USER'S GUIDE

Wireless Arrays

XR and XN Series
January 10, 2013
Release 6.4

XIRRUS
High Performance Wireless Networks

Wireless Array™

XR and XN Series

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

Trademarks

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

Please see Legal Notices, Warnings, Compliance Statements, and Warranty and License Agreements in "Appendix C: Notices" on page 471.

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

The Command Line Interface ... 377

List of Figures

Introduction

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

The Xirrus Family of Products

Figure 1. Xirrus Arrays: XR Series

The Xirrus family of products includes the following:

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

- **The XN Series of Xirrus Wireless Arrays**

  The Xirrus Wireless Arrays have the speed and reach of IEEE 802.11n technology. The XN Series of Arrays feature the capacity and performance needed to replace switched Ethernet to the desktop.

  XN Series Arrays integrate multiple Integrated Access Points—radios with high-gain directional antennas for increased range and coverage. The Array also incorporates an onboard multi-gigabit switch, wireless controller, and firewall into a single device, along with a dedicated wireless threat sensor and an embedded spectrum analyzer. The Wireless Array provides more than enough bandwidth, security, and control to replace switched Ethernet to the desktop as the primary network connection.

- **Xirrus Management System (XMS)**

  XMS is used for managing large Array deployments from a centralized Web-based interface. The XMS server is available pre-installed on the Xirrus Management Appliance series, or as a software package to be installed on your own server hardware (optionally under VMware).

  Users start the XMS client simply by entering the URL of the XMS server on a web browser. The XMS server manages a number of Wireless Arrays via SNMP.

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

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

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

Nomenclature

Throughout this User's Guide, the Xirrus Wireless Array is also referred to as simply the **Array**. In some instances, the terms **product** and **unit** are also used. When discussing specific products from the Xirrus family, the product name is used (for example, XR-4830). The Wireless Array's operating system is referred to as the **ArrayOS**. The Web Management Interface for browser-based management of the Array is referred to as **WMI**.

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

The XN series of Arrays have two types of radios—the 5 GHz 802.11a/n radios are named **an1** through **an12** (for 16-port models). The 802.11a/b/g/n radios are named **abgn1** to **abgn4**, and they also support both 2.4GHz and 5 GHz.

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

Why Choose the Xirrus Wireless Array?

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

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

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

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

See Also

Key Features and Benefits
Wireless Array Product Overview
The Xirrus Family of Products

Wireless Array Product Overview

Part of the family of Xirrus products, the Wireless Array is a high capacity, multi-mode device designed with 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 450 Mbps throughput (on XR-1000 and higher Array modesl).

Figure 2. Wireless Array (XR Series)

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

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

XR Wireless Array Product Family

XR-500 Series Arrays

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

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

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

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

XR-1000 and XR-2000 Series Arrays

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

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

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

Like all XR Arrays except the XR-500 Series, these models integrate multi-state radios with high gain directional antennas, an onboard multi-gigabit switch, controller, firewall, threat sensor and spectrum analyzer all built on a modular chassis designed for future extensibility.

Feature	XR-1220	XR-1230	XR-2220	XR-2230	XR-2420	XR-2430
No. radios: 802.11 a/b/g/n/monitor	2	2	2	2	4	4
Radio type	2x2	3x3	2x2	3x3	2x2	3x3
# Integrated antennas	4	6	4	6	8	12
Integrated wireless switch ports	2	2	4	4	4	4
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes	Yes	Yes
1 Gigabit Uplink Ports	1	1	1	1	1	1
Wireless bandwidth	600 Mbps	900 Mbps	600 Mbps	900 Mbps	1.2 Gbps	1.8 Gbps
Users supported	480	480	480	480	960	960

XR-4000 Series Arrays

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

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

XR-6000 Series Arrays

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

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

See Also

Key Features and Benefits
Wireless Array Product Overview
Power over Gigabit Ethernet (PoGE)

XN Wireless Array Product Family

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

XN Family of Arrays

Feature	XN16	XN12	XN8	XN4
Number of 802.11a/b/g/n radios	4	4	4	4
Number of 802.11a/n radios	12	8	4	0
Total radios	**16**	**12**	**8**	**4**
Number of integrated antennas	48	36	36	20
Integrated Wi-Fi switch ports	16	12	8	4
Integrated RF spectrum analyzer, threat sensors	Yes	Yes	Yes	Yes
Uplink Ports	2	2	2	1
Wireless bandwidth	4.8 Gbps	3.6 Gbps	2.4 Gbps	1.2 Gbps
Users supported	1280	960	640	320

See Also

Key Features and Benefits

Wireless Array Product Overview

Power over Gigabit Ethernet (PoGE)

Why Choose the Xirrus Wireless Array?

Enterprise Class Security

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

Deployment Flexibility

Xirrus' unique multi-radio architecture (on all Arrays except the XR-500 Series) generates 360 degrees of sectored high-gain 802.11a/b/g/n coverage that provides extended range and the highest possible data rates for a large volume of clients. Each sector can be adjusted automatically or manually, creating a pattern of wireless coverage perfectly tailored to individual customer needs. For example:

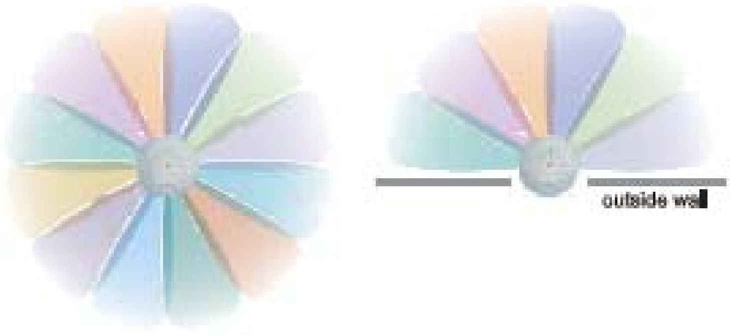


Figure 3. Wireless Coverage Patterns

Figure 3 depicts the following two scenarios:

- **Full pattern coverage**
  All radios are activated with coverage spanning 360 degrees. If within range, clients will always receive coverage regardless of their geographic

position relative to the Array. Radios may be assigned to 2.4 GHz and/or 5.0 GHz bands in any desired pattern.

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

Power over Gigabit Ethernet (PoGE)

The Xirrus-supplied XP1, XP2, and XP8 Power over Gigabit Ethernet modules provide power to your Arrays over the same Cat 5e or Cat 6 cable used for data, eliminating the need to run power cables and provide an AC power outlet in proximity to each unit. Managed modules provide the ability to control power using XMS.

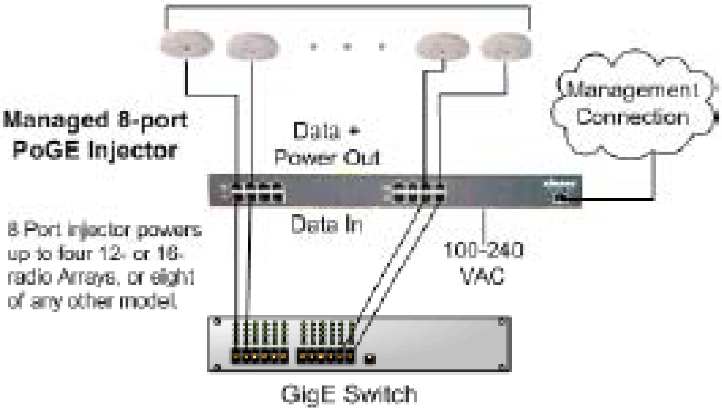


Figure 4. XP8 - Power over Ethernet Usage

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

Enterprise Class Management

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

Figure 5. WMI: Array Status

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

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

Key Features and Benefits

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

High Capacity and High Performance

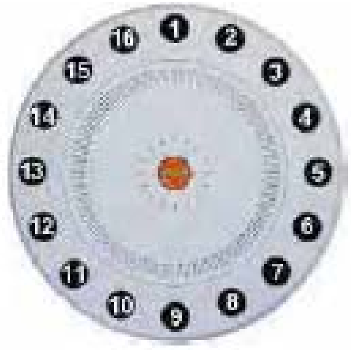


Figure 6. Layout of IAPs (XR-7630)

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

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

Extended Coverage

One XR-7630 solution enables you to replace fifteen access points (including one omnidirectional IAP for monitoring the network). Fifteen IAP radios with integrated directional antennas provide increased wireless range and enhanced data rates in all directions. With a Wireless Array deployed, far fewer access points are needed and wired-like resiliency is delivered throughout your wireless network. Your Wireless Array deployment ensures:

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

Non-Overlapping Channels

Complete use of non-overlapping channels limits interference and delivers maximum capacity. On the XR-7630, up to 16 non-overlapping channels are fully utilized across the 5GHz and 2.4GHz spectrums (up to 12 across the 5GHz spectrum plus up to 3 across the 2.4 GHz spectrum—typically, one additional radio is used as a dedicated RF monitor).

SDMA Optimization

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

Fast Roaming

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

Easy Deployment

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

Secure Wireless Access

Multiple layers of authentication and encryption ensure secure data transmissions. The Wireless Array is 802.11i compliant with line-rate encryption support for 40 and 128 bit WEP, WPA and WPA2 with TKIP and AES encryption. Authentication is provided via 802.1x, including PEAP, EAP-TLS, EAP-TTLS, EAP-SIM, EAP-GRC, and LEAP (Lightweight Extensible Authentication Protocol) passthrough. Intrusion detection and prevention provide proactive monitoring of the environment for threats.

Applications Enablement

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

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), and RF Analysis Manager (RAM). These packages are separately licensed for operation on your Array.

Xirrus Advanced RF Performance Manager (RPM)

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

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

With each of the Array's multiple radios operating on a different channel, RPM selects the ideal radio for each station. High-speed stations are grouped together on radios with other high speed stations, while lower speed stations are combined with other lower speed stations. This ensures optimal performance for high-speed 802.11n stations without compromise.

The complete feature set of the RPM package includes:

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

Xirrus Advanced RF Security Manager (RSM)

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

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

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

The complete feature set of the RSM package includes:

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

Xirrus Advanced RF Analysis Manager (RAM)

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

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

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

The key elements of the RAM package include:

- RF Analysis – An embedded Spectrum Analyzer leverages the dedicated threat sensor radio in each Wireless Array to provide a continual view of utilization, interference, and errors across all available wireless channels.
- Packet Analysis – Integrated packet capture provides filterable views of all traffic traversing on the wired and wireless interfaces of the Array.
- Performance Analysis – Embedded traffic generation enables the throughput of the Array's wireless or wired interfaces to be analyzed.
- Failure Recovery – Radio Assurance provides an automatic self-test and self healing mechanism that ensures continuous system operation.
- Netflow Support
- Network Tools: ping, RADIUS ping, traceroute

About this User's Guide

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

Organization

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

- **Introduction**

  Provides a brief introduction to wireless technology, an overview of the product, including its key features and benefits, and presents the product specifications.

- **Installing the Wireless Array**

  Defines prerequisites for deploying and installing the Array and provides instructions to help you plan and complete a successful installation.

- **The Web Management Interface**

  Offers an overview of the product's embedded Web Management Interface, including its content and structure. It emphasizes what you need to do to ensure that any configuration changes you make are applied, and provides a list of restricted characters. It also includes instructions for logging in to the Array with your Web browser.

- **Viewing Status on the Wireless Array**

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

- **Configuring the Wireless Array**

  Contains procedures for configuring the Array using its embedded Web Management Interface.

- **Using Tools on the Wireless Array**

  Contains procedures for using utility tools provided in the Web Management Interface. It includes procedures for upgrading the system firmware, uploading and downloading configurations and other files, using diagnostic tools, and resetting the Array to its factory defaults.

- **The Command Line Interface**

  Includes the commands and the command structure used by the Wireless Array's Command Line Interface (CLI), and provides a procedure for establishing a Telnet connection to the Array. This chapter also includes some sample key configuration tasks using the CLI.

- **Appendix A: Quick Reference Guide**

  Contains the product's factory default settings.

- **Appendix B: Technical Support**

  Offers guidance to resolve technical issues, including general hints and tips to enhance your product experience, and a procedure for isolating problems within an Array-enabled wireless network. Also includes Frequently Asked Questions (FAQs) and Xirrus contact information.

- **Appendix C: Notices**

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

- **Glossary of Terms**

  Provides an explanation of terms directly related to Xirrus product technology, organized alphabetically.

- **Index**

  The index is a valuable information search tool. Use the index to locate specific topics discussed in this User's Guide. Simply click on any page number in the index to jump to the referenced topic.

Notes and Cautions

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

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

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

Screen Images

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

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 23.
- "Planning Your Installation" on page 26.
- "Installation Workflow" on page 57.
- "Installing Your Wireless Array" on page 59.
- "Powering Up the Wireless Array" on page 63.
- "Establishing Communication with the Array" on page 66.
- "Performing the Express Setup Procedure" on page 71.

Installation Prerequisites

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

- **Power Source**
  Most Arrays are powered via Xirrus-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. Current Array models have integrated splitters, so no separate splitter is required.

- **Ethernet ports**
  You need at least one 100/1000 BaseT port to establish wired Gigabit Ethernet connectivity. XR Series Arrays have one, two, or four Gigabit ports, depending on the model (see "XR Wireless Array Product Family" on page 6). XN Series Arrays have one or two Gigabit ports, depending on the model. Some models also have one 10/100 BaseT port which may be used for product management if desired. See "XN Wireless Array Product Family" on page 10.

! *The Array's Ethernet ports should be connected to an Ethernet switch, not an Ethernet hub—if a hub is used, we recommend that you do not bond-pair Ethernet ports.*

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

- **Secure Web browser**

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

- **Serial connection capability**
  To connect directly to the console port on the Array (all models except XR-500 and XR-1000 Series), your computer must be equipped with a male 9-pin serial port and terminal emulation software (for example, HyperTerminal). The Xirrus Array only supports serial cable lengths up to 25' per the RS-232 specification.

  Use the following settings when establishing a serial connection:

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

Optional Network Components

The following network components are optional.

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

Client Requirements

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

See Also

Coverage and Capacity Planning
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 26
- "Coverage and Capacity Planning" on page 28
- "IEEE 802.11n Deployment Considerations" on page 35
- "Failover Planning" on page 42
- "Power Planning" on page 45
- "Security Planning" on page 46
- "Port Requirements" on page 48
- "Network Management Planning" on page 52
- "WDS Planning" on page 53
- "Common Deployment Options" on page 56

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 or 802.11a/b/g coverage that provides extended range. (Note that XR-500 Series radios are omni-directional rather than sectored.) However, the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through may affect the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise at your location. To maximize wireless range, follow these basic guidelines:

1. Keep the number of walls and ceilings between the Array and your receiving devices to a minimum—each wall or ceiling can reduce the wireless range from between 3 and 90 feet (1 to 30 meters). Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between each device. For example, a wall that is 1.5 feet thick (half a meter) at 90° is actually almost 3 feet thick (or 1 meter) when viewed at a 45° angle. At an acute 2° degree angle the same wall is over 42 feet (or 14 meters) thick! For best reception, try to ensure that your wireless devices are positioned so that signals will travel straight through a wall or ceiling.

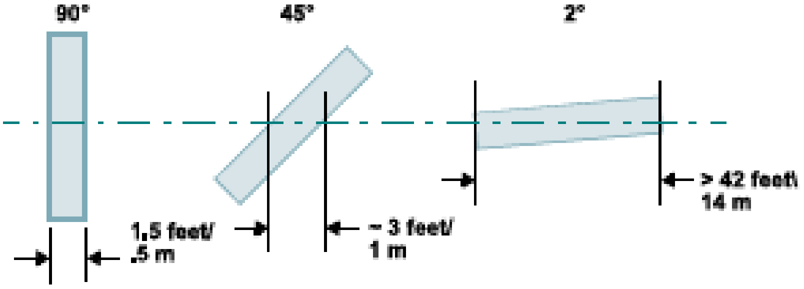


Figure 7. Wall Thickness Considerations

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

See Also

Coverage and Capacity Planning
Common Deployment Options
Installation Prerequisites

Coverage and Capacity Planning

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

Note that several advanced features in this section are part of the Xirrus Advanced RF Performance Manager (RPM). *They require the license installed on the Array to include support for RPM. Please see* ***"About Licensing and Upgrades" on page 361****.*

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

Placement

Use the following guidelines when considering placement options:

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

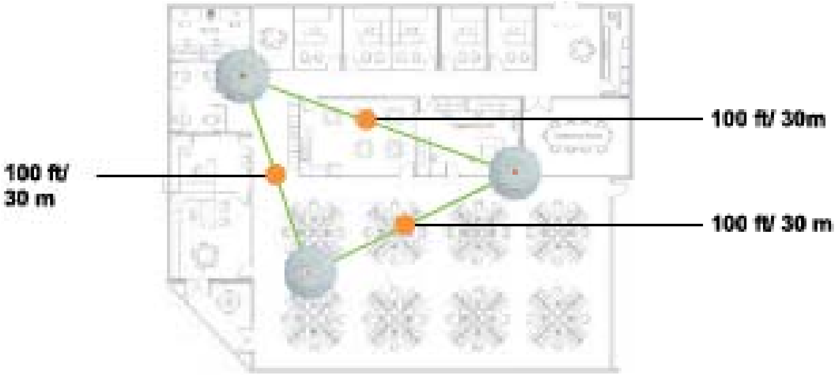


Figure 8. Unit Placement

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

RF Patterns

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

Full (Normal) Coverage

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

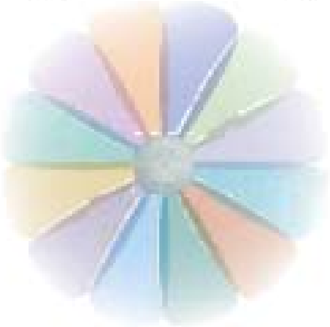


Figure 9. Full (Normal) Coverage

Half Coverage

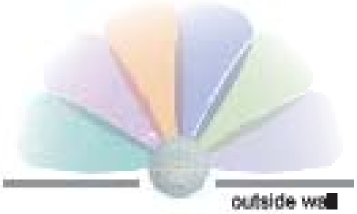


Figure 10. Adjusting RF Patterns

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

Custom Coverage

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

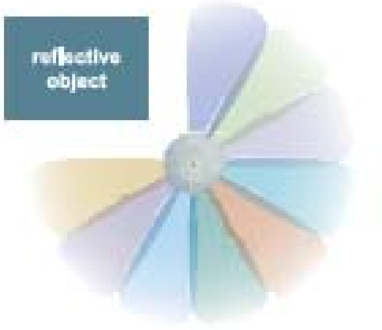


Figure 11. Custom Coverage

Capacity and Cell Sizes

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

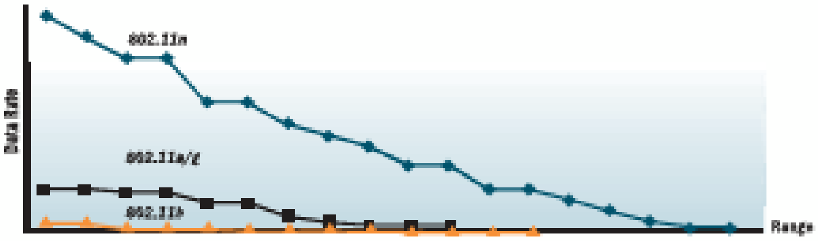


Figure 12. Connection Rate vs. Distance

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

The XN4 has a smaller range than the larger Arrays.

Fine Tuning Cell Sizes

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

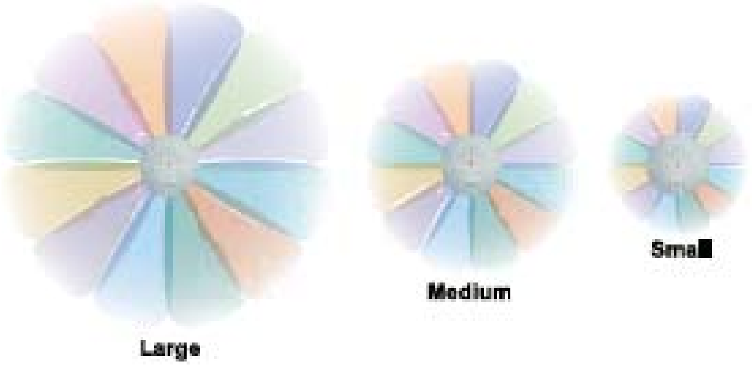


Figure 13. Transmit Power

Auto Cell Size is an automatic, self-tuning mechanism that balances cell size between Arrays to guarantee coverage while limiting the RF energy that could extend beyond the organizational boundary. Auto Cell uses communication between Arrays to dynamically set radio power so that complete coverage is provided to all areas, yet at the minimum power level required. This helps to minimize potential interference with neighboring networks. Additionally, Arrays running Auto Cell automatically detect and compensate for coverage gaps caused by system interruptions. To enable the Auto Cell Size feature, go to "RF Power & Sensitivity" on page 316. For a complete discussion of the Auto Cell size feature, see the *Xirrus Auto Cell Application Note* in the *Xirrus Resource Center*.

If you are installing many units in proximity to each other, we recommend that you use Auto Cell Size; otherwise, reduce the transmit power using manual settings to avoid excessive interference with other Arrays or installed APs. See also, "Coverage and Capacity Planning" on page 28.

Sharp Cell

XR-500 Series radios are omni-directional rather than directional (sectored),. This feature is not applicable to these Arrays.

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 316. For more information about this feature, see the *Xirrus Sharp Cell Application Note* in the *Xirrus Resource Center*.

Roaming Considerations

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

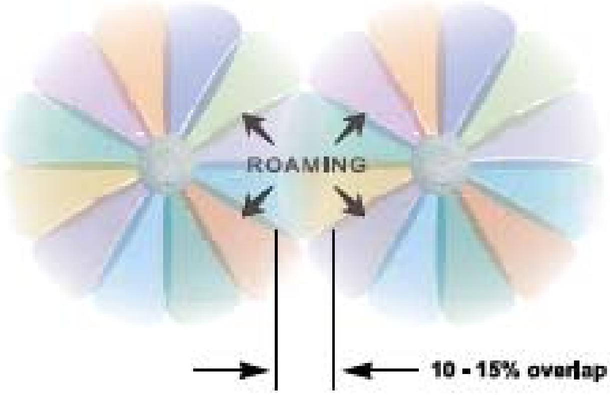


Figure 14. Overlapping Cells

Allocating Channels

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

Automatic Channel Selection

We recommend that you allow the Array to make intelligent channel allocation decisions automatically. In the automatic mode, channels are allocated dynamically, driven by changes in the environment. Auto Channel assignment is performed by scanning the surrounding area for RF activity on all channels, then automatically selecting and setting channels on the Array to the best channels available. This function is typically executed when initially installing Arrays in a new location and may optionally be configured to execute periodically to account for changes in the RF environment over time. Auto Channel selection has significant advantages, including:

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

To set up the automatic channel selection feature, go to "Advanced RF Settings" on page 313.

Manual Channel Selection

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

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

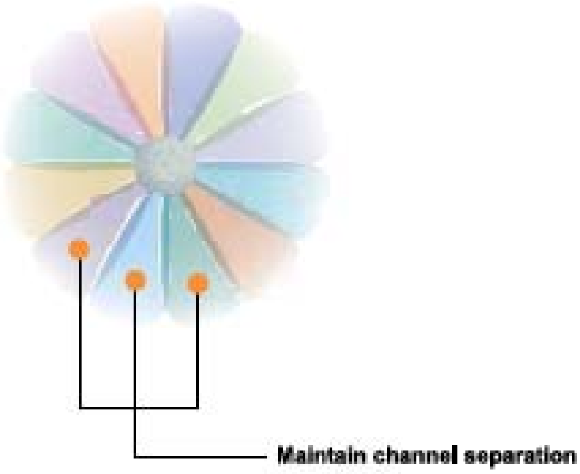


Figure 15. Allocating Channels Manually

See Also

Failover Planning

Installation Prerequisites

IEEE 802.11n Deployment Considerations

Note that the license installed on the Array must include support for 802.11n. Please see "About Licensing and Upgrades" on page 361.

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

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

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

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

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

- **"MIMO (Multiple-In Multiple-Out)" on page 36**
- **"Multiple Data Streams—Spatial Multiplexing" on page 38**
- **"Channel Bonding" on page 39**
- **"Improved MAC Throughput" on page 40**
- **"Short Guard Interval" on page 40**
- **"Obtaining Higher Data Rates" on page 41**
- **"802.11n Capacity" on page 42**

Two very important techniques to consider are Channel Bonding and Multiple Data Streams—Spatial Multiplexing because they contribute a large portion of

802.11n's speed improvements and because they are optional and configurable, as opposed to the parts of 802.11n that are fixed. While the settings for 802.11n IAPs come pre-configured on the Array for robust performance in typical usage, you should review the settings for your deployment, especially channel bonding. A global setting is provided to enable or disable 802.11n mode. See "Global Settings .11n" on page 304 to configure 802.11n operation.

MIMO (Multiple-In Multiple-Out)

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

Prior to 802.11n, a data stream was transmitted via one antenna. At the receiving end, the antenna with the best signal was selected to receive data. (Figure 16)

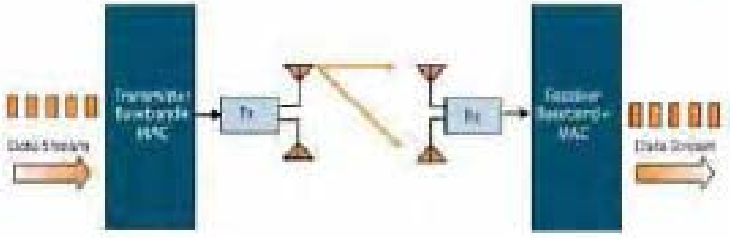


Figure 16. Classic 802.11 Signal Transmission

MIMO signal processing uses multiple antennas to send and receive data. It takes advantage of multipath reflections to improve signal coherence and greatly increase receiver sensitivity (Figure 17).

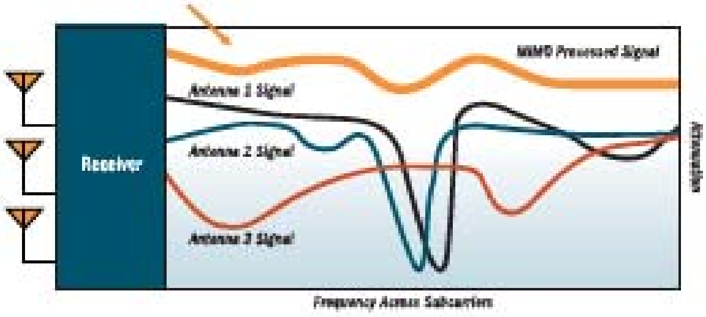


Figure 17. MIMO Signal Processing

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

Multiple Data Streams—Spatial Multiplexing

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

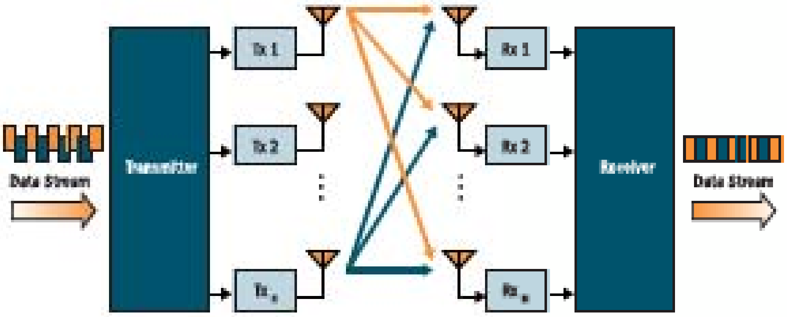


Figure 18. Spatial Multiplexing

Spatial multiplexing can double, triple, or quadruple the date rate, depending on the number of transmit antennas used. You can configure the number of chains (i.e., streams) separately for transmitting and receiving. By default, the Array uses three chains for transmitting and receiving (see "Global Settings .11n" on page 304).

Channel Bonding

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

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

The Array provides an Automatic Channel Bonding setting that will automatically select the best channel for bonding on each IAP. If you enable this option, you may select whether bonding will be dynamic (the bonded channel changes in response to environmental conditions) or static (the bonded channel will not be changed. See "Global Settings .11n" on page 304. To configure channel bonding manually, on a per-IAP basis, see "IAP Settings" on page 274.

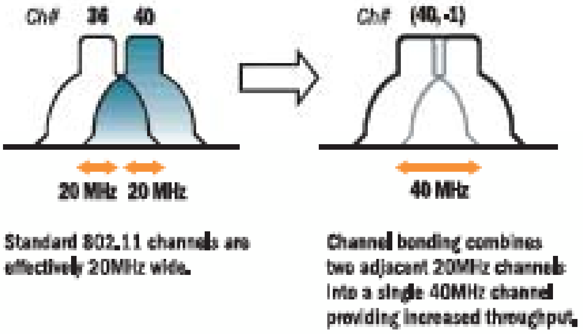

Ch# 36 40
20 MHz 20 MHz
Standard 802.11 channels are effectively 20MHz wide.
Ch# (40,-1)
40 MHz
Channel bonding combines two adjacent 20MHz channels into a single 40MHz channel providing increased throughput.

Figure 19. Channel Bonding

Improved MAC Throughput

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

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

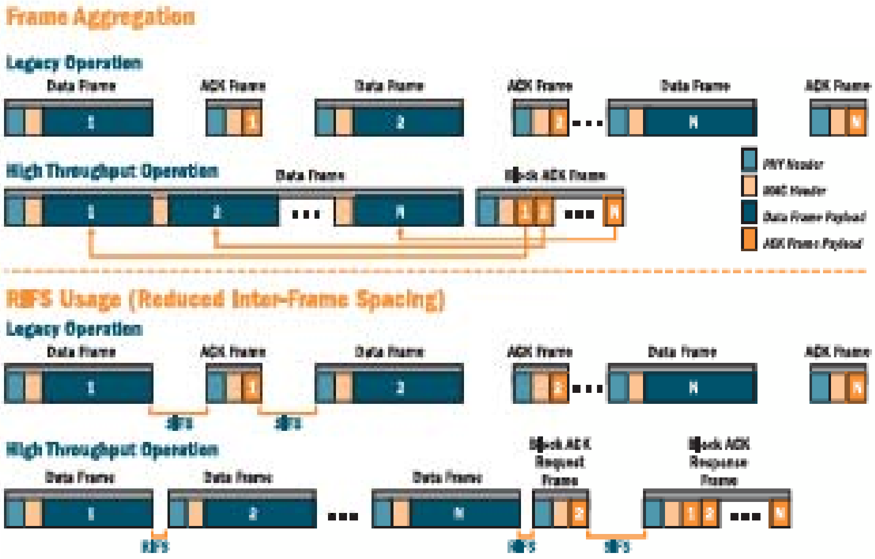


Figure 20. MAC Throughput Improvements

Short Guard Interval

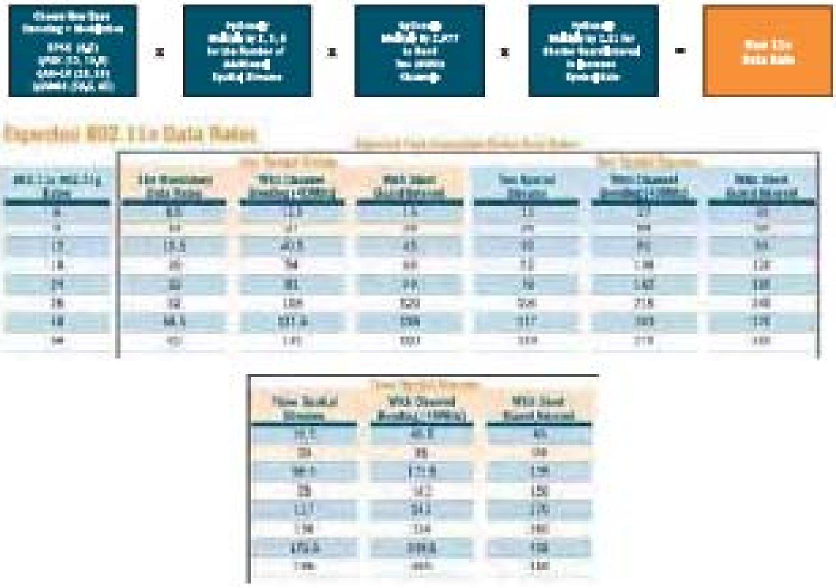
This option reduces the wait time between signals that are being sent out over the air. The guard interval provides immunity to propagation delays and reflections, and is normally 800 ns (long). By using a short guard interval (400 ns), the data rate is increased by approximately 11%. The short interval may be used in many environments (especially indoors). If the short guard interval is used in an inappropriate environment, the signal quality will suffer and throughput will decrease. See "Global Settings .11n" on page 304 to configure the guard interval.

Obtaining Higher Data Rates

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

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

See Figure 21 to see the 802.11n data rate increase for an IAP. Apply this increase to the 802.11 a, b or g data rates selected for the Array.


Choose Base Rate Encoding + Modulation
BPSK (6,9)
QPSK (12,18)
QAM-16 (24,36)
QAM64 (48,54)
x
Optionally multiply by 2, 3, 4 for the Number of Additional Spatial Streams
x
Optionally multiply by 2.077 to Bond Two 20MHz Channels
x
Optionally multiply by 1.11 for Shorter Guard Interval to Increase Symbol Rate
=
New 11n Data Rate

Expected 802.11n Data Rates

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

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

Figure 21. Computing 802.11n Data Rates

802.11n Capacity

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

802.11 Mode	# Channels	Max Theoretical Capacity
Fast Ethernet	No	Yes
802.11 a/n: 3 Streams	23	23 * 450 Mbps = 10.2 Gbps
802.11 a/n: 2 Streams	23	23 * 300 Mbps = 6.8 Gbps
802.11 a/n: 1 Stream	23	23 * 150 Mbps = 3.4 Gbps
802.11 a	23	23 * 54 Mbps = 1.2 Gbps
802.11 g/n: 3 Streams	3	3 * 450 Mbps = 1.35 Gbps (1 or 2 streams have proportionally lower capacity)
802.11 g	3	3 * 54 Mbps = 162 Mbps
802.11 b	3	3 * 11 Mbps = 33 Mbps

Failover Planning

This section discusses failover protection at the unit and port levels. To ensure that service is continued in the event of a port failure, you can utilize two Gigabit Ethernet ports simultaneously as a bonded pair (on Arrays with two or more Gigabit ports).

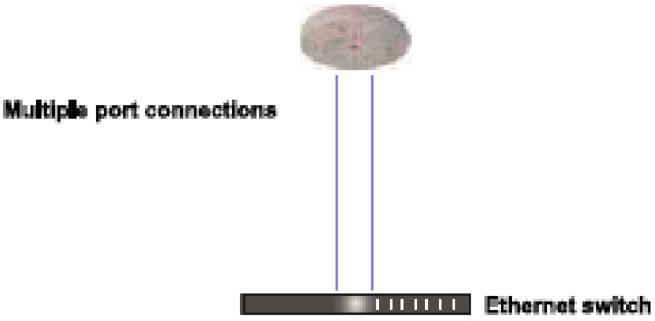


Figure 22. Port Failover Protection

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

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

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

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

For more details on Gigabit port modes and their configuration, please see "Network Bonds" on page 175.

Switch Failover Protection

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

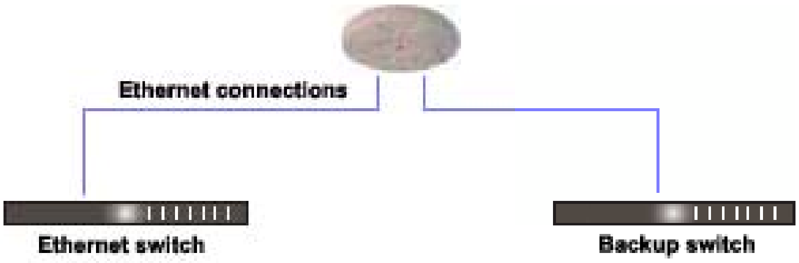


Figure 23. Switch Failover Protection

Gigabit Ethernet connections must be on the same subnet.

See Also

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

Power Planning

All XR and XN Series Array models support Power over Gigabit Ethernet (PoGE) with an integrated splitter. This section discusses PoGE power.

Power over Gigabit Ethernet

To deliver power to the Array, you must use Xirrus-supplied may use the optional XP1, XP2, or XP8 Power over Gigabit Ethernet (PoGE) modules. They provide power over Cat 5e or Cat 6 cables to the Array without running power cables—see Figure 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.

See Also

Coverage and Capacity Planning
Failover Planning
Network Management Planning
Security Planning

Security Planning

This section offers some useful guidelines for defining your preferred encryption and authentication method. For additional information, see "Understanding Security" on page 209 and the Security section of "Frequently Asked Questions" on page 452.

Note that several advanced features in this section are part of the Xirrus Advanced RF Security Manager (RSM). *They require the license installed on the Array to include support for RSM. Please see* ***"About Licensing and Upgrades" on page 361****.*

Wireless Encryption

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

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

Authentication

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

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

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

- **Xirrus Internal RADIUS server**
  Recommended for smaller numbers of users (about 100 or less). Supports EAP-PEAP only

- **Pre-Shared Key**
  Uses a pass-phrase or key that is manually distributed to all authorized users. The same passphrase is given to client devices and entered into each Array.

- **MAC Access Control Lists (ACLs)**
  MAC access control lists provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network, and can be used in addition to any of the above authentication methods. ACLs are good for embedded devices, like printers and bar-code scanners (though MAC addresses can be spoofed). The Array supports 1,000 global ACL entries. You may also define per-SSID access control lists, with up to 1000 entries each.

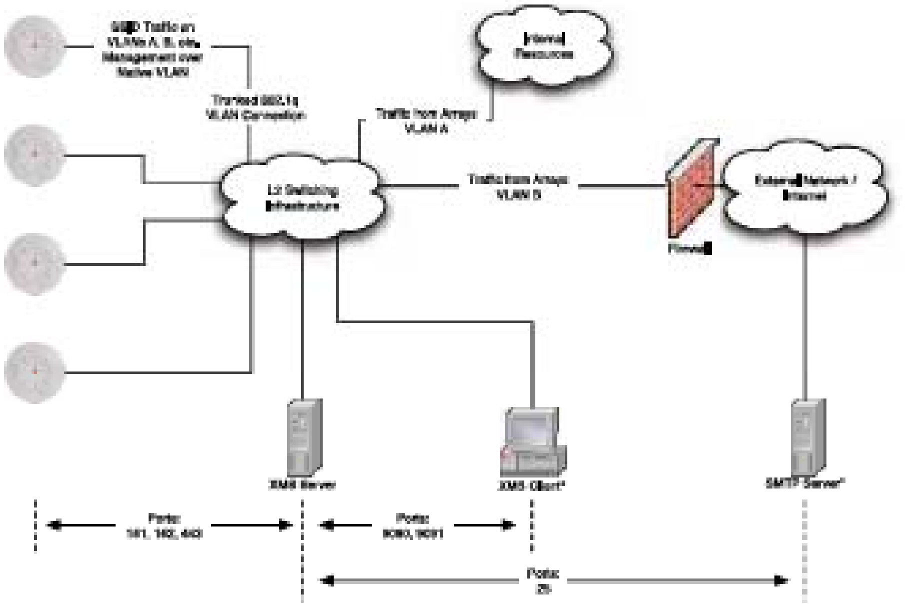
See Also

Failover Planning
Network Management Planning
Power Planning

Port Requirements

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

As an example, XMS port requirements are illustrated in Figure 24. XMS requires ports 161, 162, and 443 to be passed between Arrays and the XMS server. Similarly, ports 9090 and 9091 are required for communication between the XMS server and XMS clients, and port 25 is typically used by the XMS server to access an SMTP server to send email notifications.


SSID Traffic on VLANs A, B, etc. Management over Native VLAN
Trunked 802.1q VLAN Connection
Internal Resources
Traffic from Arrays VLAN A
L2 Switching Infrastructure
Traffic from Arrays VLAN B
Firewall
External Network / Internet
XMS Server
XMS Client*
SMTP Server*
Ports: 161, 162, 443
Ports: 9090, 9091
Ports: 25

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

Figure 24. Port Requirements for XMS

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

Port	Application	Peer	Configurable
Array			
icmp	Ping	XMS Server	No
20 tcp 21 tcp	FTP	Client	Yes
22 tcp	SSH	Client	Yes
23 tcp	Telnet	Client	Yes
25 tcp	SMTP	Mail Server	No
69 udp	TFTP	TFTP Server	No
123 udp	NTP	NTP Server	No
161 udp	SNMP	XMS Server	No
162 udp	SNMP Traphost Note - Up to four Traphosts may be configured.	XMS Server	Yes - but required by XMS
443 tcp	HTTPS (WMI,WPR)	Client	Yes
514 udp	Syslog	Syslog Server	No
1812, 1645 udp	RADIUS (some servers use 1645)	RADIUS Server	Yes
1813, 1646 udp	RADIUS Accounting (some servers still use 1646)	RADIUS Accounting Server	Yes
2055 udp	Netflow	Client	Yes
5000 tcp	Virtual Tunnel	VTUN Server	Yes
22610 udp	XRP (Xirrus Roaming)	Arrays	Yes
22612 udp	Xircon (Console Utility)	Admin Workstation	Yes

Port	Application	Peer	Configurable
XMS			
icmp	Ping	Arrays	No
22 tcp	SSH	Arrays	Yes
25 tcp	SMTP	Mail Server	Yes
123 udp	NTP	NTP Server	No
161 udp	SNMP	Arrays	No
162 udp	SNMP Traphost 1	Arrays	Via XMS config file
443 tcp	HTTPS	Arrays	No
514 udp	Resident Syslog server	Internal*	Via XMS config file
1099 tcp	RMI Registry	Internal*	No
2000 tcp	XMS Back-end Server	Internal*	No
3306 tcp	MySQL Database	Internal*	No
8001 tcp	Status Viewer	Internal*	No
8007 tcp	Tomcat Shutdown	Internal*	During installation
8009 tcp	Web Container	Internal*	During installation
9090 tcp	XMS Webserver	XMS client	During installation
9091 tcp	XMS Client Server	XMS client	Via XMS config file
9092 tcp	XMS Client Server	XMS client	Via XMS config file
9443 tcp	XMS WMI SSL	XMS web client	No
* Internal to XMS Server, no ports need to be unblocked on other network devices			

See Also

Management Control

External Radius

Services

VLAN Management

Network Management Planning

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

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

See Also

Failover Planning

Power Planning

Security Planning

WDS Planning

WDS (Wireless Distribution System) creates wireless backhauls between Arrays, allowing your wireless network to be expanded using multiple Arrays without the need for a wired backbone to link them (see Figure 25). WDS features include:

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

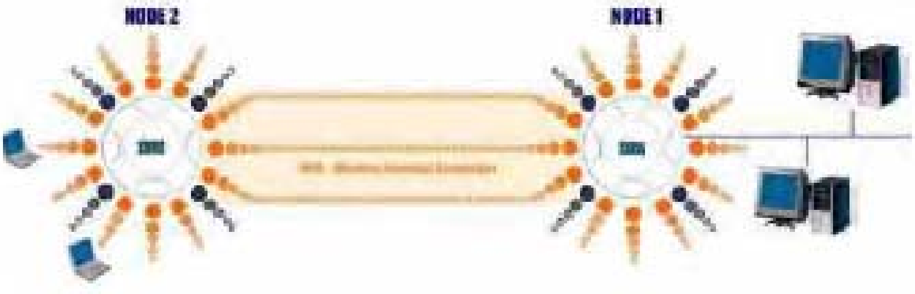


Figure 25. WDS Link

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

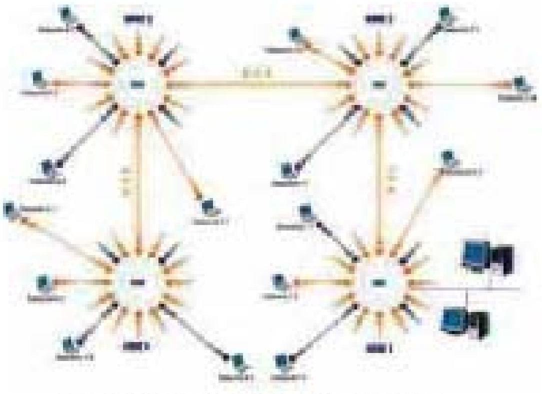


Figure 26. A Multiple Hop WDS Connection

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

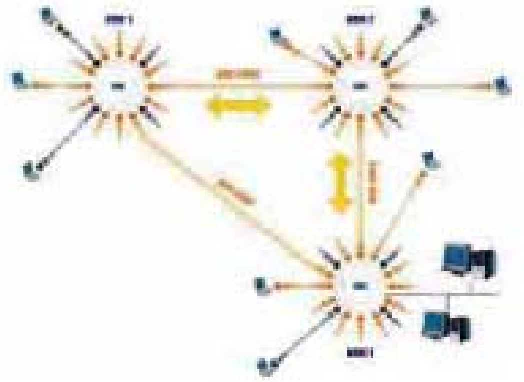


Figure 27. WDS Failover Protection

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

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

WDS configuration is performed only on the client-side Array. See "WDS" on page 338. Note that both Arrays must be configured with the same SSID name.

Common Deployment Options

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

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

See Also

Coverage and Capacity Planning

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.

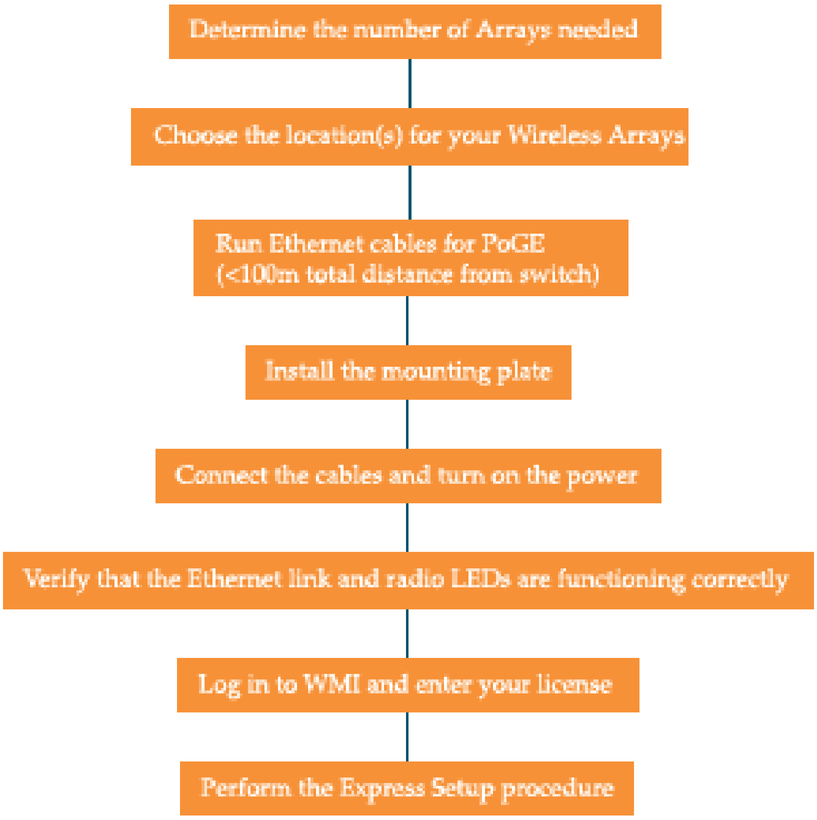

Determine the number of Arrays needed
Choose the location(s) for your Wireless Arrays
Run Ethernet cables for PoGE
(<100m total distance from switch)
Install the mounting plate
Connect the cables and turn on the power
Verify that the Ethernet link and radio LEDs are functioning correctly
Log in to WMI and enter your license
Perform the Express Setup procedure

Figure 28. Installation Workflow

See Also

Coverage and Capacity Planning

Common Deployment Options

Failover Planning

Installation Prerequisites

Planning Your Installation

Power Planning

Wireless Array Product Overview

Security Planning

Installing Your Wireless Array

This section provides instructions for completing a physical installation of your Xirrus Wireless Array.

Choosing a Location

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

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

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

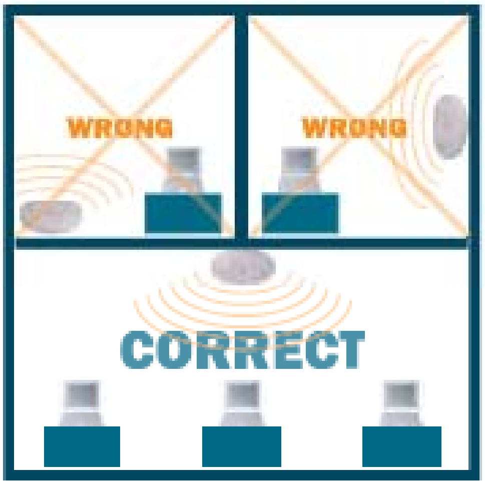


Figure 29. Array Placement

Wiring Considerations

Before using the Xirrus-supplied Power over Gigabit Ethernet modules (PoGE) to distribute power, see "Power over Gigabit Ethernet (PoGE)" on page 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 to the Array is required when using PoGE modules. The PoGE module requires a dedicated AC power outlet (100 - 240 VAC).

Network

- Gigabit POE1—If using PoGE modules, the total of all Cat 5e or Cat 6 cable segments from the Gigabit Ethernet switch to an Array Ethernet port must be less than 100m long. The Array must be connected to PoGE networks without routing cabling to the outside plant, to ensure that cabling is not exposed to lightning strikes or possible high voltage crossover.
- Gigabit POE2—For Arrays with a second POE port, the same restrictions listed above apply.(optional, not available on the four-port Arrays)
- Fast Ethernet (optional, not available on the four-port Arrays)
- Serial cable (optional) — cable lengths up to 25′ per the RS-232 specification.

Important Notes About Network Connections

Read the following notes before making any network connections.

When the unit's IP address is unknown or a network connection has not been established, the serial cable is used for connecting directly with the Command Line Interface (CLI) via HyperTerminal. When a network connection is established, the Array can be managed from any of the available network connections, either Fast Ethernet, Gigabit 1 or Gigabit 2. For the XR-1000, the Xirrus Xircon utility may be used locally to set up an IP address if necessary.

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

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

The 10/100 Ethernet Port may be used for managing the Array out of band from the Gigabit Ethernet ports. The 10/100 port will route only management traffic, using a static route that may be configured for this interface. See "interface" on page 407.

See Also

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

Mounting the Array

A number of options are available for mounting Arrays:

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

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

Dismounting the Array

To dismount any other Array model

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

Powering Up the Wireless Array

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

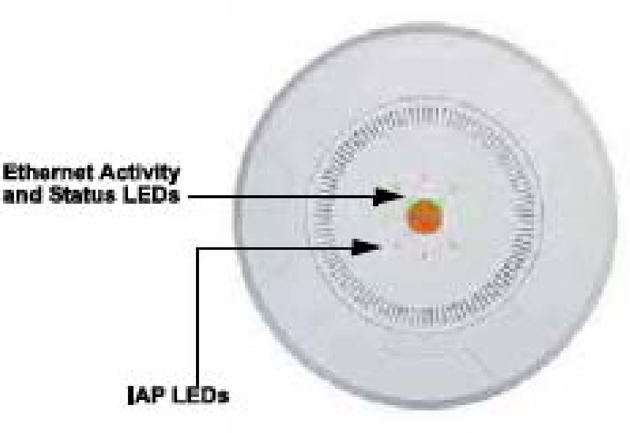


Figure 30. LED Locations

Array LED settings may be altered or disabled entirely for diagnostic purposes or for personal preference. Changes are made via the Array's Command Line Interface or the Web Management Interface—refer to "LED Settings" on page 334.

Array LED Operating Sequences

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

- "LED Boot Sequence" on page 64
- "LED Operation when Array is Running" on page 65

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 ON	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 334.

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 334 or via the CLI.

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

See Also

Installation Prerequisites
Installation Workflow
Installing Your Wireless Array
LED Settings

Establishing Communication with the Array

The Array may be configured through the Command Line Interface (CLI) using SSH, or on a browser via the graphical Web Management Interface (WMI). You may use the CLI via the serial management port (console—on all Arrays except the XR-500 and XR-1000 Series), the Fast Ethernet port, or any of the Gigabit Ethernet ports. You can use the WMI via any of the Array's Ethernet ports.

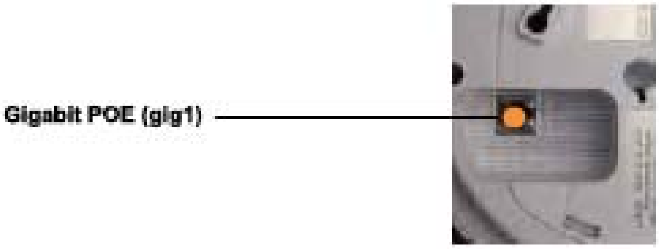


Figure 31. Network Interface Ports—XR-1000 Series

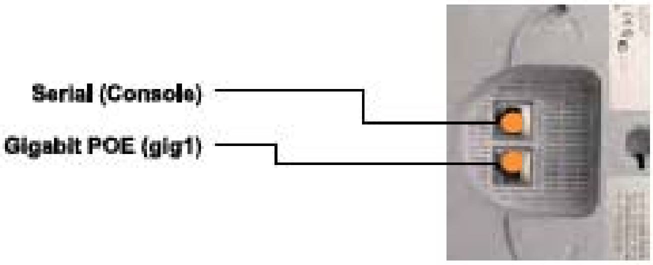


Figure 32. Network Interface Ports—XR-2000 Series

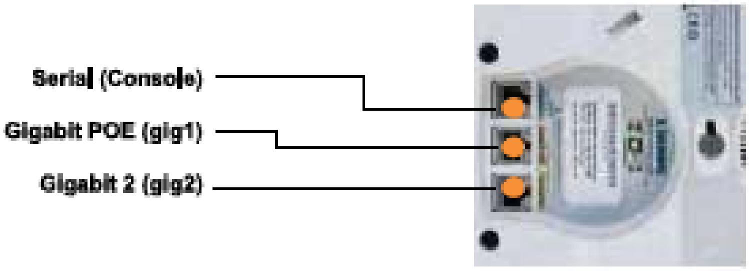


Figure 33. Network Interface Ports—XR-4000 Series

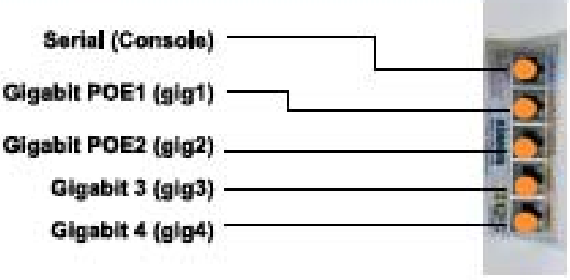


Figure 34. Network Interface Ports—XR-6000 Series

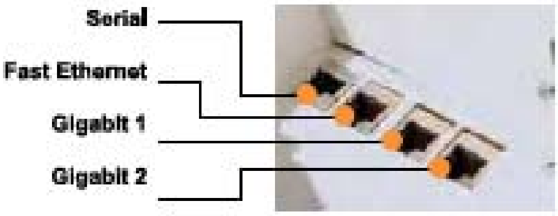


Figure 35. Network Interface Ports

The Xirrus Xircon utility may also be used to communicate with Arrays locally as an alternative to using a serial connection to the console. This is especially useful for the XR-500 and XR-1000 Series, which do not have a console port. See "Securing Low Level Access to the Array" on page 78.

Using the Serial Port

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

Using the Ethernet Ports

By default, the Array's Ethernet interfaces use DHCP to obtain an IP address. If the Array is booted and does not receive DHCP addresses on either the Fast Ethernet or Gigabit Ethernet ports, then the Fast Ethernet port will default to an

IP address of 10.0.1.1 and both Gigabit1 and its bonded pair port (if any) will default to 10.0.2.1 with a mask of 255.255.255.0.

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

1. The simplest way to address the Array is using its default hostname which is the Array's serial number (for example, XR4012N0823091CACD). If your network provides DHCP and DNS, then you can use this hostname.
2. Otherwise, examine the DHCP tables on the server and find the addresses assigned to the Array (Xirrus MAC addresses begin with 000F7D).
3. Alternatively, you may query the Array using the CLI via the console port (on all models except the wall-1000 series). Log in using the default user name **admin** and password **admin**. Use the **show ethernet** command to view the IP addresses assigned to each port.
4. If the Array cannot obtain an IP address via DHCP, the factory default uses a static IP address of 10.0.2.1 with a mask of 255.255.255.0 on its Gigabit POE port.

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

To connect to the Array, you must set your laptop to be in the same subnet as the Array: set your laptop's IP address to be in the 10.0.2.xx subnet, and set its subnet mask to 255.255.255.0. If this subnet is already in use on your network, you may connect your laptop directly to the Array by connecting the laptop to the power injector's IN port temporarily (this port may be called the SWITCH port or the DATA port on your injector).

Starting the WMI

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

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

Logging In

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

See Also

Installation Workflow
Performing the Express Setup Procedure
Powering Up the Wireless Array

Entering the License

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

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

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

1. This procedure assumes that you have pointed a browser to the Array's IP address to start WMI, and that you have logged in with the default username and password above.

2. In the left hand frame, in the **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.

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

Performing the Express Setup Procedure

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

Figure 36. Express Setup

Procedure for Performing an Express Setup

1. **Host Name**: Specify a unique host name for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is **Xirrus-WiFi-Array**.

2. **Location Information**: Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.

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

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

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

6. **License Key**: If Xirrus issued you a license that differs from the current value shown, enter it now. See also, "Entering the License" on page 69.

7. Configure **SNMPv2**: Select whether to **Enable** SNMPv2 on the Array, and change the **SNMP Community Strings** if desired. If you are using the Xirrus Management System (XMS), these strings must match the values used by XMS. The default values for the Array match the defaults in XMS. For more details, including SNMPv3, see "SNMP" on page 194.

8. Configure the **Fast Ethernet** (10/100 Megabit) and **Gigabit** network interfaces. The fields for each of these interfaces are the same, and include:

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

   b. **Allow Management on Interface**: Choose **Yes** to allow management of the Array via this network interface, or choose **No** to deny all management privileges for this interface.

For improved security, you should also take the additional steps described in "Securing Low Level Access to the Array" on page 78.

c. **Configuration Server Protocol**: Choose **DHCP** to instruct the Array to use DHCP to assign IP addresses to the Array's Ethernet interfaces, or choose **Static** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following **IP Settings**:

- **Address**: Enter a valid IP address for this Array. To use any of the remote connections (Web, SNMP, or SSH), a valid IP address must be used.
- **Subnet Mask**: Enter a valid IP address for the subnet mask (the default is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
- **Default Gateway**: Enter a valid IP address for the default gateway. This is the IP address of the router that the Array uses to forward data to other networks.
- Click the **Apply** button for this interface when done making IP changes.

9. **SSID Settings**: This section specifies the wireless network name and security settings.

a. **SSID (Wireless Network Name)**: The SSID (Service Set Identifier) is a unique name that identifies a wireless network. All devices attempting to connect to a specific WLAN must use the same SSID. The default for this field is "**xirrus.**"

For additional information about SSIDs, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 452.

b. **Wireless Security**: Select the desired wireless security scheme (Open, WEP, WPA, WPA2, or WPA-Both). WPA2 is recommended for the best Wi-Fi security.

- **Open—**This option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.

- **WEP** (Wired Equivalent Privacy)—An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.
- **WPA** (Wi-Fi Protected Access)—A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1x for authentication.
- **WPA2** (Wi-Fi Protected Access 2)—WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.
- **WPA-Both** (WPA and WPA2)—This option makes use of both WPA and WPA2.

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

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

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

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

10. **Admin Settings:** This section allows you to change the default admin username, password, and privileges for the Array. You may change the password and leave the user name as is, but we suggest that you change both to improve Array security.

    a. **New Admin User (Replaces user "admin")**: Enter the name of a new administrator user account. Be sure to record the new account name and password, because the default **admin** user will be deleted! Note that the Array also offers the option of authenticating administrators using a RADIUS server (see "Admin Management" on page 214)).

For improved security, you should also take the additional steps described in "Securing Low Level Access to the Array" on page 78.

    b. **New Admin Privilege Level**: By default, the new administrator will have read/write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). If you wish the new account to have different privileges, select the desired level from the drop-down list. For more information about user privileges, please see "Admin Privileges" on page 216.

    c. **New Admin Password**: Enter a new administration password for managing this Array. If you forget this password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).

    d. **Confirm Admin Password**: If you entered a new administration password, confirm the new password here.

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

11. **Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you're not using a server.

    a. **Current Array Date and Time:** This read-only field shows the current time for your convenience.

b. **Time Zone**: Select your time zone from the choices available in the pull-down list.

c. **Auto Adjust Daylight Savings**: If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).

d. **Use Network Time Protocol**: Check this box if you want to use an NTP server to synchronize the Array's clock. Use of NTP is mandatory for Arrays to be managed with XMS (the Xirrus Management System), and ensures that Syslog time-stamping is maintained across all units. If you check **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, leave this box unchecked (default) and set the system time on the Array manually.

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

f. **NTP Primary Authentication**: If you are using authentication with NTP, select the type of key: **MD5 or SHA1**. Select **None** if you are not using authentication (this is the default). For more information on authenticated NTP, see "Time Settings (NTP)" on page 185.

g. **NTP Primary Authentication Key ID**: Enter the key ID, which is a decimal integer.

h. **NTP Primary Authentication Key**: Enter your key, which is a string of characters.

i. **NTP Secondary Server**: Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

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

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

12. **Quick Configuration**: This offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate to your deployment, select it and click **Apply**. For example, the **High-Density** option uses best practices to configure the Array for high density settings such as lecture halls, convention centers, stadiums, etc.

13. **IAP Settings**:

    Enable/Configure All IAPs: Click on the **Execute** button to enable and auto configure all IAPs (a message displays the countdown time—in seconds—to complete the auto-configuration task). When an IAP is enabled, its LED is switched on. (Figure 37, see also "Array LED Operating Sequences" on page 64.)

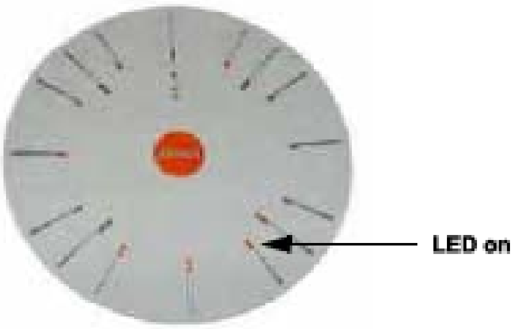


Figure 37. LEDs are Switched On

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

    This ends the Express Setup procedure.

See Also

Establishing Communication with the Array
Installation Prerequisites
Installation Workflow
Logging In
Multiple SSIDs
Security

Securing Low Level Access to the Array

Most management of the Xirrus Array is done via the Web Management Interface (WMI) as you just saw in "Performing the Express Setup Procedure" on page 71. Another often used option is CLI—see "The Command Line Interface" on page 377. The Array also has a lower level interface: XBL (Xirrus Boot Loader), which allows access to more primitive commands. You won't normally use XBL unless instructed to do so by Xirrus Customer Support. For proper security, you should replace the default XBL login username and password with your own, as instructed below. XBL has its own username and password, separate from the ArrayOS Admin User and Password (used for logging in to the WMI and CLI) that you changed in Step 10 on page 75.

Xirrus also provides the Xircon utility for connecting to Xirrus XR Arrays that are not reachable via the normal access methods (such as SSH or WMI) and that do not have a physical console port (XR-500 and XR-1000 Series Arrays), 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 67. Xircon may be needed in special circumstances as directed by Xirrus Customer Support for troubleshooting Array problems or IP connectivity. (In this case, see the *Xircon User Guide* for detailed information.)

Xircon access to the Array may be controlled:

- You may enable or disable all Xircon access to the Array as instructed in the procedure below. There are also options to allow access only to CLI (i.e., ArrayOS access) or only to XBL.
- Since XR-500 and XR-1000 Array models do not have a console port, these models have Xircon access to both XBL and CLI enabled by default. For Arrays that do not have a console port, to avoid potentially being locked out of the Array, Xircon should always be enabled at the XBL level at least.

! *If you disable Xircon access to both XBL and CLI on XR-1000 models, 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 371). Skip to Step 4 on page 80.

   To access CLI via SSH, see "Establishing a Secure Shell (SSH) Connection" on page 377. Then proceed to the next step.

2. At the **login as** prompt, log in to CLI using the username and password that you set in Step 10 on page 75.

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

   Xirrus Wi-Fi Array
   ArrayOS Version 6.1.2-3299
   Copyright (c) 2005-2012 Xirrus, Inc.
   http://www.xirrus.com

   XR4012802207C#
   ```

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

   ```
   hostname#configure
   ```

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

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

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

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

   <management-status> may be one of :

   - **on** enables both CLI and XBL access

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

Note that there is a WMI setting for changing Xircon access, timeout period, and the UDP port used. This may be used instead of CLI if you wish. See "Management Control" on page 221. Note that you cannot change the XBL username and password via the WMI.

The Web Management Interface

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

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

An Overview

The WMI is an easy-to-use graphical interface to your Wireless Array. It allows you to configure the product to suit your individual requirements and ensure that the unit functions efficiently and effectively. Options allow you to choose among different appearances for the WMI. See "Options" on page 373.

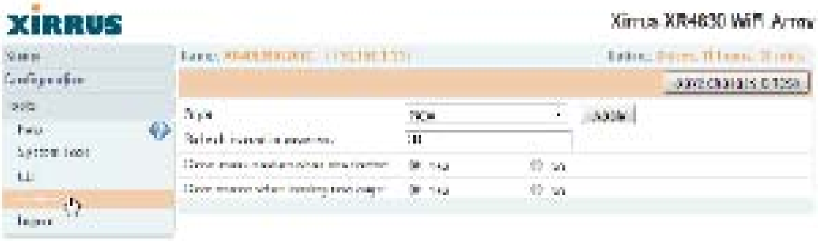


Figure 38. Web Management Interface—Option = New Style

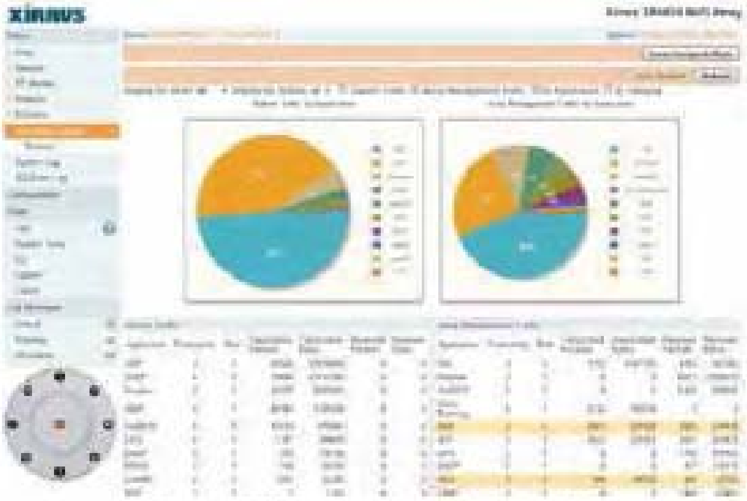
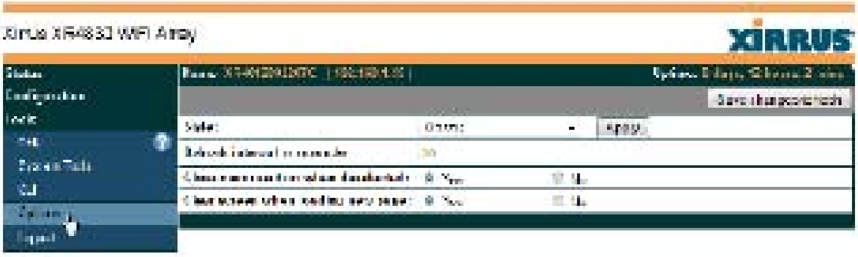


Figure 39. Web Management Interface—New Style



Xirrus XR4830 WiFi Array

Name: [illegible] | [illegible] |

Uptime: [illegible] days, [illegible] hours, [illegible] mins

Style: Classic ▾

Refresh interval in seconds: 20

Clear menu entries [illegible] dashboard: ● Yes ○ No

Clear screen when loading new page: ● Yes ○ No

Figure 40. Web Management Interface—Option = Classic Style

Figure 41. Web Management Interface—Classic Style

Structure of the WMI

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

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

- Statistics Windows
  - IAP Statistics Summary
  - Per-IAP Statistics
  - Network Statistics
  - VLAN Statistics
  - WDS Statistics
  - IDS Statistics
  - Filter Statistics
  - Station Statistics
  - Per-Station Statistics
- Application Control Windows
- System Log Window
- IDS Event Log Window

Configuration Windows

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

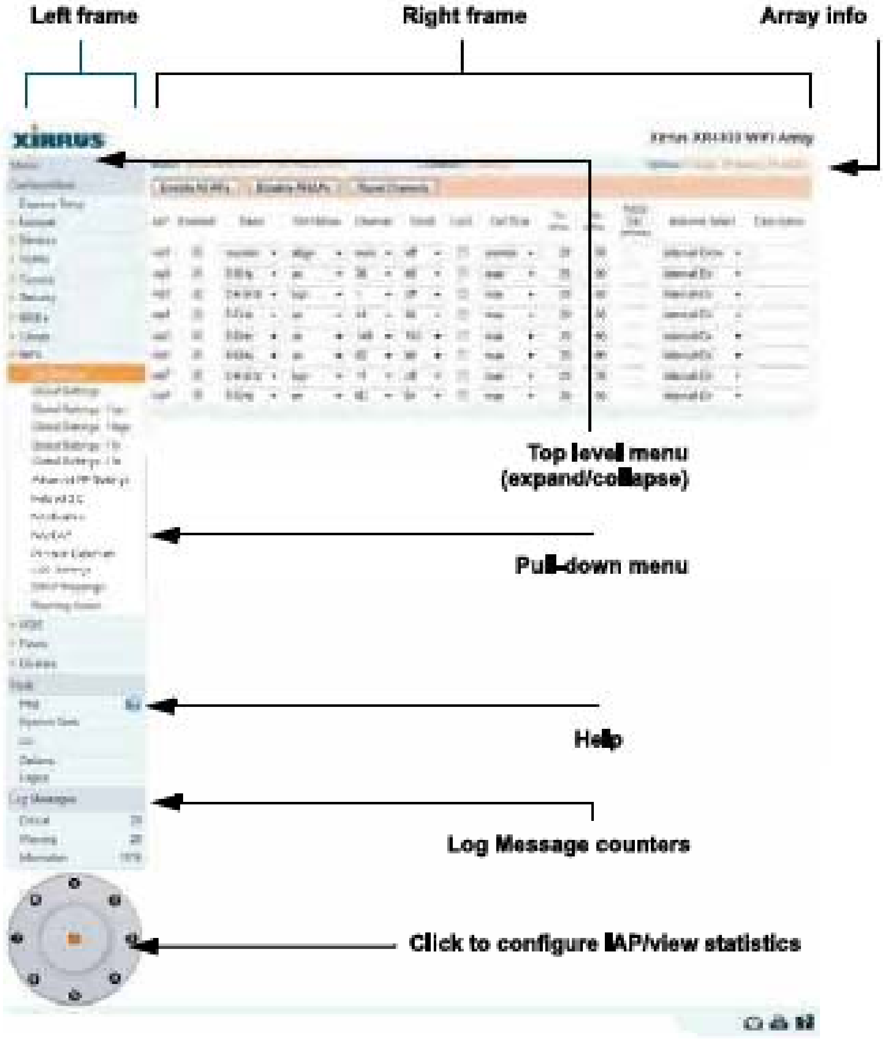
Configuration Windows (cont'd)

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

Tool Windows

- System Tools
- CLI
- Options
- Logout

User Interface



Left frame
Right frame
Array info
Top level menu (expand/collapse)
Pull-down menu
Help
Log Message counters
Click to configure IAP/view statistics

Figure 42. WMI: Frames

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

The left frame contains three main elements:

- Menu organized by function (for example, Network, SSIDs, Security, etc.). Click a heading, such as **Network**, to display a summary of its current configuration, as well as an associated pull-down menu. The three major menu sections (**Status**, **Configuration**, **Tools**) may each be collapsed down to hide the headings under them. Click again to display the headings. (Figure 43)
- 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 156.
- The Array representation contains shortcut links. Click a radio to view statistics for it. Click the center of the Array to display the IAP Settings window, which allows you to configure the Array's radios.

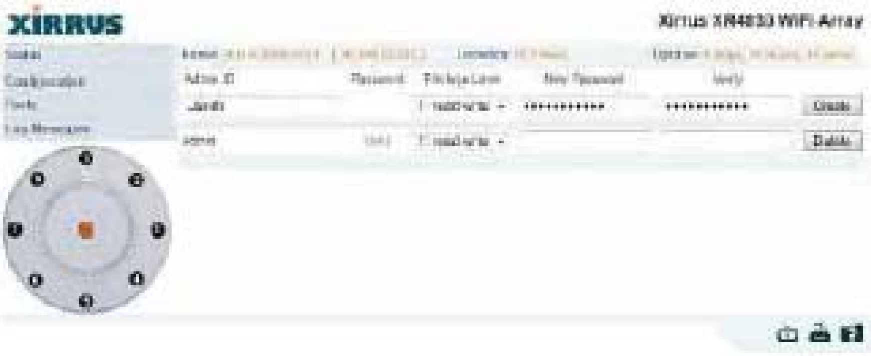


Figure 43. Major Menu Sections Collapsed (on left)

The right frame displays the status information or configuration parameters for the Wireless Array. This is where you review the Array's current status and activity or input data (if you want to make changes). The green Array information bar at the top of the frame describes the Array—the Name and IP address allow you to quickly confirm that WMI is connected to the correct Array. The current Uptime since the last reboot is also shown.

Some settings are only available if the Array's license includes appropriate Xirrus ***Advanced Feature Sets****. If a setting is unavailable (grayed out), then your license does not support the feature. See* ***"About Licensing and Upgrades" on page 361****.*

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

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

See "Options" on page 373 for more information.

Utility Buttons

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

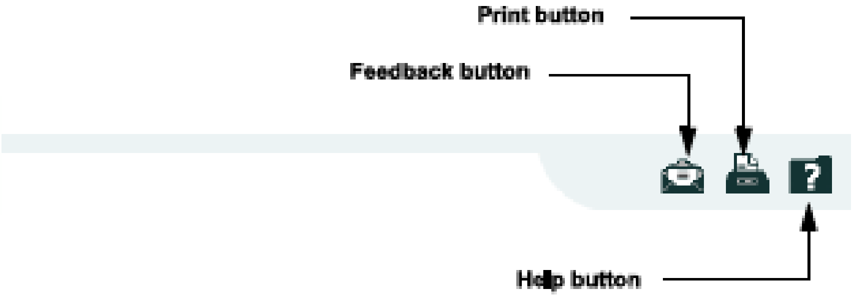


Figure 44. WMI: Utility Buttons

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

Submitting Your Comments

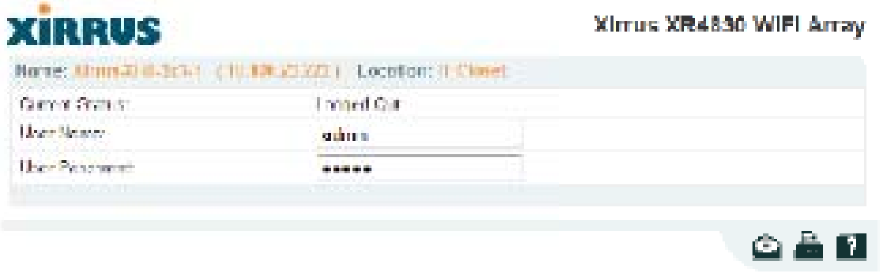
When submitting comments via the Feedback button (ensure that you provide as much detail as possible, including your contact information, the product model number that the comment relates to, and the ArrayOS software version (if known). When finished, click on the **Submit** button to submit your comment.

Logging In

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

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

   Otherwise, enter the Array's IP address. This may be determined as described in "Using the Ethernet Ports" on page 67.
3. To log in to the Array's Web Management Interface, enter **admin** for both the user name and password.



Xirrus XR4830 WIFI Array

Name: [illegible] ([illegible]) Location: [illegible]

Current Status:	Logged Out
User Name:	admin
User Password:	*****

Figure 45. Logging In to the Wireless Array

Applying Configuration Changes

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

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

Character Restrictions

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

& < > ' " / \

Viewing Status on the Wireless Array

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

- **"Array Status Windows" on page 96**
- **"Network Status Windows" on page 103**
- **"RF Monitor Windows" on page 114**
- **"Station Status Windows" on page 125**
- **"Statistics Windows" on page 140**
- **"Application Control Windows" on page 150**
- **"System Log Window" on page 156**
- **"IDS Event Log Window" on page 157**

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

- **"Configuring the Wireless Array" on page 159**
- **"Using Tools on the Wireless Array" on page 359**

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 43 on page 89)

Array Status Windows

The following Array Status windows are available:

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

Array Summary

This is a status only window that provides a snapshot of the global configuration settings for all Wireless Array network interfaces and IAPs. You must go to the appropriate configuration window to make changes to any of the settings displayed here—configuration changes cannot be made from this window. Clicking on an interface or IAP will take you to the proper window for making configuration changes.

Figure 46. Array Summary

Content of the Array Summary Window

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

- **Ethernet Settings Summary**

  This section provides information about network interface devices. To make configuration changes to these devices, go to "Network Interfaces" on page 171.

  - **Interface**: Lists the network interfaces that are available on the Array.
  - **State**: Shows the current state of each interface, either enabled or disabled.
  - **Mgmt**: Shows whether Array management traffic is allowed on this interface.
  - **Auto Neg**: Shows whether auto-negotiation is in use on this interface, to determine settings for speed, parity bits, etc.
  - **LED**: Shows whether LED display of interface status is enabled.
  - **Link**: Shows whether the link on this interface is up or down.
  - **Duplex**: Shows whether full duplex mode is in use.
  - **Speed**: Shows the speed of this interface in Mbps.
  - **MTU Size**: Shows the Maximum Transmission Unit size that has been configured. This is the largest packet size (in bytes) that the interface can pass along.
  - **DHCP**: Shows whether DHCP on this port is enabled or disabled.
  - **IP Address**: Shows the current IP address assigned to each network interface device.
  - **Subnet Mask**: Shows the subnet mask, which defines the number of IP addresses that are available on the routed subnet where the Array is located.
  - **Gateway**: Shows the IP address of the router that the Array uses to transmit data to other networks.

- **Bond Settings Summary**

  This section provides information about the relationship that has been selected for the Gigabit ports. For detailed explanations and to make configuration changes, see "Network Bonds" on page 175.

  - **Bond**: Lists all network bonds that have been configured.
  - **Mode**: Shows the type of relationship that has been selected for the Gigabit ports.
  - **Ports**: Shows the Gigabit ports that are part of this bond.
  - **Port Mode**: Shows the relationship that has been selected for the Ethernet ports. See "Network Bonds" on page 175 for details
  - **Active VLANs**: Shows the VLANs that are active in this bond.
  - **Mirror**: Shows whether mirroring is enabled on this bond.

- **Integrated Access Points Section**

  This section provides information about the Integrated Access Points (IAPs) that are contained within the Array. How many IAPs are listed depends on which product model you are using. To make configuration changes to these IAPs, go to "IAP Settings" on page 274.

  - **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 47 shows an example where iap7 is down.
  - **AP Type**: Shows the types of 802.11 clients supported by this IAP (11/a/b/g/n) and the number of separate data streams transmitted and received by the antennas of each IAP for 802.11n. For example, 3x3 means that the IAP supports three transmit chains and three receive chains. See "Multiple Data Streams—Spatial Multiplexing" on page 38.

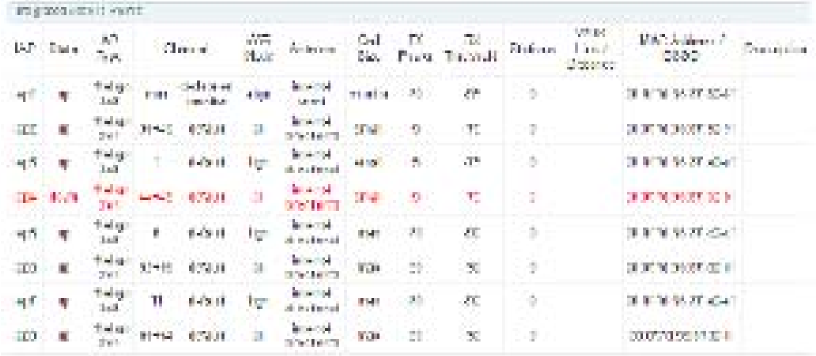


Figure 47. Disabled IAP (Partial View)

- **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 274.
- **Wi-Fi Mode**: Shows the 802.11 client types that the IAP has been configured to support.
- **Antenna**: Shows which antenna is being used by each IAP.
- **Cell Size**: Indicates which cell size setting is currently active for each IAP—small, medium, large, max, automatic, or manually defined by you. The cell size of an IAP is a function of its transmit power and determines the IAP's overall coverage. To define cell sizes, go to "IAP Settings" on page 274. 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 28.

Figure 48. IAP Cells

- **Tx Power**: Shows the transmit power for each IAP.
- **Rx Threshold**: Shows the receive threshold for each IAP.
- **Stations**: Informs you how many client stations are currently associated with each IAP.
- **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 338.
- **MAC Address/BSSID**: Shows the MAC address for each IAP.
- **Description**: The description (if any) that you set for this IAP.

Array Information

This is a status only window that shows you the current firmware versions utilized by the Array, serial numbers assigned to each module, MAC addresses, licensing information, recent boot timestamps, and current internal temperatures and fan speed.

Note that the **License Features** row lists the features that are supported by your Array's license. See "About Licensing and Upgrades" on page 361 and "Advanced Feature Sets" on page 16 for more information.

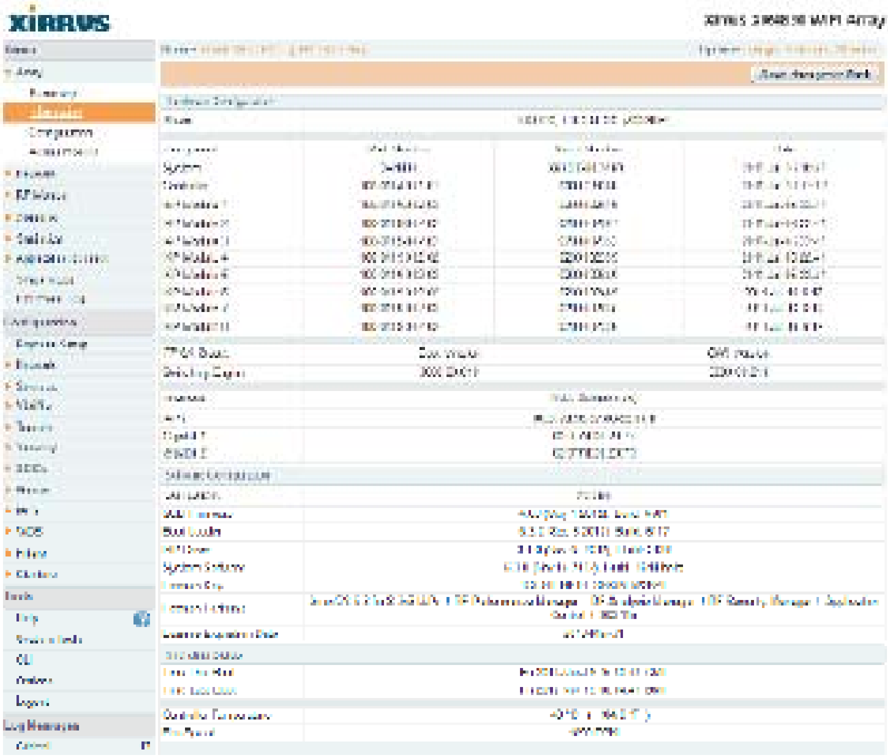


Figure 49. Array Information

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.

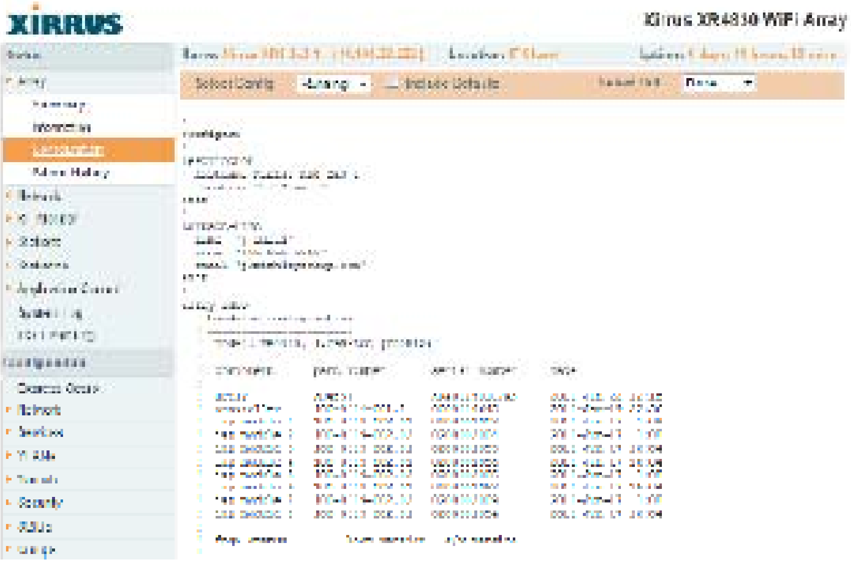


Figure 50. Show Configuration

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

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

Admin History

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

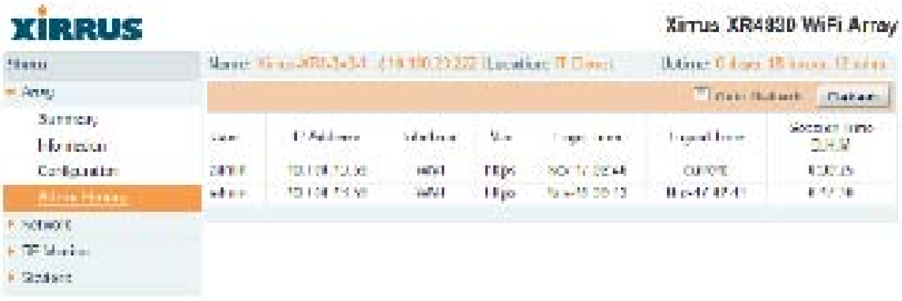


Figure 51. Admin Login History

Network Status Windows

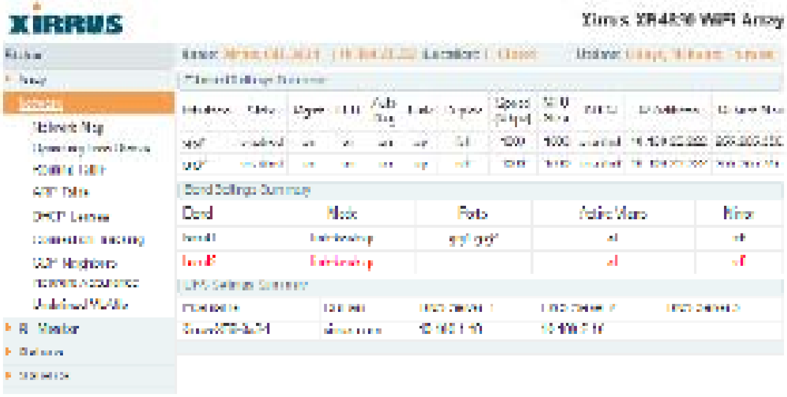
The following Network Status windows are available:

- **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.



Ethernet Settings Summary

Interface	State	[illegible]	[illegible]	Auto Neg	Link	Duplex	Speed (Mbps)	MTU Size	DHCP	IP Address	Subnet Mask
gig1	enabled	[illegible]	[illegible]	[illegible]	up	full	1000	1500	enabled	[illegible]	[illegible]
gig2	enabled	[illegible]	[illegible]	[illegible]	up	full	1000	1500	enabled	[illegible]	[illegible]

Bond Settings Summary

Bond	Mode	Ports	Active Mirror	Mirror
bond1	load-balancing	gig1 gig2	off	off
bond2	load-balancing		off	off

DNS Settings Summary

Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3
[illegible]	[illegible]	[illegible]	[illegible]	

Figure 52. Network Settings

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

- **"Network Interfaces" on page 171**
- **"Network Bonds" on page 175**
- **"DNS Settings" on page 181**
- **"CDP Settings" on page 183**

Network Map

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

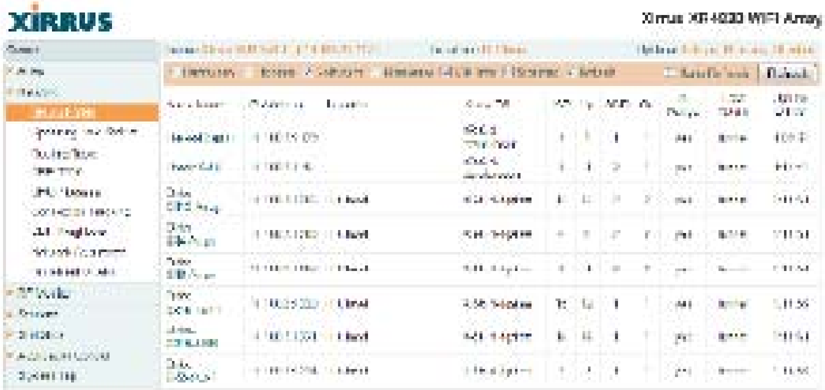


Figure 53. Network Map

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 161. 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 161.
- **Location**: The location assigned to the Array. To establish the location information, go to "Express Setup" on page 161.
- **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 161. To enable or disable individual IAPs, go to "IAP Settings" on page 274.
- **SSID**: Informs you how many SSIDs have been assigned for the Array. To assign an SSID, go to "SSID Management" on page 249.
- **(SSID) On**: Informs you how many SSIDs are enabled. To enable or disable SSIDs, go to "SSID Management" on page 249.
- **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 280.
- **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 optional features enabled by the key, if any.

Software (enabled by default)

- Enable/disable display of the Array OS column.

Firmware

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

IAP Info (enabled by default)

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

Stations

- **Stations**: Tells you how many stations are currently associated to each Array. To deauthenticate a station, go to "Stations" on page 126.

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

Default

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

Spanning Tree Status

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

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

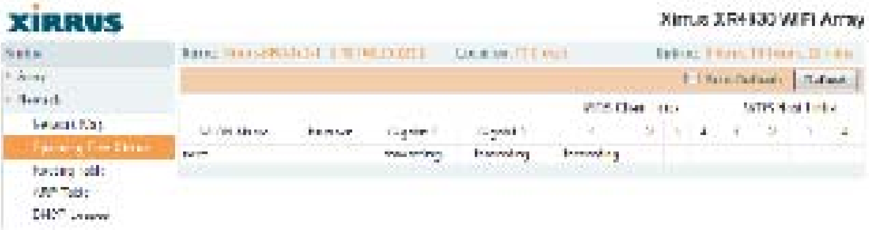


Figure 54. Spanning Tree Status

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

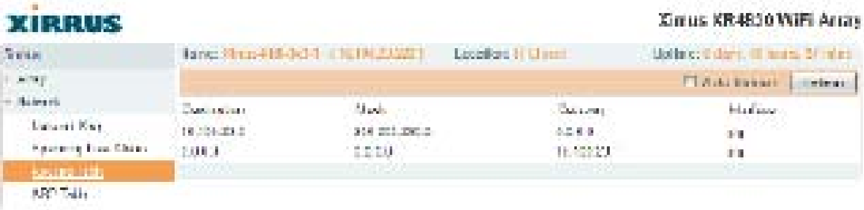
Network Status Windows

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
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

Figure 55. Routing Table

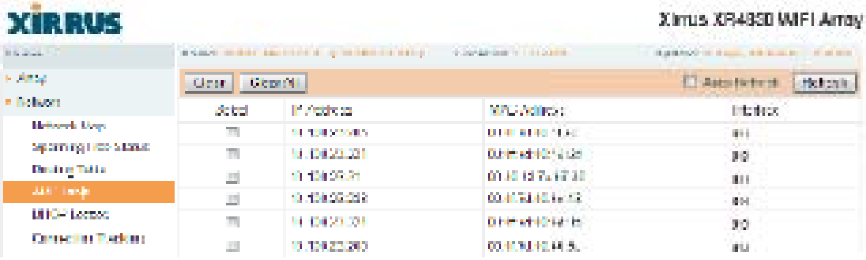
See Also

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
□	[illegible]	[illegible]	[illegible]
□	[illegible]	[illegible]	[illegible]
□	[illegible]	[illegible]	[illegible]
□	[illegible]	[illegible]	[illegible]
□	[illegible]	[illegible]	[illegible]
□	[illegible]	[illegible]	[illegible]

Figure 56. ARP Table

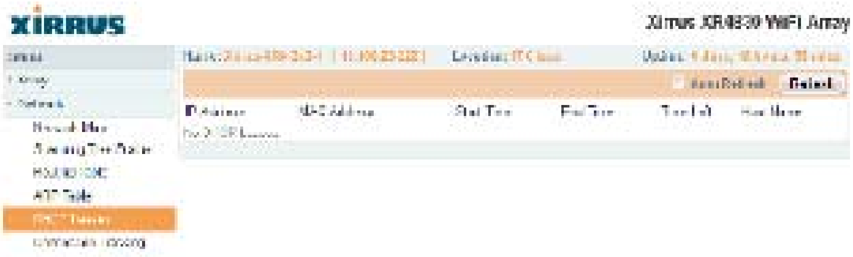
See Also

Routing Table

ARP Filtering

DHCP Leases

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



IP Address	MAC Address	Start Time	End Time	Time Left	Host Name
No DHCP Leases					

Figure 57. DHCP Leases

See Also

DHCP Server

Connection Tracking/NAT

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

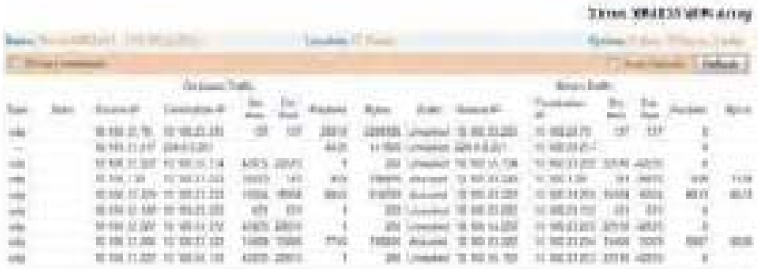


Figure 58. Connection Tracking

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

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

See Also

Filters

CDP Neighbors

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

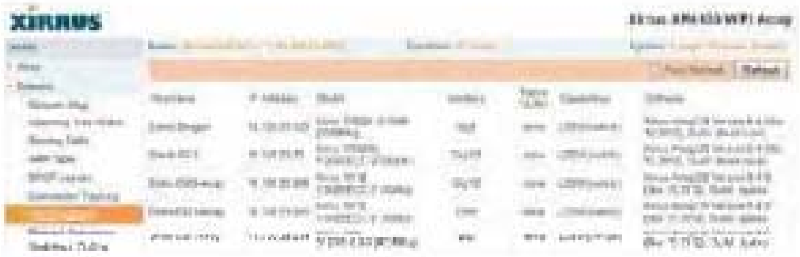


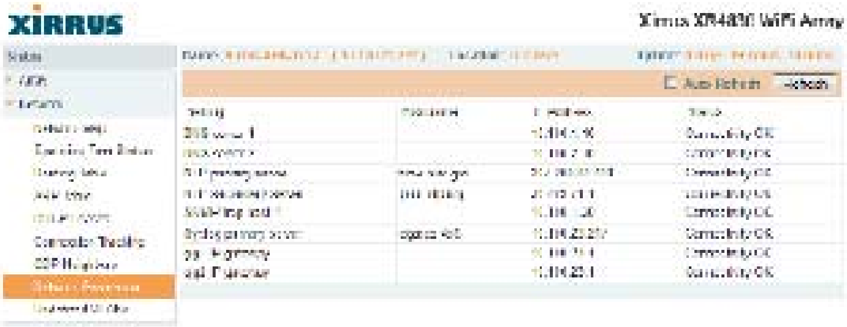
Figure 59. CDP Neighbors

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 183.

Network Assurance

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



Testing	Host name	IP Address	Status
DNS server 1		[illegible]	Connectivity OK
DNS server 2		[illegible]	Connectivity OK
NTP primary server	[illegible]	[illegible]	Connectivity OK
NTP secondary server	[illegible]	[illegible]	Connectivity OK
SNMP trap host 1		[illegible]	Connectivity OK
Syslog primary server	[illegible]	[illegible]	Connectivity OK
[illegible]		[illegible]	Connectivity OK
[illegible]		[illegible]	Connectivity OK

Figure 60. Network Assurance

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

Network assurance must be enabled on the Array in order to perform these connectivity tests and display this information. See "Management Control" on page 221.

See Also

Management Control

Undefined VLANs

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

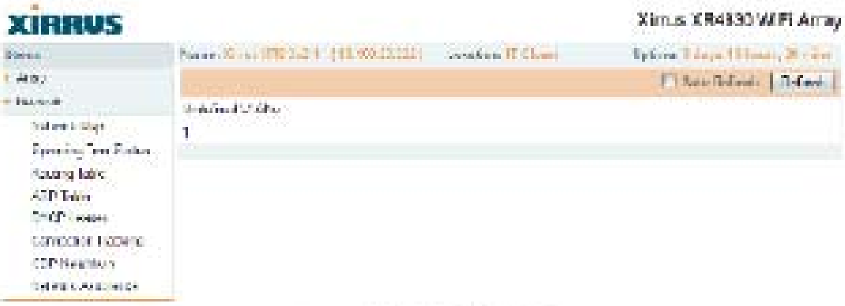


Figure 61. Undefined VLANs

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 284).

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.

Some status information is only available if the Array's license includes ***Advanced Feature Sets****. For example, the Spectrum Analyzer requires the* ***Xirrus Advanced RF Analysis Manager*** *(RAM). If a feature is unavailable, then your license does not support the feature and you will get an error message if you try to set the feature. See* ***"About Licensing and Upgrades" on page 361****.*

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

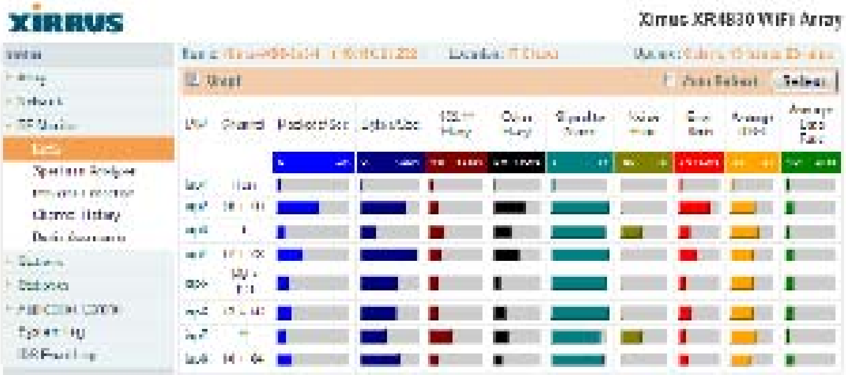
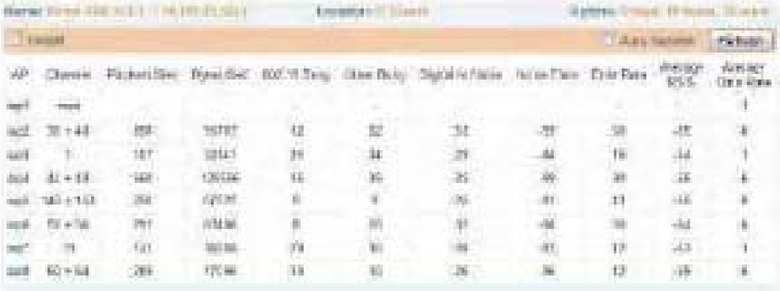


Figure 62. RF Monitor—IAPs

Figure 62 presents the data as a graphical display, enabled by selecting the **Graph** checkbox on the upper left. If this option is not selected, data is presented as a numerical table.



IAP	Channel	Packets/Sec	Bytes/Sec	802.11 Busy	Other Busy	Signal to Noise	Noise Floor	Error Rate	Average RSSI	Average Data Rate
iap1	[illegible]									1
iap2	36 + 40	[illegible]	[illegible]	12	32	33	[illegible]	[illegible]	[illegible]	6
iap3	1	187	[illegible]	[illegible]	34	29	-64	16	-34	1
iap4	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	35	[illegible]	[illegible]	[illegible]	6
iap5	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	-91	11	[illegible]	6
iap6	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	6
iap7	11	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	17	[illegible]	1
iap8	60 + 64	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	12	[illegible]	6

Figure 63. 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.

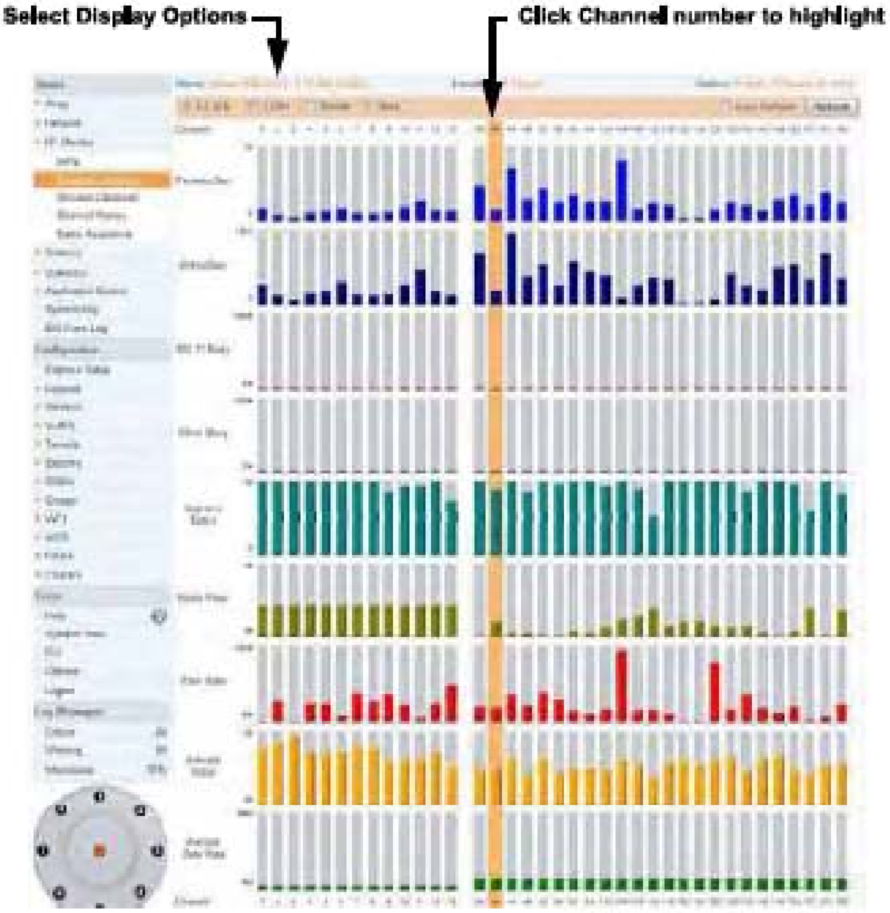
Spectrum Analyzer

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 274.*

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 64 (the default presentation), or horizontally as bar graphs or numerical RF measurements. The measurements displayed are explained in "Spectrum Analyzer Measurements" on page 118.

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



Select Display Options

Click Channel number to highlight

Figure 64. 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 331.

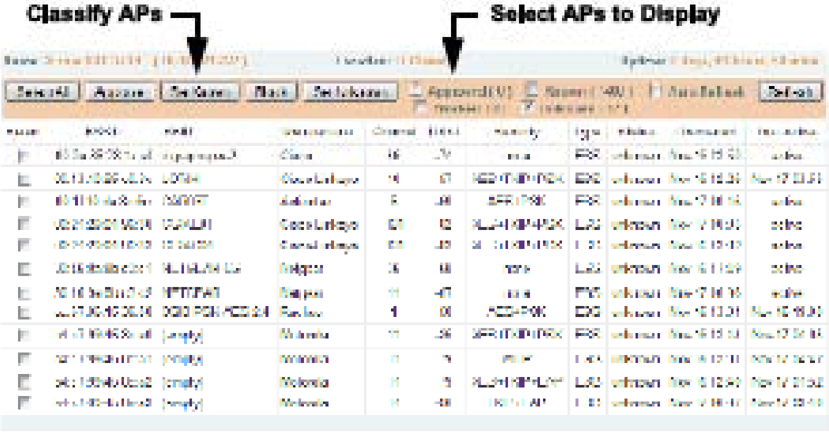


Figure 65. Intrusion Detection/Rogue AP List

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

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

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

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

See Also

Network Map
Rogue Control List
SSIDs
SSID Management

Channel History

The RF Monitor—Channel History window focuses on traffic statistics and RF readings observed for just one channel that you select in the **Channel** field. A new set of readings is added every 10 seconds for a 5 GHz channel, or every 5 seconds for a 2.4 GHz channel. For descriptions of the measurements displayed, please see "Spectrum Analyzer Measurements" on page 118.

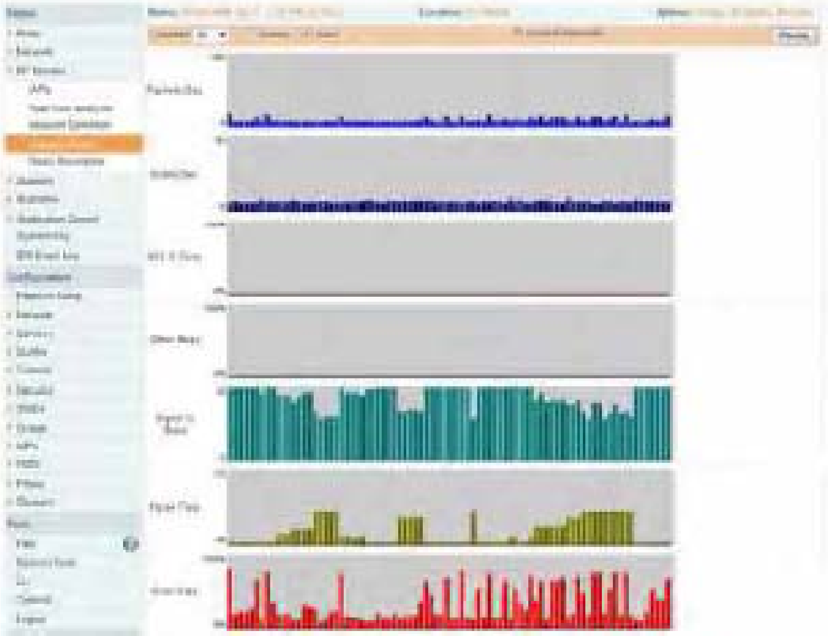


Figure 66. RF Monitor—Channel History

Figure 66 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 67)

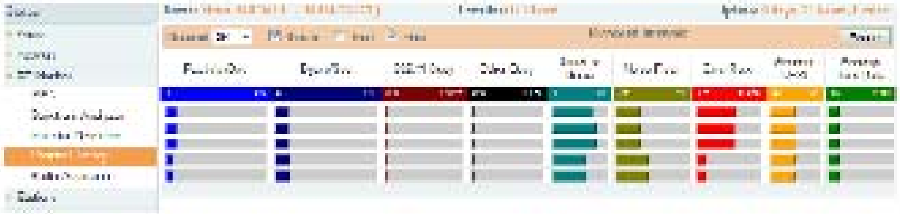


Figure 67. RF Monitor—Channel History (Rotated)

If you select **Rotate** and **Text** together, data is presented as a numerical table. (Figure 68)

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

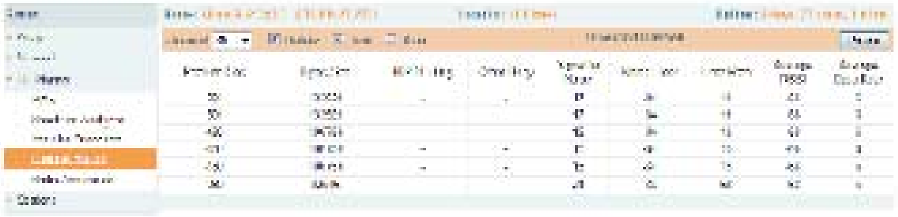


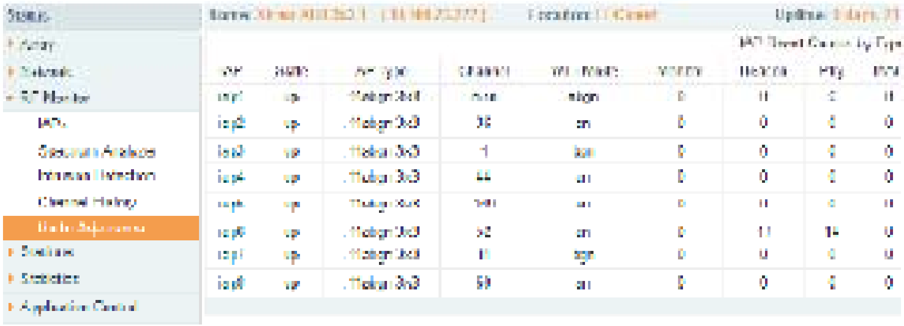
Figure 68. RF Monitor—Channel History (Text)

Radio Assurance

Radio Assurance mode is only available if the Array's license includes the ***Xirrus Advanced RF Analysis Manager (RAM).*** *If a setting is unavailable (grayed out), then your license does not support the feature. Please see* ***"About Licensing and Upgrades" on page 361****.*

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 315. 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 461.



IAP	State	IAP Type	Channel	WiFi Mode	[illegible]	[illegible]	[illegible]	[illegible]
iap1	up	abgn 3x3	mon	abgn	0	0	0	0
iap2	up	abgn 3x3	36	an	0	0	0	0
iap3	up	abgn 3x3	1	bgn	0	0	0	0
iap4	up	abgn 3x3	44	an	0	0	0	0
iap5	up	abgn 3x3	149	an	0	0	0	0
iap6	up	abgn 3x3	52	an	0	11	14	0
iap7	up	abgn 3x3	11	bgn	0	0	0	0
iap8	up	abgn 3x3	56	an	0	0	0	0

Figure 69. Radio Assurance

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

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

See Also

IAPs
Xirrus Advanced RF Analysis Manager (RAM)
RF Resilience
Radio Assurance

Station Status Windows

The following Station Status windows are available:

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

Some status information is only available if the Array's license includes the ***Xirrus Advanced RF Analysis Manager (RAM)****. If a feature is unavailable, then your license does not support the feature and you will get an error message if you try to set the feature. See* ***"About Licensing and Upgrades" on page 361****.*

Stations

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

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

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

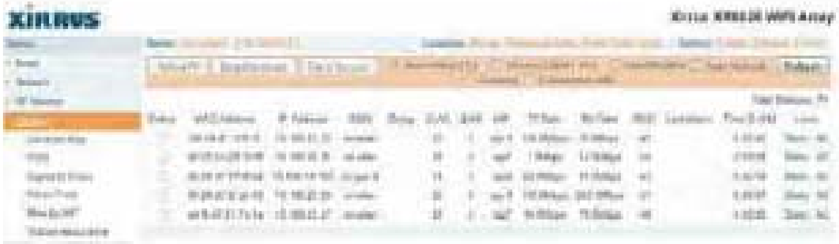


Figure 70. Stations

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

- **Deny Access:** Sends a de-authentication frame to the selected station and explicitly denies it access by adding its MAC address to the Deny List in the Access Control List window. To permit access again, go to "Access Control List" on page 227 and delete the station from the **Deny** list.
- **Deauthenticate:** Sends a de-authentication frame to the selected station. The station may re-authenticate.

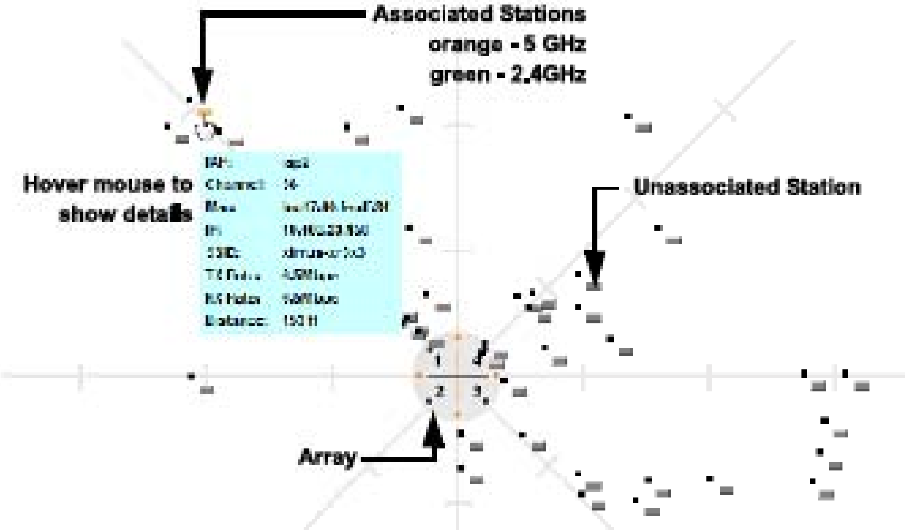
Click on the **Refresh** button to refresh the station list, or click in the **Auto Refresh** check box to instruct the Array to refresh this window automatically.

See Also

Access Control List
Station Status Windows

Location Map

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



IAP: [illegible]
Channel: [illegible]
Mac: [illegible]
IP: [illegible]
SSID: [illegible]
TX Rate: [illegible]
RX Rate: [illegible]
Distance: [illegible]

Figure 71. Location Map

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

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

You may replace the range-finder background image above with your own custom image of the floorplan of the area served by the Array—see "Working with the Custom Image" on page 131

Hover the mouse over a station to show detailed information. (Figure 71) 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.

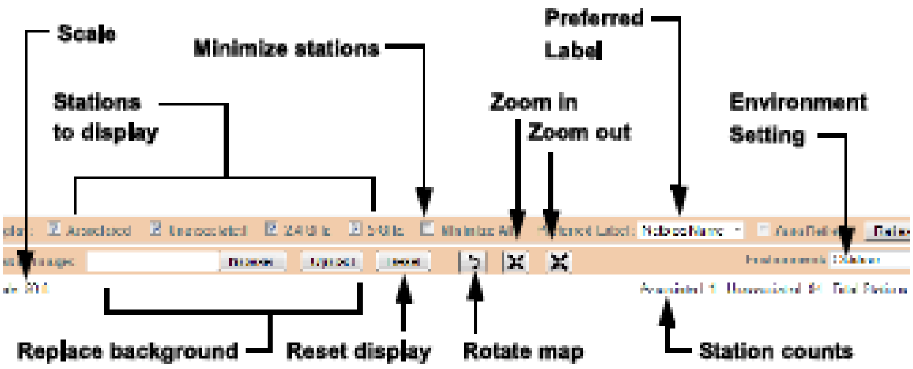


Figure 72. Controls for Location Map

- **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 selects the type of label to be displayed for stations: **Netbios Name, IP Address, MAC Address,** or **Manufacturer**. If you select NetBIOS (this is the default), then that name, if known, will be used to label each Array. Else, its IP or MAC address will be used, in that order.
- **Auto Refresh:** Instructs the Array to refresh this window automatically.
- **Refresh:** Updates the stations displayed.

- **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 131.
- **Upload**: After browsing to the desired custom image, click the **Upload** button to install it. The map is redisplayed with your new background. No hash marks (for the map scale) are added to the image display.
- **Reset**: Click this button to restore the map display to the factory settings. All attributes are restored—including the stations selected for display, the scale, the rotation, and the background map.
- **Rotate**: Click this button to rotate the orientation of the entire map. It rotates the map 45° counter-clockwise.
- **Enlarge**: Click this button to enlarge (zoom in on) the map. The displayed **Scale** is updated with the new scale for the map.
- **Reduce**: Click this button to reduce (zoom out on) the map. The displayed **Scale** is updated with the new scale for the map.

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

See Also

Station Status Windows

Working with the Custom Image

After you have uploaded a custom image (see **Custom Image** and **Upload** in "Controls and items displayed on the Location Map window" on page 129), 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.

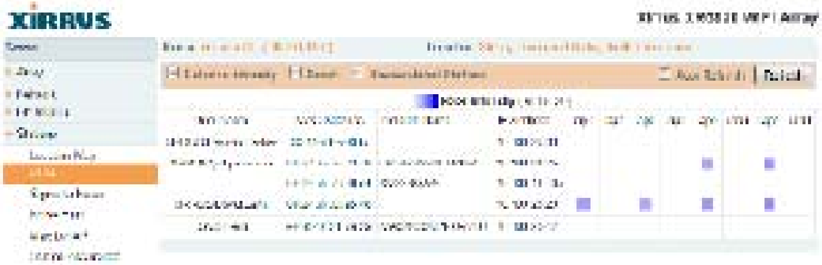


Figure 73. Station RSSI Values

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 73) If you select **Graph**, then the RSSI is shown on a representation of the Array, either colorized or numerically based on your selection. (Figure 74) The stations are listed to the left of the Array—click on a station to show its RSSI values on the Array.

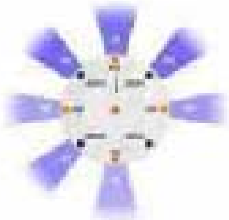


Figure 74. Station RSSI Values—Colorized Graphical View

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

See Also

Station Status Windows

RF Monitor Windows

Signal-to-Noise Ratio (SNR)

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

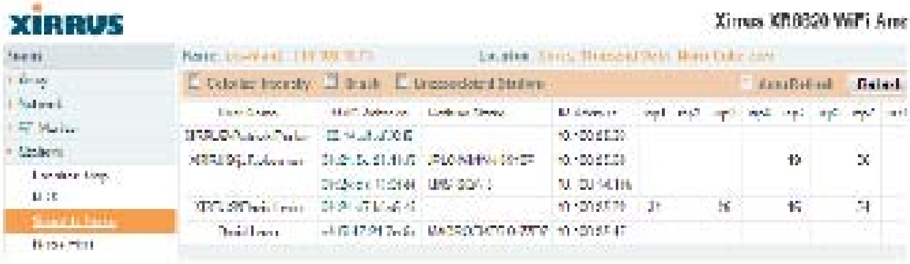


Figure 75. Station Signal-to-Noise Ratio Values

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 75) You may display the relative value using color if you select **Colorize Intensity**, with the highest SNR indicated by the most intense color. (Figure 76) 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.

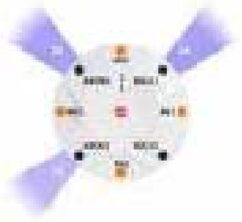


Figure 76. Station SNR Values—Colorized Graphical View

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

See Also

Station Status Windows

RF Monitor Windows

Noise Floor

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

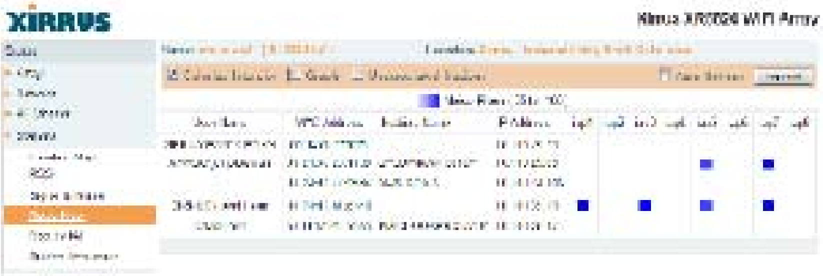


Figure 77. Station Noise Floor Values

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

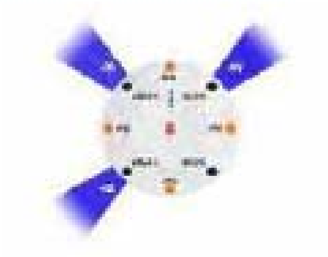


Figure 78. Station Noise Floor Values—Colorized Graphical View

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

See Also

Station Status Windows

RF Monitor Windows

Max by IAP

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

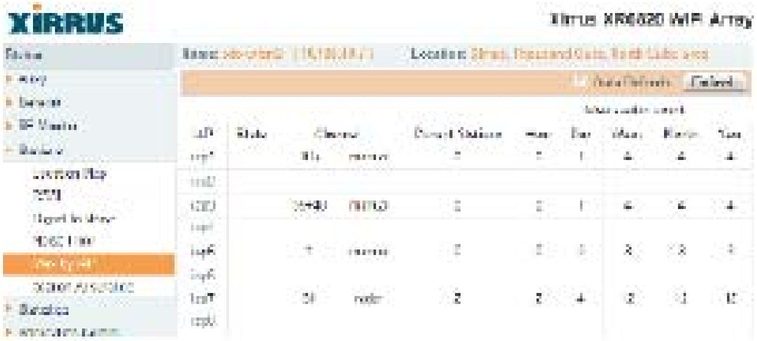


Figure 79. Max by IAP

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

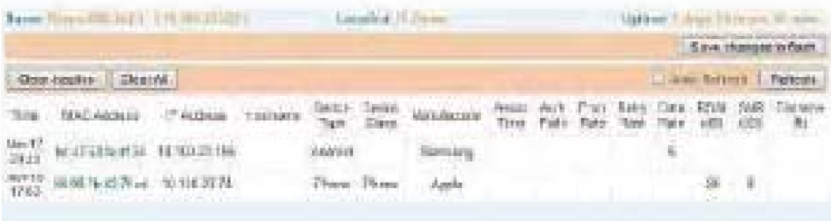
IAPs

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 320 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 320: associated time, authentication failures, packet error rate, packet retry rate, packet data rate, RSSI, signal to noise ratio (SNR), and distance.



Time	MAC Address	IP Address	Hostname	Device Type	Device Class	Manufacturer	Assoc Time	Auth Fails	Error Rate	Retry Rate	Data Rate	RSSI (dB)	SNR (dB)	Distance (ft)
[illegible]	[illegible]	[illegible]		Android		Samsung					6			
[illegible]	[illegible]	[illegible]		iPhone	iPhone	Apple						-56	8	

Figure 80. 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 141. Click the **Unicast Stats Only** checkbox on the lower left to filter the results, or clear the checkbox to show statistics for all wireless traffic.

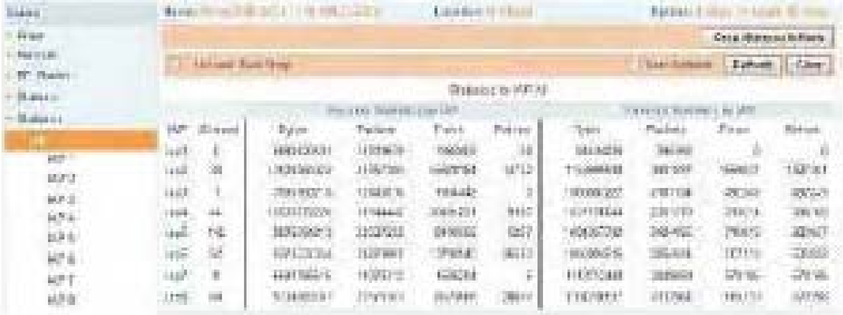


Figure 81. IAP Statistics Summary Page

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. If you click the link for **IAP All** in the left frame, each detailed statistic field will show the sum of that statistic for all IAPs. For a summary of statistics for all IAPs, see "IAP Statistics Summary" on page 140. Use the **Display Percentages** checkbox at the lower left to select the output format—check this option to express each statistic as a percentage of the total at the top of the column, or leave it blank to display raw numbers.

A quick way to display the statistics for a particular IAP is by clicking the Array graphic at the bottom left of the WMI window. Click the desired IAP, and the selected statistics will be displayed. See "User Interface" on page 88.

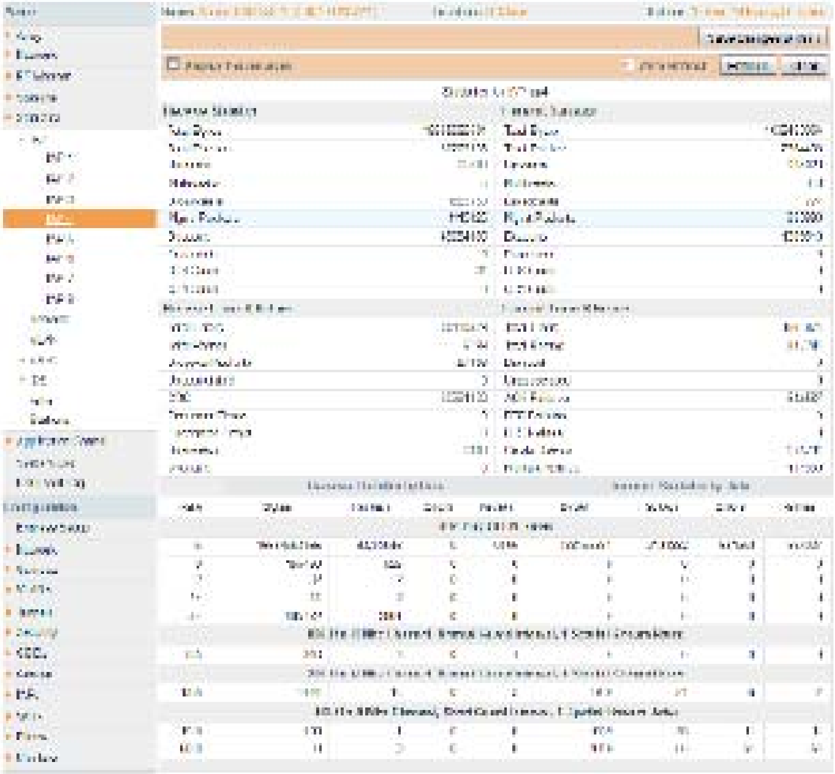


Figure 82. Individual IAP Statistics Page

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

See Also

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

Network Statistics

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

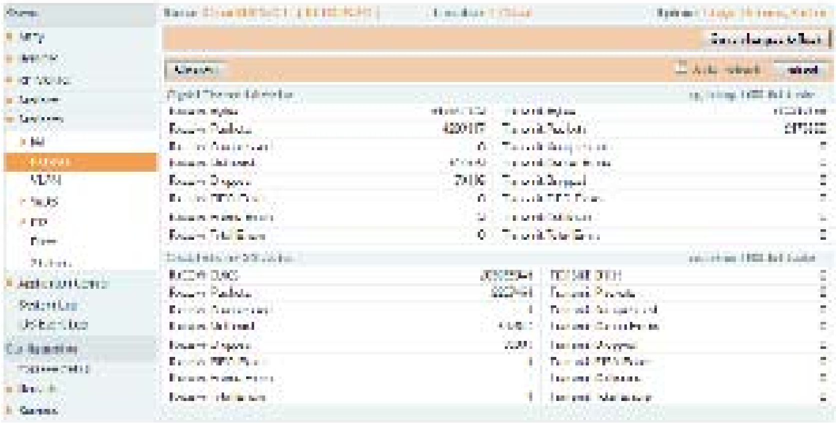


Figure 83. Network Statistics

See Also

DHCP Server

DNS Settings

Network

Network Interfaces

VLAN Statistics

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

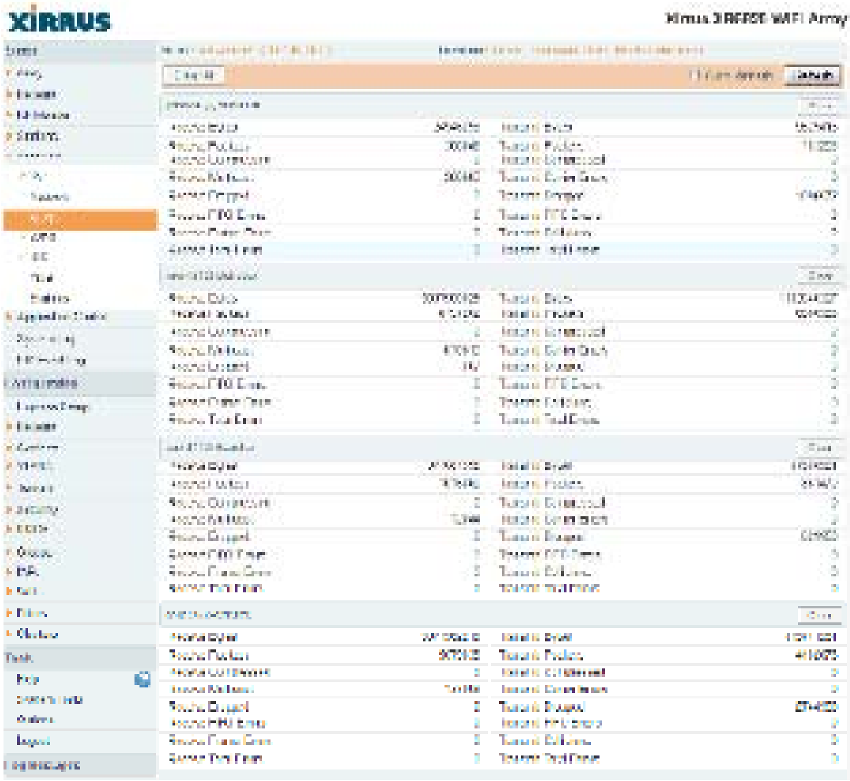


Figure 84. VLAN Statistics

See Also

VLAN Management

VLANs

WDS Statistics

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

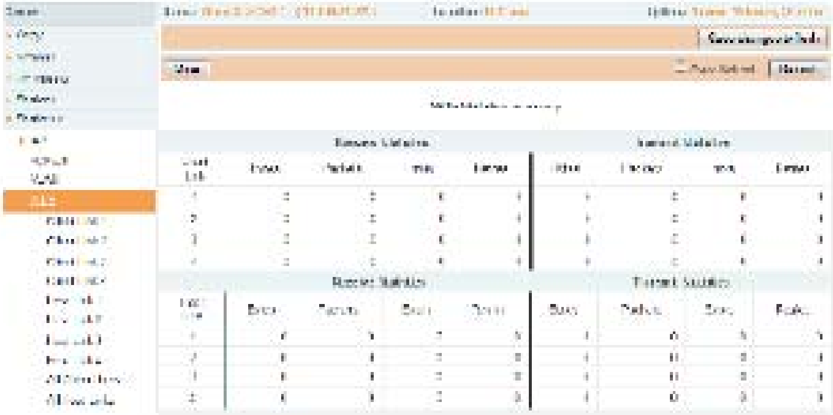


Figure 85. WDS Statistics

See Also

SSID Management

WDS

IDS Statistics

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

Note that you must have **Intrusion Detection Mode** enabled to collect IDS statistics. See "Intrusion Detection" on page 328. Information about IDS events is discussed in the "IDS Event Log Window" on page 157

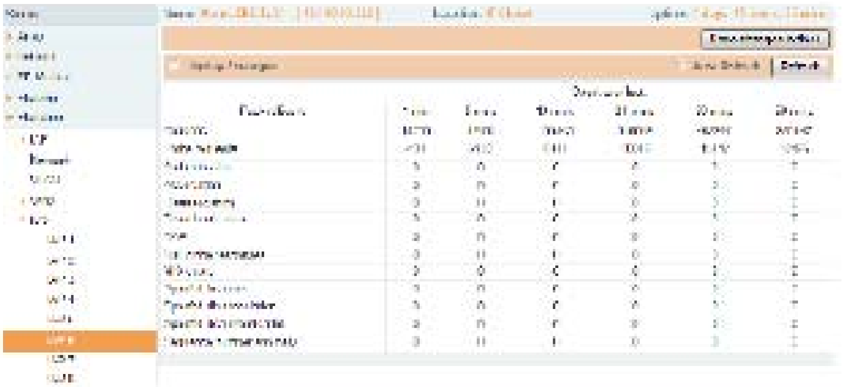


Figure 86. IDS Statistics Page

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

See Also

Intrusion Detection
IDS Event Log Window

Filter Statistics

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

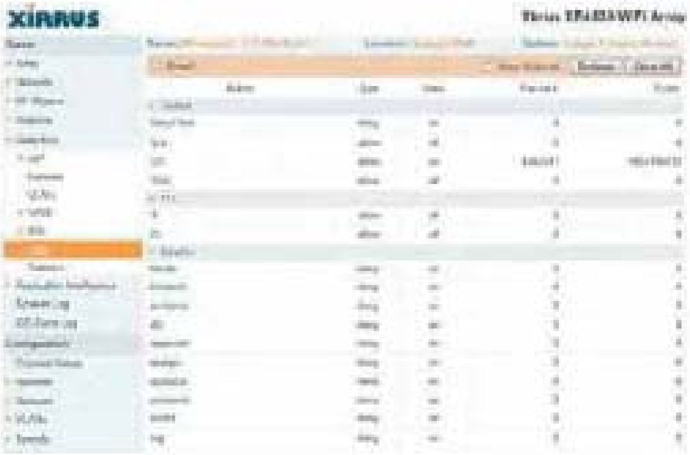


Figure 87. Filter Statistics

See Also

Filters

Application Control Windows

Station Statistics

This status-only window provides an overview of statistical data for all stations. Stations are listed by MAC address, and Receive and Transmit statistics are summarized for each. For detailed statistics for a specific station, click the desired MAC address in the **Station** column and see "Per-Station Statistics" on page 149.

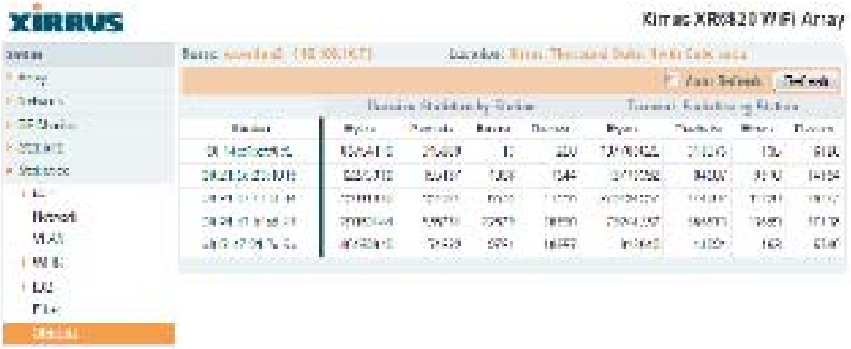


Figure 88. Station Statistics

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

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

See Also

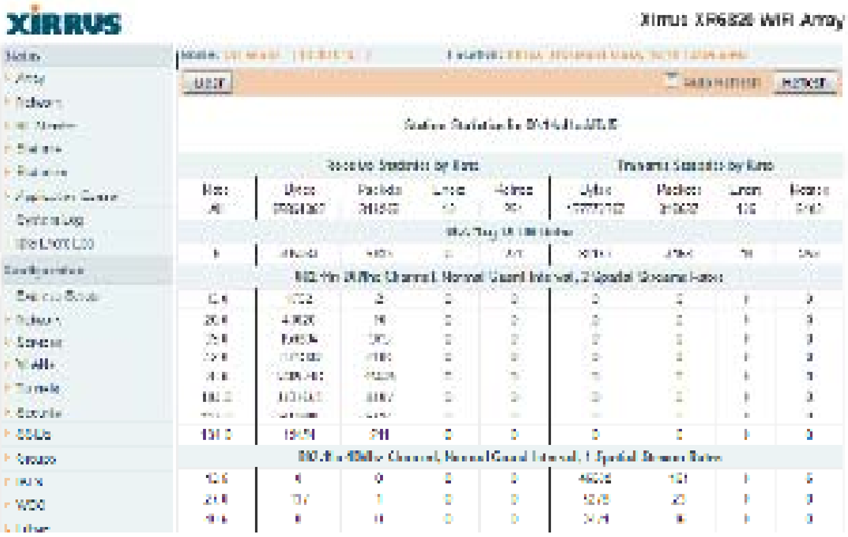
Per-Station Statistics

Per-Station Statistics

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

Receive and Transmit statistics are listed by **Rate**—this is the data rate in Mbps. For a summary of statistics for all stations, see "Station Statistics" on page 148.

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



Station Statistics for [illegible]

Receive Statistics by Rate					Transmit Statistics by Rate			
Rate	Bytes	Packets	Errors	Retries	Bytes	Packets	Errors	Retries
All	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Figure 89. 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 361**.*

Application Control data is only available from XR Series Array models. It is not available on XN Arrays.

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

Application Control is discussed in the following topics:

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

About Application Control

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

- Usage of non-productive and risky applications like BitTorrent can be restricted using Filters.
- Traffic for mission-critical applications like VoIP and WebEx may be given higher priority (QoS).
- Non- critical traffic from applications like YouTube may be given lower priority (QoS).

- Traffic flows for specific applications may be controlled by sending them into VLANs that are designated for that type of traffic.

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

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 licence that supports this feature, and you must have enabled the **Application Control** option on the **Filter Lists** page (see"Filter Lists" on page 345).

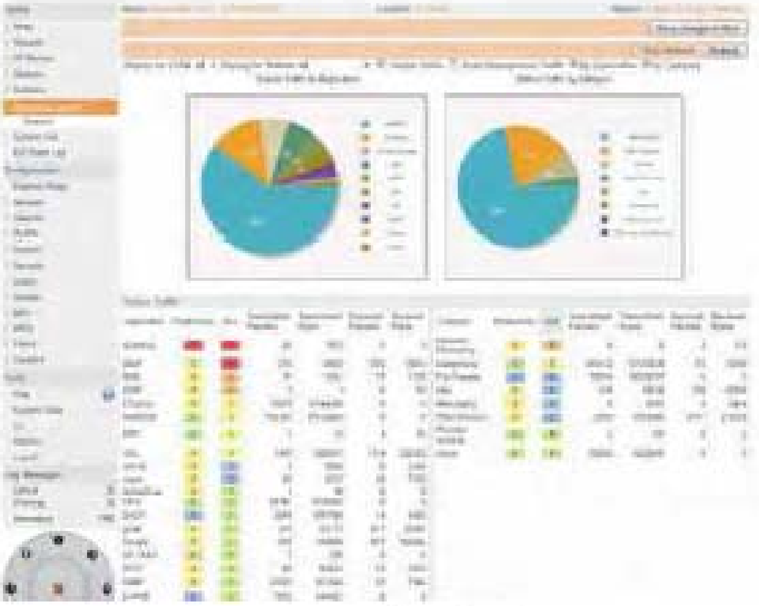


Figure 90. Application Control

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 155.
- **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

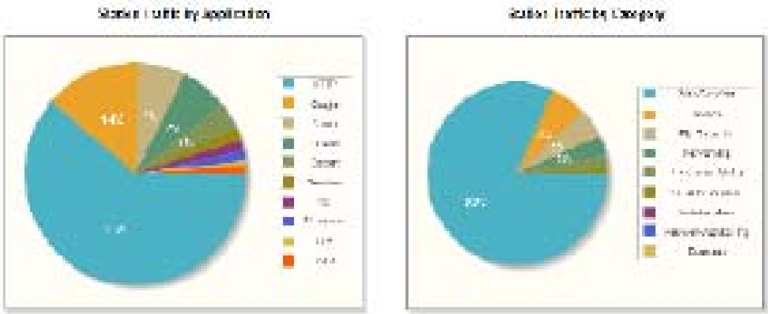


Figure 91. Application Control (Pie Charts)

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

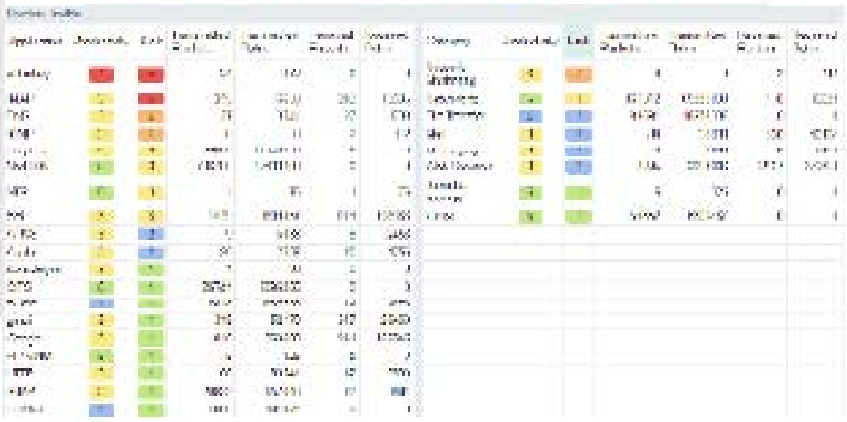


Figure 92. Application Control (Station Traffic)

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 347. 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 244.
- Lower the priority of less productive traffic—use filters to decrease the QoS assigned to traffic for applications like YouTube and Facebook.

Stations (Application Control)

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

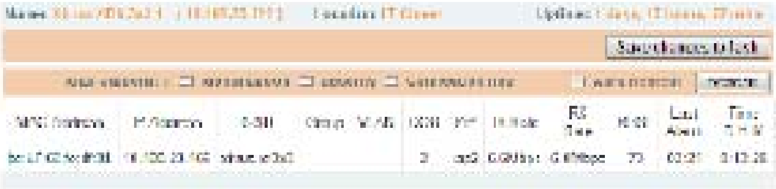


Figure 93. Stations (Application Control)

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 126.

System Log Window

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

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

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

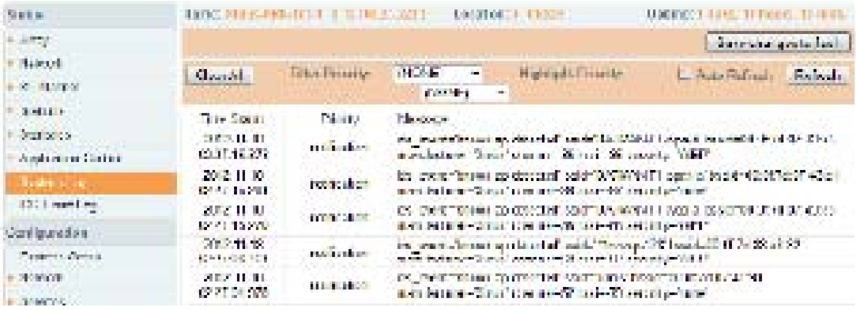


Figure 94. System Log (Alert Level Highlighted)

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 42 on page 88 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 328.

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

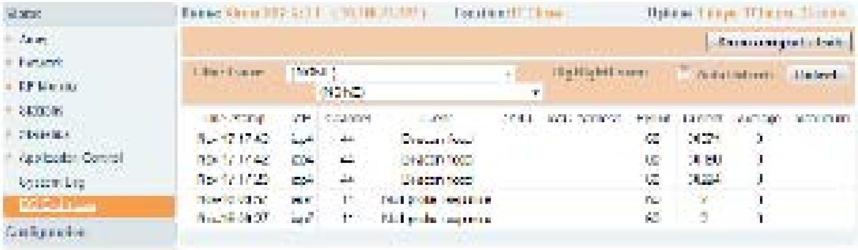


Figure 95. IDS Event Log

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

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

- **Time Stamp**—the time that the event occurred.
- **IAP**—the affected radio.
- **Channel**—the affected channel.
- **Event**—the type of attack, as described in Intrusion Detection.
- **SSID**—the SSID that was attacked.
- **MAC Address**—the MAC address of the attacker.

- **Period**—the length of the window used to determine whether the count of this type of event exceeded the threshold.
- **Current—**the count of this type of event for the current period.
- **Average**—the average count per period of this type of event.
- **Maximum**—the maximum count per period of this type of event.