

## Configuring the Wireless Array

The following topics include procedures for configuring the Array using the product's embedded Web Management Interface (WMI). Procedures have been organized into functional areas that reflect the flow and content of the WMI.

The following WMI windows allow you to establish configuration parameters for your Array, and include:

- "Express Setup" on page 161
- "Network" on page 169
- "Services" on page 184
- "VLANs" on page 199
- "Tunnels" on page 204
- "Security" on page 208
- "SSIDs" on page 242
- "Groups" on page 264
- "IAPs" on page 271
- "WDS" on page 338
- "Filters" on page 344
- "Clusters" on page 352

After making changes to the configuration settings of an Array you must click on the **Save changes to flash** button at the top of the configuration window, otherwise the changes you make will not be applied the next time the Array is rebooted.



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

Note that the **Configuration** menu section may be collapsed down to hide the headings under it by clicking it. Click again to display the headings. (See Figure 43 on page 89.)

This chapter only discusses using the configuration windows on the Array. To view status or use system tools on the Array, please see:

- [“Viewing Status on the Wireless Array” on page 95](#)
- [“Using Tools on the Wireless Array” on page 359](#)

## Express Setup

Use the Express Setup page to establish global configuration settings that enable basic Array functionality. Any changes you make in this window will affect all radios.



Figure 96. WMI: Express Setup

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

*Procedure for Performing an Express Setup*

1. **Host Name:** Specify a unique **host name** for this Array. The host name is used to identify the Array on the network. Use a name that will be meaningful within your network environment, up to 64 alphanumeric characters. The default is the Array's serial number.
2. **Location Information:** Enter a brief but meaningful description that accurately defines the physical location of the Array. In an environment where multiple units are installed, clear definitions for their locations are important if you want to identify a specific unit.
3. **Admin Contact:** Enter the name and contact information of the person who is responsible for administering the Array at the designated location.
4. **Admin Email:** Enter the email address of the admin contact you entered in Step 3.
5. **Admin Phone:** Enter the telephone number of the admin contact you entered in Step 3.
6. **License Key:** If Xirrus issued you a license that differs from the current value shown, enter it now.
7. **Configure SNMPv2:** Select whether to **Enable SNMPv2** on the Array, and set the SNMPv2 community strings. The factory default value for the **Read-Only Community String** is `xirrus_read_only`. The factory default value for the **Read-Write Community String** is `xirrus`. If you are using the Xirrus Management System (XMS), the read-write string must match the string used by XMS. XMS also uses the default value `xirrus`.
8. **Configure the Gigabit Ethernet network interface settings.** Please see ["Network Interfaces"](#) on page 171 for more information. For XN Arrays, configure the **10/100 Ethernet 0** (10/100 Mb) port as well.

The fields for each of these interfaces are similar, 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 Gigabit interface, or choose **No** to deny all management privileges for this interface. Note that for XN Arrays, the 10/100 Ethernet port is also known as the Management Port, and management is **always** enabled on this port.
- c. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** to assign IP addresses to the Array's Ethernet interfaces, or choose **Static** if you intend to enter IP addresses manually. If you choose the **Static IP** option, you must enter the following **IP Settings**:
  - **Address:** Enter a valid IP address for this Array. To use a remote connection (Web, **SNMP**, or **SSH**), a valid IP address must be used.
  - **Subnet Mask:** Enter a valid IP address for the **subnet mask** (the default is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
  - **Default Gateway:** Enter a valid IP address for the **default gateway**. This is the IP address of the router that the Array uses to forward data to other networks.
  - Click the **Apply** button for this interface when done making IP changes.
9. **SSID Settings:** This section specifies the wireless network name and security settings.
  - a. The **SSID (Wireless Network Name)** is a unique name that identifies a wireless network (SSID stands for Service Set Identifier). All devices attempting to connect to a specific WLAN must use the same SSID. The default SSID is **xirrus**. Entering a value in this field will replace the default SSID with the new name.

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

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

- **Open**—This option offers no data encryption and is not recommended, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTY.
- **WEP (Wired Equivalent Privacy)**—An optional IEEE 802.11 function that offers frame transmission privacy similar to a wired network. WEP generates secret shared encryption keys that both source and destination stations can use to alter frame bits to avoid disclosure to eavesdroppers.
- **WPA (Wi-Fi Protected Access)**—A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP or AES as an encryption method and 802.1x for authentication. WPA is the stronger of the two wireless security schemes.
- **WPA2 (Wi-Fi Protected Access 2)**—WPA2 is the follow-on security method to WPA for wireless networks and provides stronger data protection and network access control. It offers Enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Like WPA, WPA2 is designed to secure all versions of 802.11 devices, including 802.11a, 802.11b, 802.11g, and 802.11n, multi-band and multi-mode.
- **WPA-Both (WPA and WPA2)**—This option makes use of both WPA and WPA2.

For more information about security, including a full review of all security options and settings, go to [“Understanding Security”](#) on page 209.

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



- b. **Time Zone:** Select your time zone from the choices available in the pull-down list.
- c. **Auto Adjust Daylight Savings:** If you are not using NTP, check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
- d. **Use Network Time Protocol:** Check this box if you want to use an NTP server to synchronize the Array's clock. Use of NTP is mandatory for Arrays to be managed with XMS (the Xirrus Management System), and ensures that Syslog time-stamping is maintained across all units. Without using an NTP server (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies. If you select **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, select **No** (default) and set the system time on the Array manually.
- e. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
- f. **NTP Primary Authentication:** (optional) If you are using authentication with NTP, select the type of key: **MD5** or **SHA1**. Select **None** if you are not using authentication (this is the default). For more information on authenticated NTP, see "Time Settings (NTP)" on page 185.
- g. **NTP Primary Authentication Key ID:** Enter the key ID, which is a decimal integer.
- h. **NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- i. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.



- j. **Adjust Time (hrs:min:sec):** If you are not using NTP, check this box if you want to adjust the current system time. When the box is checked, the time fields become active. Enter the revised time (hours, minutes, seconds, am/pm) in the corresponding fields. If you don't want to adjust the current time, this box should be left unchecked (default).
  - k. **Adjust Date (month/day/year):** If you are not using NTP, check this box if you want to adjust the current system date. When the box is checked, the date fields become active. Enter the revised date (month, day and year) in the corresponding fields. If you don't want to adjust the current date, this box should be left unchecked (default).
12. **Quick Configuration:** This offers predefined configuration options such as **Classroom** and **High-Density** that capture best practices from years of field experience. If one of the options in the drop-down list is appropriate to your deployment, select it and click **Apply**. For example, the **High-Density** option uses best practices to configure the Array for high density settings such as lecture halls, convention centers, stadiums, etc.
13. **IAP Settings:**

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



Figure 97. LEDs are Switched On.

14. Click **Save changes to flash** at the upper right to make your changes permanent, i.e., these settings will still be in effect after a reboot.



## Network

This is a status-only window that provides a snapshot of the configuration settings currently established for the Ethernet interfaces. [DNS Settings](#) and [CDP Settings](#) (Cisco Discovery Protocol) are summarized as well. You must go to the appropriate configuration window to make changes to any of the settings displayed here (configuration changes cannot be made from this window). You can click on any item in the **Interface** column to “jump” to the associated configuration window.



| Name          | Type | Mode | L2 | L3 | L4 | L5 | L6 | L7 | L8 | L9 | L10 | L11 | L12 | L13 | L14 | L15 | L16 | L17 | L18 | L19 | L20 | L21 | L22 | L23 | L24 | L25 | L26 | L27 | L28 | L29 | L30 | L31 | L32 | L33 | L34 | L35 | L36 | L37 | L38 | L39 | L40 | L41 | L42 | L43 | L44 | L45 | L46 | L47 | L48 | L49 | L50 | L51 | L52 | L53 | L54 | L55 | L56 | L57 | L58 | L59 | L60 | L61 | L62 | L63 | L64 | L65 | L66 | L67 | L68 | L69 | L70 | L71 | L72 | L73 | L74 | L75 | L76 | L77 | L78 | L79 | L80 | L81 | L82 | L83 | L84 | L85 | L86 | L87 | L88 | L89 | L90 | L91 | L92 | L93 | L94 | L95 | L96 | L97 | L98 | L99 | L100 |
|---------------|------|------|----|----|----|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|
| Spanning Tree |      |      |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |      |
| DHCP          |      |      |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |      |
| CDP           |      |      |    |    |    |    |    |    |    |    |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |     |      |

Figure 98. Network Interfaces

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

- [“Network Interfaces” on page 171](#)
- [“Network Bonds” on page 175](#)
- [“DNS Settings” on page 181](#)
- [“CDP Settings” on page 183](#)

### See Also

[DNS Settings](#)

[Network Interfaces](#)


[Network Status Windows](#)

Spanning Tree Status  
Network Statistics



### Network Interfaces

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



|                       |                       |             |             |
|-----------------------|-----------------------|-------------|-------------|
| XR-500                | Configured Status     |             |             |
| Name                  | Interface             | Yes         | Yes         |
| IP Address            | IP Address            | 192.168.1.1 | 192.168.1.1 |
| Management Category   | Management Category   | Yes         | Yes         |
| All Enabled           | All Enabled           | Yes         | Yes         |
| All System            | All System            | Yes         | Yes         |
| Access Threshold (PT) | Access Threshold (PT) | 100         |             |
| Speed                 | Speed                 | 1000        |             |
| Configuration Level   | Configuration Level   | Yes         | Yes         |
| Password              | Password              | admin       | admin       |
| P-Setting             | P-Setting             | 100         |             |
| XR-1000               | Configured Status     |             |             |
| Name                  | Interface             | Yes         | Yes         |
| IP Address            | IP Address            | 192.168.1.1 | 192.168.1.1 |
| Management Category   | Management Category   | Yes         | Yes         |
| All Enabled           | All Enabled           | Yes         | Yes         |
| All System            | All System            | Yes         | Yes         |
| Access Threshold (PT) | Access Threshold (PT) | 100         |             |
| Speed                 | Speed                 | 1000        |             |
| Configuration Level   | Configuration Level   | Yes         | Yes         |
| Password              | Password              | admin       | admin       |
| P-Setting             | P-Setting             | 100         |             |
| XR-2000               | Configured Status     |             |             |
| Name                  | Interface             | Yes         | Yes         |
| IP Address            | IP Address            | 192.168.1.1 | 192.168.1.1 |
| Management Category   | Management Category   | Yes         | Yes         |
| All Enabled           | All Enabled           | Yes         | Yes         |
| All System            | All System            | Yes         | Yes         |
| Access Threshold (PT) | Access Threshold (PT) | 100         |             |
| Speed                 | Speed                 | 1000        |             |
| Configuration Level   | Configuration Level   | Yes         | Yes         |
| Password              | Password              | admin       | admin       |
| P-Setting             | P-Setting             | 100         |             |
| XR-4000               | Configured Status     |             |             |
| Name                  | Interface             | Yes         | Yes         |
| IP Address            | IP Address            | 192.168.1.1 | 192.168.1.1 |
| Management Category   | Management Category   | Yes         | Yes         |
| All Enabled           | All Enabled           | Yes         | Yes         |
| All System            | All System            | Yes         | Yes         |
| Access Threshold (PT) | Access Threshold (PT) | 100         |             |
| Speed                 | Speed                 | 1000        |             |
| Configuration Level   | Configuration Level   | Yes         | Yes         |
| Password              | Password              | admin       | admin       |
| P-Setting             | P-Setting             | 100         |             |
| XR-6000               | Configured Status     |             |             |
| Name                  | Interface             | Yes         | Yes         |
| IP Address            | IP Address            | 192.168.1.1 | 192.168.1.1 |
| Management Category   | Management Category   | Yes         | Yes         |
| All Enabled           | All Enabled           | Yes         | Yes         |
| All System            | All System            | Yes         | Yes         |
| Access Threshold (PT) | Access Threshold (PT) | 100         |             |
| Speed                 | Speed                 | 1000        |             |
| Configuration Level   | Configuration Level   | Yes         | Yes         |
| Password              | Password              | admin       | admin       |
| P-Setting             | P-Setting             | 100         |             |

Figure 99. Network Settings

On XN Series Arrays, this window configures the 10/100 Fast Ethernet interface and the Gigabit 1 and Gigabit2 interfaces

When finished making changes, click **Save changes to flash** if you wish to make your changes permanent. When the status of a port changes, a Syslog entry is created describing the change.

### Network Interface Ports

The following diagram shows the location of network interface ports on the underside of an XR Series Array.

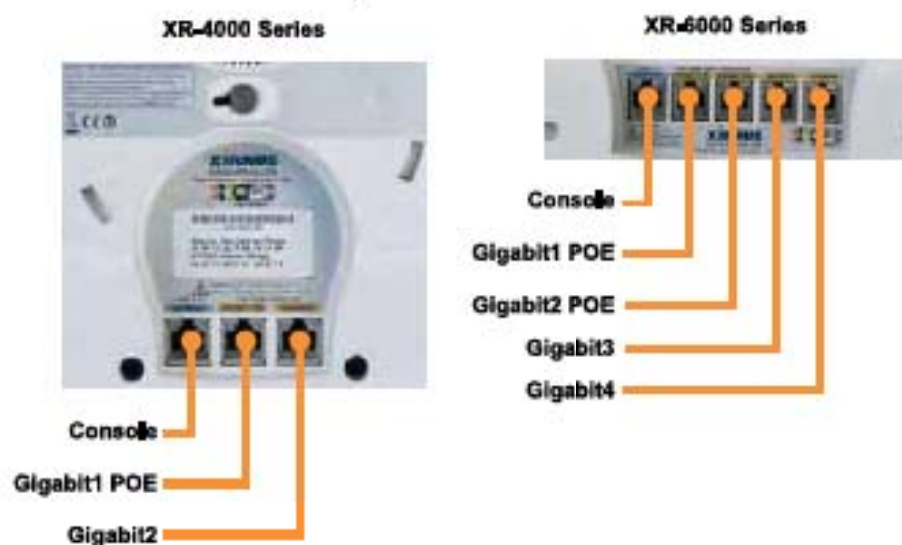


Figure 100. Network Interface Ports

### Procedure for Configuring the Network Interfaces

Configure the Gigabit network interfaces (for XN Arrays, configure the Fast Ethernet port as well). The fields for each of these interfaces are the same, and include:

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

2. **LED Indicator:** Choose **Enabled** to allow the LED for this interface to blink with traffic on the port, or choose **Disabled** to turn the LED off. The LED will still light during the boot sequence, then turn off. This option is only available for the Gigabit interfaces.
3. **Allow Management on Interface:** Choose **Yes** to allow management of this Array via the selected network interface, or choose **No** to deny all management privileges for this interface. For XN Arrays, this option is only available for the Gigabit interfaces—management is always enabled on the 10/100 interface (sometimes called the Management Port).
4. **Auto Negotiate:** This feature allows the Array to negotiate the best transmission rates automatically. Choose **Yes** to enable this feature, or choose **No** to disable this feature—the default is enabled. If you disable the Auto Negotiate feature, you must define the Duplex and Speed options manually (otherwise these options are not available). Both sides of the link **must** have the same values for the following settings, or the connection will have errors.
  - a. **Duplex:** Full-duplex mode transmits data in two directions simultaneously (for example, a telephone is a full-duplex device because both parties can talk and be heard at the same time). Half-duplex allows data transmission in one direction at a time only (for example, a walkie-talkie is a half-duplex device). If the Auto-Negotiate feature is disabled, you can manually choose **Half** or **Full** duplex for your data transmission preference.
  - b. **MTU:** the Maximum Transmission Unit size. This is the largest packet size (in bytes) that the interface can pass along.
  - c. **Speed:** If the Auto-Negotiate feature is disabled, you must manually choose the desired data transmission speed from the pull-down list. For XN Arrays, when configuring the Fast Ethernet interface the options are **10 Megabit** or **100 Megabit**. For configuring the Gigabit interfaces the options are **10 Megabit** or **100 Megabit**. (Note that 1000 Megabit speed can only be set by Auto-Negotiation.)

5. **Configuration Server Protocol / IP Settings:** Choose **DHCP** to instruct the Array to use **DHCP** when assigning IP addresses to the Array, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.
  - a. **Address:** If you selected the Static IP option, enter a valid IP address for the Array. To use any of the remote connections (Web, **SNMP**, or **SSH**), a valid IP address must be established.
  - b. **Subnet Mask:** If you selected the Static IP option, enter a valid IP address for the **subnet mask** (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
  - c. **Default Gateway:** If you selected the Static IP option, enter a valid IP address for the **default gateway**. This is the IP address of the router that the Array uses to send data to other networks. (You don't need to enter the gateway if it is on the same subnet as the Array.)
  - d. Click the **Apply** button for this interface when done making IP changes.
6. **Static Route (IP Address/Mask):** (For XN Arrays, Fast Ethernet port only) The 10-100 Ethernet Port may be used for managing the Array out of band from the Gigabit Ethernet ports. The 10-100 port will route only management traffic, using a static route that may be configured using this field.
7. When done configuring all interfaces as desired, click **Save changes to flash** if you wish to make your changes permanent.

*See Also*

[Network Bonds](#)

[DNS Settings](#)

[Network](#)

[Network Statistics](#)

[Spanning Tree Status](#)







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

#### **Procedure for Configuring Network Bonds**

Configure the bonding behavior of the Gigabit network interfaces. The fields for each of these bonds are the same, and include:

1. **Bond Mode:** Select the desired behavior for a set of bonded Gigabit Ethernet ports from the following options.

The modes below describe the relationship between a set of Gigabit ports—for example, load balancing or active backup. Use the **Bond Ports** field to select the ports that are bonded (set in [Step 2](#)). Two or more ports may be bonded. You may also include just one single port in a bond—this is useful for mirroring one Gigabit port to another port ([Step 5 on page 180](#)). In Arrays that have four Gigabit ports, you have the option of bonding three or four ports together. In this discussion, we call two ports that are bonded **Gigx** and **Gigy**.

- a. **Active Backup (gig ports fail over to each other)**—This mode provides fault tolerance and is the default mode. **Gigx** acts as the primary link. **Gigy** is the backup link and is passive. **Gigy** assumes the IP properties of **Gigx**. If **Gigx** fails, the Array automatically fails over to **Gigy**. When a failover occurs in this mode, **Gigy** issues gratuitous ARPs to allow it to substitute for **Gigx** at Layer 3 as well as Layer 2. See [Figure 102 \(a\)](#). You may include more than two ports in the bond with Active Backup to provide additional fault tolerance. For example, if you have three Gigabit ports configured in a bond, if the first two ports in the bond were to go down, the Array would fail over traffic to the third Gigabit port.

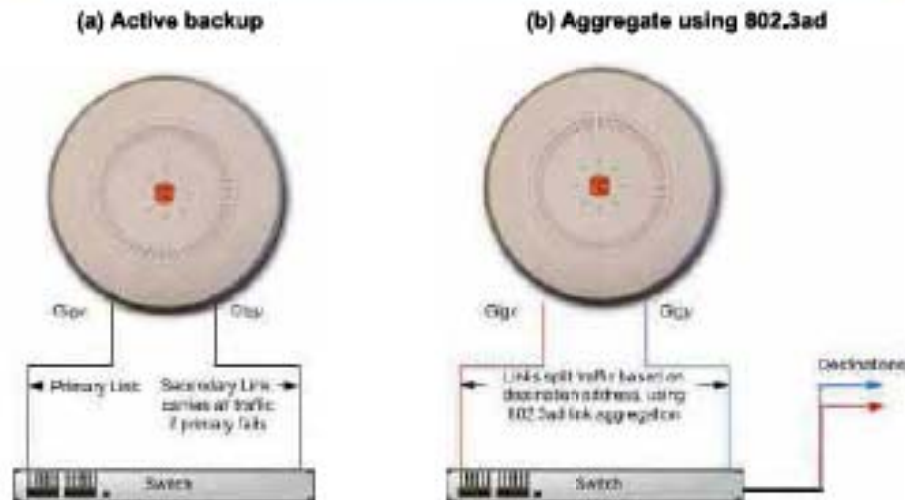


Figure 102. Port Modes (a, b)

- b. Aggregate Traffic from gig ports using 802.3ad**—The Array sends network traffic across all member Gigabit ports to increase link speed to the network. These ports act as a single logical interface, using a load balancing algorithm to balance traffic across the ports. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. If the packet is a fragment or not TCP or UDP, the source and destination IP addresses are used to do the calculation. If the packet is TCP or UDP over IP then the source IP address, destination IP address, source port number and destination port number are all used to do the calculation. The network switch must also support 802.3ad. If a port fails, the connection degrades gracefully—the other port still transmits. See [Figure 102 \(b\)](#).
- c. Transmit Traffic on all gig ports**—Transmits incoming traffic on all Gigabit ports. Any traffic received on Gigabit ports is sent to the onboard processor. This mode provides fault tolerance. See [Figure 103 \(c\)](#).

**(c) Transmit on all ports**

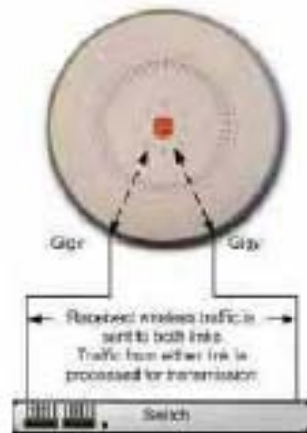


Figure 103. Port Modes (c)

**(d) Load balance traffic**

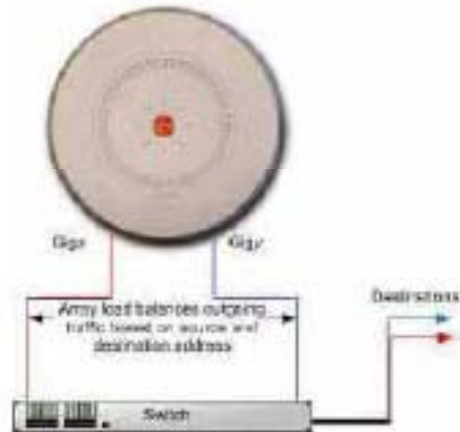


Figure 104. Port Modes (d)



Active VLANs list. If you create new VLANs, they will not be passed unless you take action to add them to the list.

5. **Mirror**—Specify one of the active bonds (Bondx) that is to be mirrored by this bond (Bondy). (Figure 105) All wireless traffic received on the Array is transmitted out both Bondx and Bondy. All traffic received on Bondx is passed on to the onboard processor as well as out Bondy. All traffic received on Bondy is passed on to the onboard processor as well as out Bondx. This allows a network analyzer to be plugged into Bondy to capture traffic for troubleshooting, while the bonded ports provide network connectivity for data traffic.

Mirroring is also used to duplicate the traffic from one bond to another bond—traffic received on Bondx is transmitted by Bondy; similarly, traffic received on Bondy is transmitted by Bondx. This allows the Array to act as a wired bridge and allows Arrays to be daisy-chained and still maintain wired connectivity.

If each bond contains just one port as is the case for XN Arrays, then you have the simple case of one port mirroring another.

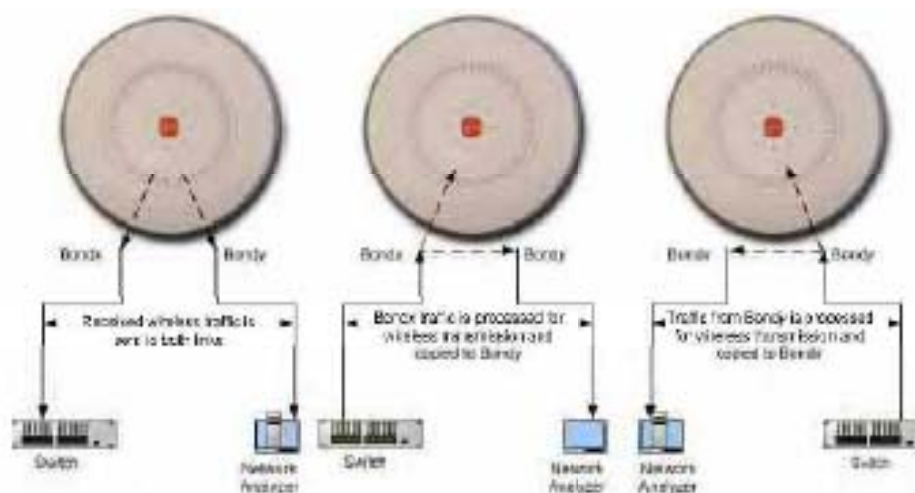


Figure 105. Mirroring Traffic

- When done configuring bonds as desired, click **Save changes to flash** if you wish to make your changes permanent.

### See Also

[Network Interfaces](#)  
[DNS Settings](#)  
[Network](#)  
[Network Statistics](#)  
[Spanning Tree Status](#)

### DNS Settings

This window allows you to establish your **DNS** (Domain Name System) settings. The Array uses these DNS servers to resolve host names into IP addresses. The Array also registers its own Host Name with these DNS servers, so that others may address the Array using its name rather than its IP address. An option allows you to specify that the Array's DNS servers will be assigned via a DHCP server on the wired network.

Note that the DNS servers defined here are not used by wireless clients—servers for stations associated to the Array are defined along with DHCP pools. See “[DHCP Server](#)” on page 197. At least one DNS server must be set up if you want to offer clients associating with the Array the ability to use meaningful host names instead of numerical IP addresses. When finished, click **Save changes to flash** if you wish to make your changes permanent.

| Status        | Power: XG-6000 3.21 (45.100.0.100) | Location: IT Dept                       | Uptime: 1 days, 18 hours, 23 mins |
|---------------|------------------------------------|---|-----------------------------------|
| Configuration | DNS Primary                        | 192.168.1.1                             |                                   |
| Export Data   | DNS Secondary                      | 192.168.1.2                             |                                   |
| Network       | DNS Server 1                       | 192.168.1.1                             |                                   |
| Interface     | DNS Server 2                       | 192.168.1.2                             |                                   |
| Name          | DNS Server 3                       |   |                                   |
| <b>DNS</b>    | Are DNS servers assigned by DHCP?  | <input checked="" type="checkbox"/> Yes | <input type="checkbox"/> No       |
| Host          |                                    |   |                                   |

Figure 106. DNS Settings

**Procedure for Configuring DNS Servers**

1. **DNS Host Name:** Enter a valid DNS [host name](#).
2. **DNS Domain:** Enter the DNS [domain](#) name.
3. **DNS Server 1:** Enter the IP address of the primary DNS server.
4. **DNS Server 2 and DNS Server 3:** Enter the IP address of the secondary and tertiary DNS servers (if required).
5. **Use DNS settings assigned by DHCP:** If you are using DHCP to assign the Array's IP address, you may turn this option **On**. The Array will then obtain its DNS domain and server settings from the network DHCP server that assigns an IP address to the Array, rather than using the DNS Server fields above. You may also configure that DHCP server to assign a host name to the Array.
6. Click **Save changes to flash** if you wish to make your changes permanent.

**See Also**[DHCP Server](#)[Network](#)[Network Interfaces](#)[Network Statistics](#)[Spanning Tree Status](#)



### CDP Settings

CDP (Cisco Discovery Protocol) is a layer 2 network protocol used to share information (such as the device manufacturer and model, network capabilities, and IP address) with other directly connected network devices. Wireless Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors (see “CDP Neighbors” on page 111).

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



| Setting       | Value                               | Unit    | Default |
|---------------|-------------------------------------|---------|---------|
| Enable CDP    | <input checked="" type="checkbox"/> |         | Off     |
| CDP Interval  | 60                                  | seconds | 60      |
| CDP Hold Time | 180                                 | seconds | 180     |

Figure 107. CDP Settings

#### Procedure for Configuring CDP Settings

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

#### See Also

[CDP Neighbors](#)  
[Network](#)  
[Network Interfaces](#)  
[Network Statistics](#)

## Services

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

The screenshot shows the 'Services' page for a Xirrus XR4000 WiFi Array. The page is divided into a left-hand navigation menu and a main content area. The 'Services' menu item is highlighted in orange. The main content area contains several tables and sections:

- System Information:** Shows IP Address (192.168.1.100), Location (1st Floor), and System Name (Xirrus XR4000).
- System Settings:** Shows System Name (Xirrus XR4000), System IP (192.168.1.100), and System Port (80).
- System Log:** A table with columns for Date, Description, and Action. It shows a log entry for 'System Log' on 10/10/2011.
- DHCP Server Settings:** A table with columns for DHCP Server, DHCP Pool Name, DHCP Pool IP, DHCP Pool Subnet, DHCP Pool Gateway, DHCP Pool Lease Time, and DHCP Pool DNS. It shows a DHCP Server 'Enabled' with a DHCP Pool Name '192.168.1.0/24'.
- SNMP Settings:** A table with columns for SNMP Server, SNMP Community, SNMP Trap, and SNMP Trap IP. It shows a SNMP Server 'Enabled' with a SNMP Community 'public'.
- Syslog Settings:** A table with columns for Syslog Server, Syslog Port, Syslog Facility, and Syslog Tag. It shows a Syslog Server 'Enabled' with a Syslog Port '514'.
- NTP Settings:** A table with columns for NTP Server, NTP Pool, and NTP Domain. It shows an NTP Server 'Enabled' with an NTP Pool '192.168.1.0/24' and an NTP Domain '192.168.1.0'.

Figure 108. Services

The following sections discuss configuring services on the Array:

- [“Time Settings \(NTP\)” on page 185](#)
- [“NetFlow” on page 187](#)
- [“Wi-Fi Tag” on page 188](#)
- [“System Log” on page 190](#)
- [“SNMP” on page 194](#)
- [“DHCP Server” on page 197](#)

### Time Settings (NTP)

This window allows you to manage the Array's time settings, including synchronizing the Array's clock with a universal clock from an NTP (Network Time Protocol) server. We recommend that you use NTP for proper operation of SNMP in XMS (the Xirrus Management System), since a lack of synchronization will cause errors to be detected. Synchronizing the Array's clock with an NTP server also ensures that Syslog time-stamping is maintained across all units.

It is possible to use authentication with NTP to ensure that you are receiving synchronization from a known source. For example, the instructions for requesting a key for the NIST Authenticated NTP server are available at [http://www.nist.gov/pml/div688/grp00/upload/ntp\\_instructions.pdf](http://www.nist.gov/pml/div688/grp00/upload/ntp_instructions.pdf). The Array allows you to enter optional authentication information.



| XIRRUS  |  | Xirrus XR4850 MFI Array |  |
|---|--|-------------------------|--|
| <ul style="list-style-type: none"> <li>Home</li> <li>Configuration</li> <li>System</li> <li>Time Settings</li> <li>Time Zone</li> <li>Auto Adjust Daylight Savings</li> <li>Use Network Time Protocol</li> <li>System Time (timestamp)</li> <li>System Date and Time</li> </ul> | <p>Current Array Date and Time: Thu Dec 10 10:17:10 2009</p> <p>Time Zone: GMT-0800 (Pacific Standard Time) [v]</p> <p>Auto Adjust Daylight Savings: <input checked="" type="checkbox"/></p> <p>Use Network Time Protocol: <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p> <p>System Time (timestamp): 12 10 10:17:10 2009</p> <p>System Date and Time: 12 10 2009</p> | <p>Save Changes</p>     |  |

Figure 109. Time Settings (Manual Time)

#### Procedure for Managing the Time Settings

1. **Current Array Date and Time:** Shows the current time for your convenience.
2. **Time Zone:** Select the time zone you want to use (normally your local time zone) from the pull-down list.
3. **Auto Adjust Daylight Savings:** Check this box if you want the system to adjust for daylight savings automatically, otherwise leave this box unchecked (default).
4. **Use Network Time Protocol:** select whether to set time manually or use NTP to manage system time.



- d. **NTP Primary Authentication Key:** Enter your key, which is a string of characters.
- e. **NTP Secondary Server:** Enter the IP address or domain name of an optional secondary NTP server to be used in case the Array is unable to contact the primary server. You may use the authentication fields as described above if you wish to set up authentication for the secondary server.

### See Also

Express Setup  
Services  
SNMP  
System Log

### NetFlow

This window allows you to enable or disable the sending of NetFlow information to a designated collector. NetFlow is a proprietary but open network protocol developed by Cisco Systems for collecting IP traffic information. When NetFlow is enabled, the Array will send IP flow information (traffic statistics) to the designated collector.

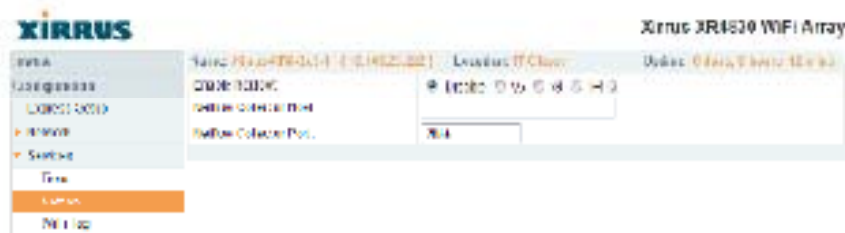


Figure 111. NetFlow

NetFlow sends per-flow network traffic information from the Array. Network managers can use a NetFlow collector to view the statistics on a per-flow basis and use this information to make key decisions. Knowing how many packets and bytes are sent to and from certain IP addresses or across specific network

interfaces allows administrators to track usage by various areas. Traffic flow information may be used to engineer networks for better performance.



*Some features, such as Netflow, are only available if the Array's license includes the Xirrus Advanced RF Analysis Manager (RAM). If a setting is unavailable (grayed out), then your license does not support the feature. See "About Licensing and Upgrades" on page 361.*

#### Procedure for Configuring NetFlow

1. **Enable NetFlow:** Select one of the Netflow versions to enable NetFlow functionality: v5, v9, or IPFIX. Internet Protocol Flow Information Export (IPFIX) is an IETF protocol ([www.ietf.org](http://www.ietf.org)) performing many of the same functions as Netflow. Choose **Disable** if you wish to disable this feature.
2. **NetFlow Collector Host (Domain or IP):** If you enabled NetFlow, enter the domain name or IP address of the collector.
3. **NetFlow Collector Port:** If you enabled NetFlow, enter the port on the collector host to which to send data.

#### Wi-Fi Tag

This window enables or disables Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channel. These tags are transmitted by specialized tag devices (for example, AeroScout Tags). A Wi-Fi tagging server (such as AeroScout) then queries the Array for a report on the tags that it has received. The Wi-Fi tagging server uses proprietary algorithms to determine locations for devices sending tag signals.



Figure 112. Wi-Fi Tag

*Procedure for Configuring Wi-Fi Tag*

1. **Enable Wi-Fi Tag:** Choose **Yes** to enable Wi-Fi tag functionality, or choose **No** to disable this feature.
2. **Wi-Fi Tag UDP Port:** If you enabled Wi-Fi tagging, enter the port on the Array which the Wi-Fi tagging server will use to query the Array for tagging data. When queried, the Array will send back information on the tags it has observed. For each, the Array sends information such as the MAC address of the tag transmitting device, and the RSSI and noise floor observed.
3. **Wi-Fi Tag Channel:** If you enabled Wi-Fi tagging, enter the 802.11 channel on which the Array will listen for tags. The tag devices must be set up to transmit on this channel. Only one channel may be configured, and it must be an 802.11b/g channel in the range of Channel 1 to 11.







3. **Local File Size (1-2000 lines):** Enter a value in this field to define how many Syslog records are retained locally on the Array's internal Syslog file. The default is 2000.
4. **Primary Server Address (Hostname or IP) and Port:** If you enabled Syslog, enter the hostname or IP address of the primary Syslog server. You may also change the port used on the server if you do not wish to use 514, the default port.
5. **Secondary/Tertiary Server Address (Hostname or IP) and Port:** (Optional) If you enabled Syslog, you may enter the hostname or IP address of one or two additional Syslog servers to which messages will also be sent. You may also change the port used on each server if you do not wish to use 514, the default port. You may set one of the server addresses to the address of a server for Splunk (see "About Using the Splunk Application for Xirrus Arrays" on page 193).
6. **Email Notification:** (Optional) The following parameters allow you to send an email to a designated address each time a Syslog message is generated. The email will include the text of the Syslog message.
  - a. **Email Syslog SMTP Server Address (Hostname or IP) and Port:** The hostname or the IP address of the SMTP server to be used for sending the email. Note that this specifies the mail server, **not** the email recipient. You may also change the port used on the server if you do not wish to use 25, the default SMTP port.
  - b. **Email Syslog SMTP User Name:** Specify a user name for logging in to an account on the mail server designated in [Step a](#).
  - c. **Email Syslog SMTP User Password:** Specify a password for logging in to an account on the mail server designated in [Step a](#).
  - d. **Email Syslog SMTP From:** Specify the "From" email address to be displayed in the email.
  - e. **Email Syslog SMTP Recipient Addresses:** Specify the entire email address of the recipient of the email notification. You may specify

additional recipients by separating the email addresses with semicolons (;).

7. **Station Formatting:** If you are sending event information to a Splunk server, select **Key/Value** to send data in Splunk's expected format, otherwise leave this at the default value of **Standard**. See "About Using the Splunk Application for Xirrus Arrays" on page 193.
8. **Syslog Levels:** For each of the Syslog destinations, choose your preferred level of Syslog reporting from the pull-down list. Messages with criticality at the selected level and above will be shown. The default level varies depending on the destination.
  - a. **Console Logging:** For messages to be echoed to the console, the default level is **Critical and more serious**. This prevents large numbers of non-critical messages from being displayed on the console. If you set this level too low, the volume of messages may make it very difficult to work with the CLI or view other output on the console.
  - b. **Local File:** For records to be stored on the Array's internal Syslog file, choose your preferred level of Syslog reporting from the pull-down list. The default level is **Debugging and more serious**.
  - c. **Primary Server:** Choose the preferred level of Syslog reporting for the primary server. The default level is **Debugging and more serious**.
  - d. **Secondary/Tertiary Server:** Choose the preferred level of reporting for the secondary/tertiary server. The default level is **Information and more serious**. (Optional)
  - e. **Email SMTP Server:** Choose the preferred level of Syslog reporting for the email notifications. The default level is **Warning and more serious**. This prevents your mailbox from being filled up with a large number of less severe messages such as informational messages.
9. Click **Save changes to flash** if you wish to make your changes permanent.

**About Using the Splunk Application for Xirrus Arrays**

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

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

You may specify Server Addresses for Syslog servers and a Splunk server on the same Array.

*See Also*

[System Log Window](#)  
[Services](#)  
[SNMP](#)  
[Time Settings \(NTP\)](#)

## SNMP

This window allows you to enable or disable SNMP v2 and SNMP v3 and define the SNMP parameters. SNMP allows remote management of the Array by the Xirrus Management System (XMS) and other SNMP management tools. SNMP v3 was designed to offer much stronger security. You may enable either SNMP version, neither, or both.

Complete SNMP details for the Array, including trap descriptions, are found in the Xirrus MIB, available at [support.xirrus.com](http://support.xirrus.com), in the **Downloads** section (login is required to download the MIB).

*NOTE: If you are managing your Arrays with XMS (the Xirrus Management System), it is very important to make sure that your SNMP settings match those that you have configured for XMS. XMS uses both SNMP v2 and v3, with v3 given preference.*

The screenshot shows the configuration page for a Xirrus X74430 WiFi Array. The left sidebar contains a navigation menu with categories like Configuration, System, and Tools. The main content area is titled 'SNMP Settings' and includes a table of various parameters such as 'Enable SNMP', 'SNMPv2 Settings', and 'SNMP Trap Settings'. The 'SNMP Trap Settings' section is expanded to show trap types and their corresponding ports.

| Category           | Parameter               | Value                               | Unit      |
|--------------------|-------------------------|-------------------------------------|-----------|
| Configuration      | Enable SNMP             | <input checked="" type="checkbox"/> | Yes       |
|                    | SNMPv2 Settings         |                                     |           |
| SNMPv2 Settings    | Enable SNMPv2           | <input checked="" type="checkbox"/> | Yes       |
|                    | Authentication          | <input checked="" type="checkbox"/> | Yes       |
|                    | Privacy                 | <input checked="" type="checkbox"/> | Yes       |
|                    | Enable SNMPv3           | <input checked="" type="checkbox"/> | Yes       |
| SNMP Trap Settings | Trap Host 1 IP Address  | 192.168.1.105                       | Port: 162 |
|                    | Trap Host 2 IP Address  |                                     | Port: 162 |
|                    | Trap Host 3 IP Address  |                                     | Port: 162 |
|                    | Trap Host 4 IP Address  |                                     | Port: 162 |
| System             | Send Trap Collect Traps | <input checked="" type="checkbox"/> | Yes       |
|                    | Keepable Trap Count     | 1                                   |           |

Figure 114. SNMP

### *Procedure for Configuring SNMP*

#### *SNMPv2 Settings*

1. **Enable SNMPv2:** Choose **Yes** to enable SNMP v2 functionality, or choose **No** to disable this feature. When used in conjunction with the Xirrus Management System, SNMP v2 (not SNMP v3) must be enabled on each Array to be managed with XMS. The default for this feature is **Yes** (enabled).
2. **SNMP Read-Write Community String:** Enter the read-write community string. The default is **xirrus**.
3. **SNMP Read-Only Community String:** Enter the read-only community string. The default is **xirrus\_read\_only**.

#### *SNMPv3 Settings*

4. **Enable SNMPv3:** Choose **Yes** to enable SNMP v3 functionality, or choose **No** to disable this feature. The default for this feature is **Yes** (enabled).
5. **Authentication:** Select the desired method for authenticating SNMPv3 packets: **SHA** (Secure Hash Algorithm) or **MD5** (Message Digest Algorithm 5).
6. **Privacy:** Select the desired method for encrypting data: **DES** (Data Encryption Standard) or the stronger **AES** (Advanced Encryption Standard).
7. **Context Engine ID:** The unique identifier for this SNMP server. We recommend that you do not change this value. The Context Engine ID must be set if data collection is to be done via a proxy agent. This ID helps the proxy agent to identify the target agent from which data is to be collected.
8. **SNMP Read-Write Username:** Enter the read-write user name. This username and password allow configuration changes to be made on the Array. The default is **xirrus-rw**.
9. **SNMP Read-Write Authentication Password:** Enter the read-write password for authentication (i.e., logging in). The default is **xirrus-rw**.

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

#### *SNMP Trap Settings*

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

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

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

#### *See Also* Services

System Log  
Time Settings (NTP)

### DHCP Server

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

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



Figure 115. DHCP Management

DHCP usage is determined in several windows—see [SSID Management](#), [Group Management](#), and [VLAN Management](#).

#### *Procedure for Configuring the DHCP Server*

- 1. New Internal DHCP Pool:** Enter a name for the new DHCP pool, then click on the Create button. The new pool ID is added to the list of available DHCP pools.
- 2. On:** Click this checkbox to make this pool of addresses available, or clear it to disable the pool.

3. **Lease Time—Default:** This field defines the default DHCP lease time (in seconds). The factory default is 300 seconds, but you can change the default at any time.
4. **Lease Time—Max:** Enter a value (in seconds) to define the maximum allowable DHCP lease time. The default is 300 seconds.
5. **Network Address Translation (NAT):** Check this box to enable the Network Address Translation feature.
6. **Lease IP Range—Start:** Enter an IP address to define the start of the IP range that will be used by the DHCP server. The default is 192.168.1.100.
7. **Lease IP Range—End:** Enter an IP address to define the end of the IP range that will be used by the DHCP server. The DHCP server will only use IP addresses that fall between the start and end range that you define on this page. The default is 192.168.1.200.
8. **Subnet Mask:** Enter the subnet mask for this IP range for the DHCP server. The default is 255.255.255.0.
9. **Gateway:** If necessary, enter the IP address of the gateway.
10. **Domain:** Enter the DNS domain name. See “DNS Settings” on page 181.
11. **DNS Servers (1 to 3):** Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. These DNS server addresses will be passed to stations when they associate, along with the assigned IP address. Note that if you leave these blank, no DNS information is sent to the stations. DHCP will not default to sending the DNS servers that are configured in DNS Settings. See also, “DNS Settings” on page 181.
12. Click **Save changes to flash** if you wish to make your changes permanent.

*See Also*

DHCP Leases  
DNS Settings  
Network Map



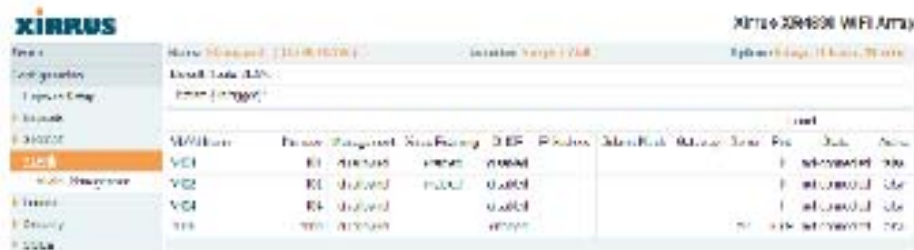
## VLANs

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



*You should create VLAN entries on the Array for all of the VLANs in your wired network if you wish to make traffic from those VLANs available on the wireless network. Each tagged VLAN should be associated with a wireless SSID (see “VLAN Management” on page 201). The Array will discard any VLAN-tagged packets arriving on its wired ports, unless the same VLAN has been defined on the Array. See “Undefined VLANs” on page 113.*

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



| XIRRUS                      |          | XIRRUS X2R4000 WiFi Array       |             |          |          |                               |        |       |      |     |               |
|-----------------------------|----------|---------------------------------|-------------|----------|----------|-------------------------------|--------|-------|------|-----|---------------|
| Name: X2R4000 (10.10.10.10) |          | Location: X2R4000 (10.10.10.10) |             |          |          | System: X2R4000 (10.10.10.10) |        |       |      |     |               |
| Configuration               |          | Default: Native VLAN            |             |          |          |                               |        |       |      |     |               |
| VLANs                       |          | Native (Untagged)               |             |          |          |                               |        |       |      |     |               |
|                             |          | VLAN                            |             |          |          |                               |        |       |      |     |               |
| VLAN                        | Priority | Management                      | Native VLAN | QoS      | Priority | Admin                         | Native | State | Port | Sub | Act           |
| V01                         | 01       | Enabled                         | Enabled     | Enabled  | Enabled  |                               |        |       |      |     | Not connected |
| V02                         | 02       | Disabled                        | Enabled     | Disabled | Disabled |                               |        |       |      |     | Not connected |
| V03                         | 03       | Disabled                        | Enabled     | Disabled | Disabled |                               |        |       |      |     | Not connected |
| V04                         | 04       | Disabled                        | Enabled     | Disabled | Disabled |                               |        |       |      |     | Not connected |
| V05                         | 05       | Enabled                         | Enabled     | Enabled  | Enabled  |                               |        |       |      |     | Not connected |

Figure 116. VLANs



*For a discussion of implementing Voice over Wi-Fi on the Array, see the [XIRRUS Voice over Wireless Application Note](#) in the [XIRRUS Resource Center](#).*

## Understanding Virtual Tunnels

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

- The XIRRUS Tunnel Server (XTS)—see the [XIRRUS Tunnel Server User's Guide](#).
- Virtual Tunnel Server (VTS)—see below.

### *Virtual Tunnel Server (VTS)*

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

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

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

### *VTS Client-Server Interaction*

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

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

### VLAN Management

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



Figure 117. VLAN Management



The Wireless Array supports dynamic VLAN assignments specified by RADIUS policy settings. When RADIUS sends these assignments, the Array dynamically assigns wireless stations to VLANs as requested. VLAN tags on traffic are passed through the Array (i.e., VLAN tags are not stripped). Once a station has been dynamically moved to a new VLAN, it will be shown in the Stations window as a member of the new VLAN. (Figure 70 on page 126)

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

### Procedure for Managing VLANs

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

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

**See Also**[VLAN Statistics](#)[VLANs](#)[Tunnels](#)

## Tunnels

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

| Tunnel Name | Status  | Type | Local Endpoints | Primary Remote Endpoint | Secondary Remote Endpoint | Tunnel ID | MTU  | Admin | Enabled |
|-------------|---------|------|-----------------|-------------------------|---------------------------|-----------|------|-------|---------|
| TUNNEL1     | Enabled | GRE  | 10.10.10.1      | 10.10.10.1              |                           | 1000      | 1500 | Admin | Enabled |
| TUNNEL2     | Enabled | GRE  | 10.10.10.1      | 10.10.10.1              |                           | 1000      | 1500 | Admin | Enabled |

Figure 118. Tunnel Summary

### About Xirrus Tunnels

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

Tunnels may be implemented with:

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

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

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

### Tunnel Management

This window allows you to create tunnels.



Figure 119. Tunnel Management

#### Procedure for Managing Tunnels

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

8. **MTU:** Set maximum transmission unit (MTU) size.
9. **Interval:** The tunnel mechanism will ping the current remote endpoint periodically to ensure that it is still reachable. Enter the ping interval (in seconds).
10. **Failures:** Enter the number of consecutive ping failures that will cause the Array to consider the tunnel to be down.
11. Click **Save changes to flash** if you wish to make your changes permanent.
12. Proceed to **SSID Assignments** to define the SSIDs (and associated VLANs) for which each tunnel will bridge data. You may create up to 16 tunnels. Each will need an SSID/VLAN pair assigned to it so that it can function properly.

### SSID Assignments

This window allows you to select the SSIDs to be bridged by each tunnel.



Figure 120. Tunnel SSID Assignments

### Procedure for Assigning SSIDs

This window lists the tunnels and SSIDs that you have defined. SSIDs to be tunneled should be associated with a VLAN (see "SSID Management" on page 249).



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

*See Also*[Tunnels](#)[VLANs](#)[SSIDs](#)



Security settings are configured with the following windows:

- “Admin Management” on page 214
- “Admin Privileges” on page 216
- “Admin RADIUS” on page 218
- “Management Control” on page 221
- “Access Control List” on page 227
- “Global Settings” on page 230
- “External Radius” on page 234
- “Internal Radius” on page 238
- “Rogue Control List” on page 240

### Understanding Security

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

Other security considerations include:

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

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

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

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

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

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

The encryption mode (WEP, WPA, etc.) is selected in the **SSIDs > SSID Management** window (see “SSID Management” on page 249). The encryption standard used with WPA or WPA2 (AES or TKIP) is selected in the **Security > Global Settings** window under **WPA Settings** (see “Global Settings” on page 230).

- **Choosing an authentication method:** User authentication ensures that users are who they say they are. For this purpose, the Array allows you to choose between the following user authentication methods:

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

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

- **RADIUS 802.1x with EAP**—802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS, EAP-PEAP, and LEAP-Passthrough. The RADIUS server can be internal (provided by the Wireless Array) or external. An external RADIUS server offers more functionality and security, and is recommended for large deployments. When using this method, user names and passwords must be entered into the RADIUS server for user authentication.
- **MAC Address ACLs (Access Control Lists)**—MAC address ACLs provide a list of client adapter MAC addresses that are allowed or denied access to the wireless network. Access Control Lists work well when there are a limited number of users—in this case, enter the MAC address of each user in the Allow list. In the event of a lost or stolen MAC adapter, enter the affected MAC

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

### Certificates and Connecting Securely to the WMI

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

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

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

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

### Using the Array's Default Certificate

|                                       |  |
|---------------------------------------|--|
| HTTPS (X.509) Certificate             |  |
| Input Xirrus Authority into Browser:  | xirrus.ca.ca   |
| Certificate Signed By:                | Xirrus   |
| External Certification Authority      |  |
| Download Certificate Signing Request: | Xirrus-WR9-CA2-1.csr   |
| Upload Signed Certificate:            | <input type="button" value="Browse..."/> <input type="button" value="Upload"/> |

Figure 122. Import Xirrus Certificate Authority

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

By clicking and opening this file, you can follow your browser's instructions and import the Xirrus CA into your CA cache (see [page 225](#) for more information). This instructs your browser to trust any of the certificates signed by the Xirrus CA, so that when you connect to any of our Arrays you should no longer see the warning about an untrusted site. Note however, that this only works if you use the host name when connecting to the Array. If you use the IP address to connect, you get a lesser warning saying that the certificate was only meant for 'hostname'.

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

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

#### Using an External Certificate Authority

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

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

WMI provides options for creating a Certificate Signing Request that you can send to an external CA, and for uploading the signed certificate to the Array after

you obtain it from the CA. This certificate will be tied to the Array's host name and private key. See "External Certification Authority" on page 226 for more details.

### Admin Management

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



Figure 123. Admin Management

#### Procedure for Creating or Modifying Network Administrator Accounts

1. **Admin ID:** Enter the login name for a new network administrator ID. The length of the ID must be between 5 and 50 characters, inclusive.
2. **Read/Write:** Choose **1:read-write** if you want to give this administrator ID full read/write privileges, or choose **0:read-only** to restrict this user to read only status. In the read only mode, administrators cannot save changes to configurations. Or you may select one of your custom-defined privilege levels (see "Admin Privileges" on page 216).
3. **New Password:** Enter a password for this ID. The length of the password must be between 5 and 50 characters, inclusive.
4. **Verify:** Re-enter the password in this field to verify that you typed the password correctly. If you do not re-enter the correct password, an error message is displayed).



5. Click on the **Create** button to add this administrator ID to the list.
6. Click **Save changes to flash** if you wish to make your changes permanent.

*See Also*

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



## Admin Privileges

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

| Configuration Section | Privilege Level | Level     |
|-----------------------|-----------------|-----------|
| Admin Privileges      | Privilege Level | None      |
| Admin Privileges      | Level 0         | Read Only |
| Admin Privileges      | Level 1         | CDM/IE    |
| Admin Privileges      | Level 2         | 1         |
| Admin Privileges      | Level 3         | 1         |
| Admin Privileges      | Level 4         | 1         |
| Admin Privileges      | Level 5         | 1         |
| Admin Privileges      | Level 6         | 1         |
| Admin Privileges      | Level 7         | 1         |

| Configuration Section | Security | Access | Privilege Level |   |   |   |   |   |   |   |
|-----------------------|----------|--------|-----------------|---|---|---|---|---|---|---|
|                       |          |        | 0               | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Admin Privileges      | 0        | 0      | 0               | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Figure 124. Admin Privileges

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

If you are using an Admin RADIUS server to define administrator accounts, please see “RADIUS Vendor Specific Attribute (VSA) for Xirrus” on page 463 to set the privilege level for each administrator.

*Procedure for Configuring Admin Privileges*

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

*See Also*

[External Radius](#)

[Groups](#)

[Admin Management](#)

[Admin RADIUS](#)

[Security](#)

### Admin RADIUS

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

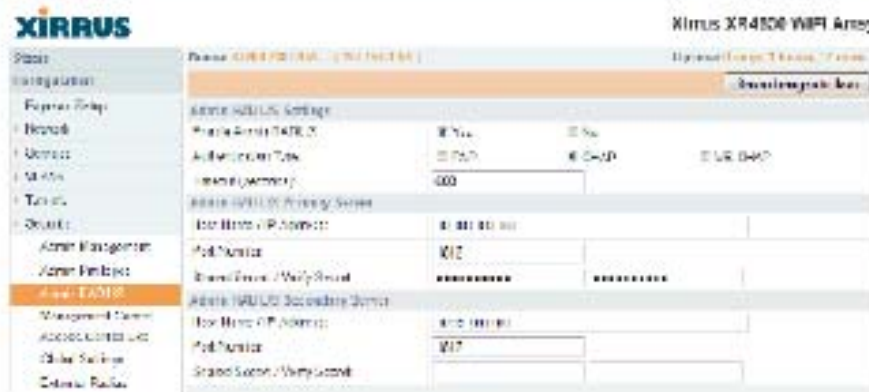
- Centralized control of administrator accounts.
- Less effort—you don't have to set up user names and passwords on each Array; just enter them once on the RADIUS server and then all of the Arrays can pull from the RADIUS server.
- Enforced policies—you may set password rules (e.g., passwords must contain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

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

#### About Creating Admin Accounts on the RADIUS Server

Permissions for RADIUS administrator accounts are controlled by the RADIUS `Xirrus-Admin-Role` attribute. This is a Vendor Specific Attribute (VSA). To define the privileges permitted to an administrator account, set the value of its `Xirrus-Admin-Role` attribute to the desired **Privilege Level Name** string, as defined in [“Admin Privileges”](#) on page 216. For more information about the RADIUS VSAs used by Xirrus, see [“RADIUS Vendor Specific Attribute \(VSA\) for Xirrus”](#) on page 463.

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



| Admin RADIUS Settings         |   |
|-------------------------------|---|
| Enable Admin RADIUS           | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No                       |
| Authentication Type           | <input type="radio"/> PAP <input checked="" type="radio"/> CHAP <input type="radio"/> EAP |
| Admin RADIUS Primary Server   | IP Address: 10.10.10.10<br>Port Number: 1812<br>Shared Secret / Verify Secret: *****      |
| Admin RADIUS Secondary Server | IP Address: 10.10.10.10<br>Port Number: 1812<br>Shared Secret / Verify Secret:            |

Figure 125. Admin RADIUS

### Procedure for Configuring Admin RADIUS

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

#### 1. Admin RADIUS Settings:

- a. **Enable Admin RADIUS:** Click **Yes** to enable the use of RADIUS to authenticate administrators logging in to the Array. You will need to specify the RADIUS server(s) to be used.
- b. **Authentication Type:** Select the protocol used for authentication of administrators, **CHAP** or **PAP** (the default).
  - **PAP** (Password Authentication Protocol), is a simple protocol. PAP transmits ASCII passwords over the network “in the clear” (unencrypted) and is therefore considered insecure.
  - **CHAP** (Challenge-Handshake Authentication Protocol) is a more secure protocol. The login request is sent using a one-way hash function.



## Management Control

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

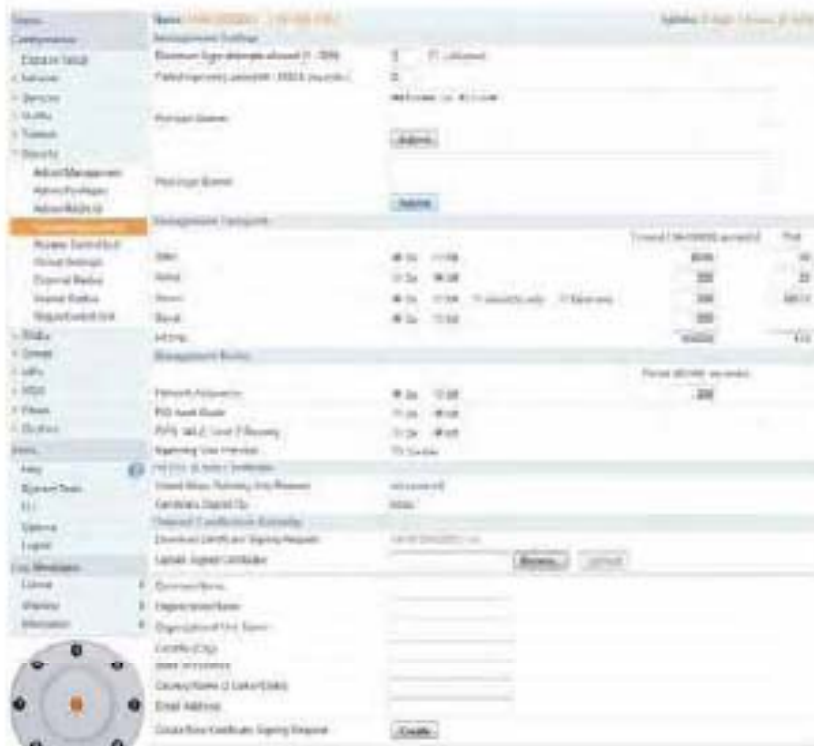


Figure 126. Management Control

### Procedure for Configuring Management Control

#### 1. Management Settings:

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

- b. **Failed login retry period (0-65535 seconds):** After the maximum number (defined above) of consecutive failing administrator login attempts via ssh or telnet, the administrator's IP address is denied access to the array for the specified period of time (in seconds). The default is 0.
- c. **Pre-login Banner:** Text that you enter here will be displayed above the WMI login prompt. (Figure 127)

The screenshot shows the login interface for the Xirrus XR4030 WiFi Array. At the top left is the XIRRUS logo, and at the top right is the device name 'Xirrus XR4030 WiFi Array'. Below the header is a light blue box containing the login form. The form has a title bar that says 'Banner: 20131128090800 (141961184)'. Inside the form, there are two columns. The left column has labels: 'Current Status', 'User Name', and 'User Password'. The right column has corresponding input fields: 'Logged On', 'Welcome to Xirrus!', a text box containing 'admin', and a password field with six asterisks. The 'Logged On' field shows 'Logged On'.

Figure 127. Pre-login Banner

- d. **Post-login Banner:** Text that you enter here will be displayed in a message box after a user logs in to the WMI.
2. **SSH**
- a. **On/Off:** Choose **On** to enable management of the Array over a Secure Shell (SSH-2) connection, or **Off** to disable this feature. Be aware that only SSH-2 connections are supported by the Array. SSH clients used for connecting to the Array must be configured to use SSH-2.
  - b. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your SSH connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
  - c. **Port:** Enter a value in this field to define the port used by SSH. The default port is 22.




### 3. Telnet:

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

### 4. Xircon

The Xircon utility is not used with XN Arrays. For those Arrays, this setting should always be turned Off.

The Xircon utility connects to Xirrus Arrays that are not reachable via the normal access methods (such as SSH or WMI) and that do not have a physical console port (XR-1000 models), or whose console port is not accessible. Please see [“Securing Low Level Access to the Array” on page 78](#) for more information about Xircon. You can enable or disable Xircon access to the Array as instructed below.

 **Warning:** *If you disable Xircon access completely on XR-1000 models, you must ensure that you do not lose track of the username and password to log in to CLI/WMI! There is no way to recover from a lost password, other than returning the Array to Xirrus.*

- a. **On/Off:** Choose **On** to enable Xircon access to the Array at the ArrayOS (CLI) and Xirrus Boot Loader (XBL) levels, or **Off** to disable access at both levels. On XR-1000 Array models only, Xircon access is **On** by default. On all other Array models, Xircon access is **Off** by default.
- b. **ArrayOS only:** Choose this radio button to enable Xircon access at the ArrayOS level only (i.e., Xircon can access CLI only). Access to the Array at the Xirrus Boot Loader (XBL) level is disabled.

- c. **Boot only:** Choose this radio button to enable Xircon access at the Xirrus Boot Loader (XBL) level only. ArrayOS level (CLI) access to the Array is disabled.
  - d. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your Xircon connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
  - e. **Port:** Enter a value in this field to define the port used by Xircon. The default port is 22612.
5. **Serial**
- a. **On/Off:** Choose **On** to enable management of the Array via a serial connection, or choose **Off** to disable this feature.
  - b. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your serial connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds.
6. **HTTPS**
- a. **Connection Timeout 30-100000 (Seconds):** Enter a value in this field to define the timeout (in seconds) before your HTTPS connection is disconnected. The value you enter here must be between 30 seconds and 100,000 seconds. Management via HTTPS (i.e., the Web Management Interface) cannot be disabled on this window. To disable management over HTTPS, you must use the Command Line Interface.
  - b. **Port:** Enter a value in this field to define the port used by SSH. The default port is 443.

## 7. Management Modes

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

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

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

To view the status of all configured servers checked by this feature, please see “[Network Assurance](#)” on page 112.

## 8. HTTPS (X.509) Certificate

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

When you assign a **Host Name** to your Array using the [Express Setup](#) window, then the next time you reboot the Array it

automatically creates a security certificate for that host name. That certificate uses Xirrus as the signing authority. Thus, in order to avoid having certificate errors on your browser when using WMI:

- You must have assigned a host name to the Array and rebooted at some time after that.
  - Use **Import Xirrus Authority into Browser**
  - Access WMI by using the host name of the Array rather than its IP address.
- b. **HTTPS (X.509) Certificate Signed By:** This read-only field shows the signing authority for the current certificate.

#### 9. External Certification Authority

This Step and [Step 10](#) allow you to obtain a certificate from an external authority and install it on an Array. “[Using an External Certificate Authority](#)” on page 213 discusses reasons for using an external CA.

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

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

External Certification Authority has the following fields:

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



There is also a per-SSID ACL (see “Per-SSID Access Control List” on page 262). If the same MAC address is listed in both the global ACL and in an SSID’s ACL, and if either ACL would deny that station access to that SSID, then access will be denied.



Figure 128. Access Control List

#### Procedure for Configuring Access Control Lists

- Access Control List Type:** Select **Disabled** to disable use of the Access Control List, or select the ACL type—either **Allow List** or **Deny List**.
  - Allow List:** Only allows the listed MAC addresses to associate to the Array. All others are denied.
  - Deny List:** Denies the listed MAC addresses permission to associate to the Array. All others are allowed.

*In addition to these lists, other authentication methods (for example, RADIUS) are still enforced for users.*
- MAC Address:** If you want to add a MAC address to the ACL, enter the new MAC address here, then click on the **Add** button. The MAC address is added to the ACL. You may use a wildcard (\*) for one or more digits to match a range of addresses. You may create up to 1000 entries.

3. **Delete:** You can delete selected MAC addresses from this list by clicking their **Delete** buttons.
4. Click **Save changes to flash** if you wish to make your changes permanent.

*See Also*

External Radius

Global Settings (IAP)

Internal Radius

Management Control

Security

Station Status Windows (list of stations that have been detected by the Array)







**Procedure for Configuring Network Security**

1. **RADIUS Server Mode:** Choose the RADIUS server mode you want to use, either **Internal** or **External**. Parameters for these modes are configured in “External Radius” on page 234 and “Internal Radius” on page 238.

**WPA Settings**

These settings are used if the WPA or WPA2 encryption type is selected on the SSIDs > SSID Management window or the Express Setup window (on this window, encryption type is set in the SSID Settings: Wireless Security field).

2. **TKIP Enabled:** Choose **Yes** to enable TKIP (Temporal Key Integrity Protocol), or choose **No** to disable TKIP.



*TKIP encryption does not support high throughput rates (see Improved MAC Throughput), per the IEEE 802.11n specification.*

*TKIP should never be used for WDS links on XR or XN Arrays.*

3. **AES Enabled:** Choose **Yes** to enable AES (Advanced Encryption Standard), or choose **No** to disable AES. If both AES and TKIP are enabled, the station determines which will be used.
4. **WPA Group Rekey Time (seconds):** Enter a value to specify the group rekey time (in seconds). The default is **Never**.
5. **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.

### WEP Settings

These settings are used if the WEP encryption type is selected on the **SSIDs > SSID Management** window or the **Express Setup** window (on this window, encryption type is set in the **SSID Settings: Wireless Security** field).

Click the **Show Cleartext** button to make the text that you type in to the Key fields visible.



*WEP encryption does not support high throughput rates or features like frame aggregation or block acknowledgements (see **Improved MAC Throughput**), per the IEEE 802.11n specification.*

*WEP should never be used for WDS links on Arrays.*

#### 6. Encryption Key 1 / Verify Key 1:

**Key Size:** Key length is automatically computed based on the Encryption Key that you enter

- 5 ASCII characters (10 hex) for 40 bits (WEP-64)
- 13 ASCII characters for (26 hex) 104 bits (WEP-128)

**Encryption Key 1 / Verify Key 1:** Enter an encryption key in ASCII or hexadecimal. The ASCII and translated hexadecimal values will appear to the right if you selected the **Show Cleartext** button.

Re-enter the key to verify that you typed it correctly. You may include special ASCII characters, except for the double quote symbol (").

7. **Encryption Key 2 to 4/ Verify Key 2 to 4/ Key Mode/Length (optional):** If desired, enter up to four encryption keys, in the same way that you entered the first key.
8. **Default Key:** Choose which key you want to assign as the default key. Make your selection from the pull-down list.

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



*After configuring network security, the configuration must be applied to an SSID for the new functionality to take effect.*


#### **See Also**

Admin Management  
External Radius  
Internal Radius  
Access Control List  
Management Control  
Security  
Security Planning  
SSID Management





**Procedure for Configuring an External RADIUS Server**

1. **Primary Server:** This is the external RADIUS server that you intend to use as your primary server.
  - a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
  - b. **Port Number:** Enter the port number of this external RADIUS server. The default is 1812.
  - c. **Shared Secret / Verify Secret:** Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.  
 *The shared secret that you define must match the secret used by the external RADIUS server.*
2. **Secondary Server (optional):** If desired, enter an alternative external RADIUS server. If the primary RADIUS server becomes unreachable, the Array will “failover” to the secondary RADIUS server (defined here).
  - a. **Host Name / IP Address:** Enter the IP address or domain name of this external RADIUS server.
  - b. **Port Number:** Enter the port number of this external RADIUS server. The default is 1812.
  - c. **Shared Secret / Verify Secret:** Enter the shared secret that this external RADIUS server will be using, then re-enter the shared secret to verify that you typed it correctly.
3. **Settings:** Define the session timeout, the NAS Identifier, and whether accounting will be used.
  - a. **Timeout (seconds):** Define the maximum idle time (in seconds) before the external RADIUS server’s session times out. The default is 600 seconds.
  - b. **DAS Port:** RADIUS Dynamic Authorization port. Some RADIUS servers have the ability to contact the Array (referred to as an NAS,

see below) to terminate a user with a Disconnect Message (DM). Or RADIUS may send a Change-of-Authorization (CoA) Message to the Array to change a user's privileges due to dynamically changing session authorizations. RADIUS will use the DAS port on the Array for this purpose. The default is port 3799.

- c. **NAS Identifier:** From the point of view of a RADIUS server, the Array is a client, also called a network access server (NAS). Enter the NAS Identifier (IP address) that the RADIUS servers expect the Array to use—this is normally the IP address of the Array's Gigabit1 port.
  - d. **Accounting:** If you would like the Array to send RADIUS Start, Stop, and Interim records to a RADIUS accounting server, click the **On** button. The account settings appear, and must be configured.
4. **Accounting Settings:**

Note that RADIUS accounting start packets sent by the Array will include the client station's Framed-IP-Address attribute.

- a. **Accounting Interval (seconds):** Specify how often Interim records are to be sent to the server. The default is 300 seconds.
- b. **Primary Server Host Name / IP Address:** Enter the IP address or domain name of the primary RADIUS accounting server that you intend to use.
- c. **Primary Port Number:** Enter the port number of the primary RADIUS accounting server. The default is 1813.
- d. **Primary Shared Secret / Verify Secret:** Enter the shared secret that the primary RADIUS accounting server will be using, then re-enter the shared secret to verify that you typed it correctly.
- e. **Secondary Server Host Name / IP Address (optional):** If desired, enter an IP address or domain name for an alternative RADIUS accounting server. If the primary server becomes unreachable, the Array will "failover" to this secondary server (defined here).

- f. **Secondary Port Number:** If using a secondary accounting server, enter its port number. The default is 1813.
  - g. **Secondary Shared Secret / Verify Secret:** If using a secondary accounting server, enter the shared secret that it will be using, then re-enter the shared secret to verify that you typed it correctly.
5. Click **Save changes to flash** if you wish to make your changes permanent.

*See Also*

Admin Management  
Global Settings (IAP)  
Internal Radius  
Access Control List  
Management Control  
Security  
Understanding Groups

### Internal Radius

This window allows you to define the parameters for the Array's internal RADIUS server for user authentication. However, 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. To set up the internal RADIUS server, you must choose **Internal** as the RADIUS server mode in Global Settings. Refer to "Global Settings" on page 230.

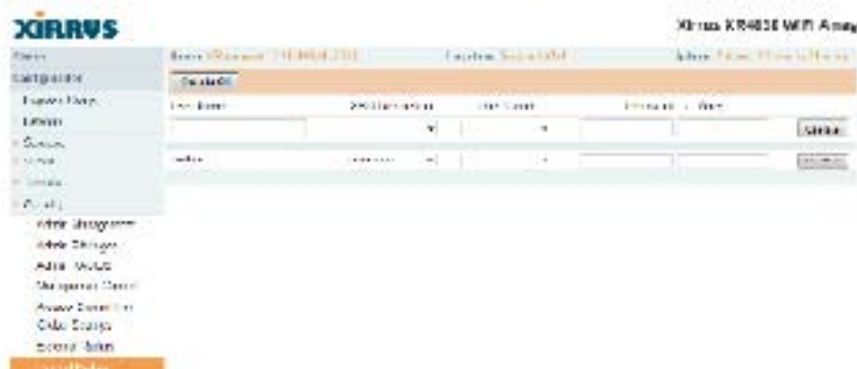


Figure 131. Internal RADIUS Server



*Clients using PEAP may have difficulty authenticating to the Array using the Internal RADIUS server due to invalid security certificate errors. To prevent this problem, the user may disable the **Validate Server Certificate** option on the station. Do this by displaying the station's wireless devices and then displaying the properties of the desired wireless interface. In the security properties, disable **Validate server certificate**. In some systems, this may be found by setting the authentication method to PEAP and changing the associated settings.*



**Procedure for Creating a New User**

1. **User Name:** Enter the name of the user that you want to authenticate to the internal RADIUS server.
2. **SSID Restriction:** (Optional) If you want to restrict this user to associating to a particular SSID, choose an SSID from the pull-down list.
3. **User Group:** (Optional) If you want to make this user a member of a previously defined user group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 264.
4. **Password:** (Optional) Enter a password for the user.
5. **Verify:** (Optional) Retype the user password to verify that you typed it correctly.
6. Click on the **Create** button to add the new user to the list.

**Procedure for Managing Existing Users**

1. **SSID Restriction:** (Optional) If you want to restrict a user to associating to a particular SSID, choose an SSID from its pull-down list.
2. **User Group:** (Optional) If you want to change the user's group, choose a group from the pull-down list. This will apply all of the user group's settings to the user. See "Understanding Groups" on page 264.
3. **Password:** (Optional) Enter a new password for the selected user.
4. **Verify Password:** (Optional) Retype the user password to verify that you typed it correctly.
5. If you want to delete one or more users, click their **Delete** buttons.
6. Click **Save changes to flash** if you wish to make your changes permanent.

**See Also**[Admin Management](#)[External Radius](#)[Global Settings \(IAP\)](#)

Access Control List  
 Management Control  
 Security  
 Understanding Groups

### Rogue Control List

This window allows you to set up a control list for rogue APs, based on a type that you define. You may classify rogue APs as blocked, so that the Array will take steps to prevent stations from associating with the blocked AP. See “About Blocking Rogue APs” on page 331. The Array can keep up to 5000 entries in this list.



*The RF Monitor > Intrusion Detection window provides an alternate method for classifying rogues. You can list all Unknown stations and select all the rogues that you'd like to set to Known or Approved, rather than entering the SSID/BSSID as described below. See “Intrusion Detection” on page 119.*

| Name     | Device | Approval | Status | MAC | Block                    | Deny                     | Warn                     | Actions |
|----------|--------|----------|--------|-----|--------------------------|--------------------------|--------------------------|---------|
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |
| 00000000 |        |          |        |     | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | Block   |

Figure 132. Rogue Control List

**Procedure for Establishing Rogue AP Control**

- 1. Rogue BSSID/SSID:** Enter the BSSID, SSID, or manufacturer string to match for the new rogue control entry. The **Match Only** radio buttons specify what to match (e.g., the MAC address, SSID, or manufacturer).  
  
You may use the "\*" character as a wildcard to match any string at this position. For example, 00:0f:7d:\* matches any string that starts with 00:0f:7d: Xirrus Arrays start with 00:0f:7d: or 50:60:28:. By default, the Rogue Control List contains two entries that match 00:0f:7d:\* and 50:60:28:\* and apply the classification **Known** to all Xirrus Arrays.
- 2. Rogue Control Classification:** Enter the classification for the specified rogue AP(s), either **Blocked**, **Known** or **Approved**.
- 3. Match Only:** Select the match criterion to compare the **Rogue BSSID/SSID** string against: **BSSID**, **Manufacturer**, or **SSID**. The BSSID field contains the MAC address.
- 4.** Click **Create** to add this rogue AP to the Rogue Control List.
- 5. Rogue Control List:** If you want to edit the control type for a rogue AP, just click the radio button for the new type for the entry: **Blocked**, **Known** or **Approved**.
- 6.** To delete rogue APs from the list, click their **Delete** buttons.
- 7.** Click **Save changes to flash** if you wish to make your changes permanent.

**See Also**

[Network Map](#)  
[Intrusion Detection](#)  
[SSIDs](#)  
[SSID Management](#)

## SSIDs

This status-only window 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, radio availability, and DHCP pools defined per SSID. Click on an SSID's name to jump to the edit page for the 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 a complete discussion of implementing Voice over Wi-Fi on the Array, see the Xirrus Voice over Wireless Application Note in the [Xirrus Resource Center](#)*

| SSID Name | Admin Name | Admin Email     | Status  | Visible | Security        | QoS         | VLAN | Radio |
|-----------|------------|-----------------|---------|---------|-----------------|-------------|------|-------|
| Corporate | Admin      | admin@corp.com  | Enabled | Yes     | WPA2-Enterprise | Best Effort | 100  | 1     |
| Guest     | Admin      | admin@guest.com | Enabled | No      | WPA2-Personal   | Best Effort | 100  | 2     |

| SSID Name | Enabled | Disabled | On       | Off      | Days On  | Days Off | Active |
|-----------|---------|----------|----------|----------|----------|----------|--------|
| Corporate | 0       | 0        | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 | Yes    |
| Guest     | 0       | 0        | 00:00:00 | 00:00:00 | 00:00:00 | 00:00:00 | No     |

Figure 133. SSIDs

The read-only **Limits** section of the SSIDs window allows you to review any limitations associated with your defined SSIDs. For example, this window shows the current state of an SSID (enabled or not), how much SSID and station traffic is allowed, time on and time off, days on and off, and whether each SSID is currently active or inactive.

For information to help you understand SSIDs and how multiple SSIDs are managed by the Wireless Array, go to “[Understanding SSIDs](#)” on page 243 and the [Multiple SSIDs](#) section of “[Frequently Asked Questions](#)” on page 452. For a description of how QoS operates on the Array, see “[Understanding QoS Priority on the Wireless Array](#)” on page 244.

SSIDs are managed with the following windows:

- “SSID Management” on page 249
- “Active IAPs” on page 261
- “Per-SSID Access Control List” on page 262

SSIDs are discussed in the following topics:

- “Understanding SSIDs” on page 243
- “Understanding QoS Priority on the Wireless Array” on page 244

### 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 via 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. Wireless Arrays support the ability to define and use multiple SSIDs 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 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 Quality of Service (QoS) definition. This SSID might also forward traffic to specific VLANs on the wired network.

#### See Also

SSID Management

SSIDs

Understanding SSIDs

#### Understanding QoS Priority on the Wireless Array



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

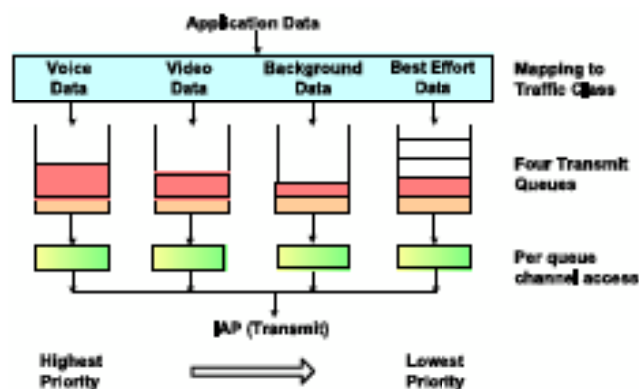


Figure 134. Four Traffic Classes

The Wireless Array's Quality of Service Priority feature (QoS) allows traffic to be prioritized according to your requirements. For example, you typically assign the highest priority to voice traffic, since this type of traffic requires delay to be under 10 ms. The Array has four separate queues for handling wireless traffic at different priorities, and thus it supports four traffic classes (QoS levels).

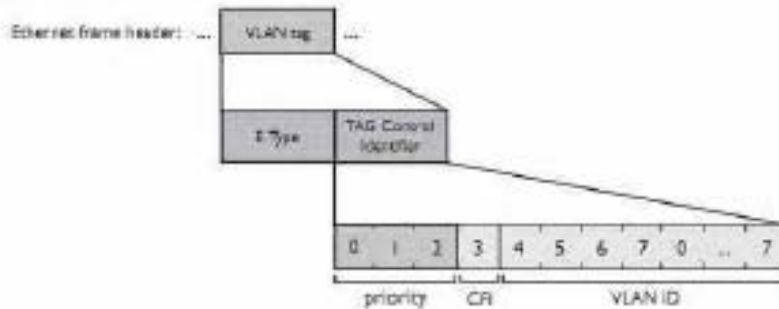


Figure 135. Priority Level—IEEE 802.1p (Layer 2)

IEEE802.1p uses three bits in an Ethernet frame header to define eight priority levels at the MAC level (Layer 2) for wired networks. Each data packet may be tagged with a priority level, i.e., a **user priority tag**. Since there are eight possible user priority levels and the Array implements four wireless QoS levels, user priorities are mapped to QoS as described below.

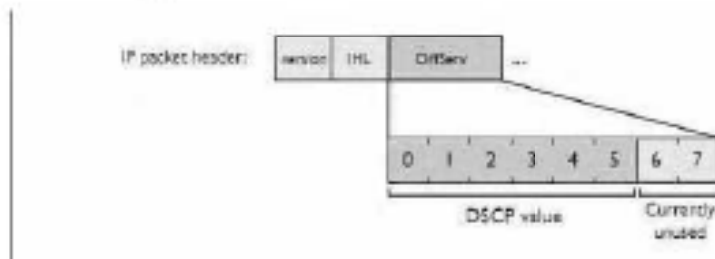


Figure 136. Priority Level—DSCP (DiffServ - Layer 3)

DSCP (Differentiated Services Code Point or DiffServ) uses 6 bits in the IPv4 or IPv6 packet header, defined in [RFC2474](#) and [RFC2475](#). The DSCP value classifies

a Layer 3 packet to determine the Quality of Service (QoS) required. DSCP replaces the outdated Type of Service (TOS) field.

The description below describes how both of these priority levels are mapped to the Array's four traffic classes.

#### End-to-End QoS Handling

- Wired QoS - Ethernet Port:

Ingress: Incoming wired packets are assigned QoS priority based on their SSID and 802.1p tag (if any), as shown in the table below. This table follows the mapping recommended by IEEE802.11e.

| FROM<br>Priority Tag<br>802.1p (Wired) | TO<br>Array QoS<br>(Wireless) | Typical Use  |
|--|-------------------------------|--|
| 0                                      | 0 (Lowest priority)           | Best Effort  |
| 1                                      | 1                             | Background—explicitly designated as low-priority and non-delay sensitive |
| 2                                      | 1                             | Spare  |
| 3                                      | 0                             | Excellent Effort   |
| 4                                      | 2                             | Controlled Load  |
| 5                                      | 2                             | Video  |
| 6                                      | 3                             | Voice - requires delay <10ms   |
| 7 (Highest priority)                   | 3 (Highest priority)          | Network control  |



- **Egress:** Outgoing wired packets are IEEE 802.1p tagged at the Ethernet port for upstream traffic, thus enabling QoS at the edge of the network.

| FROM<br>Array QoS (Wireless) | TO<br>Priority Tag 802.1p (Wired) |
|------------------------------|-----------------------------------|
| 1 (Lowest priority)          | 1                                 |
| 0                            | 0                                 |
| 2 (Default)                  | 5                                 |
| 3 (Highest priority)         | 6                                 |

#### Wireless QoS - Radios:

- Each SSID can be assigned a separate QoS priority (i.e., traffic class) from 0 to 3, where 3 is highest priority and 2 is the default. See “SSID Management” on page 249. If multiple SSIDs are used, packets from the SSID with higher priority are transmitted first.
- The Array supports IEEE802.11e Wireless QoS for downstream traffic. Higher priority packets wait a shorter time before gaining access to the air and contend less with all other 802.11 devices on a channel.
- How QoS is set for a packet in case of conflicting values:
  - a. If an SSID has a QoS setting, and an incoming wired packet’s user priority tag is mapped to a higher QoS value, then the higher QoS value is used.
  - b. If a group or filter has a QoS setting, this overrides the QoS value above. See “Groups” on page 264, and “Filters” on page 344.
  - c. Voice packets have the highest priority (see [Voice Support](#), below).
  - d. If **DSCP to QoS Mapping Mode** is enabled, the IP packet is mapped to QoS level 0 to 3 as specified in the [DSCP Mappings](#) table. This value overrides any of the settings in cases a to c above.

In particular, by default:

- DSCP 8 is set to QoS level 1.

- DSCP 40 is typically used for video traffic and is set to QoS level 2.
- DSCP 48 is typically used for voice traffic and is set to QoS level 3—the highest level
- All other DSCP values are set to QoS level 0 (the lowest level—Best Effort).

#### Packet Filtering QoS classification

- Filter rules can be used to redefine the QoS priority level to override defaults. See [“Filter Management” on page 347](#). This allows the QoS priority level to be assigned based on protocol, source, or destination.

#### Voice Support

- The QoS priority implementation on the Array give voice packets the highest priority to support voice applications.

#### High Density 2.4G Enhancement—Honeypot SSID

Some situations pose problems for all wireless APs. For example, iPhones will remember every SSID and flood the airwaves with probes, even when the user doesn't request or desire this behavior. In very high density deployments, these probes can consume a significant amount of the available wireless bandwidth.

The Array offers a feature targeting this problem—a “honeypot” SSID. Simply create an SSID named **honeypot** on the Array. Once this SSID is created and enabled, it will respond to any station probe looking for an open (unencrypted) SSID that is not configured on the Array.

Traffic for a station connected to the honeypot SSID may be handled in a various ways:

- it may be directed to WPR to display a splash page or offer the user the opportunity to sign in to your service (see [“Web Page Redirect Configuration Settings” on page 255](#));
- it may be filtered;
- or it may be dead-ended by defining a specific dead-end VLAN on the honeypot SSID to “trap” stations.