location. The Array will continue to follow the mouse pointer to allow you to make further changes to its location. When you are satisfied with its location, click the Array again to return to normal operation.

## 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.

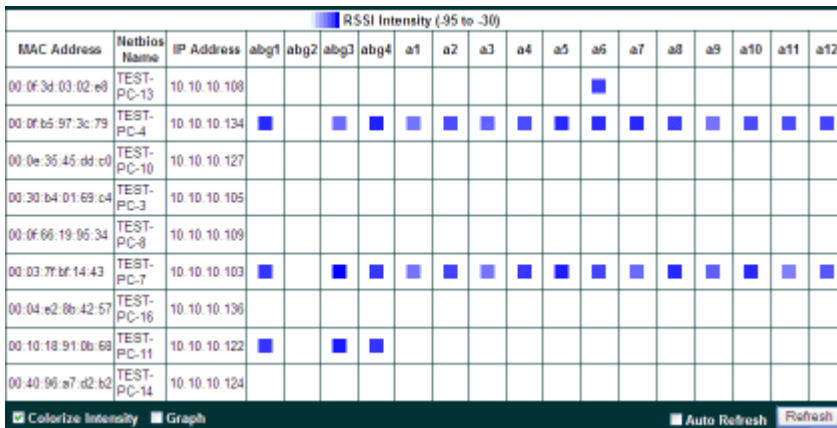


Figure 69. Station RSSI Values

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 69) If you select **Graph**, then the RSSI is shown on a representation of the Array, either colorized or numerically based on your selection. (Figure 70) The stations are listed to the left of the Array—click on a station to show its RSSI values on the Array.

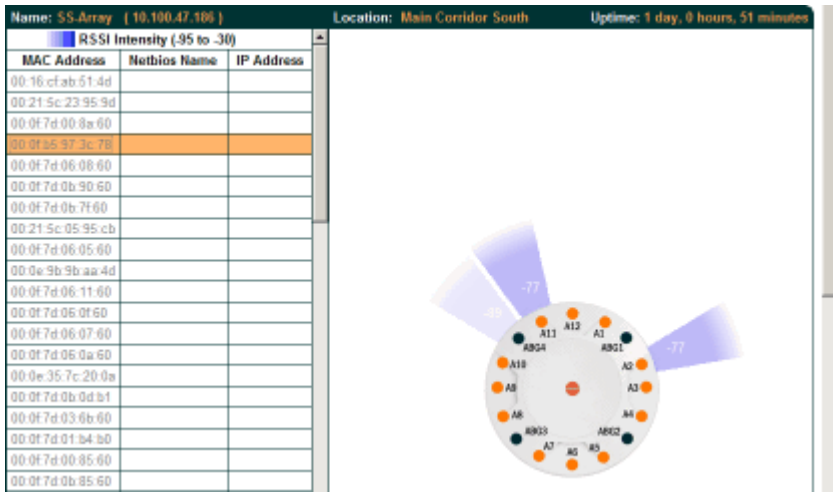


Figure 70. Station RSSI Values—Colorized Graphical View

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.

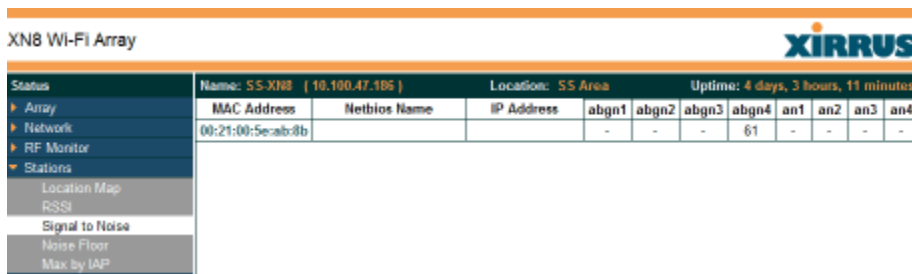
*See Also*

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.



Name: SS-XN8 ( 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:ab:8b			-	-	-	61	-	-	-	-	

Figure 71. 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 71) You may display the relative value using color if you select **Colorize Intensity**, with the highest SNR indicated by the most intense color. (Figure 72) If you select **Graph**, then the SNR is shown on a representation of the Array, either colorized 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.

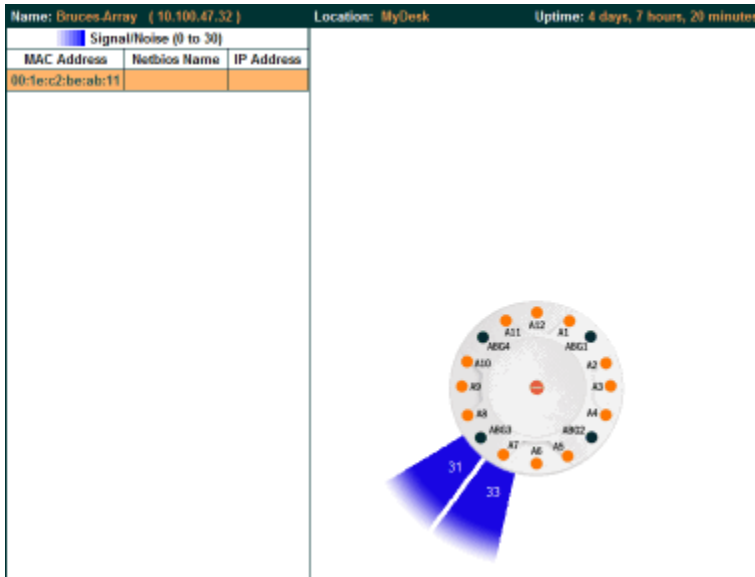


Figure 72. Station SNR Values—Colorized Graphical View

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.

XN8 Wi-Fi Array		XIRRUS									
Status		Name: SS-XN8 ( 10.100.47.185 )			Location: SS Area				Uptime: 4 days, 3 hours, 22 minutes		
Array	MAC Address	Netbios Name	IP Address	abgn1	abgn2	abgn3	abgn4	an1	an2	an3	an4
Network	00:21:00:5e:ac:8b			-96	-	-	-96	-	-	-	-
RF Monitor											
Stations											
Location Map											
RSSI											
Signal to Noise											
Noise Floor											
Max by IAP											

Figure 73. 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 73) 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 colorized or numerically based on your selection.(Figure 74) The stations are listed to the left of the Array—click on a station to show its values on the Array.

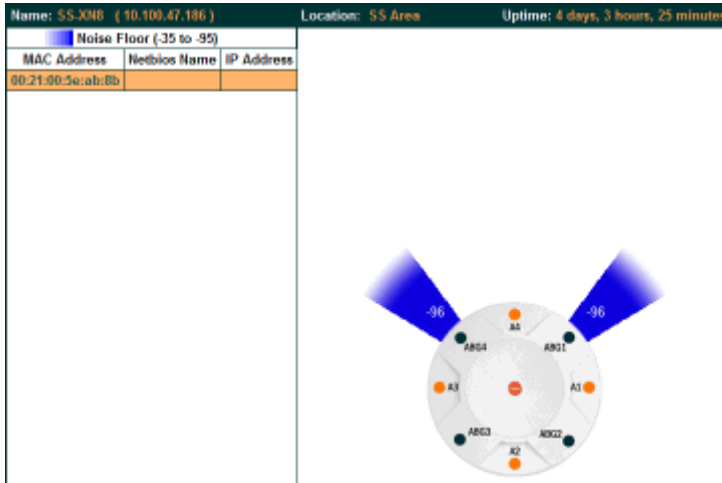


Figure 74. Station Noise Floor Values—Colorized Graphical View

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.

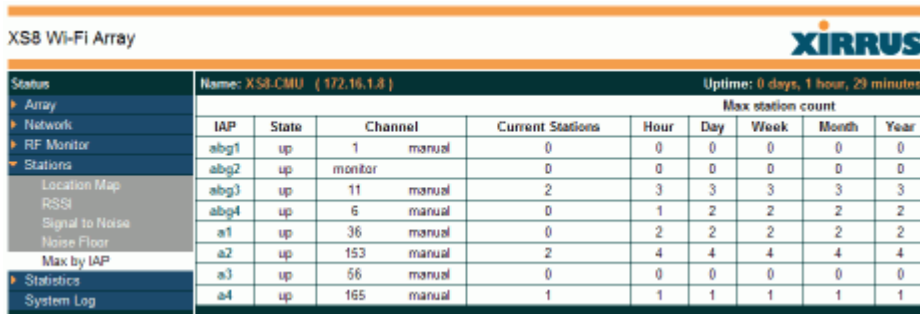
*See Also*

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: XSB.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 75. 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](#)



### Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the Wi-Fi network. This window shows client stations that have had connectivity issues. You may enable or disable the station assurance feature and set thresholds for the problems that it checks, such as excessive packet retry or packet error rates, or stations that are unable to stay associated to the Array. Please see [“Station Assurance” on page 267](#) for more information about these settings. When the Array detects that a station has reached the threshold value for one or more of the issues checked, it adds the station to this page. In addition, an event is triggered, a trap is generated, and a Syslog message is logged.

For each station, this list shows the MAC address, its IP address, its host name, its device type, device class, and manufacturer. It also shows the values of the various statistics that were monitored for problems as described in [“Station Assurance” on page 267](#): associated time, authentication failures, packet error rate, packet retry rate, packet data rate, RSSI, signal to noise ratio (SNR), and distance.

Time	MAC Address	IP Address	Hostname	Device Type	Device Class	Manufacturer	Assoc Time	Auth Fails	Error Rate	Retry Rate	Data Rate	RSSI (dB)	SNR (dB)	Di
Jul-09 05:14	e8:06:88:9a:35:7e	192.168.1.130		iPad	Tablet	Apple					6			

Figure 76. Station Assurance

You may click the **Clear Inactive** button to remove stations that are no longer connected to the Array from the list. Click the **Clear All** button to remove all entries and start fresh to add problem stations to the list as they are detected. 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

Station Assurance

## 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 127. 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 **XIRRUS**

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

IAP: an5

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	178545569	6479993	17015352	0		
abgn2	monitor	5514057421	110730414	2084140	46805	52598282	0	31687	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	2809	113	1494	722957	2259	0	0		

Unicast Stats Only  Auto Refresh

Figure 77. 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 126. 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 79.

Name: SS-X188 [ 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	7225222		
Beacons	94791259	Beacons	6976563		
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		

Display Percentages
  Auto Refresh

Figure 78. Individual IAP Statistics Page

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

Stations	Gigabit 1 Statistics		enabled, link up, 1000Mbps, full duplex	
System Log	Receive Bytes	246021597	Transmit Bytes	202395623
Configuration	Receive Packets	1745005	Transmit Packets	859020
Express Setup	Receive Compressed	0	Transmit Compressed	0
Network	Receive Multicast	0	Transmit Carrier Errors	0
Services	Receive Dropped	0	Transmit Dropped	0
VLANs	Receive FIFO Errors	0	Transmit FIFO Errors	0
Security	Receive Frame Errors	0	Transmit Collisions	0
SSIDs	Receive Total Errors	0	Transmit Total Errors	0
Groups	Gigabit 2 Statistics		enabled, link down, 1000Mbps, half duplex	
IAPs	Receive Bytes	0	Transmit Bytes	0
WDS	Receive Packets	0	Transmit Packets	0
Filters	Receive Compressed	0	Transmit Compressed	0
Tools	Receive Multicast	0	Transmit Carrier Errors	0
System Tools	Receive Dropped	0	Transmit Dropped	0
CUJ	Receive FIFO Errors	0	Transmit FIFO Errors	0
Logout	Receive Frame Errors	0	Transmit Collisions	0
Log Messages	Receive Total Errors	0	Transmit Total Errors	0
Critical 0	<input type="checkbox"/> Auto Refresh <input type="button" value="Refresh"/> <input type="button" value="Clear"/>			
Warning 1				

Figure 79. 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.

Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 4 days, 3 hours, 59 minutes
Array	VoIP (12) Statistics <span>Clear</span>		
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	Finance (5) Statistics <span>Clear</span>		
Stations	Receive Bytes	0	Transmit Bytes 3313440
System Log	Receive Packets	0	Transmit Packets 5616
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	<span>Clear All</span> <span>Auto Refresh</span> <span>Refresh</span>		
Groups			
IAPs			

Figure 80. VLAN Statistics

*See Also*

VLAN Management  
VLANs