



## Wi-Fi Arrays

January 7, 2010





# Wi-Fi Array™

XN16, XN12, XN8, XN4

XS16, XS8, XS4

XS-3900, XS-3700, XS-3500

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: 800-0006-001**  
(Revision Y)



## 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>xiii</b>
<b>Introduction .....</b>	<b>1</b>
The Xirrus Family of Products .....	2
Nomenclature .....	4
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 .....	7
Window or Page? .....	7
Why Choose the Xirrus Wi-Fi Array? .....	7
Wi-Fi Array Product Overview .....	9
Enterprise Class Security .....	9
Wi-Fi Array Product Family .....	10
XN Family of Arrays .....	10
XS Family of Arrays .....	11
Deployment Flexibility .....	12
Power over Gigabit Ethernet (PoGE) .....	13
Enterprise Class Management .....	14
Key Features and Benefits .....	16
High Capacity and High Performance .....	16
Extended Coverage .....	17
Flexible Coverage Schemes .....	18
Non-Overlapping Channels .....	18
Secure Wireless Access .....	19
Applications Enablement .....	19
SDMA Optimization .....	19
Fast Roaming .....	19
Easy Deployment .....	19
Product Specifications—XN16, XN12, and XN8 .....	20
Product Specifications—XN4 .....	27

---

Product Specifications—XS16/XS-3900, and XS8/XS-3700 .....	34
Product Specifications—XS4/XS-3500 .....	39
<b>Installing the Wi-Fi Array .....</b>	<b>45</b>
Installation Prerequisites .....	45
Optional Network Components .....	47
Client Requirements .....	47
Planning Your Installation .....	48
General Deployment Considerations .....	48
Coverage and Capacity Planning .....	50
Placement .....	50
RF Patterns .....	51
Capacity and Cell Sizes .....	52
Fine Tuning Cell Sizes .....	53
Roaming Considerations .....	54
Allocating Channels .....	54
Deployment Examples .....	57
IEEE 802.11n Deployment Considerations .....	59
MIMO (Multiple-In Multiple-Out) .....	60
Multiple Data Streams—Spatial Multiplexing .....	62
Channel Bonding .....	63
Improved MAC Throughput .....	64
Short Guard Interval .....	64
Obtaining Higher Data Rates .....	65
802.11n Capacity .....	66
Failover Planning .....	67
Port Failover Protection .....	67
Switch Failover Protection .....	68
Power Planning .....	69
AC Power .....	69
Power over Gigabit Ethernet .....	69
Security Planning .....	70
Wireless Encryption .....	70
Authentication .....	70
Meeting PCI DSS Standards .....	71
Meeting FIPS Standards .....	71

---

Port Requirements .....	72
Network Management Planning .....	75
WDS Planning .....	76
Common Deployment Options .....	79
Installation Workflow .....	80
Unpacking the Wi-Fi Array .....	81
Installing Your Wi-Fi Array .....	83
Choosing a Location .....	83
Wiring Considerations .....	84
Mounting the Array on a Ceiling .....	86
Attaching the T-Bar Clips to the Template .....	86
Secure the T-Bar Clips to the Ceiling Support Grid .....	87
Installing the Mounting Plate .....	88
Connecting the Cables—AC Option .....	89
Connecting the Cables—PoGE Option .....	90
Attaching the Array to the Mounting Plate .....	92
Securing the Array .....	94
Dismounting the Array .....	95
Mounting Array on a Wall (All models except 4-port Arrays) .....	96
Kit Contents (Wall Mount Assembly) .....	96
Tools Required .....	96
Mark the Wall Position .....	97
Install the SNAPTOGGLE™ Toggle Bolts .....	98
Attach the Mounting Plate to the Wall Mounting Bracket .....	99
Attach the Wall Mounting Bracket/Plate Assembly to the Wall .....	99
Mount the Array .....	100
Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500) .....	101
Kit Contents (Wall Mount Assembly) .....	101
Tools Required .....	101
Mark the Wall Position .....	102
Install the SNAPTOGGLE™ Toggle Bolts .....	102
Attach the Mounting Plate to the Wall Mounting Bracket .....	104
Attach the Wall Mounting Bracket/Plate Assembly to the Wall .....	105
Mount the Array .....	106
Removing the Array .....	107
Powering Up the Wi-Fi Array .....	107
Array LED Operating Sequences .....	108

---

LED Boot Sequence .....	108
LED Operation when Array is Running .....	109
Establishing Communication with the Array .....	110
Using the Serial Port .....	110
Using the Ethernet Ports .....	110
Logging In .....	111
Performing the Express Setup Procedure .....	112
Procedure for Performing an Express Setup .....	113
<b>The Web Management Interface .....</b>	<b>119</b>
An Overview .....	120
Structure of the WMI .....	121
User Interface .....	123
Utility Buttons .....	124
Logging In .....	126
Applying Configuration Changes .....	126
<b>Viewing Status on the Wi-Fi Array .....</b>	<b>127</b>
Array Status Windows .....	127
Array Summary .....	128
Content of the Array Summary Window .....	128
Array Information .....	131
Array Configuration .....	132
Admin History .....	133
Network Status Windows .....	133
Network Map .....	134
Content of the Network Map Window .....	134
Spanning Tree Status .....	137
Routing Table .....	138
ARP Table .....	138
DHCP Leases .....	139
Connection Tracking/NAT .....	140
CDP Neighbors .....	141
RF Monitor Windows .....	142
IAPs .....	143
Spectrum Analyzer .....	144
Intrusion Detection .....	148



---

Station Status Windows .....	150
Stations .....	151
Location Map .....	152
RSSI .....	157
Signal-to-Noise Ratio (SNR) .....	159
Noise Floor .....	161
Max by IAP .....	163
Statistics Windows .....	164
IAP Statistics Summary .....	164
Per-IAP Statistics .....	165
Network Statistics .....	167
VLAN Statistics .....	168
WDS Statistics .....	169
Filter Statistics .....	170
Station Statistics .....	170
Per-Station Statistics .....	171
System Log Window .....	172
<b>Configuring the Wi-Fi Array .....</b>	<b>173</b>
Express Setup .....	174
Network .....	180
Network Interfaces .....	181
Network Interface Ports .....	182
DNS Settings .....	188
CDP Settings .....	190
Services .....	192
Time Settings (NTP) .....	193
NetFlow .....	195
System Log .....	196
SNMP .....	199
DHCP Server .....	202
VLANs .....	204
Understanding Virtual Tunnels .....	204
VLAN Management .....	206
Security .....	208
Understanding Security .....	209
Certificates and Connecting Securely to the WMI .....	212

---

Using the Array's Default Certificate .....	212
Using an External Certificate Authority .....	213
Admin Management .....	214
Admin RADIUS .....	215
About Creating Admin Accounts on the RADIUS Server .....	215
Management Control .....	218
Access Control List .....	222
Global Settings .....	224
External Radius .....	227
Internal Radius .....	230
Rogue Control List .....	233
SSIDs .....	235
Understanding SSIDs .....	236
Understanding QoS Priority on the Wi-Fi Array .....	237
SSID Management .....	240
SSID List (top of page) .....	240
SSID Limits .....	244
Web Page Redirect Configuration Settings .....	245
Groups .....	248
Understanding Groups .....	248
Using Groups .....	249
Group Management .....	250
Group Limits .....	252
IAPs .....	254
Understanding Fast Roaming .....	255
IAP Settings .....	256
Global Settings (IAP) .....	261
Beacon Configuration .....	263
Station Management .....	263
Advanced Traffic Optimization .....	264
Global Settings .11a .....	268
Global Settings .11bg .....	270
Global Settings .11n .....	274
Advanced RF Settings .....	277
About Standby Mode .....	277
About Blocking Rogue APs .....	278
RF Intrusion Detection .....	279

RF Resilience .....	279
RF Power & Sensitivity .....	280
RF Spectrum Management .....	282
LED Settings .....	285
WDS .....	287
About Configuring WDS Links .....	287
WDS Client Links .....	289
Filters .....	291
Filter Lists .....	293
Filter Management .....	295
<b>Using Tools on the Wi-Fi Array .....</b>	<b>299</b>
System Tools .....	300
System .....	301
Automatic Updates from Remote Image or Configuration File ....	302
Configuration .....	303
Diagnostics .....	304
Web Page Redirect .....	306
Tools .....	307
Progress and Status Frames .....	309
CLI .....	310
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
contact-info .....	330
date-time .....	331
dhcp-server .....	332
dns .....	333
file .....	334
filter .....	337
fips .....	339
group .....	340
hostname .....	340
https .....	341
interface .....	342
license .....	343
load .....	343
location .....	344
management .....	344
more .....	344
netflow .....	345
no .....	346
pci-audit .....	348
quit .....	349
radius-server .....	349
reboot .....	350
reset .....	350
run-tests .....	351
security .....	353
snmp .....	354
ssh .....	354
ssid .....	356
standby .....	356
syslog .....	357
telnet .....	359
uptime .....	359
vlan .....	360
Sample Configuration Tasks .....	361
Configuring a Simple Open Global SSID .....	362
Configuring a Global SSID using WPA-PEAP .....	363

---

Configuring an SSID-Specific SSID using WPA-PEAP .....	364
Enabling Global IAPs .....	365
Disabling Global IAPs .....	366
Enabling a Specific IAP .....	367
Disabling a Specific IAP .....	368
Setting Cell Size Auto-Configuration for All IAPs .....	369
Setting the Cell Size for All IAPs .....	370
Setting the Cell Size for a Specific IAP .....	371
Configuring VLANs on an Open SSID .....	372
Configuring Radio Assurance Mode (Loopback Tests) .....	373
<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
Integrated Access Points (IAPs) .....	395
Server Settings .....	396
NTP .....	396
Syslog .....	396
SNMP .....	396
DHCP .....	397
Default SSID .....	397
Security .....	398
Global Settings - Encryption .....	398
External RADIUS (Global) .....	398

---

Internal RADIUS .....	399
Administrator Account and Password .....	400
Management .....	400
Keyboard Shortcuts .....	400
<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
Upgrading the Array via CLI .....	415
Sample Output for the Upgrade Procedure: .....	416
Power over Gigabit Ethernet Compatibility Matrix .....	420
Contact Information .....	422
<b>Appendix D: Implementing PCI DSS .....</b>	<b>423</b>
Payment Card Industry Data Security Standard Overview .....	423
PCI DSS and Wireless .....	424
The Xirrus Array PCI Compliance Configuration .....	425
The pci-audit Command .....	426
Additional Resources .....	427
<b>Appendix E: Implementing FIPS Security .....</b>	<b>429</b>
<b>Appendix F: Notices .....</b>	<b>437</b>
Notices .....	437
EU Directive 1999/5/EC Compliance Information .....	440
Safety Warnings .....	447
Translated Safety Warnings .....	448
Software Warranty and License Agreement .....	449
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.....	2
Figure 2.	The Xirrus Management System .....	3
Figure 3.	Wi-Fi Array (XN16) .....	9
Figure 4.	Wireless Coverage Patterns .....	12
Figure 5.	XP8 - Power over Ethernet Usage .....	13
Figure 6.	WMI: Array Status.....	14
Figure 7.	Layout of IAPs (XN16).....	16
Figure 8.	Naming of IAPs (XS16).....	17
Figure 9.	Coverage Schemes (XS16 shown).....	18
Figure 10.	Wall Thickness Considerations .....	49
Figure 11.	Unit Placement.....	50
Figure 12.	Full (Normal) Coverage.....	51
Figure 13.	Adjusting RF Patterns .....	51
Figure 14.	Custom Coverage .....	52
Figure 15.	Connection Rate vs. Distance.....	52
Figure 16.	Transmit Power.....	53
Figure 17.	Overlapping Cells.....	54
Figure 18.	Allocating Channels Manually .....	56
Figure 19.	Deployment Scenario (54 Mbps)—Per Sector .....	57
Figure 20.	Deployment Scenario (36 Mbps)—Per Sector .....	57
Figure 21.	Deployment Scenario (18 Mbps)—Per Sector .....	58
Figure 22.	Classic 802.11 Signal Transmission.....	60
Figure 23.	MIMO Signal Processing .....	61
Figure 24.	Spatial Multiplexing.....	62
Figure 25.	Channel Bonding .....	63
Figure 26.	MAC Throughput Improvements.....	64
Figure 27.	Computing 802.11n Data Rates .....	65
Figure 28.	802.11n Increases Capacity .....	66
Figure 29.	Port Failover Protection.....	67
Figure 30.	Switch Failover Protection .....	68
Figure 31.	Port Requirements for XMS .....	72
Figure 32.	WDS Link.....	76
Figure 33.	A Multiple Hop WDS Connection .....	77
Figure 34.	WDS Failover Protection .....	77

Figure 35.	Installation Workflow .....	80
Figure 36.	Array Placement .....	83
Figure 37.	Attaching the T-Bar Clips to the Template .....	86
Figure 38.	Attaching the T-Bar Clips to the Ceiling Grid.....	87
Figure 39.	Installing the Mounting Plate .....	88
Figure 40.	Connecting the Cables .....	89
Figure 41.	Connecting the Cables (Dual-PoGE connections shown).....	90
Figure 42.	Connecting the Cable (PoGE—XN4) .....	91
Figure 43.	Attaching the Unit (XN4 shown).....	92
Figure 44.	Attaching the Unit (XS-3900) .....	93
Figure 45.	Securing the Array.....	94
Figure 46.	IAP Positions (XS16 shown).....	95
Figure 47.	Wall Mount—Marking the Holes.....	97
Figure 48.	Installing the Toggle Bolts.....	98
Figure 49.	Attaching the Wall Mounting Plate .....	99
Figure 50.	Mounting the Array on a Wall .....	100
Figure 51.	Wall Mount—Marking the Holes.....	102
Figure 52.	Installing the Toggle Bolts.....	103
Figure 53.	Attaching the Array Mounting Plate .....	104
Figure 54.	Attaching the Wall Mounting Bracket to the Wall .....	105
Figure 55.	Mounting the Array on a Wall .....	106
Figure 56.	LED Locations (XS-3900) .....	107
Figure 57.	Network Interface Ports.....	110
Figure 58.	Express Setup .....	112
Figure 59.	LEDs are Switched On .....	117
Figure 60.	Web Management Interface .....	120
Figure 61.	WMI: Frames .....	123
Figure 62.	WMI: Utility Buttons.....	124
Figure 63.	Feedback Form.....	125
Figure 64.	Logging In to the Wi-Fi Array .....	126
Figure 65.	Array Summary .....	128
Figure 66.	Disabled IAP (Partial View).....	129
Figure 67.	IAP Cells .....	130
Figure 68.	Array Information .....	131
Figure 69.	Show Configuration .....	132
Figure 70.	Admin Login History.....	133
Figure 71.	Network Map .....	134

---

Figure 72.	Spanning Tree Status.....	137
Figure 73.	Routing Table.....	138
Figure 74.	ARP Table.....	138
Figure 75.	DHCP Leases.....	139
Figure 76.	Connection Tracking.....	140
Figure 77.	CDP Neighbors.....	141
Figure 78.	RF Monitor—IAPs.....	143
Figure 79.	RF Spectrum Analyzer.....	145
Figure 80.	Intrusion Detection/Rogue AP List.....	148
Figure 81.	Stations.....	151
Figure 82.	Location Map.....	152
Figure 83.	Controls for Location Map.....	153
Figure 84.	Minimizing stations.....	154
Figure 85.	Setting Array location on a Custom Image.....	156
Figure 86.	Station RSSI Values.....	157
Figure 87.	Station RSSI Values—Colorized Graphical View.....	158
Figure 88.	Station Signal-to-Noise Ratio Values.....	159
Figure 89.	Station SNR Values—Colorized Graphical View.....	160
Figure 90.	Station Noise Floor Values.....	161
Figure 91.	Station Noise Floor Values—Colorized Graphical View.....	162
Figure 92.	Max by IAP.....	163
Figure 93.	IAP Statistics Summary Page.....	165
Figure 94.	Individual IAP Statistics Page (for IAP abg(n)1).....	166
Figure 95.	Network Statistics.....	167
Figure 96.	VLAN Statistics.....	168
Figure 97.	WDS Statistics.....	169
Figure 98.	Filter Statistics.....	170
Figure 99.	Station Statistics.....	170
Figure 100.	Individual Station Statistics Page.....	171
Figure 101.	System Log.....	172
Figure 102.	WMI: Express Setup.....	174
Figure 103.	LEDs are Switched On.....	179
Figure 104.	Network Interfaces.....	180
Figure 105.	Network Settings.....	181
Figure 106.	Network Interface Ports.....	182
Figure 107.	Port Modes (a-b).....	184
Figure 108.	Port Modes (c-d).....	185

---

Figure 109. Port Modes (e-f) .....	186
Figure 110. DNS Settings.....	188
Figure 111. CDP Settings.....	190
Figure 112. Services.....	192
Figure 113. Time Settings (Manual Time).....	193
Figure 114. Time Settings (NTP Time Enabled).....	194
Figure 115. NetFlow .....	195
Figure 116. System Log .....	196
Figure 117. SNMP .....	199
Figure 118. DHCP Management .....	202
Figure 119. VLANs.....	204
Figure 120. VLAN Management .....	206
Figure 121. Security.....	208
Figure 122. Import Xirrus Certificate Authority.....	212
Figure 123. Admin Management .....	214
Figure 124. Admin RADIUS .....	216
Figure 125. Management Control .....	218
Figure 126. Access Control List.....	222
Figure 127. Global Settings (Security) .....	224
Figure 128. External RADIUS Server .....	227
Figure 129. Internal RADIUS Server .....	230
Figure 130. Rogue Control List .....	233
Figure 131. SSIDs.....	235
Figure 132. Four Traffic Classes .....	237
Figure 133. SSID Management .....	240
Figure 134. SSID Management .....	243
Figure 135. WPR Internal Splash Page Fields (SSID Management).....	246
Figure 136. Groups.....	248
Figure 137. Group Management .....	250
Figure 138. IAPs.....	254
Figure 139. IAP Settings .....	256
Figure 140. Global Settings (IAPs).....	261
Figure 141. Global Settings .11a .....	268
Figure 142. Global Settings .11bg.....	270
Figure 143. Global Settings .11n.....	274
Figure 144. Advanced RF Settings.....	277
Figure 145. LED Settings .....	285

Figure 146. WDS .....	287
Figure 147. .Configuring a WDS Link .....	288
Figure 148. WDS Client Links .....	289
Figure 149. Filters .....	292
Figure 150. Filter Lists .....	293
Figure 151. Filter Management .....	295
Figure 152. System Tools.....	300
Figure 153. Saving the Diagnostic Log.....	305
Figure 154. Managing WPR Splash/Login page files.....	306
Figure 155. System Command (Ping).....	307
Figure 156. Radius Ping Command.....	307
Figure 157. Radius Ping Output.....	308
Figure 158. CLI Window .....	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.....	362
Figure 165. Configuring a Global SSID using WPA-PEAP .....	363
Figure 166. Configuring an SSID-Specific SSID using WPA-PEAP .....	364
Figure 167. Enabling Global IAPs.....	365
Figure 168. Disabling Global IAPs.....	366
Figure 169. Enabling a Specific IAP.....	367
Figure 170. Disabling a Specific IAP.....	368
Figure 171. Setting the Cell Size for All IAPs.....	369
Figure 172. Setting the Cell Size for All IAPs.....	370
Figure 173. Setting the Cell Size for a Specific IAP .....	371
Figure 174. Configuring VLANs on an Open SSID.....	372
Figure 175. Configuring Radio Assurance Mode (Loopback Testing) .....	374
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.....	427
Figure 190. Applying Three Seals to XS16/XS8 or XS-3900/XS-3700 .....	430
Figure 191. Applying Two Tamper-evident seals to the XS4 or XS-3500 .....	431
Figure 192. SSID Management Window.....	432
Figure 193. Security/Global Settings Window .....	433
Figure 194. Security/Management Control Window .....	434
Figure 195. Services/SNMP Window .....	434
Figure 196. IAPs/Global Settings Screen.....	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 2.***
- ***"About this User's Guide" on page 4.***
- ***"Why Choose the Xirrus Wi-Fi Array?" on page 7.***
- ***"Wi-Fi Array Product Overview" on page 9.***
- ***"Key Features and Benefits" on page 16.***
- ***"Product Specifications—XN16, XN12, and XN8" on page 20.***
- ***"Product Specifications—XN4" on page 27.***
- ***"Product Specifications—XS16/XS-3900, and XS8/XS-3700" on page 34.***
- ***"Product Specifications—XS4/XS-3500" on page 39.***

## The Xirrus Family of Products



Figure 1. Xirrus Arrays

The Xirrus family of products includes the following:

- **The XS Series of Xirrus Wi-Fi Arrays (XS16 / XS8 / XS4)**  
XS Arrays integrate multiple Integrated Access Points—radios with high-gain directional antennas for increased range and coverage. The Array also incorporates an onboard multi-gigabit switch, Wi-Fi controller, and firewall into a single device, along with a dedicated Wi-Fi threat sensor and an embedded spectrum analyzer. The Wi-Fi Array provides more than enough bandwidth, security, and control to replace switched Ethernet to the desktop as the primary network connection. The XS16 has 16 IAPs, the XS8 has 8 IAPs, and the XS4 has 4 IAPs.
- **The XN Series of Xirrus Wi-Fi Arrays (XN16 / XN12 / XN8 / XN4)**  
The newest Xirrus Wi-Fi Arrays add the speed and reach of IEEE 802.11n technology to the XS series of Arrays. 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.



- **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.

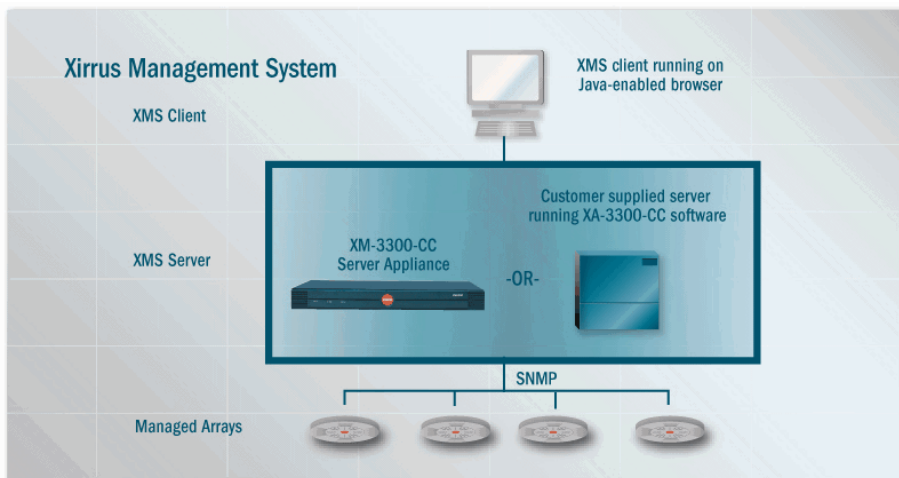


Figure 2. The Xirrus Management System

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 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, XN16, XS8, or XS-3500). 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 XS series of Arrays have two types of radios—the 5 GHz 802.11a radios are named **a1** to **a12** (for 16-port models). The 802.11a/b/g radios are named **abg1** to **abg4**, and they support both 2.4GHz and 5 GHz. The XN series of Arrays also have two types of radios—the 5 GHz 802.11a/n radios are named **an1** through **an12** (for 16-port models). The 802.11a/b/g/n radios are named **abgn1** to **abgn4**, and they also support both 2.4GHz and 5 GHz. When referring to a port that may be on either an XN or XS model, the nomenclature **abg(n)** and **a(n)** will be used, e.g., **abg(n)2** or **a(n)6**.

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 security standards with the Array, including FIPS and PCI DSS.
- **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.

## Window or Page?

Is a window a page, or is a page a window? There seems to be some dispute as to what the correct term should be. For the sake of consistency, this document uses the term **Window** when referring to how the Wi-Fi Array's Web Management Interface is displayed on your monitor.

## Why Choose the Xirrus Wi-Fi Array?

The deployment of wireless LANs 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.

Wireless LAN is also fully compatible with standard Ethernet protocols, so connectivity with existing wired infrastructures 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 infrastructure (it's only the plug that no longer exists).

Wireless LAN 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 300 Mbps, 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.

*See Also*

[Key Features and Benefits](#)

[Wi-Fi Array Product Overview](#)

[Product Specifications—XN16, XN12, and XN8](#)

[Product Specifications—XS4/XS-3500](#)

[Product Specifications—XS16/XS-3900, and XS8/XS-3700](#)

[The Xirrus Family of Products](#)

## 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 up to eight times the capacity of competitive wireless products.



Figure 3. Wi-Fi Array (XN16)

The Wi-Fi Array (regardless of the product model) is Wi-Fi® compliant and simultaneously supports 802.11a, 802.11b and 802.11g clients. XN model arrays add the enhanced abilities of 802.11n to this combination. 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: 16 IAPs (XN16, XS16, XS-3900), 12 IAPs (XN12), 8 IAPs (XN8, XS8, XS-3700), and 4 IAPs (XN4, XS4, XS-3500).

### 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 provided with 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. Rogue AP

detection, site monitoring, and RF spectrum analysis are performed in the background by the Array automatically.

### Wi-Fi Array Product Family

The following tables provide an overview of the main features supported by the Wi-Fi Array product family.

#### XN Family of Arrays

Feature	XN16	XN12	XN8	XN4
Number of 802.11a/b/g/n radios	4	4	4	4
Number of 802.11a/n radios	12	8	4	0
<b>Total radios</b>	<b>16</b>	<b>12</b>	<b>8</b>	<b>4</b>
Number of integrated antennas	48	36	24	12
Integrated Wi-Fi switch ports	16	12	8	4
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes
Uplink Ports	2	2	2	1
Wi-Fi bandwidth	4.8 Gbps	3.6 Gbps	2.4 Gbps	1.2 Gbps
Users supported	1,024	768	512	256



## XS Family of Arrays

Feature	XS16, XS-3900	XS8, XS-3700	XS4, XS-3500
Number of 802.11a/b/g radios	4	4	4
Number of 802.11a radios	12	4	0
<b>Total radios</b>	<b>16</b>	<b>8</b>	<b>4</b>
Integrated Wi-Fi switch ports	16	8	4
Integrated RF spectrum analyzer and threat sensors	Yes	Yes	Yes
Uplink Ports	2	2	1
Wi-Fi bandwidth	864 Mb	432 Mb	216 Mb
Users supported	1,024	512	256

### *See Also*

Key Features and Benefits

Wi-Fi Array Product Overview

Product Specifications—XN16, XN12, and XN8

Product Specifications—XS4/XS-3500

Product Specifications—XS16/XS-3900, and XS8/XS-3700

Power over Gigabit Ethernet (PoGE)

Why Choose the Xirrus Wi-Fi Array?

## Deployment Flexibility

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

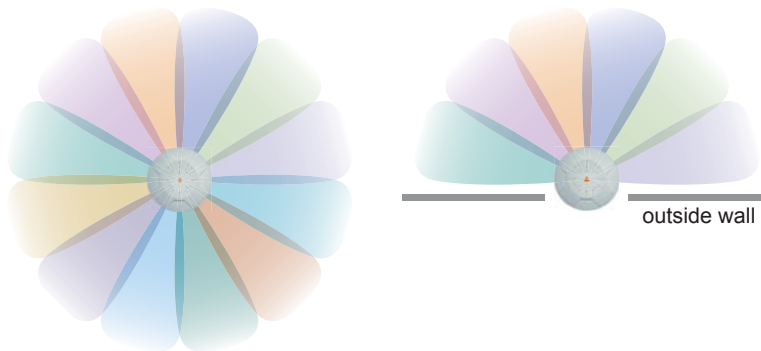


Figure 4. Wireless Coverage Patterns

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.

See also, “Flexible Coverage Schemes” on page 18.

### Power over Gigabit Ethernet (PoGE)

The Xirrus XP1, XP2, and XP8 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.

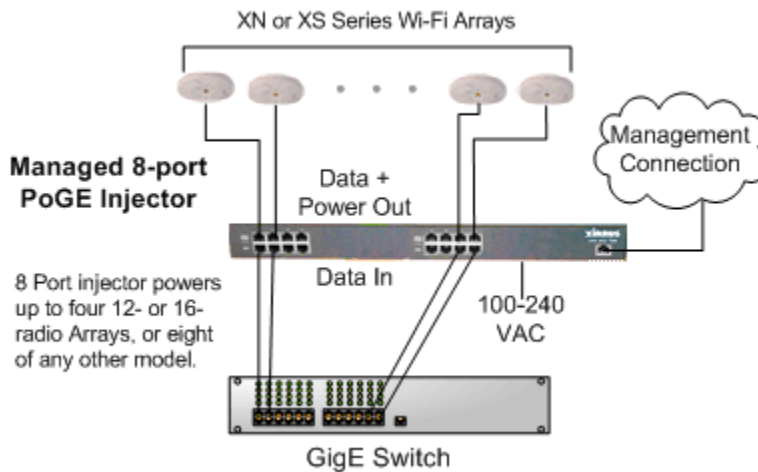


Figure 5. XP8 - Power over Ethernet Usage

Specific models of the Array are compatible with specific PoGE modules. For details, please see [“Power over Gigabit Ethernet Compatibility Matrix”](#) on [page 420](#).

#### See Also

[Key Features and Benefits](#)

[Wi-Fi Array Product Overview](#)

[Product Specifications—XN16, XN12, and XN8](#)

[Product Specifications—XS4/XS-3500](#)

[Product Specifications—XS16/XS-3900, and XS8/XS-3700](#)

[The Xirrus Family of Products](#)

[Why Choose the Xirrus Wi-Fi Array?](#)

## 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 6. 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.*

**See Also**

Key Features and Benefits

Product Specifications—XN16, XN12, and XN8

Product Specifications—XN4

Product Specifications—XS4/XS-3500

Product Specifications—XS16/XS-3900, and XS8/XS-3700

Power over Gigabit Ethernet (PoGE)

The Xirrus Family of Products

Why Choose the Xirrus Wi-Fi Array?

## 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 XN16 product is highlighted in this section).

### High Capacity and High Performance

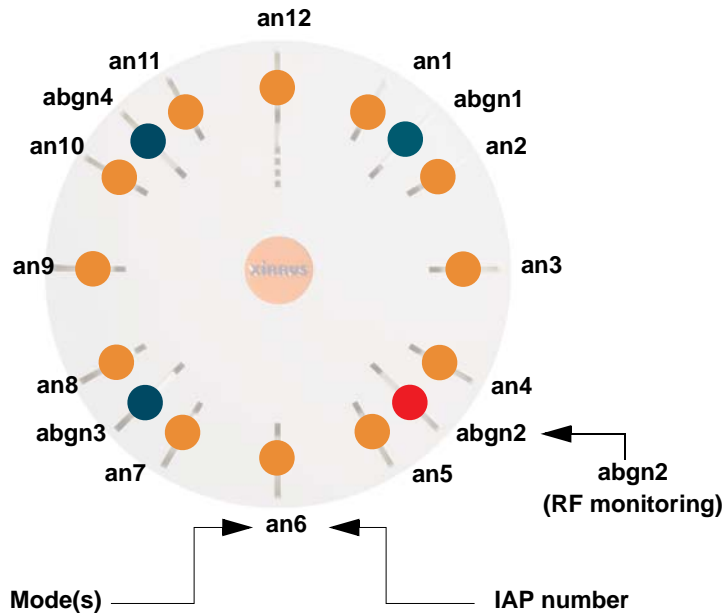


Figure 7. Layout of IAPs (XN16)

The XN16 version of the Wi-Fi Array (Figure 7) easily handles time-sensitive traffic such as voice, and can enable wireless connectivity for 1,024 users. The unit includes two Gigabit uplink ports for connection to the wired network. A total of sixteen IAPs provides a maximum wireless capacity of 4.8 Gbps, which offers ample reserves for the high demands of current and future applications. Of the sixteen IAPs, twelve operate as 802.11a/n radios (5 GHz band), and four operate as 802.11a/b/g/n radios (5 GHz or 2.4 GHz bands), providing backwards compatibility with 802.11b and 802.11g.

In the recommended configuration, IAP (radio) **abg(n)2** is configured in RF monitoring and rogue AP detection mode.

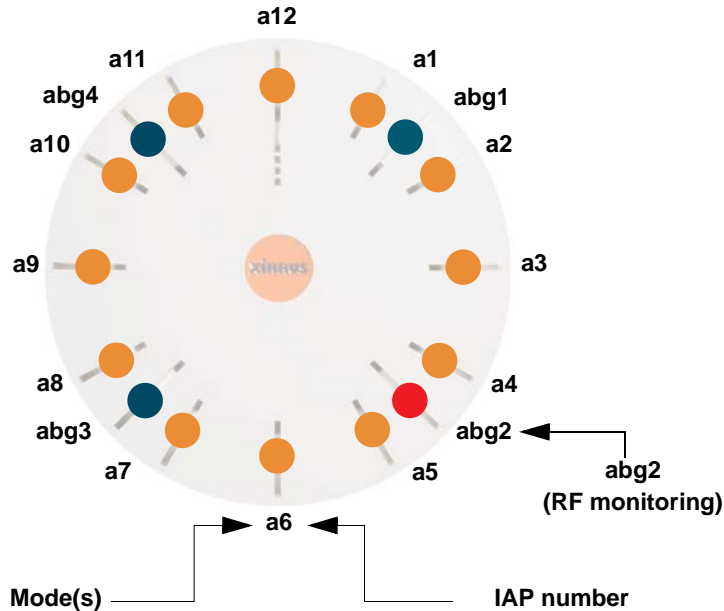


Figure 8. Naming of IAPs (XS16)

### Extended Coverage

One XN16 solution enables you to replace up to sixteen access points (includes one omnidirectional IAP for monitoring the network). Fifteen 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.

## Flexible Coverage Schemes

Your Wi-Fi Array offers flexible coverage schemes for each wireless technology.

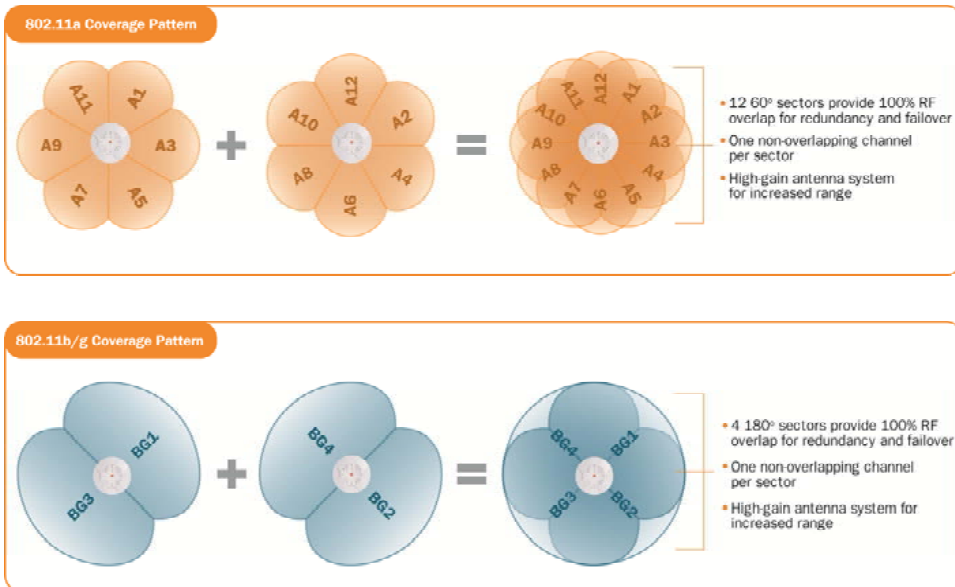


Figure 9. Coverage Schemes (XS16 shown)

- **802.11a/n, 802.11a**  
Delivers 60° wireless coverage per IAP, with 6 dBi of gain.
- **802.11b/g/n, 802.11b/g**  
Delivers 180° wireless coverage, with 3 dBi of gain.
- **802.11a/b/g/n, 802.11a/b/g (monitor only)**  
Delivers 360° wireless coverage, with 2 dBi of gain.

## Non-Overlapping Channels

Complete use of non-overlapping channels limits interference and delivers maximum capacity. On the XN16, up to 16 non-overlapping channels are fully utilized across the 5GHz and 2.4GHz spectrums (up to 12 across the 5GHz spectrum plus up to 3 across the 2.4 GHz spectrum—typically, one additional radio is used as a dedicated RF monitor).



### Secure Wireless Access

Multiple layers of authentication and encryption ensure secure data transmissions. The Wi-Fi Array is 802.11i compliant with encryption support for 40 bit and 128 bit WEP, WPA and WPA2 with TKIP and AES encryption. Authentication support is provided via 802.1x, including PEAP, EAP-TLS, EAP-TTLS, and LEAP (Lightweight Extensible Authentication Protocol) passthrough.

### Applications Enablement

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.

### 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 support.

### 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 of 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.

#### *See Also*

[Wi-Fi Array Product Overview](#)

[Product Specifications—XN16, XN12, and XN8](#)

[Product Specifications—XS4/XS-3500](#)

[Product Specifications—XS16/XS-3900, and XS8/XS-3700](#)

[Power over Gigabit Ethernet \(PoGE\)](#)

The Xirrus Family of Products  
 Why Choose the Xirrus Wi-Fi Array?

## Product Specifications—XN16, XN12, and XN8

Element	XN16/XN12/XN8 Specifications
<b>Number of Users</b>	Maximum of 64 associated users per radio XN16: 1024 users per Array XN12: 768 users per Array XN8: 512 users per Array
<b>Physical</b>	Diameter: 18.65 inches (47.37 cm) Height: 3.87 inches (9.83 cm) Weight: 10 lbs (3.63 kg)
<b>Environmental</b>	<b>Operating Temperature:</b> 0°C to 55°C 0% to 90% relative humidity (non-condensing) <b>Storage Temperature:</b> -20°C to 60°C 5% to 95% relative humidity (non-condensing)
<b>System</b>	1 GHz CPU 1 GB RAM 1 GB system flash
<b>Integrated Switch</b>	2.1 Gbps integrated wireless switch
<b>Chassis</b>	Lockable mounting plate, Kensington lock slot

Element	XN16/XN12/XN8 Specifications
<b>Electrical</b>	<p>XN12, XN16 support PoGE only                      XN8 supports both AC and PoGE                      AC Input Power: 100-240VAC at 50-60 Hz                      PoGE (DC) Input Power: Power over Gigabit Ethernet—no splitter required, 48VDC, Maximum 2A</p> <p><b>Nominal Power:</b>                      XN16: 90W                      XN12: 75W                      XN8: 60W</p> <p><b>All Models:</b>                      For PoGE, see “Power over Gigabit Ethernet Compatibility Matrix” on page 420.</p>
<b>Interfaces</b>	<p><b>Serial Console Port:</b>                      1 x RS232 – RJ45 connector, for local configuration</p> <p><b>Ethernet Interfaces:</b>                      2 x Gigabit 100/1000 Mbps uplink ports for link aggregation, redundancy, or bridging                      1 x Fast Ethernet 10/100 Mbps, for out of band management</p> <p><b>Status LEDs:</b>                      System status, Ethernet, Radio</p>
<b>Networking</b>	<p>DHCP client, DHCP server (multiple DHCP pools), DNS Client, NTP client, NAT</p>

Element	XN16/XN12/XN8 Specifications
<b>Management</b>	<p>Xirrus Management System (XMS)—Layer 3 Element Management System</p> <p>HTTPS Web Management Interface (WMI)</p> <p>CLI via SSHv2, Telnet, local serial Console</p> <p>Enable/disable management for any interface</p> <p>Read-write and read-only admin accounts may be authenticated via RADIUS</p> <p>SNMP v2c, v3</p> <p>Configuration Files—text-based files may be imported, exported, or compared</p> <p>NetFlow—IP flow information (traffic statistics may be sent to an external Collector</p> <p>FTP, TFTP</p> <p>Syslog reporting for alerts/alarms—messages may be stored on internal Syslog server or sent to up to three external syslog servers.</p> <p>Cisco Discovery Protocol (CDP)—obtain protocol addresses and platform information for neighboring devices</p>
<b>Quality of Service (QoS) Support</b>	<p><b>Multiple SSIDs:</b></p> <p>16 unique SSIDs per Array</p> <p>Each SSID beacons a unique BSSID per radio</p> <p>VLAN and QoS settings for each SSID</p> <p><b>VLANs:</b></p> <p>Up to 16 VLANs, 802.1Q, 802.1p</p> <p><b>Prioritization:</b></p> <p>802.11e wireless prioritization</p> <p>802.1p wired prioritization</p> <p>Fair queuing of downstream traffic</p> <p><b>Wireless Voice Support:</b></p> <p>Spectralink Voice Priority (SVP) protocol</p>

Element	XN16/XN12/XN8 Specifications
<p><b>Security</b></p>	<p><b>Wireless Encryption</b>                      Line speed, hardware-accelerated encryption modes:                      WPA TKIP                      WPA2 AES                      WEP 40/64                      WEP 104/128</p> <p><b>Wireless Authentication:</b>                      Open                      Pre-shared Key                      802.1X EAP                      PEAP                      EAP-TLS                      EAP-TTLS                      EAP-LEAP Pass-through                      Web Page Redirect (Captive Portal)                      MAC Address Access Control List (ACL)                      CHAP, PAP</p> <p><b>Firewall:</b>                      Integrated stateful-inspection, rules-based firewall</p> <p><b>Rogue AP detection and blocking:</b>                      Integrated Rogue AP detection and alerting via dedicated internal RF Threat Sensor. Rogue AP can be shielded</p> <p><b>Integrated RADIUS Server:</b>                      Integrated 802.1x Authentication Server supporting EAP-PEAP</p>

Element	XN16/XN12/XN8 Specifications
<b>Security (continued)</b>	<p><b>Time of Day Access:</b> Specify when access is allowed, per SSID or User Group</p> <p><b>Station-Station Blocking:</b> Station-to-Station traffic blocking option</p>
<b>Wireless</b>	<p><b>Wireless Standards:</b> 802.11a 802.11b 802.11d 802.11g 802.11e 802.11h 802.11i 802.11j 802.11n</p> <p><b>Number of Radios:</b></p> <p><b>XN16:</b> 12 x 802.11a/n radios 4 x 802.11a/b/g/n radios Only 12 radios should be used as 802.11a/n radios (i.e., 5 GHz band) concurrently. 48 integrated antennas</p> <p><b>XN12:</b> 8 x 802.11a/n radios 4 x 802.11a/b/g/n radios 36 integrated antennas</p> <p><b>XN8:</b> 4 x 802.11a/n radios 4 x 802.11a/b/g/n radios Advanced RF design includes 36 integrated antennas</p> <p><b>Spectrum Analyzer:</b> 1 integrated into Array</p>

Element	XN16/XN12/XN8 Specifications
<p><b>Wireless (continued)</b></p>	<p><b>Frequency Bands:</b>                      11a/n: 4.945 – 4.985 (restricted Public Safety band)                      11a/n: 5.15-5.25 GHz (UNII 1)                      11a/n: 5.15-5.25 GHz (TELEC)                      11a/n: 5.25-5.35 GHz (UNII 2)                      11a/n: 5.470-5.725 (ETSI)                      11a/n: 5.725-5.825 GHz (UNII 3)                      11b/g/n: 2.412-2.462 GHz (FCC)                      11b/g/n: 2.412-2.472 GHz (ETSI)                      11b/g/n: 2.412-2.484 GHz (TELEC)</p> <p><b>Channel Selection:</b>                      Manual and Automatic</p> <p><b>802.11a/n Antennas</b>                      Integrated 6dBi, sectorized</p> <p><b>802.11b/g/n Antennas</b>                      Integrated 3dBi, sectorized</p> <p><b>Wi-Fi Monitoring:</b>                      1 Integrated Access Point can be set as a dedicated Wi-Fi Threat Sensor                      2 dBi 360° omni-directional antenna</p> <p><b>802.11a/b/g/n External Antenna Connectors:</b>                      3 RP-TNC connectors (<b>NOTE:</b> TNC antenna connection is not for outside plant connection.)</p>
<p><b>Performance</b></p>	<p><b>Client Load Balancing</b>                      Automatic load balancing between system radios</p>

Element	XN16/XN12/XN8 Specifications
<b>Compliance</b>	<b>Electromagnetic:</b> ICES-003 (Canada) EN 301.893 (Europe) EN 301.489-1 and -17 (Europe) <b>Safety:</b> EN 60950 EN 50371 to 50385 CE Mark
<b>Certifications</b>	<b>Wi-Fi Alliance:</b> 802.11a/b/g/n, WPA, WPA2, and extended EAP types. <a href="#">Our certifications may be viewed here.</a>
<b>Warranty</b>	<b>Hardware:</b> Five Year Standard (extendable) <b>Software:</b> 90 Days Standard (extendable)

*See Also*

Key Features and Benefits

Wi-Fi Array Product Overview

Product Specifications—XN4

Product Specifications—XS16/XS-3900, and XS8/XS-3700

Product Specifications—XS4/XS-3500

Power over Gigabit Ethernet (PoGE)

The Xirrus Family of Products

Why Choose the Xirrus Wi-Fi Array?



## Product Specifications—XN4

Element	XN4 Specifications
<b>Number of Users</b>	Maximum of 64 associated users per radio, 256 users per XN4
<b>Physical</b>	Diameter: 12.58 inches (31.95 cm) Height: 2.58 inches (6.55 cm) Weight: 4lbs (1.81 kg)
<b>Environmental</b>	<b>Operating Temperature:</b> 0°C to 55°C 0% to 90% relative humidity (non-condensing) <b>Storage Temperature:</b> -20°C to 60°C 5% to 95% relative humidity (non-condensing)
<b>System</b>	825 MHz CPU 512 MB RAM 1 GB system flash
<b>Integrated Switch</b>	2.1 Gbps integrated wireless switch
<b>Chassis</b>	Lockable mounting plate, Kensington lock slot
<b>Electrical</b>	XN4 supports Power over Gigabit Ethernet (PoGE) only, no splitter required PoGE (DC) Input Power: 48VDC, Maximum 2A Nominal Power: 35W For PoGE, see “Power over Gigabit Ethernet Compatibility Matrix” on page 420.

Element	XN4 Specifications
<b>Interfaces</b>	<p><b>Serial Console Port:</b> 1 x RS232 – RJ45 connector, for local configuration</p> <p><b>Ethernet Interfaces:</b> 1 x Gigabit 100/1000 Mbps uplink port</p> <p><b>Status LEDs:</b> System status, Ethernet, Radio</p>
<b>Networking</b>	<p>DHCP client, DHCP server (multiple DHCP pools), DNS Client, NTP client, NAT</p>
<b>Management</b>	<p>Xirrus Management System (XMS)—Layer 3 Element Management System</p> <p>HTTPS Web Management Interface (WMI)</p> <p>CLI via SSHv2, Telnet, local serial Console</p> <p>Enable/disable management for any interface</p> <p>Read-write and read-only admin accounts may be authenticated via RADIUS</p> <p>SNMP v2c, v3</p> <p>Configuration Files—text-based files may be imported, exported, or compared</p> <p>NetFlow—IP flow information (traffic statistics may be sent to an external Collector)</p> <p>FTP, TFTP</p> <p>Syslog reporting for alerts/alarms—messages may be stored on internal Syslog server or sent to up to three external syslog servers.</p> <p>Cisco Discovery Protocol (CDP)—obtain protocol addresses and platform information for neighboring devices</p>

Element	XN4 Specifications
<p><b>Quality of Service (QoS) Support</b></p>	<p><b>Multiple SSIDs:</b>                      16 unique SSIDs per Array                      Each SSID beacons a unique BSSID per radio                      VLAN and QoS settings for each SSID</p> <p><b>VLANs:</b>                      Up to 16 VLANs, 802.1Q, 802.1p</p> <p><b>Prioritization:</b>                      802.11e wireless prioritization                      802.1p wired prioritization                      Fair queuing of downstream traffic</p> <p><b>Wireless Voice Support:</b>                      Spectralink Voice Priority (SVP) protocol</p>

Element	XN4 Specifications
<b>Security</b>	<p><b>Wireless Encryption</b></p> <p>Line speed, hardware-accelerated encryption modes:</p> <ul style="list-style-type: none"> <li>WPA TKIP</li> <li>WPA2 AES</li> <li>WEP 40/64</li> <li>WEP 104/128</li> </ul> <p><b>Wireless Authentication:</b></p> <ul style="list-style-type: none"> <li>Open</li> <li>Pre-shared Key</li> <li>802.1X EAP</li> <li>PEAP</li> <li>EAP-TLS</li> <li>EAP-TTLS</li> <li>EAP-LEAP Pass-through</li> <li>Web Page Redirect (Captive Portal)</li> <li>MAC Address Access Control List (ACL)</li> <li>CHAP, PAP</li> </ul> <p><b>Firewall:</b></p> <p>Integrated stateful-inspection, rules-based firewall</p> <p><b>Rogue AP detection and blocking:</b></p> <p>Integrated Rogue AP detection and alerting via dedicated internal RF Threat Sensor. Rogue AP can be shielded</p> <p><b>Integrated RADIUS Server:</b></p> <p>Integrated 802.1x Authentication Server supporting EAP-PEAP</p>

Element	XN4 Specifications
<p><b>Security (continued)</b></p>	<p><b>Time of Day Access:</b> Specify when access is allowed, per SSID or User Group</p> <p><b>Station-Station Blocking:</b> Station-to-Station traffic blocking option</p>
<p><b>Wireless</b></p>	<p><b>Wireless Standards:</b> 802.11a 802.11b 802.11d 802.11g 802.11e 802.11h 802.11i 802.11j 802.11n</p> <p><b>Number of Radios:</b> 4 x 802.11a/b/g/n radios Advanced RF design includes 20 integrated antennas</p> <p><b>Spectrum Analyzer:</b> 1 integrated into Array</p>

Element	XN4 Specifications
<b>Wireless (continued)</b>	<p><b>Frequency Bands:</b></p> <ul style="list-style-type: none"> <li>11a/n: 4.945 – 4.985 (restricted Public Safety band)</li> <li>11a/n: 5.15-5.25 GHz (UNII 1)</li> <li>11a/n: 5.15-5.25 GHz (TELEC)</li> <li>11a/n: 5.25-5.35 GHz (UNII 2)</li> <li>11a/n: 5.470-5.725 (ETSI)</li> <li>11a/n: 5.725-5.825 GHz (UNII 3)</li> <li>11b/g/n: 2.412-2.462 GHz (FCC)</li> <li>11b/g/n: 2.412-2.472 GHz (ETSI)</li> <li>11b/g/n: 2.412-2.484 GHz (TELEC)</li> </ul> <p><b>Channel Selection:</b></p> <p>Manual and Automatic</p> <p><b>802.11a/n Antennas</b></p> <p>Integrated 6dBi, sectorized</p> <p><b>802.11b/g/n Antennas</b></p> <p>Integrated 3dBi, sectorized</p> <p><b>Wi-Fi Monitoring:</b></p> <ul style="list-style-type: none"> <li>1 Integrated Access Point can be set as a dedicated Wi-Fi Threat Sensor</li> <li>2 dBi 360° omni-directional antenna</li> </ul> <p><b>802.11a/b/g/n External Antenna Connectors:</b></p> <ul style="list-style-type: none"> <li>1 RP-TNC connector (<b>NOTE:</b> TNC antenna connection is not for outside plant connection.)</li> </ul>
<b>Performance</b>	<p><b>Client Load Balancing</b></p> <p>Automatic load balancing between system radios</p>

Element	XN4 Specifications
<b>Compliance</b>	<b>Electromagnetic:</b> ICES-003 (Canada) EN 301.893 (Europe) EN 301.489-1 and -17 (Europe) <b>Safety:</b> EN 60950 EN 50371 to 50385 CE Mark
<b>Certifications</b>	<b>Wi-Fi Alliance:</b> 802.11a/b/g/n, WPA, WPA2, and extended EAP types. <a href="#">Our certifications may be viewed here.</a>
<b>Warranty</b>	<b>Hardware:</b> Five Year Standard (extendable) <b>Software:</b> 90 Days Standard (extendable)

### *See Also*

Key Features and Benefits

Wi-Fi Array Product Overview

Product Specifications—XN16, XN12, and XN8

Product Specifications—XS16/XS-3900, and XS8/XS-3700

Product Specifications—XS4/XS-3500

Power over Gigabit Ethernet (PoGE)

The Xirrus Family of Products

Why Choose the Xirrus Wi-Fi Array?

## Product Specifications—XS16/XS-3900, and XS8/XS-3700

Element	XS16/XS8/XS-3900/XS-3700 Specifications
<b>Number of Users</b>	Maximum of 64 associated users per radio 1024 users per Array (XS16/XS-3900) 512 users per Array (XS8/XS-3700)
<b>Physical</b>	Diameter: 18.65 inches (47.37 cm) Height: 3.87 inches (9.83 cm) Weight: 8lbs (3.63 kg)
<b>Environmental</b>	<b>Operating Temperature:</b> -10°C to 50°C 0% to 90% relative humidity (non-condensing) <b>Storage Temperature:</b> -20°C to 60°C 5% to 95% relative humidity (non-condensing)
<b>System</b>	<b>XS16/XS8:</b> 1 GHz CPU 1 GB RAM 1 GB system flash Expansion slot for future options <b>XS-3900/XS-3700:</b> 825 MHz CPU 512 MB RAM (XS-3900/XS-3700) 512 MB system flash Expansion slot for future options



Element	XS16/XS8/XS-3900/XS-3700 Specifications
<b>Interfaces</b>	<p><b>Serial:</b> 1 x RS232 – RJ45 connector</p> <p><b>Ethernet Interfaces:</b> 2 x Gigabit 100/1000 Mbps w/failover 1 x Fast Ethernet 10/100 Mbps</p> <p><b>Status LEDs:</b> System status, Ethernet, Radio</p>
<b>Electrical</b>	<p><b>XS16/XS8:</b> Each Array supports both AC and PoGE AC Input Power: 90-265VAC at 47-63Hz PoGE Input Power: Power over Gigabit Ethernet—no splitter required, 48VDC Nominal Power:     XS16: 70W     XS8: 45W</p> <p><b>XS-3900/XS-3700:</b> Separate AC and DC versions Input Power (AC version): 90VAC to 265VAC at 47Hz to 63Hz Input Power (DC version): 48VDC PoGE: requires modified DC version and splitter.</p> <p><b>All Models:</b> For PoGE, see “Power over Gigabit Ethernet Compatibility Matrix” on page 420.</p>
<b>Networking</b>	DHCP client, DHCP server, NTP client, NAT
<b>VLAN Support</b>	802.1Q, 802.1p VLAN Supports up to 16 VLANs
<b>Multiple SSID Support</b>	Allows up to 16 separate SSIDs to be defined with map security, VLAN and QoS settings for each SSID

Element	XS16/XS8/XS-3900/XS-3700 Specifications
<b>Performance</b>	<p><b>Client Load Balancing</b> Automatic load balancing between system radios</p> <p><b>Quality of Service:</b> 802.1p wired traffic prioritization Wireless packet prioritization MAP CoS to TCID Fair queuing of downstream traffic</p>
<b>Security</b>	<p><b>Wireless Security:</b> WEP 40bit/128bit encryption WPA and WPA2 with TKIP and AES encryption Rogue AP detection, with alerts and classification</p> <p><b>User and System Authentication:</b> WPA and WPA2 Pre-Shared Key authentication Internal RADIUS Server, supports EAP-PEAP only 802.1x EAP-TLS 802.1x EAP-TTLS/MSCHAPv2 802.1x PEAPv0/EAP-MSCHAPv2 802.1x PEAPv1/EAP-GTC 802.1x EAP-SIM 802.1x EAP-LEAP Passthrough External RADIUS servers Authentication of Wi-Fi Arrays to the Xirrus Management System (XMS)</p>

Element	XS16/XS8/XS-3900/XS-3700 Specifications
<p><b>Wireless</b></p>	<p><b>Number of Radios:</b></p> <p><b>XS16/XS-3900:</b> 12 x 802.11a radios 4 x 802.11a/b/g radios Only 12 radios should be used as 802.11a radios concurrently.</p> <p><b>XS8/XS-3700:</b> 4 x 802.11a radios 4 x 802.11a/b/g radios</p> <p><b>Wireless Standards:</b> 802.11a/b/g and g-only mode 802.11e, 802.11i</p> <p><b>Channel Selection:</b> Manual and Automatic</p> <p><b>Frequency Bands:</b> 11a: 4.945 – 4.985 (restricted Public Safety band) 11a: 5.15-5.25 GHz (UNII 1) 11a: 5.15-5.25 GHz (TELEC) 11a: 5.25-5.35 GHz (UNII 2) 11a: 5.470-5.725 (ETSI) 11a: 5.725-5825 GHz (UNII 3) 11b/g: 2.412-2.462 GHz (FCC) 11b/g: 2.412-2.472 GHz (ETSI) 11b/g: 2.412-2.484 GHz (TELEC)</p> <p><b>Antennas (XS16/XS-3900):</b> 12 x internal 6 dBi 60° 802.11a sectorized 4 x internal 3 dBi 180° 802.11b/g sectorized 1 x internal 2 dBi 360° omni-directional (for RF monitoring) 3 x external RP-TNC connectors for three 802.11a/b/g radios *</p>

Element	XS16/XS8/XS-3900/XS-3700 Specifications
<b>Wireless (continued)</b>	<p><b>Antennas (XS8/XS-3700):</b>                      4 x internal 6 dBi 60° 802.11a sectorized                      4x internal 3 dBi 180° 802.11b/g sectorized                      1 x internal 2 dBi 360° omni-directional (for RF monitoring)                      3 x external RP-TNC connectors for three 802.11a/b/g radios *</p> <p><b>Radio Approvals:</b>                      FCC (United States) and EN 301.893 (Europe)</p> <p>* Note: External RP-TNC antenna connectors are not for outside plant connection.</p>
<b>Management</b>	Web-based HTTPS SNMP v2c, v3 CLI via SSHv2 or Telnet FTP TFTP Serial Xirrus Management System (XMS) Syslog reporting for alerts/alarms
<b>Compliance</b>	UL / cUL 60950 and EN 60950 FCC Part 15.107 and 15109, Class A EN 301.489 (Europe) EN60601 EU medical equipment directive for EMC
<b>Certifications</b>	<p><b>Wi-Fi Alliance:</b> 802.11a/b/g, WPA, WPA2, and extended EAP types. <a href="#">Our certifications may be viewed here.</a></p> <p>Federal Information Processing Standard (FIPS) Publication 140 -2, Level 2.</p>
<b>Warranty</b>	One year (hardware and software)

*See Also*

- Key Features and Benefits
- Wi-Fi Array Product Overview
- Product Specifications—XN4
- Product Specifications—XN16, XN12, and XN8
- Product Specifications—XS4/XS-3500
- Power over Gigabit Ethernet (PoGE)
- The Xirrus Family of Products
- Why Choose the Xirrus Wi-Fi Array?

### Product Specifications—XS4/XS-3500

Element	XS4/XS-3500 Specifications
<b>Number of Users</b>	Maximum of 64 associated users per radio (256 users per Array)
<b>Physical</b>	Diameter: 12.58 inches (31.95 cm) Height: 2.58 inches (6.55 cm) Weight: 4lbs (1.81 kg)
<b>Environmental</b>	<b>Operating Temperature:</b> -10°C to 50°C 0% to 90% relative humidity (non-condensing) <b>Storage Temperature:</b> -20°C to 60°C 5% to 95% relative humidity (non-condensing)
<b>System</b>	825 MHz CPU (XS4) 666 MHz CPU (XS-3500) 512 MB RAM, expandable (XS4) 256 MB RAM, expandable (XS-3500) 512 MB system flash, expandable Expansion slot for future options

Element	XS4/XS-3500 Specifications
<b>Electrical</b>	<p><b>XS4:</b> Each Array supports both AC and PoGE AC Input Power: 90-265VAC at 47-63Hz Nominal power usage: 27W</p> <p><b>XS-3500:</b> AC Input Power: 90-265VAC at 47-63Hz Input Power (DC version): 48VDC</p> <p><b>All Models:</b> Power over Gigabit Ethernet (PoGE): all 4-port models work with all Xirrus PoGE modules, splitter required, 48VDC See “Power over Gigabit Ethernet Compatibility Matrix” on page 420.</p>
<b>Interfaces</b>	<p><b>Serial:</b> 1 x RS232 – RJ45 connector</p> <p><b>Ethernet Interfaces:</b> 1 x Gigabit 100/1000 Mbps</p> <p><b>Status LEDs:</b> System status, Ethernet, Radio</p>
<b>Management</b>	<p>Web-based HTTPS SNMP v2c, v3 CLI via SSHv2 or Telnet FTP TFTP Serial Xirrus Management System (XMS) Syslog reporting for alerts/alarms</p>
<b>Networking</b>	<p>DHCP client, DHCP server, NTP client, NAT</p>

Element	XS4/XS-3500 Specifications
<b>VLAN Support</b>	802.1Q, 802.1p VLAN Supports up to 16 VLANs
<b>Multiple SSID Support</b>	Allows up to 16 separate SSIDs to be defined with map security, VLAN and QoS settings for each SSID
<b>Performance</b>	<p><b>Client Load Balancing</b> Automatic load balancing between system radios</p> <p><b>Quality of Service:</b> 802.1p wired traffic prioritization Wireless packet prioritization MAP CoS to TCID Fair queuing of downstream traffic</p>
<b>Security</b>	<p><b>Wireless Security:</b> WEP 40bit/128bit encryption WPA and WPA2 with TKIP and AES encryption Rogue AP detection, with alerts and classification</p> <p><b>User and System Authentication:</b> WPA Pre-Shared Key authentication Internal RADIUS Server, supports EAP-PEAP only 802.1x EAP-TLS 802.1x EAP-TTLS/MSCHAPv2 802.1x PEAPv0/EAP-MSCHAPv2 802.1x PEAPv1/EAP-GTC 802.1x EAP-SIM 802.1x EAP-LEAP Passthrough External RADIUS servers Authentication of Wi-Fi Arrays to the Xirrus Management System (XMS)</p>

Element	XS4/XS-3500 Specifications
<b>Wireless</b>	<p><b>Number of Radios:</b> 4 x 802.11a/b/g radios</p> <p><b>Wireless Standards:</b> 802.11a/b/g and g-only mode 802.11e, 802.11i</p> <p><b>Channel Selection:</b> Manual and Automatic</p> <p><b>Frequency Bands:</b> 11a: 4.945 – 4.985 (restricted Public Safety band) 11a: 5.15-5.25 GHz (UNII 1) 11a: 5.15-5.25 GHz (TELEC) 11a: 5.25-5.35 GHz (UNII 2) 11a: 5.470-5.725 (ETSI) 11a: 5.725-5825 GHz (UNII 3) 11b/g: 2.412-2.462 GHz (FCC) 11b/g: 2.412-2.472 GHz (ETSI) 11b/g: 2.412-2.484 GHz (TELEC)</p> <p><b>Antennas (XS-3500):</b> 4 x internal 3 dBi 180° 802.11b/g sectorized 1 x internal 2 dBi 360° omni-directional (for RF monitoring) 1 x external RP-TNC connector for one 802.11a/b/g radio (<b>NOTE:</b> TNC antenna connection is not for outside plant connection.)</p> <p><b>Radio Approvals:</b> FCC (United States) and EN 301.893 (Europe)</p>
<b>Compliance</b>	<p>UL / cUL 60950 and EN 60950 FCC Part 15.107 and 15109, Class A EN 301.489 (Europe) EN60601 EU medical equipment directive for EMC</p>



Element	XS4/XS-3500 Specifications
<b>Certifications</b>	<p><i>Wi-Fi Alliance:</i> 802.11a/b/g, WPA, WPA2, and extended EAP types. <i>Our certifications may be viewed here.</i></p> <p>Federal Information Processing Standard (FIPS) Publication 140 -2, Level 2.</p>
<b>Warranty</b>	One year (hardware and software)

*See Also*

Key Features and Benefits

Wi-Fi Array Product Overview

Product Specifications—XN16, XN12, and XN8

Product Specifications—XN4

Product Specifications—XS16/XS-3900, and XS8/XS-3700

Power over Gigabit Ethernet (PoGE)

The Xirrus Family of Products

Why Choose the Xirrus Wi-Fi Array?



---

# Installing the Wi-Fi Array

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

- [“Installation Prerequisites” on page 45.](#)
- [“Planning Your Installation” on page 48.](#)
- [“Installation Workflow” on page 80.](#)
- [“Unpacking the Wi-Fi Array” on page 81.](#)
- [“Installing Your Wi-Fi Array” on page 83.](#)
- [“Powering Up the Wi-Fi Array” on page 107.](#)
- [“Establishing Communication with the Array” on page 110.](#)
- [“Performing the Express Setup Procedure” on page 112.](#)

## 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.

Specific models of the Array are compatible with specific PoGE modules. For details, please see [“Power over Gigabit Ethernet Compatibility Matrix” on page 420.](#)

If your Arrays are equipped to accept AC power (and you are not using PoGE), you need a dedicated power outlet to supply AC power to each unit deployed at the site.

- **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 67.*

*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 342.*

- **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 6.0 or higher), Netscape Navigator (version 7.0 or higher), or Mozilla Firefox (version 1.01 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 48
- “Coverage and Capacity Planning” on page 50
- “IEEE 802.11n Deployment Considerations” on page 59
- “Failover Planning” on page 67
- “Power Planning” on page 69
- “Security Planning” on page 70
- “Port Requirements” on page 72
- “Network Management Planning” on page 75
- “WDS Planning” on page 76
- “Common Deployment Options” on page 79



*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 sectored high-gain 802.11a/b/g/n or 802.11a/b/g 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.

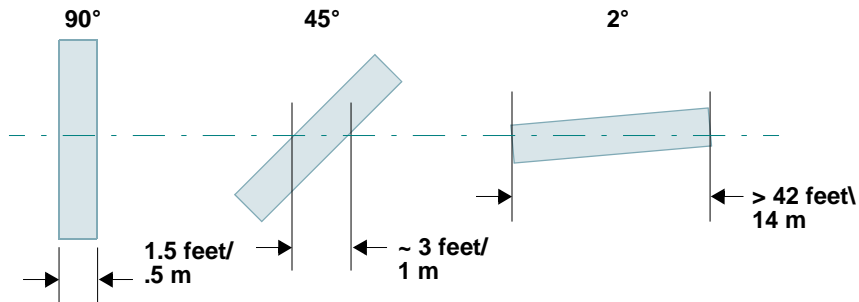


Figure 10. Wall Thickness Considerations

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.

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

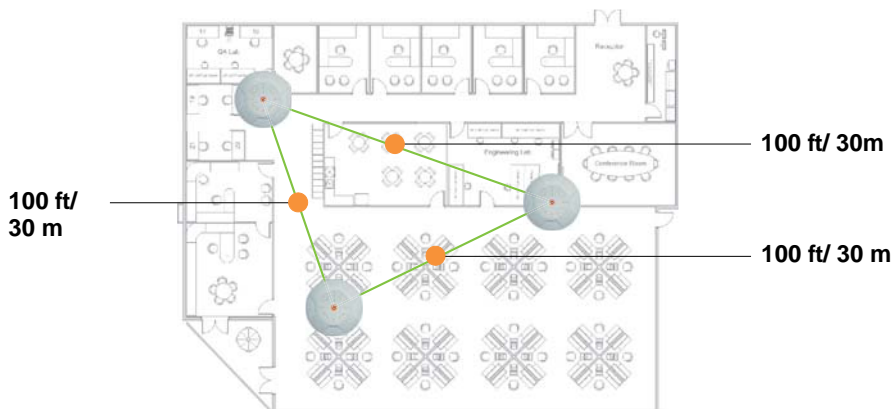


Figure 11. Unit Placement



### 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.

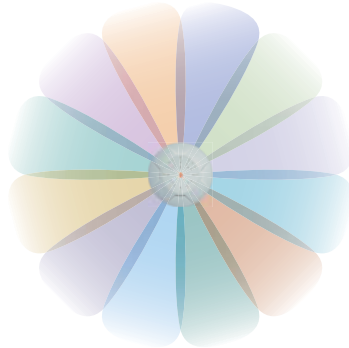


Figure 12. Full (Normal) Coverage

#### *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.

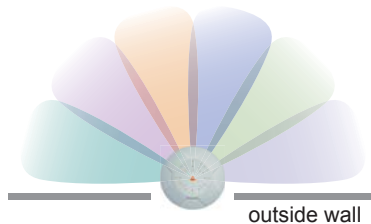


Figure 13. Adjusting RF Patterns

### Custom Coverage

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

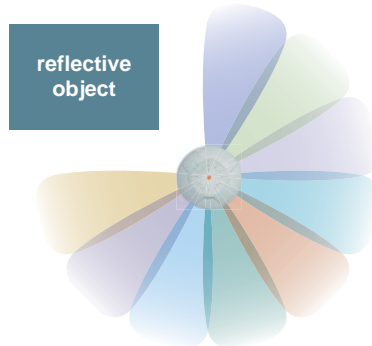


Figure 14. Custom Coverage

### 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.

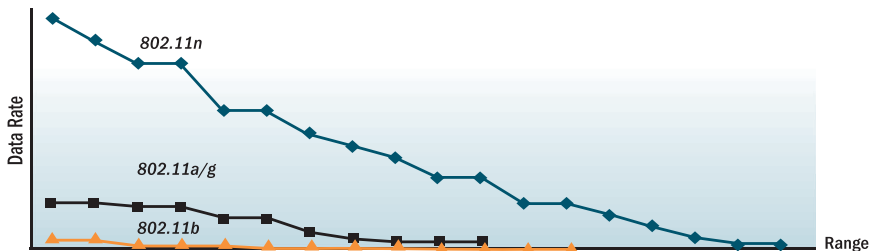


Figure 15. Connection Rate vs. Distance

Figure 15 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.



*The XS4 and XN4 have a smaller range than the larger Arrays.*

### 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.

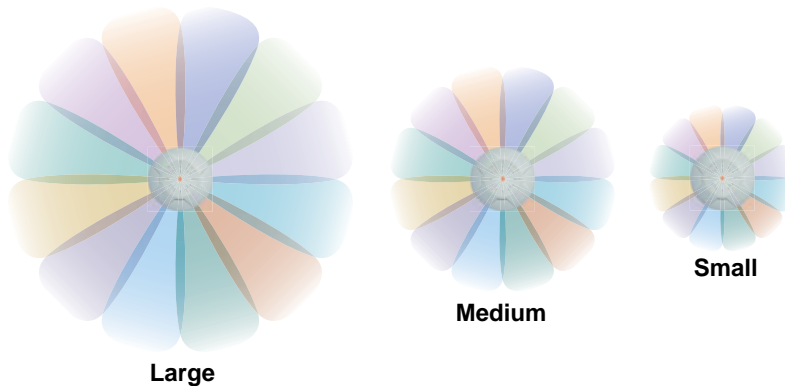


Figure 16. Transmit Power

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 280](#). 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 50.

### *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 280. 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.

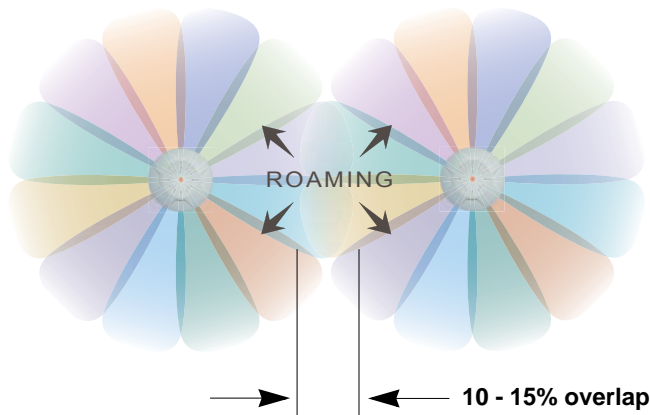


Figure 17. Overlapping Cells

### 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 277. 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.*

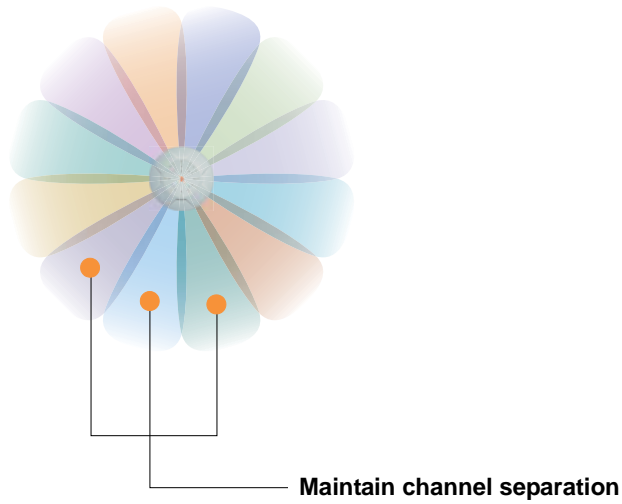


Figure 18. Allocating Channels Manually

*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).

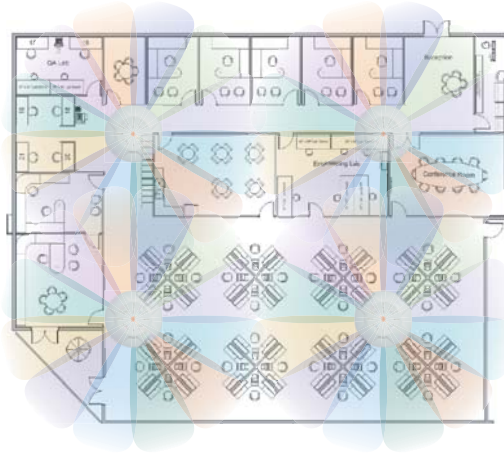


Figure 19. Deployment Scenario (54 Mbps)—Per Sector

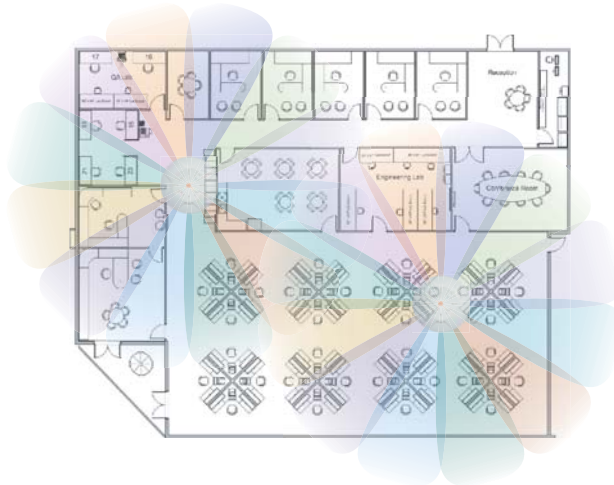


Figure 20. Deployment Scenario (36 Mbps)—Per Sector



Figure 21. 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.*

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 60
- “Multiple Data Streams—Spatial Multiplexing” on page 62
- “Channel Bonding” on page 63
- “Improved MAC Throughput” on page 64
- “Short Guard Interval” on page 64
- “Obtaining Higher Data Rates” on page 65
- “802.11n Capacity” on page 66

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 274 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 22)

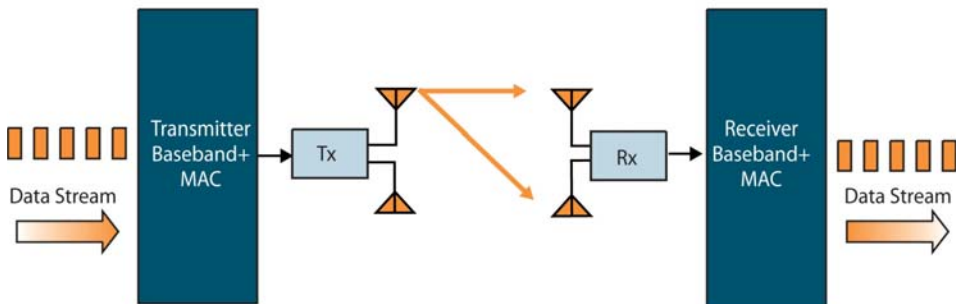


Figure 22. Classic 802.11 Signal Transmission

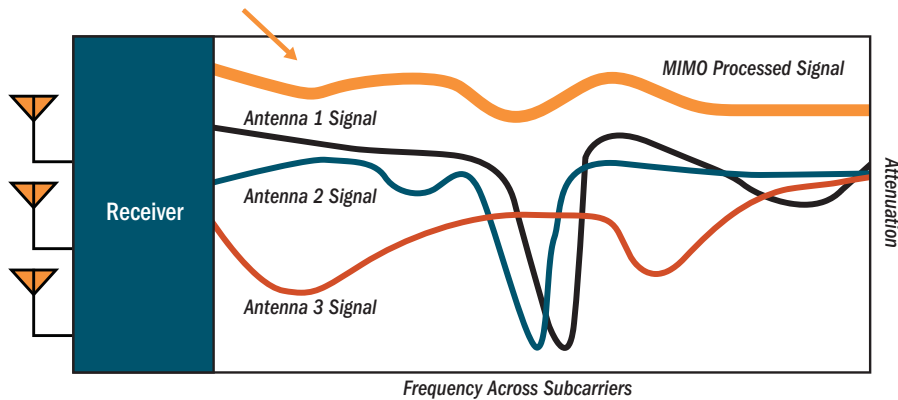


Figure 23. MIMO Signal Processing

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 23). 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.

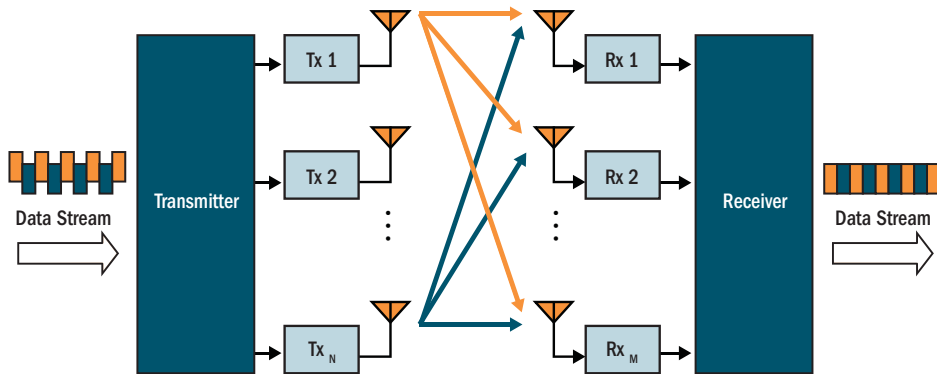


Figure 24. Spatial Multiplexing

Spatial multiplexing can double, triple, or quadruple the data rate, depending on the number of transmit antennas used. The Array uses three chains for transmitting and receiving.

## 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 274. To configure channel bonding manually, on a per-IAP basis, see “IAP Settings” on page 256.

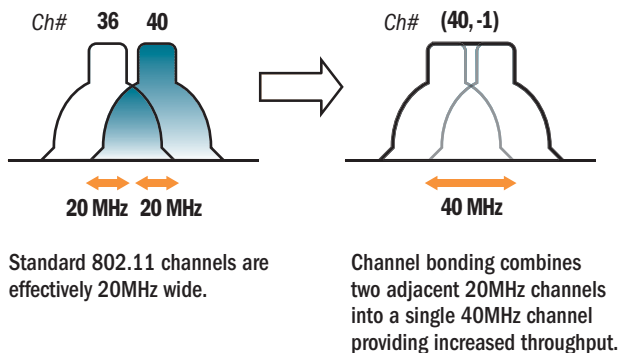


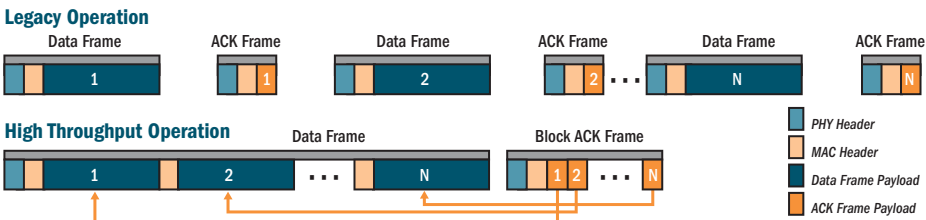
Figure 25. Channel Bonding

## 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)

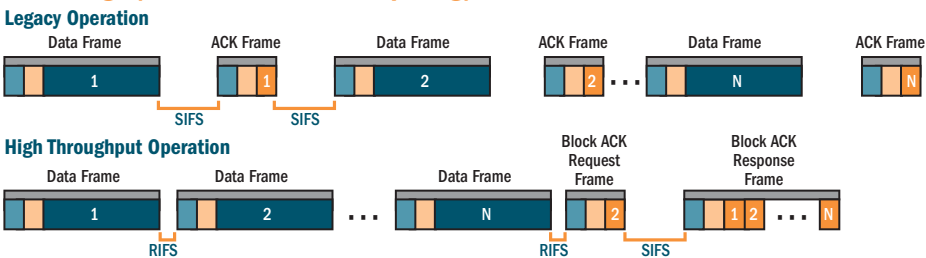


Figure 26. MAC Throughput Improvements

### 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

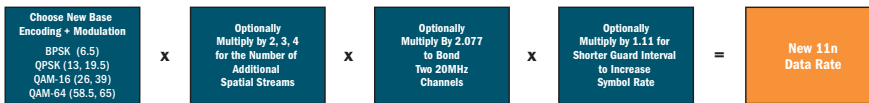
inappropriate environment, the signal quality will suffer and throughput will decrease. See “Global Settings .11n” on page 274 to configure the guard interval.

### 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 27 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					
	One Spatial Stream			Two Spatial Streams		
	11n Mandatory Data Rates	With Channel Bonding (40MHz)	With Short Guard Interval	Two Spatial Streams	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 27. Computing 802.11n Data Rates

**802.11n Capacity**

802.11n offers major increases in capacity over previous 802.11 standards, as shown in Figure 28. Note that this chart shows figures for 802.11n (with one spatial stream and channel bonding).

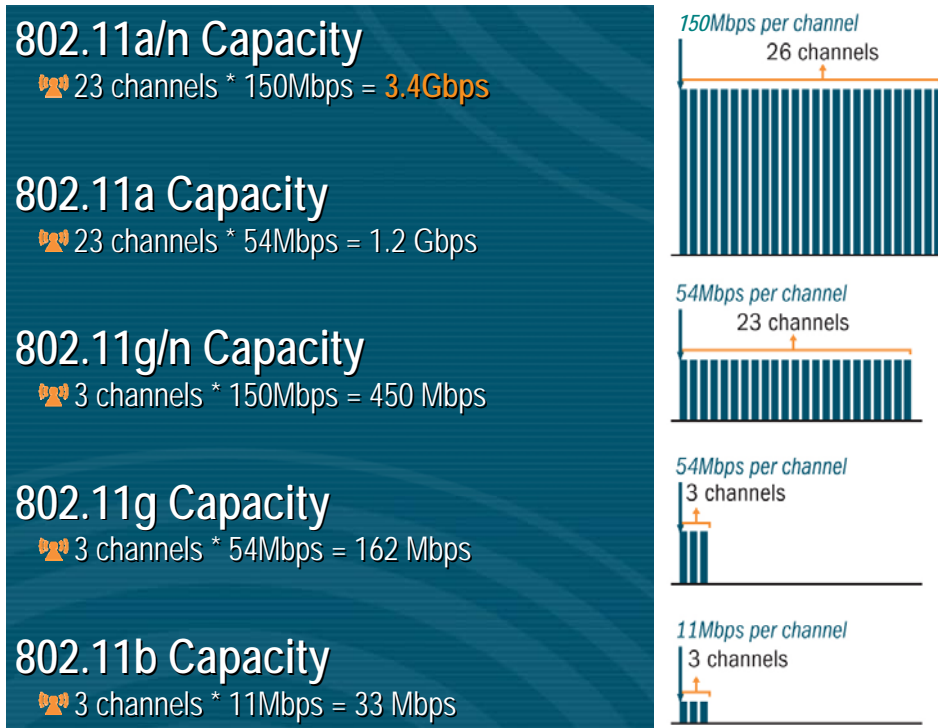


Figure 28. 802.11n Increases Capacity



## 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 ports simultaneously.

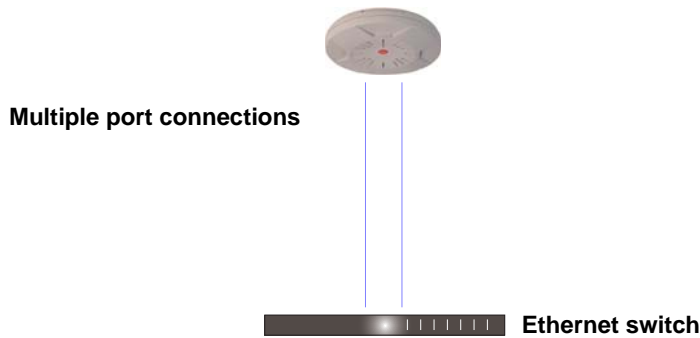


Figure 29. Port Failover Protection

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

Interface	Bridges Data?	Bridges Management Traffic?	Fails Over To:	IP address
Fast Ethernet	No	Yes	None	DHCP or static
Gigabit 1	Yes	Yes	Gigabit 2	DHCP or static
Gigabit 2	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

For more details on Gigabit port modes and their configuration, please see “Network Interface Ports” on page 182.

### 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).

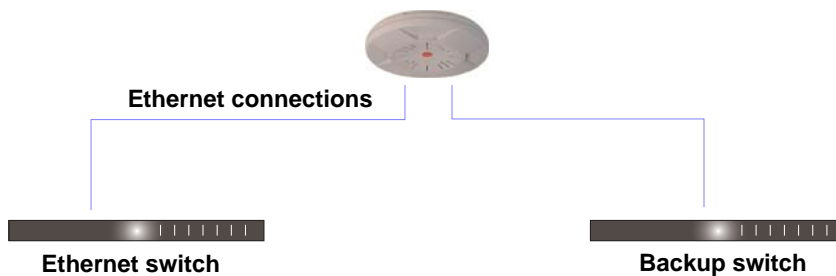


Figure 30. Switch Failover Protection



*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 XN Series Array models and XS16/8/4 Arrays support Power over Gigabit Ethernet (PoGE) with an integrated splitter. AC power is also supported on some versions of the XN8, XS8, and XS16.

This section discusses the AC and PoGE power options.

### AC Power

The AC power option requires a direct connection between the Array and a dedicated AC power outlet. The power cord is provided with the unit.

### Power over Gigabit Ethernet

To deliver power to the Array, you may use the optional XP1, XP2, or XP8 Power over Gigabit Ethernet (PoGE) modules. They provide power over Cat 5e or Cat 6 cables to the Array without running power cables—see [Figure 5 on page 13](#).

Specific models of the Array are compatible with specific PoGE modules. For details, please see [“Power over Gigabit Ethernet Compatibility Matrix” on page 420](#).



*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 209 and the Security section of “Frequently Asked Questions” on page 404.

### 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 Wi-Fi 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 the Wi-Fi Array may be configured to satisfy PCI DSS standards. For details, please see [Appendix D: Implementing PCI DSS](#).

### **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](#).

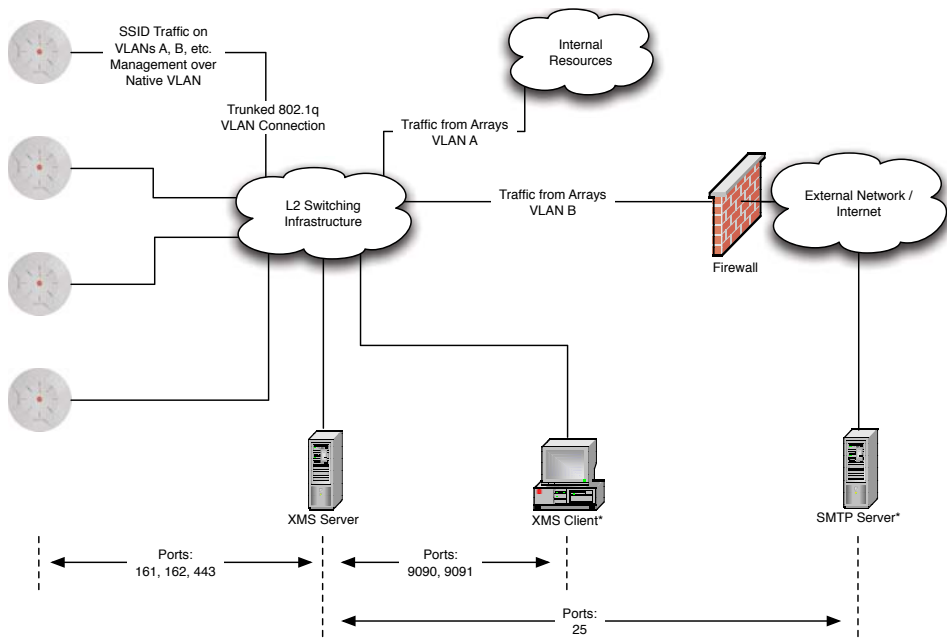
### *See Also*

[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 73](#) 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 31](#). 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.



\* XMS Client and SMTP Server may be internal or external resources.

Figure 31. 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 (XM-3300) 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 32](#)). WDS features include:

- One to three IAPs may be used to form a single WDS link, yielding up to 900 Mbps bandwidth per link (up to 162 Mbps for XS model Arrays). 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.

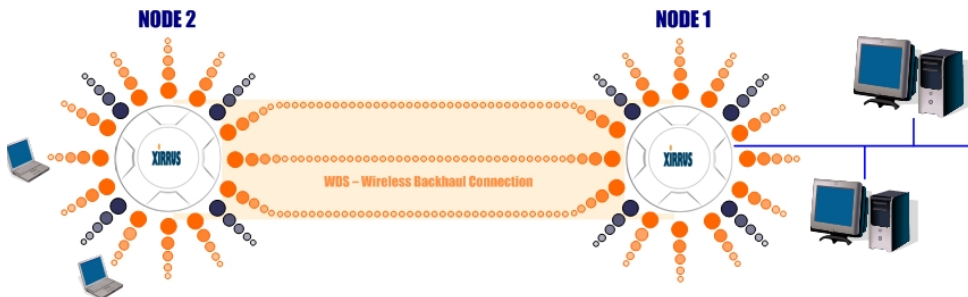


Figure 32. WDS Link

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

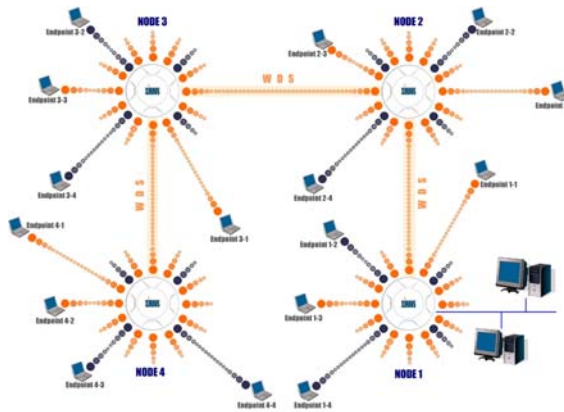


Figure 33. A Multiple Hop WDS Connection

- Multiple WDS links can provide link redundancy (failover capability - see Figure 34). A network protocol (Spanning Tree Protocol—STP) prevents Arrays from forming network loops.

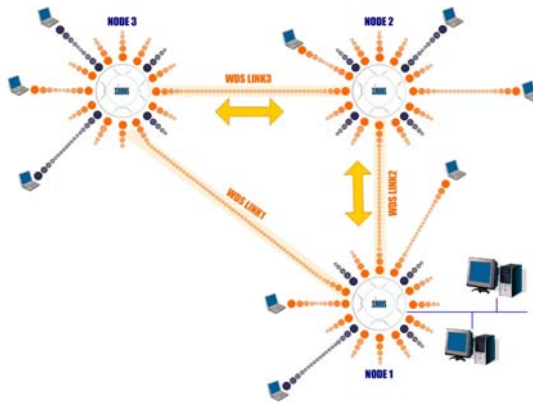


Figure 34. WDS Failover Protection

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 287](#). 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	AC (some Array models) Power over Gigabit Ethernet	AC (some Array models) 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.

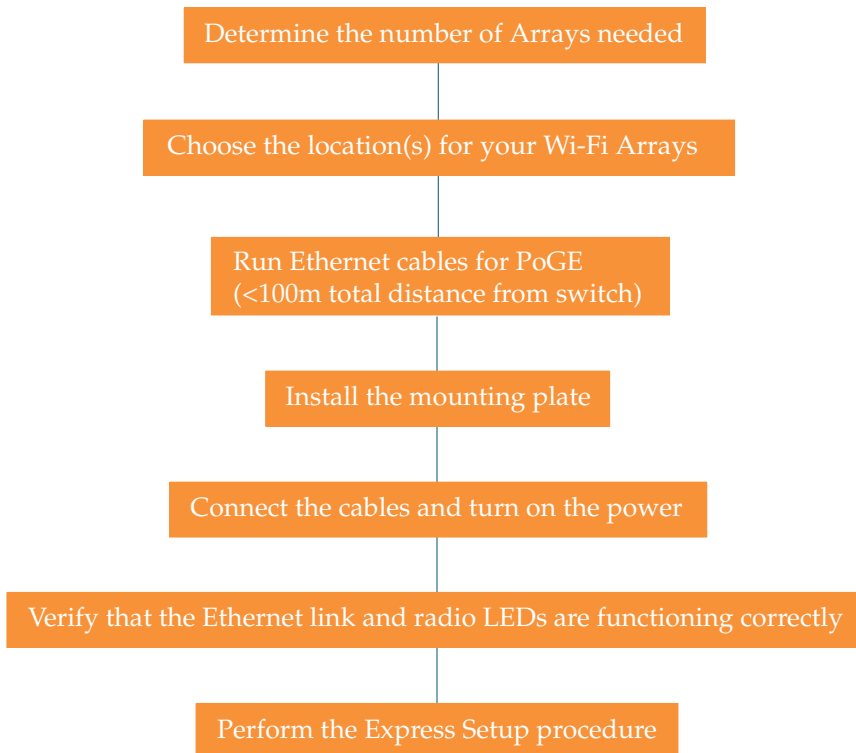


Figure 35. Installation Workflow

### *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

Product Specifications—XN16, XN12, and XN8

Product Specifications—XS16/XS-3900, and XS8/XS-3700

Product Specifications—XS4/XS-3500

Security Planning

## Unpacking the Wi-Fi Array

When you unpack your Array, you will find the following items in the carton:

Item	Quantity
Xirrus Wi-Fi Array	1
AC power cord (for AC-equipped models)	1
Console cable	1
Mounting plate	1
Mounting screws	4
Tile grid mounting clamps	4
Clamp nuts	4
Mounting template	1
CD-ROM containing: This User’s Guide in PDF format End User License Agreement (EULA) README file	1
Quick Install Guide	1
Registration Card	1

*See Also*

Installation Prerequisites

Installation Workflow



## 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. For wall mount instructions, go to [“Mounting Array on a Wall \(All models except 4-port Arrays\)”](#) on page 96.

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

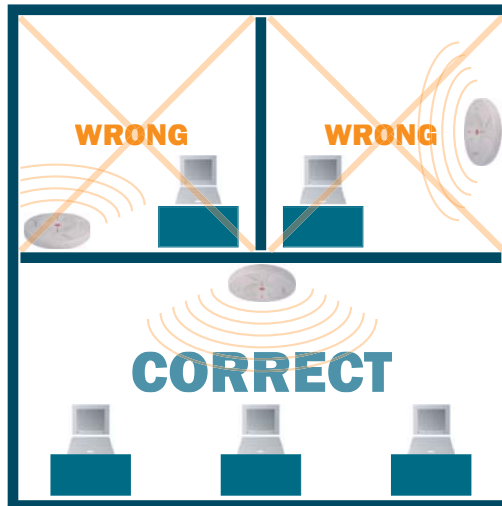


Figure 36. Array Placement

## Wiring Considerations

If you are using the Xirrus Power over Gigabit Ethernet modules (PoGE) to distribute power, see “Power over Gigabit Ethernet (PoGE)” on page 13. If you prefer to use AC power and you have an Array that supports AC, an AC power outlet must be available to the Array.

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

### Power

One of the following options:

- No power cable is required if using PoGE modules.
- Dedicated AC power if PoGE is not in use. A UL-approved cord is shipped with all AC-equipped Arrays. You must use a UL-approved cord if using AC power.

### Network

- Gigabit 1—If using PoGE modules, 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 (optional, not available on the four-port Arrays)
- Fast Ethernet (optional, not available on the four-port Arrays)
- 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 Fast Ethernet, 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 67.*

*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 342.*

#### ***See Also***

Failover Planning

Installation Prerequisites

Installation Workflow

Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500)

Mounting Array on a Wall (All models except 4-port Arrays)

Mounting the Array on a Ceiling

Power over Gigabit Ethernet (PoGE)

Unpacking the Wi-Fi Array

### Mounting the Array on a Ceiling

Most offices have drop-down acoustical ceiling tiles set into a standard grid. The Wi-Fi Array has been designed to enable mounting to a tiled ceiling via a mounting plate and clamps that attach to the grid. Once the mounting plate is attached, the Array simply rotates onto the plate (similar to a smoke detector). Once the unit is mounted it can be removed and re-attached easily, without the need for tools or modifications to the original installation.

This section assumes that you are mounting the Array to a tiled ceiling. If your ceiling is not tiled, the mounting plate can be attached directly to the ceiling with the screws and anchors provided (without using the tile grid mounting clamps).

### Attaching the T-Bar Clips to the Template

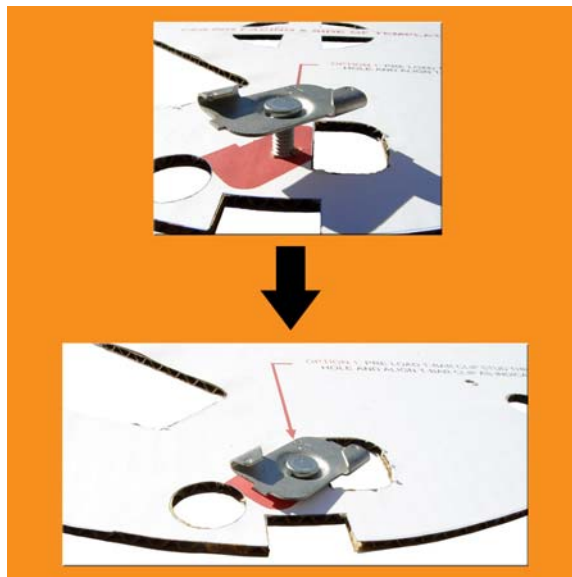


Figure 37. Attaching the T-Bar Clips to the Template

The T-bar clips create four mounting points on the ceiling tile grid for the Array mounting plate. Use the mounting template (provided) to find the correct location for all four clamps by pre-loading the 4 T-bar clips through the holes in the mounting template. Twist the clips until they are correctly aligned with the markings on the template.

### Secure the T-Bar Clips to the Ceiling Support Grid

The mounting template should be oriented so that the Array's **abg(n)2** omni-directional monitoring IAP (radio) is pointing in the direction of the least required wireless signal coverage—for example, a nearby exterior wall or entrance.

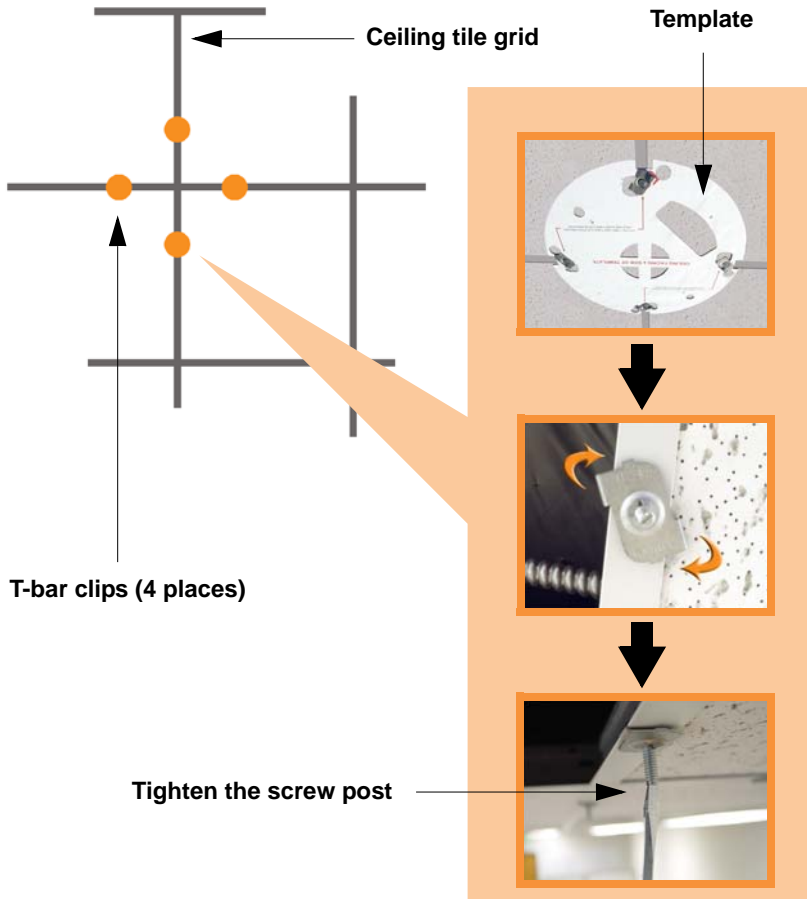


Figure 38. Attaching the T-Bar Clips to the Ceiling Grid

Use the mounting template to find the correct location for all four T-bar clips, then twist the clips onto the metal ceiling support grid (*Figure 38*). Tighten the screw posts to 10-12 lbf.ft (1.38-1.66 kgf.m). *Do not overtighten the screw posts.* Disengage the template from the four screw posts and remove the template from the ceiling.

### Installing the Mounting Plate

Locate the mounting plate on the four screw posts. Secure the plate to the four clamps using the nuts provided. Tighten the nuts to 10-12 lbf.ft (1.38-1.66 kgf.m), but *do not overtighten*.

Cut an access hole for the cables in the ceiling tile.

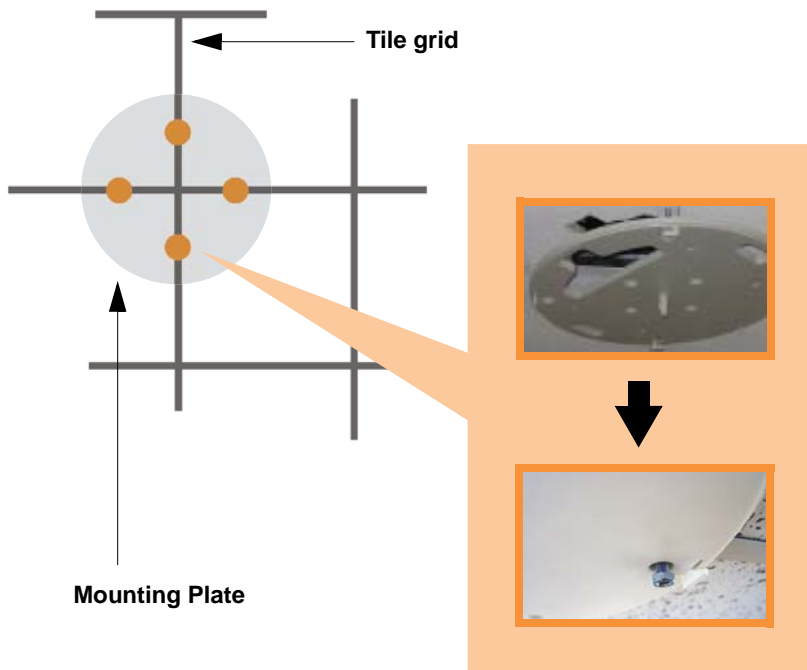


Figure 39. Installing the Mounting Plate

### Connecting the Cables—AC Option

This section is for Array models that have a separate AC input. If supplying AC to the Array directly (not using PoGE), refer to [Figure 40](#) to connect cables. Otherwise, skip to [Connecting the Cables—PoGE Option](#).

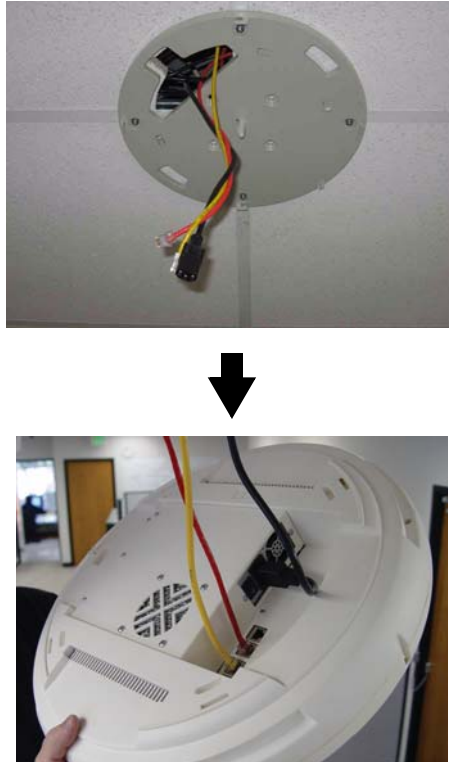


Figure 40. Connecting the Cables

Feed the power and Ethernet cables through the access hole in the tile and the mounting plate, then connect the cables to the Array. See also, [“Wiring Considerations”](#) on page 84.

- AC power cord—connect to AC source and AC socket on Array.
- Gigabit1 (mandatory)—the Array’s primary data and management port.

- Gigabit2 (optional)—may be used for load balancing, fail-over, mirroring, or increasing link speed to the wired network.
- Fast Ethernet (optional)—for a management-only connection to the Array.
- Serial cable (optional)—for connecting directly with the Array using CLI.

### Connecting the Cables—PoGE Option

For the XN16, XN12, XN8, XS8, or XS16, use the procedure below and refer to [Figure 41](#). For the XN4 or XS4, see “[For the XN4 or XS4:](#)” on page 91. All of these Array models have an integrated splitter, so an external splitter is not needed.

*For the XN16, XN12, XN8, XS8, or XS16:*

**Connect OUT ports to GIGABIT1 and GIGABIT2 ports with short cables**

**Connect Cat 5e from PoGE Injector to both IN ports.**

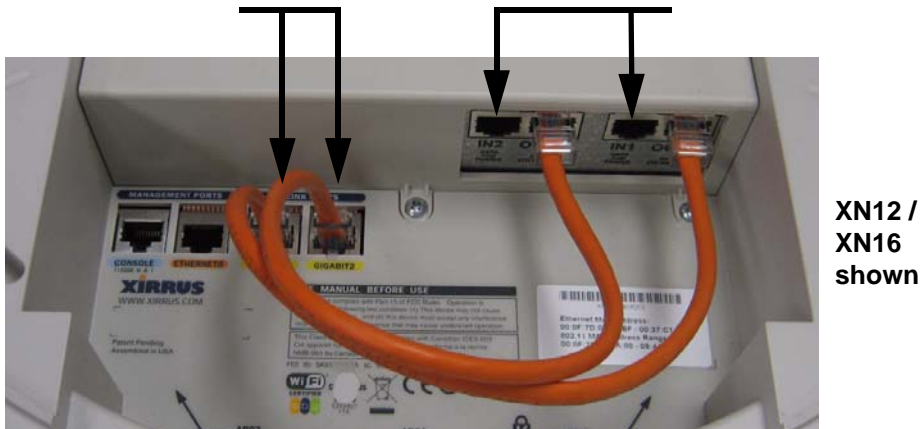


Figure 41. Connecting the Cables (Dual-PoGE connections shown)

The XN8 and the XS Arrays use one PoGE connection, while two connections are recommended for the XN12 or XN16 to support their higher bandwidth and provide redundancy. The connections may be provided using two ports on an XP2-MSI-95M or XP8-MSI-70M injector. This requires two gigabit network connections to the injector. If your application requires only one of the XN12/XN16 data ports, you may connect to a single port on the XP2-MSI-95M injector.



- Feed the Ethernet cable(s) through the access hole in the ceiling tile and the mounting plate.
- Connect the Cat 5e or Cat 6 data cable(s) coming from the PoGE injector(s) to the Array's Data and Power **IN** ports as described below and as shown in [Figure 41](#)—use one or two connections for the XN12 or XN16, and only one connection for the XN8, XS8, or XS16.

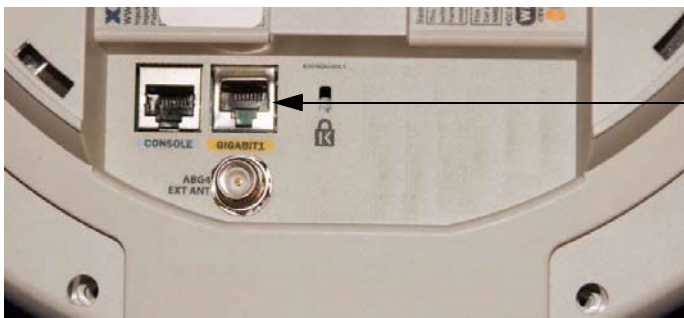


*Do not connect the cable from the injector directly to a Gigabit port! It must be connected to the **IN** port (towards the right in [Figure 41](#)).*

- XN8, XS8, and XS16: Connect a supplied short (about 6") orange Cat 5e cable from the Array's Data **OUT** port to **GIGABIT1**. Connect any additional Ethernet and serial cables as required.
- XN12 and XN16: Connect a supplied short orange Cat 5e cable from the Array's **OUT1** port to **GIGABIT1**, as shown. Similarly, connect **OUT2** to **GIGABIT2**. Connect any additional Ethernet and serial cables as required.

#### *For the XN4 or XS4:*

Feed the PoGE cable through the access hole in the ceiling tile and the mounting plate, then connect the cable to the Gigabit1 port on the Array. The Gigabit1 port is the data and management connection to the Array. A splitter is integrated with this port.



Connect Cat5e  
(from PoGE  
Injector)  
to **GIGABIT1**

**XN4, XS4**

Figure 42. Connecting the Cable (PoGE—XN4)

## Attaching the Array to the Mounting Plate



*Before attaching the Array to the mounting plate, verify that it is powering up. The Ethernet link LED lights up and the radio LEDs on the front of the unit will illuminate in rotation, indicating that the Wi-Fi Array software is loading and the unit is functioning correctly.*

### *Mounting all models except XS-3900/XS-3700*

Align the Array with the key post on the mounting plate, then turn the Array to the right to lock the unit into place at the 4 lugs—similar to a smoke detector.

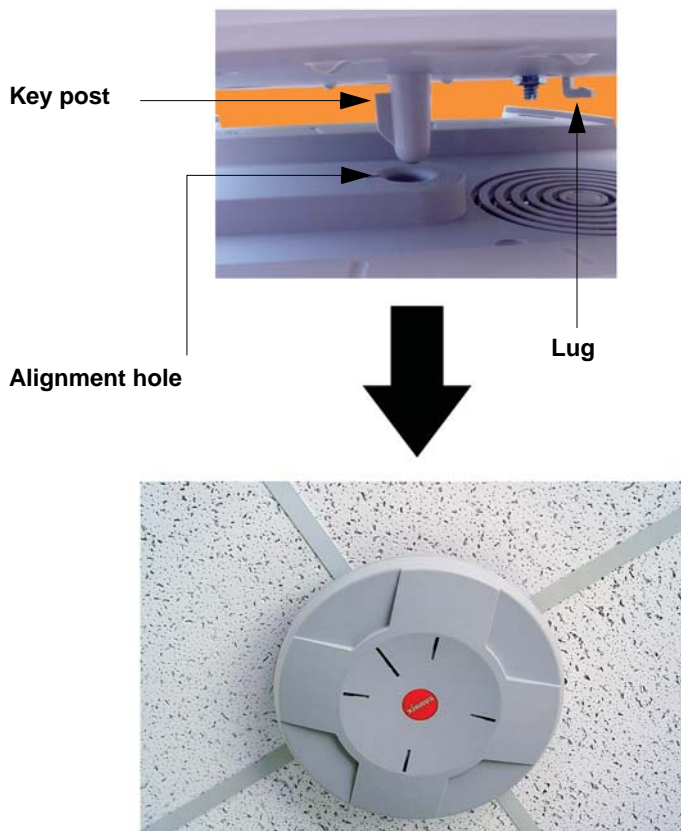


Figure 43. Attaching the Unit (XN4 shown)

*See Also*

Installation Workflow

Installing Your Wi-Fi Array

Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500)

Mounting Array on a Wall (All models except 4-port Arrays)

Securing the Array

***Mounting the XS-3900/XS-3700***

Align the port recess on the Array with the access hole in the mounting plate, then connect the Array with the lugs on the mounting plate (4 places) and turn the Array clockwise to lock the unit into place (similar to a smoke detector).



Figure 44. Attaching the Unit (XS-3900)

### Securing the Array

For added security, there is a locking bracket incorporated into the mounting plate, which will accept a small luggage-style padlock (if desired). There is also a Kensington lock slot located near the Ethernet ports. In addition, the mounting plate incorporates a positive locking tab that prevents the unit from being inadvertently released.



**Locking bracket**

Figure 45. Securing the Array

Now that the Array is physically installed, you must run the Express Setup procedure from the unit's Web Management Interface to enable the radios and establish initial system configuration settings. Go to [“Powering Up the Wi-Fi Array”](#) on page 107.

#### *See Also*

Installation Workflow

Installing Your Wi-Fi Array

Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500)

Mounting Array on a Wall (All models except 4-port Arrays)

Mounting the Array on a Ceiling

Powering Up the Wi-Fi Array

## Dismounting the Array

### *To dismount the XS-3700/3900*

To dismount the Array, place your fingers so as to increase the space between the Array and the mounting plate at the positions indicated by the decals on the mounting plate—these are aligned with IAPs (radios) abg(n)1 and abg(n)3, as indicated on the clock-face of the Array.

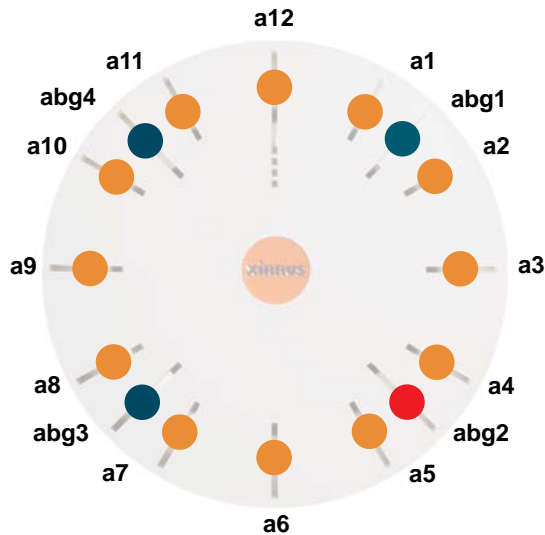


Figure 46. IAP Positions (XS16 shown)

### *To dismount any other Array model*

For all Array models other than the XS-3700/3900, 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.

### *See Also*

[Installation Workflow](#)

[Installing Your Wi-Fi Array](#)

[Mounting the Wi-Fi Array on a Wall \(XS4 and XS-3500\)](#)

[Mounting Array on a Wall \(All models except 4-port Arrays\)](#)

[Mounting the Array on a Ceiling](#)

## Securing the Array

### Mounting Array on a Wall (All models except 4-port Arrays)

This procedure is applicable to the Wi-Fi Array's 16-radio models, 12-radio models, and 8-radio models. If you are mounting a 4-radio model, go to "Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500)" on page 101.

The wall mounting assembly kit is used to mount the Wi-Fi Array (except for 4-port models) on a wall, instead of the traditional ceiling mount—if mounting the Array on the ceiling is impractical at your location.

### Kit Contents (Wall Mount Assembly)

The wall mount assembly kit includes the following items:

- 5 x SNAPTOGGLE™ toggle bolts (for attaching the wall bracket to the wall)
- 4 x 1/4 inch bolt assemblies (for attaching the mounting plate to the wall bracket)
- Wall Mounting Bracket

### Tools Required

- Power drill
- 1/2 inch (13mm) drill bit
- Cross head screwdriver
- 1/4 inch nut wrench
- Pencil
- Level

### Mark the Wall Position

1. Use the Wall Mounting Bracket as a template and mark the locations on the wall for the mounting holes.

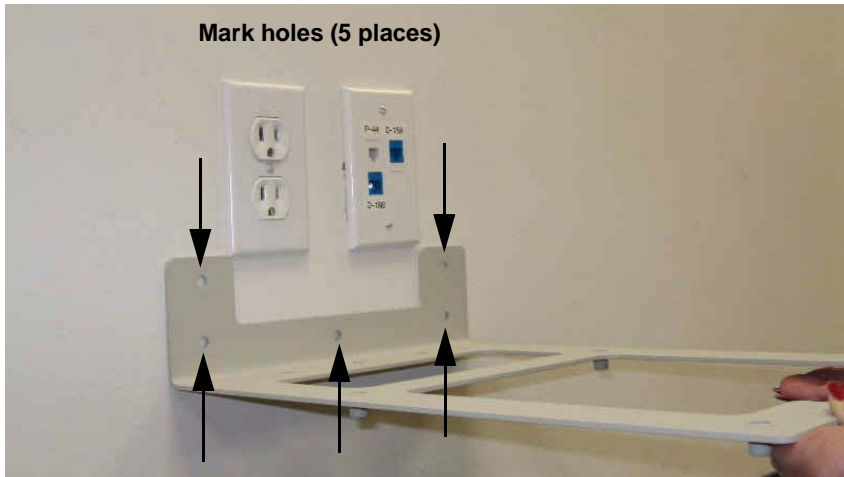


Figure 47. Wall Mount—Marking the Holes

When marking the holes, ensure that the mounting plate is level—you may need assistance.



*The bracket must be secured to the wall in 5 places, using the 2 holes at the top and the 3 holes at the bottom (5 toggle bolts are provided).*

### Install the SNAPTOGGLE™ Toggle Bolts

2. At the locations you marked in Step 1, drill a 1/2 inch (13mm) hole (there must be a minimum clearance behind the wall of 1 7/8 inches—48mm).
3. (Refer to [Figure 48](#), graphic **A**) Hold the metal channel flat alongside the plastic straps and slide the channel through the hole.

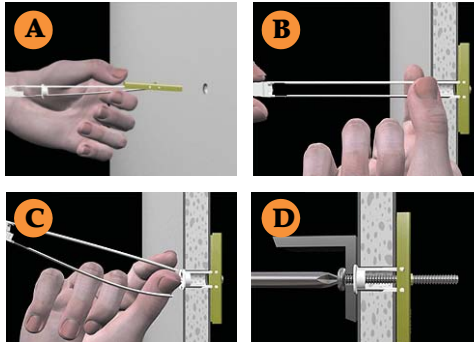


Figure 48. Installing the Toggle Bolts

4. (Refer to [Figure 48](#), graphic **B**) Hold the strap handle between your thumb and forefinger and pull towards you until the metal channel rests flush behind the wall.

Using your other hand, now slide the plastic cap along the straps until the flange of the cap is flush with wall.

*The straps provide a one-way ratcheting mechanism (similar to a cable tie). Ensure that the toggle bolt assembly is oriented correctly (as shown) before sliding the plastic cap along the straps.*

5. (Refer to [Figure 48](#), graphic **C**) Break the straps at the wall, flush with the flange of the cap. The straps can be broken by pushing them from side-to-side and simply snapping them off.

[Figure 48](#), Graphic **D** shows a cutaway example of how the toggle bolt is used to secure an item to the wall (in our case, the item is the Wall Mounting Bracket—secured to the wall with 5 toggle bolts).

*Do not attach the Wall Mounting Bracket to the wall at this time.*



**Attach the Mounting Plate to the Wall Mounting Bracket**

6. Secure the Wi-Fi Array's mounting plate to the Wall Mounting Bracket, in 4 places. Tighten the bolts to a torque of 10–12 lbf.ft (1.38–1.66 kgf.m).

*Do not overtighten the bolts.*

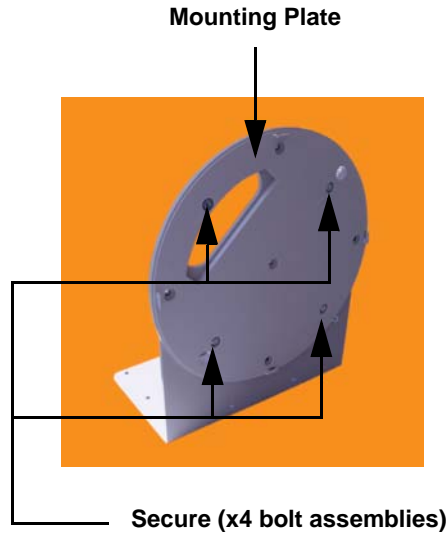


Figure 49. Attaching the Wall Mounting Plate

**Attach the Wall Mounting Bracket/Plate Assembly to the Wall**

7. Secure the Wall Mounting Bracket (with attached Mounting Plate) to the wall at the 5 toggle bolt anchors you created in Steps 1 through 5—using all 5 places.

**Mount the Array**

8. Mount the Wi-Fi Array to the Wall Mounting Bracket in the same way that you would mount the Array to a ceiling mount (the procedure is identical). See “Attaching the Array to the Mounting Plate” on page 92 or “Mounting the XS-3900/XS-3700” on page 93.



*Figure 50 shows the orientation of the Wi-Fi Array when mounted on a wall. It is not intended to show a fully installed Array.*



Figure 50. Mounting the Array on a Wall

**See Also**

Installation Workflow

Installing Your Wi-Fi Array

Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500)

Mounting the Array on a Ceiling

Securing the Array

### Mounting the Wi-Fi Array on a Wall (XS4 and XS-3500)

This procedure is applicable to the 4 radio models of the Wi-Fi Array (XS4 and XS-3500). If you are mounting a 16-, 12-, or 8-radio model, go to “[Mounting Array on a Wall \(All models except 4-port Arrays\)](#)” on page 96.

The wall mounting assembly kit is used to mount a 4-port Wi-Fi Array on a wall, instead of the traditional ceiling mount—where mounting the Array on the ceiling may be impractical at your location.

### Kit Contents (Wall Mount Assembly)

The wall mount assembly kit includes the following items:

- 5 x SNAPTOGGLE™ toggle bolts (for attaching the wall bracket to the wall)
- 4 x 1/4 inch bolt assemblies (for attaching the mounting plate to the wall bracket)
- Wall Mounting Bracket

### Tools Required

- Power drill
- 1/2 inch (13mm) drill bit
- Cross head screwdriver
- 1/4 inch nut wrench
- Pencil
- Level

### Mark the Wall Position

1. Use the Wall Mounting Bracket as a template and mark the locations on the wall for the mounting holes.

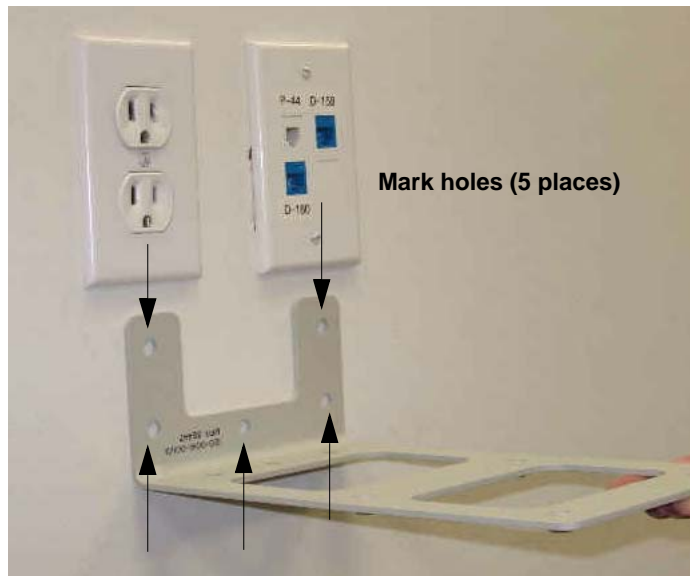


Figure 51. Wall Mount—Marking the Holes

The bracket must be secured to the wall in 5 places, using the top 2 holes and the bottom 3 holes (5 toggle bolts are provided).

When marking the holes, ensure that the mounting plate is level—you may need assistance.

### Install the SNAPTOGGLE™ Toggle Bolts

2. At the locations you marked in Step 1, drill a 1/2 inch (13mm) hole (there must be a minimum clearance behind the wall of 1 7/8 inches—48mm).

3. (Refer to [Figure 52](#), graphic **A**) Hold the metal channel flat alongside the plastic straps and slide the channel through the hole.

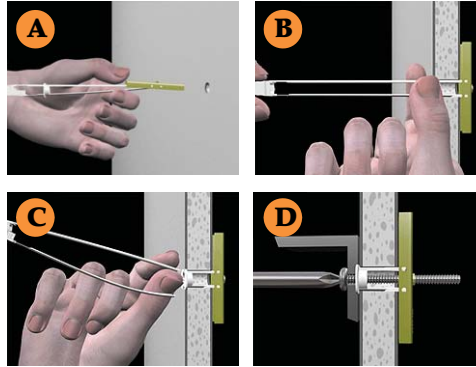


Figure 52. Installing the Toggle Bolts

4. (Refer to [Figure 52](#), graphic **B**) Hold the strap handle between your thumb and forefinger and pull towards you until the metal channel rests flush behind the wall.

Using your other hand, now slide the plastic cap along the straps until the flange of the cap is flush with wall.

*The straps provide a one-way ratcheting mechanism (similar to a cable tie). Ensure that the toggle bolt assembly is oriented correctly (as shown) before sliding the plastic cap along the straps.*

5. (Refer to [Figure 52](#), graphic **C**) Break the straps at the wall, flush with the flange of the cap. The straps can be broken by pushing them from side-to-side and simply snapping them off.

[Figure 52](#), Graphic **D** shows a cutaway example of how the toggle bolt is used to secure an item to the wall (in our case, the item is the Wall Mounting Bracket—secured to the wall with 5 toggle bolts).

*Do not attach the Wall Mounting Bracket to the wall at this time.*

**Attach the Mounting Plate to the Wall Mounting Bracket**

6. Secure the Wi-Fi Array's mounting plate to the Wall Mounting Bracket, in 4 places.

Tighten the bolts to a torque of 10–12 ft-lb (1.38–1.66 kg.m).

Do not overtighten the bolts.

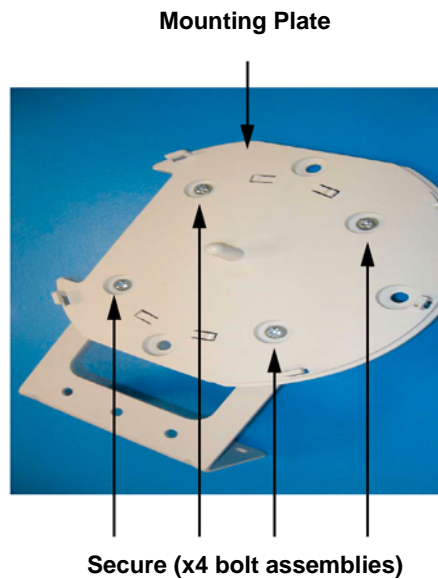


Figure 53. Attaching the Array Mounting Plate

**Attach the Wall Mounting Bracket/Plate Assembly to the Wall**

7. Secure the Wall Mounting Bracket (with attached Mounting Plate) to the wall at the 5 toggle bolt anchors you created in Steps 2 through 5—using all 5 places.



Figure 54. Attaching the Wall Mounting Bracket to the Wall

**Mount the Array**

8. Mount the Wi-Fi Array to the Wall Mounting Bracket by positioning the key post (on the underside of the mounting bracket) into the key receptacle on the underside of the Array.

When the key post is properly located, gently turn the Array in a clockwise direction to secure the Array to the mounting plate.



Figure 55. Mounting the Array on a Wall



### Removing the Array

To remove the Array from the Wall Mount Assembly, simply apply a little upward pressure to the Array, then gently turn the Array in a counterclockwise direction to release the unit from the bracket.

#### *See Also*

[Installation Workflow](#)

[Installing Your Wi-Fi Array](#)

[Mounting Array on a Wall \(All models except 4-port Arrays\)](#)

[Mounting the Array on a Ceiling](#)

[Securing the Array](#)

### 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.

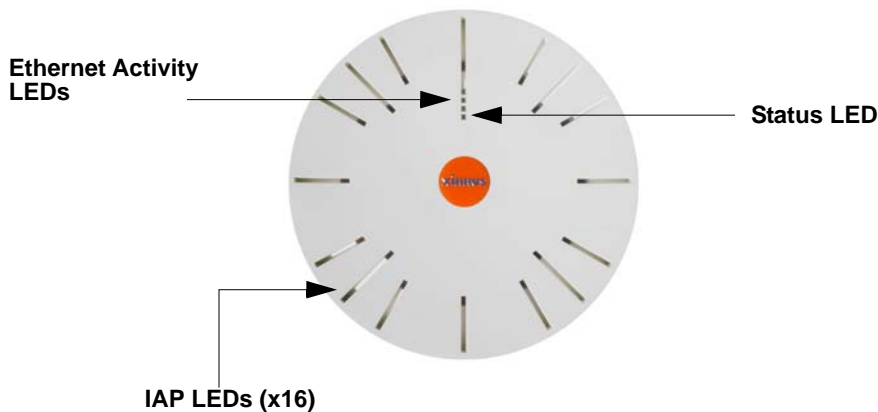


Figure 56. LED Locations (XS-3900)

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 285.

## Array LED Operating Sequences

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

### 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 RED	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, and OFF for IAPs that are down

## LED Operation when Array is Running

The normal LED operation when the Array is running is as follows:

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>	IAP <b>abg(n)2</b> 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](#)

## Establishing Communication with the Array

The Array can be configured through the Command Line Interface (CLI) or 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.

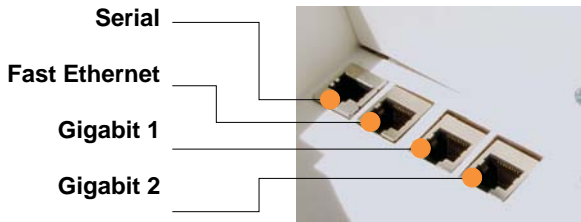


Figure 57. Network Interface Ports

### 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 on either the Fast Ethernet or Gigabit Ethernet ports, the Fast Ethernet port will default to an IP address of 10.0.1.1 and 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 two methods:

1. Examine the DHCP tables on the server and find the addresses assigned to the Array (Xirrus MAC addresses begin with 000F7D).
2. Query the Array using the CLI via the serial port. Use the **show ethernet** command to view the IP addresses assigned to each port.

---

## 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](#)

## 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-XNB ( 10.100.47.186 )	Location: SS Area	Uptime: 1 day, 23 hours, 19 minutes
Array	Host Name:	SS-XNB	
Network	Location Information:	SS Area	
RF Monitor	Admin Contact:	J Smith	
Stations	Admin Email:	jsa@xyzcorp.com	
Statistics	Admin Phone:	805-555-1212	
System Log			
<b>Configuration</b>	<b>SNMPv2 Settings</b>		
Express Setup	Enable SNMPv2:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Network	Read-Only Community String:	*****	
Services	Read-Write Community String:	*****	
VLANs	<b>10/100 Ethernet 0 Settings</b>		
Security	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
SSIDs	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
Groups	IP Address:	10.10.10.21	
IAPs	IP Subnet Mask:	255.255.255.0	
WDS	Default Gateway:	10.10.10.1	
Filters	<b>Gigabit Ethernet 1 Settings</b>		
Tools	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
System Tools	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
CLI	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	
Logout	IP Address:	10.10.10.186	
Log Messages	IP Subnet Mask:	255.255.255.0	
Critical 6	Default Gateway:	10.10.10.1	
Warning 6	<b>SSID Settings</b>		
Information 5(0)	SSID (Wireless Network Name):		
	Wireless Security:	Open	
	<b>Admin Settings</b>		
	New Admin User (Replaces user "admin"):	private	
	New Admin Password:	*****	
	Confirm Admin Password:	*****	
	<b>Time and Date Settings</b>		
	TimeZone:	(GMT - 08:00) Pacific Time (US & Canada), Tijuana	
	Auto Adjust Daylight Savings:	<input checked="" type="checkbox"/>	
	Use Network Time Protocol:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
	NTP Primary Server:	time.nist.gov	
	NTP Secondary Server:	pool.ntp.org	
	<b>IAP Settings</b>		
	Enable/Configure All IAPs:	Execute	
		Apply	Save

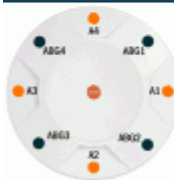


Figure 58. Express Setup

---

## 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 199.
7. **Configure the Fast Ethernet (10/100 Megabit), 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 209](#).

- c. **Wireless Key/Passphrase:** Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase.
  - d. **Confirm Key/Passphrase:** If you entered a WEP key or WPA passphrase, confirm it here.
9. **Admin Settings:** This section allows you to change the default password for the Array. Note that the Array also offers the option of authenticating administrators using a RADIUS server (see [“Admin Management” on page 214](#)).
  - a. **New Admin Password:** If desired, enter a new administration password for managing this Array. Choose a password that is not obvious, and one that you can remember. If you forget your password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
  - b. **Confirm Admin Password:** If you entered a new administration password, confirm the new password here.

- 10. Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you're not using a server.
- a. Time Zone:** Select your time zone from the choices available in the pull-down list.
  - b. Use Network Time Protocol:** Check this box if you want to use an NTP server to synchronize the Array's clock. This ensures that Syslog time-stamping is maintained across all units. Without an NTP server assigned (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies. If you check **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, leave this box unchecked (default) and set the system time on the Array manually.
  - c. NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
  - d. 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.
  - e. Set Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes, seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).
  - f. Set Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, the date fields become active. Enter the revised date (month, day and year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).
  - g. 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).

## 11. IAP Settings:

**Enable/Configure All IAPs:** Click on the **Execute** button to enable and auto configure all IAPs (a message displays the countdown time—in seconds—to complete the auto-configuration task). When an IAP is enabled, its LED is switched on. (Figure 59)



Figure 59. LEDs are Switched On

12. Click on the **Apply** button to apply the new settings to this session
13. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

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.

The screenshot displays the 'XN8 Wi-Fi Array' web management interface. The top header shows the device name '55-XN8 (10.109.47.186)', location '55 Area', and uptime '1 day, 23 hours, 24 minutes'. A left-hand navigation menu includes sections like Status, Configuration, Tools, and Log Messages. The main content area is titled 'RADIUS Server Mode' and is set to 'External'. Below this, 'WPA Settings' are shown with 'TKIP Enabled' and 'AES Enabled' both checked. 'WPA Group Rekey Time' is set to 'Never'. 'PSK Authentication' is set to 'No'. Under 'WPA Preshared Key / Verify Key', 'ASCII' is selected. 'EAP Authentication' is set to 'Yes'. The 'WEP Settings' section contains four rows for 'Encryption Key 1 / Verify Key 1' through '4', each with a masked key field and radio buttons for 'ASCII', 'Hexadecimal', '40 bit (WEP-64)', and '104 bit (WEP-128)'. The 'Default Key' is set to 'Key 2'. 'Apply' and 'Save' buttons are at the bottom right. A circular diagram of the device with antenna ports is shown in the bottom left, and a copyright notice 'Copyright © 2005-2008 by Xirus, Inc.' is in the bottom right.

Figure 60. 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> </ul> </li> <li>RF Monitor Windows             <ul style="list-style-type: none"> <li>IAPs</li> <li>Spectrum Analyzer</li> <li>Intrusion Detection</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> </ul> </li> </ul> <p><b>Configuration Windows</b></p> <ul style="list-style-type: none"> <li>Express Setup</li> <li>Network             <ul style="list-style-type: none"> <li>Network Interfaces</li> <li>DNS Settings</li> <li>CDP Settings</li> </ul> </li> </ul>	<p><b>Configuration Windows (cont'd)</b></p> <ul style="list-style-type: none"> <li>Services             <ul style="list-style-type: none"> <li>Time Settings (NTP)</li> <li>NetFlow</li> <li>System Log</li> <li>SNMP</li> <li>DHCP Server</li> </ul> </li> <li>VLANs             <ul style="list-style-type: none"> <li>VLAN Management</li> </ul> </li> <li>Security             <ul style="list-style-type: none"> <li>Admin Management</li> <li>Admin RADIUS</li> <li>Management Control</li> <li>Access Control List</li> <li>Global Settings</li> <li>External Radius</li> <li>Internal Radius</li> <li>Rogue Control List</li> </ul> </li> <li>SSIDs             <ul style="list-style-type: none"> <li>SSID Management</li> </ul> </li> <li>Groups             <ul style="list-style-type: none"> <li>Group Management</li> </ul> </li> <li>IAPs             <ul style="list-style-type: none"> <li>IAP Settings</li> <li>Global Settings (IAP)</li> <li>Global Settings .11a</li> <li>Global Settings .11bg</li> <li>Global Settings .11n</li> <li>Advanced RF Settings</li> <li>LED Settings</li> </ul> </li> <li>WDS             <ul style="list-style-type: none"> <li>WDS Client Links</li> </ul> </li> <li>Filters             <ul style="list-style-type: none"> <li>Filter Lists</li> <li>Filter Management</li> </ul> </li> </ul>
--	---

<b>Statistics Windows</b> <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>	<b>System Log Window</b> <b>Tool Windows</b> <ul style="list-style-type: none"><li>System Tools</li><li>CLI</li><li>Logout</li></ul>
---	---



## 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.

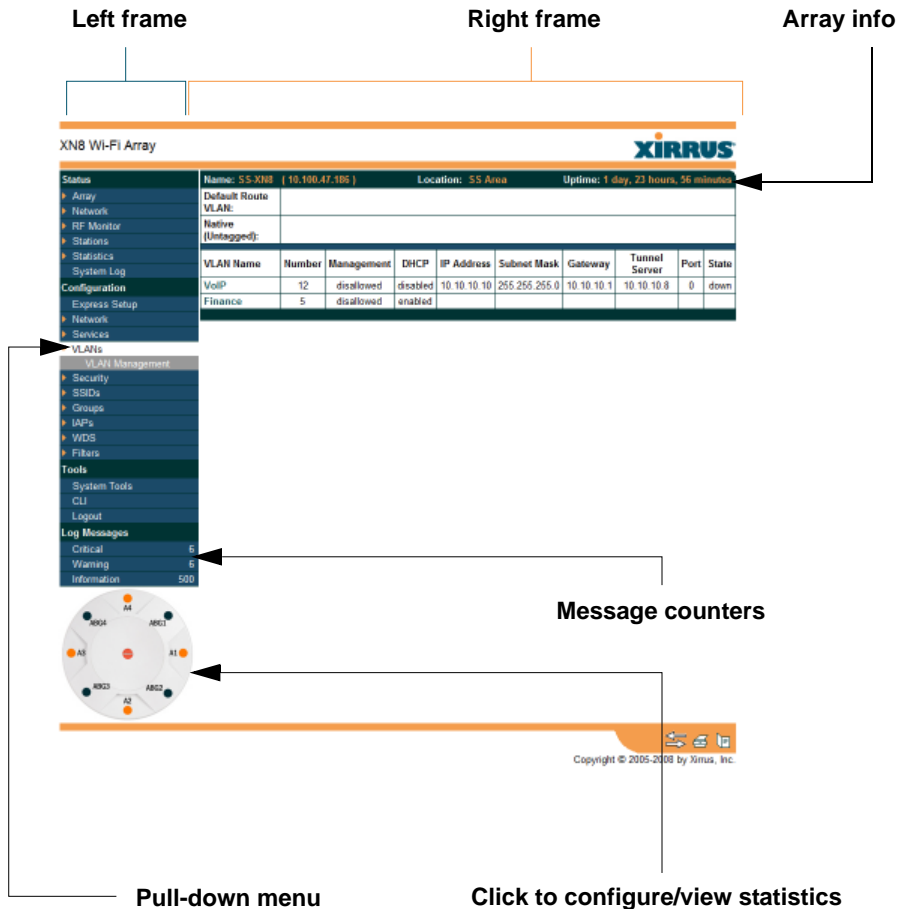


Figure 61. WMI: Frames

The left frame contains three main elements:

- Configuration menu organized by function (for example, radio interfaces, security, etc.). Click the heading to display a summary of its current configuration, as well as an associated pull-down menu.
- 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.
- 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.

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.

### 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.

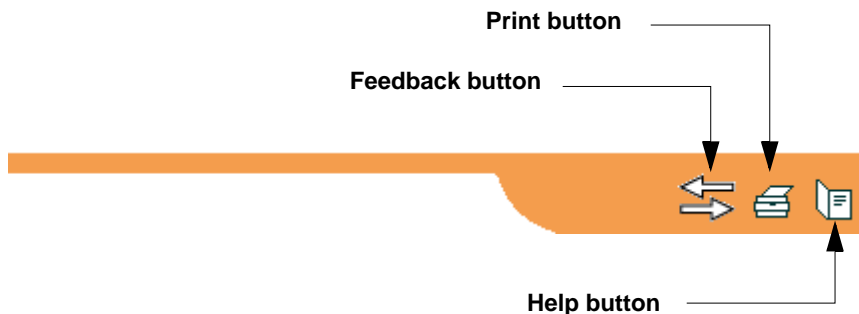


Figure 62. WMI: Utility Buttons

- 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 63 on page 125 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, 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.

Figure 63. 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. Connect to the Wi-Fi Array via its default IP address (10.0.2.1 for both Gigabit 1 and Gigabit 2 Ethernet ports) or via a DHCP assigned IP address.
3. To log in to the Array's Web Management Interface, enter **admin** when prompted for a user name and password.

Name: SS-XNB (10.100.47.106)	Location: SS Area
Current Status:	Logged Out
User Name:	admin
User Password:	*****

Login

Figure 64. Logging In to the Wi-Fi Array

## Applying Configuration Changes

When you have defined all your settings in any WMI configuration window, you must click on the **Apply** button for the changes to take effect in the current session, or click on the **Save** button to apply changes to this session and write your changes, so they will be preserved after a reboot.

### *See Also*

[Key Features and Benefits](#)

[Wi-Fi Array Product Overview](#)

# 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 127](#)
- [“Network Status Windows” on page 133](#)
- [“RF Monitor Windows” on page 142](#)
- [“Station Status Windows” on page 150](#)
- [“Statistics Windows” on page 164](#)
- [“System Log Window” on page 172](#)

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

- [“Configuring the Wi-Fi Array” on page 173](#)
- [“Using Tools on the Wi-Fi Array” on page 299](#)

## 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.

Status		Name: SS.XN8 (10.100.47.186)		Location: SS Area		Uptime: 0 days, 0 hours, 36 minutes				
<b>Ethernet Interfaces</b>										
Interface	Status	Link	Port Mode	DHCP	IP Address	Subnet Mask	Gateway			
10/100 Ethernet 0	Enabled	down		Disabled	10.100.47.21	255.255.255.0	10.100.47.1			
Gigabit Ethernet 1	Enabled	up	link-backup	Disabled	10.100.47.186	255.255.255.0	10.100.47.1			
Gigabit Ethernet 2	Enabled	down	link-backup	Disabled	10.100.47.186	255.255.255.0	10.100.47.1			
<b>Integrated Access Points</b>										
IAP	State	Channel	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link	MAC Address / BSSID	Description
abgn1	down	1	int-dir	max	20	-90	0		00:0f:7d:0b:b3:9d-91	
abgn2	up	monitor	int-omni	monitor	20	-95	0		00:0f:7d:0b:b3:b0-b1	
abgn3	down	11	int-dir	max	20	-90	0		00:0f:7d:0b:b3:d0-d1	
abgn4	up	6	int-dir	medium	12	-81	1		00:0f:7d:0b:b3:f0-f1	
an1	down	40	int-dir	medium	12	-81	0		00:0f:7d:0b:b3:a0-a1	
an2	down	56	int-dir	max	20	-90	0		00:0f:7d:0b:b3:c0-c1	
an3	down	48	int-dir	max	20	-90	0		00:0f:7d:0b:b3:e0-e1	
an4	down	64	int-dir	max	20	-90	0		00:0f:7d:0b:b3:80-81	

Figure 65. 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 181.

- **Interface:** Lists the network interfaces that are available on the Array (10/100 Ethernet 0, 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 (16 IAPs for the XN16, XS16, or XS-3900; 12 IAPs for the XN12; 8 IAPs for the XN8, XS8, or XS-3700; and 4 IAPs for the XN4, XS4 or XS-3500). To make configuration changes to these IAPs, go to [“IAP Settings” on page 256](#).

- **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 66](#) shows an example where IAP a3 is down.

Integrated Access Points										
IAP	State	Channel	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link	MAC Address / BSSID	Description
abgn1	up	1	int-dir	max	20	-90	0		00:0f:7d:0b:b3:90-91	
abgn2	up	monitor	int-omni	monitor	20	-95	0		00:0f:7d:0b:b3:b0-b1	
abgn3	down	11	int-dir	max	20	-90	0		00:0f:7d:0b:b3:d0-d1	
abgn4	up	6	int-dir	medium	12	-81	1		00:0f:7d:0b:b3:f0-f1	
an1	up	40	int-dir	medium	12	-81	0		00:0f:7d:0b:b3:a0-a1	
an2	up	56	int-dir	max	20	-90	0		00:0f:7d:0b:b3:c0-c1	
an3	up	48	int-dir	max	20	-90	0		00:0f:7d:0b:b3:e0-e1	
an4	down	64	int-dir	max	20	-90	0		00:0f:7d:0b:b3:80-81	

Figure 66. 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 256](#).
- **Antenna:** Shows which antenna is being used by each IAP.
- **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 256](#). 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 50](#).

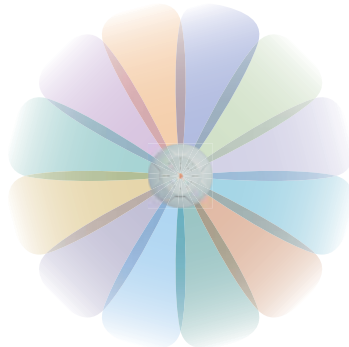


Figure 67. IAP Cells

- **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. All Arrays can handle up to 64 concurrent users per individual IAP, thus 16-port models can handle 1024 users per Array.
- **WDS Link:** The WDS Link on this radio (if any). See [“WDS” on page 287](#).
- **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.

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.

XN4 Wi-Fi Array		XIRRUS		
Status	Name: SS-XN0429091D207 ( 10.100.47.19 )		Uptime: 0 days, 0 hours, 13 mins	
Array	Hardware Configuration			
Summary	Model	XN4, 512MB-ECC (825Mhz)		
Information	Component	Part Number	Serial Number	Date
Configuration	Array	180-0035-001	XN0429091D207	2009-Jul-14 22:38
Admin History	Controller	100-0092-002.A	0000047117	2009-Jul-07 19:24
Network	IAP Module 1	100-0089-001.C	0000050577	2009-Jul-14 6:07
RF Monitor	IAP Module 2	100-0089-001.C	0000050570	2009-Jul-14 6:03
Stations	IAP Module 3	100-0089-001.C	0000050489	2009-Jul-14 7:12
Statistics	IAP Module 4	100-0089-001.C	0000050364	2009-Jul-13 19:07
System Log	FPGA Status	Boot Version	SW Version	
Configuration	Switching Engine	2000-02.022	2000-02.028	
Express Setup	Queue Processing	2002-02.037	2002-02.047	
Network	Interface	MAC Address(es)		
Services	IAPs	00:0f:7d:14:cb:80-14:cb:bf		
VLANs	Gigabit 1	00:0f:7d:00:b8:0d		
Security	Software Configuration			
SSIDs	Component	Version		
Groups	SCD Firmware	2.21 (Aug 27 2008), Build: 3157		
IAPs	Boot Loader	1.0.0 (Dec 17 2008), Build: 3090		
WDS	IAP Driver	1.5.0 (Dec 31 2009), Build: 2115		
Filters	System Software	4.0.7 (Dec 31 2009), Build: 1192		
Tools	License Key	0x4GF-PU3EV-8GGAF-M0JC7		
System Tools	License Features	Basic ArrayOS + Advanced RF Management + 802.11n		
CLI	Operating Status			
Logout	Time This Boot	Tue 2010-Jan-05 23:06:31 GMT		
Log Messages	Time Last Boot	Wed 2009-Dec-30 22:38:44 GMT		
Critical 1	Component	Temperature (C/F)		
Warning 1	Controller	32/89		
Information 13	IAP Module 1	34/93		
	IAP Module 2	29/84		
	IAP Module 3	31/87		
	IAP Module 4	37/98		

Figure 68. Array Information

## Array Configuration

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

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

The screenshot shows the 'XN8 Wi-Fi Array' configuration window. The top bar indicates the array name 'SS-XN8 (10.100.47.186)', location 'SS Area', and uptime '0 days, 2 hours, 2 minutes'. The 'Array' section is expanded to show configuration details. The 'Select Config' dropdown is set to 'Running' and 'Include Defaults' is checked. The configuration output is as follows:

```

!
configure
!
description
hostname SS-XN8
location "SS Area"
exit
!
contact-info
name "J Smith"
phone "805-555-1212"
email "jss@xyzcorp.com"
exit
!
array-info
! hardware-configuration
! =====
! model: XN8, 1.0GB (1.0GHz)
!
!
! component      part number      serial number     date
! -----
! array          180-0036-001     XN0839081AD18    2008-Sep-23 21:08
! controller    100-0030-012.G1  0000017991        2008-Sep-16  0:50
! iap module 1  100-0091-002.B2  0000022947        2008-Sep-16 11:00
! iap module 2  100-0091-002.B2  0000022933        2008-Sep-16 11:14
! iap module 3  100-0091-002.B2  0000022932        2008-Sep-16 12:37
! iap module 4  100-0091-002.B2  0000023089        2008-Sep-23  9:57
!
! fpga status      boot version     s/w version
! -----
    
```

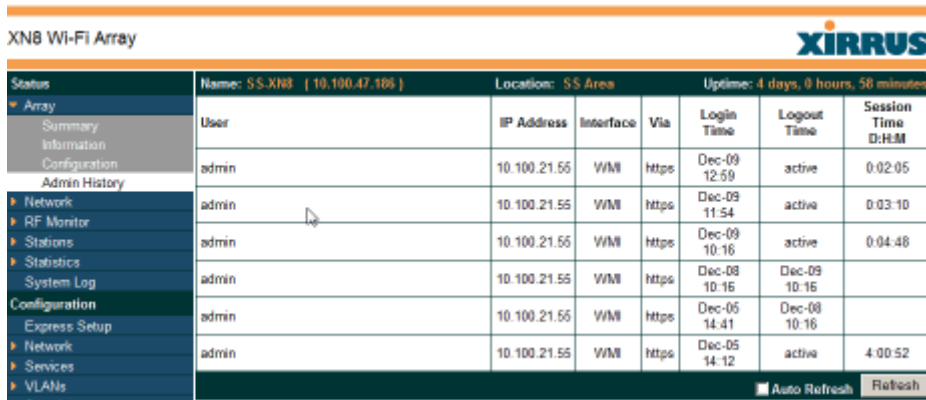
Figure 69. Show Configuration

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

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

## Admin History

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



Status	Name: S5-XNB [10.100.47.106]	Location: S5 Area			Uptime: 4 days, 0 hours, 58 minutes		
<ul style="list-style-type: none"> <li>Array               <ul style="list-style-type: none"> <li>Summary</li> <li>Information</li> <li>Configuration</li> <li>Admin History</li> </ul> </li> <li>Network</li> <li>RF Monitor</li> <li>Stations</li> <li>Statistics</li> <li>System Log</li> <li>Configuration               <ul style="list-style-type: none"> <li>Express Setup</li> </ul> </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 10:16	Dec-09 10:16	
	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 70. Admin Login History

## Network Status Windows

The following Network Status windows are available:

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

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

## Network Map

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

Status	Name: SS XNB [10.100.47.105]	Location: SS Area				Uptime: 0 days, 0 hours, 1 minute					
Array	Array Name	IP Address	Location	Array OS	IAP	Up	SSID	On	In Range	Fast Roam	Uptime D:H:M
Network	SS XNB	10.100.47.106	SS Area	XS-4.0.2-1075	8	2	2	2	yes	yes	0:00:01
Network Map	XS0037001AAEE	10.100.49.137		XS-3.5-0694	8	1	16	16			1:21:24
	XS0037001AAD5	10.100.49.124		XS-3.5-0694	8	1	16	16			1:21:37
Spanning Tree Status	X54	10.100.48.17		XS-4.0.2-1075	4	4	1	1			0:05:48
Routing Table	XS16170019B92	10.100.48.11		XS-4.0.2-1075	16	16	1	1			0:05:51
ARP Table	XS0038001AC21	10.100.49.106		XS-3.5-0694	8	1	16	16			1:21:24
DHCP Leases	XS1444001B4D8	10.100.49.155		XS-3.5-0694	4	1	1	1			1:21:34
Connection Tracking	X1370606002B1	10.100.48.14		XS-4.0.2-1075	8	8	1	1			0:05:51
CDP Neighbors	XN0050001BA86	10.100.49.181		XS-4.0.2-1074	8	1	1	1			0:22:51
RF Monitor	XN0050001BA88	10.100.49.191		XS-4.0.2-1074	8	1	1	1			1:23:52
Stations	XN0049001BA9F	10.100.49.151		XS-4.0.2-1075	8	1	1	1			0:00:11
Statistics	XN0050001BA73	10.100.49.182		XS-4.0.2-1074	8	1	1	1			2:00:09
System Log	XS0038001AC42	10.100.49.144		XS-3.5-0694	8	1	16	16			1:21:38
Configuration	X1335207104ED	10.100.48.19		XS-4.0.2-1075	4	4	1	1			0:05:47
Express Setup											
Network											
Services											

Figure 71. Network Map

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

## Content of the Network Map Window

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

- **Array Name:** The host name assigned to the Array. To establish the host name, go to “Express Setup” on page 174. 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 174](#).

- **Location:** The location assigned to the Array. To establish the location information, go to [“Express Setup” on page 174](#).
- **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 174](#). To enable or disable individual IAPs, go to [“IAP Settings” on page 256](#).
- **SSID:** Informs you how many SSIDs have been assigned for the Array. To assign an SSID, go to [“SSID Management” on page 240](#).
- **(SSID) On:** Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to [“SSID Management” on page 240](#).
- **In Range:** Informs you whether the Array is within wireless range of another Wi-Fi Array.
- **Fast Roam:** Informs you whether or not the Xirrus fast roaming feature is enabled. This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at both Layer 2 and Layer 3. To enable or disable fast roaming, go to [“Global Settings \(IAP\)” on page 261](#).
- **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 Key:** The license key of each Array.
- **Licensed Features:** Lists the optional features enabled by the key, if any.

### *Software (enabled by default)*

- Enable/disable display of the Array OS column.

### *Firmware*

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

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

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

### *Stations*

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

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

### *Default*

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

### Spanning Tree Status

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

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

Status		Name: SS-XN8 ( 10.100.47.106 )	Location: SS Area				Uptime: 4 days, 1 hour, 38 minutes						
Network		VLAN Name	Number	Gigabit1	Gigabit2	WDS Client Links				WDS Host Links			
						1	2	3	4	1	2	3	4
Network Map		(none)	-	forwarding	forwarding								
Spanning Tree Status		VoIP	12	forwarding	forwarding								
Routing Table		Finance	5	forwarding	forwarding								
ARP Table													
DHCP Leases													
Connection Tracking													
CDP Neighbors													

Figure 72. Spanning Tree Status

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

*See Also*

[Network](#)

[Network Interfaces](#)

[Network Status Windows](#)

[VLANs](#)

[WDS](#)

## Routing Table

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

XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS-XN8 ( 10.100.47.100 )	Location: SS Area	Uptime: 4 days, 1 hour, 42 minutes
Array	Destination	Mask	Gateway
Network	255.255.255.255	255.255.255.255	0.0.0.0
Network Map	10.100.47.0	255.255.255.0	0.0.0.0
Spanning Tree Status	10.100.47.0	255.255.255.0	0.0.0.0
Routing Table	10.10.10.0	255.255.255.0	0.0.0.0
ARP Table	0.0.0.0	0.0.0.0	10.100.47.1
DHCP Leases			
Connection Tracking			
CDP Neighbors			
			Interface
			eth0
			gg1/2
			eth0
			vlan12
			gg1/2
			Auto Refresh Refresh

Figure 73. Routing Table

## See Also

### VLANs

#### Configuring VLANs on an Open SSID

## ARP Table

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

XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS-XN8 ( 10.100.47.100 )	Location: SS Area	Uptime: 4 days, 1 hour, 42 minutes
Array	IP Address	MAC Address	Interface
Network	10.100.47.1	00:10:DB:FF:20:A0	gg1/2
Network Map	10.100.47.10	00:0F:7D:00:45:FA	gg1/2
Spanning Tree Status	10.100.47.21	00:0F:7D:00:43:89	gg1/2
Routing Table	10.100.47.14	00:0F:7D:00:34:17	gg1/2
ARP Table			
DHCP Leases			
Connection Tracking			
CDP Neighbors			
			Auto Refresh Refresh

Figure 74. ARP Table



*See Also*

Routing Table

ARP Filtering

### DHCP Leases

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

XN8 Wi-Fi Array						
Status	Name: SS-XN8 ( 10.100.47.186 )		Location: SS Area		Uptime: 4 days, 1 hour, 46 minutes	
Array	IP Address	MAC Address	Start Time	End Time	Time Left	Host Name
Network	192.168.1.254	00:21:00:5e:ab:8b	Dec-09 15:50:11	Dec-09 15:55:11	0 days 0:03:20	Shelly-PC

Figure 75. DHCP Leases

*See Also*

DHCP Server

## Connection Tracking/NAT

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

XNB Wi-Fi Array

Status Name: SS-XNB (10.100.47.186) Location: SS Area Uptime: 4 days, 1 hour, 48 minutes

		Outbound Traffic						Return Traffic							
Type	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	Use
udp		192.168.1.254	224.0.0.252	54904	5355	1	51	Unreplied	224.0.0.252	192.168.1.254	5355	54904	0	0	1
udp		192.168.1.254	224.0.0.252	59697	5355	1	55	Unreplied	224.0.0.252	192.168.1.254	5355	59697	0	0	1
udp		10.100.47.14	255.255.255.255	32770	22610	1	95	Unreplied	255.255.255.255	10.100.47.14	22610	32770	0	0	1
udp		10.100.49.143	10.100.47.186	32769	22610	2	306	Unreplied	10.100.47.186	10.100.49.143	22610	32769	0	0	1
udp		10.100.47.186	10.100.23.58	37848	22610	1	157	Unreplied	10.100.23.58	10.100.47.186	22610	37848	0	0	1
udp		10.100.49.109	10.100.47.186	32771	22610	2	306	Unreplied	10.100.47.186	10.100.49.109	22610	32771	0	0	1

Figure 76. Connection Tracking

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

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

*See Also*  
Filters

### CDP Neighbors

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

The screenshot shows the 'XN8 Wi-Fi Array' interface with the 'CDP Neighbors' section expanded. The table below represents the data shown in the screenshot.

XN8 Wi-Fi Array							
Name: SS-XN8 (10.100.47.186)		Location: SS Area		Uptime: 0 days, 1 hour, 29 minutes			
Status	Hostname	IP Address	Model	Interface	Native VLAN	Capabilities	Software
Array							
Network							
Network Map							
Spanning Tree Status							
Routing Table							
ARP Table							
DHCP Leases							
Connection Tracking							
CDP Neighbors							
RF Monitor							
Stations							
Statistics							
System Log							
Configuration							
Express Setup							
Network							
Services							
VLANs							

Figure 77. CDP Neighbors

CDP must be enabled on the Array in order to gather and display this information. See “CDP Settings” on page 190.

## RF Monitor Windows

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

The following RF Status windows are available:

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

### IAPs

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

Status		Uptime - 5 days, 23 hours, 24 minutes														
Array		IAP	Channel	Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate				
RF Monitor				0	0K 0	0K 0%	100% 0%	100% 0	-20	-95	-70 0%	100%	95	36	1M	Scale
IAPs																
Spectrum Analyzer		abg1	1													
Intrusion Detection		abg2	-													
Stations		abg3	11													
Statistics		abg4	6													
Event Log		a1	36													
Configuration		a2	52													
Express Setup		a3	149													
Network		a4	40													

Figure 78. RF Monitor—IAPs

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

## Spectrum Analyzer



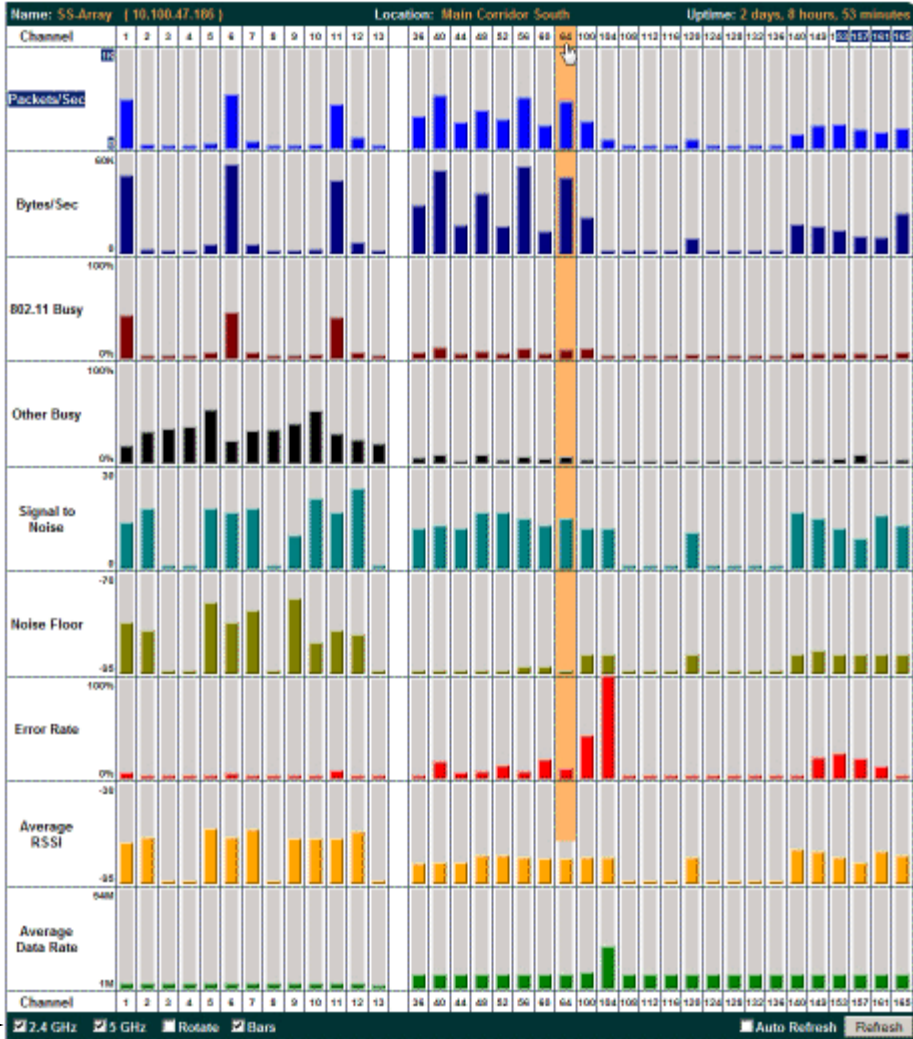
*The RF measurements for this feature are obtained by IAP **abg(n)2**, which **must** be set to **monitor** mode for any data to be available. See “IAP Settings” on page 256.*

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

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

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


Click Channel number to highlight



Select Display Options

Figure 79. RF Spectrum Analyzer

The Spectrum Analyzer offers several display options:

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

### *Spectrum Analyzer Measurements*

The spectrum analyzer displays the following information:

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

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



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

## Intrusion Detection

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

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

XN8 Wi-Fi Array

<b>Status</b>	Name: SS-XN8 ( 10.100.47.186 )		Location: SS Area		Uptime: 4 days, 2 hours, 40 minutes					
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▼ RF Monitor                             <ul style="list-style-type: none"> <li>IAPs</li> <li>Spectrum Analyzer</li> <li>Intrusion Detection</li> </ul> </li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>▶ System Log</li> <li><b>Configuration</b> <ul style="list-style-type: none"> <li>Express Setup</li> <li>▶ Network</li> <li>▶ Services</li> <li>▶ VLANs</li> </ul> </li> </ul>	Select List   Unknown									
	Select	BSSID	SSID	Manufacturer	Channel	RSSI	Security	Type	Discovered	Last Active
	<input type="checkbox"/>	00:0b:6b:e0:00:f7	wlan-ng	Wistron Neweb	6	-51	none	ESS	Dec-05 14:06	active
	<input type="checkbox"/>	00:0f:34:c0:46:30	tsunami	Cisco	11	-63	none	ESS	Dec-05 14:06	active
	<input type="checkbox"/>	00:19:33:00:18:98	Giuseppe	Strix	165	-76	TKIP+PSK	ESS	Dec-05 14:06	active
	<input type="checkbox"/>	00:0e:84:e4:19:9e	tsunami	Cisco	56	-87	none	ESS	Dec-05 14:06	active
	<input type="checkbox"/>	00:11:20:ee:dc:83	LinkFloor3	Cisco	60	-61	none	ESS	Dec-08 16:13	active
		Set Approved	Set Known	Set Blocked	<input checked="" type="checkbox"/> Auto Refresh			Refresh	Save	

**Select the type of AP to display**

Figure 80. Intrusion Detection/Rogue AP List

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

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

### *See Also*

[Network Map](#)

[Rogue Control List](#)

[SSIDs](#)

[SSID Management](#)

## Station Status Windows

The following Station Status windows are available:

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

### Stations

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

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

Status		Name: Location-XN8-Support ( 10.100.46.240 )		Location: Support area		Uptime: 10 days, 5 hours, 4							
Display		<input checked="" type="checkbox"/> Associated		<input type="checkbox"/> Unassociated		Associated: 1 Unassociated: 212 Total Station							
Select	MAC Address	Netbios Name	IP Address	Manufacturer	SSID	User Group	User Name	VLAN	QoS	IAP	TX Rate	RX Rate	RSSI
<input type="checkbox"/>	00:1d:4f:2a:ee:8d		10.100.46.167	Apple	AAAAAAAAAAAAAAAAAAAAA			-	2	abgn1	48.0	36.0	-55

Figure 81. Stations

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

- **Deny Access:** Sends a de-authentication frame to the selected station and explicitly denies it access by adding its MAC address to the Deny List in the Access Control List window. To permit access again, go to [“Access Control List” on page 222](#) and delete the station from the **Deny** list.
- **Deauthenticate:** Sends a de-authentication frame to the selected station. The station may re-authenticate.

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

*See Also*

- Access Control List
- Station Status Windows

### Location Map

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

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

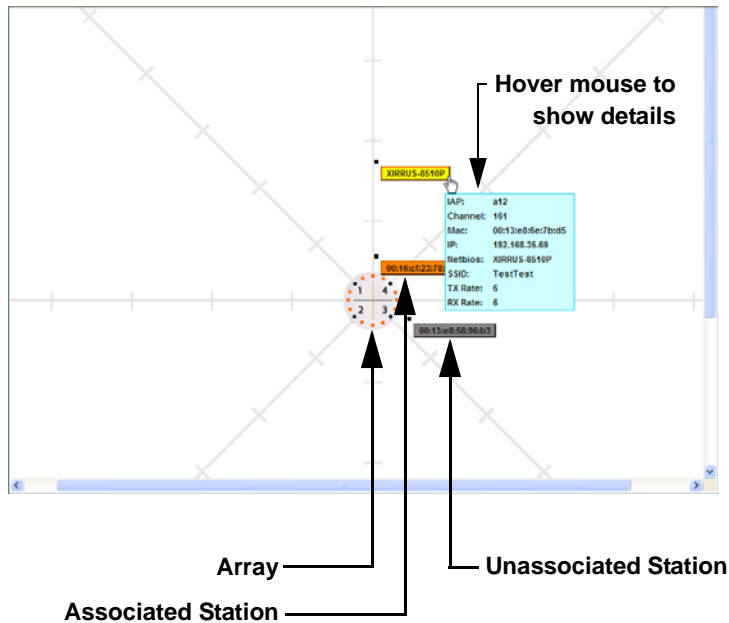


Figure 82. Location Map

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

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

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



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

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

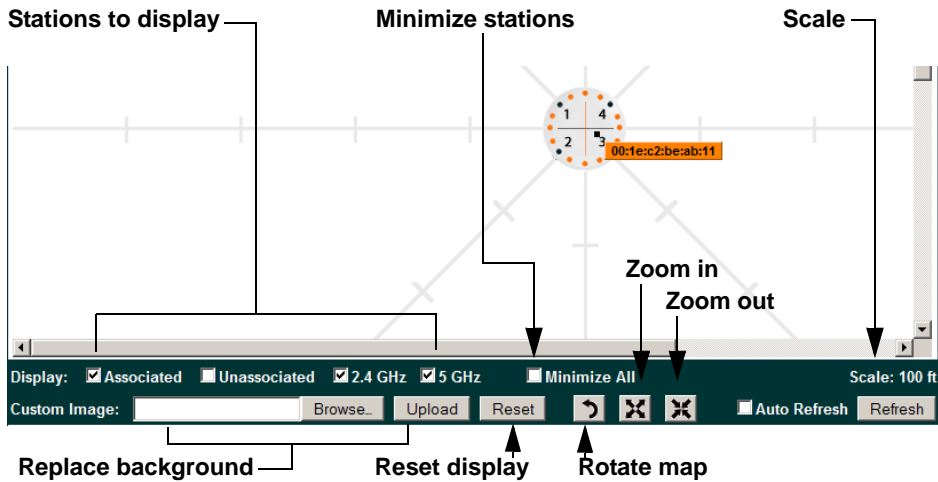


Figure 83. Controls for Location Map

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

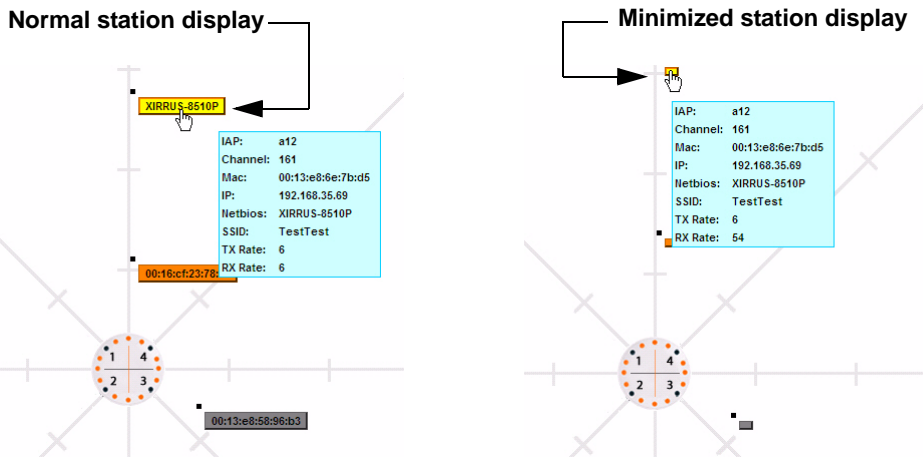





Figure 84. Minimizing stations

- **Scale:** This view-only value shows the approximate distance represented by each hashmark on the default map background. Scale is the rightmost of the items displayed in the control area - you may need to scroll to the right edge to see it.
- **Custom Image:** Use this feature to replace the default background image with your own image of the floor plan of your location. Click the **Browse** button and browse to the desired file on your computer. This may be a .gif, .jpg, .jpeg, .png, .htm, or .html file. The scale of the file should be 100 feet per inch. Then click **Upload** (see below). For more information on



using the custom, image, see “Working with the Custom Image” on page 155.

- **Upload:** After browsing to the desired custom image, click the **Upload** button to install it. The map will be redisplayed with your new background. No hash marks are added to the image display.
- **Reset:** Click this button to restore the map display to the factory settings. All attributes are restored—including the stations selected for display, the scale, the rotation, and the background map.
-  ● **Rotate:** Click this button to rotate the orientation of the entire map. It rotates the map 45° counter-clockwise.
-  ● **Enlarge:** Click this button to enlarge (zoom in on) the map. The displayed **Scale** on the bottom right is updated with the new scale for the map.
-  ● **Reduce:** Click this button to reduce (zoom out on) the map. The displayed **Scale** on the bottom right is updated with the new scale for the map
- **Auto Refresh:** Instructs the Array to refresh this window automatically.
- **Refresh:** Updates the stations displayed.

### *See Also*


[Access Control List](#)

[Station Status Windows](#)

### *Working with the Custom Image*

After you have uploaded a custom image (see **Custom Image** and **Upload** in “Controls and items displayed on the Location Map window” on page 153), you should move the display of the Array on your map to correspond with its actual location at your site. The Location Map window provides a special set of controls for moving the location of the Array. These controls are displayed on the upper right corner of the map (Figure 85). The location controls only appear when you are using a custom image for your background. You will not see them if you are using the default map background.

To move the Array on the map in a particular direction, click an arrow for the desired direction on the location controls. The inner arrows move the Array by

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

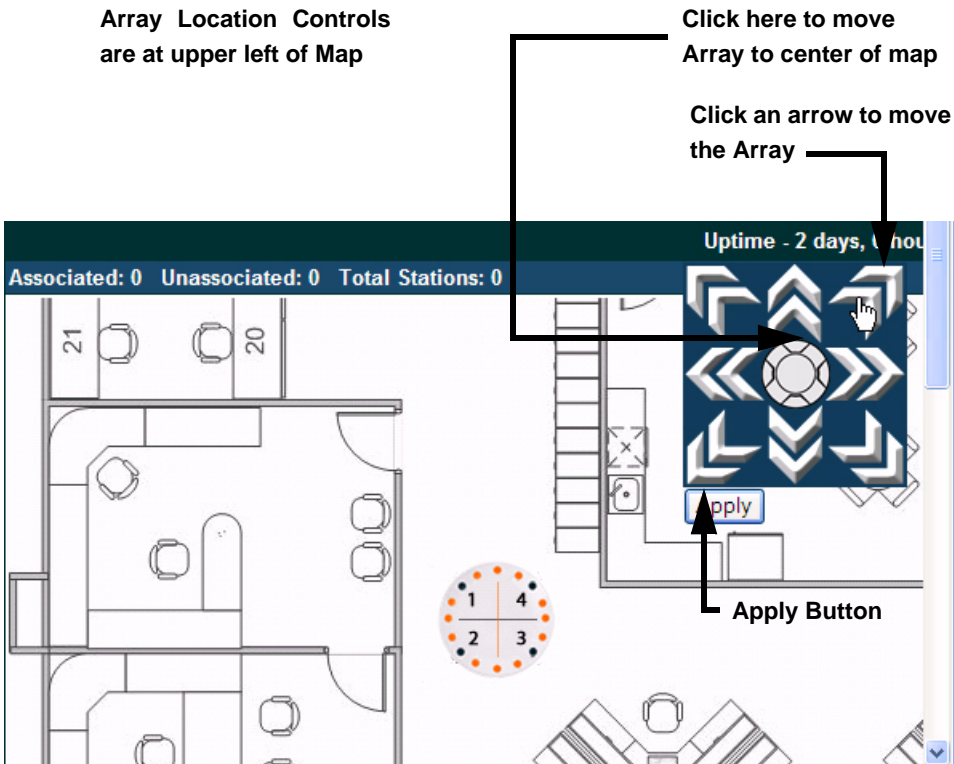


Figure 85. Setting Array location on a Custom Image

### RSSI

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

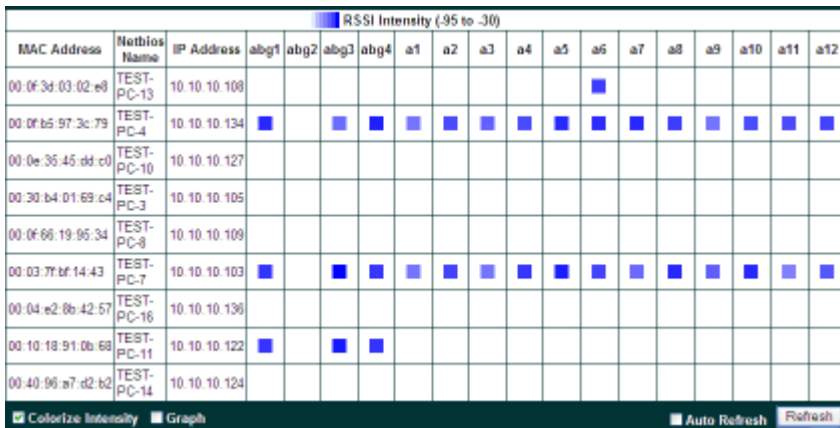


Figure 86. Station RSSI Values

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

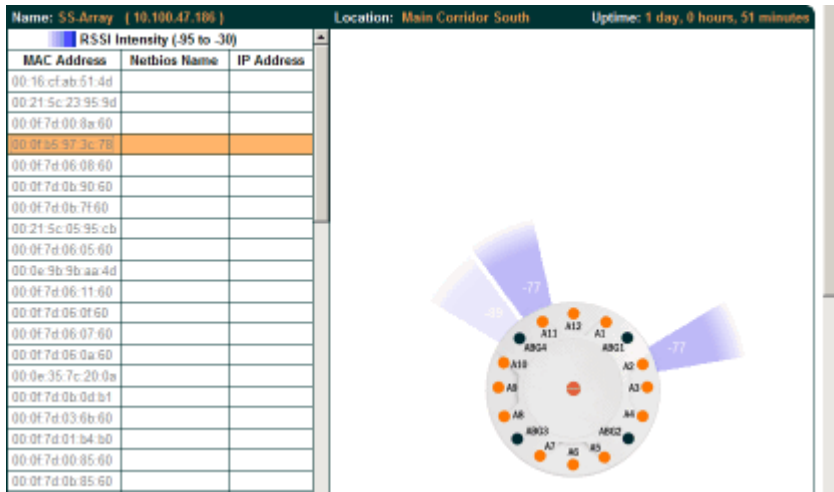



Figure 87. Station RSSI Values—Colorized Graphical View

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

*See Also*

- Station Status Windows
- RF Monitor Windows

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

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

The screenshot shows the 'Signal to Noise' window for a station named 'SS-XN8 (10.100.47.186)'. The window title is 'XN8 Wi-Fi Array' and the XIRRUS logo is in the top right. The station's location is 'SS Area' and its uptime is '4 days, 3 hours, 11 minutes'. A table displays SNR values for various IAPs (abgn1-abgn4 and an1-an4). The 'abgn4' column shows a value of 61, while others are dashes. A sidebar on the left contains navigation options: Array, Network, RF Monitor, Stations, Location Map, RSSI, Signal to Noise (selected), Noise Floor, and Max by IAP.

MAC Address	Netbios Name	IP Address	abgn1	abgn2	abgn3	abgn4	an1	an2	an3	an4
00:21:00:5e-ab:8b			-	-	-	61	-	-	-	-

Figure 88. Station Signal-to-Noise Ratio Values

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

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

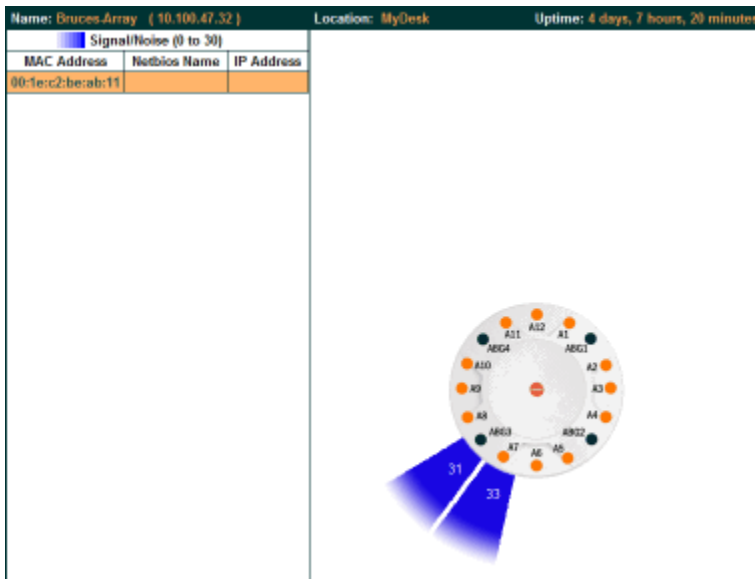



Figure 89. Station SNR Values—Colorized Graphical View

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

*See Also*

- Station Status Windows
- RF Monitor Windows

### Noise Floor

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

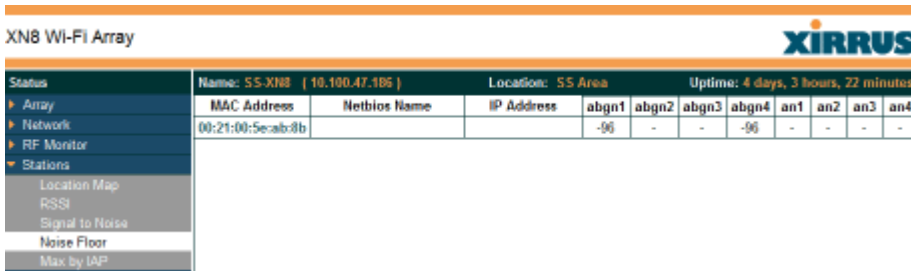


Figure 90. Station Noise Floor Values

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

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

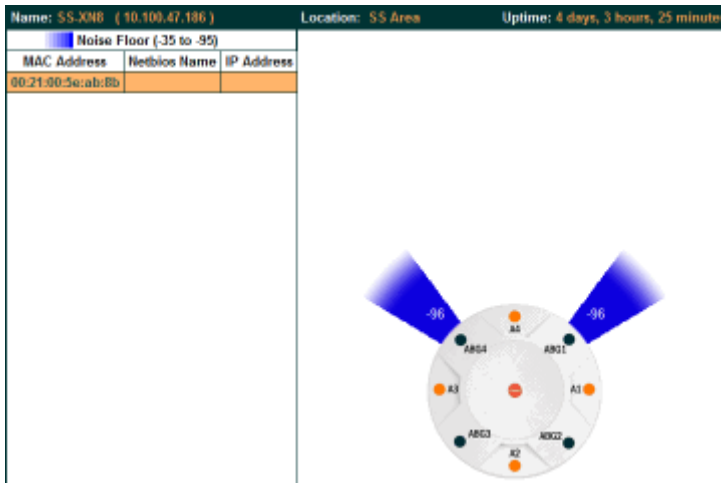


Figure 91. Station Noise Floor Values—Colorized Graphical View

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

*See Also*

- Station Status Windows
- RF Monitor Windows



### Max by IAP

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

						Max station count				
IAP	State	Channel		Current Stations	Hour	Day	Week	Month	Year	
abg1	up	1	manual	0	0	0	0	0	0	
abg2	up	monitor		0	0	0	0	0	0	
abg3	up	11	manual	2	3	3	3	3	3	
abg4	up	6	manual	0	1	2	2	2	2	
a1	up	36	manual	0	2	2	2	2	2	
a2	up	153	manual	2	4	4	4	4	4	
a3	up	56	manual	0	0	0	0	0	0	
a4	up	165	manual	1	1	1	1	1	1	

Figure 92. Max by IAP

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

*See Also*

[IAPs](#)

[Station Status Windows](#)

## Statistics Windows

The following Array Statistics windows are available:

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

### IAP Statistics Summary

This is a status only window that provides an overview of the statistical data associated with all IAPs. It also shows the channel used by each IAP. For detailed statistics for a specific IAP, see “Per-IAP Statistics” on page 165. 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 **XIRRU**

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

Statistics for IAP All

IAP	Channel	Receive Statistics by IAP				Transmit Statistics by IAP			
		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 93. IAP Statistics Summary Page

*See Also*

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

**Per-IAP Statistics**

This is a status only window that provides detailed statistics for the selected IAP. If you click the link for **IAP All** in the left frame, each detailed statistic field will show the sum of that statistic for all IAPs. For a summary of statistics for all IAPs, see “IAP Statistics Summary” on page 164. Use the **Display Percentages** checkbox at the lower left to select the output format—check this option to express each statistic as a percentage of the total at the top of the column, or leave it blank to display raw numbers.

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

Name: SS-X108 [ 10.100.47.106 ]		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	15100		
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		
<input type="checkbox"/> Display Percentages		<input type="checkbox"/> Auto Refresh		Refresh	Clear

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

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

### See Also

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

### Network Statistics

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

Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 4 days, 3 hours, 51 minutes	
▶ Array	Fast Ethernet Statistics <span style="float:right">enabled, link down, 100Mbps, full duplex</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	Gigabit 1 Statistics <span style="float:right">enabled, link up, 1000Mbps, full duplex</span>			
Stations	Receive Bytes	246021597	Transmit Bytes	202395623
System Log	Receive Packets	1745005	Transmit Packets	859020
Configuration	Receive Compressed	0	Transmit Compressed	0
Express Setup	Receive Multicast	0	Transmit Carrier Errors	0
▶ Network	Receive Dropped	0	Transmit Dropped	0
▶ Services	Receive FIFO Errors	0	Transmit FIFO Errors	0
▶ VLANs	Receive Frame Errors	0	Transmit Collisions	0
▶ Security	Receive Total Errors	0	Transmit Total Errors	0
▶ SSIDs	Gigabit 2 Statistics <span style="float:right">enabled, link down, 1000Mbps, half duplex</span>			
▶ Groups	Receive Bytes	0	Transmit Bytes	0
▶ IAPs	Receive Packets	0	Transmit Packets	0
▶ WDS	Receive Compressed	0	Transmit Compressed	0
▶ Filters	Receive Multicast	0	Transmit Carrier Errors	0
Tools	Receive Dropped	0	Transmit Dropped	0
System Tools	Receive FIFO Errors	0	Transmit FIFO Errors	0
CLI	Receive Frame Errors	0	Transmit Collisions	0
Logint	Receive Total Errors	0	Transmit Total Errors	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 0				

Figure 95. Network Statistics

*See Also*

DHCP Server

DNS Settings

Network

Network Interfaces

## VLAN Statistics

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

The screenshot shows the 'XNB Wi-Fi Array' interface. The top header includes the XIRRUS logo and system information: Name: SS-XNB (10.100.47.186), Location: SS Area, and Uptime: 4 days, 3 hours, 59 minutes. A left-hand navigation menu lists various system sections like Status, Network, Stations, Statistics, IAP, Network, VLAN, WDS, Filter, Stations, System Log, Configuration, Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, and IAPs. The main content area displays 'VoIP (12) Statistics' and 'Finance (5) Statistics' tables. The VoIP statistics table shows zero values for all metrics. The Finance statistics table shows non-zero values for Receive Bytes (3313440) and Transmit Packets (5616). At the bottom right, there are buttons for 'Auto Refresh' and 'Refresh', and a 'Clear All' button at the bottom left of the statistics area.

VoIP (12) Statistics		Clear	
Receive Bytes	0	Transmit Bytes	0
Receive Packets	0	Transmit Packets	0
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	0	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

Finance (5) Statistics		Clear	
Receive Bytes	3313440	Transmit Bytes	3313440
Receive Packets	5616	Transmit Packets	5616
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	0	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

Figure 96. VLAN Statistics

*See Also*

VLAN Management

VLANs

### WDS Statistics

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

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

Figure 97. WDS Statistics

*See Also*

SSID Management

WDS

## Filter Statistics

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

Name	Type	State	Packets	Bytes
Filter1	allow	on	1961	268436

Figure 98. Filter Statistics

*See Also*  
Filters

## Station Statistics

This status-only window provides an overview of statistical data for all stations. Stations are listed by MAC address, and Receive and Transmit statistics are summarized for each. For detailed statistics for a specific station, click the desired MAC address in the **Station** column and see “Per-Station Statistics” on page 171.

Station	Receive Statistics by Station				Transmit Statistics by Station			
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
00:0e:3d:03:02:a0	693119	2943	0	223	2368	12	0	1
00:0e:b5:97:3c:79	51442645153	52791337	0	5371976	65400578303	65515091	26764	11869632
00:0e:35:45:d4:c0	1691913717	24210701	0	8748417	168562071943	164832963	112870	104185667
00:30:b4-01-69:c4	1004756270	10171896	0	0	265914094203	259348067	10303	48699772
00:0f:66:19:95:34	1550292533	5009662	0	1202533	36006985880	36032055	309661	41993995
00:03:7f:b6:14:45	197116974748	195875363	0	32942200	277967033447	266885001	45170	60729663
00:04:a2:8b:42:57	323018216404	312187836	0	29556244	507270199576	492647649	12040	39488662
00:10:10:91:06:68	181652410042	177651569	0	18383672	264862154829	263394451	170454	36038464
00:40:96:a7:d2:b2	249090923758	247980426	0	22610375	276050170214	270423992	18482	127696107

Figure 99. Station Statistics

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



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

*See Also*

Per-Station Statistics

### Per-Station Statistics

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

Receive and Transmit statistics are listed by **Rate**—this is the data rate in Mbps. For a summary of statistics for all stations, see “[Station Statistics](#)” on page 170.

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

Station Statistics for 00:0f:3d:03:02:e0

Rate	Receive Statistics				Transmit Statistics			
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
1	1015465	18726	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
5.5	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0
6	3728543	77325	0	15	0	0	0	0
9	0	0	0	0	0	0	0	0
12	1710	5	0	3	0	0	0	0
18	1726	5	0	2	0	0	0	0
24	0	0	0	0	0	0	0	0
36	5959	22	0	2	0	0	0	0
48	73724	228	0	29	0	0	0	0
54	693119	2043	0	223	2358	12	0	1
<b>Total</b>	6620246	99354	0	274	2358	12	0	1

Auto Refresh

Figure 100. Individual Station Statistics Page

*See Also*

Station Statistics

## System Log Window

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

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

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

Status		Name: SS-Array [ 10.100.47.188 ]		Location: Main Corridor South		Uptime: 3 days, 1 hour, 8 minutes	
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>System Log</li> </ul>		Filter Priority: <input type="text" value="Notification"/>		Highlight Priority: <input type="text" value="Notification"/>			
Time Stamp	Priority	Message					
Oct 21 17:24:38	Notification	Admin user admin logged into web management interface from 10.100.21.73					
Oct 21 17:24:33	Notification	Admin user admin was logged out of web management interface due to timeout.					
Oct 21 17:04:34	Alert	Rogue AP detected. SSID: SQA-WPR-Custom, BSSID: 00:0f7d:06:cc:f0, Manufacturer: Xirus, Channel: 64, RSSI: -94, Security: none					
Oct 21 17:02:56	Alert	Rogue AP detected. SSID: zorsopen1, BSSID: 00:0f7d:09:ef:50, Manufacturer: Xirus, Channel: 60, RSSI: -93, Security: none					
Oct 21 16:57:12	Alert	Rogue AP detected. SSID: public, BSSID: 00:0f7d:04:f2:03, Manufacturer: Xirus, Channel: 161, RSSI: -90, Security: none					
Oct 21 16:55:01	Alert	Rogue AP detected. SSID: SQA-WPR-Custom, BSSID: 00:0f7d:06:cc:f0, Manufacturer: Xirus, Channel: 40, RSSI: -90, Security: none					
Oct 21 16:52:47	Alert	Rogue AP detected. SSID: SQA-WPR-Login-int, BSSID: 00:0f7d:0a:3f:51, Manufacturer: Xirus, Channel: 40, RSSI: -86, Security: none					
Oct 21 16:49:45	Alert	Rogue AP detected. SSID: fredgit, BSSID: 00:0f7d:00:8d:56, Manufacturer: Xirus, Channel: 40, RSSI: -76, Security: none					

Figure 101. System Log

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

# Configuring the Wi-Fi Array

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

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

- [“Express Setup” on page 174](#)
- [“Network” on page 180](#)
- [“Services” on page 192](#)
- [“VLANs” on page 204](#)
- [“Security” on page 208](#)
- [“SSIDs” on page 235](#)
- [“Groups” on page 248](#)
- [“IAPs” on page 254](#)
- [“WDS” on page 287](#)
- [“Filters” on page 291](#)

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

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

- [“Viewing Status on the Wi-Fi Array” on page 127](#)
- [“Using Tools on the Wi-Fi Array” on page 299](#)

## Express Setup

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

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

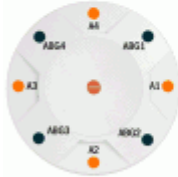


Figure 102. WMI: Express Setup

### *Procedure for Performing an Express Setup*

1. **Host Name:** Specify a unique [host name](#) for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is Xirrus-WiFi-Array.
2. **Location Information:** Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
3. **Admin Contact:** Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
4. **Admin Email:** Enter the email address of the admin contact you entered in Step 3.
5. **Admin Phone:** Enter the telephone number of the admin contact you entered in Step 3.
6. **Configure SNMP:** Select whether to **Enable** SNMP on the Array, and set the SNMP community strings. The factory default value for the **SNMP Read-Only Community String** is `xirrus_read_only`. The factory default value for the **SNMP Read-Write Community String** is `xirrus`. If you are using the Xirrus Management System (XMS), the read-write string must match the string used by XMS. XMS also uses the default value `xirrus`.
7. **Configure the 10/100 Ethernet 0 (10/100 Mb) and Gigabit Ethernet 1 network interface settings.** Note that the and Gigabit Ethernet 2 port is not configured on this page. If you need to make changes to Gigabit 2, please see [“Network Interfaces” on page 181](#).

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

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

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

- c. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** to assign IP addresses to the Array's Ethernet interfaces, or choose **Static** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following information:
  - **IP Address:** Enter a valid IP address for this Array. To use a remote connection (Web, **SNMP**, or **SSH**), a valid IP address must be used.
  - **IP Subnet Mask:** Enter a valid IP address for the **subnet mask** (the default is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
  - **Default Gateway:** Enter a valid IP address for the **default gateway**. This is the IP address of the router that the Array uses to forward data to other networks.
8. **SSID Settings:** This section specifies the wireless network name and security settings.
  - a. The **SSID (Wireless Network Name)** is a unique name that identifies a wireless network (SSID stands for Service Set Identifier). All devices attempting to connect to a specific WLAN must use the same SSID. The default SSID is **xirrus**. Entering a value in this field will replace the default SSID with the new name.

For additional information about SSIDs, go to the **Multiple SSIDs** section of "Frequently Asked Questions" on page 404.

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

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. WPA is the stronger of the two wireless security schemes.
- **WPA2** (Wi-Fi Protected Access 2)—WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.
- **WPA-Both** (WPA and WPA2)—This option makes use of both WPA and WPA2.

For more information about security, including a full review of all security options and settings, go to [“Understanding Security” on page 209](#).

- c. **Wireless Key/Passphrase:** Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase.
  - d. **Confirm Key/Passphrase:** If you entered a WEP key or WPA passphrase, confirm it here.
9. **Admin Settings:** This section allows you to change the default admin username and password for the Array.
- a. **New Admin User (Replace Default):** Enter the name of a new administrator user account. 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). The default **admin** user is deleted. Note that the Array also offers the option of authenticating administrators using a RADIUS server (see “[Admin Management](#)” on page 214)).

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



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

#### 11. IAP Settings:

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

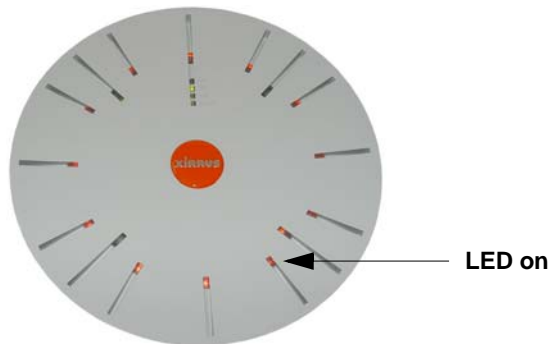


Figure 103. LEDs are Switched On

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

## Network

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

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

Figure 104. Network Interfaces

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

- [“Network Interfaces” on page 181](#)
- [“DNS Settings” on page 188](#)
- [“CDP Settings” on page 190](#)

### See Also

[DNS Settings](#)

[Network Interfaces](#)

[Network Status Windows](#)

[Spanning Tree Status](#)

[Network Statistics](#)

### Network Interfaces

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

Status	Name: SS-X100 ( 10.100.47.106 )	Location: SS Area	Uptime: 0 days, 0 hours, 26 minutes																																																														
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Stations</li> <li>▶ Statistics</li> <li>▶ System Log</li> <li>Configuration</li> <li>Express Setup</li> <li>▶ Network                             <ul style="list-style-type: none"> <li>Interfaces</li> <li>DHCP</li> <li>CDP</li> <li>Services</li> <li>VLANs</li> <li>Security</li> <li>SSIDs</li> <li>Groups</li> <li>IAPs</li> <li>WDS</li> <li>Filters</li> </ul> </li> <li>Tools                             <ul style="list-style-type: none"> <li>System Tools</li> <li>CU</li> <li>Logout</li> </ul> </li> <li>Log Messages                             <ul style="list-style-type: none"> <li>Critical 6</li> <li>Warning 8</li> <li>Information 500</li> </ul> </li> </ul>	<h4>10/100 Ethernet 0 Settings</h4> <table border="1"> <tr><td>Enable Interface:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>Auto Negotiate:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>Duplex:</td><td><input checked="" type="radio"/> Full <input type="radio"/> Half</td></tr> <tr><td>Speed:</td><td>100 Megabit</td></tr> <tr><td>Configuration Server Protocol:</td><td><input type="radio"/> DHCP <input checked="" type="radio"/> Static</td></tr> <tr><td>IP Address:</td><td>10.100.100.21</td></tr> <tr><td>IP Subnet Mask:</td><td>255.255.255.0</td></tr> <tr><td>Default Gateway:</td><td>10.100.100.1</td></tr> <tr><td>Static route (IP Address/Mask):</td><td></td></tr> </table> <h4>Gigabit Ethernet 1 Settings</h4> <table border="1"> <tr><td>Enable Interface:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>LED Indicator:</td><td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td></tr> <tr><td>Allow Management On Interface:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>Auto Negotiate:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>Duplex:</td><td><input checked="" type="radio"/> Full <input type="radio"/> Half</td></tr> <tr><td>Speed:</td><td>Gigabit</td></tr> <tr><td>Port Mode:</td><td>Active backup (gig1/2 fail over to each other)</td></tr> <tr><td>Configuration Server Protocol:</td><td><input type="radio"/> DHCP <input checked="" type="radio"/> Static</td></tr> <tr><td>IP Address:</td><td>10.100.100.186</td></tr> <tr><td>IP Subnet Mask:</td><td>255.255.255.0</td></tr> <tr><td>Default Gateway:</td><td>10.100.100.1</td></tr> </table> <h4>Gigabit Ethernet 2 Settings</h4> <table border="1"> <tr><td>Enable Interface:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>LED Indicator:</td><td><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td></tr> <tr><td>Allow Management On Interface:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>Auto Negotiate:</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td></tr> <tr><td>Duplex:</td><td><input checked="" type="radio"/> Full <input type="radio"/> Half</td></tr> <tr><td>Speed:</td><td>Gigabit</td></tr> <tr><td>Port Mode:</td><td>Active backup (gig1/2 fail over to each other)</td></tr> <tr><td>Configuration Server Protocol:</td><td><input checked="" type="radio"/> DHCP <input type="radio"/> Static</td></tr> <tr><td>IP Address:</td><td>10.100.100.186</td></tr> <tr><td>IP Subnet Mask:</td><td>255.255.255.0</td></tr> <tr><td>Default Gateway:</td><td>10.100.100.1</td></tr> </table>			Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half	Speed:	100 Megabit	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	IP Address:	10.100.100.21	IP Subnet Mask:	255.255.255.0	Default Gateway:	10.100.100.1	Static route (IP Address/Mask):		Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half	Speed:	Gigabit	Port Mode:	Active backup (gig1/2 fail over to each other)	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static	IP Address:	10.100.100.186	IP Subnet Mask:	255.255.255.0	Default Gateway:	10.100.100.1	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No	Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half	Speed:	Gigabit	Port Mode:	Active backup (gig1/2 fail over to each other)	Configuration Server Protocol:	<input checked="" type="radio"/> DHCP <input type="radio"/> Static	IP Address:	10.100.100.186	IP Subnet Mask:	255.255.255.0	Default Gateway:	10.100.100.1
Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half																																																																
Speed:	100 Megabit																																																																
Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static																																																																
IP Address:	10.100.100.21																																																																
IP Subnet Mask:	255.255.255.0																																																																
Default Gateway:	10.100.100.1																																																																
Static route (IP Address/Mask):																																																																	
Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																																																																
Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half																																																																
Speed:	Gigabit																																																																
Port Mode:	Active backup (gig1/2 fail over to each other)																																																																
Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static																																																																
IP Address:	10.100.100.186																																																																
IP Subnet Mask:	255.255.255.0																																																																
Default Gateway:	10.100.100.1																																																																
Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																																																																
Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No																																																																
Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half																																																																
Speed:	Gigabit																																																																
Port Mode:	Active backup (gig1/2 fail over to each other)																																																																
Configuration Server Protocol:	<input checked="" type="radio"/> DHCP <input type="radio"/> Static																																																																
IP Address:	10.100.100.186																																																																
IP Subnet Mask:	255.255.255.0																																																																
Default Gateway:	10.100.100.1																																																																

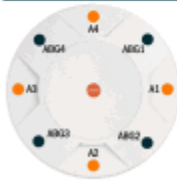


Figure 105. Network Settings



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

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

### Network Interface Ports

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

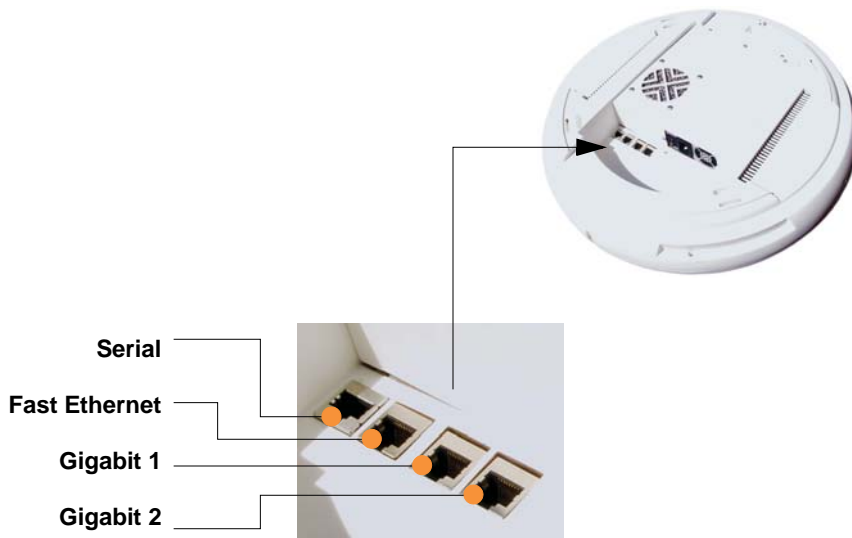


Figure 106. Network Interface Ports

### *Procedure for Configuring the Network Interfaces*

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

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

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

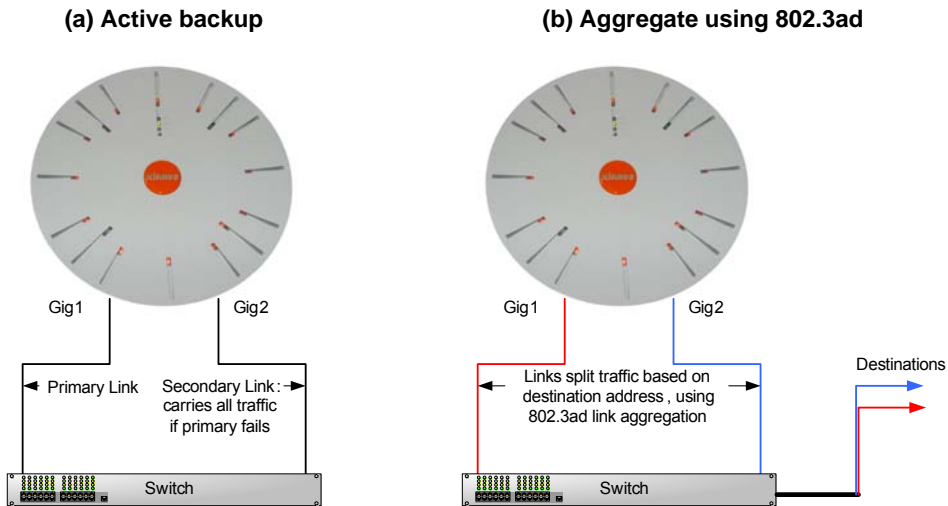


Figure 107. Port Modes (a-b)

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

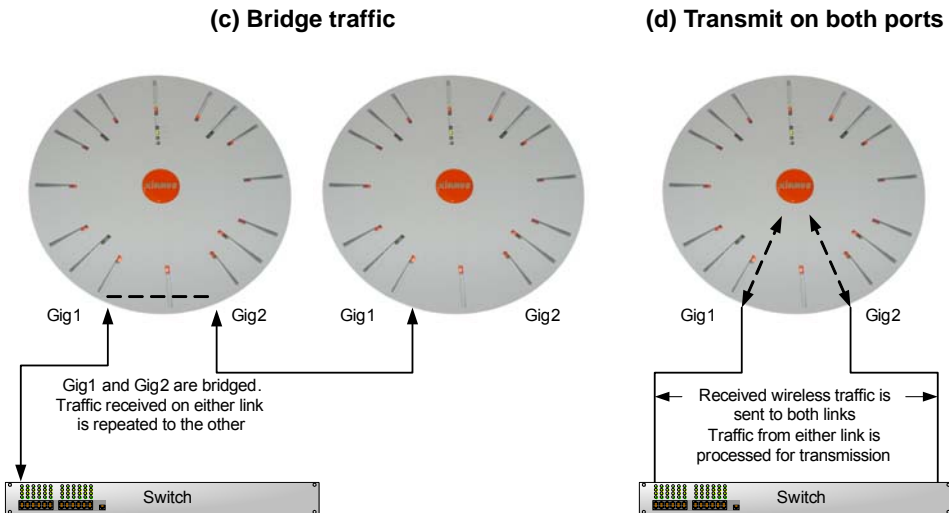
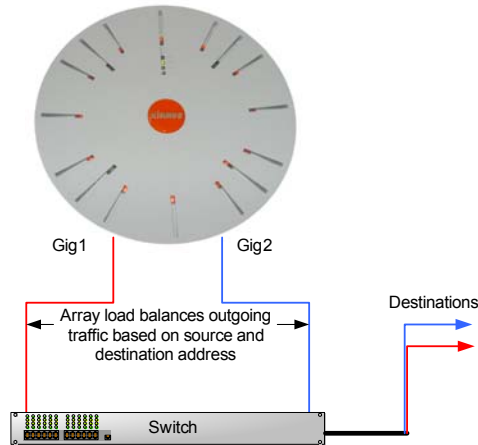


Figure 108. Port Modes (c-d)

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

(e) Load balance traffic



(f) Mirror traffic

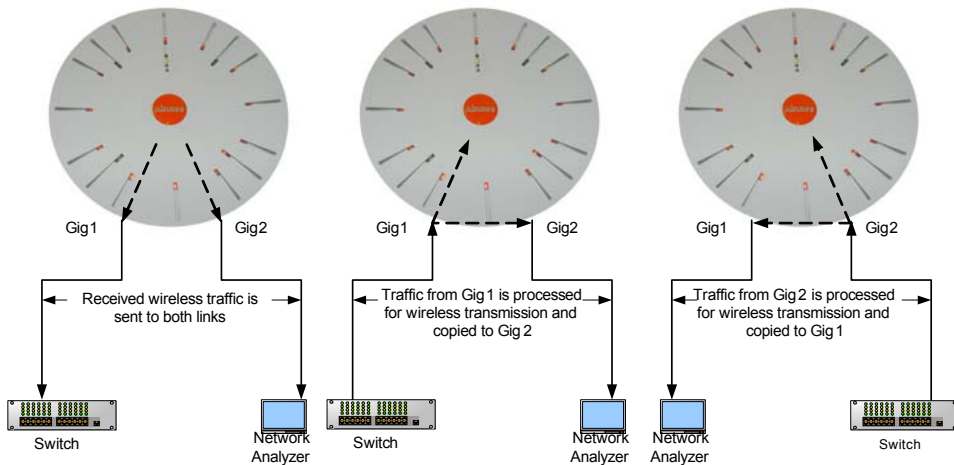


Figure 109. Port Modes (e-f)

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



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

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

*See Also*

[DNS Settings](#)

[Network](#)

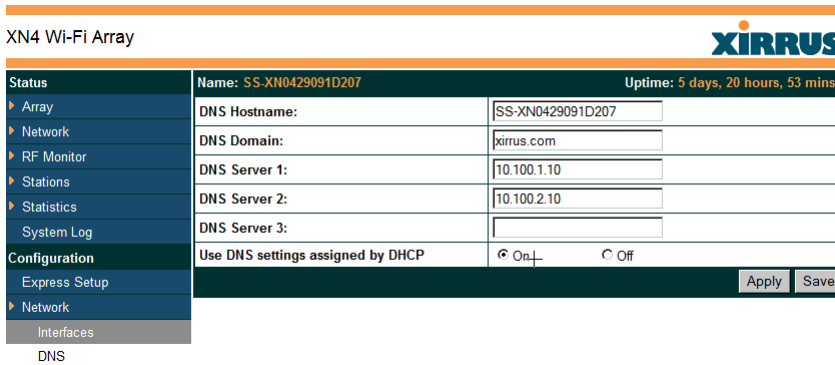
[Network Statistics](#)

[Spanning Tree Status](#)

## DNS Settings

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

Note that the DNS servers defined here are not used by wireless clients—servers for stations associated to the Array are defined along with DHCP pools. See “**DHCP Server**” on page 202. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.



XN4 Wi-Fi Array		<b>XIRRUS</b>
<b>Status</b>	Name: SS-XN0429091D207 <span style="float: right;">Uptime: 5 days, 20 hours, 53 mins</span>	
▶ Array	DNS Hostname:	<input type="text" value="SS-XN0429091D207"/>
▶ Network	DNS Domain:	<input type="text" value="xirus.com"/>
▶ RF Monitor	DNS Server 1:	<input type="text" value="10.100.1.10"/>
▶ Stations	DNS Server 2:	<input type="text" value="10.100.2.10"/>
▶ Statistics	DNS Server 3:	<input type="text"/>
System Log	Use DNS settings assigned by DHCP	<input checked="" type="radio"/> On <input type="radio"/> Off
<b>Configuration</b>	<input type="button" value="Apply"/> <input type="button" value="Save"/>	
Express Setup		
▶ Network		
Interfaces		
DNS		

Figure 110. DNS Settings

### *Procedure for Configuring DNS Servers*

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

5. **Use DNS settings assigned by DHCP:** If you are using DHCP to assign the Array's IP address, you may turn this option **On**. The Array will then obtain its DNS domain and server settings from the network DHCP server that assigns an IP address to the Array. You may also configure that DHCP server to assign a host name to the Array.
6. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

DHCP Server

Network

Network Interfaces

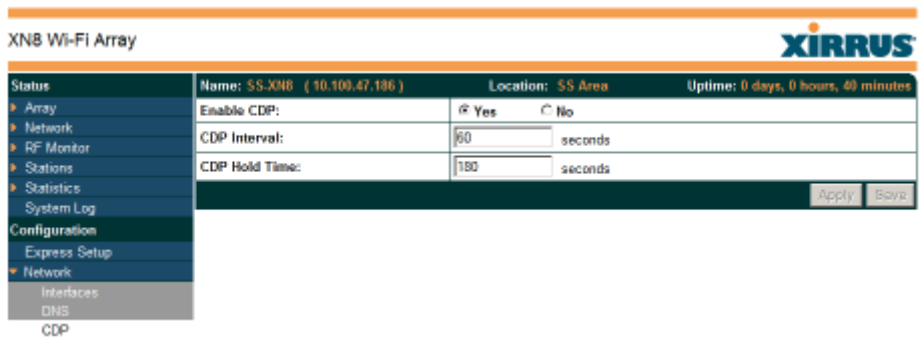
Network Statistics

Spanning Tree Status

## CDP Settings

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

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



XNB Wi-Fi Array		XIRRUS	
Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 0 days, 0 hours, 49 minutes
Array	Enable CDP:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Network	CDP Interval:	<input type="text" value="60"/>	seconds
RF Monitor	CDP Hold Time:	<input type="text" value="180"/>	seconds
Stations	<input type="button" value="Apply"/> <input type="button" value="Save"/>		
Statistics			
System Log			
Configuration			
Express Setup			
Network			
Interfaces			
DNS			
CDP			

Figure 111. CDP Settings

### *Procedure for Configuring CDP Settings*

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

*See Also*

CDP Neighbors

Network

Network Interfaces

Network Statistics

## Services

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

XN8 Wi-Fi Array							XIRRUS		
Status	Name: 55-XN8 ( 10.100.47.196 )		Location: 55 Area		Uptime: 0 days, 0 hours, 42 minutes				
Array	Time Settings Summary								
Network	NTP Server Status		NTP Server 1 Address		NTP Server 2 Address				
RF Monitor	Enabled		time.nist.gov		pool.ntp.org				
Stations	Netflow Summary								
Statistics	State		Collector Host		Collector Port				
System Log	Disabled				2055				
Configuration	System Log Settings Summary								
Express Setup	Syslog Server Status		Enabled						
Network	Console Logging		Disabled		Level 6 and lower (Information and more serious)				
Services	Local File		500 lines		Level 6 and lower (Information and more serious)				
Time	Primary Server		10.100.47.17		Level 7 and lower (Debugging and more serious)				
Netflow	Secondary Server		0.0.0.0		Level 6 and lower (Information and more serious)				
System Log	Tertiary Server				Level 6 and lower (Information and more serious)				
SNMP	Email SMTP Server				Level 4 and lower (Warning and more serious)				
DHCP Server	SNMP Settings Summary								
VLANs	SNMPv2 State		Trap Auth Failures		Trap Host IP 1	Trap Host IP 2	Trap Host IP 3	Trap Host IP 4	
Security	Enabled		Enabled		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	
SSIDs	SNMPv3 State		SNMPv3 Security		Trap Port 1	Trap Port 2	Trap Port 3	Trap Port 4	
Groups	Enabled		SHA / AES		162	162	162	162	
IAPs	DHCP Server Settings								
WDS	DHCP Name	State	NAT	IP Range/Mask		IP Gateway	Default Lease	Maximum Lease	DNS Domain
Filters	192	on	off	192.168.1.2 - 192.168.1.254 /255.255.255.0		192.168.1.1	300	300	
Tools									
System Tools									
CLI									
Logout									

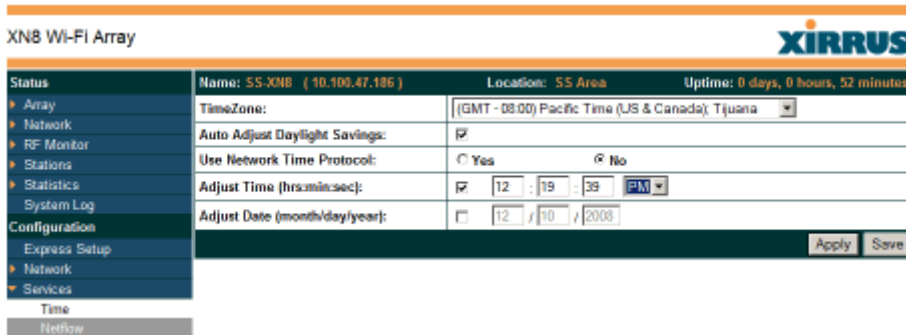
Figure 112. Services

The following sections discuss configuring services on the Array:

- “Time Settings (NTP)” on page 193
- “NetFlow” on page 195
- “System Log” on page 196
- “SNMP” on page 199
- “DHCP Server” on page 202

## Time Settings (NTP)

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



XN8 Wi-Fi Array		XIRRUS	
Status	Name: 55-XN8 (10.109.47.186)	Location: SS Area	Uptime: 0 days, 0 hours, 52 minutes
Array	TimeZone:	(GMT - 08:00) Pacific Time (US & Canada); Tijuana	
Network	Auto Adjust Daylight Savings:	<input checked="" type="checkbox"/>	
RF Monitor	Use Network Time Protocol:	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Stations	Adjust Time (hrs:min:sec):	<input checked="" type="checkbox"/>	12 : 19 : 39 PM
Statistics	Adjust Date (month/day/year):	<input type="checkbox"/>	12 / 10 / 2008
System Log	Apply Save		
Configuration			
Express Setup			
Network			
Services			
Time			
Help			

Figure 113. Time Settings (Manual Time)

### Procedure for Managing the Time Settings

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

- b. **Adjust Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, 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).

## 5. Using an NTP Server

- a. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.

The screenshot shows the configuration page for an XN8 Wi-Fi Array. The page title is "XN8 Wi-Fi Array" and the XIRRUS logo is in the top right. A navigation menu on the left includes Status, Array, Network, RF Monitor, Stations, Statistics, System Log, Configuration (selected), Express Setup, Network, Services, Time, and Reflow. The main content area shows the following settings:

Status	Name: SS-XN8 (10.100.47.126)	Location: SS Area	Uptime: 0 days, 0 hours, 52 minutes
TimeZone:	[(GMT - 08:00) Pacific Time (US & Canada), Tijuana]		
Auto Adjust Daylight Savings:	<input checked="" type="checkbox"/>		
Use Network Time Protocol:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
NTP Primary Server:	time.nist.gov		
NTP Secondary Server:	pool.ntp.org		
<input type="button" value="Apply"/> <input type="button" value="Save"/>			

Figure 114. Time Settings (NTP Time Enabled)

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

### See Also

Services

SNMP

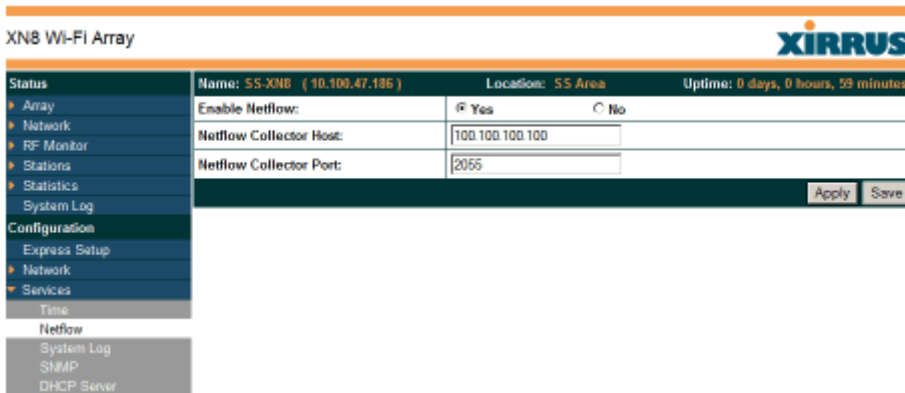
System Log



## NetFlow

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

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



Status	Name: 55-XN8 (10.100.47.186)	Location: 55 Area	Uptime: 0 days, 0 hours, 29 minutes
<ul style="list-style-type: none"> <li>Array</li> <li>Network</li> <li>RF Monitor</li> <li>Stations</li> <li>Statistics</li> <li>System Log</li> </ul>	Enable Netflow:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
	Netflow Collector Host:	100.100.100.100	
	Netflow Collector Port:	2055	
		<input type="button" value="Apply"/> <input type="button" value="Save"/>	

Figure 115. NetFlow

### *Procedure for Configuring NetFlow*

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

## System Log

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

XN8 Wi-Fi Array		XIRRUS
Status	Name: SS-XNB (10.100.47.186)	Location: SS Area Uptime: 0 days, 1 hour, 1 minute
Enable Syslog Server:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Console Logging:	<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local File Size (1-500):	<input type="text" value="500"/>	
Primary Server Address (Domain or IP):	<input type="text" value="10.100.100.117"/>	
Secondary Server Address (Domain or IP):	<input type="text" value="10.100.101.117"/>	
Tertiary Server Address (Domain or IP):	<input type="text"/>	
Email SMTP Address (Domain or IP):	<input type="text" value="mail.xyzcorp.com"/>	
Email SMTP User:	<input type="text" value="networkAdmin"/>	
Email SMTP Password:	<input type="password" value="*****"/>	
Email SMTP From:	<input type="text" value="Array12345"/>	
Email SMTP To:	<input type="text" value="networkAdmin"/>	
<b>Syslog Levels</b>		
Console Logging:	<input type="text" value="Information and more serious"/>	
Local File:	<input type="text" value="Information and more serious"/>	
Primary Server:	<input type="text" value="Information and more serious"/>	
Secondary Server:	<input type="text" value="Information and more serious"/>	
Tertiary Server:	<input type="text" value="Information and more serious"/>	
Email SMTP Server:	<input type="text" value="Warning and more serious"/>	
		<input type="button" value="Apply"/> <input type="button" value="Save"/>

Figure 116. System Log

### Procedure for Configuring Syslog

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

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

- b. **Local File:** For records to be stored on the Array's internal Syslog file, choose your preferred level of Syslog reporting from the pull-down list. The default level is **Debugging and more serious**.
  - c. **Primary Server:** Choose the preferred level of Syslog reporting for the primary server. The default level is **Debugging and more serious**.
  - d. **Secondary/Tertiary Server:** Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Information and more serious**. (Optional)
  - e. **Email SMTP Server:** Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.
8. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

System Log Window

Services

SNMP

Time Settings (NTP)

### SNMP

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

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

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

<b>Status</b> Name: 55-XN9429991D207 [ 10.190.47.19 ] Uptime: 0 days, 2 hours, 27 mins	
<b>Array</b>	
Network	Enable SNMPv2: <input checked="" type="radio"/> Yes <input type="radio"/> No
RF Monitor	Read-Write Community String: [*****]
Stations	Read-Only Community String: [*****]
Statistics	<b>SNMPv3 Settings</b>
System Log	Enable SNMPv3: <input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Configuration</b>	Authentication: <input checked="" type="radio"/> SHA <input type="radio"/> MD5
Express Setup	Privacy: <input checked="" type="radio"/> AES <input type="radio"/> DES
Network	Context Engine ID: 8000521503000f7d14cb80
Services	Read-Write Username: xirrus-rw
Time	Read-Write Authentication Password: [*****]
Netflow	Read-Write Privacy Password: [*****]
System Log	Read-Only Username: xirrus-ro
<b>SNMP</b>	Read-Only Authentication Password: [*****]
DHCP Server	Read-Only Privacy Password: [*****]
VLANs	<b>SNMP Trap Settings</b>
Security	Trap Host 1 IP Address: [xirrus-XMS] Port: [162]
SSIDs	Trap Host 2 IP Address: [ ] Port: [162]
Groups	Trap Host 3 IP Address: [ ] Port: [162]
IAPs	Trap Host 4 IP Address: [ ] Port: [162]
WDS	Send Auth Failure Traps: <input checked="" type="radio"/> Yes <input type="radio"/> No
Filters	Keepalive Trap Interval: [1]
<b>Tools</b>	[Apply] [Save]
System Tools	
CLI	

Figure 117. SNMP

---

### *Procedure for Configuring SNMP*

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

11. **SNMP Read-Only Username:** Enter the read-only user name. This username and password do not allow configuration changes to be made on the Array. The default is **xirrus-ro**.
12. **SNMP Read-Only Authentication Password:** Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.
13. **SNMP Read-Only Privacy Password:** Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.
14. **SNMP Trap Host IP Address:** Enter the **IP Address** or domain name, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. Note that by default, **Trap Host 1** sends traps to **Xirrus-XMS**. Thus, the Array will automatically communicate its presence to XMS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

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

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

### *See Also*

Services

System Log

Time Settings (NTP)

## DHCP Server

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

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

DHCP Pool	On	Lease Time		NAT	Lease IP Range		Subnet Mask	Gateway	Domain	DNS Servers	Delete
		Default	Max		Start	End					
192	<input checked="" type="checkbox"/>	300	300	<input type="checkbox"/>	192.168.1.2	192.168.1.254	255.255.255.0	192.168.1.1	whatsamattaU	192.168.1.1	<input type="checkbox"/>

Figure 118. DHCP Management

DHCP usage is determined in several windows—see [SSID Management](#), [Group Management](#), and [VLAN Management](#).

### *Procedure for Configuring the DHCP Server*

1. **New Internal DHCP Pool:** Enter a name for the new DHCP pool, then click on the **Create** button. The new pool ID is added to the list of available DHCP pools.
2. **On:** Click this checkbox to make this pool of addresses available, or clear it to disable the pool.



3. **Lease Time—Default:** This field defines the default **DHCP lease** time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
4. **Lease Time—Max:** Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.
5. **Network Address Translation (NAT):** Check this box to enable the Network Address Translation feature.
6. **Lease IP Range—Start:** Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End:** Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask:** Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway:** If necessary, enter the IP address of the gateway.
10. **Domain:** Enter the DNS domain name. See “[DNS Settings](#)” on page 188.
11. **DNS Servers (1 to 3):** Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the assigned IP address. Note that if you leave these blank, no DNS information is sent to the stations. DHCP will **not** default to sending the DNS servers that are configured in DNS Settings. See also, “[DNS Settings](#)” on page 188.
12. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

[DHCP Leases](#)  
[DNS Settings](#)  
[Network Map](#)

## VLANS

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

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN ([Step 1 page 206](#)).

VLAN Name	Number	Management	DHCP	IP Address	Subnet Mask	Gateway	Tunnel Server	Port	State
VoIP	12	disallowed	disabled	10.10.10.10	255.255.255.0	10.10.10.1	10.10.10.8	0	down
Finance	5	disallowed	enabled						

Figure 119. VLANs



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

## Understanding Virtual Tunnels

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

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

### *Virtual Tunnel Server (VTS)*

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from [vtun.sourceforge.net](http://vtun.sourceforge.net). To enable the Array to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in [Step 10](#) on [page 207](#).

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

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

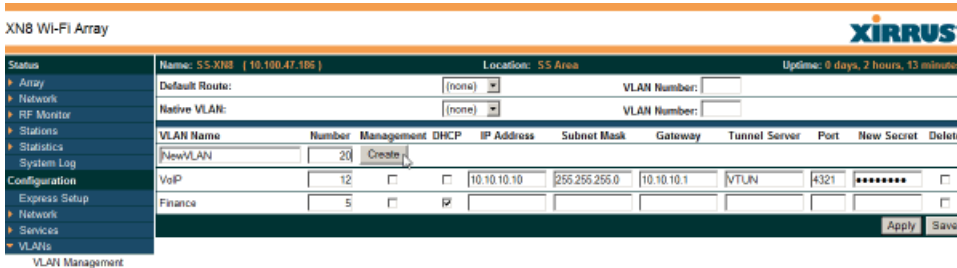
### *Client-Server Interaction*

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

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

## VLAN Management

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



The screenshot shows the 'VLAN Management' window in the XIRRUS Wi-Fi Array interface. The window title is 'XN8 Wi-Fi Array'. The top right corner shows the XIRRUS logo and 'Uptime: 9 days, 2 hours, 13 minutes'. The main configuration area includes fields for 'Default Route' (set to '(none)') and 'Native VLAN' (set to '(none)'), both with 'VLAN Number' fields. Below these is a table of VLANs:

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

At the bottom right of the table area are 'Apply' and 'Save' buttons. A 'New VLAN' dialog box is open, showing a 'Create' button.

Figure 120. VLAN Management



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

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

### Procedure for Managing VLANs

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

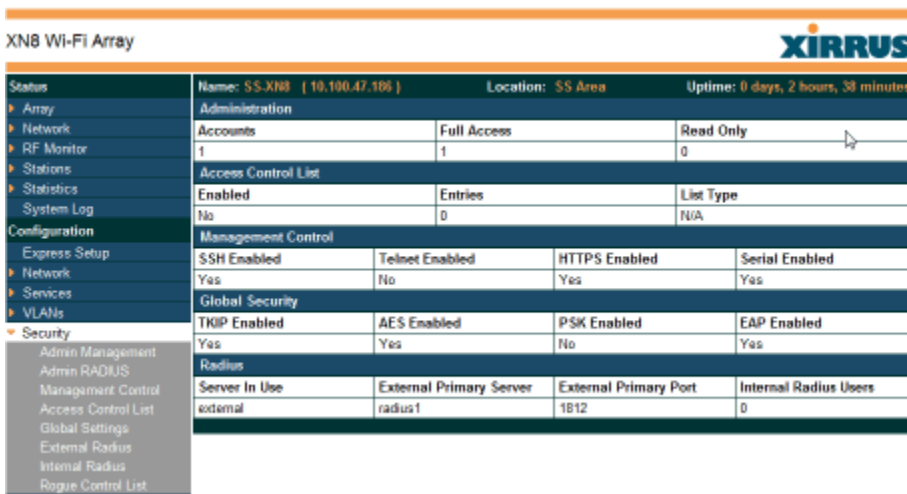
3. **New VLAN Name/Number:** Enter a name and number for the new VLAN in this field, then click on the **Create** button. The new VLAN is added to the list.
4. **VLAN Number:** Enter a number for this VLAN (1-4094).
5. **Management:** Check this box to allow management over this VLAN.
6. **DHCP:** Check this box if you want the DHCP server to assign the IP address, subnet mask and gateway address to the VLAN automatically, otherwise you must go to the next step and assign these parameters manually.
7. **IP Address:** If the DHCP option is disabled, enter a valid IP address for this VLAN association.
8. **Subnet Mask:** If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.
9. **Gateway:** If the DHCP option is disabled, enter the IP gateway address for this VLAN association.
10. **Tunnel Server:** If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see [“Understanding Virtual Tunnels” on page 204](#).
11. **Port:** If this VLAN is to be tunneled, enter the port number of the tunnel server.
12. **New Secret:** Enter the password expected by the tunnel server.
13. **Delete:** To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.
14. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

VLAN Statistics  
VLANs

## Security

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




XN8 Wi-Fi Array			
Status	Name: SS-XN8 (19.100.47.106)	Location: SS Area	Uptime: 0 days, 2 hours, 38 minutes
Array	Administration		
Network	Accounts	Full Access	Read Only
RF Monitor	1	1	0
Stations	Access Control List		
Statistics	Enabled	Entries	List Type
System Log	No	0	N/A
Configuration	Management Control		
Express Setup	SSH Enabled	Telnet Enabled	HTTPS Enabled
Network	Yes	No	Yes
Services	Global Security		
VLANs	TKIP Enabled	AES Enabled	PSK Enabled
Security	Yes	Yes	No
Admin Management	Radius		
Admin RADIUS	Server In Use	External Primary Server	External Primary Port
Management Control	external	radius1	1812
Access Control List			Internal Radius Users
Global Settings			0
External Radius			
Internal Radius			
Rogue Control List			

Figure 121. Security

For additional information about wireless network security, refer to:

- “Security Planning” on page 70
- “Understanding Security” on page 209
- The Security section of “Frequently Asked Questions” on page 404.

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

- “Certificates and Connecting Securely to the WMI” on page 212

Security settings are configured with the following windows:

- “Admin Management” on page 214

- “Admin RADIUS” on page 215
- “Management Control” on page 218
- “Access Control List” on page 222
- “Global Settings” on page 224
- “External Radius” on page 227
- “Internal Radius” on page 230
- “Rogue Control List” on page 233

### Understanding Security

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

Other security considerations include:

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

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

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

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

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

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

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see “[SSID Management](#)” on page 240). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security>Global Settings** window under **WPA Settings** (see “[Global Settings](#)” on page 224).



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

This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.
  - **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the Wi-Fi Array) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.
  - **MAC Address ACLs (Access Control Lists)**—MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC address of each user in the Allow list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the Deny list.

The Wi-Fi Array will accept up to 1,000 ACL entries.
- **PCI DSS or FIPS 140-2 Security**—to implement the requirements of these security standards on the Wi-Fi Array, please see [Appendix D: Implementing PCI DSS](#) or [Appendix E: Implementing FIPS Security](#).

## Certificates and Connecting Securely to the WMI

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

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

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

- Using the Array's Default Certificate
- Using an External Certificate Authority

### Using the Array's Default Certificate

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

Figure 122. Import Xirrus Certificate Authority

The Array's certificate is signed by a Xirrus CA that is customized for your Array and its current host name. By default, browsers will not trust the Array's certificate. You may import the Xirrus certificate to instruct the browser to trust

the Xirrus CA on all future connections to Arrays. The certificate for the Xirrus CA is available on the Array, so that you can import it into your browser's cache of trusted CAs (right alongside VeriSign, for example). On the [Management Control](#) window of the WMI you will see the `xirrus-ca.crt` file. (Figure 122)

By clicking and opening this file, you can follow your browser's instructions and import the Xirrus CA into your CA cache (see [page 220](#) for more information). This instructs your browser to trust any of the certificates signed by the Xirrus CA, so that when you connect to any of our Arrays you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the Array. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for 'hostname'.

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

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

### Using an External Certificate Authority

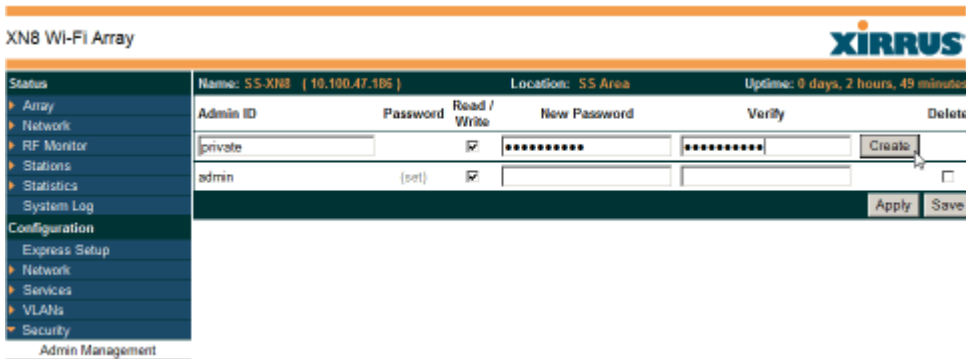
If you prefer, you may install a certificate on your Array signed by an outside CA.

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

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the Array after you obtain it from the CA. This certificate will be tied to the Array's host name and private key. See ["External Certification Authority"](#) on [page 221](#) for more details.

## Admin Management

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



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

Apply Save

Figure 123. Admin Management

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

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

### *See Also*

External Radius

Global Settings (IAP)

Internal Radius

Management Control

Security

## **Admin RADIUS**

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

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

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

### **About Creating Admin Accounts on the RADIUS Server**

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Service-Type** attribute (Attribute 6). To grant read-write permission, configure the RADIUS server to send back the Service-Type attribute with a value of **Administrative**. To grant read-only permission, the RADIUS server should send the Service-Type attribute with a value of **NAS Prompt**.

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

Figure 124. Admin RADIUS

### *Procedure for Configuring Admin RADIUS*

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

#### **1. Admin RADIUS Settings:**

- a. **Enable Admin RADIUS:** Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.
- b. **Authentication Type:** Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).
  - PAP (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network “in the clear” (unencrypted) and is therefore considered insecure.

- CHAP (Challenge-Handshake Authentication Protocol) is a more secure Protocol. The login request is sent using a one-way hash function.
  - c. **Timeout (seconds):** Define the maximum idle time (in seconds) before the RADIUS server's session times out. The default is 600 seconds.
2. **Admin RADIUS Primary Server:** This is the RADIUS server that you intend to use as your primary server.
- a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
  - b. **Port Number:** Enter the port number of this RADIUS server. The default is 1812.
  - c. **Shared Secret / Verify Secret:** Enter the shared secret that this RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.



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

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

## Management Control

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

XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 3 hours, 1 minute
Array	SSH		
Network	Enable Management:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
RF Monitor	Connection Timeout 30-100000 (Seconds):	<input type="text" value="300"/>	
Stations	Port:	<input type="text" value="22"/>	
Statistics	Telnet		
System Log	Enable Management:	<input type="radio"/> Yes	<input checked="" type="radio"/> No
Configuration	Connection Timeout 30-100000 (Seconds):	<input type="text" value="300"/>	
Express Setup	Port:	<input type="text" value="23"/>	
Network	Serial		
Services	Enable Management:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
VLANs	Connection Timeout 30-100000 (Seconds):	<input type="text" value="300"/>	
Security	HTTPS		
Admin Management	Connection Timeout 30-100000 (Seconds):	<input type="text" value="300"/>	
Admin RADIUS	Port:	<input type="text" value="443"/>	
Management Control	Import Xirrus Authority Into Browser:	<input type="text" value="xirrus-ca.crt"/>	
Access Control List	HTTPS (X.509) Certificate Signed By	<input type="text" value="Xirrus"/>	
Global Settings	External Certification Authority		
External Radius	Download Certificate Signing Request	<input type="text" value="SS-XN8.csr"/>	
Internal Radius	Upload Signed Certificate:	<input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>	
Rogue Control List	Common Name:	<input type="text" value="SS-XN8"/>	
SSIDs	Organization Name:	<input type="text"/>	
Groups	Organizational Unit Name:	<input type="text"/>	
IAPs	Locality (City):	<input type="text"/>	
WDS	State or Province:	<input type="text"/>	
Filters	Country Name (2 Letter Code):	<input type="text"/>	
Tools	Email Address:	<input type="text"/>	
System Tools	Create New Certificate Signing Request	<input type="button" value="Create"/>	
CU	<input type="button" value="Apply"/> <input type="button" value="Save"/>		
Logout			
Log Messages			
Critical 6			
Warning 8			
Information 500			

Figure 125. Management Control

### Procedure for Configuring Management Control

#### 1. SSH:

- a. **Enable Management:** Choose **Yes** to enable management of the Array over a Secure Shell (SSH-2) connection, or **No** to disable this feature. Be aware that only SSH-2 connections are supported by the



Array. SSH clients used for connecting to the Array must be configured to use SSH-2.

- b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
  - c. Port:** Enter a value in this field to define the port used by SSH. The default port is 22.
- 2. Telnet:**
- a. Enable Management:** Choose **Yes** to enable Array management over a Telnet connection, or **No** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.
  - b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
  - c. Port:** Enter a value in this field to define the port used by Telnet. The default port is 23.
- 3. Serial**
- a. Enable Management:** Choose **Yes** to enable management of the Array via a serial connection, or choose **No** to disable this feature.
  - b. Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

#### 4. HTTPS

- a. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.
- b. **Port:** Enter a value in this field to define the port used by SSH. The default port is 443.
- c. **Import Xirrus Authority into Browser:** This feature imports the Xirrus Certificate Authority (CA) into your browser (for a discussion, please see [“Certificates and Connecting Securely to the WMI” on page 212](#)). Click the link ([xirrus-ca.crt](#)), and then click **Open** to view or install the current Xirrus CA certificate. Click **Install Certificate** to start your browser’s Certificate Install Wizard. We recommend that you use this process to install Xirrus as a root authority in your browser.

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

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

## 5. External Certification Authority

This Step and [Step 6](#) allow you to obtain a certificate from an external authority and install it on an Array. “[Using an External Certificate Authority](#)” on page 213 discusses reasons for using an external CA.

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

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

External Certification Authority has the following fields:

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

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

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

*See Also*

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

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

[Admin Management](#)

[External Radius](#)

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

[Internal Radius](#)

[Access Control List](#)

[Security](#)

**Access Control List**

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

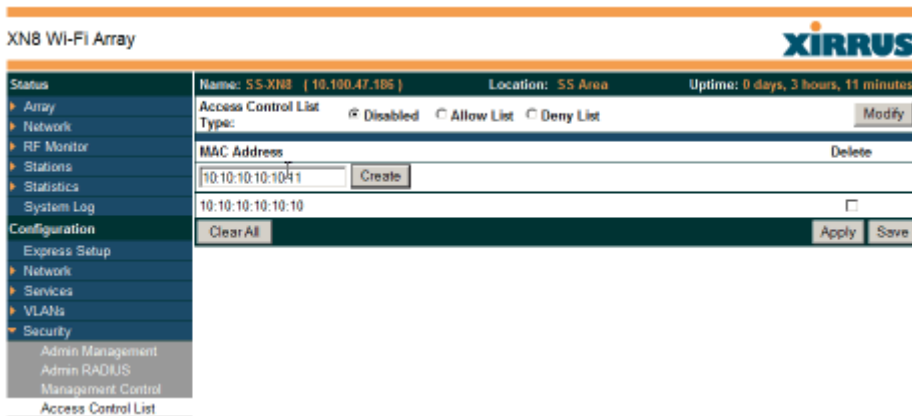


Figure 126. Access Control List

### *Procedure for Configuring Access Control Lists*

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



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

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

### *See Also*

External Radius

Global Settings (IAP)

Internal Radius

Management Control

Security

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

## Global Settings

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

For additional information about wireless network security, refer to “Security Planning” on page 70 and “Understanding Security” on page 209.

XN8 Wi-Fi Array			
<b>Status</b>	Name: SS-XN8 ( 10.100.47.186 )	Location: SS Area	Uptime: 0 days, 3 hours, 25 minutes
Array	RADIUS Server Mode:	<input type="radio"/> Internal	<input checked="" type="radio"/> External
Network	WPA Settings:		
RF Monitor	TKIP Enabled:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Stations	AES Enabled:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Statistics	WPA Group Rekey Time (seconds):	<input type="text"/>	Never: <input checked="" type="checkbox"/>
System Log	PSK Authentication:	<input type="radio"/> Yes	<input checked="" type="radio"/> No
<b>Configuration</b>	WPA Preshared Key / Verify Key:	<input type="text"/>	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
Express Setup	EAP Authentication:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Network	WEP Settings:		
Services	Encryption Key 1 / Verify Key 1:	<input type="text"/>	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
VLANs	Encryption Key 2 / Verify Key 2:	<input type="text"/>	<input checked="" type="radio"/> ASCII <input type="radio"/> Hexadecimal
Security	Encryption Key 3 / Verify Key 3:	<input type="text"/>	<input type="radio"/> ASCII <input type="radio"/> Hexadecimal
Admin Management	Encryption Key 4 / Verify Key 4:	<input type="text"/>	<input type="radio"/> ASCII <input type="radio"/> Hexadecimal
Admin RADIUS	Default Key:	Key 2	
Management Control			<input type="radio"/> 40 bit (WEP-64)
Access Control List			<input type="radio"/> 104 bit (WEP-128)
<b>Global Settings</b>			<input type="radio"/> 40 bit (WEP-64)
External Radius			<input checked="" type="radio"/> 104 bit (WEP-128)
Internal Radius			<input type="radio"/> 40 bit (WEP-64)
Rogue Control List			<input type="radio"/> 104 bit (WEP-128)
SSIDs			<input type="radio"/> 40 bit (WEP-64)
Groups			<input type="radio"/> 104 bit (WEP-128)
IAPs			
WDS			
Filters			
Tools			
			<input type="button" value="Apply"/> <input type="button" value="Save"/>

Figure 127. Global Settings (Security)

### *Procedure for Configuring Network Security*

1. **RADIUS Server Mode:** Choose the RADIUS server mode you want to use, either Internal or External. Parameters for these modes are configured in “External Radius” on page 227 and “Internal Radius” on page 230.

#### **WPA Settings**

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

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



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

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

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

## WEP Settings

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

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

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

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

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

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



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

### See Also

[Admin Management](#)  
[External Radius](#)  
[Internal Radius](#)  
[Access Control List](#)  
[Management Control](#)  
[Security](#)



### External Radius

This window allows you to define the parameters of an external RADIUS server for user authentication. To set up an external RADIUS server, you must choose **External** as the RADIUS server mode in Global Settings. Refer to “Global Settings” on page 224.

<b>Status</b>	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 0 days, 3 hours, 30 minutes
Array	Primary Server		
Network	Host Name / IP Address:	<input type="text" value="radius1"/>	
RF Monitor	Port Number:	<input type="text" value="1812"/>	
Stations	Shared Secret / Verify Secret: <input type="password" value="*****"/> <input type="password" value="*****"/>		
Statistics	Secondary Server		
System Log	Host Name / IP Address:	<input type="text"/>	
<b>Configuration</b>	Port Number:	<input type="text" value="1812"/>	
Express Setup	Shared Secret / Verify Secret: <input type="password"/> <input type="password"/>		
Network	<b>Settings</b>		
Services	Timeout (seconds):	<input type="text" value="600"/>	
VLANs	NAS Identifier:	<input type="text"/>	
Security	Accounting:	<input type="checkbox"/> Off <input checked="" type="checkbox"/> On	
Admin Management	<b>Accounting</b>		
Admin RADIUS	Accounting Interval (seconds):	<input type="text" value="300"/>	
Management Control	Primary Server Host Name / IP Address:	<input type="text" value="radius1"/>	
Access Control List	Primary Server Port Number:	<input type="text" value="1813"/>	
Global Settings	Primary Server Shared Secret / Verify Secret:	<input type="password" value="*****"/> <input type="password" value="*****"/>	
<b>External Radius</b>	Secondary Server Host Name / IP Address:	<input type="text"/>	
Internal Radius	Secondary Server Port Number:	<input type="text" value="1813"/>	
Rogue Control List	Secondary Server Shared Secret / Verify Secret:	<input type="password"/> <input type="password"/>	
SSIDs	<input type="button" value="Apply"/> <input type="button" value="Save"/>		
Groups			
IAPs			
WDS			
Filters			
<b>Tools</b>			
System Tools			
CLI			
Logout			

Figure 128. External RADIUS Server

If you want to include user group membership in the RADIUS account information for users, see “Understanding Groups” on page 248. User groups allow you to easily apply a uniform configuration to a user on the Array.

---

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

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



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

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

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

- c. **Accounting:** If you would like the Array to send RADIUS Start, Stop, and Interim records to a RADIUS accounting server, click the **On** button and click **Apply**. The account settings appear, and must be configured.
4. **Accounting Settings:**
- a. **Accounting Interval (seconds):** Specify how often Interim records are to be sent to the server. The default is 300 seconds.
  - b. **Primary Server Host Name / IP Address:** Enter the IP address or domain name of the primary RADIUS accounting server that you intend to use.
  - c. **Primary Port Number:** Enter the port number of the primary RADIUS accounting server. The default is 1813.
  - d. **Primary Shared Secret / Verify Secret:** Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.
  - e. **Secondary Server Host Name / IP Address (optional):** If desired, enter an IP address or domain name for an alternative RADIUS accounting server. If the primary server becomes unreachable, the Array will “failover” to this secondary server (defined here).
  - f. **Secondary Port Number:** If using a secondary accounting server, enter its port number. The default is 1813.
  - g. **Secondary Shared Secret / Verify Secret:** If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.
5. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

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

### Internal Radius

This window allows you to define the parameters for the Array’s internal RADIUS server for user authentication. However, the internal RADIUS server will only authenticate wireless clients that want to associate to the Array. This can be useful if an external RADIUS server is not available. To set up the internal RADIUS server, you must choose **Internal** as the RADIUS server mode in Global Settings. Refer to “Global Settings” on page 224.

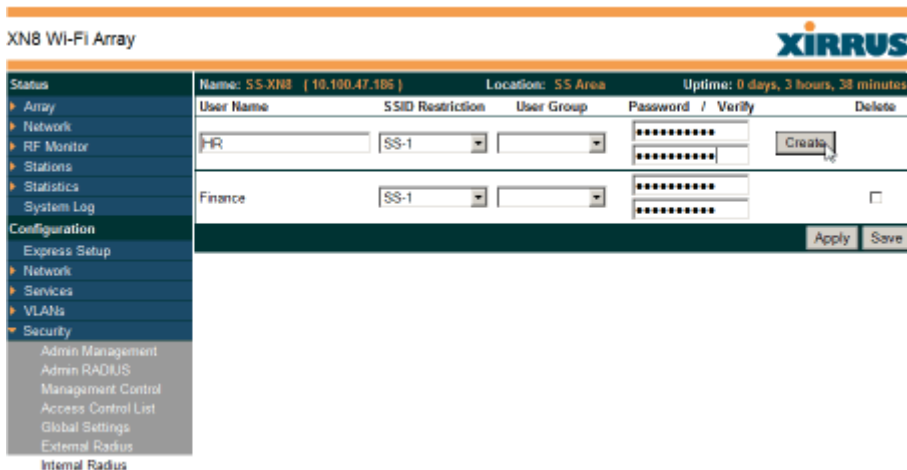


Figure 129. Internal RADIUS Server



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

#### ***Procedure for Creating a New User***

1. **User Name:** Enter the name of the user that you want to authenticate to the internal RADIUS server.
2. **SSID Restriction:** (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the pull-down list.
3. **User Group:** (Optional) If you want to make this user a member of a previously defined user group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See ["Understanding Groups"](#) on page 248.
4. **Password:** (Optional) Enter a password for the user.
5. **Verify:** (Optional) Retype the user password to verify that you typed it correctly.
6. Click on the **Create** button to add the new user to the list.

#### ***Procedure for Managing Existing Users***

1. **SSID Restriction:** (Optional) If you want to restrict a user to associating to a particular SSID, choose an SSID from its pull-down list.
2. **User Group:** (Optional) If you want to change the user's group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See ["Understanding Groups"](#) on page 248.
3. **Password:** (Optional) Enter a new password for the selected user.

4. **Verify Password:** (Optional) Retype the user password to verify that you typed it correctly.
5. If you want to delete one or more users, check their **Delete** check boxes, then click **Apply** or **Save**.
6. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

Admin Management

External Radius

Global Settings (IAP)

Access Control List

Management Control

Security

Understanding Groups

### Rogue Control List

This window allows you to set up a control list for rogue APs, based on a type that you define. You may classify rogue APs as blocked, so that the Array will take steps to prevent stations from associating with the blocked AP. See “About Blocking Rogue APs” on page 278. The Array can keep up to 5000 entries in this list. When finished, click on the **Save** button to save your changes.



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

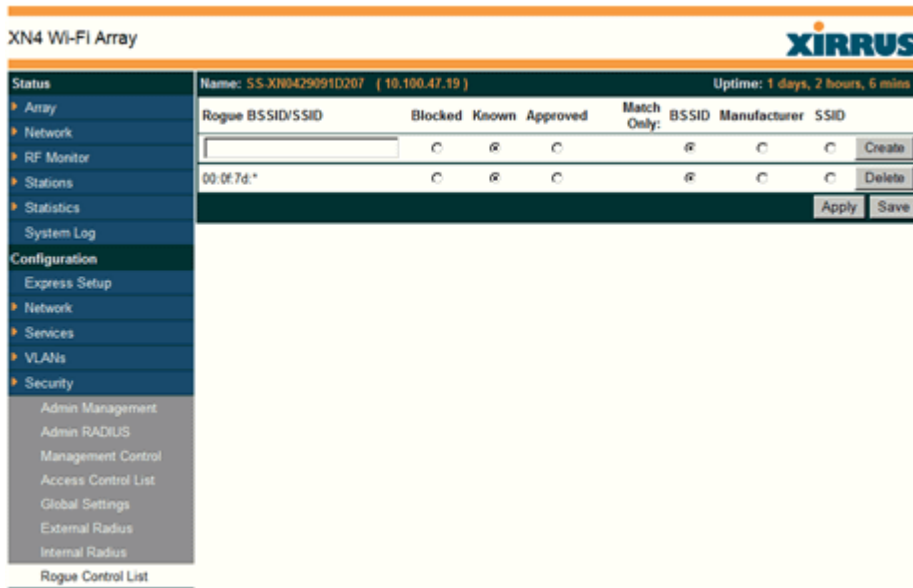


Figure 130. Rogue Control List

### *Procedure for Establishing Rogue AP Control*

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

You may use the “\*” character as a wildcard to match any string at this position. For example, 00:0f:7d:\* matches any string that starts with 00:0f:7d:. Since Xirrus Arrays start with 00:0f:7d:, this applies the Rogue Control Type to all Xirrus Arrays.

2. **Rogue Control Classification:** Enter the classification for the specified rogue AP(s), either **Blocked**, **Known** or **Approved**.
3. **Match Only:** Select the match criterion to compare the **Rogue BSSID/SSID** string against: **BSSID**, **Manufacturer**, or **SSID**. The BSSID field contains the MAC address.
4. Click **Create** to add this rogue AP to the Rogue Control List.
5. **Rogue Control List:** If you want to edit the control type for a rogue AP, just click the radio button for the new type for the entry: **Blocked**, **Known** or **Approved**, then click **Apply** or **Save** to apply your change.
6. To delete rogue APs from the list, click their **Delete** checkboxes, then click **Apply** or **Save**.
7. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

#### *See Also*

[Network Map](#)

[Intrusion Detection](#)

[SSIDs](#)

[SSID Management](#)



## SSIDs

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



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

For information to help you understand SSIDs and how multiple SSIDs are managed by the Wi-Fi Array, go to “Understanding SSIDs” on page 236 and the Multiple SSIDs section of “Frequently Asked Questions” on page 404. For a description of how QoS operates on the Array, see “Understanding QoS Priority on the Wi-Fi Array” on page 237.

XN8 Wi-Fi Array												
XIRRUS												
Status	Name: SS-XNB ( 10.100.47.186 )			Location: SS Area			Uptime: 0 days, 4 hours, 10 minutes					
Array	SSID	Authentication & Encryption	Security Settings	Filter List	VLAN	Num	QoS	Band	Roaming Layer	Broadcast	DHCP Pool	WPR
Network	testSSID	802.1x	WPA	Unique	none		2	Both	2-only	Off	none	Off
RF Monitor	SS-1	Open	None	Global	none		2	Both	2-only	On	192	Off
Stations	Limits											
Statistics	SSID	Enabled	Station Limit	SSID Traffic	Station Traffic	Time On	Time Off	Days On	Active			
System Log	testSSID	Yes	1024	Unlimited	Unlimited	Always	Never	All	Yes			
Configuration	SS-1	Yes	512	Unlimited	Unlimited	Always	Never	All	Yes			
Express Setup												
Network												
Services												
VLANs												
Security												
SSIDs												
SSID Management												

Figure 131. SSIDs

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

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

### Understanding SSIDs

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

### *Multiple SSIDs*

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

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

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

### *Using SSIDs*

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

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

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

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

*See Also*

- SSID Management
- SSIDs
- Understanding SSIDs

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



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

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

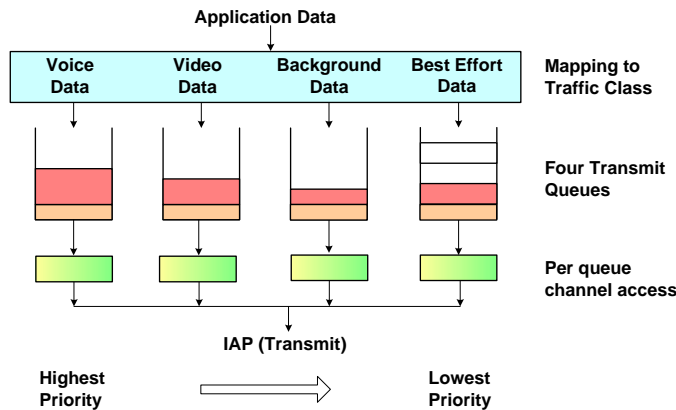


Figure 132. Four Traffic Classes

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

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

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

- Wired QoS - Ethernet Port:

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

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

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

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

#### Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 0 is the default. See [“SSID Management” on page 240](#). If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.
- The Array supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.
- How QoS is set for a packet in case of conflicting values:
  - a. If an SSID has a QoS setting, and an incoming wired packet’s user priority tag is mapped to a higher QoS value, then the higher QoS value is used.
  - b. If a group or filter has a QoS setting, this overrides the QoS value above. See [“Groups” on page 248](#), and [“Filters” on page 291](#).
  - c. Voice packets have the highest priority, as described below ([Voice Support](#)).

#### Packet Filtering QoS classification

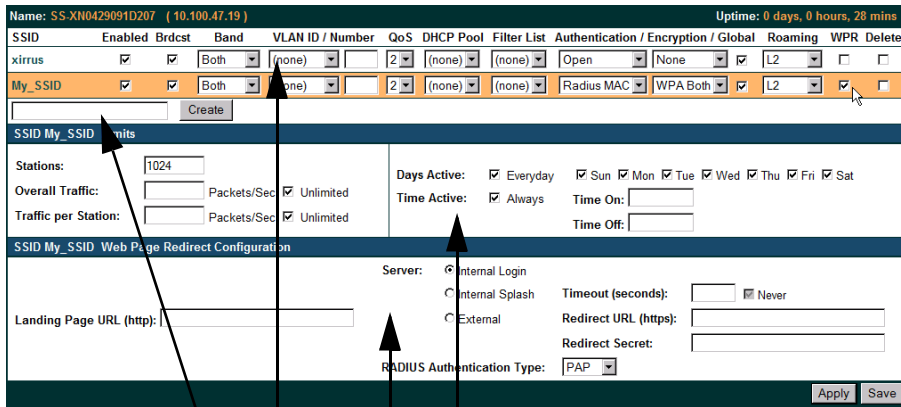
- Filter rules can be used to redefine the QoS priority level to override defaults. See [“Filter Management” on page 295](#). This allows the QoS priority level to be assigned based on protocol, source, or destination.

Voice Support

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

SSID Management

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



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

Figure 133. SSID Management

Procedure for Managing SSIDs

1. **New SSID Name:** To create a new SSID, enter a new SSID name to the left of the Create button (Figure 133), then click Create. The SSID name may only consist of the characters A-Z, a-z, 0-9, dash, and underscore. You may create up to 16 SSIDs.

SSID List (top of page)

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

3. **On:** Check this box to activate this SSID or clear it to deactivate it.
4. **Brdcast:** Check this box to make the selected SSID visible to all clients on the network. Although the Wi-Fi Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Clear this box if you do not want this SSID to be visible on the network.
5. **Band:** Choose which wireless band the SSID will be beacons on. Select either **5 GHz—802.11a(n)**, **2.4 GHz—802.11b(n)** or **Both**.
6. **VLAN ID / Number:** From the pull-down list, select a VLAN that you want this traffic to be forwarded to on the wired network. Select **numeric** to enter the number of a previously defined VLAN in the **Number** field (see “[VLANs](#)” on page 204). This step is optional.
7. **QoS:** (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:
  - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
  - 1—Medium, with QoS prioritization aggregated across all traffic types.
  - 2—High, normally used to give priority to video traffic.
  - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

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

8. **DHCP Pool:** If you want to associate an internal DHCP pool to this SSID, choose the pool from the pull--down list. An internal DHCP pool must be created before it can be assigned. To create an internal DHCP pool, go to “[DHCP Server](#)” on page 202.

9. **Filter List:** If you wish to apply a set of filters to this SSID's traffic, select the desired Filter List. See "Filters" on page 291.

10. **Authentication:** The following authentication options are available:

- **Open:** This option provides no authentication and is not recommended.
- **RADIUS MAC:** Uses an external RADIUS server to authenticate stations onto the Wi-Fi network, based on the user's MAC address. Accounting for these stations is performed according to the accounting options that you have configured specifically for this SSID or globally (see Step 12 below).



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

- **802.1x:** Authenticates stations onto the Wi-Fi network via a RADIUS server using 802.1x with EAP. The RADIUS server can be internal (provided by the Wi-Fi Array) or external.

11. **Encryption:** From the pull-down list, choose the encryption that will be required—specific to this SSID—either None, WEP, WPA, WPA2 or WPA-Both. The None option provides no security and is not recommended; WPA2 provides the best practice Wi-Fi security.

Each SSID supports only one encryption type at a time (except that WPA and WPA2 are both supported on an SSID if you select WPA-Both). If you need to support other encryption types, you must define additional SSIDs. The encryption standard used with WPA or WPA2 is selected in the Security>Global Settings window (page 224). For an overview of the security options, see "Security Planning" on page 70 and "Understanding Security" on page 209.

12. **Global:** Check the checkbox if you want this SSID to use the security settings established at the global level (refer to "Global Settings" on page 224). Clear the checkbox if you want the settings established here to take precedence. Additional sections will be displayed to allow you to



configure encryption, RADIUS, and RADIUS accounting settings. The **WPA Configuration** encryption settings have the same parameters as those described in “Procedure for Configuring Network Security” on page 225. The external RADIUS and accounting settings are configured in the same way as for an external RADIUS server (see “Procedure for Configuring an External RADIUS Server” on page 228). Note that external RADIUS servers may be specified using IP addresses or domain names.

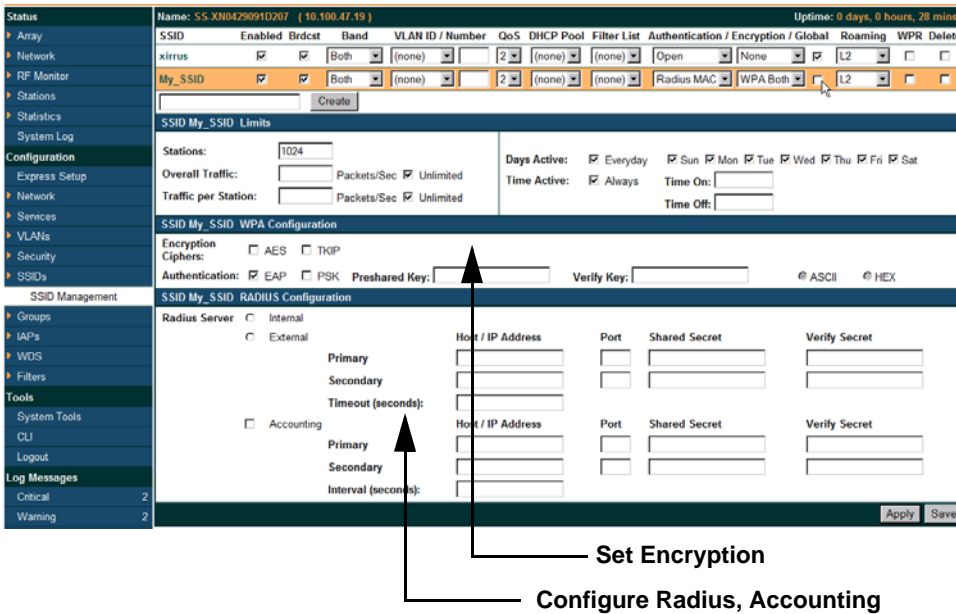


Figure 134. SSID Management

13. **L3:** For this SSID, Check the checkbox to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3, or clear the checkbox to allow roaming at Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in *Global Settings (IAP)*. See “Understanding Fast Roaming” on page 255.

- 14. WPR (Web Page Redirect):** Check the checkbox to enable the Web Page Redirect functionality, or clear it to disable this option. If enabled, WPR configuration fields will be displayed under the SSID Limits section. This feature may be used to provide an alternate mode of authentication, or to simply display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. For example, some wireless devices and users may not have a correctly configured 802.1x (RADIUS) supplicant. Utilizing WPR's Web-based login, users may be authenticated without using an 802.1x supplicant. See [“Web Page Redirect Configuration Settings”](#) on page 245 for details of WPR usage and configuration.



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

### SSID Limits

See [“Group Limits”](#) on page 252 for a discussion of the interaction of SSID limits and group limits. To eliminate confusion, we recommend that you configure one set of limits or the other, but not both.

- 15. Stations:** Enter the maximum number of stations allowed on this SSID. The default is 1024. This step is optional. Note that the IAPs - Global Settings window also has a station limit option—**Max Station Association per IAP**. If both station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.
- 16. Overall Traffic:** Choose **Unlimited** if you do not want to place a restriction on the traffic for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.
- 17. Traffic per Station:** Choose **Unlimited** if you do not want to place a restriction on the traffic per station for this SSID, or enter a value in the **Packets/Sec** field to force a traffic restriction.

18. **Days Active:** Choose **Everyday** if you want this SSID to be active every day of the week, or select only the specific days that you want this SSID to be active. Days that are not checked are considered to be the inactive days.
19. **Time Active:** Choose **Always** if you want this SSID active without interruption, or enter values in the **Time On** and **Time Off** fields to limit the time that this SSID is active.
20. To delete SSIDs, click their **Delete** checkboxes, then click **Apply** or **Save**.
21. Click **Apply** to apply the changes to the selected SSID, or click **Save** to apply your changes and make them permanent.

### *See Also*

DHCP Server

External Radius

Global Settings (IAP)

Internal Radius

Security Planning

SSIDs

Understanding QoS Priority on the Wi-Fi Array

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

If you enable WPR, the SSID Management window displays additional fields that must be configured. For example configurations and complete examples, please see *For an in-depth discussion, please see the [Xirrus Web Page Redirect Application Note](#) in the [Xirrus Library](#).*

If enabled, WPR displays a splash or login page when a user associates to the wireless network and opens a browser to any URL (provided the URL does not point to a resource directly on the user's machine). The user-requested URL is captured, the user's browser is redirected to the splash or login page, and then the browser is redirected either to your specified landing page, if any, or else back to the captured URL. The landing page may be specified for a user group as well. See *"Group Management" on page 250*. Note that if you change the management HTTPS port, WPR uses that port, too. See *"HTTPS" on page 220*.

SSID bobby\_test1 Web Page Redirect Configuration

Server:  Internal Login  
 Internal Splash  
 External

Landing Page URL (http):

Timeout (seconds):   Never

Redirect URL (https):

Redirect Secret:

RADIUS Authentication Type:

Apply Save

Figure 135. WPR Internal Splash Page Fields (SSID Management)

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

- Internal Splash page

This option displays a splash page instead of the first user-requested URL. The splash page files reside on the Array. Note that there is an upload function that allows you to replace the default splash page, if you wish. Please see [“Web Page Redirect” on page 306](#) for more information.

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

- Internal Login page

This option displays a login page (residing on the Array) instead of the first user-requested URL. There is an upload function that allows you to replace the default login page, if you wish. Please see [“Web Page Redirect” on page 306](#) for more information.

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

The user name and password are obtained by the login page, and authentication occurs according to your configured authentication information (starting with [Step 10](#) above). These parameters are

configured as described in “Procedure for Configuring Network Security” on page 225.

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



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

- External Login page

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

Authentication occurs according to your configured RADIUS information. These parameters are configured as described in “Procedure for Configuring Network Security” on page 225, except that the **RADIUS Authentication Type** is selected here, as described below. After authentication, the browser is redirected back to the captured URL. If you want the user redirected to a specific landing page instead, enter its address in **Landing Page URL**.

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

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

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

## Groups

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

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

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

XN8 Wi-Fi Array									
Name: S5-XN8 [ 10.100.47.106 ]		Location: S5 Area				Uptime: 0 days, 4 hours, 57 minutes			
Array	Group Name	Radius ID	Filter List	VLAN	Num	QoS	Roaming Layer	DHCP Pool	WPR
Network	Students		none		2		2-only		On
RF Monitor	Staff	StaffMembers	none		22	2	2-only		
Stations	<b>Limits</b>								
Statistics	Group Name	Enabled	Station Limit	SSID Traffic	Station Traffic	Time On	Time Off	Days On	Active
System Log	Students	Enabled	512	1000000	100000	7:00	18:00	Mon Tue Wed Thu Fri	Yes
Configuration	Staff	Enabled	512	Unlimited	Unlimited	Always	Never	All	Yes
Express Setup									
Network									
Services									
VLANs									
Security									
SSIDs									
Groups									
Group Management									

Figure 136. Groups

## Understanding Groups

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

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

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

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

### Using Groups

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

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

#### *See Also*

[External Radius](#)

[Internal Radius](#)

[SSIDs](#)

## Understanding QoS Priority on the Wi-Fi Array

## Web Page Redirect Configuration Settings

## Understanding Fast Roaming

### Group Management

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

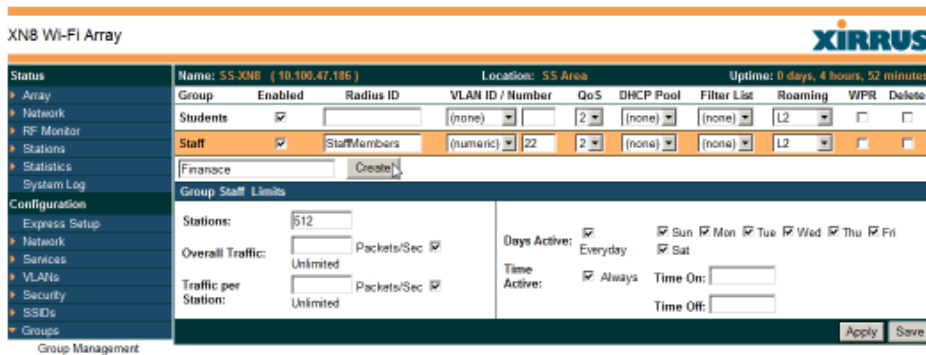


Figure 137. Group Management

### Procedure for Managing Groups

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

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

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



4. **Radius ID:** Enter a unique Radius ID for the group, to be used on an external Radius server. When adding a user account to the external server, this Radius ID value should be entered for the user. When the user is authenticated, Radius sends this value to the Array. This tells the Array that the user is a member of the group having this Radius ID.
5. **VLAN ID:** (Optional) From the pull-down list, select a VLAN for this user's traffic to use. Select **numeric** and enter the number of a previously defined VLAN (see ["VLANs" on page 204](#)). **This user group's VLAN settings supersede Dynamic VLAN settings** (which are passed to the Array by the Radius server). To avoid confusion, we recommend that you avoid specifying the VLAN for a user in two places.
6. **QoS Priority:** (Optional) Select a value in this field for QoS (Quality of Service) priority filtering. The QoS value must be one of the following:
  - 0—The lowest QoS priority setting, where QoS makes its best effort at filtering and prioritizing data, video and voice traffic without compromising the performance of the network. Use this setting in environments where traffic prioritization is not a concern.
  - 1—Medium; QoS prioritization is aggregated across all traffic types.
  - 2—High, normally used to give priority to video traffic.
  - 3—The highest QoS priority setting, normally used to give priority to voice traffic.

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

7. **Internal DHCP Pool Assigned:** (Optional) To associate an internal DHCP pool to this group, select it from the pull-down list. Only one pool may be assigned. An internal DHCP pool must be created before it can be assigned. To create a DHCP pool, go to ["DHCP Server" on page 202](#).
8. **Filter List:** (Optional) If you wish to apply a set of filters to this user group's traffic, select the desired Filter List. See ["Filters" on page 291](#).

9. **L3:** (Optional) For this group, check this box to enable fast roaming between IAPs or Arrays at Layer 2 and Layer 3. If the box is not checked, then roaming uses Layer 2 only. You may only select fast roaming at Layers 2 and 3 if this has been selected in [Global Settings \(IAP\)](#). See [“Understanding Fast Roaming”](#) on page 255.
10. **WPR (Web Page Redirect):** (Optional) Check this box if you wish to enable the Web Page Redirect functionality. This will open a **Web Page Redirect** details section in the window, where your WPR parameters may be entered. This feature may be used to display a splash screen when a user first associates to the wireless network. After that, it can (optionally) redirect the user to an alternate URL. See [“Web Page Redirect Configuration Settings”](#) on page 245 for details of WPR usage and configuration. Note that the Group Management window only allows you to set up an **Internal Splash** page and a **Landing Page URL**. The authentication options that are offered on the SSID Management page are not offered here. Since the group membership of a user is provided to the Array by a Radius server, this means the user has already been authenticated.

### Group Limits

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

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

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

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

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

### *See Also*

DHCP Server

External Radius

Internal Radius

Security Planning

SSIDs

## IAPs

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

XN8 Wi-Fi Array											
Name: jackxn8 (10.100.44.29)											Uptime: 8 days, 0 hours, 58 mins
IAP	State	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link	MAC Address / BSSID	Description
abgn1	up	1	bgn	int-dir	max	20	-90	0		00:0f:7d:0b:ac:90	
abgn2	up	monitor	abgn	int-omni	monitor	20	-95	0		00:0f:7d:0b:ac:b0	
abgn3	up	11	bgn	int-dir	max	20	-90	0		00:0f:7d:0b:ac:d0	
abgn4	up	6	bgn	int-dir	max	20	-90	0		00:0f:7d:0b:ac:f0	
an1	up	40+36	an	int-dir	small	5	-75	0		00:0f:7d:0b:ac:a0	
an2	up	56+52	an	int-dir	max	20	-90	0		00:0f:7d:0b:ac:c0	
an3	up	48+44	an	int-dir	max	20	-90	0		00:0f:7d:0b:ac:e0	
an4	up	64+60	an	int-dir	max	20	-90	0		00:0f:7d:0b:ac:80	

Figure 138. IAPs

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

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

- “Understanding Fast Roaming” on page 255

IAPs are configured using the following windows:

- “IAP Settings” on page 256
- “Global Settings (IAP)” on page 261
- “Global Settings .11a” on page 268

- [“Global Settings .11bg” on page 270](#)
- [“Global Settings .11n” on page 274](#)
- [“Advanced RF Settings” on page 277](#)
- [“LED Settings” on page 285](#)

The WMI allows you to customize many IAP settings, but there are a few settings that may only be changed using the CLI. For example, you may change the Wi-Fi mode of each IAP individually. Using the **interface iap** command, the **mode** option allows you to choose the following modes (assuming, of course, that the IAP is of the proper type): **a-only**, **an**, **b-only**, **bg**, **bgn**, **g-only**, **gn**, **n-only**.

### *See Also*

#### [IAP Statistics Summary](#)

### **Understanding Fast Roaming**

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

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

Fast Roaming is configured on two pages. To enable the fast roaming options that you want to make available on your Array, see [Step 17 to Step 19 in “Global Settings \(IAP\)” on page 261](#). To choose which of the enabled options are used by an SSID or Group, see [“Procedure for Managing SSIDs” on page 240 \(Step 13\)](#) or [“Procedure for Managing Groups” on page 250](#).

## IAP Settings

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

XN8 Wi-Fi Array										
Status		Name: SS-XNB (10.100.47.186)			Location: SS Area			Uptime: 0 days, 5 hours, 15 minutes		
IAP	Enabled	Band	Channel	Bond	Lock	Cell Size	Tx dBm	Rx dBm	Antenna Select	Description
abgn1	<input checked="" type="checkbox"/>	2.4 GHz	1	off	<input type="checkbox"/>	max	20	-90	Internal-Dir	
abgn2	<input checked="" type="checkbox"/>	monitor	mon	off	<input type="checkbox"/>	monitor	20	-95	Internal-Omni	
abgn3	<input checked="" type="checkbox"/>	2.4 GHz	11	off	<input type="checkbox"/>	max	20	-90	Internal-Dir	
abgn4	<input checked="" type="checkbox"/>	2.4 GHz	6	off	<input type="checkbox"/>	medium	12	-81	Internal-Dir	
an1	<input checked="" type="checkbox"/>	5 GHz	40	36	<input type="checkbox"/>	medium	12	-81	Internal 5GHz	
an2	<input checked="" type="checkbox"/>	5 GHz	56	52	<input type="checkbox"/>	max	20	-90	Internal 5GHz	
an3	<input checked="" type="checkbox"/>	5 GHz	48	44	<input type="checkbox"/>	max	20	-90	Internal 5GHz	
an4	<input type="checkbox"/>	5 GHz	64	60	<input type="checkbox"/>	max	20	-90	Internal 5GHz	

Figure 139. IAP Settings

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

### Procedure for Auto Configuring IAPs

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

- For all radios, go to [“Advanced RF Settings” on page 277](#).
- For all 802.11a settings, go to [“Global Settings .11a” on page 268](#).

- For all 802.11bg settings, go to “Global Settings .11bg” on page 270.
- For all 802.11n settings, go to “Global Settings .11n” on page 274.

### *Procedure for Manually Configuring IAPs*

1. In the **Enabled** column, check the box for a corresponding IAP to enable the IAP, or uncheck the box if you want to disable the IAP.
2. In the **Band** column for 802.11abg(n) radios, select the wireless band for this IAP from the choices available in the pull-down menu, either **2.4GHz** or **5 GHz**. For XN Array models, choosing the **5GHz** band will automatically select an adjacent channel for bonding when you click **Apply** or **Save**. If the mode displayed is **Auto**, the mode has been set by the auto-channel feature based on the Channel selected.

Note that IAP **abg(n)2** has an additional option—**monitor** mode. IAP **abg(n)2** should normally be set to monitor mode to enable **Spectrum Analyzer** and **Radio Assurance** (loopback testing) features.



*The XN16, XS16, and XS-3900 allow up to 12 IAPs to operate as 5 GHz — 802.11a(n) radios concurrently using internal antennas. Do not set Mode to 5 GHz for more than 12 IAPs unless you are using external antennas. Please contact Xirrus Customer Support for details. See “Contact Information” on page 422.*

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

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

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

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



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



*As mandated by FCC law, Arrays continually scan for signatures of military radar. If such a signature is detected, the Array will switch operation from conflicting channels to new ones. The Array will switch back to the original channel after 30 minutes if the channel is clear. If a radio was turned off because there were no available channels not affected by radar, the Array will now bring that radio back up after 30 minutes if that channel is clear. The 30 minute time frame complies with FCC regulations.*

4. The **Bond** column only appears for XN Array models. It works together with the channel bonding options selected on the **Global Settings .11n** page. Also see the discussion of 802.11n bonding in “Channel Bonding” on page 63.
  - **Channel number**—If a channel number appears, then this channel is already bonded to the listed channel.
  - **Off**—Do not bond this channel to another channel.
  - **On**—Bond this channel to an adjacent channel. The bonded channel is selected automatically by the Array based on the **Channel** (Step 3).



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

- **+1**—Bond this channel to the next higher channel number. Auto Channel bonding does not apply. This option is only available for some of the channels.
  - **-1**—Bond this channel to the next lower channel number. Auto Channel bonding does not apply. This option is only available for some of the channels.
5. Click the **Lock** check box if you want to lock in your channel selection so that the autochannel operation (see [Advanced RF Settings](#)) cannot change it.
  6. In the **Cell Size** column, select **Auto** to allow the optimal cell size to be automatically computed (see also, [Step 8](#) on [page 281](#)). To set the cell size yourself, choose either **Small**, **Medium**, **Large**, or **Max** to use the desired pre-configured [cell size](#), or choose **Manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx dBm** (transmit) and **Rx dBm** (receive) fields. The default is **Max**.

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

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

For additional information about cell sizes, go to “Coverage and Capacity Planning” on page 50.

7. In the **Antenna Select** column, choose the antenna you want this radio to use from the pull-down list. The list of available antennas will be different (or no choices will be available), depending on the wireless mode you selected for the IAP.
8. If desired, enter a description for this IAP in the **Description** field.
9. You may reset all of the enabled IAPs by clicking the **Reset Channels** button at the bottom of the list. A message will inform you that all enabled radios have been taken down and brought back up.



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

### *See Also*

Coverage and Capacity Planning

Global Settings (IAP)

Global Settings .11a

Global Settings .11bg

Global Settings .11n

IAPs

IAP Statistics Summary

LED Settings

**Global Settings (IAP)**

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

**XN4 Wi-Fi Array** **XIRRUS**

Name: SS-XN0429091D207 ( 10.100.47.19 ) Uptime: 1 days, 19 hours, 5 mins

<b>Status</b>	Country: United States	
Array	IAP Status: <input type="button" value="Enable All IAPs"/> <input type="button" value="Disable All IAPs"/>	
Network	Short Retry Limit (1-128):	7
RF Monitor	Long Retry Limit (1-128):	4
Stations	<b>Beacon Configuration</b>	
Statistics	Beacon Interval (20-1000):	100
System Log	DTIM Period (1-255):	1
<b>Configuration</b>	802.11h Beacon Support	<input checked="" type="radio"/> Off <input type="radio"/> On
Express Setup	<b>Station Management</b>	
Network	Station Re-Authentication Period (Seconds):	none
Services	Station Timeout Period (Seconds):	300
VLANs	Max Station Association per IAP (1-64):	64
Security	Max Phones per IAP (0-16):	16
SSIDs	Block Intra-Station Traffic:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Groups	Allow Over Air Management:	<input type="radio"/> Yes <input checked="" type="radio"/> No
IAPs	<b>Advanced Traffic Optimization</b>	
IAP Settings	Broadcast Rates:	<input type="radio"/> Optimized <input checked="" type="radio"/> Standard
Global Settings	Load Balancing:	<input type="radio"/> Off <input type="radio"/> Passive <input checked="" type="radio"/> Active
Global Settings .11a	ARP Filtering:	<input type="radio"/> Off <input checked="" type="radio"/> Pass-thru <input type="radio"/> Proxy
Global Settings .11g	Fast Roaming Mode:	<input type="radio"/> Off <input type="radio"/> Broadcast <input checked="" type="radio"/> Tunneled
Global Settings .11n	Fast Roaming Layer:	<input type="radio"/> 2 and 3 <input checked="" type="radio"/> 2 only
Advanced RF Settings	Share Roaming Info With:	<input type="radio"/> All <input checked="" type="radio"/> In Range <input type="radio"/> Target Only
LED Settings	Fast Roaming Targets:	<input type="text"/> <input type="button" value="Add"/>
WDS		<input type="text"/> <input type="button" value="Delete"/>
Filters		Name: no info Location: no info IP Address: no info
<b>Tools</b>	<input type="button" value="Apply"/> <input type="button" value="Save"/>	
System Tools		
CLI		
Logout		
<b>Log Messages</b>		

Figure 140. Global Settings (IAPs)

---

### *Procedure for Configuring Global IAP Settings*

1. **Country:** If no country is set, you may choose from the pull-down list. Once a country has been chosen, it may not be changed. You are responsible for choosing the correct country and conforming to the regulatory laws for wireless transmissions within your country. Please contact Xirrus Customer Support if you need to change the operating country after a country has already been set (see [“Contact Information” on page 422](#)).

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

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

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

### Beacon Configuration

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

### Station Management

8. **Station Re-Authentication Period:** This option allows you to specify a time (in seconds) for the duration of station reauthentications.
9. **Station Timeout Period:** Specify a time (in seconds) in this field to define the timeout period for station associations.
10. **Max Station Association per IAP:** This option allows you to define how many station associations are allowed per IAP (up to 64 stations per IAP). Note that the SSIDs —SSID Management window also has a station limit option— **Station Limit** ([page 244](#)). If both station limits are set, both will be enforced. As soon as either limit is reached, no new stations can associate until some other station has terminated its association.

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



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

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

### Advanced Traffic Optimization

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

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

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

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

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

Choose **Off** to disable load balancing.

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

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

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

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

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

17. **Fast Roaming Mode:** This feature utilizes the Xirrus Roaming Protocol (XRP) ensuring fast and seamless roaming capabilities between IAPs or Arrays at Layer 2 and Layer 3 (as specified in [Step 18](#)), while maintaining security. Fast roaming eliminates long delays for re-authentication, thus supporting time-sensitive applications such as Voice over Wi-Fi (see [“Understanding Fast Roaming” on page 255](#) for a discussion of this feature). XRP uses a discovery process to identify other Xirrus Arrays as fast roaming targets. This process has two modes:

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

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

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



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

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

### *See Also*

Coverage and Capacity Planning

Global Settings .11a

Global Settings .11bg

Global Settings .11n

Advanced RF Settings

IAPs

IAP Statistics Summary

LED Settings

IAP Settings

## Global Settings .11a

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

Status	Name: 55-XN8 (10.100.47.186)	Location: 55 Area	Uptime: 0 days, 18 hours, 4 minutes
<ul style="list-style-type: none"> <li>Array</li> <li>Network</li> <li>RF Monitor</li> <li>Stations</li> <li>Statistics</li> <li>System Log</li> <li>Configuration                             <ul style="list-style-type: none"> <li>Express Setup</li> <li>Network</li> <li>Services</li> <li>VLANs</li> <li>Security</li> <li>SSIDs</li> <li>Groups</li> <li>IAPs                                     <ul style="list-style-type: none"> <li>IAP Settings</li> <li>Global Settings</li> <li><b>Global Settings .11a</b></li> <li>Global Settings .11b</li> <li>Global Settings .11n</li> </ul> </li> </ul> </li> </ul>	802.11a Data Rates:	6.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 9.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 12.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 18.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 24.0 <input checked="" type="checkbox"/> Supported <input checked="" type="checkbox"/> Basic 36.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 48.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic 54.0 <input checked="" type="checkbox"/> Supported <input type="checkbox"/> Basic	
	Data Rate Presets:	Optimize Range	Optimize Throughput
	802.11a IAP Status:	Enable All 802.11a IAPs	Disable All 802.11a IAPs
	Channel Configuration:	Auto Configure	Factory Defaults
	Cell Size Configuration:	Auto Configure	
	Set Cell Size:	auto	
	Fragmentation Threshold (256-2346):	2346	
	RTS Threshold (1-2347):	2347	
		Apply	Save

Figure 141. Global Settings .11a

### Procedure for Configuring Global 802.11a IAP Settings

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

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

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

### *See Also*

Coverage and Capacity Planning  
Global Settings (IAP)

Global Settings .11bg

Global Settings .11n

IAPs

IAP Statistics Summary

Advanced RF Settings

IAP Settings

## Global Settings .11bg

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

The screenshot shows the 'Global Settings .11bg' configuration page for an XNB Wi-Fi Array. The page is titled 'XNB Wi-Fi Array' and features the XIRRUS logo. The left sidebar contains a navigation menu with options like Status, Array, Network, RF Monitor, Stations, Statistics, System Log, Configuration, Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, IAPs, IAP Settings, Global Settings, Global Settings .11n, Global Settings .11bg (selected), Global Settings .11n, Advanced RF Settings, LED Settings, WDS, Filters, Tools, System Tools, CLI, Logout, Log Messages, and Critical. The main content area displays the following settings:

Name: SS-XNB (10.100.47.100)		Location: SS Area		Uptime: 0 days, 18 hours, 11 minutes
802.11g Data Rates:	6.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
	9.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
	12.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
	18.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
	24.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
	36.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
	48.0	<input checked="" type="checkbox"/> Supported	<input type="checkbox"/> Basic	
802.11b Data Rates:	1.0	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Basic	
	2.0	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Basic	
	5.5	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Basic	
	11.0	<input checked="" type="checkbox"/> Supported	<input checked="" type="checkbox"/> Basic	
Data Rate Presets:	<input type="button" value="Optimize Range"/>	<input type="button" value="Optimize Throughput"/>	<input type="button" value="Restore Defaults"/>	
802.11bg IAP Status:	<input type="button" value="Enable All 802.11b/g IAPs"/>		<input type="button" value="Disable All 802.11b/g IAPs"/>	
Channel Configuration:	<input type="button" value="Auto Configure"/>		<input type="button" value="Factory Defaults"/>	
Cell Size Configuration:	<input type="button" value="Auto Configure"/>			
Set Cell Size:	auto			
802.11g Only:	<input type="radio"/> On	<input checked="" type="radio"/> Off		
802.11g Protection:	<input checked="" type="radio"/> Auto CTS	<input type="radio"/> Off		
	<input type="radio"/> Auto RTS			
802.11g Slot:	<input checked="" type="radio"/> Auto	<input type="radio"/> Short Only		
802.11b Preamble:	<input checked="" type="radio"/> Auto	<input type="radio"/> Long Only		
Fragmentation Threshold (256-2346):	<input type="text" value="2346"/>			
RTS Threshold (1-2347):	<input type="text" value="2347"/>			
				<input type="button" value="Apply"/> <input type="button" value="Save"/>

Figure 142. Global Settings .11bg

---

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

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

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

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

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

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

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

*See Also*

Coverage and Capacity Planning

Global Settings (IAP)

Global Settings .11a

Global Settings .11n

Advanced RF Settings

LED Settings

IAP Settings

IAP Statistics Summary

## Global Settings .11n

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

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

Name: SS-XN0429091D207 ( 10.100.47.19 )		Uptime: 5 days, 21 hours, 2 mins					
	Spacial Streams	Modulation & Coding	Standard Rate	Bonded Rate	Bonded short GI Rate	Supported	Basic
802.11n Data Rates:	1	MCS0	6.5	13.5	15.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS1	13.0	27.0	30.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS2	19.5	40.5	45.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS3	26.0	54.0	60.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS4	39.0	81.0	90.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS5	52.0	108.0	120.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS6	58.5	121.5	135.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	2	MCS7	65.0	135.0	150.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS8	13.0	27.0	30.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS9	26.0	54.0	60.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS10	39.0	81.0	90.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS11	52.0	108.0	120.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS12	78.0	162.0	180.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS13	104.0	216.0	240.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
		MCS14	117.0	243.0	270.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MCS15	130.0	270.0	300.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
802.11n Mode:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled						
TX Chains:	<input type="radio"/> 1 <input type="radio"/> 2 <input checked="" type="radio"/> 3						
RX Chains:	<input type="radio"/> 1 <input type="radio"/> 2 <input checked="" type="radio"/> 3						
Guard interval:	<input checked="" type="radio"/> Short <input type="radio"/> Long						
Auto bond 5 GHz channels:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled						
5 GHz channel bonding:	<input checked="" type="radio"/> Dynamic <input type="radio"/> Static						
2.4 GHz channel bonding:	<input type="radio"/> Dynamic <input checked="" type="radio"/> Static						
Global channel bonding:	<input type="button" value="Enable bonding on all IAPs"/> <input type="button" value="Disable bonding on all IAPs"/>						

Figure 143. Global Settings .11n



---

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

1. **802.11n Data Rates:** The Array allows you to define which data rates are supported for all 802.11n radios. Select (or deselect) 11n data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.
  - **Basic Rate**—a wireless station (client) must support this rate in order to associate.
  - **Supported Rate**—data rates that can be used to transmit to clients.
2. **802.11n Mode:** Select **Enabled** to operate in 802.11n mode, with four 802.11b/g/n mode ports and the remaining IAPs operating in 802.11a/n mode. Use of this mode is controlled by the Array's license key. The key must include 802.11n capability, or you will not be able to enable this mode. See [“License” on page 136](#) to view the features supported by your license key. Contact Xirrus Customer support for questions about your license.

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

3. **TX Chains:** Select the number of separate data streams transmitted by the antennas of each IAP. The default is 3. See [“Multiple Data Streams—Spatial Multiplexing” on page 62](#).
4. **RX Chains:** Select the number of separate data streams received by the antennas of each IAP. This number should be greater than or equal to **TX Chains**. The default is 3. See [“Multiple Data Streams—Spatial Multiplexing” on page 62](#).
5. **Guard interval:** Select **Short** to increase the data transmission rate by decreasing wait intervals in signal transmission. Select **Long** to use the standard interval. The default is Short. See [“Short Guard Interval” on page 64](#).

6. **Auto bond 5 GHz channels:** Select **Enabled** to use Channel Bonding on 5 GHz channels and automatically select the best channels for bonding. The default is **Enabled**. See “[Channel Bonding](#)” on page 63.
7. **5 GHz channel bonding:** Select **Dynamic** to have auto-configuration for bonded 5 GHz channels be automatically updated as conditions change. For example, if there are too many clients to be supported by a bonded channel, dynamic mode will automatically break the bonded channel into two channels. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**. See “[Channel Bonding](#)” on page 63.
8. **2.4 GHz channel bonding:** Select **Dynamic** to have auto-configuration for bonded 2.4 GHz channels be automatically updated as conditions change. Select **Static** to have the bonded channels remain the same once they are selected. The Dynamic option is only available when **Auto bond 5 GHz channels** is enabled. The default is **Dynamic**. See “[Channel Bonding](#)” on page 63.
9. **Global channel bonding:** These buttons allow you to turn channel bonding on or off for all IAPs in one step. The effect of using one of these buttons will be shown if you go to the **IAP Settings** window and look at the **Bond** column. Clicking **Enable bonding on all IAPs** causes all IAPs to be bonded to their auto-bonding channel immediately, if appropriate. For example, IAP abgn2 will not be bonded if it is set to monitor mode, and 2.4 GHz radios will not be bonded. Click **Disable bonding on all IAPs** to turn off bonding on all IAPs immediately. See “[Channel Bonding](#)” on page 63. Settings in [Step 7](#) and [Step 8](#) are independent of global channel bonding.

## Advanced RF Settings

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

Name: SS-X108 ( 10.100.47.106 )		Location: SS Area		Uptime: 0 days, 18 hours, 35 minutes																																																																																																																																																																	
<b>RF Intrusion Detection</b>																																																																																																																																																																					
Intrusion Detection Mode:	<input type="radio"/> Off	<input checked="" type="radio"/> Standard	<input type="radio"/> Advanced																																																																																																																																																																		
Auto Block Unknown Rogue APs:	<input type="radio"/> Off	<input checked="" type="radio"/> On																																																																																																																																																																			
Auto Block RSSI:	<input type="text" value="-50"/>																																																																																																																																																																				
Auto Block Level:	Automatically block unknown rogue APs with no encryption																																																																																																																																																																				
<b>RF Resilience</b>																																																																																																																																																																					
Radio Assurance Mode:	Disabled																																																																																																																																																																				
Enable Standby Mode:	<input type="radio"/> Yes	<input checked="" type="radio"/> No																																																																																																																																																																			
Standby Target Address:	<input type="text"/>																																																																																																																																																																				
<b>RF Power &amp; Sensitivity</b>																																																																																																																																																																					
Cell Size Configuration:	Auto Configure																																																																																																																																																																				
Auto Cell Size Period (seconds):	<input type="text"/>	<input checked="" type="checkbox"/> None																																																																																																																																																																			
Auto Cell Size Overlap (%):	<input type="text" value="0"/>																																																																																																																																																																				
Auto Cell Min Tx Power (dBm):	<input type="text" value="10"/>	<input type="checkbox"/> Default																																																																																																																																																																			
Sharp Cell:	<input checked="" type="radio"/> Off	<input type="radio"/> On																																																																																																																																																																			
<b>RF Spectrum Management</b>																																																																																																																																																																					
Channel Configuration:	Factory Defaults	Auto Configure	Auto Negotiate & Configure																																																																																																																																																																		
Channel Configuration Status:	Idle																																																																																																																																																																				
Auto Channel Configuration Mode:	<input type="radio"/> On Array PowerUp	<input checked="" type="radio"/> Disabled																																																																																																																																																																			
Auto Channel Configure on Time (h:mm):	<input type="text"/>																																																																																																																																																																				
Channel List Selection:	<input checked="" type="checkbox"/> 1	<input type="checkbox"/> 2	<input type="checkbox"/> 3	<input type="checkbox"/> 4	<input type="checkbox"/> 5	<input checked="" type="checkbox"/> 6	<input type="checkbox"/> 7	<input type="checkbox"/> 8	<input type="checkbox"/> 9	<input type="checkbox"/> 10	<input checked="" type="checkbox"/> 11	<input type="checkbox"/> 12	<input type="checkbox"/> 13	<input type="checkbox"/> 14	<input type="checkbox"/> 15	<input checked="" type="checkbox"/> 16	<input type="checkbox"/> 17	<input type="checkbox"/> 18	<input type="checkbox"/> 19	<input type="checkbox"/> 20	<input type="checkbox"/> 21	<input type="checkbox"/> 22	<input type="checkbox"/> 23	<input type="checkbox"/> 24	<input type="checkbox"/> 25	<input type="checkbox"/> 26	<input type="checkbox"/> 27	<input type="checkbox"/> 28	<input type="checkbox"/> 29	<input type="checkbox"/> 30	<input type="checkbox"/> 31	<input type="checkbox"/> 32	<input type="checkbox"/> 33	<input type="checkbox"/> 34	<input type="checkbox"/> 35	<input type="checkbox"/> 36	<input checked="" type="checkbox"/> 37	<input checked="" type="checkbox"/> 38	<input checked="" type="checkbox"/> 39	<input checked="" type="checkbox"/> 40	<input checked="" type="checkbox"/> 41	<input checked="" type="checkbox"/> 42	<input checked="" type="checkbox"/> 43	<input checked="" type="checkbox"/> 44	<input checked="" type="checkbox"/> 45	<input checked="" type="checkbox"/> 46	<input checked="" type="checkbox"/> 47	<input checked="" type="checkbox"/> 48	<input checked="" type="checkbox"/> 49	<input checked="" type="checkbox"/> 50	<input checked="" type="checkbox"/> 51	<input checked="" type="checkbox"/> 52	<input checked="" type="checkbox"/> 53	<input checked="" type="checkbox"/> 54	<input checked="" type="checkbox"/> 55	<input checked="" type="checkbox"/> 56	<input checked="" type="checkbox"/> 57	<input checked="" type="checkbox"/> 58	<input checked="" type="checkbox"/> 59	<input checked="" type="checkbox"/> 60	<input type="checkbox"/> 61	<input type="checkbox"/> 62	<input type="checkbox"/> 63	<input type="checkbox"/> 64	<input type="checkbox"/> 65	<input type="checkbox"/> 66	<input type="checkbox"/> 67	<input type="checkbox"/> 68	<input type="checkbox"/> 69	<input type="checkbox"/> 70	<input type="checkbox"/> 71	<input type="checkbox"/> 72	<input type="checkbox"/> 73	<input type="checkbox"/> 74	<input type="checkbox"/> 75	<input type="checkbox"/> 76	<input type="checkbox"/> 77	<input type="checkbox"/> 78	<input type="checkbox"/> 79	<input type="checkbox"/> 80	<input type="checkbox"/> 81	<input type="checkbox"/> 82	<input type="checkbox"/> 83	<input type="checkbox"/> 84	<input type="checkbox"/> 85	<input type="checkbox"/> 86	<input type="checkbox"/> 87	<input type="checkbox"/> 88	<input type="checkbox"/> 89	<input type="checkbox"/> 90	<input type="checkbox"/> 91	<input type="checkbox"/> 92	<input type="checkbox"/> 93	<input type="checkbox"/> 94	<input type="checkbox"/> 95	<input type="checkbox"/> 96	<input type="checkbox"/> 97	<input type="checkbox"/> 98	<input type="checkbox"/> 99	<input type="checkbox"/> 100	<input type="checkbox"/> 101	<input type="checkbox"/> 102	<input type="checkbox"/> 103	<input type="checkbox"/> 104	<input type="checkbox"/> 105	<input type="checkbox"/> 106	<input type="checkbox"/> 107	<input type="checkbox"/> 108	<input type="checkbox"/> 109	<input type="checkbox"/> 110	<input type="checkbox"/> 111	<input type="checkbox"/> 112	<input type="checkbox"/> 113	<input type="checkbox"/> 114	<input type="checkbox"/> 115	<input type="checkbox"/> 116	<input type="checkbox"/> 117	<input type="checkbox"/> 118	<input type="checkbox"/> 119	<input type="checkbox"/> 120	<input type="checkbox"/> 121	<input type="checkbox"/> 122	<input type="checkbox"/> 123	<input type="checkbox"/> 124	<input type="checkbox"/> 125	<input type="checkbox"/> 126	<input type="checkbox"/> 127	<input type="checkbox"/> 128	<input type="checkbox"/> 129	<input type="checkbox"/> 130	<input type="checkbox"/> 131	<input type="checkbox"/> 132	<input type="checkbox"/> 133	<input type="checkbox"/> 134	<input type="checkbox"/> 135	<input type="checkbox"/> 136	<input type="checkbox"/> 137	<input type="checkbox"/> 138	<input type="checkbox"/> 139	<input type="checkbox"/> 140	<input type="checkbox"/> 141	<input type="checkbox"/> 142	<input type="checkbox"/> 143	<input type="checkbox"/> 144	<input type="checkbox"/> 145	<input type="checkbox"/> 146	<input type="checkbox"/> 147	<input type="checkbox"/> 148	<input type="checkbox"/> 149	<input type="checkbox"/> 150	<input type="checkbox"/> 151	<input type="checkbox"/> 152	<input type="checkbox"/> 153	<input type="checkbox"/> 154	<input type="checkbox"/> 155	<input type="checkbox"/> 156	<input type="checkbox"/> 157	<input type="checkbox"/> 158	<input type="checkbox"/> 159	<input type="checkbox"/> 160	<input type="checkbox"/> 161	<input type="checkbox"/> 162	<input type="checkbox"/> 163	<input type="checkbox"/> 164	<input type="checkbox"/> 165
Auto Channel List:	Use Defaults		Use All Channels																																																																																																																																																																		
Public Safety:	<input checked="" type="radio"/> Off	<input type="radio"/> On																																																																																																																																																																			
Apply Save																																																																																																																																																																					

Figure 144. Advanced RF Settings

## About Standby Mode

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

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

### About Blocking Rogue APs

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

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

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

---

## *Procedure for Configuring Advanced RF Settings*

### **RF Intrusion Detection**

- 1. Intrusion Detection Mode:** This option allows you to choose the **Standard** intrusion detection method, or you can choose **Off** to disable this feature. See “[Array Monitor and Radio Assurance Capabilities](#)” on [page 412](#) for more information.
  - **Standard**—enables the abg(n)2 radio as a monitor which collects Rogue AP information.
  - **Off**—IAP abg(n)2 does not function as a monitor.
- 2. Auto Block Unknown Rogue APs:** Enable or disable auto blocking (see “[About Blocking Rogue APs](#)” on [page 278](#)). Note that in order to set **Auto Block RSSI** and **Auto Block Level**, you must set Auto Block Unknown Rogue APs to **On**, and click **Apply**. Then the remaining Auto Block fields will be active.
- 3. Auto Block RSSI:** Set the minimum RSSI for rogue APs to be blocked. APs with lower RSSI values will not be blocked. They are assumed to be farther away, and probably belonging to neighbors and posing a minimal threat.
- 4. Auto Block Level:** Select rogue APs to block based on the level of encryption that they are using. The choices are:
  - Automatically block unknown rogue APs regardless of encryption.
  - Automatically block unknown rogue APs with no encryption.
  - Automatically block unknown rogue APs with WEP or no encryption.

### **RF Resilience**

- 5. Radio Assurance Mode:** When this mode is enabled, IAP abg(n)2 performs loopback tests on the Array. This mode requires Intrusion Detection to be set to **Standard** ([Step 1](#)) to enable abg(n)2’s self-monitoring functions. It also requires abg(n)2 to be set to monitoring mode (see “[Enabling Monitoring on the Array](#)” on [page 412](#)).

Operation of Radio Assurance mode is described in detail in “[Array Monitor and Radio Assurance Capabilities](#)” on page 412.

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

- **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
  - **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of one or all of the radios if needed.
  - **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets, and schedule reboots if needed.
  - **Disabled**—Disable IAP radio assurance tests (no self-monitoring occurs). Loopback tests are disabled by default.
6. **Enable Standby Mode:** Choose **Yes** to enable this Array to function as a backup unit for the target Array, or choose **No** to disable this feature. See “[About Standby Mode](#)” on page 277.
  7. **Standby Target Address:** If you enabled the Standby Mode, enter the MAC address of the target Array (i.e., the address of the primary Array that is being monitored and backed up by this Array). To find this MAC address, open the Array Info window on the target Array, and use the Gigabit1 MAC Address.

### RF Power & Sensitivity

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



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

*The abg(n)2 radio must be in **monitor** mode, and all other IAPs that will use Auto Cell must have **Cell Size** set to **auto**. See “[Procedure for Manually Configuring IAPs](#)” on page 257.*

8. **Cell Size Configuration:** Click on the **Auto Configure** button to instruct the Array to determine and set the best cell size for each enabled IAP, based on changes in the environment. This is the recommended method for setting cell size. On the IAP settings window, each enabled IAP will have its cell size set to **Auto**.
9. **Auto Cell Size Period:** You may set up auto-configuration to run periodically, readjusting optimal cell sizes for the current conditions. Enter a number of seconds to specify how often auto-configuration will run. If you select **None**, then auto-configuration of cell sizing will not be run periodically. You do not need to run Auto Cell often unless there are a lot of changes in the environment. If the RF environment is changing often, running Auto Cell every twenty-four hours (86400 seconds) should be sufficient).
10. **Auto Cell Size Overlap (%):** Enter the percentage of cell overlap that will be allowed when the Array is determining automatic cell sizes. For 100% overlap, the power is adjusted such that neighboring Arrays that hear each other best will hear each other at -70dB. For 0% overlap, that number is -90dB.
11. **Auto Cell Min Tx Power (dBm):** Enter the minimum transmit power that the Array can assign to a radio when adjusting automatic cell sizes.
12. **Sharp Cell:** This feature reduces interference between neighboring Arrays or other Access Points by limiting to a defined boundary (cell size) the trailing edge bleed of RF energy. Choose **On** to enable the Sharp Cell functionality, or choose **Off** to disable this feature. See also, “[Fine Tuning Cell Sizes](#)” on page 53.

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

## RF Spectrum Management

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

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

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

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

Factory Preset Channels (US) for both XN and XS models				
IAP	16-Radio Models	12-Radio Models	8-Radio Models	4-Radio Models
abg(n)1	1	1	1	1
abg(n)2	mon	mon	mon	mon



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

14. **Channel Configuration Status:** Shows the status of auto channel configuration. If an operation is in progress, the approximate time remaining until completion is displayed; otherwise **Idle** is displayed.
15. **Auto Channel Configuration Mode:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP when the Array is powered up. Choose **On Array PowerUp** to enable this feature, or choose **Disabled** to disable this feature.

16. **Auto Channel Configure on Time:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here (in hours and minutes, using the format: hh:mm). Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated.
17. **Channel List Selection:** This list selects which channels are available to the auto channel algorithm. Channels that are not checked are left out of the auto channel selection process. Note that channels that have been locked by the user are also not available to the auto channel algorithm.
18. **Auto Channel List: Use All Channels** selects all available channels (this does not include locked channels). **Use Defaults** sets the auto channel list back to the defaults. This omits newer channels (100-140)—many wireless NICs don't support these channels.



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

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

### *See Also*

Coverage and Capacity Planning

Global Settings .11a

Global Settings .11bg

Global Settings .11n

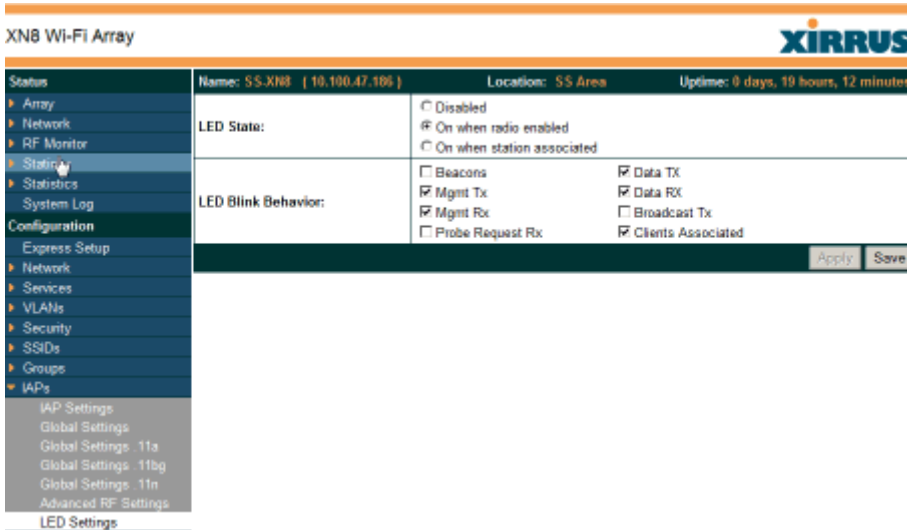
IAPs

IAP Statistics Summary

## IAP Settings

## LED Settings

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



XN8 Wi-Fi Array		XIRRUS	
Status	Name: SS.XN8 (10.100.47.108)	Location: SS Area	Uptime: 0 days, 10 hours, 12 minutes
<ul style="list-style-type: none"> <li>▶ Array</li> <li>▶ Network</li> <li>▶ RF Monitor</li> <li>▶ Status</li> <li>▶ Statistics</li> <li>▶ System Log</li> <li>Configuration               <ul style="list-style-type: none"> <li>▶ Express Setup</li> <li>▶ Network</li> <li>▶ Services</li> <li>▶ VLANs</li> <li>▶ Security</li> <li>▶ SSIDs</li> <li>▶ Groups</li> <li>▶ IAPs                   <ul style="list-style-type: none"> <li>IAP Settings</li> <li>Global Settings</li> <li>Global Settings: 11a</li> <li>Global Settings: 11bg</li> <li>Global Settings: 11n</li> <li>Advanced RF Settings</li> <li>LED Settings</li> </ul> </li> </ul> </li> </ul>	LED State:	<input type="checkbox"/> Disabled <input checked="" type="checkbox"/> On when radio enabled <input type="checkbox"/> On when station associated	
	LED Blink Behavior:	<input type="checkbox"/> Beacons <input checked="" type="checkbox"/> Mgmt Tx <input checked="" type="checkbox"/> Mgmt Rx <input type="checkbox"/> Probe Request Rx	<input checked="" type="checkbox"/> Data TX <input checked="" type="checkbox"/> Data RX <input type="checkbox"/> Broadcast Tx <input checked="" type="checkbox"/> Clients Associated
		<input type="button" value="Apply"/> <input type="button" value="Save"/>	

Figure 145. LED Settings

### Procedure for Configuring the IAP LEDs

1. **LED State:** This option determines which event triggers the LEDs, either when an IAP is enabled or when an IAP first associates with the network. Choose **On Radio Enabled** or **On First Association**, as desired. You may also choose **Disabled** to keep the LEDs from being lit. The LEDs will still light during the boot sequence, then turn off.
2. **LED Blink Behavior:** This option allows you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink. See also, “Array LED Operating Sequences” on page 108.
3. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

*See Also*

Global Settings (IAP)

Global Settings .11a

Global Settings .11bg

IAPs

LED Boot Sequence

## WDS

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

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

Figure 146. WDS

### About Configuring WDS Links

A WDS link connects a client Array and a host Array (see Figure 147 on page 288). The host must be the Array that has a wired connection to the LAN. Client links from one or more Arrays may be connected to the host, and the host may also have client links. See “WDS Planning” on page 76 for more illustrations.

The configuration for WDS is performed on the client Array only, as described in “WDS Client Links” on page 289. No WDS configuration is performed on the host Array. First you will set up a client link, defining the target (host) Array and SSID, and the maximum number of IAPs in the link. Then you will select the IAPs to be used in the link. When the client link is created, each member IAP will associate to an IAP on the host Array.

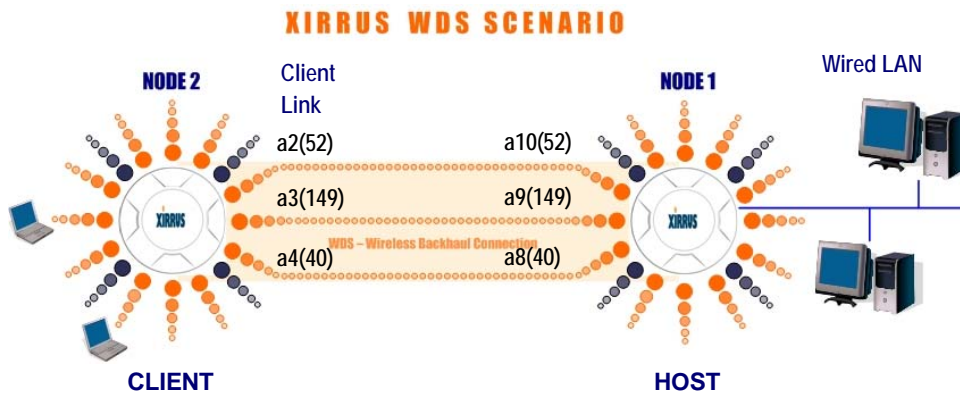





Figure 147. .Configuring a WDS Link

- 

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

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

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

### See Also

SSID Management

WDS Client Link IAP Assignments:

WDS Client Links

WDS Statistics

WDS Client Links

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

**WDS Client Link Settings** hours, 44 mins

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

WDS Link	IAP/ Channel							
	abgn1 11	abgn2 monitor	abgn3 40+36	abgn4 165	an1 112+108	an2 140	an3 100+104	an4 56+52
Client Link 1	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Client Link 2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Client Link 3	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Client Link 4	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
None	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

IAP Channel Assignment:

WDS Host Link Settings

Allow Concurrent Stations:  Yes  No

Figure 148. WDS Client Links

*Procedure for Setting Up WDS Client Links*

**WDS Client Link Settings:**

- Client Link:** Shows the ID (1 to 4) of each of the four possible WDS links.
- Enabled:** Check this box if you want to enable this WDS link, or uncheck the box to disable the link.
- Max IAPs Allowed (1-3):** Enter the maximum number of IAPs for this link, between 1 and 3.

4. **Target Array Base MAC Address:** Enter the base MAC address of the target Array (the host Array at the other side of this link). To find this MAC address, open the **WDS** window on the *target* Array, and use **This Array Address** located on the right under the Summary of WDS Host Links.
5. **Target SSID:** Enter the SSID that the target Array is using.
6. **Username:** Enter a username for this WDS link. A username and password is required if the SSID is using PEAP for WDS authentication from the internal RADIUS server.
7. **Password:** Enter a password for this WDS link.
8. **Clear Settings:** Click on the **Clear** button to reset all of the fields on this line.
9. Click on the **Apply** button to apply your changes to this session, or click **Save** to apply your changes and make them permanent.

#### WDS Client Link IAP Assignments:

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



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

11. **IAP Channel Assignment:** Click **Auto Configure** to instruct the Array to automatically determine the best channel allocation settings for each IAP that participates in a WDS link, based on changes in the environment. These changes are executed immediately, and are automatically applied.
12. **Allow Concurrent Stations:** Click **Yes** to instruct the Array to allow stations to associate to IAPs on a host Array that participate in a WDS link. The WDS host IAP will send beacons announcing its availability to wireless clients.
13. **Reset All Links:** this command tears down all links configured on the Array and sets them back to their factory defaults, effective immediately.



*See Also*[SSID Management](#)[WDS Planning](#)[WDS](#)[WDS Statistics](#)

## Filters

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

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

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

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

it is filtering, which port it applies to, source and destination addresses, and QoS and VLAN assignments.

The screenshot shows the configuration page for an XN8 Wi-Fi Array. The page title is 'XN8 Wi-Fi Array' and the XIRRUS logo is in the top right. The main content area displays a table of filters. The table has columns for Name, Type, Protocol, Port, Source, Destination, Set QoS, Set VLAN, and Enabled. The filters are organized into sections: Global and Filters-A. An orange arrow points to the 'Filters-A' section header.

XN8 Wi-Fi Array									
Status		Name: SS-XN8 (10.100.47.186)			Location: SS Area		Uptime: 0 days, 22 hours, 5 minutes		
Name	Type	Protocol	Port	Source	Destination	Set QoS	Set VLAN	Enabled	
Global									
new	allow	any	any	any	any			Yes	
no-telnet	allow	any	any	any	any			Yes	
Filters-A									
-111	deny	any	any	111.111.111.0/24	any			Yes	
no-telnet	allow	any	any	any	any			Yes	

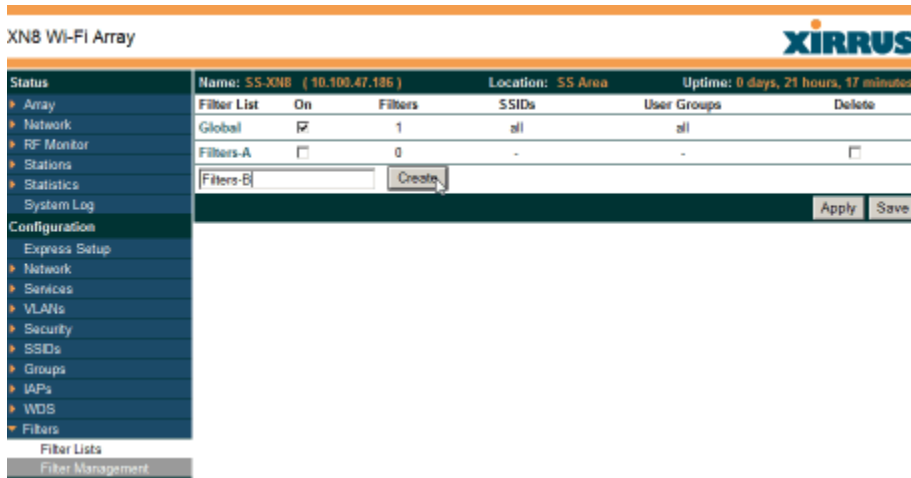
Configuration menu items: Express Setup, Network, Services, VLANs, Security, SSIDs, Groups, IAPs, WDS, Filters (Filter Lists, Filter Management).

Orange arrow expands/collapses display

Figure 149. Filters

## Filter Lists

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



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

Name: SS-XN8 ( 10.100.47.186 )      Location: SS Area      Uptime: 0 days, 21 hours, 17 minutes

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

**Filter Lists**  
Filter Management

Figure 150. Filter Lists

### Procedure for Managing Filter Lists

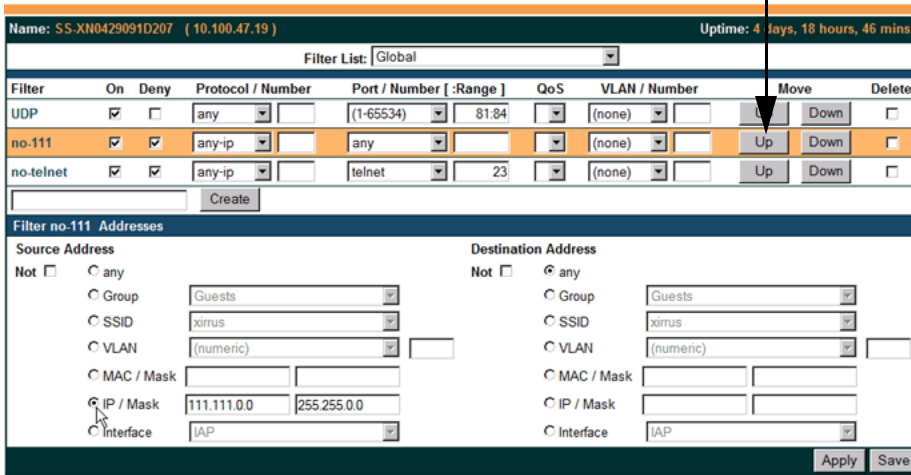
1. **Stateful Filtering:** Stateful operation of the integrated firewall can be **Enabled** or **Disabled**. If you have a large number of filters and you don't want to apply them in a stateful manner, you may use this option to turn the firewall off.
2. **New Filter List Name:** Enter a name for the new filter list in this field, then click on the Create button to create the list. All new filters are disabled when they are created. The new filter list is added to the Filter List table in the window. Click on the filter list name, and you will be taken to the **Filter Management** window for that filter list.

3. **On:** Check this box to enable this filter list, or leave it blank to disable the list. If the list is disabled, you may still add filters to it or modify it, but none of the filters will be applied to data traffic.
4. **Filters:** This read-only field displays the number of filters that belong to this filter list.
5. **SSIDs:** This read-only field lists the [SSIDs](#) that use this filter list.
6. **User Groups:** This read-only field lists the [Groups](#) that use this filter list.
7. **Delete:** Click this checkbox and then click the **Apply** or **Save** button to delete this filter list.
8. Click on the **Apply** button to apply your changes to the selected filter, or click **Save** to apply your changes and make them permanent.
9. Click a filter list to go to the [Filter Management](#) window to create and manage the filters that belong to this list.

## Filter Management

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

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



Filter	On	Deny	Protocol / Number	Port / Number [ :Range ]	QoS	VLAN / Number	Move	Delete
UDP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	any	(1-65534)	81.84	(none)	Up Down	<input type="checkbox"/>
no-111	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any-ip	any		(none)	Up Down	<input type="checkbox"/>
no-telnet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	any-ip	telnet	23	(none)	Up Down	<input type="checkbox"/>

Filter no-111 Addresses

Source Address

Not  any

Group: Guests

SSID: xirus

VLAN: (numeric)

MAC / Mask: /

IP / Mask: 111.111.0.0 / 255.255.0.0

Interface: IAP

Destination Address

Not  any

Group: Guests

SSID: xirus

VLAN: (numeric)

MAC / Mask: /

IP / Mask: /

Interface: IAP

Apply Save

Figure 151. Filter Management

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

### Procedure for Managing Filters

1. **Filter List:** Select the filter list to display and manage on this window. All of the filters already defined for this list are shown, and you may create additional filters for this list.
2. **New Filter Name:** Enter a name for the new filter in the field next to the **Create** button, then click on the **Create** button to create the filter. All new filters are added to the table of filters at the top of the window. The filter name must be unique within the list, but it may have the same name as a

filter in a different filter list. Two filters with the same name in different filter lists will be completely unrelated to each other—they may be defined with different parameter values.

- Filter:** Choose a filter entry to modify from the list at the top of the window.
- On:** Use this field to enable or disable this filter.
- Deny:** Choose whether this filter will be an **Allow** filter or a **Deny** filter. If you define the filter as an Allow filter, then any associations that meet the filter criteria will be allowed. If you define the filter as a Deny filter, any associations that meet the filter criteria will be denied.
- Protocol:** Choose a specific filter protocol from the pull-down list, or choose **numeric** and enter a **Number**, or choose **any** to instruct the Array to use the best filter. This is a match criterion.
- Port:** This is a match criterion. From the pull-down list, choose the target port type for this filter. Choose **any** to instruct the Array to apply the filter to any port, or choose **1-65534** and enter a **Number**.

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

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

- QoS:** (Optional) Set packets that match the filter criteria to this QoS level (0 to 3), selected from the pull-down list. Level 0 has the lowest priority; level 3 has the highest priority. By default, this field is blank and the filter does not modify QoS level. See “Understanding QoS Priority on the Wi-Fi Array” on page 237.
- VLAN ID:** (Optional) Set packets that match the filter criteria to this VLAN. Select a VLAN from the pull-down list, or select **numeric** and enter the number of a previously defined VLAN (see “VLANs” on page 204).
- Move Up/Down:** The filters are applied in the order in which they are displayed in the list, with filters on the top applied first. To change an entry’s position in the list, just click its **Up** or **Down** button.

11. **Source Address:** Define a source address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.
12. **Destination Address:** Define a destination address to match as a filter criterion. Click the radio button for the desired type of address (or other attribute) to match. Then specify the value to match in the field to the right of the button. Choose **Any** to use any source address. Check **Not** to match any address except for the specified address.
13. To delete a filter, check its **Delete** checkbox, then click the **Apply** or **Save** button.
14. Click on the **Apply** button to apply your changes to the selected filter, or click **Save** to apply your changes and make them permanent.

*See Also*

[Filters](#)

[Filter Statistics](#)

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

[VLANs](#)





---

# Using Tools on the Wi-Fi Array

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

- **[“System Tools” on page 300](#)**
- **[“CLI” on page 310](#)**
- **[“Logout” on page 312](#)**

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

- **[“Viewing Status on the Wi-Fi Array” on page 127](#)**
- **[“Configuring the Wi-Fi Array” on page 173](#)**

## System Tools

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

XN8 Wi-Fi Array

Status	Name: Bruce.XN8-Array ( 10.100.47.10 )    Location: Office    Uptime: 5 days, 23 hours, 38 mins
▶ Array	System <span style="float: right;">Current Version: 4.0.6 (Oct 14 2009), Build: 1169</span>
▶ Network	Reboot: <input type="button" value="Save &amp; Reboot"/> <input type="button" value="Reboot"/>
▶ RF Monitor	Software Upgrade: <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upgrade"/>
▶ Stations	License Key: <input type="text" value="0FA20-5KPJC-J6NUC-MFNWB"/> <input type="button" value="Upgrade"/>
▶ Statistics	Remote TFTP Server: <input type="text"/>
System Log	Remote Boot Image: <input type="text"/>
Configuration	
Express Setup	Remote Configuration: <input type="text"/>
▶ Network	Configuration
▶ Services	Update From Remote File: <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Update"/>
▶ VLANs	Update From Local File: <input type="text"/> <input type="button" value="Update"/>
▶ Security	Download Current Configuration: <input type="text" value="xs_current.conf"/>
▶ SSIDs	Reset to Factory Defaults: <input type="button" value="Reset"/> <input type="button" value="Reset/Preserve IP Settings"/>
▶ Groups	Diagnostics
▶ IAPs	Dagnostic Log: <input type="text" value="xs_diagnostic.log"/> <input type="button" value="Create"/>
▶ WDS	Web Page Redirect
▶ Filters	Upload File: <input type="text"/> <input type="button" value="Browse..."/> <input type="button" value="Upload"/>
Tools	Remove File: <input type="text"/> <input type="button" value="Delete"/> <input type="button" value="List Files"/>
System Tools	Download Sample Files: <input type="text" value="wpr.pl"/> <input type="text" value="hs.css"/>
CLI	Network Tools
Logout	System Command: <input type="radio"/> Trace Route <input checked="" type="radio"/> Ping <input type="radio"/> RADIUS Ping
Log Messages	Hostname / IP Address: <input type="text" value="10.100.47.186"/>
Critical 1	Timeout: <input type="text" value="10"/>
Warning 5	Execute System Command: <input type="button" value="Execute"/>
Information 118	Progress
	Status
	Please wait while executing command.
	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>←</p> <p><b>Status is shown here</b></p> </div> <div style="text-align: center;"> <p>←</p> <p><b>Progress is shown here</b></p> </div> </div>
	<input type="button" value="Save"/>

Figure 152. System Tools

## *Procedure for Configuring System Tools*

These tools are broken down into the following sections:

- System
- Configuration
- Diagnostics
- Web Page Redirect
- Tools
- Progress and Status Frames

### System

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

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



*If you have difficulty upgrading the Array using the WMI, see “[Upgrading the Array via CLI](#)” on [page 415](#) for a lower-level procedure you may use.*

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

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

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

### Automatic Updates from Remote Image or Configuration File

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

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

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



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

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

A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your Arrays but don't want to have the same IP address for each Array, you may remove the **ipaddr** line from the file. You can then load the file on each Array and the local IP addresses will not change.

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

## Configuration

- 7. Update from Remote File:** This field allows you to define the path to a configuration file (one that you previously saved—see [Step 9](#) below). Click on the **Browse** button if you need to browse for the location of the file, then click **Update** to update your configuration settings.
- 8. Update from Local File:** This field updates Array settings from a local configuration file on the Array. Select one of the following files from the drop-down list:
  - **factory.conf:** The factory default settings
  - **lastboot.conf:** The setting values from just before the last reboot
  - **saved.conf:** The last settings that were explicitly savedClick **Update** to update your configuration settings.

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



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

- 10. Reset to Factory Defaults:** Click on the **Reset/Preserve IP Settings** button to reset the system's current configuration settings to the factory default values, *except for the Array's management IP address which is left unchanged.* This function allows you to maintain management connectivity to the Array even after the reset. This will retain the Gigabit Ethernet port's IP address (see "[Network Interfaces](#)" on page 181), or if you have configured management over a VLAN it will maintain the management VLAN's IP address (see "[VLAN Management](#)" on page 206). *All other previous configuration settings will be lost.*

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



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

## Diagnostics

- 11. Diagnostic Log:** Click the **Create** button to save a snapshot of Array information for use by Xirrus Customer Support personnel. The [Progress](#) and [Status Frames](#) show the progress of this operation. When the process

is complete, the filename `xs_diagnostic.log` will be displayed in blue and provides a link to the newly created log file. Click the link to download this file to the `C:\` folder on your local computer. (Figure 153)

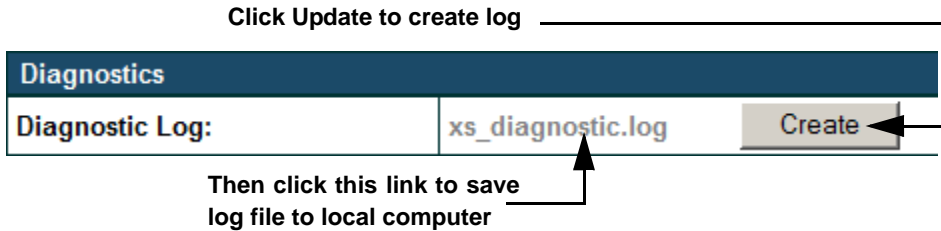


Figure 153. Saving the Diagnostic Log

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

The diagnostic log is always saved as a file named `xs_diagnostic.log` on your `C:\` drive, so you should immediately rename the file to save it. This way, it will not be lost the next time you save a diagnostic log. Often, Customer Support will instruct you to save two diagnostic logs about ten minutes apart so that they can examine the difference in statistics between the two snapshots (for example, to see traffic and error statistics for the interval). Thus, you must rename the first diagnostic log file.



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

## Web Page Redirect

The Array uses a Perl script and a cascading style sheet to define the default splash/login Web page that the Array delivers for WPR. You may replace these files with files for one or more custom pages of your own. See [Step 14](#) below to view the default files. See [Step 14 on page 244](#) for more information about WPR and how the splash/login page is used.

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

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

Figure 154. Managing WPR Splash/Login page files

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

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



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

Tools

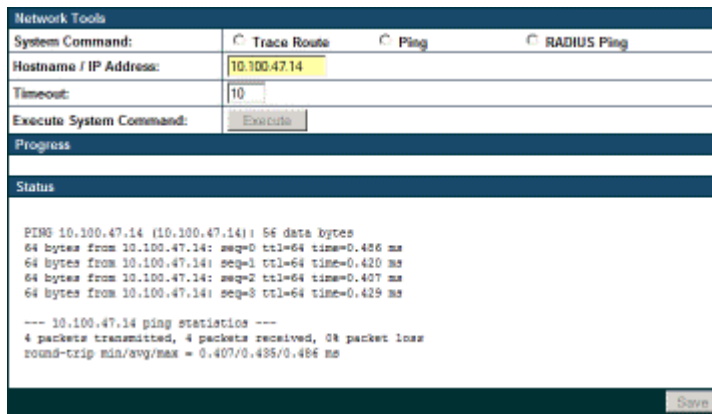


Figure 155. System Command (Ping)

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

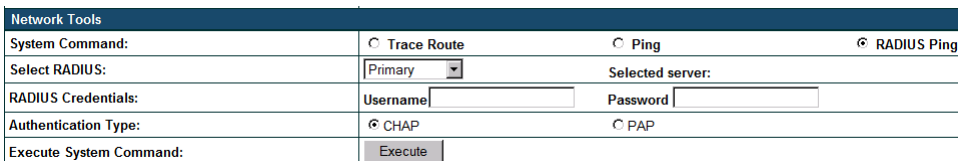


Figure 156. Radius Ping Command

The RADIUS Ping command is a simple utility that tests connectivity to a RADIUS server by attempting to log in with the specified Username and Password. When using a RADIUS server, this command allows you to verify that the server configuration is correct and whether a particular Username and Password are set up properly. If a client is having trouble accessing the network, you can quickly determine if there is a basic RADIUS problem by using the RADIUS Ping tool. For example, in [Figure 157 \(A\)](#), RADIUS Ping is unable to contact the server. In [Figure 157 \(B\)](#), RADIUS Ping verifies that the host information and secret for a RADIUS server are correct, but that the user account information is not.

**Select RADIUS** allows you to select a RADIUS server that you have already configured. When you make a choice in this field, additional fields will be displayed. Set **Select RADIUS** to **External Radius**, **Internal Radius**, or a server specified for a particular SSID, or select **Other Server** to specify another server by entering its **Host** name or IP address, **Port**, and shared **Secret**.

Enter the **RADIUS Credentials: Username** and **Password**. Select the **Authentication Type**, **PAP** or **CHAP**. Click the **Execute** button to run the command. The message **Testing RADIUS connection** appears. Click **OK** to proceed.

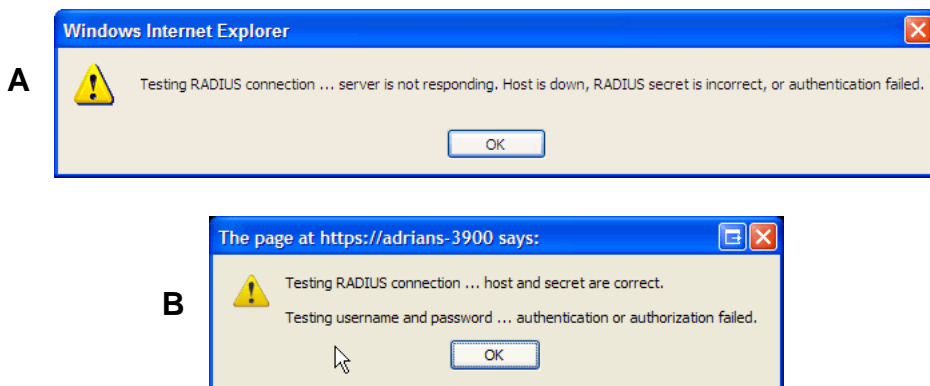


Figure 157. Radius Ping Output

16. **IP Address:** For Ping or Trace Route, enter the IP address of the target device.
17. **Timeout:** For Ping or Trace Route, enter a value (in seconds) before the action times out.
18. **Execute System Command:** Click **Execute** to start the specified command. Progress of command execution is displayed in the **Progress** frame. Results are displayed in the **Status** frame.

### Progress and Status Frames

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

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

## CLI

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

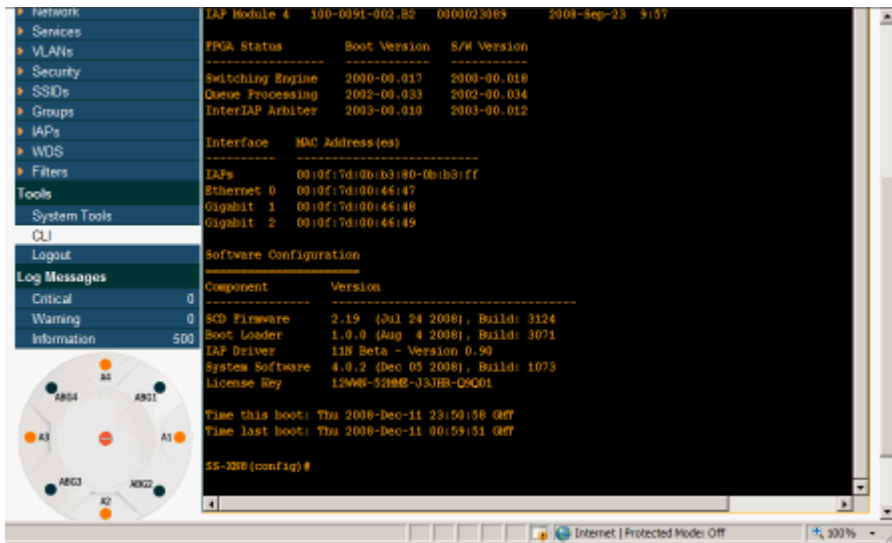


Figure 158. CLI Window

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

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

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

**config-iap**. The prompt will indicate the current command mode, for example:

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

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

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

## Logout

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

XN8 Wi-Fi Array		XIRRUS
Name: SS-XN8 (10.100.47.186)	Location: SS Area	
Current Status:	Logged Out	
User Name:	<input type="text"/>	
User Password:	<input type="password"/>	
		Login

Figure 159. Login Window

# The Command Line Interface

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

- [“Establishing a Secure Shell \(SSH\) Connection” on page 313.](#)
- [“Getting Started with the CLI” on page 315.](#)
- [“Top Level Commands” on page 317.](#)
- [“Configuration Commands” on page 326.](#)
- [“Sample Configuration Tasks” on page 361.](#)

## *See Also*

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

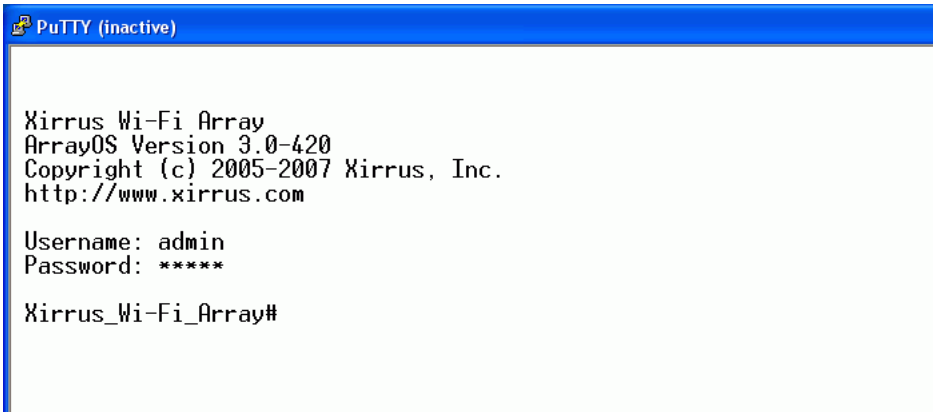
## Establishing a Secure Shell (SSH) Connection

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

1. Start your SSH session and communicate with the Array via its IP address.
  - If the Array is connected to a network that uses DHCP, use the address assigned by DHCP. We recommend that you have the network administrator assign a reserved address to the Array for ease of access in the future.
  - If the network does not use DHCP, use the factory default address 10.0.2.1 to access either the Gigabit 1 or Gigabit 2 Ethernet port. You may need to change the IP address of the port on your computer that

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

- If your Array is an 8-, 12-, or 16-port model, it has a 10/100Mb Ethernet port called Ethernet0. This management port has a default IP address of 10.0.1.1. You may connect your computer directly to this port, but you will need to set the IP address of the connected port on your computer to the 10.0.1.xx subnet.
2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the Array’s Command Line Interface.



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

Username: admin
Password: *****

Xirrus_Wi-Fi_Array#
```

Figure 160. Logging In



## Getting Started with the CLI

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

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

## Inputting Commands

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

## Getting Help

The CLI offers the following two levels of assistance:

- **help Command**

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



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

Username: admin
Password: *****

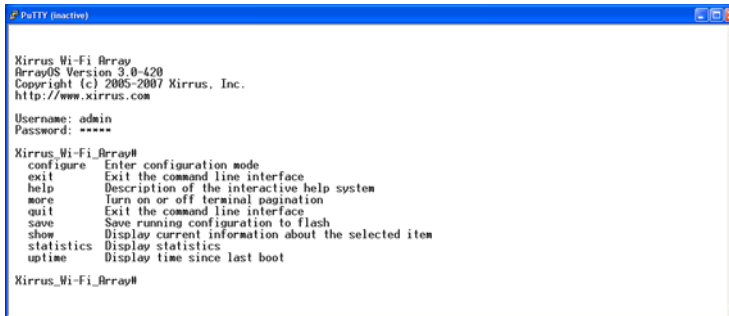
Xirrus_Wi-Fi_Array# help
Help may be requested at any point in a command by entering
a question mark '?'. If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.

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

Figure 161. Help Window

- **? Command**

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



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

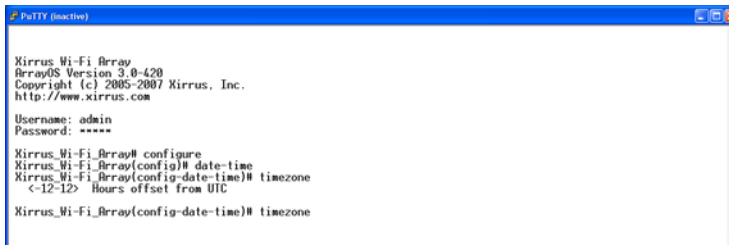
Username: admin
Password: *****

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

Xirrus_Wi-Fi_Array#
```

Figure 162. Full Help

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



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

Username: admin
Password: *****

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

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

Figure 163. Partial Help

## Top Level Commands

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

All other commands are considered second level configuration commands—these are the commands you use to configure specific elements of the Array’s features and functionality. For a listing of these commands with examples of command formats and structure, go to [“Configuration Commands” on page 326](#).

### Root Command Prompt

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

Command	Description
@	Type <b>@n</b> to execute command <b>n</b> (as shown by the <a href="#">history</a> command).
<b>configure</b>	Enter the configuration mode. See <a href="#">“Configuration Commands” on page 326</a> .
<b>exit</b>	Exit the CLI and terminate your session—if this command is used at any level other than the root command prompt you will simply exit the current level (step back) and return to the previous level.
<b>help</b>	Show a description of the interactive help system. See also, <a href="#">“Getting Help” on page 315</a> .
<b>history</b>	List history of commands that have been executed.
<b>more</b>	Turn terminal pagination ON or OFF.
<b>quit</b>	Exit the Command Line Interface (from any level).
<b>search</b>	Search for pattern in show command output.

Command	Description
<b>show</b>	Display information about the selected item. See “show Commands” on page 321.
<b>statistics</b>	Display statistical data about the Array. See “statistics Commands” on page 324.
<b>uptime</b>	Display the elapsed time since the last boot.

### configure Commands

The following table shows the second level commands that are available with the top level **configure** command [**Xirrus\_Wi-Fi\_Array(config)#**].

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

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

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

## show Commands

The following table shows the second level commands that are available with the top level **show** command [**Xirrus\_Wi-Fi\_Array# show**].

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

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



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

### statistics Commands

The following table shows the second level commands that are available with the top level **statistics** command [**Xirrus\_Wi-Fi\_Array# statistics**].

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

---

Command	Description
<cr>	Display configuration or status information.

## Configuration Commands

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

To see examples of some of the key configuration tasks and their associated commands, go to “[Sample Configuration Tasks](#)” on page 361.

### acl

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

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

## admin

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

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

## cdp

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

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

**clear**

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

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

### contact-info

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

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



## date-time

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

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

### dhcp-server

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

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

## dns

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

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

## file

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

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

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

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

## filter

The **filter** command [Xirrus\_Wi-Fi\_Array(config-filter)#] is used to manage protocol filters and filter lists.

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

Command	Description
<b>off</b>	Disable a filter list. FORMAT: <b>filter off</b>
<b>on</b>	Enable a filter list. FORMAT: <b>filter on</b>
<b>reset</b>	Delete all protocol filters and filter lists. FORMAT: <b>filter reset</b>
<b>stateful</b>	Enable or disable stateful filtering (firewall). FORMAT: <b>Stateful [enable   disable   on   off]</b>



**fips**

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

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

### group

The **group** command [Xirrus\_Wi-Fi\_Array(config)# **group**] is used to create and configure user groups. User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs. For more information, see “Groups” on page 248.

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

### hostname

The **hostname** command [Xirrus\_Wi-Fi\_Array(config)# **hostname**] is used to change the hostname used by the Array.

Command	Description
<b>hostname</b>	Change the hostname of the Array. FORMAT: <b>hostname [name]</b>

## https

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

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

## interface

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

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

## license

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

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

## load

The **load** command [**Xirrus\_Wi-Fi\_Array(config)# load**] loads a configuration file.

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

### location

The **location** command [**Xirrus\_Wi-Fi\_Array(config)# location**] is used to set the location for the Array.

Command	Description
<b>&lt;cr&gt;</b>	Set the location for the Array. FORMAT: <b>location [newlocation]</b>

### management

The **management** command [**Xirrus\_Wi-Fi\_Array(config)# management**] enters management mode, where you may configure console management parameters.

Command	Description
<b>&lt;cr&gt;</b>	Enter management mode. FORMAT: <b>management &lt;cr&gt;</b>

### more

The **more** command [**Xirrus\_Wi-Fi\_Array(config)# more**] is used to turn terminal pagination ON or OFF.

Command	Description
<b>off</b>	Turn OFF terminal pagination. FORMAT: <b>more off</b>
<b>on</b>	Turn ON terminal pagination. FORMAT: <b>more on</b>

## netflow

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

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

**no**

The **no** command [Xirrus\_Wi-Fi\_Array(config)# **no**] is used to disable a selected element or set the element to its default value.

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



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

### pci-audit

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

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

## quit

The **quit** command [Xirrus\_Wi-Fi\_Array(config)# **quit**] is used to exit the Command Line Interface.

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

## radius-server

The **radius-server** command [Xirrus\_Wi-Fi\_Array(config-radius-server)#] is used to configure the external and internal RADIUS server parameters.

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

### reboot

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

Command	Description
<b>&lt;cr&gt;</b>	Reboot the Array. FORMAT: <b>reboot</b>
<b>delay</b>	Reboot the Array after a delay of 1 to 60 seconds. FORMAT: <b>reboot delay [n]</b>

### reset

The **reset** command [Xirrus\_Wi-Fi\_Array(config)# **reset**] is used to reset all settings to their default values then reboot the Array.

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

## run-tests

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

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

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

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

### security

The **security** command [Xirrus\_Wi-Fi\_Array(config-security)#] is used to establish the security parameters for the Array.

Command	Description
<b>wep</b>	Set the WEP encryption parameters. FORMAT: <b>security wep</b>
<b>wpa</b>	Set the WEP encryption parameters. FORMAT: <b>security wpa</b>

## snmp

The **snmp** command [**Xirrus\_Wi-Fi\_Array(config-snmp)#**] is used to enable, disable, or configure SNMP.

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

## ssh

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

Command	Description
<b>disable</b>	Disable SSH. FORMAT: <b>ssh disable</b>
<b>enable</b>	Enable SSH. FORMAT: <b>ssh enable</b>



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

## ssid

The **ssid** command [Xirrus\_Wi-Fi\_Array(config-ssid)#] is used to establish your SSID parameters.

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

## standby

The **standby** command [Xirrus\_Wi-Fi\_Array(config-ssid)#] sets this Array to function as a standby unit for another Array.

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

## syslog

The **syslog** command [**Xirrus\_Wi-Fi\_Array(config-syslog)#**] is used to enable, disable, or configure the Syslog server.

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

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

### telnet

The **telnet** command [Xirrus\_Wi-Fi\_Array(config)# telnet] is used to enable or disable Telnet.

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

### uptime

The **uptime** command [Xirrus\_Wi-Fi\_Array(config)# uptime] is used to display the elapsed time since you last rebooted the Array.

Command	Description
<b>&lt;cr&gt;</b>	Display time since last reboot. FORMAT: <b>uptime</b>

## vlan

The **vlan** command [**Xirrus\_Wi-Fi\_Array(config-vlan)#**] is used to establish your VLAN parameters.

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

## Sample Configuration Tasks

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

- [“Configuring a Simple Open Global SSID” on page 362.](#)
- [“Configuring a Global SSID using WPA-PEAP” on page 363.](#)
- [“Configuring an SSID-Specific SSID using WPA-PEAP” on page 364.](#)
- [“Enabling Global IAPs” on page 365.](#)
- [“Disabling Global IAPs” on page 366.](#)
- [“Enabling a Specific IAP” on page 367.](#)
- [“Disabling a Specific IAP” on page 368.](#)
- [“Setting Cell Size Auto-Configuration for All IAPs” on page 369](#)
- [“Setting the Cell Size for All IAPs” on page 370.](#)
- [“Setting the Cell Size for a Specific IAP” on page 371.](#)
- [“Configuring VLANs on an Open SSID” on page 372.](#)
- [“Configuring Radio Assurance Mode \(Loopback Tests\)” on page 373.](#)

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

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

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

## Configuring a Simple Open Global SSID

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

```

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

Username: admin
Password: *****

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

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

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

Figure 164. Configuring a Simple Open Global SSID



## Configuring a Global SSID using WPA-PEAP

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

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

Username: admin
Password: *****

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

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

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

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

Username             SSID
-----             -
Mike                 Companyx

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

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

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

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

Figure 165. Configuring a Global SSID using WPA-PEAP

## Configuring an SSID-Specific SSID using WPA-PEAP

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

```

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

Username: admin
Password: *****

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

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

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

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

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

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

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

Figure 166. Configuring an SSID-Specific SSID using WPA-PEAP

## Enabling Global IAPs

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

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

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# all_up
Interface IAP a1 state changed to up
Interface IAP a3 state changed to up
Interface IAP a4 state changed to up
Interface IAP a5 state changed to up
Interface IAP a6 state changed to up
Interface IAP a7 state changed to up
Interface IAP a8 state changed to up
Interface IAP a9 state changed to up
Interface IAP a10 state changed to up
Interface IAP a11 state changed to up
Interface IAP a12 state changed to up
Interface IAP abg2 state changed to up
Interface IAP abg3 state changed to up
Interface IAP abg4 state changed to up

Xirrus_Wi-Fi_Array(config-iap-global)# save
Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
```

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

Figure 167. Enabling Global IAPs

## Disabling Global IAPs

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

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

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# all_down
  Interface IAP a1 state changed to down
  Interface IAP a2 state changed to down
  Interface IAP a3 state changed to down
  Interface IAP a4 state changed to down
  Interface IAP a5 state changed to down
  Interface IAP a6 state changed to down
  Interface IAP a7 state changed to down
  Interface IAP a8 state changed to down
  Interface IAP a9 state changed to down
  Interface IAP a10 state changed to down
  Interface IAP a11 state changed to down
  Interface IAP a12 state changed to down
  Interface IAP abg1 state changed to down
  Interface IAP abg2 state changed to down
  Interface IAP abg3 state changed to down
  Interface IAP abg4 state changed to down

Xirrus_Wi-Fi_Array(config-iap-global)# save
Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

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

Figure 168. Disabling Global IAPs

## Enabling a Specific IAP

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

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

Username: admin
Password: *****

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

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

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

Figure 169. Enabling a Specific IAP

## Disabling a Specific IAP

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

```

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

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a2 down
Xirrus_Wi-Fi_Array(config-iap)# save
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table

```

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

```

Xirrus_Wi-Fi_Array(config-iap)#

```

Figure 170. Disabling a Specific IAP

## Setting Cell Size Auto-Configuration for All IAPs

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

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

```

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

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

IAP Summary Table
-----
IAP State Channel Antenna Cell Size TX Power RX Threshold Stations WDS MAC address / BSSID Description
-----
a1 down 36 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:10
a2 up 36 int-dir auto -10dBm -65dBm 0 00:0F:7D:03:C3:30
a3 up 157 int-dir auto -10dBm -65dBm 0 00:0F:7D:03:C3:40
a4 up 56 int-dir auto -10dBm -65dBm 0 00:0F:7D:03:C3:50
a5 down 56 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:70
a6 down 157 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:80
a7 down 44 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:90
a8 down 60 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:b0
a9 up 153 int-dir auto -10dBm -65dBm 0 00:0F:7D:03:C3:c0
a10 down 48 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:d0
a11 down 64 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:f0
a12 down 161 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:00
abg1 down 1 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:20
abg2 up monitor int-omni manual 20dBm -95dBm 0 00:0F:7D:03:C3:60
abg3 down 11 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:a0
abg4 down 6 int-dir max 20dBm -90dBm 0 00:0F:7D:03:C3:e0

Xirrus-WiFi-Array(config-iap)#

```

Figure 171. Setting the Cell Size for All IAPs

## Setting the Cell Size for All IAPs

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

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

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

Username: admin
Password: *****

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

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

Figure 172. Setting the Cell Size for All IAPs



## Setting the Cell Size for a Specific IAP

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

```
Xirrus Wi-Fi Array

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

Username: admin
Password: *****

Running configuration has not been saved.

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

IAP Summary Table

```

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

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

Figure 173. Setting the Cell Size for a Specific IAP

## Configuring VLANs on an Open SSID

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

```

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

Username: admin
Password: *****

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

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

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

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

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

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

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

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

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

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



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

Figure 174. Configuring VLANs on an Open SSID

### Configuring Radio Assurance Mode (Loopback Tests)

The Array uses the built-in monitor radio, IAP abg(n)2, to monitor other radios in the Array. Tests include sending probes on all channels and checking for a response, and checking whether beacons are received from the other radio. If a problem is detected, corrective actions are taken to recover. Loopback mode operation is described in detail in “Array Monitor and Radio Assurance Capabilities” on page 412.

The following actions may be configured:

- **alert-only**—the Array will issue an alert in the Syslog.
- **repair-without-reboot**—the Array will issue an alert and reset radios at the Physical Layer (Layer 1) and possibly at the MAC layer. The reset should not be noticed by users, and they will not need to reassociate.
- **reboot-allowed**—the Array will issue an alert, reset the radios, and schedule the Array to reboot at midnight (per local Array time) if necessary. All stations will need to reassociate to the Array.
- **off**—Disable IAP loopback tests (no self-monitoring occurs). Radio Assurance mode is off by default.

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

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

```

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

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

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

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

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

```

Figure 175. Configuring Radio Assurance Mode (Loopback Testing)

# Appendices



Page is intentionally blank

## Appendix A: Servicing the Wi-Fi Array

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

- “Removing the Access Panel” on page 379.
- “Reinstalling the Access Panel” on page 382.
- “Replacing the FLASH Memory Module” on page 384.
- “Replacing the Main System Memory” on page 386.
- “Replacing the Integrated Access Point Radio Module” on page 388.
- “Replacing the Power Supply Module” on page 391.

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

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

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

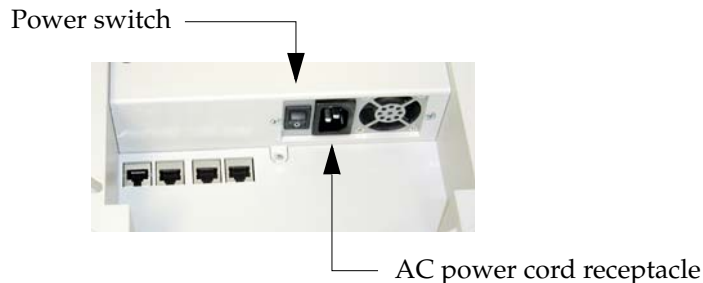


Figure 176. Disconnecting Power from the Array



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

*See Also*

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module



## Removing the Access Panel

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

1. Turn OFF the Array's main power switch (XS-3900 and XS-3700 only).
2. Disconnect the AC power cord or Ethernet cable supplying power from the Array.
3. Place the Array face-down on a flat surface. Avoid moving the unit to reduce the risk of damage (scratching) to the finished enclosure.
4. Remove the screws (3 places) that secure the access panel to the main body of the Array.

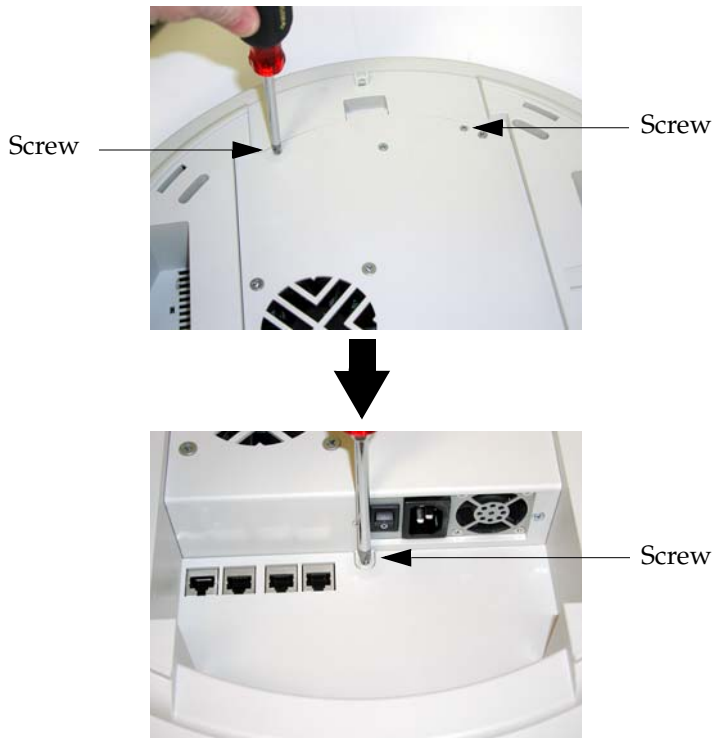


Figure 177. Removing the Access Panel Screws

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



Lift up the access panel

Figure 178. Removing the Access Panel

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



Fan connector

Power supply connector

Figure 179. Disconnecting the Power Supply and Fan

7. The access panel can now be safely removed.

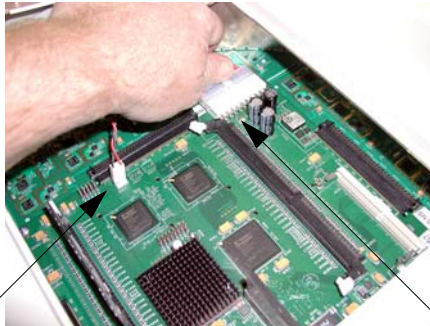
*See Also*

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

## Reinstalling the Access Panel

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

1. Reconnect the fan and power supply.



Fan connector

Power supply connector

Figure 180. Reconnecting the Fan and Power Supply

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



Figure 181. Reinstalling the Access Panel

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

*See Also*

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

## Replacing the FLASH Memory Module

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

1. Remove the system's access panel. Refer to "Removing the Access Panel" on page 379.
2. Remove the FLASH memory module, taking care not to "wiggle" the module and risk damaging the connection points.

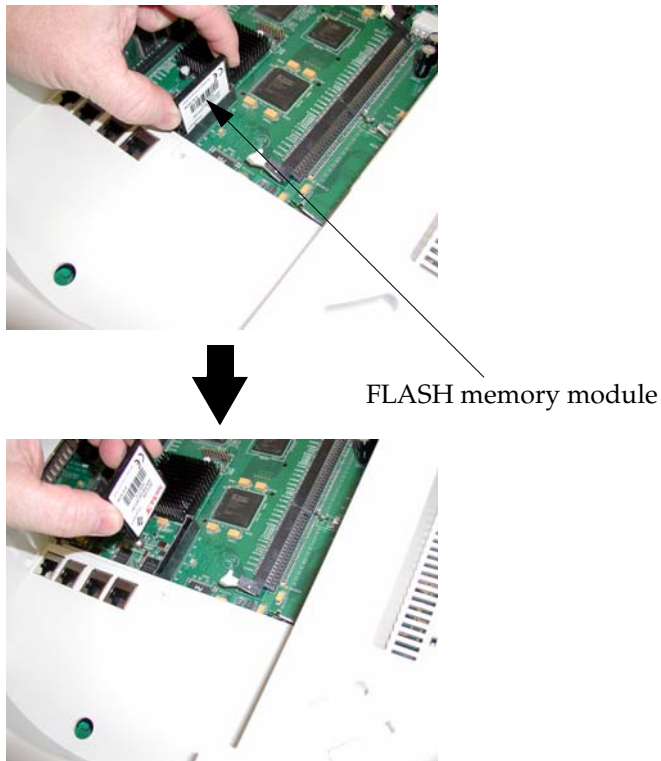


Figure 182. Removing the FLASH Memory Module

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

4. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 382).

*See Also*

Reinstalling the Access Panel

Removing the Access Panel

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

## Replacing the Main System Memory

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

1. Remove the access panel (refer to “Removing the Access Panel” on page 379).
2. Remove the DIMM memory module, taking care not to “wobble” the module and risk damaging the connection points.

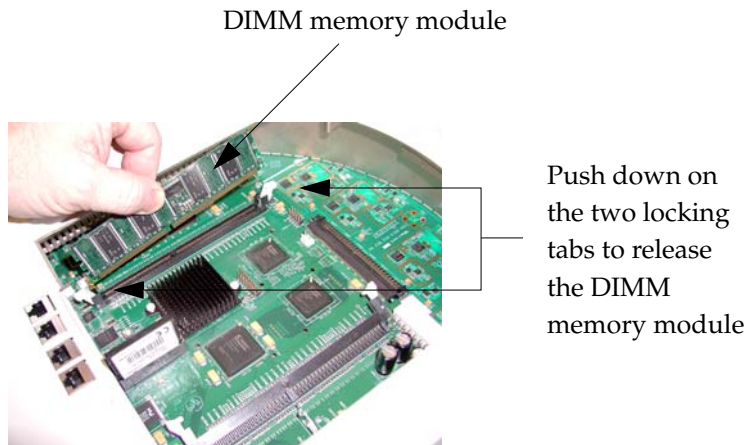


Figure 183. Removing the DIMM Memory Module

3. The removal procedure is complete. You can now reinstall the DIMM memory module (or install a new module). Ensure that the DIMM memory module is seated evenly and the locking tabs are in the upright position. The DIMM memory module is keyed to fit in its socket in one direction only.
4. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 382).

### *See Also*

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module



Replacing the Integrated Access Point Radio Module

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

## Replacing the Integrated Access Point Radio Module

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

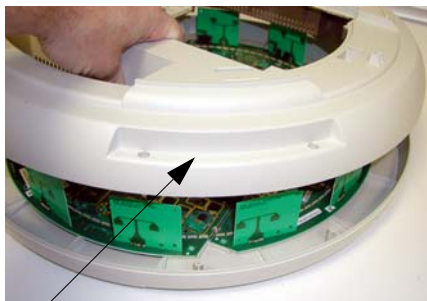
1. Remove the access panel (refer to “Removing the Access Panel” on page 379).
2. Remove the locking screws (8 places) that secure the chassis cover to the main body of the Wi-Fi Array.



Screws (8 places)

Figure 184. Removing the Chassis Cover Screws

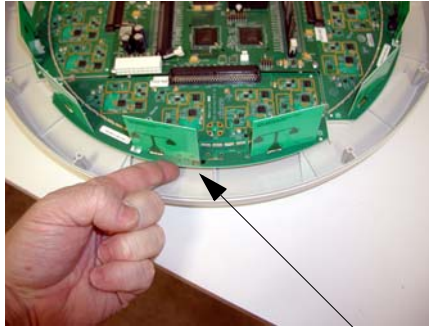
3. Lift and remove the chassis cover.



Remove the chassis cover

Figure 185. Removing the Chassis Cover

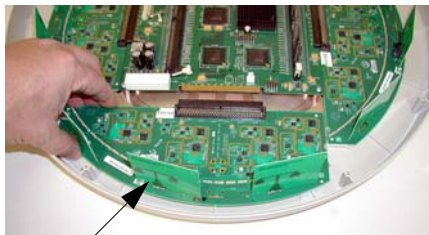
4. Lift the edge of the integrated access point module.



Lift here (do not force)

Figure 186. Lifting the Integrated Access Point Module

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



Disconnect the module

Figure 187. Disconnect the Integrated Access Point Module

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

7. Reinstall the chassis cover (see warnings).
  - ! *When reinstalling the chassis cover, take care to align the cover correctly to avoid damaging the antenna modules. Do not force the chassis cover onto the body of the unit.*
  - ! *Do not overtighten the locking screws.*
8. Reinstall the locking screws (8 places) to secure the chassis cover in place—do not overtighten.
9. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 382).

*See Also*

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

## Replacing the Power Supply Module

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

1. Remove the access panel (refer to “Removing the Access Panel” on page 379).
2. Because the power supply unit is molded into the access panel, you must install a new access panel assembly (with the power supply attached). Refer to “Reinstalling the Access Panel” on page 382.



Access panel (with power supply and fan)

Figure 188. Installing a New Access Panel (with Power Supply)

### *See Also*

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

Use this Space for Your Notes



## Appendix B: Quick Reference Guide

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

- “Factory Default Settings” on page 393.
- “Keyboard Shortcuts” on page 400.

### Factory Default Settings

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

#### Host Name

Setting	Default Value
Host name	Xirrus-WiFi-Array

#### Network Interfaces

##### Serial

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

### Gigabit 1 and Gigabit 2

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

### Fast Ethernet

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



Setting	Default Value
MTU Size	1500
Management Enabled	Yes

### Integrated Access Points (IAPs)

Setting	Default Value
IAP abg2 Defaults	Enabled Mode = Monitor Channel = Monitor Cell Size = Manual Antenna = Internal-Omni
Enabled (Radio State)	No
Mode <ul style="list-style-type: none"> <li>● XS16, XS-3900</li> <li>● XS8, XS-3700</li> <li>● XS4, XS-3500</li> </ul>	802.11a for a1 to a12 802.11bg for abg1 to abg4  802.11a for a1 to a4 802.11bg for abg1 to abg4  802.11bg for abg1 to abg4
Channel	Auto
Cell Size	Max
Maximum Transmit Power	20
Antenna Selected	Internal

## Server Settings

### NTP

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

### Syslog

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

### SNMP

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

Setting	Default Value
Trap Port	162
Authorization Fail Port	On

## DHCP

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

## Default SSID

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

Setting	Default Value
Broadcast	On

## Security

### Global Settings - Encryption

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

### External RADIUS (Global)

Setting	Default Value
Enabled	Yes
Primary Server	None
Primary Port	1812

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

### Internal RADIUS

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

## Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

## Management

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

## Keyboard Shortcuts

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

Action	Shortcut
Cut selected data and place it on the clipboard.	<b>Ctrl + X</b>
Copy selected data to the clipboard.	<b>Ctrl + C</b>

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

*See Also*  
[An Overview](#)

Use this Space for Your Notes



## Appendix C: Technical Support

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

- [“General Hints and Tips” on page 403](#)
- [“Frequently Asked Questions” on page 404](#)
- [“Array Monitor and Radio Assurance Capabilities” on page 412](#)
- [“Upgrading the Array via CLI” on page 415](#)
- [“Power over Gigabit Ethernet Compatibility Matrix” on page 420](#)
- [“Contact Information” on page 422](#)

### General Hints and Tips

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

- The Wi-Fi Array requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.
- If using multiple Arrays in the same area, maintain a distance of at least 100 feet (30m) between Arrays if there is direct line-of-sight between the units, or at least 50 feet (15 m) if a wall or other barrier exists between the units.
- Keep the Wi-Fi Array away from electrical devices or appliances that generate RF noise. Because the Array is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).
- If using AC power, each Wi-Fi Array requires its own dedicated AC power outlet. Do not attempt to “piggy-back” AC power to multiple units. To avoid needing to run separate power cables to one or more Arrays, consider using Power over Gigabit Ethernet.

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

### *See Also*

Contact Information

Multiple SSIDs

Security

VLAN Support

## Frequently Asked Questions

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

### Multiple SSIDs

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

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

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

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

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

**Q. What would I use SSIDs for?**

- A.** The creation of different wireless network names allows system administrators to separate types of users with different requirements. The following policies can be tied to an SSID:
- Minimum security required to join this SSID.
  - The wireless Quality of Service (QoS) desired for this SSID.
  - The wired VLAN associated with this SSID.

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

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

**Q. How do I set up SSIDs?**

- A.** Use the following procedure as a guideline. For more detailed information, go to “SSIDs” on page 235.
1. From the Web Management Interface, go to the [SSID Management](#) page.
  2. Select **Yes** to make the SSID visible to all clients on the network. Although the Wi-Fi Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
  3. Select the minimum security that will be required by users for this SSID.
  4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.
  5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.

6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.
7. Click on the **Apply** button to apply your changes to this session.
8. Click on the **Save** button to save your changes.
9. If you need to edit any of the SSID settings, you can do so from the [SSID Management](#) page.

### *See Also*

Contact Information

General Hints and Tips

Security

SSIDs

SSID Management

VLAN Support

## Security

- Q. How do I ensure that an Array meets FIPS requirements?**
- A.** To meet the Level 2 security requirements of FIPS 140-2, follow the instructions in [Appendix E: Implementing FIPS Security](#).
- Q. How do I ensure that an Array meets PCI DSS requirements?**
- A.** To meet PCI DSS requirements, follow the instructions in [Appendix D: Implementing PCI DSS](#).
- Q. How do I know my management session is secure?**
- A.** Follow these guidelines:
- Administrator passwords  
Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.

- SSH versus Telnet  
Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY. The Array only allows SSH-2 connections, so your SSH utility must be set up to use SSH-2.
- Configuration auditing  
Do not change approved configuration settings. The optional Xirrus Management System (XMS) offers powerful management features for small or large Wi-Fi Array deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.

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

- A.** Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The Wi-Fi Array allows you to establish the following data encryption configuration options:
- Open  
This option offers no data encryption and is **not recommended**, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTY.
  - WEP (Wired Equivalent Privacy)  
This option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
  - WPA (Wi-Fi Protected Access)  
This is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

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

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

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



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

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

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

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

- Pre-Shared Key

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

- RADIUS 802.1x with EAP

802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal

(provided by the Wi-Fi Array) or external. An external RADIUS server offers more functionality and is **recommended** for large Enterprise deployments.

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

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

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

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

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

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

*See Also*

Contact Information

General Hints and Tips

Multiple SSIDs

VLAN Support

---

## VLAN Support

**Q. What Are VLANs?**

- A.** VLANs (Virtual Local Area Networks) are a logical grouping of network devices that share a common network broadcast domain. Members of a particular VLAN can be on any segment of the physical network but logically only members of a particular VLAN can see each other.

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

**Q. What would I use VLANs for?**

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

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

**Q. What are Wireless VLANs?**

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

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

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



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

### *See Also*

Contact Information

General Hints and Tips

Multiple SSIDs

Security

## Array Monitor and Radio Assurance Capabilities

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

### Enabling Monitoring on the Array

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

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

The settings above will automatically set the **Antenna** selection to **Internal-Omni.**, also required for monitoring. See the “[IAP Settings](#)” on page 256 for more details. The values above are the factory default settings for the Array.

### How Monitoring Works

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

1. The monitor radio scans all channels with a 200ms dwell time, hitting all channels about once every 10 seconds.
2. Each time it tunes to a new channel it sends out a probe request in an attempt to smoke out rogues.
3. It then listens for all probe responses and beacons to detect any rogues within earshot.
4. Array radios respond to that probe request with a probe response.

**Intrusion Detection** is enabled or disabled separately from monitoring. See [Step 1](#) in “[Advanced RF Settings](#)” on page 277.

## Radio Assurance

The Array is capable of performing continuous, comprehensive tests on its radios to assure that they are operating properly. Testing is enabled using the **Radio Assurance Mode** setting on the [Advanced RF Settings](#) window (Step 5 in “[Advanced RF Settings](#)” on page 277). When this mode is enabled, IAP abg(n)2 performs loopback tests on the Array. Radio Assurance Mode requires **Intrusion Detection** to be set to **Standard** (See Step 1 in “[Advanced RF Settings](#)” on page 277).

When **Radio Assurance Mode** is enabled:

1. The Array keeps track of whether or not it hears beacons and probe responses from the Array’s radios.
2. After 10 minutes (roughly 60 passes on a particular channel by the monitor radio), if it has not heard beacons or probe responses from one of the Array’s radios it issues an alert in the Syslog. If repair is allowed (see “[Radio Assurance Options](#)” on page 414), the Array will reset and reprogram that particular radio at the Physical Layer (PHY—Layer 1). This action takes under 100ms and stations are not deauthenticated, thus users should not be impacted.
3. After another 10 minutes (roughly another 60 passes), if the monitor still has not heard beacons or probe responses from the malfunctioning radio it will again issue an alert in the Syslog. If repair is allowed, the Array will reset and reprogram the MAC (the lower sublayer of the Data Link Layer) and then all of the PHYs. This is a global action that affects all radios. This action takes roughly 300ms and stations are not deauthenticated, thus users should not be impacted.
4. After another 10 minutes, if the monitor still has not heard beacons or probe responses from that radio, it will again syslog the issue. If reboot is allowed (see “[Radio Assurance Options](#)” on page 414), the Array will schedule a reboot. This reboot will occur at one of the following times, whichever occurs first:
  - When no stations are associated to the Array
  - Midnight

### Radio Assurance Options

If the monitor detects a problem with an Array radio as described above, it will take action according to the preference that you have specified in the **Radio Assurance Mode** setting on the [Advanced RF Settings](#) window (see [Step 5](#) page 279):

- **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
- **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of the PHY and MAC as described above.
- **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets of the PHY and MAC, and schedule reboots as described above.
- **Disabled**—Disable IAP loopback tests (no self-monitoring occurs). Loopback tests are disabled by default.

## Upgrading the Array via CLI

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

1. Download the latest software update from the Xirrus FTP site using your Enhanced Care FTP username and password. If you do not have an FTP username and password, contact Xirrus Customer Service for assistance (support@xirrus.com). The software update is provided as a zip file. Unzip the contents to a local temp directory. Take note of the extracted file name in case you need it later on—you may also need to copy this file elsewhere on the network depending on your situation.
2. Install a TFTP server software package if you don't have one running. It may be installed on any PC on your network, including your desktop or laptop. The Solar Winds version is freeware and works well.

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

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

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

3. Determine the IP address of the computer hosting the TFTP server. (To display the IP address, open a command prompt and type **ipconfig**)
4. Connect your Array to the computer running TFTP using a serial cable, and open a terminal program if you haven't already. Attach a network cable to the Array's GIG1 port, if it is not already part of your network.

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

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

5. Type **dhcp** and hit return. This instructs the Array to obtain a DHCP address and use it during this boot in the bootloader environment.
6. Type **dir** and hit return to see what's currently in the compact flash.
7. Type **del** and hit return to delete the contents of the compact flash.
8. Type **update server <TFTP-server-ip-addr> xs-3.x-xxxx.bin** (the actual Xirrus file name will vary depending on Array model number and software version—use the file name from your software update) and hit return. The software update will be transferred to the Array's memory and will be written to the it's compact flash card. (See output below.)
9. Type **reset** and hit return. Your Array will reboot, running your new version of software.

### Sample Output for the Upgrade Procedure:

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

```
Username: admin
```

```
Password: *****
```

```
Xirrus-WiFi-Array# configure
```

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

```
Are you sure you want to reboot? [yes/no]: yes
```

```
Array is being rebooted.
```

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

```
Processor | Motorola PowerPC, PVR=80200020 SVR=80300020
```

```
Board | Xirrus MPC8540 CPU Board
```

```
Clocks | CPU : 825 MHz DDR : 330 MHz Local Bus: 41 MHz
```

```

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

```

```

In: serial
Out: serial
Err: serial

```

**Press space bar to exit to bootloader:**

```

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

```

[CFCard] Directory of /

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

3 file(s), 2 dir(s)

```
XBL>del *
[CFCard] Delete : 2 file(s) deleted

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

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

```
XBL>reset
[RESET ]
```

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

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



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

In: serial  
Out: serial  
Err: serial

Press space bar to exit to bootloader:

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

Initializing hardware ..... OK

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

Username:

## Power over Gigabit Ethernet Compatibility Matrix

The Xirrus Power over Gigabit Ethernet (PoGE) solution includes different modules to be used with particular Array models. The following two tables indicate the proper PoGE injectors to use with each Array. **X** indicates that products are INCOMPATIBLE.

Table 1: Compatibility of Arrays and PoGE Injectors

Array Model	Summary	XP1-MSI (60W)	XP1-MSI-75, XP1-MSI-75M	XP2-MSI-95M	XP8-MSI-70M
XN4	Works with any PoGE injector	✓	✓	✓	✓
XN8	Requires 70W or higher	<b>X</b>	✓	✓	✓
XN12	XP2-MSI-95M is preferred	<b>2*</b>	<b>2*</b>	✓	<b>2*</b>
XN16	XP2-MSI-95M is preferred	<b>2*</b>	<b>2*</b>	✓	<b>2*</b>
XS4	Works with any PoGE injector	✓	✓	✓	✓
XS8	Works with any PoGE injector	✓	✓	✓	✓
XS16		<b>X</b>	✓	✓	✓
XE-4000 PoE	XE-4000 PoE Outdoor Enclosure draws up to 70W		✓	✓	✓
<b>2*</b> – Two ports are required to provide power to the XN12 or XN16					

NOTE: The XP1-MSI-75M, XP2-MSI-95M, and XP8-MSI-70M can all be managed remotely using SNMP.

NOTE: An 8-port XP8-MSI-70M injector powers up to eight of the XS Arrays or XN4 or XN8 Arrays; or four XN12 or XN16 Arrays.

Table 2: Legacy PoGE Injectors/Splitters

Array Model	Compatible Xirrus Injector	XP1-MSI-X Injector	XP8-MSI Injector	XP1-MSI Injector
XS4	Works with any PoGE injector	✓	✓	✓
XS8, XN4	Works with any PoGE injector, no splitter required	✓	✓	✓
XN16/XN12/ XN8/XN4, XS16	Works with two injector options, no splitter required	✓	✓ <sup>1</sup>	✗

1. The 8-port XP8-MSI-H and XP8-MSI injectors each power up to eight 4-port or 8-port Arrays; or four 16-port Arrays.

For compatibility information for older -H model PoGE injectors or for XS-3500, XS-3700, and XS-3900 Arrays, please see the Compatibility Matrix in the *Xirrus Wi-Fi Array User's Guide for Release 3.5*, available at [support.xirrus.com](http://support.xirrus.com) in the Downloads area.

---

## Contact Information

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

Xirrus, Inc.

2101 Corporate Center Drive

Thousand Oaks, CA 91320

USA

Tel: 1.805.262.1600

1.800.947.7871 Toll Free in the US

Fax: 1.866.462.3980

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

[support.xirrus.com](http://support.xirrus.com)

## Appendix D: Implementing PCI DSS

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

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

### Payment Card Industry Data Security Standard Overview

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

PCI DSS Control Objectives and Associated Requirements
<p><b>Objective: Build and Maintain a Secure Network</b></p> <ul style="list-style-type: none"> <li>● Requirement 1: Install and maintain a firewall configuration to protect cardholder data.</li> <li>● Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.</li> </ul>
<p><b>Objective: Protect Cardholder Data</b></p> <ul style="list-style-type: none"> <li>● Requirement 3: Protect stored cardholder data.</li> <li>● Requirement 4: Encrypt transmission of cardholder data across open, public networks.</li> </ul>

### PCI DSS Control Objectives and Associated Requirements

**Objective: Maintain a Vulnerability Management Program**

- Requirement 5: Use and regularly update anti-virus software.
- Requirement 6: Develop and maintain secure systems and applications.

**Objective: Implement Strong Access Control Measures**

- Requirement 7: Restrict access to cardholder data by business need-to-know.
- Requirement 8: Assign a unique ID to each person with computer access.
- Requirement 9: Restrict physical access to cardholder data.

**Objective: Regularly Monitor and Test Networks**

- Requirement 10: Track and monitor all access to network resources and cardholder data.
- Requirement 11: Regularly test security systems and processes.

**Objective: Maintain an Information Security Policy**

- Requirement 12: Maintain a policy that addresses information security.

## PCI DSS and Wireless

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

## The Xirrus Array PCI Compliance Configuration

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

✓	Xirrus Wi-Fi Array Configuration for PCI DSS	See...
<ul style="list-style-type: none"> <li>( )</li> <li>( )</li> </ul>	<p>Register at the Xirrus Support Site to ensure notification and access to software updates.</p> <p>Confirm that the latest version of the Array OS is being used by checking the Xirrus web site.</p>	<p><a href="http://support.xirrus.com">support.xirrus.com</a></p>
<ul style="list-style-type: none"> <li>( )</li> </ul>	<p>Enable PCI Mode after configuring the Array in a PCI compliant state to ensure configuration changes cannot be saved that would invalidate a PCI compliant configuration. This item is covered on the following pages.</p>	<p>The <code>pci-audit</code> Command, p. 426</p>
<ul style="list-style-type: none"> <li>( )</li> </ul>	<p>Allow only necessary protocols and networks to be accessed by configuring your corporate firewall or using the internal Array firewall.</p>	<p>Filters, p. 291</p>
<ul style="list-style-type: none"> <li>( )</li> <li>( )</li> <li>( )</li> <li>( )</li> <li>( )</li> <li>( )</li> </ul>	<p>Change the default Admin account password.</p> <p>Remove any unnecessary admin or user accounts.</p> <p>Change the SNMP community string from the default password.</p> <p>Use WPA2 and 802.1x authentication.</p> <p>Change default SSID from Xirrus to a user-defined SSID.</p> <p>Disable SSID broadcast for all PCI compliant SSIDs.</p>	<p>Express Setup, p. 174</p> <p>Admin Management, p. 214</p> <p>SNMP, p. 199</p> <p>SSIDs, p. 235 and Global Settings, p. 224</p> <p>SSIDs, p. 235</p> <p>SSIDs, p. 235</p>
<ul style="list-style-type: none"> <li>( )</li> <li>( )</li> <li>( )</li> </ul>	<p>Enable Secure Shell (ssh) for CLI (command line) access.</p> <p>Confirm telnet access is disabled (done by default).</p> <p>Confirm management over the wireless network is disabled.</p>	<p>Management Control, p. 218</p> <p>Global Settings (IAP), p. 261</p>

✓	Xirrus Wi-Fi Array Configuration for PCI DSS	See...
( )	Check that external RADIUS servers have been configured for use with 802.1x and WPA/WPA2 wireless security.	SSIDs, p. 235 and Global Settings, p. 224
( )	Ensure that Array Administration Accounts are being validated by External RADIUS servers.	Admin RADIUS, p. 215
( )	Ensure that each Xirrus Array is physically inaccessible such that console ports and management ports are not accessible.	Securing the Array, p. 94 See Indoor Enclosure
( )	Enable syslog messaging and define a syslog server on the wired network to receive syslog messages.	System Log, p. 196
( )	Enable NTP and define an NTP server (optional).	Time Settings (NTP), p. 193
( )	Enable the RF Monitor radio in the Xirrus Array. Categorize known or approved devices as such. Respond to any alert of unknown or unapproved wireless devices discovered by the RF Monitor.	IAP Settings, p. 256 Rogue Control List, p. 233 Intrusion Detection, p. 148

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

## The pci-audit Command

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



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

The `pci-audit` command checks items such as:

- Telnet is disabled.
- Admin RADIUS is enabled (admin login authentication is via RADIUS server).
- An external Syslog server is in use.
- All SSIDs must set encryption to WPA or better (which also enforces 802.1x authentication)

Sample output from this command is shown below.

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

Figure 189. Sample output of `pci-audit` command

## Additional Resources

- PCI Security Standards Web site: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)
- List of Qualified PCI Security Assessors: [www.pcisecuritystandards.org/pdfs/pci\\_qsa\\_list.pdf](http://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf)
- For the latest version of the Xirrus White Paper, *PCI Data Security Standard*, and the latest versions of Xirrus software, please check [www.xirrus.com](http://www.xirrus.com)



## Appendix E: Implementing FIPS Security

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

The following topics are discussed:

- “To implement FIPS 140-2, Level 2 using WMI” on page 429.
- “To check if an Array is in FIPS mode:” on page 435
- “To implement FIPS 140-2, Level 2 using CLI:” on page 435

### *To implement FIPS 140-2, Level 2 using WMI*

1. Apply the supplied tamper-evident seals to the unit as indicated in the figures below. The procedure is slightly different, depending on the model.
  - Before you apply the tamper-evident seal, clean the area of any grease, dirt, or oil. We recommend using alcohol-based cleaning pads for this.
  - Each seal must be applied to straddle both sides of an opening so that it will show if an attempt has been made to open the Array.

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

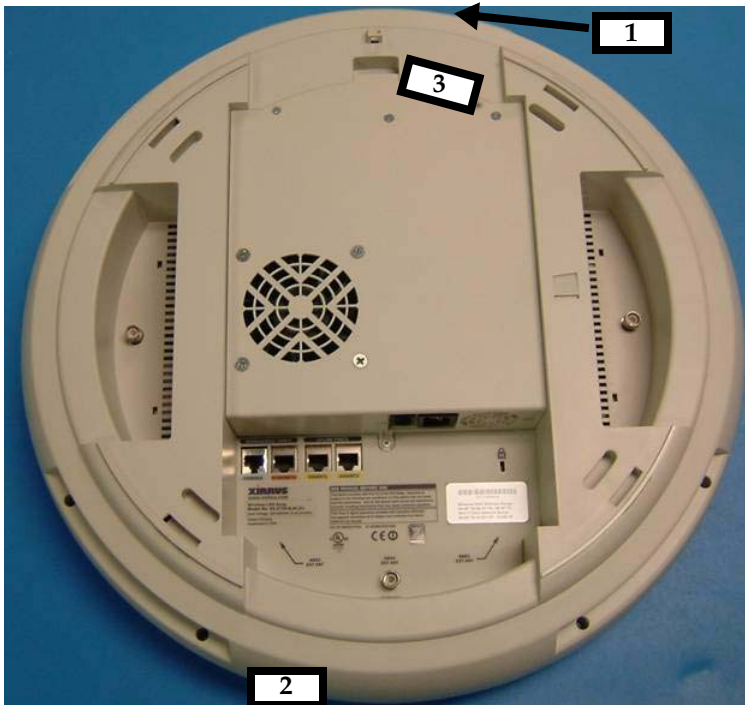


Figure 190. Applying Three Seals to XS16/XS8 or XS-3900/XS-3700

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

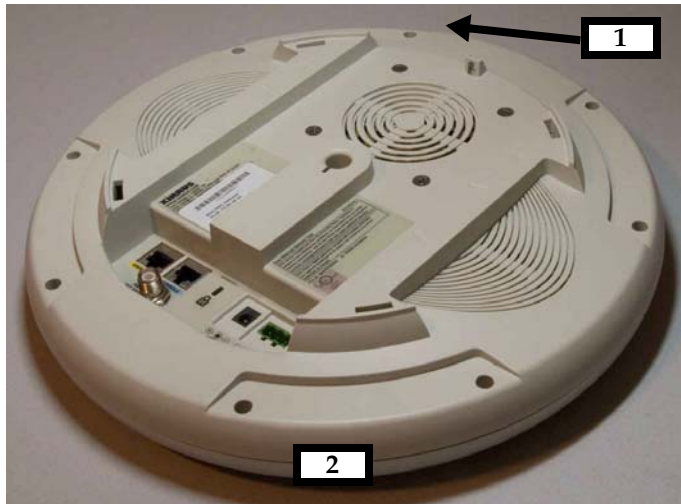


Figure 191. Applying Two Tamper-evident seals to the XS4 or XS-3500

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

```
Xirrus_Wi-Fi_Array(config)# https on
```

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

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

The screenshot displays the 'XS-3900 Wi-Fi Array' management interface. On the left is a navigation menu with categories like Status, Configuration, and Tools. The main area is titled 'SSID Management' and shows a form for creating or editing an SSID. The 'New SSID Name' field is empty, and the 'SSID' list contains one entry: 'xirus (Broadcast)'. Below this, various configuration parameters are set, including 'State: Enable', 'Broadcast SSID: Enable', 'Band Association: Both', 'QoS Priority: 2', 'Station Limit: 1024', and 'Encryption Type: WPA2'. A status summary at the bottom left shows 60 Critical Msgs, 0 Warning Msgs, and 73 General Msgs. The 'Modify' and 'Save' buttons are visible at the bottom right of the configuration panel.

Figure 192. SSID Management Window

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



Figure 193. Security/Global Settings Window

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

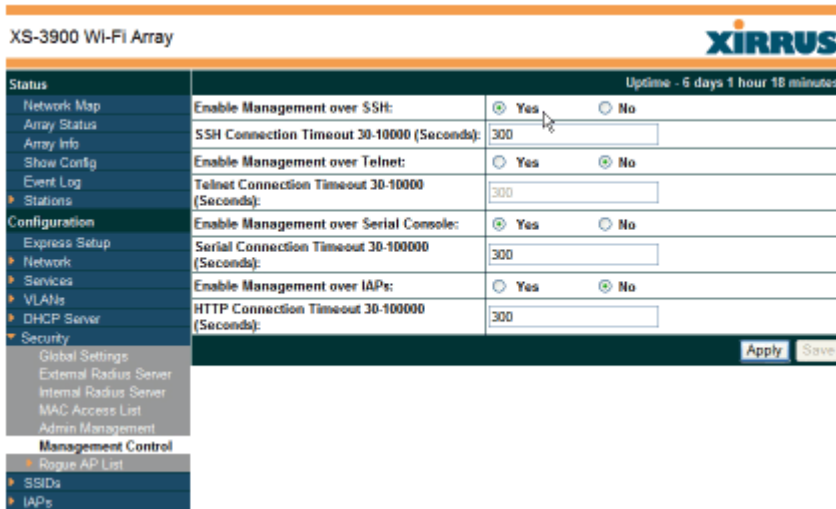


Figure 194. Security/Management Control Window

- In the Services/SNMP window, select **No** for **Enable SNMP**. Click **Apply**, then **Save**.

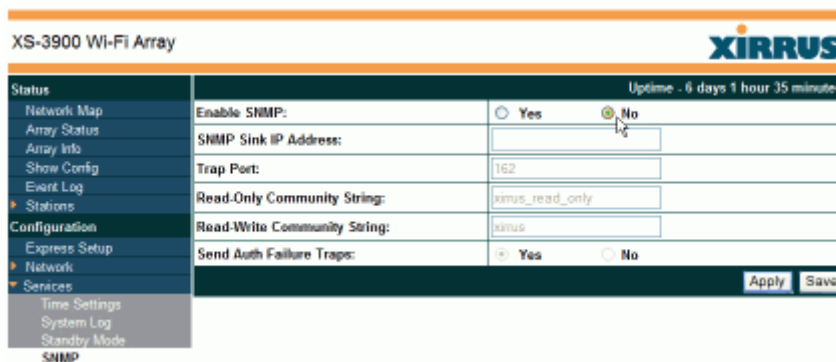


Figure 195. Services/SNMP Window



- In the IAPs/Global Settings window, select **Off** for **Fast Roaming**. Click **Apply**, then **Save**.

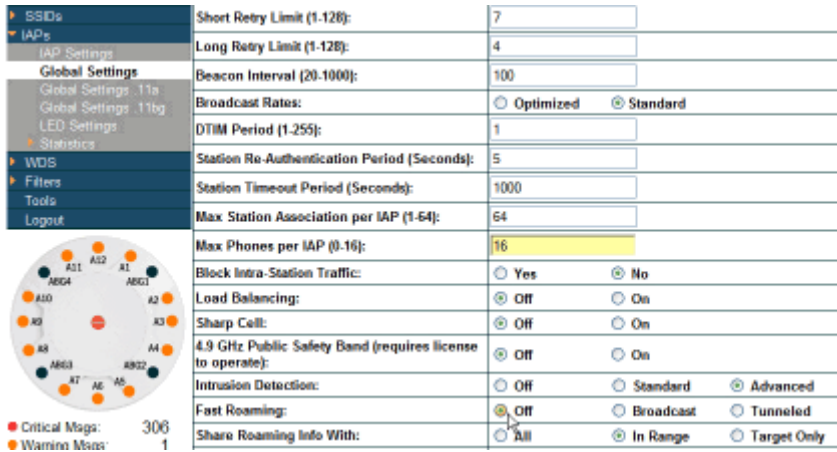


Figure 196. IAPs/Global Settings Screen

*To check if an Array is in FIPS mode:*

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

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

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

**Xirrus\_Wi-Fi\_Array(config)# fips on**

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

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

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

**Xirrus\_Wi-Fi\_Array(config)# fips off**

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

*See Also*

The Web Management Interface

The Command Line Interface

## Appendix F: Notices

This appendix contains the following information:

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

### Notices

#### Wi-Fi Alliance Certification



[www.wi-fi.org](http://www.wi-fi.org)

#### FCC Notice

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

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

determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following safety measures:

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

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

### **RF Radiation Hazard Warning**

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

### **Non-Modification Statement**

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

### **Indoor Use**

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

### **Cable Runs for Power over Gigabit Ethernet (PoGE)**

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

### **Use of RP-TNC External Antenna Connectors**

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

### **Battery Warning**

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

### **Power Cord**

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

### **Maximum Antenna Gain**

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

### **High Power Radars**

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

### **Industry Canada Notice and Marking**

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

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

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

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

## EU Directive 1999/5/EC Compliance Information

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

### Declaration of Conformity

- Cesky [Czech]** Toto zahzení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
- Dansk [Danish]** Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
- Deutsch [German]** Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
- Eesti [Estonian]** See seande vastab direktiivi 1999/5/EU oluliste nõuetele ja teistele asjakohastele sätetele.
- English** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
- Español [Spain]** Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
- Ελληνική [Greek]** Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
- Français [French]** Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.

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

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

### Assessment Criteria

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

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

### CE Marking

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





## WEEE Compliance



- Natural resources were used in the production of this equipment.
- This equipment may contain hazardous substances that could impact the health of the environment.
- In order to avoid harm to the environment and consumption of natural resources, we encourage you to use appropriate take-back systems when disposing of this equipment.
- The appropriate take-back systems will reuse or recycle most of the materials of this equipment in a way that will not harm the environment.
- The crossed-out wheeled bin symbol (in accordance with European Standard EN 50419) invites you to use those take-back systems and advises you not to combine the material with refuse destined for a land fill.
- If you need more information on collection, re-use and recycling systems, please contact your local or regional waste administration.
- Please contact Xirrus for specific information on the environmental performance of our

## National Restrictions

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

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

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

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

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

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

### Belgium

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

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

*Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez [www.bipt.be](http://www.bipt.be) pour de plus amples détails.*

### Greece

A license from EETT is required for the outdoor operation in the 5470 MHz to 5725 MHz band. Xirrus recommends checking [www.eett.gr](http://www.eett.gr) for more details.

*Η δη ιουργβάικτ ωνεξωτερικο ρουστη ζ νησυ νοτ των 5470–5725 MHz ε ιτρ ετάιωνο ετάά άάδειά της EETT, ου ορηγεβτάι στερά ά ό σ φωνη γν η του ΓΕΕΘΑ. επισσότερες λε τομ ρειεωστο [www.eett.gr](http://www.eett.gr)*

### Italy

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

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

### Norway, Switzerland and Liechtenstein

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

## Calculating the Maximum Output Power

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

## Antennas

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

## Operating Frequency

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

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

Xirrus, Inc.  
2101 Corporate Center Drive  
Thousand Oaks, CA 91320  
USA  
Tel: 1.805.262.1600  
1.800.947.7871 Toll Free in the US  
Fax: 1.866.462.3980  
[www.xirrus.com](http://www.xirrus.com)

## Safety Warnings

### Safety Warnings

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

### Explosive Device Proximity Warning

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

### Lightning Activity Warning

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

### Circuit Breaker Warning

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

Translated safety warnings appear on the following page.

## Translated Safety Warnings

### Avertissements de Sécurité

- ! **Sécurité**

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

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

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

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

## Software Warranty and License Agreement

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

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

### 1. Definitions

- 1.1 “Documentation” means the user manuals and all other all documentation, instructions or other similar materials accompanying the Software covering the installation, application, and use thereof.
- 1.2 “Licensor” means XIRRUS and its suppliers.
- 1.3 “Product” means a multi-radio access point containing four or more distinct radios capable of simultaneous operation on four or more non-overlapping channels.
- 1.4 “Software” means, collectively, each of the application and embedded software programs delivered to Customer in connection with this Agreement. For purposes of this Agreement, the term Software shall be deemed to include any and all Documentation and Updates provided with or for the Software.
- 1.5 “Updates” means any bug-fix, maintenance or version release to the Software that may be provided to Customer from Licensor pursuant to this Agreement or pursuant to any separate maintenance and support agreement entered into by and between Licensor and Customer.

## 2. Grant of Rights

- 2.1 **Software.** Subject to the terms and conditions of this Agreement, Licensor hereby grants to Customer a perpetual, non-exclusive, non-sublicenseable, non-transferable right and license to use the Software solely as installed on the Product in accordance with the accompanying Documentation and for no other purpose.
- 2.2 **Ownership.** The license granted under Sections 2.1 above with respect to the Software does not constitute a transfer or sale of Licensor's or its suppliers' ownership interest in or to the Software, which is solely licensed to Customer. The Software is protected by both national and international intellectual property laws and treaties. Except for the express licenses granted to the Software, Licensor and its suppliers retain all rights, title and interest in and to the Software, including (i) any and all trade secrets, copyrights, patents and other proprietary rights therein or thereto or (ii) any Marks (as defined in Section 2.3 below) used in connection therewith. In no event shall Customer remove, efface or otherwise obscure any Marks contained on or in the Software. All rights not expressly granted herein are reserved by Licensor.
- 2.3 **Copies.** Customer shall not make any copies of the Software but shall be permitted to make a reasonable number of copies of the related Documentation. Whenever Customer copies or reproduces all or any part of the Documentation, Customer shall reproduce all and not efface any titles, trademark symbols, copyright symbols and legends, and other proprietary markings or similar indicia of origin ("Marks") on or in the Documentation.
- 2.4 **Restrictions.** Customer shall not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) sell, rent, lease, license or sublicense, assign or otherwise transfer the Software, or any of Customer's rights and obligations under this Agreement except as expressly permitted herein; (ii) decompile, disassemble, or reverse engineer the Software, in whole or in part, provided that in those jurisdictions in which a total prohibition on any reverse engineering is prohibited as a matter of law and such prohibition is not cured by the fact that this Agreement is subject to the laws of the State of California, Licensor agrees to grant Customer, upon Customer's written request to Licensor, a limited reverse engineering license to permit interoperability of the Software with other software or code used by Customer; (iii) allow access to the Software by any user other than by Customer's employees and contractors who are bound in writing to confidentiality and non-use restrictions at least as protective as those set forth herein; (iv) except as expressly set forth herein, write or develop any derivative software or any other software program based upon the Software; or (v) use any



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

### 3. Limited Warranty and Limitation of Liability

- 3.1 **Limited Warranty & Exclusions.** Licensor warrants that the Software will perform in substantial accordance with the specifications therefor set forth in the Documentation for a period of ninety [90] days after Customer's acceptance of the terms of this Agreement with respect to the Software ("Warranty Period"). If during the Warranty Period the Software does not perform as warranted, Licensor shall, at its option, correct the relevant Software giving rise to such breach of performance or replace such Software free of charge. THE FOREGOING ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE FOREGOING WARRANTY. THE WARRANTY SET FORTH ABOVE IS MADE TO AND FOR THE BENEFIT OF CUSTOMER ONLY. The warranty will apply only if (i) the Software has been used at all times and in accordance with the instructions for use set forth in the Documentation and this Agreement; (ii) no modification, alteration or addition has been made to the Software by persons other than Licensor or Licensor's authorized representative; and (iii) the Software or Product on which the Software is installed has not been subject to any unusual electrical charge.
- 3.2 **DISCLAIMER.** EXCEPT AS EXPRESSLY STATED IN THIS SECTION 3, ALL ADDITIONAL CONDITIONS, REPRESENTATIONS, AND WARRANTIES, WHETHER IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, ACCURACY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY DISCLAIMED BY LICENSOR AND ITS SUPPLIERS. THIS DISCLAIMER SHALL APPLY EVEN IF ANY EXPRESS WARRANTY AND LIMITED REMEDY OFFERED BY LICENSOR FAILS OF ITS ESSENTIAL PURPOSE. ALL WARRANTIES PROVIDED BY LICENSOR ARE SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN THIS AGREEMENT.
- 3.3 **HAZARDOUS APPLICATIONS.** THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF A NUCLEAR FACILITY, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROLS OR OTHER

DEVICES OR SYSTEMS IN WHICH A MALFUNCTION OF THE SOFTWARE WOULD RESULT IN FORESEEABLE RISK OF INJURY OR DEATH TO THE OPERATOR OF THE DEVICE OR SYSTEM OR TO OTHERS (“HAZARDOUS APPLICATIONS”). CUSTOMER ASSUMES ANY AND ALL RISKS, INJURIES, LOSSES, CLAIMS AND ANY OTHER LIABILITIES ARISING OUT OF THE USE OF THE SOFTWARE IN ANY HAZARDOUS APPLICATIONS.

#### 3.4 Limitation of Liability.

- (a) **TOTAL LIABILITY.** NOTWITHSTANDING ANYTHING ELSE HEREIN, ALL LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMER FOR THE RELEVANT SOFTWARE, OR PORTION THEREOF, THAT GAVE RISE TO SUCH LIABILITY OR ONE HUNDRED UNITED STATES DOLLARS (US\$100), WHICHEVER IS GREATER. THE LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS SECTION SHALL BE CUMULATIVE AND NOT PER INCIDENT.
- (b) **DAMAGES.** IN NO EVENT SHALL LICENSOR, ITS SUPPLIERS OR THEIR RELEVANT SUBCONTRACTORS BE LIABLE FOR (A) ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR LOST OR DAMAGED DATA, OR ANY INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE OR (B) ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES IN EACH CASE, EVEN IF LICENSOR OR ITS SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

- 3.5 **Exclusions.** SOME JURISDICTIONS DO NOT PERMIT THE LIMITATIONS OF LIABILITY AND LIMITED WARRANTIES SET FORTH UNDER THIS AGREEMENT. IN THE EVENT YOU ARE LOCATED IN ANY SUCH JURISDICTION, THE FOREGOING LIMITATIONS SHALL APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED IN SUCH JURISDICTIONS. IN NO EVENT SHALL THE FOREGOING EXCLUSIONS AND LIMITATIONS ON DAMAGES BE DEEMED TO APPLY TO ANY LIABILITY BASED ON FRAUD, WILLFUL MISCONDUCT, GROSS NEGLIGENCE OR PERSONAL INJURY OR DEATH.

#### 4. Confidential Information

- 4.1 **Generally.** The Software (and its accompanying Documentation) constitutes Licensor's and its suppliers' proprietary and confidential information and contains valuable trade secrets of Licensor and its suppliers ("Confidential Information"). Customer shall protect the secrecy of the Confidential Information to the same extent it protects its other valuable, proprietary and confidential information of a similar nature but in no event shall Customer use less than reasonable care to maintain the secrecy of the Confidential Information. Customer shall not use the Confidential Information except to exercise its rights or perform its obligations as set forth under this Agreement. Customer shall not disclose such Confidential Information to any third party other than subject to non-use and non-disclosure obligations at least as protective of a party's right in such Confidential Information as those set forth herein.
- 4.2 **Return of Materials.** Customer agrees to (i) destroy all Confidential Information (including deleting any and all copies contained on any of Customer's Designated Hardware or the Product) within fifteen (15) days of the date of termination of this Agreement or (ii) if requested by Licensor, return, any Confidential Information to Licensor within thirty (30) days of Licensor's written request.

#### 5. Term and Termination

- 5.1 **Term.** Subject to Section 5.2 below, this Agreement will take effect on the Effective Date and will remain in force until terminated in accordance with this Agreement.
- 5.2 **Termination Events.** This Agreement may be terminated immediately upon written notice by either party under any of the following conditions:
- (a) If the other party has failed to cure a breach of any material term or condition under the Agreement within thirty (30) days after receipt of notice from the other party; or
  - (b) Either party ceases to carry on business as a going concern, either party becomes the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation, which proceeding is not dismissed within ninety (90) days, or a receiver is appointed with respect to a substantial part of its assets.

### 5.3 Effect of Termination.

- (a) Upon termination of this Agreement, in whole or in part, Customer shall pay Licensor for all amounts owed up to the effective date of termination. Termination of this Agreement shall not constitute a waiver for any amounts due.
- (b) The following Sections shall survive the termination of this Agreement for any reason: Sections 1, 2.2, 2.4, 3, 4, 5.3, and 6.
- (c) No later than thirty (30) days after the date of termination of this Agreement by Licensor, Customer shall upon Licensor's instructions either return the Software and all copies thereof; all Documentation relating thereto in its possession that is in tangible form or destroy the same (including any copies thereof contained on Customer's Designated Hardware). Customer shall furnish Licensor with a certificate signed by an executive officer of Customer verifying that the same has been done.

## 6. Miscellaneous

If Customer is a corporation, partnership or similar entity, then the license to the Software and Documentation that is granted under this Agreement is expressly conditioned upon and Customer represents and warrants to Licensor that the person accepting the terms of this Agreement is authorized to bind such entity to the terms and conditions herein. If any provision of this Agreement is held to be invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect. During the course of use of the Software, Licensor may collect information on your use thereof; you hereby authorize Licensor to use such information to improve its products and services, and to disclose the same to third parties provided it does not contain any personally identifiable information. The express waiver by either party of any provision, condition or requirement of this Agreement does not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Customer and Licensor are independent parties. Customer may not export or re-export the Software or Documentation (or other materials) without appropriate United States, European Union and foreign government licenses or in violation of the United State's Export Administration Act or foreign equivalents and Customer shall comply with all national and international laws governing the Software. This Agreement will be governed by and construed under the laws of the State of California and the United States as applied to agreements entered into and to be performed entirely within California, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer

Information Transactions Act (as promulgated by any State) to this Agreement. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of, the state and federal courts located in Ventura County, California. Customer may not assign this Agreement by operation of law or otherwise, without the prior written consent of Licensor and any attempted assignment in violation of the foregoing shall be null and void. This Agreement cancels and supersedes all prior agreements between the parties. This Agreement may not be varied except through a document agreed to and signed by both parties. Any printed terms and conditions contained in any Customer purchase order or in any Licensor acknowledgment, invoice or other documentation relating to the Software shall be deemed deleted and of no force or effect and any additional typed and/or written terms and conditions contained shall be for administrative purposes only, i.e. to identify the types and quantities of Software to be supplied, line item prices and total price, delivery schedule, and other similar ordering data, all in accordance with the provisions of this Agreement.

## Hardware Warranty Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT

BY USING THIS PRODUCT, YOU ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

LIMITED WARRANTY. Xirrus warrants that for a period of one year from the date of purchase by the original purchaser ("Customer"): (i) the Xirrus Equipment ("Equipment") will be free of defects in materials and workmanship under normal use; and (ii) the Equipment substantially conforms to its published specifications. Except for the foregoing, the Equipment is provided AS IS. This limited warranty extends only to Customer as the original purchaser. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' option, repair, replacement, or refund of the Equipment if reported (or, upon request, returned) to the party supplying the Equipment to Customer. In no event does Xirrus warrant that the Equipment is error free or that Customer will be able to operate the Equipment without problems or interruptions.

This warranty does not apply if the Equipment (a) has been altered, except by Xirrus, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Xirrus, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra-hazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL XIRRUS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE EQUIPMENT EVEN IF XIRRUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Xirrus' or its suppliers' liability to Customer,

whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer.

The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any evaluation Equipment made available for testing or demonstration purposes. All such Equipment is provided AS IS without any warranty whatsoever.

Customer agrees the Equipment and related documentation shall not be used in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or cause or permit any third party to do any of the foregoing.

All information or feedback provided by Customer to Xirrus with respect to the Product shall be Xirrus' property and deemed confidential information of Xirrus.

Equipment including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Equipment.

This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this Warranty shall remain in full force and effect. This Warranty constitutes the entire agreement between the parties with respect to the use of the Equipment.

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





---

# Glossary of Terms

## 802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

## 802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

## 802.11d

A supplement to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It allows Access Points to communicate information on the permissible radio channels with acceptable power levels for user devices. Because the 802.11 standards cannot legally operate in some countries, 802.11d adds features and restrictions to allow WLANs to operate within the rules of these countries.

## 802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

## 802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

## 802.1Q

An IEEE standard for MAC layer **frame** tagging (also known as encapsulation). Frame tagging uniquely assigns a user-defined ID to each frame. It also enables a switch to communicate **VLAN** membership information across multiple (and multi-vendor) devices by frame tagging.

## AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

**authentication**

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

**bandwidth**

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

**beacon interval**

When a device in a wireless network sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. Network administrators can adjust the beacon interval—usually measured in milliseconds (ms) or its equivalent, kilo-microseconds (Kmsec).

**bit rate**

The transmission rate of binary symbols ('0' and '1'), equal to the total number of bits transmitted in one second.

**BSS**

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

**BSSID**

The unique identifier for an access point in a [BSS](#) network. See also, [SSID](#).

**CDP**

(Cisco Discovery Protocol) CDP is a layer 2 network protocol which runs on most Cisco equipment and some other network equipment. It is used to share information with other directly connected network devices. Information such as the model, network capabilities, and IP address is shared. Wi-Fi Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors.

**cell**

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

**channel**

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11). In the 5 GHz band, 802.11a uses 8 channels for indoor use and 4 for outdoor use, none of which overlap. In the U.S., additional channels are available, to bring the total to 24 channels.

**CoS**

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

**default gateway**

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

**DHCP**

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

**DHCP lease**

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

## DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

## domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the “domain” address for Xirrus is: <http://www.xirrus.com>, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.
- **www** is a reference to the World Wide Web.
- **xirrus** refers to the company.
- **com** specifies that the domain belongs to a commercial enterprise.

## DTIM

(Delivery Traffic Indication Message) A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

## EAP

(Extensible Authentication Protocol) When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). However, LCP is somewhat inflexible because it has to specify an authentication device early in the process. EAP allows the system to gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP (for example, passwords and public keys).

## **EDCF**

(Enhanced Distributed Coordinator Function) A [QoS](#) extension which uses the same contention-based access mechanism as current devices but adds “offset contention windows” that separate high priority [packets](#) from low priority packets (by assigning a larger random backoff window to lower priorities than to higher priorities). The result is “statistical priority,” where high-priority packets usually are transmitted before low-priority packets.

## **encapsulation**

A way of wrapping protocols such as TCP/IP, AppleTalk, and NetBEUI in Ethernet frames so they can traverse an Ethernet network and be unwrapped when they reach the destination computer.

## **encryption**

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

## **Fast Ethernet**

A version of standard Ethernet that runs at 100 Mbps rather than 10 Mbps.

## **FCC**

(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

## **FIPS**

The [Federal Information Processing Standard \(FIPS\) Publication 140-2](#) establishes a computer security standard used to accredit cryptographic modules. The standard is a joint effort by the U.S. and Canadian governments.

## **frame**

A [packet](#) encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

## **Gigabit 1**

The primary Gigabit Ethernet interface. See also, [Gigabit Ethernet](#).

## Gigabit 2

The secondary Gigabit Ethernet interface. See also, [Gigabit Ethernet](#).

## Gigabit Ethernet

The newest version of Ethernet, with data transfer rates of 1 Gigabit (1,000 Mbps).

## Group

A user group, created to define a set of attributes (such as VLAN, traffic limits, and Web Page Redirect) and privileges (such as fast roaming) that apply to all users that are members of the group. This allows a uniform configuration to be easily applied to multiple user accounts. The attributes that can be configured for user groups are almost identical to those that can be configured for SSIDs.

## host name

The unique name that identifies a computer on a network. On the Internet, the host name is in the form **comp.xyz.net**. If there is only one Internet site the host name is the same as the [domain](#) name. One computer can have more than one host name if it hosts more than one Internet site (for example, **home.xyz.net** and **comp.xyz.net**). In this case, **comp** and **home** are the host names and **xyz.net** is the domain name.

## IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs.

## MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

## Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

## MTU

(Maximum Transmission Unit) The largest physical packet size—measured in bytes—that a network can transmit. Any messages larger than the MTU are divided into smaller [packets](#) before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

## NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

## packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

## PLCP

(Physical Layer Convergence Protocol) Defined by IEEE 802.6, a protocol specified within the Transmission Convergence layer that defines exactly how cells are formatted within a data stream for a particular type of transmission facility.

## PoGE

This refers to the optional Xirrus XP1 Power over Gigabit Ethernet modules that provide DC power to Arrays. Power is supplied over the same Cat 5e or Cat 6 cable that supplies the data connection to your gigabit Ethernet switch, thus eliminating the need to run a power cable. See [“Power over Gigabit Ethernet Compatibility Matrix”](#) on [page 420](#) for a list of Xirrus PoGE modules and the modules that are compatible with each Array.

### **preamble**

Preamble (sometimes called a header) is a section of data at the head of a **packet** that contains information that the access point and client devices need when sending and receiving packets. **PLCP** has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

### **private key**

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

### **PSK**

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

### **public key**

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

### **QoS**

(Quality of Service) QoS can be used to describe any number of ways in which a network provider prioritizes or guarantees a service's performance.

### **RADIUS**

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

### **RSSI**

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.



## **SDMA**

(Spatial Division Multiple Access) A wireless communications mode that optimizes the use of the radio spectrum and minimizes cost by taking advantage of the directional properties of antennas. The antennas are highly directional, allowing duplicate frequencies to be used for multiple zones.

## **SNMP**

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

## **SNTP**

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

## **SSH**

(Secure SHell) Developed by SSH Communications Security, Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. The Array only allows SSH-2 connections. SSH-2 provides strong authentication and secure communications over insecure channels. SSH-2 protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot “play back” the traffic or hijack the connection when encryption is enabled. When using SSH-2’s slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords. Be aware that your SSH utility must be set up to use SSH-2.

## **SSID**

(Service Set Identifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

**subnet mask**

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

**TKIP**

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven't been tampered with.

**transmit power**

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

**User group**

See [Group](#).

**VLAN**

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

**VLAN tagging**

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the [802.11n](#) standard, traffic can be confined to VLANs that exist on

multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

1. That the packet has a tag.
2. Whether the packet should have priority over other packets.
3. Which VLAN it belongs to, so that the switch can forward or filter it correctly.

### **WDS (Wireless Distribution System)**

WDS creates wireless backhauls between arrays. These links between arrays may be used rather than having to install data cabling to each array.

### **WEP**

(Wired Equivalent Privacy) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

### **Wi-Fi Alliance**

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

### **Wi-Fi Array**

A high capacity Wi-Fi networking device consisting of multiple radios arranged in a circular array.

### **WPA**

(Wi-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1x for authentication.

**WPA2**

(Wi-Fi Protected Access 2) WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.

**Xirrus Management System (XMS)**

A Xirrus product used for managing large Wi-Fi Array deployments from a centralized Web-based interface.

**XP-3100**

The Xirrus XP Power System (XP-3100) is a discontinued Xirrus product that provides distributed DC power to multiple XS-3900 units.

**XP1 and XP8—Power over Gigabit Ethernet modules**

See PoGE.

**XPS—Xirrus Power System**

A family of optional Xirrus products that provides power over Gigabit Ethernet. See PoGE.

# Index

## Numerics

11n

see IEEE 802.11n 59

4.9 GHz Public Safety Band 284

802.11a 7, 9, 256, 268

802.11a/b/g 48

802.11a/b/g/n 17

802.11a/n 17, 107, 240

802.11b 7, 9, 270

802.11b/g 256, 270

802.11b/g/n 17, 107, 240

802.11e 19

802.11g 7, 9, 270

802.11i 9, 112, 174

802.11n

see IEEE 802.11n 59

WMI page 274

802.11p 19

802.11q 19

802.1x 9, 70, 79, 112, 174, 406

## A

abg(n)

nomenclature 4

abg(n)2

intrusion detection 279

self-monitoring

radio assurance (loopback mode) 279

AC power 69, 81, 83, 379, 382

Access Control List 208

Access Control Lists 406

access control lists (ACLs) 222

Access Panel 379, 382, 391

access panel

reinstalling 382

removing 379

ACLs 70, 208, 406

Address Resolution Protocol

window 138

Address Resolution Protocol (ARP)

265

Admin 406

Admin ID 214

admin ID

authentication via RADIUS 215

Admin Management 214

admin RADIUS account

if using Console port 215

admin RADIUS authentication 215

administration 112, 174, 208

Administrator Account 400

Advanced Encryption Standard 70, 406

AES 9, 19, 70, 79, 112, 174, 398, 406

allow traffic

see filters 291

approved

setting rogues 148

APs 79, 148, 233, 406

rogues, blocking 278

APs, rogue

see rogue APs 277

ARP filtering 265

ARP table window 138

Array 50, 86, 94, 95, 107, 120, 174, 181

connecting 86

dismounting 95

management 299

mounting 86

powering up 107

securing 94

Web Management Interface 120

ArrayOS

upgrade 301

associated users 50

assurance (radio loopback testing) 277  
authentication 19  
    of admin via RADIUS 215  
authority  
    certificate 212, 220  
auto negotiate 181  
auto-blocking  
    rogue APs 278  
auto-configuration 112, 261, 268, 270  
    channel and cell size 277  
automatic update from remote server  
    configuration files, boot image 302

## B

backhaul  
    see WDS 76  
backup unit  
    see standby mode 277  
band association 240  
beacon interval 261  
Beacon World Mode 261  
beam distribution 17  
benefits 16  
blocking  
    rogue APs 278  
blocking rogue APs 277  
boot 301  
broadcast 266  
    fast roaming 266  
browser  
    certificate error 212, 220  
BSS 404  
BSSID 148, 404  
buttons 124

## C

capacity  
    of 802.11n 66  
cascading style sheet  
    sample for web page redirect 307

cdp 328  
CDP (Cisco Discovery Protocol)  
    settings 190  
cdp CLI command 328  
cell  
    sharp cell 277  
cell size 50, 256, 395  
    auto-configuration 277  
cell size configuration 277  
certificate  
    about 212, 220  
    authority 212, 220  
    error 212, 220  
    install Xirrus authority 220  
    X.509 212, 220  
channel  
    auto-configuration 277  
    configuration 277  
    list selection 277  
    public safety 277  
channels 50, 148, 256, 261, 268, 270,  
    395  
    factory default 282  
    factory presets 282  
    non-overlapping 18  
CHAP (Challenge-Handshake Au-  
    thentication Protocol)  
    Admin RADIUS settings 217  
    web page redirect 247  
CHAP Challenge Handshake Authen-  
    tication Protocol)  
    RADIUS ping 308  
Chassis Cover 388  
chassis cover 388  
Cisco Discovery Protocol  
    see cdp 328  
Cisco Discovery Protocol (CDP) 190  
CLI 9, 79, 83, 110, 313  
    executing from WMI 310  
    using to upgrade software image

- 415
- CLI commands
  - see commands 328
- client
  - web page redirect 306
- Command Line Interface 9, 75, 83, 107, 110, 313, 406
  - configuration commands 326
  - getting help 315
  - getting started 315
  - inputting commands 315
  - sample configuration tasks 361
  - SSH 313
  - top level commands 317
- command, utilities
  - ping, traceroute, RADIUS ping 307
- commands
  - acl 326
  - admin 327
  - cdp 328
  - clear 329
  - configure 318
  - contact-info 330
  - date-time 331
  - dhcp-server 332
  - dns 333
  - file 334
  - filter 337
  - fips 339
  - group 340
  - hostname 340
  - https 341
  - interface 342
  - license 343
  - load 343
  - location 344
  - management 344
  - more 344
  - netflow 345
  - no 346
  - pci-audit 348
  - quit 349
  - radius-server 349
  - reboot 350, 359
  - reset 350
  - run-tests 351
  - security 353
  - show 321
  - snmp 354
  - ssh 354
  - ssid 356
  - standby 356
  - statistics 324
  - syslog 357
  - telnet 359
  - vlan 360
- Community String 396
- configuration 173, 406
  - express setup 174
  - reset to factory defaults 304
- configuration changes
  - applying 126
- configuration files
  - automatic update from remote server 302
  - download 303
  - update from local file 303
  - update from remote file 303
- connection
  - tracking window 140
- Console port
  - login via 215
- Contact Information 422
- contact information 422
- coverage 50, 83
  - extended 17
- coverage patterns 9
- critical messages 123
- CTS/RTS 268, 270

**D**

- data rate 268, 270
- data rates
  - increased by 802.11n 65
- date/time restrictions
  - and interactions 252
- DC power 69, 83
- default
  - preset channels 282
- default gateway 112, 181
- default settings 393
- Default Value 397, 398
  - DHCP 397
- defaults
  - reset configuration to factory defaults 304
- Delivery Traffic Indication Message 261
- deny traffic
  - see filters 291
- deployment 48, 57, 75, 79, 83, 406
  - ease of 19
  - examples 57
  - scenarios 57
- DHCP 50, 110, 112, 174, 181, 396
  - default settings 397
  - leases window 139
- DHCP Server 192
- diagnostics
  - log, create file 304
- DIMM 386
- DIMM Memory Module 386
- DIMM module
  - replacing 386
- DNS 112, 174, 188
- DNS domain 188
- DNS server 188
- Domain Name System 188
- DTIM 261
- DTIM period 261

- duplex 181
- dynamic VLAN
  - overridden by group 251

**E**

- EAP 398, 406
- EAP-MDS 19
- EAP-PEAP 406
- EAP-TLS 19, 70, 406
- EAP-TTLS 19, 70, 406
- EDCF 261
- Encryption 398, 406
- encryption 19
- encryption method
  - recommended (WPA2 with AES) 210
  - setting 210
  - support of multiple methods 210
- encryption method (encryption mode)
  - Open, WEP, WPA, WPA2, WPA-Both 209
- encryption standard
  - AES, TKIP, both 210
  - setting 210
- End User License Agreement 81
- Enterprise 2, 7, 406
  - WLAN 7
- Enterprise Class Management 9
- Enterprise Class Security 9
- ESS 404
- ESSID 404
- Ethernet 83, 86, 94, 107, 110, 112, 174
- EULA 81
- event log
  - see system log 172
- event messages 123
- Express Setup 94, 112, 174
- express setup 112, 174
- Extended Service Set 404
- Extensible Authentication Protocol 406



external RADIUS server 802.1x 47

## F

factory default settings 393  
factory defaults 395, 396, 397, 398, 400  
    DHCP 397  
    reset configuration to 303  
factory preset  
    channels 282  
factory.conf 303  
fail-over  
    standby mode 277  
failover 67, 79  
Fan 379, 382  
FAQs 404  
Fast Ethernet 83, 110, 174, 181, 393  
fast roaming 19, 135, 266  
    about 255  
    and VLANs 255  
features 16, 75, 181, 195, 196, 261, 406  
    and license key 302  
Federal Information Processing Standard (FIPS)  
    see FIPS 429  
feedback 124  
filter list 293  
filter name 295  
filters 291, 293, 295  
    stateful filtering, disabling 293  
    statistics 170  
FIPS  
    CLI command 339  
FIPS 140-2 Security 429  
firewall 291  
    and port usage 72  
    stateful filtering, disabling 293  
FLASH 384  
FLASH memory  
    replacing 384  
FLASH Memory Module 384

fragmentation threshold 268, 270  
frequently asked questions 404  
FTP 406  
FTP server 47

## G

General Hints 403  
getting started  
    express setup 174  
Gigabit 83, 110, 112, 174, 181, 393  
global settings 261, 268, 270  
glossary of terms 459  
Group  
    management 250  
group 248  
    CLI command 340  
    VLAN overrides dynamic VLAN 251  
group limits and interactions 252  
Group Rekey 398  
guard interval  
    short, for IEEE 802.11n 64

## H

Help button 120  
help button 124  
host name 112, 120, 174, 188  
hs.css 307  
HTTPS  
    certificate, see certificate 220  
HTTPS port  
    web page redirect 245  
HyperTerminal 46, 83

## I

IAP 50, 107, 112, 174, 256, 268, 270, 285, 395  
    fast roaming 255  
    mode, Wi-Fi 255

- naming 4
- settings 256
- Wi-Fi mode 255
- IAP LED 107, 285
- IAP LED settings 285
- IAPs
  - default channels 282
- IEEE 7, 112, 174
- IEEE 802.11n
  - capacity, increased 66
  - deployment considerations 59
  - guard interval, short 64
  - improved MAC throughput 64
  - increased data rates 65
  - MIMO 60
  - multiple data streams 62
  - spatial multiplexing 62
  - WMI page 274
- IEEE 802.1Q 410
- image
  - upgrade software image 301
- implementing Voice over Wi-Fi 48, 204, 237
- installation 45, 80, 86, 375
  - installing the MCAP-3616 83
  - mounting the unit 86
  - requirements 45
  - unpacking the unit 81
  - workflow 80
- installation workflow 80
- Integrated Access Point Module 388
- integrated radio module
  - replacing 388
- interfaces 174
  - Web 119
- internal login page
  - web page redirect 246
- internal splash page
  - web page redirect 246
- Internet Explorer 46
- intrusion detection 148, 279
  - configuration 277
  - setting as approved or known 148
- IP Address 50, 112, 120, 126, 148, 174, 181, 188, 196, 199, 299, 396
- IP Subnet Mask 112
- K**
- key
  - license, setting 343
  - upgrade 302
- key features 16
- Keyboard Shortcuts 400
- keyboard shortcuts 400
- known
  - setting rogues 148
- L**
- lastboot.conf 303
- Layer 3
  - fast roaming 255
- lease 396
- Lease Time 396
- leases, DHCP
  - viewing 139
- LEDs 107
  - sequence 107
  - settings 285
- license Key
  - upgrading 302
- license key
  - setting 343
- limits
  - group 252
  - interactions 252
  - station 252
  - traffic 252
- list, access control
  - see access control list 222
- list, MAC access

- see access control list 222
- location information 112, 120, 174
- log
  - diagnostics, create file 304
- log messages
  - counters 124
- log, system (event)
  - viewing window 172
- logging in 110, 126
- Login 126
- login
  - via Console port 215
- login page
  - web page redirect 246, 306
- logout 312
- long retry limit 261
- loopback
  - see radio assurance 373
- loopback testing
  - radio assurance mode 277

## M

- MAC 70, 110, 404, 406
- MAC Access Control Lists 70
- MAC Access List 222
- MAC address 222, 404, 406
- MAC throughput
  - improved by IEEE 802.11n 64
- Main System Memory 386
- Management 400, 406
- management
  - of Arrays 299
  - Web Management Interface (WMI) 119
- maximum lease 396
- Maximum Lease Time 396
- Megabit 112
- Message Integrity Check 406
- messages
  - syslog counters 124

- MIC 19, 406
- MIMO (Multiple-In Multiple-Out) 60
- mode, Wi-Fi 255
- monitoring
  - intrusion detection 148
  - see intrusion detection 279
- mounting 86
- mounting plate 86, 94, 95
- mounting the unit 86
- MTU 181
  - size 181
- multiple data streams 62

## N

- NAT
  - table - see connection tracking 140
- Netflow 195
- netflow
  - CLI command 345
- Netscape Navigator 45, 46
- network
  - interfaces 180
  - settings 181
- network connections 83, 126, 406
- network installation 45, 375
- network interface ports 110
- network interfaces 181, 393
- network status
  - ARP table window 138
  - connection
    - tracking window 140
  - routing table window 138
  - viewing leases 139
- Network Time Protocol 112, 174, 193
- nomenclature 4
- non-overlapping channels 18
- NTP 112, 174, 193, 396
- NTP Server 193

**O**

Open (encryption method) 209  
optimization, VLAN 266  
overview 9

**P**

PAP (Password Authentication Protocol)  
Admin RADIUS settings 216  
RADIUS ping 308  
web page redirect 247  
passphrase 70, 112, 174  
Password 400, 406  
password 126  
Payment Card Industry Data Security  
Standard  
see PCI DSS 423  
PCI DSS 423  
CLI command 348  
pci-audit  
CLI command 348  
PDF 81  
PEAP 19, 289  
performance 16  
Ping 299  
ping 307  
planning 67, 69, 70, 75  
failover 67  
network management 75  
port failover 67  
power 69  
security 70  
switch failover 67  
WDS 76  
PoGE 45  
see Power over Gigabit Ethernet 13  
port failover 67  
port requirements 72  
power cord 379  
power outlet 45

Power over Gigabit Ethernet 3, 21, 27,  
35, 40, 45, 69, 84  
compatibility with Array models  
420  
Power over Gigabit Ethernet (PoGE) 13  
power planning 69  
Power Supply 379, 382, 391  
power supply  
replacing 391  
power switch 379  
pre-shared key 70, 79, 406  
Print button 120  
print button 124  
probe  
see Netflow 195  
product installation 45, 375  
product overview 9  
product specifications 20, 27, 34, 39  
PSK 79, 398  
public safety band 284  
public safety channels 277  
PuTTY 45, 75, 112, 174, 406  
PuTTY 46

**Q**

QoS 19, 240, 397, 404, 466  
conflicting values 239  
levels defined 241, 251  
priority 240  
SSID 236, 241  
about setting QoS 405  
default QoS 397  
user group 251  
Quality of Service 19  
see QoS 241, 251  
Quick Install Guide 81  
quick reference guide 393  
quick start  
express setup 174

**R**

## radio

- assurance (self-test) 279

- radio assurance (loopback testing) 277

- radio assurance (loopback) mode 279

- radio distribution 16

## radios

- default channels 282

- naming 4

- RADIUS 9, 45, 70, 79, 208, 222, 396, 406

- admin authentication 215

- RADIUS ping

- CHAP Challenge Handshake Authentication Protocol) 308

- PAP (Password Authentication Protocol) 308

- RADIUS Ping command 308

- RADIUS Server 396

- RADIUS server 47

- RADIUS settings

- web page redirect 247

- README file 81

- reauthentication 261

- reboot 301

- redirect (WPR) 306

- registration card 81

- remote boot image

- automatic update from remote TFTP server 302

- remote configuration

- automatic update from remote server 302

- remote TFTP server

- automatic update of boot image, configuration 302

- Reset 299, 396

- reset configuration

- to factory defaults 304

- restrictions

- date/time 252

- stations 252

- traffic 252

## RF

- intrusion detection 277

- spectrum management 277

- RF configuration 277

- RF management

- see channel 277

- RF resilience 277

- roaming 19, 135, 266

- see fast roaming 255

- Rogue AP 9, 75, 148, 233, 406

- rogue AP

- blocking 278

- Rogue AP List 148

- rogue APs

- blocking 277

- Rogue Control List 233

- rogue detection 17

- rogues

- setting as known or approved 148

- root command prompt 317

- route

- trace route utility 307

- routing table window 138

- RSSI 148

- RTS 268, 270

- RTS threshold 268, 270

**S**

- sample Perl and CSS files for 306

- save

- with reboot 301

- Save button 120

- saved.conf 303

- scalability 7

- schedule

- auto channel configuration 277

- Secondary Port 396

- Secondary Server 396
- secret 396
- Secure Shell 46
- secure Shell 45
- Security
  - FIPS 429
  - PCI DSS 423
- security 9, 19, 208, 404, 406
  - certificate, see certificate 220
- see group 248
- self-monitoring 279
  - radio assurance 373
  - radio assurance options 279
- self-test
  - radio assurance mode 279
- serial port 46, 110, 406
- server, VTun
  - see VTun 207
- Service Set Identifier 112
- Services 192, 379, 382, 404
- servicing 377
- servicing the unit 375
- settings 174
- setup, express 174
- sharp cell 277
  - setting in WMI 281
- short retry limit 261
- signal processing
  - MIMO 61
- SNMP 9, 14, 112, 174, 181, 192, 199, 396
  - required for XMS 199, 200
- software
  - upgrade license key 302
- software image
  - upgrading via CLI 415
- Software Upgrade 299
- software upgrade 301
- spatial multiplexing 62
- specifications 20, 27, 34, 39
- spectrum (RF) management 277
- speed 7, 110, 181
  - 11 Mbps 7
  - 54 Mbps 7
- splash page
  - web page redirect 246, 306
- SSH 45, 46, 75, 112, 174, 181, 209, 400, 406
- SSH-2 209
- SSID 9, 112, 120, 148, 174, 233, 240, 397, 404, 410
  - about usage 405
  - QoS 236, 241
    - about using 405
  - QoS, about usage 405
  - web page redirect settings 244
  - web page redirect settings, about 245
- SSID Management 240, 397, 404
- standby mode 277
- stateful filtering
  - disabling 293
- static IP 112, 174, 181
- station timeout period 261
- Stations 404
- stations
  - limits and interactions 252
  - rogues 148
  - statistics 170
  - statistics per station 171
- statistics 174
  - filters 170
  - netflow 195
  - per-station 171
  - stations 170
  - WDS 169
- status bar 120, 124
- submitting comments 124
- subnet 45, 67, 112, 181
- switch failover 67

synchronize 112, 174, 193  
 Syslog 112, 120, 174, 192, 196, 396  
     time-stamping 112  
 syslog messages  
     counters 124  
 Syslog reporting 196  
 Syslog Server 196  
 system commands  
     ping, trace route, RADIUS ping 307  
 System Configuration Reset 299  
 System Log 196  
 system log  
     viewing window 172  
 system memory  
     replacing 386  
 System Reboot 299  
 System Tools 299  
 system tools 300

**T**

T-bar 86  
 T-bar clips 86  
 TCP  
     port requirements 72  
 technical support  
     contact information 422  
     frequently asked questions 404  
 Telnet 209, 400, 406  
 Temporal Key Integrity Protocol 406  
 TFTP server  
     automatic update of boot image, configuration 302  
 Time Out 396  
 time zone 112, 174, 193  
 timeout 261, 299  
 Tips 403  
 TKIP 19, 70, 79, 112, 174, 398, 406  
 tool  
     ping, trace route, RADIUS ping

    307  
 Tools 299, 406  
 tools, system 300  
 trace route utility 307  
 traffic  
     filtering 291  
     limits and interactions 252  
 transmit power 50, 395  
 Trap Host 396  
 trap port 199, 396  
 tunneled  
     fast roaming 266  
 tunnels  
     see VTun 204, 207

**U**

UDP  
     port requirements 72  
 Unit 86  
     attaching 86  
     mounting 86  
 unknown  
     setting rogues 148  
 unpacking the unit 81  
 upgrade  
     license key 302  
     software image 301  
 upgrading software image  
     via CLI 415  
 UPS 45, 79  
 user group 248  
     QoS 251  
 user group limits and interactions 252  
 user interface 119  
 utilities  
     ping, trace route, RADIUS ping 307  
 utility buttons 124

**V**

- virtual tunnels
  - see VTun 207
- VLAN 9, 79, 240, 397, 404, 410
  - broadcast optimization 266
  - dynamic
    - overridden by group 251
    - group (vs. dynamic VLAN) 251
- VLAN ID 240
- VLANs 204
  - and fast roaming 255
- voice
  - fast roaming 255
  - implementing on Array 48, 204, 237
- Voice-over IP 270
- VoIP 270
- VoWLAN 19
- VPN 112, 174, 406
- VTS
  - Virtual Tunnel Server 204, 207
- VTun
  - specifying tunnel server 204, 207
  - understanding 204

**W**

- wall thickness considerations 48
- warning messages 123
- WDS 287, 289
  - about 76
  - planning 76
  - statistics 169
- WDS Client Links 289
- Web interface
  - structure and navigation 123
- web interface 119
- Web Management Interface 75, 94, 107, 110, 126, 404
- Web Management Interface (WMI) 119
- web page redirect 306

- also called WPR 306
- CHAP (Challenge-Handshake Authentication Protocol) 247
- HTTPS port 245
- install files for 306
- internal login page 246
- internal splash page 246
- PAP, CHAP 247
- RADIUS settings 247
- remove files for 307
- sample WPR files 307
- SSID settings 244
- SSID settings, about 245
- WEP 19, 70, 112, 174, 208, 240, 398, 406
- WEP (Wired Equivalent Privacy)
  - encryption method 210
- Wi-Fi mode 255
- Wi-Fi Protected Access 9, 70, 112, 174, 406
- Wired Equivalent Privacy 112, 406
- Wireless Distribution System 287
- wireless LAN 7
- wireless security 174
- WLAN 174
- WMI 9, 75, 79, 110, 119, 256
  - certificate error 212, 220
  - executing CLI commands 310
- workflow 80
- WPA 9, 79, 112, 174, 208, 240, 398, 406
- WPA (Wi-Fi Protected Access) and WPA2
  - encryption method 210
- WPA2 9
- WPR
  - see web page redirect 306
- wpr.pl 306, 307

**X**

- X.509



- certificate 212, 220
- Xirrus
  - certificate authority 220
- Xirrus Management System 9, 14, 19, 47
  - SNMP required 199, 200
- Xirrus Power over Gigabit Ethernet 45
- Xirrus Remote DC Power System 2, 45, 83
- Xirrus Roaming Protocol 19, 135, 266
- Xirrus Wireless Management System 2, 45, 75, 406
- XM-3300 2, 9, 45, 75, 79, 199, 406
- XMS 9, 14, 19, 47
  - port requirements 72
  - setting IP address of 199
  - SNMP required 199, 200
- XN Arrays
  - see also IEEE 802.11n 59
- XN16
  - management 299
- XP1, XP8
  - see Power over Gigabit Ethernet 13
- XP-3100 2, 45, 79, 83
- XPS 45
- XRP 19, 135, 266
- xs\_current.conf 303
- xs\_diagnostic.log 305
- XS16
  - management 127, 173, 299
- XS-3500 2, 9
- XS-3700 2, 9
- XS-3900 2, 9, 50, 70, 240, 261, 388, 404, 406, 410
  - management 127, 173, 299





# User's Guide



## Wi-Fi Arrays