

filter

The **filter** command [**Xirrus_Wi-Fi_Array(config-filter)#**] is used to manage protocol filters and filter lists.

Command	Description
add	Add a filter. FORMAT: filter add [name]
add-list	Add a filter list. FORMAT: filter add-list [name]
del	Delete a filter. FORMAT: filter del [name]
del-list	Delete a filter list. FORMAT: filter del-list [name]
edit	Edit a filter. FORMAT: filter edit [name type]
edit-list	Edit a filter list FORMAT: filter edit-list [name type]
enable	Enable a filter list. FORMAT: filter enable
move	Change a filter priority. FORMAT: filter move [name priority]

Command	Description
off	Disable a filter list. FORMAT: filter off
on	Enable a filter list. FORMAT: filter on
reset	Delete all protocol filters and filter lists. FORMAT: filter reset

fips

The **fips** command [Xirrus_Wi-Fi_Array(config)# **fips**] is used to set the parameter values required for FIPS 140-2, Level 2 security. For more information, see [Appendix E: Implementing FIPS Security](#).

Command	Description
disable	Reverts FIPS settings to the values they had before performing a fips on command. FORMAT: fips disable
enable	Set FIPS security on the Array. Remembers the values of parameters prior to setting them. FORMAT: fips enable
off	Reverts FIPS settings to the values they had before performing a fips on command. FORMAT: fips off
on	Set FIPS security on the Array. Remembers the values of parameters prior to setting them. FORMAT: fips on

group

The **group** command [Xirrus_Wi-Fi_Array(config)# **group**] is used to create and configure user groups. User groups allow administrators to assign specific network parameters to users through RADIUS privileges rather than having to map users to a specific SSID. Groups provide flexible control over user privileges without the need to create large numbers of SSIDs. For more information, see “Groups” on page 247.

Command	Description
add	Create a new user group. FORMAT: group add [group-name]
del	Delete a user group. FORMAT: group del [group-name]
edit	Set parameters values for a group. FORMAT: group edit [group-name]
reset	Reset the group. FORMAT: group reset

hostname

The **hostname** command [Xirrus_Wi-Fi_Array(config)# **hostname**] is used to change the hostname used by the Array.

Command	Description
hostname	Change the hostname of the Array. FORMAT: hostname [name]

https

The **https** command [Xirrus_Wi-Fi_Array(config)# **https**] is used to enable or disable the Web Management Interface (https), which is enabled by default. It also allows you to establish a timeout for your Web management session.

Command	Description
disable	Disable the https feature. FORMAT: https disable
enable	Enable the https feature. FORMAT: https enable
off	Disable the https feature. FORMAT: https off
on	Enable the https feature. FORMAT: https on
timeout	Define an elapsed period (in seconds) after which the Web Management Interface will time out. FORMAT: https timeout 5000

interface

The **interface** command [**Xirrus_Wi-Fi_Array(config)# interface**] is used to select the interface that you want to configure. To see a listing of the commands that are available for each interface, use the **?** command at the selected interface prompt. For example, using the **?** command at the **Xirrus_Wi-Fi_Array(config-gig1)#** prompt displays a listing of all commands for the **gig1** interface.

Command	Description
console	Select the console interface. The console interface is used for management purposes only. FORMAT: interface console
eth0	Select the Fast Ethernet interface. The Fast Ethernet interface is used for management purposes only. FORMAT: interface eth0 Note: To configure a static route for management traffic, next enter: static-route addr [ip-addr] static-route mask [subnet-mask]
gig1	Select the Gigabit 1 interface. FORMAT: interface gig1
gig2	Select the Gigabit 2 interface. FORMAT: interface gig2
iap	Select an IAP. FORMAT: interface iap

license

The **license** command [**Xirrus_Wi-Fi_Array(config)# license**] is used to set the license key for the Array. A valid license is required for Array operation, and it controls the features available on the Array.

Command	Description
<cr>	Set the license for the Array. FORMAT: license <license-key> When you enter the new key obtained from Xirrus, simply hit the Enter key <cr> to apply it.

load

The **load** command [**Xirrus_Wi-Fi_Array(config)# load**] loads a configuration file.

Command	Description
factory.conf	Load the factory settings configuration file. FORMAT: load [factory.conf]
lastboot.conf	Load the configuration file from the last boot-up. FORMAT: load [lastboot.conf]
[myfile].conf	If you have saved a configuration, enter its name to load it. FORMAT: load [myfile.conf]
saved.conf	Load the configuration file with the last saved settings. FORMAT: load [saved.conf]

location

The **location** command [**Xirrus_Wi-Fi_Array(config)# location**] is used to set the location for the Array.

Command	Description
<cr>	Set the location for the Array. FORMAT: location [newlocation]

management

The **management** command [**Xirrus_Wi-Fi_Array(config)# management**] enters management mode, where you may configure console management parameters.

Command	Description
<cr>	Enter management mode. FORMAT: management <cr>

more

The **more** command [**Xirrus_Wi-Fi_Array(config)# more**] is used to turn terminal pagination ON or OFF.

Command	Description
off	Turn OFF terminal pagination. FORMAT: more off
on	Turn ON terminal pagination. FORMAT: more on

netflow

The **netflow** command [**Xirrus_Wi-Fi_Array(config-netflow)#**] is used to enable or disable, or configure sending IP flow information (traffic statistics) to the collector you specify.

Command	Description
disable	Disable netflow. FORMAT: netflow disable
enable	Enable netflow. FORMAT: netflow enable
off	Disable netflow. FORMAT: netflow off
on	Enable netflow. FORMAT: netflow on
collector	Set the netflow collector IP address or fully qualified domain name (host.domain). Only one collector may be set. If port is not specified, the default is 2055. FORMAT: netflow collector host {<ip-addr> <domain>} [port <port#>]

no

The **no** command [Xirrus_Wi-Fi_Array(config)# **no**] is used to disable a selected element or set the element to its default value.

Command	Description
acl	Disable the Access Control List. FORMAT: no acl
dot11a	Disable all 802.11a(n) IAPs (radios). FORMAT: no dot11a
dot11bg	Disable all 802.11bg(n) IAPs (radios). FORMAT: no dot11bg
https	Disable https access. FORMAT: no https
intrude-detect	Disable intrusion detection. FORMAT: no intrude-detect
management	Disable management on all Ethernet interfaces. FORMAT: no management
more	Disable terminal pagination. FORMAT: no more
ntp	Disable the NTP server. FORMAT: no ntp

Command	Description
snmp	Disable SNMP features. FORMAT: no snmp
ssh	Disable ssh access. FORMAT: no ssh
syslog	Disable the Syslog services. FORMAT: no syslog
telnet	Disable Telnet access. FORMAT: no telnet
ETH-NAME	Disable the selected Ethernet interface (eth0, gig1 or gig2). You cannot disable the console interface. with this command. FORMAT: no eth0 (gig1 or gig2)

pci-audit

The **pci-audit** command [**Xirrus_Wi-Fi_Array(config)# pci-audit**] checks the configuration of the Array for conformance with PCI DSS standards. When you enter the **pci-audit** command, it lists any settings that violate PCI DSS requirements. In addition, if **pci-audit** is on (enabled), the Array will warn you if you change any parameters in a way that violates PCI DSS requirements. For example, if you enable **pci-audit** and then set encryption to **none** on an SSID (in the CLI or the WMI), a warning will be displayed and a Syslog message will be issued. For more information, see [Appendix D: Implementing PCI DSS](#).

Command	Description
disable	The Array will not check configuration changes for PCI DSS violations. FORMAT: pci-audit disable
enable	The Array reports any current settings that violate PCI DSS, and will warn you and issue a Syslog message if you attempt to save configuration changes that violate PCI DSS. FORMAT: pci-audit enable
off	The Array will not check configuration changes for PCI DSS violations. FORMAT: pci-audit off
on	The Array reports any current settings that violate PCI DSS, and will warn you and issue a Syslog message if you make configuration changes that that violate PCI DSS. FORMAT: pci-audit on

quit

The **quit** command [Xirrus_Wi-Fi_Array(config)# **quit**] is used to exit the Command Line Interface.

Command	Description
<cr>	Exit the Command Line Interface. FORMAT: quit If you have made any configuration changes and your changes have not been saved, you are prompted to save your changes to Flash. At the prompt, answer Yes to save your changes, or answer No to discard your changes.

radius-server

The **radius-server** command [Xirrus_Wi-Fi_Array(config-radius-server)#] is used to configure the external and internal RADIUS server parameters.

Command	Description
external	Configure an external RADIUS server. FORMAT: radius-server external To configure a RADIUS server (primary, secondary, or accounting server, by IP address or host name), and the reporting interval use: radius-server external accounting
internal	Configure the external RADIUS server. FORMAT: radius-server internal
use	Choose the active RADIUS server (either external or internal). FORMAT: use external (or internal)

reboot

The **reboot** command [**Xirrus_Wi-Fi_Array(config)# reboot**] is used to reboot the Array. If you have unsaved changes, the command will notify you and give you a chance to cancel the reboot.

Command	Description
<cr>	Reboot the Array. FORMAT: reboot
delay	Reboot the Array after a delay of 1 to 60 seconds. FORMAT: reboot delay [n]

reset

The **reset** command [**Xirrus_Wi-Fi_Array(config)# reset**] is used to reset all settings to their default values then reboot the Array.

Command	Description
<cr>	Reset all configuration parameters to their factory default values. FORMAT: reset The Array is rebooted automatically.
preserve-ip-settings	Preserve all ethernet and VLAN settings and reset all other configuration parameters to their factory default values. FORMAT: reset preserve-ip-settings The Array is rebooted automatically.

run-tests

The **run-tests** command [**Xirrus_Wi-Fi_Array(run-tests)#**] is used to enter run-tests mode, which allows you to perform a range of tests on the Array.

Command	Description
<cr>	Enter run-tests mode. FORMAT: run-tests
iperf	Execute iperf utility. FORMAT: run-tests iperf
kill-beacons	Turn off beacons for selected single IAP. FORMAT: run-tests kill-beacons [off iap-name]
kill-probe-responses	Turn off probe responses for selected single IAP. FORMAT: run-tests kill-probe-responses [off iap-name]
led	LED test. FORMAT: run-tests led [flash rotate]
memtest	Execute memory tests. FORMAT: run-tests memtest
ping	Execute ping utility. FORMAT: run-tests ping [host-name ip-addr]

Command	Description
radius-ping	<p>Special ping utility to test the connection to a RADIUS server.</p> <p>FORMAT:</p> <p>run-tests radius-ping [external ssid <ssidnum>] [primary secondary] user <raduser> password <radpasswd> auth-type [CHAP PAP]</p> <p>run-tests radius-ping [internal server <radserver> port <radport> secret <radsecret>] user <raduser> password <radpasswd> auth-type [CHAP PAP]</p> <p>You may select a RADIUS server that you have already configured (ssid or external or internal) or specify another server (server).</p>
rlb	<p>Run manufacturing radio loopback test.</p> <p>FORMAT:</p> <p>run-tests rlb {optional command line switches}</p>
self-test	<p>Execute self-test.</p> <p>FORMAT:</p> <p>run-tests self-test {logfile-name (optional)}</p>
site-survey	<p>Enable or disable site survey mode.</p> <p>FORMAT:</p> <p>run-tests site-survey [on off enable disable]</p>
ssh	<p>Execute ssh utility.</p> <p>FORMAT:</p> <p>run-tests ssh [hostname ip-addr] [command-line-switches (optional)]</p>
tcpdump	<p>Execute tcpdump utility to dump traffic for selected interface or VLAN.</p> <p>FORMAT:</p> <p>run-tests tcpdump</p>

Command	Description
telnet	Execute telnet utility. FORMAT: run-tests telnet [hostname ip-addr] [command-line-switches (optional)]
traceroute	Execute traceroute utility. FORMAT: run-tests traceroute [host-name ip-addr]

security

The **security** command [Xirrus_Wi-Fi_Array(config-security)#] is used to establish the security parameters for the Array.

Command	Description
wep	Set the WEP encryption parameters. FORMAT: security wep
wpa	Set the WEP encryption parameters. FORMAT: security wpa

snmp

The **snmp** command [**Xirrus_Wi-Fi_Array(config-snmp)#**] is used to enable, disable, or configure SNMP.

Command	Description
v2	Enable SNMP v2. FORMAT: snmp v2
v3	Enable SNMP v3. FORMAT: snmp v3
trap	Configure traps for SNMP. Up to four trap destinations may be configured, and you may specify whether to send traps for authentication failure. FORMAT: snmp trap

ssh

The **ssh** command [**Xirrus_Wi-Fi_Array(config)# ssh**] is used to enable or disable the SSH feature. The Array only allows SSH-2 connections, so be sure that your SSH client is configured to use SSH-2.

Command	Description
disable	Disable SSH. FORMAT: ssh disable
enable	Enable SSH. FORMAT: ssh enable

Command	Description
off	Disable SSH. FORMAT: ssh off
on	Enable SSH. FORMAT: ssh on
timeout	Set the SSH inactivity timeout. FORMAT: ssh timeout 300 (in seconds)

ssid

The **ssid** command [**Xirrus_Wi-Fi_Array(config-ssid)#**] is used to establish your SSID parameters.

Command	Description
add	Add an SSID. FORMAT: ssid add [newssid]
del	Delete an SSID. FORMAT: ssid del [oldssid]
edit	Edit an existing SSID. FORMAT: ssid edit [existingssid]
reset	Delete all SSIDs and restore the default SSID. FORMAT: ssid reset

standby

The **standby** command [**Xirrus_Wi-Fi_Array(config-ssid)#**] sets this Array to function as a standby unit for another Array.

Command	Description
mode	Enable or disable standby mode on this Array. FORMAT: standby mode [disable enable off on]
target	Specify the MAC address of the target Array to be monitored for failure. FORMAT: standby target [AA:BB:CC:DD:EE:FF]

syslog

The **syslog** command [**Xirrus_Wi-Fi_Array(config-syslog)#**] is used to enable, disable, or configure the Syslog server.

Command	Description
console	Enable or disable the display of Syslog messages on the console, and set the level to be displayed. All messages at this level and lower (i.e., more severe) will be displayed. FORMAT: syslog console [on/off] level [0-7]
disable	Disable the Syslog server. FORMAT: syslog disable
email	Disable the Syslog server. FORMAT: syslog email from [email-from-address] level [0-7] password [email-acct-password] server [email-server-IPaddr] test [test-msg-text] to-list [recipient-email-addresses] user [email-acct-username]
enable	Enable the Syslog server. FORMAT: syslog enable
local-file	Set the size and/or severity level (all messages at this level and lower will be logged). FORMAT: syslog local-file size [1-500] level [0-7]
no	Disable the selected feature. FORMAT: syslog no [feature]

Command	Description
off	Disable the Syslog server. FORMAT: syslog off
on	Enable the Syslog server. FORMAT: syslog on
primary	Set the IP address of the primary Syslog server and/or the severity level of messages to be logged. FORMAT: syslog primary [1.2.3.4] level [0-7]
secondary	Set the IP address of the secondary (backup) Syslog server and/or the severity level of messages to be logged. FORMAT: syslog primary [1.2.3.4] level [0-7]

telnet

The **telnet** command [**Xirrus_Wi-Fi_Array(config)# telnet**] is used to enable or disable Telnet.

Command	Description
disable	Disable Telnet. FORMAT: telnet disable
enable	Enable Telnet. FORMAT: telnet enable
off	Disable Telnet. FORMAT: telnet off
on	Enable Telnet. FORMAT: telnet on
timeout	Set the Telnet inactivity timeout. FORMAT: telnet timeout 300 (in seconds)

uptime

The **uptime** command [**Xirrus_Wi-Fi_Array(config)# uptime**] is used to display the elapsed time since you last rebooted the Array.

Command	Description
<cr>	Display time since last reboot. FORMAT: uptime

vlan

The `vlan` command [`Xirrus_Wi-Fi_Array(config-vlan)#`] is used to establish your VLAN parameters.

Command	Description
add	Add a VLAN. FORMAT: vlan add [newvlan]
default-route	Assign a VLAN for the default route (for outbound management traffic). FORMAT: vlan default-route [defaultroute]
delete	Delete a VLAN. FORMAT: vlan delete [oldvlan]
edit	Modify an existing VLAN. FORMAT: vlan edit [existingvlan]
native-vlan	Assign a native VLAN (traffic is untagged). FORMAT: vlan native-vlan [nativevlan]
no	Disable the selected feature. FORMAT: vlan no [feature]
reset	Delete all existing VLANs. FORMAT: vlan reset

Sample Configuration Tasks

This section provides examples of some of the common configuration tasks used with the Wi-Fi Array, including:

- [“Configuring a Simple Open Global SSID” on page 356.](#)
- [“Configuring a Global SSID using WPA-PEAP” on page 357.](#)
- [“Configuring an SSID-Specific SSID using WPA-PEAP” on page 358.](#)
- [“Enabling Global IAPs” on page 359.](#)
- [“Disabling Global IAPs” on page 360.](#)
- [“Enabling a Specific IAP” on page 361.](#)
- [“Disabling a Specific IAP” on page 362.](#)
- [“Setting Cell Size Auto-Configuration for All IAPs” on page 363](#)
- [“Setting the Cell Size for All IAPs” on page 364.](#)
- [“Setting the Cell Size for a Specific IAP” on page 365.](#)
- [“Configuring VLANs on an Open SSID” on page 366.](#)
- [“Configuring Radio Assurance Mode \(Loopback Tests\)” on page 367.](#)

To facilitate the accurate and timely management of revisions to this section, the examples shown here are presented as screen images taken from a Secure Shell (SSH) session (in this case, PuTTY). Depending on the application you are using to access the Command Line Interface, and how your session is set up (for example, font and screen size), the images presented on your screen may be different than the images shown in this section. However, the data displayed will be the same.

Some of the screen images shown in this section have been modified for clarity. For example, the image may have been “elongated” to show all data without the need for additional images or scrolling. We recommend that you use the Adobe PDF version of this User’s Guide when reviewing these examples—a hard copy document may be difficult to read.

As mentioned previously, the root command prompt is determined by the host name assigned to your Array.

Configuring a Simple Open Global SSID

This example shows you how to configure a simple open global SSID.

```

PuTTY (inactive)
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption none broadcast
  Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
  Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
  Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
=====
State           Enabled
Active          Yes
Encryption      Global Open
VLAN Name       -
VLAN Number     -
QoS Level       2
Active Band     802.11a & 802.11bg
Broadcast       On
DHCP Pool       none
Traffic Limit   Unlimited
Traffic/Station Unlimited
Time on         Always
Time off        Never
Days on         All
Web Page Redirect Disabled
```

Figure 162. Configuring a Simple Open Global SSID

Configuring a Global SSID using WPA-PEAP

This example shows you how to configure a global SSID using WPA-PEAP encryption in conjunction with the Array's Internal RADIUS server.

```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption wpa broadcast
Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
-----
State           Disabled
Active          No
Encryption      Global WPA
VLAN Name
VLAN Number     -
QoS Level       2
Active Band     802.11a & 802.11bg
Broadcast       On
DHCP Pool       none
Traffic Limit   Unlimited
Traffic/Station Unlimited
Time on         Always
Time off        Never
Days on         All
Web Page Redirect Disabled

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# top
Xirrus_Wi-Fi_Array(config)# radius-server use internal
Xirrus_Wi-Fi_Array(config)# radius-server internal add Mike password Jones ssid Companyx
Xirrus_Wi-Fi_Array(config)# radius-server internal
Xirrus_Wi-Fi_Array(config-radius-internal)# show

Username           SSID
-----
Mike               Companyx

Xirrus_Wi-Fi_Array(config-radius-internal)# save
Xirrus_Wi-Fi_Array(config-radius-internal)# top
Xirrus_Wi-Fi_Array(config)# security wpa
Xirrus_Wi-Fi_Array(config-security-wpa)# show

Global Security Settings Summary
-----
WEP:  key 1 size : not set (default)
      key 2 size : not set
      key 3 size : not set
      key 4 size : not set

WPA:  cipher      : TKIP on, AES off
      key mgmt    : EAP on, PSK off
      rekey time  : disabled
      passphrase  : not set

Xirrus_Wi-Fi_Array(config-security-wpa)#
```

Figure 163. Configuring a Global SSID using WPA-PEAP

Configuring an SSID-Specific SSID using WPA-PEAP

This example shows you how to configure an SSID-specific SSID using WPA-PEAP encryption in conjunction with the Array's Internal RADIUS server.

```

Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption wpa ssid_specific broadcast
  Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# radius-server use internal
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# radius-server internal add Mike password Jones
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
sXirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
=====
State                Enabled
Active               Yes
Encryption           SSID specific WPA
VLAN Name
VLAN Number         -
QoS Level            2
Active Band          802.11a & 802.11bg
Broadcast            On
DHCP Pool            none
Traffic Limit        Unlimited
Traffic/Station      Unlimited
Time on              Always
Time off             Never
Days on              All
Web Page Redirect    Disabled

SSID Specific WPA Security Settings
-----
Key Management        EAP on, PSK off
PSK Passphrase        not set
Radius Server         internal

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# top
Xirrus_Wi-Fi_Array(config)# radius-server internal
Xirrus_Wi-Fi_Array(config-radius-internal)# show

Username              SSID
-----              -----
Mike                  Companyx

Xirrus_Wi-Fi_Array(config-radius-internal)# save
Xirrus_Wi-Fi_Array(config-radius-internal)#
  
```

Figure 164. Configuring an SSID-Specific SSID using WPA-PEAP

Enabling Global IAPs

This example shows you how to enable all IAPs (radios), regardless of the wireless technology they use.

```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# all_up
Interface IAP a1 state changed to up
Interface IAP a3 state changed to up
Interface IAP a4 state changed to up
Interface IAP a5 state changed to up
Interface IAP a6 state changed to up
Interface IAP a7 state changed to up
Interface IAP a8 state changed to up
Interface IAP a9 state changed to up
Interface IAP a10 state changed to up
Interface IAP a11 state changed to up
Interface IAP a12 state changed to up
Interface IAP abg2 state changed to up
Interface IAP abg3 state changed to up
Interface IAP abg4 state changed to up

Xirrus_Wi-Fi_Array(config-iap-global)# save
Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
          Cell  TX    RX
IAP State Channel Antenna  Size Power Threshold Stations WDS MAC address / BSSID  Description
-----
a1 up    64   int-dir max    20dBm -90dBm    0  C-1 00:0f:7d:03:5e:10-11
a2 up    48   int-dir max    20dBm -90dBm    0  C-2 00:0f:7d:03:5e:30-31
a3 up   157   int-dir max    20dBm -90dBm    0  C-3 00:0f:7d:03:5e:40-41
a4 up    60   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:50-51
a5 up    44   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:70-71
a6 up   153   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:80-81
a7 up    56   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:90-91
a8 up    40   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:b0-b1
a9 up   149   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:c0-c1
a10 up   52   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:d0-d1
a11 up   36   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:f0-f1
a12 up   161   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:00-01
abg1 up   11   int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:20-21
abg2 up  monitor int-omni manual 20dBm -95dBm    0  00:0f:7d:03:5e:60-61
```

Figure 165. Enabling Global IAPs

Disabling Global IAPs

This example shows you how to disable all IAPs (radios), regardless of the wireless technology they use.

```
Xirrus Wi-Fi Array
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# all_down
Interface IAP a1 state changed to down
Interface IAP a2 state changed to down
Interface IAP a3 state changed to down
Interface IAP a4 state changed to down
Interface IAP a5 state changed to down
Interface IAP a6 state changed to down
Interface IAP a7 state changed to down
Interface IAP a8 state changed to down
Interface IAP a9 state changed to down
Interface IAP a10 state changed to down
Interface IAP a11 state changed to down
Interface IAP a12 state changed to down
Interface IAP abg1 state changed to down
Interface IAP abg2 state changed to down
Interface IAP abg3 state changed to down
Interface IAP abg4 state changed to down

Xirrus_Wi-Fi_Array(config-iap-global)# save
Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
          Cell  TX    RX
IAP State Channel Antenna  Size Power Threshold Stations WDS MAC address / BSSID  Description
-----
a1 down    64   int-dir max    20dBm -90dBm      0  C-1 00:0f:7d:03:5e:10-11
a2 down    48   int-dir max    20dBm -90dBm      0  C-2 00:0f:7d:03:5e:30-31
a3 down   157   int-dir max    20dBm -90dBm      0  C-3 00:0f:7d:03:5e:40-41
a4 down    60   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5e:50-51
a5 down    44   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5e:70-71
a6 down   153   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5d:80-81
a7 down    56   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5d:90-91
a8 down    40   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5d:b0-b1
a9 down   149   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5d:c0-c1
a10 down   52   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5d:d0-d1
a11 down   36   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5d:f0-f1
a12 down   161   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5e:00-01
abg1 down   11   int-dir max    20dBm -90dBm      0    00:0f:7d:03:5e:20-21
```

Figure 166. Disabling Global IAPs

Enabling a Specific IAP

This example shows you how to enable a specific IAP (radio). In this example, the IAP that is being enabled is **a1** (the first IAP in the summary list).

```
Xirrus Wi-Fi Array
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a1 up
Xirrus_Wi-Fi_Array(config-iap)# save
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
          Cell TX    RX
IAP State Channel Antenna  Size Power Threshold Stations WDS MAC address / BSSID Description
-----
a1 up      64  int-dir max    20dBm -90dBm    0  C-1 00:0f:7d:03:5e:10-11
a2 down    48  int-dir max    20dBm -90dBm    0  C-2 00:0f:7d:03:5e:30-31
a3 down   157  int-dir max    20dBm -90dBm    0  C-3 00:0f:7d:03:5e:40-41
a4 down    60  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:50-51
a5 down    44  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:70-71
a6 down   153  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:80-81
a7 down    56  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:90-91
a8 down    40  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:b0-b1
a9 down   149  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:c0-c1
a10 down   52  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:d0-d1
a11 down   36  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:f0-f1
a12 down  161  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:00-01
abg1 down   11  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:20-21
abg2 down  monitor int-omni manual 20dBm -95dBm    0  00:0f:7d:03:5e:60-61
abg3 down    6  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:a0-a1
abg4 down    1  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:e0-e1

Xirrus_Wi-Fi_Array(config-iap)#
```

Figure 167. Enabling a Specific IAP

Disabling a Specific IAP

This example shows you how to disable a specific IAP (radio). In this example, the IAP that is being disabled is **a2** (the second IAP in the summary list).

```

Xirrus Wi-Fi Array
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a2 down
Xirrus_Wi-Fi_Array(config-iap)# save
Xirrus_Wi-Fi_Array(config-iap)# show

IAP Summary Table
      Cell  TX    RX
IAP State Channel Antenna  Size  Power Threshold Stations WDS MAC address / BSSID  Description
-----
a1 up    64  int-dir max    20dBm -90dBm    0  C-1 00:0f:7d:03:5e:10-11
a2 down  48  int-dir max    20dBm -90dBm    0  C-2 00:0f:7d:03:5e:30-31
a3 up   157  int-dir max    20dBm -90dBm    0  C-3 00:0f:7d:03:5e:40-41
a4 up    60  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:50-51
a5 up    44  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:70-71
a6 up   153  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:80-81
a7 up    56  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:90-91
a8 up    40  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:b0-b1
a9 up   149  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:c0-c1
a10 up   52  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:d0-d1
a11 up   36  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:f0-f1
a12 up  161  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:00-01
abg1 up   11  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5e:20-21
abg2 up  monitor int-omni manual 20dBm -95dBm    0  00:0f:7d:03:5e:60-61
abg3 up    6  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:a0-a1
abg4 up    1  int-dir max    20dBm -90dBm    0  00:0f:7d:03:5d:e0-e1

Xirrus_Wi-Fi_Array(config-iap)#
    
```

Figure 168. Disabling a Specific IAP

Setting Cell Size Auto-Configuration for All IAPs

This example shows how to set the cell size for all enabled IAPs to be auto-configured (**auto**). (See “Fine Tuning Cell Sizes” on page 53.) The **auto_cell** option may be used with **global_settings**, **global_a_settings**, or **global_bg_settings**. It sets the cell size of the specified IAPs to **auto**, and it launches an auto-configuration to adjust the sizes. Be aware that if the **intrude-detect** feature is enabled on **abg(n)2**, its cell size is unaffected by this command. Also, any IAPs used in WDS links are unaffected.

Auto-configuration may be set to run periodically at intervals specified by **auto_cell period** (in seconds) if **period** is non-zero. The percentage of overlap allowed between cells in the cell size computation is specified by **auto_cell overlap** (0 to 100). This example sets auto-configuration to run every 1200 seconds with an allowed overlap of 5%. It sets the cell size of all IAPs to **auto**, and runs a cell size auto-configure operation which completes successfully.

```

192.168.39.125 - PuTTY
Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# auto_cell overlap 5
Xirrus-WiFi-Array(config-iap-global)# auto_cell period 1200
Xirrus-WiFi-Array(config-iap-global)# auto_cell
Auto cell size configuration completed successfully.

Xirrus-WiFi-Array(config-iap-global)# save
Xirrus-WiFi-Array(config-iap-global)# exit
Xirrus-WiFi-Array(config-iap)# show

IAP Summary Table
-----
IAP State Channel Antenna Cell Size TX Power RX Threshold Stations WDS MAC address / BSSID Description
-----
a1 down 36 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:10
a2 up 36 int-dir auto -10dBm -65dBm 0 00:0F:7d:03:c3:30
a3 up 157 int-dir auto -10dBm -65dBm 0 00:0F:7d:03:c3:40
a4 up 56 int-dir auto -10dBm -65dBm 0 00:0F:7d:03:c3:50
a5 down 56 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:70
a6 down 157 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:80
a7 down 44 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:90
a8 down 60 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:b0
a9 up 153 int-dir auto -10dBm -65dBm 0 00:0F:7d:03:c3:c0
a10 down 48 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:d0
a11 down 64 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:f0
a12 down 161 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:00
abg1 down 1 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:20
abg2 up monitor int-omni manual 20dBm -95dBm 0 00:0F:7d:03:c3:60
abg3 down 11 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:a0
abg4 down 6 int-dir max 20dBm -90dBm 0 00:0F:7d:03:c3:e0

Xirrus-WiFi-Array(config-iap)#

```

Figure 169. Setting the Cell Size for All IAPs

Setting the Cell Size for All IAPs

This example shows you how to establish the cell size for all IAPs (radios), regardless of the wireless technology they use. Be aware that if the **intrude-detect** feature is enabled on **abg(n)2** the cell size cannot be set globally—you must first disable the intrude-detect feature on **abg(n)2**.

In this example, the cell size is being set to **small** for all IAPs. You have the option of setting IAP cell sizes to small, medium, large, or max. See also, “[Fine Tuning Cell Sizes](#)” on page 53.

```
Xirrus Wi-Fi Array
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# global_settings
Xirrus_Wi-Fi_Array(config-iap-global)# cellsize small
Xirrus_Wi-Fi_Array(config-iap-global)# save
Xirrus_Wi-Fi_Array(config-iap-global)# exit
Xirrus_Wi-Fi_Array(config-iap)# show
```

IAP Summary Table										
				Cell	TX	RX				
IAP	State	Channel	Antenna	Size	Power	Threshold	Stations	WDS	MAC address / BSSID	Description
a1	up	64	int-dir	small	5dBm	-75dBm	0	C-1	00:0f:7d:03:5e:10-11	
a2	up	48	int-dir	small	5dBm	-75dBm	0	C-2	00:0f:7d:03:5e:30-31	
a3	up	157	int-dir	small	5dBm	-75dBm	0	C-3	00:0f:7d:03:5e:40-41	
a4	up	60	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5e:50-51	
a5	up	44	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5e:70-71	
a6	up	153	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:80-81	
a7	up	56	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:90-91	
a8	up	40	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:b0-b1	
a9	up	149	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:c0-c1	
a10	up	52	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:d0-d1	
a11	up	36	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:f0-f1	
a12	up	161	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5e:00-01	
abg1	up	11	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5e:20-21	
abg2	down	1	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5e:60-61	
abg3	up	6	int-dir	small	5dBm	-75dBm	0		00:0f:7d:03:5d:a0-a1	

Figure 170. Setting the Cell Size for All IAPs

Setting the Cell Size for a Specific IAP

This example shows you how to establish the cell size for a specific IAP (radio). In this example, the cell size for **a2** is being set to **medium**. You have the option of setting IAP cell sizes to small, medium, large, or max (the default is max). See also, “Fine Tuning Cell Sizes” on page 53.

```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Running configuration has not been saved.

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# interface iap
Xirrus_Wi-Fi_Array(config-iap)# a2
Xirrus_Wi-Fi_Array(config-iap-a2)# cellsize medium
Xirrus_Wi-Fi_Array(config-iap-a2)# save
Xirrus_Wi-Fi_Array(config-iap-a2)# exit
Xirrus_Wi-Fi_Array(config-iap)# show
```

IAP Summary Table										
IAP	State	Channel	Antenna	Cell Size	TX Power	RX Threshold	Stations	WDS	MAC address / BSSID	Description
a1	up	64	int-dir	max	20dBm	-90dBm	0	C-1	00:0f:7d:03:5e:10-11	
a2	up	48	int-dir	medium	11dBm	-81dBm	0	C-2	00:0f:7d:03:5e:30-31	
a3	up	157	int-dir	max	20dBm	-90dBm	0	C-3	00:0f:7d:03:5e:40-41	
a4	up	60	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5e:50-51	
a5	up	44	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5e:70-71	
a6	up	153	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:80-81	
a7	up	56	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:90-91	
a8	up	40	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:b0-b1	
a9	up	149	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:c0-c1	
a10	up	52	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:d0-d1	
a11	up	36	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:f0-f1	
a12	up	161	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5e:00-01	
abg1	up	11	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5e:20-21	
abg2	down	1	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5e:60-61	
abg3	up	6	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:a0-a1	
abg4	up	1	int-dir	max	20dBm	-90dBm	0		00:0f:7d:03:5d:e0-e1	

```
Xirrus_Wi-Fi_Array(config-iap)# _
```

Figure 171. Setting the Cell Size for a Specific IAP

Configuring VLANs on an Open SSID

This example shows you how to configure VLANs on an Open SSID.

```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# configure
Xirrus_Wi-Fi_Array(config)# vlan
Xirrus_Wi-Fi_Array(config-vlan)# add VLAN2301 number 2301 ip addr 192.168.39.100 mask 255.255.255.0 gateway
Changing IP address to 192.168.39.100.
Do you want to proceed? [yes/no]: y
Xirrus_Wi-Fi_Array(config-vlan)# show

VLAN Summary Table
-----
VLAN Name          Number  Management  DHCP   IP Address      IP Mask          IP Gateway
-----
VLAN2301           2301   disallowed  disabled 192.168.39.100  255.255.255.0    192.168.39.1

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

Xirrus_Wi-Fi_Array(config-vlan)# default-route 2301
Xirrus_Wi-Fi_Array(config-vlan)# show

VLAN Summary Table
-----
VLAN Name          Number  Management  DHCP   IP Address      IP Mask          IP Gateway
-----
VLAN2301           2301   disallowed  disabled 192.168.39.100  255.255.255.0    192.168.39.1

Default Route      VLAN: "VLAN2301" / 2301
Native (untagged) VLAN: none

Xirrus_Wi-Fi_Array(config-vlan)# exit
Xirrus_Wi-Fi_Array(config)# ssid
Xirrus_Wi-Fi_Array(config-ssid)# add Companyx encryption none broadcast
Note: New SSID is created disabled. Enable after configuration.

Xirrus_Wi-Fi_Array(config-ssid)# edit Companyx
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# vlan 2301
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# enable
Xirrus_Wi-Fi_Array(config-ssid-Companyx)# show

SSID "Companyx" Settings
-----
State              Enabled
Active             Yes
Encryption         Global Open
VLAN Name          VLAN2301
VLAN Number       2301
QoS Level          2
Active Band        802.11a & 802.11bg
Broadcast          On
DHCP Pool          none
Traffic Limit      Unlimited
Traffic/Station    Unlimited
Time on            Always
Time off           Never
Days on            All
Web Page Redirect  Disabled

Xirrus_Wi-Fi_Array(config-ssid-Companyx)# save
Xirrus_Wi-Fi_Array(config-ssid-Companyx)#
```



Setting the default route enables the Array to send management traffic, such as Syslog messages and SNMP information to a destination behind a router.

Figure 172. Configuring VLANs on an Open SSID

Configuring Radio Assurance Mode (Loopback Tests)

The Array uses the built-in monitor radio, IAP abg(n)2, to monitor other radios in the Array. Tests include sending probes on all channels and checking for a response, and checking whether beacons are received from the other radio. If a problem is detected, corrective actions are taken to recover. Loopback mode operation is described in detail in “Array Monitor and Radio Assurance Capabilities” on page 406.

The following actions may be configured:

- **alert-only**—the Array will issue an alert in the Syslog.
- **repair-without-reboot**—the Array will issue an alert and reset radios at the Physical Layer (Layer 1) and possibly at the MAC layer. The reset should not be noticed by users, and they will not need to reassociate.
- **reboot-allowed**—the Array will issue an alert, reset the radios, and schedule the Array to reboot at midnight (per local Array time) if necessary. All stations will need to reassociate to the Array.
- **off**—Disable IAP loopback tests (no self-monitoring occurs). Radio Assurance mode is off by default.

This is a global IAPs setting—abg(n)2 will monitor all other radios according to the settings above, and it cannot be set up to monitor particular radios. Radio assurance mode requires Intrusion Detection to be set to Standard.

The following example shows you how to configure a loopback test.

```

192.168.39.125 - PuTTY

Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# intrude-detect standard
Interface IAP abg2 state changed to down
Interface IAP abg2 band changed to monitor
Interface IAP abg2 channel changed to monitor
Interface IAP abg2 antenna changed to internal omni
Interface IAP abg2 tx-power changed to 20
Interface IAP abg2 rx-threshold changed to -95
Interface IAP abg2 state changed to up

Xirrus-WiFi-Array(config-iap-global)# loopback-test
  alert-only          Enable IAP loopback tests with failure alerts only
  off                 Disable IAP loopback tests
  reboot-allowed      Enable IAP loopback tests with alerts & repairs & reboots if n
  repair-without-reboot Enable IAP loopback tests with alerts & repairs, but no reboots
  <cr>               Set global IAP parameters

Xirrus-WiFi-Array(config-iap-global)# loopback-test repair-without-reboot
Xirrus-WiFi-Array(config-iap-global)#
Xirrus-WiFi-Array(config-iap-global)# show

Global IAP Settings Summary
-----
Country code          not set (defaults to US: United States)
Beacon interval       100 Kusec
Broadcast rates       standard
DTIM period           1 beacon
Short retries          7
Long retries           4
Total IAPs            16
Max stations/IAP      64
Max phones /IAP       16
Station timeout       1000 sec
Station reauth time   5 sec
Management            disallowed
Station to station    forward
Load balancing        off
Intrusion detection   standard
Auto chan power up    off
Auto chan schedule    none
Auto cell period      1200 sec
Auto cell overlap     5%
Xirrus Fast Roaming   via tunnels to arrays in-range or targeted
Sharp cell TX power   off
Public Safety Band    disabled
802.11h support       on
Loopback test mode    repair w/o reboot
LED activity           on when IAP up
                     blink on data frame transmitted
                     blink on data frame received
                     blink on management frame transmitted
                     blink on management frame received
                     blink heartbeat on station associated

Xirrus-WiFi-Array(config-iap-global)#
Do you want to save changes to flash [yes/no]: █

```

Figure 173. Configuring Radio Assurance Mode (Loopback Testing)

Appendices



Page is intentionally blank

Appendix A: Servicing the Wi-Fi Array

This appendix contains procedures for servicing the Xirrus Wi-Fi Array, including the removal and reinstallation of major hardware components. Topics include:

- “Removing the Access Panel” on page 373.
- “Reinstalling the Access Panel” on page 376.
- “Replacing the FLASH Memory Module” on page 378.
- “Replacing the Main System Memory” on page 380.
- “Replacing the Integrated Access Point Radio Module” on page 382.
- “Replacing the Power Supply Module” on page 385.

! *Always disconnect the power source from the Array before attempting to remove or replace components. Never work on the unit with the power connected.*

! *You must be grounded and the work surface must be static-free.*

! *Caution! The Array contains a battery which is not to be replaced by the customer. Danger of Explosion exists if the battery is incorrectly replaced.*

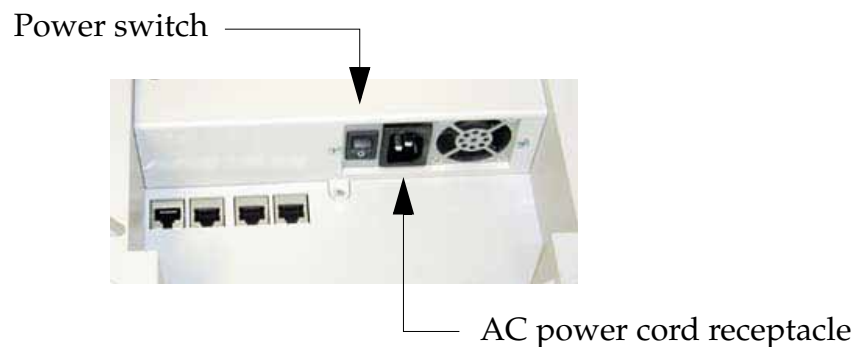


Figure 174. Disconnecting Power from the Array



Most service activities are performed with the Array placed face-down on a flat work surface. To avoid damaging the finished enclosure, we recommend using a protective material between the work surface and the unit (a clean sheet of paper will do the trick).

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Removing the Access Panel

Use this procedure when you want to remove the system's access panel. You must remove this panel whenever you need to service the internal components of the Array.

1. Turn OFF the Array's main power switch (XS-3900 and XS-3700 only).
2. Disconnect the AC power cord or Ethernet cable supplying power from the Array.
3. Place the Array face-down on a flat surface. Avoid moving the unit to reduce the risk of damage (scratching) to the finished enclosure.
4. Remove the screws (3 places) that secure the access panel to the main body of the Array.

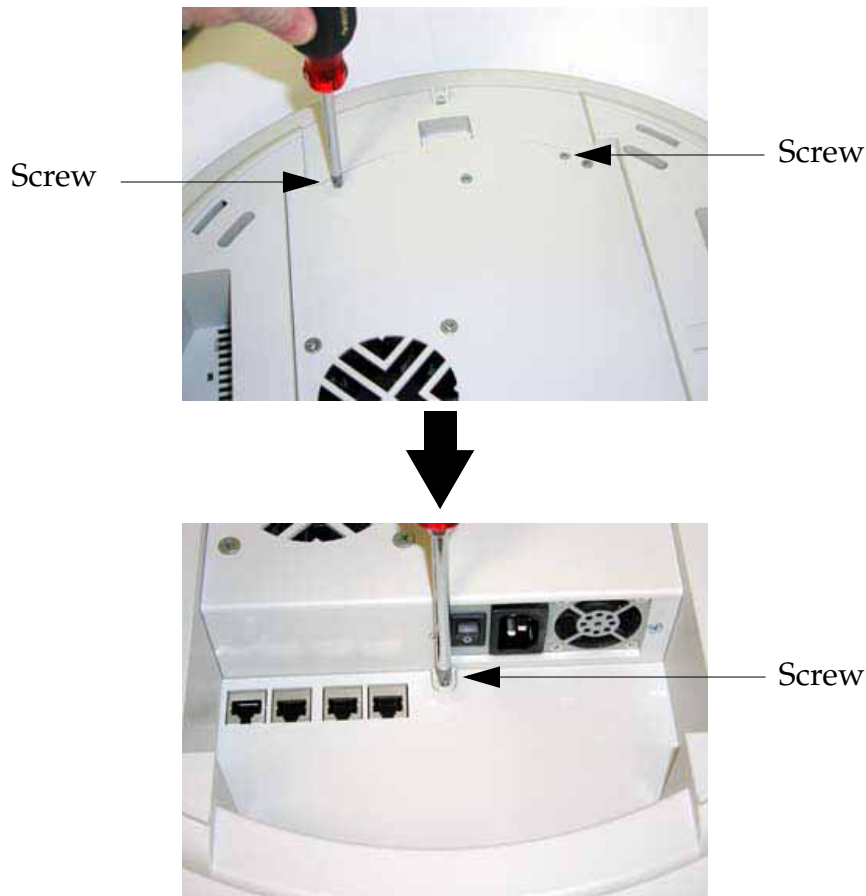


Figure 175. Removing the Access Panel Screws

5. Lift up the access panel to reveal the main system board.



Lift up the access panel

Figure 176. Removing the Access Panel

6. Disconnect the connectors to the power supply and the fan.



Fan connector

Power supply connector

Figure 177. Disconnecting the Power Supply and Fan

7. The access panel can now be safely removed.

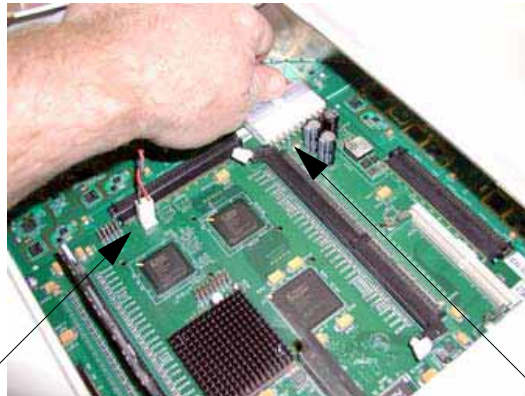
See Also

- Reinstalling the Access Panel
- Replacing the FLASH Memory Module
- Replacing the Integrated Access Point Radio Module
- Replacing the Main System Memory
- Replacing the Power Supply Module
- Appendix A: Servicing the Wi-Fi Array

Reinstalling the Access Panel

Use this procedure when you need to reinstall the access panel after servicing the Array's internal components.

1. Reconnect the fan and power supply.



Fan connector

Power supply connector

Figure 178. Reconnecting the Fan and Power Supply

2. Reinstall the access panel and secure the panel with the three screws.



Figure 179. Reinstalling the Access Panel

3. Reconnect the power source and turn ON the main power switch (if applicable).

See Also

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the FLASH Memory Module

Use this procedure when you want to replace the system's FLASH memory module.

1. Remove the system's access panel. Refer to "Removing the Access Panel" on page 373.
2. Remove the FLASH memory module, taking care not to "wiggle" the module and risk damaging the connection points.

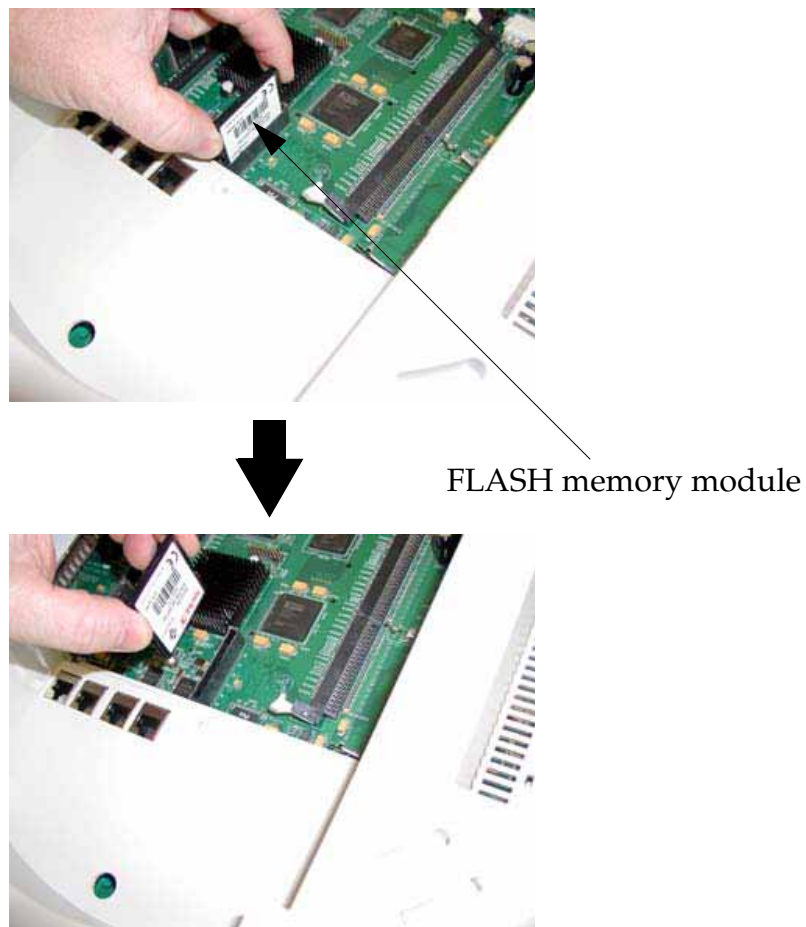


Figure 180. Removing the FLASH Memory Module

3. The removal procedure is complete. You can now reinstall the FLASH memory module (or install a new module).

4. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 376).

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the Main System Memory

Use this procedure when you want to replace the main system memory.

1. Remove the access panel (refer to “Removing the Access Panel” on page 373).
2. Remove the DIMM memory module, taking care not to “wiggle” the module and risk damaging the connection points.

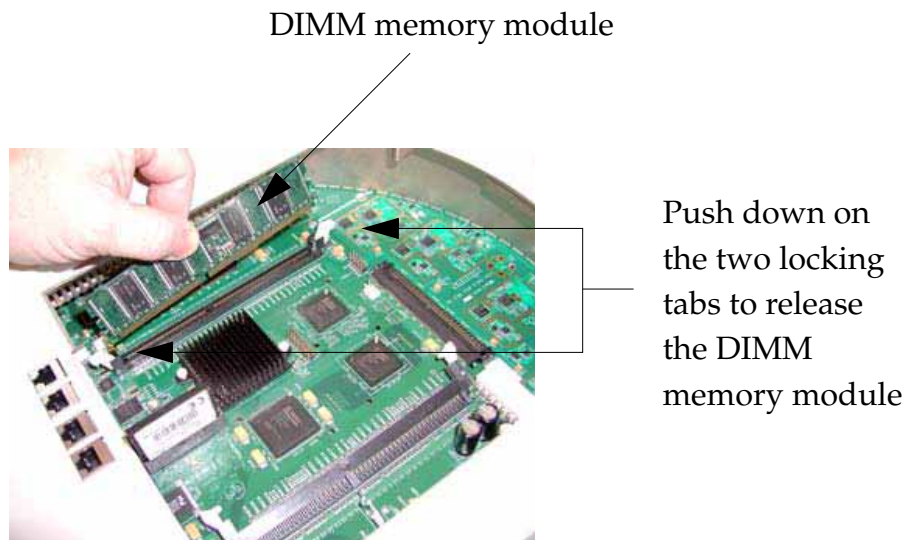


Figure 181. Removing the DIMM Memory Module

3. The removal procedure is complete. You can now reinstall the DIMM memory module (or install a new module). Ensure that the DIMM memory module is seated evenly and the locking tabs are in the upright position. The DIMM memory module is keyed to fit in its socket in one direction only.
4. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 376).

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the Integrated Access Point Radio Module

Use this procedure when you want to replace the integrated access point radio module.

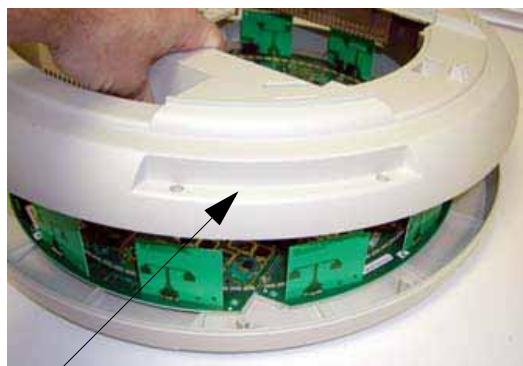
1. Remove the access panel (refer to “Removing the Access Panel” on page 373).
2. Remove the locking screws (8 places) that secure the chassis cover to the main body of the Wi-Fi Array.



Screws (8 places)

Figure 182. Removing the Chassis Cover Screws

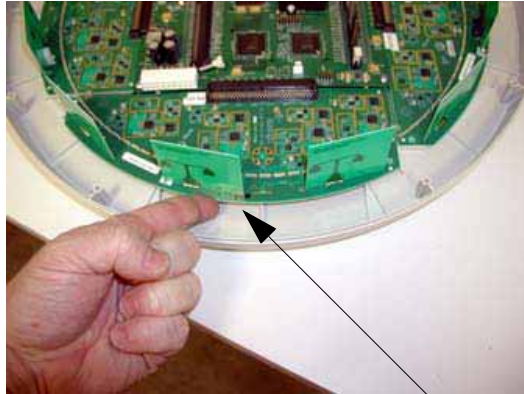
3. Lift and remove the chassis cover.



Remove the chassis cover

Figure 183. Removing the Chassis Cover

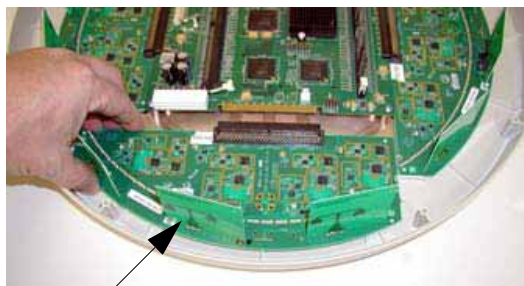
4. Lift the edge of the integrated access point module.



Lift here (do not force)

Figure 184. Lifting the Integrated Access Point Module

5. Slide the integrated access point module away from the unit to disconnect it from the main system board.



Disconnect the module

Figure 185. Disconnect the Integrated Access Point Module

6. The removal procedure is complete. You can now reinstall the integrated access point module (or install a new module).

7. Reinstall the chassis cover (see warnings).

! *When reinstalling the chassis cover, take care to align the cover correctly to avoid damaging the antenna modules. Do not force the chassis cover onto the body of the unit.*

! *Do not overtighten the locking screws.*

8. Reinstall the locking screws (8 places) to secure the chassis cover in place—do not overtighten.
9. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 376).

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Main System Memory

Replacing the Power Supply Module

Appendix A: Servicing the Wi-Fi Array

Replacing the Power Supply Module

Use this procedure when you want to replace the power supply module.

1. Remove the access panel (refer to “Removing the Access Panel” on page 373).
2. Because the power supply unit is molded into the access panel, you must install a new access panel assembly (with the power supply attached). Refer to “Reinstalling the Access Panel” on page 376.



Access panel (with power supply and fan)

Figure 186. Installing a New Access Panel (with Power Supply)

See Also

Reinstalling the Access Panel

Removing the Access Panel

Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

Replacing the Main System Memory

Appendix A: Servicing the Wi-Fi Array

Use this Space for Your Notes



Appendix B: Quick Reference Guide

This section contains product reference information. Use this section to locate the information you need quickly and efficiently. Topics include:

- “Factory Default Settings” on page 387.
- “Keyboard Shortcuts” on page 394.

Factory Default Settings

The following tables show the Wi-Fi Array’s factory default settings.

Host Name

Setting	Default Value
Host name	Xirrus-WiFi-Array

Network Interfaces

Serial

Setting	Default Value
Baud Rate	115200
Word Size	8 bits
Stop Bits	1
Parity	No parity
Time Out	10 seconds

Gigabit 1 and Gigabit 2

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.2.1
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1504
Management Enabled	Yes

Fast Ethernet

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.1.1
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	100 Mbps

Setting	Default Value
MTU Size	1500
Management Enabled	Yes

Integrated Access Points (IAPs)

Setting	Default Value
IAP abg2 Defaults	Enabled Mode = Monitor Channel = Monitor Cell Size = Manual Antenna = Internal-Omni
Enabled (Radio State)	No
Mode <ul style="list-style-type: none"> ● XS16, XS-3900 ● XS12 ● XS8, XS-3700 ● XS4, XS-3500 	802.11a for a1 to a12 802.11bg for abg1 to abg4 802.11a for a1 to a8 802.11bg for abg1 to abg4 802.11a for a1 to a4 802.11bg for abg1 to abg4 802.11bg for abg1 to abg4
Channel	Auto
Cell Size	Max
Maximum Transmit Power	20
Antenna Selected	Internal

Server Settings

NTP

Setting	Default Value
Enabled	No
Primary	time.nist.gov
Secondary	pool.ntp.org

Syslog

Setting	Default Value
Enabled	Yes
Local Syslog Level	Information
Maximum Internal Records	500
Primary Server	None
Primary Syslog Level	Information
Secondary Server	None
Secondary Syslog Level	Information

SNMP

Setting	Default Value
Enabled	Yes
Read-Only Community String	xirrus_read_only
Read-Write Community String	xirrus
Trap Host	null (no setting)

Setting	Default Value
Trap Port	162
Authorization Fail Port	On

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes
IP Start Range	192.168.1.2
IP End Range	192.168.1.254
NAT	Disabled
IP Gateway	None
DNS Domain	None
DNS Server (1 to 3)	None

Default SSID

Setting	Default Value
ID	xirrus
VLAN	None
Encryption	Off
Encryption Type	None
QoS	2
Enabled	Yes

Setting	Default Value
Broadcast	On

Security

Global Settings - Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)
WEP Key Length	null (all 4 keys)
Default Key ID	1
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	Yes
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	Disabled

External RADIUS (Global)

Setting	Default Value
Enabled	Yes
Primary Server	None
Primary Port	1812

Setting	Default Value
Primary Secret	xirrus
Secondary Server	null (no IP address)
Secondary Port	1812
Secondary Secret	null (no secret)
Time Out (before primary server is retired)	600 seconds
Accounting	Disabled
Interval	300 seconds
Primary Server	None
Primary Port	1813
Primary Secret	xirrus
Secondary Server	None
Secondary Port	1813
Secondary Secret	null (no secret)

Internal RADIUS

Setting	Default Value
Enabled	No
The user database is cleared upon reset to the factory defaults. For the Internal RADIUS Server you have a maximum of 1,000 entries.	

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
SSH	On
SSH timeout	300 seconds
Telnet	Off
Telnet timeout	300 seconds
Serial	On
Serial timeout	300 seconds
Management over IAPs	Off
http timeout	300 seconds

Keyboard Shortcuts

The following table shows the most common keyboard shortcuts used by the Command Line Interface.

Action	Shortcut
Cut selected data and place it on the clipboard.	Ctrl + X
Copy selected data to the clipboard.	Ctrl + C

Action	Shortcut
Paste data from the clipboard into a document (at the insertion point).	Ctrl + V
Go to top of screen.	Ctrl + Z
Copy the active window to the clipboard.	Alt + Print Screen
Copy the entire desktop image to the clipboard.	Print Screen
Abort an action at any time.	Esc
Go back to the previous screen.	b
Access the Help screen.	?

See Also
[An Overview](#)

Use this Space for Your Notes



Appendix C: Technical Support

This appendix provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all topics below and try to determine if your problem resides with the Wi-Fi Array or your network infrastructure. Topics include:

- [“General Hints and Tips” on page 397](#)
- [“Frequently Asked Questions” on page 398](#)
- [“Array Monitor and Radio Assurance Capabilities” on page 406](#)
- [“Upgrading the Array via CLI” on page 409](#)
- [“Power over Gigabit Ethernet Compatibility Matrix” on page 414](#)
- [“Contact Information” on page 417](#)

General Hints and Tips

This section provides some useful tips that will optimize the reliability and performance of your Wi-Fi Arrays.

- The Wi-Fi Array requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.
- If using multiple Arrays in the same area, maintain a distance of at least 100 feet (30m) between Arrays if there is direct line-of-sight between the units, or at least 50 feet (15 m) if a wall or other barrier exists between the units.
- Keep the Wi-Fi Array away from electrical devices or appliances that generate RF noise. Because the Array is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).
- If using AC power, each Wi-Fi Array requires its own dedicated AC power outlet. Do not attempt to “piggy-back” AC power to multiple units. To avoid needing to run separate power cables to one or more Arrays, consider using Power over Gigabit Ethernet.

- If you are deploying multiple units, the Array should be oriented so that the **abg(n)2** radio is oriented in the direction of the least required coverage, because when in monitor mode the abg(n)2 radio does not function as an AP servicing stations.
- The Wi-Fi Array should only be used with Wi-Fi certified client devices.

See Also

Contact Information

Multiple SSIDs

Security

VLAN Support

Frequently Asked Questions

This section answers some of the most frequently asked questions, organized by functional area.

Multiple SSIDs

Q. What Are BSSIDs and SSIDs?

- A.** BSSID (Basic Service Set Identifier) refers to an individual access point radio and its associated clients. The identifier is the MAC address of the access point radio that forms the BSS.

A group of BSSs can be formed to allow stations in one BSS to communicate to stations in another BSS by way of a backbone that interconnects each access point.

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

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

Q. What would I use SSIDs for?

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

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

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

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

Q. How do I set up SSIDs?

A. Use the following procedure as a guideline. For more detailed information, go to “SSIDs” on page 235.

1. From the Web Management Interface, go to the [SSID Management](#) page.
2. Select **Yes** to make the SSID visible to all clients on the network. Although the Wi-Fi Array will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
3. Select the minimum security that will be required by users for this SSID.
4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.
5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.

6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.
7. Click on the **Apply** button to apply your changes to this session.
8. Click on the **Save** button to save your changes.
9. If you need to edit any of the SSID settings, you can do so from the [SSID Management](#) page.

See Also

Contact Information

General Hints and Tips

Security

SSIDs

SSID Management

VLAN Support

Security

- Q. How do I ensure that an Array meets FIPS requirements?**
- A.** To meet the Level 2 security requirements of FIPS 140-2, follow the instructions in [Appendix E: Implementing FIPS Security](#).
- Q. How do I ensure that an Array meets PCI DSS requirements?**
- A.** To meet PCI DSS requirements, follow the instructions in [Appendix D: Implementing PCI DSS](#).
- Q. How do I know my management session is secure?**
- A.** Follow these guidelines:
- Administrator passwords
Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.
 - SSH versus Telnet

Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY. The Array only allows SSH-2 connections, so your SSH utility must be set up to use SSH-2.

- Configuration auditing
Do not change approved configuration settings. The optional Xirrus Management System (XMS) offers powerful management features for small or large Wi-Fi Array deployments, and can audit your configuration settings automatically. In addition, using the XMS eliminates the need for an FTP server.

Q. Which wireless data encryption method should I use?

A. Wireless data encryption prevents eavesdropping on data being transmitted or received over the airwaves. The Wi-Fi Array allows you to establish the following data encryption configuration options:

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

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

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

Any of the above encryption modes can be used (and can be used at the same time).

Q. Which user authentication method should I use?

A. User authentication ensures that users are who they say they are. For example, the most obvious example of authentication is logging in with a user name and password. The Wi-Fi Array allows you to choose between the following user authentication methods:

- Pre-Shared Key

Users must manually enter a key (pass phrase) on the client side of the wireless network that matches the key stored by the administrator in your Wi-Fi Arrays.

- RADIUS 802.1x with EAP

802.1x uses a RADIUS server to authenticate large numbers of clients, and can handle different EAP (Extensible Authentication Protocol) authentication methods, including EAP-TLS, EAP-TTLS and EAP-PEAP. The RADIUS server can be internal (provided by the Wi-Fi Array) or external. An external RADIUS server offers more functionality and is **recommended** for large Enterprise deployments.

When using this method, user names and passwords must be entered into the RADIUS server for user authentication.

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

Q. Why do I need to authenticate my Wi-Fi Array units?

- A.** When deploying multiple Wi-Fi Arrays, you may need to define which units are part of which wireless network (for example, if you are establishing more than one network). In this case, you need to employ the Xirrus Management System (XMS) which can authenticate your Arrays automatically and ensure that only authorized units are associated with the defined wireless network.

Q. What is rogue AP (Access Point) detection?

- A.** The Wi-Fi Array has a dedicated radio, IAP abg(n)2, which constantly scans the local wireless environment for rogue APs (non-Xirrus devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

See Also

Contact Information

General Hints and Tips

Multiple SSIDs

VLAN Support

VLAN Support

Q. What Are VLANs?

- A.** VLANs (Virtual Local Area Networks) are a logical grouping of network devices that share a common network broadcast domain. Members of a

particular VLAN can be on any segment of the physical network but logically only members of a particular VLAN can see each other.

VLANs are defined and implemented using the wired network switches that are VLAN capable. Packets are tagged for transmission on a particular VLAN according to the IEEE 802.1Q standard, with VLAN switches processing packets according to the tag.

Q. What would I use VLANs for?

- A.** Logically separating different types of users, systems, applications, or other logical division aids in performance and management of different network devices. Different VLANs can also be assigned with different packet priorities to prioritize packets from one VLAN over packets from another VLAN.

VLANs are managed by software settings—instead of physically plugging in and moving network cables and users—which helps to ease network management tasks.

Q. What are Wireless VLANs?

- A.** Wireless VLANs allow similar functionality to the wired VLAN definitions and extend the operation of wired VLANs to the wireless side of the network.

Wireless VLANs can be mapped to wireless SSIDs so that traffic from wired VLANs can be sent to wireless users of a particular SSID. The reverse is also true, where wireless traffic originating from a particular SSID can be tagged for transmission on a particular wired VLAN.

Sixteen SSIDs can be defined on your Wi-Fi Array, allowing a total of sixteen VLANs to be accessed (one per SSID).

As an example, to provide guest user access an SSID of **guest** might be created. This SSID could be mapped to a wired VLAN that segregates unknown users from the rest of the wired network and restricts them to Internet access only. Wireless users could then associate to the wireless network via the **guest** SSID and obtain access to the Internet through the

selected VLAN, but would be able to access other privileged network resources.

See Also

Contact Information

General Hints and Tips

Multiple SSIDs

Security

Array Monitor and Radio Assurance Capabilities

All models of the Wi-Fi Array have a monitor radio, **abg(n)2**, that checks that the Array's radios are functioning correctly, and acts as a dedicated threat sensor to detect and prevent intrusion from rogue access points.

Enabling Monitoring on the Array

IAP **abg(n)2** may be set to monitor the Array or to be a normal IAP radio. In order to enable the functions required for intrusion detection and for monitoring the other Array radios, you **must** configure **abg(n)2** on the IAP Settings window as follows:

- Check the **Enabled** checkbox.
- Set **Mode** to **Monitor**.
- Set **Channel** to **Monitor**.

The settings above will automatically set the **Antenna** selection to **Internal-Omni.**, also required for monitoring. See the “[IAP Settings](#)” on page 255 for more details. The values above are the factory default settings for the Array.

How Monitoring Works

When the monitor radio **abg(n)2** has been configured as just described, it performs these steps continuously (24/7) to check the other radios on the Array and detect possible intrusions:

1. The monitor radio scans all channels with a 200ms dwell time, hitting all channels about once every 10 seconds.
2. Each time it tunes to a new channel it sends out a probe request in an attempt to smoke out rogues.
3. It then listens for all probe responses and beacons to detect any rogues within earshot.
4. Array radios respond to that probe request with a probe response.

Intrusion Detection is enabled or disabled separately from monitoring. See [Step 1](#) in “[Advanced RF Settings](#)” on page 275. Note that the **Advanced** setting is only used with the optional Xirrus Defense Module (XDM) software package.

Radio Assurance

The Array is capable of performing continuous, comprehensive tests on its radios to assure that they are operating properly. Testing is enabled using the **Radio Assurance Mode** setting on the [Advanced RF Settings](#) window (Step 5 in “Advanced RF Settings” on page 275). When this mode is enabled, IAP abg(n)2 performs loopback tests on the Array. Radio Assurance Mode requires **Intrusion Detection** to be set to **Standard** (See Step 1 in “Advanced RF Settings” on page 275).

When **Radio Assurance Mode** is enabled:

1. The Array keeps track of whether or not it hears beacons and probe responses from the Array’s radios.
2. After 10 minutes (roughly 60 passes on a particular channel by the monitor radio), if it has not heard beacons or probe responses from one of the Array’s radios it issues an alert in the Syslog. If repair is allowed (see “[Radio Assurance Options](#)” on page 408), the Array will reset and reprogram that particular radio at the Physical Layer (PHY—Layer 1). This action takes under 100ms and stations are not deauthenticated, thus users should not be impacted.
3. After another 10 minutes (roughly another 60 passes), if the monitor still has not heard beacons or probe responses from the malfunctioning radio it will again issue an alert in the Syslog. If repair is allowed, the Array will reset and reprogram the MAC (the lower sublayer of the Data Link Layer) and then all of the PHYs. This is a global action that affects all radios. This action takes roughly 300ms and stations are not deauthenticated, thus users should not be impacted.
4. After another 10 minutes, if the monitor still has not heard beacons or probe responses from that radio, it will again syslog the issue. If reboot is allowed (see “[Radio Assurance Options](#)” on page 408), the Array will schedule a reboot. This reboot will occur at one of the following times, whichever occurs first:
 - When no stations are associated to the Array
 - Midnight

Radio Assurance Options

If the monitor detects a problem with an Array radio as described above, it will take action according to the preference that you have specified in the **Radio Assurance Mode** setting on the [Advanced RF Settings](#) window (see [Step 5 page 278](#)):

- **Failure alerts only**—The Array will issue alerts in the Syslog, but will not initiate repairs or reboots.
- **Failure alerts & repairs, but no reboots**—The Array will issue alerts and perform resets of the PHY and MAC as described above.
- **Failure alerts & repairs & reboots if needed**—The Array will issue alerts, perform resets of the PHY and MAC, and schedule reboots as described above.
- **Disabled**—Disable IAP loopback tests (no self-monitoring occurs). Loopback tests are disabled by default.

Upgrading the Array via CLI

If you are experiencing difficulties communicating with the Array using the Web Management Interface, the Array provides lower-level facilities that may be used to accomplish an upgrade via the CLI and the Xirrus Boot Loader (XBL).

1. Download the latest software update from the Xirrus FTP site using your Enhanced Care FTP username and password. If you do not have an FTP username and password, contact Xirrus Customer Service for assistance (support@xirrus.com). The software update is provided as a zip file. Unzip the contents to a local temp directory. Take note of the extracted file name in case you need it later on—you may also need to copy this file elsewhere on the network depending on your situation.
2. Install a TFTP server software package if you don't have one running. It may be installed on any PC on your network, including your desktop or laptop. The Solar Winds version is freeware and works well.

<http://support.solarwinds.net/updates/New-customerFree.cfm?ProdId=52>

The TFTP install process creates the **TFTP-Root** directory on your C: drive, which is the default target for sending and receiving files. This may be changed if desired. This directory is where you will place the extracted Xirrus software update file(s). If you install the TFTP server on the same computer to which you extracted the file, you may change the TFTP directory to C:\xirrus if desired.

You must make the following change to the default configuration of the Solar Winds TFTP server. In the **File/Configure** menu, select **Security**, then select **Transmit only** and click **OK**.

3. Determine the IP address of the computer hosting the TFTP server. (To display the IP address, open a command prompt and type **ipconfig**)
4. Connect your Array to the computer running TFTP using a serial cable, and open a terminal program if you haven't already. Attach a network cable to the Array's GIG1 port, if it is not already part of your network.

Boot your Array and watch the progress messages. When **Press space bar to exit to bootloader:** is displayed, press the space bar. The rest of this procedure is performed using the bootloader.

The following steps assume that you are running DHCP on your local network.

5. Type **dhcp** and hit return. This instructs the Array to obtain a DHCP address and use it during this boot in the bootloader environment.
6. Type **dir** and hit return to see what's currently in the compact flash.
7. Type **del** and hit return to delete the contents of the compact flash.
8. Type **update server <TFTP-server-ip-addr> xs-3.x-xxxx.bin** (the actual Xirrus file name will vary depending on Array model number and software version—use the file name from your software update) and hit return. The software update will be transferred to the Array's memory and will be written to the it's compact flash card. (See output below.)
9. Type **reset** and hit return. Your Array will reboot, running your new version of software.

Sample Output for the Upgrade Procedure:

The user actions are highlighted in the output below, for clarity.

```
Username: admin
```

```
Password: *****
```

```
Xirrus-WiFi-Array# configure
```

```
Xirrus-WiFi-Array(config)# reboot
```

```
Are you sure you want to reboot? [yes/no]: yes
```

```
Array is being rebooted.
```

```
Xirrus Boot Loader 1.0.0 (Oct 17 2006 - 13:11:42), Build: 2725
```

```
Processor | Motorola PowerPC, PVR=80200020 SVR=80300020
```

```
Board | Xirrus MPC8540 CPU Board
```

```
Clocks | CPU : 825 MHz DDR : 330 MHz Local Bus: 41 MHz
```


L1 cache | Data: 32 KB Inst: 32 KB Status : Enabled
Watchdog | Enabled (5 secs)
I2C Bus | 400 KHz
DTT | CPU:34C RF0:34C RF1:34C RF2:27C RF3:29C
RTC | Wed 2007-Nov-05 6:43:14 GMT
System DDR | 256 MB, Unbuffered Non-ECC (2T)
L2 cache | 256 KB, Enabled
FLASH | 4 MB, CRC: OK
FPGA | 2 Devices programmed
Packet DDR | 256 MB, Unbuffered Non-ECC, Enabled
Network | Mot FEC Mot TSEC1 [Primary] Mot TSEC2
IDE Bus 0 | OK
CFCard | 122 MB, Model: Hitachi XXM2.3.0
Environment | 4 KB, Initialized

In: serial
Out: serial
Err: serial

Press space bar to exit to bootloader:

```
XBL>dhcp
[DHCP ] Device : Mot TSEC1 1000BT Full Duplex
[DHCP ] IP Addr : 192.168.39.195
XBL>dir
```

[CFCard] Directory of /

Date	Time	Size	File or Directory name
2007-Nov-05	6:01:56	29	lastboot
2007-Apr-05	15:47:46	28210390	xs-3.1-0433.bak
2007-Mar-01	16:39:42		storage/
2007-Apr-05	15:56:38	28210430	xs-3.1-0440.bin
2007-Mar-03	0:56:28		wpr/

3 file(s), 2 dir(s)

```
XBL>del *
[CFCard] Delete : 2 file(s) deleted

XBL>update server 192.168.39.102 xs-3.0-0425.bin

[TFTP ] Device : Mot TSEC1 1000BT Full Duplex
[TFTP ] Client : 192.168.39.195
[TFTP ] Server : 192.168.39.102
[TFTP ] File : xs-3.0-0425.bin
[TFTP ] Address : 0x1000000
[TFTP ] Loading : #####
[TFTP ] Loading : #####
[TFTP ] Loading : ##### done
[TFTP ] Complete: 12.9 sec, 2.1 MB/sec
[TFTP ] Bytes : 27752465 (1a77811 hex)
[CFCard] File : xs-3.0-0425.bin
[CFCard] Address : 0x1000000
[CFCard] Saving : ##### done
[CFCard] Complete: 137.4 sec, 197.2 KB/sec
[CFCard] Bytes : 27752465 (1a77811 hex)
```

```
XBL>reset
[RESET ]
```

Xirrus Boot Loader 1.0.0 (Oct 17 2006 - 13:11:42), Build: 2725

```
Processor | Motorola PowerPC, PVR=80200020 SVR=80300020
Board     | Xirrus MPC8540 CPU Board
Clocks    | CPU : 825 MHz  DDR : 330 MHz  Local Bus: 41 MHz
L1 cache  | Data: 32 KB  Inst: 32 KB  Status : Enabled
Watchdog  | Enabled (5 secs)
I2C Bus   | 400 KHz
DTT       | CPU:33C RF0:32C RF1:31C RF2:26C RF3:27C
RTC       | Wed 2007-Nov-05 6:48:44 GMT
System DDR | 256 MB, Unbuffered Non-ECC (2T)
```

L2 cache | 256 KB, Enabled
FLASH | 4 MB, CRC: OK
FPGA | 2 Devices programmed
Packet DDR | 256 MB, Unbuffered Non-ECC, Enabled
Network | Mot FEC Mot TSEC1 [Primary] Mot TSEC2
IDE Bus 0 | OK
CFCard | 122 MB, Model: Hitachi XXM2.3.0
Environment | 4 KB, Initialized

In: serial
Out: serial
Err: serial

Press space bar to exit to bootloader:

[CFCard] File : xs*.bin
[CFCard] Address : 0x1000000
[CFCard] Loading : ##### done
[CFCard] Complete: 26.9 sec, 1.0 MB/sec
[CFCard] Bytes : 27752465 (1a77811 hex)
[Boot] Address : 0x01000000
[Boot] Image : Verifying checksum OK
[Boot] Unzip : Multi-File Image OK
[Boot] Initrd : Loading RAMDisk Image
[Boot] Initrd : Verifying checksum OK
[Boot] Execute : Transferring control to OS

Initializing hardware OK

Xirrus Wi-Fi Array
ArrayOS Version 3.0-425
Copyright (c) 2005-2007 Xirrus, Inc.
<http://www.xirrus.com>

Username:

Power over Gigabit Ethernet Compatibility Matrix

The Xirrus Power over Gigabit Ethernet (PoGE) solution includes different modules to be used with particular Array models. The following two tables indicate the proper PoGE injector/splitters to use with each Array. **X** indicates products are INCOMPATIBLE. NA=Not Applicable.

Table 1: Current PoGE Injectors/Splitters

Array Model	Compatible Xirrus Injector/Splitter	XP1-MSI-X Injector	XP8-MSI Injector	XP1-MSI Injector	XP1-SPL Splitter
XS4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS8, XN4	Works with any PoGE injector, no splitter required	✓	✓	✓	NA
XN16/XN12/ XN8/XN4, XS16/XS12	Works with two injector options, no splitter required	✓	✓ ¹	X	NA
XS-3500-4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS-3700-8, DC (modified) ²	Works only with legacy injector/splitter models, see Table 2 .	X	X	X	X
XS-3900-16, DC (modified) ²		X	X	X	X
XS-3700-8, DC (unmodified)	DO NOT connect unmodified XS-3700/3900 with -H or -HX injectors or splitter.	X	✓	✓	✓
XS-3900-16, DC (unmodified)		X	✓ ¹	✓	✓

1. The 8-port XP8-MSI-H and XP8-MSI injectors each power up to eight 4-port or 8-port Arrays; or four 16-port Arrays.
2. To see whether an Array is modified, see [Figure 188 on page 416](#).



IMPORTANT NOTE: Only use -H versions of injectors/splitters together, and use non-H versions of injectors/splitters together - do not mix or match the two types.

Table 2: Legacy PoGE Models

Array Model	Compatible Xirrus Injector/Splitter	XP1-MSI-H Injector	XP1-MSI-HX Injector	XP8-MSI-H Injector	XP1-SPL-H Splitter
XS4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS8	Works with any PoGE injector, no splitter required	✓	✓	✓	NA
XS16/XS12	Works with two injector options, no splitter required	X	✓	✓ ¹	NA
XS-3500-4	Works with any PoGE injector/splitter	✓	✓	✓	✓
XS-3700-8, DC (modified) ²	Works only with -H version injector/splitters	✓	✓	✓	✓
XS-3900-16, DC (modified) ²	Works only with -HX or XP8 version injector/splitters	X	✓	✓ ¹	✓
XS-3700-8, DC (unmodified)	DO NOT connect unmodified XS-3700/3900 with -H or -HX injectors or splitter.	X	X	X	X
XS-3900-16, DC (unmodified)		X	X	X	X

1. The 8-port XP8-MSI-H and XP8-MSI injectors each power up to eight 4-port or 8-port Arrays; or four 16-port Arrays.
2. To see whether an Array is modified, see [Figure 188 on page 416](#).

Determining If an XS-3700 or XS-3900 is Modified for PoGE

The following pictures show how different Array power supply types look. On the XS-3700/XS-3900 Arrays, it is VERY important to note the yellow sticker (Figure 188 on page 416) that differentiates between modified and unmodified DC power versions.

Connect Data OUT to Gig1 or Gig2 port with short cable

Connect Cat 5e (from PoGE Injector) to IN port

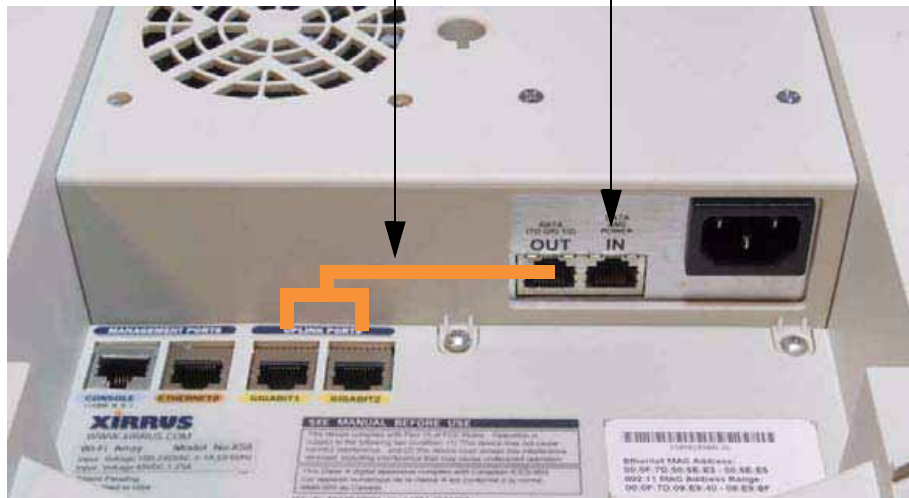


Figure 187. XN8/XN12/XN16/XS8/XS12/XS16: Integrated Splitter

Modified XS-3700/XS-3900 (DC Version)
 Accepts XP1-SPL-H splitter output
 Must have yellow label

Unmodified XS-3700/XS-3900 (DC Version)
 Accepts XP1-SPL splitter output
 Has no yellow label

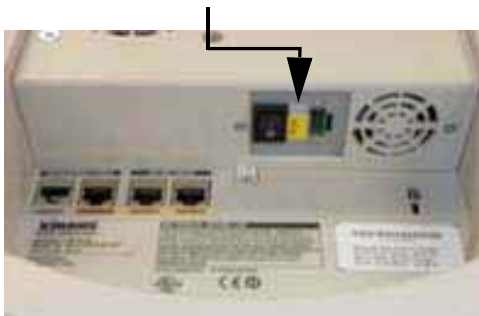


Figure 188. Determining if XS-3700/3900 is modified

Contact Information

Xirrus, Inc. is located in Thousand Oaks, California, just 55 minutes northwest of downtown Los Angeles and 40 minutes southeast of Santa Barbara.

Xirrus, Inc.

2101 Corporate Center Drive

Thousand Oaks, CA 91320

USA

Tel: 1.805.262.1600

1.800.947.7871 Toll Free in the US

Fax: 1.866.462.3980

www.xirrus.com

support.xirrus.com



Appendix D: Implementing PCI DSS

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed by major credit card companies to help those that process credit card transactions (or cardholder information) in order to secure cardholder information and protect it from unauthorized access, fraud and other security issues. The major contributors to the standard are VISA, MasterCard, American Express, JCB, and Discover. The standard also helps consolidate various individual standards that were developed by each of the listed card companies. Merchants or others who process credit card transactions are required to comply with the standard and to prove their compliance by way of an audit from a Qualified Security Assessor.

PCI DSS lays out a set of requirements that must be met in order to provide adequate security for sensitive data.

Payment Card Industry Data Security Standard Overview

The PCI Data Security Standard (PCI DSS) has 12 main requirements that are grouped into six *control objectives*. The following table lists each control objective and the specific requirements for each objective. For the latest updates to this list, check the PCI Security Standards Web site: www.pcisecuritystandards.org.

PCI DSS Control Objectives and Associated Requirements
<p>Objective: Build and Maintain a Secure Network</p> <ul style="list-style-type: none"> ● Requirement 1: Install and maintain a firewall configuration to protect cardholder data. ● Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
<p>Objective: Protect Cardholder Data</p> <ul style="list-style-type: none"> ● Requirement 3: Protect stored cardholder data. ● Requirement 4: Encrypt transmission of cardholder data across open, public networks.

PCI DSS Control Objectives and Associated Requirements

Objective: Maintain a Vulnerability Management Program

- Requirement 5: Use and regularly update anti-virus software.
- Requirement 6: Develop and maintain secure systems and applications.

Objective: Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know.
- Requirement 8: Assign a unique ID to each person with computer access.
- Requirement 9: Restrict physical access to cardholder data.

Objective: Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data.
- Requirement 11: Regularly test security systems and processes.

Objective: Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security.

PCI DSS and Wireless

The Xirrus Wi-Fi Array provides numerous security features that allow it to be a component of a PCI DSS-compliant network. The following sections indicate the specific features that allow the Xirrus Wi-Fi Array to operate in a PCI DSS mode.

The Xirrus Array PCI Compliance Configuration

The check list below is designed to help ensure that Xirrus Wi-Fi Arrays are configured in a manner that is supportive of PCI Data Security Standards. Detailed configuration steps for each item are found in the referenced section of the User's Guide.

✓	Xirrus Wi-Fi Array Configuration for PCI DSS	See...
<ul style="list-style-type: none"> () () 	<ul style="list-style-type: none"> Register at the Xirrus Support Site to ensure notification and access to software updates. Confirm that the latest version of the Array OS is being used by checking the Xirrus web site. 	<p style="text-align: center;">support.xirrus.com</p>
()	<p>Enable PCI Mode after configuring the Array in a PCI compliant state to ensure configuration changes cannot be saved that would invalidate a PCI compliant configuration. This item is covered on the following pages.</p>	<p>The pci-audit Command, p. 422</p>
()	<p>Allow only necessary protocols and networks to be accessed by configuring your corporate firewall or using the internal Array firewall.</p>	<p>Filters, p. 289</p>
<ul style="list-style-type: none"> () () () () () () 	<ul style="list-style-type: none"> Change the default Admin account password. Remove any unnecessary admin or user accounts. Change the SNMP community string from the default password. Use WPA2 and 802.1x authentication. Change default SSID from Xirrus to a user-defined SSID. Disable SSID broadcast for all PCI compliant SSIDs. 	<ul style="list-style-type: none"> Express Setup, p. 176 Admin Management, p. 215 SNMP, p. 200 SSIDs, p. 235 and Global Settings, p. 225 SSIDs, p. 235 SSIDs, p. 235
<ul style="list-style-type: none"> () () () 	<ul style="list-style-type: none"> Enable Secure Shell (ssh) for CLI (command line) access. Confirm telnet access is disabled (done by default). Confirm management over the wireless network is disabled. 	<ul style="list-style-type: none"> Management Control, p. 219 Global Settings (IAP), p. 260

✓	Xirrus Wi-Fi Array Configuration for PCI DSS	See...
() ()	Check that external RADIUS servers have been configured for use with 802.1x and WPA/WPA2 wireless security. Ensure that Array Administration Accounts are being validated by External RADIUS servers.	SSIDs, p. 235 and Global Settings, p. 225 Admin RADIUS, p. 216
()	Ensure that each Xirrus Array is physically inaccessible such that console ports and management ports are not accessible.	Securing the Array, p. 94 See Indoor Enclosure
() ()	Enable syslog messaging and define a syslog server on the wired network to receive syslog messages. Enable NTP and define an NTP server (optional).	System Log, p. 197 Time Settings (NTP), p. 194
()	Enable the RF Monitor radio in the Xirrus Array. Categorize known or approved devices as such. Respond to any alert of unknown or unapproved wireless devices discovered by the RF Monitor.	IAP Settings, p. 255 Rogue Control List, p. 233 Intrusion Detection, p. 148

Additional information regarding implementation of PCI DSS on the Wi-Fi Array is described in the Xirrus White Paper, [PCI Data Security Standard](#), available on the Xirrus web site.

The `pci-audit` Command

The Array provides a CLI command, `pci-audit`, that checks whether the Array's configuration satisfies PCI DSS wireless requirements. This command does not change any parameters, but will inform you of any violations that exist. Furthermore, the command `pci-audit enable` will put the Array in PCI Mode and monitor changes that you make to the Array's configuration in CLI or the WMI. PCI Mode will warn you (and issue a Syslog message) if the change violates PCI DSS requirements. A warning is issued when a non-compliant change is first applied to the Array, and also if you attempt to save a configuration that is non-compliant. Use this command in conjunction with [The Xirrus Array PCI](#)

Compliance Configuration above to ensure that you are using the Array in accordance with the PCI DSS requirements.

The pci-audit command checks items such as:

- Telnet is disabled.
- Admin RADIUS is enabled (admin login authentication is via RADIUS server).
- An external Syslog server is in use.
- All SSIDs must set encryption to WPA or better (which also enforces 802.1x authentication)

Sample output from this command is shown below.

```
SS-Array(config)# pci-audit
PCI audit failure: telnet enabled.
PCI audit failure: admin RADIUS authentication disabled.
PCI audit failure: SSID ssid2 encryption too weak.
PCI audit failure: SSID ssid3 encryption too weak.
PCI audit failure: SSID ssid4 encryption too weak.
PCI audit failure: SSID ssid5 encryption too weak.
PCI audit failure: SSID ssid6 encryption too weak.
```

Figure 189. Sample output of pci-audit command

Additional Resources

- PCI Security Standards Web site: www.pcisecuritystandards.org
- List of Qualified PCI Security Assessors: www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- For the latest version of the Xirrus White Paper, [PCI Data Security Standard](#), and the latest versions of Xirrus software, please check www.xirrus.com

Appendix E: Implementing FIPS Security

Wi-Fi Arrays may be configured to satisfy the requirements for Level 2 of [Federal Information Processing Standard \(FIPS\) Publication 140-2](#). The procedure in this section lists simple steps that must be followed exactly to implement FIPS 140-2, Level 2. The procedure includes physical actions, and parameters that must be set in Web Management Interface (WMI) windows in the Security section and in other sections.

The following topics are discussed:

- “To implement FIPS 140-2, Level 2 using WMI” on page 425.
- “To check if an Array is in FIPS mode:” on page 431
- “To implement FIPS 140-2, Level 2 using CLI:” on page 431

To implement FIPS 140-2, Level 2 using WMI

1. Apply the supplied tamper-evident seals to the unit as indicated in the figures below. The procedure is slightly different, depending on the model.
 - Before you apply the tamper-evident seal, clean the area of any grease, dirt, or oil. We recommend using alcohol-based cleaning pads for this.
 - Each seal must be applied to straddle both sides of an opening so that it will show if an attempt has been made to open the Array.

- XS16, XS12, XS8, XS-3900, or XS-3700—Apply two seals, one on either side of the Array about 180° apart from each other, as shown. Apply a third seal to the access panel opening, as shown. **IMPORTANT: Make sure that each seal straddles a seam.**

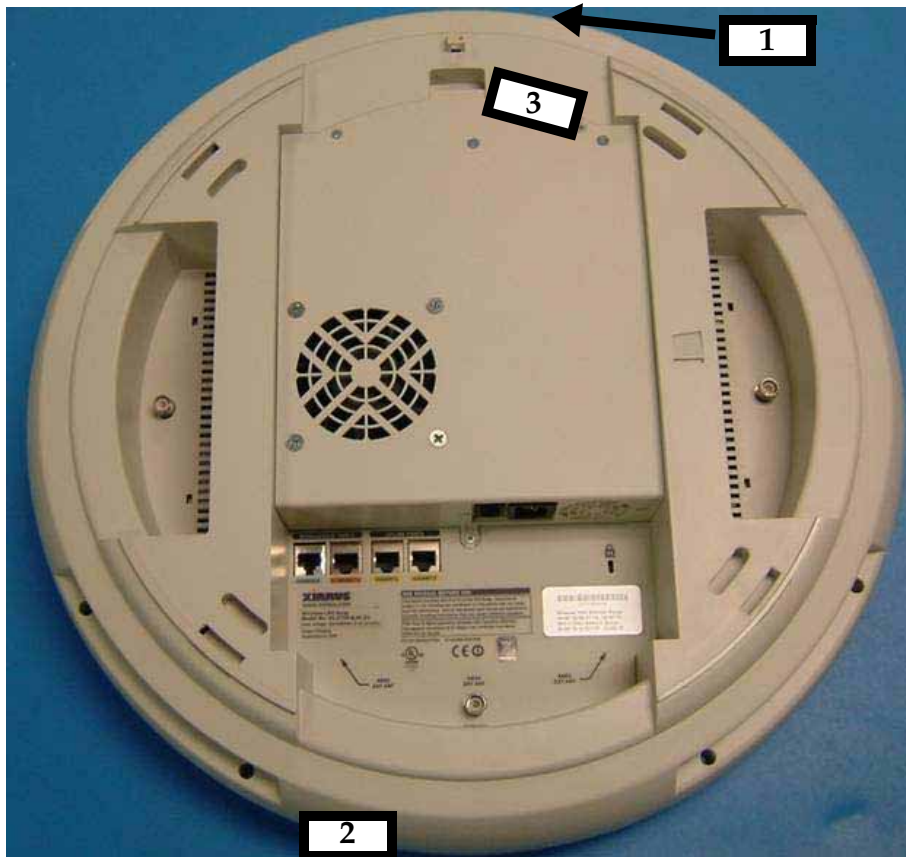


Figure 190. Applying Three Seals to XS16/XS12/XS8 or XS-3900/XS-3700

- XS4 or XS-3500—Apply two seals, one on either side of the Array about 180° apart from each other, as shown. **IMPORTANT: Make sure that each seal straddles a seam.**

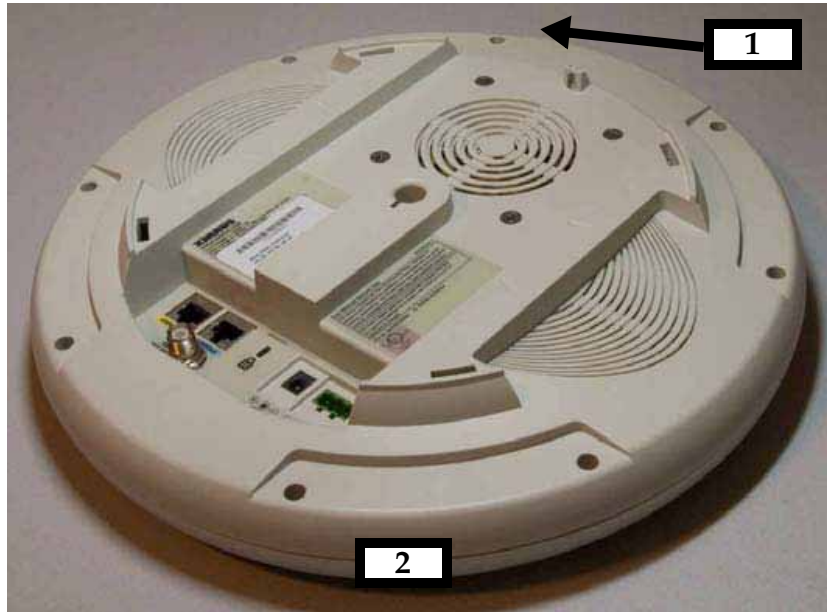


Figure 191. Applying Two Tamper-evident seals to the XS4 or XS-3500

2. Enable HTTPS using the CLI if it is not already enabled, using the following command:

```
Xirrus_Wi-Fi_Array(config)# https on
```

This allows the Web Management Interface to be used for the rest of this procedure. HTTPS is enabled on Arrays by default.

3. Select the SSIDs/SSID Management window. Set **Encryption Type** to **WPA2** (Figure 192). Click **Modify**, then **Save**. Make sure that this is set for each SSID.

The screenshot shows the 'XS-3900 Wi-Fi Array' management interface. The top right corner displays the XIRRUS logo and the system uptime: 'Uptime - 6 days 1 hour 1 minute'. On the left, a sidebar menu includes sections for 'Status' (Network Map, Array Status, Array Info, Show Config, Event Log, Stations), 'Configuration' (Express Setup, Network, Services, VLANs, DHCP Server, Security, SSIDs), and 'Tools' (IAPs, WDS, Filters, Tools, Logout). The 'SSIDs' section is expanded, showing 'SSID Limits Summary' and 'SSID Management'. The 'SSID Management' section is active, displaying a table of SSIDs. The first SSID is 'xirus (Broadcast)'. Below the table, various configuration options are shown for this SSID: State (radio buttons for Enable and Disable, with Enable selected), Broadcast SSID (radio buttons for Enable and Disable, with Enable selected), Band Association (radio buttons for 802.11a, 802.11b/g, and Both, with Both selected), QoS Priority (dropdown menu set to 2), VLAN ID (dropdown menu set to none) and VLAN Number (input field), Internal DHCP Pool Assigned (dropdown menu set to none), Station Limit (input field set to 1024), Overall Traffic Limit (checkbox for Unlimited selected, with a Packets/Sec input field), Traffic Limit per Station (checkbox for Unlimited selected, with a Packets/Sec input field), Day/Time Limit (checkbox for Active selected), Time Active (checkbox for Always selected, with Time On and Time Off input fields), Days Active (checkboxes for All, Sun, Mon, Tue, Wed, Thu, Fri, Sat, with All selected), Web Page Redirect (WPR) (radio buttons for Enable and Disable, with Disable selected), Authentication Type (dropdown menu set to Open), Encryption Type (dropdown menu set to WPA2), and Security Settings (radio buttons for Use Global Settings and Use Unique Settings, with Use Global Settings selected). At the bottom right of the configuration area are 'Modify' and 'Save' buttons. In the bottom left corner, a circular message summary shows: Critical Msgs: 60, Warning Msgs: 0, and General Msgs: 73.

Figure 192. SSID Management Window

- In the Security/Global Settings window, select **No** for TKIP Enabled and **Yes** for AES Enabled. Click **Apply**, then **Save**.

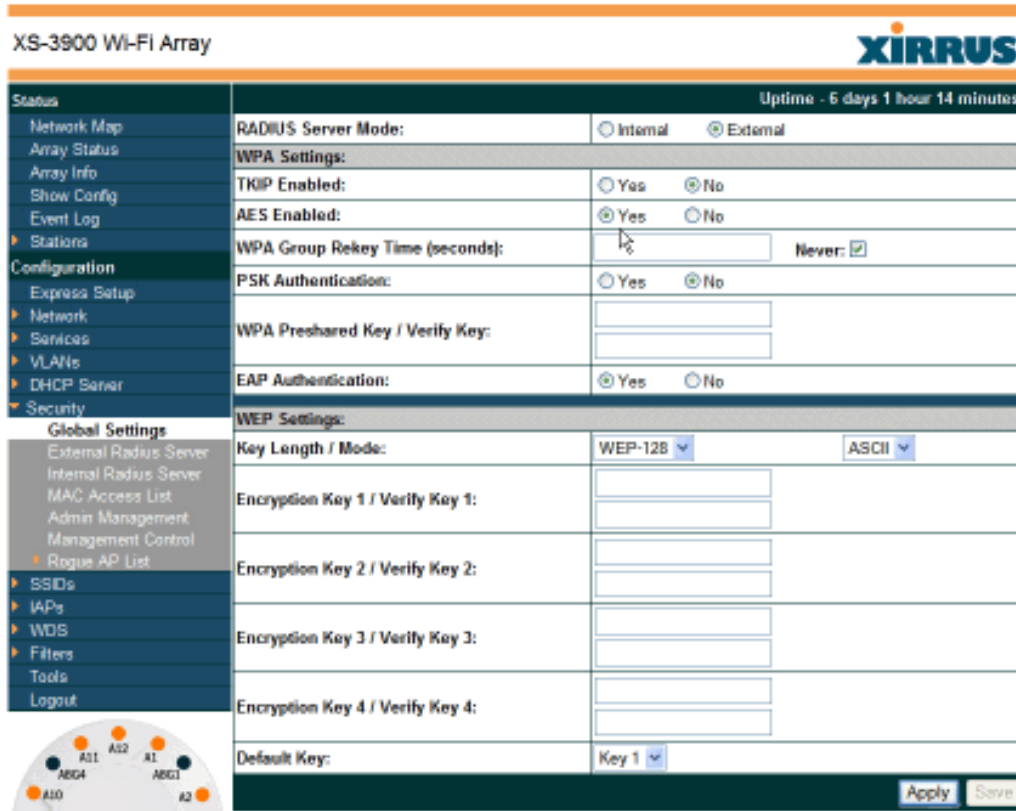


Figure 193. Security/Global Settings Window

- In the Security/Management Control window, select **Yes** for **Enable Management over SSH**. Select **No** for **Enable Management over Telnet** and for **Enable Management over IAPs**. Click **Apply**, then **Save**.

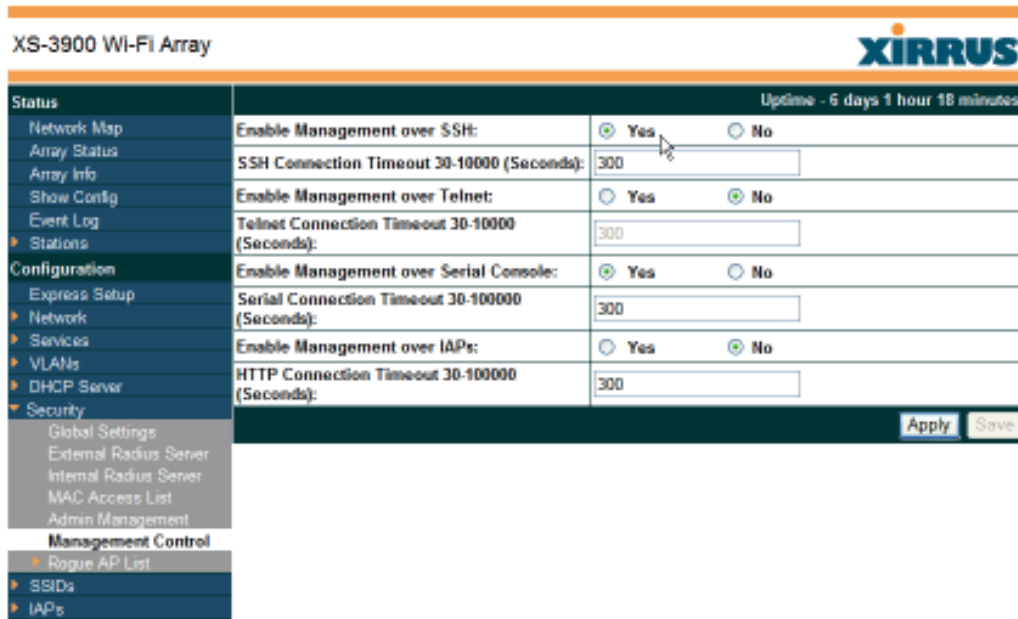


Figure 194. Security/Management Control Window

- In the Services/SNMP window, select **No** for **Enable SNMP**. Click **Apply**, then **Save**.

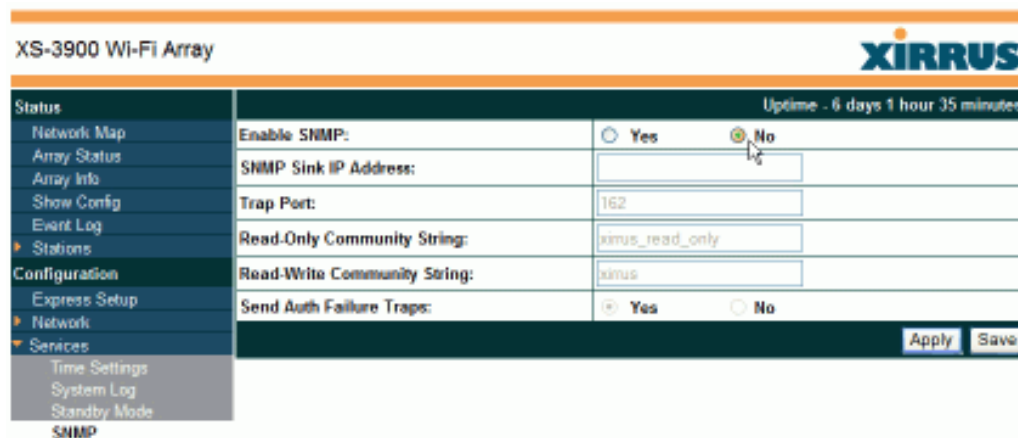


Figure 195. Services/SNMP Window

- In the IAPs/Global Settings window, select **Off** for **Fast Roaming**. Click **Apply**, then **Save**.

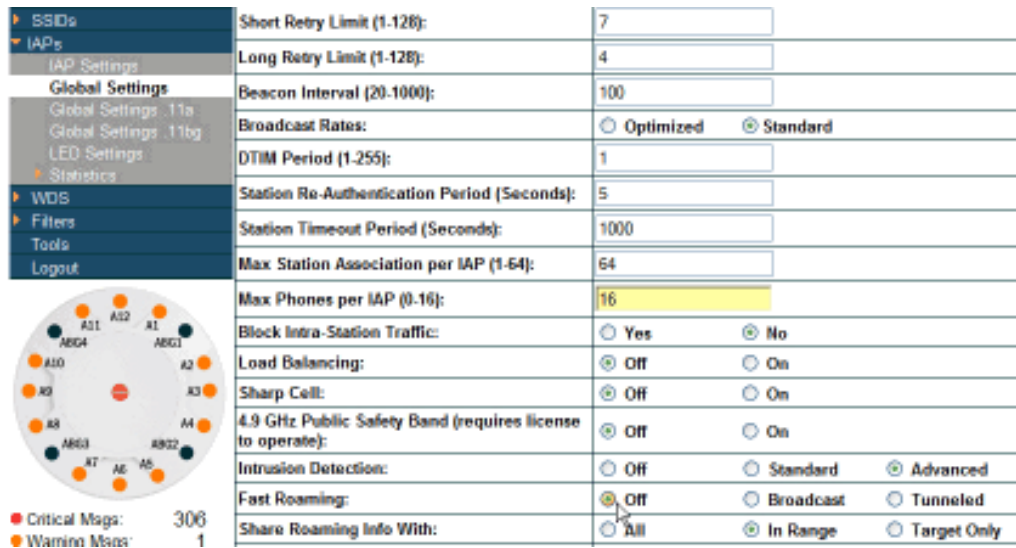


Figure 196. IAPs/Global Settings Screen

To check if an Array is in FIPS mode:

You may determine whether or not the Array is running in FIPS mode by verifying that the settings described in the previous procedure are in effect.

To implement FIPS 140-2, Level 2 using CLI:

- The following CLI command will perform all of the settings required to put the Array in FIPS mode:.

Xirrus_Wi-Fi_Array(config)# fips on

This command remembers your previous settings for FIPS-related attributes. They will be restored if you use the **fips off** command.

Use the **save** command to save these changes to flash memory.

- Use the **fips off** command if you would like to revert the FIPS settings back to the values they had before you entered the **fips on** command.

Xirrus_Wi-Fi_Array(config)# fips off

Use the **save** command to save these changes to flash memory.

See Also

The Web Management Interface

The Command Line Interface

Appendix F: Notices

This appendix contains the following information:

- “Notices” on page 433
- “EU Directive 1999/5/EC Compliance Information” on page 436
- “Safety Warnings” on page 443
- “Translated Safety Warnings” on page 444
- “Software Warranty and License Agreement” on page 445
- “Hardware Warranty Agreement” on page 452

Notices

FCC Notice

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

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

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

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

RF Radiation Hazard Warning

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

Non-Modification Statement

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

Indoor Use

This product has been designed for indoor use. Operation of channels in the 5150MHz to 5250MHz band is permitted indoors only to reduce the potential for harmful interference to co-channel mobile satellite systems.

Cable Runs for Power over Gigabit Ethernet (PoGE)

If using PoGE, the Array must be connected to PoGE networks without routing cabling to the outside plant—this ensures that cabling is not exposed to lightning strikes or possible cross over from high voltage.

Battery Warning

Caution! The Array contains a battery which is not to be replaced by the customer. Danger of Explosion exists if the battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Power Cord

If you will be using the Array with a power cord, you must use a UL-Approved cord (supplied with the unit). Order new power cords from the Xirrus product list—Xirrus supplies only UL-approved power cords.

Maximum Antenna Gain

Currently, the maximum antenna gain for external antennas is limited to 5.2dBi for operation in the 2400MHz to 2483.5MHz, 5150MHz to 5250MHz and 5725MHz to 5825MHz bands. The antenna gains must not exceed maximum EIRP limits set by the FCC / Industry Canada.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5150MHz to 5250MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LELAN devices used in Canada.

Industry Canada Notice and Marking

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

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

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

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

EU Directive 1999/5/EC Compliance Information

This section contains compliance information for the Xirrus Wi-Fi Array family of products, which includes the XN16, XN12, XN8, XN4, XS16, XS12, XS8, XS4, XS-3900, XS-3700 and XS-3500. The compliance information contained in this section is relevant to the European Union and other countries that have implemented the EU Directive 1999/5/EC.

Declaration of Conformity

- Cesky [Czech]** Toto zahzení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
- Dansk [Danish]** Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
- Deutsch [German]** Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
- Eesti [Estonian]** See seande vastab direktiivi 1999/5/EU oluliste nõuetele ja teistele asjakohastele sätetele.
- English** This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
- Español [Spain]** Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
- Ελληνική [Greek]** Αυτό το εξοπλισμό είναι σε συμμόρφωση με τις ουσιαστικές απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
- Français [French]** Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.

- Íslenska [Icelandic]** Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
- Italiano [Italian]** Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
- Latviski [Latvian]** Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajā prasībām un citiem ar to saistītajiem noteikumiem.
- Lietuvių [Lithuanian]** Šis įrenginys tenkina 1995/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.
- Nederlands [Dutch]** Dit apparant voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1995/5/EC.
- Malti [Maltese]** Dan l-apparant huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
- Magyar [Hungarian]** Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
- Norsk [Norwegian]** Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
- Polski [Polish]** Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi mi warunkami określony mi Dyrektywą. UE:1999/5/EC.
- Português [Portuguese]** Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
- Slovensko [Slovenian]** Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi popoji Direktive 1999/5/EC.

Slovensky [Slovak] Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.

Suomi [Finnish] Tämä laite täyttää direktiivin 1999/5/ /EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.

Svenska [Swedish] Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

Assessment Criteria

The following standards were applied during the assessment of the product against the requirements of the Directive 1999/5/EC:

- Radio: EN 301 893 and EN 300 328 (if applicable)
- EMC: EN 301 489-1 and EN 301 489-17
- Safety: EN 50371 to EN 50385 and EN 60601

CE Marking

For the Xirrus Wi-Fi Array (XN16, XN12, XN8, XN4, XS16, XS12, XS8, XS4, XS-3900, XS-3700 and XS-3500), the CE mark and Class-2 identifier opposite are affixed to the equipment and its packaging:



WEEE Compliance



- Natural resources were used in the production of this equipment.
- This equipment may contain hazardous substances that could impact the health of the environment.
- In order to avoid harm to the environment and consumption of natural resources, we encourage you to use appropriate take-back systems when disposing of this equipment.
- The appropriate take-back systems will reuse or recycle most of the materials of this equipment in a way that will not harm the environment.
- The crossed-out wheeled bin symbol (in accordance with European Standard EN 50419) invites you to use those take-back systems and advises you not to combine the material with refuse destined for a land fill.
- If you need more information on collection, re-use and recycling systems, please contact your local or regional waste administration.
- Please contact Xirrus for specific information on the environmental performance of our

National Restrictions

In the majority of the EU and other European countries, the 2.4 GHz and 5 GHz bands have been made available for the use of Wireless LANs. The following table provides an overview of the regulatory requirements in general that are applicable for the 2.4 GHz and 5 GHz bands.

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor	Outdoor
2400–2483.5	100	X	X**
5150–5350*	200	X	N/A
5470–5725*	1000	X	X

**Dynamic frequency selection and Transmit Power Control is required in these frequency bands.*

***France is indoor use only in the upper end of the band.*

The requirements for any country may change at any time. Xirrus recommends that you check with local authorities for the current status of their national regulations for both 2.4 GHz and 5 GHz wireless LANs.

The following countries have additional requirements or restrictions than those listed in the above table:

Belgium

The Belgian Institute for Postal Services and Telecommunications (BIPT) must be notified of any outdoor wireless link having a range exceeding 300 meters. Xirrus recommends checking at www.bipt.be for more details.

Draadloze verbindingen voor buitengebruik en met een reikwijdte van meer dan 300 meter dienen aangemeld te worden bij het Belgisch Instituut voor postdiensten en telecommunicatie (BIPT). Zie www.bipt.be voor meer gegevens.

Les liaisons sans fil pour une utilisation en extérieur d'une distance supérieure à 300 mètres doivent être notifiées à l'Institut Belge des services Postaux et des Télécommunications (IBPT). Visitez www.bipt.be pour de plus amples détails.

Greece

A license from EETT is required for the outdoor operation in the 5470 MHz to 5725 MHz band. Xirrus recommends checking www.eett.gr for more details.

Η δη ιουργβάικτ ωνεξωτερικο ρουστη ζ νησν νοτ των 5470–5725 MHz ε ιτρ ετάιωνο ετάά όάδειά της EETT, ου ορηγεβτάι στερά ά ό σ φωνη γν η του ΓΕΕΘΑ. ερισσότερες λε τομ ρειεωστο www.eett.gr

Italy

This product meets the National Radio Interface and the requirements specified in the National Frequency Allocation Table for Italy. Unless this wireless LAN product is operating within the boundaries of the owner's property, its use requires a "general authorization." Please check with www.comunicazioni.it/it/ for more details.

Questo prodotto é conforme alla specifiche di Interfaccia Radio Nazionali e rispetta il Piano Nazionale di ripartizione delle frequenze in Italia. Se non viene installato all'interno del proprio fondo, l'utilizzo di prodotti wireless LAN richiede una "autorizzazione Generale." Consultare www.comunicazioni.it/it/ per maggiori dettagli.

Norway, Switzerland and Liechtenstein

Although Norway, Switzerland and Liechtenstein are not EU member states, the EU Directive 1999/5/EC has also been implemented in those countries.

Calculating the Maximum Output Power

The regulatory limits for maximum output power are specified in EIRP (radiated power). The EIRP level of a device can be calculated by adding the gain of the antenna used (specified in dBi) to the output power available at the connector (specified in dBm).

Antennas

The Xirrus Wi-Fi Array employs integrated antennas that cannot be removed and which are not user accessible. Nevertheless, as regulatory limits are not the same throughout the EU, users may need to adjust the conducted power setting for the radio to meet the EIRP limits applicable in their country or region. Adjustments can be made from the product's management interface—either Web Management Interface (WMI) or Command Line Interface (CLI).

Operating Frequency

The operating frequency in a wireless LAN is determined by the access point. As such, it is important that the access point is correctly configured to meet the local regulations. See [National Restrictions](#) in this section for more information.

If you still have questions regarding the compliance of Xirrus products or you cannot find the information you are looking for, please contact us at:

Xirrus, Inc.

2101 Corporate Center Drive

Thousand Oaks, CA 91320

USA


Tel: 1.805.262.1600


1.800.947.7871 Toll Free in the US


Fax: 1.866.462.3980


www.xirrus.com

Safety Warnings

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

-  **Explosive Device Proximity Warning**
Do not operate the XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 unit near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.


-  **Lightning Activity Warning**
Do not work on the XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 or connect or disconnect cables during periods of lightning activity.


-  **Circuit Breaker Warning**
The XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.


Translated safety warnings appear on the following page.


Translated Safety Warnings

Avertissements de Sécurité

-  **Sécurité**

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

N'utilisez pas l'unité XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.
-  **Foudre**

N'utilisez pas l'unité XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.
-  **Disjoncteur**

L'unité XN16/XN12/XN8/XN4/XS16/XS12/XS8/XS4/XS-3900/XS-3700/XS-3500 dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Software Warranty and License Agreement

THIS SOFTWARE LICENSE AGREEMENT (THE “AGREEMENT”) IS A LEGAL AGREEMENT BETWEEN YOU (“CUSTOMER”) AND LICENSOR (AS DEFINED BELOW) AND GOVERNS THE USE OF THE SOFTWARE INSTALLED ON THE PRODUCT (AS DEFINED BELOW). IF YOU ARE AN EMPLOYEE OR AGENT OF CUSTOMER, YOU HEREBY REPRESENT AND WARRANT TO LICENSOR THAT YOU HAVE THE POWER AND AUTHORITY TO ACCEPT AND TO BIND CUSTOMER TO THE TERMS AND CONDITIONS OF THIS AGREEMENT (INCLUDING ANY THIRD PARTY TERMS SET FORTH HEREIN). IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT RETURN THE PRODUCT AND ALL ACCOMPANYING MATERIALS (INCLUDING ALL DOCUMENTATION) TO THE RELEVANT VENDOR FOR A FULL REFUND OF THE PURCHASE PRICE THEREFOR.

CUSTOMER UNDERSTANDS AND AGREES THAT USE OF THE SOFTWARE SHALL BE DEEMED AN AGREEMENT TO THE TERMS AND CONDITIONS GOVERNING SUCH SOFTWARE AND THAT CUSTOMER IS BOUND BY AND BECOMES A PARTY TO THIS AGREEMENT.

1. Definitions

- 1.1 “Documentation” means the user manuals and all other all documentation, instructions or other similar materials accompanying the Software covering the installation, application, and use thereof.
- 1.2 “Licensor” means XIRRUS and its suppliers.
- 1.3 “Product” means a multi-radio access point containing four or more distinct radios capable of simultaneous operation on four or more non-overlapping channels.
- 1.4 “Software” means, collectively, each of the application and embedded software programs delivered to Customer in connection with this Agreement. For purposes of this Agreement, the term Software shall be deemed to include any and all Documentation and Updates provided with or for the Software.
- 1.5 “Updates” means any bug-fix, maintenance or version release to the Software that may be provided to Customer from Licensor pursuant to this Agreement or pursuant to any separate maintenance and support agreement entered into by and between Licensor and Customer.

2. Grant of Rights

- 2.1 **Software.** Subject to the terms and conditions of this Agreement, Licensor hereby grants to Customer a perpetual, non-exclusive, non-sublicenseable, non-transferable right and license to use the Software solely as installed on the Product in accordance with the accompanying Documentation and for no other purpose.
- 2.2 **Ownership.** The license granted under Sections 2.1 above with respect to the Software does not constitute a transfer or sale of Licensor's or its suppliers' ownership interest in or to the Software, which is solely licensed to Customer. The Software is protected by both national and international intellectual property laws and treaties. Except for the express licenses granted to the Software, Licensor and its suppliers retain all rights, title and interest in and to the Software, including (i) any and all trade secrets, copyrights, patents and other proprietary rights therein or thereto or (ii) any Marks (as defined in Section 2.3 below) used in connection therewith. In no event shall Customer remove, efface or otherwise obscure any Marks contained on or in the Software. All rights not expressly granted herein are reserved by Licensor.
- 2.3 **Copies.** Customer shall not make any copies of the Software but shall be permitted to make a reasonable number of copies of the related Documentation. Whenever Customer copies or reproduces all or any part of the Documentation, Customer shall reproduce all and not efface any titles, trademark symbols, copyright symbols and legends, and other proprietary markings or similar indicia of origin ("Marks") on or in the Documentation.
- 2.4 **Restrictions.** Customer shall not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) sell, rent, lease, license or sublicense, assign or otherwise transfer the Software, or any of Customer's rights and obligations under this Agreement except as expressly permitted herein; (ii) decompile, disassemble, or reverse engineer the Software, in whole or in part, provided that in those jurisdictions in which a total prohibition on any reverse engineering is prohibited as a matter of law and such prohibition is not cured by the fact that this Agreement is subject to the laws of the State of California, Licensor agrees to grant Customer, upon Customer's written request to Licensor, a limited reverse engineering license to permit interoperability of the Software with other software or code used by Customer; (iii) allow access to the Software by any user other than by Customer's employees and contractors who are bound in writing to confidentiality and non-use restrictions at least as protective as those set forth herein; (iv) except as expressly set forth herein, write or develop any derivative software or any other software program based upon the Software; or (v) use any

computer software or hardware which is designated to defeat any copy protection or other use limiting device, including any device intended to limit the number of users or devices accessing the Product.

3. Limited Warranty and Limitation of Liability

3.1 Limited Warranty & Exclusions. Licensor warrants that the Software will perform in substantial accordance with the specifications therefor set forth in the Documentation for a period of ninety [90] days after Customer's acceptance of the terms of this Agreement with respect to the Software ("Warranty Period"). If during the Warranty Period the Software does not perform as warranted, Licensor shall, at its option, correct the relevant Software giving rise to such breach of performance or replace such Software free of charge. THE FOREGOING ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THE FOREGOING WARRANTY. THE WARRANTY SET FORTH ABOVE IS MADE TO AND FOR THE BENEFIT OF CUSTOMER ONLY. The warranty will apply only if (i) the Software has been used at all times and in accordance with the instructions for use set forth in the Documentation and this Agreement; (ii) no modification, alteration or addition has been made to the Software by persons other than Licensor or Licensor's authorized representative; and (iii) the Software or Product on which the Software is installed has not been subject to any unusual electrical charge.

3.2 DISCLAIMER. EXCEPT AS EXPRESSLY STATED IN THIS SECTION 3, ALL ADDITIONAL CONDITIONS, REPRESENTATIONS, AND WARRANTIES, WHETHER IMPLIED, STATUTORY OR OTHERWISE, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, ACCURACY, AGAINST INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE, ARE HEREBY DISCLAIMED BY LICENSOR AND ITS SUPPLIERS. THIS DISCLAIMER SHALL APPLY EVEN IF ANY EXPRESS WARRANTY AND LIMITED REMEDY OFFERED BY LICENSOR FAILS OF ITS ESSENTIAL PURPOSE. ALL WARRANTIES PROVIDED BY LICENSOR ARE SUBJECT TO THE LIMITATIONS OF LIABILITY SET FORTH IN THIS AGREEMENT.

3.3 HAZARDOUS APPLICATIONS. THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF A NUCLEAR FACILITY, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROLS OR OTHER

DEVICES OR SYSTEMS IN WHICH A MALFUNCTION OF THE SOFTWARE WOULD RESULT IN FORESEEABLE RISK OF INJURY OR DEATH TO THE OPERATOR OF THE DEVICE OR SYSTEM OR TO OTHERS (“HAZARDOUS APPLICATIONS”). CUSTOMER ASSUMES ANY AND ALL RISKS, INJURIES, LOSSES, CLAIMS AND ANY OTHER LIABILITIES ARISING OUT OF THE USE OF THE SOFTWARE IN ANY HAZARDOUS APPLICATIONS.

3.4 Limitation of Liability.

- (a) **TOTAL LIABILITY.** NOTWITHSTANDING ANYTHING ELSE HEREIN, ALL LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMER FOR THE RELEVANT SOFTWARE, OR PORTION THEREOF, THAT GAVE RISE TO SUCH LIABILITY OR ONE HUNDRED UNITED STATES DOLLARS (US\$100), WHICHEVER IS GREATER. THE LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS SECTION SHALL BE CUMULATIVE AND NOT PER INCIDENT.
- (b) **DAMAGES.** IN NO EVENT SHALL LICENSOR, ITS SUPPLIERS OR THEIR RELEVANT SUBCONTRACTORS BE LIABLE FOR (A) ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR LOST OR DAMAGED DATA, OR ANY INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE OR (B) ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES IN EACH CASE, EVEN IF LICENSOR OR ITS SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 **Exclusions.** SOME JURISDICTIONS DO NOT PERMIT THE LIMITATIONS OF LIABILITY AND LIMITED WARRANTIES SET FORTH UNDER THIS AGREEMENT. IN THE EVENT YOU ARE LOCATED IN ANY SUCH JURISDICTION, THE FOREGOING LIMITATIONS SHALL APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED IN SUCH JURISDICTIONS. IN NO EVENT SHALL THE FOREGOING EXCLUSIONS AND LIMITATIONS ON DAMAGES BE DEEMED TO APPLY TO ANY LIABILITY BASED ON FRAUD, WILLFUL MISCONDUCT, GROSS NEGLIGENCE OR PERSONAL INJURY OR DEATH.

4. Confidential Information

- 4.1 **Generally.** The Software (and its accompanying Documentation) constitutes Licensor's and its suppliers' proprietary and confidential information and contains valuable trade secrets of Licensor and its suppliers ("Confidential Information"). Customer shall protect the secrecy of the Confidential Information to the same extent it protects its other valuable, proprietary and confidential information of a similar nature but in no event shall Customer use less than reasonable care to maintain the secrecy of the Confidential Information. Customer shall not use the Confidential Information except to exercise its rights or perform its obligations as set forth under this Agreement. Customer shall not disclose such Confidential Information to any third party other than subject to non-use and non-disclosure obligations at least as protective of a party's right in such Confidential Information as those set forth herein.
- 4.2 **Return of Materials.** Customer agrees to (i) destroy all Confidential Information (including deleting any and all copies contained on any of Customer's Designated Hardware or the Product) within fifteen (15) days of the date of termination of this Agreement or (ii) if requested by Licensor, return, any Confidential Information to Licensor within thirty (30) days of Licensor's written request.

5. Term and Termination

- 5.1 **Term.** Subject to Section 5.2 below, this Agreement will take effect on the Effective Date and will remain in force until terminated in accordance with this Agreement.
- 5.2 **Termination Events.** This Agreement may be terminated immediately upon written notice by either party under any of the following conditions:
- (a) If the other party has failed to cure a breach of any material term or condition under the Agreement within thirty (30) days after receipt of notice from the other party; or
 - (b) Either party ceases to carry on business as a going concern, either party becomes the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation, which proceeding is not dismissed within ninety (90) days, or a receiver is appointed with respect to a substantial part of its assets.

5.3 Effect of Termination.

- (a) Upon termination of this Agreement, in whole or in part, Customer shall pay Licensor for all amounts owed up to the effective date of termination. Termination of this Agreement shall not constitute a waiver for any amounts due.
- (b) The following Sections shall survive the termination of this Agreement for any reason: Sections 1, 2.2, 2.4, 3, 4, 5.3, and 6.
- (c) No later than thirty (30) days after the date of termination of this Agreement by Licensor, Customer shall upon Licensor's instructions either return the Software and all copies thereof; all Documentation relating thereto in its possession that is in tangible form or destroy the same (including any copies thereof contained on Customer's Designated Hardware). Customer shall furnish Licensor with a certificate signed by an executive officer of Customer verifying that the same has been done.

6. Miscellaneous

If Customer is a corporation, partnership or similar entity, then the license to the Software and Documentation that is granted under this Agreement is expressly conditioned upon and Customer represents and warrants to Licensor that the person accepting the terms of this Agreement is authorized to bind such entity to the terms and conditions herein. If any provision of this Agreement is held to be invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect. During the course of use of the Software, Licensor may collect information on your use thereof; you hereby authorize Licensor to use such information to improve its products and services, and to disclose the same to third parties provided it does not contain any personally identifiable information. The express waiver by either party of any provision, condition or requirement of this Agreement does not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Customer and Licensor are independent parties. Customer may not export or re-export the Software or Documentation (or other materials) without appropriate United States, European Union and foreign government licenses or in violation of the United State's Export Administration Act or foreign equivalents and Customer shall comply with all national and international laws governing the Software. This Agreement will be governed by and construed under the laws of the State of California and the United States as applied to agreements entered into and to be performed entirely within California, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer

Information Transactions Act (as promulgated by any State) to this Agreement. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of, the state and federal courts located in Ventura County, California. Customer may not assign this Agreement by operation of law or otherwise, without the prior written consent of Licensor and any attempted assignment in violation of the foregoing shall be null and void. This Agreement cancels and supersedes all prior agreements between the parties. This Agreement may not be varied except through a document agreed to and signed by both parties. Any printed terms and conditions contained in any Customer purchase order or in any Licensor acknowledgment, invoice or other documentation relating to the Software shall be deemed deleted and of no force or effect and any additional typed and/or written terms and conditions contained shall be for administrative purposes only, i.e. to identify the types and quantities of Software to be supplied, line item prices and total price, delivery schedule, and other similar ordering data, all in accordance with the provisions of this Agreement.

Hardware Warranty Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT

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

LIMITED WARRANTY. Xirrus warrants that for a period of one year from the date of purchase by the original purchaser ("Customer"): (i) the Xirrus Equipment ("Equipment") will be free of defects in materials and workmanship under normal use; and (ii) the Equipment substantially conforms to its published specifications. Except for the foregoing, the Equipment is provided AS IS. This limited warranty extends only to Customer as the original purchaser. Customer's exclusive remedy and the entire liability of Xirrus and its suppliers under this limited warranty will be, at Xirrus' option, repair, replacement, or refund of the Equipment if reported (or, upon request, returned) to the party supplying the Equipment to Customer. In no event does Xirrus warrant that the Equipment is error free or that Customer will be able to operate the Equipment without problems or interruptions.

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

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

IN NO EVENT WILL XIRRUS OR ITS SUPPLIERS BE LIABLE FOR ANY LOST REVENUE, PROFIT, OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE THE EQUIPMENT EVEN IF XIRRUS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall Xirrus' or its suppliers' liability to Customer,

whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer.

The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. SOME STATES DO NOT ALLOW LIMITATION OR EXCLUSION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES.

The above warranty DOES NOT apply to any evaluation Equipment made available for testing or demonstration purposes. All such Equipment is provided AS IS without any warranty whatsoever.

Customer agrees the Equipment and related documentation shall not be used in life support systems, human implantation, nuclear facilities or systems or any other application where failure could lead to a loss of life or catastrophic property damage, or cause or permit any third party to do any of the foregoing.

All information or feedback provided by Customer to Xirrus with respect to the Product shall be Xirrus' property and deemed confidential information of Xirrus.

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

This Agreement shall be governed by and construed in accordance with the laws of the State of California, United States of America, as if performed wholly within the state and without giving effect to the principles of conflict of law. If any portion hereof is found to be void or unenforceable, the remaining provisions of this Warranty shall remain in full force and effect. This Warranty constitutes the entire agreement between the parties with respect to the use of the Equipment.

Manufacturer is Xirrus, Inc. 2101 Corporate Center Drive Thousand Oaks, CA 91320

Glossary of Terms

802.11a

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 5 GHz and data rates of up to 54 Mbps.

802.11b

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 11 Mbps.

802.11d

A supplement to the Media Access Control (MAC) layer in 802.11 to promote worldwide use of 802.11 WLANs. It allows Access Points to communicate information on the permissible radio channels with acceptable power levels for user devices. Because the 802.11 standards cannot legally operate in some countries, 802.11d adds features and restrictions to allow WLANs to operate within the rules of these countries.

802.11g

A supplement to the IEEE 802.11 WLAN specification that describes radio transmissions at a frequency of 2.4 GHz and data rates of up to 54 Mbps.

802.11n

A supplement to the IEEE 802.11 WLAN specification that describes enhancements to 802.11a/b/g to greatly enhance reach, speed, and capacity.

802.1Q

An IEEE standard for MAC layer **frame** tagging (also known as encapsulation). Frame tagging uniquely assigns a user-defined ID to each frame. It also enables a switch to communicate **VLAN** membership information across multiple (and multi-vendor) devices by frame tagging.

AES

(Advanced Encryption Standard) A data encryption scheme that uses three different key sizes (128-bit, 192-bit, and 256-bit). AES was adopted by the U.S. government in 2002 as the encryption standard for protecting sensitive but unclassified electronic data.

authentication

The process that a station, device, or user employs to announce its identify to the network which validates it. IEEE 802.11 specifies two forms of authentication, open system and shared key.

bandwidth

Specifies the amount of the frequency spectrum that is usable for data transfer. In other words, it identifies the maximum data rate a signal can attain on the medium without encountering significant attenuation (loss of power).

beacon interval

When a device in a wireless network sends a beacon, it includes with it a beacon interval, which specifies the period of time before it will send the beacon again. The interval tells receiving devices on the network how long they can wait in low power mode before waking up to handle the beacon. Network administrators can adjust the beacon interval—usually measured in milliseconds (ms) or its equivalent, kilo-microseconds (Kmsec).

bit rate

The transmission rate of binary symbols ('0' and '1'), equal to the total number of bits transmitted in one second.

BSS

(Basic Service Set) When a WLAN is operating in infrastructure mode, each access point and its connected devices are called the Basic Service Set.

BSSID

The unique identifier for an access point in a **BSS** network. See also, **SSID**.

CDP

(Cisco Discovery Protocol) CDP is a layer 2 network protocol which runs on most Cisco equipment and some other network equipment. It is used to share information with other directly connected network devices. Information such as the model, network capabilities, and IP address is shared. Wi-Fi Arrays can both advertise their presence by sending CDP announcements, and gather and display information sent by neighbors.

cell

The basic geographical unit of a cellular communications system. Service coverage of a given area is based on an interlocking network of cells, each with a radio base station (transmitter/receiver) at its center. The size of each cell is determined by the terrain and forecasted number of users.

channel

A specific portion of the radio spectrum—the channels allotted to one of the wireless networking protocols. For example, 802.11b and 802.11g use 14 channels in the 2.4 GHz band, only 3 of which don't overlap (1, 6, and 11). In the 5 GHz band, 802.11a uses 8 channels for indoor use and 4 for outdoor use, none of which overlap. In the U.S., additional channels are available, to bring the total to 24 channels.

CoS

(Class of Service) A category based on the type of user, type of application, or some other criteria that QoS systems can use to provide differentiated classes of service.

default gateway

The gateway in a network that a computer will use to access another network if a gateway is not specified for use. In a network using subnets, a default gateway is the router that forwards traffic to a destination outside of the subnet of the transmitting device.

DHCP

(Dynamic Host Configuration Protocol) A method for dynamically assigning IP addresses to devices on a network. DHCP issues IP addresses automatically within a specified range to client devices when they are first powered up.

DHCP lease

The DHCP lease is the amount of time that the DHCP server grants to the DHCP client for permission to use a particular IP address. A typical DHCP server allows its administrator to set the lease time.

DNS

(Domain Name System) A system that maps meaningful domain names with complex numeric IP addresses. DNS is actually a separate network—if one DNS server cannot translate a domain name, it will ask a second or third until a server is found with the correct IP address.

domain

The main name/Internet address of a user's Internet site as registered with the InterNIC organization, which handles domain registration on the Internet. For example, the “domain” address for Xirrus is: <http://www.xirrus.com>, broken down as follows:

- **http://** represents the Hyper Text Teleprocessing Protocol used by all Web pages.
- **www** is a reference to the World Wide Web.
- **xirrus** refers to the company.
- **com** specifies that the domain belongs to a commercial enterprise.

DTIM

(Delivery Traffic Indication Message) A DTIM is a signal sent as part of a beacon by an access point to a client device in sleep mode, alerting the device to a packet awaiting delivery.

EAP

(Extensible Authentication Protocol) When you log on to the Internet, you're most likely establishing a PPP connection via a remote access server. The password, key, or other device you use to prove that you are authorized to do so is controlled via PPP's Link Control Protocol (LCP). However, LCP is somewhat inflexible because it has to specify an authentication device early in the process. EAP allows the system to gather more information from the user before deciding which authenticator to use. It is called extensible because it allows more authenticator types than LCP (for example, passwords and public keys).

EDCF

(Enhanced Distributed Coordinator Function) A QoS extension which uses the same contention-based access mechanism as current devices but adds “offset contention windows” that separate high priority packets from low priority packets (by assigning a larger random backoff window to lower priorities than to higher priorities). The result is “statistical priority,” where high-priority packets usually are transmitted before low-priority packets.

encapsulation

A way of wrapping protocols such as TCP/IP, AppleTalk, and NetBEUI in Ethernet frames so they can traverse an Ethernet network and be unwrapped when they reach the destination computer.

encryption

Any procedure used in cryptography to translate data into a form that can be decrypted and read only by its intended receiver.

Fast Ethernet

A version of standard Ethernet that runs at 100 Mbps rather than 10 Mbps.

FCC

(Federal Communications Commission) US wireless regulatory authority. The FCC was established by the Communications Act of 1934 and is charged with regulating Interstate and International communications by radio, television, wire, satellite and cable.

FIPS

The [Federal Information Processing Standard \(FIPS\) Publication 140-2](#) establishes a computer security standard used to accredit cryptographic modules. The standard is a joint effort by the U.S. and Canadian governments.

frame

A packet encapsulated to travel on a physical medium, like Ethernet or Wi-Fi. If a packet is like a shipping container, a frame is the boat on which the shipping container is loaded.

Gigabit 1

The primary Gigabit Ethernet interface. See also, [Gigabit Ethernet](#).

Gigabit 2

The secondary Gigabit Ethernet interface. See also, [Gigabit Ethernet](#).

Gigabit Ethernet

The newest version of Ethernet, with data transfer rates of 1 Gigabit (1,000 Mbps).

Group

A user group, created to define a set of attributes (such as VLAN, traffic limits, and Web Page Redirect) and privileges (such as fast roaming) that apply to all users that are members of the group. This allows a uniform configuration to be easily applied to multiple user accounts. The attributes that can be configured for user groups are almost identical to those that can be configured for SSIDs.

host name

The unique name that identifies a computer on a network. On the Internet, the host name is in the form **comp.xyz.net**. If there is only one Internet site the host name is the same as the [domain](#) name. One computer can have more than one host name if it hosts more than one Internet site (for example, **home.xyz.net** and **comp.xyz.net**). In this case, **comp** and **home** are the host names and **xyz.net** is the domain name.

IPsec

A Layer 3 authentication and encryption protocol. Used to secure VPNs.

MAC address

(Media Access Control Address) A 6-byte hexadecimal address assigned by a manufacturer to a device.

Mbps

(Megabits per second) A standard measure for data transmission speeds (for example, the rate at which information travels over the Internet). 1 Mbps denotes one million bits per second.

MTU

(Maximum Transmission Unit) The largest physical packet size—measured in bytes—that a network can transmit. Any messages larger than the MTU are divided into smaller [packets](#) before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

NTP

(Network Time Protocol) An Internet standard protocol (built on top of TCP/IP) that ensures the accurate synchronization (to the millisecond) of computer clock times in a network of computers. Running as a continuous background client program on a computer, NTP sends periodic time requests to servers, obtaining server time stamps and using them to adjust the client's clock.

packet

Data sent over a network is broken down into many small pieces—packets—by the Transmission Control Protocol layer of TCP/IP. Each packet contains the address of its destination as well the data. Packets may be sent on any number of routes to their destination, where they are reassembled into the original data. This system is optimal for connectionless networks, such as the Internet, where there are no fixed connections between two locations.

PLCP

(Physical Layer Convergence Protocol) Defined by IEEE 802.6, a protocol specified within the Transmission Convergence layer that defines exactly how cells are formatted within a data stream for a particular type of transmission facility.

PoGE

This refers to the optional Xirrus XP1 Power over Gigabit Ethernet modules that provide DC power to Arrays. Power is supplied over the same Cat 5e or Cat 6 cable that supplies the data connection to your gigabit Ethernet switch, thus eliminating the need to run a power cable. See [“Power over Gigabit Ethernet Compatibility Matrix”](#) on page 414 for a list of Xirrus PoGE modules and the modules that are compatible with each Array.

preamble

Preamble (sometimes called a header) is a section of data at the head of a **packet** that contains information that the access point and client devices need when sending and receiving packets. **PLCP** has two structures, a long and a short preamble. All compliant 802.11b systems have to support the long preamble. The short preamble option is provided in the standard to improve the efficiency of a network's throughput when transmitting special data, such as voice, VoIP (Voice-over IP) and streaming video.

private key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The private key is provided only to the requestor and never shared. The requestor uses the private key to decrypt text that has been encrypted with the public key by someone else.

PSK

(Pre-Shared Key) A TKIP passphrase used to protect your network traffic in WPA.

public key

In cryptography, one of a pair of keys (one public and one private) that are created with the same algorithm for encrypting and decrypting messages and digital signatures. The public key is made publicly available for encryption and decryption.

QoS

(Quality of Service) QoS can be used to describe any number of ways in which a network provider prioritizes or guarantees a service's performance.

RADIUS

(Remote Authentication Dial-In User Service) A client-server security protocol, developed to authenticate, authorize, and account for dial-up users. The RADIUS server stores user profiles, which include passwords and authorization attributes.

RSSI

(Received Signal Strength Indicator) A measure of the energy observed by an antenna when receiving a signal.

SDMA

(Spatial Division Multiple Access) A wireless communications mode that optimizes the use of the radio spectrum and minimizes cost by taking advantage of the directional properties of antennas. The antennas are highly directional, allowing duplicate frequencies to be used for multiple zones.

SNMP

(Simple Network Management Protocol) A standard protocol that regulates network management over the Internet.

SNTP

(Simple Network Time Protocol) A simplified version of NTP. SNTP can be used when the ultimate performance of the full NTP implementation described in RFC 1305 is not needed or justified.

SSH

(Secure SHell) Developed by SSH Communications Security, Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. The Array only allows SSH-2 connections. SSH-2 provides strong authentication and secure communications over insecure channels. SSH-2 protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot “play back” the traffic or hijack the connection when encryption is enabled. When using SSH-2's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords. Be aware that your SSH utility must be set up to use SSH-2.

SSID

(Service Set IDentifier) Every wireless network or network subset (such as a BSS) has a unique identifier called an SSID. Every device connected to that part of the network uses the same SSID to identify itself as part of the family—when it wants to gain access to the network or verify the origin of a data packet it is sending over the network. In short, it is the unique name shared among all devices in a WLAN.

subnet mask

A mask used to determine what subnet an IP address belongs to. An IP address has two components: (1) the network address and (2) the host address. For example, consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

TKIP

(Temporal Key Integrity Protocol) Provides improved data encryption by scrambling the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the encryption keys haven't been tampered with.

transmit power

The amount of power used by a radio transceiver to send the signal out. Transmit power is generally measured in milliwatts, which you can convert to dBm.

User group

See [Group](#).

VLAN

(Virtual LAN) A group of devices that communicate as a single network, even though they are physically located on different LAN segments. Because VLANs are based on logical rather than physical connections, they are extremely flexible. A device that is moved to another location can remain on the same VLAN without any hardware reconfiguration.

VLAN tagging

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the [802.11n](#) standard, traffic can be confined to VLANs that exist on

multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

1. That the packet has a tag.
2. Whether the packet should have priority over other packets.
3. Which VLAN it belongs to, so that the switch can forward or filter it correctly.

WDS (Wireless Distribution System)

WDS creates wireless backhubs between arrays. These links between arrays may be used rather than having to install data cabling to each array.

WEP

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

Wi-Fi Alliance

A nonprofit international association formed in 1999 to certify interoperability of wireless Local Area Network products based on IEEE 802.11 specification. The goal of the Wi-Fi Alliance's members is to enhance the user experience through product interoperability.

Wi-Fi Array

A high capacity Wi-Fi networking device consisting of multiple radios arranged in a circular array.

WPA

(Wi-Fi Protected Access) A Wi-Fi Alliance standard that contains a subset of the IEEE 802.11i standard, using TKIP as an encryption method and 802.1x for authentication.

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.

Xirrus Management System (XMS)

A Xirrus product used for managing large Wi-Fi Array deployments from a centralized Web-based interface.

XP-3100

The Xirrus XP Power System (XP-3100) is a discontinued Xirrus product that provides distributed DC power to multiple XS-3900 units.

XP1 and XP8—Power over Gigabit Ethernet modules

See PoGE.

XPS—Xirrus Power System

A family of optional Xirrus products that provides power over Gigabit Ethernet. See PoGE.

Index

Numerics

11n
 see IEEE 802.11n 59
 4.9 GHz Public Safety Band 282
 802.11a 7, 9, 255, 267
 802.11a/b/g 48
 802.11a/b/g/n 17
 802.11a/n 17, 107, 240
 802.11b 7, 9, 269
 802.11b/g 255, 269
 802.11b/g/n 17, 107, 240
 802.11e 19
 802.11g 7, 9, 269
 802.11i 9, 112, 176
 802.11n
 see IEEE 802.11n 59
 WMI page 273
 802.11p 19
 802.11q 19
 802.1x 9, 70, 79, 112, 176, 400

A

abg(n)
 nomenclature 4
 abg(n)2
 intrusion detection 277
 self-monitoring
 radio assurance (loopback mode) 278
 AC power 69, 81, 83, 373, 376
 Access Control List 209
 Access Control Lists 400
 access control lists (ACLs) 223
 Access Panel 373, 376, 385
 access panel
 reinstalling 376

 removing 373
 ACLs 70, 209, 400
 Address Resolution Protocol
 window 138
 Address Resolution Protocol (ARP)
 264
 Admin 400
 Admin ID 215
 admin ID
 authentication via RADIUS 216
 Admin Management 215
 admin RADIUS account
 if using Console port 216
 admin RADIUS authentication 216
 administration 112, 176, 209
 Administrator Account 394
 Advanced Encryption Standard 70,
 400
 advanced intrusion detection 277
 AES 9, 18, 70, 79, 112, 176, 392, 400
 allow traffic
 see filters 289
 approved
 setting rogues 148
 APs 79, 148, 233, 400
 rogues, blocking 276
 APs, rogue
 see rogue APs 275
 ARP filtering 264
 ARP table window 138
 Array 50, 86, 94, 95, 107, 120, 176, 183
 connecting 86
 dismounting 95
 management 295
 mounting 86
 powering up 107
 securing 94
 Web Management Interface 120
 ArrayOS
 upgrade 297

- associated users 50
- assurance (radio loopback testing) 275
- authentication 18
 - of admin via RADIUS 216
- authority
 - certificate 213, 221
- auto negotiate 183
- auto-blocking
 - rogue APs 276
- auto-configuration 112, 260, 267, 269
 - channel and cell size 275

B

- backhaul
 - see WDS 76
- backup unit
 - see standby mode 275
- band association 240
- beacon interval 260
- Beacon World Mode 260
- beam distribution 17
- benefits 16
- blocking
 - rogue APs 276
- blocking rogue APs 275
- boot 297
- broadcast 265
 - fast roaming 265
- browser
 - certificate error 213, 221
- BSS 398
- BSSID 148, 398
- buttons 124

C

- capacity
 - of 802.11n 66
- cascading style sheet
 - sample for web page redirect 301
- cdp 322

- CDP (Cisco Discovery Protocol)
 - settings 191
- cdp CLI command 322
- cell
 - sharp cell 275
- cell size 50, 255, 389
 - auto-configuration 275
- cell size configuration 275
- certificate
 - about 213, 221
 - authority 213, 221
 - error 213, 221
 - install Xirrus authority 221
 - X.509 213, 221
- channel
 - auto-configuration 275
 - configuration 275
 - list selection 275
 - public safety 275
- channels 50, 148, 255, 260, 267, 269, 389
 - factory default 280
 - factory presets 281
 - non-overlapping 18
- Chassis Cover 382
- chassis cover 382
- Cisco Discovery Protocol
 - see cdp 322
- Cisco Discovery Protocol (CDP) 191
- CLI 9, 79, 83, 110, 307
 - executing from WMI 303
 - using to upgrade software image 409
- CLI commands
 - see commands 322
- client
 - web page redirect 300
- Command Line Interface 9, 75, 83, 107, 110, 307, 400
 - configuration commands 320

- getting help 309
 - getting started 309
 - inputting commands 309
 - sample configuration tasks 355
 - SSH 308
 - top level commands 311
 - command, utilities
 - ping, traceroute, RADIUS ping 301
 - commands
 - acl 320
 - admin 321
 - cdp 322
 - clear 323
 - configure 312
 - contact-info 324
 - date-time 325
 - dhcp-server 326
 - dns 327
 - file 328
 - filter 331
 - fips 333
 - group 334
 - hostname 334
 - https 335
 - interface 336
 - license 337
 - load 337
 - location 338
 - management 338
 - more 338
 - netflow 339
 - no 340
 - pci-audit 342
 - quit 343
 - radius-server 343
 - reboot 344, 353
 - reset 344
 - run-tests 345
 - security 347
 - show 315
 - snmp 348
 - ssh 348
 - ssid 350
 - standby 350
 - statistics 318
 - syslog 351
 - telnet 353
 - vlan 354
 - Community String 390
 - configuration 175, 400
 - express setup 176
 - reset to factory defaults 298
 - configuration changes
 - applying 126
 - configuration files
 - download 298
 - update from local file 298
 - update from remote file 298
 - connection
 - tracking window 140
 - Console port
 - login via 216
 - Contact Information 417
 - contact information 417
 - coverage 50, 83
 - extended 17
 - coverage patterns 9
 - critical messages 123
 - CTS/RTS 267, 269
- D**
- data rate 267, 269
 - data rates
 - increased by 802.11n 65
 - DC power 69, 83
 - default
 - preset channels 281
 - default gateway 112, 183
 - default settings 387
 - Default Value 391, 392

- DHCP 391
- defaults
 - reset configuration to factory defaults 298
- Delivery Traffic Indication Message 260
- deny traffic
 - see filters 289
- deployment 48, 57, 75, 79, 83, 400
 - ease of 19
 - examples 57
 - scenarios 57
- DHCP 50, 110, 112, 176, 183, 390
 - default settings 391
 - leases window 139
- DHCP Server 193
- diagnostics
 - log, create file 299
- DIMM 380
- DIMM Memory Module 380
- DIMM module
 - replacing 380
- DNS 112, 176, 190
- DNS domain 190
- DNS server 190
- Domain Name System 190
- DTIM 260
- DTIM period 260
- duplex 183
- dynamic VLAN
 - overridden by group 250

E

- EAP 392, 400
- EAP-MDS 18
- EAP-PEAP 400
- EAP-TLS 18, 70, 400
- EAP-TTLS 18, 70, 400
- EDCF 260
- Encryption 392, 400

- encryption 18
- encryption method
 - recommended (WPA2 with AES) 211
 - setting 211
 - support of multiple methods 211
- encryption method (encryption mode) Open, WEP, WPA, WPA2, WPA-Both 210
- encryption standard
 - AES, TKIP, both 211
 - setting 211
- End User License Agreement 81
- Enterprise 2, 7, 400
 - WLAN 7
- Enterprise Class Management 9
- Enterprise Class Security 9
- ESS 398
- ESSID 398
- Ethernet 83, 86, 94, 107, 110, 112, 176
- EULA 81
- event log
 - see system log 173
- event messages 123
- Express Setup 94, 112, 176
- express setup 112, 176
- Extended Service Set 398
- Extensible Authentication Protocol 400
- external RADIUS server 802.1x 47

F

- factory default settings 387
- factory defaults 389, 390, 391, 392, 394
 - DHCP 391
 - reset configuration to 298
- factory preset
 - channels 281
- factory.conf 298
- fail-over
 - standby mode 275

- failover 67, 79
 - Fan 373, 376
 - FAQs 398
 - Fast Ethernet 83, 110, 176, 183, 387
 - fast roaming 19, 135, 265
 - about 254
 - features 16, 75, 183, 196, 197, 260, 400
 - and license key 297
 - Federal Information Processing Standard (FIPS)
 - see FIPS 425
 - feedback 124
 - filter list 290
 - filter name 291
 - filters 289, 290, 291
 - statistics 171
 - FIPS
 - CLI command 333
 - FIPS 140-2 Security 425
 - firewall 289
 - and port usage 72
 - FLASH 378
 - FLASH memory
 - replacing 378
 - FLASH Memory Module 378
 - fragmentation threshold 267, 269
 - frequently asked questions 398
 - FTP 400
 - FTP server 47
- G**
- General Hints 397
 - getting started
 - express setup 176
 - Gigabit 83, 110, 112, 176, 183, 387
 - global settings 260, 267, 269
 - glossary of terms 455
 - Group
 - management 249
 - group 247
- CLI command 334
 - VLAN overrides dynamic VLAN 250
- Group Rekey 392
 - guard interval
 - short, for IEEE 802.11n 64
- H**
- Help button 120
 - help button 124
 - host name 112, 120, 176, 190
 - hs.css 301
 - HTTPS
 - certificate, see certificate 221
 - HyperTerminal 46, 83
- I**
- IAP 50, 107, 112, 176, 255, 267, 269, 283, 389
 - fast roaming 254
 - naming 4
 - settings 255
 - IAP LED 107, 283
 - IAP LED settings 283
 - IAPs
 - default channels 280
 - IEEE 7, 112, 176
 - IEEE 802.11n
 - capacity, increased 66
 - deployment considerations 59
 - guard interval, short 64
 - improved MAC throughput 64
 - increased data rates 65
 - MIMO 60
 - multiple data streams 62
 - spatial multiplexing 62
 - WMI page 273
 - IEEE 802.1Q 403
 - image
 - upgrade software image 297

- implementing Voice over Wi-Fi 48, 205, 237
 - installation 45, 80, 86, 369
 - installing the MCAP-3616 83
 - mounting the unit 86
 - requirements 45
 - unpacking the unit 81
 - workflow 80
 - installation workflow 80
 - Integrated Access Point Module 382
 - integrated radio module
 - replacing 382
 - interfaces 176
 - Web 119
 - Internet Explorer 46
 - intrusion detection 148, 277
 - configuration 275
 - setting as approved or known 148
 - IP Address 50, 112, 120, 126, 148, 176, 183, 190, 197, 200, 295, 390
 - IP Subnet Mask 112
- K**
- key
 - license, setting 337
 - upgrade 297
 - key features 16
 - Keyboard Shortcuts 394
 - keyboard shortcuts 394
 - known
 - setting rogues 148
- L**
- lastboot.conf 298
 - Layer 3
 - fast roaming 254
 - lease 390
 - Lease Time 390
 - leases, DHCP
 - viewing 139
 - LEDs 107
 - sequence 107
 - settings 283
 - license Key
 - upgrading 297
 - license key
 - setting 337
 - list, access control
 - see access control list 223
 - list, MAC access
 - see access control list 223
 - location information 112, 120, 176
 - log
 - diagnostics, create file 299
 - log messages
 - counters 124
 - log, system (event)
 - viewing window 173
 - logging in 110, 126
 - Login 126
 - login
 - via Console port 216
 - login page
 - web page redirect 300
 - logout 305
 - long retry limit 260
 - loopback
 - see radio assurance 367
 - loopback testing
 - radio assurance mode 275
- M**
- MAC 70, 110, 398, 400
 - MAC Access Control Lists 70
 - MAC Access List 223
 - MAC address 223, 398, 400
 - MAC throughput
 - improved by IEEE 802.11n 64
 - Main System Memory 380
 - Management 394, 400

management
of Arrays 295
Web Management Interface (WMI)
119

maximum lease 390

Maximum Lease Time 390

Megabit 112

Message Integrity Check 400

messages

syslog counters 124

MIC 18, 400

MIMO (Multiple-In Multiple-Out) 60

monitoring

intrusion detection 148

see intrusion detection 277

mounting 86

mounting plate 86, 94, 95

mounting the unit 86

MTU 183

size 183

multiple data streams 62

N

NAT

table - see connection tracking 140

Netflow 196

netflow

CLI command 339

Netscape Navigator 45, 46

network

interfaces 182

settings 183

network connections 83, 126, 400

network installation 45, 369

network interface ports 110

network interfaces 183, 387

network status

ARP table window 138

connection

tracking window 140

routing table window 138

viewing leases 139

Network Time Protocol 112, 176, 194

nomenclature 4

non-overlapping channels 18

NTP 112, 176, 194, 390

NTP Server 194

O

Open (encryption method) 210

optimization, VLAN 265

overview 9

P

passphrase 70, 112, 176

Password 394, 400

password 126

Payment Card Industry Data Security

Standard

see PCI DSS 419

PCI DSS 419

CLI command 342

pci-audit

CLI command 342

PDF 81

PEAP 18, 287

performance 16

Ping 295

ping 301

planning 67, 69, 70, 75

failover 67

network management 75

port failover 67

power 69

security 70

switch failover 67

WDS 76

PoGE 13, 45

see Power over Gigabit Ethernet 13

port failover 67

- port requirements 72
 - power cord 373
 - power distribution 13
 - power outlet 45
 - Power over Gigabit Ethernet 3, 13, 21, 27, 35, 40, 45, 69, 84
 - compatibility with Array models 414
 - Power over Gigabit Ethernet (PoGE) 13
 - power planning 69
 - Power Supply 373, 376, 385
 - power supply
 - replacing 385
 - power switch 373
 - pre-shared key 70, 79, 400
 - Print button 120
 - print button 124
 - probe
 - see Netflow 196
 - product installation 45, 369
 - product overview 9
 - product specifications 20, 27, 34, 39
 - PSK 79, 392
 - public safety band 282
 - public safety channels 275
 - PuTTY 45, 75, 112, 176, 400
 - PuTTY 46
- Q**
- QoS 19, 240, 391, 398, 462
 - conflicting values 239
 - levels defined 241, 250
 - priority 240
 - SSID 236, 241
 - about setting QoS 399
 - default QoS 391
 - user group 250
 - Quality of Service 19
 - see QoS 241, 250
 - Quick Install Guide 81
 - quick reference guide 387
 - quick start
 - express setup 176
- R**
- radio
 - assurance (self-test) 278
 - radio assurance (loopback testing) 275
 - radio assurance (loopback) mode 278
 - radio distribution 16
 - radios
 - default channels 280
 - naming 4
 - RADIUS 9, 45, 70, 79, 209, 223, 390, 400
 - admin authentication 216
 - RADIUS Ping command 301
 - RADIUS Server 390
 - RADIUS server 47
 - README file 81
 - reauthentication 260
 - reboot 297
 - redirect (WPR) 300
 - registration card 81
 - remote DC power 13
 - Reset 295, 390
 - reset configuration
 - to factory defaults 298
 - RF
 - intrusion detection 275
 - spectrum management 275
 - RF configuration 275
 - RF management
 - see channel 275
 - RF resilience 275
 - RFprotect, see XDM 277
 - roaming 19, 135, 265
 - roaming, fast 254
 - Rogue AP 9, 75, 148, 233, 400
 - rogue AP

- blocking 276
 - Rogue AP List 148
 - rogue APs
 - blocking 275
 - Rogue Control List 233
 - rogue detection 17
 - rogues
 - setting as known or approved 148
 - root command prompt 311
 - route
 - trace route utility 301
 - routing table window 138
 - RSSI 148
 - RTS 267, 269
 - RTS threshold 267, 269
- S**
- sample Perl and CSS files for 300
 - save
 - with reboot 297
 - Save button 120
 - saved.conf 298
 - scalability 7
 - schedule
 - auto channel configuration 275
 - Secondary Port 390
 - Secondary Server 390
 - secret 390
 - Secure Shell 46
 - secure Shell 45
 - Security
 - FIPS 425
 - PCI DSS 419
 - security 9, 18, 209, 398, 400
 - certificate, see certificate 221
 - see group 247
 - self-monitoring 277
 - radio assurance 367
 - radio assurance options 278
 - self-test
 - radio assurance mode 278
 - serial port 46, 110, 400
 - server, VTun
 - see VTun 208
 - Service Set Identifier 112
 - Services 193, 373, 376, 398
 - servicing 371
 - servicing the unit 369
 - settings 176
 - setup, express 176
 - sharp cell 275
 - setting in WMI 280
 - short retry limit 260
 - signal processing
 - MIMO 61
 - SNMP 9, 14, 112, 176, 183, 193, 200, 390
 - required for XMS 200, 201
 - software
 - upgrade license key 297
 - software image
 - upgrading via CLI 409
 - Software Upgrade 295
 - software upgrade 297
 - spatial multiplexing 62
 - specifications 20, 27, 34, 39
 - spectrum (RF) management 275
 - speed 7, 110, 183
 - 11 Mbps 7
 - 54 Mbps 7
 - splash page
 - web page redirect 300
 - SSH 45, 46, 75, 112, 176, 183, 210, 394, 400
 - SSH-2 210
 - SSID 9, 112, 120, 148, 176, 233, 240, 391, 398, 403
 - about usage 399
 - QoS 236, 241
 - about using 399

- QoS, about usage 399
- SSID Management 240, 391, 398
- standby mode 275
- static IP 112, 176, 183
- station timeout period 260
- Stations 398
- stations
 - rogues 148
 - statistics 171
 - statistics per station 172
- statistics 176
 - filters 171
 - netflow 196
 - per-station 172
 - stations 171
 - WDS 170
- status bar 120, 124
- submitting comments 124
- subnet 45, 67, 112, 183
- switch failover 67
- synchronize 112, 176, 194
- Syslog 112, 120, 176, 193, 197, 390
 - time-stamping 112
- syslog messages
 - counters 124
- Syslog reporting 197
- Syslog Server 197
- system commands
 - ping, trace route, RADIUS ping 301
- System Configuration Reset 295
- System Log 197
- system log
 - viewing window 173
- system memory
 - replacing 380
- System Reboot 295
- System Tools 295
- system tools 296

T

- T-bar 86
- T-bar clips 86
- TCP
 - port requirements 72
- technical support
 - contact information 417
 - frequently asked questions 398
- Telnet 210, 394, 400
- Temporal Key Integrity Protocol 400
- Time Out 390
- time zone 112, 176, 194
- timeout 260, 295
- Tips 397
- TKIP 18, 70, 79, 112, 176, 392, 400
- tool
 - ping, trace route, RADIUS ping 301
- Tools 295, 400
- tools, system 296
- trace route utility 301
- traffic
 - filtering 289
- transmit power 50, 389
- Trap Host 390
- trap port 200, 390
- tunneled
 - fast roaming 265
- tunnels
 - see VTun 205, 208

U

- UDP
 - port requirements 72
- Unit 86
 - attaching 86
 - mounting 86
- unknown
 - setting rogues 148
- unpacking the unit 81

- upgrade
 - license key 297
 - software image 297
 - upgrading software image
 - via CLI 409
 - UPS 45, 79
 - user group 247
 - QoS 250
 - user interface 119
 - utilities
 - ping, trace route, RADIUS ping 301
 - utility buttons 124
- V**
- virtual tunnels
 - see VTun 208
 - VLAN 9, 79, 240, 391, 398, 403
 - broadcast optimization 265
 - dynamic
 - overridden by group 250
 - group (vs. dynamic VLAN) 250
 - VLAN ID 240
 - voice
 - fast roaming 254
 - implementing on Array 48, 205, 237
 - Voice-over IP 269
 - VoIP 269
 - VoWLAN 19
 - VPN 112, 176, 400
 - VTS
 - Virtual Tunnel Server 205, 208
 - VTun
 - specifying tunnel server 205, 208
 - understanding 205
- W**
- wall thickness considerations 48
 - warning messages 123
 - WDS 285, 287
 - about 76
 - planning 76
 - statistics 170
 - WDS Client Links 287
 - Web interface
 - structure and navigation 123
 - web interface 119
 - Web Management Interface 75, 94, 107, 110, 126, 398
 - Web Management Interface (WMI) 119
 - web page redirect 300
 - install files for 300
 - remove files for 301
 - sample WPR files 301
 - WEP 18, 70, 112, 176, 209, 240, 392, 400
 - WEP (Wired Equivalent Privacy)
 - encryption method 211
 - Wi-Fi Protected Access 9, 70, 112, 176, 400
 - Wired Equivalent Privacy 112, 400
 - Wireless Distribution System 285
 - wireless LAN 7
 - wireless security 176
 - WLAN 176
 - WMI 9, 75, 79, 110, 119, 255
 - certificate error 213, 221
 - executing CLI commands 303
 - workflow 80
 - WPA 9, 79, 112, 176, 209, 240, 392, 400
 - WPA (Wi-Fi Protected Access) and WPA2
 - encryption method 211
 - WPA2 9
 - WPR 300
 - wpr.pl 300, 301
- X**
- X.509

- certificate 213, 221
- Xirrus
 - certificate authority 221
- Xirrus Defense Module (XDM) 277
- Xirrus Management System 9, 14, 19, 47
 - SNMP required 200, 201
- Xirrus Power over Gigabit Ethernet 45
- Xirrus Power over Gigabit Ethernet (PoGE) 13
- Xirrus Remote DC Power System 2, 45, 83
- Xirrus Roaming Protocol 19, 135, 265
- Xirrus Wireless Management System 2, 45, 75, 400
- XM-3300 2, 9, 45, 75, 79, 200, 400
- XMS 9, 14, 19, 47
 - port requirements 72
 - setting IP address of 200
 - SNMP required 200, 201
- XN Arrays
 - see also IEEE 802.11n 59
- XN16
 - management 295
- XP1, XP8
 - see Power over Gigabit Ethernet 13
- XP-3100 2, 45, 79, 83
- XPS 45
- XRP 19, 135, 265
- xs_current.conf 298
- xs_diagnostic.log 299
- XS16
 - management 127, 175, 295
- XS-3500 2, 9
- XS-3700 2, 9
- XS-3900 2, 9, 50, 70, 240, 260, 382, 398, 400, 403
 - management 127, 175, 295

User's Guide



XIRRUS[®]

Wi-Fi Arrays