Command Reference

Airgo Networks AGN1200AP

Release 1.0

Airgo Networks, Inc.
900 Arastradero Road
Palo Alto, CA 94304
P: 650-475-1900
F: 650-475-1708
www.airgonetworks.com

Part Number: 640-00040-00
Published: February 2004

Contents

Preface

This guide explains how to install and configure the Airgo Access Point (Airgo AP), which is used with Wi-Fi certified clients to provide PC laptop and desktop users with wireless network access.

The Airgo Access Point provides the following features:

- High throughput and range through dual-band radio transceivers with as much as nine times the data rate and three times the range of most other vendors’ products
- Easy installation
- Wireless networking features that include bridging, VLAN, Quality of Service (QoS), IP routing, and network backhaul capabilities
- Seamless mobility within bridged wireless VLANs
- Comprehensive security that includes support for WEP, TKIP, AES, EAP-PEAP, EAP-TLS, and RADIUS
- Automated radio resource management, including controls for operating channels, capacity, and range
- Policy-based management, offering session, system, and network-level management

Audience

This guide is designed to help you install and configure the Airgo Access Point hardware successfully even if you are unfamiliar with wireless networking technology. It is expected that you have some familiarity with local area networking technology. If you encounter a term or acronym with which you are unfamiliar, refer to the glossary at the end of the guide, just before the index.

Conventions Used in this Guide

This guide uses the following conventions for instructions and information.

Notes, Cautions, and Warnings

Notes, cautions, and time-saving tips use the following conventions and symbols.

ℹ **NOTE:** Notes contain helpful suggestions or information that may be of importance to the task at hand

! **CAUTION:** Caution indicates that there is a risk of equipment damage or loss of data when certain actions are performed.

ϟ **WARNING:** Warnings are intended to alert you to situations that could result in injury (such as exposure to electric current, for example).

Command Conventions

Table 1 describes the command syntax used in this document.

Table 1: Command Conventions

Convention	Description
boldface	Commands and keywords.
italic	Command input that is supplied by you.
[ ]	Optional keywords and default responses to system prompts appear within square brackets.
{**x** | **x** | **x**}	A choice of keywords (represented by **x**) appears in braces separated by vertical bars. You must select one.
Ctrl	Represent the key labeled *Ctrl*. For example, when you read ^*D* or *Ctrl-D*, you should hold down the Control key while you press the D key.
`panel font`	Examples of information displayed on a panel.
`boldface panel font`	Examples of information that you must enter.

CLI AP-Quick-Start Configuration Command Structure

ap-quick-start(config)>

- **add-ssid**- Add an SSID filter show mode.
  - *ssid* - ssid
- **admin-contact** - Set administrator contact information.
  - *contact*- contact
- **channel** - Configure channel parameters for an interface.
  - *interface* - specify valid interface name
    - — auto-select-periodic- periodic trigger 30 - 1440 minutes
    - — auto-select-startup- auto select trigger at startup
    - — channel- specify channel-id
- **channel-set** - Configure DFS channel-set.
  - *interface* - specify valid interface name
    - — band - Specify band type
    - — channel-list - List of space separated channel numbers in quotes; Refer to the User Guide for valid list
- **date** - Set system date manually.
  - *mm-dd-yyyy*- specify date in mm-dd-yyyy format
- **dns** - Configure domain name servers.
  - *delete-all-dns-servers*- delete-all-dns-servers
  - *dns-servers*- dns-servers address(es)
- **email** - Configure smtp-server and notify-email address.
  - *smtp-server* - smtp-server
- **exit** - Exit from ap-quick-start.

- **hostname** - Configure system hostname.
  - *name* - name
- **logout** - Logout and close connection to CLI engine.
- **mgmt-ipaddress** - Configure management interface's IP address and default gateway.
  - *dhcp-assigned* - get an IP address from DHCP server
  - *ipaddress* - A.B.C.D/E (e.g. 1.2.3.4/24 where 24=255.255.255.0)
- **network-connectivity**- Configure network connectivity.
  - *any* - any network connectivity
  - *wired-only* - wired-only network connectivity
  - *wireless-only*- wireless-only network connectivity
- **network-density**- Configure network density.
  - *high* - high network density (APs in close proximity)
  - *low* - low network density (few APs, far apart)
  - *medium* - medium network density (APs equally distributed)
- **portal-services**- Enable/disable various portal services.
  - *enrollment* - enrollment service enable/disable
  - *nm* - network mgmt service enable/disable
  - *security* - security service enable/disable
- **rename-ssid** - Rename an SSID.
  - *old-ssid* - old-ssid
    - new-ssid - new-ssid
- **save** - Save running configuration to flash.
- **security-modes**- Set AP global security modes.
  - *open-access* - open access enable/disable
    - disable - disable
    - enable - enable
  - *wep*- wep enable/disable
    - disable - disable
    - enable - enable
  - *wpa* - wpa enable/disable
    - disable - disable
    - enable - enable
- **time** - Set system time manually.
  - *hh:mm:ss* - specify time in hh:mm:ss format
- **time-sync**- Setup how time-of-day will be synchronized.
  - *manual* - manual
  - *ntp-servers*- ntp-servers
- **time-zone** - Configure time zone.

  - *gmt-minus* - specify value in HH:MM format
  - *gmt-plus* - specify value in HH:MM format
  - *us-zone* - us-zone
- **wep-key** - Configure WEP keys for the AP.
  - *key-index* - wep key index

Relationship Between CLI AP-Quick-Start and Standard CLI Commands

The ap-quick-start CLI function is a scripted interface to standard CLI commands. It provides a single CLI configuration entry point to enable a rapid deployment of a single access point when Web User Interface (Web UI) access is unavailable. Table 2 lists the ap-quick-start configuration commands and the CLI standard commands that each executes. For appropriate command usage and format, refer to the standard CLI command descriptions.

Table 2: Relationship Between CLI AP-Quick-Start and Standard CLI Commands

CLI Command	Function	CLI Standard Command
ap-quick-start(config)>		
add-ssid	Add an SSID.	ssid(config)> add-ssid
admin-contact	Set administrator contact information.	system(config)> admin-contact
ap-location	Set location of an access point.	system(config)> ap-location
channel	Configure channel parameters for an interface.	radio(config)> channel
channel-set	Configure DFS channel-set.	radio(config)> channel-set
date	Cet system date manually.	system(config)> date
dns	Configure domain name servers.	system(config)> dns
email	Configure smtp-server and notify-email address.	system(config)> email
exit	Exit from current mode.	exit
hostname	Configure system hostname.	system(config)> hostname
logout	Logout and close connection to CLI engine.	logout
mgmt-ipaddress and default gateway	Configure management interface's IP address.	system(config)>mgmt-ipaddress
network-connectivity	Configure network connectivity.	radio(config)> network-connectivity
network-density	Configure network density.	radio(config)> network-density
portal-services	Enable/disable various portal services.	portal(config)> portal-services
rename-ssid	Rename an SSID.	ssid(config)> rename-ssid
save	Save running configuration to flash.	ssid(config)> save
security-modes	Set AP global security modes.	security(config)> security-modes

Table 2: Relationship Between CLI AP-Quick-Start and Standard CLI Commands (continued)

time	Set system time manually.	system(config)> time
time-sync	Setup how time-of-day will be synchronized.	system(config)> time-sync
time-zone	Configure time zone.	system(config)> time-zone
wep-key	Configure WEP keys for the AP.	security(config)> wep-key

Related Documentation

The following documentation related to the Airgo Networks wireless networking product line is available on CD-ROM and also on the Airgo Networks website, http://www.airgonetworks.com.

- **Airgo Client Installation and User Guide** — Explains how to install and configure the Airgo Wireless LAN Client Adapter, which provides PC laptop and desktop users with access to the Airgo Access Point products.
- **Airgo NMS Pro Installation and Configuration Guide** — Explains how to use Airgo NMS Pro to manage an enterprise wireless network.

1 Backhaul CLIs

This chapter includes information about the following backhaul commands:

- **backhaul(config)> bp-add-bssid**
- **backhaul(config)> bp-delete-bssid**
- **backhaul(config)> bp-retrunk-now**
- **backhaul(config)> bp-uplink-bssid-criteria**
- **backhaul(show)> bp-uplink-candidates**
- **backhaul(config)> bp-uplink-criteria**
- **backhaul(show)> bp-uplink-criteria**
- **backhaul(config)> reset-to-defaults**
- **backhaul(show)> statistics**
- **backhaul(show)> trunk-table**

backhaul(config)> bp-add-bssid

Use this command to configure a list of uplink BSSIDs with which the radio in BP mode should or should not form the backhaul link.

Syntax

```
bp-add-bssid { all-interfaces| interface interface-name } bssid bssid {...}
```

Input Parameters

all-interfaces	Apply to all radio interfaces of this AP.
interface	Apply to specific radio interfaces that operate in BP mode.
bssid	One or more BSSIDs of uplink AP radios.

Output Parameters

Success or Failure

Description

This command is used to configure a set of BSSIDs. Subsequently, based on the configuration of bp-uplink-bssid-criteria, this list is used by the radio in BP mode to either accept or reject backhaul formation with those BSSIDs (uplink APs).

Defaults

None

Usage Guidelines

This configuration is only required when you want an explicitly configured wireless backhaul network.

This command should be applied on the radio operating in BP mode.

Examples

```
bp-add-bssid all-interfaces bssid “0a:22:3f:ff:2c:8f 00:de:ad:ef:01”
```

See Also

```
backhaul(config)> bp-delete-bssid
backahul(show)> bp-uplink-candidates
```

backhaul(config)> bp-delete-bssid

Use this command to delete BSSID from a list of configured uplink BSSIDs used in conjunction with bp-uplink-bssid-criteria.

Syntax

```
bp-delete-bssid [ interface interface-name] { all-bssid | bssid bssid {...} }
```

Input Parameters

interface	Apply this command to a specific radio interface.
all-bssids	Delete all entries of BSSIDs.
bssid	Delete a specific set of BSSIDs.

Output Parameters

Success or Failure

Description

This command is used to delete a set of BSSIDs used in conjunction with bp-uplink-bssid-criteria. The list can be used as an accept list or an discard list based on the bp-uplink-bssid-criteria configuration.

Defaults

None

Usage Guidelines

To delete one or many uplink BSSIDs that have been added to the uplink BSSID list.

Examples

```
bp-delete-bssid all-bssids, bp-delete-bssid interface wlan0 bssid
“00:0a:de:ad:be:ef 00:de:ad:be:ef:0a”
```

See Also

```
backhaul(config)> bp-add-bssid
backhaul(config)> bp-uplink-bssid-criteria
```

backhaul(config)> bp-retrunk-now

Use this command to force a downlink BP radio to retrunk (reform) the backhaul.

Syntax

```
bp-retrunk-now interface interface-name
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is useful to force retrunking of a downlink BP radio. This command allows an administrator to run the retrunking algorithm upon invocation of this command.

Defaults

None

Usage Guidelines

This command lets you retrunk upon specific administrative situations, such as activation of new uplink AP radios in the network, or update of the BP uplink criteria configuration. This command is valid only for radio interfaces operating in BP mode.

Examples

```
bp-retrunk-now interface wlan1
```

See Also

```
backhaul(config)> bp-uplink-criteria
```

backhaul(config)> bp-uplink-bssid-criteria

Use this command to accept or discard uplink APs as wireless backhaul candidates, based on uplink bssid list configuration of BP radios.

Syntax

```
bp-uplink-bssid-criteria { all-interfaces | interface interface-name } {
accept | discard }
```

Input Parameters

all-interfaces	Apply this command to all radio interfaces.
interface	Apply this command to a specific radio interface.
accept	Accept as uplink candidates only those BSSIDs which are members of the uplink bssid list.
discard	Discard as uplink candidates only those BSSIDs which are members of the uplink bssid list, accept all other BSSIDs.

Output Parameters

Success or Failure

Description

This command is used to configure the criteria by which a BP radio can choose to either accept or discard candidate uplink AP radios identified by their corresponding BSSIDs.

Defaults

None

Usage Guidelines

This command is useful to make sure only authorized list of uplink AP radios can form a wireless backhaul with this downlink radio (BP), when the bp-uplink-bssid-criteria is set to accept. If this criteria is set to discard, then the same list of uplink AP radios (identified by their corresponding BSSIDs) is used to not allow them form wireless backhaul with this downlink radio.

Examples

```
bp-uplink-bssid-criteria all-interfaces accept
```

See Also

```
backhaul(config)> bp-add-bssid
backhaul(config)> bp-delete-bssid
backhaul(show)>bp-uplink-criteria
backhaul(show)>bp-uplink-candidates
```

backhaul(show)> bp-uplink-candidates

Use this command to list of uplink candidates as seen by a BP radio.

Syntax

```
bp-uplink-candidates [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to show the list of uplink candidates for a BP radio based on detection of AP beacons and application of rules based on BP uplink criteria configuration. The uplink candidates are identified by remote MAC address (BSSID) and beacon name of the AP.

Defaults

None

Usage Guidelines

This command give you a snap-shot of what potential backhaul candidates a BP radio sees based on its wireless beacon scan.

Examples

```
backhaul(show)> bp-uplink-candidates

interface   : wlan0
mac         : 00:0a:f5:00:06:17
beacon name : AP-00:0a:f5:00:01:f2

--------------------------------------------------------------------------

interface   : wlan0
mac         : 00:0a:f5:00:06:5a
beacon name : AP-00:0a:f5:00:01:f2
```

See Also

```
backhaul(config)> bp-uplink-criteria
backhaul(config)> bp-uplink-bssid-criteria
backhaul(show)>bp-uplink-criteria
```

backhaul(config)> bp-uplink-criteria

Use this command to configure the uplink criteria used by the BP radio to form wireless backhaul trunks.

Syntax

```
bp-uplink-criteria { all-interfaces | interface interface-name } { [ ssid ssid
] [ ipnetaddr ipaddress/numsubnetmaskbits ] [ path-selection { lowest-
weighted-cost | smallest-hop-count | highest-node-priority } ] }
```

Input Parameters

all-interfaces	Apply this command to all radio interfaces.
interface	Apply this command to a specific radio interface.
ssid	Specific SSID to associate with.
ipnetaddr	Specific IP subnet ID to associate with.
path-selection	Path selection criteria for trunk formation with an AP.
• *lowest-weighted-cost*	Associate with an AP that offers lowest weighted cost.
• *smallest-hop-count*	Associate with an AP that is minimum number of hops away from wired network.
• *highest-node-priority*	Associate with an AP that has highest node priority.

Output Parameters

Success or Failure

Description

This command configures the bp-uplink-criteria parameters, which are used as rules based on which wireless backhaul trunks are formed. These parameters restrict association of the BP radios with specific uplink candidate AP radios based on SSID, IP network-address, or path-selection criteria.

Defaults

None

Usage Guidelines

If SSID for bp-uplink-criteria is configured, only AP candidates that advertise the specified SSID are chosen during trunk formation or retrunking (auto or manual).

If IP network address (entered as ip address/subnet mask) is configured for bp-uplink-criteria, the BP radio will select those APs as candidates that advertise the specified subnet. Configuration of IP network address 0.0.0.0 would result in the BP radio ignoring subnet ID as a criteria to select AP candidates for trunk formation.

By setting path-selection criteria, the criterion for selecting the best wireless backhaul path is chosen. When the lowest weighted cost is chosen, candidate parent APs are selected in ascending order of path cost. Path cost is a cumulative metric where each hop contributes a certain value. It factors in the backhaul and non-backhaul traffic load on the candidate AP and quality of the link between the backhaul end points. When smallest hop count is chosen, candidate parents are selected in ascending order of hop count (hop count pertains to number of hops to wired network). When highest node priority is chosen, candidate parents are selected in ascending order of priority determined by the configured uplink bssid list.

It is safe to always use the defaults.

Examples

```
bp-uplink-criteria interface wlan1 ssid “airgo_networks”
```

See Also

```
backhaul(show)> bp-uplink-criteria
backhaul(config)> bp-uplink-bssid-criteria
backhaul(show)> bp-uplink-candidates
```

backhaul(show)> bp-uplink-criteria

Use this command to show the uplink criteria from the point of view of downlink radio.

Syntax

```
bp-uplink-criteria [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is show the current state of bp-uplink-criteria configuration. The information displayed per radio interface includes SSID, IP Subnet, Path Selection criteria, uplink bssid criteria, and uplink bssid list.

Defaults

None

Usage Guidelines

None

Examples

```
backhaul(show)> bp-uplink-criteria

interface      : wlan0
ssid           : DeerCreekCo
path-selection : lowest-weighted-cost
bssid-criteria : accept
bssid          :
--------------------------------------------------------------------------

interface      : wlan1
ssid           : DeerCreekCo
path-selection : lowest-weighted-cost
bssid-criteria : accept
bssid          :
```

See Also

```
backhaul(config)> bp-uplink-criteria
backhaul(config)> bp-uplink-bssid-criteria
backhaul(show)> bp-uplink-candidates
```

backhaul(config)> clear-statistics

Use this command to clear backhaul statistics of a specific radio interface or all radio interfaces of this AP.

Syntax

```
clear-statistics { all-interfaces | interface interface-name }
```

Input Parameters

interface	Optional parameter to specify all or specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to clear accumulated backhaul statistics on a specific or all radio interfaces. After this command is issued, all the counters will be reset to zero.

Defaults

None

Usage Guidelines

Use this command to diagnose specific problems with wireless configuration when you want to determine whether a certain set of packets were exchanged between two backhaul end points.

Examples

```
clear-statistics interface wlan1
```

See Also

```
backhaul(show)> statistics
```

backhaul(config)> reset-to-defaults

Use this command to reset the backhaul configuration to factory defaults.

Syntax

```
reset-to-defaults
```

Input Parameters: None

Output Parameters: None

Success or Failure

Description

This command lets you reset all backhaul configuration parameters to factory defaults.

Defaults

None

Usage Guidelines

This command is useful in reseting selective or full backhaul configuration.

Examples

```
reset-to-defaults
```

See Also

None

backhaul(show)> statistics

Use this command to show wireless backhaul statistics.

Syntax

```
statistics [ interface interface-name]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to show statistics of wireless backhaul uplink and downlink trunks. The statistics include number of transmit and received bytes, number of transmit and received packets, and number of received multicast packets.

Defaults

None

Usage Guidelines

None

Examples

```
backhaul(show)> statistics

interface     : wlan0.tk0
rcv-byte      : 22901
rcv-pkt       : 284
xmt-byte      : 16797
xmt-pkt       : 204
rcv-multicast : 143
```

See Also

None

backhaul(show)> trunk-table

Use this command to show the current uplink (via BP mode radio) and downlink (via AP mode radio) trunks that are formed on this AP.

Syntax

```
trunk-table [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to display list of current uplink and downlink that are formed on this AP.

Defaults

None

Usage Guidelines

This command shows the list of uplink and downlink trunks formed on this AP. To find out stations associated to this AP or specific radio, use the radio(show)> station- association-table command. The information displayed includes the band/channel the wireless trunk is formed on, the number of times retrunking has occurred, and the type of trunk (uplink or downlink).

Examples

```
backhaul(show)> trunk-table

interface       : wlan0
frequency band  : 5GHz
trunk-to-mac    : 00:0a:f5:00:06:17
channel-id      : 64
retrunk count   : 0
trunk-direction : uplink
```

See Also

```
radio(show)> station-association-table
```

2 Bridge CLIs

This chapter includes information about the following bridge commands:

- **bridge(show)> arp-table**
- **bridge(show)> bridge-forwarding-table**
- **bridge(show)> bridge-table**
- **bridge(config)> clear-arp-cache**
- **bridge(config)> clear-statistics**
- **bridge(show)> statistics**
- **bridge(config)> stp**
- **bridge(show)> stp**
- **bridge(config)> stp-portfast**
- **bridge(show)> stp-portfast**

bridge(show)> arp-table

Use this command to display the ARP cache on the access point.

Syntax

```
arp-table
```

Output Parameters

interface	Name of the bridge
ipaddress	Resolved IP address
mac	MAC address corresponding to the resolved IP address

Description

This command displays the ARP cache of the AP, which stores a mapping of IP addresses to their corresponding MAC addresses.

Defaults

Br1, the default bridge, is always present.

Usage Guidelines

This command can be used to verify if the IP to MAC address mapping is up-to-date on the AP if an IP-addressable endpoint on one of the AP’s local subnets becomes unreachable.

Examples

```
bridge(show)> arp-table

interface : br1
ipaddress : 192.168.168.1
mac       : 00:e0:18:fb:f8:ef
---------------------------------------------------------------------------

interface : br1
ipaddress : 192.168.168.24
mac       : 00:0a:f5:00:01:f2
```

See Also

```
bridge(config)> clear-arp-cache
diagnostics(config)> ping
```

bridge(show)> bridge-forwarding-table

Use this command to display the fowarding tables for the bridges instantiated in the AP.

Syntax

```
bridge-forwarding-table [bridge bridge-name]
```

Input Parameters

bridge *bridge-name* (optional) Only show the forwarding table for bridge *bridge-name*. The forwarding tables for all bridges instantiated in the AP are displayed if *bridge-name* is not specified.

Output Parameters

bridge-id Name of the bridge.

interface Name of an interface attached to the bridge.

sta-mac MAC addresses learned on this interface of this bridge.

Description

This command displays the MAC addresses learned by the bridges instantiated in the AP.

Defaults

Br1, the default bridge, and br4094, the bridge used for Spanning Tree Protocol, are always present.

Usage Guidelines

The bridge forwarding table can be used to help locate an endpoint by displaying the bridge port on which an endpoint's MAC address was learned.

Examples

```
bridge(show)> bridge-forwarding-table

bridge-id : br1
interface : eth0
sta-mac   : 00:0a:f5:00:02:9a
--------------------------------------------------------------------------

bridge-id : br1
interface : wlan0.tk0
sta-mac   : 00:08:0d:5c:27:65 00:0a:f5:00:01:f2 00:0a:f5:00:02:e2
00:0a:f5:00:06:ac 00:e0:18:fb:f8:ef
--------------------------------------------------------------------------

bridge-id : br1
interface : wlan1
sta-mac   : 00:0a:f5:00:04:84
--------------------------------------------------------------------------

bridge-id : br4094
interface : eth0
sta-mac   : 00:0a:f5:00:02:9a
--------------------------------------------------------------------------

bridge-id : br4094
```

```
interface : wlan0.tk0
sta-mac   : 00:0a:f5:00:06:17 00:0a:f5:00:06:ac
--------------------------------------------------------------------------

bridge-id : br4094
interface : wlan1
sta-mac   : 00:0a:f5:00:04:84
```

See Also

```
radio(show)> station-association-table
```

bridge(show)> bridge-table

Use this command to display the interfaces attached to the bridges instantiated in the AP.

Syntax

```
bridge-table [bridge bridge-name]
```

Input Parameters

bridge *bridge-name* (Optional) Only show the interfaces attached to bridge *bridge-name*. The bridge tables for all bridges instantiated in the AP are displayed if *bridge-name* is not specified.

Output Parameters

bridge-id Name of the bridge.

interfaces List of interfaces attached to this bridge.

Description

This command displays the list of interfaces attached to each bridge instantiated in the AP.

Defaults

Br1, the default bridge, and br4094, the bridge used for Spanning Tree Protocol, are always present.

Usage Guidelines

This command can be used to verify if the bridges in the AP have been configured with the correct set of interfaces.

Examples

```
bridge(show)> bridge-table

bridge-id  : br1
interfaces : eth0 wlan0.tk0 wlan1
--------------------------------------------------------------------------

bridge-id  : br4094
interfaces : eth0 wlan0.tk0 wlan1
```

See Also

```
vlan(show)> vlan-table
```

bridge(config)> clear-arp-cache

Use this command to clear the access point’s ARP cache.

Syntax

```
clear-arp-cache
```

Description

This command clears the AP’s ARP cache, which stores a mapping of IP addresses to their corresponding MAC addresses.

Defaults

None

Usage Guidelines

Clearing the ARP cache will force the access point to relearn all IP address to MAC address mappings. This is useful when the access point needs to resume communication with an end station whose IP address has changed.

Examples

```
clear-arp-cache
```

See Also

```
bridge(show)> arp-table
```

bridge(config)> clear-statistics

Use this command to clear bridge statistics.

Syntax

```
clear-statistics {all-bridges | bridge bridge-name}
```

Input Parameters

all-bridges	Clear statistics for all bridges.
bridge *bridge-name*	Clear statistics only for bridge *bridge-name*.

Output Parameters

Success or Failure

Description

This command clears the statistics for bridges instantiated in the AP.

Defaults

None

Usage Guidelines

The counters that comprise the bridge statistics are set to zero when cleared.

Examples

```
clear-arp-cache bridge br1
```

See Also

```
bridge(show)> statistics
```

bridge(show)> statistics

Use this command to display the statisics for bridges instantiated on the AP.

Syntax

```
statistics [bridge bridge-name]
```

Input Parameters

bridge *bridge-name* — (Optional) Only show the statistics for bridge *bridge-name*. The statistics for all bridges instantiated on the access point will be displayed if *bridge-name* is not specified.

Output Parameters

bridge-id — Name of the bridge.

rcv-byte — Number of bytes received by all interfaces attached to this bridge.

rcv-pkt — Number of frames received by all interfaces attached to this bridge.

xmt-byte — Number of bytes transmitted by all interfaces attached to this bridge.

xmt-pkt — Number of packets transmitted by all interfaces attached to this bridge.

rcv-multicast — Number of multicast address frames received by all interfaces attached to this bridge.

Description

This command displays the statistics for bridges instantiated on the AP.

Defaults

Br1, the default bridge, and br4094, the bridge used for Spanning Tree Protocol, are always present.

Usage Guidelines

This command can be used to determine the amount of data each bridge forwards to and from its attached interfaces in the AP.

Examples

```
bridge(show)> statistics

bridge-id     : br1
rcv-byte      : 52788
rcv-pkt       : 464
xmt-byte      : 71994
xmt-pkt       : 648
rcv-multicast : 8
--------------------------------------------------------------------------

bridge-id     : br4094
rcv-byte      : 24360
rcv-pkt       : 474
xmt-byte      : 51200
xmt-pkt       : 800
rcv-multicast : 474
```

See Also

```
bridge(config)> clear-statistics
```

bridge(config)> stp

Use this command to enable and disable Spanning Tree Protocol (STP) on the AP.

Syntax

```
stp {disable | enable}
```

Input Parameters

disable	Disables STP.
enable	Enables STP.

Output Parameters

Success or Failure

Description

This command enables and disables STP on the access point.

Defaults

STP is enabled.

Usage Guidelines

The AP runs a single instance of STP on bridge br4094 when enabled. Bridge br4094 contains all interfaces without an IP address assigned.

Examples

```
stp disable
```

See Also

```
bridge(show)> stp
```

bridge(show)> stp

Use this command display administrative status of the Spanning Tree Protocol (STP) on the AP.

Syntax

```
stp
```

Output Parameters

stp	Spanning Tree Protocol status.

Description

This command displays whether STP is enabled or disabled in the AP.

Defaults

None

Usage Guidelines

This command can be used to check if STP has been enabled or disabled in the AP.

Examples

```
bridge(show)> stp-portfast

interface      : backhauls
portfast-state : auto
--------------------------------------------------------------------------

interface      : wlan0
portfast-state : disable
-------------------------------------------------------------------------

interface      : wlan1
portfast-state : disable
-------------------------------------------------------------------------

interface      : eth0
portfast-state : enable
```

See Also

```
bridge(config)> stp
```

bridge(config)> stp-portfast

Use this command to enable or disable fast Spanning Tree Protocol (STP) port state transition.

Syntax

```
stp-portfast {all-interfaces | backhaul-interfaces | interface interface-name}
{disable | enable | auto-for-backhaul}
```

Input Parameters

all-interfaces	Apply stp-portfast state for all interfaces.
backhaul-interfaces	Apply stp-portfast state for backhaul interfaces only.
interface *interface-name*	Apply stp-portfast state for the specified interface.
disable	Never transition a bridge interface to the forwarding state quickly.
enable	Always transition a bridge interface to the forwarding state quickly.
auto-for-backhaul	Have the AP automatically determine when to transition backhaul interfaces to the forwarding state quickly.

Output Parameters

Success or Failure

Description

This command controls which bridged interfaces the AP can transition into the forwarding state without the delays incurred in the listening and learning STP states. Bridge interfaces are interfaces that have not been assigned an IP address. When fast transitioning into the forwarding state is automatically determined, the AP and backhaul point will transition their corresponding backhaul interfaces quickly to the forwarding state if the backhaul point is not attached to the wired network.

Defaults

The AP automatically determines when to enable stp-portfast for backhaul interfaces. The stp-portfast is enabled for the wired interface, disabled for the wireless interface.

Usage Guidelines

Caution must be used when applying this command because it can result in undesirable network behavior. Disabling fast STP forwarding state transitions for backhaul interfaces may result in service interrupts when a backhaul point retrunks to a different access point. Enabling fast STP forwarding state transitions for backhaul interfaces may result in the formation of a bridge loop if both the AP and backhaul point are attached to the wired network. Enabling fast STP forwarding state transitions on wired or wireless interfaces may result in packets destined for local endpoints to be forwarded to other bridge ports and bridge loops being formed.

Examples

```
stp-portfast interface eth0 disable
```

See Also

```
bridge(show)> stp-portfast
```

bridge(show)> stp-portfast

Use this command display configured stp-portfast state for all interfaces in the AP.

Syntax

```
stp-portfast
```

Output Parameters

interface	Interface attached to a bridge
portfast-state	Configured stp-portfast state

Description

This command displays the configured stp-portfast state for all interfaces in the AP.

Defaults

None

Usage Guidelines

This command can be used to check the stp-portfast state of an interface when it is attached to a bridge instantiated in the AP.

Examples

```
bridge(show)> stp-portfast

interface      : backhauls
portfast-state : auto
------------------------------------------------------------------------------

interface      : wlan0
portfast-state : disable
------------------------------------------------------------------------------

interface      : wlan1
portfast-state : disable
------------------------------------------------------------------------------

interface      : eth0
portfast-state : enable
```

See Also

```
bridge(config)> stp-portfast
```

3 DHCP Server CLIs

This chapter includes information about the following DHCP server commands:

- **dhcp-server(config)> add-ipaddress-range**
- **dhcp-server(config)> add-static-ipaddress**
- **dhcp-server(config)> admin-state**
- **dhcp-server(config)> delete-ipaddress-range**
- **dhcp-server(config)> delete-static-ipaddress**
- **dhcp-server(config)> dns-server**
- **dhcp-server(config)> gateway**
- **dhcp-server(show)> global-options**
- **dhcp-server(show)> ipaddress-range-table**
- **dhcp-server(show)> lease-table**
- **dhcp-server(config)> lease-time**
- **dhcp-server(config)> max-leases**
- **dhcp-server(config)> ntp-servers**
- **dhcp-server(show)> static-ipaddress-table**
- **dhcp-server(config)> wins-server**

dhcp-server(config)> add-ipaddress-range

Use this command to add a range of IP addresses that the DHCP server should serve.

Syntax

```
{ ipaddress-range ipaddress/numsubnetmaskbits } | { start-ipaddress ipaddress
end-ipaddress  ipaddress }
```

Input Parameters

ipaddress-range	The IP address and number of mask bits specified as A.B.C.D/N.
start-ipaddress	The starting IP address.
end-ipaddress	The ending IP address.

Output Parameters

Success or Failure	Command can fail if the address is not valid.

Description

This command is used to add a range of IP addresses that the DHCP server should serve. The range of addresses that the DHCP Server should server can be specified in one of two formats:

- As an address range specified by A.B.C.D/N, example: 192.168.10.0/24 where 24 represents the number of mask bits and is equivalent to 255.255.255.0
- As a start and end address.

The address range specified should fall within the subnet associated with the IP address of the default VLAN.

The DHCP server supports only one address range.

Once an address range has been added the server must be stopped and restarted for the new range to take effect.

Usage Guidelines

Configure an IP address range then restart the server using the admin-state command.

Examples

```
add-ipaddress-range ipaddress-range 192.168.10.0/24
```

See Also

```
vlan-table delete-ipaddress-range, admin-state, ipaddress-range-table
```

dhcp-server(config)> add-static-ipaddress

Use this command to configure a fixed IP address for a known MAC address.

Syntax

```
fqdn fqdn host-mac mac-address static-ipaddress ipaddress-and-nummaskbits
```

Input Parameters

fqdn	The fully qualified domain name
host-mac	The MAC address for which the IP address is specified
static-ipaddress	The IP address that should be assigned for the above MAC address

Output Parameters

Success or Failure

Description

Use this command to establish a fixed IP address for a known MAC address. After this static address has been set up, whenver a DHCP request for an IP address is received by the DHCP server from the configured MAC address, the statically configured IP address is returned.

The static IP address configured must fall within the address range configured using the add-ipaddress-range command. The server must be stopped and restarted for the changes to take effect. The fully qualified name of the client is tracked, but not distributed to the client.

Defaults

None

Usage Guidelines

Configure Static IP to MAC address mapping when the set of DHCP clients is known and they need a fixed IP address. If the DHCP clients keep changing over time then it is preferable not to fix the client addresses.

Examples

```
add-static-ipaddress fqdn mypc.abc.com host-mac 00:01:0a:02:03:0F static-
ipaddress 192.168.10.2/24
```

See Also

```
delete-static-ipaddress, static-ipaddress-table
```

dhcp-server(config)> admin-state

Use this command to stop or start the DHCP server.

Syntax

```
{ disable | enable }
```

Input Parameters

disable/enable	Disable – Stops the server. Enable – Starts the server.

Output Parameters

Success or Failure

Description

Use this command to stop or start the DHCP server.

Defaults

None

Usage Guidelines

When any DHCP server configuration change is made this command should be used to stop and restart the server for the changes to take effect.

dhcp-server(config)> delete-ipaddress-range

Use this command to delete the address range that has been configured for the DHCP server.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to delete the IP address range that had been configured for the DHCP server. After the address range has been deleted, the DHCP server must be stopped and restarted using the admin-state command for the configuration change to take effect.

Defaults

None

See Also

`ipaddress-range-table, admin_state`

dhcp-server(config)> delete-static-ipaddress

Use this command to delete a configured MAC to IP address mapping.

Syntax

```
{ all-entries | { host-mac mac-address } }
```

Input Parameters

all-entries	Delete all configured entries.
host-mac	Delete the mapping for the specified MAC address.

Output Parameters

Success or Failure

Description

Use this command to delete a MAC to IP address mapping or to delete all the MAC to IP address mappings. The server must be restarted for the change to take effect.

Defaults

None

Examples

```
delete-static-ipaddress host-mac 00:01:0a:02:03:0F
```

See Also

```
admin-state
```

dhcp-server(config)> dns-server

Use this command to configure the set of DNS servers that the DHCP server should offer.

Syntax

```
dns-server-address ipaddress {…}
```

Input Parameters

dns-server-address	The list of DNS server addresses that the DHCP server should offer.

Output Parameters

Success or Failure

Description

Use this command to configure the set of DNS servers that the DHCP server should offer.

Defaults

None

Usage Guidelines

See Also

```
admin-state
```

dhcp-server(config)> gateway

Use this command to configure the default gateway that the DHCP server should offer.

Syntax

```
gateway-address ipaddress
```

Input Parameters

gateway-address	The default gateway address that the DHCP server should offer.

Output Parameters

Success or Failure

Description

Use this command to configure the default gateway address that the DHCP server should offer.

Defaults

None

Usage Guidelines

See Also

```
admin-state, global-options
```

dhcp-server(show)> global-options

Use this command to view the configured global options for the DHCP server.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to view the currently configured set of global DHCP server options, such as max-leases.

Defaults

None

Usage Guidelines

Examples

```
dhcp-server(show)> global-options

lease-time : 1
-----------------------------------------------------------------------

ntp-server : 192.168.168.1
```

See Also

```
max-leases
```

dhcp-server(show)> ipaddress-range-table

Use this command to view the configured IP address range for the DHCP server.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to view the currently configured IP address range for the DHCP server.

Defaults

None

Usage Guidelines

Examples

```
dhcp-server(show)> ipaddress-range-table

interface : br1
iprange   : 192.168.168.0/24
startip   : 192.168.168.200
endip     : 192.168.168.225
```

See Also

```
add-ipaddress-range
```

dhcp-server(show)> lease-table

Use this command to view the currently leased IP addresses.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to view the currently leased IP addresses.

Defaults

None

Usage Guidelines

Examples

```
dhcp-server(show)> lease-table

mac                  : 00:0a:f5:00:06:8b
leased-ip            : 192.168.168.200
remaining-lease-time : 0 days, 0 hours, 59 minutes, 2 seconds
```

See Also

```
add-ipaddress-range
```

dhcp-server(config)> lease-time

Use this command to configure the lease time that the DHCP server should offer.

Syntax

```
lease-time hours
```

Input Parameters

lease-time	The lease time for the address in hours.

Output Parameters

Success or Failure

Description

Use this command to configure the lease time for the allocated address in hours.

Defaults

None

Usage Guidelines

See Also

```
admin-state, global-options
```

dhcp-server(config)> max-leases

Use this command to configure the total number of leases that the DHCP server should offer.

Syntax

```
max max-leases
```

Input Parameters

max	The total number of IP addresses to be leased out by the server.

Output Parameters

Success or Failure

Description

Use this command to configure the total number of leases that the DHCP server should offer. This command controls the number of IP addresses that the DHCP server will lease out, irrespective of the size of the subnet configured.

Defaults

None

Usage Guidelines

The total number of addresses that may be offered by the DHCP server is determined by the configured subnet. If this address range is large and if the number of clients are large then the load on the DHCP server will be high as it will have to service all the clients. Use this command to restrict the number of clients that the DHCP server will actively serve.

See Also

`admin-state, global-options, add-ipaddress-range`

dhcp-server(config)> ntp-servers

Use this command to configure the set of NTP servers that the DHCP server should offer.

Syntax

```
host ipaddress {…}
```

Input Parameters

host	The list of NTP server addresses that the DHCP server should offer.

Output Parameters

Success or Failure

Description

Use this command to configure the set of NTP servers that the DHCP server should offer.

Defaults

None

Usage Guidelines

See Also

`admin-state, global-options`

dhcp-server(show)> static-ipaddress-table

Use this command to view the currently configured static IP address table..

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to view the currently configured static IP address table.

Defaults

None

Usage Guidelines

Examples

```
dhcp-server(show)> static-ipaddress-table

fqdn      : a@airgodemo.com
mac       : 00:0a:f5:00:05:fe
static-ip : 192.168.168.201/24
```

See Also

```
add-static-ipaddress
```

dhcp-server(config)> wins-server

Use this command to configure the set of WINS servers that the DHCP server should offer.

Syntax

```
wins-server-address ipaddress {…}
```

Input Parameters

wins-server-address	The list of WINS server addresses that the DHCP server should offer.

Output Parameters

Success or Failure

Description

Use this command to configure the set of WINS servers that the DHCP server should offer.

Defaults

None

Usage Guidelines

See Also

`admin-state, global-options`

4 Filter CLIs

This chapter includes information about the following filter commands:

- **filter(config)> add-ethertype-filter**
- **filter(config)> clear-statistics**
- **filter(config)> delete-ethertype-filter**
- **filter(show)> filter-table**
- **filter(show)> statistics**

filter(config)> add-ethertype-filter

Use this command to create or modify EtherType filters.

Syntax

```
add-ethertype-filter interface interface-name [accept | discard] [ingress |
egress] {unmatched | {ethertype ethertype{…}}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface on which the filter will be created.
accept	(Optional) Allow frames satisfying this filter to pass through the access point. This is the default if filter action is not specified.
discard	(Optional) Drop frames satisfying this filter.
ingress	(Optional) Apply filter to frames as they are received. This is the default if filter direction is not specified.
egress	(Optional) Apply filter to frames as they are transmitted.
unmatched	This is the filter that is applied when a frame does not satisfy any filter for a specific EtherType.
ethertype *ethertype {…}*	Specify one or more EtherTypes for a filter.

Output Parameters

Success or Failure

Description

This command adds a filter to an interface that will be applied to either incoming or outgoing frames.

Defaults

The AP creates the umatched filter for all interfaces automatically to accept frames of all EtherTypes.

Usage Guidelines

Use this command to change the behavior of existing EtherType filters as well as create new ones.

Examples

```
add-ethertype-filter interface eth0 ingress discard ethertype “0x8137 0x8053”
```

See Also

```
filter(config)> delete-ethertype-filter
filter(show)> filter-table
```

filter(config)> clear-statistics

Use this command to clear EtherType filters statistics.

Syntax

```
clear-statistics {all-interfaces | interface interface-name}
```

Input Parameters

all-interfaces	Clear filter statistics for all interfaces.
interface *interface-name*	Clear filter statistics for interface *interface-name.*

Output Parameters

Success or Failure

Description

This command clears EtherType filter statistics.

Defaults

None

Usage Guidelines

The EtherType filter statistics are set to zero when cleared.

Examples

```
delete-ethertype-filter interface eth0 ingress ethertype "0x8137 0x8053"
```

See Also

```
filter(show)> statistics
```

filter(config)> delete-ethertype-filter

Use this command to remove EtherType filters.

Syntax

```
delete-ethertype-filter interface interface-name {{all-filters | all-ingress-
filters | all-egress-filters} | {[ingress | egress] {ethertype ethertype{…}}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface on which the filter will be created.
all-filters	Remove all ingress and egress filters.
all-ingress-filters	Remove all filters for incoming traffic.
all-egress-filters	Remove all filters for outgoing traffic.
ingress	(Optional) Apply filter to frames as they are received. This is the default if filter direction is not specified.
egress	(Optional) Apply filter to frames as they are transmitted.
ethertype *ethertype {…}*	Specify one or more EtherTypes for a filter.

Output Parameters

Success or Failure

Description

This command removes filters for specific EtherTypes.

Defaults

None

Usage Guidelines

Interfaces’ unmatched filter cannot be deleted. When all-filters, all-ingress-filters, or all-egress-fitters is specified, the corresponding unmatched filter behavior for the interface will revert to accept all frames.

Examples

```
delete-ethertype-filter interface eth0 ingress ethertype “0x8137 0x8053”
```

See Also

```
filter(config)> add-ethertype-filter
filter(show)> filter-table
```

filter(show)> filter-table

Use this command to display EtherType filters.

Syntax

```
filter-table [interface interface-name]
```

Input Parameters

interface *interface-name* — (optional) Display the Ethertype filters created on interface *interface-name*. Filters created for all interfaces are displayed if *interface-name* is not specified.

Output Parameters

interface — Name of the interface.

direction — Direction of the traffic to which the filter will be applied.

policy — Action of the filter when a filter is applied.

unmatched — Indicates this filter will be applied to frames which do not satisfy filters with a specify EtherType.

ethertype — The Ethertype a frame must contain before this filter is applied.

Description

This command displays EtherTypes created on the access point.

Defaults

None

Usage Guidelines

This command can be used to verify whether the desired EtherType filters have been created on the appropriate interfaces.

Examples

```
filter(show)> filter-table

interface : eth0
direction : ingress
policy    : accept
unmatched :
--------------------------------------------------------------------------

interface : eth0
direction : egress
policy    : accept
unmatched :
--------------------------------------------------------------------------

interface : wlan0
direction : ingress
policy    : accept
unmatched :
---------------------------------------------------------------------------
```

```
interface : wlan0
direction : egress
policy    : accept
unmatched :
-------------------------------------------------------------------------

interface : wlan1
direction : ingress
policy    : accept
unmatched :
-------------------------------------------------------------------------

interface : wlan1
direction : egress
policy    : accept
unmatched :
--------------------------------------------------------------------------

interface : wlan1.tk0
direction : ingress
policy    : accept
unmatched :
--------------------------------------------------------------------------

interface : wlan1.tk0
direction : egress
policy    : accept
unmatched :
```

See Also

```
filter(config)> add-ethertype-filter
filter(config)> delete-ethertype-filter
```

filter(show)> statistics

Use this command to display EtherType filters statistics.

Syntax

```
statistics
```

Output Parameters

interface	Name of the interface.
direction	Direction of the traffic to which the filter was be applied.
unmatched	Indicates this filter was applied to frames which did not satisfy filters with a specify EtherType.
ethertype	The Ethertype a frame contained when this filter was applied.
numofhits	Number of times this filter was applied.

Description

This command display EtherType filter statistics.

Defaults

None

Usage Guidelines

This command can be used to determine the number of times a filter has been applied.

Examples

```
filter(show)> statistics

interface : eth0
direction : ingress
policy    : accept
unmatched :
numofhits : 6964
---------------------------------------------------------------------------

interface : eth0
direction : egress
policy    : accept
unmatched :
numofhits : 5855
---------------------------------------------------------------------------

interface : wlan0
direction : ingress
policy    : accept
unmatched :
numofhits : 0
---------------------------------------------------------------------------

interface : wlan0
direction : egress
policy    : accept
unmatched :
```

```
numofhits : 2085
---------------------------------------------------------------------------

interface : wlan1
direction : ingress
policy    : accept
unmatched :
numofhits : 1253
---------------------------------------------------------------------------

interface : wlan1
direction : egress
policy    : accept
unmatched :
numofhits : 3219
---------------------------------------------------------------------------

interface : wlan1.tk0
direction : ingress
policy    : accept
unmatched :
numofhits : 2923
--------------------------------------------------------------------------

interface : wlan1.tk0
direction : egress
policy    : accept
unmatched :
numofhits : 3769
```

See Also

```
filter(config)> clear-statistics
```

5 Guest Access CLIs

This chapter includes information about the following guest access commands:

- **guest-access(config)>clear-statistics [HEAP2]**
- **guest-access(config)>guest-password**
- **guest-access(show)>statistics [HEAP2]**
- **portal(config)>auto-guest-password**
- **portal(show)>auto-guest-password**
- **ssid(config)>disable-guest-access**
- **ssid(config)> disable-guest-access**
- **ssid(config)>enable-guest-access**
- **ssid(show)>guest-access**

guest-access(config)>clear-statistics [HEAP2]

To be provided later for HEAP2.

guest-access(config)>guest-password

Use this command to configure the local guest-access password on this AP.

Syntax

`guest-password` **`new-password`** *`password`* **`confirm-password`** *`password`*

Input Parameters

new-password	Specifies the password to be used to authenticate a guest user on the AP’s internal landing page.
confirm-password	Confirms the password to be used to authenticate a guest user on the AP’s internal landing page.

Output Parameters

Success or Failure

Description

This command is used to configure the local guest-access password on this AP.

Defaults

None

Usage Guidelines

The guest landing pages on an AP (internal landing pages) provides web-based password authentication. This command sets the guest password when guest access is enabled on an SSID and guest access uses the internal landing page.

Guest-access passwords may also be set with the auto-guest-password command on a portal AP. This is a different password and identity than the local guest password and are (unlike this local password) available to all APs that have the NM/portal AP configured as their authentication server. This is a RADIUS based password that is a complimaentary mechansim to the guest password local to the AP.

When an external-landing-page is selected, all guest autentication for the SSID is provided by an external web server.

Examples

```
guest-password new-password hoxawuki confirm-password hoxawuki
```

See Also

```
portal(config)>auto-guest-password
portal(show)>auto-guest-password
ssid(config)>enable-guest-access
ssid(show)>guest-access
guest-access(config)>guest-access-password
```

guest-access(show)>statistics [HEAP2]

To be provided later for HEAP2.

portal(config)>auto-guest-password

Use this command to configure the automatic generation of guest passwords.

Syntax

```
auto-guest-password { { disable } | { enable { daily | weekly | 2-hours | 4-
hours | 8-hours | 12-hours } } }
```

Input Parameters

enable	Configure automatic generation of passwords for the guest access user supported by this NM/portal.
disable	Turn off the auto-generation of guest-access passwords on this portal AP.
daily, weekly, 2-hours, 4-hours, 8-hours, 12-hours	Specify how often the guest-access password is changed and distributed.

Output Parameters

Success or Failure

Description

This command is used to enable or disable the automatic generation of the guest passwords used by the internal landing page for guest authentication. An interval must be configured to determine how often the password is changed.

Defaults

Automatic generation of guest-access passwords is disabled by default.

Usage Guidelines

Guest users will typically be given a password by a reciptionist or administor to enable limited access to the wireless network. The shared guest passwords need to be changed on a regular basis to prevent inappropriate reuse of the passwords. The auto-generated passwords simplify the admistration of the guest access by periodically changing the password and distributing the password automatically.

The generated passwords are pronouncible passwords that are placed into the Sec/P RADIUS server. The AP’s internal landing page checks validity by examining both the local guest password and the SSIDs RADIUS server for a guest identitiy. The password is then available for guest use by any enrolled AP. This password is only usable for guest access and only used for internal landing pages.

After a guest-access password is generated, the new password is e-mailed to the administrator email account configured for this NM/portal. This allows the password to be redistributed as appropriate.

Examples

```
auto-guest-password enable 2-hours
auto-guest-password disable
```

See Also

```
portal(show)> auto-guest-password
system(config)> email
ssid(config)> enable-guest-access
ssid(show)> guest-access
guest-access(config)>guest-password
```

portal(show)>auto-guest-password

Use this command to show the auto-generated guest password that is currently active on this portal.

Syntax

```
auto-guest-password
```

Input Parameters

NA	None.

Output Parameters

login	RADIUS “username” for the Guest Access authentication “user”. Always shows __guest__.
password	The current eight character, random, pronouncible, password.
admin-state	This shows if automatically generated guest passwords are enabled or disabled.
periodic	This shows the periodic after which a new guest-access password will be generated.

Description

The command is used to display the current settings affecting the automatic generation of passwords on the portal. These passwords are used in the authentication of guest-access clients that use the internal landing page.

Defaults

Automatic generation of guest-access passwords is disabled by default. See the auto-guest-password enable command for how to enable.

Usage Guidelines

The current automatic guest password and password validity period can be viewed.

Examples

```
auto-guest-password
```

See Also

```
portal(config)> auto-guest-password
guest-access(config)>guest-password
```

ssid(config)>disable-guest-access

Use this command to disable guest-access authentication and services on an SSID.

Syntax

```
disable-guest-access { { all-ssids } | { ssid ssid } }
```

Input Parameters

all-ssids	Specifies that guest access is disabled on all SSIDs.
ssid	Specifies the SSID on which to disable guest access.

Output Parameters

Success or Failure

Description

This command is used to disable guest-access authentication and services on the specified SSID. It can also be used to disable guest authentication and services on all SSIDs.

Defaults

None

Usage Guidelines

Used to disable guest authentication and network services for guests on an SSID. Guest traffic is usually segregated from enterprise user traffic. With guest access disabled, the only acccess permitted on this SSID will be through the other service profiles that are bound to this SSID.

Examples

```
disable-guest-access ssid guestPortal
disable-guest-access all-ssids
```

See Also

```
ssid(config)> enable-guest-access
ssid(show)> guest-access
```

ssid(config)> disable-guest-access

Use this command to disable Guest Access authentication and services on an SSID.

Syntax

```
disable-guest-access [ ssid ssid service-profile profilename] {{internal-
landing-page} | {external-landing-page landingpage-url server-secret
password}} {open-access ipaddress/nummaskbits}
```

Input Parameters

all-ssids	Specifies that guest-access is disabled on all SSIDs.
ssid	Specifies the SSID on which to disable guest access.

Output Parameters

Success or Failure

Description

This command is used to disable guest-access authentication and services on a single SSID or all SSIDs.

Defaults

None

Usage Guidelines

Used to disable guest authentication and network services for guests on an SSID. Guest traffic is usually segregated from enterprise user traffic. With guest access disabled, the only acccess permitted on this SSID will be through the other service profiles that are bound to this SSID.

Examples

```
disable-guest-access ssid guestPortal
```

See Also

```
ssid(config)> enable-guest-access
ssid(show)> guest-access
```

ssid(config)>enable-guest-access

Use this command to enable guest-access authentication and services on an SSID.

Syntax

```
enable-guest-access [ ssid ssid service-profile profilename] {{internal-
landing-page} | {external-landing-page landingpage-url server-secret
password}} {open-access ipaddress/nummaskbits}
```

Input Parameters

ssid	Specifies the SSID.
service-profile	Identifies the service profile that will be enabled for guest access.
internal-landing-page	Specifies that the landing page internal to the access point will be used for authenticating “guest” stations.
external-landing-page	Specifies that a web server external to the access point will be used as the landing page for guest users.
landingpage-url	If the external-landing-page is selected, then a URL to this page must be entered.
server-secret	The server secret shared with the external landing page server.
open-access	Used to configure a subnet that guest stations may access – even BEFORE completing authentication.

Output Parameters

Success or Failure

Description

This command enables guest-ccess authentication and services on the specified SSID. A service profile is bound to an SSID that determines the nework services provided to authenticated guest stations. The type of landing page and an optional open-access subnet can be configured.

Usage Guidelines

Guest stations are users that do not match the authentication requirements of the other profiles bound to an SSID. This allows unregistered guests to associate to an AP and subsequently use web based authentication. When guest stations are associated, they are able to be obtain an IP address (DHCP) and use DNS services. Other network communications are blocked and all web traffic (HTTP and HTTPS) outside of an open-access range are captured and redirected to a landing page. The optionally open-access range can be reached without web authentication and must be a single contiguous subnet. The landing page can be either an internal landing page or an external landing page. The external landing page requires a shared secret to be configured to provide secure communications between the external server and the AP.

Examples

```
enable-guest-access ssid guestPortal service-profile guest-profile
                    internal-landing-page open-access 192.168.254.19/32
enable-guest-access ssid guestPortal service-profile guest-profile
                    external-landing-page open-access 192.168.254.19/32
```

See Also

```
ssid(config)> disable-guest-access
ssid(show)> guest-access
portal(config)> auto-guest-password
guest-access(config)>guest-password
```

ssid(show)>guest-access

Use this command to show the current guest-access authentication and services settings on an SSID.

Syntax

```
guest-access { ssid ssid }
```

Input Parameters

ssid	Specifies the SSID for which to display guest-access settings.

Output Parameters

ssid	The SSID.
profile	The service profile which determines the networks service provided to the guest stations.
internal-landing-page	Indicates that the internal-landing-page is configured for guest station authentication on this SSID.
external-landing-page	Specifies the URL to use to authenticate guest stations on this SSID.

Description

This command is used to show the current guest-access authentication and services settings on an SSID.

Defaults

Defaults to the currently active SSID if multiple SSIDs are not enabled.

Usage Guidelines

Used to display the current guest-access authentication and services settings on an SSID.

Examples

```
guest-access ssid guestPortal
```

See Also

```
ssid(config)> enable-guest-access
ssid(config)> disable-guest-access
```

6 Interface CLIs

This chapter includes information about the following interface commands:

- **interface(config)> add-ipaddress**
- **interface(config)> admin-state**
- **interface(config)> clear-statistics**
- **interface(config)> delete-ipaddress**
- **interface(config)> encapsulation-format**
- **interface(show)> encapsulation-format**
- **interface(show)> interface-table**
- **interface(show)> statistics**

interface(config)> add-ipaddress

Use this command to assign an IP address to an interface.

Syntax

```
add-ipaddress interface interface-name ipaddress ip-address/subnet-mask-
length
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface to which the IP address will be assigned.
ipaddress *ip-address/ subnet-mask-length*	The IP address and subnet mask to be assigned to *interface-name*.

Output Parameters

Success or Failure

Description

This command assigns an IP address and subnet mask to an interface. The subnet mask is specified by its bit length. (For example, 255.255.255.0 has a subnet mask length of 24.)

Defaults

None

Usage Guidelines

When an interface is assigned an IP address, the interface becomes routable and will be removed from the default bridge, br1, and the STP bridge, br4094. An IP address cannot be assigned to an interface belonging to any other bridges. For example, this command will fail if the interface has been added to a user created VLAN.

Examples

```
add-ipaddress interface eth0 ipaddress 10.1.2.3/24
```

See Also

```
interface(config)> delete-ipaddress
interface(show)> interface-table
```

interface(config)> admin-state

Use this command to enable and disable an interface on the AP.

Syntax

```
admin-state interface interface-name {disable | enable}
```

Input Parameters

interface *interface-name*	The name of the interface to enable or disable.
disable	Disables *interface-name*.
enable	Enables *interface-name*.

Output Parameters

Success or Failure

Description

This command enables and disables the Ethernet interface on the AP.

Defaults

None

Usage Guidelines

Use radio(config)> admin-state to enable or disable radio interfaces.

Examples

```
admin-state interface eth0 disable
```

See Also

```
interface(show)> interface-table
radio(config)> admin-state
```

interface(config)> clear-statistics

Use this command to clear interface statistics on the AP.

Syntax

```
clear-statistics {all-interfaces | interface interface-name}
```

Input Parameters

all-interfaces	Clear statistics for all interfaces.
interface *interface-name*	Clear statistics for interface *interface-name*.

Output Parameters

Success or Failure

Description

This command clears the statistics for interfaces on the AP.

Defaults

None

Usage Guidelines

The counters that comprise the interface statistics are set to zero when cleared.

Examples

```
clear-statistics interface wlan0
```

See Also

```
interface(show)> statistics
```

interface(config)> delete-ipaddress

Use this command to remove an IP address from an interface.

Syntax

```
delete-ipaddress interface interface-name
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface to which the IP address will be assigned.

Output Parameters

Success or Failure

Description

This command removes an IP address from an interface.

Defaults

None

Usage Guidelines

When the IP address has been removed from an interface, that interface become unroutable. Consequently, the AP will make the interface a part of the default bridge, br1, and the STP bridge, br4094.

Examples

```
delete-ipaddress interface eth0
```

See Also

```
interface(config)> add-ipaddress
interface(show)> interface-table
```

interface(config)> encapsulation-format

Use this command to change the 802.11 frame encapsulation format of the AP.

Syntax

```
encapsulation-format {802.1h-translated | encapsulated}
```

Input Parameters

802.1h-translated	Ethernet frames will be translated to 802.11 frames per 802.1h.
encapsulated	The entire Ethernet frame will be forwarded in the 802.11 frame payload.

Output Parameters

Success or Failure

Description

This command modifies the 802.11 frame encapsulation format for the AP.

Defaults

802.1h-translated

Usage Guidelines

The encapsulated mode is provided to interoperate with older 802.11 equipment that does not comply with WECA interoperability requirements.

Examples

```
encapsulation-format 802.1h-translated
```

See Also

```
interface(show)> encapsulation-format
```

interface(show)> encapsulation-format

Use this command to display the 802.11 frame encapsulation format of the AP.

Syntax

```
encapsulation-format
```

Output Parameters

802.1h	Ethernet frames are translated per 802.1h to 802.11 frames.
encapsulated	The entire Ethernet frame will be forwarded in the 802.11 frame payload.

Description

This command displays the 802.11 frame encapsulation format for the AP.

Defaults

None

Usage Guidelines

The command can be used to display the current 802.11 frame encapsulation format of the AP.

Examples

```
interface(show)> encapsulation-format

encapsulation format : 802.1h
```

See Also

```
interface(config)> encapsulation-format
```

interface(show)> interface-table

Use this command to display information about the interfaces of the AP.

Syntax

```
interface-table [interface interface-name]
```

Input Parameters

interface *interface-name*

(Optional) Display information for interface *interface-name*. Information for all interfaces in the access point is displayed if *interface-name* is not specified.

Output Parameters

interface

Name of the interface.

ipaddress

IP address and subnet mask length assigned to the interface.

admin-state

Administrative state of the interface.

operation-state

Operational state of the interface is the combination of the administrative state and the interface’s actual readiness for data transfer.

mac

MAC address of the interface.

Description

This command displays information for interfaces in the AP.

Defaults

Information for all interfaces in the AP is displayed.

Usage Guidelines

The command can be used to verify the configuration for each interface in the AP.

Examples

```
interface(show)> interface-table interface wlan1

interface       : wlan1
ipaddress       : 0.0.0.0/0
admin-state     : enable
operation-state : up
mac             : 00:0a:f5:00:06:1
```

See Also

```
interface(config)> add-ipaddress
interface(config)> admin-state
interface(config)> delete-ipaddress
```

interface(show)> statistics

Use this command to display interface networking statistics.

Syntax

```
statistics [interface interface-name]
```

Input Parameters

interface *interface-name*
(Optional) Display statistics for interface *interface-name.* Statistics for all interfaces in the access point are displayed if *interface-name* is not specified.

Output Parameters

interface
Name of the interface.

rcv-byte
Number of bytes the interface has received.

rcv-pkt
Number of frames the interface has received.

xmt-byte
Number of bytes the interface has transmitted.

xmt-pkt
Number of frames the interface has transmitted.

rcv-multicast
Number of multicast addressed frames received.

Description

This command displays networking statistics for interfaces in the AP.

Defaults

Networking statistics for all interfaces in the AP are displayed.

Usage Guidelines

The command can be used to verify the configuration for each interface in the AP.

Examples

```
interface(show)> statistics interface wlan1

interface          : wlan1
rcv-byte           : 6787
rcv-pkt            : 55
xmt-byte           : 14568
xmt-pkt            : 302
rcv-multicast      : 0
rx-error-pkts      : 0
rx-drop-pkts       : 33
rx-misaligned-pkts : 33
rx-fifo-errors     : 0
tx-error-pkts      : 0
tx-drop-pkts       : 62
```

See Also

```
interface(config)> clear-statistics
```

7 IP Route CLIs

This chapter includes information about the following IP route commands:

- **ip-routing(config)> add-route**
- **ip-routing(config)> delete-route**
- **ip-routing(show)> route-table**

ip-routing(config)> add-route

Use this command to add an IP route to AP.

Syntax

```
add-route dest-ip ip-address/subnet-mask-length gateway-ipaddress gateway-ip-
address [interface interface-name | vlan-id vlan-id]
```

Input Parameters

dest-ip *ip-address/ subnet-mask-length*
Specifies *ip-address/subnet-mask-length* as the destination IP subnet address.

gateway-ipaddress *gateway-ip-address*
Specifies *gateway-ip-address* as the next-hop router for IP packets destined to the IP subnet specified by dest-ip.

interface *interface-name*
(Optional) Specifies *interface-name* as the interface through which the gateway can be reached.

vlan-id *vlan-id*
(Optional) Specifies *vlan-id* as the VLAN through which the gateway can be reached.

Output Parameters

Success or Failure

Description

This command adds an IP route to the AP's IP route table.

Defaults

None

Usage Guidelines

This command can be used to specify the next-hop router IP packets will be forwarded to when the AP is operating as an IP packet forwarding device. Use dest-ip *0.0.0.0/0* to specify the default route. Use dest-ip *A.B.C.D/32* to specify a host route. If the egress interface or VLAN is not specified, the AP will attempt to determine the appropriate output port to transmit an IP packet based on pre-existing routes. The AP automatically inserts routes into its route table for local subnets that are reachable directly through one of the AP's interfaces or VLANs.

Examples

```
add-route dest-ip 0.0.0.0/0 gateway-ipaddress 192.168.88.254 vlan-id 1
```

See Also

```
ip-routing(config)> delete-route
ip-routing(show)> route-table
system(config)> mgmt-ipaddress
```

ip-routing(config)> delete-route

Use this command to delete an IP route from the AP.

Syntax

```
delete-route {all-routes | dest-ip ip-address/subnet-mask-length [interface
interface-name | vlan-id vlan-id] }
```

Input Parameters

all-routes	Remove all routes from the AP except the default and interface routes.
dest-ip *ip-address/ subnet-mask-length*	Remove the route to subnet address *ip-address/subnet-mask-length.*
vlan-id *vlan-id*	Remove the route using VLAN *vlan-id* as the egress port.
interface *interface-name*	Remove the route using interface *interface-name* as the egress port.

Output Parameters

Success or Failure

Description

This command deletes an IP route from the AP's IP route table.

Defaults

None

Usage Guidelines

This command can be used to remove a route from the AP's route table. Use dest-ip 0.0.0.0/0 to specify the default route.

Examples

```
delete-route dest-ip 0.0.0.0/0
```

See Also

```
ip-routing(config)> add-route
ip-routing(show)> route-table
```

ip-routing(show)> route-table

Use this command to display the AP’s IP route table.

Syntax

```
route-table
```

Output Parameters

dest-ip	The destination subnet address.
gateway-ip	IP address of the next-hop router.
interface	The egress interface for packets forwarded according to this route.
vlan-id	The egress VLAN for packets forwarded according to this route.

Description

This command displays the route table in the AP.

Defaults

None

Usage Guidelines

This command can be used to show how forward IP packets will be forwarded when the AP is behaving as an IP packet forwarding device.

Examples

```
ip-routing(show)> route-table

dest-ip    : 192.168.68.0/24
gateway-ip : 0.0.0.0
interface  : br254
vlanid     : 254
---------------------------------------------------------------------------

dest-ip    : 192.168.168.0/24
gateway-ip : 0.0.0.0
interface  : br1
vlanid     : 1
---------------------------------------------------------------------------

dest-ip    : 0.0.0.0/0
gateway-ip : 192.168.168.254
interface  : br1
vlanid     : 1
```

See Also

```
ip-routing(config)> add-route
ip-routing(config)> delete-route
system(config)> mgmt-ipaddress
```

8 Portal CLIs

This chapter includes information about the following portal commands:

- **portal(config)> add-ap**
- **portal(config)> add-discovery-scope**
- **portal(config)> add-remote-portal**
- **portal(show)> auto-db-sync-frequency**
- **portal(config)> auto-discovery-criteria**
- **portal(show)> auto-discovery-criteria**
- **portal(show)> auto-discovery-scope**
- **portal(show)> auto-discovery-state**
- **portal(config)> auto-guest-password**
- **portal(show)> auto-guest-password**
- **portal (config)> auto-sync-db-frequency**
- **portal (config)> classify-rogue-ap**
- **portal(config)> commit-enrollment**
- **portal (show)> db-version-table**
- **portal(config)> delete-ap**
- **portal(config)> delete-discovery-scope**
- **portal (config)> delete-policy-files**
- **portal(config)> delete-remote-portal**
- **portal(config)> delete-rogue-ap**
- **portal(config)> distribute-policy-now**
- **portal(config)> enroll-ap**
- **portal(show)> enrolled-ap-list**
- **portal (config)> generate-default-policy**
- **portal(show)> ip-rogue-ap-list**
- **portal (show)> list-policy-files**
- **portal (config)> notify-by-email**
- **portal(show)> notify-by-email**
- **portal (show)> policy-file-contents**
- **portal (config)> portal-backup**
- **portal (config)> portal-restore**
- **portal(config)> portal-services**
- **portal(show)> portal-services**
- **portal(show)> portal-table**
- **portal(config)> rediscover-now**
- **portal(config)> reject-ap**
- **portal (config)> remote-reboot**

- **portal (config)> remote-save**
- **portal (config)> rogue-ap-discovery**
- **portal (config)> sync-security-db-now**
- **portal(show)> topology-db**
- **portal(show)> unenrolled-ap-list**
- **portal(show)> wireless-neighbors**
- **portal(show)> wireless-rogue-ap-list**

portal(config)> add-ap

Use this command to add an access point to the discovered network.

Syntax

```
add-ap ap hostname/ipaddress {…}
```

Input Parameters

hostname/ipaddress	The hostname or IP address of the access point added to the discovered network.

Output Parameters

Success or Failure	Command can fail if the address is not valid.

Description

This command is used to add an access point to the discovered network. After an access point is made available as part of the discovered network, it may then be enrolled to become part of the managed network. If a hostname is specified, make sure that the DNS addresses on the AP is configured correctly so that the hostname is resolved correctly. After an access point is added to the discovered network, it will be kept persistently on the portal. This command executes in the background, that is, the command will return successfully and portal AP will contact the identified AP and gather information about the AP and add it to the discovered network.

Usage Guidelines

In a typical deployment, the portal AP automatically detects the access points that are present in the network that the portal is connected to, so this command need not be used. If you want to manage an AP that is IP reachable, but is part of a different subnet, use this command to add the access point to the discovered network. After an AP is made part of the discovered network, you can then enroll that AP into the managed network.

Examples

```
add-ap ap engAp.abc.com
```

See Also

```
portal(show)> topology-db
```

portal(config)> add-discovery-scope

Use this command to add an IP subnet that needs to be discovered for management.

Syntax

```
scope-ip ipaddress/numbsubnetmaskbits [seed-ap hostname/ipaddress ]
```

Input Parameters

scope-ip	The subnet to be discovered, specified as an IP address with the number of mask bits as: A.B.C.D/16
seed-ap	Address of one Airgo access point in the scope-ip subnet.

Output Parameters

Success or Failure

Description

The portal AP provides facilities to manage the network of access points. The discovery service on the access point automatically discovers the network of connected access points. The automatic discovery is restricted to the set of subnets that are directly configured on the portal. The portal AP will normally discover the subnet to which it it connected. Use this command to allow the discovery service to discover other subnets that are reachable from this access point (that is, are routed) but are not directly attached to this access point. The scope-ip identifies the reachable subnet that needs to be discovered. The seed-ap if specified identifies one Airgo access point within the scope-ip subnet that will act as the proxy for the discovery. Specifying the seed-ap will speed up the discovery of the new subnet dramatically. If the seed-ap is not specified, the discovery service will traverse all the addresses in the scope-ip subnet one by one. This can take a very long time if the subnet is a large. After the subnet is added, you must execute the rediscover-now command to enable the discovery service to discover the network again.

Defaults

None

Usage Guidelines

A typical usage scenario is when the portal is expected to manage a network of access points that are in a multiple subnets. Typically this can happen if the access points in different floors or in different buildings are in different subnets for traffic segregation. In such a case, use this command to add the set of other subnets that the portal AP needs to discover. Then execute the redisocver-now command to allow the subnets to be discovered.

Examples

```
portal(config)> add-discovery-scope scope-ip 2.2.2.2/24 seed-ap 2.2.2.2 <cr>
portal(config)> add-discovery-scope scope-ip 2.2.2.2/24 seed-ap 2.2.2.2
Success portal(config)>
```

portal(config)> add-remote-portal

Use this command to add a standby security portal to the network.

Syntax

```
ap hostname/ipaddress
```

Input Parameters

hostname/ipaddress	The hostname or IP address of an enrolled AP.

Output Parameters

Success or Failure

Description

This command is used to promote an enrolled access point as a security portal. A security portal is an access point that provides radius server functionality. Any enrolled aceess point can be promoted as a security portal. When this command is executed, an enrolled access point is converted into a security portal to operate seamlessly in the network managed by the portal (NM portal). After an access point is converted into a security portal, all the user mangement databases are synchronized with the NM portal. After established, this security portal will provide all the authentication functionality that is provided by NM portal. So even if the NM portal is taken down for maintainence or upgrades, this security portal will provide the authentication services.

A standby security portal will not provide interfaces to configure or manage any users in the network. All user management must be performed from the NM portal alone. But the standby security portal will provide authentication services for the already configured user population.

Defaults

None

Usage Guidelines

In a network managed by NM portal, it is advisable to configure a standby security portal as this provides runtime redundancy. As a security portal contains the authentication functionality, it contains the security information about the network. So it is important to keep the standby security portal in a secure place as opposed to normal access points.

Examples

```
add-remote-portal 192.168.1.25
```

See Also

```
portal(show) portal-table, portal-services
```

portal(show)> auto-db-sync-frequency

Use this command to show data base synchronziziation frequency.

Syntax

```
Auto-db-sync-frequency
```

Input Parameters

None

Output Parameters

Success or Failure

Description

The NM portal manages a set of databases that are kept synchronized across the managed network. The frequency at which the databases are checked may be controlled. This command shows the frequency at which the NM portal checks the network for consistency

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> auto-db-sync-frequency

period (minutes) : 3
```

See Also

```
portal(config)> auto-db-sync-frequency
```

portal(config)> auto-discovery-criteria

Use this command to configure the operation of the discovery service.

Syntax

```
discovery-limit max-ap-count periodic mm
```

Input Parameters

max-ap-count	Specify the maximum number of access points this portal should discover.
mm	Specify the frequency at which the discovery service must re-discover the network.

Output Parameters

Success or Failure

Description

The command is used to limit the size of the network that the discovery service allowed to discover. The frequency at which the network is re-scanned to detect the presence of new Airgo APs can also be configured using this command.

The discovery service periodically scans two kinds of networks, the IP reachable network and the wireless network. The IP reachable network is defined by the discovery address scope (see add-auto-discovery-scope command). The wireless network is the set of beaconing radios that are detected by the enrolled nodes in the network. The scope of the wireless network is defined by the set of enrolled nodes in the network.

Defaults

By default an NM portal will discover 50 nodes; using this command that may be further restricted. The discovery service scans the IP network once every 60 minutes, the wireless network is scanned every 15 minutes, and the discovered network is polled every 15 minutes to determine the status of the access points in the network. Using this command, the rate at which the IP network is scanned may be controlled. It is not possible to change the wireless and status poll intervals.

Usage Guidelines

In a network managed by NM portal, there are two types of AP limits. The first is the total number of nodes that may be discovered in the defined set of discovery scopes. The second is the set of nodes from within this set of discovered nodes that may be actively managed.

The discovered nodes limit is controlled using this command. The set of actively managed nodes are the set of enrolled nodes. The maximum number nodes that may be managed is determined by the license installed on the NM portal AP. During normal operation when either limit is exceeded, appropriate faults are generated to keep track of the operation of the network.

Examples

```
auto-discovery-criteria discovery-limit 25 periodic 120
```

See Also

```
portal(show) auto-discovery-criteria
```

portal(show)> auto-discovery-criteria

Use this command to show discovery service limits.

Syntax

```
auto-discovery-criteria
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the limits configured for the discovery service.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> auto-discovery-criteria

discovery-limit    : 50
periodic           : 60
rogue-ap-discovery : enable
```

See Also

```
portal(config)> auto-discovery-criteria
```

portal(show)> auto-discovery-scope

Use this command to show discovery scopes configured on the NM portal.

Syntax

```
Auto-discovery-scope
```

Input Parameters

None

Output Parameters

Parameters	The requested details.

Description

This command is used to show the state of discovery service on the NM portal.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> auto-discovery-scope

scope-ip : 192.168.168.1/24
seed-ap  : 192.168.168.24
```

See Also

```
portal(show)> portal(config)> add-discovery-scope
```

portal(show)> auto-discovery-state

Use this command to show status of discovery service running on NM portal.

Syntax

```
portal-services
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the status of the discovery server. The discovery server must have completed its operations to get a consistent view of the network.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> auto-discovery-state

server-state : Discovery complete
```

See Also

```
portal(config)> rediscover-now
```

portal(config)> auto-guest-password

Use this command to configure the auto-guest-password generation.

Syntax

```
{ { disable } | { enable { daily | weekly | 2-hours | 4-hours | 8-hours | 12-
hours } } }
```

Input Parameters

disable	Disables auto-guest-password generation.
enable	Enables auto-guest-password generation. The durations are daily, weekly. 2-hours, 4-hours, 8-hours and 12-hour. These are the durations at which the password will be generated

Output Parameters

Success or Failure

Description

The command is used to enable or disable auto-guest-password generation. When guest access is enabled, guest users are allowed to access the nework. They need a password to access the network, this may be configured using the guest-access(config) guest-password.

On an NM portal, this guest password may be generated automatically at fixed intervals and mailed to the administrator. This command allows the guest password to be generated automatically.

When enabled, the password is generated automatically once:

- Daily
- Weekly – starting from today
- Every 2, 4, 8, or 12 hours starting from midnight local time.

When the password is generated it is mailed to the administrator e-mail address configured using the e-mail command.

When the password generation is disabled, an e-mail stating this is sent to the administrator as well.

For security reasons, it is useful to enable a guess access password in a network managed by NM portal. However, manually configuring the password on every enrolled access point is cumbersome. Use this command to automatically generate guess access passwords and then share them with all enrolled access points. One auto-generated password is used across the managed network for controlling guest access.

Defaults

By default auto-guest-password generation is disabled.

Usage Guidelines

It is recommended to have automatic guest access password generation enabled.

Examples

```
auto-guest-password enable 8-hours
```

See Also

`(show)auto-guest-password, e-mail`

portal(show)> auto-guest-password

Use this command to show status of auto-guest password generation.

Syntax

```
Auto-guest-password
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the status and the automatically generated password for guest access.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> auto-guest-password

login        : __guest__
password     : heyocaha
admin-state  : enable
periodic     : daily
```

See Also

```
portal(config)> auto-guest-password
```

portal (config)> auto-sync-db-frequency

Use this command to configure the database synchronization frequency.

Syntax

```
{ autonomous | periodic mm }
```

Input Parameters

autonomous	Use default sync frequency.
mm	Set the sync frequency to **mm** minutes.

Output Parameters

Success or Failure

Description

This command is used to set the DB synchronization frequency. The NM portal maintains multiple databases that need to be synchronized with the set of standby security portals in the NM portal network. The databases are synchronized automatically at a predefined interval. Using this command the synchronization frequency may be changed.

Defaults

None

Usage Guidelines

It is recommended that the default setting not be changed.

Examples

```
portal(config)> auto-sync-db-frequency autonomous

Success

portal(show)> auto-db-sync-frequency

period (minutes) : 5
```

portal (config)> classify-rogue-ap

Use this command to classify detected rogue APs as known access points.

Syntax

```
{ rogue-ap-mac mac-address | rogue-ip rogue-ipaddress } class { our-network |
neighbor-network }
```

Input Parameters

rogue-ap-mac	The MAC address of the rogue AP.
rogue-ip	The IP address of the rogue AP.
class	The class of neighbor this AP belongs to.

Output Parameters

Success or Failure

Description

This command is used to classify rogue AP(s) into identifiable groups.

A rogue AP is an access point that is only wirelessly detectable or it is IP reachable but the AP fails security validations. In a wireless deployment, access points that are not part of managed network but belonging ‘known’ entities may be detected. These access point may be grouped as follows:

- Our-network – Access points belong to the local company network but are not being managed by this Portal
- Neighbor-network – Access points belong to the neighboring company but are known entities.

In a wireless deployment there are likely to be a large number of rogue APs. By categorizing them into these groups, it is easier to track the real rogue APs in the network.

This command may be used to classify a detected rogue AP as a known access point. Use the wireless-rogue-ap-list and ip-rogue-ap-list commands to display the detected list of wireless rogue APs or IP rogue APs.

After rogue APs have been classified, they are maintained persistently across reboots.

Defaults

None

Usage Guidelines

Examples

```
portal(config)> classify-rogue-ap rogue-ap-mac 00:0A:F5:00:02:D1 class our-
network.

Success
```

portal(config)> commit-enrollment

Use this command to set complete the enrollment of set of nodes enrolled so far.

Syntax

```
commit-enrollment
```

Output Parameters

Success or Failure

Description

This command is used complete the enrollment process. When this command is executed, the entired network is synchronized to assure that the newly enrolled nodes are made securely manageable in the network.

Commit-enrollment command must be invoked to successfully complete enrollment.

Defaults

None

Usage Guidelines

Commit-enrollment may be called after enrolling one or more access points. It is recommended that commit-enrollment be called after enrolling multiple nodes to minimize the number of network wide updates.

Examples

```
commit-enrollment
```

See Also

`enroll-ap, reject-ap`

portal (show)> db-version-table

Show the database version table of all access points enrolled by the portal.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the current database running versions of all access points enrolled by the portal.

Defaults

None

Usage Guidelines

Show running database version table.

Examples

```
portal(show)> db-version-table

ap                   : 192.168.168.24
device-id            : AP_00-0A-F5-00-01-F2
enrolled             : 1
radius-client-db-ver : 2.0
radius-user-db-ver   : 2.0
cert-db-ver          : 2.0
-------------------------------------------------------------------------

ap                   : 192.168.168.14
device-id            : AP_00-0A-F5-00-02-9A
enrolled             : 1
radius-client-db-ver : N/A
radius-user-db-ver   : N/A
cert-db-ver          : 2.0
```

See Also

None

portal(config)> delete-ap

Use this command to delete a discovered access point from the topology.

Syntax

```
{ ap hostname/ipaddress | ap-mac macaddress }
```

Input Parameters

ap	The hostname or IP address of the access point to be deleted from topology.
ap-mac	The MAC address of the access point to be deleted from the topology.

Output Parameters

Success or Failure

Description

Use this command to delete an access point from the discovered network. Access points may be discovered either via the IP network or via the wireless network. If the access point is IP addressable then the access point may be deleted via the IP address. If the access point is wirelessly reachable, then the access point may be deleted using the MAC address of the wireless access point.

An enrolled node cannot be deleted. It must first be unenrolled before it can be deleted. Deleting a node causes the sytem to remove all the details about the node including any security credentials, and state details of the node.

After a node is deleted, it can be rediscovered in the next discovery cycle.

Defaults

None

Usage Guidelines

In a small network, this command need not be used. But in a network with a large number of access points, this command may be used to remove the unwanted nodes from the discovered database. Removing unwanted nodes will reduce the number of nodes that will be polled.

Examples

```
Delete-ap ap 192.168.1.20
```

See Also

```
portal(show)> unenrolled-ap-list, topology-db, enrolled-ap-list
```

portal(config)> delete-discovery-scope

Use this command to delete a discovery scope that discovery service uses.

Syntax

```
{ all-scopes | scope-ip ipaddress/numsubnetmaskbits }
```

Input Parameters

all-scopes	Delete all scopes configured on the portal.
scope-ip	Identify a particular scope to be deleted.

Output Parameters

Success or Failure

Description

This command is used to delete the auto-discovery-scope. Auto-discovery-scope determines the range of IP addresses that the discovery server will scan. When a particular scope is not needed, the scope may be deleted.

Deleting a scope will not delete any nodes already discovered or nodes already enrolled from that scope. But after the scope is deleted, the subsequent discovery scans will not scan the deleted scope.

If all scopes are deleted, discovery service will not discover any nodes at all.

Defaults

None

Usage Guidelines

Use this command to tune the set of subnets that this portal should manage.

Examples

```
delete-discovery-scope all-scopes
```

See Also

```
portal(show)> auto-discover-scope
```

portal (config)> delete-policy-files

Use this command to delete existing policy files.

Syntax

```
{ all-policy-files | policy-file filename }
```

Input Parameters

all-policy-files	Delete all existing policy files.
filename	The policy file to be deleted.

Output Parameters

Success or Failure

Description

This command is used to delete existing policy files. Use the portal(show) list-policy-files command to list the existing policy files in the policy repository.

Defaults

None

Usage Guidelines

Examples

```
system(config)> delete-policy policy-file bootstrap.xml
```

See Also

```
list-policy-files, generate-default-policy, create-policy
```

portal(config)> delete-remote-portal

Use this command to delete a security portal from the network.

Syntax

```
ap hostname/ipaddress
```

Input Parameters

ap	Hostname or IP address of the remote portal to be deleted.

Output Parameters

Success or Failure

Description

This command is used to remove a security portal from the network. The hostname or IP addres should identify a security portal. When a security portal is deleted, all the authentication services that had been enabled on the security portal are turned off.

All security credentials the relating to the security portal are removed from the NM portal. In addition, all security credentials are removed on the security portal itself that it can no longer function as a standby security portal.

After this command completes successfully, the AP is demoted to a normal AP status. As a normal AP it will still be enrolled and will be part of the network.

Defaults

None

Usage Guidelines

Use this command to remove security portals in the network. It is very important to delete a security portal from the NM portal before using the access point for other purposes. Deleteing a security portal from the NM portal ensures that all the trust that had been established between the NM portal and security portal are removed.

Examples

```
delete-remote-portal 192.168.1.21
```

See Also

```
portal-table
```

portal(config)> delete-rogue-ap

Use this command to delete detected rouge APs on the portal.

Syntax

```
rogue-aps { wireless-unclassified | ip-unclassified | wireless-classified |
ip-classified |  wireless-all-rogues | ip-all-rogues }
```

Input Parameters

rogue-aps	The group of rogue APs to delete.

Output Parameters

Success or Failure

Description

This command is used to delete the currently detected rogue APs.

The groups of rogue AP are:

- Wireless-unclassified: All wireless rouge APs that have not been classified as yet.
- Wireless-classified: All wireless access points that have been classified.
- Ip-classified: All IP rogue APs that have been classified.
- Ip-unclassified: All IP rogue APs that have not been classified as yet.
- Wireless-all-rogues: All wireless classified and unclassified rogue APs.
- Ip-all-rogues: All IP rogue APs that are classified and unclassified.

Defaults

None

Usage Guidelines

Use this command to delete the appropriate group. Removing the group and re-discovering the network will detect the latest rogue APs in the network.

Examples

```
delete-rogue-ap rogue-aps wireless-all-rogues
```

See Also

```
classify-rogue-aps
```

portal(config)> distribute-policy-now

Use this command to distribute a policy present on the NM portal to an enrolled access point.

Syntax

```
{ all-policy-files | { policy-file policy-filename-on-ap } } { all-discovered-
aps | { target-aps hostname/ipaddress {…} } }
```

Input Parameters

all-policy-files	All the policy files on the NM portal.
policy-file	Name of a policy file on the NM portal.
all-discovered-aps	The set of enrolled access points on the NM portal.
target-aps	IP addresses of one or more enrolled access points.

Output Parameters

Success or Failure

Description

This command is used to distribute one or more policies defined on the NM portal to one or more enrolled access points.

The command selects the set of policies to distribute as all-policy-files or one named policy.

The target enrolled access point is specified as all-discovered-aps – this represents the entire enrolled network. Or a set of access points may be explicitly specified.

This commands returns success immediately and the policies are pushed to the target access points in the background. Success or failure of the policy push is logged to the alarm-table.

Defaults

None

Usage Guidelines

When an access point is enrolled the default-policy is pushed to the enrolled access point. Use this command if the configuration of the NM portal is changed and the enrolled access point network needs to be re-synchronized to the configuration on the NM portal. Or if a particular policy needs to be pushed to the access point.

Examples

```
Distribute-policy-now all-policy-files target-ap 192.168.1.21
```

See Also

```
generate-default-policy, list-policy-files
```

portal(config)> enroll-ap

Use this command to securely enroll an access point into the managed network.

Syntax

```
ap hostname/ipaddress ap-device-id ap-device-id ap-password password [ portal
{ disable | enable } ]
```

Syntax

Input Parameters

ap	Hostname or IP address of the access point to be enrolled.
ap-device-id	The device identifier for the access point to be enrolled.
ap-password	The manufacturing password that the access point ships with.
portal	Enable or disable flag to convert the access point to a security portal.

Output Parameters

Success or Failure

Description

This command is used to securely admit a new access point into the managed network. Every Airgo AP ships with a predefined device ID, a password, and a certificate that is burnt into the access point at manufacturing time.

In an NM portal managed network, only access point s that have been enrolled will be actively managed. Enrollment is the process of establishing a secure two-way handshake between the NM portal and the access point. On successful completion of the two way handshake, the NM portal trusts the access point as an authorized node in the network and the new access point trusts the NM portal as its authorized manager.

In a managed network, an enrolled access point will accept policy distribution, software images, security updates, and wireless backhaul authentication transactions **only** from an NM portal.

The IP address of the access point that is specified in this command must be unique to the access point and must not change during the life time of the access point within this managed network. Fixing the IP address of an access point is critical for both management and security reasons.

When an access point is enrolled from an NM portal, the bootstrap policy that is established on the NMPortal is distributed to the enrolled access point. This ensures that the enrolled access point is configured as required as soon as the enrollment is complete.

Defaults

An access point is, by default, not enrolled as a security portal.

Usage Guidelines

Irrespective of how automated the security checking may be, it is critical for an administrator to approve an AP before it may be trusted. The act of an adminstrator approving an access point is done as follows:

- An NM portal discovers the network of access point s that may be managed. Use the command portal(show)> unenrolled-ap-list to determine the set of access point s that have validated (by the system) security credentials that may be enrolled.
- Compare the Thumbprint shown on the screen with the Thumbprint shipped with the access point. If they match, then this access point is an authorized access point that you can trust. Then you can use this command to enroll the access point into the network.
- After enrollment you can still login into the access point and configure it as an individual access point, but it is recommended that you do not reset the access point to factory defaults as this will destroy the trust between NM portal and the access point.
- <u>Moving access points within the managed network:</u> After an access point has been enrolled, it may be disconnected and re-connected back to the network as long as its IP address remains the same. The trust relationship between the NM portal and the access point will be retained.
- <u>Moving an access point to a different managed network:</u> If you want to reuse an enrolled access point in another network. While the access point is connected to the networks, unenroll the access point from NM portal, delete the access point from the discovered list. Then move it to the new network.

Examples

```
enroll-ap ap 192.168.1.21 ap-device-id AP_00_02_03_04_05_06 password manfpassw
```

See Also

```
portal(show) >unenrolled-ap-list, enrolled-ap-list, topology-db, delete-ap
portal(config)> generate-default-policy
```

portal(show)> enrolled-ap-list

Use this command to show list of the access points enrolled into the managed network.

Syntax

```
portal-services
```

Input Parameters

None

Output Parameters

Output details	The list of enrolled nodes.

Description

This command is used to show the set of access points that have been enrolled into the managed network.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> enrolled-ap-list

ap            : 192.168.168.24
device-id     : AP_00-0A-F5-00-01-F2
role          : Enrollment-Portal
time-enrolled : Sat Jan  1 00:11:14 2000
primary-nms   : 0.0.0.0
auxiliary-nms : 192.168.168.24
node-uptime   : Days:0, Hrs:0, Mins:35, Secs:30
-------------------------------------------------------------------------

ap            : 192.168.168.14
device-id     : AP_00-0A-F5-00-02-9A
role          : Access Point
time-enrolled : Sat Jan  1 00:16:46 2000
primary-nms   : 0.0.0.0
auxiliary-nms : 192.168.168.24
node-uptime   : Days:0, Hrs:1, Mins:58, Secs:42
```

See Also

```
portal(config)> enroll-ap
portal(show)> topology-db
```

portal (config)> generate-default-policy

Use this command to generate the bootstrap policy from the portals current startup configuration or from a specified policy filename.

Syntax

```
{ startup-config | { policy-file filename } } [ exclude-auth-config ]
```

Input Parameters

startup-config	Keyword to generate from the current startup configuration.
filename	The policy filename from which to generate the bootstrap policy.
exclude-auth-config	Excludes security details in the generated policy.

Output Parameters

Success or Failure

Description

This command is used to generate the default policy. The default policy is downloaded to an access point when the access point is enrolled. The default policy may be generated either from the startup configuration of the NM portal or from a named policy file. If the exclude-auth-config option is specified, the generated policy will not include any references to auth-zones or auth-servers.

Defaults

The default policy filename is defaultpolicy.xml.

Usage Guidelines

When an access point is bootstrapped as an NM portal, the default policy is generated using the startup configuration of the NM portal. Every access point enrolled from that NM portal is configured using the default policy. It is very likely that after the initial bootstrap, configuration of the NM portal and the managed network of access point s needs to be changed. In such a case, the NM portal can be configured as needed. Then issuing this command will regenerate the default policy from the configuration of the NM portal. This generated default policy will then be used to configure any access point s that will get enrolled.

To generate a default policy suitable for enrollment, execute this command as follows:

```
Portal(config) > generate-default-policy startup-config
```

Examples

```
system(config)> generate-bootstrap-policy startup-config
```

See Also

```
save delete-policy-files
distribute-policy-now
create-policy
```

portal(show)> ip-rogue-ap-list

Use this command to show list of IP reachable rogue APs detected.

Syntax

```
portal-services
```

Input Parameters

None

Output Parameters

Output details	The list of enrolled nodes.

Description

This command is used to show the list of IP rechable rogue APs detected.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> ip-rogue-ap-list
portal(show)>
```

See Also

```
portal(config)> rogue-ap-discovery
```

portal (show)> list-policy-files

Shows a list current policy files in the policy repository.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the list of current policy files in the policy repository.

Defaults

None

Usage Guidelines

Show current policy files.

Examples

```
portal(show)> list-policy-files

policy-name : defaultpolicy.xml

description : NULL
policy-date : Sat Jan  1 00:11:28 2000
```

See Also

```
policy-file-contents
```

portal (config)> notify-by-email

Use this command to enable or disable the e-mail notification of faults.

Syntax

```
{ enable | disable }
```

Input Parameters

enable/disable	Enable or disable e-mail notification from NM portal.

Output Parameters

Success or Failure

Description

This command is used to enable or disable e-mail notifications. When faults are detected on the access point, an e-mail alert can be sent to the administrator. This command enables or disables such alerts.

Defaults

By default the alerts are disabled.

Usage Guidelines

None

Examples

```
portal(config)> notify-by-email enable
```

See Also

```
system(config)> e-mail
```

portal(show)> notify-by-email

Syntax

```
Use this command to show whether e-mail notification is enabled or disabled.
```

Input Parameters

None

Output Parameters

Enabled or disabled status.

Description

This command is used to show whether e-mail notification for faults is enabled or disabled.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> notify-by-email

enable-or-disable : disable
```

See Also

```
portal(config)> notify-by-email
```

portal (show)> policy-file-contents

Shows the contents of the current bootstrap policy or a specific policy file.

Syntax

{ bootstrap-policy | policy-file **policy-filename** }

Input Parameters

bootstrap-policy	Shows the contents of the current bootstrap policy.
policy-filename	A specific policy filename. This filename must be one of the filenames produced by the list-policy-files command.

Output Parameters

Success or Failure

Description

This command is used to show the policy contents of the current default policy or a specific policy file. The specified policy-filename must be one of the filenames shown by the list-policy-files command.

Defaults

None

Usage Guidelines

Shows policy contents.

Examples

```
portal(show)> policy-file-contents policy-file defaultpolicy.xml

Command : config backhaul delete-uplink-bssid
bssid          :

Command : config backhaul uplink-criteria
interface      : wlan0
ssid           : DeerCreekCo
ipnetaddr      : 0.0.0.0/0
path-selection : lowest-weighted-cost

Command : config backhaul uplink-criteria
interface      : wlan1
ssid           : DeerCreekCo
ipnetaddr      : 0.0.0.0/0
path-selection : lowest-weighted-cost
--------------------------------------------------------------------------

Command : config radio network-density
network-density : low

Command : config radio channel
interface       : wlan0
periodic period : 30

Command : config radio channel-set
```

```
interface       : wlan0
scanned-band    : any

Command : config radio channel
interface       : wlan1
periodic period : 30

Command : config radio channel-set
interface       : wlan1
scanned-band    : any

Command : config radio commit-global-settings
--------------------------------------------------------------------------

Command : config vlan reset-to-defaults
--------------------------------------------------------------------------

Command : config filter reset-to-defaults
--------------------------------------------------------------------------
|
Command : config security delete-wep-keys

Command : config security delete-auth-server
all-external-auth-servers :

Command : config security delete-authzone
all-external-auth-zones   :

Command : config security security-modes
wpa                       : enable
wep                       : disable
open-access               : disable

Command : config security wpa-modes
auth-type                 : psk-only
encryption-type           : aes-only

Command : config security commit-global-settings
--------------------------------------------------------------------------

Command : config portal reset-to-defaults
--------------------------------------------------------------------------

Command : config snmp reset-to-defaults
--------------------------------------------------------------------------

Command : config dhcp-server reset-to-defaults
--------------------------------------------------------------------------

Command : config qos reset-to-defaults
--------------------------------------------------------------------------

Command : config bridge reset-to-defaults
--------------------------------------------------------------------------
|
Command : config system delete-event-filter
all          : 48
```

```
Command : config ap-quick-start timezone
timezone     : pst8pdt

Command : config system email
smtp-server  : 191.168.168.1
notify-email : admin@deercreekco.com

Command : config system admin-contact
contact      : admin@deercreekco.com
--------------------------------------------------------------------------

Command : config interface reset-to-defaults
--------------------------------------------------------------------------

Command : config ip-routing reset-to-defaults
--------------------------------------------------------------------------

Command : config ssid delete-ssid
all-ssids            :

Command : config guest-access delete-guest-from-ssid
all-ssids            :

Command : config ssid delete-service-profile
all-service-profiles :

Command : config ssid add-ssid
ssid                 : DeerCreekCo
max-stations         : 512

Command : config ssid add-security-to-ssid
ssid                 : DeerCreekCo
psk-password         : password
portal-auth-zone    :
mac-acl              : disable
```

See Also

```
list-policy-files
```

portal (config)> portal-backup

Use this command to back up the portal configuration to a TFTP server.

Syntax

```
tftp-server hostname/ipaddress [ to-file pathname-on-tftp-server ]
```

Input Parameters

hostname/ipaddress	Hostname or IP address of the TFTP server.
pathname-on-tftp-server	An optional filename or path-and-filename, relative from the TFTP root directory. The default portal backup configuration filename is “portalCfg.tar.gz” if the to-file parameter is not specified.

Output Parameters

Success or Failure

Description

This command is used to upload the configuration of the portal into a file on a TFTP server. The result file is in the gzip-ed tar file format.

This command backs up the configuration of the portal, that is, it includes all the databases and all the security credentials present on the portal, so that it may be restored at a later point in time. Care must be taken to make sure that the tftp server to which the backup is upladed is secure.

Defaults

The default output filename is portalCfg.tar.gz if the to-file parameter is not specified.

Usage Guidelines

Use this command to backup the entire portal configuration onto a TFTP server.

Examples

```
system(config)> portal-backup tftp-server 10.0.0.77
```

See Also

```
system(config)> portal-restore
```

portal (config)> portal-restore

Use this command to restore a backed up portal configuration to an AP.

Syntax

```
tftp-server hostname/ipaddress [ from-file pathname-on-tftp-server ] [ reboot
]
```

Input Parameters

hostname/ipaddress — Hostname or IP address of the TFTP server.

pathname-on-tftp-server — An optional filename or path-and-filename, relative from the TFTP root directory, of the previously backed-up file generated by the *system(config) portal-backup* command.

The default filename is “portalCfg.tar.gz” if the from-file parameter is not specified.

Output Parameters

Success or Failure

Description

This command is used to restore the configuration of a portal from a previously backed up configuration. This command must be used with care as it will re-create an NM portal with all the security credentials available in the portalCfg.tar.gz file.

To transform an access point into the equivalent functioning NM portal, follow these steps:

1. Reset the access point to factory defaults
2. Make sure that the access point has the same IP address as the address of the portal which was backed up. If the IP address is different, security accesses will fail.
3. Use this command to restore the configuration.
4. Reboot the access point for the configuration to take effect by specifying the reboot option.

Defaults

The default image filename is portalCfg.tar.gz if the from-file parameter is not specified.

Usage Guidelines

It is recommended to keep a NM portal in a secure place.

Examples

```
system(config)> portal-restore tftp-server 10.0.0.77
```

See Also

```
system(config) portal-backup
```

portal(config)> portal-services

Use this command to enable network-management and security-management services in designated access points.

Syntax

```
portal-services { [ enrollment { disable | enable } ] [ nm { disable | enable
} ] [ security { disable | enable } ] }
```

Input Parameters

enrollment	Enable/disable enrollment portal service on this access point.
nm	Enable/disable network-management portal service on this access point.
security	Enable/disable security portal service on this access point.

Output Parameters

Success or Failure

Description

This command is used to enable portal services, which is a rich set of features in Airgo APs. Portal services ease secure deployment of the network, user administration, and management of networks from within a designated portal AP.

Three services are:

1. **Enrollment**: aids in secure deployment of new Airgo APs in the network.
2. **NM**: aids in managing a small number of Airgo APs without the need of external NM system.
3. **Security**: aids in managing user-security via built-in RADIUS server and rich set of subscriber management features.

Refer to the *Airgo AP Installation Guide* for details.

Defaults

None

Usage Guidelines

Use this command to configure portal services on a designated Airgo AP. This allows for a rapid deployment of Airgo APs with rich built-in functions that enhance secruity and manageability of the Airgo network. Portal services obviate the need to prepare back-office servers and dramatically reduce complexity of network deployment.

Refer to the *Airgo AP Installation Guide* for detailed scenarios of usage and how to secure deployment, enhance manageability of networks and users, and improve reliability by replicating security services on more than one portal APs.

Examples

```
portal-services enrollment enable nm enable security enable
```

See Also

```
ap-quickstart(show)> portal-services
```

portal(show)> portal-services

Use this command to show status of portal services running on this access point.

Syntax

```
portal-services
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the status of portal services, whether each of the portal services; enrollment, nm, or security; are enabled or disabled.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> portal-services

enrollment : enable
nm         : enable
security   : enable
```

See Also

```
ap-quickstart(config)> portal-services
```

portal(show)> portal-table

Use this command to show the set of security or NM portals that have been detected in the IP network.

Syntax

```
portal-table
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the set of security or NM portals that have been detected in the IP network. Note that depending on the discovery scope, this command will show all the portals in the discovered network, not just the enrolled portals.

Defaults

None

Usage Guidelines

None

Examples

```
portal(show)> portal-table

ap           : 192.168.168.24
ap-device-id : AP_00-0A-F5-00-01-F2
enrolled     : 1
```

See Also

```
ap-quickstart(config)> portal-services
```

portal(config)> rediscover-now

Use this command to trigger a discovery of the access points in the network.

Syntax

```
[ { force-all } | { discovery-method { all | ip | wireless } } ]
```

Input Parameters

force-all	Force a rediscovery.
discovery-method	Specifies the kinds of discovery to be triggered.

Output Parameters

Success or Failure

Description

This command is used to trigger a discovery of the access point s in the network. The access point s in the network are discovered using IP or wireless discovery.

This command triggers a long operation so the command will return immediately and will continue the discovery process in the background. Refer to See Also below.

The force-all option will cause any currently executing discovery operations to be stopped and both IP and wireless discovery are restarted.

The discovery-method specifies which type of discovery should be started:

1. all – Starts both IP and wireless discovery.
2. IP – Starts only the IP discovery of the network.
3. wireless – Starts only the wireless discovery of the network.

If no parameter is specified, it starts discovering both IP and wireless networks if a discovery is not already in progress.

Defaults

By default both IP and wireless discovery are triggered.

Usage Guidelines

Use this command when you have added or delete discovery scopes or when you need to synchronize the network topology immediately instead of waiting for the periodic discovery. Use this command to also scan for all access points as part of the wireless network. This command is useful if want to find out the presence of unauthorized wireless access points in the neighborhood, but don’t want to wait for the periodic discovery to start.

Examples

```
portal(config)rediscover-now
```

See Also

```
portal(config)add-discovery-scope
delete-discovery-scope
portal(show)> auto-discovery-state
wireless-topology
```

portal(config)> reject-ap

Use this command to unenroll and reject an access point from the managed network.

Syntax

```
ap hostname/ipaddress ap-device-id ap-device-id [ reject-reason user-comment-
reason-string ]
```

Input Parameters

ap	The hostname or IP address of an enrolled access point.
ap-device-id	The device-ID of the enrolled access point.
reject-reason	The administrative reason for rejecting the access point.

Output Parameters

Success or Failure

Description

This command is used to remove the security credentials and unmanage a node.

Rejecting an access point deletes the following security associations with the access point:

- It is no longer trusted, so it will no longer be actively managed, that is, it will not receive any policy, security, image updates etc.
- All radius authentication configurations are removed so any wireless clients that could access the wireless network via the enrolled access point before can no longer access the network, that is, the wireless access is cut off.
- It also ensures that the rejected access point will not be allowed to form a wireless backhaul with ANY access point in the authorized network. So the authenticated network cannot be breached via a rejected access point.

Defaults

None

Usage Guidelines

Use this command when you to move an access point from one managed network to another. After the access point has been rejected, it must be enrolled again if needs to be part of the managed network.

Examples

```
portal(config)reject-ap ap 192.168.1.21 ap-device-id AP_01_02_03_04_05_06
```

See Also

```
portal(config)enroll-ap
portal(show)> enrolled-ap-list
unenrolled-ap-list
```

portal (config)> remote-reboot

Use this command to reboot a remote access point.

Syntax

```
ap hostname/ipaddress [ force ]
```

Input Parameters

hostname/ipaddress	Hostname or IP address of the remote access point.
force	Unconditional reboot even if the access points configuration is dirty.

Output Parameters

Success or Failure

Description

This command is used to reboot a remote access point. Note that you can only remote-reboot an enrolled access point. If the remote access points configuration is dirty, you will have to is issue a remote-save or over-ride with the *force* option.

Defaults

None

Usage Guidelines

Use this command to reboot a remote access point.

Examples

```
portal(config)> remote-reboot ap 192.168.75.168
```

See Also

```
remote-save
```

portal (config)> remote-save

Use this command to save the running configuration of the remote access point.

Syntax

```
ap hostname/ipaddress
```

Input Parameters

hostname/ipaddress	Hostname or IP address of the remote access point

Output Parameters

Success or Failure

Description

This command is used to save the running configuration of a remote access point. Note that you can only *remote-save* an enrolled access point.

Executing a remote-save is identical to logging into that access point and executing a save operation.

Defaults

None

Usage Guidelines

Use this command to remotely save the running configuration of an access point.

Examples

```
portal(config)> remote-save ap 192.168.75.168
```

See Also

`remote-reboot`

portal (config)> rogue-ap-discovery

Use this command to save the running configuration of the remote access point.

Syntax

```
{ disable | enable }
```

Input Parameters

disable/enable	Disables or enables rogue AP discovery.

Output Parameters

Success or Failure

Description

This command is used to enable or disable rogue AP discovery. When enabled, the portal will periodically scan the network to detect rogue APs.

Defaults

Rogue AP discovery is disabled by default.

Usage Guidelines

Examples

```
portal(config)> rogue-ap-discovery enable
```

See Also

```
classify-rogue-ap
```

portal (config)> sync-security-db-now

Unconditionally synchronize all security databases to all managed access points.

Syntax

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to synchronize all security databases of all the managed access points.

Defaults

None

Usage Guidelines

Use this command to synchronize all security databases.

Examples

```
portal(config)> sync-security-db-now

Success
```

portal(show)> topology-db

Use this command to show the set of access points discovered using IP discovery.

Syntax

```
Topology-db
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the set of access points discovered. The access points discovered depend on the discovery-scope configured. For each access point the core parameteres for the access point are displayed. If an access point is rejected but not deleted, it will show up in the topology database. The state of the node will be appropriately reflected. Also note that the list of nodes shown in this command are a superset of the nodes shown in unenrolled-ap-list and enrolled-ap-list commands.

Defaults

None

Usage Guidelines

Use this command to get a complete picture of the all the nodes discovered.

Examples

```
portal(show)> topology-db

ap                : 192.168.168.24
device-id         : AP_00-0A-F5-00-01-F2
thumb-print       :
00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
portal-services   : Enrollment-Portal
oper-state        : enable
auto-or-manual    : auto-discovered
discovery-time    : Sat Jan  1 00:11:13 2000
node-state        : Authorized-node
radio-mac-address : 00:0A:F5:00:06:5A, 00:0A:F5:00:06:17
--------------------------------------------------------------------------

ap                : 192.168.168.14
device-id         : AP_00-0A-F5-00-02-9A
thumb-print       :
dc:a6:cf:da:d1:73:c9:93:1c:4e:0d:fe:ab:81:50:dc:6a:32:ac:2d
portal-services   : Access Point
oper-state        : enable
auto-or-manual    : auto-discovered
discovery-time    : Sat Jan  1 00:16:00 2000
node-state        : Authorized-node
radio-mac-address : 00:0A:F5:00:06:AC, 00:0A:F5:00:04:84
--------------------------------------------------------------------------
```

```
ap                : 192.168.168.21
device-id         : AP_00-0A-F5-00-02-E2
thumb-print       :
b7:f4:c0:b4:88:a2:39:02:a6:3e:ed:51:4b:c2:15:cc:77:8c:cb:e2
portal-services   : Access Point
oper-state        : enable
auto-or-manual    : auto-discovered
discovery-time    : Sat Jan  1 00:11:20 2000
node-state        : Unauthorized-node
radio-mac-address : 00:0A:F5:00:06:DC, 00:0A:F5:00:06:35
```

See Also

```
portal(config)> add-discovery-scope, rediscover-now
```

portal(show)> unenrolled-ap-list

Use this command to show the set of unenrolled access points in the discovered network.

Syntax

```
Topology-db
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the set of access points that may be enrolled into the network. Every parameter in this output is an important identifying criteria of the access point. Before enrolling an access point, review the information presented in the command. If the details presented are correct, then the access point may be safely and securely enrolled into the managed network.

Defaults

None

Usage Guidelines

Using the output from this command verify the device-id and the thumb-print to make sure that it is a known access point. Then you may enroll the access point.

Examples

```
portal(show)> unenrolled-ap-list

ap                : 192.168.168.21
device-id         : AP_00-0A-F5-00-02-E2
thumb-print       : b7:f4:c0:b4:88:a2:39:02:a6:3e:ed:51:4b:c2:15:cc:77:8c:cb:e2
unenrolled on     : Wed Dec 31 16:00:00 1969
ap-serial-number  : AIRGO-P2-0xxxxxxxxx
ap                : 192.168.75.189
device-id         : AP_00-0A-F5-00-00-1D
thumb-print       : 9c:67:3e:14:1c:d1:b1:87:c9:84:18:9e:53:fc:0b:66:97:fa:65:64
unenrolled on     : Wed Dec 31 16:00:00 1969
ap-serial-number  : AIRGO-P2-0xxxxxxxxx
-----------------------------------------------------------------------------

portal(show)>
```

See Also

```
portal(config)> enroll-ap, reject-ap
```

portal(show)> wireless-neighbors

Use this command to show the set radios discovered in the managed network.

Syntax

```
Topology-db
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the set of radios that are discovered wirelessly via beacons. Use the time-discovered, reporting-time, and reporting-ap parameters to determine the when and how frequently these access points are being observed in the network. If the discovered Radio is IP reachable then the IP address field will be displayed.

Wireless neighbor discovery is run periodically. If a radio neighbor was detected in the last discovery run but is not detected in the latest run, then the reporting-ap will be empty.

Defaults

None

Usage Guidelines

Use this command to get a complete picture of the all the wireless radios in the managed network.

Examples

```
portal(show)> wireless-neighbors

MAC address     : 00:0D:88:AA:40:C1
IP address      :
reporting AP    :
current time    : 0:49:41
classification  : radio-neighbor
RSSI (dBm)      : -89
BSS type        : infrastructure
SSID            : VoltageWireless
radio channel   : 6
time-discovered : 0:32:9
--------------------------------------------------------------------------

MAC address     : 00:01:24:F1:E8:EB
IP address      :
reporting AP    : AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-neighbor
RSSI (dBm)      : -84
BSS type        : infrastructure
SSID            : imdemo
radio channel   : 11
```

```
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:0A:F5:00:06:AC
IP address      : 192.168.168.14
reporting AP    : AP_00-0A-F5-00-01-F2, AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-and-ip-neighbor
RSSI (dBm)      : -27
BSS type        : infrastructure
SSID            : DeerCreekCo
radio channel   : 157
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:80:C8:1B:2D:55
IP address      :
reporting AP    : AP_00-0A-F5-00-01-F2, AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-neighbor
RSSI (dBm)      : -31
BSS type        : infrastructure
SSID            : Dlink
radio channel   : 1
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:0A:F5:00:06:5A
IP address      : 192.168.168.24
reporting AP    : AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-and-ip-neighbor
RSSI (dBm)      : -83
BSS type        : infrastructure
SSID            : DeerCreekCo
radio channel   : 11
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:0A:F5:00:06:17
IP address      : 192.168.168.24
reporting AP    : AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-and-ip-neighbor
RSSI (dBm)      : -29
BSS type        : infrastructure
SSID            : DeerCreekCo
radio channel   : 149
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:0A:F5:00:06:35
IP address      : 192.168.168.21
reporting AP    : AP_00-0A-F5-00-01-F2, AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-and-ip-neighbor
RSSI (dBm)      : -34
BSS type        : infrastructure
```

```
SSID            : AniNet
radio channel   : 6
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:0A:F5:00:06:DC
IP address      : 192.168.168.21
reporting AP    : AP_00-0A-F5-00-01-F2, AP_00-0A-F5-00-02-9A
current time    : 0:49:41
classification  : radio-and-ip-neighbor
RSSI (dBm)      : -28
BSS type        : infrastructure
SSID            : AniNet
radio channel   : 153
time-discovered : 0:47:10
--------------------------------------------------------------------------

MAC address     : 00:0A:F5:00:04:84
IP address      : 192.168.168.14
reporting AP    : AP_00-0A-F5-00-01-F2
current time    : 0:49:41
classification  : radio-and-ip-neighbor
RSSI (dBm)      : -22
BSS type        : infrastructure
SSID            : DeerCreekCo
radio channel   : 1
time-discovered : 0:47:9
```

See Also

```
portal(config)> rediscover-now
```

portal(show)> wireless-rogue-ap-list

Use this command to show the set wireless rouge APs discovered in the network.

Syntax

```
Topology-db
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the set of wireless rogue APs discovered in the netowork. When rogue AP discovery is enabled, the portal will periodically scan the network to detect the wireless rouge APs.

Defaults

None

Usage Guidelines

Use this command to get a complete picture of the all the wireless rogue APs in the network.

Examples

```
portal(show)> wireless-rogue-ap-list

rogue-mac        : 00:0D:88:AA:40:C1
reporting-ap     :
reporting-time   : 0:50:18
rogue-class      : radio-neighbor
rogue-rssi       : -89
rogue-bss-type   : 0
rogue-ssid       : VoltageWireless
rogue-channel-id : 6
time-discovered  : 0:32:9
-------------------------------------------------------------------------

rogue-mac        : 00:01:24:F1:E8:EB
reporting-ap     : AP_00-0A-F5-00-02-9A
reporting-time   : 0:50:18
rogue-class      : radio-neighbor
rogue-rssi       : -84
rogue-bss-type   : 0
rogue-ssid       : imdemo
rogue-channel-id : 11
time-discovered  : 0:47:10
-------------------------------------------------------------------------

rogue-mac        : 00:80:C8:1B:2D:55
reporting-ap     : AP_00-0A-F5-00-01-F2, AP_00-0A-F5-00-02-9A
reporting-time   : 0:50:18
rogue-class      : radio-neighbor
rogue-rssi       : -31
```

```
rogue-bss-type   : 0
rogue-ssid       : Dlink
rogue-channel-id : 1
time-discovered  : 0:47:10
```

9 QoS CLIs

This chapter includes information about the following QoS commands:

- qos(config)> add-ipproto-to-cos
- qos(config)> clear-statistics
- qos(config)> cos-to-tcid
- qos(show)> cos-to-tcid
- qos(config)> delete-ipproto-to-cos
- qos(config)> dscp-to-cos
- qos(show)> dscp-to-cos
- qos(config)> ingress-class-order
- qos(show)> ingress-class-order
- qos(config)> interface-to-cos
- qos(show)> interface-to-cos
- qos(config)> ipprecedence-to-cos
- qos(show)> ipprecedence-to-cos
- qos(show)> ipprotocol-to-cos
- qos(show)> statistics
- qos(config)> tcid-to-cos
- qos(show)> tcid-to-cos
- qos(config)> vlan-to-cos
- qos(show)> vlan-to-cos

qos(config)> add-ipproto-to-cos

Use this command to assign a class of service (cos) to an IP protocol on an interface.

Syntax

```
add-ipproto-to-cos interface interface-name proto protocol-value cos cos-value
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface for which the IP protocol to cos classification rule will be created.
proto *protocol-vlaue*	Specifies the IP protocol value to which the cos will be assigned. Protocol value range is 0 – 255.
cos *cos-value*	Specifies the cos value that will be assigned to the specified protocol value. Cos value range is 0 – 7.

Output Parameters

Success or Failure

Description

This command creates a classification rule for the IP protocol-to-cos classifier, which assigns a cos values to IP packets based on the IP header's protocol field.

Defaults

None

Usage Guidelines

The cos value assigned to the IP protocol specified in this command will be assigned to the received frame if the classification rule created by this command is satisfied and classifiers with higher precedence cannot determine the frame's cos value. Include the ipprotocol classifier in the class-order string when configuring ingress-class-order to determine a frame's cos value using its IP protocol.

Examples

```
add-ipproto-to-cos interface eth0 proto 17 cos 6
```

See Also

```
qos(config)> delete-ipproto-to-cos
qos(config)> ingress-class-order
qos(show)> ipprotocol-to-cos
```

qos(config)> clear-statistics

Use this command to clear Quality of Service (QoS) statistics on the AP.

Syntax

```
clear-statistics {all-interfaces | interface interface-name}
```

Input Parameters

all-interfaces	Clear statistics for all interfaces.
interface *interface-name*	Clear statistics for interface *interface-name*.

Output Parameters

Success or Failure

Description

This command clears the QoS statistics on the AP.

Defaults

None

Usage Guidelines

The counters that comprise the VLAN statistics are set to zero when cleared.

Examples

```
clear-statistics interface eth0
```

See Also

```
qos(show)> statistics
```

qos(config)> cos-to-tcid

Use this command to assign 802.11 traffic classes to various class of service (cos) values.

Syntax

```
cos-to-tcid interface interface-name {default | tcid cos0-tcid ... cos7-tcid}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the radio interface for which the cos to TCID classification rule will be created.
default	Revert to the default cos/TCID mapping: 0/0, 1/1, 2/2, … 7/7.
tcid cos0-tcid … cos7-tcid	A list of eight TCIDs corresponding to cos 0 … cos 7 that represent the cos/TCID mapping.

Output Parameters

Success or Failure

Description

This command maps cos values to traffic class identifier (TCID) by specifying the TCIDs for various cos values.

Defaults

The default cos/TCID mapping is 0/0, 1/1, 2/2, 3/3, 4/4, 5/5, 6/6, 7/7.

Usage Guidelines

The AP determines a frame’s cos value upon reception and preserves this cos value when transmitting the frame out of the radio by mapping the cos value to a TCID as specified with this command. The AP determines a frame’s cos value by applying a set of classifiers to the frame and assigning the cos value associated with the first classification rule that is satisfied to the frame. The default set of classifiers for the wireless interface classify frames based on TCID, station MAC address, VLAN ID, and receive interface. The default set of classifiers for the Ethernet interface classify frames based on VLAN ID and receive interface.

Examples

```
cos-to-tcid interface eth0 tcid “7 6 5 4 3 2 1 0”
```

See Also

```
qos(config)> ingress-class-order
qos(config)> interface-to-cos
qos(config)> tcid-to-cos
qos(config)> vlan-to-cos
qos(show)> cos-to-tcid
ssid(config)> define-service-profile
```

qos(show)> cos-to-tcid

Use this command to display the class of service (cos) to 802.11 traffic class maps.

Syntax

```
cos-to-tcid [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the cos to traffic class identifier (TCID) classification rule for interface *interface-name*. The cos to TCID classification rule for each radio in the AP is displayed if *interface-name* is not specified.

Output Parameters

interface	Name of the radio interface.
tcid	A list of eight TCIDs corresponding to each cos value.

Description

This command displays which TCID will be sent in the 802.11 frame header for various cos values.

Defaults

The cos to TCID classification rules for all radio interfaces are displayed.

Usage Guidelines

This command can be used to determine which TCID will be used to represent various cos values in the 802.11 frame header.

Examples

```
qos(show)> cos-to-tcid interface wlan1

interface : wlan1
tcid      : 0 1 2 3 4 5 6 7
```

See Also

```
qos(config)> cos-to-tcid
```

qos(config)> delete-ipproto-to-cos

Use this command to delete IP protocol to class of service (cos) classification rules.

Syntax

```
delete-ipproto-to-cos [interface interface-name] {all-entries | proto
protocol-value}
```

Input Parameters

interface *interface-name*	(Optional) Specifies *interface-name* as the interface on which IP protocol to cos classification rules will be removed. When *interface-name* is not specified, then IP protocol to cos classification rules will be removed on all interfaces.
all-entries	All IP protocol to cos classification rules will be removed.
proto *protocol-value*	Specifies the IP protocol classification rule corresponding to *protocol-value* will be removed. Protocol value range is 0 – 255.

Output Parameters

Success or Failure

Description

This command removes classification rules for the IP protocol-to-cos classifier, which assigns a cos value to an IP packet based on the IP header’s protocol field.

Defaults

None

Usage Guidelines

Use this command to remove the classification rules for the IP protocol-to-cos classifier created by the add-ipproto-to-cos command. Exclude the ipprotocol classifier from the class-order string when configuring ingress-class-order to prevent frames from being assigned a cos value using its IP protocol.

Examples

```
delete-ipproto-to-cos all-entries
delete-ipproto-to-cos interface eth0 all-entries
delete-ipproto-to-cos interface eth0 proto 17
```

See Also

```
qos(config)> add-ipproto-to-cos
qos(config)> ingress-class-order
qos(show)> ipproto-to-cos
```

qos(config)> dscp-to-cos

Use this command to modify the class of service (cos) value mapped to DiffServ Code Points.

Syntax

```
dscp-to-cos interface interface-name {default | {dscp string-with-max-eight-
dscp-values {no-cos | cos cos-value}}}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface for which the dscp to cos classification rule will be modified.
default	Reverts the dscp to cos classification rule to its default configuration. See defaults.
dscp *string-with-max-eight-dscp-values*	A string containing up to eight DiffServ Code Points to map to a cos value. The dscp value range is 0 – 63.
no-cos	Removes the cos value(s) currently mapped to the DiffServ Code Points appearing in the dscp values string. The cos value for frames bearing the DiffServ Code Points appearing in the dscp values will be determined by other classifiers.
cos *cos-value*	Specifies the cos value to be mapped to DiffServ Code Points appearing in the dscp values string. The cos value range from 0 – 7.

Output Parameters

Success or Failure

Description

This command modifies the DiffServ Code Point (dscp) to class of service (cos) classification rules mapping a cos value to the set of dscp values appearing in the dscp values string.

Defaults

dscp values 0 1 2 3 4 5 6 7 map to cos 0.
dscp values 8 9 10 11 12 13 14 15 map to cos 1.
dscp values 16 17 18 19 20 21 22 23 map to cos 2.
dscp values 24 25 26 27 28 29 30 31 map to cos 3.
dscp values 32 33 34 35 36 37 38 39 map to cos 4.
dscp values 40 41 42 43 44 45 46 47 map to cos 5.
dscp values 48 49 50 51 52 53 54 55 map to cos 6.
dscp values 56 57 58 59 60 61 62 63 map to cos 7.

Usage Guidelines

The cos value mapped to the dscp values specified in this command will be assigned to the received frame if one of the dscp values is found in the frame and the classifiers with higher precedence cannot determine the frame’s cos value. If the dscp value found within the received frame is mapped to the cos value of no-cos, then the dscp-to-cos classifier will not be able to determine the cos value for the frame. In this case, a classifier with lower precedence must determine the cos value for the received frame. Include the dscp classifier in the class-order string when configuring ingress-class-order to determine a frame’s cos value using its DSCP.

Examples

```
dscp-to-cos interface eth0 default
dscp-to-cos interface eth0 dscp “1 5 10 30 20” cos 6
dscp-to-cos interface eth0 dscp “2 3 4 6 7 8 11” no-cos
```

See Also

```
qos(config)> ingress-class-order
qos(show)> dscp-to-cos
```

qos(show)> dscp-to-cos

Use this command to display the class of service (cos) assigned to DiffServ Code Points on an interface.

Syntax

```
dscp-to-cos [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the DiffServ Code Point to cos classification rules for interface *interface-name*. The DiffServ Code Point to cos classification rules for all interfaces will be shown if *interface-name* is not specified.

Output Parameters

interface	Name of the interface.
dscp	DiffServ Code Point values ranging from 0 – 63.
cos	cos with values ranging from 0 – 7, or not defined.

Description

This command displays DiffServ Code Point (dscp) to cos classification rules mapping cos values to dscp values on an interface.

Defaults

The dscp-to-cos classification rules for all interfaces are displayed.

Usage Guidelines

This command can be used to verify which cos value will be assigned to IP packets containing various dscp values when no classifier with higher precedence has been satisfied.

Examples

```
qos(show)> dscp-to-cos interface wlan1

interface : wlan1
dscp      : 0 1 2 3 4 5 6 7
cos       : 0
---------------------------------------------------------------------------

interface : wlan1
dscp      : 8 9 10 11 12 13 14 15
cos       : 1
---------------------------------------------------------------------------

interface : wlan1
dscp      : 16 17 18 19 20 21 22 23
cos       : 2
---------------------------------------------------------------------------

interface : wlan1
dscp      : 24 25 26 27 28 29 30 31
cos       : 3
---------------------------------------------------------------------------
```

```
interface : wlan1
dscp      : 32 33 34 35 36 37 38 39
cos       : 4
--------------------------------------------------------------------------

interface : wlan1
dscp      : 40 41 42 43 44 45 46 47
cos       : 5
--------------------------------------------------------------------------

interface : wlan1
dscp      : 48 49 50 51 52 53 54 55
cos       : 6
--------------------------------------------------------------------------

interface : wlan1
dscp      : 56 57 58 59 60 61 62 63
cos       : 7
```

See Also

```
qos(config)> dscp-to-cos
qos(show)> ingress-class-order
```

qos(config)> ingress-class-order

Use this command to specify the classifiers in the order they will be applied to frames received on an interface.

Syntax

```
ingress-class-order interface interface-name { default | class-order string-of-the-orderlist }
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface to which the set of classifiers will be applied.
default	Reverts to the default set of classifiers for the interface. See defaults.
class-order *string-of-the-orderlist*	The set of classifiers to be applied to frames received on an interface. The available classifiers are tcid, ipprotocol, dscp, ipprecedence, mac, vlan, and interface.

Output Parameters

Success or Failure

Description

This command defines which classifiers are applied to frames received on an interface. Received frames can be classified by Traffic Class Identifier (TCID) on wireless interfaces, IP protocol, DiffServ Code Point (DSCP), IP precedence, station MAC address, VLAN ID, and the frame’s receive interface. The order in which the classifiers are applied to received frames is specified by the order in which the classifiers appear in the class-order string.

Defaults

Default ingress classifiers for the Ethernet interface are vlan interface.
Default ingress classifiers for the wireless interface are tcid mac vlan interface.

Usage Guidelines

The AP determines a received frame’s class of service (cos) by using the classifiers specified in this command. Each classifier will determine if the frame satisfies any of its classification rules. For example, the TCID field within a received 802.11 frame’s header, when present, will satisfy one of the rules within the TCID classifier. The AP will assign the cos value associated with the first classification rule that is satisfied to the frame.

Examples

```
ingress-class-order interface eth0 class-order “dscp vlan interface”
ingress-class-order interface wlan0 class-order “tcid ipprotocol vlan interface”
ingress-class-order interface eth0 default
```

See Also

```
qos(show)> ingress-class-order
qos(config)> tcid-to-cos
qos(config)> add-ipproto-to-cos
qos(config)> dscp-to-cos
qos(config)> ipprecedence-to-cos
qos(config)> vlan-to-cos
qos(config)> interface-to-cos
ssid(config)> define-service-profile
```

qos(show)> ingress-class-order

Use this command to display the set of classifiers in the order they are applied to frames received on an interface.

Syntax

```
ingress-class-order [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the set of classifiers applied to frames received on interface *interface-name*. The set of classifiers on all interfaces will be shown if *interface-name* is not specified.

Output Parameters

interface	Name of the interface.
class-order	The set of classifiers in the order they are applied on the interface.

Description

This command displays the set of classifiers applied to the frames received on an interface. The set of classifiers is shown in the order which in they are applied to received frames.

Defaults

The set of classifiers on all interfaces will be displayed.

Usage Guidelines

The command can be used to verify which classifiers are applied to frames received on an interface when determining the frames’ class of service.

Examples

```
qos(show)> ingress-class-order interface wlan1

interface   : wlan1
class-order : tcid mac vlan interface
```

See Also

```
qos(config)> ingress-class-order
```

qos(config)> interface-to-cos

Use this command to assign a class of service (cos) value for frames received on an interface.

Syntax

```
interface-to-cos **interface** *interface-name* {**default** | **cos** *cos-value*}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface for which the interface to cos classification rule will be created.
default	Revert the cos value to be assigned to frames received on interface *interface-name* to zero.
cos *cos-value*	The cos value to be assigned to frames received on interface *interface-name.*

Output Parameters

Success or Failure

Description

This command creates a classification rule for the interface-to-cos classifier, which assigns a cos value to frames received on an interface.

Defaults

A cos value of zero is assigned to received frames.

Usage Guidelines

The cos value assigned to the interface with this command will be assigned to the received frame when classifiers with higher precedence cannot determine the frame's cos value. The default set of classifiers for the wireless interface classify frames based on TCID, station MAC address, VLAN ID, and receive interface. The default set of classifiers for the Ethernet interface classify frames based on VLAN ID and receive interface.

Examples

```
interface-to-cos interface eth0 cos 2
```

See Also

```
qos(config)> ingress-class-order
qos(config)> tcid-to-cos
qos(config)> vlan-to-cos
qos(show)> interface-to-cos
ssid(config)> define-service-profile
```

qos(show)> interface-to-cos

Use this command to display the class of service (cos) value assigned to frames received on the AP's interfaces.

Syntax

```
interface-to-cos [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the interface to cos classification rule for interface *interface-name*. The interface to cos classification rules for all interfaces will be shown if *interface-name* is not specified.

Output Parameters

name	Name assigned to the interface.
cos	Class of service value assigned to the interface.

Description

This command displays the classification rule for the interface-to-cos classifier, which assigns a cos value to frames received on an interface.

Defaults

The interface-to-cos classification rules for all interfaces will be shown.

Usage Guidelines

This command can be used to verify what cos value will be assigned to frames when classifiers with higher precedence are not satisfied.

Examples

```
qos(show)> interface-to-cos interface eth0

interface : eth0
cos       : 0
```

See Also

```
qos(config)> interface-to-cos
qos(show)> ingress-class-order
```

qos(config)> ipprecedence-to-cos

Use this command to modify the class of service (cos) value mapped to IP precedence values.

Syntax

```
ipprocedence-to-cos interface interface-name {default | cos string-with-eight-cos-values}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface for which the IP precedence value to cos classification rule will be modified.
default	Reverts the IP precedence value to cos classification rule to its default configuration. See defaults.
cos *string-with-eight-cos-values*	Specifies the eight cos values to be mapped to the corresponding eight IP precedence values (0 1 2 3 4 5 6 7). The cos values range from 0 – 8. Cos values 0 to 7 corresponds to the eight cos levels supported within the AP. Cos value 8 is used when no cos level should be assigned to an IP precedence value. The actual cos value for frames bearing IP precedence values mapped to cos value 8 will be determined by other classifiers.

Output Parameters

Success or Failure

Description

This command modifies the IP precedence to class of service (cos) classification rule to map the eight IP precedence values to the eight cos values specified in this command on an interface.

Defaults

IP precedence value 0 maps to cos 0.
IP precedence value 1 maps to cos 1.
IP precedence value 2 maps to cos 2.
IP precedence value 3 maps to cos 3.
IP precedence value 4 maps to cos 4.
IP precedence value 5 maps to cos 5.
IP precedence value 6 maps to cos 6.
IP precedence value 7 maps to cos 7.

Usage Guidelines

The cos values specified in this command will be assigned to the received frame if one of the eight IP precedence values is found in the frame and the classifiers with higher precedence cannot determine the frame’s cos value. If the IP precedence value found within the received frame is mapped to cos value 8, then the ipprecedence-to-cos classifier will not be able to determine the actual cos value for the frame. In this case, a classifier with lower precedence must determine the cos value for the received frame. Include the ipprecedence classifier in the class-order string when configuring ingress-class-order to determine a frame’s cos value using its IP precedence.

Examples

```
ipprecedence-to-cos interface eth0 default
ipprecedence-to-cos interface eth0 cos “1 5 3 6 7 8 0 2”
```

See Also

```
qos(config)> ingress-class-order
qos(show)> ipprecedence-to-cos
```

qos(show)> ipprecedence-to-cos

Use this command to display class of service (cos) values mapped to IP precedence values.

Syntax

```
ipprecedence-to-cos [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the IP precedence to cos classification rules for interface *interface-name*. The IP precedence to cos classification rules for all interface are shown if *interface-name* is not specified.

Output Parameters

interface	Name of the interface.
cos	cos values ranging from 0 – 7, or 8 (means not defined) corresponding to the eight IP precedence values.

Description

This command displays the classification rule for the ipprecedence-to-cos classifier, which maps cos values to the IP precedence values.

Defaults

None

Usage Guidelines

The command can be used to verify which cos value will be assigned to IP packets containing various IP precedence values when no classifier with higher precedence has been satisfied.

Examples

```
qos(show)> ipprecedence-to-cos interface eth0

interface : eth0
cos       : 0 1 2 3 4 5 6 7
```

See Also

```
qos(config)> ipprecedence-to-cos
qos(show)> ingress-class-order
```

qos(show)> ipprotocol-to-cos

Use this command to display the class of service (cos) values assigned to IP protocols on an interface.

Syntax

```
ipprotocol-to-cos [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the IP protocol to cos classification rules for interface *interface-name*. The IP protocol to cos classification rules for all interfaces will be shown if *interface-name* is not specified.

Output Parameters

interface	Name of the interface
proto	IP protocol with values ranging from 0 – 255.
cos	cos with values ranging from 0 – 7.

Description

This command displays the classification rules for the IP protocol-to-cos classifier, which assigns cos values to IP packets based on the IP header’s protocol field.

Defaults

The IP protocol-to-cos classification rules for all interfaces are displayed.

Usage Guidelines

This command can be used to verify which cos value will be assigned to IP packets containing various IP protocols when no classifier with higher precedence has been satisfied.

See Also

```
qos(show)> ipprotocol-to-cos interface eth0

interface : eth0
proto     : 57
```

See Also

```
cos       : 3qos(config)> add-ipproto-to-cos
qos(config)> delete-ipproto-to-cos
qos(show)> ingress-class-order
```

qos(show)> statistics

Use this command to display Quality of Service (QoS) statistics.

Syntax

```
statistics [interface interface-name]
```

Input Parameters

interface *interface-name* — (Optional) Display QoS statistics for interface *interface-name.* Statistics for all interfaces in the AP are displayed if *interface-name* is not specified.

Output Parameters

interface — Name of the interface.

in-pktcount-index-to-cos — A set of counters corresponding to the number packets the access point has received and classified to each cos value.

out-pkt-count-index-to-cos — A set of counters corresponding to the number of packets the access point has transmitted at each cos value.

Description

This command displays the number of packets the AP has received and transmitted for each cos value.

Defaults

QoS statistics for all interfaces in the AP are displayed.

Usage Guidelines

This command can be used to determine the distribution of packets across all cos values.

Examples

```
qos(show)> statistics

interface                 : wlan1
in-pktcount-index-to-cos  : 0 0 0 0 0 0 0 0
out-pktcount-index-to-cos : 221 0 0 0 0 0 0 467
--------------------------------------------------------------------------

interface                 : wlan0
in-pktcount-index-to-cos  : 0 0 0 0 0 0 0 0
out-pktcount-index-to-cos : 220 0 0 0 0 0 0 467
--------------------------------------------------------------------------

interface                 : eth0
in-pktcount-index-to-cos  : 1136 0 0 0 0 0 475 0
out-pktcount-index-to-cos : 353 0 0 0 0 0 1124 4
```

See Also

```
qos(config)> clear-statistics
```

qos(config)> tcid-to-cos

Use this command to assign class of service (cos) values to 802.11 traffic classes.

Syntax

tcid-to-cos **interface** *interface-name* {**default** | **cos** *tcid0-cos … tcid7-cos*}

Input Parameters

interface *interface-name*	Specifies *interface-name* as the radio interface for which the TCID to cos classification rule will be configured.
default	Revert to the default TCID/cos mapping: 0/0, 1/1, 2/2, … 7/7.
cos *tcid0-cos* … *tcid7-cos*	A list of eight cos values corresponding to TCID 0 … TCID 7, which represent the TCID/cos mapping.

Output Parameters

Success or Failure

Description

This command creates a classification rule for the TCID-to-cos classifier which establishes the traffic class identifier (TCID) to cos mapping by specifying the cos values for various TCIDs.

Defaults

The default TCID/cos mapping is 0/0, 1/1, 2/2, 3/3, 4/4, 5/5, 6/6, 7/7.

Usage Guidelines

802.11 frames with a TCID received by the AP will be assigned cos values defined by this command when classifiers with higher precedence cannot determine the frames’ cos value. The default set of classifiers for the wireless interface classify frames based on TCID, station MAC address, VLAN ID, and receive interface.

Examples

```
tcid-to-cos interface eth0 cos “7 6 5 4 3 2 1 0”
```

See Also

```
qos(config)> cos-to-tcid
qos(config)> ingress-class-order
qos(show)> tcid-to-cos
```

qos(show)> tcid-to-cos

Use this command to display 802.11 traffic class to class of service (cos) maps.

Syntax

```
tcid-to-cos [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the traffic class identifier (TCID) to cos classification rule for interface *interface-name*. The TCID to cos classification rule for each radio in the AP is displayed if *interface-name* is not specified.

Output Parameters

interface	Name of the interface.
cos	A list of eight cos values corresponding to each TCID.

Description

This command displays the classification rule for the tcid-to-cos classifier, which maps cos values to 802.11 frames containing various TCIDs.

Defaults

tcid-to-cos classification rules for all radio interfaces are displayed.

Usage Guidelines

This command can be used to determine which cos value will be assigned to an 802.11 frame containing various TCIDs when no classifier with higher precedence has been satisfied.

Examples

```
qos(show)> tcid-to-cos interface wlan1

interface : wlan1
cos       : 0 1 2 3 4 5 6 7
```

See Also

```
qos(config)> tcid-to-cos
qos(show)> ingress-class-order
```

qos(config)> vlan-to-cos

Use this command to assign a class of service (cos) to a VLAN on an interface.

Syntax

```
vlan-to-cos interface interface-name vlan-id vlan-id (default | no-cos | cos
cos-value}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface for which the VLAN to cos classification rule will be created.
vlan-id *vlan-id*	Specifies the VLAN to which the cos value will be assigned.
default	Revert the cos assigned to the VLAN to no-cos on the interface.
no-cos	Specifies no cos value will be assigned to vlan *vlan-id* on the interface.
cos *cos-value*	Cos *cos-value* will be assigned to vlan *vlan-id* on the interface.

Output Parameters

Success or Failure

Description

This command creates a classification rule for the VLAN-to-cos classifier, which assigns cos values to untagged frames placed into one of the VLANs the interface is a member of.

Defaults

Cos value 0 is assigned to a VLAN by default.

Usage Guidelines

Untagged frames that have been placed into the VLAN specified by this command will be assigned the associated cos value when classifiers with higher precedence cannot determine the frame’s cos value. The default set of classifiers for the wireless interface classify frames based on TCID, station MAC address, VLAN ID, and receive interface. The default set of classifiers for the Ethernet interface classify frames based on VLAN ID and receive interface.

Examples

```
vlan-to-cos interface eth0 vlan-id 2 cos 2
```

See Also

```
qos(config)> ingress-class-order
qos(config)> tcid-to-cos
qos(show)> vlan-to-cos
```

qos(show)> vlan-to-cos

Use this command to display the class of service (cos) value assigned to VLANs created in the AP.

Syntax

```
vlan-to-cos [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display the VLAN to cos classification rules for interface *interface-name.* The VLAN to cos classification rules for all interfaces will be shown if *interface-name* is not specified.

Output Parameters

vlanid	VLAN identifier of the VLAN.
interface	Name of the interface.
cos	The cos value assigned to the VLAN on this interface.

Description

This command displays the classification rules for the VLAN-to-cos classifier which assigns cos values to untagged frames placed into one of the VLANs the interface is a member of.

Defaults

VLAN-to-cos classification rules for all interfaces are displayed.

Usage Guidelines

This command can be used to verify which cos value will be assigned to untagged frames that did not satisfy any classifier with higher precedence.

Examples

```
qos(show)> vlan-to-cos interface wlan0

vlanid    : 1
interface : wlan0
cos       : 0
---------------------------------------------------------------------------

vlanid    : 88
interface : wlan0
cos       : 0
---------------------------------------------------------------------------

vlanid    : 254
interface : wlan0
cos       : 0
```

See Also

```
qos(config)> vlan-to-cos
qos(show)> ingress-class-order
```

10 Radio CLIs

This chapter includes information about the following radio commands:

- **radio(config)> admin-state**
- **radio(config)> ap-name-in-beacon**
- **radio(show)> ap-name-in-beacon**
- **radio(config)> background-scanning**
- **radio(show)> background-scanning**
- **radio(config)> basic-rate-set**
- **radio(show)> basic-rate-set**
- **radio(config)> beacon**
- **radio(show)> beacon**
- **radio(config)> channel**
- **radio(show)> channel**
- **radio(config)> channel-set**
- **radio(show)> channel-set**
- **radio(config)> clear-iapp-statistics**
- **radio(config)> clear-radio-statistics**
- **radio(config)> clear-station-statistics**
- **radio(config)> commit-global-settings**
- **radio(config)> disassociate**
- **radio(config)> dot11-extensions**
- **radio(show)> dot11-extensions**
- **radio(config)> dot11g-protection**
- **radio(show)> dot11g-protection**
- **radio(config)> dot11-mac**
- **radio(show)> dot11-mac**
- **radio(config)> dot11-mode-in-2.4band**
- **radio(show)> dot11-mode-in-2.4band**
- **radio(config)> dot11-qos**
- **radio(config)> iapp**
- **radio(show)> iapp**
- **radio(show)> iapp-neighbor-statistics**
- **radio(show)> iapp-statistics**
- **radio(show)> iapp-topology**
- **radio(config)> network-connectivity**
- **radio(show)> network-connectivity**
- **radio(config)> network-density**
- **radio(show)> network-density**

- **radio(config)> persona**
- **radio(show)> persona**
- **radio(show)> radio-neighbors**
- **radio(show)> radio-state**
- **radio(show)> radio-statistics**
- **radio(show)> radio-version**
- **radio(config)> rate**
- **radio(show)> rate**
- **radio(config)> reselect-channel**
- **radio(config)> reset-radio**
- **radio(show)> station-association-table**
- **radio(show)> station-link-statistics**
- **radio(show)> station-security-statistics**
- **radio(config)> world-mode**
- **radio(show)> world-mode**

radio(config)> admin-state

Use this command to enable or disable an AP radio.

Syntax

```
admin-state interface interface-name { disable | enable }
```

Input Parameters

interface	Apply only to specific radio interfaces acting as an AP.
admin-state	Disable or enable the radio interface.

Output Parameters

Success or Failure

Description

This command is used to disable or enable a radio interface operating in AP mode. When you disable an AP radio, all the currently associated stations are forced to disassociate. When the radio is enabled, the radio interface is reinitialized. A radio which is operating in BP mode cannot be administratively disabled.

Defaults

None

Usage Guidelines

Changing the admin-state of a radio must be done with caution because it forces a reinitialization of the radio interface. Such changes result in disruption to existing WLAN usage and are best done during a maintenance window when the access-point is not heavily used.

Examples

```
admin-state interface wlan0 disable
<do radio configuration>
admin-state interface wlan0 enable
```

See Also

```
radio(show)> radio-config
radio(show)> radio-state
```

radio(config)> ap-name-in-beacon

Use this command to configure AP name in beacon to facilitate ease of identifying this specific AP during troubleshooting.

Syntax

```
ap-name-in-beacon name name
```

Input Parameters

name	Use the name for identifying this AP.

Output Parameters

Success or Failure

Description

This command is used to configure a proprietary feature. By using this command, all radios in this AP will send out a proprietary information-element in the beacon to advertise itself by name. Typically, all APs advertise their BSSIDs, which are the unique mac-address of each of their radios. Airgo APs can identify themselves by name in addition to BSSID to improve ease with which they can be identified. The identification would be only visible to Airgo Clients.

Defaults

None

Usage Guidelines

Identifying APs by name, especially when they have more than one radio, makes it easy for an administrator to connect to the AP for troubleshooting purposes. Administrator would need an Airgo client to use this proprietary feature. By default the APs ethernet MAC address is set as the AP name in beacon. It is recommended that you change the default setting.

Examples

```
ap-name-in-beacon name “california-ap-21”
```

See Also

```
radio(show)> ap-name-in-beacon
radio(show)> radio-state
```

radio(show)> ap-name-in-beacon

Use this command to display configured AP name in beacon.

Syntax

```
ap-name-in-beacon
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to display configured AP name in beacon.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> ap-name-in-beacon

beacon name : AP-00:0a:f5:00:01:f2
```

See Also

```
radio(config)> ap-name-in-beacon
radio(show)> radio-state
```

radio(config)> background-scanning

Use this command to enable or disable background scanning on the AP.

Syntax

```
background-scanning { disable | enable }
```

Input Parameters

admin-state	Enable/disable background scanning.

Output Parameters

Success or Failure

Description

This command is used to enable/disable background scanning.

Defaults

None.

Usage Guidelines

TBD.

Examples

```
Background-scanning enable
```

See Also

None

radio(show)> background-scanning

Use this command to display configured background scanning state.

Syntax

```
background-scanning
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to display configured background scanning state.

Defaults

None.

Usage Guidelines

None.

Examples

```
radio(show)> background-scanning

background-scanning : enable
```

radio(config)> basic-rate-set

Use this command to configure basic rate set of a AP radio interface, for IEEE 802.11a-g or IEEE802.11b modes.

Syntax

```
basic-rate-set interface interface-name { [ dot11a-rates rate {...} ] [
dot11g-rates rate {...} ] [ dot11b-rates rate {...} ] }
```

Input Parameters

interface	Apply this command to a specific radio interface.
dot11a-rates	Series of standard data rates in mbits/sec for dot11a mode.
dot11g-rates	Series of standard data rates in mbits/sec for do11g mode.
dot11b-rates	Series of standard data rates in mbits/sec for do11b mode.

Output Parameters

Success or Failure

Description

This command is used to configure a basic rate on a AP radio interface for the dot11a, dot11g and dot11b modes. The basic rate set is advertised in the beacons and probe responses to STAs. STAs have to support the minimum set of basic rates to be part of the BSS.

Mode	Standard Data Rates (mbits/sec)
IEEE 802.11a	6, 9, 12, 18, 24, 36, 48 and 54
IEEE 802.11g	6, 9, 12, 18, 24, 36, 48 and 54
IEEE 802.11b	1, 2, 5.5 and 11

Defaults

None

Usage Guidelines

Using this command, the basic rate set can be configured. STAs have to support the minimum set of basic rates to be part of the BSS. In addition, 802.11 control frames such as RTS, CTS, or ACKs are transmitted at basic rates.

Examples

```
basic-rate-set interface wlan0 dot11b 1 5.5 11
basic-rate-set interface wlan0 dot11a 9 18 36 48 54
```

See Also

```
radio(show)> basic-rate-set
radio(show)> radio-state
```

radio(show)> basic-rate-set

Use this command to display configured basic rate set of a AP radio interface for IEEE 802.11a-g or IEEE802.11b modes.

Syntax

```
basic-rate-set [ interface interface-name ]
```

Input Parameters

interface Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to display configured basic data rates on a AP radio interface for the dot11a, dot11b and dot11g modes.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> basic-rate-set

interface             : wlan0
persona               : any
dot11b-basic-rate-set : 1 2 5.5 11
dot11a-basic-rate-set : 6 12 24
dot11g-basic-rate-set : 6 12 24
---------------------------------------------------------------------------

interface             : wlan1
persona               : any
dot11b-basic-rate-set : 1 2 5.5 11
dot11a-basic-rate-set : 6 12 24
dot11g-basic-rate-set : 6 12 24

radio(show)> basic-rate-set interface wlan0

interface             : wlan0
persona               : any
dot11b-basic-rate-set : 1 2 5.5 11
dot11a-basic-rate-set : 6 12 24
dot11g-basic-rate-set : 6 12 24
```

See Also

```
radio(config)> basic-rate-set
radio(show)> radio-state
```

radio(config)> beacon

Use this command to configure beacon parameters on each radio interface.

Syntax

```
beacon interface interface-name beacon-period value-in-microseconds dtim-
period count
```

Input Parameters

interface	Optional parameter to specify radio interface.
beacon-period	Beacon period in units of milli-seconds.
dtim-period	DTIM period count in multiples of beacon-period.

Output Parameters

Success or Failure

Description

This command allows you to configure the beacon-period and dtim-period on a per radio interface basis. The following section describes the configuration parameters in detail. These parameters are applicable to radio interfaces operating in AP mode. If applied to a radio currently in BP mode, the configuration is cached until such time that the radio interface is reverted to AP mode. For the parameters to take effect, you must use reset-radio command after issuing this command.

Parameter	Description
Beacon-Period	This defines the beacon interval for the BSS (or radio with AP persona) in milli-seconds. The valid range is 50 to 65000 milli-seconds. The default value is 100 milli-seconds.
DTIM Period	This defines the periodicity of the traffic indication map for a STA in units of *n* times beacon period. The valid range is 1 to 10.

Defaults

None

Usage Guidelines

It is recommended that the default settings are not changed. These settings could be modified for diagnostic purposes.

Examples

```
auto-trunking
```

See Also

```
radio(show)> beacon
radio(config)> ap-name-in-beacon
radio(show)> radio-state
```

radio(show)> beacon

Use this command to display beacon configuration on each radio interface.

Syntax

```
beacon [ interface interface-name ]
```

Input Parameters

interface	Optional parameter to specify radio interface.

Output Parameters

Success or Failure

Description

This command allows you to display configured *beacon-period* and *dtim-period* on a per radio interface basis.

Defaults

None

Examples

```
radio(show)> beacon interface wlan0

interface     : wlan0
persona       : any
beacon-period : 100
dtim-period   : 1
```

See Also

None

radio(config)> channel

Use this command to either configure a radio to automatically select the best available channel or manually set to a specific channel.

Syntax

```
channel interface interface-name { channel channel-id | auto-select-startup |
auto-select-periodic seconds }
```

Input Parameters

interface	Apply this command to a specific radio interface.
channel	Set the channel to a fixed legal value (based on allowable channel set).
auto-select-startup	Use DFS to auto-select channel only once, at system startup time.
auto-select-periodic *Seconds*	Use DFS to auto select channel and reevaluate and change the channel if necessary by executing DFS algorithm periodically, as set in units of seconds.

Output Parameters

Success or Failure

Description

This command is used either to configure a specific channel on a radio interface or allow it to be auto-configured.

Parameter	Description
auto-select-startup	This mode triggers the use of one of the configured DFS algorithms only when AP is rebooted. Subsequently, no DFS algorithms are run.
auto-select-periodic	This mode triggers periodic evaluation of best channel.

Using the DFS algorithms, auto-select channel settings would ensure that the AP chooses the best channel and network operates efficiently to maximize system throughput. Depending on the needs, DFS can be run only once at startup time or run periodically.

The following are the valid channel IDs:

Channel-ID	Frequency (Center Frequency in MHZ)
1	2.4 GHZ Band – 2412 MHZ
2	2.4 GHZ Band – 2417 MHZ
3	2.4 GHZ Band – 2422 MHZ
4	2.4 GHZ Band – 2427 MHZ
5	2.4 GHZ Band – 2432 MHZ
6	2.4 GHZ Band – 2437 MHZ
7	2.4 GHZ Band – 2442 MHZ
8	2.4 GHZ Band – 2447 MHZ

Channel-ID	Frequency (Center Frequency in MHZ)
9	2.4 GHZ Band – 2452 MHZ
10	2.4 GHZ Band – 2457 MHZ
11	2.4 GHZ Band – 2462 MHZ
12	2.4 GHZ Band – 2467 MHZ
13	2.4 GHZ Band – 2472 MHZ
34	5 GHZ Band – 5170 MHZ
36	5 GHZ Band – 5180 MHZ
38	5 GHZ Band – 5190 MHZ
40	5 GHZ Band – 5200 MHZ
42	5 GHZ Band – 5210 MHZ
44	5 GHZ Band – 5220 MHZ
46	5 GHZ Band – 5230 MHZ
48	5 GHZ Band - 5240 MHZ
52	5 GHZ Band - 5260 MHZ
56	5 GHZ Band - 5280 MHZ
60	5 GHZ Band - 5300 MHZ
64	5 GHZ Band - 5320 MHZ
100	5 GHZ Band - 5500 MHZ
104	5 GHZ Band - 5520 MHZ
108	5 GHZ Band - 5540 MHZ
112	5 GHZ Band - 5560 MHZ
116	5 GHZ Band - 5580 MHZ
120	5 GHZ Band - 5600 MHZ
124	5 GHZ Band - 5620 MHZ
128	5 GHZ Band - 5640 MHZ
132	5 GHZ Band - 5660 MHZ
136	5 GHZ Band - 5680 MHZ
140	5 GHZ Band - 5700 MHZ
149	5 GHZ Band - 5745 MHZ
153	5 GHZ Band - 5765 MHZ
157	5 GHZ Band - 5785 MHZ
161	5 GHZ Band - 5805 MHZ

Defaults

None

Usage Guidelines

In most circumstances, choosing an auto-select channel is most optimum and reduces the complexity of deployment. Use of DFS (auto-select-channel) avoids the need for an elaborate site survey. The DFS is most useful if it is used periodically, not just at system startup time. This ensures that Airgo network auto-adapts to changing RF characteristics of the domain it serves.

Examples

```
channel interface wlan0 auto-select-periodic 360
```

See Also

```
radio(show)> channel
radio(config)> channel-set
radio(show)> channel-set
radio(show)> radio-state
```

radio(show)> channel

Use this command to display channel configuration of a radio.

Syntax

```
channel [ interface interface-name ]
```

Input Parameters

interface Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

Use this command to display whether the radio interface is either configured to be on a specific channel or auto-select feature has been enabled.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> channel interface wlan0

interface        : wlan0
persona          : any
dfs-trigger-type : auto-select-startup
```

See Also

```
radio(config)> channel
radio(config)> channel-set
radio(show)> channel-set
radio(show)> radio-state
```

radio(config)> channel-set

Use this command to configure the band or explicit list of channels that can be used by a specific radio interface.

Syntax

```
channel-set interface interface-name { { band { 2.4 | 5 | both | any }} | {
channel-list channel-id {...} }
```

Input Parameters

interface	Apply this criteria to a specific radio interface only.
band	Band settings - either 2.4 GHZ, 5 GHZ, both, or any of the two.
channel-list	List of channels, as specified by their IDs.

Output Parameters

Success or Failure

Description

This command can be used to configure either the band or the channels that can be used specific radio interface. When a band is specified, all channels in that band are available for scanning and channel selection. Similarly, if a specific list of channels are specified, only those channels are scanned (or validated against, when set manually).

When setting channel-list explicitly, only legal channels for the specific world-mode (country setting) are allowed, as shown below:

Channel-ID	Frequency (Center Frequency in MHZ)
1	2.4 GHZ Band – 2412 MHZ
2	2.4 GHZ Band – 2417 MHZ
3	2.4 GHZ Band – 2422 MHZ
4	2.4 GHZ Band – 2427 MHZ
5	2.4 GHZ Band – 2432 MHZ
6	2.4 GHZ Band – 2437 MHZ
7	2.4 GHZ Band – 2442 MHZ
8	2.4 GHZ Band – 2447 MHZ
9	2.4 GHZ Band – 2452 MHZ
10	2.4 GHZ Band – 2457 MHZ
11	2.4 GHZ Band – 2462 MHZ
12	2.4 GHZ Band – 2467 MHZ
13	2.4 GHZ Band – 2472 MHZ
34	5 GHZ Band - 5170 MHZ
36	5 GHZ Band - 5180 MHZ
38	5 GHZ Band - 5190 MHZ

Channel-ID	**Frequency (Center Frequency in MHZ)**
40	5 GHZ Band - 5200 MHZ
42	5 GHZ Band - 5210 MHZ
44	5 GHZ Band - 5220 MHZ
46	5 GHZ Band - 5230 MHZ
48	5 GHZ Band - 5240 MHZ
52	5 GHZ Band - 5260 MHZ
56	5 GHZ Band - 5280 MHZ
60	5 GHZ Band - 5300 MHZ
64	5 GHZ Band - 5320 MHZ
100	5 GHZ Band - 5500 MHZ
104	5 GHZ Band - 5520 MHZ
108	5 GHZ Band - 5540 MHZ
112	5 GHZ Band - 5560 MHZ
116	5 GHZ Band - 5580 MHZ
120	5 GHZ Band - 5600 MHZ
124	5 GHZ Band - 5620 MHZ
128	5 GHZ Band - 5640 MHZ
132	5 GHZ Band - 5660 MHZ
136	5 GHZ Band - 5680 MHZ
140	5 GHZ Band - 5700 MHZ
149	5 GHZ Band - 5745 MHZ
153	5 GHZ Band - 5765 MHZ
157	5 GHZ Band - 5785 MHZ
161	5 GHZ Band - 5805 MHZ

Defaults

None

Usage Guidelines

In certain deployments, a specific band is desirable from either RF planning or for backward compatibility with existing deployment. In other circumstances, a specific channel-list may be used as part of site-planning to ensure that DFS does not assign any other channels except from the specified list. If radio interface operates in BP mode, the channel set configuration determines the channels which the BP radio will scan.

Examples

```
channel-set interface wlan0 band 5
channel-set interface wlan1 channel-list 3 5 11
```

See Also

```
radio(show)> channel-set
radio(config)> channel
radio(show)> channel
radio(show)> radio-state
```

radio(show)> channel-set

Use this command to display configured band or explicit list of channels to be used by a specific radio interface.

Syntax

```
channel-set [ interface interface-name ]
```

Input Parameters

interface	Apply this criteria to a specific radio interface only.

Output Parameters

Success or Failure.

Description

Use this command to display the configured state of channel-set, which can either be a specific band or an explicit list of channels, assigned to a radio interface.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> channel-set

interface    : wlan0
persona      : any
scanned-band : any
---------------------------------------------------------------------------

interface    : wlan1
persona      : any
```

See Also

```
scanned-band : anyradio(config)> channel-set
radio(config)> channel
radio(show)> channel
radio(show)> radio-state
```

radio(config)> clear-iapp-statistics

Use this command to clear IAPP statistics.

Syntax

```
clear-iapp-statistics
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to clear the IAPP statistics counters.

Defaults

None

Usage Guidelines

None

Examples

```
clear-iapp-statistics
```

See Also

```
radio(show)> iapp-statistics
radio(show)> radio-config
radio(show)> radio-state
```

radio(config)> clear-radio-statistics

Use this command to clear radio statistics.

Syntax

```
clear-radio-statistics { interface interface-name}
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to clear the radio statistics counters.

Defaults

None

Usage Guidelines

None

Examples

```
clear-radio-statistics interface wlan0
```

See Also

```
radio(show)> radio-statistics
radio(show)> radio-state
```

radio(config)> clear-station-statistics

Use this command to clear station statistics, including station-link and station-security statistics.

Syntax

```
clear-station-statistics {station-mac station-mac-address
```

Input Parameters

station-mac	Apply this command to a specific associated station.

Output Parameters

Success or Failure

Description

This command is used to clear the station statistics counters of associated stations.

Defaults

None

Usage Guidelines

None

Examples

```
clear-station-statistics station-mac 00:0a:ff:21:2c:33
```

See Also

```
radio(show)> station-link-statistics
radio(show)> station-security-statistics
radion(show)> station-association-table
radio(show)> radio-state
```

radio(config)> commit-global-settings

Use this command to commit all radio-specific global settings that have been configured previously.

Syntax

```
commit-global-settings
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to commit global radio-specific configuration settings. Configuration settings for all radios in the node are applied.

Defaults

None

Usage Guidelines

TBD.

Examples

```
commit-global-settings
```

See Also

```
radio(config)> reset-radio
```

radio(config)> disassociate

Use this command to force a specific station to be disassociated.

Syntax

```
disassociate station-mac sta-mac-address
```

Input Parameters

station-mac	Station mac-address.

Output Parameters

Success or Failure

Description

This command is used to force a station disassociation.

Defaults

None

Usage Guidelines

This command can be used for administrative purposes to disassociate a station after the user has removed from the radius server.

Examples

```
disassociate station-mac 00:ff:0c:09:3c:21
```

See Also

```
radio(show)> station-association-table
radio(show)> radio-state
```

radio(config)> dot11-extensions

Use this command to enable/disable IEEE 802.11 extensions or Airgo proprietary extensions to IEEE 802.11 standards on a radio interface.

Syntax

```
dot11-extensions interface interface-name { [ standard { disable | enable } ]
[ enhanced { disable | enable } ] }
```

Input Parameters	
interface	Apply this command to a specific radio interface.
standard	Enable/disable IEEE 802.11 standard extensions.
enhanced	Enable/disable Airgo proprietary IEEE 802.11 enhancements.

Output Parameters

Success or Failure

Description

This command is used to enable/disable IEEE 802.11 standard extensions or Airgo enhancements to IEEE 802.11 standards on a radio interface.

The standard IEEE 802.11 extensions are QoS (dot11-e), Spectrum Management (dot11-h), and ERP (dot11-g).

The Airgo enhancements include the following:

Airgo Feature	Description/Benefits
Enhanced data rate set	Provide higher data rates in 801.11b-g modes. This includes 72, 96, and 108 mbits/sec.
Burst Ack	Increase throughput by reducing number of acks.
Advanced Rate Adaptation	Enhanced automatic rate adaptation for maximum system throughput.
Wireless Backhaul	All Wireless Networking - Wireless Distribution System.
AP Name in Beacon	Enables easy identification of APs during STA association.

Defaults

None

Usage Guidelines

Airgo-enhanced extensions should be used when you have many, if not all, STAs that have Airgo-compatible clients. Airgo-enhanced extensions are also valuable when you have Airgo APs deployed, especially while using All Wireless Networking.

Examples

```
dot11-extensions interface wlan0 ieee-extensions disable
```

See Also

```
radio(show)> dot11-extensions
radio(show)> radio-state
```

radio(show)> dot11-extensions

Use this command to display configuration of IEEE 802.11 extensions or Airgo proprietary extensions on a radio interface.

Syntax

```
dot11-extensions [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

Use this command to display configuration of IEEE 802.11 extensions or Airgo enhancements to IEEE 802.11 standards on a radio interface.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> dot11-extensions interface wlan0

interface                : wlan0
persona                  : any
standard ieee-extensions : enable
enhanced-extensions      : enable
```

See Also

```
radio(config)> dot11-extensions
radio(show)> radio-state
```

radio(config)> dot11g-protection

Use this command to enable or disable dot11g protection on a specific radio interface.

Syntax

```
dot11g-protection interface interface-name { disable | enable }
```

Input Parameters

interface	Apply this command to a specific radio interface.
admin-state	Enable/disable background scanning.

Output Parameters

Success or Failure

Description

This command is used to enable/disable dot11g protection.

Defaults

None

Usage Guidelines

TBD.

Examples

```
dot11g-protection enable
```

See Also

None

radio(show)> dot11g-protection

Use this command to display configured dot11g protection state.

Syntax

```
dot11g-protection [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to display configured dot11g protection state.

Defaults

None

Usage Guidelines

None

Examples

```
dot11g-protection interface wlan0
```

See Also

None

radio(config)> dot11-mac

Use this command to configuration IEEE 802.11 MAC operational parameters.

Syntax

```
dot11-mac interface interface-name { [ frag-threshold frag-count ] [ rts-
threshold rts-threshold-value ] [ short-retry-limit short-retry-limit ] [
long-retry-limit long-retry-limit ] }
```

Input Parameters

interface	Apply this command to a specific radio interface.
frag-threshold	Fragment threshold settings.
rts-threshold	RTS threshold value.
short-retry-limit	Short retry limit.
long-retry-limit	Long retry limit.

Output Parameters

Success or Failure

Description

This command is used to set IEEE 802.11 MAC operational parameters of a radio. The following describes each of the operational parameters in detail. These parameters apply to both modes of the radio, AP or BP.

Parameter	Description
Fragment Threshold	This is the minimum packet size before fragmentation starts. The valid range is 256 to 2346. The default-value is 256.
RTS Threshold	This is the minimum packet-size before RTS/CTS is needed. The valid range is 0 to 2347. The default value is 2347.
Short Retry Limit	This is the maximum number of retries for non RTS-CTS packets. The valid range is 1 to 255. The default value is 7.
Long Retry Limit	This is the maximum number of retries for RTS-CTS packets. The valid range is 1 to 255. The default value is 4.

Defaults

See above.

Usage Guidelines

It is recommended that the default settings are not changed. The configuration should be changed only for diagnostic purposes.

Examples

```
dot11-mac interface wlan0 frag-threshold 512 rts-threshold 1024 short- retry-
limit 15 long-retry-limit 7
```

See Also

```
radio(show)> dot11-mac
radio(show)> radio-state
```

radio(show)> dot11-mac

Use this command to display configuration of IEEE 802.11 MAC operational parameters.

Syntax

```
dot11-mac [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to display IEEE 802.11 MAC operational parameters of a radio.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> dot11-mac interface wlan0

interface         : wlan0
persona           : any
frag-threshold    : 2000
rts-threshold     : 2347
short-retry-limit : 100
long-retry-limit  : 100
```

See Also

```
radio(config)> dot11-mac
radio(show)> radio-state
```

radio(config)> dot11-mode-in-2.4band

Use this command to configure the mode of operation to be either IEEE 802.11b only or IEEE 802.11g when operating in 2.4 GHz band on a specific radio interface.

Syntax

```
dot11-mode interface interface-name { dot11b-mode | dot11g-mode }
```

Input Parameters

interface	Apply this command a specific radio interface.
dot11b-mode	Operate the radio interface in dot11b mode.
dot11g-mode	Operate the radio interface in dot11g mode.

Output Parameters

Success or Failure

Description

This command is used to restrict the radio to either operate in the dot11b mode or in dot11g mode when operating in 2.4 GHz band.

Defaults

None

Usage Guidelines

By setting the dot11-mode on a radio to say dot11b-mode, you can ensure that dot11b compliant client stations can get service. On the other hand, by setting to dot11g-mode can prohibit dot11b clients can get service.

Examples

```
dot11-mode interface wlan0 dot11g-mode
```

See Also

```
radio(show)> dot11-mode
radio(show)> radio-state
```

radio(show)> dot11-mode-in-2.4band

Use this command to display the configured mode of operation in 2.4 GHz band to be either IEEE 802.11b only or IEEE 802.11g on a specific radio interface.

Syntax

```
dot11-mode [ interface interface-name ]
```

Input Parameters

interface	Apply this command a specific radio interface.

Output Parameters

Success or Failure

Description

This command is used to show the configured mode of operation in 2.4 GHz band, which is either dot11b or dot11g mode for each radio interface.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> dot11-mode-in-2.4band interface wlan0

interface        : wlan0
persona          : any
dot11-mode-state : dot11g
```

See Also

```
radio(config)> dot11-mode
radio(show)> radio-state
```

radio(config)> dot11-qos

Use this command to enable or disable IEEE 802.11e QoS features completely on the specified radio interface.

Syntax

```
dot11-qos interface interface-name { disable | enable }
```

Input Parameters

interface	Apply this command a specific radio interface.
admin-state	Enable/disable IEEE 802.11e QoS feature.

Output Parameters

Success or Failure

Description

This command is used to enable/disable IEEE 802.11e QoS features on a specific radio interface. By the default when QoS is enabled, the mode is set to EDCF. When disabled the mode is set to DCF.

Defaults

None

Usage Guidelines

TBD.

Examples

```
dot11-qos interface wlan0 enable
```

See Also

```
radio(show)> radio-config
radio(show)> radio-state
```

radio(config)> iapp

Use this command to configure Inter-Access-Point-Protocol (IAPP).

Syntax

```
iapp { disable | enable }
```

Input Parameters

admin-state	Enable/Disable IAPP.

Output Parameters

Success or Failure

Description

This command is used to configure IAPP, which is used to facilitate mobility of stations between APs. When IAPP is enabled, it enables faster convergence of L2 handoffs between APs using the IEEE 802.11f protocol. IAPP is also used for certain Airgo-specific enhanced features.

Defaults

None

Usage Guidelines

TBD.

Examples

```
iapp enable
```

See Also

```
radio(show)> iapp
radio(show)> iapp-neighbor-statistics
radio(show)> iapp-statistics
radio(show)> iapp-topology
```

radio(show)> iapp

Use this command to show the state of Inter-Access-Point-Protocol (IAPP).

Syntax

```
iapp
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the configured state of IAPP, which is used to facilitate mobility of stations between APs.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> iapp

admin-state : enable
oper-state  : enable
```

See Also

```
radio(config)> iapp
radio(show)> iapp-neighbor-statistics
radio(show)> iapp-statistics
radio(show)> iapp-topology
```

radio(show)> iapp-neighbor-statistics

Use this command to show IAPP-specific statistics of all neighbor radios discovered by this AP.

Syntax

```
iapp-neighbor-statistics [ radio-mac neighbor-radio-macaddr ]
```

Input Parameters

radio-mac	MAC address of neighbor radio discovered by IAPP.

Output Parameters

Success or Failure

Description

This command is used to show the IAPP-specific statistics of all radio neighbors discovered by this AP. The statistics include number of add notifications sent, number of add notifications received, number of move notifications sent, number of move notifications received, number of move responses sent, and number of move responses received.

Defaults

None

Usage Guidelines

These statistics are good to troubleshoot issues with L2 Mobility.

Examples

```
iapp-neighbor-statistics radio-mac 00:0a:ff:37:07:1c
```

See Also

```
radio(config)> iapp
radio(show)> iapp
radio(show)> iapp-statistics
radio(show)> iapp-topology
```

radio(show)> iapp-statistics

Use this command to show IAPP-specific global statistics.

Syntax

```
iapp-statistics
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show the IAPP-specific global statistics. The statistics include number of add notifications sent, number of add notifications received, number of move notifications sent, number of move notifications received, number of move responses sent, number of move responses received, number of move notification timeouts, number of move notifications retransmitted, number of move response failures sent, number of move response failures received, number of intra-AP moves, and number of intra-AP move failures.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> iapp-statistics

add-notify-packet-sent        : 1
add-notify-packet-rcvd        : 1
move-notify-packet-sent       : 0
move-notify-packet-rcvd       : 0
move-notify-packet-timeout    : 0
move-notify-packet-retransmit : 0
move-response-packet-sent     : 0
move-response-packet-rcvd     : 0
move-response-failures-sent   : 0
move-response-failures-rcvd   : 0
intra-ap-moves                : 0
intra-ap-move-failures        : 0
```

See Also

```
radio(config)> iapp
radio(show)> iapp
radio(show)> iapp-neighbor-statistics
radio(show)> iapp-topology
```

radio(show)> iapp-topology

Use this command to see the IAPP topology, comprising of all the radios discovered by this AP for IAPP interactions.

Syntax

```
iapp-topology
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to see the IAPP topology discovered by this access-points. This IAPP topology would provide a view of which other APs this AP is able to communicate with via IAPP and assist in seamless L2 mobility.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> iapp-topology

bssid      : 00:0a:f5:00:06:35
ipaddr     : 192.168.168.21
compatible : compatible
---------------------------------------------------------------------------

bssid      : 00:0a:f5:00:04:84
ipaddr     : 192.168.168.14
compatible : compatible
---------------------------------------------------------------------------

bssid      : 00:0a:f5:00:06:ac
ipaddr     : 192.168.168.14
compatible : compatible
---------------------------------------------------------------------------

bssid      : 00:0a:f5:00:06:dc
ipaddr     : 192.168.168.21
compatible : compatible
```

See Also

```
radio(config)> iapp
radio(show)> iapp
radio(show)> iapp-neighbor-statistics
radio(show)> iapp-statistics
```

radio(config)> network-connectivity

Use this command to configure network connectivity of this AP.

Syntax

```
network-connectivity { any | wired-only | wireless-only }
```

Input Parameters

any	This AP will accept either wired or wireless network connectivity.
wired-only	This AP will only accept wired network connectivity.
wireless-only	This AP will only accept wireless network connectivity.

Output Parameters

Success or Failure

Description

This command is used to configure network connectivity of the AP. When All-Wireless-Networking feature is available, the network connectivity setting of an AP would ensure that network connectivity of the AP is controlled and does not create side-effects.

For example, when an AP is only be used with Ethernet connectivity, setting that AP to wired-only will ensure that it will not participate in All-Wireless-Networking feature even when Ethernet media is disconnected.

Defaults

None

Usage Guidelines

The default value of Any means that the AP auto-determines whether or not to initiate a backhaul based on the presence or absence of an active Ethernet link. The Any setting is influenced by the number of radios in the Airgo AP and whether or not the AP has active Ethernet connectivity. If Any is selected, then the Airgo AP is allowed to change between wireless and wired mode based on a change in Ethernet status. The Wired-Only button means that the Airgo AP operates only as wired node. The node is disabled if the Ethernet link is not active. All radios take on the AP persona unless explicitly configured as a BP radio. The Wireless value means that the AP operates only as a wireless backhaul node with wireless backhaul connectivity to the wired network. On radio is automatically assigned the BP persona. It is recommended that you accept the default setting of Any.

Examples

```
network-connectivity wired-only
```

See Also

```
radio(show)> network-connectivity
radio(show)> radio-state
```

radio(show)> network-connectivity

Use this command to display configured state of network connectivity of this AP.

Syntax

```
network-connectivity
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show configured mode of network connectivity for the AP.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> network-connectivity

network-connectivity : any
```

See Also

```
radio(config)> network-connectivity
radio(show)> radio-state
```

radio(config)> network-density

Use this command to configuration the density of network deployment for this AP.

Syntax

```
network-density { low | medium | high }
```

Input Parameters

low	This AP is deployed in a low density network of APs.
medium	This AP is deployed in a medium density network of APs.
high	This AP is deployed in a high density network of APs.

Output Parameters

Success or Failure

Description

Network density configuration means how sparse is the AP deployed with other APs in the network. For example, in high-usage areas, where higher than normal network capacity is needed, it is recommended to deploy more APs in a denser configuration. By setting the network-density configuration parameter to match the physical deployment characteristics, APs will adjust their defer threshold to optimize overall system performance and maximize capacity.

This command is applicable to AP or BP persona of a radio interface. When using it for AP or BP mode, use reset-radio command to apply this change.

Defaults

Low

Usage Guidelines

When deploying more APs in a dense configuration, (for example, in a large conference room) setting the corresponding network-density settings to medium or high will ensure proper system behavior.

Examples

```
network-density high
```

See Also

```
radio(show)> wireless-config
radio(show)> radio-config
radio(show)> radio-state
```

radio(show)> network-density

Use this command to display configured state of network-density on this AP.

Syntax

```
network-density
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command can be used to show the current settings of network density.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> network-density

network-density : low
```

See Also

```
radio(config)> network-density
radio(show)> radio-state
```

radio(config)> persona

Use this command to configure the persona of each of the radios in an AP.

Syntax

```
persona **interface** *interface-name* { **any** | **ap-only** | **bp-only** }
```

Input Parameters

interface	Apply this command to a specific radio interface.
any	This radio interface can either be an AP or a BP radio.
ap-only	This radio interface will operate only as an AP.
bp-only	This radio interface will operate only as a BP.

Output Parameters

Success or Failure

Description

When persona is set to any, a radio can take on the operational mode of an AP or a BP. If it is set to AP only, then radio will operate in AP mode only, and if it is set to BP only it will operate in BP mode.

Defaults

Any

Usage Guidelines

Setting the any option would result in the system determining the mode of operation of the radio based on network connectivity, number of radios, and presence of ethernet connectivity. It is recommended that the default setting of any is not changed.

Examples

```
persona interface wlan0 ap-only
persona interface wlan1 bp-only
```

See Also

```
radio(show)> persona
radio(show)> radio-state
```

radio(show)> persona

Use this command to display current configured persona of each of the radios.

Syntax

```
persona [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command displays current configuration of persona of radio interfaces.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> persona

interface : wlan0
persona   : any
-------------------------------------------------------------------------

interface : wlan1
persona   : any
```

See Also

```
radio(config)> persona
radio(show)> radio-state
```

radio(show)> radio-neighbors

Use this command to see all the radio neighbors and their information.

Syntax

```
radio-neighbors [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command shows detailed information of all the neighboring radios as seen by this AP (or its specific radio). This information is extracted from beacons detected from these neighbor APs (BSSs). Information includes BSSID (MAC address of neighbor AP radio), SSID, BSS Type (infrastructure or ad-hoc), channel where neighbor BSS is detected, AP name in beacon, compatibilty status (indicates whether neighbor AP is Airgo), signal strength (Signal strength of neighbor AP signal), load percentage, and number of STAs.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> radio-neighbors

interface       : wlan0
bssid           : 00:0a:f5:00:04:84
ssid            : DeerCreekCo
channel-id      : 1
beacon name     : AP-00:0a:f5:00:02:9a
compatibility   : compatible
rssi            : -22
load-percentage : 0
bss-type        : infrastructure
----------------------------------------------------------------------------

interface       : wlan0
bssid           : 00:0a:f5:00:06:35
ssid            : AniNet
channel-id      : 6
beacon name     : AP-00:0a:f5:00:02:e2
compatibility   : compatible
rssi            : -49
load-percentage : 29
bss-type        : infrastructure
Success
---------------------------------------------------------------------------
```

```
interface       : wlan1
bssid           : 00:0a:f5:00:06:ac
ssid            : DeerCreekCo
channel-id      : 157
beacon name     : AP-00:0a:f5:00:02:9a
compatibility   : compatible
rssi            : -27
load-percentage : 0
bss-type        : infrastructure
--------------------------------------------------------------------------

interface       : wlan1
bssid           : 00:0a:f5:00:06:dc
ssid            : AniNet
channel-id      : 153
beacon name     : AP-00:0a:f5:00:02:e2
compatibility   : compatible
rssi            : -28
load-percentage : 1
bss-type        : infrastructure
```

See Also

```
radio(show)> radio-state
```

radio(show)> radio-state

Use this command to see all the radio state information.

Syntax

```
radio-state [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command shows detailed state information of radio interfaces of an AP. Information includes persona (AP or BP) of radio, MAC address, admin state (enabled or disabled), operational state (enabled or disabled), channel (current operating channel), number of associated stations (valid only for AP radio), number of trunks (valid only for AP radio), number of channel changes (valid only for AP radio), frequency change reason (reason for last frequency change), interference (on current channel), average station load (AP radio only), average channel utilization, average number of load-balanced stations, CFP period, CFP max duration, basic rate set, operational rate set, CCA mode supported, current CCA mode, temperaure mode, maximum MSDU receive lifetime, and external antenna (present or not).

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> radio-state

interface           : wlan0
oper-persona        : ap
mac                 : 00:0a:f5:00:06:ac
admin-state         : enable
oper-state          : enable
radio band          : 2.4GHz
radio channel       : 11
num-assoc-sta       : 0
num-trunks          : 0
num-channel-changes : 1
freq-change-cause   : no-change
interference        : -62
avg-sta-load        : 0
avg-channel-util    : 0
dot11-qos-type      : edcf
num-load-balanced   : 0
external-antenna    : no
---------------------------------------------------------------------------
```

```
interface           : wlan1
oper-persona        : bp
mac                 : 00:0a:f5:00:04:84
admin-state         : enable
oper-state          : enable
radio band          : 5GHz
radio channel       : 149
dot11-qos-type      : edcf
external-antenna    : no
```

radio(show)> radio-statistics

Use this command to see all the radio specific statistics.

Syntax

```
radio-statistics [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command shows detailed statistics of radio interfaces of an AP. The information includes transmitted fragment count, transmitted multicast frame count, count of failed MSDU transmissions, received fragment count, received frame count, FCS error count, received multicast frame count, multiple retry count, retry count, frame duplicate count, ack failure count, RTS success count, RTS fail count, transmitted frame count, WEP undecryptable count, and # of transmitted beacons.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> radio-statistics interface wlan0

interface                : wlan0
xmt-frg-cnt              : 28444
xmt-frame-cnt            : 28444
xmt-multicast-frame-cnt  : 518
failed-cnt               : 0
multiple-retry-cnt       : 1
retry-cnt                : 241
ack-failure-cnt          : 242
xmt-beacon               : 6652
rcv-fragment-cnt         : 8690
rcv-frame-cnt            : 46
fcs-error-cnt            : 4221
rcv-multicast            : 0
frame-dup-cnt            : 19
rts-success-cnt          : 0
rts-fail-cnt             : 0
wep-undecryptable-cnt    : 0
drop-cnt                 : 0
```

See Also

```
radio(config)> clear-radio-statistics
radio(show)> radio-state
```

radio(show)> radio-version

Use this command to see the hardware version and the mac-address assigned to all the radios of this AP.

Syntax

```
radio-version
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command shows hardware version information of all radios of an AP. The information includes radio hardware version and MAC address.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> radio-version

interface  : wlan0
mac        : 00:0a:f5:00:06:5a
product-id : AGN1323AR-00
hw-version : 1.3.0
--------------------------------------------------------------------------

interface  : wlan1
mac        : 00:0a:f5:00:06:17
product-id : AGN1323AR-00
hw-version : 1.3.0

interface      : wlan0
persona        : any
enhanced-rates : enable
autoadapt type : basic-auto-adapt
ack-mode       : immediate-ack
--------------------------------------------------------------------------

interface      : wlan1
persona        : any
enhanced-rates : enable
autoadapt type : basic-auto-adapt
ack-mode       : immediate-ack
```

See Also

```
radio(show)> radio-state
```

radio(config)> rate

Use this command to enable or disable Airgo-enhanced rates, set the ack-mode, or activate rate-adaptation features or set fixed rate for a radio interface.

Syntax

```
rate { interface interface-name   [ ack-mode { immediate-ack | burst-ack | no-
ack | auto-ack-policy } ] [ basic-auto-adapt | advance-auto-adapt |  fixed-
rate newrate ] [ enhanced-rates { disable | enable } ] }
```

Input Parameters

interface	Apply this command to a specific radio interface.
enhanced-rates	Enable/disable Airgo enhanced data rates.
basic-auto-adapt	Enable basic automatic data rate adaptation.
advance-auto-adapt	Enable advance automatic data rate adaptation.
fixed-rate	Disable automatic data rate adaptation and instead fix it a specific rate.
ack-mode	Set ack-mode to immediate-ack or burst-ack | no-ack | auto-ack-policy
immediate-ack	Immediate acknowledgements
burst-ack	Burst acknowledgements
no-ack	No acknowledgements
auto-ack-policy	Auto acknowledgements

Output Parameters

Success or Failure

Description

This command enables or disables the use of enhanced data rates on a specific radio interface of this AP. Independently, it lets you configure automatic rate adaptation feature at two levels: basic or advance; or you can completely bypass this feature to instead set a fixed data rate on this radio. In addition, Airgo-prorietary ack-mode can be configured.

Parameter	Description
Enhanced Rates	The enhanced rates are rates higher than IEEE 802.11a/g rate of 54 mbits/sec. These are Airgo-enhanced rates of 72, 96, and 108 mbits/sec. When enhanced rates are enabled, the radio interface will select the best rates possible, even beyond the standard of 54 mbits/sec.
Basic Auto Rate Adaptation	This configuration enables basic automatic rate adaptation feature. This one uses the transmitter-based rate adaptation algorithm.
Advance Auto Rate Adaptation	This configuration enables advanced automatic rate adaptation feature. This one uses the receiver-based rate adaptation algorithm (receiver measured link quality based).
Rate	The radio can be set to operate at a fixed rate (standard or proprietary). With this option, rate adaptation is automatically disabled.
Acknowledgements mode	

Defaults

None

Usage Guidelines

In all Airgo networks, when both AP and STA are Airgo equipment, enabling enhanced-rates would get you the higher data-rate without compromising interoperability with other non-Airgo clients. ack-mode can be configured in an all Airgo network (AP and stations are Airgo).

Examples

```
rate interface wlan0 enhanced-rate enable advance-auto-adapt
```

See Also

```
radio(show)> rate
radio(config)> basic-rate-set
radio(show)> basic-rate-set
radio(config)> dot11-extensions
radio(show)> dot11-extensions
radio(show)> radio-state
```

radio(show)> rate

Use this command to display current rate settings of a radio interface.

Syntax

```
rate [ interface interface-name ]
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

This command displays the current state of rate configuration on radio interfaces of this AP.

Defaults

None

Usage Guidelines

None

Examples

```
rate interface wlan0
```

See Also

```
radio(config)> rate
radio(config)> basic-rate-set
radio(show)> basic-rate-set
radio(config)> dot11-extensions
radio(show)> dot11-extensions
radio(show)> radio-state
```

radio(config)> reselect-channel

Use this command to execute channel auto-selection (DFS) algorithm now on a specific radio interface.

Syntax

```
reselect-channel interface interface-name
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

When auto-select channel is enabled, it runs during radio initialization, or at a preconfigured time interval. This command lets you run the DFS algorithm on an AP radio at that instant, when triggered by the user.

Defaults

None

Usage Guidelines

If auto-select channel is used and channel-related configuration has changed or surrounding RF environment (for example addition of a new neighboring APs), use this command to trigger the DFS algorithm. This will result in the selection of best available channel and a switch over to that channel. This command applies only for radios operating in AP mode.

Examples

```
Reselect-channel interface wlan0
```

See Also

```
radio(config)> channel
radio(show)> channel
radio(config)> channel-set
radio(show)> channel-set
radio(show)> radio-state
```

radio(config)> reset-radio

Use this command to reset a specific radio interface.

Syntax

```
reset-radio interface interface-name
```

Input Parameters

interface	Apply this command to a specific radio interface.

Output Parameters

Success or Failure

Description

Use this command to reset a radio interface. This command is also recommended to be used for specific radio configurations to take effect.

Defaults

None

Usage Guidelines

This is a service-affecting action command. The radio should be reset only during maintenance windows.

Examples

```
reset-radio interface wlan0
```

See Also

```
radio(show)> radio-state
```

radio(show)> station-association-table

Use this command to see all the STAs associated with this AP, on a per-radio basis.

Syntax

```
station-association-table [ interface interface-name ]
```

Input Parameters

interface	This command applies to a specific radio interface.

Output Parameters

Success or Failure

Description

Use this command to display all the associated stations, and related station information such as station mac-address, user name, ssid, group station belongs to, association status (associated or reassociated), association typet (normal or transferred), type of authentication used, encryption used, and current association status.

Defaults

None

Usage Guidelines

Use this information to monitor the stations connected to this AP. You may force a station to be disconnected by using *disassociate* radio config command.

Examples

```
radio(show)> station-association-table

interface        : wlan1
station-mac-addr : 00:0a:f5:00:05:fe
assoc-type       : Normal
auth-type        : WPA PSK
encryption-type  : AES
status           : associated
ssid             : DeerCreekCo
group-name       :
compatibility    : compatible
```

See Also

```
radio(config)> disassociate
radio(show)> station-link-statistics
radio(show)> station-security-statistics
radio(show)> radio-state
```

radio(show)> station-link-statistics

Use this command to see the link statistics of an associated STA.

Syntax

```
station-link-statistics station-mac station-mac-address
```

Input Parameters

station-mac	This command applies to an associated station.

Output Parameters

Success or Failure

Description

Use this command to display all the link statistics of an associated station, such as associated mode (11a/b/g), uplink and downlink signal-strength or signal-quality, uplink rate, downlink rate, number of packets/bytes sent and received, number of transmitted fragments, number of failed transmitted packets, number of single retry packets, number of multiple retry packets, number of ack timeouts, etc.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> station-link-statistics station-mac 00:0a:f5:00:05:fe

station-mac            : 00:0a:f5:00:05:fe
sta-mode               : 802.11a
sta-uplink-rssi        : 100
sta-uplink-sinr        : 100
sta-uplink-rate        : 18
sta-downlink-rssi      : 100
sta-downlink-sinr      : 100
sta-downlink-rate      : 96
sta-rcv-byte-cnt       : 96806
sta-xmt-byte-cnt       : 76634
sta-xmt-frg-cnt        : 1120
sta-failed-xmt-pkt     : 0
sta-single-retry-pkt   : 539
sta-multiple-retry-pkt : 279
sta-ack-timeouts       : 1089
```

See Also

```
radio(config)> disassociate
radio(show)> station-association-table
radio(show)> station-security-statistics
radio(show)> radio-state
```

radio(show)> station-security-statistics

Use this command to see the security statistics of an associated STA.

Syntax

```
station-security-statistics station-mac station-mac-address
```

Input Parameters

station-mac	This command applies to an associated station.

Output Parameters

Success or Failure

Description

Use this command to display all the security statistics of an associated station, such as authentication type, encryption type, number of AES transmitted blocks, number of received AES blocks, number of AES replays, number of AES decrypt errors, WEP excluded count, and WEP undecryptable count.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> station-security-statistics station-mac 00:0a:f5:00:05:fe

station-mac             : 00:0a:f5:00:05:fe
sta-auth-type           : WPA-PSK
sta-encryption-type     : AES
sta-aes-xmt-blk         : 5572
sta-aes-rcv-blk         : 6837
sta-aes-replays         : 37
sta-aes-decrypt-errors  : 0
```

See Also

```
radio(config)> disassociate
radio(show)> station-association-table
radio(show)> station-link-statistics
radio(show)> radio-state
```

radio(config)> world-mode

Use this command to set the world-mode of this AP.

Syntax

```
world-mode { default-country | country country-code } [ environment { any |
indoor | outdoor } ] [ multi-domain { disable | enable } ]
```

Input Parameters

default-country	Default country code set at manufacturing time.
country	Set the world-mode to a specific country by entering its 2 letter country-code.
environment	Set the environment in which AP is deployed.
any	This AP could be deployed indoor or outdoor.
indoor	This AP is deployed indoor.
outdoor	This AP is deployed outdoor.
multi-domain	Enable/Disable of sending world mode related parameters

Output Parameters

Success or Failure

Description

Use this command to configure world-mode of this AP. Typically, AP is set to the default country-code (factory defaults). Check your installation guide to get more information about default country-code and other country codes. This information is useful for both 2.4 GHZ and 5 GHZ bands.

This command allows you to optionally set the environment parameter of whether this AP is deployed indoor or outdoor. This setting in conjunction with the country code determines the regulatory channel set and max transmit power. The channel set is used for scanning, DFS, and other enhanced radio features.

If multi-domain capability is enabled, then the supported channel-list is sent in the beacons and probe-responses along with the local and regulatory power constraints.

Defaults

None

Usage Guidelines

None

Examples

```
world-mode default-country environment indoor multi-domain enable
```

See Also

```
radio(show)> world-mode
radio(show)> radio-state
```

radio(show)> world-mode

Use this command to see the world-mode settings of this AP.

Syntax

```
world-mode
```

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to see the configured country code settings as well as the environment configuration of this AP.

Defaults

None

Usage Guidelines

None

Examples

```
radio(show)> world-mode

multi-domain     : enable
country code     : US
environment type : any
```

See Also

```
radio(config)> world-mode
radio(show)> radio-state
```

11 Security CLIs

This chapter includes information about the following security commands:

- security(config)> 802.1x
- security(show)> 802.1x
- security(config)> add-auth-server
- security(config)> add-auth-zone
- security(config)> admin-auth-zone
- security(show)> admin-auth-zone
- security(show)> auth-diag-statistics
- security(show)> auth-server-table
- security(config)> auth-server-timeout
- security(show)> auth-server-timeout
- security(show)> auth-statistics
- security(show)> auth-zone-table
- security(show)> certificate
- security(config)> change-local-admin-password
- security(config)> clear-statistics
- security(config)> commit-global-settings
- security(config)> default-wep-key-index
- security(config)> delete-auth-server
- security(config)> delete-auth-zone
- security(config)> delete-wep-keys
- security(show)> dot1x-supplicant-statistics
- security(config)> portal-auth-zone
- security(show)> portal-auth-zone
- security(config)> radius-group-attribute
- security(show)> radius-group-attribute
- security(config)> reset-to-defaults
- security(config)> security-modes
- security(show)> security-modes
- security(config)> wep-key
- security(show)> wep-keys
- security(config)> wep-key-length
- security(config)> wpa-modes
- security(show)> wpa-modes

security(config)> 802.1x

Use this command to set 802.1x session timeouts and group key rekey periods.

Syntax

```
802.1x [ session-timeout timeout ] [group-key-timeout group-rekey-period]
```

Input Parameters

session-timeout	The time in seconds that an 802.1x authenticated session can remain active before reauthentication is initiated.
group-key-timeout	The time in seconds that a 802.1x group key is valid. At the end of this period, a new key is generated and distributed to all associated stations.

Output Parameters

Success or Failure

Description

This command sets either the 802.1x session timeout or the rekey period for the group keys.

Defaults

None

Usage Guidelines

The 802.1x session timeout determines how long a wireless user can be associated without having to reauthenticate. Reauthentication is needed only to ensure that users that may be removed from a RADIUS server are dissassociated. A day (86400 seconds) is a typical setting for this policy.

The group key timeout determines how long a randomly generated group key is valid at the AP. The group key is randomly generated under WPA. It is also randomly generated under dynamic WEP, but not when a static WEP key has been manually entered. In that case the WEP key will be the group key forever. A typical setting for the group key timeout is one hour (3600 seconds).

Examples

```
802.1x session-timeout 28800
802.1x group-rekey-period 3600
```

See Also

```
security(show)> 802.1x
```

security(show)> 802.1x

Use this command to show the 802.1x configurable timeouts.

Syntax

```
802.1x
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the 802.1x session-timeout and the group-key-timeout.

Defaults

None

Usage Guidelines

None

Examples

```
session-timeout   : 28800
group-key-timeout : 3600
```

See Also

```
security(config)> 802.1x
```

security(config)> add-auth-server

Use this command to add a RADIUS authentication server and configure the IP address, port, and shared secret of the server.

Syntax

add-auth-server **auth-server** *hostname/ipaddress* **shared-secret** *sharedsecret* [*port portnumber*]

Input Parameters

auth-server	The IP address of the RADIUS server.
shared-secret	The RADIUS shared secret.
port	The optional port number for RADIUS authentication (default is 1812).

Output Parameters

Success or Failure

Description

This command configures information for a RADIUS server.

Defaults

The portnumber default value is 1812.

Usage Guidelines

RADIUS servers can be used to authenticate wireless users and administrators. Each RADIUS server must be configured by adding the server IP address and the associated shared secret for that server. The servers must then be added to an authentication zone to be used.

The typical port number for RADIUS authentication is 1812, but it can be changed if the RADIUS server is listening on a different port.

Examples

```
add-auth-server auth-server 1.2.3.4 shared-secret theSeceretPassword
```

See Also

```
security(show)> auth-server-table
security(config)> add-auth-zone
```

security(config)> add-auth-zone

Use this command to create a new authentication zone.

Syntax

```
add-auth-zone auth-zone auth-zone-name auth-servers hostname/ipaddress {...}
```

Input Parameters

auth-zone	The name to be used to identify the authentication zone.
auth-servers	A list of IP addresses identifying the RADIUS servers in the zone.

Output Parameters

Success or Failure

Description

This command creates a new authentication zone (an ordered list of RADIUS servers).

Defaults

None

Usage Guidelines

An authentication zone is used to define an ordered list of RADIUS servers. The RADIUS zones can be bound to an SSID to support wireless user authentication using WPA, or WEP with 802.1x. Also, a special admin auth zone can be identified that is used to provide single sign-on for administrative login on all managed APs.

The RADIUS servers are an ordered list that allows the use of redundant RADIUS servers. The servers are tried in the list order. If a RADIUS server in the zone does not respond, the next server in the list is tried. Servers must be configured (add-auth-server) before they can be used in a zone.

Examples

```
add-auth-zone auth-zone MsIasMachines auth-servers 1.2.3.4 1.2.3.5
```

See Also

```
security(config)> add-auth-server
security(show)> auth-zone-table
security(show)> auth-server-table
security(show)> admin-auth-zone
```

security(config)> admin-auth-zone

Use this command to define the authenticaion zone to be used to support administrative access to the AP.

Syntax

```
admin-auth-zone { portal-auth-zone |  auth-zone auth-zone-name }
```

Input Parameters

portal-auth-zone	Use the RADIUS server in the portal AP for administrative login authentication.
auth-zone	The name of the authentication zone to be designated as the administrative zone.

Output Parameters

Success or Failure

Description

This command defines which authenication zone will be used to authenticate administrative users.

Defaults

None

Usage Guidelines

Administrative access to the AP from the CLI or the web interface is authenticated using passwords. The passwords can be validated through a set of centrally managed RADIUS servers. This administrative authentication zone provides single sign-on for all APs configured to use the zone.

The RADIUS servers used for single sign-on can be either the built-in portal RADIUS servers or external RADIUS servers.

Examples

```
admin-auth-zone portal-auth-zone
admin-auth-zone auth-zone MsIasMachines
```

See Also

```
security(show)> admin-auth-zone
security(show)> auth-zone-table
```

security(show)> admin-auth-zone

Use this command to show which authentication zone is used to authenticate administrative users.

Syntax

```
admin-auth-zone
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the name of the authentication zone and the associated IP addresses of the RADIUS servers used to authenticate administrative users.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> admin-auth-zone

authzone     : Default (Portal Zone)
auth-servers : 192.168.168.24
```

See Also

```
security(config)> admin-auth-zone
security(show)> auth-server-table
security(show)> auth-zone-table
security(config)> add-auth-server
security(config)> add-auth-zone
```

security(show)> auth-diag-statistics

Use this command to display the statistics of events received from the authentication server.

Syntax

```
auth-diag-statistics
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command provides a summary of AP authenticator events received from the authentication server. These events are generated for any RADIUS based authentication and can include WPA (EAP based) or MAC-ACL authentication.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> auth-diag-statistics

BackendResponses         : 12
BackendAccessChallenges : 12
BackendAuthSuccesses    : 4
BackendAuthFails         : 23
```

See Also

```
security(show)> auth-statistics
security(show)> dot1x-supplicant-statistics
security(config)> clear-stastics
```

security(show)> auth-server-table

Use this command to all configured RADIUS authentication servers.

Syntax

```
Auth-server-table
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the IP address and port for each configured authentication server. RADIUS servers that are portal servers are indicated in the display table.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> auth-server-table

auth-server   : 192.168.168.24
is-portal     : 0
shared-secret : 9WT2YwzmgBL93Q_Ti3Xny5as8jBxBB
port          : 1812
```

See Also

```
security(config)> add-auth-server
security(config)> cportal-auth-zone
```

security(config)> auth-server-timeout

Use this command to set the authentication server timers.

Syntax

```
auth-server-timeout timeout timeoutvalue [ retries retrycount]
```

Input Parameters

timeout	The time in seconds (1 to 20) that the 802.1x networks authentication service waits before retrying.
retries	The number of retries (1 to 10) that the 802.1x network authentication service attempts before failing an authentication session.

Output Parameters

Success or Failure

Description

This command sets the timeout and retry count for the 802.1x network authentication server in the AP.

Defaults

None

Usage Guidelines

The timeout value and the retry attempts for the authentication server can be modified to match the network service. Typically these values should not be modified, however when the connectivity to the authentication server is slow, the time out and retry count can be increased to improve the system reliability.

Examples

```
auth-server-timeout timeout 4
auth-server-timeout timeout 4 retries 3
```

See Also

```
security(show)> auth-server-timeout
security(show)> auth-statistics
```

security(show)> auth-server-timeout

Use this command to set 802.1x session timeouts and group key rekey periods.

Syntax

```
auth-server-timeout
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the values for the timeout and retries configured for the network authention service on the AP.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> auth-server-timeout

timeout : 3
retries : 2
```

See Also

```
security(config)> auth-server-timeout
```

security(show)> auth-statistics

Use this command to display the statistics corresponding to messages sent between a station and the AP.

Syntax

```
auth-statistics
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays EAPOL statistics related to the messages between a station and the AP. These statistics are generated by the traffic from WPA or 8021.x based wireless authentication. Only radios in AP persona (not backhaul) will return these statistics.

Defaults

None

Usage Guidelines

None

Examples

```
auth-statstics
```

See Also

```
security(show)> auth-diag-statistics
security(show)> dot1x-supplicant-statistics
security(config)> clear-stastics security(show)>
```

security(show)> auth-zone-table

Use this command to display all the authentication zones and the RADIUS servers in each zone.

Syntax

```
auth-zone-table
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the name of every authentication zone and the IP addess of each RADIUS server in the zone.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> auth-zone-table

authzone     : DeerCreekCoAuth
auth-servers : 192.168.168.24
```

See Also

```
security(config)> add-auth-server
security(config)> add-auth-zone
security(show)> auth-server-table
```

security(show)> certificate

Use this command to show the details of the AP’s X.509 certificate.

Syntax

```
certificate
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the subject name, issuer name, and SHA-1 thumbprint associated with the AP’s certificate.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> certificate

cert : Subject Name  = "AP_00-0A-F5-00-01-F2"
Issuer Name   = "AP_00-0A-F5-00-01-F2"
Serial Number = 0
------------------------------------
X.509 Thumbprint   =
a6:58:8f:93:3c:49:1f:de:22:ae:02:73:4e:ed:cf:a6:86:26:f4:cf
SSH Fingerprint   = 9c:a2:05:df:5b:8c:f7:bc:61:5b:59:46:23:8e:0f:a5
```

See Also

```
security(show)>
```

security(config)> change-local-admin-password

Use this command to change the locally stored administrator password on an AP. This is also the SNMPv3 password on the AP.

Syntax

```
change-localadmin-password old-password old-password new-password new-
password confirm-password confirm-new-password
```

Input Parameters

old-password	The current administrator password.
new-password	The new password for the administrator.
confirm-password	The new password for the administrator, repeated to ensure that it is entered correctly.

Output Parameters

Success or Failure

Description

This command changes the local administrator password. This is also the SNMPv3 password on the AP.

Defaults

None

Usage Guidelines

Administrative access for the serial-port CLI, ssh-accessed CLI, and the web-based user interface all use the same single sign-on authentication. The administrative users credentials (user ID and password) are first checked in an AP local password storage. If this fails, the credentials are checked in the admin zone RADIUS servers if they have been configured.

The change-local-admin-password command only changes the local administrative password for the admin user id. This is also the SNMPv3 password on the AP.

Examples

```
change-local-admin-password old-password password new-password XcLn7Pwd
confirm-new-password XcLn7Pwd
```

See Also

```
security(show)> admin-auth-zone
```

security(config)> clear-statistics

Use this command to lear the security-related statistics.

Syntax

```
clear-statistics { all-statistics | auth-statistics | auth-diag-statistics |
dot1x-supplicant-statistics }
```

Input Parameters

all-statistics	Reset all security statistics.
auth-statistics	Reset the statistics that correspond to authentication messages sent between a station and the AP.
auth-diag-statistics	Reset the statistics for events received from a backend authentication server.
dot1x-supplicant-statistics	Reset the statistics that correspond to authentication messages sent between a local BP radio and the upstream AP.

Output Parameters

Success or Failure

Description

This command clears the security statistics to zero.

Defaults

None

Usage Guidelines

The security statistics can be very used to diagnose problems with the authentication process. They can also be used to examine supplicant (wireless user) access attempts.

The auth-statistics provide EAPOL statistics that correspond to authentication messages sent between a station and the AP. These statistics are generated by the traffic from WPA or 8021.x based wireless authentication. Only radios in AP persona (not backhaul) will return these statistics.

The auth-diag-stastics provide a summary of the AP authenticator events received from a backend authentication server. These events are generated for any RADIUS based authentication and can include WPA (EAP based) or MAC-ACL authentication.

The dot1x-supplicant-statistics are EAPOL statistics that correspond to authentication messages sent between a local BP radio and the upstream AP. Only radios in BP persona will return these statistics.

Examples

```
clear-statistics all-statistics
clear-statistics auth-statistics
clear-statistics auth-diag-statistics
clear-statistics dot1x-supplicant-statistics
```

See Also

```
security(show)> auth-statistics
security(show)> auth-diag-statistics
security(show)> dot1x-supplicant-statistics
```

security(config)> commit-global-settings

Use this command to commit previously set security settings.

Syntax

```
commit-global-settings
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to commit previously set security settings.

Defaults

None

Usage Guidelines

Changing security modes, the WEP keys or WPA preshared keys requires changing the state of the radio and will disassociate any stations associated to the AP. These changes are not made until the commit-global-settings is executed. After any security mode or shared key changes, the commit-global-settings must be executed for the changes to take effect.

Examples

```
wpa-modes auth-type eap-only
< other security mode changes >
commit-global-settings
```

See Also

```
ap-quick-start(show)> security-modes
```

security(config)> default-wep-key-index

Use this command to set the default WEP key index.

Syntax

```
default-wep-key-index key-index 1..4
```

Input Parameters

key-index	The key index to be used for all WEP protected transmit data.

Output Parameters

Success or Failure

Description

This command sets the default key index for WEP encryption. The default WEP key is the transmit key on the AP. It is also used for 802.11 shared-key authentication with WEP. If WEP has been enabled the default key index determines which key is used from all manually configured keys. Note that if no WEP keys are set, legacy 802.1x key distribution will be used to establish dynamic keys.

Defaults

None

Usage Guidelines

A key must be set for the index slected for WEP to function correctly. The commit-global settings command must also be given after setting the keys and default index.

Examples

```
default-wep-key-index key-index 1
```

See Also

```
security(config)> wep-keys
security(config)> security-modes
security(show)> security-modes
security(show)> wep-keys
```

security(config)> delete-auth-server

Use this command to remove the configuration of an authentication server.

Syntax

```
delete-auth-server all-auth-servers | auth-server hostname/ipaddress
```

Input Parameters

all-auth-servers	Delete all authentication server configurations.
auth-server	The IP address of the authentication server to delete.

Output Parameters

Success or Failure

Description

This command deletes the configuration of one or all RADIUS servers.

Defaults

None

Usage Guidelines

RADIUS servers can be deleted from the AP with the delete-auth-server command. To modify the password for a specific RADIUS server, you must first delete the existing configuration and then re-enter the RADIUS server with the new password. If you delete a RADIUS server, take care to delete its reference from the auth-zone it belongs to. Do not delete any RADIUS servers that are in your portal-auth-zone. If you do so, you may need to restore your configuration from backup or NMS, or re-enroll the AP.

Examples

```
delete-auth-server all-auth-servers

delete-auth-server auth-server 1.2.3.4
add-auth-server auth-server 1.2.3.4 shared-secret newSeceretPassword
```

See Also

```
security(config)> add-auth-server
security(show)> auth-server-table
security(show)> portal-auth-zone
ap-quick-start(show)> security-modes
```

security(config)> delete-auth-zone

Use this command to delete an authentication zone.

Syntax

```
delete-auth-zone { all-auth-zones |  auth-zone auth-zone-name }
```

Input Parameters

all-auth-zones	Delete all authentication zones.
auth-zone	The name of a specific authentication zone to delete.

Output Parameters

Success or Failure

Description

This command deletes one or all authentication zones. The authentication zones contain an ordered list of RADIUS servers that are identified by IP address.

Defaults

None

Usage Guidelines

The authentication zones contain RADIUS servers that have an identical set of enrolled users. Each zone can contain more than one server to support failover and load-balancing of the RADIUS servers. This command deletes a zone, but the configuration for the servers is still maintained in the authentication server table.

Examples

```
delete-auth-zone all-auth-zones
delete-auth-zone auth-zone xyz_corp_radius
```

See Also

```
security(show)> auth-zone-table
```

security(config)> delete-wep-keys

Use this command to delete all manually configured WEP keys.

Syntax

```
delete-wep-keys
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command deletes all WEP keys.

Defaults

None

Usage Guidelines

Manually configured WEP keys can be deleted to prevent and further associations using manually configured WEP encryption. Deleting all WEP keys does not mean that WEP is disabled. When WEP is enabled (even with no manual keys), the AP will use the authentication zone configured for the SSID to authenticate the user with legacy 802.1x and create dynamic keys if the user is correctly authenticated. WEP can be disabled by disabling the WEP mode (using security-modes).

Examples

```
delete-wep-keys
```

See Also

```
security(show)> wep-keys
security(config)> security-modes
ap-quick-start(show)> security-modes
```

security(show)> dot1x-supplicant-statistics

Use this command to display the statistics between a local BP radio and the upstream AP.

Syntax

```
dot1x-supplicant-statistics
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays statistics that correspond to EAPOL authentication messages sent between a local BP radio and the upstream AP. Only radios in BP persona will return these statistics.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> dot1x-supplicant-statistics

No entries found
```

See Also

```
security(show)> auth-statistics
security(show)> auth-diag-statistics
security(config)> clear-stastics
```

security(config)> portal-auth-zone

Use this command to select the security portals to be used in the portal authentication zone.

Syntax

```
portal-auth-zone auth-servers hostname/ipaddress {…}
```

Input Parameters

auth-servers	A list of IP addresses identifying the security portal to be used as the portal authentication zone.

Output Parameters

Success or Failure

Description

This command creates an ordered list of RADIUS servers to be used as the portal authentication zone. These servers should be the built-in RADIUS servers in security portals.

Defaults

None

Usage Guidelines

The selection of the security portals is typically automatically distributed as part of an NM-managed deployment of APs. This command allows the order of the RADIUS servers to be modified to better support load balancing between the servers. This is particularly useful for global deployments where the regional RADIUS server should be placed first on the list. This improves performace and system robustness by ensuring that the authention traffic stays within a local region.

Examples

```
portal-auth-zone auth-servers 1.2.3.7 2.3.4.5 5.6.7.8
```

See Also

```
security(show)> portal-auth-zone
```

security(show)> portal-auth-zone

Use this command to display the IP addresses of servers in the portal authentication zone.

Syntax

```
portal-auth-zone
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the IP address of all servers in the portal authentication zone.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> portal-auth-zone

auth-servers : 192.168.168.24
```

See Also

```
security(config)> portal-auth-zone
security(show)> auth-server-table
```

security(config)> radius-group-attribute

Use this command to select the RADIUS attribute used to determine service profiles.

Syntax

```
radius-group-attribute attribute-type type [ vendor-id oui sub-type sub-type ]
[ interpretation { string | integer } ]
```

Input Parameters

type	A number indicating the standard RADIUS attribute type. Use 26 to indicate vendor-specific.
interpretation	All RADIUS attributes must be defined as either a string or an integer
vendor-id	The vendor OUI to use for vendor-specific attributes.
sub-type	The vendor sub-type for vendor-specific attributes.

Output Parameters

Success or Failure

Description

This command allows the selection of the RADIUS attribute used to determine the service profile membership.

Defaults

type=26, oui=13586, sub-type=1, interpretation=string
These defaults are a registered VSA that should be used exclusively for group membership information.

Usage Guidelines

The AP can be configured to place users into different service profiles based on the group attribute returned from the RADIUS server. This advanced CLI allows the definition of the attribute to be changed. For example, this attribute could be changed to match an enterprise's existing VLAN attributes to create a more unified system deployment. Note that care should be taken to manage the definition of the group tags and associated profiles in a consistant manner throughout a deployment. The interpretation determines how the AP will treat the bytes the RADIUS server sends back. Strings sent from RADIUS do not have to be NULL terminated. Integers sent from RADIUS will be printed out like a string and for group matching purposes when the service-profile lookup is done.

Examples

```
(filter-id) radius-group-attribute attribute-type 11 interpretation integer
or                                                  (returning to default)
radius-group-attribute attribute-type 26 interpretation string vendor-id 13586
sub-type 1
```

See Also

```
security(show)> radius-group-attribute
```

security(show)> radius-group-attribute

Use this command to show the RADIUS group attribute configuration.

Syntax

```
radius-group-attribute
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the configuration of the RADIUS group attribute.

Defaults

None

Usage Guidelines

None

Examples

```
radius-group-attribute
```

See Also

```
security(config)> radius-group-attribute
```

security(config)> reset-to-defaults

Use this command to reset the security configuration.

Syntax

```
reset-to-defaults
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command resets all security configuration to the default values.

Defaults

None

Usage Guidelines

This command is useful to return the security configuration to a known default state.

Examples

```
reset-to-defaults
```

See Also

```
ap-quick-start(show)> security-modes
```

security(config)> security-modes

Use this command to set the allowed modes of security.

Syntax

```
security-modes { [ wpa { disable | enable } ] [ wep { disable | enable } ] [
open-access { disable | enable } ] }
```

Input Parameters

wpa	Enable or disable WPA based security.
wep	Enable or disable WEP based security.
open-access	Enable or disable open-access with no encryption.

Output Parameters

Success or Failure

Description

The security modes can be selected to allow WPA, WEP or open access. Combinations of WPA and WEP, or WPA and open are allowed.

Defaults

WPA enabled, WEP and open-access disabled.

Usage Guidelines

The WPA security modes provide very strong security using either EAP based authentication or authentication based on the distribution of preshared keys. The WPA mode is the recommended security mechanism, but older NIC cards may not support this standard. WPA may be configured with the wpa-modes command to select the authentication and prefered encryption algorithms.

WEP is widely available in NIC cards, but is not very secure. WEP can be enabled with WPA and, if desired, the less-secure WEP traffic can be segregated from the secure WPA traffic using VLANs determined by the service profiles.

Open access provides no authentication or security, but is useful for guest or open community access. The open access can be constrained to a specific VLAN using service profiles.

Note that you CANNOT enable WEP and open-access at the same time. Open access is allowed with WPA, but the service profiles must be configured to place WPA and open users into different VLANs.

To protect you from accidentally turning on multiple modes at the same time, turning on any one of them will disable the others that are unspecified in the command.

Examples

```
security-modes wpa enable
security-modes wpa disable wep enable open-access
```

See Also

```
security(show)> security-modes
security(config)> wpa-modes
ap-quick-start(show)> security-modes
```

security(show)> security-modes

Use this command to display the configuration of the security modes.

Syntax

```
security-modes
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays the configuration of the WPA, WEP, and Open Access security modes. Each of the modes may be in the enabled or disabled state.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> security-modes

wpa         : enable
wep         : enable
open-access : disable
```

See Also

```
security(config)> security-modes
ap-quick-start(show)> security-modes
```

security(config)> wep-key

Use this command to set a WEP key.

Syntax

```
wep-key key-index 1..4 { key value-in-hex }
```

Input Parameters

key-index	The index of the key to be set (1 to 4).
key	The value of the key in hex-ascii.

Output Parameters

Success or Failure

Description

This command sets a WEP key for a specific index. The keys are entered as hex-ascii values that much match the currently set wep key length.

Defaults

None

Usage Guidelines

The hex key values must be entered to use WEP with manually distributed keys. The keys must be 5 octets (10 hex-ascii characters) for 64 bit keys and 13 octets (26 hex-ascii characters) for 128 bit keys.

Examples

```
wep key-index 1 key F1DC345C4
<or for 128 bit keys>
wep key-index 1 key F529AE930A39A6C2AFE290BF25
```

See Also

```
security(show)> wep-keys
```

security(show)> wep-keys

Use this command to display information about the WEP keys.

Syntax

```
wep-keys
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command displays which WEP keys have keys, the default key index, and the configured size of the keys.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> wep-keys

key1        : **********
key2        : (null)
key3        : (null)
key4        : (null)
default-key : 1
key-length  : 64-bits
```

See Also

```
security(config)> wep-key
security(config)> wep-key-length
security(config)> default-wep-key-index
```

security(config)> wep-key-length

Use this command to set length of the WEP keys.

Syntax

```
wep-key-length { 64-bit | 128-bit }
```

Input Parameters

64-bit	Set the WEP key length to use 64 bit keys.
128-bit	Set the WEP key length to use 128 bit keys.

Output Parameters

Success or Failure

Description

This command sets the WEP key length to either 64 or 128 bit keys.

Defaults

None

Usage Guidelines

Each of the WEP keys can be individually set. All WEP keys need to be of the same size. If keys have been configured, they must be deleted before the key size can be changed. After changing the key size, the commit-global-settings must be used before the new key size takes effect.

Examples

```
wep-key-length 64-bit
```

See Also

```
security(show)> wep-keys
```

security(config)> wpa-modes

Use this command to set the authentication and encryption modes for WPA-based security.

Syntax

```
wpa-modes [auth-type {eap-only | psk-only | eap-and-psk}] [encryption-type
{aes-only | tkip-only | aes-and-tkip]
```

Input Parameters

auth-type	The types of WPA authentication supported for associations to the AP.
encryption-type	The encryption types allowed for WPA-based security.

Output Parameters

Success or Failure

Description

This command sets the allowable modes of authentication and encryption for WPA.

Defaults

None

Usage Guidelines

WPA authentication supports EAP, PSK, or both. The EAP authentication uses 802.1x to authenticate users using RADIUS servers. The preshared key (PSK) authentication uses manually distributed keys. Turning on both authentication modes simultaneously may prevent certain WPA clients from associating with the AP.

The encryption modes allow the selection of the AES or TKIP algorithms. AES is the strongest algorithm and provides financial grade security. Legacy equipment may require the use of the TKIP.

The WPA modes are enabled only if WPA is enabled by the security-modes command.

Examples

```
wpa-modes auth-type eap-only encryption-type aes-only
wpa-modes encryption-type tkip-only
```

See Also

```
security(config)> security-modes
security(show)> security-modes
security(show)> wpa-modes
ap-quick-start(show)> security-modes
```

security(show)> wpa-modes

Use this command to set display the configuration of the WPA modes.

Syntax

```
wpa-modes
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to display the configuration of the WPA authentication and encryption modes.

Defaults

None

Usage Guidelines

None

Examples

```
security(show)> wpa-modes

auth-type       : psk-only
encryption-type : aes-only
```

See Also

```
security(config)> wpa-modes
security(show)> security-mode
```

12 SNMP CLIs

This chapter includes information about the following SNMP commands:

- **snmp(config)> add-sink-host**
- **snmp(config)> delete-sink-host**
- **snmp(show)> snmp-agent**
- **snmp(config)> snmp-community**

snmp(config)> add-sink-host

Use this command to configure a list of SNMP trap destinations.

Syntax

```
add-sink-host sink-host hostname/ipaddress [ trap-community community ] [
trap-port port ]
```

Input Parameters

sink-host	Identifies the trap destination by hostname or IP address.
trap-community	The optional community to be used when sending the trap. If community is not specified, the string from a preceding trap-community directive will be used.
trap-port	The optional port to be used when sending the trap. If port is not specified, the well known SNMP trap port (162) will be used.

Output Parameters

Success or Failure

Description

This command is used to define the hosts to receive traps (and/or inform notifications). Traps that are raised with a syslog level set to LOG_CRIT will be sent out as INFORM notifications. Others will be sent as traps. A maximum of five (#5) trap destinations or sink hosts can be configured.

Defaults

None.

Usage Guidelines

Configuring various sink hosts will assist the configured host in receiving all the traps/informs that are raised by the AP. Traps/Informs will be sent to all the destinations in the same order as they are listed here.

Examples

```
add-sink-host sink-host 192.168.1.2
add-sink-host sink-host trapHost trap-community public
add-sink-host sink-host trapHost trap-community public trap-port 162
```

See Also

```
snmp(config)> delete-sink-host
snmp(config)> snmp-community
snmp(show)> snmp-agent
```

snmp(config)> delete-sink-host

Use this command to delete SNMP trap destinations from a configured set.

Syntax

```
delete-sink-host { all-sink-hosts | nms hostname/ipaddress }
```

Input Parameters

all-sink-hosts	Delete all the sink hosts that are configured.
nms	Identify the sink host by hostname or IP address and delete that entry only.

Output Parameters

Success or Failure

Description

This command is used to delete one or all of the hosts that are setup to receive traps/informs. The user can choose to delete all the configured sink hosts or delete one sink host at a time, by specifying the hostname or IP address of the host.

Defaults

None

Usage Guidelines

Specify all-sink-hosts to delete all the configured trap destinations. When deleting individual sink hosts, an entry should exist for that host in the list of configured trap destinations. If not, an error will be reported to the user.

Examples

```
delete-sink-host all-sink-hosts
delete-sink-host nms 192.168.1.2
delete-sink-host nms trapHost
```

See Also

```
snmp(config)> add-sink-host
snmp(config)> snmp-community
snmp(show)> snmp-agent
```

snmp(show)> snmp-agent

Use this command to view the SNMP related settings.

Syntax

```
snmp-agent
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to view the SNMP configuration(s) that have been set on the AP. This command will show the following:

- SNMP community strings that have been configured (both readonly and readwrite)
- List of sink hosts that have been configured (and its associated trap community and trap port, if any has been configured)

Defaults

None

Usage Guidelines

None

Examples

```
snmp(show)> snmp-agent

readwrite-community : public
```

See Also

```
snmp(config)> add-sink-host
snmp(config)> delete-sink-host
snmp(config)> snmp-community
```

snmp(config)> snmp-community

Use this command to configure the community to be used when communicating with a management entity.

Syntax

```
snmp-community { readonly communitystring }
```

Input Parameters

readonly	This defines the default community string to be used for an SNMP read-only operation.
readwrite	This defines the default community string to be used for an SNMP read-write operation.

Output Parameters

Success or Failure

Description

This command is used to define the SNMP community strings to be used when communicating with a management entity. The two types of community strings are:

- readonly – These community strings are used by a management entity to query read-only MIB objects on the agent.
- readwrite – These community strings are used by a management entity to query read-write MIB objects on the agent.

Defaults

None

Usage Guidelines

As the readonly and readwrite attributes indicate, this assists a management entity in communicating with the agent for any SNMP GET, GETNEXT, or SET request. The readwrite community strings are used for an SNMP SET requests and the readonly community strings can be used for any SNMP GET or GETNEXT request.

Examples

```
snmp-community readonly public
snmp-community readwrite private
snmp-community readonly readonly readwrite writealso
```

13 SSID CLIs

This chapter includes information about the following SSID commands:

- **ssid(config)> add-ssid**
- **ssid(config)> bind-service-profile**
- **ssid(config)> define-service-profile**
- **ssid(config)> delete-ssid**
- **ssid(config)> remove-service-profile**
- **ssid(config)> rename-ssid**
- **ssid(config)> reset-ssid-security**
- **ssid(config)> reset-to-defaults**
- **ssid (show)> security-table**
- **ssid (show)> service-profile-table**
- **ssid (show)> service-table**
- **ssid (show)> ssid**
- **ssid(config)> unbind-service-profile**
- **ssid(config)> update-ssid-security**

ssid(config)> add-ssid

Use this command to add an SSID.

Syntax

```
add-ssid { ssid ssid } [ max-stations max-stations-per-ssid ]
```

Input Parameters

ssid	SSID of AP radios that identifies the ESS.
max-stations	Maximum number of associations that can be associated with an SSID for the AP node.

Output Parameters

Success or Failure

Description

This command is used to add an SSID. The radios that operate in AP mode broadcast this SSID in the beacon. This command is also used to set the maximum number of stations that can be associated for this SSID on this AP. The default value for this maximum stations allowed is 512. Also when an SSID is added, a default service profile and security profile is associated with the SSID. SSID is a string with a maximum length of 32 characters. Not more than one SSID can be configured in the system. When the SSID is configured, all the radios operating in AP mode are reset and the new SSID configuration is applied. All stations associated with the AP radios will also be disassociated.

Defaults

Max-stations – 512

Usage Guidelines

Each AP has a unique factory default SSID configured. Using this command, this factory default SSID can be removed and a new SSID identifying the ESS can be configured. It is not recommended to use the factory default SSID for normal network operation.

Examples

```
add-ssid ssid TestNetwork max-stations 100
```

See Also

```
ssid(config)> delete-ssid
ssid(show)> ssid
```

ssid(config)> bind-service-profile

Use this command to bind a service profile to a SSID and user-group.

Syntax

```
bind-service-profile { ssid ssid } [ user-group user-group ] service-profile
profilename }
```

Input Parameters

ssid	Specifies the SSID.
user-group	Specifies the user group.
service-profile	Identifies the service profile.

Output Parameters

Success or Failure

Description

This command is used to bind a service profile to an SSID and user group. A user-configured service profile can be associated with an SSID without any user group (this is refered to as null user group). When an SSID is created by default, it is directly bound (null user group) with a factory default service profile. There are no factory default user groups except for the null user group. These user groups are identified via a group-tag.

The group-tag for the user is configured in the RADIUS server as part of the users profile. After successful association, the AP receives the group tag associated with the user from the RADIUS server and retrieves the service profile for this unique SSID and group combination. The appropriate service is enforced for the user based on the service profile attributes. If no group tag is received, then the service profile associated with the null group for the SSID is applied.

When a existing user group under an SSID is bound to a different service profile (that is, binding is modified) then all stations associated with the user group will be disassociated. On reassociation, the new service configuration is applied.

Defaults

None

Usage Guidelines

This command is used to create several user groups, each group bound with different service profiles. The attributes that define a service profile include a) which VLAN a user should be part of, b) class of service for the users traffic and c) encryption policy for the user.

One usage example would be for a company to create two user groups, one named employee and another named contractor. Each of these would be bound to different service profiles that have attributes matching the service requirements of these groups. In addition to configuring the service profiles and binding of user group tag to these service profiles on each AP, the group tag information should be associated with the user profile in the RADIUS server.

Examples

```
bind-service-profile ssid TestNetwork user-group employee service-profile
employee-profile
```

See Also

```
ssid(config)> unbind-service-profile
ssid(show)> service-table
```

ssid(config)> define-service-profile

Use this command to configure service profile and related attributes.

Syntax

```
define-service—profile service-profile profilename { [ security-enforcement {
default-enforcement | aes-only | tkip-or-aes | wep-only | no-encryption } ]  [
vlan-id vlan-id ] [ cos cosvalue ] [ description description ] }
```

Input Parameters

service-profile	Service profile identifier that is a string (up to a maximum of 32 characters).
security-enforcement	Identifies the type of security enforcement associated with this profile.
default-enforcement	Encryption mode/policy for AP is associated with this profile.
aes-only	AES is used as the encryption policy.
tkip-or-aes	TKIP or AES is used as encryption policy.
wep-only	WEP is used as encryption policy.
no-encryption	No encryption (open mode) is used.
vlan-id	Vlan associated with service profile.
cos	Cos associated with service profile.
description	Text description for service profile.

Output Parameters

Success or Failure

Description

This command is used to configure service profile and related attributes.

Security enforcement
This is used to identify the security enforcement policy for a profile. The options are: AES, TKIP or AES, WEP, Default enforcement, WEP and No encryption. It is important to note the following: when using AES or TKIP make sure the AP nodes security policy has WPA enabled. If WEP is selected make sure that the AP nodes encryption policy has WEP enabled (either WPA-WEP or legacy WEP). If no-encryption is selected traffic of stations that are associated with this profile will be transmitted in the clear.

Vlan-id
This is used to enforce user-based VLANs. The Vlan needs to be configured via the VLAN subsystem. For stations associated with this profile the VLAN policy is enforced. The VLAN can also be to default to interface VLAN (where VLAN id is set to 4095) for a service profile.

COS
This identifies the class of service associated with a service profile.

Output Parameters

Success or Failure

Defaults

Security Enforcement = default enforcement, Vlan ID = 4095, COS = 2

Usage Guidelines

Ensure that the security enforcement level associated with a profile is compatible with the AP node security modes configuration (configured using security > security-modes). The security level (that is, encryption level) is enforced after association of a station. The service profile associated with a user is determined based on the SSID and group tag (received from the RADIUS server after a successful authentication). The VLAN ID configuration can be used to enforce user based VLANs. The COS setting associated with a service profile is used to differentiate user traffic (all users associated with this service profile receive a certain quality of service).

When attributes of an existing service profile that has been bound to a SSID and group are modified, all stations associated with the service profile are disassociated. If they re-associate, the new service profile configuration will be applied.

Examples

```
define-service-profile service-profile employee-profile security-enforcement
default-enforcement vlan-id 2 cos 3 description “employee service level”
```

See Also

```
ssid(config)> remove-service-profile
ssid(show)> service-profile-table
```

ssid(config)> delete-ssid

Use this command to delete an SSID.

Syntax

```
delete-ssid { { all-ssids } | { ssid ssid } }
```

Input Parameters

all-ssids	Used to delete all SSIDs when multiple ssids have been configured.
ssid	SSID specified is deleted.

Output Parameters

Success or Failure

Description

This command is used to delete an SSID. In addition to deletion of the SSID, all configuration associated with the SSID such as user group, service profile association, and security profile for the SSID is deleted. When all SSIDs or the last user-configured SSID is deleted, the AP defaults to the factory default SSID. When this occurs, all the radios operating in AP mode are reset and the default SSID configuration is applied. All stations associated with the AP radios will also be disassociated.

Defaults

None

Usage Guidelines

Using this command to remove the user-configured SSID(s)..

Examples

```
delete-ssid ssid TestNetwork
```

See Also

```
ssid(config)> add-ssid
ssid(show)> ssid
```

ssid(config)> remove-service-profile

Use this command to remove a service profile or all service profiles.

Syntax

```
remove-service-profile { all-service-profiles | service-profile profilename }
```

Input Parameters

all-service-profiles	Used to delete all configured service profiles.
service-profile	Delete service profile identified by service profile name.

Output Parameters

Success or Failure

Description

This command is used to delete a specific service profile or all service profiles configured in the system. All service profiles in the system except the default service profile can be deleted. If a service profile is associated with an SSID and group, it cannot be deleted unless the binding is removed.

Defaults

None

Usage Guidelines

Using this command, the user-configured service profiles can be deleted.

Examples

```
reset-ssid-security ssid TestNetwork
```

See Also

```
ssid(config)> remove-service-profile
ssid(show)> service-profile-table
```

ssid(config)> rename-ssid

Use this command to add a SSID.

Syntax

```
rename-ssid old-ssid old-ssid-name new-ssid new-ssid-name
```

Input Parameters

old-ssid-name	Currently configured SSID.
new-ssid-name	New name for SSID.

Output Parameters

Success or Failure

Description

This command is used to rename an already configured SSID. All configuration related to the old SSID name, such as service profile associations and security configuration, is automatically transferred. The radios that operate in AP mode will broadcast this new SSID in the beacon. When this occurs, all the radios operating in AP mode are reset and the new SSID configuration is applied. All stations associated with the AP radios will also be disassociated.

Defaults

Max-stations – 512

Usage Guidelines

Used to rename existing SSID.

Examples

```
rename-ssid old-ssid TestNetwork new-ssid LabNetwork
```

See Also

```
ssid(config)> delete-ssid, ssid(config)> add-ssid
ssid(show)> ssid
```

ssid(config)> reset-ssid-security

Use this command to reset all security parameters related to an SSID.

Syntax

```
reset-ssid-security { { all-ssids } | { ssid ssid } }
```

Input Parameters

all-ssids	Used to reset security parameters for all SSIDs.
ssid	Reset security parameters for specific SSID.

Output Parameters

Success or Failure

Description

This command is used to reset security parameters for all SSIDs. When executed, all security parameters for that SSID are set to system defaults. All stations associated with the AP radios for this SSID will also be disassociated.

Defaults

None

Usage Guidelines

Using this command, the user-configured SSID(s) security parameters can be reset.

Examples

```
reset-ssid-security ssid TestNetwork
```

See Also

```
ssid(config)> update-ssid-security
ssid(show)> security-table
```

ssid(config)> reset-to-defaults

Use this command to reset the ssid configuration to factory defaults.

Syntax

```
reset-to-defaults
```

Input Parameters: None

Output Parameters: None

Success or Failure

Description

This command lets you reset all SSID configuration parameters to factory defaults.

Defaults

None

Usage Guidelines

This command is useful in resetting all SSID configuration.

Examples

```
reset-to-default
```

See Also

None

ssid (show)> security-table

Use this command to show configured security profile and parameters for the SSID.

Syntax

```
security-table [ssid ssid]
```

Input Parameters

ssid	Configured SSID.

Output Parameters

psk-key	Preshared key configured in hexadecimal characters.
psk-password	Preshared key configured as password.
mac-acl	Disables or enabled.
portal-auth-zone	Security portal is authentication zone for SSID domain.
auth-zone	Identifies authentication zone for SSID.

Description

This command is used to show the configured SSID security parameters.

Defaults

None

Usage Guidelines

Used to show security configuration.

See Also

```
ssid(config)> update-ssid-security
ssid(config)> reset-ssid-security
```

ssid (show)> service-profile-table

Use this command to show configured service profile and associated attributes.

Syntax

```
service-profile-table [ service-profile profilename ]
```

Input Parameters

service-profile	Identifies service profile.

Output Parameters

Security enforcement	The options can be AES, TKIP or AES, WEP, Default enforcement, WEP, and No encryption.
Vlan-id	Used to enforce user-based VLANs. The Vlan needs to be configured via the VLAN subsystem.
COS	Identifies the class of service associated with a service profile.

Description

This command is used to show the configured service profile and associated attributes.

Defaults

None

Usage Guidelines

Used to show service profile configuration. Without any parameters, all service profiles configured in the system are displayed.

Examples

```
ssid(show)> service-profile-table

profile     : Default
encryption  : no enforcement (default to node encryption)
vlanid      : default to interface vlan
cos         : not defined
description : Description
-------------------------------------------------------------------------

profile     : EmployeeProf
encryption  : no enforcement (default to node encryption)
vlanid      : 88
cos         : 5
description :
```

See Also

```
ssid(config)> define-service-profile
ssid(config)> undefine-service-profile
```

ssid (show)> service-table

Use this command to show configured service profile to SSID bindings.

Syntax

```
service-table [ ssid ssid ]
```

Input Parameters

ssid	Identifies SSID.

Output Parameters

user group	Identifies user group.
service-profile	Identifies service profile.
COS	This identifies the class of service associated with a service profile.

Description

This command is used to show the configured service profile to SSID/group bindings.

Defaults

None

Usage Guidelines

Used to show service profile to SSID/group bindings configuration. Without any parameters, service profile bindings to all SSIDs are displayed.

Examples

```
ssid(show)> service-table

ssid      : DeerCreekCo
usergroup :
profile   : Default
--------------------------------------------------------------------------

ssid      : DeerCreekCo
usergroup : employee
profile   : EmployeeProf
--------------------------------------------------------------------------

ssid      : DeerCreekGuest
usergroup :
profile   : Default
```

See Also

```
ssid(config)> bind-service-profile
ssid(config)> unbind-service-profile
```

ssid (show)> ssid

Use this command to show the configured SSID.

Syntax

```
ssid
```

Input Parameters: None

Output Parameters

SSID	Configured SSID or factory default SSID (if not configured).
Max number of stations	Maximum number of stations.

Description

This command is used to show the configured SSID and maximum number of stations that can be associated with the SSID. If no SSID has been configured by the user, then the factory default SSID is displayed.

Defaults

None

Usage Guidelines

show ssid

Examples

```
ssid(show)> ssid

ssid         : DeerCreekCo
max-stations : 512
---------------------------------------------------------------------------

ssid         : DeerCreekGuest
max-stations : 512
```

See Also

```
ssid(config)> add-ssid
ssid(config)> delete-ssid
```

ssid(config)> unbind-service-profile

Use this command to remove a binding between service profile and SSID/group.

Syntax

```
unbind-service-profile { { all-ssids }  | { ssid ssid } } [ user-group user-
group ]
```

Input Parameters

all-ssids	Used to delete all service profile bindings to all SSIDs.
ssid	Identifies SSID.
user-group	Identifies user group.

Output Parameters

Success or Failure

Description

This command is used to delete the binding between a service profile and SSID/group. All SSID service profile bindings can be removed with the all-ssids option. When a binding is removed, all currently associated users which belong to the group and SSID will be disassociated.

Defaults

None

Usage Guidelines

Using this command, the service profile to SSID bindings can be removed.

Examples

```
remove-service-profile ssid TestNetwork user-group contractor
```

See Also

```
ssid(config)> bind-service-profile
ssid(show)> service-table
```

ssid(config)> update-ssid-security

Use this command to configure security parameters and profile associated with the configured SSID.

Syntax

```
update-ssid-security { ssid ssid }  { [ psk-key value-in-hex | psk-password
passphrase ] [ mac-acl { disable | enable } ]  [ portal-auth-zone | auth-zone
auth-zone-name ] }
```

Input Parameters

ssid	SSID identifier.
psk-key	Preshared key configured in hexadecimal characters.
psk-password	Preshared key configured as password.
mac-acl	Disables or enables MAC address based access control.
portal-auth-zone	Security portal is authentication zone for SSID domain.
auth-zone	Identifies authentication zone for SSID.

Output Parameters

Success or Failure

Description

This command is used to configure security parameters associated with the configured SSID. These parameters can only be updated for a user-configured SSID. When any of the security configuration is changed using this CLI command, all client stations that associated with this AP using this SSID are disassociated.

psk-key/pask-password	When using WPA with a preshared key (PSK), the PSK can be set as a passphrase of 63 ASCII characters or less, or you may set a raw key of exactly 64 hex characters. If this parameter is not set (default), station association with WPA-PSK will fail for this SSID.
mac-acl	User can enable RADIUS based MAC address checking (MAC-ACL) for this SSID. This check will be done if the station is using one of the following modes of security that do not perform per-user authentication: open-access, static WEP, WPA-PSK.
portal-auth-zone	This parameter specifies that the security portal(s) in your network should be used as the RADIUS server(s) for this SSID. This is the default. The RADIUS servers are used for EAP authentication and any MAC-ACL lookups.
auth-zone	This parameter allows the user to specify a manually configured list of RADIUS servers for use with this SSID. The RADIUS servers are used for EAP authentication and any MAC-ACL lookups.

Output Parameters

Success or Failure

Defaults

Portal auth-zone is default.

Usage Guidelines

When AP level security mode is WPA and WPA authentication mode configured is PSK, then the user should configure either the PSK passphrase or PSK as a hexadecimal key.

Examples

```
update-ssid-security ssid TestNetwork auth-zone xanadu mac-acl enable psk-
password secretPskPassword

update-ssid-security ssid TestNetwork portal-auth-zone mac-acl disable psk-
password “secret psk pass phrase”
```

See Also

```
ssid(config)> reset-ssid-security
ssid(show)> security-table
```

14 System CLIs

This chapter includes information about the following system commands:

- system(config)> add-alarm-filter
- system(config)> add-license
- system(config)> admin-contact
- system(show)> alarm-record
- system(show)> alarm-filters
- system(show)> alarm-types
- system(show)> alarm-table
- system(show)> alarm-summary
- system(config)> ap-location
- system(show)> boot-log
- system(config)> buzzer
- system(show)> buzzer
- system(config)> cli-options
- system(show)> cli-options
- system(config)> config-backup
- system(config)> config-restore
- system(config)> date
- system(show)> default-config
- system(config)> delete-alarm-filter
- system(show)> dhcp-assigned
- system(show)> dhcp-assigned
- system(config)> dns
- system(config)> email
- system(config)> export-support-logs
- system(config)> hostname
- system(config)> mgmt-ipaddress
- system(config)> nms
- system(show)> nms
- system(config)> ntp-time-sync
- system(config)> reboot
- system(config)> reset-to-defaults
- system(config)> rtc
- system(show)> rtc
- system(show)> running-config
- system(config)> save
- system(show)> startup-config

- system(config)> sw-image-download
- system(config)> syslog-backup
- system(config)> syslog-level
- system(show)> syslog-level
- system(config)> syslog-remoteserver
- system(show)> syslog-remoteserver
- system(show)> sys-services
- system(show)> system-group
- system(config)> time
- system(config)> time-sync
- system(config)> time-zone
- system(show)> version

system(config)> add-alarm-filter

Use this command to configure alarm filters for this AP.

Syntax

```
add-alarm-filter { { start-alarm-id alarm-id end-alarm-id alarm-id } | {
alarm-list alarm-id {…} } }
```

Input Parameters

start-alarm-id	The starting alarm ID for a range of alarm IDs.
end-alarm-id	The last alarm ID for a range of alarm IDs.
alarm-list	A list of alarm IDs.

Output Parameters

Success or Failure

Description

This command is used to configure either a range of alarm IDs or a list of alarm IDs that the AP should ignore. The alarms represent important occurrences on the AP and they are identified by alarm ID(s). These alarms are translated into corresponding SNMP traps and are forwarded to a management system. An alarm filter may be defined using this command. If an alarm filter is defined, when the alarm occurs, it will be discarded and the trap corresponding to this alarm will not be generated.

Defaults

All alarms will be forwarded as traps to the management station.

Usage Guidelines

It is recommended to use the default configuration for the operation of the AP.

Examples

```
add-alarm-filter start-alarm-id 201 end-alarm-id 203
```

See Also

```
system(show)> alarm-types
```

system(config)> add-license

Use this command to add a new license key to the AP.

Syntax

```
add-license key license-key-string
```

Input Parameters

key	The new license key that should be added to the AP.

Output Parameters

Success or Failure	Command can fail if the license key is not intended for this AP.

Description

This command is used to add a new license key to the AP. Adding a new license key enables features on the AP. After a license has been added, the AP must be rebooted for the new license key settings to take effect. License keys cannot be removed. License keys are AP specific, so a given license key can be installed only on the AP for which it was generated. License keys, once installed, are retained across configuration changes and across image updates as well.

Defaults

The AP ships with a default license key that is vendor specific.

Usage Guidelines

add-license

Examples

```
add-license key AAB0DFADCFDFCAA1234
```

See Also

```
system(show)> version
```

system(config)> admin-contact

Use this command to denote the name of the administrator who is responsible for managing this AP.

Syntax

```
admin-contact **contact** *admin-contact-info*
```

Input Parameters

contact	Name of the person managing this AP.

Output Parameters

Success or Failure

Description

This command is used to make note of the name of the administrator who is managing this AP and can be contacted for service.

Defaults

None

Usage Guidelines

It is highly recommended to set the contact information of the administrator for a large deployment.

Examples

```
admin-contact contact “john smith”
```

See Also

```
system(show)> system-group
```

system(show)> alarm-record

Use this command to display the definition of the alarm ID.

Syntax

```
alarm-record { alarm-id id }
```

Input Parameters

alarm-id	The alarm ID to search for.

Output Parameters

Success or Failure

Description

Use this command to retrieve the definition of the alarm ID.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> alarm-record alarm-id 106

event-id      : 106
event-desc    : WDS established
sub-system    : WSM
filter-status : not-filtered
```

See Also

```
system(show)> alarm-types
```

system(show)> alarm-filters

Use this command to display the set of alarm filters configured on the AP.

Syntax

```
alarm-filters
```

Description

Use this command to display the set of alarm filters that have been configured on the AP.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> alarm-filters

events-filtered : 201
```

See Also

```
system(config)> add-alarm-filter
system(config)> delete-alarm-filter
```

system(show)> alarm-types

Use this command to display the set of alarm ID defined on the AP.

Syntax

```
alarm-types
```

Description

Use this command to display the set of alarm IDs defined on the AP. Then correlate the alarm ID with the alarm data to decide whether this alarm should be filtered out or not.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> alarm-types

event-id : 201
event-id : 401
event-id : 601
event-id : 801
event-id : 202
event-id : 602
event-id : 802
event-id : 203
event-id : 803
event-id : 204
event-id : 804
event-id : 205
event-id : 805
event-id : 206
event-id : 207
event-id : 208
event-id : 209
event-id : 210
event-id : 211
event-id : 212
event-id : 213
event-id : 214
event-id : 215
event-id : 216
event-id : 217
event-id : 218
event-id : 219
event-id : 220
event-id : 101
event-id : 221
event-id : 301
event-id : 501
event-id : 701
event-id : 102
event-id : 222
event-id : 302
```

```
event-id : 502
event-id : 702
event-id : 103
event-id : 223
event-id : 303
event-id : 503
event-id : 703
event-id : 104
event-id : 224
event-id : 304
event-id : 704
event-id : 105
event-id : 225
event-id : 305
event-id : 106
event-id : 226
event-id : 107
event-id : 227
event-id : 108
event-id : 228
event-id : 109
event-id : 229
event-id : 110
event-id : 230
event-id : 231
```

See Also

```
system(config) alarm-filters
```

system(show)> alarm-table

Use this command to filter out and display a selected set of fault notifications on the AP.

Syntax

```
alarm-table [ start-time start-time end-time end-time ] [ source-ip ip-address
] [ module-name name ] [ alarm-id alarmId ]
```

Input Parameters

Start-time	Specifies the start time for searching for the alarms.
End-time	Specifies the end time for searching for the alarms.
Source-ip	Specifies the IP address of the AP that logged the fault – to be searched.
Module-name	Specifies the module name to search for.
Alarm-id	Specifies the alarm ID to search for.

Output Parameters

The filtered fault list.

Description

Use this command to filter and display the set of faults that have been logged on the AP. Every fault message has the following parameters:

- Time at which it was logged.
- The address of the AP that logged the fault. On an NM portal the fault logs from all the enrolled APs are aggregated.
- The module name – the internal module name of the server that logged the alarm.
- The alarm ID – the alarm itself.

Using this command the fault log can be searched to select and display the fault as per the selected criteria. Only faults that pass ALL the filter criteria are returned.

Usage Guidelines

None

Examples

```
system(show)> alarm-table

event-id    : 106
log-level   : 2
log-time    : Sat Jan  1 01:00:22 2000
module      : WSM
source-ip   : AP_00-0A-F5-00-01-F2
description : WDS trunk established for DeviceId AP_00-0A-F5-00-01-F2 radio 4
remote mac 00:0a:f5:00:04:84 TrunkPort count 0 CauseCode 0
---------------------------------------------------------------------------

event-id    : 103
log-level   : 2
log-time    : Sat Jan  1 01:00:32 2000
module      : WSM
source-ip   : 192.168.168.14
```

```
description : Device Id AP_00-0A-F5-00-02-9A radio 4 disabled
--------------------------------------------------------------------------

event-id    : 102
log-level   : 2
log-time    : Sat Jan  1 01:00:34 2000
module      : WSM
source-ip   : 192.168.168.14
```

See Also

```
system(show)> alarm-summary
```

system(show)> alarm-summary

Use this command to display the summary of the fault statistics collected so far on this AP.

Syntax

```
alarm-summary
```

Description

Use this command to display a summary of the alarms that have been received on this AP.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> alarm-summary

server-start-time     : Sat Jan  1 00:00:19 2000
total-events-received : 94
total-events-dropped  : 0
major-event-count     : 0
critical-event-count  : 94
```

See Also

```
system(show)> alarm-table
```

system(config)> ap-location

Use this command to denote the location where this AP is installed.

Syntax

```
ap-location location location-of-ap
```

Input Parameters

location	Arbitrary string describing AP location.

Output Parameters

Success or Failure

Description

This command is used to make note of the AP location, which is helpful when troubleshooting problems. The network administrator may be able locate the errant equipment or identify other site specific issues.

Defaults

None

Usage Guidelines

It is highly recommended to set AP location information. Different companies may have existing protocols for setting location-id that may identify an AP by city, campus, building, floor, and region through a structured location codes. These location IDs identify the equipment so that it can be found easily and serviced.

Examples

```
ap-location location “sjc-bldg2-floor1-nw2-ceiling”
```

See Also

```
system(show)> system-group
```

system(show)> boot-log

Use this command to configure the time zone on the AP.

Syntax

```
boot-log
```

Description

This is a low-level troubleshooting command. Use this command to view the contents of the system boot log. The initial boot messages generated by the AP are displayed by this command. Note that the boot messages are stored in a circular buffer, so it is likely that after a long time the contents of the buffer would have been overwritten by other messages.

Defaults

None

Usage Guidelines

Use this command only when directed by a technical support personnel.

Examples

```
system(show)> boot-log

<4>mac_mod_exit: Cleaning MAC FW module: radio Id 1
<4>[0][18][2][568668] Received ProbeRsp with out of sequence IEs, type 48
lastType 50
```

See Also

```
system(show) > system-group
```

system(config)> buzzer

Use this command to enable or disable the operation of the buzzer on the AP.

Syntax

```
buzzer { disable | enable }
```

Input Parameters

Disable or Enable	Disabling the buzzer will prevent the buzzer from sounding.

Output Parameters

Success or Failure

Description

This command is used to enable or disable the operation of the buzzer.

Defaults

Buzzer is enabled by default.

Usage Guidelines

On selected models of the Airgo AP, the buzzer is a hardware option. If present on the AP, it may be enabled or disabled. When enabled, the buzzer will generate a 1 second beep when the corresponding show command is issued. When the APs are deployed, they may be hidden behind walls or ceilings. If the AP needs to be located for troubleshooting, then the buzzer can be used to locate the AP. Using the CLI or the web interface, the buzzer can be made to beep so that the AP can be located easily.

Examples

```
buzzer enable
```

See Also

```
system(show) buzzer
```

system(show)> buzzer

Use this command to verify the presence of the buzzer on the AP.

Syntax

```
buzzer
```

Description

The Airgo AP ships with a buzzer as a hardware option. When this command is executed, the system will display a status indicating the presence or absence of the buzzer. If a buzzer is present, then the buzzer will sound a 1 second beep.

Defaults

None

Usage Guidelines

The buzzer can be used to locate an AP that is mounted in a location that is not easily visible.

Examples

```
system(show)> buzzer

status : off
```

See Also

```
system(show) > system-group
```

system(config)> cli-options

Use this command to enable pagination or command confirmation in CLI.

Syntax

```
cli-options { [ cmd-confirm { disable | enable } ] [ pagination { disable |
enable } ] }
```

Input Parameters

cmd-confim – enable/ disable	Enabling command confirmation will force the command-line interface to confirm every delete operation with the user.
pagination	Enabling pagination will allow CLI to paginate output from all CLI commands.

Output Parameters

Success or Failure

Description

This command is used to enable or disable pagination or command confirmation. Command confirmation is used to make sure that various configurations on the AP do not get accidentally deleted or modified. If command confirmation is enabled and configurations in different subsystems are deleted, then the user is presented with the question: “Are you sure Y/N ?” If the user selects Y, then the configuration is deleted. This prevents accidental deletions. The pagination option is very useful when the CLI is being accessed via a serial console where the serial console does not have facility to buffer or show large quantities of output. Enabling pagination allows the CLI to display only 24 lines of output and then present the More prompt to the user. When the user enters any key at this prompt, the next 24 lines of output are shown. This continues until all the output from the command is displayed, then the normal CLI command prompt is displayed.

Defaults

Both command confirmation is and pagination are enabled by default.

Usage Guidelines

If the CLI is being accessed via a script, then it may be useful to turn the command confirmation and pagination off. The recommeded behavior is to use the default settings.

Examples

```
cli-options cmd-confirm enable pagination disable
```

See Also

```
system(show) cli-options
```

system(show)> cli-options

Use this command to show the pagination and command confirmation status on the AP.

Syntax

```
cli-options
```

Description

Use this command to display whether command confirmation and pagination are enabled or not.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> cli-options

cmd-confirm : Enabled
pagination  : Disabled
```

See Also

```
system(show) > system-group
```

system(config)> config-backup

Use this command to backup the startup configuration of the access point.

Syntax

```
config-backup tftp-server hostname/ipaddress [ to-file pathname-on-tftp-
server ]
```

Input Parameters

hostname / ipaddress	The address of the tftp server.
Pathname-on-tftp-server	The complete path name of the of the target file.

Output Parameters

Success or Failure

Description

This command is used to backup the startup configuration of the access point to a known location on a TFTP server. If the *to-file* is not specified, then the startup configuration is stored on the default TFTP directory on the TFTP server with the name apconfig.xml. If the *to-file* is specified, then the configuration is backed up to the TFTP server under the specified name. The configuration file is a tagged-formatted ASCII file. This configuration file may be restored back on the AP using the config-restore command.

Defaults

Usage Guidelines

It is recommended that the configuration of the AP or portals be backed up on a regular basis. In addition as the configuration file contain detailed information about the AP, the configuration file must be kept in a secure place. Also note that the configuration file is not secured in any way and the TFTP protocol does not provide any security as well.

Examples

```
config-backup tftp-server 10.0.0.3
```

See Also

```
system(config) > config-restore
```

system(config)> config-restore

Use this command to restore the backed up configuration of the AP.

Syntax

```
config-resptore tftp-server hostname/ipaddress [ from-file pathname-on-tftp-
server ] [ reboot ]
```

Input Parameters

hostname / ipaddress	The address of the TFTP server.
pathname-on-tftp-server	The complete path name of the file.
reboot	Option to reboot the AP when the configuration is downloaded.

Output Parameters

Success or Failure

Description

This command is used to restore the configuration of access point from a configuration file that was backed up using the config-backup command. The hostname/ipaddress identifies the TFTP server and the pathname-on-tftp-server the name of the configuration file that was backed up. If the configuration file name is not specified, then this command will download the apconfig.xml file from the root TFTP directory on the tftp server. Specifying the reboot option causes the AP to reboot after the configuration is downloaded to the AP.

Defaults

Usage Guidelines

Configuration that was backed up from one AP cannot be restored on another AP as the configurations contain AP specific information and so cannot be interchanged. When the configuration of the AP is changed, it is highly recommended that the AP be rebooted.

Examples

```
config-restore tftp-server 10.0.0.3 reboot
```

See Also

```
system(config) > config-backup
```

system(config)> date

Use this command to set the hostname of an Airgo AP.

Syntax

```
date **mm-dd-yyyy** *mm-dd-yyyy*
```

Description

This command is used to set up the date on the AP.

Defaults

None

Usage Guidelines

The date and time on the Airgo AP can be configured in two ways, either manually using this command or by using the Network Time Protocol (NTP) service. If the AP does not have connectivity to the internet or if there are no internal NTP servers, then use this command to manually configure the date on the AP.

Examples

```
date mm-dd-yyyy 11-14-2003
```

See Also

```
system(show)> system-group
```

system(show)> default-config

Use this command to show the contents of the default configuration on the AP.

Syntax

```
default-config
```

Description

Use this command to display the contents of the default configuration on the AP. Airgo APs can be configured with an OEM-specific configuration file. This OEM configuration will be independent of the configuration that a user may establish on the AP. The OEM configuration will be made to persist on the AP even after the reset-to-defaults factory-defaults command has been executed. This command will display the contents of the OEM configuration.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> default-config

No "default" configuration data available
```

See Also

```
system(show)> startup-config
system(show)> running-config
```

system(config)> delete-alarm-filter

Use this command to delete configured alarm filters for this AP.

Syntax

```
delete-alarm-filter { { all-alarm-filters } | { start-alarm-id alarm-id end-alarm-id alarm-id } }
```

Input Parameters

all-alarm-filters	Deletes all configured alarm filters.
start-alarm-id	The starting alarm ID for a range of alarm IDs.
end-alarm-id	The last alarm ID for a range of alarm IDs.

Output Parameters

Success or Failure

Description

This command is used to delete alarm filters configured on the AP. If the all-alarm-filters keyword is used, then all the alarm filters are deleted. Or a range of filter IDs may be specified to delete that range. After the alarm filters have been deleted, the corresponding events will again be forwarded as traps to the sink-host if configured.

Defaults

None

Usage Guidelines

Examples

```
delete-alarm-filter start-alarm-id 201 end-alarm-id 203
```

See Also

```
system(show)> alarm-types
```

system(show)> dhcp-assigned

Use this command to check the status of the various DHCP assigned parameters on the AP.

Syntax

```
dhcp-assigned
```

Description

Use this command to display whether the IP address, DNS address, WINS address, and NTP address is DHCP assigned or is manually configured.

The IP address, DNS address, WINS address, and NTP server address may be obtained from the DHCP server or may be manually configured. This command shows how each of them have been configured.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> dhcp-assigned

is_ip_dhcp_assigned   : yes
is_dns_dhcp_assigned  : yes
is_wins_dhcp_assigned : no
is_ntp_dhcp_assigned  : yes
```

See Also

system(show)> dhcp-assigned

Use this command to show if certain attributes are set via a DHCP servers.

Syntax

```
dhcp-assigned
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to display if certain attributes, such as IP address, DNS address, WINS address, and NTP server address are set via an external DHCP server on this AP.

Defaults

None

Usage Guidelines

This command let you identify if certain IP addresses are set manually on this AP or are assigned via an external DHCP server, which can help troubleshoot a specific configuration problem.

Examples

```
dhcp-assigned
system(show)> dhcp-assigned
is_ip_dhcp_assigned   : yes
is_dns_dhcp_assigned  : yes
is_wins_dhcp_assigned : no
is_ntp_dhcp_assigned  : yes
```

See Also

```
system(show)> system-group
```

system(config)> dns

Use this command to configure the set of DNS servers this AP can contact for name resolution.

Syntax

```
dns { { delete-all-dns-servers } | { dns-servers ipaddress {…} } }
```

Input Parameters

delete-all-dns-servers	Specifying this value will delete all configured DNS servers.
dns-servers	Specify a list of DNS servers to be configured.

Output Parameters

Success or Failure

Description

This command is used to configure the set of DNS servers that this AP can contact. If more than one DNS server needs to be configured, then they need to be specified as a set of servers within double quotes. Using the keyword *delete-all-dns-servers* will delete all configured DNS servers.

Defaults

None

Usage Guidelines

DNS server addreses within an AP may be configured either manually using this command or by being obtained from a DHCP server – by configuring the server to return the correct DNS server address. Note: The DNS server address must be carefully configured, if misconfigured it will cause services on the AP to attempt to contact a non-existent DNS server and may cause the address lookup within the AP to slow down. It is recommended that the DNS server address be configured within a DHCP server so that all APs in the network get configured uniformly and reduce the chance of misconfiguration.

Examples

```
dns dns-servers “10.0.0.1 100.100.100.1”
```

See Also

```
system(show)> system-group
```

system(config)> email

Use this command to configure the email settings for NM portal.

Syntax

```
email smtp-server mail-server notify-email notify-email-address
```

Input Parameters

smtp-server	The address of a Simple Mail Transfer Protocol (SMTP) server that can provides email services.
notify-email	The email address of the administrator.

Output Parameters

Success or Failure

Description

This command is used to configure the email settings on the NM portal. The smtp-server address identifies the SMTP server within the network that can provide mail distribution services. The notify-email address is the address to which fault email notifications are sent to. These configurations are used for the following:

- When configured and email notification is enabled then as faults are detected on the NM portal an email notification is sent to the notify-email address.
- When wireless users are added on the NM portal, the SMTP server is used to mail the certificate for the user through that server.

Defaults

The AP ships with no SMTP server or notify email address configured.

Usage Guidelines

If an SMTP server is not configured, the AP will function normally but attempts to send email will fail.

Examples

```
email smtp-server email-server.abc.com notify-email jsmith@abc.com
```

See Also

```
system(show)> system-group
```

system(config)> export-support-logs

Use this command to export support logs on the AP to a TFTP server.

Syntax

```
export-support-logs tftp-server hostname/ipaddress [ to-file pathname-on-
tftp-server ]
```

Input Parameters

hostname/ipaddress	TFTP servers hostname or IP address.
pathname-on-tftp-server	An optional filename or path-and-filename, relative from the TFTP root directory, on the server to store system logs. If the from-file parameter is not specified, the default image filename is supportLogs.tar.gz.

Output Parameters

Success or Failure

Description

This command is used to export support logs to a TFTP server. Support logs combine vital diagnostic information, such as version of the hardware, software, and debug logs, which helps technical support organization in troubleshooting a persistent problem that can not be resolved easily.

Defaults

If the to-file parameter is not specified, the default support-log filename is supportLogs.tar.gz.

Usage Guidelines

The entire log directory is tar-ed and gzip-ed into a file and uploaded to the TFTP server. Use this command when directed by a technical support personnel. Support logs need to be sent to technical support organization for further analysis.

Examples

```
system(config)> export-support-logs tftp-server 10.0.0.77

system(config)> export-support-logs tftp-server 10.0.0.77 to-file
supportlogs.tar.gz
```

See Also

None

system(config)> hostname

Use this command to set the hostname of an Airgo AP.

Syntax

```
hostname **name** *hostname*
```

Description

This command is used to set up the host name of an Airgo AP.

Defaults

None

Usage Guidelines

Set the AP hostname with a unique string to help distinguish one AP from another.

Examples

```
hostname host “airgo-ap2000-sjc”
```

See Also

```
system(show)> system-group
```

system(config)> mgmt-ipaddress

Use this command to set the management IP address of an Airgo AP.

Syntax

mgmt-ipaddress { **dhcp-assigned** | **ipaddress** *ipaddress/numsubnetmaskbits* [**gateway** *ipaddress*] }

Input Parameters

dhcp-assigned	IP address assigned by an external DHCP server.
ipaddress	Static IP address in IP prefix format.
gateway	Default gateway IP address.

Output Parameters

Success or Failure

Description

This command is used to set up the management IP address of an Airgo AP.

Defaults

None

Usage Guidelines

Set the management IP address of the AP with a unique string to help distinguish one AP from another.

Examples

```
mgmt-ipaddress dhcp-assignedz
mgmt-ipaddress ipaddress 10.1.1.25/15 gateway 10.1.1.200
```

See Also

system(show)> system-group

system(config)> nms

Use this command to configure the network manager address for this AP.

Syntax

```
nms primary hostname/ipaddress [ auxiliary hostname/ipaddress ]
```

Input Parameters

primary	The address of the primary NMS server.
auxiliary	The address of the auxiliary NMS server.

Output Parameters

Success or Failure

Description

Airgo APs are designed to be managed by two network managers:

- NMPortal – The NM portal is identified by the *auxiliary* address. Normally this address never need be configured manually because this address is configured automatically when the AP is enrolled from the NM portal.
- An external NMS – The NMS is identified by the *primary* address. Normally this address never need be configured, manually because this address is configured automatically when the AP is enrolled from Airgo NMS-Pro system. But in case the external NMS is a third party NMS such as HP-Openview, then use this command to manually configure this address.

  This address identifies the network manager that is authorized to receive notification from this AP.

Defaults

These addresses are configured automatically when the AP is enrolled.

Usage Guidelines

For security reasons, the correct IP address must be used if manually configured, otherwise, fault notifications will be forwarded to the wrong NMS server.

Examples

```
nms primary 192.168.2.100 auxiliary 192.168.1.100
```

See Also

```
systemt(config)> nms
```

system(show)> nms

Use this command to display the network mangers authorized to manage this AP.

Syntax

```
nms
```

Description

Use this command to display the set of network managers authorized to manage this AP.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> nms

Primary Manager IP      : 0.0.0.0
Auxiliary Manager IP    : 192.168.168.24
```

See Also

system(config)> ntp-time-sync

Use this command to enable or disable time syncrhonization via an NTP server.

Syntax

```
ntp-time-sync { disable | enable }
```

Input Parameters

disable / enable	Enable or disable time synchronization.

Output Parameters

Success or Failure

Description

This command enables or disable time synchronization with a time server. If the AP has connectivity to the internet or if a corporate NTP server is available, then NTP time synchronization should be enabled so that the AP gets it time from an established reference time source.

One or more NTP servers must be configured either via an external DHCP server (if the AP's IP address is DHCP-Assigned) or explicitly configured using the time-sync command.

Defaults

Time synchronization is disabled by default.

Examples

```
ntp-time-sync enable
```

See Also

```
system(config)> system-group
system(config)> time-sync
system(show)> time
```

system(config)> reboot

Use this command to reboot the AP.

Syntax

```
reboot [ force ]
```

Input Parameters

force	When specified, will force reboot the AP without any questions.

Output Parameters

Success or Failure

Description

Use this command to reboot the AP. If configuration changes have been made on this AP, the command prints a message on the screen and will not reboot the AP. Use the save command to save the configuration on the AP then reboot the AP. To force the reboot and ignore the configuration changes, use the force option.

Defaults

None

Examples

```
reboot force
```

See Also

```
system(config)> save
```

system(config)> reset-to-defaults

Use this command to reset the configuration of the AP to a known state.

Syntax

```
reset-to-defaults [ { system-config | all-config | factory-defaults } ]
```

Input Parameters

system-config	Reset the configuration parameters of the system-group to factory default.
all-config	Reset the configuration parameters of the ALL subsystems to factory default.
factory-defaults	Reset the configuration parameters and ALL databases on the AP to factory default.

Output Parameters

Success or Failure

Description

An AP contains different classes of configuration. Using this command each of the configuration settings may be reset. When in the system group, specifying the *system-config* will reset the system-group configuration, such as NTP servers and DNS servers.

When all-config is specified, the entire startup configuration of the AP, that is, the configuration of most of the subsystems such as backhaul, bridging, radio, etc. is reset to the factory defaults. Note that all-config option does not reset security and some of the system configuration to preserve the manageability of the AP after this reset. Thus, attributes like mgmt-ip, hostname, security-modes, and AP enrollment security credentials are preserved when you select this option. All these information can be reset by choosing factory-defaults option.

When factory-defaults is specified, the startup configuration of the AP and all the databases – including the policy databases, security databases, user databases, and certificate databases will be reset.

Exercise extreme caution when attempting to reset the AP to factory defaults. If an NM portal is reset to factory defaults, the entire network of enrolled APs will have to be rest to defaults and be re-enrolled.

Defaults

The system-group configuration is reset to defaults.

Examples

```
reset-to-defaults all-config
```

See Also

```
system(config)> save
```

system(config)> rtc

Use this command to enable or disable the user of real time clock.

Syntax

```
rtc { disable | enable }
```

Input Parameters

enable/disable	Enable or disable the use of real time clock on the AP.

Output Parameters

Success or Failure

Description

Airgo APs have a real time clock installed in them as an optional component. When installed, the real time clock may be used to keep track of time. If the AP has no real time clock, then every time the AP is rebooted it will lose its current time settings.

Defaults

If RTC is available on the AP the RTC should be used to track time.

Examples

```
Rtc enable
```

See Also

```
system(show)> rtc
system(show)> time
system(config) > time-sync
```

system(show)> rtc

Use this command to display the presence or absence of a real time clock (RTC).

Syntax

```
rtc
```

Description

The teal time clock is a hardware option on the AP. Use this command to find out whether the RTC is present or not.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> rtc

RTC hardware available
```

See Also

system(show)> running-config

Use this command to display the set of configurations that have been applied to the AP.

Syntax

```
running-config
```

Description

Use this command to display the set of configurations that have been successfully applied to the AP and the configuration under which the AP is currently operating. This command will the display the configuration settings of the entire AP.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> running-config

Command : config backhaul uplink-criteria
interface      : wlan0
ssid           : DeerCreekCo
ipnetaddr      : 0.0.0.0/0
path-selection : lowest-weighted-cost
interface      : wlan1
ssid           : DeerCreekCo
ipnetaddr      : 0.0.0.0/0
path-selection : lowest-weighted-cost
--------------------------------------------------------------------------

Command : config radio network-density
network-density : low

Command : config radio channel
interface       : wlan0
periodic period : 30

Command : config radio channel-set
```

See Also

```
system(show) startup-config
```

system(config)> save

Use this command to save the configuration of the AP persistently.

Syntax

```
save
```

Input Parameters

None

Output Parameters

Success or Failure

Description

Use this command to save any configuration changes that might have been made to the AP so that the configuration may be restored when the AP is rebooted. After the configuration is saved, then when the AP is rebooted, the configuration is automatically restored.

The *save* command is available every configuration group in the CLI, this fast path option enables the configuration to be saved from every subsystem. When the save command is issued the configuration of the entire AP is saved. It is not possible to save individual subsystem configurations.

Defaults

None

Usage Guidelines

Examples

```
save
```

See Also

```
system(show) > running-config
```

system(show)> startup-config

Use this command to display the configuration settings that have been applied to the AP.

Syntax

```
startup-config
```

Description

This command displays the contents of the startup configuration stored on the AP. The startup configuration is the configuration that will get applied to the AP when it is booted up.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> startup-config

Command : config backhaul uplink-criteria
interface      : wlan0
ssid           : DeerCreekCo
ipnetaddr      : 0.0.0.0/0
path-selection : lowest-weighted-cost

Command : config backhaul uplink-criteria
interface      : wlan1
ssid           : DeerCreekCo
ipnetaddr      : 0.0.0.0/0
path-selection : lowest-weighted-cost
--------------------------------------------------------------------------

Command : config radio network-density
network-density : low

Command : config radio channel
interface       : wlan0
periodic period : 30

Command : config radio channel-set
interface       : wlan0
scanned-band    : any

Command : config radio channel
interface       : wlan1
```

See Also

```
system(show)startup-config
```

system(config)> sw-image-download

Use this command to download and apply a new software release image to the AP via a TFTP server.

Syntax

```
sw-image-download tftp-server hostname/ipaddress [ from-file pathname-on-
tftp-server ]
```

Input Parameters

hostname/ipaddress	TFTP servers hostname or IP address.
pathname-on-tftp-server	The optional filename or path-and-filename (relative from the TFTP root directory) of the image filename. If the from-file parameter is not specified, the default image filename is target.ppc.ani.img.

Output Parameters

Success or Failure

Description

This command is used to download a new software release image to the AP. Before the image is downloaded to the AP, a number of NM services will be disabled to conserve RAM for the image. When the download is complete, the new image will be verified for compatibility and validity before it is applied to AP. The AP must be rebooted for the image to take effect. Note that to use domain name for TFTP server, DNS should be configure on this AP.

Defaults

If the from-file parameter is not specified, the default image filename is target.ppc.ani.img.

Usage Guidelines

Use this command to download a new software release image to the AP via a TFTP server.

Examples

```
system(config)> sw-image-download tftp-server 10.0.0.77
TFTP software upgrade completed successfully.  Please reboot.
```

See Also

None

system(config)> syslog-backup

Use this command to backup system logs on the AP to a TFTP server.

Syntax

```
syslog-backup tftp-server hostname/ipaddress [ to-file pathname-on-tftp-
server ]
```

Input Parameters

hostname/ipaddress	TFTP servers hostname or IP address.
pathname-on-tftp-server	An optional filename or path-and-filename, relative from the TFTP’s root directory, on the server to store system logs. If the from-file parameter is not specified, the default image filename is syslog.tar.gz.

Output Parameters

Success or Failure

Description

The syslog service on the Airgo AP captures detailed information about the operation of the system. These logs are very useful in troubleshooting the system. Use this command to make a backup of the log files to a known location on a TFTP server. This command is used to backup the APs system logs onto a TFTP server. Note that to use domain name for TFTP server, DNS should be configure on this AP.

Defaults

If the to-file parameter is not specified, the default backup-log filename is syslog.tar.gz.

Usage Guidelines

The entire log directory is tar-ed and gzip-ed into a file and uploaded to the TFTP server.

Examples

```
system(config)> syslog-backup tftp-server tftp.abc.com
system(config)> syslog-backup tftp-server tftp.abc.com to-file aplogs.tar.gz
```

See Also

```
system(config) > export-support-logs
```

system(config)> syslog-level

Use this command to configure the logging level for troubleshooting the system.

Syntax

```
syslog-level level { emergency | alert | critical | error | warning | notice |
info | debug } [ module { all-modules | snmp | webui | cli | dhcp | networking
| security | radio | guest-access | discovery | fault | performance |
enrollment | sw-download | policy | dds | cm } ]
```

Input Parameters

level	The logging level – emergency is the least detailed logging level and debug is the most verbose logging level.
module	This refers to the different subsystem on the AP, whose logging level may be configured.

Output Parameters

Success or Failure

Description

This is a diagnostics / troubleshooting support command and must be used with care. The syslog service on the Airgo AP captures detailed information about the operation of the system. These logs are very useful in troubleshooting the system. Use this command to make a backup of the log files to a known location on a TFTP server.

Defaults

If no *to-file* is specified, then the syslogs are TARed and backed up to the TFTP server as syslog.tar.gz.

Usage Guidelines

Examples

```
syslog-backup tftp-server 10.0.0.100
```

See Also

```
system(config) > export-support-logs
```

system(show)> syslog-level

Use this command to display the syslog level that each service is operating with on the AP.

Syntax

```
syslog-level
```

Description

The syslog level can be changed to display more or less logging output.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> syslog-level

--------------------------------------------------------------------------
Module                    Level
--------------------------------------------------------------------------

networking                notice
security                  notice
radio                     notice
discovery                 notice
fault                     notice
enrollment                notice
sw-download               notice
dds                       notice
cm                        notice|
```

See Also

```
system(config)> syslog-level
```

system(config)> syslog-remoteserver

Use this command to configure the logging level for troubleshooting the system.

Syntax

```
syslog-remoteserver { { disable } | { enable  host hostname/ipaddress } }
```

Input Parameters

disable	If specified, remote logging is disabled.
enable	When specified, remote syslog support is turned on.
host	The hostname or IP address of the remote syslog server – to which syslog message will be forwarded.
port	The port that the remote syslog server is listening to.

Output Parameters

Success or Failure

Description

Use this command for troubleshooting the AP. When a lot of logging is being generated and it needs to be viewed outside of the AP, use this command to enable forwarding of the logging information to the remote server.

For this command to work, a syslog server that listens on the specified *port* must have been configured. Also make sure that the syslog server is configured to receive messages from remote entities. Normally syslog servers are set up to receive messages only from the local system.

Defaults

If no *to-file* is specified, then the syslogs are TARed and backed up to the TFTP server as syslog.tar.gz.

Usage Guidelines

For both performance and security reaons, turn off the logging level and remote logging after troubleshooting sessions are completed.

Examples

```
syslog-remoteserver enable mylogserver.abc.com
```

See Also

```
system(show) > syslog-remoteserver
```

system(show)> syslog-remoteserver

Use this command to display whether remote syslogging is enabled or not.

Syntax

```
syslog-remoteserver
```

Description

Remote syslogging can be enabled to forward syslogs to a remote server.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> syslog-remoteserver

admin-state : disable
```

See Also

```
system(config)> syslog-remoteserver
```

system(show)> sys-services

Use this command to display the set of system servers that have been started on the AP.

Syntax

```
sys-services
```

Description

Use this command to display the set of system servers that have been started on the AP.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> sys-services

dns-server    : enable
ntp           : disable
syslog-server : disable
```

See Also

system(show)> system-group

Use this command to display configuration of the system group of parameters.

Syntax

```
system-group
```

Input Parameters

None

Output Parameters

Success or Failure

Description

This command is used to show system configuration parameters.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> system-group

mgmt-ipaddress : 192.168.168.24/24
gateway        : 192.168.168.254
clock          : Sat Jan  1 01:51:24 2000
hostname       : AP_00-0A-F5-00-01-F2
time-sync-type : manual
smtp-server    : 191.168.168.1
notify-email   : admin@deercreekco.com
dns-servers    : 192.168.168.1
contact        : admin@deercreekco.com
timezone       : pst8pdt
```

See Also

```
ap-quickstart(config)> hotsname
ap-quickstart(config)> mgmt-ipaddress
ap-quickstart(config)> dns
ap-quickstart(config)> location
ap-quickstart(config)> ap-location
ap-quickstart(config)> admin-contact
ap-quickstart(config)> email
ap-quickstart(config)> date
ap-quickstart(config)> time
ap-quickstart(config)> time-zone
ap-quickstart(config)> time-sync
```

system(config)> time

Use this command to configure the time on the AP.

Syntax

```
time **hh:mm:ss** *hh:mm:ss*
```

Input Parameters

hh:mm:ss	The time in hours:minutes:seconds format.

Output Parameters

Success or Failure

Description

Use this command to set the time on the AP. If the AP has access to internet or an internal NTP server, then enable time synchronization so that time settings may be obtained from the time server instead of configuring it manually on the AP.

Defaults

None

Usage Guidelines

Examples

```
time 16:12:30
```

See Also

```
system(show) > system-group
```

system(config)> time-sync

Use this command to configure the time on the AP.

Syntax

```
time-sync { manual | ntp-servers domain-name/ipaddress {…} }
```

Input Parameters

manual	Specifies that time will be configured manually and the AP should not try to autosynchronize the time on the AP with a NTP server.
ntp-servers	A list of servers address specified within double quotes that identify the NTP servers that the AP can talk to.

Output Parameters

Success or Failure

Description

Use this command to configure the set of Network Time Protocol servers that the AP can talk to to synchronize its time with. The Airgo AP ships with five well-known NTP server addresses that it will try to contact when needed. Using this command additional servers may be configured on the AP. When time needs to be synchronized, any server configured via this command will be contacted first. If those servers do not respond, then the list of preconfigured servers will be attempted.

To ensure that NTP time synchronization works correctly, make sure that the NTP time synchronization is enabled via the *ntp-time-sync* command. Also make sure that DNS servers are correctly configured on the AP so that, if needed, the list of external NTP servers may be contacted.

Defaults

None

Usage Guidelines

Find a NTP time server closest to your locale.

Examples

```
time-sync ntp-servers clock.via.net timekeeper.isi.edu
```

See Also

```
system(show) > system-group
```

system(config)> time-zone

Use this command to configure the time zone on the AP.

Syntax

```
time-zone { { us-zone { pst8pdt | mst7mdt | cst6cdt | est5edt } } | { gmt-plus
hh:mm | gmt-minus hh:mm } }
```

Input Parameters

us-zone	Specifies a US time zone.
gmt-plus	Specified a time reference with respect to GMT time.
gmt-minus	Specifies a time reference with respect to GMT time.

Output Parameters

Success or Failure

Description

Use this command configure the current time zone. Set the time and the configure the time zone to reflect the correct local time. You can specify time relative to GMT as well.

Defaults

The AP ships with the default time zone set to pst8pdt.

Usage Guidelines

Examples

```
time-zone us-zone mst7mdt
```

See Also

```
system(show) > system-group
```

system(show)> version

Use this command to display the hardware and software versions of the components on the AP.

Syntax

```
version
```

Description

Use this command to display the hardware and software versions of the components on the AP.

Defaults

None

Usage Guidelines

None

Examples

```
system(show)> version

vendor               : Airgo Networks, Inc.
model                : AGN1201AP-000
model-type           : AGN1dev
serial-number        : AIRGO-P2-0xxxxxxxxx
sys-hw-id            : 00:0a:f5:00:01:f2
sys-hw-ver           : 1
sys-hw-options       : None
sys-sw-ver           : 1.0.0
sys-sw-buildnumber   : 64
sys-sw-builddate     : 2004-02-09,15:20:51,-08:00
sys-sw-licenses      : AIRGO-MRAP, AIRGO-HEAP
```

See Also

15 VLAN CLIs

This chapter includes information about the following VLAN commands:

- **vlan(config)> add-interface**
- **vlan(config)> add-ipaddress**
- **vlan(config)> add-vlan**
- **vlan(config)> clear-statistics**
- **vlan(config)> delete-interface**
- **vlan(config)> delete-ipaddress**
- **vlan(config)> delete-vlan**
- **vlan(config)> interface-vlan**
- **vlan(config)> mgmt-vlan**
- **vlan(show)> mgmt-vlan**
- **vlan(show)> statistics**
- **vlan(show)> user-vlan-table**
- **vlan(show)> vlan-table**

vlan(config)> add-interface

Use this command to attach interfaces to a VLAN.

Syntax

```
add-interface vlan-id vlan-id interface interface-name {…} {tagged | untagged}
```

Input Parameters

vlan-id *vlan-id*	Specifies *vlan-id* as the VLAN to which interfaces will be attached.
interface *interface-name {…}*	The list of interfaces to be attached to the VLAN.
tagged	Frames transmitted on the interfaces in the interface list for this VLAN will contain an 802.1Q VLAN tag.
untagged	Frames transmitted on the interfaces in the interface list for this VLAN will not contain an 802.1Q VLAN tag.

Output Parameters

Success or Failure

Description

This command attaches the interfaces on the interface list to the specified VLAN.

Defaults

None

Usage Guidelines

Use this command to attach interfaces to a VLAN and control whether frames transmitted out an interface for a VLAN will contain and 802.1Q VLAN tag or not. All interfaces for the interface VLAN must be configured as untagged. Radio interfaces must be configured as untagged. VLAN tagged frames received on an untagged interface will be dropped. Untagged frames received on the Ethernet interface will be classified into the interface VLAN. Untagged frames received on a radio interface will be classified into the VLAN specified in the service profile assigned to a station if defined. Otherwise, untagged frames received on a radio interface will be classified into the interface VLAN.

Examples

```
add-interface vlan-id 2 interface “wlan0 wlan1” untagged
```

See Also

```
vlan(config)> delete-interface
vlan(config)> interface-vlan
ssid(config)> define-service-profile
```

vlan(config)> add-ipaddress

Use this command to assign an IP address to a VLAN.

Syntax

```
add-ipaddress vlan-id vlan-id {ipaddress ip-address/subnet-mask-length | dhcp-assigned}
```

Input Parameters

vlan-id *vlan-id*	Specifies *vlan-id* as the VLAN to which the IP address will be assigned.
ipaddress *ip-address/ subnet-mask-length*	The IP address and subnet mask to be assigned to *vlan-id*.
dhcp-assigned	The IP address will be obtained from a DHCP server.

Output Parameters

Success or Failure

Description

This command assigns an IP address and subnet mask to a VLAN. The subnet mask is specified by its bit length. (For example, 255.255.255.0 has a subnet mask length of 24.) If dhcp-assigned is specified, the IP address will be leased from a DHCP server.

Defaults

None

Usage Guidelines

When an VLAN is assigned an IP address, the VLAN becomes a routable interface and can transfer packets with other routable interfaces in the AP.

Examples

```
add-ipaddress vlan-id 2 ipaddress 10.0.2.1/24
```

See Also

```
vlan(config)> delete-ipaddress
vlan(show)> vlan-table
```

vlan(config)> add-vlan

Use this command to create a VLAN on the AP.

Syntax

```
add-vlan vlan-id vlan-id [name name]
```

Input Parameters

vlan–id *vlan-id*	Specifies *vlan-id* as the newly created VLANs identifier.
name *name*	(Optional) Name assigned to the newly created VLAN.

Output Parameters

Success or Failure

Description

This command creates a VLAN on the AP with the specified *vlan-id* and *name*. The *vlan-id* can range from 2 to 4093.

Defaults

None

Usage Guidelines

Use this command on an existing VLAN to change its name.

Examples

```
add-vlan vlan-id 2 name vlan2
```

See Also

```
vlan(config)> delete-vlan
vlan(show)> vlan-table
```

vlan(config)> clear-statistics

Use this command to clear VLAN statistics on the AP.

Syntax

```
clear-statistics {all-vlans | vlan-id vlan-id}
```

Input Parameters

all-vlans	Clear statistics for all VLANs.
vlan-id *vlan-id*	Clear statistics for VLAN *vlan-id*.

Output Parameters

Success or Failure

Description

This command clears the statistics for interfaces on the AP.

Defaults

None

Usage Guidelines

The counters that comprise the VLAN statistics are set to zero when cleared.

Examples

```
clear-statistics vlan-id 2
```

See Also

```
vlan(show)> statistics
```

vlan(config)> delete-interface

Use this command to remove an interface from a VLAN.

Syntax

```
delete-interface vlan-id vlan-id (all-interfaces | interface interface-name
{…}}
```

Input Parameters

vlan-id *vlan-id*	Specifies the VLAN from which interfaces will be removed.
all-interfaces	All interfaces attached to VLAN *vlan-id* will be removed.
interface *interface-name {…}*	Specifies a list of interface names to be removed from VLAN *vlan-id.*

Output Parameters

Success or Failure

Description

This command removes interfaces from a VLAN.

Defaults

None

Usage Guidelines

Use this command to remove interfaces from a VLAN. Frames that are classified into a VLAN that is not attached to the receiving interface are dropped.

Examples

```
delete-interface vlan-id 2 interface “wlan0 wlan1”
```

See Also

```
vlan(config)> add-interface
vlan(config)> interface-vlan
vlan(show)> vlan-table
```

vlan(config)> delete-ipaddress

Use this command to remove an IP address from a VLAN.

Syntax

```
delete-ipaddress vlan-id vlan-id
```

Input Parameters

vlan-id *vlan-id*	Remove the IP address from VLAN *vlan-id*.

Output Parameters

Success or Failure

Description

This command removes an IP address from a VLAN.

Defaults

None

Usage Guidelines

When the IP address has been removed from a VLAN, that VLAN becomes unroutable and will not be able to transfer packets with other routable interfaces in the AP.

Examples

```
delete-ipaddress vlan-id 2
```

See Also

```
vlan(config)> add-ipaddress
vlan(show)> vlan-table
```

vlan(config)> delete-vlan

Use this command to remove a VLAN from the AP.

Syntax

```
delete-vlan {all-vlans | vlan-id vlan-id | name name}
```

Input Parameters

all-vlans	Remove all user created VLANs on the AP.
vlan-id *vlan-id*	Remove VLAN *vlan-id* from the AP.
name *name*	Remove the VLAN named *name.*

Output Parameters

Success or Failure

Description

This command removes a VLAN from the AP.

Defaults

None

Usage Guidelines

Received frames that are classified into VLANs that have not been instantiated on the AP are dropped. VLAN 1, VLAN 4094 and the management VLAN cannot be removed from the AP.

Examples

```
delete-vlan vlan-id 2
```

See Also

```
vlan(config)> add-vlan
vlan(config)> interface-vlan
vlan(show)> vlan-table
```

vlan(config)> interface-vlan

Use this command to designate the VLAN into which untagged frames will be classified.

Syntax

```
interface-vlan interface interface-name {default-vlan-id | vlan-id vlan-id}
```

Input Parameters

interface *interface-name*	Specifies *interface-name* as the interface for which the interface VLAN will be configured.
default-vlan-id	Untagged frames received on *interface-name* will be classified into VLAN 1.
vlan-id *vlan-id*	Untagged frames received on interface-name will be classified into VLAN *vlan-id.*

Output Parameters

Success or Failure

Description

This command designates the VLAN into which untagged frames will be classified.

Defaults

Untagged frames are classified into VLAN 1.

Usage Guidelines

Only a VLAN that the interface is attached to can be designated as the interface VLAN. Untagged frames classified into a VLAN that has been removed from the AP will be dropped.

Examples

```
interface-vlan interface eth0 vlan-id 2
```

See Also

```
vlan(config)> add-interface
vlan(config)> add-vlan
vlan(config)> delete-interface
vlan(config)> delete-vlan
vlan(show)> interface-vlan-table
```

vlan(show)> interface-vlan-table

Use this command to display the interface VLAN for interfaces in the AP.

Syntax

```
interface-vlan-table [interface interface-name]
```

Input Parameters

interface *interface-name*	(Optional) Display interface VLAN for interface *interface-name.* The interface VLAN assigned for each interface in the AP is displayed if *interface-name* is not specified.

Output Parameters

interface	Name of the interface.
vlanid	VLAN that has been designated as the interface VLAN for this interface.

Description

This command displays the interface VLAN for each interface in the AP.

Defaults

The interface VLAN for all interfaces in the AP are displayed.

Usage Guidelines

The command can be used to determine which VLAN untagged frames will be classified into for each interface in the AP.

Examples

```
interface-vlan-table interface eth0
interface : eth0
vlanid    : 2
```

See Also

```
vlan(config)> interface-vlan
```

vlan(config)> mgmt-vlan

Use this command to designate a VLAN as the management VLAN.

Syntax

```
mgmt-vlan {default-vlan-id | vlan-id vlan-id} [name name]
```

Input Parameters

default-vlan-id	Designate VLAN 1 as the management VLAN.
vlan-id *vlan-id*	Designate VLAN *vlan-id* as the management VLAN.
name *name*	(Optional) Assign *name* to the management VLAN.

Output Parameters

Success or Failure

Description

This command designates a VLAN as the management VLAN.

Defaults

VLAN 1 is the default management VLAN.

Usage Guidelines

The purpose of the management VLAN is to carry management traffic, such as SNMP and IAPP, to and from the AP. To manage the AP over the network, an IP address should be assigned to the management VLAN either statically or dynamically using DHCP.

Examples

```
mgmt-vlan vlan-id 2
```

See Also

```
vlan(config)> add-ipaddress
vlan(show)> mgmt-vlan
ap-quickstart(config)> mgmt-ipaddress
```

vlan(show)> mgmt-vlan

Use this command to display management VLAN information.

Syntax

```
mgmt-vlan
```

Output Parameters

vlanid	VLAN identifier of the management VLAN.
name	Name assigned to the management VLAN.
ipaddress	IP address and subnet mask length assigned to the management VLAN.
interface	Interfaces attached to the management VLAN.
sta-mac	MAC addresses of stations that have been assigned to the management VLAN based on their service profiles.

Description

This command displays information about the management VLAN.

Defaults

None

Usage Guidelines

The command can be used to verify the configuration of the management VLAN.

Examples

```
vlan(show)> mgmt-vlan

vlanid      : 1
name        : Default VLAN
ipaddress   : 192.168.168.24/24
ipaddrtype  : dhcp-assigned
interface   : eth0 wlan0 wlan1 wlan1.tk0
sta-mac     : 00:0a:f5:00:04:84 00:0a:f5:00:05:fe
```

See Also

```
ap-quickstart(config)> mgmt-ipaddress
vlan(config)> add-ipaddress
vlan(config)> add-interface
vlan(config)> mgmt-vlan
ssid(config)> define-service-profile
```

vlan(show)> statistics

Use this command to display VLAN statistics.

Syntax

```
statistics [vlan-id vlan-id]
```

Input Parameters

vlan-id *vlan-id*	(Optional) Display statistics for vlan *vlan-id*. Statistics for all VLANs in the AP are displayed if *vlan-id* is not specified.

Output Parameters

vlanid	VLAN identifier for the VLAN.
rcv-byte	Number of bytes received by all interfaces attached to the VLAN.
rcv-pkt	Number of packets received by all interfaces attached to the VLAN.
xmt-byte	Number of bytes transmitted by all interfaces attached to the VLAN.
xmt-pkt	Number of packets transmitted by all interfaces attached to the VLAN.
rcv-multicast	Number of multicast packets received by all interfaces attached to the VLAN.

Description

This command displays statistics for all VLANs in the AP.

Defaults

Statistics for all VLANs in the AP are displayed.

Usage Guidelines

This command can be used to determine the amount of data each VLAN forwards to and from its attached interfaces in the AP.

Examples

```
statistics vlan-id 1
vlanid        : 1
rcv-byte      : 606163238
rcv-pkt       : 1149791
xmt-byte      : 627116703
xmt-pkt       : 1159024
rcv-multicast : 124543
```

See Also

```
vlan(config)> clear-statistics
```

vlan(show)> user-vlan-table

Use this command to display station MAC addresses assigned to VLANs.

Syntax

```
user-vlan-table [vlan-id vlan-id]
```

Input Parameters

vlan-id *vlan-id* (Optional) Display station MAC addresses assigned to VLAN *vlan-id*. Station MAC addresses assigned to all VLANs created in the AP are displayed if *vlan-id* is not specified.

Output Parameters

vlanid VLAN identifier of the VLAN.

name Name assigned to the VLAN.

ipaddress IP address and subnet mask length assigned to the VLAN.

ipaddrtype Type of IP address: user-assigned, dhcp-assigned or blank (for not yet requested)

sta-mac MAC addresses of stations assigned to this VLAN based on their service profile.

Description

This command displays MAC addresses belong to stations that have been assigned to VLANs based on their service profiles.

Defaults

Station MAC address for all VLANs in the AP are displayed.

Usage Guidelines

The command can be used to determine the VLAN and IP subnet a station belongs to.

Examples

```
vlan(show)> user-vlan-table

vlanid     : 1
name       : Default VLAN
ipaddress  : 192.168.168.24/24
ipaddrtype : dhcp-assigned
sta-mac    : 00:0a:f5:00:04:84 00:0a:f5:00:05:fe
--------------------------------------------------------------------------

vlanid     : 88
name       : Corporate
ipaddress  : 0.0.0.0/0
ipaddrtype :
sta-mac    :
```

See Also

```
ssid(config)> define-service-profile
```

vlan(show)> vlan-table

Use this command to display information about the AP’s interfaces.

Syntax

```
vlan-table [vlan-id vlan-id]
```

Input Parameters

vlan-id *vlan-id* — (Optional) Display information for vlan *vlan-id.* Information for all VLANs created in the AP is displayed if *vlan-id* is not specified.

Output Parameters

vlanid — VLAN identifier of the VLAN.

name — Name assigned to the VLAN.

ipaddress — IP address and subnet mask length assigned to the VLAN.

ipaddrtype — Type of IP address: user-assigned, dhcp-assigned or blank (for not yet requested)

interface — Name of the interface attached to the VLAN.

tagged — Indicates whether the interface has been configured as tagged or untagged.

Description

This command displays information for VLANs in the AP.

Defaults

Information for all interfaces in the AP is displayed.

Usage Guidelines

The command can be used to verify the configuration for each VLAN in the AP.

Examples

```
vlan(show)> vlan-table

vlanid     : 1
name       : Default VLAN
ipaddress  : 192.168.168.24/24
ipaddrtype : dhcp-assigned
interface  : eth0
tagged     : no
--------------------------------------------------------------------------

vlanid     : 1
name       : Default VLAN
ipaddress  : 192.168.168.24/24
ipaddrtype : dhcp-assigned
interface  : wlan0
tagged     : no
--------------------------------------------------------------------------

vlanid     : 1
name       : Default VLAN
```

```
ipaddress  : 192.168.168.24/24
ipaddrtype : dhcp-assigned
interface  : wlan1
tagged     : no
--------------------------------------------------------------------------

vlanid     : 1
name       : Default VLAN
ipaddress  : 192.168.168.24/24
ipaddrtype : dhcp-assigned
interface  : wlan1.tk0
tagged     : no
--------------------------------------------------------------------------

vlanid     : 88
name       : Corporate
ipaddress  : 0.0.0.0/0
ipaddrtype :
interface  : wlan1.tk0
tagged     : yes
--------------------------------------------------------------------------

vlanid     : 88
name       : Corporate
ipaddress  : 0.0.0.0/0
ipaddrtype :
interface  : wlan0
tagged     : no
--------------------------------------------------------------------------

vlanid     : 88
name       : Corporate
ipaddress  : 0.0.0.0/0
ipaddrtype :
interface  : eth0
tagged     : yes
```

See Also

```
vlan(config)> add-interface
vlan(config)> add-ipaddress
vlan(config)> add-vlan
```