

Configuring the Xirrus Array

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/XS-3700/XS-3500 with your Web browser.

Section headings for this chapter include:

- “Logging In” on page 69
- “Making Configuration Changes to the Array” on page 70

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 Wireless LAN Array via its default IP address (10.0.1.1) or via a DHCP assigned IP address.
3. When connected to the Array, a login prompt appears on your screen. The default login for the user name and password is **admin** for both. Login names and passwords are case-sensitive.
4. To log in to the Array's Web Management Interface, enter **admin** when prompted for a user name and password.



Figure 46. WMI: Logging In to the Wireless LAN Array

Making Configuration Changes to the Array

This section has been organized into functional areas that reflect the flow and content of the WMI. Configuration instructions to the Wireless LAN Array 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/XS-3700/XS-3500 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).

XS-3900 Wireless LAN Array

WLAN Array Status					
Express Set-Up	Network Interface	Status	Management	Configuration	IP Address
▶ Network Interfaces	10/100 Megabit	Enabled	Enabled	DHCP	192.168.0.7
▶ IAP Interfaces	Gigabit Interface 1	Enabled	Enabled	DHCP	10.0.1.2
▶ SSID	Gigabit Interface 2	Enabled	Enabled	DHCP	10.0.1.2
▶ Security	Integrated Access Points				
▶ Stations	IAP Interface	Status	Channel	Cell Size	Associated Users
▶ Services	abg1	Enabled	1	Large	0
▶ Array Info	abg2	Enabled	6	Large	0
▶ Tools	abg3	Enabled	11	Large	0
▶ Show Config	abg4	Enabled	6	Large	0
▶ Event Log	a1	Enabled	36	Large	0
	a2	Enabled	52	Large	0
	a3	Enabled	149	Large	0
	a4	Enabled	40	Large	0
	a5	Enabled	56	Large	0
	a6	Enabled	157	Large	0
	a7	Enabled	44	Large	0
	a8	Enabled	60	Large	0
	a9	Enabled	153	Large	0
	a10	Enabled	48	Large	0
	a11	Enabled	64	Large	0
	a12	Enabled	161	Large	0

● Critical Msgs: 1

● Warning Msgs: 0

● General Msgs: 9

Location:

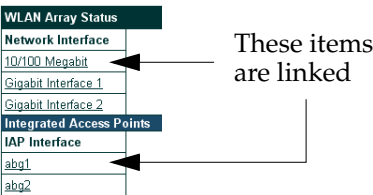
Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 47. 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:

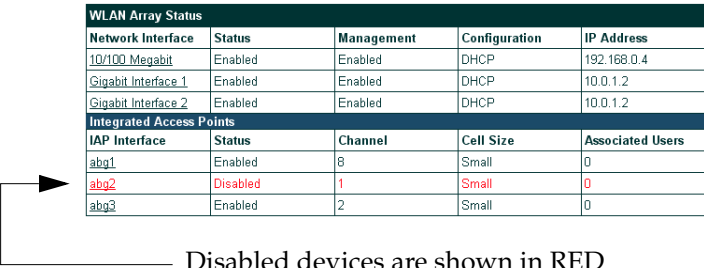
- **All devices:** A listing of the available Network Interfaces and IAPs with each item containing a link to the associated configuration page. Linked items are shown UNDERLINED. For example:



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

Figure 48. 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 49. 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 25.

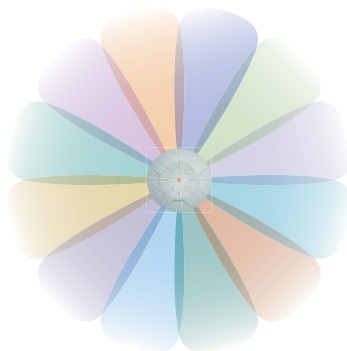


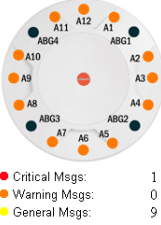
Figure 50. IAP Cells

- 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 (1024 or 960 users per Array when the monitor is enabled).

Express Setup

This page allows you to establish global configuration settings that will enable basic Array 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.

XS-3900 Wireless LAN Array



● Critical Msgs: 1
● Warning Msgs: 0
● General Msgs: 9

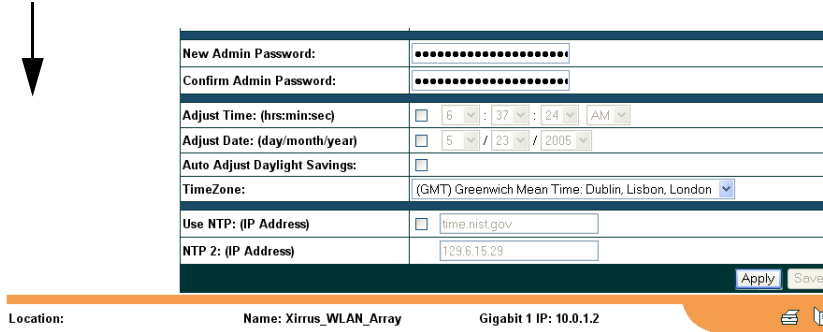


Express Set-Up	
Express Set-Up	Host Name: Xirrus_WLAN_Array
Network Interfaces	Location Information:
IAP Interfaces	Admin Contact:
SSID	Admin Email:
Security	Admin Phone:
Stations	Enable/Configure All IAP's: Execute
Services	
Array Info	
Tools	
Show Config	
Event Log	
10/100 Megabit Settings	
Enable Interface:	☒ Yes ☐ No
Allow Management On Interface:	☒ Yes ☐ No
Configuration Server Protocol:	☒ DHCP ☐ Static
IP Address:	192.168.0.7
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Gigabit Interface 1 Settings	
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	
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 51. WMI: Express Setup Page (Part 1)

... continued



The screenshot shows the 'WMI: Express Setup Page (Part 2)' for the Xirrus WLAN Array. The page has a blue header with the Xirrus logo and 'Wireless LAN Array'. Below the header, there's a section for 'New Admin Password' and 'Confirm Admin Password', both with masked input fields. The 'Adjust Time' section includes a checkbox, a time selector (6:37:24 AM), and a date selector (5/23/2005). The 'Auto Adjust Daylight Savings' section has a checkbox. The 'TimeZone' section has a dropdown menu set to '(GMT) Greenwich Mean Time: Dublin, Lisbon, London'. The 'Use NTP' section has a checkbox and a text input field containing 'time.nist.gov'. The 'NTP 2' section has a text input field containing '129.6.15.29'. At the bottom right, there are 'Apply' and 'Save' buttons. Below the form, a status bar shows 'Location:', 'Name: Xirrus_WLAN_Array', and 'Gigabit 1 IP: 10.0.1.2'.

Figure 52. WMI: Express Setup Page (Part 2)

Procedure for Performing an Express Setup

1. **Host Name:** Specify a unique **host name** for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters.
2. **Location Information:** Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
3. **Admin Contact:** Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
4. **Admin Email:** Enter the email address of the admin contact you entered in Step 3.
5. **Admin Phone:** Enter the telephone number of the admin contact you entered in Step 3.
6. **Enable/Configure All IAPs:** Click on the **Execute** button to enable and auto configure all IAPs (a message displays the countdown time—in seconds—to complete the auto-configuration task).

7. Configure the **Fast Ethernet** (10/100 Megabit), **Gigabit 1** and **Gigabit 2** network interfaces. The fields for each of these interfaces are the same, and include:
 - a. **Enable Interface:** Choose **Yes** to enable this network interface, or choose **No** to disable the interface.
 - b. **Allow Management on Interface:** Choose **Yes** to allow management of the Array via this network interface, or choose **No** to deny all management privileges for this interface.
 - c. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** to assign IP addresses to the Array's Ethernet interfaces, or choose **Static 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.
8. **SSID (Wireless Network Name):** The SSID (Service Set Identifier) is a unique name that identifies a wireless network. All devices attempting to connect to a specific WLAN must use the same SSID. The default for this field is "**xirrus**."

For additional information about SSIDs, go to the **Multiple SSIDs** section of "Frequently Asked Questions" on page 222.

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

Open

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

WEP (Wired Equivalent Privacy)

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

WPA (Wi-Fi Protected Access)

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

For more information about security, including a full review of all security options and settings, go to “[Security Management](#)” on page 113.



Security settings will only take effect if they are assigned to a specific SSID. Refer to “[SSID](#)” on page 107.

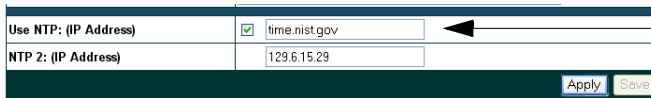
10. **Wireless Key/Passphrase:** Depending on the wireless security scheme you selected, enter a unique WEP key or WPA passphrase.
 - a. **Confirm Key/Passphrase:** If you entered a WEP key or WPA passphrase, confirm it here.
11. **New Admin Password:** If desired, enter a new administration password 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.
12. **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).
13. **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).
14. **Auto Adjust Daylight Savings:** Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
15. **Time Zone:** Select a time zone from the choices available in the pull-down list.

(GMT - 12:00) Eniwetok, Kwajalein
 (GMT - 11:00) Midway Island, Samoa</option>
 (GMT - 10:00) Hawaii
 (GMT - 09:00) Alaska
 (GMT - 08:00) Pacific Time (US & Canada); Tijuana
 (GMT - 07:00) Mountain Time (US & Canada)
 (GMT - 06:00) Central Time (US & Canada)
 (GMT - 05:00) Eastern Time (US & Canada)
 (GMT - 04:00) Atlantic Time (Canada)
 (GMT - 03:30) Newfoundland
 (GMT - 03:00) Buenos Aires, Georgetown
 (GMT - 02:00) Mid-Atlantic
 (GMT - 01:00) Azores, Cape Verde Is.
(GMT) Greenwich Mean Time: Dublin, Lisbon, London
 (GMT + 01:00) Amsterdam, Copenhagen, Madrid, Paris
 (GMT + 02:00) Israel
 (GMT + 03:00) Moscow, St. Petersburg, Volgograd
 (GMT + 03:30) Tehran
 (GMT + 04:00) Abu Dhabi, Muscat
 (GMT + 04:30) Kabul
 (GMT + 05:00) Islamabad, Karachi, Tashkent
 (GMT + 05:30) Bombay, Calcutta, Madras, New Delhi
 (GMT + 06:00) Almaty, Dhaka
 (GMT + 07:00) Bangkok, Hanoi, Jakarta
 (GMT + 08:00) Beijing, Chongqing, Hong Kong
 (GMT + 09:00) Osaka, Sapporo, Tokyo
 (GMT + 09:30) Adelaide
 (GMT + 10:00) Guam, Port Moresby
 (GMT + 11:00) Magadan, Solomon Is., New Caledonia
 (GMT + 12:00) Auckland, Wellington
 (GMT) Greenwich Mean Time: Dublin, Lisbon, London

Figure 53. WMI: Time Zones

- 16. 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.



Use NTP: (IP Address)	☒	time.nist.gov
NTP 2: (IP Address)		129.6.15.29

Apply Save

NTP enabled

Figure 54. 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.
- 17.** Click on the **Apply** button to apply the new settings to this session
- 18.** Click on the **Save** button to save your changes (otherwise your new settings will not take effect).

This ends the Express Setup procedure.

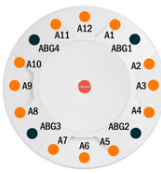
Network Interfaces

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 (underlined) in the **Interface** column to “jump” to the associated configuration page.

XS-3900 Wireless LAN Array



Array Status Express Set-Up Network Interfaces Network Settings Network Statistics DHCP Settings DNS Settings IAP Interfaces SSID Security Stations Services Array Info Tools Show Config Event Log	Array Controller Network Interfaces <table> <tr> <th>Interface</th> <th>Status</th> <th>DHCP</th> <th>IP Address</th> <th>Subnet Mask</th> <th>Gateway</th> </tr> <tr> <td><u>10/100 Megabit</u></td> <td>Enabled</td> <td>Enabled</td> <td>192.168.0.7</td> <td>255.255.255.0</td> <td>192.168.0.1</td> </tr> <tr> <td><u>Gigabit Interface 1</u></td> <td>Enabled</td> <td>Enabled</td> <td>10.0.1.2</td> <td>255.0.0.0</td> <td></td> </tr> <tr> <td><u>Gigabit Interface 2</u></td> <td>Enabled</td> <td>Enabled</td> <td>10.0.1.2</td> <td>255.0.0.0</td> <td></td> </tr> </table>	Interface	Status	DHCP	IP Address	Subnet Mask	Gateway	<u>10/100 Megabit</u>	Enabled	Enabled	192.168.0.7	255.255.255.0	192.168.0.1	<u>Gigabit Interface 1</u>	Enabled	Enabled	10.0.1.2	255.0.0.0		<u>Gigabit Interface 2</u>	Enabled	Enabled	10.0.1.2	255.0.0.0	
Interface	Status	DHCP	IP Address	Subnet Mask	Gateway																				
<u>10/100 Megabit</u>	Enabled	Enabled	192.168.0.7	255.255.255.0	192.168.0.1																				
<u>Gigabit Interface 1</u>	Enabled	Enabled	10.0.1.2	255.0.0.0																					
<u>Gigabit Interface 2</u>	Enabled	Enabled	10.0.1.2	255.0.0.0																					



Critical Msgs: 2

Warning Msgs: 0

General Msgs: 9

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2




Figure 55. 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 80.
- “Network Statistics” on page 84.
- “DHCP Settings” on page 85.
- “DNS Settings” on page 87.

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

Network Interface Settings	
10/100 Megabit Settings	
Enable Interface:	☒ Yes ☐ No
Allow Management On Interface:	☒ Yes ☐ No
Auto Negotiate:	☒ Yes ☐ No
Duplex:	☒ Full ☐ Half
Speed:	100 Megabit
MTU Size:	1500
Configuration Server Protocol:	☒ DHCP ☐ Static
IP Address:	192.168.0.7
IP Subnet Mask:	255.255.255.0
Default Gateway:	192.168.0.1
Gigabit Interface 1 Settings	
Enable Interface:	☒ Yes ☐ No
Allow Management On Interface:	☒ Yes ☐ No
Auto Negotiate:	☒ Yes ☐ No
Duplex:	☒ Full ☐ Half
Speed:	Gigabit
MTU Size:	1504
Configuration Server Protocol:	☒ DHCP ☐ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	
Gigabit Interface 2 Settings	
Enable Interface:	☒ Yes ☐ No
Allow Management On Interface:	☒ Yes ☐ No
Auto Negotiate:	☒ Yes ☐ No

more ...

Figure 56. WMI: Network Settings Page (Part 1)

... continued

Duplex:	☒ Full ☐ Half
Speed:	Gigabit
MTU Size:	1504
Configuration Server Protocol:	☒ DHCP ☐ Static
IP Address:	10.0.1.2
IP Subnet Mask:	255.0.0.0
Default Gateway:	

Apply Save

Location: Name: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 57. 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 Array.

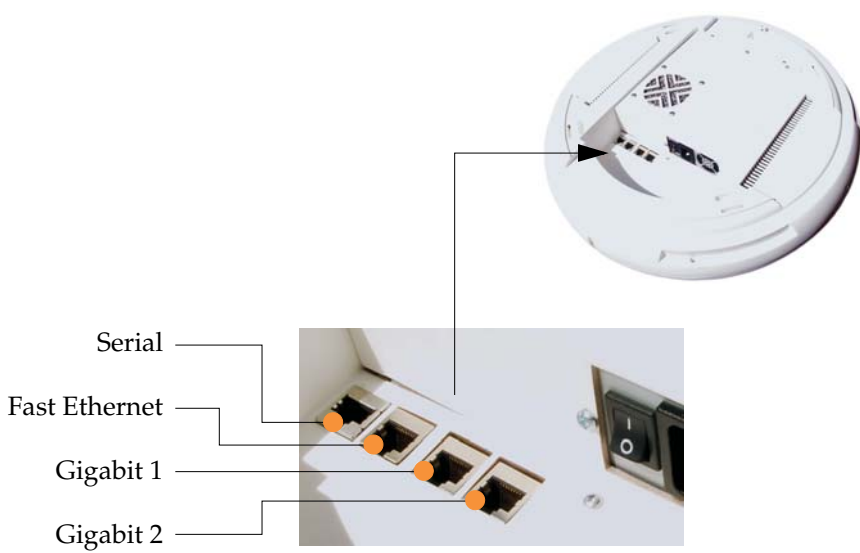


Figure 58. Network Interface Ports

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. **Enable Interface:** Choose **Yes** to enable this network interface (Fast Ethernet, Gigabit 1 or Gigabit 2), or choose **No** to disable the interface.
- b. **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.
- c. **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**.
- d. **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 1504 bytes.

- e. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** when assigning IP addresses to the Array, or choose **Static IP** if you intend to enter IP addresses manually.
 - **IP Address:** If you selected the Static IP option, enter a valid IP address for the Array. To use any of the remote connections (Web, **SNMP**, or SSH), a valid IP address must be established.
 - **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 Array 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 Array 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).

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.

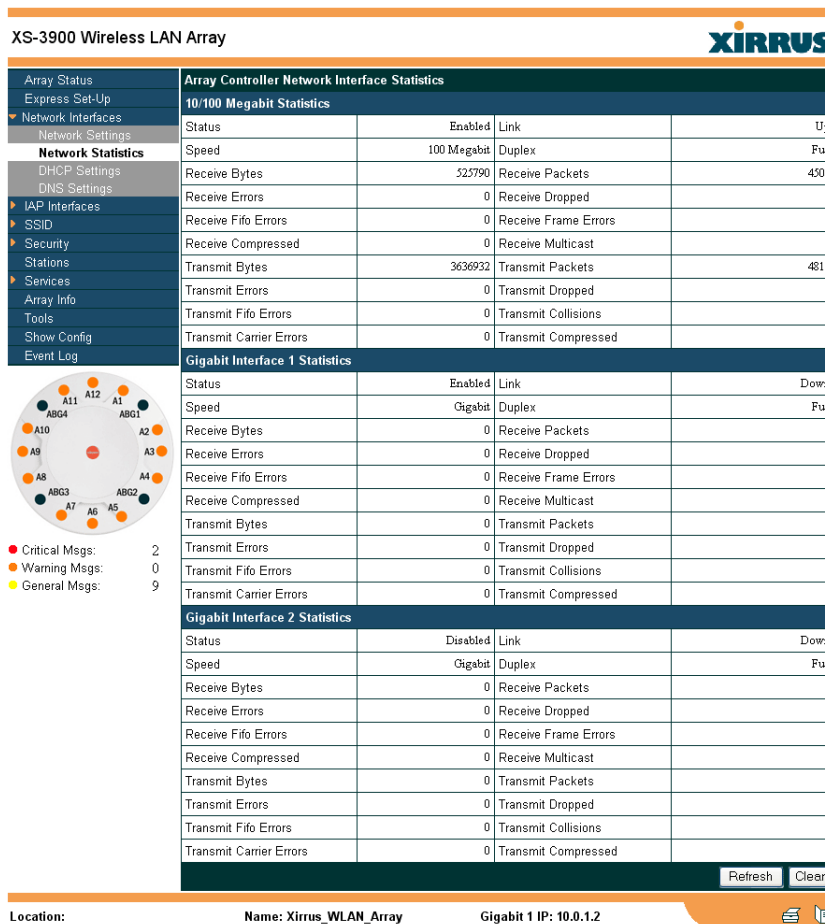


Figure 59. WMI: Network Statistics Page

DHCP 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

Array Status

Express Set-Up

Network Interfaces

Network Settings

Network Statistics

DHCP Settings

DNS Settings

IAP Interfaces

SSID

Security

Stations

Services

Array Info

Tools

Show Config

Event Log

DHCP Server	
Enable DHCP Server:	☒ Yes ☐ No
Default Lease (seconds):	300
Maximum Lease (seconds):	300
Starting IP Range:	192.168.1.100
End IP Range:	192.168.1.200

Apply

Save

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 60. 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. The default is 192.168.1.100.
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. The default is 192.168.1.200.
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 the Array 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.

XS-3900 Wireless LAN Array

Array Status

Express Set-Up

Network Interfaces

Network Settings

Network Statistics

DHCP Settings

DNS Settings

IAP Interfaces

SSID

Security

Stations

Services

Array Info

Tools

Show Config

Event Log

DNS Server

DNS Host Name:

Xirrus_WLAN_Array

DNS Domain:

DNS Server 1:

DNS Server 2:

DNS Server 3:

Apply

Save

A11

ABG4

A10

A9

A8

ABG3

A7

A6

A5

ABG2

A4

A3

A2

ABG1

A1

A12

Critical Msgs:

Warning Msgs:

General Msgs:

2

0

9

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 61. WMI: DNS Settings Page

Configuring the Xirrus Array

87

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.

XS-3900 Wireless LAN Array



Array Status	Integrated Access Point Interfaces				
Express Set-Up	IAP	Status	Channel	Cell Size	Associated Users
Network Interfaces	abg1	Enabled	1	Large	0
▼ IAP Interfaces	abg2	Enabled	6	Large	0
IAP Settings	abg3	Enabled	11	Large	0
Global Settings	abg4	Enabled	6	Large	0
Global Settings .11a	a1	Enabled	36	Large	0
Global Settings .11bg	a2	Enabled	52	Large	0
IAP LED Settings	a3	Enabled	149	Large	0
Statistics	a4	Enabled	40	Large	0
SSID	a5	Enabled	56	Large	0
Security	a6	Enabled	157	Large	0
Stations	a7	Enabled	44	Large	0
Services	a8	Enabled	60	Large	0
Array Info	a9	Enabled	153	Large	0
Tools	a10	Enabled	48	Large	0
Show Config	a11	Enabled	64	Large	0
Event Log	a12	Enabled	161	Large	0



● Critical Msgs: 2

● Warning Msgs: 0

● General Msgs: 9

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2




Figure 62. 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](#).

XS-3900 Wireless LAN Array

- Array Status
- Express Set-Up
- Network Interfaces
- IAP Interfaces
- IAP Settings**
 - Global Settings
 - Global Settings: 11a
 - Global Settings: 11bg
 - IAP LED Settings
 - Statistics
- SSID
- Security
- Stations
- Services
- Array Info
- Tools
- Show Config
- Event Log

Integrated Access Point Settings							
IAP	Enabled	Mode	Channel	Cell Size	Tx Power dB	Rx dB	Antenna Select
abg1	☒	.11b/g	1	Large	20	-95	Internal_2.4Ghz
abg2	☒	.11b/g	6	Large	20	-95	Internal_2.4Ghz
abg3	☒	.11b/g	11	Large	20	-95	Internal_2.4Ghz
abg4	☒	.11b/g	6	Large	20	-95	Internal_2.4Ghz
a1	☒	.11a	36	Large	20	-95	Internal_5Ghz
a2	☒	.11a	52	Large	20	-95	Internal_5Ghz
a3	☒	.11a	149	Large	20	-95	Internal_5Ghz
a4	☒	.11a	40	Large	20	-95	Internal_5Ghz
a5	☒	.11a	56	Large	20	-95	Internal_5Ghz
a6	☒	.11a	157	Large	20	-95	Internal_5Ghz
a7	☒	.11a	44	Large	20	-95	Internal_5Ghz
a8	☒	.11a	60	Large	20	-95	Internal_5Ghz
a9	☒	.11a	153	Large	20	-95	Internal_5Ghz
a10	☒	.11a	48	Large	20	-95	Internal_5Ghz
a11	☒	.11a	64	Large	20	-95	Internal_5Ghz
a12	☒	.11a	161	Large	20	-95	Internal_5Ghz

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 63. 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” on page 93.
- For all 802.11a radios, go to the “Global Settings .11a” on page 96.
- For all 802.11b/g radios, go to the “Global Settings .11bg” on page 99.

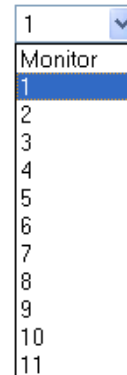
Procedure for Manually Configuring IAPs (Radios)

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 this pull-down 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.

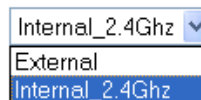
The number of users and their applications are major drivers of bandwidth requirements. The network architect must account for the number of users within the Array’s cell diameter.

In a large office, or if multiple Arrays are in use, 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 25.

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 (or no choices will be available), 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.

XS-3900 Wireless LAN Array

Array Status	Integrated Access Point Global Settings	
Express Set-Up		
Network Interfaces		
IAP Interfaces		
IAP Settings		
Global Settings		
Global Settings - 11a		
Global Settings - 11bg		
IAP LED Settings		
Statistics		
SSID		
Security		
Stations		
Services		
Array Info		
Tools		
Show Config		
Event Log		

● Critical Msgs: 2

● Warning Msgs: 0

● General Msgs: 9

Location:

Name: Xiruss WLAN Array

Gigabit 1 IP: 10.0.1.2

Figure 64. 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. **Auto Channel Configuration Mode:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP when the Array is powered up. Choose **On Array PowerUp** to enable this feature, or choose **Disabled** to disable this feature.
4. **Auto Configure on Time:** This option allows you to instruct the Array to auto-configure channel selection for each enabled IAP at a time you specify here (in hours and minutes, using the format: hh:mm). Leave this field blank unless you want to specify a time at which the auto-configuration utility is initiated.
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 Array 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. **Station Re-Authentication Period:** This option allows you to specify a time (in seconds) for the duration of station reauthentications.
10. **Station Timeout Period:** Specify a time (in seconds) in this field to define the timeout period for station associations.
11. **Max Station Association per IAP:** This option allows you to define how many station associations are allowed per IAP (up to 64 stations per IAP).
12. Click on the **Apply** button to apply the new settings to this session.
13. 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 defining which 802.11a data rates are supported, 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.

XS-3900 Wireless LAN Array

XIRRUS

Array Status

Express Set-Up

Network Interfaces

IAP Interfaces

IAP Settings

Global Settings

Global Settings .11a

Global Settings .11bg

IAP LED Settings

Statistics

SSID

Security

Stations

Services

Array Info

Tools

Show Config

Event Log

Integrated Access Point 802.11a Global Settings

802.11a Data Rates:

6.0	☒ Supported	☒ Basic
9.0	☒ Supported	☐ Basic
12.0	☒ Supported	☒ Basic
18.0	☒ Supported	☐ Basic
24.0	☒ Supported	☒ Basic
36.0	☒ Supported	☐ Basic
48.0	☒ Supported	☐ Basic
54.0	☒ Supported	☐ Basic

Optimize Data Rates:

Range

Throughput

802.11a IAP Status:

Disable 802.11a IAPs

Enable 802.11a IAPs

Channel Configuration:

Auto Configure

Fragmentation Threshold (256-2346):

2346

RTS Threshold (1-2347):

2347

Apply

Save

A11

A12

A1

ABG1

A2

A3

A4

ABG2

A5

A6

A7

ABG3

A8

A9

A10

ABG4

Critical Msgs: 3

Warning Msgs: 0

General Msgs: 9

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 65. WMI: Global Settings .11a Page

Procedure for Configuring Global 802.11a IAP Settings

1. **802.11a Data Rates:** The Array allows you to define which data rates are supported for all 802.11a radios.

6.0	☒ Supported	☒ Basic
9.0	☒ Supported	☐ Basic
12.0	☒ Supported	☒ Basic
18.0	☒ Supported	☐ Basic
24.0	☒ Supported	☒ Basic
36.0	☒ Supported	☐ Basic
48.0	☒ Supported	☐ Basic
54.0	☒ Supported	☐ Basic

Figure 66. Specifying 802.11a Data Rates

Select (or deselect) data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

- **Basic Rate**—a wireless station (client) must support this rate in order to associate.
 - **Supported Rate**—the Array will use this data rate for transmissions to clients.
2. **Optimize Data Rates:** The Xirrus Wireless LAN Array can optimize your 802.11a data rates automatically, based on range or throughput. Click on the **Range** button to optimize data rates based on range, or click on the **Throughput** button to optimize data rates based on throughput.
 3. **802.11a 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.
 4. **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.

5. **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. Smaller fragmentation numbers can help to “squeeze” packets through in noisy environments. 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).

Global Settings .11bg

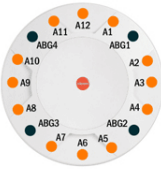
This page allows you to establish global 802.11b/g IAP (radio) settings. These settings include defining which 802.11b and 802.11g data rates are supported, enabling or disabling all 802.11b/g radios, auto-configuration of channel allocations for all 802.11b/g radios, and specifying the fragmentation and RTS thresholds for all 802.11b/g radios.

XS-3900 Wireless LAN Array

- Array Status
- Express Set-Up
- Network Interfaces
- ▼ IAP Interfaces
 - IAP Settings
 - Global Settings
 - Global Settings .11a
 - Global Settings .11bg**
 - IAP LED Settings
- Statistics
- SSID
- Security
- Stations
- Services
- Array Info
- Tools
- Show Config
- Event Log

XIRRUS

Integrated Access Point 802.11b/g Global Settings			
802.11g Data Rates:	6.0	☒ Supported	☐ Basic
	9.0	☒ Supported	☐ Basic
	12.0	☒ Supported	☐ Basic
	18.0	☒ Supported	☐ Basic
	24.0	☒ Supported	☐ Basic
	36.0	☒ Supported	☐ Basic
	48.0	☒ Supported	☐ Basic
	54.0	☒ Supported	☐ Basic
802.11b Data Rates:	1.0	☒ Supported	☒ Basic
	2.0	☒ Supported	☒ Basic
	5.5	☒ Supported	☒ Basic
	11.0	☒ Supported	☒ Basic
	Optimize Data Rates:		Range Throughput
802.11bg IAP Status:		Disable 802.11b/g IAPs Enable 802.11b/g IAPs	
Channel Configuration:		Auto Configure	
802.11g Only:		☐ On ☒ Off	
802.11g Protection:		☒ Auto ☐ Off	
802.11g Slot:		☐ Auto ☒ Short Only	
802.11b Preamble:		☒ Auto ☐ Long Only	
Fragmentation Threshold (256-2346):		2346	
RTS Threshold (1-2347):		2347	
		Apply Save	



● Critical Msgs: 3

● Warning Msgs: 0

● General Msgs: 9

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 67. WMI: Global Settings .11bg Page

Procedure for Configuring Global 802.11b/g IAP Settings

1. **802.11g Data Rates:** The Array allows you to define which data rates are supported for all 802.11g radios.

6.0	☒ Supported	☐ Basic
9.0	☒ Supported	☐ Basic
12.0	☒ Supported	☐ Basic
18.0	☒ Supported	☐ Basic
24.0	☒ Supported	☐ Basic
36.0	☒ Supported	☐ Basic
48.0	☒ Supported	☐ Basic
54.0	☒ Supported	☐ Basic

Figure 68. Specifying 802.11g Data Rates

Select (or deselect) data rates by clicking in the corresponding **Supported** and **Basic** data rate check boxes.

- **Basic Rate**—a wireless station (client) must support this rate in order to associate.
 - **Supported Rate**—the Array will use this data rate for transmissions to clients.
2. **802.11b Data Rates:** This task is similar to Step 1, but these data rates apply only to 802.11b radios.

1.0	☒ Supported	☒ Basic
2.0	☒ Supported	☒ Basic
5.5	☒ Supported	☒ Basic
11.0	☒ Supported	☒ Basic

Figure 69. Specifying 802.11b Data Rates

3. **Optimize Data Rates:** The Xirrus Wireless LAN Array can optimize your 802.11b/g data rates automatically, based on range or throughput. Click on the **Range** button to optimize data rates based on range, or click on the **Throughput** button to optimize data rates based on throughput.

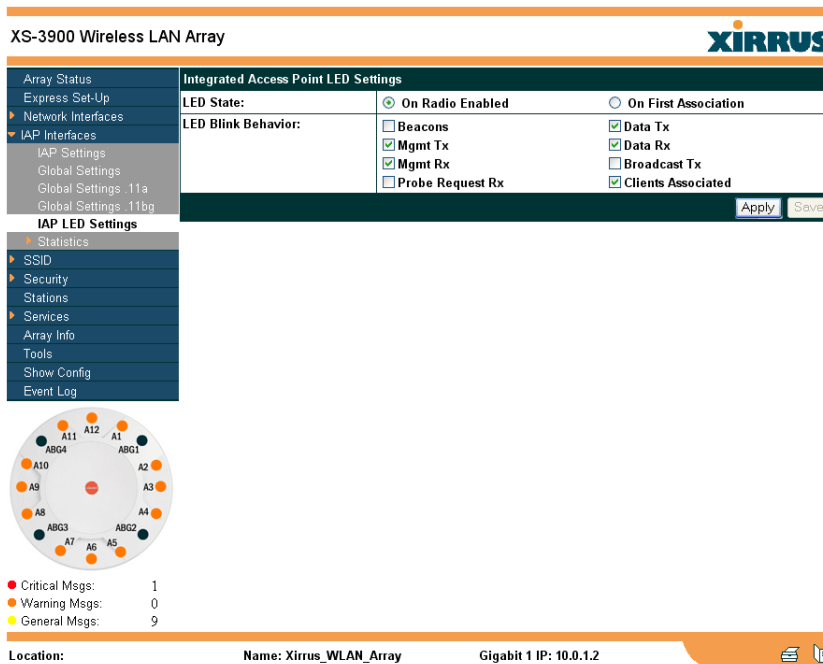
4. **802.11bg IAP Status:** Click on the **Enable 802.11b/g IAPs** button to enable all 802.11b/g radios for this Array, or click on the **Disable 802.11b/g IAPs** button to disable all 802.11b/g radios.
5. **Channel Configuration:** Click on the **Auto Configure** button to instruct the Array to determine 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.
6. **802.11g Only:** Select **On** if you want to restrict use to 802.11g mode only.. In this mode, no 802.11b rates are transmitted. Also, stations that only support 802.11b will not be able to associate.
7. **802.11g Protection:** Select **Auto** to provide automatic protection for all 802.11g radios.
8. **802.11g Slot:** Select **Auto** to instruct the Array to manage the 802.11g slot times automatically, or choose **Short Only**. Xirrus recommends using **Auto** for this settings, especially if 802.11b devices are present.
9. **802.11b Preamble:** The **preamble** contains information that the Array and client devices need when sending and receiving packets. All compliant 802.11b systems have to support the long preamble (a short preamble improves the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

Select **Auto** to instruct the Array to manage the preamble (long and short) automatically, or choose **Long Only**.
10. **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).

11. **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.
12. Click on the **Apply** button to apply the new settings to this session.
13. 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 the assignment of behavior preferences.



XS-3900 Wireless LAN Array

Integrated Access Point LED Settings

LED State:	☒ 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

Apply Save

IAP LED Settings

Statistics

SSID

Security

Stations

Services

Array Info

Tools

Show Config

Event Log



● Critical Msgs: 1
 ● Warning Msgs: 0
 ● General Msgs: 9

Location: Name: Xirrus_WLAN_Array Gigabit 1 IP: 10.0.1.2

Figure 70. WMI: IAP LED Settings Page

Procedure for Configuring the IAP LEDs

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

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.

XS-3900 Wireless LAN Array

Integrated Access Point Statistics Overview				
Array Status				
Express Set-Up				
Network Interfaces				
IAP Interfaces				
IAP Settings				
Global Settings				
Global Settings - 11a				
Global Settings - 11bg				
IAP LED Settings				
Statistics				
Statistics IAP abg1				
Statistics IAP abg2				
Statistics IAP abg3				
Statistics IAP abg4				
Statistics IAP a1				
Statistics IAP a2				
Statistics IAP a3				
Statistics IAP a4				
Statistics IAP a5				
Statistics IAP a6				
Statistics IAP a7				
Statistics IAP a8				
Statistics IAP a9				
Statistics IAP a10				
Statistics IAP a11				
Statistics IAP a12				
SSID				
Security				
Stations				
Services				
Array Info				
Tools				
Show Config				
Event Log				
	abg1	Rx Packets	0 Rx Errors	10551303
		Tx Packets	20630 Tx Errors	0
	abg2	Rx Packets	0 Rx Errors	7602327
		Tx Packets	20628 Tx Errors	0
	abg3	Rx Packets	88756 Rx Errors	12976188
		Tx Packets	20766 Tx Errors	0
	abg4	Rx Packets	103 Rx Errors	15466789
		Tx Packets	20636 Tx Errors	0
	a1	Rx Packets	0 Rx Errors	30867533
		Tx Packets	20533 Tx Errors	0
	a2	Rx Packets	0 Rx Errors	28246043
		Tx Packets	20532 Tx Errors	0
	a3	Rx Packets	0 Rx Errors	14090245
		Tx Packets	20532 Tx Errors	0
	a4	Rx Packets	0 Rx Errors	30867544
		Tx Packets	20525 Tx Errors	0
	a5	Rx Packets	0 Rx Errors	29753383
		Tx Packets	20524 Tx Errors	0
	a6	Rx Packets	0 Rx Errors	27721741
		Tx Packets	20524 Tx Errors	0
	a7	Rx Packets	0 Rx Errors	28573830
		Tx Packets	20521 Tx Errors	0
	a8	Rx Packets	0 Rx Errors	27394060
		Tx Packets	20672 Tx Errors	0
	a9	Rx Packets	0 Rx Errors	28966946
		Tx Packets	20671 Tx Errors	0
	a10	Rx Packets	0 Rx Errors	30998572
		Tx Packets	20667 Tx Errors	0
	a11	Rx Packets	0 Rx Errors	15269889
		Tx Packets	20664 Tx Errors	0
	a12	Rx Packets	0 Rx Errors	17694732
		Tx Packets	20681 Tx Errors	3

● Critical Msgs: 3

● Warning Msgs: 0

● General Msgs: 9

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2

Figure 71. 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 from the XS-3700 product of the **Statistics IAP a4** page (for the a4 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.

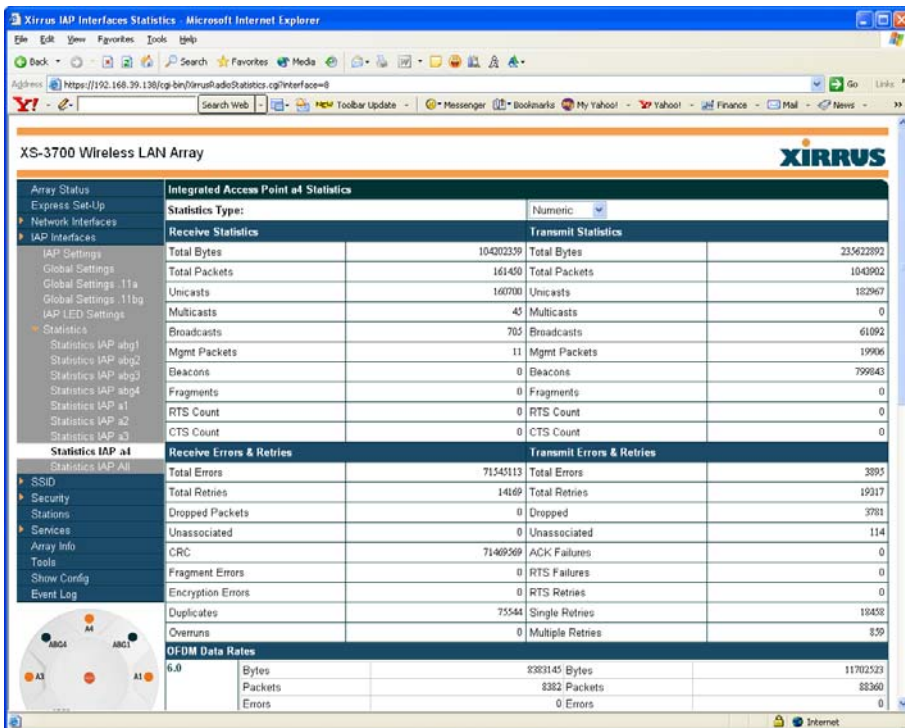


Figure 72. WMI: Statistics for IAP a4 Page (XS-3700)

Statistics (for all radios)

This page provides a detailed statistical summary of the performance of all radios, displayed either numerically or by percentage (your choice). The following image shows an example from the XS-3700 product.

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.

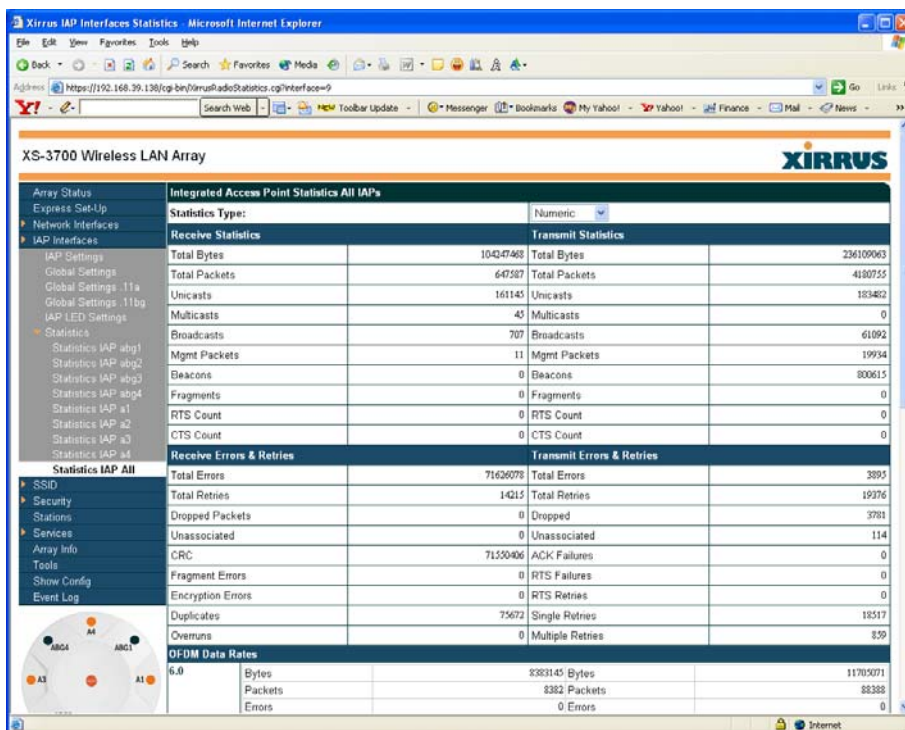


Figure 73. WMI: Statistics for All IAPs Page (XS-3700)

SSID

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 222](#).

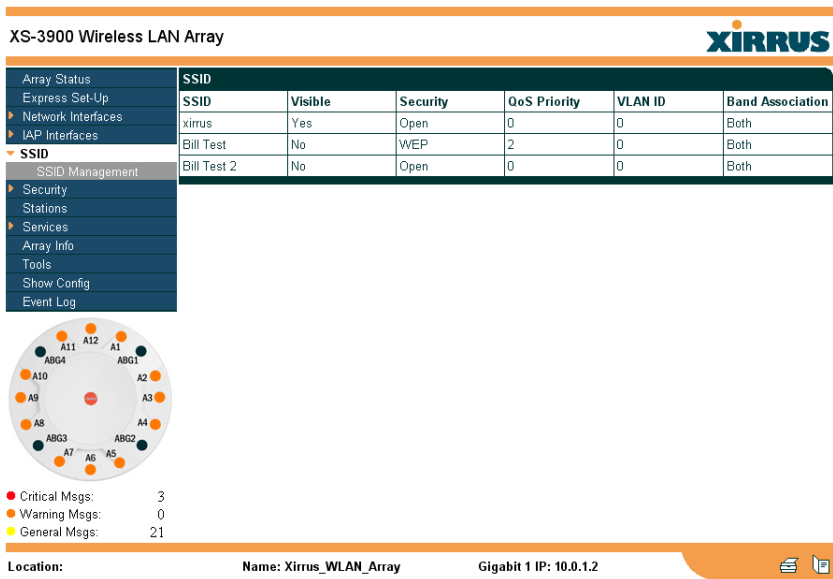


Figure 74. WMI: SSID Page

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:

- The wireless security mode needed 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.

SSID Management

This page allows you to manage SSIDs (create, edit and delete), 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.

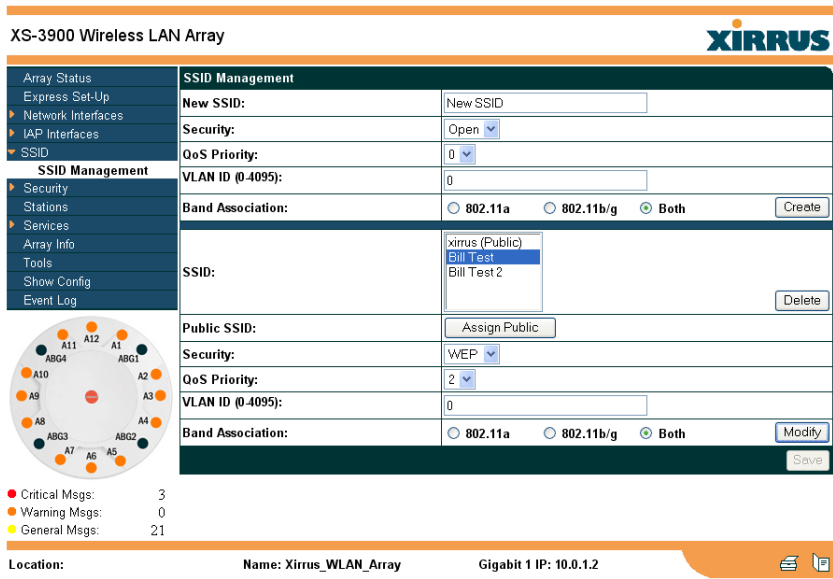
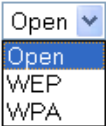


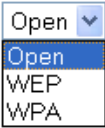
Figure 75. WMI: SSID Management Page

Procedure for Managing 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 35](#).
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. **Band Association:** The Array allows you to choose which wireless band the SSID will be beacons on. Select either **802.11a**, **802.11b/g** or **Both**.
6. Click on the **Create** button to create this SSID. The SSID you just created will appear in the SSID List below.

Editing SSIDs

7. **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.
8. **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.

9. **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 35.
- 
10. **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.
 11. **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.
 12. **Band Association:** The Array allows you to choose which wireless band to associate with each SSID. Select either **802.11a**, **802.11b/g** or **Both**.
 13. Click on the **Modify** button to edit the selected SSID.
 14. 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 35.
- The Security section of “Frequently Asked Questions” on page 222.

XS-3900 Wireless LAN Array

- Array Status
- Express Set-Up
- Network Interfaces
- WAP Interfaces
- SSID
- Security**
 - Security Management
 - Radius Server
 - Radius User
 - MAC Access List
 - Admin Management
 - Rogue AP List
- Stations
- Services
- Array Info
- Tools
- Show Config
- Event Log

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	No
Radius In Use	External Radius IP	External Radius Port	Internal Radius Users
External	0.0.0.0	1812	0



● Critical Msgs: 3

● Warning Msgs: 0

● General Msgs: 21

Location:

Name: Xirrus_WLAN_Array

Gigabit 1 IP: 10.0.1.2




Figure 76. WMI: Security Page

Security Management

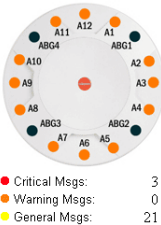
This page allows you to establish the security parameters for your wireless network, including WEP, WPA and RADIUS authentication. When finished, click on the **Apply** button to apply the new settings to this session, then click on the **Save** button to save your changes.

For additional information about wireless network security, refer to “Security Planning” on page 35.

XS-3900 Wireless LAN Array


- Array Status
- Express Set-Up
- Network Interfaces
- IAP Interfaces
- SSID
- Security
- Security Management**
- Radius Server
- Radius User
- MAC Access List
- Admin Management
- Rogue AP List
- Stations
- Services
- Array Info
- Tools
- Show Config
- Event Log

Security Management	
WPA Enabled:	☐ Yes ☒ No
TKIP Enabled:	☐ Yes ☒ No
AES Enabled:	☐ Yes ☒ No
WPA Group Rekey Time (seconds):	1000000000
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:
Name: Xirrus_WLAN_Array
Gigabit 1 IP: 10.0.1.2

Figure 77. 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 Xirrus Wireless LAN 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 Array allows you to establish the following data encryption configuration options:
 - **Open**—this option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTY.
 - **WEP (Wired Equivalent Privacy)**—this option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.

- **WPA (Wi-Fi Protected Access)**—this is a much stronger encryption mode than WEP and uses TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption Standard) to encrypt data.

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

AES is the strongest encryption standard and is used by government agencies; however, old legacy hardware may not be capable of supporting the AES mode (it probably won't work on older wireless clients). Because AES is the strongest encryption standard currently available, 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 Array allows you to choose between the following user authentication methods:

- **Pre-Shared Key**—users must manually enter a key (passphrase) on the client side of the wireless network that matches the key stored by the administrator in the Array.

This method should be used only for smaller networks when a RADIUS server is unavailable. If PSK must be used, choose a strong passphrase containing between 8 and 63 characters (20 is preferred). Always use a combination of letters, numbers and special characters. Never use English words separated by spaces.

- **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS 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 Xirrus Wireless LAN Array 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 10 hex or 26 hex characters), then re-enter the key to verify that you typed it correctly—hexadecimal characters are defined as ABCDEF and 0-9.
 - 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.



After configuring network security, the configuration must be applied to an SSID for the new functionality to 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	
Express Set-Up	RADIUS Server Mode: ☐ Internal ☒ External
Network Interfaces	External RADIUS
IAP Interfaces	Primary IP Address: 0.0.0.0
SSID	Primary Port Number: 1812
Security	Secondary IP Address:
Security Management	Secondary Port Number: 1812
Radius Server	Timeout (seconds): 600
Radius User	Primary Shared Secret / Verify Secret: ***** *****
MAC Access List	Secondary Shared Secret / Verify Secret:
Admin Management	Apply Save
Rogue AP List	
Stations	
Services	
Array Info	
Tools	
Show Config	
Event Log	

● Critical Msgs: 3

● Warning Msgs: 0

● General Msgs: 21

Location:
Name: Xirrus_WLAN_Array
Gigabit 1 IP: 10.0.1.2

Figure 78. WMI: Radius Server Page