USER'S GUIDE

Wireless Arrays and Access Points

XR Series
November 26, 2013
Release 6.7

XIRRUS®
High Performance Wireless Networks

Wireless Arrays™ and Access Points

XR Series

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

XIRRUS®

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 (Arrays except XR-500/600 and Models Ending in H)" on page 501.

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 xiii

Introduction 1

The Xirrus Family of Products 1
Nomenclature 2
Why Choose the Xirrus Wireless Array? 3
Wireless Array Product Overview 4
XR Wireless Array Product Family 6
XR-500 Series Access Points 6
XR-600 Series Access Points 7
XR-1000 8
XR-2000 Series Arrays 9
XR-4000 Series Arrays 10
XR-6000 Series Arrays 11
Enterprise Class Security 12
Deployment Flexibility 12
Power over Gigabit Ethernet (PoGE) 13
Enterprise Class Management 14
Key Features and Benefits 15
High Capacity and High Performance 15
Extended Coverage 16
Non-Overlapping Channels 16
SDMA Optimization 16
Fast Roaming 16
Ease of Deployment 16
Powerful Management 17
Secure Wireless Access 17
Applications Enablement 17
Advanced Feature Sets 17
Xirrus Advanced RF Performance Manager (RPM) 17
Xirrus Advanced RF Security Manager (RSM) 18
Xirrus Advanced RF Analysis Manager (RAM) 19
Xirrus Application Control 20

About this User's Guide 21
Organization 21
Notes and Cautions 23
Screen Images 23
Product Specifications 24

Installing the Wireless Array 25

Installation Prerequisites 25
Optional Network Components 27
Client Requirements 27
Planning Your Installation 28
General Deployment Considerations 28
Coverage and Capacity Planning 30
Placement 30
RF Patterns 31
Capacity and Cell Sizes 32
Fine Tuning Cell Sizes 33
Roaming Considerations 34
Allocating Channels 34
IEEE 802.11n Deployment Considerations 37
MIMO (Multiple-In Multiple-Out) 38
Multiple Data Streams—Spatial Multiplexing 39
Channel Bonding 40
Improved MAC Throughput 41
Short Guard Interval 41
Obtaining Higher Data Rates 42
802.11n Capacity 43
Failover Planning 43
Switch Failover Protection 45
Power Planning 46
Power over Gigabit Ethernet 46
Security Planning 47
Wireless Encryption 47
Authentication 47
Port Requirements 49
Network Management Planning 53
WDS Planning 54

Common Deployment Options 57
Installation Workflow 58
Installing Your Wireless Array 60
Choosing a Location 60
Wiring Considerations 61
Mounting and Connecting the Array 63
Dismounting the Array 63
Powering Up the Wireless Array 64
Array LED Operating Sequences 65
LED Boot Sequence 65
LED Operation when Array is Running 66
Establishing Communication 67
Zero-Touch Setup Using Mobilize 67
User Interfaces (CLI, WMI) 68
Using the Serial Port 70
Using the Ethernet Ports 70
Starting the WMI 71
Logging In 71
Licensing 71
Performing the Express Setup Procedure 72
Securing Low Level Access to the Array 73

The Web Management Interface 77

XMS-Managed Arrays Restrict Local Management 78
An Overview 80
Structure of the WMI 82
User Interface 84
Utility Buttons 87
Logging In 88
Applying Configuration Changes 88
Character Restrictions 89

Viewing Status on the Wireless Array 91

Array Status Windows 92
Array Summary 92
Content of the Array Summary Window 93
Array Information 98

Array Configuration 99
Admin History 100
Network Status Windows 100
Network 101
Network Map 102
Content of the Network Map Window 103
Spanning Tree Status 105
Routing Table 106
ARP Table 106
DHCP Leases 107
Connection Tracking/NAT 107
CDP Neighbors 108
Network Assurance 109
Undefined VLANs 110
RF Monitor Windows 111
IAPs 112
Spectrum Analyzer 113
Intrusion Detection 116
Channel History 118
Radio Assurance 120
Station Status Windows 122
Stations 123
Location Map 125
RSSI 129
Signal-to-Noise Ratio (SNR) 130
Noise Floor 132
Max by IAP 134
Station Assurance 135
Statistics Windows 137
IAP Statistics Summary 137
Per-IAP Statistics 138
Network Statistics 140
VLAN Statistics 141
WDS Statistics 142
IDS Statistics 143
Filter Statistics 144
Station Statistics 145

Per-Station Statistics 146
Application Control Windows 147
About Application Control 147
Application Control 149
Stations (Application Control) 153
System Log Window 154
IDS Event Log Window 155

Configuring the Wireless Array 157

Express Setup 159
Network 165
Network Interfaces 167
Network Interface Ports 168
Network Bonds 171
DNS Settings 177
CDP Settings 178
Services 180
Time Settings (NTP) 181
NetFlow 184
Wi-Fi Tag 185
Location 186
System Log 188
About Using the Splunk Application for Xirrus Arrays 191
SNMP 193
DHCP Server 196
VLANs 199
Understanding Virtual Tunnels 199
VLAN Management 201
Tunnels 204
About Xirrus Tunnels 204
Tunnel Management 205
SSID Assignments 207
Security 208
Understanding Security 209
Certificates and Connecting Securely to the WMI 212
Using the Array's Default Certificate 212
Using an External Certificate Authority 213

Admin Management 214
Admin Privileges 216
Admin RADIUS 218
About Creating Admin Accounts on the RADIUS Server 218
Management Control 221
Access Control List 228
Global Settings 230
External Radius 234
About Creating User Accounts on the RADIUS Server 235
Internal Radius 238
Rogue Control List 241
OAuth 2.0 Management 243
SSIDs 245
Understanding SSIDs 246
Understanding QoS Priority on the Wireless Array 247
High Density 2.4G Enhancement—Honeypot SSID 252
SSID Management 253
SSID List (top of page) 254
SSID Limits 258
Web Page Redirect Configuration Settings 260
Whitelist Configuration for Web Page Redirect 264
WPA Configuration Settings 265
RADIUS Configuration Settings 265
Active IAPs 266
Per-SSID Access Control List 267
Groups 269
Understanding Groups 269
Using Groups 270
Group Management 271
Group Limits 274
IAPs 276
Understanding Fast Roaming 278
IAP Settings 279
Global Settings (IAP) 285
Beacon Configuration 287
Station Management 288
Advanced Traffic Optimization 289

Global Settings .11an 298
Global Settings .11bgn 303
Global Settings .11n 309
Global Settings .11ac 312
Global Settings .11u 314
Understanding 802.11u 314
Advanced RF Settings 320
About Standby Mode 321
RF Monitor 321
RF Resilience 322
RF Power & Sensitivity 323
RF Spectrum Management 324
Station Assurance 327
Hotspot 2.0 329
Understanding Hotspot 2.0 329
NAI Realms 331
Understanding NAI Realm Authentication 331
NAI EAP 332
Intrusion Detection 334
DoS Attacks 335
Impersonation Attacks 336
About Blocking Rogue APs 337
RF Intrusion Detection and Auto Block Mode 338
DoS Attack Detection Settings 339
Impersonation Detection Settings 340
LED Settings 340
DSCP Mappings 341
Roaming Assist 342
WDS 345
About Configuring WDS Links 345
Long Distance Links 347
WDS Client Links 347
Filters 351
Filter Lists 352
Filter Management 354
Clusters 360
Cluster Definition 361

Cluster Management 362
Cluster Operation 363
Mobile 366
AirWatch 366
User Procedure for Wireless Access 368

Using Tools on the Wireless Array 371

System Tools 372
About Licensing and Upgrades 373
System 374
Automatic Updates from Remote Image or Configuration File 376
Configuration 377
Diagnostics 380
Application Control Signature File Management 381
Web Page Redirect 382
Network Tools 383
Progress and Status Frames 385
CLI 385
API Documentation 387
Status/Settings 388
GET Requests 389
Trying a GET Request 389
API Documentation Toolbar 391
Options 392
Logout 395

The Command Line Interface 397

Establishing a Secure Shell (SSH) Connection 398
Getting Started with the CLI 399
Inputting Commands 399
Getting Help 399
Top Level Commands 401
Root Command Prompt 401
configure Commands 402
show Commands 405
statistics Commands 408
Configuration Commands 410

acl 410
admin 411
auth 412
cdp 412
clear 414
cluster 416
contact-info 417
date-time 418
dhcp-server 419
dns 420
file 421
filter 425
    Air Cleaner 426
group 429
hostname 429
interface 430
load 430
location 431
location-reporting 432
management 433
mdm 434
more 435
netflow 436
no 437
quick-config 439
quit 440
radius-server 440
reboot 441
reset 441
restore 442
roaming-assist 443
run-tests 444
security 446
snmp 447
ssid 448
syslog 449
tunnel 450

uptime 451
vlan 451
wifi-tag 452
Sample Configuration Tasks 454
Configuring a Simple Open Global SSID 455
Configuring a Global SSID using WPA-PEAP 456
Configuring an SSID-Specific SSID using WPA-PEAP 457
Enabling Global IAPs 458
Disabling Global IAPs 459
Enabling a Specific IAP 460
Disabling a Specific IAP 461
Setting Cell Size Auto-Configuration for All IAPs 462
Setting the Cell Size for All IAPs 463
Setting the Cell Size for a Specific IAP 464
Configuring VLANs on an Open SSID 465
Configuring Radio Assurance Mode (Loopback Tests) 466

Appendices 469

Appendix A: Quick Reference Guide 471
Factory Default Settings 471
Host Name 471
Network Interfaces 471
Serial 471
Gigabit 1 and Gigabit 2 472
Server Settings 472
NTP 472
Syslog 472
SNMP 473
DHCP 473
Default SSID 474
Security 474
Global Settings - Encryption 474
External RADIUS (Global) 475
Internal RADIUS 476
Administrator Account and Password 476
Management 476
Keyboard Shortcuts 477

Appendix B: FAQ and Special Topics 479
General Hints and Tips 479
Frequently Asked Questions 480
Multiple SSIDs 480
Security 482
VLAN Support 485
Array Monitor and Radio Assurance Capabilities 488
Enabling Monitoring on the Array 488
How Monitoring Works 488
Radio Assurance 489
Radio Assurance Options 490
RADIUS Vendor Specific Attribute (VSA) for Xirrus 491
Location Service Data Formats 492
Euclid Location Server 492
Non-Euclid Location Server 492
Upgrading the Array via CLI 494
Sample Output for the Upgrade Procedure: 495
Contact Information 499

Appendix C: Notices (Arrays except XR-500/600 and Models Ending in H) 501
Notices 501
EU Directive 1999/5/EC Compliance Information 505
Compliance Information (Non-EU) 512
Safety Warnings 513
Translated Safety Warnings 514
Software License and Product Warranty Agreement 515
Hardware Warranty Agreement 521

Appendix D: Notices (XR500/600 Series Only) 523
Notices 523
EU Directive 1999/5/EC Compliance Information 527
Compliance Information (Non-EU) 534
Safety Warnings 535
Translated Safety Warnings 536
Software License and Product Warranty Agreement 537
Hardware Warranty Agreement 543

Appendix E: Medical Usage Notices 545

Glossary of Terms 551

Index 563

List of Figures

Figure 1. Xirrus Arrays: XR Series 1
Figure 2. Wireless Array (XR Series) 4
Figure 3. Wireless Coverage Patterns 12
Figure 4. XP8 - Power over Ethernet Usage 13
Figure 5. WMI: Array Status 14
Figure 6. Layout of IAPs (XR-7630) 15
Figure 7. Wall Thickness Considerations 29
Figure 8. Unit Placement 30
Figure 9. Full (Normal) Coverage 31
Figure 10. Adjusting RF Patterns 31
Figure 11. Custom Coverage 32
Figure 12. Connection Rate vs. Distance 32
Figure 13. Transmit Power 33
Figure 14. Overlapping Cells 34
Figure 15. Allocating Channels Manually 36
Figure 16. Classic 802.11 Signal Transmission 38
Figure 17. MIMO Signal Processing 38
Figure 18. Spatial Multiplexing 39
Figure 19. Channel Bonding 40
Figure 20. MAC Throughput Improvements 41
Figure 21. Computing 802.11n Data Rates 42
Figure 22. Port Failover Protection 43
Figure 23. Switch Failover Protection 45
Figure 24. Port Requirements for XMS 49
Figure 25. WDS Link 54
Figure 26. A Multiple Hop WDS Connection 55
Figure 27. WDS Failover Protection 55
Figure 28. Installation Workflow 58
Figure 29. Array Placement 60
Figure 30. LED Locations 64
Figure 31. Network Interface Ports—XR-520 (left); XR-1000 Series (right) 68
Figure 32. Network Interfaces—XR-2000 Series (left); XR-2005 Series (right) ... 69
Figure 33. Network Interface Ports—XR-4000 Series 69
Figure 34. Network Interface Ports—XR-6000 Series 69

Figure 35. Notice for XMS-Managed Array 78
Figure 36. Web Management Interface—Option = New Style 80
Figure 37. Web Management Interface—New Style (Default) 80
Figure 38. Web Management Interface—Option = Classic Style 81
Figure 39. Web Management Interface—Classic Style 81
Figure 40. WMI: Frames 84
Figure 41. Major Menu Sections Collapsed (on left) 85
Figure 42. WMI: Utility Buttons 87
Figure 43. Logging In to the Wireless Array 88
Figure 44. Array Summary 92
Figure 45. Disabled IAP (Partial View) 95
Figure 46. IAP Cells 95
Figure 47. Network Assurance and Operating Status 96
Figure 48. Array Information 98
Figure 49. Show Configuration 99
Figure 50. Admin Login History 100
Figure 51. Network Settings 101
Figure 52. Network Map 102
Figure 53. Spanning Tree Status 105
Figure 54. Routing Table 106
Figure 55. ARP Table 106
Figure 56. DHCP Leases 107
Figure 57. Connection Tracking 107
Figure 58. CDP Neighbors 108
Figure 59. Network Assurance 109
Figure 60. Undefined VLANs 110
Figure 61. RF Monitor—IAPs 112
Figure 62. RF Monitor—IAPs 112
Figure 63. RF Spectrum Analyzer 114
Figure 64. Intrusion Detection/Rogue AP List 116
Figure 65. RF Monitor—Channel History 118
Figure 66. RF Monitor—Channel History (Rotated) 119
Figure 67. RF Monitor—Channel History (Text) 119
Figure 68. Radio Assurance 120
Figure 69. Stations 123
Figure 70. Location Map 125
Figure 71. Controls for Location Map 126

Figure 72. Station RSSI Values 129
Figure 73. Station RSSI Values—Colorized Graphical View 129
Figure 74. Station Signal-to-Noise Ratio Values 130
Figure 75. Station SNR Values—Colorized Graphical View 131
Figure 76. Station Noise Floor Values 132
Figure 77. Station Noise Floor Values—Colorized Graphical View 133
Figure 78. Max by IAP 134
Figure 79. Station Assurance 135
Figure 80. IAP Statistics Summary Page 137
Figure 81. Individual IAP Statistics Page 139
Figure 82. Network Statistics 140
Figure 83. VLAN Statistics 141
Figure 84. WDS Statistics 142
Figure 85. IDS Statistics Page 143
Figure 86. Filter Statistics 144
Figure 87. Station Statistics 145
Figure 88. Individual Station Statistics Page 146
Figure 89. Application Control 149
Figure 90. Application Control (Pie Charts) 151
Figure 91. Application Control (Station Traffic) 151
Figure 92. Stations (Application Control) 153
Figure 93. System Log (Alert Level Highlighted) 154
Figure 94. IDS Event Log 155
Figure 95. WMI: Express Setup 159
Figure 96. LEDs are Switched On 164
Figure 97. Network Interfaces 165
Figure 98. Network Settings 168
Figure 99. Network Interface Ports 168
Figure 100. Network Bonds 171
Figure 101. Port Modes (a, b) 173
Figure 102. Port Modes (c) 174
Figure 103. Port Modes (d) 174
Figure 104. Mirroring Traffic 176
Figure 105. DNS Settings 177
Figure 106. CDP Settings 178
Figure 107. Services 180
Figure 108. Time Settings (Manual Time) 181

Figure 109. Time Settings (NTP Time Enabled) 182
Figure 110. NetFlow 184
Figure 111. Wi-Fi Tag 185
Figure 112. Location 186
Figure 113. System Log 188
Figure 114. SNMP 193
Figure 115. DHCP Management 196
Figure 116. VLANs 199
Figure 117. VLAN Management 201
Figure 118. Tunnel Summary 204
Figure 119. Tunnel Management 205
Figure 120. Tunnel SSID Assignments 207
Figure 121. Security 208
Figure 122. Import Xirrus Certificate Authority 212
Figure 123. Admin Management 214
Figure 124. Admin Privileges 216
Figure 125. Admin RADIUS 219
Figure 126. Management Control 221
Figure 127. Pre-login Banner 222
Figure 128. Access Control List 229
Figure 129. Global Settings (Security) 230
Figure 130. External RADIUS Server 234
Figure 131. Internal RADIUS Server 238
Figure 132. Rogue Control List 241
Figure 133. OAuth 2.0 Management - Token List 243
Figure 134. SSIDs 245
Figure 135. Four Traffic Classes 248
Figure 136. Priority Level—IEEE 802.1p (Layer 2) 248
Figure 137. Priority Level—DSCP (DiffServ - Layer 3) 249
Figure 138. SSID Management 253
Figure 139. SSID Management—Encryption, Authentication, Accounting 256
Figure 140. WPR Internal Splash Page Fields (SSID Management) 260
Figure 141. Customizing an Internal Login or Splash Page 263
Figure 142. Whitelist Configuration for WPR 264
Figure 143. Setting Active IAPs per SSID 266
Figure 144. Per-SSID Access Control List 267
Figure 145. Groups 269

Figure 146. Group Management 271
Figure 147. IAPs 276
Figure 148. Source of Channel Setting 277
Figure 149. IAP Settings 279
Figure 150. Global Settings (IAPs) 285
Figure 151. Global Settings .11an 298
Figure 152. Global Settings .11bgn 303
Figure 153. Global Settings .11n 309
Figure 154. Global Settings .11ac 312
Figure 155. 802.11u Global Settings 315
Figure 156. Advanced RF Settings 320
Figure 157. Station Assurance (Advanced RF Settings) 327
Figure 158. Hotspot 2.0 Settings 330
Figure 159. NAI Realms 331
Figure 160. NAI EAP 332
Figure 161. Intrusion Detection Settings 334
Figure 162. LED Settings 340
Figure 163. DSCP Mappings 342
Figure 164. Roaming Assist 344
Figure 165. WDS 345
Figure 166. Configuring a WDS Link 346
Figure 167. WDS Client Links 347
Figure 168. Filters 351
Figure 169. Filter Lists 352
Figure 170. Filter Management 354
Figure 171. Filter Category or Application 358
Figure 172. Clusters 360
Figure 173. Cluster Definition 361
Figure 174. Cluster Management 362
Figure 175. Cluster Mode Operation 363
Figure 176. Cluster Mode Activation 363
Figure 177. Viewing Statistics in Cluster Mode 364
Figure 178. AirWatch Settings 366
Figure 179. System Tools 372
Figure 180. Saving the Diagnostic Log 380
Figure 181. Managing Application Control Signature files 381
Figure 182. Managing WPR Splash/Login page files 382

Figure 183. System Command (Ping) 383
Figure 184. Radius Ping Output 384
Figure 185. CLI Window 385
Figure 186. API Documentation 387
Figure 187. API — Settings Requests List 388
Figure 188. API — GET Request Details 389
Figure 189. API — GET Request Response 390
Figure 190. API Documentation Toolbar 391
Figure 191. WMI Display Options 392
Figure 192. iPhone Style Option 393
Figure 193. Login Window 395
Figure 194. Logging In 398
Figure 195. Help Window 399
Figure 196. Full Help 400
Figure 197. Partial Help 400
Figure 198. Air Cleaner Filter Rules 427
Figure 199. Configuring a Simple Open Global SSID 455
Figure 200. Configuring a Global SSID using WPA-PEAP 456
Figure 201. Configuring an SSID-Specific SSID using WPA-PEAP 457
Figure 202. Enabling Global IAPs 458
Figure 203. Disabling Global IAPs 459
Figure 204. Enabling a Specific IAP 460
Figure 205. Disabling a Specific IAP 461
Figure 206. Setting the Cell Size for All IAPs 462
Figure 207. Setting the Cell Size for All IAPs 463
Figure 208. Setting the Cell Size for a Specific IAP 464
Figure 209. Configuring VLANs on an Open SSID 465
Figure 210. Configuring Radio Assurance Mode (Loopback Testing) 467

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 4**.
- **"Key Features and Benefits" on page 15**.
- **"Advanced Feature Sets" on page 17.**
- **"About this User's Guide" on page 21.**

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, application-level intelligence, increased bandwidth, and smaller size. The radios support IEEE802.11 ac, 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. Xirrus offers XMS Cloud—a software as a service option for XMS, capable of managing all aspects of your Xirrus network, including automatic software and firmware upgrades for the network. For XMS Cloud customers, all Array management is performed via the cloud. Access to Arrays via CLI and Web Management Interface is disabled. For other XMS customers, write access to Arrays via CLI and Web Management Interface is typically disabled.

  Users start the XMS client simply by entering the URL of the XMS server on a web browser. If you need detailed information about this product, refer to the *XMS User's Guide*.

- **Xirrus-supplied Power over Gigabit Ethernet (PoGE) Injectors and POE+ Switches**
  Xirrus offers 24- and 48-port enterprise-class L2+ gigabit managed access switches with IEEE802.3at PoE+, four 1G/10G SFP+ ports, and stacking. One-, two-, and eight-port PoGE injectors are also available for a range of Array power requirements.

Nomenclature

Throughout this User's Guide, Xirrus Wireless Arrays and Access Points are referred to as simply **Arrays**. 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 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 these major IEEE standards:

- **802.11ac**
  Operates in the 5 GHz range, using a number of advanced techniques to achieve a maximum speed of 1.3 Gbps. These techniques include improvements on the methods used for 802.11n, below.
- **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.
- **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.

Whether you have just a handful of users or thousands of users, the Xirrus Array 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 up to 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 up to 1.3 Gbps throughput .

Figure 2. Wireless Array (XR Series)

The Wireless Array (regardless of the product model) is Wi-Fi® compliant and simultaneously supports 802.11ac, 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-500 Series Access Points

These Access Points have one Gigabit Ethernet port and two radios—one multi-state radio (2.4GHz or 5GHz) and one 5GHz radio. They support 300Mbps, connecting up to 240 users at one time.

The XR-500 provides flexibility for delivering wireless service in low-to-medium user density scenarios, in challenging deployments in areas with high RF attenuation, and in isolated or physically separated locations.

Like XR Arrays, these models have an integrated controller, firewall, threat sensor and spectrum analyzer. Unlike other XR Arrays, these models have omni-directional antennas rather than directional antennas.

Feature	XR-520
No. radios: 802.11 a/b/g/n/monitor	2
Radio type	2x2
Integrated omni-directional antennas	4
Integrated wireless switch ports	2
Integrated RF spectrum analyzer, threat sensors	Yes
Gigabit Uplink Port	1
Wireless bandwidth	300 Mbps
Users supported	240

XR-600 Series Access Points

The XR-600 Series provides robust wireless service in low-to-medium user density scenarios. These Access Points have two Gigabit Ethernet ports and two multi-state radios (2.4GHz or 5GHz). Each of the XR-630's 3x3 802.11ac radios supports 1.3Gbps, connecting up to 240 users at one time with 2.6Gbps total Wi-Fi bandwidth.

Like XR Arrays, these models have an integrated controller, firewall, threat sensor spectrum analyzer, and application-level intelligence. Unlike larger XR Arrays, these models have omni-directional antennas rather than directional antennas.

The XR-630 supports ACExpress™ which optimizes wireless performance by automatically segmenting faster 802.11ac clients from slower Wi-Fi clients. Since Wi-Fi is a shared medium, this separation ensures slower 802.11a/b/g/n clients do not slow down 802.11ac clients from achieving high performance.

Feature	XR-620	XR-630
No. radios: 802.11 ac/a/b/g/n/monitor	2	2
Radio type	2x2	3x3
Integrated omni-directional antennas	4	6
Integrated wireless switch ports	2	2
Integrated RF spectrum analyzer, threat sensors	Yes	Yes
Gigabit Uplink Ports	2	2
Wireless bandwidth	1.7 Gbps	2.6 Gbps
Users supported	240	240

XR-1000

These Arrays include models with one Gigabit Ethernet port and two multi-state radios (2.4GHz or 5GHz) that can support 300Mbps or 450Mbps, connecting up to 480 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 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.

Like larger 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
No. radios: 802.11 a/b/g/n/monitor	2	2
Radio type	2x2	3x3
Integrated antennas	4	6
Integrated wireless switch ports	2	2
Integrated RF spectrum analyzer, threat sensors	Yes	Yes
Gigabit Uplink Port	1	1
Wireless bandwidth	600 Mbps	900 Mbps
Users supported	480	480

XR-2000 Series Arrays

These Arrays include models with one or two Gigabit Ethernet ports and two or four multi-state radios (2.4GHz or 5GHz) that can support 300Mbps or 450Mbps, connecting up to 960 users at one time.

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 1.8Gbps of bandwidth. These models support a range of low to high-performance applications, including offices, hospitals, campuses and classrooms, and hotels.

Like larger 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-2220	XR-2225	XR-2230	XR-2235	XR-2420	XR-2425	XR-2430	XR-2435
No. radios: 802.11 a/b/g/n/monitor	2	2	2	2	4	4	4	4
Radio type	2x2	2x2	3x3	3x3	2x2	2x2	3x3	3x3
Integrated antennas	4	4	6	6	8	8	12	12
Integrated wireless switch ports	4	4	4	4	4	4	4	4
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Gigabit Uplink Ports	1	2	1	2	1	2	1	2
Wireless bandwidth	600 Mbps	600 Mbps	900 Mbps	900 Mbps	1.2 Gbps	1.2 Gbps	1.8 Gbps	1.8 Gbps
Users supported	480	480	480	480	960	960	960	960

Note that XR-2000 Series Arrays ending in “0” have one Gigabit POE port and a Console port. Those ending in “5” have no console port, but have two Gigabit

ports, one of which accepts POE+ power supplied by a Xirrus-supplied power injector or an IEEE802.3at powered switch.

XR-4000 Series Arrays

These Arrays include models with two Gigabit Ethernet ports and four or eight radios (IAPs), connecting up to 1920 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 1792 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 (on all Arrays except the XR-500 Series) 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:

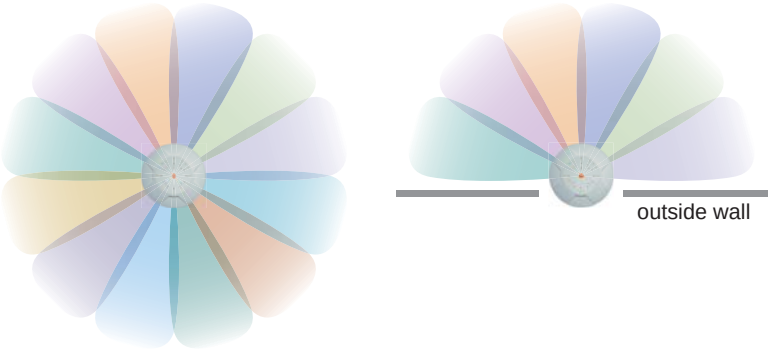


Figure 3. Wireless Coverage Patterns

Figure 3 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)

Some smaller Arrays and APs (XR-500/600 and XR-2005 Series) are compatible with IEEE802.3af and/or IEEE802.3at PoE+, and may be connected to appropriate powered switches. For example, the Xirrus XT-5024 and XT-5048 are 24-and 48-port 802.3at POE+ managed switches. See the Quick Installation Guide for the Array/AP for compatible injectors or powered switches.

The Xirrus-supplied XP1, XP2, and XP8 Power over Gigabit Ethernet modules provide power to Arrays over the same Cat 5e or Cat 6 cable used for data. Managed modules provide the ability to control power using XMS.

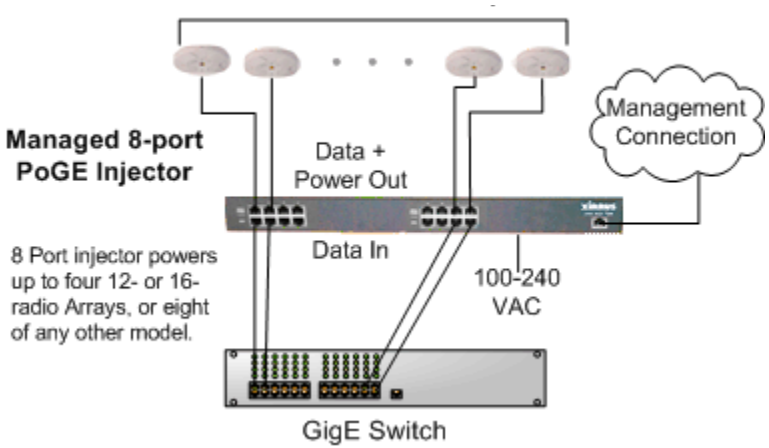


Figure 4. XP8 - Power over Ethernet Usage

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

Enterprise Class Management

The Wireless Array can be used with its default settings, or using zero touch cloud-based automated provisioning. Settings may also 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.

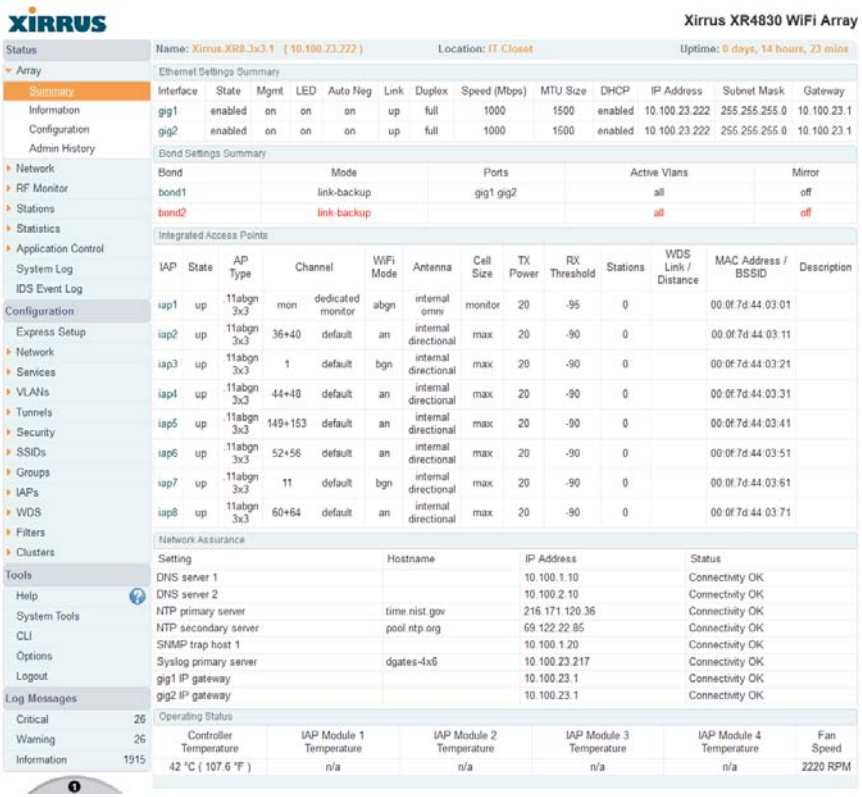


Figure 5. WMI: Array Status

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 on-premise or cloud-based Xirrus Management System (XMS). 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.

Ease of Deployment

The Xirrus Mobilize service simplifies and speeds deployment of the wireless network by automatically setting up each Array's license, software image, and initial configuration. When the Array is installed and has Internet connectivity, it contacts the Mobilize server, which performs these initialization tasks.

Powerful Management

The Xirrus Management System (XMS) offers real time monitoring and management capabilities for the wireless network.

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-GTC, EAP-AKA, EAP-AKA-Prime, 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.

See Also

Wireless Array Product Overview
Power over Gigabit Ethernet (PoGE)
Why Choose the Xirrus Wireless Array?

Advanced Feature Sets

The Wireless Array offers a family of powerful functionality packages, including the RF Performance Manager (RPM), RF Security Manager (RSM), RF Analysis Manager (RAM), and Application Control. These four packages are separately licensed for operation on your Array. RPM, RSM, and RAM are automatically included as part of all XR Arrays. Application Control is an optional feature.

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.

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

Xirrus Application Control

The Application Control feature is available on XR Arrays to provide real-time visibility of application usage by users across the wireless network. Network usage has changed enormously in the last few years, with the increase in smartphone and tablet usage stressing networks.

The Array uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productiveness. The results are presented to you both graphically and in tables. Filters may then be put in place to implement per-application policies that keep network usage focused on productive uses, eliminating risky and non-business-oriented applications such as BitTorrent. You can increase the priority of mission-critical applications like

VoIP and WebEx. See "Application Control Windows" on page 147 for more information.

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: FAQ and Special Topics**

  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 (Arrays except XR-500/600 and Models Ending in H)**

  Contains the legal notices, licensing, and compliance statements for the Array. Please read this section carefully.

- **Appendix D: Notices (XR500/600 Series Only)**

  Contains the legal notices, licensing, and compliance statements for the XR500 Series Access Points. Please read this section carefully if you are using these models.

- **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.

Product Specifications

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 25**.
- **"Planning Your Installation" on page 28**.
- **"Installation Workflow" on page 58**.
- **"Installing Your Wireless Array" on page 60**.
- **"Powering Up the Wireless Array" on page 64**.
- **"Establishing Communication" on page 67**.
- **"Performing the Express Setup Procedure" on page 72**.

Installation Prerequisites

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

- **Power Source**
  Xirrus Arrays and APs are powered via Xirrus-supplied 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.

  Some smaller Arrays and APs are compatible with IEEE802.3af and/or IEEE802.3at, and may be connected to appropriate powered switches. For example, the Xirrus XT-5024 is a 24-port 802.3at POE+ managed switch. See the Quick Installation Guide for the Array/AP for compatible injectors or powered switches.

- **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**
  Xirrus supports the latest version of the following Browsers: Internet Explorer, Mozilla Firefox, Chrome, or Safari. 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-500 and XR-1000 Series and some XR-2000 models, where Xircon can be used instead—see the *Xircon User's Guide*), 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
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 28**
- **"Coverage and Capacity Planning" on page 30**
- **"IEEE 802.11n Deployment Considerations" on page 37**
- **"Failover Planning" on page 43**
- **"Power Planning" on page 46**
- **"Security Planning" on page 47**
- **"Port Requirements" on page 49**
- **"Network Management Planning" on page 53**
- **"WDS Planning" on page 54**
- **"Common Deployment Options" on page 57**

*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

For optimal placement of Arrays, we recommend that a site survey be performed by a qualified Xirrus partner.

The Wireless Array's unique multi-radio architecture generates 360 degrees of sectored high-gain 802.11a/b/g/n coverage that provides extended range. (Note that XR-500 Series radios are omni-directional rather than sectored.) 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.

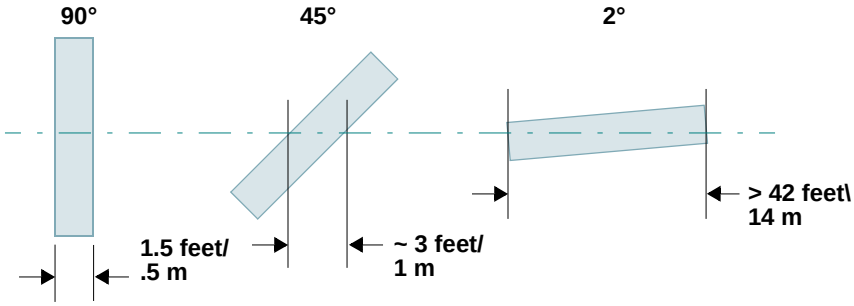


Figure 7. Wall Thickness Considerations

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
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.

XR-500 Series radios are omni-directional rather than directional (sectored), and discussions involving sectored radios are not applicable to these Arrays.

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).

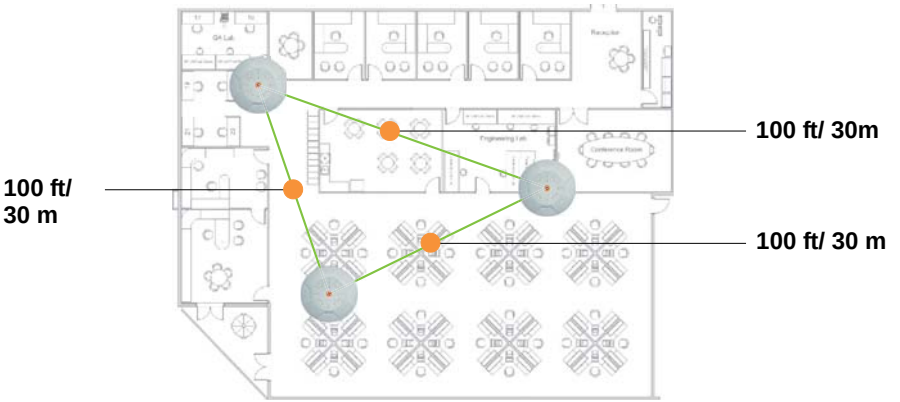


Figure 8. Unit Placement

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.

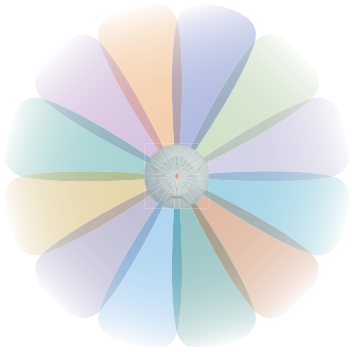


Figure 9. Full (Normal) Coverage

Half Coverage

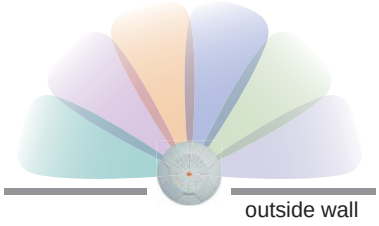


Figure 10. Adjusting RF Patterns

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.

Custom Coverage

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

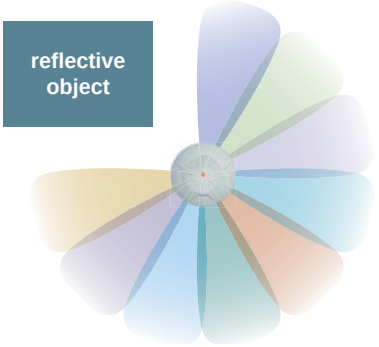


Figure 11. Custom Coverage

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.

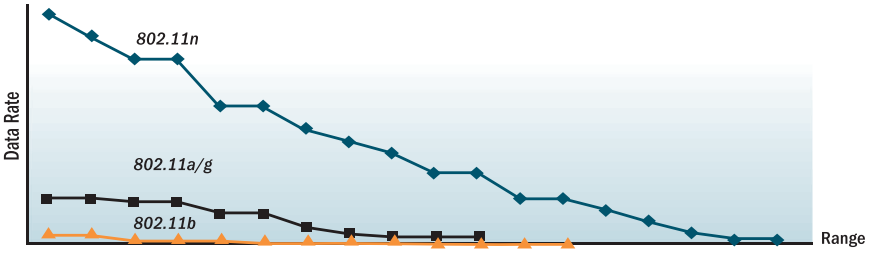


Figure 12. Connection Rate vs. Distance

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.

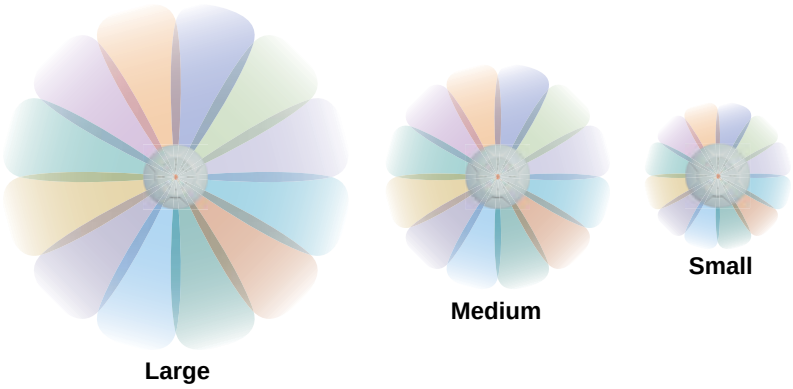


Figure 13. Transmit Power

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 323. 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 30.

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 323. 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.

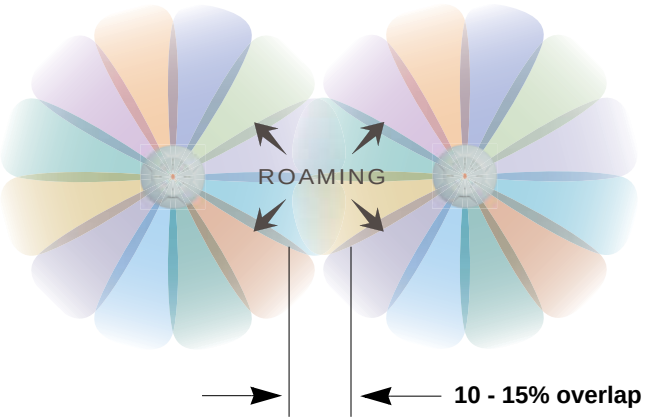


Figure 14. Overlapping Cells

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 320.

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.

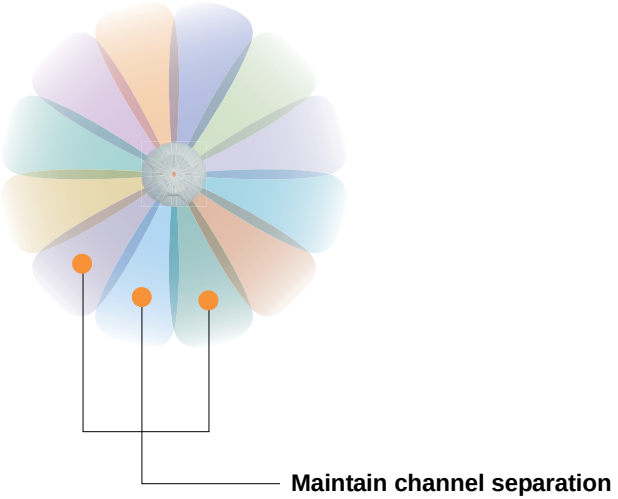


Figure 15. Allocating Channels Manually

See Also

Failover Planning
Installation Prerequisites

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 38**
- **"Multiple Data Streams—Spatial Multiplexing" on page 39**
- **"Channel Bonding" on page 40**
- **"Improved MAC Throughput" on page 41**
- **"Short Guard Interval" on page 41**
- **"Obtaining Higher Data Rates" on page 42**
- **"802.11n Capacity" on page 43**

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 309 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 16)

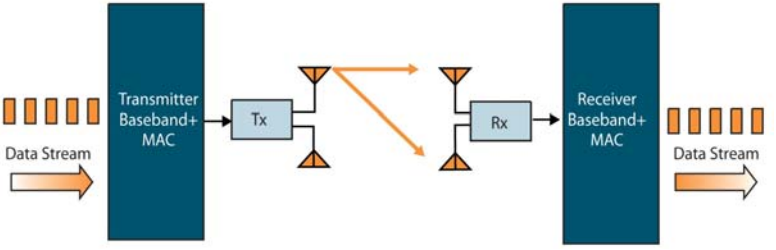


Figure 16. Classic 802.11 Signal Transmission

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 17).

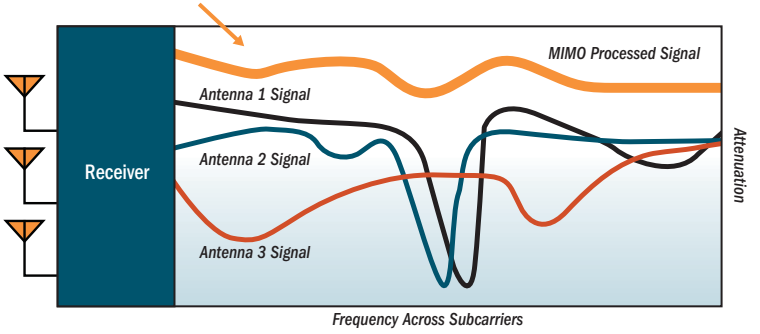


Figure 17. MIMO Signal Processing

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.

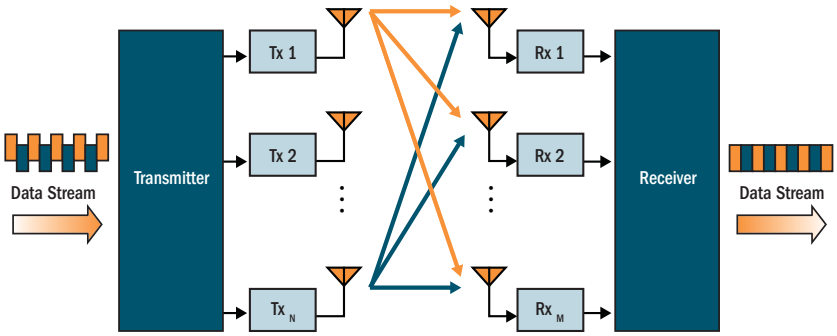


Figure 18. Spatial Multiplexing

Spatial multiplexing can double, triple, or quadruple the date 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 309).

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 309. To configure channel bonding manually, on a per-IAP basis, see "IAP Settings" on page 279.

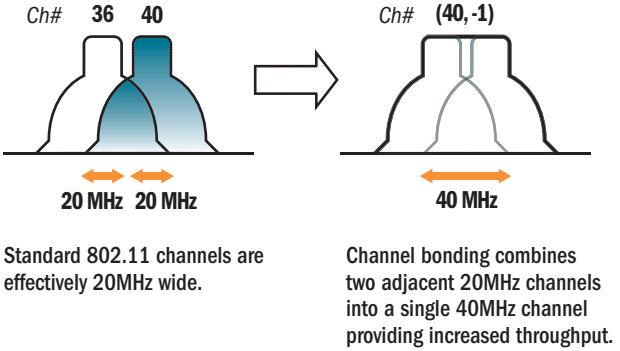


Figure 19. Channel Bonding

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.

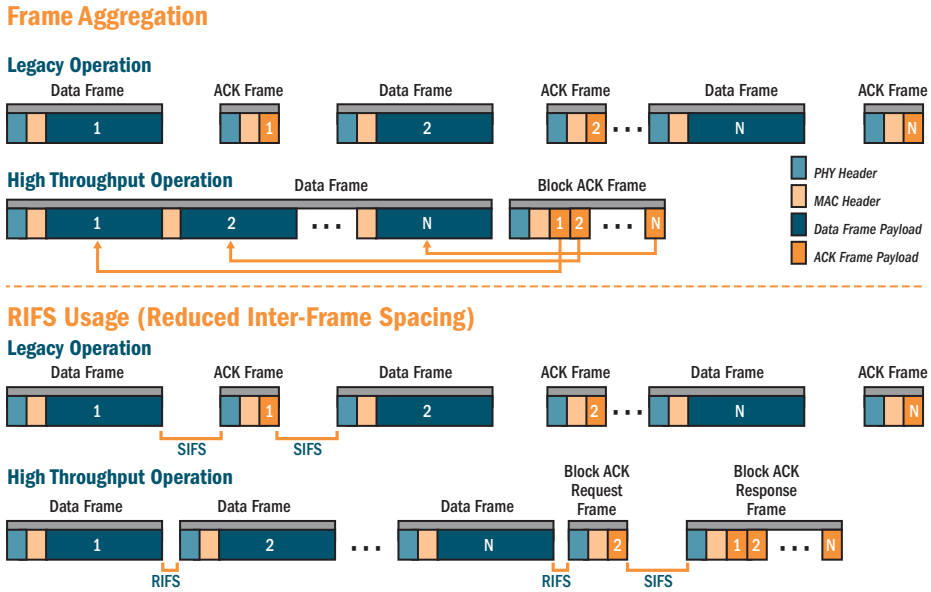


Figure 20. MAC Throughput Improvements

Short Guard Interval

This option reduces the wait time between symbols (the smallest unit of data transfer) 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 309 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 21 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 21. 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 Mbps = 10.2 Gbps
802.11 a/n: 2 Streams	23	23 * 300 Mbps = 6.8 Gbps
802.11 a/n: 1 Stream	23	23 * 150 Mbps = 3.4 Gbps
802.11 a	23	23 * 54 Mbps = 1.2 Gbps
802.11 g/n: 3 Streams	3	3 * 450 Mbps = 1.35 Gbps (1 or 2 streams have proportionally lower capacity)
802.11 g	3	3 * 54 Mbps = 162 Mbps
802.11 b	3	3 * 11 Mbps = 33 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).

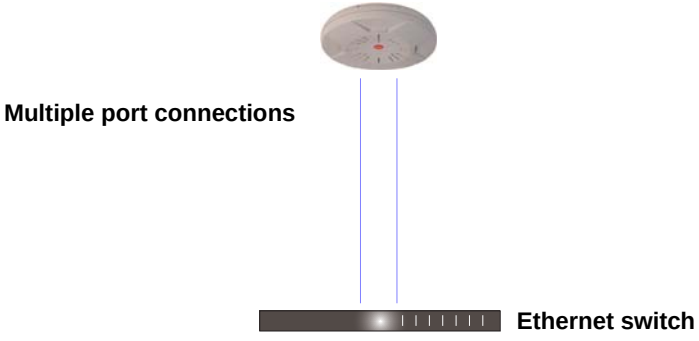


Figure 22. Port Failover Protection

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 171.

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 23. Switch Failover Protection

Gigabit Ethernet connections must be on the same subnet.

See Also

Coverage and Capacity Planning
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-supplied Power over Gigabit Ethernet (PoGE) modules or powered switches. They provide power over Cat 5e or Cat 6 cables to the Array without running power cables—see Figure 4 on page 13.

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.

Certain Xirrus models (XR-520 and XR--520H) also accept IEEE802.3af and IEEE802.3at powered switch ports.

See Also

Coverage and Capacity Planning
Failover Planning
Network Management Planning
Security Planning

Security Planning

This section offers some useful guidelines for defining your preferred encryption and authentication method. For additional information, see "Understanding Security" on page 209 and the Security section of "Frequently Asked Questions" on page 480.

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 50 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 24. XMS requires ports 161, 162, and 443 to be passed between Arrays and the XMS server. Similarly, port 9443 is 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.

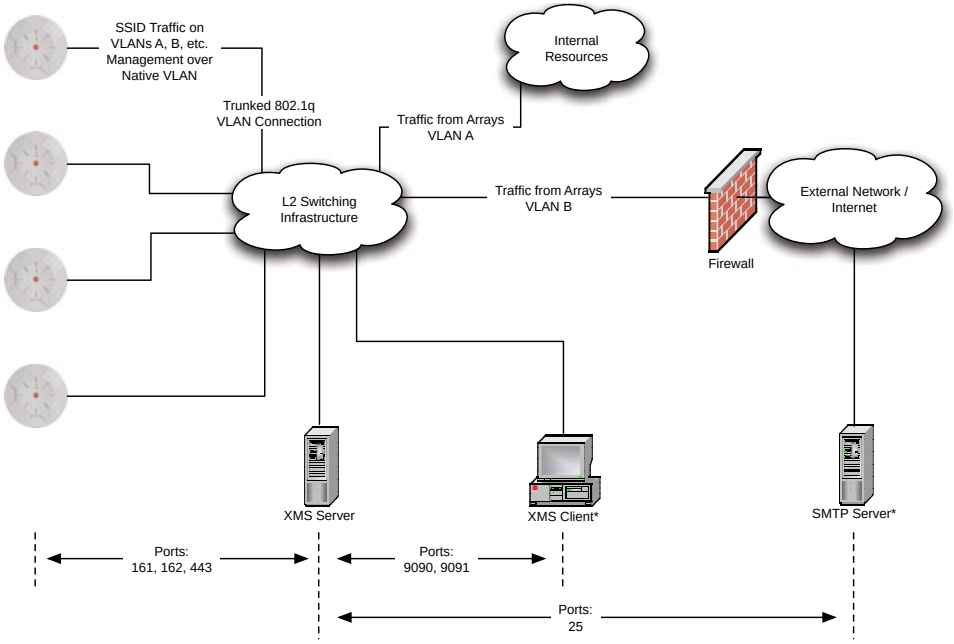


Figure 24. Port Requirements for XMS

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	Yes
* 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
  - 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 25). 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.

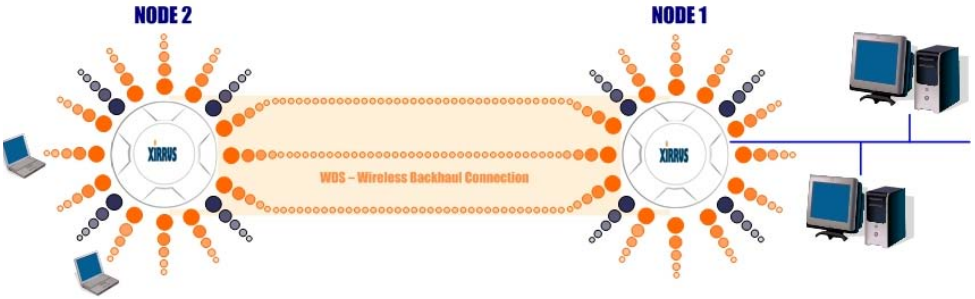


Figure 25. WDS Link

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

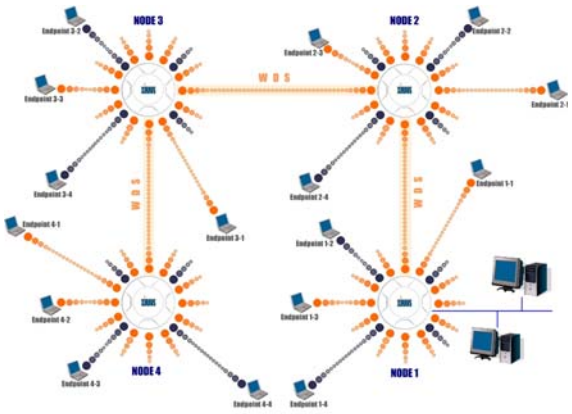


Figure 26. A Multiple Hop WDS Connection

- Multiple WDS links can provide link redundancy (failover capability - see Figure 27). A network protocol (Spanning Tree Protocol—STP) prevents Arrays from forming network loops.

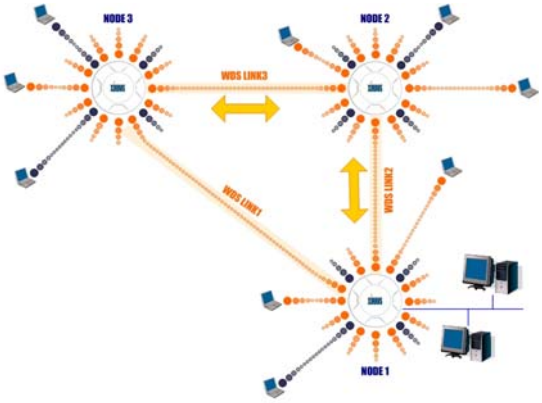


Figure 27. WDS Failover Protection

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 345. 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)	Cloud XMS or XMS (Enterprise-hosted)

See Also

Coverage and Capacity Planning
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. Cloud XMS customers will skip the last two steps.

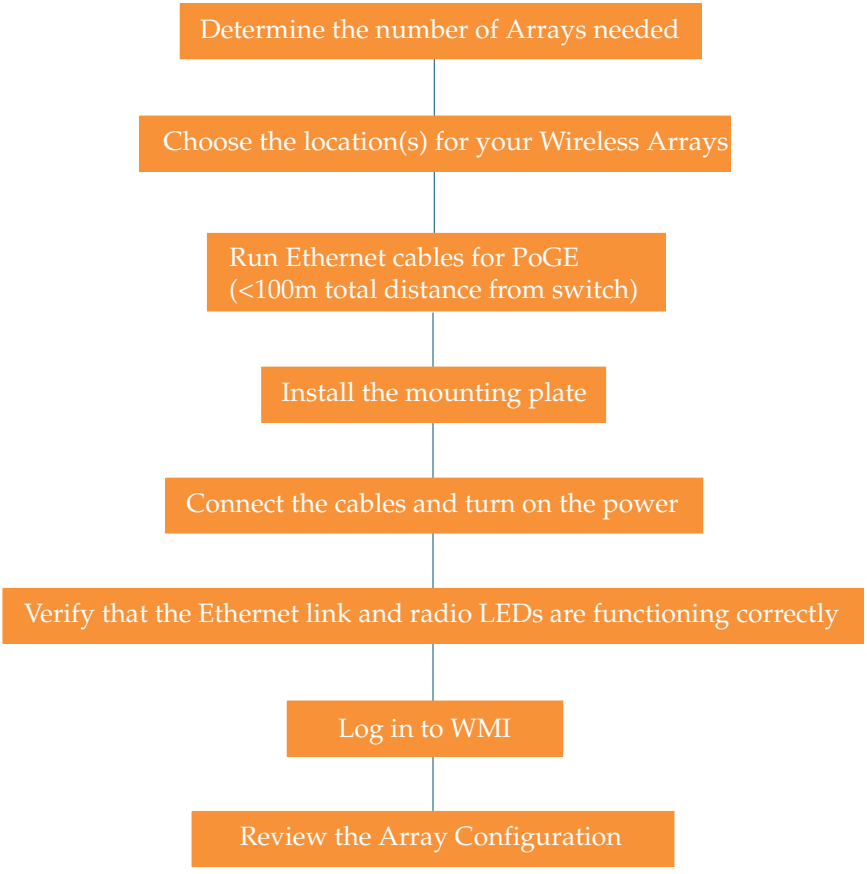


Figure 28. Installation Workflow

See Also

Coverage and Capacity Planning
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 information about the physical installation of your Xirrus Wireless Array. For complete instructions, please see the Quick Installation Guide (QIG) for your model of Array or Access Point.

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.

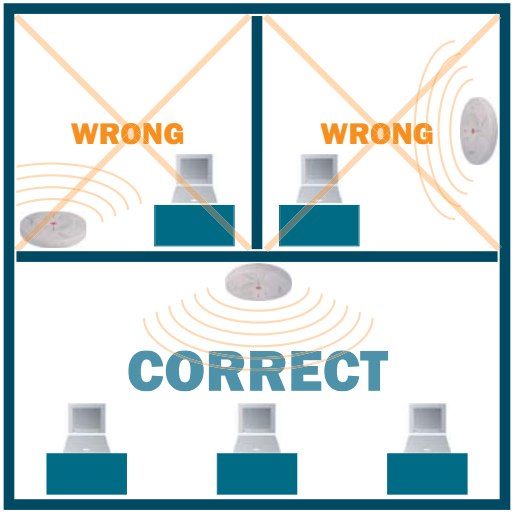


Figure 29. Array Placement

Wiring Considerations

Before using the Xirrus-supplied Power over Gigabit Ethernet modules (PoGE) to distribute power, see "Power over Gigabit Ethernet (PoGE)" on page 13.

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

Power

- No separate power cable to the Array is required when 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 models with no console port, such as the XR-500, XR-1000, and some XR-2000 models, 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 and Connecting the Array
Power over Gigabit Ethernet (PoGE)

Mounting and Connecting the Array

A number of options are available for mounting Arrays, depending on the model:

- 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 available at support.xirrus.com for the mounting option that you selected when ordering your Array. Please follow the provided instructions carefully.

Data and power connections to the Array are detailed in the *Quick Installation Guide* for the Array or Access Point model, also available at support.xirrus.com. Please follow the cabling and connection instructions carefully.

Dismounting the Array

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.

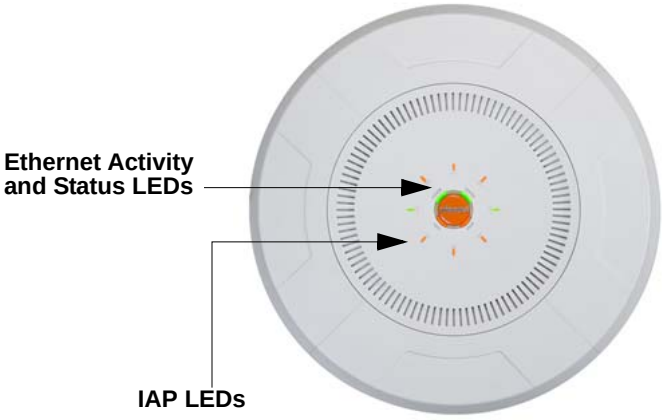


Figure 30. LED Locations

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 340.

Array LED Operating Sequences

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

- **"LED Boot Sequence" on page 65**
- **"LED Operation when Array is Running" on page 66**

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. Green or orange per table on the next page. Behavior may be changed using "LED Settings" on page 340.

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 340 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)
STATUS LED is GREEN ***	Array is operational
GIG (Ethernet) LEDs are dual color **Ethernet LED is ORANGE** **Ethernet LED is GREEN**	 Transferring data at 1 Gbps Transferring data at 10/100 Mbps
*** *NOTE: On an XR-2000 Series Array model ending an a* ***5****, there is a combined* ***GIG2/STS*** *LED. If the GIG2 port is not connected, the LED behaves as a Status LED. If the GIG2 port is connected, the LED behaves as a GIG2 LED.*	

See Also

Installation Prerequisites
Installation Workflow
Installing Your Wireless Array
LED Settings

Establishing Communication

If you are a Xirrus Cloud customer or if this Access Point is part of an XMS "profile" managed network, your Access Points are completely managed by XMS, and you will not be able to access CLI or the Web Management Interface under normal operating circumstances. In these cases, wait five minutes after powering up the Array or Access Point, then use XMS to view/manage this unit.

Zero-Touch Setup Using Mobilize

Xirrus Arrays and Access Points feature zero-touch setup. The license, software image, and configuration are all automatically downloaded to an Array after it is deployed. This occurs as soon as a new, unlicensed Array has been installed and connected to a network with DHCP and Internet access.

Note that the Array/AP must already be running ArrayOS release 6.5 or above to support Mobilize access. Without Mobilize, Arrays and APs will still obtain their licenses automatically.

After booting, the Array contacts the Xirrus Mobilize cloud service with its serial number and MAC address. Mobilize sends commands to the Array to download and update the appropriate license, software image, and configuration, and then reboots the Array. Mobilize service is included at no charge with the purchase of every Xirrus wireless device. Note that every unlicensed Array obtains its license in this way. You have the option of whether or not to use Mobilize to update your software image and download initial configuration.

The initial Array configuration sets items such as the SSIDs, encryption and authentication, and SNMP settings. Use the Mobilize service to specify these

settings for each Array before deployment. Settings may be duplicated from one Array to the next or entered in bulk. Please see the *Xirrus Mobilize User's Guide*.

Mobilize sets up an initial software image and configuration upon deployment of the Array. The Array will continue to check for further updates during a grace period after deployment (typically two weeks). After the grace period Mobilize does not provide continuing software and configuration updates. For ease of ongoing management, Xirrus recommends using XMS. Please see "Xirrus Management System (XMS)" on page 2. Note that your Xirrus wireless equipment will continue to be able to fetch and activate license updates to which you are entitled. See "License Key/Auto-provisioning:" on page 375.

User Interfaces (CLI, WMI)

With the zero-touch setup provided by Mobilize, your Xirrus network is ready for use a few minutes after deployment. We recommend that you use the Xirrus Management System (XMS) for ongoing monitoring and fine-tuning of the network.

Should you wish to check the configuration of individual Arrays locally, Array settings may be viewed or configured through the Command Line Interface (CLI) using SSH, or on a browser with the Web Management Interface (WMI). You may use the CLI via the serial management port (console—on all Arrays except the XR-500 and XR-1000 Series and some XR-2000 models) or any of the Gigabit Ethernet ports. You can use the WMI via any of the Array's Ethernet ports. Note that Arrays that are managed via XMS may only allow local access in read-only mode (see "XMS-Managed Arrays Restrict Local Management" on page 78 for details).

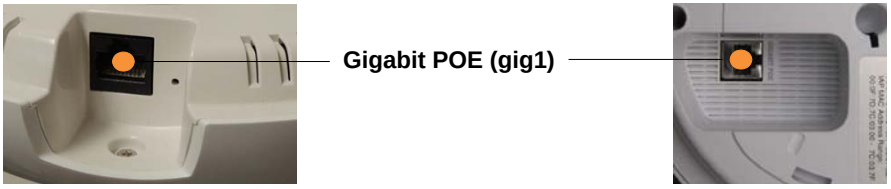


Figure 31. Network Interface Ports—XR-520 (left); XR-1000 Series (right)

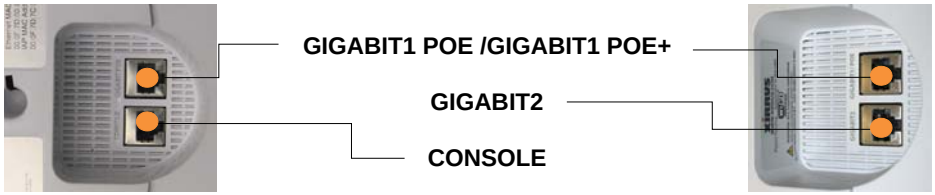


Figure 32. Network Interfaces—XR-2000 Series (left); XR-2005 Series (right)

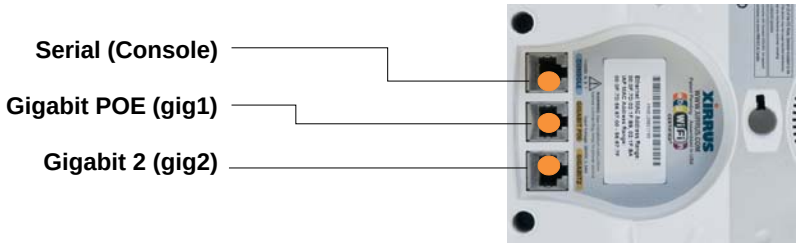


Figure 33. Network Interface Ports—XR-4000 Series

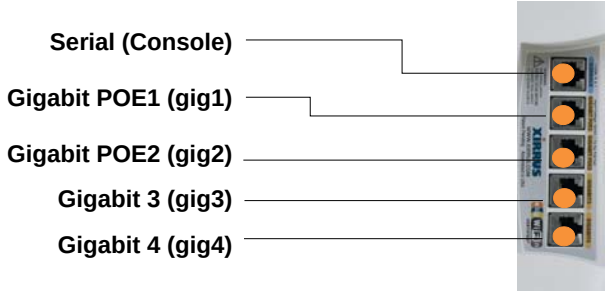


Figure 34. Network Interface Ports—XR-6000 Series

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-500 and XR-1000 Series and some XR-2000 models, which do not have a console port. See "Securing Low Level Access to the Array" on page 73.

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. You may use the serial port to change settings on the Array, even if the Array's gigabit interfaces are in XMS managed mode (i.e., read-only mode, see "XMS-Managed Arrays Restrict Local Management" on page 78).

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 (if any) will default to 10.0.2.1 with a mask of 255.255.255.0.

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 console port (on all models except the XR-500, XR-1000, and some XR-2000 models). 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.
4. If the Array cannot obtain an IP address via DHCP, the factory default uses a static IP address of 10.0.2.1 with a mask of 255.255.255.0 on its Gigabit POE port.

Take care to ensure that your network is not using the 10.0.2.1 IP address prior to connecting the Array to the network.

To connect to the Array, you must set your laptop to be in the same subnet as the Array: set your laptop's IP address to be in the 10.0.2.xx

subnet, and set its subnet mask to 255.255.255.0. If this subnet is already in use on your network, you may connect your laptop directly to the Array by connecting the laptop to the power injector's IN port temporarily (this port may be called the SWITCH port or the DATA port on your injector).

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

Licensing

When a newly deployed Array boots up, it automatically contacts Xirrus with its serial number and MAC address and obtains its license key, software image, and initial configuration. Any unlicensed Array will update in this way after it boots up, if it has Internet connectivity.

A license is needed to enable the full functionality of the Array. Without a license, the Array can be powered up and will only have a basic wireless network configuration including just one operating radio.

The Array's license determines some of the features that are available on the Array. For example, the Application Control feature on XR Arrays requires a

license. The Array's license is not installed at the factory. The Array must have a license before providing wireless service.

If you need to enter the license manually, use the following procedure. It describes entering the license key using the WMI. If you are using the Xirrus Management System (XMS), you may use it to manage and upgrade large numbers of licenses for the wireless network. XMS Cloud will perform these functions for you automatically.

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 **Configuration** section, click **Express Setup**.
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 **Apply** 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.

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. If you are not using Mobilize to perform your initial configuration, please see "Express Setup" on page 159. Also see "Zero-Touch Setup Using Mobilize" on page 67.

See Also

Establishing Communication
Installation Prerequisites
Installation Workflow
Logging In
Multiple SSIDs

Securing Low Level Access to the Array

Most local management of the Xirrus Array is done via the Web Management Interface (WMI) or CLI—see "The Command Line Interface" on page 397. 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 may change on the Express Setup page (see Step 5 on page 163).

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-500 and XR-1000 Series Arrays and some XR-2000 models), 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 70. 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-500 and XR-1000 and some XR-2000 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.

! *If you disable Xircon access to both XBL and CLI on models with no console port, you must ensure that you do not lose track of the username and password to log in to CLI/WMI! In this situation, there is no way to recover from a lost password, other than returning the Array to Xirrus. If you have Xircon access to XBL enabled, you can reset the password, but this recovery will require setting the unit to factory defaults with loss of all configuration data.*

- 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 385). Skip to Step 4 on page 75.

   To access CLI via SSH, see "Establishing a Secure Shell (SSH) Connection" on page 398. 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 5 on page 163, or the default value of **admin**/**admin** if you have not changed them.

```
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
```

```
Array42#
```

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

```
Array42#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.

```
Array42#(config)#boot-env
Array42#(config-boot)#set username newusername
Array42#(config-boot)#set password newpassword
Array42#(config-boot)#save
Saving boot environment .... OK
Array42(config-boot)# exit
```

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

```
Array42#(config)# management
Array42#(config-mgmt)# xircon <management-status>
Array42#(config-mgmt)# save
Array42#(config-mgmt)# exit
Array42#(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 221. 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:

- **XMS-Managed Arrays Restrict Local Management**
- **An Overview**
- **Structure of the WMI**
- **User Interface**
- **Logging In**
- **Applying Configuration Changes**

If you are a Cloud XMS customer, then Arrays are managed via the cloud, and local Array management interfaces are inaccessible.

If the Array is being managed by your own server for XMS Release 6.5 or above, and if the Array has been assigned to a named network in XMS, you will be restricted to read-only Array access. See "XMS-Managed Arrays Restrict Local Management" on page 78.

XMS-Managed Arrays Restrict Local Management

For Xirrus deployments of any size, we recommend that you use the Xirrus Management System (XMS) to manage the network rather than directly managing each Array individually. When Arrays are under management by XMS, configuration changes typically cannot be made directly by the WMI and CLI. This ensures that the Array configuration remains consistent with its corresponding settings in XMS, and that no settings are configured that would be incompatible with XMS management of the Array.

The Array has two operating modes: XMS Managed and Non-XMS Managed.

XMS Managed Mode:

- The Array is put into this mode if it is being managed by Release 6.5 or higher of either XMS or XMS Cloud, and if it has been assigned to a Profile Network that has been defined in XMS.
- Users, even those with administrator privileges (read-write), are restricted to read-only privileges when accessing the WMI (via HTTP and HTTPS) and CLI (via SSH and Telnet), regardless of user account write privileges. You will be advised of this at login with the following message:

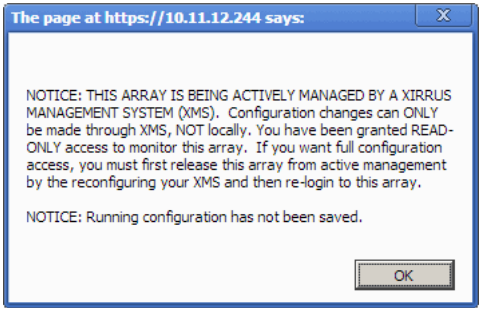


Figure 35. Notice for XMS-Managed Array

- XMS managed mode may be overridden for troubleshooting or emergency purposes using the **xms-override** CLI command (see "Top Level Commands" on page 401). After using this command, the user account's access privileges for the Array apply to the CLI session, but

only for the duration of the user session. At the next login by this user, privileges revert to read-only. There is no equivalent override command for the WMI, and it is not possible to use the WMI to make changes to the Array settings at all when the Array is in XMS managed mode.

Overriding XMS managed mode still allows XMS operations to proceed. For example:

- XMS continues polling for statistics.
- You may still make configuration changes to the Array via XMS, and those changes will be made on the Array. Similarly, changes made to an XMS Network (XMS Release 6.5 and later) that includes this Array will still be "pushed" to this Array—this will entirely replace the Array's configuration with XMS settings, replacing any local settings that you made on the Array.

XMS will be unaware of changes to Array settings that are made locally using the **xms-override** CLI command until the next XMS refresh cycle (typically daily), resulting in the Array's settings being out of synchronization with XMS. In XMS, you may go to the **Monitor > Arrays** or **Configure > Arrays** page, select the Array, and click the **Refresh** button to synchronize XMS with your change,. This causes XMS to read the current configuration of the Array and update the XMS database with these values.

For troubleshooting or emergency purposes, write access to the Array is always available via the serial (console) port. You can also use Xircon for this purpose, if so instructed by Xirrus Customer Support.

XMS Non-Managed Mode:

- The Array operates in this mode by default, and stays in this mode if it is not put into XMS managed mode as described above.
- A user with administrator privileges (read-write) has normal unrestricted access to modify settings via the WMI and CLI, as determined by the user account write privileges.

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. Options allow you to choose among different appearances for the WMI. See “Options” on page 392.

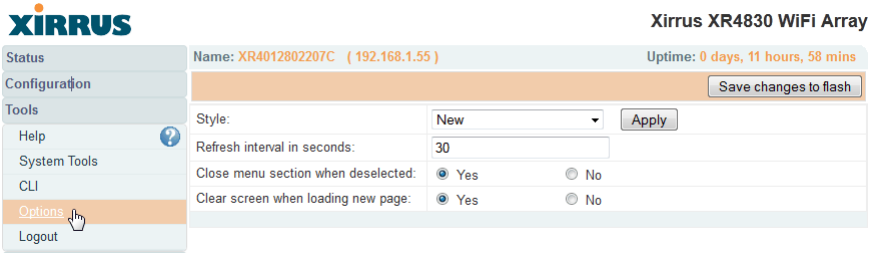


Figure 36. Web Management Interface—Option = New Style

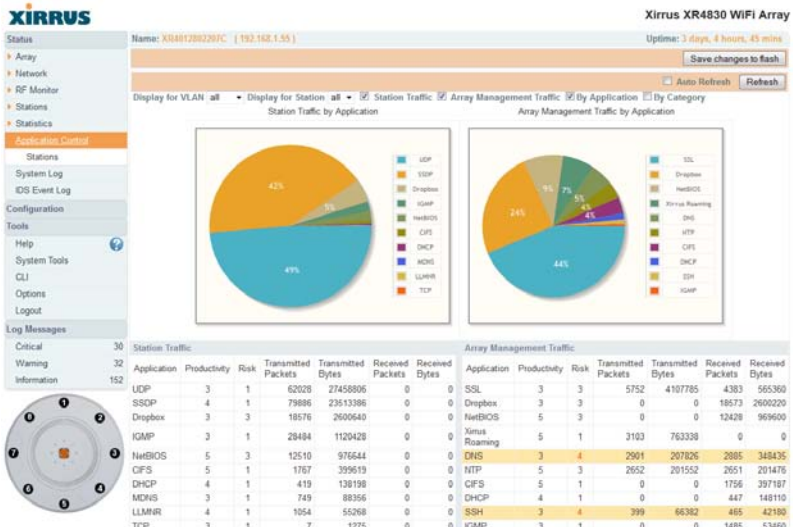


Figure 37. Web Management Interface—New Style (Default)

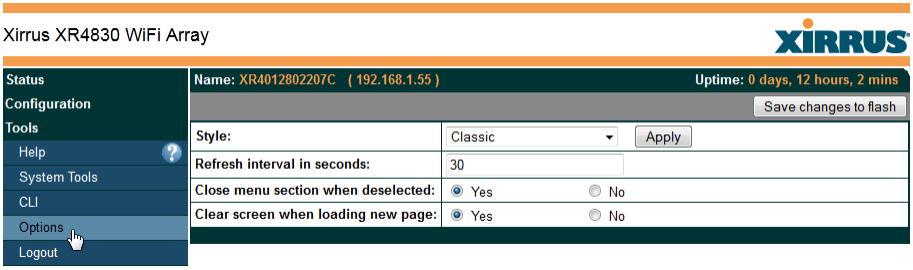


Figure 38. Web Management Interface—Option = Classic Style

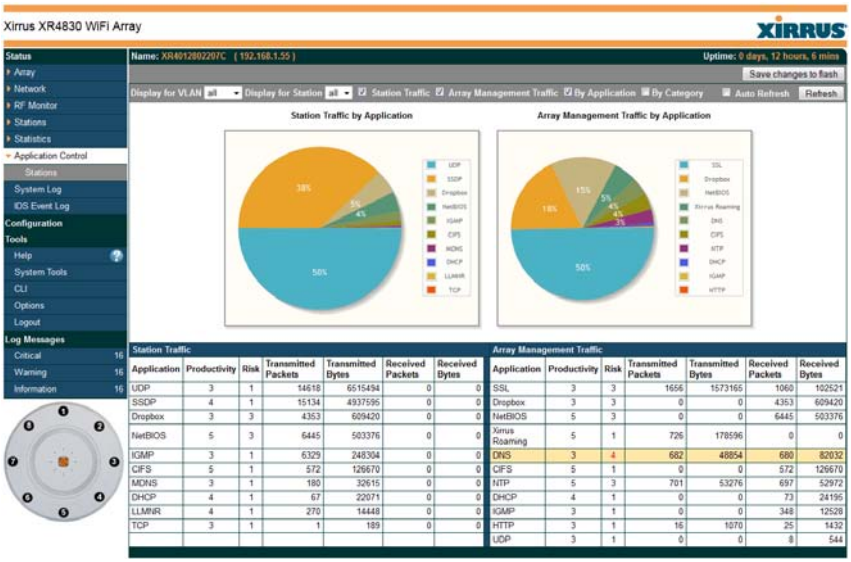


Figure 39. Web Management Interface—Classic Style

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.

Status Windows
- Array Status Windows
  - Array Summary
  - Array Information
  - Array Configuration
  - Admin History
- Network Status Windows
  - Network Map
  - Spanning Tree Status
  - Routing Table
  - ARP Table
  - DHCP Leases
  - Connection Tracking/NAT
  - CDP Neighbors
  - Network Assurance
- RF Monitor Windows
  - IAPs
  - Spectrum Analyzer
  - Intrusion Detection
  - Channel History
  - Radio Assurance
- Station Status Windows
  - Stations
  - Location Map
  - RSSI
  - Signal-to-Noise Ratio (SNR)
  - Noise Floor
  - Max by IAP
  - Station Assurance

Statistics Windows
- IAP Statistics Summary
- Per-IAP Statistics
- Network Statistics
- VLAN Statistics
- WDS Statistics
- IDS Statistics
- Filter Statistics
- Station Statistics
- Per-Station Statistics

Application Control Windows

System Log Window

IDS Event Log Window

Configuration Windows

- Express Setup
- Network
  - Network Interfaces
  - Network Bonds
  - DNS Settings
  - CDP Settings
- Services
  - Time Settings (NTP)
  - NetFlow
  - Wi-Fi Tag
  - Location
  - System Log
  - SNMP
  - DHCP Server
- VLANs
  - VLAN Management
- Tunnels
  - Tunnel Management
- Security
  - Admin Management
  - Admin Privileges
  - Admin RADIUS
  - Management Control
  - Access Control List
  - Global Settings
  - External Radius
  - Internal Radius
  - Rogue Control List
  - AirWatch
- SSIDs
  - SSID Management
  - Active IAPs
  - Per-SSID Access Control List
- Groups
  - Group Management

Configuration Windows (cont'd)

- IAPs
  - IAP Settings
  - Global Settings (IAP)
  - Global Settings .11an
  - Global Settings .11bgn
  - Global Settings .11n
  - Global Settings .11u
  - Advanced RF Settings
  - Hotspot 2.0
  - NAI Realms
  - NAI EAP
  - Intrusion Detection
  - LED Settings
  - DSCP Mappings
  - Roaming Assist
- WDS
  - WDS Client Links
- Filters
  - Filter Lists
  - Filter Management
- Clusters
  - Cluster Definition
  - Cluster Management
  - Cluster Operation

Tool Windows

- System Tools
- CLI
- Options
- Logout

User Interface

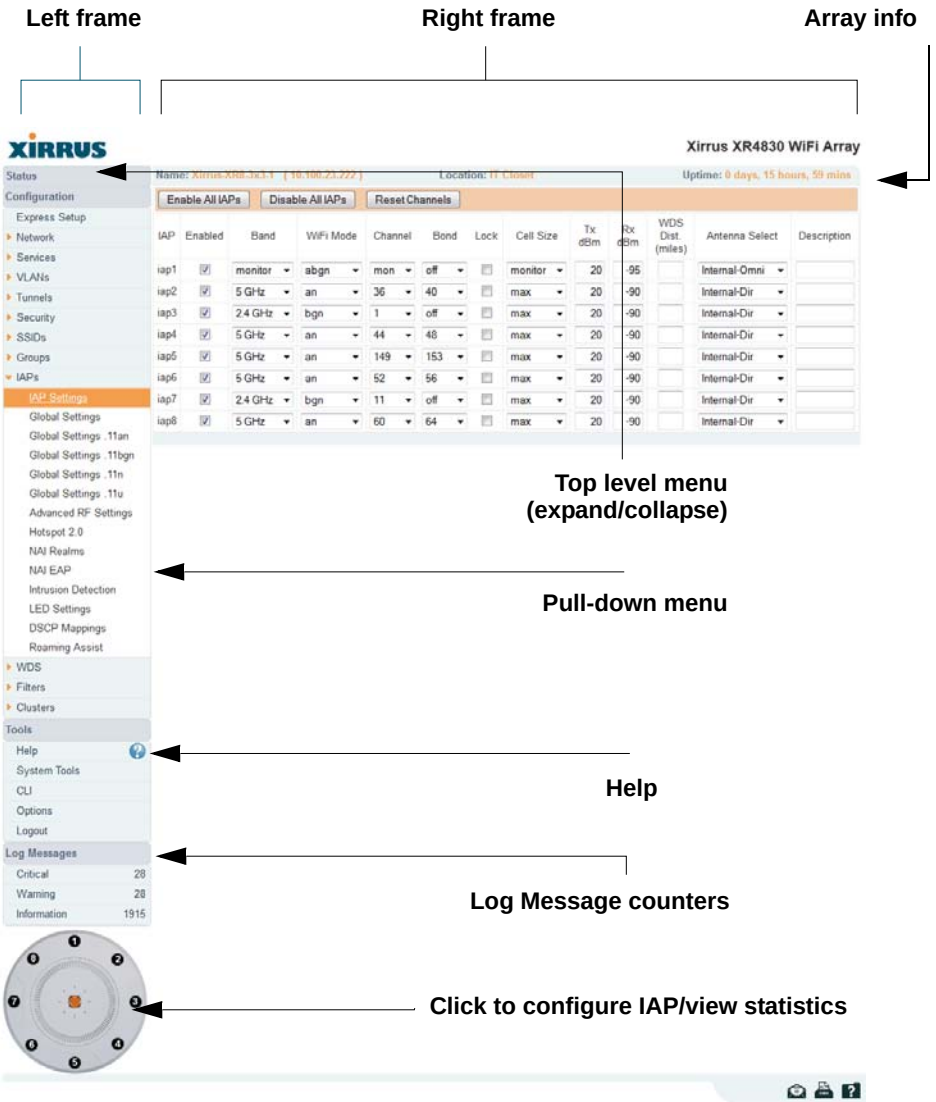


Figure 40. WMI: Frames

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.

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 154.
- 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.

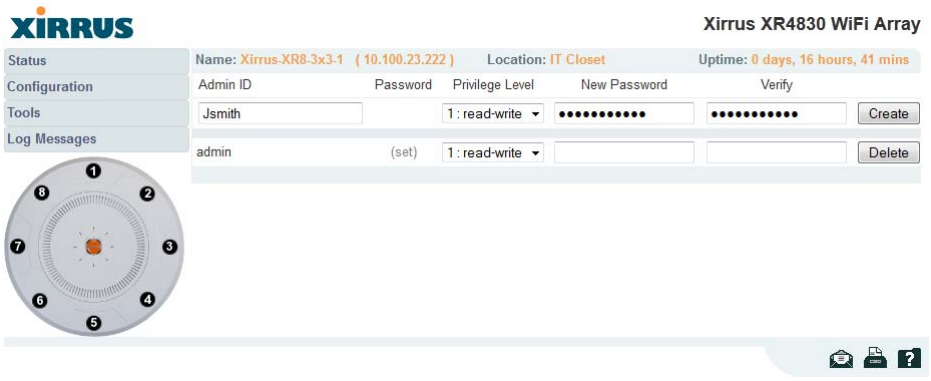


Figure 41. Major Menu Sections Collapsed (on left)

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 373**.*

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 392 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.

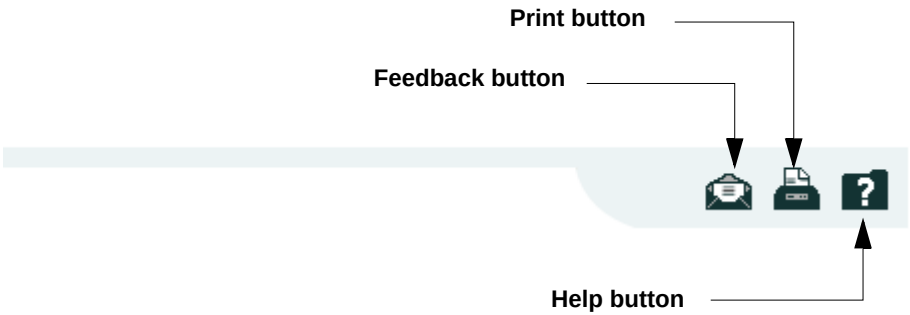


Figure 42. WMI: Utility Buttons

- Click on the **Feedback** button to generate a Web page that allows you to submit your comments to Xirrus, Inc.
- Click on the **Print** button to send a print file of the active window to your local printer.
- Click on the **Help** button to access the Array's online help system.

Submitting Your Comments

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

Logging In

If you are a Cloud XMS customer, then Arrays are managed via the cloud, and local Array management interfaces are inaccessible.

If the Array is being managed by your own server for XMS Release 6.5 or above, and if the Array has been assigned to a named network in XMS, you will be restricted to read-only Array access. See "XMS-Managed Arrays Restrict Local Management" on page 78.

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, XR0823091CACD).

   Otherwise, enter the Array's IP address. This may be determined as described in "Using the Ethernet Ports" on page 70.
3. To log in to the Array's Web Management Interface, enter **admin** for both the user name and password.

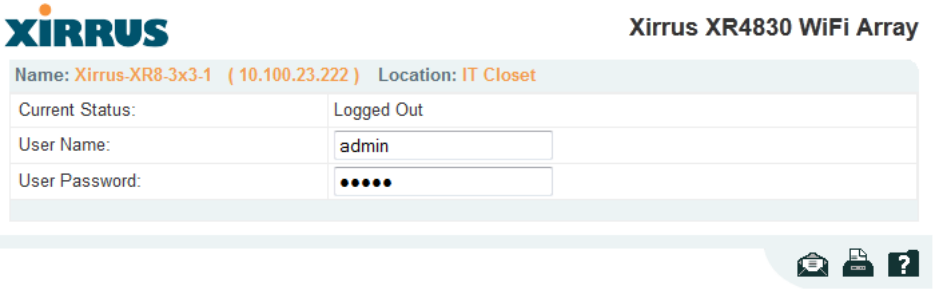


Figure 43. Logging In to the Wireless Array

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

If you are a Cloud XMS customer, then Arrays are managed via the cloud, and local Array management interfaces are inaccessible.

If the Array is being managed by your own server for XMS Release 6.5 or above, and if the Array has been assigned to a named network in XMS, you will be restricted to read-only Array access. See "XMS-Managed Arrays Restrict Local Management" on page 78.

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 92**
- **"Network Status Windows" on page 100**
- **"RF Monitor Windows" on page 111**
- **"Station Status Windows" on page 122**
- **"Statistics Windows" on page 137**
- **"Application Control Windows" on page 147**
- **"System Log Window" on page 154**
- **"IDS Event Log Window" on page 155**

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

- **"Configuring the Wireless Array" on page 157**
- **"Using Tools on the Wireless Array" on page 371**

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 85)

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.

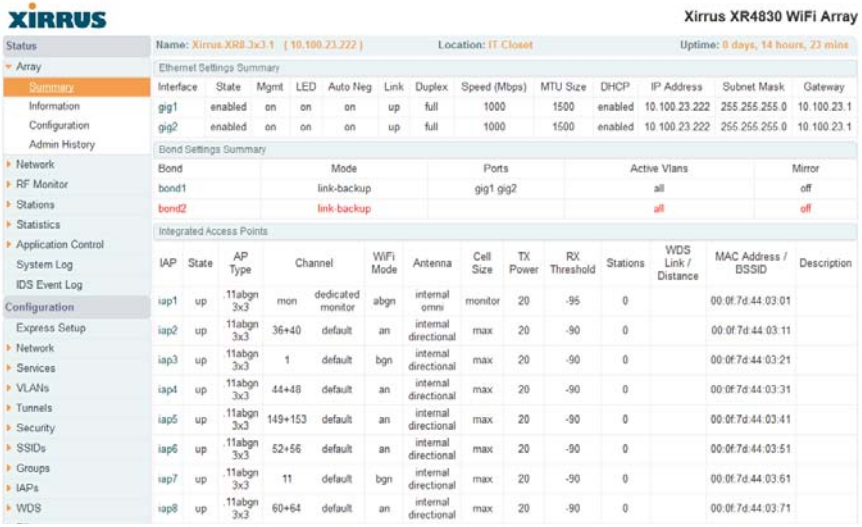


Figure 44. Array Summary

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 167.
  - **Interface**: Lists the network interfaces that are available on the Array.
  - **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 171.
  - **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 171 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 279.
  - **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 45 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 39.

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:56:87:80-81	
iap2	up	.11abgn 3x3	36+40	default	an	internal directional	small	5	-75	0		00:0f:7d:56:87:90-91	
iap3	up	.11abgn 3x3	1	default	bgn	internal directional	small	5	-75	0		00:0f:7d:56:87:a0-a1	
iap4	down	.11abgn 3x3	44+48	default	an	internal directional	small	5	-75	0		00:0f:7d:56:87:b0-b1	
iap5	up	.11abgn 3x3	6	default	bgn	internal directional	max	20	-90	0		00:0f:7d:56:87:c0-c1	
iap6	up	.11abgn 3x3	52+56	default	an	internal directional	max	20	-90	0		00:0f:7d:56:87:d0-d1	
iap7	up	.11abgn 3x3	11	default	bgn	internal directional	max	20	-90	0		00:0f:7d:56:87:e0-e1	
iap8	up	.11abgn 3x3	60+64	default	an	internal directional	max	20	-90	0		00:0f:7d:56:87:f0-f1	

Figure 45. 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 279.
- **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.

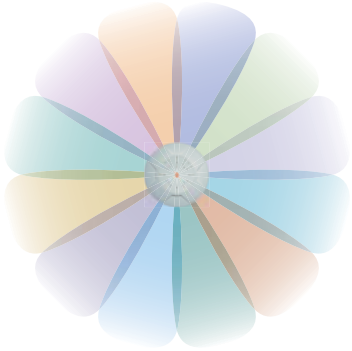


Figure 46. IAP Cells

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 279. 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 30.

- **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.
- **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 345.
- **MAC Address/BSSID**: Shows the MAC address for each IAP.
- **Description**: The description (if any) that you set for this IAP.
-

- **Network Assurance Section**

  This section shows the results of ongoing network assurance testing. This is the same as information shown in "Network Assurance" on page 109.

Network Assurance

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	204.2.134.163	Connectivity OK
RADIUS primary server	Radius1	10.100.25.12	No connectivity
RADIUS secondary server	Radius2		Hostname unresolved
SNMP trap host 1	Xirrus-XMS	10.100.23.53	Connectivity OK
gig1 IP gateway		10.100.44.1	Connectivity OK
gig2 IP gateway		10.100.44.1	No connectivity

Operating Status

Controller Temperature	Fan Speed
41 °C (105 °F)	1920 RPM

Figure 47. Network Assurance and Operating Status

The Array checks connectivity to network servers that you have configured (for example, DNS and NTP servers) on an ongoing basis. For each Setting, 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 221.

- **Operating Status Section**
  This section shows the Array controller board's current internal temperatures and current fan speed. (Figure 47)

See Also

Management Control
Network Interfaces
Network Bonds
IAP Settings
Network Assurance

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 373 and "Advanced Feature Sets" on page 17 for more information.

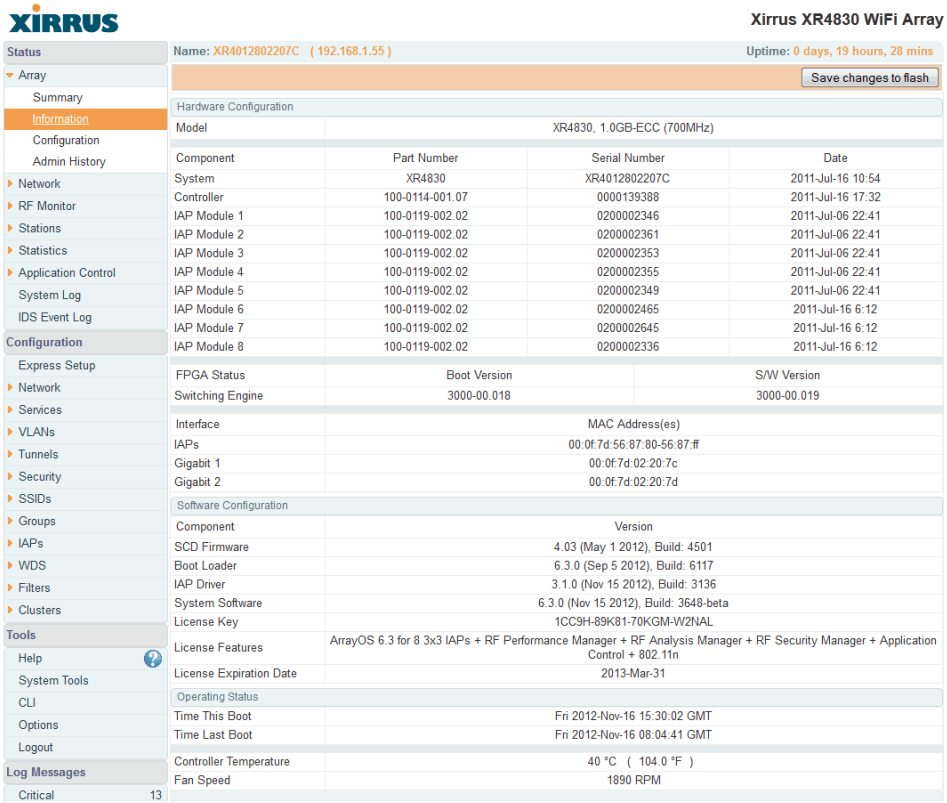


Figure 48. Array Information

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.

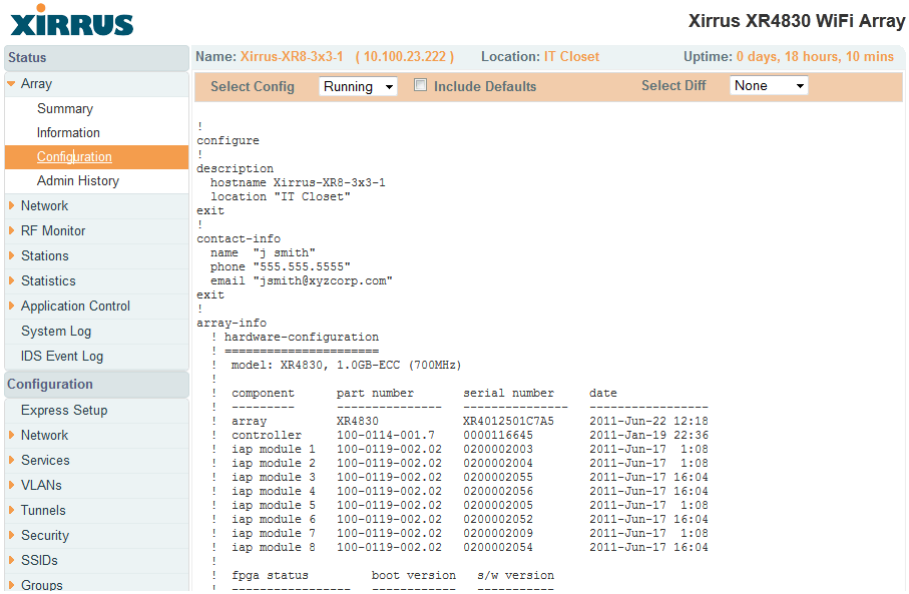


Figure 49. Show Configuration

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.

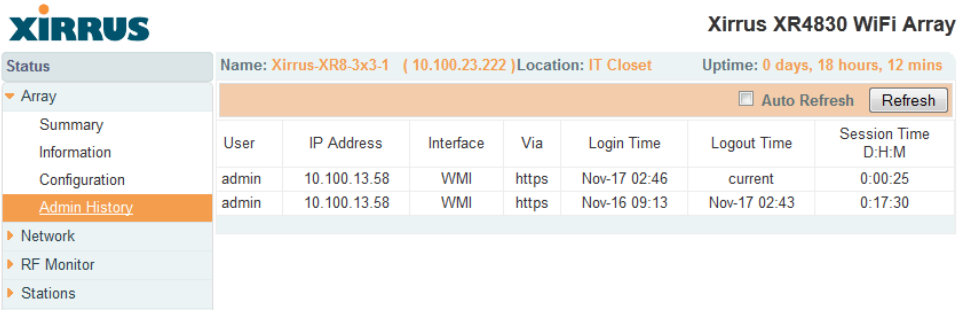


Figure 50. Admin Login History

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.
- **Undefined VLANs**—shows VLANs present on an 802.1Q connection to the Array, that are not configured in the Array's VLAN list.

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.

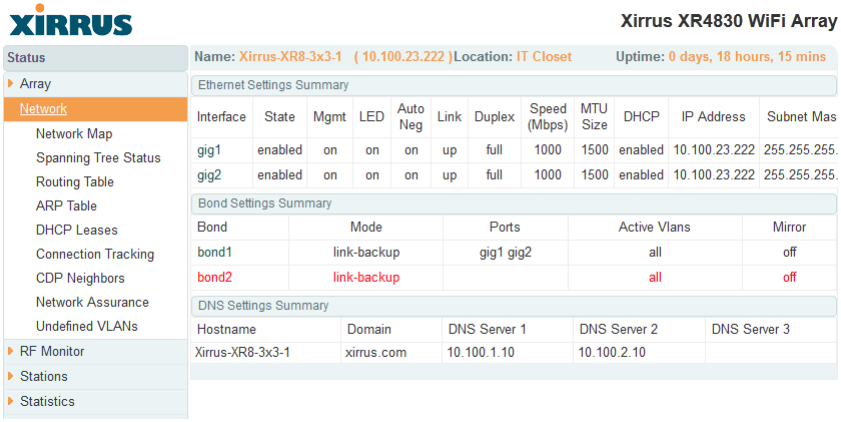


Figure 51. Network Settings

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

- **"Network Interfaces" on page 167**
- **"Network Bonds" on page 171**
- **"DNS Settings" on page 177**
- **"CDP Settings" on page 178**

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.

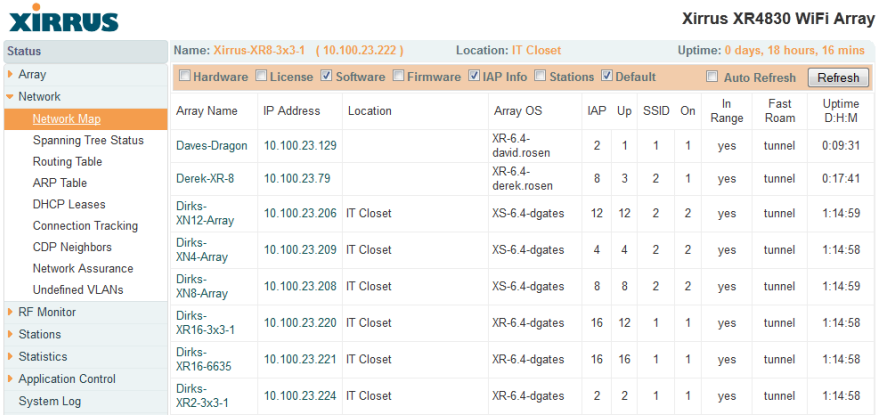


Figure 52. Network Map

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 159. 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 159.
- **Location**: The location assigned to the Array. To establish the location information, go to "Express Setup" on page 159.
- **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 159. To enable or disable individual IAPs, go to "IAP Settings" on page 279.
- **SSID**: Informs you how many SSIDs have been assigned for the Array. To assign an SSID, go to "SSID Management" on page 253.
- **(SSID) On**: Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to "SSID Management" on page 253.
- **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 285.
- **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 (XR-4820, XR-7630, 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 features enabled by the key.

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 123.

  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.

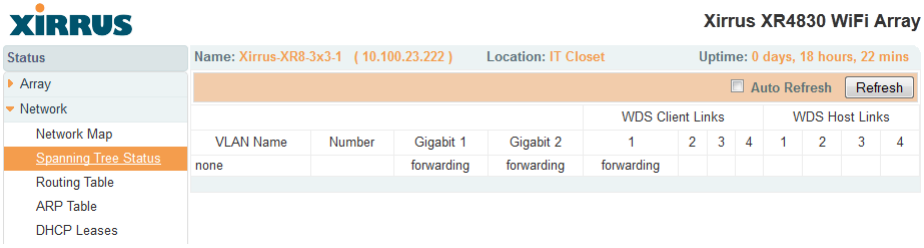


Figure 53. Spanning Tree Status

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.

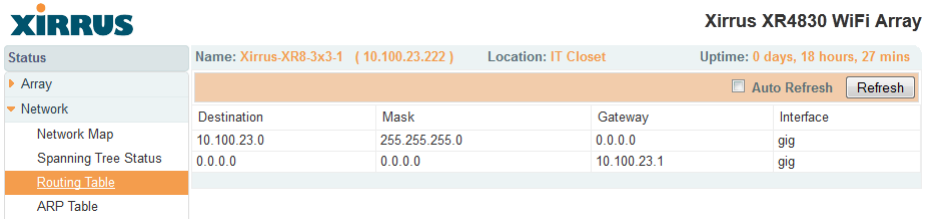


Figure 54. Routing Table

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.

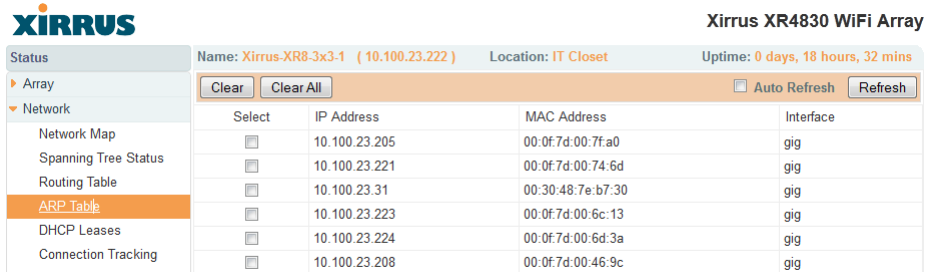


Figure 55. ARP Table

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.

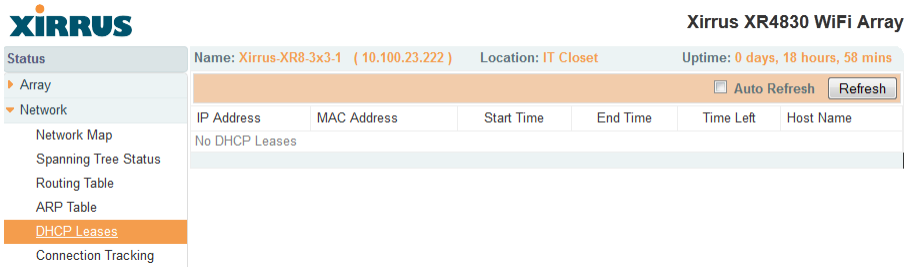


Figure 56. DHCP Leases

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.

Figure 57. Connection Tracking

Click the **Show Hostnames** checkbox at the top of the page to display name information (if any) for the source and destination location of the connection. The Hostname 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).

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 178.

Network Assurance

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

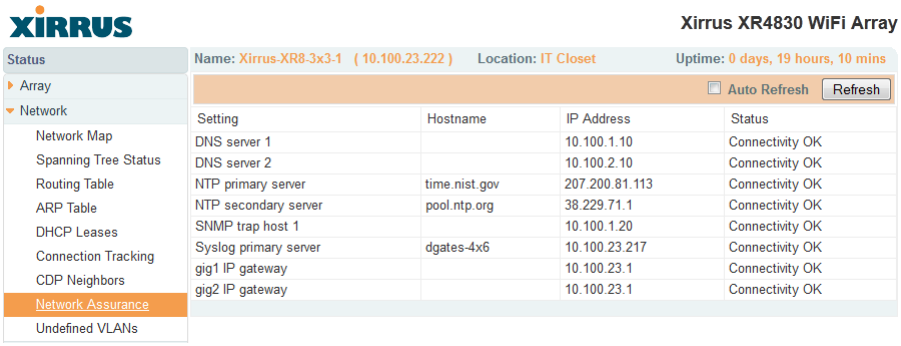


Figure 59. Network Assurance

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 221.

See Also

Management Control

Undefined VLANs

This status-only window lists VLANs that have not been configured on the Array, but that are being detected on the Array's trunk port(s), i.e. wired ports. See "VLANs" on page 199.

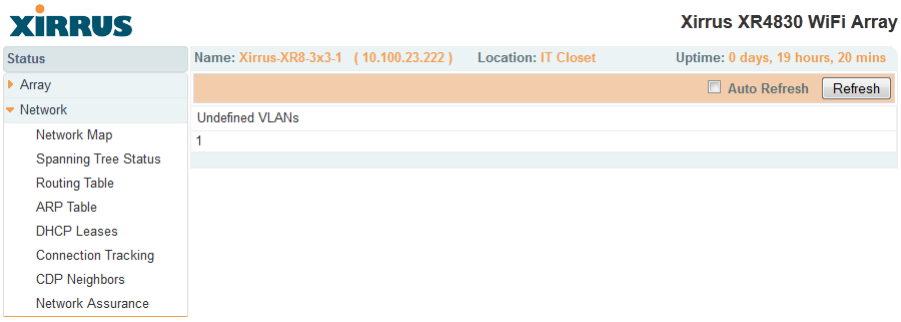


Figure 60. Undefined VLANs

This feature alerts you to the fact that an 802.1Q trunk to the Array has VLANs that are not being properly handled on the Array. To reduce unnecessary traffic, only VLANs that are actually needed on the Array should normally be on the trunk, e.g., the management VLAN and SSID VLANs. In some cases such as multicast forwarding for Apple Bonjour you may want to extend other VLANs to the Array, in order to forward Bonjour or other multicast packets (see "Advanced Traffic Optimization" on page 289).

See Also

VLANs

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.

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 118. For detailed information on the measurements displayed, please see "Spectrum Analyzer Measurements" on page 115.

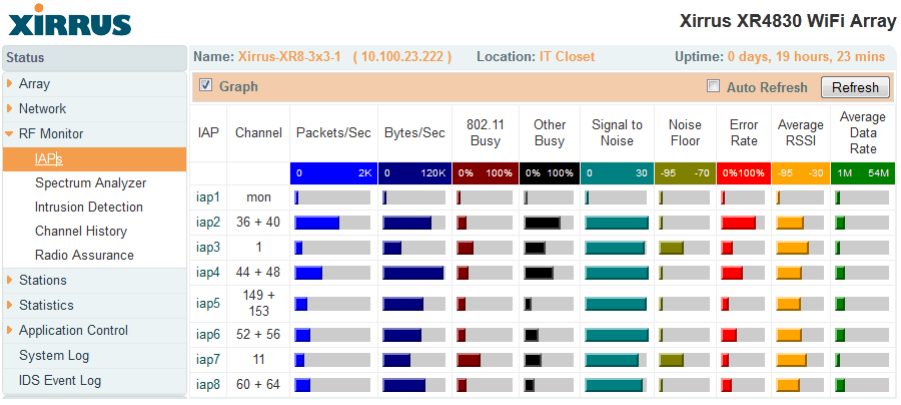
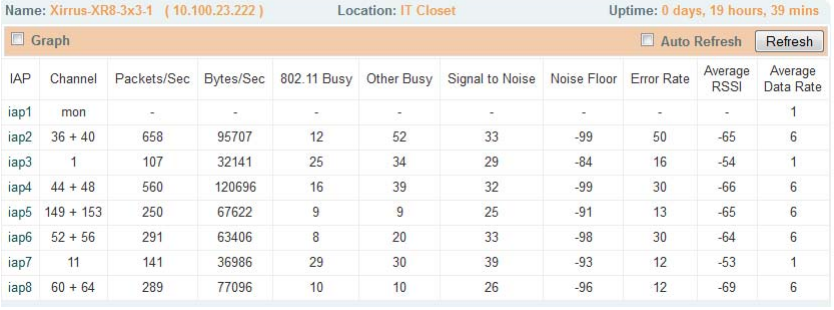


Figure 61. RF Monitor—IAPs

Figure 61 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.



IAP	Channel	Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate
iap1	mon	-	-	-	-	-	-	-	-	1
iap2	36 + 40	658	95707	12	52	33	-99	50	-65	6
iap3	1	107	32141	25	34	29	-84	16	-54	1
iap4	44 + 48	560	120696	16	39	32	-99	30	-66	6
iap5	149 + 153	250	67622	9	9	25	-91	13	-65	6
iap6	52 + 56	291	63406	8	20	33	-98	30	-64	6
iap7	11	141	36986	29	30	39	-93	12	-53	1
iap8	60 + 64	289	77096	10	10	26	-96	12	-69	6

Figure 62. 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 279.*

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 63 (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in "Spectrum Analyzer Measurements" on page 115.

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.

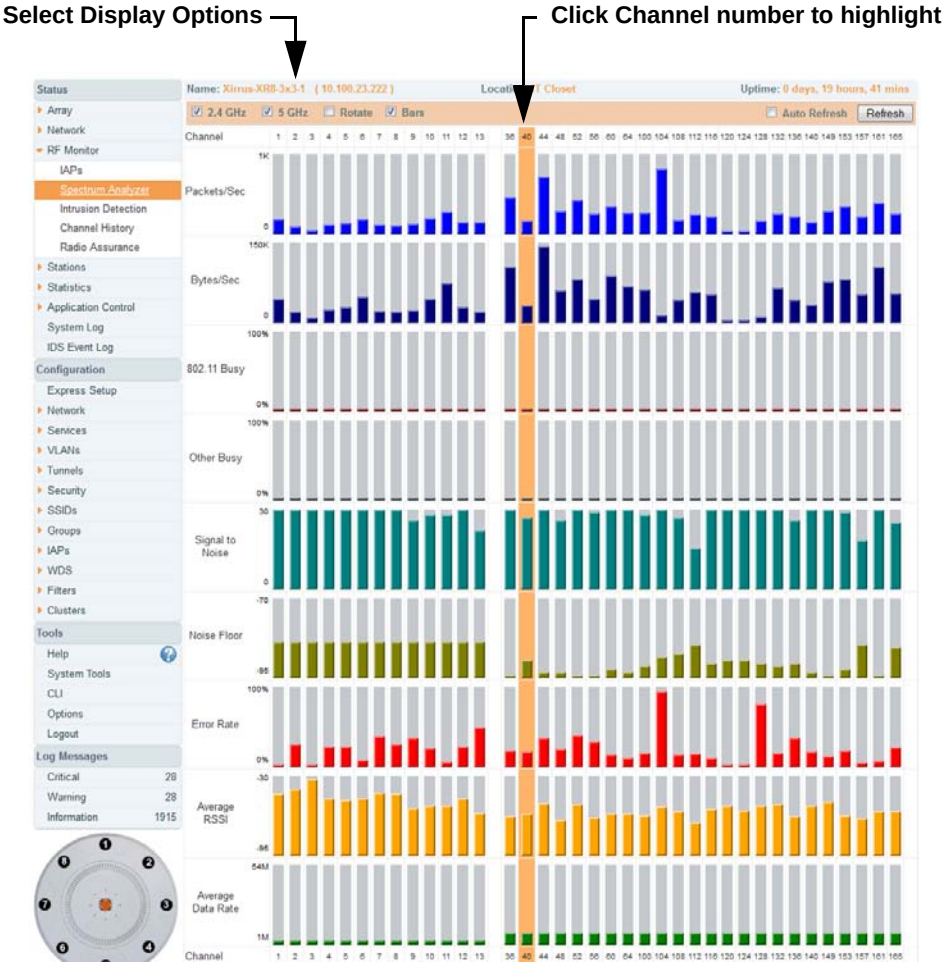


Figure 63. RF Spectrum Analyzer

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.

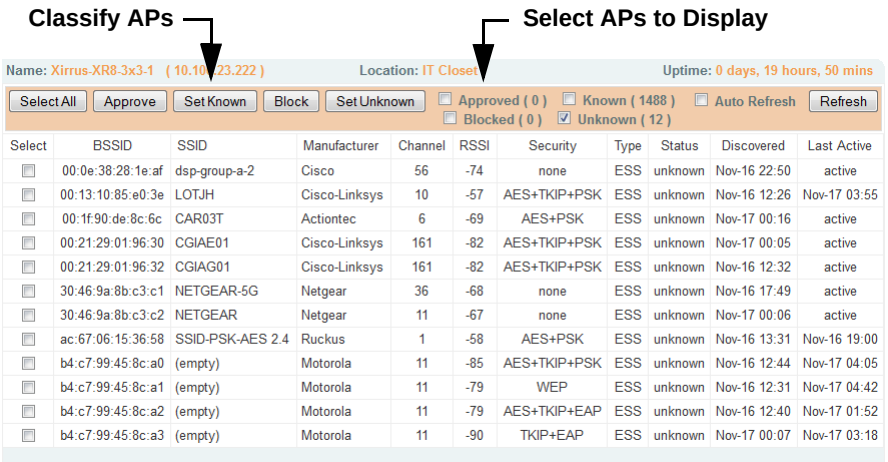
  The total busy time (802.11 Busy plus Other Busy) will never total more than 100%. The remaining time (100% minus total busy time) is quiet time—the time that no activity was seen on the channel.
- **Signal to Noise:** Average SNR (signal to noise ratio) seen on the channel, calculated from the signal 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 date 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 337.



Select	BSSID	SSID	Manufacturer	Channel	RSSI	Security	Type	Status	Discovered	Last Active
☐	00:0e:38:28:1e:af	dsp-group-a-2	Cisco	56	-74	none	ESS	unknown	Nov-16 22:50	active
☐	00:13:10:85:e0:3e	LOTJH	Cisco-Linksys	10	-57	AES+TKIP+PSK	ESS	unknown	Nov-16 12:26	Nov-17 03:55
☐	00:1f:90:de:8c:6c	CAR03T	Actiontec	6	-69	AES+PSK	ESS	unknown	Nov-17 00:16	active
☐	00:21:29:01:96:30	CGIAE01	Cisco-Linksys	161	-82	AES+TKIP+PSK	ESS	unknown	Nov-17 00:05	active
☐	00:21:29:01:96:32	CGIAG01	Cisco-Linksys	161	-82	AES+TKIP+PSK	ESS	unknown	Nov-16 12:32	active
☐	30:46:9a:8b:c3:c1	NETGEAR-5G	Netgear	36	-68	none	ESS	unknown	Nov-16 17:49	active
☐	30:46:9a:8b:c3:c2	NETGEAR	Netgear	11	-67	none	ESS	unknown	Nov-17 00:06	active
☐	ac:67:06:15:36:58	SSID-PSK-AES 2.4	Ruckus	1	-58	AES+PSK	ESS	unknown	Nov-16 13:31	Nov-16 19:00
☐	b4:c7:99:45:8c:a0	(empty)	Motorola	11	-85	AES+TKIP+PSK	ESS	unknown	Nov-16 12:44	Nov-17 04:05
☐	b4:c7:99:45:8c:a1	(empty)	Motorola	11	-79	WEP	ESS	unknown	Nov-16 12:31	Nov-17 04:42
☐	b4:c7:99:45:8c:a2	(empty)	Motorola	11	-79	AES+TKIP+EAP	ESS	unknown	Nov-16 12:40	Nov-17 01:52
☐	b4:c7:99:45:8c:a3	(empty)	Motorola	11	-90	TKIP+EAP	ESS	unknown	Nov-17 00:07	Nov-17 03:18

Figure 64. 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 115.

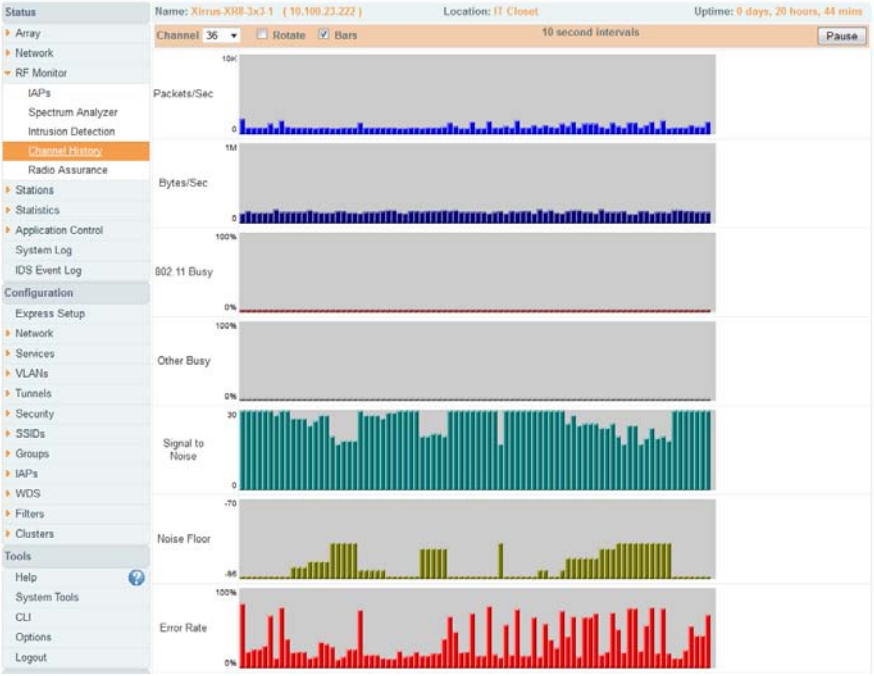


Figure 65. RF Monitor—Channel History

Figure 65 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 66)

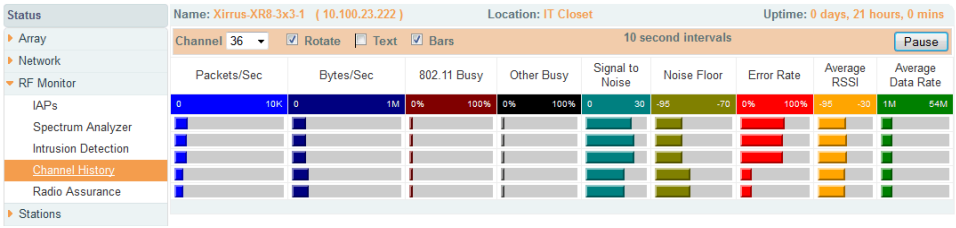


Figure 66. RF Monitor—Channel History (Rotated)

If you select **Rotate** and **Text** together, data is presented as a numerical table. (Figure 67)

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

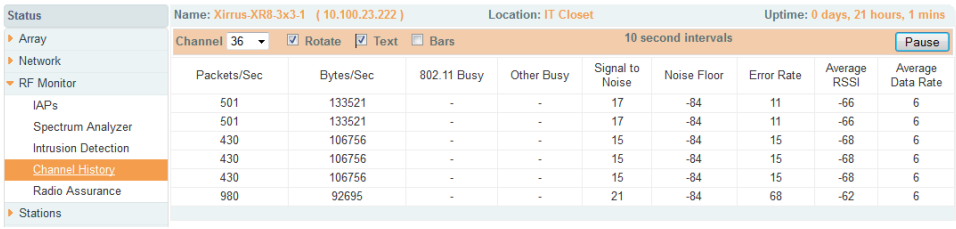


Figure 67. RF Monitor—Channel History (Text)

Radio Assurance

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 322. 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 489.

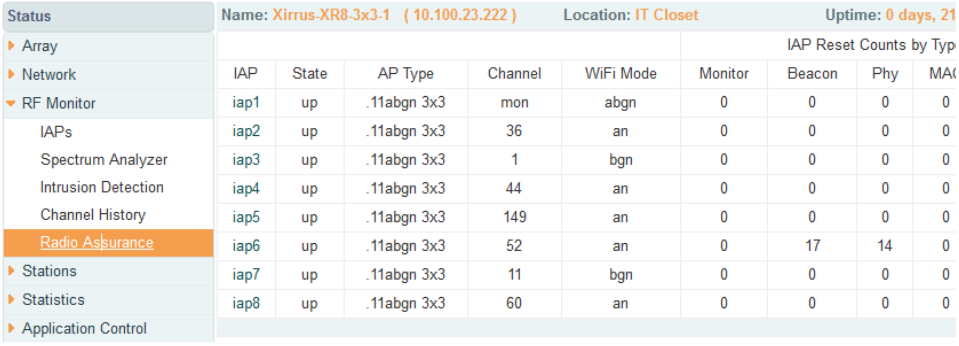


Figure 68. Radio Assurance

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.

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.

Figure 69. 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 228 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.

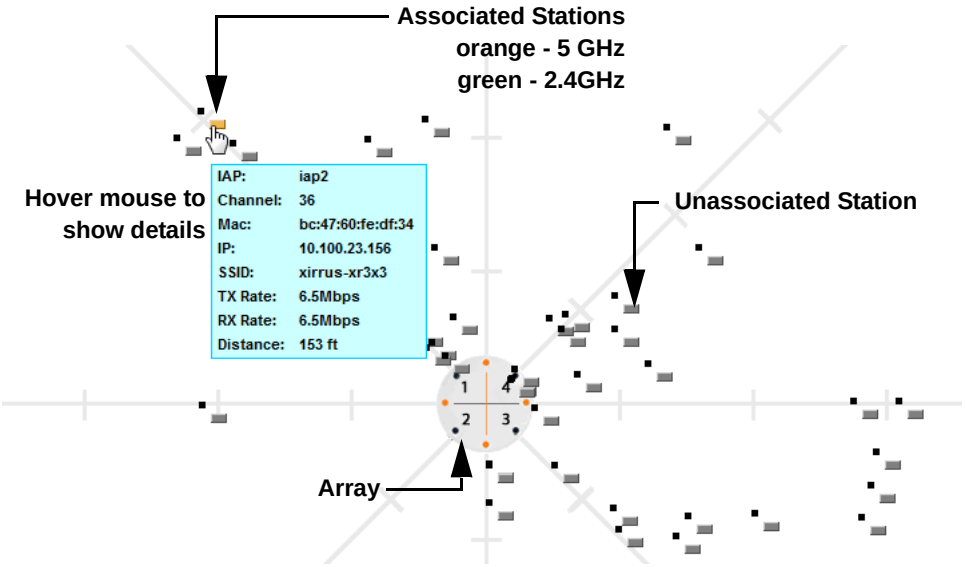


Figure 70. Location Map

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 128

Hover the mouse over a station to show detailed information. (Figure 70) 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.

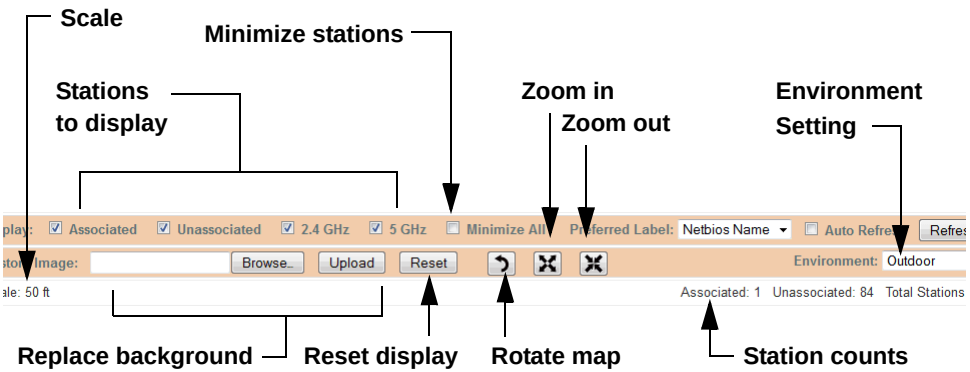


Figure 71. Controls for Location Map

- **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 802.11bgn stations, or 802.11an stations, or both.
- **Preferred Label**: This field is located on the top of the window towards the right. It shows the type of label to be displayed for stations: NetBIOS is the default, else, an 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.

- **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 128.
- **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 126), 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.

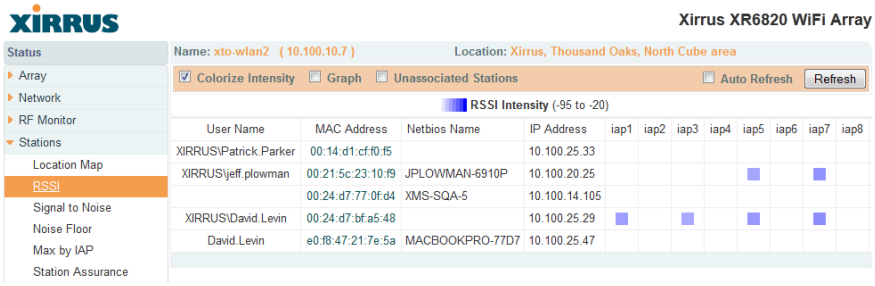


Figure 72. Station RSSI Values

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.

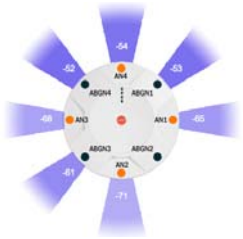


Figure 73. Station RSSI Values—Colorized Graphical View

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.

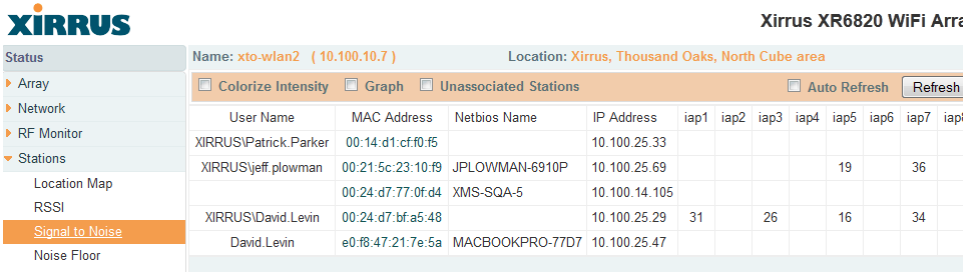


Figure 74. Station Signal-to-Noise Ratio Values

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.

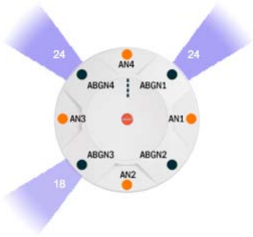


Figure 75. Station SNR Values—Colorized Graphical View

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.

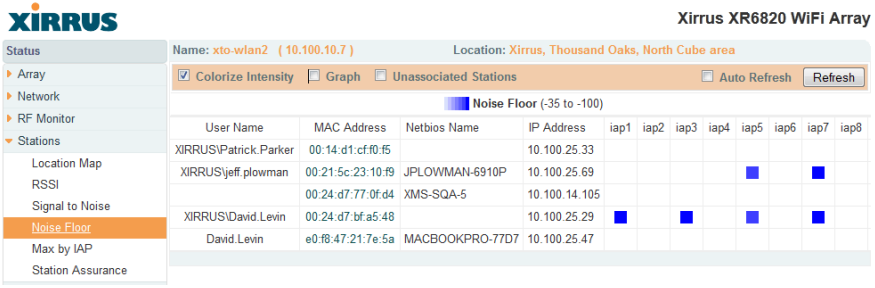


Figure 76. Station Noise Floor Values

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.

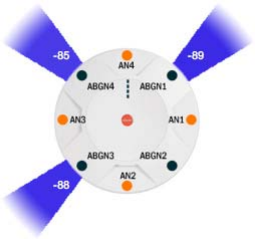


Figure 77. Station Noise Floor Values—Colorized Graphical View

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.

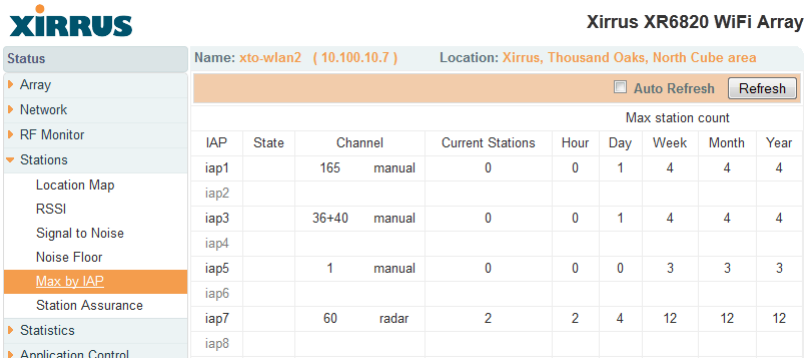


Figure 78. Max by IAP

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 327 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 327: associated time, authentication failures, packet error rate, packet retry rate, packet data rate, RSSI, signal to noise ratio (SNR), and distance.

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 138. 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.

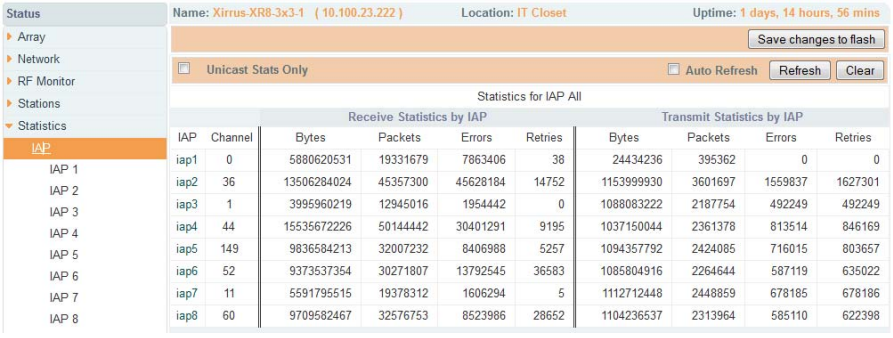


Figure 80. IAP Statistics Summary Page

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

Per-IAP Statistics

This is a status only window that provides detailed statistics for the selected IAP. For a summary of statistics for all IAPs, see "IAP Statistics Summary" on page 137. Use the **Display Percentages** checkbox at the upper 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 84.

Receive Error statistics include:

- **Total Retries**: the count of packets that were sent more than once before being received correctly.
- **CRC error**: the count of packets that were corrupted on the air and were dropped. Some level of CRC errors are expected in wireless networks. Note that all IAPs operate in a mode where they are listening to everything all the time, which means they will see many CRC errors.
- **Fragment Errors**: the count of packets that were incomplete.
- **Encryption Errors:** the count of packets that had encryption problems.
- **Duplicates**: the count of packets that were received more than once. The duplicate packets are dropped.

- **Dropped Packets**: the count of packets that were dropped due to various receive errors, including being received when all receive queues were full. These packets are dropped after being received.
- **Overruns**: indicate the number of times that First-In-First-Out (FIFO) overflow errors occur.

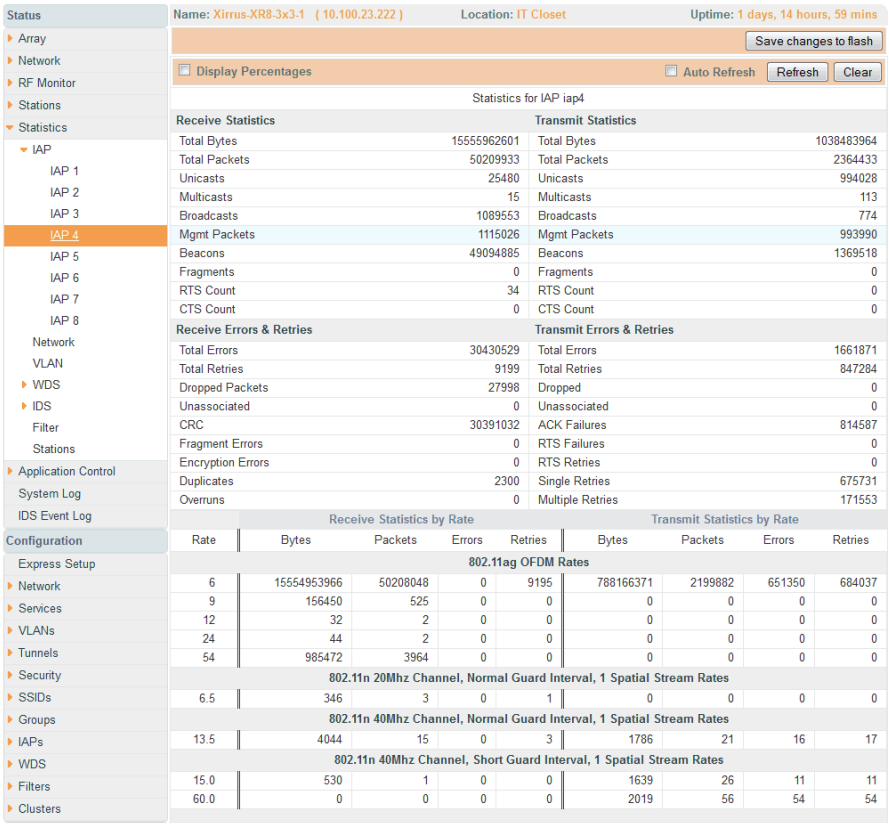


Figure 81. Individual IAP Statistics Page

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

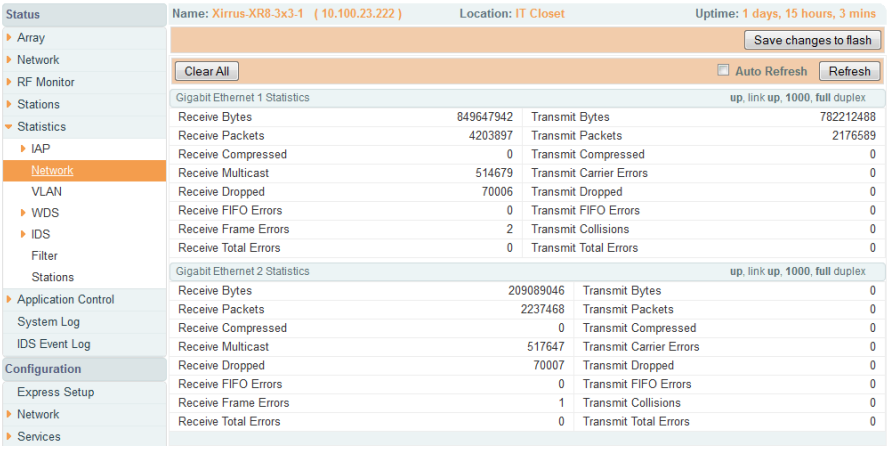


Figure 82. Network Statistics

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.

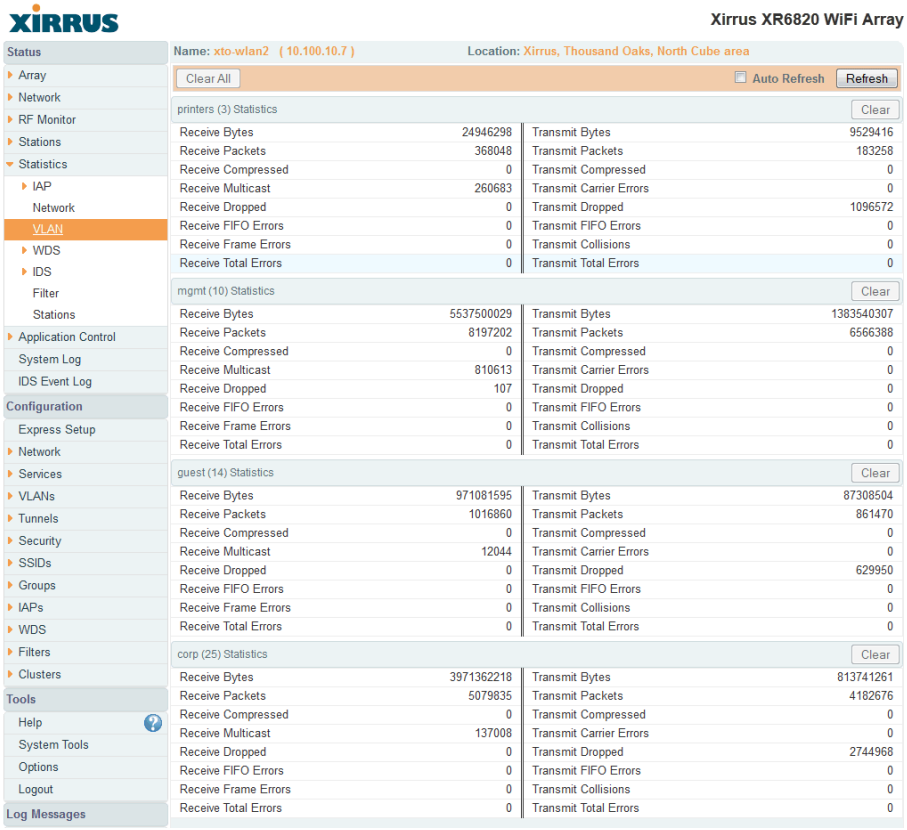


Figure 83. VLAN Statistics

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).

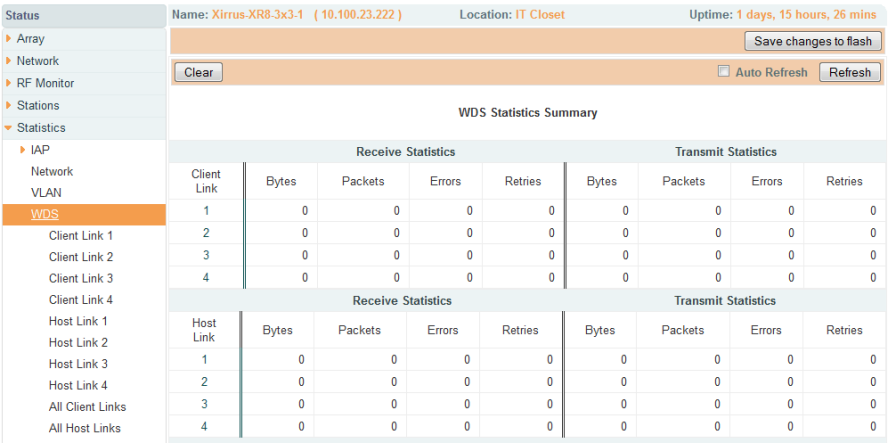


Figure 84. WDS Statistics

See Also

SSID Management
WDS

IDS Statistics

The Xirrus Array employs a number of IDS/IPS (Intrusion Detection System/ Intrusion Prevention System) strategies to detect and prevent malicious attacks on the wireless network. This status-only window provides detailed intrusion detection statistics for the selected IAP. Use the **Display Averages** checkbox at the upper left to select the output format—check this option to express each statistic as an average rate, or leave it blank to display raw counts.

Note that you must have **Intrusion Detection Mode** enabled to collect IDS statistics. See "Intrusion Detection" on page 334. Information about IDS events is discussed in the "IDS Event Log Window" on page 155

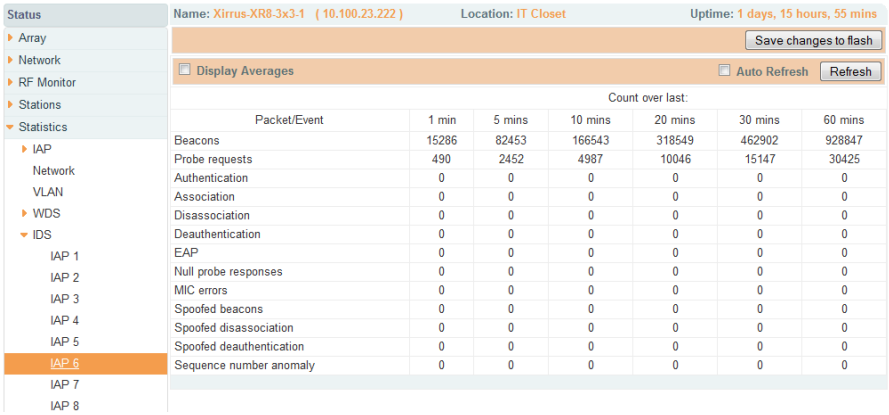


Figure 85. IDS Statistics Page

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

Intrusion Detection
IDS Event Log Window

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.

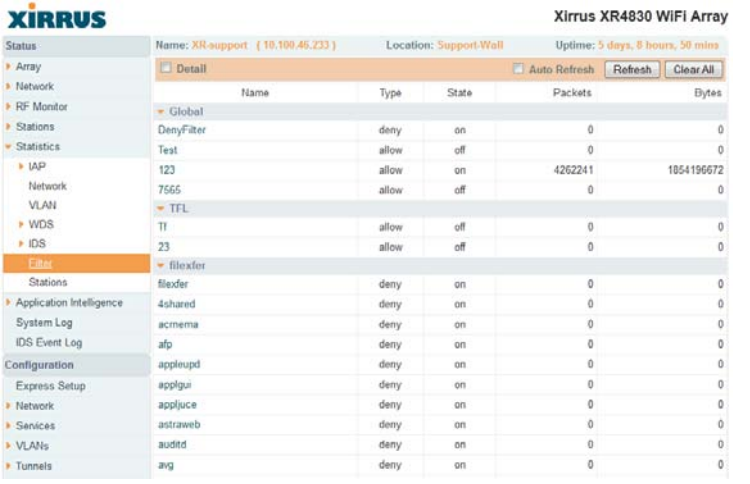


Figure 86. Filter Statistics

See Also

Filters

Application Control Windows

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 146.

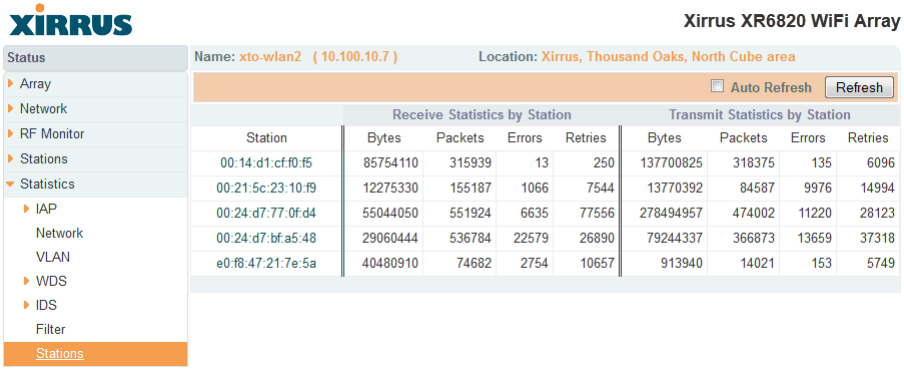


Figure 87. Station Statistics

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

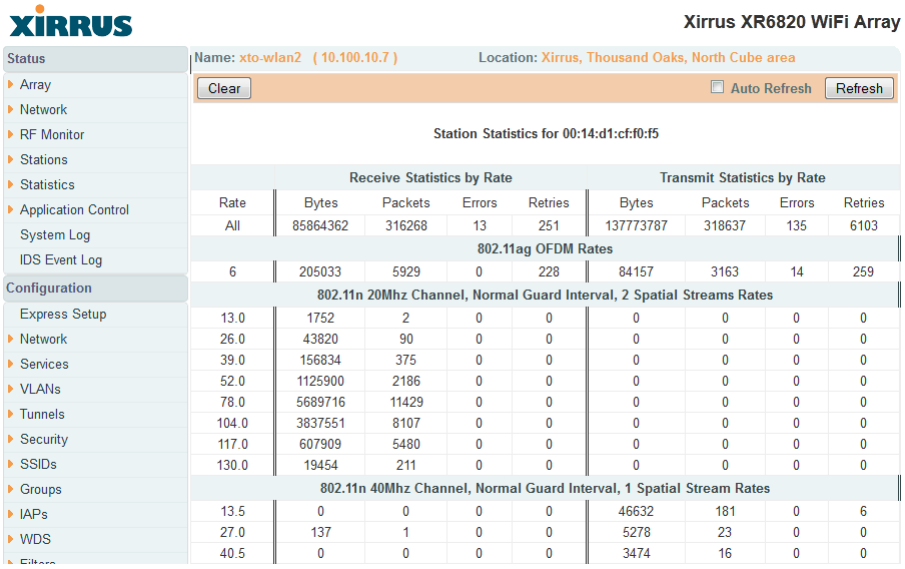
Per-Station Statistics

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 145.

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.



	Receive Statistics by Rate				Transmit Statistics by Rate			
Rate	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
All	85864362	316268	13	251	137773787	318637	135	6103
802.11ag OFDM Rates								
6	205033	5929	0	228	84157	3163	14	259
802.11n 20Mhz Channel, Normal Guard Interval, 2 Spatial Streams Rates								
13.0	1752	2	0	0	0	0	0	0
26.0	43820	90	0	0	0	0	0	0
39.0	156834	375	0	0	0	0	0	0
52.0	1125900	2186	0	0	0	0	0	0
78.0	5689716	11429	0	0	0	0	0	0
104.0	3837551	8107	0	0	0	0	0	0
117.0	607909	5480	0	0	0	0	0	0
130.0	19454	211	0	0	0	0	0	0
802.11n 40Mhz Channel, Normal Guard Interval, 1 Spatial Stream Rates								
13.5	0	0	0	0	46632	181	0	6
27.0	137	1	0	0	5278	23	0	0
40.5	0	0	0	0	3474	16	0	0

Figure 88. Individual Station Statistics Page

See Also

Station Statistics

Application Control Windows

This feature is only available if the Array license includes ***Application Control****. See* ***"About Licensing and Upgrades" on page 373****.*

The Application Control feature provides real-time visibility of application usage by users across the wireless network. Network usage has changed enormously in the last few years, with the increase in smartphone and tablet usage stressing networks. Increasing traffic from legitimate business needs such as cloud- and web-based applications, streaming media and VoIP must be handled with an adequate quality of experience.

Application Control is discussed in the following topics:

- **About Application Control**—an overview of this feature.
- **Application Control**—displays information about applications running on the wireless network.
- **Stations (Application Control)**—displays a list of stations. Click one to analyze application control information for only that station.

About Application Control

The Array uses Deep Packet Inspection (DPI) to determine what applications are being used and by whom, and how much bandwidth they are consuming. These applications are rated by their degree of risk and productiveness. Filters may then be put in place to implement per-application policies that keep network usage focused on productive uses:

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

Application Control can track application usage over time to monitor trends. Usage may be tracked by Array, VLAN, or station. Many hundreds of applications are recognized and grouped into a number of categories. The distributed architecture of Xirrus Arrays allows Application Control to scale naturally as you grow the network.

About Risk and Productivity

Application Control ranks applications in terms of their levels of risk an productivity.

Productivity indicates how appropriate an application is for business purposes. The higher the rating number, the more business-oriented an application is.

- 1—Primarily recreational
- 2—Mostly recreational
- 3—Combination of business and recreational purposes
- 4—Mainly used for business
- 5—Primarily used for business

Risk indicates how likely an application is to pose a threat to the security of your network. The higher the rating number, the more risky an application is.

- 1—No threat
- 2—Minimal threat
- 3—Some risk - may be misused
- 4—High risk - may be malware or allow data leaks
- 5—Very high risk - threat circumvents firewalls or avoids detection

Keeping Application Control Current

Applications are recognized using a signature file which may be updated using the System Tools page as new applications become popular (see "Application Control Signature File Management" on page 381).

Application Control

This display-only window provides a snapshot of the application usage on your Array. In order to view the Application Control window, the Array must have a license that supports this feature, and you must have enabled the **Application Control** option on the **Filter Lists** page (see "Filter Lists" on page 352).

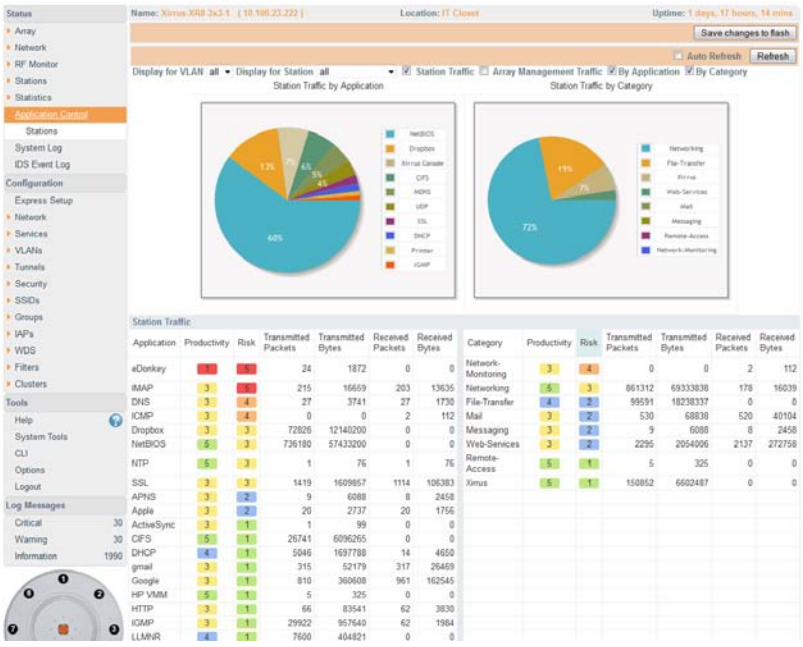


Figure 89. Application Control

The Application Control window has three sections:

- **Selection Criteria** allow you to choose the type of data to show, and to filter for a single VLAN or station.
- **Pie Charts** present a color coded at-a-glance view of the top ten applications being used by the network.
- **Traffic Tables** beneath the pie charts list the applications in use along with traffic statistics. Unique **Productivity** and **Risk** ratings let you easily assess the nature of applications in use, so that you can take action using Filter Management.

Selection Criteria

At the top of the window, the options in the gray ribbon allow you to customize the display with the following choices:

- **Display for VLAN**: Use the drop-down list if you wish to select just one VLAN to analyze, or leave the default value of **all** to see data from all VLANs.
- **Display for Station**: Use the drop-down list if you wish to select just one station to analyze (stations are listed by their MAC address), or leave the default value of **all** to see data from all stations. You may also use the Stations window to select a station to display. See "Stations (Application Control)" on page 153.
- **Station Traffic**: Check this box if you wish to analyze traffic from stations, listing the applications that they are using.
- **Array Management Traffic**: Check this box if you wish to analyze management traffic on this Array, including the load due to functions such as Xirrus Roaming. Tracking traffic into the array on the management side can alert you to nefarious activity—and even to traffic on the wired network that would best be blocked before it hits the Array. You may display both station and Array management traffic, if you wish.
- **By Application**: Check this box if you wish to analyze and list traffic by what specific applications are in use, such as WebEx or BitTorrent.
- **By Category**: Check this box if you wish to analyze and list traffic by what types of applications are in use, such as Games or Collaboration.
- **Auto Refresh** instructs the Array to periodically refresh this window automatically. Use the **Refresh** button to refresh the window right now.

Pie Charts

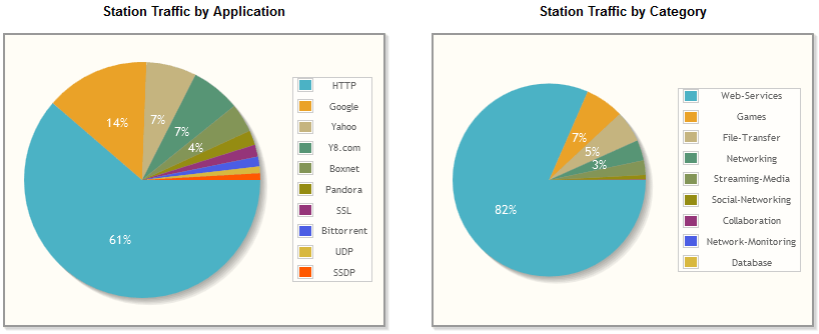


Figure 90. Application Control (Pie Charts)

These charts provide a quick way to determine how your wireless bandwidth is being used. There are charts for **Station Traffic** and/or **Array Management Traffic**, depending on which checkboxes you selected. Similarly, there are charts for **By Application** and/or **By Category**, depending on your selections. The top ten applications or categories are listed, by percentage of bandwidth usage.

Traffic Tables

Station Traffic

Application	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
eDonkey	1	5	24	1872	0	0
IMAP	3	5	215	16659	203	13635
DNS	3	4	27	3741	27	1730
ICMP	3	4	0	0	2	112
Dropbox	3	3	72826	12140200	0	0
NetBIOS	5	3	736180	57433200	0	0
NTP	5	3	1	76	1	76
SSL	3	3	1419	1609857	1114	106383
APNS	3	2	9	6088	8	2458
Apple	3	2	20	2737	20	1756
ActiveSync	3	1	1	99	0	0
CIFS	5	1	26741	6096265	0	0
DHCP	4	1	5046	1697788	14	4650
gmail	3	1	315	52179	317	26469
Google	3	1	810	360608	961	162545
HP VMM	5	1	5	325	0	0
HTTP	3	1	66	83541	62	3830
IGMP	3	1	29922	957640	62	1984
LLMNR	4	1	7600	404821	0	0

Category	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Network-Monitoring	3	4	0	0	2	112
Networking	5	3	861312	69333838	178	16039
File-Transfer	4	2	99591	18238337	0	0
Mail	3	2	530	68838	520	40104
Messaging	3	2	9	6088	8	2458
Web-Services	3	2	2295	2054006	2137	272758
Remote-Access	5	1	5	325	0	0
Xirrus	5	1	150852	6602487	0	0

Figure 91. Application Control (Station Traffic)

These tables provide detailed information about how your wireless bandwidth is being used. There are tables for **Station Traffic** and/or **Array Management Traffic**, depending on which checkboxes you selected. Similarly, there are tables for **By Application** and/or **By Category**, depending on your selections.

In addition to showing traffic statistics, there are two unique and highly useful columns. **Risk** estimates the likelihood of an application causing problems for your business, such as a file-sharing utility introducing viruses or exposing you to legal problems. Risk is rated from 1 (low risk, e.g., Google) to 5 (high risk, e.g., BitTorrent). Risky applications (rated at 4 or 5) are flagged for your attention by highlighting the entry in pale red. **Productivity** estimates the value of an activity to your business, from 1 (unproductive, e.g., Y8 gaming site) to 5 (productive, e.g., WebEx).

You may click the heading of any column to sort based on that column. Click again to sort in the reverse order. For instance, sort on **Risk** to find problem applications, or sort on **Productivity** to find applications that should be given increased or decreased handling priority.

When you find risky or unproductive applications taking up bandwidth on the network, you can easily create Filters to control them. See "Filter Management" on page 354. You may use filters to:

- Block problematic traffic, such as BitTorrent or Y8.
- Prioritize mission critical traffic—by increasing the QoS assigned to the traffic. See "Understanding QoS Priority on the Wireless Array" on page 247.
- Lower the priority of less productive traffic—use filters to decrease the QoS assigned to traffic for applications like YouTube and Facebook.

Stations (Application Control)

This status-only window shows client stations currently visible to the Array. The MAC address in the first column is a link. Click on a selected station, and the Application Control window opens with the **Display for Station** field set to that station, to perform a detailed analysis of its application usage.

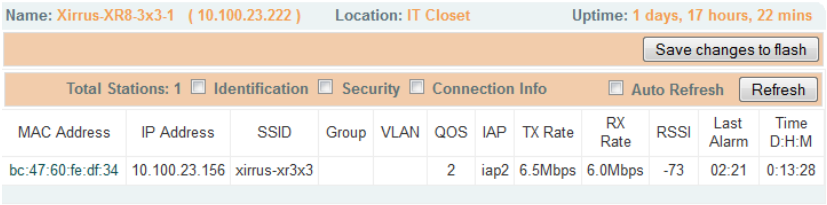


Figure 92. Stations (Application Control)

The rest of the fields and display options on this window (including the **Identification**, **Security**, and **Connection Info** checkboxes) are as described in "Stations" on page 123.

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.

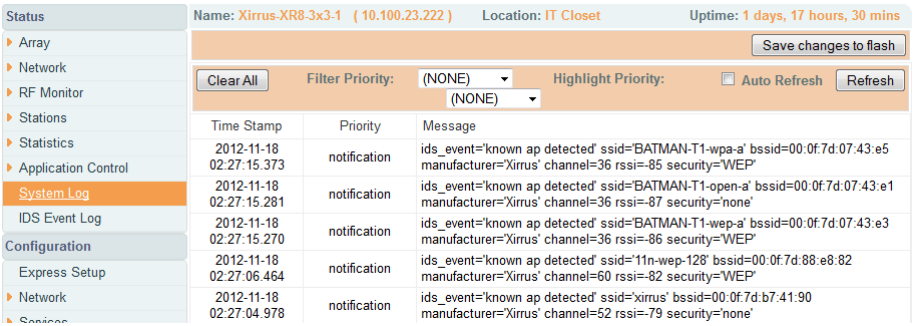


Figure 93. System Log (Alert Level Highlighted)

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 84 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 334.

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.

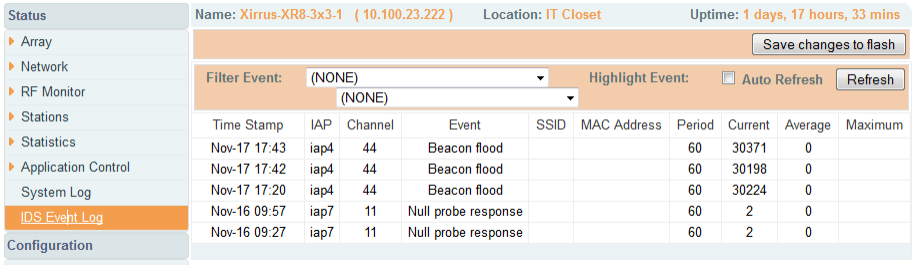


Figure 94. IDS Event Log

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.

Configuring the Wireless Array

If you are a Cloud XMS customer, then Arrays are managed via the cloud, and local Array management interfaces are inaccessible.

If the Array is being managed by your own server for XMS Release 6.5 or above, and if the Array has been assigned to a named network in XMS, you will be restricted to read-only Array access. See "XMS-Managed Arrays Restrict Local Management" on page 78.

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 159**
- **"Network" on page 165**
- **"Services" on page 180**
- **"VLANs" on page 199**
- **"Tunnels" on page 204**
- **"Security" on page 208**
- **"SSIDs" on page 245**
- **"Groups" on page 269**
- **"IAPs" on page 276**
- **"WDS" on page 345**
- **"Filters" on page 351**
- **"Clusters" on page 360**
- **"Mobile" on page 366**

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 features. If a setting is unavailable (grayed out), then your license does not support the feature. See ***"About Licensing and Upgrades" on page 373****.*

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 85.)

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 91**
- **"Using Tools on the Wireless Array" on page 371**

Express Setup

Initial Array configuration via Mobilize sets items such as the SSIDs, encryption and authentication, and SNMP settings, as described in "Zero-Touch Setup Using Mobilize" on page 67. The Express Setup page allows you to see many of these values, or change them locally.

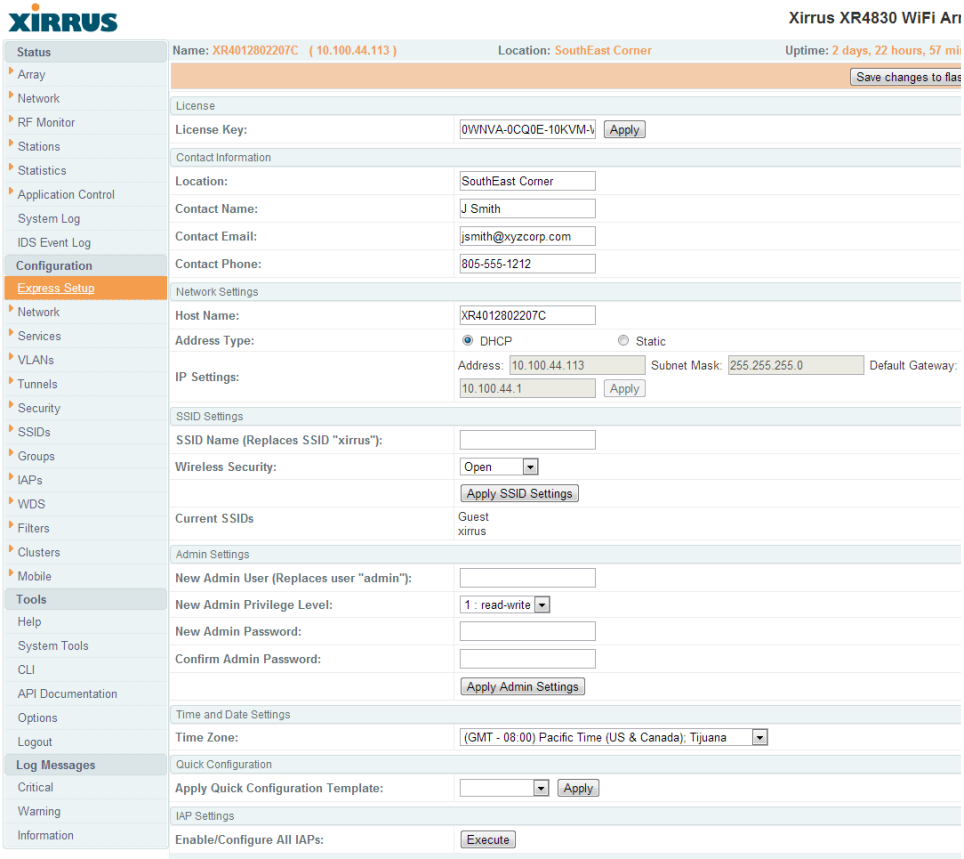


Figure 95. WMI: Express Setup

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

Procedure for Performing an Express Setup

1. **License Key**: An unlicensed Array will automatically contact Xirrus to obtain its license, if it has Internet connectivity. If you need to enter a license manually, enter it here. See "Licensing" on page 71.

2. Configure the **Contact Information** settings.

   a. **Location**: 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.

   b. **Contact Name**: Enter the name and contact information of the person who is responsible for administering the Array at the designated location.

   c. **Contact Email**: Enter the email address of the admin contact you entered in Step 3.

   d. **Contact Phone**: Enter the telephone number of the admin contact you entered in Step 3.

3. Configure the **Network** settings. Please see "Network Interfaces" on page 167 for more information.

   e. **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 the Array's serial number.

   f. **Address Type**: 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**:

   g. **IP Settings**: If you choose the **Static** IP addressing option, enter the following:

- **Address**: Enter a valid IP address for this Array. To use a remote connection (Web, SNMP, or SSH), a valid IP address must be used.
- **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.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the Array" on page 73.

4. **SSID Settings**: This section specifies the wireless network name and security settings.
   a. **SSID Name** is a unique name that identifies a wireless network. The default SSID is **xirrus**. Entering a value in this field will replace the this default SSID with the new name.

      For additional information about SSIDs, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 480.

   b. **Wireless Security**: Select the desired wireless security scheme (Open, WEP or WPA). Make your selection from the choices available in the pull-down list.

      - **Open**—This option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
      - **WEP** (Wired Equivalent Privacy)—An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both

source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

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

For more information about security, including a full review of all security options and settings, go to "Understanding Security" on page 209.

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

d. **Confirm Encryption Key/Passphrase**: If you entered a WEP key or WPA passphrase, confirm it here.

e. Click **Apply SSID Settings** when done.

f. **Current SSIDs**: This lists all of the currently defined SSIDs for you (regardless of whether they are enabled or not).

5. **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 214)).

   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 216. 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.

6. **Time and Date Settings:** System time is synchronized using NTP (Network Time Protocol) by default. Use the pull-down menu to select the **Time Zone**.

7. **Quick Configuration:** This offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate

to your deployment, select it and click **Apply**. For example, the **High-Density** option uses best practices to configure the Array for high density settings such as lecture halls, convention centers, stadiums, etc.

8. **IAP Settings:**

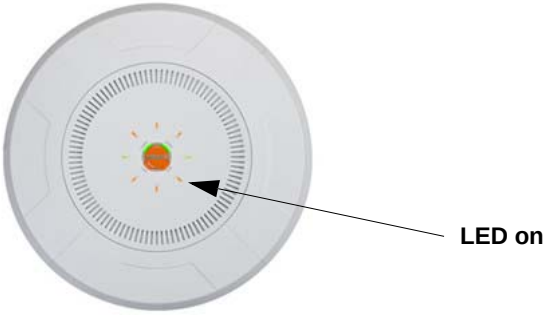


Figure 96. LEDs are Switched On

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.

9. 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.

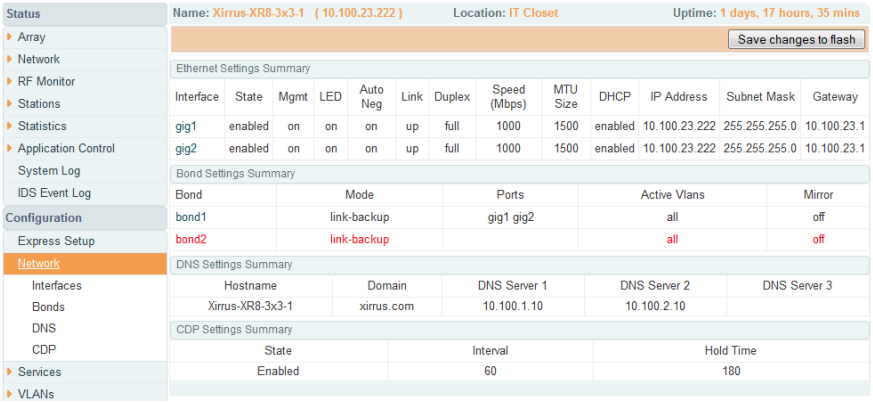


Figure 97. Network Interfaces

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

- **"Network Interfaces" on page 167**
- **"Network Bonds" on page 171**
- **"DNS Settings" on page 177**
- **"CDP Settings" on page 178**

See Also

DNS Settings
Network Interfaces
Network Status Windows

Spanning Tree Status
Network Statistics

Network Interfaces

XR-500, XR-1000, and some XR-2000 Series Arrays have one Gigabit Ethernet interface, while XR-4000 and some XR-2000 Series Arrays have two, and XR-6000 Series models have four. This window allows you to establish configuration settings for these interfaces.

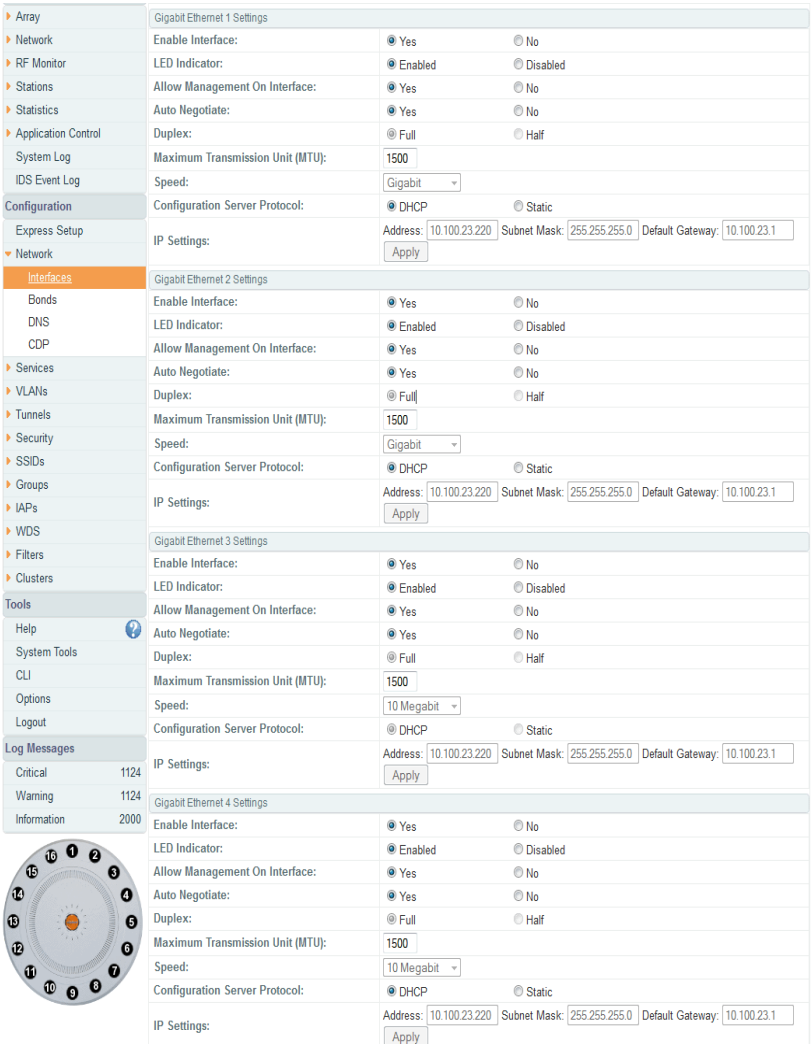


Figure 98. Network Settings

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 network interface ports on the underside of an XR Series Array.

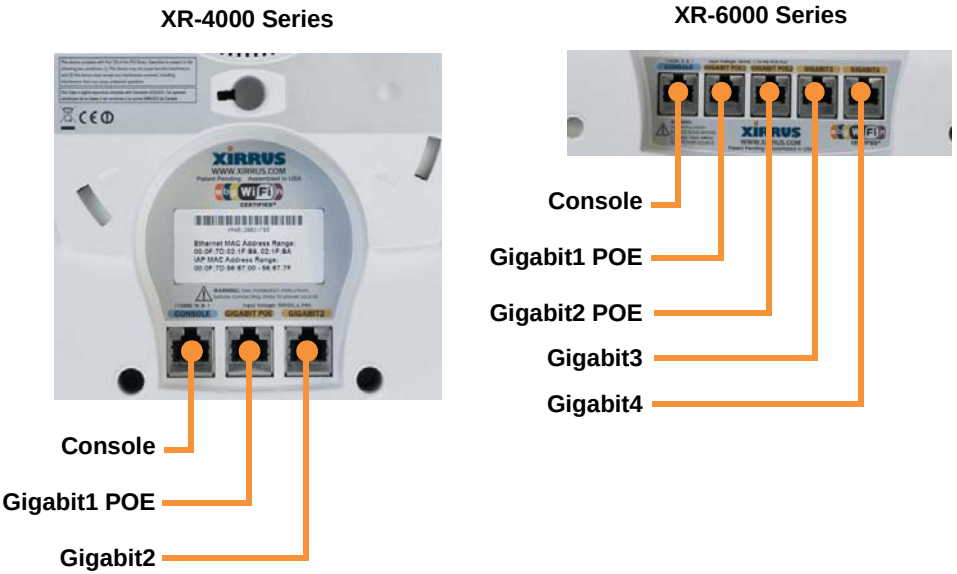


Figure 99. Network Interface Ports

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.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the Array" on page 73.

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). Both sides of the link **must** have the same values for the following settings, or the connection will have errors.

    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.

    b. **Subnet Mask**: If you selected the Static IP option, enter a valid IP address for the subnet mask (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.

    c. **Default Gateway**: If you selected the Static IP option, enter a valid IP address for the default gateway. This is the IP address of the router that the Array uses to send data to other networks. (You don't need to enter the gateway if it is on the same subnet as the Array.)

    d. Click the **Apply** button for this interface when done making IP changes.

6. When done configuring all interfaces as desired, click **Save changes to flash** if you wish to make your changes permanent.

See Also

Network Bonds
DNS Settings
Network
Network Statistics
Spanning Tree Status

Network Bonds

On models with more than one Gigabit port these ports may be bonded, i.e. configured to work together in sets. For example, one port may provide active backup or load balancing for another, or other options as described in this section. XR-6000 Series Arrays have four Gigabit ports, and you may specify which ports are bonded to work together as a pair. You may also select more than two ports to work together in one group.

You may use the mirror option to have all the traffic that is ingressing and egressing one bond be transmitted by the bond you are configuring. For example, if you configure Bond2 to mirror Bond1, then all traffic going in and out of Bond1's Gigabit ports will be transmitted out of Bond2's Gigabit ports. This way of duplicating one bond's traffic to another bond is very useful for troubleshooting with a network analyzer.

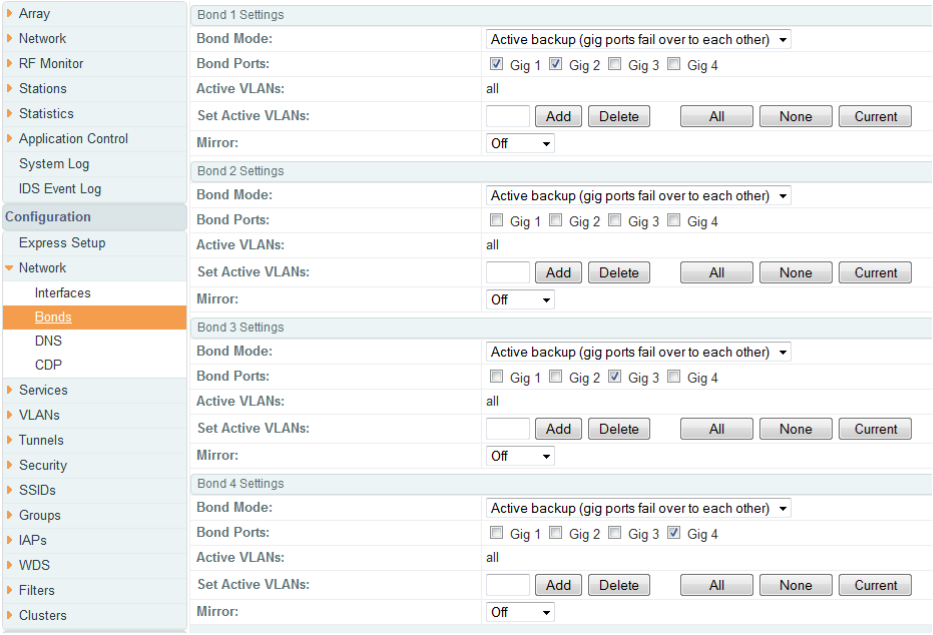


Figure 100. Network Bonds

If a set of Gigabit ports have been bonded, the IP address, IP mask, IP gateway, IP DHCP, and Management settings are shared between bonded ports. Any changes you make to these settings on one member will be reflected in the settings of the other members. Other settings may be configured individually.

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.

   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. You may also include just one single port in a bond—this is useful for mirroring one Gigabit port to another port (Step 5 on page 176). In Arrays that have four Gigabit ports, you have the option of bonding three or four ports together. In this discussion, we call two ports that are bonded **Gig*x*** and **Gig*y***.

   a. **Active Backup (gig ports fail over to each other)**—This mode provides fault tolerance and is the default mode. Gig*x* acts as the primary link. Gig*y* is the backup link and is passive. Gig*y* assumes the IP properties of Gig*x*. If Gig*x* fails, the Array automatically fails over to Gig*y*. When a failover occurs in this mode, Gig*y* issues gratuitous ARPs to allow it to substitute for Gig*x* at Layer 3 as well as Layer 2. See Figure 101 (a). You may include more than two ports in the bond with Active Backup to provide additional fault tolerance. For example, if you have three Gigabit ports configured in a bond, if the first two ports in the bond were to go down, the Array would fail over traffic to the third Gigabit port.

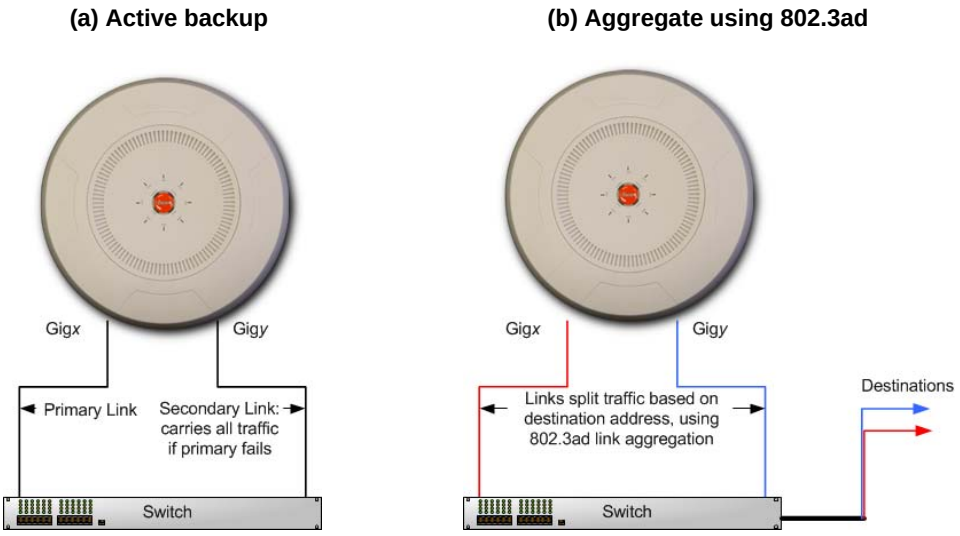


Figure 101. Port Modes (a, b)

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, 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 connection degrades gracefully—the other port still transmits. See Figure 101 (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 102 (c).

(c) Transmit on all ports

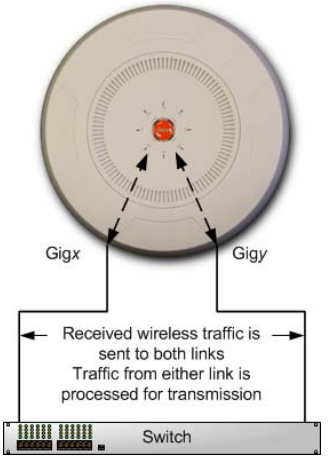


Figure 102. Port Modes (c)

(d) Load balance traffic

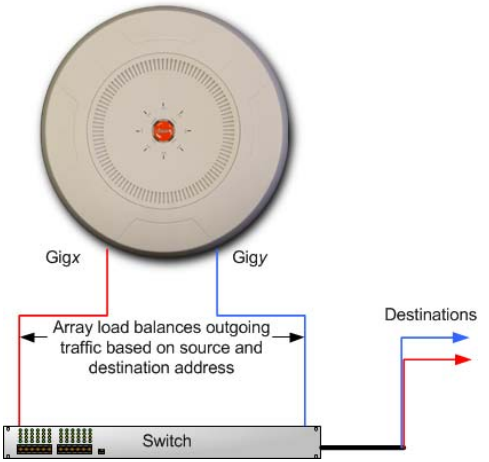


Figure 103. Port Modes (d)

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 does not use 802.3ad and 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 103 (d).

2. **Bond Ports**: Select the ports to be members of this bond for the behavior specified by **Bond Mode**. By default, Bond1 contains Gig1 and Gig2. You may also set up a bond with a single port, for example, if you wish to mirror one Gigabit port to another. In Arrays that have four Gigabit ports, you also have the option of bonding three or four ports together.

   When you check off a port to be a member of a bond, that port is automatically removed from any other bonds that contain it.

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. 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, 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 199) 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.

5. **Mirror**—Specify one of the active bonds (Bond*x*) that is to be mirrored by this bond (Bond*y*). (Figure 104) All wireless traffic received on the Array is transmitted out both Bond*x* and Bond*y*. All traffic received on Bond*x* is passed on to the onboard processor as well as out Bond*y*. All traffic received on Bond*y* is passed on to the onboard processor as well as out Bond*x*. This allows a network analyzer to be plugged into Bond*y* to capture traffic for troubleshooting, while the bonded ports provide network connectivity for data traffic.

   If each bond contains just one port, then you have the simple case of one port mirroring another.

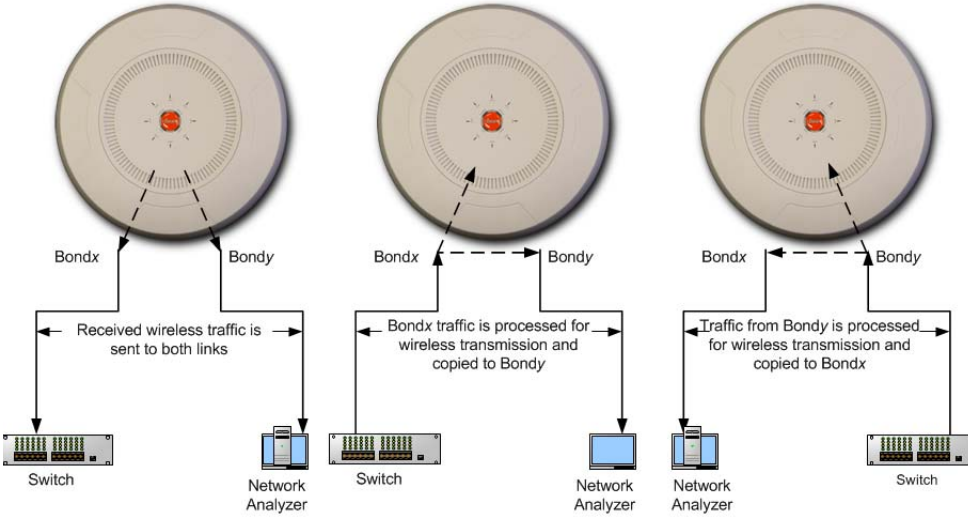


Figure 104. Mirroring Traffic

6. 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 196. 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.

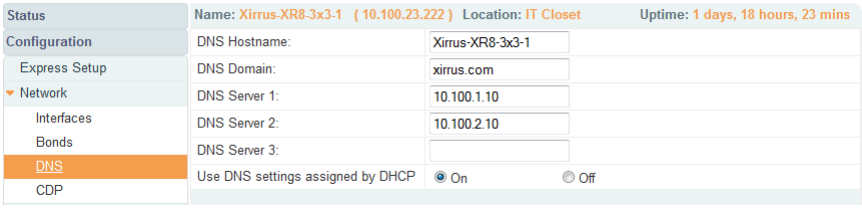


Figure 105. DNS Settings

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 108).

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

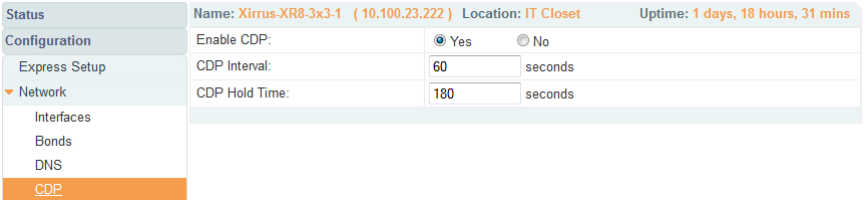


Figure 106. CDP Settings

Procedure for Configuring CDP Settings

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

See Also

CDP Neighbors
Network
Network Interfaces
Network Statistics

Services

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

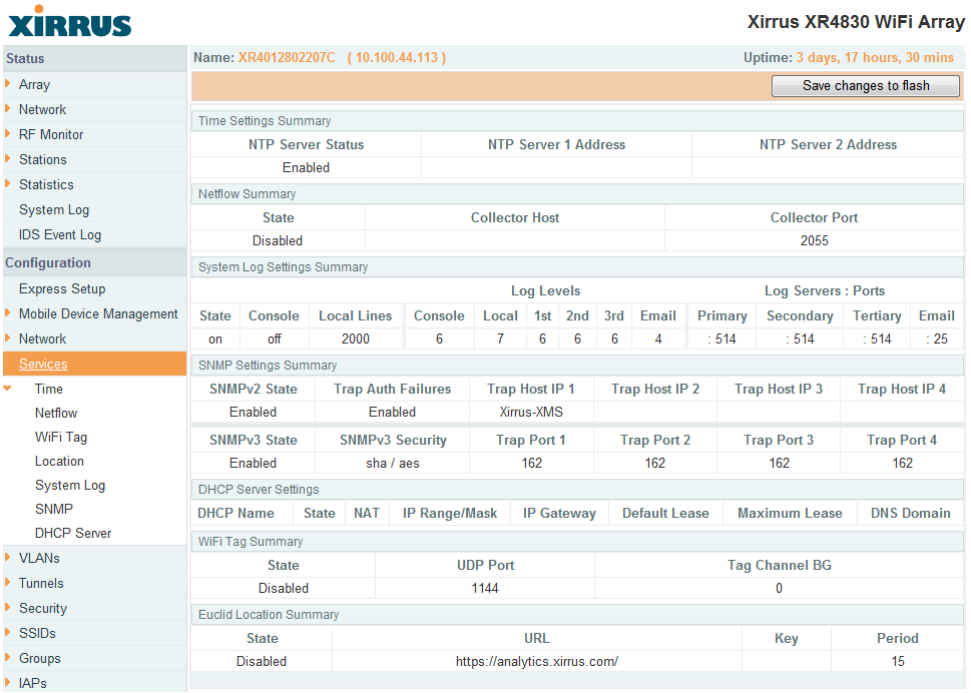


Figure 107. Services

The following sections discuss configuring services on the Array:

- **“Time Settings (NTP)” on page 181**
- **“NetFlow” on page 184**
- **“Wi-Fi Tag” on page 185**

- "Location" on page 186
- "System Log" on page 188
- "SNMP" on page 193
- "DHCP Server" on page 196

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.

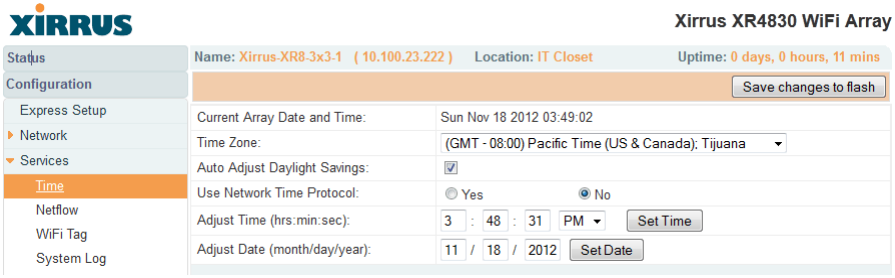


Figure 108. Time Settings (Manual Time)

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.

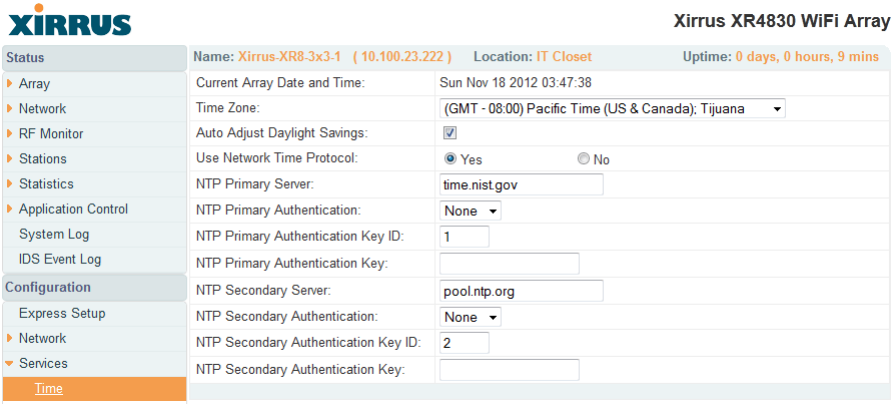


Figure 109. Time Settings (NTP Time Enabled)

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.

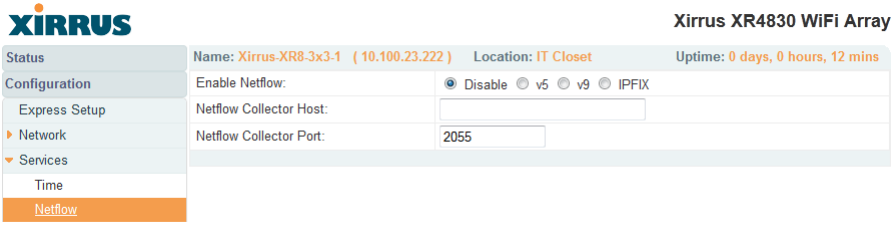


Figure 110. NetFlow

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.

Procedure for Configuring NetFlow

1. **Enable NetFlow:** Select one of the Netflow versions to enable NetFlow functionality: **v5**, **v9**, or **IPFIX**. Internet Protocol Flow Information Export (IPFIX) is an IETF protocol (www.ietf.org**)** performing many of the same functions as Netflow. Choose **Disable** if you wish 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 enables or disables 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 or Ekahau tags). A Wi-Fi tagging server 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.

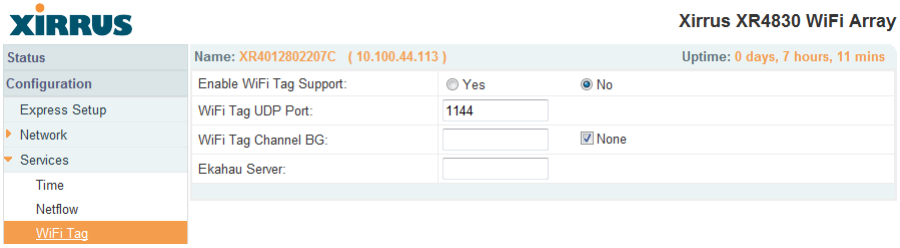


Figure 111. Wi-Fi Tag

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 Wi-Fi tagging is enabled, enter the UDP port that the Wi-Fi tagging server will use to query the Array for data. When queried, the Array will send back information on 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.
4. **Ekahau Server**: If you enabled Wi-Fi tagging and you are using an Ekahau server, enter its IP address or hostname. Ekahau Wi-Fi Tag packets received by the Array will be encapsulated as expected by Ekahau, and forwarded to the server.

Location

The Array offers an integrated capability for capturing and uploading visitor analytics data, eliminating the need to install a standalone sensor network. This data can be used to characterize information such as guest or customer traffic and location, visit duration, and frequency. Use this Location window to configure the Array to send collected data to an analytics server, such as Euclid.

When Location Support is enabled, the Array collects information about stations, including the station ID and manufacturer, time and length of the visit and related time interval statistics, and signal strength and its related statistics. Data collected from stations comprises only basic device information that is broadcast by Wi-Fi enabled devices. Devices that are only detected are included, as well as those that actually connect to the Array. The Array sending the data also sends its own ID so that the server knows where the visitors were detected. Data messages are uploaded via HTTPS, and they are encrypted if a **Location Customer Key** has been entered. Data is sent as JSON (JavaScript Object Notation) objects, as described in "Location Service Data Formats" on page 492.

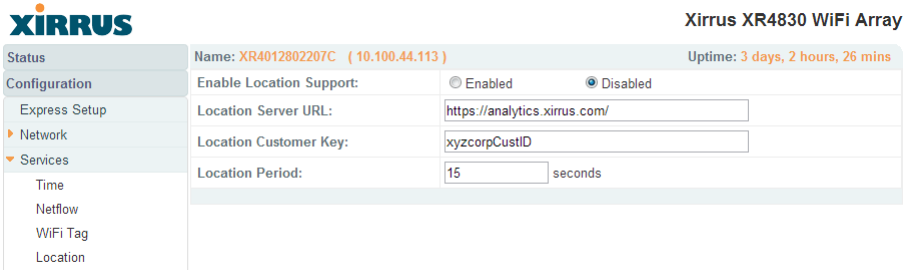


Figure 112. Location

Procedure for Configuring Location

1. **Enable Location Support:** Choose **Yes** to enable the collection and upload of visitor analytic data, or choose **No** to disable this feature.

2. **Location URL**: If Location Support is enabled, enter the IP address or hostname of the location/analytics server. If this URL contains the string **euclid**, then the Array knows that data is destined for a Euclid location server.

For a Euclid analytics server, use the URL that was assigned to you as a customer by Euclid. The Array will send JSON-formatted messages in the form required by Euclid via HTTPS.

For any other location analytics server, enter its URL. The Array will send JSON-formatted messages in the form described in "Location Service Data Formats" on page 492.

3. **Location Customer Key**: (optional) If a **Location Customer Key** has been entered, data is sent encrypted using AES with that key.
4. **Location Period**: If you enabled Location Support, specify how often data is to be sent to the server, in seconds.

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 server and for email notification—the Syslog service will send Syslog messages at the selected severity or above to the defined Syslog servers and email address. An option allows you to use a Splunk application to analyze Array events by sending data in key:value pairs, as described in "About Using the Splunk Application for Xirrus Arrays" on page 191.

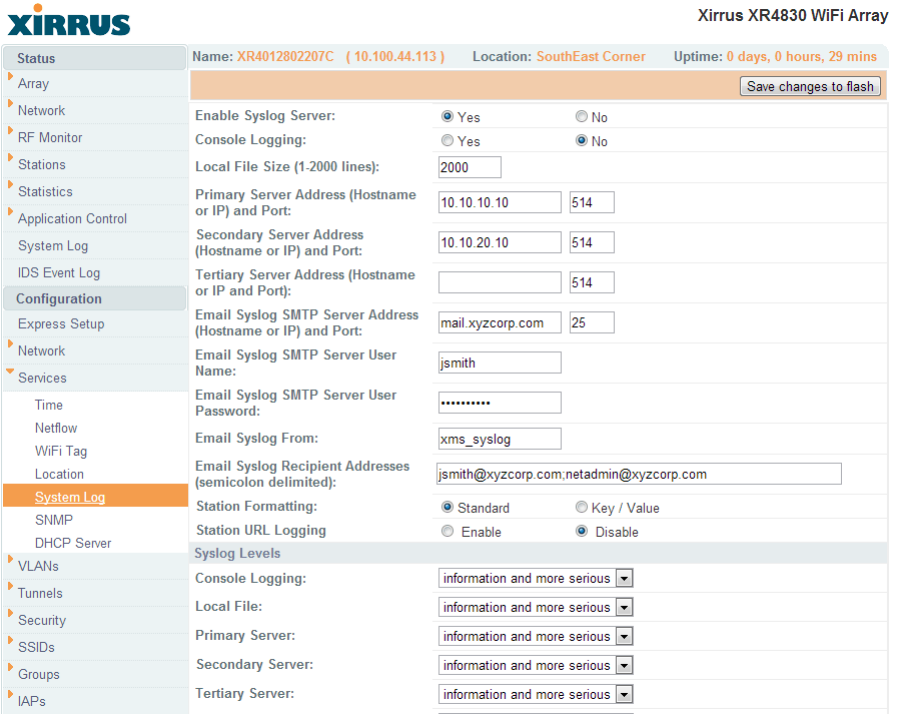


Figure 113. System Log

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 9 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. You may set one of the server addresses to the address of a server for Splunk (see "About Using the Splunk Application for Xirrus Arrays" on page 191).

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. **Station Formatting**: If you are sending event information to a Splunk server, select **Key/Value** to send data in Splunk's expected format, otherwise leave this at the default value of **Standard**. See "About Using the Splunk Application for Xirrus Arrays" on page 191.

8. **Station URL Logging**: When enabled, Syslog messages are sent for each URL that each station visits. Only HTTP destinations (port 80) are logged; HTTPS destinations (port 443) are not logged. All URLs in a domain are logged, so for example, if an HTTP request to yahoo.com generates requests to 57 other URLs, all are logged. Furthermore, each visit to the same URL generates an additional log message. No deep packet inspection is performed by the URL logging, so no Application Control information is included in the Syslog message.

   The following information is included in the syslog message:

   - Date / Time
   - Source Device MAC and IP address
   - Destination Port
   - Destination Site address (e.g., 20.20.20.1)
   - The specific URL (e.g., http://20.20.20.1.24online/images/img2.jpg)

   Station URL Logging is disabled by default.

9. **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.

10. Click **Save changes to flash** if you wish to make your changes permanent.

About Using the Splunk Application for Xirrus Arrays

Splunk may be used to provide visibility into client experience and analyze usage on XR Series Wireless Arrays. A Splunk application (Splunk for Xirrus XR Wireless Arrays) has been developed to present this operational intelligence at a glance. The app includes field extractions, event types, searches and dashboards to help shine a light on station status and activity.

To use Splunk, set up your Splunk server with the Splunk application—available from www.splunk.com at **Splunk for Xirrus XR Wireless Arrays**. Configure the Array to send data to Splunk by setting a **Primary**, **Secondary**, or **Tertiary Server Address** to the IP address or hostname of your Splunk server. Then set **Station Formatting** to **Key/Value** to send data in Splunk's expected format.

You may specify Server Addresses for Syslog servers and a Splunk server on the same Array. Selecting the **Key/Value** option will not cause any problems with Syslog.

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.

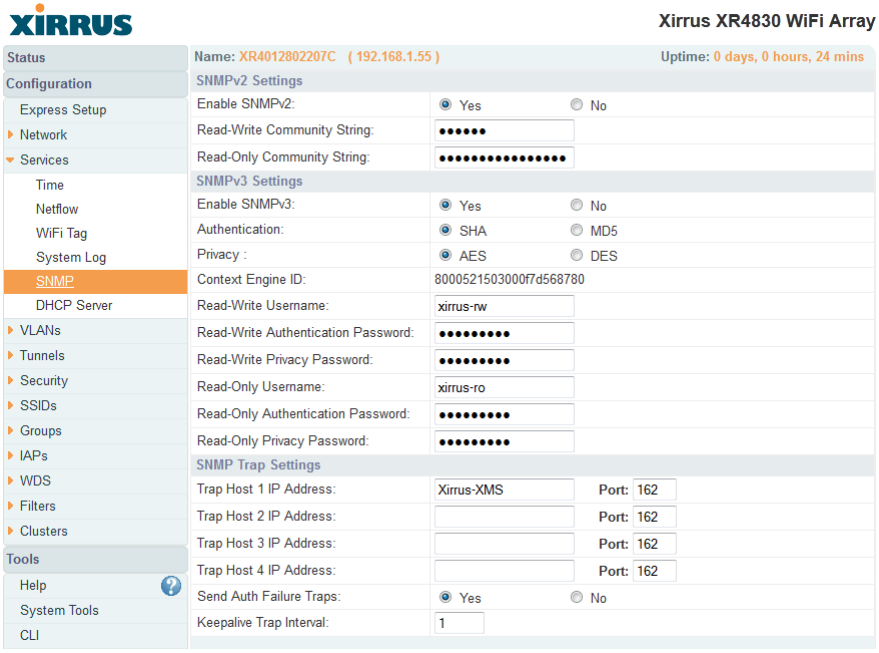


Figure 114. SNMP

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**.

10. **SNMP Read-Write Privacy Password**: Enter the read-write password for privacy (i.e., a key for encryption). The default is **xirrus-rw**.
11. **SNMP Read-Only Username**: Enter the read-only user name. This username and password do not allow configuration changes to be made on the Array. The default is **xirrus-ro**.
12. **SNMP Read-Only Authentication Password**: Enter the read-only password for authentication (i.e., logging in). The default is **xirrus-ro**.
13. **SNMP Read-Only Privacy Password**: Enter the read-only password for privacy (i.e., a key for encryption). The default is **xirrus-ro**.

SNMP Trap Settings

14. **SNMP Trap Host IP Address**: Enter the **IP Address** or hostname, as well as the **Port** number, of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps. Note that by default, **Trap Host 1** sends traps to **Xirrus-XMS**. Thus, the Array will automatically communicate its presence to XMS (as long as the network is configured correctly to allow this host name to be resolved—note that DNS is not normally case-sensitive).

    For a definition of the traps sent by Xirrus Wireless Arrays, you may download the Xirrus MIB from support.xirrus.com (login required). Search for the string **TRAP** in the MIB file.

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

See Also

Services

System Log
Time Settings (NTP)

DHCP Server

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

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

Figure 115. DHCP Management

DHCP usage is determined in several windows—see SSID Management, Group Management, and VLAN Management.

Procedure for Configuring the DHCP Server

1. **New Internal DHCP Pool**: Enter a name for the new DHCP pool, then click on the **Create** button. The new pool ID is added to the list of available DHCP pools. You may create up to 16 DHCP pools (up to 8 on the XR-500 Series).
2. **On**: Click this checkbox to make this pool of addresses available, or clear it to disable the pool.
3. **Lease Time—Default**: This field defines the default DHCP lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
4. **Lease Time—Max**: Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.
5. **Network Address Translation (NAT)**: Check this box to enable the Network Address Translation feature.
6. **Lease IP Range—Start**: Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End**: Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask**: Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway**: If necessary, enter the IP address of the gateway.
10. **Domain**: Enter the DNS domain name. See "DNS Settings" on page 177.
11. **DNS Servers** (1 to 3): Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the assigned IP address. Note that if you leave these blank, no DNS

information is sent to the stations. DHCP will **not** default to sending the DNS servers that are configured in DNS Settings. See also, "DNS Settings" on page 177.

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

See Also

DHCP Leases
DNS Settings
Network Map

VLANs

This is a status-only window that allows you to review the current status of configured VLANs. VLANs are virtual LANs used to create broadcast domains.

You should create VLAN entries on the Array for all of the VLANs in your wired network if you wish to make traffic from those VLANs available on the wireless network. Each tagged VLAN should be associated with a wireless SSID (see "VLAN Management" on page 201). The Array will discard any VLAN-tagged packets arriving on its wired ports, unless the same VLAN has been defined on the Array. See "Undefined VLANs" on page 110.

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN (Step 1 page 202).

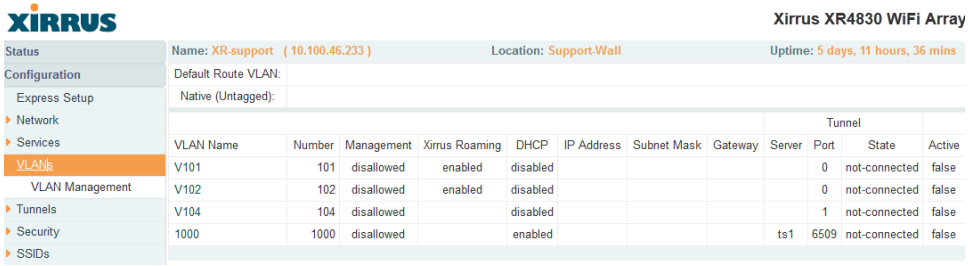


Figure 116. VLANs

For a discussion of implementing Voice over Wi-Fi on the Array, see the ***Xirrus Voice over Wireless Application Note*** *in the* ***Xirrus Resource Center****.*

Understanding Virtual Tunnels

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

- The Xirrus Tunnel Server (XTS)—see the *Xirrus Tunnel Server User's Guide*.
- Virtual Tunnel Server (VTS)—see below.

Virtual Tunnel Server (VTS)

Tunneling capability is provided by a Virtual Tunnel Server. You supply the server and deploy it in your network using open-source VTun software, available from vtun.sourceforge.net. To enable the Array to use tunneling for a VLAN, simply enter the IP address, port and secret for the tunnel server as described in Step 11 on page 203.

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

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

VTS Client-Server Interaction

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

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

VLAN Management

This window allows you to assign and configure VLANs. After creating a new VLAN (added to the list of VLANs), you can modify the configuration parameters of an existing VLAN or delete a selected VLAN. You may create up to 64 VLANs (up to 32 on the XR-500 Series).

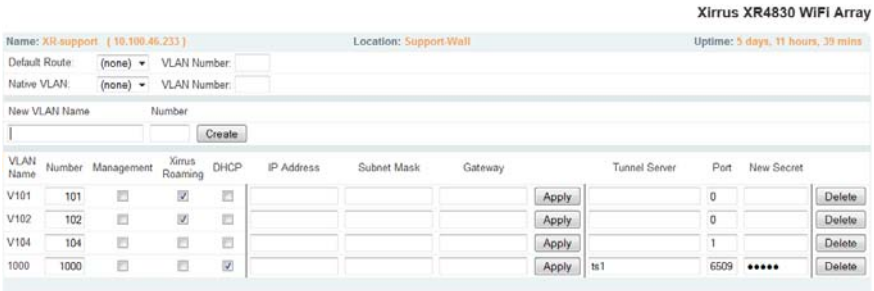


Figure 117. VLAN Management

*The Wireless Array supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Array dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Array (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (**Figure 69 on page 123**)*

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

Procedure for Managing VLANs

1. **Default Route:** This option sets a default route from the Array. The Array supports a default route on native and tagged interfaces. Once the default route is configured the Array will attempt to use Address Resolution Protocol (ARP) to find the default router. ARP finds the MAC address of a device with a given IP address by sending out a broadcast message requesting this information. This option allows you to choose a default VLAN route from the pull-down list. The IP Gateway must be established for this function to work. After changing the **Default Route**, you *must* click **Save changes to flash** *and then reboot*.
2. **Native VLAN**: This option sets whether the Array management is tagged or untagged. If you select a Native VLAN, then that VLAN will use an untagged (Native) link. Otherwise, the Array will use 802.1Q tagging and a specific VLAN ID with management enabled for management of the Array.
3. **New VLAN Name/Number**: Enter a name and number for the new VLAN in this field, then click on the **Create** button. The new VLAN is added to the list.
4. **VLAN Number**: Enter a number for this VLAN (1-4094).
5. **Management**: Check this box to allow management over this VLAN.
6. **Xirrus Roaming**: Check this box to allow roaming over this VLAN.
7. **DHCP**: Check this box if you want the DHCP server to assign the IP address, subnet mask and gateway address to the VLAN automatically, otherwise you must go to the next step and assign these parameters manually.
8. **IP Address**: If the DHCP option is disabled, enter a valid IP address for this VLAN association.
9. **Subnet Mask**: If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.

10. **Gateway**: If the DHCP option is disabled, enter the IP gateway address for this VLAN association.
11. **Tunnel Server**: If this VLAN is to be tunneled, enter the IP address or host name of the tunnel server that will perform the tunneling. For more information on virtual tunnels, please see "Understanding Virtual Tunnels" on page 199.
12. **Port**: If this VLAN is to be tunneled, enter the port number of the tunnel server.
13. **New Secret**: Enter the password expected by the tunnel server.
14. **Delete**: To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.
15. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

VLAN Statistics
VLANs
Tunnels

Tunnels

This read-only window allows you to review the tunnels that have been defined on the Array. It lists all tunnels and their settings, including the type of authentication and the local and remote endpoints for each tunnel.

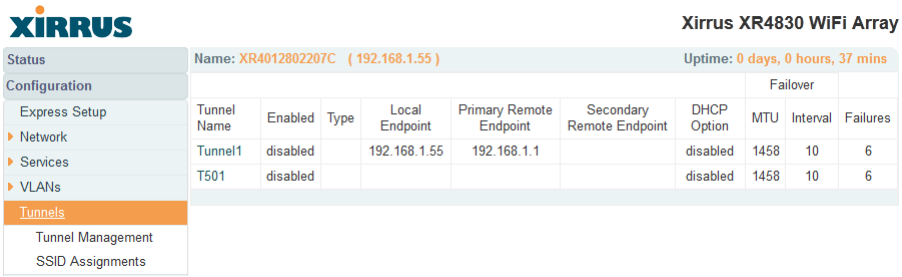


Figure 118. Tunnel Summary

About Xirrus Tunnels

Xirrus Arrays offer GRE (Generic Routing Encapsulation) tunneling with VLAN support. This allows an Array to use tunnels to bridge Layer 2 traffic for one or more SSID-VLAN pairs onto a single destination network through the Layer 3 network. GRE tunneling is quite flexible, and can encapsulate many network layer protocols. As a result, it can support a variety of applications. For example, a Wi-Fi hotspot can allow guest logins and use the tunnel to give guests direct access to the Internet, without allowing access to the local network. In a small office, you may define a tunnel to connect users to the corporate office network. Tunnels may also used when providing cellular offload capability.

Tunnels may be implemented with:

- The Xirrus Tunnel Server (XTS)—see the *Xirrus Tunnel Server User's Guide*.
- VTS —see "Virtual Tunnel Server (VTS)" on page 200.

To create a tunnel, you specify the **Local Endpoint**, which should be one of the Array's wired ports, and the **Primary Remote Endpoint**. A **Secondary Remote Endpoint** may also be specified in case of a failure at the first endpoint. Traffic for a VLAN-SSID pair is sent in GRE encapsulated packets across the Layer 3 network from the Array to the remote endpoint. When packets arrive, the

encapsulation is stripped and the resultant packets are passed to your switch with 802.1q VLAN tags for final Layer 2 processing. The process occurs in reverse for packets traveling in the other direction. One tunnel is able to transport up to 16 VLANs.

Tunnel Management

This window allows you to create tunnels.

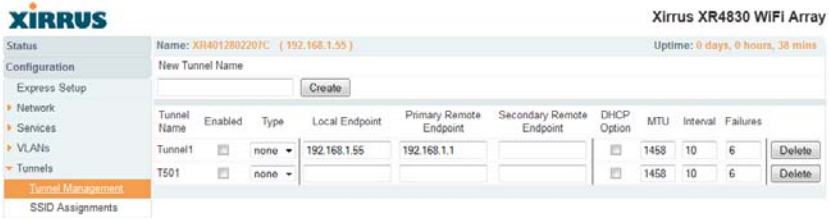


Figure 119. Tunnel Management

Procedure for Managing Tunnels

1. **New Tunnel Name**: Enter a name for the new tunnel in this field, then click on the **Create** button. The new tunnel is added to the list.
2. **Enabled**: The new tunnel is created in the disabled state. Click this checkbox to enable it.
3. **Type**: Enter the type of tunnel, **none** or **gre**.
4. **Local Endpoint**: Enter the IP address of the Array Gigabit or 10 Gigabit port where the tunnel is to begin.
5. **Primary Remote Endpoint**: Enter the IP address of the remote endpoint of the tunnel.
6. **Secondary Remote Endpoint**: This provides a failover capability. If the primary tunnel fails, traffic is switched over to the secondary tunnel. Enter the IP address of the remote endpoint of the secondary tunnel.

7. **DHCP Option**: When this option is enabled, the Array snoops station DHCP requests and inserts relay agent information (option 82, in the circuit-ID sub-option) into these DHCP packets. Information inserted includes Array BSSID, SSID name, and SSID encryption type.
8. **MTU**: Set maximum transmission unit (MTU) size.
9. **Interval**: The tunnel mechanism will ping the current remote endpoint periodically to ensure that it is still reachable. Enter the ping interval (in seconds).
10. **Failures**: Enter the number of consecutive ping failures that will cause the Array to consider the tunnel to be down.
11. Click **Save changes to flash** if you wish to make your changes permanent.
12. Proceed to SSID Assignments to define the SSIDs (and associated VLANs) for which each tunnel will bridge data. You may create up to 16 tunnels. Each will need an SSID/VLAN pair assigned to it so that it can function properly.

SSID Assignments

This window allows you to select the SSIDs to be bridged by each tunnel. Station traffic for SSIDs assigned will be bridged through a tunnel regardless of whether these SSIDs have VLANs defined for them. If there is a VLAN defined for an SSID that is assigned to a tunnel, then station traffic bridged through that tunnel will be tagged accordingly.

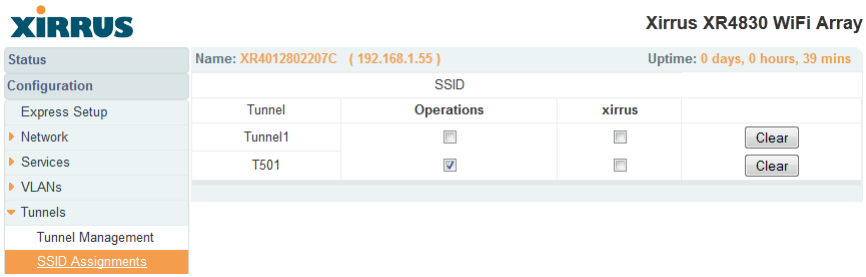


Figure 120. Tunnel SSID Assignments

Procedure for Assigning SSIDs

This window lists the tunnels and SSIDs that you have defined. SSIDs to be tunneled do not need to be associated with a VLAN (see "SSID Management" on page 253).

1. For each tunnel, select the SSIDs that are to be bridged to the remote endpoint. Clear the checkbox for any SSID that you no longer wish to include in the tunnel.
2. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Tunnels
VLANs
SSIDs

Security

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

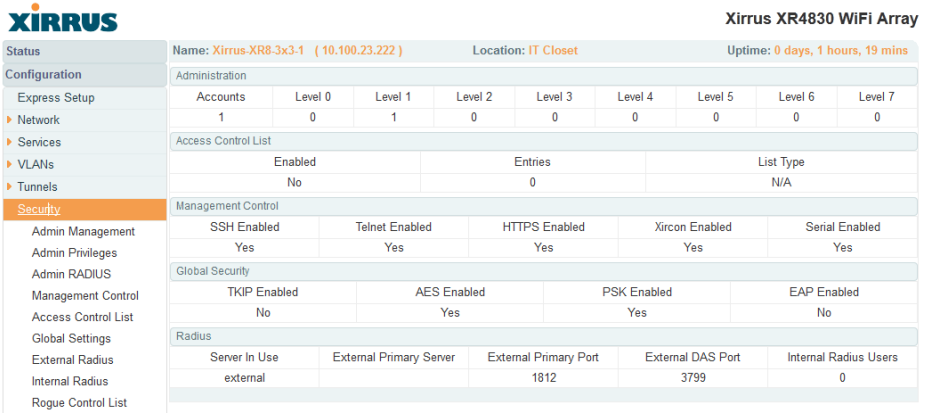


Figure 121. Security

For additional information about wireless network security, refer to:

- **"Security Planning" on page 47**
- **"Understanding Security" on page 209**
- **The Security section of "Frequently Asked Questions" on page 480**

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

- **"Certificates and Connecting Securely to the WMI" on page 212**
- **"Using the Array's Default Certificate" on page 212**
- **"Using an External Certificate Authority" on page 213**
- **"About Creating Admin Accounts on the RADIUS Server" on page 218**
- **"About Creating User Accounts on the RADIUS Server" on page 235**

Security settings are configured with the following windows:

- **"Admin Management" on page 214**
- **"Admin Privileges" on page 216**
- **"Admin RADIUS" on page 218**
- **"Management Control" on page 221**
- **"Access Control List" on page 228**
- **"Global Settings" on page 230**
- **"External Radius" on page 234**
- **"Internal Radius" on page 238**
- **"Rogue Control List" on page 241**
- **"OAuth 2.0 Management" on page 243**

Understanding Security

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

Other security considerations include:

- **SSH versus Telnet**: Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. SSH-2 provides stronger security than SSH-1. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing**: The optional Xirrus Management System (XMS) offers powerful management features for small or large Xirrus wireless deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.
- **Choosing an encryption method**: Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves.

The Array allows you to establish the following data encryption configuration options:

- **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
- **WEP (Wired Equivalent Privacy)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
- **WPA (Wi-Fi Protected Access) and WPA2**—these are much stronger encryption modes than WEP, using TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) to encrypt data.

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

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

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

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs >SSID Management** window (see "SSID Management" on page 253). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security>Global Settings** window under **WPA Settings** (see "Global Settings" on page 230).

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

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

address in the Deny list. The Wireless Array will accept up to 1,000 ACL entries.

Certificates and Connecting Securely to the WMI

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

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

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

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

Using the Array's Default Certificate

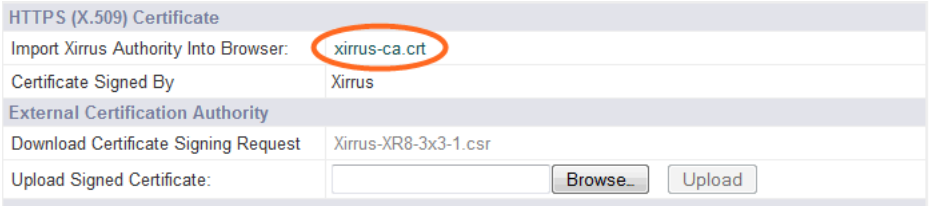


Figure 122. Import Xirrus Certificate Authority

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

By clicking and opening this file, you can follow your browser's instructions and import the Xirrus CA into your CA cache (see "HTTPS (X.509) Certificate" on page 226 for more information). This instructs your browser to trust any of the certificates signed by the Xirrus CA, so that when you connect to any of our Arrays you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the Array. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for 'hostname'.

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

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

Using an External Certificate Authority

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

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

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the Array after you obtain it from the CA. This certificate will be tied to the Array's host name and private key. See "External Certification Authority" on page 227 for more details.

Admin Management

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

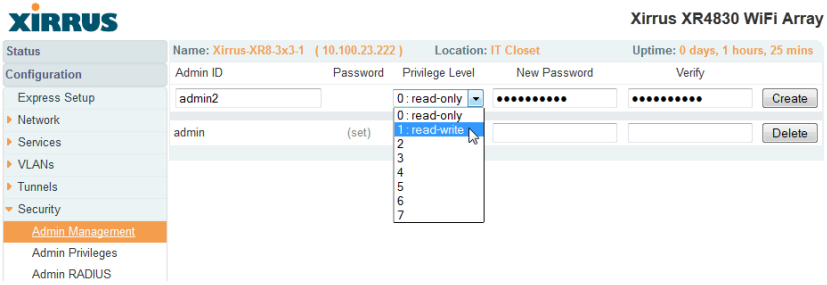


Figure 123. Admin Management

Procedure for Creating or Modifying Network Administrator Accounts

1. **Admin ID:** Enter the login name for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive.
2. **Read/Write**: Choose **1:read-write** if you want to give this administrator ID full read/write privileges, or choose **0:read-only** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations. Or you may select one of your custom-defined privilege levels (see "Admin Privileges" on page 216).
3. **New Password**: Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive.

4. **Verify**: Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).
5. Click on the **Create** button to add this administrator ID to the list.
6. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Admin Privileges
External Radius
Global Settings (IAP)
Internal Radius
Management Control

Admin Privileges

This window provides a detailed level of control over the privileges of Array administrators. Administrators may be assigned one of eight **Privilege Levels**. You may define the privilege level of each major feature (**Configuration Section**) that may be configured on the Array. For example, say that you set the privilege level to 4 for Reboot Array, Security, Radius Server, and SNMP, and you leave all other configuration sections at the default privilege level of 1. In this case, any administrator with a privilege level of 4 or higher may perform any operation on the Array, while an administrator with a privilege level lower than 4 but at least 1 may perform any operation except those whose level was set to 4. An error message will be displayed if an operation is attempted without a sufficient privilege level.

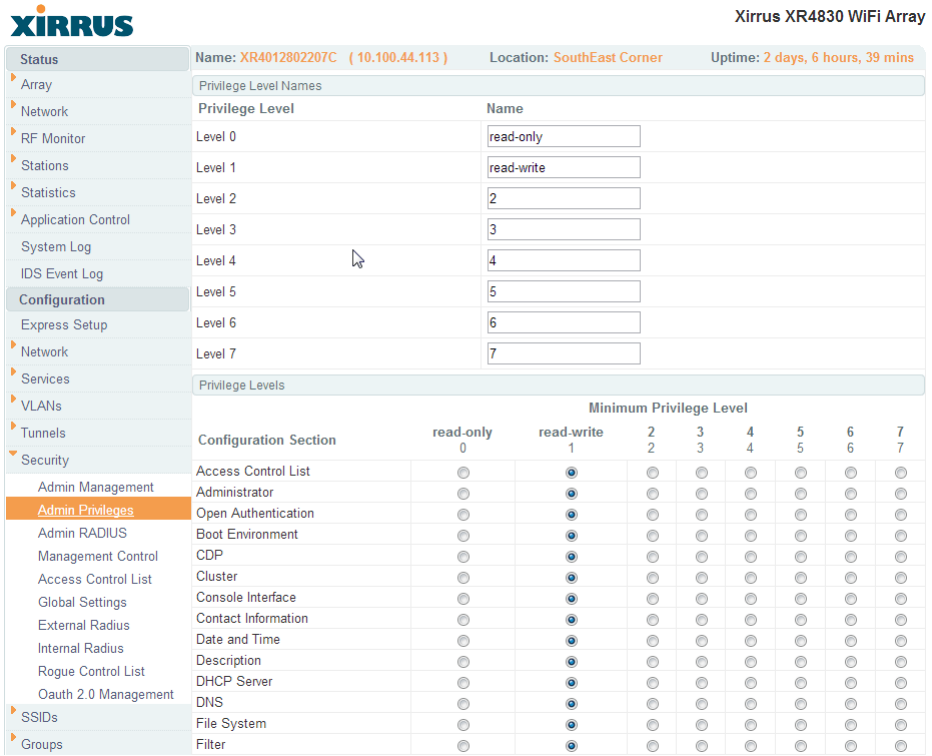


Figure 124. Admin Privileges

Privilege level 0 is **read-only**. As a minimum, all administrators have permission for read access to all areas of Array configuration. Higher privilege levels may be used to define additional privileges for specific configuration sections.

If you are using an Admin RADIUS server to define administrator accounts, please see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" on page 491 to set the privilege level for each administrator.

Procedure for Configuring Admin Privileges

1. **Privilege Level Names** (optional): You may assign a **Name** to each Privilege Level. The name may be used to describe the access granted by this level. By default, levels **0** and **1** are named **read-only** and **read-write**, respectively, and levels **2** through **7** have the same name as their level number.
2. **Privilege Levels**: Use this section to assign a **Minimum Privilege Level** to selected **Configuration Sections** as desired. By default, all sections are assigned level 1. When you select a higher privilege level for a configuration section, then only administrators who have at least that privilege level will be able to make configuration changes to that section.
3. You may click **^** at the bottom of any row to toggle the values in the entire column to either on or off.
4. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

External Radius
Groups
Admin Management
Admin RADIUS
Security

Admin RADIUS

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

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

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

About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS **Xirrus-Admin-Role** attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its Xirrus-Admin-Role attribute to the desired **Privilege Level Name** string, as defined in "Admin Privileges" on page 216. For more information about the RADIUS VSAs used by Xirrus, see "RADIUS Vendor Specific Attribute (VSA) for Xirrus" on page 491.

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

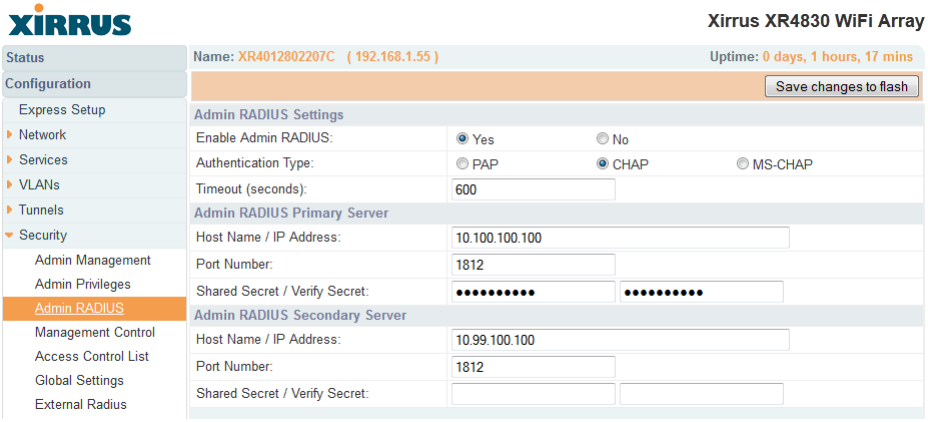


Figure 125. Admin RADIUS

Procedure for Configuring Admin RADIUS

Use this window to enable/disable administrator authentication via RADIUS, and to set up primary and secondary servers to use for authentication of administrators attempting to log in to the Array.

1. **Admin RADIUS Settings:**

   a. **Enable Admin RADIUS**: Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.

   b. **Authentication Type**: Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).

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

c. **Timeout (seconds)**: Define the maximum idle time (in seconds) before the RADIUS server's session times out. The default is 600 seconds.

2. **Admin RADIUS Primary Server**: This is the RADIUS server that you intend to use as your primary server.

   a. **Host Name / IP Address**: Enter the IP address or domain name of this external RADIUS server.

   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

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

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

3. **Admin RADIUS Secondary Server** (optional): If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will "failover" to the secondary RADIUS server (defined here).

   a. **Host Name / IP Address**: Enter the IP address or domain name of this RADIUS server.

   b. **Port Number**: Enter the port number of this RADIUS server. The default is 1812.

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

Management Control

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

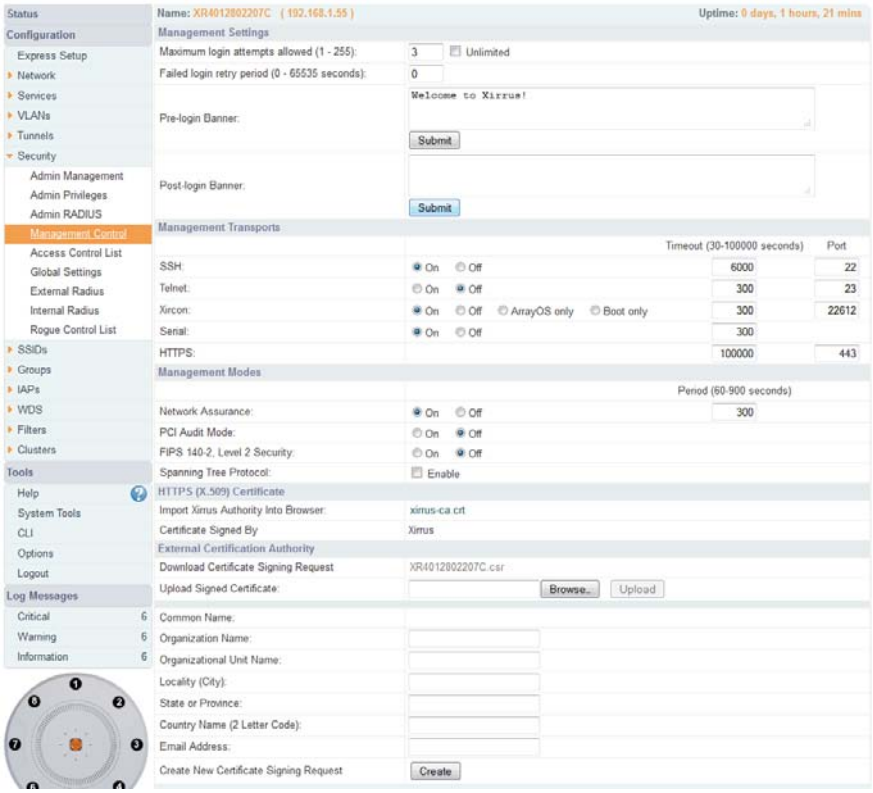


Figure 126. Management Control

Procedure for Configuring Management Control

1. **Management Settings:**

    a. **Maximum login attempts allowed (1-255)**: After this number of consecutive failing administrator login attempts via ssh or telnet, the **Failed login retry period** is enforced. The default is 3.

b. **Failed login retry period (0-65535 seconds)**: After the maximum number (defined above) of consecutive failing administrator login attempts via ssh or telnet, the administrator's IP address is denied access to the Array for the specified period of time (in seconds). The default is 0.

c. **Pre-login Banner**: Text that you enter here will be displayed above the WMI login prompt. (Figure 127)

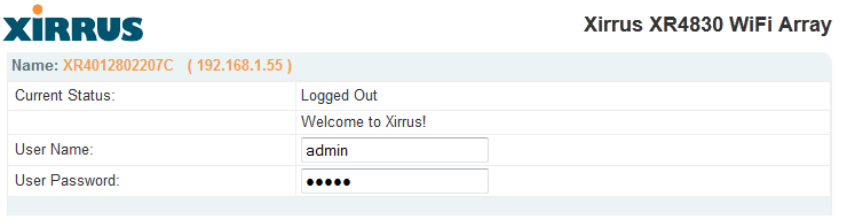


Figure 127. Pre-login Banner

d. **Post-login Banner**: Text that you enter here will be displayed in a message box after a user logs in to the WMI.

2. **SSH**

a. **On/Off**: Choose **On** to enable management of the Array over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the Array. SSH clients used for connecting to the Array must be configured to use SSH-2.

b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

c. **Port**: Enter a value in this field to define the port used by SSH. The default port is 22.

3. **Telnet:**
   a. **On/Off**: Choose **On** to enable Array management over a Telnet connection, or **Off** to disable this feature. SSH offers a more secure connection than Telnet, and is recommended over Telnet.
   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Telnet connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
   c. **Port**: Enter a value in this field to define the port used by Telnet. The default port is 23.
4. **Xircon**

   The Xircon utility connects to Xirrus Arrays that do not have a physical console port (XR-500, XR-1000 and some XR-2000 models), or whose console port is not accessible. Please see "Securing Low Level Access to the Array" on page 73 for more information about Xircon. You can enable or disable Xircon access to the Array as instructed below.

   ! *__Warning__: If you disable Xircon access completely on models that have no console port, 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.*

   a. **On/Off**: Choose **On** to enable Xircon access to the Array at the ArrayOS (CLI) and Xirrus Boot Loader (XBL) levels, or **Off** to disable access at both levels. On models that have no console port, Xircon access is **On** by default. On all other Array models, Xircon access is **Off** by default.
   b. **ArrayOS only**: Choose this radio button to enable Xircon access at the ArrayOS level only (i.e., Xircon can access CLI only). Access to the Array at the Xirrus Boot Loader (XBL) level is disabled.
   c. **Boot only**: Choose this radio button to enable Xircon access at the Xirrus Boot Loader (XBL) level only. ArrayOS level (CLI) access to the Array is disabled.

d. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your Xircon connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

e. **Port**: Enter a value in this field to define the port used by Xircon. The default port is 22612.

5. **Console**

   a. **On/Off**: Choose **On** to enable management of the Array via a serial connection, or choose **Off** to disable this feature.

   b. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.

6. **HTTPS**

   a. **Connection Timeout 30-100000 (Seconds)**: Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.

   b. **Port**: Enter a value in this field to define the port used by SSH. The default port is 443.

7. **Management Modes**

   a. **Network Assurance**: Click the **On** button to enable this mode. Network assurance checks network connectivity to each server that you configure, such as the NTP server, RADIUS servers, SNMP trap hosts, etc. By proactively identifying network resources that are unavailable, the network manager can be alerted of problems potentially before end-users notice an issue. The distributed intelligence of Arrays provides this monitoring at multiple points across the network, adding to the ability to isolate the problem and expedite the resolution

   Connectivity is checked when you configure a server. If a newly configured server is unreachable, you will be notified directly and a Syslog entry is created. Configured servers are checked once per **Period** which by default is 300 seconds (five minutes). Servers are checked regardless of whether they are configured as IP addresses or host names.

   If a server becomes unreachable, a Syslog message is generated. When the server again becomes reachable, another Syslog message is generated.

   To view the status of all configured servers checked by this feature, please see "Network Assurance" on page 109.

8. **HTTPS (X.509) Certificate**

ArrayOS releases 6.5 and above only support 2048-bit certificates, while previous releases only support 1024-bit certificates. The Array saves data related to previous 1024-bit and current 2048-bit certificates separately, thus ArrayOS can be upgraded or downgraded without losing any of this data. When ArrayOS is upgraded to 6.5, a new self-signed certificate will be automatically generated.

If you have imported a previous (pre-Release 6.5 version) Xirrus CA-signed certificate into your browser, the trusted Xirrus CA needs to be updated. Delete the current Xirrus CA in the browser. Upgrade the Array to release 6.5 or above and then download the new xirrus-ca.crt file and import it into the browser as a trusted CA, as explained below.

Similarly, if you are using a certificate signed by an external CA, you will need to update and replace that certificate on the Array.

a. **Import Xirrus Authority into Browser**: This feature imports the Xirrus Certificate Authority (CA) into your browser (for a discussion, please see "Certificates and Connecting Securely to the WMI" on page 212). Click the link (**xirrus-ca.crt**), and then click **Open** to view or install the current Xirrus CA certificate. Click **Install Certificate** to start your browser's Certificate Install Wizard. We recommend that you use this process to install Xirrus as a root authority in your browser.

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

- You must have assigned a host name to the Array and rebooted at some time after that.
- Use **Import Xirrus Authority into Browser**

- Access WMI by using the host name of the Array rather than its IP address.

b. **HTTPS (X.509) Certificate Signed By**: This read-only field shows the signing authority for the current certificate.

9. **External Certification Authority**

This step and Step 10 allow you to obtain a certificate from an external authority and install it on an Array. "Using an External Certificate Authority" on page 213 discusses reasons for using an external CA.

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

- If you don't already have the certificate from the external (non-Xirrus) Certificate Authority, see Step 10 to create a request for a certificate.
- Use Step 9a to review the request and copy its text to send to VeriSign.
- When you receive the new certificate from VeriSign, upload it to the Array using Step 9b.

External Certification Authority has the following fields:

a. **Download Certificate Signing Request**: After creating a certificate signing request (.csr file—Step 10), click the **View** button to review it. If it is satisfactory, click the name of the .csr file to display the text of the request. You can then copy this text and use it as required by the CA. You may also click on the filename of the .csr file to download it to your local computer.

b. **Upload Signed Certificate**: To use a custom certificate signed by an authority other than Xirrus, use the **Browse** button to locate the certificate file, then click **Upload** to copy it to the Array. The Array's web server will be restarted and will pick up the new certificate. This will terminate any current web sessions, and you will need to reconnect and re-login to the Array.

10. **To create a Certificate Signing Request**
    a. Fill in the fields in this section: **Common Name, Organization Name, Organizational Unit Name, Locality (City), State or Province, Country Name,** and **Email Address**. Spaces may be used in any of the fields, except for Common Name, Country Name, or Email Address. Click the **Create** button to create the certificate signing request. See Step 9 above to use this request.
11. Click **Save changes to flash** if you wish to make your changes permanent.

See Also

Network Interfaces - to enable/disable management over an Ethernet interface
Global Settings (IAP) - to enable/disable management over IAPs
Admin Management
External Radius
Global Settings (IAP)
Internal Radius
Access Control List
Security

Access Control List

This window allows you to enable or disable the use of the global Access Control List (ACL), which controls whether a station with a particular MAC address may associate to the Array. You may create station access control list entries and delete existing entries, and control the type of list.

There is only one global ACL, and you may select whether its type is an Allow List or a Deny List, or whether use of the list is disabled.

There is also a per-SSID ACL (see "Per-SSID Access Control List" on page 267). If the same MAC address is listed in both the global ACL and in an SSID's ACL, and if either ACL would deny that station access to that SSID, then access will be denied.