User’s Guide

XS

Wireless LAN Array 3900/3700

DRAFT RELEASE (C)

April 12th, 2005

XIRRUS

Wireless LAN Array

XS-3900, XS-3700, XS-3500

Part Number: 800-0006-001
(Rev. A)

370 North Westlake Blvd, Suite 200
Westlake Village, CA 91362
USA
www.xirrus.com

Trademarks

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

Notices

FCC Notice

This device complies with Part 15 of the FCC Rules, with operation subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause unwanted operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate RF energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following safety measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Consult the dealer or an experienced wireless technician for help.

Use of a shielded twisted pair (STP) cable must be used for all Ethernet connections in order to comply with EMC requirements.

RF Radiation Hazard Warning

To ensure compliance with FCC RF exposure requirements, this device must be installed in a location where the antennas of the device will have a minimum distance of at least 25 cm (9.84 inches) from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Non-Modification Statement

Unauthorized changes or modifications to the device are not permitted. Use only the supplied internal antenna, or external antennas supplied by the manufacturer. Modifications to the device will void the warranty and may violate FCC regulations. Please go to the Xirrus Web site for a list of all approved antennas.

Indoor Use

This product has been designed for indoor use. Operation of channels in the 5250MHz to 5350MHz band is permitted indoors only to reduce the potential for harmful interference to co-channel mobile satellite systems.

Maximum Antenna Gain

Currently, the maximum antenna gain is limited to 6dBi for operation in the 5250MHz to 5350MHz band and 5725MHz to 5825MHz band and must not exceed maximum EIRP limits set by the FCC / Industry Canada.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LELAN devices used in Canada.

Industry Canada Notice and Marking

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

The term "IC:" before the radio certification number only signifies that Industry Canada technical specifications were met.

Safety Warnings

Safety Warnings

Read all user documentation before powering this device. All Xirrus interconnected equipment should be contained indoors. This product is not suitable for outdoor operation. Please verify the integrity of the system ground prior to installing Xirrus equipment. Additionally, verify that the ambient operating temperature does not exceed 50°C.

Explosive Device Proximity Warning

Do not operate the XS-3900 unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

Lightning Activity Warning

Do not work on the XS-3900 or connect or disconnect cables during periods of lightning activity.

Circuit Breaker Warning

The XS-3900 relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.

Translated safety warnings appear on the following page.

Translated Safety Warnings

Avertissements de Sécurité

Sécurité

Lisez l'ensemble de la documentation utilisateur avant de mettre cet appareil sous tension. Tous les équipements Xirrus interconnectés doivent être installés en intérieur. Ce produit n'est pas conçu pour être utilisé en extérieur. Veuillez vérifier l'intégrité de la terre du système avant d'installer des équipements Xirrus. Vérifiez également que la température de fonctionnement ambiante n'excède pas 50°C.

Proximité d'appareils explosifs

N'utilisez pas l'unité XS-3900 à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.

Foudre

N'utilisez pas l'unité XS-3900 et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.

Disjoncteur

L'unité XS-3900 dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Software License Agreement

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY BEFORE DOWNLOADING OR USING THE SOFTWARE.

BY USING ANY LICENSED MATERIALS OR THE EQUIPMENT THAT CONTAINS THIS PRODUCT, YOU ACKNOWLDEGE THAT YOU HAVE READ AND UNDERSTOOD ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT AND THAT YOU ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, RETURN THE UNUSED PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

Single User License Grant: Xirrus, Inc. ("Xirrus") and its suppliers grant to Customer ("Customer") a nonexclusive and nontransferable license to use the Xirrus software and related documentation ("Software") in object code form solely on a single central processing unit owned or leased by Customer or otherwise embedded in equipment provided by Xirrus.

Multiple-Users License Grant: Xirrus Inc. ("Xirrus") and its suppliers grant to Customer ("Customer") a nonexclusive and nontransferable license to use the Xirrus software and related documentation ("Software") in object code form: (i) installed in a single location on a hard disk or other storage device on up to the number of computers owned or leased by Customer for which Customer has paid a license fee ("Permitted Number of Computers"); or (ii) provided the Software is configured for network use, installed on a single file server for use on a single local area network for either (but not both) of the following purposes: (a) permanent installation onto a hard disk or other storage device on up to the Permitted Number of Computers; or (b) use of the Software over such network, provided the number of computers connected to the server does not exceed the Permitted Number of Computers. Customer agrees to (i) only use the programs contained in the Software for which Customer has paid a license fee (or in the case of an evaluation copy, those programs Customer is authorized to evaluate), (ii) not use any component of the Software or Equipment other than solely in conjunction with operation of the Software and as applicable, Equipment, (iii) unbundle any component of the Software or Equipment, (iv) use any component of the Software for the development of or in conjunction with any software application intended for resale that employs any such component, (v) use the Licensed Materials or Equipment in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or (vi) cause or permit any third party to do any of the foregoing. Xirrus may provide updates, corrections, enhancements, modifications or bug fixes for the Software ("Updates") to Licensee. Any such Update shall be deemed part of the Software and subject to the license and all other terms and conditions hereunder.

Customer grants to Xirrus or its independent accountants the right to examine its books, records and accounts during Customer's normal business hours to verify compliance with the above provisions. In the event such audit discloses that the Permitted Number of Computers is exceeded, Customer shall promptly pay to Xirrus the appropriate license fee for the additional computers or users. At Xirrus' option, Xirrus may terminate this license for failure to pay the required license fee.

Customer may make one (1) archival copy of the Software provided Customer affixes to such copy all copyright, confidentiality, and proprietary notices that appear on the original.

EXCEPT AS EXPRESSLY AUTHORIZED ABOVE, CUSTOMER SHALL NOT: COPY, IN WHOLE OR IN PART, SOFTWARE OR DOCUMENTATION; MODIFY THE SOFTWARE; REVERSE COMPILE OR REVERSE ASSEMBLE ALL OR ANY PORTION OF THE SOFTWARE; OR RENT, LEASE, DISTRIBUTE, SELL, OR CREATE DERIVATIVE WORKS OF THE SOFTWARE.

Customer agrees that aspects of the licensed materials, including the specific design and structure of individual programs, constitute trade secrets and/or copyrighted material of Xirrus. Customer agrees not to disclose, provide, or otherwise make available such trade secrets or copyrighted material in any form to any third party without the prior written consent of Xirrus. Customer agrees to implement reasonable security measures to protect such trade secrets and copyrighted material. Title to Software and documentation shall remain solely with Xirrus.

OWNERSHIP. Xirrus or its suppliers own and shall retain all right, title and interest (including without limitation all intellectual property rights) in and to the Software and any Update, whether or not made by Xirrus. Licensee acknowledges that the licenses granted under this Agreement do not provide Licensee with title to or ownership of the Software, but only a right of limited use under the terms and conditions of this Agreement. All information or feedback provided by Licensee to Xirrus with respect to the Software or Equipment shall be Xirrus' property and deemed confidential information of Xirrus.

LIMITED WARRANTY. Xirrus warrants that for a period of ninety (90) days from purchase (i) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use, and (ii) the Software substantially conforms to its published specifications. Except for the foregoing, the Software is provided AS IS. This limited warranty extends only to Customer as the original licensee. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' or its service center's option, repair, replacement, or refund (if a standalone product) of the Software. In no event does Xirrus warrant that the Software is error free or that Customer will be able to operate the Software without problems or interruptions.

This warranty does not apply if the software (a) has been altered, except by Xirrus, (b) has not been installed, operated, repaired, or maintained in accordance with instructions supplied by Xirrus, (c) has been subjected to abnormal physical or electrical stress, misuse, negligence, or accident, or (d) is used in ultra-hazardous activities.

DISCLAIMER. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE EXTENT ALLOWED BY APPLICABLE LAW.

IN NO EVENT WILL XIRRUS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE EVEN IF XIRRUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Xirrus' or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any beta software, any software made available for testing or demonstration purposes, any temporary software modules or any software for which Xirrus does not receive a license fee. All such software products are provided AS IS without any warranty whatsoever.

This License is effective until terminated. Customer may terminate this License at any time by destroying all copies of Software including any documentation. This License will terminate immediately without notice from Xirrus if Customer fails to comply with any provision of this License. Upon termination, Customer must destroy all copies of Software.

Software, including technical data, is subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Customer agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import Software.

This License shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. Customer may not assign or transfer any of its rights or delegate any of its obligations under this agreement. No delay, failure or waiver by either party to exercise any right or remedy under this agreement shall operate to waive any exercise of such right or remedy or any other right or remedy. If any portion hereof is found to be void or unenforceable, the remaining provisions of this License shall remain in full force and effect. This License constitutes the entire License between the parties with respect to the use of the Software.

Restricted Rights - Xirrus' software is provided to non-Department of Defense agencies with RESTRICTED RIGHTS and its supporting documentation is provided with LIMITED RIGHTS. Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph "C" of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19. In the event the sale is to a Department of Defense agency, the government's rights in software, supporting documentation, and technical data are governed by the restrictions in the Technical Data Commercial Items clause at DFARS 252.227-7015 and DFARS 227.7202. Manufacturer is Xirrus, Inc. 370 North Westlake Blvd, Suite 200 Westlake Village, CA 91362.

PROPRIETARY NOTICES. Customer shall maintain and reproduce all copyright and other proprietary notices on all copies of the Software in the same form and manner that such notices are included on the Software.

Table of Contents

All topics listed in this Table of Contents are “clickable,” which means you can instantly jump to any selected topic with a click of your mouse button. Items that do not appear in the TOC list—they are part of the Front Matter, prior to this Table of Contents—include the following:

- Trademarks
- Notices
- Safety Warnings
- Translated Safety Warnings
- Software License Agreement

List of Figures

Introduction

This chapter introduces the Wireless LAN Array, including an overview of its key features and benefits, and a detailed listing of the product's physical, environmental, technology and regulatory specifications. Section headings for this chapter include:

- The Xirrus Family of Products
- About this User's Guide
- Product Overview
- Key Features and Benefits
- Product Specifications (XS-3900)

The Xirrus Family of Products

The Xirrus family of products includes the following items:

- **Xirrus Wireless LAN Array (XS-3900 / XS-3700 / XS-3500)**
  The Wireless WLAN array is specifically designed for the Enterprise market. There are three versions of this product, each with a different wireless capacity—sixteen IAPs (Integrated Access Points—radios) with the XS-3900, eight IAPs with the XS-3700, and four IAPs with the XS-3500.

  This User's Guide documents the high capacity XS-3900, and where there are operational differences between the three models these differences are highlighted.

- **Xirrus Wireless Management System (XM-3300)**
  The XM-3300 is used for managing large XS-3900 deployments from a centralized Web-based interface. The XM-3300 is occasionally referred to in this User's Guide; however, if you need detailed information about this product, refer to the XM-3300 User's Guide, part number 800-0007-001.

- **Xirrus Remote DC Power System (XP-3100)**
  The XP-3100 provides distributed DC power to multiple XS-3900 units, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.

Nomenclature

Throughout this User's Guide, the Wireless LAN Array is also referred to as the **XS-3900**, or simply the **XS**. In some instances, the terms **product**, **unit**, **array**, or **Xirrus array** are also used. When discussing wireless network environments in which the XS is employed, the most commonly used reference is **the system**.

The Xirrus Wireless Management System (XM-3300) and the Xirrus Remote DC Power System (XP-3100) are referred to as the **XM-3300** and **XP-3100**, or **XM** and **XP** respectively.

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 Xirrus 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 XS-3900
  Defines the prerequisites for deploying and installing the XS-3900 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 also emphasizes what you need to do to ensure that any configuration changes you make are applied, and provides a list of restricted characters.

- Configuring the XS-3900
  Contains procedures for configuring the XS-3900 using its embedded Web Management Interface. It also includes instructions for logging in to the XS-3900 with your Web browser, and procedures for upgrading the system firmware and resetting the XS-3900 to its factory defaults.

- The Command Line Interface
  Provides instructions for configuring the XS-3900 using keywords and commands via its embedded Command Line Interface—with examples and syntax conventions—and includes a procedure for establishing a Secure Shell (SSH) connection to the product.

- Appendix A: Servicing the XS-3900
  Contains procedures for servicing the XS-3900, including the removal and reinstallation of major hardware components.

- Appendix A: Quick Reference Guide
  Contains product reference information, including a review of the Web Management Interface pages and their content, an alphabetical listing of keywords available with the Command Line Interface, the product's factory default settings, a sample event log, and some useful keyboard shortcuts.

- Appendix B: Technical Support
  Offers guidance to resolve technical issues, including some general hints and tips to enhance your product experience, and a procedure for isolating problems within an XS-enabled wireless network. Also includes Frequently Asked Questions (FAQs), a table of error messages generated by the product, and Xirrus contact information.

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

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

Notes and Cautions

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

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

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

Screen Images

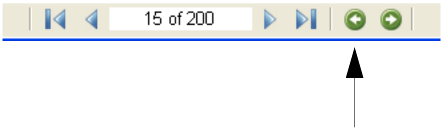
Some screen images of the Web Management Interface have been modified for clarity. For example, an image may have been cropped to highlight a specific area of the screen, and/or sample data may be included in some fields.

Your User's Guide as a PDF Document

This User's Guide is made available as a secure PDF (Portable Document Format) file and can be viewed using the Adobe® Acrobat Reader® product. It cannot be edited or modified. If you don't have Acrobat Reader, you can downloaded it free-of-charge from: http://www.adobe.com.

Hyperlinks

If you click on body text that appears in the color TEAL (with the exception of headings or notes) the embedded hyperlink within the text will immediately take you to the referenced destination. All internal and external cross-references, including page numbers within the List of Figures and the Index, have associated hyperlinks. After "jumping" to a referenced topic, if you want to return to the previous page (reference source), simply click on Acrobat's **previous page** button.



Previous page button

Figure 1. Adobe Acrobat (Version 6 and above)

Why Choose the Wireless LAN Array?

In 2003 there were approximately 30,000 Wireless Local Area Networks (WLANs) operating in the public domain. Research suggests that the number will more than quadruple by 2006. Enterprise WLANs in the private sector are also becoming increasingly common as businesses strive for greater flexibility in the workplace and the need for employee mobility rises. The only requirements for an effective wireless deployment are a power source, a couple of screws, and an imagination.

Wireless LAN is also fully compatible with standard Ethernet protocols, so connectivity with existing wired infrastructures is transparent to users—they can still access and use the same applications and network services that they use when plugged into the company's wired LAN infrastructure (it's only the plug that no longer exists).

Wireless LAN has come a long way in the past few years and now offers the performance, reliability and security that Enterprise customers have come to expect from their networks. The technology is being driven by three 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. It has a range of about 100 meters indoors and 300 meters outdoors.
- **802.11g**
  Supports a higher transmission speed of 54 Mbps in the 2.4 GHz range and is backwards compatible with 802.11b.

Whether you're a small company with just a handful of employees, or a large corporation with thousands, wireless has the scalability and flexibility to serve your needs.

Product Overview

Part of the family of Xirrus products, the Wireless LAN Array (XS-3900) is a high capacity, multi-mode WLAN array designed for the Enterprise market, with twice the range and up to sixteen times the capacity of competitive wireless products.

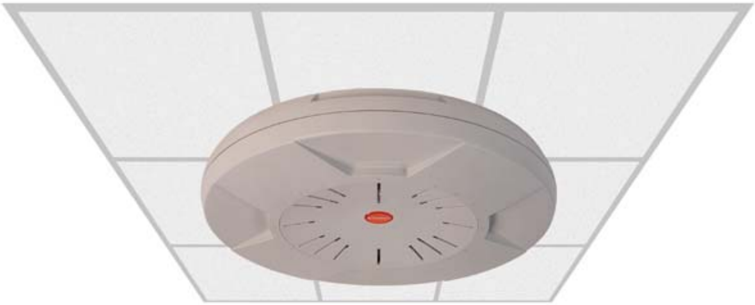


Figure 2. XS-3900

The XS-3900 is Wi-Fi® compliant and simultaneously supports 802.11a, 802.11b and 802.11g clients. 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 Wireless Management System (XM-3300) allows global management of hundreds of arrays from a central location.

The smaller XS-3700 and XS-3500 versions of the Wireless LAN Array have a correspondingly lower capacity than the XS-3900.

Enterprise Class Security

The latest and most effective wireless encryption security standards, including WPA2 (Wi-Fi Protected Access 2) with 802.11i AES (Advanced Encryption Standard) are provided with the XS-3900. In addition, the use of 802.1x with an embedded RADIUS server (or external RADIUS servers) ensures user authentication—multiple arrays can authenticate to the optional XM-3300 ensuring only authorized Xirrus Wireless LAN Arrays become part of the wireless network. Rogue AP detection and site monitoring is performed in the background by the XS-3900 automatically.

Deployment Flexibility

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

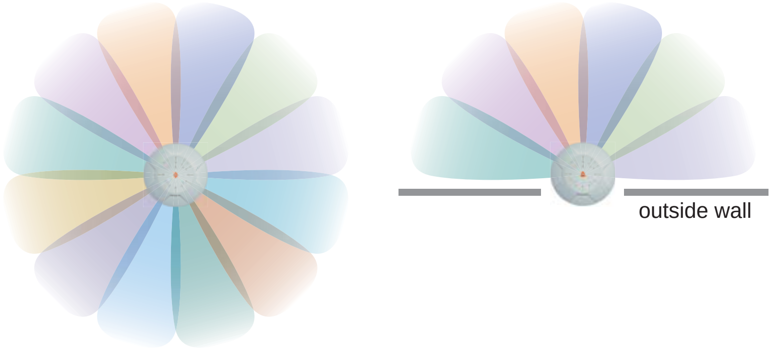


Figure 3. Wireless Coverage Patterns

Figure 2 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 XS-3900.
- **Partial pattern coverage**
  If desired, the XS-3900 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.

Remote DC Power System (Optional)

The Xirrus Remote DC Power System (XP-3100) provides distributed DC power to your XS-3900 (DC version) deployments, eliminating the need to provide an AC power outlet in close proximity to the unit(s).

In the following example, DC power is supplied to four Xirrus Arrays while utilizing only one AC power outlet.

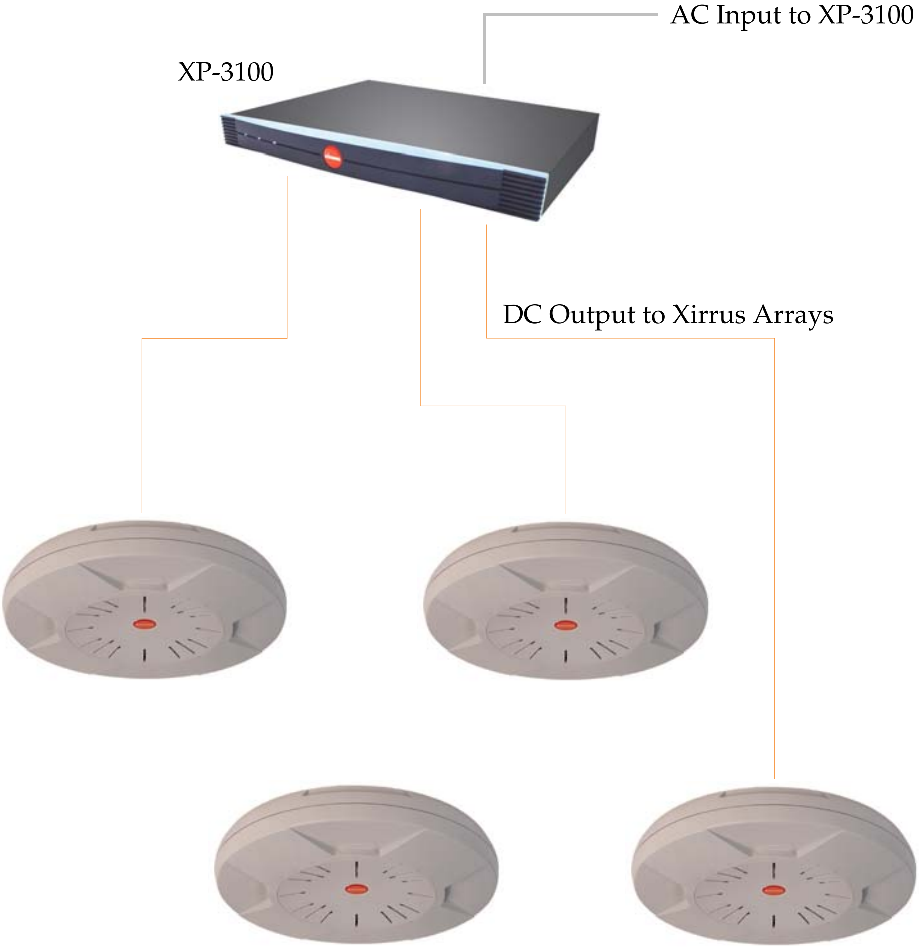
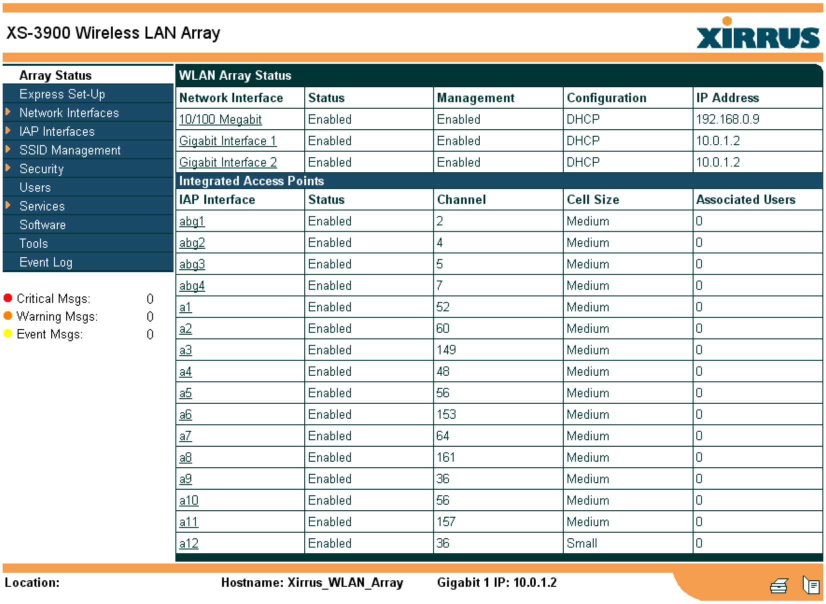


Figure 4. Remote DC Power Distribution

Enterprise Class Management

The XS-3900 can be configured with its default RF settings, or the RF settings can be customized using the array’s embedded Web Management Interface (WMI). The WMI enables easy configuration and control from a graphical console, along with a full compliment of troubleshooting tools, reports and statistics.



Critical Msgs:	0
Warning Msgs:	0
Event Msgs:	0

WLAN Array Status

Network Interface	Status	Management	Configuration	IP Address
10/100 Megabit	Enabled	Enabled	DHCP	192.168.0.9
Gigabit Interface 1	Enabled	Enabled	DHCP	10.0.1.2
Gigabit Interface 2	Enabled	Enabled	DHCP	10.0.1.2

Integrated Access Points

IAP Interface	Status	Channel	Cell Size	Associated Users
abg1	Enabled	2	Medium	0
abg2	Enabled	4	Medium	0
abg3	Enabled	5	Medium	0
abg4	Enabled	7	Medium	0
a1	Enabled	52	Medium	0
a2	Enabled	60	Medium	0
a3	Enabled	149	Medium	0
a4	Enabled	48	Medium	0
a5	Enabled	56	Medium	0
a6	Enabled	153	Medium	0
a7	Enabled	64	Medium	0
a8	Enabled	161	Medium	0
a9	Enabled	36	Medium	0
a10	Enabled	56	Medium	0
a11	Enabled	157	Medium	0
a12	Enabled	36	Small	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 5. WMI: Array Status Page

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 Wireless Management System.

For deployments of more than two XS units, we recommend that you use the Xirrus Wireless Management System (XM-3300). The XM-3300 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 XS-3900.

High Capacity and High Performance

The XS-3900 easily handles time-sensitive traffic, such as voice, and can enable wireless connectivity for nearly 1,000 users. The unit includes two Gigabit uplink ports for connection to the wired network. A total of sixteen IAPs provides a maximum wireless capacity of 864 Mbps, which offers ample reserves for the high demands of current and future applications. Of the sixteen IAPs, twelve operate in the 802.11a mode and four operate in any combination of 802.11a, 802.11b and 802.11g.

If desired, IAP (radio) **abg2** can also be configured in RF monitoring and rogue AP detection mode.

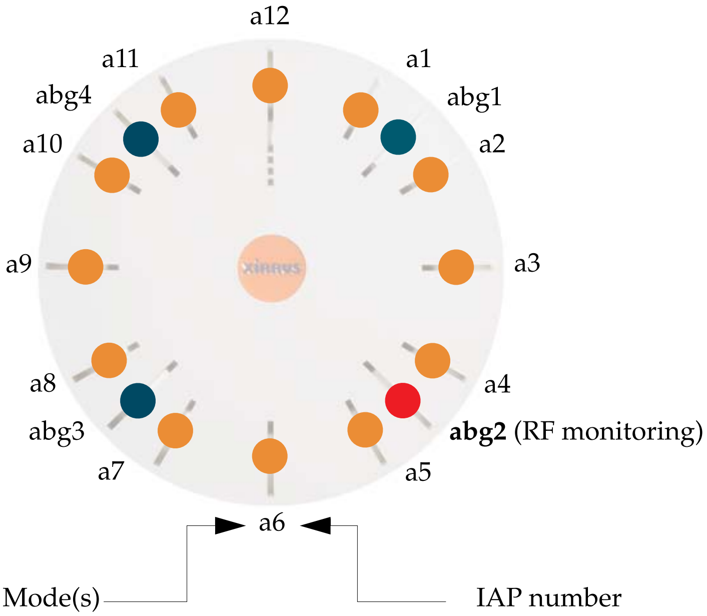
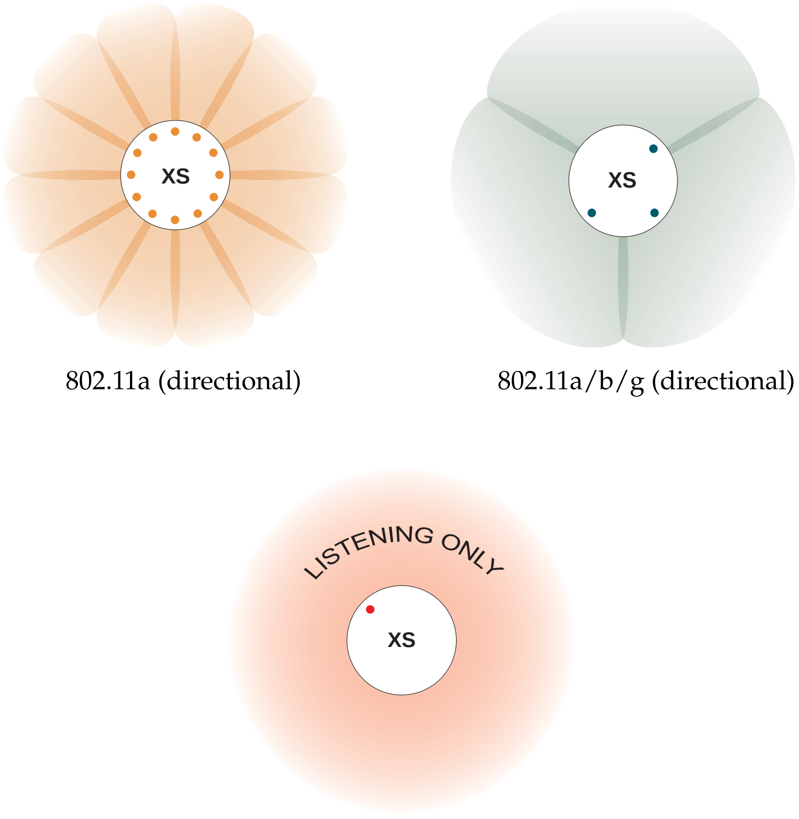


Figure 6. Layout of IAPs (XS-3900)

Extended Coverage

One XS-3900 solution enables you to replace up to sixteen access points—fifteen IAP radios with integrated directional antennas provide increased wireless range and enhanced data rates in all directions. With an XS deployed, far fewer access points are needed for your wireless network. Radio **abg2** (see Figure 6) can be switched to use an integrated omnidirectional antenna—for listening only—and can be dedicated to the tasks of site monitoring and rogue AP detection.



802.11a (directional)

802.11a/b/g (directional)

802.11a/b/g (omnidirectional)

Figure 7. Antenna Patterns

Non-Overlapping Channels

Complete use of non-overlapping channels limits interference and delivers maximum capacity. On the XS-3900, all 16 non-overlapping channels are fully utilized across the 5Ghz and 2.4Ghz spectrums (12 across the 5GHz spectrum and 4 across the 2.4GHz spectrum).

Secure Wireless Access

Multiple layers of authentication and encryption ensure secure data transmissions. The XS-3900 is 802.11i compliant with encryption support for 64 bit and 128 bit WEP, TKIP and AES.

Authentication support is provided via 802.1x, including PEAP, EAP-TLS, and EAP-TTLS.

Wi-Fi Standards Compliance

Fully meets the requirements of 802.11a/b/g standards, and guaranteed interoperability with all other Wi-Fi products certified by the Wi-Fi Alliance.

Applications Enablement

QoS (Quality of Service) functionality combined with true switch capabilities enable high density Voice over Wireless LAN deployments. Compliant with 802.11e (final draft), 802.1p and 802.1q standards.

SDMA Optimization

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

Easy Deployment

The Xirrus Wireless Management System (XM-3300) offers real time monitoring and management capabilities of the wireless network—ideal for the Enterprise market. It also allows you to import floor plans to help you plan your deployment. The XM-3300 chassis has a plenum rated, lockable and tamper resistant case.

Product Specifications (XS-3900)

Element	Specifications
Number of Users	Maximum of 64 associated users per radio 1024 users per array
Physical	Diameter: 12.9 inches (32.77 cm) Height: 2.53 inches (6.43 cm) Weight: 8lbs (3.63 kg)
Environmental	**Operating Temperature:** -10°C to 50°C 0% to 90% relative humidity (non-condensing) **Storage Temperature:** -20°C to 60°C 5% to 95% relative humidity (non-condensing) **Operating Altitude:** 2000 meters (6561 feet)
System	825 MHz CPU 128MB RAM, expandable 512MB system flash, expandable Expansion slot for future options
Electrical	Input Power (AC version): 90VAC to 265VAC at 47Hz to 63Hz Input Power (DC version): 48VDC
Interfaces	**Serial:** 1 x RS232 – RJ45 connector **Ethernet Interfaces:** 2 x Gigabit 100/1000 Mbps w/failover 1 x Fast Ethernet 10/100 Mbps **Status LEDs:** System status, Ethernet, Radio

Element	Specifications
Management	Web-based HTTPS SNMP v3 CLI via SSHv2 FTP TFTP Serial Proprietary Xirrus Wireless Management System Syslog reporting for alerts/alarms
Networking	DHCP client, DHCP server, NTP client RFC
VLAN Support	802.1Q, P VLAN Supports up to 16 VLANs
Multiple SSID Support	Allows up to 16 separate SSIDs to be defined with map security, VLAN, QoS and guest access settings for each SSID
Performance	**Client Load Balancing** Automatic load balancing between system radios **Quality of Service:** 802.1P wired traffic prioritization 802.11e wireless prioritization MAP CoS to TCID Fair queuing of downstream traffic

Element	Specifications
Security	**Wireless Security:** WEP 40bit/128bit encryption WPA with TKIP and AES encryption Misappropriated APs automatically reset to factory defaults (requires the Xirrus Wireless Management System) Rogue AP detection, with alerts and classification Denial of Service (DoS) attack detection MAC address spoofing prevention **User and System Authentication:** WPA Pre-Shared Key authentication Embedded RADIUS Server 802.1x EAP-TLS 802.1x EAP-TTLS 802.1x PEAP External RADIUS servers Authentication of Xirrus APs to the Xirrus Management System (XM-3300)

Element	Specifications
Wireless	**Number of Radios:** 12 x 802.11a radios 4 x 802.11a/b/g radios **Wireless Standards:** 802.11a/b/g and g-only mode 802.11d, 802.11e (draft), 802.11i **Channel Selection:** Manual Automatic **Frequency Bands:** 11a: 5.15-5.25 GHz (UNII 1) 11a: 5.15-5.25 GHz (TELEC) 11a: 5.25-5.35 GHz (UNII 2) 11a: 5.470-5.725 (ETSI) 11a: 5.725-5825 GHz (UNII 3) 11b/g: 2.412-2.462 GHz (FCC) 11b/g: 2.412-2.472 GHz (ETSI) 11b/g: 2.412-2.484 GHz (TELEC) **Antenna:** Internal 6dBi sectorized antenna External RP-TNC connector **Radio Approvals:** FCC (United States) EN 301.893 (Europe)
Compliance	UL / cUL 60950 and EN 60950 FCC Part 15.107 and 15109, Class A EN 301.489 (Europe)
Warranty	One year

Installing the XS-3900

This chapter defines the prerequisites for installing the XS-3900 and provides instructions to help you complete a successful installation. Section headings for this chapter include:

Installation Prerequisites

Your XS-3900 deployment requires the presence of hardware and services in the host wired/wireless network, including:

- **Dedicated AC power outlet**
  Unless you are using the Xirrus Remote DC Power System (XP-3100) with the DC version of the XS-3900, you need a dedicated power outlet to supply AC power to each unit deployed at the site. If you are using the optional XP-3100, then DC power is supplied to all units and only one AC outlet is required for the XP-3100.

- **Ethernet port**
  You need at least one 10/100/1000 BaseT port to establish wired Gigabit Ethernet connectivity (via the product's Gigabit 1 or Gigabit 2 port) and one 10/100 BaseT port (if desired) for wired Fast Ethernet connectivity.

- **Secure Shell (SSH) utility**
  To establish secure remote command line access to the XS-3900, you need a Secure Shell (SSH) utility, such as PuTTY.

- **Secure Web browser**
  Either Internet Explorer (version 6.0 or higher), Netscape Navigator (version 7.0 or higher), or Mozilla Firefox (version 1.01 or higher) and it must be available on the same subnet as the XS-3900. A secure Web browser is required for Web-based management of the XS-3900.

- **Serial connection capability**
  To connect directly to the console port on the XS-3900, your computer must be equipped with a male 9-pin serial port and terminal emulation software (for example, HyperTerminal).

  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.

- **DHCP server**
  To distribute IP addresses and ancillary information to your XS-3900.
- **Xirrus Wireless Management System (XM-3300)**

  The optional XM-3300 offers powerful management features for small or large XS-3900 deployments.
- **Xirrus Remote DC Power System (XP-3100)**
  The optional XP-3100 provides distributed DC power to multiple XS-3900 units, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.
- **External RADIUS server**
  Although your XS-3900 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 XS-3900 should only be used with Wi-Fi certified client devices.

Planning Your Installation

This section provides guidelines and examples to help you plan your XS-3900 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 XS-3900 unit you install.

General Deployment Considerations

The XS-3900's unique multi-radio architecture generates 360 degrees of sectored high-gain 802.11a/b/g coverage that provides extended range. However, the number, thickness and location of walls, ceilings or other objects that the wireless signals must pass through may affect the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise at your location. To maximize wireless range, follow these basic guidelines:

1. Keep the number of walls and ceilings between the XS-3900 and your receiving devices to a minimum—each wall or ceiling can reduce the wireless range from between 3 and 90 feet (1 to 30 meters). Position your devices so that the number of walls or ceilings is minimized.

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

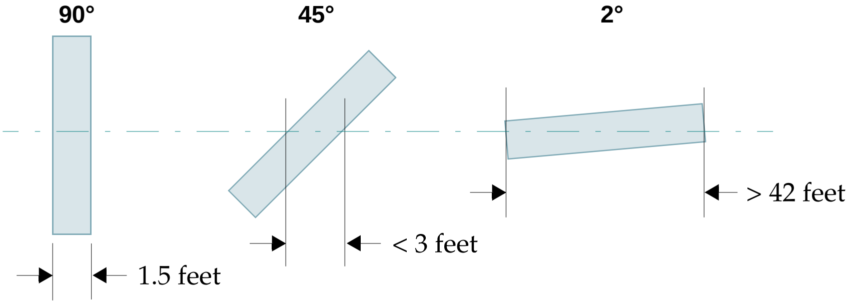


Figure 8. Wall Thickness Considerations

3. Building materials can make all the difference. For example, solid metal doors or aluminum wall studs may adversely effect wireless signals. Try to position wireless client devices so that the signal passes through drywall (between studs) or open doorways and not other materials.

Coverage and Capacity Planning

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

Placement

Use the following guidelines when considering placement options:

1. The best placement option for the XS-3900 is ceiling-mounted within an open plan environment (cubicles rather than fixed walls).
2. Keep the XS-3900 away from electrical devices or appliances that generate RF noise. Because the XS-3900 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 (or 1 to 2 meters).
3. If using multiple XS-3900s at the same location, we recommend maintaining a distance of at least 100 feet between units.

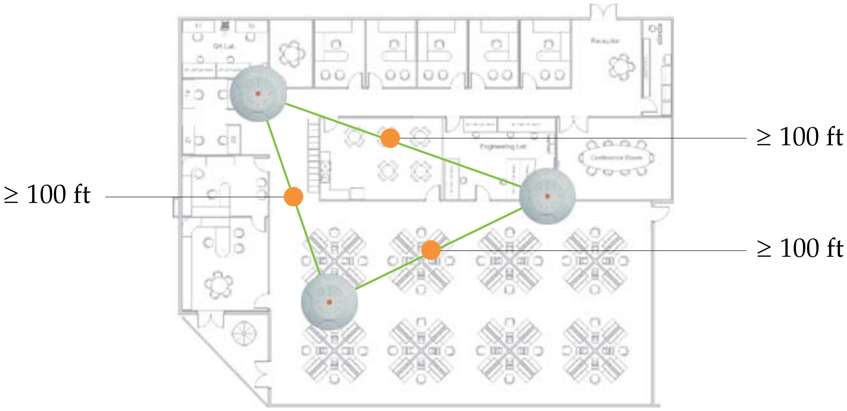


Figure 9. Unit Placement

RF Patterns

The XS-3900 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 XS-3900 provides a full 360 degrees of coverage.

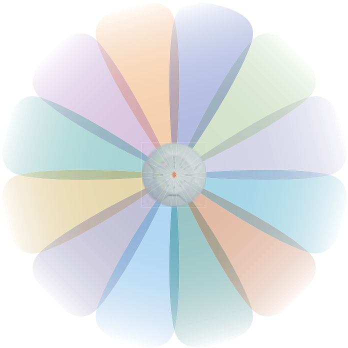


Figure 10. Full (Normal) Coverage

Half Coverage

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

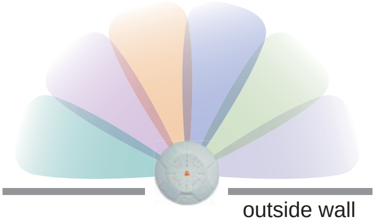


Figure 11. Adjusting RF Patterns

Custom Coverage

Where there are highly reflective objects in close proximity to the XS-3900, you can turn off specific radios to avoid interference and feedback.

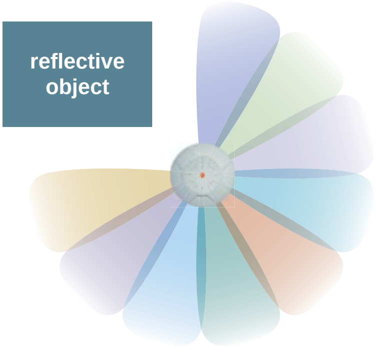


Figure 12. Custom Coverage

Calculating Areas

Before we discuss cell sizes, it is useful to know how to calculate the area of a circle (because the XS-3900 radiates a full 360 degrees). The area of a circle is equal to pi (π) times the square of the radius, where pi is equal to 3.14. The following graphic calculates the area of a circle with a radius of 20 feet.

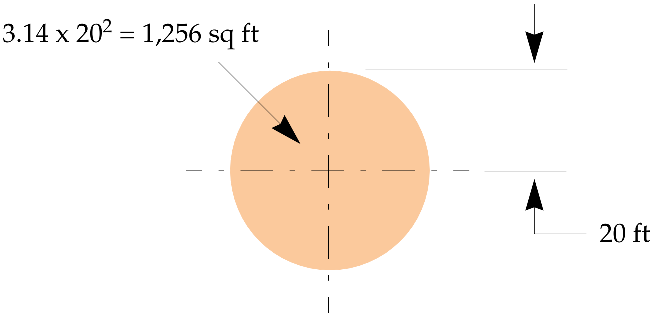


Figure 13. Calculating the Area of a Circle

Capacity and Cell Sizes

Cell sizes should be calculated based on the number of users, the applications being used (for example, data/video/voice), and the number of XS-3900 units 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.

The following chart shows the **maximum** recommended cell sizes for each data rate.

Min. Desired Data Rate (Mbps)	11a Cell Size		11b/g Cell Size	
	Radius (feet)	Area (sq. feet)	Radius (feet)	Area (sq. feet)
54	104	33,962	130	53,066
48	195	119,398	228	163,230
36	260	212,264	325	331,662
24	293	269,566	357	400,190
18	325	331,662	422	559,184
12	357.5	401,312	455	650,058
9	390	477,594	468	687,735
6	423	561,837	487	744,711
11	0	0	520	849,056
5.5	0	0	546	936,084
2	0	0	572	1,027,358
1	0	0	585	1,074,586

Sample 802.11a Cells

The following 802.11a sample cells illustrate the coverage area and minimum throughput you can expect (per sector) based on the size of each cell. Notice how the throughput increases as the cell size decreases, and vice versa.

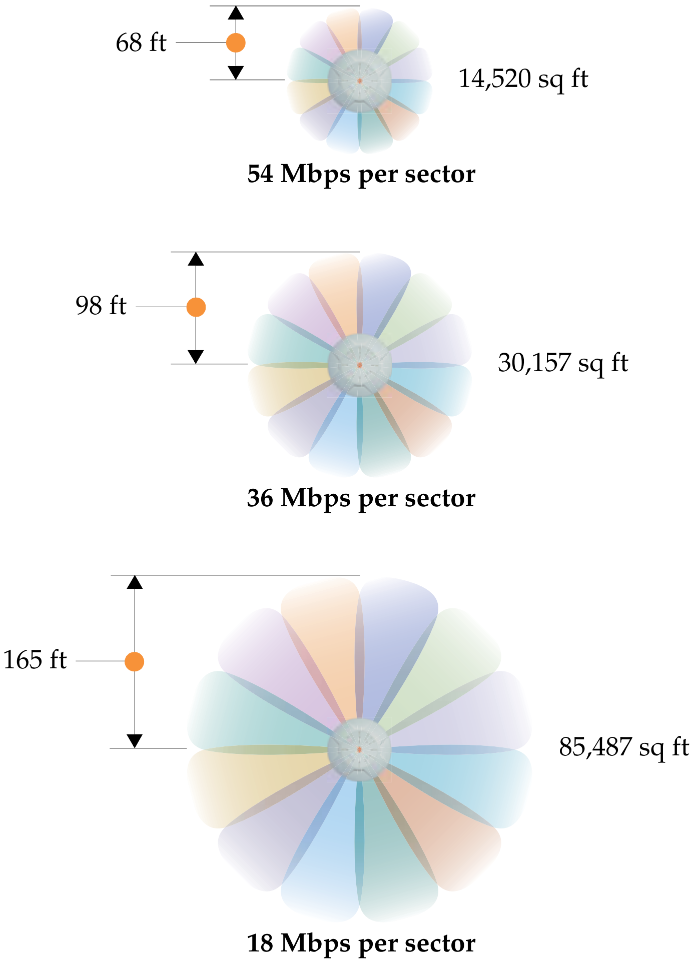


Figure 14. Sample 802.11a Cells

Fine Tuning Cell Sizes

Adjusting the transmit power allows you to fine tune cell sizes. There are three settings—Large, Medium, or Small (the default is Medium). If you are installing many units in close proximity to each other, reduce the transmit power to avoid excessive interference with other arrays or installed APs. See also, "IAP Settings" on page 79.

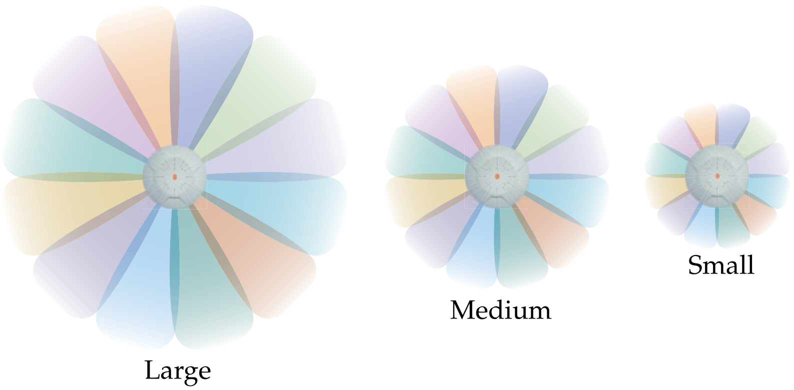


Figure 15. Transmit Power

Roaming Considerations

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

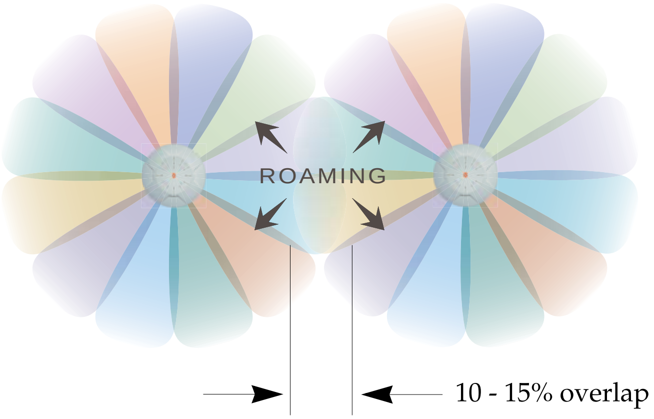


Figure 16. Overlapping Cells

Allocating Channels

Because the XS-3900 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 XS-3900 to make intelligent channel allocation decisions automatically. In the automatic mode, channels are allocated dynamically, driven by changes in the environment.

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.

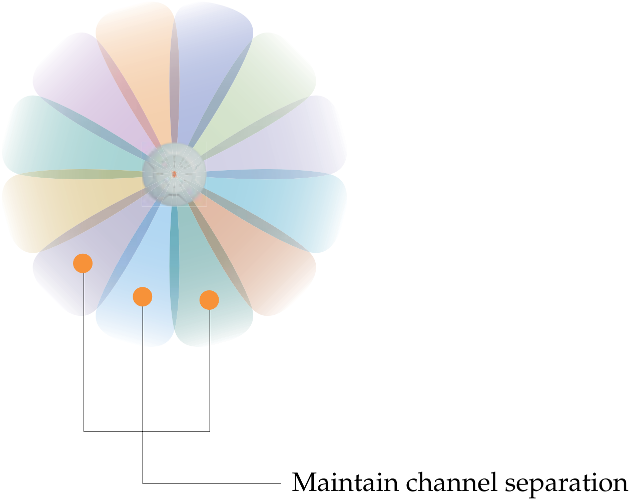


Figure 17. Allocating Channels Manually

Deployment Examples

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

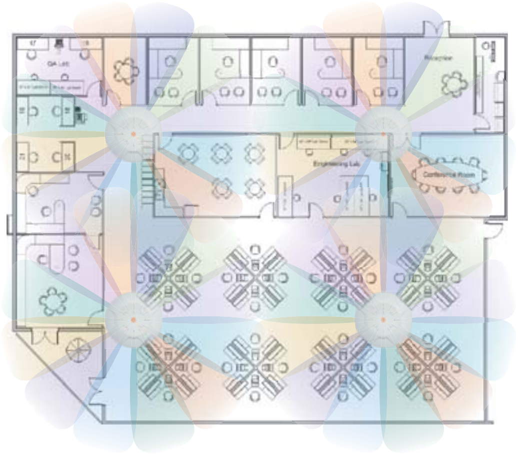


Figure 18. Deployment Scenario (54 Mbps)—Per Sector

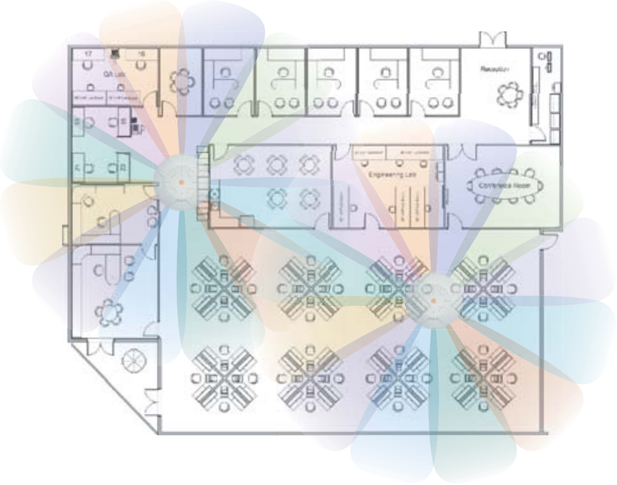


Figure 19. Deployment Scenario (36 Mbps)—Per Sector

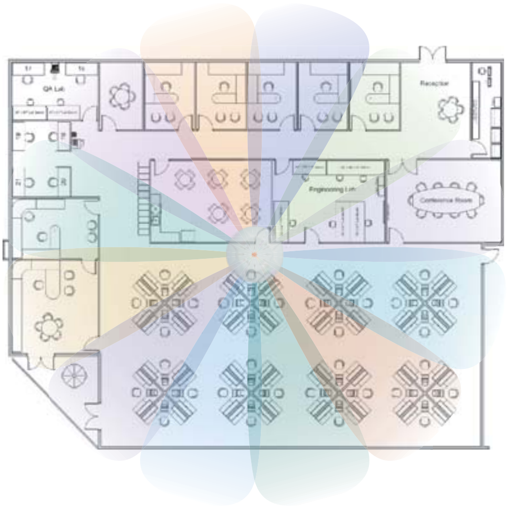


Figure 20. Deployment Scenario (18 Mbps)—Per Sector

Failover Planning

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

Unit Failover Protection

In the rare event that an XS-3900 becomes unavailable, it is suggested that you deploy a backup unit. Backup units monitor primary units via an Ethernet switch and continue to provide wireless services in the event that the primary unit becomes unavailable. Any XS-3900 can be set up as a backup unit. Backup units should be located near primary units.

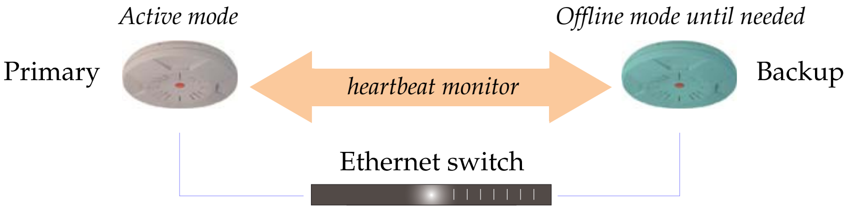


Figure 21. Unit Failover Protection

Port Failover Protection

To ensure that service is continued in the event of a port failure, you can utilize all three XS-3900 ports (Fast Ethernet, Gigabit 1 and Gigabit 2) simultaneously.

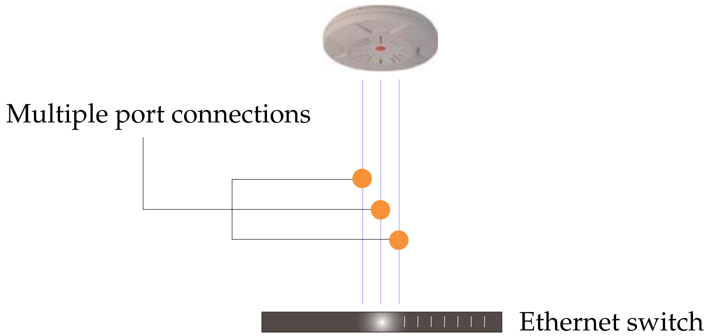


Figure 22. Port Failover Protection

Switch Failover Protection

To ensure that service is continued in the event of a switch failure, you can connect XS-3900 units to more than one Ethernet switch.

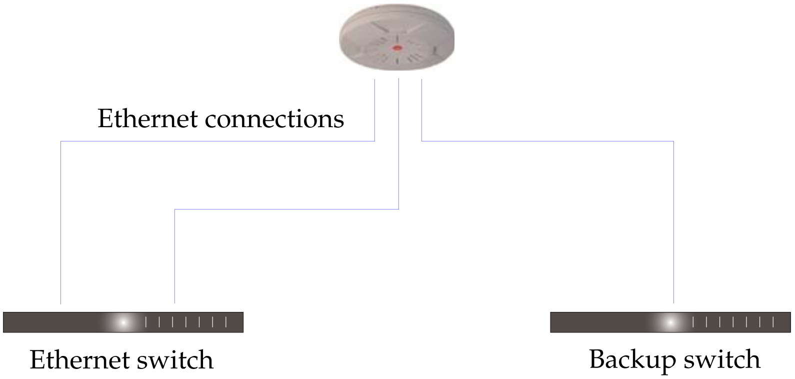


Figure 23. Switch Failover Protection

Gigabit Ethernet connections must be on the same subnet.

Power Planning

This section discusses the AC and DC power options.

AC Power

The AC power option requires a direct connection between the XS-3900 and a dedicated AC power outlet. The power cord is provided with the unit.

Remote Distributed DC Power

To deliver DC power to the XS-3900, you must have the optional Xirrus Remote DC Power System (XP-3100) and a Xirrus Array that supports DC power—see Figure 4 on page 8 . The XP-3100 provides DC power to multiple XS-3900 units from a single source, and requires only one AC power outlet.

Depending on the type of cable used, XS-3900 units can be located up to 600 feet from the XP-3100. In addition, the XP-3100 can be plugged into a UPS to prevent power failure to all XS-3900 units in the network.

When using CAT5 cable, DC power can be provided up to a distance of 300 feet.

Security Planning

This section offers some useful guidelines for defining your preferred encryption and authentication method. For additional information, go to the Security section of “Frequently Asked Questions” on page 186.

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**
  This is much more secure than WEP and uses TKIP for encryption.

- **Wi-Fi Protected Access 2**
  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 there after. The following authentication methods are available with the XS-3900:

- **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).

- **Xirrus internal RADIUS server**
  Includes all the core functionality of a full RADIUS server built into the Xirrus XS-3900. Recommended for smaller numbers of users (about 100 or less).

- **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 Xirrus 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 XS-3900 supports 512 ACL entries.

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.
- Web-based management, using the XS-3900 unit's embedded Web Management Interface (WMI). This method provides configuration and basic monitoring tools, and is good for small deployments (one or two units).
- Web-based management, using the optional Xirrus Wireless Management System (XM-3300). The XM-3300 is used for managing large XS-3900 deployments from a centralized Web-based interface and offers the following features:
    - Layer 3 appliance
    - Globally manage large numbers of XS-3900 units
    - Seamless view of the entire wireless network
    - Easily configure large numbers of XS-3900 units
    - Rogue AP monitoring
    - Easily manage system-wide firmware updates
    - Monitor performance and trends
    - Aggregation of alerts and alarms

Deployment Summary

The following table summarizes your deployment options for small and large deployments.

Function	Number of XS-3900 Units	
	One or Two	Three or More
Power	AC DC (with XP-3100)	AC DC (with XP-3100) UPS backup (recommended)
Failover	Recommended	Highly recommended
VLANs	Optional Required for guest access	Optional use, Can be used to put all APs on one VLAN or map to existing VLAN scheme Required for Guest Access
Encryption	WPA with TKIP (recommended) PSK or 802.1x	WPA2 with AES (recommended) 802.1x keying
Authentication	Internal RADIUS server Pre-Shared Key	External RADIUS server
Management	Internal WMI Internal CLI XM-3300	XM-3300

Installation Workflow

This workflow illustrates the steps that are required to install and configure the XS-3900 successfully. Review this flowchart before attempting to install the unit on a customer’s network.

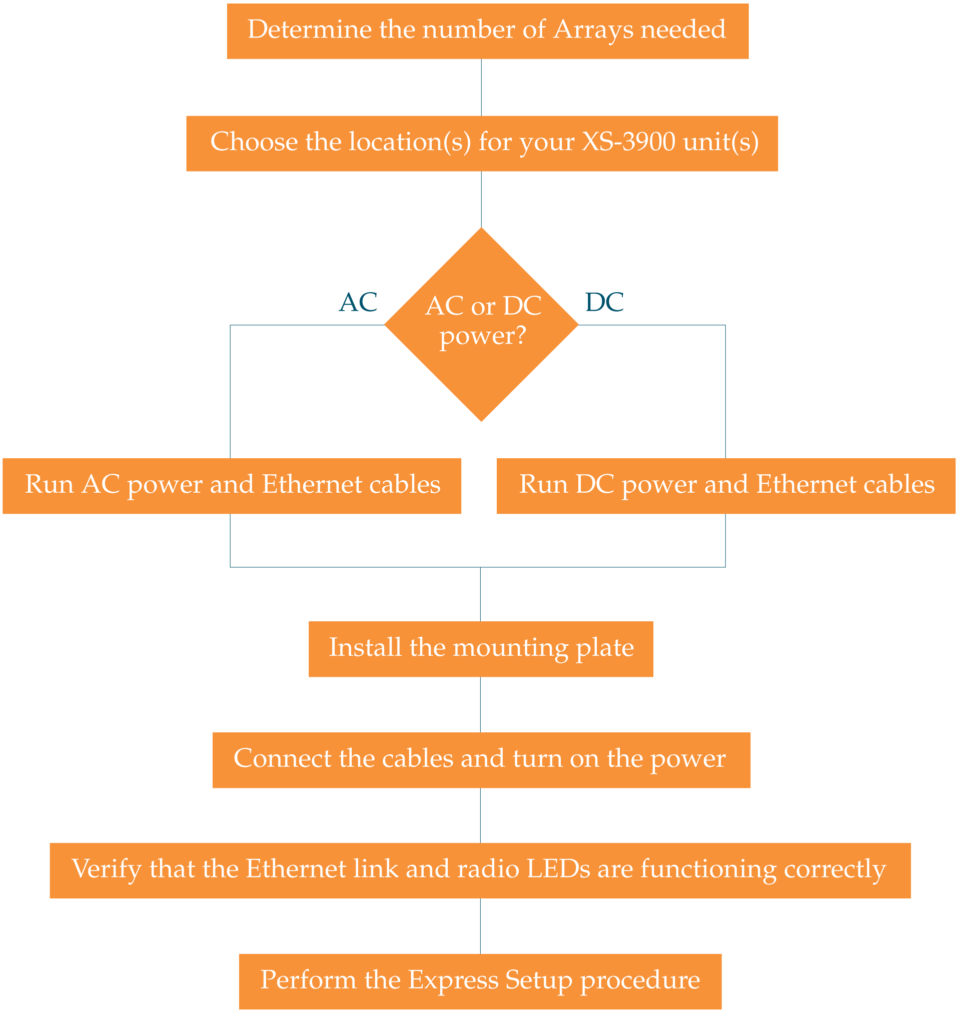

Determine the number of Arrays needed
Choose the location(s) for your XS-3900 unit(s)
AC
AC or DC power?
DC
Run AC power and Ethernet cables
Run DC power and Ethernet cables
Install the mounting plate
Connect the cables and turn on the power
Verify that the Ethernet link and radio LEDs are functioning correctly
Perform the Express Setup procedure

Figure 24. Installation Workflow

Unpacking the XS-3900

When you unpack your XS-3900, you will find the following items in the carton:

Item	Quantity
Xirrus Wireless LAN Array (XS-3900) module	1
AC power cord	1
Mounting plate	1
Mounting screws	4
Screw anchors	4
Tile grid mounting clamps	4
Clamp nuts	4
Mounting template	1
End User License Agreement (EULA)	1
CD-ROM containing: This User's Guide in PDF format README file	1
Quick Install Guide	1
Registration Card	1

Installing the XS-3900

This section provides instructions for installing the XS-3900 unit.

Choosing a Location

Based on coverage, capacity and deployment examples discussed earlier in this chapter, choose a location for your XS-3900 that will provide the best results for your needs. The XS-3900 was designed to be mounted on a ceiling where the unit is unobtrusive and wireless transmissions can travel unimpeded throughout open plan areas. Choose a location that is central to your users.

Wiring Considerations

Unless you are using the Xirrus Remote DC Power System (XP-3100) with the DC version of the XS-3900, an AC power outlet must be available to the XS-3900 (an AC power cord is provided with each unit). If you are using the XP-3100 to distribute DC power to multiple XS-3900 units, go to "Remote DC Power System (Optional)" on page 8.

Once you have determined the best location for your XS-3900, you must run cables to the location for the following services:

Power

- Dedicated AC power
- DC power (if using the XP-3100)

Network

- Gigabit 1
- Gigabit 2 (optional)
- Fast Ethernet (optional)
- Serial cable (see note)

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 XS-3900 can be managed from any of the available network connections, either Fast Ethernet, Gigabit 1 or Gigabit 2.

Mounting the Unit

Most offices have drop-down acoustical ceiling tiles set into a standard grid. The XS-3900 has been designed to enable mounting to a tiled ceiling via a mounting plate and clamps that attach to the grid. Once the mounting plate is attached, the XS-3900 simply rotates onto the plate (similar to a smoke detector). Once the unit is mounted it can be removed and re-attached easily, without the need for tools or modifications to the original installation.

This section assumes that you are mounting the XS-3900 to a tiled ceiling. If your ceiling is not tiled, the mounting plate can be attached directly to the ceiling with the screws and anchors provided (without using the tile grid mounting clamps).

Attaching the T-Bar Clips

The T-bar clips are used to create four mounting points on the ceiling tile grid for the XS-3900 mounting plate. Use the mounting template (provided) to find the correct location for all four clamps. To attach the clamps, simply twist the clamps onto the grid and tighten the screw post with a screwdriver.

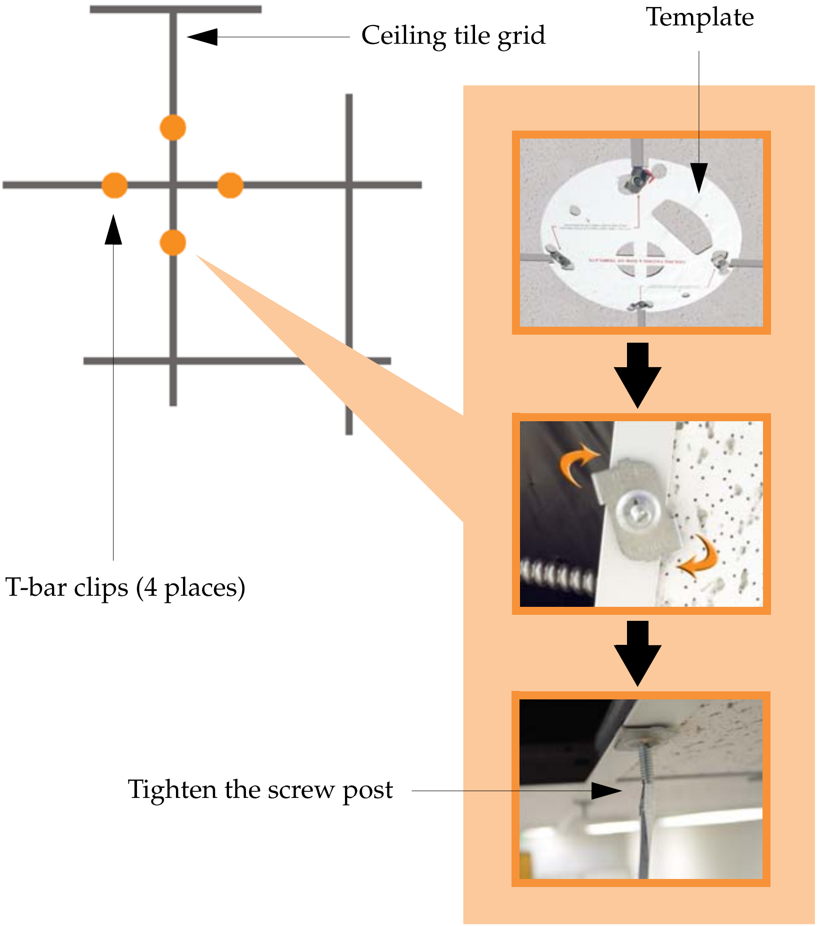


Figure 25. Attaching the T-Bar Clips

Installing the Mounting Plate

If necessary, orient the mounting plate (see "Attaching the T-Bar Clips" on page 39) and locate the plate on the four screw posts. Secure the mounting plate to the four clamps using the nuts provided. Once the mounting plate is secured, cut an access hole in the ceiling tile for the cables.

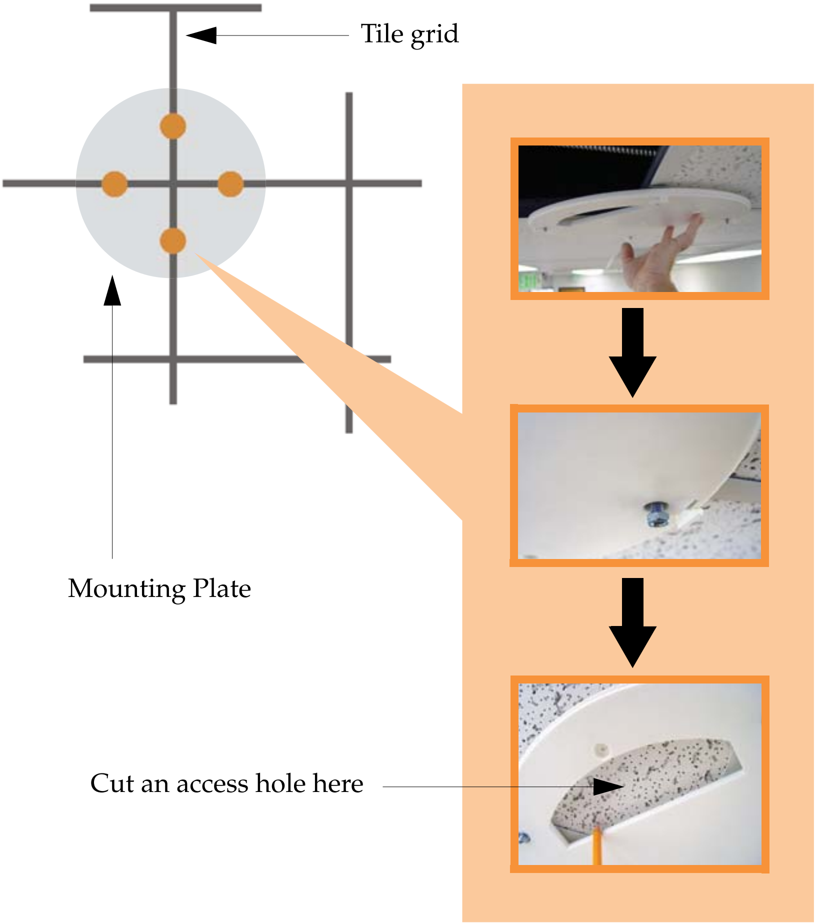


Figure 26. Installing the Mounting Plate

Connecting the Cables

Feed the power and Ethernet cables through the access hole in the tile and the mounting plate, then connect the cables to the unit. See also, "Wiring Considerations" on page 37.

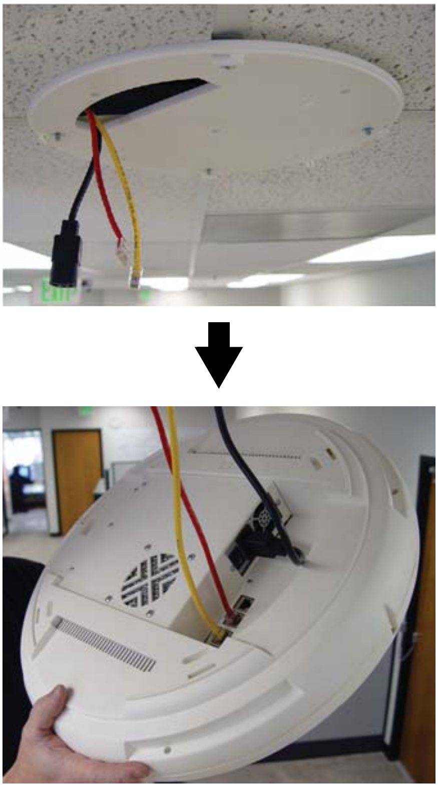


Figure 27. Connecting the Cables

When the cables are connected, turn on the power switch—before attaching the unit to the mounting plate (next step). Verify that the Ethernet link LED lights and the LED boot sequence begins. The radio LEDs on the front of the unit will illuminate in rotation, indicating that the XS-3900 software is loading and the unit is functioning correctly.

Attaching the Array to the Mounting Plate

Align the port recess on the XS-3900 with the access hole in the mounting plate, then connect the XS-3900 with the lugs on the mounting plate (4 places) and turn the XS-3900 clockwise to lock the unit into place (similar to a smoke detector).

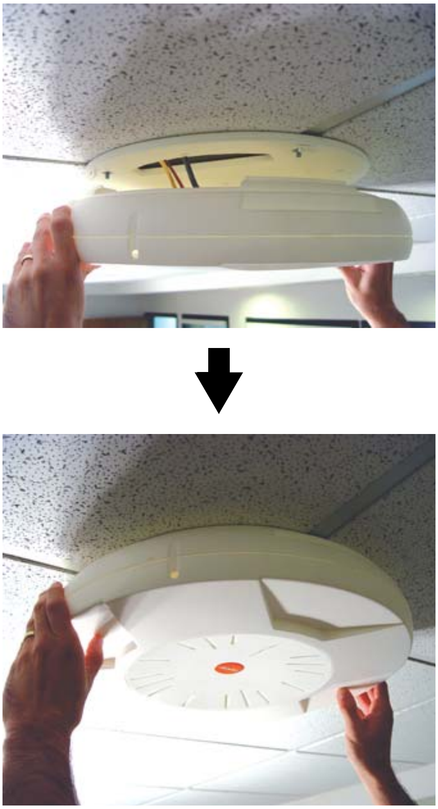


Figure 28. Attaching the Unit

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

Now that the XS-3900 is physically installed, you must run the Express Setup procedure from the unit's Web Management Interface to enable the radios and establish initial system configuration settings. Go to "Powering Up the XS-3900" on page 44.

Dismounting the Array

To dismount the array, place your fingers so as to increase the space between the array and the mounting plate at the positions indicated by the decals on the mounting plate—these are aligned with IAPs (radios) abg1 and abg3, as indicated on the clock-face of the array.

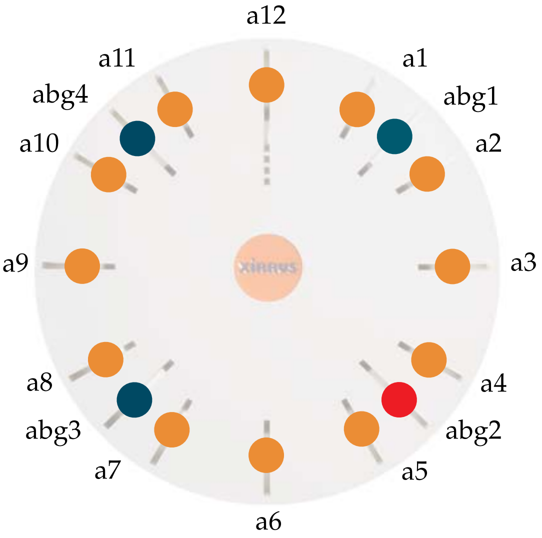


Figure 29. IAP (Radio) Positions

Powering Up the XS-3900

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. The normal boot sequence is as follows:

1. The green status LED will light first, showing a steady flashing while the unit boots. In the event of a boot failure, this LED will change to flashing red.
2. The Ethernet Link/Activity LEDs on the underside of the array will light for those ports connected to the network.
3. All IAP radio LEDs will light simultaneously.
4. While the array is booting, a sequential LED pattern will cycle through all the radio LEDs.
5. When the array completes boot, the status LED will show a steady green, and all radio lights will show the current state of those radios.

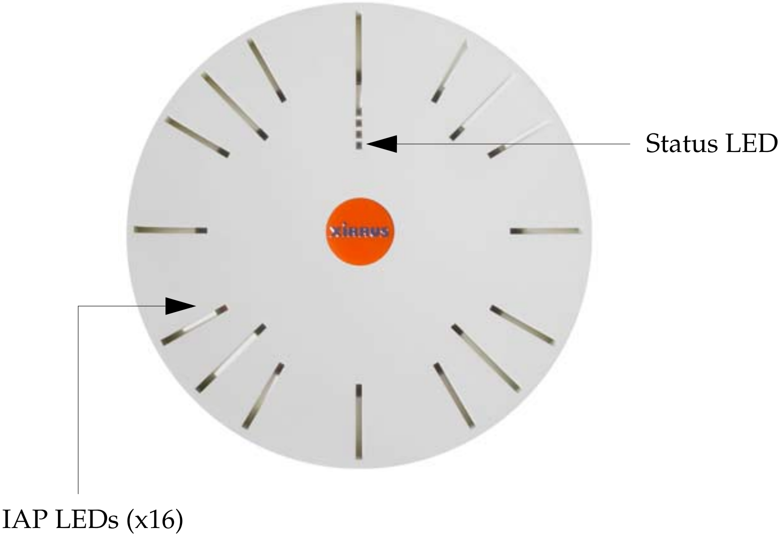
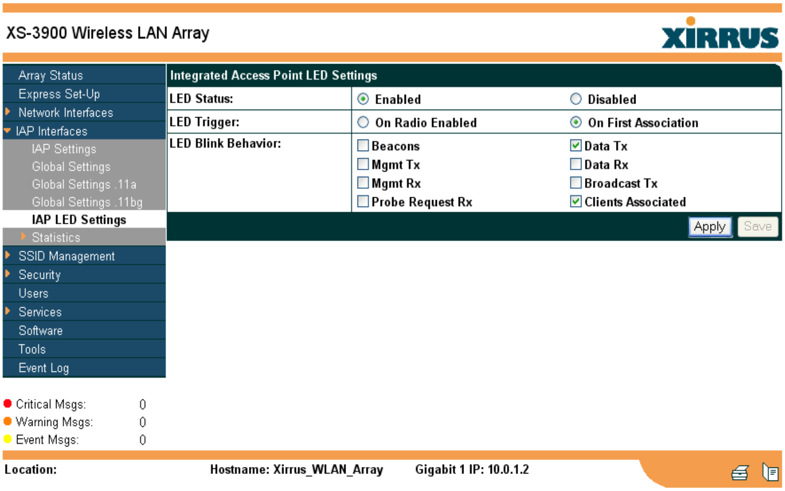


Figure 30. LED Locations

Once the unit is fully booted the default IAP LED display will be as follows:

- IAP radio LEDs that are enabled will show a steady orange for 802.11a radios, or green for 802.11b/g radios.
- Once a client associates with an individual IAP, that LED will show a slow flash (heartbeat) pattern.
- When data is transmitted or received by an IAP, that IAP's LED will flash. The rate of flashing changes with the number of packets sent or received per second—the LED will flash more quickly with a greater number of packets per second and more slowly with lower numbers of packets per second.

These 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 "IAP LED Settings" on page 88.



Integrated Access Point LED Settings

LED Status:	● Enabled	○ Disabled
LED Trigger:	○ On Radio Enabled	● On First Association
LED Blink Behavior:	☐ Beacons ☐ Mgmt Tx ☐ Mgmt Rx ☐ Probe Request Rx	☑ Data Tx ☐ Data Rx ☐ Broadcast Tx ☑ Clients Associated

● Critical Msgs: 0
● Warning Msgs: 0
● Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 31. WMI: IAP LED Settings Page

Establishing Communication with the Array

The XS-3900 can be configured through the Command Line Interface (CLI) or the graphical Web Management Interface (WMI). You can use the CLI via the serial management port, the Fast Ethernet port, or either of the Gigabit Ethernet ports. You can use the WMI via any of the array’s Ethernet ports.

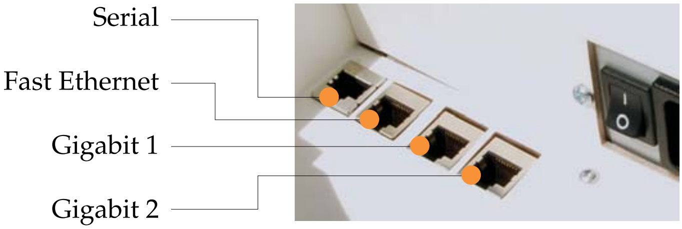


Figure 32. Network Interface Ports

Using the Serial Port

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

Using the Ethernet Ports

If the array is booted and does not receive DHCP addresses on either the Fast Ethernet or Gigabit Ethernet ports, the Fast Ethernet port will default to an IP address of 10.0.0.1 and both Gigabit Ethernet ports will default to 10.0.1.2.

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

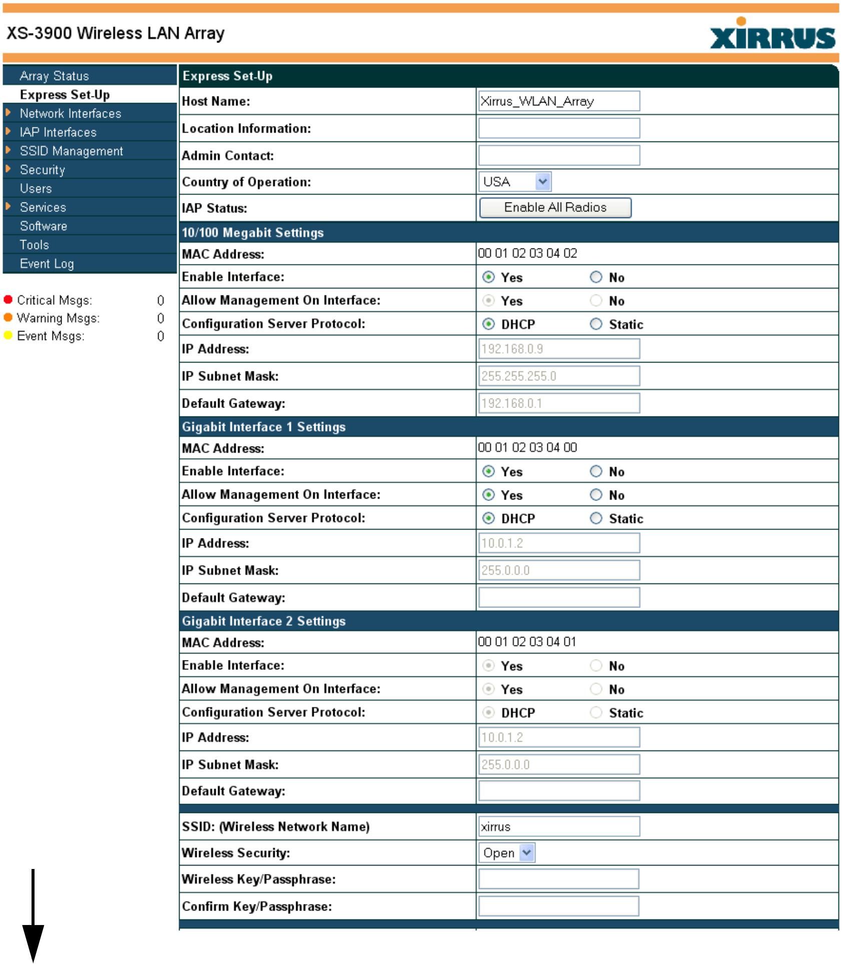
1. Examine the DHCP tables on the server and find the addresses assigned to the array (Xirrus MAC addresses begin with 000F7D).
2. Query the array using the CLI via the serial port. Use the **show summary ethernet** command to view the IP addresses assigned to each port.

Logging In

When logging in to the array, use the default user name and password (the default for both is **admin**).

Performing the Express Setup Procedure

The Express Setup procedure allows you to establish global configuration settings that will enable basic XS-3900 functionality. Any changes you make on this page will affect all radios. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.

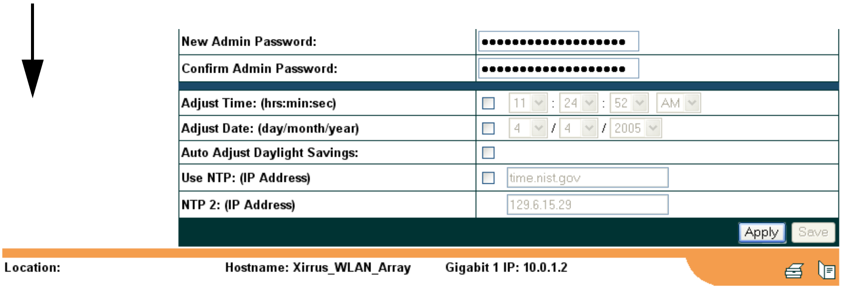


Express Set-Up	
Host Name:	Xirrus_WLAN_Array
Location Information:	
Admin Contact:	
Country of Operation:	USA
IAP Status:	Enable All Radios
10/100 Megabit Settings	
MAC Address:	00 01 02 03 04 02
Enable Interface:	◉ Yes ○ No
Allow Management On Interface:	◉ Yes ○ No
Configuration Server Protocol:	◉ DHCP ○ Static
IP Address:	192.168.0.9
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Gigabit Interface 1 Settings	
MAC Address:	00 01 02 03 04 00
Enable Interface:	◉ Yes ○ No
Allow Management On Interface:	◉ Yes ○ No
Configuration Server Protocol:	◉ DHCP ○ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	
Gigabit Interface 2 Settings	
MAC Address:	00 01 02 03 04 01
Enable Interface:	◉ Yes ○ No
Allow Management On Interface:	◉ Yes ○ No
Configuration Server Protocol:	◉ DHCP ○ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	
SSID: (Wireless Network Name)	xirrus
Wireless Security:	Open
Wireless Key/Passphrase:	
Confirm Key/Passphrase:	

more ...

Figure 33. WMI: Express Setup Page (Part 1)

... continued



New Admin Password:	•••••••••••••••••••
Confirm Admin Password:	•••••••••••••••••••
Adjust Time: (hrs:min:sec)	□ 11 : 24 : 52 AM
Adjust Date: (day/month/year)	□ 4 / 4 / 2005
Auto Adjust Daylight Savings:	□
Use NTP: (IP Address)	□ time.nist.gov
NTP 2: (IP Address)	129.6.15.29

Figure 34. WMI: Express Setup Page (Part 2)

Procedure for Performing an Express Setup

1. **Host Name**: Specify a unique host name for this XS-3900 unit. The host name is used to identify the XS-3900 on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters.

2. **Location Information**: Enter a brief but meaningful description that accurately defines the physical location of this XS-3900 unit. 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 this XS-3900 unit at the designated location.

4. **Country of Operation**: To ensure that the array remains in compliance with local regulatory laws, the Country of Operation is set at the factory and cannot be changed.

5. **IAP Status**: This option provides a button that allows you to enable all radios. Simply click on the **Enable All Radios** button to enable all radios for this Wireless LAN Array.

6. Configure the **Fast Ethernet**, **Gigabit 1** and **Gigabit 2** network interfaces. The fields for each of these interfaces are the same, and include:

   a. **MAC Address**: This field displays the hardware MAC address for the network interface and cannot be changed.

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

   c. **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.

   d. **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 IP** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following information:

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

7. **SSID (Wireless Network Name)**: Enter a unique SSID, up to 32 characters. 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 is "**xirrus**."

   For additional information about SSIDs, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 186.

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

   WEP (Wired Equivalent Privacy)
   An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

   WPA (Wi-Fi Protected Access)
   A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1X for authentication. WPA is the stronger of the two wireless security schemes.

   For more information about security, including a full review of all security options and settings, go to "Security Management" on page 98.

   Security settings will only take effect if they are assigned to a specific SSID. Refer to "SSID Management" on page 92.

9. **Wireless Key/Passphrase**: Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase.

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

10. **New Admin Password**: If desired, enter a new administration password for managing this array. Choose a password that is not obvious, and one that you can remember. If you forget your password, you must reset the array to its factory defaults so that the password is reset to **admin** (its default setting).

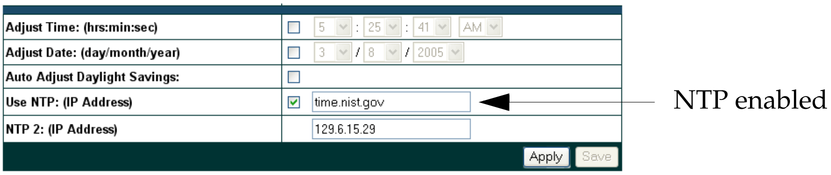
    a. **Confirm Admin Password**: If you entered a new administration password, confirm the new password here.

11. **Adjust Time (hrs:min:sec)**: 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).

12. **Adjust Date (day/month/year)**: 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 (day, month, year) in the corresponding fields. If you don’t want to adjust the current date, this box should be left unchecked (default).

13. **Auto Adjust Daylight Savings**: Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).

14. **Use NTP (IP Address)**: Check this box if you want to use an NTP (Network Time Protocol) server to synchronize the array’s clock. This ensures that syslog time-stamping is maintained across all units. Without an NTP server assigned (no universal clock), each array will use its own internal clock and stamp times accordingly, which may result in discrepancies. When this box is checked, the NTP and NTP 2 IP address fields become active. If you don’t want to use an NTP server, leave this box unchecked (default), otherwise enter the IP address or DNS name of the NTP server.



Adjust Time: (hrs:min:sec)	□ 5 : 25 : 41 AM
Adjust Date: (day/month/year)	□ 3 / 8 / 2005
Auto Adjust Daylight Savings:	□
Use NTP: (IP Address)	☑ time.nist.gov
NTP 2: (IP Address)	129.6.15.29

NTP enabled

Figure 35. Enabling the NTP Feature

a. **NTP 2 (IP Address)**: If you enabled the NTP option and the site is using a secondary NTP server, enter the IP address or DNS name of the secondary NTP server.

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

    This ends the Express Setup procedure.

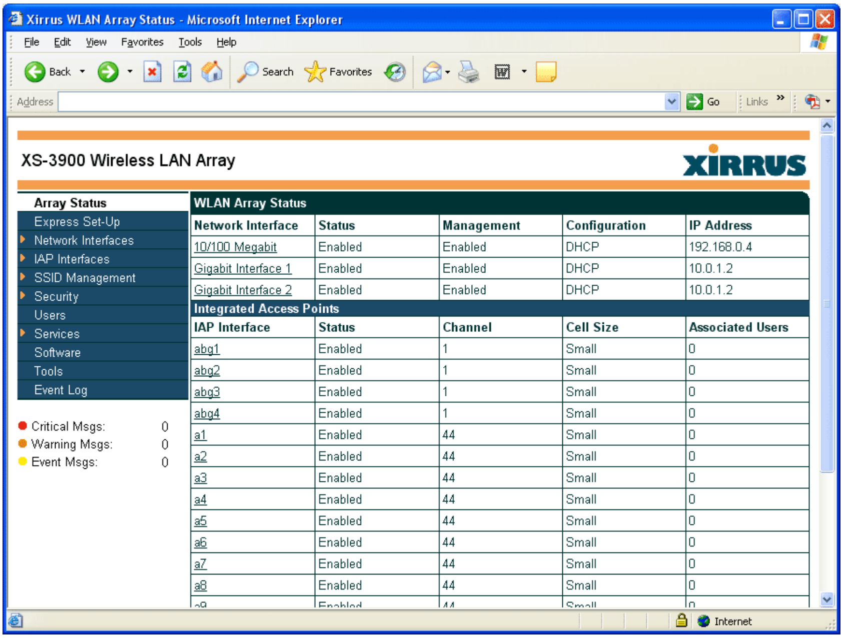
The Web Management Interface

This chapter provides an overview of the XS-3900's embedded Web Management Interface (WMI), used for establishing your network's configuration settings and wireless operating parameters. Section headings for this chapter include:

- An Overview

An Overview

The WMI is an easy-to-use graphical interface to your XS-3900. It allows you to configure the product to suit your individual requirements and ensure that the unit functions efficiently and effectively.



WLAN Array Status

Network Interface	Status	Management	Configuration	IP Address
10/100 Megabit	Enabled	Enabled	DHCP	192.168.0.4
Gigabit Interface 1	Enabled	Enabled	DHCP	10.0.1.2
Gigabit Interface 2	Enabled	Enabled	DHCP	10.0.1.2

Integrated Access Points

IAP Interface	Status	Channel	Cell Size	Associated Users
abg1	Enabled	1	Small	0
abg2	Enabled	1	Small	0
abg3	Enabled	1	Small	0
abg4	Enabled	1	Small	0
a1	Enabled	44	Small	0
a2	Enabled	44	Small	0
a3	Enabled	44	Small	0
a4	Enabled	44	Small	0
a5	Enabled	44	Small	0
a6	Enabled	44	Small	0
a7	Enabled	44	Small	0
a8	Enabled	44	Small	0
a9	Enabled	44	Small	0

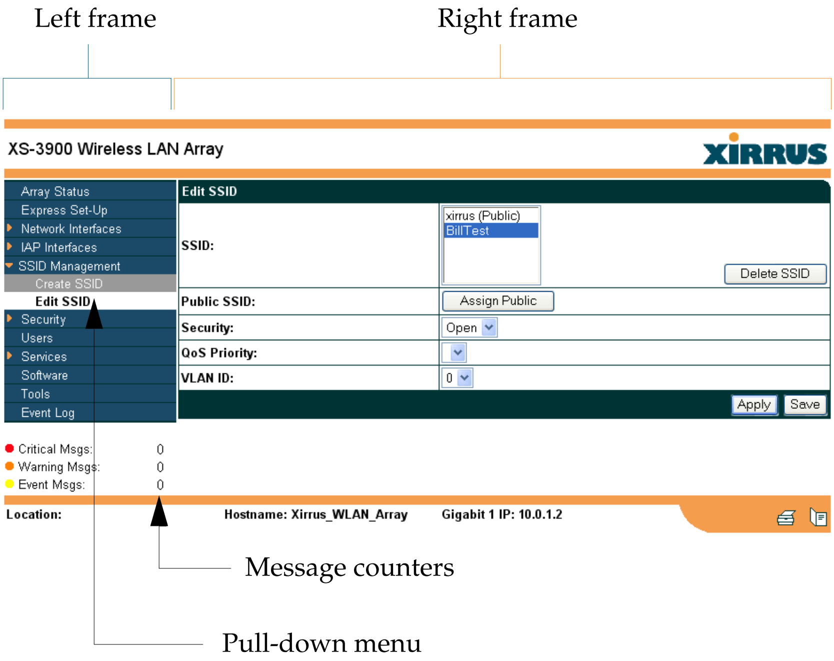
Figure 36. Web Management Interface

Content

The content of the WMI has been organized by function and hierarchy, shown here in list form. You can click on any item in the list to jump to the referenced destination.

Structure

The WMI has been designed with simplicity in mind, making navigation quick and easy. In the following example, you'll see that pages are divided into left and right frames. The left frame contains configuration elements organized by function (for example, radio interfaces, security, etc.), and where these functions are sub-divided there is an associated pull-down menu. Also included in the left frame are three counters that provide a running total of messages generated by the syslog subsystem during your session—organized into **Critical**, **Warning** and **Event** messages.



Edit SSID

SSID:	xirrus (Public) BillTest
Public SSID:	
Security:	Open
QoS Priority:	
VLAN ID:	0

Critical Msgs:	0
Warning Msgs:	0
Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 37. WMI: Frames

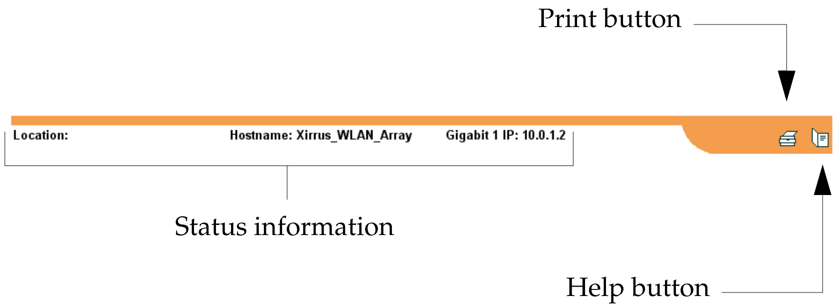
The right frame contains the configuration parameters for the XS-3900. This is where you input data (if you want to make changes) or review the XS-3900's current status and activity.

Status Bar

Below the configuration frames you will find a status bar containing information about this XS-3900 unit, including:

- Location—displays the location information assigned to the unit.
- Host name—the host name assigned to this unit.
- Network interface IP address—the IP address of the network interface that is currently being used.

Also included in the status bar is a **Print** button and a **Help** button. Click on the Print button to send a print file of the active page to your local printer, or click on the Help button to go to the XS-3900's online help system.



Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 38. WMI: Status Bar

Applying Configuration Changes

When you have defined all your settings on any WMI configuration page, you must click on the **Apply** button for the changes to take effect in the current session. Click on the **Save** button to write your changes (for future sessions).

Character Restrictions

When inputting strings in the WMI (for example, assigning SSIDs, host name, password, etc.), use only common alphanumeric characters. Do not use any of the following characters:

& < > ' “ / \

Configuring the XS-3900

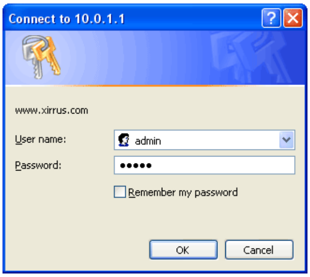
This chapter covers configuration and management tasks using the product's embedded Web Management Interface (WMI). It also includes a procedure for logging in to the XS-3900 with your Web browser. Section headings for this chapter include:

- Logging In
- Making Configuration Changes to the XS-3900

Logging In

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

1. Establish a network connection and open your Web browser.
2. Connect to the XS-3900 via its default IP address (10.0.1.1).
3. When connected to the XS-3900, a login prompt appears on your screen. The default login user name and password is **admin** (for both). Login names and passwords are case-sensitive.
4. To log in to the XS-3900's Web Management Interface, enter **admin** when prompted for a user name and password.



Connect to 10.0.1.1

www.xirrus.com

User name: admin

Password: •••••

□ Remember my password

Figure 39. WMI: Logging In to the XS-3900

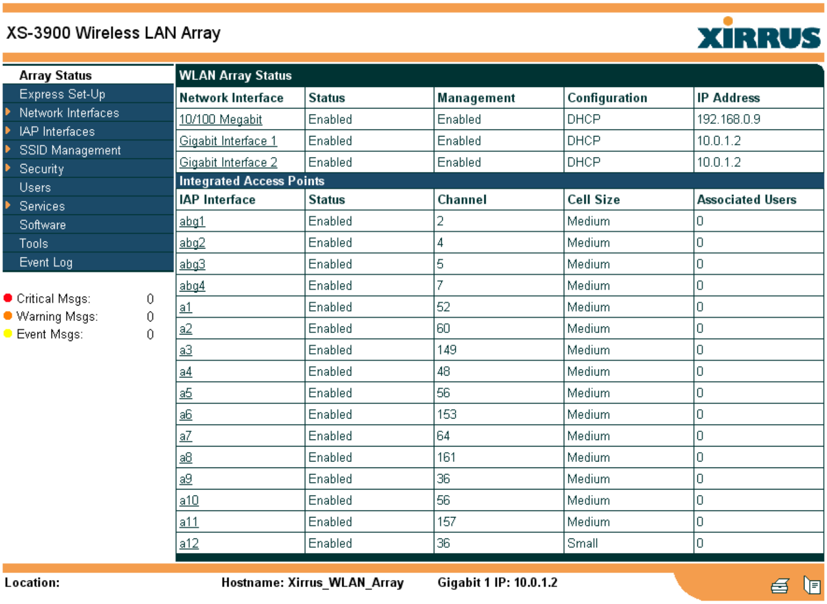
Making Configuration Changes to the XS-3900

This section has been organized into functional areas that reflect the flow and content of the WMI. Configuration instructions to the XS-3900 require you to input data in one or more of the following formats:

- Specifying data (for example, IP addresses, descriptions, etc.).
- Making selections from pull-down lists.
- Choosing an option by clicking on a radio button (for example, on/off).
- Clicking on a check box to activate/deactivate a feature.
- Clicking on a button to confirm a command or apply your changes.

Array Status

This is a status only page that provides a snapshot of the global configuration settings for all XS-3900 network interfaces and radios. You must go to the appropriate configuration page to make changes to any of the settings displayed here (configuration changes cannot be made from this page).



● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

WLAN Array Status

Network Interface	Status	Management	Configuration	IP Address
10/100 Megabit	Enabled	Enabled	DHCP	192.168.0.9
Gigabit Interface 1	Enabled	Enabled	DHCP	10.0.1.2
Gigabit Interface 2	Enabled	Enabled	DHCP	10.0.1.2

Integrated Access Points

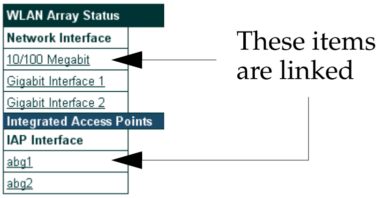
IAP Interface	Status	Channel	Cell Size	Associated Users
abg1	Enabled	2	Medium	0
abg2	Enabled	4	Medium	0
abg3	Enabled	5	Medium	0
abg4	Enabled	7	Medium	0
a1	Enabled	52	Medium	0
a2	Enabled	60	Medium	0
a3	Enabled	149	Medium	0
a4	Enabled	48	Medium	0
a5	Enabled	56	Medium	0
a6	Enabled	153	Medium	0
a7	Enabled	64	Medium	0
a8	Enabled	161	Medium	0
a9	Enabled	36	Medium	0
a10	Enabled	56	Medium	0
a11	Enabled	157	Medium	0
a12	Enabled	36	Small	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 40. WMI: Array Status Page

The Array Status page is sub-divided into the **Network Interface** and **IAP Interface** (radio) sections and provides you with the following information:

- **All devices**: A listing of the available Network Interfaces and IAPs with each item containing a link to the associated configuration page. Linked items are shown UNDERLINED. For example:

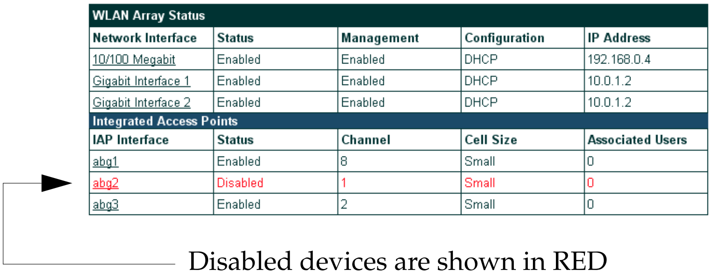


WLAN Array Status
Network Interface
10/100 Megabit
Gigabit Interface 1
Gigabit Interface 2
Integrated Access Points
IAP Interface
abg1
abg2

These items are linked

Figure 41. Linked Items

- **All devices**: The current status of each device, whether enabled or disabled. Devices that are disabled are shown in RED. For example:



WLAN Array Status

Network Interface	Status	Management	Configuration	IP Address
10/100 Megabit	Enabled	Enabled	DHCP	192.168.0.4
Gigabit Interface 1	Enabled	Enabled	DHCP	10.0.1.2
Gigabit Interface 2	Enabled	Enabled	DHCP	10.0.1.2

Integrated Access Points

IAP Interface	Status	Channel	Cell Size	Associated Users
abg1	Enabled	8	Small	0
abg2	Disabled	1	Small	0
abg3	Enabled	2	Small	0

Disabled devices are shown in RED

Figure 42. WMI: Disabled Device (Partial View)

- **Network Interface devices**:
  - The **Management** column indicates whether the network interface device is enabled or disabled. Network interfaces are enabled or disabled on the Network Settings page.
  - The **Configuration** column shows how each network interface obtains its IP address—either dynamically via DHCP or entered manually by you (static configuration) on the Network Settings page.

- The **IP Address** column shows the current IP address being used by each network interface device.

- **IAP Interface devices**:
  - The **Channel** column shows on which channel each IAP (radio) is operating. Channel selections are made on the IAP Settings page from a pull-menu. To avoid co-channel interference, adjacent radios should not be using adjacent channels.
  - The **Cell Size** column indicates which cell size setting is currently active for each radio—either small, medium, large or manually defined by you. The cell size of a radio is a function of its transmit power and determines the radio's overall coverage. Cell sizes are defined on the IAP Settings page. For additional information about cell sizes and the importance of planning for and defining the optimum sizes for your array, go to "Coverage and Capacity Planning" on page 21.

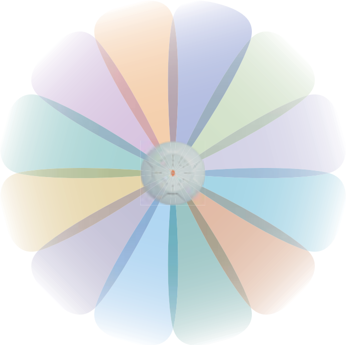
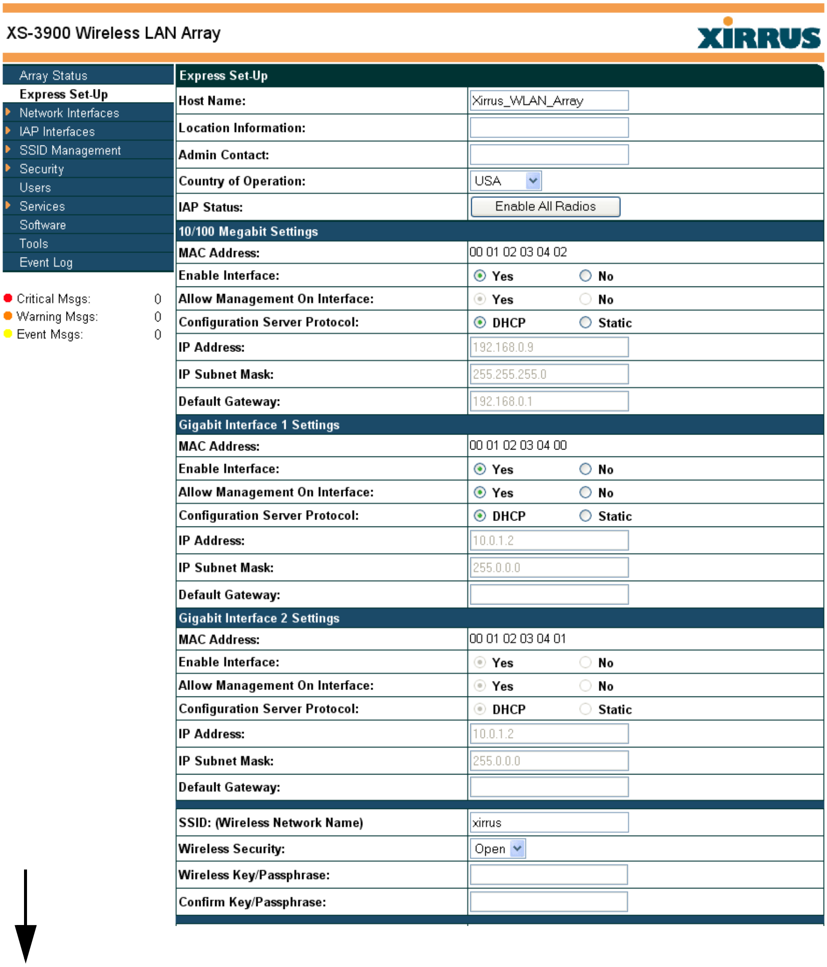


Figure 43. IAP Cells

  - The **Associated Users** column informs you how many users are currently associated with each radio. The high-capacity XS-3900 can handle up to 64 concurrent users per individual IAP radio (or 960 users per array).

Express Setup

This page allows you to establish global configuration settings that will enable basic XS-3900 functionality. Any changes you make on this page will affect all radios. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.

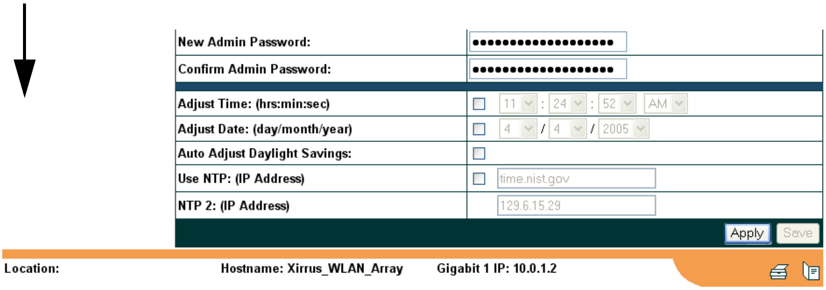


Express Set-Up	
Host Name:	Xirrus_WLAN_Array
Location Information:	
Admin Contact:	
Country of Operation:	USA
IAP Status:	Enable All Radios
10/100 Megabit Settings	
MAC Address:	00 01 02 03 04 02
Enable Interface:	● Yes ○ No
Allow Management On Interface:	● Yes ○ No
Configuration Server Protocol:	● DHCP ○ Static
IP Address:	192.168.0.9
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Gigabit Interface 1 Settings	
MAC Address:	00 01 02 03 04 00
Enable Interface:	● Yes ○ No
Allow Management On Interface:	● Yes ○ No
Configuration Server Protocol:	● DHCP ○ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	
Gigabit Interface 2 Settings	
MAC Address:	00 01 02 03 04 01
Enable Interface:	● Yes ○ No
Allow Management On Interface:	● Yes ○ No
Configuration Server Protocol:	● DHCP ○ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	
SSID: (Wireless Network Name)	xirrus
Wireless Security:	Open
Wireless Key/Passphrase:	
Confirm Key/Passphrase:	

more ...

Figure 44. WMI: Express Setup Page (Part 1)

... continued



New Admin Password:	•••••••••••••••••••
Confirm Admin Password:	•••••••••••••••••••
Adjust Time: (hrs:min:sec)	□ 11 : 24 : 52 AM
Adjust Date: (day/month/year)	□ 4 / 4 / 2005
Auto Adjust Daylight Savings:	□
Use NTP: (IP Address)	□ time.nist.gov
NTP 2: (IP Address)	129.6.15.29

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 45. WMI: Express Setup Page (Part 2)

Procedure for Performing an Express Setup

1. **Host Name**: Specify a unique host name for this XS-3900 unit. The host name is used to identify the XS-3900 on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters.

2. **Location Information**: Enter a brief but meaningful description that accurately defines the physical location of this XS-3900 unit. 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 this XS-3900 unit at the designated location.

4. **Country of Operation**: To ensure that the array remains in compliance with local regulatory laws, the Country of Operation is set at the factory and cannot be changed.

5. **IAP Status**: This option provides a button that allows you to enable all radios. Simply click on the **Enable All Radios** button to enable all radios for this Wireless LAN Array.

6. Configure the **Fast Ethernet**, **Gigabit 1** and **Gigabit 2** network interfaces. The fields for each of these interfaces are the same, and include:

   a. **MAC Address**: This field displays the hardware MAC address for the network interface and cannot be changed.

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

   c. **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.

   d. **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 IP** if you intend to enter IP addresses manually. If you choose the Static IP option, you must enter the following information:

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

7. **SSID (Wireless Network Name)**: Enter a unique SSID, up to 32 characters. 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 is "**xirrus**."

   For additional information about SSIDs, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 186.

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

   WEP (Wired Equivalent Privacy)
   An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

   WPA (Wi-Fi Protected Access)
   A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1X for authentication. WPA is the stronger of the two wireless security schemes.

   For more information about security, including a full review of all security options and settings, go to"Security Management" on page 98.

9. **Wireless Key/Passphrase**: Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase.

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

10. **New Admin Password**: If desired, enter a new administration password for managing this array. Choose a password that is not obvious, and one that you can remember. If you forget your password, you must reset the array to its factory defaults so that the password is reset to **admin** (its default setting).

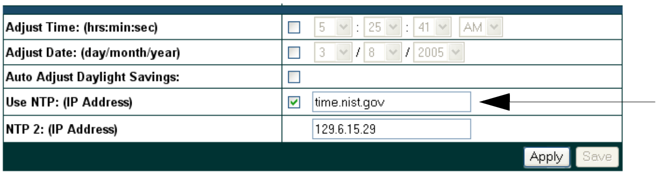
    a. **Confirm Admin Password**: If you entered a new administration password, confirm the new password here.

11. **Adjust Time (hrs:min:sec)**: 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).

12. **Adjust Date (day/month/year)**: 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 (day, month, year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).

13. **Auto Adjust Daylight Savings**: Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).

14. **Use NTP (IP Address)**: Check this box if you want to use an NTP (Network Time Protocol) server to synchronize the array's clock. This ensures that syslog time-stamping is maintained across all units. Without an NTP server assigned (no universal clock), each array will use its own internal clock and stamp times accordingly, which may result in discrepancies. When this box is checked, the NTP and NTP 2 IP address fields become active. If you don't want to use an NTP server, leave this box unchecked (default), otherwise enter the IP address or DNS name of the NTP server.



Adjust Time: (hrs:min:sec)	□ 5 : 25 : 41 AM
Adjust Date: (day/month/year)	□ 3 / 8 / 2005
Auto Adjust Daylight Savings:	□
Use NTP: (IP Address)	☑ time.nist.gov
NTP 2: (IP Address)	129.6.15.29

NTP enabled

Figure 46. Enabling the NTP Feature

a. **NTP 2 (IP Address)**: If you enabled the NTP option and the site is using a secondary NTP server, enter the IP address or DNS name of the secondary NTP server.

15. Click on the **Apply** button to apply the new settings to this session

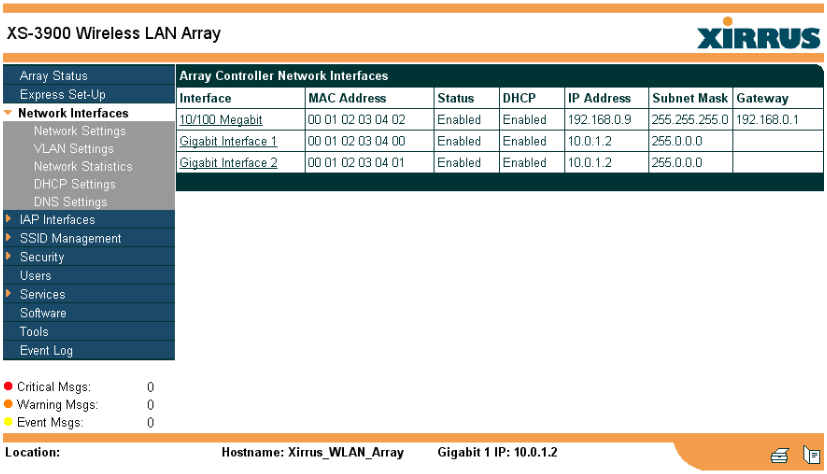
16. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

This ends the Express Setup procedure.

Network Interfaces

This is a status only page that provides a snapshot of the configuration settings currently established for the 10/100 Fast Ethernet interface and the 10/100/1000 Gigabit 1 and Gigabit 2 interfaces. You must go to the appropriate configuration page to make changes to any of the settings displayed here (configuration changes cannot be made from this page).

You can click on any item in the **Interface** column to “jump” to the associated configuration page.



Array Controller Network Interfaces

Interface	MAC Address	Status	DHCP	IP Address	Subnet Mask	Gateway
10/100 Megabit	00 01 02 03 04 02	Enabled	Enabled	192.168.0.9	255.255.255.0	192.168.0.1
Gigabit Interface 1	00 01 02 03 04 00	Enabled	Enabled	10.0.1.2	255.0.0.0	
Gigabit Interface 2	00 01 02 03 04 01	Enabled	Enabled	10.0.1.2	255.0.0.0	

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 47. WMI: Network Interfaces Page

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

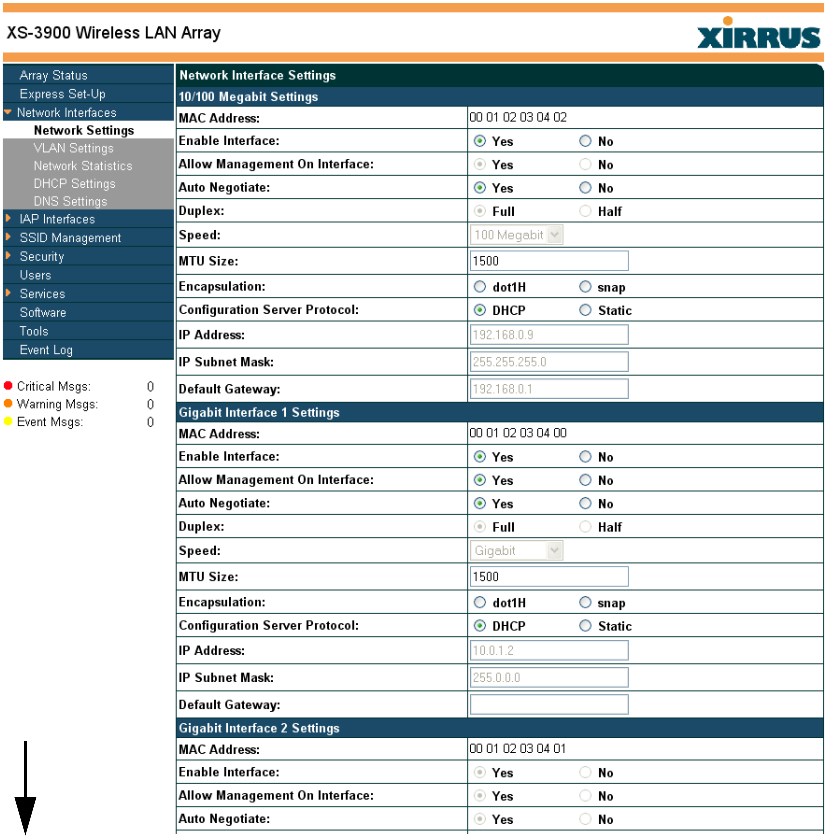
- “Network Settings” on page 67.
- “VLAN Settings” on page 71.
- “Network Statistics” on page 74.
- “DHCP Server Settings” on page 75.
- “DNS Settings” on page 76.

Network Settings

This page allows you to establish configuration settings for the 10/100 Fast Ethernet interface and the 10/100/1000 Gigabit 1 and Gigabit 2 interfaces.

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

When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



XS-3900 Wireless LAN Array

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

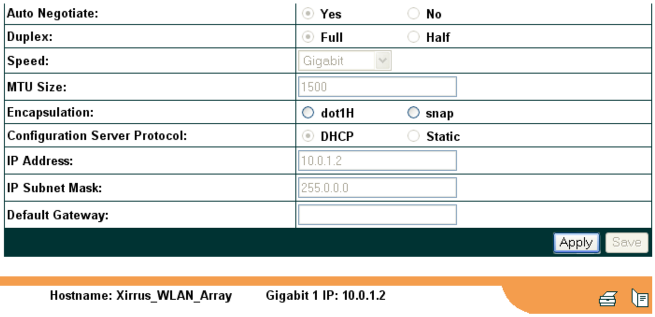
Network Interface Settings

10/100 Megabit Settings		
MAC Address:	00 01 02 03 04 02	
Enable Interface:	● Yes	○ No
Allow Management On Interface:	● Yes	○ No
Auto Negotiate:	● Yes	○ No
Duplex:	● Full	○ Half
Speed:	100 Megabit	
MTU Size:	1500	
Encapsulation:	○ dot1H	○ snap
Configuration Server Protocol:	● DHCP	○ Static
IP Address:	192.168.0.9	
IP Subnet Mask:	255.255.255.0	
Default Gateway:	192.168.0.1	
Gigabit Interface 1 Settings		
MAC Address:	00 01 02 03 04 00	
Enable Interface:	● Yes	○ No
Allow Management On Interface:	● Yes	○ No
Auto Negotiate:	● Yes	○ No
Duplex:	● Full	○ Half
Speed:	Gigabit	
MTU Size:	1500	
Encapsulation:	○ dot1H	○ snap
Configuration Server Protocol:	● DHCP	○ Static
IP Address:	10.0.1.2	
IP Subnet Mask:	255.0.0.0	
Default Gateway:		
Gigabit Interface 2 Settings		
MAC Address:	00 01 02 03 04 01	
Enable Interface:	● Yes	○ No
Allow Management On Interface:	● Yes	○ No
Auto Negotiate:	● Yes	○ No

more ...

Figure 48. WMI: Network Settings Page (Part 1)

... continued



Auto Negotiate:	● Yes ○ No
Duplex:	● Full ○ Half
Speed:	Gigabit
MTU Size:	1500
Encapsulation:	○ dot1H ○ snap
Configuration Server Protocol:	● DHCP ○ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 49. WMI: Network Settings Page (Part 2)

Network Interface Ports

The following diagram shows the location of each network interface port on the underside of the XS-3900.

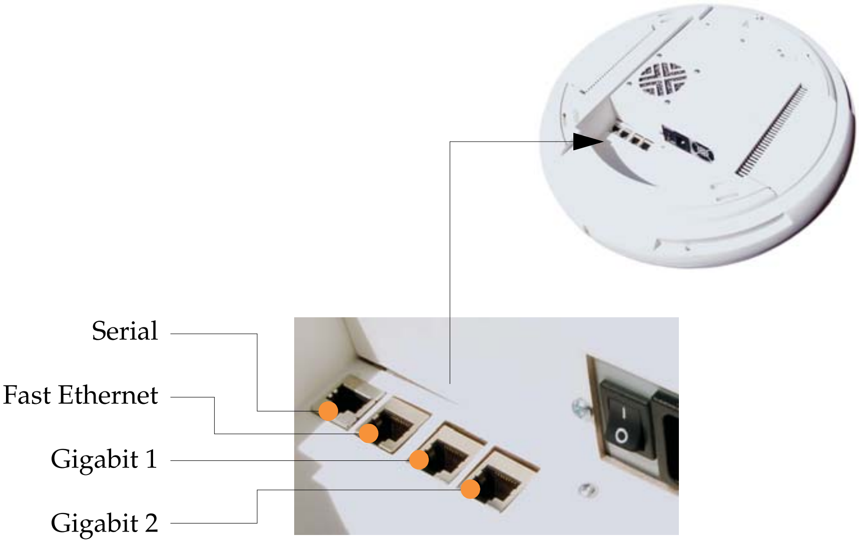


Figure 50. Network Interface Ports

Procedure for Configuring the Network Interfaces

1. Configure the **Fast Ethernet**, **Gigabit 1** and **Gigabit 2** network interfaces. The fields for each of these interfaces are the same, and include:

    a. **MAC Address**: This field shows the MAC address for this array. The MAC (hardware) address is used to identify the Xirrus array to the wired network. The MAC address is a static value and cannot be changed.

    b. **Enable Interface**: Choose **Yes** to enable this network interface (Fast Ethernet, Gigabit 1 or Gigabit 2), or choose **No** to disable the interface.

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

    d. **Auto Negotiate**: This feature allows the array to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available).

    - **Duplex**: Full-duplex refers to the transmission of data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). In contrast, half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device because it allows only one party to talk at any one time). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.
    - **Speed**: If the Auto-Negotiate feature is disabled, you can manually choose the desired data transmission speed from the pull-down list, either **Fast Ethernet** or **Gigabit**.

e. **MTU Size**: Specify the MTU (Maximum Transmission Unit) size. When you specify the MTU, you are defining—in bytes—the largest physical packet size that the network can transmit. Any messages larger than the MTU that you specify here are divided into smaller packets before being sent. The default is 1000 bytes.

f. **Encapsulation**: Choose either **dot1H** (802.1H) or **snap** (SNAP) as the Ethernet encapsulation type.

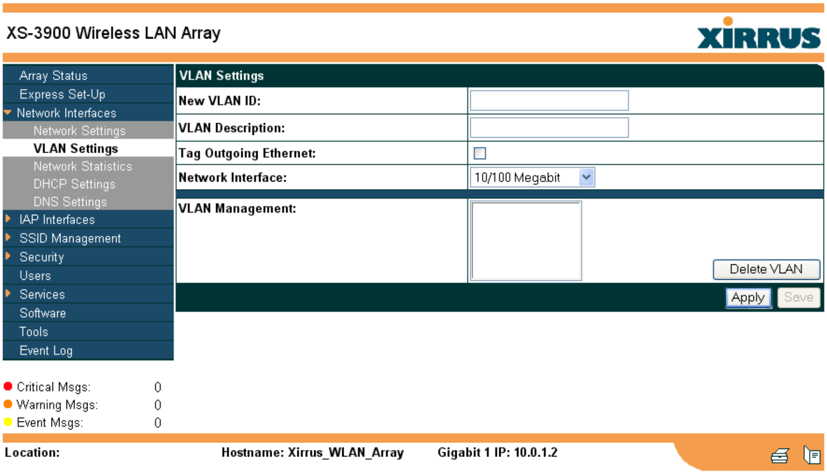
g. **Configuration Server Protocol**: Choose **DHCP** to instruct the XS-3900 to use DHCP when assigning IP addresses to the array, or choose **Static IP** if you intend to enter IP addresses manually.

- **IP Address**: If you selected the Static IP option, enter a valid IP address for this XS-3900 unit. To use any of the remote connections (Web, SNMP, or SSH), a valid IP address must be established.
- **IP Subnet Mask**: If you selected the Static IP option, enter a valid IP address for the subnet mask (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the XS-3900 is located.
- **Default Gateway**: If you selected the Static IP option, enter a valid IP address for the default gateway. This is the IP address of the router that the XS-3900 uses to transmit data to other networks.

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

VLAN Settings

This page allows you to add or remove VLANs, associate VLANs to a specific network interface, and enable VLAN tagging of outgoing traffic. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



XS-3900 Wireless LAN Array

VLAN Settings

New VLAN ID:

VLAN Description:

Tag Outgoing Ethernet: □

Network Interface: 10/100 Megabit

VLAN Management:

● Critical Msgs: 0
● Warning Msgs: 0
● Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 51. WMI: VLAN Settings Page

Understanding VLANs

A VLAN (Virtual LAN) is a switch network that is logically segmented—by functions, project teams, or applications rather than on a physical or geographical basis. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN, regardless of their physical connections to the network, or the fact that they might be intermingled with other teams. You use VLANs to reconfigure the network through software rather than physically unplugging and moving devices or wires.

A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (for example, bridges and routers), connected by a single bridging domain.

The bridging domain is supported on various pieces of network equipment, such as LAN switches, that operate bridging protocols between them with a separate group for each VLAN.

VLANs provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address scalability, security, and network management. You should consider several key issues when designing and building switched LAN networks:

- LAN segmentation
- Security
- Broadcast control
- Performance
- Network management
- Communication between VLANs

You extend VLANs into a wireless LAN by adding IEEE 802.11Q tag awareness to the Xirrus array. Frames destined for different VLANs are transmitted by the array wirelessly on different SSIDs. Conversely, packets coming from a client associated with a certain VLAN are 802.11Q tagged before they are forwarded onto the wired network.

Procedure for Configuring VLANs

1. **New VLAN ID**: Enter a new VLAN ID number (between 0 and 4012) that matches your network's VLAN scheme.
2. **VLAN Description**: Enter a meaningful description for this VLAN.
3. **Tag Outgoing**: Check this box if you want to enable VLAN tagging of outgoing traffic.
4. **Network Interface**: Select the interface you want to associate to this VLAN. Make your selection from the choices available in the pull-down list—either Fast Ethernet, Gigabit 1 or Gigabit 2.

5. **VLAN Management**: This list shows the VLANs that are currently assigned to the array. Each time you create a VLAN, the new VLAN is listed here. To delete a VLAN, select the VLAN from the list and click on the **Delete VLAN** button.

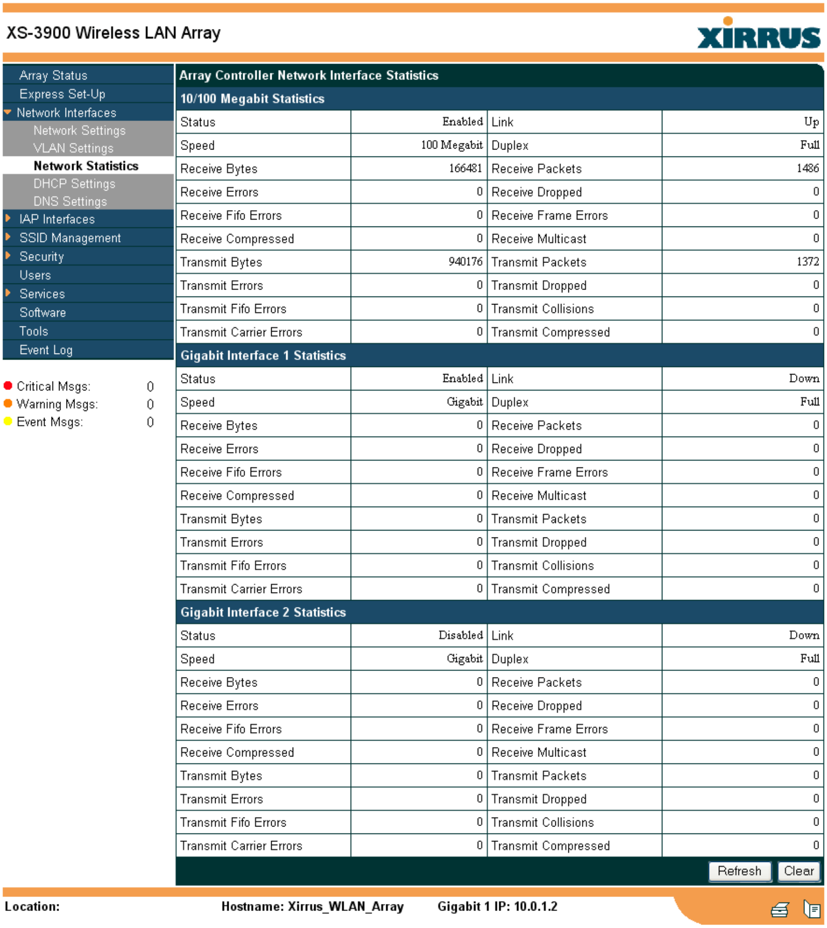
6. Click on the **Apply** button to apply the new settings to this session.

7. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

8. VLANs you defined can now be assigned to specific SSIDs.

Network Statistics

This is a status only page that allows you to review statistical data associated with each network interface and its activity. You can **Refresh** the data (update the page 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. If you are experiencing problems, you may also want to print this page for your records.



● Critical Msgs: 0
● Warning Msgs: 0
● Event Msgs: 0

Array Controller Network Interface Statistics

10/100 Megabit Statistics

Status	Enabled	Link	Up
Speed	100 Megabit	Duplex	Full
Receive Bytes	166481	Receive Packets	1486
Receive Errors	0	Receive Dropped	0
Receive Fifo Errors	0	Receive Frame Errors	0
Receive Compressed	0	Receive Multicast	0
Transmit Bytes	940176	Transmit Packets	1372
Transmit Errors	0	Transmit Dropped	0
Transmit Fifo Errors	0	Transmit Collisions	0
Transmit Carrier Errors	0	Transmit Compressed	0

Gigabit Interface 1 Statistics

Status	Enabled	Link	Down
Speed	Gigabit	Duplex	Full
Receive Bytes	0	Receive Packets	0
Receive Errors	0	Receive Dropped	0
Receive Fifo Errors	0	Receive Frame Errors	0
Receive Compressed	0	Receive Multicast	0
Transmit Bytes	0	Transmit Packets	0
Transmit Errors	0	Transmit Dropped	0
Transmit Fifo Errors	0	Transmit Collisions	0
Transmit Carrier Errors	0	Transmit Compressed	0

Gigabit Interface 2 Statistics

Status	Disabled	Link	Down
Speed	Gigabit	Duplex	Full
Receive Bytes	0	Receive Packets	0
Receive Errors	0	Receive Dropped	0
Receive Fifo Errors	0	Receive Frame Errors	0
Receive Compressed	0	Receive Multicast	0
Transmit Bytes	0	Transmit Packets	0
Transmit Errors	0	Transmit Dropped	0
Transmit Fifo Errors	0	Transmit Collisions	0
Transmit Carrier Errors	0	Transmit Compressed	0

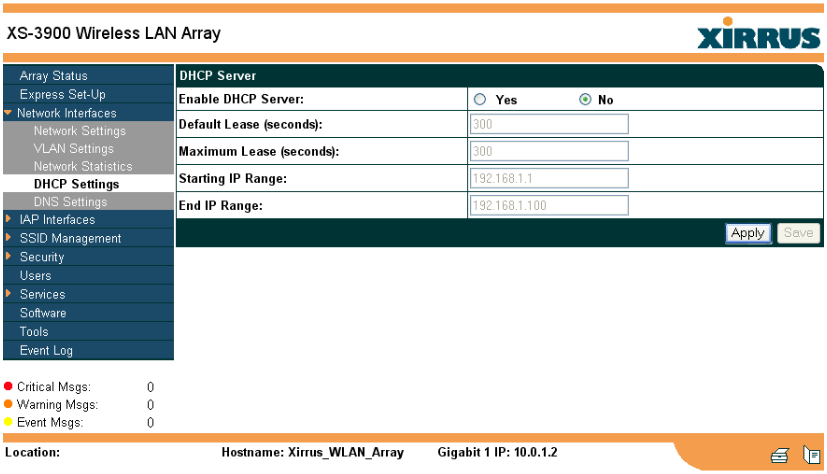
Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 52. WMI: Network Statistics Page

DHCP Server Settings

This page allows you to enable/disable DHCP (Dynamic Host Configuration Protocol) server functionality. DHCP allows the array to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network.

If you enable the DHCP server, you need to define the DHCP lease time (default and maximum) and establish the IP address range that the DHCP server can use. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



XS-3900 Wireless LAN Array

DHCP Server	
Enable DHCP Server:	○ Yes ● No
Default Lease (seconds):	300
Maximum Lease (seconds):	300
Starting IP Range:	192.168.1.1
End IP Range:	192.168.1.100

Critical Msgs:	0
Warning Msgs:	0
Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 53. WMI: DHCP Settings Page

Procedure for Configuring the DHCP Server

1. **Enable DHCP Server**: Choose **Yes** to enable DHCP services, or choose **No** to disable DHCP services.

2. **Default Lease (seconds)**: This field defines the default DHCP lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.

3. **Maximum Lease (seconds)**: Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.

4. **Starting IP Range**: Enter an IP address to define the start of the IP range that will be used by the DHCP server.

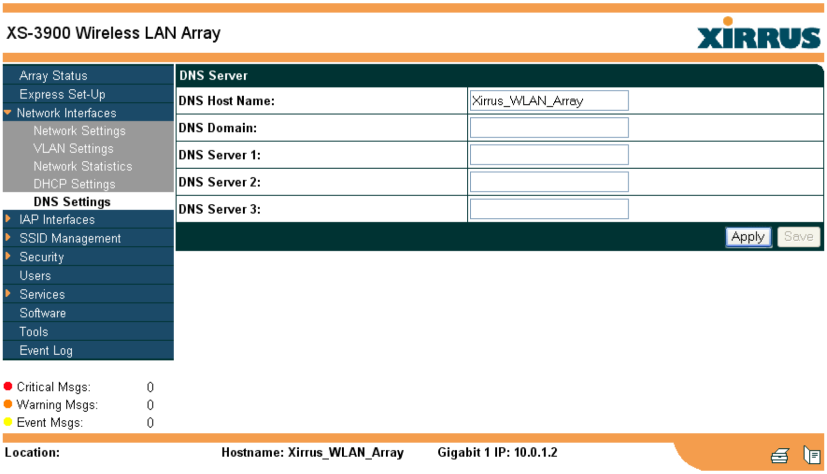
5. **End IP Range**: Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page.

6. Click on the **Apply** button to apply the new settings to this session.

7. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

DNS Settings

This page allows you to establish your DNS (Domain Name System) settings. At least one DNS server must be set up if you want to offer clients associating with this XS-3900 the ability to use meaningful host names instead of numerical IP addresses. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



DNS Server	
DNS Host Name:	Xirrus_WLAN_Array
DNS Domain:	
DNS Server 1:	
DNS Server 2:	
DNS Server 3:	

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 54. WMI: DNS Settings Page

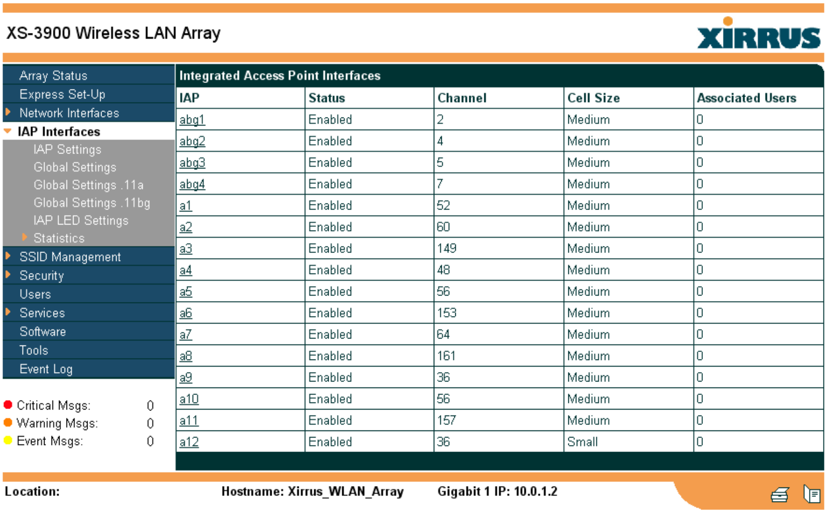
Procedure for Configuring DNS Servers

1. **DNS Host Name**: Enter a valid DNS host name.
2. **DNS Domain**: Enter the DNS domain name.
3. **DNS Server 1**: Enter the IP address of the primary DNS server.
4. **DNS Server 2**: Enter the IP address of the secondary DNS server.
5. **DNS Server 3**: Enter the IP address of the tertiary DNS server.
6. Click on the **Apply** button to apply the new settings to this session.
7. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

IAP Interfaces

This is a status only page that allows you to review configuration data associated with each Integrated Access Point (radio). It includes a list of which IAP radios are enabled, the channel that each radio is currently using, cell sizes, and how many users are currently associated with each radio. There are no configuration options available on this page, but if you are experiencing problems or simply reviewing the radio assignments, you may want to print this page for your records.

You can click on any item in the **IAP** column to “jump” to the associated configuration page.



Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Integrated Access Point Interfaces

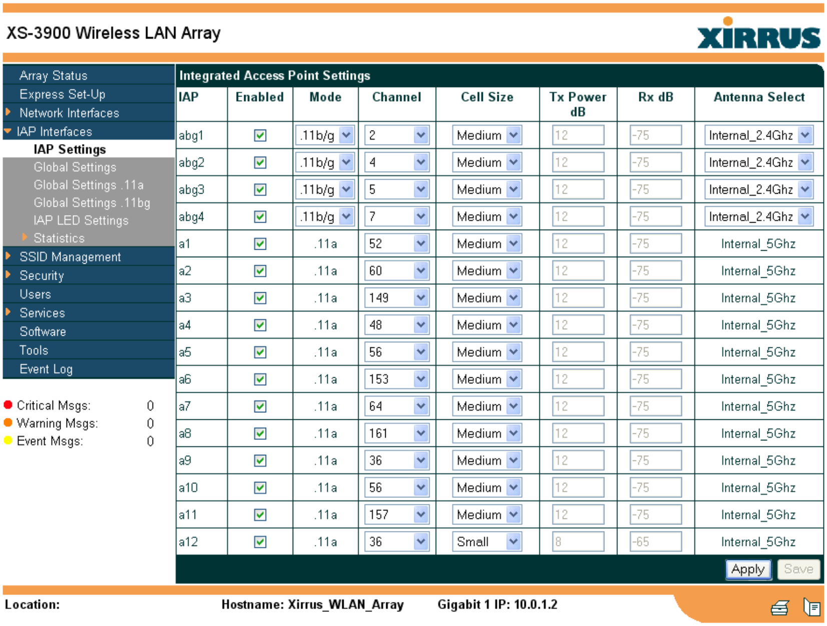
IAP	Status	Channel	Cell Size	Associated Users
abg1	Enabled	2	Medium	0
abg2	Enabled	4	Medium	0
abg3	Enabled	5	Medium	0
abg4	Enabled	7	Medium	0
a1	Enabled	52	Medium	0
a2	Enabled	60	Medium	0
a3	Enabled	149	Medium	0
a4	Enabled	48	Medium	0
a5	Enabled	56	Medium	0
a6	Enabled	153	Medium	0
a7	Enabled	64	Medium	0
a8	Enabled	161	Medium	0
a9	Enabled	36	Medium	0
a10	Enabled	56	Medium	0
a11	Enabled	157	Medium	0
a12	Enabled	36	Small	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 55. WMI: IAP Interfaces Page

IAP Settings

This page allows you to enable/disable Integrated Access Points (radios), define the wireless mode for each radio, specify the channel to be used and the cell size for each radio, establish transmit/receive parameters, and select antennas. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes. To see a diagram of the layout and naming of radios, go to Figure 6 on page 10.



Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Integrated Access Point Settings

IAP	Enabled	Mode	Channel	Cell Size	Tx Power dB	Rx dB	Antenna Select
abg1	☑	.11b/g	2	Medium	12	-75	Internal_2.4Ghz
abg2	☑	.11b/g	4	Medium	12	-75	Internal_2.4Ghz
abg3	☑	.11b/g	5	Medium	12	-75	Internal_2.4Ghz
abg4	☑	.11b/g	7	Medium	12	-75	Internal_2.4Ghz
a1	☑	.11a	52	Medium	12	-75	Internal_5Ghz
a2	☑	.11a	60	Medium	12	-75	Internal_5Ghz
a3	☑	.11a	149	Medium	12	-75	Internal_5Ghz
a4	☑	.11a	48	Medium	12	-75	Internal_5Ghz
a5	☑	.11a	56	Medium	12	-75	Internal_5Ghz
a6	☑	.11a	153	Medium	12	-75	Internal_5Ghz
a7	☑	.11a	64	Medium	12	-75	Internal_5Ghz
a8	☑	.11a	161	Medium	12	-75	Internal_5Ghz
a9	☑	.11a	36	Medium	12	-75	Internal_5Ghz
a10	☑	.11a	56	Medium	12	-75	Internal_5Ghz
a11	☑	.11a	157	Medium	12	-75	Internal_5Ghz
a12	☑	.11a	36	Small	8	-65	Internal_5Ghz

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 56. WMI: IAP Settings Page

Procedure for Auto Configuring IAPs (Radios)

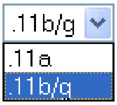
You can auto-configure radios by clicking on the **Auto Configure** button on the relevant WMI page (auto configuration only applies to enabled radios):

- For all radios, go to the Global Settings page.
- For all 802.11a radios, go to the Global Settings .11a page.
- For all 802.11b/g radios, go to the Global Settings .11bg page.

Procedure for Manually Configuring IAPs (Radios)

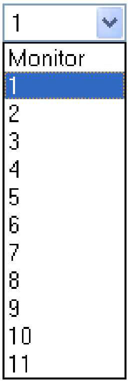
1. In the **Enabled** column, check the box of a corresponding radio to enable the radio, or uncheck the box if you want to disable the radio.

2. In the **Mode** column, select the wireless mode for this radio from the choices available in the pull-down menu (either .11a or .11b/g).



3. In the **Channel** column, select the channel you want this radio to use from the channels available in the pull-down list.

   The sample pull-down list shown here is for the **abg2** radio with its mode set to .11b/g. Any channels appearing in the list that are shown in RED are not recommended.



4. In the **Cell Size** column, choose either **Small**, **Medium**, or **Large** to define the desired pre-configured cell size, or choose **Manual** to define the wireless cell size manually. If you choose Manual, you must specify the transmit and receive power—in dB—in the **Tx Power dB** (transmit) and **Rx dB** (receive) fields.

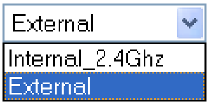
   The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the XS-3900's cell diameter.

   In a large office, or where user density is high, you should choose **Small** cells to achieve a higher data rate, since walls and other objects will not define the cells naturally.

   For additional information about cell sizes, go to "Coverage and Capacity Planning" on page 21.

5. In the **Antenna Select** column, choose the antenna you want this radio to use from the pull-down list. The list of available antennas will be different, depending on the wireless mode you selected for the radio.

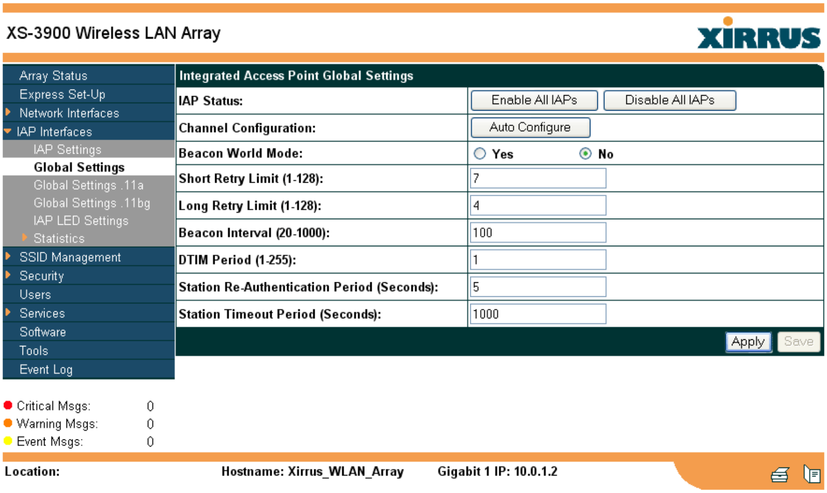
   The sample pull-down list shown here is for an 11a radio. In cases where the configuration of the array limits the antenna choice (for example, if no external antenna is available), the Antenna Select column is greyed out.



6. Click on the **Apply** button to apply the new settings to this session.
7. Click on the **Save** button to save your changes (otherwise your new settings will not take effect at the next reboot).

Global Settings

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



Integrated Access Point Global Settings

IAP Status:	Enable All IAPs Disable All IAPs
Channel Configuration:	Auto Configure
Beacon World Mode:	○ Yes ● No
Short Retry Limit (1-128):	7
Long Retry Limit (1-128):	4
Beacon Interval (20-1000):	100
DTIM Period (1-255):	1
Station Re-Authentication Period (Seconds):	5
Station Timeout Period (Seconds):	1000

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 57. WMI: Global Settings Page

Procedure for Configuring Global IAP Settings

1. **IAP Status**: Click on the **Enable All IAPs** button to enable all radios for this array, or click on the **Disable All IAPs** button to disable all radios.

2. **Channel Configuration**: Click on the **Auto Configure** button to instruct the array to determine the best channel allocation settings for each radio and select the channel automatically, based on changes in the environment. This is the recommended method for channel allocations.

3. **Beacon World Mode**: World Mode is a feature based on 802.11d. When this feature is enabled, the XS-3900 beacons out to client devices the correct legal set of channels and transmit power settings for the defined country code. This feature eliminates concerns about misconfigured client adapters because they will automatically know the correct channel set when communicating with the XS-3900. To enable the Beacon World Mode feature, choose **Yes**, or choose **No** to disable this feature. The default is disabled.

4. **Enable EDCF**: This feature allows for enhanced packet transmissions per IEEE 802.11e specifications and can improve throughput. Choose **Yes** to enable EDCF, or choose **No** to disable this feature.

5. **Short Retry Limit**: This attribute indicates the maximum number of transmission attempts for a frame, the length of which is less than or equal to the RTS Threshold, before a failure condition is indicated. The default value is 7. Enter a new value (1 to 128) in the **Short Retry Limit** field if you want to increase or decrease this attribute.

6. **Long Retry Limit**: This attribute indicates the maximum number of transmission attempts for a frame, the length of which is greater than the RTS Threshold, before a failure condition is indicated. The default value is 4. Enter a new value (1 to 128) in the **Long Retry Limit** field if you want to increase or decrease this attribute.

7. **Beacon Interval**: When the XS-3900 sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. Enter the desired value in the **Beacon Interval** field, between 20 and 1000. The value you enter here is applied to all radios.

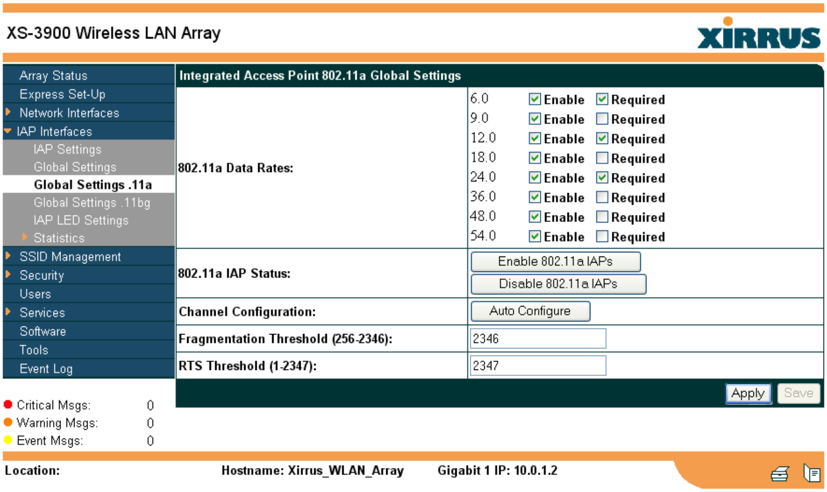
8. **DTIM Period**: A DTIM (Delivery Traffic Indication Message) is a signal sent as part of a beacon by the XS-3900 to a client device in sleep mode, alerting the device to a packet awaiting delivery. Enter the desired value in the **DTIM Period** field, between 1 and 255. The value you enter here is applied to all radios.

9. Click on the **Apply** button to apply the new settings to this session.

10. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Global Settings .11a

This page allows you to establish global 802.11a IAP (radio) settings. These settings include enabling or disabling 802.11a radios and making the data rates a required parameter, enabling or disabling all 802.11a radios, auto-configuration of channel allocations for all 802.11a radios, and specifying the fragmentation and RTS thresholds for all 802.11a radios.



Integrated Access Point 802.11a Global Settings

802.11a Data Rates:	6.0	☑ Enable	☑ Required
	9.0	☑ Enable	☐ Required
	12.0	☑ Enable	☑ Required
	18.0	☑ Enable	☐ Required
	24.0	☑ Enable	☑ Required
	36.0	☑ Enable	☐ Required
	48.0	☑ Enable	☐ Required
	54.0	☑ Enable	☐ Required
802.11a IAP Status:	Enable 802.11a IAPs Disable 802.11a IAPs		
Channel Configuration:	Auto Configure		
Fragmentation Threshold (256-2346):	2346		
RTS Threshold (1-2347):	2347		

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 58. WMI: Global Settings .11a Page

Procedure for Configuring Global 802.11a IAP Settings

1. **802.11a Data Rates**: The arrays allow you to enable or disable specific data rates for all 802.11a radios.

    - **Enabled**: Allow use of this data rate.
    - **Required**: Clients must support this data rate to associate with the network.

    In addition, you can make a specific data rate (for example, 12 Mbps) a required data rate, which means the 802.11a radios are required to support this data rate.

2. **.11a IAP Status**: Click on the **Enable 802.11a IAPs** button to enable all 802.11a radios for this array, or click on the **Disable 802.11a IAPs** button to disable all 802.11a radios.

3. **Channel Configuration**: Click on the **Auto Configure** button to instruct the array to determine the best channel allocation settings for each 802.11a radio and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11a channel allocations.

4. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11a radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346).

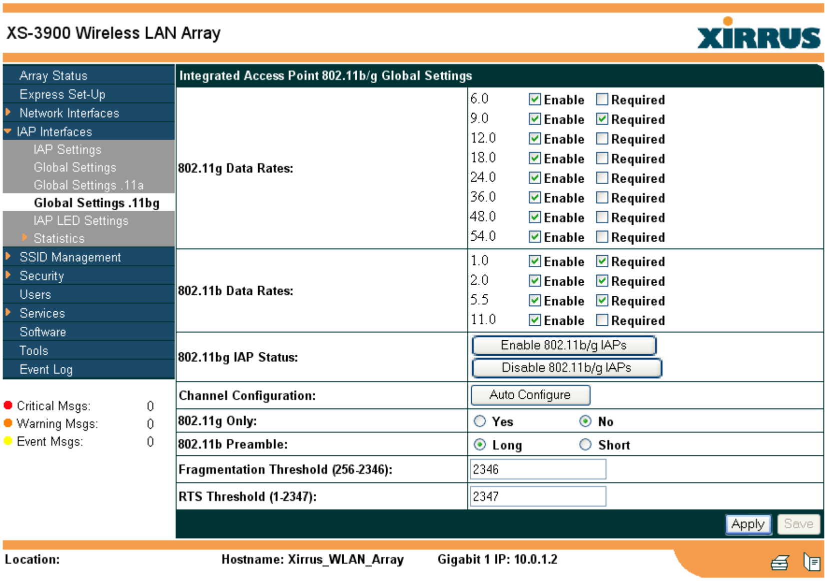
5. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.

6. Click on the **Apply** button to apply the new settings to this session.

7. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Global Settings .11bg

This page allows you to establish global 802.11a IAP (radio) settings. These settings include enabling or disabling 802.11a radios and making the data rates a required parameter, enabling or disabling all 802.11a radios, auto-configuration of channel allocations for all 802.11a radios, and specifying the fragmentation and RTS thresholds for all 802.11a radios.



Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Integrated Access Point 802.11b/g Global Settings

802.11g Data Rates:	6.0	☑ Enable	□ Required
	9.0	☑ Enable	☑ Required
	12.0	☑ Enable	□ Required
	18.0	☑ Enable	□ Required
	24.0	☑ Enable	□ Required
	36.0	☑ Enable	□ Required
	48.0	☑ Enable	□ Required
	54.0	☑ Enable	□ Required
802.11b Data Rates:	1.0	☑ Enable	☑ Required
	2.0	☑ Enable	☑ Required
	5.5	☑ Enable	☑ Required
	11.0	☑ Enable	□ Required
802.11bg IAP Status:	Enable 802.11b/g IAPs Disable 802.11b/g IAPs		
Channel Configuration:	Auto Configure		
802.11g Only:	○ Yes	● No	
802.11b Preamble:	● Long	○ Short	
Fragmentation Threshold (256-2346):	2346		
RTS Threshold (1-2347):	2347		

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 59. WMI: Global Settings .11bg Page

Procedure for Configuring Global 802.11b/g IAP Settings

1. **802.11g Data Rates**: The arrays allow you to enable or disable specific data rates for all 802.11g radios.

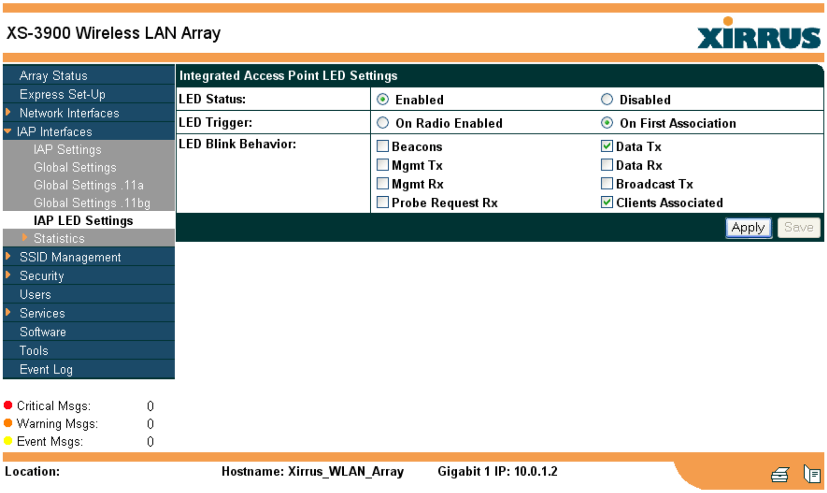
    - **Enabled**: Allow use of this data rate.
    - **Required**: Clients must support this data rate to associate with the network.

    In addition, you can make a specific data rate (for example, 12 Mbps) a required data rate, which means the 802.11a radios are required to support this data rate.

2. **802.11b Data Rates**: This task is similar to Step 1, but these data rates apply only to 802.11b radios.
3. **.11bg IAP Status**: Click on the **Enable 802.11b/g IAPs** button to enable all 802.11b/g radios for this array, or click on the **Disable 802.11b/g IAPs** button to disable all 802.11b/g radios.
4. **Channel Configuration**: Click on the **Auto Configure** button to instruct the array to determine the best channel allocation settings for each 802.11b/g radio and select the channel automatically, based on changes in the environment. This is the recommended method for 802.11b/g channel allocations.
5. **Fragmentation Threshold**: This is the maximum size for directed data packets transmitted over the 802.11b/g radio. Larger frames fragment into several packets, their maximum size defined by the value you enter here. Enter the desired **Fragmentation Threshold** value in this field, between 256 and 2346).
6. **RTS Threshold**: The RTS (Request To Send) Threshold specifies the packet size. Packets larger than the RTS threshold will use CTS/RTS prior to transmitting the packet—useful for larger packets to help ensure the success of their transmission. Enter a value between 1 and 2347.
7. Click on the **Apply** button to apply the new settings to this session.
8. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

IAP LED Settings

This page allows you to set up the array's IAP LEDs, including enabling or disabling the LED status functionality and assigning behavior preferences to the LEDs.



Integrated Access Point LED Settings

LED Status:	● Enabled	○ Disabled
LED Trigger:	○ On Radio Enabled	● On First Association
LED Blink Behavior:	□ Beacons □ Mgmt Tx □ Mgmt Rx □ Probe Request Rx	☑ Data Tx □ Data Rx □ Broadcast Tx ☑ Clients Associated

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

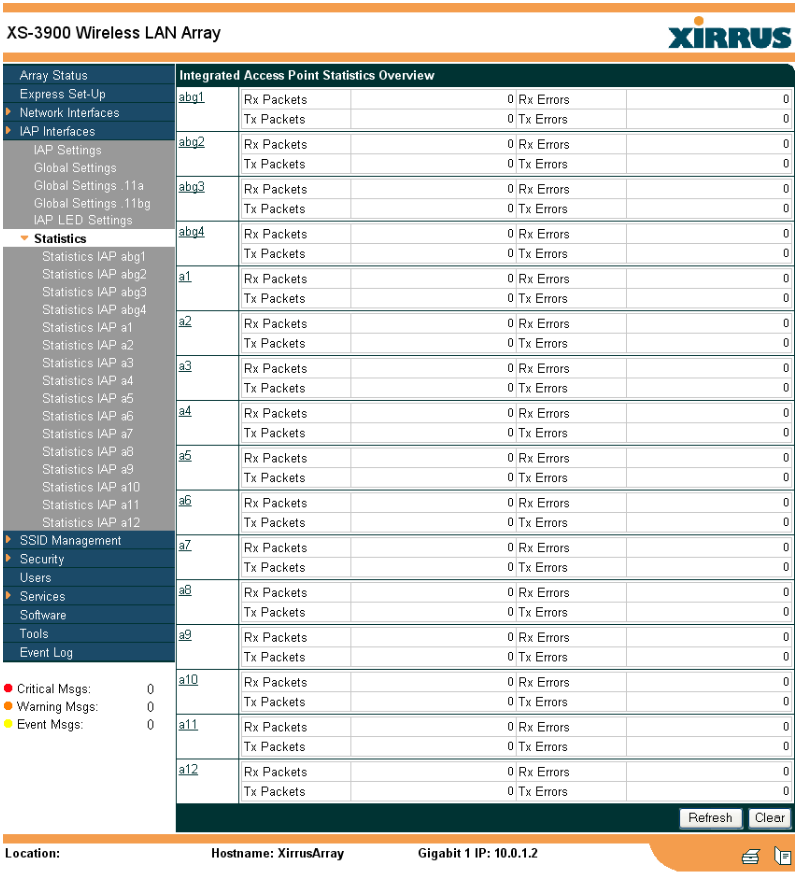
Figure 60. WMI: IAP LED Settings Page

Procedure for Configuring the IAP LEDs

1. **LED Status**: Choose **Enabled** to enable LED status functionality, or choose **Disabled** to disable the LEDs.
2. **LED Trigger**: This option determines which event triggers the LEDs, either when a radio is enabled or when a radio first associates with the network. Choose **On Radio Enabled** or **On First Association**, as desired.
3. **LED Blink Behavior**: This option allows you to select when the IAP LEDs blink, based on the activities you check here. From the choices available, select one or more activities to trigger when the LEDs blink.

Statistics

This is a status only page that provides an overview of the statistical data associated with individual radios. For more detailed information about a specific radio, simply click on any radio in the left column, or go to the statistics page for the desired radio (for example, Statistics IAP abg4). You can **Refresh** or **Clear** the data on this page at any time by clicking on the appropriate button. If you are experiencing problems, you may also want to print this page for your records.



Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Integrated Access Point Statistics Overview

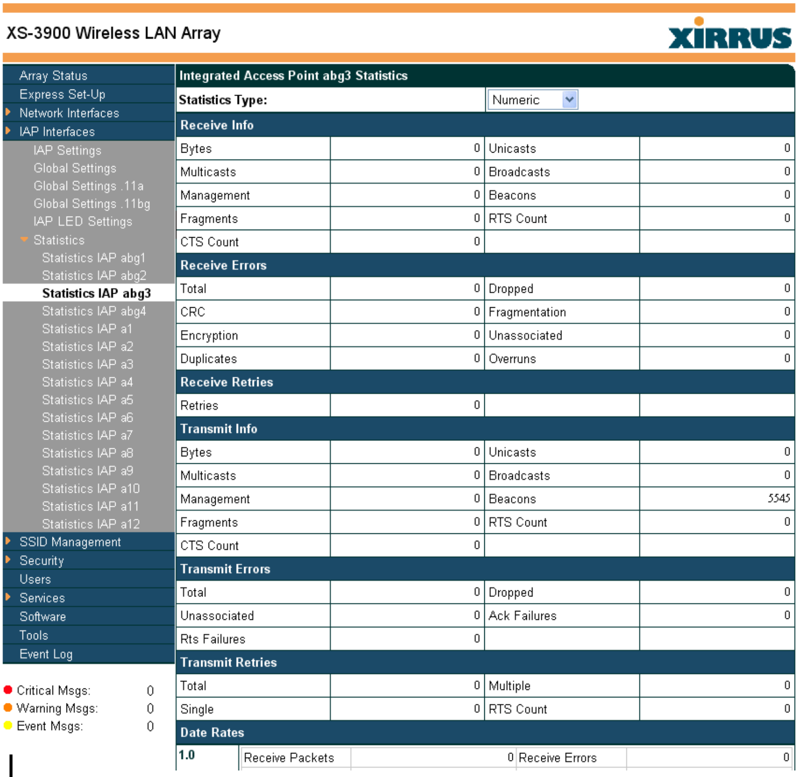
abg1	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
abg2	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
abg3	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
abg4	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a1	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a2	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a3	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a4	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a5	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a6	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a7	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a8	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a9	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a10	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a11	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0
a12	Rx Packets	0	Rx Errors	0
	Tx Packets	0	Tx Errors	0

Location: **Hostname: XirrusArray** **Gigabit 1 IP: 10.0.1.2**

Figure 61. WMI: Statistics Page

Statistics (for specific radios)

These pages provide a detailed statistical summary of each radio’s performance, displayed either numerically or by percentage (your choice). The following image shows an example of the **Statistics IAP abg3** page (for the abg3 radio). The default Statistics Type is NUMERIC, but you can change this to PERCENTAGE from the pull-down menu at the top of the page. In addition, you can **Refresh** or **Clear** the data on this page at any time by clicking on the appropriate button.



Integrated Access Point abg3 Statistics

Statistics Type: Numeric

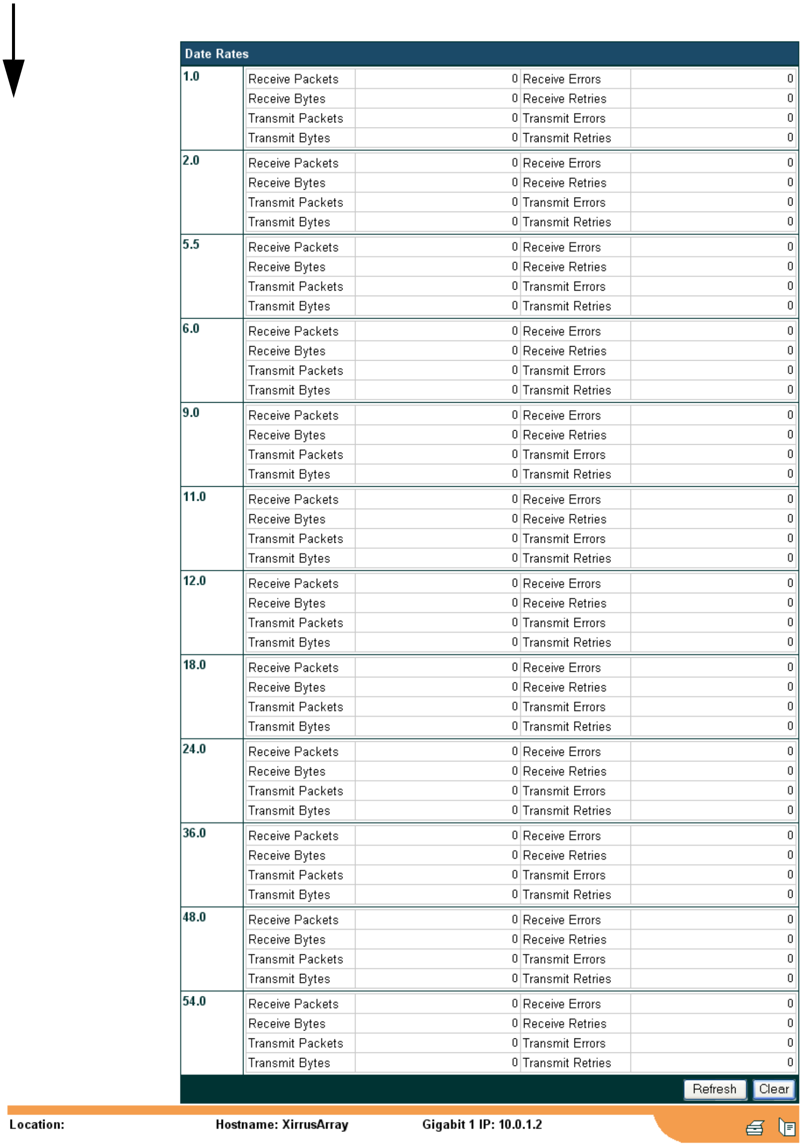
Receive Info			
Bytes	0	Unicasts	0
Multicasts	0	Broadcasts	0
Management	0	Beacons	0
Fragments	0	RTS Count	0
CTS Count	0		
Receive Errors			
Total	0	Dropped	0
CRC	0	Fragmentation	0
Encryption	0	Unassociated	0
Duplicates	0	Overruns	0
Receive Retries			
Retries	0		
Transmit Info			
Bytes	0	Unicasts	0
Multicasts	0	Broadcasts	0
Management	0	Beacons	5545
Fragments	0	RTS Count	0
CTS Count	0		
Transmit Errors			
Total	0	Dropped	0
Unassociated	0	Ack Failures	0
Rts Failures	0		
Transmit Retries			
Total	0	Multiple	0
Single	0	RTS Count	0
Date Rates			

1.0	Receive Packets	0	Receive Errors	0

more ...

Figure 62. WMI: Statistics IAP abg3 Page (Part 1)

... continued



Date Rates				
1.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
2.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
5.5	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
6.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
9.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
11.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
12.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
18.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
24.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
36.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
48.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0
54.0	Receive Packets	0	Receive Errors	0
	Receive Bytes	0	Receive Retries	0
	Transmit Packets	0	Transmit Errors	0
	Transmit Bytes	0	Transmit Retries	0

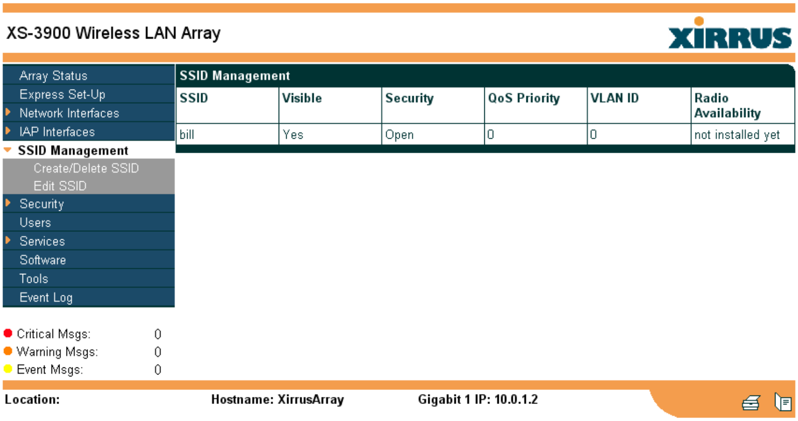
Location: Hostname: XirrusArray Gigabit 1 IP: 10.0.1.2

Figure 63. WMI: Statistics IAP abg3 Page (Part 2)

SSID Management

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

For information to help you understand SSIDs and how multiple SSIDs are managed by the XS-3900, go to the Multiple SSIDs section of "Frequently Asked Questions" on page 186.



SSID Management

SSID	Visible	Security	QoS Priority	VLAN ID	Radio Availability
bill	Yes	Open	0	0	not installed yet

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: XirrusArray Gigabit 1 IP: 10.0.1.2

Figure 64. WMI: SSID Management Page

Understanding SSIDs

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

Multiple SSIDs

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

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

Legacy access points typically support one SSID per access point. Xirrus Wireless LAN Arrays support the ability for multiple SSIDs to be defined and used simultaneously.

Using SSIDs

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

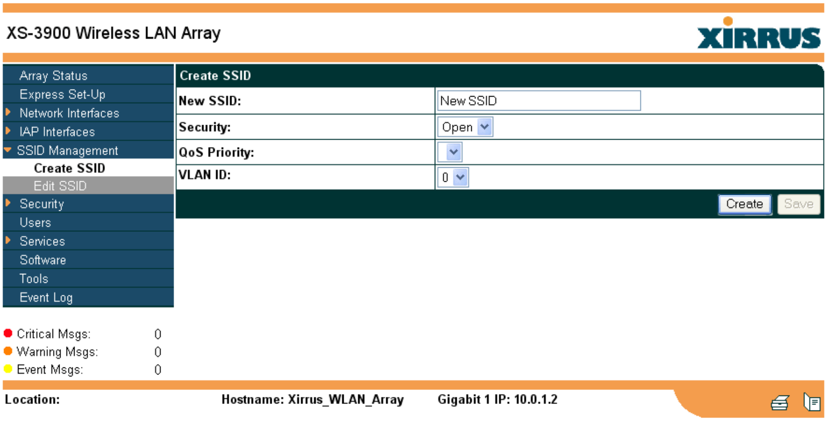
- Minimum security required to join this SSID.
- The wireless Quality of Service (QoS) desired for this SSID.
- The wired VLAN associated with this SSID.

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

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

Create SSID

This page allows you to create and manage SSIDs, and assign security parameters and VLANs on a per SSID basis. When finished, click on the **Save** button to save your changes, otherwise your changes will not take effect.



Create SSID

New SSID: New SSID
Security: Open
QoS Priority:
VLAN ID: 0

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 65. WMI: Create SSID Page

Procedure for Creating SSIDs

1. **New SSID**: Enter a new SSID definition.
2. **Security**: From the pull-down list, choose the security that will be required by users for this SSID, either Open, WEP or WPA. The Open option provides no security and is not recommended. For an overview of the security options, go to "Security Planning" on page 31.

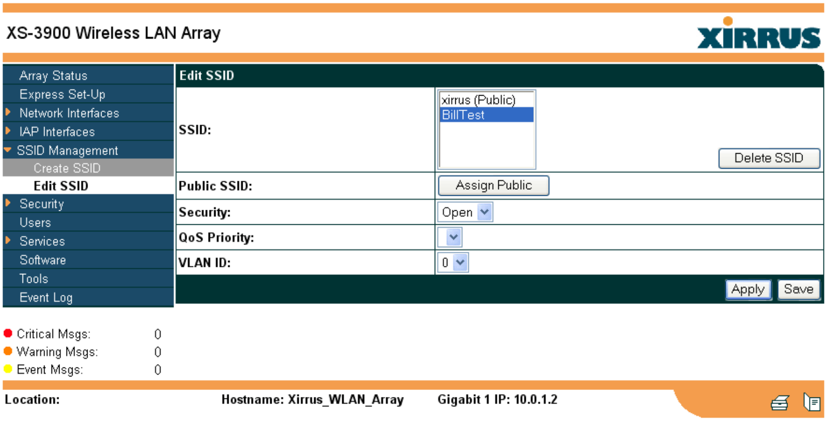
3. **Qos Priority**: From the pull-down list, select a Quality of Service (QoS) setting. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic. This step is optional.
4. **VLAN ID**: From the pull-down list, select a VLAN that you want this traffic to be forwarded to on the wired network. This step is optional.

5. Click on the **Create SSID** button to create this SSID. The SSID you just created will appear in the SSID List on the Edit SSID page.

6. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Edit SSID

This page allows you to edit existing SSIDs, and reassign security parameters and VLANs on a per SSID basis. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



SSID: xirrus (Public), BillTest

Public SSID:

Security: Open

QoS Priority:

VLAN ID: 0

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

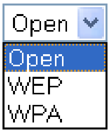
Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 66. WMI: Edit SSID Page

Procedure for Editing or Deleting SSIDs

1. **SSID**: Choose the SSID that you want to edit or delete from the list. If you are deleting a selected SSID, click on the **Delete SSID** button, otherwise go to Step 2.

2. **Public SSID**: Click on the **Assign Public** button to make the selected SSID visible to all clients on the network. Although the XS-3900 will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it. Choose **No** if you do not want this SSID to be visible on the network.



3. **Security**: From the pull-down list, choose the security that will be required by users for the selected SSID—either Open, WEP or WPA. The Open option provides no security and is not recommended. For an overview of the security options, go to "Security Planning" on page 31.

4. **QoS Priority**: From the pull-down list, select a Quality of Service (QoS) setting. The QoS setting you define here will prioritize wireless traffic for the selected SSID over other SSID wireless traffic. This step is optional.

5. **VLAN ID**: From the pull-down list, select a VLAN that you want this traffic to be forwarded to on the wired network. This step is optional.

6. Click on the **Apply** button to apply the new settings to this session.

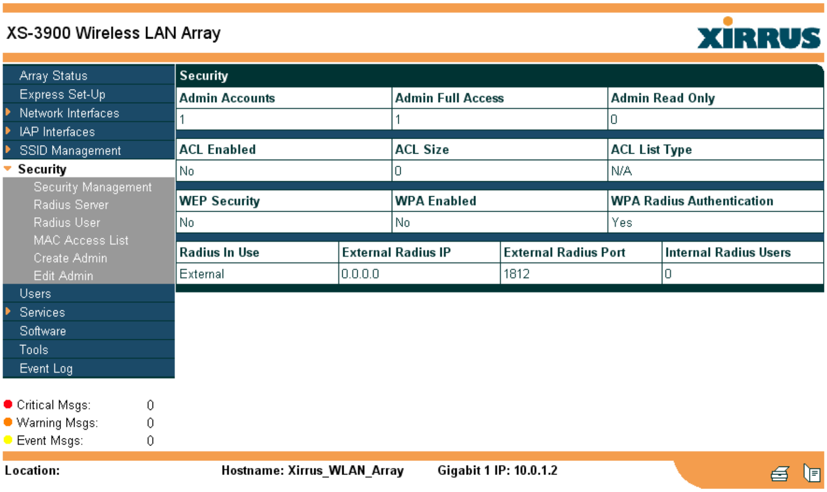
7. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Security

This is a status only page that allows you to review the array’s security parameters. It includes the assigned network administration accounts, Access Control List (ACL) values, WEP and WPA status, and RADIUS configuration settings. There are no configuration options available on this page, but if you are experiencing issues with security, you may want to print this page for your records.

For additional information about wireless network security, refer to:

- “Security Planning” on page 31.
- The Security section of “Frequently Asked Questions” on page 186.



Security

Admin Accounts	Admin Full Access	Admin Read Only
1	1	0

ACL Enabled	ACL Size	ACL List Type
No	0	N/A

WEP Security	WPA Enabled	WPA Radius Authentication
No	No	Yes

Radius In Use	External Radius IP	External Radius Port	Internal Radius Users
External	0.0.0.0	1812	0

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

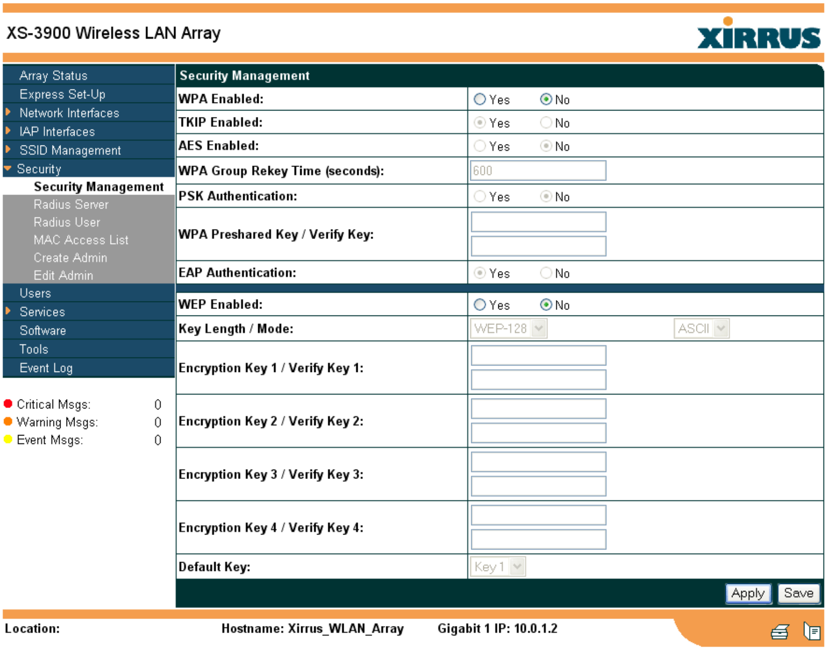
Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 67. WMI: Security Page

Security Management

This page allows you to establish the security parameters for your wireless network, including WEP, WPA and RADIUS authentication. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.

For additional information about wireless network security, refer to “Security Planning” on page 31.



Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Security Management	
WPA Enabled:	○ Yes ● No
TKIP Enabled:	● Yes ○ No
AES Enabled:	○ Yes ● No
WPA Group Rekey Time (seconds):	600
PSK Authentication:	○ Yes ● No
WPA Preshared Key / Verify Key:	
EAP Authentication:	● Yes ○ No
WEP Enabled:	○ Yes ● No
Key Length / Mode:	WEP-128 ASCII
Encryption Key 1 / Verify Key 1:	
Encryption Key 2 / Verify Key 2:	
Encryption Key 3 / Verify Key 3:	
Encryption Key 4 / Verify Key 4:	
Default Key:	Key 1

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 68. WMI: Security Management Page

Understanding Security

The Xirrus Wireless LAN Array incorporates many security features that administrators can configure. After initially installing an array, always change the default administrator password (the default is admin), and choose a strong replacement password (a strong password contains letters, numbers and special characters). When appropriate, issue read only administrator accounts.

Other security considerations include:

- **SSH versus Telnet**: Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing**: The optional Xirrus Wireless Management System (XM-3300) offers powerful management features for small or large XS-3900 deployments, and can audit your configuration settings automatically. In addition, using the XM-3300 eliminates the need for an FTP server.
- **Choosing an encryption method**: Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The XS-3900 allows you to establish the following data encryption configuration options:
    - **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTy.
    - **WEP (Wired Equivalent Privacy)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.
    - **WPA (Wi-Fi Protected Access)**—this is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

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

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

Any of the above encryption modes can be used, but only one may be used per SSID. If multiple security methods are needed, you must define multiple SSIDs.

- **Choosing an authentication method**: User authentication ensures that users are who they say they are. For this purpose, the XS-3900 allows you to choose between the following user authentication methods:
  - **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the XS-3900.

    This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing at least 12 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.
  - **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal (provided by the XS-3900) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

    The XS-3900 will accept up to 512 ACL entries.

- **MAC Address ACLs (Access Control Lists)**—MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC addresses of each user in the Allow list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the Deny list.

Procedure for Configuring Network Security

1. **WPA Enabled**: Choose **Yes** to enable WPA (Wi-Fi Protected Access), or choose **No** to disable WPA.
2. **TKIP Enabled**: Choose **Yes** to enable TKIP (Temporal Key Integrity Protocol), or choose **No** to disable TKIP.
3. **AES Enabled**: Choose **Yes** to enable AES (Advanced Encryption Standard), or choose **No** to disable AES.
4. **WPA Group Rekey Time (in seconds)**: Enter a value to specify the group rekey time (in seconds). The default is 600.
5. **PSK Authentication**: Choose **Yes** to enable PSK (Pre-Shared Key) authentication, or choose **No** to disable PSK.
6. **WPA Preshared Key / Verify Key**: If you enabled PSK, enter a passphrase here, then re-enter the passphrase to verify that you typed it correctly.
7. **EAP Authentication**: Choose **Yes** to enable EAP (Extensible Authentication Protocol) or choose **No** to disable EAP.

A RADIUS server must be defined to use EAP.

8. **WEP Enabled**: Choose **Yes** to enable WEP (Wired Equivalent Privacy) or choose **No** to disable WEP.

9. **Key Length / Mode**: If you enabled WEP, choose the desired key length (either 40 or 128) and the mode (either ASCII or Hex) from the pull-down lists. You must now provide the encryption key(s).

   a. **Encryption Key 1 / Verify Key 1**: Enter an encryption key of the length specified (either 40 or 128 characters), then re-enter the key to verify that you typed it correctly.

   b. **Encryption Key 2 / Verify Key 2** (optional): If desired, enter a second encryption key, then re-enter the key to verify that you typed it correctly.

   c. **Encryption Key 3 / Verify Key 3** (optional): If desired, enter a third encryption key, then re-enter the key to verify that you typed it correctly.

   d. **Encryption Key 4 / Verify Key 4** (optional): If desired, enter a fourth encryption key, then re-enter the key to verify that you typed it correctly.

10. **Default Key**: Choose which key you want to assign as the default key. Make your selection from the pull-down list.

11. Click on the **Apply** button to apply the new settings to this session.

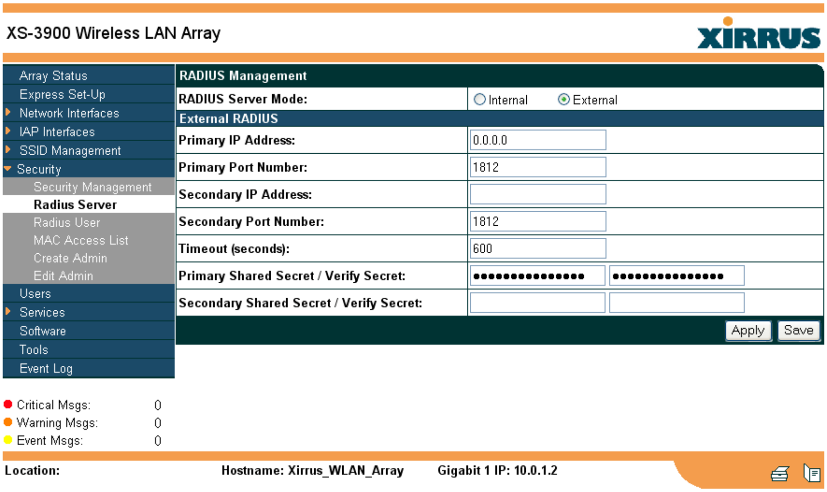
12. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Radius Server

This page allows you to set up the array's internal RADIUS server, or define the use of an external RADIUS server for user authentication.

The internal RADIUS server will only authenticate wireless clients that want to associate to the array. This can be useful if an external RADIUS server is not available.

When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



XS-3900 Wireless LAN Array

RADIUS Management

RADIUS Server Mode:	○ Internal	● External

External RADIUS

Primary IP Address:	0.0.0.0	
Primary Port Number:	1812	
Secondary IP Address:		
Secondary Port Number:	1812	
Timeout (seconds):	600	
Primary Shared Secret / Verify Secret:	●●●●●●●●●●●●●●●	●●●●●●●●●●●●●●●
Secondary Shared Secret / Verify Secret:		

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 69. WMI: Radius Server Page

Procedure for Configuring Radius Servers

1. **Radius Server Mode**: Choose **Internal** if you want to use the XS-3900's internal RADIUS server, or choose **External** to use an external RADIUS server.

2. **Primary IP Address**: If you are using an external RADIUS server, enter the primary server's IP address.

3. **Radius Primary Port Number**: If you are using an external RADIUS server, enter the primary port number.

4. **Secondary IP Address** (optional): If desired, enter the secondary RADIUS server's IP address.

   If the primary RADIUS server becomes off-line, the array will "failover" to the secondary RADIUS server (defined here).

5. **Radius Secondary Port Number**: If desired, enter the secondary port number.

6. **Radius Timeout**: Define the maximum idle time (in seconds) before the RADIUS session times out. The default is 600 seconds.

7. **Primary Shared Secret / Verify Secret**: If you are using RADIUS, enter the primary shared secret, then re-enter the primary shared secret to verify that you typed it correctly.

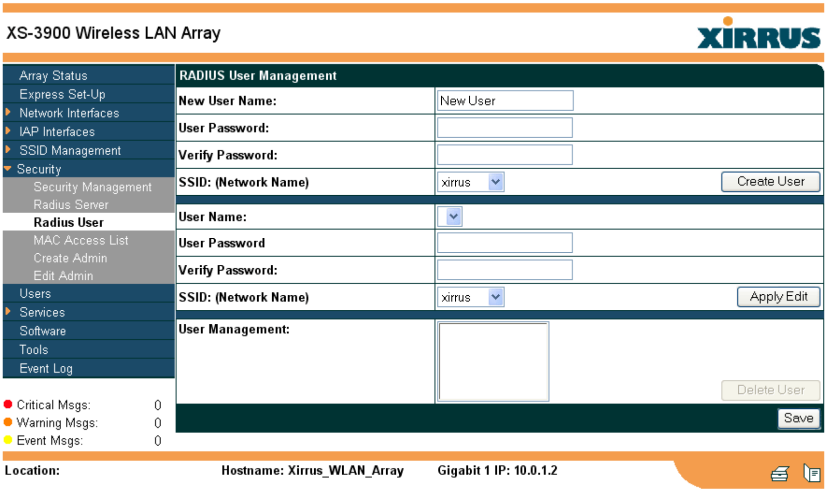
8. **Secondary Shared Secret / Verify Secret**: If you are using RADIUS, enter the secondary shared secret, then re-enter the secondary shared secret to verify that you typed it correctly.

9. Click on the **Apply** button to apply the new settings to this session.

10. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Radius User

This page allows you to create, delete and manage local RADIUS user accounts. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



XS-3900 Wireless LAN Array

RADIUS User Management

New User Name: New User

User Password:

Verify Password:

SSID: (Network Name) xirrus

User Name:

User Password

Verify Password:

SSID: (Network Name) xirrus

User Management:

Critical Msgs: 0

Warning Msgs: 0

Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 70. WMI: Radius User Page

Procedure for Configuring Radius Users

1. **New User Name**: Enter a new RADIUS user name.
2. **User Password**: Enter a password for this user.
3. **Verify Password**: Re-enter the user password to verify that you typed it correctly.
4. **SSID (Network Name)**: Choose an SSID from the pull-down list.
5. Click on the **Create User** button to add this user to the list.

6. **User Name**: If you want to edit an existing RADIUS user account, choose the user from the pull-down list. You must now enter the user password and select an SSID.

    a. **User Password**: Enter the password of the user account you want to edit.

    b. **Verify Password**: Re-enter the password to verify that you typed it correctly.

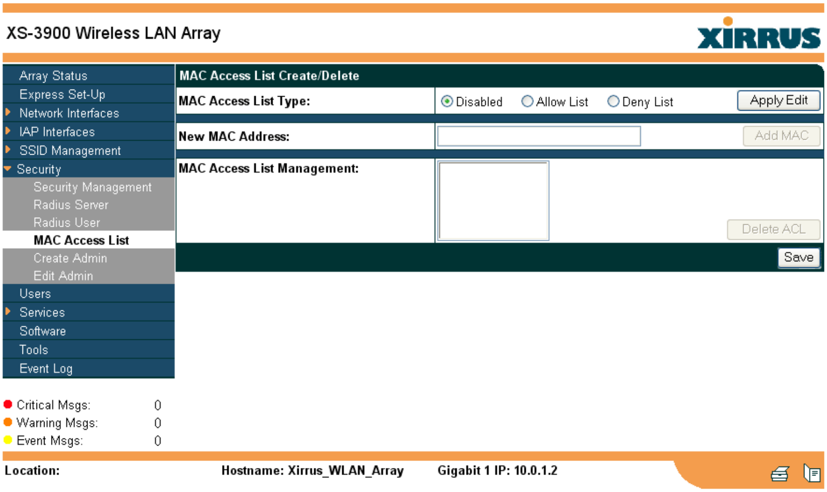
    c. **SSID (Network Name)**: Choose an SSID from the pull-down list.

7. **User Management**: You can delete users by selecting the user from the list and clicking on the **Delete User** button.

8. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

MAC Access List

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



XS-3900 Wireless LAN Array

MAC Access List Create/Delete

MAC Access List Type: ● Disabled ○ Allow List ○ Deny List

New MAC Address:

MAC Access List Management:

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 71. WMI: MAC Access List Page

Procedure for Configuring MAC Access Lists

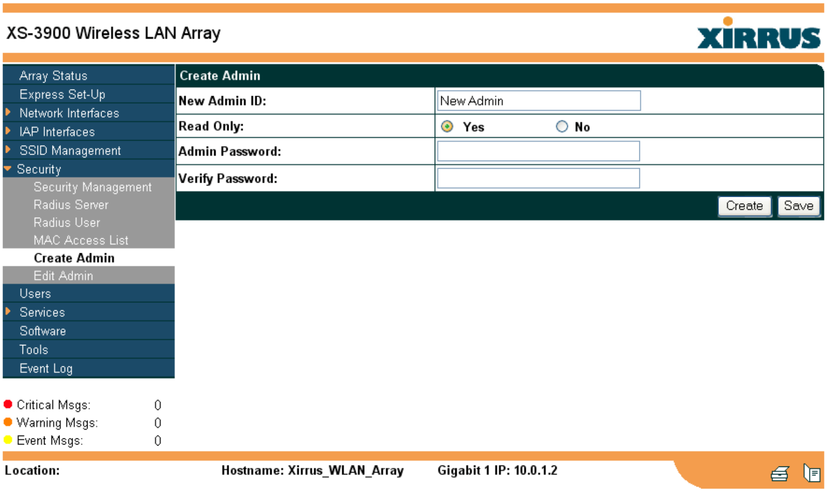
1. **MAC Access List Type**: Select the MAC Access List type—either **Disabled**, **Allow List** or **Deny List**, then click on the **Apply Edit** button to apply your changes.
    - **Allow List**: Only allows these MAC addresses to associate to the array.
    - **Deny List**: Allows all MAC addresses except the addresses defined in this list.

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

2. **New MAC Address**: If you want to add a MAC address to the ACL, enter the new MAC address here, then click on the **Add MAC** button. The MAC address is added to the ACL.
3. **MAC Access List Management**: You can delete a MAC Access List by selecting the list you want to delete then clicking on the **Delete ACL** button.
4. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Create Admin

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



Create Admin

New Admin ID:	New Admin
Read Only:	● Yes ○ No
Admin Password:	
Verify Password:	

Critical Msgs:	0
Warning Msgs:	0
Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 72. WMI: Create/Delete Admin Page

Procedure for Creating Network Administrator Accounts

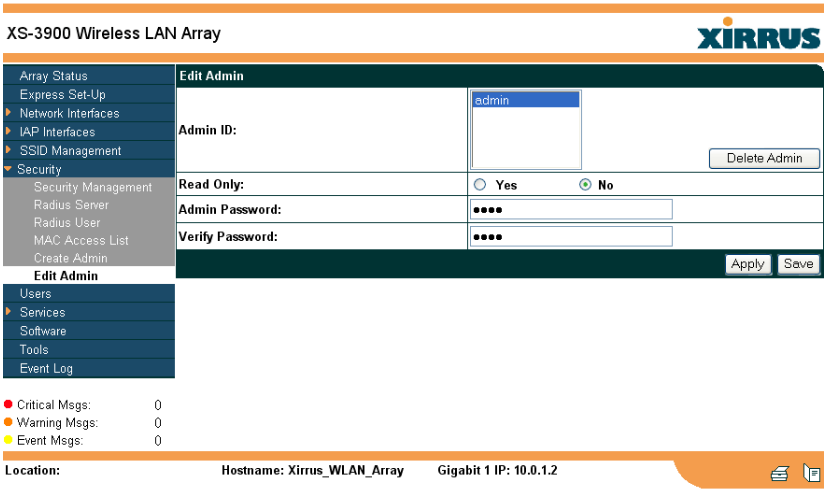
1. **New Admin ID**: Enter a meaningful description for this new network administrator ID.
2. **Read Only**: Choose **Yes** to restrict this administrator ID to read only status, or choose **No** if you want to give this administrator ID full read/write privileges. In the read only mode, administrators cannot save changes to configurations.
3. **Admin Password**: Enter a password for this ID.
4. **Verify Password**: Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).

5. Click on the **Create Admin** button to add this administrator ID to the list.

6. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Edit Admin

This page allows you to edit or delete existing administrator accounts. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



Admin ID: admin

Read Only: ○ Yes ● No

Admin Password: ••••

Verify Password: ••••

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 73. WMI: Edit Admin Page

Procedure for Modifying Network Administrator Accounts

1. **Admin ID**: Choose the administrator ID you want to edit or delete from the list. If you are deleting the selecting administrator ID, click on the **Delete Admin** button, otherwise go to Step 2.

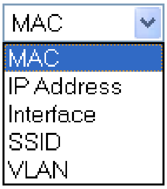
2. **Read Only**: Choose **Yes** to restrict the selected administrator ID to read only status, or choose **No** if you want to give this administrator ID full privileges.

3. **Admin Password / Verify Password**: Enter the password for the selected administrator ID in the left field, then re-enter the password in the right field (the two fields must match).

4. Click on the **Apply** button to apply the new settings to this session.

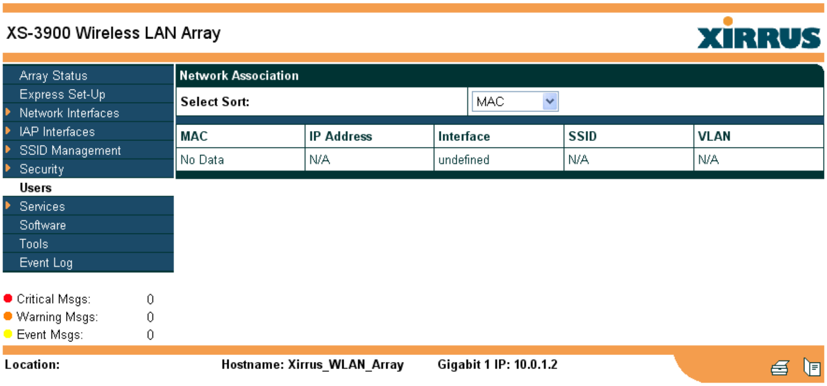
5. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Users



This is a status only page that allows you to review the users currently associated with the network. You can choose how you want to sort the information that is displayed by choosing a sort option from the pull-down list.

There are no configuration options available on this page, but if you are experiencing issues with network users, you may want to print this page for your records.



Network Association

Select Sort: MAC

MAC	IP Address	Interface	SSID	VLAN
No Data	N/A	undefined	N/A	N/A

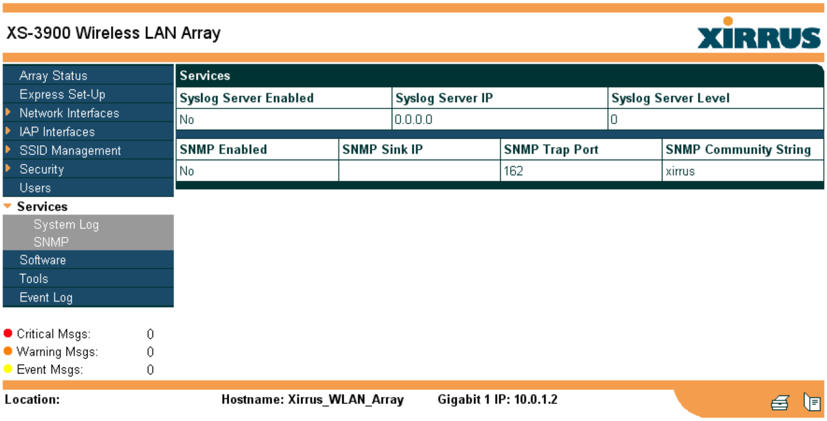
Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 74. WMI: Users Page

Services

This is a status only page that allows you to review the current status of syslog and SNMP services. There are no configuration options available on this page, but if you are experiencing issues with network services, you may want to print this page for your records.



Services

Syslog Server Enabled	Syslog Server IP	Syslog Server Level
No	0.0.0.0	0

SNMP Enabled	SNMP Sink IP	SNMP Trap Port	SNMP Community String
No		162	xirrus

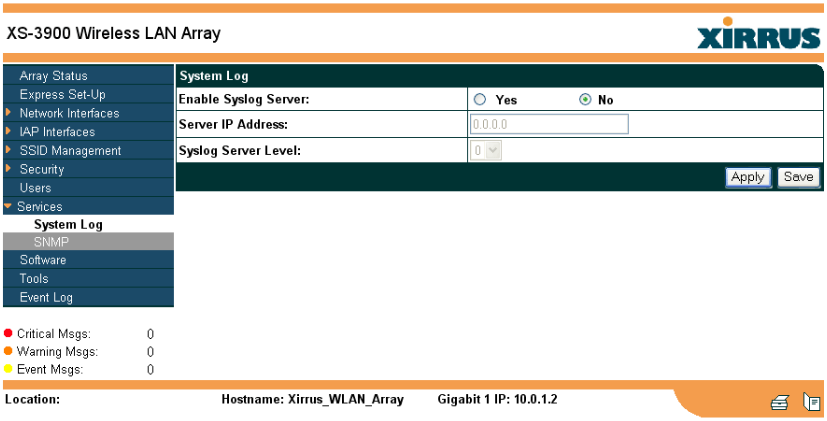
● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 75. WMI: Services Page

System Log

This page allows you to enable or disable the Syslog server, define the server's IP address, and set the level for Syslog reporting—the Syslog service will send Syslog messages to the defined Syslog server. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



System Log

Enable Syslog Server:	○ Yes ● No
Server IP Address:	0.0.0.0
Syslog Server Level:	0

Critical Msgs:	0
Warning Msgs:	0
Event Msgs:	0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

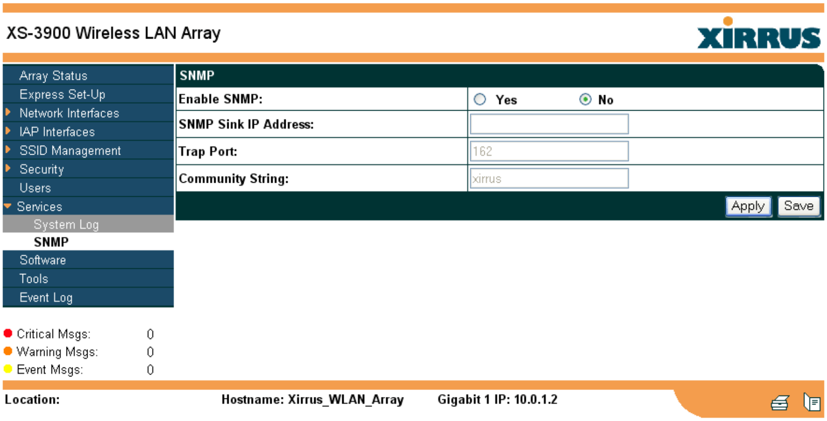
Figure 76. WMI: System Log Page

Procedure for Configuring Syslog

1. **Enable Syslog Server**: Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.
2. **Server IP Address**: If you enabled Syslog, enter the IP address of the Syslog server.
3. **Syslog Server Level**: Choose the level of Syslog reporting from the pull-down list (between 0 and 7).
4. Click on the **Apply** button to apply the new settings to this session.
5. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

SNMP

This page allows you to enable or disable SNMP and define the SNMP parameters. SNMP allows remote management of the array by the Xirrus Management System (XM-3300), or other SNMP-based management system. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.



XS-3900 Wireless LAN Array

SNMP

Enable SNMP:	○ Yes ● No
SNMP Sink IP Address:	
Trap Port:	162
Community String:	xirrus

Critical Msgs: 0
Warning Msgs: 0
Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 77. WMI: SNMP Page

Procedure for Configuring SNMP

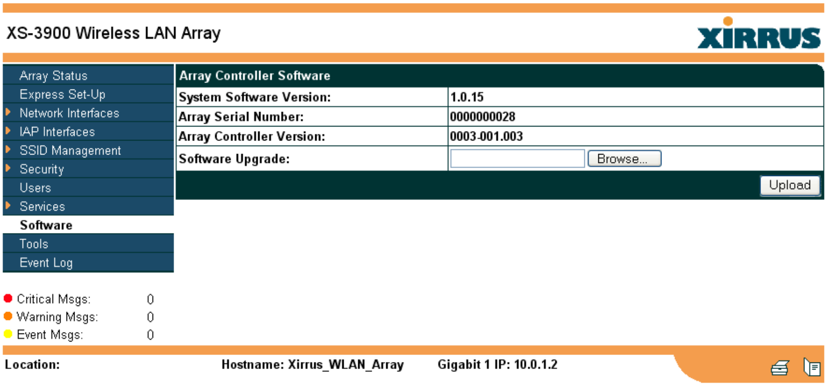
1. **Enable SNMP**: Choose **Yes** to enable SNMP functionality, or choose **No** to disable this feature.
2. **SNMP Link IP Address**: Enter the IP address of the SNMP link.
3. **Trap Port**: Enter the trap port.
4. **Community String**: Enter the community string.
5. Click on the **Apply** button to apply the new settings to this session.
6. Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

Software

This page displays the current system software version, the array's serial number, and the array's controller version. It also allows you to upgrade the system software.

Procedure for Upgrading the System Firmware

1. Download the software upgrade file to your local PC.
2. From the WMI, go to the **Software** page. This page allows you to upgrade the system firmware.



Array Controller Software

System Software Version:	1.0.15
Array Serial Number:	0000000028
Array Controller Version:	0003-001.003
Software Upgrade:	

● Critical Msgs:	0
● Warning Msgs:	0
● Event Msgs:	0

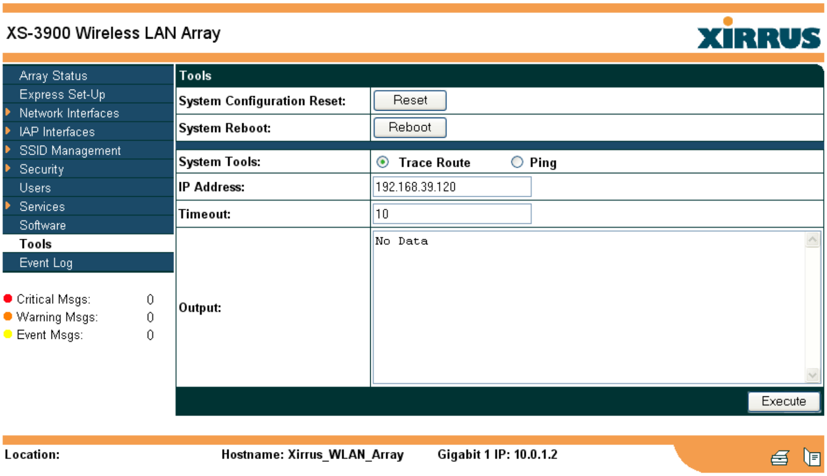
Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 78. WMI: Software Page

3. **Software Upgrade**: Enter the name of the upgrade file, then click on the **Browse** button to locate the file.
4. Click on the **Upload** button to upgrade the system software.
5. Reboot the array for the new software to take effect—*the array must be rebooted for the new software to become active.*

Tools

This page allows you to reset the system's configuration parameters to their factory default values, reboot the system, and ping other IP addresses for diagnostic purposes.



System Configuration Reset: Reset

System Reboot: Reboot

System Tools: ● Trace Route ○ Ping

IP Address: 192.168.39.120

Timeout: 10

Output:

```
No Data
```

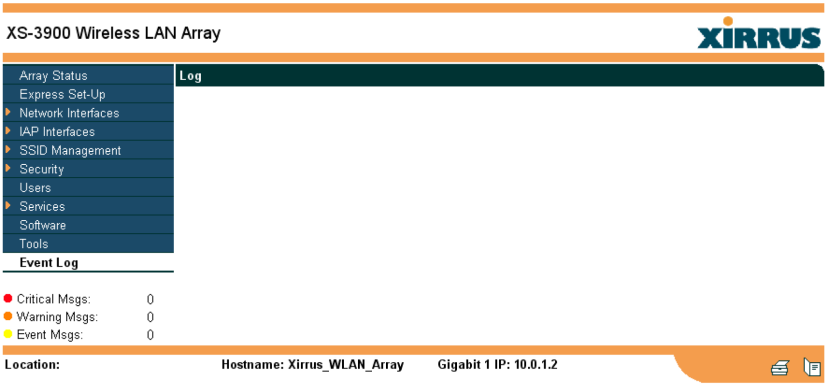
Figure 79. WMI: Tools Page

Procedure for Configuring System Tools

1. **System Configuration Reset**: Click on the **Reset** button to reset the system's current configuration settings to the factory default values—*all previous configuration settings will be lost*.
2. **System Reboot**: Click on the **Reboot** button to reboot the system—*you must reboot the array.*
3. **System Tools**: Choose **Trace Route** or **Ping**.
4. **IP Address**: Enter the IP address of the target device.
5. **Timeout**: Enter a value (in seconds) before the action times out.
6. Click on the **Execute** button to perform the test. Results are displayed in the Output frame.

Event Log

This is a status only page that allows you to review the event log. System alerts and messages are displayed on this page. There are no configuration options available on this page, but if you are experiencing issues with the network, you may want to print this page for your records.



● Critical Msgs: 0
● Warning Msgs: 0
● Event Msgs: 0

Location: Hostname: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 80. WMI: Event Log Page

The Command Line Interface

This chapter covers configuration and management tasks using the product's Command Line Interface (CLI), and includes a procedure for establishing a Telnet connection to the XS-3900. Section headings for this chapter include:

- Establishing a Secure Shell (SSH) Connection
- Basic Commands
- Command Modes
- Selecting Interfaces
- Command Line Keywords
- Interface Selection

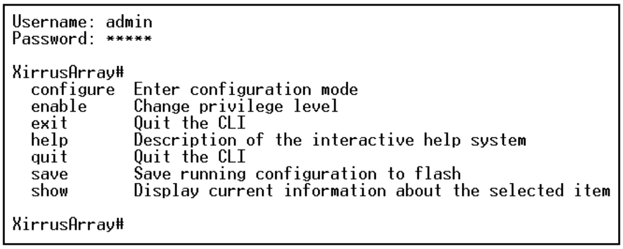
Establishing a Secure Shell (SSH) Connection

Use this procedure to initialize the system and log in to the Command Line Interface (CLI) via a Secure Shell (SSH) utility, such as PuTTY.

1. Start your SSH session and communicate with the XS-3900 via its default IP address (10.0.1.1).

   When connected to the XS-3900, a login prompt appears on your screen. The default login user name and password is **admin** (for both). Login names and passwords are case-sensitive.

2. Enter **admin** when prompted for a user name and password. You are now logged in to the XS-3900's Command Line Interface.



```
Username: admin
Password: *****

XirrusArray#
  configure  Enter configuration mode
  enable     Change privilege level
  exit       Quit the CLI
  help       Description of the interactive help system
  quit       Quit the CLI
  save       Save running configuration to flash
  show       Display current information about the selected item

XirrusArray#
```

Figure 81. Command Line Interface

Basic Commands

Help

To get help at any point type **help** or **?**.

Tab Key

The Tab Key allows auto-completion of commands such that only a few unique characters need to be entered followed by the Tab Key, which will automatically fill in the rest of the command.

? Key

The **?** key displays the list of available commands at any point of typing in the command line.

Save

You must type **save** to save the current configuration to flash memory so that changes are kept when the array is rebooted.

Command Modes

Configure Mode

Allows major functional changes to interfaces and configuration.

Requires Read/Write Administrator Privilege

```
Xirrus-Array# configure
Xirrus-Array(config)#
```

The prompt will change to show the current mode in parentheses.

SSID Mode

Allows configuration changes to SSID definitions.

Requires Read/Write Administrator Privilege

From configure mode type **ssid** <ENTER>

```
Xirrus-Array(config)# ssid
Xirrus-Array(config-SSID)#
```

Radius Mode

Allows configuration changes to the internal RADIUS server.

Requires Read/Write Administrator Privilege

From configure mode type **radius** <ENTER>

```
Xirrus-Array(config)# radius
Xirrus-Array(config-radsrv)#
```

Run Test Mode

Allows configuration and execution of tests

Requires Read/Write Administrator Privilege

From configure mode type **run-tests** <ENTER>

```
Xirrus-Array(config)# run-tests
Xirrus-Array(Run Test)#
```

Selecting Interfaces

From the configure mode select the desired interface.

interface {console | iap | gig1 | gig2 | eth0};

console	asyncronous serial console port
iap	integrated access point interface
gig1	gigabit Ethernet interface
gig2	gigabit Ethernet interface
eth0	10/100 Ethernet interface

Example:

```
Xirrus-Array(config)# interface iap
Xirrus-Array(config-iap)#
```

Command Line Keywords

This section provides a brief description of available keywords, including any user-defined parameters associated with the keyword. An example of the keyword's usage is also provided. Keywords are grouped by function. If you need to find a specific keyword, go to "Alphabetical Listing of CLI Keywords" on page 173 and click on the keyword—you will be taken to the keyword definition within this section. Functional groups in this section include:

- Interface Selection
- Interface Configuration
- Radio Configuration
- Beacon Information
- System Administration
- System Testing
- Security
- Station Timeouts
- SSID Configuration
- DNS Configuration
- NTP Configuration
- DHCP Configuration
- Syslog Configuration
- SNMP Configuration
- Filters
- Radius Configuration
- Reports
- Data Handling
- Data Clearance
- Show Information
- Remove Configuration
- Help

Interface Selection

The following keywords are used when choosing an interface.

dot11a

Description: Select 802.11a WLAN interface
Usage: interface { dot11a }
Parameters: none

dot11g

Description: Select 802.11g WLAN interface
Usage: interface { dot11g }
Parameters: none

faste

Description: Select 10/100 Fast Ethernet interface
Usage: interface { faste }
Parameters: none

gigabit

Description: Select 10/100/1000 Gigabit Ethernet interface
Usage: interface { gigabit }
Parameters: none

interface

Description: Select the interface you want to configure
Usage: interface { line | dot11a | dot11g | gigabit | faste }
Parameters: none

line

Description: Select the asynchronous serial port
Usage: interface { line }
Parameters: none

Interface Configuration

The following keywords are used for configuring the selected interface (assumes the interface has already been selected).

autoduplex

Description: Select the duplex mode automatically

Usage: <genum> | <fenum> { autoduplex }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be zero)

baud

Description: Set the asynchronous port baud rate

Usage: <linenum> { baud <brate> }

Parameters: <linenum> defines which asynchronous interface is used
<brate> defines the range for the baud rate, between 2,400 and 19,200 bps

bytesize

Description: Define the asynchronous port word size

Usage: <linenum> { bytesize <bsz> }

Parameters: <linenum> defines which asynchronous interface is used
<bsz> defines the byte/word size, either 7 or 8, where:
7 = 7 bits, 8 = 8 bits

def

Description: Reset the interface to the default values

Usage: <genum> | <fenum> { def }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be zero)
<mtusz> defines the maximum allowable Maximum Transmission Unit (MTU) , between 64 and 1794

dhcpbind

Description: Obtain a DHCP address for this interface

Usage: <genum> | <fenum> { dhcpbind <dbind> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:

1 = Primary, 2 = Secondary

<fenum> defines the Fast Ethernet interface (must be zero)

<dbind> defines how the IP address is generated, either 0 or 1, where:

0 = Use static IP address, 1 = Use DHCP to get IP address

down

Description: Shut down this interface

Usage: <genum> | <fenum> { down }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:

1 = Primary, 2 = Secondary

<fenum> defines the Fast Ethernet interface (must be zero)

fullduplex

Description: Select the full duplex mode

Usage: <genum> | <fenum> { fullduplex }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:

1 = Primary, 2 = Secondary

<fenum> defines the Fast Ethernet interface (must be zero)

gateway

Description: Define a gateway IP address

Usage: <genum> | <fenum> { gateway <gway> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:

1 = Primary, 2 = Secondary

<fenum> defines the Fast Ethernet interface (must be zero)

<gway> defines a valid gateway IP address

halfduplex

Description: Select the half duplex mode

Usage: <genum> | <fenum> { halfduplex }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be 0)

ip-addr

Description: Define a static IP address

Usage: <genum> | <fenum> { ip-addr <statip> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be zero)
<statip> defines a valid static IP address

management

Description: Allow management on this interface

Usage: <genum> | <fenum> { management <mgmt> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be zero)
<mgmt> selects management or no management, where:
0 = No, 1 = Yes

mask

Description: Define the subnet mask IP address

Usage: <genum> | <fenum> { mask <ipmask> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be zero)
<ipmask> defines a valid subnet mask IP address

mtu

Description: Set the maximum allowable MTU size

Usage: <genum> | <fenum> { mtu <mtusz> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary

<fenum> defines the Fast Ethernet interface (must be zero)

<mtusz> defines the maximum allowable MTU size, between 64 and 1794

parity

Description: Establish the asynchronous port's parity

Usage: <linenum> { parity <prty> }

Parameters: <linenum> defines which asynchronous interface is used

<prty> defines the parity, either 0, 1 or 2, where:
0 = No parity, 1 = Odd parity, 2 = Even parity

speed

Description: Set the Ethernet interface speed

Usage: <genum> | <fenum> { speed <spdsel> }

Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary

<fenum> defines the Fast Ethernet interface (must be zero)

<spdsel> defines the link speed, either 0 or 1, where:
0 = 100 Mbps, 1 = 1000 Mbps

stopbits

Description: Set the asynchronous port's number of stop bits

Usage: <linenum> { stopbits <sbit> }

Parameters: <linenum> defines which asynchronous interface is used

<sbit> defines the number of stop bits, either 0, 1 or 2

up

Description: Bring up this interface
Usage: <genum> | <fenum> { up }
Parameters: <genum> defines the Gigabit interface, either 1 or 2, where:
1 = Primary, 2 = Secondary
<fenum> defines the Fast Ethernet interface (must be zero)

Radio Configuration

The following keywords are used when configuring the XS-3900's radios (assumes the interface has already been selected).

antenna

Description: Set the direction for this radio antenna
Usage: <rnum> { antenna }
Parameters: <rnum> defines the radio number, between 1 and 16

antennaexternal

Description: Show the external antenna settings
Usage: <rnum> { antennaexternal }
Parameters: <rnum> defines the radio number, between 1 and 16

basic1

Description: Require 1 Mbps rate
Usage: <rnum> { basic1 }
Parameters: <rnum> defines the radio number, between 13 and 16

basic11

Description: Require 11 Mbps rate
Usage: <rnum> { basic11 }
Parameters: <rnum> defines the radio number, between 13 and 16

basic12

Description: Require 12 Mbps rate
Usage: <rnum> { basic12 }
Parameters: <rnum> defines the radio number, between 1 and 16

basic18

Description: Require 18 Mbps rate
Usage: <rnum> { basic18 }
Parameters: <rnum> defines the radio number, between 1 and 16

basic2

Description: Require 2 Mbps rate
Usage: <rnum> { basic2 }
Parameters: <rnum> defines the radio number, between 13 and 16

basic24

Description: Require 24 Mbps rate
Usage: <rnum> { basic24 }
Parameters: <rnum> defines the radio number, between 1 and 16

basic36

Description: Require 36 Mbps rate
Usage: <rnum> { basic36 }
Parameters: <rnum> defines the radio number, between 1 and 16

basic48

Description: Require 48 Mbps rate
Usage: <rnum> { basic48 }
Parameters: <rnum> defines the radio number, between 1 and 16

basic5

Description: Require 5 Mbps rate
Usage: <rnum> { basic5 }
Parameters: <rnum> defines the radio number, between 13 and 16

basic54

Description: Require 54 Mbps rate
Usage: <rnum> { basic54 }
Parameters: <rnum> defines the radio number, between 1 and 16

basic6

Description: Require 6 Mbps rate

Usage: <rnum> { basic6 }

Parameters: <rnum> defines the radio number, between 1 and 16

basic9

Description: Require 9 Mbps rate

Usage: <rnum> { basic9 }

Parameters: <rnum> defines the radio number, between 1 and 16

cca

Description: Employ Clear Channel Assessment function

Usage: <rnum> { cca <ccadb> }

Parameters: <rnum> defines the radio number, between 1 and 16

<ccadb> is a number between 0 and 60 to define the floor noise level in dB increments

cell-size

Description: Define cell size

Usage: <rnum> { cell-size <cszset> }

Parameters: <rnum> defines the radio number, between 1 and 16

<cszset> is defined as either 0, 1 or 2, where:

0 = smallest, 1 = medium, 2 = largest

channelnum

Description: Define static channel setting

Usage: <rnum> { channelnum <cnum> }

Parameters: <rnum> defines the radio number, between 1 and 16

<cnum> defines the static channel number

configure

Description: Configure each radio individually

Usage: <rnum> { configure }

Parameters: <rnum> defines the radio number, between 1 and 16

default_rates

Description: Set default rates

Usage: <rnum> { default_rates }

Parameters: <rnum> defines the radio number, between 1 and 16

description

Description: Specify a name to identify this interface

Usage: <rnum> { description <dot11desc> }

Parameters: <rnum> defines the radio number, between 1 and 16

<dot11desc> is defined as a string of up to 50 alphanumeric characters

dot11gonly

Description: Enable support for 802.11g only

Usage: <rnum> { dot11gonly }

Parameters: <rnum> defines the radio number, between 1 and 16

dot11preamble

Description: Define the preamble

Usage: <rnum> { dot11preamble }

Parameters: <rnum> defines the radio number, between 1 and 16

down

Description: Shut down (disable) this radio interface

Usage: <rnum> { down }

Parameters: <rnum> defines the radio number, between 1 and 16

edcf

Description: Enable EDCF support

Usage: <rnum> { edcf }

Parameters: <rnum> defines the radio number, between 1 and 16

enable1

Description: Allow 1 Mbps rate

Usage: <rnum> { enable1 }

Parameters: <rnum> defines the radio number, between 13 and 16

enable11

Description: Allow 11 Mbps rate
Usage: <rnum> { enable11 }
Parameters: <rnum> defines the radio number, between 13 and 16

enable12

Description: Allow 12 Mbps rate
Usage: <rnum> { enable12 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable18

Description: Allow 18 Mbps rate
Usage: <rnum> { enable18 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable2

Description: Allow 2 Mbps rate
Usage: <rnum> { enable2 }
Parameters: <rnum> defines the radio number, between 13 and 16

enable24

Description: Allow 24 Mbps rate
Usage: <rnum> { enable24 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable36

Description: Allow 36 Mbps rate
Usage: <rnum> { enable36 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable48

Description: Allow 48 Mbps rate
Usage: <rnum> { enable48 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable5

Description: Allow 5 Mbps rate
Usage: <rnum> { enable5 }
Parameters: <rnum> defines the radio number, between 13 and 16

enable54

Description: Allow 54 Mbps rate
Usage: <rnum> { enable54 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable6

Description: Allow 6 Mbps rate
Usage: <rnum> { enable6 }
Parameters: <rnum> defines the radio number, between 1 and 16

enable9

Description: Allow 9 Mbps rate
Usage: <rnum> { enable9 }
Parameters: <rnum> defines the radio number, between 1 and 16

frag-threshold

Description: Define the fragmentation threshold
Usage: <rnum> { frag-threshold <fragt> }
Parameters: <rnum> defines the radio number, between 1 and 16
<fragt> defines the fragment size

least_congested

Description: Scan for the best frequency
Usage: <rnum> { least_congested }
Parameters: <rnum> defines the radio number, between 1 and 16

long-retry-limit

Description: Specify the long retry limit
Usage: <rnum> { long-retry-limit <lrl> }
Parameters: <rnum> defines the radio number, between 1 and 16
<lrl> defines the long retry limit

max-client-txpwr

Description: Limit the client's maximum transmit power
Usage: <rnum> { max-client-txpwr <mcp> }
Parameters: <rnum> defines the radio number, between 1 and 16
<mcp> specifies a number (in milliwatts)

off

Description: Turn OFF this feature
Usage: <rnum> { off }
Parameters: <rnum> defines the radio number, between 1 and 16

on

Description: Turn ON this feature
Usage: <rnum> { on }
Parameters: <rnum> defines the radio number, between 1 and 16

prelong

Description: Enable long preamble for the selected radio
Usage: <rnum> { prelong }
Parameters: <rnum> defines the radio number, between 1 and 16

preshort

Description: Enable short preamble for the selected radio
Usage: <rnum> { preshort }
Parameters: <rnum> defines the radio number, between 1 and 16

range

Description: Set rates for best range
Usage: <rnum> { range }
Parameters: <rnum> defines the radio number, between 1 and 16

rate1

Description: Configure the 1 Mbps rate
Usage: <rnum> { rate1 }
Parameters: <rnum> defines the radio number, between 13 and 16

rate11

Description: Configure the 11 Mbps rate
Usage: <rnum> { rate11 }
Parameters: <rnum> defines the radio number, between 13 and 16

rate12

Description: Configure the 12 Mbps rate
Usage: <rnum> { rate12 }
Parameters: <rnum> defines the radio number, between 1 and 16

rate18

Description: Configure the 18 Mbps rate
Usage: <rnum> { rate18 }
Parameters: <rnum> defines the radio number, between 1 and 16

rate2

Description: Configure the 2 Mbps rate
Usage: <rnum> { rate2 }
Parameters: <rnum> defines the radio number, between 13 and 16

rate24

Description: Configure the 24 Mbps rate
Usage: <rnum> { rate24 }
Parameters: <rnum> defines the radio number, between 1 and 16

rate36

Description: Configure the 36 Mbps rate
Usage: <rnum> { rate36 }
Parameters: <rnum> defines the radio number, between 1 and 16

rate48

Description: Configure the 48 Mbps rate
Usage: <rnum> { rate48 }
Parameters: <rnum> defines the radio number, between 1 and 16

rate5

Description: Configure the 5 Mbps rate

Usage: <rnum> { rate5 }

Parameters: <rnum> defines the radio number, between 13 and 16

rate54

Description: Configure the 54 Mbps rate

Usage: <rnum> { rate54 }

Parameters: <rnum> defines the radio number, between 1 and 16

rate6

Description: Configure the 6 Mbps rate

Usage: <rnum> { rate6 }

Parameters: <rnum> defines the radio number, between 1 and 16

rate9

Description: Configure the 9 Mbps rate

Usage: <rnum> { rate9 }

Parameters: <rnum> defines the radio number, between 1 and 16

receiving

Description: Configure the input antenna

Usage: <rnum> { receiving }

Parameters: <rnum> defines the radio number, between 1 and 16

rts-threshold

Description: Define the RTS threshold

Usage: <rnum> { rts-threshold <rtst> }

Parameters: <rnum> defines the radio number, between 1 and 16

<rtst> defines the packet size at which the device issues a Request to Send (RTS) before sending the packet

Rxdiversity

Description: Choose the antenna with the best signal

Usage: <rnum> { Rxdiversity }

Parameters: <rnum> defines the radio number, between 1 and 16

Rxleft

Description: Specify the left antenna
Usage: <rnum> { Rxleft }
Parameters: <rnum> defines the radio number, between 1 and 16

Rxright

Description: Specify the right antenna
Usage: <rnum> { Rxright }
Parameters: <rnum> defines the radio number, between 1 and 16

short-retry-limit

Description: Define t short retry limit
Usage: <rnum> { short-retry-limit <srl> }
Parameters: <rnum> defines the radio number, between 1 and 16
<srl> defines the short retry limit

speed

Description: Set allowed radio bit rates
Usage: <rnum> { speed }
Parameters: <rnum> defines the radio number, between 1 and 16

throughput

Description: Set rates for best throughput
Usage: <rnum> { throughput }
Parameters: <rnum> defines the radio number, between 1 and 16

transmiting

Description: Configure the output antenna
Usage: <rnum> { transmiting }
Parameters: <rnum> defines the radio number, between 1 and 16

Txdiversity

Description: Choose the antenna with the best signal
Usage: <rnum> { Txdiversity }
Parameters: <rnum> defines the radio number, between 1 and 16

Txleft

Description: Specify the left antenna
Usage: <rnum> { Txleft }
Parameters: <rnum> defines the radio number, between 1 and 16

tx-pwr

Description: Define the transmit power settings
Usage: <rnum> { tx-pwr <pwrset> }
Parameters: <rnum> defines the radio number, between 1 and 16
<pwrset> is defined as either 0, 1 or 2, where:
0 = quarter, 1 = half, 2 = maximum

Txright

Description: Specify the right antenna
Usage: <rnum> { Txright }
Parameters: <rnum> defines the radio number, between 1 and 16

up

Description: Bring up (enable) this radio interface
Usage: <rnum> { up }
Parameters: <rnum> defines the radio number, between 1 and 16

worldbeacon

Description: Enable support for world mode beacons
Usage: <rnum> { worldbeacon }
Parameters: <rnum> defines the radio number, between 1 and 16

Beacon Information

The following keywords are used when establishing beacon information.

beacon

Description: Establish beacon information
Usage: beacon { period | DTIM-rate }
Parameters: none

DTIM-rate

Description: Determine beacon periods before the Delivery Traffic Indication Message (DTIM) is sent

Usage: beacon { DTIM-rate <beaconr> }

Parameters: <beaconr> defines the period between DTIM frames, in Kusecs (kilo microseconds), where 1 Kusec = 1024 microseconds

period

Description: Establish the amount of time between beacons

Usage: beacon { period <beaconp> }

Parameters: <beaconp> defines the period between beacons, in Kusecs (kilo microseconds), where 1 Kusec = 1024 microseconds

System Administration

The following keywords are used for system administration tasks.

administrator

Description: Define the administrator access parameters

Usage: administrator { defpw | userid <uid> }

Parameters: <uid> enter a unique user ID

clock-set

Description: Set the date/time within the XS-3900

Usage: clock-set <curdate>

Parameters: <curdate> defines the current date and time, specified in the following format: MMDDhhmmYYYY

contact-info

Description: Define the contact information for assistance on this XS-3900

Usage: contact-info { name <conname> | email <emailcontact> | telephone <contele> }

Parameters: <conname> defines the contact name, up to 50 characters

<emailcontact> defines the email address of the contact, up to 50 characters

<contele> defines the telephone number of the contact

copy

Description: Copy a file to another file
Usage: copy <fromfile> <tofile>
Parameters: <fromfile> specifies the originating file
<tofile> specifies the destination file

default-gateway

Description: Define the default gateway IP address
Usage: ip { default-gateway <defgtwy> }
Parameters: <defgtwy> specifies the default gateway IP address

defpw

Description: Define the default password, up to 50 characters
Usage: administrator { defpw }
Parameters: none

dhcp-server

Description: Define the DHCP server IP address
Usage: ip { dhcp-server <dhcpservr> }
Parameters: <dhcpservr> specifies the DHCP server IP address

dir

Description: List the directory contents
Usage: dir
Parameters: none

domain-name

Description: Define the domain site name
Usage: ip { domain-name <domainnm>}
Parameters: <domainnm> specifies the domain name for unqualified hosts

email

Description: Define an email address for assistance on this XS-3900

Usage: contact-info { email <emailcontact> }

Parameters: <emailcontact> defines the email address of the contact, up to 50 characters

erase

Description: Delete a file from the flash file system

Usage: erase <erasefile>

Parameters: <erasefile> specifies the target file to erase

ftp

Description: Open an FTP connection with a remote server

Usage: ftp <addr>

Parameters: <addr> specifies the host name or IP address of the FTP server

hostname

Description: Define a hostname for this XS-3900

Usage: hostname <hname>

Parameters: <hname> defines the host name given to this XS-3900

ip

Description: Define the IP command set

Usage: ip { default-gateway <defgtwy> | dhcp-server <dhcpservr> | name-server <nameservr> | domain-name <domainnm>}

Parameters: <defgtwy> specifies the default gateway IP address

<dhcpservr> specifies the DHCP server IP address

<nameservr> specifies the DNS host name

<domainnm> specifies the domain name for unqualified hosts

location

Description: Define the location for this XS-3900

Usage: location <locname>

Parameters: <locname> defines the location assigned to this XS-3900

logout

Description:	Log out the current administrator
Usage:	logout
Parameters:	none

model

Description:	Get model number
Usage:	show-version { model }
Parameters:	none

more

Description:	Get more (list file)
Usage:	more <morefile>
Parameters:	<morefile> specifies the target file to list

name

Description:	Define a contact name for assistance on this XS-3900
Usage:	contact-info { name <conname> }
Parameters:	<conname> defines the contact name, up to 50 characters

name-server

Description:	Define the DNS host name
Usage:	ip { name-server <nameservr> }
Parameters:	<nameservr> specifies the DNS host name

radios

Description:	Get radio board version numbers
Usage:	show-version { radios }
Parameters:	none

reboot

Description:	Reboot the XS-3900
Usage:	reboot
Parameters:	none

reload

Description: Reload and reset the XS-3900

Usage: reload

Parameters: none

reset

Description: Reset the XS-3900 to its factory defaults

Usage: reset

Parameters: none

serial

Description: Get serial number

Usage: show-version { serial }

Parameters: none

show-version

Description: Get system version information

Usage: show-version { model | serial | software | radios }

Parameters: none

shut-down

Description: Shut down the entire system

Usage: shut-down

Parameters: none

software

Description: Get software version

Usage: show-version { software }

Parameters: none

userid

Description: Define individual user IDs

Usage: administrator { userid <uid> }

Parameters: <uid> enter a unique user ID

System Testing

The following keywords are used for system testing.

led

Description: Run LED tests

Usage: run-tests { led <ledtst> }

Parameters: <ledtst> specifies the LED to test (defined by LED number, 0 to 9—refer to "Now that the XS-3900 is physically installed, you must run the Express Setup procedure from the unit's Web Management Interface to enable the radios and establish initial system configuration settings. Go to "Powering Up the XS-3900" on page 44." on page 43)

linktest

Description: Run link tests

Usage: run-tests { linktest <ltest> }

Parameters: <linktest> specifies the link test, 1 through 4, where:

1 = tbd, 2 = tbd, 3 = tbd, 4 = tbd

ping

Description: Execute the ping utility

Usage: run-tests { ping <pingname> }

Parameters: <pingname> specifies target IP address or DNS name to ping

run-tests

Description: Run a selected test

Usage: run-tests { traceroute <tracename> | ping <pingname> | led <ledtst> | linktest <ltest> }

Parameters: <tracename> specifies target IP address or DNS name to trace

<pingname> specifies target IP address or DNS name to ping

<ledtst> specifies the LED to test (defined by LED number, 0 to 9—refer to "Now that the XS-3900 is physically installed, you must run the Express Setup procedure from the unit's Web Management Interface to enable the radios and establish initial system configuration settings. Go to "Powering Up the XS-3900" on page 44." on page 43)

<linktest> specifies the link test, 1 through 4, where:

1 = tbd, 2 = tbd, 3 = tbd, 4 = tbd

traceroute

Description: Run a trace on an IP route or DNS name

Usage: run-tests { traceroute <tracename> }

Parameters: <tracename> specifies target IP address or DNS name to trace

Security

The following keywords are used for system security.

all11a

Description: Specify that any settings will apply to all 802.11a radios

Usage: security { radioid { all11a }}

Parameters: none

all11g

Description: Specify that any settings will apply to all 802.11g radios

Usage: security { radioid { all11g }}

Parameters: none

allradios

Description: Specify that any settings will apply to all radios

Usage: security { radioid { allradios }}

Parameters: none

broadcastkey

Description: Use the encryption key during broadcast

Usage: security { radioid { all11g { broadcastkey }}}

Parameters: none

capabilitychange

Description: Issue a new key if the previous non-key STA disassociates, or the first non-key STA associates (optional)

Usage: security { radioid { all11g { capabilitychange }}}

Parameters: none

change

Description: Specify the time between key rotations (optional)

Usage: security { radioid { all11g { change <chgsecs> }}}

Parameters: <chgsecs> sets the time (in seconds) between key rotations

ciphers

Description: Enable a cipher suite for encryption

Usage: security { radioid { allradios { encryption { ciphers { tkip { tkipwep40 }}}}}}

Parameters: none

client-timeout

Description: Define a timeout period while waiting for a client station

Usage: security { radioid { all11g { client-timeout <ct01x> }}}

Parameters: <ct01x> sets the client time out, in seconds from 1 to 65555

dot1x

Description: Specify the 802.1x STA timeout parameters

Usage: security { radioid { all11g { dot1x }}}

Parameters: none

encryption

Description: Define which WEP key will be used for data encryption

Usage: security { radioid { allradios { encryption <keynum> }}}

Parameters: <keynum> specifies the encryption key number, 1 to 4

keyhash

Description: Use encryption key hashing

Usage: security { radioid { allradios { encryption { ciphers { tkip { tkipwep40 { keyhash }}}}}}}

Parameters: none

mandatory

Description: Force station to use encryption to communicate with the XS-3900

Usage: security { radioid { allradios { encryption { mandatory }}}}

Parameters: none

membershiptermination

Description: Specify the time between key rotations (optional)
Usage: security { radioid { all11g { membershiptermination }}}
Parameters: none

mic

Description: Use the Message Integrity Check (MIC) function
Usage: security { radioid { allradios { encryption { ciphers { tkip { tkipwep40 { mic }}}}}}}
Parameters: none

optional

Description: Allow station to communicate with the XS-3900 with or without encryption
Usage: security { radioid { allradios { encryption { optional }}}}
Parameters: none

optkeyhash

Description: Use encryption key hashing (optional)
Usage: security { radioid { allradios { encryption { optional { optkeyhash }}}}}
Parameters: none

radioid

Description: Choose which radio (or all radios)
Usage: security { radioid { allradios | all11a | all11g | <radionum> }}}
Parameters: <radionum> specifies the radio number (1 to 16)

reauth-period

Description: Define the reauthentication period, in seconds
Usage: security { radioid { all11g { reauth-period <reauthper> }}}
Parameters: <reauthper> specifies the time before the next authentication attempt, between 1 and 65555 seconds

security

Description: Set the security parameters for the XS-3900's radios
Usage: security { radioid { allradios { encryption <keynum> }}}
Parameters: <keynum> specifies the encryption key number, 1 to 4

server

Description: Use the RADIUS server's reauthentication value instead of "reauth-period" value
Usage: security { radioid { all11g { server }}}
Parameters: none

tkip

Description: Specify TKIP as the cipher suite
Usage: security { radioid { allradios { encryption { ciphers { tkip { tkipwep40 }}}}}}
Parameters: none

tkipwep128

Description: Use 128 bit WEP with the TKIP cipher suite
Usage: security { radioid { allradios { encryption { ciphers { tkip { tkipwep128 }}}}}}
Parameters: none

tkipwep40

Description: Use 40 bit WEP with the TKIP cipher suite
Usage: security { radioid { allradios { encryption { ciphers { tkip { tkipwep40 }}}}}}
Parameters: none

wep

Description: Select the encryption type when configured for WEP
Usage: security { radioid { allradios { encryption { wep }}}}
Parameters: none

wep128

Description: Use 128 bit WEP encryption
Usage: security { radioid { allradios { encryption { wep128 }}}}
Parameters: none

wep40

Description: Use 40 bit WEP encryption
Usage: security { radioid { allradios { encryption { wep40 }}}}
Parameters: none

Station Timeouts

The following keywords are used for establishing STA timeouts.

activity-timeout

Description: Set the time period before the XS-3900 flags an inactive station
Usage: sta-timeouts { activity-timeout <at> }
Parameters: <at> specifies the time, in seconds, before the system flags an inactive STA

reauth-period

Description: Set the period after a station fails to authenticate before allowing more attempts
Usage: sta-timeouts { reauth-period <ht> }
Parameters: <ht> specifies the time, in seconds, before the next authentication attempt

sta-timeouts

Description: Set the station timeouts
Usage: sta-timeouts { activity-timeout <at> | reauth-period <ht> }
Parameters: <at> specifies the time, in seconds, before the system flags an inactive STA

<ht> specifies the time, in seconds, before the next authentication attempt

SSID Configuration

The following keywords are used for establishing SSID parameters.

add

Description: Add this SSID
Usage: ssid-manager { ssid <ss> { add }}
Parameters: <ss> specifies the SSID, up to 32 characters

del

Description: Delete this SSID
Usage: ssid-manager { ssid <ss> { del }}
Parameters: <ss> specifies the SSID, up to 32 characters

policy

Description: Define the policy associated with this SSID
Usage: ssid-manager { ssid <ss> { policy <sp> }}
Parameters: <ss> specifies the SSID, up to 32 characters
<sp>specifies the policy for this SSID, either 0, 1, 2 or 3, where:
0 = Open, 1 = MAC Auth., 2 = EAP Auth., 3 = Guest

qos-ssid

Description: Define QoS associated with this SSID
Usage: ssid-manager { ssid <ss> { qos-ssid <qs> }}
Parameters: <ss> specifies the SSID, up to 32 characters
<qs> identifies the QoS for this SSID

ssid

Description: Define this SSID
Usage: ssid-manager { ssid <ss> { add }
Parameters: <ss> specifies the SSID, up to 32 characters

ssid-brdcst

Description: Specify if you want to broadcast this SSID

Usage: ssid-manager { ssid <ss> { ssid-brdcst <sb> }}

Parameters: <ss> specifies the SSID, up to 32 characters

<sb> specifies if you want to broadcast this SSID, either 0 or 1, where:

0 = No, 1 = Yes

ssid-manager

Description: Set up SSID for a specific radio or the complete system

Usage: ssid-manager { ssid <ss> { add }

Parameters: <ss> specifies the SSID, up to 32 characters

vlan

Description: Define a VLAN ID associated with this SSID

Usage: ssid-manager { ssid <ss> { vlan <sv> }}

Parameters: <sv> identifies the VLAN for this SSID

DNS Configuration

The following keywords are used for establishing the DNS parameters.

dns

Description: Configure DNS settings

Usage: dns { hostname <hname> }

Parameters: <hname> specifies the host name

domain

Description: Enter your domain name

Usage: dns { domain <dom> }

Parameters: <dom> specifies your domain name, for example:

www.mydomain.com

hostname

Description: Enter your host name
Usage: dns { hostname <hname> }
Parameters: <hname> specifies the host name

server1

Description: Enter the primary DNS server
Usage: dns { server1 <srv1> }
Parameters: <srv1> specifies the primary DNS server

server2

Description: Enter the primary DNS server
Usage: dns { server2 <srv2> }
Parameters: <srv2> specifies the secondary DNS server

server3

Description: Enter the tertiary DNS server
Usage: dns { server3 <srv3> }
Parameters: <srv3> specifies the tertiary DNS server

NTP Configuration

The following keywords are used for establishing the NTP parameters.

disable

Description: Disable NTP services
Usage: ntp { disable }
Parameters: none

enable

Description: Enable NTP services
Usage: ntp { enable }
Parameters: none

ntp

Description: Enable/disable or configure NTP services
Usage: ntp { enable | disable }
Parameters: none

pri-nts

Description: Establish the primary NTP server IP address or DNS name
Usage: ntp { pri-nts <pntp> }
Parameters: <pntp> specifies the IP address or DNS name (primary)

sec-nts

Description: Establish the secondary NTP server IP address or DNS name
Usage: ntp { sec-nts <sntp> }
Parameters: <sntp> specifies the IP address or DNS name (secondary)

DHCP Configuration

The following keywords are used for establishing the DHCP parameters.

configure

Description: Configure DHCP services
Usage: dhcp { configure { start-ip-range <sipr> }}
Parameters: <sipr> specifies the starting IP address

default-lease

Description: Define the default lease period
Usage: dhcp { configure { default-lease <defl> }}
Parameters: <defl> specifies the default lease period, in minutes

dhcp

Description: Enable/disable or configure DHCP services
Usage: dhcp { enable | disable | configure { start-ip-range <sipr> }}
Parameters: <sipr> specifies the starting IP address

disable

Description: Disable DHCP services
Usage: dhcp { disable }
Parameters: none

enable

Description: Enable DHCP services
Usage: dhcp { enable }
Parameters: none

end-ip-range

Description: Define the DHCP server's ending IP address
Usage: dhcp { configure { end-ip-range <eipr> }}
Parameters: <eipr> specifies the ending IP address

max-lease

Description: Define the maximum allowable lease period
Usage: dhcp { configure { max-lease <maxl> }}
Parameters: <maxl> specifies the maximum allowable lease period, in minutes

start-ip-range

Description: Define the DHCP server's starting IP address
Usage: dhcp { configure { start-ip-range <sipr> }}
Parameters: <sipr> specifies the starting IP address

Syslog Configuration

The following keywords are used for establishing the Syslog parameters.

buffered

Description: Set the size of the local Syslog file
Usage: syslog { buffered <logfilesz> }
Parameters: <logfilesz> sets the number of records the local Syslog file holds before wrapping around

configure

Description: Configure Syslog services
Usage: syslog { configure { ipsyslog <slip> }}
Parameters: <slip> specifies the Syslog server IP address

console

Description: Display syslog messages on your console
Usage: syslog { configure { ipsyslog <slip> }}
Parameters: <slip> specifies the Syslog server IP address

ipsyslog

Description: Define the Syslog server IP address
Usage: syslog { console }
Parameters: none

level

Description: Log all messages with the level you define here
Usage: syslog { level <slev> }
Parameters: <slev> defines the syslog capture level

on

Description: Turn on Syslog services
Usage: syslog { on }
Parameters: none

syslog

Description: Turn on/off or configure Syslog services
Usage: syslog { on | configure { ipsyslog <slip> }}
Parameters: <slip> specifies the Syslog server IP address

SNMP Configuration

The following keywords are used for establishing the SNMP parameters.

community

Description: Define the SNMP communnity

Usage: snmp { community <csnmp> }

Parameters: <csnmp> specifies the SNMP Community string (letters and number only, no spaces or special characters)

disable

Description: Disable SNMP services

Usage: snmp { disable }

Parameters: none

enable

Description: Enable SNMP services

Usage: snmp { enable }

Parameters: none

snmp

Description: Enable/disable or configure SNMP services

Usage: snmp { enable | disable | snmpti <tisnmp> }

Parameters: <tisnmp> specifies the SNMP trap IP address

snmpta

Description: Send traps for authorization failures

Usage: snmp { snmpta <tasnmp> }

Parameters: <tasnmp> specifies whether or not to send traps, either 1 or 2, where:

1 = Send, 2= Don’t send

snmptp

Description: Define the SNMP trap port

Usage: snmp { snmptp <tpsnmp> }

Parameters: <tpsnmp> specifies the SNMP trap port

snmpti

Description: Define the SNMP trap IP address
Usage: snmp { snmpti <tisnmp> }
Parameters: <tisnmp> specifies the SNMP trap IP address

Filters

The following keywords are used for setting up filters.

configure

Description: Configure filters
Usage: filters { configure }
Parameters: none

disable

Description: Disable filters
Usage: filters { disable }
Parameters: none

enable

Description: Enable filters
Usage: filters { enable }
Parameters: none

filters

Description: Enable/disable or configure filters
Usage: filters { enable | disable | configure }
Parameters: none

Radius Configuration

The following keywords are used for configuring Radius services.

client-timeout

Description: Define 802.1x reply time from a client station

Usage: radius { radius-server { dot1x { client-timeout <cto1x> }}}

Parameters: <cto1x> specifies the time (in seconds) waiting for a client station 802.1x reply before timing out

configure

Description: Configure Radius server parameters

Usage: radius { radius-server { configure { radius-ip <radip> }}}

Parameters: <radip> specifies the IP address of the Radius server

dot1x

Description: Define 802.1x client (STA) settings

Usage: radius { radius-server { configure { dot1x }}}

Parameters: none

radius

Description: Configure Radius services

Usage: radius { radius-server { configure { radius-ip <radip> }}}

Parameters: <radip> specifies the IP address of the Radius server

radius-ip

Description: Define the Radius server IP address

Usage: radius { radius-server { configure { radius-ip <radip> }}}

Parameters: <radip> specifies the IP address of the Radius server

radius-port

Description: Define the Radius authentication port

Usage: radius { radius-server { configure { radius-port <radport> }}}

Parameters: <radport> specifies the Radius authentication port

radius-secret

Description: Define the Radius shared secret

Usage: radius { radius-server { configure { radius-secret <radsecret> }}}

Parameters: <radsecret> specifies the Radius shared secret

radius-server

Description: Configure the Radius server

Usage: radius { radius-server { configure { radius-ip <radip> }}}

Parameters: <radip> specifies the IP address of the Radius server

reauth-period

Description: Specify the elapsed time before allowing a client station to reattempt authentication

Usage: radius { radius-server { dot1x { reauth-period <reauthper> }}}

Parameters: <reauthper> specifies the amount of time (in seconds) after a timeout you wait before allowing a client station to retry authentication

server

Description: Use the “reauth-period” configured in the RADIUS server

Usage: radius { radius-server { dot1x { server }}}

Parameters: none

Reports

The following keywords are used for generating reports.

assoc

Description: Discover the number of devices associated with this XS-3900

Usage: reports { assoc }

Parameters: none

clear

Description: Clear all stored values for the selected interface

Usage: reports { clear { GigE <gnum> }}

Parameters: <gnum> defines the gigabit interface number, either 0 or 1

configure

Description: Configure and request reports for the selected interface
Usage: reports { configure { Dot11 <rnum> }}
Parameters: <rnum> defines the radio number, between 1 and 16

disable

Description: Disable report generation
Usage: reports { disable }
Parameters: none

Dot11

Description: Generate reports for the selected radio
Usage: reports { configure { Dot11 <rnum> }}
Parameters: <rnum> defines the radio number, between 1 and 16

enable

Description: Enable report generation
Usage: reports { enable }
Parameters: none

GigE

Description: Generate reports for the selected gigabit interface
Usage: reports { configure { GigE <gnum> }}
Parameters: <gnum> defines the gigabit interface number, either 0 or 1

num-ap

Description: Discover the number of AP devices associated with this XS-3900
Usage: reports { num-ap }
Parameters: none

num-Client

Description: Discover the number of clients associated with this XS-3900
Usage: reports { num-Client }
Parameters: none

reports

Description: Enable/disable or configure report generation
Usage: reports { enable | disable | configure | clear }}}
Parameters: none

Data Handling

The following keywords are used for defining how data is handled by the system.

packet

Description: Define global packet commands
Usage: packet { retries <pktretry> | payload-encapsulation <encap1> }
Parameters: <pktretry> specifies the packet retry value
<encap1> choose either dot1H or snap

payload-encapsulation

Description: Define the type of encapsulation to use
Usage: packet { payload-encapsulation <encap1> }
Parameters: <encap1> choose either dot1H or snap

retries

Description: Define the maximum number of retries for sending a packet
Usage: packet { retries <pktretry> }
Parameters: <pktretry> specifies the packet retry value

Data Clearance

The following keywords are used for clearing or removing data from selected elements.

clear

Description: Remove/clear requested elements
Usage: clear { dot11 { client <stamacaddr> }}
Parameters: <stamacaddr> specifies the MAC address of a client station you want to disassociate

client

Description: Designates a client station to deauthenticate

Usage: clear { dot11 { client <stamacaddr> }}

Parameters: <stamacaddr> specifies the MAC address of a client station you want to disassociate

dot11

Description: Designates a wireless interface

Usage: clear { dot11 { client <stamacaddr> }}

Parameters: <stamacaddr> specifies the MAC address of a client station you want to disassociate

statistics

Description: Designates accumulated counters, such as amount of data transmissions

Usage: clear { dot11 { statistics <statmac> }}

Parameters: <statmac> specifies the MAC address of a client station from which you want clear all statistical data

Show Information

The following keywords are used for displaying system information.

adjacent-ap

Description: Select all adjacent APs that are members of a WDS roaming neighborhood

Usage: show { dot11 { adjacent-ap }}

Parameters: none

carrier-busy

Description: Show the percentage of CCA that is busy

Usage: show { carrier-busy }

Parameters: none

controllers

Description:	Display radio baseband information
Usage:	show { controllers { dot11radio <contnum> }}
Parameters:	<contnum> specifies the radio ID or number (1 to 16)

dot11

Description:	Select the wireless interface
Usage:	show { dot11 { adjacent-ap }}
Parameters:	none

dot11radio

Description:	Select a specific radio
Usage:	show { controllers { dot11radio <contnum> }}
Parameters:	<contnum> specifies the radio ID or number (1 to 16)

file

Description:	Display the individual file size
Usage:	show { file { info <showfnm> }
Parameters:	<showfnm> specifies the individual file name

flash

Description:	Display the flash size and free space
Usage:	show { flash }
Parameters:	none

hosts

Description:	Display cached host names
Usage:	show { hosts }
Parameters:	none

info

Description:	Displayinformation that is specific to an individual file name
Usage:	show { file { info <showfnm> }
Parameters:	<showfnm> specifies the individual file name

interface

Description: Display all available interface information
Usage: show { interface }
Parameters: none

line

Description: Display the terminal status
Usage: show { line }
Parameters: none

local-server

Description: Display the embedded RADIUS server on this XS-3900
Usage: show { radius { local-server { statistics }}}
Parameters: none

radius

Description: Display the Radius server information
Usage: show { radius { local-server { statistics }}}
Parameters: none

running_config

Description: Display the configuration the XS-3900 is currently executing
Usage: show { running_config }
Parameters: none

show

Description: Display current information about the selected item
Usage: show { version }
Parameters: none

startup_config

Description: Display the configuration the XS-3900 booted from
Usage: show { startup_config }
Parameters: none

statistics

Description:	Display statistics for this embedded RADIUS server
Usage:	show { radius { local-server { statistics }}}
Parameters:	none

system-files

Description:	List all system file names and sizes
Usage:	show { file { system-files }}
Parameters:	none

users

Description:	Display user information
Usage:	show { users }
Parameters:	none

version

Description:	Display the system version information
Usage:	show { version }
Parameters:	none

Remove Configuration

The following keywords are used to remove/disable existing configurations.

activity-timeout

Description:	Set the client inactivity timeout to the default value
Usage:	no { dot11 { activity-timeout }}
Parameters:	none

authentication

Description:	Disable all authentication support (open system)
Usage:	no { security { authentication }}
Parameters:	none

beacon

Description:	Disable all beacon support
Usage:	no { dot11 { beacon }}
Parameters:	none

client

Description:	Reset to default the maximum power a client can transmit (this will be advertised by the XS-3900)
Usage:	no { dot11 { power { client }}}
Parameters:	none

client-timeout

Description:	Set to default the amount of time a client must wait for a EAP response
Usage:	no { dot1x { client-timeout }}
Parameters:	none

dhcp-server

Description:	Disable DHCP services
Usage:	no { ip { dhcp-server }}
Parameters:	none

domain-lookup

Description:	Disable all DNS servers
Usage:	no { ip { domain-lookup }}
Parameters:	none

dot11

Description:	Make the “no” command specific to the WLAN
Usage:	no { dot11 { activity-timeout }}
Parameters:	none

dot1x

Description: Make the “no” command specific to 802.1x components
Usage: no { dot1x { client-timeout }}
Parameters: none

encryption

Description: Disable all encryption
Usage: no { dot11 { encryption }}
Parameters: none

holdoff-time

Description: Set to default the amount of time to wait for client authentication
Usage: no { dot11 { holdoff-time }}
Parameters: none

http-port

Description: Set the HTTP port to the default value of 80
Usage: no { ip { http-port }}
Parameters: none

http-server

Description: Disable internal Web services (the Web-based configuration will be disabled)
Usage: no { ip { http-server }}
Parameters: none

ip

Description: Define IP’s to apply the no (removal) command
Usage: no { ip { dhcp-server }}
Parameters: none

local

Description: Reset to default the maximum power the AP can transmit

Usage: no { dot11 { power { local }}}

Parameters: none

name-server

Description: Disable this specific DNS server by IP address

Usage: no { ip { name-server <nsip> }}

Parameters: <nsip> specifies the IP address of the target name server to disable

no

Description: Disable if enabled, or set to default value

Usage: no { ip { dhcp-server }}

Parameters: none

power

Description: Reset power settings to their default values

Usage: no { dot11 { power { client }}}

Parameters: none

preamble

Description: Reset preamble to the deault

Usage: no { dot11 { preamble }}

Parameters: none

radio

Description: Disable a specific radio

Usage: no { dot11 { radio <noradionum> }}

Parameters: <noradionum> specifies the target radio to disable (1-16)

reauth-period

Description: Set the number of authentication retries to default

Usage: no { reauth-period }

Parameters: none

rts

Description: Disable RTS support
Usage: no { dot11 { rts }}
Parameters: none

security

Description: Disable security commands or reset to defaults
Usage: no { security { authentication }}
Parameters: none

ssid

Description: Remove a specific SSID
Usage: no { dot11 { ssid <nossid> }}
Parameters: <nossid> specifies the target SSID to remove from the system

syslog

Description: Disable the Syslog services
Usage: no { ip { syslog }}
Parameters: none

worldmode

Description: Disable world mode
Usage: no { worldmode }
Parameters: none

Help

The following keyword is used to provide a description of the interactive Help system.

help

Description: Provide a description of the Help system
Usage: help
Parameters: none

Appendix A: Quick Reference Guide

This chapter contains XS-3900 product reference information. Use this chapter to locate the information you need quickly and efficiently. Section headings for this chapter include:

- Review of WMI Pages
- Alphabetical Listing of CLI Keywords
- Factory Default Settings
- Keyboard Shortcuts
- Keyboard Shortcuts

Review of WMI Pages

This section provides a review of the product's WMI pages, with a brief explanation of their function and content. Click on any of the listed pages to go to the corresponding procedure at the referenced destination.

Page	Function
Array Status	Provides a snapshot of the global configuration settings for all XS-3900 network interfaces and radios.
Express Setup	Establish global configuration settings that will enable basic XS-3900 functionality.
Network Interfaces	Provides a snapshot of the configuration settings currently established for the network interfaces.
Network Settings	Establish basic configuration settings for the network interfaces.
VLAN Settings	Add or remove VLANs, associate VLANs to a specific network interface, and enable VLAN tagging of outgoing traffic.

Page	Function
Network Statistics	Provides statistical data associated with network interfaces and their activity.
DHCP Server Settings	Enable or disable DHCP (Dynamic Host Configuration Protocol) server functionality.
DNS Settings	Set up a DNS server (or multiple servers), if you want to offer clients associating with the XS-3900 the ability to use meaningful domain names (URLs) instead of numerical IP addresses.
IAP Interfaces	Provides a snapshot of global configuration data associated with radios.
IAP Settings	Enable or disable radios, define the wireless mode for each radio, establish the transmit and receive parameters, and define global settings for the beacon interval and DTIM period.
Global Settings	Establish global IAP (radio) settings. Global IAP settings include enabling or disabling all radios (regardless of their operating mode).
Global Settings .11a	Establish global 802.11a IAP (radio) settings.
Global Settings .11bg	Establish global 802.11b/g IAP (radio) settings.
IAP LED Settings	Set the behavior of LEDs.
Statistics	Provides an overview of statistical data associated with individual radios.

Page	Function
SSID Management	Provides a snapshot of SSID (Service Set IDentifier) assignments. It includes the SSID name, whether or not an SSID is visible on the network, any security and QoS parameters defined for each SSID, associated VLAN IDs, guest access, and radio availability per SSID.
Create SSID	Create, delete (or restore) and manage SSIDs. It also allows you to assign security parameters and VLANs on a per SSID basis.
Edit SSID	Edit existing SSIDs and reassign security parameters and VLANs on a per SSID basis.
Security	Provides a snapshot of XS-3900 global security configuration parameters, including administration accounts, ACL values, WEP/WPA/WPA2 status, and RADIUS configuration settings.
Security Management	Establish the security parameters for your wireless network, including WEP, WPA and RADIUS authentication.
Radius Server	Set up the XS-3900’s internal RADIUS server, or set up an external RADIUS server for user authentication.
Radius User	Create, delete and manage RADIUS user accounts.
MAC Access List	Create new MAC-based Access Control Lists (ACLs), delete existing ACLs, and add, remove, or restore MAC addresses.

Page	Function
Create Admin	Create new network administrator accounts, delete existing accounts, or restore accounts. It also allows you to limit account access to a read only status.
Edit Admin	Edit existing network administrator accounts, change passwords, and re-define whether an account is limited to a read only status.
Users	Provides a snapshot of users currently associated with the network.
Services	Provides a current status of Syslog and SNMP services.
System Log	Enable or disable the Syslog server, define the server's IP address, and set the level for Syslog reporting.
SNMP	Enable or disable SNMP and define the SNMP parameters.
Software	Upgrade the system firmware.
Tools	Ping the XS-3900 and obtain a status of the unit's performance.
Event Log	Provides an event log for the wireless network.

Alphabetical Listing of CLI Keywords

This section provides a listing of all available CLI keywords, sorted alphabetically. Where the same keyword appear multiple times, the functional areas that it pertains to are also included (italicized). Click on any keyword to jump to the referenced destination.

contact-info
controllers
copy

D

def
default-gateway
default-lease
default_rates
defpw
del
description
dhcp
dhcpbind
dhcp-server *system admin.*
dhcp-server *remove config.*
dir
disable *ntp config.*
disable *dhcp config.*
disable *snmp config.*
disable *filters*
disable *reports*
dns
domain
domain-lookup
domain-name
Dot11
dot11 *data clearance*
dot11 *show information*
dot11 *remove config.*
dot11a
dot11g
dot11gonly
dot11preamble
dot11radio
dot1x *security*
dot1x *radius config.*
dot1x *remove config.*
down *interface config.*
down *radio config.*
DTIM-rate

E

edcf
email
enable *ntp config.*
enable *dhcp config.*
enable *snmp config.*
enable *filters*
enable *reports*
enable1
enable11
enable12
enable18
enable2
enable24
enable36
enable48
enable5
enable54
enable6
enable9
encryption *security*
encryption *remove config.*
end-ip-range
erase

F

faste
file

filters
flash
frag-threshold
ftp
fullduplex

G

gateway
gigabit
GigE

H

halfduplex
help
holdoff-time
hostname *system admin.*
hostname *dns config.*
hosts
http-port
http-server

I

info
interface *interface selection*
interface *show information*
ip *system config.*
ip *remove config.*
ip-addr
ipsyslog

K

keyhash

L

least_congested
led
level
line *interface selection*
line *show information*
linktest
local
local-server
location
logout
long-retry-limit

M

management
mandatory
mask
max-client-txpwr
max-lease
membershiptermination
mic
model
more
mtu

N

name
name-server *system admin.*
name-server *remove config.*
no
ntp
num-ap
num-Client

O

off
on *radio configuration*

on *syslog configuration*
optional
optkeyhash

P

packet
parity
payload-encapsulation
period
ping
policy
power
preamble
prelong
preshort
pri-nts

Q

qos-ssid

R

radio
radioid
radios
radius *radius config.*
radius *show information*
radius-ip
radius-port
radius-secret
radius-server
range
rate1
rate11
rate12
rate18
rate2
rate24
rate36
rate48
rate5
rate54
rate6
rate9
reauth-period *security*
reauth-period *station timeouts*
reauth-period *radius config.*
reauth-period *remove config.*
reboot
receiving
reload
reports
reset
retries
rts
rts-threshold
running_config
run-tests
Rxdiversity
Rxleft
Rxright

S

sec-nts
security *security*
security *remove config.*
serial
server *security*
server *radius config.*
server1
server2

server3
short-retry-limit
show
show-version
shut-down
snmp
snmpta
snmptp
snmpti
software
speed *interface config.*
speed *radio config.*
ssid *ssid config.*
ssid *remove comfig.*
ssid-brdcst
ssid-manager
startup_config
start-ip-range
sta-timeouts
statistics *data clearance*
statistics *show information*
stopbits
syslog *syslog config.*
syslog *remove config.*
system-files

T

throughput
tkip
tkipwep128
tkipwep40
traceroute
transmiting
Txdiversity
Txleft
tx-pwr
Txright

U

up *interface config.*
up *radio config.*
userid
users

V

version
vlan

W

wep
wep128
wep40
worldbeacon
worldmode

Factory Default Settings

The following tables show the XS-3900's factory default settings.

Network Interfaces

Serial

Setting	Default Value
Baud Rate	115200
Word Size	8 bits
Stop Bits	1
Parity	No parity
Time Out	10 seconds

Gigabit 1 and Gigabit 2

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.1.2
Default IP Mask	255.0.0.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1500
Management Enabled	Yes

Fast Ethernet

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.1.1
Default IP Mask	255.0.0.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	100 Mbps
MTU Size	1500
Management Enabled	Yes

Integrated Access Points (IAPs)

Setting	Default Value
Antenna	0
Mode	11a for a1 to a12 11g for abg1 to abg4
Channel	Auto
Maximum Transmit Power	0
Cell Size	Medium

Server Settings

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes
IP Start Range	192.168.1.1
IP End Range	192.168.1.100

External RADIUS

Setting	Default Value
Enabled	Yes
Primary Server	0.0.0.0
Primary Port	1812
Primary Secret	xirrus
Secondary Server	null (no IP address)
Secondary Port	1812
Secondary Secret	null (no secret)
Time Out (before primary server is retired)	600 seconds

Internal RADIUS

Setting	Default Value
Enabled	No
The user database is cleared upon reset to the factory defaults. For the Internal RADIUS Server you have a maximum of 200 entries.	

NTP

Setting	Default Value
Enabled	No
Primary	time.nist.gov
Secondary	192.6.15.29

Syslog

Setting	Default Value
Enabled	No

SNMP

Setting	Default Value
Enabled	No
Coomunity String	xirrus
Trap Host	null (no setting)
Trap Port	162
Authorization Fail Port	1

Default SSID

Setting	Default Value
ID	xirrus
VLAN	None
Encryption	Off
Encryption Type	None
QoS	None
Enabled	Yes

Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)
WEP Key Length	null (all 4 keys)
Default Key ID	0
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	No
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	600

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
Telnet	On
SSH	On

Keyboard Shortcuts

The following table shows the most common keyboard shortcuts.

Action	Shortcut
Cut selected data and place it on the clipboard.	**Ctrl + X**
Copy selected data to the clipboard.	**Ctrl + C**
Paste data from the clipboard into a document (at the insertion point).	**Ctrl + V**
Copy the active window to the clipboard.	**Alt + Print Screen**
Copy the entire desktop image to the clipboard.	**Print Screen**
Abort an action at any time.	**Esc**
Go back to the previous screen.	**b**
Access the Help screen.	**?**

Appendix B: Technical Support

This chapter provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all sections in this chapter and try to determine if your problem resides with XS-3900 or your network infrastructure. Section headings for this chapter include:

- General Hints and Tips
- Frequently Asked Questions
- Frequently Asked Questions
- Contact Information
- Contact Information

General Hints and Tips

This section provides some useful tips that will optimize the reliability and performance of your XS-3900 unit(s).

- The XS-3900 requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.
- If using multiple XS-3900s at the same location, we recommend maintaining a distance of at least 50 feet between units.
- Keep the XS-3900 away from electrical devices or appliances that generate RF noise. Because the XS-3900 is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).
- If using AC power, each XS-3900 unit requires its own dedicated AC power outlet. Do not attempt to “piggy-back” AC power to multiple units. If deploying multiple units, consider using the optional Xirrus Remote DC Power System (XP-3100).
- If you are deploying multiple units, ensure that the “clock face” of all units is aligned in the same direction.
- The XS-3900 should only be used with Wi-Fi certified client devices.

Frequently Asked Questions

This section answers some of the most frequently asked questions, organized by functional area.

Multiple SSIDs

Q. What Are BSSIDs and SSIDs?

A. BSSID (Basic Service Set Identifier) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS.

A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS by way of a backbone that interconnects each access point.

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

Legacy access points typically support one SSID per access point. Xirrus Wireless LAN Arrays support the ability for multiple SSIDs to be defined and used simultaneously.

Q. What would I use SSIDs for?

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

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

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

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

Q. **How do I set up SSIDs?**

A. Use the following procedure as a guideline. For more detailed information, go to "SSID Management" on page 92.

1. From the Web Management Interface, go to the Create SSID page.
2. Select **Yes** to make the SSID visible to all clients on the network. Although the XS-3900 will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
3. Select the minimum security that will be required by users for this SSID.
4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.
5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.
6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.
7. Click on the **Apply** button to apply your changes to this session.
8. Click on the **Save** button to save your changes.
9. If you need to edit any of the SSID settings, you can do so from the Edit SSID page.

Security

Q. How do I know my management session is secure?

A. Follow these guidelines:

- Administrator passwords
  Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.

- SSH versus Telnet
  Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY.

- Configuration auditing
  Do not change approved configuration settings. The optional Xirrus Wireless Management System (XM-3300) offers powerful management features for small or large XS-3900 deployments, and can audit your configuration settings automatically. In addition, using the XM-3300 eliminates the need for an FTP server.

Q. Which wireless data encryption method should I use?

A. Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The XS-3900 allows you to establish the following data encryption configuration options:

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

- WEP (Wired Equivalent Privacy)
  This option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.

- WPA (Wi-Fi Protected Access)
  This is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

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

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

Any of the above encryption modes can be used (and can be used at the same time).

Q. **Which user authentication method should I use?**

A. User authentication ensures that users are who they say they are. For this purpose, the XS-3900 allows you to choose between the following user authentication methods:

- Pre-Shared Key
  Users must manually enter a key (pass phrase) on the client side of the wireless network that matches the key stored by the administrator in the XS-3900.

- RADIUS 802.1x with EAP
  802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal (provided by the XS-3900) or external. An external RADIUS server offers more functionality and is **recommended** for large Enterprise deployments.

  When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

- MAC Address ACLs (Access Control Lists)
  MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC addresses of each user in the **Allow** list. In the event of a lost or stolen MAC adapter, enter the affected MAC address in the **Deny** list.

Q. **Why do I need to authenticate my XS-3900 units?**

A. When deploying multiple XS-3900 units, you may need to define which units are part of which wireless network (for example, if you are establishing more than one network). In this case, you need to employ the Xirrus Wireless Management System (XM-3300) which can authenticate your XS-3900 units automatically and ensure that only authorized units are associated with the defined wireless network.

Q. **What is rogue AP (Access Point) detection?**

A. The XS-3900 has a dedicated radio (abg/4) which constantly scans the local wireless environment for rogue APs (non-Xirrus devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

VLAN Support

Q. **What Are VLANs?**

A. VLANs (Virtual Local Area Networks) are a logical grouping of network devices that share a common network broadcast domain. Members of a particular VLAN can be on any segment of the physical network but logically only members of a particular VLAN can see each other.

VLANs are defined and implemented using the wired network switches that are VLAN capable. Packets are tagged for transmission on a particular VLAN according to the IEEE 802.1Q standard, with VLAN switches processing packets according to the tag.

Q. **What would I use VLANs for?**

A. Logically separating different types of users, systems, applications, or other logical division aids in performance and management of different network devices. Different VLANs can also be assigned with different packet priorities to prioritize packets from one VLAN over packets from another VLAN.

VLANs are managed by software settings—instead of physically plugging in and moving network cables and users—which helps to ease network management tasks.

Q. **What are Wireless VLANs?**

A. Wireless VLANs allow similar functionality to the wired VLAN definitions and extend the operation of wired VLANs to the wireless side of the network.

Wireless VLANs can be mapped to wireless SSIDs so that traffic from wired VLANs can be sent to wireless users of a particular SSID. The reverse is also true, where wireless traffic originating from a particular SSID can be tagged for transmission on a particular wired VLAN.

Sixteen SSIDs can be defined on the XS-3900, allowing a total of sixteen VLANs to be accessed (one per SSID).

As an example, to provide guest user access an SSID of **guest** might be created. This SSID could be mapped to a wired VLAN that segregates unknown users from the rest of the wired network and restricts them to Internet access only. Wireless users could then associate to the wireless network via the **guest** SSID and obtain access to the Internet through the selected VLAN, but would be able to access other privileged network resources.

Q. **How do I set up Wireless VLANs?**

A. Use the following procedure as a guideline. For more detailed information, go to "VLAN Settings" on page 71.

1. From the Web Management Interface, go to the VLAN Settings page.
2. Create a new VLAN by defining the same VLAN ID as the one you are using on the wired network.
3. If desired (optional), assign a description to this VLAN.
4. Select the wired Ethernet interface that this VLAN is defined for.
5. Select **Tag Outgoing Packets**.
6. Go to the SSID Management menu and either create a new SSID or edit an existing SSID. From the SSID property page, choose the desired VLAN for this SSID.
7. Click on the **Apply** button to apply your changes to this session.
8. Click on the **Save** button to save your changes.

Contact Information

Xirrus, Inc. is located in Westlake Village, California, just 45 minutes northwest of downtown Los Angeles and 45 minutes southeast of Santa Barbara.

Xirrus, Inc.
370 North Westlake Blvd, Suite 200
Westlake Village, CA 91362
USA

Tel: 1.805.497.0955
Fax: 1.805.449.1180

www.xirrus.com

Use this space for your notes ...

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11d

A supplement to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It allows Access Points to communicate information on the permissible radio channels with acceptable power levels for user devices. Because the 802.11 standards cannot legally operate in some countries, 802.11d adds features and restrictions to allow WLANs to operate within the rules of these countries.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.1Q

An IEEE standard for MAC layer frame tagging (also known as encapsulation). Frame tagging uniquely assigns a user-defined ID to each frame. It also enables a switch to communicate VLAN membership information across multiple (and multi-vendor) devices by frame tagging.

AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

beacon interval

When a device in a wireless network sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. Network administrators can adjust the beacon interval—usually measured in milliseconds (ms) or its equivalent, kilo-microseconds (Kmsec).

bit rate

The transmission rate of binary symbols ('0' and '1'), equal to the total number of bits transmitted in one second.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a BSS network. See also, SSID.

cell

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11). In the 5 GHz band, 802.11a uses 8 channels for indoor use and 4 for outdoor use, none of which overlap.

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

default gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DHCP lease

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the “domain” address for Xirrus is: http://www.xirrus.com, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.
- **www** is a reference to the World Wide Web.
- **xirrus** refers to the company.
- **com** specifies that the domain belongs to a commercial enterprise.

DTIM

(Delivery Traffic Indication Message) A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

EAP

(Extensible Authentication Protocol) When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). However, LCP is somewhat inflexible because it has to specify an authentication device early in the process. EAP allows the system to gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP (for example, passwords and public keys).

EDCF

(Enhanced Distributed Coordinator Function) A QoS extension which uses the same contention-based access mechanism as current devices but adds “offset contention windows” that separate high priority packets from low priority packets (by assigning a larger random backoff window to lower priorities than to higher priorities). The result is “statistical priority,” where high-priority packets usually are transmitted before low-priority packets.

encapsulation

A way of wrapping protocols such as TCP/IP, AppleTalk, and NetBEUI in Ethernet frames so they can traverse an Ethernet network and be unwrapped when they reach the destination computer.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

Fast Ethernet

A version of standard Ethernet that runs at 100 Mbps rather than 10 Mbps.

FCC

(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

frame

A packet encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

Gigabit 1

The primary Gigabit Ethernet interface. See also, Gigabit Ethernet.

Gigabit 2

The secondary Gigabit Ethernet interface. See also, Gigabit Ethernet.

Gigabit Ethernet

The newest version of Ethernet, with data transfer rates of 1 Gigabit (1,000 Mbps).

host name

The unique name that identifies a computer on a network. On the Internet, the host name is in the form **comp.xyz.net**. If there is only one Internet site the host name is the same as the domain name. One computer can have more than one host name if it hosts more than one Internet site (for example, **home.xyz.net** and **comp.xyz.net**. In this case, **comp** and **home** are the host names and **xyz.net** is the domain name.

IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs.

MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTU

(Maximum Transmission Unit) The largest physical packet size—measured in bytes—that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

PLCP

(Physical Layer Convergence Protocol) Defined by IEEE 802.6, a protocol specified within the Transmission Convergence layer that defines exactly how cells are formatted within a data stream for a particular type of transmission facility.

preamble

Preamble (sometimes called a header) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. PLCP has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

private key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

PSK

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

public key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider guarantees a service's performance, such as an average or minimum throughput rate.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

RDPS

(Remote Distribution Power Supply) A Xirrus proprietary power supply used for delivering power from a remote source to the Xirrus family of products.

Remote DC Power System (XP-3100)

An optional Xirrus proprietary product that provides distributed DC power to multiple XS-3900 units, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SDMA

(Spatial Division Multiple Access) A wireless communications mode that optimizes the use of the radio spectrum and minimizes cost by taking advantage of the directional properties of antennas. The antennas are highly directional, allowing duplicate frequencies to be used for multiple zones.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSH

(Secure SHell) Developed by SSH Communications Security, Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. SSH protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot "play back" the traffic or hijack the connection when encryption is enabled. When using SSH's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

TKIP

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven’t been tampered with.

transmit power

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

VLAN

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

VLAN tagging

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the 802.1Q standard, traffic can be confined to VLANs that exist on multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

1. That the packet has a tag.
2. Whether the packet should have priority over other packets.
3. Which VLAN it belongs to, so that the switch can forward or filter it correctly.

WEP

(Wired Equivalent Privacy) An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. The Wired Equivalent Privacy generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.

Wi-Fi Alliance

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

Wireless LAN Array (XS-3900)

A Xirrus proprietary high capacity wireless access point utilizing multiple channels, specifically designed for the Enterprise market.

Wireless Management System (XM-3300)

A Xirrus proprietary product used for managing large XS-3900 deployments from a centralized Web-based interface.

WPA

(Wi-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1X for authentication.

XM-3300

The Xirrus Wireless Management System (XM-3300) is a Xirrus proprietary product used for managing large XS-3900 deployments from a centralized Web-based interface.

XP-3100

The Xirrus Remote DC Power System (XP-3100) is an optional Xirrus proprietary product that provides distributed DC power to multiple XS-3900 units, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.

XS-3900

The Xirrus Wireless LAN Array (XS-3900) is a high capacity, multi-wireless access point specifically designed for the Enterprise market.

Use this space for your notes ...

Index