Wireless Network Management System

Teldat Dm819-I

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual.

Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Table of Contents

I Related Documents

Teldat Dm772-I Common Configurations for Interfaces

Chapter 1 Wireless Network Management System

1.1 Introduction

The Wireless Network Management System (WNMS) lets you set up and manage a WLAN infrastructure with multiple access points (APs). WNMS uses profiles to ease the task of configuring multiple access points. The system uses the Control and Provisioning of Wireless Access Points Protocol (CAPWAP) for all communication between masters and slaves.

In CAPWAP terminology, the master that holds the configuration for the slaves is also known as an Access Controller (AC). The slaves are also known as Wireless Termination Points (WTPs). The AC serves as a central device to configure and monitor all the access points in a large wireless network infrastructure.

Using CAPWAP, the AC discovers and manages all WTPs inside the wireless network. Each of the WTPs receives a new configuration (i.e., each of them is managed via the WNMS and can no longer be configured externally).

With the WNMS, you can:

- Automatically detect individual access points (APs) and connect them to a WLAN network.
- Load firmware into the APs.
- Load a configuration into the APs.
- Monitor and manage APs.

Please refer to your gateway's data sheet to learn more about the number of APs you can manage with your gateway's WNMS and to view details of the licenses required.

1.2 Terminology

In this document, the terms Access Point, AP and WTP may be used indistinctly to refer to a managed access point. Similarly, the terms Access Controller, AC and controller may be used indistinctly to refer to the access point manager. The term WLAN controller is usually used when some functions of the data or control plane of the managed access point are moved to the WLAN controller. We will avoid using said term in this manual.

Chapter 2 Configuration

2.1 Accessing the Configuration

To access the WNMS configuration menu, enter the **feature wnms** command (main configuration menu).

Example:

```
Config>feature wnms

-- Wireless Network Management System configuration --
WNMS config>
```

2.2 WNMS role

A router can take either of the two roles in a WNMS system:

- AC role: the router configures other access-points.
- WTP role: the router is configured by another management entity that assumes the AC role.

Most of the configuration described in this manual applies to the AC role. No configuration is needed for a router to act as a WTP. As soon as the router receives a DHCP response that includes option **138** (disclosing the AC IP address), it tries to contact the AC so it can be managed. Once managed, it overwrites parts of its configuration (mainly all WLAN configuration, but also some bridge/VLAN configuration parameters apply) to follow the configuration received from the AC.

In some cases, the user may want to have the AC and WTP role in the same router: the router manages other WTPs, and said router's WLAN interface is managed via the profiles configured in the AC role. The **wtp-role** command can be used here to tweak the configuration.

2.3 Configuration profiles

To ease the task of configuring multiple APs, the configuration in the WNMS feature is based on profiles.

An access point, or WTP, has one or more radio interfaces. The following profiles can be assigned to a radio interface in the WTP:

- One radio profile. The radio profile is used to configure parameters associated with a radio interface.
- One or more BSS profiles. The BSS profile is used to configure a wireless network.

The configuration of a BSS profile, however, can also be partially comprised of other profiles:

- One AAA profile. AAA profiles are used to configure AAA parameters used for 802.1X authentication.
- One ACL profile. ACL profiles are used to configure the MAC addresses allowed to connect to a wireless network.

2.4 Global Configuration Commands

This section summarizes the global configuration commands available in the Wireless Network Management System configuration menu.

Command	Function
? (HELP)	Displays the configuration commands or their options.
AAA	Accesses the AAA profile configuration menu.
ACL	Accesses the Access Control List (ACL) profile configuration menu.
ALARM	Configures WNMS alarms.
AUTOPROFILE	The *autoprofile* menu is used to automatically configure a set of WTPs.
BSS	Accesses the BSS profile configuration menu.
CAPWAP	Configures CAPWAP protocol parameters.
ENABLE	Globally enables the WNMS feature.
LED-MODE	Configures the LED mode to be used by all managed access points.
LOST-AC-LIFETIME	Configures the lifetime of a WTP before rebooting once the connection to the AC

	is lost.
NO	Resets parameters to their default value, disables options or deletes the configuration.
RADIO	Accesses the radio profile configuration menu.
WTP	Accesses the WTP configuration menu.
WTP-ROLE	Configures parameters relative to the WTP role.
EXIT	Exits the WNMS configuration menu.

2.4.1 ? (HELP)

Displays the available commands and their options.

Command history:

Release	Modification
11.00.03	This command was introduced.

2.4.2 AAA

Accesses the Authentication, Authorization and Accounting (AAA) profile configuration menu. AAA profiles are used to configure AAA parameters needed for 802.1X authentication.

Syntax:

```
WNMS config>aaa



WNMS AAA config>?
  aaa     AAA profile configuration
  no      Negate a command or set its defaults
  exit
```

Enter **aaa <id>** to configure a particular AAA profile.

Enter **no aaa <id>** to delete a particular AAA profile.

Example:

Access configuration for AAA profile **1:**

```
WNMS AAA config>aaa 1



WNMS AAA-1 config>
```

Example:

Delete AAA profile **1**

```
WNMS AAA config>no aaa 1
```

Command history:

Release	Modification
11.00.03	The "*AAA*" command was introduced as of version 11.00.03.

2.4.3 ACL

Accesses the Access Control List (ACL) profile configuration menu. ACL profiles are used to configure the MAC addresses that can connect to a wireless network.

Syntax:

```
WNMS config>acl



WNMS ACL config>?
```

```
  acl     MAC address access profile configuration
  no      Negate a command or set its defaults
  exit
```

Enter **acl <id>** to configure a given ACL profile.

Enter **no acl <id>** to delete a given ACL profile.

Example:

Access configuration for ACL profile **1.**

```
WNMS ACL config>acl 1



WNMS ACL-1 config>
```

Example:

Delete AAA profile **1.**

```
WNMS ACL config>no acl 1
```

Command history:

Release	Modification
11.00.03	The "*ACL*" command was introduced as of version 11.00.03.

2.4.4 ALARM

Configures alarms in the wireless controller. An alarm is activated when the information reported by the controlled WTPs meets some kind of condition. Every alarm has some specific ELS events defined, which are generated if the alarm is activated or deactivated. If there is no configuration for the alarm, the default values set for the associated condition are used.

Syntax:

```
WNMS config> alarm?
  temperature     Configure an alarm for the temperature reported by the WTPs
```

ALARM TEMPERATURE

Configures the alarm that activates when the temperature reported by a WTP crosses a threshold. In this alarm, ELS event WNMS.08 is generated when the temperature reported by a WTP exceeds the configured threshold, and WNMS.09 when the reported temperature falls below said threshold.

Syntax:

```
WNMS config> alarm temperature threshold <0..100>
```

The default alarm temperature threshold is 50 ºC. Run **no alarm temperature threshold** to configure the default value.

Command history:

Release	Modification
11.00.07, 11.01.02	This command was introduced.

2.4.5 BSS

Accesses the BSS profile configuration menu. BSS profiles are used to configure a wireless network.

Syntax:

```
WNMS config>bss



WNMS BSS config>?
  bss     BSS profile configuration
  no      Negate a command or set its defaults
  exit
```

Enter **bss <id>** to configure a given BSS profile.

Enter **no bss <id>** to delete a given BSS profile.

Example:

Access configuration of BSS profile **1.**

```
WNMS BSS config>bss 1



WNMS BSS-1 config>
```

Example:

Delete BSS profile **1.**

```
WNMS BSS config>no bss 1
```

Command history:

Release	Modification
11.00.03	The "*BSS*" command was introduced as of version 11.00.03.

2.4.6 CAPWAP

Configures parameters relative to the CAPWAP protocol.

Syntax:

```
WNMS config>capwap ?
  change-state-timeout    Timeout for Change State Event Request messages
  data-check-timeout      Timeout for Data Channel Keep Alive messages
  echo-interval           Time between Echo Request messages
  max-retransmissions     Maximum number of retransmissions
  retransmit-interval     Time between retransmissions
  wait-join-timeout       Timeout for Join Request messages
```

CAPWAP CHANGE-STATE-TIMEOUT

Configures the maximum time, in seconds, the AC waits for the Change State Event Request from the WTP after having transmitted a successful Configuration Status Response message. The value is multiplied by the number of WTP radio-modules.

Syntax:

```
WNMS config>capwap change-state-timeout ?
  <0..4294967295>    Value in the specified range
```

Default is 150 seconds.

Example:

Configure Change State timeout to 60 seconds:

```
WNMS config>capwap change-state-timeout 60
```

Command history:

Release	Modification
11.00.06	This command was introduced.
11.01.02	This command was introduced.

CAPWAP DATA-CHECK-TIMEOUT

Configures the number of seconds the AC waits for the Data Channel Keep Alive, required by the CAPWAP machine's Data Check state. The AC resets the state machine if this timer expires prior to transitioning to the next state.

Syntax:

```
WNMS config>capwap  data-check-timeout ?
  <0..4294967295>    Value in the specified range
```

Default is 30 seconds.

Example:

Configure Data Check timeout to 90 seconds:

```
WNMS config>capwap data-check-timeout 90
```

Command history:

Release	Modification
11.00.06	This command was introduced.
11.01.02	This command was introduced.

CAPWAP ECHO-INTERVAL

Configures the minimum time, in seconds, between Echo Request messages sent to the AC joined by the WTP.

Syntax:

```
WNMS config>capwap  echo-interval ?
  <0..4294967295>    Value in the specified range
```

Default is 10 seconds.

Example:

Configure Echo Requests every 40 seconds:

```
WNMS config>capwap echo-interval 40
```

Command history:

Release	Modification
11.00.06	This command was introduced.
11.01.02	This command was introduced.

CAPWAP MAX-RETRANSMISSIONS

Configures the maximum number of retransmissions for a given CAPWAP packet before the link layer considers the peer dead.

Syntax:

```
WNMS config>capwap max-retransmissions ?
  <0..4294967295>    Value in the specified range
```

Default is 5 retransmissions.

Example:

Configure the maximum number of retransmissions to 10.

```
WNMS config>capwap max-retransmissions 10
```

Command history:

Release	Modification
11.00.06	This command was introduced.
11.01.02	This command was introduced.

CAPWAP RETRANSMIT-INTERVAL

Configures the minimum time, in seconds, for a non-acknowledged CAPWAP packet to be retransmitted.

Syntax:

```
WNMS config>capwap retransmit-interval ?
  <0..4294967295>    Value in the specified range
```

Default is 3 seconds.

Example:

Configure the retransmit interval to 10 seconds:

```
WNMS config>capwap retransmit-interval 10
```

Command history:

Release	Modification
11.00.06	This command was introduced.
11.01.02	This command was introduced.

CAPWAP WAIT-JOIN-TIMEOUT

Configures the maximum time, in seconds, the AC waits for the Join Request message from the WTP once the DTLS session has established.

Syntax:

```
WNMS config>capwap wait-join-timeout ?
  <20..4294967295>    Value in the specified range
```

Default is 60 seconds.

Example:

Configure Join timeout to 30 seconds:

```
WNMS config>capwap wait-join-timeout 30
```

Command history:

Release	Modification
11.00.06	This command was introduced.
11.01.02	This command was introduced.

2.4.7 ENABLE

Enables the WNMS feature. Once enabled, the router can manage discovered Access Points.

Syntax:

```
WNMS config>enable
```

Default is WNMS disabled and the router does not manage other Access Points.

Example:

Enable WNMS feature:

```
WNMS config>enable
```

Example:

Disable WNMS feature:

```
WNMS config>no enable
```

Command history:

Release	Modification
11.00.03	The "*enable*" command was introduced as of version 11.00.03.

2.4.8 LED-MODE

Selects the lighting scheme for the slave AP LEDs. This is a global parameter for all managed APs.

Syntax:

```
WNMS config>led-mode ?
  normal     normal behavior
```

```
  minimal    only Status LED blinks once a second
  off        LEDs are off
```

normal	All LEDs show their standard behavior.
minimal	Only the status LED blinks once per second.
off	All LEDs are deactivated.

Default is normal behavior.

Example:

Configure all managed APs to switch off their LEDs:

```
WNMS config>led-mode off
```

Command history:

Release	Modification
11.00.03	The "*led-mode*" command was introduced as of version 11.00.03.

2.4.9 LOST-AC-LIFETIME

Configures the lifetime of a WTP before rebooting once the connection to the AC is lost. If the connection to the AC is lost for the configured lifetime, the WTP reboots.

Syntax:

```
WNMS config>lost-ac-lifetime ?
  forever            WTP never reboots
  <0..2147483647>    time in seconds the WTP waits before rebooting
```

forever	The WTP never reboots.
value	The WTP reboots once the configured value in which there is no connection to the AC is reached.

Default is 60 seconds.

Example:

Configure the WTPs to reboot after 120 seconds of no connection to the AC:

```
WNMS config>lost-ac-lifetime 120
```

Command history:

Release	Modification
11.00.06	The "*lost-ac-lifetime*" command was introduced as of version 11.00.06.
11.01.02	The "*lost-ac-lifetime*" command was introduced as of version 11.01.02.

2.4.10 NO

Resets parameters to their default value, disables options or deletes the configuration.

Syntax:

```
WNMS config>no ?
  aaa          AAA profile configuration
  acl          MAC address access profile configuration
  alarm        Access controller alarm configuration
  bss          BSS profile configuration
  enable       Enables WLC operation
  led-mode     Led mode for all managed WTPs
  radio        Radio profile configuration
  wtp          Wireless Termination Point profile configuration
```

Example:

Disable the WNMS feature:

```
WNMS config>no enable
```

Example:

Delete all configured BSS profiles:

```
WNMS AAA config>no bss
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.4.11 RADIO

Accesses the radio profile configuration menu. The radio profiles are used to configure parameters associated with a radio interface.

Syntax:

```
WNMS config>radio



WNMS radio config>?
  no      Negate a command or set its defaults
  radio    Radio profile configuration
```

Enter **radio <id>** to configure a given radio profile.

Enter **no radio <id>** to delete a given radio profile.

Example:

Access configuration of radio profile **1**:

```
WNMS Radio config>radio 1



WNMS Radio-1 config>
```

Example:

Delete radio profile **1**:

```
WNMS Radio config>no radio 1
```

Command history:

Release	Modification
11.00.03	The "*radio*" command was introduced as of version 11.00.03.

2.4.12 WTP

Accesses the Wireless Termination Point (WTP) configuration menu used to configure parameters associated with a given AP. Radio profiles and BSS profiles are assigned to the different radio interfaces of the AP in the WTP configuration menu.

Syntax:

```
WNMS config>wtp



WNMS WTP config>?
  no      Negate a command or set its defaults
  wtp     Wireless Termination Point profile configuration
  exit
```

Enter **wtp <mac-address>** to configure a given WTP profile.

Enter **no wtp <mac-address>** to delete a given WTP profile.

Example:

Access configuration of AP with MAC address 11-22-33-44-55-66:

```
WNMS WTP config>wtp 11-22-33-44-55-66



WNMS WTP-11-22-33-44-55-66 config>
```

Example:

Delete configuration for AP with MAC address 11-22-33-44-55-66:

```
WNMS WTP config>no wtp 11-22-33-44-55-66
```

Command history:

Release	Modification
11.00.03	The "*wtp*" command was introduced as of version 11.00.03.

2.4.13 WTP-ROLE

Configures parameters relative to the WTP role.

Syntax:

```
WNMS config>wtp-role ?
  ac-address          AC IP address
  bridge-interface    bridge interface to use for WTP role
  managed             manage AP
```

WTP-ROLE AC-ADDRESS

Configures the IP address for the AC. This command can be used if the AC IP address is not obtained via DHCP.

Syntax:

```
WNMS config>wtp-role ac-address <ipv4>
```

Default is no IP address configured for the AC.

Example:

Configure IP address 10.10.10.1 as the AC address:

```
WNMS config>wtp-role ac-address 10.10.10.1
```

Command history:

Release	Modification
11.01.00	This command was introduced.

WTP-ROLE BRIDGE-INTERFACE

Configures the bridge interface to use for WLAN interfaces when acting as a WTP.

The WTP, once managed, puts all WLAN BSSs in a bridge. This bridge must be precreated in the WTP configuration. If more than one bridge exists in said configuration, this command can be used to specify the bridge interface the WLAN BSSs should be part of.

Default is the first bridge interface found is used.

Example:

Use bridge interface bvi1:

```
WNMS config>wtp-role bridge-interface bvi1
```

Command history:

Release	Modification
11.01.00	This command was introduced.

WTP-ROLE MANAGED

Enables WTP role. Usually, the AP will act as a WTP as soon as it receives an AC IP address. However, when the AC has WLAN interfaces, and the user wants to manage them via the AC configuration, he/she must explicitly enable management (for WLAN interfaces) from the AC role.

Default is WTP role unmanaged.

Example:

AC role to manage the WLAN interfaces:

```
WNMS config>wtp-role managed
```

Command history:

Release	Modification
11.01.00	This command was introduced.

2.4.14 EXIT

Exits the WNMS configuration menu.

Syntax:

```
WNMS config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.5 AAA profiles

AAA profiles are used to configure AAA parameters used for 802.1X authentication. Enter **AAA <id>** (AAA configuration menu) to configure a particular AAA profile.

Syntax:

```
WNMS config>aaa



WNMS AAA config>?
  aaa     AAA profile configuration
  no      Negate a command or set its defaults
  exit
```

Example:

Access configuration of AAA profile 1:

```
WNMS config>aaa



WNMS AAA config>aaa 1



WNMS AAA-1 config>
```

The following table summarizes the AAA profile commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
NO	Resets parameters to their default value, disables options or deletes the configuration.
RADIUS-SERVER	Configures a RADIUS server.
EXIT	Exits the AAA profile configuration menu.

2.5.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*? (HELP)*" command was introduced as of version 11.00.03.

2.5.2 NO

Resets parameters to their default value, disables options or deletes the configuration.

Example:

Delete a RADIUS server with IP address 192.168.1.1:

```
WNMS AAA-1 config>no radius-server ip-address 192.168.1.1
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.5.3 RADIUS-SERVER

Configures a RADIUS server to be used for 802.1X authentication. The server IP address and the shared key between the AC and the authentication server need to be specified.

Syntax:

```
WNMS AAA-x config>radius-server ip-address <addr> secret (plain|ciphered|ciphered-unique) <pwd>
```

addr	IP address of the RADIUS server.
plain	Choose this option to enter the shared key unciphered.
ciphered	Choose this option to enter the shared key ciphered.
ciphered-unique	Choose this option to enter the shared key ciphered with a password that is unique for a particular router.
pwd	Shared key between AC and the authentication server.

Example 1:

Configure a RADIUS server at ip address 192.168.1.1, with shared key *whatever*.

```
WNMS AAA-1 config>radius-server ip-address 192.168.1.1 secret plain whatever
```

Command history:

Release	Modification
11.00.03	The "*radius-server*" command was introduced as of version 11.00.03.

2.5.4 EXIT

Exits the AAA profile configuration menu.

Syntax:

```
WNMS AAA-x config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.6 ACL profiles

ACL profiles are used to configure the MAC addresses that may connect to a wireless network. Enter **ACL <id>** (ACL configuration menu) to configure a particular ACL.

Syntax:

```
WNMS config>acl



WNMS ACL config>?
  acl     MAC address access profile configuration
  no      Negate a command or set its defaults
  exit
```

Example:

AAA profile 1 access configuration:

```
WNMS config>acl



WNMS ACL config>acl 1



WNMS ACL-1 config>
```

The following table summarizes the ACL profile commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
ENABLE	Enables MAC Access Control.
MAC-ADDRESS	Adds a MAC address to the list of permitted MACs.
NO	Resets parameters to their default value, disables options or deletes the configuration.
EXIT	Exits the AAA profile configuration menu.

2.6.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*?(HELP)*" command was introduced as of version 11.00.03.

2.6.2 ENABLE

Enables MAC Access Control. Only explicitly allowed MAC addresses can connect to the wireless network.

Syntax:

```
WNMS ACL-x config>enable
```

Default is MAC access control enabled.

Example:

Enable MAC access control:

```
WNMS ACL-1 config>enable
```

Command history:

Release	Modification
11.00.03	The "*enable*" command was introduced as of version 11.00.03.

2.6.3 MAC-ADDRESS

Adds a MAC address to the list of permitted MACs.

Syntax:

```
WNMS ACL-x config>mac-address <mac>
```

Example:

Allow MAC 11-22-33-44-55-66 to connect to the wireless network:

```
WNMS ACL-1 config>mac-address 11-22-33-44-55-66
```

Command history:

Release	Modification
11.00.03	The "*mac-address*" command was introduced as of version 11.00.03.

2.6.4 NO

Resets parameters to their default value, disables options or deletes the configuration.

Example:

Disable MAC access control:

```
WNMS ACL-1 config>no enable
```

Example:

Deny access to previously allowed MAC 11-22-33-44-55-66:

```
WNMS ACL-1 config>no mac-address 11-22-33-44-55-66
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.6.5 EXIT

Exits the ACL profile configuration menu.

Syntax:

```
WNMS ACL-x config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.7 BSS profiles

BSS profiles are used to configure a wireless network. Enter **BSS <id>** (BSS configuration menu) to configure a particular BSS profile.

Syntax:

```
WNMS config>bss



WNMS BSS config>?
  bss     BSS profile configuration
  no      Negate a command or set its defaults
  exit
```

Example:

Access configuration for BSS profile 1:

```
WNMS config>bss


WNMS BSS config>bss 1


WNMS BSS-1 config>
```

The following table summarizes the BSS profile commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
AAA-PROFILE	Assigns an AAA profile to the BSS.
ACCESS-CONTROL-PROFILE	Assigns an ACL profile to the BSS.
AKM	Configures the authentication key management policy to use in the BSS.
ARP-PROCESSING	Enables ARP processing.
BAND-STEERING	Configures band-steering.
BLACKLIST	Configures blacklisting parameters.
CIPHER	Configures the cipher suite to use in the BSS.
CLIENT-ISOLATION	Enables isolation of the stations connected to an access point.
KEY	Configures the WEP keys.
MAX-ASSOCIATIONS	Configures the maximum number of stations that can be simultaneously associated with the BSS.
NO	Resets parameters to their default value, disables options or deletes the configuration.
PREAUTHENTICATION	Enables pre-authentication.
PRIVACY-INVOKED	Enables security in the BSS.
RSN	Configures the robust security network (RSN) to be used in the BSS.
RX-SHAPING	Selects a bandwidth limitation in reception.
SSID	Configures the network identifier (SSID) to be used.
SSID-SUPPRESS	Hides the SSID in the beacon frames.
TX-SHAPING	Selects a bandwidth limitation in transmission.
VLAN	Configures the VLAN identifier associated with the BSS.
WMM	Enables the QoS feature.
WPA-PSK	Configures the pre-shared key to use in robust security networks (WPA/WPA2).
EXIT	Exits the BSS profile configuration menu.

2.7.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*? (Help)*" command was introduced as of version 11.00.03.

2.7.2 AAA-PROFILE

Assigns an AAA profile to the BSS.

Syntax:

```
WNMS BSS-x config>aaa-profile ?
  <1..2147483647>    Value in the specified range
```

Example:

Assign AAA profile1 to the BSS profile:

```
WNMS BSS-1 config>aaa-profile 1
```

Note

The AAA profile must be created before it can be assigned to a BSS profile.

Command history:

Release	Modification
11.00.03	The "*AAA-profile*" command was introduced as of version 11.00.03.

2.7.3 ACL-PROFILE

Assigns an ACL profile to the BSS.

Syntax:

```
WNMS BSS-x config>acl-profile ?
  <1..2147483647>    Value in the specified range
```

Example:

Assign ACL profile 1 to the BSS profile:

```
WNMS BSS-1 config>acl-profile 1
```

Note

The ACL profile must be created before it can be assigned to a BSS profile.

Command history:

Release	Modification
11.00.03	The "*acl-profile*" command was introduced as of version 11.00.03.

2.7.4 AKM

Configures the Authentication Key Management (AKM) to use in BSS.

Syntax:

```
WNMS BSS-x config>akm-suite ?
  dot1x    802.1X authentication with 4-Way Handshake
  psk      Preshared Key with 4-Way Handshake
```

dot1x	802.1X authentication is used to generate the master session key. This master key is later used in conjunction with 4-Way Handshake to obtain the session keys.
psk	A pre-shared key is used to generate the master session key. This master key is later used in conjunction with 4-Way Handshake to obtain the session keys.

No authentication policy or key managed option is configured by default. You need to explicitly configure a policy to create a robust secure network (RSN).

Example:

Configure authentication using 802.1X.

```
WNMS BSS-1 config>akm dot1x
```

Command history:

Release	Modification
11.00.03	The "*AKM*" command was introduced as 11.00.03.

2.7.5 ARP-PROCESSING

Enables ARP processing. ARP processing is a feature that reduces the number of ARP broadcast packets. If the AP finds the requested IP address in the node table, it replaces the destination broadcast MAC address with the client's unicast MAC address. Unicast packets can be transmitted at a faster rate and do not need to be buffered in stations where power save functions are enabled.

Syntax:

```
WNMS BSS-x config>arp-processing
```

Processing is disabled by default.

Example:

Enable ARP processing:

```
WNMS BSS-1 config>arp-processing
```

Command history:

Release	Modification
11.00.03	The "*arp-processing*" command was introduced as of version 11.00.03.

2.7.6 BAND-STEERING

Configures the preferred band for band steering. Not all APs support this function. A dual radio setup is required for it to work, where the same wireless network is configured on both radio modules (but in different frequency bands).

Initial probe requests in the non-preferred band are deferred so that the client connects to the preferred band. This command is usually employed to move clients that support both bands from the crowded 2.4 GHz band to the less populated 5 GHz band.

Syntax:

```
WNMS BSS-x config>band-steering ?
  2.4GHz    Prefer 2.4 GHz band
  5GHz      Prefer 5 GHz band
```

2.4GHz	Prefer 2.4 GHz band.
5GHz	Prefer 5 GHz band.

Band steering is disabled by default.

Example:

Configure band steering so that it preferably selects the 5GHz band:

```
WNMS BSS-1 config>band-steering 5GHz
```

Example:

Disable band steering:

```
WNMS BSS-1 config>no band-steering
```

Command history:

Release	Modification
11.00.03	The "*band-steering*" command was introduced as of version 11.00.03.
11.01.02	Option 2_4GHz is obsolete. This has changed to 2.4GHz.

2.7.7 BLACKLIST

Enables blacklisting to identify clients that attempt to access the network without proper authorization and blocks them for a certain amount of time. A client is blocked if the number of unsuccessful login attempts within a specified time exceeds a certain count. This threshold value and the duration of the block time can be configured. A client can also be blocked permanently for security reasons.

A blocked client is blocked in all APs managed by the AC for the BSS concerned. This way, they are not able to con-

nect to that BSS through another AP in a different radio cell.

Syntax:

```
WNMS BSS-x config>blacklist ?
  <cr>         Enable blacklisting features
  attempts     Number of failed authentications before blacklisting
  time         Time window to consider failed authentications to blacklist a station
  blocktime    Time a station spends blacklisted
  station      Blacklist a station
```

BLACKLIST <cr>

Enables dynamic blacklisting.

Dynamic blacklisting is disabled by default.

Command history:

Release	Modification
11.00.03	The "*blacklist*" command was introduced as of version 11.00.03.

BLACKLIST ATTEMPTS

Configures the number of failed authentications during the time specified that make a client be blacklisted.

Syntax:

```
WNMS BSS-x config>blacklist attempts <1..255>
```

Command history:

Release	Modification
11.00.03	This command was introduced.

Default is 10 attempts.

BLACKLIST TIME

Configures the time it takes for the blacklisting option to be exercised. If a station fails to authenticate within the configured number of attempts during this time interval, it is blacklisted.

Syntax:

```
WNMS BSS-x config>blacklist time <1s..65535s>
```

Default is 60 seconds.

Command history:

Release	Modification
11.00.03	This command was introduced.

BLACKLIST BLOCKTIME

Configures the time a station remains blacklisted.

Syntax:

```
WNMS BSS-x config>blacklist blocktime <0s..65535s>
```

Default is 500 seconds.

Example:

Enable dynamic blacklisting and configure 3 failed attempts in 50 seconds to blacklist a client. The client will remain blacklisted for 600 seconds:

```
WNMS BSS-1 config>blacklist
WNMS BSS-1 config>blacklist attempts 3
WNMS BSS-1 config>blacklist time 50
WNMS BSS-1 config>blacklist blocktime 600
```

Command history:

Release	Modification
11.00.03	This command was introduced.

BLACKLIST STATION

Blacklists a client station in a wireless network. The blacklisted client station will not be able to connect to the specified wireless network. Blacklisting must be enabled in the BSS.

Syntax:

```
WNMS BSS-x config>blacklist station <mac>
```

Default is no stations blacklisted.

Example:

Blacklist client station with MAC 22-33-44-55-66-77.

```
WNMS BSS-1 config>blacklist
WNMS BSS-1 config>blacklist station 22-33-44-55-66-77
```

Command history:

Release	Modification
11.00.03	This command was introduced.

2.7.8 CIPHER

Configures the cipher suite to use in the BSS.

Syntax:

```
WNMS BSS-x config>cipher ?
  aes-ccmp    AES-CCMP
  tkip        TKIP
```

aes-ccmp	AES-CCMP is used to encrypt the data.
tkip	TKIP is used to encrypt the data.

More than one cipher suite can be configured. If more than one cipher suite is set, the client that joins the BSS can select the preferred cipher suite.

If multiple cipher suites are configured, the less secure cipher suite is used to encrypt the group frames (broadcast and multicast frames). The order of the cipher suites, from the least to the most secure, is as follows:

- TKIP
- AES-CCMP

No cipher suite is configured by default. You need to explicitly configure a cipher suite to create a robust secure network (RSN).

Example:

Use AES-CCMP encryption in a BSS:

```
WNMS BSS-1 config>cipher aes-ccmp
```

Example:

Use AES-CCMP and TKIP encryption in a BSS. TKIP encryption is used for group frames:

```
WNMS BSS-1 config>cipher aes-ccmp
WNMS BSS-1 config>cipher tkip
```

Command history:

Release	Modification
11.00.03	The "*cipher*" command was introduced as of version 11.00.03.

2.7.9 CLIENT-ISOLATION

Enables client isolation. If enabled, a client station cannot communicate with any other client station connected to the same Access Point.

Syntax:

```
WNMS BSS-x config>client-isolation
```

This command is disabled by default. WLAN clients can communicate with each other within a radio cell.

Example:

Enable isolation between stations connected to the access point:

```
WNMS BSS-1 config>client-isolation
```

Command history:

Release	Modification
11.00.03	The "*client-isolation*" command was introduced as of version 11.00.03.

2.7.10 KEY <index>

Configures WEP keys.

Syntax:

```
WNMS BSS-x config>key <index> size (40|104) (ascii|hex) (plain|ciphered) <key>
```

index	Index for the key to configure. Values range from 1 to 4.
size	WEP key size. The WEP key can be either 40 or 104 bits long.
ascii	Choose this option to enter the key using ASCII characters. Please note that an ASCII character is equivalent to 8 bits.
hex	Choose this option to enter the key using hexadecimal characters. Please note that a hexadecimal character is equivalent to 4 bits.
plain	Choose this option to enter the WEP key unciphered.
ciphered	Choose this option to enter the WEP key ciphered.
ciphered-unique	Choose this option to enter the WEP key ciphered with a unique password for a particular router.
key	WEP key value.

Example 1:

Configuration for *104-bit* long key *mydumbwepkey2* for index *2*.

```
WNMS BSS-1 config>key 2 size 104 ascii plain mydumbwepkey2
```

Example 2:

Configuration for *40-bit* long key *0x1234567890* for index *4*.

```
WNMS BSS-1 config>key 4 size 40 hex plain 1234567890
```

Command history:

Release	Modification
11.00.03	The "*key <index>*" command was introduced as of version 11.00.03.

2.7.11 KEY DEFAULT

Configures the default WEP key. The default key is used for transmission if WEP is used for encryption in the BSS.

Syntax:

```
WNMS BSS-x config>key default <index>
```

Where index is a value ranging from 1 to 4.

Key index 1 is used by default to transmit frames in a network with WEP.

Example:

Configure key index 3 as the default key:

```
WNMS BSS-1 config>key default 3
```

Command history:

Release	Modification
11.00.03	The "*key default*" command was introduced as of version 11.00.03.

2.7.12 MAX-ASSOCIATIONS

Configures the maximum number of stations that can be simultaneously associated with the BSS. As soon as the configured number is reached, new associations are not permitted.

Syntax:

```
WNMS BSS-x config>max-associations [hard|soft]
  <1..254>    Value in the specified range
```

hard

Enter the maximum number of clients that can be connected to this wireless network (SSID).

The maximum number of clients that can connect to a BSS depends on the specifications of the respective WLAN module. If the configured number of associations is reached, new associations are not allowed.

Possible values are numbers between 1 and 256.

Default is 32.

soft

Not all devices support this function.

To avoid a radio module from being fully utilized, set a *soft* restriction on the number of connected clients. If this number is reached, new connection queries are initially rejected. If the client cannot find another wireless network and, therefore, repeats its query, the connection is accepted. Queries are only definitively rejected when the *hard limit* is reached.

Soft limit must be equal to or less than hard limit.

Default is 28.

To disable this function, set the soft limit and hard limit to identical values.

Example:

Set the hard limit value for clients allowed in the BSS to 5:

```
WNMS BSS-1 config>max-associations hard 5
```

Command history:

Release	Modification
11.00.03	This command was introduced.

2.7.13 NO

Resets parameters to their default value, disables options or deletes the configuration.

Example:

Disable ARP processing:

```
WNMS BSS-1 config>no arp-processing
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.7.14 PREAUTHENTICATION

Enables EAP preauthentification. If preauthentication is enabled, WLAN clients who support this feature and are already connected to one access point, can carry out 802.1X authentication to a second AP using the connection established to the first AP. This makes roaming from the first AP to the second much faster.

This parameter only applies if 802.1X authentication is used in the wireless network (WPA Enterprise or WPA2 Enterprise).

Syntax:

```
WNMS BSS-x config>preauthentication
```

Default is enabled.

Example:

Enable preauthentication:

```
WNMS BSS-1 config>preauthentication
```

Command history:

Release	Modification
11.00.03	The "*preauthentication*" command was introduced as of version 11.00.03.

2.7.15 PRIVACY-INVOKED

Enables security in the BSS. If no robust security policy is enabled through the **rsn** command, WEP is used.

Syntax:

```
WNMS BSS-x config>privacy-invoked
```

It is disabled by default.

Example:

Enable security in the BSS:

```
WNMS BSS-1 config>privacy-invoked
```

Command history:

Release	Modification
11.00.03	The "*privacy-invoked*" command was introduced as of version 11.00.03.

2.7.16 RATES

Configures basic and supported rates in BSS.

Basic rates are mandatory rates that must be supported by all stations connecting to BSS.

Supported rates are all rates that can be used for communication within BSS.

Syntax:

```
WNMS BSS-x config>rates [2.4GHz|5GHz] [basic|supported] <rates>
```

2.4GHz	Configures rates for the 2.4 GHz band.
5GHz	Configures rates for the 5 GHz band.
basic	Configures basic rates. Basic rates are mandatory: any station willing to connect to the AP must support all basic rates.
supported	Configures rates supported by the AP in the BSS.
rates	List of valid rates, in Mbps.

The valid rates for 2.4 GHz are:

- 1, 2, 5.5, 6, 8, 11, 12, 18, 14, 36, 48, 54.

The valid rates for 5 GHz are:

- 6, 9, 12, 18, 24, 36, 48, 54.

Default for basic 2.4 GHz rates: 1, 2, 5.5, 11 Mbps.

Default for supported 2.4 GHz rates: 1, 2, 5.5, 11, 12, 18, 24, 36, 48, 54 Mbps.

Default for basic 5 GHz rates: 6, 12, 24 Mbps.

Default for supported 5 GHz rates: 6, 9, 12, 18, 24, 36, 48, 54 Mbps.

Example:

Disable 802.11b rates (1, 2, 5.5 and 11 Mbps):

```
WNMS BSS-1 config>rates 2.4GHz basic 12 18
WNMS BSS-1 config>rates 2.4GHz supported 12 18 24 36 48 54
```

Command history:

Release	Modification
11.00.06	The "*rates*" command was introduced as of version 11.00.06.
11.01.02	The "*rates*" command was introduced as of version 11.01.02.
11.01.02	Option 2_4GHz obsolete, changed to 2.4GHz.

2.7.17 RSN

Configures the type of robust security network (RSN) to be used in the BSS.

Syntax:

```
WNMS BSS-x config>rsn ?
  wpa     WPA Information Element
  wpa2    WPA2 (802.11i) Information Element
```

wpa	Enables WPA in the BSS.
wpa2	Enables WPA2 in the BSS.

Both options can be selected. If both WPA and WPA2 are enabled, the access point sends the information elements corresponding to both security policies in the beacon frames. Clients joining the wireless network can select their preferred security policy.

No robust security policy is configured by default.

Example:

Configure BSS to admit WPA and WPA2:

```
wlan3/0 bss config>rsn wpa
wlan3/0 bss config>rsn wpa2
```

Command history:

Release	Modification
11.00.03	The "*rsn*" command was introduced as of version 11.00.03.

2.7.18 RX-SHAPING

Configures a bandwidth limitation per associated station in reception (client to Access Point).

Syntax:

```
WNMS BSS-x config>rx-shaping ?
  <0..2147483647>    Value in the specified range
```

This value is configured in bits per second.

Default is no bandwidth limitation.

Example:

Configure a limitation of 10 Mbps per client in reception:

```
WNMS BSS-1 config>rx-shaping 10485760
```

Command history:

Release	Modification
11.00.03	The "*rx-shaping*" command was introduced as of version 11.00.03.

2.7.19 SSID

Configures the name of the wireless network (SSID: Service Set Identifier). The name must be an ASCII string of up to 32 characters.

Syntax:

```
WNMS BSS-x config>ssid  ?
  <1..32 chars>    Text
```

The default value is default.

Example:

Configure Guest_WLAN as network name:

```
WNMS BSS-1 config>ssid Guest_WLAN
```

Command history:

Release	Modification
11.00.03	The "*SSID*" command was introduced as of version 11.00.03.

2.7.20 SSID-SUPPRESS

Removes the SSID from beacon frames, hiding the network name. This is considered a legacy security method, since SSID is still conveyed in other unencrypted frames.

Syntax:

```
WNMS BSS-x config>ssid-suppress
```

The network identifier sent in beacon frames by default.

Example:

Hide the network name in beacon frames:

```
WNMS BSS-1 config>ssid-suppress
```

Command history:

Release	Modification
11.00.03	The "*ssid-suppress*" command was introduced as of version 11.00.03.

2.7.21 TX-SHAPING

Configures a bandwidth limitation per associated station in transmission (Access Point to client).

Syntax:

```
WNMS BSS-x config>tx-shaping ?
  <0..2147483647>    Value in the specified range
```

This value is configured in bits per second.

Default is no bandwidth limitation.

Example:

Configure a limitation of 10 Mbps per client in transmission:

```
WNMS BSS-1 config>tx-shaping 10485760
```

Command history:

Release	Modification
11.00.03	The "*tx-shaping*" command was introduced as of version 11.00.03.

2.7.22 VLAN

Configures the VLAN identifier associated with the BSS.

Syntax:

```
WNMS BSS-x config>vlan ?
  <2..4095>    Value in the specified range
```

No VLAN is configured by default.

Example:

Use VLAN 10 for traffic associated with this BSS:

```
WNMS BSS-1 config>vlan 10
```

Command history:

Release	Modification
11.00.03	The "*vlan*" command was introduced as of version 11.00.03.

2.7.23 WMM

Enables QoS (Quality of Service) in the wireless network using WMM (Wireless Multi Media). This way, optimum transmission quality is always achieved for time-critical applications.

Syntax:

```
WNMS BSS-x config>wmm
```

WMM is enabled by default.

Example:

Enable WMM:

```
WNMS BSS-1 config>wmm
```

Command history:

Release	Modification
11.00.03	The "*WMM*" command was introduced as of version 11.00.03.

2.7.24 WPA-PSK

Configures the pre-shared key to use for WPA-PSK or WPA2-PSK.

Syntax:

```
wpa-psk passphrase (plain|ciphered|ciphered-unique) <key-value>
```

passphrase	Configures the pre-shared key using an 8 to 63 character long ASCII passphrase. The key to use is obtained through a standard procedure from the configured phrase.
plain	Choose this option to enter the WPA-PSK key unciphered.
ciphered	Choose this option to enter the WPA-PSK key ciphered.
ciphered-unique	Choose this option to enter the WPA-PSK key ciphered with a unique password for a particular router.

key-value	Shared key to use.

No shared key is configured by default.

Example:

Configure the shared key using **"Teldat Wireless LAN"** passphase:

```
WNMS BSS-1 config>wpa-psk passphrase "Teldat Wireless LAN"
```

Command history:

Release	Modification
11.00.03	The "*wpa-psk*" command was introduced as of version 11.00.03.

2.7.25 EXIT

Exits the BSS profile configuration menu.

Syntax:

```
WNMS BSS-x config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.8 Radio profiles

Radio profiles are used to configure parameters associated with a radio interface. Enter **radio <id>** (radio configuration menu) to configure a particular radio profile.

Syntax:

```
WNMS config>radio


WNMS radio config>?
  no       Negate a command or set its defaults
  radio    Radio profile configuration
  exit
```

Example:

Access configuration for radio profile 1:

```
WNMS config>radio


WNMS radio config>radio 1


WNMS Radio-1 config>
```

The following table summarizes the radio profile commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
AIRTIME-FAIRNESS	Enables airtime fairness.
BAND	Selects the frequency band and wireless technology to use.
BANDWIDTH	Configures channel bandwidth.
BEACON	Configures parameters relative to beacon frames.
BURST	Enables burst mode.
CHANNEL-PLAN	Configures radio channels allowed in a frequency band.
COUNTRY	Configures the country where the wireless network is operating. The country code determines the regulations the WLAN interface must comply with. This affects the

	list of allowed channels and the maximum transmission power.
CYCLIC-BACK-GROUND-SCANNING	Enables cyclic-background-scanning.
DESCRIPTION	Configures a description for the radio profile.
FRAGMENT-THRESHOLD	Configures the fragment-threshold.
INSTALLATION	Configures the installation mode to use.
N-SPATIAL-STREAMS	Configures the number of spatial streams to use.
NO	Resets parameters to their default value, disables options or deletes the configuration.
RETRY-LIMIT	Configures the maximum number of retries to transmit a frame before it is considered a failure.
RTS	Configures parameters relative to the use of RTS/CTS control frames.
SHORT-GUARD-INTERVAL	Enables short-guard-interval.
SHUTDOWN	Disables all radio interfaces associated with this radio profile.
EXIT	Exits the radio profile configuration menu.

2.8.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*? (HELP)*" command was introduced as of version 11.00.03.

2.8.2 AIRTIME-FAIRNESS

Enables airtime fairness.

This function is not available for all WTPs.

When enabled, airtime fairness ensures that airtime resources are smartly distributed among connected clients. This way, high throughput clients (e.g., an 802.11n client) do not get penalized because of slower clients (e.g., an 802.11g or 802.11a client) connected to the same access point. Transmissions of slow clients take more air time due to lower rates so, to achieve airtime fairness, faster clients are given more access to the medium.

This feature is only applied to non-prioritized WMM Background Class frames.

Syntax:

```
WNMS Radio-x config>airtime-fairness
```

Default is airtime fairness disabled.

Example:

Enable airtime fairness:

```
WNMS Radio-1 config>airtime-fairness
```

Command history:

Release	Modification
11.00.03	The "*airtime-fairness*" command was introduced as of version 11.00.03.

2.8.3 BAND

Selects the frequency band and wireless technology to use.

Syntax:

```
WNMS Radio-x config>band <band> mode <mode>
```

band	Frequency band to use. It can be 2.4 GHz (option **2.4GHz**) or 5 GHz (option **5GHz**).

mode

Selects the wireless technology that the access point may use.

For **band** = 2.4 GHz

Possible values:

- 11g: the device operates only in compliance with 802.11g. 802.11b clients have no access.
- 11b: the device operates only in compliance with 802.11b and forces all clients to adapt to it.
- 11bg: the device adapts to client technology and operates according to either 802.11b or 802.11g.
- 11bh-long: the device adapts to client technology and operates according to either 802.11b or 802.11g. Only data rates of 1 and 2 Mbps must be supported by all clients (basic rates). This mode is also necessary for Centrino clients if connection problems occur.
- 11bg-short: the device adapts to client technology and operates according to either 802.11b or 802.11g. Data rates 5.5 and 11 Mbps must be supported by all clients (basic rates).
- 11bgn: the device operates according to either 802.11b, 802.11g or 802.11n.
- 11gn: the device operates according to either 802.11g or 802.11n.
- 11n: the device operates only according to 802.11n.

For **band** = 5 GHz

Possible values:

- 11a: the device operates only according to 802.11a.
- 11n: the device operates only according to 802.11n.
- 11an: the device operates according to either 802.11a or 802.11n.
- 11ac: the device operates according to 802.11ac. Only VHT (Very High Throughput) stations compliant with 802.11ac can connect.
- 11anac: the device operates according to either 802.11a, 802.11n or 802.11ac. In this mode, stations that do not comply with the 802.11ac standard can connect.

The access point operates in the 2.4 GHz band and in mode 11bgn by default.

Example:

Configure mode 11an in the 5 GHz band:

```
WNMS Radio-1 config>band 5GHz mode 11an
```

Command history:

Release	Modification
11.00.03	The "*band*" command was introduced as of version 11.00.03.
11.00.06	Modes 11ac and 11anac were introduced.
11.01.02	Modes 11ac and 11anac were introduced.

2.8.4 BANDWIDTH

Configures channel bandwidth.

Syntax:

```
WNMS Radio-x config>bandwidth ?
  20MHz    20 MHz channel width
  40MHz    40 MHz channel width
  80MHz    80 MHz channel width
```

20MHz One 20 MHz channel is used.

40MHz Two 20 MHz channels are combined into one 40 MHz channel. The use of 40 MHz channels may not be possible depending on neighboring wireless networks.

80MHz Four 20 MHz channels are combined into one 80 MHz channel. The use of 80

MHz channels may not be possible depending on neighboring wireless networks.

A 20MHz channel bandwidth is configured by default.

Example:

Configure 40 MHz channels:

```
WNMS Radio-1 config>bandwidth 40MHz
```

Command history:

Release	Modification
11.00.03	The "*bandwidth*" command was introduced as of version 11.00.03.
11.00.06	Bandwidth 80MHz was introduced.
11.01.02	Bandwidth 80MHz was introduced.

2.8.5 BEACON

Configures parameters relative to beacon frames.

Syntax:

```
WNMS Radio-x config>beacon ?
  period    Configures beacon transmission period in time units (TUs)
  dtim      Configures Data Beacon Rate (DTIM)
```

BEACON PERIOD

Configures the interval between beacon frames. Beacon frames are periodically sent by the access point to announce the wireless network characteristics: operating mode, supported speeds, security requirements, etc.

The beacon frame periodicity is indicated in time units. A time unit (TU) is a parameter defined in the IEEE 802.11 standard equivalent to 1024 microseconds.

The configuration of this parameter affects stations in power save mode, having similar implications as those described for the DTIM beacon parameter configuration: the greater the beacon frame periodicity, the more time the stations remain 'asleep'. However, the access point must store a larger amount of frames to be subsequently delivered.

Default is 100 (i.e., a beacon frame is sent every 102.4 milliseconds).

Example:

Send Beacon frames every 300 time units:

```
WNMS Radio-1 config>beacon period 300
```

Command history:

Release	Modification
11.00.03	This command was introduced.

BEACON DTIM

Configures the periodicity, in beacon frames, for the Delivery Traffic Indication Message (DTIM) information element. The DTIM information element is periodically included in beacon frames. It reports that multicast and broadcast frames stored in the access point are going to be sent. This information is used by clients in power save mode so they can listen to the multicast and broadcast frames.

The configuration of this parameter affects stations in power save mode. The higher the value configured, the greater the time a station remains 'asleep' without needing to wake to receive the broadcast and multicast frames. However, bear in mind that high values mean that the access point has to store more frames to be subsequently delivered. If the configured value is high, the access point may be left without resources to store the frames and will consequently drop them.

Default is 2 (i.e., the broadcast and multicast frames are delivered every 2 beacon frames).

Example:

The DTIM information element is sent every three beacon frames:

```
WNMS Radio-1 config>beacon dtim 3
```

Command history:

Release	Modification
11.00.03	This command was introduced.

2.8.6 BURST

Enables burst mode.

Activate this feature to increase the transmission speed for 802.11g through frame bursting. As a result, several packets are sent one after the other without a waiting period. This is particularly effective in 11b/g mixed operation.

If problems occur with older WLAN hardware, do not enable said feature.

Syntax:

```
WNMS Radio-x config>burst
```

Default is disabled.

Example:

Enable burst mode:

```
WNMS Radio-1 config>burst
```

Command history:

Release	Modification
11.00.03	The "*burst*" command was introduced as of version 11.00.03.

2.8.7 CHANNEL-PLAN

Configures the radio channels allowed in a frequency band.

Syntax:

```
WNMS Radio-x config>channel-plan <band>
  auto            Automatic channel plan
  user-defined    User defined channel plan
     add <channel>
```

band	Frequency band to configure. This can be 2.4 GHz (option **2.4GHz**) or 5 GHz (option **5GHz**).
auto	Use this option so the access point automatically selects the available channels.
user-defined	Use this option to explicitly configure the channels available for the access point to use.
add <channel>	Add the specified channel to the list of available channels.

Default is auto channel plan.

Example:

Configure a user defined channel plan for the 2.4 GHz band with channels 1 and 11:

```
WNMS Radio-1 config>channel-plan 2.4GHz user-defined add 1
WNMS Radio-1 config>channel-plan 2.4GHz user-defined add 11
```

Command history:

Release	Modification
11.00.03	The "*channel-plan*" command was introduced as of version 11.00.03.
11.01.02	Option 2_4GHz obsolete, changed to 2.4GHz.

2.8.8 COUNTRY

Configures the country where the wireless network operates. The country code determines the regulations the WLAN interface must comply with. This affects the list of channels allowed and the maximum transmission power.

Syntax:

```
WNMS Radio-x config>country <country-code>
```

Country-code is a two-character string corresponding to the country's ISO code. E.g., the ISO code for the United States of America is US.

Caution

If you misconfigure the country code, you may inadvertently violate the radio regulatory laws that apply in the country you are operating in.

Default country depends on the regulatory domain license.

Example:

Configure the country code for operation in the United States of America:

```
WNMS Radio-1 config>country us
```

Command history:

Release	Modification
11.00.03	The "*country*" command was introduced as of version 11.00.03.

2.8.9 CYCLIC-BACKGROUND-SCANNING

Enables **cyclic-background-scanning**. If enabled, the access point runs a background scan at regular intervals looking for neighboring or rogue access points in the network. This background scanning does not negatively impact access point performance.

Not all devices support this feature.

Syntax:

```
WNMS Radio-x config>cyclic-background-scanning
```

Cyclic-background-scanning is disabled by default.

Example:

Enable cyclic-background-scanning:

```
WNMS Radio-1 config>cyclic-background-scanning
```

Command history:

Release	Modification
11.00.03	The "*cyclic-background-scanning*" command was introduced as of version 11.00.03.

2.8.10 DESCRIPTION

Configures a radio profile description.

Syntax:

```
WNMS Radio-x config>description ?
  <1..255 chars>    Text
```

No description is configured by default.

Example:

Configure description "2.4 GHz band".

```
WNMS Radio-1 config>description "2.4 GHz band"
```

Command history:

Release	Modification
11.00.03	The "*description*" command was introduced as of version 11.00.03.

2.8.11 FRAGMENT-THRESHOLD

Configures the **fragment-threshold**. Frames bigger than the fragment-threshold are fragmented and sent as several smaller frames. Low values are recommended for this field in areas with poor reception and in the presence of radio interference.

Syntax:

```
WNMS Radio-x config>fragment-threshold ?
  <256..2346>    Value in the specified range
```

Default is 2346.

Example:

Configure the fragment-threshold so packets larger than 1500 bytes are fragmented:

```
WNMS Radio-1 config>fragment-threshold 1500
```

Command history:

Release	Modification
11.00.03	The "*fragment-threshold*" command was introduced as of version 11.00.03.

2.8.12 INSTALLATION

Configures the installation mode to use. The installation mode may affect the channels available and the maximum transmission power.

Syntax:

```
WNMS Radio-x config>installation ?
  indoor     Indoor operation
  outdoor    Outdoor operation
  both       Both indoor and outdoor operation
```

indoor	Select this option when the APs are going to be used indoors.
outdoor	Select this option when the APs are going to be used outdoors.
both	Select this option when the APs can be used indoors or outdoors. The more restrictive of indoors and outdoors regulations apply for channel availability and transmit powers.

It is set to indoors by default.

Example:

Configure radio interface to be used outdoors:

```
WNMS Radio-1 config>installation outdoor
```

Command history:

Release	Modification
11.00.03	The "*installation*" command was introduced as of version 11.00.03.

2.8.13 N-SPATIAL-STREAMS

Configures the maximum number of spatial streams to use. This parameter only applies to 802.11n APs. If the AP does not support the number of spatial streams configured, it uses its maximum value.

Syntax:

```
WNMS Radio-1 config>n-spatial-streams ?
  <1..3>    Value in the specified range
```

Default is 3 spatial streams.

Example:

Use 2 spatial streams:

```
WNMS Radio-1 config>n-spatial-streams 2
```

Command history:

Release	Modification
11.00.03	The "*n-spatial-streams*" command was introduced as of version 11.00.03.

2.8.14 NO

Resets parameters to their default value, disables options or deletes the configuration.

Example:

Set fragment-threshold to the default value:

```
WNMS Radio-1 config>no fragment-threshold
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.8.15 RETRY-LIMIT

Configures the maximum number of retries to transmit a frame before it is deemed to have failed.

Syntax:

```
WNMS Radio-x config>retry-limit [long|short] <1..255>
```

short

Maximum number of attempts to send a frame whose length is shorter than, or equal to, the value defined in *RTS THRESHOLD*. After this many failed attempts, the frame is discarded.

Default is 7.

long

Maximum number of attempts to send a frame whose length is greater than the value defined in *RTS THRESHOLD*. After this many failed attempts, the frame is discarded.

Default is 4.

Example:

Configure 3 attempts to send a frame longer than the RTS threshold:

```
WNMS Radio-1 config>retry-limit long 3
```

Command history:

Release	Modification
11.00.03	The "*retry-limit*" command was introduced as of version 11.00.03.

2.8.16 RTS

Configures parameters relative to the use of RTS/CTS control frames.

Syntax:

```
WNMS Radio-x config>rts ?
```

```
  threshold    Packet size to send an RTS
```

RTS THRESHOLD

Configures the threshold to activate the RTS/CTS mechanism to access the medium. When the frame to be sent is greater than the configured threshold, RTS/CTS is used to reserve the medium before sending the frame.

Syntax:

```
WNMS Radio-x config>rts threshold ?
  <1..2347>    Value in the specified range
```

The RTS threshold is 2347 bytes by default.

Example:

Use RTS/CTS for frames bigger than 1500 bytes.

```
WNMS Radio-1 config>rts threshold 1500
```

Command history:

Release	Modification
11.00.03	This command was introduced.

2.8.17 SHORT-GUARD-INTERVAL

Enables **short-guard-interval**. The guard interval is the time between transmitting two symbols. When short-guard-interval is enabled, said interval is reduced from 800 ns to 400 ns. This allows for better speed but can cause more interference between symbols.

Syntax:

```
WNMS config>short-guard-interval
```

Short-guard-interval is enabled by default.

Example:

Disable short-guard-interval:

```
WNMS Radio-1 config>no short-guard-interval
```

Command history:

Release	Modification
11.00.03	The "*short-guard-interval*" command was introduced as of version 11.00.03.
11.01.05	"*Short-guard-interval*" is now enabled by default.

2.8.18 SHUTDOWN

Disables all radio interfaces associated with this radio profile. All radio interfaces that use this radio profile will be disabled.

Syntax:

```
WNMS config>shutdown
```

Radio is enabled by default.

Example:

Disable all radios associated with this profile:

```
WNMS Radio-1 config>shutdown
```

Command history:

Release	Modification
11.00.03	The "*shutdown*" command was introduced as of version 11.00.03.

2.8.19 EXIT

Exits the radio profile configuration menu.

Syntax:

```
WNMS Radio-x config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.9 WTP configuration

The WTP configuration menu is used to configure parameters associated with a given AP. Enter **WTP <mac-address>** (WTP configuration menu) to configure a particular WTP.

Syntax:

```
WNMS config>wtp


WNMS WTP config>?
  no      Negate a command or set its defaults
  wtp     Wireless Termination Point configuration
  exit
```

Example:

Access the configuration for the AP with MAC address 11-22-33-44-55-66:

```
WNMS config>wtp


WNMS WTP config>wtp 11-22-33-44-55-66


WNMS WTP-11-22-33-44-55-66 config>
```

The following table summarizes the WTP configuration commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
CAPWAP-ENCRYPTED	Allows CAPWAP communication to be encrypted.
DESCRIPTION	Configures a description for the access point.
LOCATION	Configures a location for the access point.
MANAGE	Manages the access point.
NAME	Configures a name for the access point.
NO	Resets parameters to their default value, disables options or deletes the configuration.
RADIO	Accesses the radio interface configuration menu.
EXIT	Exits the WTP configuration menu.

2.9.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*? (Help)*" command was introduced as of version 11.00.03.

2.9.2 CAPWAP-ENCRYPTED

Allows CAPWAP communication to be encrypted. CAPWAP is used to manage the different access points. Disabling encrypted is usually used for debugging purposes only.

Syntax:

```
WNMS WTP-x config>capwap-encrypted
```

CAPWAP is encrypted by default.

Example:

Enable CAPWAP encrypted:

```
WNMS WTP-11-22-33-44-55-66 config>capwap-encrypted
```

Command history:

Release	Modification
11.00.03	The "*capwap-encrypted*" command was introduced as of version 11.00.03.

2.9.3 DESCRIPTION

Configures a description for the access point.

Syntax:

```
WNMS WTP-x config>description ?
  <1..63 chars>    Text
```

No description is configured by default.

Example:

```
WNMS WTP-11-22-33-44-55-66 config>description "New 802.11ac AP"
```

Command history:

Release	Modification
11.00.03	The "*description*" command was introduced as of version 11.00.03.

2.9.4 LOCATION

Configures a location for the access point.

Syntax:

```
WNMS WTP-x config>description ?
  <1..63 chars>    Text
```

Default is no location configured.

Example:

```
WNMS WTP-11-22-33-44-55-66 config>location "First floor"
```

Command history:

Release	Modification
11.00.03	The "*location*" command was introduced as of version 11.00.03.

2.9.5 MANAGE

Manages the access point. The whole configuration is controlled by the AC.

Syntax:

```
WNMS WTP-x config>manage
```

The access point is managed by default.

Example:

Manage an access point:

```
WNMS WTP-11-22-33-44-55-66 config>manage
```

Command history:

Release	Modification
11.00.03	The "*manage*" command was introduced as of version 11.00.03.

2.9.6 NAME

Configures a name for the access point.

Syntax:

```
WNMS WTP-x config>name ?
  <1..63 chars>    Text
```

No name is configured by default.

Example:

```
WNMS WTP-11-22-33-44-55-66 config>name AP1
```

Command history:

Release	Modification
11.00.03	The "*name*" command was introduced as of version 11.00.03.

2.9.7 NO

Resets parameters to their default value, disables options or deletes the configuration.

Example:

Delete a description:

```
WNMS WTP-11-22-33-44-55-66 config>no description
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.9.8 RADIO

Accesses the radio interface configuration menu.

Syntax:

```
WNMS WTP-x config>radio ?
  <1..2>    Value in the specified range
```

Each radio interface is identified by a number. If the access point only has one radio, then only radio 1 makes sense.

Example:

Access the configuration of the first radio interface:

```
WNMS WTP-11-22-33-44-55-66 config>radio 1


WNMS WTP-11-22-33-44-55-66.1 config>
```

Command history:

Release	Modification
11.00.03	The "*radio*" command was introduced as of version 11.00.03.

2.9.9 EXIT

Exits the WTP configuration menu.

Syntax:

```
WNMS WTP-x config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.10 WTP radio configuration

The WTP radio configuration menu is used to configure a specific radio interface of the AP. Enter **radio <id>** (WTP configuration menu) to configure a particular radio interface.

Example:

Access configuration for radio interface 1:

```
WNMS WTP-11-22-33-44-55-66 config>radio 1


WNMS WTP-11-22-33-44-55-66.1 config>
```

The following table summarizes the WTP radio configuration commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
BSS-PROFILE	Assigns a BSS profile to the radio interface.
CHANNEL	Configures radio channels to use.
NO	Resets parameters to their default value, disables options or deletes the configuration.
RADIO-PROFILE	Assigns a radio profile to the radio interface.
SHUTDOWN	Disables the radio interface.
TX-POWER	Configures transmit power.
EXIT	Exits the WTP radio configuration menu.

2.10.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*? (Help)*" command was introduced as of version 11.00.03.

2.10.2 BSS-PROFILE

Assigns a BSS profile to the radio interface. More than one BSS profile can be assigned to a radio interface for several wireless networks to operate in the same access point.

Syntax:

```
WNMS WTP-x.y config>bss-profile ?
  <1..2147483647>    Value in the specified range
```

Example:

Assign BSS profiles 1 and 5 to radio interface:

```
WNMS WTP-11-22-33-44-55-66.1 config>bss-profile 1
WNMS WTP-11-22-33-44-55-66.1 config>bss-profile 5
```

Note

The BSS profile must have already been created before it can be assigned to a radio interface.

Command history:

Release	Modification
11.00.03	The "*bss-profile*" command was introduced as of version 11.00.03.

2.10.3 CHANNEL

Configures radio channels to use.

The number of channels you can select depends on the country setting.

Syntax:

```
WNMS WTP-x.y config>>channel ?
  number       Channel number
      <1..200>    Radio channel
  secondary    Secondary channel for 40MHz deployments
      above    Secondary channel above primary channel
      below    Secondary channel below primary channel
```

number

Selects the channel number to use.

Configuring the network name (SSID) logically separates wireless networks, but they can still physically interfere with each other if they are operating on the same wireless channel (or on closely adjacent ones). If you are operating two or more radio networks close to each other, it is advisable to allocate the networks to different channels. Each of these should be spaced at least four channels apart to avoid interference.

When manually selecting the channel, please make sure that the APs actually support the selected channels first.

Possible values (according to the selected wireless module profile):

- For the **2.4 GHz** band:

  Possible values range from 1 to 14.
- For the **5 GHz** band:

  Possible values range from 36 to 165. Not all values are available.

Default is auto: the AP selects the best available channel.

secondary

Configures the secondary channel to use. This parameter applies if **40 MHz** channels are used. Possible values:

- above: the secondary channel is above the primary channel.
- below: the secondary channel is below the primary channel.

The default value is below.

Example:

Configure channel 6:

```
WNMS WTP-11-22-33-44-55-66.1 config>channel number 6
```

Example:

Configure channel auto:

```
WNMS WTP-11-22-33-44-55-66.1 config>no channel number
```

Command history:

Release	Modification
11.00.03	The "*channel*" command was introduced as of version 11.00.03.

2.10.4 NO

Resets parameters to their default value, disables options or deletes the configuration.

Example:

Set transmit power to its default value:

```
WNMS WTP-11-22-33-44-55-66.1 config>no tx-power value
```

Command history:

Release	Modification
11.00.03	The "*no*" command was introduced as of version 11.00.03.

2.10.5 RADIO-PROFILE

Assigns a radio profile to the radio interface.

Syntax:

```
WNMS WTP-x.y config>radio-profile ?
  <1..2147483647>    Value in the specified range
```

Example:

Assign radio profile 1 to radio interface:

```
WNMS WTP-11-22-33-44-55-66.1 config>radio-profile 1
```

Note

The radio profile must have already been created before it can be assigned to a radio interface.

Command history:

Release	Modification
11.00.03	The "*radio-profile*" command was introduced as of version 11.00.03.

2.10.6 SHUTDOWN

Disables the radio interface. When the radio interface is disabled, no wireless networks are available.

Syntax:

```
WNMS WTP-x.y config>shutdown
```

The radio interface is enabled by default.

Example:

Disable radio interface:

```
WNMS WTP-11-22-33-44-55-66.1 config>shutdown
```

Command history:

Release	Modification
11.00.03	The "*shutdown*" command was introduced as of version 11.00.03.

2.10.7 TX-POWER

Configures the transmission power.

Syntax:

```
WNMS WTP-x.y config>tx-power value <dBm>
```

The maximum available value is set by default.

Example:

Configure a transmission power of 14 dBm:

```
WNMS WTP-11-22-33-44-55-66.1 config>tx-power value 14
```

Command history:

Release	Modification
11.00.03	The "*tx-power*" command was introduced as of version 11.00.03.

2.10.8 EXIT

Exits the WTP radio configuration menu.

Syntax:

```
WNMS WTP-x.y config>exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

2.11 Autoprofile

The *autoprofile* menu is used to automatically configure a set of WTPs. The WTPs to be configured can be filtered by IP address or mac address. Enter **autoprofile <id>** to configure a particular autoprofile.

Note

Autoprofile configuration takes effect when *manage* is entered. When configuring an autoprofile in the dynamic menu, enter the *manage* command last (since this activates the autoprofile configuration).

Example:

Access configuration for autoprofile1:

```
WNMS config>autoprofile
WNMS Autoprofile config>autoprofile 1
WNMS Autoprofile-1 config>
```

The following table summarizes the autoprofile configuration commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
DESCRIPTION	Description of the WTP(s)
DHCP-AWARE	Configure WTP(s) with a DHCP-leased IP address
IP-RANGE	Filter WTP(s) by IP range
LOCATION	Location of the WTP(s)
MAC-ADDR	Filter WTP(s) by MAC address
MANAGE	Enable WTP autoconfiguration
NO	Resets parameters to their default value, disables options or deletes the configuration.

RADIO	Radio module
EXIT	Exits the autoprofile configuration menu.

Command history:

Release	Modification
11.01.08	The "*autoprofile*" menu was introduced as of version 11.01.08.

2.11.1 DESCRIPTION

Description of the WTPs managed by the autoprofile.

Syntax:

```
WNMS Autoprofile-x config>description ?
  <1..63 chars>    Text
```

Command history:

Release	Modification
11.01.08	The "*description*" command was introduced as of version 11.01.08.

2.11.2 DHCP-AWARE

Automatically configures the WTPs whose IP address has been assigned by the DHCP server installed on the router. This command replaces the *ip-range* and *mac-addr* filters. The IP address must belong to an active DHCP lease to validate the access point request and for it to be configured automatically.

Syntax:

```
WNMS Autoprofile-x config>dhcp-aware
```

Command history:

Release	Modification
11.01.08	The "*dhcp-aware*" command was introduced as of version 11.01.08.

2.11.3 IP-RANGE

Specifies the WTP subnet the autoprofile feature must configure automatically. By default, the value is 255.255.255.255 with mask 255.255.255.255 (meaning that no WTP discovered will be automatically configured).

Note

This filter *does not* annul the mac address filter. As a result, if the mac address of the discovered WTP matches the mac address filter, it will be automatically configured via *autoprofile* (regardless of the result of the IP address filter).

Syntax:

```
WNMS Autoprofile-x config>ip-range ?
  <a.b.c.d>    IP base address
WNMS Autoprofile-x config>ip-range x.x.x.x ?
  <a.b.c.d>    Address mask
```

Example:

Set *autoprofile* to configure the WTPs belonging to subnet 4.3.2.0/24:

```
WNMS Autoprofile-1 config>ip-range 4.3.2.0 255.255.255.0
```

Command history:

Release	Modification
11.01.08	The "*ip-range*" command was introduced as of version 11.01.08.

2.11.4 LOCATION

Location of the WTPs managed by the *autoprofile* feature.

Syntax:

```
WNMS Autoprofile-x config>location ?
  <1..63 chars>    Text
```

Command history:

Release	Modification
11.01.08	The "*location*" command was introduced as of version 11.01.08.

2.11.5 MAC-ADDR

Sets a mac address filter on the discovered WTPs that the *autoprofile* feature has to configure automatically. By default, its value is ff:ff:ff:ff:ff:ff (meaning the mac address of the discovered WTPs has to match this value to be automatically configured). A 00:00:00:00:00:00 value would mean the *autoprofile* feature has to configure every mac address.

Note

This filter *does not* annul the IP range filter. As a result, if the IP address of the discovered WTP matches the IP range filter, it will be automatically configured via *autoprofile* (regardless of the result of the mac address filter).

Syntax:

```
WNMS Autoprofile-x config>mac-addr ?
  <mac>    MAC format
```

Example:

Configure the discovered WTP with mac address 00:01:02:03:04:05:

```
WNMS Autoprofile-1 config>mac-addr 00:01:02:03:04:05
```

Command history:

Release	Modification
11.01.08	The "*mac-addr*" command was introduced as of version 11.01.08.

2.11.6 MANAGE

Enables or disables the *autoprofile* feature. If disabled, it will not automatically configure new discovered WTPs. It is *disabled* by default and should be the last command introduced in an autoprofile configuration (since this activates it).

Syntax:

```
WNMS Autoprofile-x config>manage
```

Command history:

Release	Modification
11.01.08	The "*manage*" command was introduced as of version 11.01.08.

2.11.7 RADIO

Configures parameters associated with a radio interface. Enter **radio <id>** (radio configuration menu) to configure a particular radio profile.

Syntax:

```
WNMS Autoprofile-x config>radio ?
  <1..2>    Value in the specified range
```

Example:

Access configuration for radio interface 1:

```
WNMS Autoprofile-1 config>radio 1
WNMS Autoprofile-1.1 config>
```

The following table summarizes the autoprofile radio configuration commands. These commands are further explained in the following sections.

Command	Function
? (HELP)	Displays the configuration commands or their options.
BSS-PROFILE	Assigns a BSS profile to the radio interface.
NO	Resets parameters to their default value, disables options or deletes the configuration.
RADIO-PROFILE	Assigns a radio profile to the radio interface.
SHUTDOWN	Disables the radio interface.
EXIT	Exits the autoprofile radio configuration menu.

Command history:

Release	Modification
11.01.08	The "*radio*" command was introduced as of version 11.01.08.

2.11.7.1 BSS-PROFILE

Assigns a BSS profile to the radio interface. More than one BSS profile can be assigned to a radio interface for several wireless networks to operate in the same access point.

Syntax:

```
WNMS Autoprofile-x.y config>bss-profile ?
  <1..2147483647>    Value in the specified range
```

Example:

Assign BSS profiles 1 and 5 to radio interface:

```
WNMS Autoprofile-1.1 config>bss-profile 1
WNMS Autoprofile-1.1 config>bss-profile 5
```

Note

The BSS profile must have already been created before it can be assigned to a radio interface.

Command history:

Release	Modification
11.01.08	The "*bss-profile*" command was introduced as of version 11.01.08.

2.11.7.2 RADIO-PROFILE

Assigns a radio profile to the radio interface.

Syntax:

```
WNMS Autoprofile-x.y config>radio-profile ?
  <1..2147483647>    Value in the specified range
```

Example:

Assign radio profile 1 to radio interface:

```
WNMS Autoprofile-1.1 config>radio-profile 1
```

Note

The radio profile must have already been created before it can be assigned to a radio interface.

Command history:

Release	Modification
11.01.08	The "*radio-profile*" command was introduced as of version 11.01.08.

2.11.7.3 SHUTDOWN

Disables the radio interface. When the radio interface is disabled, no wireless networks are available.

Syntax:

```
WNMS Autoprofile-x.y config>shutdown
```

The radio is enabled by default.

Example:

Disable radio interface:

```
WNMS Autoprofile-1.1 config>shutdown
```

Command history:

Release	Modification
11.01.08	The "*shutdown*" command was introduced as of version 11.01.08.

Chapter 3 Monitoring

3.1 Accessing the Monitoring

To access the monitoring menu for a subinterface, enter **feature wnms** (found in the main monitoring menu).

Example:

```
+feature wnms

--  WNMS Console  --
WNMS+
```

3.2 Monitoring Commands

This section summarizes the monitoring commands available in the Wireless Network Management System monitoring menu.

Command	Function
? (HELP)	Displays the configuration commands or their options.
ACTION	Invokes different actions on the managed WTPs.
CLEAR	Clears information regarding WNMS.
LIST	Displays miscellaneous information.
NO	Undoes a monitoring command.
SAVE	Saves information regarding WNMS.
EXIT	Exits the WNMS monitoring menu.

3.2.1 ? (HELP)

Displays the available commands or their options.

Command history:

Release	Modification
11.00.03	The "*? (Help)*" command was introduced as of version 11.00,03.

3.2.2 ACTION

Invokes different actions on the managed WTPs.

Syntax:

```
WNMS+action ?
  channel-reallocation   Run channel reallocation
  firmware-update        Firmware update
  scan                   Search for neighbor APs
  state                  Get state
  stop-firmware-update   Stop ongoing firmware updates
```

3.2.2.1 ACTION CHANNEL-REALLOCATION

Forces managed WTPs to run the automatic channel selection algorithm to select new channels to operate in. This action can be invoked, for instance, when a new access point has been added.

Syntax:

```
WNMS+action channel-reallocation [<cr>|<mac-address>]
```

If no additional option is selected, channel reallocation is performed on all managed WTPs. If only one WTP needs channel reallocation, specify the MAC address for that particular WTP.

Example:

Force all managed access points to reselect their operating channel.

```
WNMS+action channel-reallocation
```

Example:

Force access point with MAC address 11-22-33-44-55-66 to reselect its operating channel.

```
WNMS+action channel-reallocation 11-22-33-44-55-66
```

Command history:

Release	Modification
11.00.03	The "*action channel-reallocation*" command was introduced as of version 11.00.03.

3.2.2.2 ACTION FIRMWARE-UPDATE

Updates the firmware of managed WTPs.

Syntax:

```
WNMS+action firmware-update <url> [<cr>|<mac-address>]
```

url	The WTP retrieves the new firmware from this URL.
mac-address	If no additional option is selected, firmware updating is performed on all managed WTPs. If only one WTP needs a firmware update, specify the MAC address for that particular WTP.

Example:

Update firmware for the access point with MAC address 11-22-33-44-55-66. The new firmware is localed in a host PC at tftp://192.168.1.1/b19110p02.vig

```
WNMS+action firmware-update tftp://192.168.1.1/bl9110p02.wiq 11-22-33-44-55-66
```

Note

When a WTP reports an error, the updating process is performed repeatedly until the WTP is successfully updated, or until it is canceled by **stop-firmware-update**.

Command history:

Release	Modification
11.00.03	The "*action firmware-update*" command was introduced as of version 11.00.03.

3.2.2.3 ACTION SCAN

Forces managed WTPs to scan all channels for nearby wireless networks. A warning is displayed stating that access point performance may be affected during the scanning period.

Syntax:

```
WNMS+action scan [<cr>|force]
```

If no additional option is selected, the user is asked to confirm he/she wants to continue with the scan process. To bypass confirmation prompt, use the **force** option.

Example:

Scan for nearby wireless networks.

```
WNMS+action scan
CLI Warning: Warning!

If you continue all radio modules of the Access Points will be inactive for a certain time.

Continue?(Yes/No)? y
```

Command history:

Release	Modification
11.00.03	The "*action scan*" command was introduced as of version 11.00.03.

3.2.2.4 ACTION STATE

Managed WTPs are requested to send all configuration parameters to a file in the specified URL. The filename is made up of the WTP MAC address with extension *.cf*.

Syntax:

```
WNMS+action state <url> [<cr>|<mac-address>]
```

url	The WTP sends the state to this URL.
mac-address	If no additional option is selected, the state request is performed on all managed WTPs. If only one WTP needs to be requested, specify the MAC address of that particular WTP.

Example:

Request state for the access point with MAC address 11-22-33-44-55-66. Store it on host PC at 192.168.1.1

```
WNMS+action state 192.168.1.1 11-22-33-44-55-66
```

The state is stored in a file named 112233445566.cf

Command history:

Release	Modification
11.00.03	The "*action state*" command was introduced as of version 11.00.03.

3.2.2.5 ACTION STOP-FIRMWARE-UPDATE

Cancels any ongoing firmware updating of the managed WTPs.

Syntax:

```
WNMS+action stop-firmware-update [<cr>|<mac>]
```

mac	If no additional option is selected, the firmware updating of all managed WTPs is canceled. If only the firmware updating process of one WTP needs to be canceled, specify the MAC address for that particular WTP.

Note

The updating process of WTPs that have already begun to read and save the new firmware is not interrupted. To load the new firmware, said WTPs must be restarted manually.

Command history:

Release	Modification
11.00.07	The "*action stop-firmware-update*" option was introduced as of version 11.00.07.
11.01.02	The "*action stop-firmware-update*" option was introduced as of version 11.01.02.
11.01.01.70.05	The "*action stop-firmware-update*" option was introduced as of version 11.01.01.70.05.

3.2.3 CLEAR

Clears information relative to WNMS.

Syntax:

```
WNMS+clear ?
  wtp-info    Clean persistent WTP information
```

3.2.3.1 CLEAR WTP-INFO

Clears WTP information stored in the permanent memory.

For every managed WTP, the AC gathers information on the MAC address, the radio interface and the channel used. This information is saved into the non-volatile memory through **save wtp-info.** So, if the AC reboots, channel allocation remains the same.

The information stored in the non-volatile memory can be deleted by running **clear wtp-info.**

Syntax:

```
WNMS+clear wtp-info
```

Command history:

Release	Modification
11.00.03	The "*clear wtp-info*" command was introduced as of version 11.00.03.

3.2.4 LIST

Displays miscellaneous information.

Syntax:

```
WNMS+list ?
  action               Displays action commands information
  bss                  Displays the known BSS
  client-management    Displays client management information
  clients              Displays the known clients
  discovered-wtps      Displays the discovered WTPs
  global               Displays global parameters
  neighbors            Displays the neighbor APs
  persistent           Displays persistent information
  rogue                Displays rogue information
  wtp                  Displays WTPs information
```

3.2.4.1 LIST ACTION

Displays the current state of the actions invoked through the **action** command.

Syntax:

```
WNMS+list action ?
  status    Action status
```

Example:

```
WNMS+list action status
Index  Action status
-----  -------------
   0   Idle

Index      MAC address    Maintenance status
-----  -----------------  ------------------
   1   00-a0-f9-2c-8f-70  Done
```

Parameter	Description
Action status	Shows the global status of the last action invoked. • **Idle**: operation has finished. • **Selecting channel**: channel reallocation in progress. • **Start scanning**: starting scan for neighboring networks. • **Scanning**: scan in progress.
MAC Address	MAC address of the WTPs on which a maintenance command (either firmware update or request state) has been performed.
Maintenance status	Maintenance status of the last maintenance command (either firmware update or request state) issued. • **Idle**: no command issued. • **Start**: Starting maintenance command. • **Running**: Running maintenance command.

- **Rebooting**: WTP is rebooting with new firmware.
- **Done**: Maintenance command finished successfully.
- **Error**: An error occurred.
- **Stopped**: WTP already has the firmware version.

Note

When a WTP reports an error, the updating process is performed repeatedly until the WTP is successfully updated, or until it is canceled by the **stop-firmware-update** command. This means the status of these WTPs is constantly changing.

Command history:

Release	Modification
11.00.03	The "*list action*" command was introduced as of version 11.00.03.

3.2.4.2 LIST BSS

Shows an overview of the access points that are currently being managed and displays the wireless module assigned to each wireless network.

Syntax:

```
WNMS+list bss
```

Example:

```
WNMS+list bss
Name  Location       SSID            BSSID         Channel   Status
----  ----------  -------------  -----------------  --------  ------
AP1   FirstFloor  WTP_Test_WLAN  02-6f-81-fc-03-08  auto (1)  Up
```

Parameter	Description.
Name	Name of the access point.
Location	Configured location.
SSID	Wireless network identifier.
BSSID	Basic Service Set Identifier: MAC address of the access point.
Channel	Current channels the access point operates in. Along with the channel number, whether the channel has been manually or automatically selected is shown.
Status	Wireless network status: Up if active or Down if inactive

Command history:

Release	Modification
11.00.03	The "*list bss*" command was introduced as of version 11.00.03.

3.2.4.3 LIST CLIENT-MANAGEMENT

Shows information on client management through access points.

Syntax:

```
WNMS+list client-management
```

Example:

```
WNMS+list client-management
Name   Location       SSID            BSSID        Act.clients Band ch. Denied clients(soft/hard)
----  ----------  -------------  -----------------  ----------- --------  -------------------------
AP1   FirstFloor  WTP_Test_WLAN  02-6f-81-fc-03-08     1           0          0/0
```

Parameter	Description
Name	Name of the access point.
Location	Configured location.
SSID	Wireless network identifier.
BSSID	Basic Service Set Identifier: MAC address for the access point.

Act. clients	Number of connected clients.
Band ch.	Number of clients moved to another band by the band steering mechanism.
Denied clients (soft/hard)	Number of clients rejected when trying to connect to the wireless network. **Soft**: number of clients rejected because of the **max-associations soft** configuration parameter. **Hard**: number of clients rejected because of the **max-associations hard** configuration parameter.

Command history:

Release	Modification
11.00.03	The "*list client-management*" command was introduced as of version 11.00.03.

3.2.4.4 LIST CLIENTS

Shows information on the clients connected to the managed access points.

Syntax:

```
WNMS+list clients ?
  wtp         Select WTP
  station     Select client station
  <cr>        Show clients for every WTP
```

3.2.4.4.1 LIST CLIENTS <cr>

Shows information on all clients connected to the managed access points.

Example:

```
WNMS+list clients
Name   Location       SSID             MAC           IP Address       S/N    Tx Bytes  Rx Bytes  Tx discard  Rx discard      Status         Uptime
----   ----------  -------------  -----------------  ---------------  -------  --------  --------  ----------  ----------  -------------  --------------
AP1    FirstFloor  WTP_Test_WLAN  d8-57-ef-23-60-fd  192.168.100.102  -41/-87      1218      1272           0           0  Authenticated  0 d 0 h 0 m 8 s
```

Parameter	Description
Name	Name of the access point the client is connected to.
Location	Configured location of the access point the client is connected to.
SSID	Wireless network identifier the client is connected to.
MAC	Client MAC address.
IP Address	IP address of the client.
S/N	Received signal strength and measured noise levels in dBm.
Tx Bytes	Total number of transmitted bytes.
Rx Bytes	Total number of received bytes.
Tx Discard	Total number of discarded transmit bytes due to bandwidth limitations.
Rx Discard	Total number of discarded receive bytes due to bandwidth limitations.
Status	• **None**: Unknown client status. • **Associating**: Associating with the access point. • **Associated**: Successfully associated. • **Authenticate**: Authenticating with the access point. • **Authenticated**: Successfully authenticated.
Uptime	Total time the client has been connected after successful association.

Command history:

Release	Modification
11.00.03	The "*list clients <cr>*" command was introduced as of version 11.00.03.

3.2.4.4.2 LIST CLIENTS STATION

Shows detailed information about a particular client connected to an access point.

Syntax:

```
WNMS+list clients station <mac-address>
```

Example:

```
WNMS+list clients station d8-57-ef-23-60-fd
MAC address: d8-57-ef-23-60-fd
Index: 1
SSID: WTP_Test_WLAN
IP address: 192.168.100.102
Uptime: 0 d 0 h 21 m 32 s
Last seen: 0 seconds
Tx air time: 26892 microseconds
Rx air time: 198805 microseconds
Tx MSDU: 29
Rx MSDU: 197
Tx bytes: 2478
Rx bytes: 15080
Tx Frames 11 Mbps: 27
Tx Frames 24 Mbps: 0
Tx Frames 54 Mbps: 0
Tx Frames MCS3: 0
Tx Frames MCS7: 2
Tx Frames MCS11: 0
Tx Frames MCS15: 0
Rx Frames 11 Mbps: 12
Rx Frames 24 Mbps: 0
Rx Frames 54 Mbps: 0
Rx Frames MCS3: 15
Rx Frames MCS7: 170
Rx Frames MCS11: 0
Rx Frames MCS15: 0
Tx discards: 0
Rx discards: 0
Signal: -51
Noise: -87
RSSI 1: -56
RSSI 2: -45
RSSI 3: -54
State: Authenticated
Security: WPA-PSK
Rate: 65.0 Mbps
Rx BW 40: Yes
Tx BW 40: Yes
Rx Short Guard Interval: Yes
Tx Short Guard Interval: Yes
```

Parameter	Description
MAC address	MAC address of the client station.
Index	Unique station index.
SSID	Identifier of the wireless network the client is connected to.
IP address	Client IP address.
Uptime	Total time the client has been connected after successful association.
Last seen	Timestamp of the last frame received from this client.
Rx air time	Estimated air time, in microseconds, for frames received from the client station.
Tx air time	Estimated air time, in microseconds, for frames transmitted to the client station.
Tx MSDU	Total number of frames transmitted to the client.
Rx MSDU	Total number of frames received from the client.
Tx Bytes	Total number of bytes transmitted to the client.
Rx Bytes	Total number of bytes received from the client.
Tx Frames 11 Mbps	Number of data frames transmitted to the client at 11 Mbps or less.
Tx Frames 24 Mbps	Number of data frames transmitted to the client at rates between 11 and 24 Mbps.
Tx Frames 54 Mbps	Number of data frames transmitted to the client at rates between 24 and 54 Mbps.
Tx Frames MCS3	Number of HT (High Throughput) data frames transmitted to the client using MCS 3 or less.

Tx Frames MCS7	Number of HT (High Throughput) data frames transmitted to the client using MCS 4 to MCS 7.
Tx Frames MCS11	Number of HT (High Throughput) data frames transmitted to the client using MCS8 to MCS 11.
Tx Frames MCS15	Number of HT (High Throughput) data frames transmitted to the client using MCS 12 to MCS 15.
Rx Frames 11Mbps	Number of data frames received from the client at 11 Mbps or less.
Rx Frames 24 Mbps	Number of data frames received from the client at rates between 11 and 24 Mbps.
Rx Frames 54 Mbps	Number of data frames received from the client at rates between 24 and 54 Mbps.
Rx Frames MCS3	Number of HT (High Throughput) data frames received from the client using MCS 3 or less.
Rx Frames MCS7	Number of HT (High Throughput) data frames received from the client using MCS 4 to MCS 7.
Rx Frames MCS11	Number of HT (High Throughput) data frames received from the client using MCS8 TO MCS 11.
Rx Frames MCS15	Number of HT (High Throughput) data frames received from the client using MCS 12 to MCS 15.
Tx Discards	Total number of discarded transmit bytes due to bandwidth limitations.
Rx Discards	Total number of discarded receive bytes due to bandwidth limitations.
Signal	Signal strength received in dBm.
Noise	Measured noise levels received in dBm.
RSSI1	Signal strength received at the first radio receiver in dBm.
RSSI2	Signal strength received at the second radio receiver in dBm.
RSSI3	Signal strength received at the third radio receiver in dBm.
Status	• **None**: Unknown client status. • **Associating**: Associating with the access point. • **Associated**: Successfully associated. • **Authenticate**: Authenticating with the access point. • **Authenticated**: Successfully authenticated.
Security	Security in use. • **None**: No security • **WEP-40**: WEP cipher with 40-bit length keys. • **WEP-104**: WEP cipher with 104-bit length keys. • **WPA-PSK**: WPA or WPA2 security with PSK. • **WPA**: WPA or WPA2 security with 802.1X.
Rate	Data rate of the latest packet received from the client station in Mbps.
Rx BW 40	Whether the client station is capable of receiving frames using 40 MHz channels.
Tx BW 40	Whether the client station is capable of transmitting frames using 40 MHz channels.
Rx Short Guard Interval	Whether the client station is capable of receiving frames using short guard interval.
Tx Short Guard Interval	Whether the client station is capable of transmitting frames using short guard interval.

Command history:

Release	Modification
11.00.03	The "*list clients station*" command was introduced as of version 11.00.03.

3.2.4.4.3 LIST CLIENTS WTP

Shows information on the clients connected to a particular access point.

Syntax:

```
WNMS+list clients wtp <mac-address>
```

Example:

```
WNMS+list clients wtp 00-a0-f9-2c-8f-70
Name   Location       SSID             MAC           IP Address       S/N    Tx Bytes  Rx Bytes  Tx discard  Rx discard      Status         Uptime
----   ----------  -------------  -----------------  ---------------  -------  --------  --------  ----------  ----------  -------------  ---------------
AP1    FirstFloor  WTP_Test_WLAN  d8-57-ef-23-60-fd  192.168.100.102  -41/-87      1218      1272           0           0  Authenticated  0 d 0 h 0 m 8 s
```

Please refer to the **list clients <cr>** command (shown above) for an explanation on the different information shown.

Command history:

Release	Modification
11.00.03	The "*list clients wtp*" command was introduced as of version 11.00.03.

3.2.4.5 LIST DISCOVERED-WTPS

Shows a list of discovered WTPs. These are access points discovered using CAPWAP that are not being managed by WNMS.

Syntax:

```
WNMS+list discovered-wtps
```

Example:

```
WNMS+list discovered-wtps
       MAC                         Name
-----------------  --------------------------------
00-a0-f9-37-e0-87  W2003n
Found: 1 discovered WTPs
```

Parameter	Description
MAC	MAC address for the access point.
Name	Official name of the access point.

Command history:

Release	Modification
11.00.03	The "*list discovered-wtps*" command was introduced as of version 11.00.03.

3.2.4.6 LIST GLOBAL

Shows global configuration parameters.

Syntax:

```
WNMS+list global
```

Example:

```
WNMS+list global
AC parameters
        Admin Status: Master
        Operational Status: Master
        Max number of WTPs: 10
        Debug level: Verbose
        Action status: Idle
        Initialization of WTPs: Simultaneous
        Maximum number of simultaneous WTP initializations: 10
        Time between statistics: 30 seconds
        Time to wait for config messages before considering AC down: 10 seconds
        Time for a WTP to reboot after losing connection to the AC: 0 seconds
        LED mode: Normal
        Scan results max age: 3600 seconds
AC Statistics
        Discovered WTPs: 2
        Managed WTPs: 1
        Retransmissions: 0
        Rx Bytes: 259051
        Rx Packets: 1070
        Tx Bytes: 31243
        Tx Packets: 623
```

```
CAPWAP parameters
        CAPWAP Change State Pending Timer: 150
        CAPWAP Data Check Timer: 30
        CAPWAP Echo Interval: 10
        CAPWAP Max Retransmissions: 5
        CAPWAP Retransmit Interval: 3
        CAPWAP Wait Join Timer: 60
```

Command history:

Release	Modification
11.00.03	The "*list global*" command was introduced as of version 11.00.03.

3.2.4.7 LIST NEIGHBORS

Shows a list of detected neighbor access points.

Syntax:

```
WNMS+list neighbors
```

Example:

```
WNMS+list neighbors
       MAC          SSID           Security      Signal(dBm)  Channel          Last Seen          Type  Status    Detected by
-----------------  -------------  ------------  -----------  -------  -------------------------  ----  --------  -----------------
d0-xx-xx-xx-xx-xx  Txxxxx         WPA2-PSK             -64       44  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Vxxxxxxxxxxxx  WPA-WPA2-PSK         -88       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
c0-xx-xx-xx-xx-xx  wxxxxxx        WPA-PSK              -84       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -84       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -86       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Vxxxxxxxxxxxx  WPA-WPA2-PSK         -50       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx  Sxxxxxxxxxx    WPA2-PSK             -58       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Vxxxxxxxxxxxx  WPA-WPA2-PSK         -74       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -74       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -52       11  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Vxxxxxxxxxxxx  WPA-WPA2-PSK         -76        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -76        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx  ixxxxxxxx      WPA2-PSK             -47        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx  gxxxxxxx       WPA-PSK              -72        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Txxxxxxxx      WPA2-PSK             -58        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  axxxxxxxxxxxx  WPA-WPA2-PSK         -66        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx  wxxxxxxxxxxxx  WPA2-PSK             -60        6  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx                 WPA-WPA2-PSK         -80        1  Thu, 12 Oct 2014 01:21:46  BSS   Rogue     First Floor-AP 1
00-xx-xx-xx-xx-xx                 WPA-WPA2-PSK         -80        1  Thu, 12 Oct 2014 01:21:46  BSS   Rogue     First Floor-AP 1
00-xx-xx-xx-xx-xx                 WPA-WPA2-PSK         -78        1  Thu, 12 Oct 2014 01:21:46  BSS   Rogue     First Floor-AP 1
02-xx-xx-xx-xx-xx  Vxxxxxxxxxxxx  WPA-WPA2-PSK         -72        1  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -74        1  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Vxxxxxxxxxxxx  WPA-WPA2-PSK         -66        1  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx  Bxxxxxx        none                 -29        1  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
02-xx-xx-xx-xx-xx  Wxxxxxxxxx     WPA-WPA2-PSK         -68        1  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
00-xx-xx-xx-xx-xx  Axxxxxxx       WPA-WPA2-PSK         -60        1  Thu, 12 Oct 2014 01:21:46  BSS   Neighbor  First Floor-AP 1
```

Parameter	Description
MAC	MAC address for the detected access point.
SSID	Wireless network identifier announced by the detected access point.
Security	Security used in the detected wireless network. • **None**: No security. • **WEP**: WEP cipher. • **WPA-PSK**: WPA security with PSK. • **WPA2-PSK**: WPA2 security with PSK. • **WPA-WPA2-PSK** : WPA and WPA2 security with PSK. • **WPA-Enterprise**: WPA security with 802.1X. • **WPA2-Enterprise**: WPA2 security with 802.1X. • **WPA-WPA2-Enterprise** : WPA and WPA2 security with 802.1X.
Signal (dBm)	Signal strength detected in dBm.
Channel	Channel the wireless network is detected in.
Last Seen	Last time the access point was seen.
Type	Type of wireless network detected. • **BSS**: Normal wireless network, makes use of an access point. • **IBSS**: Independent BSS, also called *ad hoc* network. This is made up of client stations with no access point.
Status	Status of the detected wireless network.

	• **Own**: Known access point, managed by the WNMS. • **Neighbor**: Neighbor access point, the detected wireless network does not fit into any of the other categories. • **Rogue**: Unmanaged access point using one of the wireless network identifiers used by the WNMS or with hidden identifier. • **Own manipulated**: Known access point, managed by the WNMS. The configuration has been changed from the one configured in the WNMS. • **Known neighbor**: Well-known neighbor. • **Known rogue**: Well-known rogue access point.
Detected by	Location and name of the managed access point detected by the wireless network.

Command history:

Release	Modification
11.00.03	The "*list neighbors*" command was introduced as of version 11.00.03.

3.2.4.8 LIST PERSISTENT

Shows information that has already been or is about to be stored in the permanent memory.

For every managed WTP, the AC gathers the MAC address, the radio interface and the channel used. This information can be saved into the non-volatile memory through **save wtp-info**. So, if the AC reboots, the channel allocation remains the same.

The information currently stored in the non-volatile memory is displayed through **list persistent wtp-info stored**.

The information to be saved into the non-volatile memory is displayed through **list persistent wtp-info to-store**.

Syntax:

```
WNMS+list persistent wtp-info ?
  stored      Persistent WTP information stored
  to-store    Persistent WTP information to store
```

Example:

```
WNMS+list persistent wtp-info stored
File Address: 0x7fa6700
File Size: 16384

Header File
-----------
id_str: WTP-INFO
version: 1
No WTP info stored
```

Example:

```
WNMS+list persistent wtp-info to-store
Id           MAC       Radio Id  Primary channel  Secondary channel
--  -----------------  --------  ---------------  -----------------
01  00-a0-f9-2c-8f-70  1         11               below
```

Parameter	Description
MAC	MAC address of the access point.
Radio Id	Radio interface identifier.
Primary channel	Channel the AP is operating in.
Secondary channel	For 40 MHz width channels: whether the secondary channel is **above** or **below** the primary channel.

Command history:

Release	Modification
11.00.03	The "*list persistent*" command was introduced as of version 11.00.03.

3.2.4.9 LIST ROGUE CLIENTS

Shows a list of rogue clients. Rogue clients may be added manually, by running **blacklist station** configuration, or dynamically, through the access points (in the event many authentication errors show up).

Syntax:

```
WNMS+list rogue clients
```

Example:

```
WNMS+list rogue clients
Static entries

       MAC                        SSID
-----------------  --------------------------------
11-22-33-44-55-66  WTP_Test_WLAN

Dynamic entries

       MAC              SSID     Detected by   Signal(dBm)   Reason           First Seen                Last Seen
-----------------  -------------  ------------  -----------  --------  ------------------------  ------------------------
02-xx-xx-xx-xx-xx  WTP_Test_WLAN  AP 1                  -64  Bad auth  Thu, 12 Oct 2014 01:15:46  Thu, 12 Oct 2014 01:21:46
```

Parameter	Description
MAC	MAC address for the client station.
SSID	Identifier of the wireless network the client is/was connected to.
Detected by	Name configured for the access point that detected the client station.
Signal (dBm)	Last received signal strength from the client station in dBm.
Reason	Reason to blacklist the client station: • **Bad auth**: a specific number of authentications failed during a certain period of time.
First Seen	The first time the blacklisted client station drew attention.
Last Seen	The last time the blacklisted client station drew attention.

Command history:

Release	Modification
11.00.03	The "*list rogue clients*" command was introduced as of version 11.00.03.

3.2.4.10 LIST WTP

Shows information on managed and discovered access points.

Syntax:

```
WNMS+list wtp ?
  all         Show all known WTPs
  managed     Show managed WTPs
  <mac>       MAC Address of the WTP
```

3.2.4.10.1 LIST WTP ALL

Shows information on all access points configured and discovered.

Example:

```
WNMS+list wtp all
##         MAC           Name  Location       IP Address      Channel    Status
-- --------------------  ----  -----------  ---------------  ---------  -------
01   00-a0-f9-2c-8f-70   AP 1  First Floor  192.168.100.101  auto (11)  Managed
02   11-22-33-44-55-66                                                  Offline
03   22-33-44-55-66-77                                                  Offline
04   00-a0-f9-37-e0-87   AP 2  First Floor  192.168.100.100  auto (0)   Discovered
                                                             auto (0)
```

Parameter	Description
MAC	Access point's MAC address.
Name	Name of access point.
Location	Location of access point.

IP Address	Access point's IP address.
Channel	Channel the access point is operating in. If the access point has more than one radio interface, the channel for every radio interface is shown in different lines.
Status	• **Initializing**: WNMS and the AP communicate via CAPWAP. The configuration is being transferred to the AP. • **Discovered**: AP has registered at the WNMS but is not being managed. • **Managed**: WNMS has sent a configuration to the AP and has enabled it. The AP is managed centrally by the WNMS. • **Offline**: AP is either administratively disabled or not available. • **No license available**: The license in the WNMS does not allow this AP to be managed.

Command history:

Release	Modification
11.00.03	The "*list wtp all*" command was introduced as of version 11.00.03.

3.2.4.10.2 LIST WTP MANAGED

Shows information on the managed access points.

Example:

```
WNMS+list wtp managed
##         MAC           Name  Location       IP Address     Channel    Status
-- --------------------  ----  -----------  ---------------  ---------  -------
01   00-a0-f9-2c-8f-70   AP 1  First Floor  192.168.100.101  auto (11)  Managed
```

For an explanation on the different types of information shown, please see the **list wtp all** command above.

Command history:

Release	Modification
11.00.03	The "*list wtp managed*" command was introduced as of version 11.00.03.

3.2.4.10.3 LIST WTP <mac>

Shows detailed information on a particular access point.

Syntax:

```
WNMS+list wtp <mac-address>
```

Example:

```
WNMS+list wtp 00-a0-f9-2c-8f-70
WTP 00-a0-f9-2c-8f-70 detailed information
Device: bintec W1002n
Location: First Floor
Name: AP 1
Description:
CAPWAP Encryption: Enabled
Serial number: W1NACI012030043
SW version: V.9.1 Rev. 7 (Patch 2) IPSec from 2014/01/20 00:00:00
Index: 1
WTP Index: 1
Address Type 1
IP address: 192.168.100.101
Number of radios: 1
Connect time: 0 d 15 h 35 m 7 s
Rx Packets: 1882
Rx Bytes: 346463
Tx Packets: 1060
Tx Bytes: 45438
Retransmissions: 0
Last seen: Thu, 12 Oct 2000 02:43:00
State: Run
```

```
Admin SW version:
WTP index: 1
Sec index: 2147483647
EAPOL index: 0
Global index: 0
Radius server index: 0
Log Host index: 0
Local Services index: 2147483647
Admin Status: Enabled
Operational Status: Enabled
Trigger Stat: Idle
WTP Stat index: 1
WTP Temperature (C): 47
WTP Free memory (bytes): 77448354
WTP CPU usage (%): 0

Radio module 1
        Operation Mode: On (7)
        Active Radio Profile: 2.4 GHz
        Used Channel: auto (11)
        Channel utilization (%): 9
        Transmit Power: 63
        Radar detections: 0
        Assigned Wireless Networks:
                1: WTP_Test_WLAN (BSSID: 02-6f-81-fc-03-08)
                Basic Rates: 1 2 5.5 11
                Supported Rates: 1 2 54
```

Command history:

Release	Modification
11.00.03	The "*list wtp <mac-address>*" command was introduced.
11.00.06, 11.01.02	Basic and supported rates are displayed.
11.00.07, 11.01.02	New WTP information is displayed: temperature, free memory, CPU usage, channel utilization and radar detections.

3.2.5 SAVE

Saves information on WNMS.

Syntax:

```
WNMS+save ?
  wtp-info    Saves persistent WTP information
```

3.2.5.1 SAVE WTP-INFO

Saves WTP information in the permanent memory.

For every managed WTP, the AC gathers the MAC address, the radio interface and the channel used. This information can be saved into the non-volatile memory by running **save wtp-info**. This way, if the AC reboots, channel allocation remains the same.

The information currently stored in the non-volatile memory is displayed by running **list persistent wtp-info stored**.

The information to be saved into the non-volatile memory can be displayed through **list persistent wtp-info to-store**.

Syntax:

```
WNMS+save wtp-info
```

Command history:

Release	Modification
11.00.03	The "*save wtp-info*" command was introduced as of version 11.00.03.

3.2.6 EXIT

Exits the WNMS configuration menu.

Syntax:

```
WNMS+exit
```

Command history:

Release	Modification
11.00.03	The "*exit*" command was introduced as of version 11.00.03.

Chapter 4 Configuration Example

4.1 Scenario

We're going to use the WNMS to manage two APs: AP1 with MAC address 00-a0-f9-2c.8f.70 and AP2 with MAC address 00-a0-f9-37-e0-87. We'll then create two different wireless networks:

- GuestAccess with WPA-PSK security, available only on the 2.4 GHz band.
- CorporateAccess with WPA2-Enterprise security (802.1X authentication), available in both the 2.4 and 5 GHz bands.

We'll use 40 MHz in the 5 GHz band, and manually select the radio channels so that:

- AP1 uses channel 1 in the 2.4 GHz band and channels 36 and 40 in the 5 GHz band.
- AP2 uses channel 6 in the 2.4 GHz band and channels 44 and 48 in the 5 GHz band.

4.2 Configuration

4.2.1 AAA profiles

First, create an AAA profile for 802.1X authentication.

```
Config>feature wnms

-- Wireless Network Management System configuration --
WNMS config>aaa


WNMS AAA config>aaa 1

WNMS AAA-1 config>radius-server ip-address 192.168.213.45 secret plain whatever
WNMS AAA-1 config>exit
WNMS AAA config>exit
```

4.2.2 Radio profiles

Create two radio profiles, one for each band.

4.2.2.1 2.4 GHz radio profile

Only assign a band and operation mode and give the profile a meaningful description.

```
WNMS config>radio


WNMS radio config>radio 1


WNMS Radio-1 config>band 2.4GHz mode 11bgn
WNMS Radio-1 config>description "2.4GHz band"
WNMS Radio-1 config>exit
WNMS radio config>exit
WNMS config>
```

4.2.2.2 5 GHz radio profile

Band, mode and description are configured. In this case, we also configure channel width to 40 MHz.

```
WNMS config>radio


WNMS radio config>radio 2
```

```
WNMS Radio-2 config>band 5GHz mode 11an
WNMS Radio-2 config>bandwidth 40MHz
WNMS Radio-2 config>description "5GHz band"
WNMS Radio-2 config>exit
WNMS radio config>exit
WNMS config>
```

4.2.3 BSS profiles

Create two BSS profiles, one for guest access and another for corporate access.

4.2.3.1 Guest Access

Configure WPA2-PSK security with AES-CCMP.

```
WNMS config>bss


WNMS BSS config>bss 1


WNMS BSS-1 config>ssid GuestAccess
WNMS BSS-1 config>privacy-invoked
WNMS BSS-1 config>rsn wpa2
WNMS BSS-1 config>akm psk
WNMS BSS-1 config>cipher aes-ccmp
WNMS BSS-1 config>wpa-psk passphrase plain TeStiNg123!
WNMS BSS-1 config>client-isolation
```

4.2.3.2 Corporate Access

Configure WPA security with AES-CCMP. Assign the AAA profile that was previously created to perform 802.1X authentication.

```
WNMS config>bss


WNMS BSS config>bss 2


WNMS BSS-2 config>ssid CorporateAccess
WNMS BSS-2 config>privacy-invoked
WNMS BSS-2 config>rsn wpa2
WNMS BSS-2 config>akm dot1x
WNMS BSS-2 config>cipher aes-ccmp
WNMS BSS-2 config>client-isolation
WNMS BSS-2 config>aaa-profile 1
```

4.2.4 WTP configuration

Now, put it all together in the two WTPs to be managed.

```
WNMS config>wtp


WNMS WTP config>wtp 00-a0-f9-2c-8f-70

WNMS WTP-00-a0-f9-2c-8f-70 config>name AP1
WNMS WTP-00-a0-f9-2c-8f-70 config>location "First Floor"
WNMS WTP-00-a0-f9-2c-8f-70 config>capwap-encrypted
WNMS WTP-00-a0-f9-2c-8f-70 config>radio 1
```

```
WNMS WTP-00-a0-f9-2c-8f-70.1 config>channel number 1
WNMS WTP-00-a0-f9-2c-8f-70.1 config>radio-profile 1
WNMS WTP-00-a0-f9-2c-8f-70.1 config>bss-profile 1
WNMS WTP-00-a0-f9-2c-8f-70.1 config>bss-profile 2
WNMS WTP-00-a0-f9-2c-8f-70.1 config>exit
WNMS WTP-00-a0-f9-2c-8f-70 config>radio 2


WNMS WTP-00-a0-f9-2c-8f-70.2 config>channel number 36
WNMS WTP-00-a0-f9-2c-8f-70.2 config>channel secondary above
WNMS WTP-00-a0-f9-2c-8f-70.2 config>radio-profile 2
WNMS WTP-00-a0-f9-2c-8f-70.2 config>bss-profile 2
WNMS WTP-00-a0-f9-2c-8f-70.2 config>exit
WNMS WTP-00-a0-f9-2c-8f-70 config>exit
WNMS WTP config>wtp 00-a0-f9-37-e0-87


WNMS WTP-00-a0-f9-37-e0-87 config>name AP2
WNMS WTP-00-a0-f9-37-e0-87 config>location "First Floor"
WNMS WTP-00-a0-f9-37-e0-87 config>capwap-encrypted
WNMS WTP-00-a0-f9-37-e0-87 config>radio 1


WNMS WTP-00-a0-f9-37-e0-87.1 config>channel number 6
WNMS WTP-00-a0-f9-37-e0-87.1 config>radio-profile 1
WNMS WTP-00-a0-f9-37-e0-87.1 config>bss-profile 1
WNMS WTP-00-a0-f9-37-e0-87.1 config>bss-profile 2

WNMS WTP-00-a0-f9-37-e0-87.1 config>exit
WNMS WTP-00-a0-f9-37-e0-87 config>radio 2


WNMS WTP-00-a0-f9-37-e0-87.2 config>channel number 44
WNMS WTP-00-a0-f9-37-e0-87.2 config>channel secondary above
WNMS WTP-00-a0-f9-37-e0-87.2 config>radio-profile 2
WNMS WTP-00-a0-f9-37-e0-87.2 config>bss-profile 1
WNMS WTP-00-a0-f9-37-e0-87.2 config>exit
WNMS WTP-00-a0-f9-37-e0-87 config>exit
```

4.2.5 Global configuration

Finally, enable WNMS.

```
WNMS config>enable
```

4.2.6 Final WNMS configuration

The whole WNMS configuration should look like this:

```
; -- Wireless Network Management System configuration --
      enable
      aaa
         aaa 1
            radius-server ip-address 192.168.213.45 secret plain whatever
;
         exit
;
      exit
;
      bss
         bss 1
            ssid GuestAccess
            privacy-invoked
            akm psk
            cipher aes-ccmp
            client-isolation
            rsn wpa2
```

```
            wpa-psk passphrase plain TeStiNg123!
         exit
;
         bss 2
            ssid CorporateAccess
            privacy-invoked
            aaa-profile 1
            akm dot1x
            cipher aes-ccmp
            client-isolation
            rsn wpa2
         exit
;
      exit
;
      radio
         radio 1
            band 2.4GHz mode 11bgn
            description "2.4GHz band"
         exit
;
         radio 2
            band 5GHz mode 11an
            bandwidth 40MHz
            description "5GHz band"
         exit
;
      exit
;
      wtp
         wtp 00-a0-f9-2c-8f-70
            location "First Floor"
            name AP1
            radio 1
               radio-profile 1
               bss-profile 1
               bss-profile 2
;
               channel number 1
            exit
;
            radio 2
               radio-profile 2
               bss-profile 2
;
               channel number 36
               channel secondary above
            exit
;
         exit
;
         wtp 00-a0-f9-37-e0-87
            location "First Floor"
            name AP2
            radio 1
               radio-profile 1
               bss-profile 1
               bss-profile 2
;
               channel number 6
            exit
;
            radio 2
               radio-profile 2
               bss-profile 2
;
               channel number 44
```

```
               channel secondary above
            exit
;
         exit
;
      exit
```

4.2.7 DHCP configuration

To manage the WTPs, option 138 must be used to share the AC address with the WTPs. This section includes a configuration example. For more information on DHCP configuration, please see manual Teldat Dm730-I DHCP Protocol.

In the following example, we will configure a range that goes from 192.168.100.100 to 192.168.100.110. Moreover, we will set option 138 so that the AC address is 192.168.100.1 (hexadecimal value 0xc0a86401).

```
   protocol dhcp
; -- DHCP Configuration --
      server
; -- DHCP Server Configuration --
         enable
;
         shared 1
;
         subnet wifi 1 network 192.168.100.0 255.255.255.0
         subnet wifi 1 range 192.168.100.100 192.168.100.110
         subnet wifi 1 dns-domain company
         subnet wifi 1 dns-server 8.8.8.8
         subnet wifi 1 router 192.168.100.1
         subnet wifi 1 subnet-mask 255.255.255.0
         subnet wifi 1 option 138 hex c0a86401
         exit
;
   exit
```