



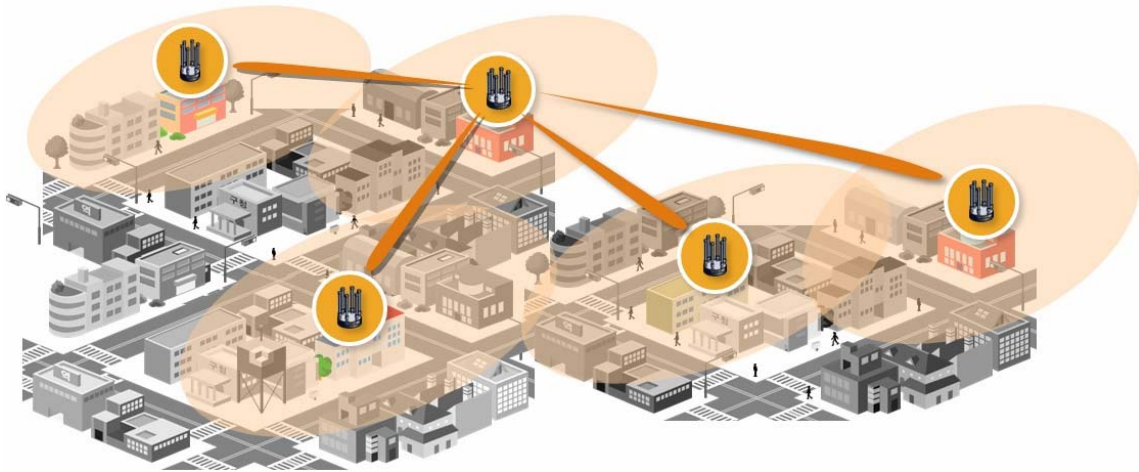
# NetPoint Pro Family

## Broadband Wireless Networking Solutions

NetPoint Pro n2S / n2C / n2S5S

---

### CLI Reference Guide



2<sup>nd</sup> Generation

This document contains information that is proprietary to Netronics Technologies Inc.

No part of this publication may be reproduced, modified, or distributed without prior written authorization of Netronics Technologies Inc.

This document is provided as is, without warranty of any kind.

### **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.

Copyright © 2011 by Netronics. All rights reserved.

# READ THIS FIRST!

## Important Safety Instructions



**Caution**

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



**Caution**

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



**Caution**

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.



**Warning**

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.



**Warning**

This apparatus must be connected to earth ground.



**Warning**

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



**Caution**

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



**Caution**

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



**Caution**

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.



**Caution**

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.



**Caution**

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

# Table of Contents

<b>Introduction .....</b>	<b>8</b>
Scope of this Document .....	8
Organization .....	8
Conventions .....	8
<b>Using the NetPoint Pro CLI .....</b>	<b>9</b>
Configurations .....	9
Special Character Functions .....	9
Enable/Disable .....	12
Using Configuration and Remove commands .....	12
Delete .....	12
Saving Configuration Changes .....	13
Radio Interfaces .....	13
<b>NetPoint Pro CLI commands .....</b>	<b>14</b>
CONFIGURE INTERFACE DOT11RADIO AIRTIME-FAIRNESS .....	14
CONFIGURE INTERFACE DOT11RADIO BEACON-PERIOD .....	14
CONFIGURE INTERFACE DOT11RADIO CHANNEL .....	15
CONFIGURE INTERFACE DOT11RADIO DISABLE .....	16
CONFIGURE INTERFACE DOT11RADIO DISTANCE.....	17
CONFIGURE INTERFACE DOT11RADIO ENABLE .....	18
CONFIGURE INTERFACE DOT11RADIO FRINGE .....	18
CONFIGURE INTERFACE DOT11RADIO GUARD-INTERVAL .....	19
CONFIGURE INTERFACE DOT11RADIO MAX-ASSOC .....	19
CONFIGURE INTERFACE DOT11RADIO MODE .....	20
CONFIGURE INTERFACE DOT11RADIO RADAR-DETECTION .....	21
CONFIGURE INTERFACE DOT11RADIO SENSITIVITY .....	21
CONFIGURE INTERFACE DOT11RADIO SERVICE .....	22
CONFIGURE INTERFACE DOT11RADIO SITE-SURVEY .....	22
CONFIGURE INTERFACE DOT11RADIO SSID .....	23
CONFIGURE INTERFACE DOT11RADIO TXPWATTN .....	23
CONFIGURE INTERFACE DOT11RADIO WME .....	24
CONFIGURE INTERFACE FASTETHERNET WME-ENABLE .....	25
CONFIGURE INTERFACE FASTETHERNET AUTO-NEGOTIATION .....	25
CONFIGURE IP DEFAULT-GATEWAY .....	26
CONFIGURE IP MTU .....	26
CONFIGURE IP SSH ENABLE .....	27
CONFIGURE IP SSH DISABLE .....	27
CONFIGURE IP SSH AUTHENTICATION-RETRIES .....	28
CONFIGURE IP TELNET ENABLE .....	28
CONFIGURE IP TELNET DISABLE .....	29
CONFIGURE IP VLAN .....	29
CONFIGURE MAC-FILTER LIST ADD-MAC .....	29
CONFIGURE MAC-FILTER LIST NEW .....	30
CONFIGURE MAC-FILTER LIST REMOVE-LIST .....	31
CONFIGURE MAC-FILTER LIST REMOVE-MAC .....	31
CONFIGURE MESH CONNECTIVITY_TEST .....	31
CONFIGURE MESH MODE .....	32
CONFIGURE MESH NETWORK-ID .....	33
CONFIGURE MESH PRIVACY .....	33
CONFIGURE MESH REROUTE-NOW .....	34
CONFIGURE MESH STAND-ALONE .....	34
CONFIGURE MESH STAND-ALONE-PASSPHRASE .....	35

CONFIGURE MESH STAND-ALONE-PASSPHRASE .....	35
CONFIGURE PRIVACY WEP SSID AUTH-TYPE .....	35
CONFIGURE PRIVACY WEP SSID DEFAULT-KEY .....	36
CONFIGURE PRIVACY WEP SSID INDEX .....	36
CONFIGURE PRIVACY WPA SSID .....	37
CONFIGURE RADIUS .....	38
CONFIGURE RADIUS INTERIM-INTERVAL .....	39
CONFIGURE RADIUS RETRANSMIT-MAX-COUNT .....	39
CONFIGURE RADIUS RETRANSMIT-WAIT .....	39
CONFIGURE RETRY-PRIMARY-INTERVAL .....	40
CONFIGURE SNMP PORT .....	40
CONFIGURE SNMP ROCOMMUNITY .....	41
CONFIGURE SNMP RWCOMMUNITY .....	41
CONFIGURE SSID .....	41
CONFIGURE SSID BAND-STEERING .....	42
CONFIGURE SSID FIXED-RATE .....	43
CONFIGURE SSID PRIVACY-METHOD .....	44
CONFIGURE SSID REMOVE .....	44
CONFIGURE SSID RENAME .....	45
CONFIGURE SSID TYPE .....	45
CONFIGURE SSID VLAN .....	45
CONFIGURE SYSTEM CLOCK .....	46
CONFIGURE SYSTEM HOSTNAME .....	46
CONFIGURE SYSTEM INACTIVITY-TIMEOUT .....	47
CONFIGURE SYSTEM LOGGING DESTINATION CLI .....	47
CONFIGURE SYSTEM LOGGING DESTINATION HISTORY .....	48
CONFIGURE SYSTEM LOGGING DESTINATION REMOTE .....	48
CONFIGURE SYSTEM LOGGING DESTINATION SERIAL .....	49
CONFIGURE SYSTEM LOGGING MODULE .....	50
CONFIGURE SYSTEM LOGGING TEST-MESSAGE .....	50
CONFIGURE SYSTEM TIMEZONE .....	51
CONFIGURE SYSTEM WEB-SERVICE .....	52
CONFIGURE TRAP-NOTIFY-FILTER .....	52
CONFIGURE TRAP-TARGET ADD .....	53
CONFIGURE TRAP-TARGET REMOVE .....	54
CONFIGURE USERNAME .....	54
CONFIGURE USERNAME MODIFY .....	55
COPY RUNNING-CONFIG STARTUP-CONFIG .....	56
DELETE STARTUP-CONFIG .....	56
EXPORT STARTUP-CONFIG .....	56
EXPORT SYSTEM-BACKUP .....	57
IMPORT IMAGE .....	57
IMPORT STARTUP-CONFIG .....	58
IPRF-CLIENT .....	58
IPRF-SERVER .....	59
PING .....	59
RELOAD .....	60
SHOW ASSOCIATED-STATIONS .....	60
SHOW DEFAULT-CONFIG .....	60
SHOW INTERFACE DOT11RADIO .....	61
SHOW INTERFACE DOT11RADIO FRINGE_LIST .....	61
SHOW INTERFACE DOT11RADIO FRINGE_PARAMS .....	62
SHOW INTERFACE DOT11RADIO PARAMS .....	62
SHOW INTERFACE DOT11RADIO SITE-SURVEY .....	63

SHOW INTERFACE DOT11RADIO STATS .....	63
SHOW INTERFACE DOT11RADIO WME .....	63
SHOW INTERFACE FASTETHERNET .....	64
SHOW INTERFACE FASTETHERNET STATS .....	64
SHOW INTERFACE SSIDS .....	65
SHOW INTERFACE WIFI-STATS .....	65
SHOW IP ADDRESS .....	66
SHOW IP PARAMS .....	66
SHOW LOGGED-IN-USERS.....	66
SHOW MAC-FILTER INDICES .....	67
SHOW MAC-FILTER LIST .....	67
SHOW MANUFACTURE-DETAILS .....	67
SHOW MESH PARAMS .....	68
SHOW MESH ROUTE .....	68
SHOW MESH STAND-ALONE .....	69
SHOW PRIVACY WEP .....	69
SHOW PRIVACY WEP PARAMS .....	69
SHOW PRIVACY WPA .....	70
SHOW RADIUS .....	70
SHOW RUNNING-CONFIG .....	71
SHOW SOFTWARE-BANKS .....	71
SHOW SNMP COMMUNITIES .....	71
SHOW SPECTRUM-MANAGEMENT CLEAR-COUNT-PERCENT .....	72
SHOW SPECTRUM-MANAGEMENT DOA .....	72
SHOW SSID BAND-STEERING .....	73
SHOW SSID PARAMS .....	73
SHOW STARTUP-CONFIG.....	73
SHOW SYSTEM CLOCK .....	74
SHOW SYSTEM COUNTRY-CODE .....	74
SHOW SYSTEM INACTIVITY-TIMEOUT .....	74
SHOW SYSTEM LOGGING DESTINATIONS .....	75
SHOW SYSTEM LOGGING HISTORY .....	75
SHOW SYSTEM LOGGING MODULES .....	76
SHOW SYSTEM NTP .....	76
SHOW SYSTEM SYSTEM-BACKUP .....	76
SHOW SYSTEM TEMPERATURE .....	77
SHOW SYSTEM TIMEZONE .....	77
SHOW SYSTEM UPTIME .....	77
SHOW SYSTEM VERSION .....	78
SHOW SYSTEM WEB-SERVICE .....	78
SHOW TRAP-NOTIFY-FILTERS .....	79
SHOW USERS .....	79



# 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 devices.
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 by using a specific command. For example,

```
/configure ip telnet {enable | disable}
```

In this case the configure command enables or disables the use of telnet server, 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 NetPointPro 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 an attached SSID to interface 0, execute the following command with the remove option:

```
ap> /configure interface dot11radio 0 ssid 2 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
```

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

Each NetPoint Pro device uses multiple radio interfaces to communicate with other NetPoint Pro devices and customer stations. The actual type of radio interfaces available is dependent on the model of the NetPoint Pro device. 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
NetPoint Pro n	800001	xRF 2.4GHz	xRF 5 GHz

Only 5.4 Ghz and 5.8 Ghz interfaces are defined as 802.11a backhaul radio interfaces, by default. All 2.4 Ghz 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 4.0 that you use to configure and manage your NetPoint Pro access point. The commands are listed alphabetically.

#### CONFIGURE INTERFACE DOT11RADIO AIRTIME-FAIRNESS

**Function:** Enables or disabled the airtime-fairness feature which is responsible for an equal division of throughput between associated Wi-Fi clients.

**Command Syntax:** `/configure interface Dot11Radio <interface number> airtime-fairness { enable | disable }`

**Command Description:**

Parameter	Value
enable   disable	Enable – enables Airtime-Fairness on the specified interface Disable – Disables Airtime-Fairness on the specified interface

**Example:** `/configure interface Dot11Radio 0 airtime-fairness enable`

**Permission Level:** admin

**Related Commands:**

`show interface dot11radio params`

#### CONFIGURE INTERFACE DOT11RADIO BEACON-PERIOD

**Function:** Configure 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
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/n interface is 100 (100 msec).

**Example:**             `/configure interface Dot11Radio 0 beacon-period 200`

**Permission Level:**     admin

**Related Commands:**

show interface Dot11Radio  
show interface Dot11Radio params

## CONFIGURE INTERFACE DOT11RADIO CHANNEL

**Function:**             Configure 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/n) 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>}`

**Command Description:**

Parameter	Value														
interface number	Radio interface number. Depending on the unit, the value can be set to 0 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.														
<channel number>   default   auto	Channel and Frequencies IEEE 802.11b/g/n:  <table style="margin-left: auto; margin-right: auto;"> <tbody> <tr> <td>1– 2412 Mhz</td> <td>8– 2447 Mhz</td> </tr> <tr> <td>2– 2417 Mhz</td> <td>9– 2452 Mhz</td> </tr> <tr> <td>3– 2422 Mhz</td> <td>10– 2457 Mhz</td> </tr> <tr> <td>4– 2427 Mhz</td> <td>11– 2462 Mhz</td> </tr> <tr> <td>5– 2432 Mhz</td> <td>12– 2467 Mhz</td> </tr> <tr> <td>6– 2437 Mhz</td> <td>13– 2472 Mhz</td> </tr> <tr> <td>7– 2441 Mhz</td> <td></td> </tr> </tbody> </table> Default value for Dot11Radio 0 is channel 4 (2427 MHz).	1– 2412 Mhz	8– 2447 Mhz	2– 2417 Mhz	9– 2452 Mhz	3– 2422 Mhz	10– 2457 Mhz	4– 2427 Mhz	11– 2462 Mhz	5– 2432 Mhz	12– 2467 Mhz	6– 2437 Mhz	13– 2472 Mhz	7– 2441 Mhz	
1– 2412 Mhz	8– 2447 Mhz														
2– 2417 Mhz	9– 2452 Mhz														
3– 2422 Mhz	10– 2457 Mhz														
4– 2427 Mhz	11– 2462 Mhz														
5– 2432 Mhz	12– 2467 Mhz														
6– 2437 Mhz	13– 2472 Mhz														
7– 2441 Mhz															

<channel number> | default | auto (continue)   Channel and Frequencies for IEEE 802.11a:

36 - 5180 MHz	124 - 5620 MHz
40 - 5200 MHz	128 - 5640 MHz
44 - 5220 MHz	132 - 5660 MHz
48 - 5240 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
108 - 5540 MHz	184 - 4920 MHz
112 - 5560 MHz	188 - 4940 MHz
116 - 5580 MHz	192 - 4960 MHz
120 - 5600 MHz	196 - 4980 MHz

Default channel for 802.11a radio is 100 (5500 MHz).

Channel and Frequencies for 4.9 GHz 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).

**Example:** /configure interface Dot11Radio 0 channel 6

**Permission Level:** admin

**Related Commands:**

show interface Dot11Radio  
show interface Dot11Radio params

### 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.

**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 802.11an backhaul radio interface. For 802.11b/g/n access radio interface, this command defines the distance between the node unit and the client.

These values (SlotTime, AckTimeout, CTSTimeout) are changed according to distance setting and 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 300 meters or less, specify 300.
- For a maximum distances greater than 300 meters, specify the actual distance.
- Specify the same value for all units in the network.

The distance specified for the 802.11b/g/n 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
distance	Distance in meters: 0 – 8192 Default value for 802.11a interface is 300 (300 meters). Default value for 802.11b/g/n interface is 300 (300 meters).

**Example:** `/configure interface Dot11Radio 1 distance 1800`

**Permission Level:** super

**Related Commands:**



```
show interface Dot11Radio
show interface Dot11Radio params
show interface Dot11Radio stats
```

## 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.

**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 FRINGE

**Function:** Disconnecting sta's which are located far away, or interfere with the normal AP operation due to packet drop, low rate and retransmission.

The AP will check last <Buffer size> packet of every STA.

And if the number of packets lower than the packets-threshold, modulation is lower than rate-threshold, AP defines this STA is located fringe area (far from the AP).

Then the AP will send de-association message and in addition the STA will not be able to associate for ban- time <second>.

**Command Syntax:** `/configure interface Dot11Radio <#> fringe ban-time <X> buffer-size <X> packets-threshold <X> rate-threshold <X>`

`/configure interface Dot11Radio <#> fringe enable`

**Command Description:**

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0 or 1. The last interface is used for 5GHz communications and the first radio interface is used for 2.4GHz communications.
ban-time	For how long <sec> to ban the "bad user".

buffer-size	The amount of packet from which "packets-threshold" should be exceeded. Value <1-100>
packets-threshold	How many packets out of "buffer-size" should be under the "rate-threshold". Value <1-100>
rate-threshold	Rate the downstream packet size limit that should be considered as "bad client". 1 - Tx Rate (CCK)    2 - Tx Rate (CCK) 5.5 - Tx Rate (CCK)    6 - Tx Rate (OFDM) 9 - Tx Rate (OFDM)    11 - Tx Rate (CCK) 12 - Tx Rate (OFDM)    18 - Tx Rate (OFDM) 24 - Tx Rate (OFDM)    36 - Tx Rate (OFDM) 48 - Tx Rate (OFDM)    54 - Tx Rate (OFDM)
enable   disable	enable – Enables the Fringe Feature. disable – Disables the Fringe Feature. Default value is disable.

**Example:** /configure interface dot11Radio 0 fringe ban-time 60 buffer-size 70  
packets-threshold 60 rate-threshold 12

**Permission Level:** super

**Related Commands:**

show interface dot11radio fringe\_params  
show interface dot11radio fringe\_list

### CONFIGURE INTERFACE DOT11RADIO GUARD-INTERVAL

**Function:** Configures the guard-interval of the Radio interface.

**Command Syntax:** **configure interface Dot11Radio** <interface number> guard-interval { short | long }

**Command Description:**

Parameter	Value
Guard-interval	Radio guard-interval. Can be set to short (400ns) or set to long (800ns)

**Example:** configure interface Dot11Radio 0 max-assoc 100

**Permission Level:** admin

**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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
maximum associated clients	Maximum number of associated clients: 1-250 The default value is 250.

**Example:** `configure interface Dot11Radio 0 max-assoc 100`

**Permission Level:** super

**Related Commands:**

`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 {auto | b | g | bgnHT40 | a | an | anHT40}`

**Command Description:**

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
auto   b   g   bgn   bgnHT40   a   an   anHT40	Actual available modes are dependent on the radio interface type.  <b>auto</b> – Enables all modes. <b>b</b> – Limits the specified access radio interface to communicate only with 802.11b clients. <b>g</b> – Limits the specified access radio interface to communicate only with 802.11g clients. <b>bgnHT40</b> – Limits the specified access radio interface to communicate only with 802.11 b, 802.11g and 802.11n clients with bandwidth of 40 Mhz. <b>a</b> – Limits the specified access radio interface to communicate only with 802.11a clients. <b>an</b> –Enables the specified radio interface to communicate with 802.11an stations. <b>anHT40</b> –Enables the specified radio interface to communicate with 802.11a stations with bandwidth of 40 Mhz.

**Example:** `configure interface Dot11Radio 0 mode auto`

**Permission Level:** admin

**Related Commands:**

show interface Dot11Radio  
 show interface Dot11Radio params

**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. Interface 1 is used for 5 GHz communication.
enable   disable	enable - enable 802.11h functionality disable - disable 802.11h functionality 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 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 or 1.
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 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
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 SITE-SURVEY**

**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 interface dot11radio site-survey* command. These results can then be used to assist you in selecting the best available channel.

**Command Syntax:** **configure interface Dot11Radio** <interface number> **site-survey**

**Command Description:**

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.

**Example:** configure interface Dot11Radio 0 site-survey

**Permission Level:** super

**Related Commands:**

show interface Dot11Radio site-survey

**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	Radio interface number. Depending on the unit, the value can be set to 0 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
index number	SSID index number: 1-14
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 (Configuring TX Atten to 5 will decrease attenuation by 5 dB).

**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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
pwr	Transmission Power Attenuation (dB): 0-32 The default value is 2 (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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.
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 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:**

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 ENABLE

**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 enable`

**Command Description:**

Parameter	Value
None	

**Example:** `configure ip ssh enable`

**Permission Level:** super

**Related Commands:**

`configure ip ssh enable`  
`configure ip ssh authentication-retries`  
`configure ip vlan`  
`show ip params`

## 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 enable  
 configure ip ssh authentication-retries  
 configure ip vlan  
 show ip params

**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 enable  
 configure ip ssh disable  
 configure ip vlan  
 show ip params

**CONFIGURE IP TELNET ENABLE**

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

**Command Syntax:** `configure ip telnet enable`

**Command Description:**

Parameter	Value
None	

**Example:** `configure ip telnet enable`

**Permission Level:** admin

**Related Commands:**

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 enable`

**Permission Level:** admin

**Related Commands:**

`configure ip telnet enable`  
`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 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:** `configure 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:**

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 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:**  
 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:**  
 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 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 units using WEP security. The WEP key must be defined. AES passphrase – Connects to other NetPoint Pro 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 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 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 {Dot11Radio | disable | force-stay}`

**Command Description:**

Parameter	Value
Dot11Radio   disable   force-stay	Dot11Radio – Enables the mesh stand-alone mode on a specific radio interface. 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 disable.

**Example:** `configure mesh stand-alone disable`

**Permission Level:** super

**Related Commands:**

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  
 show mesh params  
 show mesh stand-alone

**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. 1-14
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 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. 1-14
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 ssid  
show ssid params  
show privacy wep  
show privacy wep params

**CONFIGURE PRIVACY WEP KEY SSID KEY-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. 1-14
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 ssid  
 show ssid params  
 show privacy wep  
 show privacy wep params

**CONFIGURE PRIVACY WPA SSID**

**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** 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: 1-14
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 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.
wpa1   wpa2   wpa2only	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.
enable   disable	An existing SSID index number: 1-14

**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: 1-14
priority number	Define 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 radius interim-interval`  
`configure radius retry-primary-interval`  
`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 RETRANSMIT-MAX-COUNT

**Function:** Defines the Max number of attempts to retransmit a RADIUS message.

**Command Syntax:** `configure radius retransmit-max-count <interval number>`

**Command Description:**

Parameter	Value
interval number	Defines the amount of retransmitting to send to the Radius server 0 – 100 The default value is 3.

**Example:** `configure radius retransmit-max-count 10`

**Permission Level:** super

**Related Commands:**

`show radius`

## CONFIGURE RADIUS RETRANSMIT-WAIT

**Function:** Defines the retransmit wait time of a RADIUS message.

**Command Syntax:** `configure radius retransmit-wait <interval number>`

**Command Description:**

Parameter	Value
interval number	Defines the amount of retransmitting to send to the Radius server 0 – 100

**Example:** configure radius retransmit-wait 10

**Permission Level:** super

**Related Commands:**

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 SNMP PORT

**Function:** Configures the SNMP Port number.

**Command Syntax:** **configure snmp port** <port number>

**Command Description:**

Parameter	Value
Port number	The port number assigned to the SNMP service. Port can be 161 or between 1024 to 6000.

**Example:** configure snmp port 2020

**Permission Level:** admin

**Related Commands:**

configure snmp rwcommunity

show snmp communities

## 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:**

`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:



	1-14
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 <i>configure privacy</i> 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  
 /configure ssid 1 name NPP-1 vlan 0 privacy-method none type bssid

**Permission Level:** admin

**Related Commands:**  
 configure ssid remove  
 show interface ssids  
 show ssid params  
 show privacy wep  
 show privacy wpa

## CONFIGURE SSID BAND-STEERING

**Function:** Configures the Band-Steering Feature. This Feature is used to steer good clients from the 2.4 GHz interface into the 5 GHz interface in-order to use both interfaces and capacity in the most optimal way.

If a Client has a good link and supports the 5 GHz, he will be steered to connect to the 5 GHz Interface.

To display the current parameters of the band-steering, use the *show ssid band-steering* command.

**Command Syntax:** /configure ssid <#> band-steering rssithreshold <X>  
 /configure ssid <#> band-steering suppress\_auth\_count <X>  
 /configure ssid <#> band-steering suppress\_prob\_count <X>  
 /configure ssid <#> band-steering {enable | disable}

**Command Description:**

Parameter	Value
rssithreshold	Specify the RSSI threshold for that a client must meet to be affected by the band-steering feature.
suppress_auth_count	Specify how many authentication requests the AP will receive before answering with an authentication response.
suppress_prob_count	Specify how many probe requests the AP will receive before answering with a probe response.
enable   disable	enable – Enables the Band-steering feature. disable – Disables the Band-steering feature.

**Example:** /configure ssid 1 band-steering rssithreshold -100  
/configure ssid 1 band-steering suppress\_probe\_count 50  
/configure ssid 1 band-steering enable

**Permission Level:** admin

**Related Commands:**

show ssid band-steering

**CONFIGURE SSID FIXED-RATE**

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

**Command Syntax:** **configure ssid** <ssid 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication.																																		
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	<table border="0"> <tr> <td>Transmission Rate:</td> <td>MCS8 - 2 Streams (RC 0x88)</td> </tr> <tr> <td>6 - 1 Stream (RC 0x0B)</td> <td>MCS9 - 2 Streams (RC 0x89)</td> </tr> <tr> <td>9 - 1 Stream (RC 0x0F)</td> <td>MCS10 - 2 Streams (RC 0x8A)</td> </tr> <tr> <td>12 - 1 Stream (RC 0x0A)</td> <td>MCS11 - 2 Streams (RC 0x8B)</td> </tr> <tr> <td>18 - 1 Stream (RC 0x0E)</td> <td>MCS12 - 2 Streams (RC 0x8C)</td> </tr> <tr> <td>24 - 1 Stream (RC 0x09)</td> <td>MCS13 - 2 Streams (RC 0x8D)</td> </tr> <tr> <td>36 - 1 Stream (RC 0x0D)</td> <td>MCS14 - 2 Streams (RC 0x8E)</td> </tr> <tr> <td>48 - 1 Stream (RC 0x08)</td> <td>MCS15 - 2 Streams (RC 0x8F)</td> </tr> <tr> <td>54 - 1 Stream (RC 0x0C)</td> <td>MCS16 - 3 Streams (RC 0x90)</td> </tr> <tr> <td>MCS0 - 1 Stream (RC 0x80)</td> <td>MCS17 - 3 Streams (RC 0x91)</td> </tr> <tr> <td>MCS1 - 1 Stream (RC 0x81)</td> <td>MCS18 - 3 Streams (RC 0x92)</td> </tr> <tr> <td>MCS2 - 1 Stream (RC 0x82)</td> <td>MCS19 - 3 Streams (RC 0x93)</td> </tr> <tr> <td>MCS3 - 1 Stream (RC 0x83)</td> <td>MCS20 - 3 Streams (RC 0x94)</td> </tr> <tr> <td>MCS4 - 1 Stream (RC 0x84)</td> <td>MCS21 - 3 Streams (RC 0x95)</td> </tr> <tr> <td>MCS5 - 1 Stream (RC 0x85)</td> <td>MCS22 - 3 Streams (RC 0x96)</td> </tr> <tr> <td>MCS6 - 1 Stream (RC 0x86)</td> <td>MCS23 - 3 Streams (RC 0x97)</td> </tr> <tr> <td>MCS7 - 1 Stream (RC 0x87)</td> <td></td> </tr> </table>	Transmission Rate:	MCS8 - 2 Streams (RC 0x88)	6 - 1 Stream (RC 0x0B)	MCS9 - 2 Streams (RC 0x89)	9 - 1 Stream (RC 0x0F)	MCS10 - 2 Streams (RC 0x8A)	12 - 1 Stream (RC 0x0A)	MCS11 - 2 Streams (RC 0x8B)	18 - 1 Stream (RC 0x0E)	MCS12 - 2 Streams (RC 0x8C)	24 - 1 Stream (RC 0x09)	MCS13 - 2 Streams (RC 0x8D)	36 - 1 Stream (RC 0x0D)	MCS14 - 2 Streams (RC 0x8E)	48 - 1 Stream (RC 0x08)	MCS15 - 2 Streams (RC 0x8F)	54 - 1 Stream (RC 0x0C)	MCS16 - 3 Streams (RC 0x90)	MCS0 - 1 Stream (RC 0x80)	MCS17 - 3 Streams (RC 0x91)	MCS1 - 1 Stream (RC 0x81)	MCS18 - 3 Streams (RC 0x92)	MCS2 - 1 Stream (RC 0x82)	MCS19 - 3 Streams (RC 0x93)	MCS3 - 1 Stream (RC 0x83)	MCS20 - 3 Streams (RC 0x94)	MCS4 - 1 Stream (RC 0x84)	MCS21 - 3 Streams (RC 0x95)	MCS5 - 1 Stream (RC 0x85)	MCS22 - 3 Streams (RC 0x96)	MCS6 - 1 Stream (RC 0x86)	MCS23 - 3 Streams (RC 0x97)	MCS7 - 1 Stream (RC 0x87)	
Transmission Rate:	MCS8 - 2 Streams (RC 0x88)																																		
6 - 1 Stream (RC 0x0B)	MCS9 - 2 Streams (RC 0x89)																																		
9 - 1 Stream (RC 0x0F)	MCS10 - 2 Streams (RC 0x8A)																																		
12 - 1 Stream (RC 0x0A)	MCS11 - 2 Streams (RC 0x8B)																																		
18 - 1 Stream (RC 0x0E)	MCS12 - 2 Streams (RC 0x8C)																																		
24 - 1 Stream (RC 0x09)	MCS13 - 2 Streams (RC 0x8D)																																		
36 - 1 Stream (RC 0x0D)	MCS14 - 2 Streams (RC 0x8E)																																		
48 - 1 Stream (RC 0x08)	MCS15 - 2 Streams (RC 0x8F)																																		
54 - 1 Stream (RC 0x0C)	MCS16 - 3 Streams (RC 0x90)																																		
MCS0 - 1 Stream (RC 0x80)	MCS17 - 3 Streams (RC 0x91)																																		
MCS1 - 1 Stream (RC 0x81)	MCS18 - 3 Streams (RC 0x92)																																		
MCS2 - 1 Stream (RC 0x82)	MCS19 - 3 Streams (RC 0x93)																																		
MCS3 - 1 Stream (RC 0x83)	MCS20 - 3 Streams (RC 0x94)																																		
MCS4 - 1 Stream (RC 0x84)	MCS21 - 3 Streams (RC 0x95)																																		
MCS5 - 1 Stream (RC 0x85)	MCS22 - 3 Streams (RC 0x96)																																		
MCS6 - 1 Stream (RC 0x86)	MCS23 - 3 Streams (RC 0x97)																																		
MCS7 - 1 Stream (RC 0x87)																																			

**Example:** `configure ssid <ssid number> fixed-rate rate 12`

**Permission Level:** super

**Related Commands:**

`show interface Dot11Radio params`

## 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. 1-14
none   wep   wpa	Defines the basic privacy method of this SSID. none – No privacy wep – WEP privacy wpa – WPA privacy Use the <i>configure privacy</i> command for additional privacy configuration options.

**Example:** `configure ssid 1 privacy-method none`

**Permission Level:** admin

**Related Commands:**

`configure ssid`  
`show ssid params`  
`show privacy wep`

## CONFIGURE SSID REMOVE

**Function:** Deletes the specified SSID.

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

**Command Description:**

Parameter	Value
index number	SSID index number. 1-14

**Example:** `configure ssid 1 remove`

**Permission Level:** admin

**Related Commands:**

`configure ssid`  
`show ssid params`  
`show privacy wap`

## 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. 1-14
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  
show ssid params  
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. 1-14
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 ssid params  
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. 1-14
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  
show ssid params  
show privacy wep  
show privacy wpa

## CONFIGURE SYSTEM CLOCK

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

**Command Syntax:** `configure system clock <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 YYYY – Year

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

```
/configure system clock 072311472007
```

**Permission Level:** admin

**Related Commands:**

show system clock

## CONFIGURE SYSTEM HOSTNAME

**Function:** Defines a new CLI prompt.

**Command Syntax:** `configure system hostname <prompt string>`

**Command Description:**

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

**Example:** /configure system hostname Netronics

**Permission Level:** admin

**Related Commands:**

None

**CONFIGURE SYSTEM 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 system 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 system inactivity-timeout 30

**Permission Level:** admin

**Related Commands:**

show system inactivity-timeout

**CONFIGURE SYSTEM LOGGING DESTINATION 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 system logging destination 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	Messages 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.  
 warning –Emergency, alert, critical, error, warning messages are sent.  
 notice –Emergency, alert, critical, error, warning, notice messages are sent.  
 The default value is emergency.

---

**Example:** `/configure system logging destination cli level critical`

**Permission Level:** super

**Related Commands:**  
 show system logging destinations

## CONFIGURE SYSTEM LOGGING DESTINATION 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 system logging destination 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	Messages sent to the history: 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. warning –Emergency, alert, critical, error, warning messages are sent. notice –Emergency, alert, critical, error, warning, notice messages are sent. The default value is emergency.

---

**Example:** `configure system logging destination history level critical`

**Permission Level:** super

**Related Commands:**  
 show system logging destinations

## CONFIGURE SYSTEM LOGGING DESTINATION REMOTE

**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 system logging destination remote host <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 system logging destination remote host 1.1.1.3 port 514 enable`

**Permission Level:** super

**Related Commands:**

`show system logging destinations`

## CONFIGURE SYSTEM LOGGING DESTINATION SERIAL

**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 system logging destination serial {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	Messages 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. warning – Emergency, alert, critical, error, warning messages are sent.



---

notice –Emergency, alert, critical, error, warning, notice messages are sent.  
The default value is emergency.

---

**Example:** configure system logging destination serial level critical

**Permission Level:** super

**Related Commands:**

show system logging destinations

## CONFIGURE SYSTEM 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 <module-name/all> {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.
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. warning –Emergency, alert, critical, error, warning messages are sent. notice –Emergency, alert, critical, error, warning, notice messages are sent. The default value is error.

---

**Example:** configure system logging module wl-radio level critical

**Permission Level:** super

**Related Commands:**

show system logging modules

## CONFIGURE SYSTEM LOGGING TEST-MESSAGE

**Function:** Sent a test message to the syslog server to verify working functionality.

**Command Syntax:** `configure system logging test-message level <level>`

**Command Description:**

Parameter	Value
level	Messages 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.  
 warning – Emergency, alert, critical, error, warning messages are sent.  
 notice – Emergency, alert, critical, error, warning, notice messages are sent.  
 The default value is emergency.

---

**Example:** configure system logging test-message level notice

**Permission Level:** super

**Related Commands:**  
 show system logging destinations

## CONFIGURE USERNAME

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

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

**Command Description:**

Parameter	Value
ipaddress	IP address of the NTP server.
time	Defines the time interval used to synchronize the unit's system clock with the NTP server (seconds). 60 - 604800
enable   disable	enable – Enables the NTP daemon. disable – Disables the NTP daemon. The default value is disable.

---

**Example:** configure system ntp host 192.168.0.1 interval 10

**Permission Level:** super

**Related Commands:**  
 show system ntp

## CONFIGURE SYSTEM TIMEZONE

**Function:** Configure the timezone.

**Command Syntax:** `/configure system timezone <timezone>` – time-zone string in the format GMT+x or GMT-x or GMT

**Command Description:**

Parameter	Value
timezone	Time-zone string: GMT+x GMT-x GMT where x= integer

**Example:** This example demonstrates how to set the timezone to GMT+2.

```
/configure system timezone GMT+2
```

**Permission Level:** admin

**Related Commands:**

configure system clock

**CONFIGURE SYSTEM WEB-SERVICE**

**Function:** Enable or disable the access to the web service for the configuration or displaying of AP parameters.

**Command Syntax:** **configure system web-service** {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 system web-service enable

**Permission Level:** super

**Related Commands:**

show system web-service

**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: <b>boot</b> – Defines whether the boot category traps are sent <b>interface</b> – Defines whether the interface category traps are sent

---

	<p><b>system</b> – Defines whether the system category traps are sent</p> <p><b>operation</b> – Defines whether the operations category traps are sent</p> <p><b>configuration</b> – Defines whether the configuration category traps are sent</p> <p><b>cli</b> – Defines whether the CLI category traps are sent</p> <p><b>aaa</b> – Defines whether the radius category traps are sent</p> <p><b>sm</b> – Defines whether the sm category traps are sent</p> <p><b>mesh</b> – Defines whether the Mesh category traps are sent</p> <p><b>sta</b> – Defines whether the station category traps are sent</p> <p><b>wifi</b> – Defines whether the Wi-Fi category traps are sent</p>
enable   disable	<p><b>enable</b> – The specified trap category is sent to the trap targets.</p> <p><b>disable</b> – The specified trap category is not sent to the trap targets.</p> <p>The default value is enable for all trap categories except for the station category (sta).</p>

---

**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-target remove  
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-target add  
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> } 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	Password types: password – Defines a CLI non-encrypted user password. encrypted-password – Defines a CLI user with an encrypted 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 password guestpass 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	Password types: password – Defines a CLI non-encrypted user password. encrypted-password – Defines a CLI user with an encrypted 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 password 12345678`

**Permission Level:** super

**Related Commands:**

configure username  
 show default-config  
 show running-config  
 show startup-config  
 show users

## 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

## 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 npp\_config.txt

**Permission Level:** super

**Related Commands:**  
import startup-config  
show startup-config

## EXPORT SYSTEM-BACKUP

**Function:** Exports the entire system configuration, syslog logs & other AP Statistic information to the TFTP server.

**Command Syntax:** export system-backup {tftp | now | interval | enable | disable}

### Command Description:

Parameter	Value
tftp	IP address of the TFTP server.
now	Send system-backup file once to TFTP server.
Interval	Configure the interval time <sec> between each system-backup log file to be outputted to TFTP server.
Enable   disable	Enable or disables the system-backup Feature.

---

**Example:** export system-backup now

**Permission Level:** super

**Related Commands:**  
show system system-backup

## 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 system version

## 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 npp\_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

**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 system uptime  
show software-banks

## 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 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 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication. 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 channel
configure interface Dot11Radio mode
configure interface Dot11Radio service
```

**SHOW INTERFACE DOT11RADIO FRINGE\_LIST**

**Function:** Displays the clients that are currently in the fringe ban-list and how much time left to get out of the ban list.

**Command Syntax:** **show interface dot11radio <#> fringe\_list**

**Command Description:**

Parameter	Value
None	

**Example:** show interface Dot11Radio 0 fringe\_list

**Permission Level:** viewer

**Related Commands:**

```
configure interface dot11radio fringe
show interface dot11radio fringe_params
```

## SHOW INTERFACE DOT11RADIO FRINGE\_PARAMS

**Function:** Displays the fringe parameter. It displays the fringe ban-time, packet-threshold, buffer size, rate threshold and whether Fringe is Enabled or disabled.

**Command Syntax:** `show interface dot11radio <#> fringe_params`

**Command Description:**

Parameter	Value
None	

**Example:** `show interface Dot11Radio 0 fringe_params`

**Permission Level:** viewer

**Related Commands:**

configure interface dot11radio fringe  
show interface dot11radio fringe\_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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication. 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 channel  
configure interface Dot11Radio max-assoc  
configure interface Dot11Radio sensitivity  
configure interface Dot11Radio service  
configure interface Dot11Radio wme-enable

## SHOW INTERFACE DOT11RADIO SITE-SURVEY

**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 interface dot11radio site-survey* command.

**Command Syntax:** **show interface dot11radio** <interface number> **site-survey**

### Command Description:

Parameter	Value
interface number	Radio interface number. Depending on the unit, the value can be set to 0 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication. This parameter is optional. If not specified, the statistics for all radio interfaces are displayed.

**Example:** show interface Dot11Radio 0 site-survey

**Permission Level:** admin

### Related Commands:

configure interface Dot11Radio site-survey

## 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication. 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 or 1. Interface 0 is used for 2.4 GHz communication and Interface 1 is used for 5 GHz communication. 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 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-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 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 enable`

`configure ip telnet enable`

`show ip address`

## 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 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 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 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 reroute-now
- show mesh params

## 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`

## 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 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 ssid  
 show privacy wpa  
 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  
 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 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:**

None

## 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 system version

## 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 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**

- 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 SSID BAND-STEERING**

**Function:** Displays the current configuration of the Band-steering Feature on the AP.

**Command Syntax:** `show ssid band-steering`

**Command Description:**

Parameter	Value
None	

**Example:** `show ssid band-steering`

**Permission Level:** super

**Related Commands:**

configure ssid band-steering

**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:** super

**Related Commands:**

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 CLOCK

**Function:** Display the system clock time and date.

**Command Syntax:** `show system clock`

**Command Description:**

Parameter	Value
None	

**Example:** `show system clock`

**Permission Level:** viewer

**Related Commands:**

configure system clock

## SHOW SYSTEM COUNTRY-CODE

**Function:** Displays the current country code.

**Command Syntax:** `show system country-code`

**Command Description:**

Parameter	Value
None	

**Example:** `show system country-code`

**Permission Level:** admin

**Related Commands:**

None

## SHOW SYSTEM 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 system inactivity-timeout`

**Command Description:**

Parameter	Value
None	

**Example:** show system inactivity-timeout

**Permission Level:** viewer

**Related Commands:**

configure system inactivity-timeout

**SHOW SYSTEM 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 system logging destinations

**Command Description:**

Parameter	Value
None	

**Example:** show system logging destinations

**Permission Level:** viewer

**Related Commands:**

configure system logging destination cli

configure system logging module

**SHOW SYSTEM LOGGING HISTORY**

**Function:** Displays the logging history.

**Command Syntax:** show logging history

**Command Description:**

Parameter	Value
None	

**Example:** show logging history

**Permission Level:** viewer

**Related Commands:**

configure system logging destination history

## SHOW SYSTEM LOGGING MODULES

**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 system logging modules`

**Command Description:**

Parameter	Value
None	

**Example:** `show system logging modules`

**Permission Level:** admin

**Related Commands:**

`configure system logging modules`

## SHOW SYSTEM NTP

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

**Command Syntax:** `show system ntp`

**Command Description:**

Parameter	Value
None	

**Example:** `show system ntp`

**Permission Level:** super

**Related Commands:**

`configure system ntp`

## SHOW SYSTEM SYSTEM-BACKUP

**Function:** Displays the parameters for the system-backup feature, such as interval and tftp server ip.

**Command Syntax:** `show system system-backup`

**Command Description:**

Parameter	Value
None	

**Example:** `show system system-backup`

**Permission Level:** super

**Related Commands:**

Export system-backup

**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 SYSTEM TIMEZONE****Function:** Shows configured timezone.**Command Syntax:** show system timezone**Command Description:**

Parameter	Value
None	

**Example:** This example demonstrates how to display the configured timezone.

show system timezone

**Permission Level:** admin**Related Commands:**

show system clock

**SHOW SYSTEM UPTIME****Function:** Displays time the system has been running since the last restart.**Command Syntax:** show system uptime

**Command Description:**

Parameter	Value
None	

**Example:** show system uptime

**Permission Level:** viewer

**Related Commands:**

None

**SHOW SYSTEM VERSION**

**Function:** Displays the current firmware version and release date

**Command Syntax:** show system version

**Command Description:**

Parameter	Value
None	

**Example:** show system version

**Permission Level:** viewer

**Related Commands:**

None

**SHOW SYSTEM WEB-SERVICE**

**Function:** Displays the current status of the web service.

**Command Syntax:** show system web-service

**Command Description:**

Parameter	Value
None	

**Example:** show system web-service

**Permission Level:** super

**Related Commands:**

configure system web-service

**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-target add  
configure trap-target remove

## 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-filters**

**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 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

# Appendix A

---

## List of Acronyms

<b>Acronym</b>	<b>Explanation</b>
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	Extended 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	<b>Green</b> – There is power to the unit. <b>Unlit</b> – There is no power to the unit.
STAT	<b>Green</b> – The operational status of the unit is normal. <b>Red</b> – The unit is in a failure state. <b>Unlit</b> – There is no power to the unit.
ACT	<b>Green</b> – When the LED is on, there is a communication connection. When the LED is flashing, traffic is flowing through the unit. <b>Unlit</b> – There is no communication connection.
BH	<b>Green</b> – On a Mesh-Gateway, the mesh functionality is activated. On a Mesh-Node, the unit is connected to the mesh. <b>Unlit</b> – 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