

USAGE GUIDELINES

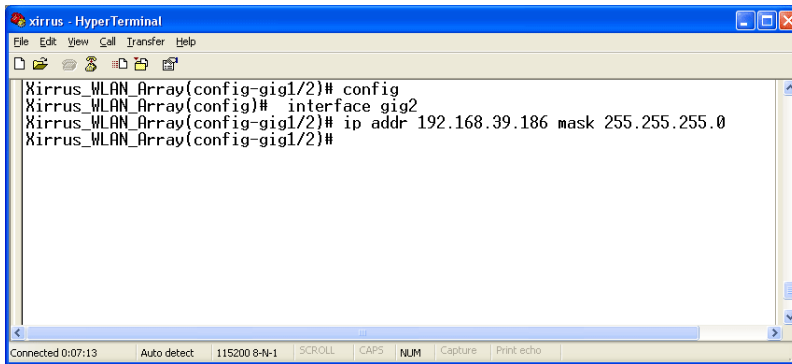
Setting Gigabit2 Interface parameters will automatically set the Gigabit1 parameters to the same values for failover purposes.

EXAMPLE

To set the IP address of the gigabit Ethernet interfaces:

```
config-interface gig2
```

```
((config-gig1/2)# ip addr 192.168.39.186 mask 255.255.255.0
```



```
xirrus - HyperTerminal
File Edit View Call Transfer Help
Xirrus_WLAN_Array(config-gig1/2)# config
Xirrus_WLAN_Array(config)# interface gig2
Xirrus_WLAN_Array(config-gig1/2)# ip addr 192.168.39.186 mask 255.255.255.0
Xirrus_WLAN_Array(config-gig1/2)#
```

Figure 101. CLI: Setting the IP Address for the Gigabit 2 Interface

SEE ALSO

```
config-interface gig1
```

```
config-interface eth0
```

hostname

DESCRIPTION

Sets the host name for this Array—available from the **config** command mode.

SYNTAX

hostname <hname> “hostname string”

PARAMETERS

None.

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

To set the hostname for the Xirrus Array:

```
(config)# hostname Xirrus_Array_3900
```

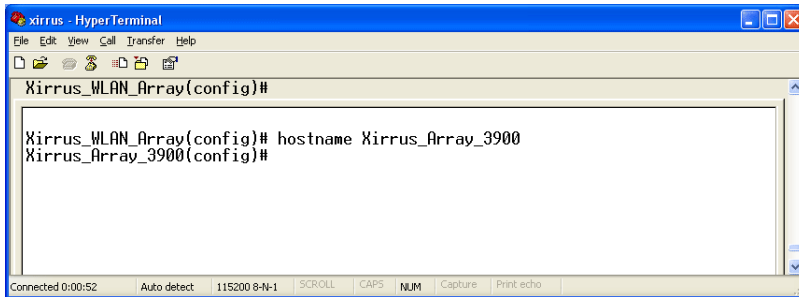


Figure 102. CLI: Setting the Host Name of the Array

The hostname is displayed immediately below the command line, as follows:

```
Xirrus_Array_3900(config)#
```

SEE ALSO

None.

iap

DESCRIPTION

Changes the configuration of a specific Integrated Access Point (IAP) radio interface—available from the **config-interface** command mode. Groups of interfaces can be accessed via the following interface commands.

- **iap number**: Configuration for a specific IAP. The prompt will change to: IAP number (config-iap-a12)#.
- **global_a_settings**: Common configuration for all 802.11a IAPs. The prompt will change to: (config-iap-global-a)#.
- **global_bg_settings**: Common configuration for all 802.11b/g IAPs. The prompt will change to: (config-iap-global-bg)#.
- **global_settings**: Common configuration for all IAPs. The prompt will change to: (config-iap-global)#.

SYNTAX

```
interface iap <IAP number> {channel <cnum> | description <dot11desc> |
down | up | cellsize {small | medium | large} | rx-threshold <thresrx> |
tx-power <powertx>} }
```

PARAMETERS

cellsize	Cell size setting
channel	Channel number
description	Name to identify this IAP (up to 32 characters)
down	Shut down (disable) this IAP
rx-threshold	Deferred threshold (receive sensitivity)
tx-power	Maximum transmit power
up	Bring up (enable) this IAP
dot11a	Set 802.11a mode
dot11bg	Set 802.11b/g mode (<i>only available on abg1, 2, 3, 4</i>)
antenna	Select the antenna for the IAP
<i>internal</i>	Internal directional 2.4GHz antenna

<i>monitor</i>	Internal omni-directional monitor antenna (available on <i>abg2</i> IAP only)
<i>external</i>	Select the external antenna (Available on IAP <i>abg1</i> , <i>abg3</i> , and <i>abg4</i> only)

DEFAULTS

None.

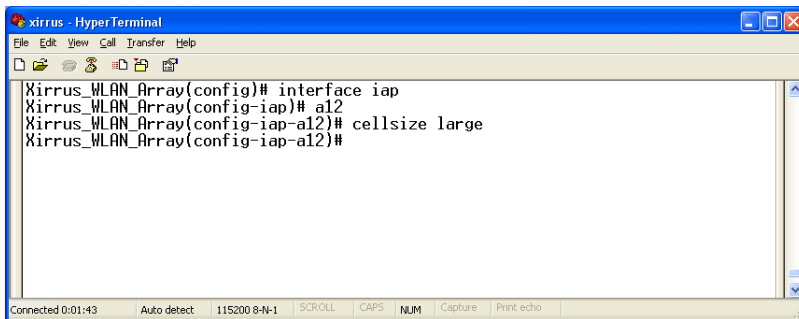
USAGE GUIDELINES

None.

EXAMPLE

To set the cell size to large for the integrated access point a12:

```
(config-iap)# a12  
(config-iap-a12)# cellsize large
```



The screenshot shows a HyperTerminal window titled "xirrus - HyperTerminal". The window contains the following CLI commands and their outputs:

```
Xirrus_WLAN_Array(config)# interface iap  
Xirrus_WLAN_Array(config-iap)# a12  
Xirrus_WLAN_Array(config-iap-a12)# cellsize large  
Xirrus_WLAN_Array(config-iap-a12)#
```

The status bar at the bottom of the window shows: "Connected 0:01:43", "Auto detect", "115200 8-N-1", "SCROLL", "CAPS", "NUM", "Capture", and "Print echo".

Figure 103. CLI: Setting the Cell Size of an IAP

SEE ALSO

- `iap global_a_settings`
- `iap global_bg_settings`
- `iap global_settings`
- `show iap all`

iap global_settings

DESCRIPTION

Makes global configuration changes to all Integrated Access Point (IAP) radio interfaces—available from the **config-interface** command mode.

This command allows configuration changes to all IAP interfaces. Other global settings can be made for specific groups of IAPs by using one of the below parameters in the interface IAP command mode:

- **iap number**: Configuration for a specific IAP. The prompt will change to: IAP number (config-iap-a12)#
- **global_a_settings**: Common configuration for all 802.11a IAPs. The prompt will change to: (config-iap-global-a)#
- **global_bg_settings**: Common configuration for all 802.11b/g IAPs. The prompt will change to: (config-iap-global-bg)#
- **global_settings**: Common configuration for all IAPs. The prompt will change to: (config-iap-global)#

SYNTAX

```
iap global_settings {all_down | all_up | [no] rogue_detect [ on | off |
add <ssa> {approved | known} | del <ssid> | list ] | auto_channel
[no][power_up [ on | off ] | schedule [<ts>]] | long-retries <rlr> | short-
retries <sr> | cellsize {small | medium | large} | rx-threshold <thresrx> |
tx-power <powertx> | beacon-rate <brate> | beacon-dtim <bdtim> |
inactive-time <at> | reauth-period <ht> | led {disable | enable {iap_up |
associated}} | led_activity {beacon | tx_data | rx_data | tx_mgmt |
rx_mgmt | broadcast | probe_req | assoc}}
```

PARAMETERS

led	Enable or disable the IAP leds
<i>disable</i>	Do not turn IAP leds on
<i>enable</i>	Turn an IAP led on when up (default) or when a station is associated
<i>iap_up</i>	Turn an IAP led on when the IAP is up
<i>associated</i>	Turn an IAP led on when at least one station is associated with it

led_activity	Set IAP led behavior based on certain conditions
beacon	Blink an IAP led when a beacon is transmitted
tx_data	Blink an IAP led when a data frame is transmitted
rx_data	Blink an IAP led when a data frame is received
tx_mgmt	Blink an IAP led when a management frame is transmitted
rx_mgmt	Blink an IAP led when a management frame is received
broadcast	Blink an IAP led when a broadcast frame is transmitted
probe_req	Blink an IAP led when a probe request is received
assoc	Blink an IAP led heartbeat when stations are associated
beacon-rate	Time between beacons in kilo-microseconds (Kusec)
beacon-dtim	Beacons between Delivery Traffic Indication Messages (DTIM)
all_down	Shut down (disable) all IAPs
all_up	Bring up (enable) all IAPs
short-retries	Short retry limit
long-retries	Long retry limit
inactive-time	Time that an AP tracks an inactive station
reauth-period	Time between 802.1x re-authentication attempts
rogue_detect	Enable/disable rogue AP detection on IAP abg2
<i>on</i>	Enable rogue AP detection
<i>off</i>	Disable rogue AP detection
<i>add</i>	Add SSID to rogue database
<i>del</i>	Delete SSID from rogue database
<i>approved</i>	Mark SSID as approved (stop reporting and displaying)
<i>known</i>	Mark SSID as known (stop reporting but display with an *)
<i>list</i>	List rogue database
cellsize	Cell size setting
<i>small</i>	Small cell size
<i>medium</i>	Medium cell size
<i>large</i>	Large cell size
rx-threshold	Deferred threshold
tx-power	Maximum transmit power

auto_channel	Automatically assign channels to all IAPs
power_up	Automatically run automatic channel assignment at power up
schedule	Run automatic channel assignment at scheduled time(s)
on	Enable autochannel at power up
off	Disable autochannel at power up

DEFAULTS

None.

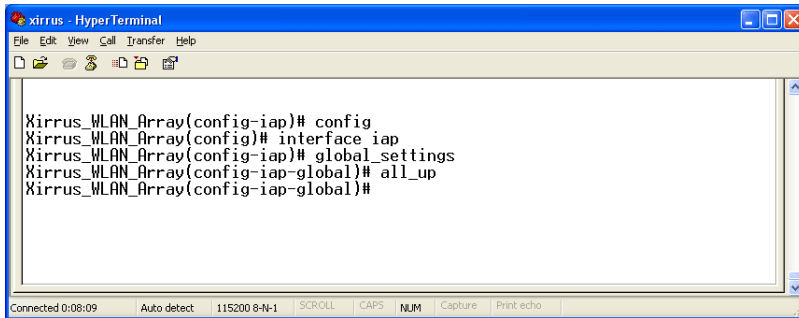
USAGE GUIDELINES

None.

EXAMPLE

To enable all the radio interfaces:

```
(config-iap)# global_settings  
(config-iap-global)# all_up
```



```
xirrus - HyperTerminal  
File Edit View Call Transfer Help  
Xirrus_WLAN_Array(config-iap)# config  
Xirrus_WLAN_Array(config)# interface iap  
Xirrus_WLAN_Array(config-iap)# global_settings  
Xirrus_WLAN_Array(config-iap-global)# all_up  
Xirrus_WLAN_Array(config-iap-global)#  
Connected 0:08:09 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print-echo
```

Figure 104. CLI: Enabling All Radio Interfaces

SEE ALSO

```
iap global_a_settings  
iap global_bg_settings  
iap global_settings  
show iap all
```

iap global_a_settings

DESCRIPTION

Makes global configuration changes to all 802.11a Integrated Access Point (IAP) radio interfaces—available from the **Config->Interface** command mode.

This command allows configuration changes to all 802.11a IAP interfaces. Other global settings can be made for specific groups of IAPs by using one of the following parameters in the interface IAP command mode:

- **iap number:** Configuration for a specific IAP. The prompt will change to: IAP number (config-iap-a12)#
- **global_bg_settings:** Common configuration for all 802.11b/g IAPs. The prompt will change to: (config-iap-global-bg)#
- **global_settings:** Common configuration for all IAPs. The prompt will change to: (config-iap-global)#

SYNTAX

```
iap global_a_settings {all_down | all_up | rts-threshold <rtst> | frag-
threshold <fragt> | auto_channel | cellsize {small | medium | large} | rx-
threshold <thresrx> | tx-power <powertx> | rates {defaults |
optimize_range | optimize_throughput | { basic { <br1> [<br2> [<br3>
<br4> [<br5> [<br6> [<br7> [<br8>]]]]]] | supported { [<sr1> [<sr2>
<sr3> [<sr4> [<sr5> [<sr6> [<sr7> [<sr8>]]]]]]]]}}
```

PARAMETERS

frag-threshold	802.11a fragmentation threshold packet size above which a packet will be fragmented
rts-threshold	802.11a RTS threshold packet size above which an RTS is issued before sending
auto_channel	Automatically assign channels to 802.11a IAPs
rates	Set allowed 802.11a data rates by listing the rates that will be used (6, 9, 12, 18, 24, 36, 48, 54, etc.)
<i>basic</i>	Set 802.11a basic (required) rates by listing the rates a client must support to associate
<i>supported</i>	Set the 802.11a supported (accepted) rates
<i>defaults</i>	Use the default 802.11a rates

<i>optimize_range</i>	Set 802.11a rates for the best range
<i>optimize_throughput</i>	Set 802.11a rates for the best throughput
all_down	Shut down (disable) all 802.11a IAPs
all_up	Bring up (enable) all 802.11a IAPs
cellsize	Cell size setting
<i>small</i>	Small cell size
<i>medium</i>	Medium cell size
<i>large</i>	Large cell size
rx-threshold	Deferred threshold, packets with a lower signal strength that the rx-threshold will be ignored
tx-power	Maximum transmit power in dB
parameter (-100,0) thresrx	Deferred threshold value
parameter (0,20) powertx	Maximum transmit value

DEFAULTS

None.

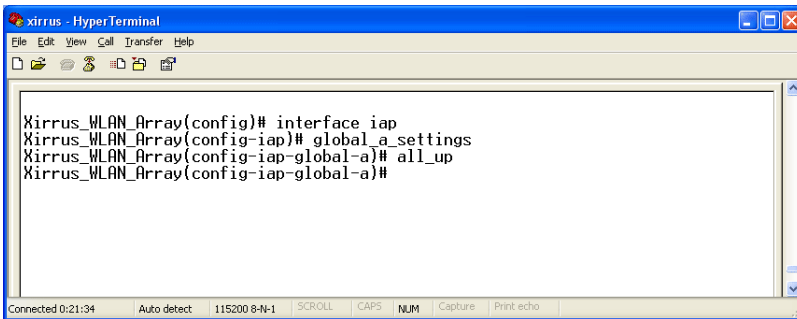
USAGE GUIDELINES

None.

EXAMPLE

To enable all 802.11a radio interfaces:

```
((config-iap)# global_a_settings
(config-iap-global-a)# all_up
```



```
xirrus - HyperTerminal
File Edit View Call Transfer Help
Xirrus_WLAN_Array(config)# interface iap
Xirrus_WLAN_Array(config-iap)# global_a_settings
Xirrus_WLAN_Array(config-iap-global-a)# all_up
Xirrus_WLAN_Array(config-iap-global-a)#
```

Connected 0:21:34 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print-echo

Figure 105. CLI: Enabling All 802.11a Radio Interfaces

SEE ALSO

```
iap global_bg_settings
iap global_settings
show iap all
```

iap global_bg_settings

DESCRIPTION

Makes global configuration changes to all 802.11bg Integrated Access Point (IAP) radio interfaces—available via the **Config-> Interface** command mode.

This command allows configuration changes to all 802.11bg IAP interfaces. Other global settings can be made for specific groups of IAPs by using one of the below parameters in the **Interface IAP** command mode::

- **iap number**: Configuration for a specific IAP. The prompt will change to: IAP number (config-iap-a12)#
- **global_bg_settings**: Common configuration for all 802.11b/g IAPs. The prompt will change to: (config-iap-global-bg)#
- **global_settings**: Common configuration for all IAPs. The prompt will change to: (config-iap-global)#

SYNTAX

```
IAPGlobalBG {all_down | all_up | slot_time {short_slot | long_slot} |
[no] dot11g_protect [on | off] | [no] dot11g_only [on | off] | cellsize {small
| medium | large} | rx-threshold <thresrx> | tx-power <powertx> |
preamble {short_preamble | long_preamble} | auto_channel |
rts-threshold <rtst> | frag-threshold <fragt> | rates {defaults |
optimize_range | optimize_throughput | { basic { <br1> [<br2> [<br3>
<br4> [<br5> [<br6> [<br7> [<br8> [<br9> [<br10> [<br11>
<br12>]]]]]]]]] | supported { [<sr1> [<sr2> [<sr3> [<sr4> [<sr5> [<sr6>
<sr7> [<sr8> [<sr9> [<sr10> [<sr11> [<sr12>]]]]]]]]]]}}}
```

PARAMETERS

frag-threshold	802.11b/g fragmentation threshold packet size above which a packet will be fragmented
rts-threshold	802.11b/g RTS threshold packet size above which an RTS is issued before sending
auto_channel	Automatically assign channels to 802.11b/g IAPs
rates	Set allowed 802.11b/g bit rates
<i>basic</i>	Set 802.11b/g basic (required) rates
<i>supported</i>	Set 802.11b/g supported (accepted) rates
<i>defaults</i>	Set default 802.11b/g rates
<i>optimize_range</i>	Set 802.11b/g rates for best range
<i>optimize_throughput</i>	Set 802.11b/g rates for best throughput
all_down	Shut down (disable) all 802.11b/g IAPs
all_up	Bring up (enable) all 802.11b/g IAPs
preamble	Set 802.11b preamble length
short_preamble	Enable cck short preamble (56 sync bits)
long_preamble	Use only cck long preamble (128 sync bits)
slot_time	Set 802.11b/g slot time
short_slot	Enable short slot time (9 us)
long_slot	Use only long slot time (20 us)
dot11g_protect	Enable or disable 802.11g protection
dot11g_only	Enable or disable 802.11g only mode
<i>on</i>	Enable 802.11g only (or protection) mode
<i>off</i>	Disable 802.11g only (or protection) mode
cellsize	Cell size setting
<i>small</i>	Small cell size
<i>medium</i>	Medium cell size
<i>large</i>	Large cell size
rx-threshold	Deferred threshold (receive sensitivity)
tx-power	Maximum transmit power

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

None.

location

DESCRIPTION

Defines the location description for this Xirrus Array—available from the **config** command mode.

SYNTAX

location <locname>

PARAMETERS

locname Input location name for this Array

DEFAULTS

None.

USAGE GUIDELINES

Quotes must be used around the location text if spaces are used between words.

Typing **location** with no parameters will clear any set value.

EXAMPLE

To set the location description for the Xirrus Array:

```
(config)# location "Building 11 Floor 2"
```

SEE ALSO

None.

more

DESCRIPTION

Lists the contents of a file, one screen at a time.

SYNTAX

More <file name>

PARAMETERS

<file name> The file name for which to display the contents

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

None.

radius-server

DESCRIPTION

Configures the external or internal (local) radius server settings—available from the **Config-> radius-server** command mode

SYNTAX

```
radius-server [no] external [ {on | off | ip <pri_ip> | port <pri_port> |  
secret [enc] [<pri_secret>] | timeout <tmout>}@ ] | secondary [ {ip  
[<sec_ip>] | port [<sec_port>] | secret [enc] [<sec_secret>}}] |  
[no] internal [ {on | off | {add <aid> password [enc] <passwd> ssid <ss>} |  
del <did>} ]
```

PARAMETERS

external	Configure the primary external RADIUS server parameters <i>Prompt will change to (config-radius-external)#</i>
secondary	Configure the secondary external RADIUS server parameters <i>Prompt will change to (config-radius-secondary)#</i>
ip	IP address of the RADIUS server
port	Authentication port of the RADIUS server
secret	Shared secret for the RADIUS server
enc	Enter encrypted shared secret for the RADIUS server
on	Enable external RADIUS server
off	Disable external RADIUS server
timeout	Timeout (in seconds) before the server is retried after it initially failed
internal	Configure internal RADIUS server parameters
<i>on</i>	Enable internal RADIUS server
<i>off</i>	Disable internal RADIUS server
<i>add</i>	Add this user
<i>del</i>	Delete this user
<i>password</i>	User password
<i>enc</i>	Enter encrypted password
<i>ssid</i>	SSID with which the user is allowed to associate
show	Display current radius server settings

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

None.

reboot

DESCRIPTION

Reboots the Xirrus Array.

SYNTAX

reboot

PARAMETERS

None.

DEFAULTS

None.

USAGE GUIDELINES

When rebooting the Array, you must respond to the following prompts:

- The system will prompt you to save any unsaved configuration changes.
- The system will prompt you to confirm the reboot action.

EXAMPLE

To reboot the Xirrus Array type the following.

```
Xirrus_WLAN_Array(config)# reboot  
Do you want to save changes to flash? [yes/no]: y  
are you sure you want to reboot? [yes/no]: y
```

SEE ALSO

None.

reset

DESCRIPTION

Resets all settings to the factory defaults, then reboots the Xirrus Array.

SYNTAX

reset

PARAMETERS

None.

DEFAULTS

None.

USAGE GUIDELINES

When you enter the reset command, the system will prompt you to confirm the reset action.

EXAMPLE

To reset the Xirrus Array back to factory defaults, type:

```
Xirrus_WLAN_Array(config)# reset
```

```
Are you sure you want to reset to factory settings and reboot? [yes/no]:y
```

SEE ALSO

reboot

run-script

DESCRIPTION

Run a CLI command script.

SYNTAX

```
run-script <file name>
```

PARAMETERS

<file name> name of command script file

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

None.

run-tests**DESCRIPTION**

Runs network diagnostic tests from the run-test command mode—available from the **config-run-tests** command mode.

SYNTAX

tracroute <tracename> | ping <pingname>

PARAMETERS

tracroute <IP Address or DNS name>	Run a trace on IP route or DNS name
<i>ping</i> <IP Address or DNS name>	Execute ping utility

DEFAULTS

None.

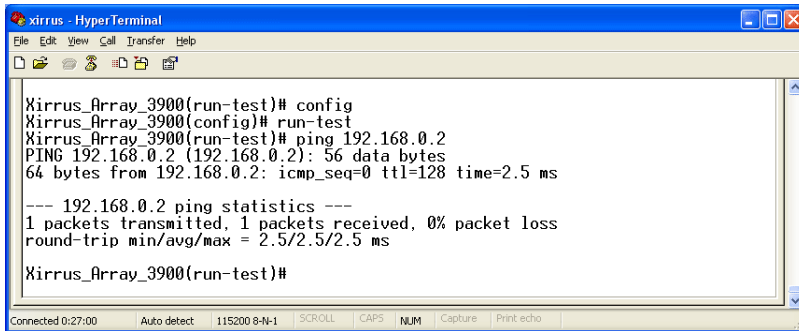
USAGE GUIDELINES

You access the **run-tests** command mode from the **config** mode.

EXAMPLE

To test connectivity to a client device at IP address 192.168.0.2 type:

```
(config)# run-tests
(config-run-test)# ping 192.168.0.2
```



```
xirrus - HyperTerminal
File Edit View Call Transfer Help
Xirrus_Array_3900(run-test)# config
Xirrus_Array_3900(config)# run-test
Xirrus_Array_3900(run-test)# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2): 56 data bytes
64 bytes from 192.168.0.2: icmp_seq=0 ttl=128 time=2.5 ms

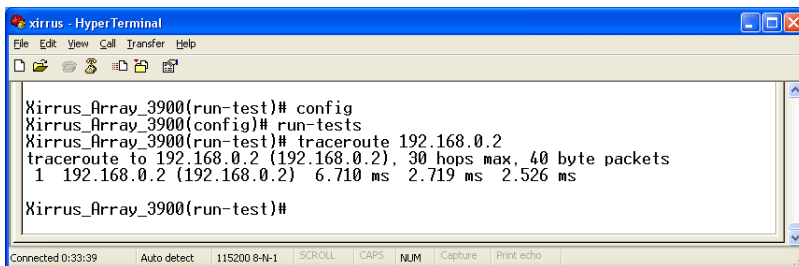
--- 192.168.0.2 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.5/2.5/2.5 ms

Xirrus_Array_3900(run-test)#
```

Figure 106. CLI: Testing Client Connectivity

To view the network routing to another device use **traceroute**:

```
(config)# run-tests
(config-run-test)# traceroute 192.168.0.2
```



```
xirrus - HyperTerminal
File Edit View Call Transfer Help
Xirrus_Array_3900(run-test)# config
Xirrus_Array_3900(config)# run-tests
Xirrus_Array_3900(run-test)# traceroute 192.168.0.2
traceroute to 192.168.0.2 (192.168.0.2), 30 hops max, 40 byte packets
 1 192.168.0.2 (192.168.0.2) 6.710 ms 2.719 ms 2.526 ms

Xirrus_Array_3900(run-test)#
```

Figure 107. CLI: Viewing the Routing to a Client

SEE ALSO

None.

save

DESCRIPTION

Permanently saves the current configuration so that changes will be available at the next system boot.

SYNTAX

save

PARAMETERS

None.

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

To permanently save the current configuration, type:

```
Xirrus_WLAN_Array(config)# save
```

SEE ALSO

None.

security

DESCRIPTION

Set wireless and other security parameters for the Xirrus Array. Available via the **config-security** command mode.

There are two options available from the Security command mode:

- **wep**: Set WEP encryption parameters
- **wpa**: Set WPA encryption parameters

SYNTAX

```
wep { on | off | default_key <keyid> | key {<keynum> size [not_set |
<wepsz> { ascii | hex | enc } <keystr> ] } }
```

PARAMETERS

on	Enable WEP encryption
off	Disable WEP encryption
key	Set static WEP key number 1-4
size	Key size (40 or 128 bits, default = 128)
ascii	ASCII characters
hex	Hex digits
enc	Encrypted form
default_key	Default key ID 1-4

SYNTAX

```
wpa { on | off | rekey { never | <ti> } | { no } tkip [ on | off ] | [ no ] aes [ on
| off ] | [ no ] eap [ on | off ] | [ no ] psk [ on | off ] | passphrase { not_set |
<pstr> | enc <epstr> } }
```

PARAMETERS

on	Enable WPA encryption
off	Disable WPA encryption
rekey	Time interval for rekeying broadcast encryption keys
never	Disable rekeying broadcast encryption keys
tkip	Enable or disable Temporal Key Integrity Protocol (TKIP)
on	Enable TKIP
off	Disable TKIP
aes	Enable or disable AES in counter mode with CBC-MAC (CCMP)
on	Enable AES
off	Disable AES
eap	Enable or disable 802.1x EAP
on	Enable EAP
off	Disable EAP
psk	Enable or disable Pre-Shared Key (PSK)
on	Enable PSK
off	Disable PSK
passphrase	WPA PSK (Pre-Shared Key) passphrase

enc Enter an encrypted form of the passphrase in double quotes

DEFAULTS

None.

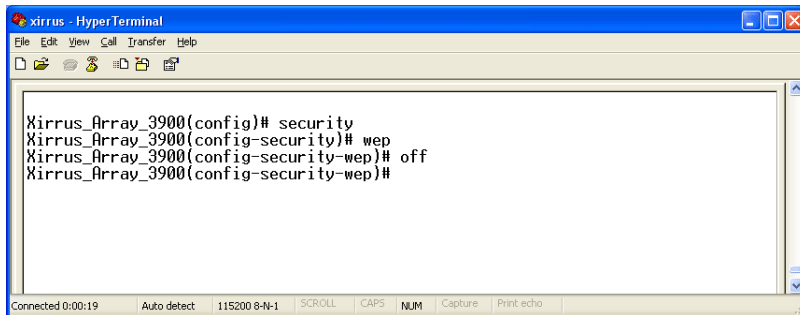
USAGE GUIDELINES

None.

EXAMPLE

To disable WEP encryption, type:

```
(config)# security  
(config-security) wep  
(config-security-wep) off
```



```
xirrus - HyperTerminal  
File Edit View Call Transfer Help  
Xirrus_Array_3900(config)# security  
Xirrus_Array_3900(config-security)# wep  
Xirrus_Array_3900(config-security-wep)# off  
Xirrus_Array_3900(config-security-wep)#  
Connected 0:00:19 Auto detect 115200 8-N-1 SCROLL CAPS NUM Capture Print echo
```

Figure 108. CLI: Disabling WEP Encryption

SEE ALSO

None.

show

DESCRIPTION

Displays settings and information, and is useful when verifying the current configuration of the Array.

SYNTAX

```
show [ acl | admin | array_info | console | contact_info | date_time |  
dhcp_server | diff | dns | ethernet | external_radius | factory_config | iap  
| internal_radius | log | rogue_ap | running_config | saved_config |  
security | snmp | ssid | startup_config | stations | statistics ]
```

PARAMETERS

acl	Display access control list
admin	Display administrator accounts list
array_info	Display system information
console	Display terminal settings
contact_info	Display contact information
date_time	Display date and time settings summary
dhcp_server	Display internal DHCP server settings summary
diff	Display the differences between configurations
dns	Display DNS summary
ethernet	Display eth0 and gig1/gig2 interface summary
external_radius	Display external RADIUS server settings summary
factory_config	Display the array configuration from the factory
iap	Display IAP configuration summary
internal_radius	Display all users defined for the embedded RADIUS server
log	Display the event log
rogue_ap	Display rogue AP information
running_config	Display the array configuration that is currently running
saved_config	Display the array configuration that was last saved
security	Display security settings summary
snmp	Display SNMP summary
ssid	Display SSID summary
startup_config	Display the array configuration from the last boot

stations	Display station (client) information
statistics	Display interface statistics

DEFAULTS

None.

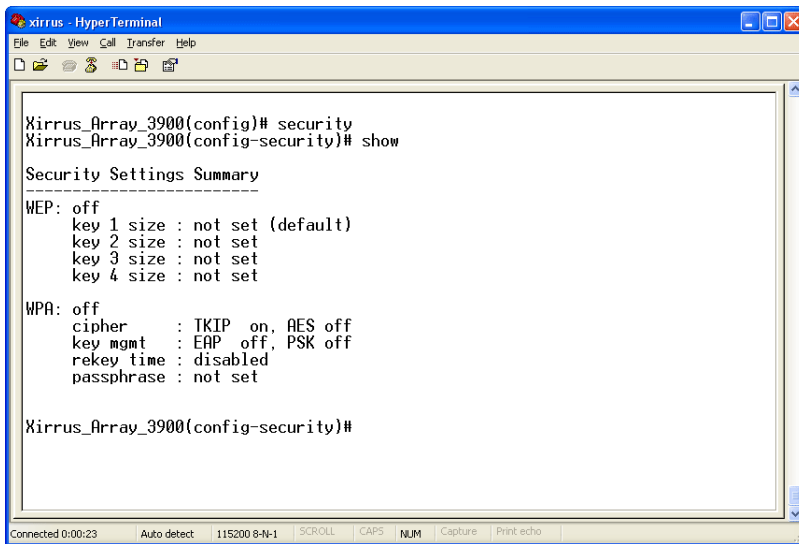
USAGE GUIDELINES

None.

EXAMPLE

To display the current security settings, type:

```
(config)# security
(config-security) show
```



```
xirrus - HyperTerminal
File Edit View Call Transfer Help
Xirrus_Array_3900(config)# security
Xirrus_Array_3900(config-security)# show

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

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

Xirrus_Array_3900(config-security)#

Connected 0:00:23  Auto detect  115200 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Figure 109. CLI: Displaying the Current Security Settings

SEE ALSO

None.

snmp

DESCRIPTION

Configures SNMP (Simple Network Management Protocol). This command is available from the **config->snmp** command mode.

SYNTAX

```
snmp {on | off | [no] trap [enable | disable] | host [<thsnmp>] | port <tpsnmp> | community <csnmp>}
```

PARAMETERS

on	Enable SNMP
off	Disable SNMP
host	SNMP trap IP address or host name
port	SNMP trap port
community	SNMP community string Note no spaces or special characters may be used
trap	Send traps for authentication failures
no	Disable selected feature
enable	Enable traps
disable	Disable traps

DEFAULTS

SNMP is disabled by default.

USAGE GUIDELINES

SNMP community string *cannot* have spaces or special characters.

EXAMPLE

None.

SEE ALSO

None.

ssh

DESCRIPTION

Enables or disables **ssh** (secure shell) access to the Command Line Interface.

SYNTAX

ssh {on | off}

PARAMETERS

on	Enable ssh access
off	Disable ssh access

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

telnet.

syslog

DESCRIPTION

Configures the syslog server settings. This command is available from the **config->syslog** command mode.

SYNTAX

```
syslog {on | off | {ipsyslog <ip address> | [no] console [on | off] | level <slev> | buffered <logfilesz> | show}}
```

PARAMETERS

on	Enable Syslog server
off	Disable Syslog server
ipsyslog <ip address>	Syslog IP address (in A.B.C.D format)
level	Syslog message level (log all messages with this level and lower)
buffered	Set the size of the local Syslog file
console	Enable or disable display of Syslog messages on the console
<i>no</i>	Disable console feature
<i>on</i>	Enable Syslog messages on the console
<i>off</i>	Disable Syslog messages on the console
show	Show current syslog messages

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

None.

telnet

DESCRIPTION

Enables or disables telnet access to the Command Line Interface.

SYNTAX

telnet {on | off}

PARAMETERS

on	Enable telnet access
off	Disable telnet access

DEFAULTS

None.

USAGE GUIDELINES

None.

EXAMPLE

None.

SEE ALSO

None.

Use this space for your notes ...



Appendices

Page is intentionally blank

Appendix A: Servicing the Xirrus Array

This chapter contains procedures for servicing the Xirrus Array, including the removal and reinstallation of major hardware components. Section headings for this chapter include:

- “Removing the Access Panel” on page 200
- “Reinstalling the Access Panel” on page 202
- “Replacing the FLASH Memory Module” on page 203
- “Replacing the Main System Memory” on page 204
- “Replacing the Integrated Access Point Radio Module” on page 205
- “Replacing the Power Supply Module” on page 207

! *Always turn OFF the Array’s power switch and disconnect the AC power cord before attempting to remove or replace components. Never work on the unit with the power connected.*

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

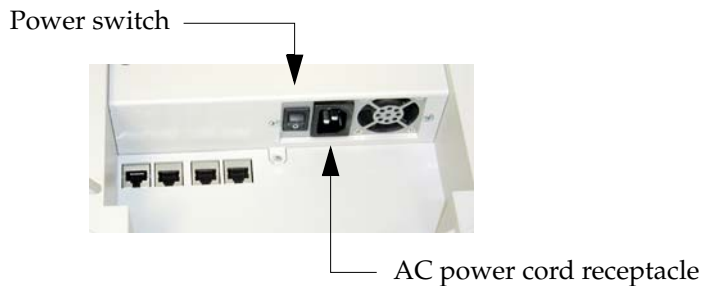


Figure 110. Disconnecting Power from the Array



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

Removing the Access Panel

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

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

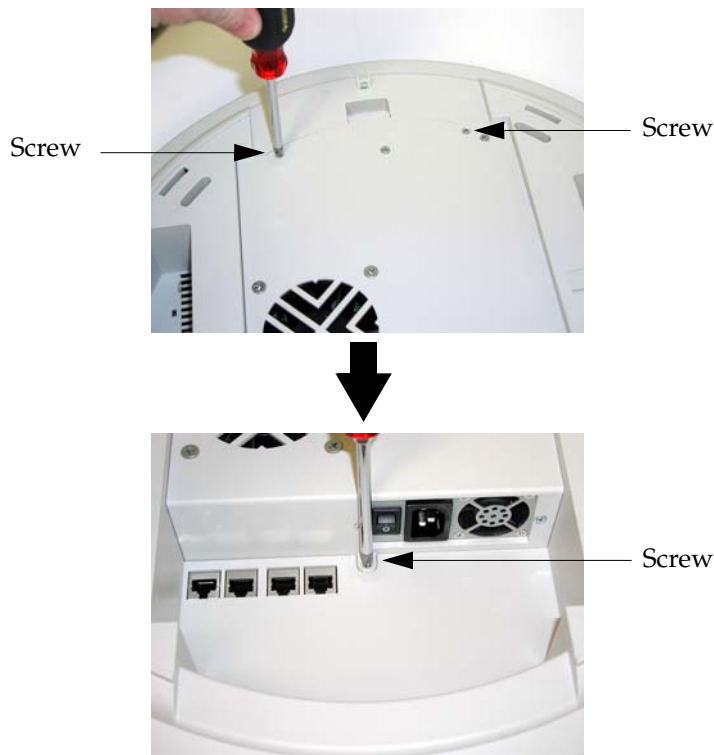


Figure 111. Removing the Access Panel Screws

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



Lift up the access panel

Figure 112. Removing the Access Panel

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



Fan connector

Power supply connector

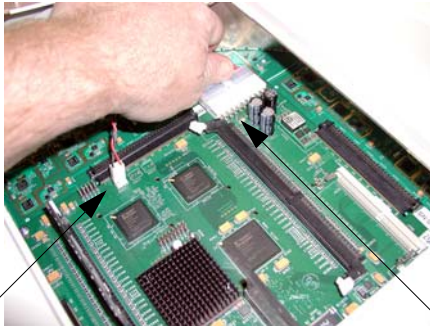
Figure 113. Disconnecting the Power Supply and Fan

7. The access panel can now be safely removed.

Reinstalling the Access Panel

Use this procedure when you need to reinstall the access panel after servicing the XS-3900's internal components.

1. Reconnect the fan and power supply.



Fan connector

Power supply connector

Figure 114. Reconnecting the Fan and Power Supply

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



Figure 115. Reinstalling the Access Panel

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

Replacing the FLASH Memory Module

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

1. Remove the system's access panel. Refer to "Removing the Access Panel" on page 200.
2. Remove the FLASH memory module, taking care not to "wiggle" the module and risk damaging the connection points.

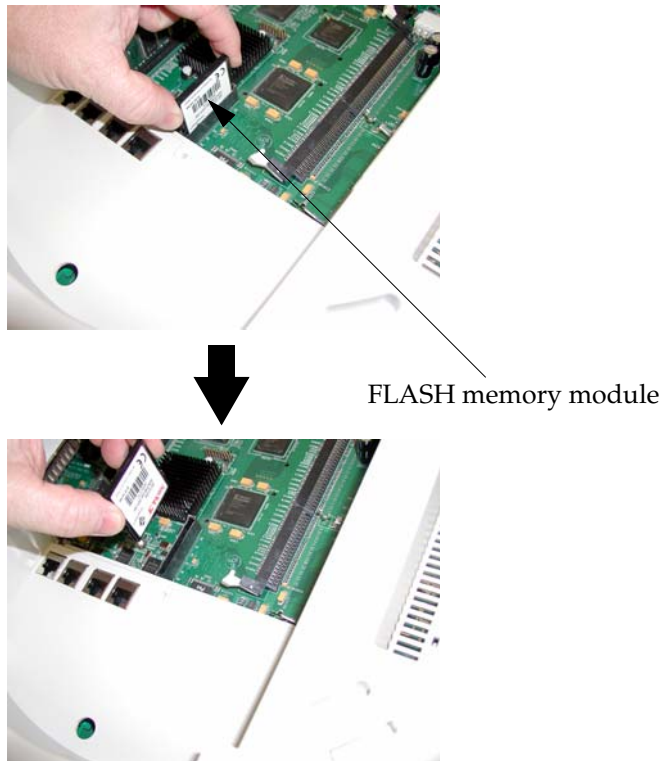


Figure 116. Removing the FLASH Memory Module

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

4. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 202).

Replacing the Main System Memory

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

1. Remove the access panel (refer to “Removing the Access Panel” on page 200).
2. Remove the DIMM memory module, taking care not to “wiggle” the module and risk damaging the connection points.

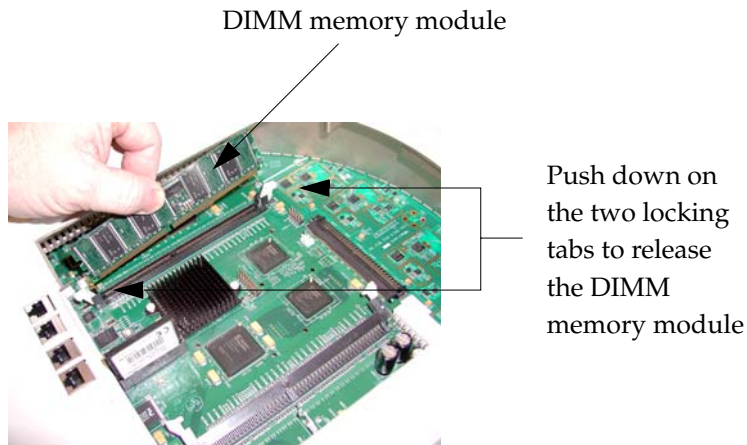


Figure 117. Removing the DIMM Memory Module

3. The removal procedure is complete. You can now reinstall the DIMM memory module (or install a new module). Ensure that the DIMM memory module is seated evenly and the locking tabs are in the upright position.



The DIMM memory module is keyed to fit in its socket in one direction only.

4. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 202).

Replacing the Integrated Access Point Radio Module

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

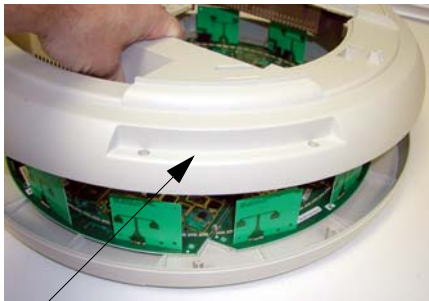
1. Remove the access panel (refer to “Removing the Access Panel” on page 200).
2. Remove the nylon locking screws (8 places) that secure the chassis cover to the main body of the XS-3900.



Nylon screws (8 places)

Figure 118. Removing the Chassis Cover Nylon Screws

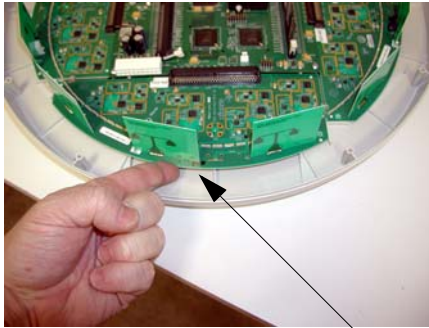
3. Lift and remove the chassis cover.



Remove the chassis cover

Figure 119. Removing the Chassis Cover

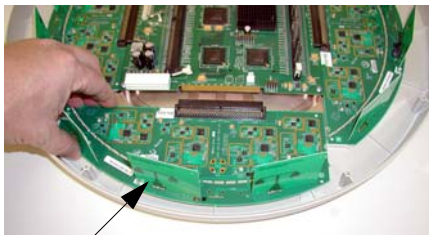
4. Lift the edge of the integrated access point module.



Lift here (do not force)

Figure 120. Lifting the Integrated Access Point Module

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



Disconnect the module

Figure 121. Disconnect the Integrated Access Point Module

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

7. Reinstall the chassis cover (see warnings).
 - ! *When reinstalling the chassis cover, take care to align the cover correctly to avoid damaging the antenna modules. Do not force the chassis cover onto the body of the unit.*
 - ! *Do not overtighten the nylon locking screws.*
8. Reinstall the nylon locking screws (8 places) to secure the chassis cover in place—do not overtighten.
9. Reinstall the access panel (refer to “Reinstalling the Access Panel” on page 202).

Replacing the Power Supply Module

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

1. Remove the access panel (refer to “Removing the Access Panel” on page 200).
2. Because the power supply unit is molded into the access panel, you must install a new access panel assembly (with the power supply attached). Refer to “Reinstalling the Access Panel” on page 202.



Access panel (with power supply and fan)

Figure 122. Installing a New Access Panel (with Power Supply)

Use this space for your notes ...

Appendix B: Quick Reference Guide

This chapter contains product reference information. Use this chapter to locate the information you need quickly and efficiently. Section headings for this chapter include:

- “Review of WMI Pages” on page 209
- “Factory Default Settings” on page 213
- “Keyboard Shortcuts” on page 219

Review of WMI Pages

This section provides a review of the product’s WMI pages, with a brief explanation of their function and content. Click on any of the listed pages to go to the corresponding procedure at the referenced destination.

Page	Function
Array Status	Provides a snapshot of the global configuration settings for all Array network interfaces and radios.
Express Setup	Establish global configuration settings that will enable basic XS-3900 functionality.
Network Interfaces	Provides a snapshot of the configuration settings currently established for the network interfaces.
Network Settings	Establish basic configuration settings for the network interfaces.
Network Statistics	Provides statistical data associated with network interfaces and their activity.
DHCP Settings	Enable or disable DHCP (Dynamic Host Configuration Protocol) server functionality.

Page	Function
DNS Settings	Set up a DNS server (or multiple servers), if you want to offer clients associating with the Array the ability to use meaningful domain names (URLs) instead of numerical IP addresses.
IAP Interfaces	Provides a snapshot of global configuration data associated with radios.
IAP Settings	Enable or disable radios, define the wireless mode for each radio, establish the transmit and receive parameters, and define global settings for the beacon interval and DTIM period.
Global Settings	Establish global IAP (radio) settings. Global IAP settings include enabling or disabling all radios (regardless of their operating mode).
Global Settings .11a	Establish global 802.11a IAP (radio) settings.
Global Settings .11bg	Establish global 802.11b/g IAP (radio) settings.
IAP LED Settings	Set the behavior of LEDs.
Statistics	Provides an overview of statistical data associated with individual radios.

Page	Function
SSID	Provides a snapshot of SSID (Service Set Identifier) assignments. It includes the SSID name, whether or not an SSID is visible on the network, any security and QoS parameters defined for each SSID, associated VLAN IDs, guest access, and radio availability per SSID.
SSID Management	Manage SSIDs (create, modify or delete). It also allows you to assign security parameters and VLANs on a per SSID basis.
Security	Provides a snapshot of Array global security configuration parameters, including administration accounts, ACL values, WEP/WPA/WPA2 status, and RADIUS configuration settings.
Security Management	Establish the security parameters for your wireless network, including WEP, WPA and RADIUS authentication.
Radius Server	Set up the XS-3900's internal RADIUS server, or set up an external RADIUS server for user authentication.
Radius User	Create, delete and manage RADIUS user accounts.
MAC Access List	Create new MAC-based Access Control Lists (ACLs), delete existing ACLs, and add, remove, or restore MAC addresses.
Admin Management	Manage network administrator accounts (create, modify or delete), restore accounts, or limit account access to a read only status.

Page	Function
Rogue AP List	Displays rogue APs, according to the sort list you select (either Unknown, Known or Approved).
Rogue Control List	Establishes a control list for rogue APs, based on a type that you define.
Stations	Displays stations that are currently associated with the Array.
Services	Provides a current status of Syslog and SNMP services.
Time Settings	Synchronizes the Array's clock with a universal clock from an NTP server.
System Log	Enable or disable the Syslog server, define the server's IP address, and set the level for Syslog reporting.
SNMP	Enable or disable SNMP and define the SNMP parameters.
Array Info	Displays the current status of the Array.
Tools	Ping the Array and obtain a status of the unit's performance.
Show Config	Displays the configuration settings (Current/Saved/Start) for the Array.
Event Log	Provides an event log for the network.

Factory Default Settings

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

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	10.0.1.2
Default IP Mask	255.0.0.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	1000 Mbps
MTU Size	1504
Management Enabled	Yes

Fast Ethernet

Setting	Default Value
Enabled	Yes
DHCP Bind	Yes
Default IP Address	10.0.1.1
Default IP Mask	255.0.0.0
Default Gateway	None
Auto Negotiate	On
Duplex	Full
Speed	100 Mbps
MTU Size	1500
Management Enabled	Yes

Integrated Access Points (IAPs)

Setting	Default Value
Antenna	0
Mode	11a for a1 to a12 11g for abg1 to abg4
Channel	Auto
Maximum Transmit Power	0
Cell Size	Medium

Server Settings

DHCP

Setting	Default Value
Enabled	No
Maximum Lease Time	300 minutes
Default Lease Time	300 minutes
IP Start Range	192.168.1.100
IP End Range	192.168.1.200

External RADIUS

Setting	Default Value
Enabled	Yes
Primary Server	0.0.0.0
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

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 200 entries.	

NTP

Setting	Default Value
Enabled	No
Primary	time.nist.gov
Secondary	192.6.15.29

Syslog

Setting	Default Value
Enabled	No

SNMP

Setting	Default Value
Enabled	No
Community String	xirrus
Trap Host	null (no setting)
Trap Port	162
Authorization Fail Port	1

Default SSID

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

Encryption

Setting	Default Value
Enabled	Yes
WEP Keys	null (all 4 keys)
WEP Key Length	null (all 4 keys)
Default Key ID	0
WPA Enabled	No
TKIP Enabled	Yes
AES Enabled	No
EAP Enabled	Yes
PSK Enabled	No
Pass Phrase	null
Group Rekey	600

Administrator Account and Password

Setting	Default Value
ID	admin
Password	admin

Management

Setting	Default Value
Telnet	On
SSH	On

Keyboard Shortcuts

The following table shows the most common keyboard shortcuts.

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
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.	?

Use this space for your notes ...

Appendix C: Technical Support

This chapter provides valuable support information that can help you resolve technical difficulties. Before contacting Xirrus, review all sections in this chapter and try to determine if your problem resides with the Array or your network infrastructure. Section headings for this chapter include:

- “General Hints and Tips” on page 221
- “Frequently Asked Questions” on page 222
- “Contact Information” on page 228

General Hints and Tips

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

- The Array requires careful handling. For best performance, units should be mounted in a dust-free and temperature-controlled environment.
- If using multiple Arrays at the same location, we recommend maintaining a distance of at least 50 feet between units.
- Keep the Array away from electrical devices or appliances that generate RF noise. Because the Array is generally mounted on ceilings, be aware of its position relative to lighting (especially fluorescent lighting).
- If using AC power, each Array requires its own dedicated AC power outlet. Do not attempt to “piggy-back” AC power to multiple units. If deploying multiple units, consider using the optional Xirrus Remote DC Power System (XP-3100).
- If you are deploying multiple units, ensure that the “clock face” of all units is aligned in the same direction.
- The Array should only be used with Wi-Fi certified client devices.

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 LAN 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 “[SSID](#)” on page 107.
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 XS-3900 will not broadcast SSIDs that are hidden, clients can still associate to a hidden SSID if they know the SSID name to connect to it.
 3. Select the minimum security that will be required by users for this SSID.
 4. If desired (optional), select a Quality of Service (QoS) setting for this SSID. The QoS setting you define here will prioritize wireless traffic for this SSID over other SSID wireless traffic.
 5. If desired (optional), select a VLAN that you want this traffic to be forwarded to on the wired network.
 6. If desired (optional), you can select which radios this SSID will not be available on—the default is to make this SSID available on all radios.
 7. Click on the **Apply** button to apply your changes to this session.
 8. Click on the **Save** button to save your changes.
 9. If you need to edit any of the SSID settings, you can do so from the [SSID Management](#) page.

Security

Q. How do I know my management session is secure?

A. Follow these guidelines:

- Administrator passwords
Always change the default administrator password (the default is **admin**), and choose a strong replacement password. When appropriate, issue **read only** administrator accounts.
- SSH versus Telnet
Be aware that Telnet is not secure over network connections and should be used only with a direct serial port connection. When connecting to the unit's Command Line Interface over a network connection, you must use a Secure SHell (SSH) utility. The most commonly used freeware providing SSH tools is PuTTY.
- Configuration auditing
Do not change approved configuration settings. The optional Xirrus Wireless Management System (XM-3300) offers powerful management features for small or large XS-3900 deployments, and can audit your configuration settings automatically. In addition, using the XM-3300 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 XS-3900 allows you to establish the following data encryption configuration options:

- Open
This option offers no data encryption and is **not recommended**, though you might choose this option if clients are required to use a VPN connection through a secure SSH utility, like PuTTY.

- WEP (Wired Equivalent Privacy)
This option provides minimal protection (though much better than using an open network). An early standard for wireless data encryption and supported by all Wi-Fi certified equipment, WEP is vulnerable to hacking and is therefore not recommended for use by Enterprise networks.

- WPA (Wi-Fi Protected Access)
This is a much stronger encryption model than WEP and uses TKIP (Temporal Key Integrity Protocol) with AES (Advanced Encryption Standard) to prevent WEP cracks.

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

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

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

Q. Which user authentication method should I use?

- A.** User authentication ensures that users are who they say they are. For this purpose, the 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 the XS-3900.

- 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 XS-3900) 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 XS-3900 units?

- A.** When deploying multiple 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 Wireless Management System (XM-3300) 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 Xirrus Array has a dedicated radio (abg/4) which constantly scans the local wireless environment for rogue APs (non-Xirrus devices that are not part of your wireless network), unencrypted transmissions, and other security issues. Administrators can then classify each rogue AP and ensure that these devices do not interrupt or interfere with the network.

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 the XS-3900, allowing a total of sixteen VLANs to be accessed (one per SSID).

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

Contact Information

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

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

Tel: 1.805.497.0955
Fax: 1.805.449.1180

www.xirrus.com

Glossary of Terms

802.11a

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

802.11b

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

802.11d

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

802.11g

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

802.1Q

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

AES

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

authentication

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

bandwidth

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

beacon interval

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

bit rate

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

BSS

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

BSSID

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

cell

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

channel

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

CoS

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

default gateway

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

DHCP

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

DHCP lease

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

DNS

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

domain

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

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

DTIM

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

EAP

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

EDCF

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

encapsulation

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

encryption

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

Fast Ethernet

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

FCC

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

frame

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

Gigabit 1

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

Gigabit 2

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

Gigabit Ethernet

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

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.

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 guarantees a service's performance, such as an average or minimum throughput rate.

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.

RDPS

(Remote Distribution Power Supply) A Xirrus proprietary power supply used for delivering power from a remote source to the Xirrus family of products.

Remote DC Power System (XP-3100)

An optional Xirrus proprietary product that provides distributed DC power to multiple XS-3900 units, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.

RSSI

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

SDMA

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

SNMP

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

SNTP

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

SSH

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

SSID

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

subnet mask

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

TKIP

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

transmit power

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

VLAN

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

VLAN tagging

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

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

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 LAN Array (XS-3900)

A Xirrus proprietary high capacity wireless access point utilizing multiple channels, specifically designed for the Enterprise market.

Wireless Management System (XM-3300)

A Xirrus proprietary product used for managing large XS-3900 deployments from a centralized Web-based interface.

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.

XM-3300

The Xirrus Wireless Management System (XM-3300) is a Xirrus proprietary product used for managing large XS-3900 deployments from a centralized Web-based interface.

XP-3100

The Xirrus Remote DC Power System (XP-3100) is an optional Xirrus proprietary product that provides distributed DC power to multiple XS-3900 units, eliminating the need to run dedicated AC power to each unit and facilitating backup power when connected via a UPS.

XS-3900

The Xirrus Wireless LAN Array (XS-3900) is a high capacity, multi-wireless access point specifically designed for the Enterprise market.

Use this space for your notes ...

Index

Numerics

802.11a 11
802.11a/b/g 11
802.11b/g 11
802.11e 12
802.11p 12
802.11q 12

A

access panel
 reinstalling 202
 removing 200
AES 12
authentication 12

B

beam distribution 11
benefits 10

C

channels
 non-overlapping 12
character restrictions 68
chassis cover 205
CLI
 Telnet connection 143
Command Line Interface 143
commands
 CLI 143
configuration changes
 applying 68
contact information 228
coverage
 extended 11
critical messages 67

D

default settings 213
deployment
 ease of 12
DHCP server 23, 85
DIMM module
 replacing 204
DNS settings 87

E

EAP-MDS 12
EAP-TLS 12
EAP-TTLS 12
encryption 12
event log 142
event messages 67
express setup 54, 73
external RADIUS server 802.1x 23

F

factory default settings 213
FAQs 222
features 10
FLASH memory
 replacing 203
frequently asked questions 222
FTP server 23

G

glossary of terms 229

H

help button 68
HyperTerminal 22

I

installation 21, 197
 installing the MCAP-3616 41

- mounting the unit 43
- requirements 21
- unpacking the unit 40
- workflow 39

installation workflow 39

integrated radio module replacing 205

interfaces

- Web 65

Internet Explorer 22

K

- key features 10
- keyboard shortcuts 219

L

- logging 133, 142
- logging in 69

M

- MIC 12
- mounting the unit 43

N

- Netscape Navigator 22
- network
 - interfaces 79
 - settings 80
 - statistics 84
- network installation 21, 197
- non-overlapping channels 12

O

- overview 6

P

- password 69
- PEAP 12

- performance 10
- power cord 200
- power outlet 21
- power supply
 - replacing 207
- power switch 200
- print button 68
- product installation 21, 197
- product overview 6
- product specifications 13, 17
- PuTTY 22

Q

- QoS 12
- Quality of Service 12
- quick reference guide 209

R

- radio distribution 10
- RADIUS server 23, 118, 120
- rogue detection 11

S

- Secure Shell 22
- security 6, 12, 112
 - management 113
 - RADIUS server 118, 120
- serial port 22
- services 130
- servicing the unit 197
- SNMP 9, 135
- specifications 13, 17
- SSH 22
- SSID
 - management 107
- statistics 84
- status bar 68
- system log 133
- system memory

replacing 204

T

technical support
 contact information 228
 frequently asked questions 222
Telnet
 establishing a connection 143
TKIP 12
tools 138

U

unpacking the unit 40
user interface 65

V

VoWLAN 12

W

warning messages 67
Web interface 65
 structure and navigation 67
WEP 12
workflow 39
WPA2 6

X

Xirrus Management System 6, 9, 12, 23
Xirrus Remote Power System 21, 23
XMS 6, 9, 12, 23
XRPS 21, 23
XS 3900
 management 69

Page is intentionally blank