USER'S GUIDE

Wireless Arrays and Access Points

XR Series
March 10, 2014
Release 6.7

XIRRUS®
High Performance Wireless Networks

Wireless Arrays™ and Access Points

XR Series

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

Part Number: 800-0022-001
(Revision 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 -H Models)" on page 511.

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 5
XR-500 Series Access Points 5
XR-600 Series Access Points 6
XR-1000 7
XR-2000/2005 Series Arrays 8
XR-4000 Series Arrays 9
XR-6000 Series Arrays 10
Enterprise Class Security 11
Deployment Flexibility 11
Power over Gigabit Ethernet (PoGE) 12
Enterprise Class Management 13
Key Features and Benefits 14
High Capacity and High Performance 14
Extended Coverage 15
Flexible Coverage Schemes 15
Non-Overlapping Channels 16
SDMA Optimization 17
Fast Roaming 17
Ease of Deployment 17
Powerful Management 17
Secure Wireless Access 17
Applications Enablement 17
Advanced Feature Sets 18
Xirrus Advanced RF Performance Manager (RPM) 18
Xirrus Advanced RF Security Manager (RSM) 19
Xirrus Advanced RF Analysis Manager (RAM) 20

Xirrus Application Control 21
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
About IEEE 802.11ac 37
Up to Eight Simultaneous Data Streams—Spatial Multiplexing 39
MIMO (Multiple-In Multiple-Out) 39
MU-MIMO (Multi-User Multiple-In Multiple-Out) 40
Higher Precision in the Physical Layer 42
80 MHz and 160 MHz Channel Widths (Bonding) 43
802.11ac Data Rates 44
ACExpress™ 45
802.11ac Deployment Considerations 45
Failover Planning 47
Switch Failover Protection 48
Power Planning 49
Power over Gigabit Ethernet 49
Security Planning 50
Wireless Encryption 50
Authentication 50
Port Requirements 52

Network Management Planning 56
WDS Planning 57
Common Deployment Options 60
Installation Workflow 61
Installing Your Wireless Array 63
Choosing a Location 63
Wiring Considerations 63
Mounting and Connecting the Array/AP 66
Dismounting the Array 66
Powering Up the Wireless Array 66
Array LED Operating Sequences 67
LED Boot Sequence 67
LED Operation when Array is Running 68
Zero-Touch Provisioning and Ongoing Management 69
XMS Cloud Next Generation (XMS-9500-CL-x) 69
XMS Enterprise 69
If you are not using XMS 70
Array/AP Management Interfaces 71
User Interfaces (CLI, WMI) 71
Using the Serial Port 73
Using the Ethernet Ports 73
Starting the WMI 74
Logging In 74
Licensing 74
Performing the Express Setup Procedure 75
Securing Low Level Access to the Array 76

The Web Management Interface 81

Managing Arrays Locally or via XMS 81
An Overview 82
Structure of the WMI 83
User Interface 85
Logging In 88
Applying Configuration Changes 89
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 102
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 128
Signal-to-Noise Ratio (SNR) 130
Noise Floor 131
Max by IAP 133
Station Assurance 134
Statistics Windows 135
IAP Statistics Summary 135
Per-IAP Statistics 136
Network Statistics 138

VLAN Statistics 139
WDS Statistics 140
IDS Statistics 141
Filter Statistics 143
Station Statistics 144
Per-Station Statistics 145
Application Control Windows 146
About Application Control 146
Application Control 148
Stations (Application Control) 152
System Log Window 153
IDS Event Log Window 155

Configuring the Wireless Array 157

Express Setup 159
Network 165
Network Interfaces 166
Network Interface Ports 167
Bonds and Bridging 169
DNS Settings 176
CDP Settings 177
Services 179
Time Settings (NTP) 180
NetFlow 182
Wi-Fi Tag 183
Location 184
System Log 186
About Using the Splunk Application for Xirrus Arrays 189
SNMP 191
DHCP Server 194
Proxy Forwarding 196
About Proxy Forwarding 196
Proxy Forwarding for HTTPS 197
Summary of Proxy Forwarding Behavior on the Array 198
VLANs 204
Understanding Virtual Tunnels 204

VLAN Management 206
Tunnels 209
About Xirrus Tunnels 209
Tunnel Management 210
SSID Assignments 211
Security 213
Understanding Security 214
Certificates and Connecting Securely to the WMI 217
Using the Array's Default Certificate 217
Using an External Certificate Authority 218
Admin Management 219
Admin Privileges 221
Admin RADIUS 223
About Creating Admin Accounts on the RADIUS Server 223
Management Control 226
Access Control List 234
Global Settings 236
External Radius 240
About Creating User Accounts on the RADIUS Server 241
Internal Radius 244
Active Directory 246
Rogue Control List 250
OAuth 2.0 Management 251
SSIDs 254
Understanding SSIDs 255
Understanding QoS Priority on the Wireless Array 256
High Density 2.4G Enhancement—Honeypot SSID 261
SSID Management 262
SSID List (top of page) 263
SSID Limits 267
Web Page Redirect (Captive Portal) Configuration 269
Whitelist Configuration for Web Page Redirect 273
WPA Configuration 274
Authentication Service Configuration 274
Active IAPs 275
Per-SSID Access Control List 276
Honeypots 278

Groups 280
Understanding Groups 280
Using Groups 281
Group Management 282
Group Limits 285
IAPs 287
Understanding Fast Roaming 288
IAP Settings 290
Global Settings (IAP) 295
Beacon Configuration 297
Station Management 298
Advanced Traffic Optimization 300
Global Settings .11an 311
Global Settings .11bgn 316
Global Settings .11n 322
Global Settings .11ac 325
Global Settings .11u 327
Understanding 802.11u 327
Advanced RF Settings 333
About Standby Mode 334
RF Monitor 334
RF Resilience 335
RF Power & Sensitivity 336
RF Spectrum Management 337
Station Assurance 340
Hotspot 2.0 342
Understanding Hotspot 2.0 342
NAI Realms 344
Understanding NAI Realm Authentication 344
NAI EAP 346
Intrusion Detection 348
DoS Attacks 349
Impersonation Attacks 350
About Blocking Rogue APs 351
RF Intrusion Detection and Auto Block Mode 352
DoS Attack Detection Settings 353
Impersonation Detection Settings 354

LED Settings 354
DSCP Mappings 355
Roaming Assist 356
WDS 358
About Configuring WDS Links 358
Long Distance Links 360
WDS Client Links 361
Filters 365
Filter Lists 366
Filter Management 368
Clusters 374
Cluster Definition 375
Cluster Management 376
Cluster Operation 377
Mobile 380
AirWatch 380
User Procedure for Wireless Access 382

Using Tools on the Wireless Array 385

System Tools 386
About Licensing and Upgrades 387
System 388
Automatic Updates from Remote Image or Configuration File 390
Configuration 391
Diagnostics 394
Application Control Signature File Management 395
Web Page Redirect (Captive Portal) 396
Network Tools 397
Progress and Status Frames 399
CLI 399
API Documentation 401
Status/Settings 402
GET Requests 402
Trying a GET Request 403
API Documentation Toolbar 405
Options 406
Logout 407

The Command Line Interface 409

Establishing a Secure Shell (SSH) Connection 409
Getting Started with the CLI 411
Inputting Commands 411
Getting Help 411
Top Level Commands 413
Root Command Prompt 413
configure Commands 414
show Commands 417
statistics Commands 420
Configuration Commands 422
acl 422
admin 423
auth 424
cdp 424
clear 426
cluster 428
contact-info 429
date-time 430
dhcp-server 431
dns 432
file 433
filter 437
Air Cleaner 438
group 441
hostname 441
interface 442
load 442
location 443
location-reporting 444
management 445
mdm 446
more 447
netflow 448
no 449
quick-config 451
quit 452

authentication-server 452
reboot 453
reset 453
restore 454
roaming-assist 455
run-tests 456
security 458
snmp 459
ssid 460
syslog 461
tunnel 462
uptime 463
vlan 463
wifi-tag 464
Sample Configuration Tasks 466
Configuring a Simple Open Global SSID 467
Configuring a Global SSID using WPA-PEAP 468
Configuring an SSID-Specific SSID using WPA-PEAP 469
Enabling Global IAPs 470
Disabling Global IAPs 471
Enabling a Specific IAP 472
Disabling a Specific IAP 473
Setting Cell Size Auto-Configuration for All IAPs 474
Setting the Cell Size for All IAPs 475
Setting the Cell Size for a Specific IAP 476
Configuring VLANs on an Open SSID 477
Configuring Radio Assurance Mode (Loopback Tests) 478

Appendices 481

Appendix A: Quick Reference Guide 483
Factory Default Settings 483
Host Name 483
Network Interfaces 483
Serial 483
Gigabit 1 and Gigabit 2 484
Server Settings 484
NTP 484

Syslog 484
SNMP 485
DHCP 485
Default SSID 486
Security 486
Global Settings - Encryption 486
External RADIUS (Global) 487
Internal RADIUS 488
Administrator Account and Password 488
Management 488
Keyboard Shortcuts 489

Appendix B: FAQ and Special Topics 491
General Hints and Tips 491
Frequently Asked Questions 492
Multiple SSIDs 492
Security 494
VLAN Support 497
Array Monitor and Radio Assurance Capabilities 500
Enabling Monitoring on the Array 500
How Monitoring Works 500
Radio Assurance 501
Radio Assurance Options 502
RADIUS Vendor Specific Attribute (VSA) for Xirrus 503
Location Service Data Formats 504
Euclid Location Server 504
Non-Euclid Location Server 504
Upgrading the Array via CLI 506
Sample Output for the Upgrade Procedure: 507

Appendix C: Notices (Arrays except XR-500/600 and -H Models) 511
Notices 511
EU Directive 1999/5/EC Compliance Information 515
Compliance Information (Non-EU) 522
Safety Warnings 523
Translated Safety Warnings 524
Software License and Product Warranty Agreement 525
Hardware Warranty Agreement 531

Appendix D: Notices (XR500/600 Series Only) 533
Notices 533
EU Directive 1999/5/EC Compliance Information 537
Compliance Information (Non-EU) 544
Safety Warnings 545
Translated Safety Warnings 546
Software License and Product Warranty Agreement 547
Hardware Warranty Agreement 553

Appendix E: Medical Usage Notices 555

Glossary of Terms 561

Index 573

List of Figures

Figure 1. Xirrus Arrays: XR Series 1
Figure 2. Wireless Array (XR Series) 4
Figure 3. Wireless Coverage Patterns 11
Figure 4. XP8 - Power over Ethernet Usage 12
Figure 5. WMI: Array Status 13
Figure 6. Layout of IAPs (XR-7630) 14
Figure 7. Coverage Schemes (XR-7230 shown) 16
Figure 8. Wall Thickness Considerations 29
Figure 9. Unit Placement 30
Figure 10. Full (Normal) Coverage 31
Figure 11. Adjusting RF Patterns 31
Figure 12. Custom Coverage 32
Figure 13. Connection Rate vs. Distance 32
Figure 14. Transmit Power 33
Figure 15. Overlapping Cells 34
Figure 16. Allocating Channels Manually 36
Figure 17. Spatial Multiplexing 39
Figure 18. MIMO Signal Processing 40
Figure 19. MU-MIMO with Four Antennas 41
Figure 20. Physical Layer Data Encoding 42
Figure 21. Channel Bonding (Channels 36-64 shown) 44
Figure 22. Maximum 802.11ac Data Rates 44
Figure 23. Port Failover Protection 47
Figure 24. Switch Failover Protection 48
Figure 25. Port Requirements for XMS 52
Figure 26. WDS Link 57
Figure 27. A Multiple Hop WDS Connection 58
Figure 28. WDS Failover Protection 58
Figure 29. Installation Workflow 61
Figure 30. Array Placement 63
Figure 31. LED Locations 66
Figure 32. Network Interface Ports—XR-520 (left); XR-1000 Series (right) 71
Figure 33. Network Interface Ports—XR-600 Series 71
Figure 34. Network Interfaces—XR-2000 Series (left); XR-2005 Series (right) ... 72

Figure 35. Network Interface Ports—XR-4000 Series 72
Figure 36. Network Interface Ports—XR-6000 Series 72
Figure 37. Web Management Interface 82
Figure 38. WMI: Frames 85
Figure 39. WMI Header 86
Figure 40. WMI Command Log 87
Figure 41. WMI: Utility Buttons 87
Figure 42. Logging In to the Wireless Array 88
Figure 43. Array Summary 92
Figure 44. Disabled IAP (Partial View) 95
Figure 45. IAP Cells 95
Figure 46. Network Assurance and Operating Status 96
Figure 47. Array Information 98
Figure 48. Show Configuration 99
Figure 49. Admin Login History 100
Figure 50. Network Settings 101
Figure 51. Network Map 102
Figure 52. Spanning Tree Status 105
Figure 53. Routing Table 106
Figure 54. ARP Table 106
Figure 55. DHCP Leases 107
Figure 56. Connection Tracking 107
Figure 57. CDP Neighbors 108
Figure 58. Network Assurance 109
Figure 59. Undefined VLANs 110
Figure 60. RF Monitor—IAPs 112
Figure 61. RF Monitor—IAPs 112
Figure 62. RF Spectrum Analyzer 114
Figure 63. Intrusion Detection/Rogue AP List 116
Figure 64. RF Monitor—Channel History 118
Figure 65. RF Monitor—Channel History (Rotated) 119
Figure 66. RF Monitor—Channel History (Text) 119
Figure 67. Radio Assurance 120
Figure 68. Stations 123
Figure 69. Location Map 125
Figure 70. Controls for Location Map 126
Figure 71. Station RSSI Values 128

Figure 72. Station RSSI Values—Colorized Graphical View 129
Figure 73. Station Signal-to-Noise Ratio Values 130
Figure 74. Station SNR Values—Colorized Graphical View..... 130
Figure 75. Station Noise Floor Values 131
Figure 76. Station Noise Floor Values—Colorized Graphical View 132
Figure 77. Max by IAP 133
Figure 78. Station Assurance 134
Figure 79. IAP Statistics Summary Page..... 135
Figure 80. Individual IAP Statistics Page 137
Figure 81. Network Statistics..... 138
Figure 82. VLAN Statistics..... 139
Figure 83. WDS Statistics 140
Figure 84. IDS Statistics Page 141
Figure 85. Filtered IDS Statistics 142
Figure 86. Filter Statistics 143
Figure 87. Station Statistics 144
Figure 88. Individual Station Statistics Page..... 145
Figure 89. Application Control 148
Figure 90. Application Control (Pie Charts)..... 150
Figure 91. Application Control (Station Traffic)..... 151
Figure 92. Stations (Application Control)..... 152
Figure 93. System Log (Alert Level Highlighted) 153
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 166
Figure 99. Network Bonds and Bridging..... 169
Figure 100. Bridging Traffic..... 170
Figure 101. Port Modes (a, b) 172
Figure 102. Port Modes (c, d) 173
Figure 103. Mirroring Traffic 175
Figure 104. DNS Settings..... 176
Figure 105. CDP Settings..... 177
Figure 106. Services..... 179
Figure 107. Time Settings (Manual Time)..... 180
Figure 108. Time Settings (NTP Time Enabled)..... 181

Figure 109. NetFlow 182
Figure 110. Wi-Fi Tag 183
Figure 111. Location 185
Figure 112. System Log 186
Figure 113. SNMP 191
Figure 114. DHCP Management 194
Figure 115. Proxy Forwarding Example 196
Figure 116. Set up a Proxy Server on each Client (Windows) 199
Figure 117. Specify Proxy Servers (Windows) 200
Figure 118. Set up a Proxy Server on each Client (Apple) 201
Figure 119. Specify Proxy Servers (Apple) 202
Figure 120. Proxy Forwarding 203
Figure 121. VLANs 204
Figure 122. VLAN Management 206
Figure 123. Tunnel Summary 209
Figure 124. Tunnel Management 210
Figure 125. Tunnel SSID Assignments 211
Figure 126. Security 213
Figure 127. Import Xirrus Certificate Authority 217
Figure 128. Admin Management 219
Figure 129. Admin Privileges 221
Figure 130. Admin RADIUS 224
Figure 131. Management Control 226
Figure 132. Pre-login Banner 227
Figure 133. Access Control List 234
Figure 134. Global Settings (Security) 236
Figure 135. External RADIUS Server 240
Figure 136. Internal RADIUS Server 244
Figure 137. Active Directory Server 247
Figure 138. Finding the Domain Name from Active Directory 248
Figure 139. Rogue Control List 250
Figure 140. OAuth 2.0 Management - Token List 252
Figure 141. SSIDs 254
Figure 142. Four Traffic Classes 257
Figure 143. Priority Level—IEEE 802.1p (Layer 2) 257
Figure 144. Priority Level—DSCP (DiffServ - Layer 3) 258
Figure 145. SSID Management 262

Figure 146. SSID Management—Encryption, Authentication, Accounting 265
Figure 147. WPR Internal Splash Page Fields (SSID Management)..... 269
Figure 148. Customizing an Internal Login or Splash Page 272
Figure 149. Whitelist Configuration for WPR..... 273
Figure 150. Setting Active IAPs per SSID 275
Figure 151. Per-SSID Access Control List 276
Figure 152. Honeypot Whitelist 278
Figure 153. Groups..... 280
Figure 154. Group Management 282
Figure 155. IAPs..... 287
Figure 156. Source of Channel Setting 287
Figure 157. IAP Settings 290
Figure 158. Global Settings (IAPs) 295
Figure 159. Multicast Processing 300
Figure 160. Additional Optimization Settings 306
Figure 161. Global Settings .11an 311
Figure 162. Global Settings .11bgn 316
Figure 163. Global Settings .11n 322
Figure 164. Global Settings .11ac 325
Figure 165. 802.11u Global Settings..... 328
Figure 166. Advanced RF Settings..... 333
Figure 167. Station Assurance (Advanced RF Settings) 341
Figure 168. Hotspot 2.0 Settings..... 343
Figure 169. NAI Realms 345
Figure 170. NAI EAP 346
Figure 171. Intrusion Detection Settings..... 348
Figure 172. LED Settings 354
Figure 173. DSCP Mappings..... 355
Figure 174. WDS..... 358
Figure 175. Configuring a WDS Link 359
Figure 176. WDS Client Links 361
Figure 177. Filters 365
Figure 178. Filter Lists 366
Figure 179. Filter Management 368
Figure 180. Filter Category or Application..... 372
Figure 181. Clusters 374
Figure 182. Cluster Definition 375

Figure 183. Cluster Management 376
Figure 184. Cluster Mode Operation 377
Figure 185. Cluster Mode Activation 377
Figure 186. Viewing Statistics in Cluster Mode 378
Figure 187. AirWatch Settings 380
Figure 188. System Tools 386
Figure 189. Saving the Diagnostic Log 394
Figure 190. Managing Application Control Signature files 395
Figure 191. Managing WPR Splash/Login page files 396
Figure 192. System Command (Ping) 397
Figure 193. Radius Ping Output 398
Figure 194. CLI Window 399
Figure 195. API Documentation 401
Figure 196. API — GET Request Details 402
Figure 197. API — GET Request Response 404
Figure 198. API Documentation Toolbar 405
Figure 199. WMI Display Options 406
Figure 200. Login Window 407
Figure 201. Logging In 410
Figure 202. Help Window 411
Figure 203. Full Help 412
Figure 204. Partial Help 412
Figure 205. Air Cleaner Filter Rules 439
Figure 206. Configuring a Simple Open Global SSID 467
Figure 207. Configuring a Global SSID using WPA-PEAP 468
Figure 208. Configuring an SSID-Specific SSID using WPA-PEAP 469
Figure 209. Enabling Global IAPs 470
Figure 210. Disabling Global IAPs 471
Figure 211. Enabling a Specific IAP 472
Figure 212. Disabling a Specific IAP 473
Figure 213. Setting the Cell Size for All IAPs 474
Figure 214. Setting the Cell Size for All IAPs 475
Figure 215. Setting the Cell Size for a Specific IAP 476
Figure 216. Configuring VLANs on an Open SSID 477
Figure 217. Configuring Radio Assurance Mode (Loopback Testing) 479

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 14.**
- **"Advanced Feature Sets" on page 18.**
- **"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, 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, providing zero-touch provisioning and initial startup for new Array/AP deployments. XMS is capable of managing large numbers of Arrays, including automated software and firmware upgrades for the network.

  Another option is XMS, hosted on your own server. It manages all aspects of your Xirrus wireless network. For customers using the XMS-9000-CL-x Cloud-hosted version, all Array management is performed via the cloud. For detailed information about XMS, 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 Array**s**. 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.

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. On Arrays featuring 802.11ac, this option is also included. 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 iap**1, 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 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 Point (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 Access Point 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.

These models have an integrated controller, firewall, threat sensor and spectrum analyzer. 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

Some smaller Arrays/APs have less memory (XR-500/1000 Series and XR-620) and are not able to run all ArrayOS features at the same time. You will receive an error message if you attempt to configure a feature when there is not enough memory left.

XR-600 Series Access Points

These Access Points provide 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), so that as more of your clients migrate to 802.11ac, you can increase the number of radios operating at 5 GHz. Each of the XR-630's two 3x3 802.11ac radios supports 1.3Gbps, connecting up to 240 users at one time with 2.6Gbps total Wi-Fi bandwidth.

These models have an integrated controller, firewall, threat sensor spectrum analyzer, and application-level intelligence. These models have omni-directional antennas rather than directional antennas.

The XR-630 supports a unique feature that 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

Some smaller Arrays/APs have less memory (XR-500/1000 Series and XR-620) and are not able to run all ArrayOS features at the same time. You will receive an error message if you attempt to configure a feature when there is not enough memory left.

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

Some smaller Arrays/APs have less memory (XR-500/1000 Series and XR-620) and can't run all ArrayOS features simultaneously. You will see an error message if you configure a feature when there is not enough memory.

XR-2000/2005 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 on a modular chassis designed for 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” (called the XR-2005 Series) 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)

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:

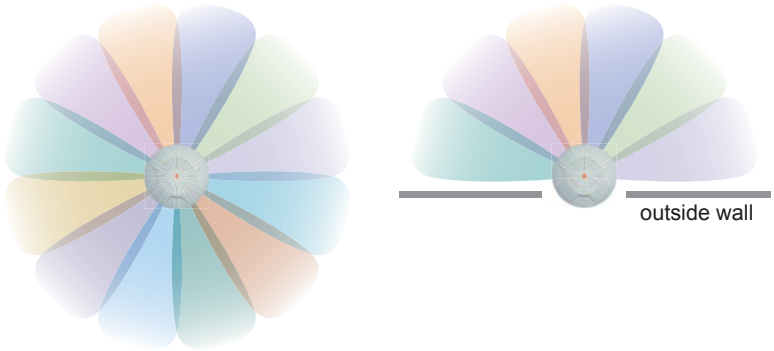


Figure 3. Wireless Coverage Patterns

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-2000 models ending in "5", and XR-500/600 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.

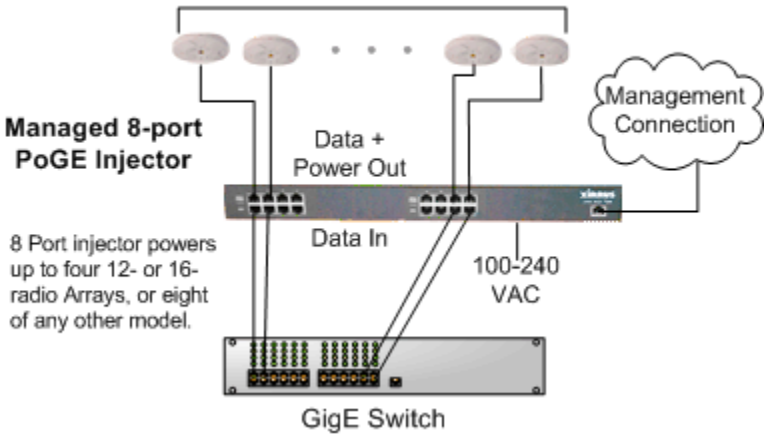


Figure 4. XP8 - Power over Ethernet Usage

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.

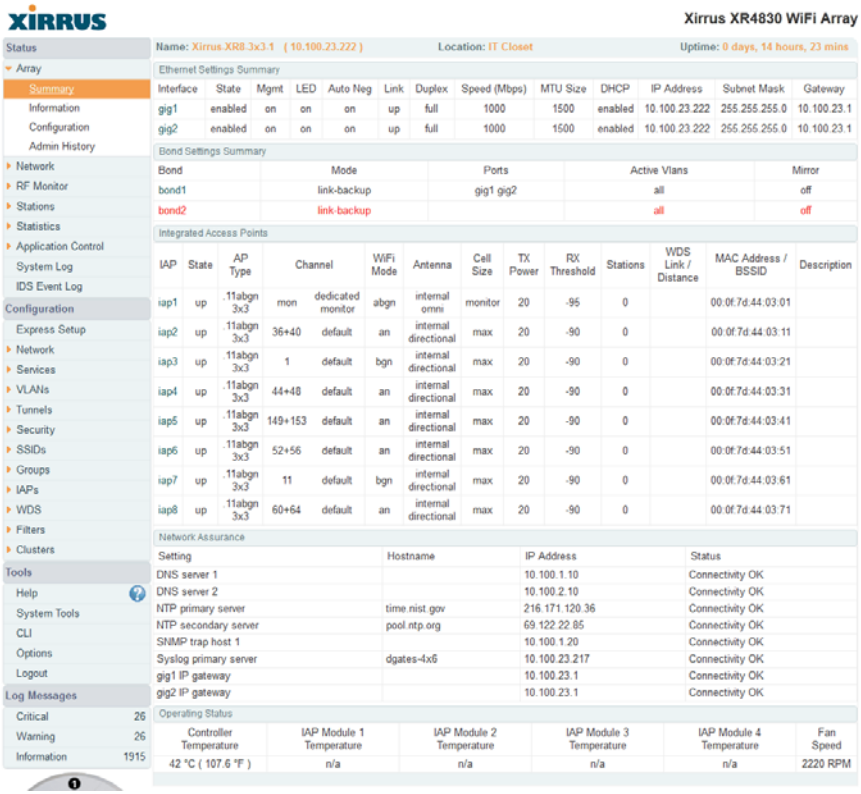


Figure 5. WMI: Array Status

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 cloud-based or enterprise version of 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.

Flexible Coverage Schemes

Your Wireless Array offers flexible coverage schemes for each wireless technology.

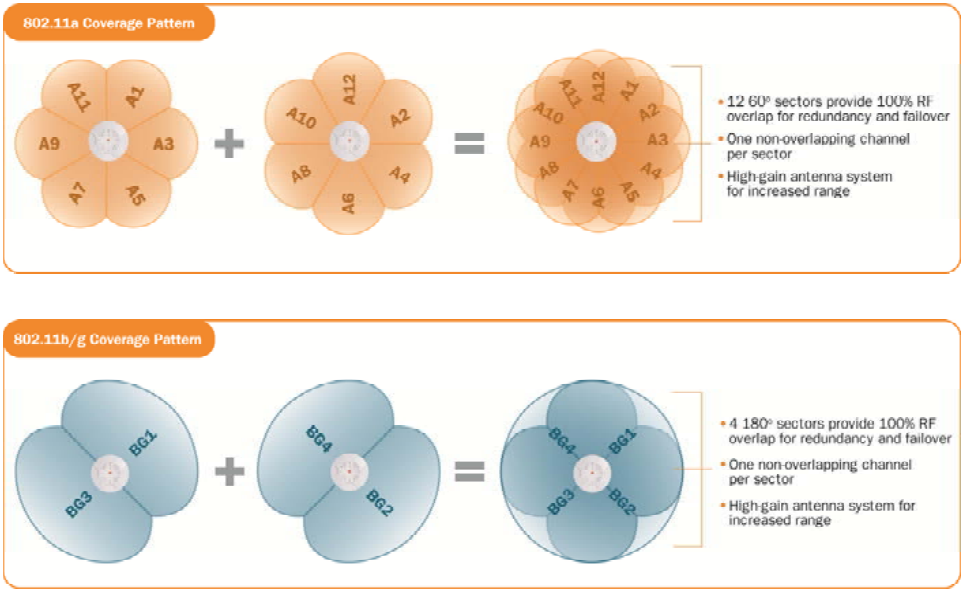


Figure 7. Coverage Schemes (XR-7230 shown)

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

Non-Overlapping Channels

Complete use of non-overlapping channels limits interference and delivers maximum capacity. On the 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 XMS and Mobilize services simplify and speed 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 Xirrus, 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 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 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 802.11ac 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 802.11 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 "bring your own device" (BYOD) becomes ubiquitous in enterprise networks, defending against these threats becomes more critical. With the Array's 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 wireless networks. The deployment of 802.11ac presents a set of unique challenges based on technology differences with legacy 802.11a/b/g/n 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 802.11ac installation, as well as give IT administrators the ability to troubleshoot issues that may occur within the wireless environment.

802.11ac deployment will continue to evolve over the next several years with additional performance and optional functions, along with an 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 smart phone 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 146 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 -H Models)**

  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 61**.
- **"Installing Your Wireless Array" on page 63**.
- **"Powering Up the Wireless Array" on page 66**.
- **"Zero-Touch Provisioning and Ongoing Management" on page 69**.
- **"Performing the Express Setup Procedure" on page 75**.

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.

- Array**Ethernet ports**
  You need at least one 100/1000 BaseT port to establish wired Gigabit Ethernet connectivity. XR Series Arrays have different numbers of ports,

depending on the model (see "XR Wireless Array Product Family" on page 5).

! *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**
  A serial port (console) is present on all Arrays/APs except XR-500/600/1000 Series and some XR-2000 models, where Xircon can be used instead—see the Xircon *User's Guide*. To connect directly to the console port on the Array, your computer must be equipped with a male 9-pin serial port and terminal emulation software (for example, HyperTerminal). The Xirrus Array only supports serial cable lengths up to 25' per the RS-232 specification.

  Use the following settings when establishing a serial connection:

Bits per second	115,200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

Optional Network Components

The following network components are optional.

- **Xirrus Management System (XMS)**
  The optional XMS offers powerful management features for small or large 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**
- **"About IEEE 802.11ac" on page 37**
- **"Failover Planning" on page 47**
- **"Power Planning" on page 49**
- **"Security Planning" on page 50**
- **"Port Requirements" on page 52**
- **"Network Management Planning" on page 56**
- **"WDS Planning" on page 57**
- **"Common Deployment Options" on page 60**

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/ac coverage that provides extended range. (Note that XR-500/600 Series radios are omni-directional rather than sectored.) 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.

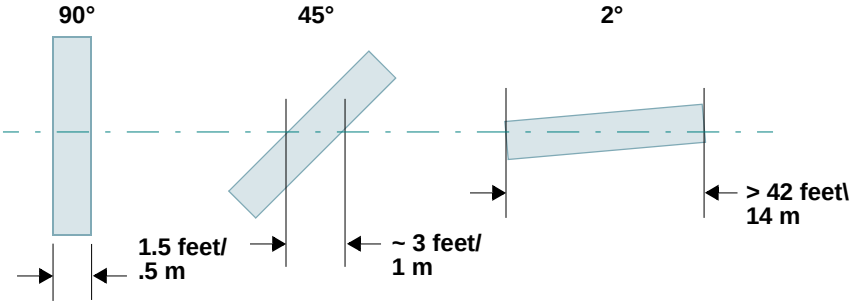


Figure 8. Wall Thickness Considerations

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).

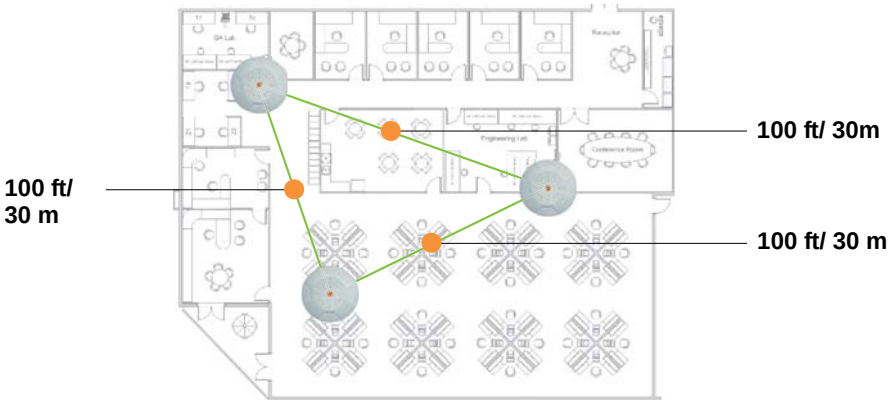


Figure 9. Unit Placement

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.

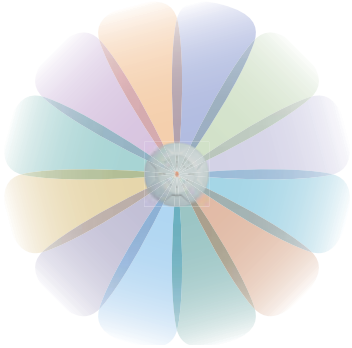


Figure 10. Full (Normal) Coverage

Half Coverage

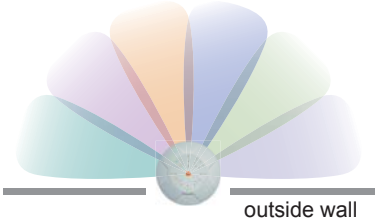


Figure 11. Adjusting RF Patterns

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.

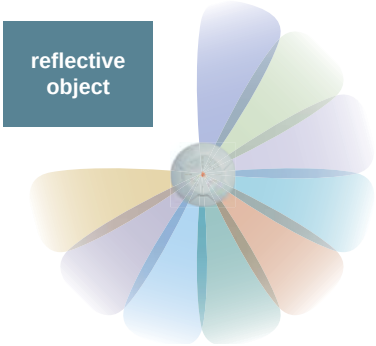


Figure 12. Custom Coverage

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.

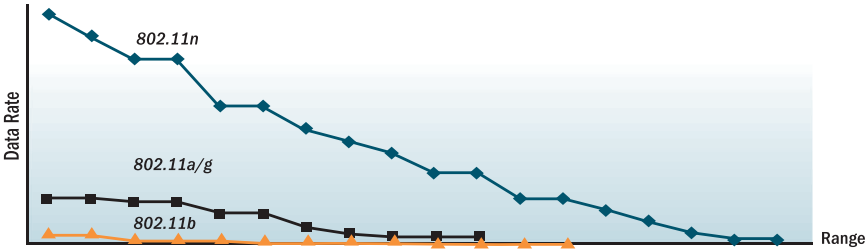


Figure 13. Connection Rate vs. Distance

Figure 13 shows relative connection rates for 802.11n vs. 802.11a/g and 802.11b, and the effect of distance on the connection rates. 802.11ac rates behave like 802.11n over distance—see Figure 22 for 802.11ac data 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.

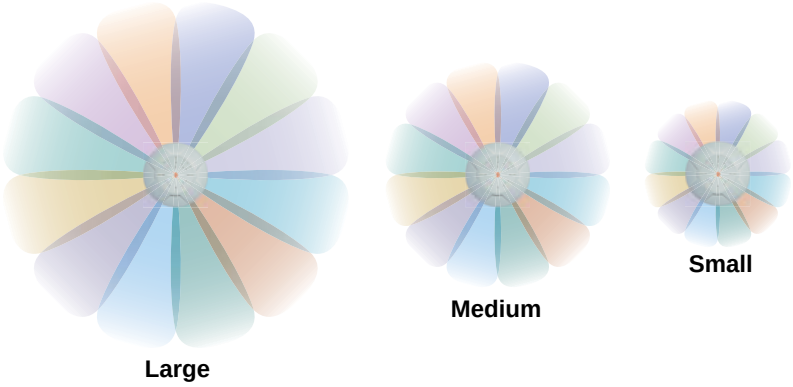


Figure 14. Transmit Power

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 336. XirrusXirrus

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 336.

Roaming Considerations

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

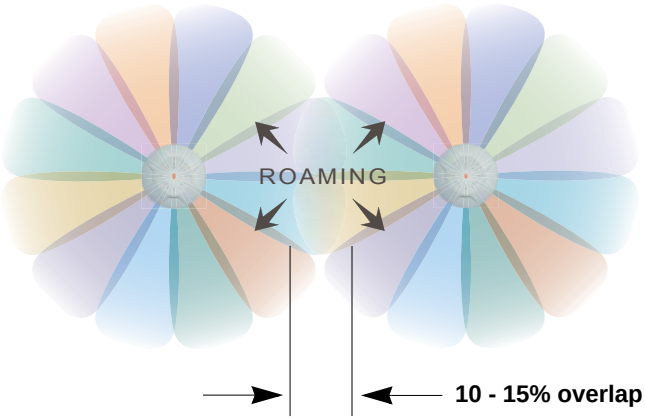


Figure 15. Overlapping Cells

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 333.

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.

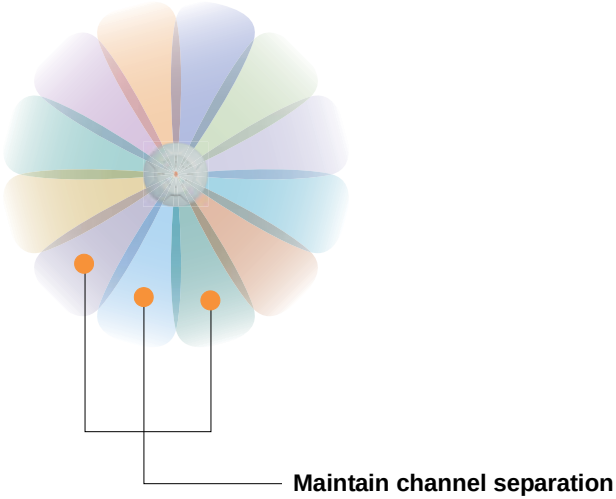


Figure 16. Allocating Channels Manually

See Also

Failover Planning

Installation Prerequisites

About IEEE 802.11ac

802.11ac is a continuation of the IEEE 802.11 standard. It multiplies the maximum data rate—up to ten times the 802.11n maximum will ultimately be available. Along with increased data rates, it offers simultaneous transmission to multiple clients.

802.11ac will be rolled out in two phases. Wave 1 products available in 2012-2013 support 80MHz channels and up to 3 data streams for a maximum data rate of 1.3 Gbps. Wave 2 and future products will add 160MHz channels and up to 8 streams, for a maximum data rate of 6.93Gbps.

Xirrus currently supports up to three streams (in units with 3x3 radios) and 80 MHz channels. Xirrus models that offer 802.11ac support this technology on all IAPs, not just on one. IAPs are individually configurable to different modes or groups of modes (such as 802.11a, 11b, 11g, and 11n). Xirrus optimizes 802.11ac performance further with ACExpress™. This innovation intelligently separates high-speed and lower-speed mobile devices on separate IAPs to maximize system performance.

The major advantages of 802.11ac are:

- Faster speeds than 802.11n over the same coverage area, operating at up to 1.3 Gbps in Wave 1 implementations. While the maximum distance that a Wi-Fi signal can reach is unchanged with 802.11ac, multiple antennas increase the data rate at every distance.
- Operates only in the less congested 5 GHz spectrum, which offers “cleaner” air and supports much greater capacity than the 2.4 GHz spectrum still used by 802.11n.
- Supports simultaneous communications to multiple clients on a single channel with multi-user MIMO in future Wave 2 products.
- Extends the techniques pioneered in 802.11n: more antennas, more spatial streams and wider channels to improve throughput.

The techniques that 802.11ac uses to realize these performance improvements and the expected results are discussed in:

- **"Up to Eight Simultaneous Data Streams—Spatial Multiplexing" on page 39**
- **"MIMO (Multiple-In Multiple-Out)" on page 39**
- **"MU-MIMO (Multi-User Multiple-In Multiple-Out)" on page 40**
- **"Higher Precision in the Physical Layer" on page 42**
- **"80 MHz and 160 MHz Channel Widths (Bonding)" on page 43**
- **"802.11ac Data Rates" on page 44**
- **"ACExpress™" on page 45**

It is important to consider 80 MHz and 160 MHz Channel Widths (Bonding) when planning your deployment, since it contributes greatly to 802.11ac's speed improvements and because it is configured separately for each IAP. Your selection of channel width in IAP Settings—40 MHz or 80 MHz or 20 MHz (if bonding is turned off)—has a major effect on your channel planning. A global setting is provided to enable or disable 802.11ac mode. See "Global Settings .11ac" on page 325 to configure operation.

There are other factors to keep in mind when planning a roll-out of 802.11ac. Please see "802.11ac Deployment Considerations" on page 45.

Up to Eight Simultaneous Data Streams—Spatial Multiplexing

Spatial Multiplexing transmits completely separate data streams on different antennas (in the same channel) that are recombined to produce new 802.11ac data rates. Previously used for 802.11n, the maximum number of streams for 802.11ac has been increased to eight. 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.

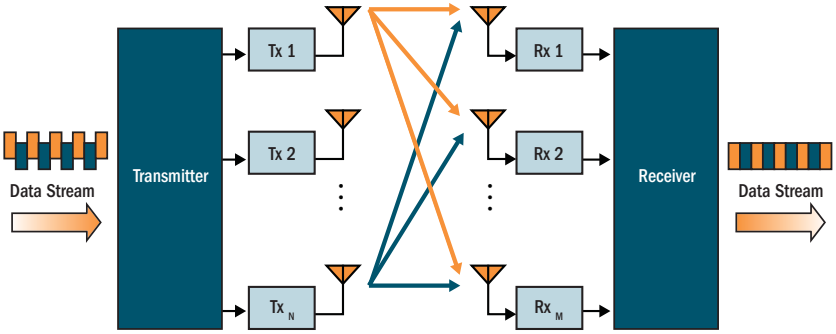


Figure 17. Spatial Multiplexing

The date rate increases directly with the number of transmit antennas used. Note that mobile devices in the near future will support up to three or four streams at most, with many supporting less.

MIMO (Multiple-In Multiple-Out)

MIMO (Multiple-In Multiple-Out) signal processing is one of the core technologies of 802.11n and 802.11ac. 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. 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 18). Multipath signals were considered to be interference by

802.11a/b/g radios, and degraded performance. In 802.11n and 802.11ac, these signals are used to enhance performance.

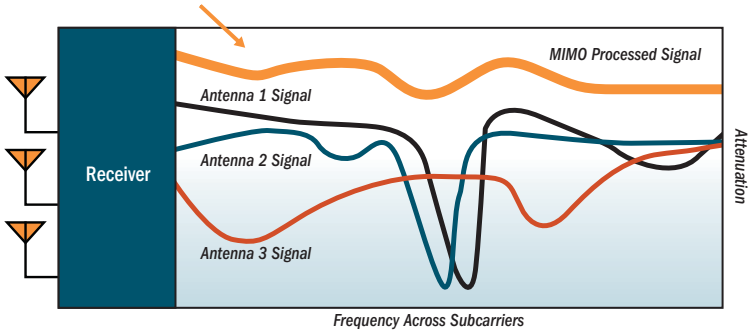


Figure 18. MIMO Signal Processing

802.11ac increases the number of antennas and spatial streams from a maximum of four in 802.11n to a maximum of eight, contributing to much higher maximum data rates (up to 6.93Gbit/s). The spatial streams can be concurrently allocated to more than one receiving device when the AP operates in multi-user MIMO mode (MU-MIMO, see the next section).

MU-MIMO (Multi-User Multiple-In Multiple-Out)

MU-MIMO (multi-user multiple-in/multiple-out) signal processing uses multiple antennas on the transmitter and receiver operating on the same channel. With spatial multiplexing in 802.11ac, up to 8 data streams may be concurrently transmitted. MU-MIMO's innovation allows the streams to be split between multiple devices at once.

With 802.11n, whenever the IAP transmitted data, all of the traffic at any instant of time was directed to a single client. As a consequence, if a set of devices included a mix of fast and slow client clients, the fast traffic was often substantially delayed by the transmission to slower clients. 802.11ac MU-MIMO works by directing some of the spatial streams to one client and other spatial streams to other clients, up to four at a time

For example, in the figure below, the transmitter has four antennas. Three are transmitting to an 802.11ac laptop that has three antennas, while the remaining

one is directed to a mobile phone. When a transmission is complete, the antennas are reallocated.

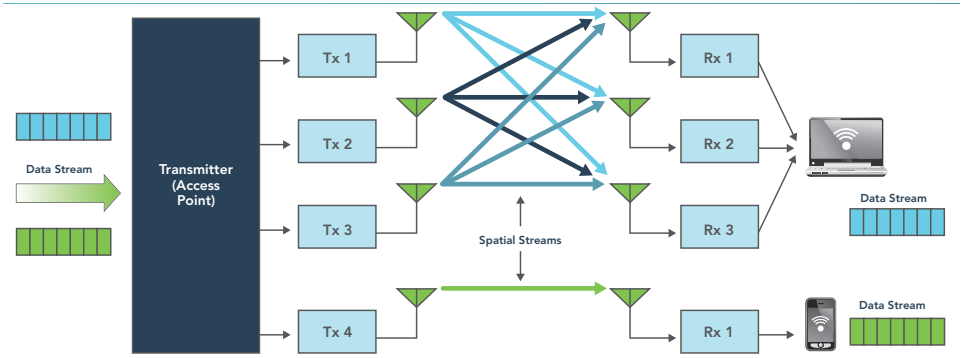


Figure 19. MU-MIMO with Four Antennas

The table below illustrates how data streams might be allocated to multiple users on an 802.11ac transmitter with multiple antennas.

# of AP Antennas	Possible Combinations of Receiver Antennas
2	1 station w/ 2 antennas -or- 2 stations w/ 1 antenna
3	1 station w/ 3 antennas -or- 1 station w/ 2 antennas + 1 station w/ 1 antenna -or- 3 stations w/ 1 antenna
4	1 station w/4 antennas -or- 2 stations w/2 antennas -or- 1 station w/2 antennas + 2 stations w/1 antenna -or- 4 stations w/ 1 antenna
8	1 station w/ 8 antennas -or- 2 stations w/ 4 antennas -or- 1 station w/ 4 antennas + 2 stations w/ 2 antennas -or- 2 stations w/ 2 antennas + 4 stations w/1 antenna -or- … many other combinations …

Higher Precision in the Physical Layer

Wi-Fi utilizes several digital modulation techniques and automatically switches between them to optimize for throughput or range. The basic unit of data transmitted is called a symbol. The number of points in the modulation constellation determines the number of bits of data conveyed with each symbol.

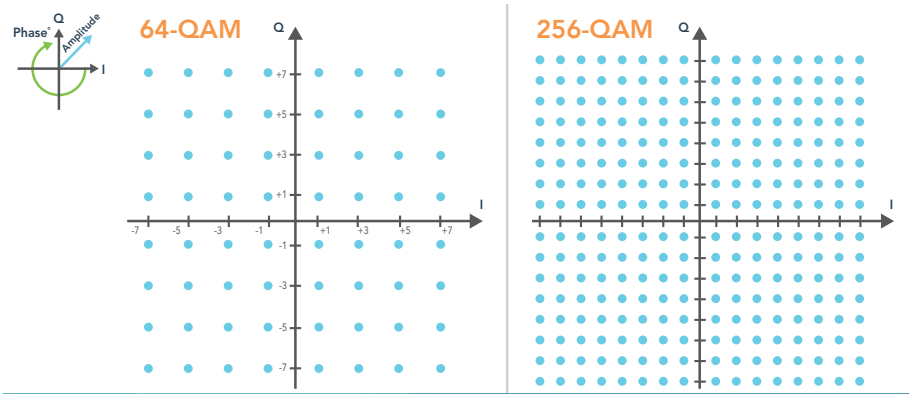


Figure 20. Physical Layer Data Encoding

802.11n uses 16 QAM (Quadrature Amplitude Modulation), which conveys log2(16) = 4 bits per symbol and 64 QAM, which conveys 6 bits per symbol. 802.11ac adds 256 QAM which conveys 8 bits per symbol for a 33% increase in throughput vs. the highest 802.11n data rate.

You may select the highest Modulation and Coding Scheme (MCS) level allowed with **1**, **2**, or **3 Spatial Streams (**see the **Max MCS** setting in "Procedure for Configuring Global 802.11ac IAP Settings" on page 326). You may limit the highest level of modulation to 64-QAM, or allow 256-QAM. It also determines the coding scheme used for error correction. Higher MCS levels allocate fewer bits to error correction, and thus more bits are used for data. The default value is **MCS9**, the highest level.

The higher the MCS value, the higher the data rate, as shown in the table below. Xirrus Arrays/APs support MCS7 -MCS9. Higher MCS levels require higher

signal-to-noise ratios (i.e., a less noisy environment) and shorter transmission distances.

MCS index value	Modulation	Code rate (R)
0	BPSK	1/2
1	QPSK	1/2
2	QPSK	3/4
3	16-QAM	1/2
4	16-QAM	3/4
5	64-QAM	2/3
6	64-QAM	3/4
7	64-QAM	5/6
8	256-QAM	3/4
9	256-QAM	5/6

80 MHz and 160 MHz Channel Widths (Bonding)

Channel bonding increases data rates by combining two, four, or eight adjacent 20 MHz channels into one channel. This increases the data rate proportional to the width of the bond.

Bonding is specified on the IAP Settings page for each IAP in terms of the primary channel and the width of the bond. Be aware that Channel Bonding impacts channel planning, since you are using multiple channels for an IAP.

802.11ac allows creation of 20, 40, 80, or 160 MHz wide channels. The 160MHz channel can also be a combination of two non-contiguous 80MHz channels (80+80). Although channel bonding increases bandwidth, wider channels are more susceptible to signal interference which may lead to reduced range and poorer signal quality. Figure 21 is an example showing how Channels 36-64 may be used: as eight 20 MHz channels; four 40 MHz channels; two 80 MHz channels; or one 160 MHz channel. Xirrus currently supports channels up to 80 MHz wide.

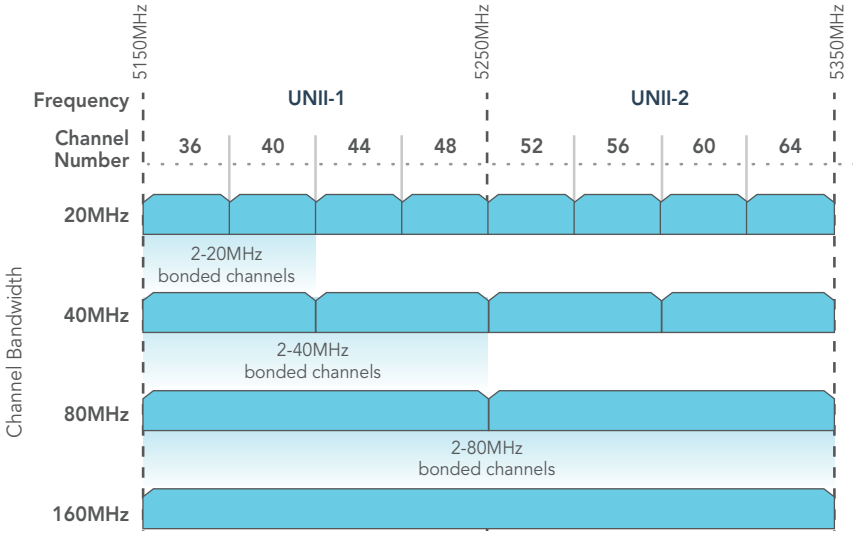


Figure 21. Channel Bonding (Channels 36-64 shown)

802.11ac Data Rates

Maximum Data Rate	# Transmit Antennas	Bandwidth (MHz)	# Streams	Modulation	
293Mbps	1	40	1	64QAM	Phase 1
433Mbps	1	80	1	256QAM	
867Mbps	2	80	2	256QAM	
1.299Gbps	3	80	3	256QAM	
1.730Gbps	4	80	4	256QAM	Phase 2+
3.470Gbps	8	80	8	256QAM	
867Mbps	1	160	1	256QAM	
1.730Gbps	2	160	2	256QAM	
3.470Gbps	8	160	4	256QAM	
6.930Gbps	8	160	8	256QAM	

Figure 22. Maximum 802.11ac Data Rates

IEEE 802.11ac data rates are dependent on the number of spatial streams obtained through the use of MU-MIMO, 80 vs. 160MHz channel widths, the number of transmit antennas, and the type of modulation. Figure 22 shows the maximum

data rate achievable at each level, with many additional lower rates occurring at each level dependent on signal level, signal to noise ratio in the environment, etc.

Phase 1 802.11ac, first available in consumer products in 2012 and enterprise products in 2013, supports up to 80MHz channels and up to 3 spatial streams for a maximum data rate of 1.3Gbps.

Phase 2 and beyond products, expected starting in 2014, will add 160MHz channels and up to 8 spatial streams for a maximum data rate of 6.9Gbps.

ACExpress™

Xirrus 802.11ac IAPs use ACExpress™ to optimize wireless performance by automatically separating faster 802.11ac clients from slower Wi-Fi clients. Since Wi-Fi is a shared medium, this separation ensures that slower 802.11a/b/g/n clients do not starve the performance of 802.11ac clients. For example, the data rate of an 802.11n client is less than 25% of the rate of an 802.11ac client, and thus will take four times as much air time for a given amount of data. This takes available bandwidth away from faster clients, reducing their performance significantly. ACExpress intelligently separates clients by type onto different radios, grouping fast clients separately from slow clients, thereby maximizing performance for all. ACExpress is supported on all Xirrus 802.11ac products, both APs and Arrays. ACExpress may be enabled or disabled as part of the Load Balancing feature. See Step 26 on page 307.

802.11ac Deployment Considerations

The theoretical data rates shown are just that, theoretical. For 802.11ac deployments, numerous factors affect real-world performance. These are some important considerations in the deployment of networks that include 802.11ac:

- **Wireless networks are not wired networks.** Wired network users who share a Gigabit network can expect to see bursts of up to 900Mbps, depending on their hardware. Maximum Wi-Fi data rates are reduced by signaling overhead and media contention. Most 802.11ac users will see data rates less than 100Mbps as the effective bandwidth is shared among all devices connecting to a given radio.

- **Migration to 802.11ac will take time.** Older Wi-Fi technologies will continue to be with us for years. In order for 802.11ac to provide maximum data rates, it is important to keep interference from earlier Wi-Fi standards at a minimum. For example, 802.11n devices operating in the 5GHz band can slow down 802.11ac devices to 300Mbps or 450Mbps depending on the 2x2 or 3x3 MIMO technology used.
- **Infrastructures must be upgraded as well.** The bandwidth required out of 802.11ac APs will certainly exceed 1Gbps and may reach 10Gbps. The links from the APs to the core network must keep pace with this need. Centralized firewalls, LAN controllers, and authentication servers may also reach their limits. Migration to a decentralized architecture, with intelligence at the edge of the network may be a more scalable solution, avoiding single points of failure.
- **More power.** Multi-antenna APs handling 802.11ac speeds will likely require more power. Power planning for your access switches should be carefully considered.
- **A new site survey may be needed.** Wireless networks established as recently as a few years ago were probably designed for coverage and not capacity. APs were placed so that there were no dead zones, without considering future capacity needs. With the increasing use of mobile devices, new site surveys that ensure enough bandwidth for anticipated usage should precede deployment of 802.11ac APs.
- **Manage application usage.** With 802.11ac, a range of applications are now practical on mobile devices that were previously only used over wired networks or on laptops. Uncontrolled use of Wi-Fi bandwidth can cause wireless networks to quickly degrade. Network control elements must control use of applications and prioritize critical applications.

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).

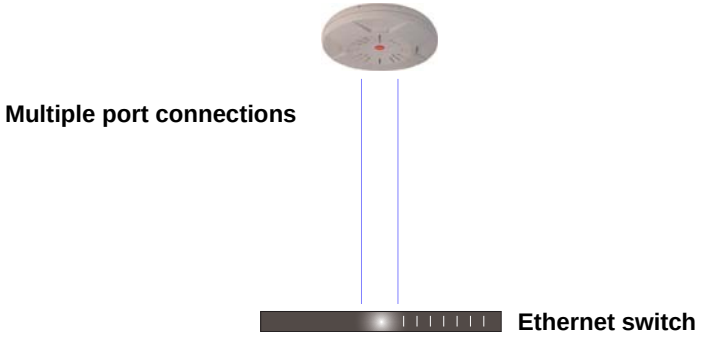


Figure 23. Port Failover Protection

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 "Bonds and Bridging" on page 169.

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 24. 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 12.

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-500/600 Series and some XR-2000 models) also accept IEEE802.3af and/or 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 214 and the Security section of "Frequently Asked Questions" on page 492.

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.

ArrayArrayArray*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 53 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 25. 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.

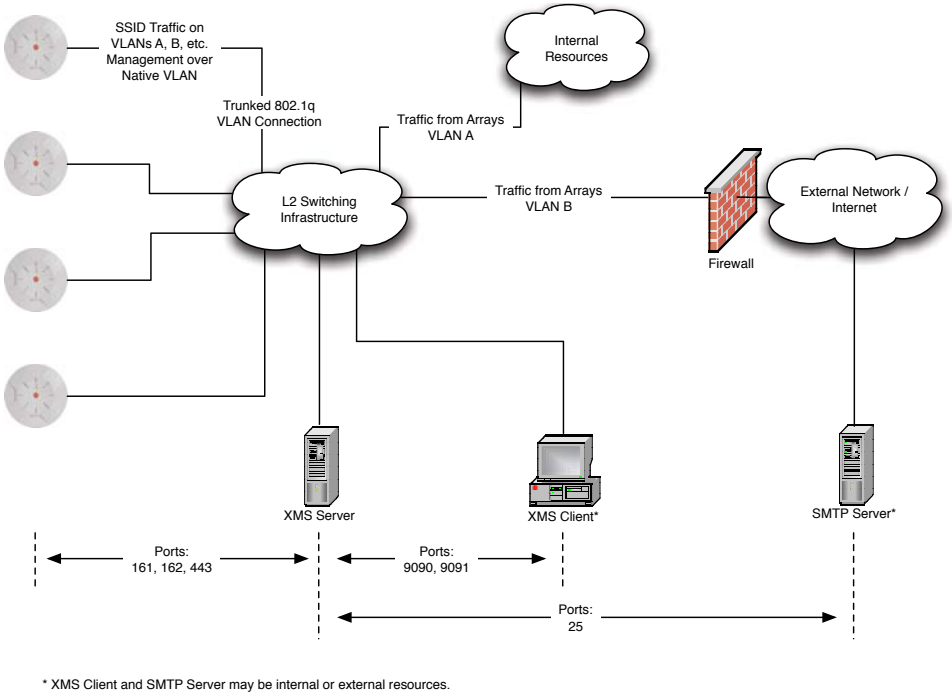


Figure 25. Port Requirements for XMS

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:

- Centralized Web-based management, using the optional Xirrus Management System (XMS). XMS Cloud provides zero-touch provisioning and ongoing management. XMS is run on a dedicated Xirrus appliance or your own server. XMS manages 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
- 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).

See Also

Failover Planning
Power Planning
Security Planning

WDS Planning

WDS (Wireless Distribution System) creates wireless backhaul connections between Arrays, allowing your wireless network to be expanded using multiple Arrays without the need for a wired backbone to link them (see Figure 26). 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 26. WDS Link

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

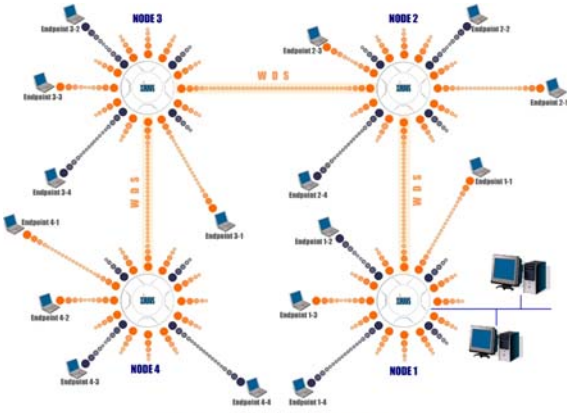


Figure 27. A Multiple Hop WDS Connection

- Multiple WDS links can provide link redundancy (failover capability - see Figure 28). A network protocol (Spanning Tree Protocol—STP) prevents Arrays from forming network loops.

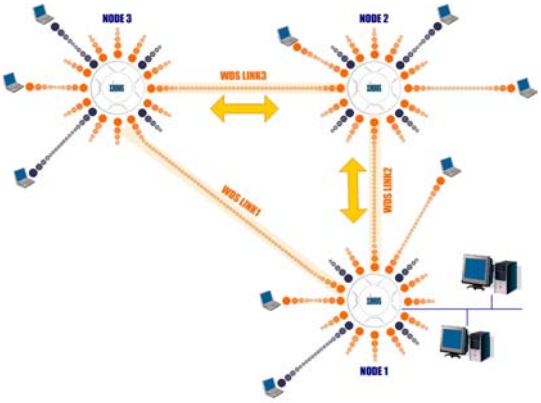


Figure 28. WDS Failover Protection

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 358. 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	Cloud XMS or InternalWMII 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.

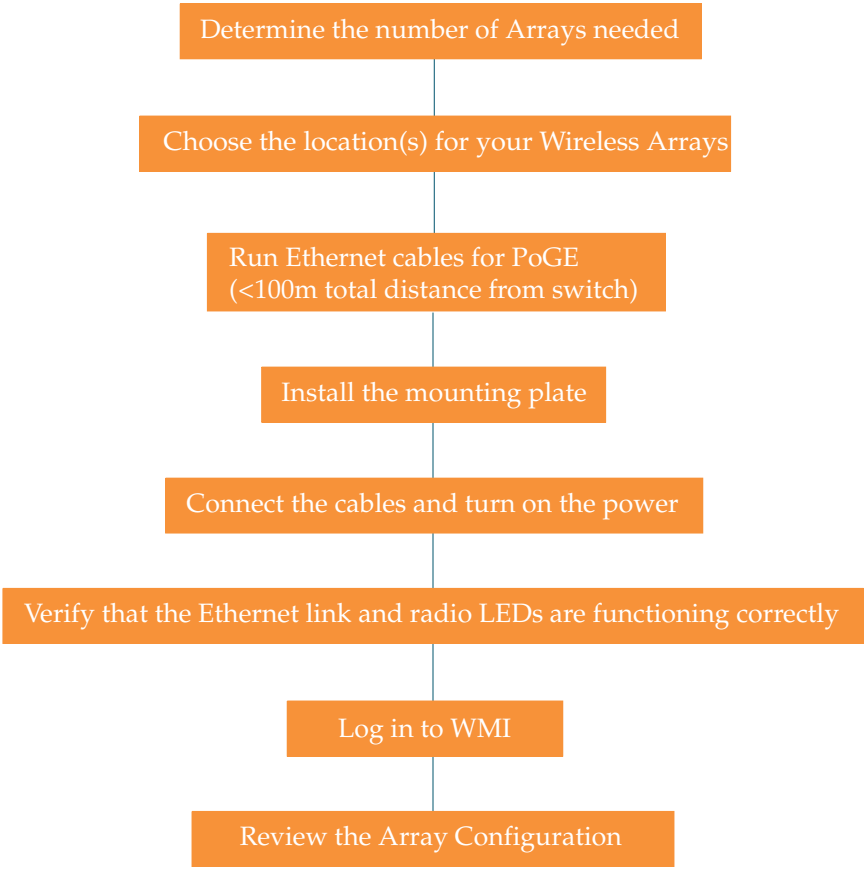


Figure 29. Installation Workflow

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.

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

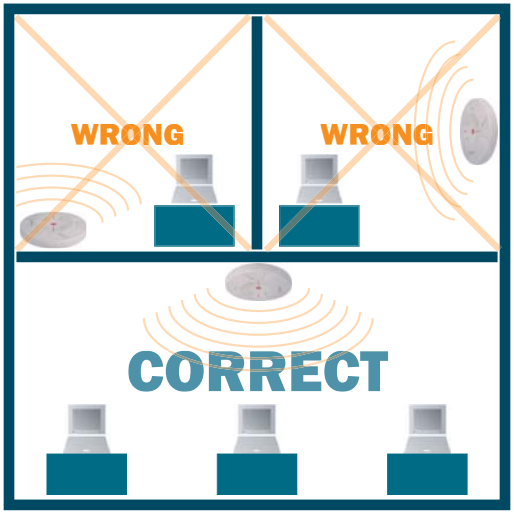


Figure 30. Array Placement

Wiring Considerations

Before using the Xirrus-supplied Power over Gigabit Ethernet modules (PoGE) to distribute power, see "Power over Gigabit Ethernet (PoGE)" on page 12.

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 is required to the Array—Xirrus wireless Arrays and APs use PoGE (Power over Gigabit Ethernet). See the *Quick Installation Guide* for your Array/AP model for compatible power injectors or switches.

The total of all Cat 5e or Cat 6 cable segments from the Gigabit Ethernet switch to the power injector and then to an Array PoGE 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.

Network

Arrays and APs all have at least one PoGE port to supply power and data over the same cable. Many models have additional gigabit ports, or even additional PoGE ports. Please see the *Quick Installation Guide* for your Array/AP model for detailed information about running cables to the Array and connecting it.

Some models also have a serial (console) port. The Serial cable may be up to 25 feet long per the RS-232 specification.

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 theXRR-500,XRR-1000, and someXRR-2000 models, theXirrus Xircon utility may be used locally to set up an IP address if necessary.

Important Note About Network Connections

> ! *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/AP
Power over Gigabit Ethernet (PoGE)

Mounting and Connecting the Array/AP

A detailed *Quick Installation Guide* is available at support.xirrus.com that describes mounting your Array/AP. Please follow the provided instructions carefully. Data and power connections to the Array are also detailed in the *Quick Installation Guide*. Please follow the cabling and connection instructions carefully.

Dismounting the Array

For all Array/AP models, push up on the Array/AP (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.

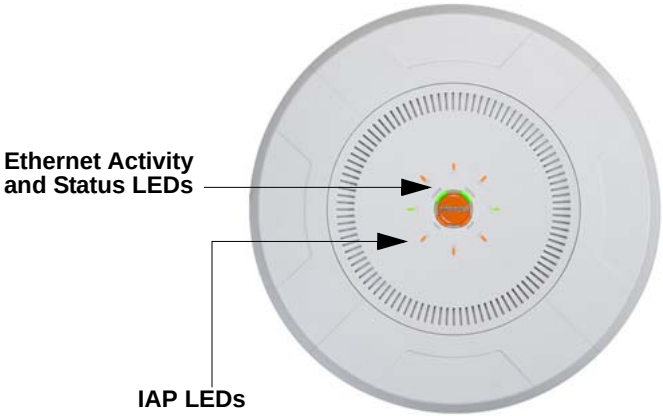


Figure 31. LED Locations

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 354.

Array LED Operating Sequences

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

- **"LED Boot Sequence" on page 67**
- **"LED Operation when Array is Running" on page 68**

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 354.

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 354 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

Zero-Touch Provisioning and Ongoing Management

Most customers employ the Xirrus Management System (XMS) for the initial setup and continuing management of Xirrus devices. XMS users can readily set up their new devices for zero touch provisioning and ongoing maintenance via the following platforms.

XMS Cloud Next Generation (XMS-9500-CL-x)

XMS in the cloud performs zero touch provisioning as shown in this quick video guide: www.xirrus.com/TV/Training/XMS-Cloud-Next-Generation. New Arrays/APs appear in XMS even before you receive your equipment. When the email arrives with your login information, use XMS Cloud to specify the initial settings for your Arrays/APs. A Guided Tour will walk you through the basic steps of creating a profile containing configuration settings, including creating SSIDs and firewall/application control rules. Once a new, unlicensed Array/AP is connected to a network with DHCP and Internet connectivity, it will automatically contact Xirrus for cloud-based zero touch provisioning per your settings. It will first install the latest applicable license, and upgrade the Array/AP to the latest software version as appropriate.

XMS Enterprise

(Also available as a cloud-deployed solution: XMS-9000-CL-x) This enterprise-hosted platform automatically detects and provisions new Xirrus devices deployed in your network via a zero touch provisioning approach similar to that described above. Create and configure a default profile for newly added Arrays/APs—these new devices will automatically receive the configuration defined in your default profile.

If you are an XMS or XMS-9000-CL-x customer, we recommend that you manage your Arrays/APs completely by XMS. Wait five minutes after powering up the Array or Access Point, then use XMS to view/manage this unit. If you change settings directly on the Array/AP, XMS may not sync up with these changes for up to 24 hours.

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

If you are not using XMS

New devices can be auto-provisioned upon initial deployment via the Xirrus Mobilize platform (pre-order required) as shown in this video: www.xirrus.com/TV/Training/Mobilize-Training. Your welcome email will contain login/account information.

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. Note that every unlicensed Array with Internet connectivity obtains its license by contacting Xirrus. 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 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.

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 389.

If you are not using XMS or Mobilize, please proceed to the rest of this chapter to configure your Array/AP manually via the Express Setup menu option.

Array/AP Management Interfaces

User Interfaces (CLI, WMI)

With zero-touch setup provided by XMS and 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-500/600/1000 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. ArrayXMS

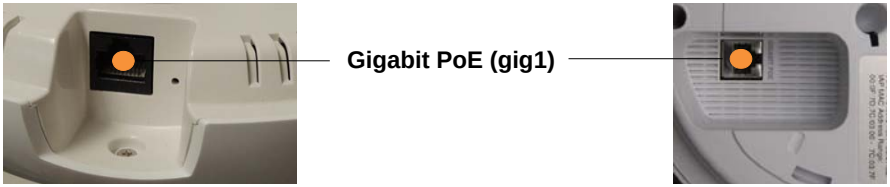


Figure 32. Network Interface Ports—XR-520 (left); XR-1000 Series (right)

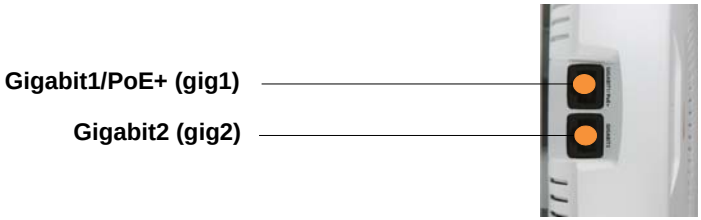


Figure 33. Network Interface Ports—XR-600 Series

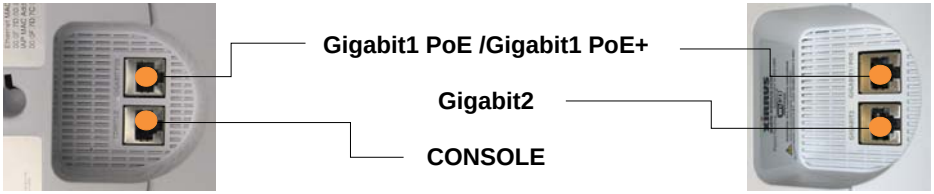


Figure 34. Network Interfaces—XR-2000 Series (left); XR-2005 Series (right)

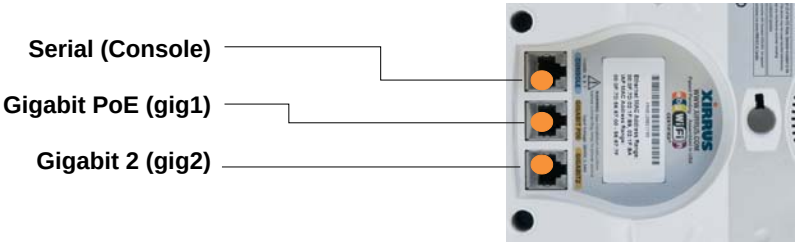


Figure 35. Network Interface Ports—XR-4000 Series

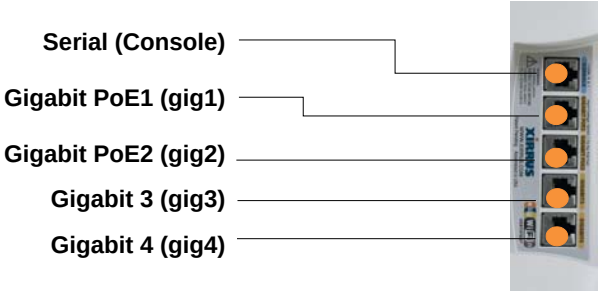


Figure 36. Network Interface Ports—XR-6000 Series

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-500/600/1000 Series and some XR-2000 models, which do not have a console port. See "Securing Low Level Access to the Array" on page 76.

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 "Managing Arrays Locally or via XMS" on page 81).

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, found on the Array label and shipping container (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 00:0F:7D or 50:60:28 and are found on the Array label and shipping container).
3. Alternatively, you may query the Array using the CLI via the console port (on all models except the XR-500/600/1000, 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.

   http://<hostname or IPaddress>

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 from XMS or Mobilize. Any unlicensed Array running ArrayOS release 6.5 or above 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.

1. This procedure assumes that you have pointed a browser to the Array 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 XMS or Mobilize to perform your initial configuration, please see "Express Setup" on page 159. Also see "Zero-Touch Provisioning and Ongoing Management" on page 69.

See Also

Zero-Touch Provisioning and Ongoing Management
Installation Prerequisites
Installation Workflow
Logging In

Multiple SSIDs
Security

Securing Low Level Access to the Array

XirconXBLXRXirconMost local management of the Xirrus Array is done via the Web Management Interface (WMI) or CLI—see "The Command Line Interface" on page 409. 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). XBLXirconXBL

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-500/600/1000 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 73. 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 some 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 399). Skip to Step 4 on page 78.

   To access CLI via SSH, see "Establishing a Secure Shell (SSH) Connection" on page 409. 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 226. 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:

- **Managing Arrays Locally or via XMS**
- **An Overview**
- **Structure of the WMI**
- **User Interface**
- **Logging In**
- **Applying Configuration Changes**

Managing Arrays Locally or via XMS

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. You may change settings directly on the Array/AP—but be aware that XMS may not sync up with these changes for up to 24 hours. All XMS versions automatically "rediscover" the wireless network once a day by default, and XMS will fetch updated settings into its database at that time. If you are an XMS-Cloud customer (XMS-9500-CL-x), you may wish to use WMI or CLI directly on the wireless device to change settings that may not be available in XMS-Cloud.

To immediately sync up XMS with changes that you have made to a particular Array, you may go to the XMS **Monitor > Arrays** or **Configure > Arrays** page. Select the Array, and click the **Refresh** button to update XMS with your changes on an Array. This causes XMS to read the current configuration of the Array and update the XMS database with these values.

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.

Figure 37. Web Management Interface

Structure of the WMI

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

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
  - Bonds and Bridging
  - DNS Settings
  - CDP Settings
- Services
  - Time Settings (NTP)
  - NetFlow
  - Wi-Fi Tag
  - Location
  - System Log
  - SNMP
  - DHCP Server
  - Proxy Forwarding
- VLANs
  - VLAN Management
- Tunnels
  - Tunnel Management
  - SSID Assignments
- Security
  - Admin Management
  - Admin Privileges
  - Admin RADIUS
  - Management Control
  - Access Control List
  - Global Settings
  - External Radius
  - Internal Radius
  - Active Directory
  - Rogue Control List
  - OAuth 2.0 Management
- SSIDs
  - SSID Management
  - Active IAPs
  - Per-SSID Access Control List
  - Honeypots

Configuration Windows (cont'd)
- Groups
  - Group Management
- IAPs
  - IAP Settings
  - Global Settings (IAP)
  - Global Settings .11an
  - Global Settings .11bgn
  - Global Settings .11n
  - Global Settings .11u
  - Global Settings .11ac
  - 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
- Mobile
  - AirWatch

Tool Windows
- System Tools
- CLI
- API Documentation
- Options
- Logout

User Interface

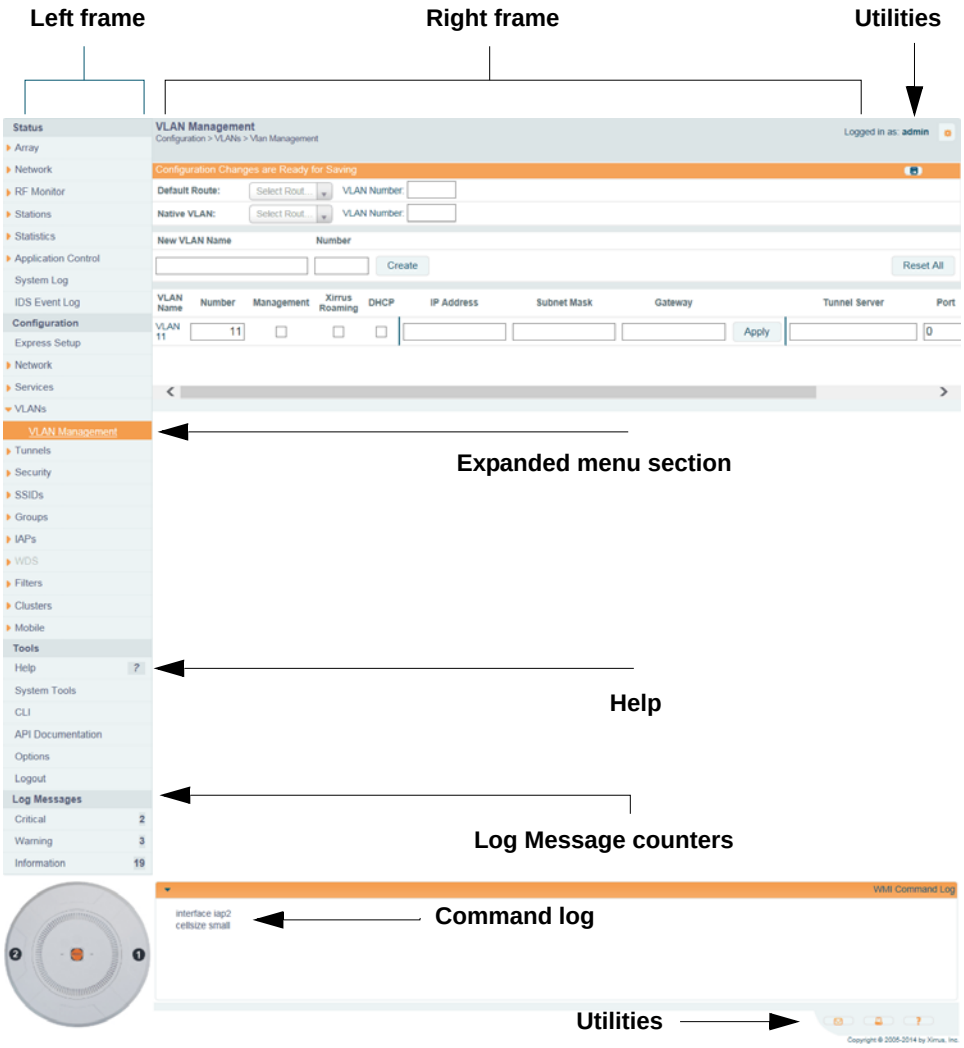


Figure 38. WMI: Frames

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. (Figure 38)

The left frame contains two main elements:

- The menu is organized into three major sections (**Status**, **Configuration**, **Tools**). Each has headings for major functions, such as Network, SSIDs, Security, etc. Click a heading, such as **Network**, to display a page showing a summary of its current configuration, as well as to show links for all of its associated WMI pages.
- 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 153.

The right frame has four main elements:

- The header shows the Array type in the upper right corner, along with the hostname (this defaults to the unit's serial number) an IP address. the Uptime underneath shows the time since the Array was last rebooted.

  Below this is the page title, and the user name you used to log in. On the right, click the Utilities button for a drop-down menu that allows you to **Refresh Page**, **Save** your changes, open the **Help** system, or **Logout**. If you have any unsaved changes, the **Save** button is displayed on the right, in an orange line.

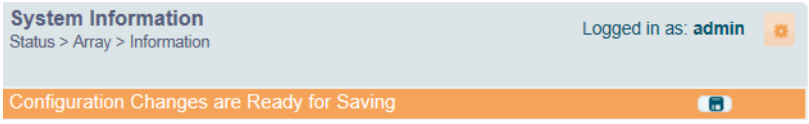


Figure 39. WMI Header

- The main window displays the status information or configuration page that you requested. This is where you review the Array's current status and activity or enter changes if you wish.
- The Command Log shows the results of recent commands.

Figure 40. WMI Command Log

- Utility buttons are located at the bottom right of each window—a **Feedback** button, a **Print** button and a **Help** button.

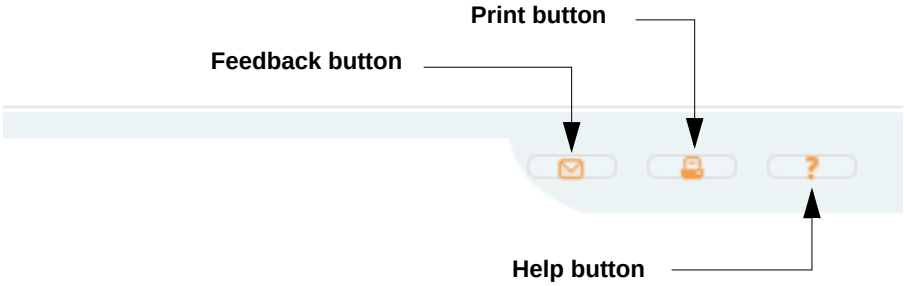


Figure 41. WMI: Utility Buttons

- Click the **Feedback** button to generate a Web page that allows you to submit your comments to Xirrus, Inc.
- Click the **Print** button to open a print dialog to send a copy of the active window to your local printer.
- Click 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.

Some pages or individual 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 387****.*

Note that WMI provides an option that allows you to change its behavior. You may change:

- **Refresh Interval**—the refresh interval, if automatic refresh is selected.

See "Options" on page 406 for more information.

Logging In

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

1. Establish a network connection and open your Web browser.
2. If your network supports DHCP and DNS, enter the Array's default host name in the browser's URL. The default host name is simply the Array's serial number (for example, XR0823091CACD).

   Otherwise, enter the Array's IP address. This may be determined as described in "Using the Ethernet Ports" on page 73.
3. The default login to the Array's Web Management Interface is **admin** for both the user name and password.

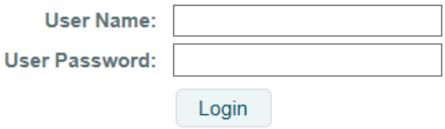


Figure 42. Logging In to the Wireless Array

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

Character Restrictions

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

& < > ' " / \

Viewing Status on the Wireless Array

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

- **"Array Status Windows" on page 92**
- **"Network Status Windows" on page 100**
- **"RF Monitor Windows" on page 111**
- **"Station Status Windows" on page 122**
- **"Statistics Windows" on page 135**
- **"Application Control Windows" on page 146**
- **"System Log Window" on page 153**
- **"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 385**

Note that the **Status** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See Figure 39 on page 86)

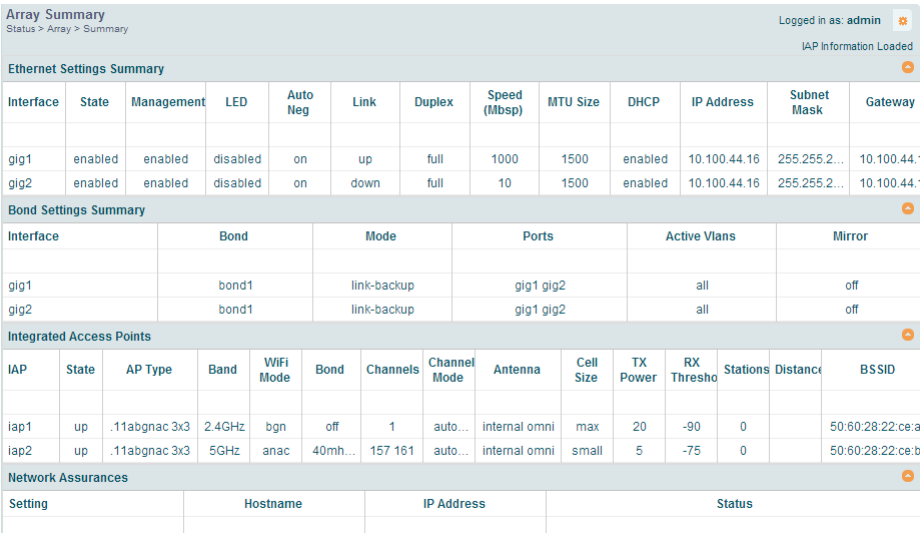
Array Status Windows

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.



Array Summary
Status > Array > Summary

Logged in as: admin
IAP Information Loaded

Ethernet Settings Summary

Interface	State	Management	LED	Auto Neg	Link	Duplex	Speed (Mbsp)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	enabled	enabled	disabled	on	up	full	1000	1500	enabled	10.100.44.16	255.255.2...	10.100.44.
gig2	enabled	enabled	disabled	on	down	full	10	1500	enabled	10.100.44.16	255.255.2...	10.100.44.

Bond Settings Summary

Interface	Bond	Mode	Ports	Active Vlans	Mirror
gig1	bond1	link-backup	gig1 gig2	all	off
gig2	bond1	link-backup	gig1 gig2	all	off

Integrated Access Points

IAP	State	AP Type	Band	WiFi Mode	Bond	Channels	Channel Mode	Antenna	Cell Size	TX Power	RX Thresho	Stations	Distance	BSSID
iap1	up	.11abgnac 3x3	2.4GHz	bgn	off	1	auto...	internal omni	max	20	-90	0		50:60:28:22:ce:a
iap2	up	.11abgnac 3x3	5GHz	anac	40mh...	157 161	auto...	internal omni	small	5	-75	0		50:60:28:22:ce:b

Network Assurances

Setting	Hostname	IP Address	Status

Figure 43. Array Summary

Content of the Array Summary Window

The Array Summary window is sub-divided into the **Ethernet Interfaces** section and the Integrated Access Point (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 166.
  - **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 "Bonds and Bridging" on page 169.
  - **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 "Bonds and Bridging" on page 169 for details
  - **Active VLANs**: Shows the VLANs that are active in this bond.
  - **Mirror**: Shows whether mirroring is enabled on this bond.
- **Integrated Access Point Section**
  This section provides information about the Integrated Access Point (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 290.
  - IAP: Lists the IAPs that are available on the Array.
  - **State**: Shows the current state of each IAP, either up or down. IAPs that are down are shown in RED. Figure 44 shows an example where **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 "Up to Eight Simultaneous Data Streams—Spatial Multiplexing" on page 39.

Integrated Access Points

IAP	State	AP Type	Band	WiFi Mode	Bond	Channels	Channel Mode	Antenna	Cell Size	TX Power	RX Thresho	Stations	Distance	BSSID
iap1	up	.11abgnac 3x3	2.4GHz	bgn	off	1	auto...	internal omni	max	20	-90	0		50:60:28:22:c
iap2	up	.11abgnac 3x3	5GHz	anac	40mhz +1	157 161	auto...	internal omni	small	5	-75	0		50:60:28:22:c

Figure 44. Disabled IAP (Partial View)

- **Channel**: Shows which channel each IAP is using, and the channel setting. To avoid co-channel interference, adjacent radios should not be using adjacent channels. To make channel selections for a specific IAP, go to "IAP Settings" on page 290.
- **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.

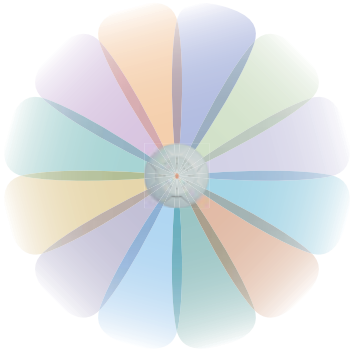


Figure 45. IAP Cells

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 290. 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.XN Arrays can handle up to 96 concurrent users per individual IAP, thus 16-port XN models can handle 1536 users per Array.
- **WDS Link/Distance**: The WDS Link on this radio (if any), and whether the link has been set to support Long Distance Links. See "WDS" on page 358.
- **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 Assurances

Setting	Hostname	IP Address	Status
DNS server 1		10.100.1.10	Connectivity OK
DNS server 2		10.100.2.10	Connectivity OK
SNMP trap host 1	Xirrus-XMS	10.100.44.72	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	Compass Heading
-	-	-1°

Figure 46. 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 226.

- **Operating Status Section**
  This section shows the Array controller board's current internal temperatures, current fan speed, and compass heading. (Figure 46)

See Also

Management Control
Network Interfaces
Bonds and Bridging
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 387 and "Advanced Feature Sets" on page 18 for more information.

System Information
Status > Array > Information

Logged in as: **admin**

Hardware Configuration

Model	XR630, 1.0GB (400MHz)

Component	Part Number	Serial Number	Date
System	XR630	XR073470256F8	2013-Nov-18 11:43
Controller	100-0167-001.A	0000153336	2013-Nov-18 11:43
IAP Module 1	100-0166-001.2	-	-
IAP Module 2	100-0166-001.2	-	-

Interface	MAC Address(es)
IAPs	50:60:28:22:ce:a0-22:ce:bf
Gigabit 1	50:60:28:02:56:f8
Gigabit 2	50:60:28:02:56:f9

Software Configuration

Component	Version
SCD Firmware	5.00 (Oct 1 2012), Build: 4651
Boot Loader	6.3.0 (Jan 10 2014), Build: 6158
IAP Driver	3.1.0 (Jan 30 2014), Build: 3546
System Software	6.7.3 (Jan 31 2014), Build: 4511-beta
DPI Signature File	navl_signatures-6.7.0.tar.gz
License Key	1D04J-D17GJ-9WD51-AHH3J
License Features	ArrayOS 6.7 for 2 3x3 IAPs + RF Performance Manager + RF Analysis Manager + RF Security Manager + Application Control + 802.11ac + 802.11n

Operating Status

Time This Boot	Fri 2014-Jan-31 22:47:27 GMT
Time Last Boot	Tue 2014-Jan-28 01:14:51 GMT

Figure 47. 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.

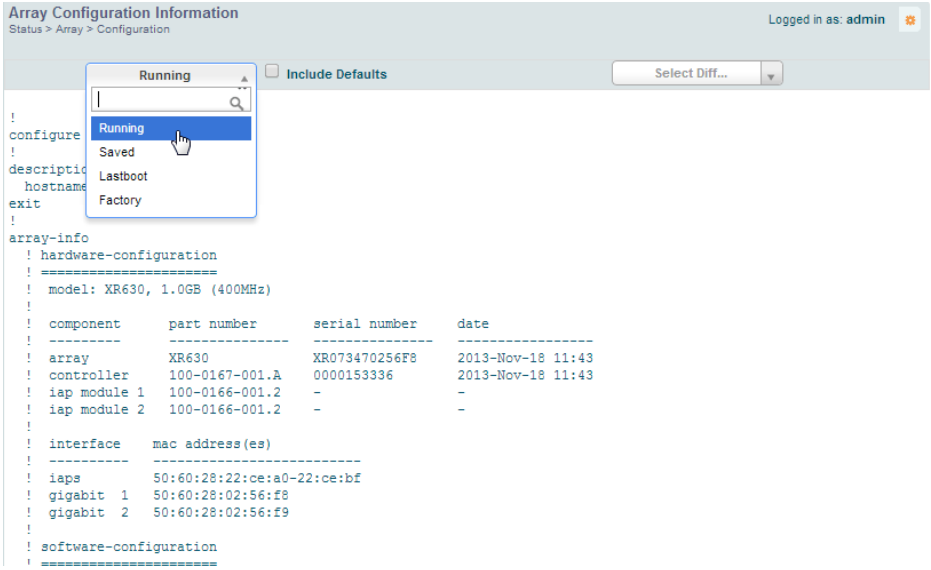


Figure 48. Show Configuration

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.

Administration History
Status > Array > Admin History

Logged in as: admin

Auto Refresh

User	IP Address	Interface	Via	Login Time	Logout Time	Session Time D:H:M
admin	10.100.21.37	WMI	https	Feb-03 18:50	Feb-04 22:37	1:03:47
admin	10.100.21.37	WMI	https	Feb-03 18:50	Feb-04 02:32	0:07:42
admin	10.100.21.37	WMI	https	Feb-04 02:37	current	0:21:09
admin	10.100.21.37	WMI	https	Feb-04 18:31	current	0:05:14
admin	10.100.21.37	WMI	https	Feb-04 18:33	current	0:05:13
admin	10.100.21.37	WMI	https	Feb-04 19:50	current	0:03:55
admin	10.100.21.37	WMI	https	Feb-04 21:14	current	0:02:32
admin	10.100.21.37	WMI	https	Jan-31 22:52	Feb-02 05:53	1:07:00

Figure 49. 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.

Network Settings Summary
Status > Network
Logged in as: admin
Ethernet Information Loaded

Ethernet Settings Summary

Interface	State	Management	LED	Auto Neg	Link	Duplex	Speed (Mbsp)	MTU Size	DHCP	IP Address	Subnet Mask	Gateway
gig1	ena...	enabled	disabled	on	up	full	1000	1500	enabled	10.10...	255.2...	10.100.4.
gig2	ena...	enabled	disabled	on	down	full	10	1500	enabled	10.10...	255.2...	10.100.4.

Bond Settings Summary

Interface	Bond	Mode	Ports	Active Vlans	Mirror
gig1	bond1	link-backup	gig1 gig2	all	off
gig2	bond1	link-backup	gig1 gig2	all	off

DNS Settings Summary

Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3
XR073470256F8	xirrus.com	10.100.1.10	10.100.2.10	

Figure 50. Network Settings

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

- **"Network Interfaces" on page 166**
- **"Bonds and Bridging" on page 169**
- **"DNS Settings" on page 176**

- "CDP Settings" on page 177

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.

Network Map
Status > Network > Network Map

Logged in as: admin

☐ Hardware ☐ License ☑ Software ☐ Firmware ☑ IAP Info ☐ Stations ☑ Default ☐ Auto Refresh

Array Name	IP Address	Location	Array OS	IAP	Up	SSID	On	In Range	Fast Roam	Uptime D:H:M
adrians-xn8-2	10.100.44.37		XS-6.4.4-3886	8	0	1	1	no	off	54:03:57
adrians-xn4-1	10.100.44.74		XS-6.4.4-3886	4	4	2	1	no	tunnel	18:01:18
XR073470256F8	10.100.44.16		XR-6.7.3-4511	2	2	1	0	yes	tunnel	4:01:08
adrians-xr-630	10.100.44.80		XR-6.7.3-4508	2	1	2	1	no	tunnel	8:03:20
XR073470257E2	10.100.44.131		XR-6.7.2-4482	2	1	1	1	no	tunnel	27:01:06
XC402410065A9	10.100.44.57		XR-6.7-vdykhne	8	1	8	8	no	off	0:00:08
XR07347025718	10.100.44.100		XR-6.7-n678d	2	2	4	4	no	tunnel	0:00:13
DBR-XR630	10.100.44.28		XR-6.7-dbrosen	2	1	1	1	no	tunnel	0:00:01
XR4014702915D	10.100.44.34		XR-6.6.2-4264	8	2	1	1	no	off	0:07:18
XR203070EA297	10.100.44.39		XR-6.6.2-4264	4	2	1	1	no	off	0:07:18
XR103390EEF50	10.100.44.56		XR-6.6.2-4264	2	2	1	1	no	off	0:07:17
XR103180EC2F1	10.100.44.60		XR-6.6.2-4264	2	2	1	1	no	off	0:07:16
XR502490001A9	10.100.44.68		XR-6.6.0-4243	2	1	2	1	no	tunnel	0:05:34
adrians-xr-1	10.100.44.70		XR-6.6.0-4243	8	0	2	1	no	tunnel	4:04:20

Figure 51. 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 290.
- **SSID**: Informs you how many SSIDs have been assigned for the Array. To assign an SSID, go to "SSID Management" on page 262.
- **(SSID) On**: Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to "SSID Management" on page 262.
- **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 295.
- **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 de-authenticate 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.

				WDS Client Links				WDS Host Links			
VLAN Name	Number	Gigabit 1	Gigabit 2	1	2	3	4	1	2	3	4
none		forwarding	forwarding	forwarding							
VLAN 11	11	forwarding	forwarding	forwarding							

Figure 52. Spanning Tree Status

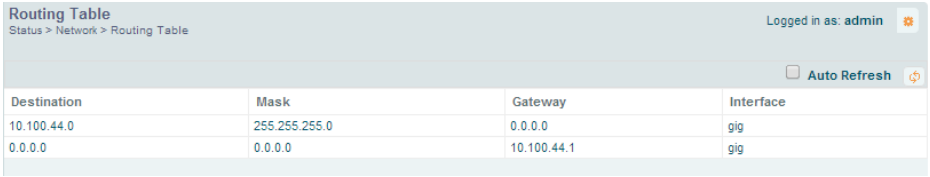
This window shows the spanning tree status (forwarding or blocked) for path segments that terminate on the gigabit ports and WDS links of this Array. You may sort the rows based on the **VLAN Name** or **Number** columns by clicking the column header. Click **Refresh** to update the information at any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



Destination	Mask	Gateway	Interface
10.100.44.0	255.255.255.0	0.0.0.0	gig
0.0.0.0	0.0.0.0	10.100.44.1	gig

Figure 53. Routing Table

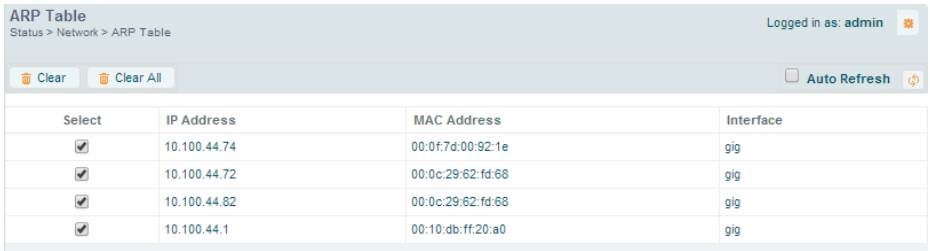
See Also

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.



Select	IP Address	MAC Address	Interface
✓	10.100.44.74	00:0f:7d:00:92:1e	gig
✓	10.100.44.72	00:0c:29:62:fd:68	gig
✓	10.100.44.82	00:0c:29:62:fd:68	gig
✓	10.100.44.1	00:10:db:ff:20:a0	gig

Figure 54. 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.

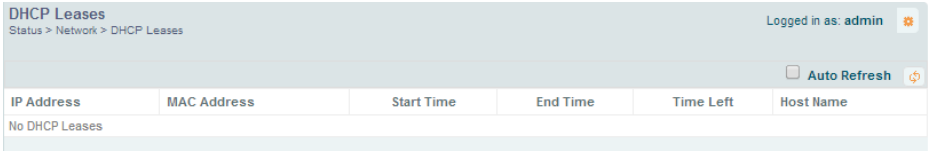


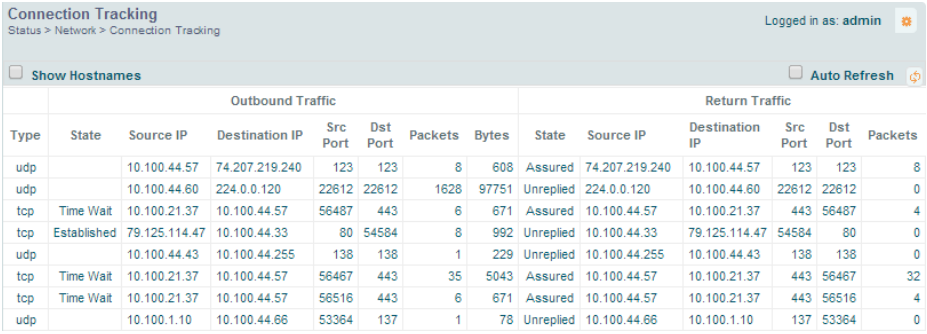
Figure 55. DHCP Leases

See Also

DHCP Server

Connection Tracking/NAT

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



	Outbound Traffic							Return Traffic					
Type	State	Source IP	Destination IP	Src Port	Dst Port	Packets	Bytes	State	Source IP	Destination IP	Src Port	Dst Port	Packets
udp		10.100.44.57	74.207.219.240	123	123	8	608	Assured	74.207.219.240	10.100.44.57	123	123	8
udp		10.100.44.60	224.0.0.120	22612	22612	1628	97751	Unreplied	224.0.0.120	10.100.44.60	22612	22612	0
tcp	Time Wait	10.100.21.37	10.100.44.57	56487	443	6	671	Assured	10.100.44.57	10.100.21.37	443	56487	4
tcp	Established	79.125.114.47	10.100.44.33	80	54584	8	992	Unreplied	10.100.44.33	79.125.114.47	54584	80	0
udp		10.100.44.43	10.100.44.255	138	138	1	229	Unreplied	10.100.44.255	10.100.44.43	138	138	0
tcp	Time Wait	10.100.21.37	10.100.44.57	56467	443	35	5043	Assured	10.100.44.57	10.100.21.37	443	56467	32
tcp	Time Wait	10.100.21.37	10.100.44.57	56516	443	6	671	Assured	10.100.44.57	10.100.21.37	443	56516	4
udp		10.100.1.10	10.100.44.66	53364	137	1	78	Unreplied	10.100.44.66	10.100.1.10	137	53364	0

Figure 56. 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.

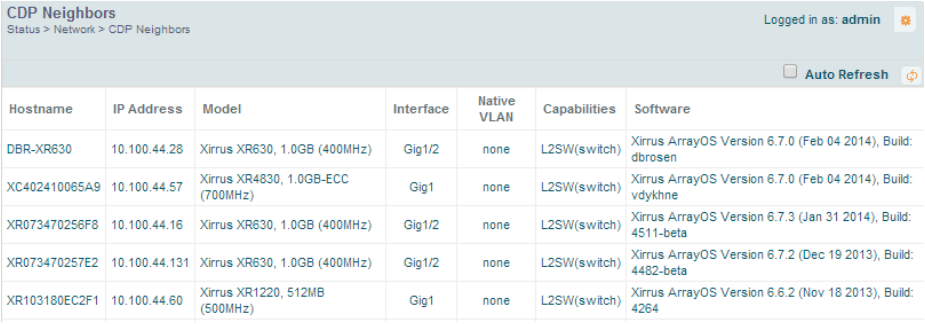
You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon. Click **Refresh** to update the information at any time. Click **Auto Refresh** to instruct the Array to refresh this window automatically.

See Also

Filters

CDP Neighbors

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



CDP Neighbors
Status > Network > CDP Neighbors

Logged in as: admin

Auto Refresh

Hostname	IP Address	Model	Interface	Native VLAN	Capabilities	Software
DBR-XR630	10.100.44.28	Xirrus XR630, 1.0GB (400MHz)	Gig1/2	none	L2SW(switch)	Xirrus ArrayOS Version 6.7.0 (Feb 04 2014), Build: dbrosen
XC402410065A9	10.100.44.57	Xirrus XR4830, 1.0GB-ECC (700MHz)	Gig1	none	L2SW(switch)	Xirrus ArrayOS Version 6.7.0 (Feb 04 2014), Build: vdykhne
XR073470256F8	10.100.44.16	Xirrus XR630, 1.0GB (400MHz)	Gig1/2	none	L2SW(switch)	Xirrus ArrayOS Version 6.7.3 (Jan 31 2014), Build: 4511-beta
XR073470257E2	10.100.44.131	Xirrus XR630, 1.0GB (400MHz)	Gig1/2	none	L2SW(switch)	Xirrus ArrayOS Version 6.7.2 (Dec 19 2013), Build: 4482-beta
XR103180EC2F1	10.100.44.60	Xirrus XR1220, 512MB (500MHz)	Gig1	none	L2SW(switch)	Xirrus ArrayOS Version 6.6.2 (Nov 18 2013), Build: 4264

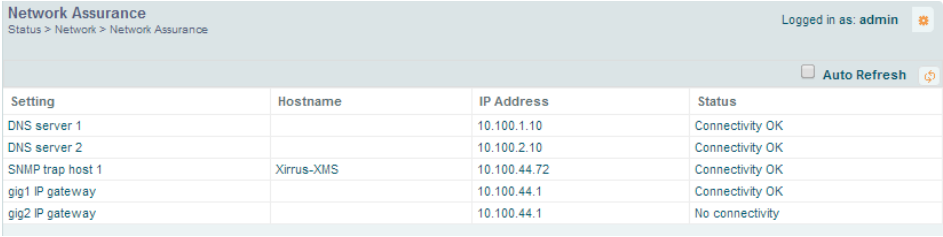
Figure 57. CDP Neighbors

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 177.

Network Assurance

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



Setting	Hostname	IP Address	Status
DNS server 1		10.100.1.10	Connectivity OK
DNS server 2		10.100.2.10	Connectivity OK
SNMP trap host 1	Xirrus-XMS	10.100.44.72	Connectivity OK
gig1 IP gateway		10.100.44.1	Connectivity OK
gig2 IP gateway		10.100.44.1	No connectivity

Figure 58. 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 226.

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 204.

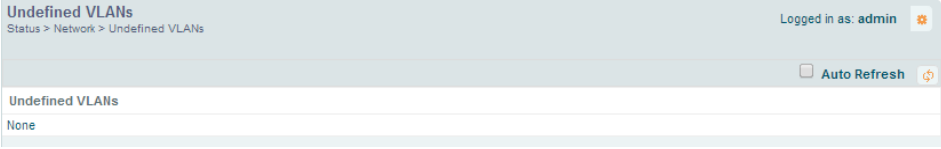


Figure 59. Undefined VLANs

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 300).

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.

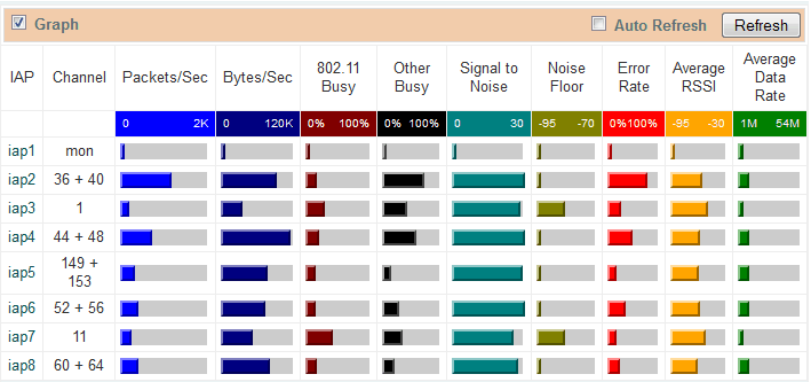
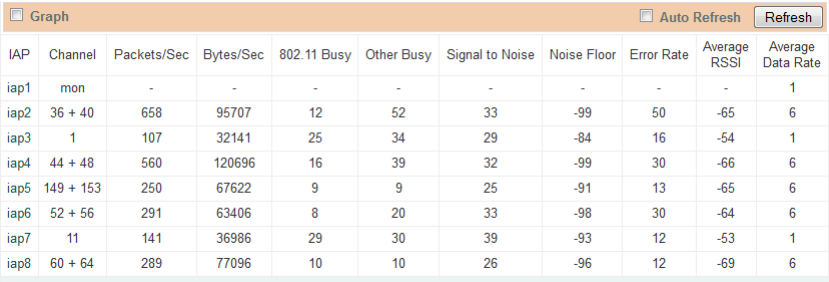


Figure 60. RF Monitor—IAPs

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



Graph | Auto Refresh | Refresh

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 61. RF Monitor—IAPs

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

Spectrum Analyzer

*The RF measurements for this feature are obtained by the monitor radio. You **must** have a radio set to **monitor** mode for any data to be available. See "IAP Settings" on page 290.*

Spectrum Analysis is not available for Arrays or Access Points featuring 802.11ac IAPs.

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

The RF Spectrum Analyzer window displays instantaneous traffic statistics and RF readings for all channels, as measured by the Array's monitor radio. This differs from the RF Monitor-IAPs window, which displays values measured by each IAP radio for its current assigned channel. For the spectrum analyzer, the monitor radio is in a listen-only mode, scanning across all wireless channels. Each channel is scanned in sequence, for a 250 millisecond interval per channel. The spectrum analyzer window presents the data as a graphical display of vertical bar graphs for each statistic as shown in Figure 62 (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in "Spectrum Analyzer Measurements" on page 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.

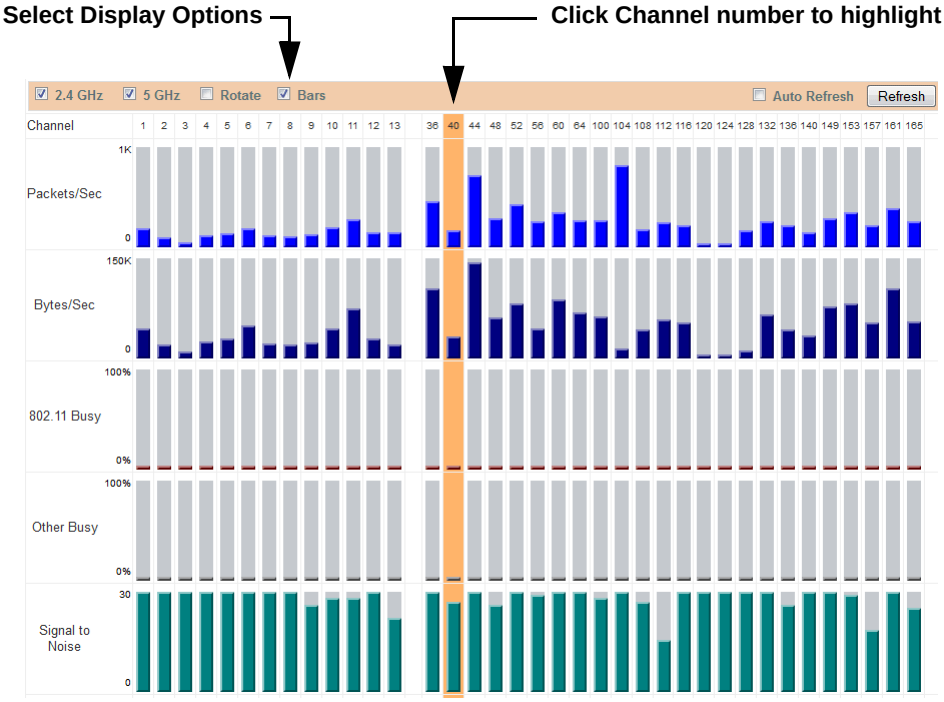


Figure 62. RF Spectrum Analyzer

The Spectrum Analyzer offers several display options:

- To display horizontal bar graphs, click the **Rotate** checkbox at the bottom of the data window.
- In the rotated view, if you wish to view data as a numerical table, click the **Text** checkbox. Click again to return to a graphical display. The text option is only available in the rotated view.
- When viewing a graphical display, click **Bars** to have the bar graphs displayed against a gray background—you may find this easier on the eyes. This operation is not available when Text is selected.

- You may sort the rows based on any column that has an active column header, indicated when the mouse pointer changes to the hand icon. Sorting is only available in the rotated view.
- At the bottom left of the frame, you may select whether to display only 2.4 GHz channels, 5 GHz channels, or both (the default is both). Note that the data is an instantaneous snapshot—it is not an average or a cumulative total.

Spectrum Analyzer Measurements

The spectrum analyzer displays the following information:

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

  The total busy time (802.11 Busy plus Other Busy) will never total more than 100%. The remaining time (100% minus total busy time) is quiet time—the time that no activity was seen on the channel.
- **Signal to Noise:** Average SNR (signal to noise ratio) seen on the channel, calculated from the signal seen on valid 802.11 packets less the noise floor level. A dash value "-"means no SNR data was available for the interval.
- **Noise Floor:** Average noise floor reading seen on the channel (ambient noise). A dash value "-"means no noise data was available for the interval.
- **Error Rate:** Percentage of the total number of wireless packets seen on the channel that have CRC errors. The Error rate percentage may be high on some channels since the monitor radio is set to receive at a very sensitive level, enabling it to hear packets from devices at far distances.

- **Average RSSI:** Average RSSI level seen on 802.11 packets received on the channel. A dash value "-"means no RSSI data was available for the interval.
- **Average Data Rate:** Average data rate over time (per byte, not per packet) seen on 802.11 packets received on the channel. A dash value "-"means no data rate information was available for the interval. A higher 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 351.

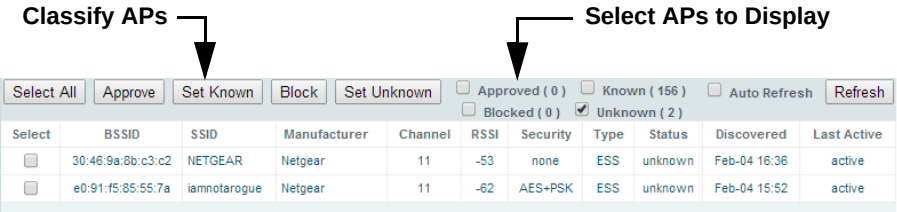


Figure 63. Intrusion Detection/Rogue AP List

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

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

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

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

See Also

Network Map
Rogue Control List
SSIDs
SSID Management

Channel History

Channel History is not available for Arrays or Access Points featuring 802.11ac IAPs.

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.

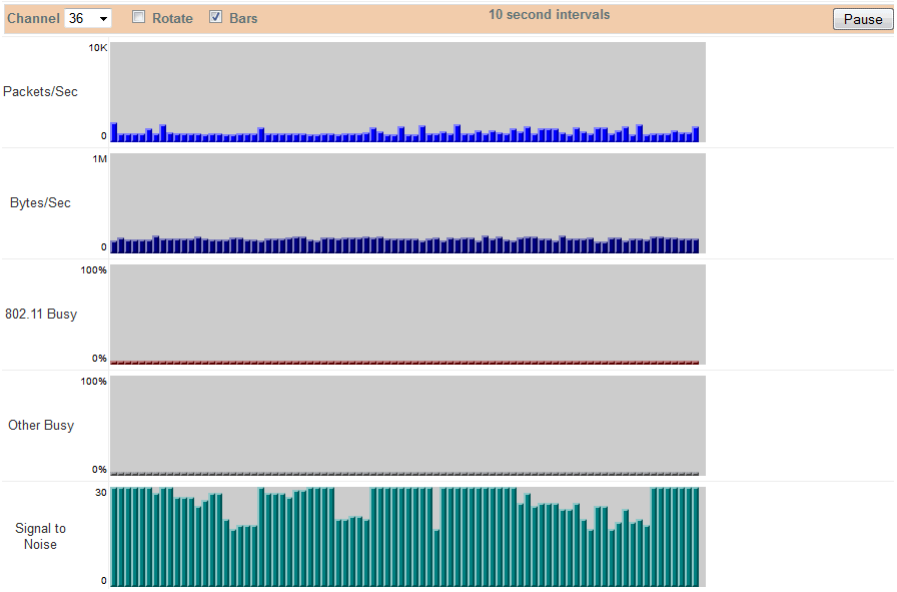


Figure 64. RF Monitor—Channel History

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

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

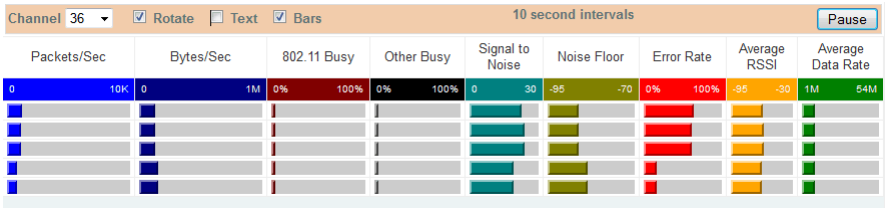
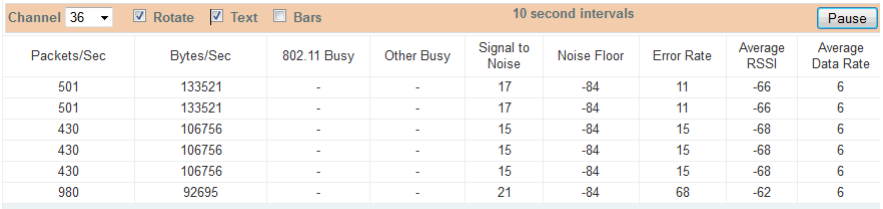


Figure 65. RF Monitor—Channel History (Rotated)

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

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



Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate
501	133521	-	-	17	-84	11	-66	6
501	133521	-	-	17	-84	11	-66	6
430	106756	-	-	15	-84	15	-68	6
430	106756	-	-	15	-84	15	-68	6
430	106756	-	-	15	-84	15	-68	6
980	92695	-	-	21	-84	68	-62	6

Figure 66. 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 335. 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 501.

					IAP Reset Counts by Type				
IAP	State	AP Type	Channel	WiFi Mode	Monitor	Beacon	Phy	MAC	System
iap1	up	.11abgnac 2x2	11	bgn	0	0	0	0	0
iap2	up	.11abgnac 2x2	52	an	0	0	0	0	0

Figure 67. Radio Assurance

For each of the Array's radios, this window shows the radio's state, its type (IEEE 802.11 type, and antenna type—2x2 or 3x3), the assigned channel, and the selected 802.11 wireless mode. To the right, the table shows counts for the number of times, if any, that radio assurance has performed each of the following types of resets since the last reboot, as described in Radio Assurance:

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

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.

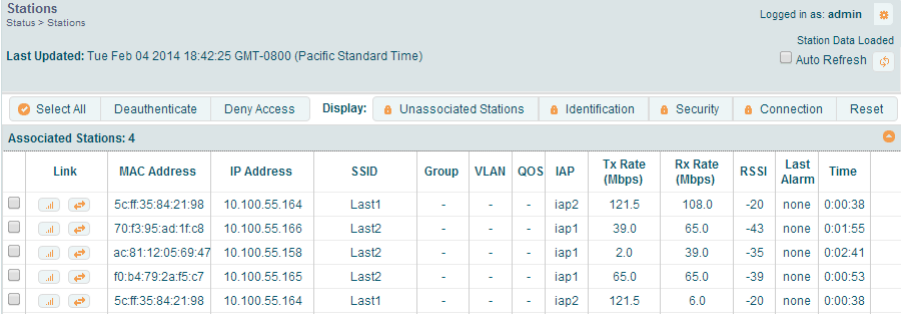
Stations

This window shows client stations currently visible to the Array. You may choose to view only stations that have **Associated** to the Array, or include stations that are **Unassociated** by selecting the appropriate buttons 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).

In the Link column, click the details button to jump to a detailed statistics page for this station. Click to see Application Control information.

You may click other buttons 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—**Encryption** type, **Cipher** used, and Key **Management** used by the station.
- **Connection Info**: shows the **Band** (5GHz or 2.4 GHz) used. Shows an additional RF measurement that affects the quality of the connection: **SNR** (signal to noise ratio).
- **Reset**: click this button to return the display to showing just the default columns.



Link	MAC Address	IP Address	SSID	Group	VLAN	QOS	IAP	Tx Rate (Mbps)	Rx Rate (Mbps)	RSSI	Last Alarm	Time
	5c:ff:35:84:21:98	10.100.55.164	Last1	-	-	-	iap2	121.5	108.0	-20	none	0:00:38
	70:f3:95:ad:1f:c8	10.100.55.166	Last2	-	-	-	iap1	39.0	65.0	-43	none	0:01:55
	ac:81:12:05:69:47	10.100.55.158	Last2	-	-	-	iap1	2.0	39.0	-35	none	0:02:41
	f0:b4:79:2a:f5:c7	10.100.55.165	Last2	-	-	-	iap1	65.0	65.0	-39	none	0:00:53
	5c:ff:35:84:21:98	10.100.55.164	Last1	-	-	-	iap2	121.5	6.0	-20	none	0:00:38

Figure 68. Stations

You may sort the rows based on any column that has an active column header. Click again to reverse the sort order. You may select one or more specific stations 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 234 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
Station Statistics

Location Map

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

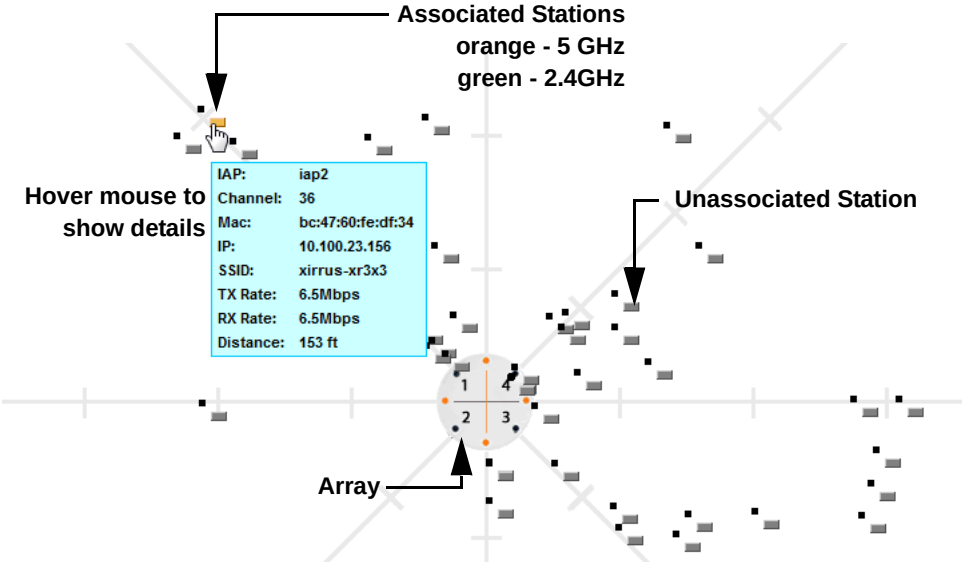


Figure 69. Location Map

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

A station is identified by the type of **Preferred Label** that you select: **Netbios Name**, **IP Address**, **MAC Address**, or **Manufacturer**. If multiple stations are near each other, they will be displayed slightly offset so that one station does not

completely obscure another. You may minimize a station that is not of interest by clicking it. There is also a **Minimize All** button.

You may replace the range-finder background image above with your own custom image of the floor plan 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 69) For a station that is associated to this Array, the details include:

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

Controls and items displayed on the Location Map window

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

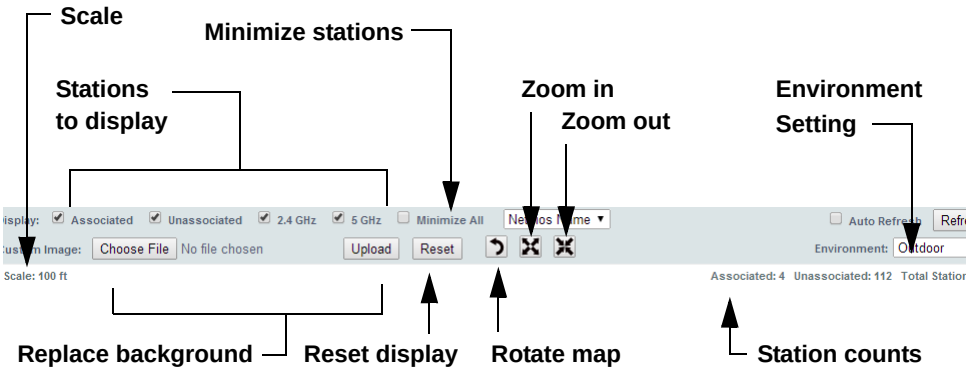


Figure 70. Controls for Location Map

- **Display Associated/Unassociated**: Select whether to display stations that are associated to the Array, stations that are not associated, or both.
- **Display 2.4 GHz/5 GHz**: Select whether to display 802.11bgn 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 hash mark 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.

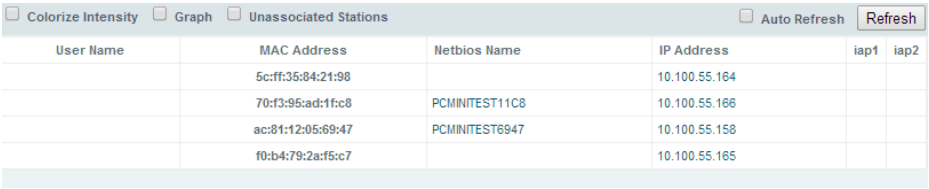


Figure 71. Station RSSI Values

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

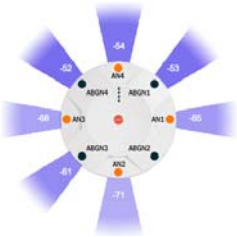


Figure 72. Station RSSI Values—Colorized Graphical View

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.

Colorize Intensity Graph Unassociated Stations Auto Refresh Refresh

User Name	MAC Address	Netbios Name	IP Address	iap1	iap2
	5c:ff:35:84:21:98		10.100.55.164		
	70:f3:95:ad:1f:c8	PCMINITEST11C8	10.100.55.166		
	ac:81:12:05:69:47	PCMINITEST6947	10.100.55.158		
	f0:b4:79:2a:f5:c7		10.100.55.165		

Figure 73. 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 73) You may display the relative value using color if you select **Colorize Intensity**, with the highest SNR indicated by the most intense color. (Figure 74) 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.

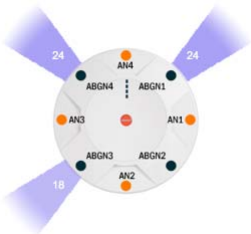


Figure 74. Station SNR Values—Colorized Graphical View

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.

☑ Colorize Intensity ☐ Graph ☐ Unassociated Stations ☐ Auto Refresh Refresh

Noise Floor (-35 to -100)

User Name	MAC Address	Netbios Name	IP Address	iap1	iap2	iap3	iap4	iap5	iap6	iap7	iap8
XIRRUS\Patrick.Parker	00:14:d1:cf:f0:f5		10.100.25.33								
XIRRUS\jeff.plowman	00:21:5c:23:10:f9	JPLOWMAN-6910P	10.100.25.69					■		■	
	00:24:d7:77:0f:d4	XMS-SQA-5	10.100.14.105								
XIRRUS\David.Levin	00:24:d7:bf:a5:48		10.100.25.29	■		■		■		■	
David.Levin	e0:f8:47:21:7e:5a	MACBOOKPRO-77D7	10.100.25.47								

Figure 75. 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 75) 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 76) The stations are listed to the left of the Array—click on a station to show its values on the Array.

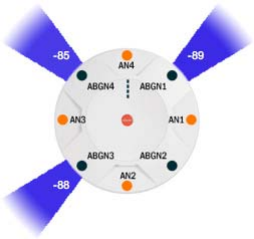


Figure 76. Station Noise Floor Values—Colorized Graphical View

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.

Auto Refresh Refresh

					Max station count				
IAP	State	Channel		Current Stations	Hour	Day	Week	Month	Year
iap1		11	automatic	3	3	3	3	3	3
iap2		52+56	manual	1	1	1	1	1	1

Figure 77. 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 340 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 340: associated time, authentication failures, packet error rate, packet retry rate, packet data rate, RSSI, signal to noise ratio (SNR), and distance.

Figure 78. 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 136. 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.

Unicast Stats Only Auto Refresh Refresh Clear

Statistics for IAP All

		Receive Statistics by IAP				Transmit Statistics by IAP			
IAP	Channel	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
iap1		1555981246	165067186	161215208	205554	64511516	277045	12888	12852
iap2		2167877730	188101159	182055641	392481	71314092	288703	18463	18463

Figure 79. 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. Scroll the window down to see a breakout of the statistics by connection rate. For a summary of statistics for all IAPs, see "IAP Statistics Summary" on page 135. 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.

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.

Display Percentages | Auto Refresh | Refresh | Clear

Statistics for IAP iap1

Receive Statistics		Transmit Statistics	
Total Bytes	1586982283	Total Bytes	65603844
Total Packets	3713991	Total Packets	255910
Unicasts	1140195	Unicasts	20982
Multicasts	0	Multicasts	41402
Broadcasts	292960	Broadcasts	22242
Mgmt Packets	3681260	Mgmt Packets	202043
Beacons	2280836	Beacons	171284
Fragments	0	Fragments	0
RTS Count	0	RTS Count	0
CTS Count	0	CTS Count	0
Receive Errors & Retries		**Transmit Errors & Retries**	
Total Errors	163475838	Total Errors	26134
Total Retries	209347	Total Retries	13049
Dropped Packets	5658920	Dropped	13049
Unassociated	2	Unassociated	35
CRC	157607569	ACK Failures	1
Fragment Errors	0	RTS Failures	0
Encryption Errors	0	RTS Retries	0
Duplicates	0	Single Retries	0
Overruns	0	Multiple Retries	13049

	Receive Statistics by Rate				Transmit Statistics by Rate			
Rate	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
802.11b CCK Rates								
1	859054437	2933287	0	209219	52362	430	0	0
2	0	0	0	0	953102	1841	0	0
5.5	27	1	0	1	0	0	0	0
802.11ag OFDM Rates								
6	18170087	65688	0	127	53097960	171284	0	0
12	3927	23	0	0	0	0	0	0
48	0	0	0	0	228	3	0	0
802.11n 20Mhz Channel, Normal Guard Interval, 1 Spatial Stream Rates								
6.5	368	5	0	0	7178	56	0	0
13.0	816	3	0	0	60597	225	0	0
19.5	15656	101	0	0	20286	139	0	0
26.0	45408	320	0	0	44204	298	0	0
39.0	149038	1050	0	0	194078	1078	0	0
52.0	228190	1149	0	0	93592	598	0	0
58.5	109758	703	0	0	47957	468	0	0

Figure 80. 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

Clear All Auto Refresh Refresh

Gigabit Ethernet 1 Statistics			up, link up, 1000, full duplex
Receive Bytes	87042992	Transmit Bytes	81393195
Receive Packets	460104	Transmit Packets	263877
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	52999	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0
Gigabit Ethernet 2 Statistics			**up, link down, 10, half duplex**
Receive Bytes	0	Transmit Bytes	0
Receive Packets	0	Transmit Packets	0
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	0	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

Figure 81. 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.

Clear All | Auto Refresh | Refresh

printers (3) Statistics			Clear
Receive Bytes	24946298	Transmit Bytes	9529416
Receive Packets	368048	Transmit Packets	183258
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	260683	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	1096572
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

mgmt (10) Statistics			Clear
Receive Bytes	5537500029	Transmit Bytes	1383540307
Receive Packets	8197202	Transmit Packets	6566388
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	810613	Transmit Carrier Errors	0
Receive Dropped	107	Transmit Dropped	0
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

guest (14) Statistics			Clear
Receive Bytes	971081595	Transmit Bytes	87308504
Receive Packets	1016860	Transmit Packets	861470
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	12044	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	629950
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

corp (25) Statistics			Clear
Receive Bytes	3971362218	Transmit Bytes	813741261
Receive Packets	5079835	Transmit Packets	4182676
Receive Compressed	0	Transmit Compressed	0
Receive Multicast	137008	Transmit Carrier Errors	0
Receive Dropped	0	Transmit Dropped	2744968
Receive FIFO Errors	0	Transmit FIFO Errors	0
Receive Frame Errors	0	Transmit Collisions	0
Receive Total Errors	0	Transmit Total Errors	0

Figure 82. 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).

Clear | Auto Refresh | Refresh

WDS Statistics Summary

	Receive Statistics				Transmit Statistics			
Client Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
	Receive Statistics				Transmit Statistics			
Host Link	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0

Figure 83. 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.

Note that you must have **Intrusion Detection Mode** enabled to collect IDS statistics. See "Intrusion Detection" on page 348. Information about IDS events is discussed in the "IDS Event Log Window" on page 155.

Last Updated: Tue Feb 04 2014 19:53:12 GMT-0800 (Pacific Standard Time) Auto Refresh

IDS Statistics

Filter IAP Equal To Filter Reset

IAP	Packet/Event	Count						Average					
		1 min	5 min	10 min	20 min	30 min	60 min	1 min	5 min	10 min	20 min	30 min	60 min
iap1	beacon	8381	41748	81551	159515	244305	483492	8381	8349	8155	7975	8143	8058
iap1	probeReq	561	2715	5292	10483	16269	33510	561	543	529	524	542	558
iap1	auth	0	0	0	0	0	0	0	0	0	0	0	0
iap1	assoc	0	0	0	0	0	0	0	0	0	0	0	0
iap1	disassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap1	deauth	0	0	0	0	0	0	0	0	0	0	0	0
iap1	eap	0	0	0	0	0	0	0	0	0	0	0	0
iap1	micError	0	0	0	0	0	0	0	0	0	0	0	0
iap1	spoofedBeacon	0	0	0	0	0	0	0	0	0	0	0	0
iap1	spoofedDisassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap1	spoofedDeauth	0	0	0	0	0	0	0	0	0	0	0	0
iap1	seqNumAnomaly	0	0	0	0	0	0	0	0	0	0	0	0
iap2	beacon	11202	57402	115932	225745	337295	669645	11202	11480	11593	11287	11243	11160
iap2	probeReq	983	5087	10116	20238	30140	60795	983	1017	1011	1011	1004	1013
iap2	auth	0	0	0	0	0	0	0	0	0	0	0	0
iap2	assoc	0	0	0	0	0	0	0	0	0	0	0	0
iap2	disassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap2	deauth	0	0	0	0	0	0	0	0	0	0	0	0
iap2	eap	0	0	0	0	0	0	0	0	0	0	0	0
iap2	micError	0	0	0	0	0	0	0	0	0	0	0	0

Figure 84. IDS Statistics Page

Use the filter feature to show only information for a selected IAP or for selected event types. Select the type of **Filter**: IAP to select IAPs, or **Packet/Event** to select particular attack types. Select the type of string matching, for example, **Begins with** or **Contains**. Then enter the string to be matched and click the **Filter** button.

For example, in Figure 85, the filter **Packet/Event Contains assoc** finds events that include the string **assoc** in any position. If you have an Array with 12 IAPs, then IAP **Contains 1** will show entries for iap**1**, iap**10**, iap**11**, and iap**12**. Click the **Reset** button to return to showing all entries.

IDS Statistics

Filter Packet/Event ▾ Contains ▾ assoc Filter Reset

IAP	Packet/Event	Count						Average					
		1 min	5 min	10 min	20 min	30 min	60 min	1 min	5 min	10 min	20 min	30 min	60 min
iap2	spoofedDisassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap2	disassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap2	assoc	0	0	0	0	0	0	0	0	0	0	0	0
iap1	spoofedDisassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap1	disassoc	0	0	0	0	0	0	0	0	0	0	0	0
iap1	assoc	0	0	0	0	0	0	0	0	0	0	0	0

Figure 85. Filtered IDS Statistics

Many of the column headers may be clicked to sort the entries in ascending or descending order based on that column. You can **Refresh** the data (update the window with the latest information) at any time by clicking the **Refresh** button on the upper right. 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.

Detail Auto Refresh Refresh Clear All

Name	Type	State	Packets	Bytes
Global				
No filters defined				
Last3				
fks1	deny	on	0	0
PDA				
Block Firewall 1	deny	off	0	0
Block All Proxy Apps	deny	on	0	0
group-111				
Block Firewall 1	deny	off	0	0

Figure 86. Filter Statistics

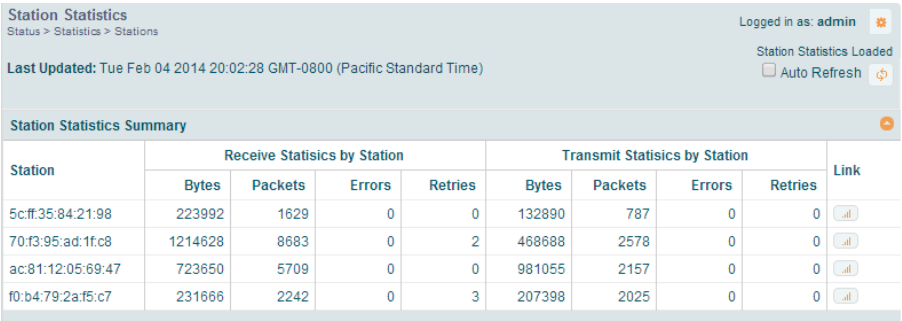
See Also

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 or click the details button in the station's **Link** column, and see "Per-Station Statistics" on page 145.



Station	Receive Statisics by Station				Transmit Statisics by Station				Link
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries	
5c:ff:35:84:21:98	223992	1629	0	0	132890	787	0	0	
70:f3:95:ad:1f:c8	1214628	8683	0	2	468688	2578	0	0	
ac:81:12:05:69:47	723650	5709	0	0	981055	2157	0	0	
f0:b4:79:2a:f5:c7	231666	2242	0	3	207398	2025	0	0	

Figure 87. Station Statistics

Click on a column header to sort the rows based on that column. You can **Refresh** the data (update the window with the latest information) at any time by clicking the refresh button . You can also click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

See Also

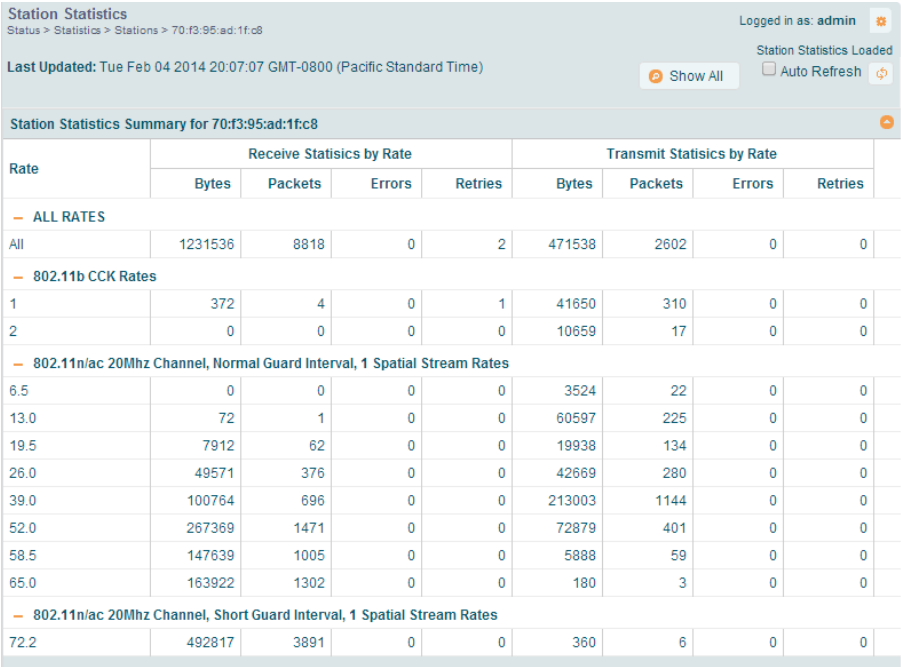
Per-Station Statistics
Stations

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 144.

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.



Rate	Receive Statisics by Rate				Transmit Statisics by Rate			
	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
– ALL RATES								
All	1231536	8818	0	2	471538	2602	0	0
– 802.11b CCK Rates								
1	372	4	0	1	41650	310	0	0
2	0	0	0	0	10659	17	0	0
– 802.11n/ac 20Mhz Channel, Normal Guard Interval, 1 Spatial Stream Rates								
6.5	0	0	0	0	3524	22	0	0
13.0	72	1	0	0	60597	225	0	0
19.5	7912	62	0	0	19938	134	0	0
26.0	49571	376	0	0	42669	280	0	0
39.0	100764	696	0	0	213003	1144	0	0
52.0	267369	1471	0	0	72879	401	0	0
58.5	147639	1005	0	0	5888	59	0	0
65.0	163922	1302	0	0	180	3	0	0
– 802.11n/ac 20Mhz Channel, Short Guard Interval, 1 Spatial Stream Rates								
72.2	492817	3891	0	0	360	6	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 387****.*

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 smart phone 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

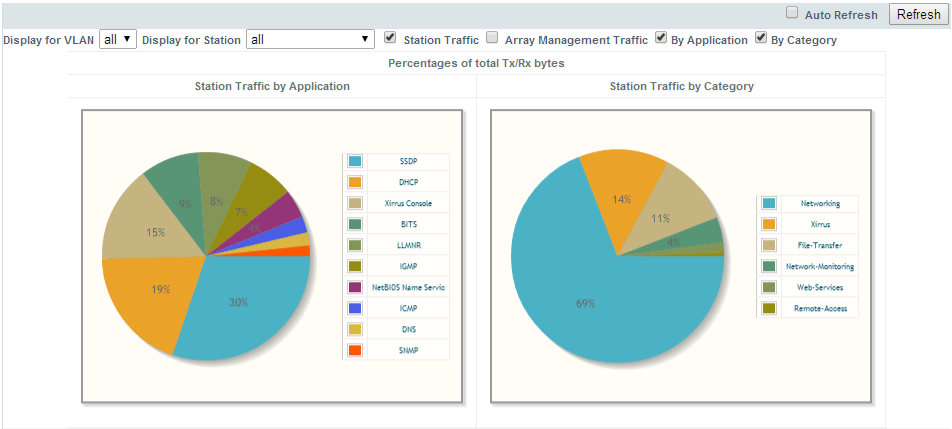
For an additional discussion, see the *Application Control Application Note* in the ***Xirrus Resource Center***.

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 395).

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 366).



Station Traffic

Application	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
SSDP	4	1	8488	1603154	6945	1116739
DHCP	4	1	3571	1174463	1715	569160
Xirrus Console	5	1	42014	1347996	0	0
BITS	4	1	567	791733	319	29337
LLMNR	4	1	9408	548720	3580	211948
IGMP	3	1	11019	441576	5152	206176
NetBIOS Name Servic	5	3	4580	357240	485	38514
ICMP	3	4	286	93206	519	132493
DNS	3	4	876	105322	1090	77126
SNMP	4	4	1336	94188	982	54992
Windows Update	4	2	89	30913	116	111142
IP	3	1	1792	136192	0	0
UDP	3	1	4	4084	117	119148
HTTP	3	1	451	65314	473	43795
CIFS	5	1	297	69512	90	20252
TeamViewer	4	2	320	21659	591	33595
TFTP	3	5	888	42780	0	0
TCP	3	1	8	416	638	38934
Google	3	1	35	16254	44	11814
SSL	3	3	22	8238	32	3120
MDNS	3	1	89	8851	0	0
Apple	3	2	11	983	16	1990

Category	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Networking	4	1	39864	4382457	19737	2378815
Xirrus	5	1	42016	1348060	0	0
File-Transfer	4	1	1841	934938	525	160731
Network-Monitoring	3	4	1622	187394	1501	187485
Web-Services	3	1	508	89806	549	58729
Remote-Access	4	2	320	21659	591	33595

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 152.
- **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

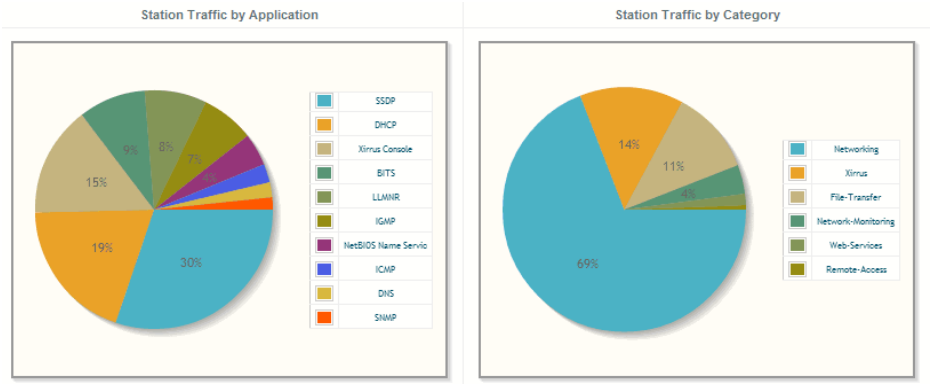


Figure 90. Application Control (Pie Charts)

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
SSDP	4	1	8488	1603154	6945	1116739
DHCP	4	1	3571	1174463	1715	569160
Xirrus Console	5	1	42014	1347996	0	0
BITS	4	1	567	791733	319	29337
LLMNR	4	1	9408	548720	3580	211948
IGMP	3	1	11019	441576	5152	206176
NetBIOS Name Servic	5	3	4580	357240	485	38514
ICMP	3	4	286	93206	519	132493
DNS	3	4	876	105322	1090	77126
SNMP	4	4	1336	94188	982	54992
Windows Update	4	2	89	30913	116	111142
IP	3	1	1792	136192	0	0
UDP	3	1	4	4084	117	119148
HTTP	3	1	451	65314	473	43795
CIFS	5	1	297	69512	90	20252
TeamViewer	4	2	320	21659	591	33595
TFTP	3	5	888	42780	0	0
TCP	3	1	8	416	638	38934
Google	3	1	35	16254	44	11814
SSL	3	3	22	8238	32	3120
MDNS	3	1	89	8851	0	0

Category	Productivity	Risk	Transmitted Packets	Transmitted Bytes	Received Packets	Received Bytes
Networking	4	1	39864	4382457	19737	2378815
Xirrus	5	1	42016	1348060	0	0
File-Transfer	4	1	1841	934938	525	160731
Network-Monitoring	3	4	1622	187394	1501	187485
Web-Services	3	1	508	89806	549	58729
Remote-Access	4	2	320	21659	591	33595

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 368. 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 256.
- 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.

Total Stations: 4 ☐ Identification ☐ Security ☐ Connection Info ☐ Auto Refresh Refresh

MAC Address	IP Address	SSID	Group	VLAN	QOS	IAP	TX Rate	RX Rate	RSSI	Last Alarm	Time D:H:M
5c:ff:35:84:21:98	10.100.55.164	Last1			0	iap2	150.0Mbps	6.0Mbps	-20	none	0:02:18
70:f3:95:ad:1f:c8	10.100.55.166	Last2			0	iap1	58.5Mbps	52.0Mbps	-43	none	0:03:36
ac:81:12:05:69:47	10.100.55.158	Last2			0	iap1	2.0Mbps	52.0Mbps	-35	none	0:04:21
f0:b4:79:2a:f5:c7	10.100.55.165	Last2			0	iap1	65.0Mbps	65.0Mbps	-39	none	0:02:33

Figure 92. Stations (Application Control)

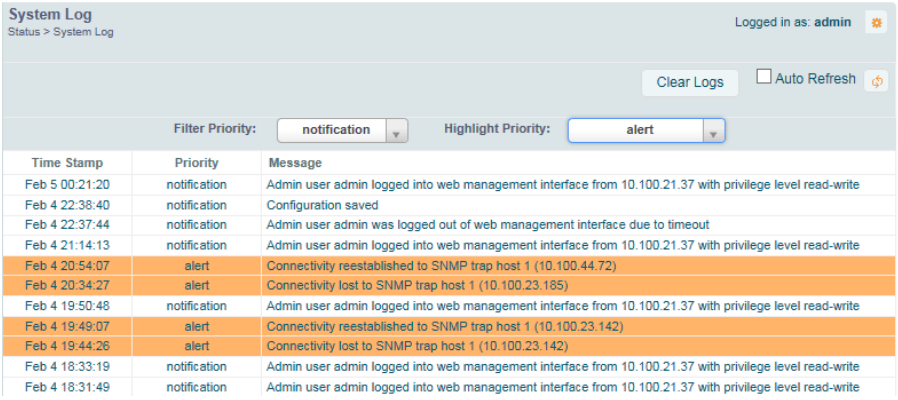
The rest of the fields and display options on this window (including the **Identification**, **Security**, and **Connection Info** checkboxes) are as described in "Stations" on page 123.

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.



Time Stamp	Priority	Message
Feb 5 00:21:20	notification	Admin user admin logged into web management interface from 10.100.21.37 with privilege level read-write
Feb 4 22:38:40	notification	Configuration saved
Feb 4 22:37:44	notification	Admin user admin was logged out of web management interface due to timeout
Feb 4 21:14:13	notification	Admin user admin logged into web management interface from 10.100.21.37 with privilege level read-write
Feb 4 20:54:07	alert	Connectivity reestablished to SNMP trap host 1 (10.100.44.72)
Feb 4 20:34:27	alert	Connectivity lost to SNMP trap host 1 (10.100.23.185)
Feb 4 19:50:48	notification	Admin user admin logged into web management interface from 10.100.21.37 with privilege level read-write
Feb 4 19:49:07	alert	Connectivity reestablished to SNMP trap host 1 (10.100.23.142)
Feb 4 19:44:26	alert	Connectivity lost to SNMP trap host 1 (10.100.23.142)
Feb 4 18:33:19	notification	Admin user admin logged into web management interface from 10.100.21.37 with privilege level read-write
Feb 4 18:31:49	notification	Admin user admin logged into web management interface from 10.100.21.37 with privilege level read-write

Figure 93. System Log (Alert Level Highlighted)

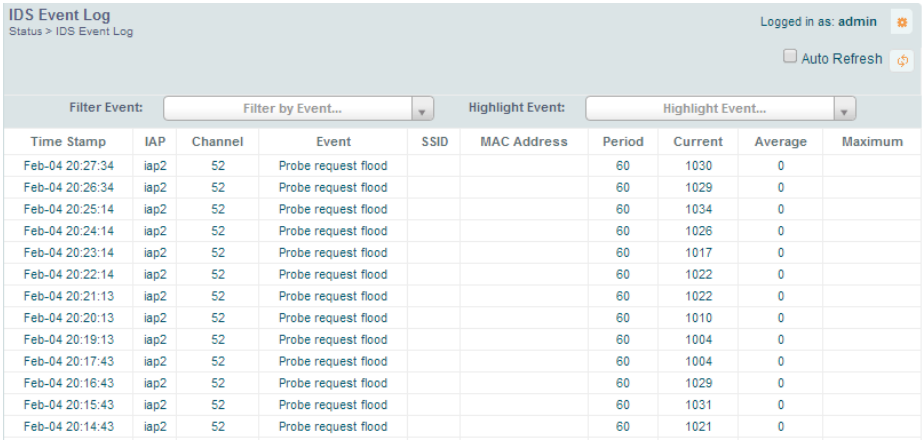
Use the **Highlight Priority** field if you wish to highlight messages at the selected priority level. Click on the **Refresh** button to refresh the message list, or click on the **Clear All** button at the upper left to delete all messages. You can also click in the **Auto Refresh** check box to instruct 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 38 on page 85 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 348.

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



Time Stamp	IAP	Channel	Event	SSID	MAC Address	Period	Current	Average	Maximum
Feb-04 20:27:34	iap2	52	Probe request flood			60	1030	0	
Feb-04 20:26:34	iap2	52	Probe request flood			60	1029	0	
Feb-04 20:25:14	iap2	52	Probe request flood			60	1034	0	
Feb-04 20:24:14	iap2	52	Probe request flood			60	1026	0	
Feb-04 20:23:14	iap2	52	Probe request flood			60	1017	0	
Feb-04 20:22:14	iap2	52	Probe request flood			60	1022	0	
Feb-04 20:21:13	iap2	52	Probe request flood			60	1022	0	
Feb-04 20:20:13	iap2	52	Probe request flood			60	1010	0	
Feb-04 20:19:13	iap2	52	Probe request flood			60	1004	0	
Feb-04 20:17:43	iap2	52	Probe request flood			60	1004	0	
Feb-04 20:16:43	iap2	52	Probe request flood			60	1029	0	
Feb-04 20:15:43	iap2	52	Probe request flood			60	1031	0	
Feb-04 20:14:43	iap2	52	Probe request flood			60	1021	0	

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 a column header to sort the rows based on that column. 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.