The Command Line Interface

This section covers the commands and the command structure used by the Wireless Array's Command Line Interface (CLI), and provides a procedure for establishing an SSH connection to the Array. Topics discussed include:

- **"Establishing a Secure Shell (SSH) Connection" on page 377**.
- **"Getting Started with the CLI" on page 379.**
- **"Top Level Commands" on page 381.**
- **"Configuration Commands" on page 390.**
- **"Sample Configuration Tasks" on page 426.**

> *Some commands are only available if the Array's license includes appropriate Xirrus **Advanced Feature Sets**. If a command is unavailable, an error message will notify you that your license does not support the feature. See **"About Licensing and Upgrades" on page 361**.*

See Also

Establishing Communication with the Array
Network Map
System Tools

Establishing a Secure Shell (SSH) Connection

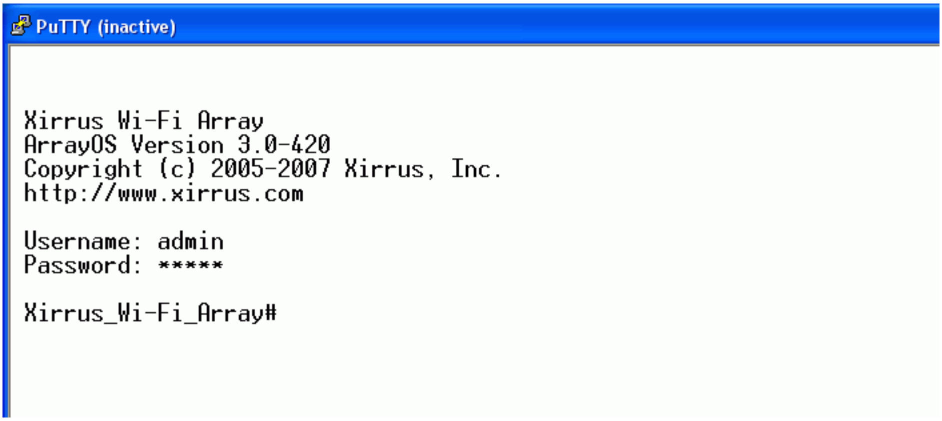
Use this procedure to initialize the system and log in to the Command Line Interface (CLI) via a Secure Shell (SSH) utility, such as PuTTY. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell version 2 (SSH-2) utility. Make sure that your SSH utility is set up to use SSH-2.

1. Start your SSH session and communicate with the Array via its IP address.

   - If the Array is connected to a network that uses DHCP, use the address assigned by DHCP. We recommend that you have the network administrator assign a reserved address to the Array for ease of access in the future.

- If the network does not use DHCP, use the factory default address 10.0.2.1 to access either the Gigabit 1 or Gigabit 2 Ethernet port. You may need to change the IP address of the port on your computer that is connected to the Array—change that port's IP address so that it is on the same 10.0.2.xx subnet as the Array port.
- If your Array is an 8-, 12-, or 16-port model, it has a 10/100Mb Ethernet port called Ethernet0. This management port has a default IP address of 10.0.1.1. You may connect your computer directly to this port, but you will need to set the IP address of the connected port on your computer to the 10.0.1.xx subnet.

2. At the login prompt, enter your user name and password (the default for both is **admin**). Login names and passwords are case-sensitive. You are now logged in to the Array's Command Line Interface.



```
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#
```

Figure 184. Logging In

Getting Started with the CLI

The root command prompt (**Root Command Prompt**) is the first prompt you see after logging in to the CLI. If you are at a level other than the root command prompt you can return to this prompt at any time by using the **exit** command to step back through each command prompt level. The root command prompt you see in the CLI window is determined by the host name you assigned to your Array. The prompt **Xirrus_Wi-Fi_Array** is displayed throughout this document simply because this is the host name assigned to the Array used for development. To terminate your session at any time, use the **quit** command.

Inputting Commands

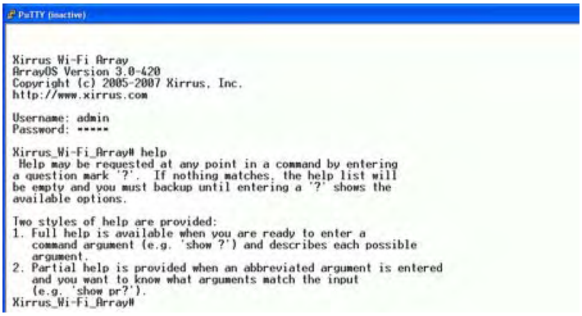
When inputting commands you need only type as many characters as the system requires before it recognizes your input. For example, you can type the abbreviated term **config** to access the configure prompt.

Getting Help

The CLI offers the following two levels of assistance:

- **help Command**

  The **help** command is only available at the root command prompt. Initiating this command generates a window that provides information about the types of help that are available with the CLI.

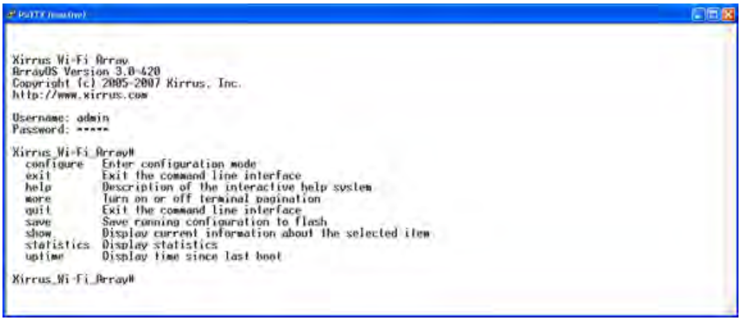


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

Username: admin
Password: *****

Xirrus_Wi-Fi_Array# help
 Help may be requested at any point in a command by entering
a question mark '?'.  If nothing matches, the help list will
be empty and you must backup until entering a '?' shows the
available options.

Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show pr?').
Xirrus_Wi-Fi_Array#
```

Figure 185. Help Window

- **? Command**

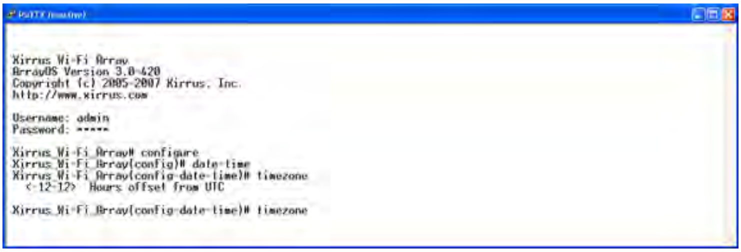
This command is available at any prompt and provides either FULL or PARTIAL help. Using the **?** (question mark) command when you are ready to enter an argument will display all the possible arguments (full help). Partial help is provided when you enter an abbreviated argument and you want to know what arguments will match your input.



```
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   Enter configuration mode
  exit        Exit the command line interface
  help        Description of the interactive help system
  more        Turn on or off terminal pagination
  quit        Exit the command line interface
  save        Save running configuration to flash
  show        Display current information about the selected item
  statistics  Display statistics
  uptime      Display time since last boot

Xirrus_Wi-Fi_Array#
```

Figure 186. Full Help

Figure 187 shows an example of how the Help system can provide the argument and format when specifying the time zone under the **date-time** command.



```
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)# date-time
Xirrus_Wi-Fi_Array(config-date-time)# timezone
  <-12-12>  Hours offset from UTC

Xirrus_Wi-Fi_Array(config-date-time)# timezone
```

Figure 187. Partial Help

Top Level Commands

This section offers an at-a-glance view of all top level commands—organized alphabetically. Top level commands are defined here as commands that are directly accessible from the root command prompt (**Xirrus_Wi-Fi_Array#**). The root command prompt is based on the host name assigned to your Array. When inputting commands, be aware that all commands are **case-sensitive**.

All other commands are considered second level configuration commands—these are the commands you use to configure specific elements of the Array's features and functionality. For a listing of these commands with examples of command formats and structure, go to "Configuration Commands" on page 390.

Root Command Prompt

The following table shows the top level commands that are available from the root command prompt [**Xirrus_Wi-Fi_Array**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
configure	Enter the configuration mode. See "Configuration Commands" on page 390.
exit	Exit the CLI and terminate your session—if this command is used at any level other than the root command prompt you will simply exit the current level (step back) and return to the previous level.
help	Show a description of the interactive help system. See also, "Getting Help" on page 379.
history	List history of commands that have been executed.
more	Turn terminal pagination ON or OFF.
quit	Exit the Command Line Interface (from any level).
search	Search for pattern in show command output.

Command	Description
show	Display information about the selected item. See "show Commands" on page 385.
statistics	Display statistical data about the Array. See "statistics Commands" on page 388.
uptime	Display the elapsed time since the last boot.

configure Commands

The following table shows the second level commands that are available with the top level **configure** command [**Xirrus_Wi-Fi_Array(config)#**].

Command	Description
@	Type **@n** to execute command n (as shown by the history command).
acl	Configure the Access Control List.
admin	Define administrator access parameters.
cdp	Configure Cisco Discovery Protocol settings.
clear	Remove/clear the requested elements.
cluster	Make configuration changes to multiple Arrays.
contact-info	Contact information for assistance on this Array.
date-time	Configure date and time settings.
dhcp-server	Configure the DHCP Server.
dns	Configure the DNS settings.
end	Exit the configuration mode.
exit	Go UP one mode level.
file	Manage the file system.

Command	Description
filter	Define protocol filter parameters.
group	Define user groups with parameter settings
help	Description of the interactive Help system.
history	List history of commands that have been executed.
hostname	Host name for this Array.
interface	Select the interface to configure.
load	Load running configuration from flash
location	Location name for this Array.
management	Configure array management parameters
more	Turn ON or OFF terminal pagination.
netflow	Configure NetFlow data collector.
no	Disable (if enabled) or set to default value.
quit	Exit the Command Line Interface.
radius-server	Configure the RADIUS server parameters.
reboot	Reboot the Array.
reset	Reset all settings to their factory default values and reboot.
restore	Reset all settings to their factory default values and reboot.
run-tests	Run selective tests.
save	Save the running configuration to FLASH.
search	Search for pattern in show command output.
security	Set the security parameters for the Array.

Command	Description
show	Display current information about the selected item.
snmp	Enable, disable or configure SNMP.
ssid	Configure the SSID parameters.
statistics	Display statistics.
syslog	Enable, disable or configure the Syslog Server.
uptime	Display time since the last boot.
vlan	Configure VLAN parameters.
wifi-tag	Configure VLAN parameters.

show Commands

The following table shows the second level commands that are available with the top level **show** command [**Xirrus_Wi-Fi_Array# show**].

Command	Description
acl	Display the Access Control List.
admin	Display the administrator list or login information.
array-info	Display system information.
associated-stations	Display stations that have associated to the Array.
boot-env	Display Boot loader environment variables.
capabilities	Display detailed station capabilities.
cdp	Display Cisco Discovery Protocol settings.
channel-list	Display list of Array's 802.11an and bgn channels.
clear-text	Display and enter passwords and secrets in the clear.
conntrack	Display the Connection Tracking table.
console	Display terminal settings.
contact-info	Display contact information.
date-time	Display date and time settings summary.
dhcp-leases	Display IP addresses (leases) assigned to stations by the DHCP server.
dhcp-pool	Display internal DHCP server settings summary information.
diff	Display the difference between configurations.
dns	Display DNS summary information.

Command	Description
error-numbers	Display the detailed error number in error messages.
ethernet	Display Ethernet interface summary information.
external-radius	Display summary information for the external RADIUS server settings.
factory-config	Display the Array factory configuration information.
filters	Display filter information.
iap	Display IAP configuration information.
internal-radius	Display the users defined for the embedded RADIUS server.
lastboot-config	Display Array configuration at the time of the last boot-up.
management	Display settings for managing the Array, plus Standby, FIPS, and other information.
network-map	Display network map information.
realtime-monitor	Display realtime statistics for all IAPs.
rogue-ap	Display rogue AP information.
route	Display the routing table.
rssi-map	Display RSSI map by IAP for station.
running-config	Display configuration information for the Array currently running.
saved-config	Display the last saved Array configuration.
security	Display security settings summary information.
self-test	Display self test results.
snmp	Display SNMP summary information.

Command	Description
spanning-tree	Display spanning tree information.
spectrum-analyzer	Display spectrum analyzer measurements.
ssid	Display SSID summary information.
stations	Display station information.
statistics	Display statistics.
syslog	Display the system log.
syslog-settings	Display the system log (Syslog) settings.
temperature	Display the current board temperatures.
unassociated-stations	Display unassociated station information.
vlan	Display VLAN information.
wds	Display WDS information.
<cr>	Display configuration or status information.

statistics Commands

The following table shows the second level commands that are available with the top level **statistics** command [**Xirrus_Wi-Fi_Array# statistics**].

Command	Description
ethernet	Display statistical data for all Ethernet interfaces.
Ethernet Name **eth0**, **gig1**, **gig2**	Display statistical data for the defined Ethernet interface (either eth0, gig1 or gig2). FORMAT: **statistics gig1**
filter	Display statistics for defined filters (if any). FORMAT: **statistics filter [detail]**
filter-list	Display statistics for defined filter list (if any). FORMAT: **statistics filter <filter-list>**
iap	Display statistical data for the defined IAP. FORMAT: **statistics iap iap2** **statistics iap abgn4**
station	Display statistical data about associated stations. FORMAT: **statistics station billw**
vlan	Display statistical data for the defined VLAN. You must use the VLAN number (not its name) when defining a VLAN. FORMAT: **statistics vlan 1**

Command	Description
wds	Display statistical data for the defined active WDS (Wireless Distribution System) links. FORMAT: **statistics wds 1**
<cr>	Display configuration or status information.

Configuration Commands

All configuration commands are accessed by using the **configure** command at the root command prompt (**Xirrus_Wi-Fi_Array#**). This section provides a brief description of each command and presents sample formats where deemed necessary. The commands are organized alphabetically. When inputting commands, be aware that all commands are **case-sensitive**.

To see examples of some of the key configuration tasks and their associated commands, go to "Sample Configuration Tasks" on page 426.

acl

The **acl** command [**Xirrus_Wi-Fi_Array(config)# acl**] is used to configure the Access Control List.

Command	Description
add	Add a MAC address to the list. FORMAT: **acl add AA:BB:CC:DD:EE:FF**
del	Delete a MAC address from the list. FORMAT: **acl del AA:BB:CC:DD:EE:FF**
disable	Disable the Access Control List FORMAT: **acl disable**
enable	Enable the Access Control List FORMAT: **acl enable**
reset	Delete all MAC addresses from the list. FORMAT: **acl reset**

admin

The **admin** command [**Xirrus_Wi-Fi_Array(config-admin)#**] is used to configure the Administrator List.

Command	Description
add	Add a user to the Administrator List. FORMAT: **admin add [userID]**
del	Delete a user to the Administrator List. FORMAT: **admin del [userID]**
edit	Modify user in the Administrator List. FORMAT: **admin edit [userID]**
radius	Define a RADIUS server to be used for authenticating administrators. FORMAT: **admin radius [disable | enable | off | on | timeout <seconds> | auth-type [PAP | CHAP]]** **admin radius [primary |secondary] port <portid> server [<ip-addr> | <host>] secret <shared-secret>**
reset	Delete all users and restore the default user. FORMAT: **admin reset**

cdp

The **cdp** command [**Xirrus_Wi-Fi_Array(config)# cdp**] is used to configure the Cisco Discovery Protocol.

Command	Description
disable	Disable the Cisco Discovery Protocol FORMAT: **cdp disable**
enable	Enable the Cisco Discovery Protocol FORMAT: **cdp enable**
hold-time	Select CDP message hold time before messages received from neighbors expire. FORMAT: **cdp hold-time [# seconds]**
interval	The Array sends out CDP announcements at this interval. FORMAT: **cdp interval [# seconds]**
off	Disable the Cisco Discovery Protocol FORMAT: **cdp off**
on	Enable the Cisco Discovery Protocol FORMAT: **cdp on**

clear

The **clear** command **[Xirrus_Wi-Fi_Array(config)# clear]** is used to clear requested elements.

Command	Description
authentication	Deauthenticate a station. FORMAT: **clear station [authenticated station]**
history	Clear the history of CLI commands executed. FORMAT: **clear history**
screen	Clear the screen where you're viewing CLI output. FORMAT: **clear syslog**
statistics	Clear the statistics for a requested interface. FORMAT: **clear statistics [eth0]**
syslog	Clear all Syslog messages, but continue to log new messages. FORMAT: **clear syslog**

cluster

The **cluster** command [**Xirrus_Wi-Fi_Array(config)# cluster**] is used to create and operate clusters. Clusters allow you to configure multiple Arrays at the same time. Using CLI (or WMI), you may define a set of Arrays that are members of the cluster. Then you may switch the Array to Cluster operating mode for a selected cluster, which sends all successive configuration commands issued via CLI or WMI to all of the member Arrays. When you exit cluster mode, configuration commands revert to applying only to the Array to which you are connected.

For more information, see "Clusters" on page 352.

Command	Description
add	Create a new Array cluster. Enters edit mode for that cluster to allow you to specify the Arrays that belong to the cluster. FORMAT: **cluster add [cluster-name]**
del	Delete an Array cluster. Type **del ?** to list the existing clusters. FORMAT: **cluster del [cluster-name]**
edit	Enter edit mode for selected cluster to add or delete Arrays that belong to the cluster. FORMAT: **cluster edit [cluster-name]**
end	Exit Cluster configuration mode. Configuration returns to normal operation, affecting this Array only. FORMAT: **cluster end**

Command	Description
operate	Enter Cluster operation mode. All configuration commands are applied to all of the selected cluster's member Arrays until you give the **end** command (see above). FORMAT: **cluster operate [cluster-name]**
reset	Delete all clusters. FORMAT: **cluster reset**

contact-info

The **contact-info** command **[Xirrus_Wi-Fi_Array(config)# contact-info]** is used for managing administrator contact information.

Command	Description
email	Add an email address for the contact (must be in quotation marks). FORMAT: **contact-info email ["contact@mail.com"]**
name	Add a contact name (must be in quotation marks). FORMAT: **contact-info name ["Contact Name"]**
phone	Add a telephone number for the contact (must be in quotation marks). FORMAT: **contact-info phone ["8185550101"]**

date-time

The **date-time** command **[Xirrus_Wi-Fi_Array(config-date-time)#]** is used to configure the date and time parameters. Your Array supports the Network Time Protocol (NTP) in order to ensure that the Array's internal time is accurate. NTP is set to UTC time by default; however, you can set the time zone so that your Array will display local time. This is done by defining an offset from the UTC value. For example, Pacific Standard Time is 8 hours behind UTC time, so the offset from UTC time would be -8.

Command	Description
dst_adjust	Enable adjustment for daylight savings. FORMAT: **date-time dst_adjust**
no	Disable daylight savings adjustment. FORMAT: **date-time no dst_adjust**
ntp	Enable the NTP server. FORMAT: **date-time ntp on** (or **off** to disable)
offset	Set an offset from Greenwich Mean Time. FORMAT: **date-time no dst_adjust**
set	Set the date and time for the Array. FORMAT: **date-time set [10:24 10/23/2007]**
timezone	Configure the time zone. FORMAT: **date-time timezone [-8]**

dhcp-server

The **dhcp-server** command [**Xirrus_Wi-Fi_Array(config-dhcp-server)**#] is used to add, delete and modify DHCP pools.

Command	Description
add	Add a DHCP pool. FORMAT: **dhcp-server add [dhcp pool]**
del	Delete a DHCP pool. FORMAT: **dhcp-server del [dhcp pool]**
edit	Edit a DHCP pool FORMAT: **dhcp-server edit [dhcp pool]**
reset	Delete all DHCP pools. FORMAT: **dhcp-server reset**

dns

The **dns** command [**Xirrus_Wi-Fi_Array(config-dns)#**] is used to configure your DNS parameters.

Command	Description
domain	Enter your domain name. FORMAT: **dns domain [www.mydomain.com]**
server1	Enter the IP address of the primary DNS server. FORMAT: **dns server1 [1.2.3.4]**
server2	Enter the IP address of the secondary DNS server. FORMAT: **dns server1 [2.3.4.5]**
server3	Enter the IP address of the tertiary DNS server. FORMAT: **dns server1 [3.4.5.6]**

file

The **file** command [**Xirrus_Wi-Fi_Array(config-file)#**] is used to manage files.

Command	Description
active-image	Validate and commit a new array software image.
backup-image	Validate and commit a new backup software image.
check-image	Validate a new array software image.
chkdsk	Check flash file system.
copy **cp**	Copy a file to another file. FORMAT: **file copy [sourcefile destinationfile]**
dir	List the contents of a directory. FORMAT: **file dir [directory]**
erase	Delete a file from the FLASH file system. FORMAT: **file erase [filename]**
format	Format flash file system.
ftp	Open an FTP connection with a remote server. Files will be transferred in binary mode. FORMAT: **file ftp host {<hostname> |<ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the Array, it **must** be transferred in binary mode, or the file may be corrupted.
list	List the contents of a file. FORMAT: **file list [filename]**

Command	Description
remote-config	When the Array boots up, it fetches the specified configuration file from the TFTP server defined in the **file remote-server** command, and uses this configuration. This must be an Array configuration file with a **.conf** extension. A partial configuration file may be used. For instance, if you wish to use a single configuration file for all of your Arrays but don't want to have the same IP address for each Array, you may remove the **ipaddr** line from the file. You can then load the file on each array and the local IP addresses will not change. FORMAT: **file remote-config <config-file.conf>** **Note:** If you enter **file remote-config ?**, the help response suggests possibilities by listing all of the configuration files that are currently in the Array's flash.
remote-image	When the Array boots up, it fetches the named image file from the TFTP server defined in the **file remote-server** command, and upgrades to this file before booting. This must be an Array image file with a **.bin** extension. FORMAT: **file remote-image <image-file.bin>** **Note**: This will happen every time that the Array reboots. If you only want to fetch the remote-image one time be sure to turn off the remote image option after the initial download.
remote-server	Sets up a TFTP server to be used for automated remote update of software image and configuration files when rebooting. FORMAT: **file remote-server A.B.C.D**
rename	Rename a file.

Command	Description
scp	Copy a file to or from a remote system. You may specify the port to use.
tftp	Open a TFTP connection with a remote server. FORMAT: **file tftp host {<hostname> |<ip>} [port <port_#>] [user {anonymous | <username> password <passwd> }] { put <source_file> [<dest_file>] | get <source_file> [<dest_file>] }** **Note:** Any time you transfer any kind of software image file for the Array, it **must** be transferred in binary mode, or the file may be corrupted.

filter

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

Command	Description
add	Add a filter. Details about the air cleaner feature are after the end of this table. FORMAT: **filter add [air-cleaner |name]**
add-list	Add a filter list. FORMAT: **filter add-list [name]**
del	Delete a filter. FORMAT: **filter del [name]**
del-list	Delete a filter list. FORMAT: **filter del-list [name]**
edit	Edit a filter. FORMAT: **filter edit [name type]**
edit-list	Edit a filter list FORMAT: **filter edit-list [name type]**
enable	Enable a filter list. FORMAT: **filter enable**
move	Change a filter priority. FORMAT: **filter move [name priority]**

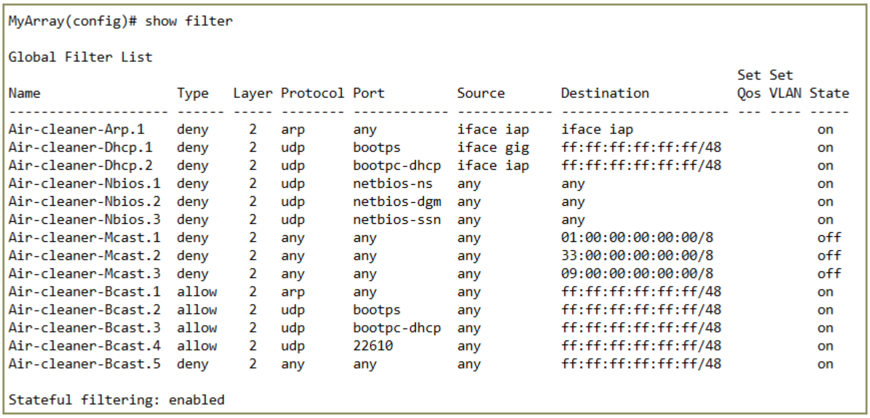
Command	Description
off	Disable a filter list. FORMAT: **filter off**
on	Enable a filter list. FORMAT: **filter on**
reset	Delete all protocol filters and filter lists. FORMAT: **filter reset**
stateful	Enable or disable stateful filtering (firewall). FORMAT: **Stateful [enable | disable | on |off]**

Air Cleaner

The air cleaner feature offers a number of predetermined filter rules that eliminate a great deal of unnecessary wireless traffic, resulting in improved performance. You may select **all** of the air cleaner rules for the greatest effect, or only specific rules, such as **broadcast** or **multicast**, to eliminate only a particular source of traffic. The following options are offered:

```
MyArray(config)# filter add air-cleaner
  all        All air cleaner filters
  arp        Eliminate station to station ARPs over the air
  broadcast  Eliminate broadcast traffic from the air
  dhcp       Eliminate stations serving DHCP addresses from the air
  multicast  Eliminate chatty multicast traffic from the air
  netbios    Eliminate NetBIOS traffic from the air
```

If you select all, the rules shown in Figure 188 are added to the predefined filter list named **Global**. These rules assume that you have station-to-station blocking enabled, that a DHCP server is on the Array's wired connection, and that you want to block most all multicast and all broadcast traffic not vital to normal operation. If you find that there is a particular type of multicast or broadcast traffic that you want to allow, just add a specific allow filter for it before the deny filter in this list that would normally block it. Add or delete any of the Multicast rules as necessary for a specific site. Remember that the order of the rules is important.



```
MyArray(config)# show filter

Global Filter List
                                                                                           Set Set
Name                 Type   Layer Protocol Port         Source       Destination           Qos VLAN State
-------------------- ------ ----- -------- ------------ ------------ --------------------- --- ---- -----
Air-cleaner-Arp.1    deny     2   arp      any          iface iap    iface iap                       on
Air-cleaner-Dhcp.1   deny     2   udp      bootps       iface gig    ff:ff:ff:ff:ff:ff/48            on
Air-cleaner-Dhcp.2   deny     2   udp      bootpc-dhcp  iface iap    ff:ff:ff:ff:ff:ff/48            on
Air-cleaner-Nbios.1  deny     2   udp      netbios-ns   any          any                             on
Air-cleaner-Nbios.2  deny     2   udp      netbios-dgm  any          any                             on
Air-cleaner-Nbios.3  deny     2   udp      netbios-ssn  any          any                             on
Air-cleaner-Mcast.1  deny     2   any      any          any          01:00:00:00:00:00/8             off
Air-cleaner-Mcast.2  deny     2   any      any          any          33:00:00:00:00:00/8             off
Air-cleaner-Mcast.3  deny     2   any      any          any          09:00:00:00:00:00/8             off
Air-cleaner-Bcast.1  allow    2   arp      any          any          ff:ff:ff:ff:ff:ff/48            on
Air-cleaner-Bcast.2  allow    2   udp      bootps       any          ff:ff:ff:ff:ff:ff/48            on
Air-cleaner-Bcast.3  allow    2   udp      bootpc-dhcp  any          ff:ff:ff:ff:ff:ff/48            on
Air-cleaner-Bcast.4  allow    2   udp      22610        any          ff:ff:ff:ff:ff:ff/48            on
Air-cleaner-Bcast.5  deny     2   any      any          any          ff:ff:ff:ff:ff:ff/48            on

Stateful filtering: enabled
```

Figure 188. Air Cleaner Filter Rules

Explanations of some sample rules are below.

- **Air-cleaner-Arp.1** blocks ARPs from one client from being transmitted to clients via all of the radios. The station to station block setting doesn't block this traffic, so this filter eliminates this unnecessary traffic.
- **Air-cleaner-Dhcp.1** drops all DHCP client traffic coming in from the gigabit interface. This traffic doesn't need to be transmitted by the radios since there shouldn't be any DHCP server associated to the radios and offering DHCP addresses. For large subnets the DHCP discover/request broadcast traffic can be significant.
- **Air-cleaner-Dhcp.2** drops all DHCP server traffic coming in from the radio interfaces. There should not be any DHCP server associated to the radios. These rogue DHCP servers are blocked from doing any damage with this filter. There have been quite a few cases in public venues like schools and conventions where such traffic is seen.

- **Air-cleaner-Mcast.1** drops all multicast traffic with a destination MAC address starting with 01. This filters out a lot of IP multicast traffic that starts with 224.
- **Air-cleaner-Mcast.2** drops all multicast traffic with a destination MAC address starting with 33. A lot of IPv6 traffic and other multicast traffic is blocked by this filter.
- **Air-cleaner-Mcast.3** drops all multicast traffic with a destination MAC address starting with 09. A lot of Appletalk traffic and other multicast traffic is blocked by this filter. Note that for OSX 10.6.* Snow Leopard no longer supports Appletalk.
- **Air-cleaner-Bcast.1** allows all ARP traffic (other than the traffic that was denied by **Air-cleaner-Arp.1**). This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.4** allows all XRP traffic from Arrays to be received from the wire. This is needed because **Air-cleaner-Bcast.5** would drop this valid traffic.
- **Air-cleaner-Bcast.5** drops all other broadcast traffic that hasn't previously been explicitly allowed. This filter will catch all UDP broadcast traffic as well as all other known and unknown protocol broadcast traffic.

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 264.

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]**

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]**

management

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

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

The following types of settings may be configured in management mode:

banner	Configure login banner messages
console	Configure console management parameters
https	Enable/disable HTTPS access
license	Set array software license key
load	Load running configuration from flash
max-auth-attempts	Maximum number of authentication (login) attempts (0 means unlimited)
network-assurance	Enable/disable network assurance
reauth-period	Time between failed CLI login attempts
restore	Restore to previous saved config
revert	Revert to saved configuration after delay if configuration not saved
save	Save running configuration to flash
ssh	Enable/disable SSH access
standby	Configure standby parameters
telnet	Enable/disable telnet access
uptime	Display time since last boot
xircon	Enable/disable xircon access. See *Xircon User's Guide* for more information. Not available for XN Arrays.

more

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

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

netflow

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

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

no

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

Command	Description
acl	Disable the Access Control List. FORMAT: **no acl**
dot11a	Disable all 802.11an IAPs (radios). FORMAT: **no dot11a**
dot11bg	Disable all 802.11bgn 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 an external RADIUS server. FORMAT: **radius-server external** To configure a RADIUS server (primary, secondary, or accounting server, by IP address or host name), and the reporting interval use: **radius-server external accounting**
internal	Configure the external RADIUS server. FORMAT: **radius-server internal**
use	Choose the active RADIUS server (either external or internal). FORMAT: **use external** (or internal)

reboot

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

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

reset

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

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

restore

The **restore** command [**Xirrus_Wi-Fi_Array(config)# restore**] is used to restore configuration to a version that was previously saved locally.

Command	Description
?	Use this to display the list of available config files. FORMAT: **restore ?**
<filename>	Enter the name of the locally saved configuration to restore. FORMAT: **restore <config-filename>**

run-tests

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

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

Command	Description
radius-ping	Special ping utility to test the connection to a RADIUS server. FORMAT: **run-tests radius-ping [external | ssid <ssidnum>] [primary | secondary] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** **run-tests radius-ping [internal | server <radserver> port <radport> secret <radsecret>] user <raduser> password <radpasswd> auth-type [CHAP | PAP]** You may select a RADIUS server that you have already configured (**ssid** or **external** or **internal**) or specify another **server**.
rlb	Run manufacturing radio loopback test. FORMAT: **run-tests rlb {optional command line switches}**
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. Supports 802.11 headers. FORMAT: **run-tests tcpdump**

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

security

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

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

snmp

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

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

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**

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]**

uptime

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

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

vlan

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

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

wifi-tag

The **wifi-tag** command [**Xirrus_Wi-Fi_Array(config-wifi-tag)#**] is used to enable or disable Wi-Fi tag capabilities. When enabled, the Array listens for and collects information about Wi-Fi RFID tags sent on the designated channels. See also "Wi-Fi Tag" on page 188.

Command	Description
disable	Disable wifi-tag. FORMAT: **wifi-tag disable**
enable	Enable wifi-tag. FORMAT: **wifi-tag enable**
off	Disable wifi-tag. FORMAT: **wifi-tag off**
on	Enable wifi-tag. FORMAT: **wifi-tag on**
tag-channel-bg	Set an 802.11b or g channel for listening for tags. FORMAT: **wifi-tag tag-channel-bg <1-255>**
udp-port	Set the UDP port which a tagging server will use to query the Array for tagging information. FORMAT: **wifi-tag udp-port <1025-65535>**

Sample Configuration Tasks

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

- **"Configuring a Simple Open Global SSID" on page 427.**
- **"Configuring a Global SSID using WPA-PEAP" on page 428.**
- **"Configuring an SSID-Specific SSID using WPA-PEAP" on page 429.**
- **"Enabling Global IAPs" on page 430.**
- **"Disabling Global IAPs" on page 431.**
- **"Enabling a Specific IAP" on page 432.**
- **"Disabling a Specific IAP" on page 433.**
- **"Setting Cell Size Auto-Configuration for All IAPs" on page 434**
- **"Setting the Cell Size for All IAPs" on page 435.**
- **"Setting the Cell Size for a Specific IAP" on page 436.**
- **"Configuring VLANs on an Open SSID" on page 437.**
- **"Configuring Radio Assurance Mode (Loopback Tests)" on page 438.**

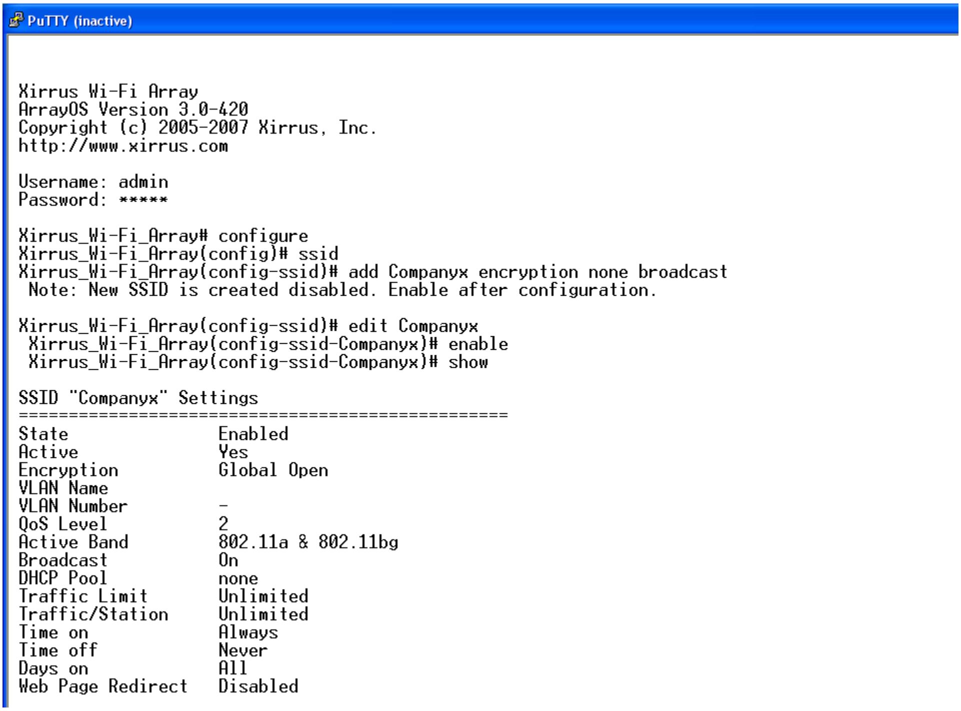
To facilitate the accurate and timely management of revisions to this section, the examples shown here are presented as screen images taken from a Secure Shell (SSH) session (in this case, PuTTY). Depending on the application you are using to access the Command Line Interface, and how your session is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

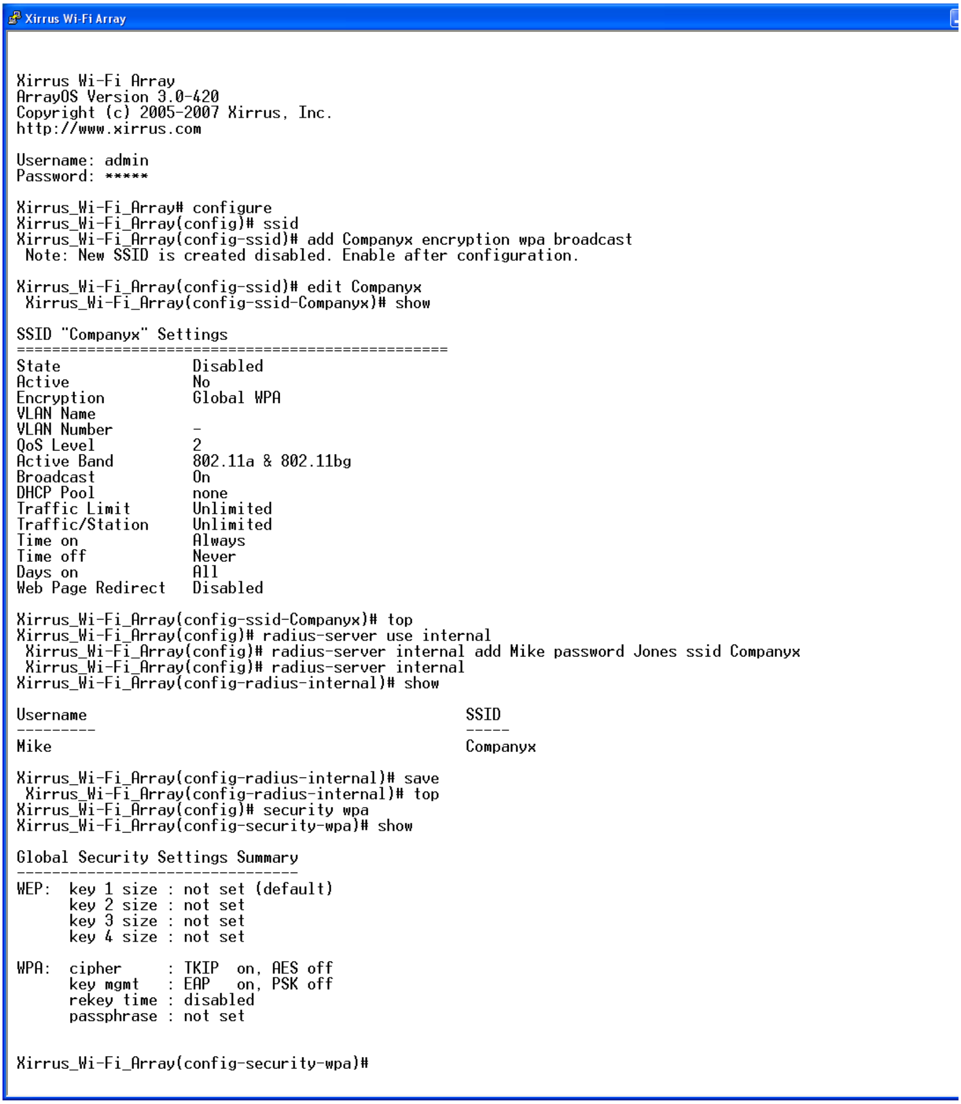


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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
```

Figure 189. 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.

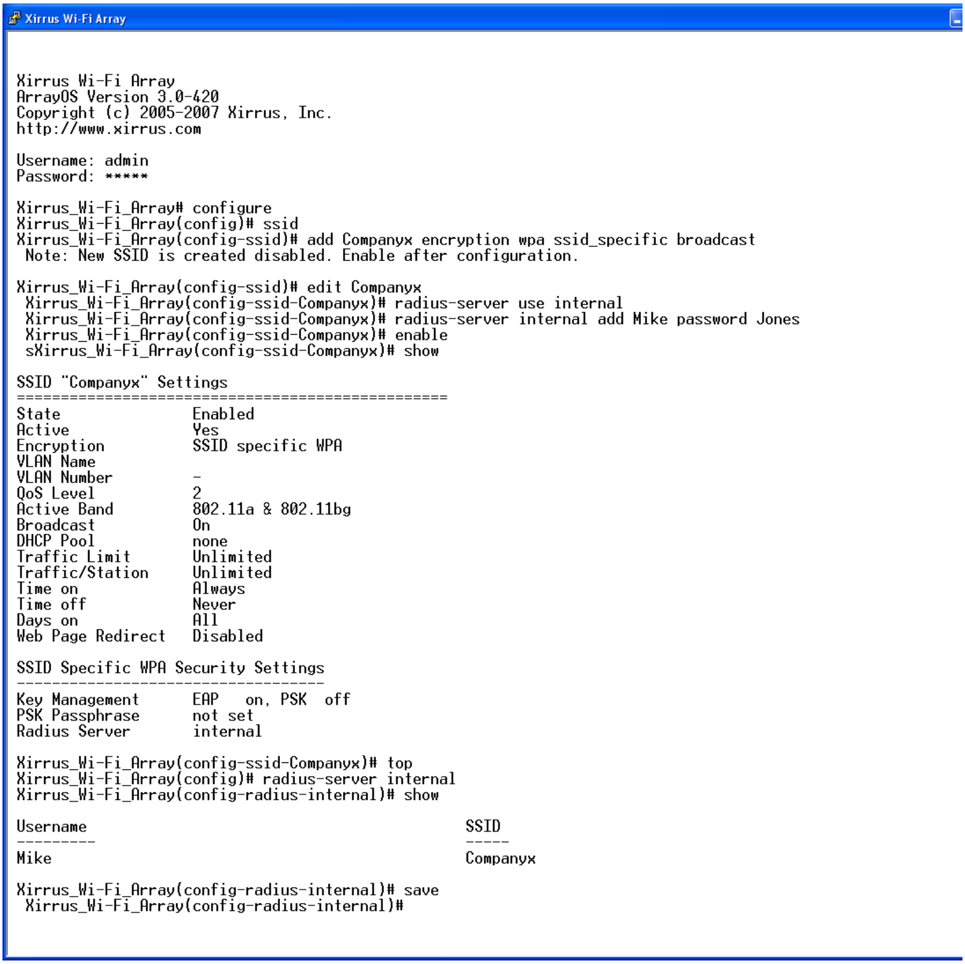


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 190. 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.

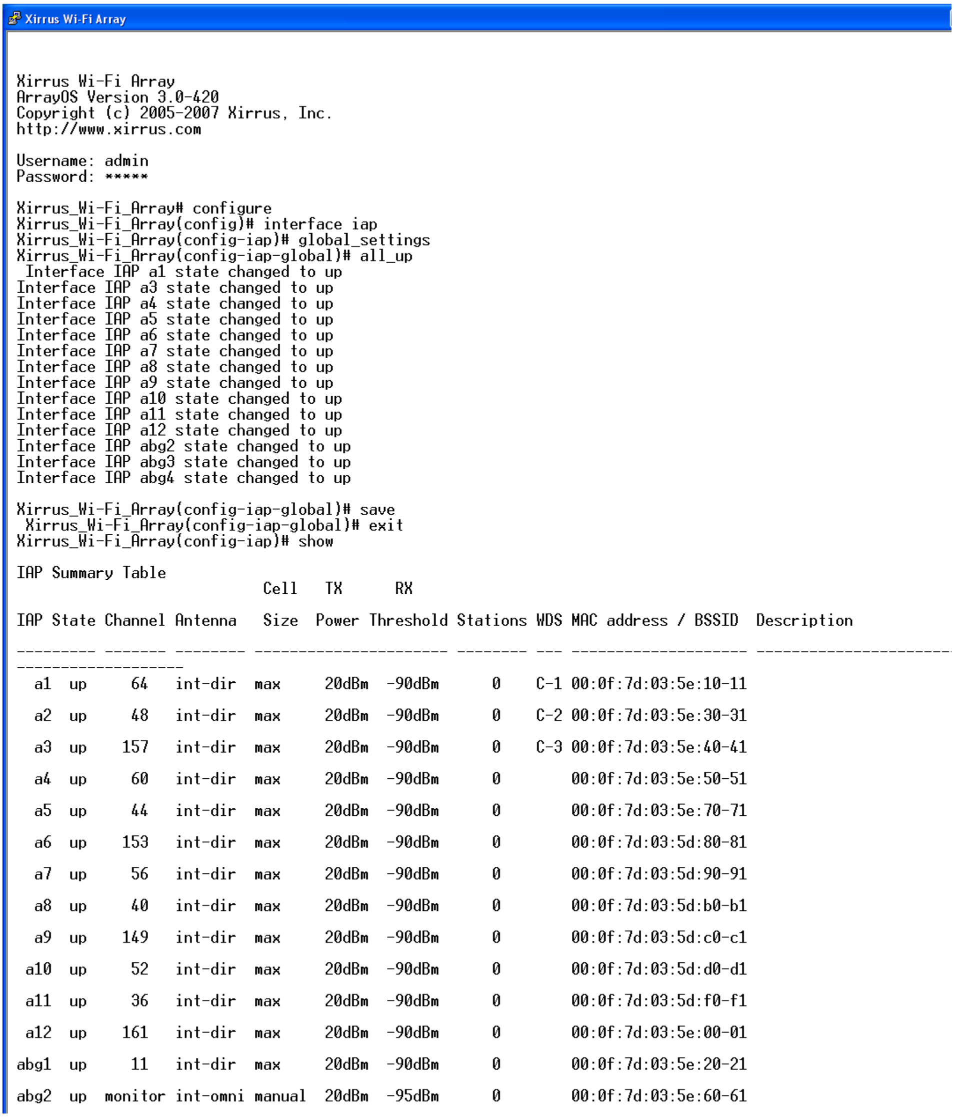


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 191. 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.

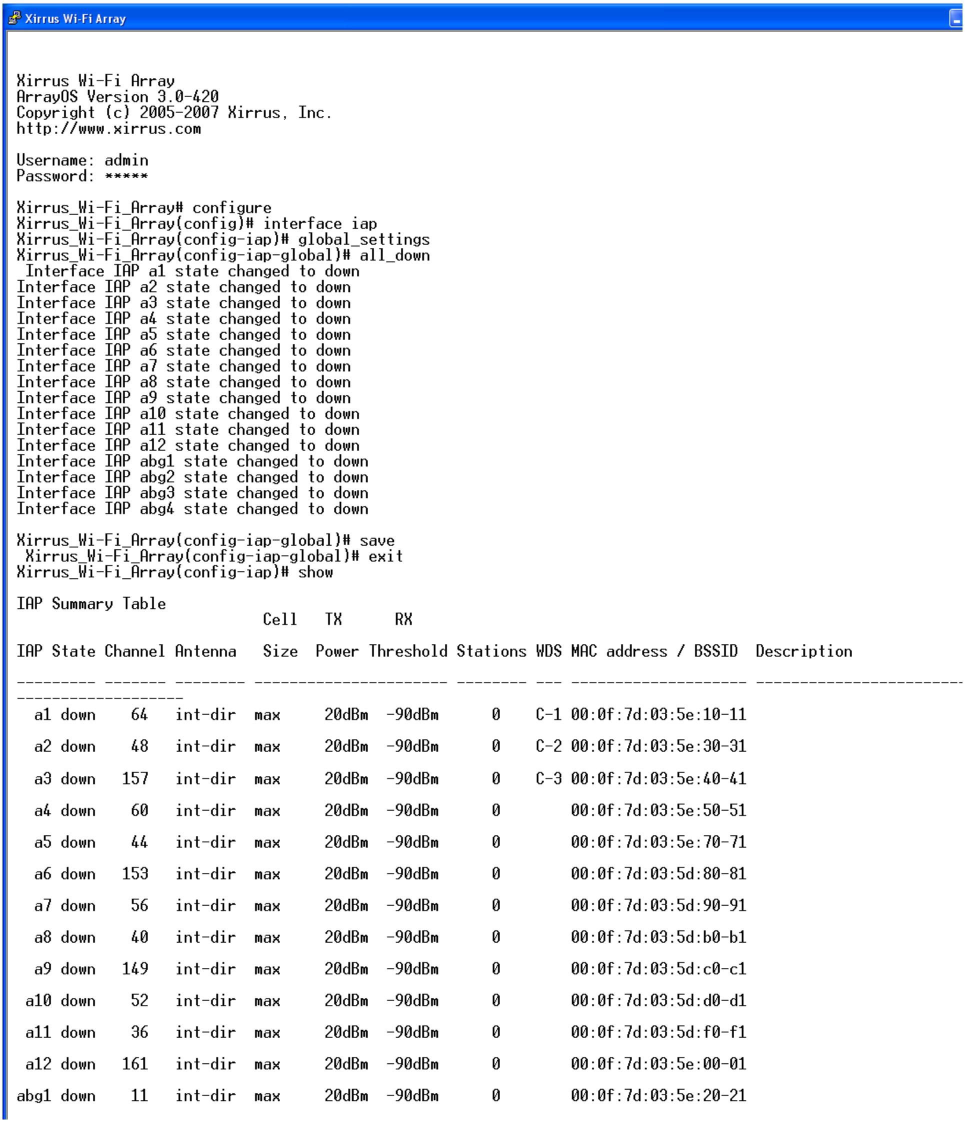


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 192. Enabling Global IAPs

Disabling Global IAPs

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

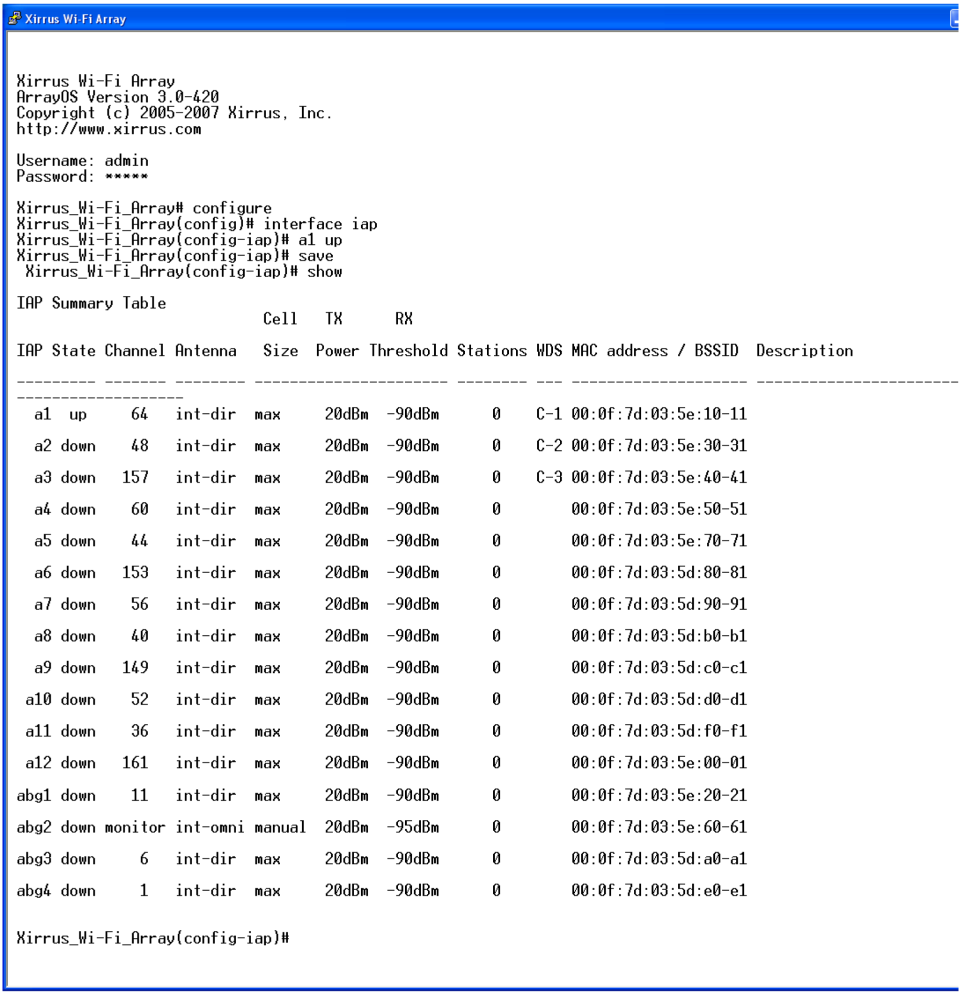


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 193. 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).

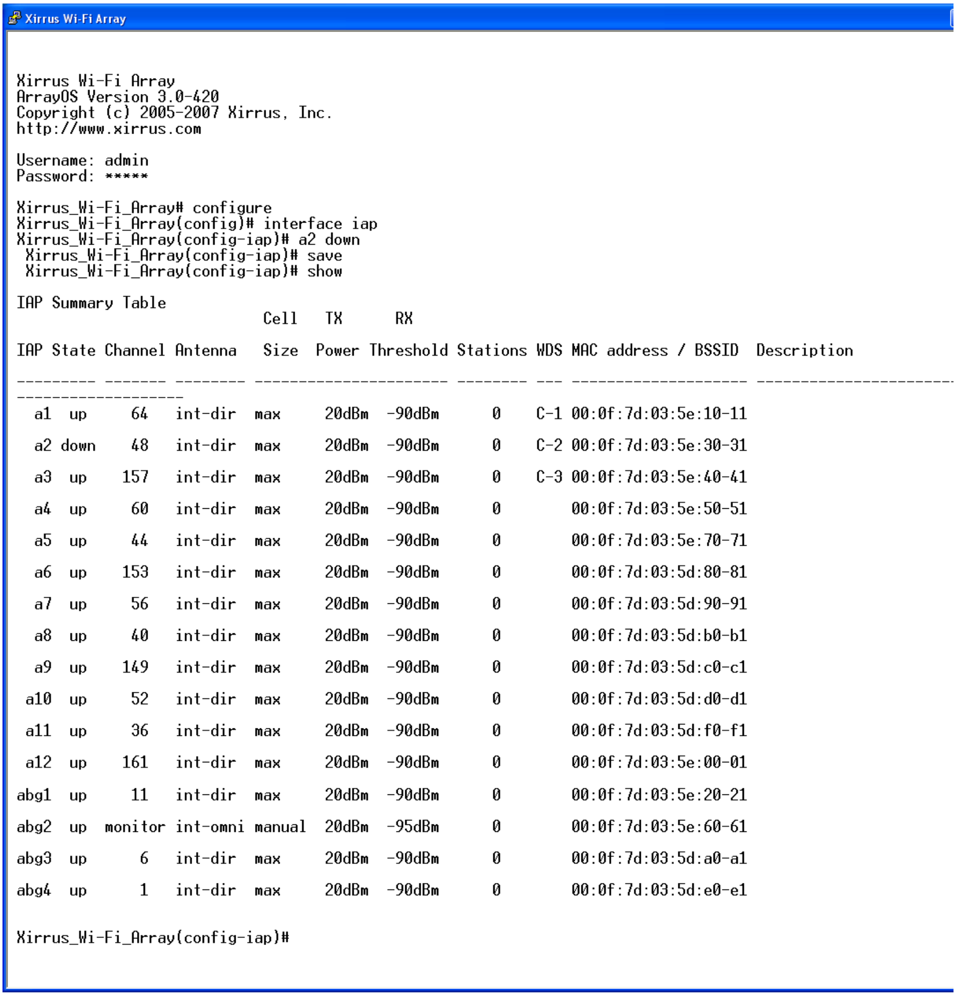


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 194. 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).



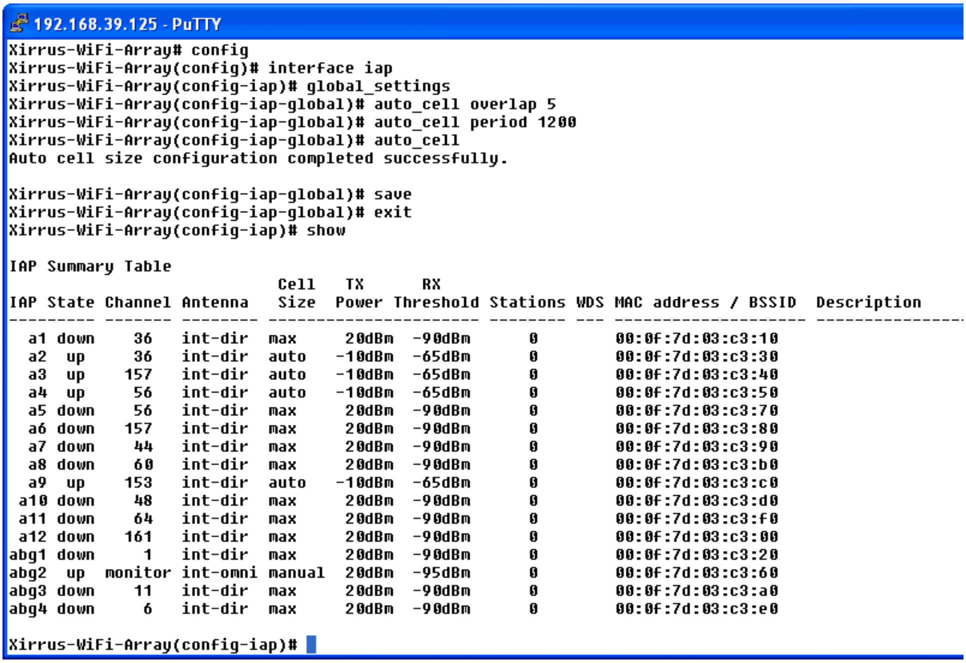
```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 195. 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 31.) 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 the **monitor** radio, 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.



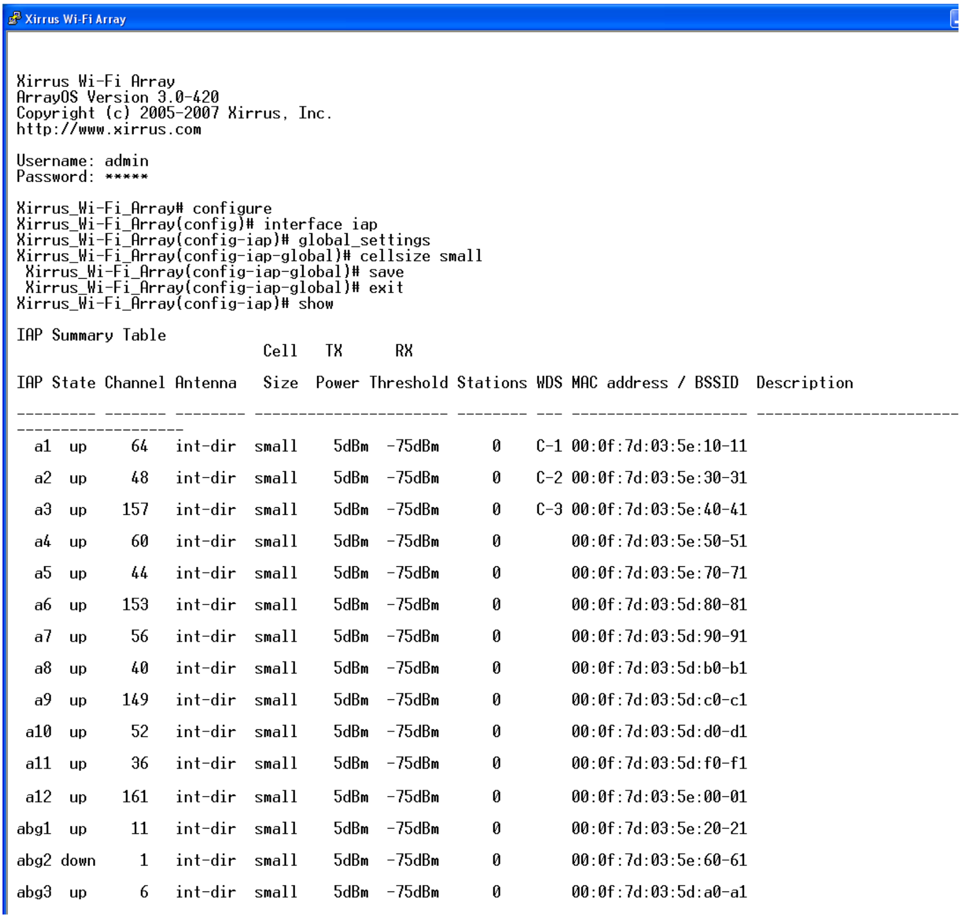
```
Xirrus-WiFi-Array# config
Xirrus-WiFi-Array(config)# interface iap
Xirrus-WiFi-Array(config-iap)# global_settings
Xirrus-WiFi-Array(config-iap-global)# auto_cell overlap 5
Xirrus-WiFi-Array(config-iap-global)# auto_cell period 1200
Xirrus-WiFi-Array(config-iap-global)# auto_cell
Auto cell size configuration 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 196. 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 the monitor radio the cell size cannot be set globally—you must first disable the intrude-detect feature on the monitor radio.

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 31.

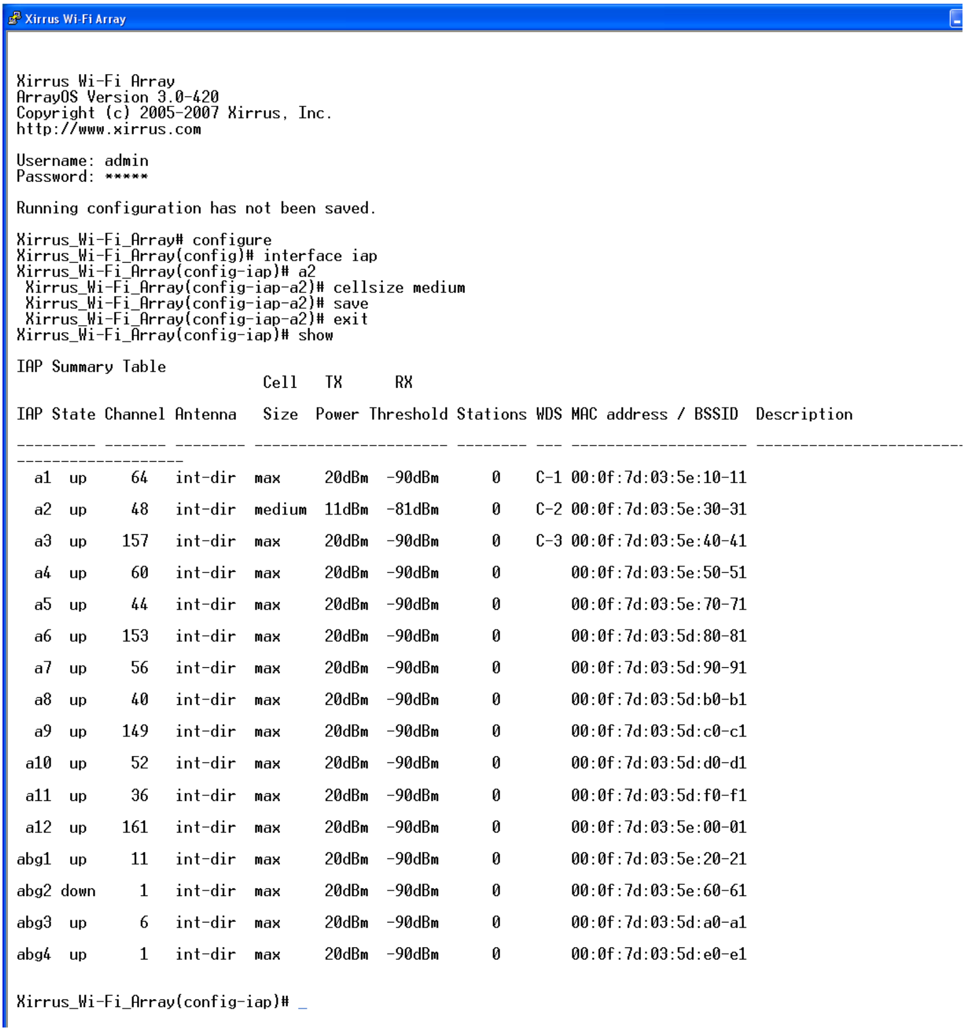


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 197. 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 31.

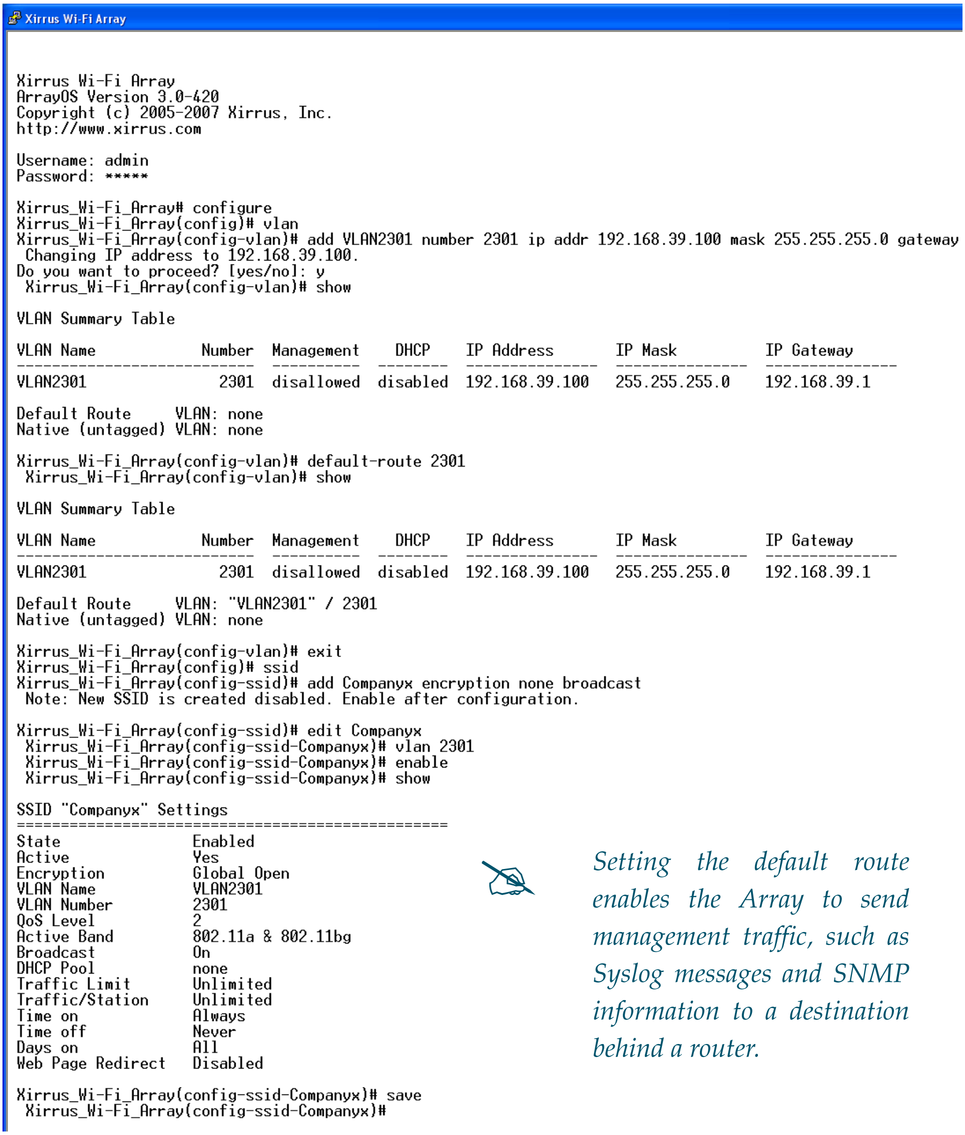


```
Xirrus Wi-Fi Array
ArrayOS Version 3.0-420
Copyright (c) 2005-2007 Xirrus, Inc.
http://www.xirrus.com

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 198. 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 199. Configuring VLANs on an Open SSID

Configuring Radio Assurance Mode (Loopback Tests)

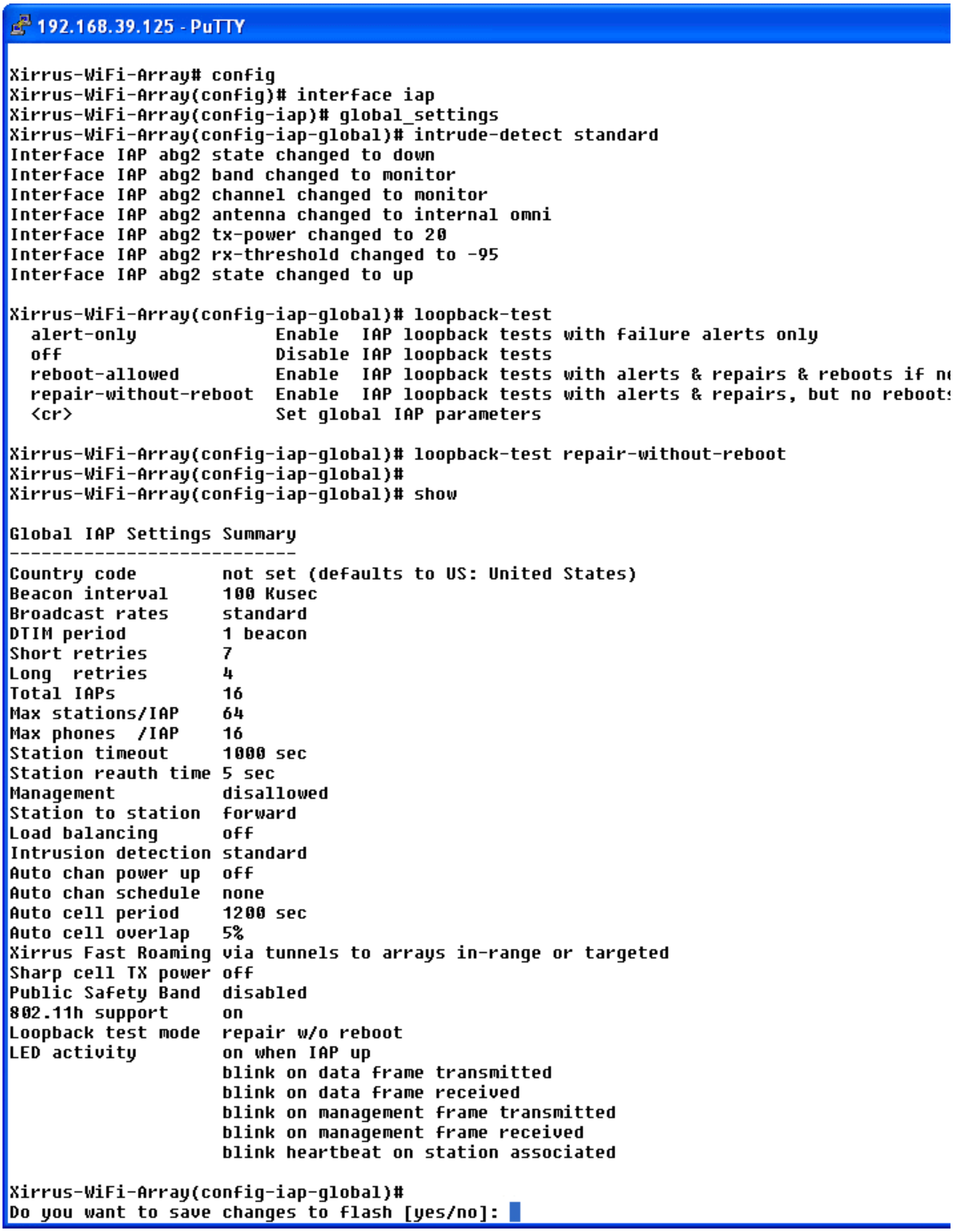
The Array uses its built-in monitor radio to monitor other radios in the Array. Tests include sending probes on all channels and checking for a response, and checking whether beacons are received from the other radio. If a problem is detected, corrective actions are taken to recover. Loopback mode operation is described in detail in "Array Monitor and Radio Assurance Capabilities" on page 460.

The following actions may be configured:

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

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

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



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

Xirrus-WiFi-Array(config-iap-global)# loopback-test
  alert-only              Enable  IAP loopback tests with failure alerts only
  off                     Disable IAP loopback tests
  reboot-allowed          Enable  IAP loopback tests with alerts & repairs & reboots if n
  repair-without-reboot   Enable  IAP loopback tests with alerts & repairs, but no reboot
  <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 200. Configuring Radio Assurance Mode (Loopback Testing)

Appendices

Page is intentionally blank

Appendix A: 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 443**.
- **"Keyboard Shortcuts" on page 449**.

Factory Default Settings

The following tables show the Wireless Array's factory default settings.

Host Name

Setting	Default Value
Host name	Xirrus-WiFi-Array

Network Interfaces

Serial

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

Gigabit 1 and Gigabit 2

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.2.1
Default IP Mask	255.255.255.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1500
Management Enabled	Yes

Server Settings

NTP

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

Syslog

Setting	Default Value
Enabled	Yes

Setting	Default Value
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
IP Start Range	192.168.1.2
IP End Range	192.168.1.254

Setting	Default Value
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)
WEP Key Length	null (all 4 keys)
Default Key ID	1

Setting	Default Value
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
Primary Server	None
Primary Port	1813

Setting	Default Value
Primary Secret	null (no secret)
Secondary Server	None
Secondary Port	1813
Secondary Secret	null (no secret)

Internal RADIUS

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

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
SSH	On
SSH timeout	300 seconds
Telnet	Off
Telnet timeout	300 seconds

Setting	Default Value
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 B: 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 Wireless 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 Wireless Arrays.

- The Wireless 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 Wireless 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 you are deploying multiple units, the Array should be oriented so that the monitor **abgn2** radio is oriented in the direction of the least required coverage, because when in monitor mode the radio does not function as an AP servicing stations.

- The Wireless 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 Wireless 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 242.

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

8. 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. The Array only allows SSH-2 connections, so your SSH utility must be set up to use SSH-2.

- Configuration auditing
  Do not change approved configuration settings. The optional Xirrus Management System (XMS) offers powerful management features for small or large Wireless 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 Wireless 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).

TKIP encryption does not support high throughput rates, per the IEEE 802.11n.

TKIP should never be used for WDS links on XN arrays.

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 Wireless 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 Wireless 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 Wireless 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 Wireless Array units?**

A. When deploying multiple Wireless 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 Wireless Array has integrated monitor capabilities, which can constantly scan 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 Wireless 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 unable to access other privileged network resources.

See Also

Array Monitor and Radio Assurance Capabilities

All models of the Wireless Array have integrated monitoring capabilities to check that the Array's radios are functioning correctly, and act as a threat sensor to detect and prevent intrusion from rogue access points.

Enabling Monitoring on the Array

Any radio IAP abgn2 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 one monitor radio 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 274 for more details. The values above are the factory default settings for the Array.

How Monitoring Works

When the monitor radio 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 313.

Radio Assurance

The Array is capable of performing continuous, comprehensive tests on its radios to assure that they are operating properly. Testing is enabled using the **Radio Assurance Mode** setting on the Advanced RF Settings window (Step 2 in "Advanced RF Settings" on page 313). When this mode is enabled, the monitor radio performs loopback tests on the Array. Radio Assurance Mode requires **Intrusion Detection** to be set to **Standard** (See Step 1 in "Advanced RF Settings" on page 313).

When **Radio Assurance Mode** is enabled:

1. The Array keeps track of whether or not it hears beacons and probe responses from the Array's radios.
2. After 10 minutes (roughly 60 passes on a particular channel by the monitor radio), if it has not heard beacons or probe responses from one of the Array's radios it issues an alert in the Syslog. If repair is allowed (see "Radio Assurance Options" on page 462), the Array will reset and reprogram that particular radio at the Physical Layer (PHY—Layer 1). This action takes under 100ms and stations are not deauthenticated, thus users should not be impacted.
3. After another 10 minutes (roughly another 60 passes), if the monitor still has not heard beacons or probe responses from the malfunctioning radio it will again issue an alert in the Syslog. If repair is allowed, the Array will reset and reprogram the MAC (the lower sublayer of the Data Link Layer) and then all of the PHYs. This is a global action that affects all radios. This action takes roughly 300ms and stations are not deauthenticated, thus users should not be impacted.
4. After another 10 minutes, if the monitor still has not heard beacons or probe responses from that radio, it will again syslog the issue. If reboot is allowed (see "Radio Assurance Options" on page 462), the Array will schedule a reboot. This reboot will occur at one of the following times, whichever occurs first:
   - When no stations are associated to the Array
   - Midnight

Radio Assurance Options

If the monitor detects a problem with an Array radio as described above, it will take action according to the preference that you have specified in the **Radio Assurance Mode** setting on the Advanced RF Settings window (see Step 2 page 315):

- **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.

RADIUS Vendor Specific Attribute (VSA) for Xirrus

A RADIUS VSA is defined for Xirrus Arrays to control administrator privileges settings for user accounts. The RADIUS VSA is used by Arrays to define the following attribute for administrator accounts:

- **Array administrators**—the **Xirrus-Admin-Role** attribute sets the privilege level for this account. Set the value to the string defined in **Privilege Level Name** as described in "About Creating Admin Accounts on the RADIUS Server" on page 218.

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-5.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 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 Thousand Oaks, California, just 55 minutes northwest of downtown Los Angeles and 40 minutes southeast of Santa Barbara.

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

Tel:	1.805.262.1600
	1.800.947.7871 Toll Free in the US
Fax:	1.866.462.3980

www.xirrus.com
support.xirrus.com

Appendix C: Notices

This appendix contains the following information:

Notices

Wi-Fi Alliance Certification

www.wi-fi.org

FCC Notice

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

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced wireless technician for help.

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

! ***FCC Caution:*** *Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.*

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LE-LAN devices.

Non-Modification Statement

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

Cable Runs for Power over Gigabit Ethernet (PoGE)

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

Battery Warning

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

UL Statement

Use only with listed ITE product.

RF Radiation Hazard Warning

To ensure compliance with FCC and Industry Canada RF exposure requirements, this device must be installed in a location where the antennas of the device will have a minimum distance of at least 30 cm (12 inches) from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Installez l'appareil en veillant à conserver une distance d'au moins 30 cm entre les éléments rayonnants et les personnes. Cet avertissement de sécurité est conforme aux limites d'exposition définies par la norme CNR-102 at relative aux fréquences radio.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution :

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250-5 350 MHz et 5 650-5 850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

High Power Radars

High power radars are allocated as primary users (meaning they have priority) in the 5250MHz to 5350MHz and 5650MHz to 5850MHz bands. These radars could cause interference and/or damage to LELAN devices used in Canada.

Les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5 250 - 5 350 MHz et 5 650 - 5 850 MHz. Ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

EU Directive 1999/5/EC Compliance Information

This section contains compliance information for the Xirrus Wireless Array family of products. The compliance information contained in this section is relevant to the European Union and other countries that have implemented the EU Directive 1999/5/EC.

Declaration of Conformity

Cesky [Czech] Toto zahzeni je v souladu se základnimi požadavky a ostatnimi odpovidajcimi ustano veni mi Směrnice 1999/5/EC.

Dansk [Danish] Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.

Deutsch [German] Dieses Gerat entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtinie 1999/5/EU.

Eesti [Estonian] See seande vastab direktiivi 1999/5/EU olulistele nöuetele ja teistele as jakohastele sätetele.

English This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spain] Este equipo cump le con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.

Ελληνυκη [Greek] Αυτόζ ο εξοπλτσμόζ είναι σε συμμόρφωση με τιζ ουσιώδειζ απαιτήσειζ και ύλλεζ σχετικέζ διατάξειζ τηζ Οδηγιαζ 1999/5/EC.

Français [French] Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.

Íslenska [Icelandic] Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.

Italiano [Italian] Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.

Latviski [Latvian] Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajā prasībām un citiem ar to saistītajiem noteikumiem.

Lietuvių [Lithuanian] Šis įrenginys tenkina 1995/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Nederlands [Dutch] Dit apparant voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1995/5/EC.

Malti [Maltese] Dan l-apparant huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.

Margyar [Hungarian] Ez a készülék teljesiti az alapvetö követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.

Norsk [Norwegian] Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.

Polski [Polish] Urządzenie jest zgodne z ogólnymi wymaganiami oraz sczególnymi mi warunkami określony mi Dyrektywą. UE:1999/5/EC.

Portuguès [Portuguese] Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.

Slovensko [Slovenian] Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi popoji Direktive 1999/5/EC.

Slovensky [Slovak] Toto zariadenie je v zhode so základnými požadavkami a inými prislušnými nariadeniami direktiv: 1999/5/EC.

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

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

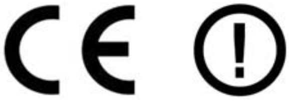
Assessment Criteria

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

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

CE Marking

For the Xirrus Wireless Array, the CE mark and Class-2 identifier opposite are affixed to the equipment and its packaging:



WEEE Compliance

Waste
Electrical and
Electronic
Equipment
(WEEE)

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

National Restrictions

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

Frequency Band (MHz)	Max Power Level (EIRP) (mW)	Indoor	Outdoor
2400–2483.5	100	X	X**
5250–5350*	200	X	N/A
5470–5725*	1000	X	X

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

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

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

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

Belgium

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

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

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

Greece

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

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

Italy

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

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

Norway, Switzerland and Liechtenstein

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

Calculating the Maximum Output Power

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

Antennas

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

Operating Frequency

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

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

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

Tel: 1.805.262.1600
1.800.947.7871 Toll Free in the US
Fax: 1.866.462.3980

www.xirrus.com

Compliance Information (Non-EU)

This section contains compliance information for the Xirrus Wireless Array family of products. The compliance information contained in this section is relevant to the listed countries (outside of the European Union and other countries that have implemented the EU Directive 1999/5/EC).

Declaration of Conformity

Mexico	XN16: Cofetel Cert #: RCPXIXN10-1052 XN12: Cofetel Cert #: RCPXIXN10-1052-A1 XN8: Cofetel Cert #: RCPXIXN10-1052-A2 XN4: Cofetel Cert #: RCPXIXN10-1052-A3
Thailand	This telecommunication equipment conforms to NTC technical requirement.

Safety Warnings

Safety Warnings

Read all user documentation before powering this device. All Xirrus interconnected equipment should be contained indoors. This product is not suitable for outdoor operation. Please verify the integrity of the system ground prior to installing Xirrus equipment. Additionally, verify that the ambient operating temperature does not exceed 40°C.

Explosive Device Proximity Warning

Do not operate the XR Series Wireless Array near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

Lightning Activity Warning

Do not work on the XR Series Wireless Array or connect or disconnect cables during periods of lightning activity.

Circuit Breaker Warning

The XR Series Wireless Array relies on the building's installation for over current protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A (U.S.) or 240 VAC, 10A (International) is used on all current-carrying conductors.

Translated safety warnings appear on the following page.

Translated Safety Warnings

Avertissements de Sécurité

Sécurité

Lisez l'ensemble de la documentation utilisateur avant de mettre cet appareil sous tension. Tous les équipements Xirrus interconnectés doivent être installés en intérieur. Ce produit n'est pas conçu pour être utilisé en extérieur. Veuillez vérifier l'intégrité de la terre du système avant d'installer des équipements Xirrus. Vérifiez également que la température de fonctionnement ambiante n'excède pas 40°C.

Proximité d'appareils explosifs

N'utilisez pas l'unité XR Wireless Array à proximité d'amorces non blindées ou dans un environnement explosif, à moins que l'appareil n'ait été spécifiquement modifié pour un tel usage.

Foudre

N'utilisez pas l'unité XR Wireless Array et ne branchez pas ou ne débranchez pas de câbles en cas de foudre.

Disjoncteur

L'unité XR Wireless Array dépend de l'installation du bâtiment pour ce qui est de la protection contre les surintensités. Assurez-vous qu'un fusible ou qu'un disjoncteur de 120 Vca, 15 A (États-Unis) ou de 240 Vca, 10 A (International) maximum est utilisé sur tous les conducteurs de courant.

Software License and Product Warranty Agreement

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

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

1.0 DEFINITIONS

1.1 "Documentation" means the user manuals and all other all documentation, instructions or other similar materials accompanying the Software covering the installation, application, and use thereof.

1.2 "Licensor" means XIRRUS and its suppliers.

1.3 "Product" means a multi-radio access point containing four or more distinct radios capable of simultaneous operation on four or more non-overlapping channels.

1.4 "Software" means, collectively, each of the application and embedded software programs delivered to Customer in connection with this Agreement. For purposes of this Agreement, the term Software shall be deemed to include any and all Documentation and Updates provided with or for the Software.

1.5 "Updates" means any bug-fix, maintenance or version release to the Software that may be provided to Customer from Licensor pursuant to this Agreement or pursuant to any separate maintenance and support agreement entered into by and between Licensor and Customer.

2.0 GRANT OF RIGHTS

2.1 Software. Subject to the terms and conditions of this Agreement, Licensor hereby grants to Customer a perpetual, non-exclusive, non-sublicenseable, non-transferable right and license to use the Software solely as installed on the Product in accordance with the accompanying Documentation and for no other purpose.

2.2 Ownership. The license granted under Sections 2.1 above with respect to the Software does not constitute a transfer or sale of Licensor's or its suppliers' ownership interest in or to the Software, which is solely licensed to Customer. The Software is protected by both national and international intellectual property laws and treaties. Except for the express licenses granted to the Software, Licensor and its suppliers retain all rights, title and interest in and to the Software, including (i) any and all trade secrets, copyrights, patents and other proprietary rights therein or thereto or (ii) any Marks (as defined in Section 2.3 below) used in connection therewith. In no event shall Customer remove, efface or otherwise obscure any Marks contained on or in the Software. All rights not expressly granted herein are reserved by Licensor.

2.3 Copies. Customer shall not make any copies of the Software but shall be permitted to make a reasonable number of copies of the related Documentation. Whenever Customer copies or reproduces all or any part of the Documentation, Customer shall reproduce all and not efface any titles, trademark symbols, copyright symbols and legends, and other proprietary markings or similar indicia of origin (“Marks”) on or in the Documentation.

2.4 Restrictions. Customer shall not itself, or through any parent, subsidiary, affiliate, agent or other third party (i) sell, rent, lease, license or sublicense, assign or otherwise transfer the Software, or any of Customer's rights and obligations under this Agreement except as expressly permitted herein; (ii) decompile, disassemble, or reverse engineer the Software, in whole or in part, provided that in those jurisdictions in which a total prohibition on any reverse engineering is prohibited as a matter of law and such prohibition is not cured by the fact that this Agreement is subject to the laws of the State of California, Licensor agrees to grant Customer, upon Customer's written request to Licensor, a limited reverse engineering license to permit interoperability of the Software with other software or code used by Customer; (iii) allow access to the Software by any user other than by Customer's employees and contractors who are bound in writing to confidentiality and non-use restrictions at least as protective as those set forth herein; (iv) except as expressly set forth herein, write or develop any derivative software or any other software program based upon the Software; (v) use any computer software or hardware which is designated to defeat any copy protection or other use limiting device, including any device intended to limit the number of users or devices accessing the Product; (vi) disclose information about the performance or operation of the Product or Software to any third party without the prior written consent of Licensor; or (vii) engage a third party to perform benchmark or functionality testing of the Product or Software.

3.0 LIMITED WARRANTY AND LIMITATION OF LIABILITY

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

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

3.3 HAZARDOUS APPLICATIONS. THE SOFTWARE IS NOT DESIGNED OR INTENDED FOR USE IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF A NUCLEAR FACILITY, AIRCRAFT NAVIGATION OR COMMUNICATIONS SYSTEMS, AIR TRAFFIC CONTROLS OR OTHER DEVICES OR SYSTEMS IN WHICH A MALFUNCTION OF THE SOFTWARE WOULD RESULT IN FORSEEABLE RISK OF INJURY OR DEATH TO THE OPERATOR OF THE DEVICE OR SYSTEM OR TO OTHERS ("HAZARDOUS APPLICATIONS"). CUSTOMER ASSUMES ANY AND ALL RISKS, INJURIES, LOSSES, CLAIMS AND ANY OTHER LIABILITIES ARISING OUT OF THE USE OF THE SOFTWARE IN ANY HAZARDOUS APPLICATIONS.

3.4 Limitation of Liability.

(a) TOTAL LIABILITY. NOTWITHSTANDING ANYTHING ELSE HEREIN, ALL LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS AGREEMENT SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMER FOR THE RELEVANT SOFTWARE, OR PORTION THEREOF, THAT GAVE RISE TO SUCH LIABILITY OR ONE HUNDRED UNITED STATES DOLLARS (US$100), WHICHEVER IS GREATER. THE LIABILITY OF LICENSOR AND ITS SUPPLIERS UNDER THIS SECTION SHALL BE CUMULATIVE AND NOT PER INCIDENT.

(b) DAMAGES. IN NO EVENT SHALL LICENSOR, ITS SUPPLIERS OR THEIR RELEVANT SUBCONTRACTORS BE LIABLE FOR (A) ANY INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST PROFITS OR LOST OR DAMAGED DATA, OR ANY INDIRECT DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY) OR OTHERWISE OR (B) ANY COSTS OR EXPENSES FOR THE PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES IN EACH CASE, EVEN IF LICENSOR OR ITS SUPPLIERS HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES.

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

4.0 CONFIDENTIAL INFORMATION

4.1 Generally. The Software (and its accompanying Documentation) constitutes Licensor's and its suppliers' proprietary and confidential information and contains valuable trade secrets of Licensor and its suppliers (“Confidential Information”). Customer shall protect the secrecy of the Confidential Information to the same extent it protects its other valuable, proprietary and confidential information of a similar nature but in no event shall Customer use less than reasonable care to maintain the secrecy of the Confidential Information. Customer shall not use the Confidential Information except to exercise its rights or perform its obligations as set forth under this Agreement. Customer shall not disclose such Confidential Information to any third party other than subject to non-use and non-disclosure obligations at least as protective of a party's right in such Confidential Information as those set forth herein.

4.2 Return of Materials. Customer agrees to (i) destroy all Confidential Information (including deleting any and all copies contained on any of Customer's Designated Hardware or the Product) within fifteen (15) days of the date of termination of this Agreement or (ii) if requested by Licensor, return, any Confidential Information to Licensor within thirty (30) days of Licensor's written request.

5.0 TERM AND TERMINATION

5.1 Term. Subject to Section 5.2 below, this Agreement will take effect on the Effective Date and will remain in force until terminated in accordance with this Agreement.

5.2 Termination Events. This Agreement may be terminated immediately upon written notice by either party under any of the following conditions:

(a) If the other party has failed to cure a breach of any material term or condition under the Agreement within thirty (30) days after receipt of notice from the other party; or

(b) Either party ceases to carry on business as a going concern, either party becomes the object of the institution of voluntary or involuntary proceedings in bankruptcy or liquidation, which proceeding is not dismissed within ninety (90) days, or a receiver is appointed with respect to a substantial part of its assets.

5.3 Effect of Termination.

(a) Upon termination of this Agreement, in whole or in part, Customer shall pay Licensor for all amounts owed up to the effective date of termination. Termination of this Agreement shall not constitute a waiver for any amounts due.

(b) The following Sections shall survive the termination of this Agreement for any reason: Sections 1, 2.2, 2.4, 3, 4, 5.3, and 6.

(c) No later than thirty (30) days after the date of termination of this Agreement by Licensor, Customer shall upon Licensor's instructions either return the Software and all copies thereof; all Documentation relating thereto in its possession that is in tangible form or destroy the same (including any copies thereof contained on Customer's Designated Hardware). Customer shall furnish Licensor with a certificate signed by an executive officer of Customer verifying that the same has been done.

6. MISCELLANEOUS

If Customer is a corporation, partnership or similar entity, then the license to the Software and Documentation that is granted under this Agreement is expressly conditioned upon and Customer represents and warrants to Licensor that the person accepting the terms of this Agreement is authorized to bind such entity to the terms and conditions herein. If any provision of this Agreement is held to be invalid or unenforceable, it will be enforced to the extent permissible and the remainder of this Agreement will remain in full force and effect. During the course of use of the Software, Licensor may collect information on your use thereof; you hereby authorize Licensor to use such information to improve its products and services, and to disclose the same to third parties provided it does not contain any personally identifiable information. The express waiver by either party of any provision, condition or requirement of this Agreement does not constitute a waiver of any future obligation to comply with such provision, condition or requirement. Customer and Licensor are independent parties. Customer may not export or re-export the Software or Documentation (or other materials) without appropriate United States, European Union and foreign government licenses or in violation of the United State's Export Administration Act or foreign equivalents and Customer shall comply with all national and international laws governing the Software. This Agreement will be governed by and construed under the laws of the State of California and the United States as applied to agreements entered into and to be performed entirely within California, without regard to conflicts of laws provisions thereof and the parties expressly exclude the application of the United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer Information Transactions Act (as promulgated by any State) to this Agreement. Suits or enforcement actions must be brought within, and each party irrevocably commits to the exclusive jurisdiction of, the state and federal courts located in Ventura County, California. Customer may not assign this Agreement by operation of law or otherwise, without the prior written consent of Licensor and any attempted assignment in violation of the foregoing shall be null and void. This Agreement cancels and supersedes all prior agreements between the parties. This Agreement may not be varied except through a document agreed to and signed by both parties. Any printed terms and conditions contained in any Customer purchase order or in any Licensor acknowledgment, invoice or other documentation relating to the Software shall be deemed deleted and of no force or effect and any additional typed and/or written terms and conditions contained shall be for administrative purposes only, i.e. to identify the types and quantities of Software to be supplied, line item prices and total price, delivery schedule, and other similar ordering data, all in accordance with the provisions of this Agreement.

Hardware Warranty Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT

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

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

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

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

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

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

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

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

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

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

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

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

Glossary of Terms

802.11a

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

802.11b

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

802.11d

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

802.11g

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

802.11n

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

802.1Q

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

AES

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

authentication

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

bandwidth

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

beacon interval

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

bit rate

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

BSS

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

BSSID

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

CDP

(Cisco Discovery Protocol) CDP is a layer 2 network protocol which runs on most Cisco equipment and some other network equipment. It is used to share information with other directly connected network devices. Information such as the model, network capabilities, and IP address is shared. Wireless 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).

CoS

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

default gateway

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

DHCP

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

DHCP lease

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

DNS

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

domain

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

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

DTIM

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

EAP

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

EDCF

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

encapsulation

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

encryption

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

Fast Ethernet

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

FCC

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

FIPS

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

frame

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

Gigabit 1 through 4

The Gigabit Ethernet interfaces on XR Series Arrays. XR-4000 Series Arrays have two gigabit interfaces, while XR-6000 Series and higher models have four gigabit interfaces. See also, Gigabit Ethernet.

Gigabit Ethernet

A 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-supplied 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.

preamble

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

private key

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

PSK

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

public key

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

QoS

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

RADIUS

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

RSSI

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

SDMA

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

SNMP

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

SNTP

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

SSH

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

SSID

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

subnet mask

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

TKIP

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

transmit power

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

User group

See Group.

VLAN

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

VLAN tagging

(Virtual LAN tagging) Static port-based VLANs were originally the only way to segment a network without using routing, but these port-based VLANs could only be implemented on a single switch (or switches) cabled together. Routing was required to transfer traffic between unconnected switches. As an alternative to routing, some vendors created proprietary schemes for sharing VLAN information across switches. These methods would only operate on that vendor's equipment and were not an acceptable way to implement VLANs. With the adoption of the 802.11n standard, traffic can be confined to VLANs that exist on multiple switches from different vendors. This interoperability and traffic containment across different switches is the result of a switch's ability to use and recognize 802.1Q tag headers—called VLAN tagging. Switches that implement 802.1Q tagging add this tag header to the frame directly after the destination and source MAC addresses. The tag header indicates:

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

WDS (Wireless Distribution System)

WDS creates wireless 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.

Wireless Array

A high capacity wireless 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 Wireless 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-supplied products that provides power over Gigabit Ethernet. See PoGE.

Index

High Performance Wireless Networks

1.800.947.7871 Toll Free in the US
+1.805.262.1600 Sales
+1.805.262.1601 Fax
2101 Corporate Center Drive
Thousand Oaks, CA 91320, USA

To learn more visit:
xirrus.com or
email info@xirrus.com