

USER'S GUIDE

Wireless Arrays

DRAFT5

XR Series
May 5, 2012
Release 6.1



Wireless Array™

XR Series

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

Part Number: 800-0022-001
(Revision D)



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 C: Notices” on page 431.

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

Table of Contents

List of Figures.....	xi
Introduction	1
The Xirrus Family of Products	1
Nomenclature	3
Why Choose the Xirrus Wireless Array?	3
Wireless Array Product Overview	5
XR Wireless Array Product Family	6
XR-1000 and XR-2000 Series Arrays	6
XR-4000 Series Arrays	7
XR-6000 Series Arrays	8
Enterprise Class Security	9
Deployment Flexibility	9
Power over Gigabit Ethernet (PoGE)	10
Enterprise Class Management	10
Key Features and Benefits	12
High Capacity and High Performance	12
Extended Coverage	12
Non-Overlapping Channels	13
SDMA Optimization	13
Fast Roaming	13
Easy Deployment	13
Secure Wireless Access	13
Applications Enablement	14
Advanced Feature Sets	14
Xirrus Advanced RF Performance Manager (RPM)	14
Xirrus Advanced RF Security Manager (RSM)	15
Xirrus Advanced RF Analysis Manager (RAM)	16
About this User's Guide	17
Organization	17
Notes and Cautions	19
Screen Images	19
Your User's Guide as a PDF Document	19

Hyperlinks	19
Product Specifications—XR Array Family	20
Installing the Wireless Array	21
Installation Prerequisites	21
Optional Network Components	23
Client Requirements	23
Planning Your Installation	24
General Deployment Considerations	24
Coverage and Capacity Planning	26
Placement	26
RF Patterns	27
Capacity and Cell Sizes	28
Fine Tuning Cell Sizes	29
Roaming Considerations	30
Allocating Channels	30
Deployment Examples	33
IEEE 802.11n Deployment Considerations	35
MIMO (Multiple-In Multiple-Out)	36
Multiple Data Streams—Spatial Multiplexing	37
Channel Bonding	38
Improved MAC Throughput	39
Short Guard Interval	39
Obtaining Higher Data Rates	40
802.11n Capacity	41
Failover Planning	41
Switch Failover Protection	43
Power Planning	44
Power over Gigabit Ethernet	44
Security Planning	45
Wireless Encryption	45
Authentication	45
Port Requirements	47
Network Management Planning	51
WDS Planning	52
Common Deployment Options	55
Installation Workflow	56

Installing Your Wireless Array	58
Choosing a Location	58
Wiring Considerations	58
Mounting the Array	61
Dismounting the Array	61
Powering Up the Wireless Array	62
Array LED Operating Sequences	63
LED Boot Sequence	63
LED Operation when Array is Running	64
Establishing Communication with the Array	65
Using the Serial Port	66
Using the Ethernet Ports	66
Starting the WMI	67
Logging In	67
Entering the License	67
Performing the Express Setup Procedure	69
Procedure for Performing an Express Setup	70
Securing Low Level Access to the Array	76
The Web Management Interface	79
An Overview	80
Structure of the WMI	81
User Interface	83
Utility Buttons	85
Logging In	87
Applying Configuration Changes	87
Character Restrictions	88
Viewing Status on the Wireless Array	89
Array Status Windows	90
Array Summary	90
Content of the Array Summary Window	91
Array Information	95
Array Configuration	96
Admin History	97
Network Status Windows	97
Network	98

Network Map	99
Content of the Network Map Window	99
Spanning Tree Status	102
Routing Table	103
ARP Table	103
DHCP Leases	104
Connection Tracking/NAT	104
CDP Neighbors	105
Network Assurance	106
RF Monitor Windows	107
IAPs	108
Spectrum Analyzer	109
Intrusion Detection	112
Channel History	114
Radio Assurance	116
Station Status Windows	118
Stations	119
Location Map	120
RSSI	125
Signal-to-Noise Ratio (SNR)	127
Noise Floor	129
Max by IAP	131
Station Assurance	132
Statistics Windows	134
IAP Statistics Summary	134
Per-IAP Statistics	135
Network Statistics	137
VLAN Statistics	138
WDS Statistics	139
Filter Statistics	140
Station Statistics	140
Per-Station Statistics	141
System Log Window	142
IDS Event Log Window	143
Configuring the Wireless Array.....	147
Express Setup	149

Network	156
Network Interfaces	157
Network Interface Ports	158
Network Bonds	160
DNS Settings	167
CDP Settings	168
Services	170
Time Settings (NTP)	171
NetFlow	173
Wi-Fi Tag	175
System Log	176
SNMP	179
DHCP Server	182
VLANs	185
Understanding Virtual Tunnels	185
VLAN Management	187
Security	190
Understanding Security	191
Certificates and Connecting Securely to the WMI	194
Using the Array's Default Certificate	194
Using an External Certificate Authority	195
Admin Management	196
Admin Privileges	198
Admin RADIUS	200
About Creating Admin Accounts on the RADIUS Server	200
Management Control	203
Access Control List	209
Global Settings	212
External Radius	216
About Creating User Accounts on the RADIUS Server	216
Internal Radius	219
Rogue Control List	222
SSIDs	224
Understanding SSIDs	225
Understanding QoS Priority on the Wireless Array	226
SSID Management	231
SSID List (top of page)	232

SSID Limits	236
Web Page Redirect Configuration Settings	237
WPA Configuration Settings	241
RADIUS Configuration Settings	242
Active IAPs	243
Per-SSID Access Control List	244
Groups	246
Understanding Groups	246
Using Groups	247
Group Management	248
Group Limits	250
IAPs	253
Understanding Fast Roaming	255
IAP Settings	256
Global Settings (IAP)	261
Beacon Configuration	263
Station Management	263
Advanced Traffic Optimization	264
Global Settings .11an	270
Global Settings .11bgn	274
Global Settings .11n	279
Advanced RF Settings	282
About Standby Mode	282
RF Monitor	283
RF Resilience	284
RF Power & Sensitivity	285
RF Spectrum Management	287
Station Assurance	288
Intrusion Detection	291
DoS Attacks	292
Impersonation Attacks	293
About Blocking Rogue APs	294
RF Intrusion Detection and Auto Block Mode	294
DoS Attack Detection Settings	295
Impersonation Detection Settings	296
LED Settings	297
DSCP Mappings	298

Roaming Assist	299
WDS	302
About Configuring WDS Links	302
Long Distance Links	303
WDS Client Links	304
Filters	308
Filter Lists	309
Filter Management	311
Clusters	314
Cluster Definition	315
Cluster Management	316
Cluster Operation	317
Using Tools on the Wireless Array.....	319
System Tools	320
About Licensing and Upgrades	321
System	322
Automatic Updates from Remote Image or Configuration File	323
Configuration	324
Diagnostics	326
Web Page Redirect	328
Network Tools	329
Progress and Status Frames	331
CLI	332
Options	333
Logout	336
The Command Line Interface	337
Establishing a Secure Shell (SSH) Connection	337
Getting Started with the CLI	339
Inputting Commands	339
Getting Help	339
Top Level Commands	341
Root Command Prompt	341
configure Commands	342
show Commands	345
statistics Commands	348

Configuration Commands	350
acl	350
admin	351
cdp	352
clear	353
cluster	354
contact-info	355
date-time	356
dhcp-server	357
dns	358
file	359
filter	362
Air Cleaner	363
group	366
hostname	366
interface	367
load	367
location	368
management	368
more	370
netflow	371
no	372
quit	374
radius-server	374
reboot	375
reset	375
restore	376
run-tests	377
security	379
snmp	380
ssid	381
syslog	382
uptime	383
vlan	384
wifi-tag	385
Sample Configuration Tasks	386
Configuring a Simple Open Global SSID	387

Configuring a Global SSID using WPA-PEAP	388
Configuring an SSID-Specific SSID using WPA-PEAP	389
Enabling Global IAPs	390
Disabling Global IAPs	391
Enabling a Specific IAP	392
Disabling a Specific IAP	393
Setting Cell Size Auto-Configuration for All IAPs	394
Setting the Cell Size for All IAPs	395
Setting the Cell Size for a Specific IAP	396
Configuring VLANs on an Open SSID	397
Configuring Radio Assurance Mode (Loopback Tests)	398
Appendices	401
Appendix A: Quick Reference Guide	403
Factory Default Settings	403
Host Name	403
Network Interfaces	403
Serial	403
Gigabit 1 and Gigabit 2	404
Server Settings	404
NTP	404
Syslog	404
SNMP	405
DHCP	405
Default SSID	406
Security	406
Global Settings - Encryption	406
External RADIUS (Global)	407
Internal RADIUS	408
Administrator Account and Password	408
Management	408
Keyboard Shortcuts	409
Appendix B: Technical Support	411
General Hints and Tips	411
Frequently Asked Questions	412
Multiple SSIDs	412

Security	414
VLAN Support	417
Array Monitor and Radio Assurance Capabilities	420
Enabling Monitoring on the Array	420
How Monitoring Works	420
Radio Assurance	421
Radio Assurance Options	422
RADIUS Vendor Specific Attribute (VSA) for Xirrus	423
Upgrading the Array via CLI	424
Sample Output for the Upgrade Procedure:	425
Contact Information	429
Appendix C: Notices	431
Notices	431
EU Directive 1999/5/EC Compliance Information	435
Compliance Information (Non-EU)	442
Safety Warnings	443
Translated Safety Warnings	444
Software License and Product Warranty Agreement	445
Hardware Warranty Agreement	451
Glossary of Terms.....	453
Index.....	465

List of Figures

Figure 1.	Xirrus Arrays: XR Series	1
Figure 2.	The Xirrus Management System	2
Figure 3.	Wireless Array (XR Series)	5
Figure 4.	Wireless Coverage Patterns	9
Figure 5.	WMI: Array Status	11
Figure 6.	Layout of IAPs (XR-7630)	12
Figure 7.	Wall Thickness Considerations	25
Figure 8.	Unit Placement	26
Figure 9.	Full (Normal) Coverage	27
Figure 10.	Adjusting RF Patterns	27
Figure 11.	Custom Coverage	28
Figure 12.	Connection Rate vs. Distance	28
Figure 13.	Transmit Power	29
Figure 14.	Overlapping Cells	30
Figure 15.	Allocating Channels Manually	32
Figure 16.	Deployment Scenario (54 Mbps)—Per Sector	33
Figure 17.	Deployment Scenario (36 Mbps)—Per Sector	33
Figure 18.	Deployment Scenario (18 Mbps)—Per Sector	34
Figure 19.	Classic 802.11 Signal Transmission	36
Figure 20.	MIMO Signal Processing	36
Figure 21.	Spatial Multiplexing	37
Figure 22.	Channel Bonding	38
Figure 23.	MAC Throughput Improvements	39
Figure 24.	Computing 802.11n Data Rates	40
Figure 25.	Port Failover Protection	41
Figure 26.	Switch Failover Protection	43
Figure 27.	Port Requirements for XMS	47
Figure 28.	WDS Link	52
Figure 29.	A Multiple Hop WDS Connection	53
Figure 30.	WDS Failover Protection	53
Figure 31.	Installation Workflow	56
Figure 32.	Array Placement	58
Figure 33.	LED Locations	62
Figure 34.	Network Interface Ports—XR-1000 Series	65

Figure 35.	Network Interface Ports—XR-2000 Series ??OK??	65
Figure 36.	Network Interface Ports—XR-4000 Series	65
Figure 37.	Network Interface Ports—XR-6000 Series	66
Figure 38.	Express Setup	69
Figure 39.	Web Management Interface	80
Figure 40.	WMI: Frames	83
Figure 41.	Major Menu Sections Collapsed (on left).....	84
Figure 42.	WMI: Utility Buttons.....	85
Figure 43.	Feedback Form.....	86
Figure 44.	Logging In to the Wireless Array	87
Figure 45.	Array Summary	90
Figure 46.	Disabled IAP (Partial View).....	93
Figure 47.	IAP Cells	94
Figure 48.	Array Information	95
Figure 49.	Show Configuration	96
Figure 50.	Admin Login History.....	97
Figure 51.	Network Settings	98
Figure 52.	Network Map	99
Figure 53.	Spanning Tree Status.....	102
Figure 54.	Routing Table	103
Figure 55.	ARP Table	103
Figure 56.	DHCP Leases.....	104
Figure 57.	Connection Tracking	104
Figure 58.	CDP Neighbors	105
Figure 59.	Network Assurance.....	106
Figure 60.	RF Monitor—IAPs	108
Figure 61.	RF Monitor—IAPs	108
Figure 62.	RF Spectrum Analyzer	110
Figure 63.	Intrusion Detection/Rogue AP List.....	112
Figure 64.	RF Monitor—Channel History.....	114
Figure 65.	RF Monitor—Channel History (Rotated)	115
Figure 66.	RF Monitor—Channel History (Text)	115
Figure 67.	Radio Assurance	116
Figure 68.	Stations.....	119
Figure 69.	Location Map.....	120
Figure 70.	Controls for Location Map	122
Figure 71.	Minimizing stations.....	123

Figure 72.	Station RSSI Values	125
Figure 73.	Station RSSI Values—Colorized Graphical View	126
Figure 74.	Station Signal-to-Noise Ratio Values	127
Figure 75.	Station SNR Values—Colorized Graphical View.....	128
Figure 76.	Station Noise Floor Values	129
Figure 77.	Station Noise Floor Values—Colorized Graphical View	130
Figure 78.	Max by IAP	131
Figure 79.	Station Assurance	132
Figure 80.	IAP Statistics Summary Page.....	135
Figure 81.	Individual IAP Statistics Page	136
Figure 82.	Network Statistics.....	137
Figure 83.	VLAN Statistics.....	138
Figure 84.	WDS Statistics	139
Figure 85.	Filter Statistics	140
Figure 86.	Station Statistics	140
Figure 87.	Individual Station Statistics Page.....	141
Figure 88.	System Log (Alert Level Highlighted)	142
Figure 89.	IDS Event Log	143
Figure 90.	WMI: Express Setup	149
Figure 91.	Network Interfaces	156
Figure 92.	Network Settings	157
Figure 93.	Network Interface Ports.....	158
Figure 94.	Network Bonds	161
Figure 95.	Port Modes (a, b).....	162
Figure 96.	Port Modes (c)	163
Figure 97.	Port Modes (d)	164
Figure 98.	Mirroring Traffic.....	166
Figure 99.	DNS Settings.....	167
Figure 100.	CDP Settings.....	168
Figure 101.	Services.....	170
Figure 102.	Time Settings (Manual Time).....	171
Figure 103.	Time Settings (NTP Time Enabled).....	172
Figure 104.	NetFlow.....	174
Figure 105.	Wi-Fi Tag.....	175
Figure 106.	System Log	176
Figure 107.	SNMP	179
Figure 108.	DHCP Management.....	182

Figure 109. VLANs.....	185
Figure 110. VLAN Management.....	187
Figure 111. Security.....	190
Figure 112. Import Xirrus Certificate Authority.....	194
Figure 113. Admin Management.....	196
Figure 114. Admin Privileges.....	198
Figure 115. Admin RADIUS.....	201
Figure 116. Management Control.....	203
Figure 117. Pre-login Banner.....	204
Figure 118. Access Control List.....	210
Figure 119. Global Settings (Security).....	212
Figure 120. External RADIUS Server.....	216
Figure 121. Internal RADIUS Server.....	219
Figure 122. Rogue Control List.....	222
Figure 123. SSIDs.....	224
Figure 124. Four Traffic Classes.....	226
Figure 125. Priority Level—IEEE 802.1p (Layer 2).....	227
Figure 126. Priority Level—DSCP (DiffServ - Layer 3).....	227
Figure 127. SSID Management.....	231
Figure 128. SSID Management.....	235
Figure 129. WPR Internal Splash Page Fields (SSID Management).....	238
Figure 130. Customizing an Internal Login or Splash Page.....	241
Figure 131. Setting Active IAPs per SSID.....	243
Figure 132. Per-SSID Access Control List.....	244
Figure 133. Groups.....	246
Figure 134. Group Management.....	248
Figure 135. IAPs.....	253
Figure 136. Source of Channel Setting.....	254
Figure 137. IAP Settings.....	256
Figure 138. Global Settings (IAPs).....	261
Figure 139. Global Settings .11an.....	270
Figure 140. Global Settings .11bgn.....	274
Figure 141. Global Settings .11n.....	279
Figure 142. Advanced RF Settings.....	282
Figure 143. Station Assurance (Advanced RF Settings).....	289
Figure 144. Intrusion Detection Settings.....	291
Figure 145. LED Settings.....	297

Figure 146. DSCP Mappings.....	298
Figure 147. Roaming Assist	300
Figure 148. WDS.....	302
Figure 149. .Configuring a WDS Link.....	303
Figure 150. WDS Client Links	304
Figure 151. Filters	308
Figure 152. Filter Lists	309
Figure 153. Filter Management	311
Figure 154. Clusters	314
Figure 155. Cluster Definition	315
Figure 156. Cluster Management.....	316
Figure 157. Cluster Mode Operation.....	317
Figure 158. Cluster Mode Activation	317
Figure 159. Viewing Statistics in Cluster Mode.....	318
Figure 160. System Tools.....	320
Figure 161. Saving the Diagnostic Log.....	327
Figure 162. Managing WPR Splash/Login page files.....	328
Figure 163. System Command (Ping).....	329
Figure 164. Radius Ping Command.....	329
Figure 165. Radius Ping Output.....	330
Figure 166. CLI Window	332
Figure 167. WMI Display Options	333
Figure 168. iPhone Style Option.....	334
Figure 169. Login Window	336
Figure 170. Logging In.....	338
Figure 171. Help Window.....	339
Figure 172. Full Help	340
Figure 173. Partial Help.....	340
Figure 174. Air Cleaner Filter Rules	364
Figure 175. Configuring a Simple Open Global SSID.....	387
Figure 176. Configuring a Global SSID using WPA-PEAP	388
Figure 177. Configuring an SSID-Specific SSID using WPA-PEAP	389
Figure 178. Enabling Global IAPs.....	390
Figure 179. Disabling Global IAPs.....	391
Figure 180. Enabling a Specific IAP.....	392
Figure 181. Disabling a Specific IAP.....	393
Figure 182. Setting the Cell Size for All IAPs.....	394

Figure 183. Setting the Cell Size for All IAPs.....	395
Figure 184. Setting the Cell Size for a Specific IAP	396
Figure 185. Configuring VLANs on an Open SSID.....	397
Figure 186. Configuring Radio Assurance Mode (Loopback Testing)	399

Introduction

These topics introduce the Xirrus Wireless Array, including an overview of its key features and benefits.

- “The Xirrus Family of Products” on page 1.
- “Why Choose the Xirrus Wireless Array?” on page 3.
- “Wireless Array Product Overview” on page 5.
- “Key Features and Benefits” on page 12.
- “Advanced Feature Sets” on page 14.
- “About this User’s Guide” on page 17.

The Xirrus Family of Products



Figure 1. Xirrus Arrays: XR Series

The Xirrus family of products includes the following:

- **The XR Series of Xirrus Wireless Arrays**
The newest Xirrus Wireless Arrays have been completely redesigned to provide distributed intelligence, integrated switching capacity of up to 10 Gbps, increased bandwidth, and smaller size. The radios support IEEE802.11 a, b, g, and n clients, and feature the capacity and performance needed to replace switched Ethernet to the desktop. Modular radios allow you to increase the number of radios, upgrade to more powerful radios, or even upgrade later to future technologies like 802.11ac and 802.11.ad as they are introduced.

- **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 Management Appliance series, or as a software package to be installed on your own server hardware (optionally under VMware).

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 Wireless Arrays via SNMP.

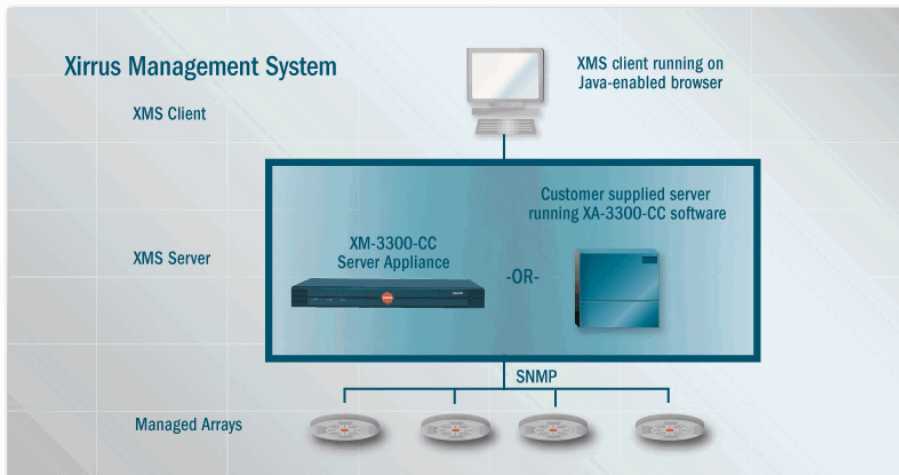


Figure 2. The Xirrus Management System

If you need detailed information about this product, refer to the *XMS User's Guide*.

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

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

Nomenclature

Throughout this User's Guide, the Xirrus Wireless 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, XR-4830). The Wireless Array's operating system is referred to as the **ArrayOS**. The Web Management Interface for browser-based management of the Array is referred to as **WMI**.

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

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

Why Choose the Xirrus Wireless Array?

The deployment of wireless is a necessity as businesses strive for greater flexibility in the workplace and the need for employee mobility rises. The user community is placing spiraling and often unanticipated demands on the wireless network, with the rapid proliferation of devices such as iPads and wireless enabled phones. Xirrus Wireless Arrays have the capability to support the large number of user devices present in today's environments, with superior range and coverage. Wireless is compatible with standard Ethernet protocols, so connectivity with existing wired infrastructure is transparent to users—they can still access and use the same applications and network services that they use when plugged into the company's wired LAN (it's only the plug that no longer exists).

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

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

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

See Also

[Key Features and Benefits](#)

[Wireless Array Product Overview](#)

[The Xirrus Family of Products](#)

Wireless Array Product Overview

Part of the family of Xirrus products, the Wireless Array is a high capacity, multi-mode device designed with four times the coverage and eight times the bandwidth and user density compared with legacy thin access point wireless products. Its distributed intelligence eliminates the use of separate controllers and their accompanying bottlenecks. Each radio, with its directional high-gain antennas, can achieve 450 Mbps throughput.



Figure 3. Wireless Array (XR Series)

The Wireless Array (regardless of the product model) is Wi-Fi® compliant and simultaneously supports 802.11a, 802.11b, 802.11g, and 802.11n clients. The multi-state design allows you to assign radios to 2.4 GHz and 5 GHz bands (or both) in any desired arrangement. Integrated switching and active enterprise class features such as **VLAN** support and multiple **SSID** capability enable robust network compatibility and a high level of scalability and system control. The optional Xirrus Management System (XMS) allows global management of hundreds of Arrays from a central location.

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

XR Wireless Array Product Family

XR-1000 and XR-2000 Series Arrays

xxx Shelly - check pagination before final. These Arrays include models with one Gigabit Ethernet port and two or four multi-state radios (2.4GHz or 5GHz) that can support 300Mbps or 450Mbps, connecting upwards of 320 users at one time.

The Xirrus XR-1000 Series Wireless Array is a two slot chassis available in a two multi-state (2.4GHz or 5GHz) radio configuration supporting up to 160 users with up to 900Mbps of bandwidth (up to 450 Mbps per radio). The XR-1000 provides flexibility for delivering wireless service in low user density scenarios, challenging deployments in areas with high RF attenuation, and in isolated or physically separated locations. The elliptical-shaped coverage pattern produced by its directional antennas is ideal for covering facilities with central hallways and adjacent rooms commonly found in office buildings, hotels, and dormitories.

The Xirrus XR-2000 Series Wireless Array is a four slot chassis available in a four multi-state (2.4GHz or 5GHz) radio configuration supporting up to 320 users with up to 1.8Gbps of bandwidth. These models support a range of low to high-performance applications, including offices, hospitals, campuses and classrooms, and hotels.

Like all XR Arrays, these models integrate multi-state radios with high gain directional antennas, an onboard multi-gigabit switch, controller, firewall, threat sensor and spectrum analyzer all built on a modular chassis designed for future extensibility.

Feature	XR-1220	XR-1230	XR-2220	XR-2230	XR-2420	XR-2430
No. radios: 802.11 a/b/g/n/monitor	2	2	2	2	4	4
Radio type	2x2	3x3	2x2	3x3	2x2	3x3
# Integrated antennas	4	6	4	6	8	12
Integrated wireless switch ports	2	2	4	4	4	4

Feature	XR-1220	XR-1230	XR-2220	XR-2230	XR-2420	XR-2430
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes	Yes	Yes
1 Gigabit Uplink Ports	1	1	1	1	1	1
Wireless bandwidth	600 Mbps	900 Mbps	600 Mbps	900 Mbps	1.2 Gbps	1.8 Gbps
Users supported	480	480	480	480	960	960

XR-4000 Series Arrays

These Arrays include models with two Gigabit Ethernet ports and four or eight radios (IAPs), connecting up to 640 users at one time and offering a maximum wireless bandwidth of 3.6 Gbps (up to 450 Mbps per radio). Smaller models may be upgraded to eight radios later when your needs change.

Feature	XR-4420	XR-4430	XR-4820	XR-4830
Number of radios: 802.11a/b/g/n/monitor	4	4	8	8
Radio type	2x2	3x3	2x2	3x3
# Integrated antennas	8	12	16	24
Integrated wireless switch ports	8	8	8	8
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes
1 Gigabit Uplink Ports	2	2	2	2
Wireless bandwidth	1.2 Gbps	1.8 Gbps	2.4 Gbps	3.6 Gbps
Users supported	960	960	1920	1920

XR-6000 Series Arrays

These Arrays include models with four Gigabit Ethernet ports and up to sixteen radios, connecting up to 1280 users at one time and offering a maximum wireless bandwidth of 7.2 Gbps (up to 450 Mbps per radio). Smaller models may be upgraded to sixteen radios later when your needs change. A 10 Gigabit modular Ethernet expansion port (DVI connector) is available to meet high traffic demands. It is used only with an optional Xirrus 10 Gig fiber optics adapter.

Feature	XR-6820	XR-6830	XR-7220	XR-7230	XR-7620	XR-7630
Number of radios: 802.11a/b/g/n/monitor	8	8	12	12	16	16
Radio type	2x2	3x3	2x2	3x3	2x2	3x3
Number of integrated antennas	16	24	24	36	32	48
Integrated wireless switch ports	16	16	16	16	16	16
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes	Yes	Yes
1 Gigabit Uplink Ports	4	4	4	4	4	4
External 10 Gigabit Modular Expansion Port	1	1	1	1	1	1
Wireless bandwidth (Gbps)	2.4	3.6	3.6	5.4	4.8	7.2
Users supported	896	896	1344	1344	1792	1792

See Also

Key Features and Benefits

Wireless Array Product Overview

Power over Gigabit Ethernet (PoGE)

Why Choose the Xirrus Wireless Array?

Enterprise Class Security

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

Deployment Flexibility

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

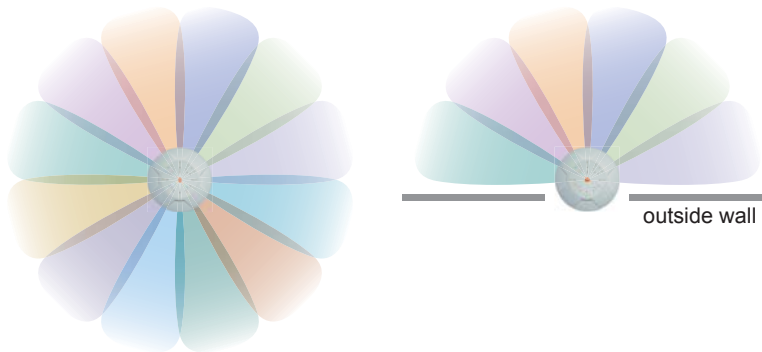


Figure 4. Wireless Coverage Patterns

Figure 4 depicts the following two scenarios:

- **Full pattern coverage**

All radios are activated with coverage spanning 360 degrees. If within range, clients will always receive coverage regardless of their geographic position relative to the Array. Radios may be assigned to 2.4 GHz and/or 5.0 GHz bands in any desired pattern.

- **Partial pattern coverage**

If desired, the Wireless Array can be deployed close to an exterior wall. In this case, half of all available radios have been deactivated to prevent redundant signals from “bleeding” beyond the site’s perimeter wall. This configuration may also be used in those cases where you want to restrict wireless coverage to selected areas of the building’s interior.

Power over Gigabit Ethernet (PoGE)

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

Enterprise Class Management

The Wireless 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, plus a full complement of troubleshooting tools and statistics.

XR4830 Wi-Fi Array												
Name: XR4012002207C (192.168.1.55)											Uptime: 0 days, 1 hours, 21 mins	
<div style="float: right;">Save changes to flash</div>												
Ethernet Settings Summary												
Interface	State	Mgmt	LED	Auto Neg	Link	Duplex	Speed (Mbps)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	on	on	on	up	full	100	1500	enabled	192.168.1.55	255.255.255.0	192.168.1.254
gig2	enabled	on	on	on	down			1500	enabled	192.168.1.55	255.255.255.0	192.168.1.254
Bond Settings Summary												
Bond			Mode			Ports			Active VLANs			Mirror
bond1			link-backup			gig1 gig2			all			off
bond2			link-backup						all			off
Integrated Access Points												
IAP	State	AP Type	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link / Distance	MAC Address / BSSID	Description
iap1	up	11abgn 3x3	mon	dedicated monitor	abgn	internal omni	monitor	20	-95	0		
iap2	up	11abgn 3x3	36	default	an	internal directional	max	20	-90	0		00:0f:7d:56:87:80
iap3	up	11abgn 3x3	1	default	bgn	internal directional	max	20	-90	0		00:0f:7d:56:87:a0
iap4	up	11abgn 3x3	44	default	an	internal directional	max	20	-90	0		00:0f:7d:56:87:b0
iap5	up	11abgn 3x3	6	default	bgn	internal directional	max	20	-90	0		00:0f:7d:56:87:c0
iap6	up	11abgn 3x3	52	default	an	internal directional	max	20	-90	0		00:0f:7d:56:87:d0
iap7	up	11abgn 3x3	11	default	bgn	internal directional	max	20	-90	0		00:0f:7d:56:87:e0
iap8	up	11abgn 3x3	60	default	an	internal directional	max	20	-90	0		00:0f:7d:56:87:f0

Figure 5. WMI: Array Status

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



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

Key Features and Benefits

This section describes some of the key product features and the benefits you can expect when deploying the Wireless Array (the XR-7630 product is used as an example in this section).

High Capacity and High Performance



Figure 6. Layout of IAPs (XR-7630)

The XR-7630 version of the Wireless Array (Figure 6) enables wireless connectivity and easily handles time-sensitive traffic such as voice. This model includes four Gigabit uplink ports for connection to the wired network. Its sixteen IAPs (radios) provide a maximum wireless capacity of 7.2 Gbps, which offers ample reserves for the high demands of current and future applications. Of the sixteen IAPs, fifteen operate as radios which may be set up to serve your choice of client types—any or all of 802.11a/b/g/n (5 GHz or 2.4 GHz bands), providing backwards compatibility with 802.11b and 802.11g.

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

Extended Coverage

One XR-7630 solution enables you to replace fifteen access points (including 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 Wireless Array deployed, far fewer access points are needed and wired-like resiliency is delivered throughout your wireless network. Your Wireless Array deployment ensures:

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

Non-Overlapping Channels

Complete use of non-overlapping channels limits interference and delivers maximum capacity. On the XR-7630, up to 16 non-overlapping channels are fully utilized across the 5GHz and 2.4GHz spectrums.

SDMA Optimization

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

Fast Roaming

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

Easy Deployment

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

Secure Wireless Access

Multiple layers of authentication and encryption ensure secure data transmissions. The Wireless Array is 802.11i compliant with line-rate encryption support for 40 and 128 bit WEP, WPA and WPA2 with TKIP and AES encryption. Authentication is provided via 802.1x, including PEAP, EAP-TLS, EAP-TTLS,

EAP-SIM, EAP-GRC, and LEAP (Lightweight Extensible Authentication Protocol) passthrough. Intrusion detection and prevention provide proactive monitoring of the environment for threats.

Applications Enablement

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

Advanced Feature Sets

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

Xirrus Advanced RF Performance Manager (RPM)

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

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

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

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

The complete feature set of the RPM package includes:

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

Xirrus Advanced RF Security Manager (RSM)

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

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

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

The complete feature set of the RSM package includes:

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

Xirrus Advanced RF Analysis Manager (RAM)

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

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

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

The key elements of the RAM package include:

- RF Analysis – An embedded Spectrum Analyzer leverages the dedicated threat sensor radio in each Wireless Array to provide a continual view of utilization, interference, and errors across all available wireless channels.
- Packet Analysis – Integrated packet capture provides filterable views of all traffic traversing on the wired and wireless interfaces of the Array.

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

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 Wireless 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 Wireless 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 Wireless Array**
Describes the status and statistics displays available on the Array using its embedded Web Management Interface.

- [Configuring the Wireless Array](#)
Contains procedures for configuring the Array using its embedded Web Management Interface.
- [Using Tools on the Wireless 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 Wireless 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: Quick Reference Guide](#)
Contains the product's factory default settings.
- [Appendix B: 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 C: 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.

Product Specifications—XR Array Family

Please refer to the Xirrus web site for the latest specifications for these Arrays—
www.xirrus.com

Installing the Wireless Array

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

- [“Installation Prerequisites” on page 21.](#)
- [“Planning Your Installation” on page 24.](#)
- [“Installation Workflow” on page 56.](#)
- [“Installing Your Wireless Array” on page 58.](#)
- [“Powering Up the Wireless Array” on page 62.](#)
- [“Establishing Communication with the Array” on page 65.](#)
- [“Performing the Express Setup Procedure” on page 69.](#)

Installation Prerequisites

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

- **Power Source**

Most Arrays are powered via Xirrus Power over Gigabit Ethernet. PoGE supplies power over the same Cat 5e or Cat 6 cable used for data, thus reducing cabling and installation effort. PoGE power injector modules are available in 1-, 2-, and 8-port configurations and are typically placed near your Gigabit Ethernet switch. An AC outlet is required for each injector module. Current Array models have integrated splitters, so no separate splitter is required.
- **Ethernet ports**

You need at least one 100/1000 BaseT port to establish wired Gigabit Ethernet connectivity. XR Series Arrays have one, two, or four Gigabit ports, depending on the model (see “XR Wireless Array Product Family” on page 6).

! *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 do not bond-pair Ethernet ports.*

- **Secure Shell (SSH) utility**

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

- **Secure Web browser**

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

- **Serial connection capability**

To connect directly to the console port on the Array (all models except XR-1000 Series), 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 Wireless 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 Wireless 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 Wireless 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 24
- “Coverage and Capacity Planning” on page 26
- “IEEE 802.11n Deployment Considerations” on page 35
- “Failover Planning” on page 41
- “Power Planning” on page 44
- “Security Planning” on page 45
- “Port Requirements” on page 47
- “Network Management Planning” on page 51
- “WDS Planning” on page 52
- “Common Deployment Options” on page 55



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

General Deployment Considerations

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

1. Keep the number of walls and ceilings between the Array and your receiving devices to a minimum—each wall or ceiling can reduce the

wireless range from between 3 and 90 feet (1 to 30 meters). Position your devices so that the number of walls or ceilings is minimized.

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

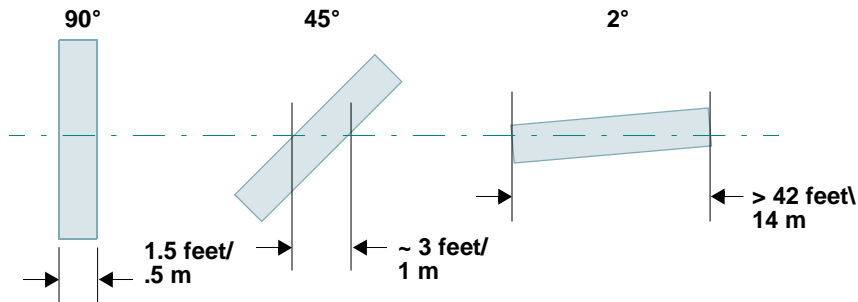


Figure 7. Wall Thickness Considerations

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

See Also

Coverage and Capacity Planning

Deployment Examples

Common Deployment Options

Installation Prerequisites

Coverage and Capacity Planning

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



Note that several advanced features in this section are part of the Xirrus Advanced RF Performance Manager (RPM). They require the license installed on the Array to include support for RPM. Please see “About Licensing and Upgrades” on page 321.

Placement

Use the following guidelines when considering placement options:

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

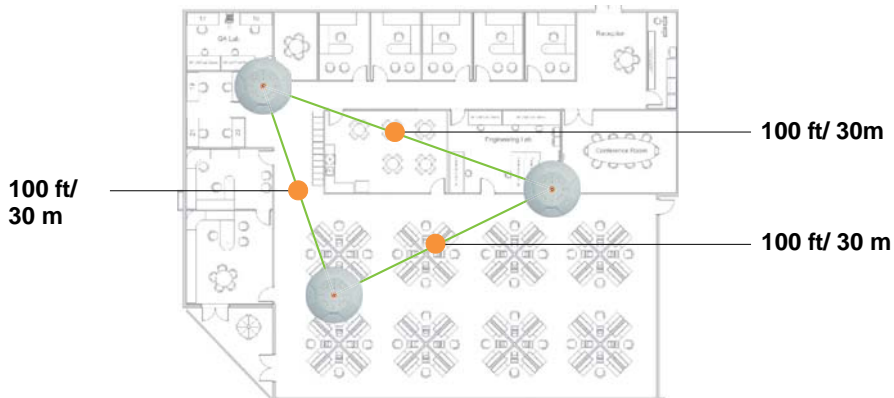


Figure 8. Unit Placement

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

RF Patterns

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

Full (Normal) Coverage

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

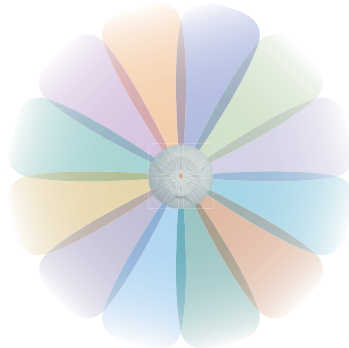


Figure 9. Full (Normal) Coverage

Half Coverage

If installing a unit close to an exterior wall, you can deactivate half of the radios to prevent redundant signals from “bleeding” beyond the wall and extending service into public areas. The same principle applies if you want to restrict service to an adjacent room within the site.

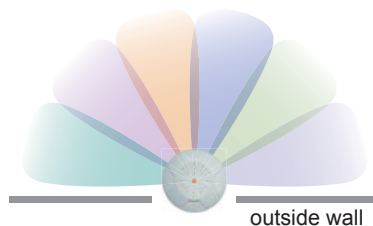


Figure 10. Adjusting RF Patterns

Custom Coverage

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

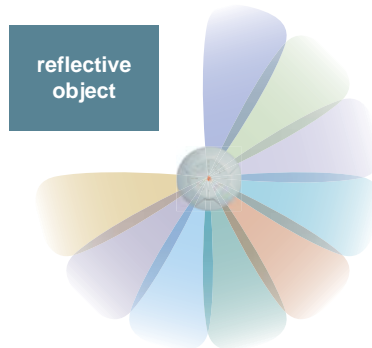


Figure 11. Custom Coverage

Capacity and Cell Sizes

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

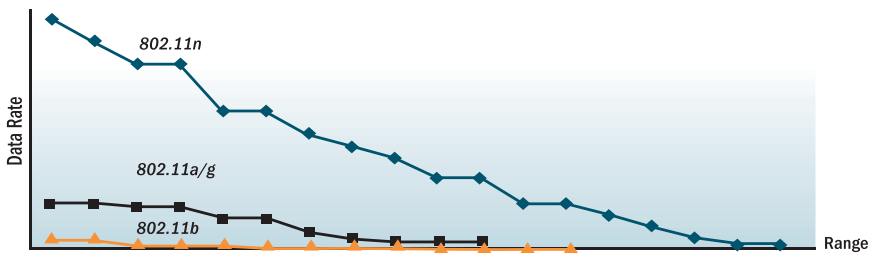


Figure 12. Connection Rate vs. Distance

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

Fine Tuning Cell Sizes

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

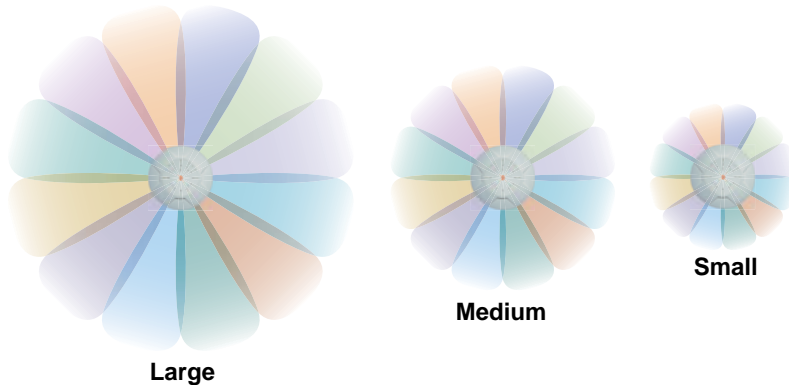


Figure 13. Transmit Power

Auto Cell Size is an automatic, self-tuning mechanism that balances cell size between Arrays to guarantee coverage while limiting the RF energy that could extend beyond the organizational boundary. Auto Cell uses communication between Arrays to dynamically set radio power so that complete coverage is provided to all areas, yet at the minimum power level required. This helps to minimize potential interference with neighboring networks. Additionally, Arrays running Auto Cell automatically detect and compensate for coverage gaps caused by system interruptions. To enable the Auto Cell Size feature, go to “[RF Power & Sensitivity](#)” on page 285. For a complete discussion of the Auto Cell size feature, see the *Xirrus Auto Cell Application Note* in the [Xirrus Resource Center](#).

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 26.

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 Wireless Arrays or other Access Points. To enable the Sharp Cell feature, go to “RF Power & Sensitivity” on page 285. For more information about this feature, see the *Xirrus Sharp Cell Application Note* in the [Xirrus Resource Center](#).

Roaming Considerations

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

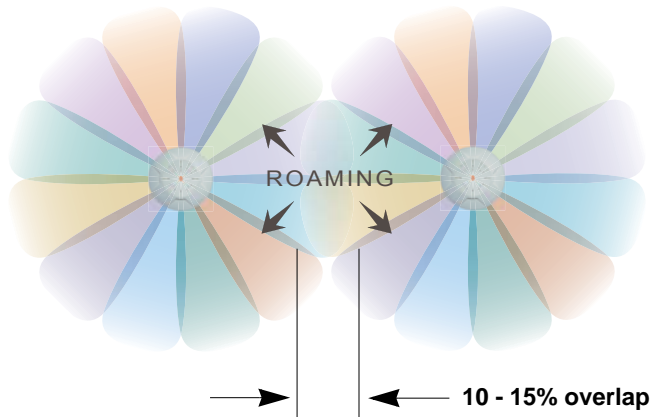


Figure 14. Overlapping Cells

Allocating Channels

Because the Wireless 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 wireless 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 282.

Manual Channel Selection

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



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

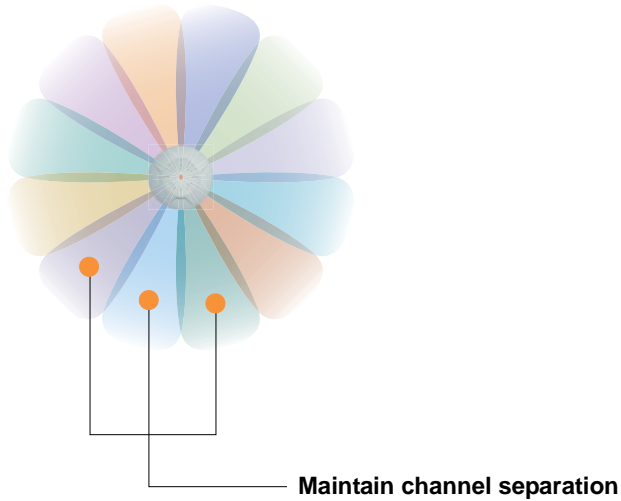


Figure 15. Allocating Channels Manually

See Also

Deployment Examples

Failover Planning

Installation Prerequisites

Deployment Examples

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

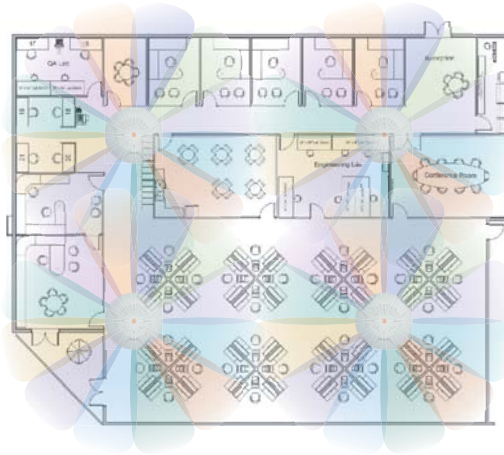


Figure 16. Deployment Scenario (54 Mbps)—Per Sector



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



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

See Also

Coverage and Capacity Planning

Failover Planning

Planning Your Installation

IEEE 802.11n Deployment Considerations

The Xirrus 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 36
- “Multiple Data Streams—Spatial Multiplexing” on page 37
- “Channel Bonding” on page 38
- “Improved MAC Throughput” on page 39
- “Short Guard Interval” on page 39
- “Obtaining Higher Data Rates” on page 40
- “802.11n Capacity” on page 41

Two very important techniques to consider are [Channel Bonding](#) and [Multiple Data Streams—Spatial Multiplexing](#) because they contribute a large portion of 802.11n’s speed improvements and because they are optional and configurable, as opposed to the parts of 802.11n that are fixed. While the settings for 802.11n IAPs come pre-configured on the Array for robust performance in typical usage, you

should review the settings for your deployment, especially channel bonding. A global setting is provided to enable or disable 802.11n mode. See “Global Settings .11n” on page 279 to configure 802.11n operation.

MIMO (Multiple-In Multiple-Out)

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

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

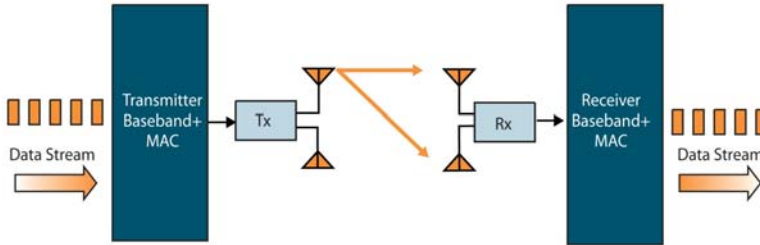


Figure 19. Classic 802.11 Signal Transmission

MIMO signal processing uses multiple antennas to send and receive data. It takes advantage of multipath reflections to improve signal coherence and greatly increase receiver sensitivity (Figure 20).

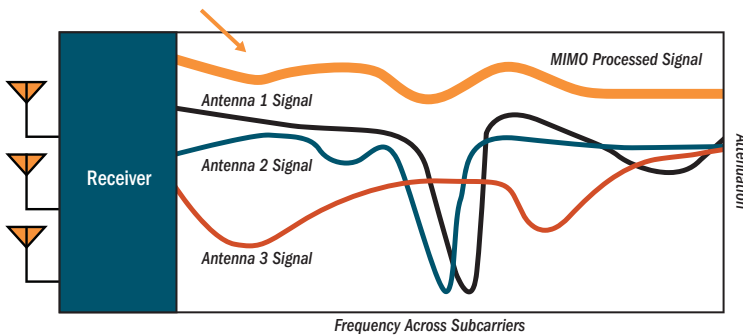


Figure 20. MIMO Signal Processing

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

Multiple Data Streams—Spatial Multiplexing

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

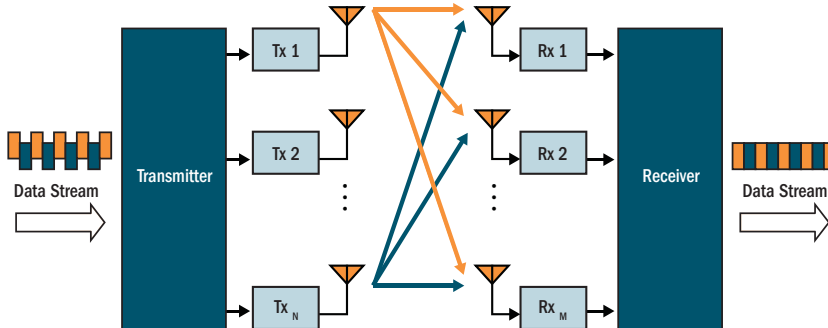


Figure 21. Spatial Multiplexing

Spatial multiplexing can double, triple, or quadruple the data rate, depending on the number of transmit antennas used. You can configure the number of chains (i.e., streams) separately for transmitting and receiving. By default, the Array uses three chains for transmitting and receiving (see [“Global Settings .11n”](#) on page 279).

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

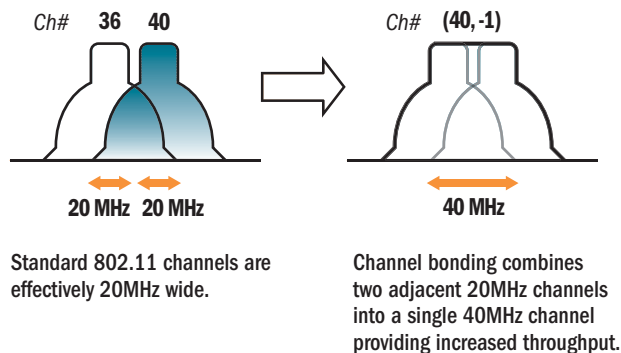


Figure 22. Channel Bonding

Improved MAC Throughput

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

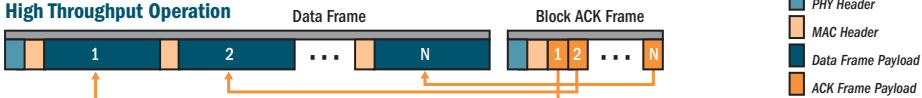
- MAC data frames are combined and given a single PHY header.
- Implicit Block ACK acknowledges all data frames within a combined frame.
- Spacing between frames is reduced.

Frame Aggregation

Legacy Operation

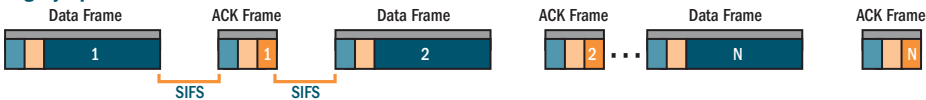


High Throughput Operation



RIFS Usage (Reduced Inter-Frame Spacing)

Legacy Operation



High Throughput Operation



Figure 23. MAC Throughput Improvements

Short Guard Interval

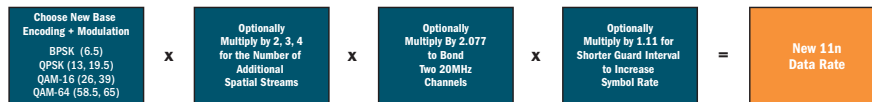
This option reduces the wait time between signals that are being sent out over the air. The guard interval provides immunity to propagation delays and reflections, and is normally 800 ns (long). By using a short guard interval (400 ns), the data rate is increased by approximately 11%. The short interval may be used in many environments (especially indoors). If the short guard interval is used in an inappropriate environment, the signal quality will suffer and throughput will decrease. See “Global Settings .11n” on page 279 to configure the guard interval.

Obtaining Higher Data Rates

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

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

See [Figure 24](#) to see the 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

Three Spatial Streams		
Three Spatial Streams	With Channel Bonding (40MHz)	With Short Guard Interval
19.5	40.5	45
39	81	90
58.5	121.5	135
78	162	180
117	243	270
156	324	360
175.5	364.5	405
195	405	450

Figure 24. Computing 802.11n Data Rates

802.11n Capacity

802.11n offers major increases in capacity over previous 802.11 standards, as shown in the table below.

802.11 Mode	# Channels	Max Theoretical Capacity
802.11 a/n: 3 Streams	23	$23 * 450 \text{ Mbps} = 10.2 \text{ Gbps}$
802.11 a/n: 2 Streams	23	$23 * 300 \text{ Mbps} = 6.8 \text{ Gbps}$
802.11 a/n: 1 Stream	23	$23 * 150 \text{ Mbps} = 3.4 \text{ Gbps}$
802.11 a	23	$23 * 54 \text{ Mbps} = 1.2 \text{ Gbps}$
802.11 g/n: 3 Streams	3	$3 * 450 \text{ Mbps} = 1.35 \text{ Gbps}$ (1 or 2 streams have proportionally lower capacity)
802.11 g	3	$3 * 54 \text{ Mbps} = 162 \text{ Mbps}$
802.11 b	3	$3 * 11 \text{ Mbps} = 33 \text{ Mbps}$

Failover Planning

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

To ensure that service is continued in the event of a port failure, you can utilize two Gigabit Ethernet ports simultaneously as a bonded pair (on Arrays with two or more Gigabit ports).

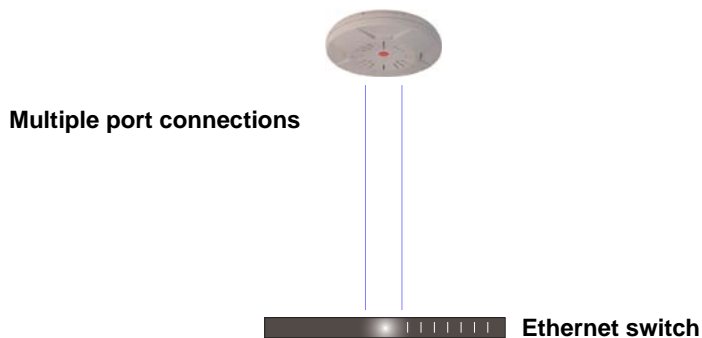


Figure 25. Port Failover Protection

In addition, the Array has full failover protection between the bonded-pair Gigabit ports (see following table).

Interface	Bridges Data?	Bridges Management Traffic?	Fails Over To:	IP address
Gigabit port	Yes	Yes	Bonded port	DHCP or static
Bonded Gigabit port	Yes	Yes	Bonded port	Same

The Wireless Array Gigabit Ethernet ports actually support a number of modes:

- 802.3ad Link Aggregation
- Load Balancing
- Broadcast
- Link Backup
- Mirrored

For more details on Gigabit port modes and their configuration, please see “Network Bonds” on page 160.

Switch Failover Protection

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



Figure 26. Switch Failover Protection



Gigabit Ethernet connections must be on the same subnet.

See Also

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

Power Planning

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

Power over Gigabit Ethernet

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

Specific models of the Array are compatible with specific PoGE modules. For details, please see the *Power over Gigabit Ethernet Installation and User Guide*.



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 191 and the Security section of “Frequently Asked Questions” on page 412.



Note that several advanced features in this section are part of the Xirrus Advanced RF Security Manager (RSM). They require the license installed on the Array to include support for RSM. Please see “About Licensing and Upgrades” on page 321.

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 Wireless Array:

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

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

- **Xirrus Internal RADIUS server**
Recommended for smaller numbers of users (about 100 or less). Supports EAP-PEAP only
- **Pre-Shared Key**
Uses a pass-phrase or key that is manually distributed to all authorized users. The same passphrase is given to client devices and entered into each Array.
- **MAC Access Control Lists (ACLs)**
MAC access control lists provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network, and can be used in addition to any of the above authentication methods. ACLs are good for embedded devices, like printers and bar-code scanners (though MAC addresses can be spoofed). The Array supports 1,000 global ACL entries. You may also define per-SSID access control lists, with up to 1000 entries each.

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 48](#) 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 27](#). XMS requires ports 161, 162, and 443 to be passed between Arrays and the XMS server. Similarly, ports 9090 and 9091 are required for communication between the XMS server and XMS clients, and port 25 is typically used by the XMS server to access an SMTP server to send email notifications.

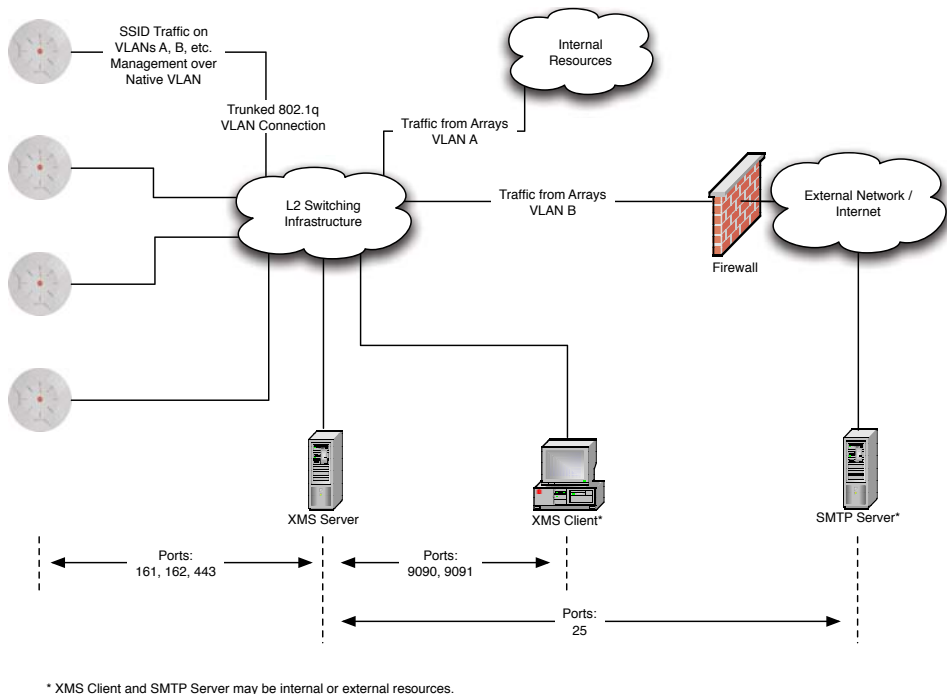


Figure 27. Port Requirements for XMS

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
Array			
icmp	Ping	XMS Server	No
20 tcp 21 tcp	FTP	Client	Yes
22 tcp	SSH	Client	Yes
23 tcp	Telnet	Client	Yes
25 tcp	SMTP	Mail Server	No
69 udp	TFTP	TFTP Server	No
123 udp	NTP	NTP Server	No
161 udp	SNMP	XMS Server	No
162 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
22610 udp	XRP (Xirrus Roaming)	Arrays	Yes
22612 udp	Xircon (Console Utility)	Admin Workstation	Yes

Port	Application	Peer	Configurable
XMS			
icmp	Ping	Arrays	No
22 tcp	SSH	Arrays	Yes
25 tcp	SMTP	Mail Server	Yes
123 udp	NTP	NTP Server	No
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
9092 tcp	XMS Client Server	XMS client	Via XMS config file
9443 tcp	XMS WMI SSL	XMS web client	No
* Internal to XMS Server, no ports need to be unblocked on other network devices			

See Also

Management Control

External Radius

Services

VLAN Management

Network Management Planning

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

- Command Line Interface, using an SSH (Secure Shell) utility, like PuTTY. The utility **must** be set up to use SSH-2, since the Array will only allow SSH-2 connections.
- Web-based management, using the Array's embedded Web Management Interface (WMI). This method provides configuration and basic monitoring tools, and is good for small deployments (one or two units).
- Centralized Web-based management, using the optional Xirrus Management System (XMS), which can be run on a dedicated Xirrus appliance or your own server. The XMS is used for managing large Wireless 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 28](#)). WDS features include:

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



Figure 28. WDS Link

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

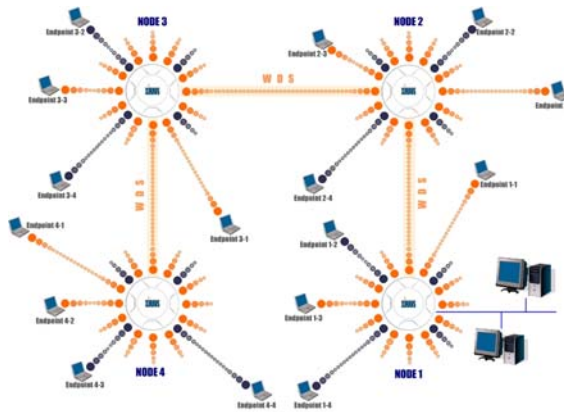


Figure 29. A Multiple Hop WDS Connection

- Multiple WDS links can provide link redundancy (failover capability - see Figure 30). A network protocol (Spanning Tree Protocol—STP) prevents Arrays from forming network loops.

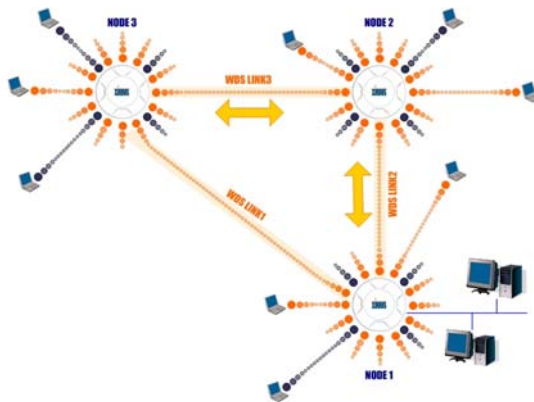


Figure 30. WDS Failover Protection

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

See Also

Coverage and Capacity Planning

Deployment Examples

Network Management Planning

Planning Your Installation

Power Planning

Security Planning

Installation Workflow

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

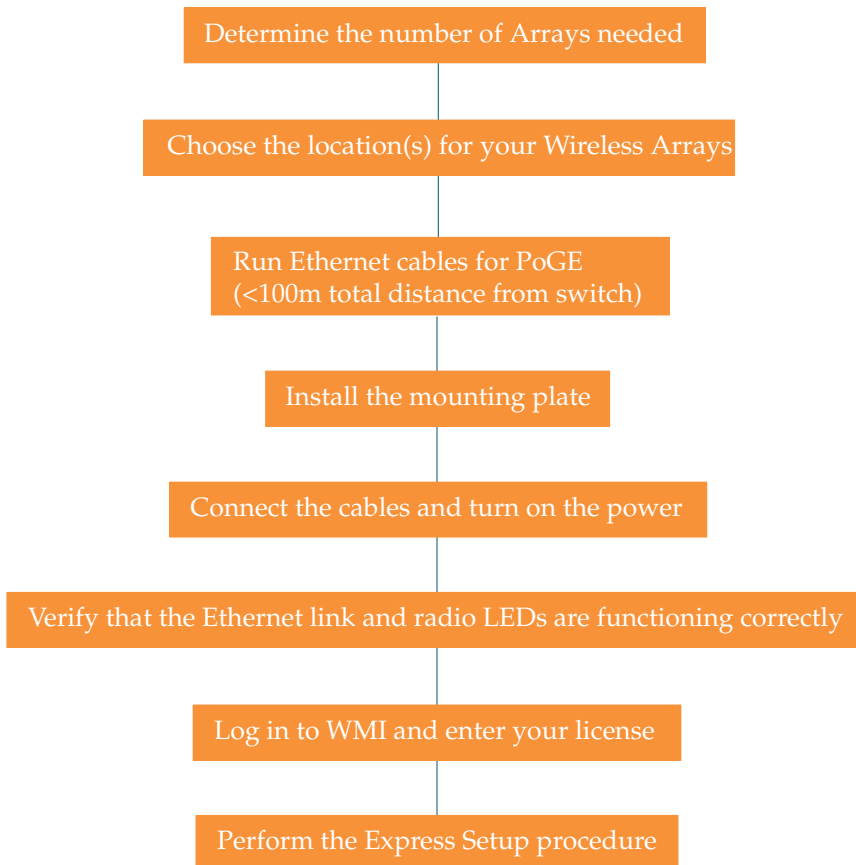


Figure 31. Installation Workflow

See Also

Coverage and Capacity Planning
Deployment Examples

- Common Deployment Options
- Failover Planning
- Installation Prerequisites
- Planning Your Installation
- Power Planning
- Wireless Array Product Overview
- Security Planning

Installing Your Wireless Array

This section provides instructions for completing a physical installation of your Xirrus Wireless 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 Wireless Array was designed to be mounted on a ceiling where the unit is unobtrusive and wireless transmissions can travel unimpeded throughout open plan areas.

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

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

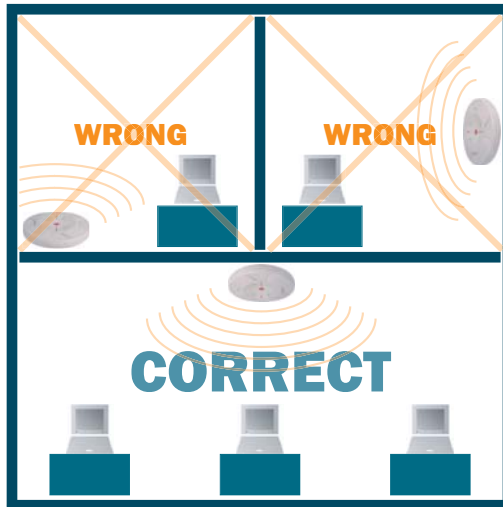


Figure 32. Array Placement

Wiring Considerations

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

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

Power

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

Network

- Gigabit POE1—the total of all Cat 5e or Cat 6 cable segments from the Gigabit Ethernet switch to an Array Ethernet port 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 POE2—For Arrays with a second POE port, the same restrictions listed above apply.
- Serial cable (optional) — cable lengths up to 25' per the RS-232 specification.

Important Notes About Network Connections

Read the following notes before making any network connections.



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

For the XR-1000, the Xirrus Xircon utility may be used locally to set up an IP address if necessary.



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.

See Also

Failover Planning

Installation Prerequisites

Installation Workflow

Mounting the Array

Power over Gigabit Ethernet (PoGE)

Mounting the Array

A number of options are available for mounting Arrays:

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

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

Dismounting the Array

To dismount any other Array model

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

Powering Up the Wireless 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.

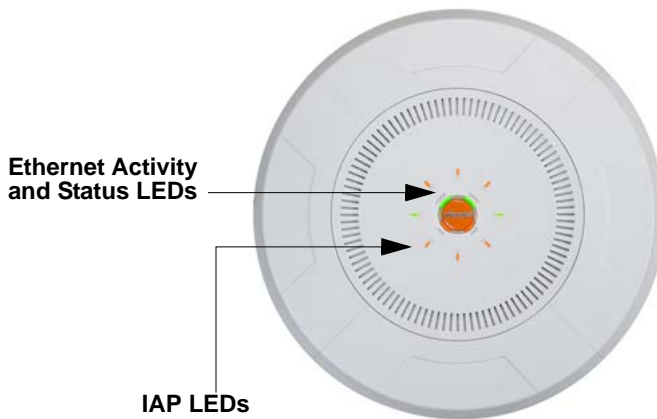


Figure 33. LED Locations

Array LED settings may be altered or disabled entirely for diagnostic purposes or for personal preference. Changes are made via the Array's Command Line Interface or the Web Management Interface—refer to “LED Settings” on page 297.

Array LED Operating Sequences

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

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

LED Boot Sequence

The normal boot LED sequence is as follows:

Array Activity	Status LED	IAP LEDs
Power ON	Blinking GREEN	All OFF
Boot loader power ON self-test	Blinking GREEN	All ON
Image load from compact FLASH	Blinking GREEN	Spinning pattern (rotate all to ON, then all to OFF)
Image load failure	Blinking ORANGE	All OFF
Hand off to ArrayOS	Solid GREEN	All OFF
System software initialization	Solid GREEN	Walking pattern—(LED rotating one position per second)
Up and running	Solid GREEN	ON for IAPs that are up: OFF for IAPs that are down. Behavior may be changed using "LED Settings" on page 297.

LED Operation when Array is Running

The normal LED operation when the Array is running is shown in the table below. Note that behavior may be modified using “LED Settings” on page 297 or via the CLI.

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

See Also

[Installation Prerequisites](#)

[Installation Workflow](#)

[Installing Your Wireless Array](#)

[LED Settings](#)

Establishing Communication with the Array

The Array may be configured through the Command Line Interface (CLI) using SSH, or on a browser via the graphical Web Management Interface (WMI). You may use the CLI via the serial management port (console—on all Arrays except the XR-1000 Series) or any of the Gigabit Ethernet ports. You can use the WMI via any of the Array’s Ethernet ports.

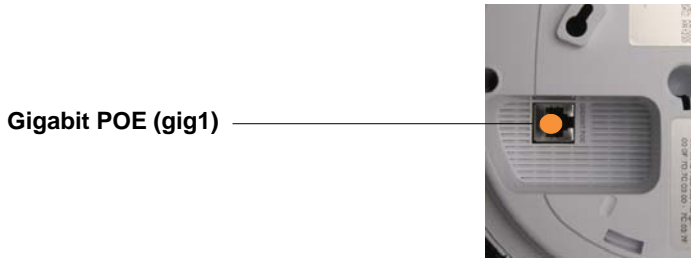


Figure 34. Network Interface Ports—XR-1000 Series

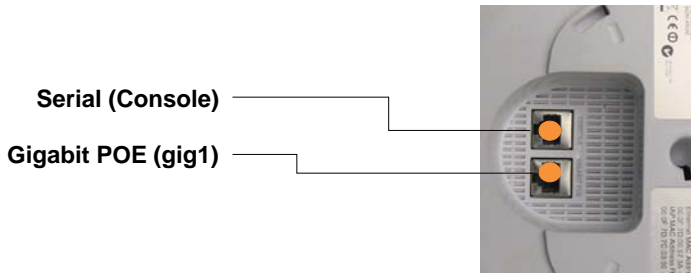


Figure 35. Network Interface Ports—XR-2000 Series **??OK??**

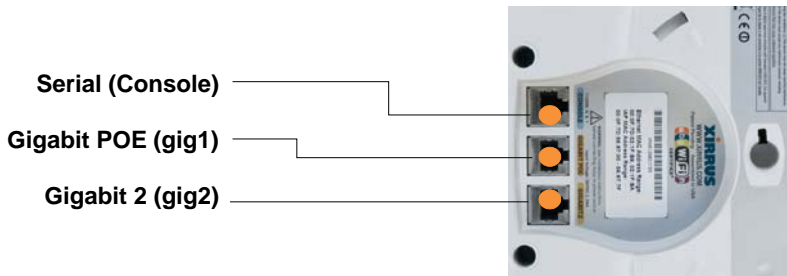


Figure 36. Network Interface Ports—XR-4000 Series

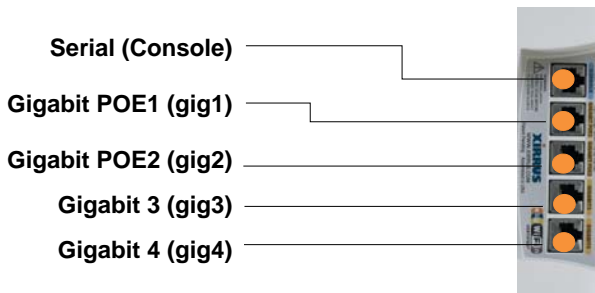


Figure 37. Network Interface Ports—XR-6000 Series



The Xirrus Xircon utility may also be used to communicate with Arrays locally as an alternative to using a serial connection to the console. This is especially useful for the XR-1000, which does not have a console port.

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 Gigabit Ethernet ports, then both Gigabit1 and its bonded pair port will default to 10.0.2.1.

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

1. The simplest way to address the Array is using its default hostname which is the Array's serial number (for example, XR40123091CACD). If your network provides DHCP and DNS, then you can use this hostname.
2. Otherwise, examine the DHCP tables on the server and find the addresses assigned to the Array (Xirrus MAC addresses begin with 000F7D).

3. Alternatively, you may query the Array using the CLI via the serial port. Log in using the default user name **admin** and password **admin**. Use the **show ethernet** command to view the IP addresses assigned to each port.

Starting the WMI

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

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

Logging In

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

See Also

[Installation Workflow](#)

[Performing the Express Setup Procedure](#)

[Powering Up the Wireless Array](#)

Entering the License

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

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

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

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

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



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

Performing the Express Setup Procedure

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

Status		Name: XR40140026956 (10.100.48.61)		Uptime: 0 days, 12 hours, 56 mins	
Array	Host Name:	XR40140026956		Save changes to flash	
Network	Location Information:				
RF Monitor	Admin Contact:				
Stations	Admin Email:				
Statistics	Admin Phone:				
System Log	License Key:	0K0FT-4DRNP-FUMA		Apply	
IDS Event Log	SNMPv2 Settings				
Configuration	Enable SNMPv2:	<input checked="" type="radio"/> Yes		<input type="radio"/> No	
Express Setup	Read Only Community String:	*****			
Network	Read Write Community String:	*****			
Services	Gigabit Ethernet 1 Settings				
VLANs	Enable Interface:	<input checked="" type="radio"/> Yes		<input type="radio"/> No	
Security	Allow Management On Interface:	<input checked="" type="radio"/> Yes		<input type="radio"/> No	
SSIDs	Configuration Server Protocol:	<input type="radio"/> DHCP		<input checked="" type="radio"/> Static	
Groups	IP Settings:	Address: 10.100.48.61	Subnet Mask: 255.255.255.0	Default Gateway:	
IAPs		10.100.48.1		Apply	
WDS	Gigabit Ethernet 2 Settings				
Filters	Enable Interface:	<input checked="" type="radio"/> Yes		<input type="radio"/> No	
Clusters	Allow Management On Interface:	<input checked="" type="radio"/> Yes		<input type="radio"/> No	
Tools	Configuration Server Protocol:	<input type="radio"/> DHCP		<input checked="" type="radio"/> Static	
Help	IP Settings:	Address: 10.100.48.61	Subnet Mask: 255.255.255.0	Default Gateway:	
System Tools		10.100.48.1		Apply	
CLI	SSID Settings				
Options	SSID (Wireless Network Name):				
Logout	Wireless Security:	Open		Apply SSID Settings	
Log Messages	Admin Settings				
Critical	New Admin User (Replaces user "admin"):				
Warning	New Admin Privilege Level:	1: read-write			
Information	New Admin Password:				
	Confirm Admin Password:				
		Apply Admin Settings			
	Time and Date Settings				
	Current Array Date and Time:	Mon Mar 12 2012 08:42:09			
	Time Zone:	(GMT) Greenwich Mean Time: Dublin, Lisbon, London			
	Auto Adjust Daylight Savings:	<input type="checkbox"/>			
	Use Network Time Protocol:	<input checked="" type="radio"/> Yes		<input type="radio"/> No	
	NTP Primary Server:	time.nist.gov			
	NTP Primary Authentication:	None			
	NTP Primary Authentication Key ID:	1			
	NTP Primary Authentication Key:				
	NTP Secondary Server:	pool.ntp.org			
	NTP Secondary Authentication:	None			
	NTP Secondary Authentication Key ID:	2			
	NTP Secondary Authentication Key:				
	IAP Settings				
	Enable/Configure All IAPs:	Execute			

Figure 38. 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. **License Key:** If Xirrus issued you a license that differs from the current value shown, enter it now.
7. **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 179.
8. **Configure the Gigabit 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.



For improved security, you should also take the additional steps described in “Securing Low Level Access to the Array” on page 76.

- 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 **IP Settings**:

 - **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.
 - **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.
 - Click the **Apply** button for this interface when done making IP changes.
- 9. 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 412.
 - 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 191](#).

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

- 10. Admin Settings:** This section allows you to change the default admin username, password, and privileges for the Array. You may change the password and leave the user name as is, but we suggest that you change both to improve Array security.
- a. New Admin User (Replaces user “admin”):** Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the Array also offers the option of authenticating administrators using a RADIUS server (see “Admin Management” on page 196)).



For improved security, you should also take the additional steps described in “Securing Low Level Access to the Array” on page 76.

- b. New Admin Privilege Level:** By default, the new administrator will have read/write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see “Admin Privileges” on page 198.
 - c. New Admin Password:** Enter a new administration password for managing this Array. If you forget this password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
 - d. Confirm Admin Password:** If you entered a new administration password, confirm the new password here.
 - e. Click Apply Admin Settings** when done.
- 11. Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you’re not using a server.
- a. Current Array Date and Time:** This read-only field shows the current time for your convenience.

- b. **Time Zone:** Select your time zone from the choices available in the pull-down list.
- c. **Auto Adjust Daylight Savings:** If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
- d. **Use Network Time Protocol:** Check this box if you want to use an NTP server to synchronize the Array's clock. Use of NTP is mandatory for Arrays to be managed with XMS (the Xirrus Management System), and ensures that Syslog time-stamping is maintained across all units. If you check **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, leave this box unchecked (default) and set the system time on the Array manually.
- e. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
- f. **NTP Primary Authentication:** If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default). For more information on authenticated NTP, see "[Time Settings \(NTP\)](#)" on page 171.
- g. **NTP Primary Authentication Key ID:** Enter the key ID, which is a decimal integer.
- h. **NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- i. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.
- j. **Adjust Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes,

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

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

12. IAP Settings:

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

- 13. Click on the **Save changes to flash button** at the top right if you wish to make your changes permanent.

This ends the Express Setup procedure.

See Also

[Establishing Communication with the Array](#)

[Installation Prerequisites](#)

[Installation Workflow](#)

[Logging In](#)

[Multiple SSIDs](#)

[Security](#)

Securing Low Level Access to the Array

??Please review this whole section carefully. This section on Xircon disable and XBL password is being included in both the XR manual and the XN manual, on the assumption that when the XS 6.1 releases, it will include the Xircon options. OK?? Most management of the Xirrus Array is done via the Web Management Interface (WMI) as you just saw in “Performing the Express Setup Procedure” on page 69. Another often used option is CLI—see “The Command Line Interface” on page 337. The Array also has a lower level interface: XBL (Xirrus Boot Loader), which allows access to more primitive commands. You won’t normally use XBL unless instructed to do so by Xirrus Customer Support. For proper security, you should replace the default XBL login username and password with your own, as instructed below. XBL has its own username and password, separate from the ArrayOS Admin User and Password (used for logging in to the WMI and CLI) that you changed in Step 10 on page 73. ?? xxx Is changing XBL password really only necessary if Xircon is enabled? There aren’t other ways to get at XBL that would benefit from securing the password?

Xirrus also provides the Xircon utility for connecting to Xirrus XR Arrays that are not reachable via the normal access methods (such as SSH or WMI) and that do not have a physical console port (XR-1000), or whose console port is not accessible. Xircon discovers Arrays on your network subnet by sending IP/UDP broadcast packets. Once an Array is discovered, Xircon can establish an encrypted console session to the Array via the network even if the Array IP configuration is incorrect. Xircon allows you to manage the Array using CLI, just as you would if connected to the console port. Xircon also has an option for easily accessing XBL.

In normal circumstances Xirrus Arrays should be configured and managed through secure shell (SSH) or via the Web Management Interface (WMI). A connection is established using either the Array hostname or DHCP-assigned IP address, or via the other options described in “Using the Ethernet Ports” on page 66. Xircon may be needed in special circumstances as directed by Xirrus Customer Support for troubleshooting Array problems or IP connectivity. (In this case, see the *Xircon User Guide* for detailed information.)

Xircon access to the Array may be controlled:

- You may enable or disable all Xircon access to the Array as instructed in the procedure below. There are also options to allow access only to CLI (i.e., ArrayOS access) or only to XBL.
 - Since XR-1000 Array models do not have a console port, these models have Xircon access to both XBL and CLI enabled by default. For Arrays that do not have a console port, to avoid potentially being locked out of the Array, Xircon should always be enabled at the XBL level at least.
- ! *Warning: If you disable Xircon access completely on XR-1000 models, you must ensure that you do not lose track of the username and password to log in to CLI/WMI! There is no way to recover from a lost password, other than returning the Array to Xirrus.*
- On all other Array models (those with a console port), Xircon access to both XBL and CLI is disabled by default. If Xircon is not going to be used to access an Array, we recommend leaving Xircon access disabled.

Procedure for Securing Low Level Array Access

Use the following steps to replace the default XBL username and password, and optionally to change the type of Xircon management access that is allowed. These steps use CLI commands.

1. To access CLI via the WMI, click **CLI** under the **Tools** section on the left (for detailed instructions see “CLI” on page 332). Skip to **Step 4** on page 78.

To access CLI via SSH, see “Establishing a Secure Shell (SSH) Connection” on page 337. Then proceed to the next step.

2. At the **login as** prompt, log in to CLI using the username and password that you set in **Step 10** on page 73.

```
login as: jsmith
jsmith@xr4012802207c's password:

Xirrus Wi-Fi Array
ArrayOS Version 6.1.2-3299
Copyright (c) 2005-2012 Xirrus, Inc.
```

```
http://www.xirrus.com
```

```
XR4012802207C#
```

3. Type **configure** to enter the CLI config mode.

```
hostname#configure
```

4. If Xircon access at the XBL level is to be allowed, use the following three commands to change the XBL username and password from the default values of **admin/admin**. In the example below, replace **newusername** and **newpassword** with your desired entries. Note that these entries are case-sensitive.

```
(config)#boot-env set username newusername
(config)#boot-env set password newpassword
(config)#save
```

5. Enter the following commands if you wish to change Xircon access permission:

```
(config)# management
(config-mgmt)# xircon <management-status>
(config-mgmt)# save
(config-mgmt)# exit
(config)#
```

<*management-status*> may be one of :

- **on** enables both CLI and XBL access
- **off** disables both CLI and XBL access
- **aos-only** enables only CLI (i.e. ArrayOS) access
- **boot-only** enables only XBL access

Note that there is a WMI setting for changing Xircon access, timeout period, and the UDP port used. This may be used instead of CLI if you wish. See “[Management Control](#)” on [page 203](#). Note that you cannot change the XBL username and password via the WMI.

The Web Management Interface

| This topic provides an overview of the Xirrus Wireless 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 Wireless Array. It allows you to configure the product to suit your individual requirements and ensure that the unit functions efficiently and effectively.

XR4830 Wi-Fi Array **XIRRUS**

Status: **Name: Robin.XR4830 (10.100.48.24)** Uptime: 0 days, 0 hours, 18 mins

Configuration Save changes to flash

- Express Setup
- Network
- Services
- VLANs
- Security
- SSIDs
- Groups
- IAPs
 - IAP Settings
 - Global Settings
 - Global Settings: 11an
 - Global Settings: 11bgn
 - Global Settings: 11n
 - Advanced RF Settings
 - Intrusion Detection
 - LED Settings
 - DSCP Mappings
 - Roaming Assist
- WDS
- Filters
- Clusters
- Tools
 - Help
 - System Tools
 - CLI
 - Options
 - Logout
- Log Messages
 - Critical 3
 - Warning 4
 - Information 161

IAP	State	AP Type	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link / Distance	MAC Address / BSSID	Description
iap1	up	11abgn 3x3	mon dedicated monitor	abgn	internal omni	monitor	20	-95	0		00:0f:7d:0b:6d:80	
iap2	up	11abgn 3x3	64 automatic	an	internal directional	max	20	-90	0		00:0f:7d:0b:6d:90	
iap3	up	11abgn 3x3	11 automatic	bgn	internal directional	max	20	-90	0		00:0f:7d:0b:6d:a0	
iap4	up	11abgn 3x3	136 automatic	an	internal directional	max	20	-90	0		00:0f:7d:0b:6d:b0	
iap5	up	11abgn 3x3	40 automatic	an	internal directional	max	20	-90	0		00:0f:7d:0b:6d:40	
iap6	up	11abgn 3x3	104 automatic	an	internal directional	max	20	-90	0		00:0f:7d:0b:6d:50	
iap7	up	11abgn 3x3	6 automatic	bgn	internal directional	max	20	-90	0		00:0f:7d:0b:6d:60	
iap8	up	11abgn 3x3	153 automatic	an	internal directional	max	20	-90	0		00:0f:7d:0b:6d:70	

Copyright © 2005-2012 by Xirrus, Inc.

Figure 39. 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>Status Windows</p> <ul style="list-style-type: none"> Array Status Windows <ul style="list-style-type: none"> Array Summary Array Information Array Configuration Admin History Network Status Windows <ul style="list-style-type: none"> Network Map Spanning Tree Status Routing Table ARP Table DHCP Leases Connection Tracking/NAT CDP Neighbors Network Assurance RF Monitor Windows <ul style="list-style-type: none"> IAPs Spectrum Analyzer Intrusion Detection Channel History Radio Assurance Station Status Windows <ul style="list-style-type: none"> Stations Location Map RSSI Signal-to-Noise Ratio (SNR) Noise Floor Max by IAP Station Assurance 	<p>Statistics Windows</p> <ul style="list-style-type: none"> IAP Statistics Summary Per-IAP Statistics Network Statistics VLAN Statistics WDS Statistics Filter Statistics Station Statistics Per-Station Statistics <p>System Log Window</p> <p>IDS Event Log Window</p>
---	--

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

User Interface

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

Left frame **Right frame** **Array info**

XR4820 Wi-Fi Array **XIRRUS**

Status: Name: XR4012601C5B6 (10.100.54.55) Uptime: 5 days, 14 hours, 42 mins

Configuration

Express Setup

- Network
- Services
- VLANs
- Security
- SSIDs
- Groups
- IAPs

IAP Settings

- Global Settings
- Global Settings - 11a
- Global Settings - 11b
- Global Settings - 11n
- Advanced RF Settings
- Intrusion Detection
- LED Settings

WDS

- Filters
- Clusters

Tools

- Help
- System Tools
- CLI
- Options
- Logout

Log Messages

- Critical: 81
- Warning: 84
- Information: 244

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

Pull-down menu

Help

Log Message counters

Click to configure/view statistics

Copyright © 2005-2011 by Xirrus, Inc.

Figure 40. WMI: Frames

The left frame contains three main elements:

- Menu organized by function (for example, Network, SSIDs, Security, etc.). Click a heading, such as **Network**, to display a summary of its current configuration, as well as an associated pull-down menu. The three major menu sections (**Status**, **Configuration**, **Tools**) may each be collapsed down to hide the headings under them. Click again to display the headings. (Figure 41)
- Three **Log Messages** counters are located at the bottom of the menu. They provide a running total of messages generated by the ArrayOS Syslog subsystem during your session—organized into **Critical**, **Warning**, and **General** messages. Click on a counter to display the associated Syslog messages. Messages at the selected level or higher will be shown. For more information, please see “System Log Window” on page 142.
- The Array representation contains shortcut links. Click a radio to view statistics for it. Click the center of the Array to display the **IAP Settings** window, which allows you to configure the Array’s radios.

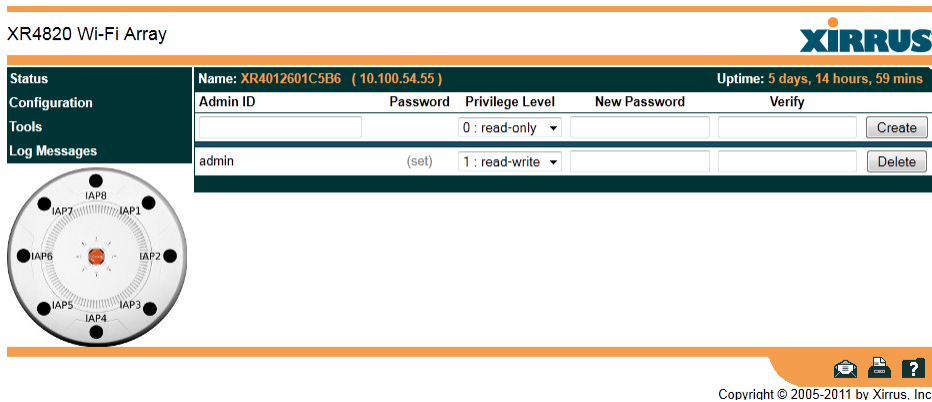


Figure 41. Major Menu Sections Collapsed (on left)

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

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



*Some settings are only available if the Array's license includes appropriate Xirrus **Advanced Feature Sets**. If a setting is unavailable (grayed out), then your license does not support the feature. See “**About Licensing and Upgrades**” on page 321.*

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

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

See “**Options**” on page 333 for more information.

Utility Buttons

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

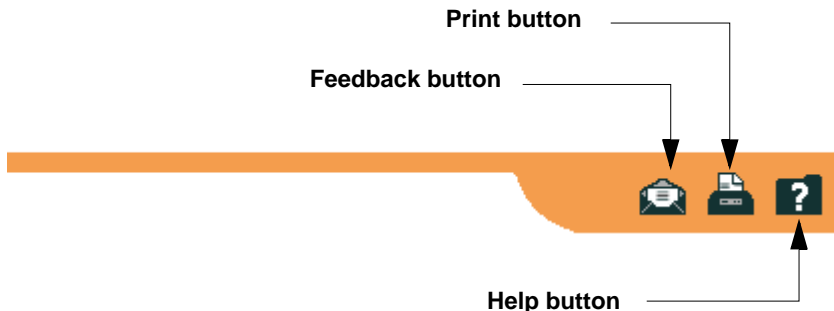


Figure 42. WMI: Utility Buttons

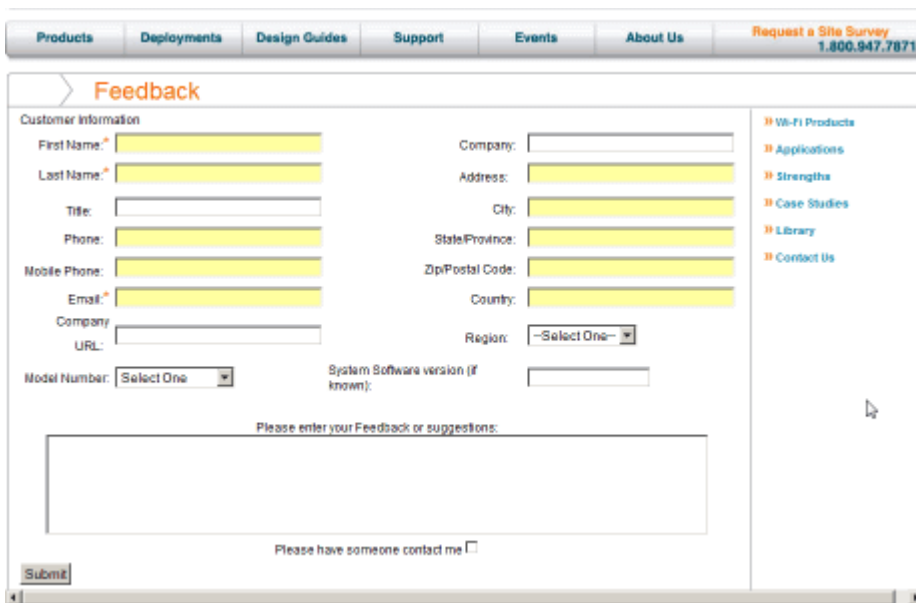
- Click on the **Feedback** button to generate a Web page that allows you to submit your comments to Xirrus, Inc. You can also access the feedback

page at <http://www.xirrus.com/public/feedback/>. Refer to Figure 43 on page 86 to see a sample of the feedback form.

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

Submitting Your Comments

When submitting comments via the Feedback button (Figure 43), ensure that you provide as much detail as possible, including your contact information, the product model number that the comment relates to, and the ArrayOS software version (if known). When finished, click on the **Submit** button to submit your comment.



The screenshot shows the XIRRUS Feedback Form. At the top, there is a navigation bar with links for Products, Deployments, Design Guides, Support, Events, About Us, and a Request a Site Survey button with the phone number 1.800.947.7871. The main heading is "Feedback".

The form is divided into two main sections: Customer Information and Feedback. The Customer Information section includes fields for First Name, Last Name, Title, Phone, Mobile Phone, Email, Company, URL, Company, Address, City, State/Province, Zip/Postal Code, Country, Region, Model Number (a dropdown menu), and System Software version (if known). The Feedback section includes a large text area for entering feedback or suggestions and a checkbox for "Please have someone contact me". A Submit button is located at the bottom left of the form.

On the right side of the form, there is a sidebar with a list of links: Wi-Fi Products, Applications, Strengths, Case Studies, Library, and Contact Us.

Figure 43. Feedback Form

Logging In

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

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

Otherwise, enter the Array's IP address. This may be determined as described in "Using the Ethernet Ports" on page 66.

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

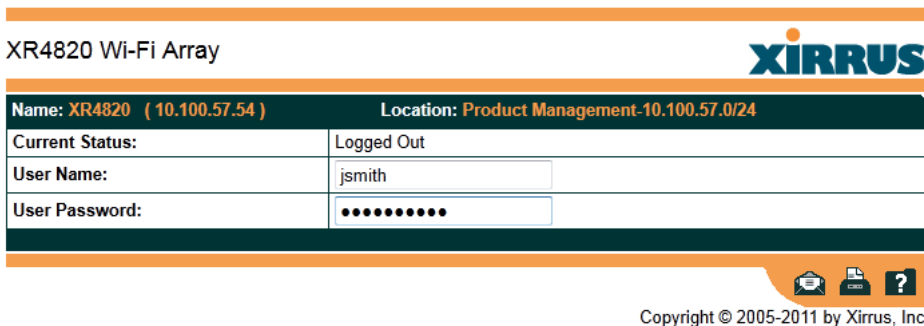


Figure 44. Logging In to the Wireless Array

Applying Configuration Changes

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

In both cases described above, the changes that you have made are not saved to the latest configuration file in the Array's flash memory, so they will not be restored after a reboot. Click the **Save changes to flash** button (located on the

upper right of each page) in order to make sure that these changes will be applied after rebooting. This will save the entire current configuration, not only the changes on current WMI page.

Character Restrictions

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

& < > ' " / \

Viewing Status on the Wireless 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 90](#)
- [“Network Status Windows” on page 97](#)
- [“RF Monitor Windows” on page 107](#)
- [“Station Status Windows” on page 118](#)
- [“Statistics Windows” on page 134](#)
- [“System Log Window” on page 142](#)
- [“IDS Event Log Window” on page 143](#)

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

- [“Configuring the Wireless Array” on page 147](#)
- [“Using Tools on the Wireless Array” on page 319](#)

Note that the **Status** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See [Figure 41](#) on [page 84](#))

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 Wireless 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.

XR4830 Wi-Fi Array												
Name: XR4012802207C (192.168.1.55)											Uptime: 0 days, 1 hours, 21 mins	
Ethernet Settings Summary												
Interface	State	Mgmt	LED	Auto Neg	Link	Duplex	Speed (Mbps)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	on	on	on	up	full	100	1500	enabled	192.168.1.55	255.255.255.0	192.168.1.254
gig2	enabled	on	on	on	down				enabled	192.168.1.55	255.255.255.0	192.168.1.254
Bond Settings Summary												
Bond	Mode	Ports	Active Vlans	Mirror								
bond1	link-backup	gig1 gig2	all	off								
bond2	link-backup		all	off								
Integrated Access Points												
IAP	State	AP Type	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link / Distance	MAC Address / BSSID	Description
iap1	up	11abgn 3x3	mon	dedicated monitor	abgn internal omni	monitor	20	-95	0		00:0f:7d:56:87:80	
iap2	up	11abgn 3x3	36	default	an internal directional	max	20	-90	0		00:0f:7d:56:87:90	
iap3	up	11abgn 3x3	1	default	bgn internal directional	max	20	-90	0		00:0f:7d:56:87:a0	
iap4	up	11abgn 3x3	44	default	an internal directional	max	20	-90	0		00:0f:7d:56:87:b0	
iap5	up	11abgn 3x3	6	default	bgn internal directional	max	20	-90	0		00:0f:7d:56:87:c0	
iap6	up	11abgn 3x3	52	default	an internal directional	max	20	-90	0		00:0f:7d:56:87:d0	
iap7	up	11abgn 3x3	11	default	bgn internal directional	max	20	-90	0		00:0f:7d:56:87:e0	
iap8	up	11abgn 3x3	60	default	an internal directional	max	20	-90	0		00:0f:7d:56:87:f0	

Figure 45. 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 Settings Summary**

This section provides information about network interface devices. To make configuration changes to these devices, go to “[Network Interfaces](#)” on page 157.

- **Interface:** Lists the network interfaces that are available on the Array: (gig1 and gig2).
- **State:** Shows the current state of each interface, either enabled or disabled.
- **Mgmt:** Shows whether Array management traffic is allowed on this interface.
- **Auto Neg:** Shows whether auto-negotiation is in use on this interface, to determine settings for speed, parity bits, etc.
- **LED:** Shows whether LED display of interface status is enabled.
- **Link:** Shows whether the link on this interface is up or down.
- **Duplex:** Shows whether full duplex mode is in use.
- **Speed:** Shows the speed of this interface in Mbps.
- **MTU Size:** Shows the Maximum Transmission Unit size that has been configured. This is the largest packet size (in bytes) that the interface can pass along.
- **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.

- **Bond Settings Summary**

This section provides information about the relationship that has been selected for the Gigabit ports. For detailed explanations and to make configuration changes, see [“Network Bonds” on page 160](#).

- **Bond:** Lists all network bonds that have been configured.
- **Mode:** Shows the type of relationship that has been selected for the Gigabit ports.
- **Ports:** Shows the Gigabit ports that are part of this bond.
- **Port Mode:** Shows the relationship that has been selected for the Ethernet ports. See [“Network Bonds” on page 160](#) for details
- **Active VLANs:** Shows the VLANs that are active in this bond.
- **Mirror:** Shows whether mirroring is enabled on this bond.

- **Integrated Access Points Section**

This section provides information about the Integrated Access Points (IAPs) that are contained within the Array. How many IAPs are listed depends on which product model you are using. To make configuration changes to these IAPs, go to [“IAP Settings” on page 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 46](#) shows an example where **iap7** is down.
- **AP Type:** Shows the types of 802.11 clients supported by this IAP (11/a/b/g/n) and the number of separate data streams transmitted and received by the antennas of each IAP for 802.11n. For example, 3x3 means that the IAP supports three transmit chains and three receive chains. See [“Multiple Data Streams—Spatial Multiplexing” on page 37](#).

Integrated Access Points												
IAP	State	AP Type	Channel	WiFi Mode	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS Link / Distance	MAC Address / BSSID	Description
iap1	up	.11abgn 3x3	161 default	an	internal directional	max	20	-90	0		00:0f:7d:44:0f:01	
iap2	up	.11abgn 3x3	56 default	an	internal directional	small	5	-75	0		00:0f:7d:44:0f:11	
iap3	up	.11abgn 3x3	11 manual	gn	internal directional	small	5	-75	0		00:0f:7d:44:0f:21	
iap4	up	.11abgn 3x3	48 default	an	internal directional	small	5	-75	0		00:0f:7d:44:0f:31	
iap5	up	.11abgn 3x3	153 default	an	internal directional	small	5	-75	0		00:0f:7d:44:0f:41	
iap6	up	.11abgn 3x3	mon default	abgn	internal omni	monitor	20	-95	0		00:0f:7d:44:0f:51	
iap7	down	.11abgn 3x3	1 default	gn	internal directional	small	5	-75	0		00:0f:7d:44:0f:61	
iap8	up	.11abgn 3x3	40 default	an	internal directional	small	5	-75	2		00:0f:7d:44:0f:71	

Figure 46. 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](#).
- Wi-Fi Mode:** Shows the 802.11 client types that the IAP has been configured to support.
- 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 26](#).

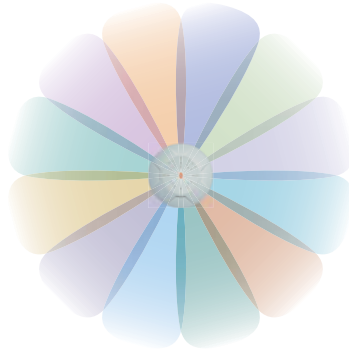


Figure 47. IAP Cells

- **Tx Power:** Shows the transmit power for each IAP.
- **Rx Threshold:** Shows the receive threshold for each IAP.
- **Stations:** Informs you how many client stations are currently associated with each IAP. XN Arrays can handle up to 96 concurrent users per individual IAP, thus 16-port XN models can handle 1536 users per Array.
- **WDS Link/Distance:** The WDS Link on this radio (if any), and whether the link has been set to support [Long Distance Links](#). See “WDS” on page 302.
- **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 and fan speed.

Note that the **License Features** row lists the features that are supported by your Array's license. See "About Licensing and Upgrades" on page 321 and "Advanced Feature Sets" on page 14 for more information.


XR4830 Wi-Fi Array			
Status	Name: XR4830 (10.100.57.51)		Location: Product Management-10.100.57.0/24 Uptime: 10 days, 3 hours, 6 mins
▼ Array			Save changes to flash
Summary	Hardware Configuration		
Information	Model	XR4830, 1.0GB-ECC (700MHz)	
Configuration	Component	Part Number	Serial Number
Admin History	System	XR4830	XR4012601C7ED
▶ Network	Controller	100-0114-001.7	0000116717
▶ RF Monitor	IAP Module 1	100-0119-002.02	0200002342
▶ Stations	IAP Module 2	100-0119-002.02	0200002338
▶ Statistics	IAP Module 3	100-0119-002.02	0200002337
System Log	IAP Module 4	100-0119-002.02	0200002099
IDS Event Log	IAP Module 5	100-0119-002.02	0200002333
Configuration	IAP Module 6	100-0119-002.02	0200002340
Express Setup	IAP Module 7	100-0119-002.02	0200002344
▶ Network	IAP Module 8	100-0119-002.02	0200002341
▶ Services	FPGA Status	Boot Version	SW Version
▶ VLANs	Switching Engine	3000-00.010	3000-00.010
▶ Security	Interface	MAC Address(es)	
▶ SSIDs	IAPs	00:0f:7d:44:0f:00-44:0f:7f	
▶ Groups	Gigabit 1	00:0f:7d:01:c7:ed	
IAPs	Gigabit 2	00:0f:7d:01:c7:ee	
WDS	Software Configuration		
Filters	Component	Version	
Clusters	SCD Firmware	3.07 (Jun 1 2011), Build: 4166	
Tools	Boot Loader	6.0.0 (Jul 2 2011), Build: 6022	
Help	IAP Driver	3.1.0 (Aug 26 2011), Build: 2736	
System Tools	System Software	6.0.1 (Aug 27 2011), Build: 3089	
CLI	License Key	135B5-TAALQ-K7JQQ-D6E20	
Options	License Features	ArrayOS 6.0 for 8 3x3 IAPs + RF Performance Manager + RF Analysis Manager + RF Security Manager + 802.11n	
Logout	Operating Status		
Log Messages	Time This Boot	Fri 2011-Sep-16 01:25:46 GMT	
Critical 1478	Time Last Boot	Fri 2011-Sep-16 00:57:21 GMT	
	Component	Temperature °C (F)	
	Controller	55 (131.0)	
	Fan Speed	2040 RPM ()	

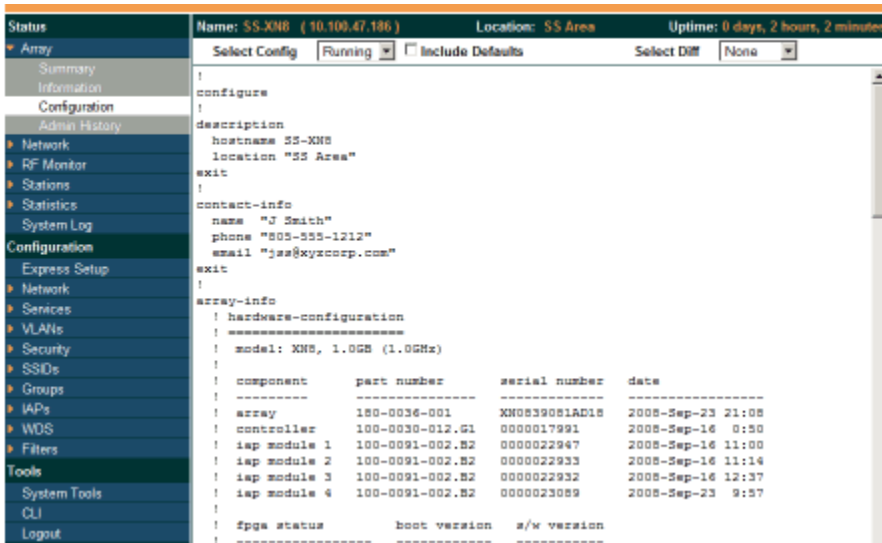
Figure 48. Array Information

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

Array Configuration

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

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



```

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

!
configure
!
description
hostname SS-X08
location "SS Area"
exit
!
contact-info
name "J Smith"
phone "805-555-1212"
email "jss@xyzcorp.com"
exit
!
array-info
! hardware-configuration
! =====
! model: X08, 1.0GB (1.0GHz)
!
!
! component      part number      serial number     date
! -----
! array          100-0036-001     XH0839081AD18    2008-Sep-23 21:08
! controller    100-0030-012.G1 0000017991        2008-Sep-16  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 0000023059        2008-Sep-23  9:57
!
!
! fpga status      boot version      s/w version
! -----
    
```

Figure 49. 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.X700 [10.100.47.100]		Location: S5 Area		Uptime: 4 days, 0 hours, 50 minutes		
▼ Array	User	IP Address	Interface	Via	Login Time	Logout Time	Session Time D:H:M
Summary	admin	10.100.21.55	VM1	https	Dec-09 12:59	active	0:02:05
Information	admin	10.100.21.55	VM1	https	Dec-09 11:54	active	0:03:10
Configuration	admin	10.100.21.55	VM1	https	Dec-09 10:16	active	0:04:48
Admin History	admin	10.100.21.55	VM1	https	Dec-08 10:15	Dec-09 10:15	
► Network	admin	10.100.21.55	VM1	https	Dec-05 14:41	Dec-08 10:16	
► RF Monitor	admin	10.100.21.55	VM1	https	Dec-05 14:12	active	4:00:52
► Stations							
► Statistics							
System Log							
Configuration							
Express Setup							
► Network							
► Services							
► VLANs							

Figure 50. Admin Login History

Network Status Windows

The following Network Status windows are available:

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

- **CDP Neighbors**—lists neighboring network devices using Cisco Discovery Protocol.
- **Network Assurance**—shows results of connectivity tests for network servers.

Network

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

XR6830 Wi-Fi Array

Status Name: Robin-VW-XR6830 (10.100.48.65) Uptime: 2 days, 19 hours, 35 mins

Array Save changes to flash

Network		Ethernet Settings Summary										
Interface	State	Mgmt	LED	Auto Neg	Link	Duplex	Speed (Mbps)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	on	on	on	down			1500	disabled	10.100.48.65	255.255.255.0	10.100.48.1
gig2	enabled	on	on	on	down			1500	disabled	10.100.48.65	255.255.255.0	10.100.48.1
gig3	enabled	on	on	on	up	full	1000	1500	disabled	10.100.48.65	255.255.255.0	10.100.48.1
gig4	enabled	on	on	on	up	full	1000	1500	disabled	10.100.48.65	255.255.255.0	10.100.48.1
Bond Settings Summary												
Bond	Mode	Ports		Active Vlans		Mirror						
bond1	link-backup	gig1 gig2		all		off						
bond2	link-backup	gig3		all		off						
bond3	link-backup	gig3		all		off						
bond4	link-backup	gig4		all		off						
DNS Settings Summary												
Hostname	Domain	DNS Server 1			DNS Server 2			DNS Server 3				
Robin-VW-XR6830												

Figure 51. Network Settings

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


- “Network Interfaces” on page 157
- “Network Bonds” on page 160
- “DNS Settings” on page 167
- “CDP Settings” on page 168

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: XR4830 (10.100.57.51)		Location: Product Management 10.100.57.0/24		Uptime: 3 days, 11 hours, 58 mins						
Network Map		Save changes to flash										
Network		Hardware	License	Software	Firmware	IAP Info	Stations	Default	Auto Refresh	Refresh		
Network Map		Array Name	IP Address	Location	Array OS	IAP	Up	SSID	On	In Range	Fast Room	Uptime D:MM
Spanning Tree Status		Dirks-XH12-Array	10.100.23.205	Glass House	XS-6.1-dgates	12	12	2	2	yes	tunnel	2:05:17
Routing Table		Dirks-XH4-Array	10.100.23.213	Glass House	XS-6.1-dgates	4	4	2	2	yes	tunnel	2:05:17
ARP Table		Dirks-XNB-Array	10.100.23.207	Glass House	XS-6.1-dgates	8	8	2	2	yes	tunnel	2:05:17
DHCP Leases		Dirks-XR16.3x3	10.100.23.29	Unknown	XR-6.1-dgates	16	16	1	1	yes	tunnel	2:05:16
Connection Tracking		Dirks-XR8.3x3-1	10.100.23.14	Glass House	XR-6.1-dgates	8	7	1	1	yes	tunnel	2:05:16
CDP Neighbors		Dirks-XR8.3x3-2	10.100.23.22	Glass House	XR-6.1-dgates	8	8	1	1	yes	tunnel	2:05:17
Network Assurance		Dirks-XS16-Array	10.100.23.204	Glass House	XS-6.1-dgates	16	16	2	2	yes	tunnel	2:05:17
RF Monitor		XNB-1	10.100.57.52	Product Management-10.100.57.0/24	XS-5.1.1-1633	8	0	2	1	yes	off	12:16:13
Stations		XNB-2	10.100.57.53	Product Management-10.100.57.0/24	XS-5.1.1-1633	8	0	2	0	no	tunnel	16:12:44
Statistics		XR4420	10.100.57.55	Product Management-10.100.57.0/24	XR-6.0.2-3097	8	0	1	1	no	tunnel	4:16:45
System Log		XR4820	10.100.57.54	Product Management-10.100.57.0/24	XR-6.0.2-3097	8	0	2	1	no	tunnel	4:16:46
IDS Event Log		XR4830	10.100.57.51	Product Management-10.100.57.0/24	XR-6.0-asmith	8	8	1	1	yes	tunnel	3:11:58
		xir-ih-wlan2	10.100.10.7	Xirus, Thousand Oaks, North Cube area	XS-5.1.2-1639	12	12	3	3	yes	tunnel	2:15:00

Figure 52. Network Map

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

Content of the Network Map Window

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

- **Array Name:** The host name assigned to the Array. To establish the host name, go to “[Express Setup](#)” on page 149. 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 149.

- **Location:** The location assigned to the Array. To establish the location information, go to [“Express Setup” on page 149](#).
- **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 149](#). 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 231](#).
- **(SSID) On:** Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to [“SSID Management” on page 231](#).
- **In Range:** Informs you whether the Array is within wireless range of another Wireless 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:** 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 119](#).

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

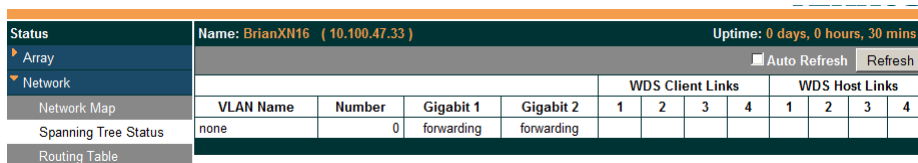
Default

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

Spanning Tree Status

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

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



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

Figure 53. Spanning Tree Status

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

See Also

[Network](#)

[Network Interfaces](#)

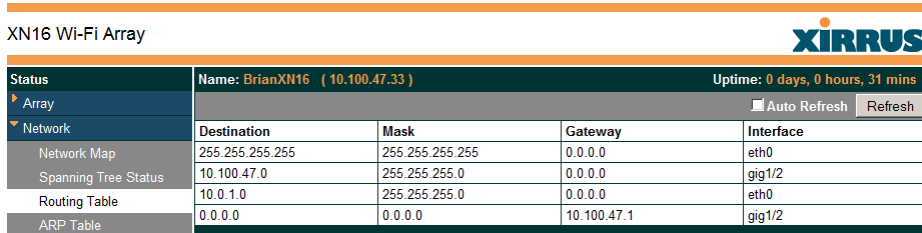
[Network Status Windows](#)

[VLANs](#)

[WDS](#)

Routing Table

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



The screenshot shows the XN16 Wi-Fi Array interface with the Routing Table selected. The table displays the following data:

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

Figure 54. Routing Table

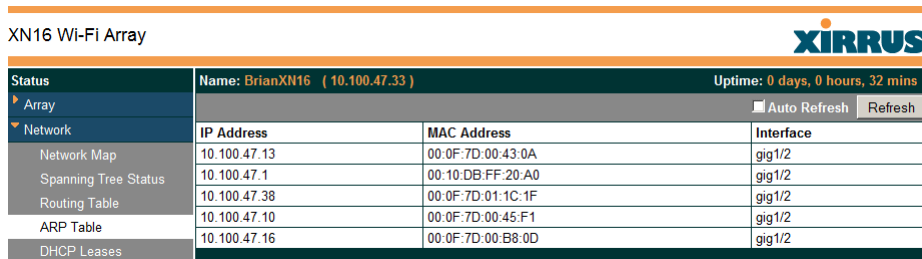
See Also

VLANs

Configuring VLANs on an Open SSID

ARP Table

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



The screenshot shows the XN16 Wi-Fi Array interface with the ARP Table selected. The table displays the following data:

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

Figure 55. ARP Table

See Also

Routing Table

ARP Filtering

DHCP Leases

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

IP Address	MAC Address	Start Time	End Time	Time Left	Host Name
192.168.1.254	00:21:00:5e:ab:8b	Dec-09 15:50:11	Dec-09 15:55:11	0 days 0:03:20	Shelly-PC

Figure 56. 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.

Type	State	Outbound Traffic						Return Traffic						Use	
		Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	State	Source IP	Destination IP	Src Port	Dst Port	Packets		Bytes
udp		10.100.47.10	255.255.255.255	39127	22610	1	220	Unreplied	255.255.255.255	10.100.47.10	22610	39127	0	0	1
udp		10.100.47.16	10.100.40.137	60161	22610	1	214	Unreplied	10.100.40.137	10.100.47.16	22610	60161	0	0	1
udp		10.100.47.16	10.100.47.33	15004	15003	995	87688	Assured	10.100.47.33	10.100.47.16	15003	15004	995	87688	1
udp		10.100.46.16	10.100.47.16	41319	161	211873	74205993	Assured	10.100.47.16	10.100.46.16	161	41319	211873	87025111	1
udp		10.100.47.16	10.110.37.8	60161	22610	1	214	Unreplied	10.110.37.8	10.100.47.16	22610	60161	0	0	1
udp		10.100.47.16	10.100.1.13	48391	162	1	229	Unreplied	10.100.1.13	10.100.47.16	162	48391	0	0	1
udp		10.100.47.16	255.255.255.255	60161	22610	1	214	Unreplied	255.255.255.255	10.100.47.16	22610	60161	0	0	1

Figure 57. Connection Tracking

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

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

See Also

Filters

CDP Neighbors

This status-only window lists devices on the Array's network that support the Cisco Discovery Protocol (CDP).

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

Figure 58. CDP Neighbors

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

CDP must be enabled on the Array in order to gather and display this information. For details and some restrictions, see "CDP Settings" on page 168.

Network Assurance

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

Status	Name: BrianXN16 (10.100.47.33)			Uptime: 0 days, 0 hours, 29 mins
<ul style="list-style-type: none"> ▸ Array ▾ Network <ul style="list-style-type: none"> Network Map Spanning Tree Status Routing Table ARP Table DHCP Leases Connection Tracking CDP Neighbors Network Assurance 	<input type="checkbox"/> Auto Refresh Refresh			
	Setting	Hostname	IP Address	Status
	DNS server 1		10.100.1.10	Connectivity OK
	DNS server 2		10.100.2.10	Connectivity OK
	NTP primary server	ntp.xirrus.com	72.18.205.156	Connectivity OK
	SNMP trap host 1	Xirrus-XMS	10.100.1.13	Connectivity OK
	gig1 IP gateway		10.100.47.1	Connectivity OK
	gig2 IP gateway		10.100.47.1	Connectivity OK

Figure 59. Network Assurance

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

Network assurance must be enabled on the Array in order to perform these connectivity tests and display this information. See “Management Control” on page 203.

See Also

Management Control

RF Monitor Windows

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

The following RF Status windows are available:

- **IAPs**—displays current statistics and RF measurements for each of the Array's IAPs.
- **Spectrum Analyzer**—displays current statistics and RF measurements for each of the Array's channels.
- **Intrusion Detection**—displays rogue APs that have been detected by the Array.
- **Channel History**—charts ongoing statistics and RF measurements for one selected channel over time.
- **Radio Assurance**—displays counts of types of problems that caused each IAP to reset.



*Some status information is only available if the Array's license includes **Advanced Feature Sets**. For example, the Spectrum Analyzer requires the **Xirrus Advanced RF Analysis Manager (RAM)**. If a feature is unavailable, then your license does not support the feature and you will get an error message if you try to set the feature. See "**About Licensing and Upgrades**" on page 321.*

IAPs

The RF Monitor—IAPs window displays traffic statistics and RF readings observed by each Array IAP (radio). Note that the data is an instantaneous snapshot for the IAP—it is not an average or a cumulative total. To graph these values over time for a particular channel, see “Channel History” on page 114. For detailed information on the measurements displayed, please see “Spectrum Analyzer Measurements” on page 111.

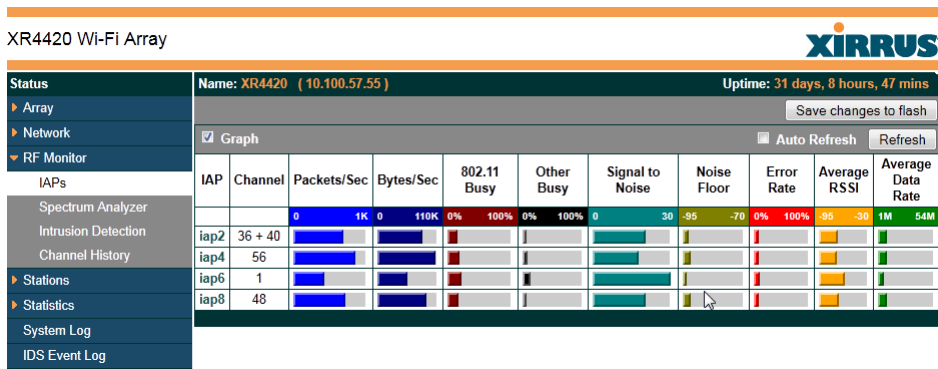


Figure 60. RF Monitor—IAPs

Figure 60 presents the data as a graphical display, enabled by selecting the **Graph** checkbox on the upper left. If this option is not selected, data is presented as a numerical table.

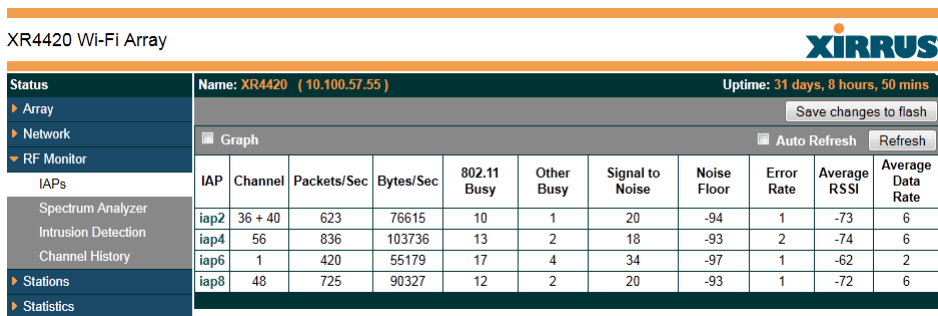



Figure 61. RF Monitor—IAPs

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

Spectrum Analyzer



*The RF measurements for this feature are obtained by the monitor radio. You **must** have a radio set to **monitor** mode for any data to be available. See “IAP Settings” on page 256.*

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

The RF Spectrum Analyzer window displays instantaneous traffic statistics and RF readings for all channels, as measured by the Array’s monitor radio. This differs from the RF Monitor-IAPs window, which displays values measured by each IAP radio for its current assigned channel. For the spectrum analyzer, the monitor radio is in a listen-only mode, scanning across all wireless 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 62](#) (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in “Spectrum Analyzer Measurements” on page 111.

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

Select Display Options Click Channel number to highlight

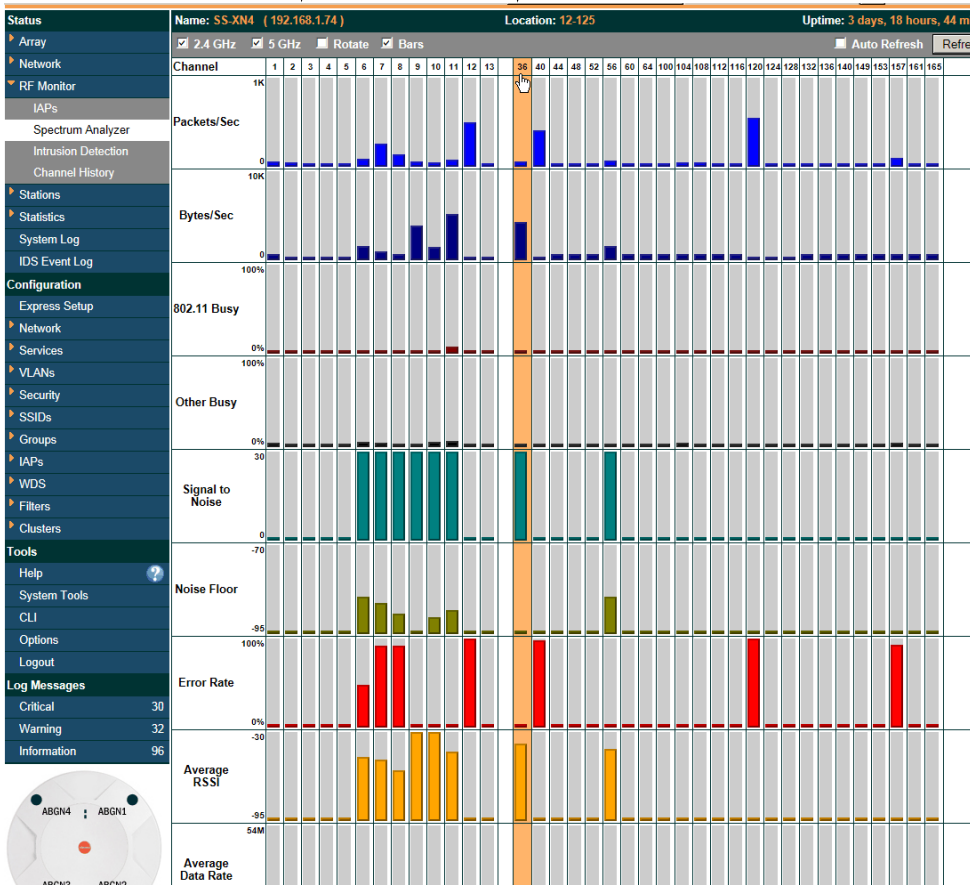



Figure 62. RF Spectrum Analyzer

The Spectrum Analyzer offers several display options:

- To display horizontal bar graphs, click the **Rotate** checkbox at the bottom of the data window.
- In the rotated view, if you wish to view data as a numerical table, click the **Text** checkbox. Click again to return to a graphical display. The text option is only available in the rotated view.

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

Spectrum Analyzer Measurements

The spectrum analyzer displays the following information:

- | ● **Packets/Sec:** Total number of wireless packets per second on the channel, both valid and errored packets.
- | ● **Bytes/Sec:** Total number of wireless 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 wireless packets seen on the channel that have CRC errors. The Error rate percentage may be high on

some channels since the monitor radio is set to receive at a very sensitive level, enabling it to hear packets from devices at far distances.

- **Average RSSI:** Average RSSI level seen on 802.11 packets received on the channel. A dash value “-” means no RSSI data was available for the interval.
- **Average Data Rate:** Average data rate over time (per byte, not per packet) seen on 802.11 packets received on the channel. A dash value “-” means no data rate information was available for the interval. A higher data rate (above 6 Mbps) typically indicates user data traffic on the channel. Otherwise, the data rate reflects control packets at the lower basic rates.

Intrusion Detection

This window displays all detected access points, according to the classifications you select from the checkboxes at the top—**Blocked**, **Unknown**, **Known**, or **Approved**. This includes ad hoc access points (station-to-station connections). For more information about intrusion detection, rogue APs, and blocking, please see “About Blocking Rogue APs” on page 294.

Classify APs

Select APs to Display

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

Figure 63. Intrusion Detection/Rogue AP List

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

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

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

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

See Also

[Network Map](#)

[Rogue Control List](#)

[SSIDs](#)

[SSID Management](#)

Channel History

The RF Monitor—Channel History window focuses on traffic statistics and RF readings observed for just one channel that you select in the **Channel** field. A new set of readings is added every 10 seconds for a 5 GHz channel, or every 5 seconds for a 2.4 GHz channel. For descriptions of the measurements displayed, please see “Spectrum Analyzer Measurements” on page 111.

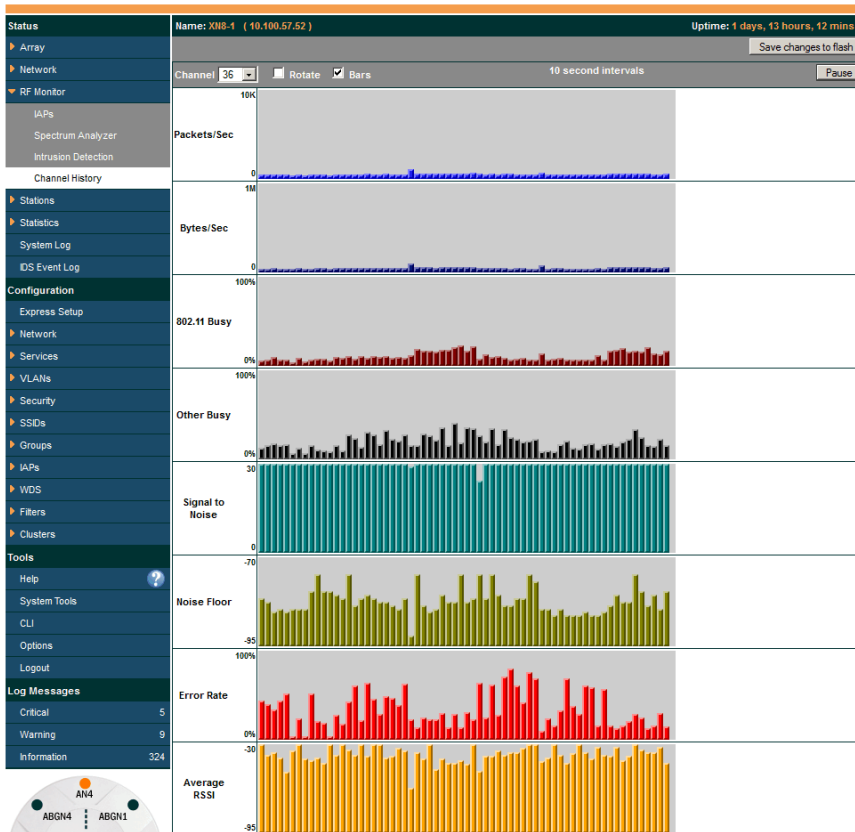


Figure 64. RF Monitor—Channel History

Figure 64 presents the data in graphical form. New data appears at the left, with older readings shifting to the right. To make the data appear as a barchart, click the **Bar** checkbox which will shade the background.

You also have the option of clicking the **Rotate** checkbox to give each statistic its own column. In other words, the graph for each statistic will grow down the page as new readings display at the top. (Figure 65)

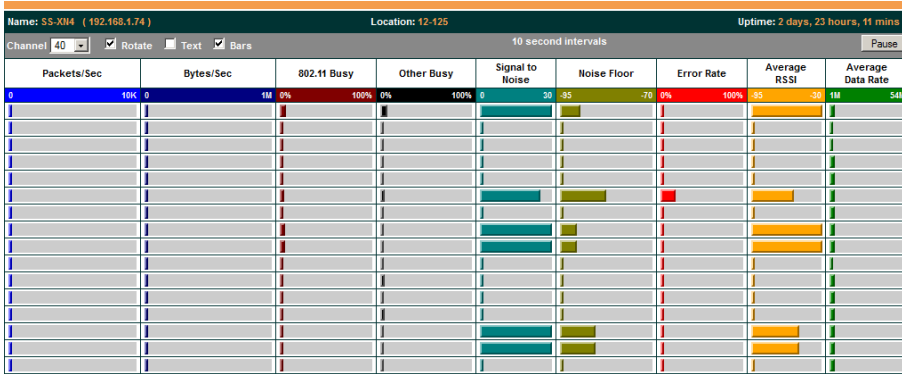


Figure 65. RF Monitor—Channel History (Rotated)

If you select **Rotate** and **Text** together, data is presented as a numerical table. (Figure 66)

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

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

Figure 66. RF Monitor—Channel History (Text)

Radio Assurance



Radio Assurance mode is only available if the Array's license includes the Xirrus Advanced RF Analysis Manager (RAM). If a setting is unavailable (grayed out), then your license does not support the feature. Please see "About Licensing and Upgrades" on page 321.

When Radio Assurance mode is enabled, the monitor radio performs loopback tests on the Array's radios. When problems are encountered, the Array can take various actions to correct them by performing different levels of reset on the affected radio. This window shows which resets, if any, have been performed on which radios since the last reboot.

The Array's response to radio problems is controlled by the **Radio Assurance Mode** selected, as described in "RF Resilience" on page 284. If you have selected **Failure Alerts & Repairs** (with or without reboots), then the Array can take corrective action if a problem is detected. Note that radio assurance requires RF Monitor Mode to be enabled in [Advanced RF Settings](#) to turn on self-monitoring functions. It also requires a radio to be set to monitoring mode. For a detailed discussion of the operation of this feature and the types of resets performed, see "Radio Assurance" on page 421.

Status	Name: XR4830 (10.100.57.51)		Location: Product Management-10.100.57.0/24							
▶ Array	Save changes to flash									
▶ Network										
▼ RF Monitor						IAP Reset Counts by Type				
	IAP	State	AP Type	Channel	WiFi Mode	Monitor	Beacon	Phy	MAC	System
IAPs	iap1	down	.11abgn 3x3	161	an	0	0	0	0	0
Spectrum Analyzer	iap2	down	.11abgn 3x3	56	an	0	0	0	0	0
Intrusion Detection	iap3	down	.11abgn 3x3	11	gn	0	0	0	0	0
Channel History	iap4	down	.11abgn 3x3	48	an	0	0	0	0	0
Radio Assurance	iap5	down	.11abgn 3x3	153	an	0	0	0	0	0
	iap6	down	.11abgn 3x3	mon	abgn	0	0	0	0	0
▶ Stations	iap7	down	.11abgn 3x3	1	gn	0	0	0	0	0
▶ Statistics	iap8	up	.11abgn 3x3	40	an	0	0	0	0	0

Figure 67. Radio Assurance

For each of the Array's radios, this window shows the radio's state, its type (IEEE 802.11 type and antenna type—2x2 or 3x3), the assigned channel, and the selected 802.11 wireless mode. To the right, the table shows counts for the number of

times, if any, that radio assurance has performed each of the following types of resets since the last reboot, as described in [Radio Assurance](#):

- Monitor
- Beacon
- Phy
- MAC
- System (i.e., reboot the Array)

See Also

IAPs

Xirrus Advanced RF Analysis Manager (RAM)

RF Resilience

Radio Assurance

Station Status Windows

The following Station Status windows are available:

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



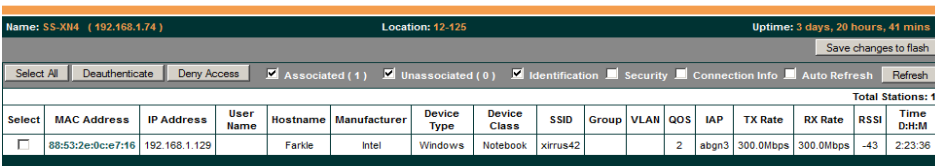
Some status information is only available if the Array’s license includes the Xirrus Advanced RF Analysis Manager (RAM). If a feature is unavailable, then your license does not support the feature and you will get an error message if you try to set the feature. See “About Licensing and Upgrades” on page 321.

Stations

This status-only window shows client stations currently visible to the Array. You may choose to view only stations that have **Associated** to the Array, or only stations that are **Unassociated**, or both, by selecting the appropriate checkboxes above the list. The list always shows the MAC address of each station, its IP address, the SSID used for the association, the **Group** (if any) that this station belongs to, its VLAN, its QoS, the IAP used for the association, transmit and receive rates, the **RSSI** for each station, and how long each association has been active (up time).


You may click other checkboxes above the list to show a number of additional columns:

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



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

Figure 68. 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 209 and delete the station from the **Deny** list.
- **Deauthenticate:** Sends a de-authentication frame to the selected station. The station may re-authenticate.

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

See Also

Access Control List

Station Status Windows

Location Map

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

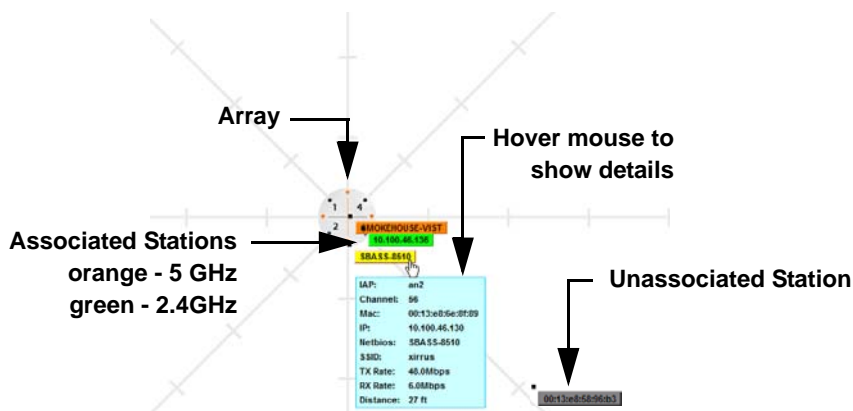


Figure 69. Location Map

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

A station is identified by the type of **Preferred Label** that you select: **Netbios Name**, **IP Address**, **MAC Address**, or **Manufacturer**. If multiple stations are near each other, they will be displayed slightly offset so that one station does not completely obscure another. You may minimize a station that is not of interest by clicking it. There is also a **Minimize All** button.

You may replace the range-finder background image above with your own custom image of the floorplan of the area served by the Array—see “Working with the Custom Image” on page 124

Hover the mouse over a station to show detailed information. (Figure 69) For a station that is associated to this Array, the details include:

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

Controls and items displayed on the Location Map window



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

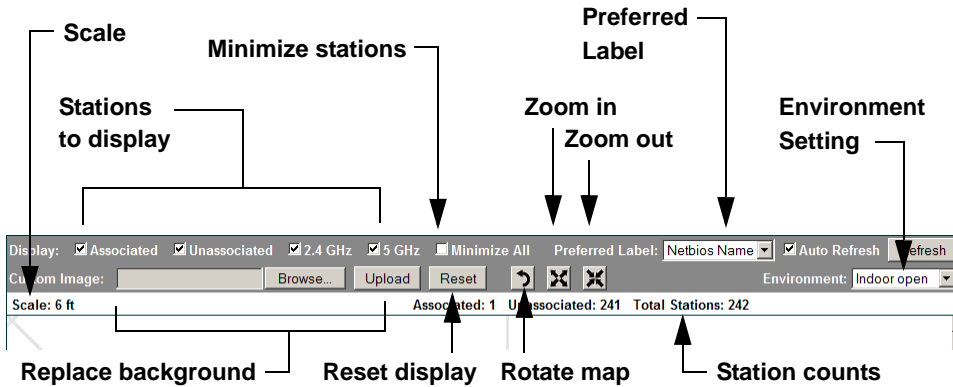


Figure 70. Controls for Location Map

- **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. (Figure 71) You may still display detailed information for the station by hovering over it. To enlarge all rectangles, clear the Minimize All checkbox.
- **Preferred Label:** This field is located on the top of the window towards the right. It selects the type of label to be displayed for stations: **Netbios Name**, **IP Address**, **MAC Address**, or **Manufacturer**. If you select NetBIOS (this is the default), then that name, if known, will be used to label each Array. Else, its IP or MAC address will be used, in that order.
- **Auto Refresh:** Instructs the Array to refresh this window automatically.
- **Refresh:** Updates the stations displayed.

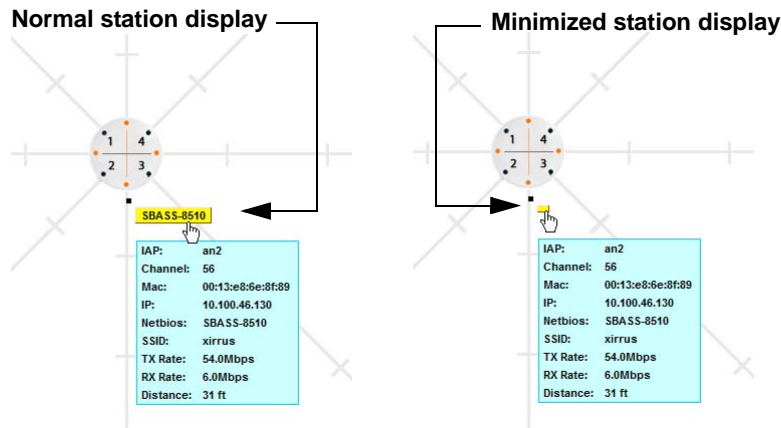





Figure 71. Minimizing stations

- **Custom Image:** Use this feature to replace the default background image with your own image of the floor plan of your location. Click the **Browse** button and browse to the desired file on your computer. This may be a .gif, .jpg, .jpeg, .png, .htm, or .html file. The scale of the file should be 100 feet per inch. Then click **Upload** (see below). For more information on using the custom, image, see “Working with the Custom Image” on page 124.
- **Upload:** After browsing to the desired custom image, click the **Upload** button to install it. The map is redisplayed with your new background. No hash marks (for the map scale) are added to the image display.
- **Reset:** Click this button to restore the map display to the factory settings. All attributes are restored—including the stations selected for display, the scale, the rotation, and the background map.
-  **Rotate:** Click this button to rotate the orientation of the entire map. It rotates the map 45° counter-clockwise.
-  **Enlarge:** Click this button to enlarge (zoom in on) the map. The displayed **Scale** is updated with the new scale for the map.
-  **Reduce:** Click this button to reduce (zoom out on) the map. The displayed **Scale** is updated with the new scale for the map.

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

See Also

Station Status Windows

Working with the Custom Image

After you have uploaded a custom image (see **Custom Image** and **Upload** in “Controls and items displayed on the Location Map window” on page 122), you should move the display of the Array on your map to correspond with its actual location at your site.

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

RSSI

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

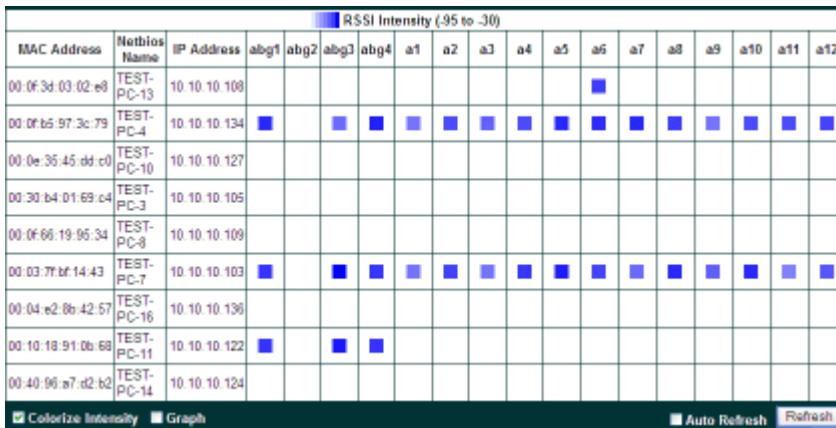


Figure 72. Station RSSI Values

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 72) If you select **Graph**, then the RSSI is shown on a representation of the Array, either colorized or numerically based on your selection. (Figure 73) The stations are listed to the left of the Array—click on a station to show its RSSI values on the Array.

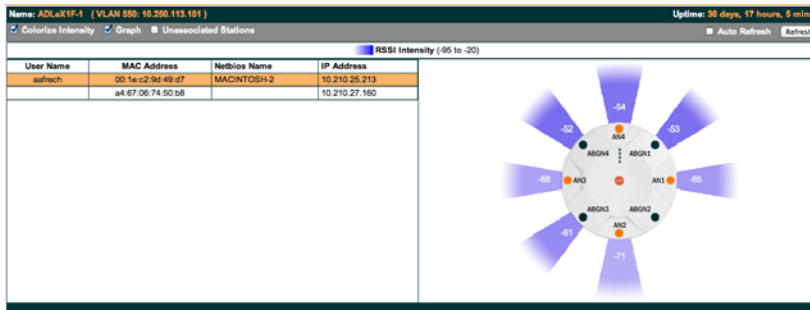


Figure 73. Station RSSI Values—Colorized Graphical View

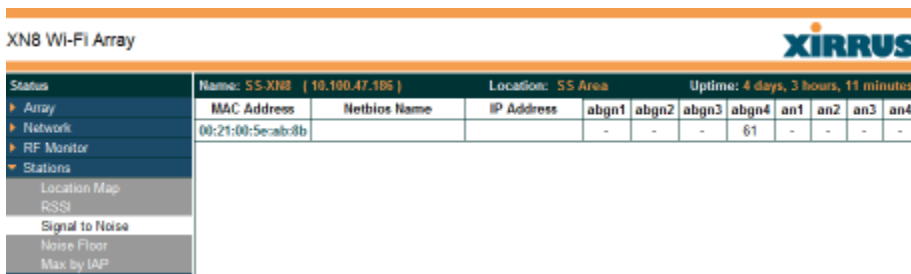
In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to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



XN8 Wi-Fi Array		Name: SS-XN8 (10.100.47.186)		Location: SS Area		Uptime: 4 days, 3 hours, 11 minutes					
Status	MAC Address	Netbios Name	IP Address	abgn1	abgn2	abgn3	abgn4	an1	an2	an3	an4
<ul style="list-style-type: none"> ▶ Array ▶ Network ▶ RF Monitor ▶ Stations Location Map RSSI Signal to Noise Noise Floor Max by IAP 	00:21:00:5e-abc8b			-	-	-	61	-	-	-	-

Figure 74. 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 74) You may display the relative value using color if you select **Colorize Intensity**, with the highest SNR indicated by the most intense color. (Figure 75) If you select **Graph**, then the SNR is shown on a representation of the Array, either colorized or numerically based on your selection. The stations are listed to the left of the Array—click on a station to show its SNR values on the Array.

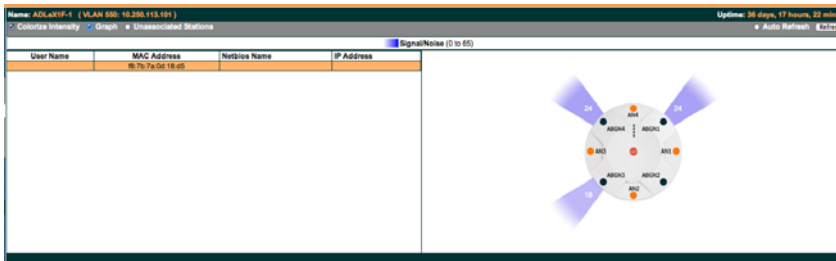


Figure 75. Station SNR Values—Colorized Graphical View

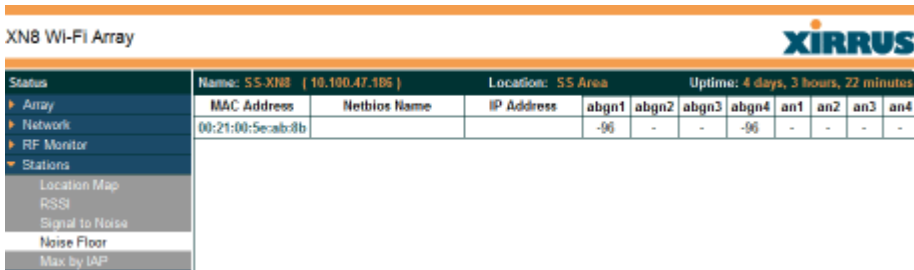
In either graphical or tabular view, you may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon . Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to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

See Also

- Station Status Windows
- RF Monitor Windows

Noise Floor

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



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

Figure 76. 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 76) 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 77) The stations are listed to the left of the Array—click on a station to show its values on the Array.

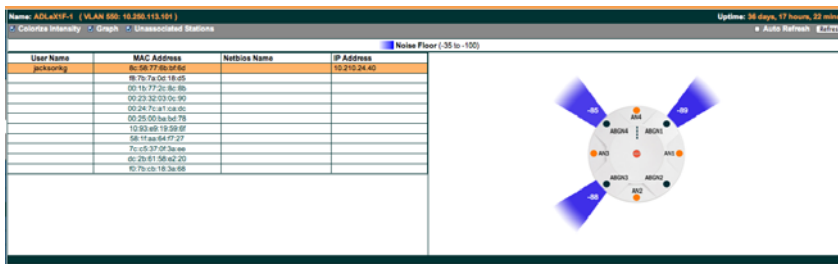


Figure 77. Station Noise Floor Values—Colorized Graphical View

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.

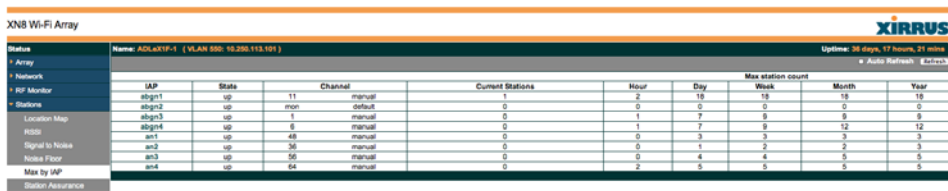
See Also

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.



IAP	State	Channel	Current Stations	Max station count				
				Hour	Day	Week	Month	Year
abgn1	up	11	1	2	18	18	18	18
abgn2	up	mon	0	0	0	0	0	0
abgn3	up	1	0	1	7	9	9	9
abgn4	up	6	0	1	7	9	12	12
an1	up	48	0	3	3	3	3	3
an2	up	56	0	1	2	2	2	2
an3	up	50	0	0	4	4	5	5
an4	up	64	0	2	5	5	5	5

Figure 78. Max by IAP

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

See Also

[IAPs](#)

[Station Status Windows](#)

Station Assurance

Station assurance monitors the quality of the connections that users are experiencing on the wireless network. This window shows client stations that have had connectivity issues. You may enable or disable the station assurance feature and set thresholds for the problems that it checks, such as excessive packet retry or packet error rates, or stations that are unable to stay associated to the Array. Please see “Station Assurance” on page 288 for more information about these settings. When the Array detects that a station has reached the threshold value for one or more of the issues checked, it adds the station to this page. In addition, an event is triggered, a trap is generated, and a Syslog message is logged.

For each station, this list shows the MAC address, its IP address, its host name, its device type, device class, and manufacturer. It also shows the values of the various statistics that were monitored for problems as described in “Station Assurance” on page 288: associated time, authentication failures, packet error rate, packet retry rate, packet data rate, RSSI, signal to noise ratio (SNR), and distance.

Name: ADLArray-1 (VLAN 600:10.210.113.101)													Uptime: 58 days, 17 hours, 30 mins		
Time	MAC Address	IP Address	Hostname	Device Type	Device Class	Manufacturer	Assoc. Time	Auth Fails	Error Rate	Retry Rate	Data Rate	RSSI (dB)	SNR (dB)	Distance (ft)	
Oct03 01 42	10:30:0b:19:88:df	10.210.5.42		IPad	Tablet	Apple	12			26	6			683	
Oct03 07 30	a4:d1:d2:4a:aa:ea	10.210.26.44	Library-IPad-TV	IPad	Tablet	Apple	7			30	6				
Oct03 07 05	28:e0:2c:31:e4:93	10.210.26.154		Mac	Notebook	Apple		426		30	6		9	543	
Oct03 04 09	88:c8:63:aa:04:af	10.210.27.189		IPad	Player	Apple				29	6				
Oct03 02 04	00:23:3d:8c:8b:da			IPad	Notebook	Apple				6	6				
Oct03 02 03	00:1f:3a:8c:5d:c4			Windows	Notebook	Hon Hai				0	6				
Oct03 01 59	88:4b:4a:7d:21:6c	10.210.24.32		android	Phone	Motorola	21			28	6				
Oct03 01 58	00:20:83:3a:aa:ea					Apple				28	6				
Oct03 01 55	10:83:e8:5a:31:8f	10.210.24.144		IPad	Tablet	Apple	28			30	6				
Oct03 01 47	24:ab:81:1b:aa:65	10.210.26.157		Barnes-iPhone	iPhone	Apple	21			30	6				
Oct03 01 42	00:20:83:0b:84:81	10.210.26.71		iPhone	Phone	Apple	15	6		27	6		9		
Oct03 01 36	00:20:83:3a:8d:d5			iPhone	Phone	Apple				35	3				
Oct03 01 29	a4:d1:d2:3a:5b:63			IPad	Tablet	Apple	27			30	6				
Oct03 01 17	a4:d7:06:87:67:d3	10.210.24.157		IPad	Tablet	Apple	9			30	6				
Oct03 00 32	78:ea:39:af:b8:ed			iPhone	Phone	Apple	30			30	6			609	
Oct03 00 25	00:23:0f:06:8d:68	10.210.6.261				Apple				28	3				
Oct03 00 24	00:20:41:75:ab:2c	10.210.25.190	Heathens-iPod	IPod	Player	Apple				28	6				
Oct03 00 07	90:27:44:a3:2a:ef			IPod	Player	Apple				6	6				
Oct02 23 03	8c:5b:77:4e:a3:84			iPhone	Phone	Apple				6	6				
Oct02 23 47	8c:5b:77:7f:31:84	10.210.27.85	Crista-iPhone	iPhone	Phone	Apple	12			30	6				
Oct02 23 46	00:21:8c:4b:8d:9d	10.210.4.160		Windows	Notebook	Intel				31	6				
Oct02 23 40	24:ab:81:e3:2a:8b	10.210.4.86		iPhone	Phone	Apple	26			30	6		8	543	
Oct02 23 39	04:0c:ca:4b:8c:09			iPhone	Phone	Apple	28			38	6		8	787	
Oct02 23 33	28:8a:ca:05:1b:c7			IPad	Tablet	Apple				38	6				
Oct02 23 31	a4:d7:06:83:06:33			IPad	Tablet	Apple				38	6			609	
Oct02 23 29	50:ea:09:4e:50:48	10.210.26.89		iPhone	Phone	Apple				42	6				
Oct02 23 18	a9:18:47:fa:cc:ea			iPhone	Phone	Apple				42	6				
Oct02 23 13	18:7b:7a:8b:20:99	10.210.4.143		android	Phone	Motorola				40	9		8	609	
Oct02 23 09	14:3a:04:4b:5b:0c	10.210.26.106	Owen-r-iPhone	iPhone	Phone	Apple	18			28	6			543	
Oct02 23 08	24:ab:81:c1:2a:3a			iPhone	Phone	Apple	20			30	6				
Oct02 23 08	00:28:4b:2b:1e:04	10.210.5.110		iPhone	Phone	Apple	29			27	9				
Oct02 23 04	78:ea:39:af:b8:ed			Windows	Notebook	Apple	24			30	6				
Oct02 23 02	00:24:3a:7b:a0:42			Windows	Notebook	Hon Hai				29	6			543	
Oct02 23 01	18:e7:1d:d3:83:75			IPod	Player	Apple				28	6				
Oct02 23 01	a9:1a:8d:ad:4e:18			Windows	Notebook	Universal Display Scientific				29	6			543	
Oct02 22 58	00:28:e7:3a:8e:24			Windows	Notebook	Intel				28	3			543	
Oct02 22 44	0c:7d:c2:ac:32:7d			iPhone	Phone	Apple				28	6				
Oct02 22 44	88:4b:4a:84:95:12			android	Phone	Motorola				28	6				

Figure 79. Station Assurance

You may click the **Clear Inactive** button to remove stations that are no longer connected to the Array from the list. Click the **Clear All** button to remove all

entries and start fresh to add problem stations to the list as they are detected. Click on the **Refresh** button to refresh the station list, or click **Auto Refresh** to instruct the Array to refresh this window automatically.

See Also

IAPs

Station Status Windows

Station Assurance

Statistics Windows

The following Array Statistics windows are available:

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

IAP Statistics Summary

This is a status only window that provides an overview of the statistical data associated with all IAPs. It also shows the channel used by each IAP. For detailed statistics for a specific IAP, see “Per-IAP Statistics” on page 135. Click the **Unicast Stats Only** checkbox on the lower left to filter the results, or clear the checkbox to show statistics for all wireless traffic.

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

XN8 Wi-Fi Array XIRRUS

Status Uptime: 56 days, 17 hours, 53 mins

Name: AOL-x11f-1 (VLAN 600: 10.200.110.101) Auto Refresh Refresh Clear

Array Unicast State Drop

Network

RF Monitor

Statistics

Statistics for IAP All

IAP	Channel	Receive Statistics by IAP			Transmit Statistics by IAP				
		Bytes	Packets	Errors	Bytes	Packets	Errors		
abgn1	11	5720283200	61728875	4546643	4846625	8048014052	155860978	4205817	4824145
abgn2	0	20991037779	190325842	98380245	601	502000983	7429508	47727	0
abgn3	1	2307602832	18076955	28208835	1205957	5204830844	141745848	1781901	1840564
abgn4	6	748380011	72831116	54401623	3340115	5555748454	142511370	4043359	3412567
an1	48	772236568	526829	502484	240384	4277388147	158751675	48833	241505
an2	38	187705058	5611511	1167699	215848	40705735874	128153613	41954	151696
an3	56	498415787	3049982	144165520	223931	40780007743	120994491	49187	193793
an4	64	228622880	8762052	119642384	618648	45385128139	131743275	209319	488219

IAP abgn1
IAP abgn2
IAP abgn3
IAP abgn4
IAP an1
IAP an2
IAP an3
IAP an4

Figure 80. IAP Statistics Summary Page

See Also

System Log Window

Global Settings (IAP)

Global Settings .11an

Global Settings .11bgn

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 134. 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 83.

Name: SS-X188 [10.100.47.186]		Location: SS Area		Uptime: 4 days, 3 hours, 39 minutes	
Statistics for IAP abg4					
Receive Statistics			Transmit Statistics		
Total Bytes	8848640898	Total Bytes	1976503120		
Total Packets	197226805	Total Packets	7034604		
Unicasts	25841	Unicasts	106		
Multicasts	0	Multicasts	15180		
Broadcasts	102409705	Broadcasts	42755		
Mgmt Packets	0	Mgmt Packets	7225222		
Beacons	94791259	Beacons	6976563		
Fragments	0	Fragments	0		
RTS Count	0	RTS Count	0		
CTS Count	0	CTS Count	0		
Receive Errors & Retries			Transmit Errors & Retries		
Total Errors	9533147	Total Errors	14015458		
Total Retries	5820027	Total Retries	0		
Dropped Packets	24	Dropped	8212136		
Unassociated	0	Unassociated	0		
CRC	3711363	ACK Failures	6803322		
Fragment Errors	0	RTS Failures	0		
Encryption Errors	1484	RTS Retries	0		
Duplicates	249	Single Retries	0		
Overruns	0	Multiple Retries	6804862		
<input type="checkbox"/> Display Percentages		<input type="checkbox"/> Auto Refresh		Refresh	Clear

Figure 81. Individual IAP Statistics Page

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

See Also

- System Log Window
- Global Settings (IAP)
- Global Settings .11an
- Global Settings .11bgn
- IAPs

Network Statistics

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

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

Figure 82. Network Statistics

See Also

[DHCP Server](#)

[DNS Settings](#)

[Network](#)

[Network Interfaces](#)

VLAN Statistics

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

Status	Name: SS-XNB (10.100.47.186)	Location: SS Area	Uptime: 4 days, 3 hours, 59 minutes
Array	VoIP (12) Statistics Clear		
Network	Receive Bytes	0	Transmit Bytes 0
RF Monitor	Receive Packets	0	Transmit Packets 0
Stations	Receive Compressed	0	Transmit Compressed 0
Statistics	Receive Multicast	0	Transmit Carrier Errors 0
IAP	Receive Dropped	0	Transmit Dropped 0
Network	Receive FIFO Errors	0	Transmit FIFO Errors 0
VLAN	Receive Frame Errors	0	Transmit Collisions 0
WDS	Receive Total Errors	0	Transmit Total Errors 0
Filter	Finance (5) Statistics Clear		
Stations	Receive Bytes	0	Transmit Bytes 3313440
System Log	Receive Packets	0	Transmit Packets 5616
Configuration	Receive Compressed	0	Transmit Compressed 0
Express Setup	Receive Multicast	0	Transmit Carrier Errors 0
Network	Receive Dropped	0	Transmit Dropped 0
Services	Receive FIFO Errors	0	Transmit FIFO Errors 0
VLANs	Receive Frame Errors	0	Transmit Collisions 0
Security	Receive Total Errors	0	Transmit Total Errors 0
SSIDs	Clear All Auto Refresh Refresh		
Groups			
IAPs			

Figure 83. VLAN Statistics

See Also

VLAN Management
VLANs

WDS Statistics

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

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

Figure 84. WDS Statistics

See Also

SSID Management

WDS

Filter Statistics

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

Name	Type	State	Packets	Bytes
Global	allow	on	1961	268436

Figure 85. 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 141.

Station	Receive Statistics by Station				Transmit Statistics by Station			
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
00:0E:3d:03:02:a8	693119	2043	0	223	2368	12	0	1
00:0E:b5:07:3c:79	51442645153	52791337	0	5371975	65480578303	65515091	26764	118569632
00:0e:35:45:d8:e0	1691913717	24210701	0	8748417	168562071943	164832863	112870	104185667
00:30:b4:01:69:c4	1004756270	10171896	0	0	265914094203	259348067	10303	48599772
00:0E:66:19:95:34	1550292533	5009662	0	1202533	36006965880	36032055	309651	41933995
00:03:76:b6:14:43	197116974748	195875363	0	32942200	277967033447	2668865001	45170	60729663
00:04:a2:8b:42:57	323018216404	312187936	0	29556244	507270199576	492647649	12040	39468662
00:10:18:91:0e:66	181652416042	177651569	0	18383672	264062154029	263394451	170454	36038464
00:40:96:a7:82:b2	249090923768	247980426	0	22610375	276050170214	270423992	18482	127696107

Figure 86. 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 140.

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

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

Rate	Receive Statistics				Transmit Statistics				
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries	
1	1015465	18726	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
5.5	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0
6	3728543	77325	0	15	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
12	1710	5	0	3	0	0	0	0	0
18	1726	5	0	2	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0
36	5959	22	0	2	0	0	0	0	0
48	73724	228	0	29	0	0	0	0	0
54	693119	2043	0	223	2358	12	0	1	1
Total	6520246	98354	0	274	2358	12	0	1	1

Clear Auto Refresh Refresh

Figure 87. Individual Station Statistics Page

See Also

Station Statistics

System Log Window

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

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

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

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

Figure 88. System Log (Alert Level Highlighted)

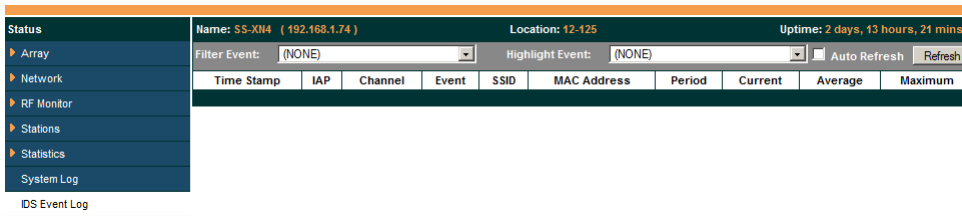
Use the **Highlight Priority** field if you wish to highlight messages at the selected priority level. Click on the **Refresh** button to refresh the message list, or click on the **Clear All** button at the upper left to delete all messages. You can also click in the **Auto Refresh** check box to instruct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

Note that there is a shortcut way to view system log messages. If you click **Log Messages** near the bottom of the left hand frame, WMI displays counts of log messages at different severity levels. Click a count to display just those messages in the System Log window. See [Figure 40 on page 83](#) for more information.

IDS Event Log Window

This status only window displays the Intrusion Detection System (IDS) Event log, listing any detected attacks on your network. For descriptions of the types of attacks detected, as well as the settings to fine-tune IDS on the Array, please see “Intrusion Detection” on page 291.

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



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

Figure 89. IDS Event Log

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

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

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

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

Use this Space for Your Notes





Configuring the Wireless 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 149](#)
- [“Network” on page 156](#)
- [“Services” on page 170](#)
- [“VLANs” on page 185](#)
- [“Security” on page 190](#)
- [“SSIDs” on page 224](#)
- [“Groups” on page 246](#)
- [“IAPs” on page 253](#)
- [“WDS” on page 302](#)
- [“Filters” on page 308](#)
- [“Clusters” on page 314](#)

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



*Some settings are only available if the Array's license includes appropriate Xirrus **Advanced Feature Sets**. If a setting is unavailable (grayed out), then your license does not support the feature. See [“About Licensing and Upgrades” on page 321](#).*

Note that the **Configuration** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See [Figure 41 on page 84](#).)

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 Wireless Array” on page 89](#)**
- **[“Using Tools on the Wireless Array” on page 319](#)**

Express Setup

Use the Express Setup page to establish global configuration settings that enable basic Array functionality. Any changes you make in this window will affect all radios.

Status		Name: XR40140026956 (10.100.48.61)		Uptime: 0 days, 12 hours, 56 mins	
Array		Save changes to flash			
Network		Host Name:	XR40140026956		
RF Monitor		Location Information:			
Stations		Admin Contact:			
Statistics		Admin Email:			
System Log		Admin Phone:			
IDS Event Log		License Key:	0KDFT-4DRNP-FUMN		Apply
Configuration		SNMPv2 Settings			
Express Setup		Enable SNMPv2:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Network		Read Only Community String:	*****		
Services		Read Write Community String:	*****		
VLANs		Gigabit Ethernet 1 Settings			
Security		Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
SSIDs		Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Groups		Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static		
IPs		IP Settings:	Address: 10.100.48.61	Subnet Mask: 255.255.255.0	Default Gateway: 10.100.48.1
WDS		Apply			
Filters		Gigabit Ethernet 2 Settings			
Clusters		Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Tools		Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
Help		Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static		
System Tools		IP Settings:	Address: 10.100.48.61	Subnet Mask: 255.255.255.0	Default Gateway: 10.100.48.1
CLI		Apply			
Options		SSID Settings			
Logout		SSID (Wireless Network Name):			
Log Messages		Wireless Security:	Open		
Critical 8		Apply SSID Settings			
Warning 9		Admin Settings			
Information 57		New Admin User (Replaces user "admin"):			
		New Admin Privilege Level:	1: read-write		
		New Admin Password:			
		Confirm Admin Password:			
		Apply Admin Settings			
		Time and Date Settings			
		Current Array Date and Time:	Mon Mar 12 2012 08:42:09		
		Time Zone:	(GMT) Greenwich Mean Time: Dublin, Lisbon, London		
		Auto Adjust Daylight Savings:	<input type="checkbox"/>		
		Use Network Time Protocol:	<input checked="" type="radio"/> Yes <input type="radio"/> No		
		NTP Primary Server:	time.nist.gov		
		NTP Primary Authentication:	None		
		NTP Primary Authentication Key ID:	1		
		NTP Primary Authentication Key:			
		NTP Secondary Server:	pool.ntp.org		
		NTP Secondary Authentication:	None		
		NTP Secondary Authentication Key ID:	2		
		NTP Secondary Authentication Key:			
		IAP Settings			
		Enable/Configure All IAPs:	Execute		



Figure 90. WMI: Express Setup

When finished, click **Save changes to flash** if you wish to make your changes permanent.

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. **License Key:** If Xirrus issued you a license that differs from the current value shown, enter it now.
7. **Configure SNMP:** Select whether to **Enable SNMPv2** on the Array, and set the SNMPv2 community strings. The factory default value for the **Read-Only Community String** is `xirrus_read_only`. The factory default value for the **Read-Write Community String** is `xirrus`. If you are using the Xirrus Management System (XMS), the read-write string must match the string used by XMS. XMS also uses the default value `xirrus`.
8. **Configure the Gigabit Ethernet network interface settings.** Please see “Network Interfaces” on page 157 for more information.

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

- a. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.

- **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 191.

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

- e. Click **Apply SSID Settings** when done.
- 10. Admin Settings:** This section allows you to change the default admin username, password, and privileges for the Array. You may change the password and leave the user name as is, but we suggest that you change both to improve Array security.
- a. **New Admin User (Replaces user “admin”):** Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the Array also offers the option of authenticating administrators using a RADIUS server (see “Admin Management” on page 196).
 - b. **New Admin Privilege Level:** By default, the new administrator will have read/write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see “Admin Privileges” on page 198. Take care to make sure to leave yourself enough read/write privileges on at least one account to be able to administer the Array.
 - c. **New Admin Password:** Enter a new administration password for managing this Array. If you forget this password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
 - d. **Confirm Admin Password:** If you entered a new administration password, confirm the new password here.
 - e. Click **Apply Admin Settings** when done.
- 11. Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you’re not using a server.
- a. **Current Array Date and Time:** This read-only field shows the current time for your convenience.

- b. Time Zone:** Select your time zone from the choices available in the pull-down list.
- c. Auto Adjust Daylight Savings:** If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
- d. Use Network Time Protocol:** Check this box if you want to use an [NTP](#) server to synchronize the Array's clock. Use of NTP is mandatory for Arrays to be managed with XMS (the Xirrus Management System), and ensures that Syslog time-stamping is maintained across all units. Without using an NTP server (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies. If you select **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, select **No** (default) and set the system time on the Array manually.
- e. NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
- f. NTP Primary Authentication:** (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default). For more information on authenticated NTP, see "Time Settings (NTP)" on page 171.
- g. NTP Primary Authentication Key ID:** Enter the key ID, which is a decimal integer.
- h. NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- i. NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

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

12. 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.

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

Network

This is a status-only window that provides a snapshot of the configuration settings currently established for the Ethernet 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.

XR4830 Wi-Fi Array

Status	Name: Robin-XR4830 (10.100.48.24)		Uptime: 0 days, 0 hours, 49 mins										
Array	Save changes to flash												
Network	Ethernet Settings Summary												
RF Monitor	Interface	State	Mgmt LED	Auto Neg	Link	Duplex	Speed (Mbps)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway	
Stations	gig1	enabled	on	on	on	up	full	1000	1500	disabled	10.100.48.24	255.255.255.0	10.100.48.1
Statistics	gig2	enabled	on	on	on	down			1500	disabled	10.100.48.24	255.255.255.0	10.100.48.1
System Log	Bond Settings Summary												
IDS Event Log	Bond	Mode	Ports	Active Vlans	Mirror								
Configuration	bond1		link-backup	gig1 gig2	all	off							
	bond2		link-backup		all	off							
Express Setup	DNS Settings Summary												
Network	Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3								
	Robin-XR4830												
Interfaces	CDP Settings Summary												
Bonds	State	Interval	Hold Time										
DNS	Enabled	60	180										

Figure 91. Network Interfaces

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

- [“Network Interfaces” on page 157](#)
- [“Network Bonds” on page 160](#)
- [“DNS Settings” on page 167](#)
- [“CDP Settings” on page 168](#)

See Also

[DNS Settings](#)

[Network Interfaces](#)

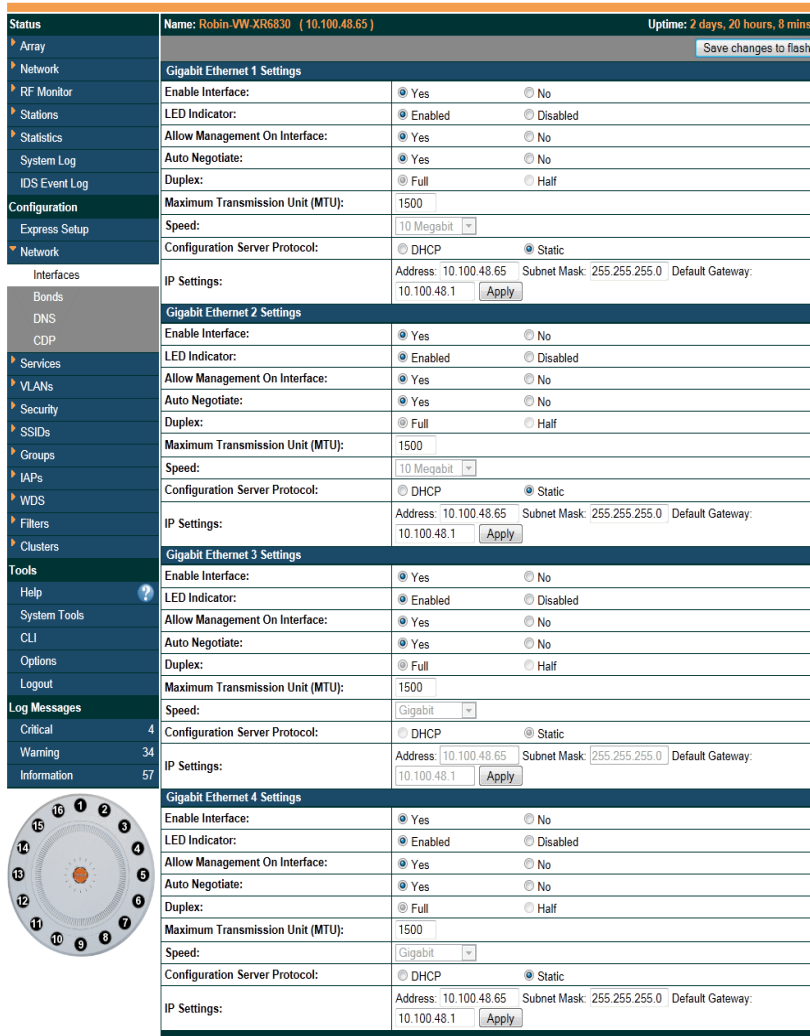
[Network Status Windows](#)

[Spanning Tree Status](#)

[Network Statistics](#)

Network Interfaces

XR-1000 and XR-2000 Series Arrays have one Gigabit Ethernet interface, while XR-4000 Series Arrays have two, and XR-6000 Series models have four. This window allows you to establish configuration settings for these interfaces.



The screenshot displays the network configuration page for a device named "Robin-VW-XR6830 (10.100.48.65)" with an uptime of 2 days, 20 hours, and 8 minutes. The interface is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes sections for Status, Network, Configuration, Tools, and Log Messages. The main configuration area is titled "Gigabit Ethernet Settings" and contains four identical configuration blocks for Gigabit Ethernet 1, 2, 3, and 4. Each block includes settings for Enable Interface, LED Indicator, Allow Management On Interface, Auto Negotiate, Duplex, Maximum Transmission Unit (MTU), Speed, Configuration Server Protocol, and IP Settings. The IP Settings field includes fields for Address, Subnet Mask, and Default Gateway, along with an "Apply" button. A "Save changes to flash" button is located at the top right of the configuration area. A circular navigation dial is visible in the bottom left corner of the screenshot.

Status	Name: Robin-VW-XR6830 (10.100.48.65)	Uptime: 2 days, 20 hours, 8 mins
Array	Save changes to flash	
Network	Gigabit Ethernet 1 Settings	
RF Monitor	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Stations	LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Statistics	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
System Log	Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No
IDS Event Log	Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half
Configuration	Maximum Transmission Unit (MTU):	1500
Express Setup	Speed:	10 Megabit
Network	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Interfaces	IP Settings:	Address: 10.100.48.65 Subnet Mask: 255.255.255.0 Default Gateway: 10.100.48.1 <input type="button" value="Apply"/>
Bonds	Gigabit Ethernet 2 Settings	
DNS	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
CDP	LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Services	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
VLANs	Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Security	Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half
SSIDs	Maximum Transmission Unit (MTU):	1500
Groups	Speed:	10 Megabit
IAPs	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
WDS	IP Settings:	Address: 10.100.48.65 Subnet Mask: 255.255.255.0 Default Gateway: 10.100.48.1 <input type="button" value="Apply"/>
Filters	Gigabit Ethernet 3 Settings	
Clusters	Enable Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
Tools	LED Indicator:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Help	Allow Management On Interface:	<input checked="" type="radio"/> Yes <input type="radio"/> No
System Tools	Auto Negotiate:	<input checked="" type="radio"/> Yes <input type="radio"/> No
CLI	Duplex:	<input checked="" type="radio"/> Full <input type="radio"/> Half
Options	Maximum Transmission Unit (MTU):	1500
Logout	Speed:	Gigabit
Log Messages	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
Critical 4	IP Settings:	Address: 10.100.48.65 Subnet Mask: 255.255.255.0 Default Gateway: 10.100.48.1 <input type="button" value="Apply"/>
Warning 34	Gigabit Ethernet 4 Settings	
Information 57	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
	Maximum Transmission Unit (MTU):	1500
	Speed:	Gigabit
	Configuration Server Protocol:	<input type="radio"/> DHCP <input checked="" type="radio"/> Static
	IP Settings:	Address: 10.100.48.65 Subnet Mask: 255.255.255.0 Default Gateway: 10.100.48.1 <input type="button" value="Apply"/>

Figure 92. Network Settings

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

Network Interface Ports

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

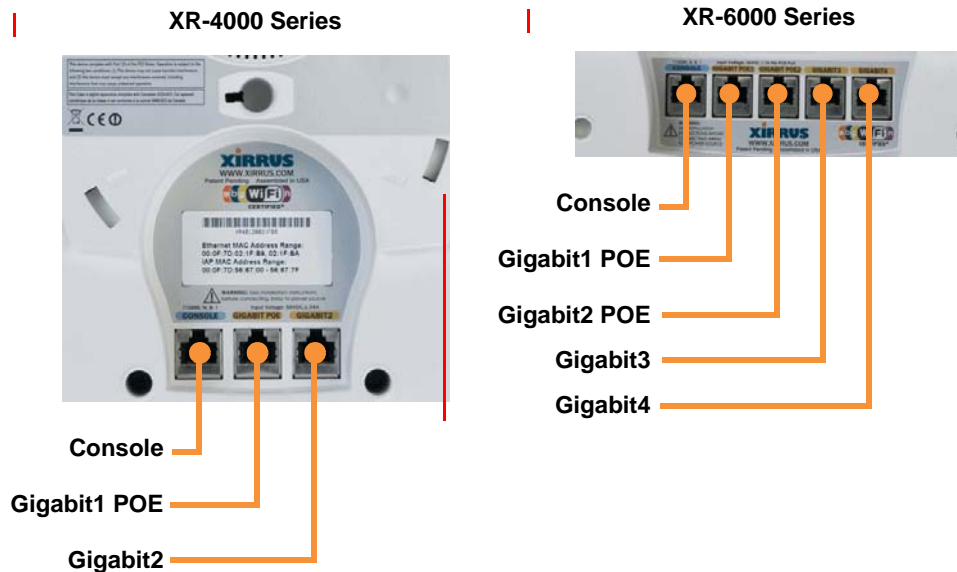


Figure 93. Network Interface Ports

Procedure for Configuring the Network Interfaces

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

1. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.
2. **LED Indicator:** Choose **Enabled** to allow the LED for this interface to blink with traffic on the port, or choose **Disabled** to turn the LED off.

The LED will still light during the boot sequence, then turn off. This option is only available for the Gigabit interfaces.

3. **Allow Management on Interface:** Choose **Yes** to allow management of this Array via the selected network interface, or choose **No** to deny all management privileges for this interface.
4. **Auto Negotiate:** This feature allows the Array to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available).
 - a. **Duplex:** Full-duplex mode transmits data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). Half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.
 - b. **MTU:** the Maximum Transmission Unit size. This is the largest packet size (in bytes) that the interface can pass along.
 - c. **Speed:** If the Auto-Negotiate feature is disabled, you must manually choose the desired data transmission speed from the pull-down list. For configuring the Gigabit interfaces the options are **10 Megabit** or **100 Megabit**. (Note that 1000 Megabit speed can only be set by Auto-Negotiation.)
5. **Configuration Server Protocol / IP Settings:** 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. **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.

Status		Name: Robin-VW-XR6830 (10.100.48.65)	Uptime: 2 days, 20 hours, 12 mins
Array	Save changes to flash		
Network	Bond 1 Settings		
RF Monitor	Bond Mode:	Active backup (gig ports fail over to each other) ▾	
Stations	Bond Ports:	<input checked="" type="checkbox"/> Gig 1 <input checked="" type="checkbox"/> Gig 2 <input type="checkbox"/> Gig 3 <input type="checkbox"/> Gig 4	
Statistics	Active VLANs:	all	
System Log	Set Active VLANs:	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="All"/> <input type="button" value="None"/> <input type="button" value="Current"/>	
IDS Event Log	Mirror:	Off ▾	
Configuration	Bond 2 Settings		
Express Setup	Bond Mode:	Active backup (gig ports fail over to each other) ▾	
Network	Bond Ports:	<input type="checkbox"/> Gig 1 <input type="checkbox"/> Gig 2 <input type="checkbox"/> Gig 3 <input type="checkbox"/> Gig 4	
Interfaces	Active VLANs:	all	
Bonds	Set Active VLANs:	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="All"/> <input type="button" value="None"/> <input type="button" value="Current"/>	
DNS	Mirror:	Off ▾	
CDP	Bond 3 Settings		
Services	Bond Mode:	Active backup (gig ports fail over to each other) ▾	
VLANs	Bond Ports:	<input type="checkbox"/> Gig 1 <input type="checkbox"/> Gig 2 <input checked="" type="checkbox"/> Gig 3 <input type="checkbox"/> Gig 4	
Security	Active VLANs:	all	
SSIDs	Set Active VLANs:	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="All"/> <input type="button" value="None"/> <input type="button" value="Current"/>	
Groups	Mirror:	Off ▾	
IAPs	Bond 4 Settings		
WDS	Bond Mode:	Active backup (gig ports fail over to each other) ▾	
Filters	Bond Ports:	<input type="checkbox"/> Gig 1 <input type="checkbox"/> Gig 2 <input type="checkbox"/> Gig 3 <input checked="" type="checkbox"/> Gig 4	
Clusters	Active VLANs:	all	
Tools	Set Active VLANs:	<input type="text"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="All"/> <input type="button" value="None"/> <input type="button" value="Current"/>	
	Mirror:	Off ▾	

Figure 94. Network Bonds

Procedure for Configuring Network Bonds

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

1. **Bond Mode:** Select the desired behavior for a set of bonded 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 Resource Center](#).

The modes below describe the relationship between a set of Gigabit ports—for example, load balancing or active backup. Use the **Bond Ports** field to select the ports that are bonded (set in [Step 2](#)). Two or more ports may be bonded. In Arrays that have four Gigabit ports, you have the option of bonding all four ports together. **True??** In this discussion, we

call two ports that are bonded **Gigabitx** and **Gigabit y**. [x Shelly - paginate and check refs for XR and XN versions!!](#)

- a. **Active Backup (gig ports fail over to each other)**—This mode provides fault tolerance and is the default mode. Gigabitx acts as the primary link. Gigabit y is the backup link and is passive. Gigabit y assumes the IP properties of Gigabitx. If Gigabitx fails, the Array automatically fails over to Gigabit y. When a failover occurs in this mode, Gigabit y issues gratuitous ARPs to allow it to substitute for Gigabitx at Layer 3 as well as Layer 2. See Figure 95 (a). [??Are more than 2 ports in this bond OK? How would it work??](#)

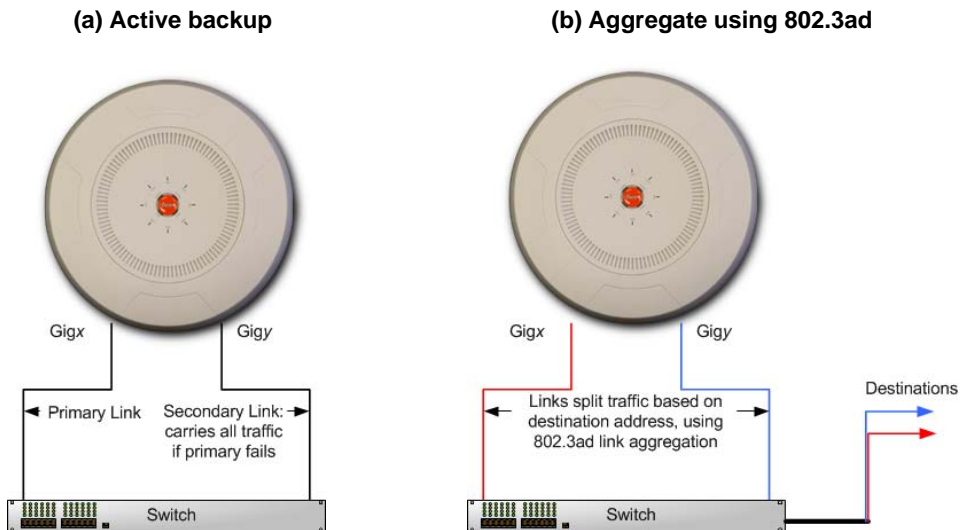


Figure 95. Port Modes (a, b)

- b. **Aggregate Traffic from gig ports using 802.3ad**—The Array sends network traffic across all member Gigabit ports to increase link speed to the network. These ports act as a single logical interface (trunk), using a load balancing algorithm to balance traffic across the ports. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. If the packet is a fragment or not

TCP or UDP, the source and destination IP addresses are used to do the calculation. If the packet is TCP or UDP over IP then the source IP address, destination IP address, source port number and destination port number are all used to do the calculation. The network switch must also support 802.3ad. If a port fails, the trunk degrades gracefully—the other port still transmits. See Figure 95 (b).

- c. **Transmit Traffic on all gig ports**—Transmits incoming traffic on all Gigabit ports. Any traffic received on Gigabit ports is sent to the onboard processor. This mode provides fault tolerance. See Figure 96 (c).

(c) Transmit on all ports

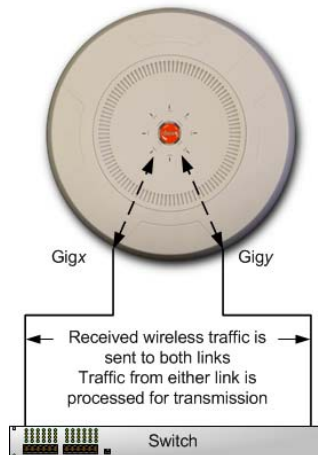


Figure 96. Port Modes (c)

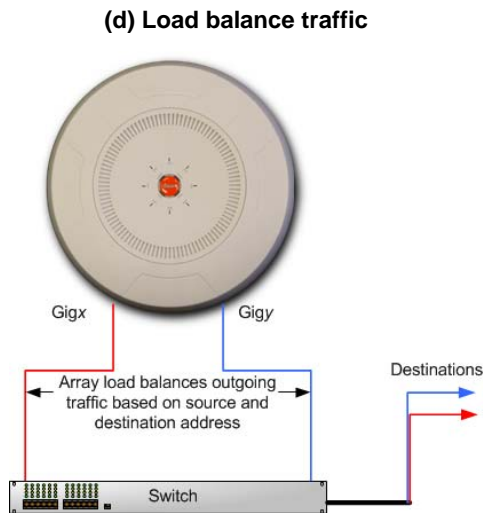


Figure 97. Port Modes (d)

- d. **Load balance traffic between gig ports**—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 97 (d).
2. **Bond Ports:** Select the ports to be members of this bond for the behavior specified by **Bond Mode**. By default, $Bond_n$ contains only the Gig_n port for convenience in use with the Mirror option; these default memberships are removed as appropriate when the ports are added to other bonds. In Arrays that have four Gigabit ports, you also have the option of bonding all four ports together.
3. **Active VLANs:** **Active VLANs** is a read-only field that shows the VLANs that you have selected to be passed through this port. You may modify this list by making selections in **Set Active VLANs**.

4. **Set Active VLANs:** Create and manage the list of VLANs that are allowed to be passed through this port. Traffic will be dropped for VLANs that are not in this list. ??Is this correct?? You may view the complete list of VLANs whose traffic will be passed in the **Active VLANs** list, above. The default setting is to pass All VLANs.
 - a. To add a VLAN to the list of allowed VLANs, type its name or number ??OK??, and click **Add**. To allow all VLANs (current or future) to be passed, click the **All** button.
 - b. To remove a VLAN from the list of allowed VLANs, type its name or number, and click **Delete**. To remove all VLANs from the Active VLANs list, click **None**.
 - c. To allow only the set of currently defined VLANs (see “VLANs” on page 185) to be passed, click the **Current** button. Essentially, this “fixes” the Active VLANs list to contain the Array’s currently defined VLANs, and only this set, until you make explicit changes to the Active VLANs list. If you create new VLANs, they will not be passed unless you take action to add them to the list. ??All OK??
5. ??Is this correct?? **Mirror**—Specify one of the active bonds (Bondx) that is to be mirrored by this port (Gigabit). All wireless traffic received on the Array is transmitted out both Bondx and Gigabit. All traffic received on Bondx is passed on to the onboard processor as well as out Gigabit. All traffic received on Gigabit is passed on to the onboard processor as well as out Bondx. This allows a network analyzer to be plugged into Gigabit to capture traffic for troubleshooting, while the bonded ports provide network connectivity for data traffic. See [Figure 98](#).

??True?? Mirroring is also used to bridge traffic between gig ports—Traffic received on Bondx is transmitted by Gigabit; similarly, traffic received on Gigabit is transmitted by Bondx. This allows the Array to act as a wired bridge and allows Arrays to be daisy-chained and still maintain wired connectivity.

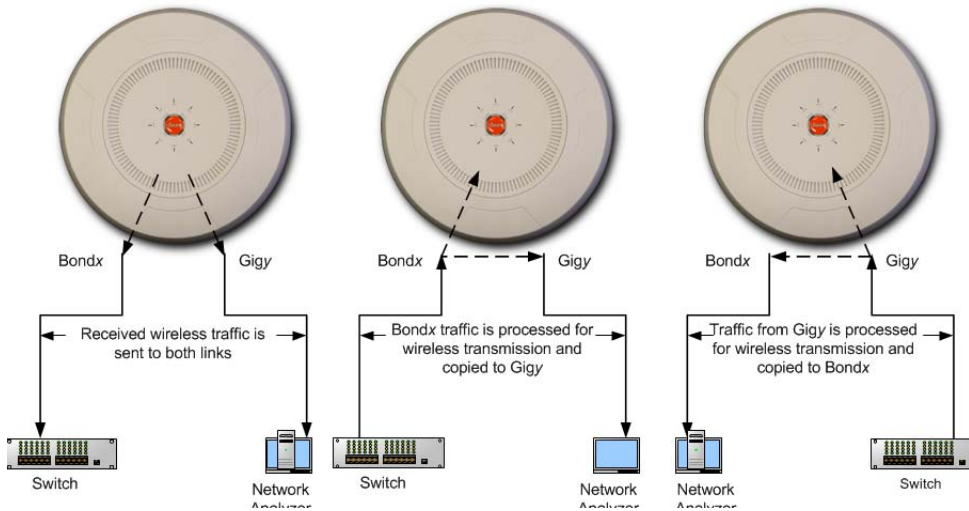


Figure 98. Mirroring Traffic

- When done configuring bonds as desired, click **Save changes to flash** if you wish to make your changes permanent.

See Also

Network Interfaces

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 182. At least one DNS server must be set up if you want to offer clients associating with the Array the ability to use meaningful host names instead of numerical IP addresses. When finished, click **Save changes to flash** if you wish to make your changes permanent.

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

Figure 99. DNS Settings

Procedure for Configuring DNS Servers

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

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

See Also

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

CDP Settings

CDP (Cisco Discovery Protocol) is a layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Wireless Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors (see “CDP Neighbors” on page 105).

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

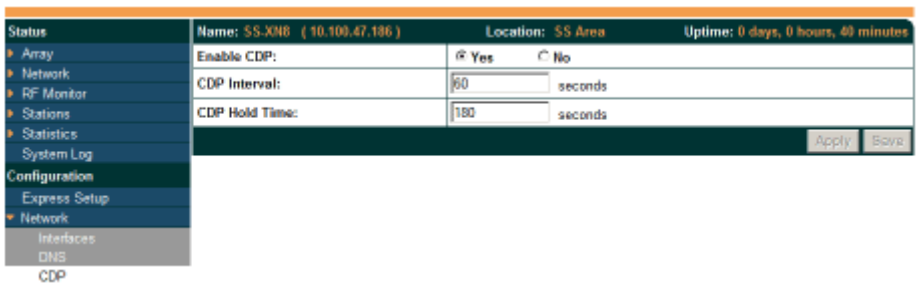


Figure 100. CDP Settings

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.



CDP works on untagged interfaces. It will not always work with tagged interfaces on Cisco devices, since they might switch from using CDP to DTP on tagged trunk links.

See Also

[CDP Neighbors](#)

[Network](#)

[Network Interfaces](#)

[Network Statistics](#)

Services

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

Status	Name: XR4820 (10.100.57.54)										Uptime: 30 days, 17 hours, 29 mins						
Configuration	Save changes to flash																
Express Setup	Time Settings Summary																
Network	NTP Server Status				NTP Server 1 Address				NTP Server 2 Address								
Services	Enabled																
Time	Netflow Summary																
Netflow	State				Collector Host				Collector Port								
WIFI Tag	Disabled								2055								
System Log	System Log Settings Summary																
SNMP	Log Levels										Log Servers						
DHCP Server	State	Console	Local Lines	Console	Local	1st	2nd	3rd	Email	Primary	Secondary	Tertiary	Email				
	on	off	2000	6	7	7	6	6	4	10.100.57.13							
VLANs	SNMP Settings Summary																
Security	SNMPv2 State			Trap Auth Failures			Trap Host IP 1			Trap Host IP 2			Trap Host IP 3			Trap Host IP 4	
SSIDs	Enabled			Enabled			Xirus-XMS										
Groups	SNMPv3 State			SNMPv3 Security			Trap Port 1			Trap Port 2			Trap Port 3			Trap Port 4	
IAPs	Disabled			sha / aes			162			162			162			162	
WDS	DHCP Server Settings																
Filters	DHCP Name	State	NAT	IP Range/Mask	IP Gateway	Default Lease	Maximum Lease	DNS Domain									
Clusters	WIFI Tag Summary																
Tools	State				UDP Port				Tag Channel BG								
	Disabled				1144				0								

Figure 101. Services

The following sections discuss configuring services on the Array:

- “Time Settings (NTP)” on page 171
- “NetFlow” on page 173
- “Wi-Fi Tag” on page 175
- “System Log” on page 176
- “SNMP” on page 179
- “DHCP Server” on page 182

Time Settings (NTP)

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

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

The Array allows you to enter optional authentication information.

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

Figure 102. Time Settings (Manual Time)

Procedure for Managing the Time Settings

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

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

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

Figure 103. Time Settings (NTP Time Enabled)

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

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

See Also

[Express Setup](#)

[Services](#)

[SNMP](#)

[System Log](#)

NetFlow

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

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

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

Figure 104. NetFlow



Some features, such as Netflow, are only available if the Array's license includes the *Xirrus Advanced RF Analysis Manager (RAM)*. If a setting is unavailable (grayed out), then your license does not support the feature. See *"About Licensing and Upgrades"* on page 321.

Procedure for Configuring NetFlow

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

Wi-Fi Tag

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

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

Figure 105. Wi-Fi Tag

Procedure for Configuring Wi-Fi Tag

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

System Log

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

Status	Name: Robin-XR4830 (10.100.48.24)		Uptime: 0 days, 2 hours, 12 mins
Configuration	Save changes to flash		
Express Setup	Enable Syslog Server:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
▶ Network	Console Logging:	<input type="radio"/> Yes	<input checked="" type="radio"/> No
▼ Services	Local File Size (1-2000 lines):	2000	
Time	Primary Server Address (Hostname or IP) and Port:	<input type="text"/>	514
Netflow	Secondary Server Address (Hostname or IP) and Port:	<input type="text"/>	514
WiFi Tag	Tertiary Server Address (Hostname or IP and Port):	<input type="text"/>	514
System Log	Email Syslog SMTP Server Address (Hostname or IP) and Port:	<input type="text"/>	25
SNMP	Email Syslog SMTP Server User Name:	<input type="text"/>	
DHCP Server	Email Syslog SMTP Server User Password:	<input type="text"/>	
▶ VLANs	Email Syslog From:	<input type="text"/>	
▶ Security	Email Syslog Recipient Addresses (semicolon delimited):	<input type="text"/>	
▶ SSIDs	Syslog Levels		
▶ Groups	Console Logging:	information and more serious ▼	
▶ IAPs	Local File:	debugging and more serious ▼	
▶ WDS	Primary Server:	information and more serious ▼	
▶ Filters	Secondary Server:	information and more serious ▼	
▶ Clusters	Tertiary Server:	information and more serious ▼	
Tools	Email SMTP Server:	warning and more serious ▼	
Help ?			
System Tools			
CLI			

Figure 106. 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** (1-2000 lines): 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 2000.
4. **Primary Server Address (Hostname or IP) and Port:** If you enabled Syslog, enter the hostname or IP address of the primary Syslog server. You may also change the port used on the server if you do not wish to use 514, the default port.
5. **Secondary/Tertiary Server Address (Hostname or IP) and Port:** (Optional) If you enabled Syslog, you may enter the hostname or IP address of one or two additional Syslog servers to which messages will also be sent. You may also change the port used on each server if you do not wish to use 514, the default port.
6. **Email Notification:** (Optional) 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 Syslog SMTP Server Address (Hostname or IP) and Port:** The hostname 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. You may also change the port used on the server if you do not wish to use 25, the default SMTP port.
 - b. **Email Syslog SMTP User Name:** Specify a user name for logging in to an account on the mail server designated in [Step a](#).
 - c. **Email Syslog SMTP User Password:** Specify a password for logging in to an account on the mail server designated in [Step a](#).
 - d. **Email Syslog SMTP From:** Specify the "From" email address to be displayed in the email.
 - e. **Email Syslog SMTP Recipient Addresses:** Specify the entire email address of the recipient of the email notification. You may specify additional recipients by separating the email addresses with semicolons (;).

7. **Syslog Levels:** For each of the Syslog destinations, choose your preferred level of Syslog reporting from the pull-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.
 - a. **Console Logging:** For messages to be echoed to the console, the default level is **Critical and more serious**. This prevents large numbers of non-critical messages from being displayed on the console. If you set this level too low, the volume of messages may make it very difficult to work with the CLI or view other output on the console.
 - b. **Local File:** For records to be stored on the Array's internal Syslog file, choose your preferred level of Syslog reporting from the pull-down list. The default level is **Debugging and more serious**.
 - c. **Primary Server:** Choose the preferred level of Syslog reporting for the primary server. The default level is **Debugging and more serious**.
 - d. **Secondary/Tertiary Server:** Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Information and more serious**. (Optional)
 - e. **Email SMTP Server:** Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.
8. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

System Log Window

Services

SNMP

Time Settings (NTP)

SNMP

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

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

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

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

Figure 107. SNMP

Procedure for Configuring SNMP

SNMPv2 Settings

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

SNMPv3 Settings

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