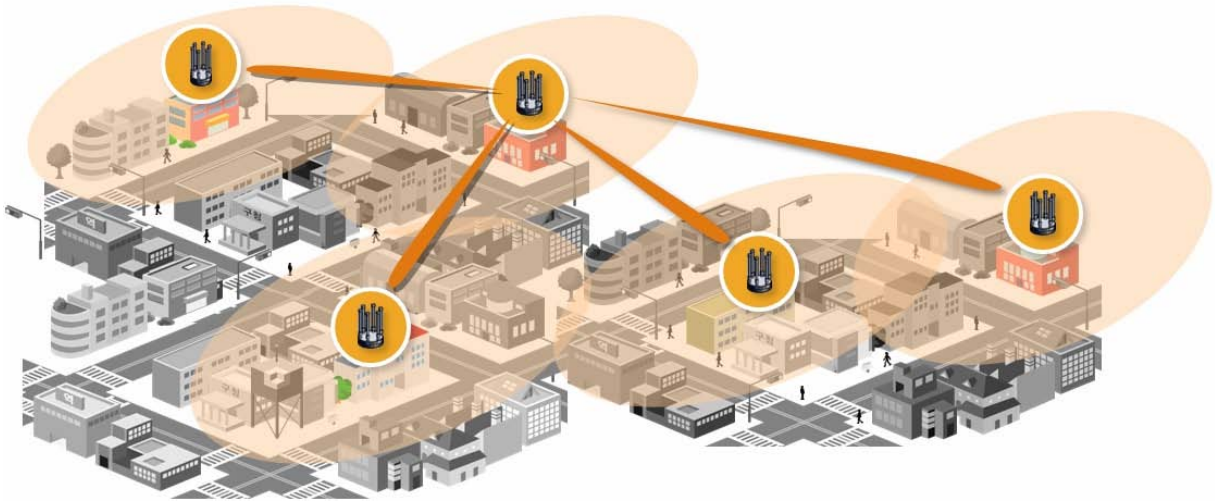
NetPoint Pro Family

Broadband Wireless Networking Solutions

NetPoint Pro 6x2.4 / 3x2.4 (G2 and G2M)

CLI Reference Guide



2nd Generation

Statement of Conditions

The information contained in this document is subject to change without notice.

Netronics shall not be liable for errors contained herein or for incidental or consequential damage in connection with the furnishing, performance, or use of this document or equipment supplied with it.

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

READ THIS FIRST!

Important Safety Instructions

Read and save these instructions. Heed all warnings. Follow all instructions.

Do not defeat the safety purpose of the grounding. Only use attachments/accessories specified by the manufacturer.

Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way. For example, if the power-supply cord or plug is damaged, liquid has been spilled on the apparatus, objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, it does not operate normally, or has been dropped.

There is a risk of personal injury or death if the NPP-6X2.4 antennas come near electric power lines. Carefully read and follow all instructions in this manual. By nature of the installation, you may be exposed to hazardous environments and high voltage. Use caution when installing the outdoor system.

This apparatus must be connected to earth ground.

Do not open the unit. There is a risk of electric shock inside.

You are cautioned that any change or modification not expressly approved in this manual could void your authority to operate this equipment.

There are no user-serviceable parts inside. All service must be performed by qualified personnel.

The RJ45 connectors of your Netronics NPP-6X2.4 may source DC power On pins 4,5 and 7,8. The IEEE 802.3 standards allow for pins 4,5 and 7,8 to be used for Power Over Ethernet. Some products may be incompatible with the Netronics Power Over Ethernet capability. If such problems occur, make sure that the unit is configured with the Power Over Ethernet capability set to Off (default setting). If problems persist, use Ethernet cables that have no connections to the unused pins 4,5 and 7,8.

The Netronics NPP-6X2.4 and NPP-3X2.4 can be installed in wet, outdoor locations. Make sure closure caps are installed and all cable connections are securely fastened and waterproofed.

The Netronics NPP-6X2.4 can only be used with approved antennas.

Table of Contents

Chapter 1

Introduction

Scope of this Document

This guide is for the networking professional using the NetPoint Pro CLI command line interface. The CLI manages NetPoint Pro access points. Before using this guide, please refer to the device user guide. Also take time to become familiar with the concepts and terminology of Wi-Fi, Ethernet and local area networking.

Organization

This guide is organized into these sections:

Chapter 1, "Using the Command-Line Interface", describes how to access the command modes and use the command-line interface (CLI) to configure software features.

Chapter 2, "NetPoint Pro CLI Commands for Access Points", describes in alphabetical order the NetPoint Pro CLI commands used to configure and monitor the access point.

Conventions

This publication uses the following conventions to convey instructions and information:

Command descriptions conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) means optional elements.
- Braces ({ }) group required choices, and vertical bars ( ) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ }]) mean a required choice within an optional element.

Chapter 2

Using the NetPoint Pro CLI

Using the NetPoint Pro CLI

The NetPoint Pro Command Line Interface (CLI) is a powerful tool to communicate with NetPoint Pro access points. CLI access is available at three levels of user privileges:

- super – The super user has the highest level of privilege.
- admin – The administrator has a medium level of privilege.
- viewer – The viewer has viewing-only privilege.

Before logging in to the NetPoint Pro CLI software, select the appropriate user level. The user level sets the subset of the available commands. To have access to all commands you must login as super user (super). Creating new user, setting a user privilege level, and setting a password is detailed in the user guide.

Configurations

There are three types of configurations on the NetPoint Pro access point units:

- Startup – The startup configuration typically is used when starting the device. This configuration is stored in non-volatile memory.
- Running – The running configuration is the current configuration of the running device. This configuration is stored in volatile memory.
- Default – The default configuration contains predetermined default values for the specific software version. This configuration is stored in non-volatile memory.

At system start the device is configured according to the startup configuration. As a result, the configuration currently running in volatile memory is exactly the same as the startup configuration. All CLI commands executed after system start affect the running configuration. In this way, you can change the current configuration without modifying the original startup configuration. By copying the running configuration to the startup configuration, the startup configuration can be modified.

The first time a device boots or when the startup configuration has been deleted, the unit loads the default configuration. The default configuration is a predetermined group of settings released per software version. A user cannot change the default configuration. When a device is shipped from the factory its startup configuration is identical to the default configuration. When the startup configuration is missing the default settings are copied to the startup configuration and used during boot time.

Most of the commands are one-time commands. The configuration commands change the running configuration. When the running configuration is saved to the startup configuration, these commands are stored in a non-volatile environment. See Saving Configuration Changes below.

Special Character Functions

abbreviated-command-entry<*Tab*>: Completes a partial command name.

ap> config<tab> results in ap> configure

The available commands depend on the current user level. Entering a question mark (**?**) at the system prompt displays a list of commands available for each command level.

? List all commands available for a particular command level.

ap>? (for example)
configure - Configures network and system parameters of the NetPoint Pro 3x2.4 OR NetPoint Pro 6x2.4.
ping - Sends ICMP ping packets.
(etc.)

command ? List the keywords or arguments that you must enter next on the command line. (There is a space between the command and the question mark.)

ap> configure ?
<enter> - Enter command mode
interface - Configures network interfaces
(etc.)

/ return to the root of the CLI command structure.

ap> configure>/
ap>

/<command to execute> return to the root of the CLI command structure after executing the command.

ap> /configure *<parameters> <enter>*
ap>

Enable/Disable

Within selected commands is the ability to enable or disable a function. For example, the configure classifier command has two parameters: <codec name> and {enable | disable}.

configure classifier <codec name> {enable | disable}

When enable is selected, the specified codec is enabled. When disable is selected, the specified codec is disabled.

Another way to enable or disable a function is by using a specific command. For example,

configure mesh filter-list {enable | disable}

In this case the configure command enables or disables the use of a mesh filter list, which is based on the value “true” or “false”.

Using Configuration and Remove commands

A configuration command defines a configuration in the running configuration.

For example, to configure an SSID:

ap> configure ssid 2 name Netronics vlan 0 privacy-method none type hidden

To unassign, to take the effect of this command out of the running configuration, execute the associated remove function. The remove functions are implemented by either the associated remove command or by the remove option.

For example to remove an existing SSID, execute the following remove command:

ap> configure ssid 2 remove

For example to remove a MAC address from the mesh filter list, execute the following command with the remove option:

ap> configure mesh filter-list 00:14:06:11:00:00 remove

Almost every configuration command has an associated remove command or remove option. In general, a configuration command causes an effect in the running configuration; “remove” takes the effect out of the running configuration.

Delete

There are two general ways to delete something from the system. The first uses a specific delete command such as deleting the startup configuration:

delete startup-config

or deleting the mac-filter list:

configure mac-filter delete <index integer>.

Another way to delete is within a command such as deleting a specified CLI user:

configure username <username string> delete.

Any time something is deleted, it is only removed from the running configuration, not the startup configuration. To make the changes permanent the running configuration must be saved to the startup configuration

Saving Configuration Changes

The concept of the three types of configuration is so important that it is repeated here.

The running configuration is non-permanent and dynamic. It changes as commands are executed in order to demonstrate the new system configuration. The running configuration does not remain over a power cycle, reboot, or system failure. This configuration can be saved to the startup configuration to make it non-volatile.

The startup configuration is non-volatile, stored in memory, and is stable over power cycle, reboot, and system failure. This configuration is loaded into the running configuration at system start.

The default settings configuration allows the startup configuration to be replaced with default settings.

To save the running configuration to the startup configuration enter the **copy running-config startup-config** command. For example:

```
ap> copy running-config startup-config
```

It might take a few seconds to save the configuration. After the configuration has been saved, the following output appears:

```
TRAP: Configuration Saved.
```

```
Configuration Action Succeeded.
ap>
```

Radio Interfaces

The NetPoint Pro device uses multiple radio interfaces to communicate with other NetPoint Pro devices and customer stations. Each radio interface is identified by an interface number, which is used by the CLI to configure and manage the NetPoint Pro devices. The following table lists the NetPoint Pro devices and the type of radio interfaces that they utilize:

Product Model	Product P/N	Interface 0	Interface 1	Interface 2
NetPoint Pro 6x2.4 F	NPP-ANT-6x2.4F	xRF 2.4Ghz	5.8Ghz	N/A
NetPoint Pro 6x2.4 E	NPP-ANT-6x2.4E	xRF 2.4Ghz	5.4Ghz	N/A
NetPoint Pro 6x2.4 M	NPP-ANT-6x2.4M	xRF 2.4Ghz	5.8Ghz	N/A

Only 5.4Ghz and 5.8Ghz interfaces are defined as 802.11a backhaul radio interfaces, by default.
All 2.4Ghz and 4.9Ghz interfaces are defined as access radio interfaces, by default.

Chapter 3

NetPoint Pro CLI Commands

NetPoint Pro CLI commands

This chapter lists and describes NetPoint Pro CLI commands in Software Release 2.6.7 that you use to configure and manage your NetPoint Pro access point. The commands are listed alphabetically.

CONFIGURE CAC

Function: Enables or disables the Call Admission Control (CAC) feature.

Command Syntax: **configure cac** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables CAC. disable – Disables CAC. The default value is disable.

Example: configure cac enable

Permission Level: admin

Related Commands:
configure cac mac_classifier
configure cac min-vc-snr
show cac active-voip-clients
show cac params

CONFIGURE CAC ALGORITHM

Function: Configures the current Call Admission Control (CAC) algorithm.

Command Syntax: **configure cac algorithm** {VA1 | VA2}

Command Description:

Parameter	Value
VA1 | VA3	VA1 – Sets the CAC algorithm based on the number of associated VoIP devices and the SNR. VA3 – Not supported in this version of the CLI. The default value is VA1.

Example: configure cac algorithm VA1

Permission Level: admin

Related Commands:
configure cac mac_classifier
configure cac min-vc-snr
show cac active-voip-clients
show cac params

CONFIGURE CAC MAC_CLASSIFIER

Function: Configures the Call Admission Control (CAC) MAC classifier feature. This feature is used to optimize traffic with VoIP devices. The VoIP devices are identified using a MAC mask.

Command Syntax: **configure cac mac_classifier** {enable | disable}
configure cac mac_classifier {add | delete} <mac mask>

Command Description:

Parameter	Value
enable | disable	enable – Enables MAC classifier. disable – Disables MAC classifier. The default value is disable.
add | delete	add – Adds a new MAC mask. delete – Deletes a MAC mask.
mac mask	MAC Mask xx:xx:xx. This parameter is used to identify the VoIP devices. Specify the first three bytes of the MAC address. This identifies the manufacturer of the devices. The value must be specified according to the following syntax (XX:XX:XX).

Example: configure cac mac_classifier add 11:01:22

Permission Level: admin

Related Commands:

configure cac
configure cac min-vc-snr
show cac active-voip-clients
show cac params

CONFIGURE CAC MAX_VC

Function: Defines the maximum number of simultaneous voice sessions on the device. The specified value defines the maximum allowed voice sessions per access channel.

Command Syntax: **configure cac max_vc** <max_vc>

Command Description:

Parameter	Value
max_vc	Maximum number of voice sessions per access channel: 0-32 The default value is 32.

Example: configure cac max_vc 20

Permission Level: admin

Related Commands:
configure cac
configure cac mac_classifier
show cac active-voip-clients
show cac params

CONFIGURE CAC MIN-VC-SNR

Function: Configures the CAC minimum voice call SNR threshold.

Command Syntax: **configure cac min-vc-snr** <threshold number>

Command Description:

Parameter	Value
threshold number	Minimum Voice Call SNR threshold number: 1-100 The default value is 12.

Example: configure cac min-vc-snr 20

Permission Level: admin

Related Commands:
configure cac
configure cac mac_classifier
show cac active-voip-clients
show cac params

CLOCK

Function: Displays the system clock time and date.

Command Syntax: **clock**

Command Description:

Parameter	Value
None	

Example: clock

Permission Level: viewer

Related Commands:
clock set

CLOCK SET

Function: Configures the system clock settings (24 hours, local time).

Command Syntax: **clock set** <datetime string>

Command Description:

Parameter	Value
datetime string	Date and time string according to the following syntax: MMDDhhmmYYYY MM – Month DD – Date hh – Hour mm – Minute CC – Century YY – Year

Example: This example demonstrates how to set the clock to July 23, 2007 at 11:47:55AM.
clock set 072311472007

Permission Level: admin

Related Commands:
Clock

CONFIGURE CALIBRATION FORCE-CALIBRATION

Function: Executes an immediate calibration of the specified 802.11b/g radio interface(s).

Command Syntax: **configure calibration force-calibration** interface {0 | 1 | all} [{short | long}]

Command Description:

Parameter	Value
0 | 1 | all	Radio interface number: 0 – Calibrates radio interface 0. 1 – Calibrates radio interface 1. all – Calibrates all 802.11b/g radio interfaces in the unit.
short | long	Type of calibration: short – Starts a short calibration. long – Starts a long calibration. This parameter is optional. The default value is short.

Example: configure calibration force-calibration interface 0 long

Permission Level: super

Related Commands:
configure interface Dot11Radio channel

CONFIGURE CLASSIFIER

Function: Configures the standard codecs that are supported by the classifier.

Command Syntax: **configure classifier** <codec name> {enable | disable}

Command Description:

Parameter	Value
codec name	Defines the standard classifier to be enabled or disabled: **g-711** – G.711 (rate 64 Kbps) codec **g-726** – G.726 (rate 24 Kbps) codec **g-728** – G.728 (rate 16 Kbps) codec **g-729** – G.729 (rate 8 Kbps) codec **g-723-1-rate5-3** – G.723.1 (rate 5.3 Kbps) codec **g-723-1-rate6-3** – G.723.1 (rate 6.3 Kbps)
enable | disable	enable – Enables the specified codec. disable – Disables the specified codec.

Example: This example demonstrates how to enable support for G.711 codec.
configure classifier g-711 enable

Permission Level: admin

Related Commands:
configure classifier add

configure classifier remove
show classifier

CONFIGURE CLASSIFIER ADD

Function: Adds, defines, and enables a new codec.

Command Syntax: **configure classifier add** <name string> interval <interval number> packet-size <packet-size number> [{bidirectional | unidirectional}] [jitter <jitter number>]

Command Description:

Parameter	Value
name string	Name of the new codec to be configured. The value can be up to 31 characters.
interval number	Packet interval. Minimum time difference between two consecutive packets (msec): 0-5000
packet-size	Maximum packet size (bytes): 20-2347
bidirectional | unidirectional	Pack direction: bidirectional – Packet direction is bidirectional. unidirectional – Packet direction is in the downstream direction towards the client. The default value is unidirectional.
jitter number	Jitter size. Defines the time variation of intervals between two consecutive packets (msec): 0-50 Maximum time interval between two consecutive packets is defined by the time values for *interval number* + *jitter number*. The default value is 15 (15 msec).

Example: configure classifier add new-codec interval 20 packet-size 80

Permission Level: admin

Related Commands:
configure classifier
configure classifier remove
show classifier

CONFIGURE CLASSIFIER REMOVE

Function: Deletes and disables the codec specified, including standard codecs. When an added codec is specified, it is removed from the running configuration.

Command Syntax: **configure classifier remove** <name string>

Command Description:

Parameter	Value
name string	Name of the codec all

Example: configure remove g-711

Permission Level: admin

Related Commands:
configure classifier
configure classifier add
show classifier

CONFIGURE ENHANCED-OMNI

Function: Enables and disables the enhanced omni mode.

Command Syntax: **configure enhanced-omni** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables the enhanced omni mode. disable – Disables the enhanced omni mode. The default mode is disable.

Example: configure enhanced-omni enable

Permission Level: admin

Related Commands:
show enhanced-omni

CONFIGURE INACTIVITY-TIMEOUT

Function: Configures the CLI timeout. Defines the time that the CLI automatically logs off the user when the user session is not active.

Command Syntax: **configure inactivity-timeout** <timeout number>

Command Description:

Parameter	Value
timeout number	CLI timeout period (minute): 1-90 The default value is 10 (10 minutes).

Example: configure inactivity-timeout 30

Permission Level: admin

Related Commands:
show inactivity-timeout

CONFIGURE INTERFACE DOT11RADIO BANDWIDTH

Function: Configures the bandwidth on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **bandwidth** {5 | 10 | 20 | 40}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
5 | 10 | 20 | 40	Bandwidth: 5 – 5 Mhz 10 – 10 Mhz 20 – 20 Mhz 40 – 40 Mhz The default value is 20 (20 Mhz).

Example: configure interface Dot11Radio 0 bandwidth 40

Permission Level: super

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO BEACON-PERIOD

Function: Configures the time period between transmitting beacons by the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **beacon-period** <period number>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
period number	Time period between beacons (msec): 100-1000 Default value for 802.11a interface is 200 (200 msec). Default value for 802.11b/g interface is 250 (250 msec).

Example: configure interface Dot11Radio 0 beacon-period 200

Permission Level: admin

Related Commands:

show interface Dot11Radio
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO BEACON-RATE

Function: Configures the transmitted beacon-rate on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **beacon-rate** <rate number>}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
<rate number>	Beacon-Rate: 1 – 1 Mbps 2 – 2 Mbps 5.5 – 5.5 Mbps 6 – 6 Mbps 11 – 11 Mbps 12 – 12 Mbps The default value is 1 (1 Mbps).

Example: configure interface Dot11Radio 0 beacon-rate 2

Permission Level: super

Related Commands:
show interface Dot11Radio
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO CHANNEL

Function: Configures the Wi-Fi channel used on the specified radio interface. The actual frequencies available are dependent on the radio interface (802.11a or 802.11b/g) and the region to which the unit was manufactured. To display all available channels for the specified radio interface, use the *show interface Dot11Radio channel-list* command.

Command Syntax: **configure interface Dot11Radio** <interface number> **channel** {<channel number> | default | auto}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio

	interfaces are used for 2.4GHz communications.
<channel number> | default | auto	Channel and Frequencies IEEE 802.11b/g: 1– 2412 Mhz 2– 2417 Mhz 3– 2422 Mhz 4– 2427 Mhz 5– 2432 Mhz 6– 2437 Mhz 9– 2447 Mhz 10– 2452 Mhz 11– 2457 Mhz 12– 2462 Mhz 13– 2467 Mhz Default value for Dot11Radio 0 is channel 4 (2427 MHz).
<channel number> | default | auto (continue)	Channel and Frequencies for IEEE 802.11a: 34 – 5170 Mhz 36 – 5180 Mhz 38 – 5190 Mhz 40 – 5200 Mhz 42 – 5210 Mhz 44 – 5220 Mhz 46 – 5230 Mhz 48 – 5240 Mhz 52 – 5260 Mhz 56 – 5280 Mhz 60 – 5300 Mhz 64 – 5320 Mhz 100 – 5500 Mhz 104 – 5520 Mhz 108 – 5540 MHz 112 – 5560 Mhz 116 – 5580 Mhz 120 – 5600 Mhz 124 – 5620 Mhz 128 – 5640 Mhz 132 – 5660 Mhz 136 – 5680 Mhz 140 – 5700 Mhz 149 – 5745 Mhz 153 – 5765 Mhz 157 – 5785 Mhz 161 – 5805 Mhz 165 – 5825 Mhz Default channel for 802.11a radio is 161 (5805 MHz). Channel and Frequencies for 4.9GHz Public Safety: 20 – 4950 Mhz 30 – 4955 Mhz 40 – 4960 Mhz 50 – 4965 Mhz 60 – 4970 Mhz 70 – 4975 Mhz 80 – 4980 Mhz Default channel for 4.9 GHz Public Safety is 20 (4950 MHz). default – Sets the Wi-Fi channel to the default channel for the specified radio interface. auto – The Wi-Fi channel is automatically selected by the system. The automatic selection of the channel is performed only after restarting the unit. After the restart, the unit performs a site survey and then selects the best channel available.

Example: configure interface Dot11Radio 0 channel 6

Permission Level: admin

Related Commands:
configure interface Dot11Radio channel-list
configure sitesurvey
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio channel-list
show sitesurvey

CONFIGURE INTERFACE DOT11RADIO CHANNEL-LIST

Function: Defines the allowable Wi-Fi channels that can be selected for the specified radio interface. The actual frequencies available are dependent on the radio interface (802.11a or 802.11b/g) and the region to which the unit was manufactured. To display all available and allowable channels for the specified radio interface, use the *show interface Dot11Radio channel-list* command.

Command Syntax: **configure interface Dot11Radio** <interface number> **channel-list** {un-allow | allow} {<channel number> | all}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
un-allow | allow	un-allow – Prohibits the specified channel or all channels from use by the specified radio interface. allow – Permits the specified channel or all channels from use by the specified radio interface.
<channel number> | all	Channel and Frequencies IEEE 802.11b/g: 1– 2412 Mhz 2– 2417 Mhz 3– 2422 Mhz 4– 2427 Mhz 5– 2432 Mhz 6– 2437 Mhz 8– 2442 Mhz 9– 2447 Mhz 10– 2452 Mhz 11– 2457 Mhz 12– 2462 Mhz 13– 2467 Mhz
<channel number> | all	Channel and Frequencies for IEEE 802.11a: 34 – 5170 Mhz 36 – 5180 Mhz 38 – 5190 Mhz 40 – 5200 Mhz 42 – 5210 Mhz 44 – 5220 Mhz 46 – 5230 Mhz 48 – 5240 Mhz 108 – 5540 Mhz 112 – 5560 Mhz 116 – 5580 Mhz 120 – 5600 Mhz 124 – 5620 Mhz 128 – 5640 Mhz 132 – 5660 Mhz 136 – 5680 Mhz

	52 – 5260 Mhz	140 – 5700 Mhz
	56 – 5280 Mhz	149 – 5745 Mhz
	60 – 5300 Mhz	153 – 5765 Mhz
	64 – 5320 Mhz	157 – 5785 Mhz
	100 – 5500 Mhz	161 – 5805 Mhz
	104 – 5520 Mhz	165 – 5825 Mhz
	all – Permits or prohibits the all channels from use by the specified radio interface.	

Example: configure interface Dot11Radio 0 channel 6

Permission Level: admin

Related Commands:
configure interface Dot11Radio channel
configure sitesurvey
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio channel-list
show sitesurvey

CONFIGURE INTERFACE DOT11RADIO DISABLE

Function: Disables the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **disable**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.

Example: configure interface Dot11Radio 0 disable

Permission Level: super

Related Commands:
configure interface Dot11Radio enable
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio stats

CONFIGURE INTERFACE DOT11RADIO DISTANCE

Function: Defines the distance between the gateway and the node units for the 802.11a backhaul radio interface. For 802.11b/g access radio interface, this command defines the distance between the node unit and the client. These values are used to optimize the Wi-Fi protocol time intervals for long distance usage on the specified radio interface.
The distance specified for the 802.11a backhaul radio interface is based on the distance between the gateway and the furthest node in the network.

The distance for the 802.11a backhaul radio interface should be specified as follows:

- For a maximum distance of 1200 meters or less, specify 1200.
- For a maximum distances greater than 1200 meters, specify the actual distance.
- Specify the same value for all units in the network.

The distance specified for the 802.11b/g access radio interfaces is based on the distance between the node and the furthest client in the network.

Command Syntax: **configure interface Dot11Radio** <interface number> **distance** <distance>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
distance	Distance in meters: 0 – 8192 Default value for 802.11a interface is 1200 (1200 meters). Default value for 802.11b/g interface is 300 (300 meters).

Example: configure interface Dot11Radio 2 distance 1800

Permission Level: super

Related Commands:
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio stats

CONFIGURE INTERFACE DOT11RADIO DTIM-PERIOD

Function: Configures how frequently the DTIM (Delivery Traffic Indication Message) informs the client in power saving mode if data is waiting to be sent. Each beacon contains a DTIM. The DTIM informs the client if data is waiting and when the next time data is available. The DTIM period defines the number of beacons that are broadcasted between sending data packets.

If the DTIM period is set to four, every fourth beacon contains a DTIM informing the client whether or not data is waiting.

Command Syntax: **configure interface Dot11Radio** <interface number> **dtim-period** <period number>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
period number	DTIM Period: 1-8 The default value is 1.

Example: configure interface Dot11Radio 0 dtim-period 4

Permission Level: admin

Related Commands:

CONFIGURE INTERFACE DOT11RADIO ENABLE

Function: Restarts the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **enable**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.

Example: configure interface Dot11Radio 0 enable

Permission Level: admin

Related Commands:
configure interface Dot11Radio disable
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio stats

CONFIGURE INTERFACE DOT11RADIO ERP-MODE

Function: Enables and disables the ERP mode. The ERP mode is used to reduce collisions when there are b and g clients. This feature is only available on 802.11b/g radio interfaces.

Command Syntax: **configure interface Dot11Radio** <interface number> **erp-mode** {enable | disable}

Command Description:

Parameter	Value
interface number	Access radio interface number. Specify an 802.11b/g radio interface. Depending on the unit, the value can be set to 0 or 1 for units with three interfaces, or only to 0 for units with two interfaces.
enable | disable	enable – Enables ERP mode. disable – Disables ERP mode. The default mode is disable.

Example: configure interface Dot11Radio 0 erp-mode enable

Permission Level: admin

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO FIXED-RATE

Function: Configures the transmission rate on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **fixed-rate** {auto | rate <rate number>}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5 GHz communications and all other radio interfaces are used for 2.4 GHz communications.
auto | rate	rate – Sets the transmission rate to a fixed rate. auto – The transmission rate will be automatically selected by the system. The default value is auto.
rate number	Transmission Rate: 1 – 1 Mbps 2 – 2 Mbps 5 – 5.5 Mbps 6 – 6 Mbps 9 – 9 Mbps 11 – 11 Mbps 12 – 12 Mbps 18 – 18 Mbps 24 – 24 Mbps 36 – 36 Mbps 48 – 48 Mbps

	54 – 54 Mbps

Example: configure interface Dot11Radio 0 fixed-rate 12

Permission Level: super

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO MAX-ASSOC

Function: Defines the maximum number of associated clients supported on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **max-assoc** <maximum associated clients>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
maximum associated clients	Maximum number of associated clients: 1-250 The default value is 250.

Example: **c**onfigure interface Dot11Radio 0 max-assoc 100

Permission Level: super

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO MAX-RATE

Function: Configures the maximum transmission rate on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **max-rate** {<rate number> |
auto}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces.
<rate number> | auto	Sets the maximum transmission rate on the specified radio interface. Maximum Transmission Rate: 1 – 1 Mbps 2 – 2 Mbps 5 – 5.5 Mbps 6 – 6 Mbps 9 – 9 Mbps 11 – 11 Mbps 12 – 12 Mbps 18 – 18 Mbps 24 – 24 Mbps 36 – 36 Mbps 48 – 48 Mbps 54 – 54 Mbps The default value is 36 (36 Mbps).
	Auto – The maximum transmission rate will be automaticallt slected by the system.

Example: configure interface Dot11Radio 0 max-rate 48

Permission Level: super

Related Commands:
configure interface Dot11Radio min-rate
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO MIN-RATE

Function: Configures the minimum transmission rate on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **min-rate** {<rate number> | none | auto}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
<rate number> | auto	Sets the minimum transmission rate on the specified radio interface. Minimum Transmission Rate: 5.5 – 5.5 Mbps 11 – 11 Mbps 12 – 12 Mbps 18 – 18 Mbps 24 – 24 Mbps 36 – 36 Mbps auto – The minimum transmission rate will be automatically selected by the system. The default value is auto.

Example: configure interface Dot11Radio 0 min-rate 36

Permission Level: super

Related Commands:
configure interface Dot11Radio max-rate
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO MODE

Function: Configures the Wi-Fi mode of the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **mode** {a | b | g | mixed | pureg}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
a | b | g | mixed | pureg	Actual available modes are dependent on the radio interface type. a – Enables the specified radio interface to communicate with 802.11a stations. b – Limits the specified access radio interface to communicate only with 802.11b clients. g – Limits the specified access radio interface to communicate only with 802.11g clients. mixed – Enables the specified access radio interface to communicate with 802.11b and 802.11b\g clients. pureg – Limits the specified access radio interface to communicate only at 802.11g rates (6 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps and 54 Mbps – OFDM rates)

Example: configure interface Dot11Radio 0 mode g

Permission Level: admin

Related Commands:
show interface Dot11Radio
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO PREAMBLE-MODE

Function: Configures the preamble mode of the specified access radio interface. The preamble mode identifies the transmitted packet as a Wi-Fi packet. This feature is only available on 802.11b/g radio interfaces.

There are two types of preamble modes:

- Long – The long preamble is 192 microseconds. It is only used with 802.11b packets.
- Short – The short preamble is 96 microseconds. It is used with 802.11b and 802.11g packets.

Command Syntax: **configure interface Dot11Radio** <interface number> **preamble-mode** {long | auto}

Command Description:

Parameter	Value
interface number	Access radio interface number. Specify an 802.11b/g radio interface. Depending on the unit, the value can be set to 0 or 1 for units with three interfaces, or only to 0 for units with two interfaces.
long | auto	long – Sets the preamble mode to long. auto – Sets the preamble mode to auto. The preamble mode will automatically selected between short or long. The default value is long

Example: configure interface Dot11Radio 0 preamble-mode auto

Permission Level: admin

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO PROFILE

Function: Defines the assigned traffic shape profile for the specified radio interface. The profile is only used when the specified radio interface supports mesh service. Changing the assign profile affects the traffic performance.

There are four predefined traffic shape profiles available. The following tables describe these profiles:

Profile 1

Category ID	AIFS	CWMax	CWMin	TXOP
besteffort	3	4	2	1000
background	7	4	2	1000
video	1	3	1	1000
voice	1	2	1	1000

Profile 2

Category ID	AIFS	CWMax	CWMin	TXOP
besteffort	3	6	4	1000
background	7	10	4	1000
video	1	4	3	1000
voice	1	3	2	1000

Profile 3

Category ID	AIFS	CWMax	CWMin	TXOP
besteffort	3	10	6	1000
background	7	10	6	1000
video	1	6	4	1000
voice	1	3	2	1000

Profile 4

Category ID	AIFS	CWMax	CWMin	TXOP
besteffort	3	10	8	1000
background	7	10	8	1000
video	1	6	4	1000
voice	1	3	2	1000

Command Syntax: **configure interface Dot11Radio** <interface number> **profile** <profile number>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
profile number	Traffic shape profile number: 1-4 The default value is 2.

Example: configure interface Dot11Radio 0 profile 3

Permission Level: super

Related Commands:
configure interface Dot11Radio service
show interface Dot11Radio profile

CONFIGURE INTERFACE DOT11RADIO RADAR-DETECTION

Function: Enables or disables radar detection on the specified 802.11a radio interface. When enabled, the unit scans for radar. If radar is detected, the unit selects a channel that does not interfere with the radar.

Command Syntax: **configure interface Dot11Radio** <interface number> **radar-detection** {enable | disable}

Command Description:

Parameter	Value
interface number	Backhaul radio interface number. Specify an 802.11a radio interface. Depending on the unit, the value can be set to 2 for units with three interfaces, or to 1 for units with two interfaces. The last interface is used for 5GHz communications (802.11a) and all other radio interfaces are used for 2.4GHz communications (802.11b/g).
enable | disable	enable – Enables radar detection. disable – Disables radar detection. The default value is disable.

Example: configure interface Dot11Radio 1 radar-detection enable

Permission Level: super

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO RANGE-OPTIMIZATION

Function: Defines the type of optimization that is implemented for the calibration of the RX sensitivity on the specified 802.11b/g radio interface. The calibration can be optimized for maximum range, maximum throughput or normal operation.

When the calibration is optimized for range, the throughput is reduced. When the calibration is optimized for throughput, the range is reduced. This feature is only supported on the NetPoint Pro 6x2.4 and NetPoint Pro 3x2.4 units.

Command Syntax: **configure interface Dot11Radio** <interface number> **range-optimization** <optimization type>

Command Description:

Parameter	Value
interface number	Access radio interface number. Specify an 802.11b/g radio interface. Depending on the unit, the value can be set to 0 or 1 for units with three interfaces, or only to 0 for units with two interfaces.
optimization type	Type of optimization: range – Calibrates the RX sensitivity for maximum range. throughput – Calibrates the RX sensitivity for maximum throughput. none – Calibrates the RX sensitivity for normal operation. The default value is normal.

Example: configure interface Dot11Radio 1 range-optimization range

Permission Level: super

Related Commands:
configure interface Dot11Radio sensitivity
show interface Dot11Radio params
show interface wifi-load-radio
show interface wifi-stats
show interface Dot11Radio range-optimization

CONFIGURE INTERFACE DOT11RADIO RTS

Function: Configures the threshold packet size for implementing RTS. Packets larger than the RTS threshold will be transmitted using RTS. The lower the threshold the more frequently the system uses RTS.

Command Syntax: **configure interface Dot11Radio** <interface number> **rts** <threshold number>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
threshold number	RTS threshold value (byte): 1-2346 The default value is 2346 (2346 bytes).

Example: configure interface Dot11Radio 0 rts 1024

Permission Level: admin

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO SENSITIVITY

Function: Configures noise floor level in dBm for the specified radio interface. All signals below the sensitivity setting are assumed to be noise and the unit does not recognize this signal.

Command Syntax: **configure interface Dot11Radio** <interface number> **sensitivity** <level number>

Command Description:

Parameter	Value
interface number	Radio interface number. Specify a radio interface. Depending on the unit, the value can be set to 0, 1 or 2.
level number	Sensitivity Level (dBm): (-101) - (-77) – For xRF radio interface (-96) - (-72) – For non-xRF 802.11b/g radio interface (-89) - (-60) – For 802.11a radio interface auto – Enables automatic noise floor setting. The default value is auto

Example: configure interface Dot11Radio 0 sensitivity -101

Permission Level: admin

Related Commands:
show interface Dot11Radio params
show interface wifi-load-radio
show spectrum-management clear-count-percent

CONFIGURE INTERFACE DOT11RADIO SERVICE

Function: Configures the type of service the specified radio interface supports.

Command Syntax: **configure interface Dot11Radio** <interface number> **service** {access | backhaul}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
access | backhaul	access – Supports only access services - no mesh service. backhaul – Supports only mesh service - no access service.

Example: configure interface Dot11Radio 0 service access

Permission Level: admin

Related Commands:
show interface Dot11Radio
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO SSID

Function: Configures the SSID for the specified access radio interface. It attaches and detaches an existing SSID from the interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **ssid** <index number> {add | remove}

Command Description:

Parameter	Value
interface number	Access radio interface number. Specify an 802.11b/g radio interface. Depending on the unit, the value can be set to 0 or 1 for units with three interfaces, or only to 0 for units with two interfaces.
index number	SSID index number: 1-8
add | remove	add – Attaches an existing SSID to the interface. remove – Detaches an existing SSID to the interface.

Example: configure interface Dot11Radio 0 ssid 4 add

Permission Level: admin

Related Commands:
show interface ssids
show ssid params

CONFIGURE INTERFACE DOT11RADIO TXPWRATTN

Function: Configures the transmission power attenuation. It decreases the transmitted power by the specified dB value.

Command Syntax: **configure interface Dot11Radio** <interface number> **txPwrAttn** <pwr>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
pwr	Transmission Power Attenuation (dB): 0-32 The default value is 0 (0 dB).

Example: configure interface Dot11Radio 1 txPwrAttn 2

Permission Level: admin

Related Commands:
show interface Dot11Radio params

CONFIGURE INTERFACE DOT11RADIO WME

Function: Configures the WME quality of service (QoS) parameters for each category on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **wme** {voice | video | besteffort | background} [cw_min <cw min number>] [cw_max <cw max number>] [aifs <slots number>] [txop-limit <time limit>]

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
voice | video | besteffort | background	voice – Specifies the voice WME category. video – Specifies the video WME category. besteffort – Specifies the best-effort WME category. background – Specifies the background WME category.
cw min number	Minimum contention window: 0-15 Default values: For voice – 2 For video – 3 For besteffort – 4 For background – 4 This parameter is optional.
cw max number	Maximum contention window: 0-15 Default values: For voice – 3 For video – 4 For besteffort – 10 For background – 10 This parameter is optional.
slots number	AIFS time period in number of slots: 0-15 Default values: For voice – 2 For video – 2 For besteffort – 3 For background – 7 This parameter is optional.
time limit	Transmission Opportunity Duration (microseconds): 0-8192 Default values: For voice – 1504 (1.504 msec) For video – 3008 (3.008 msec) For besteffort – 0 For background – 0 This parameter is optional.

Example: configure interface Dot11Radio 0 wme voice aifs 1

Permission Level: super

Related Commands:
configure interface Dot11Radio wme-enable
show interface Dot11Radio params
show interface Dot11Radio wme

CONFIGURE INTERFACE DOT11RADIO WME-ENABLE

Function: Enables or disables WME on the specified radio interface.

Command Syntax: **configure interface Dot11Radio** <interface number> **wme-enable** {true | false}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
true | false	true – Enables WME. false – Disables WME.

Example: configure interface Dot11Radio 0 wme-enable true

Permission Level: super

Related Commands:
configure interface Dot11Radio wme
show interface Dot11Radio params

CONFIGURE INTERFACE FASTETHERNET ADD-VLAN-TAG

Function: Adds VLAN tagging for traffic on the FastEthernet interface. This command can also change the VLAN tag ID. To remove VLAN tagging on the FastEthernet interface set the VLAN tag ID to 0. This command is only relevant for mesh nodes.

Command Syntax: **configure interface FastEthernet** <interface number> **add-vlan-tag** <vlan number>

Command Description:

Parameter	Value
interface number	FastEthernet interface number. In this version the interface is always set to 0.
vlan number	VLAN tag index number: 0-4095 To remove VLAN tagging set to 0. The default value is 0.

Example: configure interface FastEthernet 0 add-vlan-tag 7

Permission Level: super

Related Commands:
configure interface FastEthernet auto-negotiation
show interface FastEthernet

CONFIGURE INTERFACE FASTETHERNET AUTO-NEGOTIATION

Function: Configures the FastEthernet interface. This command allows you to configure the interface manually or by auto-negotiation.

Command Syntax: **configure interface FastEthernet** <interface number> **auto-negotiation** enable

configure interface FastEthernet <interface number> **auto-negotiation** disable speed {10 | 100} {half-duplex | full-duplex}

Command Description:

Parameter	Value
interface number	FastEthernet interface number. In this version the interface is always set to 0.
enable | disable	enable – Auto-negotiation is enabled. No additional parameters need to be defined for the FastEthernet interface. disable – Auto-negotiation is disabled. The speed and the duplex mode can be configured.
10 | 100	Defines the speed of the FastEthernet interface: 10 – 10 Mbps 100 – 100 Mbps
half-duplex | full-duplex	Defines the Duplex Mode: half-duplex – The FastEthernet interface is set to half-duplex. full-duplex – The FastEthernet interface is set to full-duplex.

Example: configure interface FastEthernet 0 auto-negotiation disable speed 100 full-duplex

Permission Level: admin

Related Commands:
configure interface FastEthernet add-vlan-tag
show interface FastEthernet

CONFIGURE IP DEFAULT-GATEWAY

Function: Configures the default gateway. This is only relevant if the IP address has been configured manually. It is not relevant if you use a DHCP server. This command should only be used when communicating with the unit via the console port.

Command Syntax: **configure ip default-gateway** {<ip ip-address> | disable}

Command Description:

Parameter	Value
ip ip-address	IP address of the default gateway.

disable	Deletes the default gateway configuration.

Example: configure ip default-gateway 192.168.250.1

Permission Level: admin

Related Commands:
configure ip vlan
show ip address

CONFIGURE IP MTU

Function: Defines the Maximum Transmission Unit (MTU) of the IP packet. This command is used to define the maximum management commands IP packet size. The MTU command should be used when external equipment connected to the network cannot support the default MTU size of 1500 bytes.

Command Syntax: **configure ip mtu** <mtu>

Command Description:

Parameter	Value
mtu	Size of the MTU (bytes): 128-1500 The default value is 1500 bytes.

Example: configure ip mtu 128

Permission Level: admin

Related Commands:
show ip params

CONFIGURE IP SSH

Function: Enables the SSH (Secure Shell) service. When enabled, SSH authentication is required to connect to the device for management access. This is enabled by default.

Command Syntax: **configure ip ssh**

Command Description:

Parameter	Value
None	

Example: configure ip ssh

Permission Level: super

Related Commands:
configure ip ssh authentication
configure ip ssh authentication-retries
configure ip ssh disable
configure ip vlan
show ip params
show ip ssh-public-keys

CONFIGURE IP SSH AUTHENTICATION

Function: Configures the SSH (Secure Shell) authentication method for the SSH management access connection.

Command Syntax: **configure ip ssh authentication** {password | publicKey}

Command Description:

Parameter	Value
password | publicKey	SSH authentication method: password – Password authentication publicKey – Public key authentication

Example: configure ip ssh authentication password

Permission Level: admin

Related Commands:
configure ip ssh
configure ip ssh authentication-retries
configure ip ssh crypto key generate
configure ip ssh crypto key public-key
configure ip vlan
show ip params
show ip ssh-public-keys

CONFIGURE IP SSH AUTHENTICATION-RETRIES

Function: Configures the number of authentication retries for the SSH (Secure Shell) management access connection.

Command Syntax: **configure ip ssh authentication-retries** <retries number>

Command Description:

Parameter	Value
retries number	Number of authentication retries: 1-5 The default value is 3.

Example: configure ip ssh authentication-retries 5

Permission Level: admin

Related Commands:
configure ip ssh
configure ip ssh authentication
configure ip ssh crypto key generate
configure ip ssh crypto key public-key
configure ip ssh disable
configure ip vlan
show ip params
show ip ssh-public-keys

CONFIGURE IP SSH CRYPTO KEY GENERATE

Function: Configures and generates the cryptography key for the SSH (Secure Shell) management access connection.

Command Syntax: **configure ip ssh crypto key generate** {rsa | dsa} [<length number>]

Command Description:

Parameter	Value
rsa | dsa	rsa – Generates the RSA key. dsa – Generates the DSA key.
length number	Configures the key length in bits: 512-2048 This parameter is optional. The default value is 1024.

Example: configure ip ssh crypto key generate rsa

Permission Level: admin

Related Commands:
configure ip ssh
configure ip ssh authentication
configure ip ssh authentication-retries
configure ip ssh crypto key public-key
configure ip ssh disable
configure ip vlan
show ip params
show ip ssh-public-keys

CONFIGURE IP SSH CRYPTO KEY PUBLIC-KEY

Function: Configures the public authentication key for the SSH (Secure Shell) management access connection.

Command Syntax: **configure ip ssh crypto key public-key** {add {ssh-dss | ssh-rsa} <key string> [<key string>] owner <owner string> | remove <owner string>

Command Description:

Parameter	Value
add | remove | remove-all	add – Adds a new authenticated public key. remove – Deletes the user and public key from the list. remove-all – Deletes all the users and public keys from the list.
ssh-dss | ssh-rsa	Defines the key type: ssh-dss – Defines the new public key as a DSA key type. ssh-rsa – Defines the new public key as an RSA key type.
key string	A string value that defines the key string of the public key. Each string value can be up to 256 characters and is case sensitive. Up to two string values can be specified and a space must be entered between the two string values.
owner string	A string value that defines the owner name of the public key. The value can be up to 32 characters and is case sensitive.

Example: configure ip ssh crypto key public key add ssh-dss PublicKey owner Netronics

Permission Level: admin

Related Commands:
configure ip ssh
configure ip ssh authentication
configure ip ssh authentication-retries
configure ip ssh disable
configure ip ssh crypto key generate
configure ip vlan
show ip params
show ip ssh-public-keys

CONFIGURE IP SSH DISABLE

Function: Disables the SSH (Secure Shell) service. SSH is enabled by default.

Command Syntax: **configure ip ssh disable**

Command Description:

Parameter	Value
None	

Example: configure ip ssh disable

Permission Level: super

Related Commands:
configure ip ssh
configure ip ssh authentication

configure ip ssh authentication-retries
configure ip vlan
show ip params
show ip ssh-public-keys

CONFIGURE IP TELNET

Function: Enables Telnet management access connection. Telnet is enabled by default.

Command Syntax: **configure ip telnet**

Command Description:

Parameter	Value
None	

Example: configure ip telnet

Permission Level: admin

Related Commands:
configure ip telnet authentication-retries
configure ip telnet disable
show ip params

CONFIGURE IP TELNET AUTHENTICATION-RETRIES

Function: Defines the number of authentication retries.

Command Syntax: **configure ip telnet authentication-retries** <retries number>

Command Description:

Parameter	Value
retries number	Number of authentication retries: 1-5

Example: configure ip telnet authentication-retries 3

Permission Level: admin

Related Commands:
configure ip telnet
configure ip telnet disable
show ip params

CONFIGURE IP TELNET DISABLE

Function: Disables Telnet management access connection. Telnet is enabled by default.

Command Syntax: **configure ip telnet disable**

Command Description:

Parameter	Value
None	

Example: configure ip telnet disable

Permission Level: admin

Related Commands:
configure ip telnet
configure ip telnet authentication-retries
show ip params

CONFIGURE IP VLAN

Function: Configures the management IP address and VLAN ID.

Command Syntax: **configure ip vlan** {<vlan number> | none} {<address ip-address> [<mask ipaddress>] | dhcp} [default-gateway <gateway ip-address>]

Command Description:

Parameter	Value
<vlan number> | none	VLAN index number: 1-4095 Specify none to set the VLAN ID to 0 with no VLAN tagging.
address ip-address	IP address of the management VLAN.
mask ip-address	Subnet Mask of the management VLAN. This parameter is optional when specifying the IP address. The default value is 255.0.0.0.
dhcp	Defines that the DHCP server automatically assigns the IP address.
gateway ip-address	IP address of the default gateway.

Example: configure ip vlan 6 192.168.250.1

Permission Level: admin

Related Commands:
configure ip default-gateway
show ip address

CONFIGURE LOGGING DEST CLI

Function: Configures the maximum level of messages in the log that are sent to the CLI. The level defines the level of details in the log that are sent.

Command Syntax: **configure logging dest cli** {level <level> | enable | disable}

Command Description:

Parameter	Value
level | enable | disable	level – Configures the logging level that are sent to the CLI. enable – Logging has been enabled and logs are sent to the CLI. disable – Logging has been disabled and no logs are sent to the CLI. The default value is disable.
level	The level that represents the level of details sent to the CLI: emergency – Only emergency messages are sent. alert – Emergency and alert messages are sent. critical – Emergency, alert and critical messages are sent. error – Emergency, alert, critical and error messages are sent. The default value is emergency.

Example: configure logging dest cli level critical

Permission Level: super

Related Commands:
show logging destinations

CONFIGURE LOGGING DEST HISTORY

Function: Configures the maximum level of messages in the log that are sent to the history stored in the RAM. The level defines the level of details in the log that are sent. The configuration of the history is also the configuration of the system log.

Command Syntax: **configure logging dest history** {level <level> | enable | disable}

Command Description:

Parameter	Value
level | enable | disable	level – Configures the logging level that are sent to the history. enable – Logging has been enabled and logs are sent to the history. disable – Logging has been disabled and no logs are sent to the history. The default value is disable.
level	The level that represents the level of details sent to the CLI: emergency – Only emergency messages are sent. alert – Emergency and alert messages are sent. critical – Emergency, alert and critical messages are sent. error – Emergency, alert, critical and error messages are sent. The default value is emergency.

Example: configure logging dest history level critical

Permission Level: super

Related Commands:
show logging destinations
show logging history
show messages

CONFIGURE LOGGING DEST RS232CONSOLE

Function: Configures the maximum level of messages in the log that are sent to the console. The level defines the level of details in the log that are sent.

Command Syntax: **configure logging dest rs232console** {level <level> | enable | disable}

Command Description:

Parameter	Value
level | enable | disable	level – Configures the logging level that are sent to the console. enable – Logging has been enabled and logs are sent to the CLI. disable – Logging has been disabled and no logs are sent to the console. The default value is disable.
level number	The level number that represents the level of details sent to the console: emergency – Only emergency messages are sent. alert – Emergency and alert messages are sent. critical – Emergency, alert and critical messages are sent. error – Emergency, alert, critical and error messages are sent. The default value is emergency.

Example: configure logging dest rs232console level critical

Permission Level: super

Related Commands:
show logging destinations

CONFIGURE LOGGING MODULE

Function: Configures the log level of the modules. The level defines the level of details saved in the log.

Command Syntax: **configure logging module** {level <level> | enable | disable}}

Command Description:

Parameter	Value
level | enable | disable	level – Configures the level of details that are recorded for the specified module. enable – Logging has been enabled and logs are sent to the CLI. disable – Logging has been disabled and no logs are recorded for the specified module. The default value is level.

level number	The level number that represents the level of details saved in the log: emergency – Only emergency messages are sent. alert – Emergency and alert messages are sent. critical – Emergency, alert and critical messages are sent. error – Emergency, alert, critical and error messages are sent. The default value is error.

Example: configure logging module level critical

Permission Level: super

Related Commands:
show logging modules-level

CONFIGURE LOGGING SYSLOG IP-ADDRESS

Function: Configures a host to receive the module log. Defines the host IP address, port and log level. The level defines the level of details saved in the log.

Command Syntax: **configure logging syslog ip-address** <host ipaddress> [port <port number>] {level <level> | enable | disable}

Command Description:

Parameter	Value
host ipaddress	IP address of the host. The default value is 127.0.0.1.
port number	Number of the port in the host: 1-65535 This parameter is optional. The default value is 514.
level | enable | disable	level – Configures the logging level that are sent to the CLI. enable – Logging has been enabled and logs are sent to the CLI. disable – Logging has been disabled and no logs are sent to the CLI. The default value is disable.
level	The level that represents the level of details sent to the CLI: emergency – Only emergency messages are sent. alert – Emergency and alert messages are sent. critical – Emergency, alert and critical messages are sent. error – Emergency, alert, critical and error messages are sent. The default value is emergency.

Example: configure logging syslog ip-address 1.1.1.3 port 514 enable

Permission Level: super

Related Commands:
show logging host
show logging destinations

CONFIGURE MAC-FILTER LIST ADD-MAC

Function: Adds a MAC address to an existing MAC Address list. This list is used to permit or deny access to a specified SSID.

Command Syntax: **configure mac-filter list** <index number> **add-mac** <macaddr>

Command Description:

Parameter	Value
index number	Index number of an existing MAC filter list: 1-16
macaddr	MAC address of the client to be added to the list.

Example: mac-filter list 3 add-mac 00:14:06:11:00:00

Permission Level: super

Related Commands:
configure mac-filter list new
configure mac-filter list remove-mac
show mac-filter indices
show mac-filter list

CONFIGURE MAC-FILTER LIST NEW

Function: Creates a new white or black MAC filter list. This list is used to permit or deny client access to the unit.

When creating a new list, an list index number must be specified for this list. Use this index number to use, configure or delete the list. To display all filter list indices use the *show mac-filter indices* command.

Command Syntax: **configure mac-filter list** <index number> **new** <name string> type {white | black}

Command Description:

Parameter	Value
index number	Index number of the new MAC filter list: 1-16
name string	A string value that defines the name of the new filter list. The value is case sensitive and can be up to 32 characters.
white | black	Type of filter list: white – Filter list can be used to permit client access. black – Filter list can be used to deny client access.

Example: configure mac-filter list 2 new WhiteList2 type white

Permission Level: super

Related Commands: mac-filter

configure mac-filter list remove-list
configure mac-filter list add-mac
configure mac-filter list remove-mac
show mac-filter indices

CONFIGURE MAC-FILTER LIST REMOVE-LIST

Function: Deletes the specified MAC filter list. Specify the filter list by its index number. To display all filter list indices use the *show mac-filter indices* command.

Command Syntax: **configure mac-filter list** <index number> **remove-list**

Command Description:

Parameter	Value
index number	Index number of an existing MAC filter list: 1-16

Example: configure mac-filter list 2 remove-list 2

Permission Level: super

Related Commands:
configure mac-filter list new
show mac-filter indices

CONFIGURE MAC-FILTER LIST REMOVE-MAC

Function: Deletes a MAC address from an existing MAC Address list. This list is used to permit or deny access to a specified SSID.

Command Syntax: **configure mac-filter list** <index number> **remove-mac** <macaddr>

Command Description:

Parameter	Value
index number	Index number of an existing MAC address list: 1-16
macaddr	MAC address of the client to be deleted from the list.

Example: configure mac-filter list 3 remove-mac 00:14:06:11:00:00

Permission Level: super

Related Commands:
configure mac-filter list new
configure mac-filter list add-mac
show mac-filter indices
show mac-filter list

CONFIGURE MESH ADVERTISE

Function: Configures advertising this unit as a candidate for the next hop in the mesh network. It defines whether the unit that can be used to establish a connection to get access to the Mesh-Gateway.

Command Syntax: **configure mesh advertise** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables advertising, which defines this unit as a candidate for the next hop in the mesh network. disable – Disables advertising. The default value is enable.

Example: configure mesh advertise disable

Permission Level: admin

Related Commands:
configure mesh interface
configure mesh mode
show mesh params

CONFIGURE MESH CONNECTIVITY_TEST

Function: Configures the mesh-gateway connectivity test. This test is typically used to check connectivity to the Internet. This test is only applied when the unit is defined as the Mesh-Gateway. The test performs a ping command every 10 seconds. A failure mode occurs after 10 ping commands fail consecutively.
If the connectivity test fails, the mesh mode will automatically switch to the node mode. When the connection is restored, the mesh mode will automatically return to the gateway mode.
To display the current status of the mesh-gateway connectivity test, use the *show mesh params* command.

Command Syntax: **configure mesh connectivity_test** target_host {<target> | none}
configure mesh connectivity_test {enable | disable}
configure mesh connectivity_test {{enable | disable} [{target_host {<target string(0-64)> | none } [target_host2 {<target string(0-64)> | none}] [timeout<timeout integer>] [retry<retry integer>] [interval<interval integer>]}]}

Command Description:

Parameter	Value
target_host	Configures the host target for the connectivity test.
<target> | none	Target Definition. Specify the target IP address or host name. The name can be up to 64 characters. Specify none to only check the internal Ethernet port. The default value is none.
enable | disable	enable – Enables the mesh-gateway connectivity test. This is only active when the mesh mode is set to gateway.

	disable – Disables the mesh-gateway connectivity test. The default value is disable.

Example: configure mesh connectivity_test enable

Permission Level: admin

Related Commands:
configure mesh mode
show mesh params

CONFIGURE MESH INTERFACE DOT11RADIO WDS

Function: Enables or disables WDS mode on the specified radio interface. WDS services are only available when the radio interface is in access mode.

Command Syntax: **configure mesh interface Dot11Radio** <interface number> **wds** {enable | disable}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
enable | disable	enable – Enables WDS. disable – Disables WDS. The default value is disable.

Example: configure mesh interface Dot11Radio 0 wds enable

Permission Level: super

Related Commands:
configure mesh interface Dot11Radio wds-peer
configure mesh interface Dot11Radio wds-privacy
show mesh interface wds-params
show mesh route
show mesh wds-peer-list

CONFIGURE MESH INTERFACE DOT11RADIO WDS-PEER

Function: Defines the associated peers of a static mesh network for the specified radio interface. Each unit must define the peers to which it is directly communicating.

To display the current mesh peers associated with the unit, use the *show mesh route* command**.**

Note: Caution should be used when configuring the mesh peers manually. Improper configuration can result with network loops.

Command Syntax: Configure mesh interface Dot11Radio <interface number> wds-peer <address macaddress> [remove]

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
macaddress	MAC address of the peer to be added or removed from the list.
remove	remove – Removes a peer from the list of associated peers by deleting its MAC address from the list.

Example: configure mesh interface Dot11Radio 0 wds-peer 00:14:06:11:00:00

Permission Level: super

Related Commands:
configure mesh interface Dot11Radio wds
configure mesh interface Dot11Radio wds-privacy
show mesh interface wds-params
show mesh route
show mesh wds-peer-list

CONFIGURE MESH INTERFACE DOT11RADIO WDS-PRIVACY

Function: Configures the WDS privacy on the specified radio interface.

Command Syntax: **configure mesh interface Dot11Radio** <interface number> **wds-privacy** none

configure mesh interface Dot11Radio <interface number> **wds-privacy** wep key {40 | 104} <key hex>
configure mesh interface Dot11Radio <interface number> **wds-privacy** AES passphrase <passphrase string>

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
none | wep key| AES passphrase	Defines the WDS privacy method: none – WDS is configured without any encryption. wep key – Configures WEP encryption on the selected WDS interface. The WEP key must be defined. AES passphrase – Configures WPA AES encryption on the selected WDS interface The WPA passphrase must be defined.

40 | 104	Defines the length of the WEP key: 40 – 40 bit key 104 – 104 bit key
key hex	Defines the key used for WEP security. For a 40 bit key specify a 5 octet string in hexadecimal format. (Example: 01:23:45:67:89) For a 104 bit key specify a 13 octet string in hexadecimal format. (Example: 01:23:45:67:89:01:23:45:67:89:01:23:45)
passphrase string	Defines the passphrase used during the key handshake process for AES encryption. The value is case sensitive and can be from 8 to 63 characters.

Example: configure mesh interface Dot11Radio 0 wds-privacy wep key 40 01:23:45:67:89

Permission Level: super

Related Commands:
configure mesh interface Dot11Radio wds
configure mesh interface Dot11Radio wds-peer
show mesh interface wds-params
show mesh route
show mesh wds-peer-list

CONFIGURE MESH FILTER-LIST

Function: Configures and enables mesh filtering. It is used to limit the structure of the mesh. Mesh filtering defines a list of MAC addresses that can be denied or permitted connectivity to the mesh interface.

Command Syntax: **configure mesh filter-list** mac <macaddress> {add | remove}
configure mesh filter-list type {permit | deny}
configure mesh filter-list {enable | disable}

Command Description:

Parameter	Value
mac	MAC address of the peer to be added or removed from the mesh filter list. The value is displayed in the following syntax (XX:XX:XX:XX:XX:XX).
add | remove	add – Adds the specified MAC address to the mesh filter list. remove – Removes the specified MAC address from the mesh filter list.
permit | deny	permit – Defines the mesh filter list as a white MAC filter list. These MAC addresses will be permitted connectivity to the mesh interface. deny – Defines the mesh filter list as a black MAC filter list. These MAC addresses will be denied connectivity to the mesh interface.
enable | disable	enable – Enables mesh filtering. disable – Disables mesh filtering. The default value is disable.

Example: configure mesh filter-list mac 00:14:06:11:00:00 add
configure mesh filter-list type permit

configure mesh filter-list enable

Permission Level: super

Related Commands:
configure mesh interface
configure mesh mode
show mesh filter-list
show mesh params

CONFIGURE MESH MODE

Function: Configures the unit as a Mesh-Gateway or Mesh-Node.

Command Syntax: **configure mesh mode** {gateway | node}

Command Description:

Parameter	Value
gateway | node	gateway – Defines the unit as the Mesh-Gateway. node – Defines the unit as a Mesh-Node. The default value is node.

Example: configure mesh mode gateway

Permission Level: admin

Related Commands:
configure mesh interface
show mesh params

CONFIGURE MESH NETWORK-ID

Function: Defines the mesh network id associated with the unit. All units in a single mesh network have the same specified network id.

Command Syntax: **configure mesh network-id** <network-id>

Command Description:

Parameter	Value
network-id	A string value that defines the name of the mesh network. The value is case sensitive and can be from 8 to 16 characters.

Example: configure mesh network-id private

Permission Level: admin

Related Commands:
configure mesh interface

configure mesh mode
show mesh params

CONFIGURE MESH PRIVACY

Function: Configures the mesh privacy. This is used to give security for the data transmitted in the mesh network.

Command Syntax: **configure mesh privacy** none
configure mesh privacy wep key {40 | 104} <key hex>
configure mesh privacy AES passphrase <passphrase string>

Command Description:

Parameter	Value
none | wep | AES	Defines the mesh privacy method: none – Mesh works without security. wep key – Connects to other NetPoint Pro 6x2.4 and NetPoint Pro 3x2.4 units using WEP security. The WEP key must be defined. AES passphrase – Connects to other NetPoint Pro 6x2.4 and NetPoint Pro 3x2.4 units using WPA security. The WPA passphrase must be defined.
40 | 104	Defines the length of the WEP key: 40 – 40 bit key 104 – 104 bit key
key hex	Defines the key used for WEP security. For a 40 bit key specify a 5 octet string in hexadecimal format. (Example: 01:23:45:67:89) For a 104 bit key specify a 13 octet string in hexadecimal format. (Example: 01:23:45:67:89:01:23:45:67:89:01:23:45)
passphrase string	Defines the passphrase used during the key handshake process for AES encryption. The value is case sensitive and can be from 8 to 63 characters.

Example: configure mesh privacy wep key 40 01:23:45:67:89

Permission Level: admin

Related Commands:
configure mesh interface
configure mesh mode
show mesh params

CONFIGURE MESH REROUTE-NOW

Function: Scans and connects to the best available next hop to establish a connection to get access to the Mesh-Gateway. This command temporarily disables its connections to all peers prior to connecting to the best available next hop.

Command Syntax: **configure mesh reroute-now**

Command Description:

Parameter	Value
None	

Example: configure mesh reroute-now

Permission Level: admin

Related Commands:
configure mesh interface
configure mesh mode
show mesh params

CONFIGURE MESH STAND-ALONE

Function: Configures the mesh stand-alone mode. When the stand-alone mode is active, the device acknowledges that it does not have communications with the gateway and disables access to the clients.

Command Syntax: **configure mesh stand-alone** {enable | disable | force-stay}

Command Description:

Parameter	Value
enable | disable | force-stay	enable – Enables the mesh stand-alone mode. If the device loses communications with the gateway, the device changes its stand-alone status to an active state. disable – Disables the mesh stand-alone mode. If the stand-alone status is active, it changes its stand-alone status to an inactive state. force-stay – If the device loses communications with the gateway, the device changes its stand-alone status to an active state. When communications returns to the gateway, the stand-alone status stays in the active state. The default mode is enable.

Example: configure mesh stand-alone disable

Permission Level: super

Related Commands:
configure mesh stand-alone-passphrase
configure mesh interface
configure mesh mode
configure mesh stand-alone-passphrase
show mesh params
show mesh stand-alone

CONFIGURE MESH STAND-ALONE-PASSPHRASE

Function: Configures the mesh stand-alone SSID pre-shared key.

Command Syntax: **configure mesh stand-alone-passphrase** <passphrase string>

Command Description:

Parameter	Value
passphrase string	Defines the passphrase used during the key handshake process. The value is case sensitive and can be from 8 to 63 characters.

Example: configure mesh stand-alone-passphrase password

Permission Level: admin

Related Commands:
configure mesh stand-alone
configure mesh interface
configure mesh mode
configure mesh stand-alone
show mesh params
show mesh stand-alone

CONFIGURE MESH TRUNK

Function: Enables and disables the mesh trunk mode.

Command Syntax: **configure mesh trunk** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables the mesh trunk mode. disable – Disables the mesh trunk mode. The default mode is enable.

Example: configure mesh trunk enable

Permission Level: admin

Related Commands:
show mesh params

CONFIGURE NTP

Function: Configures the Network Time Protocol (NTP) client on the unit.

Command Syntax: **configure ntp host** {<ipaddress> | <hostname>} **interval** <time>
configure ntp host {enable | disable}

Command Description:

Parameter	Value
ipaddress	IP address of the NTP server.
hostname	Host name of the NTP server.
time	Defines the time interval used to synchronize the unit's system clock with the NTP server (seconds). 1 – 2147483647

enable | disable	enable – Enables the NTP daemon. disable – Disables the NTP daemon. The default value is disable.

Example: configure ntp host 192.168.0.1 interval 10

Permission Level: super

Related Commands:
show ntp

CONFIGURE PINGWD

Function: Configures and enables the ping watchdog feature. When enabled, the unit sends a ping to a specified IP address. If there is no response to the ping the unit reboots.

This feature is used to confirm communications during a reconfiguration of the unit. If communications is lost due to a configuration error, the unit will reboot and restore a valid configuration.

The configuration of this feature is not saved to the startup configuration. It is recommended that you configure this feature prior to any configuration updates to the unit.

Command Syntax: **configure pingwd ip** <ip address> **timeout** <time>
configure pingwd {enable | disable}
ip <ip address> **timeout** <time>

Command Description:

Parameter	Value
ip address	IP address of the remote host.
time	Defines the time interval that the unit sends the ping packets (seconds). 1 – 3600 The default value is 10 seconds.
enable | disable	enable – Enables the ping watchdog feature. disable – Disables the ping watchdog feature. The default value is disable.

Example: configure pingwd ip 192.168.0.2 timeout 10

Permission Level: super

Related Commands:
show pingwd

CONFIGURE PRIVACY WEP SSID AUTH-TYPE

Function: Configures the WEP authentication algorithm to a specific SSID.

Command Syntax: **configure privacy wep ssid** <index number> **auth-type** {open | shared}

Command Description:

Parameter	Value
index number	SSID index number. 1-8
open | shared	Defines the authentication type: open – Open system authentication. shared – Shared key authentication.

Example: configure privacy wep ssid 3 auth-type open

Permission Level: admin

Related Commands:
configure privacy wep ssid index
configure ssid
show ssid params
show privacy wep
show privacy wep params

CONFIGURE PRIVACY WEP SSID DEFAULT-KEY

Function: Configures the default WEP key index to a specific SSID.

Command Syntax: **configure privacy wep ssid** <index number> **default-key** <key index>

Command Description:

Parameter	Value
index number	SSID index number. 1-8
key index	Defines the WEP key index number. 1-4 In this version the index number is always set to 1.

Example: configure privacy wep ssid 3 default-key 1

Permission Level: admin

Related Commands:
configure privacy wep ssid index
configure ssid
show ssid params
show privacy wep
show privacy wep params

CONFIGURE PRIVACY WEP SSID INDEX

Function: Configures the WEP key. It defines a WEP key to a specific SSID.

Command Syntax: **configure privacy wep ssid** <index number> **index** <key index> {40 | 104} <key hex>

Command Description:

Parameter	Value
index number	SSID index number. 1-8
key index	Defines the WEP key index number. 1-4 In this version the index number is always set to 1.
40 | 104	Defines the length of the WEP key: 40 – 40 bit key 104 – 104 bit key
key hex	For a 40 bit key specify a 5 octet string in hexadecimal format. (Example: 01:23:45:67:89) For a 104 bit key specify a 13 octet string in hexadecimal format. (Example: 01:23:45:67:89:01:23:45:67:89:01:23:45)

Example: configure privacy wep ssid 3 index 1 40 01:23:45:67:89

Permission Level: admin

Related Commands:
configure privacy wep ssid default-key
configure ssid
show ssid params
show privacy wep
show privacy wep params

CONFIGURE PRIVACY WPA

Function: Configures the WPA privacy for a specific SSID.

Command Syntax: **configure privacy wpa** ssid <ssid index> [passphrase <passphrase string>] [key-mngmnt {eap | psk}]
configure privacy wpa gtk-interval <interval number>
configure privacy wpa data-encryption {tkip | aes | both}
configure privacy wpa protocol {wpa1 | wpa2 | wpa2only}
configure privacy wpa preauthentication {enable | disable}

Command Description:

Parameter	Value
ssid index	An existing SSID index number: 1-8
passphrase string	Defines the passphrase used during the key handshake process for WPA encryption. The value is case sensitive and can be from 8 to 63 characters.
eap | psk | both	Defines the key management type: eap – Extended Authorization Protocol

	psk – Pre-Shared Key both – Enables both AES and TKIP
interval number	Defines the GTK (Group Temporal Key) interval in seconds. It defines the time interval the unit initiates a GTK change. 30-42949672 The default value is 3600 (1 hour).
tkip | aes	Defines the data encryption type: tkip – Temporary Key Integrity Protocol aes – Advanced Encryption Standard (AES/CCMP) The default value is tkip.
wpa1 | wpa2 | wpa2only	Defines the WPA protocol type: wpa1 – Supports WPA1 only. wpa2 – Supports WPA1 and WPA2. wpa2only – Supports WPA2 only, without support for WPA1. The default value is wpa2.
enable | disable	WPA2 Preauthentication: enable – Enables WPA2 Preauthentication disable – Disables WPA2 Preauthentication The default value is disable. To enable WPA2 Preauthentication, the WPA protocol must support WPA2.

Example: configure privacy wpa ssid 1 key-mngmnt psk

Permission Level: admin

Related Commands:
show privacy wpa

CONFIGURE RADIUS

Function: Configures communications with the Radius server. This command is used to configure the parameters required to communicate with the primary and the secondary Radius servers. For each server the authentication and accounting parameters can be configured to permit access to the Radius servers.
The accounting services monitors and records the number of packets transmitted and received by each authenticated client.
To implement Radius server services the WPA-EAP security must be configured.

Command Syntax: **configure radius** {accounting | authentication} ssid <ssid index> priority <priority number> [host <address ipaddress>] [port <port number>] key <secret string>
configure radius {accounting | authentication} ssid <ssid index> priority <priority number> remove

Command Description:

Parameter	Value
authentication | accounting	authentication – Configures parameters to communicate with the authentication services on the Radius server. accounting – Configures parameters to communicate with the accounting services on the Radius server.
ssid index	An existing SSID index number: 1-8
priority number	Defines the priority of the radius servers: 1 – Configures the parameters to communicate with the primary Radius server. 2 – Configures parameters to communicate with the secondary Radius server.
port number	Number of the authentication or accounting port on the Radius server: 1-65535 This parameter is optional. The default value for authentication port is 1812. The default value for accounting port is 1813.
address ipaddress	IP address of the authentication or accounting Radius server.
secret string	Defines the key used for Radius server security. The value is case sensitive and can be from 5 to 63 characters.
Remove	Removes the specified Radius server.

Example: configure radius authentication ssid 1 priority 1 host 192.168.0.1 key Netronics-NPP

Permission Level: super

Related Commands:

configure privacy wpa
configure radius interim-interval
configure radius retry-primary-interval
show privacy wpa
show radius

CONFIGURE RADIUS INTERIM-INTERVAL

Function: Defines the frequency that the unit sends accounting updates to the Radius server.

Command Syntax: **configure radius interim-interval** <interval number>

Command Description:

Parameter	Value
interval number	Defines the time interval that the unit waits between sending accounting updates to the Radius server (seconds). 1 – 42949672 The default value is 600 seconds (10 minutes).

Example: configure radius interim-interval 1200

Permission Level: super

Related Commands:

configure radius
show radius

CONFIGURE RADIUS RETRY-PRIMARY-INTERVAL

Function: After switching to the secondary Radius server, this configures the time interval, in seconds, that the unit waits before retrying to use the primary Radius server again.

Command Syntax: **configure radius retry-primary-interval** <interval number>

Command Description:

Parameter	Value
interval number	Defines the time interval that the unit waits before trying to use the primary Radius server (seconds). 1 – 42949672 The default value is 900 seconds (15 minutes).

Example: configure radius retry-primary-interval 1200

Permission Level: super

Related Commands:
configure radius
show radius

CONFIGURE RECOVERY-SSID

Function: Enables and disables the recovery SSID mode.

Command Syntax: **configure recovery-ssid** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables the recovery SSID mode. Enables Dot11Radio 0 disable – Disables the recovery SSID mode. The default mode is enable.

Example: configure recovery-ssid enable

Permission Level: admin

Related Commands:
show recovery-ssid status

CONFIGURE SITESURVEY

Function: Performs a site survey of all available channels, for the selected spectrum. When a site survey is performed all services from the unit are disrupted and the unit proceeds to scan each available channel.

The site survey scans each channel to determine the interference level of all available channels. To display the test results, use the *show sitesurvey* command. These results can then be used to assist you in selecting the best available channel.

Command Syntax: **configure sitesurvey start spectrum** {all | 80211bg | 80211a} **auto-channel-selection** {enable | disable}

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.
all | 80211bg | 80211a	Defines the frequency spectrum for the site survey: all – Performs the site survey on both frequency spectrums. 80211bg – Performs the site survey on the 80211bg spectrum (2.4GHz). 80211a – Performs the site survey on the 80211a spectrum (5GHz).
enable | disable	enable – Enables the automatic channel selection. disable – Disables the automatic channel selection.

Example: configure sitesurvey start spectrum all auto-channel-selection enable

Permission Level: super

Related Commands:
configure interface Dot11Radio channel
configure interface Dot11Radio channel-list
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio channel-list
show sitesurvey

CONFIGURE SNMP ROCOMMUNITY

Function: Configures the SNMP read-only community name.

Command Syntax: **configure snmp rocommunity** <rocommunity name>

Command Description:

Parameter	Value
rocommunity name	Read-only community name. The value is case sensitive and can be up to 32 characters. The default value is public.

Example: configure snmp rocommunity public

Permission Level: admin

Related Commands:
configure snmp rwcommunity
show snmp-communities

CONFIGURE SNMP RWCOMMUNITY

Function: Configures the SNMP read and write community name.

Command Syntax: **configure snmp rwcommunity** <rwcommunity name>

Command Description:

Parameter	Value
rwcommunity name	Read and write community name. The value is case sensitive and can be up to 32 characters. The default value is private.

Example: configure snmp rwcommunity private

Permission Level: admin

Related Commands:
configure snmp rocommunity
show snmp-communities

CONFIGURE SSID

Function: Configures the SSID. This command is used to create or define a unique SSID. Once created, this SSID can be share on all devices that belong to your wireless network. Use the *configure ssid remove* command to remove an existing SSID.

Command Syntax: **configure ssid** <index number> name <ssid string> vlan <vlan number> privacy-method {none | wep | wpa} type {hidden | bssid}

Command Description:

Parameter	Value
index number	SSID index number: 1-8
ssid string	A string value that defines the name of the SSID. The value can be up to 32 characters. It can contain alpha-numeric chars [a-z,A-Z,0-9], '-', '_', and '.'. Spaces may also be used, but the SSID name must be contained in quotation marks.
vlan number	VLAN index number: 0-4095 Set the value to 0 to specify no VLAN tagging.
none | wep | wpa	Defines the basic privacy method of this SSID: none – No privacy wep – WEP privacy wpa – WPA privacy Use the *configure privacy* command for additional privacy configuration options.
hidden | bssid	Defines the SSID type: hidden – Hidden SSID. Does not transmit beacons. bssid – Transmits beacons.

Example: This example demonstrates how to configure an SSID with the following parameters:
SSID name = NPP-1
SSID name = BSSID
VLAN ID = 0 (no VLAN tagging)
Privacy method = none

SSID TC profile name = TcProfile75M
User TC profile name = TcProfile3M
configure ssid 1 name NPP-1 vlan 0 privacy-method none type bssid ssid-profile TcProfile75M user-profile TcProfile3M

Permission Level: admin

Related Commands:

configure privacy wep ssid index
configure privacy wpa
configure ssid remove
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show interface ssids
show ssid params
show tc-default-profile
show tc-profiles
show privacy wep
show privacy wpa

CONFIGURE SSID FORCED-ROUTING

Function: Configures the forced-routing mode. When enabled, all communications between clients, including clients with the same VLAN or SSID, are routed through the specified router.

Command Syntax: **configure ssid** <index number**> forced-routing** [{enable | disable}] [ip <ipaddress>]

Command Description:

Parameter	Value
index number	SSID index number. 1-8
enable | disable	enable – Enables forced routing. disable – Disables forced routing. This parameter is optional. The default value is disable.
ipaddress	IP address of the target when the forced-routing mode is enabled. This parameter is optional.

Example: configure ssid 1 forced-routing enable ip 192.168.250.1

Permission Level: admin

Related Commands:

show ssid forced-routing
show ssid params

CONFIGURE SSID MACFILTER

Function: Configures or removes a MAC Filter for an existing SSID.

Command Syntax: **configure ssid** <index number> **macfilter** <mac-filter-index number>
configure ssid <index number> **macfilter** remove

Command Description:

Parameter	Value
index number	SSID index number. 1-8
mac-filter-index number	MAC Filter List index number. 1-16
remove	Removes the MAC Filter for an existing SSID.

Example: configure ssid 1 macfilter 5

Permission Level: admin

Related Commands:
show mac-filter indices
show mac-filter list

CONFIGURE SSID PRIVACY-METHOD

Function: Modifies the privacy method for an existing SSID.

Command Syntax: **configure ssid** <index number> **privacy-method** {none | wep | wpa}

Command Description:

Parameter	Value
index number	SSID index number. 1-8
none | wep | wpa	Defines the basic privacy method of this SSID. none – No privacy wep – WEP privacy wpa – WPA privacy Use the *configure privacy* command for additional privacy configuration options.

Example: configure ssid 1 privacy-method none

Permission Level: admin

Related Commands:
configure ssid
configure privacy wep ssid index
configure privacy wpa
show ssid params
show privacy wep
show privacy wpa

CONFIGURE SSID REMOVE

Function: Deletes the specified SSID.

Command Syntax: **configure ssid** <index number> **remove**

Command Description:

Parameter	Value
index number	SSID index number. 1-8

Example: configure ssid 1 remove

Permission Level: admin

Related Commands:
configure ssid
configure privacy wpa
configure privacy wep ssid index
show ssid params
show privacy wep
show privacy wpa

CONFIGURE SSID RENAME

Function: Renames an existing SSID.

Command Syntax: **configure ssid** <index number> **rename** <ssid string>

Command Description:

Parameter	Value
index number	SSID index number. 1-8
ssid string	A string value that defines the name of the SSID. The value can be up to 32 characters. It can contain alpha-numeric chars [a-z,A-Z,0-9], '-', '_', and '.'. Spaces may also be used, but the SSID name must be contained in quotation marks.

Example: configure ssid 1 rename NPP-2

Permission Level: admin

Related Commands:
configure ssid
configure privacy wep ssid index
configure privacy wpa
show ssid params
show privacy wep
show privacy wpa

CONFIGURE SSID SSID-PROFILE

Function: Modifies the assigned SSID TC profile for an existing SSID. This profile is used to define the maximum throughput for the specified SSID for each device. It limits the total traffic for all connected stations.

Command Syntax: **configure ssid** <index number> **ssid-profile** <ssid profile name>

Command Description:

Parameter	Value
index number	SSID index number. 1-8
ssid profile name	Defines the assigned SSID TC profile. Specify the name of an existing Traffic Control profile. The value is case sensitive and can be up to 32 characters.

Example: configure ssid 1 ssid-profile TcProfile75M

Permission Level: admin

Related Commands:
configure ssid
configure privacy wep ssid index
configure privacy wpa
configure ssid remove
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show interface ssids
show ssid params
show tc-default-profile
show tc-profiles
show privacy wep
show privacy wpa

CONFIGURE SSID TYPE

Function: Redefines the SSID type for an existing SSID.

Command Syntax: **configure ssid** <index number> type {hidden | bssid}

Command Description:

Parameter	Value
index number	SSID index number. 1-8
hidden | bssid	Defines the SSID type: hidden – Hidden SSID. Does not transmit beacons. bssid – Transmits beacons.

Example: configure ssid 1 type bssid

Permission Level: admin

Related Commands:

configure ssid; show privacy wpa
configure privacy wep ssid index
configure privacy wpa
show ssid params
show privacy wep

CONFIGURE SSID USER-PROFILE

Function: Modifies the assigned User TC profile for an existing SSID. This profile is used to define the maximum throughput for each user for the specified SSID.

Command Syntax: **configure ssid** <index number> **user-profile** <user profile name>

Command Description:

Parameter	Value
index number	SSID index number. 1-8
user profile name	Defines the assigned User TC profile. Specify the name of an existing Traffic Control profile. The value is case sensitive and can be up to 32 characters.

Example: configure ssid 1 user-profile TcProfile3M

Permission Level: admin

Related Commands:
configure ssid
configure privacy wep ssid index
configure privacy wpa
configure ssid remove
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show interface ssids
show ssid params
show tc-default-profile
show tc-profiles
show privacy wep
show privacy wpa

CONFIGURE SSID VLAN

Function: Modifies the VLAN index for an existing SSID.

Command Syntax: **configure ssid** <index number> **vlan** <vlan number>

Command Description:

Parameter	Value
index number	SSID index number. 1-8
vlan number	VLAN index number. 0-4095 Set the value to 0 to specify no VLAN tagging.

Example: configure ssid 1 vlan 0

Permission Level: admin

Related Commands:
configure ssid
configure privacy wep ssid index
configure privacy wpa
show ssid params
show privacy wep
show privacy wpa

CONFIGURE TC

Function: Configures the Traffic Control operation mode.

Command Syntax: **configure tc** {enabled | disabled | on | off}

Command Description:

Parameter	Value
enabled | disabled | on | off	enabled – Enables the Traffic Control operation mode. disabled – Disables the Traffic Control operation mode. on – Enables the Traffic Control controller. Changes are implemented after restarting the unit. off – Disables the Traffic Control controller Changes are implemented after restarting the unit. The default mode is disabled and off.

Example: configure tc enabled

Permission Level: admin

Related Commands:
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show tc-default-profile
show tc-profiles

CONFIGURE TC-DEFAULT-PROFILE

Function: Defines which Traffic Control profile is the system default profile. This profile is the default profile that is assigned to SSIDs. It is used to define maximum throughput. To display the existing default profile, use the *show tc-default-profile* command. To display all existing Traffic Control profiles, use the *show tc-profile* command.

Command Syntax: **configure tc-default-profile** <profile name>

Command Description:

Parameter	Value
profile name	The name of an existing Traffic Control profile to be defined as the system default Traffic Control profile. The value is case sensitive and can be up to 32 characters.

Example: configure tc-default-profile profile75Mbps

Permission Level: admin

Related Commands:
configure ssid
configure tc
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show tc-default-profile
show tc-profiles

CONFIGURE TC-PROFILE MODIFY

Function: Modifies an existing Traffic Control profile. These profiles are used in configuring SSIDs to define maximum throughput.

Command Syntax: **configure tc-profile** <profile name> **modify** [max-download <maxd1>] [max-upload <maxu1>]

Command Description:

Parameter	Value
profile name	A string value that defines the name of an existing Traffic Control profile. The value is case sensitive and can be up to 32 characters.
maxdl	Maximum download throughput (kbits/s): 1-100000 This parameter is optional.
maxul	Maximum upload throughput (kbits/s): 1-54000 This parameter is optional.

Example: configure tc-profile TcProfile2 modify max-download 45000

Permission Level: admin

Related Commands:
configure ssid
configure tc
configure tc-default-profile
configure tc-profile new
configure tc-profile remove
show tc-default-profile
show tc-profiles

CONFIGURE TC-PROFILE NEW

Function: Creates a new Traffic Control profile. These profiles are used in configuring SSIDs to define maximum throughput. To implement a Traffic Control profile, the profile can be set as the default Traffic Control profile or be assigned to an SSID. To define the default Traffic Control profile, use the *configure tc-default-profile* command. To assign a profile to an SSID, use the *configure ssid* command.

Command Syntax: **configure tc-profile** <profile name> **new** max download <maxd1> upload <maxu1>

Command Description:

Parameter	Value
profile name	A string value that defines the name of the new Traffic Control profile. The value is case sensitive and can be up to 32 characters.
maxdl	Maximum download throughput (kbits/s): 1-100000
maxul	Maximum upload throughput (kbits/s): 1-54000

Example: configure tc-profile profile50Mbps new max download 50000 upload 50000

Permission Level: admin

Related Commands:
configure ssid
configure tc
configure tc-default-profile
configure tc-profile modify
configure tc-profile remove
show tc-default-profile
show tc-profiles

CONFIGURE TC-PROFILE REMOVE

Function: Deletes an existing Traffic Control profile. If a Traffic Control profile is currently assigned to an SSID, another profile must first be assigned to the SSID before deleting. To assign a different profile to an SSID, use the *configure ssid* command.

Command Syntax: **configure tc-profile** <profile name> remove

Command Description:

Parameter	Value
profile name	A string value that defines the name of an existing Traffic Control profile. The value is case sensitive and can be up to 32 characters.

Example: configure tc-profile profile75Mbps remove

Permission Level: admin

Related Commands:
configure ssid
configure tc
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
show tc-default-profile
show tc-profiles

CONFIGURE TRAP-NOTIFY-FILTER

Function: Defines the type of traps that are sent to the trap targets. By default, all types of traps are sent to the trap targets. To display the current settings of the trap filter, use the *show trap-notify-filters* command.

Command Syntax: **configure trap-notify-filter** category <category> {enable | disable}

Command Description:

Parameter	Value
category	Defines the type of traps that are sent to the trap targets: boot – Defines whether the boot category traps are sent interface – Defines whether the interface category traps are sent system – Defines whether the system category traps are sent operation – Defines whether the operations category traps are sent configuration – Defines whether the configuration category traps are sent cli – Defines whether the CLI category traps are sent aaa – Defines whether the radius category traps are sent sm – Defines whether the sm category traps are sent mesh – Defines whether the Mesh category traps are sent sta – Defines whether the station category traps are sent wifi – Defines whether the Wi-Fi category traps are sent
enable | disable	enable – The specified trap category is sent to the trap targets. disable – The specified trap category is not sent to the trap targets. The default value is enable for all trap categories except for the station category (sta).

Example: configure trap-notify-filter category sta enable

Permission Level: super

Related Commands:
configure trap-target add
configure trap-target remove
show trap-notify-filters
show trap-targets

CONFIGURE TRAP-TARGET ADD

Function: Adds a configuration definition for sending traps. To define the type of traps that will be sent to the trap targets, use the *configure trap-notify-filter* command.

Command Syntax: **configure trap-target add** <name> <ip address> [port <port number>] [retry-count <retry-count>] [timeout <timeout>] [security-name <security-name>]

Command Description:

Parameter	Value
name	Name of the trap configuration definition.
ip address	IP address of the destination for the trap.
port number	Number of the port to which the trap is sent: 1-65535 This parameter is optional. The default value is 162.
retry-count	Number of retries to communicate with the target. This parameter is optional. The default value is 3.
timeout	Time in msec the unit waits for a response from the target. This parameter is optional. The default value is 1500 (1500 msec).
security-name	Community name that must match between the target and the unit. The default value is private.

Example: configure trap-target add nms 192.168.0.1

Permission Level: super

Related Commands:
configure trap-notify-filter
configure trap-target remove
show trap-notify-filters
show trap-targets

CONFIGURE TRAP-TARGET REMOVE

Function: Removes a configuration definition for sending traps.

Command Syntax: **configure trap-target remove** <name>

Command Description:

Parameter	Value
name	Name of the trap configuration definition.

Example: configure trap-target remove nms

Permission Level: super

Related Commands:
configure trap-notify-filter
configure trap-target add
show trap-notify-filters
show trap-targets

CONFIGURE USERNAME

Function: Configures the local CLI users.

Command Syntax: **configure username** <username string> delete
configure username <username string> {password <password string> | encrypted-password <encrypted-password string> | nopassword} privilege {super | admin | viewer}

Command Description:

Parameter	Value
username string	Name of the CLI user to be configured. The value is case sensitive and can be up to 32 characters.
delete	Deletes the specified CLI user.
password | encrypted-password | nopassword	Password types: password – Defines a CLI non-encrypted user password. encrypted-password – Defines a CLI user with an encrypted password. nopassword – Defines a CLI user without a password.
password string	A string value that defines the password for a non-encrypted password. The value is case sensitive and can be up to 32 characters.
encrypted-password string	A string value that defines the password for an encrypted password. The value is the hashing result of the actual password and this result is 32 characters.
super | admin | viewer	CLI user privilege level: viewer – Low privileges admin – Medium privileges super – High privileges

Example: configure username guest nopassword privilege viewer

Permission Level: super

Related Commands:
configure username modify
show default-config

show running-config
show startup-config
show users

CONFIGURE USERNAME MODIFY

Function: Modifies an existing local CLI user.

Command Syntax: **configure username** <username string> **modify** {password <password string> | encrypted-password <encrypted-password string> | nopassword}

Command Description:

Parameter	Value
username string	Name of the existing CLI user to be configured. The value is case sensitive and can be up to 32 characters.
password | encrypted-password | nopassword	Password types: password – Defines a CLI non-encrypted user password. encrypted-password – Defines a CLI user with an encrypted password. nopassword – Defines a CLI user without a password.
password string	A string value that defines the password for a non-encrypted password. The value is case sensitive and can be up to 32 characters.
encrypted-password string	A string value that defines the password for an encrypted password. The value is the hashing result of the actual password and this result is 32 characters.

Example: configure username guest modify nopassword

Permission Level: super

Related Commands:
configure username
show default-config
show running-config
show startup-config
show users

CONFIGURE WEB

Function: Enables and disables the web service.

Command Syntax: **configure web** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables the web service disable – Disables the web service. The default mode is enable.

Example: configure web enable

Permission Level: super

Related Commands:
show web status

COPY RUNNING-CONFIG STARTUP-CONFIG

Function: Copies the currently running configuration and replaces the existing startup configuration. The startup configuration is saved in non-volatile memory and is used when starting the unit.

Command Syntax: **copy running-config startup-config**

Command Description:

Parameter	Value
None	

Example: copy running-config startup-config

Permission Level: super

Related Commands:
show running-config
show startup-config

DELETE STARTUP-CONFIG

Function: Deletes the current startup configuration and uses the default configuration after restarting the unit. After a restart, all changes made to the configuration of this unit will be lost.

Command Syntax: **delete** startup-config

Command Description:

Parameter	Value
None	

Example: delete startup-config

Permission Level: super

Related Commands:
reload
show messages

DISASSOCIATE-STA

Function: Disconnects communications with the specified station.

Command Syntax: **disassociate-sta** <macaddr>

Command Description:

Parameter	Value
macaddr	MAC address of the station to be disconnected.

Example: disassociate-sta 00:14:06:11:00:00

Permission Level: super

Related Commands:
None

EXPORT STARTUP-CONFIG

Function: Exports the startup configuration to the TFTP server. The startup configuration is saved in non-volatile memory and is used when starting the unit.

Command Syntax: **export startup-config** to tftp <server ipaddress> <filename string>

Command Description:

Parameter	Value
server ipaddress	IP address of the TFTP server.
filename string	A string value that defines the name of the file that will be saved on the TFTP server. The value can be up to 128 characters.

Example: export startup-config to tftp 192.168.0.1 wls_config.txt

Permission Level: super

Related Commands:
import startup-config
show startup-config

EXPORT SYSTEM-BACKUP

Function: Exports the entire system configuration to the TFTP server.

Command Syntax: **export system-backup** to tftp <server ipaddress> <filename string>

Command Description:

Parameter	Value
server ipaddress	IP address of the TFTP server.
filename string	A string value that defines the name of the file that will be saved on the TFTP server. The value can be up to 128 characters.

Example: export system-backup to tftp 192.168.0.1 wls_config.txt

Permission Level: super

Related Commands:
None

HOSTNAME

Function: Defines a new CLI prompt.

Command Syntax: **hostname** <prompt string>

Command Description:

Parameter	Value
prompt string	String value defining the new CLI prompt. This value is case sensitive.

Example: hostname Netronics

Permission Level: admin

Related Commands:
none

IMPORT IMAGE

Function: Imports the firmware from the TFTP server. The TFTP server can be specified by either its IP address and filename, or its URL. To implement the new firmware, restart the unit.

Command Syntax: **import image** from {{tftp <ip> <filename string>} | {url <url string>}}

Command Description:

Parameter	Value
ip	IP address of the TFTP server.
filename string	A string value that defines the name of the software image file. The value can be up to 128 characters.
url string	A string value that defines the full url to the software image file. The value can be up to 128 characters.

Example: import image from tftp 192.168.0.1 gapsw-2.2.20.16836-Beta-13.11.2006@172953.img

Permission Level: super

Related Commands:
show version
show messages
show softload-messages

IMPORT STARTUP-CONFIG

Function: Imports the startup configuration from the TFTP server and replaces the existing startup configuration in the unit. The startup configuration is saved in non-volatile memory and is used when starting the unit.

Command Syntax: **import startup-config** from tftp <ip address> <filename string>

Command Description:

Parameter	Value
ip address	IP address of the TFTP server.
filename string	A string value that defines the name of the file to be downloaded. The value can be up to 128 characters.

Example: import startup-config from tftp 192.168.0.1 wls_config.txt

Permission Level: super

Related Commands:
show startup-config

IPRF-CLIENT

Function: Configures the Iperf client. The Iperf client is used to run performance tests of the network between this unit and the specified Iperf server.

Command Syntax: **iprf-client** restart {udp | tcp} <server ip-address> <timeout>
iprf-client status
iprf-client stop

Command Description:

Parameter	Value
restart | status | stop	restart – Starts a new Iperf session and displays the performance test results. status – Displays the current status of the Iperf client. stop – Stops the Iperf client.
udp | tcp	udp – Iperf client uses UDP packets. tcp – Iperf client uses TCP packets.
server ip-address	IP address of the Iperf server
timeout	Time period of the performance test in seconds.

Example: iprf-client restart udp 192.168.0.1 90

Permission Level: super

Related Commands:
iprf-server

IPRF-SERVER

Function: Configures the Iperf server. This server is used to test the throughput between this unit and its connected Iperf clients. Once the current telnet session is closed the Iperf server is terminated. To perform a long test the CLI timeout must be configured to a longer period of time.

Command Syntax: **iprf-server** restart {udp | tcp} **[**<timeout>]
iprf-server status
iprf-server stop

Command Description:

Parameter	Value
restart | status | stop	restart – Starts a new Iperf session. status – Displays the current status of the Iperf server. stop – Stops the Iperf server.
udp | tcp	udp – Iperf server uses UDP packets. tcp – Iperf server uses TCP packets.
timeout	Time period of the performance test in seconds. This parameter is optional.

Example: iprf-server restart udp

Permission Level: super

Related Commands:
configure inactivity-timeout
iprf-client

MORE

Function: Enables or disables the **more** display option. When this is enabled, the first page is displayed for large outputs and then pauses. Press SPACEBAR to display the next page or press ENTER to display the next line.

Command Syntax: **more** {enable | disable}

Command Description:

Parameter	Value
enable | disable	enable – Enables the **more** display option. disable – Disables the **more** display option. The default value is enabled.

Example: more disable

Permission Level: viewer

Related Commands:
None

PING

Function: Sends ICMP ping packets to the specified IP address.

Command Syntax: **ping** <dest ip-address>

Command Description:

Parameter	Value
dest ip-address	IP address for the ping destination.

Example: ping 192.168.0.1

Permission Level: admin

Related Commands:
None

RELOAD

Function: Reboots the system.

Command Syntax: **reload** [{bank1 | bank2}]

Command Description:

Parameter	Value
bank1 | bank2	bank1 – Reboots from software bank 1. bank2 – Reboots from software bank 2. This parameter is optional.

Example: reload

Permission Level: admin

Related Commands:
show uptime

SHOW ASSOCIATED-STATIONS

Function: Displays the MAC addresses of the clients connected to each radio interface.

Command Syntax: **show associated-stations**

Command Description:

Parameter	Value
None	

Example: show associated-stations

Related Commands:
show spectrum-management clear-count-percent
show spectrum-management doa

SHOW CAC ACTIVE-VOIP-CLIENTS

Function: Displays all active VoIP clients.

Command Syntax: **show cac active-voip-clients**

Command Description:

Parameter	Value
None	

Example: show cac active-voip-clients

Permission Level: viewer

Related Commands:
configure cac
configure cac min-vc-snr
show cac params

SHOW CAC MAC_CLASSIFIER_MASKS

Function: Displays all active MAC masks for VoIP.

Command Syntax: show cac mac_classifier_masks

Command Description:

Parameter	Value
None	

Example: show cac mac_classifier_masks

Permission Level: viewer

Related Commands:
configure cac

configure cac algorithm
configure cac mac_classifier
configure cac min-vc-snr
show cac active-voip-clients

SHOW CAC PARAMS

Function: Displays the current CAC configuration.

Command Syntax: **show cac params**

Command Description:

Parameter	Value
None	

Example: show cac params

Permission Level: viewer

Related Commands:
configure cac
configure cac algorithm
configure cac mac_classifier
configure cac min-vc-snr
show cac active-voip-clients

SHOW CALIBRATION STATUS

Function: Displays the calibration status of the radio interface channels.

Command Syntax: **show calibration status**

Command Description:

Parameter	Value
None	

Example: show calibration status

Permission Level: super

Related Commands:
configure interface Dot11Radio channel

SHOW CLASSIFIER

Function: Displays a table containing all the codecs currently in the classifier and the configuration for these codecs.

Command Syntax: **show classifier**

Command Description:

Parameter	Value
None	

Example: show classifier

Permission Level: viewer

Related Commands:
configure classifier
configure classifier add
configure classifier remove

SHOW COUNTRY-CODE

Function: Displays the current country code.

Command Syntax: **show country-code**

Command Description:

Parameter	Value
None	

Example: show country-code

Permission Level: admin

Related Commands:
None

SHOW DEFAULT-CONFIG

Function: Displays the default configuration of the unit. This configuration contains the factory settings.

Command Syntax: **show default-config**

Command Description:

Parameter	Value
None	

Example: show default-config

Permission Level: admin

Related Commands:
import startup-config
delete startup-config

SHOW ENHANCED-OMNI

Function: Displays the current status of the enhanced omni mode.

Command Syntax: **show enhanced-omni**

Command Description:

Parameter	Value
None	

Example: show enhanced-omni

Permission Level: admin

Related Commands:
configure enhanced-omni

SHOW INACTIVITY-TIMEOUT

Function: Displays the CLI inactivity time-out. The time displayed is the time that the CLI will automatically log off the user when the user's session is not active.

Command Syntax: **show inactivity-timeout**

Command Description:

Parameter	Value
None	

Example: show inactivity-timeout

Permission Level: viewer

Related Commands:
configure inactivity-timeout

SHOW INTERFACE DOT11RADIO

Function: Displays the typical parameter settings of the specified interface or all radio interfaces.

Command Syntax: **show interface Dot11Radio** [<interface number>]

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the typical parameter settings for all radio interfaces are displayed.

Example: show interface Dot11Radio 0

Permission Level: viewer

Related Commands:
configure interface Dot11Radio disable
configure interface Dot11Radio enable
configure interface Dot11Radio beacon-period
configure interface Dot11Radio beacon-rate
configure interface Dot11Radio channel
configure interface Dot11Radio dtim-period
configure interface Dot11Radio mode
configure interface Dot11Radio service

SHOW INTERFACE DOT11RADIO CHANNEL-LIST

Function: Displays all the Wi-Fi channels available and allowable for the specified radio interface or all radio interfaces.

Command Syntax: **show interface Dot11Radio** [<interface number>] **channel-list**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the channel list for all radio interfaces is displayed.

Example: show interface Dot11Radio 0 channel-list

Permission Level: admin

Related Commands:
configure interface Dot11Radio channel

configure interface Dot11Radio channel-list

SHOW INTERFACE DOT11RADIO MESH-SCAN-RESULTS

Function: Displays the results of the latest channel scan.

To perform a channel scan, use the *configure sitesurvey* command.

Command Syntax: **show interface Dot11Radio** <interface number> **mesh-scan-results**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the channel list for all radio interfaces is displayed.

Example: show interface Dot11Radio 0 mesh-scan-results

Permission Level: admin

Related Commands:
configure interface Dot11Radio channel
configure interface Dot11Radio channel-list
configure sitesurvey
show interface Dot11Radio channel-list

SHOW INTERFACE DOT11RADIO PARAMS

Function: Displays the configuration of the specified interface or all radio interfaces.

Command Syntax: **show interface Dot11Radio** [<interface number>] **params**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the configurations for all radio interfaces are displayed.

Example: show interface Dot11Radio 0 params

Permission Level: viewer

Related Commands:
configure interface Dot11Radio disable

configure interface Dot11Radio enable
configure interface Dot11Radio beacon-period
configure interface Dot11Radio beacon-rate
configure interface Dot11Radio channel
configure interface Dot11Radio dtim-period
configure interface Dot11Radio erp-mode
configure interface Dot11Radio fixed-rate
configure interface Dot11Radio max-assoc
configure interface Dot11Radio max-rate
configure interface Dot11Radio min-rate
configure interface Dot11Radio mode
configure interface Dot11Radio preamble-mode
configure interface Dot11Radio rts
configure interface Dot11Radio sensitivity
configure interface Dot11Radio service
configure interface Dot11Radio wme-enable

SHOW INTERFACE DOT11RADIO PROFILE

Function: Displays the current profile parameters for the specified radio interface or all radio interfaces.

Command Syntax: **show interface Dot11Radio** [<interface number>] **profile**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the profile parameters for all radio interfaces are displayed.

Example: show interface Dot11Radio 0 profile

Permission Level: super

Related Commands:
configure interface Dot11Radio profile
configure interface Dot11Radio wme
configure interface Dot11Radio wme-enable
show interface Dot11Radio params
show interface Dot11Radio wme

SHOW INTERFACE DOT11RADIO RANGE-OPTIMIZATION

Function: Displays the type of optimization that is currently implemented for the calibration of the RX sensitivity on the specified radio interface.

Command Syntax: **show interface Dot11Radio** <interface number> **range-optimization**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications.

Example: show interface Dot11Radio 0 range-optimization

Permission Level: super

Related Commands:
configure interface Dot11Radio range-optimization

SHOW INTERFACE DOT11RADIO STATS

Function: Displays the statistics of the specified interface or all radio interfaces.

Command Syntax: **show interface Dot11Radio** [<interface number>] **stats**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the statistics for all radio interfaces are displayed.

Example: show interface Dot11Radio 0 stats

Permission Level: viewer

Related Commands:
configure interface Dot11Radio disable
configure interface Dot11Radio enable

SHOW INTERFACE DOT11RADIO WME

Function: Displays the WME configuration of the specified interface or all radio interfaces.

Command Syntax: **show interface Dot11Radio** [<interface number>] **wme**

Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0, 1 or 2 for units with three interfaces, or to 0 or 1 for units with two interfaces. The last interface is used for 5GHz communications and all other radio interfaces are used for 2.4GHz communications. This parameter is optional. If not specified, the WME configuration for all radio interfaces is displayed.

Example: show interface Dot11Radio 0 wme

Permission Level: viewer

Related Commands:
configure interface Dot11Radio wme
configure interface Dot11Radio wme-enable

SHOW INTERFACE FASTETHERNET

Function: Displays the current Fast Ethernet configuration of the specified interface.

Command Syntax: **show interface FastEthernet** <interface number>

Command Description:

Parameter	Value
interface number	FastEthernet interface number. In this version the interface is always set to 0.

Example: show interface FastEthernet 0

Permission Level: viewer

Related Commands:
configure interface FastEthernet add-vlan-tag
configure interface FastEthernet auto-negotiation
show interface FastEthernet stats

SHOW INTERFACE FASTETHERNET STATS

Function: Displays the Fast Ethernet statistics of the specified interface.

Command Syntax: **show interface FastEthernet** <interface number> **stats**

Command Description:

Parameter	Value
interface number	FastEthernet interface number. In this version the interface is always set to 0.

Example: show interface FastEthernet 0 stats

Permission Level: viewer

Related Commands:

configure interface FastEthernet auto-negotiation
show interface FastEthernet

SHOW INTERFACE SSIDS

Function: Displays information on the current SSIDs for each interface.

Command Syntax: **show interface ssids**

Command Description:

Parameter	Value
None	

Example: show interface ssids
Permission Level: viewer

Related Commands:
configure interface Dot11Radio ssid
configure ssid
configure ssid remove
configure ssid rename
show ssid params

SHOW INTERFACE WIFI-LOAD-RATIO

Function: Displays the Wi-Fi load ratio of the radio interfaces. The table displays the following information:

- Clear Count Ratio – Displays the current Wi-Fi load in a percentage of the maximum air occupancy. Clear count load is the summation of the loads due to RX Frames, TX Frames and noise.
- RX Frame Count – Displays the Wi-Fi load associated with valid received frames in a percentage of the maximum air occupancy.
- TX Frame Count – Displays the Wi-Fi load associated with transmitted frames in a percentage of the maximum air occupancy.

Command Syntax: **show interface wifi-load-ratio**

Command Description:

Parameter	Value
None	

Example: show interface wifi-load-ratio

Permission Level: viewer

Related Commands:
show spectrum-management clear-count-percent

SHOW INTERFACE WIFI-STATS

Function: Displays information related to each of the radio interfaces. The table displays the following information:

- Power Saving Stations – Displays number of clients in power savings mode that are connected to each interface.
- Associated Stations – Displays number of clients that are connected to each interface.

Command Syntax: **show interface wifi-stats**

Command Description:

Parameter	Value
None	

Example: show interface wifi-stats
Permission Level: viewer

Related Commands:
configure interface Dot11Radio dtim-period
configure interface Dot11Radio sensitivity

SHOW IP ADDRESS

Function: Displays the configuration of the management interface parameters.

Command Syntax: **show ip address**

Command Description:

Parameter	Value
None	

Example: show ip address

Permission Level: viewer

Related Commands:
configure ip vlan
configure ip default-gateway

SHOW IP PARAMS

Function: Displays the configuration of telnet and SSH related parameters.

Command Syntax: **show ip params**

Command Description:

Parameter	Value
None	

Example: show ip params

Permission Level: viewer

Related Commands:
configure ip mtu
configure ip ssh
configure ip telnet
show ip address
show ip ssh-public-keys

SHOW IP SSH-PUBLIC-KEYS

Function: Displays the configuration of the SSH public authorized keys.

Command Syntax: **show ip ssh-public-keys**

Command Description:

Parameter	Value
None	

Example: show ip ssh-public-keys

Permission Level: admin

Related Commands:
configure ip ssh
show ip params

SHOW LOGGED-IN-USERS

Function: Displays information about the users that are currently logged on the CLI.

Command Syntax: **show logged-in-users**

Command Description:

Parameter	Value
None	

Example: show logged-in-users

Permission Level: super

Related Commands:
configure username

SHOW LOGGING DESTINATIONS

Function: Displays the configuration of the log destinations. It displays the status and the maximum level of messages that are sent to each destination. The configuration of the ram destination is also the configuration of the system log.

Command Syntax: **show logging destinations**

Command Description:

Parameter	Value
None	

Example: show logging destinations

Permission Level: viewer

Related Commands:
configure logging dest cli
configure logging dest history
configure logging dest rs232console
show logging host
configure logging module
configure logging syslog ip-address
show messages

SHOW LOGGING HISTORY

Function: Displays the logging history.

Command Syntax: **show logging history**

Command Description:

Parameter	Value
None	

Example: show logging history

Permission Level: admin

Related Commands:
configure logging dest history

SHOW LOGGING HOST

Function: Displays the log destination host and port. It displays Host's IP address and communication port.

Command Syntax: **show logging host**

Command Description:

Parameter	Value
None	

Example: show logging host

Permission Level: viewer

Related Commands:
configure logging syslog ip-address
show logging destinations

SHOW LOGGING MODULES-LEVEL

Function: Displays the log level of the modules. The level defines the level of details saved in the log. The higher the number displayed the more details that are recorded.

Command Syntax: **show logging modules-level**

Command Description:

Parameter	Value
None	

Example: show logging modules-level

Permission Level: admin

Related Commands:
configure logging module
show messages

SHOW MAC-FILTER INDICES

Function: Displays the configuration of the current MAC filter lists.

Command Syntax: **show mac-filter indices**

Command Description:

Parameter	Value
None	

Example: show mac-filter indices

Permission Level: viewer

Related Commands:
configure mac-filter list new
configure mac-filter list remove-list

SHOW MAC-FILTER LIST

Function: Displays the list of MAC addresses contained in the specified MAC filter lists.

Command Syntax: **show mac-filter list** <index number>

Command Description:

Parameter	Value
index number	Index number of an existing MAC filter list: 1-16

Example: show mac-filter list 3
Permission Level: viewer

Related Commands:
configure mac-filter list add-mac
configure mac-filter list new
configure mac-filter list remove-list
configure mac-filter list remove-mac

SHOW MANUFACTURE-DETAILS

Function: Displays the unit's serial number and MAC address.

Command Syntax: **show manufacture-details**

Command Description:

Parameter	Value
None	

Example: show manufacture-details

Permission Level: viewer

Related Commands:
None

SHOW MESH INTERFACE-WDS-PARAMS

Function: Displays the WDS parameters for each radio interface.

Command Syntax: **show mesh interface-wds-params**

Command Description:

Parameter	Value
None	

Example: show mesh interface-wds-params

Permission Level: super

Related Commands:
configure mesh interface Dot11Radio wds
configure mesh interface Dot11Radio wds-peer
configure mesh interface Dot11Radio wds-privacy
show mesh route
show mesh wds-peer-list

SHOW MESH FILTER-LIST

Function: Displays the mesh filtering configuration of the unit. It displays whether mesh filtering is enabled, the type of mesh filter list and the list of MAC addresses in the list.

Command Syntax: **show mesh filter-list**

Command Description:

Parameter	Value
None	

Example: show mesh filter-list

Permission Level: admin

Related Commands:
configure mesh filter-list
show mesh params

SHOW MESH PARAMS

Function: Displays the mesh configuration of the unit. It displays the mesh timeout, mesh interface, mesh security settings and whether the unit has been defined as a Mesh-Gateway or Mesh-Node.

Command Syntax: **show mesh params**

Command Description:

Parameter	Value
None	

Example: show mesh params

Permission Level: viewer

Related Commands:
configure mesh connectivity_test
configure mesh interface
configure mesh mode
configure mesh privacy

SHOW MESH ROUTE

Function: Displays a routing table that contains the routing entry for the current next hop to get access to the Mesh-Gateway. It also displays all the alternative next hop routing entries.

Command Syntax: **show mesh route**

Command Description:

Parameter	Value
None	

Example: show mesh route

Permission Level: super

Related Commands:
configure mesh interface Dot11Radio wds
configure mesh reroute-now
show mesh params
show mesh wds-peer-list

SHOW MESH STAND-ALONE

Function: Displays the current stand alone mode and status.

Command Syntax: **show mesh stand-alone**

Command Description:

Parameter	Value
None	

Example: show mesh stand-alone

Permission Level: super

Related Commands:
configure mesh stand-alone
configure mesh stand-alone-passphrase
configure mesh interface
configure mesh mode
configure mesh privacy

SHOW MESH WDS-PEER-LIST

Function: Displays the WDS peers.

Command Syntax: **show mesh wds-peer-list**

Command Description:

Parameter	Value
None	

Example: show mesh wds-peer-list

Permission Level: super

Related Commands:
configure mesh interface Dot11Radio wds
configure mesh interface Dot11Radio wds-peer
configure mesh interface Dot11Radio wds-privacy
show mesh interface wds-params
show mesh route

SHOW MESSAGES

Function: Displays the specified message types from the system log.

Command Syntax: **show messages** <message type>

Command Description:

Parameter	Value
message type	defaults-loading – Displays all the messages that contain commands related to default configuration loading and their results. config-loading – Displays all the messages that contain commands related to startup configuration loading and their results. software-loading – Displays all the messages related to software downloading.

Example: show messages software-loading

Permission Level: admin

Related Commands:
configure logging dest history
show logging destinations
show logging modules-level
show softload-messages

SHOW NTP

Function: Displays the current configuration of the NTP client on the unit.

Command Syntax: **show ntp**

Command Description:

Parameter	Value
None	

Example: show ntp

Permission Level: super

Related Commands:
configure ntp

SHOW PINGWD

Function: Displays the current configuration of the ping watchdog feature.

Command Syntax: **show pingwd**

Command Description:

Parameter	Value
None	

Example: show pingwd

Permission Level: super

Related Commands:
configure pingwd

SHOW PRIVACY WEP

Function: Displays the current configuration for all the WEP keys.

Command Syntax: **show privacy wep**

Command Description:

Parameter	Value
None	

Example: show privacy wep

Permission Level: viewer

Related Commands:
configure privacy wep ssid index
configure ssid
show privacy wep params
show ssid params

SHOW PRIVACY WEP PARAMS

Function: Displays the current configuration for the WEP parameters.

Command Syntax: **show privacy wep params**

Command Description:

Parameter	Value
None	

Example: show privacy wep

Permission Level: viewer

Related Commands:
configure privacy wep ssid index
configure ssid
show privacy wep
show ssid params

SHOW PRIVACY WPA

Function: Displays the current information on WPA privacy.

Command Syntax: **show privacy wpa**

Command Description:

Parameter	Value
None	

Example: show privacy wpa

Permission Level: admin

Related Commands:
configure ssid
configure privacy wpa
show ssid params

SHOW RADIUS

Function: Displays configuration for the specified radius server.

Command Syntax: **show radius** {accounting | authentication | params}

Command Description:

Parameter	Value
accounting | authentication | params	accounting – Displays the configuration of the accounting Radius server. authentication – Displays the configuration of the authentication Radius server. params – Displays the general parameters of the Radius server.

Example: show radius params

Permission Level: viewer

Related Commands:
configure radius
configure radius interim-interval
configure radius retry-primary-interval

SHOW RECOVERY-SSID STATUS

Function: Displays the current status of the recovery SSID mode.

Command Syntax: **show recovery-ssid status**

Command Description:

Parameter	Value
None	

Example: show recovery-ssid status

Permission Level: super

Related Commands:
configure recovery-ssid

SHOW RUNNING-CONFIG

Function: Displays the current configuration of the unit. This configuration is saved in volatile memory.

Command Syntax: **show running-config**

Command Description:

Parameter	Value
None	

Example: show running-config

Permission Level: admin

Related Commands:

SHOW SITESURVEY

Function: Displays the test results of the latest site survey of all available channels. These results can then be used to assist you in selecting the best available channel.

To perform a site survey, use the *configure sitesurvey* command.

Command Syntax: **show sitesurvey**

Command Description:

Parameter	Value
None	

Example: show sitesurvey

Permission Level: admin

Related Commands:
configure interface Dot11Radio channel
configure interface Dot11Radio channel-list
configure sitesurvey
show interface Dot11Radio params
show interface Dot11Radio channel-list

SHOW SNMP-COMMUNITIES

Function: Displays the current SNMP community names.

Command Syntax: **show snmp-communities**

Command Description:

Parameter	Value
None	

Example: show snmp-communities

Permission Level: viewer

Related Commands:
configure snmp rocommunity
configure snmp rwcommunity

SHOW SOFTLOAD-MESSAGES

Function: Displays the messages related to the *import image* command and its results.

Command Syntax: **show softload-messages**

Command Description:

Parameter	Value
None	

Example: show softload-messages

Permission Level: admin

Related Commands:
import image
show messages

SHOW SOFTWARE-BANKS

Function: Displays information on the unit's software memory banks. It displays a table that shows which software version is in each bank and which bank is active. It also displays which bank will be active for the next restart.

Command Syntax: **show software-banks**

Command Description:

Parameter	Value
None	

Example: show software-banks

Permission Level: admin

Related Commands:
import image
show version

SHOW SPECTRUM-MANAGEMENT CLEAR-COUNT-PERCENT

Function: Displays the Clear Count ratio of the radio interfaces and other related data. The table displays the following information:

- TX Frame Count – Displays the Wi-Fi load associated with transmitted frames in a percentage of the maximum air occupancy.
- RX Frame Count – Displays the Wi-Fi load associated with valid received frames in a percentage of the maximum air occupancy.
- Clear Count Ratio – Displays the current Wi-Fi load in a percentage of the maximum air occupancy. Clear count load is the summation of the loads due to RX Frames, TX Frames and noise.
- Sensitivity Level – Displays the sensitivity setting for each interface.
- Noise Level – Displays the sensitivity level for each interface. This defines the noise floor level in dBm.

Command Syntax: **show spectrum-management clear-count-percent**

Command Description:

Parameter	Value
None	

Example: show spectrum-management clear-count-percent

Permission Level: viewer

Related Commands:
configure interface Dot11Radio sensitivity
show associated-stations
show spectrum-management doa

SHOW SPECTRUM-MANAGEMENT DOA

Function: Displays the number of packets received from the clients per Direction of Arrival (DOA). The number of packets is displayed based on the angle from the antenna. It is displayed in 16 segments. The value displayed is the number of packets received during the last four seconds.

Command Syntax: **show spectrum-management doa**

Command Description:

Parameter	Value
None	

Example: show spectrum-management doa

Permission Level: viewer

Related Commands:
show associated-stations
show spectrum-management clear-count-percent

SHOW SSID PARAMS

Function: Displays the current configuration for all SSIDs.

Command Syntax: **show ssid params**

Command Description:

Parameter	Value
None	

Example: show ssid params

Permission Level: viewer

Related Commands:
configure privacy wep ssid index

configure ssid

SHOW STARTUP-CONFIG

Function: Displays the startup configuration of the unit. This configuration is saved in non-volatile memory and is used when starting the unit.

Command Syntax: **show startup-config**

Command Description:

Parameter	Value
None	

Example: show startup-config

Permission Level: admin

Related Commands:
delete startup-config
copy running-config startup-config
export startup-config
import startup-config

SHOW SYSTEM-TEMPERATURE

Function: Displays the temperature of the unit's internal modules.

Command Syntax: **show system-temperature**

Command Description:

Parameter	Value
None	

Example: show system-temperature

Permission Level: super

Related Commands:
None

SHOW TC-DEFAULT-PROFILE

Function: Displays the default Traffic Control profile of the unit. This profile is the default profile that is assigned to SSIDs. It is used to define maximum throughput.

Command Syntax: **show tc-default-profile**

Command Description:

Parameter	Value
None	

Example: show tc-default-profile

Permission Level: admin

Related Commands:
configure ssid
configure tc
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show tc-profiles

SHOW TC-PROFILES

Function: Displays all the existing Traffic Control profile. These profiles are used in configuring SSIDs to define maximum throughput.

Command Syntax: **show tc-profiles**

Command Description:

Parameter	Value
None	

Example: show tc-profiles

Permission Level: viewer

Related Commands:
configure ssid
configure ssid ssid-profile
configure ssid user-profile
configure tc
configure tc-default-profile
configure tc-profile modify
configure tc-profile new
configure tc-profile remove
show tc-default-profile

SHOW TRAP-NOTIFY-FILTERS

Function: Displays a table of all the trap categories and their current trap filter settings. When a category is enabled the traps associated this category is sent to the trap targets. To configure settings of the trap filter, use the *configure trap-notify-filter* command.

Command Syntax: **show trap-notify-filter**

Command Description:

Parameter	Value
None	

Example: show trap-notify-filters

Permission Level: super

Related Commands:
configure trap-notify-filter
configure trap-target add
configure trap-target remove
show trap-targets

SHOW TRAP-TARGETS

Function: Displays a table containing all current trap targets in the unit. Each trap target displayed includes the configuration definition for sending traps to the target.

Command Syntax: **show trap-targets**

Command Description:

Parameter	Value
None	

Example: show trap-targets

Permission Level: viewer

Related Commands:
configure trap-notify-filter
configure trap-target add
configure trap-target remove
show trap-notify-filters

SHOW UPTIME

Function: Displays time the system has been running since the last restart.

Command Syntax: **show uptime**

Command Description:

Parameter	Value
None	

Example: show uptime

Permission Level: viewer

SHOW USERS

Function: Displays the table of all configured local users.

Command Syntax: **show users**

Command Description:

Parameter	Value
None	

Example: show users

Permission Level: admin

Related Commands:
configure username

SHOW VERSION

Function: Displays the current firmware version and release date.

Command Syntax: **show version**

Command Description:

Parameter	Value
None	

Example: show version

Permission Level: viewer

SHOW WEB STATUS

Function: Displays the current status of the web service.

Command Syntax: **show web status**

Command Description:

Parameter	Value
None	

Example: show web status

Permission Level: super

Related Commands:
configure web

Appendix A

List of Acronyms

Acronym	Explanation
802.11	A family of specifications related to wireless networking, including: 802.11a, 802.11b, and 802.11g.
AP	Access Point. The hub of a wireless network. Wireless clients connect to the access point, and traffic between two clients must travel through the access point. Access points are often abbreviated to AP
BSSID	Broadcast Service Set Identifier
CPE	Customer Premises Equipment
DHCP	Dynamic Host Configuration Protocol. A protocol which enables a server to automatically assign an IP address to clients so that the clients do not have to configure the IP addresses manually.
EAP	Extensible Authentication Protocol. A standard form of generic messaging used in 802.1X.
ESSID	EGOed Service Set Identifier
PMK	Pairwise Master Key
SSID	Service Set Identifier, a set of characters that give a unique name to a WLAN.
TKIP	Temporal Key Integrity Protocol
VLAN	Virtual Local Access Network
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy. An encryption system created to prevent eavesdropping on wireless network traffic.

WMG	Wireless Media Gateway of the Netronics solution.
WNC	Wireless Network Controller of the Netronics solution.
WPA	Wi-Fi Protected Access. A modern encryption system created to prevent eavesdropping on wireless network traffic. It is considered more secure than WEP.
WPA-EAP	WPA-Extensible Authentication Protocol
WPA-PSK	WPA-Pre-Shared Key

Appendix B

Wiring Specifications

Console Port (DTE)	RJ-45-to-RJ-45 Straight Cable		RJ-45 to DB-9 Terminal Adapter	Console Device
Signal	RJ-45 Pin	RJ-45 Pin	DB-9 Pin	Signal
No connection	1	1	8	CTS
No connection	2	2	6	DSR
No connection	3	3	5	GND
GND	4	4	5	GND
RxD	5	5	3	TxD
TxD	6	6	2	RxD
No connection	7	7	4	DTR
No connection	8	8	7	RTS

Table 1: Console Port Signalling and Cabling with a DB-9 Adapter for the NetPoint Pro 6x2.4 Unit

Appendix C

Power Up and Software Configuration

The NetPoint Pro units are normally mounted on streetlights (poles or walls) where it is inconvenient to configure. Therefore, it is recommended that wireless communication be established to the unit prior to installation, so that the unit can later be configured and monitored remotely. To verify communications when installing the unit, the Mesh-Gateways must be installed and powered up first.

The LEDs on the unit indicate the status of communications between the unit and the network. See Table 5 for more information on the LED indicators.

The ACT LED on the Mesh-Gateway should be checked to verify that wired communications have been established. The BH LED on the Mesh-Gateway should be checked to verify that wireless communications have been established.

When powering up a Mesh-Node, the BH LED should be lit to verify that the unit's wireless communication is connected. The boot time is about 2.5 minutes. The BH LED indicator will light up after the boot is completed.

LED	Function
PWR	**Green** – There is power to the unit. **Unlit** – There is no power to the unit.
STAT	**Green** – The operational status of the unit is normal. **Red –** The unit is in a failure state. **Unlit** – There is no power to the unit.
ACT	**Green** – When the LED is on, there is a communication connection. When the LED is flashing, traffic is flowing though the unit. **Unlit** – There is no communication connection.
BH	**Green** – On a Mesh-Gateway, the mesh functionality is activated. On a Mesh-Node, the unit is connected to the mesh. **Unlit** – On a Mesh-Gateway, the mesh functionality is not activated or no Ethernet link is available. On a Mesh-Node, the unit is not configured or failed to connect to the mesh.

Table 2: LED Indicators