

write privileges on the Array (i.e., the new user will be able to change the configuration of the Array). The default **admin** user is deleted.

- b. New Admin Password:** If desired, enter a new administration password for managing this Array. Choose a password that is not obvious, and one that you can remember. If you forget your password, you must reset the Array to its factory defaults so that the password is reset to **admin** (its default setting).
 - c. Confirm Admin Password:** If you entered a new administration password, confirm the new password here.
- 10. Time and Date Settings:** This section specifies an optional time (NTP - Network Time Protocol) server or modifies the system time if you're not using a server.
 - a. Time Zone:** Select your time zone from the choices available in the pull-down list.
 - b. 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).
 - c. Use Network Time Protocol:** Check this box if you want to use an [NTP](#) server to synchronize the Array's clock. This ensures that Syslog time-stamping is maintained across all units. Without an NTP server assigned (no universal clock), each Array will use its own internal clock and stamp times accordingly, which may result in discrepancies. If you check **Yes**, the NTP server fields are displayed. If you don't want to use an NTP server, leave this box unchecked (default) and set the system time on the Array manually.
 - d. NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.
 - 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.

- f. **Set 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).
- g. **Set 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).

11. 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.

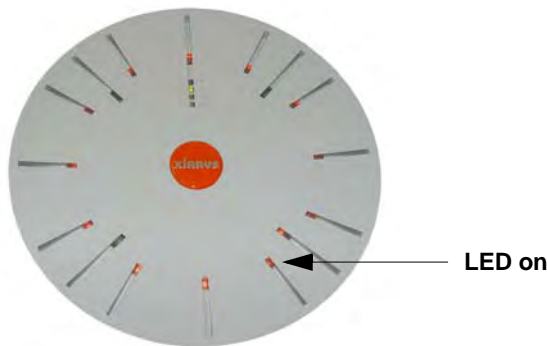


Figure 88. LEDs are Switched On

- 12. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

This ends the Express Setup procedure.

Network

This is a status only window that provides a snapshot of the configuration settings currently established for the 10/100 Ethernet 0 interface and the Gigabit 1 and Gigabit 2 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.

XS-3900 Wi-Fi Array

Status Uptime - 2 days, 3 hours, 3 minutes

Interface Settings Summary								
Interface	Status	Link	Port Mode	DHCP	IP Address	Subnet Mask	Gateway	
10/100 Ethernet 0	Enabled	down		Enabled	10.0.1.1	255.255.255.0		
Gigabit Ethernet 1	Enabled	up	link-backup	Enabled	192.168.36.200	255.255.255.0	192.168.36.1	
Gigabit Ethernet 2	Enabled	down	link-backup	Enabled	192.168.36.200	255.255.255.0	192.168.36.1	

DNS Settings Summary				
Hostname	Domain	DNS Server 1	DNS Server 2	DNS Server 3
SS-Array	xirrus.com	192.168.39.13	192.168.39.7	

CDP Settings Summary		
State	Interval	Hold Time
Enabled	60	180

Figure 89. Network Interfaces

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

- [“Network Interfaces” on page 141](#)
- [“DNS Settings” on page 148](#)
- [“CDP Settings” on page 149](#)

See Also

[DNS Settings](#)

[Network Interfaces](#)

[Network Status Windows](#)

[Spanning Tree Status](#)

[Network Statistics](#)

Network Interfaces

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

Status		Uptime - 1 day, 23 hours, 20 minutes	
<ul style="list-style-type: none"> ▶ Array ▶ Network ▶ RF Monitor ▶ Stations ▶ Statistics ▶ System Log Configuration <ul style="list-style-type: none"> Express Setup ▼ Network <ul style="list-style-type: none"> Interfaces <ul style="list-style-type: none"> DNS CDP ▶ Services ▶ VLANs ▶ Security ▶ SSIDs ▶ Groups ▶ IAPs ▶ WDS ▶ Filters Tools <ul style="list-style-type: none"> System Tools CLI Logout 	10/100 Ethernet 0 Settings		
	Enable Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	Auto Negotiate:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	Duplex:	<input checked="" type="radio"/> Full	<input type="radio"/> Half
	Speed:	100 Megabit	
	Configuration Server Protocol:	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
	IP Address:	10.0.1.1	
	IP Subnet Mask:	255.255.255.0	
	Default Gateway:		
	Static route (IP Address/Mask):	192.168.39.0 / 255.255.255.0	
	Gigabit Ethernet 1 Settings		
	Enable Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	LED Indicator:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
	Allow Management On Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	Auto Negotiate:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	Duplex:	<input checked="" type="radio"/> Full	<input type="radio"/> Half
	Speed:	Gigabit	
	Port Mode:	Active backup (gig1/2 fail over to each other)	
	Configuration Server Protocol:	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
	IP Address:	192.168.36.200	
	IP Subnet Mask:	255.255.255.0	
	Default Gateway:	192.168.36.1	
	Gigabit Ethernet 2 Settings		
	Enable Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	LED Indicator:	<input checked="" type="radio"/> Enabled	<input type="radio"/> Disabled
	Allow Management On Interface:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	Auto Negotiate:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
	Duplex:	<input checked="" type="radio"/> Full	<input type="radio"/> Half
	Speed:	Gigabit	
	Port Mode:	Active backup (gig1/2 fail over to each other)	
	Configuration Server Protocol:	<input checked="" type="radio"/> DHCP	<input type="radio"/> Static
	IP Address:	192.168.36.200	
	IP Subnet Mask:	255.255.255.0	
	Default Gateway:	192.168.36.1	
		<input type="button" value="Apply"/>	<input type="button" value="Save"/>

● Critical Msgs: 4
● Warning Msgs: 1
● General Msgs: 184

Figure 90. Network Settings



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

When finished making changes, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

Network Interface Ports

The following diagram shows the location of each network interface port on the underside of the Array.

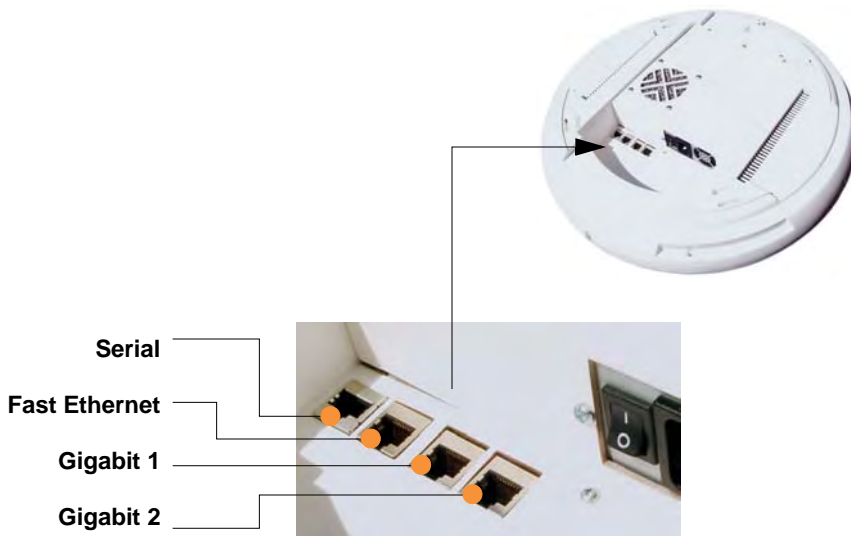


Figure 91. Network Interface Ports

Procedure for Configuring the Network Interfaces

Configure the **Fast Ethernet** and **Gigabit 1** network interfaces (some **Gigabit 2** settings cannot be configured separately and will mirror **Gigabit 1**). The fields for each of these interfaces are the same, and include:

1. **Enable Interface:** Choose **Yes** to enable this network interface (Fast Ethernet, Gigabit 1 or Gigabit 2), 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. 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).
 - a. **Duplex:** Data is transmitted 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. **Speed:** If the Auto-Negotiate feature is disabled, you can manually choose the desired data transmission speed from the pull-down list. If configuring the Fast Ethernet interface the options are **10 Megabit** or **100 Megabit**. If configuring the Gigabit 1 or Gigabit 2 interfaces the options are **100 Megabit** or **Gigabit**.
5. **Port mode:** Select the desired behavior for the gigabit Ethernet ports from the following options:
 - a. **Active Backup (gig1/gig2 failover to each other)**—This mode provides fault tolerance and is the default mode. Gigabit 1 acts as the primary link. Gigabit2 is the backup link and is passive. Gigabit2 assumes the IP properties of Gigabit1. If Gigabit 1 fails the Array

automatically fails over to Gigabit2. When a failover occurs in this mode, Gigabit2 issues gratuitous ARPs to allow it to substitute for Gigabit1 at Layer 3 as well as Layer 2. See [Figure 92 \(a\)](#).

- b. Aggregate Traffic from gig1 & gig2 using 802.3ad**—The Array sends network traffic across both gigabit ports to increase link speed to the network. Both ports act as a single logical interface (trunk), using a load balancing algorithm to balance traffic across the ports. The destination IP address of a packet is used to determine its outgoing adapter. For non-IP traffic (such as ARP), the last byte of the destination MAC address is used to do the calculation. The network switch must also support 802.3ad. If a port fails, the trunk degrades gracefully—the other port still transmits. See [Figure 92 \(b\)](#).

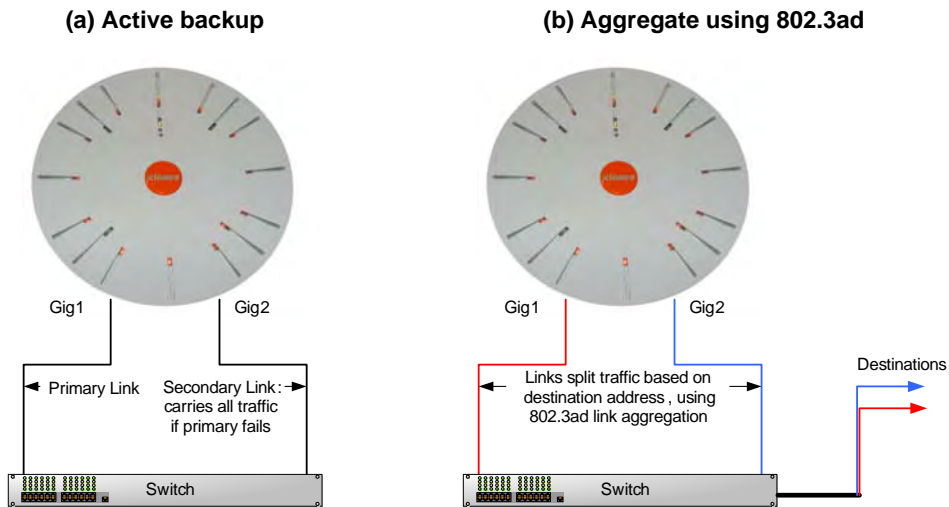


Figure 92. Port Modes (a-b)

- c. Bridge traffic between gig1 & gig2**—Traffic received on Gigabit1 is transmitted by Gigabit2; similarly, traffic received on Gigabit2 is transmitted by Gigabit1. This allows the Array to act as a wired bridge and allows Arrays to be daisy-chained and still maintain wired connectivity. See [Figure 93 \(c\)](#).

- d. **Transmit Traffic on both gig1 & gig2**—Transmits incoming traffic on both Gigabit1 and Gigabit2. Any traffic received on Gigabit1 or Gigabit2 is sent to the onboard processor. This mode provides fault tolerance. See [Figure 93](#) (d).

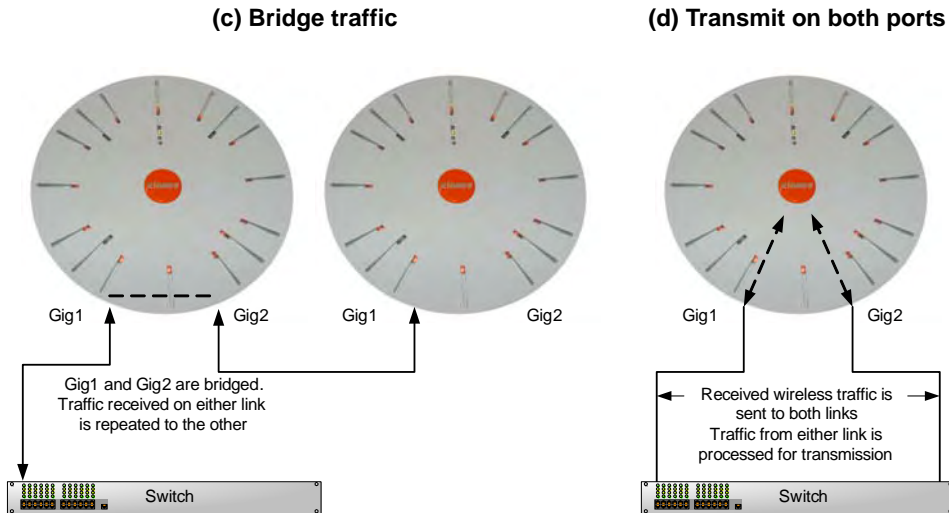
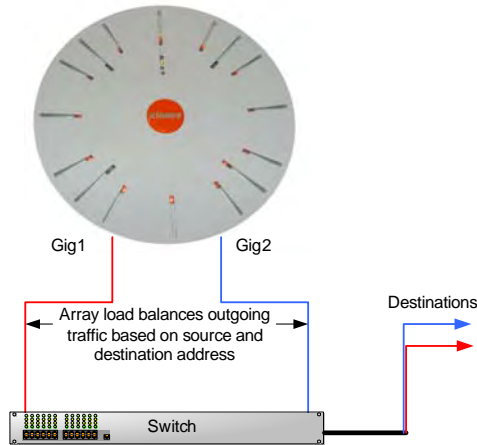


Figure 93. Port Modes (c-d)

- e. **Load balance traffic between gig1 & gig2**—This option provides trunking, similar to option (b)—**Aggregate Traffic from gig1 & gig2 using 802.3ad**, but it uses a different load balancing algorithm to determine the outgoing gigabit port. The outgoing port used is based on an exclusive OR of the source and destination MAC address. Like option (b), this mode also provides load balancing and fault tolerance. See [Figure 94](#) (e).
- f. **Mirror traffic on both gig1 & gig2**—all traffic received on the Array is transmitted out both Gigabit1 and Gigabit2. All traffic received on Gigabit1 is passed on to the onboard processor as well as out Gigabit2. All traffic received on Gigabit2 is passed on to the onboard processor as well as out Gigabit1. This allows a network analyzer to be plugged into one port to capture traffic for troubleshooting, while

the other port provides network connectivity for data traffic. See Figure 94 (f).

(e) Load balance traffic



(f) Mirror traffic

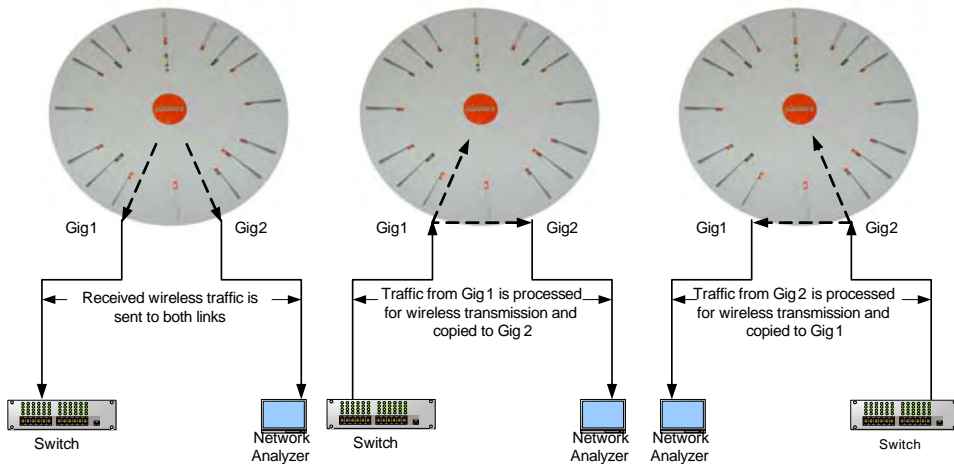


Figure 94. Port Modes (e-f)

6. **Configuration Server Protocol:** Choose **DHCP** to instruct the Array to use **DHCP** when assigning IP addresses to the Array, or choose **Static IP** if you intend to enter IP addresses manually. If you select the Static IP option you must specify the IP address, IP subnet mask and default gateway.
 - a. **IP Address:** If you selected the Static IP option, enter a valid IP address for the Array. To use any of the remote connections (Web, **SNMP**, or SSH), a valid IP address must be established.
 - b. **IP Subnet Mask:** If you selected the Static IP option, enter a valid IP address for the **subnet mask** (the default for Class C is 255.255.255.0). The subnet mask defines the number of IP addresses that are available on the routed subnet where the Array is located.
 - 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 transmit data to other networks.
7. **Static Route (IP Address/Mask):** (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.
8. When done configuring all interfaces as desired, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

[DNS Settings](#)

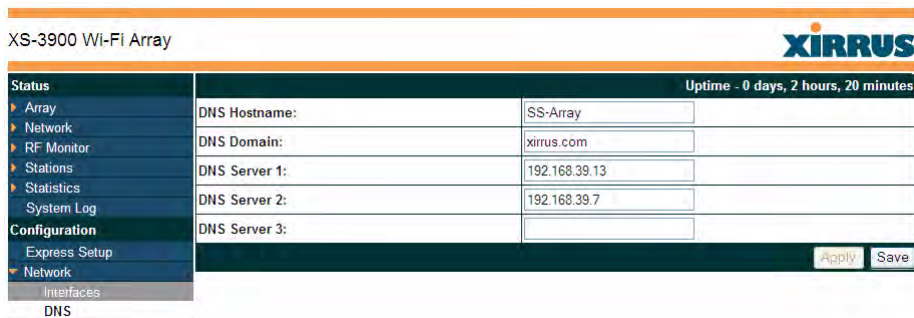
[Network](#)

[Network Statistics](#)

[Spanning Tree Status](#)

DNS Settings

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



XS-3900 Wi-Fi Array		XIRRUS	
Status		Uptime - 0 days, 2 hours, 20 minutes	
▶ Array	DNS Hostname:	<input type="text" value="SS-Array"/>	
▶ Network	DNS Domain:	<input type="text" value="xirrus.com"/>	
▶ RF Monitor	DNS Server 1:	<input type="text" value="192.168.39.13"/>	
▶ Stations	DNS Server 2:	<input type="text" value="192.168.39.7"/>	
▶ Statistics	DNS Server 3:	<input type="text"/>	
System Log			
Configuration			
Express Setup			
▼ Network			<input type="button" value="Apply"/> <input type="button" value="Save"/>
Interfaces			
DNS			

Figure 95. 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. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

[Network](#)

[Network Interfaces](#)

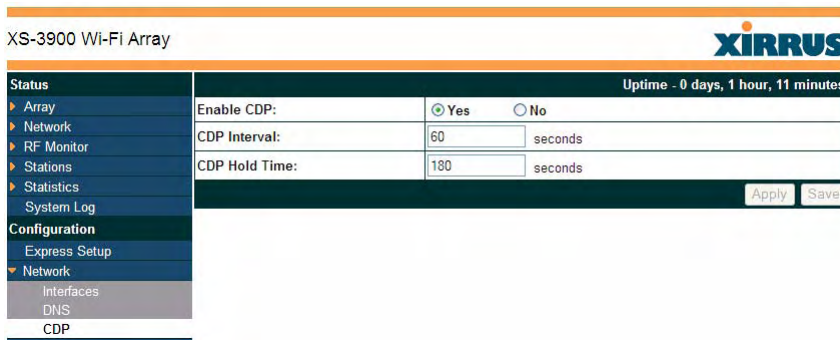
[Network Statistics](#)

[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. Wi-Fi Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors (see “CDP Neighbors” on page 103).

This window allows you to establish your CDP settings. When finished, click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.



XS-3900 Wi-Fi Array		XIRRUS	
Status Array Network RF Monitor Stations Statistics System Log		Uptime - 0 days, 1 hour, 11 minutes	
Configuration Express Setup Network Interfaces DNS CDP		Enable CDP:	<input checked="" type="radio"/> Yes <input type="radio"/> No
		CDP Interval:	60 seconds
		CDP Hold Time:	180 seconds
		<input type="button" value="Apply"/> <input type="button" value="Save"/>	

Figure 96. 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.

XS-3900 Wi-Fi Array

Status	Uptime - 2 days, 3 hours, 7 minutes							
▶ Array	Time Settings Summary							
▶ Network	NTP Server Status		NTP Server 1 Address		NTP Server 2 Address			
▶ RF Monitor	Disabled		time.nist.gov		pool.ntp.org			
▶ Stations	System Log Settings Summary							
▶ Statistics	Syslog Server Status			Enabled				
▶ System Log	Console Logging			Disabled				
Configuration	Local File			500 lines				
▶ Express Setup	Primary Server			0.0.0.0				
▶ Network	Secondary Server			0.0.0.0				
Services	Email SMTP Server			Level 4 and lower (Warning and more serious)				
▶ Time	SNMP Settings Summary							
▶ System Log	SNMP Status	Trap Auth Failures		Trap Host IP 1	Trap Host IP 2	Trap Host IP 3	Trap Host IP 4	
▶ SNMP	Enabled	Enabled						
▶ DHCP Server	R/O Community String	R/W Community String		Trap Port 1	Trap Port 2	Trap Port 3	Trap Port 4	
▶ VLANs	*****	*****		162	162	162	162	
▶ Security	DHCP Server Settings							
▶ SSIDs	DHCP Name	State	NAT	IP Range/Mask	IP Gateway	Default Lease	Maximum Lease	DNS Domain
▶ Groups	pool1	on	off	192.168.1.2 - 192.168.1.254 /255.255.255.0	192.168.1.1	300	300	whatsamattaU
▶ IAPs	Tools							
▶ WDS								
▶ Filters								

Figure 97. Services

The following sections discuss configuring services on the Array:

- “Time Settings (NTP)” on page 152
- “System Log” on page 154
- “SNMP” on page 157
- “DHCP Server” on page 158

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. Synchronizing the Array's clock with an NTP server ensures that Syslog time-stamping is maintained across all units.

Figure 98. Time Settings (Manual Time)

Procedure for Managing the Time Settings

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

- b. **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).
5. **Using an NTP Server**
- a. **NTP Primary Server:** If you are using NTP, enter the IP address or domain name of the NTP server.

Uptime - 0 days, 1 hour, 27 minutes	
TimeZone:	(GMT - 08:00) Pacific Time (US & Canada); Tijuana
Auto Adjust Daylight Savings:	<input type="checkbox"/>
Use Network Time Protocol:	<input checked="" type="radio"/> Yes <input type="radio"/> No
NTP Primary Server:	time.nist.gov
NTP Secondary Server:	pool.ntp.org
<input type="button" value="Apply"/> <input type="button" value="Save"/>	

Figure 99. Time Settings (NTP Time Enabled)

- b. **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.
6. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Services

SNMP

System Log

System Log

This window allows you to enable or disable the Syslog server, define a primary and secondary server, set up email notification, and set the level for Syslog reporting for each of the servers and for email notification—the Syslog service will send Syslog messages that are at the selected severity or above to the defined Syslog servers and email address.

XS-3900 Wi-Fi Array		Uptime - 0 days, 1 hour, 46 minutes
Status	Enable Syslog Server:	<input checked="" type="radio"/> Yes <input type="radio"/> No
▶ Array	Console Logging:	<input type="radio"/> Yes <input checked="" type="radio"/> No
▶ Network	Local File Size (1-500):	<input type="text" value="500"/>
▶ RF Monitor	Primary Server Address (Domain or IP):	<input type="text"/>
▶ Stations	Secondary Server Address (Domain or IP):	<input type="text"/>
▶ Statistics	Email SMTP Address (Domain or IP):	<input type="text"/>
▶ System Log	Email SMTP User:	<input type="text"/>
Configuration	Email SMTP Password:	<input type="text"/>
▶ Express Setup	Email SMTP From:	<input type="text"/>
▶ Network	Email SMTP To:	<input type="text"/>
▶ Services	Syslog Levels	
Time	Console Logging:	Information and more serious ▼
System Log	Local File:	Information and more serious ▼
SNMP	Primary Server:	Information and more serious ▼
Standby Mode	Secondary Server:	Information and more serious ▼
DHCP Server	Email SMTP Server:	Warning and more serious ▼
▶ VLANs		
▶ Security		
▶ SSIDs		
▶ IAPs		
▶ WDS		
▶ Filters		
Tools		
System Tools		

Figure 100. System Log

Procedure for Configuring Syslog

- 1. Enable Syslog Server:** Choose **Yes** to enable Syslog functionality, or choose **No** to disable this feature.
- 2. Console Logging:** If you enabled Syslog, select whether or not to echo Syslog messages to the console as they occur. If you enable console logging, be sure to set the Console Logging level (see [Step 7](#) below).
- 3. Local File Size (1-500):** 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 500.

4. **Primary Server Address (Domain or IP):** If you enabled Syslog, enter the domain name or IP address of the primary Syslog server.
5. **Secondary Server Address (Domain or IP):** If you enabled Syslog, you may enter the domain name or IP address of another Syslog server to which messages will also be sent. (Optional)
6. **Email Notification:** 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 SMTP Address (Domain or IP):** The domain name 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.
 - b. **Email SMTP User/Email SMTP Password:** Specify a user name and password for logging in to an account on the mail server designated in [Step a](#).
 - c. **Email SMTP From:** Specify the “From” email address to be displayed in the email.
 - d. **Email SMTP To:** Specify the entire email address of the recipient of the email notification.
7. **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 Server:** Choose the preferred level of reporting for the secondary 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 you mailbox from being filed up with a large number of less severe messages such as informational messages.
8. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

System Log Window

Services

SNMP

Time Settings (NTP)

SNMP

This window allows you to enable or disable SNMP and define the SNMP parameters. SNMP allows remote management of the Array by the Xirrus Management System (XMS).

*NOTE: If you are managing your Arrays with XMS (the Xirrus Management System), it is very important to use the correct **Read-Write Community String** for proper operation of XMS with the Array. Both XMS and the Array must have the same value for this string.*

XS-3900 Wi-Fi Array

Status	Uptime - 0 days, 1 hour, 49 minutes		
▶ Array	Enable SNMP:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
▶ Network	SNMP Read-Only Community String:	*****	
▶ RF Monitor	SNMP Read-Write Community String:	*****	
▶ Stations	SNMP Trap Host 1 IP Address:	<input type="text" value="192.168.100.100"/>	Port: <input type="text" value="162"/>
▶ Statistics	SNMP Trap Host 2 IP Address:	<input type="text"/>	Port: <input type="text" value="162"/>
▶ System Log	SNMP Trap Host 3 IP Address:	<input type="text"/>	Port: <input type="text" value="162"/>
Configuration	SNMP Trap Host 4 IP Address:	<input type="text"/>	Port: <input type="text" value="162"/>
▶ Express Setup	Send Auth Failure Traps:	<input checked="" type="radio"/> Yes	<input type="radio"/> No
▶ Network	<input type="button" value="Apply"/> <input type="button" value="Save"/>		
▼ Services			
Time			
System Log			
SNMP			

Figure 101. SNMP

Procedure for Configuring SNMP

1. **Enable SNMP:** Choose **Yes** to enable SNMP functionality, or choose **No** to disable this feature. When used in conjunction with the Xirrus Management System, SNMP must be enabled on each Array. The default for this feature is Yes (enabled).
2. **SNMP Read-Only Community String:** Enter the read-only community string. The default is `xirrus_read_only`.
3. **SNMP Read-Write Community String:** Enter the read-write community string. The default is `xirrus`.
4. **SNMP Trap Host IP Address:** Enter the IP address of an SNMP management station that is to receive SNMP traps. You may specify up to four hosts that are to receive traps.

5. **SNMP Trap Port:** Enter the trap port for each trap host that you entered. The default is port 162.
6. **Send Auth Failure Traps:** Choose **Yes** to log authentication failure traps or **No** to disable this feature.
7. Click on the **Apply** button to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

Services

System Log

Time Settings (NTP)

DHCP Server

This window allows you to create, modify and delete **DHCP** (Dynamic Host Configuration Protocol) pools and enable or disable DHCP server functionality. DHCP allows the Array to provide wireless clients with IP addresses and other networking information. The DHCP server will not provide DHCP services to the wired side of the network.

If you enable the DHCP server, you need to define the **DHCP lease** time (default and maximum) and establish the IP address range that the DHCP server can use.

The screenshot shows a web interface for DHCP Management. At the top right, it displays 'Uptime - 2 days, 3 hours, 26 minutes'. Below this is a 'New DHCP Pool' section with a text input field and a 'Create' button. The main part of the interface is a table with the following columns: DHCP Pool, On, Lease Time (Default, Max), NAT, Lease IP Range (Start, End), Subnet Mask, Gateway, Domain, DNS Servers, and Delete. Two rows are visible: 'pool1' and 'pool2'. 'pool1' has 'On' checked, lease times of 300, NAT unchecked, IP range 192.168.1.2 to 192.168.1.254, subnet mask 255.255.255.0, gateway 192.168.1.1, domain 'whatsamattaU', and DNS server '192.168.1.1'. 'pool2' has 'On' unchecked, lease times of 300, NAT unchecked, IP range 192.168.2.2 to 192.168.2.254, and subnet mask 255.255.255.0. At the bottom right, there are 'Apply' and 'Save' buttons.

DHCP Pool	On	Lease Time		NAT	Lease IP Range		Subnet Mask	Gateway	Domain	DNS Servers	Delete
		Default	Max		Start	End					
pool1	<input checked="" type="checkbox"/>	300	300	<input type="checkbox"/>	192.168.1.2	192.168.1.254	255.255.255.0	192.168.1.1	whatsamattaU	192.168.1.1	<input type="checkbox"/>
pool2	<input type="checkbox"/>	300	300	<input type="checkbox"/>	192.168.2.2	192.168.2.254	255.255.255.0				<input type="checkbox"/>

Figure 102. DHCP 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 also, “DNS Settings” on page 148.
11. **DNS Servers (1 to 3):** Enter the IP address of the primary DNS server, secondary DNS server and tertiary DNS server. See also, “DNS Settings” on page 148.
12. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them 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 assigned VLANs. A VLAN (Virtual LAN) is comprised of a group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

In addition to listing all VLANs, this window shows your settings for the Default Route VLAN and the Native (Untagged) VLAN ([Step 1 page 162](#)).

XS-3900 Wi-Fi Array **XIRRUS**

Uptime - 0 days, 2 hours, 28 minutes

Status

- ▶ Array
- ▶ Network
- ▶ RF Monitor
- ▶ Stations
- ▶ Statistics
- ▶ System Log

Configuration

- ▶ Express Setup
- ▶ Network
- ▶ Services
- ▼ **VLANs**
 - VLAN Management

Default Route VLAN:						
Native (Untagged):						
VLAN Name	Number	Management	DHCP	IP Address	Subnet Mask	Gateway
Voice	5	disallowed	disabled	10.10.10.2	255.255.255.0	10.10.10.1
Video	101	disallowed	enabled			

Figure 103. VLANs

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.

XS-3900 Wi-Fi Array **XIRRUS**

Status Uptime - 2 days, 4 hours, 4 minutes

Default Route: (none) VLAN Number:
 Native VLAN: (none) VLAN Number:

VLAN Name	Number	Management	DHCP	IP Address	Subnet Mask	Gateway	Delete
<input type="text"/>	<input type="text"/>	<input type="button" value="Create"/>					
VLAN-Voice	5	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/>

VLAN Management

Figure 104. VLAN Management



The Wi-Fi 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 67 on page 112)

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 allows you to choose a default VLAN route from the pull-down list. When you click **Apply** the VLAN you choose will appear in the corresponding VLAN Number field. The IP Gateway must be established for this function to work.

2. **Native VLAN:** This option allows you to choose the Native VLAN from the pull-down list. When you click **Apply** the VLAN you choose will appear in the corresponding VLAN Number field.
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 (1-4095).
5. **Management:** Check this box if you want to allow management over this VLAN.
6. **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.
7. **IP Address:** If the DHCP option is disabled, enter a valid IP address for this VLAN association.
8. **Subnet Mask:** If the DHCP option is disabled, enter the subnet mask IP address for this VLAN association.
9. **Gateway:** If the DHCP option is disabled, enter the IP gateway address for this VLAN association.
10. **Delete:** To delete the selected VLAN, simply click the **Delete** button to remove the VLAN from the list.
11. Click **Apply** to apply the new settings to this session, or click **Save** to apply your changes and make them permanent.

See Also

VLAN Statistics

VLANs

Security

This status-only window allows you to review the Array's security parameters. It includes the assigned network administration accounts, Access Control List (ACL) values, management settings, encryption and authentication protocol settings, and RADIUS configuration settings. There are no configuration options available in this window, but if you are experiencing issues with security, you may want to print this window for your records.

XS-3900 Wi-Fi Array		XIRRUS	
Status		Uptime - 2 days, 4 hours, 16 minutes	
Array	Administration		
Network	Accounts	Full Access	Read Only
RF Monitor	1	1	0
Stations	Access Control List		
Statistics	Enabled	Entries	List Type
System Log	No	0	N/A
Configuration		Management Control	
Express Setup	SSH Enabled	Telnet Enabled	HTTPS Enabled
Network	Yes	No	Yes
Services	Global Security		
VLANs	TKIP Enabled	AES Enabled	PSK Enabled
Security	Yes	Yes	No
Admin Management	Radius		
Management Control	Server In Use	External Primary Server	External Primary Port
Access Control List	external		1812
Global Settings			Internal Radius Users
External Radius			0
Internal Radius			
Rogue Control List			

Figure 105. Security

For additional information about wireless network security, refer to:

- “Security Planning” on page 42
- “Understanding Security” on page 165
- The Security section of “Frequently Asked Questions” on page 334.

Security settings are configured with the following windows:

- “Admin Management” on page 168
- “Management Control” on page 169
- “Access Control List” on page 172
- “Global Settings” on page 174

- [“External Radius” on page 177](#)
- [“Internal Radius” on page 180](#)
- [“Rogue Control List” on page 182](#)

Understanding Security

The Xirrus Wi-Fi 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). See also, [“Character Restrictions” on page 89](#). When appropriate, issue read only administrator accounts.

Other security considerations include:

- **SSH versus Telnet:** Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit’s Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY.
- **Configuration auditing:** The optional Xirrus Management System (XMS) offers powerful management features for small or large Xirrus Wi-Fi 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 189). 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 174).

- **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: