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**

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 196.

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**

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]** When you enter the location, simply hit the Enter key **<cr>** to input the new location.

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**

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 802.11an IAPs (radios). FORMAT: **no dot11a**
dot11bg	Disable all 802.11bg 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)

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 the external RADIUS server. FORMAT: **radius-server external** To configure the RADIUS accounting server (primary or secondary, 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]**
rlb	Run manufacturing radio loopback test. FORMAT: **run-tests rlb {optional command line switches]**

Command	Description
self-test	Execute self-test. FORMAT: **run-tests self-test {logfile-name (optional)]**
site-survey	Enable or disable site survey mode. FORMAT: **run-tests site-survey [on | off | enable | disable]**
ssh	Execute ssh utility. FORMAT: **run-tests ssh [hostname | ip-addr] [command-line-switches (optional)]**
tcpdump	Execute tcpdump utility to dump traffic for selected interface or VLAN. FORMAT: **run-tests tcpdump**
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
community	Set the SNMP read-only or read-write community string. FORMAT: **snmp community [newcommunity]**
disable	Disable SNMP. FORMAT: **snmp disable**
enable	Enable SNMP. FORMAT: **snmp enable**
no	Disable the selected feature. FORMAT: **snmp no [feature]**
off	Disable SNMP. FORMAT: **snmp off**
on	Enable SNMP. FORMAT: **snmp on**
trap-auth	Send traps for authentication failures. FORMAT: **snmp trap-auth [trap]**
trap-host[1-4]	Set the SNMP trap IP address or host name. Up to four trap hosts may be set, one at a time. FORMAT: **snmp trap-host 1.2.3.4**

Command	Description
trap-port[1-4]	Set the SNMP trap port. FORMAT: **snmp trap-port 240**

ssh

The **ssh** command [**Xirrus_Wi-Fi_Array(config)# ssh**] is used to enable or disable the SSH feature.

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

Command	Description
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]**

Command	Description
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 292**.
- **"Configuring a Global SSID using WPA-PEAP" on page 293**.
- **"Configuring an SSID-Specific SSID using WPA-PEAP" on page 294**.
- **"Enabling Global IAPs" on page 295**.
- **"Disabling Global IAPs" on page 296**.
- **"Enabling a Specific IAP" on page 297**.
- **"Disabling a Specific IAP" on page 298**.
- **"Setting Cell Size Auto-Configuration for All IAPs" on page 299**
- **"Setting the Cell Size for All IAPs" on page 300**.
- **"Setting the Cell Size for a Specific IAP" on page 301**.
- **"Configuring VLANs on an Open SSID" on page 302**.
- **"Configuring Self-Monitoring Mode (Loopback Tests)" on page 303.**

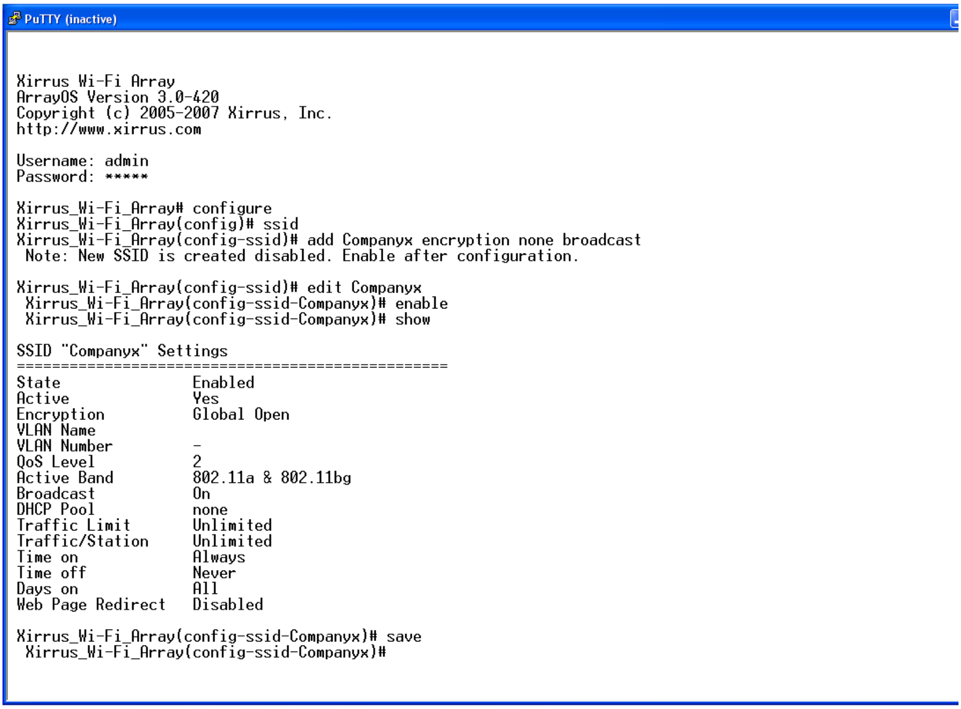
To facilitate the accurate and timely management of revisions to this section, the examples shown here are presented as screen images taken from a Secure Shell (SSH) session (in this case, PuTTY). Depending on the application you are using to access the Command Line Interface, and how your session is 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.

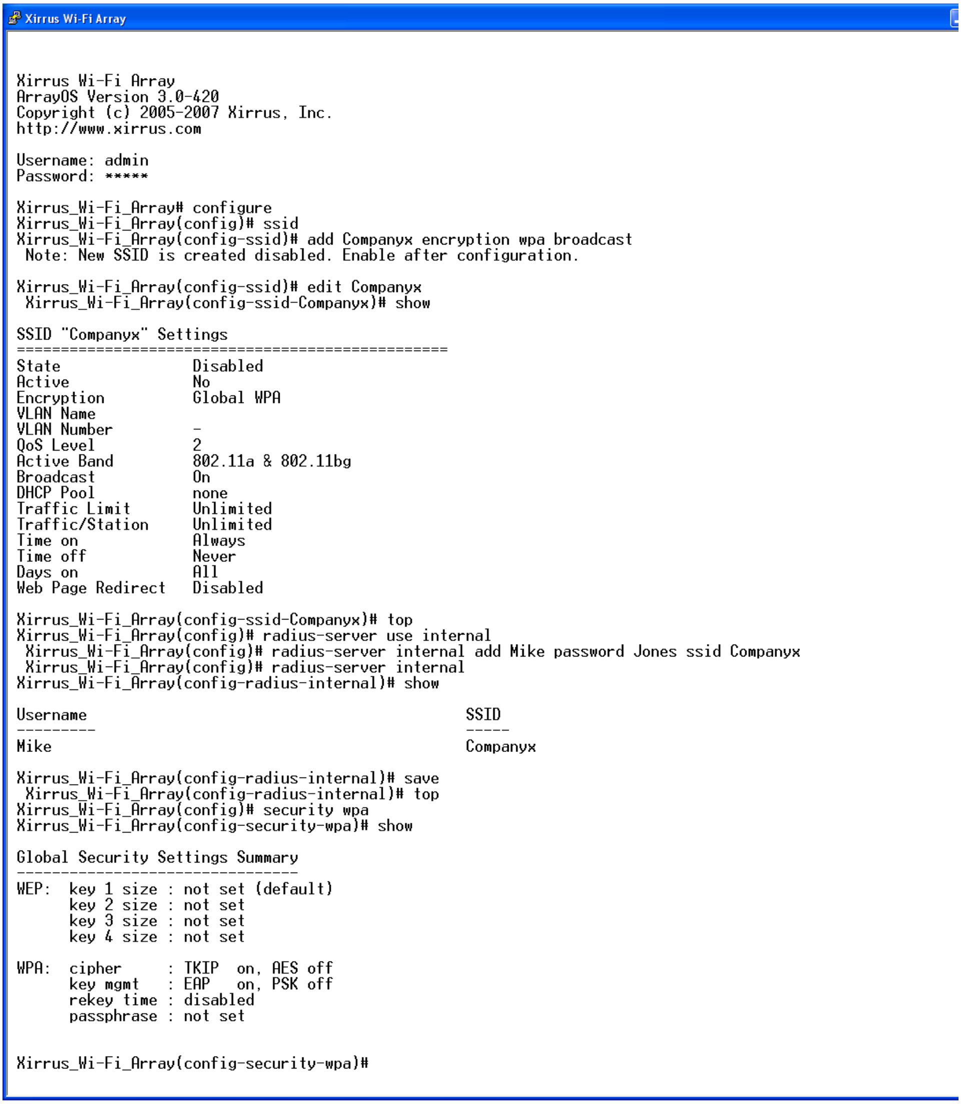


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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

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

Figure 142. 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.

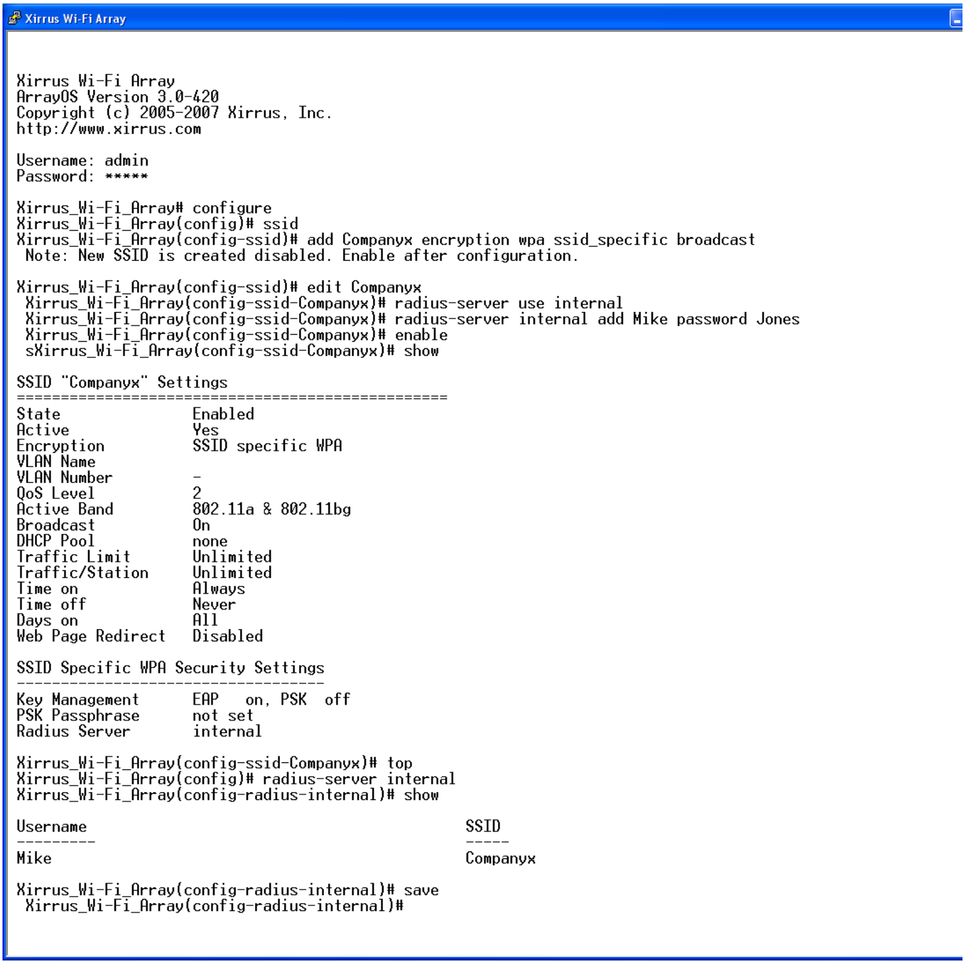


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 143. 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.

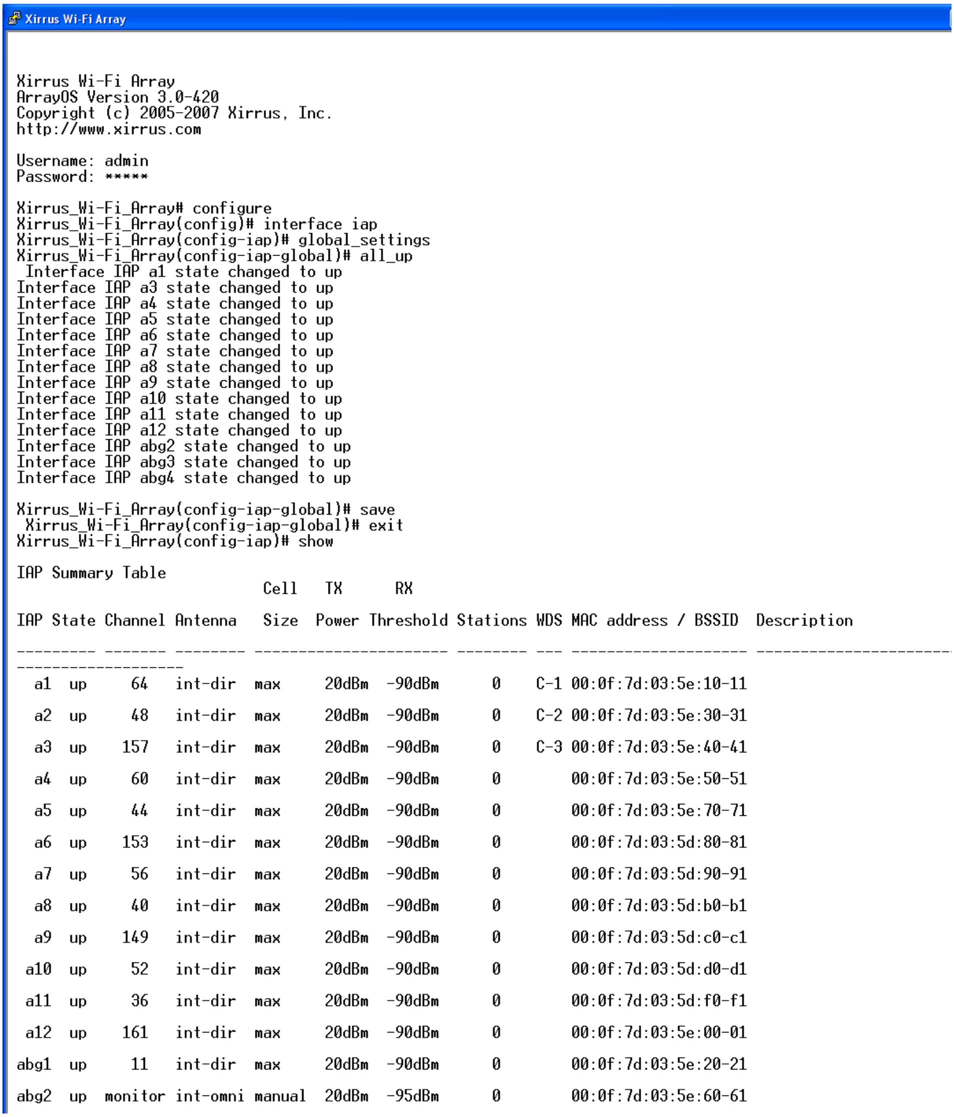


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 144. 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.

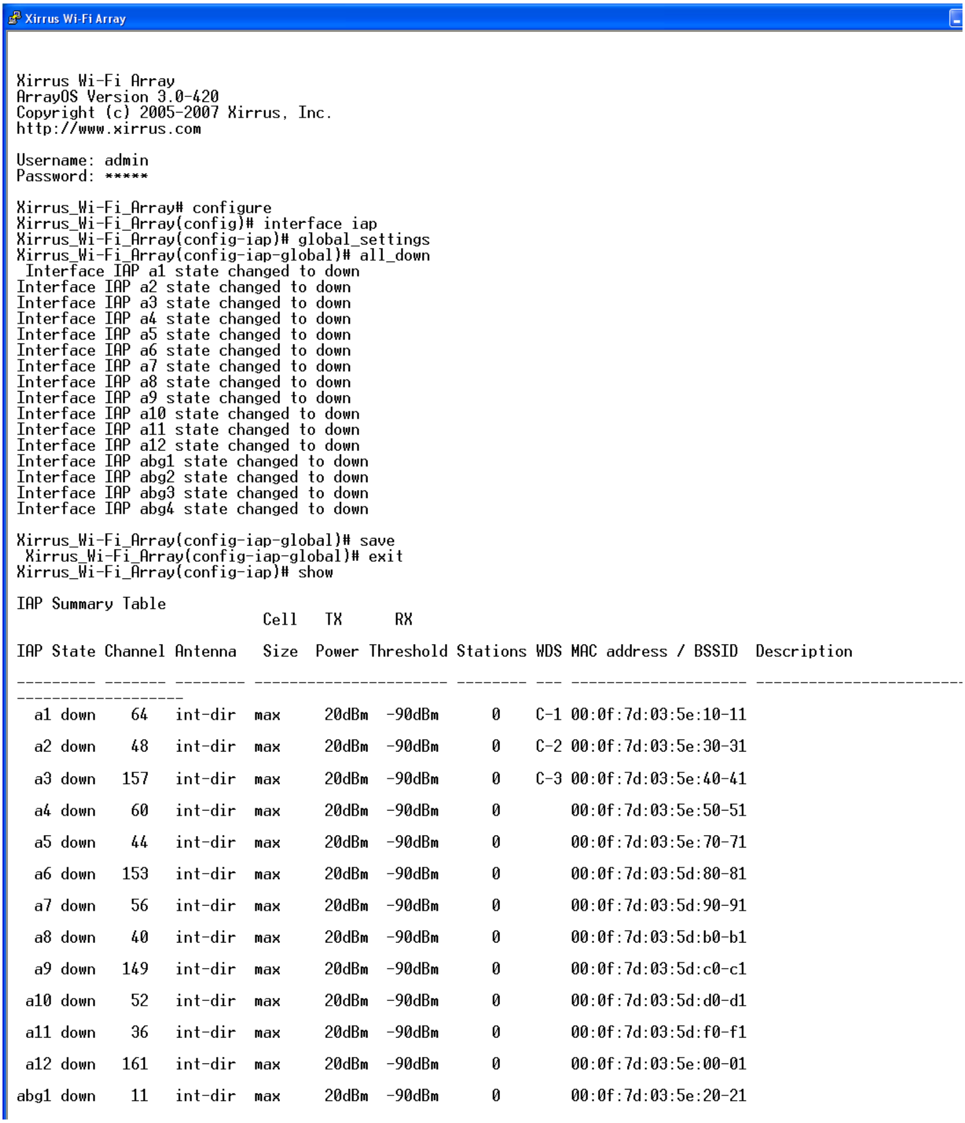


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 145. Enabling Global IAPs

Disabling Global IAPs

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

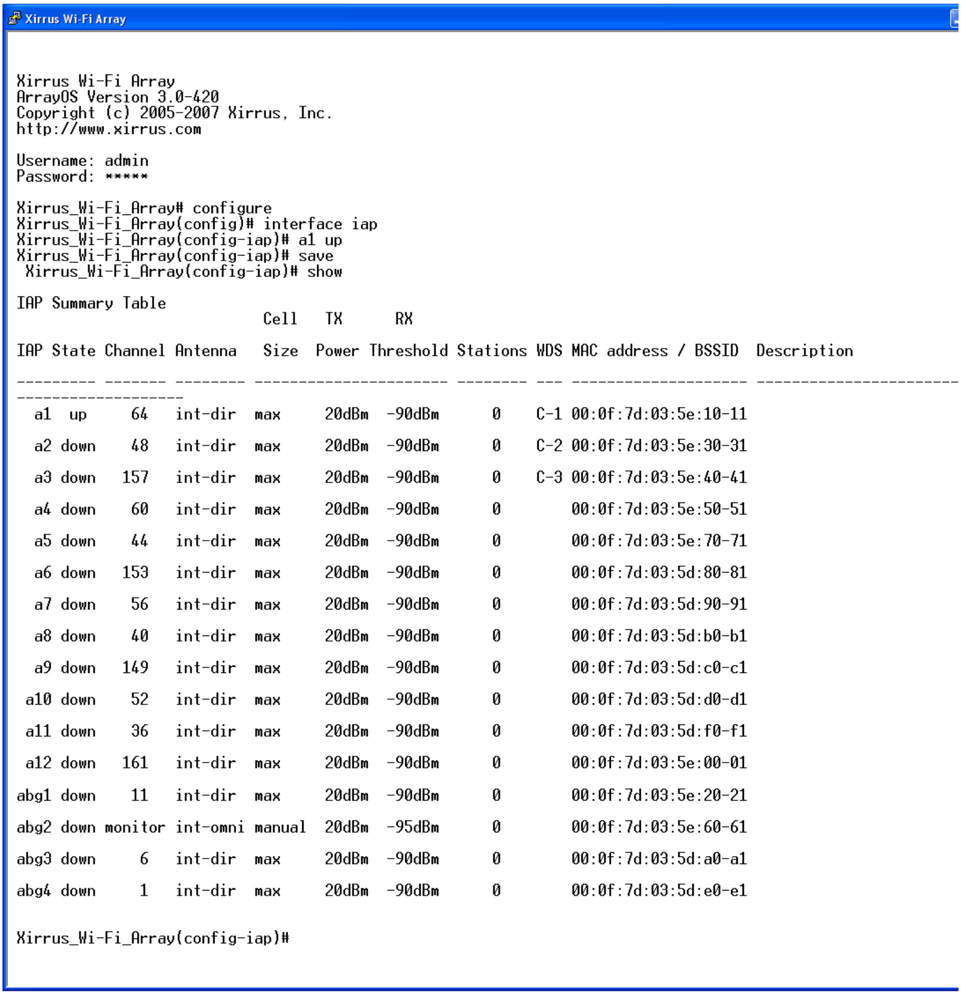


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 146. 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).

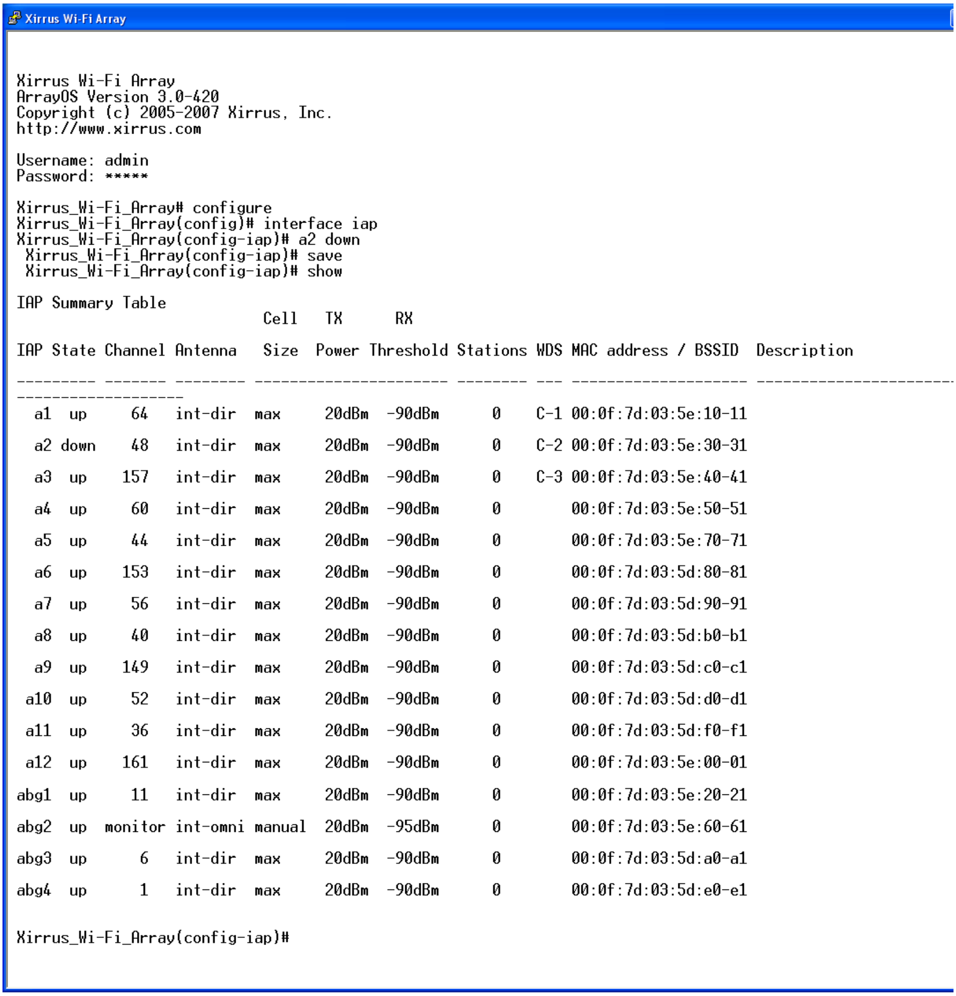


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 147. 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).



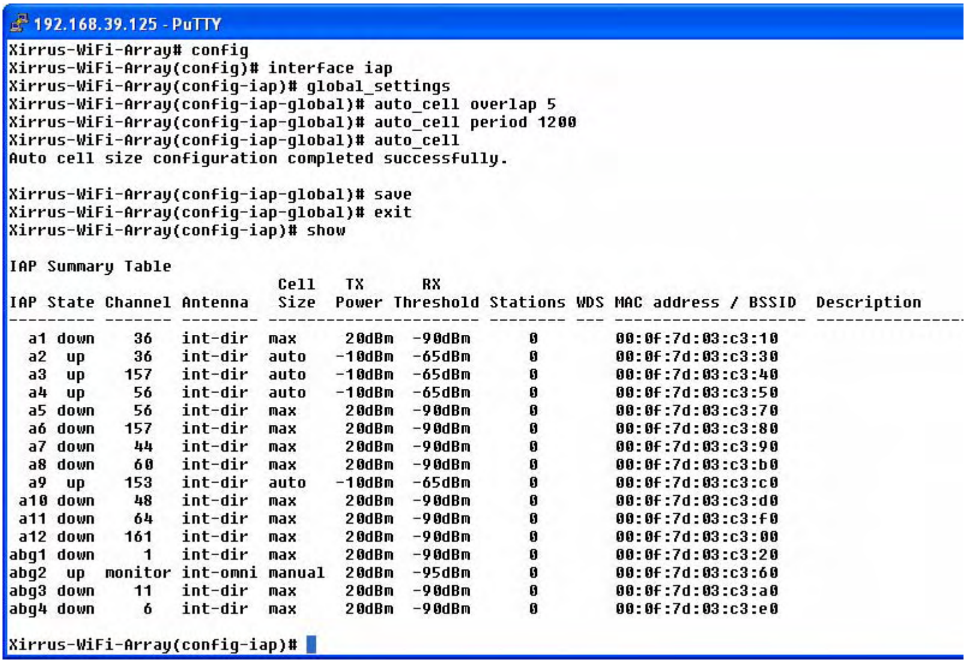
```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 148. 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 35.) 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 **abg2,** 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

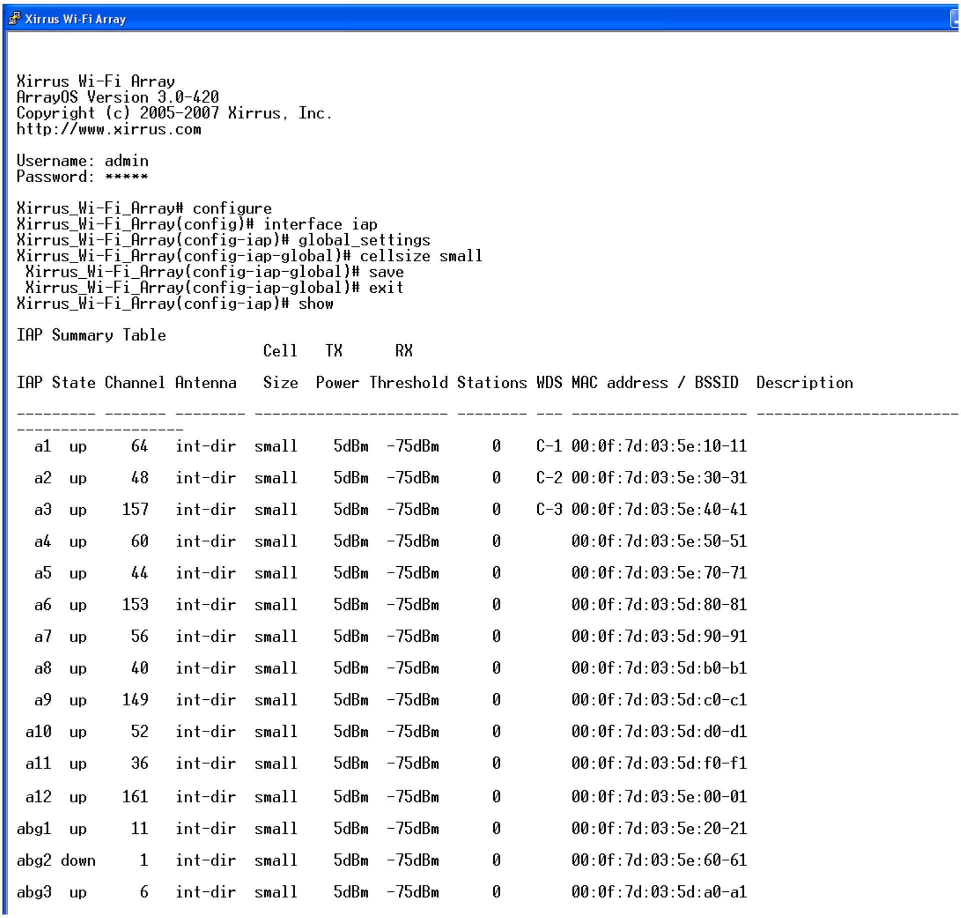
```
Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# auto_cell overlap 5
Xirrus-WiFi-Array(config-iap-global)# auto_cell period 1200
Xirrus-WiFi-Array(config-iap-global)# auto_cell
Auto cell size configuration 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
                                 Cell   TX      RX
IAP State Channel Antenna      Size  Power 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 149. 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 **abg2** the cell size cannot be set globally—you must first disable the intrude-detect feature on **abg2**.

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 35.

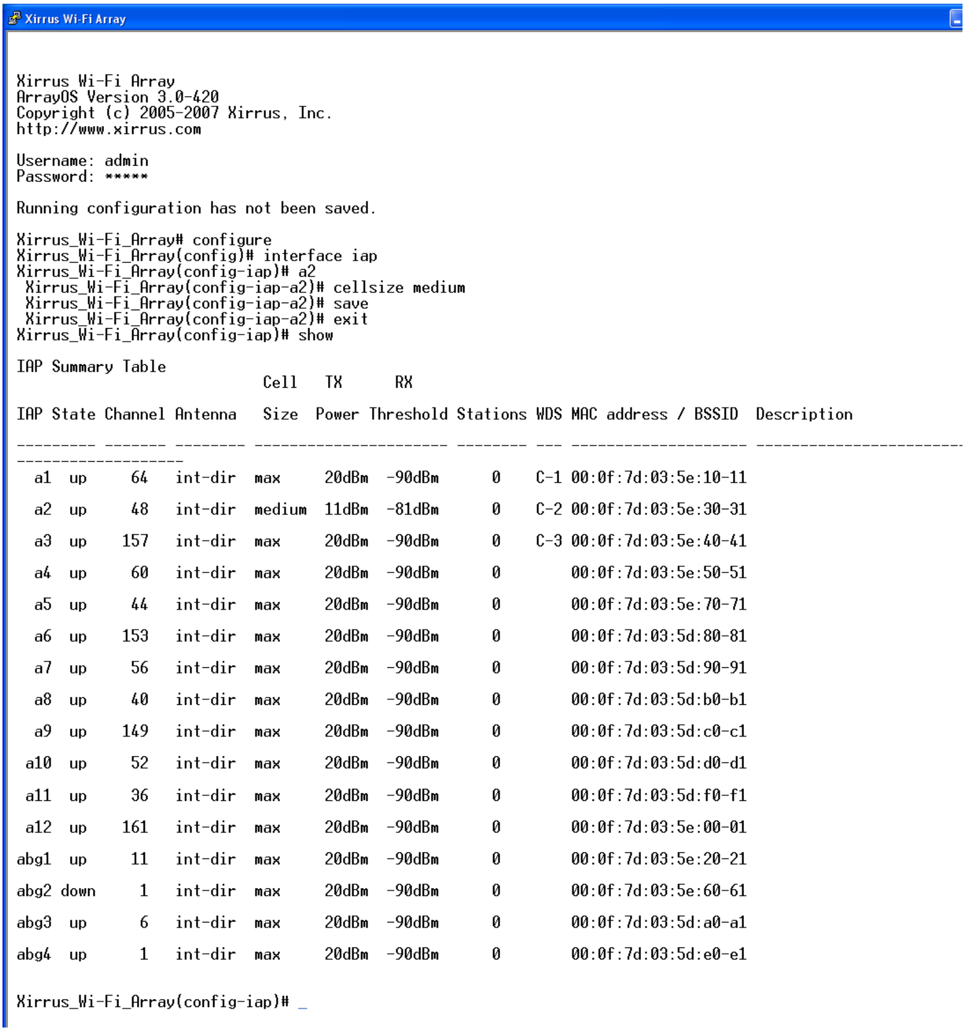


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 150. 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 35.

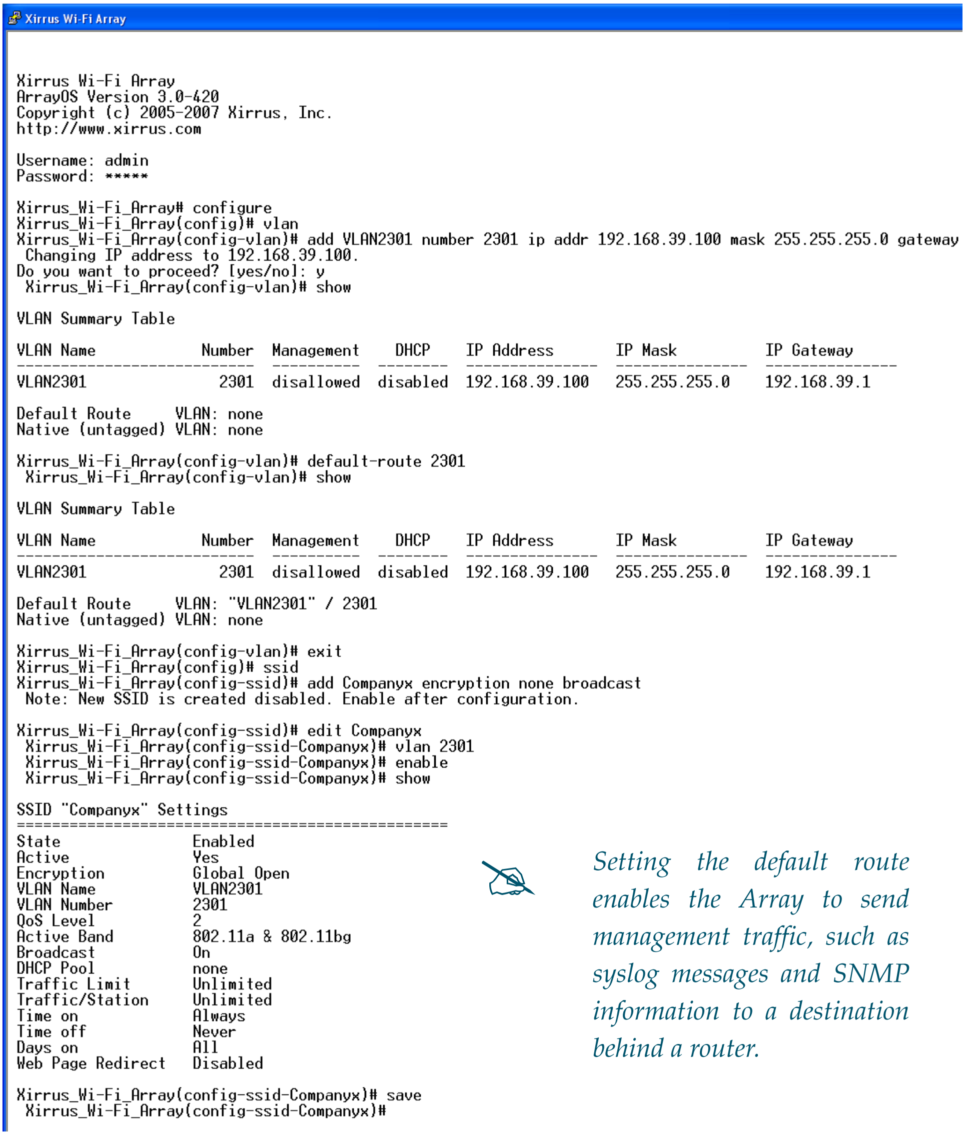


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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
                            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  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 151. 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 152. Configuring VLANs on an Open SSID

Configuring Self-Monitoring Mode (Loopback Tests)

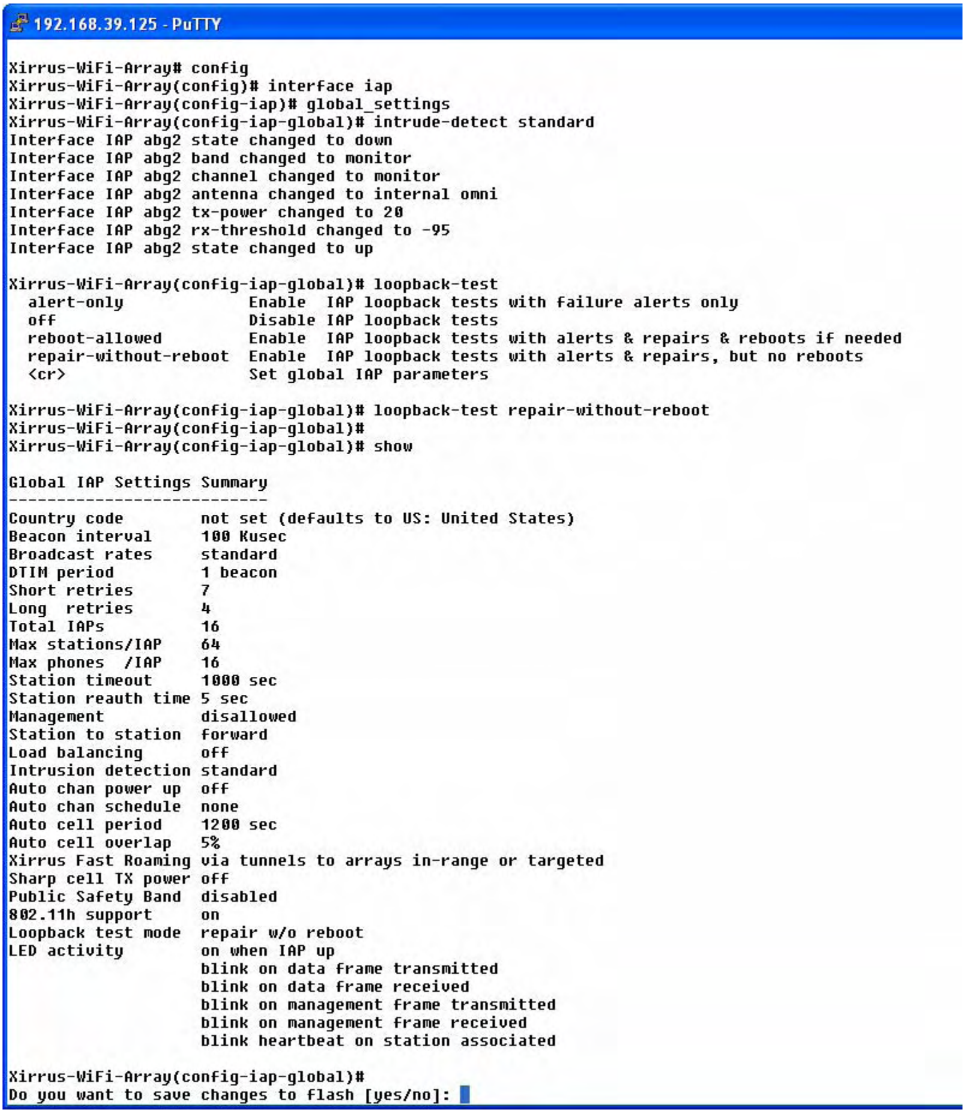
The Array uses the built-in monitor radio (IAP abg2) to monitor other radios in the Array. Tests include sending probes on all channels and checking for a response, and checking whether beacons are received from the other radio. If a problem is detected, corrective actions are taken to recover. Loopback mode operation is described in detail in "Array Monitor and Loopback Testing Capabilities" on page 341.

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). Loopback tests are off by default.

This is a global IAPs setting—abg2 will monitor all other radios according to the settings above, and it cannot be set up to monitor particular radios. Self-monitoring mode requires Intrusion Detection to be set to Standard.

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



```
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 needed
  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 153. Configuring a Loopback Test

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 309**.
- **"Reinstalling the Access Panel" on page 312**.
- **"Replacing the FLASH Memory Module" on page 314**.
- **"Replacing the Main System Memory" on page 316**.
- **"Replacing the Integrated Access Point Radio Module" on page 318**.
- **"Replacing the Power Supply Module" on page 321**.

! *Always turn OFF the Array's power switch and disconnect the AC power cord 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.*

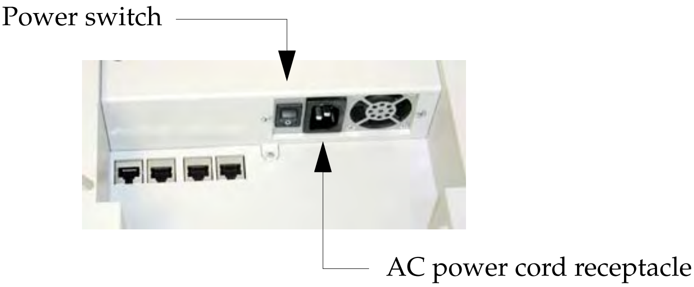


Figure 154. Disconnecting Power from the Array

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 (XN16 and XN8 only).
2. Disconnect the AC power cord 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.

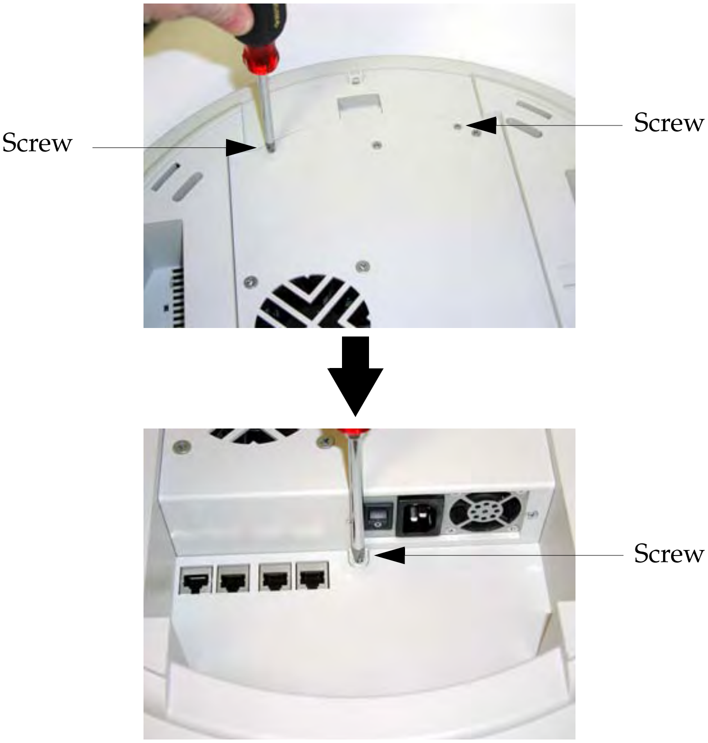


Figure 155. Removing the Access Panel Screws

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

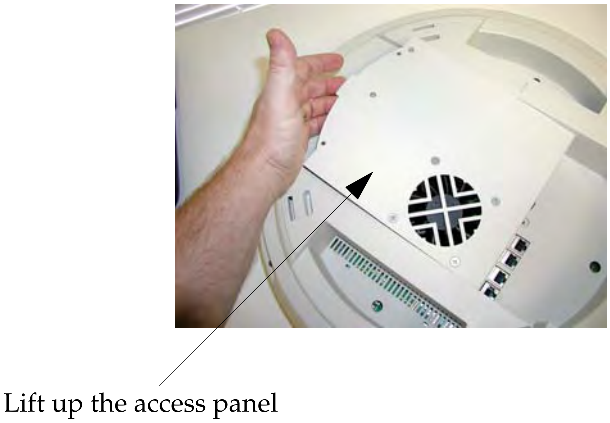


Figure 156. Removing the Access Panel

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

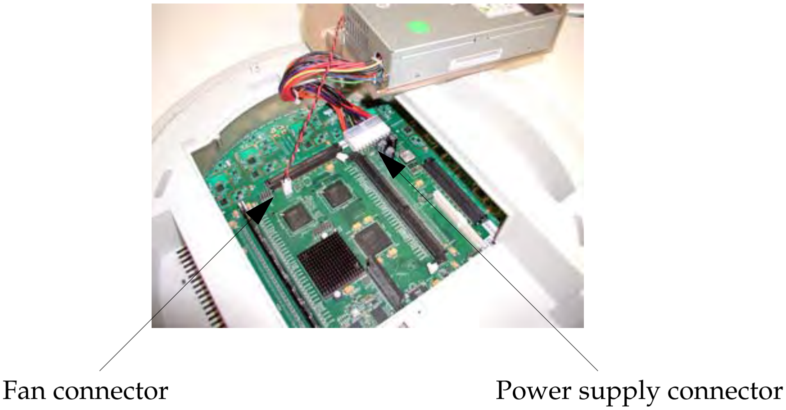


Figure 157. Disconnecting the Power Supply and Fan

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.

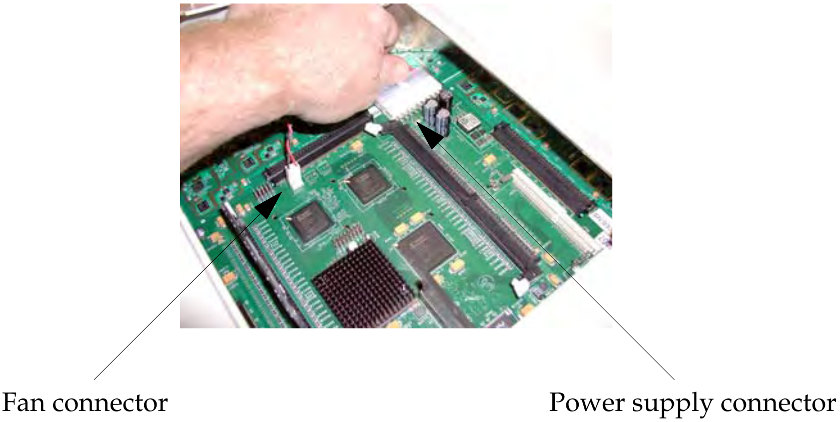


Figure 158. Reconnecting the Fan and Power Supply

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

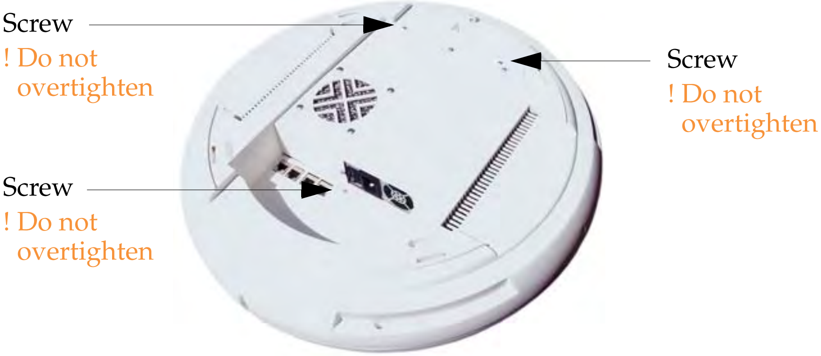


Figure 159. Reinstalling the Access Panel

3. Reconnect the AC power cord and turn ON the main power switch.

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 309.
2. Remove the FLASH memory module, taking care not to "wiggle" the module and risk damaging the connection points.

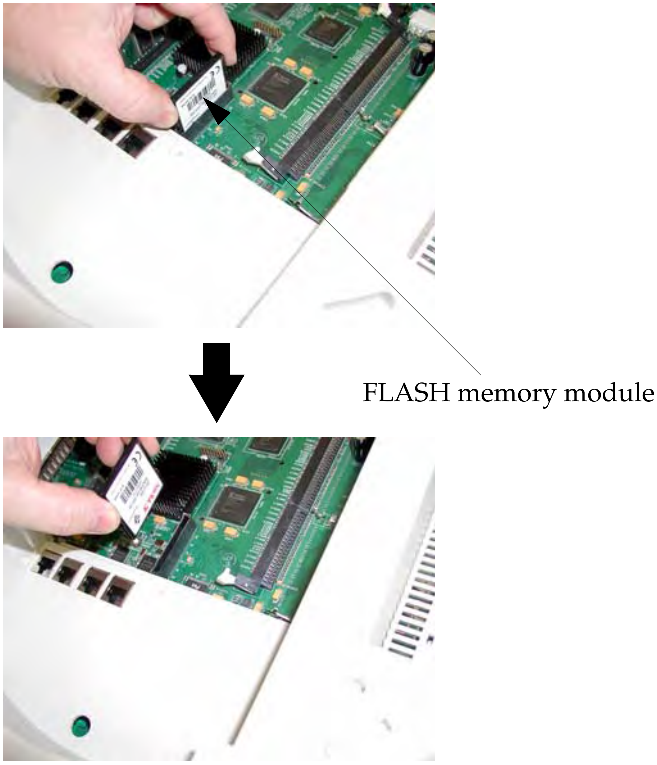


Figure 160. Removing the FLASH Memory Module

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 312).

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 309).
2. Remove the DIMM memory module, taking care not to "wiggle" the module and risk damaging the connection points.

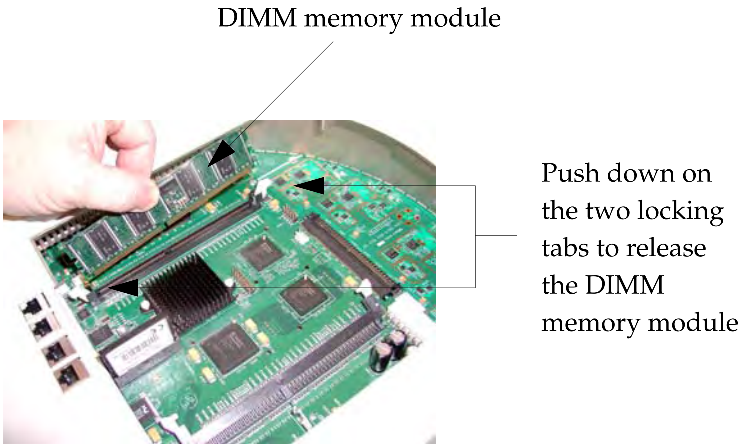

DIMM memory module
Push down on the two locking tabs to release the DIMM memory module

Figure 161. 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 312).

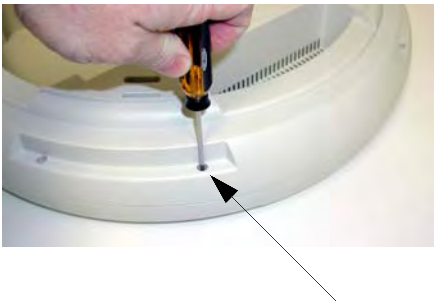
See Also

Reinstalling the Access Panel
Removing the Access Panel
Replacing the FLASH Memory Module

Replacing the Integrated Access Point Radio Module

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

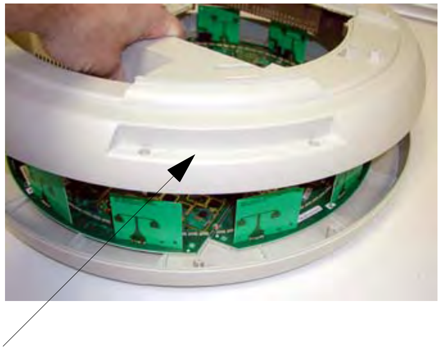
1. Remove the access panel (refer to "Removing the Access Panel" on page 309).
2. Remove the locking screws (8 places) that secure the chassis cover to the main body of the Wi-Fi Array.



Screws (8 places)

Figure 162. Removing the Chassis Cover Screws

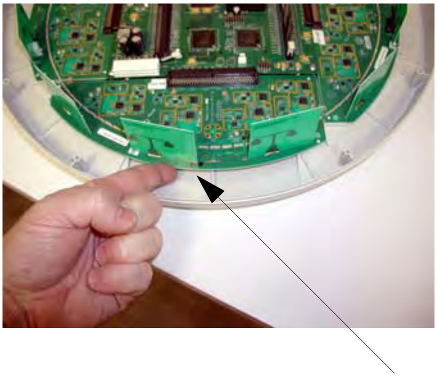
3. Lift and remove the chassis cover.



Remove the chassis cover

Figure 163. Removing the Chassis Cover

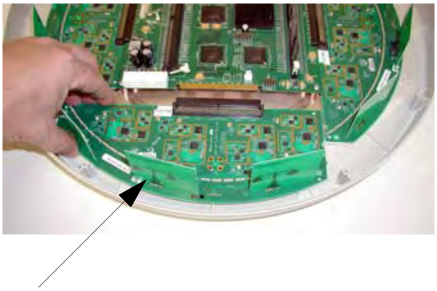
4. Lift the edge of the integrated access point module.



Lift here (do not force)

Figure 164. 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 165. 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 312).

See Also

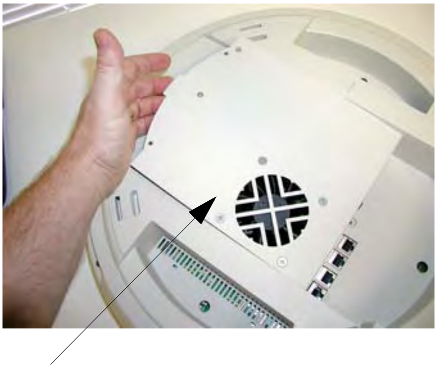
Reinstalling the Access Panel
Removing the Access Panel
Replacing the FLASH Memory Module
Replacing the Main System Memory
Replacing the Power Supply Module
Appendix A: Servicing the Wi-Fi Array

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 309).

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 312.



Access panel (with power supply and fan)

Figure 166. 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 323**.

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

Setting	Default Value
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
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	
● XN16	802.11an for a1 to a12 802.11bg for abg1 to abg4
● XN8	802.11an for a1 to a4 802.11bg for abg1 to abg4
● XN4	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)
Trap Port	162
Authorization Fail Port	On

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes

Setting	Default Value
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
Broadcast	On

Security

Global Settings - Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)

Setting	Default Value
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
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

Setting	Default Value
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

Setting	Default Value
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**
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

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 **abg2** radio is oriented in the direction of the least required coverage, because when in monitor mode the abg2 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 184.

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 know my management session is secure?

A. Follow these guidelines:

- Administrator passwords
  Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.

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

- Configuration auditing

Do not change approved configuration settings. The optional Xirrus 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 (abg/4) which constantly scans the local wireless environment for rogue APs (non-Xirrus devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

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 Loopback Testing Capabilities

All models of the Wi-Fi Array have a monitor radio, **abg2,** 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 abg2 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 abg2 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 204 for more details. The values above are the factory default settings for the Array.

How Monitoring Works

When the monitor radio abg2 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 221. Note that the **Advanced** setting is only used with the optional Xirrus Defense Module (XDM) software package.

Loopback Testing

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 221). When this mode is enabled, IAP abg2 performs loopback tests on the Array. Radio Assurance Mode (also called loopback mode) requires **Intrusion Detection** to be set to **Standard** (See Step 1 in "Advanced RF Settings" on page 221).

When **Loopback 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 "Loopback Mode Options" on page 343), 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 "Loopback Mode Options" on page 343), 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

Loopback Mode 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 223):

- **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:
```

Contact Information

Xirrus, Inc. is located in Westlake Village, California, just 45 minutes northwest of downtown Los Angeles and 45 minutes southeast of Santa Barbara.

Xirrus, Inc.
370 North Westlake Blvd, Suite 200
Westlake Village, CA 91362
USA

Tel: 1.805.497.0955
Fax: 1.805.449.1180

www.xirrus.com

support.xirrus.com

Glossary of Terms

802.11a

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

802.11b

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

802.11d

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

802.11g

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

802.1Q

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

AES

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

authentication

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

bandwidth

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

beacon interval

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

bit rate

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

BSS

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

BSSID

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

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.

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 “Contact Information” on page 349 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. It provides strong authentication and secure communications over insecure channels. SSH protects a network from attacks, such as IP spoofing, IP source routing, and DNS spoofing. Attackers who has managed to take over a network can only force SSH to disconnect—they cannot "play back" the traffic or hijack the connection when encryption is enabled. When using SSH's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted making it almost impossible for an outsider to collect passwords.

SSID

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

subnet mask

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

TKIP

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

transmit power

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

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

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

WDS (Wireless Distribution System)

WDS creates wireless backhauls 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.

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.

Use this Space for Your Notes

Index

User's Guide

XIRRUS®

Wi-Fi Arrays